Configuring the Nexus Data Broker

This chapter contains the following sections:

- Viewing Topology, on page 2
- Configuring Port Definition, on page 2
- Port Channels, on page 6
- Configuring Port Groups, on page 6
- Adding a Monitoring Device, on page 8
- Adding a Remote Monitoring Device, on page 9
- Adding a Remote Source Edge SPAN, on page 10
- Editing In Use Monitoring Device, on page 12
- Adding a Service Node, on page 13
- User Defined Field, on page 14
- Adding Filters, on page 16
- Adding Connections, on page 24
- Connection with AutoPriority, on page 28
- Adding Redirections, on page 30
- Viewing Statistics, on page 34
- Viewing Connection Port Statistics, on page 36
- Deleting Flow and Port Statistics, on page 36
- Device Return Material Authorization, on page 36
- Purging Device Configuration, on page 37
- Exporting and Importing NDB Configuration, on page 37
- Managing Sampled Flow Configuration , on page 38
- Configuring MPLS Filtering, on page 39
- Configuring Symmetric/Non-Symmetric Load Balancing and MPLS Tag Stripping , on page 41
- Configuring PTP Using NDB, on page 42
- NetFlow, on page 43
- Configuring Packet Truncation, on page 47
- Show Tech for NX-API Devices , on page 49
- Syslog, on page 52

Viewing Topology

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

Note Starting with Cisco NDB Release 3.7, additional information such as hardware detail and software detail is displayed for each device along with the port count in the topology diagram.

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

Complete the following steps to configure a port.

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**
- **Packet Truncation Port**
- **Remote Source Edge Span 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.

Packet Truncation Port—Creates packet truncation on egress ports.

Remote Source Edge Span Port—Configures remote source monitoring.

Note Starting with Cisco NDB Release 3.6, you can configure Maximum Transmission Unit (MTU) for all the Cisco Nexus 9xxx devices in NX-API mode using NDB GUI. MTU can be configured at the system level (node level or global level) and the Interface Level (supported only on SPAN and TAP ports). The default value for MTU is 1500 and you can configure MTU between 1500 and 9216.

Jumbo MTU is the maximum MTU that can be configured for a node. When you configure Jumbo MTU at the system level, the same MTU value is applied to all the node ISLs.

Note Starting with Cisco NDB Release 3.4, a description can have a leading numerical for Edge-SPAN, Edge-TAP, Monitoring devices, Production ports, Filter names, Connections, and Redirections (NX-API, OpenFlow and NX-AUX mode).

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 bpdufilter 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 bpdufilter enable
```

Note Production port has be 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 bpdufilter 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 Required: 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 for both Edge-SPAN and Edge-TAP where you can block the traffic that is being transmitted out of Edge-SPAN AND Edge-TAP interface.

Step 9 A check box is added for **Drop ICMPv6 Neighbour Solicitation** and by default all the ICMP traffic is blocked for all the 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.

Step 10 A check box is added for **Enable Timestamp Tagging** to append timestamp tag on the packets using the Timestamp Tagging feature. You can configure this feature on a single device or multiple devices.

For Nexus 9300-EX and 9200 series switches, this feature is applicable for Edge-SPAN and Edge-TAP ports and on the Monitoring devices. 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. For Nexus 3500 Series switches, the Timestamp Tagging feature is applicable only for the Monitoring devices.

Step 11 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.

Editing In Use Ports

Starting with NDB Release 3.4, you can edit the select fields under Port configuration(Edge-Span, Edge-Tap or Production) while in use. Ports can be edited in all the modes of connection. The following table lists the fields that you can edit for port in use.:

Section	Field	Editable
Port Configuration	Port Description	Yes
	Block Tx	Yes
	Port Type	No
	VLAN Packet Truncation	No
	Drop ICMPv6 Neighbour Solicitation	Yes
	Enable Timestamp Taggin	Yes

Enabling or Disabling Ports

Starting with Cisco NDB Release 3.4, you can now enable or disable an interface using the NDB GUI. This feature is currently available for NX-API and NX-AUX based switches. A switch based on OpenFlow mode does not support this feature.

Step 1 Select the switch for which you want to configure the port details on the **Port Configuration** screen.

Step 2 Click **Enable/Disable** to enable or disable the selected port.

Note You can enable or disable only one interface at a time.

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.

Port Channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to 8 individual active links into a port channel to provide increased bandwidth and redundancy. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

You create a port channel by bundling compatible interfaces. You can configure and run either static port channels or ports channels running the Link Aggregation Control Protocol (LACP).

Any configuration changes that you apply to the port channel are applied to each member interface of that port channel. For example, if you configure Spanning Tree Protocol (STP) parameters on the port channel, the Cisco NX-OS applies those parameters to each interface in the port channel.

You can use static port channels, with no associated protocol, for a simplified configuration. For more efficient use of the port channel, you can use the Link Aggregation Control Protocol (LACP), which is defined in IEEE 802.3ad. When you use LACP, the link passes protocol packets.

Configuring Port Groups

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

Complete the following steps to configure port groups:

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**.

Starting with NDB 3.4 release, you can now configure selected fields under Port Group. This feature is supported on the switches running in NX-API, OpenFlow, or NX-AUX mode.

Starting with Cisco NDB Release 3.7, **Created By** and **Modified By** information is displayed for Port Groups in the NDB UI.

The following table lists the fields that you can configure for a Port Group:

Section	Field	Editable
Port Group	Port Description	Yes
	Port	Yes
	Port Name	Yes (If the port is not part of an active connection)
	Port Group	Yes (If the port group is not part of an active connection)

Editing In Use Port Groups

You can edit an in-use port group using NDB GUI. To edit an in-use port group, complete the following steps:

Note Starting with Cisco NDB release 3.8, you can now rename an in-use port group.

Note Starting with NDB 3.4 release, you can edit the port groups that are currently in use in a connection. This feature is supported on the switches running in NX-API, OpenFlow, or NX-AUX mode.

Step 1 Select the switch for which you want to configure the port details on the **Port Group** pane.

Step 2 Click **Edit** on the listed table row.

Editable Attributes for In Use Port Groups

The following table lists the fields that you can edit for a Port Group that is currently in use:

Section	Field	Editable
Port Group	Port Description	Yes
	Port	Yes
	Port Name	Yes.
	Port Group	Yes (If the port group is not part of an active connection)

Adding a Monitoring Device

To add a new monitoring device, complete these steps:

Step 1 Navigate to the **Monitoring Device** tab under **Configuration**.

Step 2 Click **Add 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: period ("."), underscore ("_"), and hyphen ("-").
Select Switch Node	Select the switch node.
Select Port	Select the port.
Port Description	Description for the port.

Name	Description
Icons	Select a Monitoring Device Icon.
Local Monitor Device	Indicates that the monitoring device is available in the local network.
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. **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).
Enable Timestamp Tagging	Time stamp tagging is supported on Cisco Nexus 3500, 9200 and 93XXX-EX Series switches. Cisco Nexus 3500 Series switches require NX-OS Release 6.0(2)A8(1) or later version.
Enable Timestamp Strip	Select this option to remove timestamp tag from the source packets.
MTU	You can configure MTU at the system level (node level or global level) and the Interface Level. The default value for MTU is 1500 and you can configure MTU between 1500 and 9216. Jumbo MTU is the maximum MTU that can be configured for a node. When you configure Jumbo MTU at the system level, the same MTU value is applied to all the node ISLs.

Step 4 Click **Submit** to create the monitoring device.

Adding a Remote Monitoring Device

Starting with Cisco NDB Release 3.7, you can now 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. This feature enables you to direct the traffic for monitoring outside the local network

Note You can associate a remote delivery port to only one destination port group.

To add a new remote monitoring device, complete these steps:

Step 1 Navigate to the **Monitoring Device** tab under **Configuration**.

Step 2 Click **Add 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: period ("."), underscore ("_"), and hyphen ("-").
Select Switch Node	Select the switch node.
Select Port	Select the port.
Port Description	Description for the port.
Block Rx	Not applicable
Remote Monitor Device	Select this option to indicate that the monitoring device is available in the local network.
Enable Timestamp Tagging	Enable Timestamp Tagging for remote monitoring.
Enable Timestamp Strip	Enable Timestamp Strip for remote monitoring.
MTU	Enable MTU for remote monitoring.
Icons	Select a Monitoring Device Icon.
Interface IP	IP address to be assigned to the selected interface.
Destination IP	IP Address where ER-SPAN terminates and should be reachable from the selected port.

Step 4 Click **Submit** to create the monitoring device.

Note You cannot use more than one remote delivery port per switch per connection.

Note You cannot share the same source interface across with multiple connections.

Note Remote monitor tool involving inter switched links is restricted to only one connection per ISL.

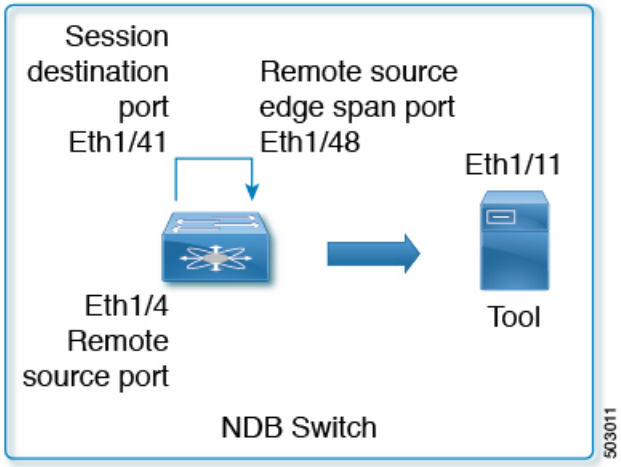
Adding a Remote Source Edge SPAN

Starting with Cisco Nexus Data Broker Release 3.8, you can now configure remote source monitoring on devices (Nexus 9300-EX, 9300-FX, 9300-FX2, 9500-EX, and 9500-FX) running NX-OS version 9.3(1) or later.

From Release 3.9, traffic from APIC can be captured on NDB via remote source (ERSPAN).

After you add a remote source edge-span, you can edit all fields except the remote source and the IP address fields. To edit these fields, you must remove this configuration and redo the configuration.

For better understanding, consider the topology as shown below. The image represents the configuration of a remote source edge span, on a device where the interface ethernet1/4 of the device is a L3 port which receives traffic from the ERSPAN source. Interface ethernet1/41 of the device is configured as session destination, interface ethernet1/48 of the device is configured as remote source edge span and interface ethernet1/11 of the device is configured as a monitoring tool.



Step 1 Configure remote source termination. Navigate to the **CONFIGURATION** > **Port Definitions** .

Step 2 In the **Port Definition** page, click **Configure** for an interface to configure remote source monitoring. The **Configure Ports** dialog box opens.

Step 3 From the **Select a port type** drop-down list, select **Remote Source Egde-SPAN**.

Step 4 In the **Port Description** field, enter the port configuration.

Step 5 (Optional) In the **VLAN ID** field, enter the VLAN ID for the port that you want to set for this configuration.

Step 6 (Optional) In the **Enable Packet Truncation** field, enter the packet length.

Step 7 In the **ERSPAN ID** field, enter ERSPAN Id for the Remote Source Termination session. The range of ERSPAN ID is from 1 to 1023.

This value should be the same as that of ERSPAN source session.

Step 8 (Optional) Check the **Use Loopback interface** dialog box to create a loopback. From the **Select Loopback** drop-down list, select a loopback. You can also create a new loopback, if not available. To create a new loopback, click **Configure Loopback**. In the **Configure Loopback Interface** dialog box that appears, do the following:

a) Enter loopback ID in the **Loopback ID** field.
b) Enter IP address in the **IP Address** field.
c) Click **Submit** to create a new loopback and close the **Configure Loopback Interface** dialog box. The Loopback IP address will be used for the session creation.

Step 9 From the **Session Destination** drop-down list select session destination port for the monitoring session.

The interface configured as session destination (Eth1/41) redirects decapsulated traffic to remote source edge span. For this redirection to work, the session destination interface should have physical loopback cable with remote source edge span (Eth1/48).

Step 10 From the **Remote Source** drop-down list, select the interface to be configured as a remote source port, where ERSPAN encapsulated packets are received.

Remote source configured on Ethernet1/4 interface is an L3 port which receives traffic either through IP address (when loopback interface is not selected) or loopback interface (when loopback interface is configured). The IP address must be similar to the destination IP address configured in the ERSPAN source session.

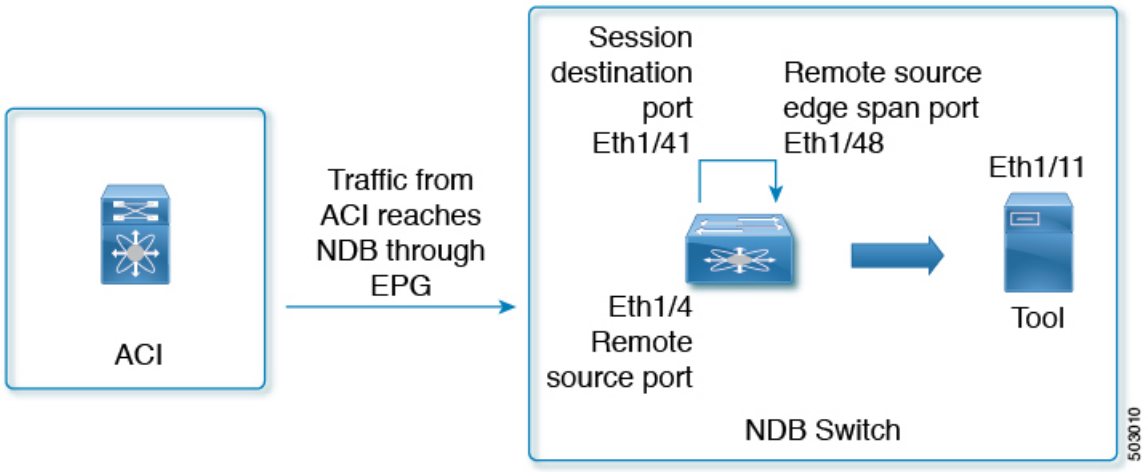
Step 11 In the **IP Address** field, enter IP address of the packet source. This IP address is used to create the monitor session if the **use loopback** option is not enabled.

Step 12 If you have APIC configured, the Destination pane is displayed and the Node Type is automatically populated with APIC (which cannot be changed). For details about SPAN Destination creation, see Adding SPAN Destination.

Step 13 Click **Submit** to complete the process.

The remote source edge span configured on interface ethernet 1/48, receives the decapsulated traffic and redirects it to the monitoring tool.

Note For adding Remote source edge span for ACI, traffic from the ACI reaches the NDB through EPG (as shown below). The behavior of the remote source, session destination and the created remote source edge span is similar to what is defined in the this task. The value of the ERSPAN ID is the Flow ID for the span destination.



Editing In Use Monitoring Device

Starting with Cisco NDB, Release 3.4, you can edit a monitoring device configuration using the NDB GUI. Support to edit description of a Monitoring device is available for NX-API, OpenFlow, and NX-AUX based switches. For the OpenFlow devices, the updated descriptions are synchronized to NDB User Interface (UI) only. For NX-API and NX-AUX devices, the updates are synchronized to NDB UI and the switch interface.

The following table lists the fields that you can configure for Monitoring Devices:

Section	Field	Editable
Monitor Devices	Monitor Devices Name	Yes (If the monitoring device is not in use)
	Port Description	Yes
	Block Rx	Yes
	Icons	Yes
	Enable Timestamp Tagging	Yes
	Enable Timestamp Strip	Yes
	MTU	Yes

Adding a Service Node

Starting with Cisco NDB Release 3.7, **Created By** and **Modified By** information is displayed for Service Nodes in the NDB UI.

Complete the following steps to add 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**.

Editable Fields for an Active Service Node

Starting with Cisco NDB, Release 3.4, you can now edit and configure Service Node fields using the NDB GUI. For the OpenFlow devices, the updated descriptions are synchronized to NDB User Interface (UI) only. For NX-API and NX-AUX devices, the updates are synchronized to NDB UI and the switch interface.

The following table lists the fields that you can configure for an active Service Node:

Section	Field	Editable
Service Node	Description	Yes
	Icon	Yes
	Service Node Health Check	Yes
	Service Node Name	Yes (If the service node is not in use)
	Service Node Ingress Port	No
	Service Node Egress Port	No
	Ingress port Description	Yes
	Egress port Description	Yes

User Defined Field

You can define a User Defined Field (UDF) and use it while creating a filter for traffic management.

Starting with Cisco NDB Release 3.7, **Created By** and **Modified By** information is displayed for User Defined Fields in the NDB UI.

Note Starting with Cisco NDB Release 3.6, you can add multiple UDFs while defining a filter. You can add upto four UDFs for each filter.

Table 1: UDF Support Matrix

UDF Ethertype	NDB Version	NXOS Version	Platform
IPv4	3.3	7.0(3)I5(2)	9200 & 9300
IPv6	3.6	7.0(3)I6(1)	93xx EX/FX , 95xx EX/FX , 92xx

Note Please refer the NXOS documentation for number of UDF support per platform.

To use UDF to manage traffic, you need to:

- Define a UDF, see Defining a UDF.
- Create a filter using the UDF, see Adding Filters.
- Apply the filter (configured with UDF) to a connection to manage traffic, see Adding Connections.

Table 2: Qualifying Region for UDF for Different Platforms

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

Defining a UDF

Complete the following steps to define a UDF:

Step 1 Log into NDB application.

Step 2 Navigate to **Configuration** tab, click **UDF Definition** to define a user defined filter. The **UDF Definition** window is displayed.

Step 3 In the **UDF Definition** window, complete the following fields:

Name	Description
Name field	The name of the user defined field.
Keyword	If **Header** option is selected, the Inner (Offset base from inner/outer header) and L3/L4 (Offset base from L3/L4 header) is enabled.
Offset field	Number of characters to offset while using matching criteria.
Devices	Cisco Nexus 9000 Series switch name.
Type	Specifiy UDFv4 or UDFv6 support.

Step 4 Click **Add UDF**. The newly added UDF appears in the **UDF Definition** window.

Note Any change in a UDF definition requires device reboot.

Note By default, NDB generates a UDF named *udfInnerVlan* and *udfInnerVlanv6*, used to match the inner VLAN in the ISL ports.

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 color.

Adding Filters

Beginning with Cisco Nexus Data Broker, Release 3.3, the Default-Match-All filter includes the following protocols packet filtering:

- IPv4
- IPv6
- ARP
- MPLS Unicast
- MPLS Multicast
- MAC

Before you begin

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

Note Beginning with NDB 3.4 release, you can now edit Filter Name using the NDB GUI. This feature is supported on the switches running in NX-API, OpenFlow, or NX-AUX mode.

Step 1 On the **Filters** tab, click **Add 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.
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	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • IPv6 • ARP • LLDP • Predefined EtherTypes • All EtherTypes • Enter Ethernet Type—If you choose Enter Ethernet Type as the type, enter the Ethernet type in hexadecimal format. If you choose Predefined EtherTypes, all predefined Ethernet types contained in the config.in file are associated with the rule, and you should not configure any other parameters.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Add Filter** window, update the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • Discontiguous source IP address, for example, 10.10.10.10, 10.10.10.11, 10.10.10.12 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • An IPv4 subnet, for example, 10.1.1.0/24 • The host IP address in IPv6 format, for example, 2001::0 • Combination of range and simple IP addresses, for example, 4.4.4.1,4.4.4.2-4.4.4.4,4.4.4.5. **Note** • 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. **Note** When using IPv6 address in the filter, the **Ethernet Type** should be set to IPv6.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.11 • An IPv4 address range, for example, 10.10.10.11-10.10.10.18 • An IPv4 subnet, for example, 10.1.1.0/24 • The host IP address in IPv6 format, for example, 2001::4 • The subnet, for example, 10.0.0.0/25 **Note** • 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	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. • ICMP • TCP • UDP • Enter Protocol

Name	Description
UDF drop-down list	User Defined Field. • UDF: UDF name. • UDF value: Value to be matched in decimal notation (0-65535). Example: if you want to match 0x0806, enter 2054 which is 0x0806 in decimal notation. • UDF Mask: Mask value in packet to be matched. Mask is applied to the value for matching purposes. Example: to exactly match 2054 (0x0806) enter 65535 (0xffff), to match 2048-2063 (0x0800-0x080f) use 65520 (0xfff0). **Note** If Add default udf for inner vlan option is selected, you can add only one UDF (UDF that matches outervlan offset). The udfInnerVlan is applied to the ISL links along with QinQ vlan specified on the SPAN port. **Note** UDF option is enabled for IPv4 and IPv6 ethertypes.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.
Advanced Filter field	Advanced filter, combination of Ethernet type and attributes to manage traffic.

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

Name	Description
Source Port drop-down list	Choose the source port of the Layer 4 traffic. This can be one of the following: • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Source Port **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. **Note** • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 2 VLAN identifiers

Name	Description
Destination Port drop-down list	Choose the destination port of the Layer 4 traffic. This can be one of the following: • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Destination Port **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. **Note** • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers

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

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

Step 7 Click **Add Filter**.

Advanced Filter support

Starting with Cisco Nexus Data Broker, Release 3.3, advanced filtering option is available to manage the traffic. 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 3: 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

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

Important The value of Time to Live (TTL) attribute ranges 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.

While configuring advanced filtering support, you cannot:

- Configure DSCP and Precedence together in advance filtering.
- Configure fragments and ACK or SYN or FIN or PSH or RST together in advance filtering.
- Configure fragments and port numbers with UDP and IPv4 or IPv6 Combination
- Configure Precedence and HTTP Methods with IPv4 and TCP Combination.

Adding Connections

Starting with Cisco Nexus Data Broker Release 3.7, you can lock a connection while creating it using the **Lock Connection** option on the **Add Connection** page. Locking a connection prevents unauthorized changes to a connection.

Before you begin

- Add a filter to be assigned to the connection.
- Configure a monitoring device (optional).

- Configure an edge port or multiple edge ports (optional).

Beginning with Release 3.9.2, Q-in-Q VLAN is mandatory on all source ports in an ISL connection. After an upgrade to Release 3.9.2, the connections created in the previous releases are available, but if you need to modify/clone any of the connections created earlier, adding Q-in-Q VLAN is mandatory, else you will not be able to save your changes to the updated connection.

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 <2-10000>. Priority is applicable to the ACL rules on the span port. Connection with a higher priority takes precedence. Traffic will pass through a connection with a higher priority based on the match criteria (filters). For example, connection with priority 101 is given preference when compared to a connection with priority 100.
Lock Connection	Select this option to lock the connection you are creating to prevent any unauthorized modification.

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.
Select Destination Port Group(s) field	Select **Port Group** option and then selet the destination port group from th drop-down list for the new connection.

Field	Description
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The Strip VLAN at delivery port action is only valid for connections with a single edge port and one or more delivery devices for a single, separate node. 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.

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.

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

Note Similar to the number of Edge-TAP or Edge-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 **Dry Run** to estimate the amount of traffic that will be generated on the new connection.
- Click **Close** to exit the connection without saving it.

If Cisco NDB detects two connections having the same Q-in-Q VLAN (while adding a new connection or modifying an existing one), merging the connections is possible. After clicking **Save Connection** or **Install Connection**, a pop-up window is displayed. Click **Yes** to merge the two connections.

Note You can estimate the amount of traffic generated for a new connection using the Dry Run feature. This feature samples the traffic for 30 seconds for the new connection and estimates the approximate traffic generated for the connection. You can use the Dry Run feature before adding a new connection.

You can manage the Dry Run feature using the mm.dryrun.timer parameter in the `config.ini` file. To enable the Dry Run feature, set the mm.dryrun.timer paramter to a value greater than zero. If the mm.dryrun.timer paramter is set to zero, the Dry Run feature is disabled.

The Dry Run feature shows the topology for the new connection with information about the estimated traffic. The feature samples the traffic for few (mm.dryrun.timer value in config.ini file) seconds for the new connection and estimates the approximate traffic generated for the connection. You can use the Dry Run feature before adding a new connection.

The following fields are displayed on the **Connection Setup** screen:

- Name
- Allow Filters
- Drop Filters
- Source Ports/Port Groups
- Devices
- Priority
- Last Modified By
- Description
- Status
- Action

Note A color coded band highlighting all the above fields indicates the status of the connection. The factors affecting the status of a connection are - operational and administration state of the source ports, operational state and administration state of the monitoring tools and the sessions involved in the connection. A green band indicates that the connection is operational, else the band is indicated in yellow or pink. A yellow band indicates the connection is partially successful; one or more source port(s) and monitoring tools have errors. A pink band indicates that the connection has failed; check the state of all the source ports and monitoring tools.

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**.

Note If a remote monitoring tool is selected, same sources or remote monitoring tool cannot be shared across connections. This condition applies to ISL links also.

Connection with AutoPriority

Starting with Cisco NDB Release 3.4, you can configure filters with overlapping IP address. The traffic from the interfaces with overlapping IP addresses is forwarded to all the monitors configured for the IP address. This feature is supported for the switches running NX-API, OpenFlow, and AUX mode.

You can also configure rules with common IP addresses.You can configure IP address and port overlapping in the same filter.

Beginning with Cisco Nexus Data Broker, Release 3.3, you can now add a new connection with AutoPriority. This functionality provides flexibility to map filters to mulitple destination devices in a connection.The priority of a connection with Auto-Priority is set to the value configured in **config.ini** file. You can configure the *connection.autopriority.priorityValue* attribute in the **config.ini** file with a priority value to be used for all the new connections with auto-priority. The connection information lists the allowed filters along with the destination devices.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines for creating a connection with auto-priority:

- To add a new connection with AutoPriority across devices (with multiple hops), the QinQ VLAN configuration is required.
- You can configure only one connection with Auto-Priority mode for each source port/port group.

Adding a New Connection With Auto-Priority

To add a new connection with Auto-Priority, complete these steps:

Before you begin

Ensure that you have configured the monitoring device, destination device, and filters before adding a new connection.

Step 1 Log into the NDB application.

Step 2 Navigate to **Configuration** -> **Connection**, and click **New Connection with AutoPriority** to add a new connection. The **New Connection with AutoPriority** window is displayed.

Step 3 In the **New Connection with AutoPriority** window, complete the following fields:

Name	Description
Connection Name field	The name of the connection.
Description field	Short description of the connection.
Devices/Port Groups drop-down list	The name of the destination device or the destination port group. Select **Devices** and then select a destination device from the Destination Device drop-down list and select corresponding filter from the Allow Filter drop-down list. You can add multiple destination devices with filters for a connection with AutoPriority mode. Select **Port Group** and then select destination port group.
Allow Filters list	Filter to apply to the destination device.

Name	Description
Set VLAN field	VLAN ID range to override the incoming tagged VLAN traffic.
(Optional) **Source Ports** Section	Select Source Ports or Port Group button to create or modify a connection.
Select Source Node drop-down list	Source Node Id.
Select Source port drop-down list	Source Node port number.
Select Port Group	If Port Group Button is enabled, select a Port Group from the drop down for creating or modifying a connection.

Adding Redirections

Note The redirection setup feature is supported on Cisco Nexus 3000 Series and Cisco Nexus 9300 switches with Release 7.x.

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.

Field	Description
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	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. 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. The following optios are displayed in the drop-down list: • 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 Drc field—The source MAC address to be matched for the incoming traffic. An asterisk ("*") indicates any source MAC address.
- DL Dst field—The destination MAC address to be matched for the incoming traffic. An asterisk ("*") indicates any destination MAC address.
- DL Type field—The Ethertype to be matched for the incoming traffic. For example, "IPv4" or "IPv6" is used for all IP traffic types.
- DL VLAN field—The VLAN ID to be matched for the incoming traffic. An asterisk ("*") indicates any VLAN ID.
- VLAN PCP field—The VLAN priority to be matched for the incoming traffic. An asterisk ("*") is almost always displayed in this field.
- NW Src field—The IPv4 or IPv6 source address for the incoming traffic. An asterisk ("*") indicates any source address based on IPv4 or IPv6 Ethertypes.
- NW Dst field—The IPv4 or IPv6 destination address for the incoming traffic. An asterisk ("*") indicates any destination address based on IPv4 or IPv6 Ethertypes.

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

Step 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

Viewing Connection Port Statistics

Starting with Cisco NDB Release 3.4, port statistics are shown along with the connection path information in the NDB GUI. This feature is supported for Nexus 9K and Nexus 3K Series switches based on NX-API, OpenFlow, and NX-AUX mode.

To view the port statistics for a connection, complete the following steps:

Step 1 Navigate to **CONFIGURATION** -> **Connections** .

Step 2 On the **Connection** page, click a connection name for which you want to view the port statistics.

Step 3 Click **Port Statistics** to open the **Flow Statistics** page.

Step 4 Click **Port** tab to view the port statistics for the selected connection.

Deleting Flow and Port Statistics

Starting with Cisco NDB release 3.4, you can now clear port and flow statistics using the NDB GUI. You can either clear all the port related statistics for a switch or clear statistics for a specific port on the switch. For This feature is currently available only for NXAPI based Nexus 9K and Nexus 3K switches.

To clear flow statistics, complete the following steps:

Step 1 Navigate to the **CONFIGURATION** → **Statistics** and click the **Flows** tab to clear flow statistic. Click **Delete ALL** to clear all the flow statistics such as byte count and packet count for the switch.

Step 2 Click the **Ports** tab to clear port statistics.

a) Select a port and click **Delete** to delete statistics for the selected port.

b) Click **Delete All** to clear statistics for all the ports (interfaces) on the switch.

Device Return Material Authorization

Starting with Cisco NDB release 3.8, you can initiate Return Material Authorization (RMA) for a NDB device. This feature maps the configuration from the RMA device to the new device. To RMA a device, complete these steps:

Step 1 Navigate to **ADMINISTRATION** > **Devices** > **DEVICE CONNECTIONS** tab.

Step 2 On the **DEVICE CONNECTIONS** tab, select the switch you want to RMA and click **Remove Devices**. The **Remove Devices** dialog box opens.

Step 3 In the **Remove Devices** dialog box, click **Remove Device**.

Note Do not use **Purge & Remove Device** option, this option removes the device and deletes all the configuration from the NDB.

Step 4 Click **RMA** tab, for the device to RMA, enter the serial number for NX-API device or DPID for OpenFlow devices. For Auxilary devices, you need to enter both OF and serial number.

Note To get the serial number for a NX-API device, use **show module** command for non-modular chassis (look for Serial-Num in the output) or use **show hardware** command for modular chassis switches (look for serial number under Switch hardware ID information in the output).

Note To get the DPID for OpenFlow device, use **show openflow switch 1** command and look for DPID value under the OF features.

Step 5 Click **Submit**.

Step 6 Add a new device. For information about adding a new device, see Adding a Device.

Purging Device Configuration

Starting with Cisco NDB release 3.6, you can now remove and purge all the configuration information (such as connection and redirection) associated with a device that has been removed from the NDB.

To remove device configuration, complete the following steps:

Step 1 Navigate to the **ADMINISTRATION** > **Devices** > **Purge Devices**.

Step 2 Select the devices for which you want to remove all the configuration information and click **Purge Devices**. All the configurations associated with the removed device will be deleted from NDB database.

Exporting and Importing NDB Configuration

You can export and import the device configuration in JSON file format. The configuration file includes information about the connected as well as disconnected devices with all the configuration information (other than port-channel).

Exporting NDB Configuration

Complete the following steps to export a configuration from NDB:

Step 1 Navigate to **Administration** -> **System** -> **Backup/Restore** -> **Node**, and click **Export** tab.

Step 2 Click **Refresh** to list the latest list of NDB devices.

Step 3 Select a device for exporting the configuration from the **Configuration** Pane.

Step 4 (Optional) Select **Include Connections** check box to include connection information such as filters and connections.

Step 5 (Optional) Select **Include Redirections** check box to include connection information such as filters, service nodes, and redirections.

Step 6 Click **Generate new Configuration** to create and save the configuration in JSON format.

Importing NDB Configuration

Complete the following steps to import a configuration into NDB:

Step 1 Navigate to **Administration** -> **System** -> **Backup/Restore**-> **Node**, and click **Import** tab.

Step 2 Click **Select Configuration**, the **File Upload** dialog box appears.

Step 3 Select a JSON file and click **Open**. The selected configuration appears in the **Import** section.

Step 4 Click **Edit** to enter device password (applicable only for NXAPI and NX-AUX mode).

Step 5 (Optional) Select **Include Connections** check box to include connection information such as filters and connections.

Step 6 (Optional) Select **Include Redirections** check box to include connection information such as filters, service node, and redirections.

Step 7 Click **Apply** to apply the configuration to NDB. The **Compatibility Matrix** page appears.

Step 8 Select **Accept and continue** to import the configuration.

Managing Sampled Flow Configuration

Starting with Cisco NDB Release 3.4, you can now manage the Sampled Flow (sFlow) on NDB switches that are based on NX-API. This feature is currently not available for OpenFlow and NX-AUX based switches. 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.

To enable sFlow on a port, complete the following steps:

Step 1 Log into the NDB GUI.

Step 2 Navigate to **CONFIGURATION** -> **Port Definition** tab.

Step 3 Click **Configure Node** to open the **Node Configuration** pane. The **Node Configuration** window is displayed.

Step 4 Click **Configure sFlow** to open the **Configure sFlow** pane.

Step 5 Select **Enable sFlow** from the **Enable/Disable sFlow** drop-down list to open the **Confiigure sFlow** pane.

Step 6 In the **Confiigure sFlow** pane, enter the following details and click Submit.

Field	Description
Agent IP address	sFlow agent IP address.
Select a VRF	VRF to use to reach the SFlow collector IP address.
Collector IP address	SFlow collector address.
Collector UDP	SFlow collector UDP.
Counter Poll Interval	SFlow counter poll interval.
Max Datagram Size	Maximum sampling data size.
Sampling rate	Data sampling rate.
Select Data Source(s)	SFlow datasource interface (Edge-ports)

Note Use **Add to Group** option to add the configured port to a Group of ports.

Note In Sflow pane, the **Select Data Source** field displays only those ports that are configured either as a Edge-SPAN or as a Edge-TAP .

To verify SFLow configuration on a switch, use the show sflow command:

```
RU-29-2003(config)# show sflow
sflow sampling-rate : 4096
sflow max-sampled-size : 128
sflow counter-poll-interval : 20
sflow max-datagram-size : 1400
sflow collector-ip : 0.0.0.0 , vrf : default
sflow collector-port : 6343
sflow agent-ip : 10.16.206.122
sflow data-source interface Ethernet1/1
```

Configuring MPLS Filtering

Starting with Cisco NDB release 3.8, you can filter MPLS traffic. To configure a MPLS filter, complete the following steps:

Step 1 Navigate to **CONFIGURATION** > **Port Definition**.

Step 2 Click **Configure Node** to open **Node Configuration** window.

Step 3 Select **Enable MPLS Filtering** from the **MPLS Filter Configuration** drop-down list.

Step 4 Click **Submit** to enable MPLS ACL configuration on the selected device globally.

Step 5 Create a MPLS filter, navigate to **CONFIGURATION** > **Filters**.

Step 6 In the **Filter** window, click **Add Filter**.

Step 7 Enter filter name in the **Name** text-field.

Step 8 Select **Enter Ethernet Types** from the **Ethernet Type** drop-down list. In the text-field below, enter the hexadecimal values for ethernet types. Ethernet types can be unicast or multicast. For MPLS ACL, enter 0x8847 and 0x8848.

Step 9 Select a MPLS label from the **MPLS Label** drop-down list.

Step 10 Enter MPLS value in the **MPLS Value** text-field.

Step 11 Click **Add** to add the MPLS label to the filter. You can add up to four MPLS labels to a filter.

Step 12 Click **Add Filter** to create a filter with MPLS ACLs.

Step 13 Create a connection, navigate to **CONFIGURATION** > **Connections** > **User Connections** tab.

Step 14 Click **Connections** > **Add a Connection**.

Step 15 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>.
Lock Connection	Select this option to lock the connection you are creating to prevent any unauthorized modification.

Step 16 In the **Allow Matching Traffic** area, modify the following fields:

Field	Description
Allow Filters drop-down list	Choose the MPLS filter you created to allow matching MPLS traffic
Set VLAN field	The VLAN ID that you want to set for the connection. **Note** This functionality is available only in Openflow mode.
Destination Detail	Specifiy the destination details.
Device radio-button	Select this option and from the list of devices select the monitoring device.
Source Ports radio-button	Select this option to specify the source port.
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter.
Select Source Port drop-down list	Choose the port on the source node that you want to assign.

Step 17 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.

Step 18 Verify the configuration using the **show** command

Configuring Symmetric/Non-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 **Load Balancing Type Configuration** drop-down list, select the type and corresponsing **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.

Note MPLS strip is only supported for L3 packets under the MPLS label stack. MPLS strip for pseudowires or VPLS is not supported.

Step 6 Click **Submit**.

Symmetric/Non-Symmetric Load Balancing Options

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

Table 4: Symmetric / Non-Symmetric Load Balancing Port Channel Support

Configuration type	Hashing Configuration	Platforms	Options
Symmetric	SOURCE_DESTINATION	N9K*, N3K-C3164XXX, N3K-C32XXX	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		Rest	IP, IP-GRE, PORT, MAC, IP-ONLY, PORT-ONLY
Non-symmetric	SOURCE DESTINATION	N9K*, N3K-C3164XXX, N3K-C32XXX	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		Rest	IP, IP-GRE, PORT, MAC

Configuring PTP Using NDB

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

Starting with Cisco NDB Release 3.4, you can configure PTP Timestamping feature using the NDB GUI. PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP).

Note Starting with Cisco NDB release, 3.8, you can configure PTP on Nexus 3548 switches.

Note For Cisco NDB 3.4 release and later, PTP Timestamp Tagging feature is supported on the Cisco Nexus 93XXX-EX and 92XX Series switches.

Note Starting with Cisco NDB release 3.8, Timestamp Tagging is supported on Cisco Nexus 9500 Series switches.

Note You need to enable PTP for all the devices in the network to ensure PTP clock time synchronization.

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

To configure PTP using NDB GUI, complete these steps:

Step 1 Log into Cisco NDB GUI.
Step 2 Navigate to **CONFIGURATION** -> **Port Definition** tab.
Step 3 Click **Configure Node** to open the **Node Configuration** pane.
Step 4 Click **Configure PTP** to open the **Configure PTP** pane.
Step 5 Select **Enable PTP** from the **Enable/Disable PTP** drop-down list.
Step 6 Enter the PTP source IP address in the **Source IP Address** text field.
Step 7 Select the interfaces on which you want to enable PTP from the **Select Port(s)** list.
Step 8 Click **Submit** to enable PTP on the selected interfaces.

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.

Note 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. For more information, see the "Configuring ACL TCAM Region Sizes" section in the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Netflow is supported on the following platforms:

- 9300-FX
- 9300-EX
- 9300-FX2
- 9500-EX
- 9500-FX

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

Configuring NetFlow

Starting with Cisco Nexus Data Broker, release 3.8, you can configure NetFlow using NDB. Complete these steps to configure NetFlow using NDB:

- Creating a Flow Record, on page 44
- Creating a Flow Exporter, on page 45
- Creating a Flow Monitor, on page 46
- Applying a Flow Monitor to an Interface, on page 47

Creating a Flow Record

You can create a flow record and add keys to match on and nonkey fields to collect in the flow.

Step 1 Navigate to **CONFIGURATION** > **Port Definitions** > **PORT CONFIGURATION** tab.

Step 2 Click **Configure Node**.

Step 3 In the **Node Configuration** dialog box, click **Configure Netflow**. The **Configure Netflow** page appears.The **Configure Netflow** page contains three sections: **Records**, **Exporter**, and **Monitor**.

Step 4 Click **Add Record** to open **Add Record** dialog box.

Step 5 In the **Name** field, enter a name for the record. You can enter up to 63 alphanumeric characters for the flow record name.

Step 6 In the **Description** field, enter description for the record.

Step 7 From the **Match parameters** drop-down list, select a paramter for the flow record.

Table 5: Match Paramters

Parameter	Description
IP Protocol	Specifies that the IP protocol field is to be matched.
IP TOS	Specifies that the ToS field is to be matched.
IPv4 Source Address	Specifies that the IPv4 source address field is to be matched.
IPv4 Destination Address	Specifies that the IPv4 destination address field is to be matched.
IPv6 Source Address	Specifies that the IPv6 source address field is to be matched.
IPv6 Destination Address	Specifies that the IPv6 destination address field is to be matched.
IPv6 Flow-Label	Specifies that the IPv6 flow label field is to be matched.

Parameter	Description
IPv6 Options	Specifies that the IPv6 options field is to be matched
Transport Source Port	Specifies that the transport source port field is to be matched.
Transport Destination Port	Specifies that the transport destination port field is to be matched.
MAC Source Address	Specifies that the MAC source address field is to be matched.
MAC Destination Address	Specifies that the MAC destination address field is to be matched.
Ethertype	Specifies that the ethertype field is to be matched.
VLAN	Specifies that the VLAN field is to be matched.

Note Ensure that you select either Layer 2 parameters or Layer 3 parameters.

Ensure that you select at least one match parameter and one collect parameter.

Step 8 From the **Collect parameters**, select a paramter for the flow record.

Table 6: Collect Paramters

Parameter	Description
Counter Bytes	Collects bytes based counters.
Counter Packets	Collects packet based counters.
IP Version	Collects the IP version of the flow
Transport TCP Flags	Collects the TCP transport layer flags for the packets in the flow.
SYS Uptime First	Collects the system up time for the first packet in the flow.
SYS Uptime Last	Collects the system up time for the last packet in the flow.

Step 9 Click **Submit** to create a new record. The new record is listed under the **Records** section.

Creating a Flow Exporter

Creating a Flow Exporter

The flow exporter configuration defines the export parameters for a flow and specifies reachability information for the remote NetFlow Collector.

Step 1 Click **Add Exporter** in the **Configure Netflow** page.

Step 2 In the **Add Exporter** dialog box, enter the following details:

Table 7: Add Exporter Fields

Field	Description
Name	Name of the flow exporter being configured.
Description	Description for the flow exporter.
Destination	IP address of the exporter.
Source	Interface on the switch through which the flow cache reaches the destination port.
Transport UDF Port	Specifies the UDP port to use to reach the NetFlow Collector. The range is from 0 to 65535.
DSCP	Differentiated services codepoint value. The range is from 0 to 63.
Version	NetFlow export version.
Option Exporter	Flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Template Date Timeout	Template data resend timer. The range is from 1 to 86400 seconds.

Step 3 Click **Submit** to create a flow exporter.

Creating a Flow 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.

Step 1 On the **Configure Netflow** page, click **Add Monitor**. The **Add Monitor** dialog box appears.

Step 2 In the **Add Monitor** dialog box, enter the following details:

Table 8: Flow Monitor Details

Field	Description
Name	Name of the Flow Monitor.
Description	Description for the Flow Monitor.
Record	Record to attach to the Flow Monitor.

Field	Description
Exporter	Flow Exported to attach to the Flow Monitor. You can select a maximum of 2 Flow Exporters for each Flow Monitor.

Step 3 Click **Submit** to create the Flow Monitor. The new Flow Monitor is listed under the **Monitor** section on the **Configure Netflow** page.

Applying a Flow Monitor to an Interface

You need to apply a flow monitor to an Edge-SPAN port (interface or VLAN) to complete the Netflow configuration and select VLAN from the **Port Configuration** page. Complete these steps to apply a Flow Monotor to an interface:

Step 1 Navigate to **CONFIGURATION** > **Port Definitions** > **PORT CONFIGURATION**.

Step 2 Click **Configure** for the Ethernet interface on which you plan to attach the Flow Monitor.

Step 3 In the **Configure Ports** dialog box, select **Edge Port - SPAN** from the **Select a port type** drop-down list.

Step 4 Enter VLAN number in the **VLAN ID** field. VLAN field is mandatory if the flow monitor is mapped with a L3 record.

Step 5 Select a Netflow monitor from the **Netflow Monitor** drop-down list.

Step 6 Click **Submit** to apply the selected Netflow monitor to the interface. The flow monitor name appears for the configured interface in the **PORT CONFIGURATION** tab.

Configuring Packet Truncation

Starting with Cisco NDB Release 3.5, you can configure packet truncation on egress ports for Cisco Nexus 9300 FX and EX series switches. 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.

Packet truncation enables users to perform header analytics efficiently on the main information in the initial part of the packet . This helps in tools optimization like improving tools performance by eliminating transmission of the unnecessary part of the packet payload and increases storage capacity, by giving tools more room to store the important portions of each packet.

Table 9: Support for Packet Truncation

EX Chassis	FX Chassis	Nexus 9364C, Nexus 9332C	Nexus 9336C-FX2	EOR switches with -EX or -FX LCs
Support started from NX-OS Release 7.0(3)I7(1)	Support started from NX-OS Release 7.0(3)I7(1)	Support started from NX-OS Release 7.0(3)I7(2)	Support started from NX-OS Release 7.0(3)I7(3)	9.3(1)
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

EX Chassis	FX Chassis	Nexus 9364C, Nexus 9332C	Nexus 9336C-FX2	EOR switches with -EX or -FX LCs
Four active localized SPAN sessions	Four active localized SPAN sessions	Four active localized SPAN sessions	Four active localized SPAN sessions	-

Note Starting with Cisco NDB release 3.8, you can now configure packet truncation on Cisco Nexus 9500 Series switches.

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

To configure packet truncation on a device, you need to:

1. Configuring a Packet Truncation Interface
2. Defining a Monitoring Device with Packet Truncation Interface

Configuring a Packet Truncation Interface

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

To configure a packet truncation interface, complete these steps:

Step 1 Log into NDB.

Step 2 Navigate to the **CONFIGURATION** > **Port Definition** and select the switch for which you plan to configure packet truncation.

Step 3 Click **PORT CONFIGURATION** tab.

Step 4 Click **Configure** for the interface selected for configuration.

Step 5 In the **Configure Ports** pane, click **Select a port type** and then click **Packet Truncation Port**.

Step 6 (Optional) Enter description for the port in the **Port Description** text field.

Step 7 Click **Submit** to create a packet truncation port.

By default a packet truncation port is blocked for ingress traffic.

Note 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 the same NDB switch. To change the port Layer 2 status to Up, you need to connect to another switch or create a loopback using a third party loopback fiber optic.

What to do next

After the packet truncation port is created, you need to create a monitoring device with the packet truncation port. For more information, see Defining a Monitoring Device with Packet Truncation Interface section.

Defining a Monitoring Device with Packet Truncation Interface

Complete the following steps to define a monitoring device with a packet truncation interface:

Step 1 Navigate to the **CONFIGURATION** > **Port Definition** and select the switch for which you plan to configure packet truncation.

Step 2 Click **PORT CONFIGURATION** tab.

Step 3 Click **Configure** for the interface selected for configuration.

Step 4 In the **Configure Ports** pane, click **Add Monitoring Device**.

Step 5 In the **Monitoring Device** window, complete the following fields:

Name	Description
Monitoring Device Name	Name of the monitoring device.
Select Switch Name	Name of the switch to add the monitoring device to.
Select Port	Packet truncation port you configured.
Port Description	Description of the port.

Step 6 Select **Packet Truncation**.

Step 7 Enter maximum packet size in the **MTU Size** text field. The MTU size can be between 320 and 1518 bytes.

Packet truncation discards bytes from the header of an incoming packet based on the set MTU size.

Step 8 From the **Select Packet Truncation Port** drop-down list, select the packet truncation port you created on the same switch.

Step 9 (Optional) Select device icon for the monitoring device.

Step 10 Click **Submit** to create the monitoring device.

What to do next

Create a new connection using the monitoring device to implement the packet truncation feature. For more information, see Adding Connections.

Show Tech for NX-API Devices

The show tech for NX-API devices feature enables you to collect information from one or more switches in one attempt, instead of collecting data separately from each switch. This is useful during debugging as all the relevant logs are readily available and can be downloaded.

Limitations

- Supported only on Nexus switches in NX-API mode.

Prerequisites

- Ensure that one or more switches are connected to the NDB server and the AUX mode is disabled.

Show tech data collection from switches can be performed in two modes:

Basic mode– contains the below set of show commands:

- **show version**
- **show hostname**
- **show hardware**
- **show modules**
- **show cores**
- **show system uptime**
- **show system reset-reason**
- **show running-config**

Advanced mode– contains a broader set of show commands and they are:

- **show version**
- **show hostname**
- **show hardware**
- **show modules**
- **show cores**
- **show system uptime**
- **show system reset-reason**
- **show accounting-log**
- **show logging logfile**
- **show running-config**
- **show nxapi**
- **show nxapi retries**
- **show processes memory | grep nginx**
- **show processes memory | grep vsh**
- **show nxapi-server logs**
- **show interface**
- **show lldp neighbors detail**
- **show access-lists**
- **show access-lists summary**
- **show hardware access-list tcam region**

Configuring Show Tech

This task has details about how to configure a show tech job.

Step 1 Login to the NDB UI.

Step 2 Navigate to **Administration**> **System**> **Tech Support**.

Step 3 Click **Trigger** to trigger a tech support job.

The Trigger Show Tech pane is displayed.

Step 4 Select the devices for which you need to collect the data. Click each device for it to get selected.

You can click **Select All** to select all the displayed devices.

The devices you have selected are displayed in the Selected Switches area.

Step 5 Select the **Type of Operation** by choosing the required radio button – Basic or Advanced (the applicable commands for each have been discussed earlier). The commands applicable for Basic and Advanced are displayed in the area below.

Step 6 Click **Submit** to trigger the tech support job.

At any given time, only one job is executed.

Step 7 The job is created and the job details are displayed in a table format with the following details:

- Job ID – job identification which includes the date the job was created. The most recently created job appears at the beginning of the table. Click the job ID to view more details about the job, such as, node and host details , status and reason.
- Job Type – job type based on type of operation selected.
- Status – the current status of the job. The statuses are color-coded for easy identification. The available statuses are –
  - Success – job is successfully completed.
  - Partial – job is partially successful. For eg, if multiple devices were selected, then, may be the failure has occurred on one of the selected switches.
  - Failure – job is not successful.
  - In progress – job is currently in progress.
  - Created – job is ready for execution, but is in a queue.
  - Aborted – job was created but was not allowed to complete.
- Action – when a job is successfully completed, you can perform either of the actions- Delete or Download and Delete.
- Download – a zip file is downloaded onto your local machine.
- Download and Delete – a zip file is downloaded on to your local machine and the file is removed from the server.

Note The following folders are by default downloaded besides the show tech folder – configuration folder, configuration start up folder and general logs. This enables the tech support team to get all the information together and results in faster analysis.

What to do next

You can do any of the following operations after submitting a show tech job.

- Re-trigger – Select the check box next to the job ID and click re-trigger to re-trigger a job. In progress and Created jobs cannot be re-triggered. The show tech log files are replaced with the latest set of files, after retriggered job is successful.
- Abort – Select the check box next to the job ID and click Abort. Only In progress and Created jobs can be aborted.
- Remove – Select the check box next to the job ID and click Remove.

Multiple eligible jobs can be removed/aborted/re-triggered at a time.

Syslog

In the NDB server backend, you can tune the `logback.xml` file to send logs to the Syslog server. You can customize the log format as per your requirement.

If NDB server(s) are running, restart the servers after the changes are made in the `logback.xml` file.

```
File Location: /xnc/configuration/logback.xml

Sample Syslog configuration:
Add below config with respective Syslog server IP address and port number in logback.xml
file.
  <appender name="SYSLOG" class="ch.qos.logback.classic.net.SyslogAppender">
    <syslogHost>10.16.206.171</syslogHost>
    <facility>LOCAL7</facility>
    <port>514</port>
    <suffixPattern>[%thread] %logger %msg</suffixPattern>
  </appender>

Append "<appender-ref ref="SYSLOG" />" in root as shown below,
  <root level="error">
    <appender-ref ref="STDOUT" />
    <appender-ref ref="SYSLOG" />
    <appender-ref ref="xnc.log" />
  </root>
```

After upgrade, these configuration changes in the `logback.xml` file will be lost. Thus, after upgrading the controller to newer a NDB version, check and restore this configuration manually.