White Paper
Intel® Open Network Platform
Software Defined Networking Division

Going Virtual: Intel and Red Hat Demonstrate SDN Service-Chaining Solutions

As software-defined networking (SDN) and network function virtualization (NFV) have gained traction in the marketplace, many organizations—from enterprise IT to cloud and telecommunications service providers—have discovered the benefits of virtualizing compute and networking components. Enterprises and service providers face intense pressure to support the rapid deployment of new services, and this is one of the key factors driving the industry shift to SDN and NFV solutions. Service chaining adds another dimension to virtualization possibilities: added flexibility in integrating virtual appliances into the mix to handle routing, switching, and other functions as part of the service chain.

Service chaining provides a flexible means of managing network traffic more intelligently—with greater agility—when moving from physical networking machines, such as routers and switches, to virtual network appliances that implement multiple virtual machines on each standard high-volume server (SHVS). To advance this technology further, the Intel® Open Network Platform (Intel® ONP) reference architecture and Red Hat's Enterprise Linux* OpenStack* platform, combined with open-source components and virtual appliances from Intel® Network Builders partners, form the basis of a powerful demonstration that shows the practical capabilities of service chaining in action.

This paper explains the concepts that characterize service chaining and discusses the multi-vendor demo that illustrates the benefits of this technology to enterprises, cloud, and telecommunications companies.

Table of Contents

What is the Intel ONP Reference Architecture?

Developed to streamline the design, deployment, and manageability of open solutions within SDN and NFV environments, the Intel ONP reference architecture provides a blueprint for enabling commercial adoption of validated hardware and software in key industry sectors. Telecom carrier networks, enterprise environments, and cloud data centers can more easily build solutions using an open-source software stack running on standard high-volume servers, as delineated by the reference architecture. An ecosystem has been built around the foundation established by the Intel ONP reference architecture with collaboration, contributions, and the support of industry consortiums, telecommunications and cloud providers, Intel® Network Builders, and leading companies involved in open-source projects.

Technology Challenge: Realizing the Promise of Dynamic Service Chaining

Traditionally, network services are implemented in static chains. This can create technical challenges and introduce network management issues when network functions are virtualized. In an environment using static chains, service functions—including WAN optimization, load balancing, security, and additional value-added services—exist in a rigid path dictated by the hardware configuration. Making modifications to the components in this path requires substantial manual intervention. In this type of implementation, data exchanged between communicating peers adds inefficiencies, reduces overall bandwidth, and typically leads to significant numbers of duplicated functions.

Dynamic service chaining offers a means to improve efficiency and systematically direct packets, flows, or messages across the network. Intelligent network orchestration is at the heart of this technology. With NFV, a centralized master with visibility into all available networking devices manages and provisions network functions, simplifying the combining and coordination of services.

To accomplish SDN/NFV service chaining requires overcoming these challenges:

- **Packet flow issues**. Determining a logical packet flow is necessary—packets sometimes need to traverse physical links multiple times.
- **Managing L2/L3 packet forwarding**. In enterprise environments, network address translation would modify the IP address. Any modifications to the L2/L3 header can disrupt consistency in the chain because control mechanisms within a flow are identified by the header.
- **Managing L4/L7 service processing**. Service processing, such as that performed by application delivery controllers (ADCs) and WAN optimizers often modifies L4 - L7 operations, which can terminate some flows and start up others unexpectedly.
- **Orchestration and controller issues**. Placement of services must be coordinated. Services that depend on conditions and states to control operations must use a single path in both directions.

Intel® Open Network Platform Reference Architecture

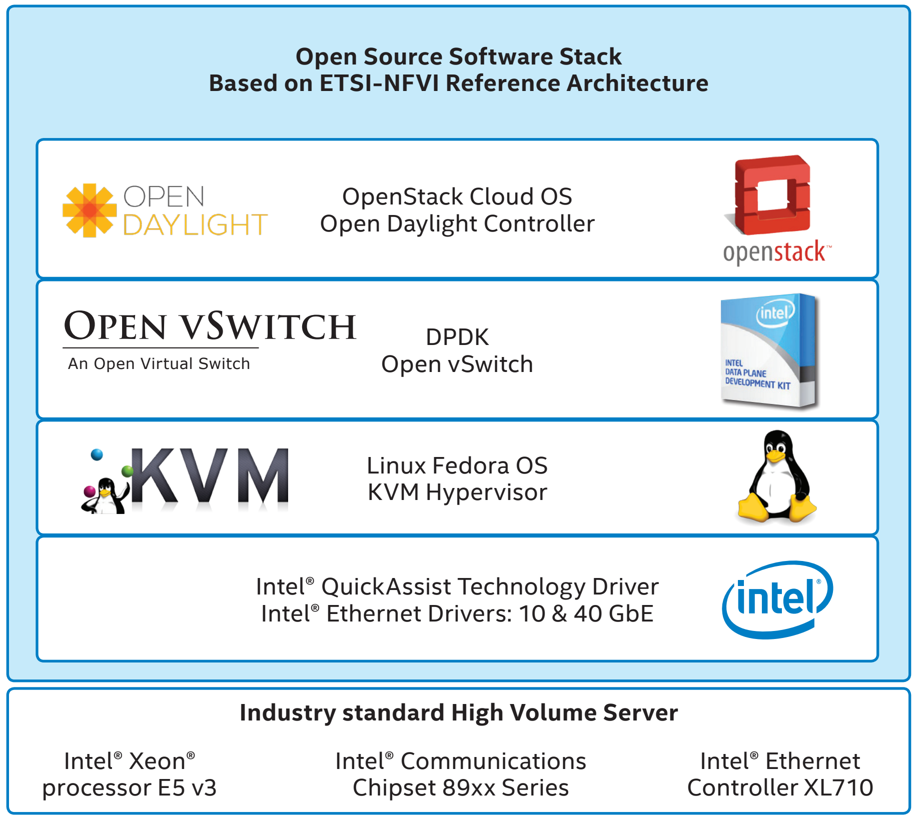

Figure 1. Software stack and hardware platform for the Intel® Open Network Platform reference architecture, release 1.2.

As dynamic service chaining matures, solutions for these challenges are being researched and explored, including the following techniques:

- **Coordinating service segments through the SDN controller** offers a potential solution currently being explored, but it adds complexity to service chain operations.
- **Use of a dedicated service chain header** can indicate the appropriate service path and provide this data to the controller to select the optimal path.
- **Performing deep packet inspection** gives the SDN controller the information to more intelligently handle the packet ordering and flow.

Ongoing work in this area focuses on gaining a better understanding of these service-chaining challenges as new solutions are developed.

Supporting Reference Architecture Used for the Demonstration

Intel ONP is a reference architecture that defines a modular framework for a wide range of SDN and NFV vendor solutions. Virtual appliances from F5, Riverbed, Brocade, and other vendors have been used as part of the service-chaining demo.

The software stack for the Intel ONP reference architecture, shown in Figure 1, runs on the latest Intel® processor: the Intel® Xeon® processor E5 v3 family. The OpenDaylight* Helium controller and the OpenStack Juno platform provide SDN/NFV control and orchestrations, respectively. The software components in the compute node stack are based entirely on open-source projects, including the Data Plane Development Kit (DPDK), Open vSwitch*, Kernel-based Virtual Machine (KVM*), and Fedora Linux. To improve interoperability with Intel ONP, Intel submitted optimizations for OpenStack and demonstrated compatibility with OpenDaylight.

Hardware components included in the demo as a part of the implementation of Intel ONP are the Intel® QuickAssist Adapter 8950 and the Intel® Ethernet Controller XL710. Other hardware and software configurations are supported by the Intel ONP reference architecture release 1.2 as well. An array of validated solutions from the Intel Network Builders ecosystem (see Figure 2) makes it possible to quickly construct a high-performance SDN/NFV solution and to implement versatile service chaining functionality.

The reference architecture is strongly aligned with the NFV architecture specifications established by ETSI and the guidelines formulated by the Open Platform for NFV* (OPNFV*) project, making it possible to achieve greater interoperability through Intel ONP.

A Deeper Look at Service Chaining

Service chaining within an SDN/NFV environment enables the connection of network and security services into the flow of network traffic in a dynamic manner, using software and virtual appliances rather than physical appliances. Service-chaining actions are initiated and performed through a centralized controller.

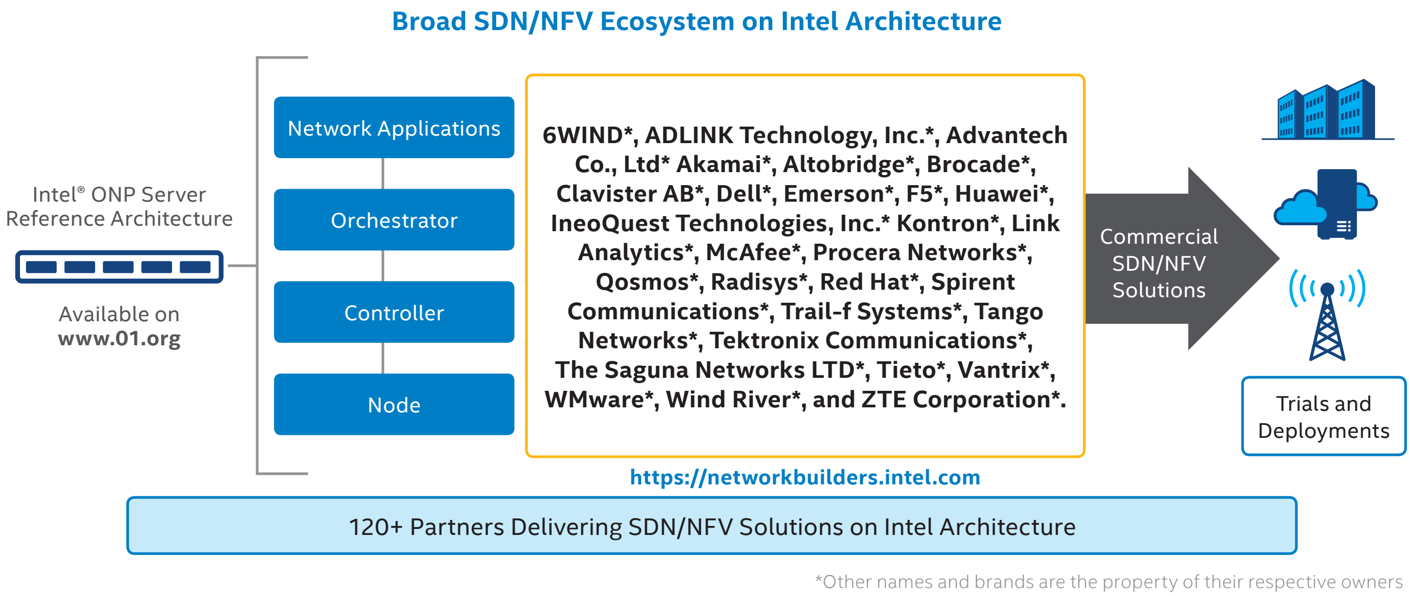

Figure 2. Reference architecture components of Intel® Open Network Platform Server.

Support for SDN service chaining relies on a platform upon which the controller functions are decoupled from hardware and in which the control and data planes are separated, and NFV principles are used to substitute virtual appliances for proprietary, dedicated hardware appliances. In the case of the demo discussed in this paper, the platform is based on the Intel ONP reference architecture and a collection of components assembled from a number of different vendors.

With dynamic service chaining, all the applications in the network are working together, rather than having applications residing in individual silos. Load balancers can determine what node a series of packets has to go through, but traffic has to go through the router and firewall. The virtual appliances are chained together, rather than having physical appliances through which the data is flowing. The same virtual appliances may reside on the same server. For example, the firewall and router could both be running on the same server. Traffic is going to be chained or running through the virtual appliances.

Within this model, the administrator can dynamically adjust traffic routing, depending on what types of operations are taking place with the server—whether it is media distribution, handling incoming transactions, or any other type of operation.

The key to the value of service chaining is its dynamic aspect—being able to adjust on-the-fly in response to changing network conditions, rather than being locked into a static situation. This allows resources to be used more intelligently, which is the true value of having a dynamic service chain.

Rapid Provisioning and Enhanced Network Management through Service Chaining

The service-chaining demo uses a number of virtual applications—from several different vendors—running on a Dell Server with open-source components, including Linux, Red Hat OpenStack, and the OpenDaylight controller. Core components are based on the blueprint provided by the Intel ONP reference architecture, release 1.2.

Virtual appliances used in the demo make it possible to automate the provisioning and scale as required to meet operational requirements. The demo includes the following virtual appliances (but is not limited to these):

- F5® BIG-IP® Advanced Firewall Manager™ (AFM) Virtual Edition
- F5® BIG-IP® Local Traffic Manager™ (LTM) Virtual Edition
- Riverbed SteelHead* vWAN - Virtual WAN
- Brocade Vyatta* 5600 vRouter- Virtual router

These virtual applications replace physical appliances that perform the same tasks in the network. The SDN/NFV platform can also work in combination with existing physical appliances that are included as part of a solution. As more virtual appliances are deployed, the need for manual configuration and administration of physical appliances is reduced. Because dynamic service chaining lets administrators adjust operations dynamically to changing conditions and preset thresholds within the network, all virtual appliances are subject to control using automated management processes. Routing and traffic flow more efficiently as available resources are enabled or freed for other uses, as necessary.

The specific virtual appliances used in this particular Intel and Red Hat demo are not necessarily fixed. Many substitutes exist across a large array of compatible appliances that work well with the Intel ONP architecture. For example, plugging in the Qosmos Deep Packet Inspection* virtual application enhances the intelligent routing capabilities and plugging in the McAfee® Network Security Platform (NSP) virtual intrusion prevention system increases the network security. Dozens of additional appliances available from the Intel Network Builders ecosystem and ISVs extend capabilities, create value-added services, and respond to unique implementation requirements.

The demo illustrates clearly the ease in which virtual appliances from multiple vendors can be rapidly and efficiently provisioned through the SDN controller and orchestration layer. Network management becomes much simpler, leading to reduced operational costs, increased agility, and a lower total cost of ownership. Even after the network is set up and operating, there is no need to shut down the system and reconfigure the network components to directly plug in any number of virtual appliances.

Overcoming Network Infrastructure Weaknesses

Managing the traditional network infrastructure today in which physical devices are used to carry out fundamental network services presents significant challenges. Consider the steps an IT professional or technician must perform to complete basic tasks. For example, to deploy a new router the hardware must first be located in inventory and, if not available, must be ordered from a supplier. The router must then be physically moved to the location for deployment and configured by a technician. This generally requires manual configuration, setup, and testing before the router can be brought online. If the router hardware has to be ordered, the entire process can take weeks or even months to add the router to the network and complete the deployment.

In comparison, as the demo highlights, a virtual appliance can be provisioned and added to a network service chain in a matter of minutes. Figure 3 shows the Network Topology window within the OpenStack administration tab. From this high-level view of the network, administrators can configure virtual appliances and structure the network topology for effective resource use. For example, a **Create Router** button provides a means to insert a virtual router at a designated position within the network.

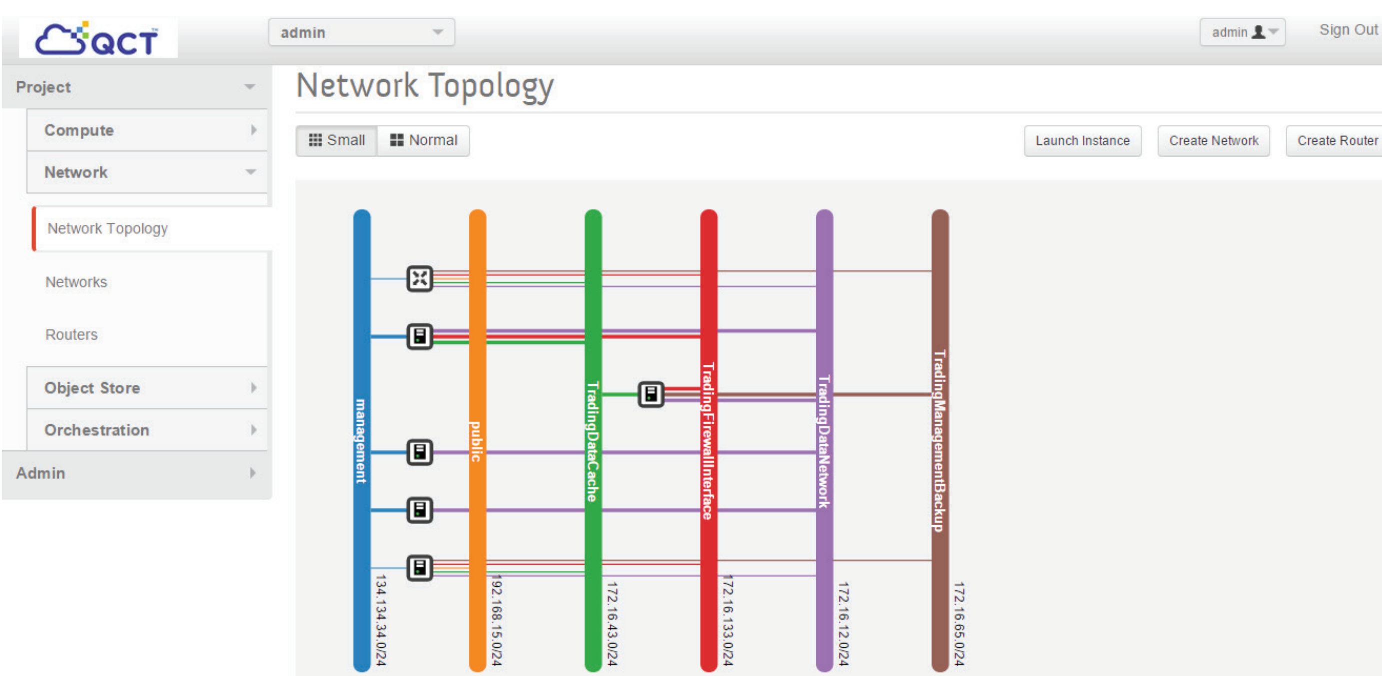

Figure 3. An overview of the network topology from the OpenStack* console.

Individual virtual appliances within the virtualized environment typically have their own management consoles, providing fine-grained control over the configuration options. For example, Figure 4 shows the management console for accessing the Riverbed SteelHead virtual WAN capabilities, supporting consolidation of servers in a virtual environment. Tabs within the console enable an administrator to set limits for CPU usage, set alarms, perform diagnostics, and configure settings.

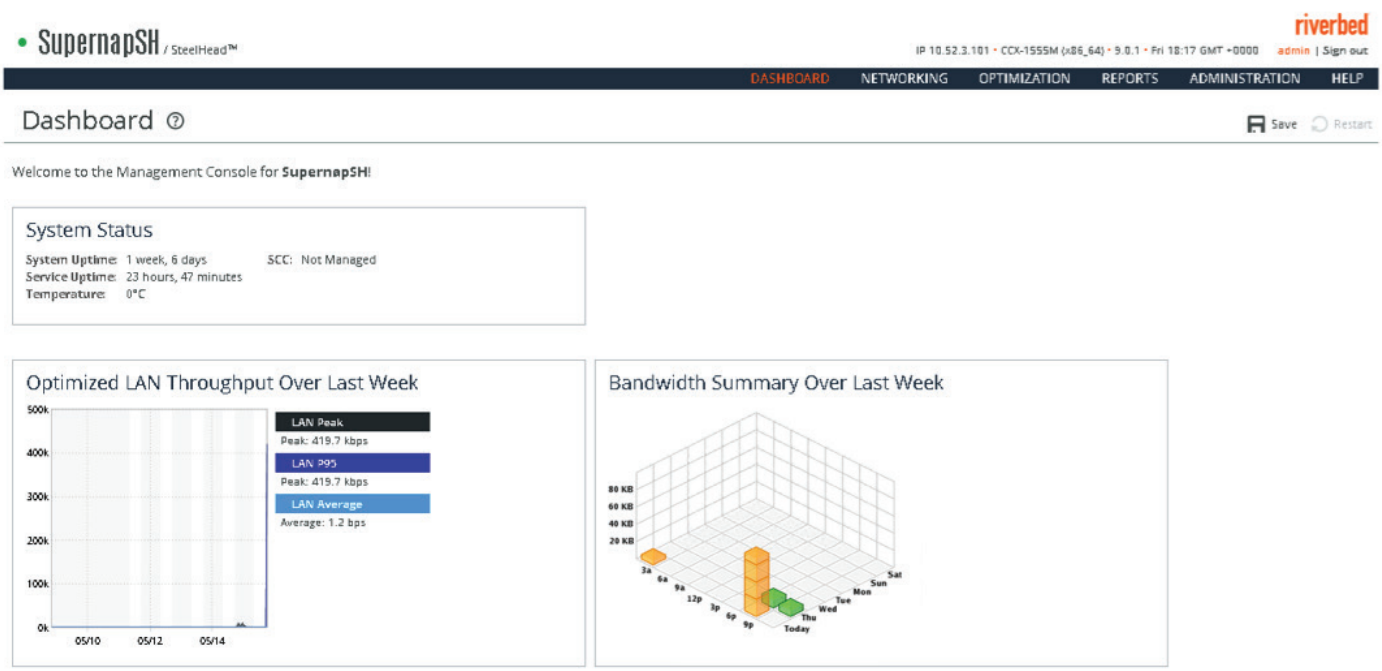

Figure 4. Management console for Riverbed Steelhead* VCX.

Virtual appliances eliminate the need to manually provision physical hardware, providing the following advantages:

- Improved efficiency in network performance through intelligent routing and better use of resources
- Better scalability by controlling platform access to server resources through virtual components deployed as network demands vary
- Fluid provisioning through automation based on presets and defined thresholds
- Increased agility through centralized management

Before standards and reference architectures were developed to provide the foundation to integrate services for SDN/NFV across the span of network layers, these technologies were difficult to develop and deploy, because of the complicated mix of vendor configurations and capabilities. The Intel ONP reference architecture will open opportunities for service chaining using SDN/NFV on networks by delineating the hardware and software components that, together, constitute the necessary network infrastructure and support for the virtualized functionality.

Building a High-Performance SDN/NFV Platform

The use of Red Hat OpenStack as the cloud-computing platform in the demo provides considerable flexibility in creating a network environment suitable for showcasing SDN service chaining. OpenStack lets users create VMs on available hosts and connect networks in accordance with whatever plan IT has in effect. From within OpenStack, the administrator can configure those vendor virtual application resources (such as the virtual appliances from F5, Riverbed, Brocade, and Qosmos).

The OpenDaylight component configures the controller that manages the flow between the virtual machines, enabling the primary network efficiency benefits. The readily available open-source tools to configure the environment make it possible to freely deploy virtual appliances from a large array of vendors, rather than being locked into a single provider.

The contribution from the Intel ONP reference architecture is stability and interoperability through the use of pre-tested components that have been shown to work together effectively. When customers request servers based on the Intel ONP reference architecture, they know the resulting solution will provide them with a high-performance SDN/NFV platform that takes advantage of engineering advances, such as the DPDK ensuring that packet flow through the server will be optimized for high performance. A server that is not based on Intel ONP reference architecture is unlikely to achieve the same performance levels.

Major computer equipment manufacturers, including HP and Dell, have built server solutions around the Intel ONP reference architecture. These solutions have been tuned and optimized for the unique system characteristics and hardware components referenced in the architecture blueprint.

Overcoming Latency for Network Function Virtualization (NFV) Servers

Typical NFV server solutions are not well suited for data plane processing applications. Packet latency is a critical problem due to the way the routing is handled, with the virtual infrastructure and virtualized data plane sending packets needlessly through the operating system, hypervisor, and processor. This inefficient routing negates many of the benefits inherent in the technology.

The Data Plane Development Kit (DPDK) Accelerated Open vSwitch*, an ingredient in the Intel® Open Network Platform reference architecture, provides software enhancements to improve packet processing. Processing time is saved in the following ways:

- Using core affinity
- Disabling interrupts generated by packet I/O; instead a Poll Mode Driver is used
- Enforcing cache alignment
- Prefetching
- Implementing large-scale pages to minimize cache misses

DPDK libraries and drivers are available as open-source code at **www.01.org** for the use of developers who want to enhance and accelerate software-based packet processing.

Traffic Flow through a Service-Aware NFV Infrastructure

The demo of a complete service-aware NFV infrastructure from Red Hat, Intel, and multiple virtual appliance vendors shows enhanced service chaining and reduced costs through intelligent traffic routing.

As shown earlier in Figure 3, OpenStack provides a graphical view of the components in the network infrastructure. This view shows individual networks, virtual appliances, compute nodes, and other characteristics of the virtualized environment. The lines shown in Figure 5 represent a conceptual view of the traffic flow through the network (colors and appearance differ from the OpenStack console view). The key point to remember is that OpenStack lets administrators add networks, virtual appliances, and compute resources, as well as make changes to the network topology directly from the console—relying on virtualized components. For example, the box in Figure 5 that resembles an "x" represents a virtual router—the Brocade Vyatta 5600 vRouter—residing on the public network and controlling traffic flow into the data network and other networks. The fact that traffic flow can be handled fluidly in the virtual mode—by modifying router configurations and network topology—is the reason this technology works so well for service chaining. Operations are structured around the most efficient paths and sequences available, making it possible to configure the network intelligently to optimize traffic flow.

Unlike a physical network configured with physical devices, OpenStack allows the administrator to visualize the network structure on screen and determine the optimal deployment and provisioning of virtual components on any selected portion of the available networks. All network configurations are managed through the console and implemented without ever having to touch a physical device.

To provide a better sense of the traffic flow, Figure 5 illustrates the sequence that takes place when a request for multi-media content takes place.

1. User requests multi-media content on a server.
2. The request is routed to the firewall.
3. The firewall approves the request and lets it through.
4. The request goes to the load balancer, which determines the optimal server to handle it. In this example, it is the Apache server.
5. The requested content is located on the server.

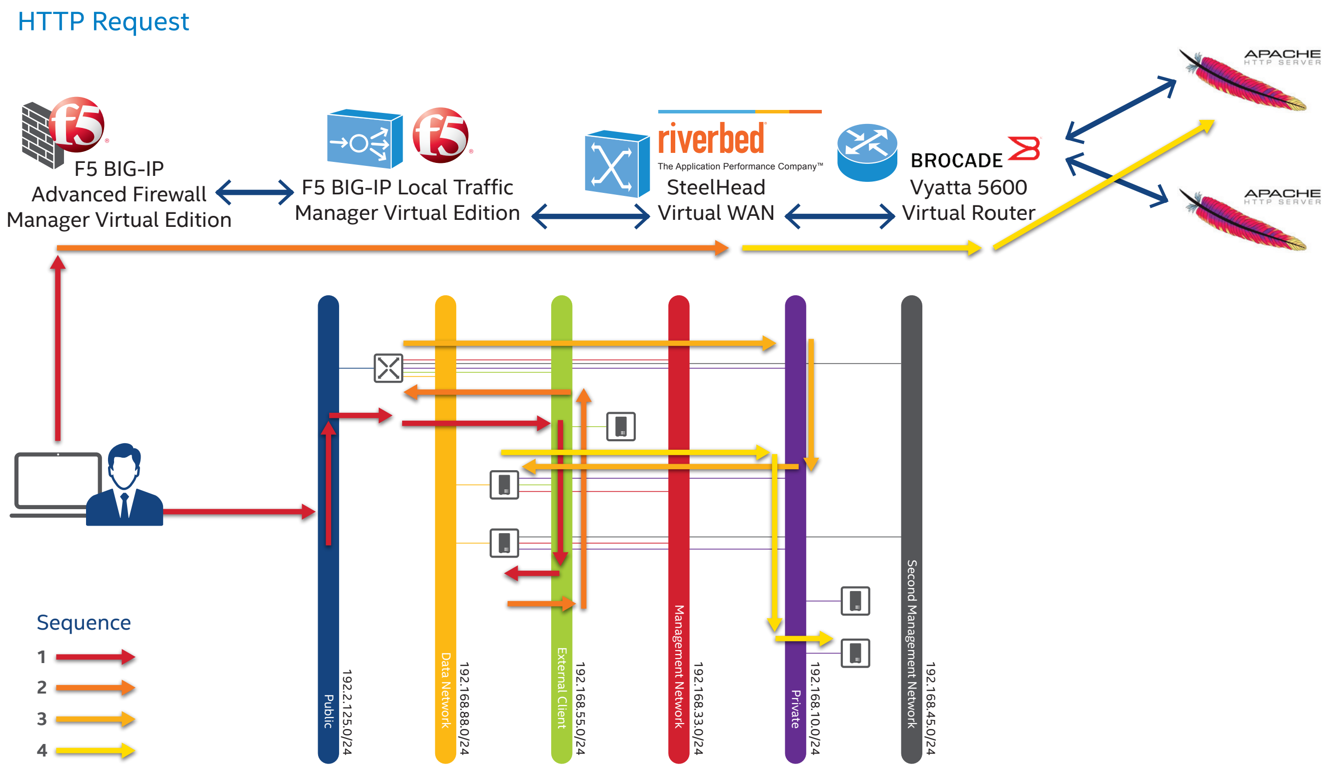

Figure 5. The sequence of handling an HTTP request.

The HTTP response, shown in Figure 6, follows this sequence:

1. The content is located on the server.
2. The content is delivered back to the user.

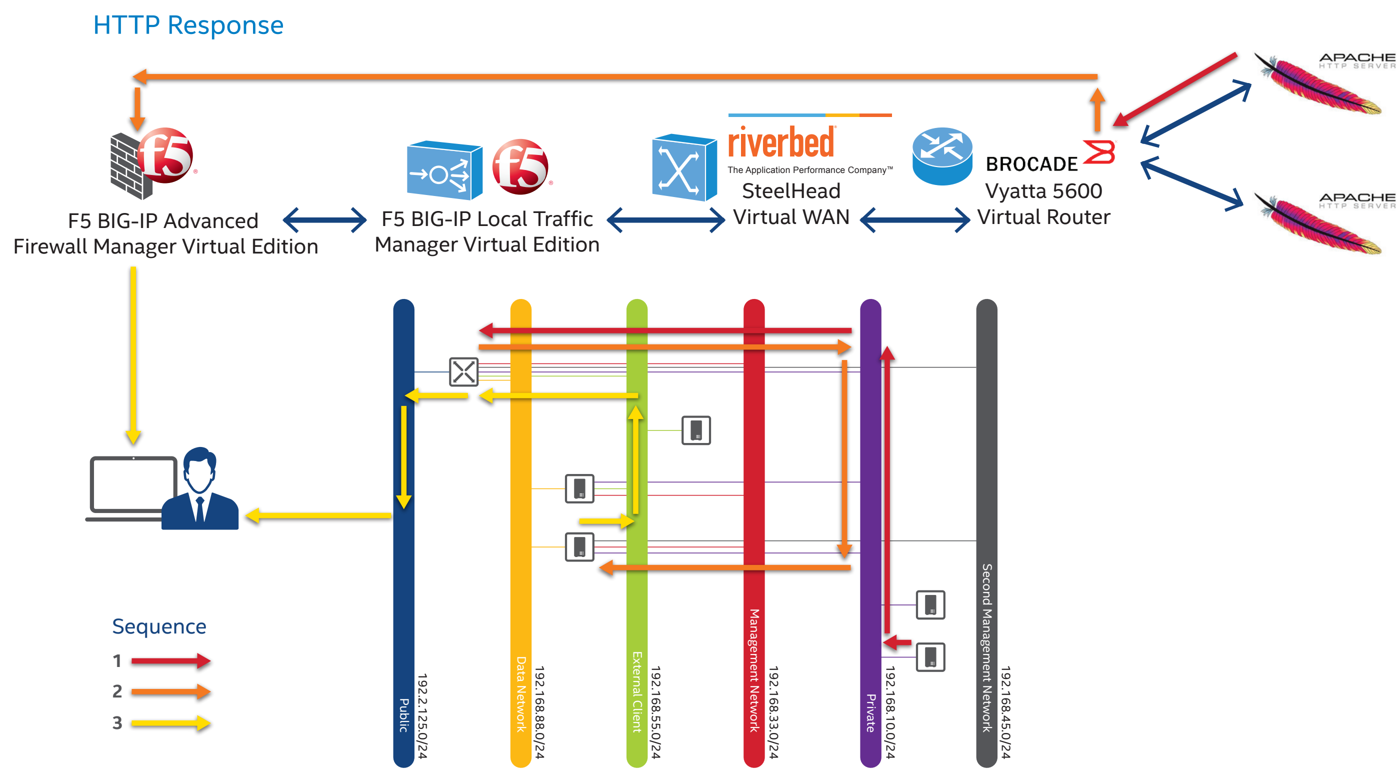

Figure 6. The sequence of handling an HTTP response.

"Service providers are likely closer to recognizing that technologies like service chaining are as much about orchestrating a business process as they are about how to direct traffic around a network. Service chaining allows the network to grow up and really participate in business processes."[1]

– Lori MacVittie, DevOps Journal

Summary

The new foundation being established for dynamic service chaining builds on the technologies that underlie SDN and NFV. The blueprint offered by the Intel Open Network Platform Server reference architecture provides a commercially viable way—based on SDN—to create catalogs of network resources and associated policies abstracted from the hardware. Dynamic service chaining extends this concept and uses the SDN framework to automatically optimize the number and sequence of service functions required to control traffic intelligently across the network.

The service chain demo based on Intel ONP reference architecture helps solve many of the challenges in setting up service chaining and controlling traffic routing. As shown in the demo, the combination of Red Hat OpenStack, a platform powered by an Intel Xeon processor-based server, OpenDaylight, and multi-vendor virtual appliances greatly simplified many of the most difficult challenges of service chaining and created an environment where dynamic resource allocation and centralized control functions add efficiency and cost savings to operational workloads.

Learn more about the Intel® Open Network Platform:
www.intel.com/ONP

Download the Intel Open Network Platform Server Reference Architecture for NFV and SDN:
www.01.org

Learn more about Intel Network Builders:
https://networkbuilders.intel.com/

[1] MacVittie, Lori (2014). "Service Chaining Is Business Process Orchestration in the Network," DevOps Journal. http://devops.sys-con.com/node/3036678

0515/NU/MESH/PDF 332521-001US