Filtering Flows

This chapter contains the following sections:

- About Cisco Monitor Manager Networks, page 1
- About Forwarding Path Options, page 1
- About Filters and Rules, page 2
- Adding a Filter, page 2
- Editing a Filter, page 6
- Deleting a Filter, page 9
- Adding a Rule, page 9
- Modifying a Rule, page 11
- Deleting a Rule, page 13

About Cisco Monitor Manager Networks

A Cisco Monitor Manager network consists of one or more Cisco Nexus 3000 and 3100 Series switches with Cisco Plug-in for OpenFlow dedicated for connecting multiple spanned ports and network taps from the production network infrastructure. Cisco Extensible Network Controller (XNC) programs the switches using the OpenFlow protocol. Cisco Monitor Manager filters the packets that travel the network and delivers them to a pool of connected monitoring devices.

About Forwarding Path Options

Cisco Monitor Manager supports the following forwarding path options:

- Multipoint-to-Multipoint—With the Multipoint-to-Multipoint (MP2MP) forwarding path option, both the ingress edge port where SPAN or TAP traffic is coming into the monitor network and the egress delivery ports are defined. Cisco Monitor Manager uses the delivery ports to direct traffic from those ingress ports to one or more devices.

- Any-to-Multipoint—With the Any-to-Multipoint (A2MP) forwarding path option, the ingress edge port of the monitor network is not known, but the egress delivery ports are defined. Cisco Monitor Manager automatically calculates a loop-free forwarding path from the root node to all other nodes using the Single Source Shortest Path (SSSP) algorithm.

About Filters and Rules

Filters

In Cisco Monitor Manager, you can use a filter to define the Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) criteria used to filter traffic. Traffic that matches the criteria in the filter is routed to the delivery ports and from there to the attached monitor devices.

Rules

You can use rules to associate filters to configured monitor devices. You can configure rules with or without a source. Rules with a source node and port use the Multipoint-to-Multipoint forwarding path option. Rules without a source port on a node use the loop-free Any-to-Multipoint forwarding path option.

When a rule is configured with the Deny option, the ingress edge ports may or may not be defined. Cisco Monitor Manager drops traffic on the specified ingress edge port(s) or on all nodes if no ingress edge ports are defined.

Each rule has a priority that can be configured. Rules with a higher priority are given precedence over those with a lower priority.

Rules can be created and saved without installing them. After they are saved, installation can be toggled on and off in the Cisco Monitor Manager GUI.

Adding a Filter

Note The priority setting was moved from filters to rules in Cisco Extensible Network Controller (XNC) Release 1.5. If you upgraded from Cisco Extensible Network Controller (XNC) Release 1.0 to Cisco Extensible Network Controller (XNC) Release 1.5, any filters and rules that you previously configured in Cisco Monitor Manager 1.0 are automatically converted to the new format in Cisco Monitor Manager, Release 1.5.

Step 1 On the **Configure Filters** tab, click **Add Filter**.

Step 2 In the **Filter Description** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Name field	The name of the filter. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

Step 3 In the **Layer 2** section of the **Add Filter** dialog box, complete the following fields:
>

Step 4 In the **Layer 3** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** • You cannot enter a range of IPv6 addresses in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** • You cannot enter a range of IPv6 addresses in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports.
Protocol drop-down list	Choose the Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Step 5 In the **Layer 4** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source Port drop-down list	Choose the source port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Source Port** If you choose **Enter Source Port**, enter either a single port number or a range of source port numbers. **Note** If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses.
Destination Port drop-down list	Choose the destination port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Destination Port** If you choose **Enter Destination Port**, enter either a single port number or a range of destination port numbers. **Note** If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses.

Step 6 Click **Add Filter**.

Editing a Filter

Before You Begin

You must add a filter before you can edit it.

Note You cannot change the filter **Name** in the **Edit Filter** dialog box.

Step 1 On the **Configure Filters** tab, click the **Edit** button next to the **Name** of the filter that you want to edit.

Step 2 In the **Edit Filter** dialog box, edit the following fields:

Name	Description
Name field	The name of the filter. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

Step 3 In the **Layer 2** section of the **Edit Filter** dialog box, edit the following fields:

Name	Description
Ethernet Type field	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • **IPv6** • **ARP** • **LLDP** • **Predefined EtherTypes** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format. If you choose **Predefined EtherTypes**, all predefined Ethernet types contained in the config.ini file are associated with the rule, and you should not configure any other parameters. **Note** If you do configure any other parameters along with **Predefined EtherTypes**, then click **Save Rule**, an error message will be displayed.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Edit Filter** dialog box, edit the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** • You cannot enter a range of IPv6 addresses in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports.
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** • You cannot enter a range of IPv6 addresses in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports.
Protocol drop-down list	Choose the Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.

Name	Description
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Deleting a Filter

You can delete a filter that has associated rules, resulting in removal of all the rules at the same time.

Step 1 On the **Configure Filters** tab, check the check box next to filter or filters that you want to delete, and then click **Remove Filters**.
When filters have rules associated with them, this information is displayed in the **Remove Filters** dialog box.

Step 2 In the **Remove Filters** dialog box, click **Remove Filters**.

Adding a Rule

Before You Begin

- Add a filter to be assigned to the rule.
- Configure a monitoring device (optional).
- Configure an edge port or multiple edge ports (optional).

Step 1 On the **Apply Filters** tab, click the **Add Rule** button.

Step 2 In the **Add Rule** dialog box, complete the following fields in the **Rule Details** area:

Field	Description
Rule Name field	The name of the rule. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The **Rule Name** cannot be modified after the rule is saved.
Rule Filter drop-down list	Choose the filter that you want to assign to the rule. **Note** The **Rule Filter** cannot be modified after the rule is saved.
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, complete the following fields:

Field	Description
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.
Deny all matching traffic check box	Check this box if you want to drop all traffic based on the filter. **Note** If you check the **Deny all matching traffic** check box, you cannot select destination monitoring devices.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes.

Step 4 (Optional) In the **Assign Source Ports** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports.

Step 5 Do one of the following:

- Click **Save Rule** to save the rule, but not to install it until later.
- Click **Install Rule** to save the rule and install it at the same time.

Modifying a Rule

Note You cannot modify the **Rule Name** or **Rule Filter** in the **Modify Rule** dialog box.

Before You Begin

You must add the rule before you can modify it.

Step 1 On the **Apply Filters** tab, click the **Edit** button next to the **Name** of the rule that you want to modify.

Step 2 In the **Modify Rule** dialog bog you can modify the **Rule Priority** in the **Rule Details** area:

Field	Description
Rule Name field	The name of the rule. **Note** The **Rule Name** cannot be modified after the rule is saved.
Rule Filter drop-down list	The filter applied to the rule. **Note** The **Rule Filter** cannot be modified after the rule is saved.

Field	Description
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, modify the following fields:

Field	Description
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.
Deny all matching traffic check box	Check this box if you want to drop all traffic based on the filter. **Note** If you check the **Deny all matching traffic** check box, you cannot select destination monitoring devices.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes.

Step 4 In the **Assign Source Ports** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports.

Step 5 Click **Submit**.

Deleting a Rule

Step 1 Navigate to the **Apply Filters** tab.

Step 2 Check the check box for the rule or rules that you want to delete.

Step 3 Click **Remove Rules**.