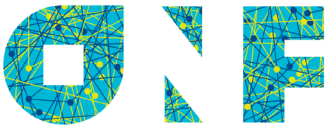


OPEN NETWORKING FOUNDATION

Request for Information (RFI) Template for Migration to Software Defined Networking (SDN)

Version 1.0
February 9, 2016

ONF TR-524

ONF Document Type: Technical Recommendation
ONF Document Name: Request for Information (RFI) Template for Migration to Software Defined Networking (SDN)

Disclaimer

Open Networking Foundation
2275 E. Bayshore Road, Suite 103, Palo Alto, CA 94303
www.opennetworking.org

Table of Contents

1. Introduction 4
1.1 RFI Template Development Objective 4
1.2 Intended Audience and Updates 4
1.3 Terminology 5

2. Architecture for SDN Migration 7

3. Operator Type and Identity Information 9

4. Considerations for Gathering Information 11
4.1 General Migration Requirements 11
4.2 SDN Migration Solution Requirements 13
4.3 SDN Migration Device and Function Requirements 13
4.3.1 Common Set of Requirements 13
4.3.2 Industry/Service Specific Requirements 16

5. Conclusions 18

6. Acknowledgements 19

7. Revision History 19

8. References 20

Appendix A: SDN Migration Prototyping Results 21

Contributors 24

1 1. Introduction

1.1 RFI Template Development Objective

A request for information (RFI) is a standard business process whose purpose is to collect written information about the capabilities of various suppliers, vendors, or providers. Normally it follows a format that can be used for comparative purposes, and is usually a preliminary activity in an acquisition or deployment process. The objective of this document is to offer a generic Request for Information (RFI) template for the Operators and Service Providers who are at the early stage of use case [1] based migration from a traditional network to a Software Defined Network (SDN [2, 3]).

This document also attempts to describe the challenges that the network operators must address for migration from a traditional network to an SDN based architecture. The migrated network may contain both traditional and SDN based networking elements in order to facilitate multi-phase migration to full SDN based system.

1.2 Intended Audience and Updates

This RFI template is intended to serve as a guideline for network services operators who are considering gathering information on migrating to SDN based network architectures, in particular when OpenFlow is used as the protocol for the interface between separated control and data planes.

Since SDN capabilities of interest may be different for various network segments and the respective operators, the first section of this RFI allows the operators to describe their interest to the vendors and provide information about their existing operations and architecture.

This allows the solution providers and vendors to be more precise in answering the questions related to their equipment capabilities.

It is expected this document will be updated frequently as the requirements and use cases evolve.

1.3 Terminology

The terminology used in this document is based on those in the Architecture documents [3].

API: Application Programming Interface – an Interface that can be directly called by software.

Application-Controller Plane Interface (A-CPI) / North-Bound Interface (NBI): An Interface Permitting SDN Clients to interact with the network via SDN Controllers.

(SDN) Controller Plane: The architectural plane (layer) performing logically centralized control and management of physical and virtual network elements/resources.

Data-Controller Plane Interface (D-CPI)/ South-Bound Interface (SBI): An Interface through which a real or virtual NE can be controlled / configured / managed (e.g. OF-Config / Netconf), monitored (e.g. SNMP or sFlow), or have its forwarding behavior influenced by an external entity (e.g. by an SDN Controller via OF-Switch).

Domain: A set of Network resources that is controlled in some sense by a specific entity: an administrative domain is administered by the entity, a business domain is owned by the entity, etc. (Although not the norm, multiple entities can in some cases jointly control a domain.)

Interface: A mechanism to permit software / hardware entities to interact, either within a processor / element (API) or between processors (RPC Interface / Protocol Interface).

Inter-SDN-Controller Interface: An interface permitting SDN Controllers to interact, either within the same administrative domain (intra-domain) or between administrative domains (inter-domain).

IP / IPv4 / IPv6: Internet Protocol / IP version 4 / IP version 6.

MPLS / MPLS-TP: Multi-Protocol Label Switching / MPLS Transport Profile.

Network Element (NE): An instance of network resources that is managed as a unit. The instance terminates/originates traffic and/or process traffic for forwarding the traffic flows. Examples include an OpenFlow switch, a web server, an L2 switch, an L3 router, a firewall, a load balancer, etc.

Network Function (NF) / Network Service (NS): A specific data plane traffic-processing function (or set of functions) performed by the network, e.g. load balancing, network access control, content caching, etc. Some use the term Network Service for a set of associated individual Network Functions.

NFV: Network Functions Virtualization.[1]

[1] ETSI/ISG NFV, http://www.etsi.org/technologies-clusters/technologies/nfv

OF-Config Protocol: An ONF protocol that addresses the interface between an SDN Controller and a physical network element (physical switch).

OF-Switch Protocol (formerly known as OpenFlow Protocol): An ONF protocol that addresses the interface between an SDN Controller and a logical switch. Together with the OF-Config Protocol, this represents an instance of a Data-Controller Plane Interface (Southbound Interface).

OTN: Optical Transport Network.

Protocol Interface (PI): An Interface implemented as a (network) protocol.

SDN: Software Defined Networking.

SDN Controlled: Controlled using SDN mechanisms (e.g. OF-Switch / OF-Config, with network resources being controlled by the logically centralized SDN Controller).

SDN Controller: A software/hardware system performing logically centralized control and management of network elements and offering network services to zero or more tenants or apps. The SDN controller may be physically implemented on a single platform, or it may be physically distributed.

SDO: Standards Development Organization.

SNMP: Simple Network Management Protocol.

Traditionally Controlled: Controlled using non-SDN mechanisms (typically using a distributed control plane protocol like OSPF / STP, implemented on fully-distributed network controllers.

Tunnel: A tunnel transparently conveys client traffic (i.e., traffic using the tunnel) from an origination point to a termination point over an underlay network.

VNF: Virtual Network Function.

2 Architecture for SDN Migration

A simple high-level SDN architecture is as shown in Figure 1a.

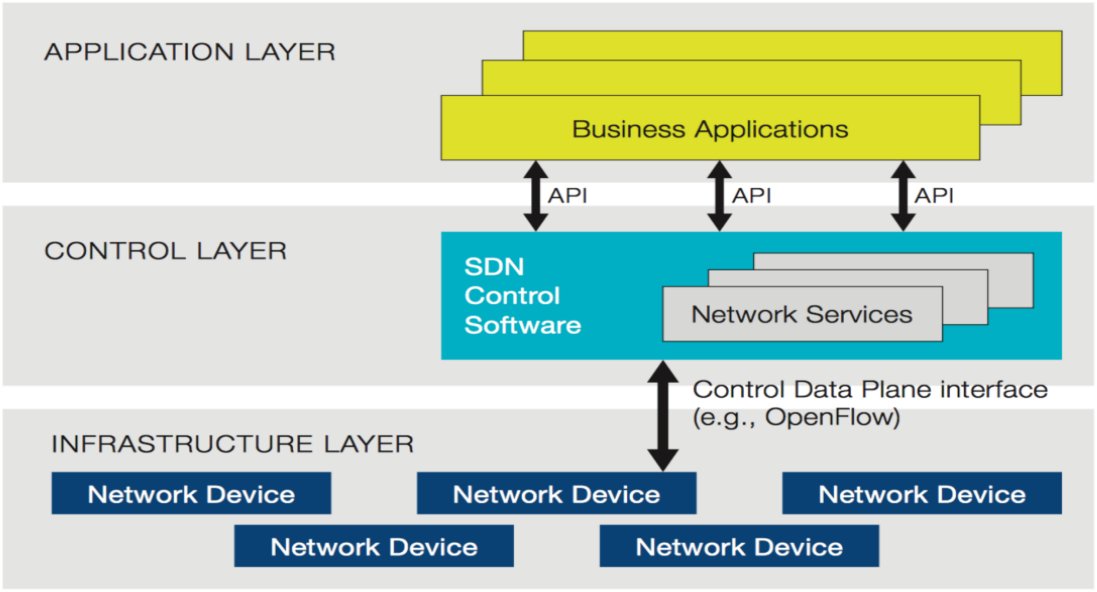


Figure 1a: High-Level SDN Architecture

(Source:https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf)

Another more generic, high-level SDN architecture is as shown in Figure 1b.

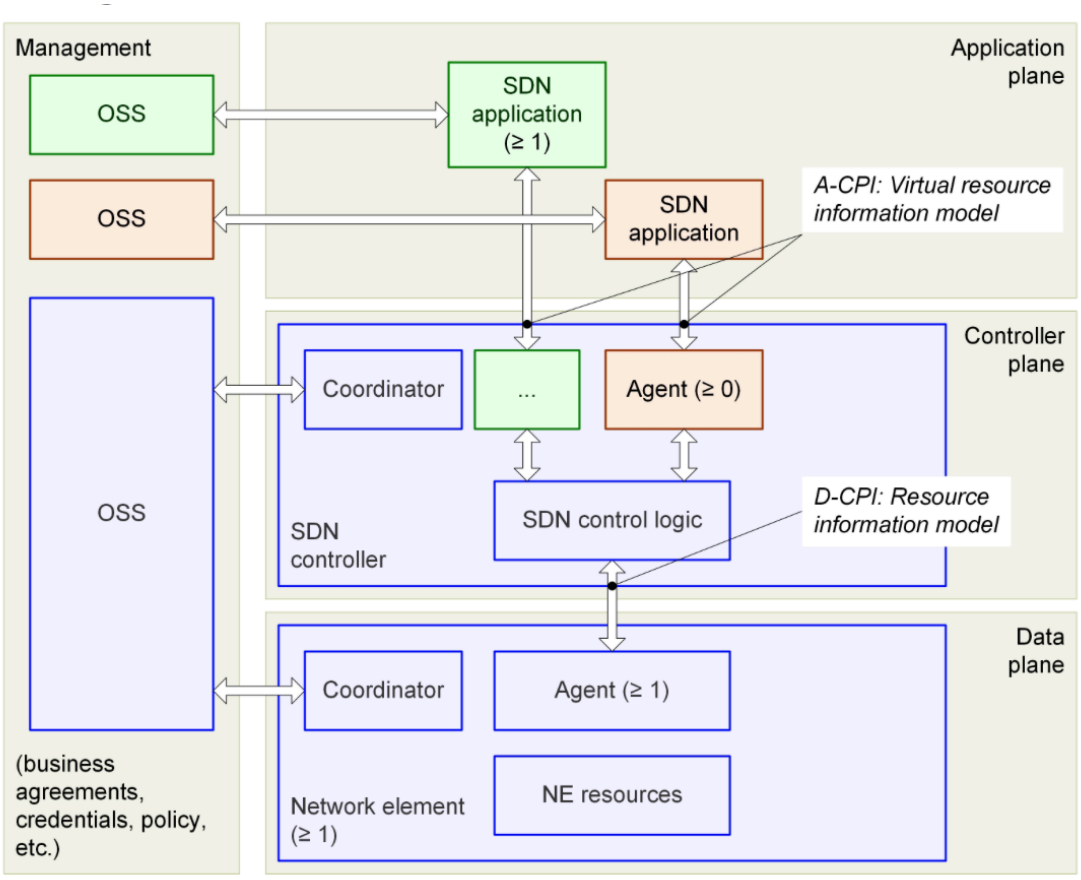


Figure 1b: High-Level SDN Architecture with Management Plane

(Source: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN-ARCH-Overview-1.1-11112014.02.pdf)

The above diagram shows a more detailed SDN architecture where it is possible to support integration with a traditional (legacy) network via the operations support system (OSS) and management plane elements.

Table-1 has high-level requirements for migration to SDN based network. The degree to which these requirements need to be addressed may vary depending on the type of operator and the services.

Table-1: General Architecture Requirements for Migration to SDN

Requirement Number	Requirement Description	Comments
Req-Arch-01	Separation of control and forwarding; apps and service may remain a part of control domain initially	
Req-Arch-02	Virtualization, on if and as needed basis	
Req-Arch-03	Logical centralization of all of the controls; different controllers may manage different network sections and domains including controlling the security of the physical and virtual devices	
Req-Arch-04	Automation of provisioning and management	
Req-Arch-05	Orchestration and brokering of resources management. This may be driven by application and service requirements	
Req-Arch-06	Stability and survivability of the network and services	
Req-Arch-07	Support of the SDN migration plan, seamlessly	
Reg-Arch-08	Security Framework for Services and Controller Access	

3 Operator Type and Identity Information

Flexibility of the SDN architecture allows any and all types of Operators and Service Providers to use, integrate with, and deploy both physical and virtual infrastructure based networked services. It is very helpful for solution and equipment suppliers to know the type and identity of the Operator in order to satisfactorily answer the requirements related queries.

Table-2 focuses on operator type and identity related information (following page).

Table-2: Operator Type and Identity Related Information

Op Type Identity No.	Description	Comments
Op-Type-01	Operator Type: a. Traditional wireline or wireless or both types of operators b. Data Center Operators to support content distribution, mobile audio/video/data services, analytics, storage and recovery services, etc. c. Enterprise (both virtual and infrastructure based) Service Providers d. ISPs, CSPs, and others (XSPs) e. Virtual operator (MVNO) f. Campus Networks (University, Hospital/Healthcare, Finance etc. networks) g. Cloud Services Provider h. Others (please be specific)	
Op-Type-02	Existing Network Architecture (migration candidate): a. CPE devices b. Access network c. Edge Network d. Transit Networks e. Core Network f. Interconnection networks g. Special Purpose Networks (e.g., GENI, I-2 regional networks, etc.) h. Others (please be specific)	
Op-Type-03	Identification of Migration Paradigms and Points a. Software based Migration b. Hardware up-date/-grade based Migration c. Other options, … … …	
Op-Type-04	Use of virtualization during/after Migration a. Timeline for introducing virtualization b. Role of virtualization during/after Migration c. Type of virtualization and orchestration infrastructure d. Others …	
Op-Type-05	Site or PoP Requirements and Architecture, as/if applicable a. Initial Phase b. Target with timeline (3 year, 5 year, etc.) c. Intermediate Phases	

Op-Type-06	Testing and Certifications requirements for new equipment in the network (self-testing or third-party facility for testing)	
Op-Type-07	SDN Controller being used or in plans, if known or if there is any preference of Open Source or others	
Op-Type-08	Software Stack to be used with on top of OpenFlow enabled controller/nodes, if known or if there is any preference	
Op-Type-09	Training and (ONF) certification requirements for the migration team	
Op-Type-10	Any requirements to integrate with existing Security Framework and Infrastructure	

4 Considerations for Gathering Information

Once an Operator selects a high-level SDN Architecture, both general and specific (to network and services) requirements must be satisfied before committing to any deployment phase.

4.1 General Migration Requirements

In order to maintain the same level of service quality and user experience, the Operator may need to satisfy the following (**Table-3**) general migration requirements.

Table-3: General Requirements for Migration to SDN

Requirement Number	Requirement Description	Comments
Req-Gen-01	Continued Interoperability: Interoperability between the existing networking infrastructure and the new SND infrastructure guarantees seamless service experience	
Req-Gen-02	Desired Level of Scalability: Initial deployment may need to be scaled for certain segments of the network; as the SDN capable elements are introduced throughout many segments of the network, the scalability of the control plane elements will be required, and both hierarchical and peered sub-controllers may need to be supported The scalability of the value-added networking/service functions and forwarding elements may need a combination of both virtual and physical devices	

Req-Gen-03	Desired Level of Security: Deployment of SDN elements must not impact the security policy of network operation; the principles and practices for securing SDN can be found in the ONF Security WG documents (https://www.opennetworking.org/technical-communities/areas/services) Different levels of authentication and authorization are likely to be needed for control, data, management, and operations planes Event Logging and monitoring will be needed for audits and verification	
Req-Gen04	Desired Level of Resiliency and Fault Tolerance: In order to maintain a desired level of resilient and fault-tolerant operations, deployment of any or all components of SDN architecture must handle errors, transient conditions, and component/element failures gracefully Handling of Errors: The elements of SDN architecture must handle the error scenarios and conditions gracefully without impacting any other interface and network/service functions. Any propagation of error throughout other network functions /components must also be prevented or must be kept contained within a pre-specified (logical) boundary Handling of Transient Conditions: During any single- or multi-phase deployment of SDN architecture, both controller and forwarding elements must handle the transition phases gracefully. Some platforms may offer testing and verification of configuration of control and forwarding entities during the transition (from legacy to SDN) period before committing any service to SDN based operation Supporting High Availability: The SDN architecture is expected to offer a higher level of reliability and availability of services. This must be maintained by incorporating appropriate 1:1 or 1:N level of redundancy in the critical elements — be it in the control, data, or management plane	
Req-Gen-05	Unified Management and Monitoring: During initial deployment of SDN components, many adjunct configuration, bootstrapping, and in-/out-band control of network/service functions may be needed in order to address the migration, repair and maintenance of network monitoring and operations management	

4.2 SDN Migration Solution Requirements

Table-4 lists SDN migration requirements from a Solution perspective.

Table-4: General SDN Migration Solution Requirements

Requirement Number	Requirement Description	Comments
Req-Soln-01	SDN domain solution prototyping (e.g., proof-of-concept) requirements	
Req-Soln-02	SDN domain solution roll-out (test, verify, commit, roll-/fall-back) requirements	
Req-Soln-03	SDN domain solution scale in/out requirements	
Req-Soln-04	Requirements to support SDN domain solution, service and device/function health monitoring	
Req-Soln-05	Requirements to support SDN domain solution stability and its assessment	
Req-Soln-06	Requirements to support SDN domain solution reliability/ survivability and its assessment	
Req-Soln-07	Requirements to support SDN domain solution's seamless interworking with legacy for delivering uniform quality of user experience	

4.3 4.3 SDN Migration Device and Function Requirements

4.3.1 4.3.1 Common Set of Requirements

The common set of requirements for SDN migration includes the requirements for elements (devices and functions) in each of the horizontal (as shown in Fig.1) and vertical (management

and orchestration, as shown in Fig.1b) planes of the architecture. These requirements are as discussed in **Table-5** below.

Table-5: SDN Migration Device and Function Common Requirements

Requirement Number	Requirement Description	Comments
Req-Cmn-01	SDN Forwarding and switching plane device and function requirements including South-bound interface (SBI) requirements	
Req-Cmn-02	SDN Controller functions and server (host) requirements including North-, South-, East- and West-bound interfaces requirements. East- and West-bound interfaces support interaction with management domain (see Fig.1b) and user domains, as depicted in Fig.1 (page 40) of the ZTE Communications Magazine (http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2013/4/)	
Req-Cmn-03	SDN application and service plane device and function requirements including South-bound interface (SBI) requirements	
Req-Cmn-04	SDN device/function configuration control and management interface and host requirements	
Req-Cmn-05	SDN device/function interworking (with legacy network device/function) interface and capability requirements	
Req-Cmn-06	Trusted Boot and Attestation requirements	
Req-Cmn-07	Trust boundary establishment requirements	
Req-Cmn-08	Authentication and Authorization requirements	

Req-Cmn-09	Encryption requirements	
Req-Cmn-10	Audits and verification requirements	
Req-Cmn-11	General security requirements; the principles and practices for securing SDN can be found in the ONF Security WG documents (https://www.opennetworking.org/technical-communities/areas/services)	
Req-Cmn-12	Network (layer-2 and layer-3) overlay, underlay and tunneling (over and across IP, MPLS, GMPLS, Optical, Ethernet) management requirements	
Req-Cmn-13	SDN domain address management requirements	
Req-Cmn-14	SDN domain resources management and migration requirements	
Req-Cmn-15	Requirements to support SDN domain interworking with legacy control, forwarding and management devices and functions	
Req-Cmn-16	Requirements to support SDN domain redundancy and fall-back (to legacy and/or other SDN domain)	

4.3.2 Industry/Service Specific Requirements

The service specific set of requirements for SDN migration includes the requirements for supporting networking and value-added services specific to certain sectors.

These sectors include SDN based access/edge, aggregation and transport (one and multi-admin domains) networking, data center networking and enterprise/campus networking.

The requirements are as discussed in **Table-6** below.

Table-6: Service Specific SDN Migration Requirements

Requirement Number	Requirement Description	Comments
Req-Srvc-01	SDN based Edge/Access and Aggregation Networking: a. Edge and aggregation switch for quality of service (QoS) aware routing b. VLAN support with bandwidth protection capability c. QnQ support d. Group Table support e. MPLS support f. IPv6 support g. Auxiliary control channel support h. Multiple Table and Tenancy support i. Line rate switching support j. Latency for new rules setup k. Max packet punt rate support l. Version(s) of OpenFlow specs. supported m. OpenSource controller and switch support (with test results)	
Req-Srvc-02	SDN based Transport (One Admin) Networking: a. Network function instantiation, management, and control for wide area bandwidth and traffic management b. Multilevel provisioning by transport-type, e.g., IP, MPLS, MPLS-TP, GMPLS, wavelength, etc.	

Req-Srvc-03	a. SDN based Transport (Multi-Admin) Networking: b. Network function instantiation, management, control, and orchestration for wide area bandwidth and traffic management over multiple admin domains c. Multilevel provisioning of bandwidth by transport type (IP, MPLS, MPLS-TP, GMPLS, optical) over multiple admin domains d. Provisioning and management of bandwidth and value-added advanced services (NAT, PAT, firewall, service chain, etc.) for retailing and wholesaling e. Operation and service management in federated or hierarchical modes over multiple admin domains	
Req-Srvc-04	Intra-Data-Center-SDN: a. Automated provisioning and mobility management of virtual machines for seamless service management b. Seamless integration with virtual storage for on-demand file capacity management c. Client-specific security and tunnel management d. Service-specific security and tunnel management e. On-demand service acceleration management f. Virtual and physical domain compute, storage and networking resources lifecycle management g. Generic resources sanity and regulatory management	
Req-Srvc-05	SDN for Data-Center-Interconnection: a. Automated provisioning and control of bandwidth for seamless traffic management services b. Seamless support of interconnection among multi-domain (private, public, hybrid) virtualized resources c. Multi-domain tunneling and centralized control	

Req-Srvc-06	SDN based Enterprise/Campus: a. Automated provisioning and control of convergence services b. Policy based design and management (enforcement) of converged services c. Automated provisioning and management of network (bandwidth, quality-of-service, security, etc.) and service (DNS, DHCP, etc.) resources d. User and application/service profile based resource management	

5 Conclusions

The document presents a high-level RFI template for migration to SDN-based network architecture.

It is expected to be equally helpful to both network and service providers who are considering migration to SDN architecture using physical or virtual or hybrid (physical and virtual) network elements /functions. In many ways, an RFI process can be a signal to a group of vendors that the acquisition and deployment for new technologies like SDN will follow a proven and deliberative path. The solicitor of information will not be swayed by mass advertising or the claims of one particular sales representative, but rather will be guided by a careful investigation of the comprehensive data across an entire spectrum of providers. Rather than signal that the inquirer is not educated about the technology, are well-crafted RFI signals that this particular customer will not be swayed by either the first or last marketing campaign (s)he has heard. It further signals that this organization is going to move with measure steps on a path of innovation, and wants assurance by potential providers—in writing—that vendor claims can be substantiated. This process will signal to all parties—internal and external to the deploying organization—that those who direct the RFI are competent, deliberate, and careful with the resources of the company, and are on their way toward innovation that is borne of good decision-making.

In the case of a nascent technology like SDN, the hyperbole and claims made in the initial phases of product development and release can be difficult to separate from the realities about what improvements can be reasonably expected from SDN. A well-crafted RFI can help separate the wheat from the chaff and give greater confidence to those making their first steps in an SDN deployment.

6 Acknowledgements

We gratefully acknowledge the contributions of reviewers of earlier versions of this document.

7 Revision History

Date	Rev	Description	Editor
08April-2015	0.1a	Initial release to the Migration Working Group	B. Khasnabish
14April-2015	0.1b	Added structure, split out Operator/Vendor requirements; common/service specific requirements. Added requirements	E. Salahuddin
06May-2015	0.1c	Added architecture diagrams and some more requirements	E. Salahauddin
13-May-2015	0.1d	Updates and revision	B. Khasnabish
19-May-2015	0.1e	Added template, architectures, and tables for different sections	B. Khasnabish
20-May-2015	0.1f	Updates and revision	E. Salahauddin
21-May-2015	0.1g	Edits, updates and revision	B. Khasnabish
02-June-2015	0.1h	Edits and updates	E. Salahuddin
03-June-2015	0.1i	Minor updates after review with the team	E. Salahuddin
03-June-2015	0.1j	Added contents to Appendix-A	G. Reffet and N. Kumar
13-July-2015	0.1k	Edits and updates	E. Ganon
15-July-2015	0.1l	Edits, updates and revision	B. Khasnabish
15-July-2015	0.1m	Updates during WG review	B. Khasnabish
05-Aug-2015	0.1n	Updates to address the comments from Dacheng	B. Khasnabish
12-Aug-2015	0.1o	Updates based on Beth’s comments	B. Khasnabish
15-Oct2015	0.1p	Edits and updates	B. Khasnabish

8 References

1. ONF Migration Use Cases and Methods
   https://www.opennetworking.org/images/stories/downloads/sdn-resources/use-cases/Migration-WG-Use-Cases.pdf
2. Software-Defined Networking (SDN) Definition
   https://www.opennetworking.org/sdn-resources/sdn-definition
3. SDN Architecture Overview v1.1:
   https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN-ARCH-Overview-1.1-11112014.02.pdf

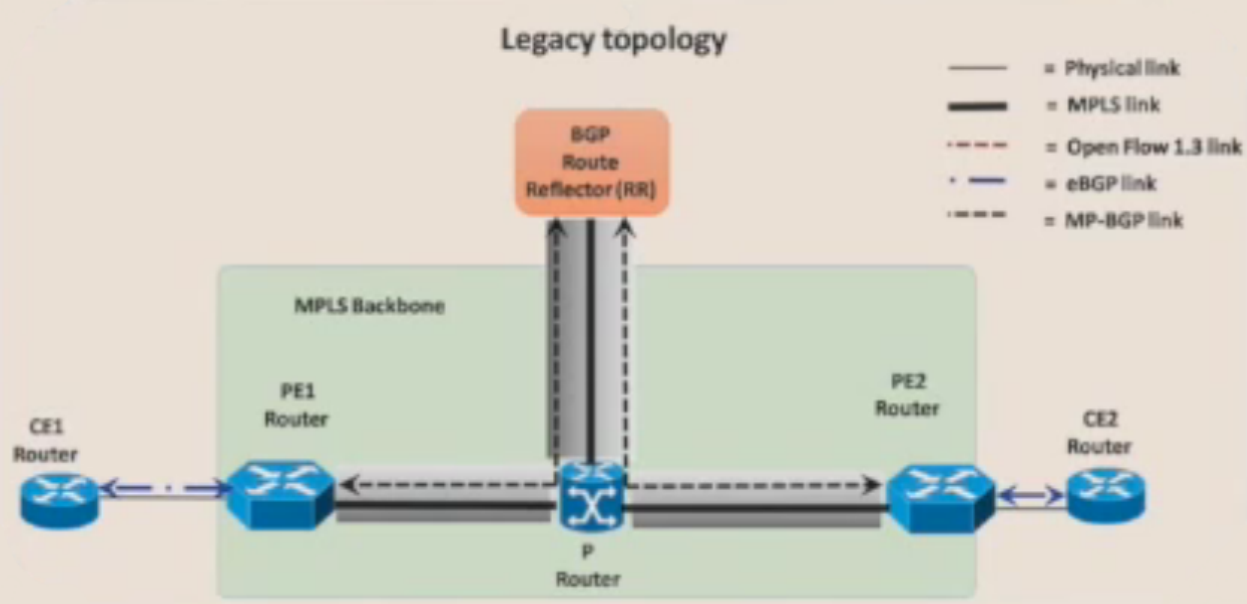
9 Appendix A: SDN Migration Prototyping Results

Based on a deployment use case provided by NTT, the ONF Migration Working Group designed several methods to migrate from a legacy BGP based network edge to OpenFlow-based "SDN-ized" network edge with seamless interworking.

The different methods are described in the following documents: SDN Migration Prototype & Demo Proposals (onf2014.308.12).

A first prototype was created to demonstrate that it is possible to migrate easily to an SDNized network.

The initial network is composed of two CE (CE1 – CE2) at each extremity of the network, two PE (PE1 – PE2) which are connected by a P Router and a Route Reflector, as shown below.

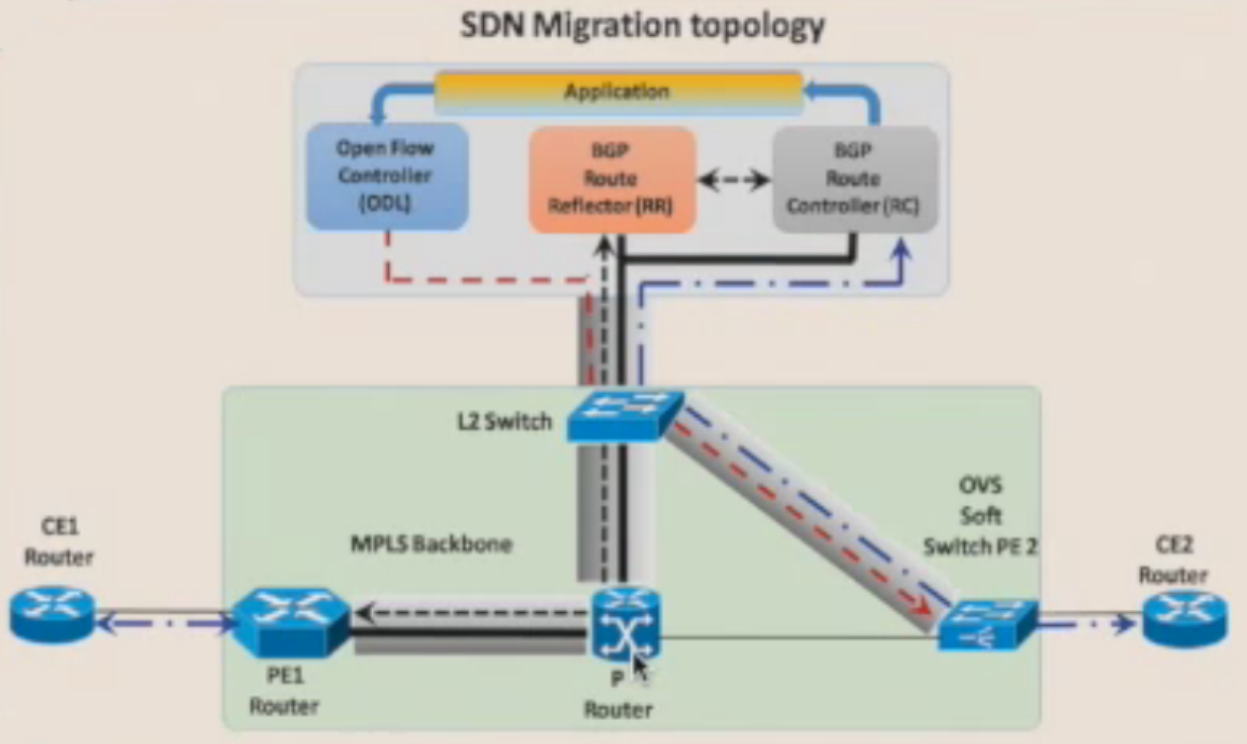


In term of connection, there is an eBGP link between the CE and the PE (CE1 to PE1 and CE2 to PE2). The PE1 is connected to the Route Reflector using a MP-BGP link and it is a similar connection to connect PE2.

In this legacy topology, the control plane and data plane are duplicated in all network elements. That means if CE2 pings CE1, the data goes to CE2 to PE2, forwarded to P Router, forwarded to PE1, forwarded to CE1.

The goal of this prototype is to migrate to a hybrid network using SDN.

According to the schema below, the PE2 router will be replaced by an OpenVSwitch, and an SDN controller OpenDaylight and a Route Controller will be added on this SDN migration topology.



Thanks to this topology, the data plane is on the OpenVSwitch but the control plane is now on the SDN controller. With the same example, when CE2 pings CE1, the packet goes to CE2 to the OVS PE2 that has been programmed by OpenDayLight the packet is automatically forwarded to the P router, forwarded to PE1, forwarded to CE1. The data plane is similar to the legacy network, but the control plane of one element is now centralized in the SDN controller.

Based on the SDN topology, the CE2 device's interface is not yet configured, the CE1 is not able to ping CE2:

```
root@pedgequaga-vM:/usr/local/quagga# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 eth1
5.5.5.5         192.168.26.2    255.255.255.255 UGH   0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
192.168.2.0     0.0.0.0         255.255.255.0   U     1      0        0 eth1
192.168.26.0    0.0.0.0         255.255.255.0   U     1      0        0 eth0
root@pedgequaga-vM:/usr/local/quagga#
root@pedgequaga-vM:/usr/local/quagga#
root@pedgequaga-vM:/usr/local/quagga# ping 4.4.4.4 -I 6.6.6.6
PING 4.4.4.4 (4.4.4.4) from 6.6.6.6 : 56(84) bytes of data.
```

The network is now configured on CE2:

```
ce2(config-router)#network 4.4.4.4 mask 255.255.255.255
```

The application has now reflected that the network that has been added:

```
Fetching MPLS VPN labels from RC...
Adding POP flows to the ODL...
4.4.4.4=4007=
Fetching MPLS VPN labels from RC...
```

On the OpenVSwitch a new table has been added

```
 cookie=0x0, duration=20.252s, table=0, n_packets=20, n_bytes=2040, idle_age=0, priority=1110,mpls,i
n_port=3,mpls_label=4007,mpls_bos=1 actions=pop_mpls:0x0800
```

CE1 is now able to ping CE2

```
64 bytes from 4.4.4.4: icmp_req=22 ttl=253 time=2.51 ms
64 bytes from 4.4.4.4: icmp_req=23 ttl=253 time=2.50 ms
64 bytes from 4.4.4.4: icmp_req=24 ttl=253 time=2.61 ms
64 bytes from 4.4.4.4: icmp_req=25 ttl=253 time=2.54 ms
64 bytes from 4.4.4.4: icmp_req=26 ttl=253 time=2.52 ms
64 bytes from 4.4.4.4: icmp_req=27 ttl=253 time=2.38 ms
64 bytes from 4.4.4.4: icmp_req=28 ttl=253 time=2.52 ms
64 bytes from 4.4.4.4: icmp_req=29 ttl=253 time=2.43 ms
64 bytes from 4.4.4.4: icmp_req=30 ttl=253 time=2.69 ms
64 bytes from 4.4.4.4: icmp_req=31 ttl=253 time=2.54 ms
```

On the same way, if the interface on CE2 is removed

```
ce2(config-router)#no network 4.4.4.4 mask 255.255.255.255
ce2(config-router)#
```

CE1 is no longer able to ping

```
64 bytes from 4.4.4.4: icmp_req=47 ttl=253 time=2.48 ms
64 bytes from 4.4.4.4: icmp_req=48 ttl=253 time=2.51 ms
```

The application detects this change

```
Fetching MPLS VPN labels from RC...
Deleting POP flows to the ODL...
4007
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5826    0  5826    0     0   198k      0 --:--:-- --:--:-- --:--:--  210k
Fetching MPLS VPN labels from RC...
```

And the OpenVSwitch is reconfigured, the flow is removed

```
cnlabs@cnlabs:~$ sudo ovs-ofctl dump-flows br1 | grep 4007
cnlabs@cnlabs:~$
```

10 Contributors

Bhumip Khasnabish (ZTE) — Editor

Dacheng Zhang (Alibaba)

Edna Ganon (MRV)

Esa Salahuddin (Cisco)

Guillaume Reffet (Ubiqube)

Hakki Cankaya(Fujitsu)

Marty Ma (Tencent)

Naresh Kumar (Criterion)