Filtering Flows

This chapter contains the following sections:

Cisco Monitor Manager Networks

A Cisco Monitor Manager network consists of one or more Cisco Nexus 3000 Series switches with Cisco Plug-in for OpenFlow dedicated for connecting multiple spanned ports and network taps from the production network infrastructure. Cisco 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.

Cisco Monitor Manager 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 in to the monitor network and the egress delivery ports are defined. Cisco Monitor Manager uses the delivery ports to direct traffic from that ingress port 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.

Cisco Monitor Manager Filters and Rules

Filters

You can use a filter to define the Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) criteria used by Cisco Monitor Manager 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.

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

Adding a Filter

Note The priority you want to set was moved from filters to rules in Cisco XNC Release 1.5. If you upgraded from Cisco XNC Release 1.0 to Cisco XNC Release 1.5, any filters and rules that you previously configured in Cisco Monitor Manager 1.0 will automatically be converted to the new format in Cisco Monitor Manager 1.5.

Step 1 In 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 may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@). The name cannot be changed once you have saved it.

Name	Description
Bidirectional checkbox	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC to a destination IP, destination port, or destination MAC, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC.

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

Name	Description
Ethernet Type drop-down list	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** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format.
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 **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 for the **Source IP Address**.

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 for the **Destination IP Address**.
Protocol drop-down list	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	The source port of the Layer 4 traffic. Choose one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Source Port** If you choose Enter Source Port, enter the source port number.
Destination Port drop-down list	The destination port of the Layer 4 traffic. Choose one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Destination Port** If you choose Enter Destination Port, enter the destination port number.

Step 6 Click **Add Filter**.

Editing a Filter

Before You Begin

You must have added a filter before you can edit it.

Note You cannot change the filter **Name** and you cannot edit the **Layer 4** section fields in the **Edit Filter** dialog box.

Step 1 In the **Configure Filters** tab, click **Edit Filter** button next to the **Name** of the filter 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 may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@). The name cannot be changed once you have saved it.
Bidirectional checkbox	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC to a destination IP, destination port, or destination MAC, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC.

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

Name	Description
Ethernet Type drop-down list	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** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format.
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.

Name	Description
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 for the **Source IP Address**.
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 for the **Destination IP Address**.
Protocol drop-down list	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.

Deleting a Filter

You can delete filters that are associated with rules and the rules are deleted at the same time.

Step 1 On the **Configure Filters** tab, click the checkbox next to filter or filters that you want to delete, 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

- Configure a monitoring device.
- Add a filter to be assigned to the rule.
- Optional: Configure an edge port or multiple edge ports.

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

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

Field	Description
Rule Name field	The name of the rule. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).
Rule Filter drop-down list	Choose the filter that you want to assign to the rule.
Priority field	The priority you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.
Set VLAN field	The VLAN ID you want to set for the rule.

Field	Description
Deny all matching traffic checkbox	Check this box if you want to drop all traffic based on the filter. **Note** If deny all matching traffic is checked, you will be unable to select destination monitoring devices.
Destination Devices field	The monitoring devices that you want to associate with the filter. You can choose one or more devices.
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 non-delivery 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 3 Click **Submit**.

Viewing and Modifying Rules

After you have created a rule, you can modify the devices associated with the rule or delete the rule.

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

Step 2 The **Rules** table displays the following information for each rule:

Field	Description
Rule Name field	The name that you assigned to the rule.
Filter Name field	The filter that you assigned to the rule.
Port Name field	The source port that you assigned to the rule, if any.
Switch Name field	The source node that you assigned to the rule, if any.
Devices field	The monitor devices that are associated with the filter.
Created by field	The name and role of the user who created the rule.

Step 3 Click a rule to view the forwarding path for that rule in the topology diagram.
The path is highlighted in red.

Step 4 Click the **Edit** button to modify a rule.

Step 5 In the **Modify Rule** dialog box, perform one of the following tasks:

- Add or remove devices and click **Submit**.
- Click **Remove Rule** to delete the rule.
- Click **Close** to close the dialog box without making any changes.

Deleting a Rule

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

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

Step 3 Click **Remove Rules**.