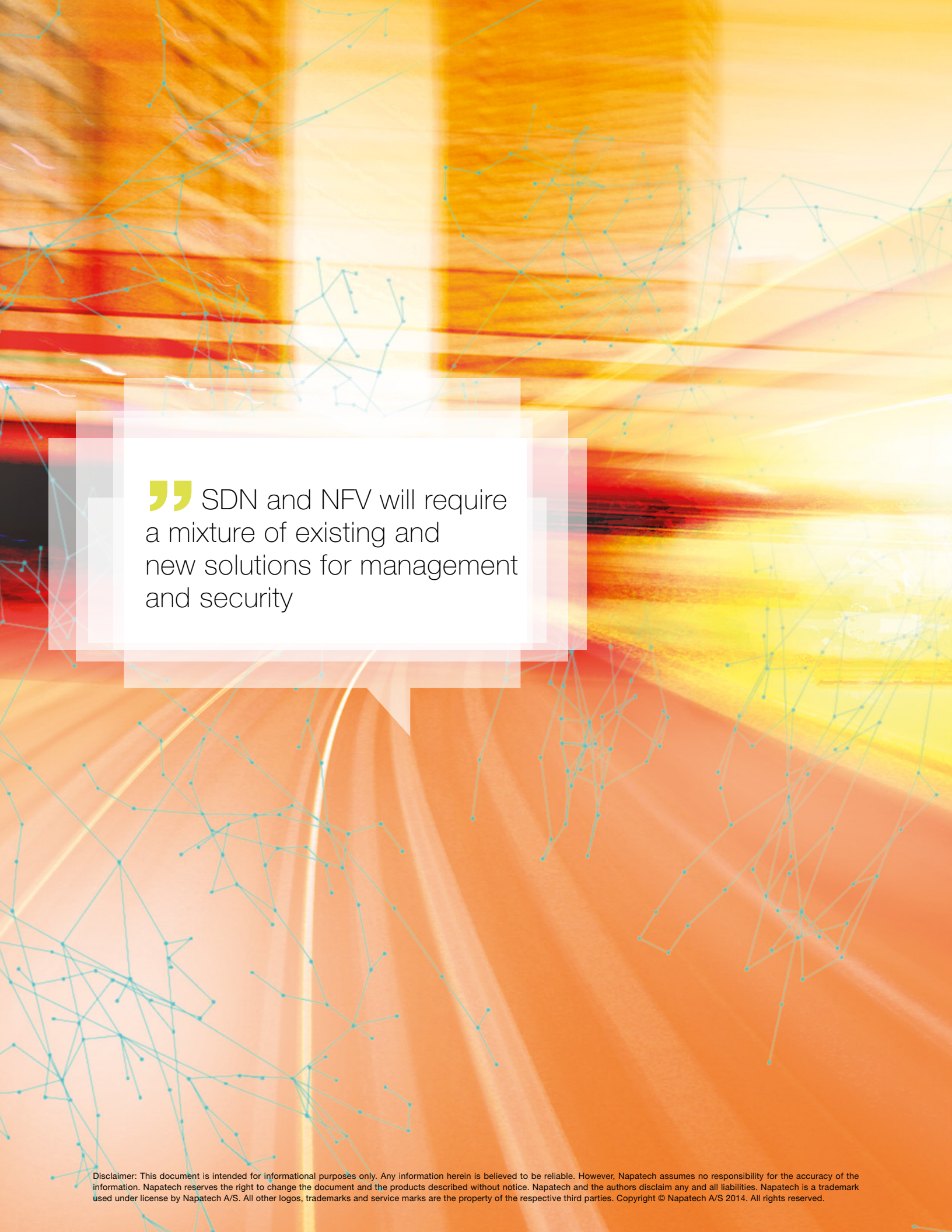
TIME TO RETHINK
SDN AND NFV PERFORMANCE

The key challenges in deploying SDN and NFV effectively are network management and ensuring performance at high speeds. Virtualization-aware appliances provide the solution by being the bridge between the networks of today and the software-based models of the future. They enable real-time insight that allows SDN controllers and NFV management to administer and secure networks at speeds of 10, 40 or even 100 Gbps.



TIME TO RETHINK
SDN AND NFV PERFORMANCE

As Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) enter the commercialization phase, general consensus in the industry is that the move to a pure software model will enable the agility and flexibility that traditional networks have never been able to achieve. While the communication challenge appears to be solved, the next problems facing network engineers are management and ensuring high performance levels at speeds of 10, 40 or even 100 Gbps.

Performance and the ability to assure reliable, real-time data for management and analytics are already a concern today and will be no less of a concern when virtualizing the network. Network appliances provide the real-time insight needed to continuously monitor, collect and analyze traffic for management and security purposes. Appliances can be virtualized, but the same constraints that affect the performance of physical appliances will also affect virtual ones.

Virtualization-aware appliances provide the bridge between the networks of today and the software-based models of the future. The real-time insight provided by virtualization-aware appliances using analysis acceleration enables event-driven automation of policy decisions and real-time reaction to those events, thereby allowing the full agility and flexibility of SDN and NFV to unfold.

THE SDN AND NFV MANAGEMENT CHALLENGE

Managing SDN and NFV proves a challenge for most telecom carriers given the fact that a considerable investment has been made in OSS/BSS systems and infrastructure. This must now be adapted not only to SDN and NFV, but also to Ethernet and IP networks.

Most of the OSS/BSS systems installed have their grounding in the Fault, Configuration, Accounting, Performance and Security (FCAPS) model of management first introduced by ITU-T in 1996 in M.3010. This concept was simplified in the Enhanced Telecom Operations Map (eTOM) to Fault, Assurance and Billing (FAB). Management systems tend to focus on one of these areas and often do so in relation to a specific part of the network or technology, such as optical access fault management.

One of the issues with using FCAPS and FAB is that the foundation of these models was traditional, voice-centric networks based on Plesiochronous Digital Hierarchy (PDH) and Synchronous Digital Hierarchy (SDH). They were static, engineered, centrally-controlled and planned networks where the protocols involved provided rich management information. This made centralized management possible.

Nevertheless, there have been various attempts to inject Ethernet and IP into these management concepts. For example, Call Detail Records (CDRs) have been used for billing of voice services, so the natural extension of this concept is to use IP Detail Records (IPDRs) for billing of IP services. xDRs are typically collected in 15 minute intervals, which are sufficient for billing. This does not, in most cases, need to be real-time. However, xDRs are also used by other management systems and solutions as a source of information to make decisions.

The issue with this is that while traditional telecom networks do not change in a 15 minute interval, since they are centrally controlled and engineered, Ethernet and IP networks are completely different. Ethernet and IP are dynamic and bursty by nature. Because the network makes autonomous routing decisions, traffic patterns on a given connection can change from one IP packet or Ethernet frame to the next. When you consider that Ethernet frames in a 100 Gbps network can be transmitted with as little as 6.7 nanoseconds between each frame, you begin to understand a significant distinction when working with a packet network.

Another issue with Ethernet and IP is that they do not provide a large amount of management information. If a carrier wants to manage a service provided over Ethernet and IP, they need to collect all the Ethernet frames and IP packets related to that service and reassemble the

Network Port Speed	Frames per second		
	64B	300B	1518B
1 x 1G	1.5 M	0.4 M	0.1 M
1 x 10G	14.9 M	3.9 M	0.8 M
1 x 40G	59.5 M	15.6 M	3.3 M
1 x 100G	148.8 M	39.1 M	8.1 M

Network Port Speed	Time between frames		
	64B	300B	1518B
1 x 1G	672 ns	2,560 ns	12,304 ns
1 x 10G	67.2 ns	256 ns	1,230.4 ns
1 x 40G	16.8 ns	64 ns	307.6 ns
1 x 100G	6.7 ns	25.6 ns	123 ns

FIGURE 1
Ethernet and IP Networks: More Data, Less Time to React

information to get the full picture. While switches and routers could be used to provide this kind of information, it became obvious that continuous monitoring of traffic in this fashion would impact switching and routing performance. Hence, the introduction of dedicated network appliances that could continuously monitor, collect and analyze network traffic for management and security purposes.

MANAGING IP AND ETHERNET NETWORKS WITH NETWORK APPLIANCES

To manage Ethernet and IP networks effectively, network appliances are necessary. This is because all Ethernet frames and IP packets need to be collected and reassembled to enable effective management of services. This, in turn, requires continuous monitoring of the network, even at speeds of 100 Gbps, without losing any information. Network appliances provide this capability in real time.

In order for the analysis to be reliable, network appliances must capture and collect all network information. Network appliances receive data either from a Switched Port Analyzer (SPAN) port on a switch or router that replicates all traffic, or from passive taps that provide a copy of network traffic. They then need to precisely time stamp each Ethernet frame to allow accurate determination of events and latency measurements for quality of experience assurance. Network appliances also recognize the encapsulated protocols, as well as determine flows of traffic that are associated with the same senders and receivers.

For effective, high-performance management and security of Ethernet and IP networks, appliances are broadly used. However, the taxonomy of network appliances has grown outside of the FCAPS and FAB nomenclature. The first appliances were used for troubleshooting performance and security issues, but have gradually become more proactive, predictive and preventive in their functionality. The real-time capabilities that all appliances provide make them essential to effective management of Ethernet and IP networks. For this reason, network appliances need to be encompassed in frameworks for managing and securing SDN and NFV.

REAL-TIME INSIGHT WITH ANALYSIS ACCELERATION

Appliances can be based on commercial off-the-shelf servers with standard Network Interface Cards (NICs), but these are not designed for continuous capture of large amounts of data and tend to lose packets. For guaranteed data capture and delivery for analysis, hardware acceleration solutions are used, such as analysis accelerators, which are intelligent adapters designed for analysis applications.

Analysis accelerators meet the nanosecond-precision requirements for real-time monitoring and are designed specifically for analysis. They are similar to NICs for communication, but differ in the fact that they are designed specifically for continuous monitoring and analysis of high speed traffic at maximum capacity. For monitoring of a 10 Gbps bi-directional connection, this means processing of 30 million packets per second. Typically, a NIC is designed

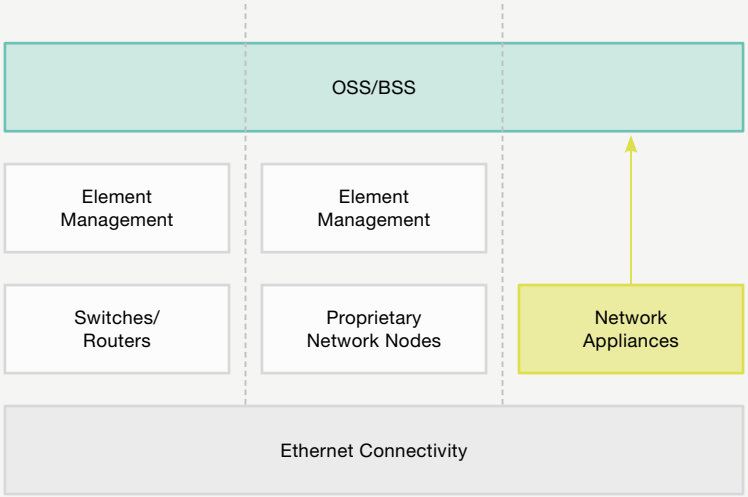


FIGURE 2
Managing Ethernet and IP Networks Today

for processing of 5 million packets per second. It is very rare that a communication session between two parties would require more than this amount of data.

In addition, analysis accelerators provide extensive functionality for off-load of data pre-processing tasks from the analysis application. This ensures that as few server CPU cycles as possible are used on data pre-processing and enables more analysis processing to be performed.

By continuously monitoring the network, carriers assess the performance of the network in real time and get an overview of application and network usage. This information can also be stored directly to disk, again in real time, as it is being analyzed. This is typically used in troubleshooting to determine what might have caused a performance issue in the network. It is also used by security systems to detect any abnormal behavior in the past.

However, if these concepts are taken a stage further, there is the possibility to detect performance degradations and security breaches in real time. The network data that is captured to disk can be used to build a profile of normal network behavior. By comparing this profile to real-time captured information, it is possible to detect anomalies and raise a flag.

This kind of capability can be very useful in a policy-driven SDN and NFV network. If performance degradation is flagged, then a policy can automatically take steps to address the issue. If a security breach is detected, a policy can initiate more security measurements and correlation of data with other security systems. It can also go so far as to use SDN and NFV to reroute traffic around the affected area and potentially block traffic from the sender in question.

With the fundamental capabilities that network appliances with hardware acceleration can provide through real-time capture, capture-to-disk and anomaly detection, SDN and NFV performance can be maximized through a policy-driven framework.

VIRTUALIZATION-AWARE NETWORK APPLIANCES

In SDN and NFV environments, network appliances can be used to provide real-time insight for management and security. But a key question remains: can network appliances be fully virtualized and provide high performance at speeds of 10, 40 or even 100 Gbps?

In many ways, network appliances lend themselves very well to virtualization. They are already based on standard server hardware with applications that are designed to run on standard x86 CPU architectures. The issue is performance. Virtual appliances are sufficient for low speed rates and small data volumes, but not for high speeds and large data volumes.

Even for physical network appliances, performance at high speed is an issue. That is why most high-performance appliances use analysis acceleration hardware. While

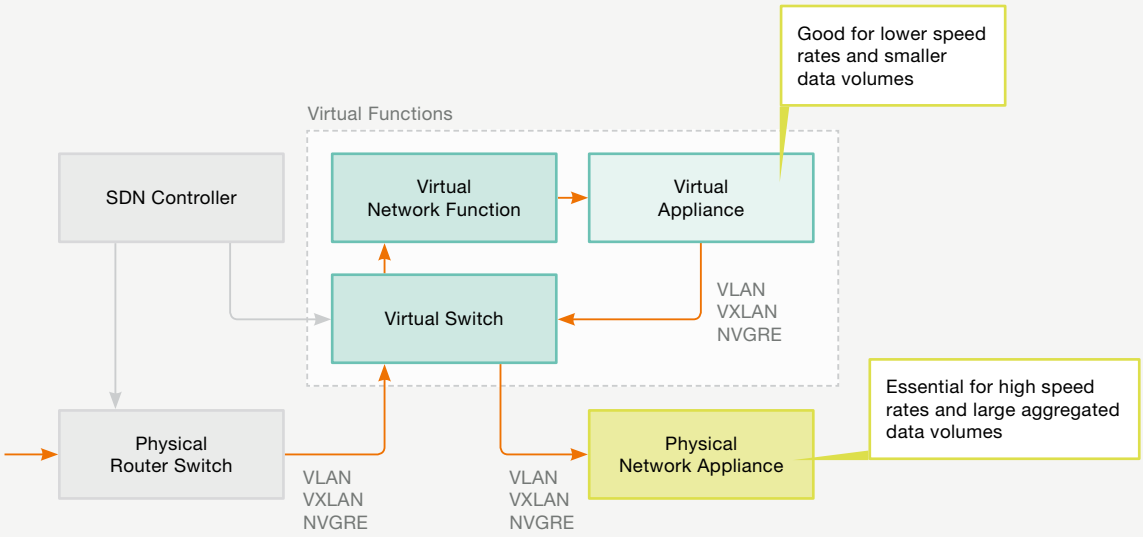


FIGURE 3
Virtual and Virtualization-Aware Appliances

analysis acceleration hardware does free-up CPU cycles for more analysis processing, most network appliances still use all the CPU processing power available to perform their tasks.

From a virtualization point of view, this means that virtualization of appliances can only be performed to a certain extent. If the data rate and the amount of data to be processed are low, then a virtual appliance can be used, even on the same server as the clients being monitored.

However, once the data rate and volume of data increases, the CPU processing requirements for the virtual appliance increases. At first, this will mean that the virtual appliance will need exclusive access to all the CPU resources available. But, even then, it will run into some of the same performance issues as physical network appliances using standard NIC interfaces with regard to packet loss, precise time-stamping capabilities and efficient load balancing across the multiple CPU cores available.

Virtualization of appliances cannot escape the constraints that network appliances face in the physical world. These same constraints will be an issue in the virtualized world and must be confronted.

One way of addressing this issue is to consider the use of physical appliances to monitor and secure virtual networks. Virtualization-aware network appliances can be “service-chained” with virtual clients as part of the service definition. It requires that the appliance can identify virtual networks, which is typically done using VLAN encapsulation today, which is already broadly supported by high-performance appliances and analysis acceleration hardware. This enables the appliance to provide its analysis functionality in relation to the specific VLAN and virtual network.

This can be a very useful solution in a practical phased approach to SDN and NFV migration. It is broadly accepted that there are certain high-performance functions in the network that will be difficult to virtualize at this time without resulting in performance degradation. A pragmatic solution is a SDN and NFV management and orchestration approach that takes account of physical and virtual network elements. This means that policy and configuration does not have to concern itself with whether the resource is virtualized or not, but can use the same mechanisms to “service-chain” the elements as required.

It is clear that the introduction of SDN and NFV will require a mixture of existing and new solutions for management and security. These should be deployed under a common framework with common interfaces and topology mechanisms. With this in place, functions can be virtualized when and where it makes sense without affecting the overall framework or processes.

ENSURING SDN AND NFV PERFORMANCE

As SDN and NFV are increasingly deployed, the high speed, nanosecond-precision of tomorrow’s networks presents numerous performance challenges. The ability to ensure reliable, real-time data for management and analytics becomes critical.

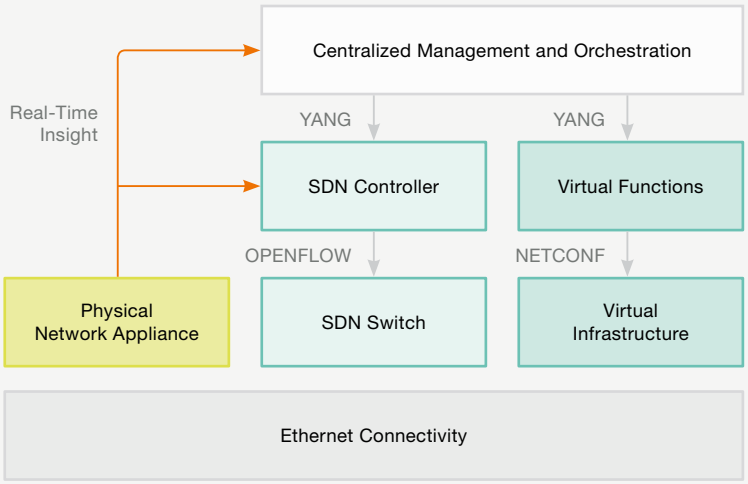


FIGURE 4
Real-Time Insight Powering SDN/NFV Performance

Network appliances provide the real-time insight needed to monitor, collect and analyze traffic for management and security. Appliances can be virtualized, but the same constraints that affect the performance of physical appliances will also affect virtual ones. A practical approach to SDN management and orchestration is one that takes into account both physical and virtual elements.

Virtualization-aware appliances are the bridge between the networks of today and the software-based model of the future. They provide real-time insight that enables event-driven automation of policy decisions and real-time reaction to those events, thereby allowing the full promise of SDN and NFV to unfold.

DISCOVER THE POWER OF NAPATECH

Napatech accelerators are designed to handle the maximum theoretical throughput of data for a given port speed. Napatech offers a range of accelerators supporting speeds from 10 Mbps to 100 Gbps. A single, common Application Programming Interface (API) allows application software to be developed once and used with a broad range of Napatech accelerators. This allows combinations of different accelerators with different port speeds to be installed in the same server. Additional features include:

- Napatech accelerators can identify, filter and distribute flows to up to 32 CPU cores
- Data merging functionality allows flows from different ports on different accelerators to be merged for analysis
- Data sharing functionality allows multiple applications to access the same data at the same time
- All of this can be performed with very low server CPU load

CHOOSE THE MARKET LEADER

Napatech is the market leading provider of accelerators for network management and security applications. Napatech provides global sales and support from local offices in all major continents, which is included in the price of the accelerator. This means that our highly experienced support resources are available for design and integration support, as well as field support without extra charge.

Napatech accelerators are manufactured to the highest standards by outsourced manufacturers in Switzerland and the USA supporting all major certifications including NEBS for telecom applications.

COMPANY PROFILE

Napatech is the world leader in accelerating network management and security applications. As data volume and complexity grow, the performance of these applications needs to stay ahead of the speed of networks in order to do their jobs. We make this possible, for even the most demanding financial, telecom, corporate and government networks.

Now and in the future, we enable our customers' applications to run faster than the networks they need to manage and protect.

Napatech. FASTER THAN THE FUTURE

EUROPE, MIDDLE EAST AND AFRICA
Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500
ntemeasales@napatech.com
www.napatech.com

NORTH AMERICA
Napatech Inc.
Boston, Massachusetts
Mountain View, California
Washington D.C.

Tel. +1 888 318 8288
ntamericassales@napatech.com
www.napatech.com

SOUTH AMERICA
Napatech
São Paulo, Brazil

Tel. +55 11 2127 0782
ntsouthamericasales@napatech.com
www.napatech.com

APAC
Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

Napatech Korea
Seoul, South Korea
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com