HP Network Optimizer SDN Application

Technical Solution Guide

Version: 1.0
March 2014

Table of Contents

Introduction

The world is moving faster than ever. Transactions must be processed at lightning speed. Mountains of data must be transformed into insights. Customers want exceptional service. Employees want access to information and applications from any device. Delivering on those expectations requires data centers that are more powerful, agile, and automated than ever before, and a campus environment that responds to a dynamic and changing workforce.

Server and storage architectures have modernized to keep pace with the unyielding expectations of an always-on world, but the underlying network has not. The data center network itself, while certainly bigger and faster, has largely been built the same way for two decades. Evolution of campus networks has been slow, despite the mobility revolution.

Whether in the data center or on the campus, when legacy networks are pushed to the limit, they become fragile, difficult to manage, vulnerable, and expensive to operate. Manual configuration and operation simply won't scale to the demands of today's applications, users, and business requirements. Businesses whose networks are at this breaking point risk missing the next wave of opportunity.

This technical white paper provides an overview of the HP Virtual Application Networks (VAN) SDN Controller and how we are fostering the development of a vibrant SDN ecosystem to help enterprises, cloud providers, and developers unleash new levels of automation and efficiency in data center and campus networks.

Simplify and transform with SDN

At HP Networking, we've been leading the way in simplifying and transforming the network to meet your organization's needs for mobility, virtualization, high-definition video, rich-media collaboration tools, and cloud computing. With the HP FlexNetwork architecture, your business gains an open and standards-based network solution designed to scale on three dimensions—security, agility, and consistency.

By embracing a software-defined network, you'll be able to reap the full value of your network investment. SDN, delivered through our market-leading solutions, will help your users and organization experience applications as never before. It will free your IT administrators from the drudgery of manual network configuration and reconfiguration because the network will be automatically tuned to application and business needs. Your IT staff can focus more on the quality of the business experience, and spend less time managing the details of the underlying networking infrastructure.

Our SDN strategy is built on the foundation of our open and scalable HP FlexNetwork architecture, which covers the entire path from the end user to the data center, as well as the technology stack from infrastructure to management.

HP Virtual Application Networks are at the core of our SDN strategy. With HP Virtual Application Networks, you can move to service-centric management and orchestration and gain business agility. To help ease your move to an SDN architecture, we've enabled OpenFlow in more than 50 of our switch models. And we plan to extend support across the FlexNetwork architecture. We're also building a vibrant third-party SDN developer ecosystem to further drive the open and extensible nature of the HP Virtual Application Networks SDN Controller.

SDN in a nutshell is

"… In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications …"

Open Networking Foundation

Value Proposition

The HP Software-defined Networking (SDN) provides an end-to-end solution to automate the network from data

center to campus and branch. Expanding the innovation of SDN, HP SDN ecosystem delivers resources to develop and create a market place for SDN applications.

The HP SDN ecosystem delivers the following benefits:

- Simple - Extending simplicity of programmability across the network with OpenFlow-enabled devices
- Open - Raising the value of SDN with an open environment delivered by SDN Software Development Kit (SDK).
- Enterprise ready - Fostering innovations with industry's first SDN App Store market place for SDN applications.

History

HP has been a leader in SDN since its inception. Dating back to the 2007, HP Networking started working with Stanford to deliver Ethane – the precursor to OpenFlow. In 2008 HP delivered the industry's first OpenFlow demo software for our switches. This is at least 6 years before any other vendor even started talking about OpenFlow – let alone deliver the code. In 2009, HP Networking was able to scale R&D lighthouse customers to 10. By 2010, HP had 60 R&D lighthouse customers. In 2011, HP delivered industry's first enterprise-class commercial software. HP was the first tier-1 networking vendor to deliver this capability. In 2012, HP announced the industry's first complete SDN solution spanning all three architectural layers – infrastructure, control and applications – and lead the industry in OpenFlow-enabled switches with more than 40 and 10 routers. And the industry's first cloud network technology that enables the deployment of cloud applications in minutes rather than months with Virtual Application Networks. HP delivered to market the VAN SDN Controller in September 2013 and will deliver enterprise ready applications in the spring of 2014.

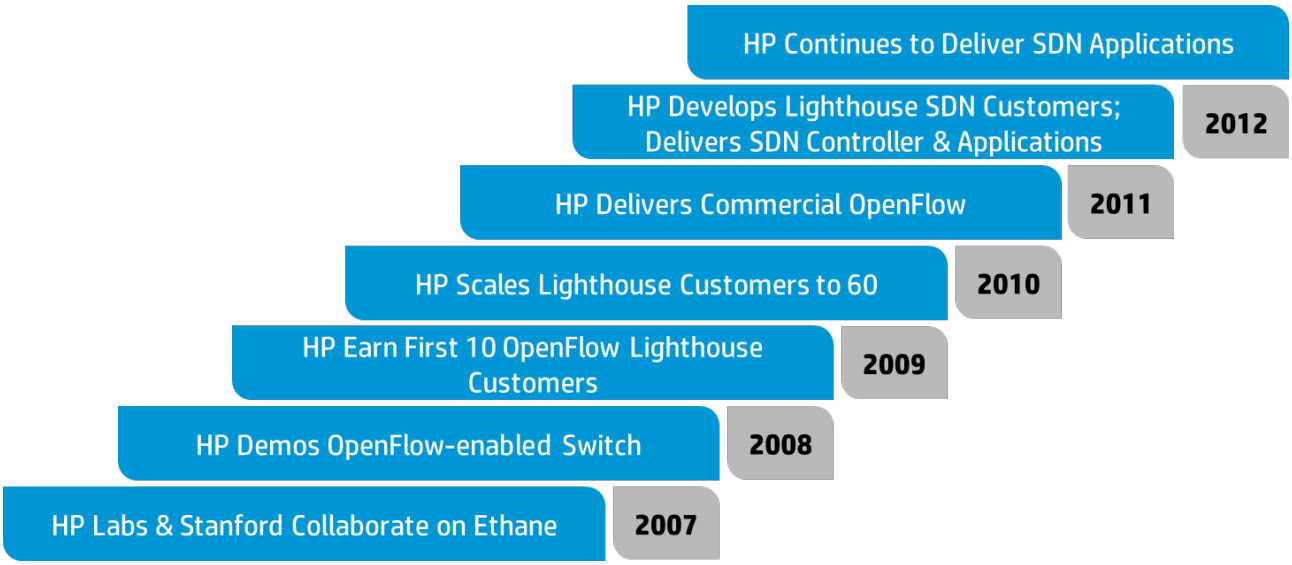


Figure 1: HP leading the industry in SDN

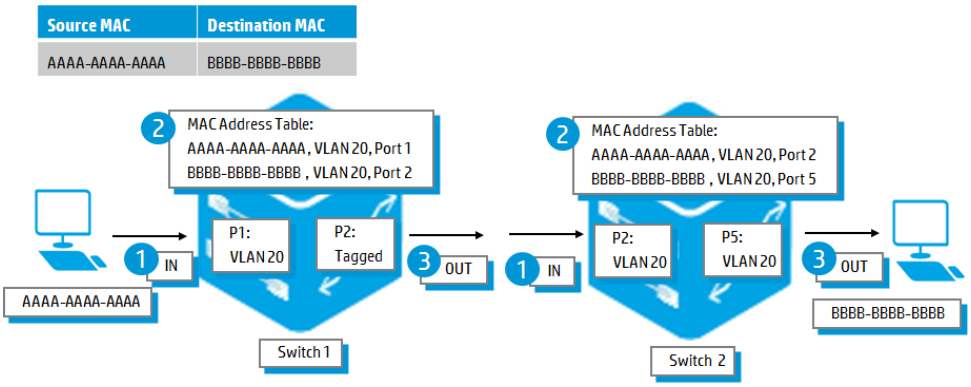
Virtual Application Networks is a framework for automating network operations using HP's industry-leading software-defined network technology to deliver the agility required for business to respond in minutes, not months.

Traditional Switching and Openflow

Destination Address-based Switching

In a traditional layer 2 switching environment, switching is performed based on destination MAC address. Each switch has its own MAC address table and each switch learns where devices are located.

Figure 2: Switching decisions based on destination MAC address



Process:

1. Frame arrives at Switch 1 from PC A (MAC = AAAA.AAAA.AAAA) to PC B (MAC = BBBB.BBBB.BBBB)
2. MAC address table is checked for location of PC B
3. Entry is found in forwarding table
4. Frame is transmitted out of port 2

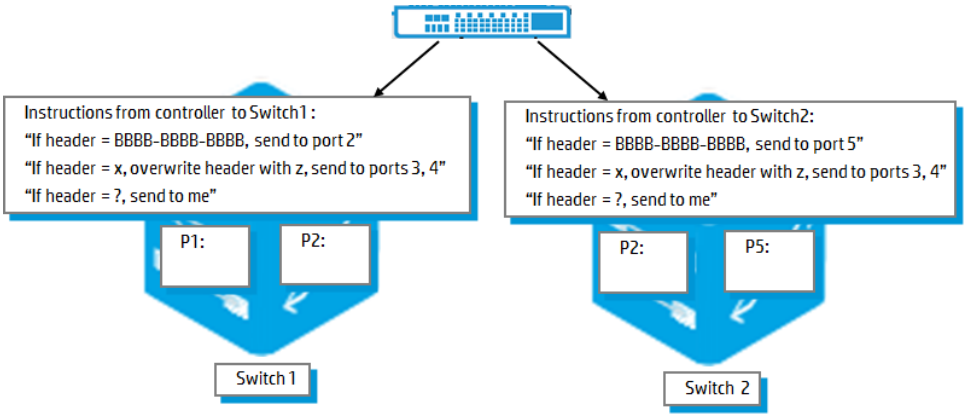
This process is repeated at every switch in the network.

A router would use a similar type of process based on destination IP address (unicast routing) and a routing table (RIB) and forwarding information based (FIB).

Flow-based Switching

In an OpenFlow environment, flow tables are used by devices rather than routing or MAC address tables.

Figure 3: Flow-based forwarding table configuration

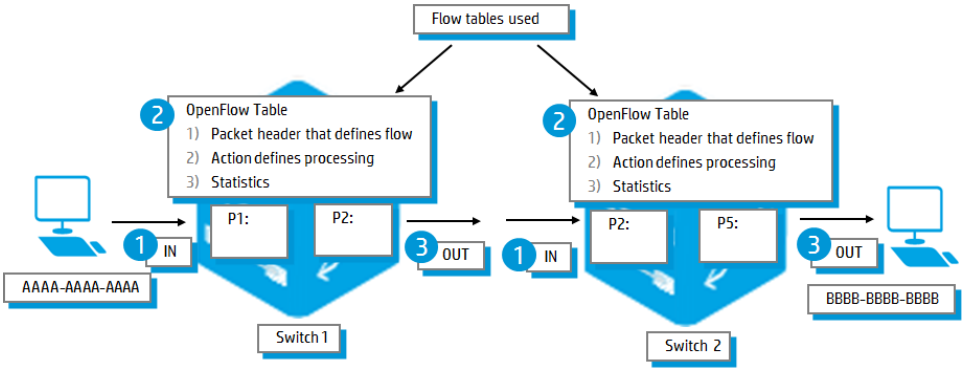


Each flow entry has an action associated with it. The three actions that all dedicated OpenFlow switches must support are:

- Forward: The first options is to forward this flow's packets to a given port (or set of ports). This allows packets to be switched through the network. In most switches it is expected that this takes place at line rate speeds.
- Redirect: The second option is to encapsulate the packet and forward this flow's packets to the SDN controller. The packet is delivered via a secure channel using TLS. The controller makes a decision and forwards the packet back to the switch. Typically, this method is only used for the first packet in a new flow, so a controller can decide if the flow should be added to the Flow Table. Or in some experiments, it could be used to forward all packets to a controller for processing.

- **Drop**: The third option is to drop this flow's packets. This can be used for security reasons to block unauthorized traffic, to stop denial of service attacks, or to reduce spurious broadcast traffic from end-hosts. HP Network Protector application can be used for this purpose.

Figure 4: OpenFlow table entries



An entry in the Flow-Table has three fields:

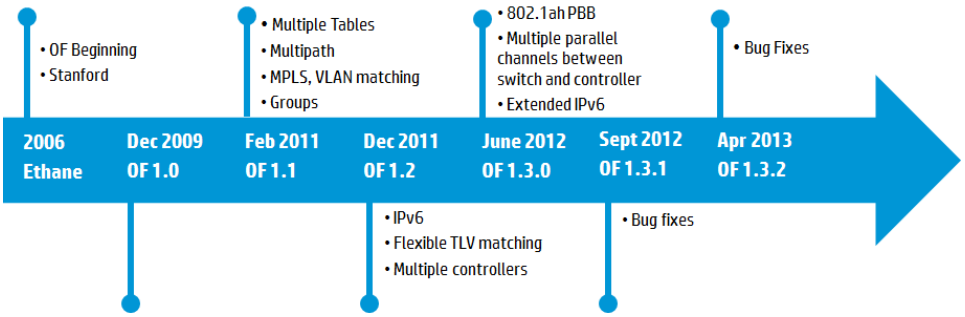
- A packet header that defines the flow (TCP port 80 traffic for example)
- The action that defines how the packets should be processed (Forward out of port G1/0/1)
- Statistics that keep track of the number of packets and bytes for each flow. (100 packets 8000 bytes for example). The time since the last packet matched the flow is also recorded so as to remove inactive flows. This can be configured within the HP SDN Controller. The default is a flow is active for 300 seconds.

OpenFlow Architecture

HP's SDN Controller supports OpenFlow versions from 1.0 to 1.3.1.

In 2006, Stanford PhD student, Martin Casado and others developed Ethane. This used the idea and approach to effectively and centrally manage global network policy. Ethane uses a flow based network and central controller with a focus on network security. Ethane later inspired the concept of OpenFlow.

Figure 5: OpenFlow roadmap



OpenFlow is a standards based protocol allowing for a centralized control plane in a separate device (the controller). Openflow provides hardware abstraction providing the controller a method to communicate with multiple vendor devices, multiple hardware types (routers, switches, load balancers and others), using a standard interface. This takes the control logic on how to perform packet forwarding and packet rules and putting those rules down into a hardware abstraction here where they can be followed by the individual network device.

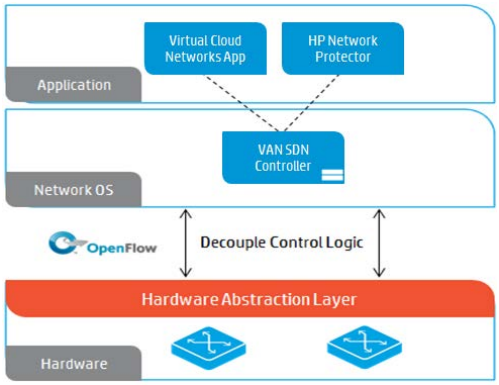
Most initial SDN devices are routers and switches. However, OpenFlow and SDN make provision for many device types and are not restricted to routers or switches. Other devices such as load balancers, firewalls and WAN optimization devices may also support SDN in future - any network forwarding device that can programmed to perform variety of activities is envisioned as part of SDN and OpenFlow.

OpenFlow is managed by the Open Networking Foundation (ONF).

OpenFlow is asynchronous. Switches can initiate conversations to the controller and the controller can initiate conversations to switches.

The Openflow protocol is a specification that defines the API to the forwarding point of an individual device.

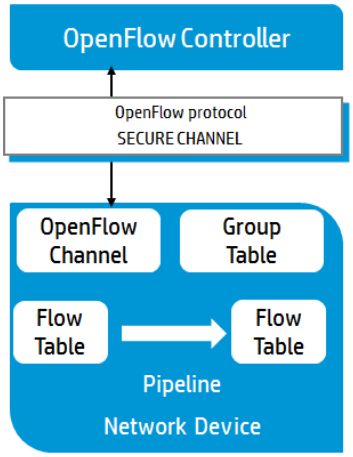
Figure 6: SDN architecture



OpenFlow Switch Components

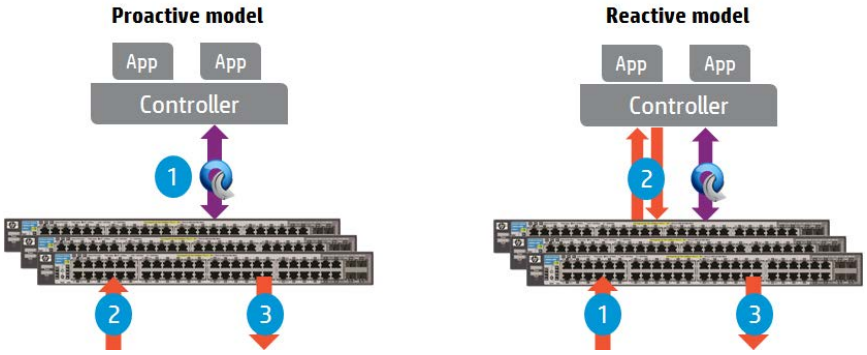
An OpenFlow Switch consists of one or more flow tables and a group table, which perform packet lookups and forwarding, and an OpenFlow channel to the HP SDN Controller. The switch communicates with the HP SDN controller and the controller manages the switch via the OpenFlow protocol. Is OpenFlow secure? Is there a security risk of someone hacking into my device and injecting rules that affect the traffic flows? The OpenFlow protocol provides a secure channel that is certificate based. This is TLS (Transport Layer Security) based. TLS is the successor to SSL (Secure Sockets Layer) and provides cryptographic protocols for communication security. TLS is used widely for secure transmissions on the Internet.

Figure 7: OpenFlow switch components



Using the OpenFlow protocol, the controller can add, update, and delete flow entries in flow tables, both reactively (in response to packets) and proactively. Each flow table in the switch contains a set of flow entries; each flow entry consists of match fields, counters, and a set of instructions to apply to matching packets.

Figure 8: Proactive and reactive flow table updates



Matching starts at the first flow table and may continue to additional flow tables. Flow entries match packets in priority order, with the first matching entry in each table being used. If a matching entry is found, the instructions associated with the specific flow entry are executed. If no match is found in a flow table, the outcome depends on configuration of the table-miss flow entry: for example, the packet may be forwarded to the controller over the OpenFlow channel, dropped, or may continue to the next flow table.

Instructions associated with each flow entry either contain actions or modify pipeline processing. Actions included in instructions describe packet forwarding, packet modification and group table processing. Pipeline processing instructions allow packets to be sent to subsequent tables for further processing and allow information, in the form of metadata, to be communicated between tables. Table pipeline processing stops when the instruction set associated with a matching flow entry does not specify a next table; at this point the packet is usually modified and forwarded.

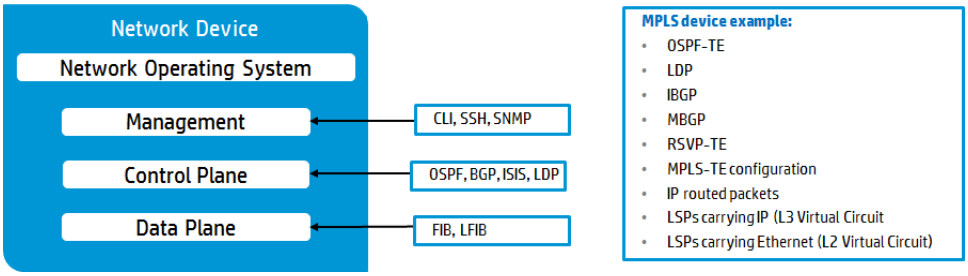
Operational Planes

Traditional Switch

In traditional network devices there are three planes of operation

- Management Plane
- Control Plane
- Forwarding Plane

Figure 9: Traditional device architecture



In a traditional router or switch, the forwarding or data plane and the high level routing decisions (control plane) occur on the same device. Examples of control plane protocols include OSPF, BGP, ISIS and LDP.

Tables used in the data plane include the Forwarding information base (FIB) or Label Forwarding information base (LFIB).

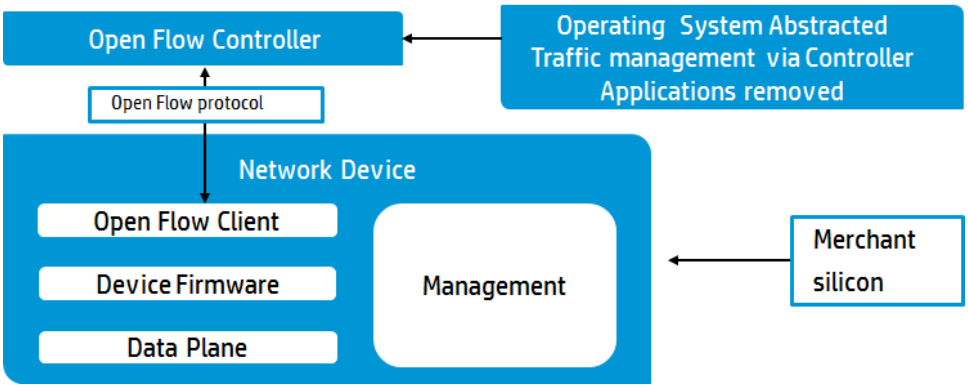
Pure OpenFlow Switch

A pure OpenFlow Switch separates these two functions. The data path portion still resides on the switch, while high-level routing decisions are moved to a separate controller, typically a standard server.

The OpenFlow Switch and Controller communicate via the OpenFlow protocol, which defines messages, such as packet-received, send-packet-out, modify-forwarding-table, and get-stats.

A pure OpenFlow switch is essentially a "dumb" device that forwards packets between ports, as directed by the SDN Controller. In this context, flows are broadly defined, and are limited only by the capabilities of the particular implementation of the Flow Table.

Figure 10: OpenFlow switch architecture

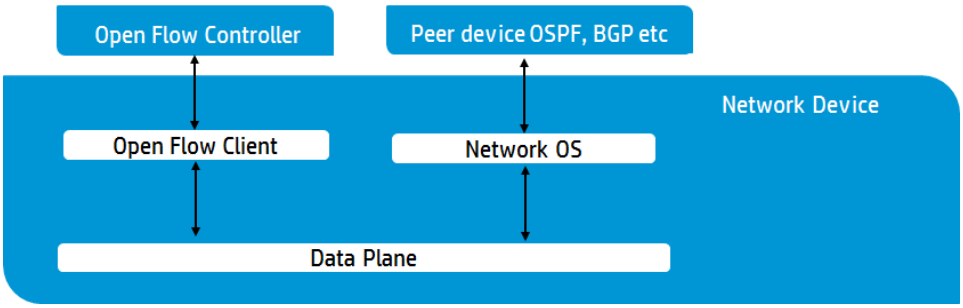


Hybrid Switch

The hybrid mode answers the question: Do I have to have a green field environment to build an Openflow network? The answer is No.

The approach that HP taken is to allow hybrid mode where a single VLAN can be run in OpenFlow while other VLANs run in traditional mode using traditional protocols. This occurs within the same network device.

Figure 11: Hybrid switch architecture

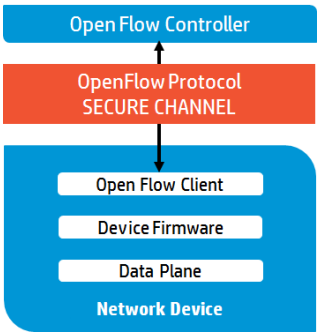


This approach allows for simple migration starting with a set of Openflow devices connected to the "openflow" VLAN.

OpenFlow Security

As OpenFlow is a critical component of the network, the communication between the controller and the devices needs to be protected. The OpenFlow protocol provides a secure channel that is certificate based. This is TLS (Transport Layer Security) based. TLS is the successor to SSL (Secure Sockets Layer) and provides cryptographic protocols for communication security. TLS is used widely for secure transmissions on the Internet.

Figure 12: OpenFlow Secure Channel



HP VAN SDN Solutions for the Campus

Two of the SDN solutions for the Campus LAN from HP include HP Network Protector and HP Network Optimizer.

Network Protector utilizes SDN and the OpenFlow protocol to push security to the edge of the network where clients connect. Instead of malicious traffic traversing a network to the core and getting blocked by an IPS, it can now be blocked at the edge without having to add a dedicated security appliance. Network Protector can be used to turn a traditional access layer switch into a security appliance.

Network Optimizer utilizes SDN and the OpenFlow protocol to dynamically provision QoS for Microsoft Lync voice, video, and application sharing calls in a way that is not possible with traditional QoS.

This document discusses the HP Network Optimizer solution.

About HP Network Optimizer

Deploying trusted and granular quality of service (QoS) can be extremely complex and require implementing tedious and time-intensive manual configurations on a device-by-device basis. In fact, it is nearly impossible to implement traffic policy using deep packet inspection (DPI) for soft clients with legacy networks because of because of SIP TLS encryption and dynamic application ports used by UC&C applications, resulting in poor application traffic visibility.

HP is announcing a new SDN application to address these issues.

This SDN application will automate policy deployment dynamically on a per-connection basis for voice, video, and application sharing to deliver a better user experience and reduce operational costs. When a desktop sharing, voice, or video connection is initiated using the Microsoft® Lync client in the campus or branch office, the Lync Server in the data center provides the HP Network Protector SDN Application with call details such as source and destination IP address, protocol type, application ports, and bandwidth requirements at the start and end of every call. Network Optimizer then uses these per-connection application details to dynamically provision the end-to-end network path and QoS policy via the HP Virtual Application Networks (VAN) SDN Controller using OpenFlow.

Once the QoS policies and path are programmed via OpenFlow, the call is connected to the destination client. The HP Network Optimizer SDN Application uses the intelligence from Lync Server and the Lync SDN API, along with the robust capabilities of the HP VAN SDN controller, to implement consistent QoS across the network. All of this is done dynamically through a central point of control; eliminating the need for manual, device-by-device configuration via the CLI, which greatly simplifies policy deployment and reduce the likelihood of human errors.

Figure 13: Network Optimizer Dashboard

How the Solution Works

The Network Optimizer SDN application utilizes OpenFlow to dynamically prioritize traffic at the edge of a network. Traditionally there are 4 ways that traffic can be identified so that it can be prioritized.

- First, it is possible to prioritize all traffic from a device. This method is used with traditional VoIP phones by placing the phone in a voice VLAN and prioritizing all traffic in that VLAN. Typically, an ACL would also be used to stop all traffic not destined for the VoIP server. This solution is not possible with Microsoft Lync because the client is a soft client running on PC.
- Second, if a solution uses a predefined TCP or UDP port number, traffic matching that port can be prioritized. This is not an option with Lync because it dynamically assigns ports from a wide range so that it can support multiple calls between many parties simultaneously.
- Third, it is possible to copy network traffic to an analyzer to determine its nature. Even when this solution is possible, it requires a significant amount of network bandwidth and processing power on the analyzer which is a waste of expensive and precious resources. However, in the case of Lync this is not possible because all traffic is encrypted, making analysis impossible.
- Lastly, it is possible for the client to tag traffic as important and configure the network to trust the tags. While this will work and Lync does support it, this solution requires a level of trust from network clients that is not reasonable. As soon as the network trusts a client, there will be users who abuse the trust and artificially prioritize all of their traffic. In other words, a user could use a company's network to watch Netflix movies in full HD.

This left HP and Microsoft to determine a new method to prioritize traffic. It was realized that the Lync server had complete knowledge of all calls happening in an environment. Microsoft, in collaboration with HP, developed an API that installs on the Lync server and can make RESTful API calls to HPs Network Optimizer SDN Application with

all of the call details, including users, type of call, and bandwidth requirements. Network Optimizer can then dynamically prioritize traffic on the network for the duration of the call.

There are two ways to prioritize the interesting traffic based on the capabilities of the network. When HP first demonstrated this solution, it was assumed that the entire network was OpenFlow enabled. This is a great solution because it doesn't require any QoS configuration on the network. According to some enterprises, it can take more than six months to deploy a QoS solution on a network.

However, it became apparent that the assumption of a 100% OpenFlow enabled network was not reasonable. Therefore, it was decided to approach the first release of the product with the assumption of a hybrid network where only the edge, or access devices, were OpenFlow enabled. In this case, the Lync SDN solution does DSCP remarking at the edge of the network and the rest of the network is configured to trust the markings supplied by the access layer device. It was previously described that trusting QoS settings was a bad idea. But in this case, the access layer devices are doing the marking and not the end user clients. When Network Optimizer boots, a default flow is pushed to all access devices that remarks all traffic to normal priority in the specified VLANs. Then it is possible for Network Optimizer to dynamically prioritize the Lync traffic to an administratively assigned priority.

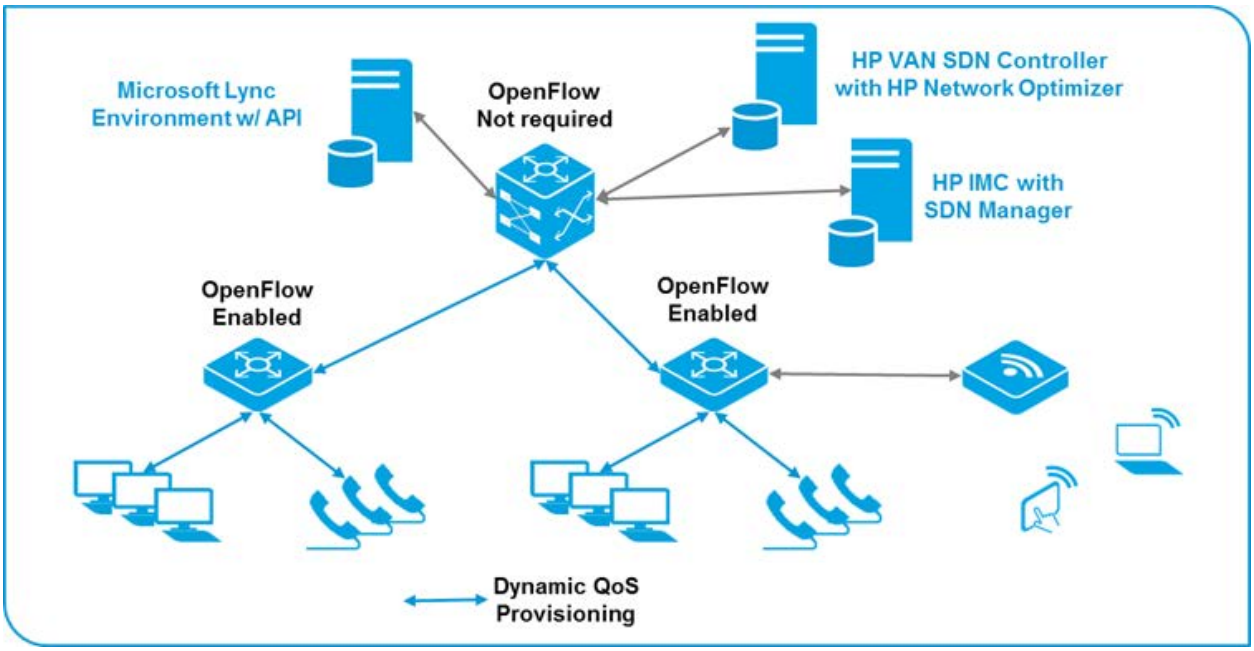
Out of the box, this solution will work without additional configuration for clients that are attached to OpenFlow enabled devices. In the case where one client is not directly connected to an OpenFlow enabled device, it is possible for a network administrator to configure a gateway for a known group of devices. This will enable prioritization to be dynamically assigned for the network under an administrator's control.

Deployment

SDN applications will have varying deployment requirements. Applications that operate in a proactive method have more flexibility in their deployment options. Whereas, reactive SDN applications should be deployed as close as possible to the network they control. This is required to reduce network latency and improve user experience. While HP Network Optimizer is a proactive SDN application it is recommended that it be deployed as close to the network under its control as possible. Therefore it may be necessary to deploy several instances of Network Optimizer to support physically separated networks.

The topology below shows a typical deployment for a single site with less than 10,000 users.

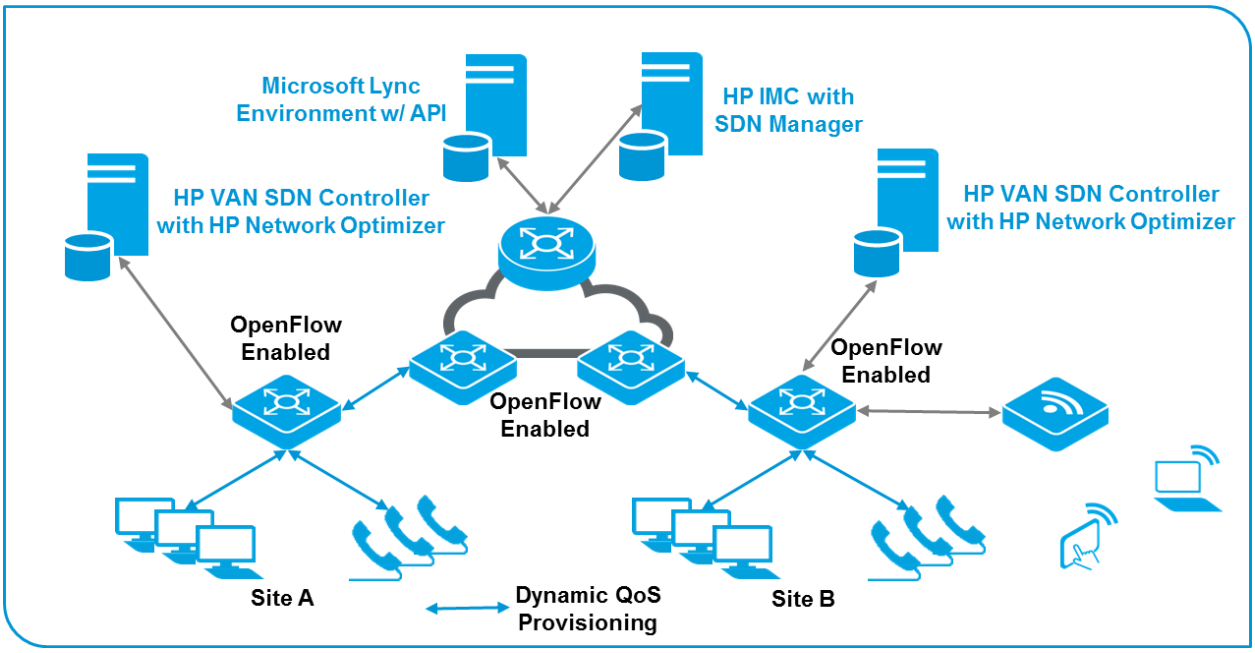
Figure 14: HP Network Optimizer Deployment on a single site



The topology below shows a typical deployment with multiple sites. In this case it is recommended to deploy an instance of the HP VAN SDN Controller with HP Network Optimizer on each site. This deployment does require additional configuration. Within the configuration of Network Optimizer on each site it is necessary to define the IP

address range on the other site and the address of the gateway used to reach the other site. This enables dynamic provisioning of QoS between the client and the gateway.

Figure 15: HP Network Optimizer Multi-Site Deployment



If there is a single site with more than 10,000 users, it would be necessary to break up the site as if it were multiple sites.

Performance

An instance of Network Optimizer can support an infrastructure up to 2,000 OpenFlow enabled devices and up to 10,000 users. These numbers assume minimum system requirements of a quad-core processor, 8GB of RAM, and 64GB of available disk space.

Redundancy

In the first release of HP Network Optimizer, HA is not supported. To maximize network availability, the OpenFlow enabled devices in a network should be configured to fail open in the case of controller unavailability. Network Optimizer is designed to operate in a hybrid way. That means that traffic is forwarded using traditional networking methods based on destination MAC address or destination IP address. When a switch fails open, these same traditional forwarding mechanisms will continue to forward traffic as expected.

Security

Network security has been a critical concern for a very long time. With the advent of SDN that does not change. The methods of securing a network do require an evaluation. There are several mechanisms that aid in securing an SDN environment. First, the connection between a switch and controller should be passed on a dedicated management VLAN or, for addition security, be handled on a completely out of band network. An out of band network is likely not possible in a campus LAN but may be possible in a datacenter. Second, the communication between an OpenFlow device and the controller should be authenticated and encrypted. The HP VAN SDN Controller and HP switches support mutual authentication using certificates and TLS. Access to the controller for management purposes is also encrypted using TLS and authenticated using OpenStack Keystone.

Specifications

HP Network Optimizer version 1.0	
Supported Platform	Supported Platform: HP Virtual Application Networks (VAN) SDN Controller version 2.2 • Quad-core CPU

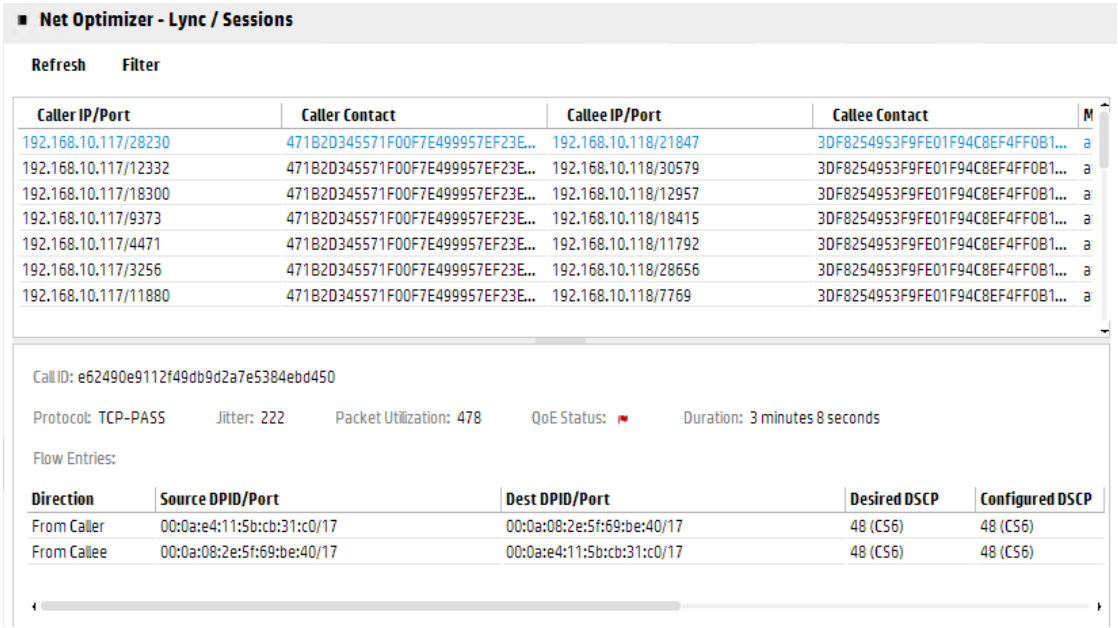
	• 8GB RAM • 64GB available disk space • One 10Gbps network interface • Ubuntu 12.04 • Prerequisites: openjdk-7-jre update 25, keystone, unzip, curl
Supported Switches	HP 8200zl running K.15.14 or higher (Note: higher user density is supported with only v2 modules installed and the command “no allow-v1-modules”)
	HP 6600 running K.15.14 or higher
	HP 6200yl running K.15.14 or higher
	HP 5400zl running K.15.14 or higher (Note: higher user density is supported with only v2 modules installed and the command “no allow-v1-modules”)
	HP 3800 running KA.15.14 or higher
	HP 3500 running K.15.14 or higher
	HP 2920 running WB.15.14 or higher
	Open vSwitch with DSCP remark capability using OpenFlow 1.0
Microsoft Lync	Version 2010 or 2013
Microsoft Lync SDN API	Microsoft Lync SDN API version 1.2 or 2.0

Note:
Software version K/KA/WB15.15 adds improvements in user density.

Value Proposition

HP Network Optimizer provides and experience with the Microsoft Lync soft client that users have come to expect with traditional analog voice connections and VoIP based on hard phones. This allows an enterprise to support the mobility demanded by employees and users and offered by Microsoft Lync and still get the experience they want. Calls are dynamically provisioned without administrative involvement.

Figure 16: Network Optimizer Sessions



Frequently Asked Questions

What is required to implement Network Optimizer? Network Optimizer requires OpenFlow enabled switches at the access layer of the network. It is installed as an application on the HP VAN SDN Controller. The controller can be deployed as a virtual machine or on a bare metal server. However, higher network throughputs can be supported when installed on a bare metal server. It is also necessary to configure QoS on the distribution and core devices in a network to trust the DSCP markings that are set at the edge of the network. This solution also requires the Microsoft SDN API and SDN Manager to be installed in the Lync environment.

How does Network Optimizer work with Lync hard phones? Network Optimizer can be configured to provide dynamic provisioning for hard phones in addition to soft phones. It is also possible to maintain an installed and configured voice VLAN for these hard phones in collaboration with Network Optimizer.

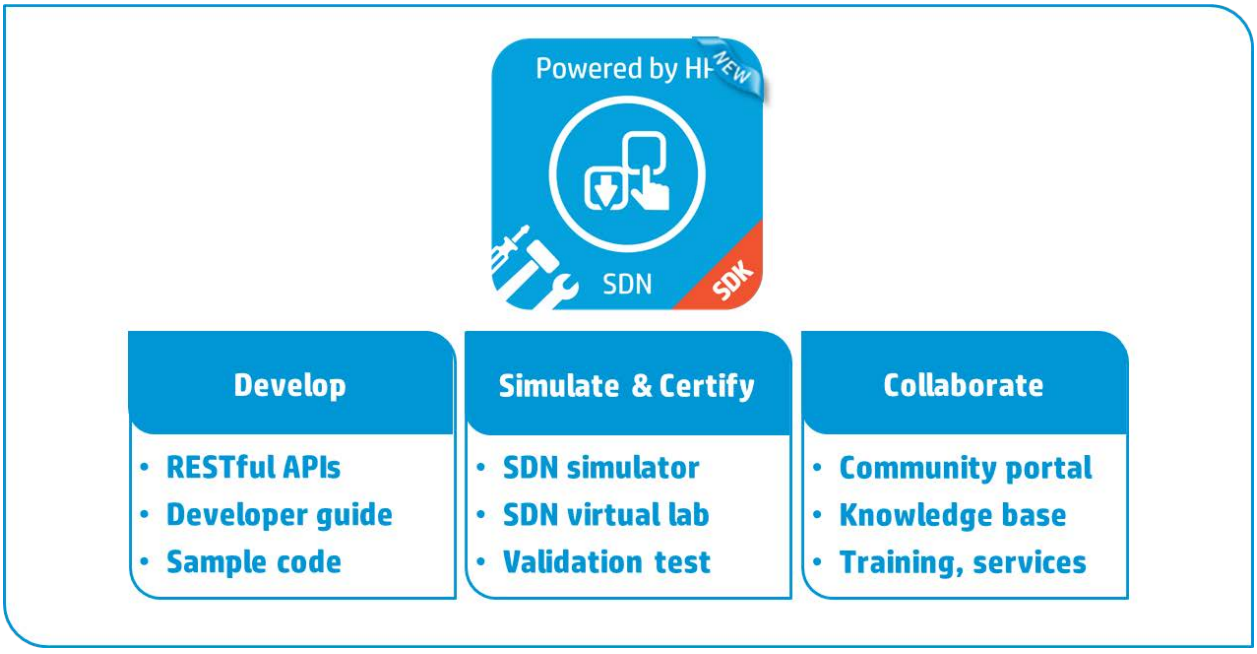
How does Network Optimizer scale? An instance of Network Optimizer can support an infrastructure up to 2,000 OpenFlow enabled devices and up to 10,000 users.

Where should Network Optimizer be deployed? Network Optimizer should be deployed local to the LAN it is configured to provision. Any additional latency added by a remote connection, could delay QoS provisioning and the user experience.

HP SDN Software Development Kit (SDK)

HP has made an SDK available with the VAN SDN Controller that provides developers all the tools necessary to build SDN applications for the HP Controller. The SDK includes documentation for both the Java and REST APIs as well as all of the jar files necessary during compilation. A sample application is also included. For Alliance ONE partners there is also a remote lab available for testing SDN applications with real hardware. HP also hosts and monitors a developer's forum where developers can collaborate to get answers to questions. For more information and help with developing a new application, please go to http://sdndevcenter.hp.com.

Figure 17: HP SDN SDK

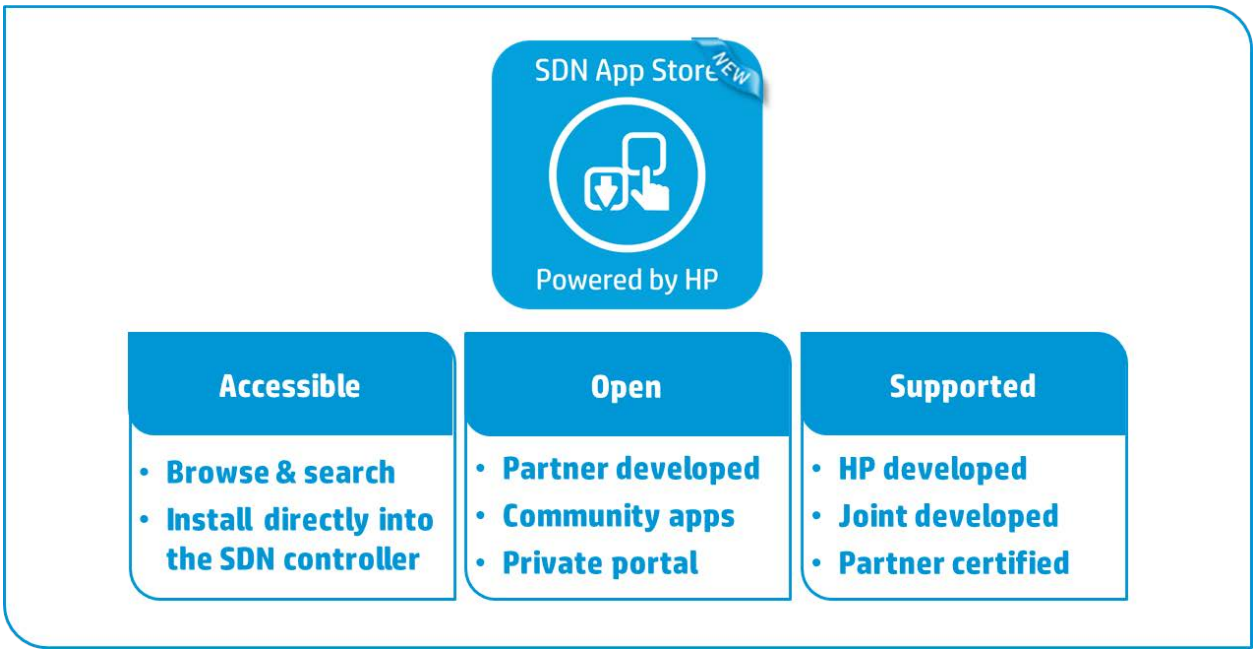


HP SDN App Store

HP is hosting an App Store for the delivery of SDN applications. Application from HP, Alliance ONE partners and the community at large will be made available in the App Store. All Apps will be purchasable with a credit card and

select HP and Partner Apps will also be available for purchase through the traditional channel with deliver through the App Store

Figure 18: HP SDN App Store



HP SDN Services

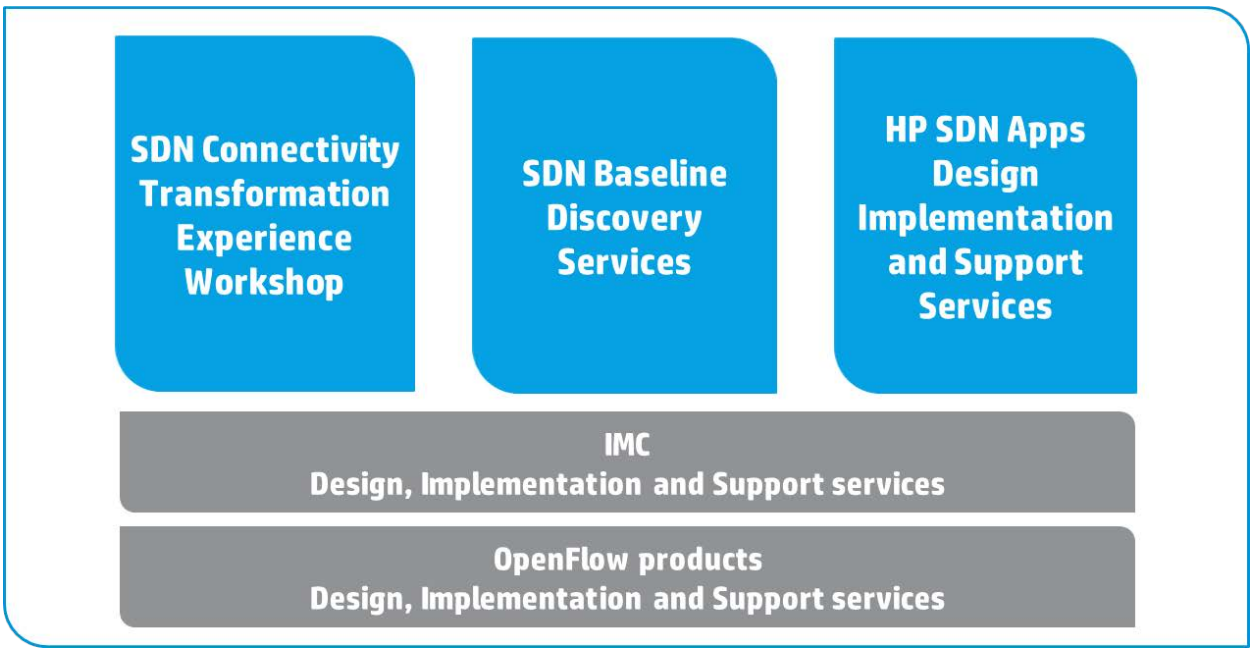
HP SDN Services provide a pragmatic path to assist customers in their SDN journey.

HP's strategy services such as the SDN Connectivity Transformation experience workshop focuses on achieving alignment on a future vision, current reality and an initiative roadmap on the transformational journey.

HP's SDN Baseline Discovery Services help customers to understand their current state from multiple dimensions – network baseline, network characterization and network provisioning baseline (including people and process elements)

Complementing our strategy services and current state definitions services, customers can then take advantage of HP's SDN Apps, IMC and OpenFlow products design, implementation and support services which offers expertise and capabilities to bring the right SDN solutions and deploy them in their environment.

Figure 19: HP SDN Services



Resources, contacts, or additional links

HP Software-defined Networking
hp.com/sdn

SDN Develeopers Central
sdndevcenter.hp.com

Learn more at
hp.com/networking

Sign up for updates

hp.com/go/getupdated

Share with colleagues

Rate this document

Created March 2014