|  |  |
| --- | --- |
| INTERNATIONAL TELECOMMUNICATION UNION | **Joint Coordination Activity  On Software Defined Networks** |
| **TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | **JCA-SDN-D-001 Rev.5** |
| **English only****Original: English** |
|  | Geneva, 9 February 2017 |
| **DOCUMENT** |
| **Source:** | Editor of the SDN standardization activity roadmap |
| **Title:** | Update of the SDN standardization activity roadmap |

**Version**

This document represents the sixth official version of the SDN standardization activity roadmap (JCA-SDN-D-001r5), first deliverable of the JCA-SDN. It has been produced by the editor after the 10th JCA‑SDN meeting (Geneva, 9 February 2017), according to all the inputs received and as agreed by the 9th JCA-SDN meeting (Geneva, 30 June 2016) and 10th JCA-SDN meeting (Geneva, 9 February 2017. NOTE – The revision marks show the changes from the previous version of this roadmap (JCA-SDN-D-001r4).

***Editor’s note: status and open points of this sixth version (20170209):***

*It has to be decided how to close the Editor’s note at the beginning of clause II (see the yellow highlights).*

**Introduction**

Since Software-Defined Networking (SDN) relates to various aspects of networking, many SDOs, forums, consortia, open-source activities are involved in its standardization today, and it becomes difficult to have up-to-date information on SDN standardization activities.

The ITU-T Joint Coordination Activity on SDN (JCA-SDN) therefore decided to keep an up-to-date information about the various standardization activities which are ongoing worldwide on SDN (including virtualization of network functions, network virtualization, programmable networks and Network as a Service), and publish a brief summary of them as roadmap.

The following roadmap is composed of two parts:

* ***Part I – High-level description of each SDO’s activity***Part I summarizes each SDO’s activity about SDN in order to provide an overview.
* ***Part II – Detailed description about each work item*** Part II describes in table format the available work items (including published and ongoing specifications) from each SDO.

This document will be kept updated according to new or updated information received, and a new version will be published at least after each JCA-SDN meeting.

1. Part I. High-level description of each SDO’s activity

This part provides a high-level description of each SDO’s SDN-related activity, first ITU-T activity, then other standardization activities and open source software activities based on the information exchange with JCA-SDN.

* 1. ITU-T

ITU-T ([http://www.itu.int/ITU-T/](http://www.itu.int/ITU-T)) is the standardization sector of International Telecommunication Union (ITU), an agency of the United Nations specialized for information and communication technologies (ICTs), and develops international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of ICTs.

* + 1. Study Group (SG) 13 (Future networks including cloud computing, mobile and next-generation networks)

SG13 is a group for network requirements and architecture, and standardizes them for various networks and networking technologies. SG13 is the lead study group of SDN in ITU-T, and develops the SDN framework, including SDN terminology, as baseline of all ITU-T SDN standardization activities. Question 14 (Q.14), *Software Defined-Networking and Service-aware networking of future networks*, is responsible of such framework and also discusses network virtualization, and has developed Recommendation ITU-T Y.3300, *Framework of software-defined networking*. Question 2 (Q.2), *Requirements for NGN evolution (NGN-e) and its capabilities including support of IoT and use of software-defined networking,* studies SDN and virtualization aspects for next generation networks (NGN) from requirements and capabilities perspectve. Question 3 (Q.3), *Functional architecture for NGN evolution (NGN-e) including support of IoT and use of software-defined networking,* studies SDN and virtualization aspects for next generation networks (NGN) from architecture perspective.

* + 1. Study Group (SG) 11 (Signalling requirements, protocols and test specifications)

SG11 is a group for signalling and testing, and standardizes protocols and its requirements, as well as test specifications, for various networks and networking technologies. Aligning its work with SG13, Question 4 (Q.4), *Signalling requirements and protocols for Bearer and Resource control in emerging telecommunication environments,* is developing a supplement (non-normative document) that describes the framework of SDN signalling. Question 6 (Q.6), *Protocol procedures relating to specific services over IPv6,* is studying how to apply SDN technologies for IPv6.

* + 1. Study Group (SG) 15 (Transport, Access and Home)

SG15 is responsible for the development of standards on optical transport network, access network, home network, and power utility network infrastructures, systems, equipment, optical fibres and cables, and their related installation, maintenance, management, test, instrumentation and measurement techniques, and control plane technologies to enable the evolution toward intelligent transport networks. As allocated from TSAG, SG15 is studying “Transport aspects of SDN” and has commenced a new draft Recommendation “Architecture for SDN control of Transport Networks”, aligned with the ONF’s “SDN architecture”, Issue 1, and a new draft Recommendation “Common Control Aspects” on common aspects of the interaction between the ASON control plane, SDN controller plane, management plane and transport plane.

* + 1. Study Group (SG) 16 (Multimedia)

SG16 is responsible for the development of standards on multimedia coding, systems and applications, ubiquitous and Internet of Things (IoT) applications, telecommunication/ICT accessibility for persons with disabilities, intelligent transport system (ITS) communications, e-health, and Internet Protocol television (IPTV). Question 3 (Q.3), *Multimedia gateway control architectures and protocols*, is evaluating OpenFlow versus H.248 as a protocol to control packet flows. Question 21 (Q.21), *Multimedia framework, applications and services*, is studying virtual content delivery networks.

* + 1. Study Group (SG) 17 (Security)

SG17 is responsible for the coordination on security-related work across all ITU-T Study Groups. Often working in cooperation with other standards development organizations (SDOs) and various ICT industry consortia, SG17 deals with a broad range of standardization issues. Question 6 (Q.6), *Security aspects of ubiquitous telecommunication services*, is studying security by SDN, which covers the security services using SDN: draft Recommendation ITU-T X.sdnsec-1 is developing requirements for security services based on SDN. Question 2 (Q.2), *Security architecture and framework,* is studyingsecurity of SDN, which covers the security architectural aspects of SDN and how to secure the SDN environment.

* 1. SDO, Forums, Consortia
		1. ATIS NFV Forum (NFV-F)

The ATIS NFV Forum was launched in September 2014 as a follow-on activity upon the completion of the previous SDN Landscape Team and SDN/NFV Focus Groups initiated in May 2013. The NFV Forum (NFV-F) is identifying and defining a set of service primitives that allow a framework of virtual functions to be managed, moved, and chained across service providers. The NFV Forum will build on and work closely with existing industry SDN/NFV activities with its unique contribution on inter-provider and enterprise-to-service provider interconnection, interoperability and interworking solutions. The NFV Forum will:

* Define and prioritize service provider-to-service provider and enterprise-to-service provider use cases where NFV capabilities are required to generate new value;
* Establish a common catalog of service descriptions that can be instantiated between service providers including runtime, network, and operational functions;
* Specify the service advertising and discovery mechanisms that allow companies to find and incorporate these services;
* Incorporate service creation tools such as service chaining for construction of business applications and models;
* Enable integration of web-scale, enterprise, and service provider applications through programmable network APIs; and
* Provide coordinated member contributions into open source and other relevant activities to further industry objectives.

The initial set of use cases from which the other work items above will be derived includes: virtual network operator, cooperative cloud-based CDN, roaming, enterprise voice/collaboration, and third party VNF applications use cases.

More information can be found https://www.atis.org/NFV/index.asp

* + 1. BBF

The Broadband Forum is the central organization driving broadband wireline solutions and empowering converged packet networks worldwide to better meet the needs of vendors, service providers and their customers. It develops multi-service broadband packet networking specifications addressing interoperability, architecture and management. Its output enables home, business and converged broadband services, encompassing customer, access and backbone networks.

There are two technical working groups (WGs) relevant to SDN. One is Service Innovation & Market Requirements (SIMR) WG. Its scope is to evaluate market/technology trends with 3 to 10 years horizon, to identify and assess potential enablers and disruptors, to guide BBF with future requirements and directions, to analyse market buzz/hype, to conduct Gap analysis to identify what dots BBF needs to connect, to develop service(s) description, business requirements, use cases, to recommend what role BBF should play and in what areas BBF may develop technical work in the mid and longer terms, and to help coordinate strategic external liaison relationships. In SIMR, SDN is analysed from this viewpoint.

The other WG is End to End Architecture (E2E) WG. It discusses end-to-end architecture issues, and, because of its nature, some of the issues (e.g. IPv6, QoS, security etc.) are discussed at joint sessions between this WG and one or more other WGs, dynamically arranged depending on the topic to be addressed.

More information can be found at <https://www.broadband-forum.org>

* + 1. CCSA

China Communications Standards Association (CCSA) is a non-profit legal person organization established by enterprises and institutes in China for carrying out standardization activities in the field of Information and Communications Technology (ICT) across China. CCSA is organized with the approval of MII and registration in the Ministry of Civil Affairs.

In CCSA, multiple TCs are developing SDN-related standards, i.e., TC1 SWG3 FDN, TC3 WG1-SVN, TC5 WG5 & WG9, TC6 WG1, TC7 WG2 and TC8 WG1.

TC1 SWG3, a special working group for FDN (future data network), has developed two standards by November 2014: “Scenarios and requirements of FDN” and “Function Architecture of FDN”. 14 more standards are under development. They cover protocol framework of FDN, SDN based IPRAN network, FDN service orchestration based on cloud management platform, FDN based data center internal network, FDN based inter-data center network, and others. In “Scenarios and requirements of FDN”, 15 scenarios in 6 categories, i.e., data center, MAN (Metropolitan Area Network), core network, enterprise network, backbone network and IPv6 transition, are provided. In “Function architecture of FDN,” data plane, control plane, application plane and relevant functional entities in the three planes are defined.

TC3 WG1, a working group for SVN (Software Smart and virtualized Networking), mainly focuses on the standard activities on SDN-based smart network, network virtualization, and future network from carriers’ perspective. Two standards are completed: “General Requirements for Network Intelligent Capability Enhancement making usage of software defined networking technologies (S-NICE)” and “Research on VCN (Virtualization of Control Network-entity)”. Besides these two standards, 6 more standards are under development. They cover virtualization of control network-entity, SDN-based intelligent aware system architecture, virtualized IMS network.

Other groups are: TC5, researching on the Mobile Softnet; TC6, doing research on software defined optical access network and software defined beyond 100G optical transponder technology; TC7, working on network management of SDN; TC8, focused on security requirement of SDN.

More information can be found at <http://www.ccsa.org/>.

* + 1. ETSI NFV ISG

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

The ETSI's Industry Specification Group for Network Functions Virtualization (NFV ISG) was setup to achieve a consistent approach and common architecture for the hardware and software infrastructure needed to support virtualized network functions. Network Functions Virtualization and Software Defined Networking are highly complementary, but not dependent of each other: Network Functions can be virtualized and deployed without an SDN being required and vice-versa.

The first 5 deliverables by ETSI NFV ISG were published as ETSI Group Specifications (GSs) in October 2013: four of them, designed to align understanding about NFV across the industry, cover NFV use cases, requirements, architectural framework and terminology; the fifth one defines a framework for coordinating and promoting public demonstrations of Proof of Concept (PoC) platforms illustrating key aspects of NFV, with the objective to encourage the development of an open ecosystem by integrating components from different players. Other 3 deliverables have been published at the date of November 2014 dealing with, respectively, methodology to describe interfaces and abstractions for NFV infrastructure, problem statement for NFV security and NFV performance & portability best practises.

Other draft GSs have been released for comment in August 2014.

More information can be found at <http://www.etsi.org/technologies-clusters/technologies/nfv>.

* + 1. IEEE P1903 WG (NGSON)

IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

The IEEE P1903 WG was setup to develop specifications for Next Generation Service Overlay Networks (NGSON).

IEEE approved in 2011 the IEEE Standard 1903-2011 for the Functional Architecture of Next Generation Service Overlay Networks, whichdescribes a framework of Internet Protocol (IP)-based service overlay networks and specifies context-aware, dynamically adaptive, and self-organizing networking capabilities, including advanced routing and forwarding schemes, that are independent of underlying transport networks.

The standard aims to enable network operators, service/content providers, and end-users to provide and consume collaborative services in a more efficient way by the deployment of context-aware, dynamically adaptive, and self-organizing networking capabilities.

The P1903 WG is currently working on the specification of service enabling functions which can be provided as Virtualized Network Functions (VNFs) to support NFV applications. Technical aspects which may be related to SDN are mechanisms for Service Composition, Service Routing and Self Organization aiming to provide service level virtualization.

More information can be found at <http://standards.ieee.org/develop/wg/1903_WG.html>

* + 1. IETF/IRTF

The Internet Engineering Task Force (IETF) is an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The actual technical work of the IETF is done in its working groups (WGs), which are organized by topic into several areas (applications, internet, operation and management, real-time application and infrastructure, routing, security, transport and general). A lot of work is handled via mailing lists. The IETF holds meetings three times per year.

There are many working groups in all areas related to SDN. To name a few, NVO3 (Network Virtualization Overlays) WG works on signalling for tunnelling protocol, it has completed requirements and framework in 2013, and protocol extension is currently work in progress. SFC (Service Function Chaining) WG is working on service function chaining, mainly for mobile networks. SPRING (Source Packet Routing in Networking) WG is about how specific data packets should be routed in the network.

While IETF is focused on standardization, the Internet Research Task Force (IRTF) is focused on long-term research. Currently there is a SDN RG (research group), which investigates on various aspects of SDN from definition, taxonomies to scalability and applicability, security and many others. NFV RG (not yet official) started its activity in November 2014. Its near-term focus is on analytics architecture for visibility and orchestration, architecture for policy based resource management, performance benchmarking architecture in controlled environments, and architecture for security and service verification of NFV. It will become an official RG if its one-year activity from its establishment meets the criteria.

More information can be found at <https://www.ietf.org/> and <https://irtf.org/>

* + 1. ONF

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

ONF working groups analyse SDN requirements, evolve the OpenFlow Standard to address the needs of commercial deployments, and research new standards to expand SDN benefits.

The technical communities are organized into Areas, Councils and Groups. Areas handle specific issues related to SDN, and collaborate with the world’s leading experts on SDN and the OpenFlow Standard regarding SDN concepts, frameworks, architecture, software, standards and certifications. Councils provide overall leadership with respect to strategy, operational execution and technical direction of the organization. Groups provide guidance and advise ONF on activities to help accomplishing the organization’s goals.

More information can be found at <https://www.opennetworking.org/>.

* + 1. TTA

Telecommunications Technology Association (TTA) is a non-government and non-profit organization for ICT standardization, testing and certification services that seeks out and establishes new standards for the ICT industry in Korea.

TTA ICT standardization committee develops ICT standards in a timely manner to meet the industry’s needs and enhance consumers’ convenience. As of November 2014, TTA standardization committee is composed of 6 technical committees, 2 special technical committees and 53 project groups including ‘Future Internet’ project group (PG220).

Future Internet project group (PG220) is a lead project group of SDN issues related to ITU-T SG13. PG220 is now developing TTA standards which describe common hardware and software platforms to support open programmable networking and SDN/NFV enabled services. In 2014, PG220 has successfully completed standardization related to hardware platform including network function boards, which defines mechanical specification, shelf hardware management, power and ground, heating, data transmission and interconnect, and regulatory guidelines. In 2015, PG220 will mainly focus on software aspects.

More information can be found at <http://www.tta.or.kr/English/index.jsp>.

* + 1. 3GPP

The 3rd Generation Partnership Project (3GPP) unites six telecommunications SDOs (ARIB, ATIS, CCSA, ETSI, TTA, TTC), and provides their members with a stable environment to produce the Reports and Specifications that define the 3GPP technologies.

The project covers cellular telecommunications network technologies, including radio access, core transport network and service capabilities (including work on codecs, security, quality of service), and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.

There are four Technical Specification Groups (TSGs) in 3GPP, i.e., Radio Access Networks (RAN), Service & Systems Aspects (SA), Core Network & Terminals (CT) and GSM EDGE Radio Access Networks (GERAN), and there are Working Groups (WGs) in each TSG.

TSG SA WG5, or SA5, a group for telecom management, has started a new study item on Network Management of Virtualized Networks, which is planned for completion in June 2015. Its objective is to study representative scenarios, use cases and concepts for the network management of Virtualized Networks, to identify the requirements for potential solutions, and to do gap analysis between the identified requirements and current 3GPP Management reference model.

**I.2.10 Open Cloud Connect**

OpenCloud Connect is a global industry alliance founded to address the need for scaling and enhancing current network technologies to meet the stringent demands of delivering cloud services.

With virtual machine populations running into the millions across geographically dispersed datacenters plus the migration of storage networks to Ethernet, OpenCloud Connect provides a framework to develop solutions that address technical challenges such as VLAN scaling, layer 2 performance and resilience across very large domains and consolidating storage network technologies onto Ethernet.

* 1. Open Source Software projects
		1. OpenDaylight

OpenDaylight is a collaborative, open source project to advance Software-Defined Networking (SDN). OpenDaylight is a community-led, open, industry-supported framework, consisting of code and blueprints, for accelerating adoption, fostering new innovation, reducing risk and creating a more transparent approach to Software-Defined Networking. Many companies in ICT industry sponsor and contribute to the project.

OpenDaylight framework divides the problem space into four areas, (1) network applications, orchestration and services such as virtual tenant network (VTN) coordinator or DDoS protection, (2) controller platform such as topology manager or network configuration, (3) southbound interfaces & protocols such as netconf or OpenFlow plugins, and (4) data plane elements (virtual switches, physical device interfaces) such as OpenFlow-enabled devices or Open vSwitches. OpenDaylight focuses on the first three areas. (1) and (2) are connected with RESTful OpenDaylight APIs.

OpenDaylight is composed of nearly 30 projects, and releases their outputs in simultaneous manner. After its first release, Hydrogen, in February 2014, it successfully delivered the second one, Helium, at the end of September 2014.

One way to use OpenDaylight is to call it from OpenStack. Icehouse release of OpenStack Neutron includes a driver for OpenDaylight API, and enables other OpenStack services to use OpenDaylight services.

More information can be found at <http://www.opendaylight.org/>.

* + 1. OpenStack

OpenStack is an open source software project that aims to produce an open source cloud operating system. It provides multi-tenant IaaS, and aims to meets the needs of public and private clouds regardless of size, by being simple to implement and massively scalable. The project started on 2010 by Rackspace and NASA, has grown drastically, and is now governed by OpenStack Foundation, a non-profit foundation. SDN technology is expected to contribute to its networking part, and to make the cloud operating system more efficient, flexible and reliable.

OpenStack is organised around three major pillars, compute, networking and storage. OpenStack Compute (codename: Nova) aims to provision and manage large networks of virtual machines. OpenStack Networking (codename: Neutron) aims to provide pluggable, scalable, API-driven network and IP management. OpenStack Storage aims to provide object storage (codename: Swift) and block storage (codename: Cinder) for use with servers and applications. It also has several shared services to make cloud service easier to implement and operate. These services include identity management, image management, a web interface and many others.

OpenStack is composed of many projects. When OpenStack started, there were two projects, Nova for compute and Swift for object storage. The number of projects steadily increased over time, and as of November 2014, there are more than 10 projects.

One of them, Neutron, is dedicated for networking. It provides Network as a Service (NaaS) to other OpenStack services (e.g., nova). Almost all SDN controllers have provided plugins for Neutron, and through them, services on OpenStack and/or other OpenStack services can build rich networking topologies, and can configure advanced network policies in the cloud.

More information can be found at <http://www.openstack.org/>.

* + 1. OPNFV

*Editor’s note: text below is an extract from the OPNFV home web page.*

Open Platform for NFV (OPNFV) is a new open source project focused on accelerating the evolution of Network Functions Virtualization (NFV). OPNFV will establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and to ensure consistency, performance and interoperability among multiple open source components. Because multiple open source NFV building blocks already exist, OPNFV will work with upstream projects to coordinate continuous integration and testing while filling development gaps.

The initial scope of OPNFV is on building NFV Infrastructure (NFVI), Virtualized Infrastructure Management (VIM), and including application programmable interfaces (APIs) to other NFV elements, which together form the basic infrastructure required for Virtualized Network Functions (VNF) and Management and Network Orchestration (MANO) components. OPNFV is expected to increase performance and power efficiency; improve reliability, availability, and serviceability; and deliver comprehensive platform instrumentation.

OPNFV will work closely with ETSI’s NFV ISG, among other Standards Development Organizations (SDOs), to drive consistent implementation of standards for an open NFV reference platform. Increasingly, standards are being drafted in conjunction with major open source projects. Since feedback from open source implementations can drive the rapid evolution and adoption of standards, this tight coordination of otherwise independent processes is crucial to the establishment of an NFV ecosystem. When open source software development is aligned with standards development, it can root out issues earlier, identify resolutions, and potentially establish de facto standards, resulting in a far more economical approach to platform development.

More information can be found at <http://www.opnfv.org/>.

* + 1. ONF Atrium

ONF Atrium is an open SDN software distribution designed to help the networking industry as a whole more easily adopt open SDN by integrating established open source SDN software with some critical connecting pieces. It aims to be a Linux-like distribution(s) containing SDN applications and controllers that are interoperable with a wide range of forwarding planes. The first release, Atrium 2015/A, incorporates the Border Gateway Protocol (BGP), the Open Network Operating System (ONOS), and Open Compute Project (OCP) components. The software elements run in either controllers or switches, communicating via the OpenFlow protocol, and include plugin opportunities for other switching solutions to help foster an open ecosystem of interoperable, hardware-based OpenFlow switches.

Atrium will provide releases twice a year. Atrium 2015/B plans to develop BGP router application for ODL controller, to extend the concept of flow objects to ODL, to harden and to scale, to provide new applications developed for ONOS controller, and to expect more switch vendor participation.

* + 1. ONOS

The Open Network Operating System (ONOS) is a software defined networking (SDN) OS for service provider networks claiming scalability, high availability, high performance and abstractions to make it easy to create applications and services. It is claimed that, as a distributed (cluster based) operating system, ONOS scales horizontally with network size and application demand. Application programming simplification is claimed via rich northbound abstractions all while maintaining a network view for applications. A southbound interface allows control of both legacy and OpenFlow enabled devices.

Eight ONOS releases have been announced, including “Avocet” for Architecture and “Blackbird” for Performance. Concerning the platform architecture:

* the northbound abstractions include network graph, application intents, flow objectives, virtualization and slicing ;
* the core is distributed, protocol independent and provides abstraction on back-end store;
* the southbound interface, based on a “provider” model”, is pluggable and extensible.

The platform features have grown from an initial control-centric, openflow network based platform to a control and configuration platform, supporting operators’ current networks and providing enhanced core features and enhanced northbound/southbound protocols. The core has evolved from the basic distributed core services to extensions and network applications.

ONOS claims that its solution (under development) for dynamic configuration of devices (based on NetConf and Yang) provides benefits for both operators and vendors.

ONOS supports a variety of distributed data stores with different consistency, availability and durability attributes: a new - model agnostic - distributed data store called DocTree has been created to implement Device Configuration Data Store on the ONOS cluster.

ONOS claims to have demonstrated industry leading performance with high application throughput and low event response latency (ONOS white paper on performance).

Some ONOS-based commercial SDN controllers have been announced.

The ONOS community has grown to include at February 2017 16 partners, +60 collaborators and +250 code contributors. The community contributes to all aspects of the project including use cases such as CORD (Central Office Re-architected as a Datacenter) [<http://opencord.org/>], multi-layer network control, abstraction and control TE network, agile VPN.

More information can be found at http://onosproject.org/

* + 1. OPEN-O

The OPEN Orchestrator project (OPEN-O) is an open source project hosted by the Linux Foundation that enables leading telecommunications, cable and cloud operators end-to-end service orchestration over network functions virtualization (NFV) infrastructure, along with software-defined networks (SDN) and legacy networks. It develops a unified orchestration platform for end-to-end service orchestration across both NFV and SDN network domains, as well as legacy networks.

The OPEN-O vision enables orchestration of any service over any network by using modular approach that integrates with multiple VNF managers, SDN controllers and virtual infrastructure managers (VIMs). OPEN-O also allows service providers to manage legacy network infrastructures and interwork with legacy OSS and BSS systems.

Among the multiple open source MANO projects, OPEN-O intends to distinguish itself for going beyond network management and orchestration to tackle end-to-end service delivery, across both legacy and virtualized networks.

OPEN-O's first software release will include code for each of the group's initial projects. Those projects include global service orchestrator (GS-O), NFV orchestrator (NFV-O), SDN orchestrator (SDN-O), a VNF software development kit API, Common Services, Common TOSCA and integration across the software platform.

OPEN-O also is also pursuing a new project, focused on creating a generic VNF manager in order to avoid having to create VNF-specific managers.

More information can be found at <https://www.open-o.org/>

1. Part II. Detailed description about each work item

This section describes each work item inside each SDO using a unique table format.

**NOTE – This section is expected to be enhanced with additional information in the following versions of this document.**

***Editor’s note*** *related to the 24 April 2015 JCA-SDN meeting output version:*

* *ETSI NFV ISG (jca-sdn-i-23): this version of the document contains only the documents published at the date of November 2014*
* *ONF (jca-sdn-i-18 and jca-sdn-i-30): no documents identified at this stage; 9 Feb 2017 version: ONF TR-540 has been included*
* *CCSA (jca-sdn-i-19): no documents identified at this stage, detailed input is expected by next JCA-SDN meeting*
* *OpenDaylight (jca-sdn-i-37): no documents identified at this stage*
* *OpenStack (jca-sdn-i-39): no documents identified at this stage*
* *MEF**related information was provided in jca-sdn-i-07. Up-to-date MEF related information has been requested via liaison.*
* *OPNFV (jca-sdn-i-62): no documents identified at this stage; Concerning jca-sdn-i-054 (TTA), in this 24 April version the first two rows provided in 054 have been simply added, but it is required confirmation if they are actually in addition or if they replace the two TTA rows already present in the November 2014 roadmap version.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Activity domain | Stage (topic) | Area | Entity | Title of deliverable | Scope of deliverable | Current status | Starting date | Target date |
| SDN | Network function virtualization | Network virtualization | Programmable network | Network as a Service | Use cases | framework | requirements | architecture | protocol | e.g. Network | service | application, mobile | fixed, access | core | SDO, and WG if possible | **Name**  | **acronym** | **Reference** | This document aims to … | Draft ITU-T Recommendation | International Standard | Specification | yyyy.mm | yyyy.mm |
| SDN | Framework | General | ITU-T SG13 Q14(2013 ~ 2016) | **ITU-T Y.3300**, Framework of SDN (Software-Defined Networking) | This Recommendation describes framework of SDN (Software-Defined Networking) to specify common part of SDN which is commonly agreeable part of SDN requirements and architectures including terminologies among collaborative SDOs/open source software community and ITU-T Study Groups.  | ITU-T Recommendation | 2012.2 | 2014.6 |
| SDN | Requirements | Formal methodology | ITU-T SG13 Q14(2013 ~ 2016) | **ITU-T**  **Y.3320,**  Requirements of formal specification and verification methods for software-defined networking | This Recommendation describes requirements for using formal specification and verification techniques in the context of software-defined networking (SDN) for Future Networks.The scope of this Recommendation covers:\* Definition and overview of formal methods for SDN, and\* Requirements of formal specification and verification methods for SDN | ITU-T Recommendation | 2012.7 | 2014.8 |
| Network virtualization | Requirements | Network | ITU-T SG13 Q14(2013 ~ 2016) | **ITU-T**  **Y.3312,** Requirements of network virtualization for future networks | This Recommendation specifies the requirements of network virtualization in future networks, in particular requirements on physical resource management, virtual resource management, logically isolated network partition (LINP) management, service management, authentication, authorization and accounting of LINP, LINP federation and service mobility. | ITU-T Recommendation | 2012.2 | 2014.4 |
| Network virtualization | Framework | Network | ITU-T SG13 Q14(2013 ~ 2016) | **ITU-T Y.3011,** Framework of network virtualization for future networks | This Recommendation defines network virtualization and provides an overview of, and motivation for, network virtualization. It also describes problem spaces, design goals, and applicability of network virtualization. Use cases for network virtualization are discussed in an appendix. | ITU-T Recommendation | 2010.1 | 2012.1 |
| Network virtualization | Requirements | Network | ITU-T SG13 Q14(2013 ~ 2016) | **ITU-T Y.3012,** Requirements of network virtualization for future networks | The scope of this Recommendation is to provide requirements of network virtualization for future networks. | ITU-T Recommendation | 2012.1 | 2014.4 |
| Network virtualization | Architecture | Network | ITU-T SG13 Q14(2013 ~ 2016) | **ITU-T Y.3015,** Functional architecture of network virtualization for future networks | This Recommendation describes functional architecture of network virtualization.The scope of this Recommendation covers:* Overall functional architecture of network virtualization
* Player’s role in network virtualization
* Functions of network virtualization
* Relationship among overall functions.
 | ITU-T Recommendation | 2014.2 | 2016.02 |
| SDN | Requirements | General | ITU-T SG13 Q14(2013 ~ 2016) | **Draft Y.SDN-req**, Functional requirements of software-defined networking | Recommendation ITU-T Y.3300 (Framework of software-defined networking) describes fundamentals of SDN including the definitions, objectives, high-level capabilities, requirements, and the high-level architecture of SDN. Based on Y.3300, this Recommendation describes the details of capabilities, and the functional requirements to realize them. 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 Appendix of Y.3300 are considered in describing the requirements. | Draft ITU-T Recommendation | 2014.11 | 2016.07 |
| SDN | Architecture | General | ITU-T SG13 Q14(2013 ~ 2016) | **Draft Y.SDN-arch**, Functional architecture of software-defined networking | Recommendation ITU-T Y.3300 (Framework of Software-Defined Networking) includes definitions, objectives, high-level capabilities, requirements, and the high-level architecture of SDN. Based on Y.3300, the Recommendation describes 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.). | Draft ITU-T Recommendation | 2014.11 | 2016.07 |
| SDN  | Requirements (for NGN evolution)  | Network, service | ITU-T SG13 Q2(2013 ~ 2016) | **ITU-T Y.3321,**  Requirements and capability framework for NICE implementation making usage of software defined networking technologies (S-NICE) | This Recommendation provides the requirements and capability framework for software defined network intelligence capability enhancement (S-NICE). S-NICE is a specific implementation of NICE [ITU-T Y.2301] making usage of software defined networking technologies. NICE being an evolved version of NGN, S-NICE supports the intelligent features (five major features) of NICE and makes usage of software defined networking technologies. This Recommendation specifies the requirements and capabilities of S-NICE at the NGN service stratum and NGN network stratum.  | ITU-T Recommendation  | 2013.2 | 2015.6 |
| Network function virtualization  | Requirements (for NGN evolution)  | Network | ITU-T SG13 Q2(2013 ~ 2016) | **ITU-T Y.2320,**  Requirements of VCN (Virtualization of Control Network-entities) for NGN evolution | This Recommendation defines the requirements of VCN (**V**irtualization of **C**ontrol **N**etwork-entities) for NGN evolution. The requirements are built upon the virtualization scenarios provided in Appendix. The support of virtualization capabilities in NGN evolution - i.e. the application of virtualization techniques to NGN - enables a virtualized running environment (for control network entities) in NGN evolution.  | ITU-T Recommendation | 2013.6 | 2015.9 |
| SDN  | Architecture (for NGN evolution)  | Network, service | ITU-T SG13 Q3(2013 ~ 2016) | Draft Y.S-NICE-arch, The functional architecture and implementations of S-NICE (Software defined Network Intelligence Capability Enhancement) | This Recommendation provides the architecture and implementations of Software-defined NICE(S-NICE). S-NICE is the evolved NGN which support intelligent features and is based on software defined networking technologies. This Recommendation defines the architecture of S-NICE, the enhancement functions about relevant functions in NICE, the reference point between different functions and implementations realizing intelligent features.This Recommendation builds on Y.3321 and Y.2302. | Draft ITU-T Recommendation |  | 2016.6 |
| Network function virtualization  | Architecture (for NGN evolution)  | Network | ITU-T SG13 Q3(2013 ~ 2016) | Draft Y.NGN-VCN-Arch, Functional Architecture of VCN in NGN | This Recommendation specifies a cost-effective, flexible, scalable and reliable VCN functional architecture which provides a virtualized running environment for NGN control functional entities such as PCSC-FE, SCSC-FE, etc. The definition of the functional architecture of VCN (**V**irtualization of **C**ontrol Network-entities) for NGN includes the detailed capabilities of Functions, functional entities and the reference points. | Draft ITU-T Recommendation |  | 2016.6 |
| Network function virtualization  | Architecture (for NGN evolution)  | Network | ITU-T SG13 Q3(2013 ~ 2016) | **Draft**  Y.NGN-VCNMO-arch, The functional architecture of VCNMO(Virtualized Control Network entities Management and Orchestration) in NGN evolution | This Recommendation defines the functional architecture of VCNMO (Virtualized Control Network-entity Management and Orchestrator) and specifies the related reference points of VCNMO and its subcomponents, which includes orchestrator, VCNM and VIM of VCN. This Recommendation builds on Y.2320 and Y.NGN-VCN-arch.  | Draft ITU-T Recommendation |  | 2017.11 |
| Network as a Service | Use cases, framework, requirements | Network, service, application | ITU-T SG13 Q18 (2013 ~2016) | **ITU-T Y.3512,** Cloud computing - Functional Requirements of Network as a Service | This Recommendation describes the concept of Network as a Service (NaaS) and its functional requirements. It provides typical use cases of NaaS and specifies the functional requirements of three aspects, ranging from NaaS application, NaaS platform, and NaaS connectivity, which are based on the corresponding uses cases and cloud capabilities types.This Recommendation provides use cases and functional requirements of Network as a Service (NaaS), one of the representative cloud service categories. This Recommendation covers the following:* High level concept of NaaS;
* Functional requirements of NaaS;
* Typical NaaS use cases.

This Recommendation provides use cases and functional requirements of NaaS application, NaaS platform and NaaS connectivity. | ITU-T Recommendation | 2013.02 | 2014.08 |
| Network as a Service | Architecture | Network, service, application | ITU-T SG13 Q18 (2013 ~2017) | **ITU-T Y.3515**, Cloud computing - Functional Architecture of Network as a Service | This Recommendation provides Network as as Service (NaaS) functional architecture by specifying functionalities and functional components as well as reference points for Operation System Support (OSS). The scope of this Recommendation consists of:1. Overview of NaaS functional architecture
2. Functionalities of NaaS
3. Functional components of NaaS
4. Reference points for OSS of NaaS

This Recommendation also describes: 1. Mapping between functionalities and functional requirements of NaaS specified in [ITU-T Y.3512];
2. Relationship between NaaS functional architecture and Software Defined Networking (SDN);
3. Illustrated usage of SDN and Network Functions Virtualisation (NFV) in support of NaaS architecture.
 | ITU-T Recommendation | 2014.07 | 2017.02 |
| SDN |  Framework, signalling requirements and architecture | SDN signalling framework  | ITU-T SG11 Q4(2013 ~ 2016) | **ITU-T Supplement 67 to Q-series Recommendations**, Framework of signalling for SDN | This Supplement provides the framework of signalling for Software-Defined Networking (SDN) by specifying the signalling requirements and architecture for SDN, as well as the interfaces and signalling protocol procedures. These requirements and the signaling information elements identified will enable the development of a signalling protocol(s) capable of supporting traffic flows. | ITU-T Supplement  | 2013.2  | 2015.4 |
| SDN | Signalling requirements | SDN for Broadband Access Network  | ITU-T SG11 Q4(2013 ~ 2016) | **Draft Q.SBAN,**  Scenarios and signalling requirements for software-defined BAN (SBAN) | This Recommendation describes the scenarios using software defined networking technologies in Broadband Access Network (BAN). This software-defined BAN (SBAN) includes broadband aggregation layer and access layer networks. Meanwhile, this Recommendation specifies signalling requirements of Northbound Interface between application and Control plane and signalling requirements of Southbound Interface between Control plane and Forwarding plane. | Draft ITU-T Recommendation | 2013.2 | 2016.07 |
| SDN | Signalling requirements and protocols | Resource control and management | ITU-T SG11 Q4(2013 ~ 2016) | **Draft Q.3316,**Interface and Signalling Requirements and Specification for Cross Stratum Optimization | This Recommendation provides interface and signalling requirements and specification for cross stratum optimization (CSO) based on the resource control and management architecture defined in Y.VNC. | ITU-T Recommendation | 2013.02 | 2016.02 |
| SDN | Signalling requirements and protocols | Signalling requirement, interface requirement and protocols | ITU-T SG11 Q4(2013 ~ 2016) | **Draft Q.PVMapping**, Signalling Requirements for Mapping between Physical and Virtual Networks | The scope of this Recommendation includes, but is not limited to:1. Interfaces requirements for mapping between SDN based physical underlay networks and virtual overlay networks.
2. Signalling requirements for mapping between SDN based physical underlay networks and virtual overlay networks.
3. Typical scenarios and procedures.
 | Draft ITU-T Recommendation | 2015.07 | 2017.11 |
| SDN | Signalling requirements and protocols | SDN for Metro Orchestration | ITU-T SG11 Q4(2013 ~ 2016) | **Draft Q.SMO,**Signalling requirements of Software-defined Metro Orchestration |  The scope of this Recommendation is to describe the signalling requirement for Software-defined Metro Orchestration (SMO). This Recommendation specifies the scenarios, signalling architecture and requirements of SMO. This document will focus on following aspects between aggregation node and metro core:1) Centralized orchestration of multiple networks in the metro area for E2E service delivery;2) Unified traffic management and optimization of metro services with different SLAs;3) Northbound application for metro network services; | Draft ITU-T Recommendation | 2015.04 | 2017.11 |
| SDN, Network function virtualization | Use cases, Signalling requirement | SDN based Central Office | ITU-T SG11 Q4(2013 - 2016) | **Draft Q.SCO**, Scenarios and signalling requirements for SDN based Central Office | This Recommendation specifies the signalling architecture and requirements for SDN based Central Office (CO) services. The interfaces Si between the NFVO and the SDN controller, as well as the signalling protocol procedures at this interface, will be described to support this service. These requirements and signalling information elements identified will enable the development of a signalling protocol(s) capable of supporting traffic flows for SDN based central office services | Draft ITU-T Recommendation | 2015.12 | 2017.12 |
| SDN | Use cases, Signalling requirement | Network, fixed | ITU-T SG11 Q4(2013 ~ 2016) | Draft Q.SVDC, Signalling requirements of the Sew interface for Virtual Data Center | This Recommendation defines Scenarios and signalling requirements between multi-controllers within Virtual Data Centers. The interface is defined as the Sew interface in ITU-T Q.Suppl.67, and this Recommendation mainly focuses in the inter-domain Sew interface for multi-vendor interoperability. This Recommendation builds on ITU-T Y.3300 and Q.Suppl.67. | Draft ITU-T Recommendation | 2016.6 | 2018.12 |
| SDN | Signalling requirements and protocols | Dynamic bandwidth adjustment on demand on broadband network gateway | ITU-T SG11 Q5(2013 ~ 2016) | **Draft Q.BNG DBoD,** Signalling requirements for dynamic bandwidth adjustment on broadband network gateway implemented by SDN technologies  | This Recommendation describes the signalling requirements for dynamic bandwidth adjustment on demand on broadband network gateway implemented by SDN technologies. The signalling is to support the dynamic bandwidth adjustment on demand on the BNG. This Recommendation focuses on the signalling between the S-DBoD and BNG. | Draft ITU-T Recommendation | 2015.04 | 2017.06 |
| SDN | Network function virtualization | Signalling requirements | Network，service | ITU-T SG11 Q5(2013 ~ 2016) | **ITU-T Q.3315**, Signalling requirements for flexible network service combination on Broadband Network Gateway | This Recommendation describes the signalling requirements for the flexible network service combination on Broadband Network Gateway (BNG). The signalling is to support the service routing, service combination, service deployment and service provision on the BNG. This Recommendation focuses on the signalling between the service platform and BNG. Signalling above the service platform is out of scope of this Recommendation. | ITU-T Recommendation | 2013.2 | 2015.01 |
| SDN, | Signalling requirement | Network, fixed | ITU-T SG11 Q5(2013 ~ 2016) | **Draft Q.BNG IAP**, Signalling requirements of IP address pool based on broadband network gateway by SDN technologies | This Recommendation defines the signalling requirements for implementation of IP address pool resource efficient utilization using software defined networking technologies on the broadband network gateways. The signalling requirements will cover IP address pool resource distribution, monitor and recycle, etc. | Draft ITU-T Recommendation | 2016.6 | 2018.12 |
| SDN | Use cases , Signalling requirement and protocols | IPv6 | ITU-T SG11 Q6(2013 ~ 2016) |  **Draft Q.IPv6UIP,** Scenarios and signalling requirements of unified intelligent programmable interface for IPv6  | This Recommendation describes the scenarios and signalling requirements of unified intelligent programmable interface for IPv6 service deployment. The data model (e.g., YANG) and signalling protocol (e.g., xml) procedures at this interface will also be described in the document to support protocol unaware flow forwarding in the data plane. The IPv6 technologies supported will include the following but not limited to: DS-Lite, IPv6 only, 6RD, 4RD, MAP-E, MAP-T, Lightweight4over6 and 464XLAT.  | Draft ITU-T Recommendation | 2013.2 | 2016.07 |
| SDN | Signalling requirement and protocols | SDN for Access Network | ITU-T SG11 Q7 (2013 – 2016) | **Draft Q.SAN-MIM,** Signalling requirements of SDN-based access networks with media independent management capabilities | This Recommendation describes the signalling architecture, signalling requirements, and signalling protocol procedures for SDN-based access networks with Media Independent Management (MIM) capabilities. This document introduces signalling architecture models of the SDN-based access networks with MIM capabilities. Various signalling architecture models are described for the loosely and tightly coupled integrations between SDN and MIM control frameworks. Signalling requirements and protocol procedures for resource management and seamless handover are described for each signalling architecture model of SDN-based access networks with MIM capabilities. | Draft ITU-T Recommendation | 2015.12 | 2017.12 |
| SDN | Architecture | Transport networks | ITU-T SG15 Q12 & Q14 (2013 ~ 2016) | **Draft G.astdn**, Architecture for SDN control of Transport Networks | The scope of this Recommendation is the specification of a 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. The architecture will utilize the abstract control component approach for representing specific functions that has been employed in ITU-T G.8080 and other ASON Recommendations. | Draft ITU-T Recommendation | 2014.04 | 2016.03 |
| SDN | Framework | Transport networks | ITU-T SG15 Q12 (2013 ~ 2016) | **Draft G.7701,** Common Control Aspects  | This Recommendation describes concepts that are common to both SDN controller and Automatically Switched Optical Network control approaches. The Recommendation describes those concepts based on the component approach in G.8080. Its scope includes common aspects of the interaction between the ASON control plane, SDN controller plane, management plane and transport plane. | Draft ITU-T Recommendation | 2014.07 | 2016.09 |
| SDN | Protocol | Network | ITU-T SG16 Q3(2013 ~ 2016) | **Draft H.Sup.OpenFlow**, Protocol evaluation – OpenFlow versus H.248 (Ed. 0.4) | The "vertical" decomposition of network elements (in packet based communication infrastructures), driven by network evolution scenarios which will demand for "open control" interfaces between the packet transport, forwarding and routing domain and the overlay domain of application/service control, demands for technologies for controlling of packet flows in the most general sense.There are a number of candidate technologies for such network solutions. Purpose of this document is an attempt in comparing H.248 with OpenFlow. | Draft ITU-T Supplement | 2013.10 | 2015 |
| Network virtualization | Scenarios, requirements, architecture |  | ITU-T SG16 Q21(2013 ~ 2016) | **Draft H.VCDN-RA,** Functional requirements and architecture model for virtual content delivery network | This Recommendation identifies scenarios, requirements and functional architecture that enable content delivery service in VCDN (Virtual Content Delivery Network). Some of the considered aspects include:* QoE and QoS assurance on providing video and audio service in VCDN.
* GSLB or SLB on cooperative work with virtual cache servers.
* Security requirement on providing various services to multiple vendors.
 | Draft ITU-T Recommendation | 2014.06 | 2016 |
| SDN | Network as a Service | Use cases | Security application | ITU-T SG17 Q6(2013 ~ 2016) | **Draft X.sdnsec-1,**  Security services using the Software-Defined Networking | This Recommendation is to support the protection of network resources using security services based on software-defined networking (SDN).  This Recommendation covers as follows: Classify the network resources using SDN in various security services; Define the security requirements in security services using SDN; Define use cases for security services by using SDN. | Draft ITU-T Recommendation | 2014.09 | 2017.02 |
| SDN | Network as a Service | Requirements | Architecture | Security architecture | ITU-T SG17 Q2(2013 ~ 2016) | **Draft X.sdnsec-2**, Security requirements and reference architecture for Software-Defined Networking | This Recommendation is to support security protection for software defined networking (SDN). This Recommendation covers as follows: Describe use cases to detail new security threats when introducing SDN; Identify security threats; Define security requirements; Provide possible security mechanisms for new security threats; and Design security reference architecture for SDN. | Draft ITU-T Recommendation | 2015.04 | 2017.09 |
| SDN | Network function virtualization | Architecture  | service | application | IEEE SA, P1903 WG | **IEEE Standard for the Functional Architecture of Next Generation Service Overlay Networks** | A framework of Internet Protocol (IP)‐based service overlay networks is described and context‐aware [e.g., such as required Quality of Service (QoS) level; type of servicesuch as real time versus data; nature of data stream such as Iframe versus B‐frame; and type of terminal such as TV monitor versus personal digital assistant],dynamically adaptive (e.g., using locally derived information to discover, organize, and maintaintraffic flows in the network within a local area network), and selforganizing networking capabilities(e.g., developing network structures based on the needs ofthe customers and the capabilities of existing network structures), including advanced routing and forwarding schemes, that are independent of underlying networks, are specified in this Next Generation Service Overlay Network (NGSON) standard. The NGSON architecture provides advanced service‐ and transport related functions to support context‐aware, dynamicallyadaptive, and self‐organizing networks. This standard specifies a functional architecture for NGSON.The functional architecture consists of a set of functional entities (FEs), their functions, reference points,and information flows to illustrate service interaction and media delivery among FEs and externalcomponents. NGSON may operate with different underlying networks such as IP Multimedia Subsystem(IMS), next generation network (NGN), peer‐to‐peer (P2P) overlay, or Web to transmit NGSON signaling messages and/or media among its users and services.Specifications of underlying networks are outside scope of this standard. | InternationalStandard | - | 2011.09 |
| SDN | Network function virtualization |Programmablenetwork | Protocol | service | application | IEEE SA, P1903.1 | **Standard for Content Delivery Protocols of Next Generation Service Overlay Network (NGSON)** | 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. | Protocol StandardSpecification | 2011.12 | 2015.12 |
| SDN | Network function virtualization |Programmablenetwork | Protocol | service | application | IEEE SA, P1903.2 | **Standard for Service****Composition Protocols****of Next Generation****Service Overlay****Network (NGSON)** | This standard specifies protocols among Service Composition (SC) Functional Entity (FE), ServiceDiscovery and Negotiation (SDN) FE, Context InformationManagement (CIM) FE, Service Routing (SR) FE and Service Policy Decision (SPD) FE to supportservice composition capabilities in next generation service overlay network. The capabilities of servicecomposition aim to support service chaining and instantiation, specification interpretation, servicebrokering and execution, and context aware and dynamically adaptive service composition. | Protocol StandardSpecification | 2011.12 | 2015.12 |
| SDN | Network function virtualization |Programmablenetwork | Protocol | service | application | IEEE SA, P1903.3 | **Standard for Self‐****Organizing****Management Protocols****of Next Generation****Service Overlay****Network (NGSON)** | This standard specifies protocols among Service Composition (SC) Functional Entity (FE), ServiceDiscovery and Negotiation (SDN) FE, Context InformationManagement (CIM) FE, Service Routing (SR) FE and Service Policy Decision (SPD) FE to supportservice composition capabilities in next generation service overlay network. The capabilities of servicecomposition aim to support service chaining and instantiation, specification interpretation, servicebrokering and execution, and context aware and dynamically adaptive service composition. | Protocol StandardSpecification | 2011.12 | 2015.12 |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV-INF 007**Network Functions Virtualisation (NFV); Infrastructure; Methodology to describe Interfaces and Abstractions | The present document describes how Network Functions Virtualisation (NFV) related interfaces and abstractions are to be derived and specified. It describes the concepts associated with these interfaces and abstractions. It covers the specification process / methodology in general. It presents a cross-cutting framework which covers compute, hypervisor and infrastructure network domains, also data, control and management planes.. | Published specification  |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV-SEC 001** Network Functions Virtualisation (NFV); NFV Security; Problem Statement  | The present document aims to:• To identify potential security vulnerabilities of NFV and to determine whether they are new problems, or justexisting problems in different guises.• To provide a reference framework within which these vulnerabilities can be defined.Out of scope: To list vulnerabilities that NFV suffers from that are no different from pre-existing vulnerabilities ofnetworking and virtualisation technologies and are not altered by the virtualisation of network functions.  | Published specification  |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV-PER 001**Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises | The present document provides a list of features which the performance and portability templates (Virtual MachineDescriptor and Compute Host Descriptor) should contain for the appropriate deployment of Virtual Machines over aCompute Host (i.e. a "telco datacentre").In addition, the document provides a set of recommendations and best practises on the minimum requirements that the HW and hypervisor should have for a "telco datacentre" suitable for data-plane workloads. | Published specification  |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV 001**Network Functions Virtualisation (NFV); Use Cases | The scope of the present document is to describe use cases of interest for NFV. | Published specification |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV 002**Network Functions Virtualisation (NFV); Architectural Framework | The present document describes the high level functional architectural framework and design philosophy of virtualized network functions and of the supporting infrastructure. It also defines the scope of the NFV ISG activities to realize this framework.  | Published specification  |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV 003**Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV | The present document provides terms and definitions for conceptual entities within the NFV ISG scope.  | Published specification  |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV 004**Network Functions Virtualisation (NFV); Virtualisation Requirements | The present document specifies the requirements that Telecommunications Operations put on Network Functions Virtualisation. | Published specification  |  |  |
| Network function virtualization |  |  | ETSI NFV ISG | **GS NFV-PER 002**Network Functions Virtualisation (NFV); Proofs of Concepts; Framework | The present document defines a framework for usage within ETSI NFV ISG to coordinate and promote public demonstrations of Proof of Concepts illustrating key aspects of NFV.  | Published specification  |  |  |
| SDN | Use cases | framework | business requirements  | Fixed network | BBF (SIMR WG) | **SD-313,** Business Requirements and Framework for SDN in Telecommunication Broadband Networks | Software Defined Networking (SDN) may create a long-term evolution within telecommunication broadband networks. By incrementally introducing SDN concepts, without rebuilding the whole network, operators have the opportunity to migrate to SDN while protecting existing investment. This project will examine some deployment scenarios including where only some of the network equipment would support SDN functionalities, as well as possibility of supporting SDN capabilities by upgrading software only. Per the mission of SIMR WG, SD-313 will include recommendations for follow-on Broadband Forum work regarding SDN. | Draft | 2012.12 | 2014.09 |
| Programmable network | Use cases | framework | business requirements | Fixed network | BBF (SIMR WG) | **SD-326,** Flexible Service Chaining | In order to support business and residential, fixed and mobile, wholesale and retail markets, TR-144 described various requirements including the need for network interconnection standards for broadband access, QoS support, Bandwidth on demand, increased overall bandwidth, higher network reliability and availability.New ways of defining services are required to keep up with market needs, seeking more flexibility in service deployment, faster service feature delivery, increased automation, elastic service bursting, etc.Service chaining allows complex services to be created out of simpler service-enabling elements through composition, e.g. stringing service points together while possibly constraining the corresponding data path.The output of this project will provide guidance to BBF's Technical and Marketing Committees on the work needed to bring flexible service chaining concepts to the level of detail necessary to define broadband network element requirements for implementation. This Study Document will also provide a reference for other service chaining standards organizations. | Draft | 2013.09 | 2014.09 |
| NFV | Network virtualization  | Technical requirements | architecture | Fixed network | BBF (E2E WG) | **WT-317,** Network Enhanced Residential Gateway | This Working Text specifies the Network Enhanced Residential Gateway (NERG) architecture. This architecture consists in shifting some of the functionalities of a residential gateway to the operator's network, for enabling network based features. The aim is to facilitate the deployment, maintenance and evolution of both existing and new capabilities without adding complexity to the RG and/or the home network. | Draft  | 2013.02 | 2015.03 |
| NFV | Network virtualization  | Technical requirements | architecture | Fixed network | BBF (E2E WG) | **WT-328,** Virtual Business Gateway | The virtual business gateway architecture describes the migration of functionalities running on a business gateway to the network service provider’s infrastructure for enabling network-based features and services. This Working Text specifies such architecture as well as deployment scenarios. This architecture targets different business premises sizes, e.g., small and medium enterprises (SMEs), campus, as well as single office and home offices (SOHO). The scope of the Working Text includes:- Business drivers (both sides)- Defining an appropriate set of network architectures- Specifying the nodal requirements to support the proposed architectures.- Management and orchestration within the architectures- Defining QoS, Security and Privacy- Enabling Multi-homing | Draft  | 2013.09 | 2015.03 |
| Network manage­ment of Virtual­ized Networks | Requirements, architecture and protocols | Manage­ment of mobile networks and its services | 3GPP SA WG5 | **TR 32.842,** Study on network management of Virtualized Networks | The TR will describe the representative scenarios, use cases, and concepts for the network management of Virtualized Networks (Objective Set1).It will describe the recommendation of potential solutions for the support of the management of Virtualized Networks (Objective Set 2). | Draft (Technical Report) | 2014.08 | 2015.06 |
| SDN and Network Function Virtualization | Architecture | Network and Protocols | TTA PG220 | **Common Hardware** **Platform (Network Functions Boards, Management Protocols, etc.)**  | This documents aim to specify common hardware platforms for SDN and NFV support network equipment and appliances. | TTA Standards (Domestic)  | 2013.05  | 2014.11  |
| SDN and Network function virtualization | Framework and Requirements | Network and Protocols | TTA PG220 | **Common Platform for Network Software****(Framework, Requirements, Management Protocols, etc.)** | This document aims to specify definitions, terminologies, and a reference model of common software platforms for SDN and NFV support network equipment and appliances. | TTA Standards(Domestic) | 2015.02 | 2015.12 |
| SDN and Network Function Virtualization | Architecture | Network and Protocols | TTA PG220 | **Smart Node Software Platform (System Interface Specification, Service Interfaces Specification, etc.)**  | This documents aim to specify Framework and APIs for Smart Node Software Platform. | TTA Standards (Domestic)  | 2013.05  | 2014.11  |
| SDN andNetwork function virtualization | Architecture | Network and Protocols | TTA PG220 | **Common Platform for Network Hardware****(Shelf Management Function)** | This document aims to specify the system architecture and interfaces of network function boards of common hardware platforms for SDN and NFV support network equipment and appliances. | TTA Standards (Domestic) | 2014.05 | 2015.12 |
| SDN and Network Function Virtualization | Architecture | Network and Protocols | TTA PG220 | **SDN Application Programming Interfaces**  | This document aims to specify Open Interfaces and APIs for SDN Application Programming.  | TTA Standards (Domestic)  | 2013.05  | 2014.11  |
| NFV | Network virtualization | Use cases |, Requirements |, Framework | Applications |, Network service |, Management |, for Mobile and Fixed | ATIS NFV Forum (NFV-F) | **Use Cases** | Define and prioritize service provider-to-service provider and enterprise-to-service provider use cases where NFV capabilities are required to generate new value | Draft Baseline use cases document including virtual network operator, cooperative cloud-based CDN, roaming, enterprise voice/collaboration, and third party VNF applications | 2014.10 | 2015.03 |
| NFV | Network virtualization | Framework |, Protocols | Applications |, Network service |, Management |, for Mobile and Fixed | ATIS NFV Forum (NFV-F) | **Service Descriptor Catalog** | Establish a common catalog of service descriptions that can be instantiated between service providers including runtime, network, and operational functions |  | 2015.02 | TBD |
| NFV | Network virtualization | Framework |, Protocols | Applications |, Network service |, Management |, for Mobile and Fixed | ATIS NFV Forum (NFV-F) | **Service Advertising and Discovery** | Specify the service advertising and discovery mechanisms that allow service providers and/or enterprises to find and incorporate these services |  | TBD | TBD |
| NFV | Network virtualization | Framework |, Protocols | Applications |, Network service |, Management |, for Mobile and Fixed | ATIS NFV Forum (NFV-F) | **Service Creation and Chaining**  | Incorporate service creation tools such as service chaining for construction of business applications and models |  | TBD | TBD |
| CloudSDN | Area | Application | IETF | Application Area | The Applications Area has historically focused on three clusters of protocols. The first cluster contains application protocols that have been ubiquitous for some time but which continue to develop (e.g., email,HTTP, FTP). The second cluster contains protocols which are used for Internetinfrastructure (e.g., IDNA and EPP). The third cluster contains "building block" protocols which are designed for re-use in a variety of more specific applications (e.g., LDAP, MIME types, URI schemes, URNs, OAuth, language tags). Current working groups include topics such as: email, web foundations and security, calendaring, internationalization, virtual worlds, personal address books, simple resource manipulation protocol for devices in constrained networks, some helper technologies for network storage and peer-to-peer applications. [IETF Areas] | Relevant working groups: httpbis (Hypertext Transfer Protocol Bis), scim (System for Cross-domain Identity Management), weirds (Web Extensible Internet Registration Data Service) |  |  |
| CloudSDN | Working Group | Application | IETF | httpbis (Hypertext Transfer Protocol Bis) | This Working Group is charged with maintaining and developing the "core" specifications for HTTP https://datatracker.ietf.org/wg/httpbis/charter/  | Working Group Documents: https://datatracker.ietf.org/wg/httpbis/ |  |  |
| CloudSDN | Working Group | Application | IETF | scim (System for Cross-domain Identity Management) | The System for Cross-domain Identity Management (SCIM) working group will standardize methods for creating, reading, searching, modifying, and deleting user identities and identity-related objects across administrative domains, with the goal of simplifying common tasks related to user identity management in services and applications. http://datatracker.ietf.org/wg/scim/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/scim/ |  |  |
| CloudSDN | Working Group | Application | IETF | weirds (Web Extensible Internet Registration Data Service) | Internet registries for both number resources and names have historically maintained a lookup service to permit public access to some portion of the registry database. Most registries offer the service via WHOIS (RFC 3912), with additional services being offered via world wide web pages, bulk downloads, and other services, such as RPSL (RFC 2622). http://datatracker.ietf.org/wg/weirds/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/weirds/ |  |  |
| CloudSDN | Area | Internet | IETF | Internet Area | The primary technical topics covered by the Internet Area include IP layer (both IPv4 and IPv6), implications of IPv4 address depletion, co-existence between the IP versions, DNS, DHCP, host and router configuration, mobility, multihoming, identifier-locator separation, VPNs and pseudowires along with related MPLS issues, and various link layer technologies. The Internet Area is also responsible for specifying how IP will run over new link layer protocols. [IETF Areas] | Relevant Working Groups: lisp (Locator/ID Separation Protocol) |  |  |
| CloudSDN | Working Group | Application | IETF | lisp (Locator/ID Separation Protocol) | The basic idea behind the separation is that the Internet architecture combines two functions, routing locators, (where you are attached to the network) and identifiers (who you are) in one number space: The IP address. Proponents of the separation architecture postulate that splitting these functions apart will yield several advantages, including improved scalability for the routing system. The separation aims to decouple locators and identifiers, thus allowing for efficient aggregation of the routing locator space and providing persistent identifiers in the identifier space. https://datatracker.ietf.org/wg/lisp/charter/ | Working Group Documents: https://datatracker.ietf.org/wg/lisp/ |  |  |
| CloudSDN | Area | Management | IETF | Operations and Management Area | The primary technical areas covered by the Operations & Management (OPS) Area include: Network Management, AAA, and various operational issues facing the Internet such as DNS operations, IPv6 operations, operational security and Routing operations. [IETF Areas] | Relevant Working Groups: dnsop (Domain Name System Operations), lmap (Large-Scale Measurement of Broadband Performance), netconf (Network Configuration), netmod (NETCONF Data Modeling Language) |  |  |
| CloudSDN | Working Group | Management | IETF | dnsop (Domain Name System Operations) | The DNS Operations Working Group will develop guidelines for the operation of DNS software servers and the administration of DNS zone files. These guidelines will provide technical information relating to the implementation of the DNS protocol by the operators and administrators of DNS zones. http://datatracker.ietf.org/wg/dnsop/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/dnsop/ |  |  |
| CloudSDN | Working Group | Management | IETF | lmap (Large-Scale Measurement of Broadband Performance) | The Large-Scale Measurement of Broadband Performance (LMAP) working group standardizes the LMAP measurement system for performance measurements of broadband access devices such as home and enterprise edge routers, personal computers, mobile devices, set top box, whether wired or wireless. http://datatracker.ietf.org/wg/lmap/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/lmap/ |  |  |
| CloudSDN | Working Group | Management | IETF | netconf (Network Configuration) | Configuration of networks of devices has become a critical requirement for operators in today's highly interconnected networks. Large and small operators alike have developed their own mechanisms or have used vendor specific mechanisms to transfer configuration data to and from a device and to examine device state information which may impact the configuration. Each of these mechanisms may be different in various aspects, such as session establishment, user authentication, configuration data exchange, and error responses. http://datatracker.ietf.org/wg/netconf/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/netconf/ |  |  |
| CloudSDN | Working Group | Management | IETF | netmod (NETCONF Data Modeling Language) | The NETCONF Working Group has completed a base protocol to be used for configuration management. However, the NETCONF protocol does not include a modeling language or accompanying rules that can be used to model the management information that is to be configured using NETCONF. The NETMOD working group has defined the data modeling language YANG but no IETF models exist yet. The purpose of the NETMOD working group is to support the ongoing deployment of YANG by developing a set of core YANG data models and other activities that will allow network operators to use YANG for configuration and management of network elements. http://datatracker.ietf.org/wg/netmod/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/netmod/ |  |  |
| CloudSDN | Area | Internet | IETF | Real-time Applications and Infrastructure Area | The Real-Time Applications and Infrastructure (RAI) Area develops protocols and architectures for delay-sensitive interpersonal communications. Work in the RAI Area serves an industry whose applications and services include voice and video over IP, instant messaging, and presence. These applications and services are "real-time" in the sense described in RFC 3550. [IETF Areas] | Relevant Working Groups: geopriv (Geographic Location/Privacy) |  |  |
| CloudSDN | Working Group | Real-Time Applications | IETF | geopriv (Geographic Location/Privacy) | The IETF has recognized that many applications are emerging that require geographic and civic location information about resources and entities, and that the representation and transmission of that information has significant privacy and security implications. We have created a suite of protocols that allow such applications to represent and transmit such location objects and to allow users to express policies on how these representations are exposed and used. The IETF has also begun working on creating applications that use these capabilities, for emergency services, general real-time communication, and other usages. https://datatracker.ietf.org/wg/geopriv/charter/ | Working Group Documents: https://datatracker.ietf.org/wg/geopriv/ |  |  |
| CloudSDN | Area | Routing | IETF | Routing Area | The Routing Area is responsible for ensuring continuous operation of the Internet routing system by maintaining the scalability and stability characteristics of the existing routing protocols, as well as developing new protocols, extensions, and bug fixes in a timely manner. Forwarding methods (such as destination-based unicast and multicast forwarding, MPLS, and pseudowire) as well as associated routing and signalling protocols (such as OSPF, IS-IS, BGP, RSVP-TE, LDP, PIM, L1-, L2-, and L3-VPNs) are within the scope of the Routing Area. Traffic engineering routing and signaling protocols are in scope, as is the architecture and protocols for the Path Computation Element that helps to select end-to-end paths for traffic-engineered routing. The Routing Area also works on Generalized MPLS used in the control plane of optical networks as well as security aspects of the routing system. The Routing Area has recently developed a routing protocol (RPL) for use in low- powered and lossy networks. [IETF Areas] | Relevant Working Groups: forces, i2rs, idr, karp, l2vpn, l3vpn, nvo3, pce, sfc, sidr, spring |  |  |
| CloudSDN | Working Group | Routing | IETF | forces (Forwarding and Control Element Separation) | The ForCES working group has created a framework, requirements, a solution protocol, a logical function block library, and other associated documents in support of Forwarding and Control Element Separation. http://datatracker.ietf.org/wg/forces/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/forces/ |  |  |
| CloudSDN | Working Group | Routing | IETF | i2rs (Interface to the Routing System) | I2RS facilitates real-time or event driven interaction with the routing system through a collection of protocol-based control or management interfaces. These allow information, policies, and operational parameters to be injected into and retrieved (as read or by notification) from the routing system while retaining data consistency and coherency across the routers and routing infrastructure, and among multiple interactions with the routing system. The I2RS interfaces will co-exist with existing configuration and management systems and interfaces. http://datatracker.ietf.org/wg/i2rs/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/i2rs/ |  |  |
| CloudSDN | Working Group | Routing | IETF | idr (Inter-Domain Routing) | The Inter-Domain Routing Working Group is chartered to standardize, develop, and support the Border Gateway Protocol Version 4 (BGP-4) [RFC 4271] capable of supporting policy based routing for TCP/IP internets. http://datatracker.ietf.org/wg/idr/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/idr/ |  |  |
| CloudSDN | Working Group | Routing | IETF | karp (Keying and Authentication for Routing Protocols) | The KARP working group is tasked to work with the routing protocol working groups in order to improve the communication security of the packets on the wire used by the routing protocols. This working group is concerned with message authentication, packet integrity, and denial of service (DoS) protection. At present, this charter explicitly excludes confidentiality and non-repudiation concerns. http://datatracker.ietf.org/wg/karp/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/karp/ |  |  |
| CloudSDN | Working Group | Routing | IETF | l2vpn (Layer 2 Virtual Private Networks) | The L2VPN working group is responsible for defining and specifying a limited number of solutions for supporting provider-provisioned Layer-2 Virtual Private Networks (L2VPNs). It will also address requirements driven by cloud computing services and data centers as they apply to Layer-2 VPN services. http://datatracker.ietf.org/wg/l2vpn/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/l2vpn/ |  |  |
| CloudSDN | Working Group | Routing | IETF | l3vpn (Layer 3 Virtual Private Networks) | This working group is responsible for defining, specifying and extending BGP/MPLS IP VPNs solutions (based on RFC4364 and RFC4659) for supporting provider-provisioned Layer-3 (routed) Virtual Private Networks (L3VPNs). http://datatracker.ietf.org/wg/l3vpn/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/l3vpn/ |  |  |
| CloudSDN | Working Group | Routing | IETF | nvo3 (Network Virtualization Overlays) | Support for multi-tenancy has become a core requirement of data centers (DCs), especially in the context of data centers supporting virtualized hosts known as virtual machines (VMs). http://datatracker.ietf.org/wg/nvo3/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/nvo3/ |  |  |
| CloudSDN | Working Group | Routing | IETF | pce (Path Computation Element) | The PCE Working Group is chartered to specify the required protocols so as to enable a Path Computation Element (PCE)-based architecture for the computation of paths for MPLS and GMPLS Point to Point and Point to Multi-point Traffic Engineered LSPs. http://datatracker.ietf.org/wg/pce/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/pce/ |  |  |
| CloudSDN | Working Group | Routing | IETF | sfc (Service Function Chaining) | Network operators frequently utilize service functions such as packet filtering at firewalls, load-balancing and transactional proxies (for example spam filters) in the delivery of services to end users. Delivery of these types of services is undergoing significant change with the introduction of virtualization, network overlays, and orchestration. http://datatracker.ietf.org/wg/sfc/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/sfc/ |  |  |
| CloudSDN | Working Group | Routing | IETF | sidr (Secure Inter-Domain Routing) | The purpose of the SIDR working group is to reduce vulnerabilities in the inter-domain routing system. http://datatracker.ietf.org/wg/sidr/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/sidr/ |  |  |
| CloudSDN | Working Group | Routing | IETF | spring (Source Packet Routing in Networking) | Source-based routing mechanisms have previously been specified for network protocols, but have not seen widespread adoption other than in MPLS traffic engineering. These network functions may require greater flexibility and per packet source imposed routing than can be achieved through the use of the previously defined methods. In the context of this charter, 'source' means 'the point at which the explicit route is imposed'. http://datatracker.ietf.org/wg/spring/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/spring/ |  |  |
| CloudSDN | Area | Security | IETF | Security Area | The Security Area is the home for working groups focused on security protocols. They provide one or more of the security services: integrity, authentication, non-repudiation, confidentiality, and access control. Since many of the security mechanisms needed to provide these security services employ cryptography, key management is also vital. [IETF Areas] | Relevant Working Groups: abfab (Application Bridging for Federated Access Beyond web), dane (DNS-based Authentication of Named Entities), httpauth (Hypertext Transfer Protocol Authentication), kitten (Common Authentication Technology Next Generation) |  |  |
| CloudSDN | Working Group | Security | IETF | abfab (Application Bridging for Federated Access Beyond web) | Federated identity facilitates the controlled sharing of information about principals, commonly across organisational boundaries. This avoids redundant registration of principals who operate in multiple domains, reducing administrative overheads and improving usability while addressing privacy-related concerns and regulatory and statutory requirements of some jurisdictions. A number of such mechanisms are in use for the Web. This working group will specify a federated identity mechanism for use by other Internet protocols not based on HTML/HTTP, such as for instance IMAP, XMPP, SSH and NFS.  The design will combine existing protocols, specifically the the Extensible Authentication Protocol (EAP - RFC 3748), Authentication , Authorization and Account Protocols (RADIUS – RFC 2865 and Diameter – RFC 3588), and the Security Assertion Markup Language (SAML). http://datatracker.ietf.org/wg/abfab/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/abfab/ |  |  |
| CloudSDN | Working Group | Security | IETF | dane (DNS-based Authentication of Named Entities) | Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name. http://datatracker.ietf.org/wg/dane/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/dane/ |  |  |
| CloudSDN | Working Group | Security | IETF | httpauth (Hypertext Transfer Protocol Authentication) | Authentication of users to servers over HTTP has always been a weak point in web services. The current HTTP authentication mechanisms, basic and digest, pass the credentials in the clear or employ weak algorithms and are considered to be insecure today. Authentication through non-standard web forms is much more commonly used, but also pass the credentials in the clear. There is a need for improved mechanisms that can replace or augment HTTP authentication without the need to rely on transport layer security. Only HTTP authentication is in scope for this WG; form-based or "web" authentication is out of scope. http://datatracker.ietf.org/wg/httpauth/charter/ | Working Group Documents: http://datatracker.ietff.org/wg/httpauth/ |  |  |
| CloudSDN | Working Group | Security | IETF | kitten (Common Authentication Technology Next Generation) | The purpose of the Common Authentication Technology Next Generation (Kitten) working group (WG) is to develop extensions/improvements to the GSS-API and to the Kerberos authentication system, shepherd specific GSS-API security mechanisms, and provide guidance for any new SASL-related submissions. http://datatracker.ietf.org/wg/kitten/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/kitten/ |  |  |
| CloudSDN | Area | Transport | IETF | Transport Area | The transport and services area - usually just called "transport area" or "TSV area" - covers a range of technical topics related to data transport in the Internet. The Transport Area works on mechanisms related to end-to-end data transport to support Internet applications and services that exchange potentially large volumes of traffic at potentially high bandwidths. A key focus are mechanisms to detect and react to congestion in the Internet, such as the congestion control algorithms in Internet transport control protocols such as TCP, SCTP, and DCCP, as well as congestion management schemes such as PCN and CONEX. [IETF Areas] | Relevant Working Groups: alto (Application-Layer Traffic Optimization), cdni (Content Delivery Networks Interconnection), storm (STORage Maintenance) |  |  |
| CloudSDN | Working Group | Transport | IETF | alto (Application- Layer Traffic Optimization) | A significant part of the Internet traffic today is generated by peer-to-peer (P2P) applications used for file sharing, real-time communications, and live media streaming. P2P applications exchange large amounts of data, often uploading as much as downloading. In contrast to client/server architectures, P2P applications often must choose one or more suitable candidates from a selection of peers offering the same resource or service. http://datatracker.ietf.org/wg/alto/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/alto/ |  |  |
| CloudSDN | Working Group | Transport | IETF | cdni (Content Delivery Networks Interconnection) | A Content Delivery Network (CDN) is an infrastructure of network elements operating at layer 4 through layer 7, arranged for the efficient distribution and delivery of digital content. Such content includes, but is not limited to, web pages and images delivered via HTTP, and streaming of continuous media delivered via HTTP, RTSP, RTMP, etc. CDNs typically provide services to multiple Content Service Providers (CSPs). http://datatracker.ietf.org/wg/cdni/charter/ | Working Group Documents: http://datatracker.ietf.org/wg/cdni/ |  |  |
| CloudSDN | Working Group | Transport | IETF | storm (STORage Maintenance) | The IETF IPS (IP Storage) and RDDP (Remote Direct Data Placement) working groups have produced a significant number of storage protocols (e.g., iSCSI, iSER and FCIP) for which there is significant usage. The time has come to reflect feedback from implementation and usage into updated RFCs; this work may include: - Implementation-driven revisions and updates to existing protocols (i.e., updated RFCs that match the "running code"). - Interoperability reports as needed for the resulting revised protocols that are appropriate for Draft Standard RFC status. - Minor protocol changes or additions. Backwards compatibility is required. http://datatracker.ietf.org/wg/storm/charter/  | Working Group Documents: http://datatracker.ietf.org/wg/storm/ |  |  |
| CloudSDN | Non-Working Group Mailing List | Management | IETF | openv6 | Discussion of an open interface and a programmable platform to support various IPv6 applications, which may include IPv6 transition technologies, SAVI (Source Address Validation and Traceback), security, data center and etc. This discussion will focus on the problem space, use case and possible protocol extensions. https://www.ietf.org/mailman/listinfo/openv6  | 　 |  |  |
| CloudSDN | Research | Applications, Routing, Transport | IRTF | ICNRG (Information- Centric Networking Research Group) | <http://irtf.org/icnrg> | Current Work: http://trac.tools.ietf.org/group/irtf/trac/wiki/icnrg |  |  |
| CloudSDN | Research | Applications, Routing, Management, Transport | IRTF | SDNRG (Software-Defined Networking Research Group) | SDN aims to benefit all types of networks, including wireless, cellular, home, enterprise, data centers, and wide-area networks. The Software-Defined Networking Research Group (SDNRG) investigates SDN from various perspectives with the goal of identifying the approaches that can be defined, deployed and used in the near term as well identifying future research challenges. In particular, key areas of interest include solution scalability, abstractions, and programming languages and paradigms particularly useful in the context of SDN. In addition, it is an explicit goal of the SDNRG to provide a forum for researchers to investigate key and interesting problems in the Software-Defined Networking field. Finally, the SDNRG provides objective definitions, metrics and background research with the goal of providing this information as input to protocol, network and service design to SDOs and others standards producing organizations such as IETF, ETSI, ATIS, ITU-T, IEEE, ONF, MEF and DMTF. http://irtf.org/sdnrg  | Current Work: http://trac.tools.ietf.org/group/irtf/trac/wiki/sdnrg |  |  |
| NFV | Research | 　 | IRTF | NFVRG (Network Functions Virtualization Research Group) | Proposed new research group. | Current Work: http://trac.tools.ietf.org/group/irtf/trac/wiki/nfvrg |  |  |
| Cloud SDN and NFV | Architecture | Implementations of Cloud Services Architectures using SDN and NFV constructs | OpenCloud Connect Technical Committee | OCC 1.0 Reference Architecture with SDN and NFV Constructs | The purpose of the document is to describe possible implementations of Cloud Services Architectures using Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) constructs. | Technical Specification |  | 2015.09 |
| SDN | Architecture | Orchestration | ONF | ONF TR-540 “Orchestration: A More Holistic View” | The purpose of this document is to expand upon the commonly used concept of orchestration and provide further insights regarding its wider features. It offers a brief discussion of differences in the way the term has been used across the industry, and why and how these differences matter. The document explores the overall functionality that must be provided, whether encompassed in a single large-scale orchestration wrapper or partitioned into several sub- functions, of which only one component is called an orchestrator. | Technical Recommendation |  | 2017-02 |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_