Cisco Nexus Data Broker Overview

This chapter contains the following sections:

About Cisco Nexus Data Broker

Visibility into application traffic has traditionally been important for infrastructure operations to maintain security, troubleshooting, and compliance and perform resource planning. With the technological advances and growth in cloud-based applications, it has become imperative to gain increased visibility into the network traffic. Traditional approaches to gain visibility into network traffic are expensive and rigid, making it difficult for managers of large-scale deployments.

Cisco Nexus Data Broker with Cisco Nexus Switches provides a software-defined, programmable solution to aggregate copies of network traffic using Switched Port Analyzer (SPAN) or network Test Access Point (TAP) for monitoring and visibility. As opposed to traditional network taps and monitoring solutions, this packet-brokering approach offers a simple, scalable and cost-effective solution that is well-suited for customers who need to monitor higher-volume and business-critical traffic for efficient use of security, compliance, and application performance monitoring tools.

With the flexibility to use a variety of Cisco Nexus Switches and the ability to interconnect them to form a scalable topology provides the ability to aggregate traffic from multiple input TAP or SPAN ports, and replicate and forward traffic to multiple monitoring tools which may be connected across different switches. Combining the use of Cisco plugin for OpenFlow and the Cisco NX-API agent to communicate to the switches, Cisco Nexus Data Broker provides advance features for traffic management.

Cisco Nexus Data Broker provides management support for multiple disjointed Cisco Nexus Data Broker networks. You can manage multiple Cisco Nexus Data Broker topologies that may be disjointed using the same application instance. For example, if you have 5 data centers and want to deploy an independent Cisco Nexus Data Broker solution for each data center, you can manage all 5 independent deployments using a single application instance by creating a logical partition (network slice) for each monitoring network.

Starting with Cisco NDB release 3.6, when a new switch is discovered on NDB, the following connections are installed on the ISL interfaces:

- Default-Deny-ISL connection with Default-Deny-All, Default-Deny-MPLS, and Default-Deny-ARP filters. This connection is supported on all the types of switches in NXAPI mode.
- Default-Deny-ISL-ICMP connection with Default-Deny-ICMP and Default-Deny-ICMP-All filters. This connection is supported on 9200, 9300EX, 9300FX, 9500EX, and 9500FX switches in NXAPI mode.

All the ACLs related to the default filters are installed on the ISL interfaces of the new switch. By default, this feature is enabled for all the new ISL interfaces.

Starting with Cisco Nexus Data Broker, Release 3.8:

- Add newly supported feature list.

Note You can configure a maximum of 30 unique Port ACLs (PACLs) for the Cisco Nexus 9300 FX Platform.

Note Each PACL takes one label. If the same PACL is configured on multiple interfaces, the same label is shared. If each PACL has unique entries, the PACL labels are not shared, and the label limit is 30.

Note You can manage this feature using the mm.addDefaultISLDenyRules attribute in config.ini file. By default, themm.addDefaultISLDenyRules attribute is not be present in config.in file. To disable this feature, you need to add the mm.addDefaultISLDenyRules attribute to config.ini file ans set it to false and restart the device. For example:

```
mm.addDefaultISLDenyRules = false
```

Note A Cisco Nexus Data Broker instance can support either the OpenFlow or NX-API device configuration mode, it does not support both device types.

Note Starting with Cisco NDB release 3.6, Global ACLs are automatically added to all the interfaces on a device. By default, Global ACLs are enabled for a device. To manage Global ACLs, you need to add the configure.global.acls parameter in the config.ini file. Set the configure.global.acls parameter to *false* and restart the device to disable Global ACLs on the device.

Note Starting with Cisco NDB release 3.6, constistency check option is now available for NX-API based devices along with the OpenFlow based devices.

Note Starting with Cisco NDB Release 3.4, you can configure the timeout interval for NDB GUI. By default, a user is logged out if the session is inactive for more than 10 minutes. You can configure the inactive timeout interval by modifying the timeout interval attribute in the *xnc/configuration/web.xml* file. You need to restart the NDB to apply the new interval.

Note Starting with Cisco NDB Release 3.6.2, you can now configure the inactivity timeout interval in NDB GUI instead of updating the *xnc/configuration/web.xml* file. By default, a user is logged out if the session is inactive for more than 10 minutes. You need to re-log in to the NDB to apply the new interval. For more information, see *Configuring Inactivity Timeout* section. .

Note Starting with Cisco Nexus Data Broker, Release 3.3:

- Advanced filtering based on TCP AND UDP flags is supported to filter the traffic.
- IPv6, QinQ, and UDF are supported for NX-OS I6 release platform.
- You can define a User Defined Filter (UDF) and use it while creating a filter for traffic management.
- Edit Priority field for the connections is configurable. By default, edit is enabled for the Cisco NDB administrator role.

Note Starting with Cisco NDB release 3.2.2, IPv6 addressing is supported in centralized mode. You can configure NDB to use either IPv6 addressing or both IPv4 and IPv6 addressing. Set `ipv6.strict` attribute in config.ini file to *true* to make NDB accessible only through IPv6 address. If you set the `ipv6.strict` attribute to *false*, you can access NDB through IPv4 or IPv6 address.

Note Starting with Cisco Nexus Data Broker Release 3.1, the user strings for Cisco Nexus Data Broker can contain alphanumeric characters including the following special characters: period (.), underscore (_), or hyphen (-) . These are the only special characters that are allowed in the user strings.

Note The hostname string for Cisco Nexus Data Broker can contain between 1 and 256 alphanumeric characters including the following special characters: period (.), underscore (_), or hyphen (-) . These are the only special characters that are allowed in the user strings.

Note Nexus 3548 does not support Block-Tx feature.

Cisco Nexus Data Broker provides the following:

- Support for the OpenFlow mode or the NX-API mode of operation.

Note The OpenFlow mode and the NX-API mode are supported on both Cisco Nexus 3000 Series and Cisco Nexus 9000 Series switches. Cisco Nexus 9500, 9200, and 9300-EX switches support only NX-API mode of deployment. Cisco Nexus 3500 supports only Openflow mode of deployment. You can enable only one mode, either OpenFlow or NX-API mode, at a time.

You can enable only one mode, either OpenFlow or NX-API mode, at a time.

When using OpenFlow mode, NX-API is available for auxiliary configurations only, for example, Enabling Q-in-Q on the SPAN and TAP ports.

Cisco Nexus 9300-EX Series switches support only Cisco NX-OS Release 7.0(3)I5(1) and later releases.

The configuration that is supported in the AUX mode is:

- Pull and push of interface description
- Q-in-Q configuration
- Redirection
- Port Channel load balancing
- MPLS Stripping

Note Starting with Cisco Nexus 3000 Release 7.x, the NX-API configuration is supported on the following Cisco Nexus Series switches:

- Cisco Nexus 3172 switches
- Cisco Nexus 3132 switches
- Cisco Nexus 3164 switches
- Cisco Nexus 31128 switches
- Cisco Nexus 3232 switches
- Cisco Nexus 3264 switches
- Cisco Nexus 3100-V switches

- The features that are supported with the Cisco Nexus 9500 Series switches are:
  - The NX-API feature is supported. (OpenFlow is not supported.)
  - The MPLS strip feature is supported.
  - The label age CLI feature is not supported.

- Support for Layer-7 filtering for the HTTP traffic using the HTTP methods.
- Support for VLAN filtering.
- Support for MPLS tag strippng.
- A scalable topology for TAP and SPAN port aggregation.
- Support for Q-in-Q to tag input source TAP and SPAN ports.
- Symmetric load balancing.
- Rules for matching monitoring traffic based on Layer 1 through Layer 4 information.
- The ability to replicate and forward traffic to multiple monitoring tools.
- Time stamping using Precision Time Protocol (PTP).
- Packet truncation beyond a specified number of bytes to discard payload.
- Reaction to changes in the TAP/SPAN aggregation network states.
- Security features, such as role-based access control (RBAC), and integration with an external Active Directory using RADIUS, TACACS, or LDAP for authentication, authorization, and accounting (AAA) functions.
- End-to-end path visibility, including both port and flow level statistics for troubleshooting.
- Robust Representational State Transfer (REST) API and a web-based GUI for performing all functions
- Support for Cisco plugin for Open Flow, version 1.0
- Cisco Nexus Data Broker adds NX-API plugin to support Cisco Nexus 9000 Series switches as TAP/SPAN aggregation. The NX-API supports JSON-RPC, XML, and JSON. Cisco Nexus Data Broker interacts with Cisco Nexus 9000 Series using the NX-API in JSON message formats.
- Beginning with Cisco Nexus Data Broker, Release 3.1, Cisco Nexus Data Broker is certified with Cisco Nexus 9200 Series and Cisco Nexus 9300-EX Series switches.

  The following features are supported on the Cisco Nexus 9300-EX, -FX, -FX2 Series switches:

  - Symmetric Load Balancing
  - Q-in-Q
  - Switch Port Configuration
  - MPLS Stripping
  - BlockTx
  - Truncate

- Beginning with Cisco Nexus Data Broker, Release 3.1, Cisco Nexus Data Broker is shipped with a certificate for the HTTPS connection between the Cisco Nexus Data Broker and a browser. Now with this feature, you can change to a different certificate than the shipped certificate.

  The script **generateWebUIcertificate.sh** is available in the **xnc/configuration** folder. If you execute this script, it moves the shipped certificate to **old_keystore** and the new certificate is generated in **keystore**. On the next Cisco Nexus Data Broker restart, this new certificate is used.

With Cisco Nexus Data Broker, you can:

- Classify Switched Port Analyzer (SPAN) and Test Access Point (TAP) ports.
- Integrate with Cisco ACI through Cisco APIC to configure SPAN destinations and SPAN sessions.
- Add monitoring devices to capture traffic.
- Filter which traffic should be monitored.
- Redirect packets from a single or multiple SPAN or TAP ports to multiple monitoring devices through delivery ports.
- Restrict which users can view and modify the monitoring system.
- If Cisco Nexus 9000 Series switch is using 7.0(3)I4(1) or later version in NX-API mode and if a flow is installed using a VLAN filer, then the device goes through an IP access list and it does not match on the Layer 2 packet.
- Configure these additional features, depending upon the type of switch:
  - Enable MPLS Tag stripping.
  - Set VLAN ID on Cisco Nexus 3000 Series switches.
  - Symmetric load balancing on Cisco Nexus 3100 Series switches and Cisco Nexus 9000 Series switches.
  - Q-in-Q on Cisco Nexus 3000 Series switches, 3100 Series switches, and Cisco Nexus 9000 Series switches.
  - Timestamp tagging and packet truncation on Cisco Nexus 3500 Series switches.
  - You can now configure the **watchdog_timer** configuration parameter in the **config.ini** file. If the value of the parameter is set to 0, the watchdog timer functionality is not available. The value of 30 seconds is a minimum value of the parameter and if the value of the parameter is set to a value more the 30 seconds, the watchdog timer monitors the JAVA process for the configured time interval.

Supported Web Browsers

The following Web browsers are supported for Cisco Nexus Data Broker Embedded:

- Firefox 45.x and later versions
- Chrome 45.x and later versions
- Internet Explorer 11 and later versions
- Microsoft Edge 42 or later versions.

Note JavaScript 1.5 or a later version must be enabled in your browser.

Prerequisites for Cisco Nexus Series Switches

Cisco Nexus Data Broker is supported on Cisco Nexus 3000, 3100, 3200, 3500, and 9000 series switches. Before you deploy the software, you must do the following:

- Ensure that you have administrative rights to log in to the switch.
- Verify that the management interface of the switch (mgmt0) has an IP address configured using the **show running-config interface mgmt0** command.
- Ensure that the switch is in Multiple Spanning Tree (MST) mode. You can use **spanning-tree mode mst** command to enable MST mode on a switch.
- Add the VLAN range in the database that is to be used in Cisco Nexus Data Broker for tap aggregation and inline monitoring redirection to support VLAN filtering. For example, the VLAN range is <1-3967>.
- Ensure that the spanning tree protocol is disabled for all the VLANs. You can use the **no spanning-tree vlan 1-3967** to disable spanning tree on all the VLANs.
- For the first NDB deployment with NXOS version 9.2(1), ensure that the **feature nxapi** and **nxapi http port 80** commands are configured on the NDB switch. If you upgrading NDB switch from NXOS version I7(x) to 9.2(1), the **feature nxapi** and **nxapi http port 80** configurations are not required.

For running the OpenFlow and NX-API mode on the Cisco Nexus Series switches, see the following pre-requisites.

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

Note The TCAM configurations are based on the type of filters required. You may configure multiple TCAM entries from a specific region based on the network requirement. For example, *ing-ifacl* is the TCAM region to cater MAC, IPv4, IPv6 filters in case of N93180YC-E. You may configure multiple TCAM from this region to fit more filtering ACL TCAM entries.

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 3000 Series switches	Enter the **# hardware profile openflow** command at the prompt.	

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 3164Q, 3132Q switches	Enter the **# hardware profile openflow** command at the prompt. **Note** The OpenFlow mode is not supported on the Nexus 3164Q switches.	Enter the following commands at the prompt: • **# 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 access-list tcam region mac-ifacl 512** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 3172 Series switches	Enter the **# hardware profile openflow** command at the prompt.	Use the **hardware profile mode tap-aggregation** [**l2drop**] CLI command to enable tap aggregation and to reserve entries in the interface table that are needed for VLAN tagging. The l2drop option drops non-IP traffic ingress on tap interfaces.

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 3200 Series switches	Enter the **hardware access-list tcam region openflow 256** command at the prompt.	Enter the following commands at the prompt: • **# 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 mac-ifacl 512** • **# hardware access-list tcam region ipv6-ifacl 256** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 3500 series switches	Enter either of the following commands at the prompt to configure OpenFlow TCAM: • **# hardware profile forwarding-mode openflow-hybrid** • **#hardware profile forwarding-mode openflow-only**	

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 9300 Series switches	Enter the **hardware access-list tcam region openflow 512 double-wide** command at the prompt to configure the MAC filters. For IPv4 and IPv6, enter the **hardware access-list tcam region openflow 512** command. **Note** IPv6 and IPv4 dual stack is not supported in I6 and I7.	Enter the following commands at the prompt: • **# 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** • **# hardware access-list tcam region ipv6-ifacl 512** • **#feature nxapi** • **#feature lldp**

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 9200, 9300-EX, 9336C-FX2, and 93240YC-FX2 switches	The OpenFlow mode is not supported on the 9200, 9300-EX, 9336C-FX2, and 93240YC-FX2 switches.	Enter the following commands at the prompt: • **#hardware access-list tcam region ing-l2-span-filter 0** (For Cisco Nexus 93108 series switch only) • **#hardware access-list tcam region ing-l3-span-filter 0** (For Cisco Nexus 93108 series switch only) • **# hardware access-list tcam region ing-racl 0** • **hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 9500-EX and 9500-FX Series switches	The OpenFlow mode is not supported on the Cisco Nexus 9500-EX and 9500-FX Series switches.	Enter the following commands at the prompt: • **# hardware access-list tcam region ing-racl 0** • **# hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024** • **#feature nxapi** • **#hardware acl tap-agg** • **#feature lldp**

Cisco Nexus Data Broker Software Release Filename Matrix

See the Cisco Nexus Data Broker software release filename matrix for more information on the software images:

Mode of Deployment	NXOS Image	Mode	File Name
Embedded	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	NXAPI	`ndb1000-sw-app-emb-i6-plus-k9-3.9.0.zip`
Embedded	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	OpenFlow	`ndb1000-sw-app-emb-i6-plus-k9-3.9.0.zip`
Embedded	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	NXAPI	`ndb1000-sw-app-emb-nxapi-3.9.0-k9.zip`

Mode of Deployment	NXOS Image	Mode	File Name
Embedded	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	Openflow	ndb1000-sw-app-emb-3.9.0-ofa_mmemb-2.1.4-r2-nxos-SPA-k9.zip
Embedded	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	Openflow	ndb1000-sw-app-emb-3.9.0-ofa_mmemb-1.1.5-r3-n3000-SPA-k9.zip
Centralized	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	NXAPI	ndb1000-sw-app-k9-3.9.0.zip
Centralized	7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(7), 9.2(1) to 9.2(4), 9.3(1) to 9.3(4)	OpenFlow	ndb1000-sw-app-k9-3.9.0.zip

Nexus Data Broker Hardware and Software Interoperability Matrix

See Cisco Nexus Data Broker Release Notes, Release 3.9 for the latest matrix.

Python Activator Scripts for NX-OS Images

The following table lists the Python Activator scripts and corresponding NX-OS Image names:

Note The activator scripts are availble for download at: https://github.com/datacenter/nexus-data-broker.

Note Check the Guestshell version using the **show guestshell** command. If the Guestshell version is 2.2 or earlier, either upgrade the Guestshell or destroy and re-run the script to start NDB embedded.

Table 1: Python Activator Scripts for NX-OS Images

Python activator script file name	NX-OS Image
NDBActivator2.0_A6_A8_Plus.py	Cisco NXOS versions A6 and A8
NDBActivator2.0_I3_I4.py	Cisco NXOS versions I3 and I4
NDBActivator3.0_I5_Plus.py	Cisco NXOS version I5 and above.