Best Practices for Utilizing Network Monitoring Switches in Cisco Environments

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Ixia

March 2013

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Best Practices for Utilizing Network Monitoring Switches in Cisco Environments

Table of Contents

Best Practices for Utilizing Network Monitoring Switches in Cisco Environments

Executive Summary

As networks expand and the criticality of the applications and services they deliver climbs, network planning, management, and security teams are increasingly turning towards network monitoring switches as a key element within monitoring architectures. In parallel, monitoring switches are maturing rapidly, adding advanced features to meet specific packet-based monitoring requirements.

Cisco Systems® offers advanced network equipment that commonly comprises enterprise network infrastructures and creates specific needs and opportunities that must be accommodated within any monitoring strategy. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) paper reviews specific challenges with deploying packet-based monitoring in Cisco-based networks and examines how the Ixia Anue Net Tool Optimizer® solution can be used to meet those needs.

Evolution of Packet-Based Monitoring

Few would question the value and utility of analyzing packet streams as an essential method for both network and security management. Use cases range from application awareness in performance monitoring to data loss prevention, from unified communications quality measurements to intrusion detection and prevention, and from regulatory compliance monitoring to deep protocol analysis and troubleshooting. EMA research indicates that a steadily growing number of packet inspection-based monitoring and management product types are being deployed in enterprises worldwide, resulting in a continuously growing demand for packet streams.

Network monitoring switches collect packet streams and distribute them, along with filtering and grooming as necessary, to multiple packet inspection and analysis tools.

With this growth in the use of monitoring tools have come some significant challenges, both at a technical level as well as at a business/cost level. Network infrastructure elements are restricted in the number of copies of packet sequences and streams they can deliver, and in a growing number of cases this number of copies is less than the number of potential analyzers. Further, sustained growth in network bandwidth and network usage volumes is pushing network and security operators towards purchasing monitoring tools that have been upgraded for high network speeds, such as 10G and 40G Ethernet, and which cost significantly more than products rated for lower speeds. These two factors have driven interest in a category of solutions known as network monitoring switches, whose primary role is to collect packet streams from network TAPs (Test Access Points) and SPANs (Switch Port Analyzers) and distribute them, along with filtering and grooming as appropriate and necessary, to multiple packet inspection and analysis tools/consumers.

The latest generation of network monitoring switches, such as the Ixia Anue Net Tool Optimizer (NTO), has been designed to provide substantial flexibility and control in managing packet streams for network and security monitoring. Such solutions commonly provide simple aggregation, port speed conversion, and multiplexing/broadcast features, so that multiple tools may receive the same packets and/or a single tool can receive packet streams from multiple sources. More advanced features include the ability to slice and filter packets, remove duplicate packets, add port identities and timestamps, strip encapsulation headers, and more.

Packet-Based Monitoring for Cisco Environments

While there are many manufacturers and providers of network infrastructure equipment, the globally acknowledged market leader is Cisco Systems. Cisco's product lines include routers and switches for the network core, distribution, and access layers. As a result, network management and security professionals are commonly working in and around Cisco equipment when planning and deploying packet-based monitoring products and technologies.

Along the way, practitioners encounter a number of challenges that will exist regardless of which manufacturer's equipment is in use, but also some that are specific to Cisco products and Cisco-based networks. For instance, challenges exist with deciding where and how to instrument high density, rack-based computing clusters for packet monitoring, some of which are simply related to scaling challenges regardless of networking equipment, but some more specific to Cisco Fabric Extender (FEX) deployments. There are port mirroring (SPAN) limitations to many network devices, and some that are specific to Cisco switches.

Following are four key use cases where specific challenges with monitoring Cisco-based networks are discussed, including how the Ixia Anue NTO can be used to ensure optimal results.

Addressing Limitations of SPAN

While there are a number of ways to get streams of packets out of a networking infrastructure for the purposes of monitoring, the use of SPAN (a.k.a. port mirroring) is very common. SPAN allows the configuration of two ports per switch for generating a copy of switch traffic for the purposes of monitoring and troubleshooting. Within Cisco networks, SPAN is available today on most all Catalyst and Nexus switches.

There are a number of challenges represented by the use of SPAN, however. Following are some of the most common, and the ways in which they can be overcome:

1. The design limitation of two SPAN ports per switch means that only two monitoring devices can be connected directly to any one switch at any time. Rather than limit the number of monitoring devices that can be deployed, use of a network monitoring switch such as the Ixia Anue NTO facilitates the sharing and distribution of SPANs to multiple analysis consumers.
2. Switch backplanes can handle far more traffic volume than outbound ports configured as SPAN ports, so it is possible to exceed the capacity of the SPAN port, resulting in dropped packets and missed visibility. Further, in some switches a 10G SPAN port can only effectively deliver 6-7 Gbps in actual traffic due to switch architecture and design. Overcoming this problem may mean not using SPAN in the first place, and instead turning towards TAPs as a means to gather data, which in turn will increase the number of physical layer packet collection devices and streams. In order to re-aggregate those streams, a network monitoring switch or other aggregation device will be required.

Key technical and logistical limitations of SPAN can be overcome by using network monitoring switches

3. If more than one switch port is being routed to the SPAN, it is likely that there will be duplicate packets (as many as 50% duplicates!) in cases where traffic is inbound on one monitored port and outbound on another monitored port. Packet de-duplication is a common feature among

packet analysis monitoring products, however this increases processing load during the monitoring process. An alternative approach is possible using network monitoring switches, which can de-duplicate packets at wire speed before handing the packet streams off to the monitoring tools, and thus increasing inbound capacity of monitoring tools by as much as 50%.

It is worth mentioning here that Cisco provides functionality called VLAN Access Control List, or VACL for short, which can be used in a similar fashion to SPAN. This is a useful mechanism for helping to manage the granularity of switch traffic to be monitored down to specific traffic types or VLANs, and thus avoid potential overflow situations. But there is a downside – VACLs, if not configured properly, can create significant switch CPU load. Some organizations require rigorous change board review for VACL use due to adverse prior experiences. So VACLs can definitely help, but must be used judiciously!

Monitoring Virtualized, n-Tier Architectures

The introduction of server virtualization has opened a brand-new world of flexibility and scalability for deploying applications and workloads, including new options for clustering and n-tier architecture deployment. But along with these advantages has also come the disadvantage of lost visibility. Within a virtual host, network traffic can traverse the intrinsic virtual switch from one VM to another and never be visible to the outside world. This blind spot creates a barrier to both performance and security visibility, and negatively impacts troubleshooting processes.

Cisco Systems provides highly optimized compute platforms that leverage server virtualization within its UCS product line, and also offers hypervisor–independent distributed virtual switching via the Nexus 1000V. There are a number of helpful capabilities with the Cisco Nexus® 1000V that are of great value for network and security monitoring. In particular, the Nexus 1000V supports SPAN functionality, so that any VM-to-VM traffic can be mirrored out a physical port for packet analysis and monitoring. Network monitoring switches such as the NTO can be used to collect and aggregate such SPAN traffic from multiple locations in physical server clusters or racks, providing a single point of access for monitoring tools.

Network monitoring switches can aggregate SPANs from multiple Nexus 1000V switches and strip VN-Tags in VN-Link settings

Part of Cisco's approach to scalable and predictable virtual switching can also introduce new challenges for packet monitoring. Cisco's VN–Link solution adds VN-Tags, which are encapsulations of virtual machine traffic allowing the same physical address to be served both inbound and outbound on a single physical port in an external physical switch. Unfortunately, VN-Tags obscure the true address and identity of the encapsulated traffic, and must be stripped as part of packet monitoring and analysis. Such tag stripping can be performed by some packet analysis and monitoring products, however as with de-duplication, this additional processing load can also be offloaded to network monitoring switches such as the NTO.

Packet Monitoring in Top of Rack (ToR) Switching Architectures

In high density computing environments, the predominant network architecture choices are End of Row (EoR) switching and Top of Rack (ToR) switching. Cisco offers both solutions, and specifically offers its Fabric Extender (FEX) solution for ToR applications, as a means to consolidate and direct network traffic and connectivity back into the core data center network. The most advanced Cisco solutions come from combinations of the Nexus 7000 series in the core, complemented by Nexus5K aggregation switches and Nexus 2K fabric extenders on top of each rack. With so many physical links involved, as well as even more virtual network links within virtual server hosts in each server rack, deciding how and where to instrument for packet monitoring can be a nontrivial challenge.

In particular, there may be a desire simply to monitor in the aggregation layer, using SPAN from the Nexus 5K. With 968 Gbps of backplane capacity, the Nexus 5K can quickly surpass packet volumes supported by even leading edge 10G and 40G–rated monitoring tools. A best practices alternative would include tapping links coming from the Nexus 2ks into the 5K and using a high-end network monitoring switch such as the Ixia NTO to aggregate and tune this traffic for monitoring systems.

Monitoring high-density rack computing infrastructure is a challenge – network monitoring switches deployed alongside ToR solutions like the Nexus 2k/5k provides a practical option

Further, some traffic may never reach the aggregation tier, instead staying within individual racks. When visibility is needed within each rack, it is instead recommended to tap pNIC links or create SPANs from virtual switches servicing the virtual hosts in the rack (as described above), and then aggregating those streams through a network monitoring switch placed within each rack.

Special Practices for Security Monitoring Use Cases

The scenarios described above all reflect situations that are applicable to network and application monitoring as well as security monitoring. There are some cases, however, that are more specific to one monitoring discipline or another, such as packet-based security monitoring. Following are two specific examples, involving the use of IDS/IPS and firewalls:

1. The purpose of an intrusion prevention system (IPS) such as Cisco's ASA IPS, ISR IPS, or IPS 4k, is to recognize threats within network traffic streams, identify them to security operators, and even to take a direct action to interrupt traffic flows. One of the greatest concerns with deploying such technology is accidental interruption of legitimate traffic. The answer to this is to use training so that the IPS can build an understanding of normal versus abnormal traffic patterns and activities. But since IPS products have a non-zero impact on overall performance, it is often preferable to first deploy an IPS out-of-band, rather than in-line whereby all traffic must flow through it. Network monitoring switches such as the NTO can be very useful in setting up training configurations, so individual or multiple flows of live traffic can be directed to an IPS without affecting production activity. Once training is complete, the IPS can be deployed in-line for regular operations.
2. The most common in-line network security devices are firewalls, such as the Cisco ASA NG Firewall. Firewalls do stateful packet inspection in order to recognize and block categories of known risky or threatening traffic from entering at the edge of the network. Firewalls can also create problems, if the rules they are using are obsolete or incorrect. A common technique for assessing rule integrity and firewall performance is to capture packet sequences before and after passing through a firewall and comparing them to determine what has been blocked and how much latency has been introduced. Network monitoring switches such as the NTO are commonly used for such purposes, allowing packet monitoring systems to gain access to the streams before and after a single firewall or multiple firewalls. This is especially useful for service providers

that offer outsourced firewalling services to businesses and who must be able to monitor firewall activity to prove that firewalls are not adversely interrupting legitimate traffic or creating undue delivery delays. This configuration can also be useful for testing new firewall configurations to ensure proper traffic delivery as well as firewall CPU loading.

EMA Perspective

Packet-based monitoring is here to stay and its use is growing steadily. Whether the purpose is security monitoring, compliance monitoring, network performance analysis, or application performance visibility, the growing appetite for packet analysis means that IT professionals must seek new approaches to establishing reliable, flexible, and scalable access to network packets. When applying these approaches to Cisco–based network infrastructures, practitioners must accommodate both general architectural challenges as well as Cisco-specific products and feature sets.

The Ixia Net Tool Optimizer is commonly deployed to overcome monitoring challenges that are general in nature, but also those specific to Cisco-based networks.

The growing popularity of network monitoring switches such as the Ixia Anue Net Tool Optimizer is testament to their utility in effectively overcoming such challenges. The NTO, in particular, has been deployed in many different ways to accommodate limitations of SPAN, instrumentation in virtualized n-tier architectures, monitoring of high density rack-based compute environments, and special needs of individual monitoring and control technologies such as firewalls and IDS/IPS. EMA recommends that IT infrastructure practitioners look to products such as the NTO to put them in the position for delivering packet-based visibility both in the short term as well as into the future.

About Ixia

From the lab to the network to the cloud, Ixia solutions optimize networks and data centers to accelerate, secure, and scale the delivery of applications and services.

Ixia Network Visibility Solutions make monitoring today's complex networks stunning simply by optimizing the visibility, control and performance of network traffic. The award-winning Ixia Anue Net Tool Optimizer® (NTO) is deployed in minutes and forms an intelligent layer between the network and monitoring tools enabling network and security engineers to aggregate and filter data, load-balance network traffic, and spot suspicious activity. The Anue NTO boosts productivity and works with current monitoring tools to save time and money. To learn more, go to www.ixiacom.com or send an email to visibility@ixiacom.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2637.032813