BayRS Version 15.6.0.0

Part No. 314470-15.6 Rev 00
March 2005

600 Technology Park Drive
Billerica, MA 01821-4130

BayRS Version 15.6.0.0 Document Change Notice

314470-15.6 REV 00

NORTEL NETWORKS™

Copyright © 2005 Nortel Networks

Trademarks

Restricted Rights Legend

Statement of Conditions

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

Chapter 7
Configuring DLSw Services

Chapter 13
Configuring IP Multicasting and Multimedia Services

Chapter 14
Configuring PPP Services

Chapter 15
Configuring RADIUS

Preface

BayRS* Version 15.6.0.0 is a software release that includes bug fixes and new features added since BayRS Version 15.5.0.0. This document change notice contains additions and amendments to the following BayRS publications since Version 15.1.0.0:

- *BayRS Online Library*
- *Configuring and Managing Routers with Site Manager*
- *Configuring ATM Services*
- *Configuring Bridging Services*
- *Configuring Data Compression Services*
- *Configuring Differentiated Services*
- *Configuring DLSw Services*
- *Configuring Ethernet, FDDI, and Token Ring Services*
- *Configuring Frame Relay Services*
- *Configuring GRE, NAT, RIPSO, and BFE Services*
- *Configuring IP, ARP, RARP, RIP, and OSPF Services*
- *Configuring IP Exterior Gateway Protocols (BGP and EGP)*
- *Configuring IP Multicasting and Multimedia Services*
- *Configuring PPP Services*
- *Configuring RADIUS*
- *Configuring Traffic Filters and Protocol Prioritization*
- *Configuring VRRP Services*
- *Configuring X.25 Services*

- *Quick-Starting Routers*
- *Reference for BCC IP show Commands*
- *Upgrading Routers to BayRS Version 15.x*
- *Using Technician Interface Scripts*
- *Using Technician Interface Software*
- *Using the Bay Command Console (BCC)*

Before You Begin

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

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring Remote Access for AN and Passport ARN Routers*, or *Connecting ASN Routers to a Network).*

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

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter **ping 192.32.10.12**.
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.

braces ({ })

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is:
show ip {**alerts** | **routes**}, you must enter either:
show ip alerts or **show ip routes**, but not both.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is:
show ip interfaces [**-alerts**], you can enter either:
show ip interfaces or **show ip interfaces -alerts**.

italic text

Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: If the command syntax is:
show at <*valid_route*>, *valid_route* is one variable and you substitute one value for it.

separator (>)

Shows menu paths.

Example: Protocols > IP identifies the IP option on the Protocols menu.

vertical line (|)

Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.

Example: If the command syntax is:
show ip {**alerts** | **routes**}, you enter either:
show ip alerts or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
AS	autonomous system
ASE	autonomous system external
ATM	asynchronous transfer mode
BGP	Border Gateway Protocol
DLSw	data link switching
DSCP	differentiated services code point
DSQMS	differentiated services queue management and scheduling
ECMP	equal-cost multipath
FDDI	Fiber Distributed Data Interface
GRE	Generic Routing Encapsulation
HSSI	High Speed Serial Interface
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
LCP	Link Control Protocol
LLC	logical link control
LMI	Local Management Interface
LQM	Link Quality Monitoring
LQR	Link Quality Report
LSA	link state advertisement
LSDB	link state database
MIB	management information base
MTU	maximum transmission unit

NAT	Network Address Translation
NLPID	network layer protocol identifier
NSSA	not-so-stubby area
OSPF	Open Shortest Path First
PBBI	PIM bootstrap border interface
PBBR	PIM bootstrap border router
PIM	Protocol Independent Multicast
PMC	PCI mezzanine card
PPP	Point-to-Point Protocol
PVC	permanent virtual circuit
QLLC	Qualified Logical Link Control
QoS	quality of service
RADIUS	Remote Access Dial-In User Services
RARP	Reverse Address Resolution Protocol
RED	random early detection
RIP	Routing Information Protocol
RP	rendezvous point
SM	sparse mode
SNMP	Simple Network Management Protocol
SSM	source-specific multicast
SRB	source route bridge
SVC	switched virtual circuit
ToS	type of service
VC	virtual circuit
VRRP	Virtual Router Redundancy Protocol

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

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortel.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortel.com/help/contact/erc/index.html URL.

Chapter 1
BayRS Online Library CD

The *BayRS Online Library* documentation CD (Part No. 314472-A) was last updated for BayRS Version 15.2.0.0. This document change notice contains amendments to the BayRS software manuals since BayRS Version 15.1.0.0. Any hardware guide that has been revised since the final documentation CD was released is posted on the Nortel Networks Technical Support site.

Accessing Nortel Networks Documentation on the Web

To access the latest version of BayRS hardware and software documents on the Nortel Networks Technical Support Web page:

1. Go to the Technical Support URL www.nortel.com/support.
2. Click on the “Browse product support” tab.
3. From the Product Families list, choose “BayRS Routers.”
4. From the Product list, choose the hardware platform for which you need documentation (for example, Multiprotocol Router 5430).

Note: The Passport 5430 and the Passport 2430 are now referred to as the Multiprotocol Router 5430 and the Multiprotocol Router 2430.

5. From the Content list, choose “Documentation” and then click on Go.

On the resulting documentation page, you can use keywords or menu options to search for specific documents. You can view, print, and download any document from the Web site.

Chapter 2
Configuring and Managing Routers with Site Manager

Version 15.3.0.0

The following section is an amendment to Chapter 7, “Monitoring Trap and Event Messages,” in *Configuring and Managing Routers with Site Manager.*

Changing the Trap Port for Multiple Network Management Applications

If you are running more than one network management application on your Site Manager workstation, you must configure Site Manager to receive trap messages from the SNMP agent on a port other than the default port, 162. This is necessary for the following reasons:

- The agent can only send trap messages to one network management application at a time.
- Only one application can map to a UDP port at a time.

  By default, the network management application on your workstation is assigned to User Datagram Protocol (UDP) port 162. This port is dedicated to receiving SNMP trap messages from the SNMP agent.

  Site Manager is the preferred network management application for receiving trap messages. To avoid any problems when running another network management application, Nortel Networks recommends that you configure Site Manager to map to an alternative UDP port. This allows you to send trap messages to Site Manager directly.

To reconfigure the trap port:

1. **In the Configuration Manager window, choose Protocols > IP > SNMP > Communities.**

   The SNMP Community List window opens.

2. **Choose Community > Managers.**

   The SNMP Manager List window opens.

3. **Choose Manager > Edit Manager.**

   The Trap Port and Trap Types window opens.

4. **Type a new port number for the Trap Port parameter, then click on OK.**

   You can enter any port number on your Site Manager workstation, as long as another application is not using that port.

   You return to the Configuration Manager window.

5. **Choose File > Save to save this configuration file.**

   See Chapter 3 in *Configuring and Managing Routers Using Site Manager* for instructions on saving configuration files.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

7. **Restart Site Manager according to the instructions in Chapter 1 of *Configuring and Managing Routers Using Site Manager*.**

   To make sure that Site Manager is able to listen to the port that you configured in step 4, restart Site Manager using the **wfsm -e** command or the Trap Monitor using the **wftraps -e** command. For more information, about using the **wfsm** and **wftraps** commands with the **-e** option, see Appendix A in *Configuring and Managing Routers with Site Manager*.

Note: You can also change the trap port on a PC by editing the snmp-trap 162/udp snmp string in the Services file. From the Start menu, choose **Programs** > **Windows Explorer**. Open the Services file and edit the string snmp-trap 162/udp snmp. For example, to change the trap port from 162 to 779, enter **snmp-trap 779/udp snmp** and reboot the PC. Site Manager PC is then able to receive the traps from the router on port 779.

Chapter 3
Configuring ATM Services

Version 15.2.0.0

The following section is new to *Configuring ATM Services*. You use the procedures in this section to configure an ATM T3/E3 PMC module installed in a Passport* 5430. For information about installing an ATM T3/E3 PMC module, see *ATM T3/E3 PMC Module Supplement*.

Creating an ATM Circuit for a T3 or E3 Connection on a Passport 5430

To start ATM services on an ATM T3/E3 PMC module in the Passport 5430, you do the following:

1. Configure the physical ATM circuit.
2. Add protocols and other services to that circuit.

This section describes how you create a physical ATM circuit for a T3 or E3 connection on a Passport 5430, then directs you to *Configuring ATM Services* for information about adding protocols and further configuring ATM services.

Using the BCC

To add ATM to a Passport 5430 with a T3/E3 connector, navigate to the box prompt and enter:

atm slot *<slot_number>* **pci-slot** *<pci_slot>* **module** *<module_number>* **connector** *<connector_number>* **mode** {**t3** | **e3**}

slot_number is the number of the chassis slot containing the ATM T3/E3 PMC module.

pci_slot is the number of the PCI slot containing the ATM T3/E3 PMC module. The PCI slot number for the ATM T3/E3 PMC module is always 1.

module_number is always 2 for the ATM interface.

connector_number is the number of a connector on the ATM T3/E3 PMC module.

mode t3 or **mode e3** specifies whether the ATM interface is a T3 or E3 interface.

For example, the following command adds an ATM T3 interface to the Passport 5430 configuration on slot 1, PCI slot 1, module 2, connector 1:

```
box# atm slot 1 pci-slot 1 module 2 connector 1 mode t3
atm/1/1/2/1#
```

To configure T3/E3 parameters, use the following procedures.

Specifying the Cable Length

To specify the cable length, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

cable-length *<length>*

length is either short (default) or long. Specify short for a cable less than 225 feet long; specify long for a cable length of 225 feet or more.

For example, the following command changes the cable length to long:

```
atm-e3/1/1/2/1# cable-length long
atm-e3/1/1/2/1#
```

Specifying the Clear Alarm Threshold

To specify the duration of time (in seconds) that elapses following the clearing of a performance failure (before the condition is registered and logged), navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

clear-alarm-threshold *<integer>*

integer is a value from 2 through 10 seconds, inclusive.

For example, the following command changes the clear alarm threshold from 2 to 8 seconds:

atm-e3/1/1/2/1# **clear-alarm-threshold 8**
atm-e3/1/1/2/1#

Specifying the Line Coding Method

To specify the line coding method, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

line-coding {hdb3 | b3zs}

The default for the ATM E3 interface is hdb3 and the default value for the ATM T3 interface is b3zs.

Specifying the Line Type

To specify the line type for this interface, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

line-type *<type>*

type is autodetect, ds3m23, or ds3cbitparity for the ATM T3 interface and e3framed or e3plcp for the ATM E3 interface.

If the line type is ds3m23, the framing mode should be m23 or t3m23plcp.

If the line type is ds3cbitparity, the framing mode should be cbit or t3cbitplcp.

If the line type is either e3framed or e3plcp, the framing mode should be either g751or g832.

For instructions on setting the framing-mode parameter, see *Configuring ATM Services.*

Specifying the Loopback Mode

To force the interface into loopback mode so that the far-end or intermediate equipment can perform diagnostics on the network between that equipment and the T3/E3 interface, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

loopback-mode *<type>*

type is payloadloop or lineloop.

If you select payloadloop, the received signal at this interface is looped through the device. Typically, the received signal is looped back for retransmission after it has passed through the device's framing function.

If you select lineloop, the received signal at this interface does not go through the framing device (minimum penetration) but is looped back out. The default is noloop.

For example, the following command changes the loopback mode to payloadloop:

```
atm-e3/1/1/2/1# loopback-mode payloadloop
atm-e3/1/1/2/1#
```

Defining the Interface MTU

The maximum transmission unit (MTU) is the largest possible unit of data that the physical medium can transmit. By default, the interface allows an MTU size of 4608 octets. This value can handle most packet sizes. However, you can set the MTU to any value from 3 through 4608 octets.

To modify the interface MTU, navigate to the ATM interface prompt (for example,
box; **atm/1/1/2/1**; **atm-e3**) and enter:

mtu *<integer>*

integer is the MTU size in octets.

For example, the following command sets the MTU size to 3000 octets:

```
atm-e3/1/1/2/1# mtu 3000
atm-e3/1/1/2/1#
```

Defining the Primary Clock Source

To define the clock signal source, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

primary-clock-source *<value>*

value is internal or loop. If you select internal, the router will generate the clock signal source. If you select the default, loop, the clock signal source will be external to the router.

For example, the following command sets the clock source to internal:

```
atm-e3/1/1/2/1# primary-clock-source internal
atm-e3/1/1/2/1#
```

Specifying the Setup Alarm Threshold

To specify the duration of time (in seconds) that elapses following the detection of a performance failure, before the condition is registered and logged, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

setup-alarm-threshold *<integer>*

integer is a value from 2 through 10 seconds, inclusive.

For example, the following command changes the setup alarm threshold from 2 to 8 seconds:

```
atm-e3/1/1/2/1# setup-alarm-threshold 8
atm-e3/1/1/2/1#
```

Disabling and Reenabling the ATM interface

By default, the ATM interface is enabled when you create the circuit. However, you can disable or reenable the interface at any time. When the interface is enabled, traffic can flow over the interface. When the interface is disabled, traffic cannot flow over the interface.

To disable or reenable the ATM interface, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

state {**disabled** | **enabled**}

For example, the following commands disable and reenable the ATM interface:

```
atm-e3/1/1/2/1# state disabled
atm-e3/1/1/2/1# state enabled
atm-e3/1/1/2/1#
```

Using Site Manager

To create an ATM circuit for a T3 or E3 connection on a Passport 5430, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the ATM DS3/E3 interface (**ATM1**) in slot 1, PCI slot 1, module 2.	The Add Circuit window opens.
2. Click on **OK** to accept the default circuit name.	The ATM Configuration window opens.
3. Click on **Physical Layer Configuration**.	The Physical Layer Configuration window opens.
4. Click on either **DS3** or **E3**.	The Port Parameters window opens.
5. To configure port parameters, set the following parameters as needed: • **Enable/Disable** • **Line Type** • **Setup Alarm Threshold (seconds)** • **Clear Alarm Threshold (seconds)** • **Loopback Configuration** • **Primary Clock** Click on **Help** or see the parameter descriptions in "ATM Line Parameters," beginning on page A-3.	
6. Click on **OK**.	The Physical Layer Configuration window opens.
7. Click on **Done**.	The ATM Configuration window opens.
8. Click on **ATM Line Attributes.**	The ATM Line Driver Attributes window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Set the the following parameters as needed: • **Enable** • **Interface MTU** • **Data Path Enable** • **Data Path Notify Timeout** • **Framing Mode** • **Cell Scrambling** • **Per-VC Clipping** • **DS3 Line Build Out** Note: The **Cell Scrambling** parameter value must be the same as for the other ATM devices on your network. See your system administrator or your service provider for the appropriate value. Click on **Help** or see the parameter descriptions in "ATM Line Parameters" on page A-3.	
10. Click on **OK.**	The ATM Configuration window opens.
11. Click on **ATM**.	The Edit ATM Connector window opens.
12. Go to "Defining an ATM Service Record" in *Configuring ATM Services*.	

After you create the ATM circuit, go to Chapter 2, "Starting ATM and ATM Router Redundancy," in *Configuring ATM Services* to finish configuring ATM services.

Configuring ATM Services also provides more information about ATM services and how to modify an existing ATM configuration.

Version 15.3.0.0

The following sections contain amendments to Chapter 3, "Customizing an ATM Interface," in *Configuring ATM Services*.

Defining the SVC Inactivity Timeout

When you enable the SVC inactivity timeout function (the default), the router automatically terminates any SVCs that have not received or transmitted any cells. If you disable the SVC inactivity timeout function, all SVCs on the line remain open until you close them by another method.

When enabled, the SVC inactivity timeout function also requires a timer value. This timer value specifies how long you want the ATM router to wait before disabling inactive SVCs. By default, if the router does not receive or transmit any cells for 1200 seconds, the inactive SVCs are disabled. However, you can set this timer to any value from 60 to 3600 seconds.

Using the BCC

To disable the SVC inactivity timeout function, navigate to the ATM prompt (for example, **box; atm/11/1**) and enter:

vc-inactivity-control disabled

For example, the following command disables the SVC inactivity timeout function on the ATM interface:

```
atm/11/1# vc-inactivity-control disabled
atm/11/1#
```

To reenable the SVC inactivity timeout function, navigate to the ATM prompt and enter:

vc-inactivity-control enabled

Note: The **vc-inactivity-control** parameter is not available for use with the ATM T3/E3 PMC module. Instead, the **vc-inact-control** parameter appears for this module. The **vc-inact-control** parameter cannot be modified.

To change the SVC inactivity timeout value, navigate to the ATM prompt and enter:

vc-inactivity-timeout *<integer>*

integer is the amount of time (in seconds) that the router waits before it disables inactive SVCs.

For example, the following command sequence reenables the SVC inactivity timeout function on the ATM interface and sets the SVC inactivity timeout value to 2400 seconds:

```
atm/11/1# vc-inactivity-control enabled
atm/11/1# vc-inactivity-timeout 2400
atm/11/1#
```

Note: The **vc-inactivity-timeout** parameter is not available for use with the ATM T3/E3 PMC module. Instead, the **vc-inact-timeout** parameter appears for this module. The **vc-inact-timeout** parameter cannot be modified.

Defining the Clocking Signal Source

You can specify either an internal or external clocking source for time signals. Internal clocking uses the router clock; external clocking uses the line clock.

Using the BCC

To change the source of the ATM clocking signal, navigate to the ATM prompt (for example, **box; atm/11/1**) and enter:

clock-signal-source *<source>*

source is either internal (default) or external.

For example, the following command changes the ATM clocking signal source to external:

`atm/11/1#` **clock-signal-source external**

`atm/11/1#`

Note: The **clock-signal-source** parameter is not available for use with the ATM T3/E3 PMC module. Instead, the **clk-signal-source** parameter appears for this module. The **clk-signal-source** parameter cannot be modified.

Version 15.5.0.0

The following sections contain amendments to Chapter 3, "Customizing an ATM Interface," in *Configuring ATM Services*.

Turning DS-3 and E3 Cell Scrambling On and Off

Beginning with BayRS Version 15.5.0.0, the BCC parameter used to turn ATM cell scrambling on and off for DS-3 and E3 interfaces has a new, more specific name. To eliminate confusion, the **scrambling** parameter is now named **ds3e3-scrambling**.

The default value (off) for the **ds3e3-scrambling** parameter (ATM cell scrambling feature) remains the same.

The procedure for using Site Manager to configure ATM cell scrambling on DS-3 and E3 interfaces has not changed.

Note: ATM cell scrambling is supported only for DS-3 and E3 interfaces. Attempts to configure the **ds3e3-scrambling** parameter on other interfaces (for example, OC-3 interfaces), generates the following error message:

```
Scrambling can be modified only for DS3/E3 Interface.
```

Using the BCC

To turn on cell scrambling for a DS-3 or E3 interface, navigate to the ATM prompt (for example, **box; atm/11/1**) and enter:

ds3e3-scrambling on

For example, the following command turns on cell scrambling for ATM connector 1 in slot 11:

```
atm/11/1# ds3e3-scrambling on
atm/11/1#
```

To turn cell scrambling off, navigate to the ATM prompt and enter:

ds3e3-scrambling off

For example, the following command turns cell scrambling off for ATM connector 1 in slot 11:

```
atm/11/1# ds3e3-scrambling off
atm/11/1#
```

Version 15.6.0.0

The following section contains amendments to Chapter 5, "Customizing PVC Service Records and PVCs," and Chapter 7, "Customizing Classical IP Service Records," in *Configuring ATM Services* (part number 308612-15.1 Rev 00).

Virtual Circuit Monitoring with the ifSpeed MIB Attribute

A number of network management and performance management applications use the ifSpeed MIB attribute to calculate traffic utilization on virtual circuits and to generate alarms when traffic utilization exceeds certain thresholds. Before Version 15.6, BayRS automatically set the ifSpeed MIB attribute to the line speed of the interface, not to the speed of the ATM virtual circuits on that interface.

BayRS Version 15.6 supports a new parameter—called Optional Line Speed—for ATM service records; the value that you set for this parameter is reported by the ifSpeed MIB variable. In this way, network management applications can use SNMP to obtain a user-configured value for the ifSpeed variable for a virtual circuit and generate alarms as appropriate.

Note: This new parameter applies to the service record only regardless of how many virtual circuits are configured under that service record.

By default, the ifSpeed variable is set to the line speed of the interface. You can set the optional line speed parameter to a value corresponding to the rate of the virtual circuit; that value will be reflected in the corresponding ifSpeed entry for each VC on the service record.

Note: The value that you set is for reporting purposes only; it has no effect on the actual performance of the ATM virtual circuit.

You can use the BCC or Site Manager to configure the optional line speed parameter on a service record.

Using the BCC

You can specify a line speed value for a PVC service record or for a classical IP service record.

To set the line speed value, navigate to the service record prompt (for example, **box; atm/11/1; pvc-service/boston** or **box; atm/11/1; classical-ip-service/dallas**) and enter:

optional-line-speed *<integer>*

integer is the line speed for the service record in bits per second.

For example, the following command sets the line speed for classical IP service record "dallas" to 1000000 bits per second:

```
classical-ip-service/dallas# optional-line-speed 1000000
classical-ip-service/dallas#
```

Using Site Manager

To specify a line speed value for a PVC service record or for a classical IP service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the ATM interface (**ATM1**) that you want to modify.	The Select Connection Type window opens (BN), or the ATM Configuration window opens (Passport 5430).
2. Click on **ATM**.	The Edit ATM Connector window opens.
3. Click on **Service Attributes**.	The ATM Service Records List window opens.
4. Click on the PVC or classical IP service record that you want to configure a line speed for.	
5. Set the **Optional Line Speed** parameter. Click on **Help** or see the parameter description on page A-10.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **Done**.	You return to the Edit ATM Connector window.
7. Click on **Done**.	You return to the ATM Configuration or the Select Connection Type window.
8. Click on **Done**.	You return to the Configuration Manager window.

Chapter 4
Configuring Bridging Services

Version 15.2.0.0

The following section corrects an error in *Configuring Bridging Services*.

Interfaces Supported

The section "Interfaces Supported" under "Implementation Notes" in *Configuring Bridging Services* incorrectly states that the translation bridge can operate on all source routing (SR) interfaces supported by Nortel Networks routers except IP. The translation bridge can operate on all SR interfaces supported by Nortel Networks routers except for interfaces configured for SRB with IP encapsulation.

Version 15.5.0.0

The following section corrects an omission in the "Customizing Global Source Routing Bridge Parameters" section of Chapter 7, "Configuring Source Routing Bridge Services Using the BCC," in *Configuring Bridging Services*.

Specifying the IP Network Ring ID for the Source Routing Bridge

You can use the BCC to specify a ring ID for the backbone IP network to which the source routing bridge connects. You must specify the same IP network ring ID for each Nortel Network's source routing bridge that connects to the network.

To specify the ring ID for the backbone IP network to which the source routing bridge connects, navigate to the global srb prompt (for example, **box; srb**) and enter:

ip-net-ring-id *<id_number>*

id_number is a hex value from 0x0 to 0xffe. The default value is 0x0. Assign the same value to all Nortel Network's source routing bridges that border the IP network cloud. The IP network ring ID must be unique among any other group LAN IDs, ring IDs, or internal LAN IDs in the network.

For example, the following command assigns the IP network ring ID value 0x1 to the source routing bridge:

`srb#` **ip-net-ring-id 0x1**

Chapter 5
Configuring Data Compression Services

Version 15.5.0.0

The following notice supplements Chapter 1, "Starting Compression Services," in *Configuring Data Compression Services*.

Hi/fn LZS Compression for Passport 2430 and Passport 5430

Beginning with Version 15.5.0.0, BayRS adds Hi/fn LZS (Lempel Ziv STAC) compression capability to the Passport 2430 and Passport 5430, thus extending optional Hi/fn* LZS* compression capability to all BayRS router platforms.

The use of Hi/fn compression improves the bandwidth utilization of a wide area network (WAN) link by removing redundancies in data traffic, which increases the effective throughput of the link. Hi/fn compression is standards based and permits interoperability with third party routers.

For information about configuring Hi/fn LZS compression, see *Configuring Data Compression Services*.

Version 15.6.0.0

The following information supplements Chapter 1, "Starting Compression Services," in *Configuring Data Compression Services*.

IP Payload Compression over GRE Tunnels

Before Version 15.6, BayRS implemented software-based data compression that compresses the entire IP packet for transmission over PPP, frame relay, and X.25 networks. As service providers increasingly adopt IP/MPLS topologies, the IP header of the packet must be left uncompressed to route packets around the IP/MPLS core. *IP payload compression* provides a means for compressing only the data that follows the IP header.

IP payload compression provides Layer 3 compression end-to-end over low-speed Ethernet and WAN interfaces. IP payload compression is transparent to the underlying Layer 2 protocols and therefore increases compression interoperability with other IP devices in the network.

The BayRS implementation of IP payload compression operates between two BayRS routers and uses the STAC LZS compression algorithm.

Note: The Hi/fn LZS compression software is licensed from Hi/fn, Inc. You must separately purchase a license for the Hi/fn LZS compression software, which is delivered on a separate CD by Nortel Networks.

You configure IP payload compression on the logical IP address associated with a GRE tunnel end point. Compression (or decompression) is applied to the packets before they exit the GRE tunnel end point.

IP payload compression is supported on all BayRS routers on the following low-speed interfaces: 10BASE-T Ethernet, serial, T1/FT1, E1/FE1, ISDN BRI, and 56/64K CSU/DSU.

Note: You can configure IP payload compression on only one 10BASE-T Ethernet interface per slot.

IP payload compression is not supported on 100BASE or 1000BASE Ethernet interfaces, HSSI interfaces, or ATM DS3/OC3 interfaces.

How IP Payload Compression Is Accomplished

IP payload compression is performed on packets that are originated by the router and on packets that pass through the router. (Packets that are smaller than 90 bytes are not compressed.) The process of IP payload compression is briefly summarized here:

1. In the IP header, the original IP protocol type is replaced with the value for IPCOMP (108).
2. Following the original IP header, an IP compression header is added that contains the IP protocol field from the original IP header, a flags field, and the compression protocol index (that is, STAC LZS).
3. The length of the IP header and its checksum are updated to reflect the compressed data and the addition of the new IP compression header.

Note: If the total size of the compressed payload and the IP compression header is not smaller than the size of the original payload, the IP packet is sent in its original uncompressed form, with no IP compression header added to it.

For more information about IP payload compression, refer to the following documents:

- Shacham, A., B. Monsour, R. Pereria, and M. Thomas. *IP Payload Compression Protocol (IPComp)*. RFC 3173. Network Working Group. September 2001.
- Friend, R., and R. Monsour. *IP Payload Compression Using LZS*. RFC 2395. Network Working Group. December 1998.

Implementation Notes

Before you configure IP payload compression, note the following considerations:

- To support IP payload compression, Hi/fn LZS compression is now available for the FRE-4-PPC module. If you plan to use IP payload compression on a BN router with a FRE-4-PPC module, see "Hi/fn LZS Compression for BN Routers with FRE-4-PPC Modules" on page 5-7.
- The BayRS implementation of IP payload compression operates only between two BayRS routers over a GRE tunnel.
- You cannot configure both IP payload compression (Layer 3) and PPP or frame relay compression (Layer 2) on the same interface.

- IP payload compression is not supported with IPsec/IKE.
- Small packets may not compress well. (Packets smaller than 90 bytes are sent uncompressed.)
- If packet fragmentation is also configured, compression of outbound IP packets is performed before packet fragmentation.
- Certain packet filters that are based on Layer 4 information may not work with IP payload compression.

To implement IP payload compression, you must do the following (Figure 5-1):

1. Configure a GRE tunnel between two Nortel Networks routers.
2. Add a logical IP interface to the local and remote tunnel end points.
3. Enable IP payload compression on each logical IP interface.

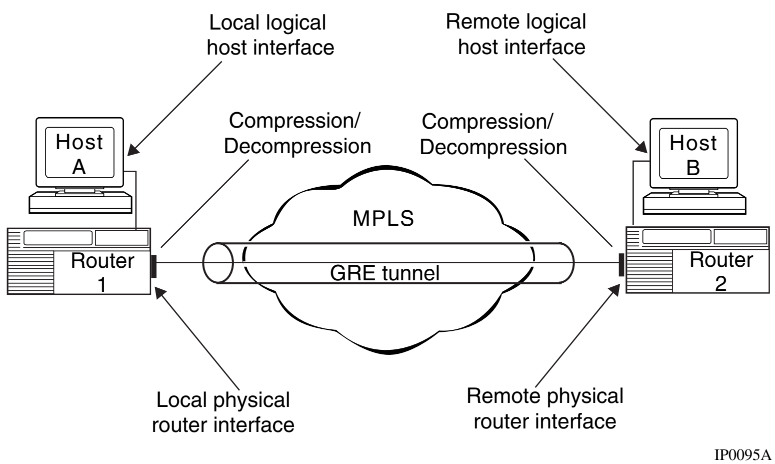

Figure 5-1. Implementation of IP Payload Compression

Configuring IP Payload Compression

You can use the BCC or Site Manager to configure IP payload compression on an IP interface that is configured on a GRE tunnel. By default, IP payload compression is disabled.

Using the BCC

To enable or disable IP payload compression and decompression, go to the IP interface prompt configured on the GRE tunnel (for example, **box; tunnels; gre/chicago; ip/2.2.2.2/255.255.0.0**) and enter:

payload-compression *<state>*

state is one of the following:

enabled
disabled (default)

For example, the following command sequences enables IP payload compression and decompression on logical IP interface 2.2.2.2 configured on GRE tunnel chicago:

```
box# tunnels
tunnels# gre/chicago
gre/chicago# ip/2.2.2.2/255.255.0.0
ip/2.2.2.2/255.255.0.0# payload-compression enabled
ip/2.2.2.2/255.255.0.0#
```

The following command disables IP payload compression and decompression on logical IP interface 2.2.2.2 configured on the GRE tunnel chicago:

```
ip/2.2.2.2/255.255.0.0# payload-compression disabled
ip/2.2.2.2/255.255.0.0#
```

Using Site Manager

To enable or disable IP payload compression and decompression over a GRE tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Select the IP interface configured on a GRE tunnel that you want to edit for IP payload compression.	Site Manager displays the parameter values for that interface.
5. Set the **IP Payload Compression** parameter. Click on **Help** or see the parameter description on page A-50.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Displaying Statistics for IP Payload Compression

To display the list of GRE IP interfaces that are configured for IP payload compression, enter the BCC command **`show hifn ipcomp`**.

```
bcc> show hifn ipcomp

show hifn ipcomp                       Feb 17, 2005 15:35:54 [EST]

hifn ipcomp entries
----------------------------------------------

Circuit    IP              IP         Compression
Name       Address         State      State
---------  ---------       ---------- --------------
GRE1       1.1.1.1          notpres   enabled
GRE2       2.2.2.2          notpres   enabled
PPP_Demand 10.10.10.1       notpres   disabled
_2
E111       192.32.140.36    notpres   disabled
```

To display statistics for the interfaces configured for IP payload compression, including the number of bytes compressed and decompressed, enter the BCC command **show hifn ipcomp stats**.

```
box# show hifn ipcomp stats
show hifn ipcomp stats                         Feb 17, 2005 15:36:08 [EST]

hifn Performance And Data Statistics
------------------------------------------------------------------------
          Ratio                Compressor    Decompressor   CPC Packets
Circuit   ------------------   ------------- -------------- -------------
Name      Compress Decompress In        Out  Agg.In Agg.Out   Tx      Rx
--------- -------- ---------- ------ ------ ------ ------- ------ ------
GRE1      4.222    4.006      202772  48017  21140   84692      0      0
GRE2      --       4.006           0      0  21140   84692      0      0
```

Hi/fn LZS Compression for BN Routers with FRE-4-PPC Modules

To support IP payload compression, BayRS Version 15.6.0.0 adds Hi/fn LZS compression capability to the FRE-4-PPC module installed in a BN router. You must separately purchase a license for the Hi/fn LZS compression software, which is delivered on a separate CD by Nortel Networks.

This section supplements the CD insert that accompanies the Hi/fn LZS Compression Option CD; it provides instructions for copying the new hifn.ppc file from the Hi/fn CD to the BN router image.

Note: This information applies to BayRS Version 15.6 only. If you are installing the Hi/fn software on a router other than a BN or on a BN that has no FRE-4-PPC module, you do not need to read this section.

To install the Hi/fn LZS compression software on a BN router with a FRE-4-PPC module:

1. From the Site Manager main window, choose Tools > Image Builder to start the Image Builder.

Note: For complete information about the Image Builder and the Router Files Manager, see *Configuring and Managing Routers with Site Manager.*

2. In the Image Builder window, choose File > Open and navigate to the copy of the current BN router image (bn.exe) on your workstation.
3. Click on Details below the Current Components box.
4. Select the hifn.exe file under Baseline Router Software and click on Remove.

   This hifn.exe file is only a placeholder. Note that the Component Information box shows its compressed size as less than 2 KB.
5. Choose File > Save to save the modified image.
6. Exit the Image Builder.
7. Open the Image Builder directory for the BN router:

   On a PC, the default directory is wf\builder.dir\rel<*release_number*>\bn, for example, wf\builder.dir\rel15600\bn.

   On a UNIX* platform, the default directory is ~/.builder/rel<*release_number*>/bn, for example, ~/.builder/rel15600/bn.
8. Insert the Hi/fn LZS software CD into the CD-ROM drive.
9. Open the following folders on the CD in order: 15.6.0.0 (or greater), bn.

   The bn directory contains the hifn.exe file and a directory called fre4.
10. If the BN router has FRE-2 or FRE-2-060 modules on which you want to run Hi/fn LZS compression, copy the file 15*xxx*/bn/hifn.exe from the Hi/fn CD to the BN platform directory under the Image Builder directory.

    When you copy the hifn.exe file to an HP platform, it is automatically renamed HIFN.EXE;1. You must rename the file to hifn.exe by executing the following command:

    mv “HIFN.EXE;1” hifn.exe

    Note that you must use quotation marks before and after HIFN.EXE;1.
11. Open the bn/fre4 directory on the Hi/fn CD.

    To run IP payload compression on FRE-4-PPC modules, you must install the hifn.ppc file that is in the bn/fre4 directory.
12. From the Hi/fn CD, copy the file 15*xxx*/bn/fre4/hifn.ppc to the BN platform directory under the Image Builder directory.

When you copy the hifn.ppc file to an HP platform, it is automatically renamed HIFN.PPC;1. You must rename the file to hifn.ppc by executing the following command:

mv “HIFN.PPC;1” hifn.ppc

Note that you must use quotation marks before and after HIFN.PPC;1.

13. Start the Image Builder again and open the BN router image from which you removed the hifn.exe file.
14. Click on Details under the Available Components box, select hifn.ppc (and hifn.exe, if necessary), and click on Add.
15. Save the modified image that includes Hi/fn LZS compression to a new directory and exit the Image Builder.
16. Use the Router Files Manager to transfer the new image to the BN router.
17. Perform a named boot with the new image, following the directions in *Configuring and Managing Routers with Site Manager.*

You can now use Hi/fn LZS compression software on the BN router with a FRE-4-PPC module.

Chapter 6
Configuring Differentiated Services

Version 15.1.0.0

The following section describes a change to *Configuring Differentiated Services*.

Modifying RED Parameters

The following change is required to Table 6-1 in the "Modifying RED Parameters" section of *Configuring Differentiated Services*.

The proper range of values for the **id** parameter is from 1 through 65535. The proper range is shown in the following table, which lists RED parameters that can be configured under **dsqms-red**, their values, and functions.

Parameter	Values	Function
id	integer 1 through 65535	Identifies the RED function. You cannot change this parameter.
min-threshold	integer 0 through 100 (default 20)	Indicates the queue size below which no packets are dropped by RED
max-threshold	integer 1 through 100 (default 80)	Indicates the queue size above which all packets are dropped by RED
first-order-const	integer 0 through 100 (default 1)	Specifies the first-order constant used when calculating drop probability based on the average queue fraction, the queue size, and the min-threshold value
second-order-const	integer 0 through 1000 (default 10)	Specifies the second-order constant used when calculating drop probability based on the average queue fraction, the queue size, and the min-threshold value

Version 15.2.0.0

The following section corrects the description of the Site Manager Priority parameter, which appears in Appendix A of *Configuring Differentiated Services*.

Priority Parameter

The description of the Priority parameter, which appears on the COPS Server List window, incorrectly states that the lower the number, the higher the priority. The description should state that the higher the number, the higher the priority. For example, a COPS server with a priority of 2 will be the active server before a server with a priority of 1.

Version 15.3.0.0

The following section is an amendment to Chapter 2, "Starting Differentiated Services," in *Configuring Differentiated Services*.

Implementation Notes

The following guidelines can help you successfully configure DSQMS on your router:

- You can configure DSQMS on these interfaces only: HSSI, MCT1, MCE1, T1/FT1, E1/FE1, and synchronous.
- If you enable flow fairness on a queue, you cannot configure that queue as a best-effort queue. For information about enabling flow fairness on a queue or designating the queue as best effort, see "Modifying a DSQMS Queue" in *Configuring Differentiated Services*.
- If you configure both weighted and priority queues on an interface, you may experience latency problems with the highest priority queues. To avoid such problems:
  - Ensure that the amount of high-priority traffic is not excessive in the highest priority queues.

— Set the DSQMS interface parameter **dequeue-at-line-rate** to **enabled** (the default value is **disabled**). See “Configuring DSQMS to Dequeue Packets at Line Rate” in *Configuring Differentiated Services* for instructions.

Caution: Enabling the **dequeue-at-line-rate** parameter may cause packet loss in both priority and weighted queues in certain configurations when higher traffic levels are seen in these queues.

- If you implement RED for queue management instead of tail-drop (that is, you set the queue parameter **drop-type** to **red** and you associate the queue classifier with a RED function), the probability of dropping packets may adversely affect the latency requirements of some applications. Adjust the following parameters to achieve the required latency levels for the queue:

  — RED parameters **min-threshold** and **max-threshold** (see “Modifying RED Parameters” on page 3-1 for instructions).

  — Queue parameters **average-queue-gain** and **idle-queue-loss-rate** (see “Modifying a DSQMS Queue” in *Configuring Differentiated Services* for instructions).

Version 15.4.0.0

The following section is an amendment to Chapter 2, “Starting Differentiated Services,” in *Configuring Differentiated Services*.

Implementation Notes

The following guidelines can help you successfully configure DSQMS on your router:

- You can configure DSQMS on these interfaces only: Ethernet, HSSI, MCT1, MCE1, T1/FT1, E1/FE1, and synchronous.

Caution: 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.

- If the Ethernet interface is connected to an external access device such as DSL or cable modem, then Nortel Networks recommends considering policing on the ingress interface of the router by configuring traffic filters and also enabling the **dequeue-at-line-rate** parameter in DSQMS on the egress Ethernet interface for traffic management.
- If you enable flow fairness on a queue, you cannot configure that queue as a best-effort queue. For information about enabling flow fairness on a queue or designating the queue as best effort, see "Modifying a DSQMS Queue" in *Configuring Differentiated Services*.
- If you configure both weighted and priority queues on an interface, you may experience latency problems with the highest priority queues. To avoid such problems:
  - Ensure that the amount of high-priority traffic is not excessive in the highest priority queues.
  - Set the DSQMS interface parameter **dequeue-at-line-rate** to **enabled** (the default value is **disabled**). See "Configuring DSQMS to Dequeue Packets at Line Rate" in *Configuring Differentiated Services* for instructions.

Caution: Enabling the **dequeue-at-line-rate** parameter may cause packet loss in both priority and weighted queues in certain configurations when higher traffic levels are seen in these queues.

- If you implement RED for queue management instead of tail-drop (that is, you set the queue parameter **drop-type** to **red** and you associate the queue classifier with a RED function), the probability of dropping packets may adversely affect the latency requirements of some applications. Adjust the following parameters to achieve the required latency levels for the queue:
  - RED parameters **min-threshold** and **max-threshold** (see "Modifying RED Parameters" on page 3-1 for instructions).
  - Queue parameters **average-queue-gain** and **idle-queue-loss-rate** (see "Modifying a DSQMS Queue" in *Configuring Differentiated Services* for instructions).

Version 15.5.0.0

The following section is new to Chapter 4, "Customizing Differentiated Services," in *Configuring Differentiated Services*.

DSCP Tagging for Router-Generated Packets

Beginning with Version 15.5.0.0, BayRS supports differentiated services code point (DSCP) tagging of internally generated router packets, such as OSPF Hello packets. This feature automatically provides differentiated services queue management system (DSQMS) queuing for all router-generated packets based on the internal mapping between the DSCP tag values and the DSQMS queues.

This feature enhances quality of service (QoS) on BayRS routers by marking router-generated packets and providing the appropriate queuing treatment to marked traffic flows by the DSQMS. This QoS enhancement provides default settings and behaviors for different categories of network traffic based on the Nortel Networks service class (NNSC).

Table 6-1 lists the correlation of traffic categories, Nortel Networks service classes, and DSCPs.

Table 6-1. Correlation of Traffic Categories, Nortel Networks Service Codes, and DiffServ Code Points

Traffic Category	NNSC	DSCP
Critical Control	Critical	CS7
Network Control	Network	CS6
Interactive	Premium	EF, CS5
	Platinum	AF4x, CS4
Responsive	Gold	AF3x, CS3
	Silver	AF2x, CS2
Timely	Bronze	AF1x, CS1
	Standard	DF (CS0)

Beginning with Version 15.5.0.0, protocol packets originating from the BayRS router are marked with the DSCP tags (markings) shown in Table 6-2. These markings are **not** configurable; they are hard-coded and cannot be changed.

Table 6-2. Mapping of BayRS Protocols and DiffServ Code Points

Traffic Category	NNSC	Network Protocol	DSCP	Scheduler
Critical Control	Critical	COPS, frame relay LMI, LCP Echo Request, MOSPF Hello, OSPF Hello, PPP LQR	CS7 ('111000')	Strict Priority
Network Control	Network	BGP, DVMRP, EGP, MOSPF, OSPF, PIM-SM, RIP, VRRP	CS6 ('110000')	Strict Priority
Responsive	Silver	BootP, DHCP, DLSw, DNS, ICMP*, IGMP, IPEX, NTP, RADIUS, RSVP, SNMP*	AF21 ('010010')	User Configurable
Timely	Standard	FTP, IKE, HTTP, non-IP traffic, Telnet*, TFTP	DF (CS0) ('000000')	User Configurable

* For additional information about ICMP, SNMP, and Telnet tagging, see "DSCP Tagging of ICMP, SNMP, and Telnet Packets" on page 6-7.

Note: The Timely category in Table 6-2 is redundant because all packets have a default DSCP value of CS0. However, it is included in the table to indicate which protocols receive best-effort treatment. Packets from all network protocols that are not included in the first three traffic categories in the table (Critical Control, Network Control, and Responsive) are directed to the best-effort queue, which corresponds to the Standard service class.

DSCP Tagging of ICMP, SNMP, and Telnet Packets

This section supplements the information provided in Table 6-2.

The BayRS router tags ICMP, SNMP, and Telnet packets differently depending on whether the router initiates the ICMP, SNMP, or Telnet session, or whether the router is responding to packets sent to it.

- When the router initiates an ICMP, SNMP, or Telnet connection, it tags the packets with the DSCP specified for each protocol in Table 6-2.
- When the router responds to incoming ICMP, SNMP, and Telnet packets, it copies the DSCP from the incoming packets into the outgoing ICMP, SNMP, and Telnet response packets.

Note: If the DSCP of the incoming ICMP or SNMP packet is best-effort, the router sets the DSCP to the same value as for a router-originated ICMP or SNMP packet.

Traffic Filters and DSCP Tagging of ICMP, SNMP, and Telnet Packets

Differentiated services traffic filters that mark incoming packets can affect the DSCP tagging of ICMP, SNMP, and Telnet packets unless you configure the filter to match specific criteria.

For example, assume that a traffic filter has been configured to mark all packets traversing the router as EF. If an SNMP connection is initiated with the router and the incoming SNMP packets are marked as AF41, the diffserv traffic filter will mark the outgoing SNMP response packets with a DSCP of EF instead of AF41. That is, the DSCP specified by the traffic filter will be used instead of the DSCP in the incoming SNMP packets.

To avoid unexpected DSCP tagging of ICMP, SNMP, and Telnet packets, configure diffserv traffic filters to match specific criteria, such as the protocol ID or the source or destination network. For complete information about configuring diffserv traffic filters, see Chapter 3 of *Configuring Differentiated Services*.

DSCP Tagging of IPsec Packets

The DSCP in the IP headers of IPsec packets remains the same as the DSCP of the original encapsulated IP packet. Therefore, IPsec packets are queued based on the DSCP of the original packets and are not subject to default queue mapping.

Mapping of Router-Generated Packets to DSQMS Queues

After they are marked with a DSCP tag, router-generated packets are mapped to DSQMS queues based on the mapping scheme shown in Table 6-3. As the table indicates, critical and network control traffic is automatically directed to the two internal queues that have strict priority scheduling.

You cannot change the mappings for the two internal queues. However, you can override the default mappings of the user configurable queues. For information about changing the mappings of user configurable queues, see *Configuring Differentiated Services.*

Note: You should use BayRS traffic filters on untrusted ingress interfaces to limit the critical and network control traffic entering the router. These traffic filters minimize congestion in the high-priority internal queues.

Table 6-3. Mapping of DSQMS Queues and DSCP

Number of DSQMS Queues Configured	Total Number of DSQMS Queues (excluding the FR Shaped Queue)	DSQMS Queue Number	Differentiated Services Code Point (DSCP)
1	3	INTQ1 INTQ2 Q1	CS7 CS6 CS5, EF, AFxx, CS1-4, DF (CS0)
2	4	INTQ1 INTQ2 Q1 Q2	CS7 CS6 CS5, EF AFxx, CS1-4, DF (CS0)
4	6	INTQ1 INTQ2 Q1 Q2 Q3 Q4	CS7 CS6 CS5, EF AF4x, CS4 AF3x, CS3 AF2x, CS2, AF1x, CS1, DF (CS0)

(continued)

Table 6-3. Mapping of DSQMS Queues and DSCP *(continued)*

Number of DSQMS Queues Configured	Total Number of DSQMS Queues (excluding the FR Shaped Queue)	DSQMS Queue Number	Differentiated Services Code Point (DSCP)
5	7	INTQ1 INTQ2 Q1 Q2 Q3 Q4 Q5	CS7 CS6 CS5, EF AF4x, CS4 AF3x, CS3 AF2x, CS2 AF1x, CS1, DF (CS0)
6	8	INTQ1 INTQ2 Q1 Q2 Q3 Q4 Q5 Q6	CS7 CS6 CS5, EF AF4x, CS4 AF3x, CS3 AF2x, CS2 AF1x, CS1 DF (CS0)

Note: INTQ1 and INTQ2 are internal queues. EF, CS5, CS4, CS3, and AF3x are DSCPs associated with traffic types that are not router generated. This QoS enhancement deals only with the DSCP tag values listed in Table 6-2. The other tag values are included in the table as a reference for facilitating configuration recommendations.

To support this QoS enhancement, BCC **show** command statistics output is expanded to provide additional information, as described in the next section.

BCC show Command Enhancement

The following information supersedes that provided in Appendix C, "Using BCC show Commands," in *Configuring Differentiated Services*.

show dsqms queues stats

The BCC **show dsqms queues stats** command displays a table of DSQMS queues or more specific information based on any filter argument entered, with a subset of information from the **show dsqms queues detail** command. This command displays statistics for the DSQMS configured queues and the reserved DSQMS queues (two internal queues and the frame relay shaped queue). It is the only command that provides any information about the DSQMS reserved queues.

This command allows the following command filter flag and argument:

-circuit *<circuit_no.>*	Displays information about queues on the specified circuit only.

The output now includes the new DSQMS reserved queue types added for Version 15.5.0.0 and provides the following information:

Cct	Name of the circuit
Id/Type	Identification number of configured queue or type of reserved queue
Pkt Count	Number of packets queued
Byte Count	Number of octets queued
Xmit Pkts	Number of packets transmitted
Xmit Bytes	Number of octets transmitted
Dropped Pkts	Number of dropped packets
Dropped Bytes	Number of dropped octets

The DSQMS reserved queue types are as follows:

- Internal Queue 1 (IntQ1)
- Internal Queue 2 (IntQ2)
- Frame Relay Shaped Queue (FR ShQ)

Interoperability of Protocol Prioritization (Priority Queuing) and DSQMS

There is a common misconception that protocol prioritization (priority queuing) and DSQMS cannot co-exist. On the contrary, these two features can be configured at the same time. In fact, there are situations when DSQMS is configured in which protocol prioritization also must be configured, such as in the case of prioritizing the frame relay Local Management Interface (LMI) traffic into IntQ1. The same situation also applies when prioritizing PPP Link Quality Report (LQR) packets and Link Control Protocol (LCP) echo requests.

The interoperability of these two features can be summarized as follows:

- DSQMS operates at the driver level only.
- When frame relay is configured, protocol prioritization operates at the driver level as well as at the frame relay level.
- When both protocol prioritization and DSQMS are configured, at the driver level DSQMS always takes precedence. This means that such a configuration is inconsequential as far as protocol prioritization is concerned because at the driver level, DSQMS will be running.
- When both protocol prioritization and DSQMS are configured, at the frame relay level only protocol prioritization operates (because DSQMS operates only at the driver level). BayRS code (even before the DSCP tagging feature was available) tags frame relay LMI as interrupt traffic only if protocol prioritization is configured. So, the purpose of protocol prioritization configuration for LMI is only to tag packets (in the frame relay code) so they can be identified later (in the driver code). When a tagged LMI packet comes to the driver, the following occurs:
  - When DSQMS is not configured, protocol prioritization operates at the driver level. In this case, protocol prioritization identifies the tag and puts the LMI traffic into the Interrupt Queue.
  - When DSQMS is configured, it takes precedence over protocol prioritization. In this case, DSQMS identifies the tag and puts the LMI traffic into Internal Queue 1 (IntQ1).

Version 15.6.0.0

The following sections contain additions and amendments to *Configuring Differentiated Services* (part number 308620-14.20 Rev 00).

Mapping of Router-Generated Protocol Packets to DSCPs

The DSCPs for several protocols have been changed for Version 15.6.0.0. The following section revises Table 6-2 on page 6-6. For complete information about DSCP tagging of router-generated packets, see "DSCP Tagging for Router-Generated Packets" on page 6-5.

Beginning with Version 15.6.0.0, protocol packets originating from the BayRS router are marked with the DSCP tags (markings) shown in Table 6-4. (These markings are **not** configurable; they are hard-coded and cannot be changed.)

Table 6-4. Mapping of BayRS Protocols to DSCPs

Traffic Category	NNSC	Network Protocol	DSCP	Scheduler
Critical Control	Critical	COPS, frame relay LMI, LCP Echo Request, MOSPF Hello, OSPF Hello, PPP LQR	CS7 ('111000')	Strict Priority
Network Control	Network	BGP, BootP, DHCP, DNS, DVMRP, EGP, MOSPF, OSPF, PIM-SM, RIP, VRRP	CS6 ('110000')	Strict Priority
Interactive	Platinum	IPEX	AF41 ('100010')	User Configurable
Responsive	Silver	DLSw, ICMP*, IGMP, NTP, RADIUS, RSVP	AF21 ('010010')	User Configurable

(continued)

Table 6-4. Mapping of BayRS Protocols to DSCPs *(continued)*

Traffic Category	NNSC	Network Protocol	DSCP	Scheduler
Timely	Bronze	SNMP*	AF11 ('001010')	User Configurable
	Standard	FTP, IKE, HTTP, non-IP traffic, Telnet*, TFTP	DF (CS0) ('000000')	User Configurable

* For additional information about ICMP, SNMP, and Telnet tagging, see "DSCP Tagging of ICMP, SNMP, and Telnet Packets" on page 6-7.

Note: The Timely-Standard category in Table 6-4 is redundant because all packets have a default DSCP value of CS0. However, it is included in the table to indicate which protocols receive best-effort treatment. Packets from all network protocols that are not included in any other traffic category in the table (Critical Control, Network Control, Interactive, and Responsive) are directed to the best-effort queue, which corresponds to the Standard service class.

Interoperability of Protocol Prioritization and DSQMS

The interoperability of protocol prioritization (priority queuing) and DSQMS has changed for Version 15.6.0.0. This section updates the information in "Interoperability of Protocol Prioritization (Priority Queuing) and DSQMS" on page 6-11.

With Version 15.6.0.0, DSQMS operates at the driver level *and* at the frame relay level to allow DSQMS to be used as the QoS mechanism at the frame relay level. In earlier versions of BayRS, only protocol prioritization operated at the frame relay level, even if DSQMS was configured at the interface level.

Note: For more information about frame relay traffic shaping using DSQMS, see "Frame Relay Traffic Shaping with DSQMS" on page 9-5.

The treatment of the following traffic is the same as in earlier versions of BayRS: frame relay Local Management Interface (LMI) traffic and PPP Link Quality Report (LQR) packets and Link Control Protocol (LCP) echo requests.

BayRS tags frame relay LMI as interrupt traffic only if protocol prioritization is configured. So, the purpose of protocol prioritization configuration for LMI is only to tag packets (in the frame relay code) so they can be identified later (in the driver code). When a tagged LMI packet comes to the driver, the following occurs:

- When DSQMS is not configured, protocol prioritization operates at the driver level. In this case, protocol prioritization identifies the tag and puts the LMI traffic into the Interrupt Queue.
- When DSQMS is configured, it takes precedence over protocol prioritization. In this case, DSQMS identifies the tag and puts the LMI traffic into Internal Queue 1 (IntQ1).

Using Site Manager to Configure DSQMS

The following section supplements Chapter 2, "Starting Differentiated Services," and Chapter 6, "Customizing Queue Management and Scheduling," in *Configuring Differentiated Services* (part number 308620-14.20 Rev 00).

Beginning with Version 15.6.0.0, you can use Site Manager to configure DSQMS on the router. Before Version 15.6.0.0, you could only use the BCC to configure DSQMS.

Note: Using Site Manager, you can configure DSQMS on PPP multiline and multilink bundles. (The BCC does not support multiline or multilink configuration.) However, DSQMS traffic shaping is not supported on frame relay multiline/multilink.

For an overview of queue management and scheduling, see the following sections in *Configuring Differentiated Services*.

- "Queue Management and Scheduling (QMS)" in Chapter 1
- "How DSQMS Elements Work Together" in Chapter 2

Also, see the earlier sections of this chapter in the Document Change Notice, especially "Implementation Notes" on page 6-3.

DSQMS Configuration Steps

To start DSQMS on the router, perform the following steps. These steps are described in the following sections.

1. If necessary, configure a circuit on a slot and connector.
2. Enable DSQMS on the circuit.

Note: For frame relay circuits, you enable DSQMS on the default service record only. You cannot enable DSQMS on any other service record.

---

3. Create one or more sets of RED attributes that can be used by queues on the interfaces.
4. Create one or more queues on the interface.
5. Create one or more traffic classifiers on each queue.

For information and instructions on configuring a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

Enabling DSQMS on an Interface

After you successfully configure a new circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, select **DSQMS**.	
2. Click on **OK**.	The Edit DSQMS Parameters window opens.
3. If necessary, set the following parameters: • **Debug Level** • **Dequeue At Line Rate** Click on **Help** or see the parameter descriptions beginning on page A-17.	
4. Click on **Apply** then click on **Done**.	You return to the Configuration Manager window.

Creating RED Instances for Use by Traffic Classifiers

Each instance of DSQMS RED defines a set of attributes for use in traffic classifiers that are associated with DSQMS queues. To create RED instances, perform the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DSQMS**.	The DSQMS menu opens.
3. Choose **RED**.	The Edit RED Parameters window opens.
4. Click on **Add**.	
5. Set the following parameters: • **First Order Const** • **Second Order Const** • **Min Threshold** • **Max Threshold** Click on **Help** or see the parameter descriptions beginning on page A-14.	
6. Click on **Apply** then click on **Done**.	
7. To configure more RED instances, repeat steps 4 through 6.	
8. Click on **Done**.	You return to the Configuration Manager window.

Creating DSQMS Queues and Associated Traffic Classifiers

To create a DSQMS queue and its associated traffic classifiers, perform the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DSQMS**.	The DSQMS menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **Interface**.	The Edit DSQMS Parameters window opens.
4. Click on **Queues**.	The Edit DSQMS Queue List window opens.
5. Click on **Add**.	The Edit DSQMS Parameters window opens.
6. Set the **Enable** parameter to **Enable**. Click on **Help** or see the parameter description on page A-19.	
7. Set other queue parameters as needed. Click on **Help** or see the parameter descriptions beginning on page A-19.	
8. Click on **OK**.	You return to the Edit DSQMS Queue List window.
9. To configure a traffic classifier for the queue, click on **Classifier**.	The Edit DSQMS Classifier List window opens.
10. Click on **Add**.	The Classifier ID Selection window opens.
11. Type an 8-digit (binary octet) DSCP. See the parameter description on page A-25.	
12. Click on **OK**.	You return to the Edit DSQMS Classifiers window opens.
13. Set the following parameters: • **Classifier Queue ID** • **Classifier RED ID** Click on **Help** or see the parameter descriptions beginning on page A-25.	
14. Click on **Done**.	You return to the Edit DSQMS Classifier List window.
15. To configure more classifiers, repeat steps 9 through 14.	
16. Click on **Done**.	You return to the Edit DSQMS Queue List window.
17. To configure more queues, repeat steps 5 through 16.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
18. Click on **Done**.	You return to the Edit DSQMS Parameters window.
19. Click on **Done**.	You return to the Configuration Manager window.

Modifying RED Parameters

You can modify parameters for an instance of DSQMS RED. To edit an RED instance, perform the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DSQMS**.	The DSQMS menu opens.
3. Choose **RED**.	The Edit RED Parameters window opens.
4. Select the RED instance that you want to edit.	
5. Edit one or more of the following parameters: • **Second Order Const** • **First Order Const** • **Min Threshold** • **Max Threshold** Click on **Help** or see the parameter descriptions beginning on page A-14.	
6. Click on **Apply** then click on **Done**.	You return to the Configuration Manager window.

Modifying DSQMS Interface Parameters

You can modify DSQMS parameters for an interface. To edit DSQMS interface parameters, perform the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DSQMS**.	The DSQMS menu opens.
3. Choose **Interface**.	The Edit DSQMS Parameters window opens.
4. Select the interface that you want to edit.	
5. Edit one or more of the following parameters: • **Enable** • **Debug Level** • **Dequeue At Line Rate** Click on **Help** or see the parameter descriptions beginning on page A-16.	
6. Click on **Apply**.	
7. Click on **Restart**. When you edit parameters for a DSQMS interface, you must restart DSQMS on the interface for the changes to take effect.	
8. Click on **Done**.	You return to the Configuration Manager window.

Modifying DSQMS Queues

You can modify DSQMS queues on an interface. To edit DSQMS queue parameters, perform the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DSQMS**.	The DSQMS menu opens.
3. Choose **Interface**.	The Edit DSQMS Parameters window opens.
4. Select the interface that has the DSQMS queue that you want to edit.	
5. Click on **Queues**.	The Edit DSQMS Queue List window opens.
6. Select the queue that you want to edit.	
7. Edit queue parameters as needed. Click on **Help** or see the parameter descriptions beginning on page A-19.	
8. Click on **Apply** and then click on **Done**.	You return to the Edit DSQMS Parameters window.
9. Click on **Restart**. When you edit parameters for a DSQMS queue, you must restart DSQMS on the interface for the changes to take effect.	
10. Click on **Done**.	You return to the Configuration Manager window.

Chapter 7
Configuring DLSw Services

Version 15.5.0.0

The following section supplements Chapter 4, “Customizing DLSw Services,” in *Configuring DLSw Services*.

DLSw Protocol Prioritization

DLSw protocol prioritization is an outbound filtering mechanism that enables you to assign preference to specific types of traffic supported by DLSw. DLSw protocol prioritization does not affect traffic as it enters the router, but affects the sequence in which traffic exits the router.

Prior to Version 15.5.0.0, only Site Manager could be used to configure DLSw protocol prioritization. The following sections explain how to use the BCC to configure this feature. For general information on DLSw protocol prioritization and for information on using Site Manager to configure it, see *Configuring DLSw Services*.

Configuring DLSw Protocol Prioritization using the BCC

Note: This section assumes that DLSw is already configured on an interface and that the peer table is complete. For information about configuring a circuit with DLSw and setting the slot, peer, and SAP parameters, refer to *Configuring DLSw Services*.

There are three parts to configuring DLSw protocol prioritization using the BCC:

- Configuring and enabling global parameters for DLSw protocol prioritization
- Customizing and enabling DLSw priority queues for specific DLSw peers
- Creating and enabling priority outbound filters for DLSw traffic

Configuring and Enabling Global Parameters for DLSw Protocol Prioritization

DLSw protocol prioritization is disabled by default. When you enable it, it takes effect using the currently configured values (default or customized) for all global DLSw protocol prioritization parameters. You can customize the DLSw protocol prioritization configuration to meet the specific needs of your site by changing the default settings of the global DLSw protocol prioritization parameters.

Customizing Global Parameters for DLSw Protocol Prioritization

To meet the specific needs of your site, you can modify the default settings of one or more of the following DLSw protocol prioritization global parameters:

- max-queue-buffers-unconfig-peers—specifies the maximum number of packets in each queue
- max-queue-size-unconfig-peers—specifies the maximum size (in bytes) of each queue
- default-bandwidth—specifies the number of queues to be used and allocates the bandwidth for each

max-queue-buffers-unconfig-peers

To specify the maximum number of packets in each queue, navigate to the dlsw-protocol-prioritization prompt (for example, **box**; **dlsw; dlsw-protocol-prioritization**) and enter:

max-queue-buffers-unconfig-peers *<value>*

value is an integer between 10 and 2147483647, inclusive. The default value is 50.

For example, to specify 100 as the maximum number of packets in each default queue, enter:

```
dlsw-protocol-prioritization# max-queue-buffers-unconfig-peers 100
dlsw-protocol-prioritization#
```

max-queue-size-unconfig-peers

To specify the maximum size (in bytes) of each default queue, navigate to the dlsw-protocol-prioritization prompt (for example, **box**; **dlsw; dlsw-protocol-prioritization**) and enter:

max-queue-size-unconfig-peers *<value>*

value is an integer between 5,000 and 2,147,483,647, inclusive. The default value is 16000.

For example, to specify 18000 as the maximum number of packets in each default queue, enter:

```
dlsw-protocol-prioritization# max-queue-size-unconfig-peers 18000
dlsw-protocol-prioritization#
```

default-bandwidth

To specify the number of default queues to be used and allocate the bandwidth for each, navigate to the dlsw-protocol-prioritization prompt (for example, **box**; **dlsw; dlsw-protocol-prioritization**) and enter:

default-bandwidth *<value>*

value is the allocated bandwidth for each of the 10 default priority queues (0-9). The default value is {60, 40, 0, 0, 0, 0, 0, 0, 0, 0}. Thus, the default setting utilizes only two priority queues by allocating 60% for queue 0, 40% for queue 1, and 0% for each of the remaining 8 queues. A valid value is any combination of 10 entries that add up to 100. Each entry represents the allocated bandwidth percentage for one of the 10 queues (0 through 9). You must enter a value for each of the 10 queues. The sum of the specified bandwidth percentages must equal 100.

For example, to allocate 10 percent of the bandwidth to each of the 10 queues, navigate to the dlsw-protocol-prioritization prompt (for example, **box**; **dlsw; dlsw-protocol-prioritization**) and enter:

`dlsw-protocol-prioritization#` **default-bandwidth {10 10 10 10 10 10 10 10 10 10}**
`dlsw-protocol-prioritization#`

For example, to allocate 40 percent of the bandwidth to queue 0, 30 percent of the bandwidth to queue 1, and 30% of the bandwidth to queue 3, navigate to the dlsw-protocol-prioritization prompt (for example, **box**; **dlsw; dlsw-protocol-prioritization**) and enter:

`dlsw-protocol-prioritization#` **default-bandwidth {40 30 30 0 0 0 0 0 0 0}**
`dlsw-protocol-prioritization#`

Enabling and Disabling DLSw Protocol Prioritization for Configured and Unconfigured Peers

When you enable DLSw protocol prioritization, it takes effect using the currently configured values (default or customized) for the global parameters.

Enabling DLSw protocol prioritization for configured peers

To enable DLSw protocol prioritization for configured peers, navigate to the global dlsw prompt (for example, **box**; **dlsw**) and enter:

dlsw-protocol-prioritization protocol-priority enabled

For example, to enable DLSw protocol prioritization for configured peers using the currently configured values for the global DLSw protocol prioritization parameters, navigate to the global dlsw prompt and enter:

`dlsw#` **dlsw-protocol-prioritization protocol-priority enabled**
`dlsw-protocol-prioritization#`

The default setting for **protocol-priority** is disabled. To disable DLSw protocol prioritization for configured peers after enabling it, navigate to the global dlsw prompt and enter:

dlsw-protocol-prioritization protocol-priority disabled

Enabling DLSw protocol prioritization for unconfigured peers

To enable DLSw protocol prioritization for unconfigured peers using the currently configured values (default or customized) for the global DLSw protocol prioritization parameters, navigate to the global dlsw prompt (for example, **box**; **dlsw**) and enter:

dlsw-protocol-prioritization pp-unconfigured-peers enabled

For example, to enable DLSw protocol prioritization for unconfigured peers using the currently configured values for the global DLSw protocol prioritization parameters, navigate to the global dlsw prompt and enter:

`dlsw#` **dlsw-protocol-prioritization pp-unconfigured-peers enabled**
`dlsw-protocol-prioritization#`

The default setting for **pp-unconfigured-peers** is disabled. To disable DLSw protocol prioritization for unconfigured peers after enabling it, navigate to the global dlsw prompt and enter:

dlsw-protocol-prioritization pp-unconfigured-peers disabled

Customizing and Enabling DLSw Priority Queues for Specific Peers

You can fine tune DLSw priority queues for a specific peer by performing the following tasks:

- Specify a peer for custom DLSw priority queue configuration.
- Customize the DLSw priority queue parameters for the specified peer.
- Enable the specified peer’s custom DLSw priority queue configuration.

Note: Peer-specific priority queue configurations take precedence over any currently enabled global DLSw protocol prioritization queue configuration.

Specifying a Peer for Custom DLSw Priority Queue Configuration

To specify a peer for custom DLSw priority queue configuration, navigate to the global dlsw prompt (for example, **box**; **dlsw**) and enter:

peer-queue-configuration peer-ip-addr *<value>*

value is the IP address of the peer for which you want to configure custom DLSw priority queues.

For example, to specify custom DLSw priority queue configuration for a peer with an IP address of 192.168.1.1, enter:

```
dlsw# peer-queue-configuration peer-ip-addr 192.168.1.1
dlsw-peer-queue-configuration/192.168.1.1#
```

Customizing the DLSw Priority Queues for a Specific Peer

For a specified peer, you can override the currently configured global DLSw protocol prioritization parameters for the following elements:

- maximum buffer size for each queue
- maximum number of packets per queue
- allocated bandwidth for each of the 10 DLSw priority queues (0-9)

max-queue-buffers

To specify the maximum number of packets for each of a peer's DLSw priority queues, navigate to the peer's dlsw-peer-queue-configuration prompt (for example, **box**; **dlsw; dlsw-peer-queue-configuration/**<*peer-IP-address*>) and enter:

max-queue-buffers <*value*>

value is the maximum number of packets allowed in each of this peer's priority queues. The range of valid values is from 10 to 2147483647, inclusive. The default is 50.

For example, to specify 200 as the maximum number of packets in each of the DLSw priority queues for a peer with an IP address of 192.168.1.1, navigate to the peer's dlsw-peer-queue-configuration prompt and enter:

```
dlsw-peer-queue-configuration/192.168.1.1# max-queue-buffers 200
dlsw-peer-queue-configuration/192.168.1.1#
```

bandwidth-allocation

To allocate the bandwidth for each of the peer's 10 DLSw priority queues, first navigate to the peer's dlsw-peer-queue-configuration prompt (for example, **box**; **dlsw; dlsw-peer-queue-configuration/**<*peer-IP-address*>) and enter:

bandwidth-allocation

This action displays the bandwidth-allocation/<*peer-IP-address*> prompt for the peer.

At the bandwidth-allocation/<*peer-IP-address*> prompt for the peer, enter:

dlsw-queue <*value*>

value is the allocated bandwidth for each of the 10 DLSw priority queues (0-9). The default value is {60, 40, 0, 0, 0, 0, 0, 0, 0, 0}. A valid value is any combination of 10 entries that add up to 100. Each entry represents the allocated bandwidth percentage for one of the 10 queues (0 through 9). You must enter a value for each of the 10 queues. The sum of the specified bandwidth percentages must equal 100.

For example, to allocate 10 percent of the bandwidth to each of the 10 queues, navigate to the peer's bandwidth-allocation prompt and enter:

```
bandwidth-allocation/192.168.1.1# dlsw-queue {10 10 10 10 10 10 10 10 10 10}
bandwidth-allocation/192.168.1.1#
```

max-queue-size

To specify the maximum size (in bytes) of each queue for a peer, navigate to the peer's dlsw-peer-queue-configuration prompt (for example, **box**; **dlsw; dlsw-peer-queue-configuration/**<*peer-IP-address*>) and enter:

max-queue-size <*value*>

value is the maximum size (in bytes) for each of this peer's priority queues. The range of valid values is from 5000 to 2147483647, inclusive. The default is 16000.

For example, to specify 20000 as the maximum number of packets allowed in each DLSw priority queue for a peer with an IP address of 192.168.1.1, navigate to the peer's dlsw-peer-queue-configuration prompt and enter:

```
dlsw-peer-queue-configuration/192.168.1.1# max-queue-size 20000
dlsw-peer-queue-configuration/192.168.1.1#
```

Enabling and Disabling a Peer's DLSw Priority Queues

Peer-specific DLSw priority queues are disabled by default. To enable the customized DLSw priority queues that you have configured for a specific peer, navigate to the peer's dlsw-peer-queue-configuration prompt (for example, **box**; **dlsw; dlsw-peer-queue-configuration/**<*peer-IP-address*>) and enter:

protocol-priority enabled

For example, to enable the customized DLSw priority queues that you configured for a peer with an IP address of 192.168.1.1, navigate to the peer's dlsw-peer-queue-configuration prompt and enter:

```
dlsw-peer-queue-configuration/192.168.1.1# protocol-priority enabled
dlsw-peer-queue-configuration/192.168.1.1#
```

To disable the customized DLSw priority queues for a specific peer again, navigate to the peer's dlsw-peer-queue-configuration prompt (for example, **box**; **dlsw; dlsw-peer-queue-configuration/**<*peer-IP-address*>) and enter:

protocol-priority disabled

For example, to disable the customized DLSw priority queues for a peer with an IP address of 192.168.1.1, navigate to the peer's dlsw-peer-queue-configuration prompt and enter:

```
dlsw-peer-queue-configuration/192.168.1.1# protocol-priority disabled
dlsw-peer-queue-configuration/192.168.1.1#
```

Creating and Enabling Priority Outbound Filters for DLSw traffic

You can create priority filters for outbound DLSw traffic for specific peers that determine which traffic is sent to which DLSw priority queue (0 through 9).

To create a DLSw priority filter for outbound traffic, navigate to the global dlsw prompt (for example, **box**; **dlsw**) and enter:

dlsw-priority-outbound-filter-name <*filter_name*> **peer-ip-addr** <*value*>

filter_name is a descriptive name of the outbound traffic filter you are creating. For example, use the name *dsap_01and02_q3* for a filter that sends traffic with a destination SAP address of 01 or 02 to queue 3. The filter name can be up to 30 alphanumeric characters in length.

value is the IP address of the peer for which you are creating the filter.

For example, to create a DLSw outbound filter named *dsap_01and02_q3* for a DLSw peer with an IP address of 192.168.1.1, navigate to the global dlsw prompt (for example, **box**; **dlsw**) and enter:

dlsw-priority-outbound-filter-name dsap_01to02_q3 peer-ip-addr 192.168.1.1

Enabling and Disabling DLSw Outbound Filters

By default, an outbound filter is enabled when you create it.

Disabling an Outbound Filter

To disable a DLSw priority filter, navigate to the peer's filter prompt (for example, **box**; **dlsw; dlsw-priority-outbound-filter/***<filter_name>***/***<peer_address>*) and enter:

state disabled

For example, to disable a DLSw outbound filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the peer's filter prompt (**box**; **dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1**) and enter:

`dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1#` **state disabled**

`dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1#`

Enabling an Outbound Filter

To enable a DLSw priority filter again, navigate to the peer's filter prompt (for example, **box**; **dlsw; dlsw-priority-outbound-filter/***<filter_name>***/** *<peer_address>*) and enter:

state enabled

For example, to enable a DLSw outbound filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the peer's filter prompt (**box**; **dlsw; dlsw-priority-outbound-filter/dsap_01and02_q/192.168.1.1***)* and enter:

`dlsw-priority-outbound-filter/dsap_01and02_q/192.168.1.1#` **state enabled**

```
dlsw-priority-outbound-filter/dsap_01and02_q/192.168.1.1#
```

Specifying Match Criteria for DLSw Priority Outbound Filters

For DLSw priority outbound filters, you can specify SAP source and destination addresses and MAC source and destination addresses as match criteria. Traffic that matches the configured match criteria for a filter is handled according to the configured filter actions.

Note: The BCC does not support the use of predefined match criteria for FID2 and FID4 frames in DLSw outbound filters in Version 15.5.0.0, or earlier. However, Site Manager supports the use of these predefined match criteria.

To prepare to specify the filtering match criteria, navigate to the peer's filter prompt (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>*, and enter:

match

This action displays the priority outbound filter's match prompt. For example, to display the match prompt for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the peer's filter prompt (**box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1**) and enter:

```
dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1# match
match/dsap_01and02_q3/192.168.1.1#
```

Specifying MAC destination addresses

To specify a MAC destination address as a filter criteria, navigate to the peer filter's match prompt, (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>***; match**), and enter:

pri-dlsw-mac-dest-addr *<address_range>*

<address_range> is the range of MAC destination addresses for the filter in hexadecimal notation. Valid values are in the range of 0-FFFFFFFFFFFF, inclusive. For a range with only one value, enter only one MAC destination address. The BCC automatically uses that value for both the minimum and maximum values in the address range.

For example, to specify a range of MAC destination addresses from 0aaa to 0aab as a match criteria for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's match prompt, (**box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1; match**), and enter:

`match/dsap_01and02_q3/192.168.1.1#` **pri-dlsw-mac-dest-addr {0aaa-0aab}**

`match/dsap_01and02_q3/192.168.1.1#`

Specifying MAC source addresses

To specify a MAC source address as a filter criteria, navigate to the peer filter's match prompt, (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>*; **match**), and enter:

pri-dlsw-mac-src-addr *<address_range>*

<address_range> is the range of MAC destination addresses for the filter in hexadecimal notation. Valid values are in the range of 0-FFFFFFFFFFFF, inclusive. For a range with only one value, enter only one MAC source address. The BCC automatically uses that value for both the minimum and maximum values in the address range.

For example, to specify a range of MAC source addresses from 0000a2000001 to 0000a2000003 as a match criteria for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's match prompt, (**box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1; match**), and enter:

`match/dsap_01and02_q3/192.168.1.1#` **pri-dlsw-mac-src-addr {0000a2000001-0000a2000003}**

`match/dsap_01and02_q3/192.168.1.1#`

Specifying SAP destination addresses

To specify a SAP destination address as a filter criteria, navigate to the peer filter's match prompt, (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>*; **match**), and enter:

pri-dlsw-dsap *<address_range>*

<address_range> is the range of SAP destination addresses for the filter. Valid values are in the range of 0-65535, inclusive. For a range with only one value, enter only one SAP destination address. The BCC automatically uses that value for both the minimum and maximum values in the address range.

For example, to specify a range of SAP destination addresses from 1 to 2 as a match criteria for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's match prompt, (**box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1; match**), and enter:

```
match/dsap_01and02_q3/192.168.1.1# pri-dlsw-dsap {1-2}
match/dsap_01and02_q3/192.168.1.1#
```

Specifying SAP source addresses

To specify a SAP source address as a filter criteria, navigate to the peer filter's match prompt, (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>*; **match**), and enter:

pri-dlsw-ssap *<address_range>*

<address_range> is the range of SAP source addresses for the filter. Valid values are in the range of 0-65535, inclusive. For a range with only one value, enter only one SAP source address. The BCC automatically uses that value for both the minimum and maximum values in the address range.

For example, to specify a range of SAP source addresses from 4 to 5 as a match criteria for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's match prompt, (**box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1; match**), and enter:

```
match/dsap_01and02_q3/192.168.1.1# pri-dlsw-ssap {4-5}
match/dsap_01and02_q3/192.168.1.1#
```

Specifying the Action for DLSw Priority Outbound Filters

You can specify the following actions for DLSw priority outbound filters:

- **queue**—specifies to which DLSw priority queue (0-9) traffic that matches the filter's match criteria will be sent

- **action-log**—specifies whether the router will send an entry to the system log file for traffic that matches the filter's match criteria

To prepare to specify the filter action, navigate to the peer's filter prompt (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>*, and enter:

actions

This action displays the priority outbound filter's actions prompt. For example, to display the actions prompt for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the peer's filter prompt **(box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1**) and enter:

```
dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1# actions
actions/dsap_01and02_q3/192.168.1.1#
```

Specifying the Queue Action

To specify the priority queue for traffic that matches the filter's match criteria, navigate to the peer filter's actions prompt, (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>***; actions**), and enter:

queue *<value>*

<value> is the number of the DLSw priority queue for this filter. Valid values are from 0 to 9, inclusive.

For example, to specify queue 1 as the priority queue for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's actions prompt, (**box; dlsw; dlsw-priority-outbound-filter/ dsap_01and02_q3/192.168.1.1; actions**), and enter:

```
actions/dsap_01and02_q3/192.168.1.1# queue 1
actions/dsap_01and02_q3/192.168.1.1#
```

Specifying the Log Action

To specify the log action for traffic that matches the filter's match criteria, navigate to the peer filter's actions prompt, (for example, **box; dlsw; dlsw-priority-outbound-filter/** *<filter_name>/ <peer_address>***; actions**), and enter:

action-log {on | off}

on (the default) indicates that when an outbound packet matches the filter's match criteria, the DLSw outbound priority filter adds an entry to the system log file.

off specifies that no DLSw outbound priority filter information is written to the system event log file.

For example, to turn off logging for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's actions prompt, **(box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1; actions**), and enter:

`actions/dsap_01and02_q3/192.168.1.1#` **action-log off**

`actions/dsap_01and02_q3/192.168.1.1#`

For example, to turn logging on again for a filter named *dsap_01and02_q3* for a peer with an IP address of 192.168.1.1, navigate to the filter's actions prompt, **(box; dlsw; dlsw-priority-outbound-filter/dsap_01and02_q3/192.168.1.1; actions**), and enter:

`actions/dsap_01and02_q3/192.168.1.1#` **action-log on**

`actions/dsap_01and02_q3/192.168.1.1#`

Chapter 8
Configuring Ethernet, FDDI, and Token Ring Services

Version 15.4.0.0

The following section is new to Chapter 2 of *Configuring Ethernet, FDDI, and Token Ring Services*.

The sections “Router Processing of Tagged Frames,” “Implementation Considerations,” “Adding a Tagged Circuit to an Unconfigured 10BASE-T or 100BASE-T Interface,” and “Adding a Tagged Circuit to an Existing 10BASE-T or 100BASE-T Interface” contain amendments to Chapter 5 of *Configuring Ethernet, FDDI, and Token Ring Services*.

Specifying the DSQMS Line Speed

You specify the DSQMS line speed using the **dsqms-line-speed** parameter. You access this parameter by navigating to the Ethernet prompt (for example, **box**; **ethernet 2/1**) and entering the following command:

dsqms-line-speed <*value*>

value specifies the line speed (in bits per second) for the DSQMS client. The default is 1250000 (1.25 Mb/s).

In network configurations where the Ethernet interface is connected to an external access device such as DSL or a cable modem, the **dsqms-line-speed** parameter can be used in conjunction with the **dequeue-at-line-rate** parameter enabled on the egress interface and traffic policing on the ingress interface for traffic management.

For example, to change the line speed to 10 Mb/s:

```
ethernet/2/1# dsqms-line-speed 10000000
ethernet/2/1#
```

Router Processing of Tagged Frames

802.1Q tagging is supported on 10BASE-T and 100BASE-T interfaces that connect the Nortel Networks router to an 802.1Q-compliant switch or routing switch. With 802.1Q tagging enabled, the physical connection between the router and the adjacent device supports multiple virtual connections.

The number of connections is equal to the number of virtual connections plus a default physical connection that provides transit services for other non-VLAN traffic that may be received from or forwarded to the adjacent device.

Upon receipt of a frame across a virtual connection, a circuit manager strips the four bytes of 802.1Q header information and directs a now standard Ethernet frame to a connection-specific routing process. The routing process consults its forwarding table and, in turn, directs the frame to a circuit manager handling the next-hop connection. If that connection is a non-tagged, non-virtual connection, processing is completed as for any other standard Ethernet frame.

However, if the next-hop connection is a tagged, virtual connection, the circuit manager inserts the four bytes of 802.1Q header information that identify that VLAN into the standard Ethernet header. After performing the 802.1Q encapsulation, the circuit manager forwards the frame across the virtual connection toward the destination VLAN.

Implementation Considerations

Before you configure 802.1Q tagging on a router, note the following considerations:

- 802.1Q tagging is supported on 10BASE-T and 100BASE-T interfaces; it is not supported on other LAN interfaces.
- 802.1Q tagging cannot be used to extend a VLAN across multiple devices.
- The VLAN type (port-based, protocol-based, address-based, and so on) is ignored by the router.

Table 8-1 lists the platform modules that support 802.1Q tagging.

Table 8-1. Supported Modules for 802.1Q Tagging

Platform	Ethernet Interface Type
Passport 2430	10/100 Base Unit
Passport 2430	Second Ethernet Module
ARN	Ethernet Base Unit
ARN	ARN -48VDC Ethernet Base Unit
ARN	10/100-TX UTP Base Unit
ARN	Ethernet Expansion Module
ARN	Ethernet and Tri-Serial Expansion Module
ARN	Ethernet and 7-Serial Expansion Module
Passport 5430	Dual 10/100 Ethernet Base Unit
ASN	Dual Ethernet Net Module
BLN/BCN	Quad Port Ethernet FRE2-060
BLN/BCN	Quad Port Ethernet – High Speed Filters FRE2-060
BLN/BCN	Dual Ethernet/Dual Sync – No Filters FRE2-060
BLN/BCN	Dual Ethernet/Dual Sync – Max. Filters FRE2-060
BLN/BCN	Ethernet Sync/Async No Filters (ESAF) FRE2-060E
BLN/BCN	Ethernet Sync/Async With Filters (ESAFNF) FRE2-060E
BLN/BCN	Quad Port 10/100Base-TX with FRE4-PPC

Adding a Tagged Circuit to an Unconfigured 10BASE-T or 100BASE-T Interface

The following procedure describes how to add an 802.1Q tagged circuit to a previously unconfigured 10BASE-T or 100BASE-T interface. The procedure assumes that you are configuring the 802.1Q tagged circuit for IP routing. To enable other routing protocols on an 802.1Q tagged circuit, see the appropriate guide for that protocol.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a 10BASE-T or 100BASE-T connector.	The Add Circuit window opens.
2. Click on **OK**.	The Select Protocols window opens.
3. Choose **VLAN**, then click on **OK**.	The Edit VLAN Interface Parameters window opens.
4. Click on **Add**.	The TAG1Q Parameters window opens.
5. Set the following parameters: • **VLAN Name** • **Global VLAN Id** Click on **Help** to see the parameter descriptions.	
6. Click on **OK**.	The Edit VLAN Interface Parameters window opens. Note that 802.1Q tagged circuits are displayed with a V*n* extension.
7. Select the 802.1Q tagged circuit that you are adding. Set the **Protocol Type (hex)** parameter. Retain the default value for connection to Nortel Networks 802.1Q-enabled devices.	
8. Click on **Apply** and **Done**.	You return to the Configuration Manager window.
To add IP routing to the 802.1Q tagged circuit:	
9. Choose **Circuits**.	
10. Choose **Edit Circuits**.	The Circuit List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
11. Select the 802.1Q tagged circuit. Note that 802.1Q tagged circuits are displayed with a V*n* extension.	
12. Click on **Edit**.	The Circuit Definition window opens.
13. Choose **Protocols**.	
14. Choose **Add/Delete**.	The Select Protocols window opens.
15. Select **IP** and click on **OK**.	The IP Configuration window opens.
16. Enter an IP address and subnet mask and click on **OK**.	The Circuit Definition window opens.
17. Choose **File**.	
18. Choose **Exit**.	The Circuit List window opens.
19. Click on **Done**.	You return to the Configuration Manager window.

Adding a Tagged Circuit to an Existing 10BASE-T or 100BASE-T Interface

To add an 802.1Q tagged circuit to an existing 10BASE-T or 100BASE-T interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a 10BASE-T or 100BASE-T connector.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Choose **VLAN**, then click on **OK**.	The Edit VLAN Interface Parameters window opens.
6. Click on **Add**.	The TAG1Q Parameters window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Set the following parameters: • **VLAN Name** • **Global VLAN Id** Click on **Help** to see the parameter descriptions.	
8. Click on **OK**.	The Edit VLAN Interface Parameters window opens. Note that 802.1Q tagged circuits are displayed with a V*n* extension.
9. Select the 802.1Q tagged circuit that you are adding. Set the **Protocol Type (hex)** parameter. Retain the default value for connection to Nortel Networks 802.1Q-enabled devices.	
10. Click on **Apply** and **Done**.	You return to the Configuration Manager window.
To add IP routing to the 802.1Q tagged circuit:	
11. Choose **Circuits**.	
12. Choose **Edit Circuits**.	The Circuit List window opens.
13. Select the 802.1Q tagged circuit. Note that 802.1Q tagged circuits are displayed with a V*n* extension.	
14. Click on **Edit**.	The Circuit Definition window opens.
15. Choose **Protocols**.	
16. Choose **Add/Delete**.	The Select Protocols window opens.
17. Select **IP** and click on **OK**.	The IP Configuration window opens.
18. Enter an IP address and subnet mask and click on **OK**.	The Circuit Definition window opens.
19. Choose **File**.	
20. Choose **Exit**.	The Circuit List window opens.
21. Click on **Done**.	You return to the Configuration Manager window.

Version 15.5.0.0

The following implementation note is being added to the *BayRS Version 15.5.0.0 Documentation Change Notice* since it became available after publication of the 15.4.0.0 documentation.

Implementation Note for the ARN Router

When you configure VLAN tagging on an ARN 10MB Ethernet Base Module, the MTU for the Ethernet interface is set to 1518 bytes for the packets on this line. Although the ARN 10MB Ethernet Base Module supports tagged packets, it does not support 802.1Q tagged frames that are larger than 1518 bytes (1514 bytes plus the 4-byte tag).

However, there are other Ethernet interfaces (such as the Ethernet and Tri-Serial Expansion Module and the 10/100-TX UTP Base Module) that have an MTU of 1522 bytes and consequently, do support the maximum size tagged packet (1518 bytes plus the 4-byte tag).

Because of differences in the MTU size supported, when you configure VLAN tagging on an ARN 10MB Ethernet Base Module, you must make sure that no other tagged hosts on the LAN that are attached to the 10BT motherboard Ethernet port have MTUs greater than 1518 bytes. If they do, you must reset their respective MTUs to 1518 bytes so that they can interoperate properly with the ARN 10MB Ethernet Base Module.

Version 15.6.0.0

The following section supplements the information in Chapter 5, "Configuring 802.1Q Tagging," in *Configuring Ethernet, FDDI, and Token Ring Services* (part number 308623-15.0).

Using the BCC to Configure 802.1Q Tagged Circuits

Before Version 15.6, 802.1Q tagged ports could only be configured using Site Manager. With this release of BayRS, you can now use the BCC to configure 802.1Q tagged ports.

Note: The BayRS implementation of 802.1Q tagging has not changed for this release. The only change is that you can now set the same MIB variables with the BCC as you could with Site Manager.

For complete information about the BayRS implementation of VLANs and 802.1Q tagging, see *Configuring Ethernet, FDDI, and Token Ring Services* and the following sections in this chapter:

- "Router Processing of Tagged Frames" on page 8-2
- "Implementation Considerations" on page 8-2
- "Implementation Note for the ARN Router" on page 8-7

Adding a Tagged Circuit to a 10BASE-T or 100BASE-T Interface

To add an 802.1Q tagged circuit to a 10BASE-T or 100BASE-T interface, follow these steps:

1. Navigate to the 10BASE-T or 100BASE-T interface where you will configure the VLAN.

```
box# ethernet/2/1
ethernet/2/1#
```

2. Create a VLAN by entering this command:

vlan vlan-name *<vlan-name>* **global-vlan-id** *<global-vlan-ID>* [**protocol-type** *<protocol-type>*]

Table 8-2 describes the parameters and values that you enter.

Table 8-2. BCC VLAN Definition Parameters

Parameter	Values	Function
global-vlan-id	1 through 4095	Specifies a unique identifier for the VLAN within the Layer 2/Layer 3 topology. This numeric value must match the one assigned to the VLAN when it was initially configured on the adjacent Layer 2 device.
protocol-type	0x8100 (default) 0xf5EA-0xFFFF	Specifies the contents of the TPID field in 802.1Q encapsulated frames originated by this VLAN. This hexadecimal value must match the one assigned to the VLAN when it was initially configured on the adjacent Layer 2 device. You can accept the default value (0x8100) if this router connects to a Nortel Networks 802.1Q Layer 2/Layer 3 device.
vlan-name	string	Specifies a name to associate with the VLAN. BayRS does not use this string.

For example, the following command creates a VLAN called "test" with a global VLAN ID of "4."

```
ethernet/2/1# vlan vlan-name test global-vlan-id 4
vlan/test/4#
```

You can also enter the same command as follows:

```
ethernet/2/1# vlan test/4
vlan/test/4#
```

The following example creates a VLAN called "finance" with a global VLAN ID of 7 and a protocol type of 4705 (hex).

```
ethernet/2/1# vlan finance/7 protocol-type 4705
vlan/finance/7#
```

When you add a VLAN to the configuration, the VLAN is enabled by default.

3. Add an IP address to the configured VLAN.

```
vlan/test/4# ip 1.1.1.1/24
ip/1.1.1.1/255.255.255.0#
```

Editing a Tagged Circuit

The only VLAN parameter that you can change—other than the **state** parameter that disables and reenables a VLAN—is the **protocol-type** parameter. By default, this parameter is set to 0x8100 to allow this router to connect to a Nortel Networks 802.1Q Layer 2/Layer 3 device. If the router is connected to a non-Nortel Networks device, set this parameter to the appropriate value.

The following example changes the value of the **protocol-type** parameter for the VLAN "test" and displays the edited parameter.

```
ethernet/2/1# vlan test/4
vlan/test/4# protocol-type fffd
vlan/test/4# info
  global-vlan-id 4
  protocol-type 0xfffd
  state enabled
  virtual-port-type tagged
  vlan-name test
vlan/test/4#
```

Note: You cannot edit the **global-vlan-id** or **vlan-name** parameter. To change either parameter, you must delete the VLAN and re-create it with the correct VLAN name and global VLAN ID. Also, the only legal value for the **virtual-port-type** parameter is **tagged**, so do not try to edit this parameter.

Disabling a Tagged Circuit

To disable a tagged circuit, go to the VLAN prompt (for example, **box; eth 2/1; vlan engineering/2**) and enter:

state disabled

For example, the following commands disable and reenable the VLAN "engineering" on Ethernet interface 2/1:

```
box# ethernet/2/1
ethernet/2/1# vlan engineering/2
vlan/engineering/2# state disabled
vlan/engineering/2# info
  global-vlan-id 2
  protocol-type 0x8100
  state disabled
  virtual-port-type tagged
  vlan-name engineering
```

```
vlan/engineering/2# state enabled
vlan/engineering/2# info
  global-vlan-id 2
  protocol-type 0x8100
  state enabled
  virtual-port-type tagged
  vlan-name engineering
vlan/engineering/2#
```

Deleting a Tagged Circuit

To delete a tagged circuit from an Ethernet interface, go to the VLAN prompt (for example, **box; eth 2/1; vlan engineering/2**) and enter:

delete

For example, the following commands delete the VLAN “engineering” from Ethernet interface 2/1:

```
box# ethernet/2/1
ethernet/2/1# vlan engineering/2
vlan/engineering/2# delete
ethernet/2/1#
```

Displaying Information about Tagged Circuits

The BCC command **show tag1q circuits** displays information about the tagged circuits on the router. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tagged circuits only.
-enabled	Displays information about enabled tagged circuits only.
-circuit <*circuit_no*>	Displays information about the specified tagged circuit only.

The following example displays information about all tagged circuits configured on the router.

```
box# show tag1q circuits
show tag1q circuits                                  Nov 05, 2004 18:09:19 [EST]

Vlan (tag1q) Circuits
---------------------
---------------------------------------------------------------------------
                Vlan       Physical    <cct.#>              Protocol Enabled/
Vlan Name       Circuit    Circuit     Local Id Global Id Type     Disabled
------------  ---------    ---------  -------  --------- -------- --------
test             test        test       2        100        0x33024   enabled
test             test        test       3        101        0x33024   enabled
test             test        test       4        102        0x33024   disabled
```

The following example displays information about all enabled tagged circuits.

```
box# show tag1q circuits -enabled
show tag1q circuits -enabled                         Nov 05, 2004 18:12:20 [EST]

Vlan (tag1q) Circuits
---------------------
---------------------------------------------------------------------------
                Vlan       Physical    <cct.#>              Protocol Enabled/
Vlan Name       Circuit    Circuit     Local Id Global Id Type     Disabled
------------  ---------    ---------  -------  --------- -------- --------
test             test        test       2        100        0x33024   enabled
test             test        test       3        101        0x33024   enabled
```

The following example displays information about tagged circuit 3.

```
box# show tag1q circuits -circuit 3

show tag1q circuits -circuit 3                       Nov 05, 2004 18:12:34 [EST]

Vlan (tag1q) Circuits
---------------------
---------------------------------------------------------------------------
                Vlan       Physical    <cct.#>              Protocol Enabled/
Vlan Name       Circuit    Circuit     Local Id Global Id Type     Disabled
------------  ---------    ---------  -------  --------- -------- --------
test             test        test       3        101        0x33024   enabled
box#
```

Chapter 9
Configuring Frame Relay Services

Version 15.1.0.0

The following changes are required to the *Configuring Frame Relay Services* book.

A new frame relay parameter, Bw Threshold, has been added to the PVC List for Services window in Site Manager. The Bw Threshold parameter works in conjunction with the Committed Burst, Excess Burst, and Throughput parameters to shape traffic.

The following section updates the Site Manager procedure within the "Using Traffic Shaping" section in Chapter 4 and adds the parameter description to Appendix A, "Site Manager Parameters."

Using Traffic Shaping – Site Manager

To enable traffic shaping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Select the appropriate service record and click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on a PVC that you want to configure for traffic shaping.	
6. Set the following parameters: • **Committed Burst** • **Excess Burst** • **Throughput** • **Bw Threshold** Click on **Help** or see the parameter description in "Frame Relay PVC Parameters" on page A-27.	
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the Configuration Manager window.

Version 15.2.0.0

The following section describes a limitation that was omitted from *Configuring Frame Relay Services*.

Deleting PVCs from Service Records

The section "Deleting PVCs from Service Records" in *Configuring Frame Relay Services* should include the statement that Site Manager does not allow users to delete or move the last PVC in the only non-default service record. If you want to delete or move the last PVC, you must remove the entire service record.

Version 15.6.0.0

The following sections contain additions or amendments to *Configuring Frame Relay Services* (part number 308624-15.0 Rev 00).

Virtual Circuit Monitoring with the ifSpeed MIB Attribute

The following section contains amendments to Chapter 4, “Customizing PVCs,” in *Configuring Frame Relay Services* (part number 308624-15.0 Rev 00).

A number of network management and performance management applications use the ifSpeed MIB attribute to calculate traffic utilization on virtual circuits and to generate alarms when traffic utilization exceeds certain thresholds. Before Version 15.6, BayRS automatically set the ifSpeed MIB attribute to the line speed of the interface, not to the speed of the frame relay virtual circuits on that interface.

BayRS Version 15.6 supports a new parameter—called Optional Line Speed—for frame relay service records; the value that you set for this parameter is reported by the ifSpeed MIB variable. In this way, network management applications can use SNMP to obtain a user-configured value for the ifSpeed variable for a virtual circuit and generate alarms as appropriate.

Note: This new parameter applies to the service record only regardless of how many virtual circuits are configured under that service record.

By default, the ifSpeed variable is set to the line speed of the interface. You can set the optional line speed parameter to a value corresponding to the rate of the virtual circuit; that value will be reflected in the corresponding ifSpeed entry for each VC on the service record.

Note: The value that you set is for reporting purposes only; it has no effect on the actual performance of the frame relay virtual circuit.

You can use the BCC or Site Manager to configure the optional line speed parameter on a service record.

Using the BCC

To set a line speed value on a frame relay service record, navigate to the service record prompt (for example, **box; serial/3/1; frame-relay/3/1; service/kiev**) and enter:

optional-line-speed *<integer>*

integer is the line speed for the service record in bits per second.

For example, the following command sets the line speed for frame relay service record “kiev” to 1000000 bits per second:

```
serial/3/1# frame-relay
frame-relay/3/1# service kiev
service/kiev# optional-line-speed 1000000
service/kiev#
```

Using Site Manager

To specify a line speed value for a frame relay service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Click on the service record that you want to configure a line speed for.	
5. Set the **Optional Line Speed** parameter. Click on **Help** or see the parameter description on page A-31.	
6. Click on **Done**.	You return to the Configuration Manager window.

Frame Relay Traffic Shaping with DSQMS

Before Version 15.6.0.0, frame relay traffic shaping was implemented using protocol prioritization (priority queuing) as the QoS mechanism. That is, priority queuing was used to shape PVCs at the frame relay level, even if DSQMS was configured at the interface level.

With Version 15.6.0.0, when you configure DSQMS at the interface level, DSQMS will also be used as the QoS mechanism at the frame relay level. (Only PVCs can use DSQMS; SVCs are not supported.)

Note: PVCs use the DSQMS configuration on the interface; you do not configure DSQMS directly on a PVC.

The combination of traffic shaping and DSQMS queuing and scheduling enhances QoS over frame relay virtual circuits and enables you to monitor traffic statistics for individual virtual circuits using DSQMS MIB attributes. This feature is supported on all frame relay interfaces—other than dial and multiline/multilink interfaces—across all BayRS router platforms.

- At the frame relay level, DSQMS enforces the following behavior:
  - All IP packets, including router-generated IP packets from shaped PVCs, are classified on the basis of DSCP values and queued accordingly. Non-IP packets receive best-effort treatment.
  - Each PVC uses two reserved queues (IntQ1 and IntQ2) as well as queues that you configure. (Statistics are reported for up to eight configurable queues only.)
- At the driver/interface level, DSQMS enforces the following behavior:
  - All packets from shaped PVCs are placed in the frame relay shaped queue.
  - Packets from non-shaped PVCs are classified on the basis of DSCP values and queued accordingly.

For information about configuring traffic shaping for frame relay PVCs, see Chapters 1 and 4 in *Configuring Frame Relay Services*, as well as "Using Traffic Shaping – Site Manager" on page 9-1. For information about configuring DSQMS, see Chapters 2 and 6 in *Configuring Differentiated Services*, as well as Chapter 6, "Configuring Differentiated Services in this Document Change Notice.

Configuration Prerequisites

To use DSQMS as the QoS mechanism for frame relay PVCs, you must:

- Configure DSQMS on the interface.
- Enable traffic shaping on one or more PVCs on the frame relay interface.

DSQMS applies only to shaped PVCs; traffic from non-shaped PVCs is processed by the DSQMS instance running on the interface.

Implementation Note: Configuring the Packet Limit for Queues

To use DSQMS as the QoS mechanism for frame relay PVCs, you may need to adjust the value of the Packet Limit parameter (for a description of the Site Manager parameter, see page A-22). The Packet Limit parameter specifies the maximum number of packets that this queue can hold. When the queue is used by shaped frame relay PVCs, the default value of 0 sets the packet limit to 20.

In some cases, this default value increases clipping of voice packets. If you discover that voice packets are being lost, Nortel recommends that you reset the Packet Limit parameter on the queue that services EF packets to a higher value, for example, 128 or 256. However, be aware that this higher value may increase latency. You may need to fine-tune the value of the Packet Loss parameter to find one that works best for your configuration.

Note: After you reset this parameter, you must save the configuration file and reboot the router.

BCC show Command Enhancement

To support this QoS enhancement, the output of the BCC **show frame-relay stats** command provides DSQMS statistics at the frame relay PVC level. The following information supplements Appendix C, "Monitoring Frame Relay Using the BCC show Command," in *Configuring Frame Relay Services*.

show frame-relay stats shaping dsqms-queues

Displays outbound traffic statistics for traffic-shaped PVCs at the frame relay level when DSQMS is configured at the interface.

This command supports the following subcommand options:

-circuit *<circuit>*	Displays information about the PVCs configured on the specified circuit only.
-dlci *<dlci>*	Displays information about PVCs with the specified DLCI only.

Following is an example of the output from a single-PVC configuration with two queues:

`bcc>` **show frame-relay stats shaping dsqms-queues**

```
show frame-relay stats shaping dsqms-queues        Apr 23, 2005 08:16:52 [GMT]

                                Pkt      Byte     Xmit      Xmit     Dropped      Dropped
Cct      DLCI        Id/Type    Count    Count    Pkts      Bytes    Pkts         Bytes
------   --------    -------    -------- -------- --------  -------- --------     --------
   N/C indicates "Not Configured"
S12      100         IntQ1     0            0           0         0           0            0
S12      100         IntQ2     0            0           0         0           0            0
S12      100         1         0            0           0         0           0            0
S12      100         2         0            0          43      2010           0            0
S12      100         3 (N/C)   0            0           0         0           0            0
S12      100         4 (N/C)   0            0           0         0           0            0
S12      100         5 (N/C)   0            0           0         0           0            0
S12      100         6 (N/C)   0            0           0         0           0            0
S12      100         7 (N/C)   0            0           0         0           0            0
S12      100         8 (N/C)   0            0           0         0           0            0
```

New Technician Interface Script

To support this QoS enhancement, a new Technician Interface script file called pvc_stats.bat is now available. Like the BCC **show frame-relay stats shaping dsqms-queues** command, this script provides DSQMS statistics at the frame relay PVC level.

The syntax of this script is as follows:

show pvc_stats [**-dlci** *<dlci>*] [**-circuit** *<circuit>*]

New MIB for Monitoring DSQMS at the PVC Level

You can also monitor DSQMS traffic statistics at the frame relay PVC level using a new MIB called wfFrVCStatsEntry. This transient statistics MIB record is only present when frame relay traffic shaping functionality uses DSQMS.

Configuring FRF.9 Compression

Before Version 15.6.0.0, frame relay data compression was performed by the proprietary Nortel Networks compression protocol WCP. WCP provides superior performance for BayRS routers, but it does not interoperate with other vendors' equipment. With Version 15.6.0.0, BayRS also supports frame relay data compression as per FRF.9 to allow interoperation with other equipment.

FRF.9 is a frame relay standard for data compression on virtual connections. FRF.9 improves bandwidth utilization on frame relay links and, unlike WCP, supports interoperability with other vendors' equipment.

BayRS supports FRF.9 end to end, that is, from data termination equipment (DTE) to DTE over a frame relay core network. FRF.9 data compression is supported on all frame relay interfaces—other than dial and multiline/multilink interfaces—across all BayRS router platforms. FRF.9 is configurable on a per-VC basis and is disabled by default.

Caution: Software data compression, including the BayRS implementation of FRF.9, is a computationally intensive operation. On high-speed interfaces, a router may have insufficient resources to sustain the compressed data stream. Configure FRF.9 compression on slow-speed lines only (lines not exceeding the E1 rate).

The BayRS implementation of FRF.9 is based on the Stac LZS algorithm, and the compression control protocol is based on the Data Compression Protocol (DCP) as recommended in the FRF.9 specification. The combination of the Stac LZS compression algorithm and the DCP handshake protocol is referred to as LZS-DCP and is specified in Annex A of the FRF.9 standard.

The Data Compression Protocol includes these PDUs:

- DCP control PDUs: used in the handshake procedure between the peers
- DCP data PDUs: carry the compressed or uncompressed payload

DCP also includes support for anti-expansion and synchronization procedures.

An FRF.9 frame contains a DCP header and DCP payload and is identified with a network layer protocol identifier (NLPID) of 0xB0. For complete information about FRF.9 data compression, see “Data Compression over Frame Relay Implementation Agreement - FRF.9,” Frame Relay Forum Technical Committee, January 22, 1996.

Implementation of FRF.9 Compression on BayRS Routers

The BayRS implementation of FRF.9 data compression provides the following:

- FRF.9 data compression is supported on PVCs and SVCs.
- FRF.9 compression is not supported for multilink frame relay circuits or for dial interfaces.
- Compression is available in software only.
- BayRS implementation of FRF.9 compression uses only one compression algorithm: Hi/fn Stac LZS, as per FRF.9 Annex A.

➡ **Note:** The Hi/fn LZS compression software is licensed from Hi/fn, Inc. You must separately purchase a license for the Hi/fn LZS compression software, which is delivered on a separate CD by Nortel Networks.

- Compression options and compression history synchronization are in conformance with FRF.9 Annex A. (BayRS supports only one compression history—or context—per VC, which is the default value in FRF.9 Annex A.)
- FRF.9 standard contains two modes of operation for the DCPCP: Mode 1 and Mode 2. BayRS supports Mode 1 only.
- Error detection method, history context selection, and compression process options are as provided for by FRF.9 Annex A and selected by Mode 1 negotiation of that standard.

Configuration Considerations

Before you configure FRF.9, be aware of the following considerations:

- You cannot enable both WCP and FRF.9 compression on a VC. WCP is enabled by default, so you may need to disable WCP before you can enable FRF.9 compression. (You can disable both WCP and FRF.9 compression.)

- Configure FRF.9 on low-speed interfaces to optimize bandwidth utilization. All BayRS routers support slow-speed lines configured with FRF.9 compression, but full line rate data compression on high-speed interfaces cannot be supported on even the fastest processors of BayRS routers.
- Small frames are less likely to experience a reduction in byte count from compression. You can set a threshold to instruct the router to skip compression when a frame is smaller than the byte count you specify. This test of the compression threshold is performed for each outgoing buffer.
- Some frame relay configurations have large numbers of virtual circuits, and each circuit must have separate context information, so the amount of memory consumed per VC may be excessive. The use of Hi/fn software to perform compression makes the size of this memory area fixed at approximately 24 KB per VC.
- With Stac LZS compression, data can expand in size (byte count) as a result of compression, particularly if the data has already undergone a compression process (JPEG files, for example). A frame that expands due to compression is sent, as long as the outgoing frame does not exceed the MTU. This behavior may result in less than optimal bandwidth utilization.

FRF.9, FRF.12, and Traffic Shaping

FRF.9 data compression, FRF.12 fragmentation and interleaving, and PVC traffic shaping can all work together. When configured together, these features are executed on an outgoing PVC in this order:

1. Traffic shaping with DSQMS or protocol prioritization takes place (if FRF.12 is configured, you must use traffic shaping with DSQMS).
2. FRF.9 compresses traffic from the shaped PVCs.
3. FRF.12 fragments the compressed packets.

On an incoming PVC, reassembly of fragmented packets is done before decompression.

Note: Testing indicates that configuring frame relay traffic shaping with DSQMS, FRF.9, and FRF.12 on the same PVC is very CPU intensive and performance degradation is expected. It is recommended that either FRF.9 or FRF.12 be used, whichever is applicable to the network need.

Configuring FRF.9 Compression

You can use the BCC or Site Manager to configure FRF.9 compression on frame relay PVCs and SVCs. By default, FRF.9 compression is disabled.

Using the BCC

To enable FRF.9 compression on a frame relay PVC or SVC, navigate to the PVC or SVC prompt (for example, **box; serial/3/1; frame-relay; service/paris; pvc/3/1/33** or **box; serial/3/2; frame-relay; service/newyork; svc-options/ toronto**) and enter:

frf9-control {**enabled** | **disabled**}

Note: WCP compression and FRF.9 compression cannot be enabled at the same time. Because WCP compression is enabled by default, you will probably need to disable WCP before you can enable FRF.9 compression.

To set a minimum size for frames to be compressed by FRF.9 on the PVC or SVC, enter:

frf9-min-compress-size *<integer>*

<integer> is the minimum byte count for frames to be compressed by FRF.9. The default value is 0—that is, all frames going out this PVC or SVC are compressed.

For example, the following commands disable WCP compression, enable FRF.9 compression, and set the minimum frame size for FRF.9 compression to 500 bytes on PVC 3/1/33.

```
serial/3/1# frame-relay
frame-relay/3/1# service paris
service/paris# pvc/3/1/33
pvc/3/1/33# wcp-control disabled
pvc/3/1/33# frf9-control enabled
pvc/3/1/33# frf9-min-compress-size 500
pvc/3/1/33#
```

The following commands disable WCP compression and enable FRF.9 compression on SVC toronto.

```
serial/3/2# frame-relay
frame-relay/3/2# service/newyork; svc-options/toronto
svc-options/toronto# wcp-control disabled
svc-options/toronto# frf9-control enabled
```

Using Site Manager

To configure FRF.9 compression on a frame relay PVC, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Select the service record that has the PVC that you want to configure FRF.9 for.	
5. Click on **PVCs**.	The FR PVC List for Service window opens.
6. Select the PVC that you want to configure for FRF.9.	
7. If necessary, set the **WCP Enable** parameter to **Disable**. WCP and FRF.9 cannot operate on one PVC. WCP is enabled by default.	
8. Set the **FRF.9 Enable** parameter to **Enable**. Click on **Help** or see the parameter description on page A-29.	
9. If necessary, set the **FRF.9 Min Compress Size** parameter. Click on **Help** or see the parameter description on page A-29.	
10. Click on **Done**.	You return to the Frame Relay Service List window.
11. Click on **Done**.	You return to the Configuration Manager window.

To configure FRF.9 compression on a frame relay SVC, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Select the service record that has the SVC that you want to configure FRF.9 for.	
5. Click on **SVCs**.	The FR SVC Options List for Service window opens.
6. Select the SVC that you want to configure for FRF.9.	
7. If necessary, set the **WCP Enable** parameter to **Disable**. WCP and FRF.9 cannot operate on one SVC. WCP is enabled by default.	
8. Set the **FRF.9 Enable** parameter to **Enable**. Click on **Help** or see the parameter description on page A-32.	
9. If necessary, set the **FRF.9 Min Compress Size** parameter. Click on **Help** or see the parameter description on page A-32.	
10. Click on **Done**.	You return to the Frame Relay Service List window.
11. Click on **Done**.	You return to the Configuration Manager window.

Configuring FRF.12 Fragmentation and Interleaving

With Version 15.6.0.0, BayRS implements the Frame Relay Fragmentation Implementation Agreement, FRF.12, supporting the end-to-end fragmentation format only.

Overview of FRF.12 Fragmentation and Interleaving

FRF.12 defines frame relay extensions that allow a sender to fragment the packets within a VC. With FRF.12, transmitting frame relay DTEs and DCEs fragment long frames into a sequence of shorter frames; the receiving peer DTE or DCE reassembles the fragments into the original frame.

FRF.12 defines only packet fragmentation and reassembly; it does not define an interleaving scheme for the fragments. However, FRF.12 fragmentation allows high-priority packets of one VC to be sent (interleaved) between fragments of lower-priority packets of the same or other VCs.

The BayRS implementation of FRF.12 provides a Layer 2 fragmentation and interleaving solution for frame relay WANs to ensure high voice quality for VoIP packets transmitted with data packets over links slower than T1 speeds. FRF.12 fragmentation and interleaving is supported on all frame relay interfaces—other than dial and multiline/multilink interfaces—across all BayRS router platforms, subject to memory and performance constraints.

The BayRS implementation of FRF.12 produces better voice quality by addressing the problem of “jitter” due to large data packets being transmitted between small VoIP packets. When FRF.12 is enabled, large data packets are fragmented into smaller packets and higher-priority voice packets are sent between (interleaved with) the data packet fragments. (VoIP packets are never fragmented.)

Data packets are fragmented to a fixed size as they are transmitted over the WAN. You can change the default data fragment size and the number of voice packets to be interleaved between data packet fragments. By default, one voice packet followed by one data packet fragment are transmitted over the WAN after fragmentation and interleaving.

Interleaving of fragments is supported over a single VC or across multiple VCs on an interface. In a multiple-VC configuration, all VCs must be configured for FRF.12; each VC can be configured to carry a certain type of traffic, for example, EF, AF*xx*, or DF.

Packet Fragmentation and Reassembly

The end-to-end fragmentation format is based on the frame structure identified in the FRF.12 standard. An NLPID of 0xB1 is used to identify the end-to-end fragmentation format. Each packet fragment has a separate sequence number.

When FRF.12 fragmentation is enabled, packets are fragmented and reassembled as follows:

1. Data fragments are created based on the configured fragment size. The first fragment for a specific frame has the B (Begin) bit set, and the last fragment has the E (End) bit set. Every fragment in the series contains the same address octets that were on the original unfragmented frame, including the frame relay congestion bits.
2. The receiver for the PVC keeps track of the incoming sequence numbers and maintains the most recently received sequence number. The receiver detects the end of a reassembled frame when it receives a fragment bearing the E (End) bit.
3. If a fragment is detected as missed on the receiving PVC, the receiver discards all currently unassembled and subsequently received fragments for that packet until it receives the first fragment that bears the B (Begin) bit.

Note: Any packet not marked with a DSCP of "EF" is fragmented, even packets smaller than the configured fragment size; these small packets contain the B (Begin) and E (End) bits in the same packet. (If you examine a trace of traffic from a frame relay link running FRF.12, the only traffic that is not fragmented is the EF-marked VoIP packets.)

Interoperability of BayRS FRF.12 Implementation

The BayRS implementation of FRF.12 fragmentation and interleaving interoperates with the following FRF.12 implementations:

- Nortel Networks Passport 7000/15000

  The Passport 7000/15000 support FRF.12 in the end-to-end (DTE-to-DTE) fragmentation format only. For good voice quality using FRF.12, the Passport 7000/15000 requires more than one PVC to each destination.

- Cisco* 3600/7000 series routers

  The Cisco implementation must use end-to-end fragmentation.

- FRF.5 frame relay/ATM network interworking (as defined in Section 7 and Appendix A of the FRF.12 specification)

  The fragment size must be set to an even multiple of the underlying ATM cell payload size in order to optimize the performance at the ATM layer.

Implementation of FRF.12 Fragmentation and Interleaving on BayRS

BayRS implements FRF.12 fragmentation and interleaving as follows:

- FRF.12 is supported for PVCs only and is configurable on a per-PVC basis. The fragment size is configurable for each FRF.12 PVC.
- You can configure the fragment size of data packets on each PVC; the default fragment size is 80 bytes. Packets smaller than the configured fragment size are sent without fragmentation.
- VoIP packets are not fragmented.
- FRF.12 is not supported on dial or multiline/multilink frame relay interfaces.
- BayRS supports the end-to-end fragmentation format only.

  The end-to-end fragmentation format is used in both the DTE-to-DTE configuration (BayRS-to-BayRS) and in the DTE-to-DCE configuration (BayRS-to-Passport 7000/15000).

➡ **Note:** FRF.12 interface fragmentation format (UNI and NNI fragmentation) and the FRF.11 Annex C fragmentation format are not supported.

- Both sides of the circuit must be configured for FRF.12 fragmentation.
- FRF.12 fragmentation is implemented within frame relay. The associated interleaving is implemented at the interface level (within DSQMS). Interleaving uses only two classes of packets—voice (DSCP-defined) and non-voice—and no reordering of packets occurs within either class.
- Enabling and disabling FRF.12 fragmentation causes the PVC to restart.
- DSQMS traffic shaping must be configured on the PVCs. (Protocol prioritization is not supported at the PVC or interface level for FRF.12.)
- DSQMS and FRF.12 interleaving must be configured on the interface associated with an FRF.12 PVC.

- If any PVC on a slow-speed interface (1 Mb/s or less) is configured for FRF.12, all other PVCs on that interface must also be configured for FRF.12.

  For higher-speed interfaces, all PVCs to the same destination over that interface must also be configured for FRF.12.

FRF.9, FRF.12, and Traffic Shaping

FRF.9 data compression, FRF.12 fragmentation and interleaving, and PVC traffic shaping can all work together. When configured together, these features are executed on an outgoing PVC in this order:

1. Traffic shaping with DSQMS takes place (when FRF.12 is configured, you must use traffic shaping with DSQMS).
2. FRF.9 compresses traffic from the shaped PVCs.
3. FRF.12 fragments the compressed packets.

On an incoming PVC, reassembly of fragmented packets is done before decompression.

Note: Testing indicates that configuring frame relay traffic shaping with DSQMS, FRF.9, and FRF.12 on the same PVC is very CPU intensive and performance degradation is expected. It is recommended that either FRF.9 or FRF.12 be used, whichever is applicable to the network need.

Configuration Considerations

Before you configure FRF.12 fragmentation and interleaving, be aware of the following considerations:

- You may need to configure ingress diffserv filters to mark voice and data packets with diffserv code points (DSCPs). Make sure that VoIP packets are marked with the expedited forwarding (EF) diffserv marking in the IP header.
- Implementing FRF.12 increases the volume of small packets. High volumes of small packets are known to affect the performance of BayRS routers.

  You should set the data fragment size as close to the VoIP packet size as possible to optimize the link. For improved VoIP performance, data fragments are needed, but for CPU performance, you want fewer fragments. You may need to fine-tune the data fragment size to find one that works best for your configuration. The type of VoIP equipment in use affects this value.

- Scaling limitations may apply on the number of PVCs that can be supported with FRF.12 on an interface or slot, especially for routers such as the BN that provide VC aggregation in an end-to-end frame relay network.

  These scaling limitations are affected by the processor speed, the fragment size (and the size of the data packet to be fragmented), and the number of PVCs that implement FRF.12 on the slot.

Configuring FRF.12 Fragmentation and Interleaving

To configure FRF.12 fragmentation and interleaving on the router, you must enable traffic shaping and FRF.12 fragmentation on the frame relay PVCs and configure DSQMS parameters on the interface associated with the PVCs.

Note: To implement FRF.12 fragmentation and interleaving, you may also need to configure ingress traffic filters to mark VoIP packets with the EF DSCP. For instructions on configuring ingress traffic filters, see Chapter 3 of *Configuring Differentiated Services* (part number 308620-14.20 Rev 00).

You can use the BCC or Site Manager to configure FRF.12 fragmentation and interleaving on the router. By default, FRF.12 fragmentation and interleaving are disabled.

Configuration Steps

To configure FRF.12 fragmentation and interleaving on the router, perform the following steps. These steps are described in detail in the following sections.

1. Configure DSQMS on the interface.

   If necessary, add DSQMS to the list of protocols on the interface.

2. Configure traffic shaping on the PVC or PVCs.

   Set values for these traffic shaping parameters: committed information rate (CIR), committed burst, and excess burst.

3. Enable FRF.12 fragmentation on the PVCs and reset the data packet fragmentation size if necessary.

4. Enable FRF.12 interleaving on the interface and reset the weighting of data packet fragments and voice packets in the stream, if necessary.

For information and instructions on configuring a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

If you will use the BCC to configure FRF.12 parameters, go to the next section. If you will use Site Manager, go to “Using Site Manager” on page 9-23.

Using the BCC

The following sections describe how to use the BCC to configure FRF.12 fragmentation and interleaving on the router.

Configure DSQMS on the Interface

To configure DSQMS on the interface where the frame relay PVCs are configured, navigate to the appropriate interface and enter the **dsqms** command:

```
box# serial 3/1
serial/3/1# dsqms
dsqms/serial/3/1/S31#
```

Note: For complete information about configuring DSQMS queues and classifiers, see Chapter 2 and Appendix B of *Configuring Differentiated Services* (part number 308624-14.20 Rev 00).

Configure Traffic Shaping on the PVCs

To configure traffic shaping on the PVCs where frame relay fragmentation will occur, follow these steps:

1. Navigate to a PVC that will fragment data packets as per FRF.12.

   ```
   dsqms/serial/3/1/S31# back
   serial/3/1# frame-relay; service/boston
   service/boston# pvc 33
   pvc/3/1/33#
   ```

2. Set the committed information rate (CIR) for the PVC.

   ```
   pvc/3/1/33# cir <integer>
   ```

   integer is the number of guaranteed bits/s that the router can transmit over a specified time interval when no congestion is occurring.

Note: For complete information about configuring traffic shaping on PVCs, see *Configuring Frame Relay Services* (part number 308624-15.0 Rev 00).

3. Set the committed burst rate (B_c) for the PVC. In general, you set this parameter to 1/4 the value of the CIR.

   `pvc/3/1/33#` **committed-burst** *<integer>*

   integer is the maximum number of bits/s that the router can transmit over a specified time interval when congestion occurs.

4. Set the excess burst rate (B_e) for the PVC. If you set this parameter to a value other than 0 (the default value), the router can send traffic exceeding the CIR.

   `pvc/3/1/33#` **excess-burst** *<integer>*

   integer is the number of extra bits/s that the router attempts to transmit over a specified time interval when congestion occurs.

Configure FRF.12 Fragmentation on the PVCs

To configure FRF.12 fragmentation on the appropriate PVCs, follow these steps:

1. Navigate to a PVC that will fragment data packets as per FRF.12.

   `serial/3/1#` **frame-relay; service/boston; pvc 33**
   `pvc/3/1/33#`

2. Enable FRF.12 fragmentation on the PVC.

   `pvc/3/1/33#` **frf12-fragmentation-enable enabled**

   (To disable FRF.12, enter **frf12-fragmentation-enable disabled**.)

3. If necessary, change the minimum size of data packets to be fragmented on the PVC. The default value is 80 bytes.

   `pvc/3/1/33#` **frf12-fragmentation-trigger-size** *<integer>*

   integer is the minimum size of a data packet to fragment on this PVC; this value specifies the size of the fragmented packet payload. Any packet smaller than the specified number of bytes will not be fragmented.

Configure FRF.12 Interleaving on the Interface

To configure FRF.12 interleaving on the interface where the PVCs are configured, follow these steps:

1. Navigate to the appropriate interface DSQMS prompt.

   ```
   pvc/3/1/33# box
   box# serial/3/1; dsqms
   dsqms/serial/3/1/S31#
   ```

2. Enable FRF.12 interleaving on the interface.

   `dsqms/serial/3/1/S31#` **frf12-frag-interleaving-enable enabled**

   (To disable interleaving, enter **frf12-frag-interleaving-enable disabled**.)

3. If needed, change the maximum number of consecutive data packet fragments to send with no voice packets interleaved. The default value is 3.

   `dsqms/serial/3/1/S31#` **frf12-nonpriority-high-water-mark** *<integer>*

   integer is a value from 1 through 64. DSQMS stops dequeuing packets when the value specified by this parameter is reached if it does not find any voice packets to interleave with the data packet fragments.

4. If necessary, change the number of voice packets to interleave between data packet fragments. The default value is 1.

   `dsqms/serial/3/1/S31#` **frf12-priority-fragment-weight** *<integer>*

   integer is a value from 1 through 64.

Configuration Example Using the BCC

Following is an extended example of using the BCC to configure all FRF.12 fragmentation and interleaving parameters.

```
box# serial 3/1
serial/3/1# dsqms
dsqms/serial/3/1/S31# back
serial/3/1# frame-relay
frame-relay/3/1# service boston
service/boston# pvc 33
pvc/3/1/33# info
  cir 0
  clear-high-water 0
  committed-burst 0
  congestion-control inherit
  congestion-counter 20
```

```
  congestion-method inherit
  congestion-timer 1
  dlci 33
  excess-burst 0
  frf12-fragmentation-enable enabled
  frf12-fragmentation-trigger-size 100
  frf9-control enabled
  frf9-min-compress-size 0
  high-queue-limit inherit
  low-queue-limit inherit
  multicast-control disabled
  normal-queue-limit inherit
  primary-ignore-status-timer 30
  startup-delay-timer disabled
  vc-state active
  wcp-control disabled
pvc/3/1/33# cir 5000
pvc/3/1/33# committed-burst 1250
pvc/3/1/33# excess-burst 1000
pvc/3/1/33# frf12-fragmentation-enable enabled
pvc/3/1/33# frf12-fragmentation-trigger-size 100
pvc/3/1/33# box
box# serial/3/1; dsqms
dsqms/serial/3/1/S31# info
  debug-level none
  dequeue-at-line-rate disabled
  frf12-frag-interleaving-enable disabled
  frf12-nonpriority-high-water-mark 3
  frf12-priority-fragment-weight 1
  restart notset
  state enabled
dsqms/serial/3/1/S31# frf12-frag-interleaving-enable enabled
dsqms/serial/3/1/S31# frf12-nonpriority-high-water-mark 5
dsqms/serial/3/1/S31# frf12-priority-fragment-weight 2
dsqms/serial/3/1/S31#
```

Using Site Manager

To configure FRF.12 fragmentation and interleaving on the router, complete the tasks in this section. It is assumed that the frame relay interface and PVCs have already been configured.

Enabling DSQMS on the Frame Relay Interface

If DSQMS is already enabled on the frame relay interface where you will configure FRF.12, go to the next section, "Configuring Traffic Shaping on the Frame Relay PVCs" on page 9-25.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Select the default service record. You can add DSQMS only to the default service record.	
5. Choose **Protocols** > **Add/Delete**.	The Select Protocols window opens.
6. In the Select Protocols window, select **DSQMS** and click on **OK**.	The Edit DSQMS Parameters window opens.
7. If necessary, set the following parameters: • **Debug Level** • **Dequeue At Line Rate** Click on **Help** or see the parameter descriptions beginning on page A-17.	
8. Click on **Restart**. When you edit parameters for a DSQMS interface, you must restart DSQMS on the interface for the changes to take effect.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
11. Click on **Done**.	You return to the Configuration Manager window.

Configuring Traffic Shaping on the Frame Relay PVCs

If traffic shaping is already configured, go to the next section, "Configuring FRF.12 Fragmentation on the Frame Relay PVCs" on page 9-26. To enable traffic shaping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Select the appropriate service record and click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on a PVC that you want to configure traffic shaping on.	
6. Set the following parameters: • **Committed Burst** • **Excess Burst** • **Throughput** • **Bw Threshold** Click on **Help** or see the parameter descriptions beginning on page A-27.	
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the Configuration Manager window.

Configuring FRF.12 Fragmentation on the Frame Relay PVCs

To configure FRF.12 fragmentation on the PVCs, complete the following tasks.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Select the appropriate service record and click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on a PVC that you want to configure FRF.12 fragmentation on.	
6. Set the following parameters: • **FRF.12 Fragmentation Enable** • **FRF.12 Fragmentation Trigger Size** Click on **Help** or see the parameter descriptions beginning on page A-30.	
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the Configuration Manager window.

Configuring FRF.12 Interleaving on the Frame Relay Interface

To configure FRF.12 interleaving on the frame relay interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **DSQMS**.	The DSQMS menu opens.
4. Choose **Interface**.	The Edit DSQMS Parameters window opens.
5. Select the interface that you want to configure FRF.12 interleaving on.	
6. Set the following parameters: • **FRF.12 Interleaving Enable** • **FRF.12 NonPriority High Water Mark** • **FRF.12 Priority Fragment Weight** Click on **Help** or see the parameter descriptions beginning on page A-18.	
7. Click on **Done**.	You return to the Configuration Manager window.

Chapter 10
Configuring GRE, NAT, RIPSO, and BFE Services

Version 15.5.0.0

The following information supplements Chapter 1, "Configuring GRE Tunnels," in *Configuring GRE, NAT, RIPSO, and BFE Services*.

Configuring GRE Keepalive Functionality

Beginning with Version 15.5.0.0, BayRS provides a more robust environment for packet forwarding over Generic Routing Encapsulation (GRE) tunnels by creating a keepalive mechanism that enables a router to monitor GRE traffic from a remote end point. When this feature is enabled, a router can verify that the status of a tunnel's state is 'up' before it forwards packets over it.

You configure GRE keepalive functionality by performing the following tasks:

- Enabling or disabling keepalive messages
- Configuring the keepalive retry timeout interval
- Configuring the keepalive retries value

The output for the following BCC **show** commands is enhanced to provide information about the GRE keepalive mechanism:

- **show gre logical-ip-tunnels**
- **show gre logical-ipx-tunnels**
- **show gre physical-tunnels**

For information about the enhanced output of these BCC **show** commands, see Chapter 20, "Reference for BCC IP show Commands," in this document.

Enabling and Disabling GRE Keepalive Messages for a Remote Tunnel End Point

The GRE keepalive message functionality is disabled by default.

You can use the BCC or Site Manager to enable and disable the transmission of GRE keepalive messages between a GRE tunnel's local end point and one of its configured remote tunnel end points.

Using the BCC

To enable and disable the transmission of GRE keepalive messages between a tunnel's local end point and one of its remote tunnel end points, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

keepalive *<state>*

state is one of the following:

enabled
disabled (default)

For example, the following command sequence enables transmission of GRE keepalive messages between the local end point and the remote end point *austin* and verifies the change:

```
remote-endpoint/austin# keepalive enabled
remote-endpoint/austin# info
  address 192.168.2.4
  keepalive enabled
  logical-ip-address 0.0.0.1
  logical-ipx-address 000000000001
  name austin
  keepalive-retries 3
  keepalive-retry-timeout 10
  state enabled
```

Using Site Manager

To enable and disable the transmission of GRE keepalive messages between a tunnel's local end point and one of its configured remote end points, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Select the remote tunnel end point that you want to disable or reenable from the list.	
6. Set the **Keepalive** parameter. Click on Help or see the parameter description on page A-33.	
7. Click on **Apply.**	The transmission of GRE keepalive messages is enabled or disabled for the selected tunnel end point.

Setting the Timeout Interval for GRE Keepalive Messages

When you enable the GRE keepalive message functionality, the timeout interval is set to 10 seconds by default. The timeout interval is the amount of time in seconds that the router waits between sending successive keepalive messages from a GRE tunnel's local end point to one of its remote end points.

You can use the BCC or Site Manager to change the value of the timeout interval.

Using the BCC

To change the default value of the GRE keepalive retry timeout interval for a GRE tunnel's remote end point, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

keepalive-retry-timeout-<*value*>

value is an integer between 1 and 32766, inclusive. It represents the number of seconds that the router waits between sending successive GRE keepalive messages from the GRE tunnel's local end point to one of its remote end points.

For example, the following command sequence changes the keepalive retry timeout interval for the remote tunnel *austin* to 20 seconds and verifies the change:

```
remote-endpoint/austin# keepalive-retry-timeout 20
remote-endpoint/austin# info
  address 192.168.2.4
  keepalive enabled
  logical-ip-address 0.0.0.1
  logical-ipx-address 000000000001
  name austin
  keepalive-retries 3
  keepalive-retry-timeout 20
  state enabled
```

Using Site Manager

To change the default value of the GRE keepalive retry timeout interval for a remote tunnel end point, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Click on **Remote Conn**.	The GRE Remote Connections List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Select the remote tunnel end point for which you want to set the keepalive retry timeout interval value from the list.	
6. Set the **Keepalive Retry Timeout** parameter. Click on **Help** or see the parameter description on page A-33.	
7. Click on **Apply.**	The GRE keepalive timer is set for the selected tunnel end point.

Setting the Keepalive Retries Parameter for GRE Keepalive Messages

When you enable the GRE keepalive message functionality, the value of the keepalive retries parameter is set to 3 by default. The keepalive retries parameter is the multiplier used to calculate the amount of time that the router waits for a reply after sending a GRE keepalive message to a remote end point before declaring that the GRE tunnel is down.

You can use the BCC or Site Manager to change the value of the timer interval.

Using the BCC

To change the default value of the GRE keepalive retries parameter for a remote tunnel end point, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

keepalive-retries *<value>*

value is an integer between 2 and 254, inclusive. The default value is 3. It represents the number by which to multiply the currently configured value of the keepalive retry timeout interval. For example, if the keepalive retry timeout interval is set to 20 (seconds) and you set the keepalive retries value to 6, then the router waits for 120 seconds (6 x 20 seconds) for a reply message before declaring that the GRE tunnel is down.

For example, the following command sequence changes the keepalive retries value for the remote tunnel *austin* to 6 times the current value of the keepalive timer interval (20) and verifies the change:

```
remote-endpoint/austin# keepalive-retries 6
remote-endpoint/austin# info
  address 192.168.2.4
  keepalive enabled
  logical-ip-address 0.0.0.1
  logical-ipx-address 000000000001
  name austin
  keepalive-retries 6
  keepalive-retry-timeout 20
  state enabled
```

Using Site Manager

To change the default value of the GRE Keepalive Retries parameter for a remote tunnel end point, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Select the remote tunnel end point for which you want to set the keepalive retries value from the list.	
6. Set the **Keepalive Retries** parameter. Click on **Help** or see the parameter descriptions beginning on page A-33.	
7. Click on **Apply.**	The GRE keepalive retries value is set for the selected tunnel end point.

Chapter 11
Configuring IP, ARP, RARP, RIP, and OSPF Services

Version 15.3.0.0

The following section is new to Chapter 1, “IP Concepts, Terminology, and Features,” in *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

RFC 826 Support

BayRS now supports RFC 826: An Ethernet Address Resolution Protocol. According to RFC 826, when a router interface receives an ARP request or reply, it checks the source IP address to make sure that it is valid and the router’s translation table for the destination IP and MAC address pair. If the saved MAC address in the table is different from the reported MAC address, the router replaces the old MAC address with the new one. The interface then checks for the message type (request or reply). If the router cannot find the MAC address in the translation table, it discards the message.

Version 15.4.0.0

The following sections are amendments to *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Defining BGP Peers for BGP, OSPF, and RIP Announce Policies

When defining a BGP peer for an announce policy, the peer must be identified by its BGP router ID. To verify the router ID of the BGP peer, on the peer router, check the configured value for the Site Manager BGP Global parameter, BGP Identifier, or the BCC BGP parameter, router-id. For information about supplying a router ID for a BGP router, see *Configuring IP Exterior Gateway Protocols (BGP and EGP)*.

Importing RIP Updates

You can now select whether the router imports RIP-1 updates only, RIP-2 updates only, or both RIP-1 and RIP-2 updates from a neighbor router. The following procedures describe how to configure this feature using the BCC and Site Manager.

Using the BCC

To have RIP-1 accept both RIP-1 broadcast and RIP-2 multicast packets (and have RIP-2 always use multicast for transmitting updates), go to the RIP interface prompt (for example, **box**; **eth 2/2**; **ip/10.1.1.2/255.255.0.0**; **rip**) and enter:

rip1-comp disable

For example, to disable rip1-comp, enter:

```
rip/10.1.1.2# rip1-comp disable
rip/10.1.1.2#
```

To have RIP-1 accept RIP-1 broadcast and RIP-2 broadcast packets only (RIP-1 will not accept RIP-2 multicast packets) and have RIP-2 broadcast the packets, making it compatible with RIP-1, go to the RIP interface prompt (for example, **box**; **eth 2/2**; **ip/10.1.1.2/255.255.0.0**; **rip**) and enter:

rip1-comp enable

For example, to enable rip1-comp, enter:

```
rip/10.1.1.2# rip1-comp enable
rip/10.1.1.2#
```

Using Site Manager

To have RIP-1 accept both RIP-1 broadcast and RIP-2 multicast packets (and have RIP-2 always use multicast for transmitting updates), or to have RIP-1 accept RIP-1 and RIP-2 broadcast packets only, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **RIP Interfaces**.	The IP RIP Interface Configuration window opens.
4. Click on the RIP interface that you want to edit.	The parameter values for that interface appear in the IP RIP Interface Configuration window.
5. Set the **Rip Compatible** parameter. Click on **Help** or see the parameter description on page A-65.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

MIB Object IDs

Please note the changes to the following MIB object IDs (OIDs):

Note: To get to the following parameters, use the path Configuration Manager > Protocols > IP > Interfaces or Configuration Manager > Protocols > IP > Global

Site Manager Parameter Name	Old OID	New OID
Subnet Mask	1.3.6.1.4.1.18.3.5.3.2.1.4.1.6	1.3.6.1.4.1.18.3.5.3.2.1.24.1.6
UnNumbered Assoc Addr	1.3.6.1.4.1.18.3.5.3.2.1.4.1.110	1.3.6.1.4.1.18.3.5.3.2.1.24.1.47
Mask	1.3.6.1.4.1.18.3.5.3.2.1.4.1.6	1.3.6.1.4.1.18.3.5.3.2.1.24.1.6
Broadcast Address	1.3.6.1.4.1.18.3.5.3.2.1.4.1.9	1.3.6.1.4.1.18.3.5.3.2.1.24.1.8
Cost	1.3.6.1.4.1.18.3.5.3.2.1.4.1.8	1.3.6.1.4.1.18.3.5.3.2.1.24.1.7
Host Cache	1.3.6.1.4.1.18.3.5.3.2.1.24.1.18	1.3.6.1.4.1.18.3.5.3.2.1.24.1.17
TR End Station	1.3.6.1.4.1.18.3.5.3.2.1.4.1.64	1.3.6.1.4.1.18.3.5.3.2.1.24.1.19
TR End Station ARP Type	1.3.6.1.4.1.18.3.5.3.2.1.4.1.127	1.3.6.1.4.1.18.3.5.3.2.1.24.1.56
Redirect	1.3.6.1.4.1.18.3.5.3.2.1.4.1.70	1.3.6.1.4.1.18.3.5.3.2.1.24.1.25
Ethernet Arp Encaps	1.3.6.1.4.1.18.3.5.3.2.1.4.1.71	1.3.6.1.4.1.18.3.5.3.2.1.24.1.26
SMDS Group Address	1.3.6.1.4.1.18.3.5.3.2.1.4.1.65	1.3.6.1.4.1.18.3.5.3.2.1.24.1.20
SMDS Arp Request Address	1.3.6.1.4.1.18.3.5.3.2.1.4.1.66	1.3.6.1.4.1.18.3.5.3.2.1.24.1.21
WAN Broadcast (was FRB Broadcast)	1.3.6.1.4.1.18.3.5.3.2.1.4.1.67	1.3.6.1.4.1.18.3.5.3.2.1.24.1.22
WAN Multicast #1 (was FRM Cast 1 DLCI)	1.3.6.1.4.1.18.3.5.3.2.1.4.1.68	1.3.6.1.4.1.18.3.5.3.2.1.24.1.23
WAN Multicast #2 (was FRM Cast 2 DLCI)	1.3.6.1.4.1.18.3.5.3.2.1.4.1.69	1.3.6.1.4.1.18.3.5.3.2.1.24.1.24

Site Manager Parameter Name	Old OID	New OID
Slot Mask	1.3.6.1.4.1.18.3.5.3.2.1.4.1.75	1.3.6.1.4.1.18.3.5.3.2.1.24.1.27
Max Forwarding Table Size (was Forward Cache Size)	1.3.6.1.4.1.18.3.5.3.2.1.4.1.104	1.3.6.1.4.1.18.3.5.3.2.1.24.1.46
Unnumbered Associated Alternate	1.3.6.1.4.1.18.3.5.3.2.1.4.1.111	1.3.6.1.4.1.18.3.5.3.2.1.24.1.47
IP OSPF Maximum Path	1.3.6.1.4.1.18.3.5.3.2.3.1.18	1.3.6.1.4.1.18.3.5.3.2.1.1.21

Version 15.5.0.0

The following section, Enabling and Disabling Unique Identifiers for ICMP Echo Requests, is an addition to Chapter 3, "Configuring and Customizing IP," in *Configuring IP, ARP, RARP, RIP, and OSPF Services*:

The section RFC 3101 Forwarding Address Compatibility for OSPF NSSA, on page 11-7, is an addition to Chapter 6, "Configuring and Customizing OSPF," in *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Enabling and Disabling Unique Identifiers for ICMP Echo Requests

Beginning with BayRS Version 15.5.0.0, you can send an ICMP echo request with a unique identifier. Utilizing this enhancement can help with problems pinging from a BayRS router to another network point through third-party Network Address Translation (NAT) routers that require a unique identifier for each ICMP echo request message.

A new global IP MIB, wfIpBaseIcmpEchoUniIdEnable, enables and disables this feature. When this feature is enabled, a unique identifier is added to each ICMP echo request message.

This enhancement to ICMP echo requests is disabled by default. You can use the BCC or Site Manager to enable and disable this feature as required.

Using the BCC

To enable or disable unique identifiers for ICMP echo requests, go to the global IP prompt (for example, **box; ip**) and enter:

icmp-echo-request-unique-id *<state>*

state is one of the following:

disable (default)
enable

For example, the following command enables unique identifiers for ICMP echo requests:

```
ip# icmp-echo-request-unique-id enable
ip#
```

Using Site Manager

To enable or disable unique identifiers for ICMP echo requests, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	
3. Choose **Global**.	The Edit IP Global Parameters window opens.
4. Set the **Icmp Echo Request Unique Id** parameter. Click on **Help** or see the parameter description on page A-47.	
5. Click on **OK**.	You return to the Configuration Manager window.

RFC 3101 Forwarding Address Compatibility for OSPF NSSA

Beginning with BayRS Version 15.5.0.0, you can configure the autonomous system external (ASE) forwarding address of the type 7 not-so-stubby-area (NSSA) link state database (LSDB) to any valid IP address on the network. The reason for this improvement is that in BayRS Version 15.5.0.0, the Open Shortest Path First (OSPF) NSSA is enhanced to comply with section 2.5, "Calculating Type-7 AS External Routes," and some parts of Appendix F, "Differences from RFC 1587," of RFC 3101. Full implementation of RFC 3101 is planned for a future release.

Using the enhanced functionality in Version 15.5.0.0, a network administrator now has the option to import summary route advertisements into the NSSAs. If the option to import summary advertisements is not enabled, then the NSSA autonomous system (AS) boundary router (ASBR) generates a default summary route for the NSSA that enables inter-area routing from the NSSA to the other areas. In addition to this new option, an administrator now also can set the autonomous system external (ASE) forwarding address of the AS external routes that are generated in the NSSA.

In prior implementations of OSPF NSSA, which were based on RFC 1587, Nortel routers selected as the ASE forwarding address, the lowest IP address of the interfaces that were up at that time on the router. However, this implementation sometimes caused convergence problems when the interface with the lowest IP address went down and the next available interface IP address was used as the ASE forwarding address.

Using the Version 15.5.0.0 functionality, a network administrator now can specify the IP address to be used as the ASE forwarding address, thus enabling him or her to specify the IP address of an interface that is known to stay up all the time. To ensure maximum up time, it is recommended that you use the IP address of the circuitless IP interface on the router as the ASE forwarding address.

To use this functionality, you must configure two new parameters as described in the following sections:

- Enabling and Disabling RFC 3101 Forwarding Address Compatibility
- Configuring the Not-So-Stubby Area (NSSA) Forwarding Address

When you start OSPF on the router, RFC 3101 compatibility is disabled by default. When RFC 3101 compatibility is disabled, any configured ASE forwarding address is ignored.

Enabling and Disabling RFC 3101 Forwarding Address Compatibility

You can use the BCC or Site Manager to enable and disable RFC 3101 compatibility on the router.

Using the BCC

To enable or disable RFC 3101 compatibility on the router, go to the global OSPF prompt (for example, **box; ip; ospf**) and enter:

rfc3101-fwd-addr-compatibility *<state>*

state is one of the following:

disable (default)
enable

For example, the following command enables RFC 3101 compatibility on the router:

`ospf#` **rfc3101-fwd-addr-compatibility enable**
`ospf#`

Using Site Manager

To enable or disable RFC 3101 compatibility on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF/MOSPF menu opens.
4. Choose **Global**.	The Edit OSPF Global Parameters window opens.
5. Set the **Rfc 3101 Compatibility Enable** parameter. Click on **Help** or see the parameter description on page A-51.	The value you chose appears in the Rfc 3101 Compatibility Enable field.
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring the Not-So-Stubby Area (NSSA) Forwarding Address

Once you enable RFC 3101 compatibility on the router, you must specify the IP address to be used as the new ASE forwarding address for the NSSA. You can specify this address using the BCC or Site Manager.

➡ **Note:** To configure this parameter, you first must enable the origination of a type 7 default route by the AS boundary router.

Using the BCC

Before you can configure a not-so-stubby area (NSSA) forwarding address, you first must enable the **nssa-default-originate** parameter.

To configure a not-so-stubby area (NSSA) forwarding address, go to the area prompt (for example, **box; ip; ospf; area/0.0.0.3**) and enter:

nssa-route-fwd-addr *<value>*

value is any valid IP address in the network.

Using Site Manager

Before you can configure a not-so-stubby area (NSSA) forwarding address, you first must set the NSSA Originate Def Route parameter to Enable.

To configure a not-so-stubby area (NSSA) forwarding address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **OSPF/MOSPF**.	The OSPF/MOSPF menu opens.
4. Choose **Areas**.	The OSPF Areas window opens.
5. Click on the area that you want to edit.	The parameter values for that area appear in the OSPF Areas window.
6. Set the **NSSA Forward Address** parameter. Click on **Help** or see the parameter descriptions beginning on page A-51.	**Note:** To use this parameter, you first must set the **NSSA Originate Def Route** parameter to Enable.
7. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Chapter 12
Configuring IP Exterior Gateway Protocols (BGP and EGP)

Version 15.5.0.0

The following section is an update to Chapter 1, “Exterior Gateway Protocols (BGP and EGP),” in *Configuring IP Exterior Gateway Protocols (BGP and EGP)*.

BGP Implementation Notes

For BayRS Version 15.5.0.0, 128 MB of optional memory is available for the Passport 5430. The standard 64 MB of memory on the Passport 5430 is no longer adequate to run the full complement of Internet routes, which currently can be as many as 125,000 routes. Therefore, it is recommended that you upgrade to 128 MB of memory if you want to run full Internet routes on a Passport 5430. Because of this situation, the following update to the BGP Implementation Notes is necessary:

To configure BGP and download full Internet routes on the Passport 5430 Multiservice Access Switch, you must install the router with 128 MB of memory.

For additional information, refer to the “BGP Guidelines” section of the *Release Notes for BayRS Version 15.5.0.0*.

Chapter 13
Configuring IP Multicasting and Multimedia Services

Version 15.2.0.0

The following section is new to *Configuring IP Multicasting and Multimedia Services* (part number 308629-15.1 Rev 00).

Configuring a PIM Bootstrap Border Router

You can define a router as a PIM bootstrap border router (PBBR) by specifying at least one of its interfaces as a PIM bootstrap border interface (PBBI). A bootstrap border router prevents a bootstrap message that is received from one side of a border router from being passed to the other side of the router. The bootstrap border router allows you to create two or more PIM bootstrap domains in one PIM domain so that the rendezvous point (RP) information kept in the routers can be different.

To specify a PIM bootstrap router as a border router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Bootstrap Border** parameter. Click on **Help** or see the parameter description in "PIM Interface Parameter" on page A-57.	
6. Click on **OK**.	You return to the Configuration Manager window.

Version 15.6.0.0

This section provides instructions on how to configure IGMP Version 3 and PIM-SSM, as well as how to configure static RP routers for PIM-SM. This chapter includes the following topics:

Overview of IGMP Version 3 and PIM-SSM

BayRS Version 15.6 implements source-specific multicasting (SSM) with the introduction of PIM-SSM and IGMP Version 3. In the SSM model, IP traffic is forwarded to receivers from only those multicast sources which the receivers have explicitly joined. With source-specific multicasting, hosts behind BayRS routers can subscribe to multicast information from specific sources only.

IGMP is the Internet Engineering Task Force (IETF) standards track protocol used by hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which enables hosts to report interest in receiving packets from specific source addresses, or from "all but" specific source addresses.

PIM-SSM, the routing protocol that supports the implementation of SSM, is derived from PIM sparse mode (PIM-SM). PIM-SSM forwarding is based on a source-based shortest-path tree, unlike PIM-SM, which supports a shared tree rooted at the rendezvous point (RP). For complete information about PIM-SM and how BayRS implements it, see *Configuring IP Multicasting and Multimedia Services* (part number 308629-15.1 Rev 00).

IGMP Version 3 and PIM-SSM offer the following advantages:

- Customers can deploy one-to-many audio and video broadcast applications that make use of source-specific multicast technology for distributing multimedia content.
- PIM-SSM optimizes the use of network resources and reduces latency in transmitting multicast information.
- PIM-SSM reduces the complexity of the multicast routing infrastructure because it requires only a source-based forwarding tree instead of an RP-based shared-tree infrastructure.
- Access control is improved because a receiver that subscribes to a channel receives data from a specific source only.

How BayRS Implements SSM

BayRS implements PIM-SSM and IGMP Version 3 as follows:

- IGMP Version 3 is backward compatible with IGMP Versions 2 and 1; a BayRS router running IGMP Version 3 supports Version 1, Version 2, and Version 3 hosts in the network.
- IGMP Version 3 and Version 2 are implemented on a per-interface basis. Both versions can coexist on the same router.
- If multiple routers share the same LAN, all interfaces to that LAN must run the same version of IGMP if there are local IGMP group members.
- BayRS routers support networks with PIM-SM only, PIM-SSM only, and mixed PIM-SM/PIM-SSM environments.
- SSM is implemented only on addresses within the configured SSM address range. The default SSM address range is 232.0.0.0 through 232.255.255.255. You can configure other non-overlapping SSM ranges, for example, 232.0.0.0/8 and 233.1.0.0/16.

- With IGMP Version 3 enabled, a host can signal that it wants to receive traffic only from specific sources sending to the multicast group (INCLUDE mode), or that it wants to receive traffic from all sources sending to a group except for specific sources (EXCLUDE mode). BayRS supports INCLUDE mode but only supports EXCLUDE mode with an empty source list for query and report messages.

Note: For IGMP Version 3, new IGMP global and interface parameters were added and some existing parameters were changed or made obsolete. For this reason, all IGMP global and interface parameters are provided in Appendix A, "Site Manager Parameters, beginning on page A-35.

References

For complete information about IGMP Version 3, PIM-SSM, and PIM-SM, see the following documents:

- Internet Group Management Protocol, Version 3, RFC 3376, B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, 10/2002 (http://www.ietf.org/rfc/rfc3376.txt)
- An Overview of Source-Specific Multicast (SSM), RFC 3569, S. Bhattacharyya, Ed., 7/2003 (http://www.ietf.org/rfc/rfc3569.txt)
- Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification, RFC 2362, D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei, 6/1998 (http://www.ietf.org/rfc/rfc2362.txt)
- Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised), Internet Draft, Bill Fenner, Mark Handley, Hugh Holbrook, Isidor Kouvelas, 10/2004 (http://www.ietf.org/internet-drafts/draft-ietf-pim-sm-v2-new-11.txt)
- Source Specific Multicast for IP, Internet Draft, H. Holbrook, B. Cain, 9/2004 (http://www.ietf.org/internet-drafts/draft-ietf-ssm-arch-06.txt)

Starting IGMP Version 3 and PIM-SSM

This section explains how to start IGMP Version 3 and PIM-SSM on a router.

- If IGMP and PIM are not yet configured on the router, go to the next section, "Adding IGMP Version 3 and PIM-SSM to the Router" on page 13-5.
- If IGMP and PIM are already configured on the router and you want to support IGMP Version 3 and PIM-SSM, go to "Editing IGMP and PIM Parameters for PIM-SSM" on page 13-7.

Note: Every router interface on the same network should be configured with the same version of IGMP.

Adding IGMP Version 3 and PIM-SSM to the Router

This section describes how to create a basic PIM-SSM and IGMP Version 3 configuration by specifying values for required parameters only and accepting default values for all other parameters.

IGMP is required for all types of multicasting. IGMP Version 3 is required for PIM-SSM. If you want the router to receive and forward multicast packets (that is, packets with destination addresses from 224.0.1.0 through 239.255.255.255), IGMP must be running on the slot and circuit—even if the circuit is a point-to-point circuit that will not be involved in IGMP group queries and join messages.

Configuration Prerequisites

Before you can configure PIM-SSM on a router, you must configure the router as follows:

- Disable IGMP Relay on the router on which you want to configure PIM.

  PIM and IGMP Relay cannot be configured on the same router.

- Delete DVMRP and MOSPF from the interface on which you want to configure PIM.

  PIM, DVMRP, and MOSPF cannot be configured on the same interface.

- Configure a unicast protocol (RIP or OSPF) on the same interface on which you want to configure PIM. (Or you can configure the interface as a static unicast route.)

PIM requires a unicast protocol to propagate multicast traffic within the network. For information about configuring unicast protocols, see *Configuring IP, ARP, RARP, RIP, and OSPF Services.*

Configuring PIM-SSM and IGMP Version 3

To start PIM-SSM and IGMP Version 3 on the router:

1. **Configure a circuit on a slot and connector.**
2. **Configure an IP interface on the circuit.**
3. **Add PIM to the IP interface.**

For information and instructions on configuring a circuit on a slot and connector, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

After you successfully configure the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose the following protocols: • **IP** • **PIM**	When you select PIM, IGMP is automatically selected.
2. Click on **OK**.	The IP Configuration window opens.
3. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** For information about these parameters, click on **Help**.	
4. Click on **OK**.	The PIM Global Configuration window opens.
5. Set the **Source-Specific Multicast** parameter to **Enable**. Click on **Help** or see the parameter description on page A-53.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **OK**.	If this is the first IGMP interface on the router, the Initial IGMP Global Configuration window opens. Otherwise, you return to the Configuration Manager window.
7. In the Initial IGMP Global Configuration window, click on **OK** to accept the default values.	You return to the Configuration Manager window.

PIM-SSM and IGMP Version 3 are now running on the router with default values for all global and interface parameters. For information about customizing IGMP or PIM-SSM parameters, see "Customizing IGMP Version 3 and PIM-SSM" on page 13-9.

Editing IGMP and PIM Parameters for PIM-SSM

If IGMP Version 2 and PIM-SM are already configured on the router and you want to configure IGMP Version 3 and PIM-SSM, you need to edit IGMP and PIM parameters as follows:

- Configure the IGMP interface to support Version 3.
- Enable the source-specific multicast mode for PIM.
- Disable the PIM candidate BSR and RP configurations if you plan to run PIM-SSM only.

To edit IGMP parameters to support Version 3 and PIM-SSM, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Select the interface that you want to run PIM-SSM on.	The values for that interface are displayed in the window.
6. Set the **Net Version** parameter to **IGMPV3**.	
7. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

To edit PIM parameters to support IGMP Version 3 and PIM-SSM, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Global**.	The PIM Global Configuration window opens.
5. Set the **Source-Specific Multicast** parameter to **Enable**. Click on **Help** or see the parameter description on page A-53.	
6. If you plan to run PIM-SSM only, disable the following parameters: • **Candidate BSR** • **Candidate RP** If you plan to run both PIM-SM and PIM-SSM, do not delete the BSR and RP.	When you disable these parameters, all related BSR and RP parameters are grayed out.
7. Click on **OK**.	You return to the Configuration Manager window.

Customizing IGMP Version 3 and PIM-SSM

When you configure IGMP Version 3 and PIM-SSM on the router, the protocols are automatically enabled with default values for most parameters. You can customize IGMP and PIM-SSM as described in this section:

Note: This section describes how to customize parameters that are specific to IGMP Version 3 and PIM-SSM. For information about customizing other IGMP and PIM parameters, see *Configuring IP Multicasting and Multimedia Services* (part number 308629-15.1 Rev 00).

Disabling and Reenabling PIM-SSM

To disable and reenable PIM-SSM on the router, complete the following tasks:

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

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Source-Specific Multicast** parameter to **Disable**. Click on **Help** or see the parameter description on page A-53.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring Equal-Cost Multipath Support for PIM-SSM

To distribute PIM-SSM traffic to the same destination over multiple equal-cost paths in the IP routing table, enable equal-cost multipath (ECMP) support. ECMP enables PIM-SSM to choose different forwarding paths for different (source, group) pairs. These forwarding paths are multicast table manager (MTM) entries with different incoming or outgoing interfaces.

To enable ECMP support for PIM-SSM, perform these steps:

1. Set the Equal Cost Multipath parameter to Enable on the PIM Global Configuration window.
2. Choose an ECMP method by setting the Multiple Nexthop Calculation Method parameter on the Edit IP Global Parameters window.

You can select any method to enable ECMP support for PIM-SSM, but ECMP for PIM-SSM always uses the source-destination hash algorithm based on the source and destination address. (IP forwards all packets with a given source and destination address to the same next hop.)

If you select multicast-only distribution, ECMP is disabled for unicast forwarding, and the configured equal-cost paths are used for PIM-SSM forwarding only.

Note: The Multicast-Only setting for the IP global parameter Multiple Nexthop Calculation Method applies only to PIM-SSM, not to PIM-SM, DVMRP, or MOSPF.

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

To enable or disable equal-cost multipath support for PIM-SSM, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Global**.	The Edit IP Global Parameters window opens.
4. Set the **Multiple Nexthop Calculation Method** parameter to any value other than **None**. Click on **Help** or see the parameter descriptions beginning on page A-49.	
5. Click on **OK**.	You return to the Configuration Manager window.
6. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
7. Choose **IP**.	The IP menu opens.
8. Choose **PIM**.	The PIM menu opens.
9. Choose **Global**.	The PIM Global Configuration window opens.
10. Set the **Equal Cost Multipath** parameter to **Enable**. Click on **Help** or see the parameter description on page A-53.	
11. Click on **OK**.	You return to the Configuration Manager window.

Configuring PIM-SSM Address Ranges

When you enable PIM-SSM, the multicast group address range 232.0.0.0–232.255.255.255 is reserved for PIM-SSM. You can change the group address range or create more than one PIM-SSM range (multiple SSM ranges cannot overlap). You can configure any multicast address range as an SSM range.

To add or change multicast group address ranges for PIM-SSM, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Global**.	The IGMP Global Configuration window opens.
5. Set the **SSM Ranges** parameter. Click on **Help** or see the parameter description on page A-38.	
6. Click on **OK**.	You return to the Configuration Manager window.

Editing IGMP Interface Fine-tuning Parameters

IGMP interface fine-tuning parameters are set to default values that should work in most networks. These parameters set timers and counters as follows:

- Robustness Variable—Specifies a tuning value for the expected packet loss on the network. By default, this parameter is set to 2. You can configure a value from 1 through 8.
- Startup Query Interval—Specifies the number of seconds that can elapse between general queries sent by the router on this interface. By default, this parameter is set to 31 seconds. If you reset the Interface Query Rate parameter, you should reset the Startup Query Interval parameter to 1/4 the value of the Interface Query Rate parameter.
- Startup Query Count—Specifies the number of general queries sent by the router on this interface. By default, this parameter is set to 2. If you reset the Robustness Variable parameter, you should reset the Startup Query Count parameter to the same value as the Robustness Variable parameter.
- Last Member Query Interval—Specifies in tenths of one second the maximum response time inserted into group-specific queries and group-and-source-specific queries sent in response to a leave-group message. By default, this parameter is set to 10 tenths of one second. You can configure a value from 1 through 31,744. A reduced value results in reduced time to detect the loss of the last member of a group or source.
- Last Member Query Count—Specifies the number of group-specific queries sent by the router on this interface before the router assumes that there are no more local members. For IGMP Version 3, this parameter specifies the maximum number of group-and-source-specific queries sent before the router assumes that there are no listeners for a particular source. By default, this parameter is set to 2. If you reset the Robustness Variable parameter, you should reset the Last Member Query Count to the same value as the Robustness Variable parameter.

To edit one or more IGMP fine-tuning parameters, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Interfaces**.	The IGMP Interface Parameters window opens.
5. Select the interface that you want to edit.	The values for that interface are displayed in the window.
6. Edit one or more of the following parameters: • **Robustness Variable** • **Startup Query Interval** • **Startup Query Count** • **Last Member Query Interval** • **Last Member Query Count** Click on **Help** or see the parameter descriptions beginning on page A-43.	
7. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Configuring the PIM-SM/PIM-SSM Translation Table

The BayRS implementation of IGMP Version 3 and PIM-SSM can operate in environments with mixed PIM-SM and PIM-SSM domains. To eliminate the need to reconfigure hosts and routers running IGMP Version 2, the BayRS implementation of IGMP Version 3 and PIM-SSM supports a *translation table*.

The translation table maps IGMP Version 2 groups to IGMP Version 3 (group, source) pairs. For each source group, the table provides a static mapping of IGMP Version 2/PIM-SM (*,g) join/prune requests to IGMP Version 3/PIM-SSM (s,g) join/prune requests.

The translation table is configured on a PIM domain border router. Using the translation table, the PIM-SSM router can accept IGMP Version 2 join/leave packets from IGMP Version 2 hosts if an entry is created to associate a multicast group with one or more source addresses in the table.

Before you enable the translation table, your configuration must meet these criteria:

- PIM-SSM must already be enabled (see "Starting IGMP Version 3 and PIM-SSM" on page 13-5).
- Any source group that will be specified in the translation table must have an address in the SSM range.
- If the border router on which the translation table will be created has a directly attached IGMP Version 2 host, the connecting interface on the router must be configured as an IGMP Version 2 interface.

To enable the translation table, perform these steps on the PIM domain border router:

1. Create the translation table entries in the IGMP Translation Table window.
2. Enable PIM-SM/PIM-SSM translation by setting the Translation Enable parameter on the IGMP Global Configuration window.

Note: Create the translation table before you globally enable translation. Making changes to the table after you enable translation globally resets IGMP.

To create a PIM-SM/IGMP Version 2-PIM-SSM/IGMP Version 3 translation table and to enable or disable translation, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
4. Choose **Translation Table**.	The IP IGMP Translation Table window opens.
5. Click on **Add**.	The IGMP Translation Table window opens.
6. Set the **Group Address** parameter. Click on **Help** or see the parameter description on page A-45.	
7. Set the **Translation Source List** parameter. Click on **Help** or see the parameter description on page A-46.	
8. Click on **OK**.	You return to the IP IGMP Translation Table window.
9. Click on **OK**.	You return to the Configuration Manager window.
10. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
11. Choose **IP**.	The IP menu opens.
12. Choose **IGMP/IGMP Relay**.	The IGMP menu opens.
13. Choose **Global**.	The IGMP Global Configuration window opens.
14. Set the **Translation Enable** parameter to **Enable**. Click on **Help** or see the parameter description on page A-39.	
15. Click on **OK**.	You return to the Configuration Manager window.

Configuring Static RP Routers for PIM-SM

The revised draft of the PIM-SM specification stipulates that RFC-compliant implementations of PIM-SM must support a statically configured RP. BayRS now supports static RP routers, along with the dynamically configured RP routers—discovered using the bootstrap method—that were supported before Version 15.6. Static RPs and dynamically configured RPs can coexist in the same PIM domain.

You can designate one or more PIM routers as static RPs by mapping the IP address of the router interface to a multicast group address and prefix, and assigning a priority level. (The interface on which you configure static RP must have PIM-SM already configured on it.) A PIM router can serve as a static RP for more than one group, and a group can have more than one static RP.

To configure a router as a static RP, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.
4. Choose **Static RP**.	The IP Static RP List window opens.
5. Click on **Add**.	The PIM Static RP window opens.
6. Set the following parameters: • **RP Address** • **Group Address** • **Prefix Length** • **Priority** Click on **Help** or see the parameter descriptions beginning on page A-58.	
7. Click on **OK**.	You return to the IP Static RP List window.
8. Click on **Done**.	You return to the Configuration Manager window.

Chapter 14
Configuring PPP Services

Version 15.5.0.0

The following section is new to Chapter 3, “Customizing PPP Services,” in *Configuring PPP Services* (308639-14.00 Rev 00).

Multi-Class Extension to Multi-Link PPP

Beginning with Version 15.5.0.0, BayRS supports RFC 2686, “Multi-Class Extension to Multi-Link PPP.” This feature provides a Layer 2 fragmentation and interleaving solution for Point-to-Point Protocol (PPP) wide area networks (WANs) that ensures high voice quality for voice over IP (VoIP) packets transmitted with data packets over a WAN. When this feature is enabled, large data packets are fragmented into smaller packets and higher-priority voice packets are sent between (interleaved with) the data packet fragments.

Multiclass extension (MCE) to multilink PPP (MLPPP) is a QoS enhancement for bandwidth limited PPP connections (link speeds less than T1 speeds). Utilization of this feature minimizes the serialization delay and delay variance (jitter) of VoIP packets over low speed links by fragmenting large data packets and interleaving higher-priority voice packets with the data packet fragments.

Packets are prioritized based on PPP service classes that are defined in the MLPPP header. A mapping has been defined between the PPP service classes and DiffServ code points (DSCPs) in IP headers based on Nortel Networks Service Class (NNSC) definitions. The mapping of PPP classes to DSCP is shown in Table 14-1.

Table 14-1. Mapping of PPP Classes to DiffServ Code Points

PPP Class Number	Nortel Networks Service Class	DiffServ Code Point
5	Premium	EF, CS5
4	Critical, Network	CS7, CS6
3	Platinum	AF4x, CS4
2	Gold	AF3x, CS3
1	Silver, Bronze	AF2x, CS2, AF1x, CS1
0	Standard	DF, CS0

The implementation of this feature supports six service classes using round robin weighted queues with integrated queuing and scheduling. Only long sequence number format is supported. If compression is enabled on the link, fragmentation and interleaving happens after compression is complete.

For multiclass circuits, this feature can be configured to operate over a single line. However, if multiple lines are configured in the bundle, they all must have the same line speed.

This feature can fully interoperate with the DiffServ marking of internally generated router packets feature (see "DSCP Tagging for Router-Generated Packets" on page 6-5).

Although RFC 2686 provides the option of prefix elision, the Nortel Networks implementation on BayRS routers does not support it. This implementation also does not support DSQMS (Differentiated Services Queue Management System) on any interface on which this feature is enabled.

When utilizing this feature, it is recommended that you make sure that VoIP packets are marked with the EF DiffServ code point (for Premium service class). Voice packets that are marked with the EF DiffServ code point will never be fragmented.

Note: You must use Site Manager to configure the multilink multiclass PPP feature. There is no BCC support for this feature.

Enabling and Disabling Multilink Multiclass on Interfaces

You enable and disable multilink multiclass on interfaces by setting the Multilink MultiClass Enable parameter on the PPP Interface List window shown in Figure 14-1.

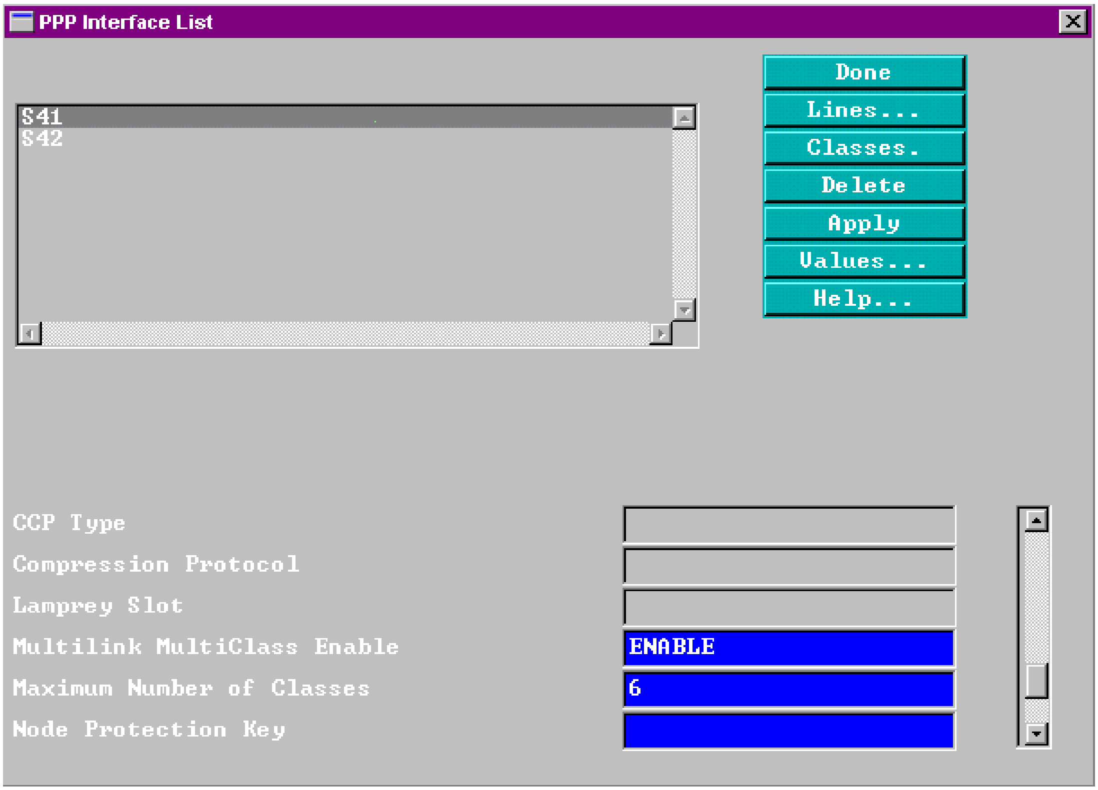

Figure 14-1. Site Manager PPP Interface List Window

To enable or disable multilink multiclass on interfaces using Site Manager, perform the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **PPP**.	
3. Choose **Interfaces.**	The PPP Interface List window opens.
4. Click on the interface for which you want to enable/disable multilink multiclass.	
5. Set the **Multilink MultiClass Enable** parameter. Click on **Help** or see the parameter description on A-59.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Specifying the Fragment Size for PPP Multilink Classes

You specify the minimum size of a packet that Multilink will fragment for each class of the interface by setting the Fragment Size parameter on the PPP Multiclass Classes window shown in Figure 14-2.

You can set the fragment size for each of the 6 classes (x.0 through x.5) for the selected interface, or you can use the default value (80). The six classes for the selected interface shown in Figure 14-2 are numbered 5.0 through 5.5. The fragment size is the minimum size of a packet to be fragmented for the selected class.

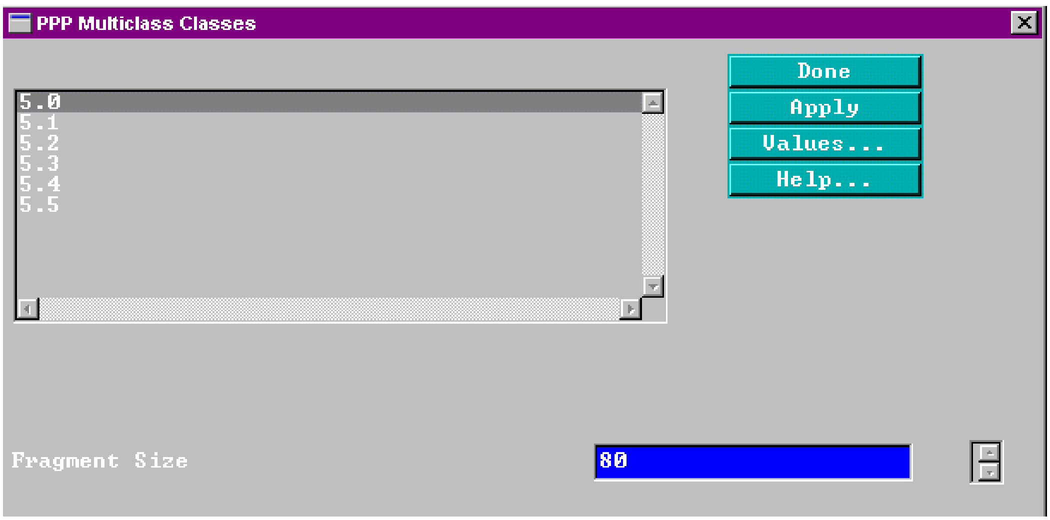

Figure 14-2. Site Manager PPP Multiclass Classes Window

To specify the fragment size for PPP multilink multiclass using Site Manager, perform the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **PPP**.	
3. Choose **Interfaces.**	The PPP Interface List window opens.
4. Click on the interface for which you want to set the fragment size.	
5. Click on **Classes**.	The PPP Multiclass Classes window opens (only if Multilink MultiClass is enabled for the selected interface).
6. Click on the class for which you want to set the fragment size.	
7. Set the **Fragment Size** parameter. Click on **Help** or see the parameter descriptions beginning on A-60.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the PPP Interface List window.
10. Repeat steps 5 through 9 for each class for which you want to set the fragment size.	
11. Click on **Done**.	You return to the PPP Interface List window.
12. Click on **Done**.	You return to the Configuration Manager window.

Enabling and Disabling Multilink Multiclass on Dial-up Lines

For dial-in connections, in addition to enabling the Multilink MultiClass Enable parameter on the PPP Interface List window (Figure 14-1 on page 14-3), you also must enable multilink multiclass on the dial-up line.

You enable and disable multilink multiclass on dial-up lines by setting the Multilink Multiclass for Dialup parameter on the PPP Line Lists window shown in Figure 14-3.

Note: Multilink multiclass for dial-up lines applies only to incoming calls.

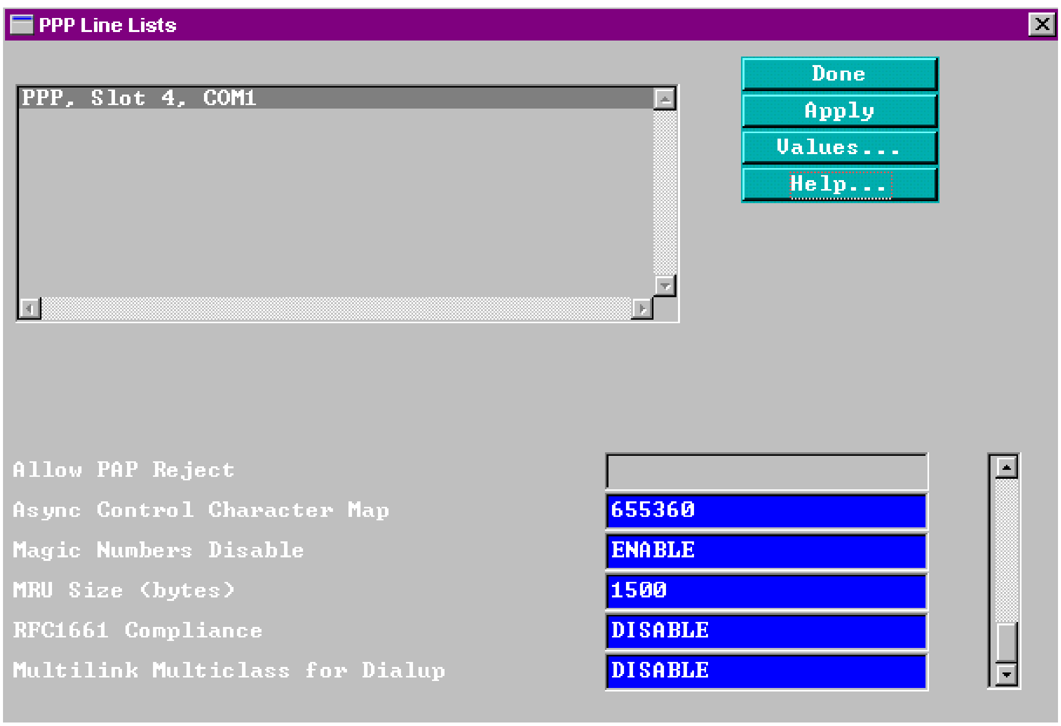

Figure 14-3. Site Manager PPP Line Lists Window

To enable or disable multilink multiclass on dial-up lines using Site Manager, perform the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **PPP**.	
3. Choose **Interfaces.**	The PPP Interface List window opens.
4. Click on the interface on which you want to enable/disable multilink multiclass.	
5. Click on **Lines**.	The PPP Line Lists window opens for the selected interface.
6. Click on the line on which you want to enable/disable multilink multiclass.	
7. Set the **Multilink Multiclass for Dialup** parameter. Click on **Help** or see the parameter description on A-61.	
8. Click on **Apply**.	
9. Repeat steps 6 through 8 for each line on which you want to enable/disable multilink multiclass.	
10. Click on **Done**.	You return to the PPP Interface List window.
11. Click on **Done** again.	You return to the Configuration Manager window.

Version 15.6.0.0

The following section supplements and amends information in Chapters 2 and 3 of *Configuring PPP Services* (308639-14.00 Rev 00).

PPP Link Quality Monitoring and Reporting for HSSI Interfaces

Before Version 15.6, BayRS supported PPP link quality monitoring (LQM) and link quality reporting (LQR) over standard synchronous interfaces only. With the release of Version 15.6, BayRS supports PPP LQM and LQR over High-Speed Serial Interfaces (HSSI) as well.

Note: The BayRS implementation of PPP LQM and LQR has not changed for this release. The only change is that you can now configure PPP link quality monitoring and reporting on HSSI lines.

For complete information about the BayRS implementation of PPP LQM and LQR, see *Configuring PPP Services*.

Using Site Manager

To configure PPP link quality monitoring and reporting on a HSSI interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **PPP**.	The PPP menu opens.
3. Choose **Interfaces.**	The PPP Interface List window opens.
4. Click on the HSSI interface for which you want to configure link quality monitoring and reporting.	The PPP interface values for the HSSI interface are displayed.
5. Click on **Lines.**	The PPP Line Lists window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Set the following parameters: • **Link Quality Protocol** • **Peer Link Quality Report Timer** • **LQR Reporting Period** • **Inbound Link Quality** • **Outbound Link Quality** Click on **Help** or see the parameter descriptions in Appendix A of *Configuring PPP Services*.	
7. Click on **Apply**.	
8. Click on **Done.**	You return to the PPP Interface List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Using the BCC

To configure PPP link quality monitoring and reporting on a HSSI interface:

1. Navigate to the HSSI interface where you will configure PPP link quality monitoring and reporting.

```
box# hssi/3/1
hssi/3/1#
```

2. Navigate to the PPP line parameters.

```
hssi/3/1# ppp
ppp/3/1# line
line/3/1#
```

3. Display the PPP line parameters. (The link quality monitoring and link quality reporting parameters are in **bold**.)

```
line/3/1# info
  allow-pap-project disabled
  async-control-character-map 655360
  chap-local-name {}
  chap-periodic-timer 0
  chap-secret {}
  echo-replies-lost 3
  echo-requests 0
  enable-pap-fallback disabled
```

```
    link-quality-protocol none
    local-authentication-protocol none
    local-pap-id {}
    local-pap-password {}
    lqr-percentage-received 90
    lqr-percentage-sent 90
    lqr-reporting-period 3
    magic-number enabled
    max-configure-fails 10
    max-configure-requests 10
    max-terminate-requests 2
    mru-size 1500
    peer-lqr-timer enabled
    remote-pap-id {}
    remote-pap-password {}
    restart-timer 3
    rfc1661-compliance disabled
    state enabled
  line/3/1#
```

4. Edit the PPP link quality monitoring and link quality reporting parameters as necessary.

   For complete information about PPP LQM and LQR parameters, see *Configuring PPP Services*.

Example

The following example configures PPP LQM on the HSSI interface as follows:

- Enables link quality monitoring
- Specifies that the remote peer should maintain the LQR timer (default value)
- Specifies an LQR reporting period of 5 seconds
- Sets the acceptable inbound success rate to 85 percent
- Sets the acceptable outbound success rate to 95 percent

```
hssi/3/1# ppp; line
line/3/1# link-quality-protocol linkqr
line/3/1# peer-lqr-timer enabled
line/3/1# lqr-reporting-period 5
line/3/1# lqr-percentage-received 85
line/3/1# lqr-percentage-sent 95
```

Chapter 15
Configuring RADIUS

Version 15.2.0.0

The following sections are amendments to *Configuring RADIUS*:

Configuring a RADIUS Client Using Site Manager

With earlier versions of Site Manager, you configured RADIUS only on link modules that had synchronous interfaces. With Version 15.2.0.0, you can use Site Manager to configure RADIUS on any link module, including Quad Ethernet, FDDI, and token ring. Consequently, Site Manager no longer automatically configures a demand circuit group when you use it to configure a RADIUS client.

To enable RADIUS on a router slot and configure the RADIUS client:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, select **Protocols > Global Protocols > RADIUS > Create RADIUS**.	The RADIUS Client Parameters window opens. The window lists the slots that already have RADIUS configured on them.
2. Click on **Add**.	For multislot routers, the RADIUS Slot Selection window opens. For single-slot routers, the RADIUS Client Parameters window opens. Go to step 4.
3. Enter the slot number on which you want to configure RADIUS and click on **OK**.	The RADIUS Client Parameters window opens.
4. Set the following parameters: • **Authentication** • **Accounting** • **Client IP Address** • **Debug Message Level** Click on **Help** or see the parameter descriptions beginning on page A-62.	
5. Click on **OK**.	You return to the RADIUS Client Parameters window.

Modifying Router Access Using the BCC or Site Manager

With RADIUS, you can modify access to the router using the user/manager lock and the login accounting feature.

User/Manager Lock

With earlier versions of BayRS, you enabled the user/manager lock using the Technician Interface only. You can now enable it using the BCC or Site Manager. The lock is disabled by default, allowing access by all users with the user or manager profile, and also by individual users with a unique profile. You enable the lock when both the RADIUS client and server are available. You disable the lock if the RADIUS server is not available, allowing the user to log in with the manager or user profile.

When you enable the user/manager lock and a RADIUS server is unavailable for authentication, the router automatically disables the user/manager lock. When the RADIUS server becomes available, the router automatically enables the user/manager lock.

Note: Be sure to configure RADIUS and assign the appropriate access to individuals with unique profiles before you enable the user/manager lock; otherwise you may lock out system managers from the router.

Using the BCC

To restrict access to individual users only, navigate to the access prompt (for example, **box; access**) and enter:

user-manager-lock enable

To allow access by all users with the manager or user profile, in addition to users with a unique profile, navigate to the access prompt (for example, **box; access**) and enter:

user-manager-lock disable

Using Site Manager

To restrict access to individual users only, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols > Global Protocols > RADIUS > Access Control**.	The RADIUS Access Control window opens.
2. Set the **User Manager Lock** parameter to **Enable**. For more information, click on **Help** or see the parameter descriptions beginning on page A-62.	
3. Click on **OK**.	You return to the Configuration Manager window.

Login Accounting

BayRS RADIUS accounting is now supported for console and Telnet router logins. The following sections, new to *Configuring RADIUS*, describe the functionality that was added to support this feature.

You determine whether a console or Telnet login session should allow RADIUS accounting messages to be sent to the RADIUS server by enabling or disabling RADIUS accounting access to the server.

Using the BCC

To allow RADIUS accounting messages to be sent to the RADIUS server, navigate to the access prompt (for example, **box; access**) and enter:

user-access-radius-account-enable enable

To prevent RADIUS accounting messages from being sent to the RADIUS server, navigate to the access prompt (for example, **box; access**) and enter:

user-access-radius-account-enable disable

Note: If you enable login accounting, and the RADIUS server becomes unavailable, the value for the **user-access-radius-account-enable** parameter is automatically set to "serverwait." When the RADIUS server becomes available again, the value reverts to enabled.

Using Site Manager

To allow RADIUS accounting messages to be sent to the RADIUS server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols > Global Protocols > RADIUS > Access Control**.	The RADIUS Access Control window opens.
2. Set the **Login Accounting** parameter to **Enable**. For more information, click on **Help** or see the parameter descriptions beginning in page A-62.	
3. Click on **OK**.	You return to the Configuration Manager window.

Using SecurID for RADIUS Authentication

The section "Using SecurID for RADIUS Authentication" on page 1-6 of *Configuring RADIUS* incorrectly states that Nortel Networks implements SecurID on ARN routers only. Nortel Networks implements SecurID on all router platforms that operate as RADIUS clients.

Chapter 16
Configuring Traffic Filters and Protocol Prioritization

Version 15.4.0.0

The following section is new to *Configuring Traffic Filters and Protocol Prioritization* (part number 308645-15.0 Rev 00).

Configuring IP Outbound Traffic Filters Using the BCC

Outbound traffic filters act on packets that the router forwards to a local area network (LAN) or (WAN) through a particular interface. Protocol prioritization allows the router to sort traffic into prioritized delivery queues (high, normal, low). These queues affect the sequence in which data leaves an interface. You can create outbound traffic filters for the following interfaces: ATM, Ethernet (10BASE-T or 100BASE-T), FDDI, token ring, HSSI, MCE1, MCT1, FT1/FE1, and synchronous.

The BayRS Version 15.4.0.0 implementation of this feature has the following limitations:

- Supports traffic with IP headers only
- Allows you to create traffic filters only; the ability to create templates is not available
- Does not allow you to change the order of precedence for outbound filters
- Is not supported on X.25 interfaces
- Is not supported on Data Link Switching (DLSw) interfaces

The following sections describe how to use the BCC to enable protocol prioritization and configure outbound traffic filters.

You implement protocol prioritization by applying an outbound traffic filter that includes a prioritizing (priority queue) action. This type of outbound traffic filter is called a *priority filter*. The next section describes how to edit protocol prioritization parameters that affect the way priority filters work.

Configuring Protocol Prioritization

To configure priority queues with default values, do the following:

1. **Configure protocol priority on the circuit, as described in this section.**
2. **Apply outbound traffic filters with prioritizing action to the circuit, as described in "Creating Outbound Traffic Filters," later in this chapter.**

To configure protocol priority, navigate to the interface prompt (for example, **box**; **ethernet/2/1**) and enter:

protocol-priority

For example, the following command configures protocol priority on connector 1 of an Ethernet module installed in slot 2:

```
ethernet/2/1# protocol-priority
protocol-priority/ethernet/2/1#
```

Displaying Protocol Priority Parameter Values

To view the current values of the protocol priority parameters, navigate to the protocol-priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

info

For example, the following command shows the current parameter values for protocol priority:

```
protocol-priority/ethernet/2/1# info
   dequeue-at-line-rate disabled
   high-queue-percentage-bandwidth 70
   high-queue-size 20
   high-water-packets-clear 0
   low-queue-percentage bandwidth 10
   low-queue-size 20
   max-high-queue-latency 250
   normal-queue-percentage-bandwidth 20
   normal-queue-size 20
   prioritization-algorithm-type bandwidth-allocation
   state enabled
protocol-priority/ethernet/2/1#
```

Customizing Protocol Prioritization

When you configure protocol prioritization on a circuit, the router uses default values that help determine how priority filters work. These defaults are designed to work well for most configurations. However, you can customize protocol prioritization to maximize its impact on your network.

For information about when you might want to customize protocol prioritization, see Chapter 2 in *Configuring Traffic Filters and Protocol Prioritization*.

To customize protocol prioritization parameters, use the following procedures:

Procedure	Page
Displaying Protocol Priority Parameter Values	16-2
Enabling or Disabling Protocol Priority	16-4
Specifying the High Queue Size	16-4
Specifying the Normal Queue Size	16-5
Specifying the Low Queue Size	16-5
Specifying the Maximum High Queue Latency	16-5
Clearing the High Water Marks	16-6
Selecting the Prioritization Algorithm Type	16-6
Selecting the High Queue Percentage Bandwidth	16-7
Selecting the Normal Queue Percentage Bandwidth	16-7

Enabling or Disabling Protocol Priority

When you configure protocol priority on a circuit, it is enabled by default. To disable protocol priority, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

state disabled

If you set this parameter to disabled, all outbound traffic filters will be disabled on this interface. Setting this parameter to disabled is useful if you want to temporarily disable all outbound traffic filters rather than delete them.

To re-enable protocol priority, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

state enabled

For example, the following command enables protocol priority on the selected circuit:

```
protocol-priority/ethernet/2/1# state enabled
protocol-priority/ethernet/2/1#
```

Specifying the High Queue Size

To specify the maximum number of packets in the High queue at any one time, regardless of packet size, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

high-queue-size <*value*>

value is any integer value; the default is 20.

For example, the following command changes the high queue size to 50:

```
protocol-priority/ethernet/2/1# high-queue-size 50
protocol-priority/ethernet/2/1#
```

Specifying the Normal Queue Size

To specify the maximum number of packets in the Normal queue at any one time, regardless of packet size, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

normal-queue-size <*value*>

value is any integer value; the default is 20 (200 for frame relay).

For example, the following command changes the normal queue size to 50:

```
protocol-priority/ethernet/2/1# normal-queue-size 50
protocol-priority/ethernet/2/1#
```

Specifying the Low Queue Size

To specify the maximum number of packets in the Low queue at any one time, regardless of packet size, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

low-queue-size <*value*>

value is any integer value; the default is 20.

For example, the following command changes the low queue size to 50:

```
protocol-priority/ethernet/2/1# low-queue-size 50
protocol-priority/ethernet/2/1#
```

Specifying the Maximum High Queue Latency

To specify the greatest delay that a high-priority packet can experience and, consequently, how many normal-priority or low-priority bits can be in the transmit queue at any one time, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

max-high-queue-latency <*value*>

value is between 100 to 5000 ms, inclusive. The default is 250 ms. Nortel Networks recommends accepting the default value of 250 ms.

For example, the following command changes the maximum high queue latency to 500:

```
protocol-priority/ethernet/2/1# max-high-queue-latency 500
```

```
protocol-priority/ethernet/2/1#
```

Clearing the High Water Marks

When you change the queue depth (by changing the value of the high queue, normal queue, or low queue size), you can also reset the high-water mark by changing the value of this parameter. When you change the value of this parameter, you reset the high-water mark for all three queues to zero.

To clear the existing high-water marks, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

high-water-packets-clear <*value*>

value is any integer value; the default is 0.

For example, the following command clears the existing high-water marks for the priority queues:

```
protocol-priority/ethernet/2/1# high-water-packets-clear 1
protocol-priority/ethernet/2/1#
```

Selecting the Prioritization Algorithm Type

To select the dequeuing algorithm that protocol prioritization uses to drain priority queues and transmit traffic, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

prioritization-algorithm-type {**bandwidth-allocation | strict**}

If you select strict queueing, the router always transmits traffic in the High queue before transmitting traffic in the other queues. If you accept the default, bandwidth allocation queueing, the router transmits traffic in a queue until the utilization percentage for that queue is reached; then, the router transmits traffic in the next-lower-priority queue. (You configure the percentages for bandwidth allocation by setting the high-queue, normal-queue, and low-queue percentage bandwidth parameters).

For example, the following command changes the dequeuing algorithm to strict:

```
protocol-priority/ethernet/2/1# prioritization-algorithm-type strict
protocol-priority/ethernet/2/1#
```

Selecting the High Queue Percentage Bandwidth

If you selected the bandwidth allocation dequeuing algorithm, to specify the percentage of the synchronous line's bandwidth allocated to traffic that has been sent to the High queue, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

high-queue-percentage-bandwidth <*percent*>

percent is a value between 0 to 100, inclusive. The default is 70 percent. When you set this parameter to a value less than 100, each time the percentage of bandwidth used by high-priority traffic reaches this limit, the router transmits traffic in the Normal and Low queues, up to the configured percentages for those priority queues. The high queue, normal queue, and low queue percentage bandwidth values must total 100.

For example, the following command changes the high queue percentage bandwidth to 50 percent:

```
protocol-priority/ethernet/2/1# high-queue-percentage-bandwidth 50
protocol-priority/ethernet/2/1#
```

Selecting the Normal Queue Percentage Bandwidth

If you selected the bandwidth allocation dequeuing algorithm, to specify the percentage of the synchronous line's bandwidth allocated to normal-priority traffic, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

normal-queue-percentage-bandwidth <*percent*>

percent is a value between 0 to 100, inclusive. The default is 20 percent. The high queue, normal queue, and low queue percentage bandwidth values must total 100.

For example, the following command changes the normal queue percentage bandwidth to 30 percent:

```
protocol-priority/ethernet/2/1# normal-queue-percentage-bandwidth
30
protocol-priority/ethernet/2/1#
```

Selecting the Low Queue Percentage Bandwidth

If you selected the bandwidth allocation dequeuing algorithm, to specify the percentage of the synchronous line's bandwidth allocated to low-priority traffic, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

low-queue-percentage-bandwidth <*percent*>

percent is a value between 0 to 100, inclusive. The default is 10 percent. The high queue, normal queue, and low queue percentage bandwidth values must total 100.

For example, the following command changes the low queue percentage bandwidth to 20 percent:

```
protocol-priority/ethernet/2/1# low-queue-percentage-bandwidth 20
protocol-priority/ethernet/2/1#
```

Controlling the Dequeuing of Packets

To control the dequeuing of packets from the queues to the driver, navigate to the protocol priority prompt (for example, **box**; **ethernet/2/1**; **protocol-priority**) and enter:

dequeue-at-line-rate {**disabled | enabled**}

When limited bandwidth is available, select enabled to reduce delay in queues that need a constant delay rate, such as Voice over IP. Accept the default, disabled, if you do not need constant bandwidth for traffic that requires a constant delay rate.

For example, the following command enabled the dequeue-at-line-rate feature:

```
protocol-priority/ethernet/2/1# dequeue-at-line-rate enabled
protocol-priority/ethernet/2/1#
```

Creating Outbound Traffic Filters

You can create outbound traffic filters for the following interfaces: Ethernet (10Base-T or 100BASE-T), FDDI, token ring, HSSI, MCE1, MCT1, and synchronous. The current implementation of this feature supports only traffic with IP headers. The following section describes how to create an IP-routed outbound traffic filter for an interface.

To create outbound traffic filters, use the following procedures:

Creating a Filter for IP-Routed Packets

To create an outbound traffic filter for IP-routed packets, navigate to the protocol priority prompt (for example, **box**; **serial/3/1**; **protocol-priority**) and enter:

ip-outbound-filter <*filter_name*>

filter_name is a descriptive name for the filter. For example, use the name *drop_telnet_s31* for a filter that drops outbound Telnet traffic on a serial module in slot 3, connector 1.

For example, the following command creates an outbound filter with the name drop_telnet_s31:

```
protocol-priority/serial/3/1# ip-outbound-filter drop_telnet_s31
ip-outbound-filter/drop_telnet_s31/S31#
```

Displaying Priority Outbound Filter Parameter Values

To view the current values of the outbound filter, navigate to the traffic filter prompt (for example, **box**; **serial/3/1**; **protocol-priority; ip-outbound-filter** <*filter_name*>) and enter:

info

For example, the following command shows the current parameter values for the priority outbound filter:

```
ip-outbound-filter/drop_telnet_s31/S31# info
    filter-name drop_telnet_s31
    state enabled
ip-outbound-filter/drop_telnet_s31/S31#
```

Enabling or Disabling the Outbound Filter

When you create an outbound filter on a circuit, it is enabled by default. To disable the filter, navigate to the traffic filter prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>) and enter:

state disabled

If you set this parameter to disabled, the specified outbound traffic filter will be disabled on this interface. Setting this parameter to disabled is useful if you want to temporarily disable the outbound traffic filter rather than delete it.

To re-enable the outbound filter, navigate to the traffic filter prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>) and enter:

state enabled

For example, the following command enables the outbound filter on the selected circuit:

```
ip-outbound-filter/drop_telnet_s31/S31# state enabled
ip-outbound-filter/drop_telnet_s31/S31#
```

Specifying Match Criteria for IP-to-IP Outbound Traffic Filters

The match criteria in a filter specify which fields in the IP header of each packet must contain the values that you specify. You can also specify certain fields in the headers of TCP and UDP packets contained in the IP data field of IP packets.

To prepare to specify the filtering criteria, navigate to the traffic filter prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>) and enter:

match-ip-ip

You can specify match criteria for filters as described in the following sections:

Topic	Page
Source and destination network	16-11
Source and destination TCP and UDP port	16-12
Protocol type	16-15
Type of service	16-16
Established TCP ports	16-16
User-defined criteria	16-24

Specifying Source and Destination Networks As Match Criteria

To filter on source and destination networks, go to the match-ip-ip prompt (for example, (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**) and do the following for each source and destination network that you want to filter on:

1. **Enter the following command:**

   {**source** | **destination**}**-network** *<address_range>*

   <address_range> specifies a range of IP addresses for source and destination networks.

   The source network or destination network prompt appears.

2. **Go back to the match-ip-ip prompt:**

   back

Example

```
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31# source-network
10.1.0.0-10.1.255.255
source-network/ip-outbound-filter/drop_telnet_s31/S31/
10.1.0.0-10.1.255.255# back
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#
destination-network 10.2.0.0-10.2.255.255
destination-network/ip-outbound-filter/drop_telnet_s31/S31/
10.2.0.0-10.2.255.255# back
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#
```

Specifying Source and Destination TCP and UDP Ports As Match Criteria

To filter on TCP ports, UDP ports, or both, you can specify only one of the following criteria for each filter:

- Source TCP ports, destination TCP ports, or both
- Source UDP ports, destination UDP ports, or both
- Both destination TCP and UDP ports
- Both source TCP and UDP ports

After you specify one of these options, the BCC prevents you from specifying another in the same filter. For example, if you specify source TCP ports, you can also specify destination TCP ports, but you cannot specify source UDP ports.

When you specify one of these values, the BCC automatically assigns the associated protocol ID (6 for TCP or 17 for UDP) to the protocol parameter. Therefore, you cannot modify the protocol parameter of a filter that specifies a TCP or UDP port value.

To filter on TCP or UDP ports, navigate to the match-ip-ip prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**) and enter the following command:

<*parameter*> {<*range_of_ports*>}

parameter is one of the following (Table 16-1):

Table 16-1. TCP and UDP Match Criteria Parameters

Parameter	Specifies
pri-ip-ip-src-tcp-ports	Source TCP port through which traffic is exiting the network
pri-ip-ip-dest-tcp-ports	Destination TCP port through which traffic is entering the network
pri-ip-ip-src-udp-ports	Source UDP port through which traffic is exiting the network
pri-ip-ip-dest-udp-ports	Destination UDP port through which traffic is entering the network

(continued)

Table 16-1. TCP and UDP Match Criteria Parameters *(continued)*

Parameter	Specifies
pri-ip-ip-dest-tcp-udp-ports	Both destination TCP and UDP ports through which traffic is entering the network
pri-ip-ip-src-tcp-udp-ports	Both source TCP and UDP ports through which traffic is exiting the network

range_of_ports is a space-delimited list.

Table 16-2 lists some common TCP port values.

Table 16-2. Common TCP Ports

Description	TCP Port
FTP	20, 21
Telnet	23
SMTP	25
DNS	53
Gopher	70
World Wide Web http	80-84
DLSw read port	2065
DLSw write port	2067

Table 16-3 lists some common UDP port values.

Table 16-3. Common UDP Ports

Description	UDP Port
DNS	53
TFTP	69
SNMP	161
SNMPTRAP	162

Example - Source TCP Port

This example specifies source TCP ports 20, 80, and 53 through 56 as match criteria for the filter template telnet-in:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-src-tcp-ports {20 80 53-56}
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Example - Destination TCP Port

This example specifies destination TCP ports 30, 90, and 50 through 53 as match criteria:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-dest-tcp-ports {30 90 50-53}
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Example - Source UDP Port

This example specifies source UDP port 162 as match criteria:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-src-udp-ports 162
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Example - Destination UDP Port

This example specifies destination UDP port 69 as match criteria:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-dest-udp-ports 69
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Example - Destination TCP and UDP Ports

This example specifies both destination TCP and UDP ports 53 as match criteria:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-dest-tcp-udp-ports 53
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Example - Source TCP and UDP Ports

This example specifies both source TCP and UDP ports 53 as match criteria:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-src-tcp-udp-ports 53
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Specifying Protocol Identifiers As Match Criteria

Internet Protocol Version 4 (IPv4) specifies an 8-bit protocol field to identify the next-level protocol. You can use the protocol field to identify traffic that you want to accept or drop.

Note: If you filter on a TCP or UDP source or destination, the software automatically changes the value to the protocol number associated with TCP or UDP.

If you specify a protocol other than TCP or UDP, the software prevents you from filtering on the TCP or UDP source or destination. Otherwise, the offset associated with one of the parameters in the non-UDP/TCP packet could coincidentally match the filter, and the software would perform the filter's action.

To filter traffic using the protocol field, navigate to the match-ip-ip prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**) and enter the following command:

pri-ip-ip-protocol {<*list_of_protocols*>}

list_of_protocols can include any number of protocol identifiers. It can also specify ranges of protocol identifiers.

Table 16-4 lists some common protocol ID codes for IP traffic.

Table 16-4. Common Protocol IDs for IP Traffic

Protocol	ID Code (Decimal)
ICMP (Internet Control Message Protocol)	1
IGMP (Internet Group Management Protocol)	2
TCP (Transmission Control Protocol)	6
EGP (Exterior Gateway Protocol)	8
IGP (Interior Gateway Protocol)	9
UDP (User Datagram Protocol)	17
RSVP (Resource Reservation Protocol)	46
GRE (Generic Routing Encapsulation)	47
NHRP (Next Hop Resolution Protocol)	54
OSPF (Open Shortest Path First)	89

Example

To match IGP packets, enter the following command:

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`
pri-ip-ip-protocol 9
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Specifying the Type of Service (ToS) As Match Criteria

You can discriminate higher priority traffic from lower priority traffic by specifying the type of service as the matching criteria for the traffic filter.

To specify the type of service portion of the IP header, enter the following command at the match-ip-ip prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**) and enter:

pri-ip-ip-tos {<*list_of_values*>}

list_of_values is a space-delimited list. It can be any number of values from 0 through 65,535. It can also specify ranges of values. Use a dash instead of a space to indicate a range.

Example

In this example, the router matches packets whose ToS bit is set to 1.

`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#` **pri-ip-ip-tos 1**
`match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#`

Specifying TCP-Established Match Criteria

By default, the router does not filter packets on the ACK and RESET bits in the TCP header. To allow the router to filter packets with the ACK and RESET bits, go to the match-ip-ip prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**) and enter the following command:

pri-ip-ip-tcp-established {**on** | **off**}

Example

In this example, the router filters packets with the ACK and RESET bits in the TCP header turned on.

```
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#
```
pri-ip-ip-tcp-established on
```
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#
```

Specifying Match Criteria for IP-to-Source Routing Outbound Traffic Filters

To prepare to specify the filtering criteria, navigate to the match-ip-ip prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **match-ip-ip**) and enter:

match-ip-source-routing

Specifying SSAPs as Match Criteria

To filter on a range of session service access points (SSAPs), navigate to the match-ip-source-routing prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip; match-ip-source-routing**) and enter the following command:

pri-ip-sr-ssap <*range*>

range specifies any number of session service access points (SSAPs). It can also specify ranges of SSAPs.

Specifying Source and Destination Networks As Match Criteria

To filter on source and destination networks, go to the match-ip-source-routing prompt (for example, (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**; **match-ip-source-routing**) and enter the following command for each source and destination network that you want to filter on:

{**pri-ip-sr-src** | **pri-ip-sr-dest**}**-addr** <*address_range*>

<*address_range*> specifies a range of addresses for source and destination networks.

Example

```
match-ip-source-routing/ip-outbound-filter/drop_telnet_s31/S31#
```
pri-ip-sr-src-addr 10.1.0.0-10.1.255.255
```
pri-ip-sr-src-addr/ip-outbound-filter/drop_telnet_s31/S31/
10.1.0.0-10.1.255.255#
```
back
```
match-ip-source-routing/ip-outbound-filter/drop_telnet_s31/S31#
```
pri-ip-sr-dest-addr 10.2.0.0-10.2.255.255
```
pri-ip-sr-dest-addr/ip-outbound-filter/drop_telnet_s31/S31/
10.2.0.0-10.2.255.255#
```
back
```
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31#
```

Specifying Match Criteria for IP-to-PPP Outbound Traffic Filters

To prepare to specify the filtering criteria, navigate to the match-ip-ip prompt (for example, **box**; **mct1 4/1**; **logical-line** <*MCT_line_no*>; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **match-ip-ip**) and enter:

match-ip-ppp

Specifying Protocol IDs as Match Criteria

To filter on a range of protocol IDs, navigate to the match-ip-ppp prompt (for example, **box**; **mct1 4/1**; **logical-line** <*MCT_line_no*>; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **match-ip-ip; match-ip-ppp**) and enter the following command:

pri-ip-ppp-protocol-id <*list_of_protocols*>

list_of_protocols can include any number of protocol identifiers. It can also specify ranges of protocol identifiers.

Specifying Match Criteria for IP-to-Frame Relay Outbound Traffic Filters

To prepare to specify the filtering criteria for IP-to-frame-relay outbound filters, navigate to the match-ip-ip prompt (for example, **box**; **mct1 4/1**; **logical-line** <*MCT_line_no*>; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **match-ip-ip**) and enter:

match-ip-frame-relay

Specifying DLCIs as Match Criteria

To filter on a range of DLCIs, navigate to the match-ip-frame-relay prompt (for example, **box**; **mct1 4/1**; **logical-line** <*MCT_line_no*>; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **match-ip-ip; match-ip-frame-relay**) and enter the following command:

pri-ip-fr-{**dlci2byte** | **dlci3byte** | **dlci4byte**} <*byte_range*>

byte_range specifies the PVC identification number (used by the frame relay network to direct data) or ranges of numbers on which you want to filter outbound traffic.

For the 2-byte DLCI address field, the valid values are 16 to 1007. Enter the decimal number that the frame relay provider assigns.

For the 3-byte DLCI address field, the valid values are 1024 to 64511. Enter the decimal number that the frame relay provider assigns.

For the 4-byte DLCI address field, the valid values are 131072 to 4194303. Enter the decimal number that the frame relay provider assigns.

Specifying NLPIDs as Match Criteria

To filter on a range of NLPIDs, navigate to the match-ip-frame-relay prompt (for example, **box**; **mct1 4/1**; **logical-line** <*MCT_line_no*>; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **match-ip-ip; match-ip-frame-relay**) and enter the following command:

pri-ip-fr-nlpid <*nlpid_range*>

nlpid_range specifies any number of network layer protocol identifiers (NLPIDs). It can also specify ranges of NLPIDs.

Specifying the Action of Outbound Traffic Filters

For outbound traffic filters, you can specify different types of action:

- Filtering Actions
- Prioritizing Actions
- Dial Service Actions

Filtering Actions

The filter action determines what happens to packets that match the filter criteria. You can configure IP outbound traffic filters to perform the following actions:

- Accept

  The router processes any packet that matches the filter criteria and ranges.

- Drop

  The router does not route any packet that matches the filter criteria and ranges.

- Log

  For every packet that matches the filter criteria, the router sends an entry to the system event log. You can specify the log action in combination with other actions.

Note: Specify the Log action to record abnormal events only; otherwise, the Events log will fill up with filtering messages, leaving no room for critical log messages.

To specify an action, navigate to the actions prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **actions**) and enter:

action {**accept** | **drop**}

For example, to change the action to drop, enter the following command:

```
actions/ip-outbound-filter/drop_telnet_s31/S31# action drop
actions/ip-outbound-filter/drop_telnet_s31/S31#
```

To log an entry to the system Events log for every packet that matches the filter criteria and ranges, navigate to the ip-outbound-filter prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>) and enter:

action-log on

For example, to log entries to the Events log, enter the following command:

```
actions/ip-outbound-filter/drop_telnet_s31/S31# action-log on
actions/ip-outbound-filter/drop_telnet_s31/S31#
```

The default value for this parameter is off.

Prioritizing Actions

You can apply the following actions to outbound traffic filters for WAN protocols:

- High

  Directs packets that match the filter criteria and ranges to the High queue

- Low

  Directs packets that match the filter criteria and ranges to the Low queue

- Length

  Uses the length of packets to determine the priority queue

Outbound traffic filters with a prioritizing action are called *priority filters.*

Note: You can apply prioritizing actions only to MCE1, MCT1, and synchronous interfaces. The BCC does not support priority filters on the LAN interfaces.

To direct packets that match the filter criteria and ranges to the High queue, navigate to the actions prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **actions**) and enter:

action high-queue

To direct packets that match the filter criteria and ranges to the Low queue, navigate to the actions prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **actions**) and enter:

action low-queue

To use the length of packets to determine the priority queue, navigate to the actions prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **actions**), and use the following procedure:

1. **Enter the following command:**

   action length

   The actions prompt is re-displayed (for example, `actions/ip-outbound-filter/test/S31#`)

2. **At the actions prompt, enter:**

   prioritization-length

   The prioritization-length prompt is displayed (for example, `prioritization-length/ip-outbound-filter/test/S31#`)

3. **Enter one of the following commands:**

   {**greater-than-queue** <*greater_than_queue_value*> |
   less-than-or equal-queue <*less_than_or_equal_queue_value*> |
   packet-length <*packet_length_value*>}

   greater_than_queue_value specifies which queue a packet is placed in if its packet length is greater than the value of the packet-length parameter. Valid values are high, low, or normal.

   less_than_or_equal_queue_value specifies which queue a packet is placed in if its packet length is less than or equal to the value of the packet-length parameter. Valid values are high, low, or normal.

   packet_length_value defines a packet length measurement to which each packet is compared. An action is imposed on every packet, depending on whether it is less than, equal to, or greater than the value you set for this parameter. This action depends on the values of the less-than-or-equal-queue and the greater-than-queue parameters. Enter a packet length value in bytes (0 through 4608). The default is 256.

Example

This example specifies that packets with lengths greater than 156 bytes are placed in the normal queue and that packets with lengths less than or equal to 156 bytes are placed in the high queue.

```
actions/ip-outbound-filter/drop_telnet_s31/S31# action length
actions/ip-outbound-filter/drop_telnet_s31/S31# prioritization-length
prioritization-length/ip-outbound-filter/drop_telnet_s31/S31#
greater-than-queue normal
prioritization-length/ip-outbound-filter/drop_telnet_s31/S31#
less-than-or-equal-queue high
prioritization-length/ip-outbound-filter/drop_telnet_s31/S31#
packet-length 156
```

Note: If you attempt to delete an IP traffic filter for which the action parameter is set to "length," the value for that parameter changes to "accept" and the IP traffic filter is not deleted.

Dial Service Actions

You can apply the following actions to outbound traffic filters for interfaces configured as dial-up lines:

- No Call

  Packets that match the filter criteria and ranges are dropped and do not initiate a dial connection. (By default, packets transmitted on dial-on-demand lines always trigger the router to establish a connection.)

- No Reset

  Packets that match the filter criteria and ranges are processed but do not reset the inactivity timer.

Note: Although No Call and No Reset are available when creating any outbound traffic filter, these actions are useful only on dial-up interfaces such as synchronous modem lines or MCT1 interfaces configured with ISDN PRI.

To enable the no-call feature, navigate to the actions prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **actions**) and enter:

no-call on

For example, to drop packets that match the filter criteria and ranges, enter the following command:

```
actions/ip-outbound-filter/drop_telnet_s31/S31# no-call on
actions/ip-outbound-filter/drop_telnet_s31/S31#
```

To enable the no-reset feature, navigate to the actions prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>; **actions**) and enter:

no-reset on

For example, to process packets that match the filter criteria and ranges but do not reset the inactivity timer, enter the following command:

```
actions/ip-outbound-filter/drop_telnet_s31/S31# no-reset on
actions/ip-outbound-filter/drop_telnet_s31/S31#
```

Specifying User-Defined Criteria

You can specify user-defined criteria in IP outbound traffic filters by specifying an offset and length based on the reference fields in the IP header.

To specify user-defined criteria, navigate to the match prompt (for example, **box**; **serial/3/1**; **protocol-priority**; **ip-outbound-filter** <*filter_name*>); **match-ip-ip**) and enter:

user-defined reference <*value*> **offset** <*value*> **bitwidth** <*value*> **range** <*value*>

reference is a known bit position in the packet header. Valid values are ip-wan-header-start, ip-wan-header-end, x25-mac-start, x25-snap-start, x25-nlpid-start, x25-nlpdu-start.

offset specifies the first position of the filtered bit pattern in relation to the reference point (measured in bits).

bitwidth specifies the total bit length that matches the packet criteria.

range specifies a minimum and maximum target value to apply to the match criterion. For a single value, you must specify the minimum value in hexadecimal format. You can precede the value with 0x.

Example

This example specifies user-defined criteria to create an IP traffic filter that drops every packet that has a value of 192 at offset 96 from the beginning of the IP header.

```
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31# user-defined
reference ip-wan-header-start offset 96  bitwidth 16 range 0192
user-defined/filter/drop_telnet_231/start-ip-header/96/16/0192#
back
match-ip-ip/ip-outbound-filter/drop_telnet_s31/S31# back
ip-outbound-filter/drop_telnet_231/S31# actions
actions/ip-outbound-filter/drop_telnet_s31/S31# action drop
```

Chapter 17
Configuring VRRP Services

Version 15.3.0.0

The following section is new to Chapter 3, "Customizing VRRP," in *Configuring VRRP Services*.

Enabling or Disabling VRRP Ping

When enabled, this feature allows you to ping a master virtual router that is not the owner of the virtual IP address. By default, VRRP ping is disabled.

Using the BCC

To enable VRRP ping, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

ping-enable enabled

To disable VRRP ping, access the virtual router and enter:

ping-enable disabled

For example, to enable VRRP ping, enter the following command:

```
vrrp/192.41.31.21/2# ping-enable enabled
vrrp/192.41.31.21/2#
```

Using Site Manager

To enable VRRP ping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **VRRP Address Ping** parameter. Click on **Help** or see the parameter description on page A-65.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Chapter 18
Configuring X.25 Services

Version 15.4.0.0

The following sections are new to *Configuring X.25 Services:*

The section "X.25 PAD" contains an amendment to Chapter 1 of *Configuring X.25 Services*.

Enabling the QLLC XID Retry Feature

Some OS/2 PCs configured with QLLC service for X.25 may take 20 to 50 seconds to become ready to respond to an XID3. Consequently, the PC ignores the first XID3 that it received and cannot establish a connection. QLLC can now retransmit the XID3 every 10 seconds to the QLLC endstation until it receives a response. You can enable or disable this feature using the XID Retry parameter on the QLLC Mapping Table Configuration window.

For information about accessing the parameters on the QLLC Mapping Table Configuration window, see *Configuring X.25 Services*. For more information about the XID Retry parameter, see page A-61.

Setting the LLC Connect Timer

Some IBM hosts may take several minutes to establish connections over QLLC service for X.25, thereby exceeding the hard-coded 25 second timeout interval for DLSw. You can now configure the DLSw timeout interval to values greater than 25 seconds (up to 600 seconds), using the Technician Interface.

Caution: The default value for wfDlsLLCConnectTime is 25 seconds. You should never change this value unless absolutely necessary. This value should not be changed unless there is a justifiable network requirement.

Accepting Incoming X.25 Calls for QLLC Service

BayRS now accepts incoming X.25 calls for QLLC service from devices that do not have an X.121 calling address. Only one X.25 connection can be supported at any given time. You can enable or disable this feature using the No Calling Address parameter on the X.25 Service Configuration window. For information about accessing the parameters on the X.25 Service Configuration window, see *Configuring X.25 Services*. For more information about the No Calling Address parameter, see see page A-66.

X.25 PAD

An X.25 packet assembler/disassembler (PAD) provides access to an X.25 network for devices, often character terminals, that are not capable of sending and receiving traffic across the X.25 interface. The PAD establishes and maintains the link with the packet-switched network, assembles and disassembles packets, communicates with the character terminal, and handles special control processes for the character terminal. Nortel Networks X.25 PAD services comply with the CCITT so-called Triple X Standards: Recommendations X.3, X.28, and X.29.

Nortel Networks X.25 PAD services work only with X.25 SVCs for the current software release, and only with the ARN router. Only one ISDB per ARN is supported.

For instructions on installing an X.25 PAD, see *Installing the X.25 PAD*. For instructions on using Site Manager to configure X.25 PAD Services, see Chapter 7 in *Configuring X.25 Services*.

Chapter 19
Quick-Starting Routers

Version 15.3.0.0

The following section contains an amendment to Chapter 10, “Installing Site Manager on a SPARCstation,” in *Quick-Starting Routers*.

SPARCstation System Requirements

To run Site Manager, your SPARCstation* must meet the following hardware and software requirements:

- Supported workstations:
  - SPARCstation 10, 20
  - UltraSPARC*
- Supported operating systems: Solaris* 2.7 and 2.8
- Window environment:
  - CDE 1.0.1
  - OpenWindows 3.5
- 32 MB of RAM (64 MB recommended)
- 145 MB of disk space
- 32 MB of swap space
- Network adapter appropriate for your network
- CD-ROM drive

The following section contains an amendment to Chapter 12, “Installing Site Manager on an HP 9000 Workstation,” in *Quick-Starting Routers*.

HP 9000 Workstation System Requirements

To run Site Manager, your HP 9000 workstation must meet the following hardware and software requirements:

- Supported workstations: HP 9000 Series 700 and 800
- Supported operating systems: HP-UX 10.20 (BayRS Version 15.3.0.0 up to, but not including 15.5.0.0) and HP-UX 11.00, including the complete services (network services) directory
- Window environment: CDE 1.0.1
- 32 MB of RAM
- 145 MB of free disk space
- 32 MB of swap space (64 MB recommended)
- Network adapter appropriate for your network
- CD-ROM drive

Chapter 20
Reference for BCC IP show Commands

Version 15.5.0.0

The following information supplements the information provided in Chapter 4, “GRE show Commands,” of the *Reference for BCC IP show Commands*.

Modified Output for the GRE Keepalive Mechanism

The output for the following BCC **show** commands was modified to support the GRE keepalive feature introduced in Version 15.5.0.0:

- **show gre logical-ip-tunnels**
- **show gre logical-ipx-tunnels**
- **show gre physical-tunnels**

For information about the modified output to these BCC **show** commands, see the following sections.

show gre logical-ip-tunnels

The **show gre logical-ip-tunnels** command displays information about the logical IP connections configured on a GRE tunnel. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tunnels only.
-enabled	Displays information about enabled tunnels only.
-address <*address*>	Displays information for tunnels configured with the specified IP address only.
-name <*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, it displays both the filter flag and value (that is, long notation).
<*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, it displays a value only (that is, short notation).

The output includes the following information:

Tunnel Name	Name assigned to the GRE tunnel.
Local Address	IP address of the host interface on the local end of the GRE tunnel connection.
Local State	State of the local host interface: enabled or disabled.
Remote Endpoint Name	Name assigned to the host interface on the remote end of the GRE tunnel connection.
Remote Endpoint Address	IP address assigned to the host interface on the remote end of the GRE tunnel connection.
Keepalive: Enabled?	If enabled, indicates that keepalives will be sent to the remote endpoint and keepalives received from that endpoint will be acted upon: enabled or disabled.
State	State of the GRE connection: up or down. The state of a connection is ‘up’ unless it is declared ‘down’ (as a result of keepalive failure) or the GRE connection is disabled.

Timer	Interval of time (in seconds) between transmission of successive keepalive packets to the remote endpoint.
Retries	Amount of time to wait before declaring a GRE connection ‘down’. ‘Retries’ is expressed as a multiple of the configured Timer value, where “Retries” is the number by which the Timer value is multiplied.

show gre logical-ipx-tunnels

The **show gre logical-ipx-tunnels** command displays information about the logical IPX connections configured on a GRE tunnel. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tunnels only.
-enabled	Displays information about enabled tunnels only.
-address <*address*>	Displays information for tunnels configured with the specified IP address only.
-name <*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, it displays both the filter flag and value (that is, long notation).
<*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, it displays a value only (that is, short notation).

The output includes the following information:

Tunnel Name	Name assigned to the GRE tunnel.
Local Network Address	Address of the host interface on the local end of the GRE tunnel connection.
Local State	State of the local host interface: enabled or disabled.
Remote Endpoint Name	Name assigned to the host interface on the remote end of the GRE tunnel connection.
Remote Endpoint Address	Name of the host on the remote end of the GRE tunnel connection.
Keepalive: Enabled?	If enabled, indicates that keepalives will be sent to the remote endpoint and keepalives received from that endpoint will be acted upon: enabled or disabled.

State	State of the GRE connection: up or down. The state of a connection is 'up' unless it is declared 'down' (as a result of keepalive failure) or the GRE connection is disabled.
Timer	Interval of time (in seconds) between transmission of successive keepalive packets to the remote endpoint.
Retries	Amount of time to wait before declaring a GRE connection 'down'. 'Retries' is expressed as a multiple of the configured Timer value, where "Retries" is the number by which the Timer value is multiplied.

show gre physical-tunnels

The **show gre physical-tunnels** command displays information about the router interfaces at either end of the physical GRE tunnel. This command allows for the following command filters and arguments:

-disabled	Displays information about disabled tunnels only.
-enabled	Displays information about enabled tunnels only.
-address <*address*>	Displays information for tunnels configured with the specified IP address only.
-name <*name*>	Displays information for tunnels configured with the specified name only. When you specify this filter, displays both the filter flag and value (that is, long notation).
<*name*>	Displays information for tunnels configured with the specified tunnel name only. When you specify this filter, displays a value only (that is, short notation).

The output includes the following information:

Tunnel Name	Name assigned to the GRE tunnel.
Local Address	IP address of the router interface on which the GRE tunnel is configured.
Local State	State of the router interface: enabled or disabled.
Remote Endpoint Name	Name assigned to the interface at the tunnel's remote end point.
Remote Endpoint Address	IP address of the interface at the tunnel's remote end point.
Encaps Protocols	Protocol for which the tunnel is configured.

Keepalive: Enabled?	If enabled, indicates that keepalives will be sent to the remote endpoint and keepalives received from that endpoint will be acted upon: enabled or disabled.
State	State of the GRE connection: up or down. The state of a connection is ‘up’ unless it is declared ‘down’ (as a result of keepalive failure) or the GRE connection is disabled.
Timer	Interval of time (in seconds) between transmission of successive keepalive packets to the remote endpoint.
Retries	Amount of time to wait before declaring a GRE connection ‘down’. ‘Retries’ is expressed as a multiple of the configured Timer value, where “Retries” is the number by which the Timer value is multiplied.

Chapter 21
Upgrading Routers to BayRS Version 15.*x*

Version 15.2.0.0

The following section describes changes to *Upgrading Routers to BayRS Version 15.x*.

Why You Upgrade Boot and Diagnostic PROMs

Table A-1 in "Why You Upgrade Boot and Diagnostic PROMs" of *Upgrading Routers to BayRS Version 15.x* has been modified to include the latest boot and diagnostic PROM file names and associated revision numbers for router platforms running BayRS Version 15.*x*.

Router Platform	Diagnostic PROM File Name	Diagnostic PROM Revision Number	Reason for Upgrading PROM	Boot PROM File Name	Boot PROM Revision Number
AN/ANH*	andiag.exe	7.36	Strata flash feature support	anboot.exe	9.00d
ARN	arndiag.exe	2.24	Strata flash feature support	arnboot.exe	1.27
	arndiag.rom	2.24	Not applicable	arnboot.rom	1.27
	e7srom.rom	2.16	E7S feature support	isdb.rom	1.06
	arn_pdbrom.rom	1.22	Not applicable		

Router Platform	Diagnostic PROM File Name	Diagnostic PROM Revision Number	Reason for Upgrading PROM	Boot PROM File Name	Boot PROM Revision Number
ASN*	asndiag.exe	2.36	Strata flash feature support	asnboot.exe	13.00
	asndiag.rom	2.36	Not applicable		
BN*	frediag.exe	5.16	Strata flash feature support	freboot.exe	13.00
	fre4diag.ppc	1.14	FRE-4 board support	fre4boot.ppc	13.20
ARE (BN, 5782 MPE)	arediag.ppc	1.22	Strata flash feature support	areboot.ppc	14.0.1.0
Passport 2430	pp2430diag.exe	2.06	Not applicable	pp2430boot.ppc	15.4.0.0
	pp2430ram.exe	2.06	Not applicable		
	pp2430diag.a	2.06	Not applicable		
Passport 5430	pp5430diag.exe	1.16	Not applicable	pp5430boot.ppc	15.4.2.0
	pp5430ram.exe	1.16	Not applicable		
	pp5430diag.a	1.16	DS3/E3 feature support and quad serial feature support		
System 5000* net modules	s5000diag.exe	0.04	Strata flash feature support	s5000boot.exe	13.00

Version 15.3.0.0

The following section describes changes to *Upgrading Routers to BayRS Version 15.x*.

Site Manager Upgrade Prerequisites

Before you upgrade to Site Manager Version 15.*x*, review Site Manager system requirements.

Reviewing Site Manager System Requirements

Site Manager is a graphical user interface (GUI) for router configuration and management over an IP network. To run Site Manager Version 15.*x*, your PC, IBM* workstation, SPARCstation*, or HP* 9000 must meet the hardware and software requirements listed in Table 21-1.

Table 21-1. Site Manager System Requirements

Platform	Hardware and Software Requirements
PC	• 486 PC (Pentium* recommended) • Microsoft* Windows* 98 or 2000 (32-bit) or Windows NT* Version 4.0 (32-bit) • 16 MB of RAM (minimum) • 90 MB of free disk space • Microsoft TCP/IP for Windows 98 or 2000 and compatible network adapter and driver • CD-ROM drive • VGA monitor (SuperVGA monitor recommended)
SPARCstation	• Supported workstations: SPARCstation 10, 20, and UltraSPARC • Supported operating system: Solaris 2.7 and 2.8 • Window environments: CDE 1.0.1 and OpenWindows 3.5 • 32 MB of RAM (64 MB recommended) • 145 MB of disk space • 32 MB of swap space • Network adapter appropriate for your network • CD-ROM drive

Table 21-1. Site Manager System Requirements *(continued)*

Platform	Hardware and Software Requirements
IBM workstation	• Supported workstations: RS/6000 340, 370, and PowerPC • Supported operating system: IBM AIX* Version 4.3 • Window environments: CDE 1.0.1 and AIX Motif* 1.2 • 32 MB of RAM (64 MB recommended) • 140 MB of disk space • 32 MB of swap space (64 MB recommended; use 96 MB of swap space with the NetView* for AIX application) • Network adapter appropriate for your network • CD-ROM drive
HP 9000	• Supported workstations: HP 9000 Series 700 and 800 • Supported operating system: HP-UX 10.20 (BayRS Version 15.3.0.0 up to, but not including, 15.5.0.0) and HP-UX 11.00, including the complete network services directory • Window environment: CDE 1.0.1 • 32 MB of RAM • 145 MB of free disk space • 32 MB of swap space (64 MB recommended) • Network adapter appropriate for your network • CD-ROM drive

Version 15.4.0.0

The following sections replace the existing sections in Chapter 4 and Chapter 5, respectively.

Upgrading and Verifying PROMs

When you upgrade PROMs, the system erases the existing PROM image and copies the contents of the newer PROM image file to the PROM. To verify the PROM, the system compares the contents of the new image file to the actual contents of the PROM. See Table A-1 on page A-2 of *Upgrading Routers to BayRS Version 15.x.* for Version 15.0 boot and diagnostic PROM file names and associated revision numbers for all router platforms.

Note: Before you upgrade any router software, make sure that you save a copy of the original configuration file and boot image as a safeguard in case you encounter problems after upgrading.

You use the **prom** command from the Technician Interface to upgrade and verify the software on the diagnostic or boot PROM. This command is restricted to the Manager access level.

To upgrade and verify PROMs on a router, begin at the Technician Interface prompt and complete the following steps:

1. **Establish a Technician Interface session with the router.**

   Enter the following command at the Technician Interface prompt:

   Manager

   For more information about how to open a Technician Interface session with the router, see *Using Technician Interface Software*.

2. **Insert a flash card with contiguous free space sufficient to accommodate the PROM images that you want to transfer to the router.**

   To determine the amount of contiguous free space, display the directory of the flash volume by entering the following command at the Technician Interface prompt:

   dir *<volume_no.>***:**

   volume_no. is the slot in which the flash card resides.

   If you need more contiguous free space for the PROM image:

   a. **Delete unnecessary or obsolete files.**

   b. **Compact the contents of the flash card by entering:**

      compact *<volume_no.>***:**

      The following message appears:

      ```
      Compacting file system on volume <vol>:...
      This may take several minutes...Please wait...
      100% Complete
      Compaction completed
      ```

      The space is compacted when the Technician Interface prompt reappears.

   c. **Verify that the amount of contiguous free space and available free space on the volume are the same by entering:**

      dir *<volume_no.>***:**

3. **Transfer the PROM image files (for example, freboot.exe and frediag.exe) from the Site Manager PC or workstation to the router's flash card by using the tftp command.**

   For more information about the **tftp** command, see *Using Technician Interface Software*.

4. **Update the boot PROM by entering:**

   prom -w *<volume_no.>*:*<Boot_PROM_source_file> <slot_ID>*

   volume_no. is the slot number of the boot PROM source file.

   Boot_PROM_source_file is the name of the boot PROM source file (for example, freboot.exe).

   slot_ID is the slot location of the boot PROM that you want to update.

   For AN, ANH, or ARN routers, the *slot_ID* is always 1.

> **Note:** To update the boot PROM on the Passport 2430 router, copy the latest pp2430boot.ppc file to the PCMCIA card along with the image. This router does not require that the boot code be burned in to the PROM.

   For example, enter the following command:

   prom -w 2:freboot.exe 3

   This command erases the boot PROM image on slot 3 and copies the contents of the freboot.exe file on volume 2 to the PROM on slot 3.

> **Note:** After you enter the **prom** command, it must run to completion. The [Control]-c (abort) command is disabled for the duration of the **prom** command execution. Updating takes from 2 through 10 minutes per PROM. Verifying takes up to 2 minutes per PROM.

5. **Update the diagnostic PROM by entering:**

   prom -w *<volume_no.>*:*<Diag_PROM_source_file> <slot_ID>*

   volume_no. is the slot number of the diagnostic PROM source file.

   Diag_PROM_source_file is the name of the diagnostic PROM source file (for example, frediag.exe).

slot_ID is the slot location of the diagnostic PROM that you want to update.

For AN, ANH, ARN, and Passport 2430 routers, the *slot_ID* is always 1.

For example, enter the following command:

prom -w 2:frediag.exe 3

This command erases the diagnostic PROM image on slot 3 and copies the contents of the frediag.exe file on volume 2 to the PROM on slot 3.

6. **Upgrade PROMs on multiple slots on your router.**

   If you need to update PROM images on multiple slots, use a dash to indicate a range of slots (2-5), or use commas or spaces to separate multiple slot locations (2, 3, 5 or 2 3 5).

   For example, enter the following command:

   prom -w 2:frediag.exe 2, 3, 5

   This command erases the diagnostic PROM images on slots 2, 3, and 5 and copies the contents of the frediag.exe file on volume 2 to the PROMs on slots 2, 3, and 5.

7. **Verify the PROM upgrade by entering the following command:**

   prom -v *<volume_no.>*:*<PROM_source_file> <slot_ID>*

   For example, for a boot PROM, enter:

   prom -v 1:arnboot.exe 1

   For a diagnostic PROM, enter:

   prom -v 1:arndiag.exe 1

   The system verifies that the PROM image on a designated flash volume (that is, the image file used as a source for upgrading the PROM) matches the image actually stored in the boot or diagnostic PROM on the designated slot.

   The console displays one of the following messages after the verification terminates:

   ```
   prom: slot <slot ID> completed successfully
   prom: PROM data does not match file data on slot <slot ID>
   ```

   If the operation succeeds, the new images stored in the boot and diagnostic PROMs run when you reboot the router.

   If the operation fails, the console displays a message describing the cause of the failure.

Task 2: Updating the Existing Configuration File

This section describes how to upgrade your existing configuration files to support the new Version 15.*x* features. Optionally, you can create a new Version 15.*x* configuration file to replace your existing configuration file for the router.

Booting the Existing Configuration File

To upgrade an existing configuration file to Version 15.*x*, boot it on a router running a Version 15.*x* router software image. The router software loads the existing configuration file into router memory and updates the configuration file's version stamp to match the Version 15.*x* router software. It does not, however, automatically save that version to the file on the flash card until you save the configuration file in dynamic mode. After you save the file in dynamic mode, reboot the router, using the updated configuration file.

Saving the Configuration File in Dynamic Mode

After you boot the router with a Version 15.*x* image and the existing configuration file, save the configuration file in dynamic mode to save it directly to the router.

To save the existing configuration file in dynamic mode:

1. **In the Site Manager window, choose Tools > Configuration Manager > Dynamic.**

   The Configuration Manager window opens (Figure 21-1), displaying the real-time router hardware and software configuration.

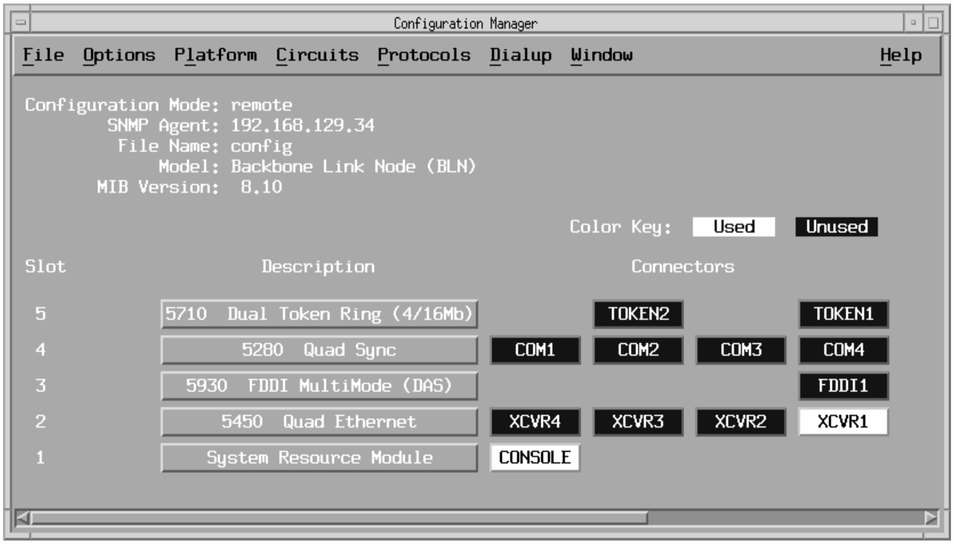

Figure 21-1. Configuration Manager Window

2. **Choose File > Save As.**

   The Save Configuration File window opens (Figure 21-2).

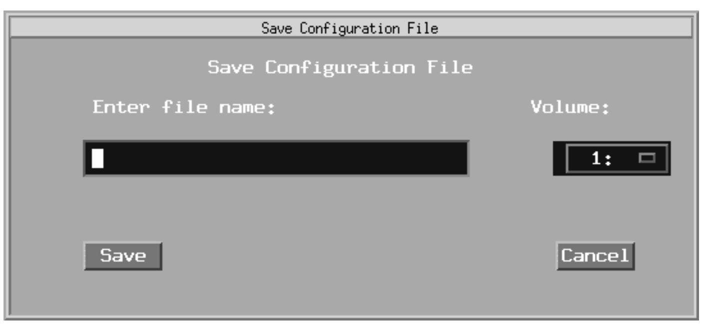

Figure 21-2. Save Configuration File Window

3. **Enter the configuration file name *config*.**
4. **Choose the correct volume by clicking in the Volume field.**

If the volume (slot location of the memory card on the router) is not the volume to which you want to save this file, choose another volume.

5. **Click on Save.**

   The File Saved window opens (Figure 21-3), asking you to confirm your decision to save the file.

Figure 21-3. File Saved Window

6. **Click on OK.**

   This action saves the configuration file (config) to the router's flash card with the Version 15.*x* version stamp.

7. **Reboot the router with the updated configuration file.**

Chapter 22
Using Technician Interface Scripts

Version 15.1.0.0

The Technician Interface is a command-line interface that Nortel Networks support technicians can use to troubleshoot and configure Nortel Networks devices.

The following section is an amendment to *Using Technician Interface Scripts*.

Using Scripts and Aliases to Dynamically Configure a Router

Use of rapid-fire scripts or aliases to dynamically set a router's configuration via the MIBs can put the router into a corrupted state and cause connectivity issues. When you use the Technician Interface to launch scripts or aliases to configure the router, be sure to include pauses (1 or 2 seconds) to allow sufficient time for the router to make the required changes to the MIBs.

Chapter 23
Using Technician Interface Software

Version 15.1.0.0

The Technician Interface is a command-line interface that Nortel Networks support technicians can use to troubleshoot and configure Nortel Networks devices.

The following sections are amendments to *Using Technician Interface Software*.

Diagnostics On/Off Option for ARN, Passport 2340, and Passport 5430

For ARN, Passport 2430, and Passport 5430 platforms *only*, the Technician Interface **diags** command supports an option to enable or disable diagnostics, effective the next time you cycle power on the router. Disabling the diagnostics results in a faster boot time, but leaves the hardware components unverified. The syntax for this option is as follows:

diags [**- on** | **off**] [<*slot_id*>]

Setting Default Route Cost Using the Technician Interface

When the routing table does not contain the route to a particular destination address, the router looks for a default route. As it does for any other route, the routing table either acquires the default route dynamically (through a routing protocol), or you can enter the default route statically.

You can use the Technician Interface to set the wfRipIntfDefaultRouteCost (RIP default route cost) MIB attribute. This attribute interacts with the Site Manager parameter Default Route Supply or the BCC parameter default-supply in one of two ways:

- If you select Enable for Default Route Supply or default-supply, RIP advertises the default route cost you set for wfRipIntfDefaultRouteCost attribute *plus* the default route learned from the network.
- If you select Generate for Default Route Supply or default-supply, RIP advertises the default route cost you set for wfRipIntfDefaultRouteCost.

For additional information, see "Supplying a Default Route on an Interface" in *Configuring IP, ARP, RARP, RIP and OSPF Services*.

With the Technician Interface, enter the following commands to set the wfRipIntfDefaultRouteCost (RIP default route cost) attribute:

set wfRipIntfDefaultRouteCost *<value>*

value is any integer from 0 through 15. The default value is 1.

commit

save config *<vol>: <filename>*

You must have Manager access to issue a **set** command. The **commit** command causes the changes you made to the configuration to take effect in active memory, but not in flash memory. The **save config** command saves changes to a configuration file (config) and flash volume on the router.

Version 15.4.0.0

The following section describes how to enable the daylight savings time feature for the router using the Technician Interface.

Setting Daylight Savings Time Using the Technician Interface

Daylight savings time is the time during which clocks are set one hour or more ahead of standard time to provide more daylight at the end of the working day during late spring, summer, and early fall. In the United States, we set the clock ahead one hour at 2:00 am on the first Sunday in April and set the clock back one hour at 2:00 am on the last Sunday in October.

When you enable the daylight savings time feature using the Technician Interface, the router's internal clock automatically sets itself one hour ahead at 2:00 am on the first Sunday in April and sets itself back one hour at 2:00 am on the last Sunday in October. Currently, only four time zones are supported: Eastern, Central, Mountain, and Pacific.

To enable the daylight savings time feature, enter the following command at the Technician Interface prompt:

set wfSys.wfSysDaylightSaving.0 1; commit

Removing the Technician Interface Login Banner

You can now replace or modify the login banner and prompt presented via a Telnet connection or on the router console. The method uses the placement of an optional text file on the router flash, named "oem.txt." If this file is present when the Technician Interface initializes for a potential login from console or via Telnet, its contents govern the nature of the login banner. This file can be used for explicit identification purposes (positive indication that the desired system has been reached), security concerns (a nonspecific banner to avoid aiding unauthorized accesses), or cosmetic reasons.

The rules are as follows:

- By default, in the absence of the file "oem.txt," the login banner and prompt appear as follows:

```
Nortel Networks, Inc. and its Licensors.
Copyright 1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,
2004,2005
All rights reserved.

Login:
```

- If the file "oem.txt" is present, its contents replace only the "Nortel Networks, Inc." portion of the banner:

```
Chicken Delight - We Deliver!! and its Licensors.
Copyright 1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,
2004,2005
All rights reserved.

Login:
```

- If the contents of “oem.txt” begin with the string "*NO BANNER*" (excluding quotes), the login banner is suppressed, but the prompt is retained:

  ```
  Login:
  ```

- If the "*NO BANNER*" string is followed by nonblank characters, they become the banner/prompt:

  ```
  Enter user name:
  ```

Note: While changes to the “oem.txt” file will be reflected when the next Telnet connection is established, the change to the console login banner/ prompt will not take effect until the next system reset.

Chapter 24
Using the Bay Command Console (BCC)

Version 15.6.0.0

The following sections contain additions to *Using the Bay Command Console (BCC)* (part number 308659-14.20 Rev 00).

Using the source Command to Configure a Router

This section is an addition to Chapter 3, "Entering Commands and Using Command Files."

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 Chapter 3 of *Using the Bay Command Console (BCC)*.

show hardware Command

This section is an addition to Appendix B, "System show Commands." It includes the new **processors** option for the **show hardware** command.

show hardware

The **show hardware** commands display information about router hardware. This command supports the following subcommand options:

backplane	memory
config_file	processors
daughter_card	proms
image	slots

backplane

Displays information about the state of the backplane hardware. The table includes the backplane type, revision, and serial number. The revision and serial numbers are in decimal format.

config_file

Displays the configuration file used to boot the router or reset a slot. The table shows the volume and file name used as the source of the configuration. The table also shows the date and load time.

daughter_card

Displays information about the hardware that is performing compression services. The table shows the slot where the compression hardware resides, as well as the card type, revision, and serial number of the compression hardware.

image

Displays the router's software image for each slot, including the integration that is the source of the image, the date and time of the image's creation, and the file name that contains the image.

memory

Displays memory configuration and capacity information for all slots or a specific slot.

Slot	Slot number.
Local Memory	Total memory capacity in megabytes (MB) of the processor on the slot.
Global Memory	Current memory configuration in MB of the processor on the slot.
Total Memory	Total local and global memory in MB.

processors

Displays processor information for all slots. The table includes the serial number and revision of the processor on each router slot.

proms

Displays PROM information for all slots. The table includes the revision and build date of the bootstrap PROM and the diagnostics PROM.

slots

Displays hardware information about all slots in the system. The table includes information about the processor module and link module for each slot, as well as the module type, revision, and serial number. The revision and serial numbers are in decimal format.

For the AN, the table indicates that the AN has an 802.3 repeater (HUB) by indicating that the link module is an ANSEDSH.

For the ASN, the table displays the revision and serial number of the chassis, processor module, and the network module type, revision, and serial number.

Configuring the BCC Inactivity Timer

This section is an addition to Appendix A, “Multilevel Access.”

With Version 15.6, you can configure an inactivity timeout to end BCC sessions when no traffic is passed from the station that opened the BCC session. This timeout ensures that when the BCC session is closed, the memory used by the old session is released.

To set a timeout for BCC sessions when there is no activity, navigate to the `bcc-config` prompt (for example, **box; access; bcc-config**) and enter:

inactivity-time *<integer>*

integer is the number of minutes that the BCC can remain idle before the session times out. Enter a value from 1 through 35791394 (the default value).

For example, the following commands set the BCC inactivity timer to 20 minutes:

```
box# access
access# bcc-config
bcc-config# inactivity-time 20
bcc-config#
```

Appendix A
Site Manager Parameters

This appendix describes the following Site Manager parameters:

You can display the same information using Site Manager online Help. For each parameter, this appendix provides the following information:

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

You can also use the Technician Interface to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is the same as modifying parameters using Site Manager. For information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Adjacent Host Parameter

You use the following parameter to configure the local IP address for an adjacent host.

Parameter: IP Local Address

Path: Configuration Manager > Protocols >IP > Adjacent Hosts

Default: 0.0.0.0

Options: Any valid IP address

Function: Specifies the IP address of the local IP interface. The adjacent host must be on the same subnet as the local IP interface.

Instructions: Enter the IP address in dotted-decimal notation.

MIB Object ID:. N/A

ATM Line Parameters

You use the following parameters to configure ATM line details on the Passport 5430. The type of ATM link module you use determines the line details that you can edit.

Parameter: Enable

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Enable

Options: Enable | Disable

Function: Enables or disables the line driver.

Instructions: Select Enable or Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.2

Parameter: Interface MTU

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: 4608

Options: 0 to 9188

Function: Specifies the largest packet size (in octets) that the router can transmit on this interface.

Instructions: Enter a value that is appropriate for the network.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.9

Parameter: Data Path Enable

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Enable

Options: Enable | Disable

Function: Specifies whether the router disables the interface between the driver and the higher-level software (the data path interface) when you disconnect the cable from the ATM module.

If you select Enable, then when you disconnect the cable from the ATM module, the router disables the data path interface after the time you specify with the Data Path Notify Timeout parameter.

If you select Disable, the router does not disable the data path interface when you disconnect the cable from the ATM module.

Instructions: Select Enable or Disable. If you select Enable, be sure to enter an appropriate value for the Data Path Notify Timeout parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.11

Parameter:	**Data Path Notify Timeout**
Path:	Configuration Manager > ATM1 > ATM Line Attributes
Default:	1
Options:	0 to 3600
Function:	Specifies the time (in seconds) that the router waits before disabling the data path interface when you disconnect the cable from the ATM module, providing that you set the Data Path Enable parameter to Enable.
Instructions:	Accept the default or enter an appropriate value.
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.3.2.1.12

Parameter:	**Framing Mode**
Path:	Configuration Manager > ATM1 > ATM Line Attributes
Default:	DS3_CBIT (for DS3 lines) | E3_G832 (for E3 lines) | T1ADM (for DS1 lines) | E1ADM (for E1 lines)
Options:	DS3_CBIT | DS3_M32 | T3CBITTPLCP | T3M23PLCP | E3_G751 | E3_G832
Function:	Specifies the transceiver mode for the physical interface.
Instructions:	Select a transceiver mode as follows: • DS3_CBIT, DS3_M32, T3CBITTPLCP, or T3M23PLCP for DS3 modules • E3_G751 or E3_G832 for E3 modules
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.3.2.1.17

Parameter: Cell Scrambling (Passport 5430)

Parameter: DS3/E3 Scrambling (BN)

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Off

Options: On | Off

Function: If you select On, the router randomizes cell payload sufficiently to guarantee cell synchronization. If you select Off, cell synchronization problems can occur.

Note that ATM devices with different settings for scrambling cannot communicate. For example, if you configure a router to enable scrambling and configure a hub to disable scrambling, the router and the hub cannot communicate.

Instructions: If you select On, be sure to enable scrambling for all devices on the network. If you select Off, be sure to disable scrambling for all devices on the network.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.22

Parameter: Per-VC Clipping

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Disable

Options: Enable | Disable

Function: Enables or disables cell clipping on a per-VC basis.

Instructions: Accept the default, Disable, for normal VC clipping. Enable this parameter if you want to clip cells on a per-VC basis.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.1.1.17

Parameter:	**DS3 Line Build Out**
Path:	Configuration Manager > ATM1 > ATM Line Attributes
Default:	Short
Options:	Short | Long
Function:	Conditions router signals to mitigate attenuation, which depends on the physical length of the line. You can set this parameter only for DS3 modules.
Instructions:	Select Short for lines shorter than 225 feet; select Long for lines 225 feet or longer.
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.3.2.1.23

ATM Port Parameters

You use the following parameters to configure the ATM T3/E3 interface on the Passport 5430.

Parameter:	**Enable/Disable**
Path:	Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables this interface.
Instructions:	Set to Disable only if you want to disable the interface.
MIB Object ID:	1.3.6.1.4.1.18.3.4.26.10.1.2

Parameter:	**Line Type**
Path:	Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**
Default:	Autodetect
Options:	For DS3, the options are DS3 M23 | DS3 CBIT Parity | Autodetect For E3, the options are E3 Framed | E3 PLCP
Function:	Sets the frame format for this interface.
Instructions:	Determines the framing mode for this interface. For DS3, if you choose DS3 M23 or DS3 CBIT Parity, be sure that the ATM line attribute Framing Mode is appropriately set: If the Line Type is DS3 M23, Framing Mode should be DS3_M23 or T3M23PLCP. If Line Type is DS3 CBIT Parity, Framing Mode should be DS3_CBIT or T3CBITPLCP. For E3, make sure that the ATM line attribute Framing Mode is set to either E3_G751 or E3_G832.
MIB Object ID:	1.3.6.1.4.1.18.3.4.26.10.1.7

Parameter:	**Setup Alarm Threshold (seconds)**
Path:	Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**
Default:	2
Options:	2 to 10
Function:	Sets the time interval (in seconds) during which the device driver tolerates a performance defect or anomaly. If the performance defect or anomaly is still present when time interval expires, the device driver records a performance failure and logs an event message.
Instructions:	Set the timer value in seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.4.26.10.1.17

Parameter: Clear Alarm Threshold (seconds)

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: 2

Options: 2 to 10

Function: Specifies the clear time (in seconds) for performance failure conditions. If the defect or anomaly clears within this interval, the device driver records a performance cleared condition and logs an event message.

Instructions: Set the timer value in seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.18

Parameter: Loopback Configuration

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: No Loopback

Options: No Loopback | Payload Loopback | Line Loopback

Function: Forces the interface into loopback mode. The far-end or intermediate equipment then performs diagnostics on the network between that equipment and the T3/E3 interface. After testing, set this parameter to No Loopback to return the interface to a normal operating mode.

- No Loopback — Returns the interface to non-loopback operation.
- Payload Loopback — The received signal at this interface is looped through the device. Typically the received signal is looped back for re-transmission after it has passed through the device's framing function.
- Line Loopback — The received signal at this interface does not go through the framing device (minimum penetration) but is looped back out.

Instructions: Select the loopback configuration option.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.9

Parameter: Primary Clock

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: Loop

Options: Internal | Loop

Function: Specifies the clock signal source.

Instructions: Select Internal if you want the router to generate the clock signal source. Otherwise, accept the default, Loop, if you want the clock signal source to be external to the router.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.11

ATM Service Record Parameter

You use the following parameter to specify a line speed value for a PVC service record or for a classical IP service record.

Parameter: Optional Line Speed

Path: Configuration Manager > Circuits > Edit Circuits > **Edit** > **ATM** > **Service Attributes**

Default: 0

Options: 0 or any positive integer

Function: Specifies the line speed, in bits per second, for this service record. This value is reported by the ifSpeed MIB variable, which is used by SNMP-based management applications to obtain a line speed for any VC configured on this service record and to generate alarms as required. If you accept the default value, 0, the line speed of the interface as a whole is displayed in network management applications that use the ifSpeed MIB variable to monitor traffic statistics. **Note**: The value that you set with this parameter is for reporting purposes only; it has no effect on the actual performance of the virtual circuit.

Instructions: Accept the default value, 0, to allow the ifSpeed MIB variable to report the interface speed. Otherwise, enter an integer value up to the maximum line speed of this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.2.1.17

Automated Security Association (IKE) Parameters

You use the following parameters to define a cryptographic key for creating IKE SAs between routers.

Parameter:	**Pre-shared Key (ascii)**
Path:	Configuration Manager > Protocols > IP > IKE Configuration Manager > Edit Circuit > Protocols > Edit IP > IKE
Default:	None
Options:	Up to 24 ASCII characters
Function:	Used as a cryptographic key for creating IKE SAs between routers. IKE is then used to create automated SAs for data packets.
Instructions:	Enter an ASCII string, up to 24 characters. Configure the same preshared key on the destination router.
MIB Object ID:	None

Parameter:	**Pre-shared Key (hex)**
Path:	Configuration Manager > Protocols > IP > IKE Configuration Manager > Edit Circuit > Protocols > Edit IP > IKE
Default:	None
Options:	Up to 24 bytes
Function:	Used as a cryptographic key for creating IKE SAs between routers. IKE is then used to create automated SAs for data packets.
Instructions:	Enter a hexadecimal number, up to 24 bytes. (Enter the prefix **0x** before the digits.) Configure the same preshared key on the destination router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.27.1.1.9

BGP-3-Specific Announce Policy Parameter

You use the following parameter to specify one or more BGP peers.

Parameter:	**Outbound Peers**
Path:	Configuration Manager > Protocols > IP > Policy Filters > BGP-3 > Announce Policies
Default:	An empty list
Options:	A list of IP numbers
Function:	Specifies the BGP router ID of the peer. To verify the router ID of the BGP peer, on the peer router, check the configured value for the Site Manager BGP Global parameter, BGP Identifier, or the BCC BGP parameter, router-id. This policy applies to BGP advertisements authored by a router on this list, and applies only to BGP-sourced routes when BGP is included as a route source.
Instructions:	Specify one or more IP addresses. Configure an empty list to indicate that this policy applies to BGP advertisements being sent to any peer.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.8.1.23

BGP-4-Specific Announce Policy Parameter

You use the following parameter to specify one or more BGP peers.

Parameter: **Outbound Peers**

Path: Configuration Manager > Protocols > IP > Policy Filters > BGP-4 > Announce Policies

Default: An empty list

Options: A list of IP addresses

Function: Specifies the BGP router ID of the peer. To verify the router ID of the BGP peer, on the peer router, check the configured value for the Site Manager BGP Global parameter, BGP Identifier, or the BCC BGP parameter, router-id.

This policy applies to BGP advertisements authored by a router on this list, and applies only to BGP-sourced routes when BGP is included as a route source.

Instructions: Specify one or more IP addresses. Configure an empty list to indicate that this policy applies to BGP advertisements being sent to any peer.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.10.1.23

DSQMS RED Parameters

The Edit Red Parameters window (Figure A-1) contains the RED parameters. These parameters define a set of attributes for the RED function. These instances of DSQMS RED are used by traffic classifiers in managed queues.

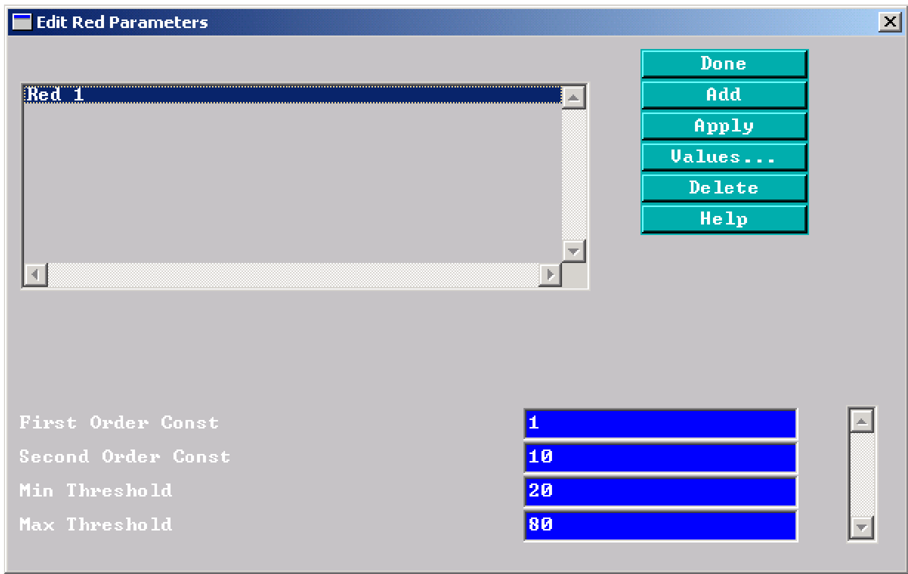

Figure A-1. Edit Red Parameters Window

Parameter: First Order Const

Path: Configuration Manager > Protocols > IP > DSQMS > RED

Default: 1

Options: 0 through 100

Function: Specifies the first-order constant used when calculating the drop probability based on the average queue fraction, the queue size, and the value of the Min Threshold parameter.

Instructions: Accept the default value, 1, or reset the first-order constant to a value from 0 through 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.4.1.5

Parameter: Second Order Const

Path: Configuration Manager > Protocols > IP > DSQMS > RED

Default: 10

Options: 0 through 1000

Function: Specifies the second-order constant used when calculating the drop probability based on the average queue fraction, the queue size, and the value of the Min Threshold parameter.

Instructions: Accept the default value, 10, or reset the second-order constant to a value from 1 through 1000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.4.1.4

Parameter: Min Threshold

Path: Configuration Manager > Protocols > IP > DSQMS > RED

Default: 20

Options: 0 through 100

Function: Indicates the queue size (as a percentage) below which no packets are dropped by RED. When the minimum threshold value is reached, the router begins dropping packets in direct relation to any increase in average queue size until the average queue size falls below the minimum threshold value.

Instructions: Accept the default value, 20 percent, or reset the minimum threshold to a value from 0 through 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.4.1.6

Parameter: Max Threshold

Path: Configuration Manager > Protocols > IP > DSQMS > RED

Default: 80

Options: 1 through 100

Function: Indicates the queue size (as a percentage) above which all packets are dropped by RED. When the maximum threshold value is reached, the router drops all packets until the average queue size falls below the maximum threshold value.

Instructions: Accept the default value, 80 percent, or reset the maximum threshold to a value from 1 through 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.4.1.7

DSQMS Interface Parameters

The Edit DSQMS Parameters window (Figure A-2) contains DSQMS parameters for the physical interface. These parameters let you enable DSQMS on the interface, set the debug level, and configure FRF.12 interleaving parameters.

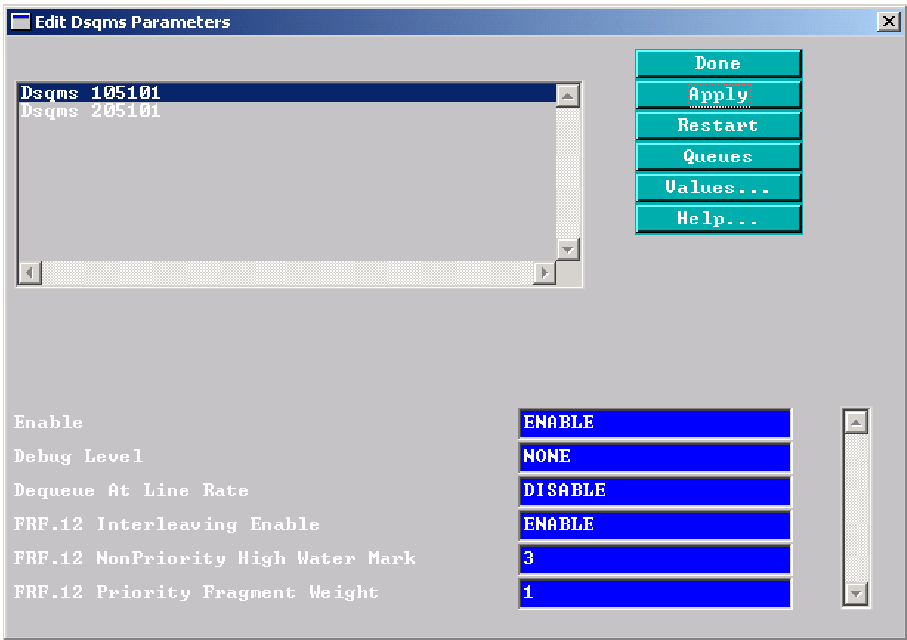

Figure A-2. Edit DSQMS Parameters Window

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > DSQMS > Interface
Default:	Enable
Options:	Enable | Disable
Function:	Disables and reenables DSQMS on the interface.
Instructions:	To disable DSQMS on the interface, select Disabled. To reenable DSQMS on the interface, select Enabled.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.16.1.1.2

Parameter:	**Debug Level**
Path:	Configuration Manager > Protocols > IP > DSQMS > Interface
Default:	None
Options:	Trace | Detailed | None
Function:	By default, the router does not log event messages generated by DSQMS. To troubleshoot a problem, set this parameter to Trace to log related DSQMS function names or to Detailed to log trace messages, some environment variables, and queue information.
Instructions:	Accept the default value, None, to prevent the router from logging DSQMS event messages. To troubleshoot a problem, set this parameter to Trace or to Detailed.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.16.1.1.11

Parameter:	**Dequeue At Line Rate**
Path:	Configuration Manager > Protocols > IP > DSQMS > Interface
Default:	Disable
Options:	Enable | Disable
Function:	Controls the dequeuing of packets from the queues to the driver and guarantees constant bandwidth for traffic that requires a constant delay rate when there are more buffers than the line can accommodate. If you configure both weighted and priority queues on an interface, you may experience latency problems with the high-priority queues. To reduce delay for queues that require a constant delay rate when limited bandwidth is available, enable this parameter. **Note**: Enabling this parameter may cause packet loss in both priority and weighted queues in certain configurations when higher traffic levels are seen in these queues.
Instructions:	To enable the interface to dequeue packets at line rate, set this parameter to Enable. To disable dequeuing at line rate on the interface, select Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.16.1.1.19

You use the following parameters to configure FRF.12 fragment interleaving on an interface.

Parameter: FRF.12 Interleaving Enable

Path: Configuration Manager > Protocols > IP > DSQMS > Interface

Default: Disable

Options: Enable | Disable

Function: Enables or disables FRF.12 fragmentation interleaving on this interface. FRF.12 interleaving is done only on packets in the DSQMS shaped pool. To use FRF.12 fragmentation, you must enable this parameter and also set FRF.12 and traffic shaping parameters on the PVCs configured on this physical interface.

Instructions: To enable FRF.12 fragmentation interleaving on this interface, set this parameter to Enable. To disable FRF.12 fragmentation interleaving, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.1.1.38

Parameter: FRF.12 NonPriority High Water Mark

Path: Configuration Manager > Protocols > IP > DSQMS > Interface

Default: 3

Options: 1 through 64

Function: Specifies the maximum number of consecutive data packet fragments to be sent to the link with no voice packets to interleave. When DSQMS dequeues packets for the link, it stops dequeuing when the number of packets specified by this parameter is reached if it does not find any intervening voice packets. If you set this parameter to a low value, link performance may be adversely affected.

Instructions: Accept the default value, 3, or enter a value from 1 through 64.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.1.1.39

Parameter: **FRF.12 Priority Fragment Weight**

Path: Configuration Manager > Protocols > IP > DSQMS > Interface

Default: 1

Options: 1 through 64

Function: Specifies the number of voice packets to be interleaved between data packet fragments when passing fragments to the link. If you set this parameter to a higher value, then more voice fragments are passed between data fragments.

Instructions: Accept the default value, 1, or enter a value from 1 through 64.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.1.1.40

DSQMS Queue Parameters

The Edit DSQMS Queue List window (Figure A-3) contains parameters for a DSQMS queue configured on the physical interface.

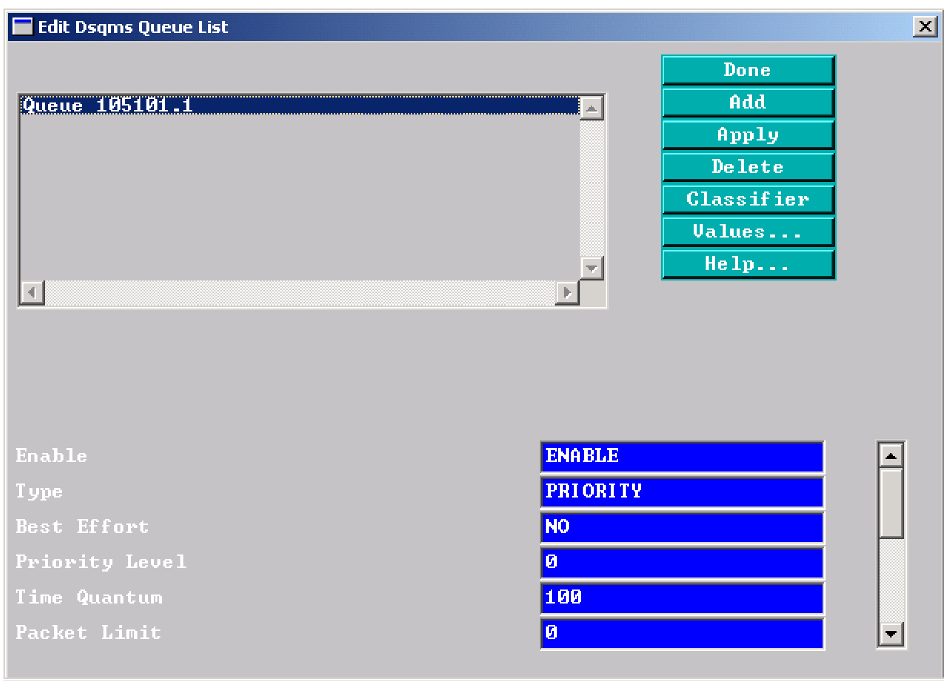

Figure A-3. Edit DSQMS Queue List Window

Parameter: Enable

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: Disable

Options: Enable | Disable

Function: Enables and disables this DSQMS queue.

Instructions: To enable this DSQMS queue, select Enable. To disable this DSQMS queue, select Disabled.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.2

Parameter: Type

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: Priority

Options: Priority | Weighted

Function: Selects the queue scheduling type: strict priority or weighted deficit round robin (DRR).

Instructions: To set the queue scheduling type to weighted deficit round robin, select Weighted. To set the queue scheduling type to strict priority, select Priority.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.6

Parameter: Best Effort

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: No

Options: No | Yes

Function: Specifies whether to use this queue for best-effort traffic. By default, DSQMS selects the weighted queue with the lowest configured weight as the best-effort queue; if all weighted queues have the same weight, the last one created becomes the best-effort queue. If priority queues only are configured on this interface, DSQMS selects the queue with the lowest priority; if all queues have the same priority, the last one created becomes the best-effort queue. Use this parameter to override the default selection and select a different best-effort queue. You cannot configure flow fairness on the best-effort queue.

Instructions: To override the default selection of the best-effort queue, select Yes or No.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.7

Parameter: Priority Level

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: 0

Options: 0 through 29

Function: Sets the priority level for this queue: 0 is the highest priority. This parameter applies to priority queues only.

Instructions: To reset the priority level for this queue, specify a value from 0 through 29. The value 0 is the highest priority.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.8

Parameter: Time Quantum

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: 100

Options: 0 through 5000

Function: Specifies the maximum amount of time (in milliseconds) that this queue is allowed to transmit data before the router must service other queues—priority and weighted. This parameter applies to priority queues only.

Instructions: To reset the maximum number of milliseconds that this queue is allowed to transmit data, enter a value from 0 through 5000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.9

Parameter: Packet Limit

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: 0

Options: 0 through 2147483647

Function: Specifies the maximum number of packets that this queue can hold. The value 0 indicates that this queue will hold a maximum number that is less than or equal to 256; the software calculates this value based on the router you are configuring and the number of queues configured. **Note**: If this queue will be used by shaped frame relay PVCs and the value of this parameter is set to 0, the packet limit for the queue defaults to 20.

Instructions: To set a maximum number of packets for this queue to hold, enter a value from 1 through 256. Or accept the default value, 0, to set the maximum packet limit to a software-determined value that is less than or equal to 256. (**Note**: If this queue will be used by shaped frame relay PVCs and the value of this parameter is set to 0, the packet limit for the queue defaults to 20.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.10

Parameter: Byte Limit

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: 0

Options: 0 through 2147483647

Function: Specifies the maximum number of bytes that this queue can hold. The value 0 indicates that this queue is limited only by global memory.

Instructions: To set a maximum number of bytes for this queue to hold, enter a value greater than 0. To set no limit on the number of bytes, accept the default value, 0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.12

Parameter:	**Config Weight**
Path:	Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**
Default:	1
Options:	1 through 100
Function:	Specifies the ratio of this queue to the sum of all weighted queues on the interface. This ratio can be calculated relative to other queue values or expressed as a percentage, provided that all weighted queues add up to 100. This parameter applies to weighted queues only.
Instructions:	Enter a value from 1 through 100, or accept the default value, 1.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.16.2.1.13

Parameter:	**Flow Fairness**
Path:	Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether a hash table is used to separate data packets into buckets within this queue. This mechanism improves fairness within a queue. You cannot configure flow fairness on the best-effort queue.
Instructions:	To enable the use of a hash table to separate data packets into buckets within this queue, select Enable. Otherwise, accept the default value, Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.16.2.1.16

Parameter:	**Jitter Constant**
Path:	Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**
Default:	Normal
Options:	Small | Normal | Large
Function:	Categorizes how sensitive traffic in this queue is to the jitter effect, and thus provides an indicator for calculating the bucket size in flow fairness. Reset this parameter if the packets that this queue will handle are small (for example, VoIP packets) or large (for example, video packets).
Instructions:	Reset this parameter if the packets that this queue will handle are small or large. Otherwise, accept the default value, Normal.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.16.2.1.17

Parameter: Drop Type

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: Tail Drop

Options: Tail Drop | RED

Function: Indicates whether RED is used for active queue management.

Instructions: To enable RED for queue management, select RED. Otherwise, accept the default value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.19

Parameter: Average Queue Gain

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: 30

Options: 1 through 100

Function: Specifies the percentage of buffer capacity that must fill for 1 second or more for DSQMS to compute a larger average queue size for use by RED.

Instructions: To specify a different percentage, enter an integer from 0 through 100. Otherwise, accept the default value, 30 percent.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.26

Parameter: Idle Loss Rate

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues**

Default: 30

Options: 1 through 99

Function: Specifies the percentage of buffer capacity that must empty for 1 second or more for DSQMS to compute a smaller average queue size for use by RED.

Instructions: To specify a different percentage, enter an integer from 1 through 99. Otherwise, accept the default value, 30 percent.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.2.1.27

DSQMS Queue Classifier Parameters

The Edit DSQMS Classifier List window (Figure A-4) contains parameters for a DSQMS classifier configured on the queue. These parameters let you specify the DSCP in the traffic header that this classifier will match, as well as the DSQMS RED instance used by the classifier.

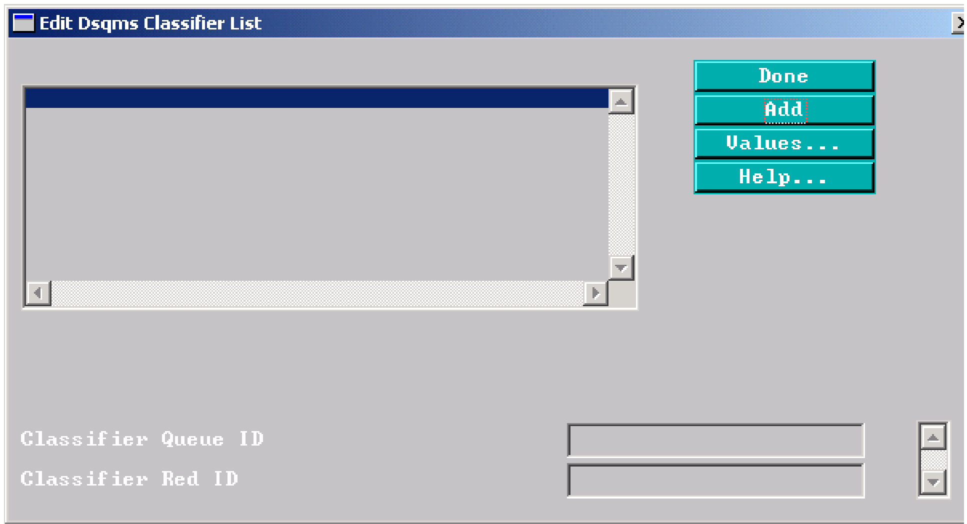

Figure A-4. Edit DSQMS Classifier List Window

Parameter: **Classifier ID**

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues** > **Classifier** > **Add**

Default: Null

Options: 8-digit differentiated services code point (binary octet)

Function: Specifies a DSCP value as an 8-digit binary octet. Traffic that matches this value is treated according to the attributes configured for the associated queue and according to the DSQMS RED instance attributes (if you also set the optional Classifier RED ID parameter).

Instructions: Enter the 8-digit DSCP value that this classifier will sort traffic on. Only traffic that includes this DSCP will be handled by this classifier.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.3.1.1

Parameter: Classifier Queue ID

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues** > **Classifier**

Default: 1

Options: 1 through 30

Function: Specifies the DSQMS queue that this classifier belongs to.

Instructions: Enter the numerical queue ID.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.3.1.4

Parameter: Classifier RED ID

Path: Configuration Manager > Protocols > IP > DSQMS > Interface > **Queues** > **Classifier**

Default: 0

Options: 0 through 65535

Function: Specifies the numerical ID of the DSQMS RED instance that this traffic classifier will use to manage traffic. (The RED instance IDs are displayed in the Edit RED Parameters window.) Set this parameter only if you are associating a set of RED attributes with the classifier.

Instructions: If this traffic classifier will use a RED instance, enter the value of the configured RED instance. Otherwise, accept the default value, 0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.16.3.1.5

Frame Relay PVC Parameters

You use the following parameters to configure traffic shaping on a frame relay PVC.

Parameter: Committed Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > **PVCs**

Default: 0

Options: 0 to 2147483647 bits

Function: The maximum number of bits that a VC can transmit during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, this parameter and the Throughput parameter (CIR) must both be greater than zero. The Committed Burst (Bc) value should be lower than the Throughput.

Instructions: Enter a value within the given range. You should set this parameter to 1/4 of the CIR unless this VC is sending frames larger than that size. If the VC is sending large frames, increase the value of this parameter to accommodate the size of those frames.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.16

Parameter: Excess Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > **PVCs**

Default: 0

Options: 0 to 2147483647 bits

Function: This value is added to the Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Excess Burst plus the Committed Burst must be less than or equal to the line speed.

Instructions: Enter a value within the given range.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.17

Parameter: Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > **PVCs**

Default: 0

Options: 0 to 2147483647 b/s

Function: Specifies the rate in bits per second at which data travels over this VC when no congestion is occurring. To enable traffic shaping, this parameter and the Committed Burst parameter must be set to values greater than zero.

Instructions: Your carrier supplies the CIR or throughput value, which you enter in this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.18

Parameter: Bw Threshold

Path: Configuration Manager > Protocols > Frame Relay > Services > **PVCs**

Default: 0

Options: 0 to maximum physical line speed (bits/s)

Function: Specifies the bandwidth threshold that you want to set for this PVC for traffic shaping purposes.

Instructions: To minimize starvation of normal- and low-priority traffic over a high-speed physical line (such as a 56 Kb/s lines over HSSI), set the bandwidth threshold to a value 3 to 10 times that set for the Throughput (CIR) parameter. Otherwise, accept the default, 0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.58

You use the following parameters to configure FRF.9 compression on a frame relay PVC.

Parameter:	**FRF.9 Enable**
Path:	Configuration Manager > Protocols > Frame Relay > Services > **PVCs**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables FRF.9 compression on this PVC. You must disable the WCP Enable parameter before you can enable FRF.9 compression.
Instructions:	To enable FRF.9 compression, select Enable. To disable FRF.9 compression, select Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.2.1.64

Parameter:	**FRF.9 Min Compress Size**
Path:	Configuration Manager > Protocols > Frame Relay > Services > **PVCs**
Default:	0
Options:	Any integer
Function:	Specifies the minimum size in bytes of an outgoing frame in order for it to be compressed using FRF.9 compression. Because small frames are less likely to experience a reduction in byte count from compression, you can use this parameter to skip compression of frames smaller than the value you specify. This test of the compression threshold is performed for each outgoing buffer.
Instructions:	To set a minimum size threshold for frames to be compressed using FRF.9 compression, specify an integer. Otherwise, accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.2.1.65

You use the following parameters to configure FRF.12 fragmentation on a frame relay PVC.

Parameter: FRF.12 Fragmentation Enable

Path: Configuration Manager > Protocols > Frame Relay > Services > **PVCs**

Default: Disable

Options: Disable | Enable

Function: Enables or disables FRF.12 fragmentation of data packets on the PVC. To accomplish interleaving of the packet fragments with voice packets (which are never fragmented), configure the FRF.12 interleaving parameters, which are associated with the interface on which this PVC is configured (see the interleaving parameter descriptions beginning on page A-18).

Instructions: To enable FRF.12 fragmentation of data packets, set this parameter to Enable. To disable FRF.12 fragmentation, set this parameter to Disable. When you change the value of this parameter, the PVC restarts.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.66

Parameter: FRF.12 Fragmentation Trigger Size

Path: Configuration Manager > Protocols > Frame Relay > Services > **PVCs**

Default: 80

Options: 1 through 32767

Function: Specifies the minimum size of a data packet to fragment on this PVC; this number of bytes is the size of the fragmented packet payload. Any packet smaller than the specified number of bytes will not be fragmented.

Instructions: To change the minimum size of a data packet to fragment on this PVC, set this parameter to the appropriate number of bytes. Otherwise, accept the default value, 80 bytes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.68

Frame Relay Service Record Parameter

You use the following parameter to specify a line speed value for a frame relay service record.

Parameter:	**Optional Line Speed**
Path:	Configuration Manager > Protocols > Frame Relay > Services
Default:	0
Options:	0 or any positive integer
Function:	Specifies the line speed, in bits per second, for this service record. This value is reported by the ifSpeed MIB variable, which is used by SNMP-based management applications to obtain a line speed for any VC configured on this service record and to generate alarms as required. If you accept the default value, 0, the line speed of the interface as a whole is displayed in network management applications that use the ifSpeed MIB variable to monitor traffic statistics. **Note**: The value that you set with this parameter is for reporting purposes only; it has no effect on the actual performance of the virtual circuit.
Instructions:	Accept the default value, 0, to allow the ifSpeed MIB variable to report the interface speed. Otherwise, enter an integer value up to the maximum line speed of this interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.5.1.38

Frame Relay SVC Parameters

You use the following parameters to configure FRF.9 compression on a frame relay SVC.

Parameter:	**FRF.9 Enable**
Path:	Configuration Manager > Protocols > Frame Relay > Services > **SVCs**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables FRF.9 compression on this SVC. You must disable the WCP Enable parameter before you can enable FRF.9 compression.
Instructions:	To enable FRF.9 compression, select Enable. To disable FRF.9 compression, select Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.35

Parameter:	**FRF.9 Min Compress Size**
Path:	Configuration Manager > Protocols > Frame Relay > Services > **SVCs**
Default:	0
Options:	Any integer
Function:	Specifies the minimum size in bytes of an outgoing frame in order for it to be compressed using FRF.9 compression. Because small frames are less likely to experience a reduction in byte count from compression, you can use this parameter to skip compression of frames smaller than the value you specify. This test of the compression threshold is performed for each outgoing buffer.
Instructions:	To set a minimum size threshold for frames to be compressed using FRF.9 compression, specify an integer. Otherwise, accept the default value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.36

GRE Remote Connection Parameters

You use the following parameter to enable and disable the transmission of GRE keepalive messages from a GRE tunnel's local endpoint to its remote endpoint.

Parameter:	**Keepalive**
Path:	Configuration Manager > Protocols > IP > GRE > Remote Conn
Default:	Disabled
Options:	Enabled | Disabled
Function:	Enables and disables the transmission of GRE keepalive messages between a GRE tunnel's local endpoint and one of its configured remote tunnel endpoints.
Instructions:	Set to enable to activate the transmission of GRE keepalive messages between a GRE tunnel's local endpoint and one of its configured remote tunnel endpoints. Set to disable to stop the transmission of GRE keepalive messages between a GRE tunnel's local endpoint and one of its configured remote tunnel endpoints
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.28.1.8

You use the following parameter to specify the number of seconds you want the router to wait before sending another keepalive packet from the GRE tunnel's local endpoint to its remote endpoint.

Parameter:	**Keepalive Retry Timeout**
Path:	Configuration Manager > Protocols > IP > GRE > Remote Conn
Default:	10 (seconds)
Options:	1 to 32,766 (seconds)
Function:	Specifies the amount of time in seconds that the router waits between sending successive keepalive packets from the GRE tunnel's local endpoint to the GRE tunnel's remote endpoint.
Instructions:	Specify the number of seconds you want the router to wait before sending another keepalive packet from the GRE tunnel's local endpoint to its remote endpoint.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.28.1.9

You use the following parameter to specify the amount of time that the router waits for a reply to a GRE keepalive message before it declares that the GRE tunnel is down.

Parameter:	**Keepalive Retries**
Path:	Configuration Manager > Protocols > IP > GRE > Remote Conn
Default:	3
Options:	2 to 254, inclusive
Function:	Specifies the amount of time that the router waits for a reply to a GRE keepalive message sent from a GRE tunnel's local endpoint to its remote endpoint before declaring that the GRE tunnel is down. This waiting period is calculated by multiplying the currently configured value of the Keepalive Retry Timeout parameter by the value of this parameter.
Instructions:	Specify the number by which to multiply the currently configured value of the Keepalive Retry Timeout parameter in order to calculate the Keepalive Retries waiting period. For example, if the Keepalive Retry Timeout parameter is set to 20 (seconds) and you set the value of this parameter to 6, then the router will wait 120 seconds (6 x 20 seconds) for a reply to the GRE keepalive message before declaring that the GRE tunnel is down.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.28.1.10

IGMP Global Parameters

For IGMP Version 3 (introduced in BayRS Version 15.6), a number of new IGMP global parameters were added and a number of existing parameters were changed or made obsolete. For this reason, all IGMP global parameters are provided in this section. Use the following descriptions to set IGMP global parameters.

Note: The global IGMP parameter Version Threshold Time is now obsolete and no longer appears on the IGMP Global Configuration window.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: Enable
Options: Enable | Disable
Function: Enables or disables this IGMP record.
Instructions: If you configured IGMP on this router, use this parameter to disable it.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.2

Parameter: Relay

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default: Disable
Options: Enable | Disable
Function: Enables and disables IGMP Relay.
Instructions: Set the parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.10

Parameter: Estimated Groups

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: 20

Options: 5 to 65,535

Function: Specifies the estimated number of multicast groups that will be simultaneously active for this router. This estimate allows the router to use memory efficiently. Exceeding this size during router operation will not cause an error but may cause the router to consume more memory than required. Do not include in the count any group from 224.0.0.0 through 224.0.0.255.

Instructions: Determine the approximate number of groups and enter the value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.4

Parameter: Debug

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: None

Options: See instructions.

Function: Causes IGMP to generate the specified log messages.

Instructions: Click on Values and select the types of log messages that you want IGMP to generate. The Debug field displays the following bitmasks for each type of message:

0x00000001 for received IGMP join/leave packets
0x00000002 for sent IGMP messages
0x00000004 for received multicast protocol messages
0x00000008 for MTRACE log messages
0x00000010 for configuration log messages
0x00000020 for interaction with multicast protocols
0x00000040 for interaction with RSVP
0x00000080 for MTM forwarding cache log messages
0x00000100 for IGMP Relay log messages
0x00000200 for received IGMP Version 3 log messages
0x00000400 for sent IGMP Version 3 log messages
0x00000800 for other IGMP Version 3 log messages

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.6

Parameter:	**Join Ack Enable**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default:	Disable
Options:	Enable | Disable
Function:	Indicates whether IGMP should send an immediate response (in the form of a query) to the group associated with this IGMP membership report.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.1.7

Parameter:	**Forward Cache Limit**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default:	512
Options:	64 to 65,535
Function:	Specifies the maximum number of MTM forwarding cache entries.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.1.8

Parameter:	**Nonlocal Reports**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default:	Ignore
Options:	Ignore | Accept
Function:	Controls whether IGMP accepts or ignores leave and join messages from a nonlocal network.
Instructions:	Set the parameter as required by your configuration.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.1.9

Parameter: SSM Ranges

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: 232.0.0.0-232.255.255.255

Options: Non-overlapping multicast address ranges

Function: Specifies one or more multicast group address ranges for SSM. If you configure more than one SSM range, the ranges cannot overlap. IGMP Version 3 packets are valid only if the multicast destination address is within a configured SSM range.

Instructions: Click in the parameter field and then click on the List button. For each range, enter an 8-octet specification. The first four octets specify the first IP address of the SSM range; the second four octets specify the network mask for the SSM range. For example, enter IP address 233.0.0.0 and network mask 255.0.0.0. Enter an exact encoding of 0.0.0.0/0.0.0.0 to disable SSM ranges.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.15

Parameter: Relay Forwarding Timeout

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: 60 seconds

Options: 0 to 65,535

Function: Sets the lifetime in seconds of IGMP Relay Multicast Table Manager forwarding entries.

Instructions: Set the timer as required by your configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.11

Parameter: Relay Upstream Forwarding

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global

Default: Primary

Options: Primary | Backup | Both

Function: Specifies whether multicast data is forwarded from the IGMP Relay device onto the primary upstream interface, the backup interface, or both when both interfaces are active.

Instructions: Select an option as required by your configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.12

Parameter:	**Translation Enable**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Global
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables the use of the PIM-SM/PIM-SSM translation table. The translation table is a migration tool to translate PIM-SM/IGMP Version 2 information into PIM-SSM/IGMP Version 3 so that the two implementations of PIM can work together. When the translation table is configured, the table translates IGMP Version 2 groups into IGMP Version 3 (group, source) pairs. The translation table is configured on a PIM domain border router only.
Instructions:	Before you enable this parameter, configure the translation table (choose Protocols > IP > IGMP/IGMP Relay > Translation Table).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.1.16

IGMP Interface Parameters

For IGMP Version 3 (introduced in BayRS Version 15.6), a number of new IGMP interface parameters were added and a number of existing parameters were changed or made obsolete. For this reason, all IGMP interface parameters are provided in this section. Use the following descriptions to set IGMP interface parameters.

Note: The IGMP interface parameters Interface Membership Timeout and Designated Router Timeout are now obsolete and no longer appear on the IGMP Interfaces Configuration window.

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Indicates whether this IGMP interface record is enabled or disabled.
Instructions:	If you configured IGMP on this interface, use this parameter to disable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.2

Parameter:	**Interface Query Rate**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	125
Options:	0 to 4096 (seconds)
Function:	Specifies how often the router sends group membership queries on the interface. If the interface is running IGMP Version 3, this parameter specifies the interval between general queries. Setting this parameter to a larger value causes queries to be sent less often.
Instructions:	If there are no multicast hosts on this circuit, set the parameter to 0 to disable queries. Specifying 0 affects queries only; the router still forwards multicast datagrams on this circuit. If another IGMP router on this network has assumed the query role, this router will not send queries unless it has not heard any queries within a specific number of seconds calculated by the router. The maximum value, 4096 seconds, is equal to 1 hour, 8 minutes, and 16 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.5

Parameter:	**Net Version**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	IGMPV2
Options:	IGMPV2 | IGMPV3
Function:	Specifies the version of IGMP that the interface is running.
Instructions:	Specify the IGMP version that the network attached to this interface is running.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.14

Parameter: Max Host Response Time

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 100

Options: 1 to 100 (tenths of a second)

Function: Specifies, in tenths of a second, the maximum amount of time that a host must wait before responding to a query. IGMP places this value in the code field of an IGMP query. This value must be smaller than the value specified by the Interface Query Rate parameter. Using this parameter, you can tune the "burstiness" of IGMP message traffic on the network: larger values cause host responses to be spread out over a larger interval.

Instructions: Specify a maximum response time for this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.15

Parameter: Mtrace Entry Lifetime

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 30

Options: 30 to 8192 (seconds)

Function: Specifies in seconds the amount of time that a router should keep a forwarding cache entry that was created specifically for Mtrace.

Instructions: Specify an Mtrace lifetime value for the interface. The maximum value, 8192 seconds, is equal to 2 hours, 16 minutes, and 32 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.18

Parameter: Query Suppression

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: No

Options: Yes | No

Function: Specifies whether IGMP queries are suppressed on this interface.

Instructions: In the Nortel Networks multicast implementation, configuring IGMP on an interface means two things: (1) the interface is used for forwarding multicast traffic and (2) IGMP is running on the interface. Therefore, on some interfaces —for example, point-to-point or nonbroadcast—even though there is no need to run the IGMP protocol, IGMP must still be configured. On such interfaces, you can disable the sending of IGMP queries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.25

Parameter: Static Forward Cache Lifetime

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 216

Options: 80 to 7200 (seconds)

Function: If the IGMP static forwarding policy is set to Static to Dynamic (static inbound and multicast protocol outbound), specifies the number of seconds that the Multicast Table Manager cache entries will be alive for, even if traffic is not present.

Instructions: Set this value based on the multicast protocol that is configured on the outbound interface. A typical value for PIM is 210 seconds (3 1/2 minutes); for DVMRP, 7200 seconds (2 hours); and for MOSPF, 600 seconds (10 minutes).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.28

Parameter: Relay Circuit Type

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default: Downstream
Options: Upstream Primary | Upstream Backup | Downstream
Function: Specifies whether the IGMP circuit is configured as the primary upstream circuit, the backup upstream circuit, or a downstream (no relay) circuit.
Instructions: You can configure only one primary and one backup upstream circuit on the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.23

Parameter: Relay Report Interval

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default: 10
Options: 0 to 255
Function: Specifies the interval (in seconds) between group membership reports on an IGMP Relay primary or backup circuit. If you set this parameter to 0, IGMP Relay sends only one unsolicited group report.
Instructions: Specify an interval in seconds.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.24

Parameter: Robustness Variable

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default: 2
Options: 1 to 8
Function: Specifies a tuning value for the expected packet loss on the network. If you anticipate greater loss of packets on the network, set this parameter to a higher value.
Instructions: Reset the robustness variable, if desired.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.29

Parameter: Startup Query Interval

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 31

Options: 2 to 240

Function: Specifies the number of seconds between general queries sent by the router on this interface when it is started up. Nortel Networks recommends that you set this parameter to 1/4 the value set for the Interface Query Rate parameter.

Instructions: Specify the number of seconds from 2 through 240.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.30

Parameter: Startup Query Count

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 2

Options: 1 to 8

Function: Specifies the number of general queries sent by the router on this interface when it is started up. Nortel Networks recommends that you set this parameter to the same value as the Robustness Variable parameter.

Instructions: Specify an integer from 1 through 8.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.31

Parameter: Last Member Query Interval

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces

Default: 10 (1 second)

Options: 1 to 31,744

Function: Specifies, in tenths of a second, the maximum response time used to calculate the maximum response code inserted into group-specific queries and group-and-source-specific queries sent in response to a leave group message. You can use this parameter to tune the “leave latency” of the network. A reduced value results in reduced time to detect the loss of the last member of a group or source.

Instructions: Specify the interval in tenths of a second.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.32

Parameter:	**Last Member Query Count**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Interfaces
Default:	2
Options:	1 to 8
Function:	Specifies the maximum number of group-specific queries sent before the router assumes that there are no more local members. For IGMP Version 3, this parameter specifies the maximum number of group-and-source-specific queries sent before the router assumes that there are no listeners for a particular source.
Instructions:	Specify an integer from 1 through 8. Nortel Networks recommends that you set this parameter to the same value as the Robustness Variable parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.33

IGMP Translation Table Parameters

For IGMP Version 3 and PIM-SSM, you can create a translation table to map IGMP Version 2 group addresses to one or more IGMP Version 3 (group, source) pairs. The translation table enables the interoperation of IGMP Version 2 and PIM-SM with IGMP Version 3 and PIM-SSM. Use the following descriptions to create translation table entries.

Parameter:	**Group Address**
Path:	Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Translation Table > **Add**
Default:	Null
Options:	IGMP group address in the SSM range
Function:	Specifies the IGMP group for which the table specifies one or more source addresses that this group will receive multicast data from.
Instructions:	Enter the IGMP group address. The address must be in the SSM range.
MIB Object ID:	99999.1099.2

Parameter: **Translation Source List**

Path: Configuration Manager > Protocols > IP > IGMP/IGMP Relay > Translation Table > **Add**

Default: Null

Options: IP addresses of sources for the specified group address

Function: Specifies a list of source IP addresses for the IGMP group. These addresses will supply multicast data to the specified IGMP group.

Instructions: Enter up to 64 source addresses in dotted-decimal notation. You should enter addresses in ascending order. Duplicate addresses are not allowed.

MIB Object ID: 99999.1099.3

IGMP Static Forwarding Policy Parameters

The following descriptions for setting IGMP static forwarding policy parameters supersede those shown in *Configuring IP Multicasting and Multimedia Services*. Use these parameters to specify multicast groups and sources for IGMP static forwarding policies.

Parameter: **Groups**

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: An empty list

Options: Leave empty or specify one or more groups.

Function: Identifies which multicast host groups match this policy.

Instructions: If you want this filter to match all multicast host groups, do not enter a value in the Groups field.

To match specific groups, click in the parameter field. Then, click on the List button and complete the following fields:

Group: Enter the IP address (or range of addresses) for the group.

Mask: Enter the subnet mask for the group address (or range of addresses).

Match Criteria: Select Exact to match only the group with the specified address and mask, or select Range to match all groups in the specified range of group addresses and masks.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.5

Parameter: Sources

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP > Static Forwarding Entries

Default: An empty list

Options: Leave empty or specify one or more multicast sources.

Function: Identifies which multicast sources match this policy.

Instructions: If you want this filter to match all multicast sources, do not enter a value in the Sources field.

To specify a particular multicast source (or range of sources), click in the parameter field. Then, click on the List button and complete the following fields:

Source Address: Enter the IP address of the device (or devices) sending the multicast data.

Source Mask: Enter the subnet mask for the source address (or range of addresses).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.20.1.10

IP Global Parameters

You use the following parameter to disable directed broadcast.

Parameter: Directed Broadcast

Path: Configuration Manager > Protocols > IP > Global

Default: Enable

Options: Enable | Disable

Function: When this parameter is enabled, a packet addressed to an IP broadcast address goes to all systems on the target network. By default, directed broadcast is enabled.

Caution: Internet service providers have reported forged ICMP echo request packets sent to IP addresses (SMURF attacks), sometimes resulting in severe network congestion. To prevent these attacks, directed broadcast must be disabled.

Instructions: Accept the default, Enable, if you want the directed broadcast feature to be enabled. Set to Disable if you want directed broadcast to be disabled.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.1.28

You use the following parameter to enable or disable ICMP ECHO request.

Parameter: Icmp Echo Request Unique Id

Path: Configuration Manager > Protocols > IP > Global

Default: Disable

Options: Enable | Disable

Function: When this parameter is enabled, a unique identifier is added to each ICMP echo request message.

Instructions: Accept the default, Disable, if you do not want to add unique identifiers to ICMP echo requests. Set to Enable if you want to add unique identifiers to ICMP echo requests.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.1.31

You use the following parameter to specify the maximum number of equal-cost multipath support on the router.

Parameter: IP OSPF Maximum Path

Path: Configuration Manager > Protocols > IP > Global

Default: 1

Options: 1 to 5

Function: Specifies the maximum number of equal cost paths allowed for a network installed by OSPF.

Instructions: Use the IP global Multipath Method parameter to enable multipath costs and specify the method that IP uses to choose the next hop for a datagram.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.1.21

You use the following parameter to set the IP global parameter Multiple Nexthop Calculation Method, which has been revised to support PIM-SSM.

Parameter: Multiple Nexthop Calculation Method

Path: Configuration Manager > Protocols > IP > Global

Default: Disable

Options: Disable | Round Robin | Source Destination Hash | Destination Hash | Multicast Only

Function: Enables and disables equal-cost multipath support for RIP, OSPF, and PIM-SSM and specifies the method that IP uses to choose the next hop when more than one is available. Set this parameter as required. (You can select any method to enable ECMP support for PIM-SSM; multicast ECMP always uses the source destination hash method for PIM-SSM forwarding table entries.)

- Round Robin: IP forwards each packet to a different next hop until it reaches the last of the available next hops, then it repeats the sequence. Round-robin distribution attempts to make full use of available resources but may cause packets to be delivered out of order.
- Source Destination Hash: IP forwards all packets with a given source and destination address to the same next hop. This method increases the chances that the packets will be delivered in order. This forwarding algorithm is compatible with RIP and OSPF and with PIM-SSM.
- Destination Hash: IP forwards all packets with the same destination address to the same next hop. This forwarding algorithm is compatible with RSVP.
- Multicast Only: ECMP is disabled for unicast forwarding, and the configured equal-cost paths are used for PIM-SSM forwarding only. ECMP enables PIM-SSM to choose different forwarding paths for different (source, group) pairs. These forwarding paths are multicast table manager (MTM) entries with different incoming or outgoing interfaces.

Instructions: Click on Values and select the appropriate setting. For unicast ECMP, configure RIP and OSPF to support equal-cost routes to the same destination. For PIM-SSM, you must also enable the Source-Specific Multicast and Equal Cost Multicast parameters on the PIM Global Configuration screen.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.1.18

IP Interface Parameter

You use the following parameter to enable or disable IP payload compression over a GRE tunnel. (This parameter is available only for the logical IP interface configured on GRE tunnels.)

Parameter:	**IP Payload Compression**
Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables IP payload compression and decompression on the logical IP interface configured on a GRE tunnel. The compressed data is sent over the GRE tunnel.
Instructions:	Specify Enable to enable IP payload compression and decompression on the IP interface of the GRE tunnel; specify Disable to disable IP payload compression and decompression on the IP interface of the GRE tunnel.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.24.1.65

NAT Global Parameter

The following parameter was used when upgrading from a pre-14.20 NAT configuration to a Version 14.20 or greater BayRS software version. This parameter should be set to Enable.

Parameter:	**Install Private Address**
Path:	Configuration Manager > Protocols > IP > NAT > Global
Default:	Enable
Options:	Enable | Disable
Function:	This parameter was added in BayRS Version 14.20 to address a compatibility issue concerning non-DNS NAT translations when upgrading a pre-14.20 NAT configuration to a Version 14.20 or greater BayRS software version. This parameter should be set to Enable. Disabling this parameter can cause unpredictable results.
Instructions:	Accept the default, Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.7.1.18

OSPF Global Parameter

Use the following parameter to enable RFC 3101 forwarding address compatibility for an OSPF NSSA.

Parameter:	**Rfc 3101 Compatibility Enable**
Path:	Configuration Manager > Protocols > IP > OSPF/MOSPF > Global
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables RFC 3101 forwarding address compatibility for the OSPF NSSA. The setting for this parameter takes effect after restarting OSPF globally.
Instructions:	Set to Enable if you want to use the forwarding address functionality and specify an ASE forwarding address for type 7 link state advertisements (LSAs). If this parameter is not enabled, any forwarding address specified in the NSSA Forward Address parameter is ignored.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.3.1.37

OSPF Area Parameter

Use the following parameter to specify the autonomous system external (ASE) forwarding address of the type 7 NSSA link state database (LSDB).

Parameter:	**NSSA Forward Address**
Path:	Configuration Manager > Protocols > IP > OSPF/MOSPF > Areas
Default:	None
Options:	Any valid IP address in the network
Function:	Specifies the forwarding address for type 7 link state advertisements (LSAs).
Instructions:	Enter the IP address of the interface to be used as the ASE forwarding address. To use this parameter, you must first set the NSSA Originate Def Route parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.3.2.1.16

OSPF/RIP Announce Policy Parameter

You use the following parameter to specify one or more BGP peers for an OSPF or RIP announce policy.

Parameter:	**From BGP Peer**
Path:	Configuration Manager > Protocols > IP > Policy Filters > RIP > Announce Policies
Path:	Configuration Manager > Protocols > IP > Policy Filters > OSPF > Announce Policies
Default:	An empty list
Options:	A list of IP addresses
Function:	Specifies the BGP router ID of the peer. To verify the router ID of the BGP peer, on the peer router, check the configured value for the Site Manager BGP Global parameter, BGP Identifier, or the BCC BGP parameter, router-id. This policy applies to BGP advertisements authored by a router on this list, and applies only to BGP-sourced routes when BGP is included as a route source.
Instructions:	Click in the From BGP Peer field and then click on the List button. Specify one or more IP addresses. Use the default empty list to indicate that this policy applies to BGP advertisements from any router.
MIB Object ID:	RIP: 1.3.6.1.4.1.18.3.5.3.2.6.2.1.19
MIB Object ID:	OSPF: 1.3.6.1.4.1.18.3.5.3.2.6.4.1.19

PIM Global Parameters

This section provides descriptions for new and changed PIM global configuration parameters that support PIM-SSM.

Parameter: Source-Specific Multicast

Path: Configuration Manager > Protocols > IP > PIM > Global
Default: Disable
Options: Enable | Disable
Function: Enables and disables source-specific multicast (SSM) on a router running PIM.
Instructions: Enable or disable SSM mode for PIM.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.37

Parameter: Equal Cost Multipath

Path: Configuration Manager > Protocols > IP > PIM > Global
Default: Disable
Options: Enable | Disable
Function: Enables and disables ECMP for PIM-SSM.
Instructions: Enable or disable ECMP for PIM-SSM. If you enable ECMP, configure the global IP configuration parameters Multiple Nexthop Calculation Method (see page A-49), IP OSPF Maximum Path, and RIP Maximum Equal Cost Paths.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.38

Parameter: **Info/Warnings**

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 | PIM modules for which you want to log info/warning messages

Function: Enables or disables the logging of PIM informational and warning messages on the PIM router.

Instructions: To disable logging of PIM informational and warning messages, accept the default value, 0. To enable logging of these messages, click on Values and select the PIM modules for which you want to log info/warning messages. The modules that you select are represented as bits values in the parameter field, as follows:

0x00000001 — Bootstrap procedure
0x00000002 — Hello procedure
0x00000004 — Join/prune send procedure
0x00000008 — Registration procedure
0x00000010 — Maintaining PIM route table
0x00000020 — Assert procedure
0x00000040 — Data forwarding/tree switching
0x00000080 — PIM main gate processing
0x00000100 — PIM Cct gate general processing
0x00000200 — PIM route change processing
0x00000400 — PIM (*,G) processing
0x00000800 — PIM pte/oif timers
0x00001000 — PIM/MTM signals/messages
0x00002000 — PIM-PIM messages
0x00004000 — PIM protocol messages/first data
0x00008000 — Join/prune received
0x00010000 — PIM utilities including timers
0x00020000 — PIM-SSM related messages

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.4

Parameter: Debug

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 | PIM modules for which you want to log PIM debug messages

Function: Enables or disables the logging of PIM debugging messages on the PIM router.

Instructions: To disable logging of PIM debug messages, accept the default value, 0. To enable logging of these messages, click on Values and select the PIM modules for which you want to log debug messages. The modules that you select are represented as bits values in the parameter field, as follows:

0x00000001 — Bootstrap procedure
0x00000002 — Hello procedure
0x00000004 — Join/prune send procedure
0x00000008 — Registration procedure
0x00000010 — Maintaining PIM route table
0x00000020 — Assert procedure
0x00000040 — Data forwarding/tree switching
0x00000080 — PIM main gate processing
0x00000100 — PIM Cct gate general processing
0x00000200 — PIM route change processing
0x00000400 — PIM (*,G) processing
0x00000800 — PIM pte/oif timers
0x00001000 — PIM-MTM signals/messages
0x00002000 — PIM-PIM messages
0x00004000 — PIM protocol messages/first data
0x00008000 — Join/prune received
0x00010000 — PIM utilities including timers
0x00020000 — PIM-SSM related messages
0x00040000 — PIM debug option for ip pim_fwd

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.5

Parameter: Trace

Path: Configuration Manager > Protocols > IP > PIM > Global

Default: 0

Options: 0 | PIM modules for which you want to log PIM trace messages

Function: Enables or disables the logging of PIM trace messages on the PIM router.

Instructions: To disable logging of PIM trace messages, accept the default value, 0. To enable logging of these messages, click on Values and select the PIM modules for which you want to log trace messages. The modules that you select are represented as bits values in the parameter field, as follows:

0x00000001 — Bootstrap procedure
0x00000002 — Hello procedure
0x00000004 — Join/prune send procedure
0x00000008 — Registration procedure
0x00000010 — Maintaining PIM route table
0x00000020 — Assert procedure
0x00000040 — Data forwarding/tree switching
0x00000080 — PIM main gate processing
0x00000100 — PIM Cct gate general processing
0x00000200 — PIM route change processing
0x00000400 — PIM (*,G) processing
0x00000800 — PIM pte/oif timers
0x00001000 — PIM-MTM signals/messages
0x00002000 — PIM-PIM messages
0x00004000 — PIM protocol messages/first data
0x00008000 — Join/prune received
0x00010000 — PIM utilities including timers
0x00020000 — PIM-SSM related messages

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.1.6

PIM Interface Parameters

You use the following parameter to determine whether the router interface will act as a PIM bootstrap border interface.

Parameter: **Bootstrap Border**

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: Disable

Options: Disable | Enable

Function: When you set this parameter to Enable, this PIM interface acts as a PIM bootstrap border interface. A bootstrap border interface discards both incoming and outgoing bootstrap messages. Incoming messages originate from other PIM routers; outgoing messages originate from other PIM interfaces on the same router. When you set this parameter to Disable, this interface operates in accordance with RFC 2362; it accepts incoming messages and forwards outgoing ones.

Instructions: Set to Enable if you want the interface to discard incoming and outgoing bootstrap messages. Accept the default, Disable, if you want the interface to accept incoming messages and forward outgoing messages.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.32

Parameter: **Outgoing Interface Deletion Delay**

Path: Configuration Manager > Protocols > IP > PIM > Interface

Default: 5

Options: 1 through 210

Function: Specifies the number of seconds that the router waits before deleting an outgoing PIM interface after it receives a prune message from a downstream neighbor. You may need to change the default value of this parameter if the BayRS router is on a LAN with routers that implement the override-interval and LAN-delay (specified in the new PIMv2 draft). In such a configuration, this parameter should be set to a value larger than the sum of the override-interval plus the LAN-delay configured on the other routers.

Instructions: Specify the number of seconds that the router should wait before deleting an outgoing interface after it receives a prune message.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.14.2.1.33

PIM Static RP Parameters

You use the following parameters to designate static rendezvous-point (RP) routers for use with PIM-SM.

Parameter: RP Address

Path: Configuration Manager > Protocols > IP > PIM > Static RP
Default: Null
Options: IP address
Function: Specifies the IP address of a statically configured RP router. PIM uses this IP address to map a group to the RP.
Instructions: Specify the IP address for the RP in dotted-decimal notation.
MIB Object ID: 99999.666.4

Parameter: Group Address

Path: Configuration Manager > Protocols > IP > PIM > Static RP
Default: Null
Options: Multicast IP address
Function: Specifies the IP address of the multicast group. PIM maps the configured group to the RP address.
Instructions: Specify the multicast group address in dotted-decimal notation.
MIB Object ID: 99999.666.5

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IP > PIM > Static RP
Default: None
Options: 4 through 32
Function: Specifies the prefix length for the specified multicast group address.
Instructions: Specify a prefix length from 4 through 32.
MIB Object ID: 99999.666.6

Parameter: **Priority**

Path: Configuration Manager > Protocols > IP > PIM > Static RP

Default: None

Options: 0 through 255

Function: Specifies the priority for the static RP. PIM elects a static RP based first on highest priority, then on the highest hash value.

Instructions: Specify the priority for this static RP.

MIB Object ID: 99999.666.7

PPP Interface Parameters

Use the following parameters to configure the PPP interface parameters associated with the RFC 2686, “Multi-Class Extension to Multi-Link PPP” feature for BayRS. For information on configuring other PPP interface parameters, see *Configuring PPP Services*.

Parameter: **Multilink MultiClass Enable**

Path: Protocols > PPP > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables Multilink Multiclass (RFC 2686) for this interface. This parameter is active only for Multilink.

Instructions: To start Multilink Multiclass on the selected interface, set this parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.82

Parameter:	**Maximum Number of Classes**
Path:	Protocols > PPP > Interfaces
Default:	6
Options:	6
Function:	Specifies the maximum number of classes that may be received or transmitted. This parameter is active only for Multilink Multiclass.
Instructions:	This parameter is preset to 6. It is displayed for reference only and cannot be changed.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.83

PPP Multilink Multiclass Classes Parameter

Use the following guidelines to configure the Multilink Multiclass PPP Classes parameter. (In the path name given, **bold** text indicates that you access the PPP Multiclass Classes window by clicking on the Classes button on the PPP Interface List window.

Parameter:	**Fragment Size**
Path:	Protocols > PPP > Interfaces > **Classes**
Default:	80
Options:	A value from 64 up to the maximum transmission unit for the circuit.
Function:	Specifies the minimum size of a packet that Multilink will fragment for this class. This parameter is active only for Multilink Multiclass.
Instructions:	Accept the default value or specify the required minimum packet size.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.6.1.3

PPP Line Parameter

Use the following guidelines to configure the PPP Line parameter associated with the RFC 2686, "Multi-Class Extension to Multi-Link PPP," feature for BayRS. (In the path name given, **bold** text indicates that you access the PPP Line Lists window by clicking on the Lines button on the PPP Interface Lists window.) For information about configuring other PPP line parameters, see *Configuring PPP Services*.

Parameter: **Multilink Multiclass for Dialup**

Path: Protocols > PPP > Interfaces > **Lines**

Default: Disable

Options: Enable | Disable

Function: Enables or disables multilink multiclass (RFC 2686) for this line. This parameter is active only for multilink on dial-up connections and applies only to incoming calls.

Instructions: To activate multilink multiclass on this dialup line, set this parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.51

QLLC Mapping Table Configuration Parameter

You use the following parameter to enable or disable the XID Retry feature.

Parameter: **XID Retry**

Path: Configuration Manager > Circuits > Edit Circuits > Edit > X.25 Protocol > Service > QLLC

Default: Disable

Options: Enable | Disable

Function: Allows the QLLC service to retransmit the XID3 every 10 seconds to the QLLC endstation until it receives a response. This ensures that the endstation will receive the XID3 and establish a connection.

Instructions: Set this parameter to Enable to have QLLC retransmit the XID3 every 10 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.4.8.1.19

RADIUS Access Control Parameters

You use the following parameters to modify router access.

Parameter: User Manager Lock

Path: Configuration Manager > Protocols > Global Protocols > RADIUS > Access Control

Default: Disabled

Options: Enable | Disable

Function: Allows you to modify access to the router by enabling or disabling the user/manager lock.

Instructions: Set to Enable to lock out the user and manager profile and allow access only by individual users with a unique profile. Accept the default value, Disable, to allow access by all users with the manager or user profile, in addition to users with a unique profile.

Note: If the user/manager lock is enabled and the RADIUS server becomes unavailable, the message "RADIUS wait state" appears in the User Manager Lock field. When the RADIUS server becomes available, the value reverts to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.22.1.10

Parameter: Login Accounting

Path: Configuration Manager > Protocols > Global Protocols > RADIUS > Access Control

Default: Disable

Options: Enable | Disable

Function: Enables or disables login accounting.

Instructions: Set to Enable if you want RADIUS Accounting messages to be sent to the RADIUS server. Accept the default value, Disable, to prevent RADIUS accounting messages from being sent to the server.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.22.1.11

RADIUS Client Parameters

You use the following parameters to configure a RADIUS client. This section replaces “Client IP Address Parameter” in Appendix A of *Configuring RADIUS*.

Parameter: Authentication

Path: Configuration Manager > Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**

or

Configuration Manager > Protocols > Global Protocols > RADIUS > Edit RADIUS

Default: Disable

Options: Enable | Disable

Function: Enables or disables the RADIUS client on the gateway.

Instructions: Set to Enable to activate the RADIUS client on the router. Accept the default value, Disable, to deactivate RADIUS authentication.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.2

Parameter: Accounting

Path: Configuration Manager > Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**

or

Configuration Manager > Protocols > Global Protocols > RADIUS > Edit RADIUS

Default: Disable

Options: Enable | Disable

Function: Enables or disables RADIUS accounting.

Instructions: Set to Enable to activate RADIUS accounting. Accept the default value, Disable, to deactivate RADIUS accounting.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.3

Parameter: Client IP Address

Path: Configuration Manager > Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**
or
Configuration Manager > Protocols > Global Protocols > RADIUS > Edit RADIUS > **Edit**

Default: None

Options: A 32-bit IP address

Function: Identifies the RADIUS client. This address applies to the entire router.

Instructions: Enter the IP address of the router. If the RADIUS server is already configured, Site Manager automatically supplies the address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.5

Parameter: Debug Message Level

Path: Configuration Manager > Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**
or
Configuration Manager > Protocols > Global Protocols > RADIUS > Edit RADIUS

Default: NODEBUG

Options: ONE | TWO | THREE | NODEBUG

Function: Assigns the level of RADIUS debug messages that the RADIUS client logs.

Instructions: Accept the default value, NODEBUG, unless you are specifically trying to debug the connection.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.7

RIP Parameter

You use the following parameter to specify whether the router imports RIP-1 updates only, RIP-2 updates only, or both RIP-1 and RIP-2 updates from a neighbor router.

Parameter: RIP Compatible

Path: Configuration Manager > Protocols > IP > RIP Interfaces

Default: Disabled

Options: Enable | Disable

Function: Specifies whether RIP-1 accepts both RIP-1 broadcast and RIP-2 multicast packets (and have RIP-2 always use multicast for transmitting updates), or whether RIP-1 accepts RIP-1 broadcast and RIP-2 broadcast packets only (RIP-1 will not accept RIP-2 multicast packets) and have RIP-2 broadcast the packets, making it compatible with RIP-1.

Instructions: Accept the default, Disable, if you want RIP-1 to accept both RIP-1 broadcast and RIP-2 multicast packets. Select Enable if you want RIP-1 to accept RIP-1 broadcast and RIP-2 broadcast packets only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.2.2.1.22

VRRP Parameter

You use the following parameter to enable or disable the VRRP ping feature.

Parameter: VRRP Address Ping

Path: Configuration Manager > Protocols > Global Protocols > IP > VRRP

Default: Disable

Options: Enable | Disable

Function: Allows you to ping a master virtual router that is not the owner of the virtual router IP address. This feature is useful for checking network connectivity.

Instructions: Set to Enable to allow the router to ping a master virtual router that is not the owner of the virtual router IP address. Accept the default, Disable, to prevent that master virtual router from responding to a ping. When this feature is disabled, VRRP is in full compliance with RFC 2338.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.25.1.1.15

X.25 Network Service Record Parameter

You use the following parameter to enable or disable the No Calling Address feature.

Parameter: No Calling Address

Path: Configuration Manager > Circuits > Edit Circuits > Choose an Interface > Edit > X25 Protocol > Service

Default: Off

Options: On | Off

Function: Allows the router to accept incoming X.25 calls for QLLC service from devices that do not have an X.121 calling address. Only one X.25 connection can be supported at any given time.

Instructions: Set this parameter to On to allow the router to accept incoming X.25 calls for QLLC service from devices that do not have an X.121 calling address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.4.2.1.55

Index

Numbers

A

B

C

D

E

F

G

Q

R

S

T

U

V

X