Configuring Ports and Devices

This chapter contains the following sections:

About Cisco Nexus Data Broker Port Types

Cisco Nexus Data Broker enables you to configure different port types. All configured ports are displayed in the **Configured Ports** table on the **Port Types** tab.

You can configure a port as an ingress TAP/SPAN port or a monitoring tool port so that it is easier to aggregate and redirect the traffic.

Note If the software version is earlier than 7.x, an error message is displayed that the TAP aggregation is not supported in the current version of the NX-OS and you have to upgrade to the specified release or above. The 7.0 software version details are applicable for NX-API only.

You can select a port and define if the port is an ingress source port or an egress re-direction port. The ingress source port in Cisco Nexus Data Broker is mapped to the Edge-SPAN or the Edge-Tap port and the egress redirect port is mapped to the monitoring tool port. The switch interconnection ports are not displayed for the selection.

Note The color coding for the port name indicates the status of the port itself. Green means that the port is up, orange means that the port is down, and red means that the port is administratively down.

Edge Ports

Edge ports are the ingress ports where traffic enters the monitor network. Cisco Nexus Data Broker supports the following edge ports:

- TAP ports—For incoming traffic connected to a physical tap wire.
- SPAN ports—For incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Configuring an edge port is optional.

Note For Any-to-Multipoint (A2MP) forwarding path option, Cisco Nexus Data Broker only uses the configured edge ports as ingress edge ports or source ports.

Delivery Ports

Delivery ports are the egress ports where the traffic exits the monitor network. These outgoing ports are connected to external monitoring devices. When you configure a monitoring device in Cisco Nexus Data Broker, you can associate a name and an icon to the monitoring device.

Configured devices are displayed in the **Monitor Devices** table on the **Devices** tab. The icon appears in the topology diagram with a line that connects it to the node.

VLAN Tagging

Cisco Nexus Data Broker enables you to configure a switch port as an edge port and specify a VLAN for that port. When you configure the VLAN ID, and the connection to the Cisco onePK agent is up, Cisco Nexus Data Broker programs the Cisco Nexus 3000 Series switches, 3100 Series switches, and Cisco Nexus 9000 Series switches so that all packets received in that port are VLAN tagged, and the VLAN ID is the one configured on the edge port. If the packets received in that port are already VLAN-tagged frames, they get double-tagged, and the outermost VLAN tag contains the VLAN ID that is associated with the configured edge port.

Note VLAN tagging with NX-API mode is now supported and it can be enabled from Cisco Nexus Data Broker UI.

Configuring a Port Type

Procedure

Step 1 In the topology diagram, click the node for which you want to configure a port.
The **Ports** area of the sidebar displays the list of ports available to configure for that node.

Step 2 In the list of ports for the node, click **Click to configure** under the port identifier of the port that you want to configure.

Step 3 From the **Select a port type** drop-down list, choose one of the following:

- **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.

Step 4 (Optional) In the **Port Description** field, enter a port description.
The port description can contain between 1 and 256 alphanumeric characters, including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 5 Enter a VLAN ID.
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 In the **Enable Packet Truncation** field, enter the packet length.

Step 7 Click **Submit**.

Configuring Multiple Ports

You can now configure multiple ports or a range or ports for port definition.

Procedure

Step 1 Click **Configure Multiple Ports** in the side bar of the GUI.

Step 2 In the **Select Ports** drop-down list field, select the ports that you want to assign. You can select multiple ports using ctrl or shift that you want to assign for redirection.

Step 3 In the **Select Port Type** drop-down list field, select the port type that you want to assign:

- Edge port-SPAN
- Edge port-TAP
- Production Port

Step 4 Click **Submit**.

Removing a Port Type Configuration

Before You Begin

- At least one port type must be configured.
- The port type configuration that you want to remove must not be used in a rule. If it is, you must either modify or remove the rule before you can remove the port type configuration.

Note If the configured port is of SPAN or Edge ports and if any connections are created based on these ports, you will not be able to delete those connections. Only after removal of the connections, the port definition of the SPAN/Edge ports can be deleted.

Procedure

Step 1 From the **Port Types** tab, choose one of the following:

- The top checkbox to select all **Configured Ports** for removal.
- The check box next to the name of only the configured port or ports that you want to remove.

Step 2 Above the list of **Configured Ports**, click **Remove Port Configuration**.

Step 3 In the **Remove Port Configuration** confirmation dialog box, click **Remove Port Configuration**.
The port configurations are removed.

Configuring a Monitoring Device

Procedure

Step 1 In the topology diagram, click the node for which you want to configure a monitoring device.
The **Port Types** tab displays the list of ports available to configure for that node.

Step 2 In the list of ports for the node, click **Click to configure** under the port identifier of the port that you want to configure.

Step 3 From the **Select a port type** drop-down list, click **Add Monitoring Device**.

Step 4 In the **Add Device** dialog box, complete the following fields:

Name	Description
Device Name field	The name that you want to use for the monitoring device. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** You can change the device name after the monitoring device has been added.
Icons selection	The choice of icons, with the first one selected by default. Choose any icon to use for the monitoring device. **Note** You can change the icon for the monitoring device after it has been added.

Step 5 Click **Submit**.

Removing a Monitoring Device

Note If the monitor device is part of a connection, Cisco Nexus Data Broker does not allow the user to delete the monitor device.

Before You Begin

- At least one monitoring device must be configured for the port.

- The monitoring device that you want to remove must not be used in a rule. If it is, you must either modify or remove the rule before you can remove the monitoring device.

Procedure

Step 1 Click the **Devices** tab.

Step 2 In the **Device Name** list, choose one of the following:

- The top checkbox to select all monitoring devices for removal.
- The checkbox next to the name of only the monitoring device or devices you want to remove.

Step 3 Above the **Device Name** list, click **Remove Monitoring Devices**.

Step 4 In the **Remove Monitoring Devices** confirmation dialog box, click **Remove Devices**.

Configuring a Root Node

A root node is automatically selected by Cisco Nexus Data Broker. If the defined root node is too far from the source switches, you can manually configure a different switch. We recommend that you choose a switch with edge ports as your new root node.

Note Root node changes do not take effect until you save the configuration.

Procedure

Step 1 From the **Root** tab, click **Configure Root Node**.

Step 2 In the **Configure Root Node** dialog box, choose a node from the drop-down list.

Step 3 Click **Configure Root Node**.
The **Configured Root Node** is displayed the **Root** tab, and below it the **Current Root Node**, if any.

Step 4 Click **Save** in the menu bar.
The root node addition or change is saved.

Cisco onePK Agent

The Cisco onePK plug-in for Cisco Nexus Data Broker communicates with onePK devices through a onePK agent on the device. To support onePK device functions in Cisco Nexus Data Broker, the application must be connected to the onePK agent. The agent is the mediator between Cisco Nexus Data Broker and onePK-enabled devices that are configured in Cisco Nexus Data Broker.

To secure communication between Cisco Nexus Data Broker onePK-enabled devices, you must configure Transport Layer Security (TLS) in Cisco Nexus Data Broker. See the *Cisco Nexus Data Broker Configuration Guide* for detailed procedures.

Connecting to a onePK Agent

You must connect to a onePK agent to support additional functionality in Cisco Nexus Data Broker, including symmetric load balancing, Q-in-Q, timestamp tagging, and packet truncation.

Procedure

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Device Connections** tab.

Step 3 Click **Add Device**.

Step 4 In the **Add Device** dialog box, choose Connection Type field as onePK.

Step 5 Click **Add Device**.

Symmetric Load Balancing

Cisco Nexus Data Broker enables you to configure symmetric load balancing settings on the egress port channels. Load balancing settings are based on Layer 2 source MAC and destination IP addresses, or Layer 2, Layer 3, or Layer 4 source and destination ports. When you configure symmetric load balancing for all the port-channel interfaces on the switch, all the traffic from specific sources and destinations in both directions always flows on the same port-channel member link.

Note Symmetric load balancing in Cisco Nexus Data Broker is available for Cisco Nexus 3100 Series switches and Cisco 9000 Series switches.

Configuring Symmetric Load Balancing

Before You Begin

- Configure and provision TLS on the switches.
- Add device to Cisco Nexus Data Broker using NX-API or onePK connection.

Procedure

Step 1 In the topology diagram, click the node for which you wish to configure symmetric load balancing.

Step 2 In the side bar, from the **Symmetric Load Balancing** drop-down list, choose one of the following:

- **SOURCE_DESTINATION_IP—**source and destination IP address (includes Layer 2)
- **SOURCE_DESTINATION_IP_ONLY—**source and destination IP addresses only
- **SOURCE_DESTINATION_PORT—**source and destination TCP/UDP port (includes Layer 2 and Layer 3)
- **SOURCE_DESTINATION_PORT_ONLY—**source and destination TCP/UDP port only

Step 3 Click **Submit**.

Enabling MPLS Tag Stripping

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

Configuring MPLS Tag Stripping

Before You Begin

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

Procedure

Step 1 In the topology diagram, click the node for which you wish to configure MPLS tag stripping.

Step 2 In the side bar, from the **MPLS Strip Configuration** drop-down list, choose one of the following:

- Enable MPLS Strip.
- Disable MPLS Strip.

Step 3 In the side bar, from the Label Age field, enter a value for the MPLS strip label age. The range for MPLS strip label age configuration is 61-31622400.

Step 4 Click **Submit**.

Configuring Q-in-Q

Note The ability to configure Q-in-Q is available for Cisco Nexus 3000 and 3100 Series switches and on Nexus 9000 switches in NX-API mode. Q-in-Q is automatically enabled when you configure a VLAN ID for an edge port, if the VLAN ID is maintained on the edge port.

Procedure

Step 1 In the topology diagram, click the node for which you wish to configure Q-in-Q.

Step 2 In the side bar, configure an edge port and set a VLAN ID on that edge port.

Step 3 Click **Enable QinQ**.

Step 4 In the **Connect to onePK Agent** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The username of the user that you want to assign to the device.
Password field	The password of the user that you want to assign to the device.

Step 5 Click **Submit**.

Configuring Packet Truncation

Note Packet truncation can only be configured on Cisco Nexus 3500 Series switches.

Before You Begin

- Configure a onePK device.
- Connect to the onePK agent.

Procedure

Step 1 In the topology diagram, click the node for which you wish to configure packet truncation.

Step 2 In the side bar, click the port for which you want to configure packet truncation.

Step 3 From the **Select a port type** drop-down list, choose one of the following:

- **Edge Port-SPAN**
- **Edge Port-TAP**

Step 4 (Optional) In the **Port Description** field, enter a port description.
The port description can contain between 1 and 256 alphanumeric characters, including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 5 (Optional) Enter a VLAN ID.
The port is configured as dot1q to preserve any production VLAN information.

Step 6 In the **Enable Packet Truncation** field, enter the truncated packet length that you want, in bytes.

Note It is recommended that you enter a minimum of 64 bytes, in multiples of 4.

Step 7 Click **Submit**.
The port configuration is saved, and the number of bytes for truncated packets is displayed in the label **TRUNC=<bytes>** beside the port name.

Configuring Timestamp Tagging

With Cisco Nexus 3500 platform switches, you can:

- Truncate the packets after a user-defined threshold at ingress.
- Time-stamp the packets using Precision Time Protocol (PTP) with nanosecond accuracy.

With PTP, the IEEE 1588 packet is time-stamped at the ingress port to record the event message arrival time in the hardware at the parser level. The time stamp points to the first bit of the packet (following the start frame delimiter [SFD]). Next, the packet is copied to the CPU with the time stamp and the destination port number. The packet next traverses the PTP stack. The advanced PTP clock algorithm in the Cisco Nexus 3548 Series switches keeps a track of all the timing and the frequency information and it makes the necessary adjustments to help ensure accurate time.

Finally, the packet is internally marked as a high-priority packet to ensure priority egress out of the switch and it is sent out at the egress port. The corresponding time stamp for the transmitted packet is available from the First In, First Out (FIFO) transmission time stamp.

The timestamp tagging feature is used to provide precision time information to monitor the devices remotely and to track the real time when the packets arrive at the Cisco Nexus 3500 Series switches. The timestamp tagging feature configures the **ttag** command on the egress interface.

The ether-type <type> option sets the Ethertype field of the ethernet frame. The Ethertype is used to indicate which protocol is encapsulated in the payload. Ethertype 1 (type 0x88B5) is used for this purpose.

Note Timestamp tagging can only be configured on Cisco Nexus 3500 Series switches.

Before You Begin

- Configure a delivery device on the node.
- Configure a onePK device.

Procedure

Step 1 In the topology diagram, click the node for which you wish to configure timestamp tagging.

Step 2 In the side bar, configure a delivery device.

Step 3 In side bar, click **Click to enable additional functionality**.

Step 4 In the **Connect to onePK Agent** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The username of the user that you want to assign to the device.
Password field	The password of the user that you want to assign to the device.

Step 5 Check the check box next to **Enable Timestamp Tagging**.

Step 6 Click **Submit**.
The port is displayed in the **Port** list with the label **TS-Tag**.