Guide

Cisco Nexus Data Broker Embedded: Implementation Quick-Start Guide

Contents

What You Will Learn

This document provides a quick-start configuration guide for implementing the Cisco Nexus® Data Broker embedded solution, which is an on-switch deployment option for network traffic visibility using a single Cisco Nexus 3000 Series Switch or Cisco Nexus 9300 platform switch for test access point (TAP) and Cisco Switched Port Analyzer (SPAN) aggregation. This document includes the steps for configuring:

- Cisco® Plug-in for OpenFlow on the Cisco Nexus 3000 Series and Cisco Nexus 9300 platform switches
- Cisco Nexus Data Broker application on the Cisco Nexus 3000 Series and Cisco Nexus 9300 platform switches
- Cisco NX-API mode configuration on the Cisco Nexus 9300 platform switches

Disclaimer: This document does not replace the configuration guide published for the products. For a list of applicable configuration guides, please see the For More Information section at the end of this document.

Cisco Nexus Data Broker Solution Overview

The Cisco Nexus Data Broker replaces a purpose-built matrix network with one or more Cisco Nexus 3000 or 9000 Series Switches for network TAP and SPAN aggregation. The traffic is tapped into this bank of Cisco Nexus 3000 or 9000 Series Switches in the same manner as in a matrix network. However, with the Cisco Nexus Data Broker application, traffic can be filtered and forwarded to the right tools. The filtering and forwarding rules can change dynamically on the basis of business logic, allowing unique traffic patterns to flow directly to the tools in real time. In addition, because the Cisco Nexus Data Broker supports common programmable interfaces such as Java and representational state transfer (REST), network operators can write applications to detect and capture unique traffic, closing any coverage gaps.

Customers who want to run Cisco Nexus Data Broker using a single Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switch in their network have the option to run Cisco Nexus Data Broker in the Linux container of the switch itself using embedded mode. Cisco Nexus Data Broker embedded software is distributed as an open virtual appliance (OVA) that can be deployed in the Cisco Nexus switch's Linux container. All features of Cisco Nexus Data Broker are available in this option as well except:

- Clustering and high availability
- Management for multiple switches for network TAP or SPAN aggregation

Table 1 summarizes the main features and functions available with the Cisco Nexus Data Broker embedded solution.

Table 1. Main Features

Feature	Benefit
Support for a variety of port capacities	• The data broker supports 1-, 10-, 40-, and 100-Gbps ports.
Support for TAP and SPAN aggregation	• You can configure ports as monitoring tool ports or as input TAP and SPAN ports. • You can set end-device names for easy identification in the topology.
Support for IEEE 802.1 Q-in-Q to tag input source TAP and SPAN port*	• You can tag traffic with a VLAN for each input TAP or SPAN port. • Q-in-Q in edge TAP and SPAN ports can uniquely identify the source of traffic and preserve production VLAN information.
Symmetric hashing or symmetric load balancing*	• You can configure hashing based on Layer 3 (IP address) or Layer 3 plus Layer 4 (protocol ports) to load-balance the traffic across a port-channel link. • You can spread the traffic across multiple tool instances to accommodate high-traffic-volume scale.

Feature	Benefit
Rules for matching monitored traffic	• You can match traffic based on Layer 1 through Layer 4 criteria. • You can configure the software to send only the required traffic to the monitoring tools without flooding the tools with unnecessary traffic. • You can configure an action to set the VLAN ID for the matched traffic.
Layer 7 monitoring for HTTP traffic*	• You can match on HTTP methods such as GET and PUT and take specific actions for that traffic. • This feature can help reduce the volume of traffic sent to any Websense tools.
Multiprotocol Label Switching (MPLS) label stripping*	• You can filter MPLS packets by enabling MPLS label stripping.
Traffic replication and forwarding	• You can aggregate traffic from multiple input TAP and SPAN ports. • You can configure the software to replicate and forward traffic to multiple monitoring tools. • This solution is the only solution that supports any-to-many forwarding.
Time stamping**	• You can time-stamp a packet at ingress using the Precision Time Protocol (PTP; IEEE 1588), thereby providing nanosecond accuracy. • You can use this capability to monitor critical transactions and archive data for regulatory compliance and advanced troubleshooting.
Packet truncation**	• You can configure the software to truncate a packet beyond a specified number of bytes. • The minimum packet size is 64 bytes. • You can retain a header for only analysis and troubleshooting. • You can configure the software to discard the payload for security or compliance reasons.
End-to-end path visibility	• For each traffic-forwarding rule, the solution provides complete end-to-end path visibility all the way from the source ports to the monitoring tools.

Cisco Nexus Data Broker Solution Lab Setup Topology

This solution implementation guide presents the steps you need to complete to set up the Cisco Nexus Data Broker embedded solution. Following are the prerequisites you need to implement before you set up the solution:

- Download the Cisco Nexus Data Broker embedded zip file from Cisco.com: https://software.cisco.com/download/release.html?mdfid=286281492&softwareid=286281554&release=2.2.0&relind=AVAILABLE&rellifecycle=&reltype=latest&i=rm. Use Table 2 to select the file to download.

Table 2. Cisco Nexus Data Broker Download File Matrix

Cisco Nexus Switch	Cisco NX-OS Version	File to Download
Cisco Nexus 3000 Series and Cisco Nexus 3100 and 9300 platforms	Cisco NX-OS Release 7.0(3)I2(1) in OpenFlow mode	ndb1000-sw-app-emb-2.2.0-ofa_mmemb-2.1.0-r1-nxos-SPA-k9.zip
Cisco Nexus 9300 platform	Cisco NX-OS Release 7.0(3)I2(1) in NX-API mode	ndb1000-sw-app-emb-nxapi-2.2.0-k9.zip
Cisco Nexus 3000 and 3500 Series and Cisco Nexus 3100 platform	Cisco NX-OS Release 6.0(2)X in OpenFlow mode	ndb1000-sw-app-emb-2.2.0-ofa_mmemb-1.1.5-r3-n3000-SPA-k9.zip

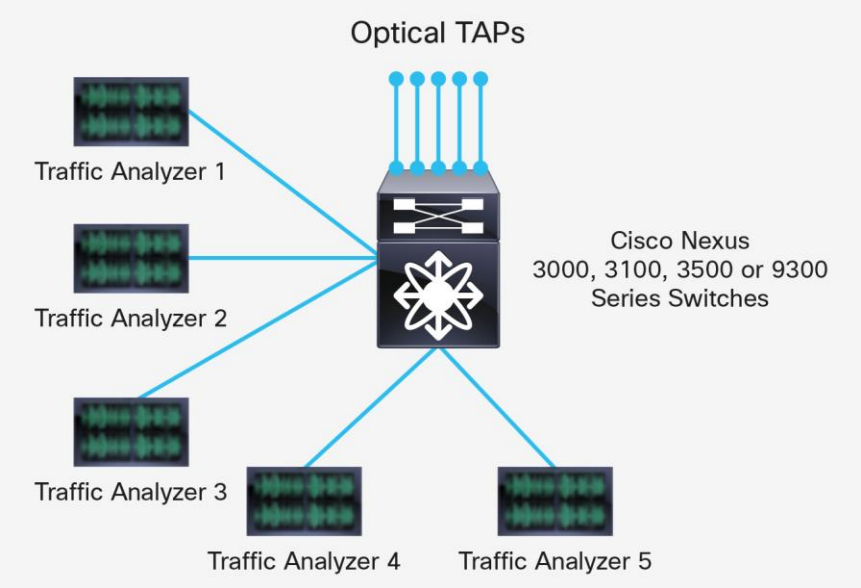
If the embedded deployment mode is OpenFlow:

- Copy the Cisco Nexus Data Broker embedded zip file to a directory; then extract the file. The zip file contains two OVA files.
- Copy the two OVA files to bootflash memory on the Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switch on which the Cisco Nexus Data Broker embedded solution will be implemented.
- Upgrade the Cisco NX-OS Software on the Cisco Nexus switches:
  - For Cisco Nexus 3000 Series and Cisco Nexus 3100 platform switches, use one of the following:
    - Cisco NX-OS Release 6.0(2)U6(4).
    - Cisco NX-OS Release 7.0(3)I2(1).

- For Cisco Nexus 3500 Series and Cisco Nexus 3500-X platform switches, upgrade NX-OS to Cisco NX-OS Release 6.0(2)A6(4).
- For each Cisco Nexus 9300 platform switch, upgrade NX-OS to Cisco NX-OS Release 7.0(3)I2(1).

Figure 1 shows the monitoring network (TAP aggregation) topology used in the configuration steps in this document. Five TAPs and five monitoring devices (traffic analyzers) are connected to the Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switch used to demonstrate the Cisco Nexus Data Broker embedded configuration.

Figure 1. Monitoring Network Topology



- Connect optical TAPs to Ethernet ports 1/10 through 1/14 on the Cisco Nexus switch.
- Connect traffic analyzer devices to Ethernet ports 1/41 through 1/45 on the Cisco Nexus switch.

Enabling Cisco Plug-in for OpenFlow on Cisco Nexus 3000 Series and Cisco Nexus 9300 Platform Switches

This section assumes that the following prerequisites have been met:

- For each switch designated for TAP and SPAN aggregation, NX-OS is upgraded to the recommended version.
- The correct Cisco Plug-in for OpenFlow agent is downloaded and available in the bootflash memory of the switch.
- The management IP address is configured on the switch, and the switch can communicate with the server on which the Cisco Nexus Data Broker software will be installed.

The process to enable the Cisco Plug-in for OpenFlow consists of the following steps:

- Enable hardware support for Cisco Plug-in for OpenFlow.
- Install and activate Cisco Plug-in for OpenFlow.
- Configure Cisco Plug-in for OpenFlow.

Enabling Hardware Support for Cisco Plug-in for OpenFlow

Use the steps shown here to enable hardware support for Cisco Plug-in for OpenFlow and to enable the Cisco ONE™ Platform Kit (onePK™). You need to implement these steps on the Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switch that is part of the Cisco Nexus Data Broker solution. The deployment uses the topology shown in Figure 1.

Following are the configuration commands that need to be run on the Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switches.

Commands for Cisco Nexus 3000 and 3500 Series and Cisco Nexus 3100 and 9300 platform switches

- **enable**
- **configure terminal**
- **spanning-tree mode mst**
- **vlan 1-3967**
- **no spanning-tree vlan 1-3967**

If switch is a Cisco Nexus 3000 Series or Cisco Nexus 3100 platform:

- **hardware profile openflow**
- **hardware profile tcam region qos 0**
- **hardware profile tcam region racl 0**
- **hardware profile tcam region vacl 0**
- **hardware profile tcam region ifacl 1024 double-wide**

If switch is a Cisco Nexus 3500 Series:

- **hardware profile tcam region qos 0**
- **hardware profile tcam region racl 0**
- **hardware profile tcam region vacl 0**
- **hardware profile tcam region ifacl 1024 double-wide**
- **hardware profile forwarding-mode openflow-hybrid**

If switch is a Cisco Nexus 9300 platform:

- **hardware access-list tcam region qos 0**
- **hardware access-list tcam region vacl 0**
- **hardware access-list tcam region racl 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region ifacl 1024 double-wide**
- **hardware access-list tcam region openflow 512**

- **exit**
- **copy running-config startup-config**
- **reload**

Installing and Activating Cisco Plug-in for OpenFlow

Follow the steps shown here to install and activate the Cisco Plug-in for OpenFlow. This example assumes that the OpenFlow OVA filename is ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova, and that it is downloaded and available in the bootflash memory of the Cisco Nexus 3000 Series Switch.

- **enable**
- **virtual-service install name ofa package bootflash: ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova**

Use the following **show** command to check the status of the virtual-service installation:

- **show virtual-service list**

After the status of the virtual service becomes listed as “Installed,” run the following commands to activate the service:

- **configure terminal**

- **virtual-service ofa**
- **activate**
- **end**
- **copy running-config startup-config**

Use the **show virtual-service list** command to verify that the service status is changed to “Activated.” This change process may take up to 2 minutes.

Configuring the Cisco Plug-in for OpenFlow

To configure the Cisco Plug-in for OpenFlow, you need to configure OpenFlow ports, provide the Cisco Nexus Data Broker IP address, and associate the OpenFlow ports with the logical switch.

All the ports that will be enabled for OpenFlow need to be set as trunk ports. The configuration commands shown here need to be present for each OpenFlow-enabled interface (use interface ranges wherever applicable to configure multiple interfaces at the same time).

Commands for Cisco Nexus 3000 and 3500 Series and Cisco Nexus 3100 platform switches

- **enable**
- **configure terminal**
- **interface Ethernet 1/10-14, Ethernet1/41-45**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **end**
- **copy running-config startup-config**

To configure the OpenFlow logical switch, you need to provide the IP address and port information for Cisco Nexus Data Broker embedded and include the OpenFlow-enabled ports. In the Cisco Nexus Data Broker embedded configuration, use the Cisco Nexus 3000 Series Switch management interface IP address as the Cisco Nexus Data Broker IP address. This configuration example assumes that 10.10.10.10 is the management interface IP address of the Cisco Nexus 3000 Series Switch.

Commands for Cisco Nexus 3000 Series and Cisco Nexus 3100 and 9300 platform switches

- **openflow**
- **switch 1**
- **pipeline 201**
- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/10**
- **of-port interface ethernet1/11**
- **of-port interface ethernet1/12**
- **of-port interface ethernet1/13**
- **of-port interface ethernet1/14**
- **of-port interface ethernet1/41**
- **of-port interface ethernet1/42**
- **of-port interface ethernet1/43**
- **of-port interface ethernet1/44**
- **of-port interface ethernet1/45**
- **end**
- **copy running-config startup-config**

Commands for Cisco Nexus 3500 Series Switches

- **openflow**

- **switch 1**
- **default-miss cascade drop**
- **pipeline 203**
- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/10**
- **of-port interface ethernet1/11**
- **of-port interface ethernet1/12**
- **of-port interface ethernet1/13**
- **of-port interface ethernet1/14**
- **of-port interface ethernet1/41**
- **of-port interface ethernet1/42**
- **of-port interface ethernet1/43**
- **of-port interface ethernet1/44**
- **of-port interface ethernet1/45**
- **end**
- **copy running-config startup-config**

Enabling Configuration for Cisco Nexus 9300 Platform Switches for Cisco NX-API Mode

This section is applicable only if you choose to use the embedded option on Cisco Nexus 9300 platform switches in NX-API mode for TAP and SPAN aggregation.

This section assumes that the following prerequisites have been met:

- For each Cisco Nexus 9300 platform switch, NX-OS is upgraded to Cisco NX-OS Release 7.0(3)I2(1).
- The management IP address is configured on the switch, and the switch can communicate with the Cisco Nexus Data Broker server.

Before you can use Cisco Nexus Data Broker with Cisco Nexus 9300 platform switches, you must configure the following settings:

- Enable Link Layer Discovery Protocol (LLDP) and NX-API features and create VLANs in each switch.
- Configure ternary content-addressable memory (TCAM) settings.
- Save the configuration and reload the switch.

Enabling LLDP and Cisco NX-API on Each Switch

To enable the LLDP and NX-API features on the Cisco Nexus 9300 platform and to create the VLANs, use the configurations shown here for each switch.

- **enable**
- **configure terminal**
- **feature lldp**
- **feature nxapi**
- **spanning-tree mode mst**
- **vlan 1-3967**
- **no spanning-tree vlan 1-3967**
- **end**
- **copy running-config startup-config**

Configuring TCAM Settings

To reconfigure the TCAM allocation on the Cisco Nexus 9300 platform, use the commands shown here on each switch. These commands allocate 1024 rules for the IP access list and 512 for the MAC address list.

Note: For the TCAM reconfiguration to take effect, you need to reboot switch. You will reboot the switch at the end of the entire process.

- **enable**
- **configure terminal**
- **hardware access-list tcam region qos 0**
- **hardware access-list tcam region vacl 0**
- **hardware access-list tcam region racl 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region ifacl 1024 double-wide**
- **hardware access-list tcam region mac-ifacl 512**
- **end**
- **copy running-config startup-config**

Saving the Configuration and Reloading the Switches

For the hardware TCAM configuration changes to take effect, you need to reboot all the switches. Follow the steps shown here to save the configuration and reload the switch.

- **enable**
- **copy running-config startup-config**
- **reload**

Enabling Cisco Nexus Data Broker Embedded Solution on Cisco Nexus 3000 Series and Cisco Nexus 9300 Platform Switches

This section assumes that the following prerequisites have been met:

- On the Cisco Nexus 3000 Series and Cisco Nexus 9300 platform switch, the Cisco Nexus Data Broker embedded OVA file is downloaded and available in the bootflash memory.
- The management IP address is configured on the Cisco Nexus 3000 Series Switch.
- Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switch bootflash memory has at least 700 MB of free space.

Installing and Activating the Cisco Nexus Data Broker Embedded Solution

Follow the steps shown here to install and activate the Cisco Nexus Data Broker embedded solution on the Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switch. This example assumes that the Cisco Nexus Data Broker embedded file is ndb1000-sw-app-emb-k9-2.2.0.ova, and that it is downloaded and available in the bootflash memory of the Cisco Nexus switch.

Commands for Cisco Nexus 3000 and 3500 Series and Cisco Nexus 3100 and 9300 platform switches

- **enable**
- **virtual-service install name ndbemb package bootflash: ndb1000-sw-app-emb-k9-2.2.0.ova**

Use the following **show** command to check the status of the virtual-service installation:

- **show virtual-service list**

After the status of the virtual service becomes listed as “Installed,” run the following commands to activate the service:

- **configure terminal**
- **virtual-service ndbemb**
- **activate**
- **end**

- **copy running-config startup-config**

Use the **show virtual-service list** command to verify that the service status is changed to “Activated.” This change process may take up to 2 minutes.

Checking the Status of the Switch Connection to the Cisco Nexus Data Broker Embedded Solution

This step is applicable only if Cisco Nexus Data Broker embedded option is used with OpenFlow mode.

Use the **show** commands presented here to verify that the switch can connect to the Cisco Nexus Data Broker instance. If the switch is successfully connected to Cisco Nexus Data Broker, the “Connected” status should be listed as “Yes.”

- **show openflow switch 1 controllers**
- **show openflow switch 1 controllers stats**

Initial Cisco Nexus Data Broker Embedded Configuration

This section assumes that the Cisco Nexus Data Broker application is running. Bring up the Cisco Nexus Data Broker web GUI using one of the supported browsers listed here (see http://10.10.10.10:8080/monitor):

- Firefox 18.0 or later
- Google Chrome 24.0 or later

In this configuration example, the Cisco Nexus Data Broker embedded application is running on the Cisco Nexus 3000 Series Switch with management IP address 10.10.10.10.

Log into the GUI using the default credentials:

- Username: admin
- Password: admin

Device and Topology Discovery with Cisco Nexus 3000 Series and Cisco Nexus 9300 Platform Switches in OpenFlow Mode

In the Cisco Nexus Data Broker web GUI, switch to the management screen by choosing the Admin > Management option, which can be found in the upper-right corner.

After the switches are connected to Cisco Nexus Data Broker, they should be displayed in the topology, and the switch name with the OpenFlow port count should be displayed on the Nodes Learned tab on the left. After the switch is discovered and visible in the Cisco Nexus Data Broker GUI, change the switch setting to the proactive mode.

- On the Cisco Nexus Data Broker management menu bar, click Devices.
- On the Nodes Learned tab, in the Node Name column, click the link for the node that you want to rename.
- In the Update Node Information dialog box, complete the following fields:
  - Node Name: If you want to change the node name, update the Node Name field. The name can contain between 1 and 256 alphanumeric characters, including the following special characters: underscore _, hyphen -, plus sign +, equal sign =, opening parenthesis (, closing parenthesis), vertical bar |, and at sign @.
  - Operation Mode drop-down list: Select Proactive Forwarding Only. The following default flows are programmed on the switch:
    - Forward Address Resolution Protocol (ARP) packets to Cisco Nexus Data Broker.
    - Forward Link Layer Discovery Protocol (LLDP) packets to Cisco Nexus Data Broker.
    - Drop all other traffic.

To configure Cisco Nexus Data Broker so that it does not process any unrelated ARP requests, follow the steps shown here.

- On the Cisco Nexus Data Broker management menu bar, click Devices.
- On the Subnet Gateway Configuration tab, click Add Gateway IP Address.
- In the Add Gateway IP Address dialog box, complete the following fields:
  - Name: Dummy
  - Gateway IP Address/Mask: 1.1.1.10/24
    - For the gateway IP address and mask, be sure to use an IP address subnet that does not exist in your network.

You can also check the flow statistics through the Troubleshooting tab.

- On the Cisco Nexus Data Broker management menu bar, click Troubleshoot.
- On the Existing Nodes tab, locate the node for which you want to view statistics.
- Click the Flows link corresponding to the node to view detailed information about all flows programmed.

Device Discovery with Cisco Nexus 9300 Platform Switches in Cisco NX-API Mode

Change to the management screen by choosing the Admin > Management option in the upper-right corner of the screen.

You need to edit the Cisco Nexus 9300 platform switch to provide a username and password and set the connection mode to NX-API.

- On the Cisco Nexus Data Broker management menu bar, click Devices.
- On the Devices, click Device Connections.
- The Cisco Nexus 9000 Series Switch will be already available.
- Click the Edit button next to the switch name.
- In the pop-up window, provide the following information:
  - Username: Login user name that Cisco Nexus Data Broker should use to connect to the switch
  - Password: Password for the switch
  - Connection Type: NX-API
- Click Edit Device Connection to save the settings.

Cisco Nexus Data Broker Configuration

Cisco Nexus Data Broker configuration consists of the following steps:

- Configure port types and map monitoring tools.
- Configure filters to match traffic.
- Configure policies to forward traffic to various monitoring tools.

Access the Cisco Nexus Data Broker GUI at http://10.10.10.10:8080/monitor.

Configuring Port Types and Mapping Monitoring Tools

The Cisco Nexus Data Broker allows you to configure a variety of port types, including:

- Edge ports (SPAN or optical TAP)
- Delivery ports

Edge ports are the ingress ports through which traffic enters the monitoring network. Typically these are network TAP or SPAN ports. Cisco Nexus Data Broker supports the following edge ports:

- TAP port: An edge port for incoming traffic connected to a physical TAP wire
- SPAN port: An edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination

Note: The Edge-Tap and Edge-SPAN options are for classification within the Cisco Nexus Data Broker application only. They do not have any implications for traffic filtering and forwarding or require changes in any network configurations.

Optionally, you can also associate a VLAN with the ingress source port. All packets entering the source port will be tagged with that VLAN ID and can be used for input port identification.

Delivery ports are the egress ports through which the traffic exits the monitor network. These outgoing ports are connected to external monitoring and analysis tools. When you configure a monitoring device in Cisco Nexus Data Broker, you can associate a name and an icon and then associate these with the switch and the port to which the switch is connected.

Configured devices are displayed in the Monitor Devices table on the Devices tab. An icon appears in the topology diagram with a line connecting it to the node.

Configuring Edge Ports

In the configuration example here, each Cisco Nexus switch has five TAP ports. The steps for configuring the edge TAP port for Cisco Nexus switch are shown here.

In the topology diagram, click the Cisco Nexus 3000 or 3500 Series or Cisco Nexus 3100 platform switch to configure the ports.

Repeat the steps provided shown here for Ethernet ports 1/10 through 1/14:

- In the list of ports for the node, click Click to Configure for the port (for example, Ethernet 1/10).
- Click the Select a Port Type drop-down list and choose Edge-Tap.
- (Optional) Enter a description for the edge TAP port.
- (Optional) Enter the VLAN ID if you want to identify the input source port.
- Click Submit.

After configuring the edge TAP ports, click the Back button (highlighted in blue) at the top of the left pane.

Configuring Delivery Ports

The configuration example shown here uses a total of five monitoring tools (traffic analyzers). Here are the steps to map the monitoring tools to the switch and the port:

In the topology diagram, click the Cisco Nexus 3000 or 3500 Series or Cisco Nexus 3100 platform switch to configure the ports.

Repeat the steps shown here for Ethernet ports 1/41 through 1/45:

- In the list of ports for the node, click Click to Configure for the port (for example, Ethernet 1/41).
- Click Add Monitoring Device.
- In the Add Device dialog box:
  - Enter the device name.
  - Choose an icon to use for the monitoring device.
- Click Submit.

After configuring the edge TAP ports, click the Back button (highlighted in blue) at the top of the left pane.

Configuring Filters to Match Network Traffic

Filters are used to define the Layer 2, Layer 3, and Layer 4 criteria used by Cisco Nexus Data Broker to filter traffic. Traffic that matches the criteria in the filter is routed to the delivery ports to which the monitoring devices are attached.

In the configuration example, use the following steps if you want to create a filter to match all preconfigured interface traffic:

- On the Configure Filters tab, click Add Filter.
- In the Add Filter dialog box, enter:
  - Name: Match-All-Traffic
  - Layer 2 – Ethernet Type: Preconfigured Ether Types

  Leave all other values at the default settings.
- Click Add Filter.

In the configuration example, use the following steps if you want to create another filter to match all FTP traffic going to a certain destination IP address:

- On the Configure Filters tab, click Add Filter.
- In the Add Filter dialog box, enter:
  - Name: Match-FTP
  - Layer 3 – Destination IP Address: 10.17.44.3
  - Layer 3 – Protocol: TCP
  - Layer 4 – Destination Port: FTP (Data)

  Leave all other values at the default settings.
- Click Add Filter.

In the configuration example, use the following steps if you want to create another filter to match all User Data Protocol (UDP) traffic for a certain IP subnet with a certain destination IP address:

- On the Configure Filters tab, click Add Filter.
- In the Add Filter dialog box, enter:
  - Name: Match-FTP
  - Bidirectional: Select this option.
  - Layer 3 – Source IP Address: 22.22.22.0/24
  - Layer 3 – Destination IP Address: 10.17.44.13
  - Layer 3 – Protocol: UDP
  - Layer 4 – Destination Port: Select the Enter Destination Port option and enter **53** in the text box.

  Leave all other values at the default settings.
- Click Add Filter.

Connections are used to associate filters and monitoring tools. When connections are configured, Cisco Nexus switches are programmed to forward the matching traffic to the destination monitoring tools. Cisco Nexus Data Broker supports:

- Multipoint-to-multipoint (MP2MP) forwarding: With the MP2MP forwarding path option, the ingress edge port, through which SPAN or TAP traffic is entering the monitor network, and the egress delivery port both are defined. Cisco Nexus Data Broker uses the delivery ports to direct traffic from that ingress port to one or more devices.
- Any-to-multipoint (A2MP): With the A2MP forwarding path option, the ingress edge port of the monitor network is not known, but the egress delivery ports are defined. Cisco Nexus Data Broker automatically calculates a loop-free forwarding path from the root node to all other nodes using the Single-Source Shortest Path (SSSP) algorithm.

In the configuration example, use the following steps if you want to forward all interface traffic to Traffic Analyzer-1, Traffic Analyzer-3, and Traffic Analyzer-5:

- Click the Connections Setup.
- Click Add Connection and use the following parameters for creating the new rule:
  - Connection Name: Name the rule **Match-All-Traffic**.
  - Select Filter: Choose Match-All-Traffic from the drop-down list.
  - Select Destination Devices: Select Traffic-Analyzer-1, Traffic-Analyzer-3 and Traffic-Analyzer-5.
  - Select Source Node: Choose the Cisco Nexus switch from the drop-down list.
  - Select Source Port: Choose Ethernet1/10 from the drop-down list.
  - Click the Add Source Port button.
  - Select Source Port: Choose Ethernet1/11 from the drop-down list.
  - Click the Add Source Port button.
  - Select Source Port: Choose Ethernet1/12 from the drop-down list.
  - Click the Add Source Port button.
  - Select Source Port: Choose Ethernet1/13 from the drop-down list.
  - Click the Add Source Port button.
  - Select Source Port: Choose Ethernet1/14 from the drop-down list.
  - Click the Add Source Port button.
- Click Submit.

In the configuration example, use the following steps if you want to forward all UDP traffic to Traffic-Analyzer-2 and Traffic-Analyzer-4:

- Click the Connections Setup tab.
- Click Add Connection and use the following parameters for creating the new rule:
  - Rule Name: Name the rule **Match-UDP**.
  - Select Filter: Choose Match-UDP from the drop-down list.
  - Select Destination Devices: Select Traffic-Analyzer-2 and Traffic-Analyzer-4.
  - Select Source Node: Use the default settings.
  - Select Source Port: Use the default settings.
- Click Submit.

You can click the connection name to see the actual traffic-forwarding path for each rule.

Now verify that the two edge ports on the switch are receiving the traffic according to the filter that was applied. Observe the flow details using the Troubleshoot tab of the Cisco Nexus Data Broker Management UI.

- On the Cisco Nexus Data Broker topology page, click the switch.
- Click Node Statistics next to the device name.
- On the Existing Nodes tab, locate the node for which you want to view statistics.
- Click the Flows link corresponding to the node to view detailed information about all flows programmed.

Conclusion

Cisco Nexus Data Broker with Cisco Nexus switches can provide scalable, cost-effective, and efficient infrastructure for network traffic monitoring and visibility. With the capability of Cisco Nexus Family switches to operate in hybrid mode, customers can get additional value from their investments without any hardware capital expenditures. Customers can dedicate a few ports to monitoring purposes, with these ports controlled by Cisco Nexus Data Broker. All remaining ports can continue to be managed by the local control plane and can be used for production traffic. This approach allows customers to introduce new functions on existing data center networks without any significant changes to their infrastructure.

For More Information

For additional information, see:

- Cisco Plug-in for OpenFlow configuration guide: http://www.cisco.com/en/US/docs/switches/datacenter/sdn/configuration/openflow-agent-nxos.html.
- Cisco Nexus Data Broker configuration guide: http://www.cisco.com/c/en/us/support/cloud-systems-management/nexus-data-broker/products-installation-and-configuration-guides-list.html.
- Cisco Nexus 9000 Series Switches configuration guide: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-736164-00 11/15