Accolade Technology

Network Monitoring Appliances (NMA)

What are they and how can they perform better?

Introduction

The phrase “network monitoring appliance” is a generic term that can be used in many contexts and is often called by other names. In this paper we consider a network monitoring appliance (NMA) to be any hardware centric device that receives network packets from some other device (e.g. network TAP, Ethernet switch SPAN port) and then analyzes those packets with software for some specific network, security or quality of service related purpose. **Figure 1** provides a high level view of some typical NMAs and their general application categories.

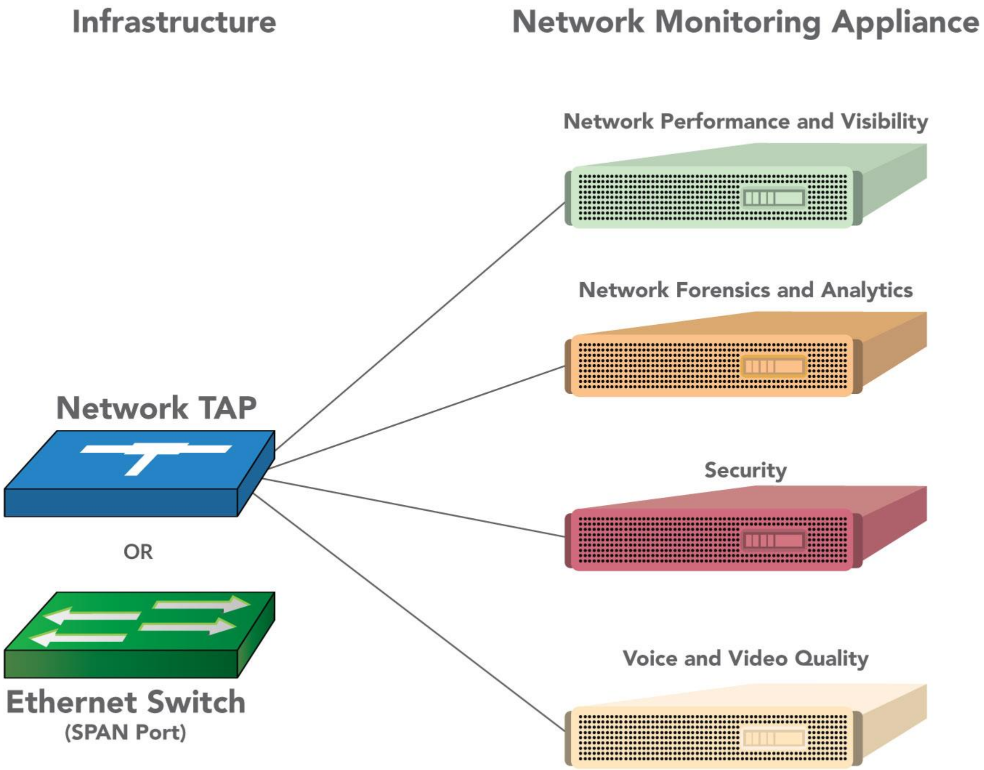
Infrastructure
Network Monitoring Appliance
Network Performance and Visibility
Network Forensics and Analytics
Network TAP
Security
OR
Voice and Video Quality
Ethernet Switch
(SPAN Port)

Figure 1: Network Monitoring Appliances (NMAs)

The purpose of these appliances runs the gamut from tracing a hacker after a security breach, to network troubleshooting, to measuring the quality of voice and video traffic. A common trait of these appliances is they are passive or work in “offline” mode. In other words, they receive packets that have been replicated from the production network-typically by a network TAP or Ethernet switch SPAN port-and therefore are not operating on live traffic.

There is a class of appliance called an "Intrusion Prevention System" or IPS that operates on live network traffic and attempts to identify malicious activity (typically based on some signature or pattern that has been previously identified) and block it. A unique requirement for an in-line IPS is a bypass switch, which "fails open" so that live network traffic is not blocked if the appliance fails. While this type of device could certainly be considered an NMA, in this paper we are more focused on NMAs that capture large volumes of traffic (often include local storage) in an offline mode and do some deep software analysis on the captured traffic. With that definition in mind, an "Intrusion Detection System" (IDS) is more what we are focused on. IPS and IDS however are very closely related and sometimes people lump them together and just call them an IDPS.

Alphabet Soup

Marketing departments and industry analysts routinely coin new terms and related acronyms to spice up the conversation, but these can add confusion if not clearly understood. We will try to demystify some of these terms in order to provide a clearer picture of the market landscape.

Network monitoring appliances (NMAs) are sometimes referred to as "probes" presumably because they are used to *search into or thoroughly examine* the packets which traverse a computer network. While the term "probe" is still occasionally used to reference an NMA it isn't the most commonly used word and thus may not provide the clearest description.

"Network sensor" is another term you might hear to refer to an NMA. This is a descriptive term and it is true that an NMA "senses" the state of network traffic. However, this term is not preferred because it can be easily confused with a wireless network sensor that is used to monitor physical or environmental conditions such as temperature, sound, or pressure.

Sometimes network monitoring appliances are generically referred to as "tools". This is presumably because these appliances come in many flavors and perform various functions such as troubleshooting, security or video quality analysis. This term however is perhaps too generic as it can be applied to almost any piece of hardware or software.

Gartner has coined the term "Network Performance Monitoring and Diagnostics" (NPMD) and even has a magic quadrant to rank vendors in this market. This term is lacking for a few reasons. First it largely ignores the security aspect of the network monitoring market in favor of the troubleshooting or fault isolation aspects. And secondly it also overlaps with the application performance monitoring (APM) market which is less about packet analysis and more about tracking the end-user performance of application components. According to Gartner; "APM differs from NPMD primarily in its focus on monitoring the quality of the end-user's experience via application interactions across all application and infrastructure tiers, including, but not limited to, the network perspective”. To further complicate the matter Gartner has also coined the term “Application-Aware Network Performance Monitoring” (AA-NPM) which contains certain aspects of APM and is considered a subset of NPMD. All of these different categories seek to slice and dice the market across different dimensions but don’t seem to capture the high level essence of what these products provide. Perhaps the easiest and most straightforward way to capture the essence is simply as “network monitoring appliances”. These three words are plenty descriptive. The word appliance clearly communicates that we are referring to something that is hardware centric as opposed to pure software. Appliance evokes the image of something you purchase from a vendor and install in a rack in your network which is precisely what you do with these products. And finally the dictionary definition of the verb monitor is: “*to watch, keep track of, or check usually for a special purpose*”. This definition clearly describes that these appliances *watch* the traffic in a network; *keep track of* what is occurring in the network and all for a *special purpose* such as troubleshooting, security or video quality analysis.

We will conclude with our concise definition of a network monitoring appliance (NMA); *a hardware centric device which captures packets from a live network and analyzes them with software for some specific network, security or quality of service related purpose*.

Network monitoring appliance (NMA); a hardware centric device which captures packets from a live network and analyzes them with software for some specific network, security or quality of service related purpose.

Network Packet Broker (NPB)

A discussion of network monitoring appliances (NMAs) would not be complete without some mention of a relatively new category called “Network Packet Broker” (NPB). These devices have been known by various other names such as packet flow switches, matrix switches or network monitoring switches. The last term is probably most descriptive because an NPB is basically a switch that shunts traffic to various NMAs based upon some configured policies as shown in **Figure 2**.

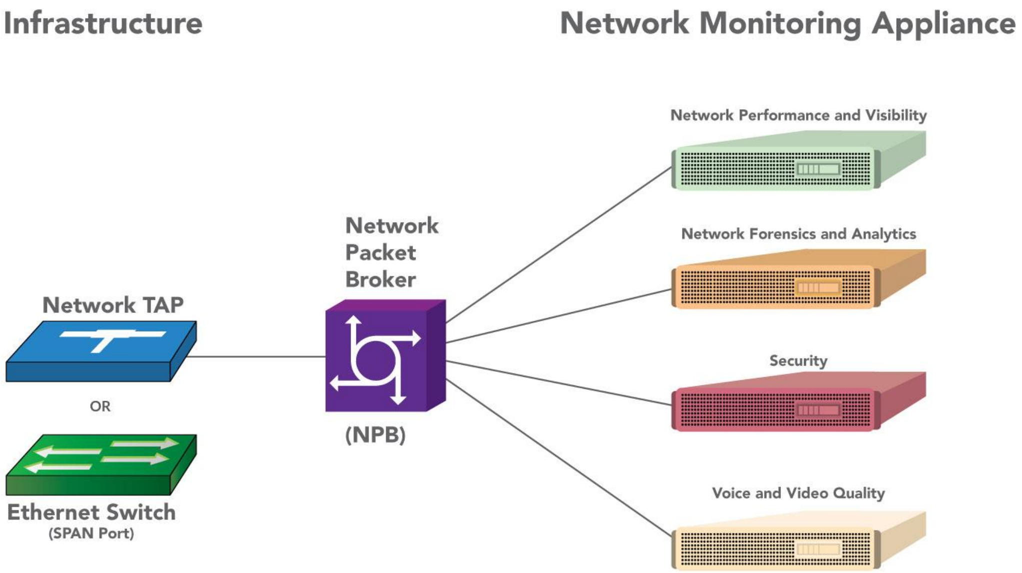

Figure 2: Network Packet Broker (NPB)

NPBs are used in modern enterprise and service provider networks for several reasons. First, due to the sheer number of different NMAs that are being added to existing networks, providing a network TAP for each NMA is sometimes not feasible. And secondly the complexity and scalability requirement of some monitoring infrastructure has far exceeded the ability of Ethernet switches to provide an adequate number of SPAN ports. These forces warrant a migration towards an additional networking monitoring layer that sits between the source of traffic (e.g. network TAP) and network monitoring appliances.

How do I accelerate my network monitoring appliance?

Most NMA vendors rely on industry standard servers from Cisco, Dell, HP, or Super Micro for their appliance hardware and spend most of their R&D dollars on software. This combination of generic hardware and proprietary software is often not powerful enough to handle the deluge of network traffic these appliances receive. This is particularly true as vendors have to contend with 10, 40 and now 100 gigabits of traffic on a single port.

There are different solutions to this conundrum but they are all bounded by at least three fundamental requirements: 1) The solution must fit in to an industry standard server, 2) must not require major modification to the vendor's software and 3) must be cost effective.

Accolade's ANIC line of FPGA-based, hardware adapters meet these three requirements and more. All ANIC adapters are fully PCIe compliant and thus fit seamlessly in to any industry standard server. The adapters come with a well-defined API and their own device drivers which facilitates easy integration with any software application. And they are very cost effective because they limit the need for horizontal server scaling; thereby saving appliance cost, rack space and power.

Furthermore, an FPGA-based ANIC adapter offers the following advantages over a standard NIC.

- **Lossless packet capture** – Each ANIC adapter has adequate onboard memory to absorb any size burst of traffic and therefore never drops a packet.
- **Acceleration Functions** – A variety of pre-processing or acceleration functions such as packet filtering, flow classification and deduplication are performed in hardware.
- **Future proof** – An FPGA is programmable, so as a vendor's needs evolve the ANIC adapter can be reprogrammed (by Accolade engineers) to accommodate new offload and acceleration requirements.

Company Profile

Accolade is the technology leader in high performance, FPGA-based, lossless packet capture and application acceleration adapters. Accolade serves the global network appliance OEM market. Customers integrate the company's ANIC adapters in to their network appliances in order to gain advanced capabilities such as line rate packet capture, time stamping, packet filtering, and flow classification. Established in 2003, Accolade Technology is a privately held company based in Massachusetts with additional offices in Silicon Valley, California and Atlanta, Georgia.

Corporate Headquarters:

124 Grove Street, Suite 315
Franklin, MA 02038
T: 877.653.1261
F: 208.275.4679

Silicon Valley:

980 Mission Court,
Fremont, CA 94539
T: 877.793.3251

South East U.S. Regional:

2997 Cobb Parkway,
Atlanta, GA 30339
T: 877.897.4833

www.accoladetechnology.com