Software Defined Networking (SDN) and Network Function Virtualisation (NFV) for Wi-Fi Network White Paper

Source: Wi-Fi Software Defined Networking & Network Function Virtualisation
Author: Wireless Broadband Alliance
Version: 1.0
Date: March 2016

Wireless
Broadband Alliance
Driving next generation Wi-Fi experience

About the Wireless Broadband Alliance

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to champion the development of the converged wireless broadband ecosystem through seamless, secure and interoperable unlicensed wireless broadband services for delivering outstanding user experience. Building on our heritage of NGH and carrier Wi-Fi, WBA will continue to drive and support the adoption of Next Gen Wi-Fi and other unlicensed wireless services across the entire public Wi-Fi ecosystem, including IoT, Big Data, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel. WBA member operators collectively serve more than 2 billion subscribers and operate more than 25 million hotspots globally.

The WBA Board includes AT&T, Boingo Wireless, BT, China Telecom, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO, Orange and Ruckus Wireless. For a complete list of current WBA members, please click here.

Follow Wireless Broadband Alliance at:
www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance
http://www.linkedin.com/groups?mostPopular=&gid=50482
https://plus.google.com/106744820987466669966/posts

Undertakings and Limitation of Liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement. In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organisations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

Contents

Figures

Executive Summary

Network Function Virtualisation (NFV) and Software Defined Network (SDN) provide the ability to separate the physical resources and switching function from the application and control function. This separation allows for the ability to program the behaviour and management of the network using well-defined interfaces.

For example, the use of Software Defined Network (SDN) in WLANs intends to bring tremendous OpEx improvements through offering Wi-Fi networks unprecedented programmability while reducing OpEx through highly automated orchestration and management by quick reaction to dynamic network condition and dynamic requirements. Moreover SDN maximizes ARPU by improved customer experience (such as low latency and high bandwidth) to those subscribers who are most willing to pay for those benefits.

At the same time, Network Function Virtualisation (NFV) in Wi-Fi network intends to move network functions like Access Controller, NAT, DPI, OAM, Firewall and so on so forth from the dedicated equipment to virtual machines running on generic hardware. The benefits for operators include:

- Efficient operation, maintenance and upgrade of network functions and service deployments
- Lowering CapEX by reducing need of dedicated telecom devices

This paper examines the usage of SDN and NFV in the deployment of Wi-Fi network providing use cases, an analysis of the state of the art, definition of requirements, architectures alternatives, challenges and gaps for the Wi-Fi network components.

This paper examines SDN and NFV in the following sections:

- Section 1 discusses the WBA motivation for developing this paper.
- Section 2 contains the definition of NFV and SDN
- Section 3 very briefly describes Carrier Wi-Fi considered as a reference architecture and which are the elements considered within the scope of this whitepaper.
- Section 4 introduces NFV and the standardization landscape.
- Section 5 introduces SDN and the standardization landscape.
- Section 6 describes the possible approaches and issue related to the introduction of SDN-based and NFV-based deployment of a Carrier Wi-Fi. At this stage of the work WBA does not intend to mandate any specific solution, but rather to identify the open issues, the gaps and, where it possible, the directions currently explored by other SDOs.
- Section 7 analyses the gaps and challenges
- Section 8 suggests actions to be taken in WBA.
- The Appendix further describes more of work done in some specific SDOs.

The whitepaper represents the first contribution of WBA to the SDN and NFV discussion describing the standardisation landscape and presenting some issues and deployment options without the intention to be exhaustive and to recommend any specific solution. The WBA effort points out the ways in which SDN and NFV are representing an important topic and a possible turning point in the evolution of telecommunications. However, it's important to remember that the Wi-Fi network is only one small part in the overall discussion, despite the fact that it is one of the most common means for connecting to today's networks, (via Smartphones, tablets, laptops, and other Wi-Fi enabled devices).

NFV and SDN provide tremendous opportunities to automate the life cycle management (LCM), service installation, and service mobility; however, these new technologies bring several challenges in the area of integration of the virtualized and non-virtualized management systems, security, and further standardisation work related to the integration between NFV and SDN. Furthermore, alternative approaches have been proposed in several areas. As the standardisation landscape shows with different players acting in NFV and SDN areas, although there is the risk of fragmentation, this represents an opportunity given by dynamic ecosystems.

1. Introduction

This whitepaper address the following issues:

- Identify the current common Wi-Fi network architecture
- Define NFV and SDN in the context of this whitepaper
- Identify the standards and examples of market deployment of NFV architecture framework
- Identify the standards and examples of market deployment of SDN architecture framework
- Identify the factors in existing architecture that influence the deployment of functions based on the NFV framework in centralized or decentralized scenarios and using the SDN framework
- Identify the gaps and recommendations, if any

2. Definitions

Network functions virtualization (NFV): principle of separating network functions from the hardware they run on by using virtual hardware abstraction [1].

Software defined networking (SDN): a set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner [2].

3. Wi-Fi Network Architecture

Over the years, WBA has put great effort into defining the requirements, architecture and features for Wi-Fi networks deployed by operators. In particular, WBA with the Next-Generation Hotspot (NGH) program enables the operator to deploy Wi-Fi networks which provide a better user experience. In such context, the NGH trial phase 3 [3][4] defines new features and will test them in the “real world”. In addition, the support of WRIX [5] enables roaming between operators and it further improves the user experience and the operator benefits from the deployment of a Wi-Fi network. Currently four classes of tier are defined within the Interoperability Compliance Program [6], including Carrier Wi-Fi requirements. The Carrier Wi-Fi guideline document [7] provides a step forward to Wi-Fi networks from the user experience point of view and from the operator point of view. Carrier Wi-Fi will be the starting point for considering the introduction of the NFV and SDN concept in Wi-Fi network.

The high-level logical architectures for the Carrier Wi-Fi network is shown in Figure 3-1, comprised of the following logical components:

- the AP complex, which may include only APs, or APs and ACs;
- the CWLAN Network Management System (CWLAN NMS), which provides configuration, fault and performance management for each CWLAN network element;
- CWLAN Service Servers (CWLAN SS), which is an application layer Service Server, such as a Wi-Fi Self Organizing Network (SON) system;
- Authentication, Authorization and Accounting (AAA) elements, which perform user authentication and performs accounting.

A Wi-Fi network , in order to be considered as a Carrier Wi-Fi for network selection and discovery, shall support WFA Passpoint™, [8] and consequently the Wi-Fi network shall support an additional set of server functionalities:

- Policy Server which provides the Passpoint profile to the user device;
- Remediation Server which provides the remediation of the subscription when it is detected to be no longer valid, e.g. when it is expired;
- OSU server which provides the capability for performing the online-signup registration from a Wi-Fi network;
- Certification Authority which provide authentication for the X.509 certificates when TTLS authentication is used;

- ANQP server which provides the configuration of the information to be transmitted in ANQP messages.

The server functionalities may be physically integrated within one of more servers depending on the deployment option.

The Wi-Fi network can be deployed in 2 scenarios: in the first one, autonomous APs are used without the presence of WLAN Access Controllers (AC) and the APs communicate with the WLAN NMS and the AAA servers; in the second, all APs are managed by ACs which communicate with the WLAN NMS and AAA servers. Other deployments are also possible, such as a combination of the two scenarios.

The WLAN AC is a network element of the Wi-Fi network which is not standardized, but it is commonly deployed in order to provide several control functionalities such as AP provisioning and OAM functions. It acts as RADIUS client interface to the AAA and generates usage based accounting information. The WLAN AC also acts as a Gateway for the data traffic implementing L2 tunneling, for example implementing different VLAN for different SSID, or performs IP routing functionalities. The protocol between the AP and the WLAN AC is generally vendor specific, and may be for example CAPWAP. The WLAN AC can be considered somehow transparent in respect to the UE and the other network elements, such as AAA server, Policy server, etc., shown in Figure 3-1. In the context of the SDN and NFV whitepaper the WLAN AC can be automatically identified with the SDN Controller, as described in the paper.

The requirements for the Carrier Wi-Fi network are defined in [7], so for more details refer to the guideline document.

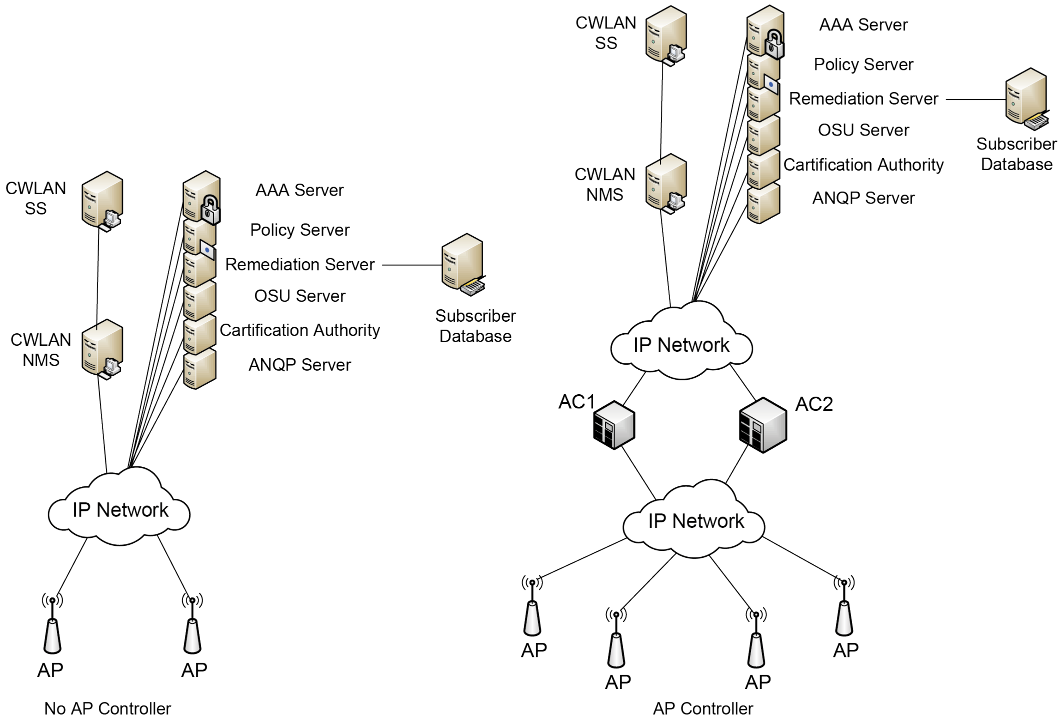


Figure 3-1 CWLAN Logical Network Architectures

The network elements part of Carrier Wi-Fi can be classified in the following categories:

a. Network function element: This category is composed by network elements that perform actions on the user plane based on interactions (e.g. instructions, requests, etc.) received by other networks via the control plane. Examples of network functions are the Wi-Fi Access point, WLAN Gateway, the router and switches.

b. IP functional element: This category is composed by network elements consuming or generating the information exchanged via user plane or interacting with the user plane. Examples of IP functional elements are the applications (video application, Voice application, data, games, etc.), the IMS service, the firewall, proxy etc.
c. Server: this category is composed of network elements which control the user and network behavior implementing only the control plane. Examples of servers are the AAA server, charging system, management, etc.;

Carrier Wi-Fi is not only composed, as we described by the Wi-Fi Access point, but from a wide set of elements, all of them are needed to provide services and applications to the end user, and the WBA operator may deploy several or only a few of them. The scope of this whitepaper is not to consider the overall network and all possible network elements which may be deployed by an operator, but to be focused on whether the virtualisation and SDN can be applied to the network elements considered under WBA scope.

In the whitepaper the applicability of NFV and SDN to the IP functional element will be not considered, since they are independent of the WLAN, however the relationship with the network element parts of Carrier Wi-Fi network will be taken into account.

The network function elements include the equipment listed below as part of Carrier Wi-Fi and so they are considered within the scope of the whitepaper:

- WLAN AP
- WLAN Gateway

At this stage, two network function elements play an essential role: the router and the switch. They are essential in making Carrier Wi-Fi a network, but they are not in the scope of WBA since they are not specific to the wireless network. For this reason, they will be taken into consideration in the analysis, bearing in mind that their standardization applying NFV and SDN is under the responsibility of other SDOs. Hence, only the issues related with interaction and integration within a Carrier Wi-Fi network will be considered.

The Server includes the essential element listed in the following which are considered within the scope of whitepaper:

- AAA proxy and AAA server (for authentication , authorization and accounting)
- ANQP server, OSU server and Remediation for the support of Passpoint
- Management server
- Passpoint Policy server
- Access Controller

The interworking scenario with 3GPP is not considered within the scope of the whitepaper and so the 3GPP network elements are considered outside of the scope of the whitepaper.

The Community Wi-Fi scenario is not considered within the scope of the whitepaper, since Broadband Forum is currently working on the migration of Fixed Broadband Network to NFV (WT-359 [9],WT-345 [10], WT-328 [11]) and SDN (SD-365 [12], WT-358 [13]), but this work is not yet concluded.

4. Introduction to NFV

Over the last decade, Wi-Fi networks have experienced a significant evolution with the emergence of new technologies and services which mainly enhance user experience and improve quality of service. Nevertheless, today's Wi-Fi networks are unable to rapidly adapt to such evolutions due to their rigid architectural design. In fact, this typically requires time-consuming and costly upgrades of existing infrastructure generally composed of proprietary hardware appliances. Consequently, the issue of implementing flexible architecture while boosting innovation and reducing the cost of network upgrades becomes a major concern to support evolving contexts and service needs.

Network Function Virtualization is an emerging industry trend which addresses such kind of challenges and brings many benefits to network operators.

4.1 NFV principles

NFV leverages standard IT virtualization technology to consolidate many network functions, which traditionally reside in purpose-built equipment, onto industry standard server hardware which could be located in data centers, network nodes and in the end user premises.

Due to its basic idea of decoupling software from hardware, it promises cost efficient realization of network functions in software deployed over commodity hardware, which can be instantiated in, or moved to, various locations in the network as required. Moreover, it encourages openness and innovation to quickly bring new services and new revenue streams at a much lower risk.

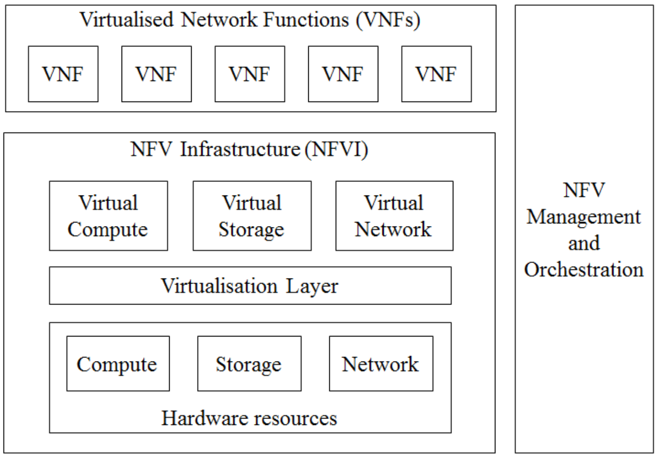


Figure 4-1 High level NFV framework

Figure 4-1 illustrates the high-level NFV framework that is composed of three main working domains:

- NFV Infrastructure (NFVI), including all the physical resources (i.e., compute, storage and network resources) and how these can be virtualized to support the execution of multiple VNFs and provide a multi-tenant infrastructure.
- Virtualized Network Function (VNF), the software implementation of a network function which is capable of running over the NFVI. VNFs may be dynamically deployed on the NFVI on demand within the capacity limits of the NFVI nodes.
- NFV Management and Orchestration, which covers the orchestration and lifecycle management of network functions, and the management of physical resources. This includes end-to-end network service mapping, VNF instantiation at appropriate location, hardware resource allocation and scaling, performance measurements, etc.

4.2 NFV standardisation landscape

4.2.1 ETSI

An ETSI Industry Specification Group (ISG) for NFV was created in November 2012 by seven of the world's leading telecoms network operators. It now consists of over 270 companies which are working to develop the required standards for Network Function Virtualisation and to set the direction for NFV implementation and deployment in an open and interoperable ecosystem [14].

NFV ISG has published a set of specifications related to different technical aspects such as architectural framework, use cases, infrastructure, management and orchestration, security, resiliency, and performance and portability. Moreover, an NFV Proof of Concept (PoC) framework has been developed to promote multi-vendor PoCs illustrating key aspects of NFV and to encourage the development of a diverse and open NFV ecosystem. 38 PoCs have been developed and their findings and lessons learnt are fed back to the NFV ISG to help the progress of specification work [15].

One of the main focuses of NFV ISG is the NFV Management and Orchestration (NFV-MANO) [16] that provides higher levels of automation for the provisioning and configuration of virtualized network functions. Such functionalities are necessary now because of the decoupling of the network functions software from the NFVI. The NFV-MANO framework is based on the NFV reference architectural framework depicted in Figure 4-2, further detailing the functionality of three key functional blocks:

- Virtualised Infrastructure Manager (VIM), which controls and manages NFVI compute, storage and network resources within a domain.
- VNF Manager (VNFM), which is responsible for VNF lifecycle management (e.g. instantiation, update, scaling, termination). The VNFM interacts with the Element Manager (EM) and the VNF for provisioning, configuration, and fault and alarm management.
- NFV Orchestrator (NFVO), which performs orchestration functions of NFVI resources across multiple VIMs and lifecycle management of network services. The NFVO interacts with the OSS/BSS for provisioning, configuration, capacity management, and policy-based management.

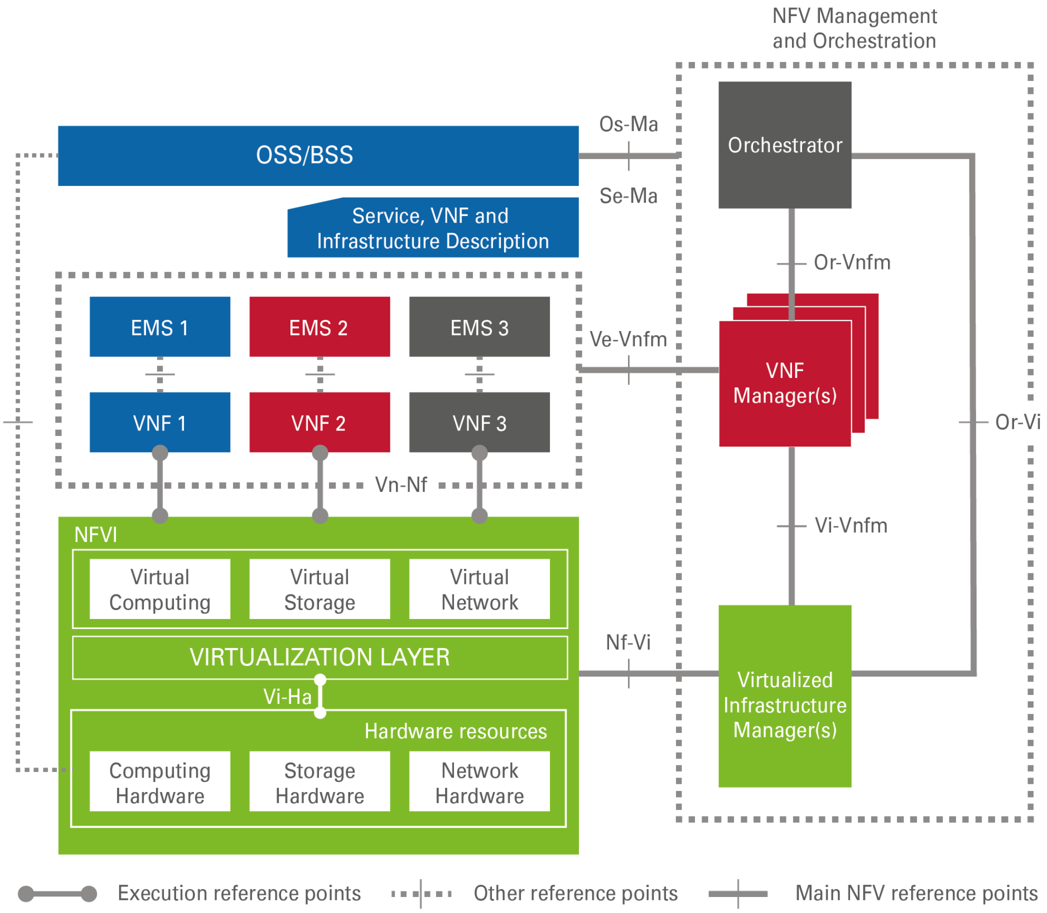


Figure 4-2 NFV reference architectural framework

4.2.2 3GPP

In March 2014, the 3GPP Telecom Management working group (SA5) issued a liaison statement towards the ETSI NFV ISG to inform them that this working group will produce a Study Item TR 32.842 [17] on the management of virtualised 3GPP network functions. It includes the description of use cases, potential requirements, potential solutions, recommendations on future normative work on the subject, and gap analysis with ETSI NFV specification. The TR 32.842 has been completed and SA5 started at the end of 2016 the normative work for mobile networks that include virtualized network functions in TS 28.500 [18] defining the architectural, concept and requirements, in TS 28.510 [19] the configuration Management, in TS 28.515 [20] the Fault Management, in TS 28.520 [21] the Performance management and in TS 28.525 [22] the Lifecycle management.

4.2.3 IETF/ IRTF

Under the umbrella of the Internet Research Task Force (IRTF), which deals primarily with long term research issues related to the Internet, a new Network Function Virtualization Research Group (NFVRG) was chartered in January 2015 [23]. This group will focus on research problems associated with NFV-related topics and aim to bring together a research community in both academia and industry to address them. As near-term work items, the NFVRG will focus on policy-based resource management, analytics for visibility and orchestration, Virtual Network Function (VNF) performance modelling to facilitate transition to NFV, and service verification with regards to security and resiliency.

There are also some IETF working groups that deal with topics related to NFV or are impacted by NFV concepts and mechanisms. Among these groups there are Service Function Chaining (SFC), Network Virtualization Overlays (NVO3), BGP (Border Gateway Protocol) Enabled Services (BESS), Traffic Engineering Architecture and Signaling (TEAS), .

SFC: Service Function Chaining [24]

User services consist of multi-tiered service functions (e.g., packet filtering, load-balancing, deep packet inspection) that are deployed at different points within a network. Delivery of these types of services is undergoing significant change with the introduction of virtualization, network overlays, and orchestration. Thus, there is a need to move to a different model, where service functions, whether physical or virtualized, are not required to reside on the direct data path and traffic is instead steered through required service functions, wherever they are deployed.

For a given service, the abstract view of the required service functions and the order in which they are to be applied is called a Service Function Chain (SFC). An SFC is instantiated through selection of specific service function instances on specific network nodes to form a service graph: this is called a Service Function Path (SFP).

The SFC working group will specify a new approach to service delivery and operation. It will produce an architecture for service function chaining that includes the necessary protocols to convey the SFC and SFP information to nodes that are involved in the implementation of Service Function Chains, as well as mechanisms for steering traffic through service functions.

The outcome of this working group can be applied on NFV environments as this involves Virtual Network Functions (VNFs), which could be located in different places in the network (e.g., data centers, network nodes, end-user premises) and must interwork with physical network appliances to deliver an end-to-end service according to a VNF Forwarding Graph (analogous to SFP mentioned above).

NVO3: Network Virtualization Overlays

NVO3 working group aims to develop a set of protocols that enable network virtualization with multi-tenancy and workload mobility within a data center (DC) environment that assumes an IP-based underlay [25].

Some of the specific approaches developed in this working group (e.g. overlays, traffic isolation, VM migration) could be extended outside the DC and applied to NFV environments.

BESS: BGP Enabled Services

One of the goals of the BESS working group is to extend BGP-enabled VPN solutions for the construction of virtual topologies in support of services such as Service Function Chaining [26]. This is the most relevant activity in the BESS that could be relevant in NFV context.

TEAS: Traffic Engineering Architecture and Signalling

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-administration, multi-vendor, multi-technology networks and to operate, control, and manage these multiple networks as if a single virtualized network. Another dimension of virtual network operation is the use of common core transport network resources by multi-tenant service networks as a way of providing a virtualized infrastructure to flexibly offer new services and applications.

Within the TEAS WG, a work effort, called Abstraction and Control of Transport Networks (ACTN) [27], is being carried out that investigates this problem space. Several use cases involved in ACTN are relevant to NFV such as “multi-tenant virtual network operators” and “mobile virtual network operation for multiple domains in a single operator network”.

VNFpool BoF

VNFpool is working on the way to group Virtual Network Functions (VNFs) of the same type into pools to improve reliability and availability by implementing stateful failover among VNF pool members and enabling scaling-out and scaling-in of VNFs within a VNF pool.

The VNFpool BoF started work on charter and use cases (e.g. vEPC, vCDN, Load balancing). However, there is no remarkable activity since July 2014.

4.2.4 DMTF

The Distributed Management Task Force (DMTF) developed Open Virtualization Format (OVF) specification to describe the packaging and distribution of software to be run in a virtual machine. This is one of the open standards that the ETSI NFV ISG is considering as part of the interface between the higher level orchestration layers and the virtualized infrastructure manager.

4.2.5 OASIS

OASIS (Advancing Open Standards for the Information Society) Topology and Orchestration Specification for Cloud Applications (TOSCA) Technical Committee announced his growing interest in NFV and recently formed a workgroup focused on creating a “TOSCA Simple Profile for NFV” [28]. This profile specifies a NFV specific data model using TOSCA language.

4.2.6 BBF

The Broadband Forum (BBF) has a formal liaison relationship with ETSI and is collaborating with the ETSI NFV ISG. The collaboration aims to achieve a consistent approach and common architecture for the infrastructure needed to support virtualized network functions, and will help to promote implementation of NFV solutions.

Many activities related to NFV are being standardised standardisation in BBF, such as:

- WT-345 [29] documents a set of architectures for broadband multi-service network, addressing infrastructures, topologies and deployment scenarios for Multi-Service Broadband Network Gateway (MS-BNG) with hierarchical instances realized as Virtualized Network Functions (VNF).
- WT-359 [30] establishes a framework to permit the Broadband Forum to effectively reference and specify systems, such that the deployment of NFV (as defined by the ETSI NFV ISG), in Broadband Forum specified networks is facilitated.
- WT-328 [31] specifies the virtual business gateway architecture as well as the user cases and deployment scenarios. The virtual business gateway architecture describes the migration of functionalities running on a BNG to the network service provider’s infrastructure for enabling network-based features and services.
- WT-317 [32] specifies the Network Enhanced Residential Gateway (NERG) architecture that consists of shifting some of the functionalities of a residential gateway to the operator’s network, for enabling network based features. This architecture involves partial virtualisation of Residential Gateway (RG) functions. Figure 4-3 depicts the NERG functional architecture where functions such as IP forwarding, routing, NAT and IP addressing related functions are located on the virtual Residential Gateway (vRG) and the forwarding plane of the gateway is configured in bridge mode and located on the Bridged Residential Gateway (BRG). The latter is located at the residential customer premise while the vRG could be located on the Access Node (AN), on the Broadband Network Gateway (BNG), or even in the Cloud.

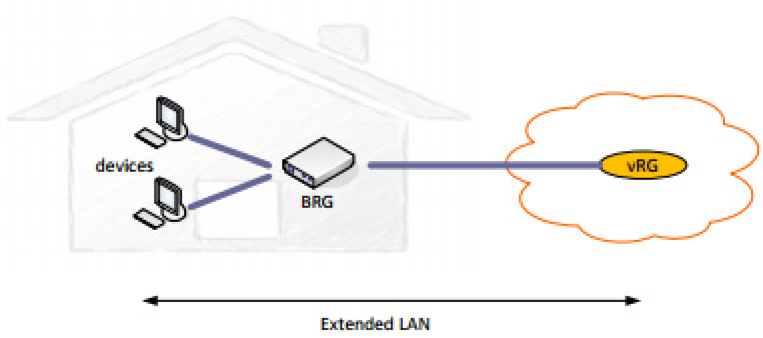


Figure 4-3 Basic NERG Functional Architecture

The finalized study documents are:

- SD-340 [33] includes 11 use cases, service provider requirements as well as recommendations of next step migration work for other work channels of the Forum.
- SD-326 [34] Flexible Service Chaining: studies the market requirements and use cases and identification of gaps for supporting Flexible Service Chaining.

4.2.7 ATIS NFV Forum[1]

Alliance for Telecommunications Industry Solutions (ATIS) ATIS has launched the NFV Forum to engage the industry in important contributions to network function virtualization and software defined networking – part of a sweeping evolution that is moving the ICT industry from integrated, hardware-centric solutions to modular, hardware-agnostic frameworks by abstracting the hardware resources into a consistent operating environment for the software. The NFV Forum focuses on the inter-domain aspects for NFV environments based on the ETSI MANO architecture [35]. The NFV forum completed the NFV Use Cases document that emphasizes the benefits of NFV in a multi-administrative domain [36]. The ATIS NFV forum is currently focused on creating an architecture and requirements document, along with an inter-administrative domain catalogue specification. The text and figure below captures the current work in progress and are subject to change.

Multi-administrative domain use cases may include multiple producer and multiple consumer administrative domains. Specifically, a consumer administrative domain can utilize service functions in one or more producer administrative domains. Similarly, a producer administrative domain may offer service functions to multiple consumer administrative domains. To simplify these relationships, we model these cases as a pairwise combination of one consumer and one producer administrative domain. This model can be scaled appropriately to address most multi-domain scenarios.

Figure 4-4 shows the architecture of a pairwise consumer/producer use case. Each administrative domain implements network functions, services and applications within a virtualization environment. Although we commonly assume the virtual environment based on ETSI NFV, the interfaces and procedures between the administrative domains can apply to any suitable virtualization environment.

[1] Only documents that are final/approved by an ATIS Committee represent the consensus of that Committee. Draft documents, on the other hand, are dynamic in nature and subject to change. Draft documents therefore may not accurately reflect the consensus of the ATIS Committee. Neither ATIS nor the Committee makes any representation or warranty, express or implied, with respect to the sufficiency, accuracy or utility of the information or opinion contained or reflected in the material utilized. ATIS further expressly advises that any use of or reliance upon the material in question is at your risk and neither ATIS nor the Committee shall be liable for any damage or injury, of whatever nature, incurred by any person arising out of any utilization of the material. It is possible that this material will at some future date be included in a copyrighted work by ATIS.

The Service Management Gateway abstracts the details associated with the virtualization environment from the interface between the two administrative domains. The Service Management Gateway in the producer administrative domain:

- Advertises and exposes the service function catalogue of the producer administrative domain to potential consumer administrative domains
- Enables a consumer administrative domain, based on policies, to select one or more service functions from the service function catalogue
- Supports service function activation for the selected service functions
- Enables the consumer administrative domain to provide configuration and service life cycle management functions as defined by the service function catalogue.

The Service Management Gateway in the consumer administrative domain enables the consumer administrative domain to:

- View the service function catalogue of producer administrative domains
- Select one or more service functions within the catalogue
- Activate selected service function(s)
- Provide configuration and service life cycle management directives as allowed by the service function catalogue

The Service Management Gateways communicate via the IAD-S interface. The IAD-S interface provides a secure interface between administrative domains to support the above named functions.

The IAD-O interface exists between administrative domains to support the exchange of fault and performance data to allow the consumer administrative domain to monitor reliability and performance aspects of the selected service functions. Information exchanged over this interface supports service level agreement (SLA) compliance for the selected service functions and may also be used to invoke service life cycle management functions that may (for example) increase or decrease the capacity of the specific service functions.

The IAD-CD interface represents service specific control and data interfaces required to support the selected service functions. Since this interface or set of interfaces is service function specific, the IAD-CD interface is not specifically defined. However, information required to establish, monitor and tear down service function specific interfaces must be included in the service function catalogue.

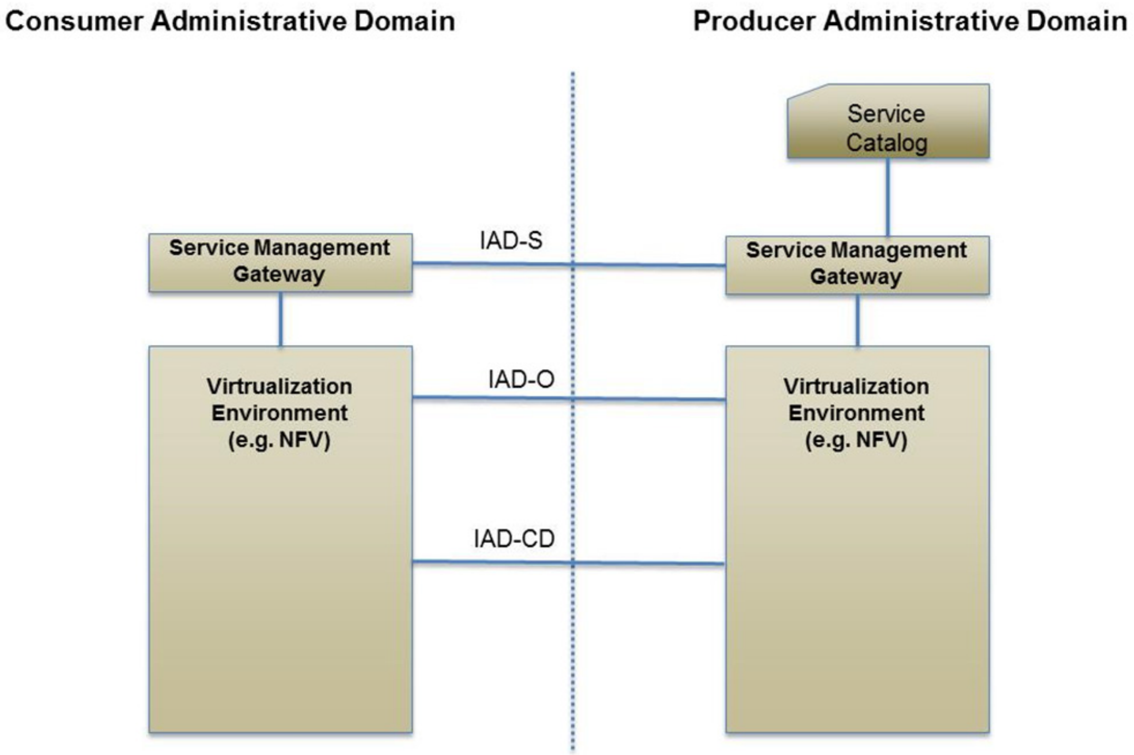

Consumer Administrative Domain
Producer Administrative Domain
Service Catalog
Service Management Gateway
Service Management Gateway
IAD-S
Virtrualization Environment (e.g. NFV)
Virtrualization Environment (e.g. NFV)
IAD-O
IAD-CD

Figure 4-4 ATIS Inter Administrative Domain Architecture

4.2.8 IEEE

Among IEEE standardisation activities, there is a number of new initiatives forming part of the “Software Defined and Virtualized” standardization program.

Study Group on “Security, Reliability, and Performance for Software Defined and Virtualized Ecosystems” (SRPSDVE) [37]:
This Study Group aims to identify primary standards development opportunities in the reliability, performance, and security aspects of SDN and NFV. The primary objective of this SG is to assess whether there is an opportunity for the IEEE to launch a standardization activity in this area and thus prepare a PAR to launch the official standardization process.

Research Group on “Software Defined and Virtualized Wireless Access” [38]:
The objective of this Research Group is to identify and address the research issues that need to be solved and assess the feasibility of launching an IEEE standardization effort on Software Defined and Virtualized Wireless Access. A recent article [39] based on the activities developed under this Research Group was published in IEEE Communications Magazine which provides an overview of the perspectives of using the software defined network paradigm at the service of the future wireless access networks, including both 5G mobile technologies and wireless local area networks.

Research Group on “SDN/NFV—Structured Abstractions” [40]:
The aim of this Research Group is to identify and formulate possible IEEE standardization efforts to define a high-level taxonomy and structure that represent the network and its functions.

4.2.9 Open Source project: OPNFV

Open Network Function Virtualization (OPNFV) [41] is an open source project formed under the Linux Foundation. This project aims to advance the evolution of NFV and accelerate the introduction of new NFV products and services through a carrier-grade, integrated, open platform.

OPNFV is considered as a complementary community to existing standards and open source bodies with a clear focus on the coordination of software development, integration and testing, documentation and API development for NFV. Particularly, OPNFV is relying on ETSI NFV ISG specifications and collaborating with open source communities (e.g., OpenStack, OpenDaylight) to achieve an industry wide NFV reference platform.

As an initial release, OPNFV will focus on the NFV Infrastructure layer by developing the two functional blocks, the Virtualization Infrastructure (NFVI) and the Virtualized Infrastructure Management (VIM) as referred to in the NFV ISG architectural framework (Figure 4-5). For this purpose, OPNFV will integrate 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.

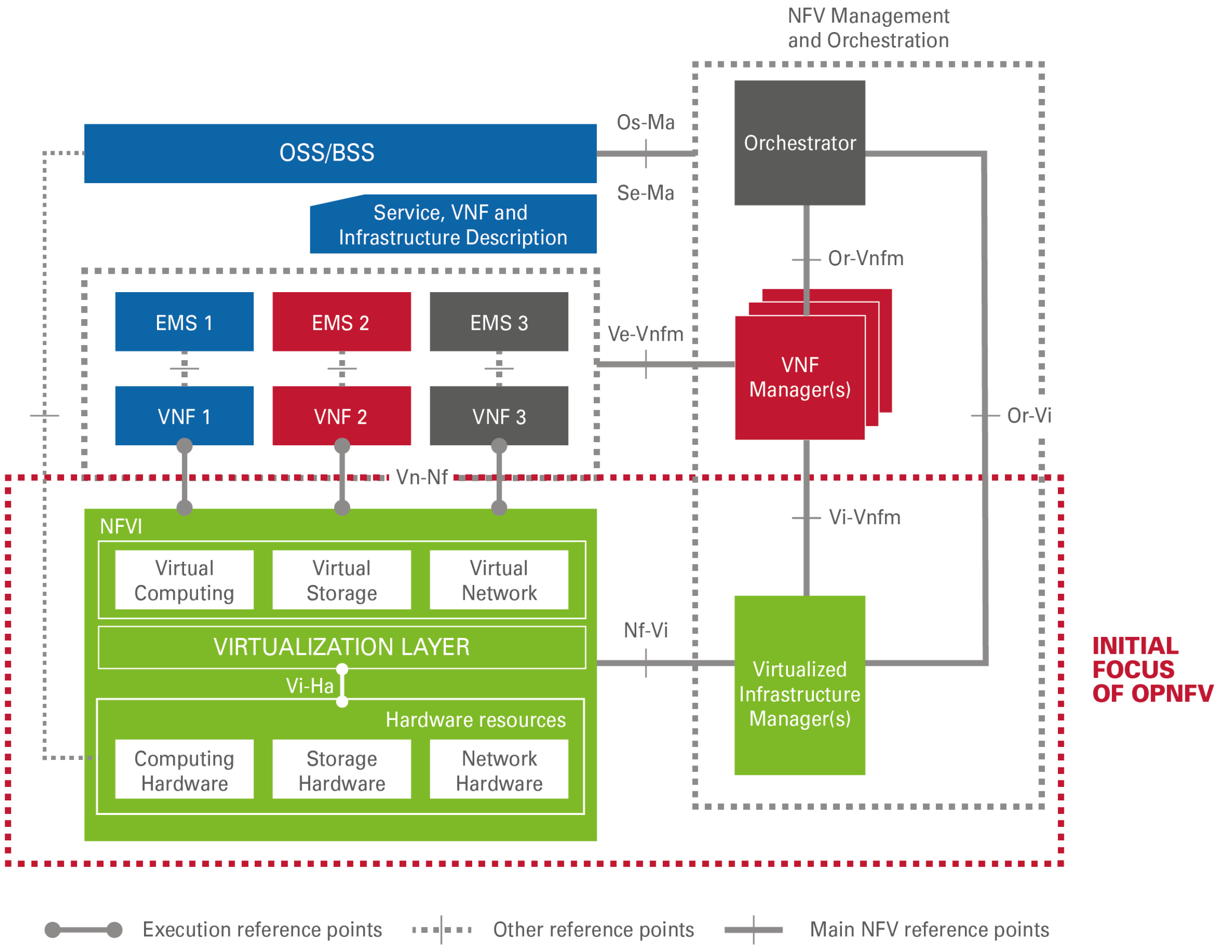


Figure 4-5 **NFV Reference Architectural Framework**

5. Introduction to SDN

The rapid growth of mobile data with mobile service evolution significantly challenges Wi-Fi networks. Present-day Wi-Fi networks are still a traditional and closed communication system for offering easy data services to the end user, which can be difficult to satisfy with the new requirements of differential accesses, guaranteed QoS, smart traffic routing, dynamic network evolution etc.

The current WLAN has specific characteristics which should be taken into account:

a. Easy deployment: WLAN has an easier deployment in respect to other wireless technologies.
b. Operation value: The Wi-Fi network is generally a closed network with a lower grade of interaction with 3rd part application.
c. Service experience: Wi-Fi networks are generally providing only a wireless pipe connection to the Internet without content awareness. In multi-user and high density scenario, Wi-Fi networks do not have a limited QoS capability.
d. Equipment compatibility: the AC and AP are connected with an interface which is a basic standardized protocol and is extensively expanded by each vendor, which can make interworking difficult.
e. Upgrade and extension: The Wi-Fi industry has a long history of working to evolve Wi-Fi technology in order to adapt to new market needs. Conversely, the continual evolution leaves behind many legacy solutions which represent a problematic constraint.

The concept of Software Defined Network (SDN) presents a business opportunity to address these issues and challenges, although SDN introduces new challenges to the industry that will be analysed in the following of this paper.

5.1 SDN principles

The main principles of SDN are the decoupling of the network's control plane and forwarding plane, and logical centralisation of the functionalities. These principles enable the implementation via software the functionalities and rapid evolvement of the network to meet the different requirements of applications, users and tenants.

The SDN architecture and layers are represented with different variants dependant on the standard and industrial organisation which are working on SDN. We will come back on the different approaches later paper, but in order to describe the main concepts let's consider the abstract model of architecture shown in Figure 5-1.

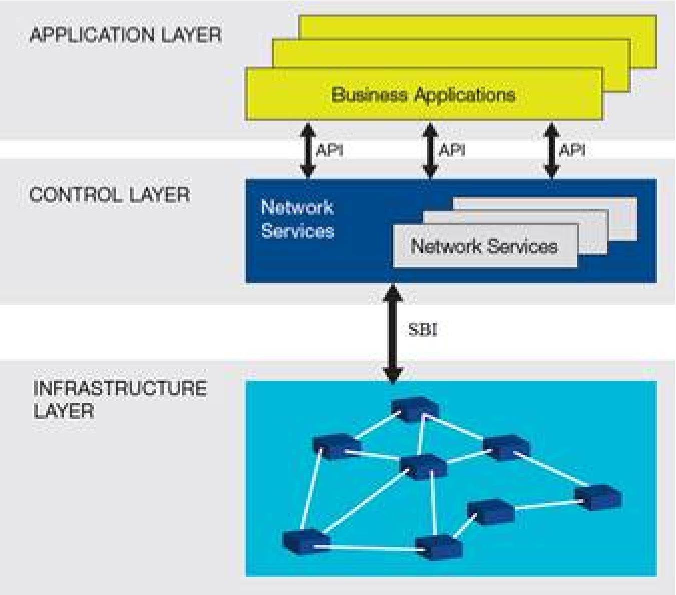


Figure 5-1 SDN architecture and layers

Based on the abstract model, three layers can be identified in the SDN architecture: the Application Layer, the Control Layer and the Infrastructure Layer. The Control Layer includes all the control functionalities which are required by a telecommunication network in order to properly perform the required actions, i.e. control the routing of traffic, security, authorisation, management, etc. The Application Layer includes application functions or services which may provide services directly to the end user or to other application. The Application Layer can include functions developed and deployed by 3rd parties. The lower layer, the Infrastructure Layer, includes the network elements where the control is enforced and where the user data plane are routed between the end points of the communication or application, i.e. from the user equipment to the application server.

The Control Layer has interfaces towards the Application Layer which are Application Program Interfaces (APIs) to support the applications running over the network. These APIs, commonly called northbound APIs, enable a network administrator to rapidly deploy new business applications and to enable, from one side, to be able to provide to applications functional information about the network and from the other side to allow the application function to send specific requests to the network. In the SDN architecture, the control plane is defined by software.

The Control Layer is connected to the Infrastructure Layer with the control plane southbound interfaces. These interfaces control the network devices providing indication on how to treat and forward the data packets (e.g. routing indication and QoS rules). These southbound interfaces can also implement the management plane to control the network operation and status.

The network entities within the Infrastructure Layer are connected via the user plane which is responsible for forwarding the user data packets. The northbound and southbound interfaces may be standardized or proprietary interfaces.

5.2 SDN standardisation landscape

The standardization landscape in SDN is already wide and is expected to keep evolving over time. While some of the activities are being carried out in standard development organizations, other related efforts are ongoing in industrial or community consortia (e.g., OpenDaylight, OpenStack, OPNFV), delivering results often considered candidates for de facto standards. These results often come in the form of open source implementations that have become the common strategy towards accelerating SDN and related cloud and networking technologies. The reason for this fragmentation is due to SDN concepts spanning different areas of IT and networking, both from a network segmentation point of view (from access to core) and from a technology perspective (from optical to wireless). The standardisation landscape has grown broadly in several industrial Fora, consortium and standardisation bodies, and SDN is continuing to evolve, taking into consideration the support of functionalities not previously supported. A comprehensive picture of such a landscape cannot be easily provided, but an extraordinary description of SDN panorama is written in [42] and [43], while in the following section the focus is on the work that is considered more relevant for the scope of this paper.

5.2.1 Open networking Foundation (ONF)

Open Networking Foundation Forum (ONF) is one of the most popular industrial Fora working on SDN. ONF defines the OpenFlow standard which enables the deployment of the SDN based network. ONF was been launched in 2011 by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo!, as a non-profit organization dedicated to rethinking networking and bringing to market SDN standards and solutions.

ONF defines the SDN architecture in [44] shown in Figure 5-2. The Agent supports the concept of exposing the underlying resources, physical in case of the Agent within the data plane, and the network capability in case of the Agent within the SDN controller. The Data Plane includes one or more network elements which contain the traffic forwarding and traffic processing resources. The Control Plane includes a set of SDN controllers which have a control over the resources exposed by network elements in the data plane. The SDN controller executes the request of supported applications and it performs the control of the data plane resources. The SDN controller may communicate with other SDN controllers as necessary. The Application Plane includes the applications.

The network elements, SDN controllers and the application have a functional interface toward the OSS which is responsible for allocating the resources in the lower plane dedicated to a specific entity in the higher plane and for making the lower and higher plane entities capable of communicating.

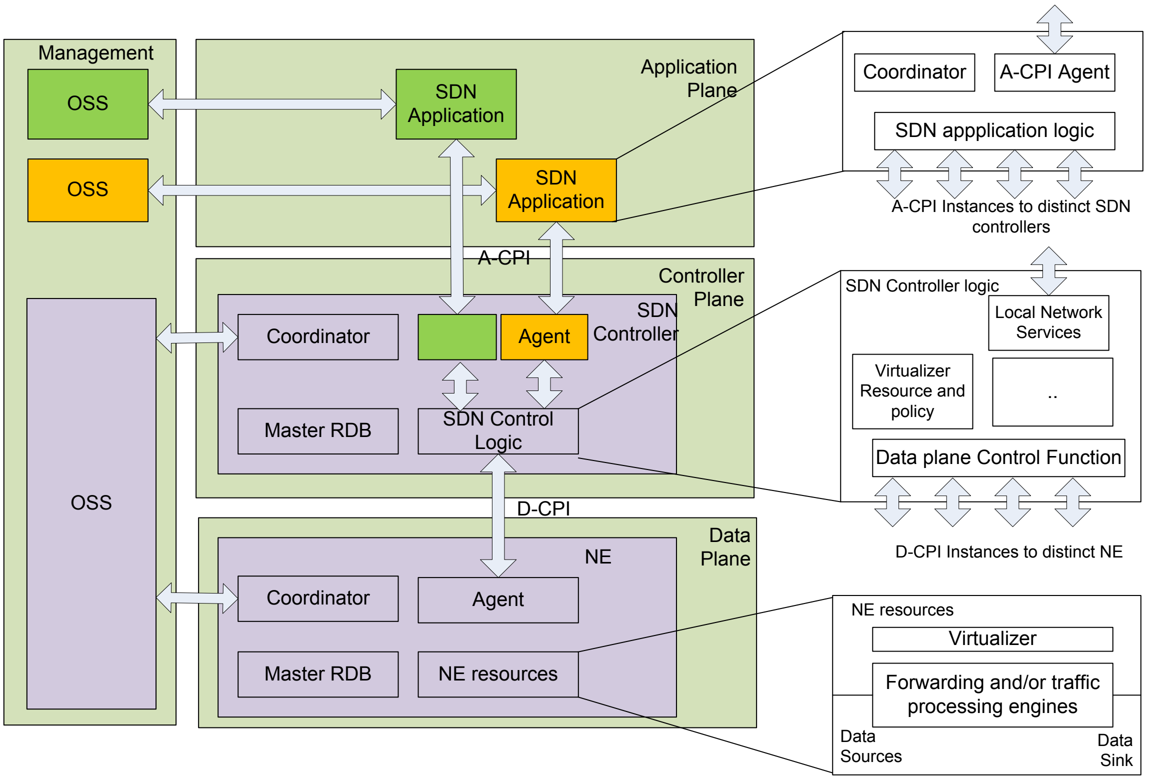


Figure 5-2 ONF SDN architecture with physical data plane

The Data Plane incorporates the Network Element entity, where the data ingresses into a physical or logical interface and is forwarded towards a physical or logical interface at the egress, and the traffic is processed under the control of the Agent. The Agent receives the rules to perform such actions from the SDN controller. In general, the rules are composed by a set of filter rules which identify the traffic ingressing with the instructions on how to treat the traffic and where to send it to output. The action includes also basic QoS operation such as rate-limiting, packet discharge, etc.

The internal architecture of the SDN controller is not specified by ONF and it is seen as a black-box where only the actions perform at the interfaces are defined. However a minimum set of functional components are specified namely the Data Plane Controller Function (DPCF), the Coordinator, the Virtualizer and the Agent.

The Agent, as previously described, plays the rule of entity exposing capabilities and receiving requests from Application. The DPCF controls the resources available and uses them according to the indication from the OSS/Coordinator or Virtualizer that controls them.

The Virtualizer is instantiated by the OSS/Coordinator for each application or operator domain. It shall be noted that the ONF Virtualizer is different from the ETSI NFV Network Virtualisation function. In fact the ONF Virtualizer abstracts the network and resources allocated to a specific client, while ETSI NFV goal is to abstract network function from dedicated hardware. The ONF Virtualizer can be seen as the process that receives client specific requests via A-CPI, validates the requests against policy and resource availability assigned to the client, translates the requests in term of underlying resources and passes to D-CPI and DPCF functions. More details on ONF virtualisation concept are described in the appendix A.3.

The Coordinator is common in the Data Plane and in the SDN Controller and it is responsible to set up the Agent, the resources, the information needed for communication between the NE and SDN controller on behalf of the OSS. More details on coordinator are described in the appendix A.3.

The Resource Database (RDB) is the database included in the NE, SDN controller and in agent that includes the description of the resource available, for example the list of port, capacity, etc for the NE, the network topology, ports, etc , representing the network in the SDN Controller. How the RDB is initially provisioned, if it is included in same entity or in separate, it is out of the ONF standardisation scope.

ONF has defined the basic function of the Network Element for performing data forwarding, named OpenSwitch, and the protocol for the southbound interface between the SDN Controller and the Open Switch named the Openflow in [45]. Openflow protocol may be transported on a implementation specific interface, but it is suggested to encrypt using TLS, but it may run on TCP associated with an IPSec VPN. For further description of Open Switch refers to [45].

The management protocol between OSS and NE, OSS and SDN controller is named Open Flow Config and it is specified in [45].

ONF has also established the Wireless and Mobile network Working Group [46] which has the scope to identify the use cases, the reference architecture that leverage the SDN OpenFlow. The scope is also to define extension of the OpenFlow protocol to support the wireless and mobile network. The WG considers both the 3GPP Mobile Network and the Wi-Fi network.

The ONF considers producing two or more deliverables collecting the relevant use cases and the related requirements, the architecture, the OpenFlow protocol issues and extension needed to support the mobile network. ONF identifies in [47] the main benefits that SDN can bring to the mobile network in terms of the capability to provide end-to-end communication across multiple access technologies, path optimisation per service, network abstraction allowing the support of a network slice per different tenant, such as OTT, MNVO, virtual enterprise network, etc. At the present time of development of this whitepaper ONF has not yet completed the work and the deliverables. Current OpenFlow specification provides Quality-of-Service support (QoS) through a simple queuing and filtering mechanism in the NE based on the rules provided by the SDN controller.

A switch can optionally have one or more queues attached to a specific output port, and those queues can be used to schedule packets exiting the data path on that output port. The packets are mapped to a specific queue and treated according to that queue's configuration (e.g. min rate). Packet scheduling using queues is not defined by the ONF switch specification and is switch dependent, in addition the queue configuration takes place outside the OpenFlow switch protocol (e.g. via an external dedicated configuration protocol). The controller can only query the switch for configured queues).

This limitation of dynamic QoS control (e.g. in term of provision of QoS policy, scheduling, etc.) has been identified, and several solutions have been proposed outside ONF; for example, the QoSFlow framework [48], the UC Software Defined Networking (UC SDN) Activity Group [49] proposed an approach proposing to add a function in SDN controller which enables the exposure of the northbound interface via an API to the QoS function allowing an application to negotiate application treatment with the network [50].

With regard to the Quality of Experience using SDN, alternative approaches have been presented in literature by Universities and vendors. ONF members also proposed to consider the QoS management as part of the extension to be considered in OpenSwitch 1.6 specification.

5.2.2 OpenDayLight

OpenDayLight (ODL) is an open source project with the scope to develop a controller implemented by software based on Java Virtual Machine (JVM), in order to be independent of hardware and operating systems.

The OpenDayLight architecture is shown in figure 5-3. The controller exposes an open northbound API which is used by applications to get network intelligence, run algorithms, to perform analytics, and then use the controller to orchestrate the new rules. The southbound interface supports multiple protocols (as separate plug-ins), e.g. OpenFlow BGP-LS, etc. These modules are dynamically linked into a Service Abstraction Layer (SAL) which exposes device services to modules in the SDN controller. The controller platform contains a collection of dynamically pluggable modules to perform needed network tasks, such as AAA, L2 switching, OpenStack, etc.

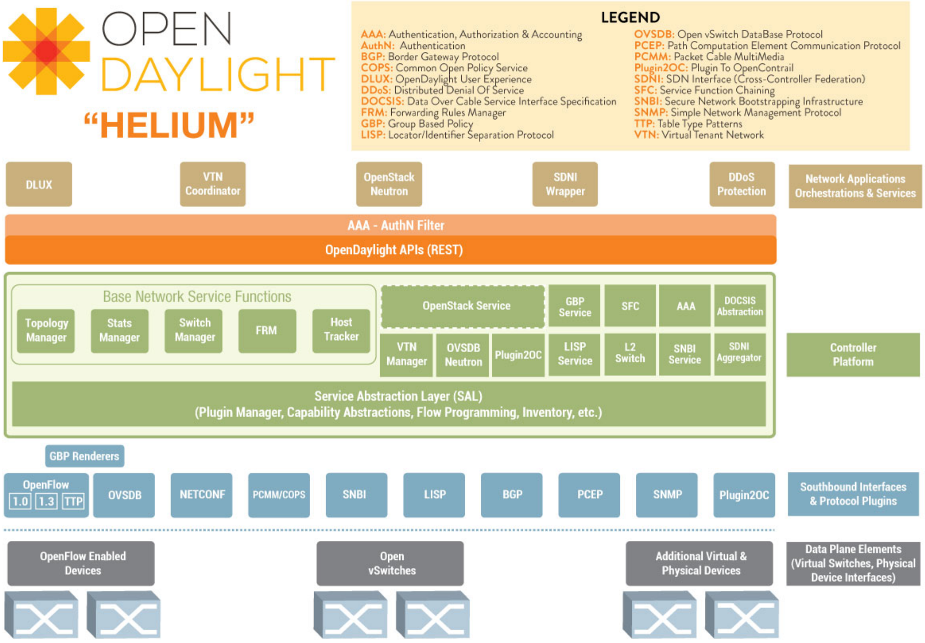

OPEN DAYLIGHT
"HELIUM"
LEGEND
AAA: Authentication, Authorization & Accounting
AuthN: Authentication
BGP: Border Gateway Protocol
COPS: Common Open Policy Service
DLUX: OpenDaylight User Experience
DDoS: Distributed Denial Of Service
DOCSIS: Data Over Cable Service Interface Specification
FRM: Forwarding Rules Manager
GBP: Group Based Policy
LISP: Locator/Identifier Separation Protocol
OVSDB: Open vSwitch DataBase Protocol
PCEP: Path Computation Element Communication Protocol
PCMM: Packet Cable MultiMedia
Plugin2OC: Plugin To OpenContrail
SDNI: SDN Interface (Cross-Controller Federation)
SFC: Service Function Chaining
SNBI: Secure Network Bootstrapping Infrastructure
SNMP: Simple Network Management Protocol
TTP: Table Type Patterns
VTN: Virtual Tenant Network
DLUX
VTN Coordinator
OpenStack Neutron
SDNI Wrapper
DDoS Protection
Network Applications Orchestrations & Services
AAA - AuthN Filter
OpenDaylight APIs (REST)
Base Network Service Functions
Topology Manager
Stats Manager
Switch Manager
FRM
Host Tracker
OpenStack Service
GBP Service
SFC
AAA
DOCSIS Abstraction
VTN Manager
OVSDB Neutron
Plugin2OC
LISP Service
L2 Switch
SNBI Service
SDNI Aggregator
Controller Platform
Service Abstraction Layer (SAL)
(Plugin Manager, Capability Abstractions, Flow Programming, Inventory, etc.)
GBP Renderers
OpenFlow
1.0
1.3
TTP
OVSDB
NETCONF
PCMM/COPS
SNBI
LISP
BGP
PCEP
SNMP
Plugin2OC
Southbound Interfaces & Protocol Plugins
OpenFlow Enabled Devices
Open vSwitches
Additional Virtual & Physical Devices
Data Plane Elements (Virtual Switches, Physical Device Interfaces)

Figure 5-3 Opendaylight architecture (from [51])

Application-Layer Traffic Optimization (ALTO) is an IETF protocol to provide network information to applications. The ALTO project in OpenDayLight is an effort to implement ALTO in OpenDayLight. In addition to implementing the ALTO base protocol (IETF RFC7285) [52], the project leverages OpenDayLight to introduce a provisioning interface for ALTO.

Although OpenDayLight already provides a topology service, it focuses more on detailed network topology (i.e., raw topology) that can be too detailed for applications and/or reveal too much network details to violate network privacy. The ALTO Protocol (IETF RFC 7285) defines abstractions and services to provide simplified network views and network services to guide applications in usage of network resources. In particular, the ALTO Protocol defines the Network and Cost Map Service, Filtered Map Service, Endpoint Property Service, and Endpoint Cost Service.

5.2.3 IETF

The IETF has under the IRTF area the Software Defined Networking Research Group (SDNRG) with the scope to investigate SDN for identifying the approaches including the area of solution scalability, abstractions, and programming languages and paradigms useful in the context of SDN. In addition SDNRG intends to provide objective definitions, metrics and background research to be provided as input to other standards producing organizations.

The group has produced the informational document RFC 7426 [53] providing reference for the SDN research community based on relevant peer-reviewed literature. IETF also produced the informational document RFC 7149 [54] aiming to provide views on the functional taxonomy of the technique which can be used in SDN. The document provides consideration on several techniques to be used in referencing to current solutions already in place in a network that may be seen in the SDN context, or vice-versa where SDN may be introduced, for example the separation of user plane and control plane, with a Controller function, is shown to be similar to the PDP (Policy Decision Point) and PEP (Policy Decision Point) framework defined in the past. The document also makes consideration from the service provider point of view on what SDN would be or should take into account.

The ForCES (Forwarding and Control Element Separation) WG was established in 2011 and closed in 2015. The ForCES framework defined in RFC 3746 [55] and the ForCES protocol has been proposed for Southbound interface of the SDN. The protocol defined in IETF RFC 5810 [56] is composed of a Control Entity (CE) controlling the Forwarding Entity (FE) (RFC 5812 [57]). The ForCES model considers the network element composed of numerous logically separate entities that cooperate to provide a given functionality (such as routing or IP switching). The ForCES protocol is agnostic to the model and can be used to monitor, configure, and control any ForCES-modeled element. Further information can be found in tutorials [58] and [59].

The Interface to the Routing System Project (I2RS) working group scope is to develop use cases and architecture to support an interface to the routing system, where the term "routing system" is referring to a hardware device, a virtual router or any software that provides routing functions. The main driver is to mirror the current typical routing implementation without requiring the re-engineering of the router. I2SR WG has not completed its work and is working on several aspects for example security requirement, definition of routing information model, and the definition of YANG data model for layer 2 and layer 3 topologies. (The complete list of document can be found in IETF WG pages https://datatracker.ietf.org/wg/i2rs/documents/)

The description of IETF work which is related to SDN is not limited to the above WGs, but several proposals and working groups are considering several approaches or adaptation of their work to the SDN scenario such as ALTO (see clause 5.2.2) SPRING, which are not described in details is this clause, but more information can be found in the IETF web pages.

5.2.4 BBF

The Broadband Forum has started a study work SD-313 [60] with the scope to examine the introduction of the SDN concept within the Broadband Access network as a long-term evolution. The study has the scope to consider some deployment scenarios in order to define the recommended action for BBF or to external SDOs. The output of the study will be the guidance for further work in this area to bring the SDN concept to broadband access networks defining for the broadband network the SDN applicability, the use cases of interest, the business requirements, identify the gaps and providing recommendations to enable a SDN and migration strategy.

The BBF work is ongoing and not yet completed. The BBF study started from the analysis of the current work on SDN in other SDOs.

It should be noted that Broadband Access network is related to some NHG network, for example Community Wi-Fi is based on the residential access opened to community user sharing the same infrastructure and in other scenarios the broadband access network may represent the backhauling of the public Wi-Fi network. For such reasons the following use cases identified by BBF that are relevant to Carrier Wi-Fi networks are briefly described:

- SDN-driven network located residential gateway: some functionalities of the RG can be moved from the RG to the network to increase the flexibility and in this context the SDN controller can control only the forwarding plane or it may also include the control functionalities moved from RG to the network;
- Subscriber-aware Traffic Steering, Service provisioning and Node Resilience using SDN with Centralized Subscriber State Management: in current BBF networks, in the post authentication process, the user information is pushed within the BNG and later on BNG may interact with the Policy Server for QoS management purposes. The SDN-based architecture can also allow having only a single point where all this information is received, the SDN controller from an external functional entity, such as AAA, Policy server, etc, and they are used to control the underlying broadband access network. This scenario enables a flexible management of the network
- Portal Based Customer Self-Provisioning: The SDN controller is exposed to the NBI interface and the information that allows the user to configure the network and the required resource.
- Hierarchical recursive SDN controller for multi-tenant environments: in this use case the multi-tenants and hierarchical recursive SDN is used in a broadband access network, for example as enabled with ONF SDN architecture.
- Support of NFV and interconnection between a network supporting NFV and a network not supporting: these scenario are related to joint usage of SDN and NFV for the same portion of network or between different portions of network, one supporting NFV and one not supporting NFV.

Based on the above use cases, and other use cases not included, the study aims to identify the requirements and the gaps in both the broadband access network and in SDN in order to provide guidelines on the future direction of the work for developing normative specification which fulfils the requirements. So far this part of the work has not yet been completed.

5.2.5 IEEE SDN Initiative

The IEEE has established the IEEE SDN initiative (http://sdn.ieee.org/) aiming to address the Cloud, SDN, and NFV within the telecommunication industry. The IEEE SDN Initiative is composed of seven committees: Conference, Education, Publications, Publicity, Standards, Pre-industrial and Outreach. The IEEE SDN initiative has tutorials and webinar available on these areas.

The Standardization work on SDN area is performed by IEEE SA P1903.1 described in clause 5.2.6 and in IEEE 802.1CF described in clause 5.2.7.

5.2.6 IEEE SA P1903 WG Next Generation Service Overlay Networks (NGSON)

Within the project the standard IEEE P1903.1 [61] provides interoperability of content services between network operators and content providers. This Standard specifies protocols among Content Delivery (CD) Functional Entity (FE), Service Routing (SR) FE, Service Policy Decision (SPD) FE, Service Discovery and Negotiation (SDN) FE, and Context Information Management (CIM) FE to support advanced content delivery capability in next generation service overlay networks. The content delivery capability aims to support content discovery, content cache and storage management, content delivery control, and transport Quality of Service (QoS) control including context-aware and dynamically adaptive content delivery operations.

The standard IEEE P1903.2 [62]
This standard specifies protocols among Service Composition (SC) Functional Entity (FE), Service Discovery and Negotiation (SDN) FE, Context Information Management (CIM) FE, Service Routing (SR) FE and Service Policy Decision (SPD) FE to support service composition capabilities in next generation service overlay network. The capabilities of service composition aim to support service chaining and instantiation, specification interpretation, service brokering and execution, and context aware and dynamically adaptive service composition.

The standard IEEE P1903.3 [63]
This standard specifies protocols between Overlay Management (OM) Functional Entity (FE) and all other NGSON FEs, and/or NGSON nodes to enable OM FE involved self-organizing management capability. This standard also specifies protocols among Service Routing (SR) FEs to enable OM FE non-involved self-organizing management capability such as re-organization of overlay structure among multiple SR FEs for recovery from a failed or overloaded SR FE or for performance improvement of service routing.

5.2.7 IEEE 802.1CF OMNIRAN

The IEEE 802.1CF OmniRAN TG [**64**] [**66**] was established and authorized in March 2014 to create a recommended practice on Network Reference Model and Functional Description of IEEE 802 Access Network. An IEEE 802 access network is characterized by a user plane forwarding Ethernet frames between the network interface in the terminal and the network interface at the access router, where the link is terminated..

The standardization project is denoted P802.1CF and describes the use of IEEE 802 technologies to build heterogeneous access networks, which may include multiple network interfaces, multiple network access technologies, and multiple network subscriptions, aimed to unify the support of different interface technologies, enabling shared network control and the use of SDN principles.

While adopting the generic concepts of SDN by splitting the network model into an infrastructure layer and a control layer with well-defined semantics for interfacing with higher layer management, orchestration and analytics functions, the specification maintains a clear separation of functional roles in the operation of access networks to support various deployment models including leveraging wholesale network services for backhaul, network sharing and roaming.

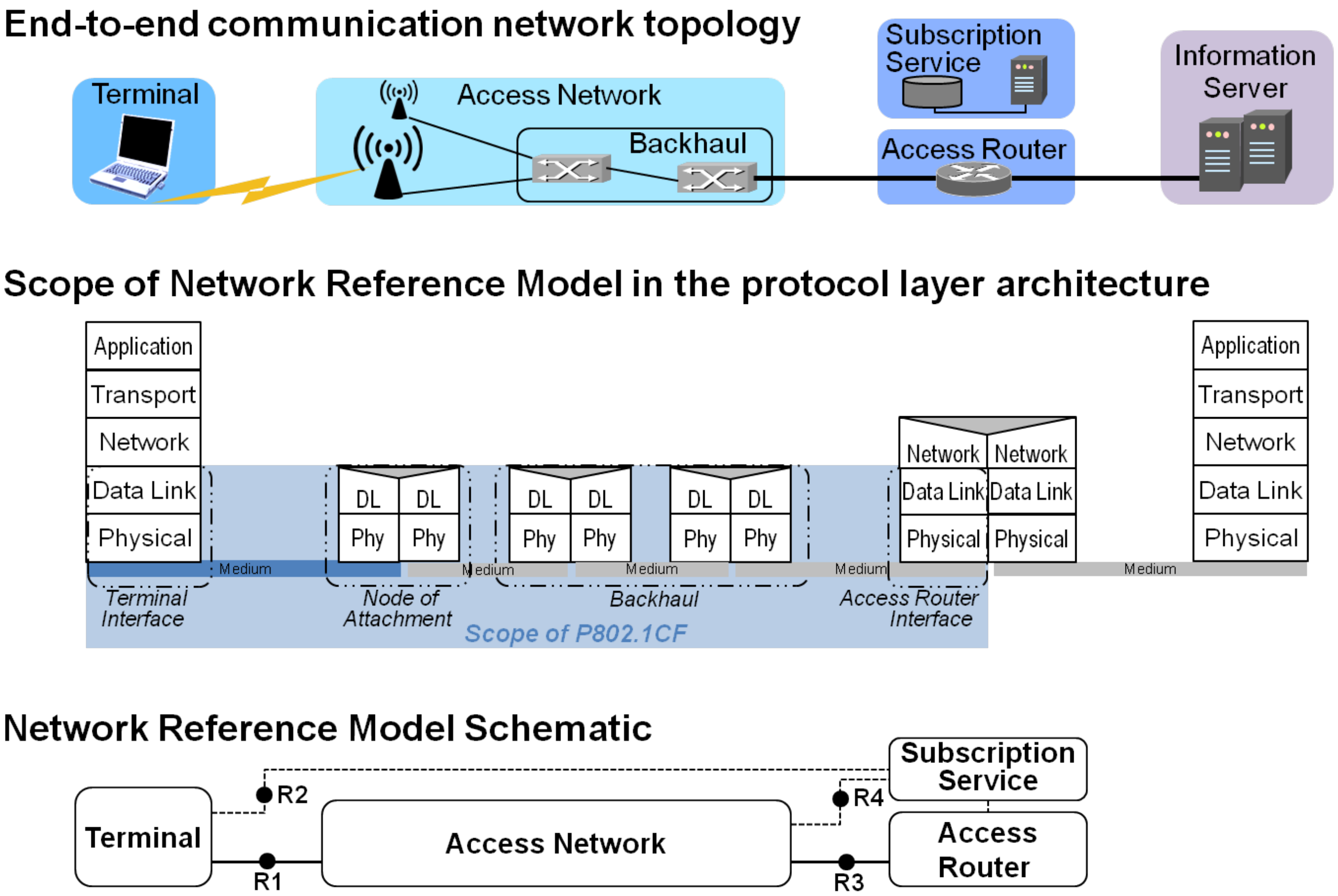


Figure 5-4 **Scope of IEEE P802.1CF**

Within the scope of the end-to-end network model for providing access to IP services, the P802.1CF deals with the communication link between the host in the terminal and the access router in the interface. User plane traffic forwarding is performed on the basis of MAC addresses, even when the Ethernet frames are tunneled over some other transport technologies in the backhaul. By avoiding the functional separation of the user plane and the transport plane in the access network, the specification provides a combined control model for integration of setting up of backhaul connectivity together with provisioning subscriber specific user connectivity as facilitated by modern IEEE 802.1 bridging technologies. For the SDN abstraction of the backhaul an opaque service model adopting well known semantics of the Metro Ethernet Forum is applied, which inherits the full functional and operational flexibility of Carrier Ethernet.

SDN is also a leading aspect for the design of the NRM consisting of the definition of the functional entities of the IEEE 802 access network as well as of the reference points for the communication between the functional entities. At a glance, the network model for IEEE 802 access network consists of the terminal, the access network comprising the node of attachment and the backhaul, the access router, and the subscription service, which provides authentication, authorization, accounting as well as policy functions for the users of the terminals. Communication interfaces between the entities are denoted by R1 for the interface between the terminal and the node of attachment, by R2 for the authentication procedures between terminal and subscription service, by R3 for the interface between the access network and the access router, and by R4 for the authorization, accounting and policy functions between the access network and the subscription service.

Figure 5-5 below presents the complete NRM, which exposes a terminal controller in the terminal and a controller in the access router, both interconnected with the access network controller in the access network. Moreover a further entity denoted coordination and information service is added for the management of shared network resources among multiple access networks like a spectrum database for controlling access to spectrum in the case of TV white space or licensed shared access.

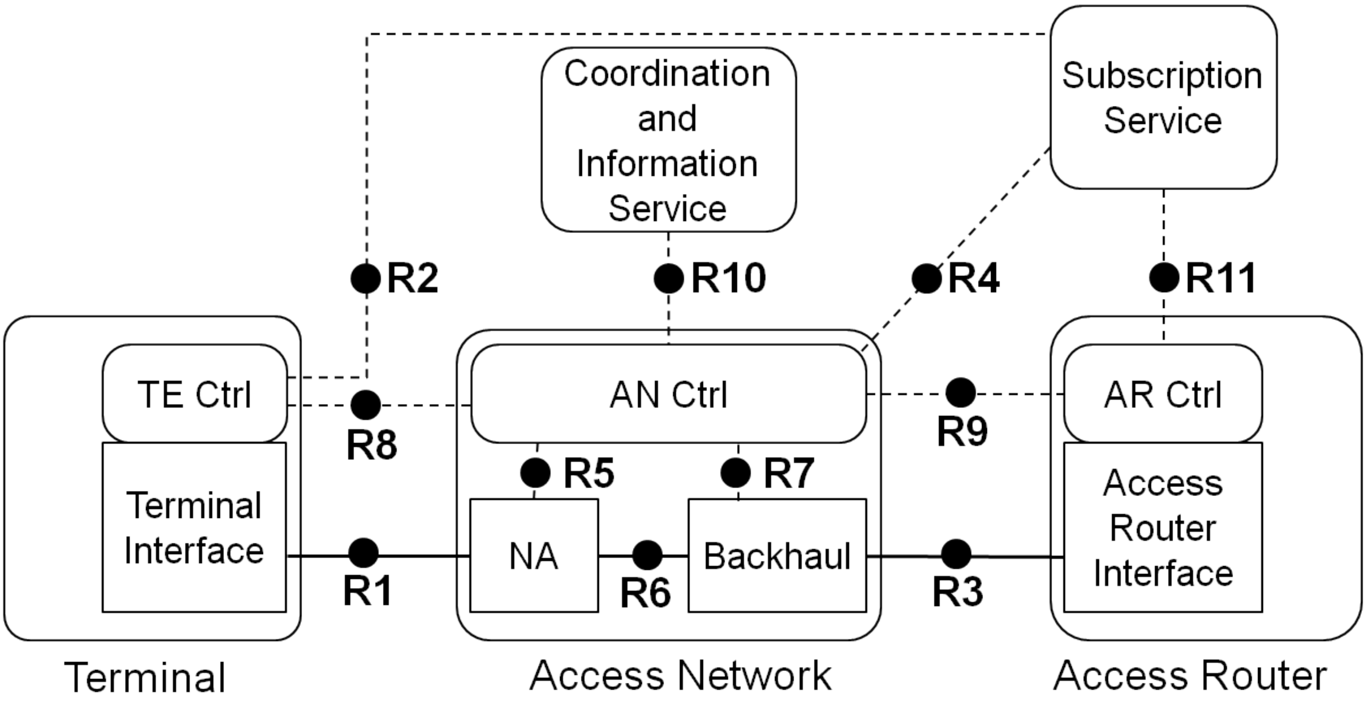


Figure 5-5 IEEE 802 Access Network Reference Model

Reference points in the NRM denote either data path interfaces forwarding Ethernet frames, or control interfaces for IEEE 802 related parameters, which may be carried either within IEEE 802 protocols or within IP based protocols. In the case that IEEE 802 specific identifiers or configuration information are carried within IP protocols, the details of the IP protocols are left open to accommodate various deployments. Nevertheless the P802.1CF specification provides a comprehensive behavioral and functional description of the message exchanges between the entities of the NRM to guide implementers in the appropriate choice of the IP protocols. By focusing its scope to the architectural model and to the specification of the related IEEE 802 identifiers and attributes P802.1CF delivers an SDN enabled abstraction of IEEE 802 access network, which fits well to various protocol proposals for communication between the SDN controller and infrastructure layer and enables interoperable implementations of SDN for IEEE 802 based access networks.

The radio access network (RAN) of a Carrier Wi-Fi network is well aligned to the P802.1CF model and scope as IEEE 802.11 APs are the node of attachments and the complete link between the terminal and the access router is enabled for transport of Ethernet frames. Authentication procedures as well as the interfaces into the AAA infrastructure are represented by the R2, R4 and R5 reference points, respectively. Even the latest enhancements in Carrier Wi-Fi like ANQP are reflected in the functional description and in the NRM by reference point R8. However due to its focus on SDN principles and IEEE 802 technologies, P802.1CF may not provide much guidance for the virtualization of legacy Carrier Wi-Fi access infrastructures, in particular for split-MAC designs with an access controller in the data path.

IEEE 802.1 OmniRAN TG continuously monitors the SDN related activities in other standardization organizations to keep the specifications aligned. To determine and evaluate emerging approaches in SDN the OmniRAN TG hosts at IEEE 802 plenary meetings a dedicated Wireless SDN Birth of Father session and maintains a wiki page listing standardization efforts in other SDOs with close relation to the technologies developed by IEEE 802.

Related Links:

- P802.1CF project status: http://www.ieee802.org/1/pages/802.1cf.html [64]
- OmniRAN TG status: https://mentor.ieee.org/omniran/bp/StartPage [65]
- OmniRAN SDN Wiki: https://mentor.ieee.org/omniran/bp/SDN_Wiki [66]

5.2.8 3GPP

Currently there is no activity related to SDN in 3GPP.

5.2.9 ITU-T

The ITU-T is working in the SDN area in several Study Groups and has produced several recommendations. In June 2013 ITU-T established the Joint Coordination Activity on Software-Defined Networking (JCA-SDN) [67] with the scope to coordinate and to ensure that the ITU-T SDN standardization work progresses in a coordinated manner among Study Group 13 on use-cases, requirements and architecture, Study Group 3 on billing, economic and regulatory considerations, Study Group 11 on protocols and interoperability, Study Group 12 on QoS, Study Group 15 on transport aspects, Study Group 16 on multimedia systems and services, and Study Group 17 on security. The JCA-SDN has also the scope to facilitate the coordination among ITU-T and other SDOs. The roadmap of the SDN work in ITU is defined in ITU-T JCA-SDN-D-001 Rev.2 [68].

The deliverables for the different SG are listed in the following (the list is limited to general SDN recommendation, for example those specific to BNG are not reported):

- ITU-T SG 11 produced the following Recommendation in the SDN area:

  - ITU-T Q.Suppl. 67 [69] providing the framework of signalling for SDN by specifying the signalling requirements and architecture for SDN, as well as the interfaces and signalling protocol procedures:
  - ITU-T Draft Q.PVMapping [70] describing the interfaces requirements for mapping between SDN based physical underlay networks and virtual overlay networks, the signalling requirements for mapping between SDN based physical underlay networks and virtual overlay networks and scenarios and procedures:

- ITU-T SG 13 produced the following Recommendations:

  - The Rec. ITU-T Y. 3300 [71] describes the framework and specifying the fundamentals of SDN. The definitions, objectives, high-level capabilities, requirements and high-level architecture of SDN are addressed in this Recommendation:
  - The Rec ITU-T Y. 3321 [72] specifying the requirements and capability framework of S-NICE (Software-Defined Network Intelligence Capability Enhancement) where NICE (ITU-T Y.2301 [73]) is an enhanced next generation network (NGN). S-NICE is a specific implementation of NICE, making use of software-defined networking technologies:
  - The Rec. ITU-T Y.3320 [74] provides an overview and requirements for applying formal methods to SDN. The formal methods are mathematics-based techniques used for specifying, developing, and verifying software and hardware systems and are expected to increase the reliability and robustness of the system:
  - ITU-T Draft Supplement Y.SDN-use cases [75] describing the use cases of Telecom SDN:
  - ITU-T Draft Y.SDN-req [76] based on ITU-T Y.3300 describing the details of capabilities, and the functional requirements to realize SDN. Various issues e.g., programmability, resource abstraction, interworking, verification of SDN applications, adaptation to large scale networks, virtualization of network elements, multi-level of programmability, programmatic extension in resource layer, and management described in are considered in describing the requirements;

  - ITU-T Draft Y.SDN-arch [77] based on ITU-T Y.3300 describing overall architecture of SDN with descriptions of its functional blocks and interfaces to make them an enabler for further work on SDN protocols, security and to customize SDN to appropriate use cases (clouds, mobile networks, etc.).

- ITU-T SG 15 produced the following Recommendation

  - ITU-T Draft G.astdn [78] specifying the transport network control plane architecture to support SDN control of transport networks that is consistent with the principles of SDN and is complementary to SDN related work in SG11, SG13, and SG17.

- ITU-T SG 17 produced the following Recommendations

  - Draft X.sdnsec-1 [79] describing the support of protection of network resources using security services based on SDN. The Rec. defines the security requirements and use cases;
  - Draft X.sdnsec-2 [80] describing the support security protection for SDN. This Recommendation describes new security threats when introducing SDN and provides possible security counter measurements;

5.3 Relationship between SDN and NFV

This clause describes the relationship between SDN and NFV; for example, if both are deployed jointly

Although SDN and NFV can be deployed separately, these two technologies complement each other and together can provide unique solutions. NFV separates the physical aspects of the hardware from the software developers to build hardware agnostic applications. SDN separates the network forwarding plane from the network control plane allowing programmatic and automated changes to connectivity between NFV components.

Having a single integrated orchestration and management for NFV that uses SDN will enable the capability to manage, computing, storage, and network resources for initiating new services as well as managing the lifecycle of these resources and services. For example, this integration enables the creation of dynamic service function chains linking together VNF components within and across data centers.

There are multiple ways to map the SDN architecture function (Resources, Controllers, management, and applications) to the ETSI MANO architecture. ETSI NFV-EVE005 [81] addresses a number of possible mappings for each function; however, this section only focuses on mapping SDN controllers to the NFV architecture. Please note that the scenarios described below are not exhaustive and the referenced document is still under development at the time of publication of this whitepaper.

SDN controller mapping to ETSI NFV Architecture: SDN Controller is software based and hence can reside in a number of NFV functions. As demonstrated in the architecture diagram below, the SDN Controller(s) may:

Reside in the Virtualised Infrastructure Manager (VIM): here the VIM maps virtual resources to physical resources that includes SDN based connectivity between those resources,

Be instantiated as a VNF instance: here SDN networking can connect together VNF components to achieve a single VNF or multiple VNFs to achieve a service,

Reside below the VIM in the NFVI layer: here the SDN controller is one type of Network Controller resource,

Become part of the OSS/BSS: here the SDN controller works in concert with network services management and control.

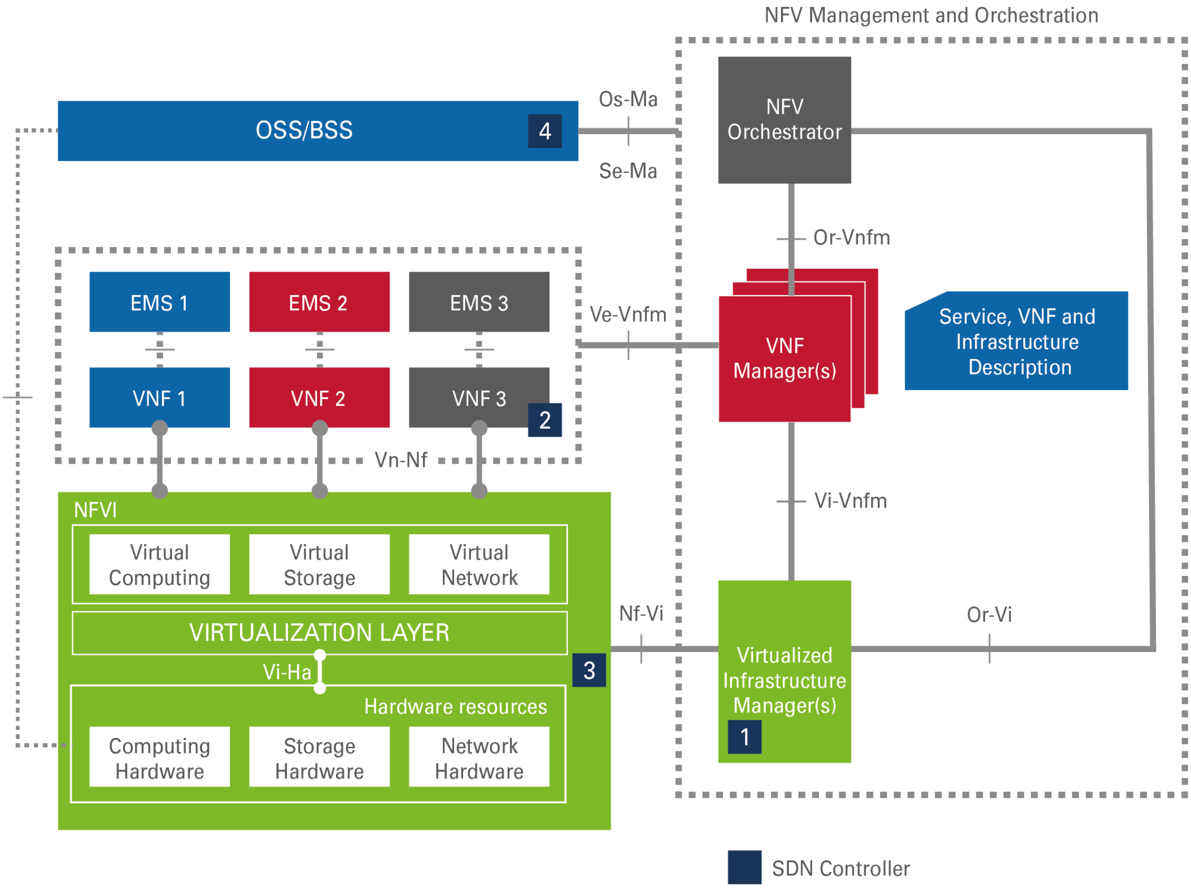


Figure 5-6 Possible SDN Controller location

6. Deployment

This clause identifies the deployment options for NFV, SDN and NFV+SDN approach.

6.1 NFV adoption strategy

6.1.1 Introduction

The success of deploying and managing a complete NFV MANO solution will require the maturity of four areas:

- Standards maturity
- Technology maturity
- Technical expertise availability
- Organizational maturity and readiness

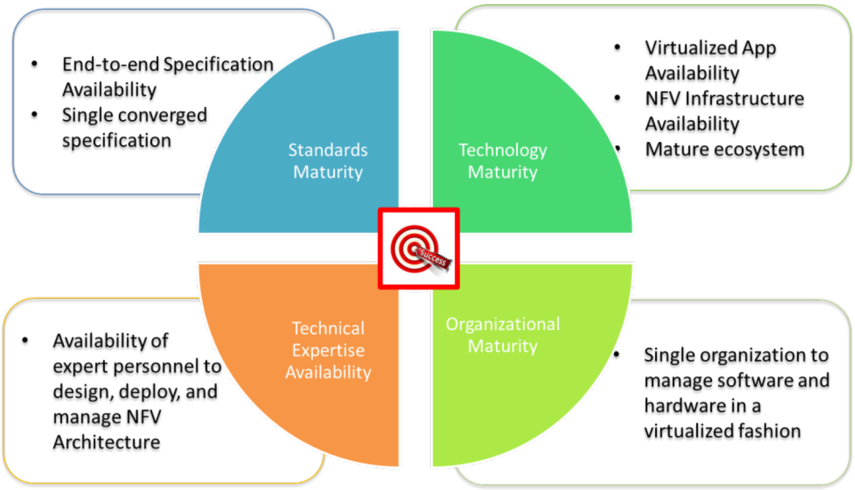

• End-to-end Specification Availability
• Single converged specification
Standards Maturity
Technology Maturity
• Virtualized App Availability
• NFV Infrastructure Availability
• Mature ecosystem
success
• Availability of expert personnel to design, deploy, and manage NFV Architecture
Technical Expertise Availability
Organizational Maturity
• Single organization to manage software and hardware in a virtualized fashion

Figure 6-1 Key enablers to adopt NFV

6.1.2 Adoption for MANO Architecture

Companies will most likely have to adopt a phased deployment for the NFV architecture that aligns with the maturity of the four areas highlighted above. Current stage-3 detail specifications that are most mature are around the definition of the Network Functional Virtualisation Orchestrator (NFVO), the Virtual Network Function Manager (VNFM) and the Virtualized Infrastructure Manager (VIM) function. Naturally, early adopters will focus on virtualizing the applications while maintaining a lot of manual processes for resource and services orchestration. Companies might start with virtualizing applications on dedicated NFV environments to get better expertise on how to manage the environment and mature to the next step to host multiple applications on a single NFV. Since the maturity of service orchestration standards might be lagging behind resource orchestration standards and due to the complexity of the service orchestration, companies might choose to deploy Resource Orchestration first and follow up with service orchestration deployment in a subsequent phase.

The figure below summarizes an example of phased deployment that maps to the expected phased maturity of the standards:

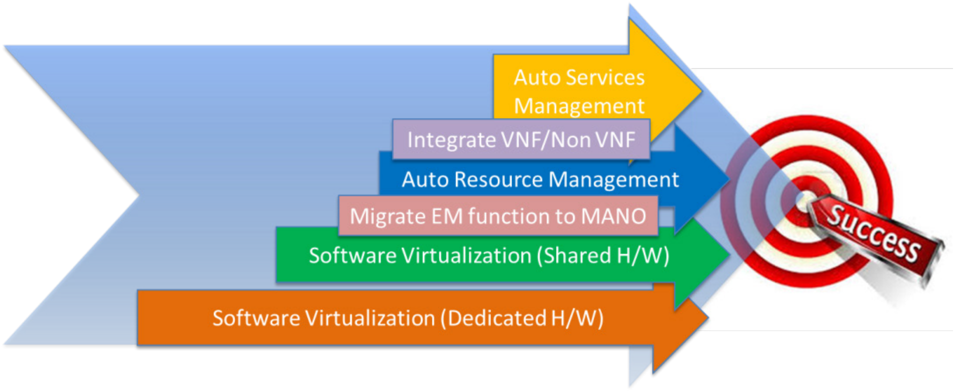

Auto Services Management
Integrate VNF/Non VNF
Auto Resource Management
Migrate EM function to MANO
Software Virtualization (Shared H/W)
Software Virtualization (Dedicated H/W)
Success

Figure 6-2 Example Phased Deployment Approach

6.1.3 Adoption for virtualized applications

Companies can adopt different approaches to achieve a fully virtualized network:

- Launch new services on virtualized environments
- Adopt a cap and grow model where new incremental capacity for non-virtualized legacy applications will be built and deployed on virtualized environments
- Convert non-virtualized legacy applications to fully virtualized environment.

Companies might choose to adopt one or more of these approaches based on their financial and technology drivers.

6.1.4 Current Challenges and Gaps

Service providers and vendors are eager to adopt NFV and SDN technologies in order to reap the promised financial and technical benefits. Although the industry is seeing early adopters to the new technology, there are a number of challenges that are slowing their adoptions. Below is a snapshot of some of the identified challenges that are causing this slowdown:

- The MANO architecture is complex with a large number of elements and interfaces. It is crucial to have the functions of these elements and the data/information models clearly defined in the standards in order to reduce the effort needed to integrate these functions. Interoperability testing between different solutions will also help identifying standards gaps and help in maturing these solutions.
- Current NFV and SDN standards are being developed in parallel in different standards organization but there is no governing entity that ensures alignments between them. The result is fragmented solutions that are hard to integrate and deploy in a standards fashion.
- Business cases for NFV are built on the OpEx savings which is mainly a result of the service’s life cycle management automation. With the lack of fully virtualized applications, it is hard to build the business case to migrate these applications to NFV environment.
- NFV and SDN technologies change the network management model and introduce more sophisticated processes that require different skill sets to design, deploy, and manage virtualized networks. Lack of expertise that has the combined IT and Network experience present a hurdle for some companies in adopting these technologies on a large scale.
- NFV and SDN technologies do not fit the traditional organizational structure since they require a merging of the IT, Network Development, and Network Operations organizations. Companies are slowly transforming their organization structure in order to support these two technologies keeping in mind that they have to maintain parallel support for their traditional non-virtualized environment for years.

6.2 NFV based framework deployment

The virtualization of network functions is an industry transition that is impacting all service provider segments and will therefore effect the realization of future carrier Wi-Fi networks.

Drivers for virtualizing network functions are similar to those that have led to the virtualization of data centers, including [82]:

- Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry.
- Shorter Time to Market by minimising the typical network cycle of innovation.
- Economies of scale required to cover investments in hardware-based functionalities are no longer applicable for software-based development, making feasible other modes of feature evolution.
- Inherent multi-tenancy, which allows use of a single platform for different applications, users and tenants.
- Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up or down as required.

The adoption of an NFV approach introduces a number of key differences compared to the traditional approach of using vendor specific software and hardware. These differences include:

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

6.2.1 NFV Use Cases

As a generic framework, the ETSI NFV architecture can in theory be applied to any network function. In order to prioritize the wide range of use cases for NFV adoption, ETSI has defined a first set of high level use cases that cover off some key prioritized applications of the NFV concepts [83].

The use cases are not intended to be exhaustive. Currently, nine use cases are defined:

- Use case #1: Network Functions Virtualisation-as-a-Service
- Use case #2: Virtual Network Functions-as-a-Service
- Use case #3: Virtual Network Platform-as-a-Service
- Use case #4: VNF Forwarding Graphs
- Use case #5: Virtualisation of Mobile Core Network and IMS
- Use case #6: Virtualisation of Mobile Base Station
- Use case #7: Virtualisation of the Home Environment
- Use case #8: Virtualisations of CDNs
- Use case #9: Fixed Access Network Functions Virtualisation

The ETSI descriptions recognise that the above list of use cases may be used by other industry forums. ETSI use cases #1 and #2 highlight the core capability of NFV implementations to support multi-tenant deployments, where a common NFVI (use case #1) or common VNF (use case #2) can be used to support multiple (WBA Operator) tenants.

Whereas the above list does not explicitly call out the Virtualized Wi-Fi access as a use case, interesting analogies can be drawn with development associated with ETSI Use Case #6, the virtualized mobile base station, discussed in the following section.

6.2.2 Virtualized Wireless Access

Unlike virtualization of other network functions, virtualization of wireless access requires that some physical network function is still present to provide the radio frequency capability necessary to support the base station operation. Hence, the first task prior to virtualizing the wireless access is to first decompose the access layer into two components. In particular Figure 6-3 illustrates alternative approaches to decomposing the Wireless Access, contrasting the conventional decomposition of the Wi-Fi access point into Access Controller (AC) and Wireless Termination Point (WTP) functions, e.g., as described in RFC 5415 [84] and RFC 5416 [85], and the ETSI Use Case #6 that is seeing the decomposition of a composed LTE eNB into a Physical Network Function (PNF) corresponding to a Remote Radio Head (RRH) and a virtualized Network Function (VNF) corresponding to the Base Band Unit (BBU).

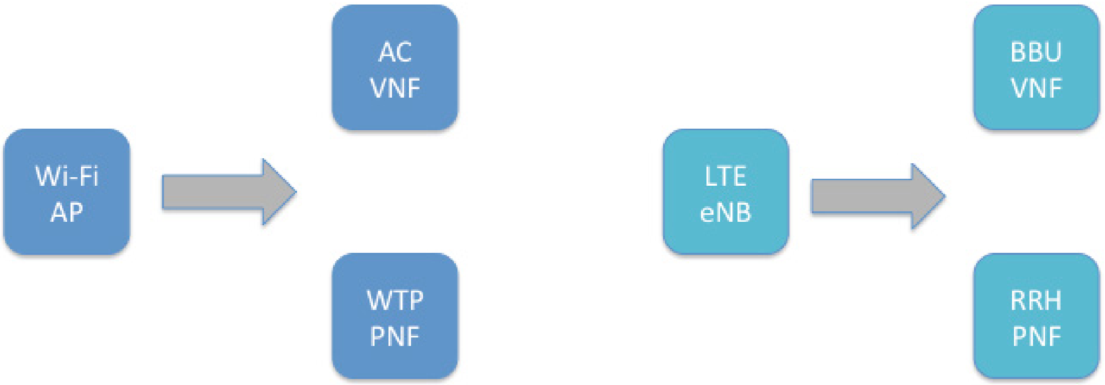


Figure 6-3 Decomposing access into PNF and VNF components

In particular, the decomposition that is driving the conventional licensed radio base station equipment to be decomposed into VNF and PNF components can be likened to the established decomposition of a Wi-Fi access point into Access Controller and Wireless Termination Point functions.

However, whilst the current functional decomposition between AC/VNF and WTP/PNF is well-understood by the Wi-Fi industry, supporting both remote MAC as well as Split-MAC realizations, there are currently discussions in the licensed radio industry as to how to optimally allocate base station functions to PNF and VNF components, with a range of different splits being analysed. For example, the Small Cell Forum SCF-106 [86] has analysed five different alternative functional decompositions between physical and virtual elements. Figure 6-4 below compares the classical local MAC and split MAC options currently supported using the Wi-Fi AC/WTP architecture with two of the five alternative splits being considered for virtualizing the LTE eNB architecture in SCF 106, corresponding to the ”remote MAC” option where the central VNF comprises PDCP functionality and the remote PNF includes RLC/MAC functions and the “split MAC” option whereby the LTE MAC is partitioned into low speed and high speed components, with only the high speed MAC functions being implemented on the PNF.

Figure 6-4 illustrates the strong similarities between the already established functional decomposition supported in Carrier Wi-Fi networks and on-going discussion about how virtualization is leading to a decomposition of classical cellular base station functions between PNF and VNF components.

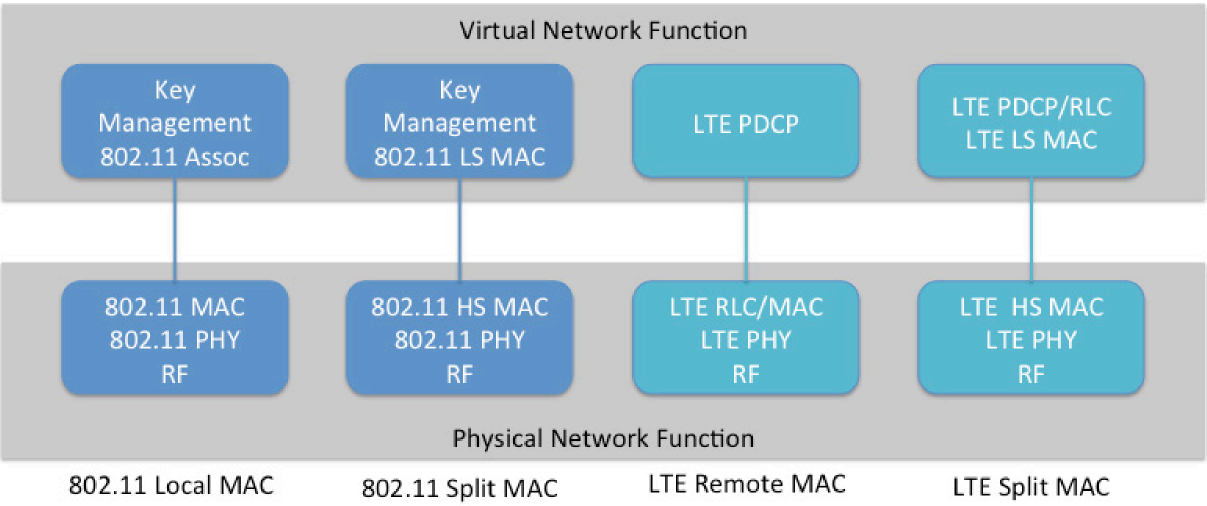


Figure 6-4 Comparing Wi-Fi decompositions described in RFC 5415 [84] [85]/RFC 5416 [79] with and candidate LTE access function decomposition

6.2.3 Management Implications of NFV Wi-Fi Access

Recognizing that the virtualized Wi-Fi access architecture will comprise both physical and virtual network components, the ETSI MANO architecture defines approaches that are able to manage both virtualized and non-virtualized network functions, enabling a virtual network service to be formed by one or more VNFs, VNF Forwarding graphs, PNFs and Virtual Links [16].

3GPP have evolved this baseline architecture still further, describing in [87] a management architecture that addresses both virtualized and non-virtualized (physical) network functions. This management architecture is shown in Figure 6-5, illustrating the management architecture, which manages both virtualized and non-virtualized network functions.

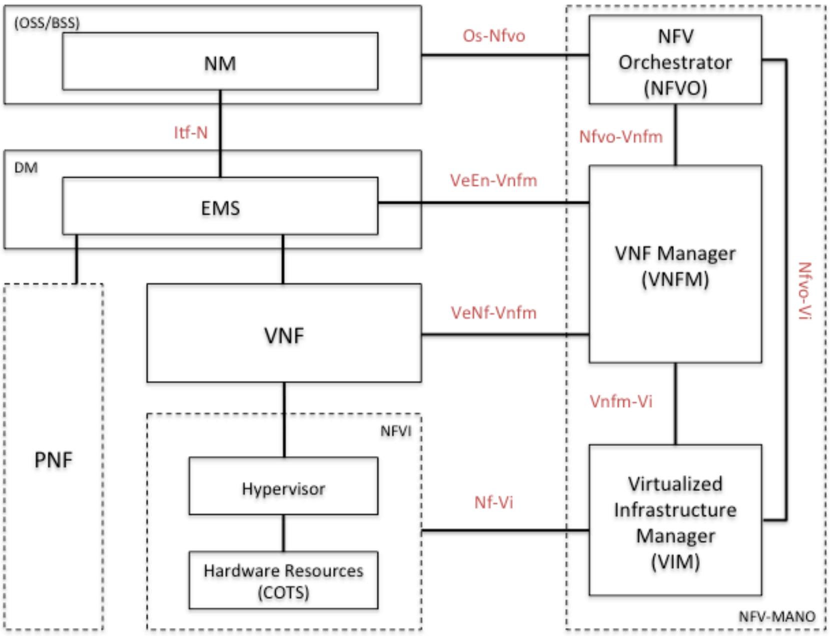


Figure 6-5 3GPP's mixed network management for virtual and physical network functions.

3GPP's mixed network management architecture assumes a clean demarcation between physical and virtual management domains. When we map the WTP/AC decomposed Wi-Fi access functions onto this figure, it is evident that conventional WTPs are managed by the Access Controllers. Hence, WBA's mixed network management architecture for virtualized Wi-Fi access is illustrated in Figure 6-6.

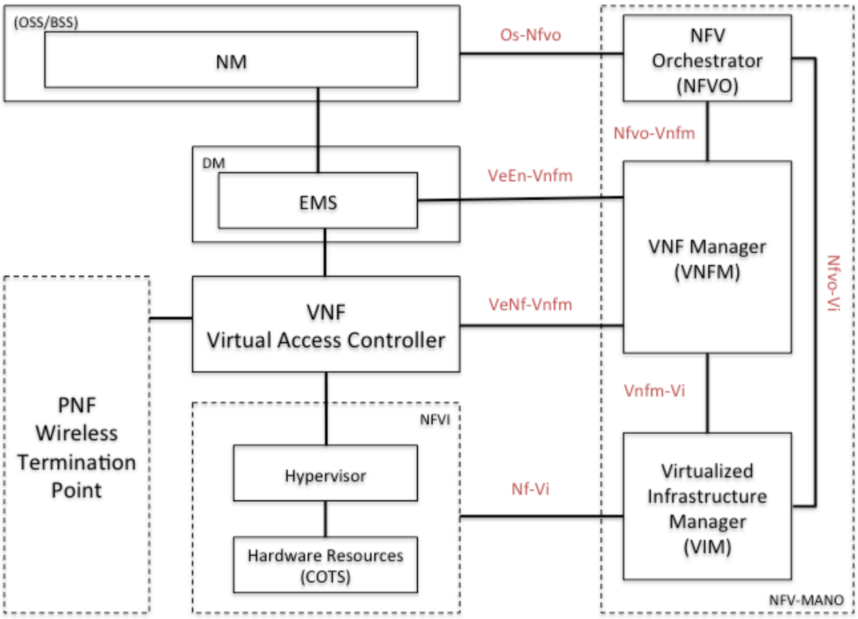


Figure 6-6 Modified mixed PNF/VNF network management to take into account WTP management by virtualized Access Controller

6.2.4 User Plane Aspects of NFV Wi-Fi Access

Whereas the virtual Access Controller can be configured to handle user plane for users attached to the virtualized Carrier Wi-Fi system, i.e., when operating in the split-MAC configuration highlighted in Figure 6-4, the local MAC option allows an alternative configuration where the virtualized Access Controller is a control plane only element and the data plane is handles directly between the PNF Wireless Termination Point and the WLAN Gateway,

In the former configuration, user plane packets are required to traverse the virtual Access Controller and virtual WLAN gateway functions. In ETSO NFV terminology, this is referred to as a Virtual Network Function Forwarding Graph (VNF-FG) [82]. As highlighted in section 6.1.1, Virtual Network Forwarding Graphs are being addressed by ETSI NFV as part of their Use Case #4. Figure 6-7 illustrates the use of VNF-FGs to support the chaining of virtualized Access Controller and WLAN Gateway functions.

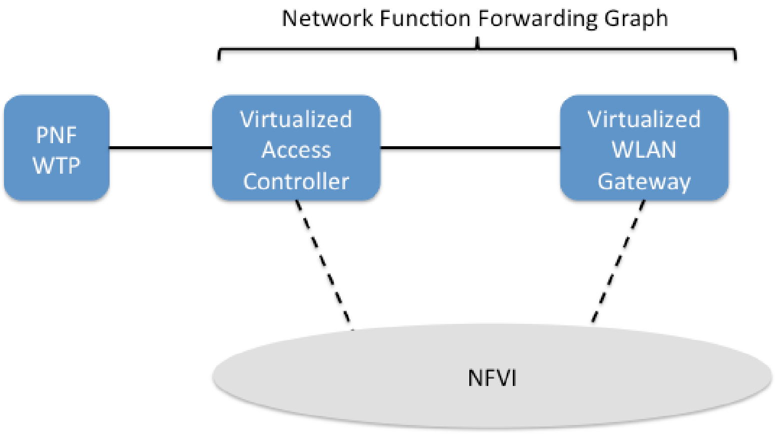

Network Function Forwarding Graph
PNF WTP
Virtualized Access Controller
Virtualized WLAN Gateway
NFVI

Figure 6-7 VNF Forwarding Graph used to integrate date plane handling by virtualized Access Controller and virtualized WLAN Gateway

In the later configuration, user plane packets are transported directly between the Physical Network Function and the Virtualized WLAN Gateway, as illustrated in Figure 6-8. In this case, different tunnel encapsulations are possible between PNF and VNF components. Specifically, draft-ietf-opsawg-capwap-alt-tunnel [88] describes alternative tunnel encapsulations that can be used between a WTP and a non-AC element, including L2TP, LT2Pv3, IP-in-IP, PMIPv6, GRE-IPv4 or GRE-IPv6

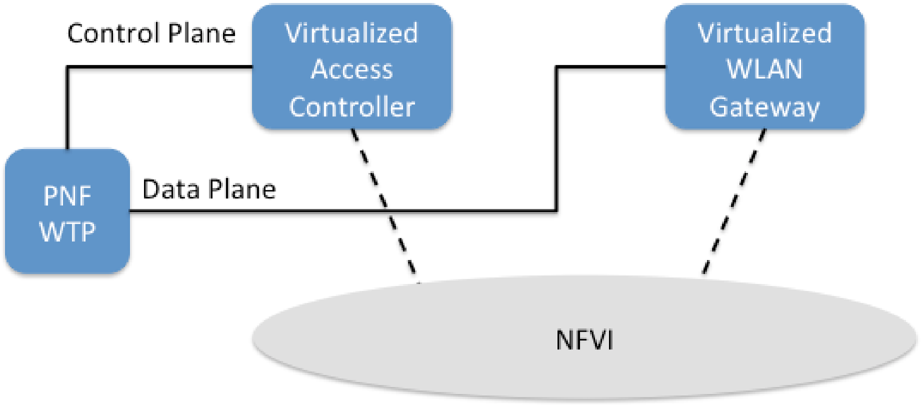


Figure 6-8 Remote MAC termination enabling direct Data Plane forwarding between PNF and virtualized WLAN Gateway

6.2.5 Virtualized Carrier Wi-Fi Management Systems

Figure 3-1 illustrates how the Carrier Wi-Fi management system is decomposed into a set of granular management functions, comprising AAA Server, Policy Server, Remediation Server, OSU Server, Certification Authority, ANQP Server, Subscriber Database as well as Network Management System and WLAN SON Server, as well as conventional DHCP and DNS functions.

The virtualization of the Wi-Fi management functions may be realized as a single multi-tenant instance or a plurality of single tenant instances. In the latter configuration, the instances need to have clear partitioning to ensure the users of one instance are not able to gain visibility of the operation of a second instance.

6.3 SDN based deployment

This clause describes the possible approaches and issues related to the introduction of SDN based deployment of a Carrier Wi-Fi. At this stage, WBA does not intend to mandate any specific solution, but rather to identify the open issues, the gaps and, where possible, the directions currently explored by other SDOs.

The current SDN technologies are mainly focused on the network programmability in the data center, forwarding functionality of switch or router, but don't cover the specific functionalities of a Carrier Wi-Fi network, such as radio resource management, mobility management, flow based QoS charging, as well as the packet forwarding between the air interface and the wired interface in WLAN AP.

The authentication of the user is a fundamental aspect of Wi-Fi network, and more in general of any modern telecommunication network. The Authentication process may be seen as an application running on top of the network or as a fundamental constituent part of the network itself. Furthermore for Wi-Fi network a consolidated authentication process based on the support of IEEE 802.1X [89] and EAP-based authentication ([90], [91], [92], [93], [94]) has been defined and is widely supported on user devices. These authentications are also the basis for roaming agreements. The support of authentication in the SDN framework is also further investigated.

Strictly connected to the authentication is the accounting functionality, that in any current deployment is performed by the same network elements, the AP less frequently or AC more frequently generates accounting information which is transmitted to AAA where they are collected and further elaborated. The accounting process, as well as the authentication, shall be supported in roaming scenario, i.e. the information shall cross the border between the operator domains. The requirement related to accounting in the SDN based deployment needs further analysis and consideration.

Last but not least, Carrier Wi-Fi includes the support of Passpoint [95] furthermore may implement mechanisms for supporting QoS, mobility of users among APs and interworking with other networks, such as fixed networks for Community Wi-Fi and 3GPP networks. This clause will address the issue related to these features.

The Wi-Fi network is also capable of interacting with the application for providing service to the end user. In today's network model each Application Server is connected to the Wi-Fi network via proprietary over the top or in some case with standard interface, but the deployment is really customized. The introduction of SDN architecture enables to interconnect the control layer with Application via API. This opportunity to expose network capabilities and interaction with applications are described more in details in the following of the document. At this stage we should not forget the basic functionalities of controlling the routing of the user data packets. On one hand, the Wi-Fi network is composed of network elements performing data forwarding and data packet processing, such as switches or routers, which can be considered not WLAN specific, while on the other hand WLAN AP requires routing data traffic from the wired interface to the UE over the Wi-Fi interfaces. In such cases the data routing shall take into account the WLAN, specifically for example, in defining the filter rules and the indication of the port on air interface. This issue needs further analysis.

6.3.1 Authentication support

SDN-enabled WLAN AP with authentication functionalities located in the SDN controller
In the SDN based architecture several architectural options can be considered. In the first option, the SDN controller replaces the role of the WLAN AC, where the authenticator function and the RADIUS client are part of the SDN controller as shown in Figure 6-9. The authentication interaction between the user device, SDN controller and AAA server shall be the same as in traditional deployment. The transport of EAP packets between the AP and WLAN AC, which is, for example, in current deployment encapsulated within CAPWAP, in SDN framework the EAP packets shall be transported over the South Bound Interface from the AP to the AAA radius server. In this deployment scenario the WLAN AP is SDN enabled supporting the SDN functionalities

Alternatively, when the authenticator is located in the WLAN AP, the SDN controller implements the AAA proxy functionalities as shown in Figure 6-10. This architecture option has the drawback that SDN controller is not limited to the decision of routing of packets and filtering, but it also implements control functionalities. In this scenario the Southbound interface from WLAN AP to SDN Controller may be a new SDN specific interface or RADIUS is used towards the SDN Controller. In the first case the SBI, for example it may be based on ONF-switch protocol where all RADIUS packets are encapsulated within the ONF protocol and forwarded to the SDN Controller. In the first scenario the WLAN AP shall be SDN enabled, since it shall support the specific SDN protocol and the related functionalities in a manner similar to scenario shown in Figure 6-9. At this stage, it is difficult to identify the differences, if any, between the scenario in Figure 6-9 and Figure 6-10, when the SBI interface is assumed to be based on a specific SDN protocol, since currently there is no standard solution defined.

In the second scenario mentioned, the WLAN AP is not SDN enabled and the interconnection with SDN controller is based on RADIUS protocol. The SDN controller may be seen, as above mentioned, as a simple AAA proxy, however the other functionalities of an SDN controller, such as exposure of sub-network, resource allocation, etc. These which are not strictly related to authentication, can be deployed.

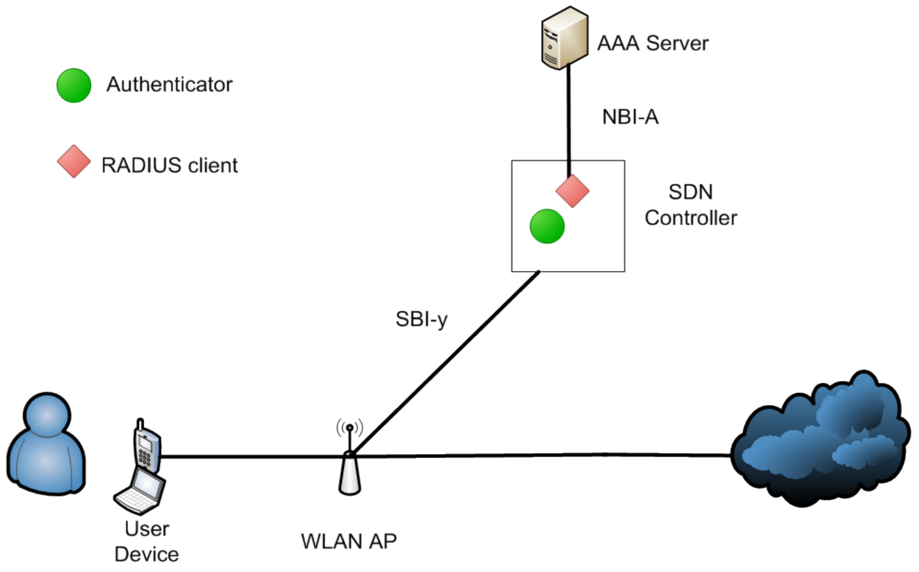


Figure 6-9 **Authentication IEEE 802.1x support for EAP-based authentication in Wi-Fi network based on SDN deployment with Authenticator and RADIUS client part of SDN Controller.**

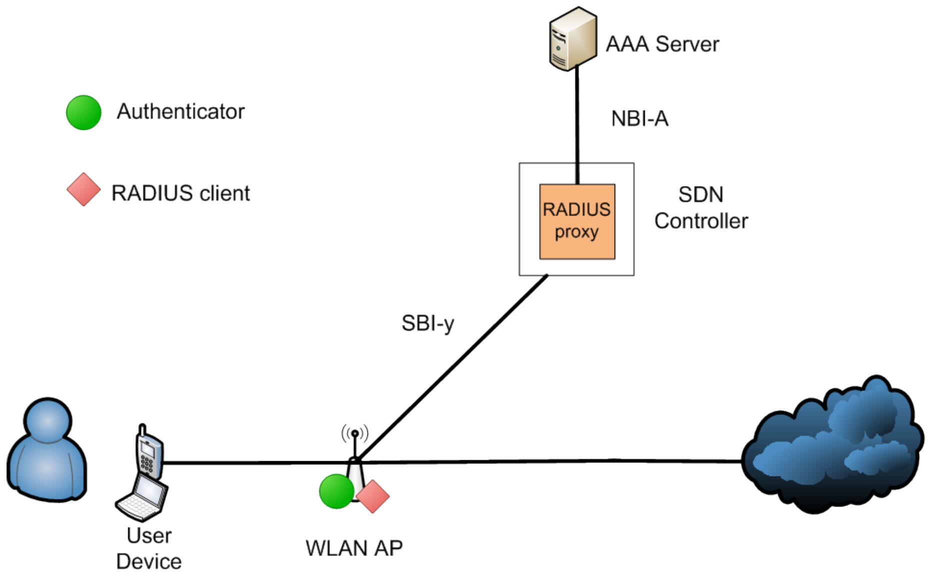


Figure 6-10 **Authentication IEEE 802.1 x supports for EAP-based authentication in Wi-Fi network based on SDN deployment with RADIUS proxy part of SDN Controller.**

SDN-enabled WLAN AP with authentication functionalities located in the Application layer
An alternative approach for improving seamless Wi-Fi authentication and authorization is to not involve the SDN controller in user authentication process but to allow an application to handle user authentication and to define a default policy template for this application so that it can authorize a user in the network. In other words, the SDN controller does not need to know who the user is, but the authentication application identifies the user and it can supply the right access control for the user. The SDN controller needs only to authorize the authentication application itself. This is really efficient since the controller does not become overwhelmed with unnecessary requests.

By considering these facts and the changes that are happening in the operators' network infrastructures to support SDN-based solution, there might be two different kinds of authentication application for user authentication -- an application produced by the operator itself and an application produced by a third party company who wants to allow their users to access the Internet by leasing a network from an operator.

SDN solutions can be used in two different scenarios – a non-roaming scenario with a single operator and a roaming scenario where there are multiple domains and multiple operators. Figure 6-11 illustrates a SDN scenario in the non-roaming case. In this scenario a user device is authenticated performing an EAP-based authentication via WLAN AP (1) . For example in case of support of ONF protocol on WLAN AP, as described above, the OF-switch forwards this request to a controller (2). Controller translates this request to RADIUS protocol and forwards it via a Northbound interface to the Authentication application which is acting as authenticator. The Authentication application processes this request interacting with an AAA server using RADIUS protocol (3) and after successful authentication, the application creates a message that is understandable by a SDN controller (REST-based language with standard format) to assign a switch port to this user so that he can have access to the network. The Authentication application may provide policy related to this user to the SDN controller which distributes them to the firewall, so that for example a new port can be opened in a firewall for this user (4) so that this user can continue using, e.g., VoIP service, while by default this service is not available to other user.

The behaviour described above is based on the new distribution of the WLAN functionalities among the WLAN AP, SDN controller and Authentication application. In addition, it is assumed that the WLAN AP is SDN capable, hence a new kind of WLAN AP.

From the SDN infrastructure point of view, the authentication is within the application so the SDN Controller passes only the request.

The simplest authentication mechanism for southbound devices is based on TLS. If other authentication mechanisms are also used in combination with TLS to authenticate a device, an additional authentication process may be requested in order that the controller does not accept any request from unknown WLAN AP. Therefore, in the first step, one of southbound REST standards such as OpenFlow, eflow, sflow, FORCE, etc. can be used to authenticate a SDN switch (OF-switch), in this case the WLAN AP. The switch, then, is authorized to submit the user authentication requests to the controller.

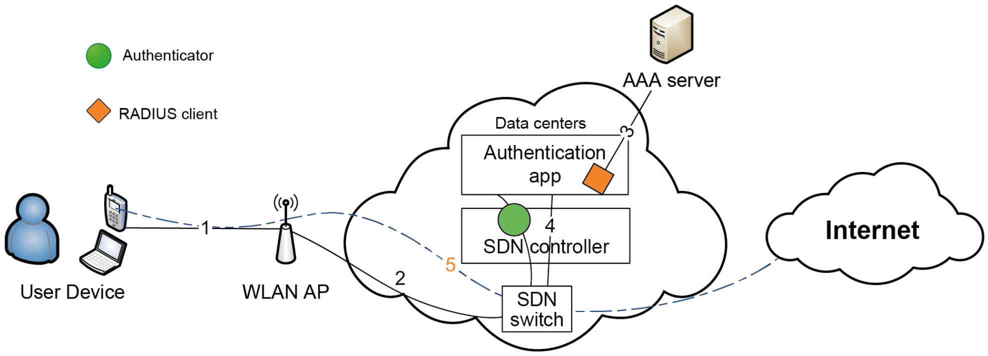


Figure 6-11 SDN Wi-Fi network architecture in non-roaming scenario

Figure 6-12 illustrates a roaming SDN scenario. In this scenario a user device authenticates to the WLAN AP via an EAP-based protocol. Since some recent versions of controller also support EAP frames, an OF-switch forwards this request to a controller. Similarly to the last scenario, the authentication might be in two steps. In the first step, one of southbound REST standards such as OpenFlow, eflow, sflow, FORCE, etc. can be used to authenticate a SDN switch (OF-switch). The switch, then, is authorized to forward the user authentication requests (i.e EAP message) to the controller. When a SDN controller in a visited network receives this request, it checks the domain name of the user and based on the domain, it forwards the request to home SDN controller where this user is a customer (2). A unit in the home SDN controller translates this request to RADIUS and forwards it to the authentication application. The authentication process between the SDN Controller, the authentication application and the AAA server in home Service provider network is performed as in the non-roaming scenario. After successful authentication, the authentication application may provide policy related to the user which is transmitted to SDN controller (foreign SDN controller). In the visited network, the foreign SDN controller, via the SDN controller in home network applies this policy in the user's visited network, after the foreign SDN controller authorized this application using SDNauth,

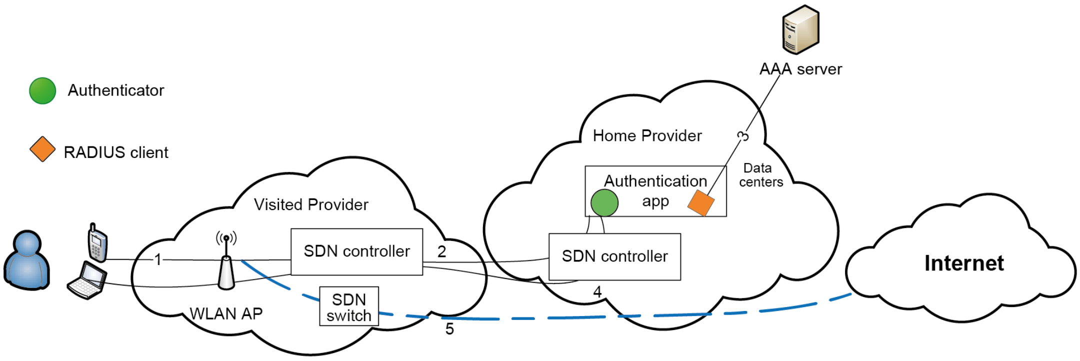


Figure 6-12 SDN Wi-Fi network architecture in roaming scenario

SDN-enabled authentication with Orchestrator layer for SDN authentication interconnection during roaming scenario

Besides the approach explained in the previous sections, there is another possible architecture to handle user authentication during roaming scenarios that is based on an orchestrator layer. Therefore, SDN controllers from different operators do not need to distinguish and trust each other for exchanging user information or allowing external application to execute on the SDN controller, but it is the orchestrator that is known and trusted by all SDN controllers. Figure 6-13 shows this scenario where the Orchestrator service provides the communications between two SDN controllers and communicates with authentication applications that might belong to different operators. This might be less complex than the direct communication between the two SDN controllers. It also puts the SDN controllers at less risk since there is only one point of communication to the SDN controllers which is the Orchestrator service.

In this model, the IP address, domain names (e.g. app1.operator1) and TLSA value [96] (certificates) are stored on a DNS server where this DNS server plays a role of PKI without the need of Certificates Authority (CA) [97]. This DNS server is local and might be maintained by the vendor where each operator can access its own zone and update the information of its own applications. Figure 6-13 shows this DNS server and its structure. This is the reliable source where the Orchestrator service can ask information about different applications.

When a user moves from the home domain to a visited domain (movement occurs) that belongs to different operators, an orchestrator service can provide the communication among applications so that the user session information can be exchanged among two different SDN controller via the orchestrator service and forwarded to a user authenticator application (Figure 6-13: step 2). This will eliminate the need for a user to also have credentials in its visited network and support a seamless authentication for this user. After the users request received by a SDN controller (via existing EAP protocol), SDN controller converts it to RADIUS protocol and encapsulates this request and adds a new header to this request so that it is understandable by the orchestrator service. Figure 6-14 shows an example encapsulation of RADIUS in another proposed protocol (SDNauth). The SDN controller then submits it to the orchestrator service (orch.operator2). orch.operator2 retrieves users domain (something like bob@app1.operator1) and queries a DNS server about the location of the user authenticator application (Figure 6-13: step 3); the one who knows this user, then after application authentication process is processed, that is based on TLS or certificates using DNS based PKI model [40], the user authentication is processed and the orchestrator forwards the controller's request to app1.operator1 (Figure 6-13: step 2). App1.operator1 decapsulates this request and forwards it to its RADIUS server components where it parses the request and queries an AAA server about user authorization information (Figure 6-13: step 4). This request is again encapsulated to SDNauth (Figure 6-14) and is forwarded to orch.operator2. Orch.operator2 processes the app1.operator1 authentication and then queries the resource policy database to retrieve authorization information for this application. Then it allows this application to have limited access to the SDN controller in the operator's domain to apply some rules on network devices, e.g. opening a port on switch so that the user can access the Internet (Figure 6-13: step 4).

Figure 6-15 shows the whole process.

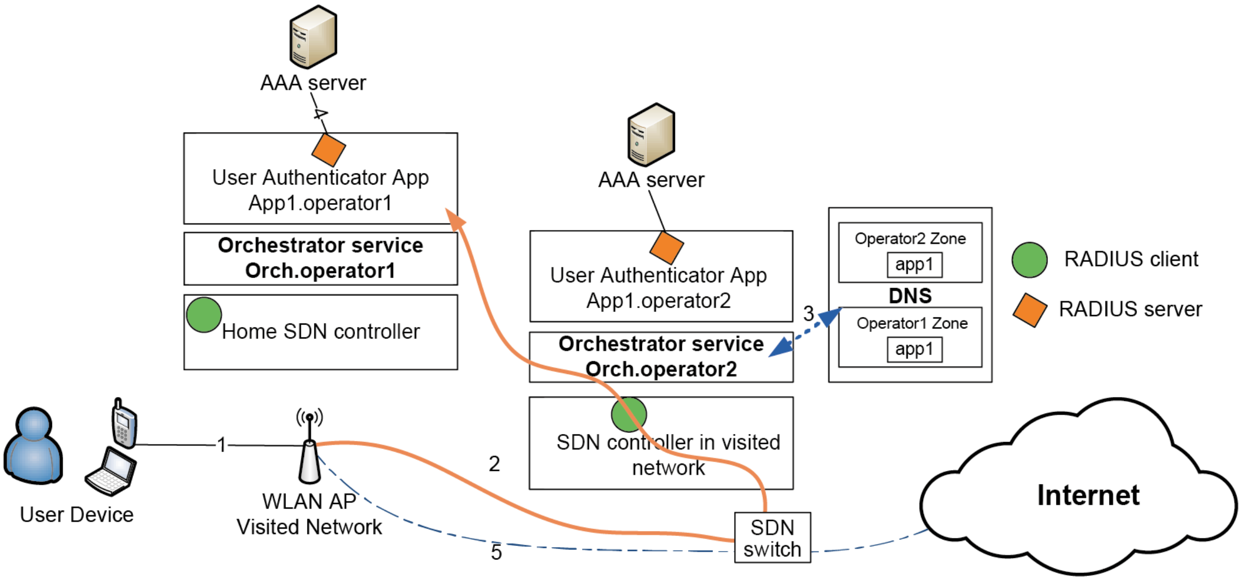


Figure 6-13 User authentication via the communications of two orchestrator services.

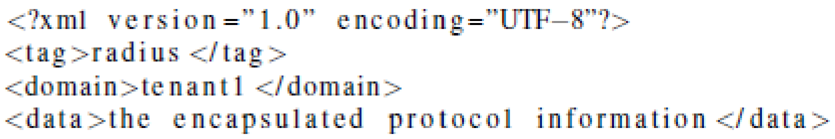

```
<?xml version="1.0" encoding="UTF-8"?>
<tag>radius </tag>
<domain>tenant1 </domain>
<data>the encapsulated protocol information </data>
```

Figure 6-14 Example of a protocol (SDNauth) to encapsulate RADIUS sent to an orchestrator service

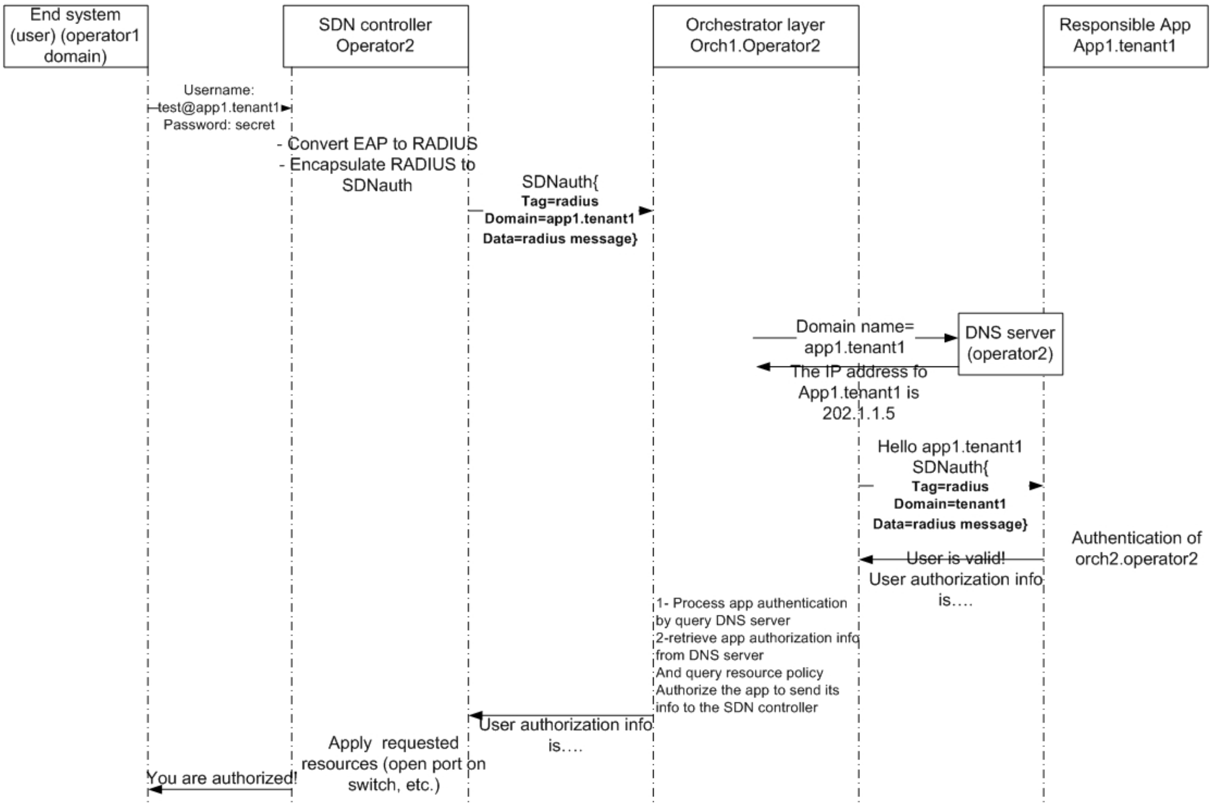

End system (user) (operator1 domain)
SDN controller Operator2
Orchestrator layer Orch1.Operator2
Responsible App App1.tenant1
Username: test@app1.tenant1 Password: secret
- Convert EAP to RADIUS
- Encapsulate RADIUS to SDNauth
SDNauth{ Tag=radius Domain=app1.tenant1 Data=radius message}
Domain name= app1.tenant1
DNS server (operator2)
The IP address fo App1.tenant1 is 202.1.1.5
Hello app1.tenant1 SDNauth{ Tag=radius Domain=tenant1 Data=radius message}
Authentication of orch2.operator2
User is valid! User authorization info is….
1- Process app authentication by query DNS server
2-retrieve app authorization info from DNS server
And query resource policy
Authorize the app to send its info to the SDN controller
User authorization info is….
Apply requested resources (open port on switch, etc.)
You are authorized!

Figure 6-15 **The process of user authentication request from the AP to a responsible application by the use of encapsulating the communications in SDNauth REST format**

WLAN AP with legacy authenticator connected to SDN-enabled aggregation network

Figure 6-16 shows the scenario of a Carrier Wi-Fi network where only SDN-enabled switches are deployed, in such scenario strictly speaking none of the Wi-Fi network elements supports SDN, but only the aggregation network is SDN-enabled. The SDN controller shall only instruct the SDN switch to route the packet transporting the EAP messages (such as CAPWAP) from the ingress to egress port without performing any specific action related to authentication process.

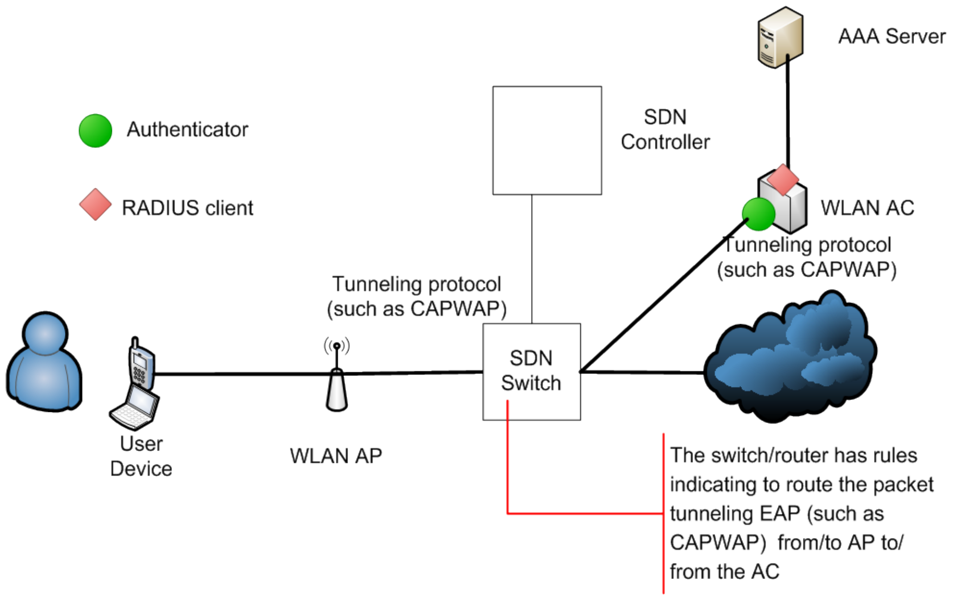


Figure 6-16 SDN Wi-Fi network architecture with unmodified Carrier Wifi network and SDN enabled switch.

Standardisation status

Since user authentication especially during roaming is a well-known problem, there are some recent research works to improve the authentication federation. Eduroam [98] is one of these research works. The purpose is to have authentication federation in academia. They use RADIUS and EAP protocols for user authentication. The implementation of this work started by some research institutions and now supported in more than 71 universities all around Europe. The idea behind this work is to access the Internet in all university campuses using a single token. However, this work is not related to a SDN solution. In IETF the ABFAB standard group [99] has the purpose to define authentication federation in the cloud. Their solution also doesn't support SDN.

SDNauth is a mailing list that works on proposals for the authentication and authorization of different SDN components from controller, to communication of applications together (via orchestrator layer). One of the important use cases in this proposal is User authentication with APs during roaming and non-roaming scenario.

In the future operators might receive their service from more than one vendor especially during roaming. Therefore, having interoperability between two controllers to exchange any information is really important. In SDNauth, to avoid hardware dependency and having a generalized solution, each SDN components were considered to be on data centers (cloud).

ONF within the Wireless and Mobile WG has Enterprise Project Team which has the scope to develop technical specification for the Enterprise use case for access using IEEE 802.1X for both wireless and wired network. The work is ongoing.

Considerations

In the section above, several possible architecture options have been described, but at this stage it is not possible to make any recommendation in respect to a preferable solution, since the standard work has not reached any conclusion and for the time being only ONF has a study on this topic and IETF is considering the issue. It is mentioned that IETF can have a role on developing elements of the solution. In general we can identify the lack of standard solution has a gap that needs to be filled in order to take the benefit of a common solution which cost a lot of effort in past time, but it now is seen as a mandatory requirement for enabling the seamless authentication and a smooth user experience. The support of EAP-based authentication is a foundation of the future Wi-Fi network and a foundation of the NGH experience, which shall be also supported in a SDN based network.

6.3.2 Accounting support

WBA defines the support of accounting inter-operator domain in WRIX-i [100], where the accounting information is exchanged for roaming scenario between the AAA proxy in the visited network and the AAA server in the home network. The RADIUS accounting protocol is usually deployed for Carrier Wi-Fi and it is bound to the RADIUS authentication process; so the architecture model and the potential solutions are related to the alternative described in clause 6.3.1

In WBA the interactions beyond the RADIUS AAA message exchanges are not standardized. In general the accounting information is created by the NAS within the WLAN AC or within the WLAN AP depending of the particular system architecture aligned with the authentication procedures.

The ONF defines in OpenFlow Switch specification [44] and [51] the capability to perform metering of traffic per flows. The metering is associated to counters which can be associated to each flow, port, queue, group, meter and meter band. For the details description of metering and counters please see clause 5.2.1. The ONF SDN Controller is able to indicate to the switch which elements (e.g. flows, ports, etc) shall be counted. The Controller can request to the switch to provide a requested statistic such as per single flow, per aggregate flows, per ports, etc. For example for the flow the switch can provide the following information:

- Time that flow has been alive
- Number of seconds in idle before expiring
- Number of seconds before expiring
- Number of bytes and packets in flow

These statistics can be used to derive the accounting information as requested per accounting purposed. However, how this is transformed in order to perform RADIUS accounting is not specified and currently there are no standardisation activities on this specific topic.

SDN-enabled WLAN AP with accounting functionalities located in the SDN controller
In first option the SDN controller replaces the role of the WLAN AC, where the accounting RADIUS client is part of the SDN controller as shown in Figure 6-17. The WLAN AP is SDN enabled and since the data traffic does not pass via the SDN controller, the WLAN AP shall perform collection of traffic statistics, for example as defined in OpenFlow switch specification, on the entities indicated by SDN controller. The collected statistics are provided to the SDN controller via the Southbound Interface, for example via OpenFlow protocol. Then the SDN controller performs the appropriate operations of interworking between the protocol used in SBI and the RADIUS protocol towards the AAA server, i.e. mapping the user identifier to the set of flows carrying the user traffic, aggregating the statistic in order to derive the accounting information as requested by the RADIUS server, etc. These operations may be not limited to a simple translation of messages, but additional operations may be required depending on the nature of the protocol used on the southbound interface.

Whether it is assumed that WLAN AP supports the metering capability specified by ONF for the Open Switch [51], the SDN Controller provides the indication on how to perform metering, e.g. per IP flow or per port, and how to perform the counting, e.g. per volume or time. Since the scope is the accounting, the SDN Controller shall be able to aggregate the traffic per single user or per operator depending by which accounting is performed. The SDN Controller shall be able to decide per each user how to meter the traffic, for example indicating to meter all traffic generated or received per user IP address or per IP flow or for any other aggregation and granularity which is required by the accounting model which needs to be implemented.

In addition the User can also move between WLAN APs, so the SDN Controller shall be able to track the user movement in order to indicate to the appropriate WLAN AP to perform the appropriate metering.

All above capabilities in the WLAN AP are not currently standardized as well as the accounting capability in SDN Controller.

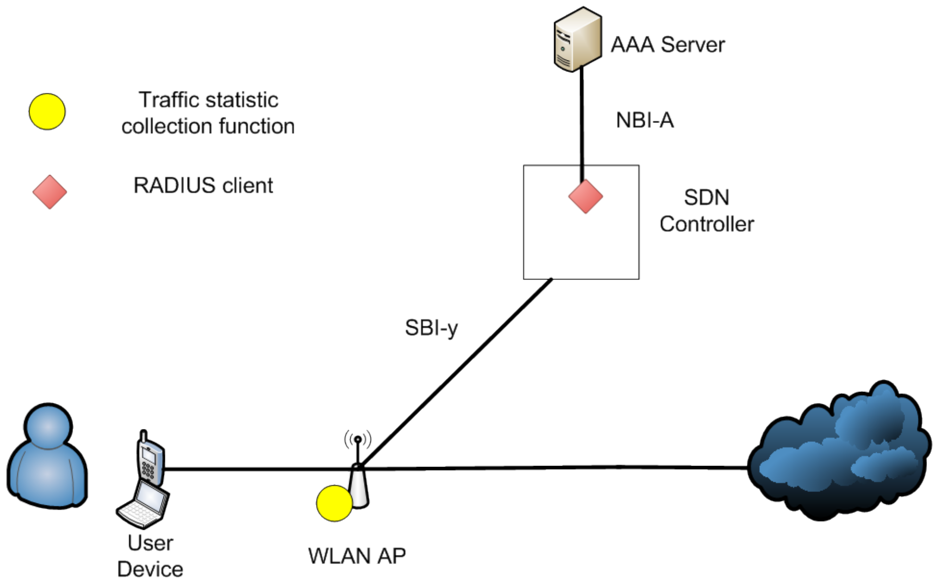


Figure 6-17 Traffic statistic function in WLAN AP with RADIUS client part of SDN Controller.

SDN-enabled WLAN AP with accounting functionalities located in the Application layer
The alternative approach is to have the accounting RADIUS client in the application layer, as shown in Figure 6-18 for the non-roaming scenario and Figure 6-19 for the roaming scenario. In this case the traffic statistic is collected in the WLAN AP, as described above for Figure 6-17, and it is transferred via the SBI interface to the SDN Controller which will forward via NBI interface to the Accounting Application. The SDN Controller may or may not perform elaboration of statistic and protocol translation between the protocol used in Southbound and Northbound interfaces depending by which protocols are used. The Accounting Application performs the interworking between the protocol used on northbound interface and RADIUS protocol used towards the AAA server.

In the roaming scenario the operator domains are connected via SDN Controllers which interact to transfer the traffic statistic information collected by the WLAN AP in the visited network with the home network. In addition other requests can also be exchanged in order to perform the appropriate accounting process.

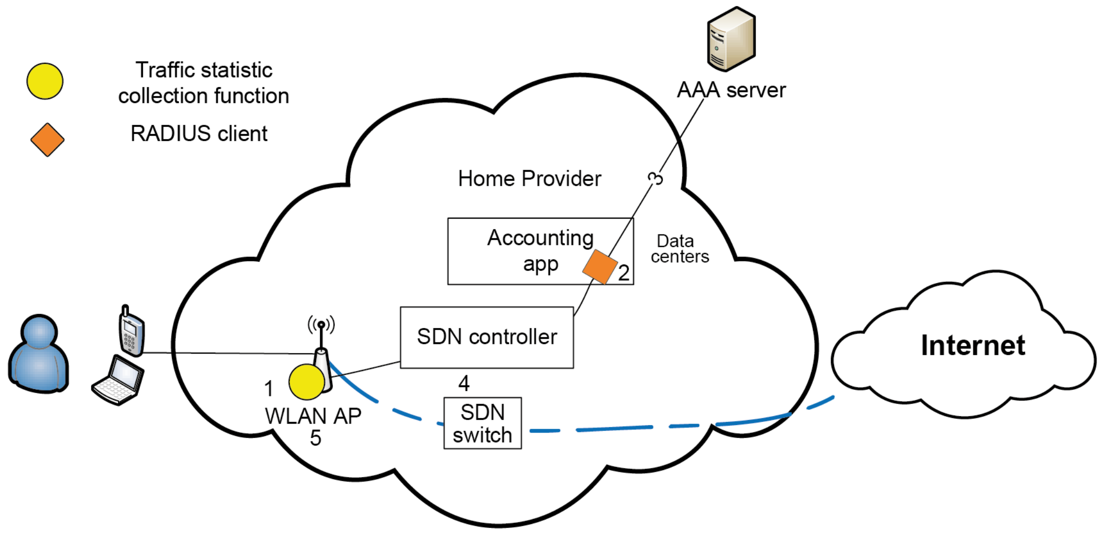


Figure 6-18 Accounting client in WLAN AP with RADIUS client in application layer.

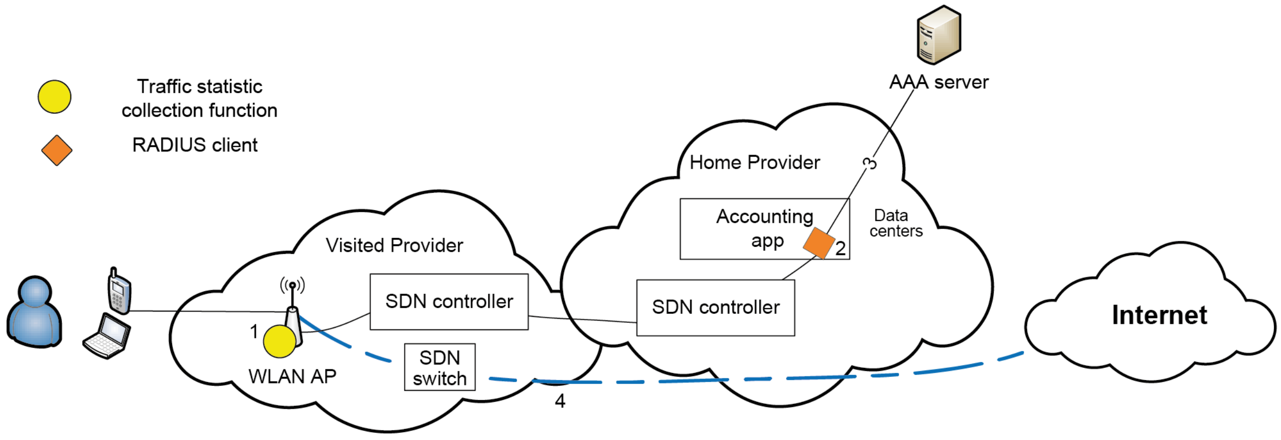


Figure 6-19 Accounting client in WLAN AP with RADIUS client in application layer in roaming scenario.

WLAN AP with legacy accounting connected to SDN-enabled aggregation network

Figure 6-19 shows the scenario of a Carrier Wi-Fi network where only SDN-enabled switches are deployed. In such a scenario, the SDN Controller shall only instruct the SDN switches to route the user flows, to the WLAN AC or to the Internet. In the case that all data traffic is tunnelled to the WLAN AC, the SDN Controller instructs the switches to route the traffic to the WLAN AC where the RADIUS accounting functionality is performed. Alternatively, if accounting functionality is performed in the WLAN AP, the SDN Controller instructs the switches to route the packet transferring the accounting information to the WLAN AC (this scenario is not described in the figure). In this approach basically the WLAN is not deployed using SDN framework, and the SDN framework shall configured to properly route the flows between WLAN AP and AC and all accounting process are performed independently by the SDN.

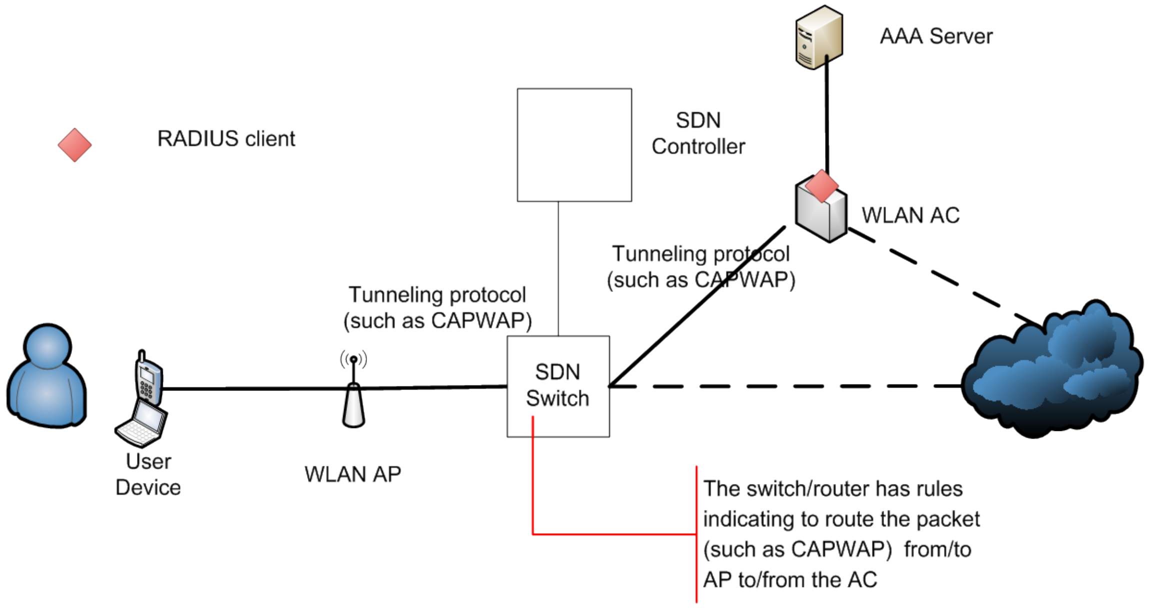

AAA Server
RADIUS client
SDN Controller
WLAN AC
Tunneling protocol (such as CAPWAP)
Tunneling protocol (such as CAPWAP)
SDN Switch
User Device
WLAN AP
The switch/router has rules indicating to route the packet (such as CAPWAP) from/to AP to/from the AC

Figure 6-20 SDN Wi-Fi network architecture with unmodified Carrier Wi-Fi network and SDN enabled switch.

Standardisation status
Currently ONF OpenFlow enables the collection of traffic statistics in the ONF switch and to provide them to the SDN controller, however there is no specific standardisation work on defining how OpenFlow features interwork with RADIUS. This is currently left to specific vendor implementation.

6.3.3 QoS support

In the Wi-Fi network the QoS is supported in the same was as any wired network via the marking of packets (e.g. DSCP marking of IP plackets) and the treatment of the packets based on the priority associated to the marking applying filtering, queuing and packet discarding. Specifically for the Wi-Fi interface, WFA has defined the WMM profile [101] for the treatment of the marking on the air interface.

In the QoS area, WBA has also recognised the importance of QoS with the introduction of real-time services (such as Voice and video) demanding more QoS control starting a new QoS project [102].

In QoS context OpenFlow, as described in clause 5.2.1, has a limited capacity to support QoS based on the treatment of packet based marking. However the configuration of treatment in the Openflow switch is not yet considered in Openflow. In that scenario we can assume that a WLAN AP SDN supporting OpenFlow may be capable to treat the packet based in the OpenSwitch procedure however the relationship between such treatment and WFA WMM profile is an open issue. For example, WMM allows configuring the association of packet marking (e.g. DSCP) to the WMM queues in the WLAN AP, but whether the OpenFlow can be used to configure such association or other mechanisms are needed is an open issue, or on other hand, whether OpenSwitch needs to be extended to support WMM specification.

In the previous clause we had considered the scenario of a WLAN AP which is not SDN enabled in a SDN enabled network. In such scenario the support of dynamic QoS and configuration of QoS policy is a more general issue of SDN framework not specific to a Wi-Fi network.

In conclusion, the support of QoS represents a gap and how such gaps can be solved is dependent on a more generic solution of supporting dynamic QoS in a SDN framework.

6.3.4 Mobility support

The support of mobility in a wireless system is a key feature that SDN should support, and several studies have been presented that consider a broad range of solutions, coming from the implementation of IP based mobility protocol in the SDN context to the usage of routing capability of the SDN, to new mobility protocols and solutions. Some studies address both the Wi-Fi network and future 5G network, while others are focused to. Also in Wi-Fi network. In this area, several proprietary SDN products address the support of mobility within the Wi-Fi network. The description of all these possible solutions, that a simple research on Google with keywords “Mobility SDN WLAN” will show[2] more than 300 000 results, so the analysis of all solutions is behind the scope of this whitepaper.

An example of a solution is provided in draft RFC draft-sarikaya-dmm-for-wifi-03 [103] where a distributed mobility management protocol, based on mobility aware virtualized routing system, with software-defined network support without any mobility client within the device. The routing is in Layer 2 in the access network and in Layer 3 in the core network. The protocol assumed the reference architecture shown Figure 6-21

The access network is connected to the Unified Gateway (the access routers at the border of the Wi-Fi network), which is a Layer 2 network where the Switches are SDN enabled. The device mobility is managed by the SDN Controller keeping the routing table dynamically updated using the association of the device IP address and the WLAN AP MAC address. The northbound interface can be ONF or any other extended protocol.

[2] Google shows for a research with “mobility AND SDN AND WLAN”” more than 338 000 references

When the device is moving between an area connected to different UG, an handover procedure takes place in order to transfer the user context between the two UGs. When this is performed the establishment of upstream route takes place. In this case it is assumed to use the NETCONF protocol and the YANG model. The old serving UG and the new serving UG perform handover and exchange of information using I2RS Agent and Client model.

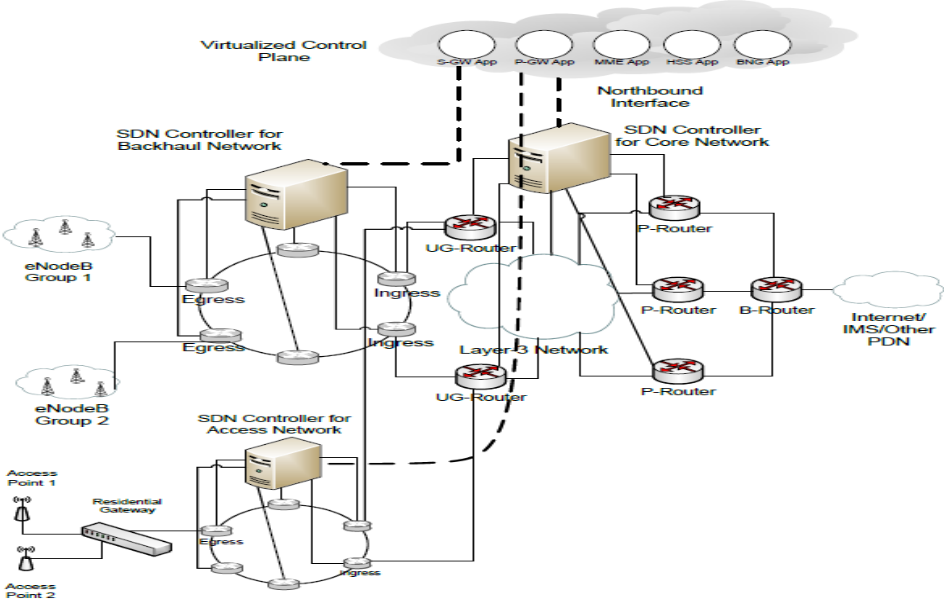


Figure 6-21 Reference architecture for [103]

6.3.5 Passpoint support

The support of Passpoint™ [104] [105] is considered an essential feature of the Carrier Wi-Fi network. Passpoint functionality is based on the feature supported in the user device, in the WLAN AP and the related server. From the SDN point of view, the interaction on the air interface, e.g. the exchange of ANQP messages, is totally independent by SDN. The Online Signup Procedure and the provisioning of profile includes interaction between the UE and the WLAN AP, via ANQP or via EAP exchange and interaction between the UE and the Servers such as AAA or Online Signup Server via IP connection; for example, the HTTP interaction with Online Signup Server for inserting subscription information and OMA DM or SOAP XML for provision of profile to the user device. These interactions, as discussed for Authentication, depend on the location of the servers, they may be part of the SDN Controller, but unlikely that it is a preferable solution as it introduces further complexity to the SDN Controller or the server that are connected via the Northbound interface to the SDN controller as shown in Figure 6-22. Alternatively they are connected to Wi-Fi network only via SDN-enabled switch as shown in Figure 6-23 where in this case the SDN Controller indicates to the Switch to forward the packet between the device, the WLAN AP and the servers.

In this area there is no standardising work ongoing in any SDOs and this is an open issue for the future.

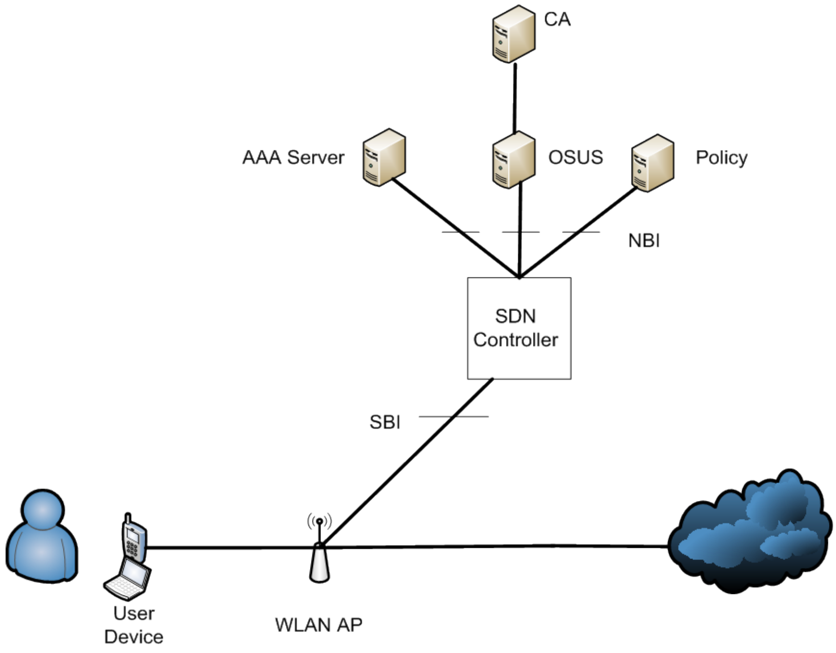
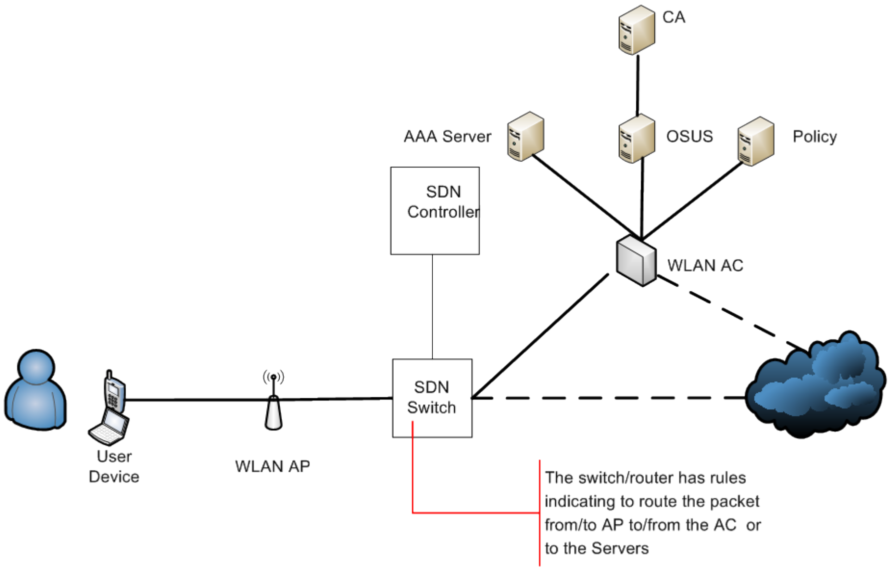


Figure 6-22 Passpoint in SDN Wi-Fi network architecture with WLAN AP SDN-enabled.



The switch/router has rules indicating to route the packet from/to AP to/from the AC or to the Servers

Figure 6-23 Passpoint in SDN Wi-Fi network architecture with unmodified Carrier Wi-Fi network and SDN enabled switch.

6.3.6 Business driver and market opportunity

The introduction of SDN-based Wi-Fi network will bring OPEX decrement through offering the network unprecedented programmability. Moreover SDN-based Wi-Fi network should maximize ARPU by improved customer experience to those subscribers who are most willing to pay for those benefits. The business driver and market opportunities are:

Cost reduction
Device with easy hardware and basic Wi-Fi network function would be welcome for SDN-based WLAN base Wi-Fi as further complex and strong network functions and applications can be developed by 3rd parties with standard APIs. Low cost Wi-Fi devices can save most of the Wi-Fi network deployment CAPEX, which will attract small operators or enterprises to participate in Wi-Fi investment.

Increase revenue
SDN-based Wi-Fi networks should not only provide basic Internet access, but also enable 3rd parties, such as other operator/OTT/enterprise, to deploy new applications and services as a win-win scenario. For example, advertisement or voice/video revenues can encourage more operators or enterprises to deploy Wi-Fi networks. A more quick and easy deployment of application and services increases the ARPU of Wi-Fi networks.

Flexible deployment and OPEX reduction
Easy deployment, upgrade and maintenance and a flexible allocation of the resources and features decreases the provision and configuration time, manpower cost, and reduces the operational costs.

User experience
A better user experience is a key element for modern telecommunications and it plays a key role for Wi-Fi networks for moving from a "free all you can eat" business model to a "pay for services" model. Carrier Wi-Fi goes in this direction and so the SDN-based Wi-Fi networks shall from this starting point move further ahead in providing an improved user experience.

Network collaborative control with 3rd operator/OTT/enterprise
SDN frameworks allow sharing Wi-Fi network among operators or OTT for the most efficient network utilization and for increasing monetisation, for example, the access control function of Wi-Fi networks can be exposed via APIs to a social OTT application or to other operators via the SDN controller or alternatively exposing a portion of Wi-Fi network resources for a wholesale model network. The user can access the Wi-Fi network using the accounts of the OTT or of the other operators. Network collaborative control with 3rd operator/OTT/enterprises enables the user to access Wi-Fi networks when roaming at an attractive price, while the operator can extend its WLAN coverage. Furthermore, network owners can increase its monetisation of Wi-Fi networks.

User and network information collection and push (e.g. data mining,)
Wi-Fi network is a source of valuable information about the customers of venues such as shopping malls, enterprises, hospitals, scenic spots, etc, which can help the venue owner to enhance the user experience and the efficiency or the profitability of its business. For example shopping malls would like to invite people to visit the mall, the enterprise network administrator may wish to know the coverage and performance of the Wi-Fi network, the hospital would like to have access to patient information, the scenic spot manager may want to know tourist behaviour, habits or from where they come from. On the other hand users in a huge building, such as mall or airport, would like more easily to find the places of interest and reach them more easily and quickly. Thanks to the SDN approach the data mining and the exposure of network information would be more efficient, flexible and target the portion of network and resource of interest, so the Wi-Fi network operator or 3rd party OTT can collect this data by standard APIs and push information to the user or allow the venue to collect the information useful to them with data mining.

Wi-Fi network function customization
SDN deployment allows the Wi-Fi network owner to customize the network function by selectively exposing network capability and resources to any operator/OTT/enterprise. The network functions may be also be seen as modules or processes hosted on SDN controllers which can be download from a Wi-Fi network function application server as applications which interact with the network via a Northbound API. In such scenarios the network function applications can be developed by application companies, operators, etc. Wi-Fi network function customization enables new deployment models, where operator A can co-operate with OTT B to provide free films to the user, while enterprise C can co-operate with OTT D to provide a VoIP service.

By now, if an operator wants to push a new network function like video/voice or location base server, the operator needs to develop a specific server which may take a long time, in addition for some applications the user device shall be equipped with the suitable operative system or application usually provided by the device vendor. Nevertheless, with standard APIs, SDN controllers can facilitate to cooperate with OTTs, so service and applications can be quickly and conveniently deployed on the Wi-Fi network.

7. Recommendations, GAP Analysis and challenges

7.1 NFV

7.1.1 Gaps and challenges

Although NFV and SDN provide tremendous opportunities to automate the life cycle management (LCM), service installation, and service mobility; these new technologies bring a number of challenges. Below are some of the identified gaps and challenges:

New services or platforms deployed in an NFV environment will have to integrate with existing non-virtualized environments. There is little guidance to define the integration of the virtualized and non-virtualized management systems, thereby making it difficult to manage services that span across the two domains.

Integration between NFV and SDN needs more definition and standardization. There are a number of integrated deployment options highlighted in this paper but there are no clear recommendations or details for these deployments.

NFV and SDN introduce new security challenges as a result of the additional layers between the hardware and the applications as well as the ability to host multiple tenants on the same environment. These new security challenges need to be explored and mitigated.

There is a need to address application resilience in the new environment. Traditionally, the resilience is built into the integrated hardware and software to ensure the availability required for each application. With the separation between the hardware and the application, new techniques are now needed when building the applications and designing for their deployment to meet the same resilience requirements.

7.2 SDN

7.2.1 Gaps and challenges

The previous clauses have described the standardisation landscape and the possible deployment options for a Wi-Fi network based on SDN. Several SDOs are working on the area developing different aspects and in some cases with alternative proposals and approaches for the same use cases. The normative work is progressing, mainly considering the routing and the fixed network while in the wireless area the discussion on the future 5G is just being initiated. Carrier Wi-Fi is composed of two set of elements, the first one not WLAN specific such as routing and switching elements and a second one more WLAN specific, such as WLAN AP, WLAN AC, and servers. The Wi-Fi network needs to support specific functionalities such as IEEE 802.1X and EAP-based authentication, Passpoint, etc. For non- WLAN specific elements one of the solutions proposed in standards or under study can be adopted, roughly transparently to the Wi-Fi network. Whilst for the WLAN specific functionalities at this stage no specific standardisation work has been completed or they have not yet been addressed, this represents a gap and challenges for future Wi-Fi network.

A challenge for Wi-Fi networks (and, in general, for networks supporting user mobility) is how the mobility should be supported. This aspect represents a challenge since it is addressed in several studies, but for the time being there is no clear direction. The standardisation landscape shows a scenario where the Wi-Fi network is marginally considered in ONF despite its being widely present in current networks. The main SDOs defining specification for mobile network, the 3GPP, hash recently kicked off a study for 5G where SDN would probably play an important role as well as the Wi-Fi network and other access technologies. At the same time, BBF is doing consistent studies on use cases, applicability and migration of fixed broadband access to SDN. Even though nowadays the Wi-Fi network plays a major role in both networks, for example integration in smartphones, for Voice over Wi-Fi network, and in fixed broadband access networks where the majority of residential gateway is equipment with a Wi-Fi interface, there is a substantial lack of requirements and of use cases addressing the Carrier Wi-Fi scenario and future evolution. Considering WBA knowledge of service provider's needs, it can play a fundamental role in filling the gap in the area of the definition of use cases and the requirements specific to the Wi-Fi network in order to provide valuable indication to other SDOs more deeply focused on development of technical solutions (e.g. architecture, protocols, etc) which are on the contrary are not within the WBA scope. Furthermore, the lack of a clear definition of use cases and requirements do not allow selection among the various proposals, since they cannot be compared and analysed against the desired objectives

8. Next steps for WBA

The path toward the introduction of NFV and SDN in future network is becoming more and more reasonable; however WLAN is not properly addressed. The whitepaper shows that WBA can consider working in the development of the definition of use cases and of related requirements specific to the migration towards a Carrier Wi-Fi network based on NFV and/or SDN.

The identified gaps and challenges will be evaluated and communicated with the appropriate SDOs for their consideration.

References

Ref	Document Number	Title
[1]	ETSI GS NFV 003	Network Functions Virtualisation (NFV);Terminology for Main Concepts in NFV
[2]	ITU-T Y 3300	Framework of software-defined networking
[3]	WBA	Next Generation Hotspot (NGH) Phase 3 Trial Scope Document
[4]	WBA	Next Generation Hotspot (NGH) Phase 3 Trial Test Plan
[5]	WRIX-i, WRIX-d, WRIX-f, WRIX-L	Wireless Broadband Alliance standards document that deals with the respective aspects of inter-operator data exchange as identified by the single letter subject area suffix: -i for Interchange deals with Walled Garden and AAA aspects; -d for Data deals with the exchange of summary usage data in the clearing process; -f for Financial deals with the financial aspects of the settlement process
[6]		ICP
[7]	Carrier Wi-Fi Guidelines	Carrier Wi-Fi Guidelines
[9]	BBF WT-359	A Framework for Virtualization
[10]	BBF WT-345	Migrating to NFV in the context of WT-178
[11]	BBF WT-328	Virtual Business Gateway
[12]	BBF SD-365	Definition of an SDN Reference Model
[13]	BBF WT-358	Support for SDN in Access Network Nodes
[14]	ETSI NFV	http://www.etsi.org/technologies-clusters/technologies/nfv
[15]	ETSI NFV Proof of Concept	http://www.etsi.org/technologies-clusters/technologies/nfv/nfv-poc
[16]	ETSI GS NFV-MAN 001	Network Functions Virtualisation (NFV); Management and Orchestration
[17]	3GPP TR 32.842	Study on network management of Virtualized Networks
[18]	3GPP TS 28.500	Management concept, architecture and requirements for mobile networks that include virtualized network functions
[19]	3GPP TS 28.510	Configuration Management for mobile networks that include virtualized network functions
[20]	3GPP TS 28.515	Fault Management for mobile networks that include virtualized network functions
[21]	3GPP TS 28.520	Performance management for mobile networks that include virtualized network functions
[22]	3GPP TS 28.525	Lifecycle management for mobile networks that include virtualized network functions
[23]	IETF NFVRG	Network Function Virtualization Research Group (NFVRG), https://irtf.org/nfvrg
[24]	IETF SFC	Service Function Chaining, https://datatracker.ietf.org/wg/sfc/charter/
[25]	IETF NVO3	Network Virtualization Overlays, https://datatracker.ietf.org/wg/nvo3/charter/
[26]	IETF BESS	BGP Enabled Services, https://datatracker.ietf.org/wg/bess/charter/
[27]		Y. Lee and al., “Problem statement for Abstraction and Control of Transport Networks”, Internet draft. [Online]. Available at: https://datatracker.ietf.org/doc/draft-leeking-teas-actn-problem-statement/?include_text=1
[28]	IETF TOSCA NFV	TOSCA Simple Profile for Network Functions Virtualization (NFV) Version 1.0 , http://docs.oasis-open.org/tosca/tosca-nfv/v1.0/csd01/tosca-nfv-v1.0-csd01.pdf
[29]	BBF WT-345	Migrating to NFV in the context of WT-178
[30]	BBF WT-359	A Framework for Virtualization
[32]	BBF WT-317	Network Enhanced Residential Gateway (NERG)
[33]	BBF SD-340	Stage 1 for introduction of Network Function Virtualization MSBN
[34]	BBF SD-326	Flexible Service Chaining
[35]	ATIS NFV Forum	http://www.atis.org/nfv/index.asp
[36]	ATSI NFV ATIS-0200012	ATIS NFV Forum Use cases , https://access.atis.org/apps/group_public/download.php/22973/NFV-Forum-Use-

Ref	Document Number	Title
		Cases.pdf
[37]	IEEE SRPSDVE	Security, Reliability, and Performance for Software Defined and Virtualized Ecosystems, http://grouper.ieee.org/groups/srpsdv/
[38]	ONF	Software Defined and Virtualized Wireless Access, http://community.comsoc.org/groups/rg-software-defined-and-virtualized-wireless-access
[39]	ONF	F. Granelli, A. A. Gebremariam, M. Usman, F. Cugini, V. Stamati, M. Alitska, and P. Chatzimisios, “Software defined and virtualized wireless access in future wireless networks: scenarios and standards,” IEEE Communications Magazine, vol. 53, no. 6, pp. 26–34, Jun. 2015.
[40]	ONF	SDN/NFV—Structured Abstractions , [http://community.comsoc.org/groups/research-group-sdnnfv-structured-abstractions
[41]	ONF	Open Network Function Virtualization, https://www.opnfv.org/
[42]	arXiv:1406.0440v3	“Software-Defined Networking: A comprehensive survey” D. Kreutz, M.V. Ramos, P. Verissimo, C. E. Rothemberg, S. Azodolmolky, S. Uhlig, IEEE version 2.01 October 2014 (http://arxiv.org/pdf/1406.0440.pdf)
[43]	IEEE Communication Surveys & Tutorials, Vol 16, No 4, Fourth Quarter 2014	A Survey on Software-Defined Networt and OpenFlow: from Concept to Implentation” Fei Hui, Qi hao, Ke Biao.
[44]	ONF	SDN architecture, issue 1, June 2014 (https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf)
[45]	ONF OP_CONFIG (1.2)	OpenFlow Management and Configuration (version 1.2) Protocolhttps://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow-config/of-config-1.2.pdf
[46]	ONF	Wireless and Mobile Working Group Charter
[47]	ONF	OpenFlow™-Enabled Mobile and Wireless Networks, ONF Solution Brief September 30, 2013
[48]		A.Ishimori, F. farias, I. Furtado, E. Cerquiera, and A. Abelem, “Automatic QoS management on OpenFlow Software-Defined network”, 2012 http://copelabs.ulusofona.pt/scicommons/index.php/attachments/single/373
[49]		UC Software Defined Networking (UC SDN) Activity Group, http://www.imtc.org/uc/ucsdn-work-group/
[50]	UC SDN	Automating Unified Communications Quality of Experience using SDN http://lp.imtc.org/IMTC-SDN
[51]	ONF Open Switch (1.3.4) ONF Open Switch (1.4.0)	Open Switch Specification (version 1.3.4) (https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.3.4.pdf) Open Switch Specification (version 1.4.0) https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf
[52]	IETF RFC 7285	Application-Layer Traffic Optimization (ALTO) Protocol
[53]	IETF RFC 7426	Software-Defined Networking (SDN): Layers and Architecture Terminology
[54]	IETF RFC 7149	Software-Defined Networking: A Perspective from within a Service Provider Environment
[55]	IETF RFC 3746	Forwarding and Control Element Separation (ForCES) Framework
[56]	IETF RFC 5810	Forwarding and Control Element Separation (ForCES) Protocol Specification
[57]	IETF RFC 5812	Forwarding and Control Element Separation (ForCES) Forwarding Element Model
[58]	IETF	SDN&NFV OpenFlow and ForCES IETF---93 http://ietf.org/edu/tutorials/sdn-nfv-openflow-forces.pdf

Ref	Document Number	Title
[59]	FORces tutorial;	Network Programmability With ForCES, Communications Surveys & Tutorials, IEEE (Volume:17 , Issue: 3), http://dx.doi.org/10.1109/COMST.2015.2439033
[60]	BBF SD-313	High Level Requirements and Framework for SDN in Telecommunication Broadband Networks
[61]	IEEE P1903.1	Standard for Content Delivery Protocols of Next Generation Service Overlay Network (NGSON)
[62]	IEEE P1903.2	Standard for Service Composition Protocols of Next Generation Service Overlay Network (NGSON)
[63]	IEEE P1903.3	Standard for Self-Organizing Management Protocols of Next Generation Service Overlay Network (NGSON)
[64]	P802.1CF project status	http://www.ieee802.org/1/pages/802.1cf.html
[65]	OmniRAN TG status	https://mentor.ieee.org/omniran/bp/StartPage
[66]	OmniRAN SDN Wiki	https://mentor.ieee.org/omniran/bp/SDN_Wiki
[67]	ITU-T JCA-SDN	Term of reference http://www.itu.int/en/ITU-T/jca/sdn/Documents/ToR-JCA-SDN.pdf
[68]	ITU-T JCA-SDN-D-001 Rev.2	https://www.itu.int/ifa/t/jca/sdn/DELIVERABLES/jca-sdn-D-001r2-sdn_standard-roadmap-20150717.docx
[69]	ITU-T Q.Suppl. 67	Framework of signalling for software-defined networking
[70]	ITU-T Draft Q.PVMapping	Signalling Requirements for Mapping between Physical and Virtual Networks
[72]	ITU-T Y 3321	Requirements and capability framework for NICE implementation making use of software-defined networking technologies
[73]	ITU-T Y 2301	
[74]	ITU-T Y 3320	Requirements for applying formal methods to software-defined networking
[75]	ITU-T Y.SDN-usecases	Use cases of Telecom SDN
[76]	ITU-T Y.SDN-req,	Functional requirements of software-defined networking
[77]	ITU-T Y.SDN-arch	Functional architecture of software-defined networking
[78]	ITU-T Draft G.astdn	Architecture for SDN control of Transport Networks
[79]	ITU-T Draft X.sdnsec-1	Security services using the Software-Defined Networking
[80]	ITU-T Draft X.sdnsec-2,	Security requirements and reference architecture for Software-Defined Networking

[81]	ETSI GS NFV-EVE005	Network Functions Virtualisation (NFV);
		Ecosystem;
		Report on SDN Usage in NFV Architectural Framework

[82]	ETSI GS NFV 002	Network Functions Virtualisation (NFV); Architecture Framework
[83]	ETSI GS NFV 001	Network Functions Virtualisation (NFV): Use Cases
[84]	IETF RFC 5415	Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
[85]	IETF RFC 5416	Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
SCF-106 [86]	Small Cell Forum SCF-106	Virtualization for small cells: overview
[87]	3GPP TR 23.842	Study on network management of virtualized networks
[88]	IETF draft-ietf-opsawg-capwap-alt-tunnel	Alternate Tunnel Encapsulation for Data Frames in CAPWAP
[89]	IEEE 802.1x	Port-Based Network Access Control
[90]	IETF RFC 3748	Extensible Authentication Protocol (EAP), June 2004
[91]	IETF RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM), , January 2006
[92]	IETF RFC 4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), , January 2006
[93]	IETF RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'), May 2009
[94]	IETF RFC 5216	The EAP-TLS Authentication Protocol, March 2008

Ref	Document Number	Title
[96]	IETF RFC 6698	TLSA record https://tools.ietf.org/html/rfc6698
[97]	IETF presentation of DNS based PKI model	https://www.ietf.org/proceedings/93/slides/slides-93-sdnrg-3.pdf
[98]	IETF draft Eduroam	The eduroam architecture for network roaming http://tools.ietf.org/html/draft-wierenga-ietf-eduroam-05
[99]	IETF ABFAB WG	IETF ABFAB Charter https://tools.ietf.org/wg/abfab/charters
[100]	WBA WRIX-i	
[101]	WFA WMM	WMM Specification v1.2
[102]	WBA	WBA QoS project
[103]	IETF draft RFC draft-sarikaya-dmm-for-wifi-03	Distributed Mobility Management Protocol for Wifi Users in Fixed Network
[104]	WFA Hotspot 2.0 Release 1 Specification	Wi-Fi Alliance Release 1 specification for the WFA Passpoint™ Certification Program
[105]	WFA Hotspot 2.0 Release 1 Specification	Wi-Fi Alliance Release 2 specification for the WFA Passpoint™ Certification Program

Acronyms and Abbreviations

Term	Description
AAA	Authentication, Authorization and Accounting, core functions commonly implemented through protocols like RADIUS and Diameter
ABFAB	Application Bridging for Federated Access Beyond web
ACTN	Abstraction and Control of Transport Networks
AN	Access Node
ANDSF	Access Network Discovery and Selection Function
ANQP	Access Network Querying Protocol
ANQP-IE	ANQP Information Element
AP	Access Point
API	Access Programming Interface
ARPU	
BBF	Broadband Forum
BESS	BGP Enabled Services
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BoF	Board of Father
BRG	Bridged Residential Gateway
BSS	When one access point (AP) is connected to a wired network and a set of wireless stations, it is referred to as a Basic Service Set (BSS).
BSSID	Basic Service Set Identification
CA	Certificates Authority
CAPWAP	Control And Provisioning of Wireless Access Points (RFC 5415)
CWLAN	Carrier Wi-Fi
DC	Data Center
Diameter	Authentication, authorization and accounting protocol for computer networks, and a successor to RADIUS . (IETF RFC 3588 [54])
DMTF	Distributed Management Task Force
DNS	Domain Name Server
DoS	Denial of Service
DPCF	Data Plane Controller Function
DPI	Deep Packet Inspection
EAP-AKA	Authentication method used with EAP to support authentication using a USIM, providing USIM Authentication and Key Agreement, as standardized in RFC 4187 (tools.ietf.org/html/rfc4187)
EAP-AKA’	Authentication method used with EAP to support authentication of EAP-AKA on networks that are not 3GPP compliant for 3GPP compliant devices, i.e. a device with a USIM wanting to authenticate on a Wi-Fi network would use EAP-AKA’, as standardized in RFC 5448 (tools.ietf.org/html/rfc5448)
EAP-SIM	Authentication method used with EAP to support authentication using a SIM, as standardized in RFC 4186 (tools.ietf.org/html/rfc4186)
EAP-TLS	Authentication method used with EAP to support authentication through Transport Layer Security, in which secure digital certificates are used to mutually identify a user and a server’s identity, as standardized in RFC 5216 (tools.ietf.org/html/rfc5216)
EAP-TTLS	Authentication method used with EAP to support authentication through Tunnelled Transport Layer Security, in which secure digital certificates are used to identify a server’s identity (and optionally, a device’s or user’s identity), establish a tunnel, and then allow for user identification over the encrypted tunnel, as standardized in RFC 5281 (tools.ietf.org/html/rfc5281), Note that there is often an inner EAP method used with EAP-TTLS, such as MSCHAPv2 (see RFC 2759)
EM	Element Manager
ESS	Extended Service Set: A set of two or more BSSs that form a single sub network.

Term	Description
ETSI ISG	ETSI Industry Specification Group
ForCES	Forwarding and Control Element Separation
HLR	Home Location Register
HSS	Home Subscriber Server
ICP	WBA’s Interoperability Compliance Program
IEEE 802.1	Institute of Electrical and Electronics Engineers LAN/MAN Standards committee 802 - Working Group 1
IEEE 802.11	Institute of Electrical and Electronics Engineers LAN/MAN Standards committee 802 - Working Group 11 is a standard for implementing wireless local area network (WLAN) computer communication (http://www.ieee802.org/11/)
IETF	Internet Engineering Task Force, a body for the development and promotion of standards for and related to the Internet. (www.ietf.org)
IPv6	Internet Protocol version 6
IRTF	Internet Research Task Force
JCA-SDN	Joint Coordination Activity on Software-Defined Networking
MAC	Media Access Control Address
NAT	Network Traversal Translation
NE	Network Element
NERG	Network Enhanced Residential Gateway
NFV	Network Virtualisation Function
NFVI	NFV Infrastructure
NFV-MANO	NFV Management and Orchestration
NFVO	NFV Orchestrator
NFVRG	Network Function Virtualization Research Group
NGH	Next Generation Hotspot
NMS	Network Management System
NOC	Network Operations Centre
NVO3	Network Virtualization Overlays
OASIS	Advancing Open Standards for the Information Society
OMA DM	Device management protocol specified by the Open Mobile Alliance (OMA) Device Management (DM) Working Group and the Data Synchronization (DS) Working Group
OPNFV	Open Network Function Virtualization
OSU	Online Signe Up
PKI	Public Key Infrastructure
PMF	Protected Management Frames (see IEEE 802.11w)
PoC	Proof of Concept
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service, a commonly used service for Authentication of user identity, Authorization of user service, and Accounting for service usage, as defined in IETF RFC 2865 and its many associated RFCs (tools.ietf.org/html/rfc2865)
RDB	Resource Database
RFC	Request For Comments, the acronym used to identify IETF standards.
RG	Residential Gateway
SDN	Software Defined Network
SDNRG	Software Defined Networking Research Group
SDO	Standard Developing Organisation
SFC	Service Function Chaining
SFP	Service Function Path
SIM	Subscriber Identity Module, earlier a chip-based module that provides the identity for a mobile subscriber which is included in mobile phones using the GSM system. Nowadays an application that resides in UICC

Term	Description
SNMPv3	Simple Network Management Protocol v3
SON	Self-Organising Network
SRPSDVE	Security, Reliability, and Performance for Software Defined and Virtualized Ecosystems
SSID	Service Set identification
STA	Station, WFA term for UE or AP
TEAS	Traffic Engineering Architecture and Signaling
TLS	Transport Layer Security
TLSA	Note from IETF RFC 6698 [96] clause 1.2 "TLSA" does not stand for anything; it is just the name of the Resource Record type
TOSCA	Topology and Orchestration Specification for Cloud Applications
UICC	Universal Integrated Circuit Card is the smart card used in mobile terminals in GSM and UMTS networks.
USIM	Authentication application that resides on UICC and provides AKA authentication for UMTS networks
vG	virtual Gateway
VIM	Virtualised Infrastructure Manager
VNF	Virtualized Network Function
VNFM	VNF Manager
WBA	Wireless Broadband Alliance, industry group made up of primarily Wi-Fi network operators and equipment vendors to further the use of wireless technologies. (www.wballiance.org)
WFA	Wi-Fi Alliance (www.wi-fi.org)
Wi-Fi	Originally called Wireless Fidelity, Wi-Fi is a wireless air interface/technology that allows an electronic device to exchange data wirelessly over a computer network, including high-speed Internet connections
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Access Network
WLAN SS	WLAN SON Sever
WPA2	Wi-Fi Protected Access II

Participant List

Company
Accuris Networks
Alcatel Lucent
AT&T
BIGLOBE Inc.
Boingo Wireless
Broadcom
China Mobile
Cisco
Comcast
Ericsson
Fon
Gemalto
Huawei Technologies
Liberty Global
Meteor Network
Nokia
NTT DOCOMO
Orange
Ruckus Wireless
Smith Micro Inc.
Spirent
Sprint
Syniverse Technologies
Telstra
Time Warner Cable