



Filtering Flows

This chapter contains the following sections:

- [About Cisco Nexus Data Broker Networks, page 1](#)
- [About Forwarding Path Options, page 1](#)
- [About Filters and Connections, page 2](#)
- [Adding a Filter, page 3](#)
- [Editing a Filter, page 7](#)
- [Deleting a Filter, page 10](#)
- [Adding a Connection, page 11](#)
- [Modifying a Connection, page 13](#)
- [Cloning a Connection, page 15](#)
- [Removing a Connection, page 17](#)

About Cisco Nexus Data Broker Networks

A Cisco Nexus Data Broker network consists of one or more Cisco Nexus 3000, 3100, or 3500 Series switches and Cisco Nexus 9000 Series switches with Cisco Plug-in for OpenFlow and for NX-API dedicated for connecting multiple spanned ports and network taps from the production network infrastructure. Cisco Nexus Data Broker programs the switches using the OpenFlow protocol. Cisco Nexus Data Broker filters the packets that travel the network and delivers them to a pool of connected monitoring devices.

About Forwarding Path Options

Cisco Nexus Data Broker 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 Nexus Data Broker 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 Nexus Data Broker 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 Connections

Filters

In Cisco Nexus Data Broker, 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.

Connections

You can use connections to associate filters to configured monitor devices. You can configure connections with or without a source. Connections with a source node and port use the Multipoint-to-Multipoint forwarding path option. Connections 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 nexus Data Broker 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. Connections with a higher priority are given precedence over those with a lower priority.

Connections can be created and saved without installing them. After they are saved, installation can be toggled on and off in the Cisco nexus Data Broker GUI.



Note

After the connections are installed or uninstalled using the Toggle functionality in Cisco Nexus Data Broker, the device should not be rebooted for 120 secs. Otherwise the configured parameters by Cisco Nexus Data Broker are not saved and you might see a inconsistency between Cisco Nexus Data Broker and the device.

Default Filter

Cisco Nexus Data Broker is pre-installed with a default filter to match all traffic. The default filter is created using pre-defined Ethernet types as the match selection. The name of the default filter is default-match-all. This filter is available out-of-the-box when Cisco Nexus Data Broker starts up from scratch.

Adding a Filter

Procedure

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	<p>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 (" @ ").</p> <p>Note The name cannot be changed once you have saved it.</p>
Bidirectional check box	<p>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 address to a source IP, source port, or source MAC address.</p>

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

Ethernet Type field	<p>Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following:</p> <ul style="list-style-type: none"> • 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.in file are associated with the rule, and you should not configure any other parameters.
---------------------	---

VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12. Note For NX-API, a VLAN ID with Layer 3 address is not supported. If a VLAN ID with Layer 3 address is configured, it results in the inconsistent flows. You have to troubleshoot and fix the flows.
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: <ul style="list-style-type: none"> • 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 • The subnet, for example, 10.0.0.0/24 Note <ul style="list-style-type: none"> • 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. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination IP Address field	<p>The destination IP address of the Layer 3 traffic. This can be one of the following:</p> <ul style="list-style-type: none"> • The host IP address, for example, 10.10.10.11 • An IPv4 address range, for example, 10.10.10.11-10.10.10.18 • The host IP address in IPv6 format, for example, 2001::4 • The subnet, for example, 10.0.0.0/25 <p>Note</p> <ul style="list-style-type: none"> • You cannot enter a range of IPv6 addresses in the Destination 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. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.
Protocol drop-down list	<p>Choose the Internet protocol of the Layer 3 traffic. This can be one of the following:</p> <ul style="list-style-type: none"> • ICMP • TCP • UDP • Enter Protocol <p>If you choose Enter Protocol as the type, enter the protocol number in decimal format.</p>
ToS Bits field	<p>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.</p>

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

Name	Description
Source Port drop-down list	<p>Choose the source port of the Layer 4 traffic. This can be one of the following:</p> <ul style="list-style-type: none">• FTP (Data)• FTP (Control)• SSH• TELNET• HTTP• HTTPS• Enter Source Port <p>If you choose Enter Source Port, enter either a single port number or a range of source port numbers.</p> <p>Note</p> <ul style="list-style-type: none">• If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses.• If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination Port drop-down list	<p>Choose the destination port of the Layer 4 traffic. This can be one of the following:</p> <ul style="list-style-type: none"> • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Destination Port <p>If you choose Enter Destination Port, enter either a single port number or a range of destination port numbers.</p> <p>Note</p> <ul style="list-style-type: none"> • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers.

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.

Procedure

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	<p>The name of the filter.</p> <p>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 ("@").</p> <p>Note The name cannot be changed once you have saved it.</p>
Bidirectional check box	<p>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.</p>

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

Name	Description
Ethernet Type field	<p>Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following:</p> <ul style="list-style-type: none"> • IPv6 • ARP • LLDP • Predefined EtherTypes • Enter Ethernet Type <p>If you choose Enter Ethernet Type as the type, enter the Ethernet type in hexadecimal format.</p> <p>If you choose Predefined EtherTypes, all predefined Ethernet types contained in the <code>config.in</code> file are associated with the rule, and you should not configure any other parameters.</p> <p>Note If you do configure any other parameters along with Predefined EtherTypes, then click Save Rule, an error message will be displayed.</p>

Name	Description
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12.
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	<p>The source IP address of the Layer 3 traffic. This can be one of the following:</p> <ul style="list-style-type: none"> • 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 <p>Note</p> <ul style="list-style-type: none"> • 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. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination IP Address field	<p>The destination IP address of the Layer 3 traffic. This can be one of the following:</p> <ul style="list-style-type: none"> • 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 <p>Note</p> <ul style="list-style-type: none"> • 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. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.
Protocol drop-down list	<p>Choose the Internet protocol of the Layer 3 traffic. This can be one of the following:</p> <ul style="list-style-type: none"> • ICMP • TCP • UDP • Enter Protocol <p>If you choose Enter Protocol as the type, enter the protocol number in decimal format.</p>
ToS Bits field	<p>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.</p>

Deleting a Filter

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

Procedure

-
- 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 Connection

Before You Begin

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

Procedure

-
- Step 1** On the **Connection Setup** tab, click **New Connection**.
- Step 2** In the **New Connection** dialog box, you can add the **Connection Name** and the **Priority** of the connection in the **Connection Details** area:

Field	Description
Connection Name	The name of the connection. 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 ("@").
Priority	The priority that you want to set for the connection. The default is 100, and the valid range of values is 0 through 10000.

- Step 3** In the **Allow Matching Traffic** area, modify the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. Note You cannot choose the same filter for Allow Filters that you choose for Traffic Drop Filters.
Set VLAN field	The VLAN ID that you want to set for the connection.
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 connections with a single edge port and one or more delivery devices for a single, separate node.
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 next to their names.
Traffic Drop Filters drop-down list	Note

Step 4 In the **Drop Matching Traffic** area, complete the following fields:

Field	Description
Traffic Drop Filters	Choose the default filter Default-Match-all or use other filters to drop the matching traffic. Note You cannot choose the same filter for Traffic Drop Filters that you choose for Allow Filters.

Step 5 In the **Source Ports (Optional)** 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.

Field	Description
Select Source Port drop-down list	<p>Choose the port on the source node that you want to assign.</p> <p>Note Only edge ports can be used as source ports.</p> <p>Note If you do not select a source port while adding a new connection, the following warning message is displayed: No source port is selected. Connection will be setup from all configured Edge-SPAN and Edge-TAP ports. Click OK to continue with the connection installation/creation. It ensures that you do not install any to multi point connection and disrupt any existing traffic. Click Cancel to take you to the connection setup page.</p>

Note Similar to the number of Edge-Tap or SPAN ports are displayed on top of each switch in the topology, the number of forwarding rules that a particular monitoring tool is part of are displayed when you hover the mouse over a switch. A popup table displays the rule (connection) names within which the monitoring tool is being used.

Step 6 Do one of the following:

- Click **Save Connection** to save the connection, but not to install it until later.
- Click **Install Connection** to save the connection and install it at the same time.
- Click **Close** to exit the connection without saving it.

Modifying a Connection

Before You Begin

You must add a connection before you can modify it.

Procedure

- Step 1** On the **Connection Setup** tab, click the **Edit** button next to the **Name** of the connection that you want to modify.
- Step 2** In the **Modify Connection** dialog box, you can modify the **Connection Name** and the **Priority** of the connection in the **Connection Details** area:

Field	Description
Connection Name	The name of the connection. 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 ("@").
Priority	The priority that you want to set for the connection. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Allow Matching Traffic** area, modify the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. Note You cannot choose the same filter for Allow Filters that you choose for Traffic Drop Filters.
Set VLAN field	The VLAN ID that you want to set for the connection.
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 connections with a single edge port and one or more delivery devices for a single, separate node.
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 next to their names.
Traffic Drop Filters drop-down list	Note

Step 4 In the **Drop Matching Traffic** area, complete the following fields:

Field	Description
Traffic Drop Filters	Choose the default filter Default-Match-all or use other filters to drop the matching traffic. Note You cannot choose the same filter for Traffic Drop Filters that you choose for Allow Filters.

Step 5 In the **Source Ports (Optional)** 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 6 Click **Submit** or **Close**.

Cloning a Connection

Before You Begin

You must add a connection before you can modify it.

Procedure

Step 1 On the **Connection Setup** tab, click the **Clone** next to the **Name** of the connection that you want to clone.

Step 2 In the **Clone Connection** dialog box, you can modify the **Connection Name** and the **Priority** of the connection in the **Connection Details** area:

Field	Description
Connection Name	The name of the connection. 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 (" @ ").
Priority	The priority that you want to set for the connection. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Allow Matching Traffic** area, modify the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. Note You cannot choose the same filter for Allow Filters that you choose for Traffic Drop Filters.
Set VLAN field	The VLAN ID that you want to set for the connection.
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 connections with a single edge port and one or more delivery devices for a single, separate node.
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 next to their names.
Traffic Drop Filters drop-down list	Note

Step 4 In the **Drop Matching Traffic** area, complete the following fields:

Field	Description
Traffic Drop Filters	Choose the default filter Default-Match-all or use other filters to drop the matching traffic. Note You cannot choose the same filter for Traffic Drop Filters that you choose for Allow Filters.

Step 5 In the **Source Ports (Optional)** 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 6** Do one of the following:
- Click **Save Cloned Connection** to save the connection, but not to install it until later.
 - Click **Install Cloned Connection** to save the connection and install it at the same time.
 - Click **Close** to exit the connection without saving it.
-

Removing a Connection

Procedure

- Step 1** Navigate to the **Connection Setup** tab.
- Step 2** Check the check box for the connection or connections that you want to delete.
- Step 3** Click **Remove Connections**.
-

