

Cisco Nexus Data Broker: Deployment Use Cases with Cisco Nexus 3000 Series Switches

What You Will Learn

Network Traffic monitoring using taps and Switched Port Analyzer (SPAN) is not a new concept. Network administrators have for several years been using various tools to perform such tasks as helping ensure compliance, security, troubleshooting connectivity and performance. This approach has become more challenging, however, as networking and applications have become more robust and are now often co-located in both private and public cloud environments.

Cisco Nexus[®] Data Broker offers an alternative to traditional tap and SPAN aggregation solutions for network traffic monitoring, at a reasonable cost. This simple and scalable solution offers several flexible implementation options that should appeal to almost any customer.

This document discusses real-world deployment use cases for Cisco Nexus Data Broker with Cisco Nexus 3000 Series Switches as currently implemented by Cisco customers.

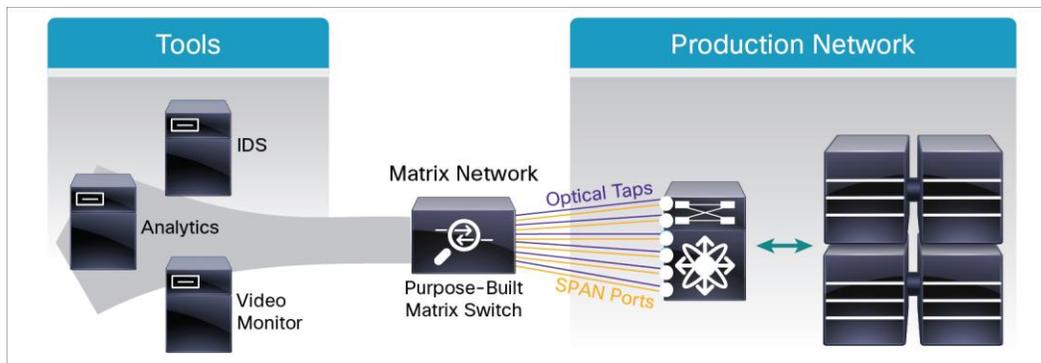
Introduction

Visibility into network traffic has traditionally been important for network operations, compliance, and security. With the exponential growth in the number of applications and the evolution of cloud-based technologies, IT departments need to find ways to maintain visibility into network traffic. Traffic visibility is needed for these main reasons:

- To demonstrate adherence to compliance and security requirements
- To intercept and record live traffic when mandated
- To verify the service-level agreements (SLAs) are met and provide actionable data to allow corrective actions to be taken as needed

Traditional approaches to network traffic visibility have used purpose-built matrix networks to aggregate network tap and SPAN data, with the monitoring and analysis tools connected to these networks. Figure 1 shows the traditional approach to network traffic monitoring.

Figure 1. Traditional Approach to Network Traffic Monitoring



The traditional approach poses three primary challenges:

- The approach is too expensive to scale to provide the visibility needed 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 the coverage area increases.
- As the need for visibility into traffic patterns unique to specific data center becomes more common, third-party tools cannot provide adequate coverage, resulting in coverage gaps.

The Cisco[®] solution consists of two elements: Cisco Nexus 3000 Series Switches and Cisco Nexus Data Broker Software. Compatible switches are:

- Cisco Nexus 3000 Series
- Cisco Nexus 3100 platform
- Cisco Nexus 3500 Series

Cisco Nexus 3000 Series Switches are used because of their flexible port options (1, 10, and 40 Gbps) and reasonable price. Customers in the financial, higher education, enterprise, and service provider sectors have implemented Cisco Nexus Data Broker.

The primary value propositions of the solution are:

- Significant reduction in capital expenditures (CapEx) compared to traditional approaches
- Efficient use of monitoring and analysis tools
- Faster troubleshooting

The Cisco solution gives customers flexibility, allowing them to use the centralized deployment option or the embedded on-switch deployment option on Cisco Nexus 3000 Series Switches.

Deployment use cases from customers across a variety of market segments provide insight into how this solution is used and the benefits gained. The following deployment use cases are discussed here:

- Centralized deployment with web-based GUI management at a large financial customer
- Centralized deployment using Representational State Transfer (REST) API management at a large financial customer

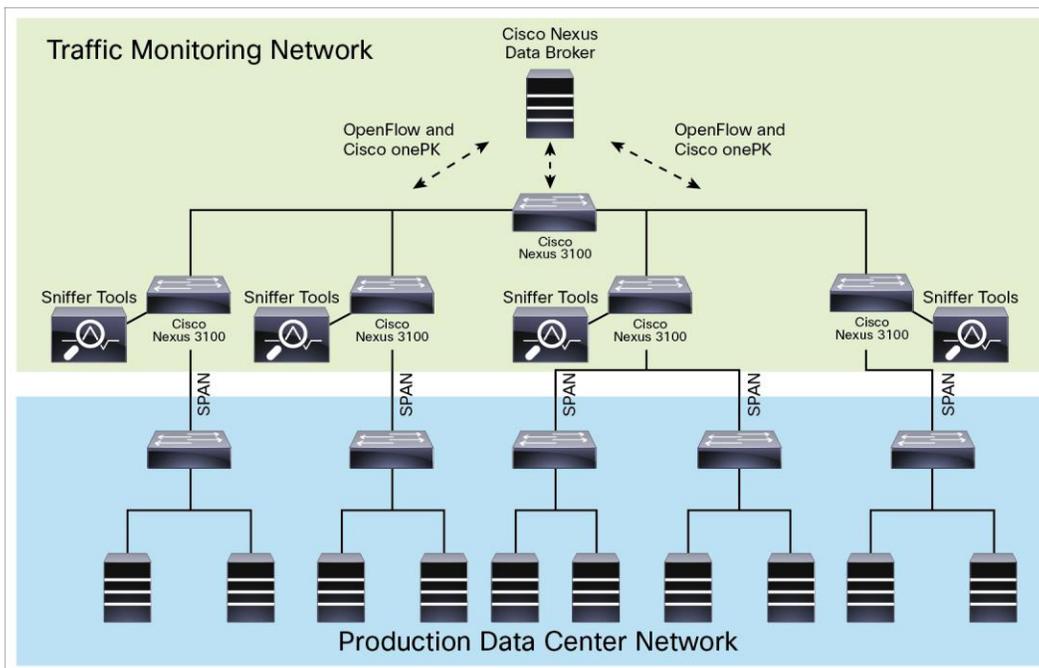
- Centralized deployment with slicing across multiple data centers at a large enterprise customer
- Embedded deployment with web-based GUI management across multiple data centers at a public sector customer
- Centralized deployment for quality assurance testing at a large enterprise customer

Centralized Deployment with Web-Based GUI Management at a Large Financial Customer

One customer in the finance sector has been using a traditional network packet broker solution to monitor network traffic for application performance measurements, network security, and network troubleshooting. The main drawbacks to this traditional approach were the high cost of the solution and the lack of flexibility in deployment, which resulted in loss of visibility and prolonged troubleshooting processes. The customer was seeking alternative solutions to overcome these challenges and enable faster troubleshooting.

With Cisco Nexus 3100 platform switches and Cisco Nexus Data Broker, the customer built a two-tier SPAN aggregation topology that met their needs for capturing and monitoring network traffic. The customer's production deployment consisted of Cisco Nexus Data Broker deployed in a separate Linux virtual machine (centralized option) to manage the traffic filtering, aggregation, and forwarding policies for the monitoring tools. Figure 2 shows the deployment architecture of Cisco Nexus Data Broker in this scenario.

Figure 2. Centralized Deployment with Web-Based GUI Management at a Large Financial Customer



In this deployment architecture, the customer set up one or more SPAN instances from every top-of-rack (ToR) production switch to Cisco Nexus 3172 Switches. Sniffer tools were also connected to these Cisco Nexus 3172 Switches. The Cisco Nexus 3132 was used as an aggregation switch to forward traffic across different Cisco Nexus 3172 Switches. By using the Cisco Nexus Data Broker web GUI, the customer was able to configure policies to match traffic based on Layer 1 through Layer 4 header information and then forward the matching traffic to one or more monitoring tools as required by the user. In addition, the customer also had the flexibility to configure VLAN tagging to identify source SPAN ports and specific service traffic.

The primary benefits of this new monitoring infrastructure for the customer are:

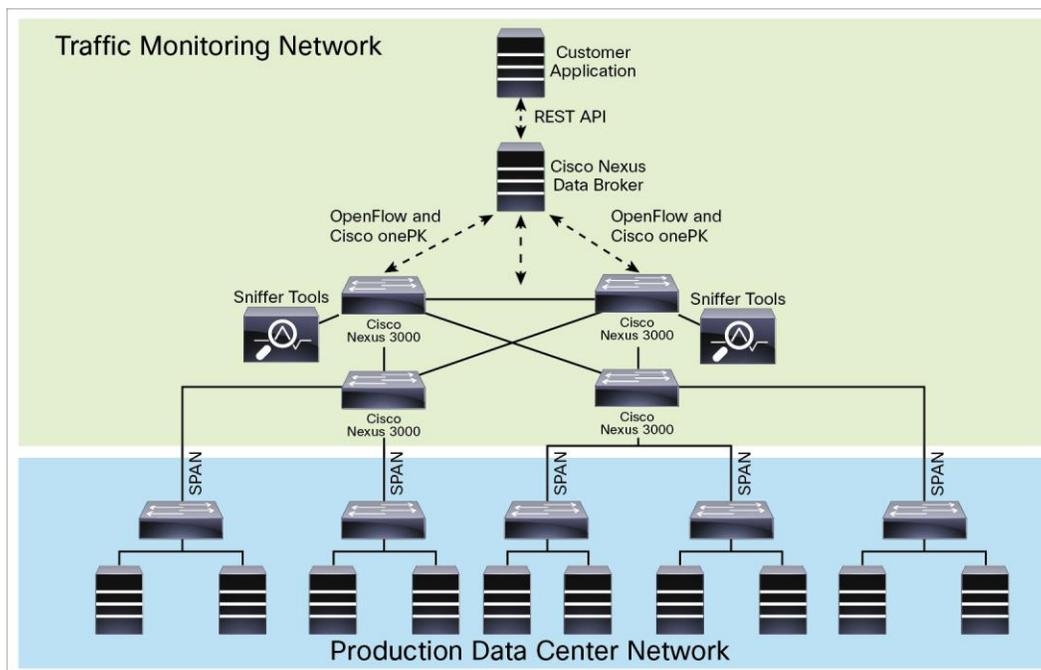
- Reduced CapEx and simpler, more cost-effective monitoring switches
- Efficient use of analysis tools from better utilization of ports
- Improved facilities because of flexibility in the placement of devices
- Faster troubleshooting and setup times, with processes reduced from days to minutes

Centralized Deployment with REST API Management at a Large Financial Customer

Another customer from the financial segment who was also using a traditional packet broker solution was not able to automate filtering and forwarding of traffic to the monitoring tools because of a lack of programmability options. This customer wanted to evaluate alternative approaches to reduce the overhead required and implement a better infrastructure for application performance monitoring. In addition, the customer wanted the solution to be able to manage multiple data centers.

The customer decided to deploy four Cisco Nexus 3064 Switches in each data center for tap and SPAN aggregation. These four Cisco Nexus switches were interconnected to allow them to forward traffic to different monitoring tools. Figure 3 shows the deployment architecture in this customer's environment.

Figure 3. Centralized Deployment with REST API Management at a Large Financial Customer



With the Cisco Nexus Data Broker REST API infrastructure, customers can perform all the same functions as with the GUI. Using this REST API approach, the customer was able to automate filtering, replication, and forwarding of traffic to monitoring tools on demand or based on events. In addition, as well as helping with configuration, the REST API can be used to query statistical information.

The primary benefits for the customer are:

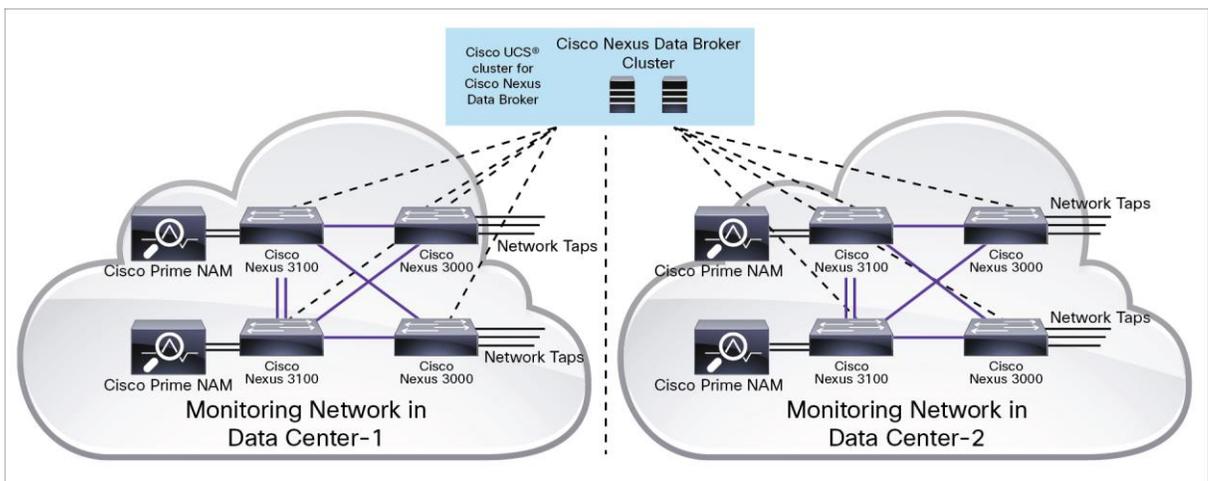
- Complete automation of the network traffic monitoring infrastructure
- Efficient use of analysis tools because traffic can be sent to specialized monitoring solutions as needed
- Faster troubleshooting and setup times, with processes reduced from days to minutes

Centralized Deployment with Slicing across Multiple Data Centers at a Large Enterprise Customer

A large enterprise customer was using a traditional network packet broker solution across multiple data centers without the capability to manage its systems centrally. In addition to being expensive, the traditional packet broker approach was cumbersome to manage, because the customer had to navigate among multiple systems to configure traffic-forwarding policies.

One of the benefits of Cisco Nexus Data Broker is the capability to manage multiple independent tap and SPAN aggregation networks from a centralized instance. These independent instances can also be spread across multiple data centers. Many of Cisco's enterprise customers are using this capability to manage multiple potentially disjointed systems all from one tool. Figure 4 shows the deployment architecture at this customer's data center.

Figure 4. Centralized Deployment with Slicing across Multiple Data Centers at a Large Enterprise Customer



In this deployment architecture, each data center uses from four to six Cisco Nexus 3000 Series or 3100 platform switches. With Cisco Nexus Data Broker, each site can be associated with a logical partition called a network slice. A single Cisco Nexus Data Broker instance can manage multiple network slices. Each network slice can have its own filtering and forwarding policies, statistics collection, and user role-based access control (RBAC) for access. This option is excellent for large enterprises with more than one location but a centrally located IT department. The only primary requirement when implementing this architecture is a reliable Layer 3 connection between sites for communication with the Cisco Nexus Data Broker Software.

The primary benefits for the customer are:

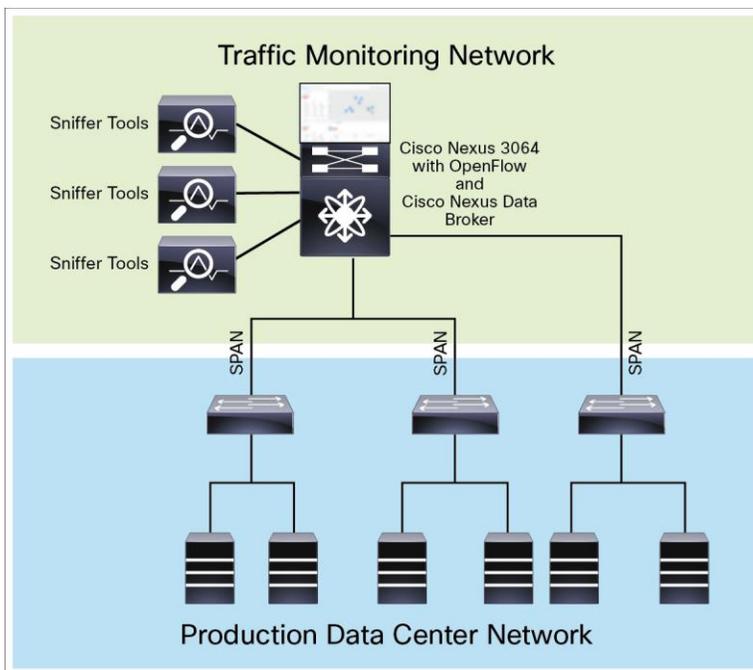
- Centralized management for all traffic monitoring networks
- Use of RBAC capabilities to provide access to users locally only for those instances
- Significant CapEx savings

Embedded Deployment with Web-Based GUI Management across Multiple Data Centers at a Public Sector Customer

A customer in the public sector segment was seeking a cost-effective option for building a tap and SPAN aggregation network for its smaller co-located facility. The customer's primary requirements were that the solution be simple to manage, include the capability to designate control to the local team, and be cost effective.

Cisco Nexus Data Broker offers an embedded deployment model that met all of the customer's criteria. In this deployment, Cisco Nexus Data Broker Software runs natively on a Linux container in the Cisco NX-OS Software on a Cisco Nexus 3000 Series Switch. Figure 5 shows the deployment architecture with the embedded model.

Figure 5. Embedded Deployment with Web-Based GUI Management across Multiple Data Centers at a Public Sector Customer



In this deployment, the customer used the Cisco Nexus Data Broker embedded option with the Cisco Nexus 3064 Switch. The Cisco Nexus 3064 provides forty-eight 10-Gbps ports and four 40-Gbps ports. The port density of this model provided the number of taps and SPAN instances that customer planned to use in the smaller co-located facility. In smaller co-location environments in which multiple-switch deployment may not be necessary, the embedded option works well. In these cases, customers can install the software on the Cisco Nexus switch itself and then manage filtering and forwarding policies through the GUI or the REST API. With the embedded deployment option, an open virtual appliance (OVA) is downloaded and installed in a Linux container on the switch. This option has all the features of the centralized use cases except clustering, high availability, and management for multiple switches in the tap and SPAN aggregation topology.

The primary benefits for the customer are:

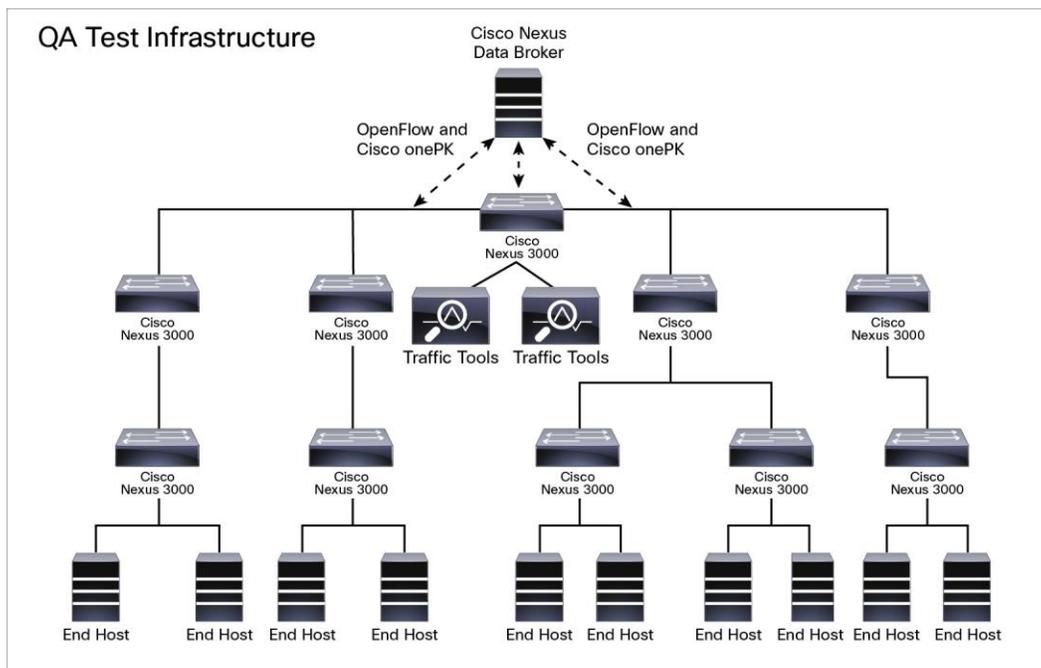
- Simple, flexible, and faster deployment
- Significant CapEx savings compared to traditional solutions
- Robust GUI and REST API for all configurations
- Proper sizing for smaller environments

Centralized Deployment for Quality Assurance Testing at a Large Enterprise Customer

One large enterprise customer wanted to build an automated and large-scale QA automation environment. Traditional solutions were expensive and did not meet the high port density requirements for the environment.

Using Cisco Nexus 3000 Series Switches, the customer was able to build a three-tier topology that allowed the customer to send traffic from any test traffic-generation system to one or more test candidates across the network. Figure 6 shows the deployment architecture for this solution.

Figure 6. Centralized Deployment for Quality Assurance Testing at a Large Enterprise Customer



In this deployment, the customer used a combination of Cisco Nexus 3016, 3064, and 3048 Switches to build the test automation environment. A three-tier topology allowed the customer to move the traffic from the test traffic generators to any end host. Instead of recabling the entire network every time traffic needed to be directed to a different part of the network, the customer used the forwarding policies in Cisco Nexus Data Broker to direct the traffic to the end hosts. With this approach, all the QA testing is essentially automated, enabling the customer to test whenever the customer chooses, with little disruption.

The primary benefits for the customer are:

- Significant CapEx savings compared to traditional solutions
- High port density on the switches for efficient use
- Robust GUI and REST API for all configurations
- Built-in automation for QA testing

Conclusion

There are several ways to deploy Cisco Nexus Data Broker to monitor your network in the most efficient way for your environment. Certain deployments will depend on the company's market segment and the size of the network being monitored. Cisco Nexus Data Broker is a very scalable solution with options ranging from a smaller one-switch, embedded deployment to a centralized deployment across many data centers in different locations. Because of this flexibility, Cisco Nexus Data Broker customers can monitor any part of their networks in an automated way at a cost-effective price.

For More Information

- For more information about Cisco Nexus Data Broker: <http://www.cisco.com/go/nexusdatabroker>.
- Cisco Nexus Data Broker data sheet: <http://www.cisco.com/c/en/us/products/cloud-systems-management/nexus-data-broker/datasheet-listing.html>.
- Cisco Nexus Data Broker quick-start guide: <http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/extensible-network-controller-xnc/guide-c07-731460.html>.
- Cisco Nexus Data Broker solution overview: <http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/extensible-network-controller-xnc/solution-overview-c22-729753.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.

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)