Cisco Nexus Data Broker for Network Traffic Monitoring and Visibility

Solution Implementation Guide

Table of Contents

What You Will Learn

This document provides a quick-start configuration guide for the Cisco Nexus® Data Broker solution. This document includes steps for configuring:

- Cisco® Plug-in for OpenFlow on Cisco Nexus 3000 Series Switches and Cisco Nexus 9300 platform switches
- Cisco NX-API configuration on the Cisco Nexus 3000 and Cisco Nexus 9000 Series Switches
- Cisco Nexus Data Broker application

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

Cisco Nexus Data Broker 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 test access point (TAP) and Cisco Switched Port Analyzer (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.

Table 1 summarizes the main functions available with the Cisco Nexus Data Broker.

Table 1 Main Functions

Feature	Benefit
Support for a variety of port capacities	• The data broker supports 1-, 10-, 40-, and 100-Gbps ports. • The data broker supports high-density 10-, 40-, and 100-Gbps options using Cisco Nexus 9500 platform switches.
Supported topology for TAP and SPAN aggregation	• The data broker software discovers the Cisco Nexus switches and associated topology 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.
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 that can be spread across multiple Cisco Nexus switches. • You can configure the software to replicate and forward traffic to multiple monitoring tools that can be connected across multiple Cisco Nexus switches. • This solution is the only solution that supports any-to-many forwarding across a topology.
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.
Response to changes in the TAP and SPAN aggregation network state	• You can monitor and keep track of network condition changes. • You can respond to link or node failures by automatically reprogramming the flows through an alternative path.
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, including the path through the network.
Management for multiple disjointed Cisco Nexus Data Broker networks	• You can manage multiple independent TAP and SPAN aggregation networks using the same data broker instance.

*Feature supported on Cisco Nexus 3100 platform and Cisco Nexus 9000 Series.

**Feature supported only on Cisco Nexus 3500 Series.

Cisco Nexus Data Broker Solution Lab Setup

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

- Download the Cisco Nexus Data Broker Release 3.0.0 zip file from Cisco.com at https://software.cisco.com/download/release.html?mdfid=286281492&softwareid=286281554&release=3.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest&i=rm.
    - Filename: ndb1000-sw-app-k9-3.0.0.zip
- Verify that the following minimum system requirements are met for the server on which the Cisco Nexus Data Broker will be installed:
    - 8 virtual CPU cores at 2 GHz or higher

- At least 8 GB of memory
- At least 40 GB of free hard-disk space available on the partition on which you will be installing the Cisco Nexus Data Broker software
- A recent 64-bit Linux distribution that supports Java, such as:
  - Ubuntu Linux
  - Red Hat Enterprise Linux (RHEL)
  - Fedora Linux
- Java Virtual Machine (JVM) Release 1.8.0_45 or later
- **$JAVA_HOME** environment variable in your profile set to the path of the JVM
- Python Release 2.7.3 to support the backup and restore script

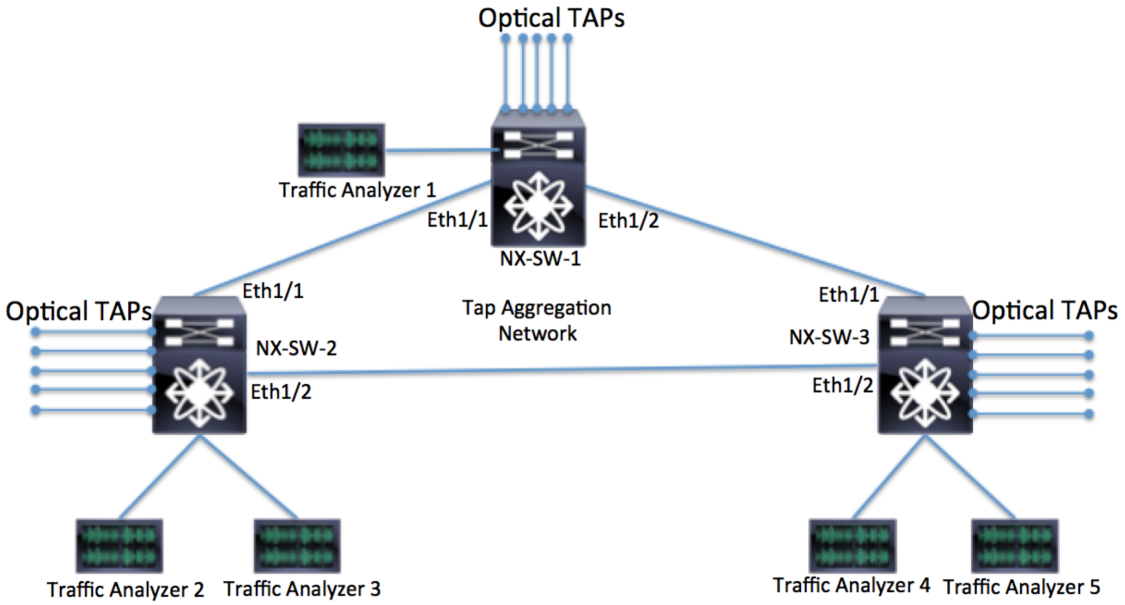
- Copy the Cisco Nexus Data Broker application zip file to a directory; then extract the file.
- From the xnc/ directory, start the controller using the script **runxnc.sh** as shown here.

```
$ runxnc.sh –start
```

- 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(3)
    - Cisco NX-OS Release 7.0(3)I2(2a)
  - For Cisco Nexus 3200 platform switches, use Cisco NX-OS Release 7.0(3)I3(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(5).
  - For each Cisco Nexus 9300 or 9500 platform switch, upgrade NX-OS to Cisco NX-OS Release 7.0(3)I2(2a).

Figure 1 shows the monitoring network (TAP aggregation) topology used in the configuration steps in this document. In this topology, three Cisco Nexus switches are connected in a full mesh. Five TAPs are connected to each switch (15 TAPs total), and five monitoring devices (traffic analyzers) are connected across these three Cisco Nexus switches.

Figure 1 Monitoring Network Topology



- Connect optical TAPs to Ethernet ports 1/10 through 1/14 on each switch.
- Connect traffic analyzer devices to Ethernet ports 1/47 and 1/48 on Cisco Nexus switches 1 and 2 (NX-SW-1 and NX-SW-2), and to Ethernet port 1/48 on NX-SW-1.

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

You first need to download the Cisco Plug-in for OpenFlow from Cisco.com. Download the version of the OpenFlow plug-in that matches your version of NX-OS.

For Cisco NX-OS Release 6.0(2)X, download the Cisco Plug-in for OpenFlow Release 1.1.5 from Cisco.com and copy it to the bootflash memory.

- http://software.cisco.com/download/release.html?mdfid=286022046&flowid=49382&softwareid=286195315&release=1.1.5&relind=AVAILABLE&rellifecycle=&reltype=latest

For Cisco NX-OS Release 7.0(3)I2(2a) or 7.0(3)I3(1), download the Cisco Plug-in for OpenFlow Release 2.1.3 from Cisco.com and copy it to the bootflash memory.

- https://software.cisco.com/download/release.html?mdfid=286022046&flowid=&softwareid=286195315&release=2.1.3&relind=AVAILABLE&rellifecycle=&reltype=latest

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.

Enabling the Cisco Plug-in for OpenFlow consists of the following steps:

- Enable hardware support for the plug-in.
- Install and activate the plug-in.
- Configure the plug-in.

Enabling Hardware Support for Cisco Plug-in for OpenFlow

The following section presents the steps for enabling hardware support for the Cisco Plug-in for OpenFlow. You need to implement these steps on all Cisco Nexus 3000 Series or Cisco Nexus 9300 platform switches that are part of the TAP aggregation environment.

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

NX-SW-1

- **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 3200 Series:

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 256 double-wide**
- **hardware access-list tcam region openflow 256**

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**

NX-SW-2

- **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 3200 Series:

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 256 double-wide**
- **hardware access-list tcam region openflow 256**

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**

NX-SW-3

- **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 3200 Series:

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 256 double-wide**
- **hardware access-list tcam region openflow 256**

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 presented here to install and activate the Cisco Plug-in for OpenFlow. Use the appropriate filename depending on the version that was downloaded to the bootflash memory.

This example assumes that the OpenFlow open virtualization appliance (OVA) filename is ofa-1.1.5-r3-n3000-SPA-k9.ova, and that it is downloaded and available in the bootflash memory of each Cisco Nexus 3000 Series Switch. Same steps apply for OpenFlow agent version 2.1.0 or 2.1.3. Only the OpenFlow agent filename will be different.

NX-SW-1

- **enable**
- **virtual-service install name ofa package bootflash: ofa-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 two minutes.

NX-SW-2

- **enable**
- **virtual-service install name ofa package bootflash:ofa-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 two minutes.

NX-SW-3

- **enable**
- **virtual-service install name ofa package bootflash:ofa-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 two 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 (to which the controller connects), 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.)

NX-SW-1

- **enable**
- **configure terminal**
- **interface ethernet 1/1-2, ethernet1/10-14, ethernet1/48**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **end**
- **copy running-config startup-config**

NX-SW-2

- **enable**
- **configure terminal**
- **interface ethernet 1/1-2, ethernet1/10-14, ethernet1/47-48**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **end**
- **copy running-config startup-config**

NX-SW-3

- **enable**
- **configure terminal**
- **interface ethernet 1/1-2, ethernet1/10-14, ethernet1/47-48**
- **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 the Cisco Nexus Data Broker and include the OpenFlow-enabled ports. This quick-start configuration assumes that Transport Layer Security (TLS) is not required. If TLS is required, see the "For More Information" section at the end of this document for configuration guides. In this configuration example, 10.10.10.10 is the IP address of the Cisco Nexus Data Broker server.

NX-SW-1

- **openflow**
- **switch 1**

If the switch is a Cisco Nexus 3000 Series or Cisco Nexus 3100 or Cisco Nexus 3200 or Cisco Nexus 9300 platform:

- **pipeline 201**

If the switch is a Cisco Nexus 3500 Series:

- **pipeline 203**

- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/1**
- **of-port interface ethernet1/2**
- **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 ethernet1/48**
- **end**
- **copy running-config startup-config**

NX-SW-2

- **openflow**
- **switch 1**

If the switch is a Cisco Nexus 3000 Series or Cisco Nexus 3100 or Cisco Nexus 3200 or Cisco Nexus 9300 platform:

- **pipeline 201**

If the switch is a Cisco Nexus 3500 Series:

- **pipeline 203**

- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/1**
- **of-port interface ethernet1/2**
- **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 ethernet1/47**
- **of-port interface ethernet1/48**
- **end**
- **copy running-config startup-config**

NX-SW-3

- **openflow**
- **switch 1**

If the switch is a Cisco Nexus 3000 Series or Cisco Nexus 3100 or Cisco Nexus 3200 or Cisco Nexus 9300 platform

- **pipeline 201**

If the switch is a Cisco Nexus 3500 Series:

- **pipeline 203**

- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/1**
- **of-port interface ethernet1/2**
- **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 ethernet1/47**
- **of-port interface ethernet1/48**
- **end**
- **copy running-config startup-config**

Checking the Status of Switch Connection to Cisco Nexus Data Broker

Use the following **show** commands to verify that the switch can connect to the Cisco Nexus Data Broker. This example assumes that the data broker is already started and running. It also assumes that if a firewall exists between the switches and the Cisco Nexus Data Broker server, all necessary ports are open.

If the switch is successfully connected to the controller, the "Connected" status should be listed as "Yes."

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

Prerequisite Configuration for Cisco Nexus 3000 series and Cisco Nexus 9000 Series Switches in Cisco NX-API Mode

This section is applicable only if you choose to use Cisco Nexus 9000 Series 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 or 9500 platform switch, NX-OS is upgraded to Cisco NX-OS Release 7.0(3)I2(2a).
- 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 3000 and Cisco Nexus 9000 Series Switches, you must configure the following settings:

- Enable Link Layer Discovery Protocol (LLDP) and NX-API features and also create VLANs in each switch.
- Configure ternary content-addressable memory (TCAM) settings.
- Configure trunk mode on all Inter-Switch Links (ISLs).
- 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 3000 and Cisco Nexus 9000 Series, use the configurations shown here for each switch.

NX-SW-1

- **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**

NX-SW-2

- **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**

NX-SW-3

- **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 9000 Series, 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.

NX-SW-1

- **enable**
- **configure terminal**

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

- **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 3200 Series:

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 512**
- **hardware access-list tcam region mac-ifacl 256**

If switch is a Cisco Nexus 9300 and Cisco Nexus 3164 switches:

- **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**

If switch is a Cisco Nexus 9500 series switches:

- **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 256**

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

NX-SW-2

- **enable**
- **configure terminal**

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

- **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 3200 Series:

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**

- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 512**
- **hardware access-list tcam region mac-ifacl 256**

If switch is a Cisco Nexus 9300 and Cisco Nexus 3164 switches:

- **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**

If switch is a Cisco Nexus 9500 series switches:

- **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 256**
- **end**
- **copy running-config startup-config**

NX-SW-3

- **enable**
- **configure terminal**

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

- **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 3200 Series:

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 512**
- **hardware access-list tcam region mac-ifacl 256**

If switch is a Cisco Nexus 9300 and Cisco Nexus 3164 switches:

- **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**

If switch is a Cisco Nexus 9500 series switches:

- **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 256**
- **end**
- **copy running-config startup-config**

Configuring Trunk Mode for ISLs

All the ISLs need to be configured in trunk mode to enable the traffic to pass through. Use the configuration shown here to enable trunk mode on the ISLs.

NX-SW-1

- **enable**
- **configure terminal**
- **interface ethernet 1/1-2**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **end**
- **copy running-config startup-config**

NX-SW-2

- **enable**
- **configure terminal**
- **interface ethernet 1/1-2**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **end**
- **copy running-config startup-config**

NX-SW-3

- **enable**
- **configure terminal**
- **interface ethernet 1/1-2**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **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.

NX-SW-1
- **enable**
- **copy running-config startup-config**
- **reload**

NX-SW-1
- **enable**
- **copy running-config startup-config**
- **reload**

NX-SW-1
- **enable**
- **copy running-config startup-config**
- **reload**

Device Settings and Topology Discovery in Cisco Nexus Data Broker

This section assumes that the Cisco Nexus Data Broker is running. Bring up the data broker web GUI using one of the supported browsers listed at this web address: https://10.10.10.10:8443/monitor . In this configuration example, the data broker is running on a server with IP address 10.10.10.10.

- Mozilla Firefox 18.0 or later
- Google Chrome 24.0 or later

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

Go to Administration screen by clicking on the "Administration" tab on the top.

After the switches are connected to the Cisco Nexus Data Broker, they should be displayed in the Devices->Nodes Learned tab. The monitoring topology may not be discovered yet. For the data broker to discover the topology, the switches must be set to proactive mode.

Repeat the steps that follow for all three switches (NX-SW-1, NX-SW-2, and NX-SW-3).

-
- 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 the data broker.
        - Forward Link LLDP packets to the data broker.
        - Drop all other traffic.

It may take a few minutes for the network topology to be discovered and displayed in the Cisco Nexus Data Broker's management GUI.

You can also check the flow statistics on the Troubleshoot 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 and Topology Discovery with Cisco Nexus 9000 Series Switches in NX-API Mode

Go to Administration screen by clicking on the "Administration" tab on the top.

You need to add the Cisco Nexus 3000 or Cisco Nexus 9000 Series Switches to the Cisco Nexus Data Broker using the IP address, username, and password. To set the switches to NX-API mode, follow the steps shown here.

Repeat the steps for each switch.

- Click on the Devices options on the left hand side pane.
- On the Devices, click Device Connections tab.
- Click Add Device.
- In the pop-up window, provide the following information:
    - Address: Management IP address of the Cisco Nexus 9000 Series Switch
    - 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 Add Device.

If the connection is successful, the switches will be discovered along with the ISLs, and the topology will be displayed in the Cisco Nexus Data Broker GUI.

Cisco Nexus Data Broker Application Configuration

The 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 the traffic to various monitoring tools.

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

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 or analysis tools. When you configure a monitoring device in the 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. The icon appears in the topology diagram with a line connecting it to the node.

Configuring Edge Ports

In the following configuration example, each Cisco Nexus switch has five TAP ports. Go the Cisco Nexus Data Broker page using the URL http://10.10.10.10:8443/monitor. The steps for configuring the edge TAP port for each Cisco Nexus switch are shown here.

In the topology diagram, click the NX-SW-1 device to configure the ports. Only ports that are not ISLs are displayed.

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, ethernet1/10).
- 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.

In the topology diagram, click the NX-SW-2 device to configure the ports. Only ports that are not ISLs are displayed.

Repeat the steps 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, ethernet1/10).
- 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.

In the topology diagram, click the NX-SW-3 device to configure the ports. Only ports that are not ISLs are displayed.

Repeat the steps 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, ethernet1/10).
- 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.

Configuring Delivery Ports

The configuration example shown here uses a total of five monitoring tools (traffic analyzers):

- One tool connected to NX-SW-1 on Ethernet port 1/48
- Two tools connected to NX-SW-2 on Ethernet ports 1/47 and 48
- Two other tools connected to NX-SW-3 on Ethernet ports 1/47 and 48

Following are the steps to map the monitoring tools to the switch and the port.

In the topology diagram, click the NX-SW-1 device to configure the ports.

- In the list of ports for the node, click Click to Configure for Ethernet port 1/48.
- Click Add Monitoring Device.
- In the Add Device dialog box:
  - Enter the device name.
  - Select the switch name
  - Select the port to which it is connected
  - Choose an icon to use for the monitoring device.
- Click Submit.

In the topology diagram, click the NX-SW-2 device to the configure ports.

Repeat the steps shown here for Ethernet ports 1/47 and 1/48.

- In the list of ports for the node, click Click to Configure for the port (for example, ethernet1/47).
- Click Add Monitoring Device.
- In the Add Device dialog box:
    - Enter the device name.
    - Select the switch name
    - Select the port to which it is connected
    - Choose an icon to use for the monitoring device.
- Click Submit.

In the topology diagram, click the NX-SW-3 device to configure the ports.

Repeat the steps shown here for Ethernet ports 1/47 and 1/48.

- In the list of ports for the node, click Click to Configure for the port (for example, ethernet1/47).
- Click Add Monitoring Device.
- In the Add Device dialog box:
    - Enter the device name.
    - Select the switch name
    - Select the port to which it is connected
    - Choose an icon to use for the monitoring device.
- Click Submit.

Configuring Filters to Match Network Traffic

Filters are used to define the Layer 2, Layer 3, and Layer 4 criteria used by the 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 this 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.

- Click “Filters” in the left hand pane , click Add Filter.
- In the Add Filter dialog box, specify:
    - 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 this configuration example, use the following steps if you want to create another filter to match all User Datagram Protocol (UDP) traffic for a certain IP subnet with a certain destination IP address.

- Click “Filters” in the left hand pane, click Add Filter.
- In the Add Filter dialog box, specify:
    - Name: Match-UDP
    - 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 rules are configured, Cisco Nexus switches are programmed to forward the matching traffic to the destination monitoring tools. The Cisco Nexus Data Broker solution supports:

- Multipoint-to-multipoint (MP2MP) forwarding: With the MP2MP forwarding path option, the ingress edge port, through which SPAN or TAP traffic enters the monitor network, and the egress delivery port both are defined. The 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 this configuration example, use the following steps if you want to forward all HTTP traffic to Traffic Analyzer 1, Traffic Analyzer 3, and Traffic Analyzer 5.

- Click “Connections” on the left hand pane.
- Click New Connection and use the following parameters for creating the new rule:
    - Connection Name: Name the rule **Match-all**.
    - Select Filter: Choose Default-Match-All from the drop-down list.
    - Select Destination Devices: Select Traffic Analyzer 1, Traffic Analyzer 3, and Traffic

Analyzer 5.

- Select Source Node: Choose NX-SW-1 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.

- Click Submit.

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

- Click "Connections" on the left hand pane.
- Click New Connection and use the following parameters for creating the new rule:
  - Connection 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 a connection name to see the actual traffic-forwarding path for each rule. The path will be displayed in a new window.

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 "Statistics" page on the left side pane.

- Click "Statistics" on the left side pane.
- Select a switch name from the drop down box
- By default Flow statistics page displayed
- You can go to port statistics by clicking "Ports" tab next to "Flows" tab.

Conclusion

The Cisco Nexus Data Broker with Cisco Nexus switches can provide scalable, cost-effective, and efficient infrastructure for monitoring and viewing network traffic. With the capability of Cisco Nexus Family switches to operate in hybrid mode, customers can get additional value from their investments without any new hardware capital expenditures. Customers can dedicate a few ports to monitoring purposes, with these ports controlled by the 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 into 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