FCC TAC Cybersecurity Working Group
Securing SDN NFV Sub-Working Group

White Paper: Considerations for Securing SDN / NFV

January 2016

Final

Executive Summary

FCC Technological Advisory Council Cybersecurity Work Group was requested to examine the special Cybersecurity challenges posed by emerging SDN (Software Defined Network) technology. This white paper (WP) describes the SDN TAC Sub Working Group analysis. The SDN TAC SWG (Sub Working Group) considered the following FCC questions in analyzing SDN.

a. What are the key security challenges that SDN architectures present? And how is the telecom industry addressing them?
b. What measures could be employed to make networks deploying SDN applications resilient and secure?
c. What is the trust model that should be applied between devices and controllers, and between controllers?
d. What, if any, high-assurance approaches may apply to SDN?
e. What specific lessons can we extract from the long running efforts to secure existing control plane protocols -- such as BGP and DNS – to benefit SDN-based networks?
f. What are the pros and cons of embedding security within the network, as opposed to embedding it in servers, storage and other computing devices?
g. What are the strengths and weaknesses of Software Defined Security (SDSEC)?
h. What role could the FCC play in facilitating positive changes in the security, privacy and resiliency of SDN?

Methodology

SDN is an evolving technology and several innovations are occurring at a fast clip. Technology choices for SDN implementations are dependent on usage scenarios. The subgroup's experts based their recommendations on analysis of information from public information sources as well as industry experts. Industry experts included SDN Vendors, SDOs (Standards Development Organizations), Service Providers and Communities from Ericsson, Alcatel-Lucent, OPNFV/Nokia, HP, IBM, Cisco, OpenDayLight, Juniper, Brocade and Fortinet.

Findings

The primary concern relating SDN and cybersecurity is a function of the separation of the control and data planes in the network and the correspondingly increased role that malleable software plays in defining the operation of the data plane and its functions (Network Function Virtualization or NFV). Various segments of the industry are cognizant of the increased threats and challenges posed by these new architectures and opportunities to leverage these

technologies to enhance security solutions. Communities are starting to work on security issues. CSA's (Cloud Security Alliance) recent position paper outlines challenges and opportunities, and security frameworks. Communities like ONOS (Open Networking Operating Systems) and ODL Open DayLight), with the participation of industry players, are addressing these challenges. Approaches such as TPM (Trusted Platform Module), vTPM (virtual TPM), bidirectional authentication between applications, controllers and network elements, repeated measurement of attestation and multiple domains trust model are being developed to address existing gaps. Industry practitioners indicate that standards are needed eventually to assure interoperability but rapid progress would be more likely achieved in open source communities on solutions for securing SDN NFV, and that such communities and SDOs have to work together.

1. Purpose

This document captures the state of the industry in handling security challenges posed by the SDN and NFV architectures and how it leverages the opportunities.

2. Scope

The WP is intended to describe key security challenges that the evolving SDN / NFV architectures present, new mitigation opportunities enabled by them, and approaches to make networks deploying SDN applications resilient and secure. As part of this investigation, the WP explores areas such as possible applicability of high-assurance approaches and lessons learned from efforts to secure existing control planes. The WP captures how the telecom industry is addressing the above aspects of the new architectures. Actionable recommendations to the FCC will point out the possible role which it could play in facilitating positive changes in the security, privacy and resiliency of these new architectures.

3. Methodology

In addition to the input from member companies of the SWG (Sub Working Group), the SWG conducted research on these topics from industry sources - Vendors, SDOs (Standards Developing Organizations), Service Providers and Communities and consulted 12 SMEs (Subject Matter Experts) on SDN / NFV security from a cross- section of the industry to understand their perspectives and insights on securing SDN / NFV. These are listed in section 13. The WP also leverages the architecture work done by FGCT (Future Game Changing Technologies) Architecture group on SDN / NFV.

4. Architecture

4.1. SDN

The aim of SDN (Software Defined Networking) is to provide open interfaces that enable the development of software Applications that can control the connectivity provided by a set of network resources and the flow of network traffic through them, along with possible inspection and modification of traffic that may be performed in the network. Figure 4.1 presents a high level overview of SDN.

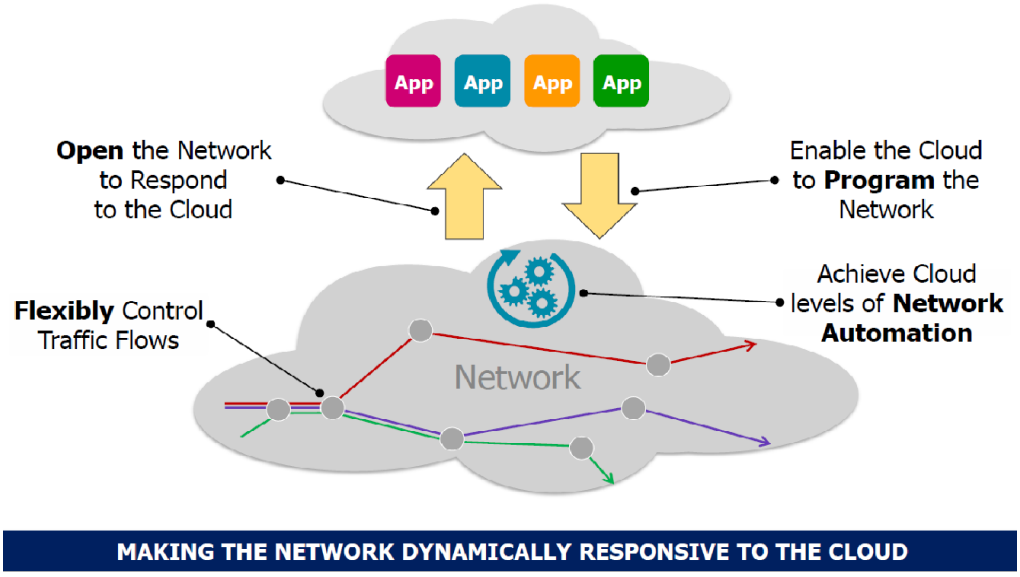


Figure 4.1: High Level Overview (source: Kevin Sparks, FGCT Architecture SWG)

A high level multi-domain SDN architecture is shown in Figure 4.2. It shows distinct application, controller and data planes, with controller plane interfaces (CPIs) designated as reference points between the SDN controller and the application plane (A-CPI) and between the SDN controller and the data plane (D-CPI). The architecture makes no statement about the physical realization of the components, such as protocols used for the A-CPI or D-CPI. Each trust domain is understood to have its own management functionality. Trust domains may logically extend into components of other trust domains, as exemplified by the green and red agents in the blue SDN controller *[Ref. a].*

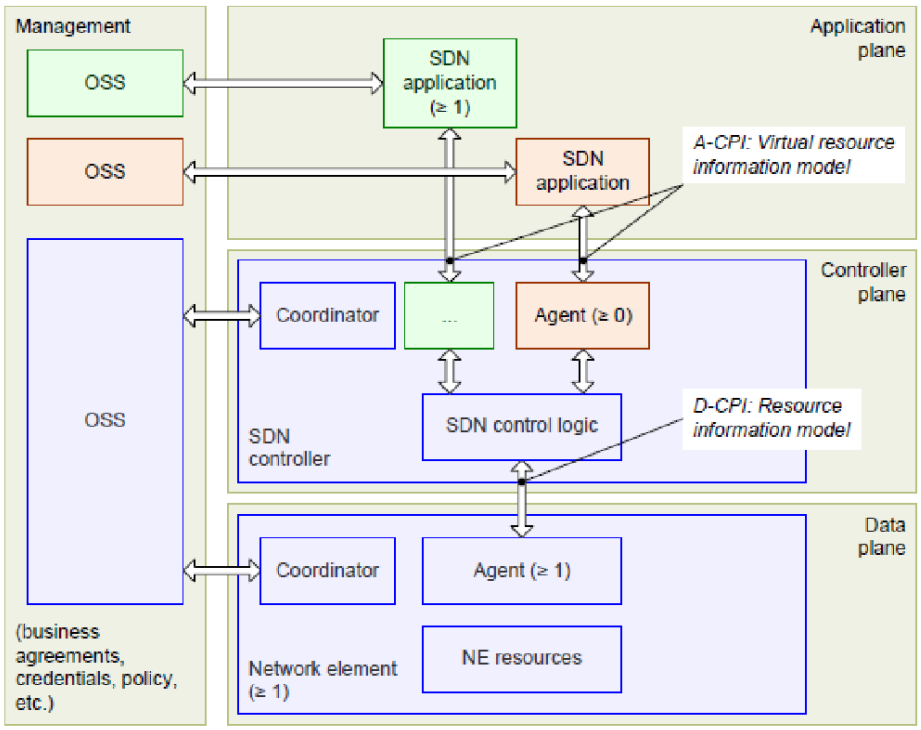


Figure 4.2: SDN Architecture (source: ONF)

4.1.1. SDN architectural principles:

Disaggregation or decoupling of control and data planes:
This principle calls for separable controller and data planes (Figure 4.3). However, it is understood that control must be exercised within data plane systems. The D-CPI between SDN controller and network element is defined in such a way that the SDN controller can delegate significant functionality to the NE (Network Element), while remaining aware of NE state

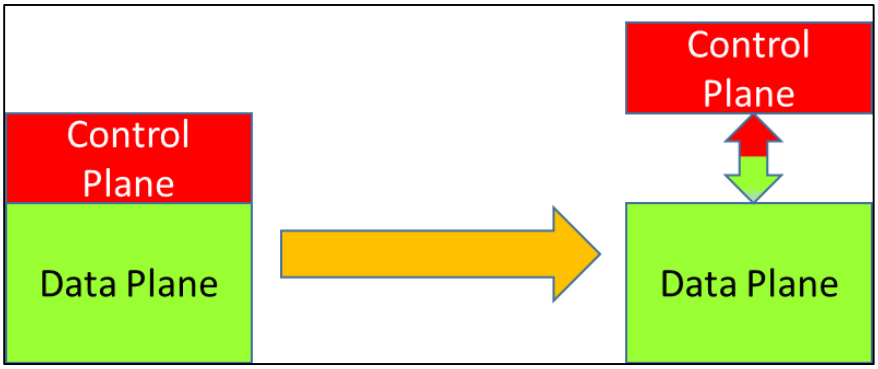


Figure 4.3: Disaggregation of Control and Data Planes

Logically centralized control (Figure 4.4):
In comparison to local control, a centralized controller has a broader perspective of the resources under its control, and can potentially make better decisions about how to deploy them. Scalability is improved both by decoupling and centralizing control, allowing for increasingly global but less detailed views of network resources

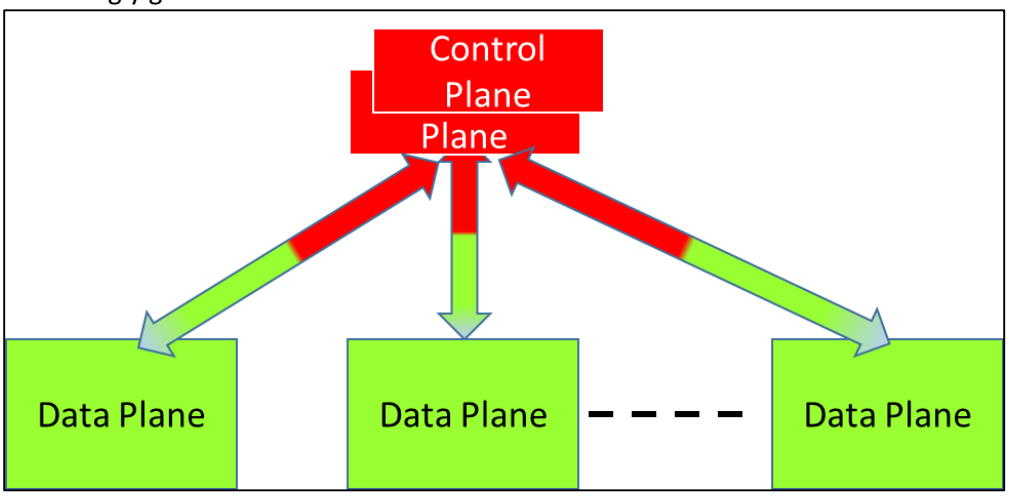


Figure 4.4: Logical Centralization of Control Plane

Abstraction:
Exposure of abstract network resources and state to external applications (Figure 4.5) is the principle of abstracting network resources and state to applications via the A-CPI allows for programmability of the network. With information about resources and their states,

applications are able to specify requirements and request changes to their network services via the SDN controller, and to programmatically react to network states

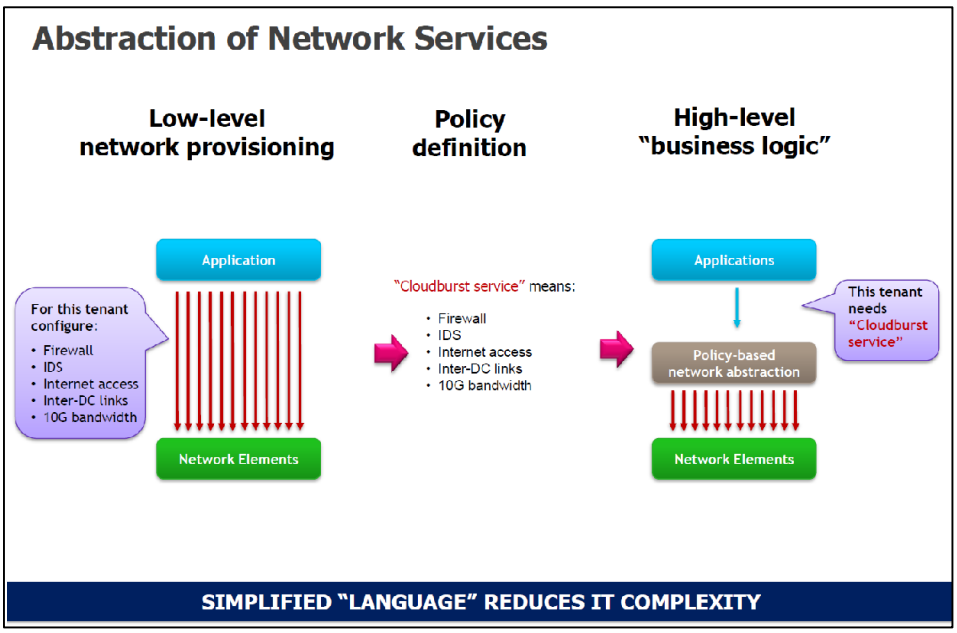


Figure 4.5: Abstraction (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

Programmability:

This attribute allows Applications to dynamically configure the network via the Control Plane (Figure 4.6). Applications express intent using the A-CPI and the Control Plane, in turn, uses the D-CPI interface to configure the network.

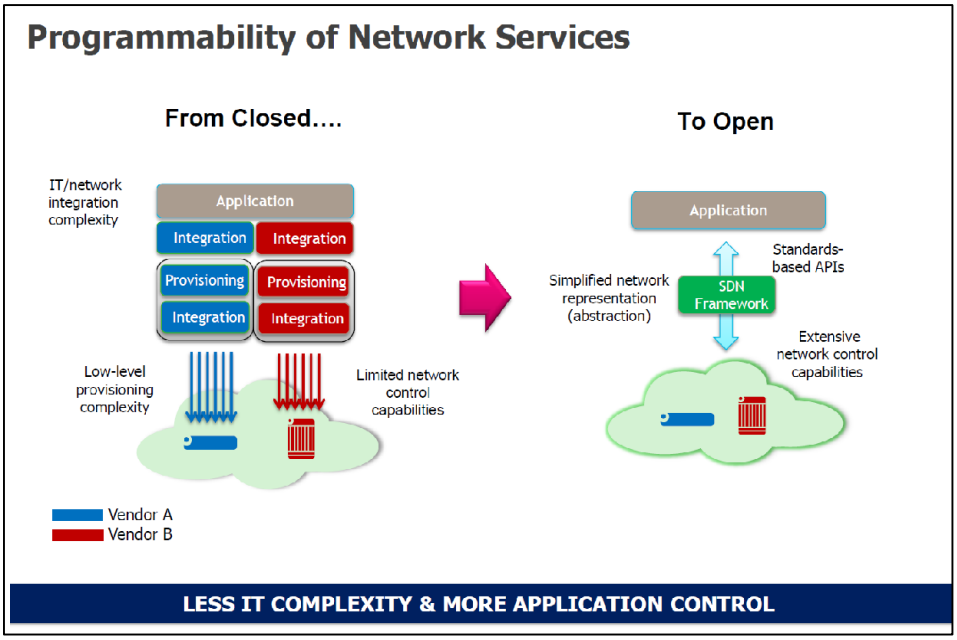


Figure 4.6: Programmability (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

Automation:

The preceding principles allow automation of provisioning and other processes with fewer manual touch points, less error prone and for scaling (Figure 4.7).

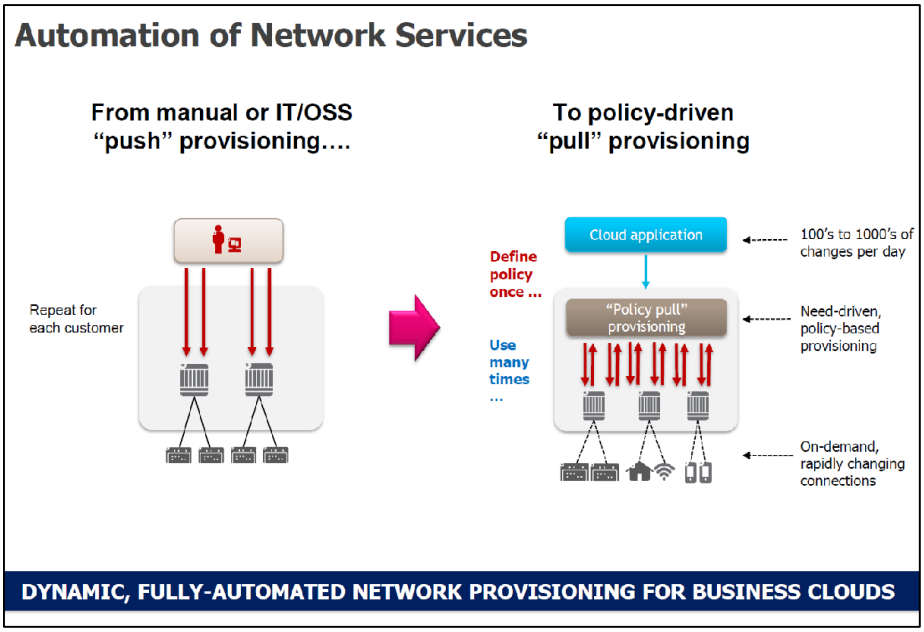


Figure 4.7: Automation (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

4.1.2. Flavors of SDN

SDN is an evolving technology and several innovations are occurring at a fast clip. SDN is used by the industry to refer to collection of architectures– reconfiguring the underlying network by directly manipulating the forwarding tables of the network to create specific paths using protocol like OpenFlow; implementing on top of an existing physical network; using rich set of APIs exposed by Network Elements to programmatically configure them, instead of using CLI manually. Industry uses SDN to describe different flavors of SDN. Here are some *[Ref. b]:*

With *Open SDN*, the fabric of the underlying network is reconfigured to provide the paths required to provide the inter-endpoint SDN connectivity (Figure 4.8). Forwarding tables of the network component are directly manipulated to create specific paths through the network using protocol like OpenFlow. The SDN controller is responsible for directly manipulating network element configuration to ensure that the requirements presented at the controller's northbound API are correctly orchestrated. The controller dictates exactly where in the network each traffic flow traverses, which is invaluable for troubleshooting, impact analysis, and security

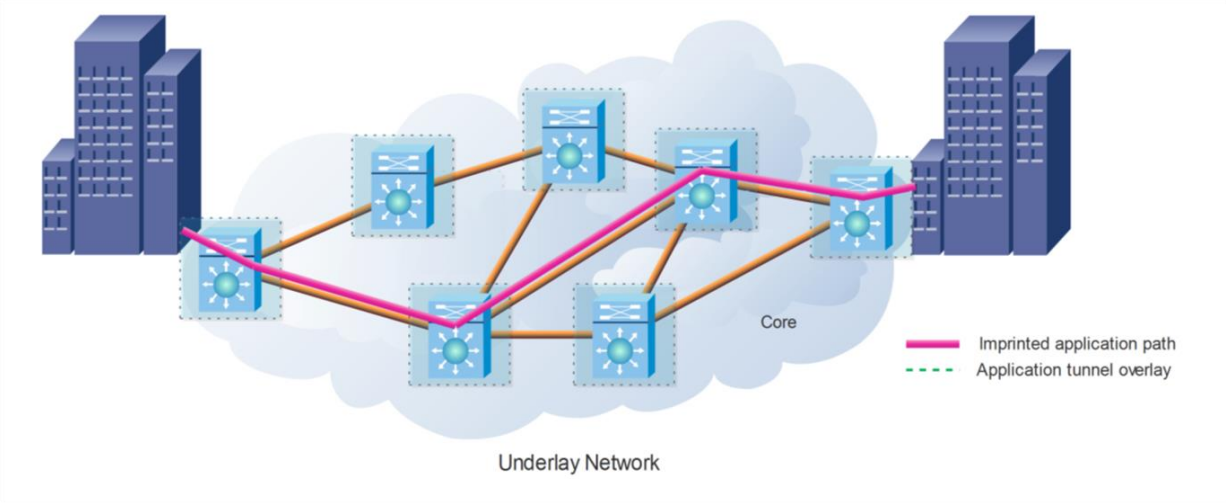


Figure 4.8: Open SDN (Source: Entuity White Paper)

With *Overlay SDN*, the SDN is implemented on top of an existing physical network (Figure 4.9). Overlay SDN use tunneling technologies such as VXLAN, and GRE and rely on the existing network fabric to transport the encapsulated packets to the relevant endpoints using existing routing and switching protocols

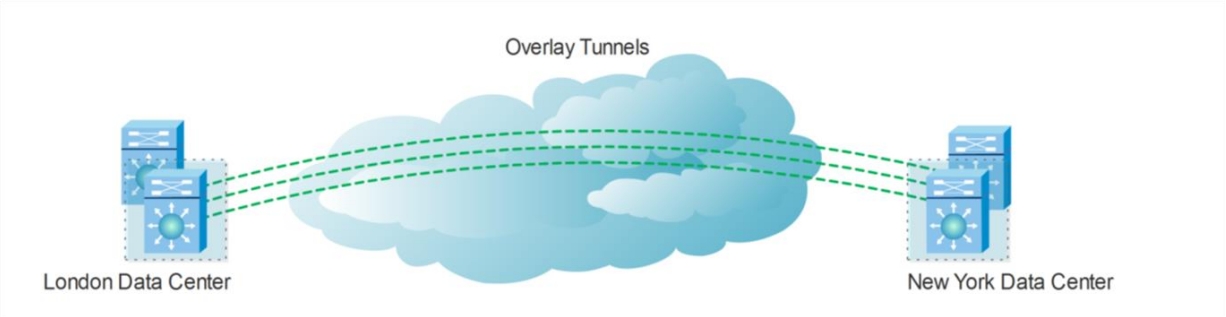


Figure 4.9: Overlay SDN (Source: Entuity White Paper)

The API flavor uses rich set of APIs exposed by Network Elements to programmatically configure them, instead of using CLI manually. This is not considered in this document.

Vendors are leading the development and SPs (Service Providers) are in various stages of POC (Proof Of Concept), Trials, and early limited roll-out. So far, SDN has been deployed only in

specific applications/ use cases such as data centers, WAN connecting data centers. All the more reason to build-in security now instead of bolting-on security into a massive installed base

4.2. NFV (Network Functions Virtualization)

While SDN provides for dynamic configuration of network connectivity by Applications, NFV focuses on network functions in software using pool of resources in a virtual environment, instead of the legacy physical appliances as shown in Figure 4.10. The difference between traditional method and NFV for providing network functions are:

- Decoupling software from hardware
- Flexible network deployment
- Dynamic operation

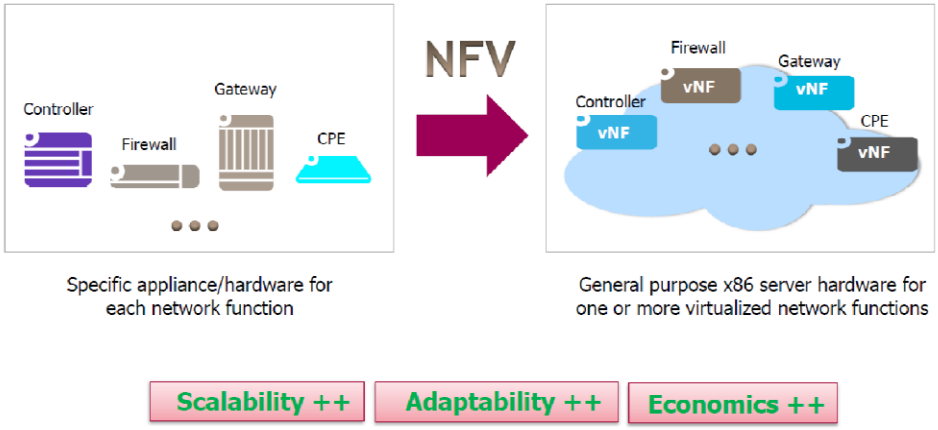


Figure 4.10: Network Functions – Legacy vs. NFV (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

SDN and NFV are complementary and often used together. Figures 4.11, 4.12 show the focus and complementariness of SDN and NFV.

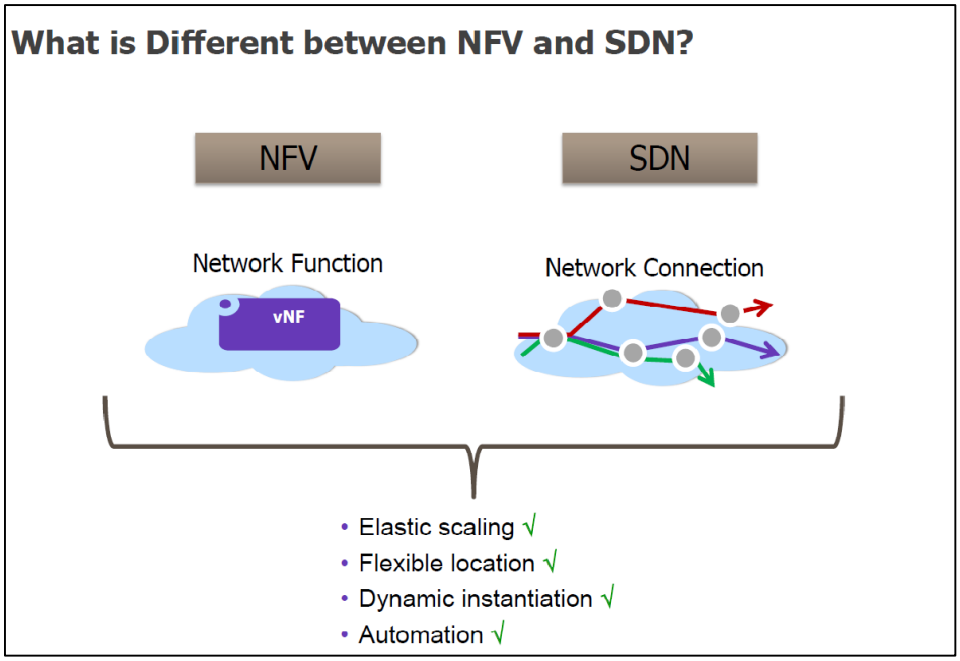


Figure 4.11: SDN and NFV Roles (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

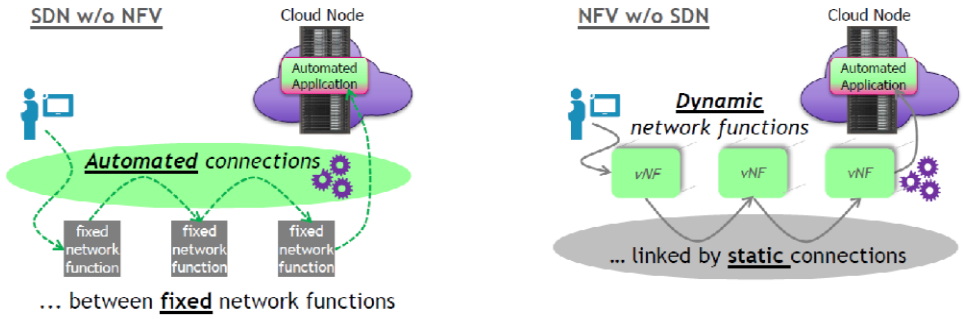


Figure 4.12: SDN and NFV Complementariness (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

4.2.1. NFV Objectives

- Improved capital efficiencies compared with dedicated hardware implementation

- Improved flexibility in assigning virtual network functions compared with dedicated hardware
- Rapid service innovation through software-based service deployments
- Improved operational efficiencies resulting from common automation and operational procedures
- Standardized and open interfaces between virtualized network functions and the infrastructure and associated management entities so that such decoupled elements can be provided by different vendors
- Reduced power usage by migrating workloads and powering down unused hardware

4.3. NFV Attributes (Figure 4.13)

- Network Functions (NF) as software-only entities
- NFs run over the NFV Infrastructure (NFVI)
- Virtualized Network Function (VNF), the software implementation of a network function capable of running over the NFVI
- NFVI includes the diversity of physical resources and how these can be virtualized. NFVI supports the execution of the VNFs
- NFV Management and Orchestration covers the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization, and the lifecycle management of VNFs

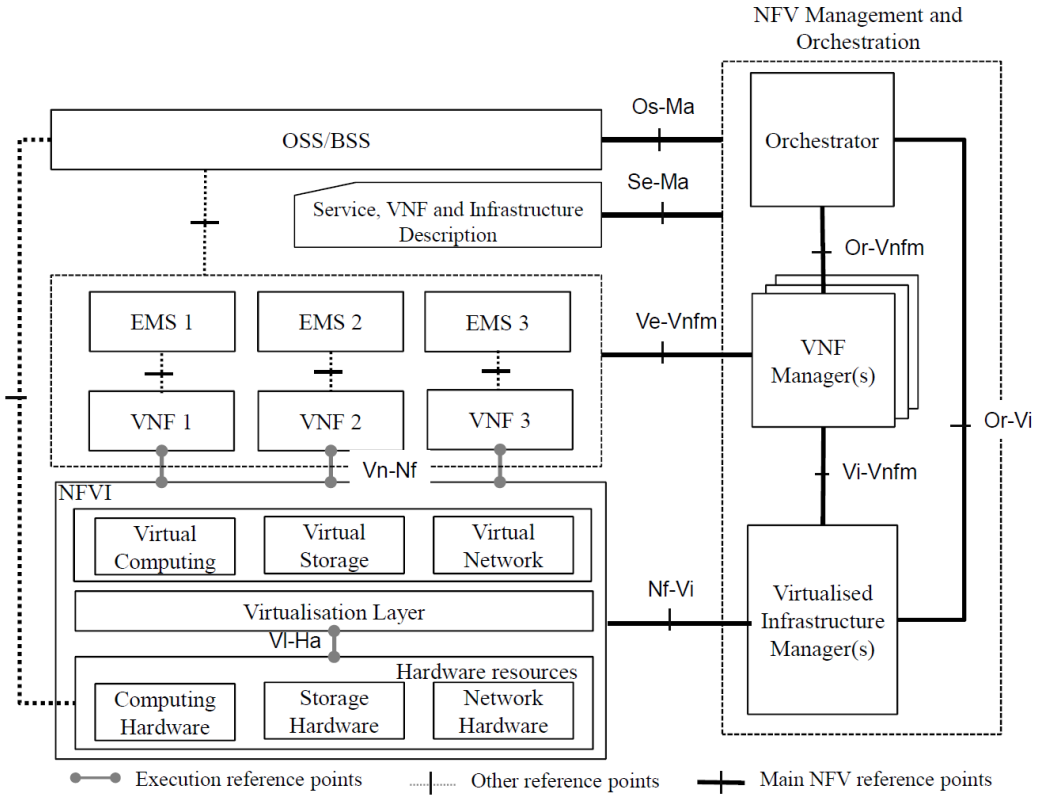


Figure 4.13: NFV Architecture (source: ETSI)

4.3.1. NFV Framework *[Ref. c]*

As shown in Figure 4.13 the NFV framework consists of the following major functional blocks:

- Virtualized Network Function (VNF) and Element Management System (EMS)
- NFV Infrastructure including hardware and virtualized resources and virtualization layer
- NFV Management and Orchestration including Virtualized Infrastructure Manager(s), Orchestrator, VNF Manager(s)
- Service, VNF and Infrastructure description
- OSS / BSS

As shown in Figures 4.14 and 4.15 SDN/NFV offers several persuasive benefits that make it attractive to Service Provider and enterprise networks alike by providing open interfaces that enable the development of software that can control the connectivity provided by a set of

network resources and the flow of network traffic though them, along with possible inspection and modification of traffic that may be performed in the network.

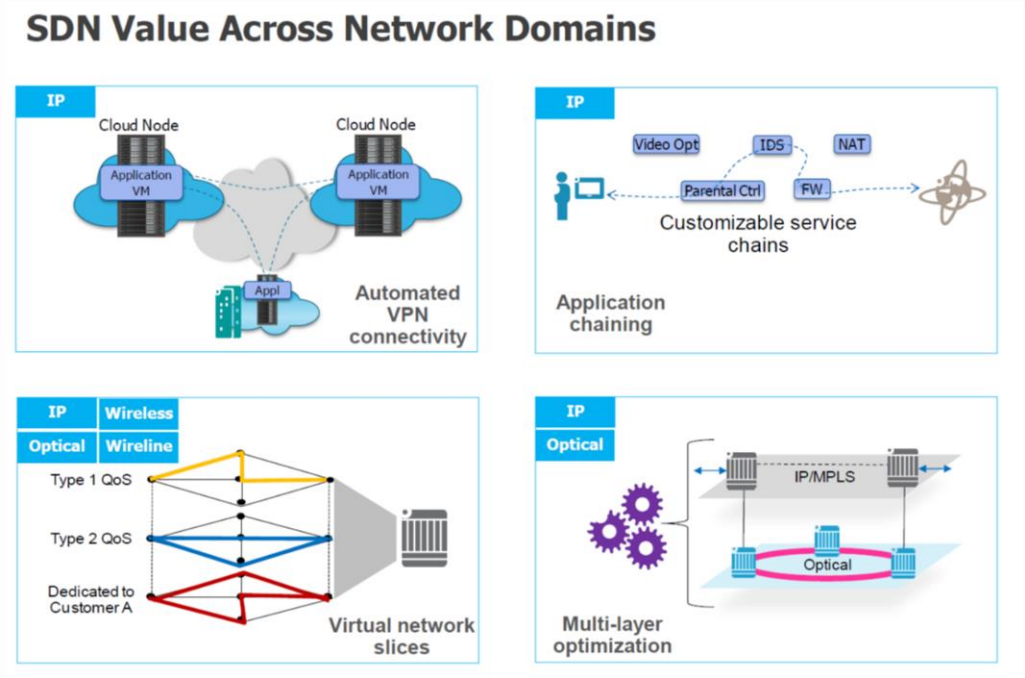


Figure 4.14: SDN Applicability (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

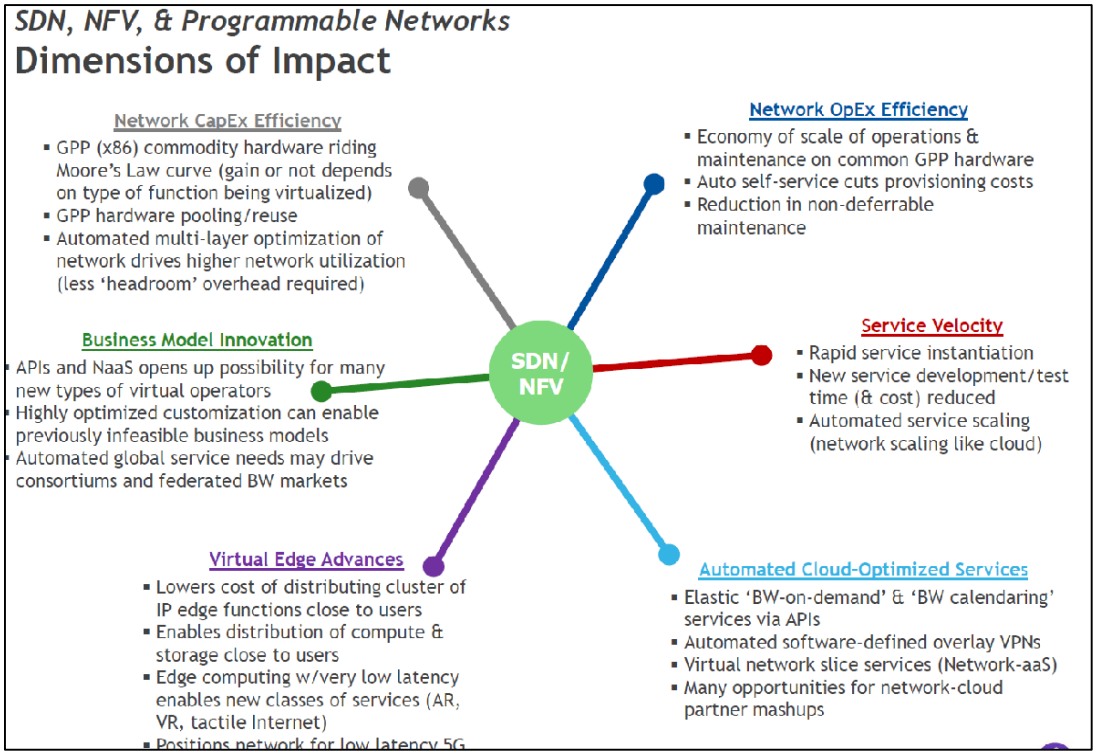


Figure 4.15: Transformational Impact of SDN and NFV (source: Kevin Sparks, FCC TAC FGCT Architecture SWG)

5. SDN Use Cases

5.1. Dominant Use Cases

SDN, Software Defined Networking is becoming a watered-down term and there is not a clear definition that is shared across the industry. Yet general principles and themes seem to be consistent when popular use cases are considered. The definition below, quoted from VMWorld Congress, is one that does a good job of capturing the essentials.

*"Software-defined networking (SDN) is an umbrella term encompassing several kinds of network technology aimed at **making the network as agile and flexible as the virtualized server** and storage infrastructure of the modern data center. The goal of SDN is to allow network engineers and administrators to respond quickly to changing business requirements. In a software-defined network, a network administrator can shape traffic from **a centralized control console** without having to touch individual switches, and can deliver services to wherever they are needed in the network, without regard to what specific devices a server or other device is connected to. The key technologies are functional separation, network virtualization and **automation through programmability**"*

This might be further summarized as "a network that is agile and flexible and automated through a centralized controller". Under this definition a number of use cases can be captured including perhaps the "original" use case of data center switching where an openflow control plane is used to program flow or state information into white box switches. That particular definition has now softened where the network element may still run a control plane and is programmed using a multitude of programmable interfaces e.g. NETCONF/YANG, JASON, REST etc. managed or orchestrated through a vendor specific or opensource controller.

To help focus the discussion in our white paper we thought it would be worthwhile to select and further define a few of the dominant SDN use cases in context and consideration of SDN security.

Discovering these dominant use cases in itself proved to be challenging as many POC's (Proof Of Concept) are still in stealth mode and public announcements lack the necessary detail. Based on general knowledge we picked up through our extensive interviews with industry vendors and service providers, our collective knowledge as a team, and the help of some industry publications like Heavy Reading survey below, provided as an example, we selected the following with no particular priority.

1. Intelligent VPN
2. Service Chaining - Combining with Cloud Services (VNF's)

3. Network Management and Traffic Control
4. Virtual CPE
5. Virtualization of CDNs (vCDN)

Figure 2.28: Additional Metro Aggregation SDN Use Case Responses

Combining with cloud services
Network management and traffic control
Improve quality and assurance service
Intelligent VPN
Dynamic quality of service for business customers
Residential automation and reduced cost of CPE
vCPE using tunneled connectivity across the L2/L3 networks
Multi-vendor networks reduce dependency and increase price pressures on vendors. Optimization of bandwidth
Resource management as a replacement for today's external offline databases – multi-layer link planning and control in one platform, which would lead to a simplification of today's NMS farms.
TCO economics are not viable enough yet. Wide adoption of white boxes is required to make it financially attractive

Source: Priming the Telco data center for NFV, A Heavy Reading Multi-client study, October 2014

5.1.1. Use Case #1 – Intelligent VPN

Traditional Virtual Private Networks (VPN) for enterprise Wide-Area Networks (WAN) require network appliances (e.g. routers, security appliances) to be deployed at the customer premises with some level of manual “fixed” configuration. As the VPN scales up so does the complexity of these configurations leading to operational challenges often requiring support engineers that are familiar with a particular customer network.

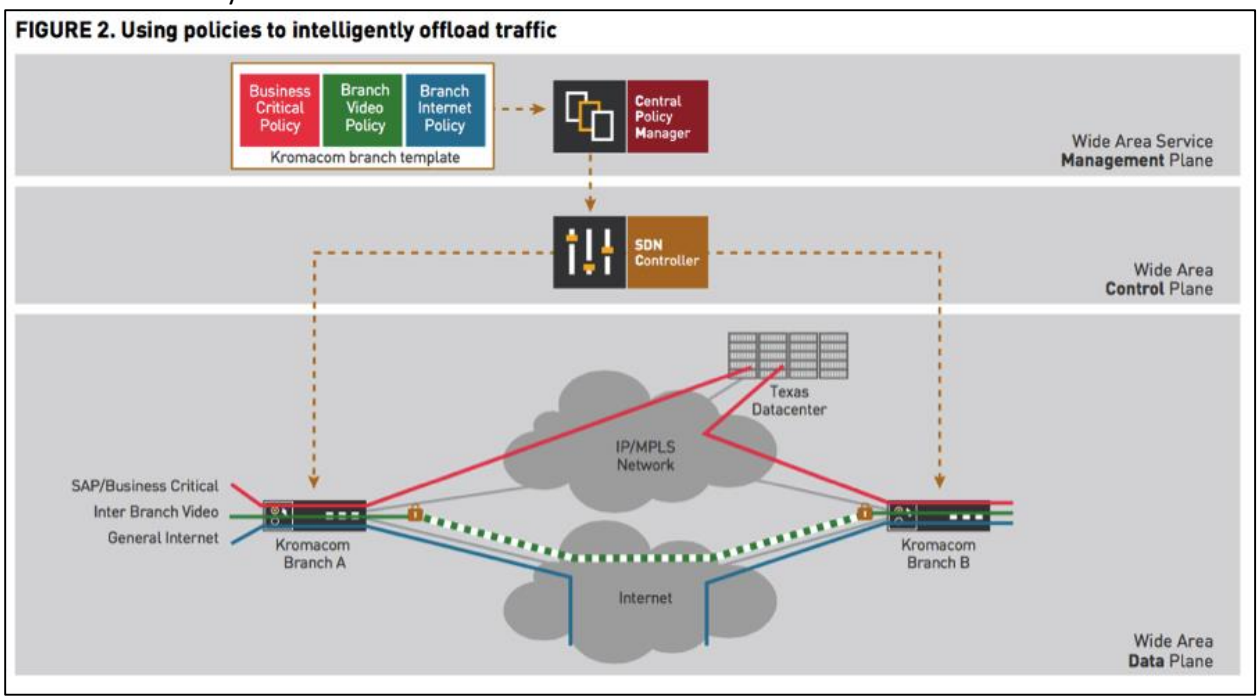
Using SDN technologies, a numbers of incumbent vendors and start up’s are developing “Intelligent VPN’s”. In this case the CPE’s are generally deployed on x86 platforms that are pre-loaded with the vendors SDN “client”, running as virtual function, before being shipped to the customer site. Much of the VPN design, cpe configuration, routing and security policies are handled via the SDN (also called SD-WAN) controller. CPE’s are initially boot strapped (basic IP connectivity) and after authentication with the controller receive a full configuration via some type of programmatic interface e.g. JSON, Openflow, Netconf etc. The orchestration of the end-to-end VPN is handled via the controller and as such, changes to the topology or

routing/security policy is fully automated and complexity abstracted from and engineer support perspective.

Intelligent VPN's have the potential to provide customer driven on-demand VPN creation and change via a service provider portal.

The diagram below, taken from a whitepaper on the ALU/Nuage website, shows the architecture of an Intelligent VPN with policy, VPN setup and traffic control all being orchestrated by the SDN controller.

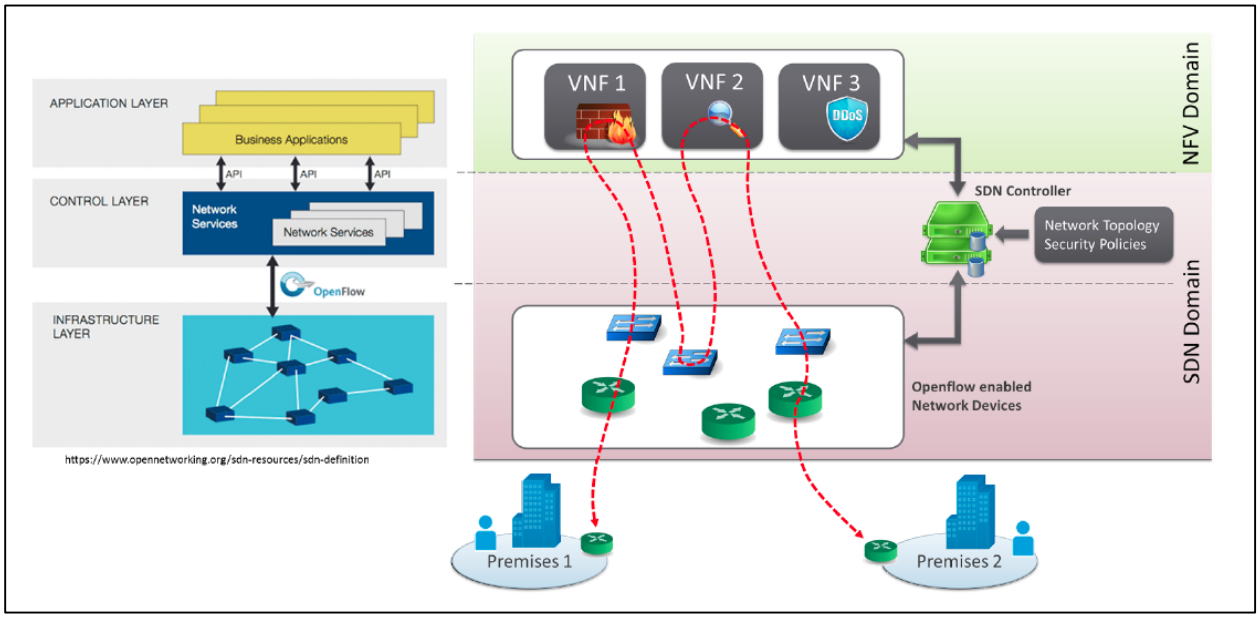
FIGURE 2. Using policies to intelligently offload traffic



5.1.2. Use Case #2 – Service Chaining - Combining with Cloud Services (VNF's)

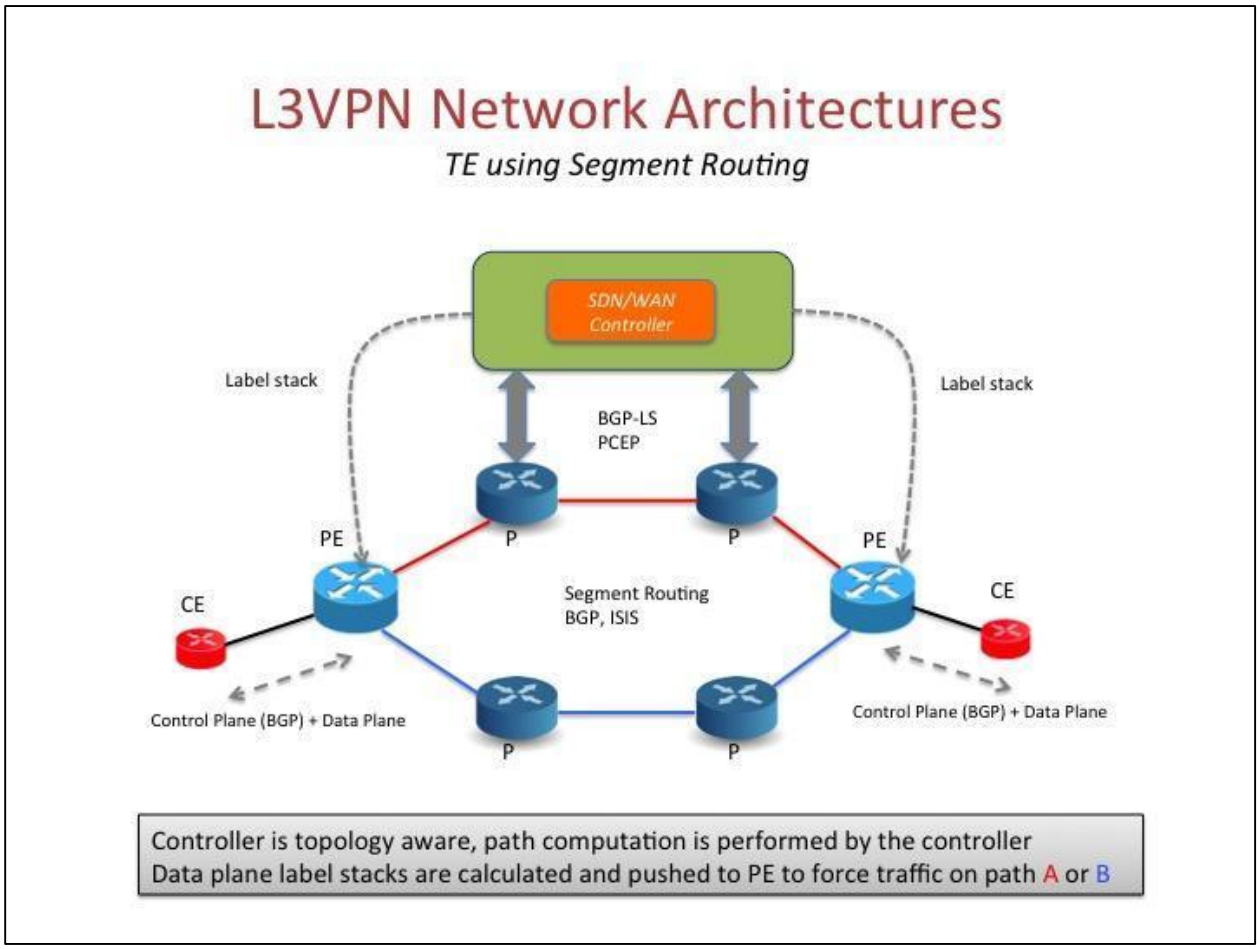
When traditional network functions are virtualized they may reside in various places in a service provider network such as central offices, head ends or data centers, depending on the particular service being offered or how it is architected. It becomes necessary then to provide a mechanism to steer or force traffic to those VNF's to carry out a desired treatment, enforce a policy etc. In the SDN world, this traffic steering is called Service Chaining.

The diagram below show an example of an enterprise site-to-site connectivity that is service chained through a number of virtual functions in the data center, all orchestrated through the SDN Controller.



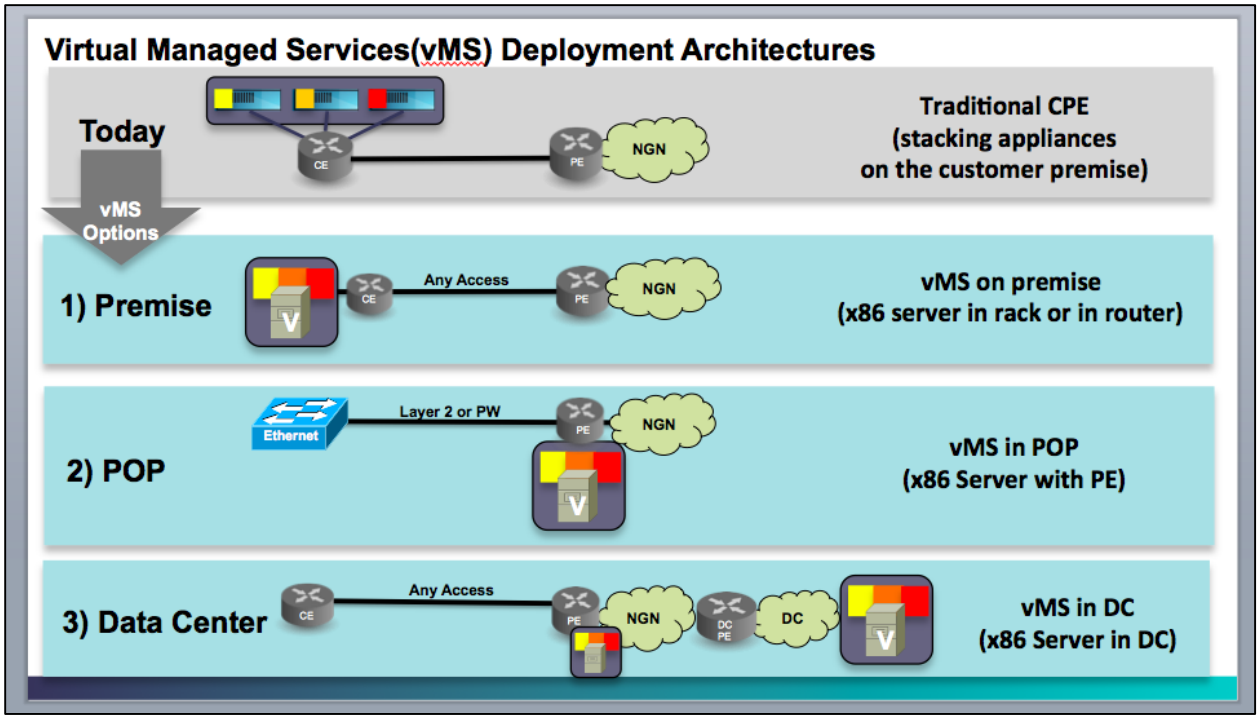
5.1.3. Use Case #3 – Network Management and Traffic Control

Service Providers are considering using SDN as an alternative mechanism for traffic engineering. A traditional traffic engineering network, where defined paths are created through the network that are purposely different from the "default" path calculated by routing protocols, BGP, ISIS etc., requires the network elements to run a TE control plane for this specific purpose, adding to the complexity of the network design as well as the feature and operational support of the network platform itself. With SDN, the controller is able to calculate and create a topology view of the network using protocols like PCEP and BGP-LS. Knowing the complete network topology, the SDN controller is able to program the necessary "state" into the packets at the edge to steer or traffic engineer the flow along the desired path.


L3VPN Network Architectures
TE using Segment Routing
SDN/WAN Controller
Label stack
Label stack
BGP-LS
PCEP
PE
P
P
PE
CE
Segment Routing
BGP, ISIS
CE
Control Plane (BGP) + Data Plane
Control Plane (BGP) + Data Plane
P
P
Controller is topology aware, path computation is performed by the controller
Data plane label stacks are calculated and pushed to PE to force traffic on path A or B

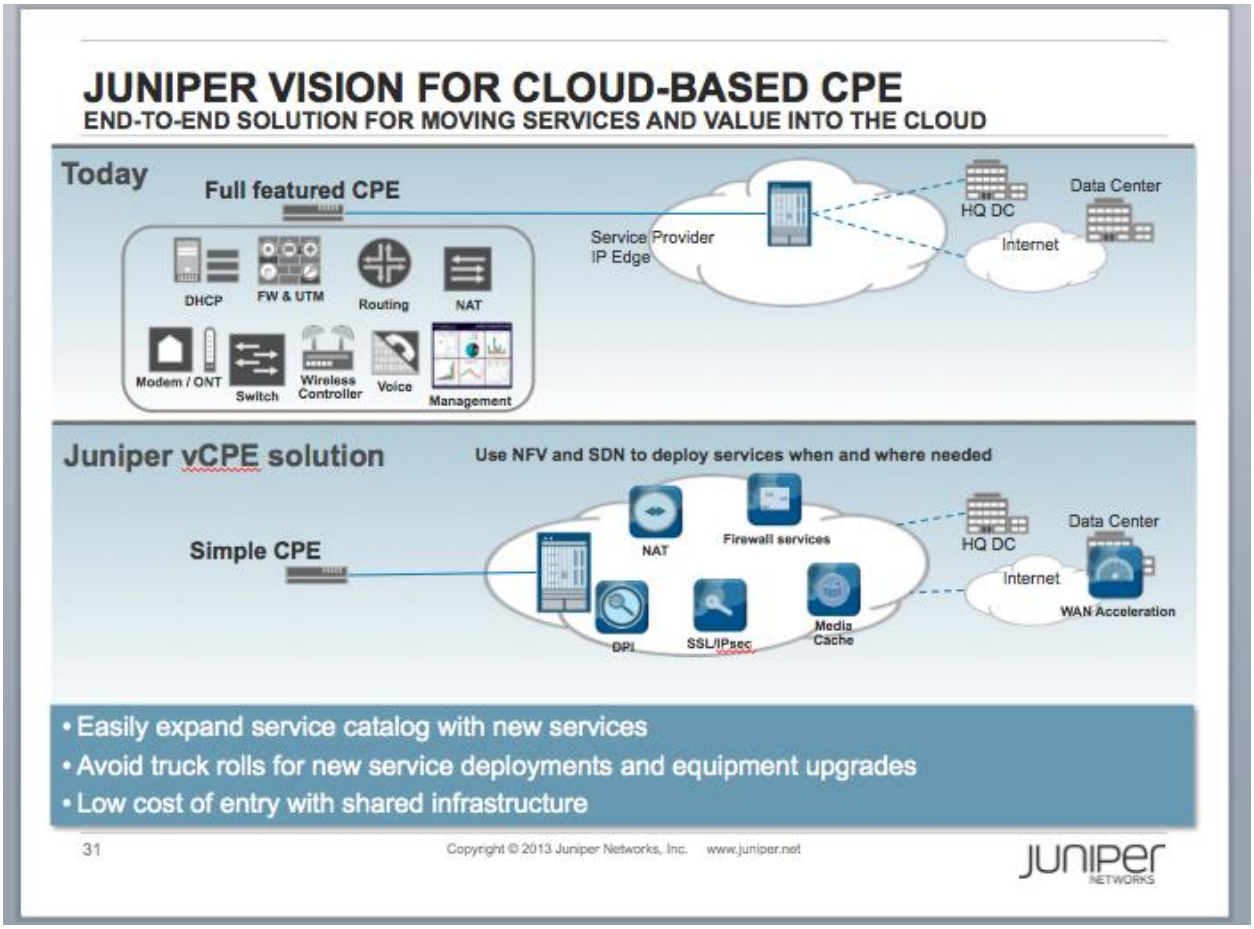
5.1.4. Use Case #4 – Virtual CPE (vCPE)

In this use case, network functions that traditionally reside on a purpose built hardware appliance(s) at the customer premise, as part of a VPN and Managed Service offering, are virtualized and run on a common x86 compute platform (replacing the purpose built appliance). This opens up the option to run the “network function” anywhere x86 compute is available in the Service Provider's network. The slide below, pulled from a recent Cisco presentation entitled “NFV, vCPE and Virtualized Managed Services” lays out a number of common architectures for vCPE.



From top to bottom, the diagram compares a traditional CPE architecture to a VNF running on x86 at the customer premise, L2 pass through at the customer premise to a VNF in the local POP (Point of Presence) and lastly a VPN connecting customer premise to a VNF in a local or regional data center. Chosen architectures would typically be balanced based on service level, performance requirements and cost.

Similarly, a Juniper Networks depiction of vCPE show how the full featured traditional CPE evolves to vCPE using VNF's in the cloud.



5.1.5. Use Case #5 – Virtualization of CDNs (vCDN)

The following is taken directly from ETSI NFV documentation describing in detail the CDN (Content Delivery Network) use case.

Motivation

Delivery of content, especially of video, is one of the major challenges of all operator networks due to massive growing amount of traffic to be delivered to end customers of the network. The growth of video traffic is driven by the shift from broadcast to unicast delivery via IP, by the variety of devices used for video consumption and by increasing quality of video delivered via IP networks in resolution and frame rate.

Complementary to the growth of today's Video Traffic, the requirements on quality are also evolving: Internet actors are more and more in position to provide both Live and On-demand Content Services to internet end-users, with similar quality constraints as for traditional TV Service of Network Operators.

Moreover more and more Cloud offers would dramatically increase the amount of contents to be stored, with the constraint of delivering them as if they were stored locally.

Description

Integrating nodes of Content Delivery Networks into operator networks can be an effective and cost-efficient way to answer to the challenges of Video Traffic Delivery. Producing the content streams out of compute/storage nodes nearer to the end customer saves upper network links and equipment and allows delivering streams with higher bandwidth in more reliable quality.

Operators are using CDNs integrated into their own networks to deliver their own managed video services (e.g. VoD complementary to IPTV, file download), but also to offer wholesale CDN services and to address OTT video traffic (e.g. via transparent caching).

Specific cases are 3rd parties like CDN provider or large content provider who ask operators to deploy their proprietary cache nodes into the ISP network (e.g. Netflix OpenConnect program, Akamai Aura CDN). This comes with benefits for both sides but also with the challenge that eventually the operators will host a zoo of different cache devices side by side in their premises.

In many current deployments, CDN cache nodes are dedicated physical appliances or software with specific requirements on standard but dedicated hardware. Often physical appliances and servers for different purposes are deployed side-by-side.

This comes with a number of disadvantages:

- The capacity of the devices needs to be designed for peak hours (typically on weekend evenings). During weekdays and business hours, the dedicated hardware appliances and CDN servers are mainly unused.
- It is not possible to react on unforeseen capacity needs e.g. in case of a live-event as hardware resources need to be deployed in advance.
- The average peak utilization and resiliency of CDN nodes for dedicated purposes or from different partners is lower than it could be if the hardware resources would be shared between virtual appliances on the same NFV Infrastructure.
- Dedicated physical devices and servers from several parties drive the complexity of the operator network and increase the operational expenses.
- Content delivery is a very volatile market driven by new content formats, protocols, device types, content protection requirements, etc. Dedicated designed hardware hinders the necessary flexibility to react on these changes.
- Content Delivery may imply some Value Added Services, e.g. for Security concerns or for optimizing Performances. It may be valuable for the Network Operator to rely on Outsourcing of a Partner's solution rather than having to operate its own solution.
- Dedicated physical devices and servers from several parties drive the complexity of the operator network and increase the operational expenses.
- Content Delivery may imply some Value Added Services, e.g. for Security concerns or for optimizing Performances. It may be valuable for the Network Operator to rely on outsourcing of a Partner's solution rather than having to operate its own solution.

Virtualization Target

CDN is a generic word to design a combination of multiple components, such as cache nodes and CDN controller.

Basically speaking, the CDN controller objective is to select a cache node (or a pool of cache nodes) for answering to the end-user request, and then redirect the end-user to the selected Cache Node. The Cache Node shall answer to the end-user request and deliver the requested content to the end user. The CDN controller is a centralized component, and CDN cache nodes are distributed within the Network and in N-PoPs.

Virtualization of CDN is potentially covering all components of the CDN, though the first impact would probably be on cache nodes for achieving acceptable performances (e.g. throughput, latency)

Deploying CDN nodes as virtual appliances on a standardized environment shall overcome most of the challenges mentioned above:

1. Resources can be allocated to other applications during weekdays and business hours.
2. Overall capacity is shared by all content delivery appliances.
3. Operational process of resources for different parties are harmonized.
4. As appliances are just software it is easy to replace or add them in case of new requirements in content delivery.
5. Running CDN nodes as virtual appliances on an operator owned infrastructure will even allow a new kind of wholesale business towards CDN providers and large content providers with private CDNs if there is a standardized way how to deploy and operate 3rd party CDN nodes in a controlled way in the operator environment beyond the point of co-location environments.

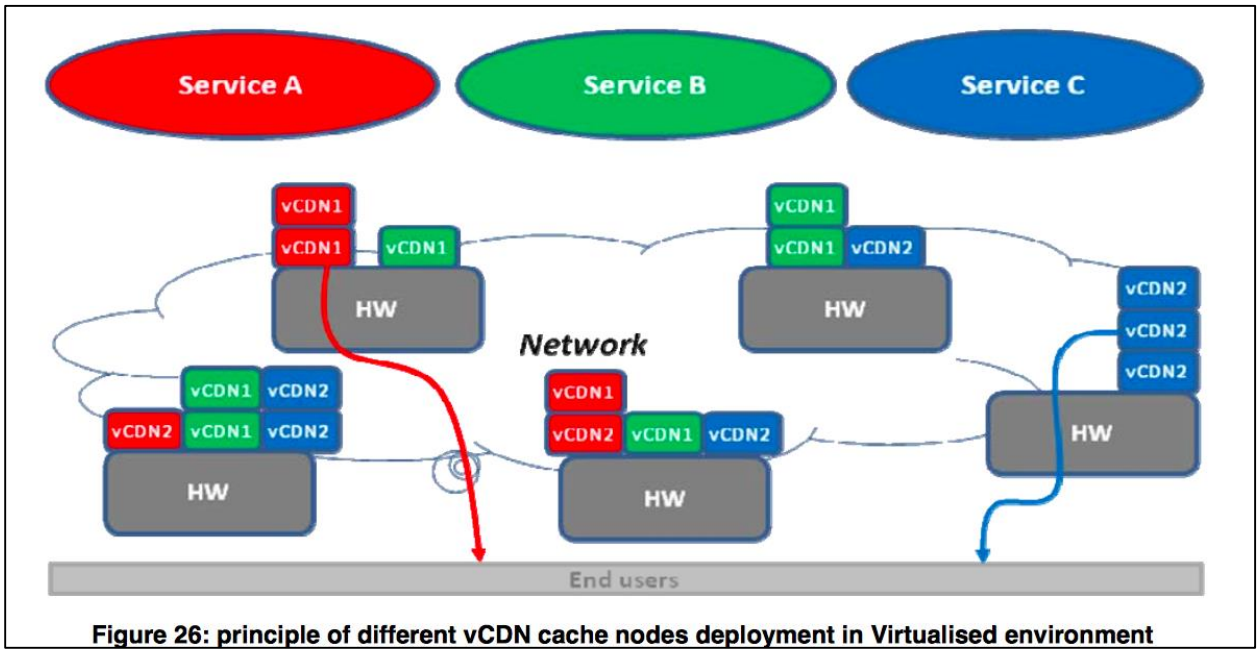


Figure 26: principle of different vCDN cache nodes deployment in Virtualised environment

5.2. Other Candidate SDN Use Cases

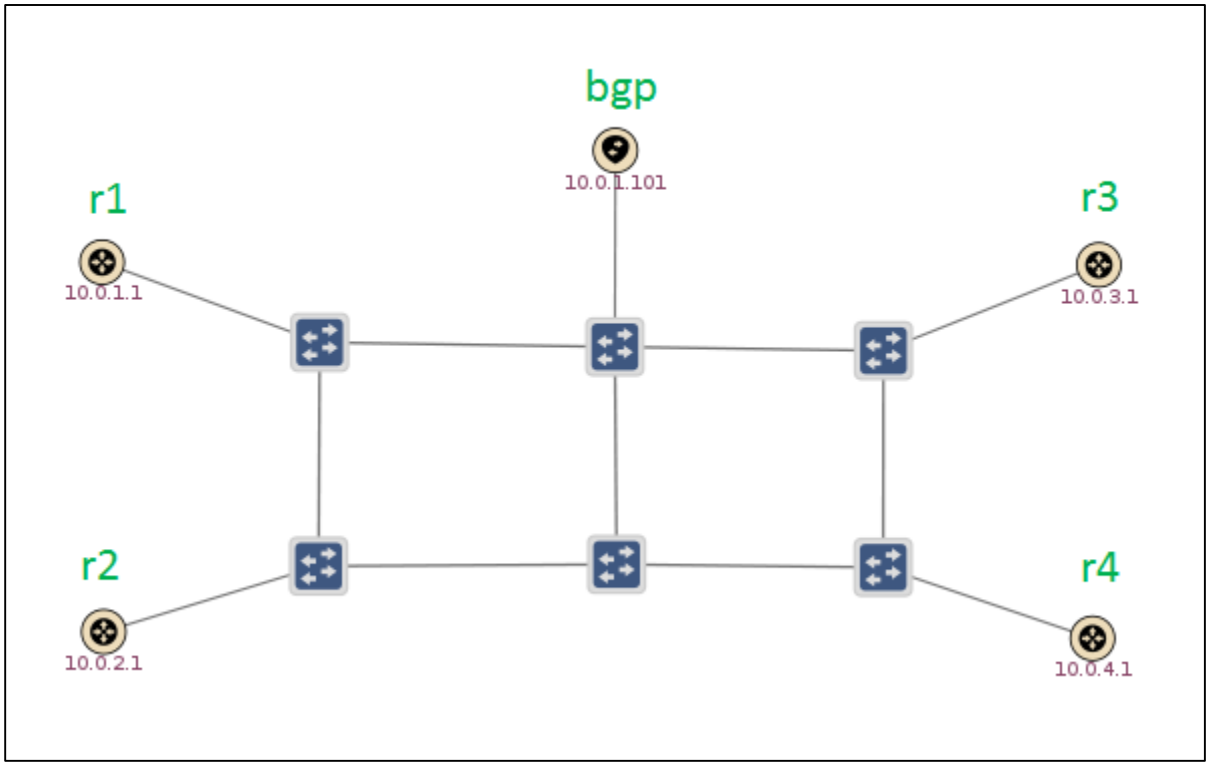
There are a number of other candidate use cases that were uncovered and considered through our research. At this point we feel these are more proof of concept based and not as widely adopted as the dominant use cases cited above, although that may change as the industry matures.

5.2.1. Use Cases Cited from ONOS

5.2.1.1. SDN-IP

The Network Topology

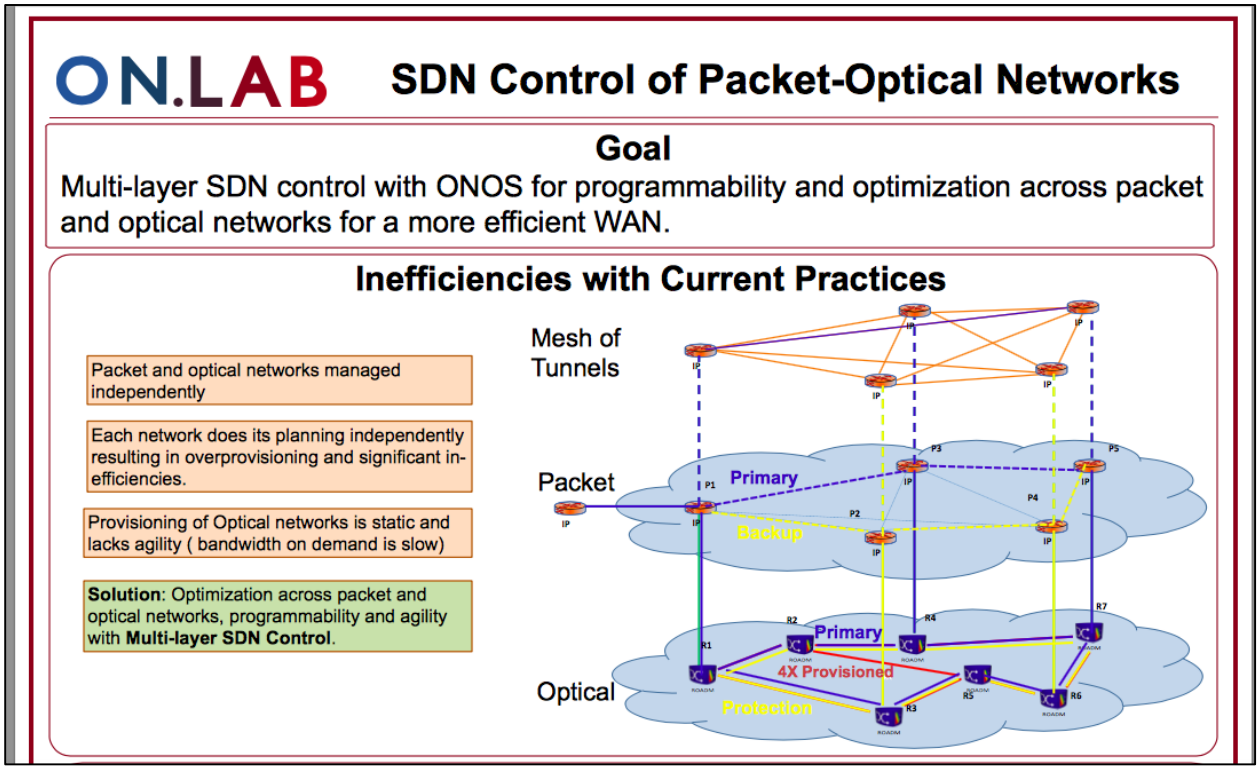
This involves a simple emulated Mininet topology, which contains some OpenFlow switches to make up the SDN network. Connected around the edges of the SDN network are emulated routers. The routers run a piece of software called Quagga, which is an open-source routing suite. Note that it is not mandatory to use Quagga; any software/hardware capable of speaking BGP will do. An example would be to run the BGP part of Quagga on them, to simulate external BGP routers belonging to other administrative domains. The goal of SDN-IP is to be able to talk BGP with these routers in order to exchange traffic between the different external ASes.

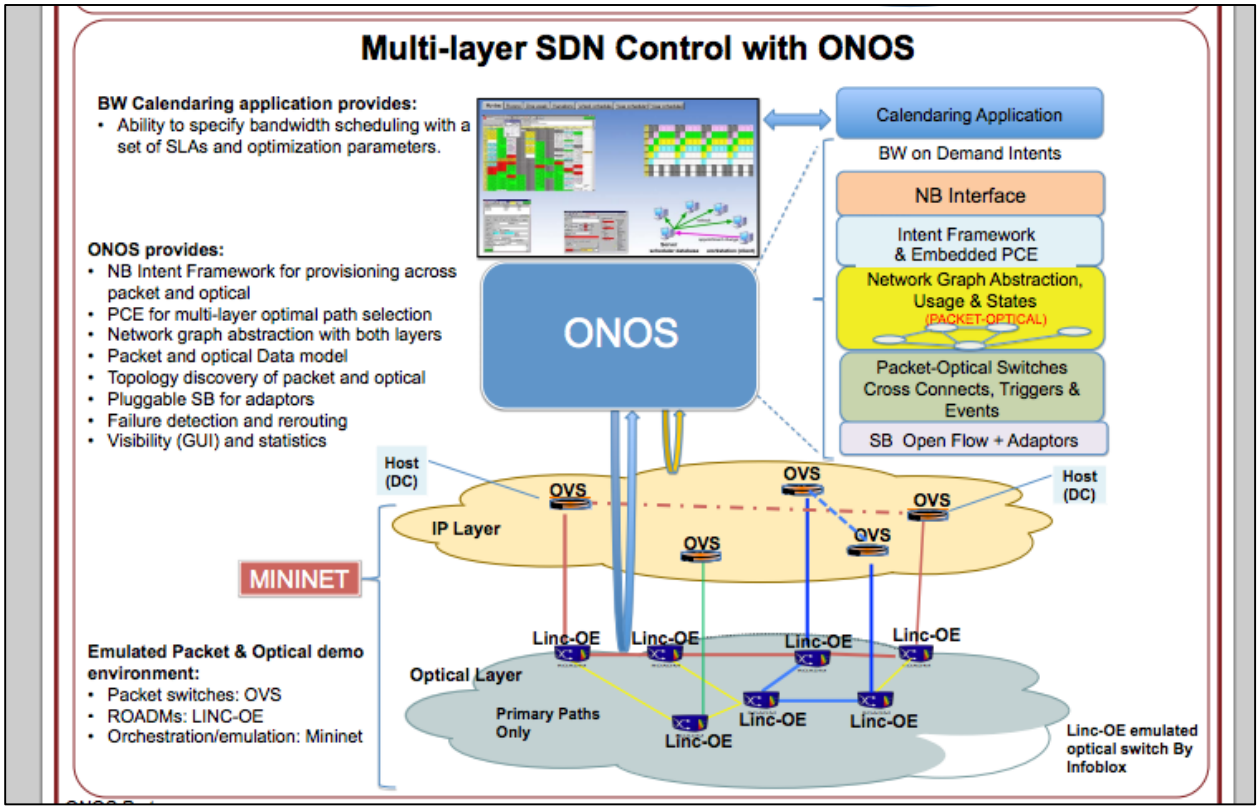


This figure shows the topology as observed by ONOS (Open Network Operating System) - 6 blue OpenFlow switches, and 5 peripheral nodes with yellow icons.

- The node labelled "bgp" is the *Internal BGP Speaker*. It sits inside the SDN network and its job is to peer with all the *External BGP Routers*, learn BGP routes from them, and relay those routes to the SDN-IP application running on ONOS.
- The other four nodes, labelled r1 through r4, are the *External BGP Routers*. They are the border routers that reside in other networks that want to exchange traffic with us.
- Behind each router is a host. These are labelled h1 through h4 in Mininet. ONOS can't see these hosts, because they reside in other networks that are not controlled by ONOS.

5.2.1.2. Packet Optical


ON.LAB
SDN Control of Packet-Optical Networks
Goal
Multi-layer SDN control with ONOS for programmability and optimization across packet and optical networks for a more efficient WAN.
Inefficiencies with Current Practices
Packet and optical networks managed independently
Each network does its planning independently resulting in overprovisioning and significant in-efficiencies.
Provisioning of Optical networks is static and lacks agility (bandwidth on demand is slow)
Solution: Optimization across packet and optical networks, programmability and agility with Multi-layer SDN Control.
Mesh of Tunnels
Packet
Primary
Backup
Optical
Primary
4X Provisioned
Protection



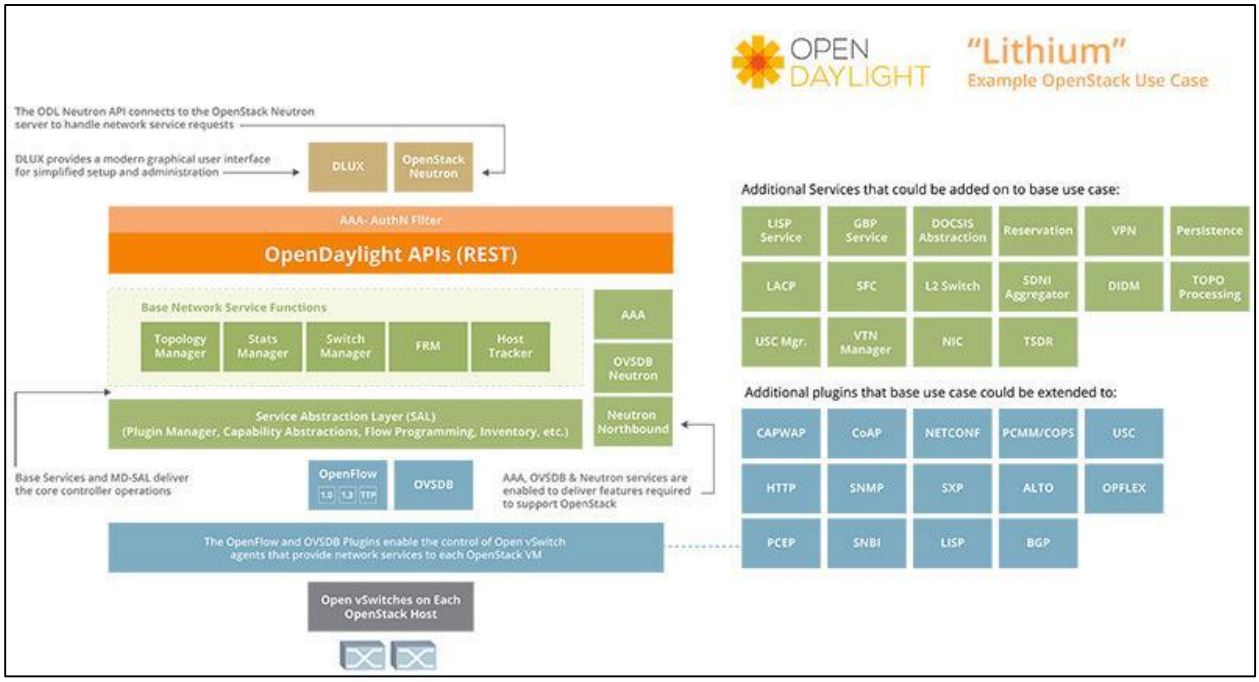
5.2.2. Use Cases Cited From Open Daylight

Network Services for Cloud Data Center

This educational use case provides a base implementation of OpenStack with the Neutron Framework using OpenDaylight to provide network virtualization services with Open vSwitch.

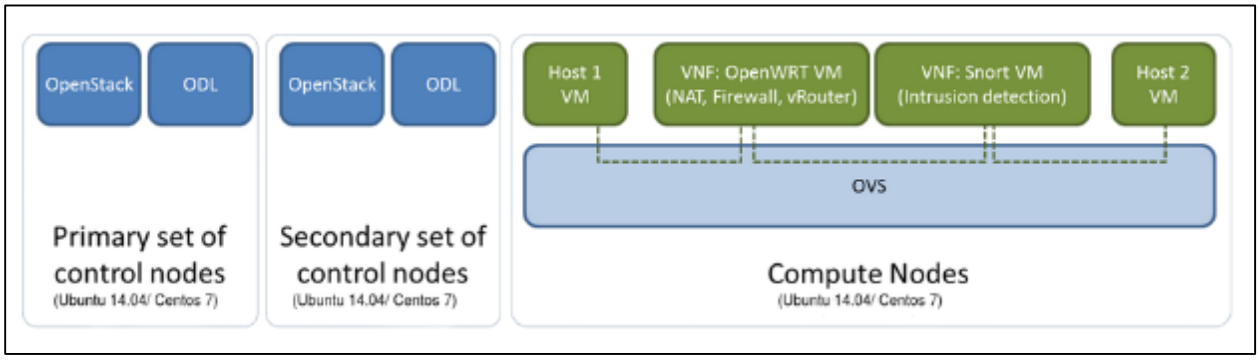
Description

Once implemented, users can create and launch virtual machines from OpenStack and the OpenDaylight controller will communicate with OpenStack servers to automate the configuration of the virtual network, enabling virtual machines to be defined and launched without manual network configuration and without needing to create scripts to automate the network configuration. Once the connection between OpenStack and OpenDaylight is setup, preparing the virtual network for new VM's becomes a simple, plug and play experience.



5.2.3. OPNFV Bootstrap

This use case provides a base implementation of OpenStack with the Neutron Framework using OpenDaylight including OPNFV optimizations for NFV use cases.



Project “Bootstrap/Get started” assembles and tests a base set of infrastructure components for OPNFV to run a few example VNFs like LBs (Load Balancer), FW (Fire Wall). It puts together a single deployment type that can both be used by developers and run in continuous integration. The goals of the GetStarted Project is to stand up quickly one or more

stacks of components, learn from their differences and commonality of deployment experience, and feed that back into producing a more flexible framework. Initially the project will focus on a single combination of components.

The project targets an installation on a virtual environment based on Linux Ubuntu 14.04/Centos 7 as base operating system and distribution. “Bootstrap/Get started” provides a solution to automatically install and configure the required components using existing installer and configuration tools and perform a set of basic system level tests (i.e. test whether OpenStack, OpenDaylight/SDN Controller, OVS components are operational, tests whether a set of VNFs can be deployed/removed on the Compute Node). The project is intended to serve as both an initial development framework and a framework for CI. It is important that developers work on realistic deployments which (‘works on devstack &/or packstack" as Compute Node VNFs) and future projects will work on development tooling.

6. Challenges engendered by the SDN / NFV architectures

6.1. Challenges

The cybersecurity threat surface is increased by the architecture attributes of SDN and NFV such as logical centralization of control, disaggregation, abstraction, multiple trust domains and Virtual Network Functions (VNF) running in virtual machines and replacing / supplementing physical network functions, as well as hypervisor vulnerabilities facilitating VM/Guest OS manipulation and data exfiltration or destruction, increased open source software usage potentially increasing software vulnerabilities and amplification attacks being enhanced by the elasticity of automatic scale-out function.

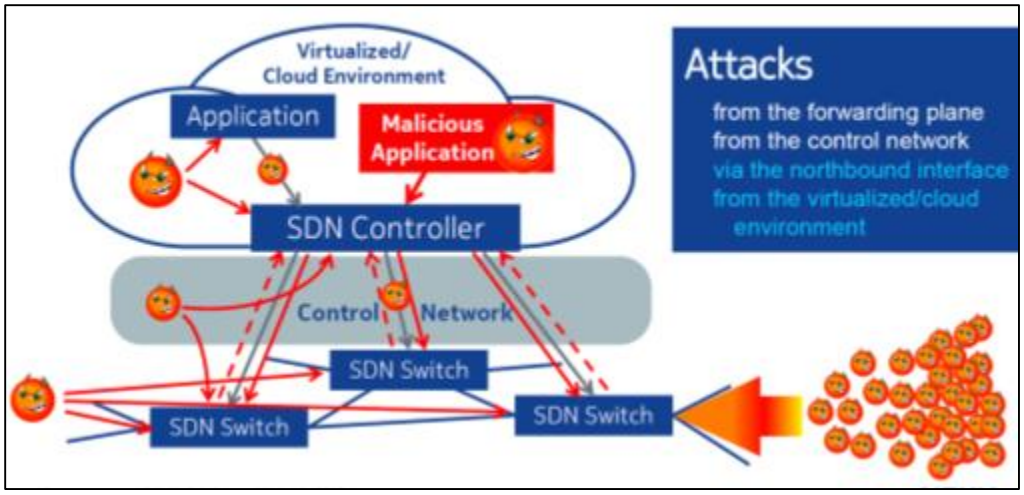


Figure 6.1 SDN Attack Surfaces (Source: Peter Schneider, Nokia)

There are other challenges faced by organizations as articulated by a leading service provider (AT&T) *[Ref. d]*

The software-centric architecture allows changing how and where many FCAPS (Fault, Configuration, Accounting, Provisioning and Security) functions are performed, and enables the transformation of many OSS (Operations Support Systems) and some BSS (Business Support Systems) platforms. Current OSS/BSS functions do not "go away" but will likely be refactored, simplified, and in some cases functionally expanded to reflect new operational needs and opportunities for operational excellence. Key to this will be the adoption of various shifts in operations. Expected operational shifts will include:

From	To
Hardware Centric	Software Centric
Separate IT/data center & Network/CO	Common technology & technical plant
Quarterly software releases	Continuous software process - "sandbox."
Geographically fixed, single purpose equipment	Highly dynamic & configurable topology & roles.
Tight coupling of NE, generic, EMS & NMS/OSS	Separation of physical & logical components.
Separation of service elements & support systems	Integrated orchestration, automation & virtualization.
Faults as service failures	Faults as capacity reduction events.
Hardware monitoring appliances	Software based monitoring.
Service specific resource combinations	Profiles, templates & reusable resource combinations.
Special design and provisioning processes	Configurable catalog/rule-driven delivery frameworks.
Optimized provider network & ops process	Optimized customer experience.
Highly constrained, independent & disaggregated control planes	Highly integrated & automated control planes driven by customer & operator policies.
Limited service dimensions	Multifaceted service dimensioning.
Highly constrained data translation & synchronization solutions for shared management knowledge between network & systems	Shared management "Data Bus" technology between network & systems.
Slow tooling changes requiring coding	Rapid tooling changes using polices/rules
Network management	Customer experience management
Long lead provisioning times – often hardware and process constrained	Real-time provisioning
Static billing and charging	Granular and dynamic usage-based charging, billing, financial management, subscription

6.2. Addressing the Challenges

6.2.1. Secure the SDN Controller

The security design for SDN needs to ensure that the SDN Controller is not a weak link in the network and cannot be compromised. Examples of security design principles include use of secure protocols, encrypted communications, implementation of scalable mutual authentication of message flows, as well as authorization and denial of service protection. The section on Industry Landscape describes how a leading Service Provider addresses the issues.

6.2.1.1. Ensure SDN Controller Availability

The SDN controller is the centralized decision point. Security attacks on the controller assets and applications will have a wider network impact. Access to the SDN controller and its applications should be tightly controlled and monitored.

6.2.1.2. Establish Trust

Protecting integrity of network and SDN topologies is critical. This means ensuring that the SDN Controller, SDN controller's applications and the devices it manages are all trusted entities which operate as they should.

6.2.1.3. Create and enforce robust policy framework:

A policy frame work helps in enforcing that SDN deployments that satisfy the design requirements. Conflict resolution of multiple SDN networks under the same controller should be addressed to satisfy availability and security requirements. Privacy and network security requirements apply to traditional cloud service as well as SDN/NFV deployments.

6.2.1.4. Security of underlying infrastructure

Network programmability of the SDN can leverage NFV infrastructure for service chaining and utilizing physical/virtualized resources. SDN/ NFV infrastructure should be resilient to DoS attacks from control, user and management data flows and applications, similar to non SDN networks.

6.2.1.5. Monitor security of SDN

The flexibility of SDN networks (and also virtualized NFV applications) presents challenges for monitoring. Security-pertinent data needs to be analyzed in the context of this dynamically-changing network topology. Data sources can include traffic counters and statistics in SDN switches, controller logs and possibly even data-plane traffic monitoring. Usage of SDN APIs also needs to be suitably monitored (probably through logging). The large volume of data from a large number of (virtualized) sources and the dynamic nature of the network implies that advanced monitoring and analytic techniques (e.g. Big-data analytics) may be required.

6.2.1.6. Securing north bound SDN API

The SDN northbound API itself needs to be secured, including authentication and authorization of applications that use it, and prevention of interference between applications. The API is an attack surface that could allow applications to attack the controller, the network, or other applications.

7. Opportunities For Enhanced Security Solutions Engendered by SDN / NFV

There are few times in our lives when we feel like we have the chance to be a part of something that changes the way that networks are operated, deployed, managed and empowering services for the next generation. SDN and NFV provide the "machinery" to make that happen. However, the application of the SDN and NFV business and technology agility has a new threat surface and new aspects of scale, resiliency and redundancy that we've yet to face in today's networks. Security MUST remain at the forefront of the evolution of service delivery to our current and new customers. The characteristics of SDN and NFV that make the opportunities possible include, but are not limited to:

- Agility in Business and Service Creation
- Agility in Technology

In today's Service Provider, it often takes 18 months or more from first idea to first dollar collected for that service. SDN and NFV services utilize service chains of virtual devices. The use of an orchestration platform and other foundational components provides the foundation to simply offer a service where a user goes to a portal, buys a service, and it is implemented in minutes. The business model has forever changed for managed services, whether a network service, an application or a hybrid of the two. The need for truck rolls and appliance deployments into data centers to support new applications has been obviated by virtualization, SDN and NFV. This agility also applies to the security of the networks that offer the aforementioned services. Security is best articulated as two very simple, yet powerful dynamics.

- Visibility & Detection: Understanding the behavior of the network in peace time so that an anomalous or suspicious event can be examined against a baseline and then …
- Mitigation Control: A mitigation control or chain of controls is deployed at the right place (network context), at the right time (minimizing mean time to mitigation) and in an optimized path to mitigate the threat, whether in a single place in the network or distributed across the network.

One of the best examples for the application of SDN and NFV threat defense is a look at how the application of BGP works in the context of threat defense services with an SDN Controller and NFV. BGP is arguably the life blood of the Internet today. It governs how organizations peer with each other. It is the standard for how business services are foundationally offered in service providers today via 2547bis services otherwise known as MPLS VPNs. These VPNs are offered at layer 2 or layer 3 today. BGP is also at the core of policy control for DDoS using BGP Flowspec. As SDN and NFV are evolutionary technology (we will apply them to existing networks we operate today) not revolutionary (start over and deploy Greenfield networks), we will continue to look to use BGP as a key component of operating SDN and NFV networks. An example of this is that in SDN controllers today, BGP-LS is often used at the MD-SAL layer to give the controller a "picture" of the network topology under the controller. This is critical and a key when the SDN controller is used as a policy fulcrum for mitigation of threats, whether DDoS or otherwise. The SDN controller is now able to offer information about the impact of a mitigation action, for example, by consulting with the BGP-LS delivered topology, making the mitigation placement a more educated choice.

The example above is just one application of BGP to an SDN and NFV network. The plethora of use cases will lead to many more in the future.

There are many opportunities coming that will push the envelope for security of SDN and NFV. Internet of Things is such an example. How might you secure and operate a network with billions of sensors with a very small memory footprint all controlled by an SDN controller? How might you secure a "connected car" when policy and other controls are articulated through SDN and NFV? How might the security concerns differ as we move toward Micro-Service architectures where services currently delivered in virtual machines are decomposed and offered in chains of agile services which protect our networks and/or provide customized monetizeable services for our customers? The opportunities, both on the business and technical side are almost infinite.

8. Industry Landscape

8.1. Service Provides and vendors

Major aspects of a leading Service Provider's (AT&T) approach to virtualization involving SDN and NFV are shown below in the Figures 8.1 – 8.3 *[Ref. e, f]*

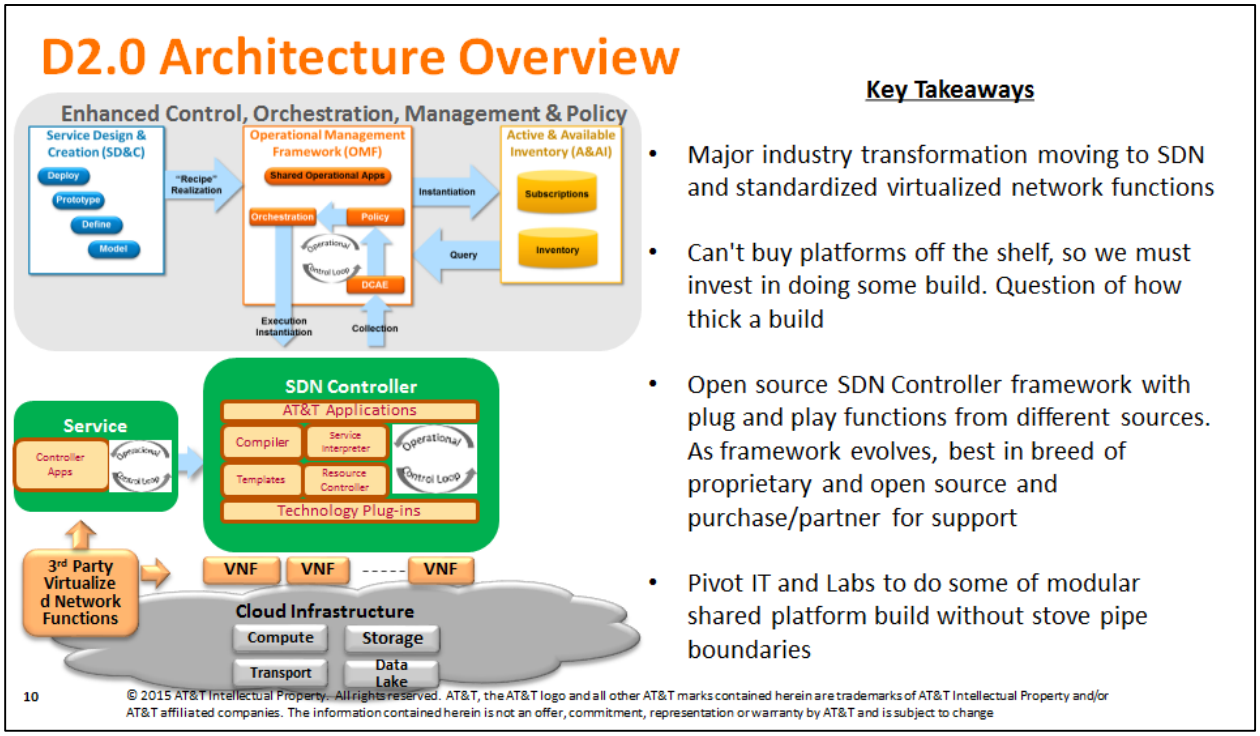


Figure 8.1 Domain 2.0 Architecture

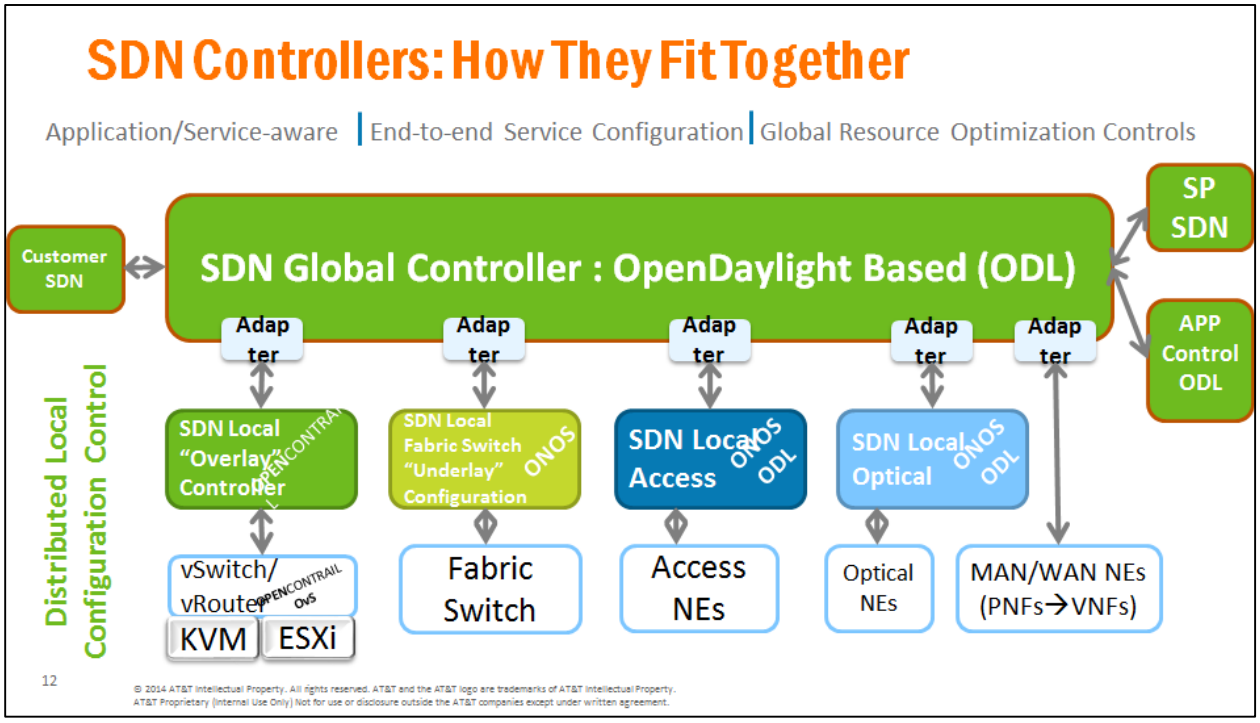


Figure 8.2 SDN Controllers in Domain 2.0

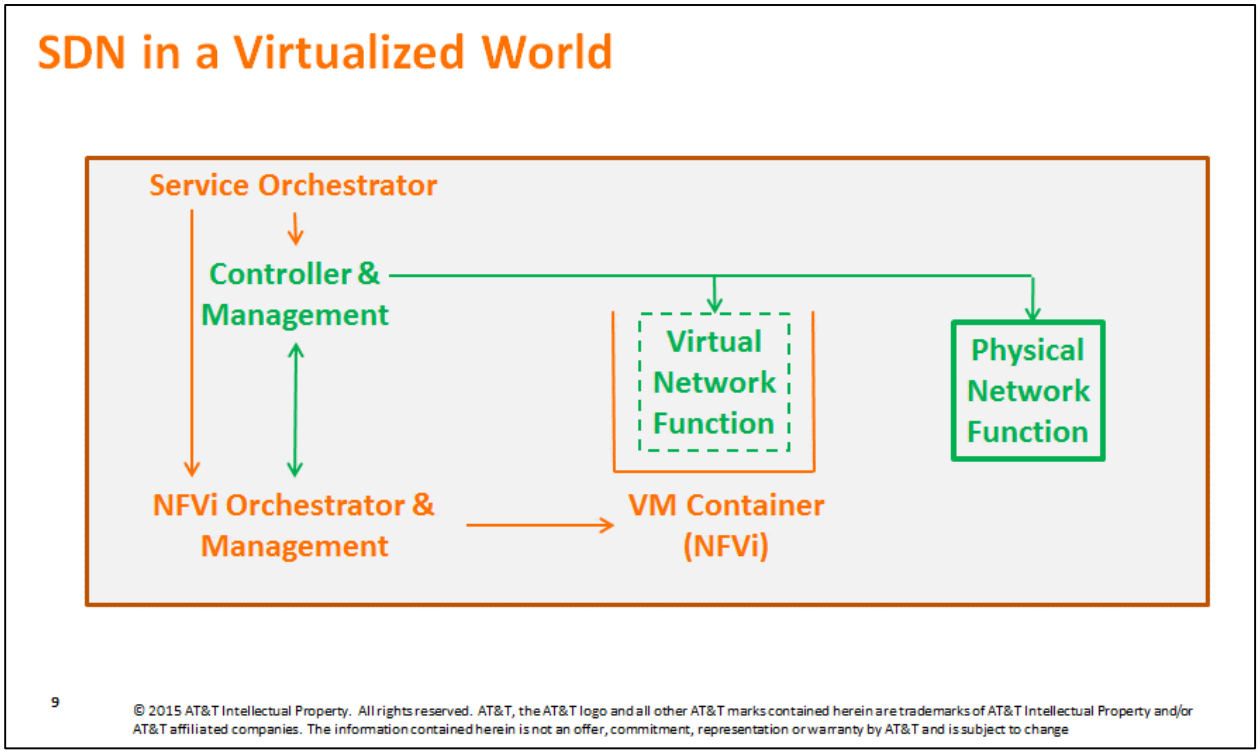


Figure 8.3 SDN and NFV Functions in Domain 2.0

Some aspects of a Service Provider's (AT&T) approach to addressing security risks, resiliency and trust model follow:

- Security Scanning, Hypervisor Hardening and Access Controls are used to mitigate Hypervisor Vulnerabilities
    - Security Scanning includes: Code scanning and system scans for vulnerabilities (i.e. bad code, Malware, misconfigurations, etc.), and applying security patches
    - Hypervisor Hardening includes: Minimizing the attack surface (i.e. closing vulnerable ports, limiting access to the Hypervisor, etc.)
    - Access Control includes: Authentication, Roles to limit the user/application to performing specific activities, activity logging
- Security Scanning and active participation in the Open Source community are used to mitigate potentially Open Source software vulnerabilities

        - Security Scanning includes: Code scanning and system scans for vulnerabilities (i.e. bad code, Malware, - misconfigurations, etc.), and applying security patches
        - Active participation in the Open Source community includes: SP as an active member/participation in Open Source Forums to lead/drive security best practices and receive real-time notifications/insight about new vulnerabilities
- Firewalls and Intrusion Detection/Prevention Systems are used to mitigate Amplification Attacks

Measures Employed to Make SDN Networks Resilient and Secure

- Network Simplification & Automation – Network posture is less vulnerable to security threats, consistent policy configuration, automated quarantine
    - A Policy function facilitates the rules for how the network is built/configured – this provides consistency and security
    - SDN/NFV Controllers working with the Policy function and the Data Collection, Analytics and Events functions facilitates automated quarantine of compromised VMs
- Flexibility & Scalability - Improved incident response time, DDoS resiliency, dynamically block/reroute malicious traffic
    - SDN/NFV Controllers working with the Policy function and the Data Collection, Analytics and Events functions can quickly instantiate(spin-up) new VMs to scale-out VNFs(virtual applications) to maintain network/service resiliency in the event of a network/security incident (e.g. DoS/DDoS)
    - SDN Controllers working with the Policy function can facilitate rerouting of malicious traffic
    - *Note: These functions are inherent with SDN/NFV*
- Security Function Virtualization – Security-on-Demand, Security-as-a-Service
    - Security Function Virtualization is the virtualization of traditional security functions such as: Firewalls and Intrusion Detection/Prevention Systems to facilitate Security-on-Demand and Security-as-a-Service

Trust Model between Devices and Controllers, and between controllers

- Secure Northbound (APIs) Interfaces via Authentication and Encryption
- Secure Southbound (XMPP/Openflow/BGP+NetConf) Interfaces via Authentication and Encryption
- Any customer access would be through API gateways that would load limit and scrub API's to prevent directly attacking the APIs on the controller.

- Southbound protocol traffic will be load managed so that attacks on the SDN enabled switches/elements will not be attack points on the SDN controller

SDN / NFV allows for greater scalability, customization as well as automation across network infrastructure. Infrastructure and server functionalities can be managed and quickly adapted to meet changing needs. Software-defined everything concepts have implications to many areas of infrastructure including networks, services, applications, devices and servers. Programmability creates new challenges, particularly for security, as visibility into the underlying mechanics of the network and all the details of what is happening are often abstracted. A combination of long-established and new networking protocols have standardized virtual networking and overlay networks across network equipment, virtual switches and cloud management systems. Examples of such protocols include Netconf, OpenFlow™ , and control-plane protocols such as BGP, DNS.

8.1.1. Attack surface & security design

The attack surface for SDN/ NFV is not static. One of SDN/NFV security design goals is to ensure NFV instances and other applications are secure and hardened. Hardening and other security measures currently in practice also apply to SDN/NFV network elements. These measures include hypervisor security, logical and physical separation to enforce security zones and traffic separation. Securing DNS/ BGP, NTP etc. and their operations should continue. SDN Controller interfaces with switching, routing s and applications need to use secure protocols, robust authentication/ authorization mechanisms and measures to mitigate DoS attacks. Multiple layers of security will be needed to protect SDN / NFV as shown in Figures 8.4 and 8.5

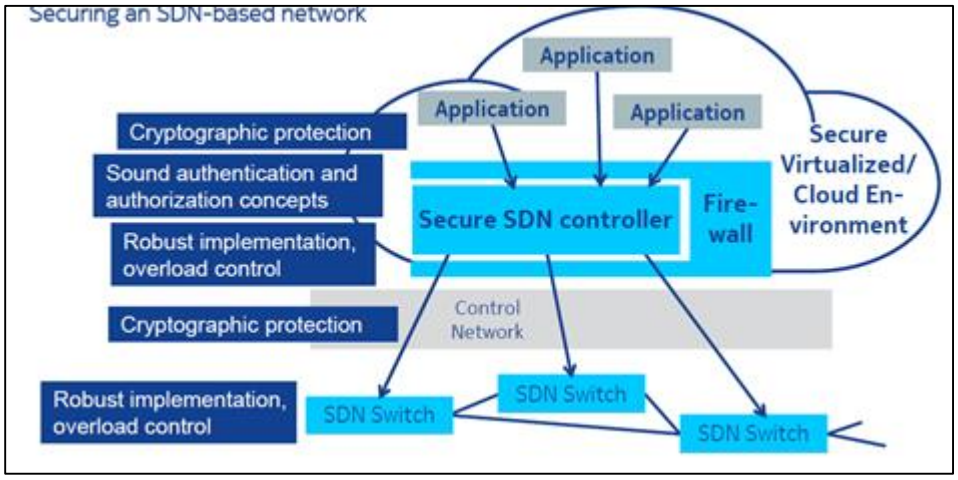


Figure 8.4 Securing SDN Based Networks (Source: Peter Schneider, Nokia)

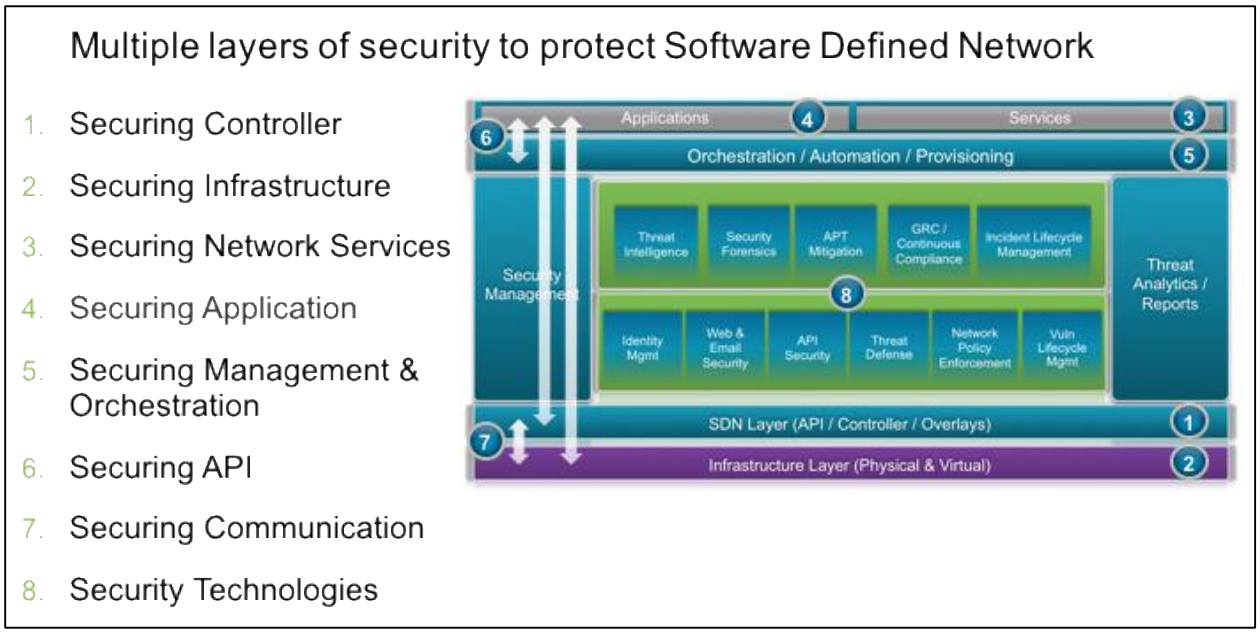


Figure 8.5 Multiple Layers of Security (Source: Mike Geller, Cisco)

8.1.2. Analytics, policy and monitoring

SDN/NFV configuration is policy and Intent driven, which requires a capability to continually monitor the infrastructure for events and changes. Monitoring and analysis needs to provide sufficient embedded intelligence that can automatically translate intent into policy driven actions.
Analytics can play an important role in security policy enforcement. Intelligence from traffic monitoring, dedicated and virtual security devices and other security applications can be used to dynamically configure security. Analytics provide advantage to combine traditional and virtualized security measures to provide fine grained security controls. Analytics make it possible to provide advanced threat protection, incorporating machine learning and anomaly detection capabilities that can understand the relevance of changes in the environment and can adapt to the risks.
Using analytics and automation, SDN can provide a fine grained security measures to different apps and end points which would have been difficult to implement in a traditional network

8.1.3. SDSec

Software Defined Security (SDsec) is a paradigm for implementing security functionality by leveraging capabilities provided by SDN/NFV. For example, SDN northbound APIs allow new security applications to be built on top of SDN. Virtual security functions are examples of VNFs in a NFV context. These can be chained and orchestrated along with other virtual network functions. Software-defined security, together with NFV provides a new way to design, deploy, and manage security services by decoupling the network function from hardware appliances.

8.1.4. DNS

The lesson that we can apply to SDN security that we learned from the operation of DNS over many years is that security is best manifested in operations with a focus on redundancy and resiliency. The architecture of DNS is hierarchical in nature delivering an alternate DNS "resolver" or "service" in the event one DNS server is under attack. SDN and NFV require a unification or standardization of both technology and operational best practice guiding the SDN controller and the network controlled by it what to do when attacked and/or over-burdened.

SDN and NFV are, at least in most of today's use cases, applied to the delivery of an application or user experience where the application asks the network for a certain behavior within constraints. We must not forget the critical role of DNS in the application delivery lifecycle. If DNS were to be attacked or made unusable, think of how many of the services we run today (Web Browsing, SIP telephony…).

SDN and NFV introduce both new challenges and opportunities in security. While subject to distinct security threats, these technologies can also be used to build novel security solutions, preserving and improving the inherent security properties of on-boarded applications, enabling security as a service.

8.2. SDOs (Standards Development Organizations)

SDOs are working on several aspects of SDN / NFV, including security.

8.2.1. ETSI

ETSI has done seminal work on NFV. In November 2012 seven of the world's leading telecoms network operators selected ETSI to be the home of the Industry Specification Group for NFV. Now three years on, there is a large community of experts working intensely to develop the required standards for Network Functions Virtualization as well as sharing their experiences of NFV development and early implementation. The membership of ISG NFV has grown to over

270 individual companies including 38 of the world's major service providers as well as representatives from both telecoms and IT vendors. ETSI is working on several areas of security. Some of the relevant documents from ETSI are here *[Ref. g, h, l, j]*

8.2.2. IETF [Ref. k]

Although their efforts are just getting started, the IETF can be expected to play a significant role in the evolution of standards for SDN and NFV. For SDN, the IETF can develop standards that complement the efforts of the Open Networking Foundation (ONF) and other relevant SDOs. In the case of NFV, the IETF can possibly play a more central role in creating standards that fit into the overall architectural frameworks defined by the ETSI NFV ISG because ETSI's work is focused on frameworks and broad specifications rather than standards per se. The IETF Service Function Chaining (SFC) Work Group (WG) currently has over forty active Internet drafts on the topic of delivering traffic along predefined logical paths incorporating a number of service functions. It is likely that the IETF's work on SFC will apply to both SDN and non-SDN environments. Some of the topics being investigated by the SFC WG include:

- Service function instances discovery;
- Service function resource management;
- Service chain creation;
- Traffic flow steering rules on a router to define network forwarding paths;
- Service chain monitoring and adaptability for reliability and optimized performance;
- Information and data models for SFC and NFV.

Another area of IETF activity related to SDN and NFV is the work the IETF has done on a security architecture that is based on horizontal (a.k.a., east/west) APIs in addition to the northbound and southbound APIs. One IETF SDN-specific activity focuses on centralized security services (i.e., firewalls and DDOS mitigation systems) designed specifically for SDN environments. Another SDN-specific Internet draft addresses the possible application of DevOps principles to service provider software defined telecom networks.

During the last IETF (itrg sdnrg, nfvrg) meetings (93 and 94) drafts presented in SDNRG / NFVRG IRTF address several aspects of securing SDN NFV such as threat analysis, secure, robust, and resilient SDN Controllers, Secure SDN Authentication, Authorization, Attestation Approach. Trust Models, Trustworthy NFV Infrastructure, Reliability and Resiliency *[Ref. l, m]*

8.2.3. MEF (Metro Ethernet Forum) *[Ref. n]*

For the MEF LSO (Lifecycle Service Orchestration) context the SDN Controller brings an important paradigm which is about providing a "Virtual Network" API abstraction for any

northbound application – agnostic to the network technology – for the network domain the SDN Controller is managing. In the presence of SDN, the MEF Service Orchestration layer is simplified and can design the end-to-end service down to a Virtual Network abstraction level, and finally delegate the network implementation of the technology-specific Virtual Networks to the Controllers (Figure 8.6). NFV Orchestrator provides Network Function and Network Service instantiation / modification APIs which abstract the elastic data center resource management requirements. MEF LSO layer can therefore request the dynamic instantiation of a network function or network service and not worry about any data center IT resource implications.

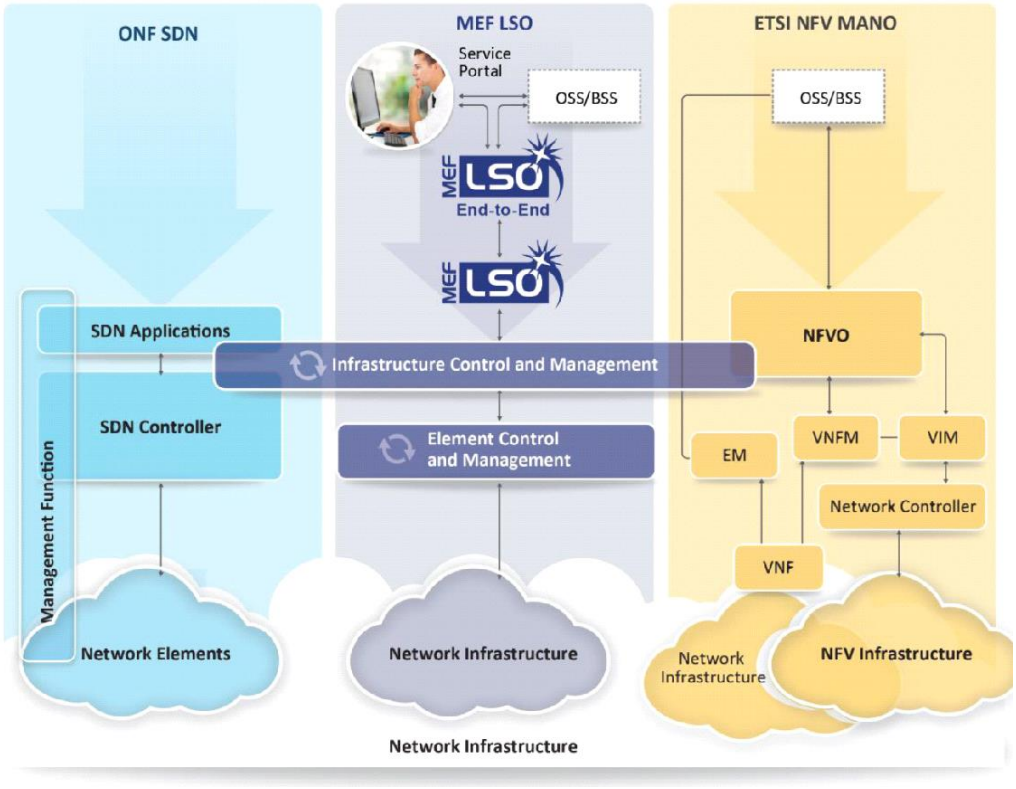


Figure 8.6: Lifecycle Service Orchestration

8.2.4. 5G Mobile Network *[Ref. o, p]*

- The design principles for the NGMN (Next Generation Mobile Network) envisions an architecture that leverages the structural separation of hardware and software, as well as the programmability offered by SDN and NFV

- The 5G architecture is a native SDN/ NFV architecture covering aspects ranging from devices, (mobile/ fixed) infrastructure, network functions, value enabling capabilities and all the management functions to orchestrate the 5G system
- To realize such a 5G system architecture, the C (Control) - and U (User) -plane functions should be clearly separated, with open interfaces defined between them, in accordance with SDN principles
- 5G should aim to virtualize as many functions as possible, including the radio baseband processing
- To realize the 5G concept of Network Slicing the C- and U-plane functions should be clearly separated, with open interfaces defined between them, in accordance with SDN principles
- 5G will be driven by software. Network functions are expected to run over a unified operating system in a number of points of presence, especially at the edge of the network for meeting performance targets. As a result, it will heavily rely on emerging technologies such as SDN and NFV.

8.3. Communities

8.3.1. OpenDayLight [Ref. r, s, t, u, v]

At this early stage of SDN and NFV adoption, the industry acknowledges the benefits of establishing an open, reference framework for programmability and control through an open source SDN and NFV solution. Such a framework maintains the flexibility and choice to allow organizations to deploy SDN and NFV as they please, yet still mitigates many of the risks of adopting early stage technologies and integrating with existing infrastructure investments.

With OpenDayLight, a community has come together to fill this need through the combination of open community developers and open source code and project governance that guarantees an open, community decision making process on business and technical issues. Establishing an open source project in this way is designed to help accelerate the development of technology available to users and enable widespread adoption of SDN and create a solid foundation for NFV.

OpenDayLight can be a core component within any SDN architecture. Building upon an open source SDN and NFV controller enables users to reduce operational complexity, extend the life of their existing infrastructure hardware and enable new services and capabilities only available with SDN. Whether your organization is an enterprise IT provider, a network service provider or a Cloud services provider, you can begin taking advantage of SDN and NFV using a community-driven, open source controller framework available today.

The OpenDayLight platform provides a common foundation and a robust array of services to enable a wide breadth of applications and use cases. ODL can deliver the benefits of SDN to use

cases as diverse as managing cable modems, connecting the Internet of Things, or controlling Ethernet switches using the OpenFlow protocol.

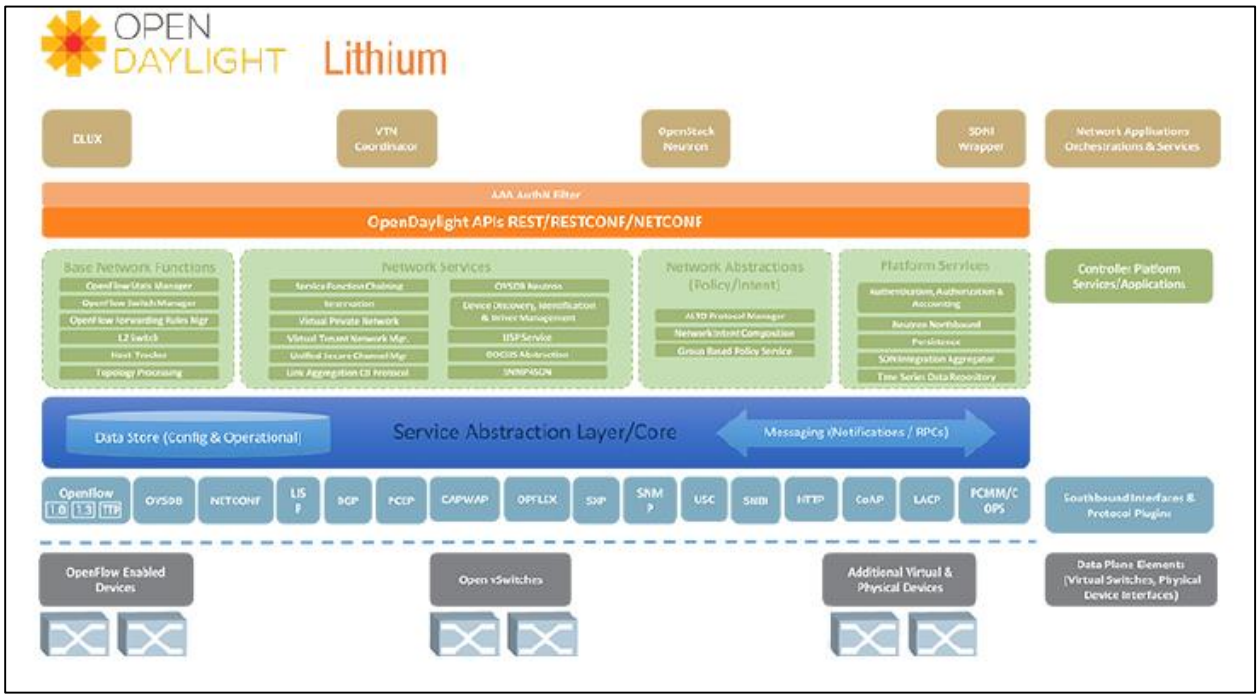


Figure 8.7: OpenDayLight Architecture

As shown in Figure 8.3.1, OpenDayLight is composed of a number of different modules that can be combined as needed to meet the requirements of a given scenario.

Amongst the large number of projects, the CrossProject: OpenDayLight Security Analysis project captures what security features are present in OpenDayLight today. In addition, it provides some recommendations for security enhancements. It addresses topics such as ODL Controller security, Secure Device/Controller BootStrap, Authentication and Authorization, Controller Clustering and Security. The Secure Network Bootstrapping Infrastructure (SNBI) project securely and automatically brings up an integrated set of network devices and controllers. Its Controller Architecture Framework address the High Availability.

The ODL has been working on use cases such as Network Services for Cloud Datacenter and, Service Function Chaining (SFC). Use Cases are based on deployments of OpenDayLight that have been implemented or tested either in a production or lab environment, and provide either detailed overviews

of how the implementation works or detailed instructions to enable users to replicate the use case. Figure 8.8 shows the architecture for the SFC use case.

The ODL has also been working on Cluster-based High Availability model. Network elements can connect to any controller in the cluster to spread the load. Network elements can be multi-homed to multiple controller nodes. Only 1 controller will control the network element. Applications can connect to any controller node and get the job done (N redundancy on northbound).

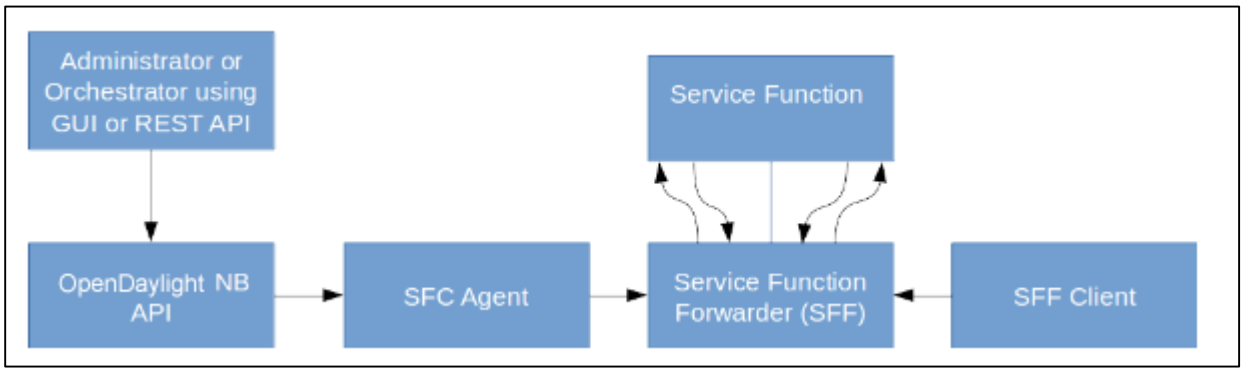


Figure 8.8: Service Function Chaining

8.3.2. OPNFV [Ref. w, x]

The OPNFV community is collaborating on a carrier-grade, integrated, open source platform to accelerate the introduction of new NFV products and services. By integrating components from upstream projects, the community can conduct performance and use case-based testing to ensure the platform's suitability for NFV use cases. The scope of OPNFV's initial release is focused on building NFV Infrastructure (NFVI) and Virtualized Infrastructure Management (VIM) by integrating components from upstream projects such as OpenDayLight, OpenStack, Ceph Storage, KVM, Open vSwitch, and Linux. These components, along with application programmable interfaces (APIs) to other NFV elements form the basic infrastructure required for Virtualized Network Functions (VNF) and Management and Network Orchestration (MANO) components. OPNFV's goal is to increase performance and power efficiency; improve reliability, availability, and serviceability; and deliver comprehensive platform instrumentation. OPNFV looks to realize the ETSI NFV ISG's architectural framework by bringing together upstream software components to implement an end-to-end platform for NFV.

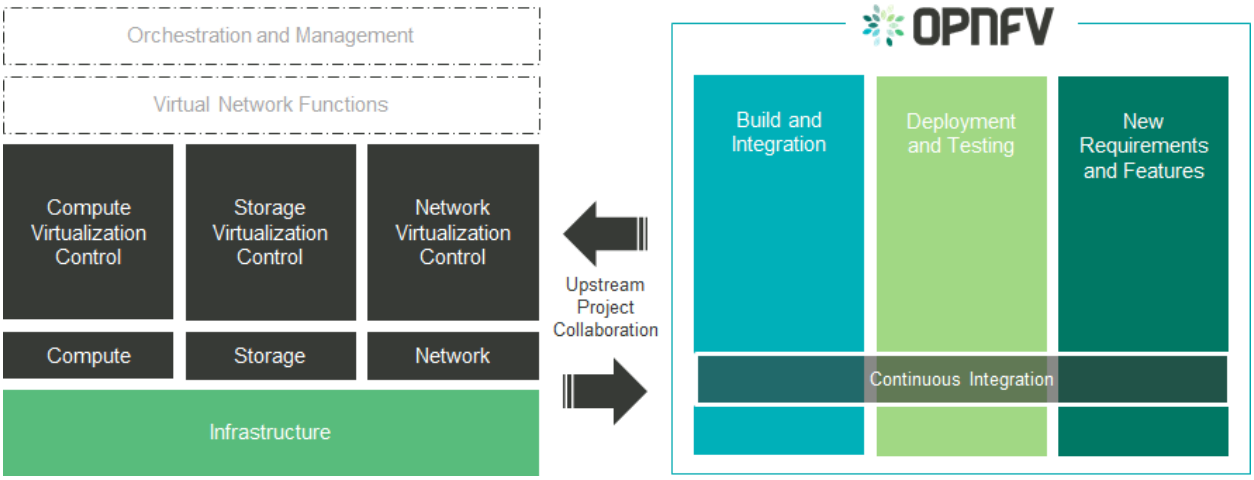


Figure 8.9 OPNFV Platform (Source: Luke Hinds, Security Project Team Lead, OPNFV, Heather Kirksey, Director, OPNFV)

OPNFV has released ARNO, a developer-focused release aimed at those who are exploring NFV for proofs-of-concept, developing Virtual Network Functions (VNF) applications and or interested in performance and use case-based testing. Virtual network functions range from mobile deployments, where mobile gateways (e.g. SGW, PGW, etc.) and related functions (e.g. MME, HLR, PCRF, etc.) are deployed as VNFs, to deployments with "virtual" customer premise equipment (CPE), tunneling gateways (e.g. VPN gateways), firewalls or application level gateways and filters (e.g. web and email traffic filters) to test and diagnostic equipment (e.g. SLA monitoring).

The OPNFV Security Group focuses on improving OPNFV security through architecture, documentation, code review, upstream inter-work with other groups, vulnerability management and security research, providing an 'umbrella' group to encourage development of security centric functions within the OPNFV eco-system and effectively handling vulnerability and threats in a coordinated manner.

8.3.3. ONOS (Open Network Operating System) [Ref. y, z]

ONOS partners with Linux Foundation and the mission is to transform service provider infrastructure with open source SDN/ NFV Platforms and Solutions and to bring economies of a datacenter and agility of a cloud to service provider infrastructure. It aims to Build open source SDN OS and SDN / NFV solutions for Service Providers, and help vendors to create value with open source and white boxes.

Here are some ways in which people have built applications upon ONOS, or integrated ONOS as part of their work:

- SDN-IP
- Packet Optical
- NFV (NFaaS)
- CORD: Leaf-Spine Fabric with Segment Routing
- IP RAN
- ONS2015 - CORD
- Peering Router - AS Apollo
- Multicast

ONOS provides useful Northbound abstractions and APIs to enable easier application development. Such abstractions and APIs are not only easy to use but also powerful as they basically allow ONOS applications to do anything desired, and it is indeed necessary to grant such a powerful authority to applications to offer as much network programmability as possible. Such powerful capabilities of ONOS applications may introduce potential misuse opportunities or software failures, and eventually affect the behavior of the managed network. In the case of the network with certain requirements (e.g., mission-critical networks), the network operators may want to configure the controller environment to be a bit more conservative by restricting the capability of the applications. For those who wish to configure ONOS to behave in a conservative manner, that Security-mode ONOS can be used.

8.3.4. CSA (Cloud Security Alliance) *[Ref. aa, bb, cc]*

CSA has developed the software defined perimeter (SDP) security framework and how it can be deployed to protect application infrastructure from network-based attacks, and “Software Defined Perimeter (SDP) protocol,” which is designed to provide on demand, dynamically provisioned, air-gapped networks. Air-gapped networks are trusted networks that are isolated from all unsecured networks and this may allow them to mitigate network-based attacks.

CSA, under its Virtualization Working Group, had been developing an NFV / SDN Position paper for expounding key security concerns and concepts relating to NFV and SDN. CSA Virtualization WG (Working Group) has now released a precursor WP, for peer review, to create a basic framework for security awareness in this context. Future deliverables from the CSA Virtualization WG will offer further, practical steps that NFV/SDN technologists can leverage to simplify the process of securing their infrastructures.

The WP offers a framework for approaching network virtualization security when applied to NFV. It references SDN concepts, because SDN is the critical virtualization enabling technology. The WP helps CSPs (Communication Service Providers) and Enterprises better understand how adopting NFV infrastructure will affect their risk profiles and how the dynamic aspects of NFV will impact their overall security frameworks. It lists the reasons why securing NFV and SDN environment pose challenges. The WP describes significant opportunities offered by deploying security functions as VNFs (Virtual Network Functions) compared to deploying them as hardware network appliances. The WP has also proposed security framework.

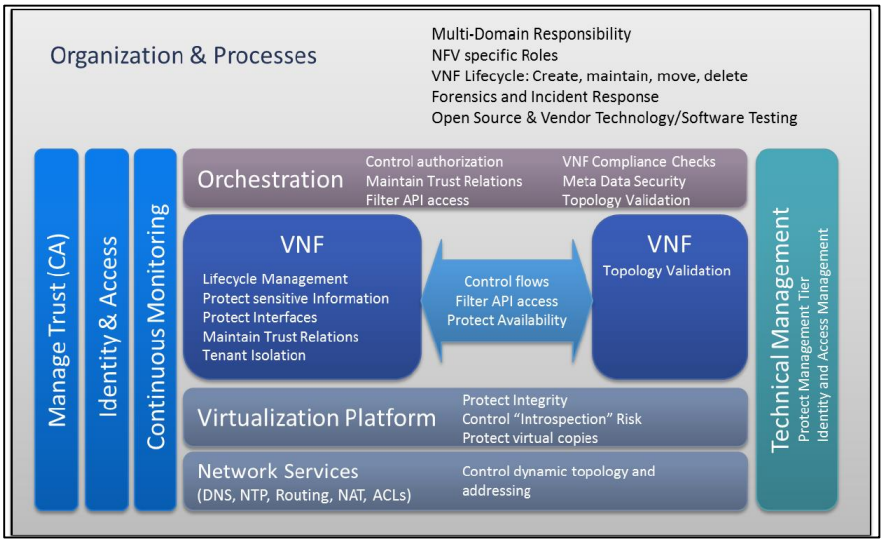


Figure 8.10: High Level View of NFV Security Framework Elements

8.3.5. ONF [Ref. dd, ee]

The Open Networking Foundation (ONF) is a user-driven organization dedicated to the promotion and adoption of Software through open standards development. ONF emphasizes an open, collaborative development process that is driven from the end-user perspective. The signature accomplishment to date is introducing the OpenFlow® Standard, which enables remote programming of the forwarding plane. The OpenFlow® Standard is the first SDN

standard and a vital element of an open software-defined network architecture. Its Technical Communities work on areas such as Carrier Grade SDN. The Services Area works on technical projects to enable applications and network operator services with SDN technologies. They include Architecture and Framework, Security, Layer 4-7 Services, Layer 4-7 Services and Information Modeling. The primary goal for the Security project is to carry out the analysis of security issues with SDN and so promote discussion of security considerations and recommendations relating to the protocols or any other proposals of ONF. Over time, this project will encourage the design/development of new security services and applications for SDN to deliver additional security functionality to systems, applications, and data.

8.3.6. Openstack [Ref. ff, gg]

The Telecommunications Working Group is working on use cases, such as VPN instantiation Chaining, Orchestration and SIP Load Balancing as a Service.

The goal of the Security Segregation use case is to present the need for a (partial) segregation of physical resources to support the well-known classic separation of DMZ and MZ, which is still needed by several applications (VNFs) and is requested by telco security rules. The main driver therefore is that a vulnerability of a single system must not affect further critical systems or endanger exposure of sensitive data. On the one side the benefits of virtualization and automation techniques are mandatory for telcos but on the other side telecommunication data and involved systems must be protected by the highest level of security and comply with local regulatory laws (which are often more strict in comparison with enterprise). Placement Zones should act as multiple lines of defense against a security breach. If a security breach happens in a placement zone, all other placement zones and related VNFs must not be affected. This must be ensured by the design. This use case affects all of the main OpenStack modules. The OpenStack Community has also published a comprehensive security guide for bolstering platform security.

As part of security hardening, Administrators can designate a group of compute hosts as trusted by using trusted compute pools. The trusted hosts use hardware-based security features, such as the Intel Trusted Execution Technology (TXT), to provide an additional level of security. Combined with an external stand-alone, web-based remote attestation server, cloud providers can ensure that the compute node runs only software with verified measurements and can ensure a secure cloud stack. Trusted compute pools provide the ability for cloud subscribers to request services run only on verified compute nodes.

The remote attestation server performs node verification like this:

- Compute nodes boot with Intel TXT technology enabled.

- The compute node BIOS, hypervisor, and operating system are measured.
- When the attestation server challenges the compute node, the measured data is sent to the attestation server.
- The attestation server verifies the measurements against a known good database to determine node trustworthiness.

The Open Attestation project describes how to implement an attestation service.

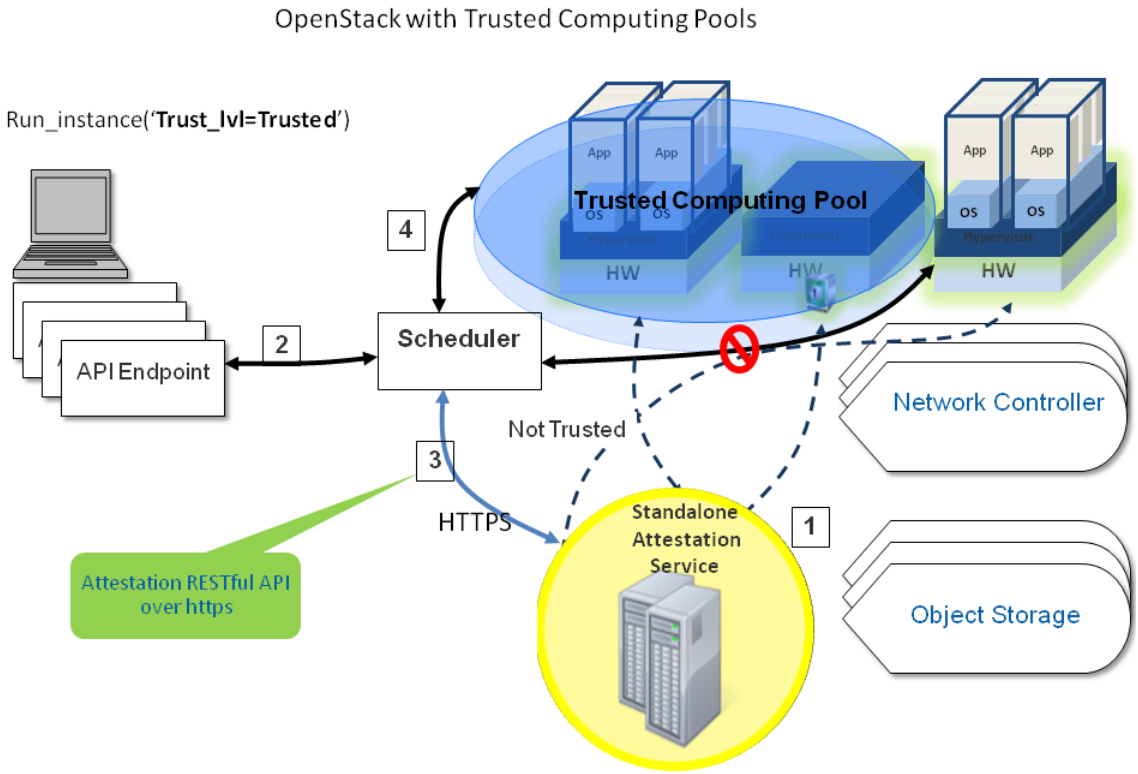


Figure 8.11: OpenStack with Trusted Computing Pools

8.3.7. Broadband Forum *[Ref. hh, ii]*

The Broadband Forum is the central organization driving broadband wireline solutions and empowering converged packet networks worldwide to better meet the needs of vendors,

service providers and their customers. It develops multi-service broadband packet networking specifications addressing interoperability, architecture and management. The work enables home, business and converged broadband services, encompassing customer, access and backbone networks. The forum is working on projects which leverage SDN / NFV architectures to revenue generating use cases. Five recently completed projects include SDN and NFV in Broadband Networks and Flexible Service Chaining and, projects in progress include Network Enhanced Residential & Virtual Business Gateway

8.3.8. Use of Open Source

A leading SP's (AT&T) perspective on Open Source are shown in Figure 8.12, 8.13 *[Ref. f]*

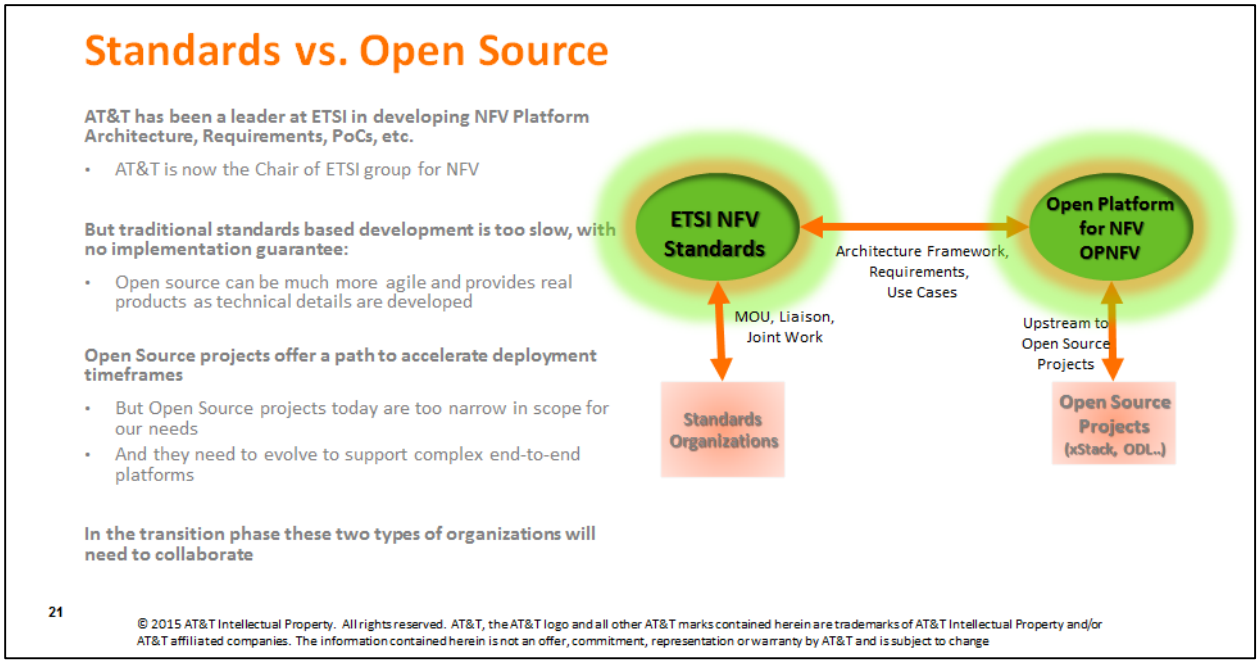


Figure 8.12 Standards vs. Open Source

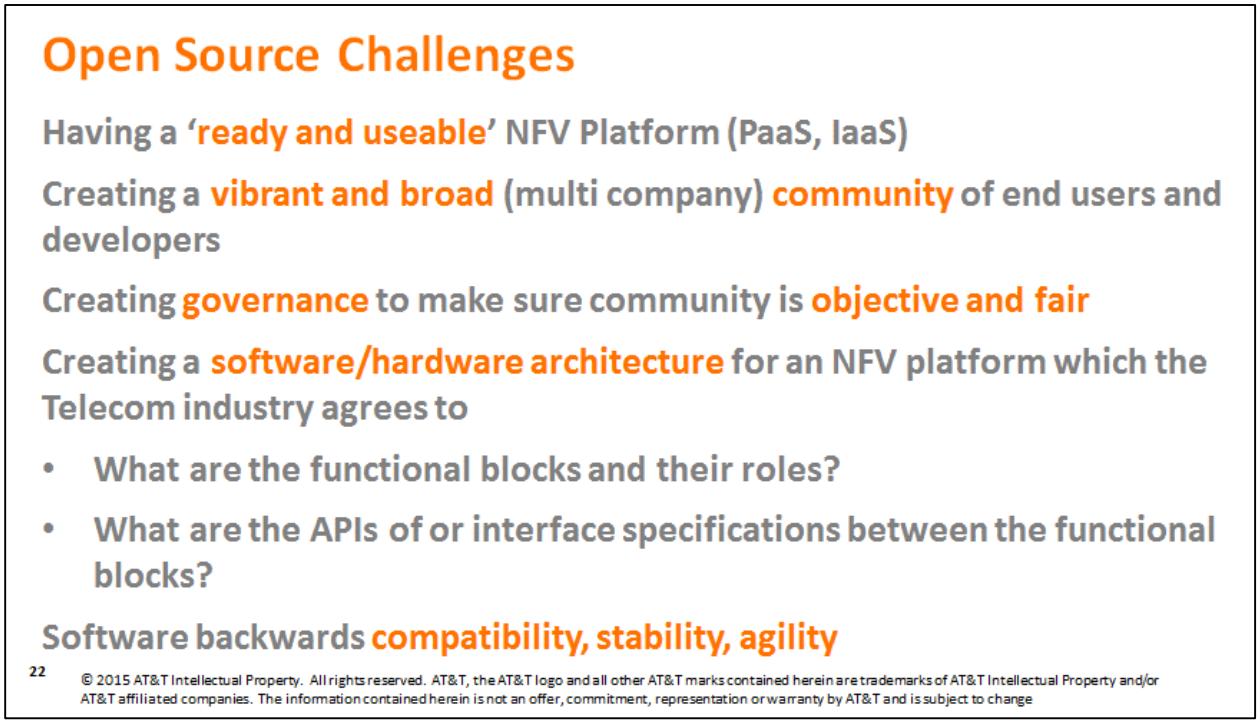


Figure 8.13 Open Source Challenges

8.4. Summary of Findings from Industry Landscape

Figure 8.14 shows the multiple layer aspects of security for the SDN / NFV environment. The tables provide a summary of challenges, Opportunities and possible security approaches to overcome. The blue block in the column SDN / NFV Attributes refers to layers in the Figure 8.14.

Multiple layers of security to protect Software Defined Network

1. Securing Controller
2. Securing Infrastructure
3. Securing Network Services
4. Securing Application
5. Securing Management & Orchestration
6. Securing API
7. Securing Communication
8. Security Technologies

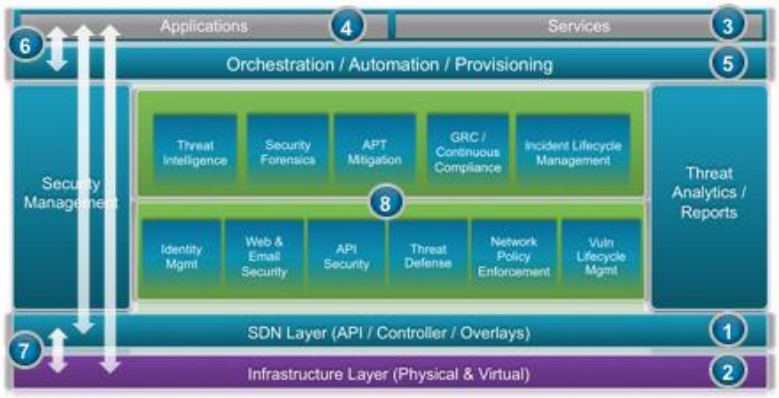


Figure 8.14 Multiple Layers of Security to protect SDN (Source: Mike Geller, Cisco)

SDN/NFV Attribute	Challenges	Opportunities	Possible security approaches
Logical centralization of Control 1. Controller 2. Infrastructure 3. securing network services	Single target of high value o successful attack can impact the entire network under control span of the controller. may be taken over by the attackers; o attack can come from devices, applications, into controllers or through communication channel o Resiliency and scaling challenges potentially impacting availability	o Centralization enables network level control and optimization resulting in: scalability, flexibility and cost savings. o Dynamic control of resources can enable flexible security architecture o Effective security measures for centralized networking assets.	Architecture options for Controller and underlying OS security: o Active / active, active / standby, clustering, geo-redundancy deployment alternatives available o Limited scope with federation may be possible o Network elements may be designed to operate with the last-good-state if controllers are down
Disaggregation - Separation of control and data planes 1. Controller 2. Infrastructure 4. Applications 5. Management & orchestration 6. API 7. Communications	Increases attack surface; o multiple devices need be protected; o communication channels and protocols must be secured o a compromised device may attack SDN controller o State of device security is non static; a compromised device may remain undetected o In Telemetry, compromised device may send false or fabricated data to the SDN controller; securing telemetry presents a significantly harder challenge*	o Each layer can scale and evolve independently; provides vendor independence to SPs.	Security for application s, underlying platform, orchestration, automation and Provisioning: o Clearly Define Security Dependencies and Trust Boundaries, Assure Robust Identity, Build Security based on Open Standards, Protect the Information Security Triad – Confidentiality, Integrity and Availability (CIA), Protect Operational Reference Data, Make Systems Secure by Default, Provide Accountability and Traceability

* Source: Dr. Kireeti Kompella, CTO, JDI, Juniper

SDN/NFV Attribute	Challenges	Opportunities	Possible security approaches
Abstraction - Programmability 1. Controller 2. Infrastructure 5. Management & orchestration, 8. Automation of Security Technologies	Abuse of control functions, exploiting vulnerabilities, compromising controllers. Semantic consistency between messages to a single device may be solvable; Semantic consistency between messages among multiple devices is harder to solve*	○ Facilitates deployment of agile, fine-grained security solutions running as applications and Software Defined Security approaches	Securing of all communication (Northbound, Southbound, East - West) channels and messages; Authentication between communicating entities, continuous attestation, not just at the time of spawning, of functions, audits and anomaly detection may be needed . Multiple layers of security would be needed
Multiple Trust Domains 1. Controller 2. Infrastructure, 5. Management, & orchestration 8. Automation of Security Technologies	New types of threats arise due to the explicit programmatic access SDN offers to clients that are typically separate organizational or business entities. Not unique to SDN is the fact that insiders represent a significant security threat, and that operator error threatens system integrity	○ Provides openness to allow customer self-service and different business models	Requires strong authentication and robust security at all interfaces. Should include strong identity and credential management functions that secure all entities and their associated state.

* Source: Dr. Kireeti Kompella, CTO, JDI, Juniper

SDN/NFV Attribute	Challenges	Opportunities	Possible security approaches
Virtual Network Functions (VNF) running in virtual machines and replace / supplement physical network functions 2. Infrastructure 3. securing network services 4. Applications 8. Security Technologies	Union of generic threats from virtualization / cloud, threats specific to previous physical network functions and new threats from the combination	Provides elastic capacity and automated provisioning. Service Chaining allows micro services to be properly sequenced to provide great flexibility and granularity and as and when needed; operating efficiencies and rapid service innovation. Recognizing the need for more holistic solution, Server / Endpoint security vendors are integrating with Network Security vendors by correlating network and server / endpoint threat data	Best Current practices of cloud (e.g. NIST, CSRIC, CSA, previous work of TAC) available. TPM and Virtual TPM for higher level of assurance. Trusted Computing practices start being used in commercial shipments ; expected to become more common in the future (e.g. Trusted Platform Module (TPM) chip on HP-UX Integrity servers, Intel Trusted Execution Technology (TXT), industry is also developing Virtual TPM for virtualized environment. It is not either network security or security embedded in hosts / servers; both are needed; significant work ongoing in ETSI – see GS NFV-Sec documents
Use of Open Source 8. Security Technologies	Being open source subject to attack	The more participants examine the code, the faster will the vulnerabilities be detected and fixed. Several vendors are enhancing Open Source and making them more rugged.	Carrier grade , including security, is work in progress in the various communities. Community is working on security areas (e.g. OpenStack Trusted Compute Pools); significant work ongoing in ETSI – see GS NFV-Sec documents

9. Gaps

SDN and NFV are both very young in terms of technological maturity. As such, the gaps that apply are best realized not as deficiencies in the technology, but more in the early stage development of operational use cases and deployments of the technology. The graphic below helps to characterize the gaps in securing SDN and NFV (Figure 9.1).

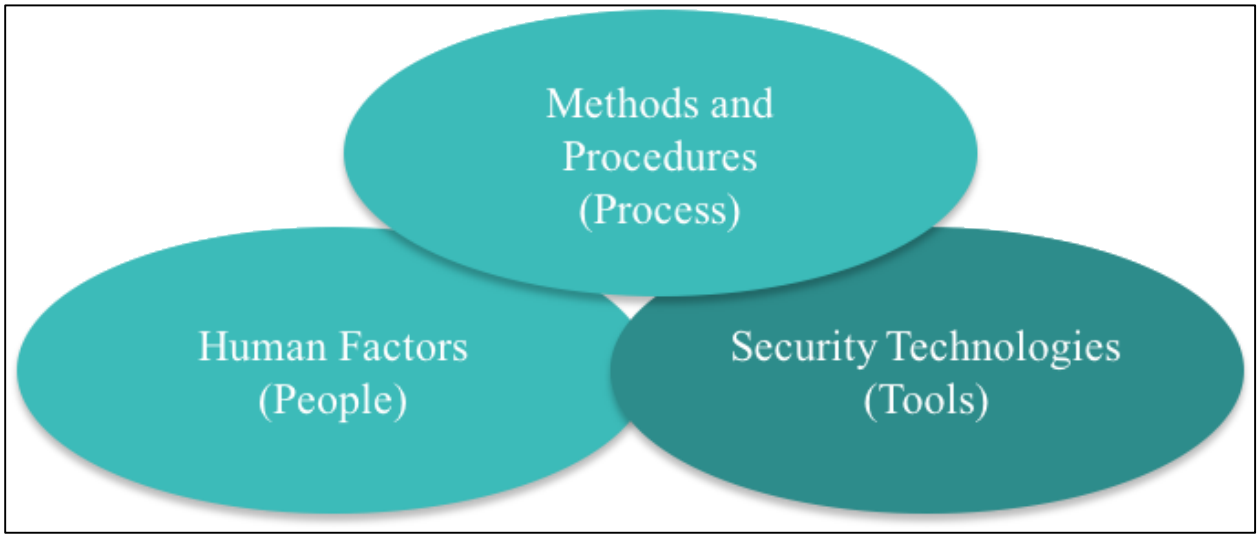


Figure 9.1 Gaps in Securing SDN and NFV

The industry gaps as they relate to SDN and NFV include, but are not limited to:

- Lack of standardization – good start but lots to do
- Lack of operational best common practices
- Lack of operationally mature use cases
- Lack of ability to deploy at scale demanded by today and tomorrow's requirements (IoT, Cloud Scale Applications…)
- Lack of operational resiliency and redundancy architectures
- Yet to be defined threat surface when SDN and NFV become a part of the "evolved" network – Some BCP (best common practices) in play today can be applied, but new and different threats and vulnerabilities certainly exist
- Trust and attestation of services, service chains, virtual network functions and services lack industry standard approaches
    - In the networks that have now become the foundation that SDN and NFV are added to in order to deliver today's applications, standard architecture and technology is applied to deliver "cryptographic trust" and the ability to attest to the veracity of the service (and its constituent elements). One aspect of this architecture is the use of a trusted platform module, sometimes referred to as a TPM. Many appliances and network hardware use a TPM for many functions in the trust chain, including storing and validating a cryptographic signature for the software running on the

system. The lack of a standard way to do this in the virtual space is an example of a GAP in today's SDN and NFV deployments.

- Once the service is running, there are various approaches to run time attestation. Run time attestation refers to the ability to verify that the originally deployed system (virtual or appliance based) is the originally provisioned system. In appliances or routers/switches, this is easier because the "service" operates in a box or a series of them connected using operationally accepted standard approaches. In the virtual space (where SDN and NFV live), there is a gap in the industry today in how run time attestation will work and to what level or layer in the architecture the operator will be able to attest when a standard based approach to do this arrives.

- The deployment of SDN and NFV services will, (some today, but much more in the future as "inter-cloud marketplaces" surface) in the very near future, require a cross domain identity capability, offering a single sign on experience, both to users and within the service chain. A cross domain trust model is a gap in today's deployments. As we move toward the ability to "trust" and "attest for" services in the virtual space, the need to extend the reach to cross domain services will come front and center.
- Figure 8.14 highlights an 8-layer approach to depict the threat surface of SDN & NFV. There are gaps at each layer that point to future work for the FCC and other organizations as SDN and NFV mature and operational standards and best practices are adopted. These important are detailed below:
  - Securing Controller, Securing Infrastructure & Securing Network Services
    - There are many well-known BCP (best common practice) that highlight how we secure the networks we run today. Given how young SDN and NFV are in terms of operational networks and services, those BCPs need to be properly connected to those that describe the SDN and NFV threats. That will naturally happen as more solutions with NFV and SDN are deployed. There are new threats when an SDN controller is deployed for network control. Questions like (gaps) "how do I secure for a rogue controller or a rogue endpoint" become very real concerns. Current and future deployments will guide us on how to evolve the best practices in question.
  - Securing Management and Orchestration
    - The management and orchestration layer is one that should be very closely examined. This is the layer that "spins" up the services to be deployed, connects them to the networks they run on and insures that all elements of the service chain are properly trusted. Many of these activities we've done for many years with traditional NMS systems, but here, we are expected to be a factor of ten times more agile. There is a gap in the industry today as to how to lock down a system (many different approaches today) that models the underlay network, models the service, and applies a customer

context to deliver the service and perhaps an additional context for threats. There are many new systems and components to secure and there is an equally challenging evolution of best common practices from existing NMS systems to fit the new world of virtualization, clouds, SDN and NFV.

- Securing API & Securing Application
  - Securing API is something that seems very straight forward, but cannot be overlooked as a major gap in the operation and security of networks that include SDN and NFV. There is an evolving set of technology and best practices to address securing the communication from one entity to another programmatically, but clearly standards are missing. The lack of BCPs and standard approaches make room for many different attacks regarding the communication over the API, security of the data itself, and the many threats resulting from unauthorized control of either of the entities that use the API to communicate.
- Securing Communication
  - Inter-layer or inter-process communications need to be secured. There is a gap in how this is done today, especially when it comes to securing communication in networks of the size and scale of "Internet of Things" deployments.
- Security Technologies
  - The security people, processes and tools continue to evolve. They have to in order to keep up with the fast paced evolution of business, regulatory and technical aspects of the services we deploy today and tomorrow. There will always be a gap between what we use today and what the people, processes and tools will protect going forward.

Every one of the gaps listed above is an opportunity. As an industry, we should continue to, via the FCC, grow consensus and use cases which include both SDN and NFV. The connection of a user running some app to a network transport to a cloud housing that app brings about a number of new trust boundaries that require very close attention. The graphic below highlights the relationships and trust boundaries driven by our team's focus on "Securing SDN and NFV." (Figure 9.2)

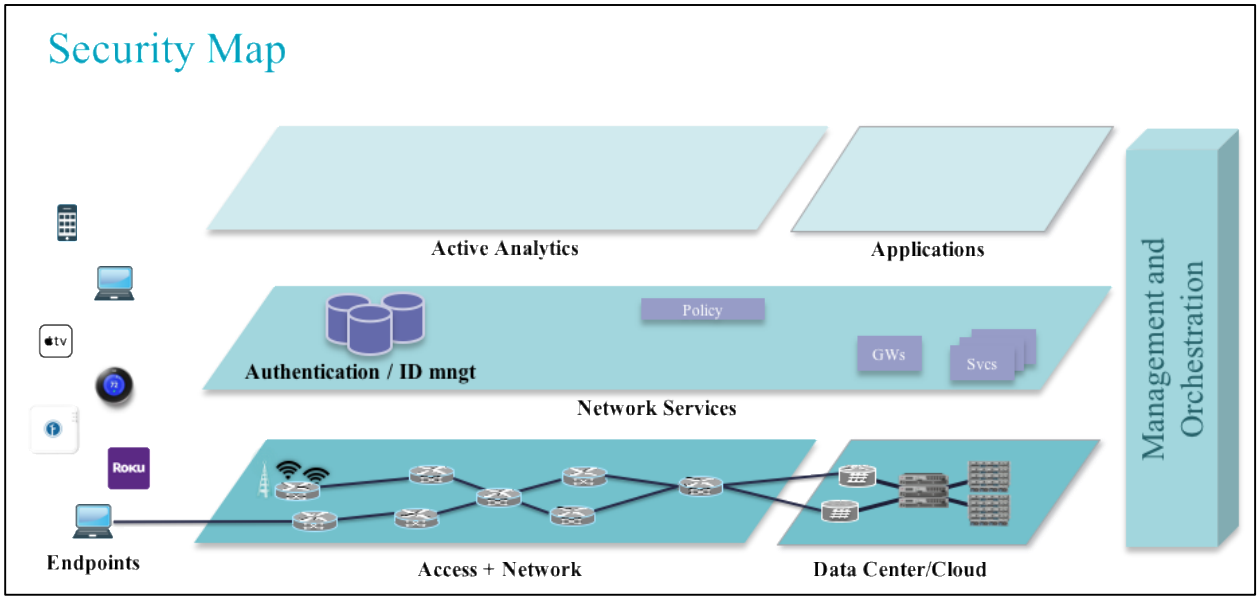


Figure 9.2 Relationships and Trust Boundaries

10. Summary

As described earlier in this WP, SDN / NFV is at an early stage of evolution and significant innovation is happening at a fast pace, open source playing a large role. So far, SDN has been deployed only in specific applications/ use cases such as data centers, WAN connecting data centers; All the more reason to build-in security now instead of trying to bolt onto a massive installed base like for previous control plane protocols. As industry gains more deployment experience supplemental security and new strategies may be needed beyond what has been learnt from building and operating existing networks.

Various segments of the industry are cognizant of the increased threats and challenges posed by these new architectures and opportunities to leverage these technologies to enhance security solutions. Communities are starting to work on security issues. CSA's recent position paper outlines challenges and opportunities, and security frameworks. Communities like ONOS and ODL, with the participation of industry players, are addressing these challenges. Approaches such as TPM (Trusted Platform Module), vTPM (virtual TPM), bidirectional authentication between applications, controllers and network elements, repeated measurement and attestation and multiple domains trust model are being developed to address existing gaps. Industry practitioners in their sessions with the SWG indicated that 1) standards are needed eventually to assure interoperability but rapid progress would be more likely achieved in open source communities on solutions for securing SDN NFV, and 2) such communities and SDOs have to work together.

11. Contributors

11.1. Ken Countway, Comcast

11.2. Brian Daly, AT&T

11.3. Martin Dolly, AT&T

11.4. Mike Geller, Cisco

11.5. Dr. Prakash Kolan, Samsung

11.6. Padma Krishnaswamy, FCC

11.7. Ahmed Lahjouji, FCC Liaison

11.8. Ramani Pandurangan, XO Communications (Lead)

11.9. Christoph Schuba, Ericsson

11.10. S Rao Vasireddy, Alcatel Lucent (Co-lead)

12. Consulted Industry Practitioners

12.1. Torsten Dinsing, “Virtualizing the Network”, Ericsson

12.2. Dr. Igor Faynberg , Dr. Hui-Lan Lu , Alcatel Lucent

12.3. Luke Hinds, Security Architect, Nokia, OPNFV Security Group Project, Team Lead

12.4. Deepak Manjal, HP

12.5. Alastair Johnson, Diego Garcia Del Rio and Furquan Haq, Alcatel Lucent

12.6. Dr. Dilip D. Kandlur, IBM

12.7. Mike Geller, Cisco

12.8. David Jorm, OpenDayLight

12.9. Dr. Kireeti Kompella, CTO, Juniper Development and Innovation, Juniper

12.10. Andrew Crawford, VP Service Provider Strategy, Brocade

12.11. Ed Lopez, VP Carrier Solutions, Fortinet

12.12. Prof. De Laat, University of Amsterdam, SARnet Principal Investigator

13. Abbreviations and Acronyms

A-CPI	Application-controller plane interface
ALU	Alcatel Lucent
API	Applications programming interface
BCP	Best Common Practice
BGP-LS	Border Gateway Protocol Link State
BIOS	Basic Input / Output System
BSS	Business Support System
CDN	Content Distribution Network
CLI	Command Language Interface
CORD	Central Office Reimagined as a Datacenter
CPE	Customer Premise Equipment
CPI	Controller plane interface
CSA	Cloud Security Alliance
CSP	Communication Service Providers
CSRIC	Communications Security, Reliability and Interoperability Council
D-CPI	Data-controller plane interface
DDOS	Distributed denial of service
DMZ	De Militarized Zone
DNS	Domain Name System
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FCAPS	Fault Configuration Accounting Performance Security
FGCT	Future Game Changing Technologies
HLR	Home Location Register
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystems
IRTF	Internet Research Task Force
ISG	Industry Specification Group
IS-IS	Intermediate System to Intermediate System
JASON	JavaScript Object Notation
LSO	Lifecycle Service Orchestration

MANO	Management and Network Orchestration
MD-SAL	Model-driven Service Abstraction Layer
MEF	Metro Ethernet Forum
MME	Mobility Management Entity
NE	Network Element
NETCONF	Network Configuration Protocol
NFaaS	Network Function as a Service
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVRG	NFV Research Group
ODL	Open DayLight
ONF	Open Networking Foundation
ONOS	Open Network Operating System
OPNFV	Open Platform for NFV Project
OSS	Operations Support System
OTT	Over The Top
PCEP	Path Computation Element Communication Protocol
PCRF	Policy and Charging Rules Function
PGW	Packet Data Network Gateway
POC	Proof Of Concept
RAN	Radio Access Network
REST	Representational State Transfer
SDN	Software Defined Networking
SDNRG	SDN Research Group
SDO	Standards Development Organization
SDSEC	Software Defined Security
SFC	Service Functions Chaining
SGW	Serving Gateway
SIP	Session Initiation Protocol
SLA	Service Level Assurance
SME	Subject Matter Expert
SWG	Sub Working Group
TAC	Technological Advisory Council
TPM	Trusted Platform Module
TXT	Trusted Execution Technology

vCDN	virtual CDN
VIM	Virtualized Infrastructure Management
VM	Virtual Machine
VNF	Virtual Network Function
VoD	Video on demand
VPN	Virtual Private Network
vTPM	virtual Trusted Platform Module
WAN	Wide Area Network
WG	Working Group
WP	White Paper
XMPP	Extensible Messaging and Presence Protocol

14. References

a. SDN architecture Issue 1 June, 2014 ONF TR-502, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf
b. Software Defined Networking: Should Do Now? Should Do Never? Simply Don't Know! By Jeff Roper, Chief Technology Officer, Entuity, http://entuity.com/resources/sdn-white-paper/
c. ETSI GS NFV 002 V1.1.1 (2013-10) Network Functions Virtualization (NFV); Architectural Framework, http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf
d. AT&T Vision Alignment Challenge Technology Survey, AT&T Domain 2.0 Vision White Paper, *November 13, 2013*
e. Regulations and possible Impact on NFV/SDN Technologies, presentation to Securing SDN SWG by Brian Daly, Martin Dolly, AT&T
f. AT&T's Domain 2.0 – SDN+Virtualization, Margaret T. Chiosi, AT&T Labs Distinguished Network Architect, Open Platform for NFV – OPNFV President (Linux Foundation), Network Function Virtualization – ETSI ISG Founding Member, presentation to Securing SDN SWG by Brian Daly, Martin Dolly, AT&T
g. ETSI http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf
h. GS NFV-SEC 001 V1.1.1 (2014-10) Network Functions Virtualization (NFV) NFV Security; Problem Statement
i. GS NFV-SEC 002 Network Functions Virtualization (NFV); NFV Security; Cataloguing security features in management software
j. GS NFV-SEC 003 V1.1.1 (2014-10) Network Functions Virtualization (NFV) NFV Security; Security and Trust 7Guidance
k. Webtorials The 2015 Guide to SDN and NFV http://www.webtorials.com/main/resource/papers/webtorials/2015-Guide-to-SDN-and-NFV/2015_Guide_Chapter_2.pdf
l. IETF 93 https://datatracker.ietf.org/meeting/93/agenda.html
m. IETF 94 https://datatracker.ietf.org/meeting/94/agenda.html
    i. SDN Threat Analysis, Haibin Song
    ii. Design and deployment of secure, robust, and resilient SDN Controllers, Sandra Scott-Hayward
    iii. Secure SDN Authentication, Hosnieh Rafiee
    iv. SDN Dependability: Assessment, Techniques, and Tools, Stenio Fernandes , Marcelo Santos

v. SDN Performance Monitoring, Klaus Wehmuth, Artur Ziviani
vi. A SDN Attestation Approach, Ludovic Jacquin, HP
vii. SDN Trust Models and Implementation Methodologies, Saurabh Chattopadhyay, Kaushik Datta, HCL Technologies ltd
viii. Building Blocks Towards a Trustworthy NFV Infrastructure, Adrian L. Shaw, , HP
ix. Investigating Intent API for Service Chaining, Andy Veitch NetCracker (NEC)
x. Gap Analysis on Network Virtualization Activities, draft-bernardos-nfvrg-gaps-network-virtualization-01
xi. Secure SDN Authentication & Authorization for Multi-tenancy
xii. VNF Pool Orchestration For Automated Resiliency in Service Chains
xiii. NFV Reliability using COTS Hardware

n. MEF, The Third Network: Lifecycle Service Orchestration Vision February 2015 https://www.mef.net/Assets/White_Papers/MEF_Third_Network_LSO_Vision_FINAL.pdf
o. 5G White Paper By NGMN Alliance version 1 17 February 2015 https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf
p. 5G Vision, The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf
q. Joint SDO/Fora Industry Harmonization for Unified Standards on Autonomic Management & Control of Networks and Services, SDN, NFV, E2E Orchestration, and Software-oriented enablers for 5G, http://www.euchina-fire.eu/wp-content/uploads/2015/06/Joint-SDOs_Harmonization_for_Unified_Standards_-AMC-E2Eorchestration_LSO-SDN-NFV_III.pdf
r. OpenDayLight Lithium , https://www.opendaylight.org/lithium
s. OpenDayLight use Cases, https:CSA SDN / NFV Position Paper//www.opendaylight.org/use-cases/
t. OpenDayLight CrossProject: OpenDayLight Security Analysis, https://wiki.opendaylight.org/view/CrossProject:OpenDayLight_Security_Analysis
u. OpenDayLight Controller: Architectural Framework, https://wiki.opendaylight.org/view/OpenDayLight_Controller:Architectural_Framework
v. OpenDayLight SDN Controller Platform (OSCP):Clustering, https://wiki.opendaylight.org/view/OpenDayLight_SDN_Controller_Platform_(OSCP):Clustering
w. OPNFV Technical Overview, https://www.opnfv.org/software/technical-overview
x. OPNFV Security Group, https://wiki.opnfv.org/security
y. ONOS Use Cases, https://wiki.onosproject.org/display/ONOS/Use+Cases
z. ONOS Security : Security-mode ONOS https://wiki.onosproject.org/display/ONOS10/ONOS+Security%3A+Security-mode+ONOS

aa. CSA, Software Defined Perimeter (SDP) Specification 1.0, April 2014, https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf
bb. CSA, Software Defined Perimeter, December 2013, https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf
cc. CSA, Security Position Paper for Network Function Virtualization, https://cloudsecurityalliance.org/document/network-functions-virtualization-position-paper/
dd. Open Networking Foundation, https://www.opennetworking.org/about/onf-overview
ee. Open Networking Foundation Service Areas, https://www.opennetworking.org/technical-communities/areas/services
ff. Openstack TelcoWorkingGroup / Use Cases https://wiki.openstack.org/wiki/TelcoWorkingGroup/UseCases
gg. Open Attestation, https://github.com/OpenAttestation/OpenAttestation
hh. Broadband Forum, https://www.broadband-forum.org/about/mission.php
ii. High-Value Services for Broadband Enabled by NFV and SDN , LightReading Webinar