Configuring the Nexus Data Broker

This chapter contains the following sections:

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 IP address, MAC address, and connection information is displayed for each device in the topologhy 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

Procedure

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

Step 2 Click **Configure** under **Action**.

The **Configure Ports** window is displayed.

Step 3 In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

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

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

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

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

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

Note 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.

Procedure

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.

Adding SPAN Destination

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

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

Procedure

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

Step 2 Click **Configure** under **Action**.

The **Configure Ports** window is displayed.

Step 3 In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

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

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

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

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

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

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

Step 4 In the SPAN DESTINATION pane, select the pod from the **Pod** drop-down list.

Step 5 Select the ACI leaf from the **Leaf** drop-down list.

Step 6 Select the port from the ACI side from the **Port** drop-down list and set the interface as SPAN destination.

Step 7 Click **Submit** to save the settings.

The port is now configured as SPAN destination part and it is displayed on the Port Definition screen.

Configuring Multiple Ports

You can configure multiple ports for a node.

Procedure

Step 1 Click **Configure Multiple Ports** on the **Port Configuration** screen. The **Configure Multiple Ports** window is displayed.

Step 2 Use **CTRL/SHIFT** to select multiple ports in the **Select Ports** field.

Step 3 Select port type from the drop-down list in the **Select Port Type** field.

Step 4 Click **Submit** to save the settings.

Configuring Port Groups

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

Before you begin

Procedure

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.

Editing In Use Port Groups

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.

Procedure

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 (If the port is not part of an active connection)
	Port Group	Yes (If the port group is not part of an active connection)

Creating Destination Port Groups

Starting with Cisco NDB Release 3.7, you can now create and configure destination port groups with monitoring devices and add the monitoring devices to a connection. You can add destination port groups to a normal connection or to an Auto-priority connection.

- You can associate one port with only one destination port group.
- You can add multiple destination port groups to a connetion.
- You can delete a destination port group only if it is not part of any connection.
- If a destination port group is part of a connection, you can edit only the port group description and ports.

To configure Destination Port Group, complete these steps:

Procedure

Step 1 Log into Cisco NDB GUI.

Step 2 Navigate to **CONFIGURATION** > **Port Groups** > **DESTINATION PORT GROUP** tab.

Step 3 Click **Add Destination Port Group** to open the **Create Destination Port Group** pane.

Step 4 In the **Create Destination Port Group** pane, enter details for the following fields:

Name	Description
Group Name	Destination port group name.
Description	Details about the destination port group..
Select Note	Select a Node.
Choose Port(s)	Select the ports to include to the new destination port group.
Selected Port(s)	List of ports selected for the new destination group

Step 5 Click **Submit** to create the new destination port group.

The new destination port group appears on the **DESTINATION PORT GROUPS** tab.

Note Edit a destination port group using the **Edit** option for the port group. To view details about a destination port group, click **View**.

Note To delete a port group, click **Delete** for the port group. You can delete a port group only if it is not part of any connection.

Note Only one Remote monitor tool can be added per switch in the group.

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. 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:

Procedure

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	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.
Remote Monitor Device	Select this option to indicate that the monitoring device is available in the local network.
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 Monitoring Device

To add a new monitoring device, complete these steps:

Procedure

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.
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.
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 timestap 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.

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:

Procedure

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.

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:

Procedure

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

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.

Procedure

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. • UDF Mask: Mask value in packet to match. **Note** Starting with Cisco NDB Release 3.6, you can add upto four UDFs to a filter. **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).

Procedure

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

Step 2 In the **Add Connections** window, you can add the **Connection Name** and the **Priority** of the connection in the **Connection Details** area:

Field	Description
Connection Name	The name of the connection.
Description	Enter the description when creating a new connection.
Priority	The priority that you want to set for the connection. Connection by default has priority of 100. It can be changed in the range of <1-10000>.
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.
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.

Field	Description
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes next to their names.

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

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

Step 5 In the **Source Ports (Optional)** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter. **Note** When setting up a new redirection, you can see the number of flows that are part of each input port. When you click the port number, the flow details are displayed.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports. **Note** If you do not select a source port while adding a new connection, the following warning message is displayed: No source port is selected. Connection will be setup from all configured Edge-SPAN and Edge-TAP ports. Click OK to continue with the connection installation/creation. It ensures that you do not install any to multi point connection and disrupt any existing traffic. Click Cancel to take you to the connection setup page.

Field	Description
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.

Note Starting with Cisco NDB Release 3.6, 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 topolgy 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 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.

Procedure

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.
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.

Procedure

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.

Procedure

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:

Procedure

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:

Procedure

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.

Adding SPAN Sessions

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

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

You can add a SPAN session in ACI.

Procedure

Step 1 Click **+ SPAN Session** to add a SPAN session. The **Add SPAN Session** window is displayed.

Step 2 In the **Add SPAN Session** window, add a session name in the **SPAN Session Name** field.

Step 3 (Optional) Select a connection in the **Select Connections** field.

Step 4 In the **Action** pane, select a priority for the SPAN session.

Step 5 Select a rule using the drop-down list in the **Rule Filter** field. You can select the default filter rule, **Default-Match-IP** or select another filter from the drop-down list.

The available filter rules are **Default-Match-IP**, **Match-HTTP**, **Match-vlan**, and **Default-Match-all**.

Step 6 Select a destination device to which the traffic is sent.

Step 7 In the **SPAN SOURCES** pane, select the device type as ACI or NXOS in the **Select Device Type** field. When you select ACI device and click +Add SPAN Source, the **Add Leaf Ports** or **+Add EPG** tabs are displayed.

a) In the **Add Leaf Ports** window, select a pod using the drop-down list in the **POD** field.
b) Select a node using the drop-down list in the **Node** field.
c) Select a port using the drop-down list in the **Port** field.
d) Click **Add Leaf Ports**.
e) In the **SPAN SOURCES** pane, select a direction from the **Incoming**, **Outgoing**, or **Both** options.

The selected Span source is displayed in the **Span Source** field.

f) If you select **+Add EPG** to add EPG source, select a tenant using the drop-down list in the **Tenant** field in the **Add EPG** window.

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

g) Select a profile using the drop-down list in the **Profile** field.
h) Select EPG associated with the tenant using the drop-down list in the **EPG** field.

The selected **SPAN Source** is displayed.

i) Select **Include All EPG Interfaces** option.

When you enable this option, the statically configured interfaces are added to the EPG.

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

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

j) Click **Add EPG**.

Step 8 In the **SPAN SOURCES** pane, when you select the device type as NXOS in the **Select Device Type** field and click **+Add SPAN Source**, the **Add Interface** or **Add VLAN** tabs are displayed.

This field allows to add NXOS SPAN session via NXAPI. It allows to add 2 types of SPAN sources. If you need to add interface as source, click **+ ADD SPAN Source** and click **Interface**. If you need to allow traffic of a particular VLAN, click **VLAN**.

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

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

Step 9 When you click **+Add Interface**, the **Add Production Switch Interface** window is displayed.

You can select a node, select an interface, and click **Submit**.

Step 10 When you click **+Add VLAN**, the **Add Production Switch VLAN** window is displayed.

You can select a node, enter a VLAN, and click **Submit**.

Step 11 In the **SPAN Destination** field, you can select the SPAN destination.

This field displays SPAN destination for ACI in the ACI SPAN session or SPAN destination for NXOS in the NXOS SPAN session.

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

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

Step 12 Click **Add SPAN Session**.

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

Step 13 Click **OK**.

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

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

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

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

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

Exporting and Importing NDB Configuration

Starting with Cisco Nexus Data Broker,Release 3.4, you can now export and import the device configuration in JSON file format.The configuration file includes information about connected as well as disconnected devices with configuration information such as filters, ports, connections, and redirections.

Exporting NDB Configuration

Complete the following steps to export a configuration from NDB:

Procedure

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:

Procedure

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:

Procedure

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 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.

Procedure

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.

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

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).

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.

Note For Cisco NDB 3.4 release and later, PTP Time-stamping feature is supported on the Cisco Nexus 93XXX-EX and 92XX 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:

Procedure

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.

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.

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

To configure a packet truncation interface, complete these steps:

Procedure

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.

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:

Procedure

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.

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.