



Configuring the Nexus Data Broker

This chapter contains the following sections:

- [Viewing Topology, page 1](#)
- [Configuring Port Definition, page 1](#)
- [Configuring Port Groups, page 5](#)
- [Configuring a Monitoring Device, page 6](#)
- [Adding a Service Node, page 7](#)
- [Configuring Symmetric Load Balancing and MPLS Tag Stripping , page 8](#)
- [Adding Filters, page 8](#)
- [Adding Connections, page 14](#)
- [Adding Redirections, page 17](#)
- [Viewing Statistics, page 21](#)
- [Adding SPAN Sessions, page 23](#)

Viewing Topology

Click the **Topology** tab in the left frame to view the topology in the network.

Configuring Port Definition

When you click **Port Definition** tab in the GUI, the **Port Definition** screen is displayed. Select the switch from the drop-down list to configure the ports.

On the **Port Definition** screen, the following two tabs are displayed:

- Port Configuration
- SPAN Destination

Click the **Port Configuration** tab, the following tabs are displayed:

- Configure Multiple Ports
- Remove port Configuration
- Add Service Node
- Add Monitoring Device

When you click **Configure Multiple Ports** tab, the **Configure Multiple Ports** window is displayed. The following details are displayed on the screen: Number, Status, Port Name, Type, In Use, Port ID, and Action.

**Note**

Beginning with Cisco Nexus Data Broker, Release 3.1, the interface description is updated from the Cisco Nexus Data Broker GUI to the switch and the interface description is also available from the switch into the Cisco Nexus Data Broker GUI. When using in Openflow mode, the NX-API auxiliary connection is required for this functionality to work.

**Note**

On the Port Configuration tab, the port name and the interface are displayed as hyperlinks. When you click the port name, you can view the running configuration for that interface on the tab.

If you want to remove any ports, select the port and click **Remove port Configuration** tab.

Click **Add Service Node** to add a service node.

Click **Add Monitoring Device** to add a monitoring device.

On the **Port Configuration** screen, the following port details are displayed for the selected node:

- Serial Number
- Status
- Port name
- Type
- In Use
- Port ID
- Action—When you click **Configure**, the **Configure Ports** window is displayed.

On the **SPAN Destination** tab, the following details are displayed:

- SPAN Destination Name
- SPAN Destinations
- Node Connector
- Monitor Port Type
- Description

Configuring Ports

- Step 1** Select the switch for which you want to configure the port details on the **Port Configuration** screen.
- Step 2** Click **Configure** under **Action**.
The **Configure Ports** window is displayed.
- Step 3** In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

- **Add Monitoring Device**
- **Edge Port-SPAN**
- **Edge Port-TAP**
- **Production Port**

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Production Port—Creates a production port for the ingress and egress traffic.

Note To receive the traffic from the production network, the production ingress port is configured. After entering the service nodes (multiple security tools), the traffic exits the data center through the production egress port.

Note Starting with Cisco Nexus Data Broker, Release 3.2, when Edge-SPAN, Edge-TAP, monitoring device, or production port is defined in NX-API mode of configuration, the CLI command, **spanning-tree bpdudfilter enable** is automatically configured in the interface mode on the ports to filter the BPDU packets. This configuration is applicable for all Cisco Nexus 3000 and 9000 Series switches. The sample configuration is displayed in the example:

```
switch#
show run interface eth1/1
interface ethernet1/1
switchport mode trunk
mode tap-aggregation
spanning-tree bpdudfilter enable
```

Note Production port has been enabled for Q-in-Q in Cisco Nexus Data Broker and a unique VLAN should be assigned for each production port. This VLAN should not overlap with any production VLAN numbers.

Note The **spanning-tree bpdudfilter enable** CLI command should be configured by the user on all the inter-switch ports for all Cisco Nexus series switches and Cisco Nexus Data Broker does not configure this command.

Note Once an interface is configured with Q-in-Q, do not configure multiple VLAN filters for the Q-in-Q configured interface.

When you select the port type, the title of the window changes to **Manage Configure Ports**.

- Step 4** (Optional) In the **Port Description** field, enter the port description.

Beginning with Cisco Nexus Data Broker, Release 3.1, the interface description is updated from the Cisco Nexus Data Broker GUI to the switch and the interface description is also available from the switch into the Cisco Nexus Data Broker GUI. When using in Openflow mode, the NX-API auxiliary connection is required for this functionality to work.

- Step 5** Enter VLAN ID for the port.
The port is configured as dot1q to preserve any production VLAN information. The VLAN ID is used to identify the port that the traffic is coming from.
- Step 6** (Optional) If APIC is available, you can select the ACI side port and designate it as the SPAN destination port.
- Step 7** In the **Enable Packet Truncation** field, enter the packet length.
- Step 8** A check box is added for **Block Tx** and it is applicable only for Edge-SPAN where you can block the traffic that is being transmitted out of Edge-SPAN interface.
- Step 9** Click **Submit** to save the settings or click **Clear** to clear the details.
Once you configure a port, you can click **Edit** under **Action** on the **Port Configuration** screen to edit the port details. You can click **Remove** under **Action** on the **Port Configuration** screen to clear the port details.

Adding SPAN Destination

When you configure a port as an edge SPAN port and the port is connected to the API side, you can select the pod, node, and port from the ACI side and set the port as SPAN destination.



Note You can add SPAN destination only after APIC has been successfully added to the network.

- Step 1** Select the switch for which you want to configure the port details on the **Port Configuration** screen.
- Step 2** Click **Configure** under **Action**.
The **Configure Ports** window is displayed.
- Step 3** In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:
- **Add Monitoring Device**
 - **Edge Port-SPAN**
 - **Edge Port-TAP**
 - **Production Port**

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Production Port—Creates a production port for the ingress and egress traffic.

When you select the port type, the title of the window changes to **Manage Configure Ports**.

- Step 4** In the SPAN DESTINATION pane, select the pod from the **Pod** drop-down list.
 - Step 5** Select the ACI leaf from the **Leaf** drop-down list.
 - Step 6** Select the port from the ACI side from the **Port** drop-down list and set the interface as SPAN destination.
 - Step 7** Click **Submit** to save the settings.
The port is now configured as SPAN destination part and it is displayed on the Port Definition screen.
-

Configuring Multiple Ports

You can configure multiple ports for a node.

-
- Step 1** Click **Configure Multiple Ports** on the **Port Configuration** screen. The **Configure Multiple Ports** window is displayed.
 - Step 2** Use **CTRL/SHIFT** to select multiple ports in the **Select Ports** field.
 - Step 3** Select port type from the drop-down list in the **Select Port Type** field.
 - Step 4** Click **Submit** to save the settings.
-

Configuring Port Groups

You can create a port group and add the ports to the connection.



Note

Starting with Cisco Nexus Data Broker, Release 3.2, you can create port groups for different source ports. The port groups can be a combination of the edge-span and the edge-tap ports across different switches. You can select ports, define port groups, provide a name to the port group, select the port group in a connection screen (only one port group per connection), and use the ports defined in the port group as source ports for creating a connection. Selecting individual ports is disabled when using a port group.

You cannot edit the port group even if it is part of a connection. The connection is automatically updated with the new port group. Deleting a port group is not allowed when the port group is in use.

Complete the following steps to configure port groups:

Before You Begin

-
- Step 1** Select the switch for which you want to configure the port details on the Port Configuration screen.
- Step 2** Click **Port Groups** tab in the left frame.
- Step 3** Click + **Add Group** to create a port group.
- Step 4** In the **Create Port Group** window, enter the group name in the **Group Name** field.
- Step 5** In the **Select Node** field, select a node, for example, N9K-116.
- Step 6** In the **Select Port** field, select a port, for example, Ethernet1/1 (Ethernet1/1).
You can add only edge-span and edge-tap ports and you cannot add production ports to the port groups.
- Step 7** Click + **Add To Group** to add the port to the group.
You can add multiple ports to the group.
- Step 8** Click **Apply**.
The port group is displayed on the **Port Groups** screen with the following information for the group, for example, **Name**, **Connection Name**, **Ports** and **Action**.
-

Configuring a Monitoring Device

-
- Step 1** Navigate to the **Monitoring Device** tab under **Configuration**.
- Step 2** Click + **Monitoring Device**.
- Step 3** In the **Monitoring Device** window, complete the following fields:

Name	Description
Monitoring Device Name	Add the service node name. Note The valid characters for the monitoring devices are the alphanumeric characters and the special characters: colon (":"), underscore ("_"), hyphen ("-"), vertical bar (" "), and period (".").
Select Switch Node	Select the switch node.
Select Port	Select the port.
Icons	Select a Monitoring Device Icon.
Block Rx	Block any traffic from being received from the monitoring tools. This option is selected by default. You can turn this option off by unchecking the box.

Name	Description
Enable Timestamp Tagging	<p>You can configure timestamp tagging only on the Cisco Nexus 3500 Series switches that are running Release 6.0(2)A8(1) or later and the mode is NX-API auxiliary.</p> <p>When you enable timestamp tagging, the TS-tag field is displayed next to the switch on the tab. With this option enabled, the ttag and ttag-marker enable CLIs are available for use.</p> <p>The ttag-marker-interval is a global option that is available on the Cisco Nexus 3500 Series switches. The default interval for this option is 3 Seconds.</p>

Step 4 Click **Save**.

Adding a Service Node

Step 1 Navigate to the **Service Nodes** tab under **Configuration** and click + **Service Node**.

Step 2 In the **Add Service Node** window, enter the name of the service node.

Step 3 Select the ingress port for the service node from the **Service Node Ingress Port** drop-down list.

Step 4 Select the egress port for the service node from the **Service Node Egress Port** drop-down list.

Step 5 Enable health check on a service node by selecting the **Service Node Health Check** option.

Beginning with Cisco Nexus Data Broker, Release 3.2, you can configure the wait interval in the **config.ini** file before the health check is up. The **ServiceNodeHealthCheckWaitInterval** is the variable in the **config.ini** file to set the wait interval. If you do not specify a value or if the value is 0 for the wait interval in the **config.ini** file, the default value of 5 Seconds is used. The wait interval is not applicable if the port is in shutdown state.

This option works only in the OpenFlow mode. The controller or the NDB injects a packet in the service node ingress port and the packet is received at the egress port. The packets are checked at the interval of every 5 seconds. If five packets are not received in 5 seconds, the health of the service node is considered as down.

For the service node, a new field is displayed in the details: Service Node Status. This field displays the status of the service node.

Step 6 Select a service node icon from the available options.

Step 7 Click **Save**.

Configuring Symmetric Load Balancing and MPLS Tag Stripping

From the Cisco Nexus Data Broker GUI and the REST API interfaces, you can now configure symmetric load balancing and enable MPLS tag stripping on the Cisco Nexus 3000 Series and Cisco Nexus 9000 Series switches using NX-API as the configuration mode.

Before You Begin

Add device to Cisco Nexus Data Broker using NX-API.

-
- Step 1** In the topology diagram, click the node for which you wish to configure MPLS tag stripping.
- Step 2** In the **Port Configuration** window, click **Configure Node**. The **Node Configuration** window is displayed.
- Step 3** In the **Symmetric Load Balancing on Port Channel** drop-down list, select the **Hashing Option**.
- Step 4** In the **MPLS Strip Configuration** drop-down list, choose one of the following:
- Enable MPLS Strip.
 - Disable MPLS Strip.
- Step 5** When you select **Enable MPLS Strip** option, the **Label Age** field is displayed. In the field, enter a value for the MPLS strip label age. The range for MPLS strip label age configuration is 61-31622400.
- Step 6** Click **Submit**.
-

Adding Filters

Before You Begin

The hardware command that is a pre-requisite for the IPv6 feature is **hardware access-list tcam region ipv6-ifacl 512 double-wide**.

-
- Step 1** On the **Filters** tab, click + **Filter** to add a filter. The **Add Filter** window is displayed.
- Step 2** In the **Filter Description** section of the **Add Filter** window, complete the following fields:

Name	Description
Name field	The name of the filter. Note The name cannot be changed once you have saved it.

Name	Description
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** window, 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 • 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. <p>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.</p>
VLAN Identification Number field	<p>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.</p> <p>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.</p>
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** window, update 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 • 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 <p>Note</p> <ul style="list-style-type: none"> • When a switch is used in NX-API mode, you can now select an IPv6 filter and setup a connection. You can enter a single IPv6 address, comma separated multiple IPv6 addresses, an IPv6 address range, and/or IPv6 subnet 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. <p>Note When using IPv6 address in the filter, the Ethernet Type should be set to IPv6.</p>

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 • 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 <p>Note</p> <ul style="list-style-type: none"> • When a switch is used in NX-API mode, you can now select a IPv6 filter and setup a connection. You can enter a single IPv6 address only in the Destination IP Address field. The comma separated multiple IPv6 addresses, an IPv6 address range, and/or IPv6 subnets are not supported. The hardware command that is a pre-requisite is for using the IPv6 feature is hardware access-list tcam region ipv6-ifacl 512. • 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: If you choose Enter Protocol as the type, enter the protocol number in decimal format.</p> <ul style="list-style-type: none"> • ICMP • TCP • UDP • Enter Protocol
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>Note Beginning with Cisco Nexus Data Broker Release 3.2 , you can enter comma separated single port numbers and a range of the source port numbers in the Enter Source Port field.</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>Note Beginning with Cisco Nexus Data Broker Release 3.2 , you can enter comma separated single port numbers and a range of the source port numbers in the Enter Destination Port field.</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 In the **Layer 7** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
HTTP Method field	<p>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.</p> <ul style="list-style-type: none"> • Connect • Delete • Get • Head • Post • Put • Trace <p>Note Layer 7 match is supported only with the NX-API mode only and it is not supported in OpenFlow.</p> <p>Note The TCP option length is enabled when you select any one of the methods from Layer 7 traffic.</p>
TCP Option Length field	<p>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.</p> <p>Enter the TCP option length in a decimal format.</p> <p>Note The value on the text box should be in the multiples of 4 and it can range from 0-40.</p>

Step 7 Click **Add Filter**.

Adding Connections

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).

Step 1 On the **Connections** tab, click + **Connection**. The **Add Connections** window is displayed.

Step 2 In the **Add Connections** window, 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.
Description	Enter the description when creating a new connection.
Priority	The priority that you want to set for the connection. Connection by default has priority of 100. It can be changed in the range of <1-10000>.

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 Drop Filters.
Set VLAN field	The VLAN ID that you want to set for the connection. Note This functionality is available only in Openflow mode.
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. This functionality is available only in Openflow mode.
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.
Drop Filters drop-down list	Note

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

Field	Description
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 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.
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.
In the Source Ports (Optional) area, select Port Group instead of Source Ports .	Select port group.
Select a port group from Select Port Group drop-down list. If you do not have any port groups configured, click + Port Group to add a port group.	Select a port group.

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.

Note In Cisco Nexus Data Broker, Release 3.2.0, you can also select a port group in which case the individual ports cannot be selected.

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
- Drop Filters
- Source Ports
- Devices
- Priority
- Last Modified By
- Description

The following fields are displayed In the Connections tab: **Status, Name, Allow Filters, Drop Filters, Source Ports/Port Group, Devices, Priority, Last modified by, Description, and Action.**



Note

Beginning with Cisco Nexus Data Broker, Release 3.2, if you have added two or more interfaces (source ports) using the Connections tab, two interfaces (source ports) are displayed by default. If you have more than two interfaces (source ports) in the **Connections** tab, you can expand or collapse the source ports by using **more...** or **less...** options that are provided in the GUI.

Click **i Search Connections** tab in the Connections screen to search for the connections using the keywords, **Success, Installing, Creating, Partial, and Failed.**

Adding Redirections



Note

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

Cisco Nexus Data Broker lets you configure redirection policies that match specific traffic, redirecting it through multiple security tools before it enters or exits your data center using redirection.

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.

Step 1 On the **Redirections** tab, click + **Redirection**. The **Add Redirection** window is displayed.

Step 2 In the **Add Redirection** window, 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. 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 redirection, The priority of the redirection is set based on the existing redirections that are installed on the selected ingress ports. If auto-priority is enabled, redirection has a default priority of 10000. Next redirection with auto-priority enabled will have the priority value as the last priority minus 1. Without the auto-priority feature, the default value is 100. It can be changed in the range of <2-10000>. Priority value 1 is reserved for the backup bypass flows. Note The priority of the redirection should not be configured as 1. Also, if the last priority is configured as 2, you cannot clone the redirection with auto-priority enabled. You have to manually clone the redirection.
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.

Starting with Cisco Nexus Data Broker, Release 3.2.0, the order of the service nodes is maintained. For example, if you have added the service nodes s1, s2, and s3 to redirection in an order. The service nodes become operationally down and therefore, they get removed from the redirection. Once the nodes become operationally up, they are added to the redirection in the same order.

Step 6

Select the **Reverse ServiceNode Direction** option to enable reverse direction on the service node.

When you enable this option and click **Submit**, the ingress and egress ports of the service node are swapped and reverse redirection is enabled on the service node. The option is also displayed as enabled in the **Redirections** tab.

Step 7

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.

Step 8

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.

Field	Description
Select Monitor Traffic drop-down list	<p>When creating inline redirection with copy, the monitoring port receives one flow from the production ingress port and another from the egress port of service node.</p> <p>Starting with Cisco Nexus Data broker Release 3.2, a filtering mechanism is added in the GUI to filter out the traffic. Use the drop down list to select the traffic to copy device in redirection.</p> <p>The following optios are displayed in the drop-down list:</p> <ul style="list-style-type: none"> • Production Ingress-- Flow from the production ingress port • Production Egress-- Flow from the egress port of the service node • Both-- Flow from both the ports (the ingress and the egress ports)

Step 9 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 10 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 11 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 Src 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 12 Click **Close** to close the flow statistics display window.

Viewing Statistics

View the flow and port statistics for the switches on the Statistics tab.



Note

When you select a switch on the statistics page, the **Auto Refresh** tab for the switch is ON by default. Click **Auto Refresh: Off** to disable auto refresh on the Statistics tab. The screen is refreshed every 30 seconds and the updated statistics for the switch are displayed on the screen.

Step 1 Navigate to the **Statistics** tab under **Configuration** and click a node from the drop-down list to check and view the flow and port statistics of that node.

You can also navigate to the statistics of another switch by selecting the switch in the drop down box.

You can view the flow statistics, for example:

- Flow Name
- In Port
- DL Source

- DL Destination
- DL Type
- DL VLAN
- VLAN PCP
- NW Source
- NW Destination
- NW Proto
- TP Source
- TP Destination
- AP HttpMd
- AP TcpOptLn
- Actions
- Byte Count
- Packet Count
- Duration Seconds
- Idle Timeout
- Priority

Step 2 Click the **Ports** tab to check the ports statistics.
You can view the ports statistics as displayed in the following fields.

Note If you are programming the switches with OpenFlow, when you navigate to the **Statistics** tab, select a switch, and select **Ports** tab, the statistics gathered from the switches for the **Rx Frame Errs** and **Collisions** are not supported. The value of -1 is displayed rather than N/A because the variable needs to be an integer.

- Port Name
- Rx Packets
- Tx Packets
- Rx Bytes
- Tx Bytes
- Rx Rate (kbps)
- Tx rate (kbps)
- Rx Drops
- Tx Drops
- Rx Errors
- Tx Errors

- Rx Frame Errors
 - Rx Overrun Errors
 - Rx CRC Errors
 - Collisions
-

Adding SPAN Sessions

On the SPAN Sessions tab, the following fields are displayed:

- SPAN Session
- Filter
- Devices
- SPAN Source
- SPAN Destination

You can add a SPAN session in ACI.

- Step 1** Click + **SPAN Session** to add a SPAN session. The **Add SPAN Session** window is displayed.
- Step 2** In the **Add SPAN Session** window, add a session name in the **SPAN Session Name** field.
- Step 3** (Optional) Select a connection in the **Select Connections** field.
- Step 4** In the **Action** pane, select a priority for the SPAN session.
- Step 5** Select a rule using the drop-down list in the **Rule Filter** field. You can select the default filter rule, **Default-Match-IP** or select another filter from the drop-down list.
The available filter rules are **Default-Match-IP**, **Match-HTTP**, **Match-vlan**, and **Default-Match-all**.
- Step 6** Select a destination device to which the traffic is sent.
- Step 7** In the **SPAN SOURCES** pane, select the device type as ACI or NXOS in the **Select Device Type** field. When you select ACI device and click +Add SPAN Source, the **Add Leaf Ports** or +**Add EPG** tabs are displayed.
- In the **Add Leaf Ports** window, select a pod using the drop-down list in the **POD** field.
 - Select a node using the drop-down list in the **Node** field.
 - Select a port using the drop-down list in the **Port** field.
 - Click **Add Leaf Ports**.
 - In the **SPAN SOURCES** pane, select a direction from the **Incoming**, **Outgoing**, or **Both** options.
The selected Span source is displayed in the **Span Source** field.
 - If you select +**Add EPG** to add EPG source, select a tenant using the drop-down list in the **Tenant** field in the **Add EPG** window.

- Note**
- All EPG interfaces work only when all the ports are within the same leaf switch.
 - If same EPG is across multiple switches, you have to select the leaf switch and the associated ports. One SPAN session needs to be setup for each leaf switch.

- g) Select a profile using the drop-down list in the **Profile** field.
- h) Select EPG associated with the tenant using the drop-down list in the **EPG** field. The selected **SPAN Source** is displayed.
- i) Select **Include All EPG Interfaces** option.
When you enable this option, the statically configured interfaces are added to the EPG.

Note This option can be used only when all EPG sources are within the same leaf switch.

If the EPG is selected, by default, Cisco Nexus Data Broker listens for the changes in the statically configured interfaces of the selected EPG. If there is any change, it is applied to the SPAN session. The web socket connection is not secured with the certificates. To disable the event listening, add `enableWebSocketHandle=false` in the `config.ini` file under `xnc/configuration` folder.

- j) Click **Add EPG**.

Step 8 In the **SPAN SOURCES** pane, when you select the device type as NXOS in the **Select Device Type** field and click **+Add SPAN Source**, the **Add Interface** or **Add VLAN** tabs are displayed. This field allows to add NXOS SPAN session via NXAPI. It allows to add 2 types of SPAN sources. If you need to add interface as source, click **+ ADD SPAN Source** and click **Interface**. If you need to allow traffic of a particular VLAN, click **VLAN**.

Note You cannot add interfaces and VLAN as SPAN source for the same NXOS SPAN session.

You cannot have ACI and NXOS SPAN sources in the same SPAN session.

Step 9 When you click **+Add Interface**, the **Add Production Switch Interface** window is displayed. You can select a node, select an interface, and click **Submit**.

Step 10 When you click **+Add VLAN**, the **Add Production Switch VLAN** window is displayed. You can select a node, enter a VLAN, and click **Submit**.

Step 11 In the **SPAN Destination** field, you can select the SPAN destination. This field displays SPAN destination for ACI in the ACI SPAN session or SPAN destination for NXOS in the NXOS SPAN session.

Note The SPAN destination should be the same leaf where the SPAN sources are being selected.

SPAN destination and SPAN source interface of ACI should be in the same node. If both are in different nodes, the SPAN session cannot be created.

Step 12 Click **Add SPAN Session**.
A message box is displayed asking you to confirm, **Are you sure you want to add SPAN session?**, if you want to add the SPAN session.

Step 13 Click **OK**.
As a result, a SPAN session is set up in ACI. It also sets up a connection automatically on the Cisco Nexus Data Broker with the same SPAN session name and this connection redirects the traffic from that source port to the monitoring device.

Note Each leaf can have a maximum of 4 SPAN sessions.

You can set up additional SPAN sessions. You can append a new SPAN session to the existing connection. In that case, you can select the new SPAN session in the Add SPAN Session window, use the same connection that is previous ly created, select new SPAN sources from different leaf ports, select the SPAN destination, and add the SPAN session.

It creates a new session in ACI, but it appends an existing connection to include the new traffic on the Cisco Nexus Data Broker side.

You can edit or clone the existing SPAN sessions. If you want to remove a SPAN session, click the session and click **Remove SPAN Session(s)**. A message box is displayed asking you to confirm, **Remove the following sessions?**, if you want to remove the displayed SPAN session. Click **Remove SPAN Sessions** to confirm. If the SPAN session is using an existing connection, the connection is updated automatically with the changes. If it is the last connection associated with the SPAN session, the connection is deleted.
