Nexus Data Broker Openflow Mode & its Limitations

Contents

Introduction

Cisco Nexus Data Broker (NDB) offers a simple, scalable, cost-effective solution for monitoring high-volume and business-critical traffic. Visibility into this traffic is critical to maintaining security, supporting troubleshooting, helping ensure compliance, and perform resource planning. This software-defined packet broker approach is available for Cisco Nexus 3000 and 9000 series data center switches.

NDB Features

Monitor Network Traffic

Visibility into application traffic is important for infrastructure operations to maintain security, resolve problems, and perform resource planning.

Scalable TAP and SPAN Aggregation

It replaces traditional purpose-built matrix switches with one or more Cisco Nexus 3000 or 9000 Series Switches that you can interconnect to build a scalable network test access port (TAP) and Cisco® Switched Port Analyzer (SPAN) aggregation infrastructure that supports 1, 10, 40, and 100 Gbps. Also it can dedicate ports both for TAP and SPAN and for traditional Ethernet connectivity.

Cisco Application Centric Infrastructure Integration

Cisco Nexus Data Broker integrates with Cisco ACI to configure SPAN sessions and/or Copy function to monitor traffic within the Cisco ACI fabric. This integration eliminates the need for the user to separately configure SPAN sessions or Copy function in the APIC.

Automated SPAN Configuration in Production Network

NDB can now add production switches in Cisco Nexus Data Broker and automate SPAN destination and session configuration. This capability allows administrators to use a single interface to bring in traffic for monitoring purposes.

Scalable Traffic Monitoring with Cisco Nexus Data Broker Inline Option

The Cisco Nexus Data Broker Inline option allows to insert one or more Cisco Nexus 3000 Series or 9300 platform switches in your production infrastructure to which the security tools (or service nodes) are connected. Using the data broker software, configure redirection policies that can match specific traffic and redirect it through multiple security tools before the traffic enters or exits data center.

It can be deplyed in following modes

- **Centralized** mode for medium to large scale tap/SPAN aggregation where NDB is installed on Linux VM.
- **Embedded** single switch mode for small scale tap/SPAN aggregation where NDB is installed on the Linux Container of the Nexus Switch itself.

Modes of operation

- **OpenFlow mode**
- **NX-API mode**

Openflow

OpenFlow is an open standardized interface that allows a software-defined networking (SDN) controller to manage the forwarding plane of a network.

Cisco OpenFlow Agent provides better control over networks making them more open, programmable, and application-aware and supports the following specifications defined by the Open Networking Foundation (ONF) standards organization:

- OpenFlow Switch Specification Version 1.0.1 (Wire Protocol 0x01) (referred to as OpenFlow 1.0)
- OpenFlow Switch Specification Version 1.3.0 (Wire Protocol 0x04) (referred to as OpenFlow 1.3)

These specifications are based on the concept of an Ethernet switch, with an internal flow table and a standardized interface to allow traffic flows on a device to be added or removed. OpenFlow 1.3 defines the communication channel between the Cisco OpenFlow Agent and controllers.

A controller can be Cisco Open SDN Controller, or any controller compliant with OpenFlow 1.3.

In an OpenFlow network, Cisco OpenFlow Agent exists on the device and controllers exist on a server that is external to the device. Flow management and any network management are either part of a controller or accomplished through a controller. Flow management includes the addition, modification, or removal of flows, and the handling of OpenFlow error messages.

Openflow components

Cisco OpenFlow Agent creates OpenFlow–based TCP/IP connections to controllers for a Cisco OpenFlow Agent logical switch. Cisco OpenFlow Agent creates databases for a configured logical switch, OpenFlow-enabled interfaces, and flows. The logical switch database contains all the information needed to connect to a controller. The interface database contains the list of OpenFlow-enabled interfaces associated with a logical switch, and the flow database contains the list of flows on a logical switch as well as for interface that is programmed into forwarded traffic.

OpenFlow controller (referred to as a controller) controls the switch and inserts flows with a subset of OpenFlow 1.3 and 1.0 match and action criteria through Cisco OpenFlow Agent logical switch. Cisco OpenFlow Agent rejects all OpenFlow messages with any other action.

Limitaion when using NDB with Openflow

When Openflow is enabled on a particular port, 'spanning-tree bpdufilter enable' is automatically configured on the interface resulting in STP BPDU drop in software.

Additionally 'no lldp transmit' is configured on the interface as well. Thus LLDP neighborship for these interfaces doesn’t get formed on the switch. LLDP packets are however captured via ACL entry.

Currently NDB doesn't capture traffic from below link-level control plane protocols:

- STP

- LACP

- CDP

Known defects

CSCvr09006 NDB with 3500 cannot capture STP/CDP packets
CSCvr01876 Re-direct STP, CDP packets similar to LLDP port for Openflow