Core Networking and Security
Scott Hogg



# Using SDN to Create a Packet Monitoring System

Packet-level Monitoring Use Case with Cisco XNC and Monitor Manager

*By Scott Hogg on Sun, 12/15/13 - 9:31am.*



Because of the limitations of SPAN/monitor ports on switches, organizations have turned to using taps and packet monitoring switches. These solutions can be expensive which has lead companies to look for alternatives. Establishing a packet monitoring system is one of the use cases for Software-Defined Networking (SDN). This solution uses lower-cost network switches with a SDN controller to allow for simple and dynamic configuration of a packet monitoring and analysis system.

## Limitations of SPAN and Monitor Ports:

Lack of visibility into Information Technology (IT) systems is a major issue. Network administrators have struggled with monitoring their data-plane traffic flowing across their networks. NetFlow can provide some high-level visibility into the flow data, but lacks the packet decode details required for some analysis or troubleshooting. Network administrators have suffered from the limitations of Switch Port Analyzer (SPAN) and port-mirroring technology within the Ethernet switches. Further exacerbating the problem is other IT groups that also want to be able to perform packet captures on the network. The security administrators and the systems administrators are often competing for the limited SPAN capabilities in the switches.

An alternative is to use a packet monitoring matrix switch. These switches connect to the various monitoring points within the network using their “monitor ports”. The “monitor ports” can connect to SPAN sessions or to optical/copper taps placed around the network topology. These packet monitoring switches also connect to the monitoring and analysis applications and tools using their “tool ports”. The “tool ports” can be anything from an Intrusion Detection System (IDS) to a Web Application Firewall (WAF) to a protocol analyzer. These switches are equipped with special programmability that allow the monitor traffic to be forwarded to the analysis tools using a variety of configurable logic. However, the downside of these products is that they can be quite expensive. It is not uncommon for an organization to spend $50K to $100K or more to obtain these switches and get them all set up correctly. Therefore, many organizations have delayed investing in these solutions because of cost.

## Using SDN for Packet Monitoring:

Software-Defined Networking is an approach to networking that separates the control plane from the forwarding plane to support virtualization. SDN is a new paradigm for network virtualization and how network traffic is forwarded across a network based on advanced policies. To learn more about the potential of SDN, check out the NWW Digital Spotlight on “The Promise of SDN”.

An emerging alternative for creating a packet monitoring overlay network is to use a Software-Defined Networking (SDN) system. SDN systems use commodity or virtualized network switches controlled by a sophisticated centralized software-based controller to create new ways of handling network traffic. In this way, the low-cost switches can connect to the points in the network where the data packets will be gathered.

### About Core Networking and Security

Scott Hogg is the CTO for Global Technology Resources, Inc. (GTRI). Scott provides network engineering, security consulting, and training services to his clients, focusing on creating reliable, high-performance, secure, manageable, and cost effective network solutions. He has a B.S. in Computer Science from Colorado State University, a M.S. in Telecommunications from the University of Colorado, along with his CCIE (#5133), CISSP (#4610), among many other vendor and industry certifications. For the past 15 years Scott has been working with IPv6 technologies. Scott is the author of the Cisco Press book IPv6 Security and has given numerous presentations and demonstrations of IPv6 technologies. He is also currently the Chair Emeritus of the Rocky Mountain IPv6 Task Force.

RSS E-Mail

### Most Discussed Posts

Did Microsoft reach into your PC to stomp a botnet?
6 comments · 8 hours ago

Boycotting RSA Conference is a misplaced endeavor
9 comments · 10 hours ago

The management and monitoring tools will also be connected to the low-cost switches. The SDN controller is used to direct the traffic from the various monitor ports to the tool ports based on the configuration in the controller. This creates an overlay monitoring network that is out-of-band (OOB) from the normal traffic paths. Therefore, the amount of traffic that this monitoring network is handling does not adversely affect the production data paths.

### Cisco's SDN and Monitor Manager Solution:

Cisco Systems has been developing their own SDN controller systems based on their Open Network Environment (ONE) Platform Kit (onePK) architecture. Cisco has now produced their Open Network Environment (ONE) Controller and many of their network devices support the onePK APIs for communications between the controller and the switches. This presentation describes several of the use cases for the ONE Controller and includes the "Conventional Monitor Matrix Solution" on slide 9.

Cisco also offers their eXtensible Network Controller (XNC) which is targeted at enterprises. The Cisco eXtensible Network Controller (XNC) has the ability to have several other applications plugged into it to give it even more functionality. Here is a video that describes the use of the XNC. One of those XNC plug-ins is the Monitor Manager application. This document covers the Cisco Extensible Network Controller with Cisco Monitor Manager Solution: Increase Network Traffic Visibility.

This Cisco solution utilizes Nexus 3000 switches as the network elements that are controlled by the XNC Monitor Manager application. These switches are recommended for this use case because of their lower cost, high performance, support for 1/10/40Gbps interfaces and very low latency. Therefore, with these Nexus 3000 switches and the Cisco XNC with the Monitor Manager application you can create a network visualization capability for cheaper than a traditional packet monitoring switch. Purchasing these products would jumpstart your organization's journey into using SDN.

### Other Vendor's SDN Network Monitoring Systems:

There are other vendors that supply SDN solutions that are capable of creating a packet monitoring capability.

Big Switch has their Big Tap solution.

Arista Networks switches running their Extensible Operating System (EOS) have the capability to perform what they call Data ANalyZer (DANZ) functionality. ExtraHop and Arista have partnered to create a Persistent Monitoring Architecture which combines the Arista switches DANZ and ExtraHop's Context and Correlation Engine (CCE).

Microsoft has their DEMon (Distributed Ethernet Monitoring) monitoring network that uses low-cost switches and an OpenFlow controller.

There are also the traditional packet monitoring switch manufacturers who are starting to get into the SDN market. Companies like Gigamon, IXIA/Anue, cPacket, and VSS Monitoring are working to insert their products into the SDN conversation.

### Summary:

It is apparent that SDN will continue to have an impact on the way networks have traditionally been designed. Network packet monitoring is just one of the use cases of SDN. SDN is having a disruptive effect on this market segment and the vendors who have offered these products in the past are having to change their product directions because of SDN. If your organization has delayed deploying a packet monitoring solution because of the high cost of packet monitoring switches, then maybe these SDN solutions will allow you to create this capability for less capital expense. Whether you use a SDN solution or use a traditional packet monitoring switch, having network visibility is key to operating a modern networked environment.

Scott



**Tags**

Network Management Cisco controller MM monitor monitor manager SDN Software Defined Network span XNC

Net Neutrality: You need to get involved
20 comments · 7 hours ago

Windows 8.1's next rebuild has leaked
1 comment · 13 hours ago

The Cybersecurity skills gap is worse than you think
5 comments · 1 day ago

### Blog Roll

**Hogg Networking**
*http://www.hoggnet.com*

## Recent Blog Posts

- iPhone + Luxi = an amazing light meter
- CenturyLink Bundles SMB Hosted VoIP With Cloud Services
- “Astonishingly accurate” optical clock could be new world time standard
- Gmail outage coincided with Google Site Reliability team's Reddit AMA
- How Microsoft can save itself in the mobile world
- Teacher’s online safety experiment takes trollish turn
- The Net Neutrality explanation you've been waiting for, courtesy of The Colbert ...
- Why VMware bought AirWatch
- Switching highlights Juniper's Q4
- Gigamon's Netflow Generation app should prove useful