Network Traffic Visibility and Analysis with Cisco Nexus Data Broker and Cisco Prime Virtual Network Analysis Module

What You Will Learn

Exponential growth in the network traffic has led to increased need for network traffic monitoring. However use of traditional network traffic monitoring approaches require significant capital expenditures (CapEx) and operating expenses (OpEx). To address this challenge, many customers are seeking virtual machine-based monitoring tools for traffic analysis and cost-effective options to deliver network traffic to these tools. This document describes Cisco Nexus® Data Broker, which offers a cost-effective approach to delivering traffic to a variety of monitoring tools including virtual machine-based monitoring tools. It also describes how Cisco Nexus Data Broker can work with the virtual machine-based Cisco Prime™ Virtual Network Analysis Module (vNAM) to provide application traffic visibility and analysis. In addition, this document presents the details of the configuration required on the hypervisor virtual switch (vSwitch) to deliver the traffic to Cisco Prime vNAM.

Introduction

Today’s resource-intensive applications are causing network traffic to grow exponentially, putting high demands on the existing network. Companies are finding it challenging to differentiate critical applications from noncritical ones and to dynamically allocate network resources to higher-priority applications. To better manage network resources, you need visibility into the network traffic. To monitor and gain visibility into the network traffic, customers typically have used purpose-built matrix switches for optical tap and Switched Port Analyzer (SPAN) aggregation.

Traditional matrix switches present three main challenges:

- High cost of the solution, which can be very expensive for large-scale deployments
- Limitations on deployment and interconnection of these matrix switches to provide a scalable monitoring network
- Static way of configuring filters and forwarding traffic, which makes it difficult to take actions based on events

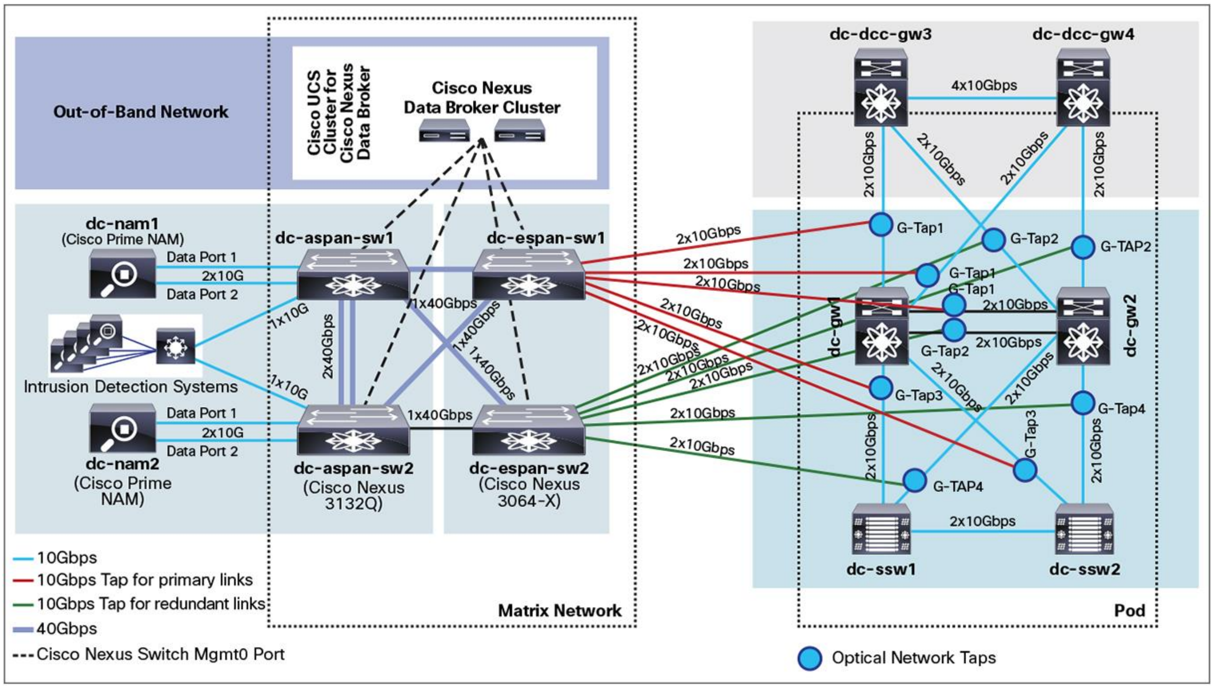
To address come these challenges, Cisco introduced Cisco Nexus Data Broker, which consists of Cisco Nexus Family switches acting as tap and SPAN aggregation switches and Cisco Nexus Data Broker software, which allows the traffic to be filtered and forwarded to various tools sets.

Cisco Nexus Data Broker

With Cisco Nexus Data Broker, matrix switches are replaced with one or more OpenFlow-enabled Cisco Nexus switches. The traffic is tapped into this bank of switches in the same way as in a matrix network. However, with Cisco Nexus Data Broker, you can interconnect these Cisco Nexus switches to build a scalable tap and SPAN aggregation infrastructure. You can use a combination of tap and SPAN sources to bring a copy of the production traffic to this tap and SPAN aggregation infrastructure. You also can distribute these tap and SPAN sources and traffic monitoring and analysis tools across multiple Cisco Nexus switches. The monitoring and analysis tools can be physical appliances or virtual machine based.

Figure 1 provides an overview of a Cisco Nexus Data Broker deployment.

Figure 1. Cisco Nexus Data Broker Deployment Architecture



Main Features and Benefits

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

Table 1. Main Features and Benefits

Feature	Benefit
Supported topology for Cisco Nexus Data Broker	Cisco Nexus Data Broker discovers the Cisco Nexus switches and associated topology for tap and SPAN aggregation, providing scalable infrastructure.
Support for QinQ to tag input source tap and SPAN ports	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*	You can configure hashing based on Layer 3 (IP address) or Layer 3 and Layer 4 (protocol ports) to load balance traffic across a PortChannel link. This feature enables you to distribute the traffic to multiple tools or multiple interfaces connected to the same tool.
Rules for matching monitored traffic	You can match traffic based on Layer 1 through Layer 4 header information.

Feature	Benefit
Traffic replication and forwarding	• You can configure the software to aggregate traffic from multiple input tap and SPAN ports, which can be spread across multiple Cisco Nexus switches. • You can replicate and forward traffic to multiple monitoring tools, which can be connected across multiple Cisco Nexus switches.
Time stamping[**]	You can time-stamp a packet at ingress using 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 advance troubleshooting.
Packet truncation[**]	You can configure the software to truncate a packet beyond a specified number of bytes.
Response to changes in tap and SPAN aggregation network states	Cisco Nexus Data Broker automatically responds to a link or node failure by 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® Monitor Manager networks	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 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)	• Application access can be integrated with the corporate authentication, authorization, and accounting (AAA) server for both authentication and authorization. • You can create port groups and associate the port groups with specific user roles.

[*] Feature supported only on Cisco Nexus 3500 Series Switches

[**] Feature supported only on Cisco Nexus 3100 platform

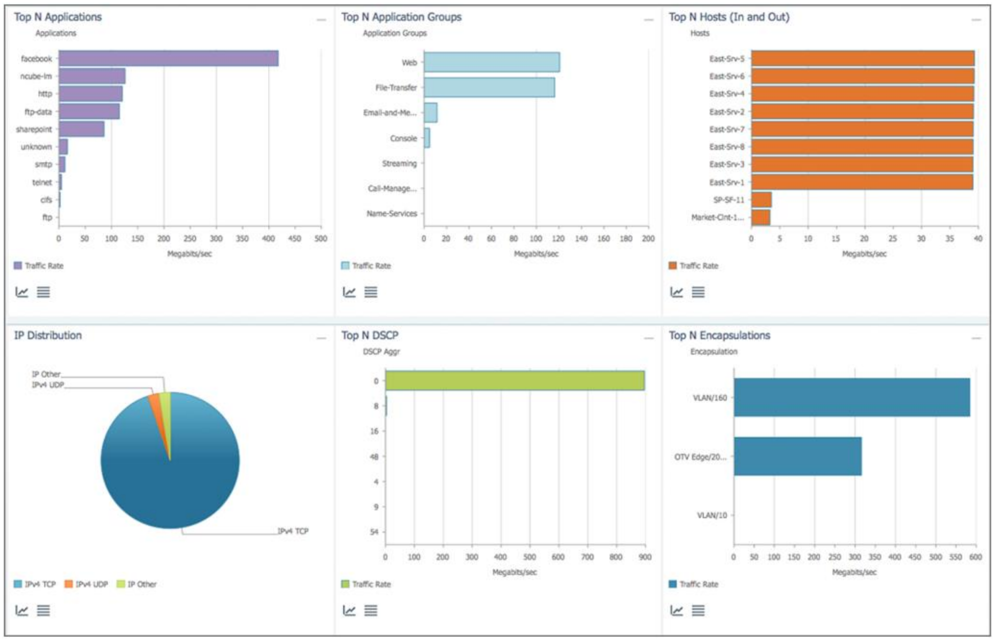
Cisco Prime vNAM

Cisco Prime vNAM provides the flexibility for customers to run the NAM software on a virtual machine. Cisco Prime vNAM combines deep application awareness, insightful performance analytics, and comprehensive network visibility to empower network administrators to efficiently and effectively manage their networks. The versatility of Cisco Prime vNAM allows you to:

- Gain Layer 4 through Layer 7 visibility using Cisco Network-based Application Recognition 2 (NBAR2) natively to easily identify business-critical applications
- Understand traffic behavior within overlay technologies such as Cisco Virtual Extensible LAN (VXLAN), Locator/ID Separation Protocol (LISP), and Overlay Transport Virtualization (OTV).
- Analyze network use by application, host, virtual machine, and conversation to identify bottlenecks that may affect performance and availability
- Troubleshoot performance problems by combining detailed traffic flow and packet analysis consistently across physical and virtual environments
- Validate infrastructure updates such as WAN optimization, Cisco TrustSec® security, and quality-of-service (QoS) policy changes
- Take advantage of an integrated web-based interface to manage a site remotely, eliminating the need to backhaul the data to a centralized location and saving WAN bandwidth

Cisco Prime vNAM comes with a remotely accessible web-based management and reporting console (Figure 2), which runs the Cisco Prime NAM Software. The software includes prepackaged dashboards that provide immediate views of network performance and workflows, helping organizations make operational decisions more quickly.

Figure 2. Cisco Prime vNAM Web-Based Management and Reporting Console



Cisco Prime vNAM offers an extensive set of features (Table 2), all in one value-based solution.

Table 2. Cisco Prime vNAM Features and Benefits

Feature	Benefit
Deployment versatility	• Deploy Cisco Prime vNAM in tenant network containers, remote sites, or almost any place in the network. • Meet the demand for operational agility in virtualized data center and cloud environments.
Deep packet inspection (DPI) with NBAR2	• Gain rapid visibility into business-critical applications with NBAR2. • Classify a range of applications such as Skype, Torrent, and Microsoft Office 365, or even mobile apps such as FaceTime.
Application performance analytics	• Characterize the end-user experience for TCP-based applications. • Isolate application response-time problems to the network, server, or application and accelerate troubleshooting.
Voice quality analytics	Gather real-time reports on the mean opinion score (MOS) and other key performance indicators (KPIs) such as jitter and packet loss to understand and improve the end-user experience for voice services.
Traffic analysis	• View short- and long-term network use by applications, hosts, conversations, and various supported encapsulations. • Identify top consumers of network resources and isolate network bottlenecks to optimize network resource allocation.
Insight into encapsulation and overlay technologies	Design overlay networks for efficient application delivery. Supported protocols include OTV, LISP, VXLAN, and Control and Provisioning of Wireless Access Points (CAPWAP).
Cisco TrustSec policy validation	Validate Cisco TrustSec policies using security group tags (SGTs) and evaluate the endpoints or hosts, applications, and conversations participating in one or more security groups.
WAN-optimized network visibility	• Accelerate your return on investment (ROI) by assessing the best site and application candidates for optimization as part of the phased rollout plan. • Obtain end-to-end proof points demonstrating improved application delivery using Cisco Wide Area Application Services (WAAS): for example, decreased application transaction times or improved WAN bandwidth use.
Deep, insightful packet analysis	• Solve complex performance problems with trigger-based capture, filter, decode, and error scan features. • Trigger packet captures based on performance thresholds, allowing you to focus on specific performance problems. • Use external storage to collect extensive packet captures for offline analysis.

Feature	Benefit
Open interface	Preserve investment in existing management assets through integration based on a standards-based (Representational State Transfer (REST) and XML) API.
Anytime, anywhere access	Access the web interface from any desktop; no need to send personnel to remote sites or send large amounts of data over WAN links to the central site.
Cisco Prime Infrastructure integration	• Manage NAMs from a single, centralized console. • Collect and view NAM statistics from across the network to get a “big picture” view of network performance.

Cisco Nexus Data Broker with Cisco Prime vNAM Topology

Cisco Nexus 3100 platform switches are used as tap and SPAN aggregation switches. An optical tap is connected to Ethernet ports 1/10 and 1/11 on each switch.

At least two interfaces are required on the Cisco UCS® server on which Cisco Prime vNAM is running: one for the Cisco Prime vNAM management connection, and another for receiving the data traffic.

Two Cisco Prime vNAMs are used: one connected to NX-SW-2, and one connected to NX-SW-3. The data port on the Cisco UCS server host on which Cisco Prime vNAM is running is connected to Ethernet port 1/47 on both switches.

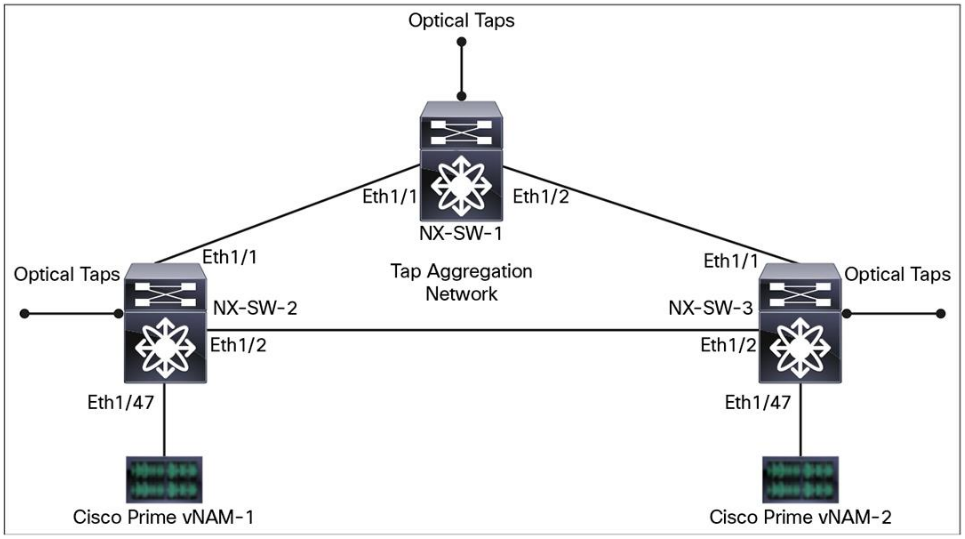
The following application traffic is received from the production network through optical taps:

- FTP control traffic
- FTP data traffic
- Telnet traffic
- Microsoft SharePoint traffic
- Cisco Jabber® traffic
- Cisco IP phone traffic
- Session Initiation Protocol (SIP) traffic
- HTTP traffic
- Network File System (NFS) traffic
- Bit-torrent traffic
- Simple Network Management Protocol (SNMP) traffic
- Domain Name System (DNS) traffic

A copy of the traffic from the production network is sent to two Cisco Prime vNAMs for analysis and reporting.

Figure 3 shows the topology used in the sample configuration in this document.

Figure 3. Topology for the Configuration Example

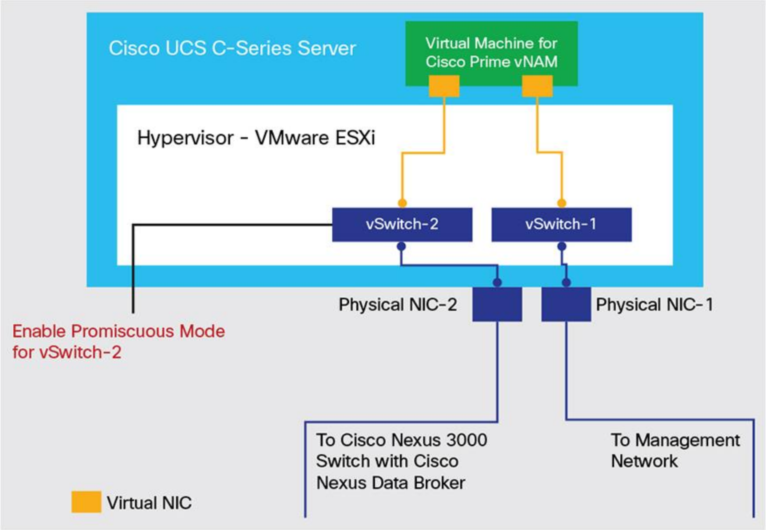


Configuring Cisco Prime vNAM to Receive Traffic

This document provides a sample configuration of virtual switch interfaces for the VMware ESXi hypervisor. For other hypervisors, please refer to the appropriate document about configuring the virtual switch interfaces. For information about installation of Cisco Prime vNAM, please refer to the Cisco Prime vNAM installation and configuration guide at http://www.cisco.com/c/en/us/td/docs/net_mgmt/network_analysis_module_software/vNAM/install/guide/cisco_prime_vnam_install_config_guide.html.

Figure 4 shows the Cisco UCS server host, hypervisor, and network connectivity.

Figure 4. Cisco UCS, Hypervisor, and Network Connectivity Configuration


Cisco UCS C-Series Server
Virtual Machine for Cisco Prime vNAM
Hypervisor - VMware ESXi
vSwitch-2
vSwitch-1
Physical NIC-2
Physical NIC-1
Enable Promiscuous Mode for vSwitch-2
To Cisco Nexus 3000 Switch with Cisco Nexus Data Broker
To Management Network
Virtual NIC

Configuring Cisco Nexus Data Broker

To configure Cisco Nexus Data, use these steps:

- Enable the Cisco plug-in for OpenFlow on Cisco Nexus 3000 Series Switches.
- Configure device settings in Cisco Nexus Data Broker.
- Configure Cisco Nexus Data Broker to filter and forward traffic.

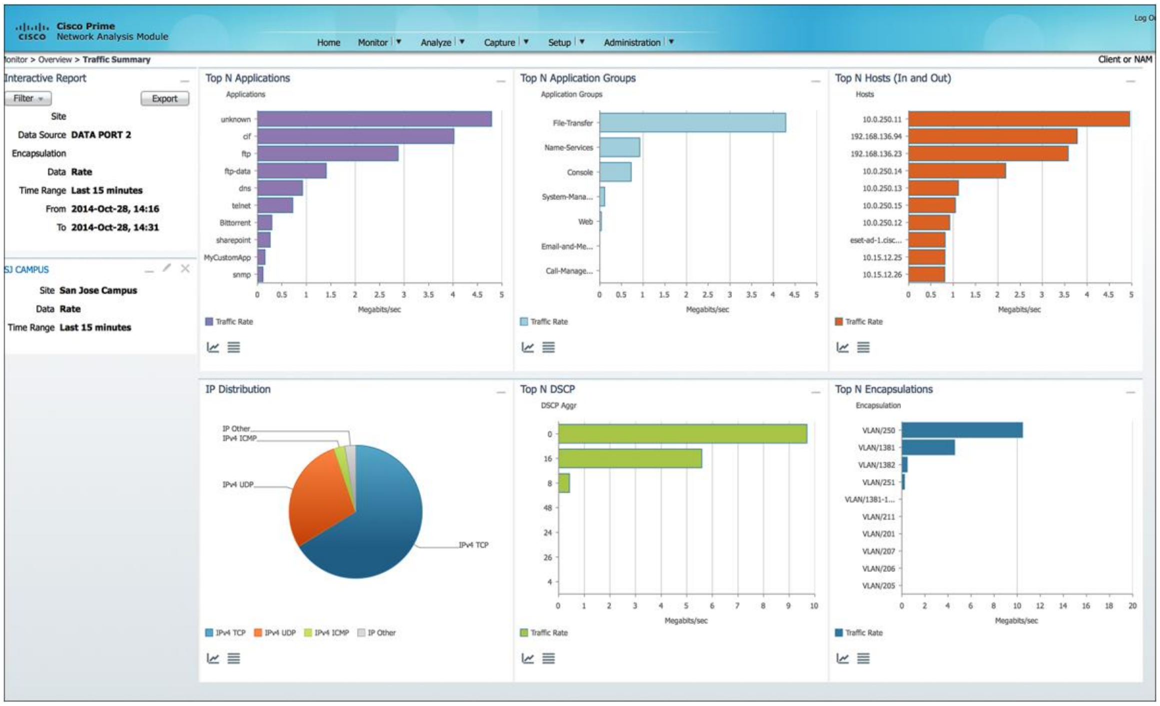
Detailed configuration steps for these activities can be found in the Cisco Nexus Data Broker solution quick-start guide at http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/extensible-network-controller-xnc/guide-c07-731460.html.

Viewing Application Traffic Details in Cisco Prime vNAM

Example 1: Traffic Analysis

View the amount of bandwidth taken by the Top N applications in the network. This view can help you understand events such as a sudden burst of traffic for an application in the network. You can view the application, the amount of bandwidth consumed by the application, and the clients and servers for this application. You can also verify that unwanted traffic such as bit torrent isn't running in your network (Figure 5).

Figure 5. Example 1: Traffic Analysis



lonitor > Overview > **Traffic Summary**

Interactive Report

Site

Data Source **DATA PORT 2**

Encapsulation

Data **Rate**

Time Range **Last 15 minutes**

From **2014-Oct-28, 14:16**

To **2014-Oct-28, 14:31**

SJ CAMPUS

Site **San Jose Campus**

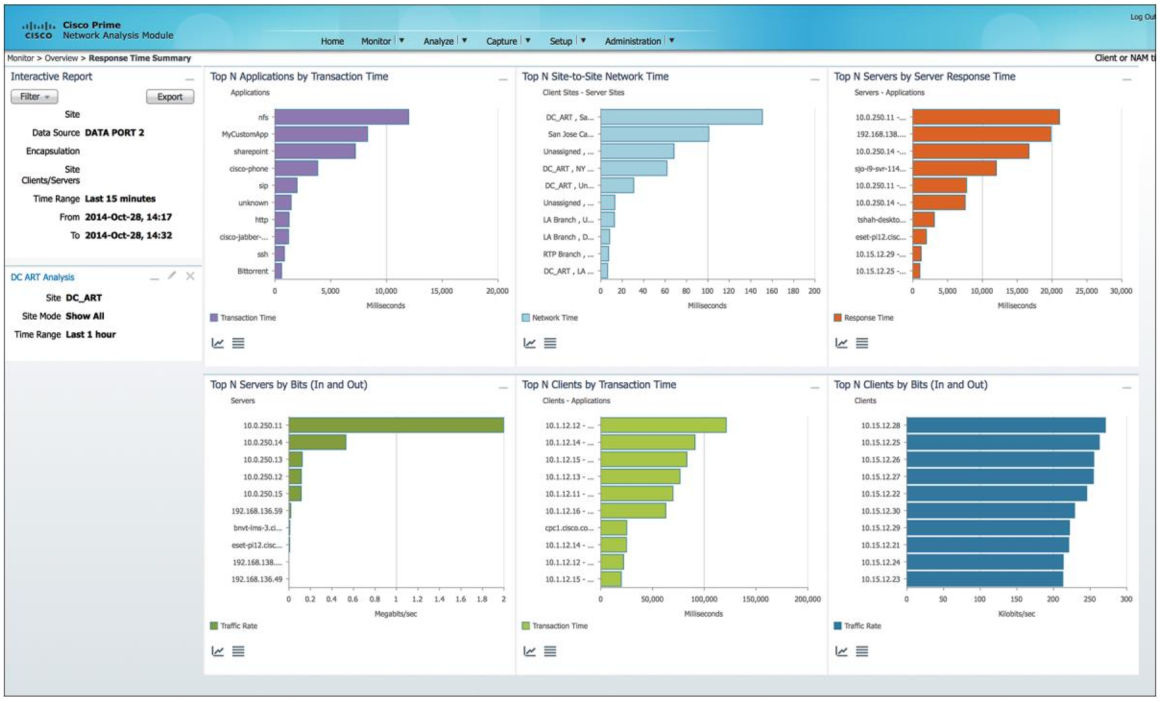
Data **Rate**

Time Range **Last 15 minutes**

Example 2: Application Response-Time Summary

Cisco Prime NAM calculates many metrics to measure the end-user experience for business critical applications. You can see the Top N applications by response time and then view deeper into a specific application to see what is causing the higher response time and which clients and servers are being affected by this application (Figure 6).

Figure 6. Example 2: Application Response-Time Summary



Monitor > Overview > **Response Time Summary**

Interactive Report

Site

Data Source **DATA PORT 2**

Encapsulation

Site Clients/Servers

Time Range **Last 15 minutes**

From **2014-Oct-28, 14:17**

To **2014-Oct-28, 14:32**

DC ART Analysis

Site **DC_ART**

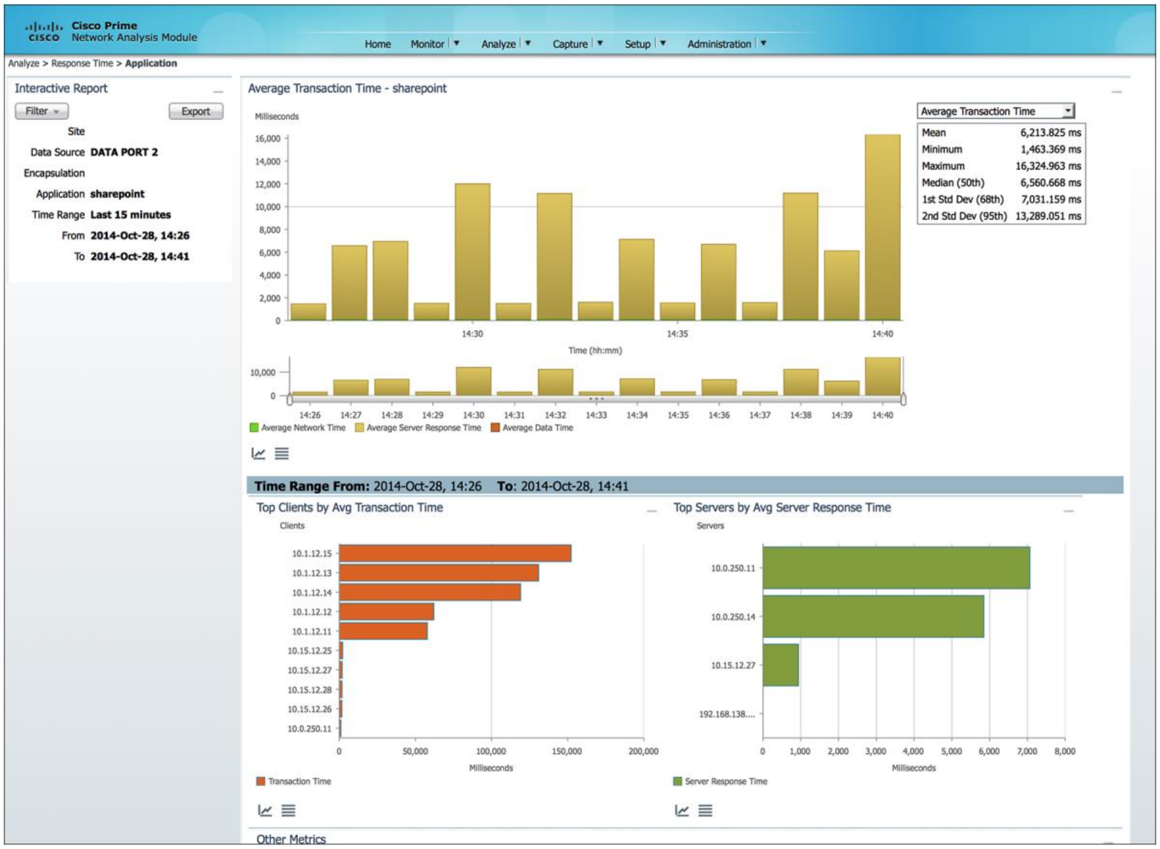
Site Mode **Show All**

Time Range **Last 1 hour**

Example 3: Application Response Time

Using Cisco Prime NAM, you can identify whether the network time, server response time, or data time is responsible for the higher response time. You can also view the Top N clients and servers for this application by client transaction time and server response time (Figure 7).

Figure 7. Example 3: Application Response Time



Site	
Data Source	**DATA PORT 2**
Encapsulation	
Application	**sharepoint**
Time Range	**Last 15 minutes**
From	**2014-Oct-28, 14:26**
To	**2014-Oct-28, 14:41**

Average Transaction Time

Mean	6,213.825 ms
Minimum	1,463.369 ms
Maximum	16,324.963 ms
Median (50th)	6,560.668 ms
1st Std Dev (68th)	7,031.159 ms
2nd Std Dev (95th)	13,289.051 ms

Time Range From: 2014-Oct-28, 14:26 **To:** 2014-Oct-28, 14:41

Conclusion

Cisco Nexus Data Broker with Cisco Prime vNAM together offer customers scalable and cost-effective application traffic visibility and analysis. Cisco Nexus Data Broker with Cisco Nexus switches is a software-defined, programmable solution that aggregates copies of network traffic using SPAN or network taps for monitoring and visibility. This packet brokering approach offers a simple, scalable, and cost-effective solution well suited for customers who need to monitor high-volume and business-critical traffic for efficient use of security, compliance, and application performance monitoring tools.

Cisco Prime vNAM gives you the flexibility to deploy the application analysis software in a virtual environment or in an appliance. Both options provide the detailed application visibility and application performance information that are essential for network administrators.

For More Information

- For more information about Cisco Nexus Data Broker, visit http://www.cisco.com/go/nexusdatabroker.
- For more information about Cisco Prime NAM, visit http://www.cisco.com/go/nam.

Configuration guides, data sheets, and solution overviews can be found in these locations.

If you need additional information, please contact your local 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.

Printed in USA

C11-733475-00 12/14