Network Analytics Probes in the NFV and SDN Era

Publication Date: July 2013

Web Site:
http://www.radcom.com

Table of Contents

Introduction

Network Functions Virtualization (NFV) and Software-defined Networking (SDN) are technologies that will play a critical role in the next generation of telecommunications.

NFV and SDN benefits include cost efficiency, flexibility, ease of scalability and quicker service introduction. The NFV terminology comes from the telco world, while SDN is from the IT domain.

NFV reduces network operator CAPEX and OPEX through reduced equipment, costs and power consumption by transitioning network functions to software-only, COTS hardware with multiple network functions running in a single chassis.

SDN architecture separates the control plane and data plane, making networks more efficient by taking concepts from the IT world. SDN networks are manageable, cost-effective, and easily adaptable to new services.

Network Analytic probes are a critical function in today's telecom networks. Network operators are using probes to analyze traffic on network interfaces and extract intelligence for multiple applications such as customer experience management, service assurance, network performance monitoring, network planning, marketing analytics, call tracing and troubleshooting and many more.

Network Analytic probes will face new challenges once network elements such as Evolved Packet Core (EPC) are transitioned to NFV and SDN. This paper analyzes these challenges and presents some recommendations and solutions. In addition, this paper analyzes how the Network Analytic probes should leverage NFV and SDN technologies to increase operators' agility and efficiency while reducing costs.

Network Functions Virtualization

Network Functions Virtualization (NFV) is a concept introduced by network operators in 2012 [Network Functions Virtualisation – Introductory White Paper]. The European Telecommunications Standards Institute (ETSI) has formed an Industry Specification Group on Network Function Virtualization (ISG NFV). NFV aims to address the challenges of using proprietary hardware appliances in network operators' networks by replacing proprietary appliances with software based solutions on standard servers.

Using proprietary hardware appliances often leads to higher space and power requirements, and requires more specific skills to design, integrate and operate.

The NFV approach is to leverage standard IT virtualization technology to consolidate network equipment types onto industry standard high volume servers, switches and storage.

Some of the benefits of virtualizing Network Functions include:

- Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry.
- Increased speed of Time to Market by minimizing the typical network operator cycle of innovation.
- Availability of network appliance multi-version and multi-tenancy, which allows use of a single platform for different applications, users and tenants. This allows network operators to share resources across services and across different customer bases.
- Targeted service introduction based on geography or customer sets becomes possible. Services can be rapidly scaled up/down as required.

NFV is highly complementary but not dependent on Software Defined Networking (SDN) described below. NFV can be deployed without an SDN being required and vice-versa.

NFV and Network Analytics Probes

The contributors of the NFV Introductory white paper as well as the ETSI ISG have identified network analytics and QoE monitoring probes in their vision as one of the functions that should be transformed from a network appliance to the network virtualization approach (see "Tester/QoE Monitor" in Figure 1).

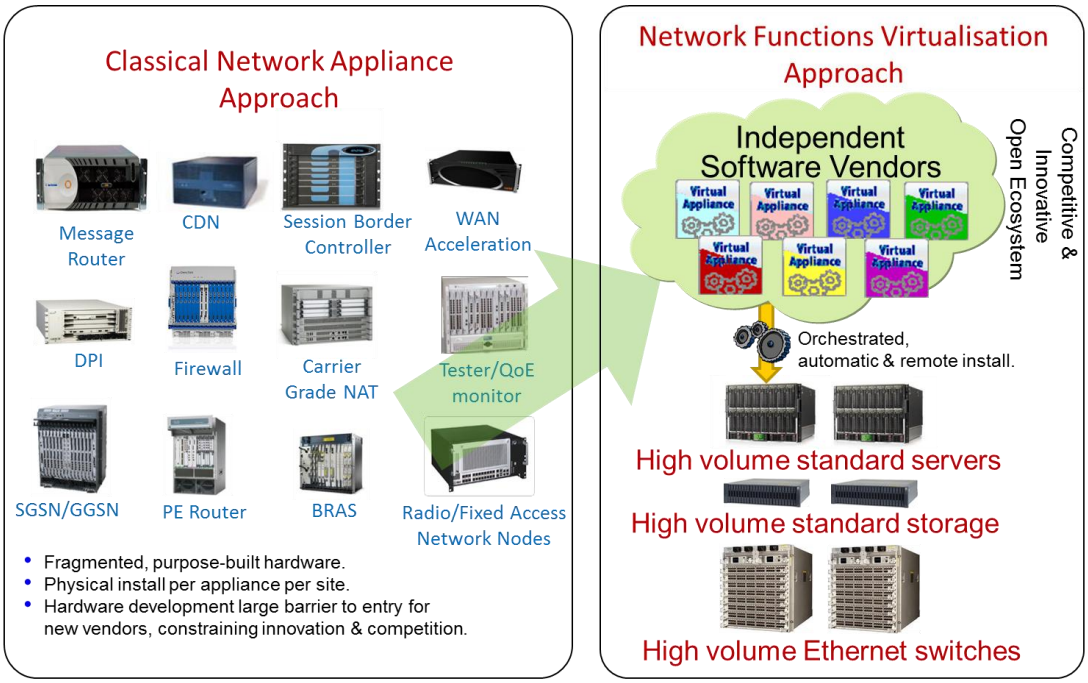

Figure 1: Vision for Network Functions Virtualization

Software Defined Networking

Software-Defined Networking (SDN) is an emerging networking architecture that is dynamic, manageable, cost-effective, and adaptable; making it ideal for the high-bandwidth, dynamic nature of today's applications. It is an approach to computer networking that decouples the system that makes decisions about where traffic is sent (the control plane) from the underlying system that forwards traffic to the selected destination (the data plane).

SDN thus enables the network control to become directly programmable, and the underlying infrastructure to be abstracted for applications and network services.

In SDN architecture, network control is directly programmable because it is decoupled from forwarding functions. Abstracting control from forwarding, lets administrators dynamically adjust network-wide traffic flow to meet changing needs. Network intelligence is centralized in software-based controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch. SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

There are several on-going industry initiatives to standardize SDN. The Open Networking Foundation consortium was formed to promote the development and standardization of SDN. In addition, the International Telecommunication Union (ITU-T) has initiated SDN standardization work. Also, the OpenDaylight Project is a networking and technology industry open-source software project created to facilitate a community-led, industry-supported open-source SDN framework.

Legacy Probe-based Network Monitoring

Traditionally the telecom network probe-based monitoring solutions industry has relied on a combination of hardware and software. Hardware devices are put into the network to either passively monitor signaling and data sessions, or remotely test specific types of technology. Legacy passive probe systems use proprietary dedicated hardware to non-intrusively monitor network links. Passive probes are principally used to monitor signaling protocols, data and media sessions. The probes analyze the traffic, extract intelligence, and measure Key Performance and Quality Indicators (KPIs/KQIs) that provide visibility into network performance and subscribers' quality of experience (QoE).

The solution typically includes a presentation layer which provides reporting, session trace using ladder diagrams, full protocol decode, detailed network analysis and visualization, service impact, and customer SLA data provided via a graphic user interface.

Typically, network analytics solutions utilize taps and aggregators to deliver the packets from the network to the probe itself. A network tap is a hardware device which provides a way to access the data flowing across a network. A tap inserted between two network elements passes all traffic through unimpeded, but also copies that same data to its monitor port, enabling the probe to listen. In addition, the solution uses Port Aggregators to combine traffic from multiple network links to a smaller number of links and copy the traffic to one or more monitoring probes. An example of a probe-based monitoring architecture for an LTE network is shown in Figure 2.

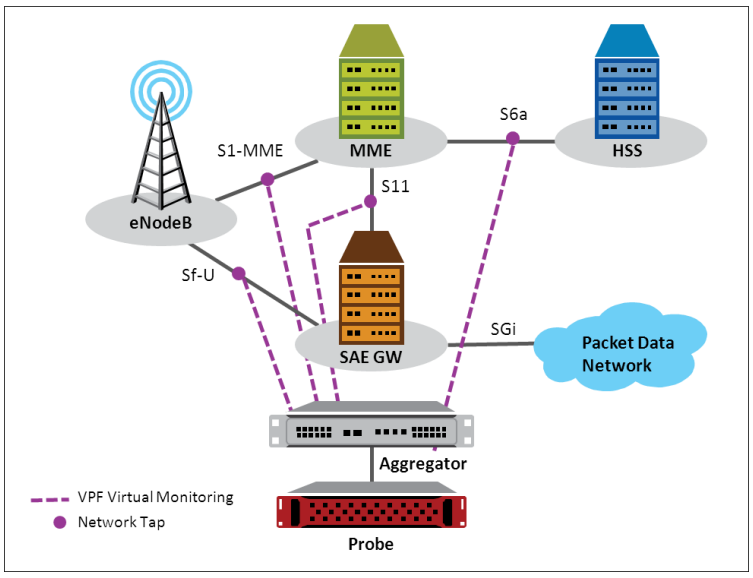

Figure 2: Legacy Probe-based Network Monitoring

Such a solution provides several benefits to network operators by providing the intelligence needed to improve users' QoE, reduce network downtime, optimize network planning and reduce engineering and support costs.

The current model requires operators to invest in hardware and software as their network capacity grows, in order to monitor the growing amount of traffic. Additional taps, aggregators and probe appliances must be deployed to capture traffic from the growing number of network interfaces and to analyze the additional traffic.

As detailed in the following sections of this paper, NFV and SDN technologies can be utilized to reduce the CAPEX and OPEX associated with network analytics monitoring solutions, as well as to improve agility and flexibility.

Network Monitoring in the World of NFV and SDN

Monitoring Traffic between Legacy Network Elements with Virtual Probes

From the early days of the NFV, Network Analytics and QoE monitoring probes have been part of the network virtualization vision. Operators who choose to transition the Network Analytics function from physical probes to a virtual function enjoy several benefits.

Operators have the ability to run the virtual probe function (VPF) and the 3rd party network function on the same physical server, removing the need for proprietary probe appliances, as shown in Figure 3. This leads to better utilization of hardware, and significant reduction of hardware, rack space, power and IT staffing costs.

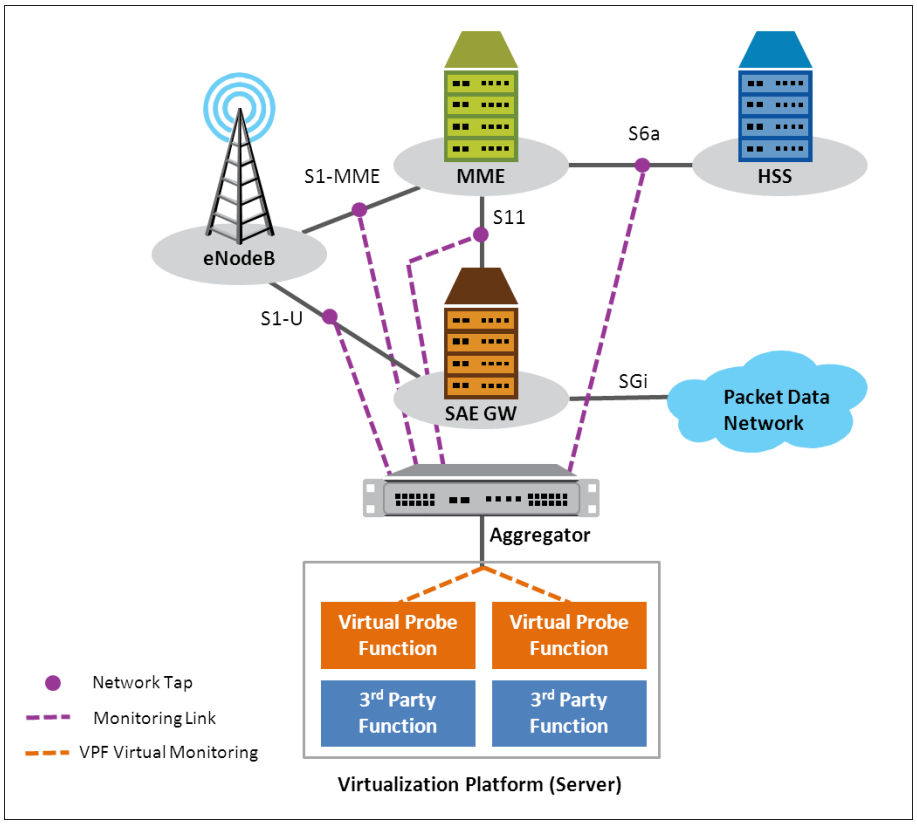

Figure 3: Monitoring Legacy Network Elements with Virtual Probes

Moreover, operators' agility and efficiency is greatly improved. Legacy probe-based proprietary hardware requires a much longer cycle for operators to design, integrate and operate. Hardware-based appliances reach end of life faster, requiring the procurement cycle to be repeated.

Using a virtual probe function, operators can rapidly increase the network analytics capacity when needed, by adding virtual probe instances on additional virtual machines on the same hardware.

This approach allows operators to align network monitoring processing capacity to business needs in a timely manner, while keeping CAPEX and OPEX under control.

For details on MaveriQ-VPF, RADCOM's Virtual Probe Function implementation – see the section "RADCOM's MaveriQ Solution" below

Monitoring Traffic Between Virtual Network Elements with Legacy Probes

Virtual Network Elements include application software for various network functions, residing on Virtual Machines. Using virtualization, a number of different network functions can reside on the same physical server.

Operators implementing NFV typically require multiple network functions at a single physical site, deployed as virtual machines on a single physical server.

For example, an LTE operator may deploy the MME, SAE GW (SGW & PGW) and HSS functions of the Evolved Packet Core (EPC) as virtual machines on a single server, a concept known as "Virtual EPC". Other network functions that are typically required on remote sites, such as eNodeB, will typically be deployed on separate servers as shown in Figure 4.

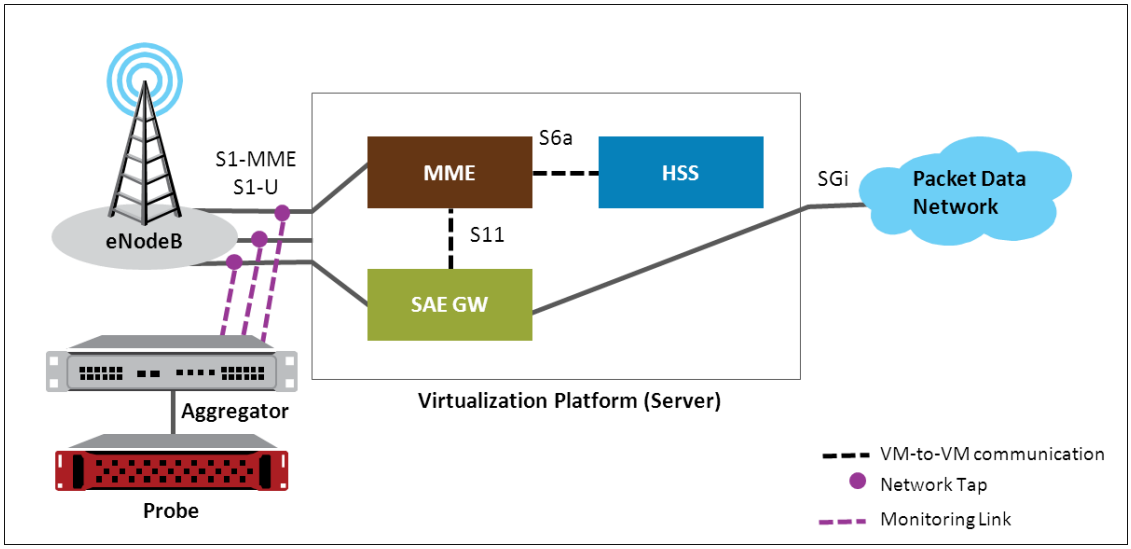

Figure 4: Monitoring Virtual Network Elements with Legacy Probes

This presents a challenge for network analytics probes. In order to extract the required network intelligence, probes need to monitor, analyze and correlate information from multiple network interfaces. For example, a basic LTE monitoring solution is required to monitor the S1-U, S1-MME, S11 and S6a interfaces to extract network intelligence from the GTP-U, GTP-C, S1AP/NAS and Diameter protocols.

In an NFV environment, traditional monitoring equipment such as taps and splitters can still monitor the traffic that traverses physical network interfaces, such as S1-U and S1-MME in the example above. However, taps or splitters cannot monitor logical interfaces that use internal VM-to-VM communication between functions hosted on the same server, such as S11 and S6a in the example above.

This fact severely limits the intelligence that can be extracted by legacy probes in an NFV environment. Without access to the GTP-C and Diameter protocol on S11 and S6a interfaces, legacy probes cannot extract user identifiers and authentication information or trace network procedures that are critical for customer experience management and service assurance.

In sum, to monitor virtual network elements, a new type of solution is required, as described in the section below.

Monitoring Traffic between Virtual Network Elements with Virtual Probe Functions

As explained in the previous section, legacy physical probes do not have access to internal VM-to-VM communication between network functions hosted on the same server, thus severely limiting their functionality in this use case.

The solution to effectively monitor traffic between virtual network elements is provided by the Virtual Probe Function (VPF). VPF can monitor all traffic in the Virtualization Platform, both external traffic on the Virtualization Platform's physical interfaces, as well as VM-to-VM communications, as shown in Figure 5.

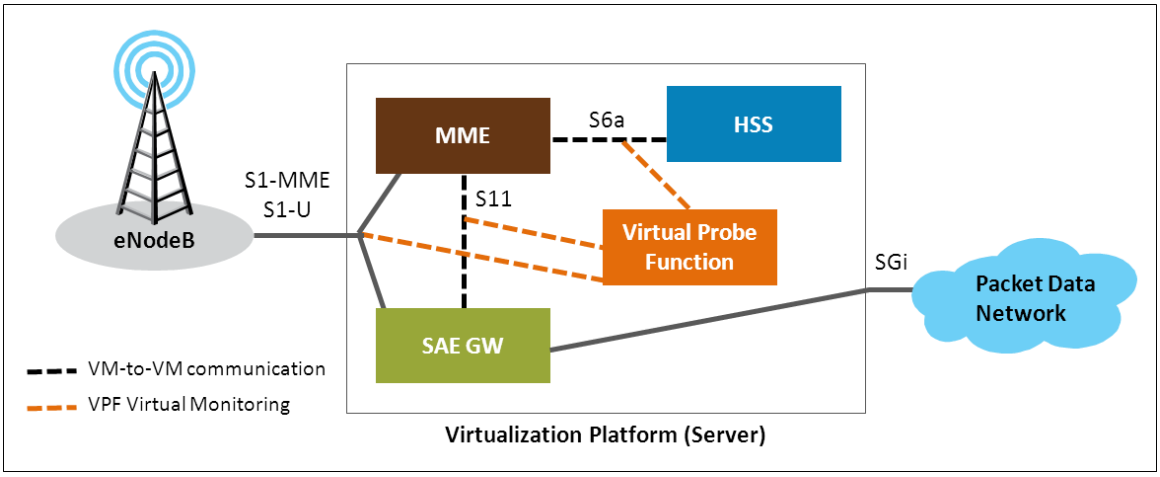

Figure 5: Monitoring Virtual Network Elements with Virtual Probes

There are several advantages of monitoring traffic between Virtual Network Elements with VPF. VPF has full visibility of all the interfaces, both physical and logical, so it can extract all the required information for customer experience management and service assurance applications.

The VPF itself is simply software residing on a VM, which can be deployed alongside any other virtualized application or network function on the same physical virtualization platform server. VPF leverages virtualization platform software capabilities to be able to non-intrusively monitor physical and VM-to-VM communications in a seamless manner.

Operators using VPF to monitor virtual network functions reduce the CAPEX and OPEX associated with the monitoring solution by using standard off-the-shelf hardware rather than proprietary appliances. Moreover, the VPF solution removes the need for proprietary hardware, and costly network taps and aggregators.

The following section, RADCOM's MaveriQ Solution, presents details of MaveriQ-VPF, RADCOM's Virtual Probe Function.

RADCOM's MaveriQ Solution

RADCOM's MaveriQ solution is an innovative service assurance and Customer Experience Management solution that addresses multiple service provider needs including customer experience monitoring, network performance monitoring, service optimization, marketing analytics, network planning and subscriber and network troubleshooting in a single solution. MaveriQ is a multi-technology solution designed for wireless and wireline networks and multiple services such as voice, data, video and Rich Communications Services. MaveriQ is optimized for LTE-Advanced, LTE, HSPA, UMTS, GPRS, CDMA, Wi-Fi, VoLTE, IMS, VoIP and SIGTRAN networks.

The MaveriQ solution simultaneously addresses the needs and requirements of different users within the organization ranging from the Network Operation Center (NOC) to Engineering, Customer Support and Marketing groups. RADCOM's solution can function independently, or be an integral part of the operator's total service offering by augmenting legacy OSS/BSS solutions.

MaveriQ is a high performance solution designed for Terabit Networks. The capability to analyze hundreds or even thousands of Gbps in real-time is achieved by utilizing technologies such as Big Data analytics engines, column-based data warehousing, Massively Parallel Processing (MPP) and ultra-fast packet processing techniques such as Intel's DPDK.

As depicted in Figure 6, the MaveriQ solution is comprised of MaveriQ probes (virtual probes or appliances) that non-intrusively monitor network interfaces and the MaveriQ Management System which provides network analytics and a presentation layer.

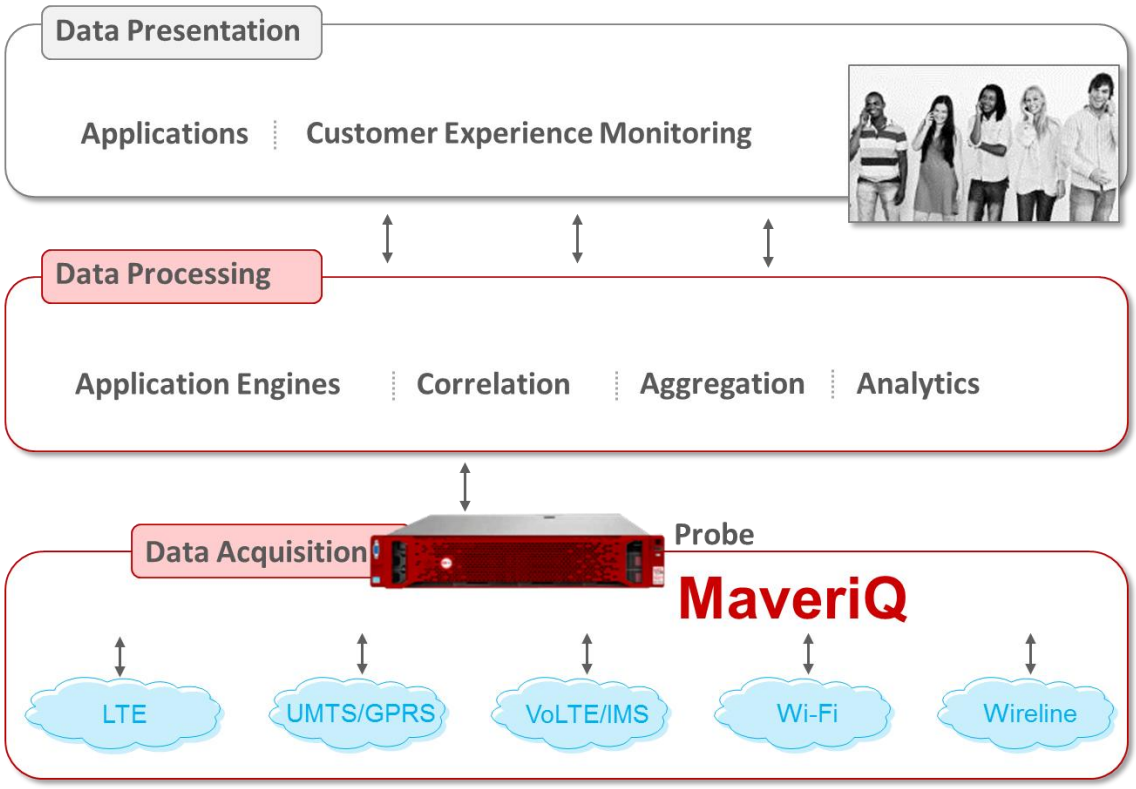

Figure 6: MaveriQ Architecture

MaveriQ Probes

MaveriQ probes can be deployed in two flavors:

- MaveriQ-VPF - a virtual probe function that resides on virtualization platforms
- MaveriQ probe appliances – a family of pre-installed probe appliances that include dedicated hardware and software, optimized for high performance and cost efficiency

The MaveriQ-VPF and MaveriQ appliance provide the same functionality and differ only in the deployment model. Both flavors can be mixed in the same network under a single MaveriQ management system, according to the network architecture and operator's needs.

MaveriQ-VPF can be deployed as a VM on 3rd party virtualization platforms. MaveriQ-VPF can be used to monitor both legacy and virtual Network Elements.

MaveriQ-VPF uses Virtual Network Interface Card (vNIC) and Virtual Switch (vSwitch) capabilities to non-intrusively monitor traffic on external network interfaces as well as internal VM-to-VM communication.

Using MaveriQ-VPF, operators can rapidly increase network analytics capacity when needed, by adding virtual probe instances on additional VMs on the same hardware, keeping CAPEX and OPEX under control. The MaveriQ-VPF VM can be easily migrated between hosts which can be used to increase redundancy and eliminate application downtime during planned server maintenance.

The **MaveriQ Probe** family includes a number of probe models optimized for different locations and network traffic volumes. For operators considering moving to NFV and SDN in the future, the MaveriQ probes can be initially deployed in the traditional model, and the software can be easily migrated to MaveriQ-NFV once the operator decides to implement NFV.

Summary

NFV and SDN technologies will transform the telecommunications industry in years to come. In a growingly competitive arena, operators will be using NFV and SDN to have greater flexibility, ease of scalability and quicker service introduction while reducing their costs.

One of the network functions that operators should consider to transition to NFV and SDN should be Network Analytics probes. Network Analytics probes are critical to network operations, planning, engineering and marketing.

Operators should consider moving the probe function from proprietary appliances to virtual machines.

Operators are expected to move core network functions such as EPC to NFV and SDN as well. When transitioning network elements to NFV, operators should consider the impact on their current monitoring solutions, some of which may become severely limited once network elements are virtualized. Operators should adjust their monitoring tools to support the new NFV network architecture and use solutions that are able to monitor internal VM-to-VM interfaces are well as physical interfaces.

One of the first solutions in the market to address the challenges of network analytics in the era of NFV and SDN is RADCOM's innovative MaveriQ-VPF.

For more details on MaveriQ, please visit www.radcom.com or contact RADCOM experts at experts@radcom.com

USA Office:
RADCOM Equipment Inc.
Tel: +1-201-518-0033 or 1-800-RADCOM-4
Fax: +1-201-556-9030
email: info@radcomusa.com

Corporate Headquarters:
RADCOM Ltd.
Tel: +972-3-645-5055
Fax: +972-3-647-4681
email: info@radcom.com

Brazil Office:
RADCOM (Brazil) LTD.
Tel: +55-11-4195-5281
email: brasil@radcom.com

Singapore Office:
RADCOM Ltd.
Tel: +65-6841-5755
Fax.: +65-6841-7971
email: singapore@radcom.com

India Office:
RADCOM Trading India Pvt. Ltd.
Tel: +91-11-4051-4079
Fax : +91-11-4051-4052
Email: mailto:indis@radcom.com

Web Site:
http://www.radcom.com