

**Bay Networks**

The Merged Company of SynOptics and Wellfleet

# Configuring Filter Options on Wellfleet Routers

Part No. 110074 A

# Configuring Filter Options on Wellfleet Routers

Router Software Version 8.10  
Site Manager Software Version 2.10

Part No. 110074 Rev. A  
February 1995



**Bay Networks**

The Merged Company of SynOptics and Wellfleet

---

**Copyright © 1995 Bay Networks, Inc.**

All rights reserved. Printed in USA. February 1995.

The information in this document is subject to change without notice. This information is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement or nondisclosure agreement and may only be used in accordance with the terms of that license. The terms of the Software License are provided with the documentation.

**Restricted Rights Legend**

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

**Notice for All Other Executive Agencies**

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

**Trademarks of Bay Networks, Inc.**

ACE, BLN, BN, and Wellfleet are registered trademarks and AFN, AN, ANH, ASN, BCN, BCNX, BLNX, BNX, CN, FN, FRE, LN, PPX, Bay Networks, and the Bay Networks logo are trademarks of Bay Networks, Inc.

**Third-Party Trademarks**

3Com is a registered trademark of 3Com Corporation.

AIX, NetView, and IBM are registered trademarks of International Business Machines Corporation.

AppleTalk and EtherTalk are registered trademarks of Apple Computer, Inc.

AT&T and ST are registered trademarks of American Telephone and Telegraph Company.

DEC, DECnet, VAX, and VT100 are trademarks of Digital Equipment Corporation.

Distinct is a registered trademark and Distinct TCP/IP is a trademark of Distinct Corporation.

Fastmac and MADGE are trademarks of Madge Networks, Ltd.

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

HP is a registered trademark of Hewlett-Packard Company.

Intel is a registered trademark of Intel Corporation.

IPX, NetWare, and Novell are registered trademarks of Novell, Inc.

MCI is a registered trademark of MCI Communications Corporation.

Microsoft, MS, and MS-DOS are registered trademarks and Windows is a trademark of Microsoft Corporation.

Motif and OSF/Motif are registered trademarks of Open Software Foundation, Inc.

Motorola is a registered trademark of Motorola, Inc.

NetBIOS is a trademark of Micro Computer Systems, Inc.

Open Look and UNIX are registered trademarks of UNIX System Laboratories, Inc.

Sun and Solaris are registered trademarks and SPARCstation is a trademark of Sun Microsystems, Inc.

VINES is a registered trademark of Banyan Systems Incorporated.

X Window System is a trademark of the Massachusetts Institute of Technology.

Xerox is a registered trademark and XNS is a trademark of Xerox Corporation.

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

---

---

# Bay Networks Software License

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

- 
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
  8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.
  9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
  10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
  11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
  12. Licensee's obligations under this license shall survive expiration or termination of this license.

# Contents

## Chapter 1

### **Inbound Traffic Filters: An Overview**

Using Inbound Traffic Filters .....	1-1
Filter Templates .....	1-3
Creating Templates .....	1-3
Applying a Template to an Interface .....	1-4
Filtering Criteria, Ranges, and Actions .....	1-5
Bridge Criteria and Actions .....	1-6
Predefined Criteria .....	1-7
User-Defined Criteria .....	1-9
Actions .....	1-11
IP Criteria and Actions .....	1-11
Predefined Criteria .....	1-11
User-Defined Criteria .....	1-12
Actions .....	1-13
DECnet Phase IV Criteria and Actions .....	1-13
Predefined Criteria .....	1-13
Actions .....	1-14

VINES Criteria and Actions .....	1-14
Predefined Criteria .....	1-14
User-Defined Criteria .....	1-15
Actions .....	1-16
IPX Criteria and Actions .....	1-16
Predefined Criteria .....	1-16
Actions .....	1-17
XNS Criteria and Actions .....	1-17
Predefined Criteria .....	1-17
Actions .....	1-18
Source Routing Criteria and Actions .....	1-18
Predefined Criteria .....	1-18
User-Defined Criteria .....	1-19
Actions .....	1-20
OSI Criteria and Actions .....	1-21
Predefined Criteria .....	1-21
User-Defined Criteria .....	1-21
Actions .....	1-22
DLSw Criteria and Actions .....	1-23
Predefined Criteria .....	1-23
User-Defined Criteria .....	1-23
Actions .....	1-24
Specifying User-Defined Criteria .....	1-24

## Chapter 2

### Using the Configuration Manager to Apply Traffic Filters

Displaying the Traffic Filters Window .....	2-2
Preparing Filter Templates .....	2-3
Creating a New Template .....	2-4
Modifying Templates .....	2-6
Copying a Template .....	2-6
Editing a Template .....	2-8
Adding Template Criteria .....	2-10
Deleting Criteria .....	2-13
Deleting Ranges .....	2-13
Modifying a Range .....	2-14
Specifying Template Actions .....	2-16
Adding an Action .....	2-16
Deleting an Action .....	2-18
Creating a Filter .....	2-18
Editing Filters .....	2-20
Specifying Filter Criteria .....	2-23
Adding Criteria .....	2-23
Deleting Criteria .....	2-25
Deleting Ranges .....	2-25
Modifying a Range .....	2-25
Specifying Filter Actions .....	2-27
Adding an Action .....	2-27
Deleting an Action .....	2-28



Deleting Filters .....	2-28
Enabling or Disabling a Filter .....	2-29
Applying Filter Precedence .....	2-30

## Chapter 3

### **Protocol Prioritization and Outbound Filters: An Overview**

Protocol Prioritization and Outbound Filters .....	3-1
Why You Would Use Protocol Prioritization .....	3-2
Example of Protocol Prioritization .....	3-3
How Protocol Prioritization Works .....	3-5
Dequeuing Algorithms .....	3-5
Bandwidth Allocation Algorithm .....	3-6
Strict Dequeuing Algorithm .....	3-8
Tuning Protocol Prioritization for Your Network .....	3-10
Queue Depth .....	3-10
Latency .....	3-12
Priority Filters .....	3-13
Creating Templates .....	3-14
Adding a Filter to an Interface .....	3-14
Filtering Criteria, Ranges, and Actions .....	3-15
Datalink, IP, and User-Defined Criteria .....	3-16
Datalink Predefined Criteria .....	3-17
IP Predefined Criteria .....	3-18
User-Defined Criteria .....	3-19
Example of User-Defined Filter .....	3-23

Implementation Notes .....	3-24
IP and Datalink Filters for Common Criteria .....	3-24
Protocol Prioritization, Outbound Filters, and Dial Backup .....	3-24
Prioritizing LAT Traffic .....	3-25
Prioritizing Telnet Traffic .....	3-25
Prioritizing RIP Traffic .....	3-25
Prioritizing OSPF Traffic .....	3-26
Prioritizing OSPF/BGP Traffic .....	3-26
Prioritizing Spanning Tree Traffic .....	3-26
Prioritizing Native Source Routed Bridge Traffic .....	3-26
Prioritizing IP Encapsulated Source Routed Bridge Traffic .....	3-27
Prioritizing Source Routed SNA Traffic .....	3-27

## Chapter 4

### Using the Configuration Manager to Configure Priority Filters

Configuring Priority Filters .....	4-1
Displaying the Priority/Outbound Filters Window .....	4-2
Preparing Filter Templates .....	4-4
Creating a New Template .....	4-5
Copying a Template .....	4-7
Editing a Template .....	4-8
Creating a Filter .....	4-15
Editing Priority Filter Criteria, Ranges, and Actions .....	4-16
Adding Criteria .....	4-16
Modifying Ranges .....	4-18
Adding Actions .....	4-18
Deleting Criteria, Ranges, and Actions .....	4-19

Applying Filter Precedence .....	4-20
Enabling or Disabling a Priority Filter .....	4-22
Deleting a Priority Filter .....	4-23
Editing Protocol Prioritization Parameters .....	4-24
Priority Interface Parameter Descriptions .....	4-25

## Index

## Figures

Figure 1-1. Headers of Encapsulation Methods Supported by Bridge Filters .....	1-7
Figure 1-2. Add User-Defined Field Window .....	1-25
Figure 1-3. VINES Header .....	1-26
Figure 2-1. Selecting the Traffic Filters Menu .....	2-2
Figure 2-2. Filters Window .....	2-3
Figure 2-3. Filter Template Management Window .....	2-4
Figure 2-4. Create Template Window .....	2-5
Figure 2-5. Copy Filter Template Window .....	2-7
Figure 2-6. Edit Filter Template Window .....	2-9
Figure 2-7. Selecting a Filter Criterion .....	2-10
Figure 2-8. Add Range Window .....	2-11
Figure 2-9. Criteria List with Range Added .....	2-12
Figure 2-10. Deleting a Filter Criterion .....	2-13
Figure 2-11. Deleting a Range .....	2-14
Figure 2-12. Modify a Range .....	2-15
Figure 2-13. Choosing the Drop Action .....	2-16
Figure 2-14. Actions List with New Action .....	2-17
Figure 2-15. Deleting an Action .....	2-18
Figure 2-16. Create Filter Window .....	2-19
Figure 2-17. New Filter Listed in Scroll Box .....	2-20
Figure 2-18. Edit Filters Window .....	2-22
Figure 2-19. Adding a Filter Criterion .....	2-23
Figure 2-20. Add Range Window .....	2-24
Figure 2-21. Modifying a Range .....	2-26
Figure 2-22. Choosing the Drop Action .....	2-27

Figure 2-23. Enabling or Disabling a Filter .....	2-29
Figure 2-24. Example Result of Applying Filter Precedence .....	2-31
Figure 2-25. Filters Appearing in the Order of Precedence .....	2-33
Figure 2-26. Change Precedence Window .....	2-34
Figure 3-1. Applying a Priority Filter in a Sample Network .....	3-4
Figure 3-2. Allotting High-Priority Status to LAT and Telnet Traffic .....	3-4
Figure 3-3. Relationship between Priority Transmit Queues .....	3-5
Figure 3-4. Bandwidth Allocation Dequeuing Algorithm .....	3-7
Figure 3-5. Strict Dequeuing Algorithm .....	3-9
Figure 3-6. Sample Statistics for the Priority Queues .....	3-11
Figure 3-7. Datalink Reference Points on an IEEE 802.3 LLC Header .....	3-20
Figure 3-8. Datalink Reference Points on a Source Routing Packet Bridged over Frame Relay.....	3-21
Figure 3-9. IP Reference Points on a PPP Packet with IP Encapsulated Source Routing .....	3-22
Figure 3-10. VINES Header .....	3-23
Figure 4-1. Selecting Protocol Priority from Protocols List .....	4-2
Figure 4-2. Selecting the Priority/Outbound Filters Window .....	4-3
Figure 4-3. Priority/Outbound Filters Window .....	4-3
Figure 4-4. Filter Template Management Window .....	4-4
Figure 4-5. Create Priority/Outbound Template Window .....	4-6
Figure 4-6. Copy Filter Template Window .....	4-8
Figure 4-7. Edit Priority/Outbound Template Window .....	4-9
Figure 4-8. Add Range Window .....	4-10
Figure 4-9. Prioritization Length Window .....	4-12
Figure 4-10. Create Filter Window .....	4-15
Figure 4-11. Edit Priority/Outbound Filters Window .....	4-17

Figure 4-12. Sample List of Priority Filters .....	4-20
Figure 4-13. Change Precedence Window .....	4-21
Figure 4-14. Example of Priority Filter Order Change .....	4-22
Figure 4-15. Filter Enable/Disable Values Selection .....	4-23
Figure 4-16. Edit Protocol Priority Interface Window .....	4-24

## Tables

Table 1-1. Bridge-Supported Encapsulation/Media Matrix .....	1-8
Table 1-2. Predefined Criteria for Bridge Filters .....	1-8
Table 1-3. Reference, Offset, and Length of Common Bridge Criteria .....	1-9
Table 1-4. Reference, Offset, and Length of Ethernet Encapsulation Criteria .....	1-10
Table 1-5. Reference, Offset, and Length of 802.2 Encapsulation Criteria .....	1-10
Table 1-6. Reference, Offset, and Length of SNAP Encapsulation Criteria .....	1-10
Table 1-7. Reference, Offset, and Length of IP Filtering Criteria .....	1-12
Table 1-8. Reference, Offset, and Length of DECnet Filtering Criteria .....	1-14
Table 1-9. Reference, Offset, and Length of VINES Filtering Criteria .....	1-15
Table 1-10. Reference, Offset, and Length of IPX Filtering Criteria .....	1-16
Table 1-11. Reference, Offset, and Length of XNS Filtering Criteria .....	1-17
Table 1-12. Reference, Offset, and Length of Source Routing Filtering Criteria .....	1-20
Table 1-13. Reference, Offset, and Length of OSI Filtering Criteria .....	1-22
Table 1-14. Reference, Offset, and Length of DLSw Filtering Criteria .....	1-24
Table 3-1. Maximum Number of Packets Queued to Achieve 250-ms Latency .....	3-13
Table 3-2. Predefined Criteria for Datalink Header .....	3-17
Table 3-3. Predefined Filter Criteria for IP Traffic .....	3-18

Table 3-4. Datalink Reference Points .....3-20

Table 3-5. IP Reference Points .....3-22

Table 3-6. Reference, Offset, and Length Values .....3-23

---

# About This Guide

If you are responsible for configuring filter options on Wellfleet<sup>®</sup> routers, you need to read this guide. It provides

- An overview of inbound traffic filters
- Instructions on configuring inbound filters
- An overview of outbound filters and protocol prioritization
- Instructions on configuring protocol prioritization and outbound filters

## Before You Begin

Before using this guide, you must complete the following procedures:

1. Install the router hardware. For instructions, refer to one of the following:
  - *Installing and Maintaining BN Routers*
  - *Installing and Maintaining ASN Routers*
  - *Installing and Starting AN Routers*
  - *Installing and Starting 8-Port Access Node Hub (ANH) Systems*
  - *Installing and Maintaining FN, LN, CN, AFN, and ALN Routers*
  - *Installing the DC Version of the BLN-2 and BCN*



2. Connect the router to a network and create a pilot configuration file. For instructions, refer to one of the following:
  - *Quick-Starting Wellfleet Routers*
  - *Administering Networks for AN and ASN Routers*
3. Make sure you are running the latest version of Wellfleet Site Manager and router software. For instructions, refer to one of the following:
  - *Upgrading Wellfleet Routers from Version 7-8.00 to Version 8.10*
  - *Upgrading Wellfleet Routers from Version 5 to Version 8.10*

## How to Get Help

For additional information or advice, contact the Bay Networks Help Desk in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-0052

## 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 command syntax is <b>ping</b> < <i>ip_address</i> >, you enter <b>ping 192.32.10.12</b>
arrow character (→)	Separates menu and option names in instructions. Example: Protocols→AppleTalk identifies the AppleTalk option in the Protocols menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
<b>user entry text</b>	Denotes text that you need to enter. Example: Start up the Windows environment by entering the following after the prompt: <b>win</b>
<b>command text</b>	Denotes command names in text. Example: Use the <b>xmodem</b> command.
<i>italic text</i>	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
screen text	Indicates data that appears on the screen. Example: Set Bay Networks Trap Monitor Filters
ellipsis points	Horizontal (. . .) and vertical (: :) ellipsis points indicate omitted information.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
vertical line ( )	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is <b>show at routes   nets</b> , you enter either <b>show at routes</b> or <b>show at nets</b> , but not both.

## Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CMIP	Common Management Information Protocol
EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Interface
IEEE	Institute of Electrical and Electronic Engineers
ILI	intelligent link interface
IS-IS	Intermediate System to Intermediate System
MAC	media access control
MOP	Maintenance Operations Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PVCs	permanent virtual circuits
QENET	Quad Ethernet Link Module
RIP	Routing Information Protocol
SMDS	Switched Multimegabit Data Services
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SRM	system resource modules
SVCs	switched virtual circuits
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TTRT	target token rotation time
VC	virtual connection
VINES	Virtual Networking System (Banyan)
XB	Translation Bridge

---

# Chapter 1

## Inbound Traffic Filters: An Overview

This chapter describes the following:

- Inbound traffic filters
- Filter templates
- Predefined criteria, ranges, and actions specific to each protocol
- Criteria that you specify (user-defined criteria)

You should read this chapter if you are responsible for configuring traffic filters for your network. If you are already familiar with the implementation of traffic filters in Configuration Manager, and with the criteria and actions associated with the protocols for which you want to create filters, you can go directly to Chapter 2, “Using the Configuration Manager to Apply Traffic Filters.”

For information on prioritizing protocols and on outbound filters, see Chapter 3, “Protocol Prioritization and Outbound Filters: An Overview,” and Chapter 4, “Using the Configuration Manager to Configure Priority Filters.”

### Using Inbound Traffic Filters

Traffic filters enable a router to selectively relay, drop, or log a packet, frame, or datagram based on standard protocol fields or user-defined fields (*criteria*).

Inbound traffic filters apply to incoming traffic; they are used primarily for security. For example, suppose a company wants only certain people to be able to access its financial network; the company can construct a filter denying everyone access to the financial network except for those people.

All filters are created from templates (files that hold the filtering information), and consist of the following three components:

- **Criteria**  
Part of a frame, packet, or datagram header that you specify to be examined on each incoming frame.
- **Ranges**  
Numeric values (usually addresses) that further specify filtering criteria.
- **Actions**  
What happens to those incoming packets that match a filter's criteria and ranges.

Each filter is associated with a particular protocol and router circuit (*interface*). Configuration Manager supports traffic filters in the following protocols:

- Bridge
- IP
- DECnet™ Phase IV
- VINES®
- Source Routing
- IPX®
- XNS™
- OSI
- DLSw

Each supported protocol allows up to 31 filters per interface. As filters are added to an interface, they are numbered chronologically in the following fashion: rule #1, rule #2, rule #3, and so on.

The order in which you add filters to an interface determines the filter *precedence*. If a packet matches two filters, the filter with the highest precedence applies.

The first filter has the highest precedence and a rule number of 1. Subsequent filters have decreasing precedence. For examples, if two traffic filters apply to a packet, but the first filter on the interface (rule # 1) accepts the packet and the second filter (rule # 2) drops the packet, rule # 1 has precedence and the packet will be accepted. See the section “Applying Filter Precedence” in Chapter 2 for more information.

## Filter Templates

To use traffic filters, it is important to understand the difference between a template and a filter. A traffic filter *template* is a reusable, predefined specification for a traffic filter. You create a *traffic filter* when you apply (save) a traffic filter template to one or more interface (circuit).

A template contains a complete filter description but is not associated with an interface or circuit. Each filter template file holds specific filtering information (criteria, ranges, and actions).

**Note:** A template contains criteria and actions for *one protocol only*.

## Creating Templates

When creating a template, you first assign a name to the template file. It is a good idea to give each template a one-word descriptive name. For example, if you are building a template that is going to contain filtering information instructing the interface to drop all DECnet Phase IV traffic with a Source Node value of 3, name it *decSnode3*.

After you name a template file, you select the criteria and address ranges for checking packets. You then select the action to impose on packets that match the specified criteria and ranges.

After you specify filtering criteria, ranges, and actions, you save the template file, thus creating a traffic filter template. You can apply a single template to as many interfaces as you want. Once you create a template file, it exists for future use unless you delete it.

For a detailed, step-by-step example of creating a filter template from scratch, follow the procedures in the “Preparing Filter Templates” section in Chapter 2.

## Applying a Template to an Interface

When you want to add a filter to an interface, you have several options:

- ❑ If there is a template that contains the exact filtering instructions that you want for this interface, you can apply (save) that template to this interface.
- ❑ If there is a template that contains filtering instructions similar to what you want, you can copy the template, rename it, and edit it. When you save the changes, you create a new template. You then apply the new template to the appropriate interface.
- ❑ If there is no template containing filtering instructions similar to what you want for this interface, you must create a template from scratch. The section “Preparing Filter Templates” in Chapter 2 describes what to do if there is no existing template similar to what you want.
- ❑ If there is already a filter applied to the interface with filtering instructions similar to what you want, you don’t need to use a filter template. You can edit the existing filter directly (see the section “Editing Filters” in Chapter 2).

Because you create traffic filters on a per-protocol basis, you must become familiar with the specific criteria and actions each protocol uses for filtering. The next section describes criteria, ranges, and actions. If you are already familiar with them, go directly to Chapter 2.

## Filtering Criteria, Ranges, and Actions

As described in the previous section, all filters are created from templates, which consist of these three components:

- Criteria

You select which incoming traffic to filter by specifying part of a packet, frame, or datagram header. The fields for filter criteria are protocol-specific. For example, in the Bridge protocol, you can specify the MAC (media access control) source address as a filtering criterion. This causes each incoming frame's MAC source address to be inspected.

- Ranges

You specify a range of applicable addresses along with filtering criteria to further select traffic. There must be at least one range per criterion. (You specify a minimum and a maximum value for each range. When you enter values, the Configuration Manager assumes the value is a decimal number. To enter a hexadecimal number, you must use the prefix 0x. For example, if you specify the MAC source address as a filtering criterion, you must specify exactly which addresses to filter. If you specify 0x0000A2000001 as the minimum value and 0x0000A2000003 as the maximum value, all incoming packets would be checked to see if their MAC Source Address was between 0x0000A2000001 and 0x0000A2000003, inclusive.)

**Note:** A range can consist of just one value or it can be a set of values. If you want a range of only one value, enter only the minimum value; the system automatically uses the value entered for both the minimum and maximum and sets a range of one value.



□ Action

An action defines what happens to incoming packets that match one of the selected ranges for every criterion in the filter.

Actions are protocol-specific, except for the following three:

— Accept

Specifies that any frame that matches the filter will be accepted.

— Drop

Specifies that any frame that matches the filter will be discarded.

— Log

Specifies that for any frame that matches the filter, an event message will be recorded in the Event Log. The Log action can be combined with any other action; however, it should be used to record abnormal events only. Otherwise, the event log will fill up with filtering messages and thus become useless.

The following sections describe each protocol's predefined filtering criteria and actions.

## Bridge Criteria and Actions

Bridge filters are the most complex because they support multiple encapsulations and media types; you can create Bridge traffic filters to filter a number of predefined filtering criteria. Bridge filters also support user-defined criteria.

You filter Bridge frames based on the header fields within each of the four supported encapsulation methods:

- Ethernet
- IEEE 802.2 logical link control (LLC)
- IEEE 802.2 LLC with SNAP header
- Novell® Proprietary

Figure 1-1 illustrates the header content of each supported encapsulation method.

### Ethernet Header

MAC Destination	MAC Source	length/type
-----------------	------------	-------------

48-bit MAC destination address  
 48-bit MAC source address  
 16-bit length/type is TYPE (> 1518)

### IEEE 802.2 LLC Header

MAC Destination	MAC Source	length/type	DSAP	SSAP	Control
-----------------	------------	-------------	------	------	---------

48-bit MAC destination address  
 48-bit MAC source address  
 16-bit length/type is LENGTH (<1519)  
 8-bit DSAP  
 8-bit SSAP  
 8-bit Control

### IEEE 802.2 LLC w/SNAP Encapsulation

MAC Destination	MAC Source	length/type	DSAP	SSAP	Control	Org. Code	Ether-type
-----------------	------------	-------------	------	------	---------	-----------	------------

48-bit MAC destination address  
 48-bit MAC source address  
 16-bit length/type is LENGTH (<1519)  
 DSAP/SSAP/CTRL is 0xAAAA03  
 24-bit Organizational Code  
 16-bit Ether-type

### Novell Proprietary Encapsulation

MAC Destination	MAC Source	length/type	FF	FF
-----------------	------------	-------------	----	----

48-bit MAC destination address  
 48-bit MAC source address  
 16-bit length/type is LENGTH (<1519)  
 next 16 bits are all ones (part of IPX header)

**Figure 1-1. Headers of Encapsulation Methods Supported by Bridge Filters**

**Note:** Only Ethernet encapsulations support a length/type criterion.

## Predefined Criteria

Each encapsulation method has specific, predefined criteria for filtering frames. Table 1-1 shows the encapsulation support for each physical access medium. Table 1-2 illustrates the predefined filtering criteria for each encapsulation method.

**Note:** Since all frame headers include both a MAC Destination Address and a MAC Source Address field, filtering on these two criteria is possible for *all* Bridge-supported encapsulations.

**Table 1-1. Bridge-Supported Encapsulation/Media Matrix**

Physical Medium	Encapsulation Method			
	Ethernet	802.2	SNAP	Novell
Ethernet/802.3	Yes	Yes	Yes	Yes
FDDI	No	Yes	Yes	No
Point-to-Point	Yes	Yes	Yes	Yes
Token Ring	No	Yes	Yes	No

**Table 1-2. Predefined Criteria for Bridge Filters**

Encapsulation Method	Predefined Criteria
All	MAC Source Address MAC Destination Address
Ethernet	Ethernet type
802.2	Length (Ethernet/802.3 and Point-to-Point only) SSAP DSAP Control
SNAP	Length Protocol ID/Organization code Ethertype

**Note:** There are no additional filtering criteria for Novell®; it allows filtering only on the MAC Source and MAC Destination Address.

## User-Defined Criteria

In addition to basic filtering options, the Bridge lets you filter traffic based upon specified bit patterns contained within either the MAC or the datalink header. When creating a filter with user-defined criteria, you specify the reference, offset, and length of each criterion to describe the location of criteria on incoming packets.

Reference

Positions the filtered bit pattern within the incoming frame. For the Bridge there are two reference points: the first is at the beginning of the MAC header, and the second is at the beginning of the datalink header.

Offset

Positions the filtered bit pattern (measured in bits) within either the MAC or the datalink header.

Length

Specifies the bit length of the filtered criteria.

Tables 1-3 through 1-6 show the reference, offset, and length for the filtering criteria each encapsulation method supports.

**Table 1-3. Reference, Offset, and Length of Common Bridge Criteria**

Field	Reference	Offset	Length
MAC Destination Address	MAC	0	48
MAC Source Address	MAC	48	48

**Table 1-4. Reference, Offset, and Length of Ethernet Encapsulation Criteria**

Field	Reference	Offset	Length
Ethernet type	MAC	96	16

**Table 1-5. Reference, Offset, and Length of 802.2 Encapsulation Criteria**

Field	Reference	Offset	Length
Length	MAC	96	16
DSAP	DATA_LINK	0	8
SSAP	DATA_LINK	8	8
Control	DATA_LINK	16	8

**Table 1-6. Reference, Offset, and Length of SNAP Encapsulation Criteria**

Field	Reference	Offset	Length
Length	MAC	96	16
Protocol ID/Organization Code	DATA_LINK	24	24
Ethertype	DATA_LINK	48	16

After specifying the reference, offset, and length of your criterion, you specify one or more range. For more information, see the section “Specifying User-Defined Criteria” later in this chapter.

## Actions

There are two Bridge-specific action in addition to the Accept, Drop, and Log actions common to all the protocols. They are

- ❑ Flood  
Specifies that any frame that matches the filter will be forwarded onto all Bridge circuits except for the circuit from which it was received.
- ❑ Forward to Circuit List  
Specifies that any frame that matches the filter will be forwarded to certain circuits that you specify.

Note that you can combine the Log action with any of the other actions. However, you should use Log only to record abnormal events; otherwise, the event log will fill up with filtering messages and thus become useless.

## IP Criteria and Actions

You can filter IP frames based on the predefined header fields within the IP header. IP also supports user-defined criteria.

### Predefined Criteria

The predefined filtering criteria for IP packets include

- ❑ Type of Service
- ❑ IP Destination Address
- ❑ IP Source Address
- ❑ UDP Source Port
- ❑ UDP Destination Port
- ❑ TCP Source Port
- ❑ TCP Destination Port
- ❑ Protocol

## User-Defined Criteria

You can filter IP traffic based on specified bit patterns contained within the IP header or the header of the upper-level protocol (TCP or UDP, for example) conveyed within the IP datagram.

When you create an IP filter with user-defined criteria, you specify the reference, offset, and length of each criterion to describe the location of criteria on incoming packets.

Reference

Positions the filtered bit pattern within the incoming frame. There are two reference points: the first is Header Start, which is the beginning of the IP header; the second is Header End, which is the beginning of the UDP or TCP header.

Offset

Positions the filtered bit pattern (measured in bits) within either the IP or the higher-level protocol header.

Length

Specifies the bit length of the filtered criteria.

Table 1-7 shows the reference, offset, and length of each IP criteria.

**Table 1-7. Reference, Offset, and Length of IP Filtering Criteria**

Field	Reference	Offset	Length
Type of Service	HEADER_START	8	8
Protocol	HEADER_START	72	8
IP Source Address	HEADER_START	96	32
IP Destination Address	HEADER_START	128	32
UDP/TCP Source Port	HEADER_END	0	16
UDP/TCP Destination Port	HEADER_END	16	16

After specifying the reference, offset, and length of your criterion, you specify one or more range. For more information, see the section “Specifying User-Defined Criteria” later in this chapter.

## Actions

There are two IP-specific actions in addition to the Accept, Drop, and Log actions common to all the protocols. They are

- **Forward to Next Hop**

Specifies that any frame that matches the filter will be forwarded to the next-hop router. You must specify the IP address of the next-hop router. If the next-hop router is not reachable, any packets matching the filter will be forwarded normally unless you also specify Drop if Next Hop is Unreachable.

If you specify 255.255.255.255 as the Next Hop, then any frame that matches this filter will be forwarded normally.

- **Drop if Next Hop is Unreachable**

Specifies that if the address specified in Forward to Next Hop is unreachable, the frame is dropped. This action is valid only when Forward to Next Hop is in use.

Note that you can combine the Log action with any of the other actions. However, you should use Log only to record abnormal events; otherwise, the event log will fill up with filtering messages and thus become useless.

## DECnet Phase IV Criteria and Actions

You can filter DECnet Phase IV traffic only on predefined criteria.

### Predefined Criteria

DECnet Phase IV predefined filtering fields include



- ❑ Destination Area
- ❑ Destination Node
- ❑ Source Area
- ❑ Source Node

Table 1-8 shows the reference, offset, and length of each DECnet predefined filtering criterion.

**Table 1-8. Reference, Offset, and Length of DECnet Filtering Criteria**

Field	Reference	Offset	Length
Destination Area	HEADER_START	0	6
Destination Node	HEADER_START	6	10
Source Area	HEADER_START	16	6
Source Node	HEADER_START	22	10

## Actions

DECnet Phase IV filtering actions include only Accept, Drop, and Log.

## VINES Criteria and Actions

You can configure VINES traffic filters to filter frames based on predefined fields within the VINES IP header. VINES also supports user-defined criteria.

### Predefined Criteria

VINES predefined filtering fields include

- ❑ Protocol Type
- ❑ Destination Address
- ❑ Source Address

---

## User-Defined Criteria

You can filter VINES traffic based on specified bit patterns contained within the VINES header.

When you create a VINES filter with user-defined criteria, you specify the reference, offset, and length of each criterion to describe the location of criteria on incoming packets.

□ Reference

Positions the filtered bit pattern within the incoming frame. There is one reference point for VINES: HEADER\_START, which indicates the start of the VINES header.

□ Offset

Positions the filtered bit pattern (measured in bits) within the OSI header.

□ Length

Specifies the bit length of the filtered criteria.

Table 1-9 shows the reference, offset, and length of the VINES predefined filtering criteria.

**Table 1-9. Reference, Offset, and Length of VINES Filtering Criteria**

Field	Reference	Offset	Length
Protocol Type	HEADER_START	40	8
Destination Address	HEADER_START	48	48
Source Address	HEADER_START	96	48

After specifying the reference, offset, and length of a criterion, you specify one or more range. For more information, see the section “Specifying User-Defined Criteria” later in this chapter.

## Actions

VINES filtering actions include Accept, Drop, and Log.

## IPX Criteria and Actions

You can configure IPX traffic filters to filter frames based on predefined fields within the IPX IP header.

### Predefined Criteria

IPX predefined filtering fields include

- Destination Network
- Source Network
- Destination Socket
- Source Socket
- Destination Address
- Source Address

Table 1-10 shows the reference, offset, and length of the IPX predefined filtering criteria.

**Table 1-10. Reference, Offset, and Length of IPX Filtering Criteria**

Field	Reference	Offset	Length
Destination Network	HEADER_START	48	32
Destination Address	HEADER_START	80	48
Destination Socket	HEADER_START	128	16
Source Network	HEADER_START	144	32
Source Address	HEADER_START	176	48
Source Socket	HEADER_START	224	16

---

## Actions

IPX filtering actions include only Accept, Drop, and Log.

## XNS Criteria and Actions

You can configure XNS traffic filters based on predefined fields within the XNS IP header. XNS does not support user-defined filters.

### Predefined Criteria

XNS predefined filtering fields include

- Destination Network
- Source Network
- Destination Socket
- Source Socket
- Destination Address
- Source Address

Table 1-11 shows the reference, offset, and length of the XNS predefined filtering criteria.

**Table 1-11. Reference, Offset, and Length of XNS Filtering Criteria**

Field	Reference	Offset	Length
Destination Network	HEADER_START	48	32
Destination Address	HEADER_START	80	48
Destination Socket	HEADER_START	128	16
Source Network	HEADER_START	144	32
Source Address	HEADER_START	176	48
Source Socket	HEADER_START	224	16

## Actions

XNS filtering actions include only Accept, Drop, and Log.

## Source Routing Criteria and Actions

You can configure Source Routing traffic filters to filter frames based on predefined fields within the Source Routing header. Source Routing filters also support user-defined criteria.

**Note:** Source Routing includes two distinctly different types of frames (*routed* frames and *explorer* frames); keep in mind that any filter you create affects *both* types of frames.

## Predefined Criteria

The predefined filtering fields for Source Routing filters include

- Next Ring
- DSAP
- SSAP
- Destination MAC Address
- Source MAC Address

**Note:** If you create a Source Routing filter that includes a Source or Destination MAC Address, you define the MAC Address in MSB (most significant bit) format. In addition, the source address you enter must have the 0x80 bit of the leftmost byte turned on to account for the RIF bit. (This bit indicates the presence of the Routing Information Field.)

- Destination NetBIOS Name
- Source NetBIOS Name

**Note:** If you create a Source Routing filter that includes a Source or Destination NetBIOS Name, you enter the NetBIOS name as the ASCII equivalent of the first 15 characters of the name. If the name is less than 15 characters, use ASCII spaces (0x20) to pad a name to 15 characters.

## User-Defined Criteria

You can filter Source Routing traffic filters to filter traffic based upon specified bit pattern(s) contained within the Source Routing header.

When you create a Source Routing filter with user-defined criteria, you specify the reference, offset, and length of each criterion to describe the location of criteria on incoming packets.

Reference

Positions the filtered bit pattern within the incoming frame. For Source Routing there are three reference points: Next Ring, Header Start, and Data Link.

Offset

Positions the filtered bit pattern (measured in bits) within either Next Ring or the MAC-level or datalink-level header.

Length

Specifies the bit length of the filtered criteria.

Table 1-12 shows the reference, offset, and length for Source Routing filtering criteria.

**Table 1-12. Reference, Offset, and Length of Source Routing Filtering Criteria**

Field	Reference	Offset	Length
Next Ring	NEXT_RING	0	12
Destination MAC Address	HEADER_START	0	48
Source MAC Address	HEADER_START	48	48
DSAP	DATA_LINK	0	8
SSAP	DATA_LINK	8	8
Destination NetBIOS Name	DATA_LINK	120	120
Source NetBIOS Name	DATA_LINK	248	120

**Note:** Creating a filter that includes Next Ring as a criterion affects only the routed frames. The Next Ring criterion does not affect explorer frames.

After specifying the reference, offset, and length of a criterion, you specify one or more range. For more information, see the section “Specifying User-Defined Criteria” later in this chapter.

## Actions

Source Routing supports two Source Routing-specific actions in addition to the Accept, Drop, and Log actions common to all protocols:

- Direct IP Explorers

Specifies that any *explorer* frame that matches the filter will be sent to some number of IP addresses. You are required to specify these IP addresses.

IP encapsulation must be configured for this action to be valid. If it is not configured, and a frame matches the filter, the frame will be flooded as if no filter existed.

- ❑ Forward to Circuits

Specifies that any frame that matches the filter will be forwarded to certain circuits that you specify.

## OSI Criteria and Actions

You can configure OSI traffic filters to filter frames based on predefined fields within the CLNP header. OSI also supports user-defined criteria.

### Predefined Criteria

OSI predefined filtering fields include

- ❑ Destination Area
- ❑ Destination System ID
- ❑ Source Area
- ❑ Source System ID

### User-Defined Criteria

You can filter OSI traffic based upon specified bit pattern(s) contained within the CLNP header.

When you create a filter with user-defined criteria, you specify the reference, offset, and length of each criterion to describe the location of criteria on incoming packets.

- ❑ Reference

Positions the filtered bit pattern within the incoming frame. There are three reference points for OSI: `OSI_BASE`, which indicates the start of the CLNP header; `OSI_DEST`, which indicates the start of the last two bytes of the Destination Area Address field; and `OSI_SRC`, which indicates the start of the last two bytes of the Source Area Address field.



- **Offset**  
Positions the filtered bit pattern (measured in bits) within the OSI header.
- **Length**  
Specifies the bit length of the filtered criteria.

After specifying the reference, offset, and length of a criterion, you specify one or more range. For more information, see the section “Specifying User-Defined Criteria” later in this chapter. Table 1-13 shows the reference, offset, and length of each OSI filtering criterion.

**Table 1-13. Reference, Offset, and Length of OSI Filtering Criteria**

<b>Field</b>	<b>Reference</b>	<b>Offset</b>	<b>Length</b>
Destination Area	OSI_DEST	0	16
Destination System ID	OSI_DEST	16	48
Source Area	OSI_SRC	0	16
Source System ID	OSI_SRC	16	48

## **Actions**

OSI filtering actions include only Accept, Drop, and Log.

## DLSw Criteria and Actions

You can filter DLSw traffic based on predefined fields within the DLSw header, as defined in RFC 1434. DLSw also supports user-defined criteria.

### Predefined Criteria

DLSw predefined filtering fields include

- ❑ Destination MAC Address
- ❑ Source MAC Address
- ❑ DSAP
- ❑ SSAP

### User-Defined Criteria

You can filter DLSw traffic based upon specified bit pattern(s) contained within the DLSw header. When you create a filter with user-defined criteria, you specify the reference, offset, and length of each criterion to describe the location of criteria on incoming packets.

- ❑ Reference

Positions the filtered bit pattern within the incoming frame. There is one reference point for DLSw, `DLS_BASE`, which is the beginning of the DLSw header.

- ❑ Offset

Positions the filtered bit pattern (measured in bits) within the DLSw header.

- ❑ Length

Specifies the bit length of the filtered criterion. After specifying the reference, offset, and length of a criterion, you specify one or more range. For more information, see the section “Specifying User-Defined Criteria” later in this chapter.

Table 1-14 shows the reference, offset, and length of each DLSw filtering criterion.

**Table 1-14. Reference, Offset, and Length of DLSw Filtering Criteria**

Field	Reference	Offset	Length
Destination MAC Address	DLS_BASE	192	48
Source MAC Address	DLS_BASE	240	48
DSAP	DLS_BASE	288	8
SSAP	DLS_BASE	296	8

## Actions

There is one DLSw-specific action in addition to the Accept, Drop, and Log actions common to all the protocols.

Forward to IP Address specifies that any frame that matches the filter will be sent to some IP address. You are required to specify the IP address.

## Specifying User-Defined Criteria

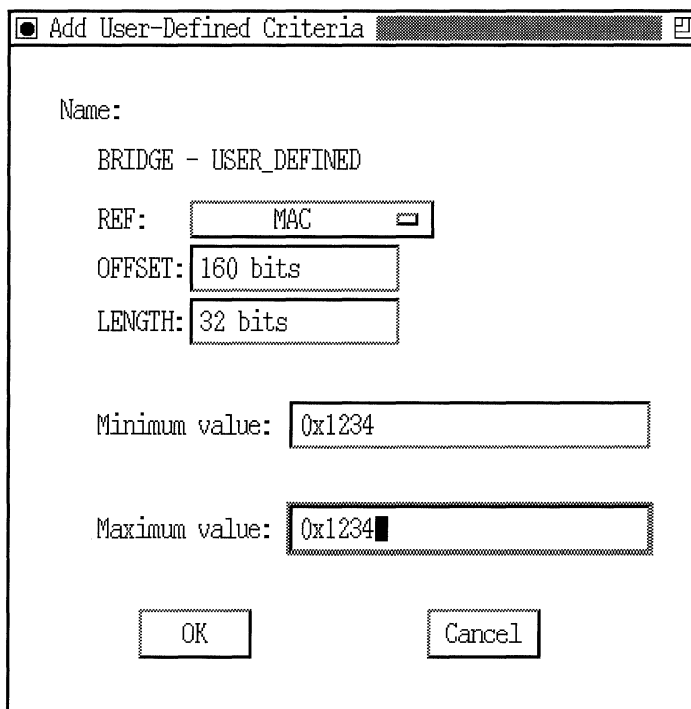
When you use the Configuration Manager to create or edit a template, you usually add or edit filtering criteria (see Chapter 2). When you access the appropriate menu to add a criterion, each predefined filtering criterion is represented as an option in that menu. In addition to the predefined criteria, the menu provides a “User-Defined” criteria choice when creating a filter for most protocols.

The User-Defined option allows you to set up specialized filtering criteria based on bit patterns within a packet’s header.

Setting up user-defined criteria is similar to setting up predefined criteria, except you must specify the criterion’s location within the packet. (With predefined criteria, the locations are established.)

Therefore, there is one extra step (window) required to specify a user-defined criterion.

When you select the User-Defined option, the Add User-Defined Criteria window appears (Figure 1-2). In this window, you specify the criterion's location within the header. To do this, you set the criterion's reference, offset, and length. Then, you specify a range associated with the bit criterion described by the reference, offset, and length.



The screenshot shows a dialog box titled "Add User-Defined Criteria". It contains the following fields and controls:

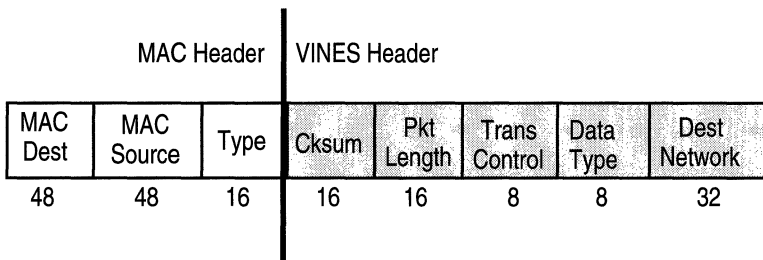
- Name:** BRIDGE - USER\_DEFINED
- REF:** A dropdown menu with "MAC" selected.
- OFFSET:** A text box containing "160 bits".
- LENGTH:** A text box containing "32 bits".
- Minimum value:** A text box containing "0x1234".
- Maximum value:** A text box containing "0x1234".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

**Figure 1-2. Add User-Defined Criteria Window**

For example, suppose that you are bridging VINES traffic over Ethernet, and you want to drop all packets with a destination network number of 1234 (hex); you would set up filtering criteria as follows:

1. Specify an Ethernet Type criterion of 0xBAD (VINES). Ethernet Type is a predefined criterion.

2. Determine the reference, offset, and length values of the Destination Network criterion within the header (Figure 1-3).



**Figure 1-3. VINES Header**

3. Set the reference, offset, and length in the Add User-Defined Criteria window, as follows:
  - Reference = MAC (beginning of frame)
  - Offset = 160 bits (sum of all criteria that precede the Destination Network field, or  $48+48+16+16+16+8+8$ )
  - Length = 32 bits
4. Specify the range to go with the criterion described by Reference, Offset, and Length.

The procedures in Chapter 2 on adding, deleting, and editing ranges for predefined criteria are the same as the procedures for a user-defined criterion.

---

# Chapter 2

## Using the Configuration Manager to Apply Traffic Filters

This chapter explains how to use the Configuration Manager tool to configure traffic filters. It explains how to:

- ❑ Display the Traffic Filters window
- ❑ Prepare filter templates
- ❑ Modify templates
- ❑ Create a filter
- ❑ Edit filters
- ❑ Delete filters
- ❑ Enable or disable a filter
- ❑ Apply filter precedence

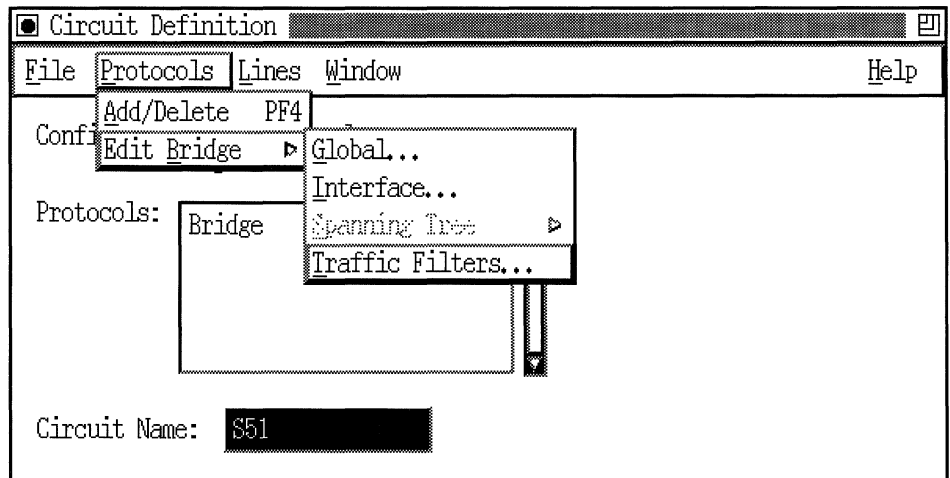
This chapter assumes that you are familiar with protocol-specific filtering criteria and actions, and with setting up user-defined criteria if you intend to do so. Refer to Chapter 1 for information on these topics.

For information on prioritizing protocols and configuring outbound filters, see Chapter 3, “Protocol Prioritization and Outbound Filters: An Overview,” and Chapter 4, “Using the Configuration Manager to Configure Priority Filters.”

## Displaying the Traffic Filters Window

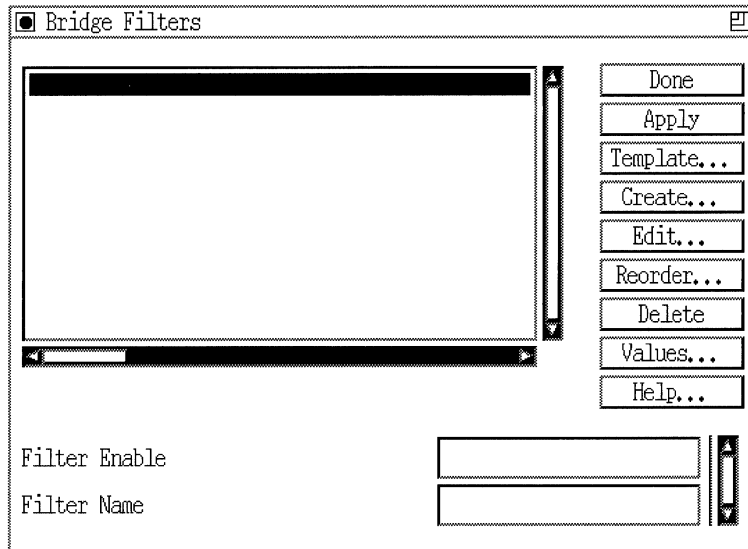
To work with traffic filters for a particular interface, you must first display the Filters window for the circuit's protocol by completing the following steps.

1. Start at the Configuration Manager window (accessible from the Wellfleet Site Manager main menu).
2. Select **Circuits**→**Edit Circuits**.  
The Circuit List window appears.
3. Select the circuit to which you want to add a traffic filter.
4. Click on the Edit button. The Circuit Definition window appears, with the circuit you just selected highlighted.
5. Select **Protocols**→**Edit (protocol)**→**Traffic Filters**, as shown in Figure 2-1.



**Figure 2-1. Selecting the Traffic Filters Menu**

The Filters window for the selected circuit and protocol appears (Figure 2-2).



**Figure 2-2. Filters Window**

**Note:** The Filters window is protocol specific. In Figure 2-2, the selected circuit was configured with the Bridge protocol. The circuit does not yet have any traffic filters configured, so the Filters scroll box is empty.

## Preparing Filter Templates

This section describes how to add a filter template to an interface by

- ❑ Creating a new filter template or using an existing template
- ❑ Adding desired filtering criteria, ranges, and actions to a template

The “Creating a Filter” section, later in this chapter, describes how to create a filter by applying (saving) a filter template to an interface.



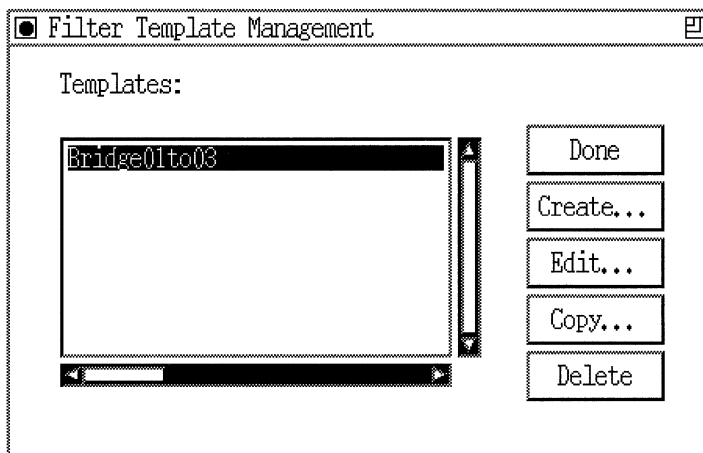
## Creating a New Template

When you add a filter to an interface, you do not always need to create a new template. Often, you can begin with an existing template. Skip this section and go to the “Modifying Templates” section if there is already a filter template for the circuit you are configuring that includes filter information you might use.

If there is no existing template to match your needs, you must first create a new template for your circuit. To create a new template from scratch, begin as follows:

1. Start at the Filters window for your selected circuit (Figure 2-2).
2. Click on the Template button.

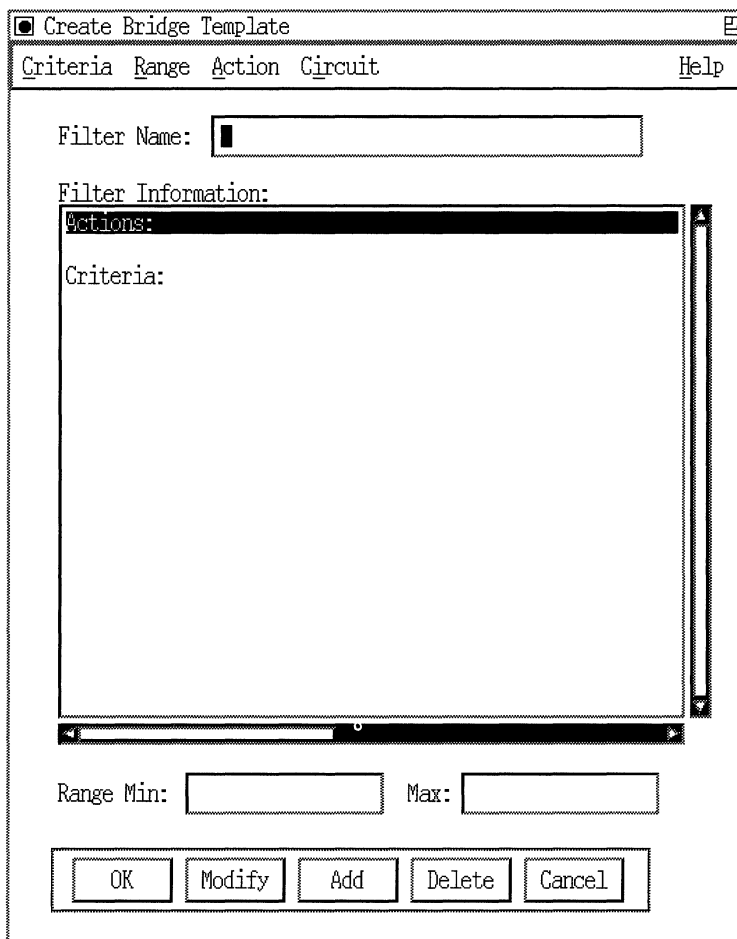
The Filter Template Management window appears, as shown in Figure 2-3.



**Figure 2-3. Filter Template Management Window**

3. Click on the Create button.

The Create Template window appears (Figure 2-4).



**Figure 2-4. Create Template Window**

**Note:** The Create Template window is protocol specific. The example in Figure 2-4 shows the Create IP Template window; the window for other protocols is similar.

4. Enter a name for the new template in the Filter Name box.

Give descriptive names to your templates. For instance, in this example, the template is named *Bridge01to03* because it will contain information for filtering bridge frames from certain MAC source addresses (0x0000A2000001 to 0x0000A2000003).

5. Click on the OK button to save the new template.

To add filter criteria and actions, proceed to **Step 6** in the “Modifying Templates” section below (skip the “Copying a Template” subsection).

## Modifying Templates

There are two ways to change a filter template:

- Copy the existing template, rename it, and then edit it.

This preserves the original template and creates an entirely new template with the same criteria and actions. You can then modify the new version to suit your needs.

- Edit the existing template.

If you do not want or need to preserve the original template, you can edit it without first copying and renaming it. (Changing a template does not affect interfaces to which the template has already been applied.)

To edit an existing template without preserving the original, proceed to **Step 6** (skip the “Copying a Template” subsection).

## Copying a Template

To duplicate an existing template, proceed with the steps below.

**Note:** You can also edit or copy a template using a text editor. The Configuration Manager stores all templates in a file called *template.ftt*.

1. Start at the Filter Template Management window (Figure 2-3).

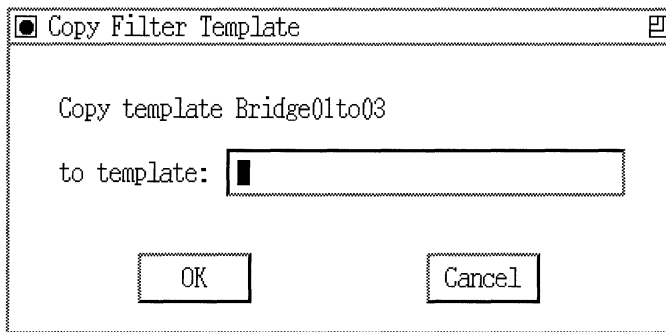
2. If the Templates box in the Filter Template Management window is displaying the name of the template you want to copy, go to the next step.

If the Templates box is *not* currently displaying the name of the template you want to copy, click on the Templates box. A menu displaying all existing templates appears; choose the template you want to copy.

If there is no existing template to match your needs, you must first create a new template for your circuit, as described in the previous section, “Creating a New Template.”

3. Click on the Copy Button.

The Copy Filter Template window appears (Figure 2-5).



**Figure 2-5. Copy Filter Template Window**

4. Enter a name for the new template in the box provided.

Remember that it is a good idea to give your template a name that reflects its contents.

5. Click on the OK button.

You are returned to the Filter Template Management window. The name you just assigned to the new template appears in the Templates box.

To edit filter criteria and actions, proceed to the next section, “Editing a Template.”

## Editing a Template

Once you create or copy a template, you edit it to apply the filters you want.

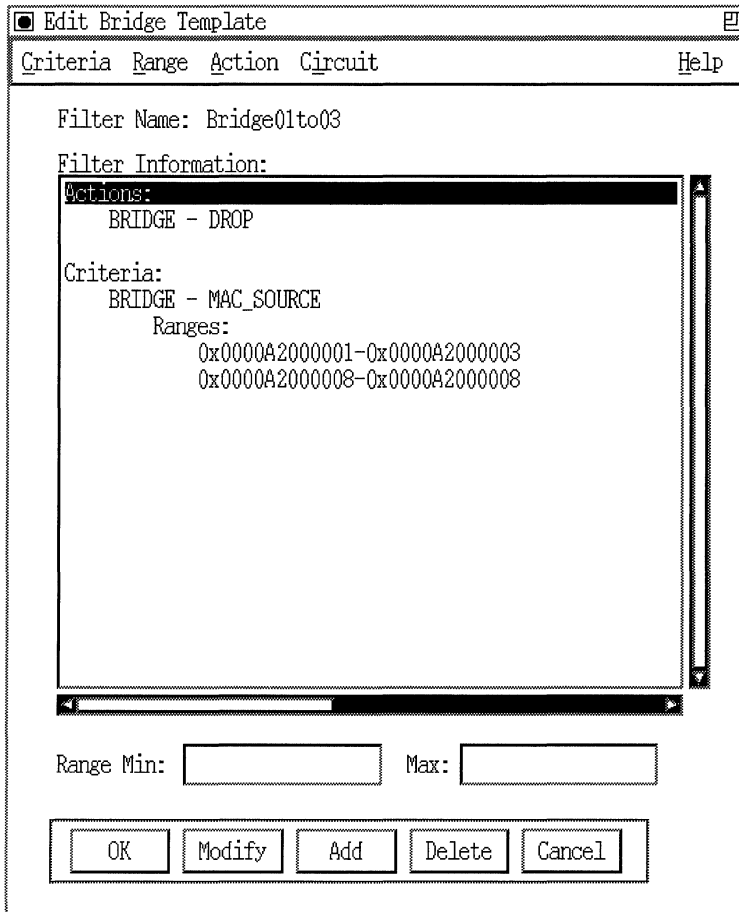
6. Start at the Filter Template Management window (Figure 2-3).
7. If the Templates box on the Filter Templates Management window is displaying the name of the template you want to edit, go to the next step.

If the Templates box is *not* currently displaying the name of the template you want to edit, click on the Templates box. A menu displaying all existing templates appears; choose the template you want to edit.

8. Click on the Edit button.

The Edit Filter Template window appears (Figure 2-6).

**Note:** The Edit Filter Template window is protocol specific. The example in Figure 2-6 shows the Edit Bridge Template window; the window for other protocols is similar.



**Figure 2-6. Edit Filter Template Window**

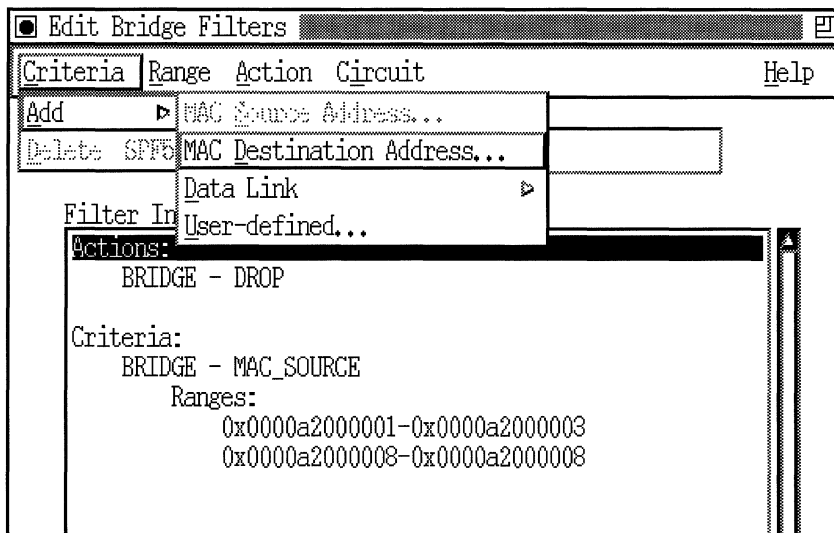
You modify a template by modifying, adding, or deleting filter criteria, ranges, and actions, as described in following subsections.

**Note:** If you intend to work with user-defined criteria, refer to the section “Specifying User-Defined Criteria” in Chapter 1, which explains the special considerations of specifying user-defined criteria.

## Adding Template Criteria

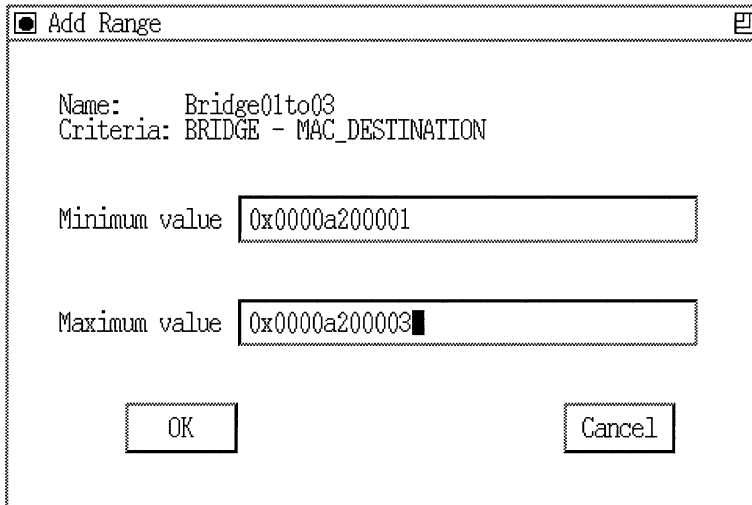
To add filter criteria to a template, begin at the Edit Filter Template window. Refer to Chapter 1 if you are not familiar with protocol-specific filtering criteria and actions.

1. Select Criteria→Add; then select the criterion that you want to filter packets.



**Figure 2-7. Selecting a Filter Criterion**

The Add Range window appears (Figure 2-8). For each criterion you choose, you must specify at least one range. You can add up to 100 ranges for a filter criterion.



**Figure 2-8. Add Range Window**

2. Specify the low and high ends of the range you want to filter in the Minimum value and Maximum value boxes.

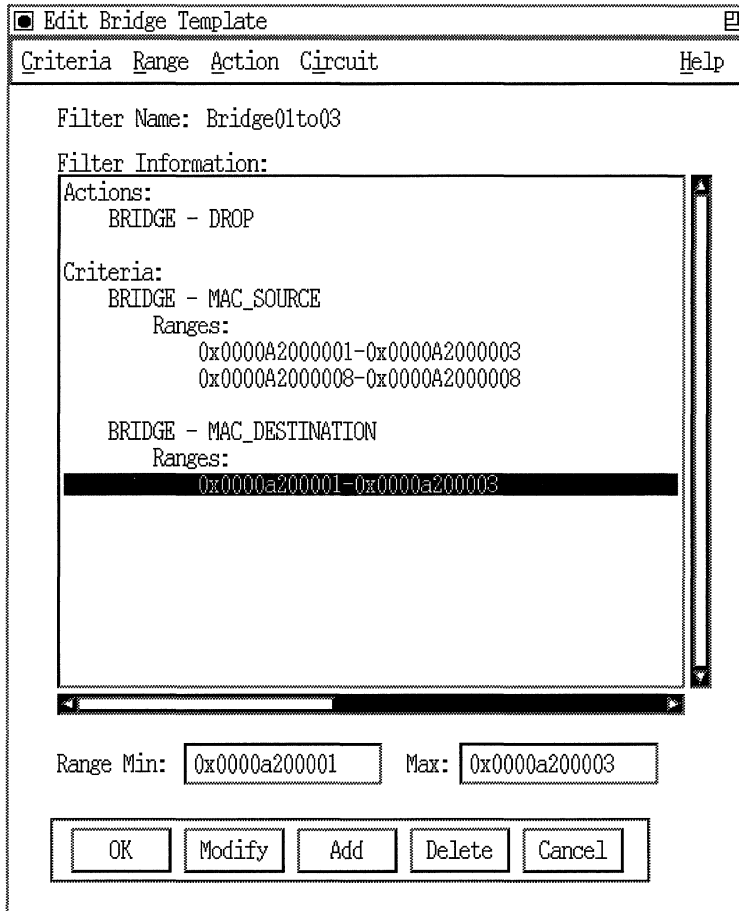
If the range you want to add consists of just one value, specify that value in both boxes. In this example (Figure 2-8), the range for the MAC source address criterion is between 0x0000A2000001 (the minimum value) and 0x0000A2000003 (the maximum value). Each incoming packet will be checked to see if its MAC source address falls into this range of addresses.

**Note:** When you enter values for minimum and maximum value, the Configuration Manager assumes the value is a decimal number. If you want to enter a hexadecimal number, you *must* use the prefix 0x.

3. Click on the OK button.

You return to the Edit Filter Template window. The new criterion and range appear in the Filter Information scroll box, as shown in Figure 2-9.





**Figure 2-9. Criteria List with Range Added**

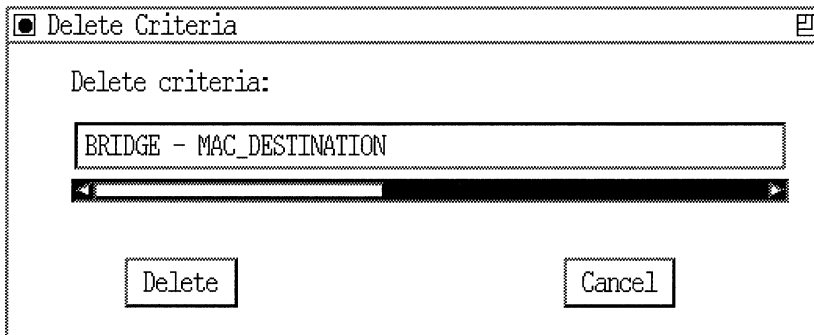
4. When you are finished adding ranges, click on the OK button to return to the Template Management window.

## Deleting Criteria

If you want to remove a configured filter criterion from a template, begin at the Edit Filter Template window (Figure 2-6); then follow these steps:

1. From the Filter Information scroll box, select the criterion you want to remove.
2. Click on the Delete button.

A Delete Criteria window appears (Figure 2-10).



**Figure 2-10. Deleting a Filter Criterion**

3. Click on the Delete button to confirm.

You are returned to the Edit Filter Template window. The criterion you just deleted no longer appears in the Filter Information scroll box.

Repeat this procedure for each criterion you want to delete from a template.

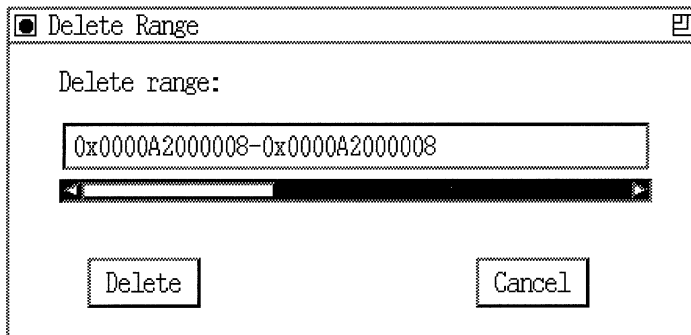
## Deleting Ranges

If you need to delete a range from a template's criteria, begin at the Edit Filter Template window (Figure 2-6); then complete the following steps.

**Note:** You must have at least one range specified for each criterion.

1. From the Filter Information scroll box, select the range (listed beneath a criterion) that you want to delete.
2. Click on the Delete button.

A Delete Range window appears (Figure 2-11).



**Figure 2-11. Deleting a Range**

3. Click on the Delete button to confirm.

The range you just deleted no longer appears in the Filter Information scroll box. Repeat this procedure for each range you want to delete from a template.

## Modifying a Range

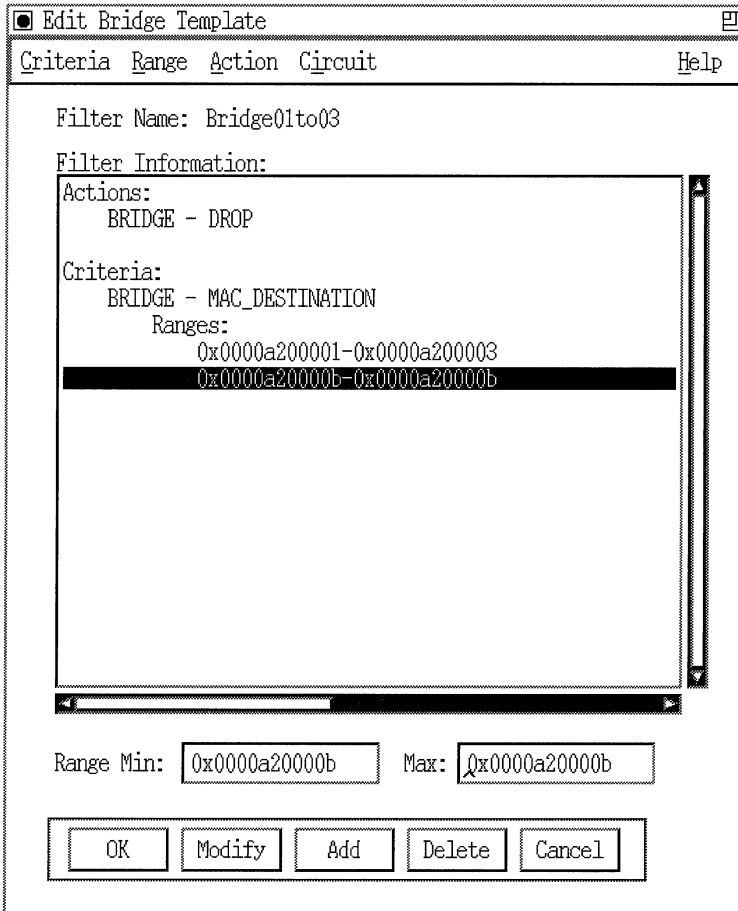
If you need to change a range for a criterion, begin at the Edit Filter Template window (Figure 2-6); then complete the following steps.

**Note:** You must have at least one range specified for each criterion.

1. Select the range you want to modify by clicking on the range line inside the Filter Information box.

For example, in Figure 2-12 you could select the range 0x0000A200001 — 0x0000A200001 or the range

0x0000A20000B — 0x0000A20000B. The 0x0000A20000B — 0x0000A20000B range is selected in this example.



**Figure 2-12. Modify a Range**

2. With the range selected, click on the Modify button.
3. Use the Range Min: and Max: value boxes (located near the bottom of the window, as shown in Figure 2-12) to specify a new low and high value for applying the selected filter criterion.

**Note:** When entering range values, you *must* use the prefix 0x to specify a hexadecimal number.

4. Click on the OK button when you are satisfied with the values for all criteria ranges.

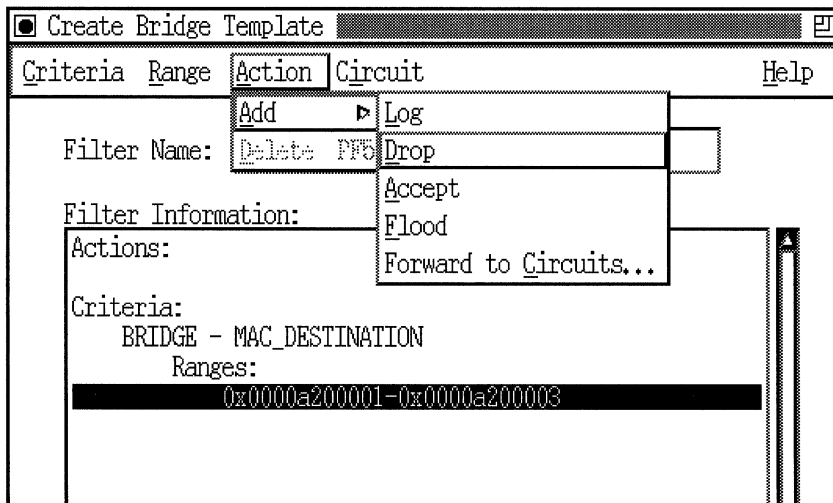
## Specifying Template Actions

To add, remove, or modify filter actions, begin at the Edit Filter Template window (Figure 2-6); then follow the applicable steps below.

### Adding an Action

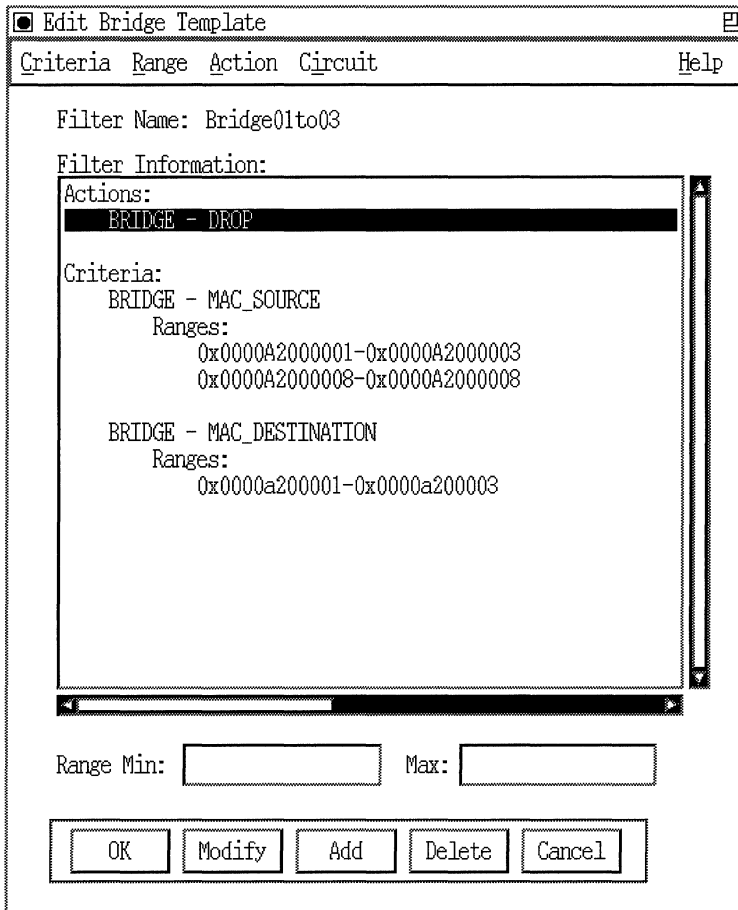
1. Select Action→Add at the Edit Filter Template window; then, select the action you want to impose on packets that match any of the template's ranges of filtering criteria.

Figure 2-13 shows choosing the Drop action.



**Figure 2-13. Choosing the Drop Action**

You return to the Edit Filter Template window. The new criterion and range appear in the Filter Information scroll box, as shown in Figure 2-14.



**Figure 2-14. Actions List with New Action**

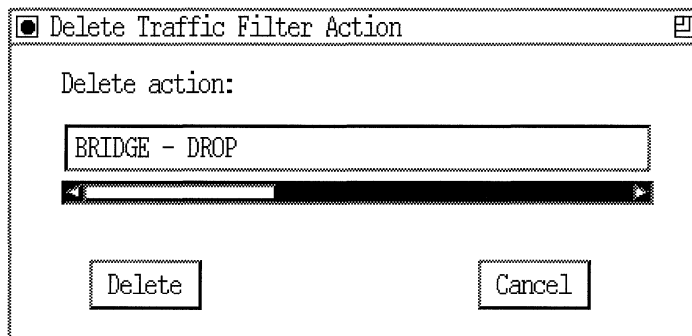
2. When you are finished adding actions to your template, click on the OK button.

## Deleting an Action

If you no longer want to include an action in a template, follow these steps to remove it:

1. From the Filter Information scroll box in the Edit Template window, select the action you want to remove.
2. Click on the Delete button.

A Delete Action window appears, as shown in Figure 2-15.



**Figure 2-15. Deleting an Action**

3. Click on the Delete button to confirm.

The action you just deleted no longer appears in the Filter Information scroll box.

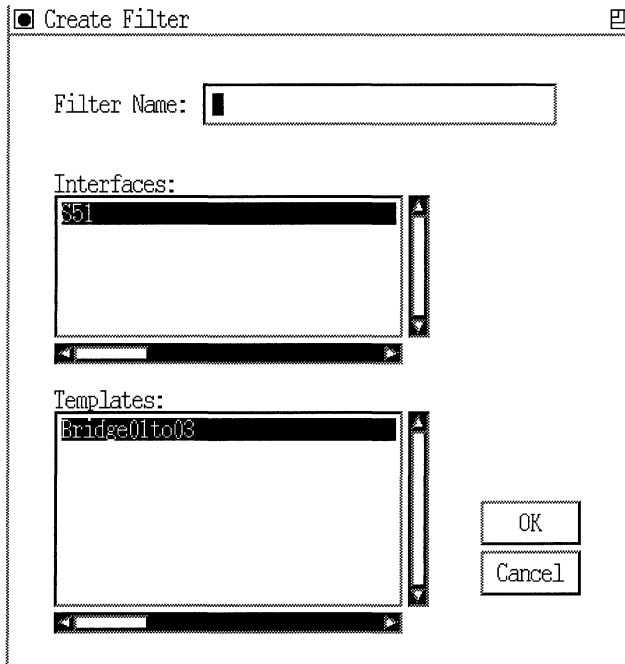
Repeat this procedure for each action you want to delete from a template.

## Creating a Filter

To create a traffic filter, complete the following steps:

1. Start at the Filters window for your selected circuit and protocol, as described in the first section of this chapter, "Displaying the Traffic Filters Window." Figure 2-2 shows the Filters window.

2. Click on the Create Filter button. The Create Filter window appears, as shown in Figure 2-16.

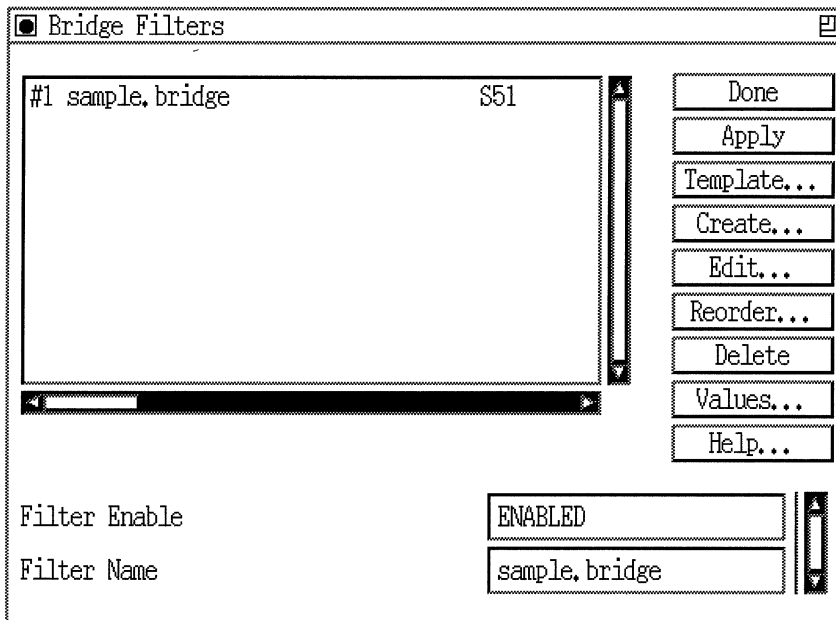


**Figure 2-16. Create Filter Window**

3. In the Filter Name field, enter a meaningful name for the new filter. Also verify the name of the selected interface.
4. With the appropriate interface and template specified, click on the OK button (and exit).

You are returned to the Filters window (Figure 2-17).





**Figure 2-17. New Filter Listed in Scroll Box**

In this example, the template selected in Figure 2-16 was applied to create a filter named *sample.bridge* on interface S51.

## Editing Filters

Once you apply a filter to an interface, you can edit its criteria, ranges, and actions. If you've used a template that was edited to suit your needs, you don't need to complete further edits.

To customize a specific filter, you have the following options, described in subsequent sections:

- Add or delete filtering criteria
- Add, modify, or delete ranges
- Add or delete actions

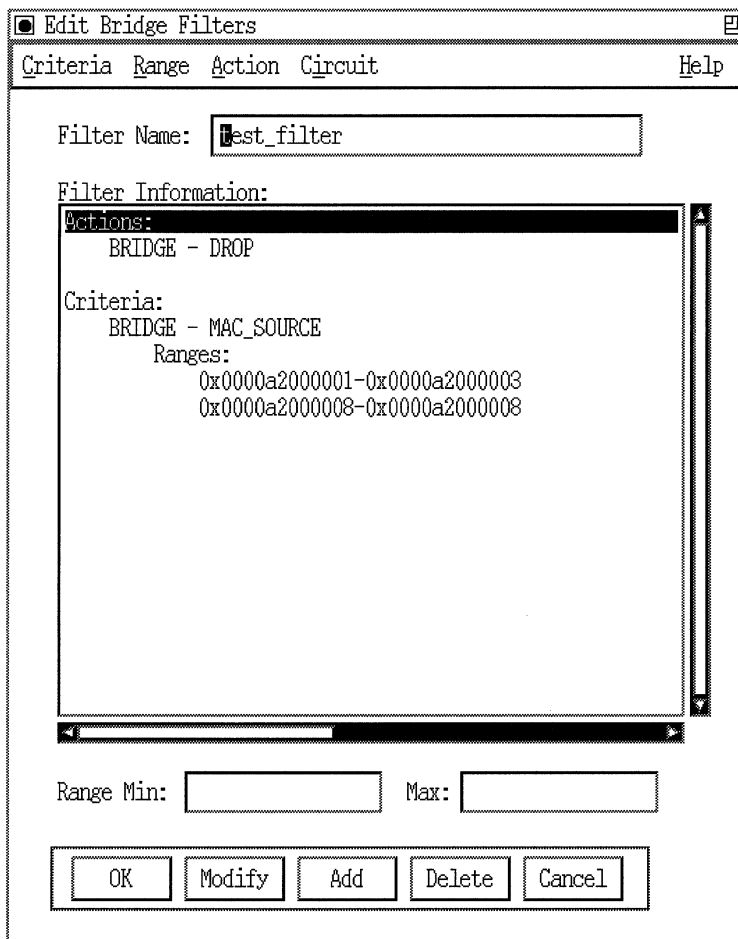
Complete the steps in applicable subsections below.

1. Start at the Filters window for the circuit you are editing (Figure 2-2).
2. If the scroll box is displaying the name of the filter you want to edit, go to the next step.

If the scroll box is *not* currently displaying the name of the template you want to edit, click on the box. A menu displaying all existing filters appears; choose the one you want to edit.

3. Click on the Edit button.

The Edit Filters window appears, as shown in Figure 2-18.



**Figure 2-18. Edit Filters Window**

**Note:** The Edit Filters window is protocol specific. The example in Figure 2-18 shows the Edit Bridge Filter window; the window for other protocols is similar.

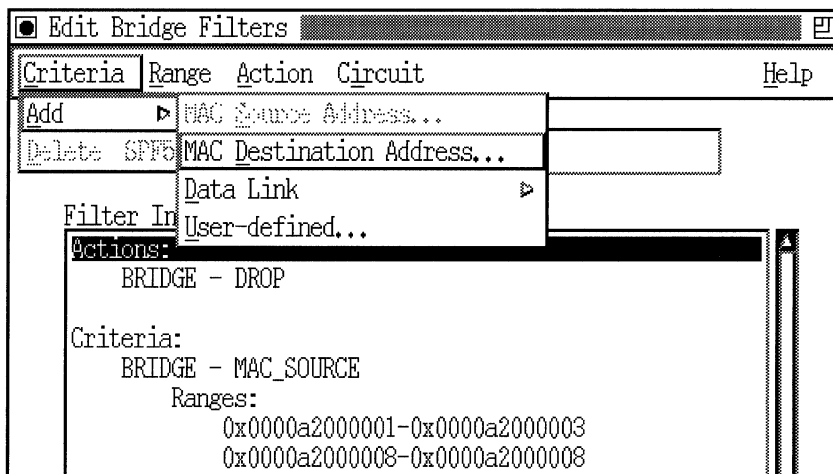
## Specifying Filter Criteria

To add or remove filter criteria, begin at the Edit Filters window.

**Note:** If you intend to work with user-defined criteria, refer to the section “Specifying User-Defined Criteria” in Chapter 1, which explains the special considerations of specifying user-defined criteria.

### Adding Criteria

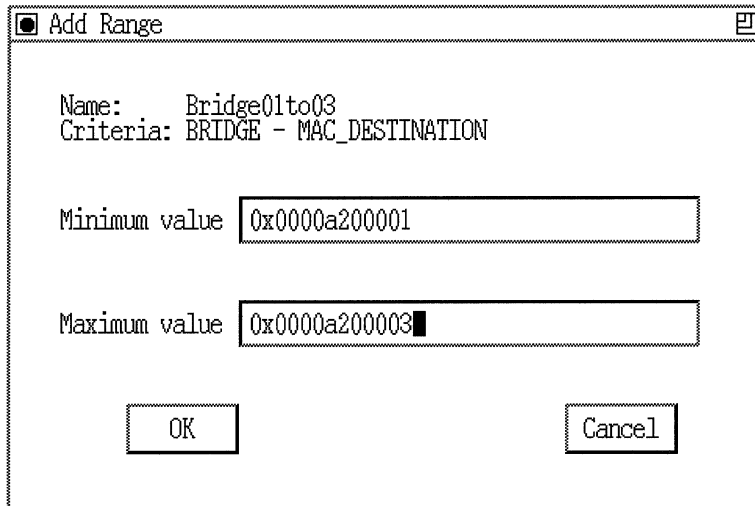
1. Select Criteria→Add; then select the criterion you want to use to filter packets. Figure 2-19 shows the MAC Destination criterion type.



**Figure 2-19. Adding a Filter Criterion**

The Add Range window appears (Figure 2-20).

**Note:** For any criterion you choose, you must specify at least one range. You can add up to 100 ranges for each filter criterion.



**Figure 2-20. Add Range Window**

2. Specify the low and high values of the criterion range in the Minimum value and Maximum value boxes.

If the range you want to add consists of just one value, specify that value in both boxes. In this example (Figure 2-20), the range for the MAC destination address criterion is between 0x0000A200001 (the minimum value) and 0x0000A200003 (the maximum value). Each incoming packet will be checked to see if its MAC destination address falls into this range of addresses.

**Note:** When you enter values for minimum and maximum value, the Configuration Manager assumes the value is a decimal number. To enter a hexadecimal number, you *must* use the prefix 0x.

3. Click on the OK button.

You return to the Edit Filters window. The range you specified appears in the scroll box for the selected criterion.

4. When you are finished adding ranges, click on the OK button to return to the Filters window.

## Deleting Criteria

If you don't want a configured filter criterion, follow these steps:

1. From the Edit Filter scroll box, select the criterion you want to delete.
2. Click on the Delete button.

You are returned to the Edit Filters window. The criterion you just deleted no longer appears in the scroll box.

Repeat this procedure for each criterion you want to delete from a template.

## Deleting Ranges

If you need to delete a range from a criterion, begin at the Edit Filters window (Figure 2-18); then, complete the following steps.

1. From the scroll box, select the range (listed beneath a criterion) that you want to delete.
2. Click on the Delete button.

## Modifying a Range

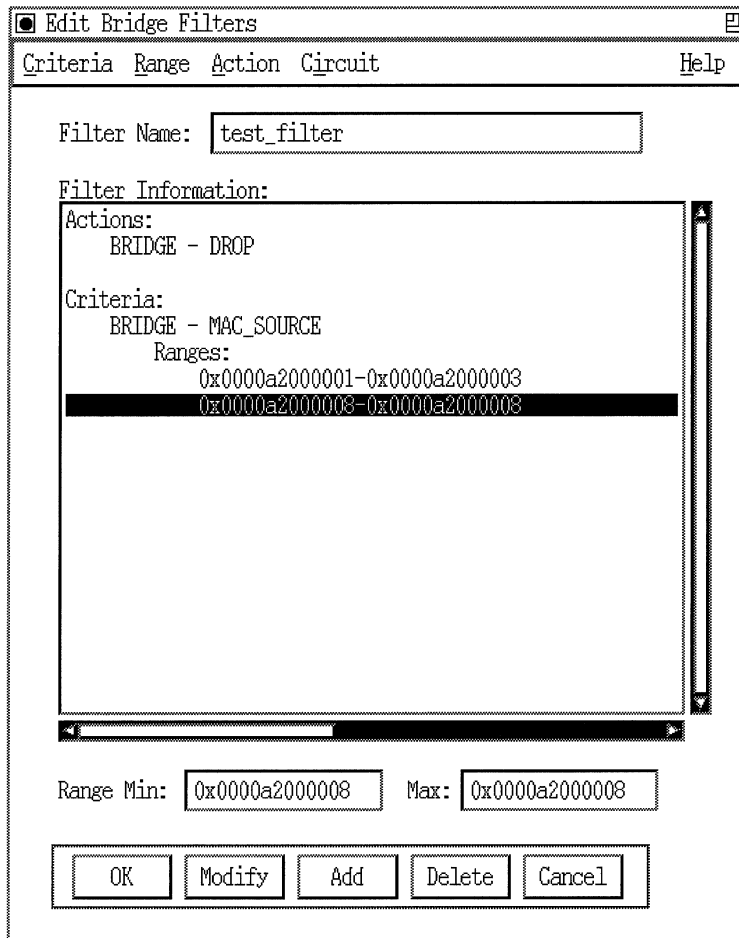
If you need to change a range for a criterion, begin at the Edit Filter Template window (Figure 2-6) or the Create Template window (Figure 2-4); then complete the following steps.

**Note:** You must have at least one range specified for each criterion.

1. Select the range you want to modify by clicking on the range line inside the Filter Information box.

For example, in Figure 2-21 you could select the range  
0x0000A200001 — 0x0000A200001 or the range  
0x0000A20000B — 0x0000A20000B.

2. With the range selected, click on the Modify button.



**Figure 2-21. Modifying a Range**

3. Use the Range Min: and Max: value boxes (located near the bottom of the window, as shown in Figure 2-21) to specify new low and high ends of the range for the selected filter criterion.

**Note:** When entering range values, you *must* use the prefix 0x to specify a hexadecimal number.

Click on the OK button when you are satisfied with the values for all criteria ranges.

## Specifying Filter Actions

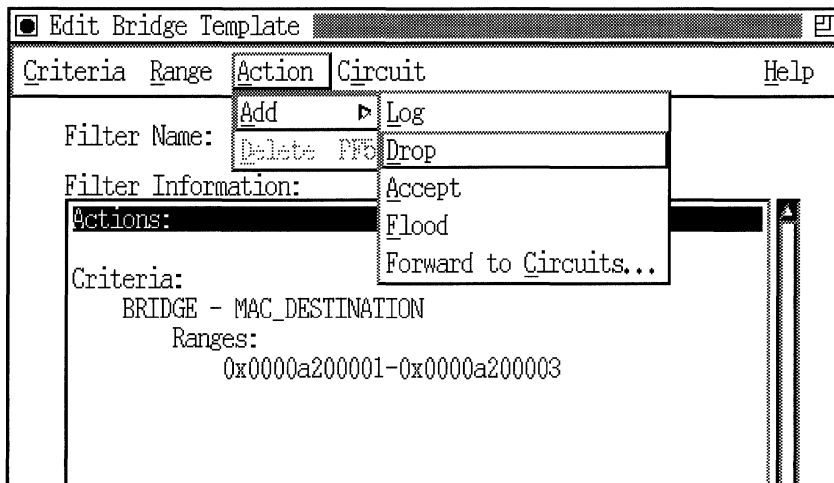
To add, remove, or modify filter actions, begin at the Edit Filters window (Figure 2-18); then follow the applicable steps below.

Refer to Chapter 1 for information about filter action options.

### Adding an Action

1. Select Action→Add at the Edit Filters window; then select the action you want to impose on packets that match any of the template's ranges of filtering criteria.

Figure 2-22 shows choosing the Drop action.



**Figure 2-22. Choosing the Drop Action**

2. When you are finished adding actions to your template, click on OK at the Edit Filters window.



## Deleting an Action

If you no longer want to include an action, follow these steps to remove it:

1. From the scroll box in the Edit Filters window, select the action you want to remove.
2. Click on the Delete button.

The action you just deleted no longer appears in the Filter Information scroll box.

Repeat these steps for each action you want to delete from a template.

## Deleting Filters

If you want, you can delete filters from individual interfaces.

**Note:** When you delete a filter, it affects only the interface from which the filter is removed.

To delete a filter from an interface, complete the following steps:

1. Start at the Filter window for the circuit from which you want to delete a filter, as described in the first section of this chapter, “Displaying the Traffic Filters Window.” Figure 2-2 shows the Filters window.
2. Select the filter that you want to delete from the filter scroll box.

**Caution:** There is no confirmation of a filter deletion; be sure to select a filter you are certain you want to delete.

3. Click on the Delete button.

The filter is deleted from the circuit and no longer appears in the scroll box on the Filters window.

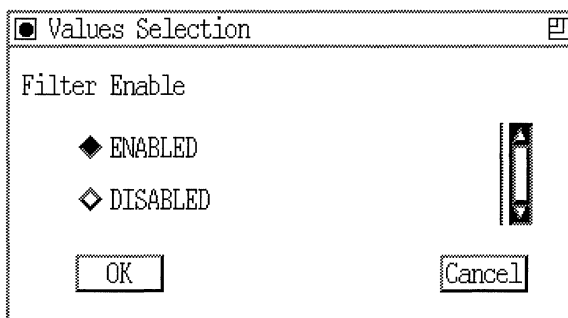
## Enabling or Disabling a Filter

Instead of deleting a filter from a circuit, you may want to turn off the filter temporarily. You can do this by disabling the filter on a circuit. Later, you can re-enable the filter. Begin at the Wellfleet Configuration Manager window, and complete the following steps to disable (or re-enable) a filter.

1. Start at the Filters window for the circuit you want to work with, as described in the first section of this chapter, “Displaying the Traffic Filters Window.” Figure 2-2 shows the Filters window.
2. Select the filter that you want to disable or re-enable from the filter scroll box.
3. Click on the Values button.

The Values Selection window appears, as shown in Figure 2-23.

4. When you want to re-enable the filter, simply change the value in the Filter Enable parameter box from Disabled to Enabled.
  5. Click on the OK button.
- You return to the Filters window.
6. Click on the Apply button to save this change.



**Figure 2-23. Enabling or Disabling a Filter**

## Applying Filter Precedence

Create filters on each interface in order of precedence. The first filter you create has the lowest precedence; the last filter you create has the highest precedence.

If possible, accomplish your filtering goals mainly with drop filters, since these result in faster router performance than accept filters do.

If your filtering strategy involves forwarding most traffic and dropping only specified packets, configure filters only for the specific traffic you want to drop.

If your strategy involves blocking most traffic and accepting only specified packets (a “firewall”), begin with a drop-all filter on the interface. Then add more specific, higher-precedence filters to achieve the desired result on the interface, as described in the next section.

## Using Drop-All Filters

The drop-all filter describes the broadest range of packets you want to block from an interface. To ensure that all unwanted traffic gets dropped, you should

1. Choose criteria that appear in *every* packet of the protocol you want to filter.
2. Determine the length of the field.
3. Determine the maximum possible value of the range.
4. Determine the minimum value of the range.
5. Enter these values when you specify the drop-all filter.

Once you specify a drop-all filter, you can then add higher-precedence filters to create exceptions (or “holes”) in the drop-all range.

For example, to configure a circuit that only accepts IP traffic addressed for destination address 192.32.28.55, you apply a drop-all filter and one accept filter, as follows:

Filter Action	Precedence	Start of Range	End of Range
Accept	1 (highest)	192.32.28.55	192.32.28.55
Drop	2 (lower)	192.32.25.00	192.32.28.255

Figure 2-24 shows a more complicated example of this strategy: a drop-all filter working in combination with three higher-precedence filters on an interface.

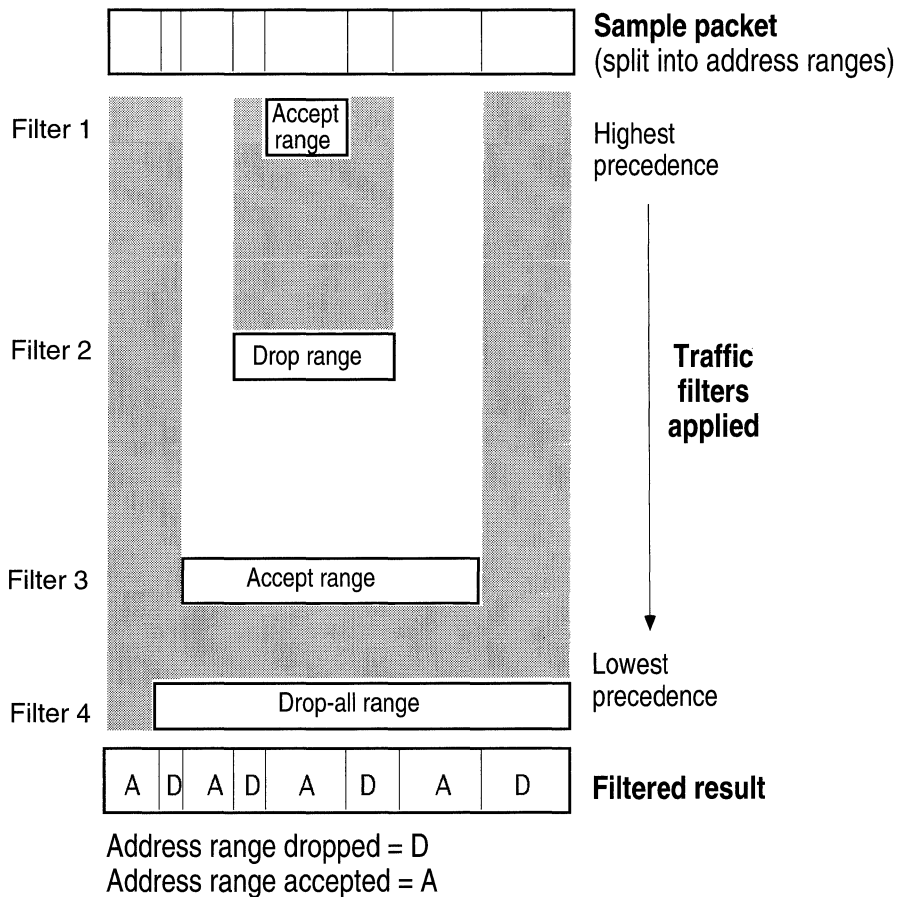
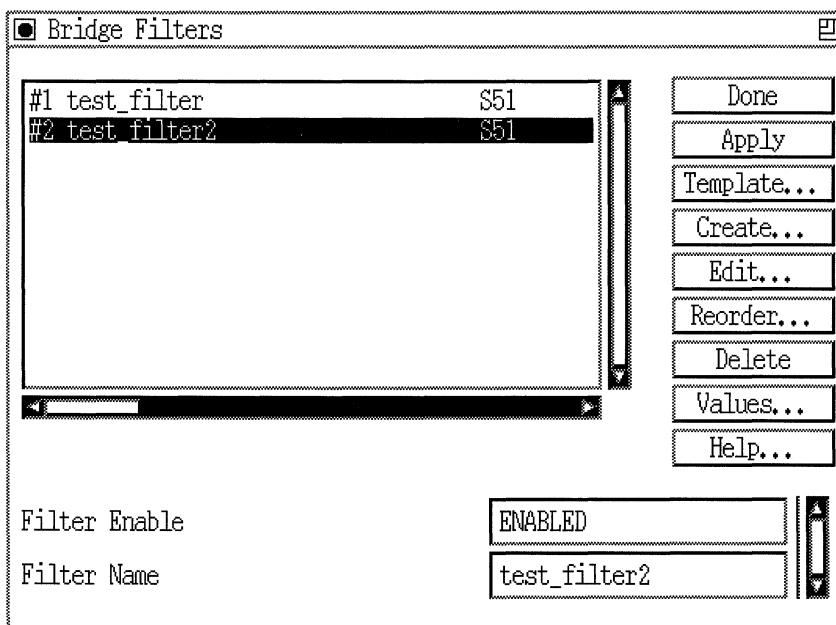


Figure 2-24. Example Result of Applying Filter Precedence

The “Filtered result” shown in Figure 2-24 indicates address intervals over which the interface will drop or accept packets it receives. Note how the highest-precedence filter in a given address range determines the result of combined filtering within that range.

Figure 2-25 shows how the Filters window displays the filters on an interface. The first filter has the highest precedence and a rule number of 1. Subsequent filters created on the interface have decreasing precedence.

If the first filter on the interface (#1) accepts a packet and the second filter (#2) drops the same packet, filter #1 has precedence and the packet will be accepted.

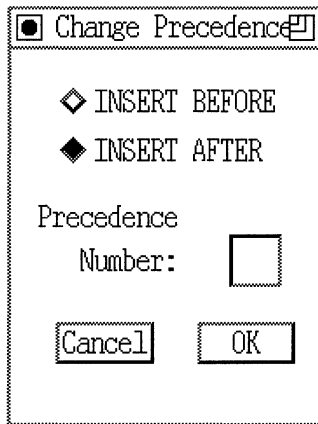


**Figure 2-25. Filters Appearing in the Order of Precedence**

If you need to change the order of precedence, complete the following steps:

1. In the Filters window, select the filter for which you wish to change the precedence.
2. Click on the Reorder button.

The Change Precedence window appears, as shown in Figure 2-26.



**Figure 2-26. Change Precedence Window**

3. Click on the button next to either INSERT BEFORE or INSERT AFTER.
4. Type a number in the Precedence Number box to indicate which filter you should insert the selected filter before or after. For the example shown, if you wish to place the selected filter after filter number 1, type a 1 in the Precedence Number box.
5. Click on the OK button.

You are returned to the Filters window. The filters are now shown in their new order of precedence.



---

# Chapter 3

## Protocol Prioritization and Outbound Filters: An Overview

This chapter includes

- An overview of protocol prioritization and outbound priority filters
- A description of how protocol prioritization works
- Instructions for tuning protocol prioritization to optimize performance on your network
- A description of how priority filters work
- A list of the predefined datalink and IP filtering criteria
- Suggestions for ways you might use priority filters for protocol prioritization

Chapter 4 provides instructions for using the Configuration Manager to configure priorities and filters.

### Protocol Prioritization and Outbound Filters

Normally, a router transmits packets in a first-in/first-out (FIFO) order. Protocol prioritization allows you to instruct the router to use a different transmit order for certain packets on an individual synchronous-line interface. Using protocol prioritization, you can also configure outbound filters that instruct the router to drop certain traffic altogether.



You assign priorities or outbound filters based on packet type, packet length, or any criteria you can identify by an offset in the packet. Depending on how you configure priority for a packet, the router holds the packet in one of three priority queues:

- ❑ High priority queue
- ❑ Normal priority queue
- ❑ Low priority queue

The router drops packets to which you assign outbound filters. The packets with no assigned priority automatically go into the normal-priority queue.

Generally, the router transmits traffic in the high-priority queue before traffic in the normal-priority queue, and transmits traffic in the normal-priority queue before traffic in the low-priority queue.

Two other configurable values in the protocol prioritization scheme, however, also affect the transmission of traffic: *queue depth* and line delay, or *latency*. Queue depth dictates the number of packets a priority queue can hold. Latency dictates the maximum time delay that high-priority traffic can experience.

See “Tuning Protocol Prioritization for Your Network” later in this chapter for a complete description of queue depth and latency and their use in optimizing protocol prioritization on your network.

## Why You Would Use Protocol Prioritization

Protocol prioritization is useful when several different kinds of traffic share a synchronous-line resource. Time-sensitive, smaller-packet traffic (for example, DEC LAT or IP Telnet) may be delayed during the transmission of larger-packet traffic (for example, file transfers). This delay results in loss of connections and poor terminal response.

Protocol prioritization solves this problem by allowing you to assign a high priority to the time-sensitive protocol traffic, thus instructing the router to transmit this traffic before normal- and low-priority traffic.

Outbound filters allow you to drop completely any traffic you do not want on the network.

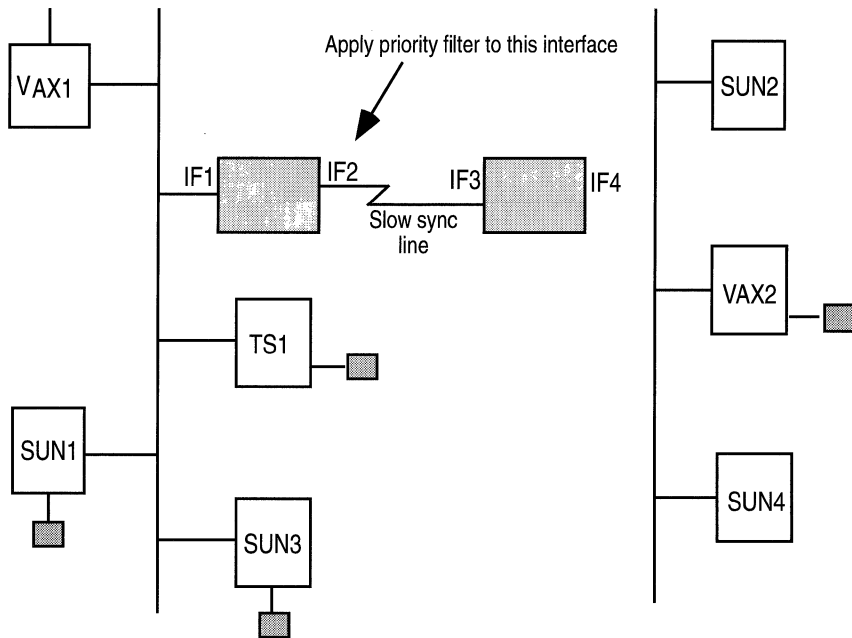
You can also use protocol prioritization to expedite traffic coming from a particular source or going to a certain destination. For example, if you want all traffic from the workstation with the source MAC address 00:00:A2:00:00:12 to take precedence over other traffic, you can assign a high priority to any traffic with that source address.

## Example of Protocol Prioritization

As an example of how protocol prioritization works, consider the network shown in Figure 3-1, and assume the following traffic conditions are typical:

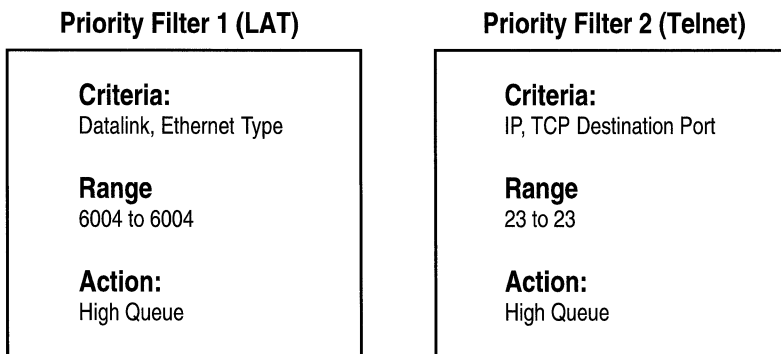
- File transfers from VAX1 to VAX 2
- File transfers from SUN1 to SUN2
- LAT sessions from TS1 to VAX2
- Telnet sessions from SUN3 to SUN4

You need to set up two priority filters to ensure that the router expedites LAT and Telnet traffic from LAN A to LAN B, so that the traffic is not delayed by the file transfers going from LAN A to LAN B. You apply these filters to Interface IF2, since prioritization is concerned with outbound traffic, and the direction of the traffic flow is from LAN A to LAN B.



**Figure 3-1. Applying a Priority Filter in a Sample Network**

Figure 3-2 shows the priority filters you would assign. Note that these filters use predefined criteria.



**Figure 3-2. Allotting High-Priority Status to LAT and Telnet Traffic**

## How Protocol Prioritization Works

As the router operates, network traffic from a variety of sources converges at the synchronous-line interface. The router sorts the traffic into the high, normal, or low queue according to the priority filters that you have configured on this interface. Or, if a queue is full, or you have configured an outbound filter, the router discards or *clips* the traffic.

Protocol prioritization uses either a strict dequeuing algorithm or a bandwidth allocation algorithm to drain the priority queues and send the traffic to the transmit queue (the differences between the two algorithms are discussed in the next section, “Dequeuing Algorithms”). Figure 3-3 illustrates the relationship between the priority queues and the transmit queue.

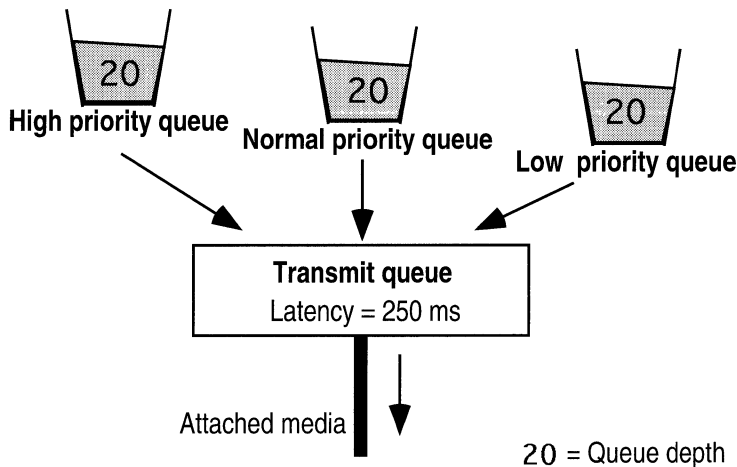


Figure 3-3. Relationship between Priority Transmit Queues

## Dequeuing Algorithms

This section describes the two dequeuing algorithms that protocol prioritization can use: the *bandwidth allocation algorithm* and the *strict dequeuing algorithm*.

## Bandwidth Allocation Algorithm

By default, protocol prioritization uses the bandwidth allocation algorithm to send traffic to the transmit queue. The bandwidth allocation algorithm configures utilization percentages for each of the queues. When the amount of traffic the router has transmitted from a particular queue reaches the utilization percentage you have configured, the router transmits traffic in the next priority queue.

By contrast, if the router uses the strict dequeuing algorithm and there is a great deal of high-priority traffic on the network, the router may never get the chance to transmit normal- and low-priority traffic.

The bandwidth allocation algorithm works as follows:

1. The transmit queue scans the high-priority queue.
  - a. If there is traffic in the high-priority queue, the router empties all packets, up to the utilization percentage you have configured (the default is 70 percent), into the transmit queue and transmits them.
  - b. If there is no traffic in the high-priority queue, the algorithm proceeds to step 2.
2. The transmit queue scans the normal-priority queue.
  - a. If there is traffic in the normal-priority queue, the router empties all packets, up to the utilization percentage you have configured (the default is 20 percent), into the transmit queue and transmits them.
  - b. If there is no traffic in the normal-priority queue, the algorithm proceeds to step 3.
3. The transmit queue scans the low-priority queue.
  - a. If there is traffic in the low-priority queue, the router empties all packets, up to the utilization percentage you have configured (the default is 10 percent), into the transmit queue and transmits them. The algorithm starts again at step 1.
  - b. If there is no traffic in the low-priority queue, the algorithm starts again at step 1.

Figure 3-4 illustrates the algorithm for bandwidth allocation dequeuing.

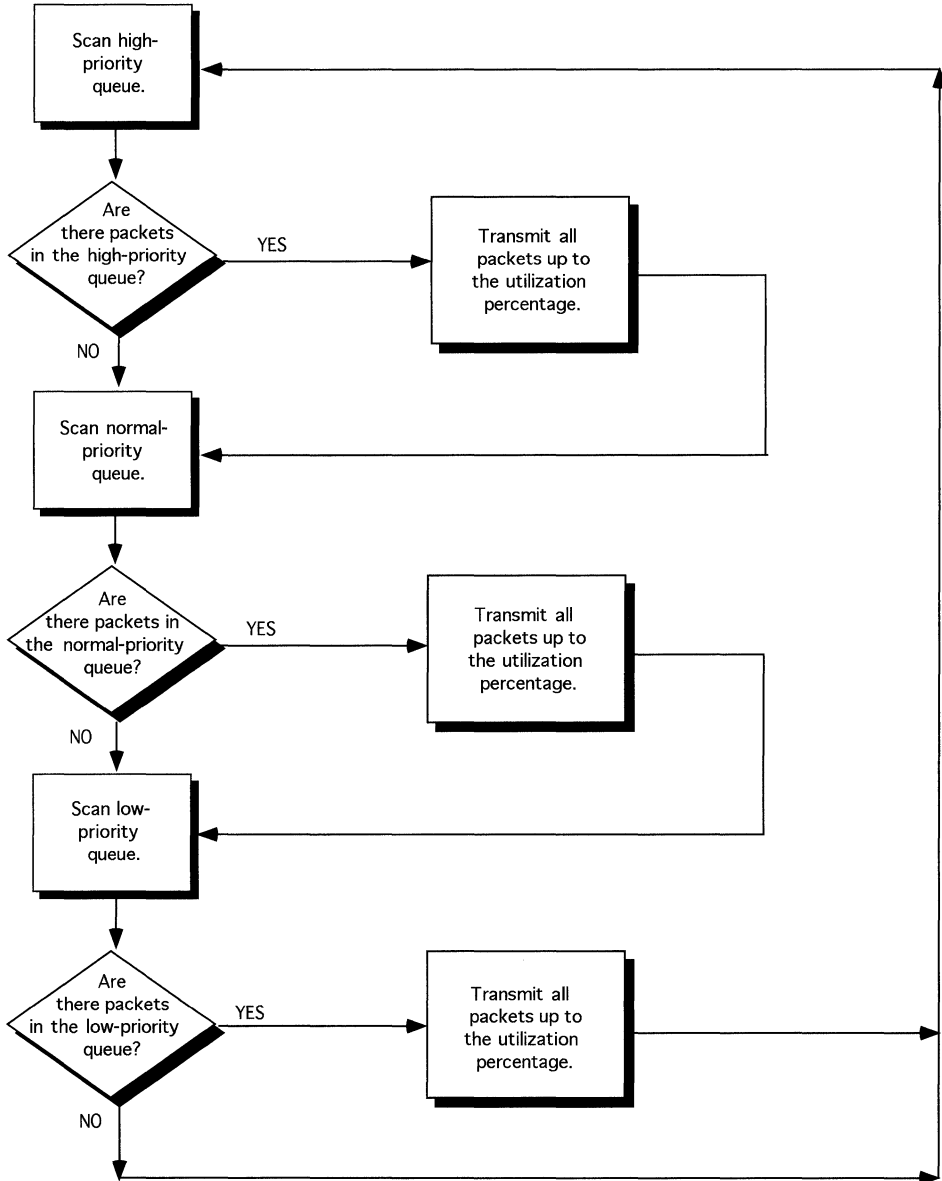


Figure 3-4. Bandwidth Allocation Dequeuing Algorithm

## Strict Dequeuing Algorithm

Protocol prioritization uses the strict dequeuing algorithm to send traffic to the transmit queue. This algorithm works as follows:

1. The transmit queue scans the high-priority queue.
  - a. If there is traffic in the high-priority queue, the router empties all packets, up to the hardware limit, into the transmit queue and transmits them. (The *hardware limit* is the maximum number of packets the router can queue to the transmit queue at one time. It is not a configurable number.)

If the latency value or the hardware limit is reached, the transmit queue starts again, scanning and emptying traffic from the high-priority queue.

If latency or the hardware limit is not reached, the algorithm proceeds to step 2.
  - b. If there is no traffic in the high-priority queue, the algorithm proceeds to step 2.
2. The transmit queue scans the normal-priority queue.
  - a. If there is traffic in the normal-priority queue, the router empties all packets, up to the latency value, into the transmit queue and transmits them.

If latency is reached, the transmit queue starts again at step 1, scanning and emptying traffic from the high-priority queue.

If latency is not reached, the algorithm proceeds to step 3.
  - b. If there is no traffic in the normal-priority queue, the algorithm proceeds to step 3.
3. The transmit queue scans the low-priority queue.
  - a. If there is traffic in the low-priority queue, the router empties all packets, up to the latency value, into the transmit queue and transmits them. At this point, whether or not latency is reached, the algorithm starts again at step 1.
  - b. If there is no traffic in the low-priority queue, the algorithm starts again at step 1.

Figure 3-5 illustrates the strict dequeuing algorithm.

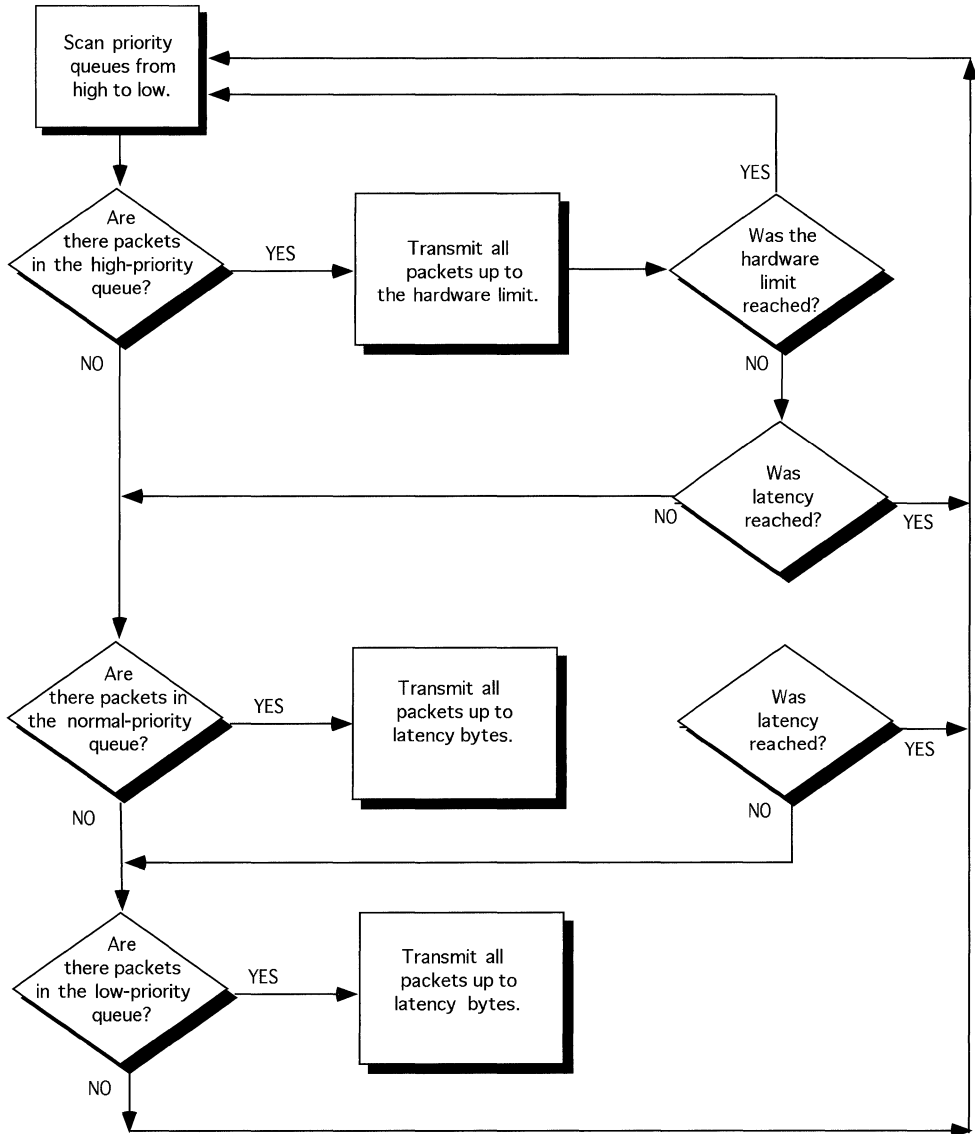


Figure 3-5. Strict Dequeuing Algorithm



## Tuning Protocol Prioritization for Your Network

This section explains how to use queue depth and latency to achieve maximum protocol prioritization results for your network.

### Queue Depth

*Queue depth* is the number of packets each queue can hold. The default value is 20 packets (regardless of packet size).

When you configure the queue depth, you assign buffers (which hold the packets) to the queue. To determine whether there are enough buffers for the traffic flow on your network, examine the following two protocol prioritization statistics, which are kept for each priority queue:

- HiWater Packets Mark

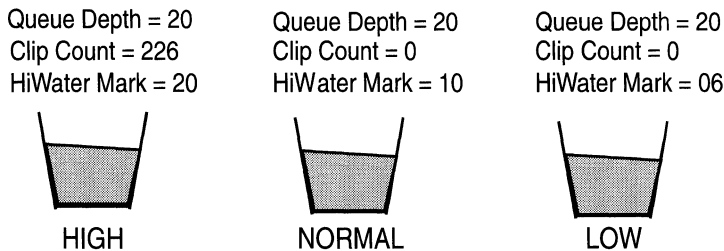
The greatest number of packets that have been in each queue.

- Clipped Packets Count

The number of packets the router has discarded from each queue. (The router discards packets from full priority queues.)

Generally, if a queue's Clipped Packets Count is high, and its HiWater Packets Mark is close to or equal to its queue depth, you have not assigned enough buffers to that queue.

For example, suppose that you use the default queue depth (20 packets) for all priority queues. Upon inspection of the statistics, you see that the high-priority queue's Clipped Packets Count is 226, and its HiWater Packets Mark is 20 (Figure 3-6).



**Figure 3-6. Sample Statistics for the Priority Queues**

The statistics indicate that the high-priority queue has been full at least once and that the router has discarded 226 packets. To determine whether this is simply a transient condition caused by router startup or some other temporary network condition, you may want to reset the Clipped Packets Count and HiWater Packets Mark (you reset the statistics by selecting the Zero Totals option on Site Manager's Protocol Prioritization Statistics window) and check them again later.

If you check the statistics later and they have similar values, you can conclude that you have not assigned enough buffers to the high-priority queue for the amount of high-priority traffic on this interface.

You can do one of two things to alleviate this problem. The first option is to reconfigure the queue depths. Looking at the statistics of the normal- and low-priority queues, you find that the low-priority queue has a Clipped Packets Count of zero, and a HiWater Packets Mark of six. Thus, there have never been more than six packets in the low-priority queue, and the router has not discarded any packets.

At this point, you may choose to reconfigure the low-priority queue depth to ten, and increase the high-priority queue depth to 30. To see whether this reallocation solves the problem, reset the Clipped Packets Count and HiWater Packets Mark counters and check them again later.

Your second option is to remove the high-priority status of some traffic. You should be selective in assigning high-priority status. If there are too many traffic types with high-priority status, the high-priority

traffic could delay the normal- and low-priority traffic, especially if you use the strict dequeuing algorithm (see the “Dequeuing Algorithms” section, earlier in this chapter, for descriptions of the two algorithms the router can use to transmit traffic).

## Latency

*Latency*, or *line delay*, specifies how many normal- or low-priority bytes the router can allocate to the transmit queue (the queue that scans and drains the priority queues and transmits traffic) at any one time. Latency determines, therefore, the greatest delay that a high-priority packet can experience.

Latency is based on the line speed of the attached media. The following formula illustrates the relationship between line speed, bits queued, and the latency value:

$$\text{Latency} = \frac{\text{Bits queued}}{\text{Line speed (bits/sec)}}$$

The default value for latency is 250 ms. This value allows good throughput and also preserves rapid terminal response (rapid echoing of keystrokes and timely response to commands) over most media. You can change the default latency value. Keep in mind, however, that if you configure a higher latency value (thus allowing more room on the transmit queue), the throughput becomes greater, but you sacrifice terminal response. We recommend accepting the default value of 250 ms.

Table 3-1 shows the number of packets of a given size that the router can queue to the transmit queue in order to achieve a latency of 250 ms over different types of media. Note that the information in this table is based on 90 percent bandwidth utilization.

**Table 3-1. Maximum Number of Packets Queued to Achieve 250-ms Latency**

<b>Number of Packets Queued Latency = 250 ms</b>	<b>T1 1.544 MB/s</b>	<b>56 KB/s</b>	<b>9.6 KBs</b>
60 bytes (small pkt)	643 pkts	23 pkts	4 pkts
1514 bytes (Ethernet)	25 pkts	0 (.92) pkts	0 (.16) pkts
4096 bytes (FDDI)	9 pkts	0 (.34) pkts	0 (.06) pkts

## Priority Filters

This section describes priority filters and templates and the parameters you specify to configure them.

When you configure protocol prioritization or outbound filters, you configure a *priority filter*; that is, a set of conditions and an action that you apply to a circuit or interface.

To use priority filters, it is important to understand the difference between a template and a filter. A filter *template* is a reusable, predefined specification for a filter. A template contains a complete filter description but is not associated with an interface or circuit.

Each supported protocol allows up to 31 filters per interface. As filters are added to an interface, they are numbered chronologically in the following fashion: rule #1, rule #2, rule #3, and so on.

The order in which you add filters to an interface determines the filter *precedence*. The first filter has the highest precedence and a rule number of 1. Subsequent filters have decreasing precedence. If two filters apply to the same packet, but the first filter on the interface (rule # 1) accepts the packet and the second filter (rule # 2) drops the packet, rule # 1 has precedence and the packet will be accepted. See the section “Applying Filter Precedence” in Chapter 4 for more information.

## Creating Templates

Each filter template file holds specific filtering information (criteria, ranges, and actions).

You create a filter when you apply (save) a template to one or more interface (circuit). You can apply a single template to as many interfaces as you want. Once you create a template file, it exists for future use unless you delete it.

When you create a template, you first assign it a name. It is a good idea to give each template file a one-word descriptive name. For example, if you are building a template that is going to contain filtering information instructing the interface to queue all LAT traffic to the high queue, you may want to name the template something like *LAThigh*.

After you name a template file, you select criteria and address ranges for checking packets. You then select the action to impose on packets that match the specified criteria and ranges.

Once you specify filtering criteria, ranges, and actions, you save the template file, thus creating a filter template. When you add this template to an interface, you have created a priority filter on that interface.

For a detailed, step-by-step example of creating a filter template from scratch, follow the procedures in Chapter 4.

## Adding a Filter to an Interface

When you want to add a priority filter to an interface, you have several options:

- ❑ If there is a template that contains the exact filtering instructions that you want for this interface, you can apply (save) that template to this interface.
- ❑ If there is a template that contains filtering instructions similar to what you want, you can copy the template, rename it, and edit it.

When you save the changes, you create a new template. You can then apply the new template to any interface for which its filtering instructions are appropriate.

- ❑ If there is no template containing filtering instructions similar to what you want for this interface, you must create a template from scratch.
- ❑ If there is an existing priority filter on the interface that contains filtering instructions similar to what you want, you don't need to use a filter template. You can edit the existing filter directly and save it.

Refer to Chapter 4, “Using the Configuration Manager to Configure Priority Filters” for instructions on each of these options.

**Note:** Because you create filters on a per-protocol basis, you must become familiar with the specific criteria and actions used for filtering by each protocol before applying filters. The next section describes criteria, ranges, and actions.

## Filtering Criteria, Ranges, and Actions

Filters include three components:

- ❑ Criteria

Filtering criteria are parts of a packet, frame, or datagram header that you specify to be checked on each frame. Each filtering criterion has one or more ranges associated with it.

- ❑ Range

A range is associated with a filtering criterion. There must be at least one range per criterion. A range can be just one value, or it can be a set of values. You specify a minimum and a maximum value for each range. For example, if you specify MAC Source Address as a filtering criterion, you must specify which address(es) to filter. You could specify 0x0000A2000001 as the minimum value and 0x0000A2000003 as the maximum value. Then the router would check all outgoing packets to see whether their MAC source

address is between 0x0000A2000001 and 0x0000A2000003, inclusive. If you want a range of only one value, enter only the minimum value; the system automatically uses that value for both the minimum and maximum and sets a range of one value.

❑ Action

An action determines what happens to outgoing packets that match one of the ranges for every criteria in the filter. Actions are

High — Any frame matching the filter is queued to the high queue.

Low — Any frame matching the filter is queued to the low queue.

Length — Once a frame has matched the filter, the frame's length determines the priority queue into which it is placed, based on levels you select.

Accept — Any frame that matches the filter is accepted.

Drop — Any frame matching the filter is dropped.

Log — Any time a frame matches the filter, the router sends notice of that match as an event to the system Events log. You can specify Log in combination with High, Low, or Drop, or Length.

You can select only one Action per criteria. Actions are mutually exclusive, except the Log Action.

**Note:** The router automatically queues any frame that does not match a filter to the normal queue.

## Datalink, IP, and User-Defined Criteria

When you create a priority or outbound filter, you have the option of using either predefined criteria or user-defined criteria. The following sections describe

- ❑ Predefined criteria for the datalink header
- ❑ Predefined criteria for IP traffic
- ❑ User-defined criteria

## Datalink Predefined Criteria

You can configure priority or outbound filters based on the predefined datalink criteria listed in Table 3-2.

**Table 3-2. Predefined Criteria for Datalink Header**

Packet Type or Component	Predefined Criteria
Datalink Type	MAC Source Address* MAC Destination Address* Ethernet Type Novell 802.2 Length 802.2 DSAP 802.2 SSAP 802.2 Control 802.2 SNAP Length 802.2 SNAP Protocol ID 802.2 SNAP Ethernet Type
Source Routing	DSAP SSAP
PPP	Protocol ID
Frame Relay	Two-byte DLCI Three-byte DLCI Four-byte DLCI NLPID Ethernet Type

\* Enter Source-Routed MAC Addresses in the following format:

Wellfleet Standard	Canonical format
PPP	MSB format
Frame Relay WF Proprietary	Canonical format
Frame Relay Standard	MSB format



## IP Predefined Criteria

You can configure priority or outbound filters based on the predefined IP criteria listed in Table 3-3.

**Table 3-3. Predefined Filter Criteria for IP Traffic**

<b>Packet Type or Component</b>	<b>Predefined Criteria</b>
IP Header	Type of Service IP Source Address IP Destination Address UDP/TCP Source Port UDP/TCP Destination Port Protocol
Source Routing	Destination Address* Source Address* SSAP DSAP
PPP	Protocol ID
Frame Relay	Two-byte DLCI Three-byte DLCI Four-byte DLCI NLPID

\* Enter Source-Routed MAC Addresses in the following format:

Wellfleet Standard	Canonical format
PPP	MSB format
Frame Relay WF Proprietary	Canonical format
Frame Relay Standard	MSB format

## User-Defined Criteria

You can configure priority or outbound filters based on specified bit patterns in the packet header. To create a priority filter on user-defined criteria, you specify Reference, Offset, and Length, which together describe the location of the criteria in the outgoing packet, as follows:

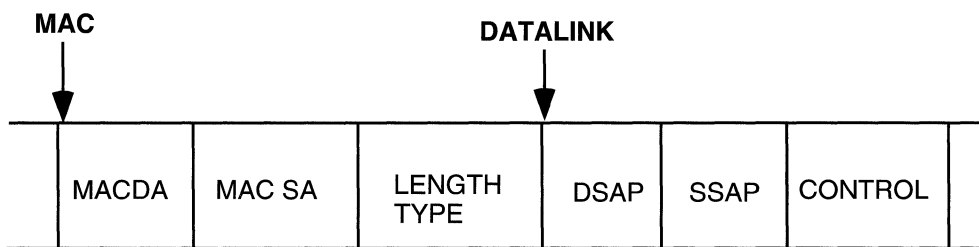
- Reference  
Positions the filtered bit pattern within the outgoing frame.
- Offset  
Positions the filtered bit pattern (measured in bits) in relation to the reference point.
- Length  
Specifies the bit length of the filtered criteria.

After specifying the reference, offset, and length of the criteria, you specify one or more ranges for that criteria.

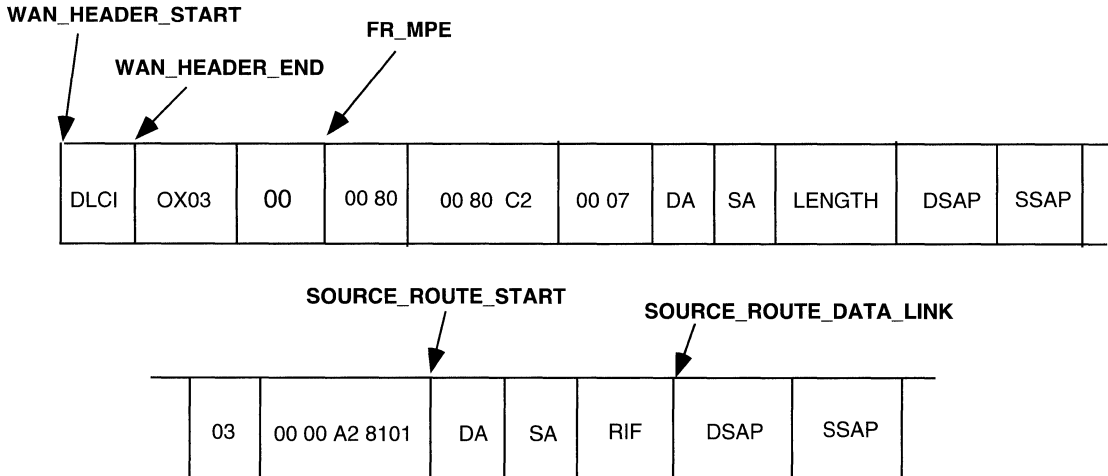
Table 3-4 defines the datalink reference points; Figures 3-7 and 3-8 show examples of where those reference points are located on a packet.

**Table 3-4. Datalink Reference Points**

Reference Point	Definition
MAC	Points to the high-order byte of the destination address.
DATA_LINK	Points to the first byte after the length/type criteria (Data Link Header).
WAN_HEADER_START	Points to the beginning of the header (beginning of the packet) for PPP and Frame Relay.
WAN_HEADER_END	Points to the first byte after DLCI in frame relay and the first byte after the protocol ID in PPP.
FR_MPE	Points to NLPID. (Used in Frame Relay only.)
SOURCE_ROUTE_START	Points to the beginning of the source routing packet, which is the high-order byte of the destination address.
SOURCE_ROUTE_DATA_LINK	Points to the first byte after the RIF field.



**Figure 3-7. Datalink Reference Points on an IEEE 802.3 LLC Header**

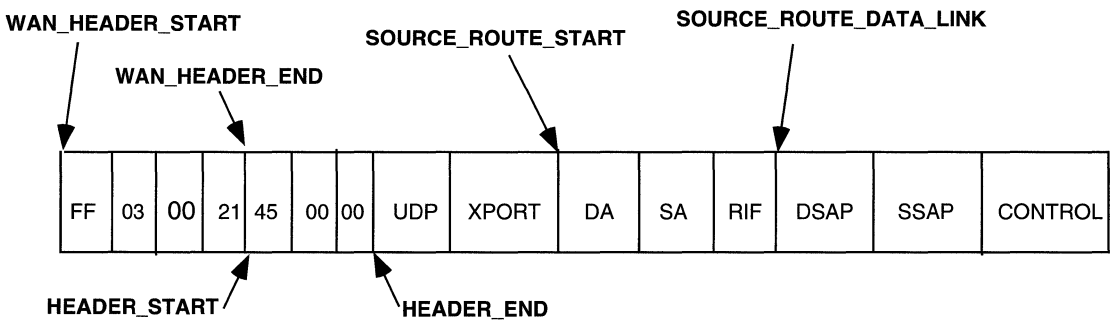


**Figure 3-8. Datalink Reference Points on a Source Routing Packet Bridged over Frame Relay**

Table 3-5 defines the IP reference points, and Figure 3-9 shows an example of where those reference points are located in a packet.

**Table 3-5. IP Reference Points**

Reference Point	Definition
HEADER_START	Points to the first byte in the IP header.
HEADER_END	Points to the first byte after the IP header.
WAN_HEADER_START	Points to the beginning of the header (beginning of the packet) for PPP and Frame Relay.
WAN_HEADER_END	Points to the first byte after DLCI in Frame Relay and the first byte after the protocol ID in PPP.
SOURCE_ROUTE_START	Points to the beginning of the source routing packet, which is the high-order byte of the destination address.
SOURCE_ROUTE_DATA_LINK	Points to the first byte after the RIF field.



**Figure 3-9. IP Reference Points on a PPP Packet with IP Encapsulated Source Routing**

### Example of User-Defined Filter

Suppose that you are bridging VINES traffic over Ethernet, and you want all packets with a destination network number of 1234 (hex) to take precedence over all other traffic. You would complete the following steps to set up filtering criteria (for specific instructions on using Configuration Manager to set up filters, see Chapter 4).

1. Specify an Ethernet Type field of 0xBAD (VINES). Ethernet Type is a predefined criteria.
2. Determine the reference, offset, and length values of the Destination Network field within the header (Figure 3-10).

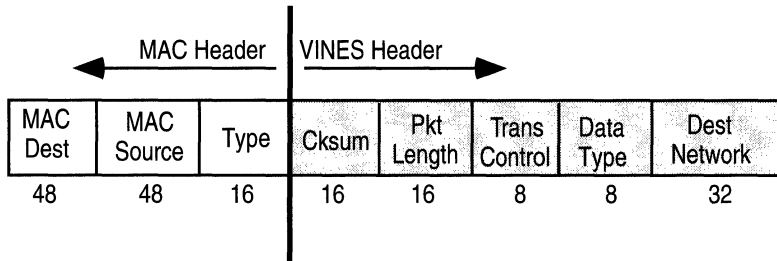


Figure 3-10. VINES Header

3. Set Reference, Offset, and Length as shown in Table 3-6.

Table 3-6. Reference, Offset, and Length Values

Criteria	Value
Reference	MAC (beginning of frame)
Offset	160 bits (sum of all criteria that precede the Destination Network field, or 48+48+16+16+16+8+8)
Length	32 bits

4. Specify the range to go with the criteria described by Reference, Offset, and Length. In this case, you would specify 0x1234 for both the minimum and maximum values.

## Implementation Notes

This section provides some suggestions about ways to use outbound filters for protocol prioritization.

### IP and Datalink Filters for Common Criteria

To configure outbound filters for criteria held in common by IP and datalink, create two filters: one for the IP type and the other for the datalink. To configure a filter to apply to either IP or datalink only, create one filter of the appropriate type.

#### Example

If you want a rule with a priority of High for all Frame Relay traffic with DLCI 400, create filters for both IP and datalink using the DLCI criterion and a range of 400 to 400.

### Protocol Prioritization, Outbound Filters, and Dial Backup

If you want to configure protocol prioritization or outbound filters on a synchronous line for which you have configured a backup line, please keep the following considerations in mind:

- If the primary line is running PPP and the line fails, the router automatically transfers all the priorities and outbound filters you have configured on the primary line to the backup line.
- If the primary line is running a wide-area protocol other than PPP and the line fails, the router does not transfer any datalink priorities or outbound filters to the backup line. You must manually configure datalink priorities and outbound filters on the backup line after that line is activated. The router does transfer IP

priorities or outbound filters to the backup line, no matter what protocol was running on the primary line.

**Note:** Be careful when configuring priorities and filters on the backup line. As soon as the primary line is reactivated, it uses the priorities and filters you configured for the backup line. These priorities and filters may be completely inappropriate for the protocol running on the primary line.

## Prioritizing LAT Traffic

To prioritize your LAT traffic, create a priority filter with the following information:

- ❑ Criteria: Datalink, Ethernet Type
- ❑ Range: 6004 to 6004
- ❑ Action: High Queue

## Prioritizing Telnet Traffic

To prioritize your Telnet traffic, create a priority filter with the following information:

- ❑ Criteria: IP, TCP Destination Port
- ❑ Range: 23 to 23
- ❑ Action: High Queue

## Prioritizing RIP Traffic

To prioritize your RIP traffic, create a priority filter with the following information:

- ❑ Criteria: IP, UDP Destination Port
- ❑ Range: 520 to 520
- ❑ Action: High Queue



## Prioritizing OSPF Traffic

To prioritize your OSPF traffic, create a priority filter with the following information:

- ❑ Criteria: IP, Protocol Type
- ❑ Range: 89 to 89
- ❑ Action: High Queue

## Prioritizing OSPF/BGP Traffic

To prioritize your OSPF/BGP traffic, create a priority filter with the following information:

- ❑ Criteria: IP, Type of Service
- ❑ Range: 0xe0 to 0xe0
- ❑ Action: High Queue

## Prioritizing Spanning Tree Traffic

To prioritize your Spanning Tree traffic, create a priority filter with the following information:

- ❑ Criteria: Datalink, DSAP/SSAP/Control
- ❑ Range: 0x42 to 0x42 | 0x42 to 0x42 | 0x03 to 0x03
- ❑ Action: High Queue

## Prioritizing Native Source Routed Bridge Traffic

To prioritize your native SRB traffic, create a priority filter with the following information:

- ❑ Criteria: Datalink, SNAP, Ethertype
- ❑ Range: 8101 to 8101
- ❑ Action: High Queue

## Prioritizing IP Encapsulated Source Routed Bridge Traffic

To prioritize your IP encapsulated SRB traffic, create a priority filter with the following information:

- ❑ Criteria: IP, UDP Destination Port
- ❑ Range: 12288 to 12288
- ❑ Action: High Queue

## Prioritizing Source Routed SNA Traffic

To prioritize your SRB SNA traffic on Wellfleet Standard, PPP or Frame Relay, create a priority filter with the following information:

- ❑ Criteria: Source Route, DSAP/SSAP
- ❑ Range: 04 to 04 | 08 to 08 | 0c to 0c
- ❑ Action: High Queue



---

# Chapter 4

## Using the Configuration Manager to Configure Priority Filters

This chapter describes how to use the Configuration Manager tool to configure priority filters and edit interface-specific protocol prioritization parameters.

To configure traffic filters, see Chapter 2, “Using the Configuration Manager to Apply Traffic Filters.”

### Configuring Priority Filters

To configure priority filters, you first display the Configuration Manager’s Priority/Outbound Filters window, as described in the next section. Then, use the Priority/Outbound Filters window as follows:

- ❑ Create, copy, or edit a filter template as described in “Preparing Filter Templates.”
- ❑ Apply a filter template to an interface as described in “Creating a Filter.”
- ❑ Change the filtering order as described in “Applying Filter Precedence.”
- ❑ Temporarily disable or enable a filter as described in “Enabling or Disabling a Priority Filter.”
- ❑ Remove a filter from an interface as described in “Deleting a Priority Filter.”

## Displaying the Priority/Outbound Filters Window

To configure outbound priority filters for a particular interface, you must first display the Priority/Outbound Filters window for the circuit's protocol.

Complete the following steps:

1. From the Configuration Manager window, select **Circuits**→**Edit Circuits**. The Circuit List window appears.
2. Select a circuit interface.
3. Click on the Edit button. The Circuit Definition window appears.
4. If you have already added protocol prioritization to the circuit, go to Step 7.

If there has never been a protocol priority on the circuit, select **Protocols**→**Add/Delete**. The Select Protocols window appears.

5. Scroll down the list of protocols to select Protocol Priority, as shown in Figure 4-1.

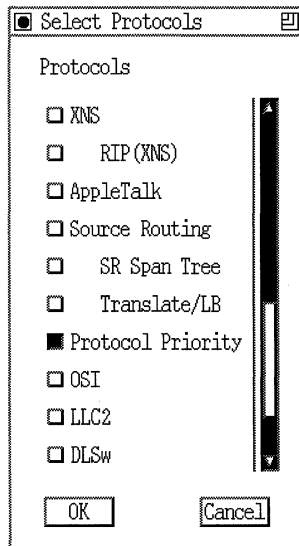
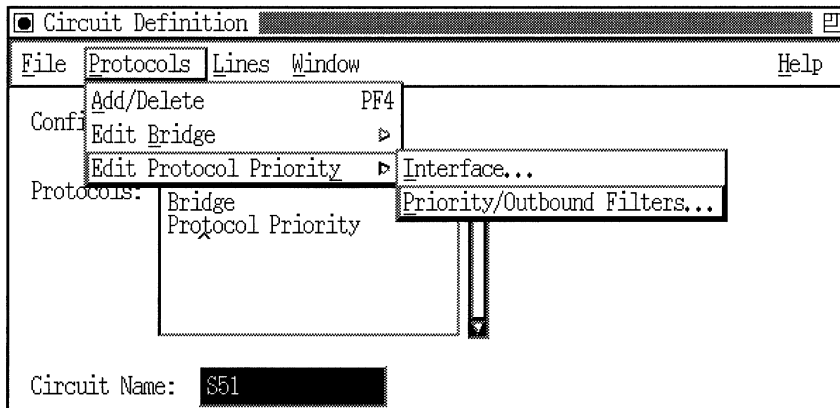


Figure 4-1. Selecting Protocol Priority from Protocols List

- Click on the OK button.

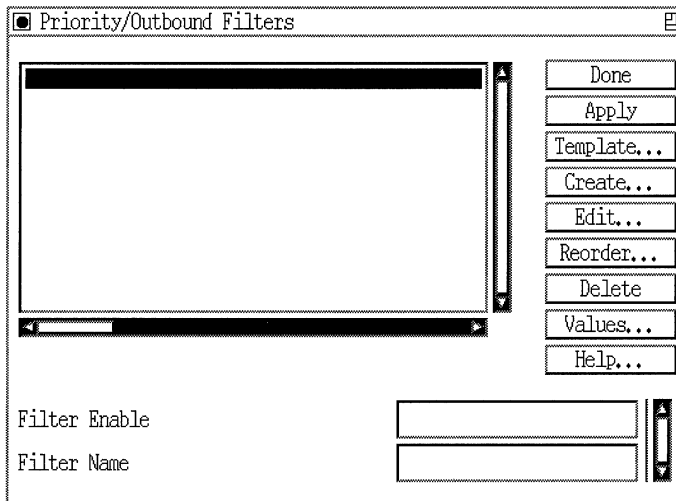
The Circuit Definition window appears.

- Select Protocols→Edit Protocol Priority→Priority/Outbound Filters, as shown in Figure 4-2.



**Figure 4-2. Selecting the Priority/Outbound Filters Window**

The Priority/Outbound Filters window appears (Figure 4-3).



**Figure 4-3. Priority/Outbound Filters Window**

Proceed now to the appropriate section:

- ❑ “Preparing Filter Templates”
- ❑ “Creating a Filter”
- ❑ “Applying Filter Precedence”
- ❑ “Enabling or Disabling a Priority Filter”
- ❑ “Deleting a Priority Filter”

## Preparing Filter Templates

To add a filter template to an interface:

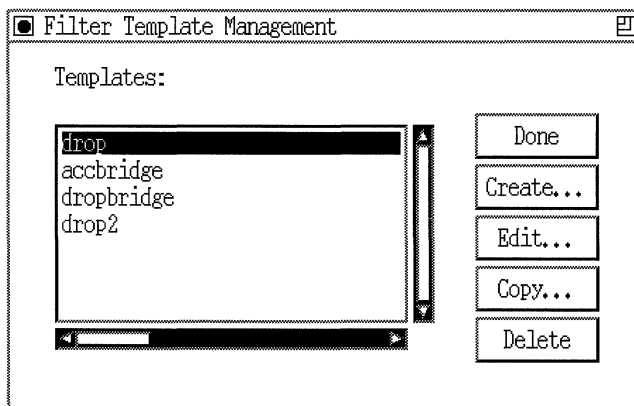
- ❑ Create a new filter template or use an existing template.
- ❑ Add desired filtering criteria, ranges, and actions to a template.

See the “Creating a Filter” section to apply (save) a filter template to an interface.

Prepare a template to use with a selected interface as follows:

1. Start at the Priority/Outbound Filters window (Figure 4-3).
2. Click on the Template button.

The Filter Template Management window appears (Figure 4-4).



**Figure 4-4. Filter Template Management Window**

3. Decide whether to create a new template or use an existing template. More often than not, you will be able to use existing templates to build new ones.

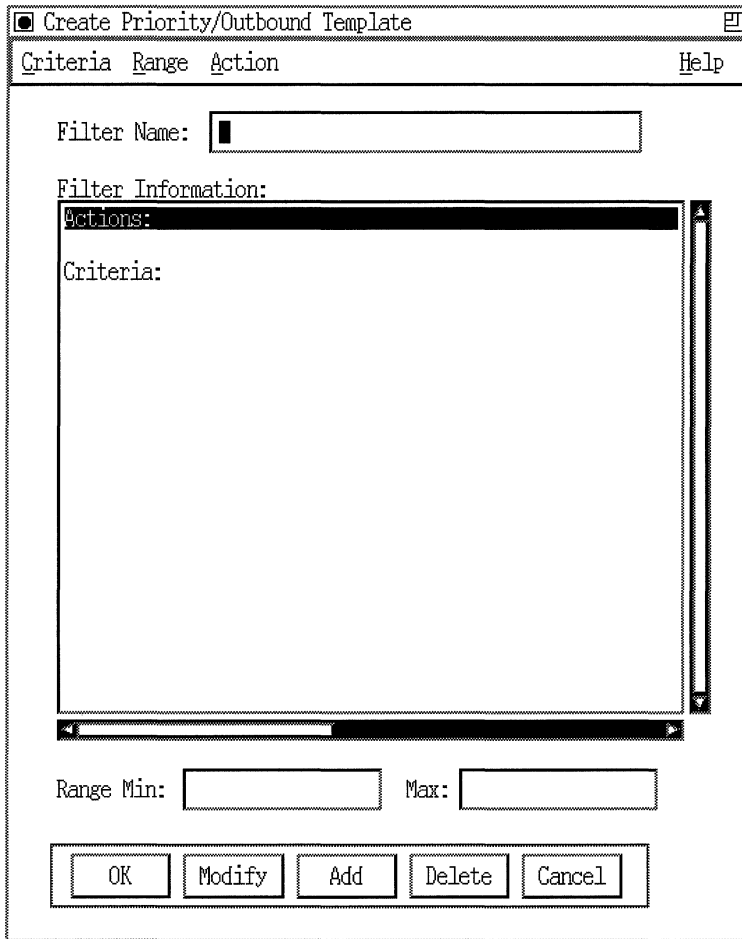
If a filter template exists with information you might use, you can copy or modify the existing template; you don't need to create a new one. Skip the next section, "Creating a New Template," and go now to the steps in "Copying a Template."

If no existing template matches your needs, you must first create a new template for your circuit as described in the next section.

### **Creating a New Template**

4. At the Filter Template Management window (Figure 4-4), click on the Create button.
5. The Create Priority/Outbound Template window appears (Figure 4-5).
6. Enter a descriptive name for the new template in the Filter Name box.
7. Click on the OK button to save the new template.





**Figure 4-5. Create Priority/Outbound Template Window**

8. Proceed with the steps in “Editing a Template.” Skip the next section, “Copying a Template.”

## Copying a Template

When you want to add a filter to an interface, you do not always have to create a new template. You can do one of two things to use an existing template:

- ❑ Copy the existing template, rename it, and then edit it.

This preserves the original template and creates an entirely new template with the same criteria and actions. You can then modify the new version to suit your needs.

- ❑ Edit the existing template.

If you do not want or need to preserve the original template, you can edit it without first copying and renaming it. (Changing a template does not affect interfaces to which the template has already been applied.)

To duplicate an existing template, proceed with the steps below.

To edit an existing template without preserving the original, proceed with the next section, “Editing a Template.”

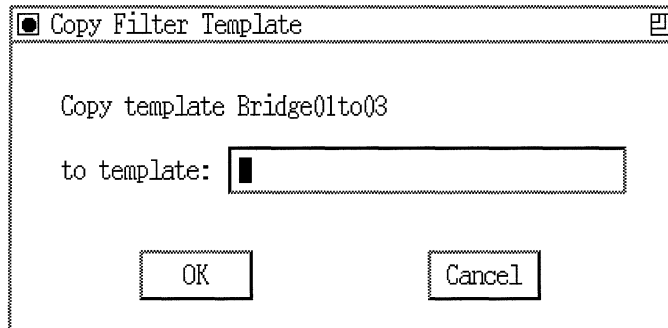
**Note:** You can also edit or copy a template using a text editor. The Configuration Manager stores all templates in a file called *template.ftt*.

1. Start at the Filter Template Management Window (Figure 4-4).
2. If the Filter Template Management box is displaying the name of the template you want to copy, go to the next step.

If the Filter Template is *not* currently displaying the name of the template you want to copy, choose the template you want to copy.

If there is no existing template to match your needs, you must first create a new template for your circuit, as described in the previous section.

3. Click the Copy Button. The Copy Filter Template window appears (Figure 4-6).



**Figure 4-6. Copy Filter Template Window**

4. Enter a name for the new template in the box provided. (Remember to give your template a name that reflects its contents.)
5. Click on the OK button.

You are returned to the Filter Template Management window. The name you just assigned to the new template appears in the Templates scroll box.

Proceed to “Editing a Template” to customize the new template.

## Editing a Template

Once you create or copy a filter template, you can edit the template to apply the filters you want.

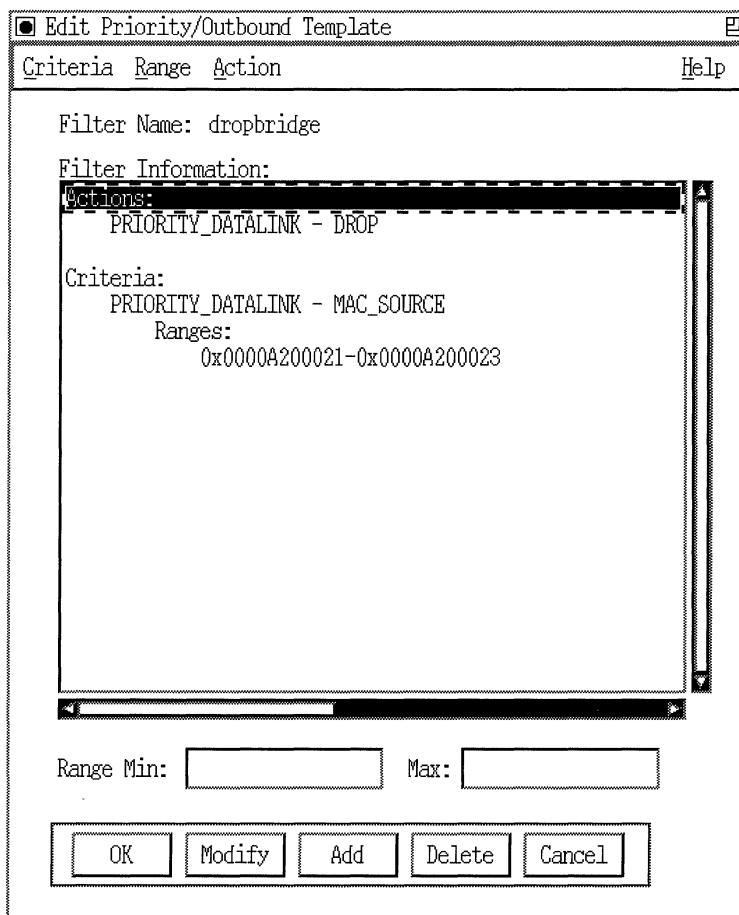
If you want to use the template without editing it, skip this section and go on to “Creating a Filter.”

1. Start at the Filter Template Management window.
2. Select the name of the template you want to edit in the Template scroll box.
3. Click on the Edit button.

The Edit Priority/Outbound Template window appears (Figure 4-7).

You modify the template by adding, modifying, or deleting filter criteria, ranges, and actions, as described in the following sections:

- “Adding Template Criteria”
- “Adding Template Actions”
- “Modifying a Template Range”
- “Deleting Template Criteria, Ranges, and Actions”



**Figure 4-7. Edit Priority/Outbound Template Window**

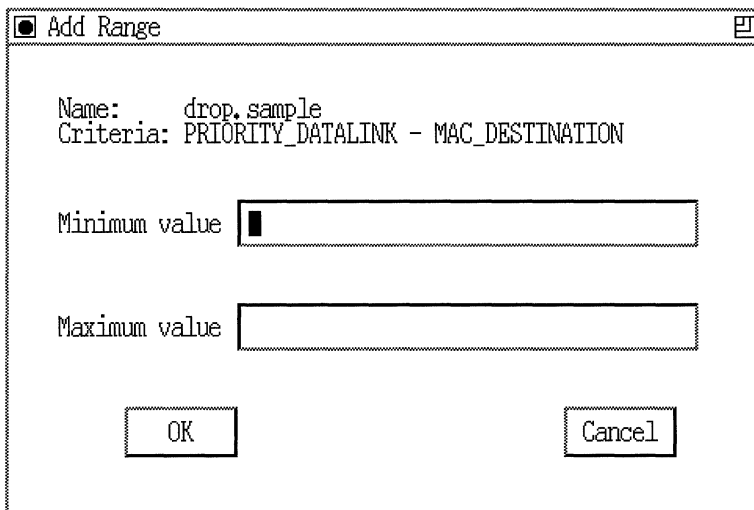
## Adding Template Criteria

To add filter criteria to a template, begin at the Edit Priority/Outbound Template window (Figure 4-7).

1. Select Criteria→Add; then select either Datalink or IP and the protocol-specific criterion you want to add.

The Add Range window appears (Figure 4-8).

**Note:** You must specify at least one range for each criterion.



**Figure 4-8. Add Range Window**

2. In the Minimum value and Maximum value boxes, specify the low and high values of the range you want to filter.

If the range you want consists of just one value, specify that value in both boxes.

**Note:** When you enter values for minimum and maximum value, the Configuration Manager assumes the value is a decimal number. You *must* use the prefix 0x to enter a hexadecimal number.

3. Click on the OK button.

The Edit Priority/Outbound Template window reappears (Figure 4-7). The new criterion and range appear in the Filter Information scroll box.

### Adding Template Actions

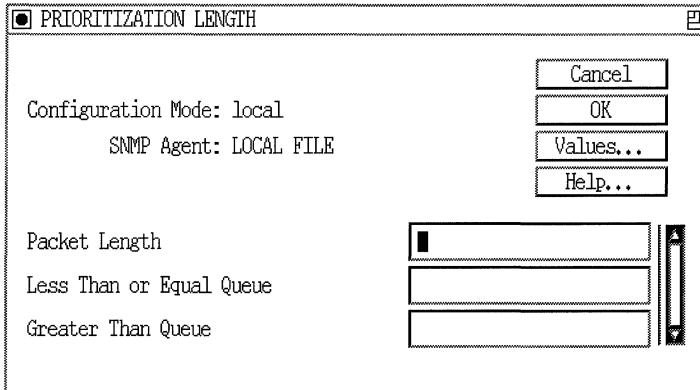
To add, remove, or modify filter actions, begin at the Edit Priority/Outbound Template window (Figure 4-7); then follow the steps below.

1. Select Action, and either IP or Datalink.
2. Select Add Action, then select the action you want to impose on packets that match any of this template's ranges of filtering criteria (High Queue, Low Queue, Length, Drop, Accept, or Log).

**Note:** You can select Log in combination with any of the other choices, or as the only selection.

3. Unless you selected the Length action, skip to Step 5 to confirm the action you selected.

If you select Length, the Prioritization Length window (Figure 4-9) appears. On this screen you can specify that when a packet matches this filter, the priority queue into which it is placed depends on the packet's length.



**Figure 4-9. Prioritization Length Window**

4. On the Prioritization Length window, edit the length parameters, using the following parameter descriptions as guidelines. Click on the OK button when you are done.

<b>Parameter:</b>	<b>Packet Length</b>
Default:	None
Range:	0 to 4608, expressed in bytes
Function:	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 also depends on the values of the Less Than or Equal Queue and the Greater Than Queue parameters.
Instructions:	Either accept the current value, or enter a new value in bytes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.4.1.7

**Parameter: Less Than or Equal Queue**

Default: Normal

Options: High | Low | Normal

Function: Dictates which queue a packet is placed in if its packet length is less than or equal to the value of Packet Length. For example, if Packet Length is 1024 bytes, any packet that is 1024 bytes or smaller is placed in the queue you choose for this parameter.

Instructions: Either accept the default, Normal, or select either Low or High.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.4.1.8

**Parameter: Greater Than Queue**

Default: Low

Options: High | Low | Normal

Function: Dictates into which queue a packet is placed if its packet length is greater than the value of Packet Length. For example, if Packet Length is 1024 bytes, any packet that is 1025 bytes or larger is placed in the queue you choose for this parameter.

Instructions: Either accept the default, Low, or select either Normal or High.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.4.1.9

5. Click on the OK button when you are done editing parameters.

The Edit Priority/Outbound Template window shows the newly selected action in the Filter Information scroll box.



## Modifying a Template Range

If you need to change a range for any criterion, begin at the Edit Priority/Outbound Template window (Figure 4-7); then complete the following steps.

**Note:** You must have at least one range specified for each criterion.

1. Select the range you want to modify by clicking on the range line inside the Filters Information box.
2. With the range selected, click on the Modify button.
3. Use the Range Min: and Max: value boxes (located near the bottom of the window, as shown in Figure 4-7) to specify a new low and high range for the selected filter criterion.

**Note:** When entering range values, you *must* use the prefix 0x to specify a hexadecimal number.

4. Click on the OK button when you are satisfied with the values for all criteria ranges.

## Deleting Template Criteria, Ranges, and Actions

If you want to remove a configured filter criterion, action, or range from a template, begin at the Edit Priority/Outbound Template window (Figure 4-7) and follow these steps:

1. From the Filter Information scroll box, select the criterion, range, or action you want to delete.
2. Click on the Delete button.

A confirmation window (Delete Criteria, Delete Range, or Delete Action) appears.

3. Click on the Delete button to confirm.

You are returned to the Edit Priority/Outbound Template window. The criterion, range, or action you just deleted no longer appears in the Filter Information scroll box.

Repeat this procedure for each item you want to delete from a template.

## Creating a Filter

To create a new filter, you apply a filter template to an interface as follows:

1. Start at the Priority/Outbound Filters window (Figure 4-3).
2. Click on the Create button.

The Create Filter window appears, as shown in Figure 4-10.

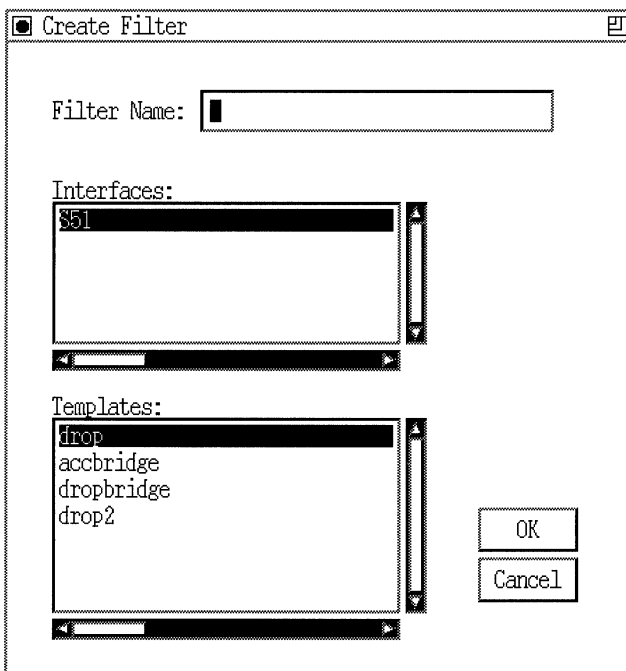


Figure 4-10. Create Filter Window

3. If the correct interface is not already highlighted, select the interface.
4. Select the template you want to use for the new filter.
5. Type a name for the new filter in the Filter Name box.
6. Click on OK.

The Priority/Outbound Filters window (Figure 4-3) appears, with the new filter displayed in the scroll box.

## Editing Priority Filter Criteria, Ranges, and Actions

You can edit priority filters on individual interfaces. When you do, only the filter on that specific interface is affected.

The Edit Priority/Outbound Filters window (Figure 4-11) provides the following options for editing a filter, described in subsequent sections:

- Adding filtering criteria
- Changing criteria ranges
- Adding actions
- Deleting criteria, actions, or ranges

### Adding Criteria

To add a filtering criterion to a priority filter, begin at the Edit Priority/Outbound Filters window (Figure 4-11) and complete the following steps:

1. Select Criteria→Add.
2. Select either the Datalink or the IP option.

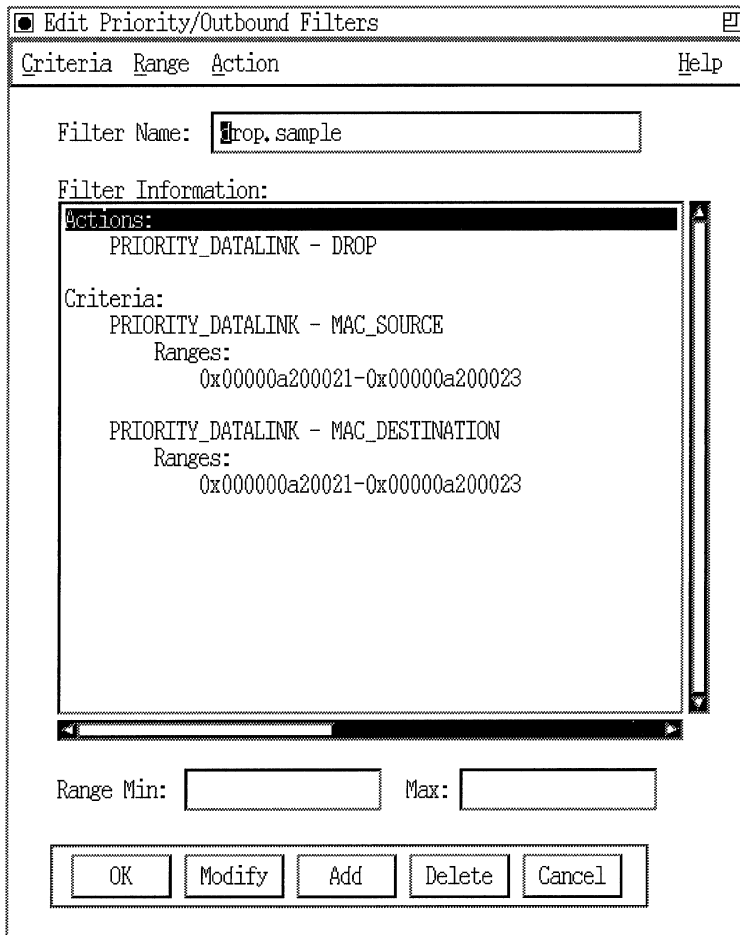
Another menu appears, showing you the header-specific filtering criteria options.

3. Select the criterion you want to add to this template.

The Add Range window appears.

- Specify the low and high ends of the range you want to filter in the Minimum value and Maximum value boxes.

If the range you want to filter consists of just one value, specify that value in the Minimum value box. The system will use that value for both the minimum and the maximum. 0 is not a valid entry for minimum or maximum value.



**Figure 4-11. Edit Priority/Outbound Filters Window**

- Click on the OK button.

The criterion and range you just specified appear in the Filter Information scroll box in the Edit Priority/Outbound Filters window.

## Modifying Ranges

To change a criterion's range, begin at the Edit Priority/Outbound Filters window (Figure 4-7) and complete the following steps:

1. Select the range you want to modify a range from the criteria list in the Filter Information scroll box.
2. Specify the new low and high ends of the range you want to filter in the Minimum value and Maximum value boxes.

If the range you want to filter consists of just one value, specify that value in the Minimum value box. The system will use that value for both the minimum and the maximum. 0 is not a valid entry for minimum or maximum value.

3. Click on the OK button.

The range you just specified appears in the Range List scroll box in the Edit Criteria window. For each range you want to modify, repeat these steps.

4. When you are finished modifying ranges for this criterion, select File→Save (and exit).

The ranges you specify appear in the Filter Information scroll box in the Edit Priority/Outbound Filters window.

## Adding Actions

To add an action to a filter, begin at the Edit Priority/Outbound Filters window (Figure 4-11) and complete the following steps:

1. From the Action menu, select either the Datalink or the IP option; then select the Add Action option.
2. Select the action you want to impose on packets that match any of the template's filtering criteria.

3. Unless you selected the Length action, skip to Step 5 to confirm the action you selected.

If you select the Length action, the Prioritization Length window (Figure 4-9) appears. On this screen you can specify that when a packet matches this filter, the priority queue into which it is placed depends on the packet's length.

4. Edit the length parameters on the screen using the parameter descriptions given earlier in this chapter.
5. Click on the OK button.

The Edit Priority/Outbound Filters window (Figure 4-11) appears. The action you have just added appears in the Filter Information scroll box.

## Deleting Criteria, Ranges, and Actions

If you no longer want to include a criterion, an action, or a configured range in a template, begin at the Edit Priority/Outbound Filters window (Figure 4-11) and complete the following steps:

**Note:** There must be at least one criterion, range, and action for a template to be complete.

1. Select the criterion, range, or action you want to remove in the Filter Information scroll box.

A Delete confirmation (Delete Criteria, Delete Range, or Delete Action window) appears.

2. Click on the Delete button.

The Edit Filter window appears. The criterion, range, or action you just deleted no longer appears in the scroll box.

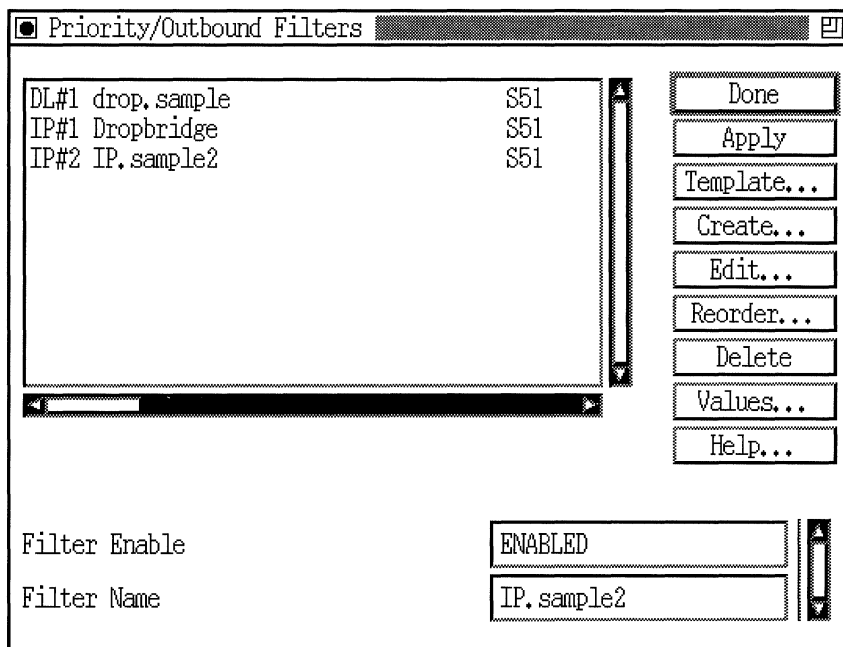
Repeat this procedure for each item you want to delete from a template.

## Applying Filter Precedence

Create filters on the interface in order of precedence.

If possible, use a strategy that accomplishes your filtering goals mainly with drop filters, since these result in faster router performance than accept filters do.

Figure 4-12 shows a sample listing of filters on an interface.



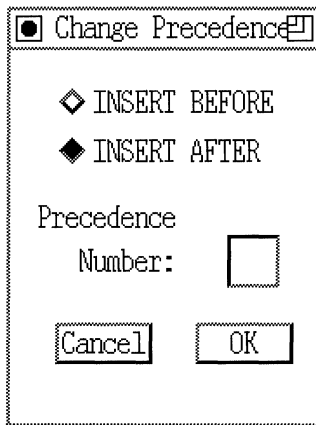
**Figure 4-12. Sample List of Priority Filters**

The first IP filter (called Dropbridge) has the highest precedence and a rule number of 1. Subsequent IP filters created on the interface have decreasing precedence. If the first IP filter on the interface (rule #1) drops a packet and the second filter (rule #2) accepts the same packet, rule #1 has precedence and the packet will be dropped.

If you need to change the order of precedence, complete the following steps:

1. In the Priority/Outbound Filters window (Figure 4-3), select the filter for which you wish to change the precedence.
2. Click on Reorder.

The Change Precedence window appears, as shown in Figure 4-13.



**Figure 4-13. Change Precedence Window**

3. Click on the button next to either INSERT BEFORE or INSERT AFTER.
4. Type a number in the Precedence Number box to indicate which filter you should insert the selected filter before or after. For the example shown, you place the selected filter (#1) after filter number 2 by typing a 1 in the Precedence Number box.
5. Click on the OK button.

You are returned to the Priority/Outbound Filters window. The filters are now shown in their new order of precedence, as shown in Figure 4-14. Compare the order of filters in Figure 4-12 with the order in Figure 4-14.



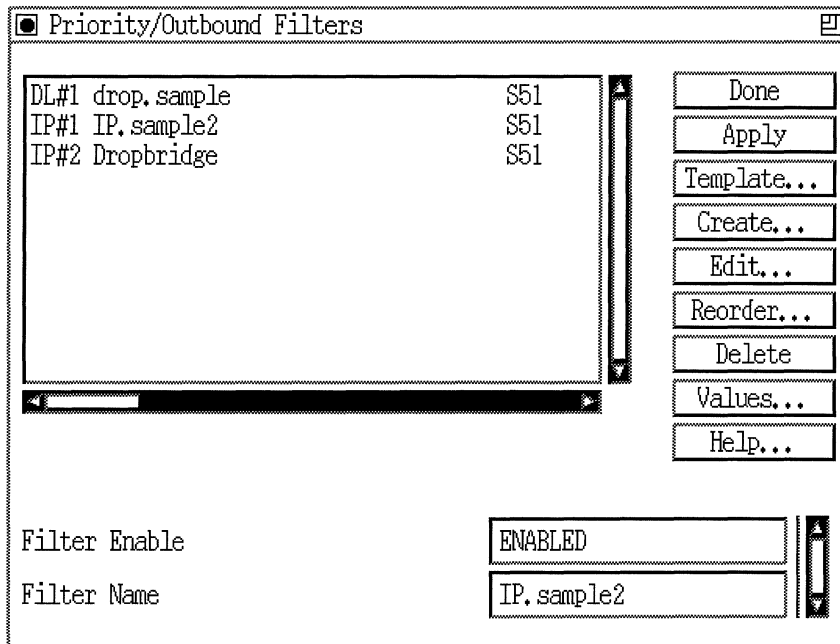


Figure 4-14. Example of Priority Filter Order Change

## Enabling or Disabling a Priority Filter

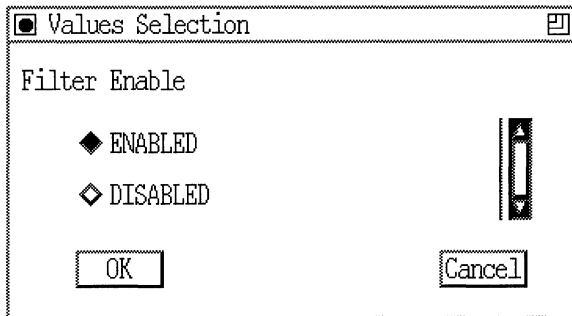
You can disable and re-enable priority filters on individual interfaces. When you do, only the filter on that specific interface is affected. To disable or re-enable a filter, complete the following steps.

1. From the Priority/Outbound Filters window (Figure 4-3) select the circuit/filter pair from the scroll box for which you want to disable or re-enable the filter.

The current filter status appears in the Filter Enable and Filter Name boxes at the bottom of the window.

2. Click on the Values button.

The Values window appears, as shown in Figure 4-15.



**Figure 4-15. Filter Enable/Disable Values Selection**

3. Select ENABLED or DISABLED.
4. Click on the OK button.
5. Repeat the steps for each filter you want to disable or re-enable.
6. Click on the Done button when you are finished.

## Deleting a Priority Filter

To delete a priority or outbound filter from an interface, complete the following steps:

1. From the Priority/Outbound Filters window (Figure 4-3) select the interface/priority filter pair you want to delete.
2. Click on the Delete button.
3. The system deletes the filter from the interface, and the filter no longer appears in the priority filters scroll box in the Priority/Outbound Filters window.

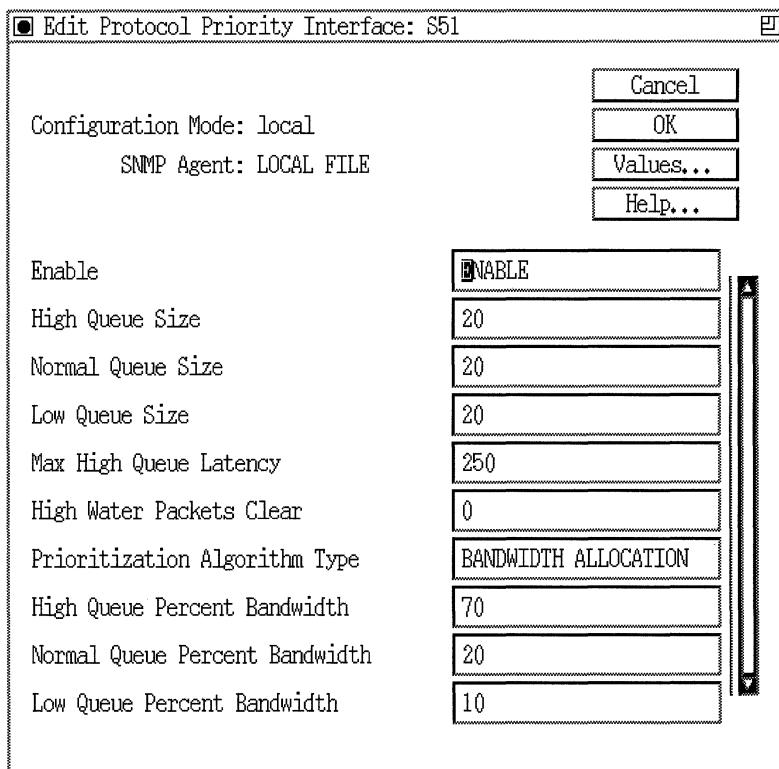
## Editing Protocol Prioritization Parameters

Any circuit to which you have added protocol prioritization uses default values that dictate how priority filters work on the interface. You can edit these parameters according to your network traffic needs. To do so, complete the following steps:

1. From the Circuit Definition window of the Configuration Manager, select **Protocols**→**Edit Protocol Priority**→**Interfaces**.

The Edit Protocol Priority Interface window (Figure 4-16) appears.

This window shows all interfaces to which protocol prioritization has been added, regardless of whether or not there are any priority filters currently active on the interfaces.



**Figure 4-16. Edit Protocol Priority Interface Window**

2. Edit those parameters you want to change, using the descriptions following this procedure as guidelines.
3. Click on the OK button when you are finished editing interface-specific parameters.

## Priority Interface Parameter Descriptions

Use the following descriptions as guidelines when you configure parameters on the Edit Protocol Priority Interface window.

<b>Parameter:</b>	<b>Enable</b>
Default:	Enable
Options:	Enable   Disable
Function:	Toggles protocol prioritization on and off on this interface. If you set this parameter to Disable, all priority and outbound filters will be disabled on this interface. Setting this parameter to Disable is useful if you want to temporarily disable all priority filters, rather than delete them.
Instructions:	Set to Disable if you want to temporarily disable all protocol prioritization activity on this interface. Set to Enable if you previously disabled protocol prioritization on this interface and now want to re-enable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.1.1.2

<b>Parameter:</b>	<b>High Queue Size</b>
Default:	20 packets
Range:	Any integer value
Function:	Dictates the size limit, in packets, of the high-priority queue. For example, if the value of this parameter is 15, there can be no more than 15

---

packets in the high-priority queue at any one time. For more information about how queue depths are used for tuning protocol prioritization in your network, see the section “Tuning Protocol Prioritization for Your Network” in Chapter 3.

**Instructions:** Either accept the default of 20 packets, or enter a new value.

**MIB Object ID:** 1.3.6.1.4.1.18.3.5.1.4.1.1.4

**Parameter: Normal Queue Size**

**Default:** 20 packets (200 packets for Frame Relay)

**Range:** Any integer value

**Function:** Dictates the size limit, in packets, of the normal-priority queue. For example, if the value of this parameter is 15, there can be no more than 15 packets in the normal-priority queue at any one time. For more information about how queue depths are used for tuning protocol prioritization in your network, see the section “Tuning Protocol Prioritization for Your Network” in Chapter 3.

**Note:** For Frame Relay interfaces, a value of less than 200 might cause a broadcast message to be clipped.

**Instructions:** Either accept the default or enter a new value.

**MIB Object ID:** 1.3.6.1.4.1.18.3.5.1.4.1.1.5

**Parameter: Low Queue Size**

**Default:** 20 packets

**Range:** Any integer value

**Function:** Dictates the size limit, in packets, of the low-priority queue. For example, if the value of this parameter is 15, there can be no more than 15 packets in the low-priority queue at any one time. For more information about how queue depths are used for tuning protocol prioritization in your network, see the section “Tuning Protocol Prioritization for Your Network” in Chapter 3.

**Instructions:** Either accept the default of 20 packets or enter a new value.

**MIB Object ID:** 1.3.6.1.4.1.18.3.5.1.4.1.1.6

**Parameter: Max High Queue Latency**

**Default:** 250 ms

**Range:** 100 to 5000 ms

**Function:** Indicates the greatest possible delay for your high-priority traffic. This parameter dictates how many normal- or low-priority bytes can be on the transmit queue at any one time, and therefore the greatest delay that a high-priority packet can experience.

Latency is based on the line speed of the attached media. For a given line speed, the number of bits that can be queued to the transmit queue at any one time is determined by the configured latency value. For more information about how latency is used for tuning protocol prioritization in your network, see the section “Latency” in Chapter 3.

**Instructions:** Either accept the default latency of 250 ms, or enter a new latency value. *We recommend accepting the default latency value of 250 ms.*

**MIB Object ID:** 1.3.6.1.4.1.18.3.5.1.4.1.1.8

**Parameter: High Water Packets Clear**

Default: None

Range: Any integer value

Function: If you change the value of High Queue Size, Normal Queue Size, or Low Queue Size, you can reset the high water marks for each queue to zero by changing the value of this parameter. If the value of this parameter is different from the last time you checked the high water statistics on Site Manager's Protocol Prioritization Statistics window, then the system resets the high water marks for each queue to zero and begins keeping statistics on the maximum number of packets queued in each queue and the number of packets discarded because the new queue depth was exceeded.

For more information about how queue depths are used for tuning protocol prioritization in your network, refer to "Tuning Protocol Prioritization for Your Network" in Chapter 3.

Instructions: Enter a new integer value for this parameter if you wish to clear the high water marks when you change a queue size.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.19

**Parameter: Prioritization Algorithm Type**

Default: BANDWIDTH ALLOC

Options: BANDWIDTH ALLOC | STRICT

Function: Selects the dequeuing algorithm used by protocol prioritization to drain priority queues and transmit traffic. With strict prioritization, the router always transmits traffic in the high-priority queue before traffic in the other queues.

With bandwidth allocation, the router transmits traffic in a queue until the utilization percentage you configure for that queue is reached, and then the router transmits traffic in the next-lower-priority queue.

Instructions: Either accept the default of BANDWIDTH ALLOC or select STRICT.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.24

**Parameter: High Queue Percent Bandwidth**

Default: 70 percent

Range: 0 to 100 percent

Function: If you select the bandwidth allocation dequeuing algorithm, this parameter specifies the percentage of the synchronous line's bandwidth allocated to traffic that has been sent to the high-priority queue. When you set this parameter to something other 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-priority queues (if any traffic is queued) up to the configured percentages for those priorities.

Instructions: Specify the percentage of the line's bandwidth that should be allocated for high-priority traffic. The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.25



**Parameter: Normal Queue Percent Bandwidth**

Default: 20

Range: 0 to 100 percent

Function: If you select the bandwidth allocation dequeuing algorithm, this parameter specifies the minimum percentage of the synchronous line's bandwidth that normal-priority traffic can use.

Instructions: Specify the minimum percentage of the line's bandwidth that should be allocated to normal traffic. The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.26

**Parameter: Low Queue Percent Bandwidth**

Default: 10 percent

Range: 0 to 100 percent

Function: If you select the bandwidth allocation dequeuing algorithm, this parameter specifies the minimum percentage of the synchronous line's bandwidth that low-priority traffic can use.

Instructions: Specify the minimum percentage of the line's bandwidth that should be allocated to low-priority traffic. The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.27

## A

- accept filters, 2-30
- actions, priority filter
  - Accept, 3-16
  - adding, 4-18
  - defined, 3-16
  - deleting from a template, 4-19
  - Drop, 3-16
  - High Queue, 3-16
  - Length, 3-16
  - Log, 3-16
  - Low Queue, 3-16
- actions, traffic filter
  - Accept, 1-6
  - adding, 2-27
  - Bridge, 1-11
    - Flood, 1-11
    - Forward to Circuit List, 1-11
    - Log, 1-11
  - DECnet Phase IV, 1-13
  - defined, 1-6
  - deleting, 2-18, 2-28
  - deleting from a template, 2-18
  - DLSw, 1-24
  - Drop, 1-6
  - IP, 1-13
  - IPX, 1-17
  - Log, 1-6, 1-11, 1-13
  - OSI, 1-22
  - Source Routing
    - Direct IP Explorers, 1-20
    - Forward to Circuit List, 1-21

- VINES, 1-16
- XNS, 1-18
- adding actions
  - priority filter, 4-18
  - traffic filter, 2-16, 2-27
- adding criteria
  - priority filters, 4-16
  - traffic filter, 2-10
- applying templates
  - priority filter, 4-15
  - traffic filter, 2-18

## B

- bandwidth allocation algorithm, 3-5
- blocking filters, 2-30
- Bridge actions, 1-11
- Bridge criteria, 1-6 to 1-10
  - 802.2
    - Control, 1-8, 1-10
    - DSAP, 1-8, 1-10
    - Length, 1-8, 1-10
    - SSAP, 1-8, 1-10
  - SNAP
    - Ethertype, 1-8, 1-10
    - Length, 1-8, 1-10
    - Protocol ID/Organization Code, 1-8, 1-10

---

## C

### changing ranges

- priority filter, 4-18
- traffic filter, 2-14

### Clipped Packets Count, 3-10

### configuring

- priority filters, 4-1
- traffic filters, 2-31

### criteria, priority filter

- adding, 4-10, 4-16
- datalink, 3-17
- Datalink Reference Points, 3-20
- defined, 3-15
- deleting, 4-14
- IP, 3-18
- user-defined, 3-18

### criteria, traffic filter

- adding, 2-10, 2-23

### Bridge

- 802.2, 1-8
- Ethernet, 1-10
- Ethernet type, 1-8
- MAC Destination Address, 1-8, 1-9
- MAC Source Address, 1-8, 1-9
- SNAP, 1-8
- user-defined, 1-9

### DECnet Phase IV, 1-13 to 1-14

- Destination Area, 1-14
- Destination Node, 1-14
- Source Area, 1-14
- Source Node, 1-14

### defined, 1-5

### deleting, 2-13, 2-25

### DLSw

- Destination MAC Address, 1-24
- DSAP, 1-24
- Source MAC Address, 1-24
- SSAP, 1-24
- user-defined, 1-23

### IP, 1-11 to 1-13

- IP Destination Address, 1-12
- IP Source Address, 1-12
- Protocol, 1-12
- TCP Destination Port, 1-12
- TCP Source Port, 1-12
- Type of Service, 1-12
- UDP Destination Port, 1-12
- UDP Source Port, 1-12
- user-defined, 1-12

### IPX, 1-16

- Destination Address, 1-16
- Destination Network, 1-16
- Destination Socket, 1-16
- Source Address, 1-16
- Source Socket, 1-16

### OSI

- Destination Area, 1-22
- Destination System ID, 1-22
- Source Area, 1-22
- Source System ID, 1-22
- user-defined, 1-21

### predefined

- Bridge, 1-8
- DLSw, 1-23
- OSI, 1-21
- Source Routing, 1-18

### Source Routing

- Destination MAC Address, 1-20
- Destination NetBIOS Name, 1-20
- DSAP, 1-20
- Next Ring, 1-20
- Source MAC Address, 1-20
- Source NetBIOS Name, 1-20
- SSAP, 1-20
- user-defined, 1-19

### user-defined, specifying, 1-24 to 1-26

---

VINES, 1-14 to 1-15  
  Destination Address, 1-15  
  Protocol Type, 1-15  
  Source Address, 1-15  
  user-defined, 1-15  
XNS, 1-17  
  Destination Address, 1-17  
  Destination Network, 1-17  
  Destination Socket, 1-17  
  Source Address, 1-17  
  Source Socket, 1-17

## D

Datalink reference points, 3-20  
deleting  
  priority filters, 4-23  
  traffic filters, 2-28  
deleting actions  
  priority filter, 4-14  
  traffic filter, 2-18, 2-28  
deleting criteria  
  priority filter, 4-14  
  traffic filter, 2-13, 2-25  
deleting ranges  
  priority filter, 4-14  
  traffic filter, 2-13, 2-25  
dequeueing algorithms  
  bandwidth allocation, 3-5  
  strict, 3-5  
disabling  
  priority filters, 4-22  
  traffic filters, 2-29  
drop traffic strategy, 2-30  
drop-all traffic filter, 2-30

## E

editing  
  priority filters, 4-16  
  template.ftl file, 4-7  
  traffic filters, 2-20 to 2-28  
enabling  
  priority filters, 4-22  
  traffic filters, 2-29

## F

fields. *See* criteria  
filter templates. *See* templates  
filters  
  inbound. *See* traffic filters  
  outbound. *See* priority filters  
  priority. *See* priority filters  
  traffic. *See* traffic filters  
firewall strategy, 2-30

## H

HiWater Packets Mark, 3-10

## I

IP actions  
  Drop if Next Hop is Unreachable, 1-13  
  Forward, 1-13  
  Log, 1-13  
IP encapsulated SRB traffic  
  prioritizing, 3-27  
IP reference points  
  figure of, 3-22  
  priority filters, 3-22

---

## L

### LAT traffic

- prioritizing, 3-25

- latency, 3-2, 3-12 to 3-13

- line delay (latency), 3-12

## M

### modifying ranges

- priority filter, 4-18

- traffic filter, 2-25

## N

### naming templates

- priority filter, 4-5

- traffic filter, 2-5

### native SRB traffic

- prioritizing, 3-26

## O

### OSPF traffic

- prioritizing, 3-26

### OSPF/BGP traffic

- prioritizing, 3-26

- outbound filters. *See* priority filters

## P

### parameters, Protocol Prioritization

- Enable, 4-25

- Greater Than Queue, 4-13

- High Queue Percent Bandwidth, 4-29

- High Queue Size, 4-25

- High Water Packets Clear, 4-28

- Less Than or Equal Queue, 4-13

- Low Queue Percent Bandwidth, 4-30

- Low Queue Size, 4-26

- Max High Queue Latency, 4-27

- Normal Queue Percent Bandwidth, 4-30

- Normal Queue Size, 4-26

- Packet Length, 4-12

- Prioritization Algorithm Type, 4-28

### precedence

- priority filters, 4-20

- traffic filters, 2-30

### priority filters

- about, 3-13 to 3-16

- adding to an interface, 4-15

- creating templates, 4-4

- deleting, 4-23

- disabling, 4-22

- editing, 4-16

- enabling, 4-22

- precedence, 4-20

- predefined criteria

  - Datalink, 3-17

  - IP, 3-18

- reordering, 4-21

- used in protocol prioritization, 3-3

- with common criteria, 3-24

### priority queues, 3-2

### protocol prioritization

- applying with a filter, 3-14

- clipped packets count, 3-10

- dequeuing algorithm, 3-9

- dequeuing algorithms, 3-5

  - bandwidth allocation, 3-5

  - strict, 3-5

- description of, 3-1

- editing interface parameters, 4-24

- hardware limit, 3-8

- HiWater packets mark, 3-10

- how it works, 3-5

- implementation notes, 3-24

- IP encapsulated SRB traffic, 3-27

- LAT traffic, 3-25

- native SRB traffic, 3-26

---

protocol prioritization (continued)

OSPF traffic, 3-26

OSPF/BGP traffic, 3-26

parameters

Enable, 4-25

Greater Than Queue, 4-13

High Queue Percent Bandwidth, 4-29

High Queue Size, 4-25

High Water Packets Clear, 4-28

Less Than or Equal Queue, 4-13

Low Queue Percent Bandwidth, 4-30

Low Queue Size, 4-26

Max High Queue Latency, 4-27

Normal Queue Percent Bandwidth,  
4-30

Normal Queue Size, 4-26

Packet Length, 4-12

Prioritization Algorithm Type, 4-28

queue depth, 3-10

using to tune protocol prioritization,  
3-10

RIP traffic, 3-25

Spanning Tree traffic, 3-26

SRB SNA traffic, 3-27

Telnet traffic, 3-25

transmit queue, 3-5

usefulness of, 3-2

## Q

queue depth, 3-2, 3-10

## R

ranges, priority filter

defined, 3-15

deleting, 4-14

modifying, 4-18

ranges, traffic filter

changing, 2-25

defined, 1-5

deleting, 2-13, 2-25

entering, 1-5

reference points

Datalink, 3-20

RIP traffic

prioritizing, 3-25

## S

Source Routing

actions, 1-20

Spanning Tree traffic

prioritizing, 3-26

specifying

user-defined criteria

priority filters, 3-18

traffic filter, 1-24 to 1-26

SRB SNA traffic

prioritizing, 3-27

strict dequeuing algorithm, 3-5

## T

Telnet traffic

prioritizing, 3-25

template.flr file, editing, 4-7

templates, priority filter

about, 3-13

actions, 3-16

adding actions, 4-11

adding criteria, 4-10

applying to an interface, 3-14

copying, 4-7

creating, 3-14, 4-4

criteria, 3-15

deleting actions, 4-19

---

templates, priority filter (continued)

- deleting criteria, 4-14, 4-19
- deleting ranges from, 4-14
- editing, 4-7
- naming, 4-5
- ranges, 3-15
- renaming, 4-8

templates, traffic filter, 1-3 to 1-4

- about, 1-3
- adding actions, 2-16
- adding criteria, 2-10
- applying to an interface, 2-18
- copying, 2-6
- creating, 1-3, 2-4
- deleting criteria, 2-13
- deleting ranges, 2-13
- editing, 2-6
- modifying ranges, 2-14
- naming, 2-5
- renaming, 2-7
- using, 1-4

traffic

- dropping/blocking strategy, 2-30
- forwarding strategy, 2-30
- undesireable, 2-30

traffic filters

- about, 1-1 to 1-3
- adding to an interface, 1-4, 2-18
- applying to an interface, 1-3, 2-18
- blocking, 2-30
- components of, 1-2
- configuring, 2-31
- creating, 2-18
  - templates, 2-3 to 2-18
- deleting from an interface, 2-28
- drop-all, 2-30
- enabling, 2-29
- precedence, 1-3, 2-30
- purpose of, 1-2
- templates, 1-3 to 1-4

## U

unwanted traffic, 2-30

user-defined criteria

- priority filters, 3-18
  - IP reference points, 3-22
  - length, 3-19
  - offset, 3-19
  - reference, 3-19
- traffic filters, 1-24 to 1-26







# Bay Networks

The Merged Company of SynOptics and Wellfleet

8 Federal Street  
Billerica, MA 01821



Printed in U.S.A. on Recycled Paper