



Using Filters

This chapter describes how to use filters to improve the performance of your bridge.

Here's what you'll find in this chapter:

- [Overview, page 9-2](#)
- [Using the Filter Menu, page 9-2](#)
- [Filtering Multicast Addresses \(Multicast\), page 9-2](#)
- [Filtering Node Addresses \(Node\), page 9-3](#)
- [Filtering Protocols \(Protocol\), page 9-4](#)
- [Accessing Packet Direction \(Direction\), page 9-8](#)

Overview

If your bridge is connected to an infrastructure with a large amount of multi-protocol traffic, you may be able to reduce the amount of radio traffic by blocking out (filtering) unneeded addresses or protocols. Filtering is especially important for battery-operated radio nodes that might otherwise have to waste considerable battery power receiving irrelevant multicast messages.

Using the Filter Menu

Use the *Filter* menu to control packet filtering.

Navigation: Choose **Main > Filter**

Filter Menu		
Option	Value	Description
1 - Multicast	[menu]	- Multicast address filtering
2 - Node	[menu]	- Node address filtering
3 - Protocols	[menu]	- Protocol filters
4 - Direction	[to_radio]	- Packet direction affected by filters

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44786

Filtering Multicast Addresses (Multicast)

The *Multicast* menu controls the filtering of multicasts based on the actual multicast address.

Navigation: Choose **Main > Filter > Multicast**

Filter Multicast Menu		
Option	Value	Description
1 - Default	[forward]	- Default multicast action
2 - Show		- Display the multicast filters
3 - Add		- Add a multicast address filter
4 - Remove		- Remove a multicast address filter

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44787

Setting the Default Action (Default)

The *Default* option controls the filtering of multicasts whose addresses are not in the table. You may pick one of the following actions:

- **Discard:** multicasts with no table entries are not forwarded out of the radio network.
- **Forward:** multicasts with no table entries are forwarded out of the radio network.

Displaying the Filters (Show)

The *Show* option displays the Multicast Filters screen. The filters are stored in the association table. The display of the multicast filters follows the format of the normal association display. At the end of each line the filter action for each address is displayed.

The multicast filters can also be displayed by choosing **Main > Association > Display**. See Chapter 8, “Using the Association Table.”

Adding a Multicast Filter (Add)

The *Add* option adds a multicast filter if there are special multicast addresses you want to filter differently than the default. You are prompted for the address and then for an action to be applied to this address only.

Removing a Filter (Remove)

The *Remove* option removes one or all of the non-default filters. The action for the removed entries reverts to the default action.

Filtering Node Addresses (Node)

The *Node* option controls the forwarding of packets based on the source node addresses. Type specific node filters by specifying the 6-byte infrastructure address of the node or by specifying its IP address. If the IP address is used, the bridge determines the infrastructure address associated with the IP address and uses it for the actual filtering. You can filter packets based on the source address in the received packet.

Navigation: Choose **Main > Filter > Node**

Filter Node Menu		
Option	Value	Description
1 - Ethdst	[forward]	- Destination address from ethernet
2 - Display		- Display the node address filters
3 - Ipdisplay		- Display the IP address filters
4 - Add		- Add a node address filter
5 - Remove		- Remove a node address filter
Enter an option number or name, "=" main menu, <ESC> previous menu		
> █		

44788

Setting the Default (Ethdst)

The *Ethdst* option sets a default that applies to those packets whose addresses do not have entries in the filter table. Options are **forward** or **discard**. Source address filtering is *forward* by default.

Displaying the Node Address Filters (Display)

The *Display* option allows you to view the table of controlled addresses. The filters are stored in the association table so that they can be accessed quickly. The display of the filters follows the format of the normal association display. At the end of each line the filter action for each address is displayed.

The node filters can also be displayed by choosing **Main > Association > Display**. See Chapter 8, “Using the Association Table.”

Displaying the IP to Network Address Table (IPdisplay)

The *IPdisplay* option displays the relationship between the IP address and its infrastructure address. When a node address filter is entered by an IP address, the bridge first determines the infrastructure address associated with this IP address. The actual filtering is based on the infrastructure address.

Updating Specific Node Address Filters (Add/Remove)

The *Add* option adds filters for specific addresses to the filter table. You will be prompted for the infrastructure address or IP address of the node to which the filter applies. You will then be asked for the filter action to be applied to this address, which is either *filter* or *discard*.

To remove one or all specific node filters use the *Remove* option. You can enter the keyword **all**, a single node's infrastructure address, or a single node's IP address. Once removed, the filter action for the removed addresses reverts to the default value.

Filtering Protocols (Protocol)

The *Protocol* option bases the filtering decision on the type of protocol used to encapsulate the data in the packet. This type of filtering can have the most value in almost all situations and is the preferred method of filtering. With this type of filtering you can set the bridge to only forward those protocols that are being used by the remote nodes. Selecting protocols is easier than setting up filters based on addresses. The bridge can be set up to monitor and record the list of protocols currently being forwarded over the radio. It records the protocols found, how many packets are encountered, and whether the packet comes from the LAN or the radio.

To set up the protocol filters, start the monitor and let it run for a while under normal use. Add filters by selecting the protocols from the monitor list. There is a default action for those protocols not in the list of explicitly filtered protocols. If you know exactly which protocols are going to be used by the radio nodes, set the default action to **discard**; then add filters to forward only those protocols that will be used. If you are not sure of all the protocols that will be used but you know that there are certain protocols you will not use, you should set the default action to **forward**; then add filters to discard only those protocols you will not use. For filtering purposes, the bridge assumes that the data portion of the packets is in one of two forms:

- The first 16 bits of the data portion contains a value that is greater than the maximum data size (1500 bits). The value is assumed to be a protocol identifier that may be used to determine which protocol is being used within the packet.
- The first 16 bits of the data portion contains a value that is less than the maximum data size. The value is interpreted as a frame length and it is assumed that a IEEE 802.2 Logical Link Control (LLC) header follows the length.

The format of the LLC header is as follows:

- DSAP, 8 bits, destination service access point (DSAP)
- SSAP, 8 bits, source service access point (SSAP)
- CTL, 8 bits, control field

If the control field has a value 3 (for an un-numbered information frame), then this header may be followed by:

- OUI, 24 bits, Organization Unique Identifier (OUI)
- SAP-PROT, 16 bits, Protocol Identifier

You can set up filters based on either a protocol identifier or a DSAP/ SSAP combination. If the filter is based on SAPs and the control field has a value of 3, the packet can also be filtered based on the OUI and LLC protocol fields. Both types of filters can also use a variable length bit mask of the packet contents to further specify which packets should be filtered.

Navigation: Choose **Main > Filter > Protocols**

Filter Protocols Menu		
Option	Value	Description
1 - Default	[off]	- Default action
2 - Unicast	[off]	- Filter unicast packets
3 - Display		- Display the protocol filters
4 - Add		- Add a protocol filter
5 - Remove		- Remove a protocol filter
6 - Length	[22]	- Length of packet data to log
7 - Monitor	[off]	- Protocol monitoring enabled
8 - Show		- Show forwarded protocol list
9 - Clear		- Clear forwarded protocol list

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44789

Setting the Default Action (Default)

The *Default* action is used for a packet whose protocol does not match any entry found in the table. It may be set to:

- **Off:** protocol filtering is not done. It is a waste of processing power for the bridge to examine each packet for its protocol only to discover no protocols need monitoring.
- **Discard:** packet is not forwarded out of the radio network.
- **Forward:** packet is forwarded out of the radio network.

Enabling Unicast Packet Filtering (Unicast)

The *Unicast* option filters unicast packets. By default, the bridge applies the protocol filters only to multicast packets. If a packet is directed to a radio node, it is likely the protocol in the packet is being used by the radio node.

Displaying the Filters (Display)

The *Display* option allows you to view the list of protocol filters you have added.

Adding a Filter (Add)

The *Add* option adds a protocol filter and specifies the type of action required. There are several ways to add a filter:

- Use a predefined filter
- Use a filter from the monitor table built by the bridge
- Manually add a filter

To add a predefined filter, follow these steps:

-
- Step 1** Type **add**.
- Step 2** Type one of the predefined strings: *inet*, *novell*, *netbios*, *tcp*, *ip_subprotocol*, *ip_port*, or *ip_address* and press **Enter**.
- Step 3** Type the action to take when the protocol is encountered: **discard**, **forward**, **high_priority** or **log**, and press **Enter**.
-

If protocol monitoring is enabled, when you select *add*, the current monitor table is displayed. Follow these steps to select a monitored protocol:

-
- Step 1** Type the desired filter protocol's number that is displayed at the start of each line of the monitor display. If the monitored protocol was unrecognized and was not given a name, you are prompted to assign a name.
- Step 2** Type the action to take when the protocol is encountered: **discard**, **forward**, **high_priority** or **log**, and press **Enter**.
-

To start adding a filter manually, follow these steps:

-
- Step 1** Type **add** and give the filter a name that does not start with a number and does not match one of the predefined names.
- Step 2** Type the action to take when the protocol is encountered: **discard**, **forward**, **high_priority** or **log**, and press **Enter**. The following message appears:

```
Enter one of [protocol, snap+protocol, llc]:
```

- Step 3** Choose whether the protocol is defined by an Ethernet or SNAP+protocol identifier or by an LLC header. If you type **protocol**:

- a. The following prompt appears:

```
Type a value in hex from 200h to ffffh:
```

Type the value for the protocol identifier to be filtered and press **Enter**. The following prompt appears:

```
Type one of [a mask start position, none]:
```

The protocol identifier value allows you to specify a bit mask and corresponding hexadecimal value to be applied to the packet. These two values must match the packet contents before the protocol is identified. You must first specify a mask start position in the packet and match the mask value. The mask start position value should be a 0-based byte offset from the start of the data portion of the frame (after the MAC layer header). If you set the position to *none*, no mask is tested.

- b. Type a mask start position value (or **none**, if applicable) and press **Enter**. The following prompt appears:

Type a hex value of 1 to 30 characters:

- c. Type the value to be matched as a string of up to 30 hexadecimal digits and press **Enter**. If the numbered digits are odd, the mask value is adjusted to ignore the lowest 4 bits of the corresponding byte. Then the following prompt appears:

Type a hex don't care mask of 1 to 6 characters:

This value allows you to type a string of hexadecimal digits to indicate which bits of the packet data are meaningful. A bit set in this value causes the corresponding bit in the packet to be ignored. Therefore, a 0 mask means that the packet contents must exactly match the previous value typed. If the mask entered is shorter than the value entered it is automatically extended to the correct length with zeros.

- d. Type the applicable hexadecimal digits and press **Enter**.

For example, to type a mask that matches the value 4128H in the 16th byte data portion of the packet and have the high bit of each byte ignored, complete as follows:

```
Type one of [a mask start position, none]: 15
Type a hex value of 1 to 30 characters: 4128
Type a hex don't care mask of 1 to 6 characters: 8080
```

If you type **llc** the following prompt appears:

Type a value in hex of ffffh or less:

- a. Type a 16-bit value for the DSAP/SSAP combination (with the DSAP being in the high 8 bits) and press **Enter**. The following prompt appears:

Type one of [a OUI value in hex of fffffffh or less, any]:

This value is used to specify an OUI value to further refine the protocol identification.

If you type a *OUI value in hex of fffffffh or less*, it must match the protocol field in addition to the SAP value.

If you type *any*, the protocol values are not checked and the protocol is defined only by the SAP values.

- b. Type the applicable OUI value or **any** and press **Enter**.

If you typed an OUI value, the following prompt appears:

Type one of [a LLC protocol value in hex of ffffh or less, any]:

- c. Type the applicable LLC protocol value or **any** and press **Enter**. You are then prompted for a mask description as described below.

If you type a LLC protocol value in hex of *ffffh* or less, the mask must match the protocol field in addition to the SAP and OUI values.

If you type *any*, the protocol values are not checked and the protocol is defined only by the SAP and OUI values.

Removing an Entry (Remove)

The *Remove* option removes a protocol filter entry. You can remove all filters by typing **all** or a single entry by typing the number assigned to the filter shown at the start of the line in the filter display.

Length of Data Displayed in Log Action (Length)

The *Length* option displays the contents of packets being forwarded to the radio. Use this option to setup the filter mask values. If you add a protocol filter whose action is *log*, each time the filter matches, the contents of the data portion of the packet (after the MAC header) is displayed on the console (in hexadecimal) for a length in bytes determined by the value of this option. The contents of the data portion displayed in the information log consists of:

- “p”
- Id number of the filter shown on the Protocol Filters screen
- Bytes of the packet displayed in hexadecimal

More than one protocol at a time can be set with a filter action of “Log.” The following is an example of a protocol filter log entry:

```
p2: 01 e0 ff ff 01 e0 00 04 00 00 01 65 ff ff ff ff ff ff 04 52 00 00
```

Protocol Monitoring (Monitor/ Show/ Clear)

The bridge allows you to create and display a list of the protocols being forwarded by the bridge. This allows you to test if packets that contain data for unused protocols are being forwarded to the radio nodes. After it is enabled by the *Monitor* option, the bridge begins to examine the protocol used in each packet forwarded. If the protocol is not already in the list, an entry is created. Otherwise, the packet count for the given protocol is incremented.

The *Show* option displays the list of currently forwarded protocols.

The *Clear* option cleared the list of found protocols. You can use either the **Clear** command or type a capital **C** at the re-display prompt of the **Show** command to invoke the *Clear* option.

Accessing Packet Direction (Direction)

The *Direction* option controls the direction a packet is traveling before it is affected by the filters. Select one of the following choices:

- **To_radio**: only packets from the LAN will have filters applied. Packets from the radio are not filtered, resulting in a reduction of the amount of LAN traffic to the radio infrastructure.
- **Both**: packets in both directions are filtered.