

Cisco Nexus Data Broker

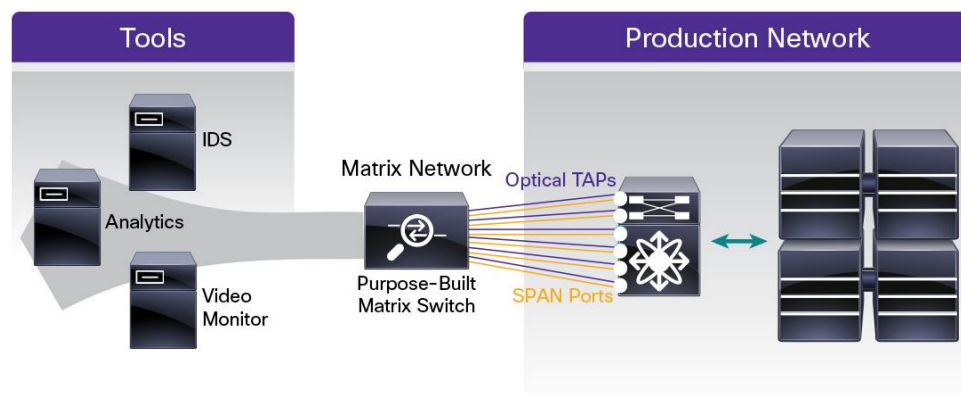
Product Overview

Every enterprise depends on the smooth running of its business applications and the underlying infrastructure. Visibility into application traffic has traditionally been important for infrastructure operations to maintain security, resolve problems, and perform resource planning. Now, however, as a result of technological advances and the ubiquity of the Internet, organizations increasingly are seeking not just visibility but real-time feedback about their business systems to more effectively engage their customers. Essentially, traffic monitoring is evolving from a tool to manage network operations to a tool for achieving smart business agility that can materially affect the revenue of the business.

Using the Cisco Nexus® Data Broker and Cisco Nexus Switches that support OpenFlow, Cisco provides a new software-defined approach to aggregate copies of network traffic using network taps or Switched Port Analyzer (SPAN) for monitoring and visibility. As opposed to traditional traffic monitoring solutions, this packet brokering approach offers a simple, scalable and cost-effective solution 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.

Traditional approaches to network traffic visibility have used some form of high-density purpose-built matrix switch to which both the Tap/SPAN input and the monitoring and analysis tools are connected. Figure 1 shows the traditional approach to network traffic monitoring.

Figure 1. Traditional Approach to Network Traffic Visibility

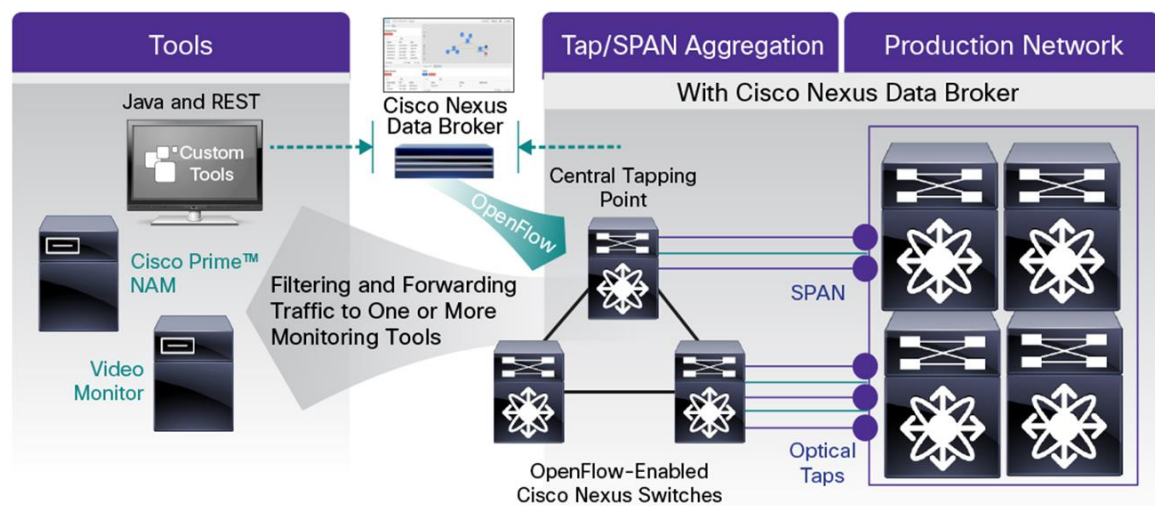


The traditional approach poses three primary challenges:

- The approach is too expensive to scale the visibility to meet today's business requirements.
- The purpose-built switches are statically programmed with predetermined filtering and forwarding rules, so they cannot act in an event-based way to provide traffic visibility in real time. This limitation lengthens response times as coverage increases.
- As the need for visibility into traffic patterns unique to a specific data center becomes more common, third-party tools cannot provide adequate coverage, resulting in coverage gaps.

Using the Cisco Nexus Data Broker, Cisco's approach replaces the matrix switches with one or more OpenFlow-enabled Cisco Nexus switches. The traffic is tapped into this bank of switches in the same manner as in a matrix network. However, with Cisco Nexus Data Broker, you can interconnect these Cisco Nexus switches to build a scalable Tap/SPAN aggregation infrastructure. You can use a combination of Tap and SPAN sources to bring the copy of the production traffic to this Tap/SPAN aggregation infrastructure. You also can distribute these Tap/SPAN sources and traffic monitoring and analysis tools across multiple Cisco Nexus switches. The monitoring and analysis tools can be physical appliance-based or virtual machine-based. Figure 2 shows the centralized deployment architecture using Cisco Nexus Data Broker.

Figure 2. Cisco Monitor Manager Solution for Network Traffic Visibility



OpenFlow implementation on Cisco Nexus switches supports hybrid mode, which allows you to use the same switch for production traffic and as a Tap/SPAN aggregation switch. With these features, the Cisco approach provides superior economics, saving both capital expenditures (CapEx) and operating expenses (OpEx) when compared with the traditional matrix network approach. The Cisco approach also helps ensure short response times and full coverage as monitoring needs scale.

Features and Benefits of Cisco Nexus Data Broker

Table 1 summarizes the main features and benefits of the Cisco Nexus Data Broker.

Table 1. Main Features and Benefits

Feature	Benefit
Supported topology for Cisco® Monitor Manager network	<ul style="list-style-type: none"> • Cisco Nexus Data Broker software discovers the Cisco Nexus switches and associated topology for Tap/SPAN aggregation. • The software allows you to configure ports as monitoring tool ports or input Tap/SPAN ports. • You can set end-device names for easy identification in the topology.
Support for QinQ to tag input source Tap/SPAN port	<ul style="list-style-type: none"> • You can tag traffic with a VLAN for each input Tap or SPAN port. • Q-in-Q support in edge Tap and SPAN ports allow you to uniquely identify the source of traffic and preserve production VLAN information.
Symmetric hashing or symmetric load balancing	<ul style="list-style-type: none"> • You can configure the hashing based on Layer 3 (IP address) or Layer 3 + Layer 4 (protocol ports) for load balancing the traffic across a port-channel link. • You can spread the traffic across multiple tool instances to meet the high-traffic-volume scale.

Feature	Benefit
Rules for matching monitored traffic	<ul style="list-style-type: none"> 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 action to set the VLAN ID for the matched traffic.
Replicate and forward traffic	<ul style="list-style-type: none"> You can configure the software to aggregate traffic from multiple input Tap/SPAN ports that could be spread across multiple Cisco Nexus switches. You can replicate and forward traffic to multiple monitoring tools that can be connected across multiple Cisco Nexus switches. This solution is the only one that supports any: many forwarding across a topology.
Time stamping**	<ul style="list-style-type: none"> 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 for critical transaction monitoring and archiving data for regulatory compliance and advance troubleshooting.
Packet truncation**	<ul style="list-style-type: none"> You can configure the software to truncate a packet beyond specified bytes. The minimum 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.
React to changes in the Tap/SPAN aggregation network states	<ul style="list-style-type: none"> You can monitor and keep track of network condition changes. You can configure the software to react to link or node failures by automatically reprogramming the flows through an alternative path.
End-to-end path visibility	<ul style="list-style-type: none"> For each traffic forwarding rule, the solution provides a complete end-to-end path visibility all the way from source ports to the monitoring tools, including the path through the network.
Management for multiple disjointed Cisco Monitor Manager networks	<ul style="list-style-type: none"> You can manage multiple independent traffic monitoring networks, which may be disjointed, using the same Cisco Nexus Data Broker instance. For example, if you have five data centers and you want to deploy an independent Cisco Monitor Manager solution for each data center, you can manage all of these five independent deployments using a single Cisco Nexus Data Broker instance by creating a logical partition (network slice) for each monitoring network.
Role Based Access Control (RBAC)	<ul style="list-style-type: none"> Application access can be integrated with corporate AAA server for both authentication and authorization You can create port groups and associate the port groups with specific user roles Capability to assign users to specific roles and port groups; users can manage only those ports

*Feature supported only on Cisco Nexus 3500.

**Feature supported only on Cisco Nexus 3100.

You can access the Cisco Nexus Data Broker application through the web-based GUI or REST API. Figures 3 and 4 show the GUI and REST API access mechanisms, respectively, for connecting to the Cisco Nexus Data Broker application.

Figure 3. Cisco Nexus Data Broker Application GUI Access Mechanism

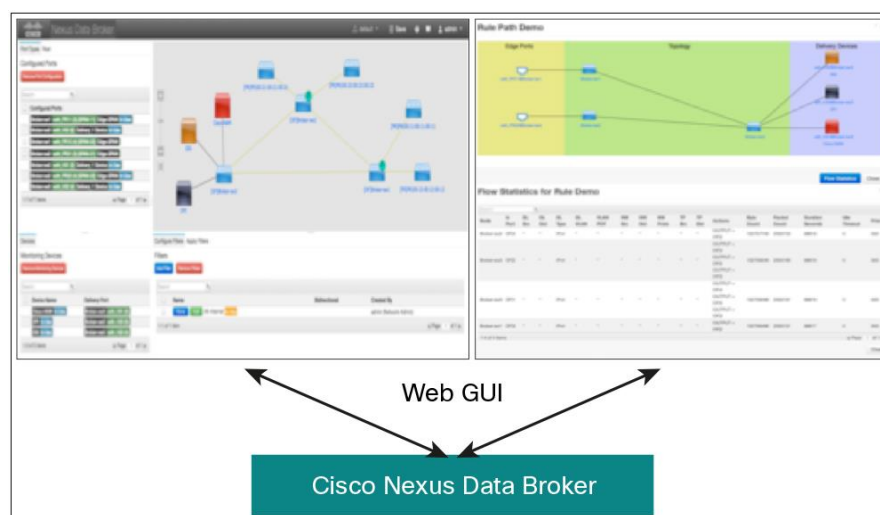
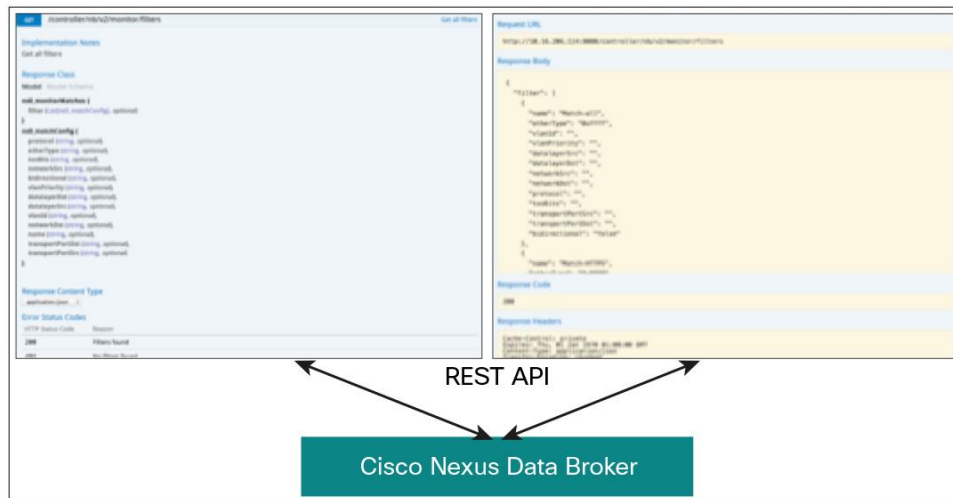


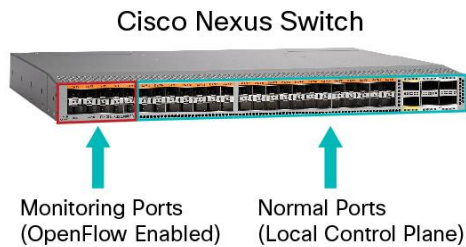
Figure 4. Cisco Nexus Data Broker Application GUI Access Mechanism



OpenFlow Hybrid Support

Cisco Nexus switches support hybrid OpenFlow mode, which allows you to allocate certain ports of Tap/SPAN aggregation that the Cisco Nexus Data Broker controls, with the remaining ports as normal ports controlled by the local control plane (Figure 5). Normal ports can carry the regular production traffic. The Cisco Nexus Data Broker application sees only the ports that are allocated for Tap/SPAN aggregation.

Figure 5. Cisco Nexus Data Broker with Hybrid Mode



Additional features include:

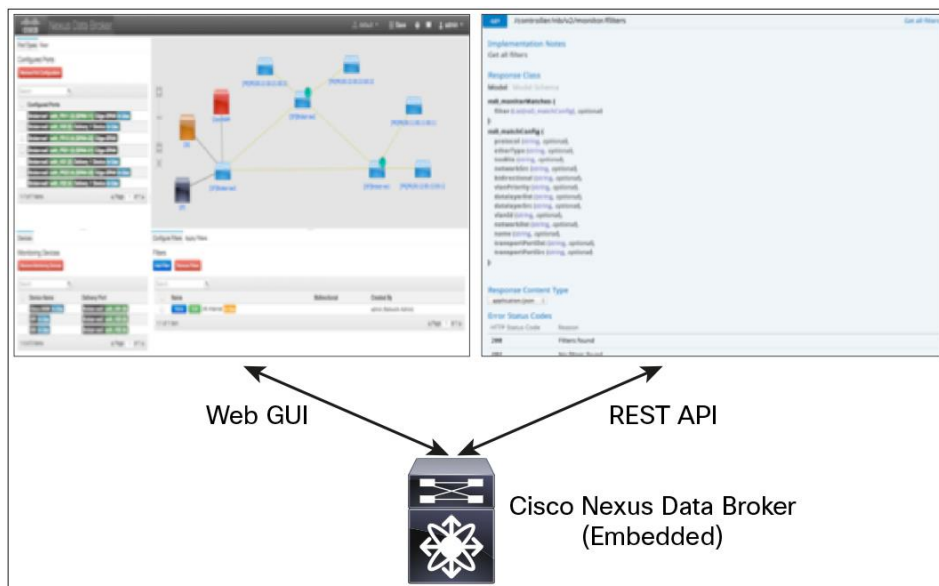
- Flexibility in assigning monitoring ports depending on the network requirements
- Ability to increase the number of monitoring ports depending on traffic requirements without having to disrupt production traffic

Cisco Nexus Data Broker Embedded

If you want to run Cisco Monitor Manager using a single Cisco Nexus 3000 Series Switch in your topology, you can run Cisco Nexus Data Broker software on the switch itself using the embedded function (Figure 6). Cisco Nexus Data Broker Embedded is provided as an open virtual appliance (OVA) that you can deploy on the Cisco Nexus Switch Linux container. After you download this OVA to the switch, you must activate it, and by default Cisco Nexus Data Broker uses the management interface IP address of the Cisco Nexus switch. All features of the Cisco Nexus Data Broker application are also available in this option except:

- Clustering and high availability
- Management for multiple switches in the network topology

Figure 6. Cisco Nexus Data Broker Embedded



Device Support Matrix for Cisco Nexus Data Broker

Table 2 lists the supported Cisco Nexus Data Broker software for the different Cisco Nexus switches.

Table 2. Cisco Nexus Data Broker Application Device Support Matrix

Device Model	Cisco Nexus Data Broker Software	Embedded Mode Support
Cisco Nexus 3000	Cisco Nexus Data Broker 2.0	Available
Cisco Nexus 3100	Cisco Nexus Data Broker 2.0	Available
Cisco Nexus 3500	Cisco Nexus Data Broker 2.0	Available
Cisco Nexus 5500	Cisco Nexus Data Broker 2.0	Not Available
Cisco Nexus 6000	Cisco Nexus Data Broker 2.0	Not Available
Cisco Nexus 7000*	Cisco Nexus Data Broker 2.0	Not Available
Cisco Nexus 7700*	Cisco Nexus Data Broker 2.0	Not Available

* Specific line cards and supervisor cards are required.

Licensing and Ordering Information

Tables 3 provide ordering information for Cisco Nexus Data Broker.

Table 3. Cisco Nexus Data Broker Software Ordering Information

Part Number	Description
L-NDB-FX-SWT-K9	Cisco Nexus Data Broker License for using single Cisco Nexus Fixed Switch in tap/SPAN aggregation mode
L-NDB-MD-M-SWT-K9	Cisco Nexus Data Broker License for using single Cisco Nexus Modular Chassis (Up to 6 slots) Switch in tap/SPAN aggregation mode
L-NDB-MD-L-SWT-K9	Cisco Nexus Data Broker License for using single Cisco Nexus Modular Chassis (> 6 slots) Switch in tap/SPAN aggregation mode

For More Information

For more information about Cisco Nexus Data Broker, please visit <http://www.cisco.com/go/nexusdatabroker> or contact your local Cisco account representative.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)