SOLUTION BRIEF

Communications Service Providers
Service Assurance

Enea's* Qosmos* NFV Probe Uses Intel® CPUs for NFV Network Troubleshooting

NFV Probe provides real-time, high-granularity data for traffic going through virtual and physical infrastructure to identify and correct network problems.

Introduction

Virtualized networks offer the ability for communications service providers to develop more agile services that can be commissioned and deployed in minutes, and similarly torn down as quickly. It's the job of the service assurance system to ensure that these services meet service level agreements, and, when problems occur, that network administrators have the data they need to uncover and correct the problems.

Physical network probes have been providing the data required for trend and capacity analysis and for troubleshooting by connecting to network switches and routers to capture packets for analysis. In a virtualized network, these probes miss a significant amount of data traffic that is switched only within the virtualized infrastructure. Qosmos,* a division of Enea* and a member of the Intel® Network Builders ecosystem, has been working with Intel® architecture-based servers to deploy its Enea Qosmos NFV Probe, which collects data from within the virtual environment, giving admins the data they need to troubleshoot their virtualized services.

The Challenge

Service assurance is a critical need for communication service provider (CommSP) networks as they migrate to an infrastructure based on network functions virtualization (NFV). The challenge is that virtual network elements have been added to the physical network, but the hardware-based service assurance infrastructure currently in place in most networks can only track the physical network elements.

Virtualization creates a new intra-server network consisting of logical interfaces to virtual switches. The impact on CommSP networks is growing and could reach levels seen today in data centers, where this traffic between virtual machines (also known as VM-to-VM or east-west traffic) makes up 76% of data center network traffic and is growing, according to the Cisco Global Cloud Index.[1]

Physical probes cannot access these logical interfaces, so they can't capture VM-to-VM communication to monitor functions hosted on the server. The physical probe is also not viable for data flows traversing a virtual overlay network created to connect a VM that is shared across different servers. Additionally, services are not necessarily hosted on a pre-determined or fixed set of VMs. The location and number of VMs can change, making it even harder to track down where specific service components reside and are executed. The inability of probes to access this data makes it harder for network admins to know the origin of the problem that is causing a poor response time, slow network response, or loss of traffic.

Without probes within virtualized networks, the data required to measure quality of service or service assurance is available only in the logs of various systems. Log data are focused on network events and provide very limited visibility at the application level, making it difficult to perform service assurance using only logs. In addition, this data must be collected and manually processed in a time-consuming and error-prone process. The difficulty of the challenge is growing in lockstep with the growth in east-west traffic between virtual machines.

What's needed is an NFVI probe that can help the CommSP map customer experience to actual network traffic on both virtual and physical infrastructure. While it's important to collect data for trending and capacity planning, the primary job of any monitoring solution is troubleshooting, that is, quickly observing the issue without affecting the behavior of the NFVI systems and using this information to isolate the root cause.

In addition to the quality of service (QoS) and service assurance metrics that must be tracked, virtualization brings additional metrics. VNFs can be deployed and perform well. But when other VNFs are loaded on to the server, this can cause contention for compute, network, or memory resources and disrupt performance. Only embedded service assurance monitoring can collect the data needed to isolate these issues.

Qosmos has developed its NFV Probe to fill the gap in the market for data capture and analysis tools for NFV infrastructure and is working with Intel to bring this solution to CommSP networks.

The Solution

The Qosmos NVF Probe is a Linux*-based virtual probe comprising a vSwitch plug-in for packet capture, a VNF for packet analysis, and a database. The NFV Probe identifies data flows using pattern matching and flow correlation algorithms and then captures the appropriate packets and inspects each one up to layer 7 of the OSI model to classify the networking protocols and applications and extract metadata.

Enea's Qosmos NFV Probe Benefits

- High-degree of information granularity for advanced troubleshooting of faults and performance issues
- Fully customizable extraction of traffic information and key performance indicators (KPIs)
- Optimized and dynamic configuration: monitoring can be turned on and off to investigate issues only when needed
- A single monitoring approach for hybrid environments where network services run across both physical and virtual functions
- Data model optimized for correlating network counters (response time, quality of experience, etc.) with infrastructure elements (VMs, containers, domains)
- Provides a view into shadow IT applications and traffic
- Follows NFV standards
- Runs on Intel® architecture hardware

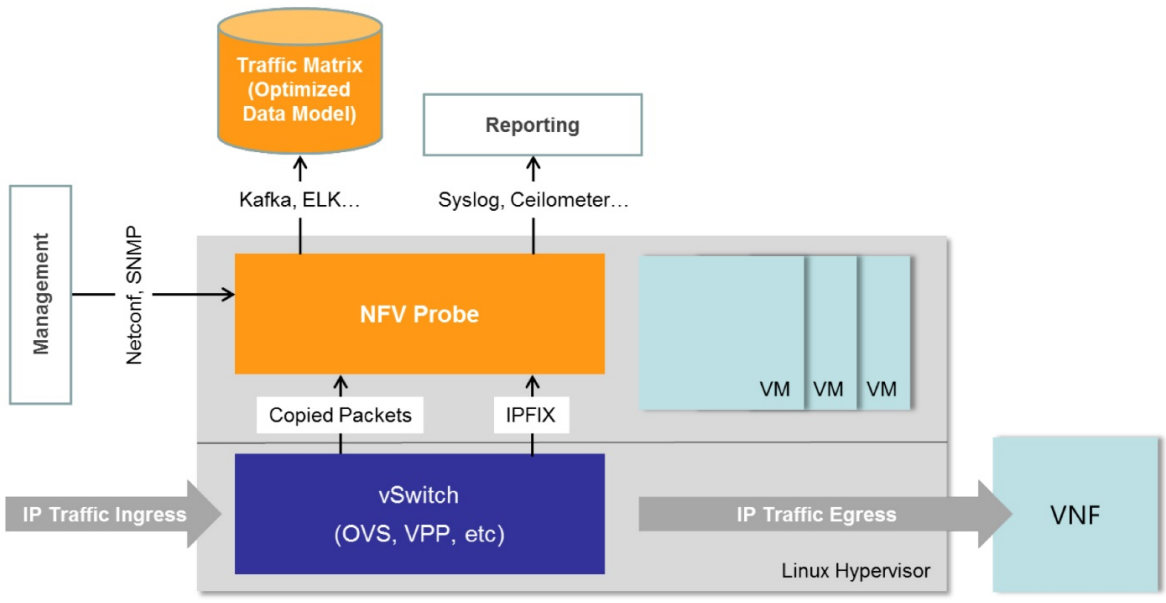
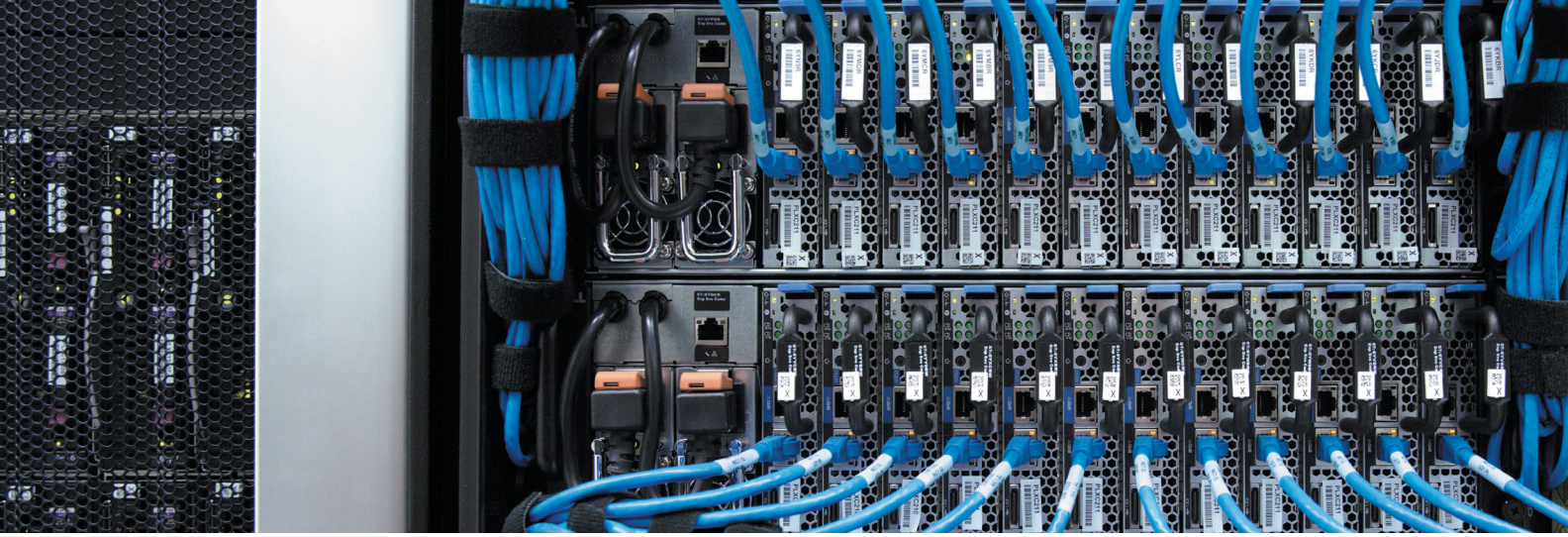


Figure 1. Block diagram of NFV Probe shows its three components: vSwitch plug-in, VNF, and Traffic Matrix data model.[2]

The NFV Probe uses flow monitoring: tracking all of the packets in a particular user's data stream, which it achieves by determining the source and destination IP addresses, the source and destination port numbers, and the protocol in use (which, combined, are called the 5-tuple) for each packet. Flow monitoring is an ideal technology for virtual environments as it provides an end-to-end view of all of the physical and virtual resources used to deliver a specific service to a specific user.



A key element of the NFV Probe is the way it is hooked to the vSwitch. Network administrators can send packet capture requests via the hook, which facilitates the examination of the packet's 5-tuple information, captures the right packets, and forwards them to the NFV Probe for analysis.

Data plane throughput is a critical aspect of plug-in performance, as the probe can examine packets for more than 3,000 protocols and extract any of 4,500 different application metadata elements. The core technology for the NFV Probe is the Qosmos ixEngine,* a deep packet inspection (DPI) engine that can provide real-time, detailed IP traffic classification and metadata extraction. Qosmos ixEngine is used for a range of monitoring applications and also for security applications.

The advantage of utilizing DPI is that the deep understanding that comes from this packet analysis can help to correlate networking issues with potential problems from other resources. This helps network admins troubleshoot a problem to the right source, which could be the network, the VM, the container, the VNF, or any number of other elements. The DPI performance of ixEngine is fully leveraged when connecting to a vSwitch based on vector packet processing (VPP) technology, an open source packet processing technology originally developed by Cisco Systems.* VPP builds on Data Plane Development Kit (DPDK) poll mode drivers.

Another component of the NFV Probe is the Traffic Matrix, which collects the metadata from every captured packet and logs the metrics into a structured data model in a time series database. From this, data visualization tools can be used to obtain a picture of trends and performance problems. The Traffic Matrix stores data from both virtual and physical switches, providing visibility and correlation capabilities across the entire infrastructure.

The Traffic Matrix, by its nature, facilitates data processing such as correlation, aggregation, and filtering for root-cause analysis and troubleshooting. This matrix provides continuous visibility to the existing OSS/BSS systems of both the virtual and physical network elements, and it alleviates the need for manual log collection and aggregation.

Programmable Granularity

The NFV Probe is designed to collect data for trend analysis, capacity planning, and troubleshooting service issues in real time. The NFV Probe features programmable packet capture granularity for each of these functions. Under normal operation, a network manager can collect a low-granularity subset of the data passing through the vSwitch. This provides a large enough data sample to track overall performance or provide insight for NFVI capacity planning.

But the network manager can also set a high-granularity collection mode for mission critical resources and services, or on a service that is experiencing difficulties. Once selected, the probe will collect every packet from all relevant data flows and provide complete metadata for the packets related to that service. This expansive data access gives network administrators the ability to drill down into the data packets to troubleshoot specific service errors. The data can also be sent to offline tools that can provide even more analysis in the event that more structural changes are needed to fix the issue.

Intel CPUs Enable Granular Probes

The use of DPI means the NFV Probe requires high-performance hardware for real-time performance. Qosmos has worked to optimize the NFV Probe on servers using Intel® architecture CPUs because these high performance CPUs provide the capability to run multiple highly granular packet captures. DPI instances run on a logical core, which processes all of the packets in a particular flow. With load dispatcher technology, the NFV Probe is able to distribute data equally across all of the cores, allowing the application to scale performance linearly with the number of available cores.

Enea's Qosmos NFV Probe runs on Intel® Xeon® processors E5-2600. The Intel Xeon processors E5-2600 provide outstanding performance for NFV and virtualized data center applications. These CPUs feature Intel® Virtualization Technology, which provides hardware assist to virtualization software to eliminate virtualization performance overhead in cache, I/O, and memory. Also built into the processors is Intel® Trusted Execution Technology (Intel TXT), a hardware feature that provides security assist capability to improve runtime defenses such as antivirus software.

Conclusion

Enea's Qosmos NFV Probe is bringing service assurance to virtualized networks and infrastructure, providing a valuable solution for tracking VM-to-VM data flows. It gives network administrators the visibility they need to troubleshoot services, but also to compile network trends and plan future capacity needs. Working with the performance of Intel Xeon processors, the NFV Probe is able to leverage DPI technology to provide a view of network conditions that results in fast problem resolution.

About Enea and Qosmos

Enea is a global supplier of network software platforms and world class services. Qosmos, a division of Enea, provides IP traffic classification and network intelligence technology used in physical, SDN, and NFV architectures. Qosmos NFV Probe is based on Qosmos ixEngine, a software development kit used by vendors and integrators in their products sold to telcos, cloud service providers, and enterprises. For more information: www.qosmos.com

About Intel Network Builders

Intel Network Builders is an ecosystem of independent software vendors (ISVs), operating system vendors (OSVs), original equipment manufacturers (OEMs), telecom equipment manufacturers (TEMs), system integrators (SIs), enterprises, and service providers coming together to accelerate the adoption of network functions virtualization (NFV)-based and software defined networking (SDN)-based solutions in telecom networks and in public, private, and hybrid clouds. The Intel Network Builders program connects service providers and enterprises with the infrastructure, software, and technology vendors that are driving new solutions to the market. Learn more at http://networkbuilders.intel.com.

[1] Blog post on Cisco.com: http://blogs.cisco.com/security/trends-in-data-center-security-part-1-traffic-trends
Note: East-west traffic is defined in this study as both VM-to-VM traffic and also traffic between VMs and applications on bare metal servers.
[2] Figure provided courtesy of Qosmos.

0817/DO/H09/PDF ♻ Please Recycle 336417-001US