Realizing the power of SDN with HP Virtual Application Networks
# Table of contents

3  Executive summary  
3  Software-defined networks (SDN)  
4  Building a software-defined network  
5  HP Virtual Application Networks  
5  HP Virtual Application Networks SDN Controller: centralized network control and automation  
6  HP Virtual Application Networks SDN Applications  
7  Enabling SDN through technology innovation  
9  Why choose HP?  
10  Additional resources
Executive summary

Many enterprises are unable to create business innovation because of aging networking environments. Network design and architectures have remained largely unchanged for more than a decade. While applications and systems have evolved to meet the demands of a world where real time rules, the underlying network infrastructure has not kept pace.

Software-defined networks (SDN) redefines the way we think about the network and removes the barriers to innovation by giving cloud providers and enterprises complete programmatic control of a dynamic, abstracted view of the network. With software-defined networks technologies, IT can become more agile by orchestrating network services and automatically controlling the network according to high-level policies, rather than low-level network device configurations.

This white paper gives an overview of software-defined networking and how HP is leveraging SDN to deliver the Virtual Application Networks strategy.

Software-defined networks (SDN)

So what is SDN?

SDN represents a new architecture that separates the network control plane from the forwarding hardware, allowing a centralized controller (or set of controllers) to define forwarding behavior through high-level policy.

HP believes that SDN is defined by the ability to apply business logic to network behavior in a dynamic fashion. This is achieved in three steps:

1. There must exist an open, standards-based mechanism to access the infrastructure.
2. The control plane and data plane functions of a device should be separated; network control is centralized while forwarding remains distributed.
3. The centralized control (or controller) should deliver open programmable interfaces to allow the orchestration of applications and automation of network functions.

Debunking the myths of SDN

SDN is neither just OpenFlow nor just OpenStack. OpenFlow is a protocol and OpenStack is an orchestration tool. These may be used to deliver SDN elements, but they are not synonymous with SDN.

SDN is not just a software implementation of a network device. HP chooses not to define software routers or virtualized appliances as “SDN.”

SDN is not just providing proprietary programmatic APIs. It is more than exposing device configuration APIs and automation.

SDN is definitely not the end of hardware innovation. HP will continue to drive hardware innovation in support of SDN.

The benefits of SDN

Networks are increasing in complexity: they are bigger and faster, and applications and services are deployed more dynamically. Both users and applications require security, resiliency, privacy, traffic separation, end-to-end virtualization, and priority treatment. In a legacy network there is a 1:1 relationship between servers and switch ports. With the adoption of server virtualization, network demand has increased dramatically by enabling as many as 50 servers behind a single port, each requiring their own network and security policies. The network can’t change or adapt fast enough today without deploying complicated and fragile programmatic network management systems or employing vast teams of network administrators to make thousands of changes per day.

Legacy inflexible network architecture vs. SDN

As you can see from in the figure above, legacy networks are difficult to automate as the control plane intelligence is distributed. SDN promises an easier, more dynamic interaction with the network through the use of a “clean” interface obtained through abstraction of the control plane. This reduces the complexity of managing, provisioning, and changing the network.
Traditional networks have also struggled to bridge the gap between the systems they support and the services they deliver. Attempts to bridge this gap in the past resulted in complex network configuration aimed at enabling network devices to monitor application traffic, infer application status and need, and then respond according to configured policy.

By separating the control plane, and the dynamic state it contains, away from the data or forwarding plane, SDN makes it possible for the network’s status and capabilities to be exposed directly to the business service layer, allowing business systems to request services from the network directly, rather than trusting the network to guess successfully.

By exposing the control plane of the network via open interfaces, SDN levels the playing field for network innovation, lowering the barriers that have previously kept new entrants from bringing new and interesting capabilities to the market, and allowing businesses to unleash the true power of the network.

Building a software-defined network

There are three critical components to a building an SDN:

The infrastructure includes the underlying ports and forwarding hardware that move data across your network. It is important in an SDN environment that the infrastructures supports a means of programmatic access to its data and control plane.

The control element of an SDN resides in a central controller. This control presents an abstracted view of the infrastructure, allowing the network administrator to apply one or more policies across the network. The controller’s job is to enforce these policies. A controller needs to communicate with the infrastructure, but must also be able to communicate with applications.

Applications in an SDN environment could be compared to the protocols that ran our legacy networks for the past 20 years. The key difference is that SDN applications are presented a view of the entire network, allowing them to focus on optimizing business applications and providing a true end-to-end SLA comprising performance, quality of service, and security. SDN applications will be responsible for tasks such as path computation, loop avoidance, and routing, but it doesn’t stop there. The promise of SDN is that applications can easily be developed to accommodate virtually any use case. As applications communicate with the control layer using open, standards-based Application Programming Interfaces (APIs), it means that applications can be developed in-house.

API directionality in SDN

The APIs used to communicate between the layers of the SDN stack are grouped based on their function in an SDN architecture:

- **Northbound APIs**
  Communicate between controllers and applications

- **Southbound APIs**
  Communicate between controller to infrastructure

- **East/Westbound APIs**
  Communicate between groups or federations of controllers to synchronize state for high availability

As SDN technologies are still maturing, there will initially be very few pure SDN deployments outside of massive provider networks that require SDN to solve their scaling problems. Within the enterprise, we will see the deployment of hybrid networks that continue to operate in a traditional fashion but leverage SDN to provide additional features and functionality.
HP Virtual Application Networks

The HP Virtual Application Networks strategy embraces software-defined networks to deliver on its three key principles:

- **Application characterization**
  Gaining intelligence and characterizing applications and traffic on the network, which is essential to consistently, reliably, and repeatedly automating network configuration for delivering specific applications

- **Network abstraction**
  Enabling multitenant networks with on-demand topologies that are device independent

- **Automated orchestration**
  Automating how the network is configured in response to the policy-driven decisions built into network applications

HP FlexNetwork Architecture forms the foundation of the HP strategy and delivers an open and standards-based infrastructure with scalability on three dimensions: security, agility, and consistency.

HP delivered on the promise of application characterization at the network edge through the release of the HP Virtual Application Networks Manager plugin for the HP Intelligent Management Center.

To deliver on the goals of network abstraction and automated orchestration, HP has developed an HP Virtual Application Networks SDN Controller. This controller is the platform for a number of SDN applications that will deliver Virtual Application Networks.

### HP FlexNetwork Architecture with HP Virtual Application Networks

The controller is further extended with robust authentication and authorization mechanisms which, in part, allow HP to expose varying levels of control and access to SDN applications residing within or interfacing with the controller. This mechanism and others work together allowing customers to reap the benefits of increased network flexibility through SDN while preserving the integrity of the network by preventing unauthorized applications from negatively impacting network stability or performance.

The HP Virtual Application Networks SDN Controller is ready for the cloud and will be integrated with OpenStack and CloudStack to provide elastic provisioning of the network alongside storage and compute. Finally, the controller provides a RESTful northbound API, which is intended to expose network features and functionality naturally to off-controller SDN applications, orchestration and management systems, and business applications.

The controller has been architected to provide enterprises and service providers with a scalable, extensible, and stable solution through which they bridge the gap between the services on which the business depends and the infrastructure over which those services run.

The Virtual Application Networks SDN Controller provides the platform for a number of network applications that leverage SDN to deliver the promise of Virtual Application Networks and increase your business agility.
HP Virtual Application Networks SDN Applications

Virtual Cloud Network

The HP Virtual Cloud Network (VCN) application delivers Virtual Application Networks elements, leveraging HP Virtual Application Networks SDN Controller and OpenFlow-compliant virtual switches, to automatically create overlay virtual networks.

HP VCN allows cloud service providers to deliver secure multi-tenant public clouds at the scale necessary to compete in their markets. Enterprises can leverage HP VCN to gain the advantages of automation within their private clouds, while enabling secure integration of public cloud environments into their private estate. HP VCN provides the network abstraction necessary for service providers and enterprises to take maximum advantage of the public and the private cloud.

The HP Virtual Cloud Network application enables public cloud providers and enterprises to overcome the challenges facing them today.

Public cloud providers require massive scale in order to meet the price points that allow them to compete in their marketplace. Yet existing network automation and virtualization solutions have difficulty scaling to the levels a public cloud provider requires.

The HP Virtual Cloud Network solution enables public cloud providers to scale and reduces their risk. First, the HP VCN overlay allows providers to scale beyond the constraints of current solutions. Second, the HP solution focuses network changes at the edge, reducing the risk of each change and making automation at scale a reality.

Enterprises are challenged to interconnect their private environments with their public cloud presences without compromising the integrity of their existing networks. HP VCN enables the enterprise to securely connect to the cloud and apply its own “identity” to its cloud environment.

Since the Virtual Cloud Network solution is already integrated with OpenStack, public cloud providers can deliver an automated self-service solution to their tenants, and enterprises can securely connect their private estate to public cloud environments.
Sentinel security
HP’s latest innovation in security is the Sentinel security application for HP Virtual Application Networks SDN Controller. Sentinel is able to stop threats before they reach your network. Sentinel security can be deployed across a campus or data center network to protect you from over 700,000 malicious malware, spyware, and botnet threats.

One possible use case for Sentinel is the redirection of Domain Name System (DNS) queries from user machines to the Sentinel application running on the HP Virtual Application Networks SDN controller. Take, for example, a corporate user who was to click a link in an email:
• First, the user’s DNS query would be sent to the local OpenFlow-enabled HP access switch.
• Second, the switch would forward the traffic to the HP Virtual Application Networks SDN controller via an OpenFlow rule implemented by the Sentinel application targeting DNS queries.
• Once the SDN controller receives the query, the Sentinel application jumps into action by checking the hostname against the HP TippingPoint DVLabs RepDV database of known threats.
• Finally, if Sentinel determines that the site is legitimate, the query is forwarded across the access layer switch. If Sentinel detects a threat, an unresolvable response is sent back to the client, the action is logged with HP ArcSight, and the user is prevented from accessing the threat.

Sentinel can be used in any network environment where security is a concern, including the data center and cloud computing environments. HP envisions a network where Sentinel security can be implemented for unprecedented network visibility, event correlation accuracy, and security control.

Enabling SDN through technology innovation
HP has made significant investments in developing the technologies behind software-defined networks.

OpenFlow: standards-based infrastructure programmability
OpenFlow is an emerging open standard protocol that has been a key enabling technology for HP Virtual Application Networks. OpenFlow development started in 2007 and was led by Stanford University and the University of California at Berkeley. In 2011, the protocol standardization was taken over by the Open Networking Foundation (ONF).

OpenFlow allows applications or SDN controllers to access the data plane of the network device. This enhanced level of access allows administrators to dynamically change the way traffic flows through the network. The OpenFlow protocol uses a standardized instruction set, which means that any OpenFlow-enabled controller can send a common set of instructions to any OpenFlow-enabled switch, regardless of vendor.

HP demonstrated the first commercial, hardware-based switch implementation of OpenFlow at ACM SIGCOMM in 2008. HP also participated in a public demonstration of OpenFlow at InteropNet Lab in May 2011. HP has been an active contributor to the OpenFlow standards effort and is a founding member of the Open Networking Foundation. HP continues to work closely with partners such as Indiana Center for Network Transactional Research and Education (InCnTRE) to drive research in SDN and ensure multivendor interoperability for OpenFlow-enabled solutions.
**How OpenFlow works**

Most modern network devices have flow tables that run at line-rate for implementing firewalls, NAT, QoS and collecting statistics. The OpenFlow protocol provides a means of programming these flow-tables from a centralized controller through a Secure Sockets Layer (SSL) channel.

OpenFlow uses a well defined set of matching rules to classify network traffic into flows. It also defines a set of actions that the network architect can use to instruct OpenFlow-enabled network devices to manage these flows. These devices may include routers, switches, virtual switches, or wireless access points. Traffic moves across paths that are predefined by characteristics such as speed, fewest hops, or lowest latency, giving network managers the ability to tailor network services to meet the needs of different types of applications and data.

**Coarse- or fine-grained control**

The OpenFlow switch flow table is used to give network managers both coarse- and fine-grained control over data flows. Network managers can use OpenFlow’s match rule attributes, such as ingress port, MAC or IP source and destination address, or VLAN ID, to take forwarding actions. These actions could be forwarding packets to switch ports or the controller, flooding along Spanning Tree, dropping packets, or pushing the packets through the device’s normal packet pipeline.

HP has extended the OpenFlow protocol with a vendor-specific attributes to allow for the enforcement of quality-of-service actions, such as queuing to a specific queue or rate limiting using a specified meter. OpenFlow can also modify traffic flows, such as changing a VLAN setup or VLAN priority, or setting the source and destination address for MAC, IP, or TCP/UDP.

The OpenFlow controller maintains all of the network rules and distributes the appropriate instructions to the network devices. The controller essentially centralizes the network intelligence, while the network maintains a distributed forwarding plane through OpenFlow-enabled switches and routers.
**OpenStack: massively scalable cloud orchestration**

OpenStack is a collection of open source software projects that enterprises/service providers can use to set up and run their cloud compute and storage infrastructure. Rackspace and NASA were the key initial contributors to the project, but since the project’s inception, the OpenStack foundation has managed to attract more than 150 members, with HP being one of the key contributors.

OpenStack provides an open framework for interacting with pools of compute, networking, and storage resources and provisioning these on demand. Corporations, service providers, VARs, SMBs, researchers, and global data centers are implementing OpenStack today to deploy large-scale cloud deployments for private or public clouds.

HP is a platinum member of the OpenStack Foundation and is committed to furthering the development of OpenStack as well as providing OpenStack support across our network portfolio.

**Why choose HP?**

As companies move to cloud and other computing environments, manual configuration of legacy networks through command-line interface (CLI) coding has proven to be error prone, as well as time- and resource-intensive.

SDN overlay point products offer a centralized control plane, but do not automate infrastructure configuration to prime the network to run the overlay, so it assumes the manual device-by-device configuration. Overlay-only approaches focus on data center applications and do not extend the benefits of an SDN to campus and branch networks.

HP is the only tier-1 networking vendor to offer a complete hardware and software SDN solution.

HP Virtual Application Networks delivers:
- Single-pane-of-glass management for the automation of infrastructure
- Open programmable access to infrastructure with OpenFlow
- Virtual Application Networks SDN Controller for centralized control plane
- SDN applications for data center, campus, and branch
- Open APIs for customers and third parties to build applications, and allows for business applications to interface directly with the controller for network-aware applications

With HP Virtual Application Networks, businesses can realize the benefits of simplicity, agility, and automation across the enterprise.
Additional resources

HP FlexNetwork Architecture

Open Networking Foundation

OpenStack Foundation

Indiana Center for Network Transactional Research and Education (InCNTRE)

HP Virtual Application Networks Blog

Software-Defined Networking: The New Norm for Networks