Filtering Flows

This chapter contains the following sections:

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), Layer 4 (L4), and Layer 7 (L7) filtering for HTTP traffic 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 All Ethertype 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.

About Redirection and Service Nodes

You can now redirect some of the traffic from the firewall or the switches to a service node, for example, SourceFire IPS, through an inline redirection Cisco Nexus 3000 or Cisco Nexus 9300 switch with Cisco Nexus Data broker enabled on it. The traffic is redirected from the production ingress port through the tap aggregation switch into the service node via the service ingress and egress ports. Finally, it is redirected from the service node to the production egress port.

Redirection Setup Using the Service Nodes

You can now clone the traffic between the two ports of the Cisco Nexus 3000 and Cisco Nexus 9000 Series switch. One port is the source port and other port is the destination port. This configuration allows you to quickly copy the traffic between the interfaces.

You can also copy the traffic to a service node, for example, QRadar and compare the traffic with the traffic that is redirected on the switch. You can copy the traffic to the external monitoring tools as the traffic is redirected. As part of the redirection rule, you can specify the destination port to which the redirected traffic should be copied. A copy of the traffic is sent from all the service node egress ports (traffic entering the switch). The port to which the traffic is copied can be a physical port or a logical port-channel. When you are using OpenFlow, you can implement the ability to support * for the Ethertype value.

There is always a 1:1 mapping between the ingress and the egress production ports. Since the switch is situated between the production and the service ports instead of a direct connection between the links, it is important to shutdown the port when either an ingress or an egress port goes operationally down. If an ingress port is down, the egress port is automatically shutdown. If an egress port goes down, the ingress port is shutdown automatically.

When an ingress or egress port connecting to a service node goes down, that service node is automatically bypassed. All the redirection associated with that service node is updated to bypass the service node.

If the traffic is not handled by the service nodes, there is a backup flow and the traffic is sent back to production ingress ports.

You can also edit the details of a service node by selecting the ingress port and by updating the details of the node. Click **Edit** to edit the details. To delete the service node, click **Remove Service Node** in the **Service Nodes** display area on the sidebar.

Note Maximum of 4 service nodes are supported per redirection.

Adding a Filter

Procedure

Step 1 On the **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:

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 • All 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. **Note** You can now configure more than 1 user-defined Ethernet type per filter. You can apply an arbitrary number of Ethernet types that are separated by "," so that a single filter can be setup for the different traffic types.

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: • The host IP address, for example, 10.10.10.10 • Discontiguous source IP address, for example, 10.10.10.10, 10.10.10.11, 10.10.10.12 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • An IPv4 subnet, for example, 10.1.1.0/24 • 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. • 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	The destination IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.11 • An IPv4 address range, for example, 10.10.10.11-10.10.10.18 • An IPv4 subnet, for example, 10.1.1.0/24 • The host IP address in IPv6 format, for example, 2001::4 • The subnet, for example, 10.0.0.0/25 **Note** • 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	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. • 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	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. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Step 6 In the **Layer 7** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
HTTP Method field	You can configure matching on the HTTP methods and redirect the traffic based on that method. Select one or more methods to match within a single filter. This option is available only when the destination port is HTTP or HTTPS. • Connect • Delete • Get • Head • Post • Put • Trace **Note** Layer 7 match is supported only with the NX-API mode only and it is not supported in OpenFlow. **Note** The TCP option length is enabled when you select any one of the methods from Layer 7 traffic.
TCP Option Length field	You can extend the filter configuration to specify the TCP option length in the text box. The default value on the text box is 0. All methods within the filter have the same option length. Enter the TCP option length in a decimal format. **Note** The value on the text box should be in the multiples of 4 and it can range from 0-40.

Step 7 Click **Add Filter**.

Editing a Filter

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	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, complete the following fields:

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 • All 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. **Note** You can now configure more than 1 user-defined Ethernet type per filter. You can apply an arbitrary number of Ethernet types that are separated by "," so that a single filter can be setup for the different traffic types.

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 **Edit 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 • Discontiguous source IP address, for example, 10.10.10.10, 10.10.10.11, 10.10.10.12 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • An IPv4 subnet, for example, 10.1.1.0/24 • 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. • 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	The destination IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.11 • An IPv4 address range, for example, 10.10.10.11-10.10.10.18 • An IPv4 subnet, for example, 10.1.1.0/24 • The host IP address in IPv6 format, for example, 2001::4 • The subnet, for example, 10.0.0.0/25 **Note** • 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	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 **Edit 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. • 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	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. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Step 6 In the **Layer 7** section of the **Edit Filter** dialog box, complete the following fields:

Name	Description
HTTP Method field	You can configure matching on the HTTP methods and redirect the traffic based on that method. Select one or more methods to match within a single filter. This option is available only when the destination port is HTTP or HTTPS. • Connect • Delete • Get • Head • Post • Put • Trace **Note** The TCP option length is enabled when you select any one of the methods from Layer 7 traffic.
TCP Option Length field	You can extend the filter configuration to specify the TCP option length in the text box. The default value on the text box is 0. All methods within the filter have the same option length. Enter the TCP option length in a decimal format. **Note** The value on the text box should be in the multiples of 4 and it can range from 0-40.

Step 7 Click **Edit Filter**.

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 **Connections** tab, click **Add Connection**.

Step 2 In the **Add 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 ("@").
Description	Enter the description when creating a new connection.
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.

Field	Description
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. **Note** When setting up a new redirection, you can see the number of flows that are part of each input port. When you click the port number, the flow details are displayed.

Field	Description
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. **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.

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.

The following fields are displayed on the Connection Setup screen.

- Name
- Allow Filters
- Deny Filters
- Source Ports
- Devices
- Priority
- Last Modified By
- Description

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 ("@").
Description	Enter the description when creating a new connection.
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.

Field	Description
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 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 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 ("@").
Description	Enter the description when creating a new connection.
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**.

Adding a Service Node

Procedure

Step 1 In the topology diagram, click the node.
Step 2 In the side bar, click **Add Service Node**. The **Add Service Node** window is displayed.
Step 3 Enter the name of the service node in the **Service Node Name** window.
Step 4 Select the ingress port for the service node in the **Service Node Ingress Port** window.
Step 5 Select the egress port for the service node in the **Service Node Egress Port** window.
Step 6 Select a service node icon.
Step 7 Click **Submit**.

Adding Redirection

Note The redirection setup feature is supported on Cisco Nexus 3000 Series switches running Release 6.0(2)U5(2) and later releases only. This feature is supported on Cisco Nexus 9300 switches starting with Release 7.x and OpenFlow.

Before You Begin

- Add a filter to be assigned to the redirection.
- Configure a monitoring device (optional).
- Configure an edge port or multiple edge ports (optional).
- The production ingress port, the production egress port, and the service node should be on the same redirection switch.

Procedure

Step 1 On the **Redirections** tab, click **Add Redirection**.
Step 2 In the **Add Redirection** dialog box, you can add the **Redirection Name** and the **Priority** of the redirection in the **Redirection Details** area:

Field	Description
Redirection Name	The name of the redirection. 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 of the redirection cannot be changed once you have saved it.
Description	Enter the description when creating a new redirection.
Set auto priority checkbox	Check this option to enable the auto priority for the redirection, The priority of the redirection is set based on the existing redirections that are installed on the selected ingress ports.
Priority	The priority that you want to set for the redirection. The valid range of the values is 0–10000. The default is 100.
Automatic Fail-safe checkbox	Check this option to enable the fail-safe feature of redirection. When you enable this feature, the direct flow from the production ingress port and the egress port is created that matches all ethertype traffic of low priority.

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

Field	Description
Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same redirection for the filter.

Step 4 In the **Redirection Switch** area, modify the following fields:

Field	Description
Select Redirection Switch drop-down list	Select the redirection switch that you want to assign.

Note You can have only one ingress port and one egress port per one redirection switch.

Step 5 In the **Service Nodes (OPTIONAL)** area, complete the following fields:

Field	Description
Select Service Node drop-down list	Select the redirection service node that you want to assign and click **Add Service Node**.

Note If you want to add multiple service nodes, you should add them in an order in which you want the packets to travel.

Step 6 In the **Production Ports** area, complete the following fields:

Field	Description
Select Production Ingress Port drop-down list	Select the production ingress port that you want to assign. **Note** You can select only one ingress port. Multiple ingress ports are not allowed. You cannot use the same ports as the ingress and the egress ports. **Note** When setting up a new redirection, you can see the number of flows that are part of each input port. When you click the port number, the flow details are displayed.
Select Production Egress Port drop-down list	Select the production egress port that you want to assign. **Note** You can select only one ingress port. Multiple ingress ports are not allowed. You cannot use the same ports as the ingress and the egress ports.

Step 7 In the **Delievery Devices to copy traffic (OPTIONAL)** area, complete the following fields:

Field	Description
Select Device drop-down list	Select a device, for example, a switch from the drop-down list, that you want to assign and click **Add Device**. **Note** You can select multiple delivery devices for the redirection.

Step 8 Do one of the following:

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

Step 9 When you click **Install Redirection** to save the redirection and install it at the same time, the redirection path on the redirection switch is displayed on the production ingress ports, service nodes, and the production egress ports.

Step 10 Click **Flow Statistics** to view the flow statistics for the redirection switch.
The following fields provide information on the flow statistics:

- In Port field—The Input port(s) from which the traffic is matched. An asterisk ("*") indicates any input port.

- DL Drc field—The source MAC address to be matched for the incoming traffic. An asterisk ("*") indicates any source MAC address.
- DL Dst field—The destination MAC address to be matched for the incoming traffic. An asterisk ("*") indicates any destination MAC address.
- DL Type field—The Ethertype to be matched for the incoming traffic. For example, "IPv4" or "IPv6" is used for all IP traffic types.
- DL VLAN field—The VLAN ID to be matched for the incoming traffic. An asterisk ("*") indicates any VLAN ID.
- VLAN PCP field—The VLAN priority to be matched for the incoming traffic. An asterisk ("*") is almost always displayed in this field.
- NW Src field—The IPv4 or IPv6 source address for the incoming traffic. An asterisk ("*") indicates any source address based on IPv4 or IPv6 Ethertypes.
- NW Dst field—The IPv4 or IPv6 destination address for the incoming traffic. An asterisk ("*") indicates any destination address based on IPv4 or IPv6 Ethertypes.
- NW Proto field—The network protocol to be matched for the incoming traffic. For example, "6" indicates the TCP protocol.
- TP Src field—The source port associated with the network protocol to be matched for the incoming traffic. An asterisk ("*") indicates any port value.
- TP Dst field—The destination port associated with the network protocol to be matched for the incoming traffic. An asterisk ("*") indicates any port value.
- Actions field—The output action to be performed for the traffic matching the criteria specified, for example, "OUTPUT = OF|2".
- Byte Count field—The aggregate traffic volume shown in bytes that match the specified flow connection.
- Packet Count field—The aggregate traffic volume shown in packets that match the specified flow connection.
- Duration Seconds field—The amount of time, in milliseconds, that the specific flow connection has been installed in the switch.
- Idle Timeout field—The amount of time, in milliseconds, that the flow can be idle before it is removed from the flow table.
- Priority field—The priority assigned to the flow. The flows with higher priority numbers take precedence.

Step 11 Click **Close** to close the flow statistics display window.

Modifying Redirection

Before You Begin

You must add a redirection before you can modify it.

Procedure

Step 1 On the **Redirection Setup** tab, click the **Edit** button next to the **Name** of the connection that you want to modify.

Step 2 In the **Modify Redirection** dialog box, you can modify the **Redirection Name** and the **Priority** of the redirection in the **Redirection Details** area:

Field	Description
Redirection Name	The name of the redirection. 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 of the redirection cannot be changed once you have saved it.
Description	Enter the description when creating a new redirection.
Set auto priority checkbox	Check this option to enable the auto priority for the redirection, The priority of the redirection is set based on the existing redirections that are installed on the selected ingress ports.
Priority	The priority that you want to set for the redirection. The valid range of the values is 0–10000. The default is 100.
Automatic Fail-safe checkbox	Check this option to enable the fail-safe feature of redirection. When you enable this feature, the direct flow from the production ingress port and the egress port is created that matches all ethertype traffic of low priority.

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

Field	Description
Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same redirection for the filter.

Step 4 In the **Redirection Switch** area, modify the following fields:

Field	Description
Select Redirection Switch drop-down list	Select the redirection switch that you want to assign. **Note** You cannot choose the same redirection switch for the filter.

Step 5 In the **Service Nodes (OPTIONAL)** area, complete the following fields:

Field	Description
Select Service Node drop-down list	Select the redirection service node that you want to assign and click **Add Service Node**.

Step 6 In the **Production Ports** area, complete the following fields:

Field	Description
Select Production Ingress Port drop-down list	Select the production ingress port that you want to assign. **Note** You can select only one ingress port. Multiple ingress ports are not allowed. You cannot use the same ports as the ingress and the egress ports.
Select Production Egress Port drop-down list	Select the production egress port that you want to assign. **Note** You can select only one ingress port. Multiple ingress ports are not allowed. You cannot use the same ports as the ingress and the egress ports.

Step 7 In the **Delievery Devices to copy traffic (OPTIONAL)** area, complete the following fields:

Field	Description
Select Device drop-down list	Select a device, for example, a switch from the drop-down list, that you want to assign and click **Add Device**. **Note** You can select multiple delivery devices for the redirection.

Step 8 Do one of the following:

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

Removing a Redirection

Procedure

Step 1 Navigate to the **Redirection Setup** tab.

Step 2 Check the check box for the redirection or redirections that you want to delete.

Step 3 Click **Remove Redirections**.