White Paper

Software-Defined Networking: How to Get Started

What You Will Learn

Software-defined networking (SDN) provides a programmatic approach and represents a major shift in the approach to networking and network operations. However, although SDN provides business benefits in the form of lower operating expenses (OpEx) and capital expenditures (CapEx), customers are hesitant to deploy SDN-based technologies in their networks because of concerns about negatively affecting production traffic. This document describes a low-risk approach to introducing SDN into your environment while solving a real-world business problem and achieving the same business benefits.

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. As a result, customers are seeking a solution to make the network application aware by intelligently monitoring and routing the network traffic. SDN provides the components necessary to make the network programmable, dynamic, and application aware.

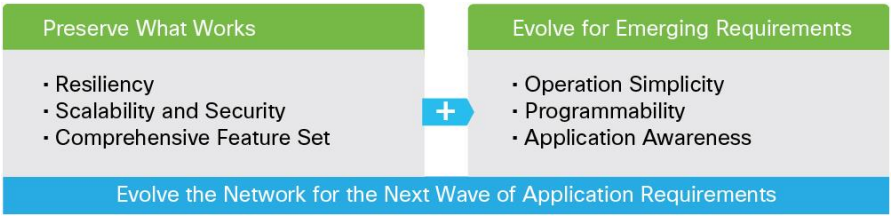
SDN is an approach to programmable networks that separates and abstracts some of the control-plane functions from the network devices and places them in a centralized controller. SDN as a concept and as a technology has evolved over the past 24 months, yet customers have not widely adopted the technology in production environments. Although this centralized approach simplifies the management of complex flows and enables programmability, it has the following drawbacks:

- It requires high-impact changes in the production network.
- This new technology involves unknown risk and could severely affect production traffic if it is not implemented correctly.
- It requires the customers to bring together networking, application, and programming skill sets.
- It allows applications to control the traffic path and requires the change management process to be updated in the network.
- Solutions from disparate vendors can trigger support-related problems.

SDN with Cisco Extensible Network Controller

With the Cisco® Extensible Network Controller (XNC) and its applications, Cisco provides a hybrid approach to SDN in which the traditional control plane continues to exist and an external controller enables programmability and application flow management for specific business requirements. With this approach, customers can continue to use their existing infrastructure and still benefit from the programmability aspects of SDN. Figure 1 shows the network evolution approach from Cisco.

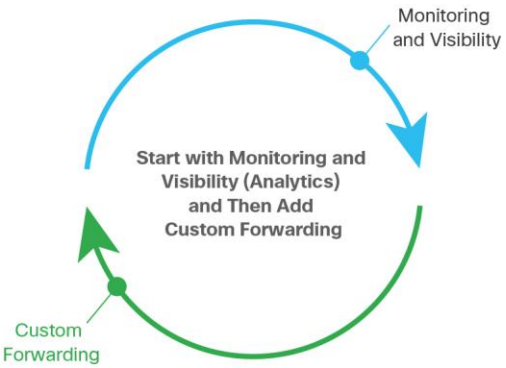
Figure 1. Evolution of the Intelligent Network



Introducing SDN into Your Environment

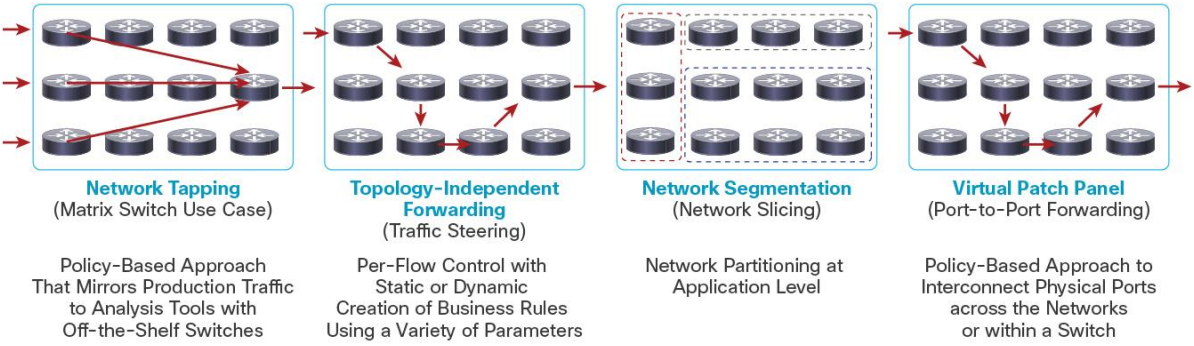
To reduce the risk associated with the introduction of SDN approaches in the network, customers are seeking a noninvasive, low-risk approach. With Cisco XNC, Cisco addresses these needs and provides an approach to evolve the network as technology changes. Cisco's blueprint for SDN adoption recommends that customers start with a network traffic monitoring and visibility use case. Figure 2 shows Cisco's recommended blueprint for SDN adoption.

Figure 2. Blueprint for Adopting SDN



After customers gain expertise with SDN technologies and have plans to mitigate the risks, they can expand SDN into the production environment with customer forwarding applications. Cisco XNC Release 1.0 follows with this blueprint, Figure 3 shows the use cases in this release.

Figure 3. Cisco XNC Release 1.6 Use Cases



Network tapping and network traffic visibility is provided by Cisco Monitor Manager, which is an application in Cisco XNC. Using Cisco Monitor Manager, customers can introduce SDN into their networks without any need for changes in the production infrastructure and without affecting production traffic.

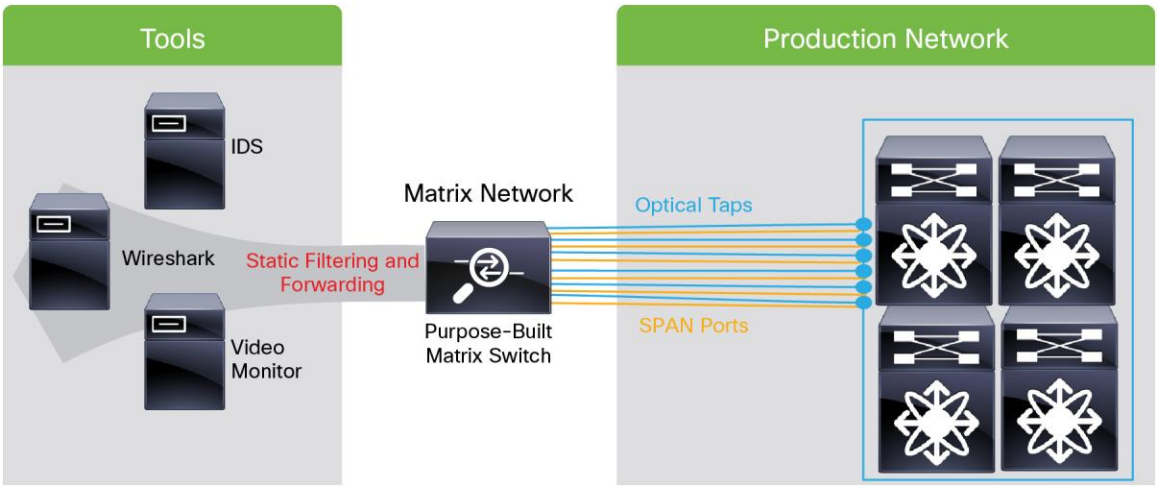
Cisco Monitor Manager Solution

With the massive growth in data, IT departments need to find ways to maintain visibility into the traffic in their networks. The main reasons that visibility is needed are to:

- Demonstrate adherence to compliance and security requirements
- Intercept and record live traffic when mandated
- Verify compliance with service-level agreements (SLAs) and provide actionable data to take corrective actions

Traditional approaches to network traffic visibility have used a purpose-built matrix network to which the monitoring and analysis tools are connected. Figure 4 shows the traditional approach to network traffic monitoring.

Figure 4. Traditional Approach to Network Monitoring

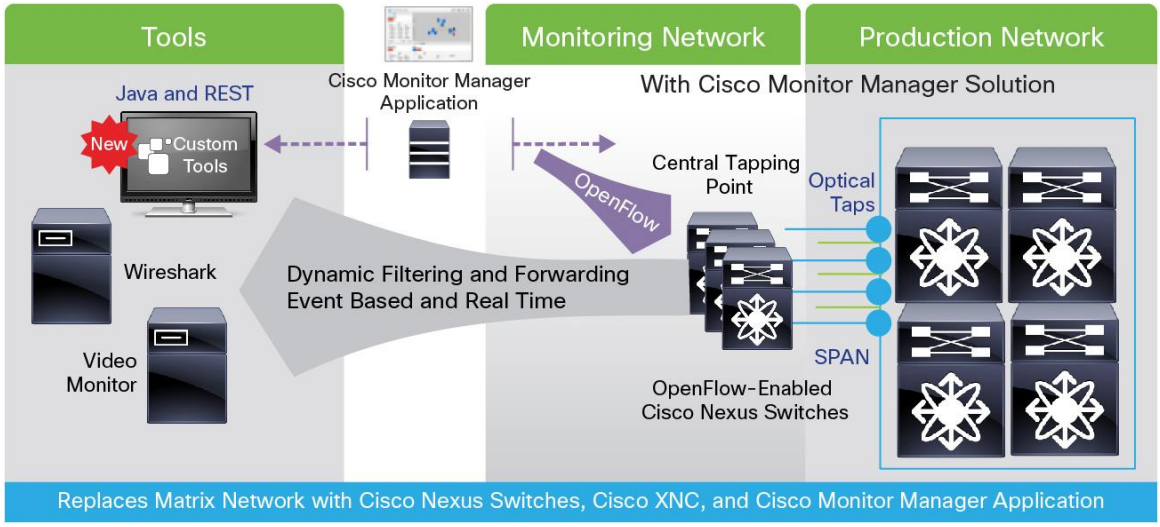


The traditional approach poses three primary challenges:

- 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, and so they cannot act in event-based ways 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.

Cisco's solution uses Cisco XNC, Cisco Monitor Manager, and one or more OpenFlow-enabled Cisco Nexus® 3000 Series Switches to help customers build a tapping environment. The traffic is tapped into this bank of Cisco Nexus 3000 Series Switches using either optical taps or Cisco Switched Port Analyzer (SPAN). However, the presence of Cisco XNC makes it possible to filter and forward the right traffic to the monitoring tools. Also, with the representational state transfer (REST) API support, filtering and forwarding rules can be created or modified dynamically - based on business logic - to allow real-time visibility. Figure 5 shows the Cisco Monitor Manager solution.

Figure 5. Cisco Monitor Manager



Features of the Cisco SDN Solution with Cisco XNC and Cisco Monitor Manager

Table 1 presents the main features of Cisco Monitor Manager.

Table 1. Cisco Monitor Manager Features

Cisco XNC with Cisco Monitor Manager Network Application Features	
Functional Area	**Feature Description**
Configuration	
GUI	Cisco XNC with the Cisco Monitor Manager application provides a web-based GUI for management of all configurations and functions. The GUI provides access features, including: • Topology and device management and assignment of port type • Mapping of the ports to the end monitoring or analysis tools • Configuration of filters to match traffic according to business needs • Set up of traffic flows from network edge ports to tool delivery ports • Event logging and troubleshooting • Flow and port statistics details • RBAC user and role management
Northbound API	The Cisco XNC and Cisco Monitor Manager REST-based API provides access to all functions that can be performed through the GUI.
Traffic Delivery (Basic)	
One-to-one connection	Establish a one-to-one connection from an edge network port to a tool delivery port across the network with no oversubscription.
One-to-many connection	Establish a one-to-many connection from an edge network port to multiple tool delivery ports.
Many-to-one connection	Establish a many-to-one connection from multiple edge network ports to a single tool delivery port.
Combination	One-to-one, one-to-many, and many-to-one connections can be established for different flows at the same time in the same monitored network.
Port-speed adaptation	One-to-one, one-to-many, and many-to-one connections can be established between ports with different speeds. For instance, a 40-Gbps port can deliver traffic to a 10-Gbps tool port to allow use of traditional tools over high-speed production networks interfaces.
Symmetric load balancing	Symmetric hashing based on Layer 3 (IP address) information or Layer 3 and Layer 4 (protocol and port) information can be configured to load balance the traffic to multiple monitoring tools.
Failure resiliency	In the event of path failure, each flow is automatically rerouted to an alternative path by the controller. If rerouting is not possible, an event is logged.

Cisco XNC with Cisco Monitor Manager Network Application Features	
Traffic Delivery (Advanced)	
Packet filtering	Traffic forwarding is based on the full flow specification, allowing detailed traffic filtering to limit the traffic to the delivery port to just what is strictly necessary.
VLAN tag rewrite	The original VLAN tag can be changed from the edge port to the delivery port either through the filter mechanism or by tagging at the edge port.
VLAN tag insertion	An additional VLAN tag can be added to the original packet to be delivered, allowing a tool to identify the origin of the traffic.
Q-in-Q support	If the packet is already tagged, Cisco XNC with Cisco Monitor Manager can add a second tag that allows the user to preserve the original tag information and also identify the edge tap and SPAN port from which the traffic is received.
Time stamping*	Packets can be time stamped using Precision Time Protocol (PTP) with nanosecond accuracy for compliance, troubleshooting, and application performance management.
Packet truncation*	Packet payloads can be stripped for security and compliance purposes. The minimum packet length is 64 bytes, and the user can specify the number of bytes to be retained. The packet payload will be truncated beyond the specified byte size and delivered to the monitoring tools.
Network Design	
Multilevel design	Cisco XNC with Cisco Monitor Manager can support multiple Cisco Nexus 3000 Series Switches connected in any topology. Analysis and monitoring devices can be connected anywhere in the topology. Typical tapping network architectures are: • Two- or three-level networks (edge, distribution layer [optional], and core) in which the delivery ports are connected to the core switches • Nonblocking leaf-and-spine architectures, in which both the edge and the delivery ports are connected to the leaf switches
Port-type assignment	Ports must be designated as edge tap or SPAN (input) or delivery (output) ports to be used to configure network connections. This feature, in combination with RBAC, increases network security.
Inter-Switch Links (ISLs)	Ports that connect switches are self-discovered and do not require additional type configuration. ISLs can use individual ports or PortChannels.
Load balancing	Data paths are evenly spread across available equal-cost links.
Loop prevention	Built-in logic prevents creation of network loops. This feature supports one-to-one, one-to-many, many-to-one, and many-to-many connection policies.
Scalability	Cisco Monitor Manager can support up to 40 switches and 2000 edge and delivery ports per instance.
High availability	Cisco XNC supports high availability through active-active clustering. In Cisco XNC Release 1.6, up to five instances can be part of the same cluster.
Security and Operations	
Role-based access control (RBAC)	Each individual port can be exclusively assigned to one or more user groups.
Logging	Cisco XNC provides system logs as well as user audit logs. In addition, it supports different logging levels depending on system needs.
Path rerouting to help guarantee delivery	If traffic is critical, data loss can impair compliance. In this case, if a failure occurs, the data flow is automatically rerouted using an alternative network path to prevent data loss and to meet compliance requirements.
Cisco Monitor Manager Components	
Cisco XNC and Cisco Monitor Manager application	Minimum system requirements: • 64-bit Linux operating system (Fedora, Ubuntu, or Red Hat) • 8 GB of RAM, 6-core CPU, and 40 GB of free space in the partition in which the controller will be installed • Java Release 1.7 (For complete system requirements, please refer to the Cisco XNC Deployment Guide.)
Cisco Nexus Switches	Cisco Nexus 3000 Series Switches Cisco Nexus 3100 platform Cisco Nexus 5548P and 5548UP Switches Cisco Nexus 6001 Switch

* Functions available only with Cisco Nexus 3500 Series Switches.

Conclusion

The Cisco XNC with Cisco Monitor Manager solution offers customers a secure and low-risk approach to introducing SDN into their network environments. In addition, as other Cisco Nexus Family platforms start supporting OpenFlow and the Cisco Open Network Environment (ONE) Platform Kit (OnePK™), customers will have the flexibility to choose among various platforms according to their business requirements. With the hybrid SDN approach used by Cisco XNC, customers can use the local control plane and the external controller's capability to make their networks programmable and application aware.

For More Information

For more information about Cisco XNC, please visit http://www.cisco.com/go/xnc.

- Cisco Monitor Manager data sheet: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps13397/ps13400/data_sheet_c78-729452.html.
- Cisco Monitor Manager solution brief: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/extensible-network-controller-xnc/solution-overview-c22-729753.html.
- Ordering information: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps13397/ps13400/guide-c07-729755.html.
- Cisco Monitor Manager implementation quick-start guide: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/extensible-network-controller-xnc/guide-c07-731460.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.

Printed in USA C11-729757-01 06/14