Components

This chapter has details about the components of the Cisco Nexus Data Broker.

Filters

The **Filters** tab displays details of all the filters available on the NDB controller. The tab provides information of the filtering criteria (used in a connection) for the incoming traffic.

The default filters include the following protocols for packet filtering:

- Default-match-all
- Default-match-IP
- Default-match-ARP
- Default-match-MPLS (unicast and multicast)
- Default-match-ICMP
- Default-match-ICMP-All

A table is displayed with the following details:

Table 1: Filters

Column Name	Description
In Use	A green tick mark indicates that the filter is in use, in a connection.

Column Name	Description
Filter	The filter name. Click **Filter**. A new pane is displayed on the right which has more information about the filter. The following additional actions can be performed from here: • Editing or Cloning a Filter **Note** Default filters cannot be edited.
Bidirectional	If a filter is bidirectional, a **Yes** is displayed; else a **No** is displayed. If a filter is marked bidirectional, incoming and outgoing traffic is filtered at the same port.
Ethertype	Layer 2 ethertype of the filter.
Protocol	Layer 3 protocol used by the filter.
Advanced Filter(s)	The advanced filters associated with the filter.
Created By	The user who created the filter.
Last Modified By	The user who last modified the filter.

The following actions can be performed from the **Filters** tab:

- **Add Filter**—Use this to add a new filter. See Adding a Filter for details about this task.
- **Delete Filter**—Select the filter(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Filter(s)**. The selected filter(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a filter.

Adding a Filter

Use this procedure to add a filter. The incoming traffic is matched based on the parameters defined in a filter.

Step 1 Navigate to **Components** > **Filters**.

Step 2 From the **Actions** drop down menu, select **Add Filter**.

Step 3 In the **Add Filter** dialog box, enter the following details:

Table 2: Add Filter

Field	Description
Filter Name	Enter a name for the filter.

Field	Description
Bidirectional	Check this box if you want the filter to capture bidirectional traffic information, that is, 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.

Layer 2	The options displayed for using Layer 2 filtering are:
	• Ethernet Type—Select the Ethernet Type from the drop-down list. The options are:
	  • IPv4
	  • IPv6
	  • LLDP
	  • MPLS
	  • ARP
	  • All Ethernet Types
	  • Predefined Ethernet Types— If you choose this option, all predefined Ethernet types contained in the `config.ini` file are associated with the rule, and you should not configure any other parameters.
	  • Enter Ethernet Type—If you choose this option, enter the ethernet type in hexadecimal format.
	• VLAN Identification Number—Enter 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.
	Maximum value is 4095.
	• VLAN Priority—Enter the VLAN priority for the traffic. VLAN Priority is matched for Layer 2 traffic only.
	• Source MAC Address—Enter the MAC address of the source device. MAC addresses are matched for Layer 2 traffic only.
	• Destination MAC Address—Enter the MAC address of the destination device. MAC addresses are matched for Layer 2 traffic only.
	• MPLS Label Value—Enter the MPLS value for Label 1, Label 2, Label 3, Label 4.
	The **MPLS Label Value** fields are displayed only if the **Ethernet Type** is set to MPLS. The MPLS label values are matched.

Field	Description
Layer 3 To enable options for Layer 3, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab.	

Field	Description

	The options displayed for Layer 3 filtering are:
	• Source IP Address—Enter the Source IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• Destination IP Address—Enter the Destination IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• L4 Protocol—Select a Layer 4 protocol from the drop down list or enter a **Protocol Number**.
	• Advanced Filter—Click the button to enable advanced filtering and check the check-boxes to select the required options. For details about the options pertaining to Advanced Filters, see Advanced Filters.
	• Custom Filter—Click the button to enable custom filtering using User Defined Fields (UDF). Click **Select UDFs** and select a filter in the **Select Custom Filters** window. The

Field	Description
	UDFs created using Adding a User Defined Field are displayed here. The selected UDF(s) are displayed in a table. Enter the following details for the selected UDF: • Value—is the value to be matched in decimal notation (0-65535). E.g. if you want to match 0x0806 enter 2054 which is 0x0806 in decimal notation. • Mask—is the mask to be applied to the value for matching purposes. E.g. to exactly match 2054 (0x0806) enter 65535 (0xffff), to match 2048-2063 (0x0800-0x080f) use 65520 (0xfff0). **Note** When the monitoring tool port is on an ISL device, it is mandatory to select **Add Default UDF for inner vlan** checkbox. Ensure the input port has Q-in-Q configured.

Field	Description

Layer 4
To enable options for Layer 4, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab and choose **TCP** or **UDP** as **L4 Protocol** under the Layer 3 tab.
	The options displayed for Layer 4 filtering are:
	• Source Port—Select the source port from the drop down list. The options are:
	  • FTP (Data)
	  • FTP (Control)
	  • SSH
	  • Telnet
	  • HTTP
	  • HTTPS
	  • Enter Source Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers.
	  Note If you enter a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP addresses or Layer 2 VLAN identifiers.
	• Destination Port—Select the destination port from the drop down list. The options are:
	  • FTP (Data)
	  • FTP (Control)
	  • SSH
	  • Telnet
	  • HTTP
	  • HTTPS
	  • Enter Destination Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers.
	  Note If you enter a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers or Layer 3 IP addresses.

Layer 7	Not supported.

Note For Custom Filtering: You can add upto four UDFs for a filter. UDF option is enabled for IPv4 and IPv6 ethertypes.

Step 4 Click **Add Filter** to add the filter.

Editing or Cloning a Filter

Use this procedure to edit or clone a filter.

Editing a filter means changing the parameters of an existing filter.

Cloning a filter means creating a new filter with the same parameters of an existing filter and making the required changes to the filter parameters. Ensure to change the name of the filter before saving it.

Note Default filters cannot be edited.

Before you begin

Add one or more filters.

Step 1 Navigate to **Components** > **Filters**.

Step 2 In the displayed table, click a **Filter**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Clone Filter**.

Step 4 In the **Clone Filter** or **Edit Filter** dialog box, the current filter information is displayed. Modify these fields, as required:

Table 3: Edit/ Clone Filter

Field	Description
Filter Name	Name of the filter.
Bidirectional	Check this box if you want the filter to capture bidirectional traffic information, that is, 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.

Field	Description

Layer 2	The options displayed while using Layer 2 are:
	• Ethernet Type—Select the Ethernet Type from the drop-down list. The options are:
	  • IPv4
	  • IPv6
	  • LLDP
	  • MPLS
	  • ARP
	  • All Ethernet Types
	  • Predefined Ethernet Types— If you choose this option, all predefined Ethernet types contained in the `config.ini` file are associated with the rule, and you should not configure any other parameters.
	  • Enter Ethernet Type—If you choose this option, enter the ethernet type in hexadecimal format.
	• VLAN Identification Number—Enter 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.
	Maximum value is 4095.
	• VLAN Priority—Enter the VLAN priority for the traffic.
	VLAN Priority is matched for Layer 2 traffic only.
	• Source MAC Address—Enter the MAC address of the source device.
	MAC addresses are matched for Layer 2 traffic only.
	• Destination MAC Address—Enter the MAC address of the destination device.
	MAC addresses are matched for Layer 2 traffic only.
	• MPLS Label Value—Enter the MPLS value for Label 1, Label 2, Label 3, Label 4.
	The **MPLS Label Value** fields are displayed only if the **Ethernet Type** is set to MPLS. The MPLS label values are matched.

Field	Description
Layer 3 To enable options for Layer 3, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab.	

Field	Description

	The options displayed while using Layer 3 are:
	• Source IP Address—Enter the Source IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• Destination IP Address—Enter the Destination IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• L4 Protocol—Select a Layer 4 protocol from the drop down list.
	• Advanced Filter—Click the button to enable advanced filtering and check the check-boxes to select the required options. For more details about Advanced Filters, see Advanced Filters.
	• Custom Filter—Click the button to enable custom filtering using User Defined Fields (UDF). Click **Select UDFs** and select a filter in the **Select Custom Filters** window.

Field	Description

Layer 4
To enable options for Layer 4, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab and choose **TCP** or **UDP** as **L4 Protocol** under the Layer 3 tab.
	The options displayed while using Layer 4 are:
	• Source Port—Select the source port from the drop down list. The options are:
	  • FTP (Data)
	  • FTP (Control)
	  • SSH
	  • Telnet
	  • HTTP
	  • HTTPS
	  • Enter Source Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers.
	  Note If you enter a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP addresses or Layer 2 VLAN identifiers.
	• Destination Port—Select the destination port from the drop down list. The options are:
	  • FTP (Data)
	  • FTP (Control)
	  • SSH
	  • Telnet
	  • HTTP
	  • HTTPS
	  • Enter Destination Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers.
	  Note If you enter a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers or Layer 3 IP addresses.

Layer 7	Not supported.

Step 5 Click **Edit Filter** or **Clone Filter**.

Advanced Filters

Advanced filtering provides multiple options to filter (permit or deny) the traffic based on Ethernet type and attributes such as Acknowledgment, FIN, Fragments , PSH, RST, SYN, DSCP, Precedence, TTL, packet-length, and NVE. Advanced filtering is available for the following Ethernet types and options:

Table 4: Advanced Filtering Support

Data Type	Supported Options
IPv4	DSCP, Fragment, Precendence, and TTL
IPv4 with TCP	Acknowledgment, DSCP, Fragment, FIN, Precedence,PSH, RST, SYN, and TTL
IPv4 with UDP	DSCP, Fragment, Precendence, and TTL
IPv6	DSCP and Fragment
IPv6 with TCP	Acknowledgment, DSCP, Fragment, FIN, PSH, RST,and SYN
IPv6 with UDP	DSCP and Fragment

Note Advanced Filtering is available only for NX-API on Cisco Nexus 9000 platform.

The Time to Live (TTL) attributes range from 0 to 255. For Nexus 9200 devices, the maximum value of TTL that can be set is 3. For rest of the Nexus 9000 series devices, the maximum TTL value can be 3 for NX-OS version 7.0(3)I6(1) and above. For NXOS versions 7.0(3)I4(1) and below, you can configure any value within the range.

Limitations for using Advanced Filtering

While configuring Advanced Filters, you cannot:

- Configure DSCP and precedence together.
- Configure fragments and ACK or SYN or FIN or PSH or RST together.
- Configure fragments and port numbers with UDP and IPv4 or IPv6 combination.
- Configure precedence and HTTP methods with IPv4 and TCP combination.

Global Configuration

The **Global Configuration** tab displays the devices connected to the NDB controller. New devices added to the NDB controller are displayed here by default.

Note Only *Connected* devices (connection status indicated in green) are displayed here. If a device is added to the NDB controller, but is *not connected* (connection status indicated in red), then, that device is not displayed here. To check the status of a device, see NDB Devices.

A table with the following details is displayed:

Table 5: Global Configuration

Column Name	Description
Device	The device name. This is a hyperlink, click the **Device** name to get the global configuration details of the device.
Loadbalancing	Displays the type of load balancing. The options are: • Symmetric • Non-symmetric
PTP	Displays if PTP is enabled or not. The options are: • Enabled • Disabled
Jumbo MTU	The Jumbo MTU size for the device. Jumbo MTU is the maximum MTU that can be configured for a device.
MPLS Strip	Displays if MPLS stripping is enabled or not on the device. The options are: • Enabled • Disabled
MPLS Filter	Displays if MPLS filtering on the device, is enabled or not. The options are: • Enabled • Disabled
Netflow	Displays if Netflow on the device, is enabled or not. The options are: • Enabled • Disabled

The following actions can be performed from the **Global Configuration** tab:

- **Edit Global Configuration**—For details of the procedure, see Editing Global Configuration for a Device, on page 15.

Editing Global Configuration for a Device

Use this procedure to edit global configuration for a device. You can make global changes to the parameters of a device. For example, the Jumbo MTU value set here, defines the MTU value for an input port of the device.

When a device is created, some basic configurations are created and some default values are set. Use this procedure to change or add one or more parameters for a device.

Before you begin

Create one or more devices. Check the status of the device.

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, enter the following details:

Table 6: Edit Global Configuration

Field	Description
General	
Device	The device name is displayed based on your earlier selection.
Load Balancing Type Configuration	Select **Symmetric** or **Non-symmetric** from the drop-down list. For details about load balancing, see Symmetric and Non-Symmetric Load Balancing.
Hashing Configuration	Select a hashing configuration from the drop-down list. The displayed drop-down list is dynamic and depends on the selected load balancing type.
Hashing Type	Select a hashing type from the drop-down list.
MPLS Configuration	
MPLS Strip Type Configuration	Click the gray button to enable MPLS strip type configuration. The button turns blue and moves to the right. All the MPLS packets from the input ports are stripped of the MPLS header. **Note** On Cisco Nexus 9300-GX Series switches, MPLS strip feature works only after switch reload.

Field	Description
Label Age	Set the time period after which the MPLS labels will age out. This field is available only for select devices. Supported platforms are the following Cisco Nexus Series switches - 93128TX, 3172, 3164, 3232, 3132C-Z.
Enable MPLS Filter Configuration	Click the gray button to enable MPLS filter configuration. The button turns blue and moves to the right. MPLS filter configuration enabled here, is applied to the input port of the device.
sFlow Configuration	
Enable sFlow	Click the gray button to enable Sampled Flow (sFlow). The button turns blue and moves to the right. For details about sFlow, see Sampled Flow. Enter the following details: • **Agent IP Address**— Enter the agent ip address. • **Select VRF**—Select a VRF from the drop-down list. • **Collector IP Address** —Enter an IP address for the collector port. • **Collector UDP Port** —Enter the UDP port for the sFlow collector. • **Counter Poll Interval**—Enter a poll interval value for sFlow. • **Max Datagram Size**—Enter the maximum datagram size. • **Max Sampled Size**—Enter the maximum sampled size. • **Sampling Rate** —Enter the data sampling rate. • **Data Sources**—Click **Select Ports** and select the ports by checking the required check boxes and click **Add**. **Note** To verify sflow configuration on a device, use the **show sflow** command.
PTP Configuration	

Field	Description
Enable PTP	Click the gray button to enable PTP and receive updates from the master. The button turns blue and moves to the right. PTP enabled here is used for timestamping in the inputs ports and monitoring tools. For details about PTP, see Precision Time Protocol. The following fields are displayed: • **Source IP Address**— Enter the source IP address for receiving PTP updates. • **Ports**—Click **Select Ports** and check the check boxes to select the required ports to which the PTP source IP is connected. **Note** You need to enable PTP for all the devices in the network to ensure PTP clock time synchronization.
Jumbo MTU Configuration	
MTU Value	Enter MTU value; range is 1502 to 9216. Jumbo MTU sets the maximum MTU value the device can accept. MTU size for traffic is typically 1500. To receive traffic with MTU more than 1500, enable this. The MTU value defined here is applied on the incoming traffic on the input ports of a device. Click **Reset to Default** to set the MTU value to the default value of 1500. **Note** MTU value must be an even number, in the specified range.
Netflow Configuration	
Enable Netflow	Click the gray button to enable netflow. The button turns blue and moves to the right. For details about Netflow, see Netflow. To define the Netflow parameters, complete the following configurations (in the specified order): • Adding a Record for NetFlow, on page 18 • Adding an Exporter for NetFlow, on page 19 • Adding a Monitor for NetFlow, on page 20 To complete the NetFlow configuration, associate the NetFlow Monitor to an input port. See Adding an Input Port.

Step 5 Click **Edit Global Configuration** .

Adding a Record for NetFlow

Use this procedure to create a NetFlow record.

A flow record defines the keys that NetFlow uses to identify packets and other fields of interest that NetFlow gathers for the flow. The flow record determines the size of the data to be collected for a flow. The key fields are specified with the *match* keyword.

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, click the gray button to **Enable Netflow**.

Step 5 Click **Add Record** and enter the following details:

Table 7: Add Record

Field	Description
Name	Name of the record.
Description	Description for the record.
Collect	Define the collection parameters. Check the corresponding check box to enable collection based on one or more of the following parameters: • Counter Bytes • Counter Packets • IP Version • Transport TCP Flags • System Uptime First • System Uptime Last
Match	Define the match parameters. The options available are **Layer 2** and **Layer 3/4**. Click either of them to select the match parameters. These parameters are discussed in the subsequent rows.

Field	Description
Layer 2	Check the check box to enable one or more matching Layer 2 parameters. • Mac Source Address • Mac Destination Address • Ethertype • VLAN
Layer 3/4	Check the check box to enable one or more matching Layer 3 and/or Layer 4 parameters. • IP Protocol • IP TOS • Transport Source Port • Transport Destination Port • IPv4 Source Address • IPv4 Destination Address • IPv6 Source Address • IPv6 Destination Address • IPv6 Flow Label • IPv6 Options

Step 6 Click **Add Record**.

Adding an Exporter for NetFlow

Use this procedure to create a NetFlow exporter. The flow exporter configuration defines the export parameters for a flow and specifies reachability information for the remote NetFlow Collector.

A flow exporter contains network layer and transport layer details for the NetFlow export packet.

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, click the gray button to **Enable Netflow**.

Step 5 Click **Add Exporter** and enter the following details:

Table 8: Add Exporter

Field	Description
Name	Name of the exporter.
Description	Description of the exporter.
Destination	Export destination IP address. Check the corresponding check box to enable collection based on one or more of the following parameters:
Source	Source IP address. Interface on the device through which the flow cache reaches the destination.
UDP Port	UDP port where the NetFlow collector is listening for NetFlow packets. The range is from 1 to 65535.
DSCP	The differentiated services codepoint value. The range is from 0 to 63.
Version	The NetFlow export version. This field cannot be changed. **Note** Cisco NX-OS supports the Version 9 export format.
Option Exporter	Flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Template Data Timeout	Template data resend timer. The range is from 1 to 86400 seconds.

Step 6 Click **Add Exporter**.

Adding a Monitor for NetFlow

Use this procedure to create a NetFlow monitor.

You can create a flow monitor and associate it with a flow record and a flow exporter. All of the flows that belong to a monitor use the associated flow record to match on the different fields, and the data is exported to the specified flow exporter.

Before you begin

Complete the following configurations:

- Adding a record
- Adding an exporter

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, click the gray button to **Enable Netflow**.

Step 5 Click **Add Monitor** and enter the following details:

Table 9: Add Monitor

Field	Description
Name	Name of the monitor.
Description	Description of the monitor.
Record	Click **Select Record**. In the **Select Record** window, choose a record by clicking the corresponding radio button. The details of the selected record are displayed on the right. Click **Select**.
Exporter	Click **Select Exporter**. In the **Select Exporter** window, choose an exporter by selecting the corresponding check box. The details of the selected exporter are displayed on the right. Click **Select**. **Note** You can select a maximum of two flow exporters for a monitor

Step 6 Click **Add Monitor**.

Symmetric and Non-Symmetric Load Balancing

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

The following table lists the symmetric and non-symmetric load balancing options:

Configuration Type	Hashing Configuration	Platforms	Options
Symmetric	SOURCE_DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC, IP-ONLY,PORT-ONLY
Non-symmetric	SOURCE, DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC

Sampled Flow

You can manage Sampled Flow (sFlow) on NDB that are based on NX-API. sFlow allows you to monitor real-time traffic in data networks that contain switches and routers. It uses the sampling mechanism in the sFlow agent software on switches and routers to monitor traffic and to forward the sample data to the central data collector.

See Editing Global Configuration for a Device, on page 15 for configuring sFlow.

Precision Time Protocol

Precision Time Protocol (PTP) devices include ordinary clocks, boundary clocks, and transparent clocks. Non-PTP devices include ordinary network switches, routers, and other infrastructure devices. A PTP system can consist of a combination of PTP and non-PTP devices.

PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other. These clocks are organized into a master-member synchronization hierarchy with the grandmaster clock, the clock at the top of the hierarchy, determining the reference time for the entire system. Synchronization is achieved by exchanging PTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. PTP operates within a logical scope called a PTP domain.

PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides excellent accuracy.

PTP is supported on the following platforms:

- Cisco Nexus 9200 switches
- Cisco Nexus 9300 switches—9300-FX, FX2, EX
- Cisco Nexus 9500 switches—9500-FX, EX
- Cisco Nexus 3548 switches

Note After PTP is configured, the default PTP configuration is synchronized with all the ISL ports of the corresponding device.

See Editing Global Configuration for a Device, on page 15 for configuring PTP.

Netflow

NetFlow identifies packet flows for ingress IP packets and provides statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

In order to provide enough free space to monitor flows, the ing-netflow TCAM region is carved to 512 by default on Cisco Nexus 9300-FX platform switches. If more space is required, use the **hardware access-list tcam region ing-netflow size** command to modify the size of this TCAM region, using a multiple of 512.

Netflow is supported on the following platforms:

- Cisco Nexus 9300 switches—9300-FX, FX2, EX

- Cisco Nexus 9500 switches—9500-FX, EX

See Editing Global Configuration for a Device, on page 15 for configuring Netflow.

For more information about Netflow, see *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.*

Input Ports

The **Input Ports** tab displays details of the inputs ports on the NDB devices.

When an Edge-SPAN or an Edge-TAP or an Remote Source Edge-SPAN port is defined in the NX-API mode of configuration, the **spanning-tree bpdufilter enable** command 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.

Ensure to configure the **spanning-tree bpdufilter enable** command on all the inter-switch ports for Cisco Nexus series switches.

A table with the following details is displayed:

Table 10: Input Ports

Column Name	Description
Device	The device on which the input port is configured. This field is a hyperlink. Click the Device name to view more information about the device. For details and procedure, see Devices chapter.
Port	The port of the device that is configured as an input port. This field is a hyperlink. Click a **Port** to view more details of the port. Additional actions that can be performed from here are: • Editing an Input Port • Remove Configuration—the port is removed as an input port for the device.
In Use	A green tick mark indicates that the input port is in use.
Configuration	The configuration information of the input port (based on the parameters set during Adding an Input Port).

Column Name	Description
Type	Port type. The displayed options are: • Edge port-SPAN • Edge port-TAP • Remote Source Edge-SPAN • Packet Truncation
Span Destination	Details of the span destination. If the port is connected to ACI, then the DN value is displayed; if the port is connected to a production switch (NX-OS), then the device ID (of the production switch) with interface(s) are displayed.
Created By	The user who created the the input port.
Modified By	The user who last modified the input port.

The following actions can be performed from the **Input Ports** tab:

- **Add Input Port** —Use this to add a new input port. See Adding an Input Port for details about this task.
- **Delete Input Port** —Select the required input port by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Input Port(s)**. The selected port(s) is deleted.

Note *In Use* input ports cannot be deleted.

If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Adding an Input Port

Use this procedure to create an input port.

Input port of a device is the port through which traffic enters the packet broker network and is directed to the monitoring tool.

Before you begin

Add one or more devices.

Some of the input port parameters are defined at the device-level using the **Global Configuration** tab. To define these parameters (listed below), see Editing Global Configuration for a Device.

- PTP
- Netflow
- MPLS Filtering

- Jumbo MTU

Step 1 Navigate to **Components** > **Input Port Configuration**.

Step 2 From the **Actions** drop-down list, select **Add Input Port**.

Step 3 In the **Add Input Port** dialog-box, enter the following details:

Table 11: Add Input Port

Field	Description
General	
Device	To select a device on which the input port is being configured. Click **Select Device** . From the **Select Device** window, select a radio button and choose a device. Click **Select**.
Port(s)	To select a port to be configured as the input port. Click **Select Port**. From the **Select Port** window, select the required port(s). Click **Select**.
Port Type	Select from the drop-down list to define the input port type. The options are: • **Edge Port - SPAN** —creates an edge-port for incoming traffic from a configured session of the production switch . • **Edge Port- TAP**—creates an edge port for incoming traffic from a physical device on an ISL. • **Remote Source Edge - SPAN** —creates an edge-port for incoming traffic from a configured remote session of the production switch.
Port Description	Enter a description for the port.
VLAN ID (QinQ Supported)	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. **Note** After an interface is configured with Q-in-Q, do not configure VLAN filters for the Q-in-Q configured interface.
Block-Tx	Check the check-box to block the traffic that is being transmitted from the input ports. **Note** Only unicast and multicast traffic is blocked.

Field	Description
Drop ICMP v6 Neighbour Solicitation	Check the check-box to drop all ICMP traffic. By default, all the ICMP traffic is blocked for Edge-SPAN and Edge-TAP port types for Nexus 9300-EX and 9200 Series switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic. This feature is currently available on NX-API based switches for NX-OS versions I5 and later.
Enable Timestamp Tagging	Check the check-box to append the timestamp tag on packets using the Timestamp Tagging feature. For Nexus 9300-EX and 9200 series switches, this feature is applicable for Edge-SPAN and Edge-TAP ports. To configure Timestamp Tagging feature, ensure that PTP feature is enabled on the device. You need to enable Timestamp tagging on monitoring device and edge ports. If Timestamp Tagging feature is not configured on either side of the connection, Edge-SPAN/Edge-TAP and Monitor Devices, the packets are not tagged with timestamp. **Note** If PTP is not enabled for the device using Global Configuration, then this option is grayed out.
Enable MPLS Filtering	Check the check-box to enable MPLS filtering. **Note** If MPLS filtering is not enabled for the device using Global Configuration, then this option is grayed out.
Apply Jumbo MTU	Check the check-box to enable the set Jumbo MTU value on this port. **Note** If Jumbo MTU is not configured for the device using Global Configuration, then this option is grayed out.
Netflow Monitor	Select an option from the drop-down list. The monitor names created at the Global Configuration level are listed here. **Note** If NetFlow is not enabled for the device using Global Configuration, then this option is grayed out.

The unique fields displayed for each **Port Type** are discussed below.

a) (Only for **Port Type**—Edge Port-SPAN) Enter the following details:

Field	Description
Destination Device Type	This is the source for the input ports (Span Destination). Select the required option from the drop down list. The options are: • ACI • NX-OS Device The options for each of the above are discussed in the subsequent rows.
Fields for **Destination Device Type : ACI** **Note** You must add an APIC/ ACI device before you configure SPAN destination.	
Span Destination Name	Enter a name for Span Destination.
Pod	Select a pod.
Node	Select a node.
Port	Select a port.
MTU	Set an MTU value for the span destination of APIC.
Fields for **Destination Device Type: NX-OS Device** **Note** You must add an NX-OS device before you configure SPAN destination.	
Span Destination Device	Click **Select Device** and select a device.
Span Destination Port	Click **Select Port** and select a port.

b) No unique fields are dispalyed, when you select **Port Type** as Edge-Port TAP.

c) (Only for **Port Type**—Remote Source Edge-SPAN) Enter the following details:

Note You can configure a maximum of four Remote Source Edge-SPAN ports, to receive traffic from a remote source.

Field	Description
Remote Input Termination Session	
ERSPAN ID	Enter an ERSPAN ID. Range is from 1 to 1023. The ERSPAN id entered here is matched with the source session id in the remote source.
Use Loopback Interface	Check the check-box to use a loopback interface.

Field	Description
Loopback	Click **Select Loopback** to select a loopback interface. If there are no configured loopback interfaces, click **Add Loopback**. See Configuring Loopback. Use a loopback interface to have more than one remote input port. Traffic from an L3 interface reaches the loopback interface and from there the session destination port. If the first remote source edge span input port was created with a loopback, then the following Remote Source Edge-SPAN ports must also be configured with the same loopback interface. If the first remote source edge span input port was created without a loopback, then the following Remote Source Edge-SPAN ports must also be configured without a loopback interface.
Session Destination	Click **Select Destination Port** and select a destination port (on the NDB device).
Remote Input Session	
Remote Input Port	Click **Remote Input Port** and select a remote input port (on the NDB device). **Note** Only one remote input port can be configured for the traffic reaching the Remote Source Edge-SPAN ports. If you have configured a loopback interface, then, the remote input ports can be different for each of the Remote Source Edge-SPAN ports.
IP Address	Enter an IP address. IP address entered here is the IP address of the remote source port to which the packets reach over L3 network. You need to enter this value only when configuring the first Remote Source Edge-SPAN port. For the next three ports that you configure, this field is grayed out as the same IP address is applied to all the four sessions with Remote Source Edge-SPAN ports.
Destination Device Type	Select the device type from the drop down list. For Remote Source Edge-SPAN ports, the supported destination type is ACI.
Span Destination ACI Fabric	Click **Select ACI Fabric** and select an ACI fabric.
Span Destination Name	Enter a name for the span destnation.
Tenant	Click **Select Tenant** to select a tenant.
Application Profile	Click **Select Application Profile** to select an application profile.
EPG	Click **Select EPG** to select an EPG.

Field	Description
Source IP Address	Enter the source IP address. This IP address is the base IP address of the IP subnet of the source packets.
Destination IP Address	This field is automatically populated. The IP address populated here is the same address that you entered as the IP address of the **Remote Input Port**. **Note** For APIC/ ACI devices, this is the destination port (remote input port), and hence called destination IP.
Flow ID	This field is automatically populated. Flow ID is the flow identifier of the SPAN packet. It is matched with the ERSPAN ID earlier specified for the Remote Source Edge-SPAN port.
TTL	Enter a TTL value. Default value is 64 hops.
DSCP	Select a DSCP value from the drop-down list.
MTU	Enter an MTU value for the span destination port. Range is from 64 to 9216.

Step 4 Click **Add Input Port**.

Editing an Input Port

Use this procedure to edit an input port.

Before you begin

Add one or more input ports.

Step 1 Navigate to **Components** > **Input Ports**.

Step 2 In the displayed table, click a **Port**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Port**.

Table 12: Edit Input Port

Field	Description
General	

Field	Description
Device	The device name on which the input port is configured. This field cannot be edited.
Port(s)	The port configured as an input port. This field cannot be edited.
Port Type	Select from the drop-down list to define the input port type. The options are: • **Edge Port - SPAN** —creates an edge-port for incoming traffic from a configured session of the production switch . • **Edge Port- TAP**—Creates an edge port for incoming traffic from a physical device on an ISL. • **Remote Source Edge - SPAN** —creates an edge-port for incoming traffic from a configured remote session of the production switch.
Port Description	Enter a description for the port.
VLAN ID (QinQ Supported)	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. **Note** After an interface is configured with Q-in-Q, do not configure VLAN filters for the Q-in-Q configured interface.
Block-Tx	Check the check-box to block the traffic that is being transmitted from the input ports. **Note** Only unicast and multicast traffic is blocked.
Drop ICMP v6 Neighbour Solicitation	Check the check-box to drop all ICMP traffic. By default, all the ICMP traffic is blocked for Edge-SPAN and Edge-TAP port types for Nexus 9300-EX and 9200 Series switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic. This feature is currently available on NX-API based switches for NX-OS versions I5 and later.

Field	Description
Enable Timestamp Tagging	Check the check-box to append the timestamp tag on packets using the Timestamp Tagging feature. For Nexus 9300-EX and 9200 series switches, this feature is applicable for Edge-SPAN and Edge-TAP ports. To configure Timestamp Tagging feature, ensure that PTP feature is enabled on the device. You need to enable Timestamp tagging on monitoring device and edge ports. If Timestamp Tagging feature is not configured on either side of the connection, Edge-SPAN/Edge-TAP and Monitor Devices, the packets are not tagged with timestamp. **Note** If PTP is not enabled for the device using Global Configuration, then this option is grayed out.
Enable MPLS Filtering	Check the check-box to enable MPLS filtering. **Note** If MPLS filtering is not enabled for the device using Global Configuration, then this option is grayed out.
Apply Jumbo MTU	Check the check-box to enable the set Jumbo MTU value on this port. **Note** If Jumbo MTU is not configured for the device using Global Configuration, then this option is grayed out.
Netflow Monitor	Select an option from the drop-down list. The monitor names created at the Global Configuration level are listed here. **Note** If NetFlow is not enabled for the device using Global Configuration, then this option is grayed out.
Destination Device Type Applicable only when the Port Type is, **Edge Port - SPAN**.	This is the source for the input ports (Span Destination). Select the required option from the drop-down list. The options are: • ACI • NX-OS The options for each of the above are discussed in the subsequent rows.
Destination Device Type: ACI **Note** You must add an APIC/ ACI device before you configure SPAN destination.	
Span Destination ACI Fabric	Click **Select ACI Fabric**. and select an ACI Fabric. Click **Select**.
Span Destination Name	Enter a name for Span Destination.
Pod	Select a pod.
Node	Select a node.

Field	Description
Port	Select a port.
MTU	Set an MTU value for the span destination of APIC.
Destination Device Type: NX-OS Device **Note** You must add an NX-OS device (production device) before you configure SPAN destination.	
Span Destination Device	Click **Select Device** and select a device in the Select Device window.
Span Destination Port	Click **Select Port** and select a port in the Select Port window.
Options available when **Port Type** is **Remote Source Edge - SPAN**. **Note** You can configure a maximum of four Remote Source Edge-SPAN ports, to receive traffic from a remote source. Enter the following **Remote Input Termination Session** details:	
ERSPAN ID	Enter an ERSPAN ID. Range is from 1 to 1023. The ERSPAN id entered here is matched with the source session id in the remote source.
Use Loopback Interface	Check the check-box to use a loopback interface.
Loopback	Click **Select Loopback** to select a loopback interface. If there are no configured loopback interfaces, click **Add Loopback**. See Configuring Loopback. Use a loopback interface to have more than one remote input port. Traffic from an L3 interface reaches the loopback interface and from there the session destination port. If the first remote source edge span input port was created with a loopback, then the following Remote Source Edge-SPAN ports must also be configured with the same loopback interface. If the first remote source edge span input port was created without a loopback, then the following Remote Source Edge-SPAN ports must also be configured without a loopback interface.
Session Destination	Click **Select Destination Port** and select a destination port (on the NDB device).
Enter the following **Remote Input Session** details:	
Remote Input Port	Click **Remote Input Port** and select a remote input port (on the NDB device). **Note** Only one remote input port can be configured for the traffic reaching the Remote Source Edge-SPAN ports. If you have configured a loopback interface, then, the remote input ports can be different for each of the Remote Source Edge-SPAN ports.

Field	Description
IP Address	Enter an IP address. IP address entered here is the IP address of the remote source port to which the packets reach over L3 network. You need to enter this value only when configuring the first Remote Source Edge-SPAN port. For the next three ports that you configure, this field is grayed out as the same IP address is applied to all the four sessions with Remote Source Edge-SPAN ports.
Destination Device Type	Select the device type from the drop-down list. For Remote Source Edge-SPAN ports, the supported destination type is ACI.
Span Destination ACI Fabric	Click **Select ACI Fabric** and select an ACI fabric.
Span Destination Name	Enter a name for the span destnation.
Tenant	Click **Select Tenant** to select a tenant.
Application Profile	Click **Select Application Profile** to select an application profile.
EPG	Click **Select EPG** to select an EPG.
Source IP Address	Enter the source IP address. This IP address is the base IP address of the IP subnet of the source packets.
Destination IP Address	This field is automatically populated. The IP address populated here is the same address that you entered as the IP address of the **Remote Input Port**. **Note** For APIC/ ACI devices, this is the destination port (remote input port), and hence called destination IP.
Flow ID	This field is automatically populated. Flow ID is the flow identifier of the SPAN packet. It is matched with the ERSPAN ID earlier specified for the Remote Source Edge-SPAN port.
TTL	Enter a TTL value. Default value is 64 hops.
DSCP	Select a DSCP value from the drop-down list.
MTU	Enter an MTU value for the span destination port. Range is from 64 to 9216.

Step 4 Click **Edit Input Port**.

Configuring Loopback

Use this procedure to configure a loopback for the Remote source edge span input port.

Step 1 Navigate to **Inputs Ports** > **Actions** > **Add Input Ports**.

Step 2 Select **Port Type** as Remote Source Edge Span Port and select the **Use Loopback Interface** check-box to select a loopback interface.

Step 3 Click **Configure Loopback** to create a new loopback interface.

In the **Configure Loopback** dialog-box, enter the following details:

Table 13: Configure Loopback

Field	Description
General	
Loopback Id	Enter a loopback ID.
IP Address	Enter the loopback IP address.

Step 4 Click **Configure Loopback**.

Monitoring Tools

The **Monitoring Tools** tab displays details of the monitoring tool ports of NDB devices. Traffic from the monitoring tool port of an NDB device is directed to the monitoring tool.

A table with the following details is displayed:

Table 14: Monitoring Tools

Column Name	Description
Status	Status is defined using two columns. First column indicates the traffic on the monitoring tool. • Green—indicates that the monitoring tool is currently carrying traffic. • Yellow—indicates that the monitoring tool is currently not carrying traffic. Second column indicates the status of the link between the monitoring tool port and monitoring tool. If the link between the monitoring tool port and the monitoring tool is up, then it is green in colour. • Green—indicates that the link is up and running. • Red—indicates that the link is down. • Yellow—indicates that the link is administratively down.
Monitoring Tool	The monitoring tool name. This field is a hyperlink. Click the **Monitoring Tool** name. A new pane is displayed on the right which has more details about the monitoring tool. The following additional actions can be performed from here: • Editing a Monitoring Tool, on page 39
Port	Monitoring tool port (with the device). Click the **Port** name to get more details of the port. The following additional actions can be performed from here: • Editing a Monitoring Tool, on page 39
Type	The type of monitoring tool. The option are: • Local Monitoring Tool—port that resides on the NDB device in the local network (L2 port). • Remote Monitoring Tool—port that resides outside the local network and reachable over L3 network.
In Use	If the monitoring tool port is in use, a *green tick mark* is displayed; else it is left blank.

Column Name	Description
Packet Truncation	If packet truncation is enabled on the monitoring tool port, a *green tick mark* is displayed; else it is left blank.
Block Rx	If incoming traffic from the monitoring tool to the monitoring tool port (on the NDB device) is blocked, then **Yes** is displayed.
Created By	The user who created the monitoring tool.
Last Modified By	The user who last modified the monitoring tool.

The following actions can be performed from the **Monitoring Tools** tab:

- **Add Monitoring Tool**—Use this to add a new monitoring device. See Adding a Monitoring Tool for details about this task.
- **Delete Monitoring Tool(s)**—Select the required device by checking the check box which is available at the beginning of the row. The selected device(s) are deleted. Click **Actions** > **Delete Monitoring Tool(s)**. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Note An *In use* monitoring tool cannot be deleted.

Adding a Monitoring Tool

Use this procedure to add a monitoring tool port. You can create a:

- Local Monitoring Tool—a port that resides on the NDB device in the local network (L2 port).
- Remote Monitoring Tool—a port that resides outside the local network and reachable over L3 network.

You can create a packet truncation port (used to block the ingress traffic) to be associated with the monitoring tool which is the egress port for a packet.

Before you begin

Restrictions:

- You cannot use more than one remote delivery port per switch per connection.
- Remote monitoring tool involving inter switched links is restricted to only one connection per ISL.
- If the monitoring tool is used with a packet truncation interface, then, ensure that the status of the packet truncation port is Administratively Up (green icon) and that the other end of the link is not connected to any NDB device. To change the port Layer 2 status to Up, you need to connect to another non-NDB device create a loopback using a third party loopback fiber optic.

Note You can configure a maximum of four monitoring tools with packet truncation on a switch.

Step 1 Navigate to **Components** > **Monitoring Tools**.

Step 2 From the **Actions** drop-down list, select **Add Monitoring Tool**.

Step 3 In the **Add Monitoring Tool** dialog box, enter the following details:

Table 15: Add Monitoring Tool

Field	Description
General	
Monitoring Tool Name	Enter a name for the monitoring tool name.
Device Name	Click **Select Device**. From the displayed list of devices, select a device using the radio button. The device details are displayed on the right. The monitoring tool port resides on this device. Click **Select Device**.
Port	Click **Select Port**. In the **Select Interface** window that opens, select a port by using the radio button. The displayed interfaces depends on the selected device. Click **Select**. The selected port is marked as the monitoring tool port. The traffic is redirected to the monitoring tool from here.
Port Description	Enter a description for the port.
Local Monitor Tool	Select the radio button to select a local monitor device. By selecting this option, a monitoring device is from the local network. The following options are displayed for local monitor device (discussed in detail in the rows below): • Block Rx • Block ICMPv6 Neighbour Solicitation • Enable Timestamp Tagging • Packet Truncation • Enable Timestamp Strip • Apply Jumbo MTU

Field	Description
Block Rx	Blocks traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. **Note** Rx traffic is blocked using Unidirectional Ethernet for Cisco N9K-95xx switches with N9K-X97160YC-EX line card (NX-OS 9.3(3) or later).
Block ICMPv6 Neighbour Solicitation	Blocks ICMP traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. Supported on Nexus 9300-EX and 9200 switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic.
Enable Timestamp Tagging	Check the check box to enable timestamp tagging. A timestamp tag is appended to all the outgoing packets of the monitoring tool port. You can configure this feature on a single device or multiple devices. To configure timestamp tagging, ensure that PTP is enabled on the device. You need to enable timestamp tagging on the monitoring device(s) and edge ports. If timestamp tagging is not configured on either side of the connection, Edge-SPAN/Edge-TAP and the monitor tools, then packets are not tagged with timestamp.
Packet Truncation	Check the check box to enable packet truncation and enter the MTU size. Packet truncation discards bytes from an incoming packet based on the MTU size. This is done in order to send only the the required traffic to the monitoring tool port. This is achieved by redirecting the traffic from the input port to the packet truncation port. The truncated packets from the packet tuncation port reach the monitoring tool. To set a packet truncation port, click **Select Packet Truncation Port**. See Adding a Packet Truncation Port, on page 42 for the detailed procedure.
Enable Timestamp Strip	Check the check box to enable timestamp strip. This removes the timestamp tag from the source packets.
Apply Jumbo MTU	Check the check box to enable jumbo MTU. Jumbo MTU sets a bigger packet size for the device. Enable **Jumbo MTU** in **Global Configuration** to apply the set Jumbo MTU size for a port of the device.

Field	Description
Remote Monitor Tool	Select the radio button to select a remote monitor device. By selecting this option, a monitoring device from a remote network is enabled. The following options are displayed for remote monitor device (discussed in detail in the rows below): • Block Rx • Interface IP • Destination IP • ERSPAN ID
Interface IP	IP address to be assigned to the monitoring tool port.
Destination IP	IP Address where ERSPAN terminates and should be reachable from the selected port.
ERSPAN ID	Enter ERSPAN id; range is 1 to 1023. You can use a device outside the network as a monitoring device using the Encapsulated Remote Switch Port Analyzer (ERSPAN) Source Session feature for Cisco Nexus 9300 FX and EX series switches.

Step 4 Click **Add Monitoring Tool**.

Editing a Monitoring Tool

Use this procedure to edit the parameters of a monitoring tool.

Before you begin

Add one or more monitoring tools.

Step 1 Navigate to **Components** > **Monitoring Tools**.

Step 2 In the displayed table, click a **Monitoring Tool** name.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Monitoring Tool**.

Step 4 In the **Edit Monitoring Tool** dialog box, the current information of the monitoring tool is displayed. Modify these fields, as required:

Table 16: Edit Monitoring Tool

Field	Description
General	
Monitoring Tool Name	Monitoring tool name is displayed; this cannot be edited.
Device Name	The device on which the monitoring tool port resides.
Port	The monitoring tool port.
Port Description	Enter a description for the port.
Local Monitor Tool	Select the radio button to select a local monitor device. By selecting this option, a monitoring device is from the local network. The following options are displayed for local monitor device (discussed in detail in the rows below): • Block Rx • Block ICMPv6 Neighbour Solicitation • Enable Timestamp Tagging • Packet Truncation • Enable Timestamp Strip • Apply Jumbo MTU
Block Rx	Blocks traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. **Note** Rx traffic is blocked using Unidirectional Ethernet for Cisco N9K-95xx switches with N9K-X97160YC-EX line card (NX-OS 9.3(3) or later).
Block ICMPv6 Neighbour Solicitation	Blocks ICMP traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. Supported on Nexus 9300-EX and 9200 switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic.

Field	Description
Enable Timestamp Tagging	Check the check box to enable timestamp tagging. A timestamp tag is appended to all the outgoing packets of the monitoring tool port. You can configure this feature on a single device or multiple devices. To configure timestamp tagging, ensure that PTP is enabled on the device. You need to enable timestamp tagging on the monitoring device(s) and edge ports. If timestamp tagging is not configured on either side of the connection, Edge-SPAN/Edge-TAP and the monitor tools, then packets are not tagged with timestamp.
Packet Truncation	Check the check box to enable packet truncation and enter the MTU size. If a packet truncation port was not configured during the addition of the monitoring tool, the **Select Packet Truncation Port** is disabled.
Enable Timestamp Strip	Check the check box to enable timestamp strip. This removes the timestamp tag from the source packets.
Apply Jumbo MTU	Check the check box to enable jumbo MTU. Jumbo MTU sets a bigger packet size for the device. Enable **Jumbo MTU** in **Global Configuration** to apply the set Jumbo MTU size for a port of the device.
Remote Monitor Tool	Select the radio button to select a remote monitor device. By selecting this option, a monitoring device from a remote network is enabled. The following options are displayed for remote monitor device (discussed in detail in the rows below): • Block Rx • Interface IP • Destination IP • ERSPAN ID
Interface IP	IP address to be assigned to the monitoring tool port.
Destination IP	IP Address where ERSPAN terminates and should be reachable from the selected port.
ERSPAN ID	Enter ERSPAN id; range is 1 to 1023. You can use a device outside the network as a monitoring device using the Encapsulated Remote Switch Port Analyzer (ERSPAN) Source Session feature for Cisco Nexus 9300 FX and EX series switches.

Step 5 Click **Save**.

Adding a Packet Truncation Port

Use this procedure to create a packet truncation port. A packet truncation port serves as an input port for the monitoring tool port. Hence, the created packet truncation port is listed as an input port, and unused packet truncation ports can be deleted from the Input Ports tab.

Before you begin

Packet truncation involves discarding bytes from a packet starting at a specified byte position. All the data after the specified byte position is discarded. Packet truncation is required when the main information of interest is in the header of a packet or in the initial part of the packet.

Table 17: Support for Packet Truncation

EX Chassis	FX Chassis	Nexus 9364C, Nexus 9332C	Nexus 9336C-FX2	EOR switches with -EX or -FX LCs
MTU size range is 320 to 1518 bytes	MTU size range is 64 to 1518 bytes	MTU size range is 64 to 1518 bytes	MTU size range is 64 to 1518 bytes	Depends on LC

Step 1 Navigate to **Components** > **Monitoring Tools**.

Step 2 From the **Actions** drop-down list, select **Add Monitoring Tool**.

Step 3 Select a device and port and check the **Packet Truncation** check-box to enable packet truncation.

Step 4 Click **Select Packet Truncation Port**.

Step 5 In the **Select Packet Truncation Port** window that is displayed, click **Add Packet Truncation Port**.

Step 6 In the **Add Packet Truncation** dialog box, enter the following details:

Table 18: Add Packet Truncation

Field	Description
General	
Device	The device name is displayed.
Port	Click **Select Port**. In the **Select Port** window, select a port by selecting a radio button. Click **Submit**.
Port Type	Packet Truncation port is selected by default.
Port Description	Port description for the truncation port.
Drop ICMPv6 Neighbour Solicitation	Blocks ingress ICMP traffic for the packet truncation port. This option is selected by default. You can turn this option off by unchecking the check box.

Step 7 Click **Add** .

Port Groups

The **Port Groups** tab has the following subtabs:

- **Input Port Group**—input ports of a device (or across devices) are grouped together to form an input port group. See Input Port Group for more details.
- **Monitoring Tool Group**—monitoring tool ports of a device (or across devices) are grouped together to form a monitoring tool group. See Monitoring Tool Group for more details.

Input Port Group

Input ports of a device (or different devices) are grouped together to form a port group. Port groups can be a combination of the edge-span and the edge-tap ports across different devices. While creating a connection, instead of choosing input ports separately, you can select more than one input port simultaneously by grouping them.

A table with the following details is displayed:

Table 19: Input Port Group

Column Name	Description
Input Port Group Name	Input port group name. This field is a hyperlink. Click the **Input Port Group Name**. A new pane is displayed on the right which provides more information about the input port group. Additional tasks that can be performed from here are: • Editing an Input Port Group
Description	Description of the input port group.
Associated Connections	The connection(s) associated with the group.
Member(s)	The number of member input ports of the group.
Created By	User who created the group.
Last Modified By	User who last modified the group.

The following actions can be performed from the **Input Port Group** tab:

- **Add Input Port Group**—Use this to add a new input port group. SeeAdding an Input Port Group for details about this task.
- **Delete Input Port Group(s)**—Select the input port group(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Input Port Group**. The

selected input port group(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select an input port group.

Adding an Input Port Group

Use this procedure to create an input port group.

While creating a connection, instead of choosing input ports separately, you can select more than one input port simultaneously by grouping them.

Before you begin

Create one or more devices.

Step 1 Navigate to **Components** > **Port Groups** > **Input Port Group**.

Step 2 From the **Actions** drop-down list, select **Add Input Port Group**.

Step 3 In the **Add Input Port Group** dialog box, enter the following details:

Table 20: Add Input Port Group

Field	Description
General	
Group Name	Enter a name for the input port group.
Description	Enter a description for the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports that are configured as inputs ports, are displayed. Click a port to select it. You can click **Add All** to select all the (input) ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 4 Click **Add Input Port Group**.

Editing an Input Port Group

Use this procedure to edit the parameters of an input port group.

Before you begin

Create one or more input port groups.

Step 1 Navigate to **Components** > **Port Groups** > **Input Port Group**.

Step 2 In the displayed table, click an **Input Port Group** name.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Input Port Group**.

Step 4 In the **Edit Input Port Group** dialog box, the current information of the group is displayed. Modify these fields, as required:

Table 21: Edit Input Port Group

Field	Description
General	
Group Name	Input port group name.
Description	Description of the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports configured as input ports, are displayed. Click a port to select it. You can click **Add All** to select all the ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 5 Click **Edit Input Port Group**.

Monitoring Tool Group

Monitoring tool ports grouped together across devices form a monitoring tool group.

A table with the following details is displayed:

Table 22: Monitoring Tool Group

Column Name	Description
Monitoring Tool Group Name	Monitoring tool group name. This field is a hyperlink. Click the **Monitoring Tool Group Name**. A new pane is displayed on the right which provides more information about the monitoring tool group. Additional tasks that can be performed from here are: • Editing a Monitoring Tool Group

Column Name	Description
Description	Description of the monitoring tool group.
Associated Connections	Connections using the monitoring tool group.
Member(s)	The number of member monitoring tool ports of the group.
Created By	User who created the group.
Last Modified By	User who last modified the group.

The following actions can be performed from the **Monitoring Tool Group** tab:

- **Add Monitoring Tool Group**—Use this to add a new monitoring tool group. See Adding a Monitoring Tool Group for details about this task.
- **Delete Monitoring Tool Group(s)**—Select the tool group(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Monitoring Tool Group(s)**. The selected tool group(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a tool group.

Adding a Monitoring Tool Group

Use this procedure to create a monitoring tool group.

Before you begin

Create one or more monitoring tools.

Step 1 Navigate to **Components** > **Port Groups** > **Monitoring Tool Group**.

Step 2 From the **Actions** drop-down list, select **Add Monitoring Tool Group**.

Step 3 In the **Add Monitoring Tool Group** dialog box, enter the following details:

Table 23: Add Monitoring Tool Group

Field	Description
General	
Group Name	Enter a name for the monitoring tool group.
Description	Enter a description for the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports that are configured as monitoring tool ports, are displayed. Click a port to select it. You can click **Add All** to select all the (monitoring) ports of a device.

Field	Description
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 4 Click **Add Monitoring Tool Group**.

Editing a Monitoring Tool Group

Use this procedure to edit the parameters of a monitoring tool group.

Before you begin

Create one or more monitoring tool groups.

Step 1 Navigate to **Components** > **Port Groups** > **Monitoring Tool Group**.

Step 2 In the displayed table, click a **Monitoring Tool Group** name.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Monitoring Tool Group**.

Step 4 In the **Edit Monitoring Tool Group** dialog box, the current information of the group is displayed. Modify these fields, as required:

Table 24: Edit Monitoring Tool Group

Field	Description
General	
Group Name	Name of the monitoring tool group.
Description	Description for the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports that are configured as monitoring tool ports, are displayed. Click a port to select it. You can click **Add All** to select all the (monitoring) ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 5 Click **Edit Monitoring Tool Group**.

Span Destination

The **Span Destination** tab displays details of the span ports connected to the input ports of NDB devices. Span destination is the traffic source (from ACI or NX-OS device) for the input ports. An L2 span destination (local) is created on an edge span port and an L3 span destination (remote) is created on a remote edge span port.

A table with the following details is displayed:

Table 25: Span Destination

Column Name	Description
Name	Name of the span destination port.
Destinations	Indicates if the span destination is on an ACI device or an NX-OS device.
Input Port	Input port of the NDB device which is connected to the span destination.
Input Port Type	Input port type. The options are: • Edge-SPAN port • Remote Source Edge-SPAN port
Span Device	Span device (traffic source). The options are: • AC—ACI device/ APIC • PS—NX-OS device (production switch)
Created By	The user who created the span destination.
Last Modified By	The user who last modified the span destination.

The following actions can be performed from the **Span Destinations** tab:

- **Delete Span Destination(s)**—Select the span destination to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Span Destination(s)**. The selected span destination is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a span destination.

Note For adding a Span Destination, see Adding an Input Port procedure. A span destination (on an ACI/ NX-OS device) is connected to the input port of an NDB device. You can add a SPAN destination only after either an ACI/ NX-OS device has been successfully added to the network.

For APIC SPAN destination, when you configure an input port as an Edge-SPAN port and the port is connected to the ACI side, you can select the pod, the node, and the port from the ACI side and set the port as SPAN

destination. For NX-OS (production switch) SPAN destination, when you configure an input port as an Edge-SPAN port and the port is connected to an NX-OS device, select a node and port on the NX-OS device, and set the port as SPAN destination.

User Defined Field

The **User Defined Field (UDF)** tab displays details of UDFs on NDB devices.

A UDF enables you to filter packets based on an offset value. An offset value in a packet can be matched within 128 bytes.

By default, NDB controller generates two UDFs named *udfInnerVlan* and *udfInnerVlanv6*, used to match the inner VLAN in the ISL ports.

Table 26: UDF Support Matrix

UDF Ethertype	Platform
IPv4	Cisco Nexus 9200 and 9300 series switches
IPv6	Cisco Nexus 93xx EX/FX , 95xx EX/FX , 92xx series switches

Table 27: Qualifying Regions for UDF

Platform	UDF Qualifying TCAM Region
Cisco Nexus 9200, 9300-EX/9300-FX and 9500-EX/9500-FX series switches	ing-ifacl
Other platforms	ifacl

A table with the following details is displayed:

Table 28: User Defined Field

Column Name	Description
UDF	The UDF name. This field is a hyperlink. Click the UDF name and a new pane is displayed on the right with more details of the UDF. Additional tasks that can be performed from here are: • Editing or Cloning a User Defined Field .
Type	Displays **IPv4** or **IPv6**.
Keyword	Displays **Packet-Start** or **Header**.
In Use	A green tick-mark indicates that the UDF is currently in use.

Column Name	Description
Offset	The set offset value.
Length	Length (number of bytes) in a packet that are matched.
Devices	Number of devices a UDF is applied on.
Created By	User who created the UDF.
Last Modified By	User who last modified the UDF.

The following actions can be performed from the **User Defined Field** tab:

- **Add UDF**—Use this to add a new UDF. See Adding a User Defined Field for details about this task.
- **Delete UDF(s)**—Select a UDF by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete UDF(s)**.

  If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a UDF.

Note Any change in a UDF definition requires device reboot.

Adding a User Defined Field

Use this procedure to add a user defined field.

Some protocols are not supported by default in some NX-OS devices. To support filtering of packets on these devices, use UDFs.

Note UDF can match a maximum of two offset bytes. To filter three consecutive bytes in a packet, we need to stack the UDFs. Create two UDFs, one after the other using the NDB GUI. The second UDF is called the stacking UDF.

Step 1 Navigate to **Components** > **User Defined Field**.

Step 2 From the **Actions** drop down list, select **Add UDF**.

Step 3 In the **Add UDF** dialog box, enter the following details:

Table 29: Add UDF

Field	Description
UDF Name	Name of the UDF.

Field	Description
Type	Select from the drop down list. The options are: • IPv4 • IPv6
Keyword	Select from the drop down list. The options are: • Header • Packet-Start If the **Header** option is selected, the Inner (Offset base from inner/outer header) and L3/L4 (Offset base from L3/L4 header) is enabled. If **Packet-Start** is selected, the offset base starts from the packet.
Header	Select from the drop down list. The options are: • Inner • Outer This field is enabled only when the selected keyword is **Header**. Enables you to select the base offset value from the inner or outer Header.
Layer	Select from the drop down list. The options are: • Layer 3 • Layer 4 This field is enabled only when the selected keyword is **Header** . Enables you to specify if the offset start value is from Layer 3 or Layer 4.
Offset	Set the byte **Offset** value; range is from 0 to 127. Filtering of packets is done based on the set offset value in UDF, packets are matched from the set offset value.
Length	Length (number of bytes) of a packet that are matched; range is from 1 to 2. The length depends on the offset value, if it is set to 1; then one byte starting with the set offset byte is matched.
Devices	Device on which the UDF is being created. Click **Select Devices**. In the **Select Device(s)** window, select a device and click **Select Device(s)**.

Step 4 Click **Add UDF**.

The created UDF is used as a *custom filter* while creating filters for a connection. See Adding a Filter for details.

Note The icon for UDF is yellow in color immediately after it is created. After you reboot the device, if the UDF is successfully installed, the UDF icon color changes to green, else it changes to red.

Editing or Cloning a User Defined Field

Use this procedure to edit or clone a user defined field.

Editing a UDF means changing the parameters of an existing UDF.

Cloning a UDF means a new UDF is created with the same parameters as an existing UDF. You can change the parameters as required.

Before you begin

Create one or more user defined fields.

Step 1 Navigate to **Components** > **User Defined Field**.

Step 2 In the displayed table, click a **UDF**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Clone UDF** or **Edit UDF** .

Step 4 In the **Clone UDF** or **Edit UDF** dialog box, the current UDF information is displayed. Modify these fields, as required:

Table 30: Edit UDF

Field	Description
UDF Name	Name of the UDF. This field cannot be changed.
Type	The type selected during UDF creation. This field cannot be changed.
Keyword	Select from the drop down list. The options are: • Header • Packet-Start
Header	The Header selected during UDF creation. This field cannot be changed.
Layer	The Layer selected during UDF creation. This field cannot be changed.

Field	Description
Offset	Set the byte **Offset** value; range is from 0 to 127. Filtering of packets is done based on the set offset value in UDF, packets are matched from the set offset value.
Length	Length (number of bytes) of a packet that are matched; range is from 1 to 2. The length depends on the offset value, if it is set to 1; then one byte starting with the set offset byte is matched.
Devices	Device on which the UDF is currently applied on. You can delete the UDF from the current device or apply the UDF on more devices. Click **Select Devices**. In the **Select Device(s)** window, select a device and click **Select Device(s)**. **Note** You can not delete an *In-use* UDF from a device.

Step 5 Click **Edit UDF** or **Clone UDF** .