International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Q
Supplement 67
(04/2015)

SERIES Q: SWITCHING AND SIGNALLING

Framework of signalling for software-defined networking

ITU-T Q-series Recommendations – Supplement 67

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 67 to ITU-T Q-series Recommendations

Framework of signalling for software-defined networking

Summary

Supplement 67 to ITU-T Q-series Recommendations 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. This Supplement should also be helpful in enabling the development of a signalling protocol(s) capable of supporting traffic flows.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q Suppl. 67	2015-04-29	11	11.1002/1000/12503

Keywords

SDN, signalling model, software-defined networking.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 67 to ITU-T Q-series Recommendations

Framework of signalling for software-defined networking

1 Scope

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 signalling information elements identified will enable the development of a signalling protocol(s) capable of supporting traffic flows.

2 References

[ITU-T M.3400] Recommendation ITU-T M.3400 (2000), *TMN management functions*.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of Software-Defined Networking*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), Information technology – *Cloud Computing – Overview and Vocabulary.*

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 Communication as a Service (CaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.2 Network as a Service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.3 service chain [ITU-T Y.3512]: An ordered set of functions that is used to enforce differentiated traffic handling policies for a traffic flow.

3.1.4 software-defined networking (SDN) [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 middlebox: A computer networking device that caches, transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding.

3.2.2 orchestration: Functionality that provides the automated management and coordination of network resources and services.

3.2.3 white-box: A general purpose data processing device that provides reconfigurable and customizable middle box functions (e.g., network address translation (NAT), cache, deep packet inspection (DPI), intrusion detection systems (IDS), etc.) for purposes other than packet forwarding. It can be implemented in a virtualized manner.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ACL	Access Control List
API	Application Programming Interface
AS	Autonomous System
BGP	Border Gateway Protocol
CaaS	Communication as a Service
CE	Control Entity
DPI	Deep Packet Inspection
FCAPS	Fault, Configuration, Accounting, Performance and Security
FE	Functional Entity
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Internet Protocol
LBS	Location-Based Service
M2M	Machine to Machine
MIS	Media Independent Service
MN	Mobile Node
MPLS	Multi-Protocol Label Switching
NaaS	Network as a Service
NAT	Network Address Translation
NE	Network Entity
NFV	Network Function Virtualization
ONF	Open Networking Foundation
QoS	Quality of Service
RAN	Radio Access Network
SDN	Software-Defined Networking
SLA	Service Level Agreement
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

5 Conventions

In this Supplement:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Supplement is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Supplement.

6 Signalling requirements and scenarios

6.1 SDN-enabled network

In the SDN-enabled network scenario, the centralized SDN controller creates a traffic path from one edge of the network to the other edge of the network using certain protocols over the southbound interface, such as OpenFlow [b-ONF], which programs this traffic on each node in the path, including edge, aggregation and core switches/routers. The first packet of the new traffic is sent to a centralized SDN controller which applies policy, computes the paths and uses the southbound interface to direct this traffic into each node on the path.

Considering that this approach brings several problems, the following issues are recommended to be solved:

- It creates an explosion of forwarding states on the physical switches/routers;
- The SDN controller should communicate with each of the physical switches/routers in the path when a new traffic is needed to be programed;
- This model unavoidably brings extra latency.

6.2 SDN-enabled overlay network

In the SDN-enabled overlay network scenario, the centralized SDN controller uses overlay tunnels to virtualize the network. These tunnels generally terminate in virtual switches/routers, and can also terminate in physical switches/routers. This scenario reduces the size of the forwarding states in the physical underlay nodes and may not touch the physical switches when adding a new tenant or virtual machine (VM). Most importantly, the SDN controller provides a seamless migration path for introducing SDN into the existing production networks.

There are multiple data plane protocols which can be used to create overlay tunnels. Taking OpenFlow as an example, it can just be deployed at the edge of the network and does not touch the aggregation and core physical switches/routers. In that case, OF-Config [b-ONF] is used to create overlay tunnels and OpenFlow is used to program traffic into the tunnels.

However, in this scenario, it is very difficult to provide per-tenant or per-VM quality of service (QoS), because every packet is encapsulated into a tunnel. Support of fine-grained queuing is recommended in order to isolate tenants and provide per-tenant QoS, respectively.

6.3 SDN controller related requirements and scenarios

6.3.1 Hybrid network

This deployment model allows the co-existence of traditional environments of closed vendors' router/switches and OpenFlow-enabled devices. This hybrid approach refers to the interconnection

of both the control and data planes of legacy and new network elements, which can be regarded as the smooth migration for the existing network. Figure 6-1 depicts the hybrid network model. The legacy controller mentioned in this figure is not limited to the server and can be extended to other device types. The route reflector for example, which is the most popular way to distribute border gateway patrol (BGP) routes between routers of the same autonomous system (AS), can be regarded as a legacy controller. It is required to provide the dedicated gateway-like component between the existing legacy controllers and OpenFlow controllers in the new control plane.

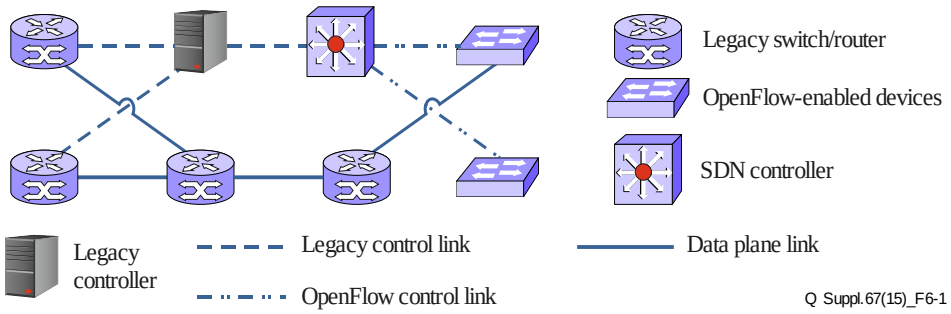

Figure 6-1 – Hybrid network model

6.3.2 Interactions between different SDN domains

With more deployments in carrier-grade networks, it is impossible for any single SDN controller to contain all of the operational states for the entire system. Therefore, the issue of interoperability of SDN controllers (also known as east-west interface) becomes critical. It is necessary to establish controller nodes peering either within the same administrative domain (intra-domain), or between administrative domains (inter-domain) in a multi-vender environment. The east-west interface signalling should guarantee the synchronization of states among the federated controller nodes. If there is transient inconsistency, it is necessary to make a local decision on which control instance state to utilize.

Considering the combined advantages of scalability, high-availability and low-cost, the requirement of smooth migration from the existing network should be taken into account. It is required to reduce network complexity, simplify operation, prevent loss of performance, and integrate SDN systems with the existing infrastructure and service logic in the carrier-grade network, such as BGP, multi-protocol label switching (MPLS) and virtual private network (VPN). Therefore, it is realistic to adopt mature protocols for the east-west interface which have been deployed in the production network for many years.

Based on the above analysis and requirements, the standard BGP can optionally be the east-west interface for the establishment of federation for SDN controllers.

6.3.3 Orchestration function based on cloud services

With the development of cloud services, more networking management and orchestration ability is required. Network as a service (NaaS), as defined in [ITU-T Y.3500], is an example of a category of cloud services in which the capability provided to the CSC is transport connectivity and related network functionalities. NaaS general requirements described in [ITU-T Y.3501] include on-demand network configuration, secure connectivity, QoS-guaranteed connectivity and heterogeneous networks compatibility. SDN is one of major supporting technologies for NaaS delivery.

In the SDN signalling model framework, NaaS can be regarded as an SDN-enabled application and delivered by cloud management platform, which needs to communicate with the SDN orchestration function. It is required to provide the interface between the cloud management platform and the SDN orchestration function in order to tightly integrate the computing and networking provision.

Taking a concrete scenario as an example, in the multi-tenant context, VM instances of the same tenant are always deployed on the different computing nodes and they interconnect via a specific tenant network, i.e., virtual local area network (VLAN). When live migration of VM occurs across different computing nodes, even a geographically distributed data center, it is necessary in order for the network policies attached to the migrated VM to be aware of the migration and to be re-deployed at the new port of the VM automatically.

6.3.4 Orchestration function for middlebox management

As deployment of middleboxes (e.g., cache, firewall, NAT, etc.) inside both fixed and mobile networks have become increasingly more widespread, it has resulted in many challenges, as well as criticism, due to poor interaction with higher layer control systems (i.e., orchestration and SDN controller). See Figure 6-2.

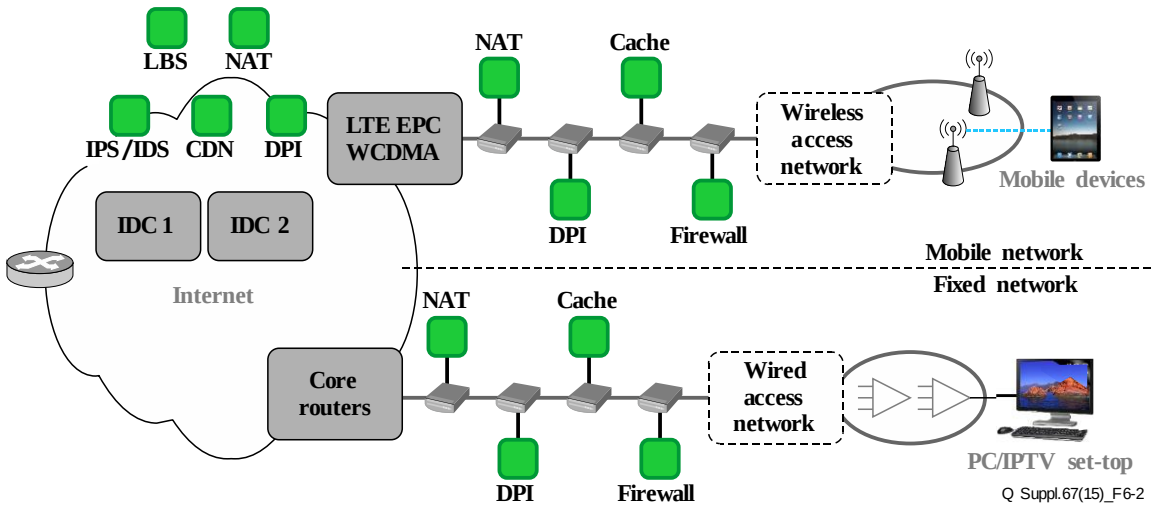

Figure 6-2 – Middleboxes in the fixed and mobile networks

In order to provide service chaining, connection establishment and fault monitoring, the SDN environment is required to support unified middlebox management to efficiently control and interconnect between network switching components and the middlebox.

It is required to:

– Support middlebox monitoring for checking their availability, resource status, etc.;

– Get the topology information of all the middlebox connectivity;

– Support middlebox control for establishing middlebox services.

6.3.5 Orchestration function for white-box management

Network function virtualization (NFV) [b-ETSI NFV] is a similar concept in nature to SDN in that both aim to transform network management from the hardware layer to the software layer. In addition, NFV is a technology that utilizes virtualization technologies to manage network functions via software as opposed to having to rely on proprietary hardware to handle these functions.

Figure 6-3 shows one possible scenario for white-box deployment in the fixed and mobile networks.

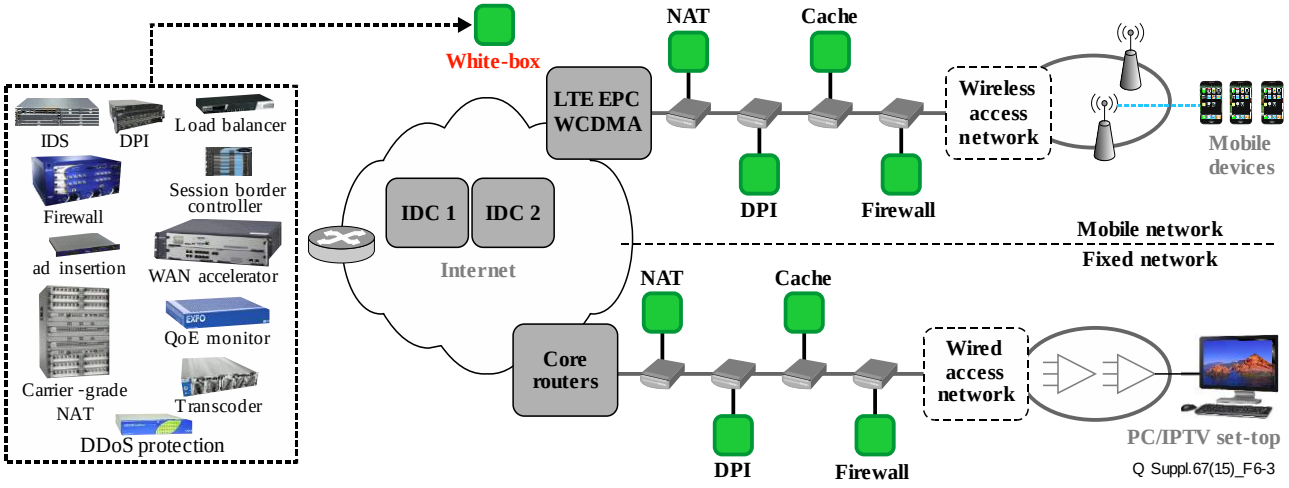

Figure 6-3 – White-boxes in the fixed and mobile networks

In order to provide installation, reconfiguration and customization regarding the SDN environment, it is needed to support unified white-box management to efficiently control and interconnect between SDN components and white-boxes.

It is additionally recommended to provide:

– Functionality of monitoring white-boxes for checking their availability, resource status (e.g., CPU, memory, storage, etc.), capacity, etc.;

– Functional information such as service description, service type, vendor, software versions, etc.;

– Topology and connectivity information of middle-boxes such as internet protocol (IP) address, network domain, port, interface, location, etc.

6.4 Software-defined mobile network

Software-defined mobile network (SDMN) is an approach to the design of wireless mobile networks where the centralized SDN controller enables a mobility management of core network, a traffic path and resource management of radio access networks (RANs) using southbound and northbound application programming interfaces (APIs). It is the future wireless mobile network integration of various RANs connected through an SDN controller. The SDMN presents an SDN architecture for a mobile network composed of a controller, access and core commodity switches, and middleboxes supporting fine-grained policies. All protocol-specific features are implemented in software, maximizing the use of generic and commodity hardware and software in both the core network and RAN. OpenFlow-like protocol could be used to control various wireless networks by supporting the requirements of long term evolution (LTE) and WiFi radio access technologies with specific southbound and northbound APIs.

In SDMNs, the logically centralized controller facilitates the implementation of cooperative techniques for mobility management in the core networks. The centralized controller will concentrate the network intelligence for reducing operational cost and providing automation. Moreover, network functions such as mobility, load balancing and firewalls will be deployed as software applications.

The logically centralized controller also enables radio resource allocation decisions to be made with global visibility across many base stations, which is far more optimal than the distributed radio resource management (RRM) and seamless handover in use today. By centralizing network intelligence, RRM decisions can be adjusted based on the dynamic power and subcarrier allocation profile of each base station to support seamless handover.

The network controller and the southbound and northbound protocols to be used in SDMN should be carefully designed and extended, and new network applications should be identified and implemented.

7 Signalling model

The signalling model presented in Figure 7-1 is aligned with the high-level architecture of SDN specified in [ITU-T Y.3300].

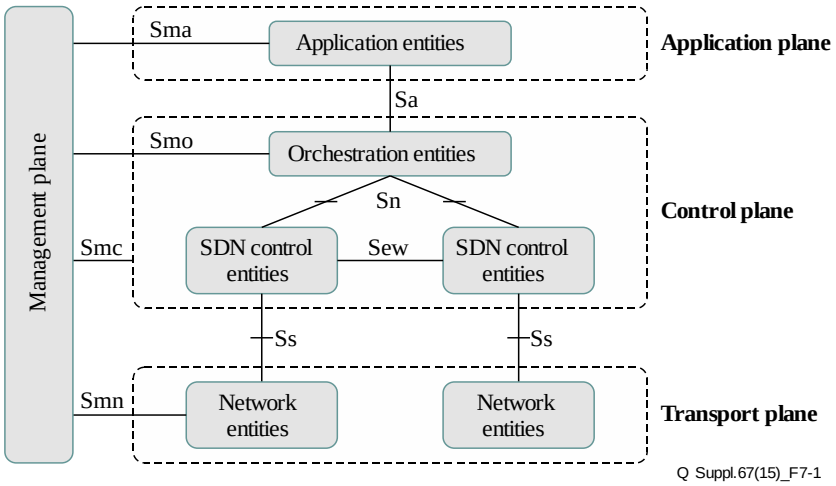

Figure 7-1 – The signalling model of SDN framework

Figure 7-1 depicts the basic signalling model of SDN framework which consists of three horizontal planes and one vertical plane. These are the: Application plane, control plane, transport plane and management plane.

In the application plane, the application entities, i.e., SDN-enabled applications, communicate their network needs/policies/requirements/hints to the orchestration entities in the control plane.

The orchestration entities in the control plane provide network service open API and service control, e.g., service provision, service composition/encapsulation/exposure and negotiation between different SDN control entities. These also provide middlebox management functions such as checking their availability, monitoring resource status and providing connection information (e.g., IP address, port, etc.).

The SDN control entities (CE) in the control plane perform logically centralized control of network entities (NEs), translating the intention communicated with orchestration entities to detailed instructions that are sent to the underlying, low-level SDN data paths, and offering an abstraction of the SDN data paths to provide a logical view of the network. There will also be interactions between SDN control entities if they are in different administrative domains.

In the transport plane, the NEs perform forwarding and processing capabilities.

The management plane provides functionalities for traditional fault management, configuration management, accounting management, performance management and security management (FCAPS), as described in [ITU-T M.3400]. The management plane interacts with all the horizontal planes.

8 Description of interfaces in the signalling model

8.1 Sa

The Sa interface permits application entities, e.g., SDN-aware network services, applications, or other users of SDN to interact with the orchestration entities. HTTP (such as RESTful web API) or other protocols may run over this interface. Applications' explicit requirements and network state, stats and events can be exchanged between application entities and orchestration entities via this interface.

8.2 Sn

The Sn interface permits interactions between orchestration entities and SDN control entities, providing the generation of detailed or abstracted views of the networks to permit the orchestration entities to configure / manage / control the SDN CEs by interacting with the view. This interface translates the applications' requirements and enforces behaviours of orchestration entities. The functions of this interface include:

- Topology discovery:

  The Sn interface exchanges an abstracted view of the network topology and the application-control commands. It is related to the network topology and status discovery of the control domains for the abstract view of the network resources (e.g., abstract topology, network state, utilization) and its corresponding signalling requirements.
- Service provisioning:

  The orchestration entities coordinate multiple SDN controller entities to enable these services. The services may be provided automatically or manually.
- Resilience and reliability:

  The Sn interface shall provide reliable transfer of signalling messages related to functionalities for supporting fault monitoring and resilience management across multiple domains.

8.3 Sew

The Sew interface permits the SDN CEs to interact, either within the same administrative domain (intra-domain), or between administrative domains (inter-domain). It is recommended that it support the following:

- Cloud mode, as well as network and communications services, e.g., NaaS and communication as a service (CaaS) as defined in [ITU-T Y.3500]. The services may be provided automatically or manually. SDN CEs should support service establishment, release, query and restoration over the Sew interface;
- Path computation element (PCE), in order to design paths that meet bandwidth, latency and other QoS requirements of services, and to make special computational components and cooperation between the different SDN domain controllers over the Sew interface. The computation of optimal inter-domain paths may be achieved using the services of one or more PCEs;
- Scalability refers to the ability of the SDN CEs to support ever-increasing requests and support for different services with an existing SDN infrastructure;
- Resilience and reliability refers to the ability of the CEs to continue operations under failure conditions and the ability of the CEs to recover their operation due to failure conditions.

The intra-domain Sew interface is typically a single-vendor interface contained within a single-carrier network. Since it is single-vendor, this interface may contain proprietary elements specific to that vendor.

The Sew interface is an inter-domain interface between controllers within the SDN networks that cross domain boundaries. Domain boundaries are defined by the carriers and can include administrative boundaries within a carrier's network, boundaries between different vendors within a carrier's network or boundaries between carriers. The information exchanged across the inter-domain Sew interface is usually more restricted than that exchanged across the intra-domain Sew interface. The intra-domain Sew interface may have proprietary elements, whereas the inter-domain Sew interface is standardized to allow for multi-vendor interoperability.

8.4 Ss

The Ss interface permits the interaction between the network entities and the SDN control entities. The OpenFlow protocol and the OF-Config protocol may run over this interface. This interface drives the low-level control of underlying network devices.

8.5 Sma

The Sma interface permits the interaction between the management plane and application entities. Via this interface, the performance of the applications can be monitored and the service level agreement (SLA) can be assured. The management plane also performs the initial configuration via this interface.

8.6 Smo

The Smo interface permits the interaction between the management plane and the orchestration entities. Via this interface, the policy configuration and the software updates of orchestration entities can be provided.

8.7 Smc

The Smc interface permits the interaction between the management plane and SDN control entities. Via this interface, the policy configuration and software update of control entities can be provided. In addition, the network status can also be collected for continuous policy adaptation over this interface.

8.8 Smn

The Smn interface permits the interaction between the management plane and the network entities. Via this interface, the initial device setup/configuration and software update of network entities can be provided. The network performance monitoring, fault isolation and energy-efficient operation can also be implemented over this interface.

9 Signalling protocol procedures

9.1 Procedure for VM live migration

As described in clause 6.3.3, VM live migration across different computing nodes, even a geographically distributed data centre, requires network policies (such as access control list (ACL), QoS, etc.) attached to the migrated VM to be aware of the migration action and be re-deployed at the new port of the VM automatically. In this context, the management plane acts as a cloud computing management platform, which is responsible for the configuration, control, deployment and management of computing and storage resources, and interacts with orchestration entities to exchange the VM migration notice. The orchestration entities take the VM migration role of awareness and trigger the updated network policies on SDN entities. The detailed information flows are illustrated in Figure 9-1, as follows:

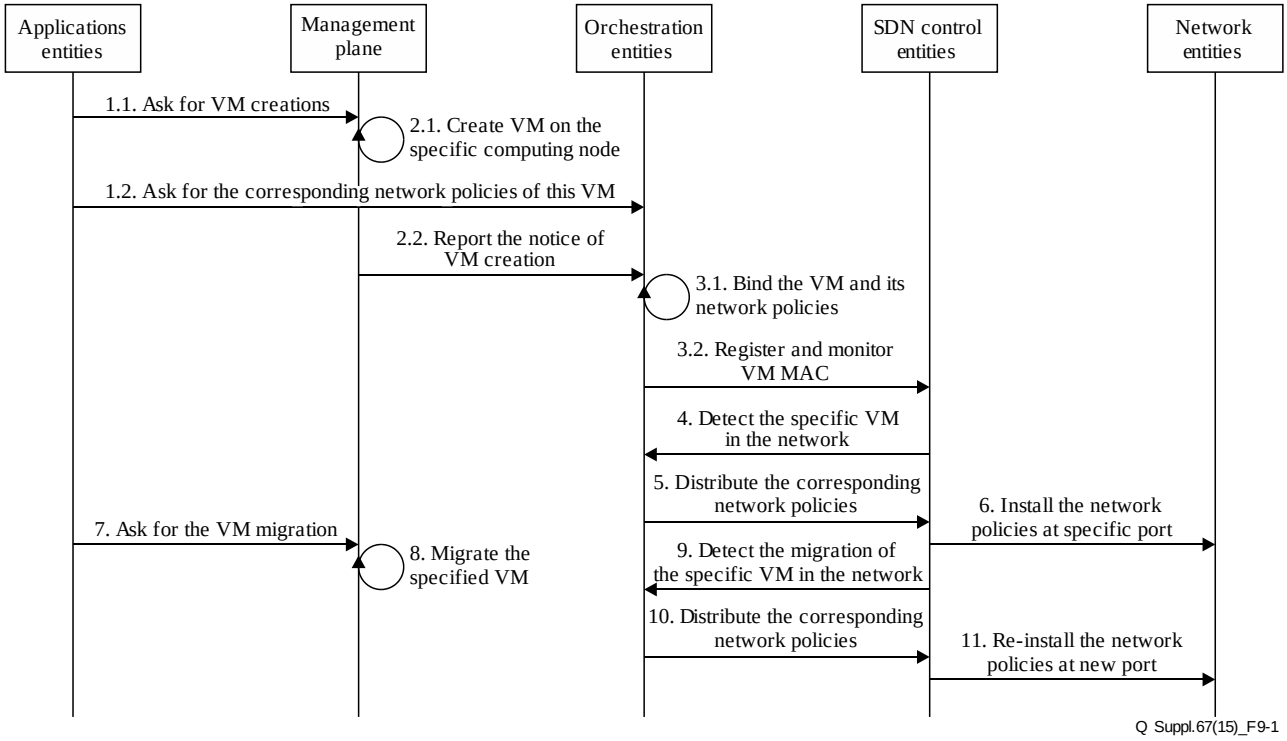

Figure 9-1 – VM live migration procedures

1. Application entities ask for VM creation and corresponding network policies from the management plane and orchestration entities, via Sma and Sa interfaces, respectively, according to the tenant's demands;
2. Management plane, acting as a cloud computing management platform, sends the command to the specific computing node and reports the VM creation to the orchestration entities via the Smo interface;

NOTE – The execution of commands received from the management plane on computing nodes, such as VM creation, VM migration, etc., is out of the scope of this Supplement.

3. Orchestration entities bind the VM and its network policies, note this mapping and register this VM MAC on SDN control entities and monitor its status changes;
4. SDN control entities detect the specific VM in its controlled network and report to the orchestration entities;
5. Orchestration entities check the VM and network policies mapping and distribute the bound network policies of the specific VM to SDN control entities;
6. SDN control entities install the network policies at the corresponding port of the specific VM;
7. Application entities ask for the VM migration;
8. The management plane sends the command to the original and target computing nodes, respectively;
9. SDN control entities detect the migration of the specific VM in its controlled network and report to the orchestration entities;
10. Orchestration entities check the VM and network policies mapping and distribute the bound network policies of the specific VM to SDN control entities;
11. SDN control entities re-install the network policies at the corresponding port of the specific VM and remove the ones at the original port.

Appendix I

Scenarios and corresponding requirements of Ss for seamless handover

Recently, about 90% of a company's traffic comes from native mobile applications. We have accomplished disruptive advances in mobile networks in terms of the number of mobile devices and services offered. Moreover, the increase in the number of mobile devices will be exponential with the explosion of the Internet of Things (IoT), including wearable computers and machine to machine (M2M) communications.

Open networking foundation (ONF) listed the challenges and benefits of SDN for mobile and wireless networks [b-ONF]. Software-defined mobile network (SDMN) is an approach to the design of wireless mobile networks where the centralized SDN controller enables a traffic path and resource management of mobile access networks using southbound and northbound APIs. The mobile access networks utilize radio access technologies that are no longer homogeneous or static.

In SDMNs, most of the mobile applications are based on radio-specific interaction functions. The interaction deals with L1/L2 functions, specifically the interaction among heterogeneous RAN technologies. This interaction also introduces new challenges in radio resource allocation or seamless handover. The SDN paradigm is used to control RANs since the centralized controller can simplify radio resource managements and lower mobility management costs.

In SDMNs, the centralized controller will concentrate the network intelligence for reducing operational cost and providing seamless mobility. The logically centralized controller facilitates the lower-level control of underlying network entities (NE). The Ss interface permits the interaction between the NEs and the SDN CEs. The OpenFlow protocol and the OF-config protocol may run over this interface. The interactions to support mobility management, seamless handover, radio resource allocation, load balancing and firewalls will be deployed as software applications.

Regarding the interaction to support mobile applications, this Supplement should present specific signalling scenarios on top of the network controller. The scenarios are related with radio resource allocation and seamless handover.

I.1 IEEE 802.21 media independent service (MIS)

The SDMN can be characterized by a clear separation of the control and data planes. The SDMN is the simplest solution for future wireless mobile networks integration where various RANs connected through gateways conserve their independence. It is possible to expect that the logically centralized controller enables the mobile node (MN) to monitor links, allocate resources and enable mobility management for MNs.

The signalling framework of IEEE 802.21-2008 standard [b-IEEE 802.21] can be a common platform to support mobility management in heterogeneous networks. The signalling framework supports seamless handover in heterogeneous RANs by the using Ss interface. Some primitives and messages help the MN to monitor link status (e.g., signal strength and data rate), and some primitives and messages help the MN to control its link layers (physical layer and data link layer) for a seamless handover in heterogeneous RANs.

Some primitives and messages can be used to transfer network configuration information for handover and mobility management via a clearly separated control plane in SDMNs, and thus they can be used to provide seamless network configuration for resource allocations while MN moving across RANs. Thus, the signalling framework using the Ss interface is appropriate for radio resource allocation and mobility management in SDMNs that use various heterogeneous RANs by a clear separation of the control and data plane.

In SDMN, the signalling framework enables the support of mobility management protocols, the interfaces and the services to provide good handover performance without any modification.

I.2 Signalling protocol procedures

In this clause, attention is given to the signalling flow to support seamless handover in heterogeneous radio access technologies. In order to illustrate the signalling flow, we introduce the high-level requirements required to support seamless handover.

Handover refers to the ability of transferring an ongoing call or data session from one NE to another NE, without any interruption, to the ongoing services. The handover procedure for radio resource allocation comprises four stages, as shown in Figure I.1.

In the first stage, handover initiation starts from the link corruption detection until the request for initiating a new link.

In the second stage, handover preparation consists of all steps of link measurements, collection of information about neighbouring networks, and exchange of information about QoS offered by these networks.

In the third stage, the handover decision is the procedure to decide whether the connection is to be switched to a new network based on parameters collected in the handover initiation phase. Radio resource allocation is decided by the NE or SDN CE, based on the radio link status or the radio resource allocation of neighbouring RANs.

In the last stage, radio resources (e.g., frequency, time, interface mode and power) are configured by the NE or SDN CE. MN prepares to connect to the RAN with the newly allocated radio resources as an action of handover execution. After that, the NE reports its allocated radio resources to the SDN CE and neighbouring NE.

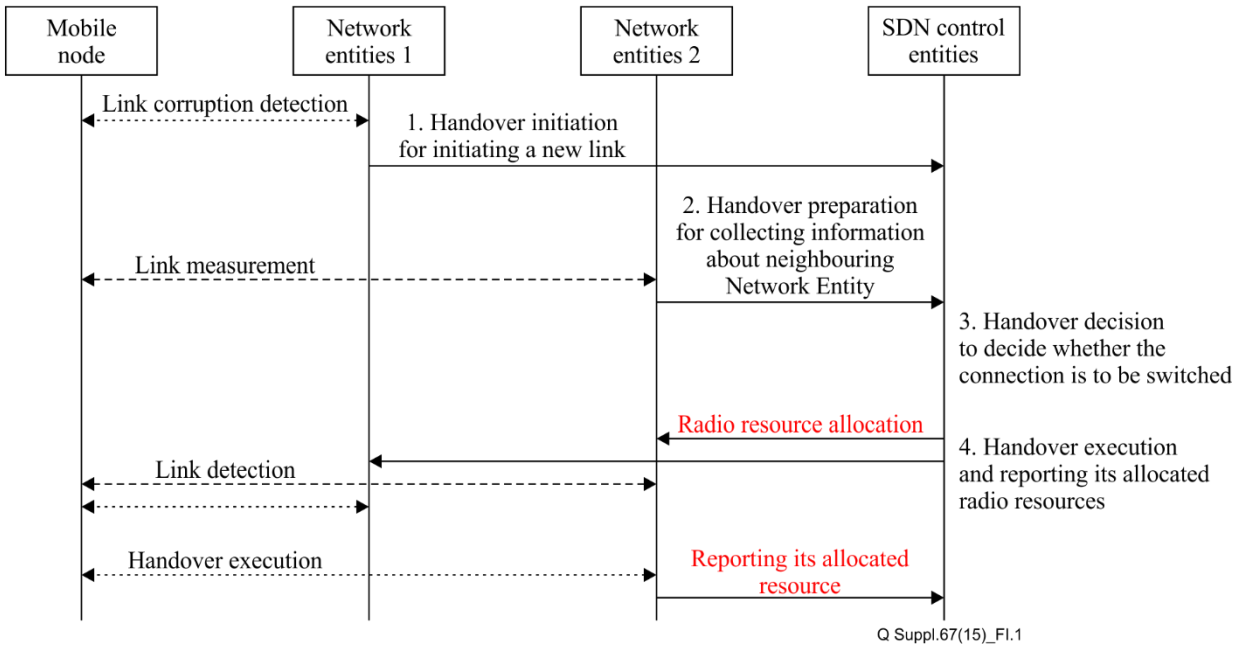

Figure I.1 – Seamless handover in SDMNs procedures

Appendix II

Development methodology of this Supplement

Considering the standardization methodology and conventional study sequence, the signalling model including the FEs and their mutual interfaces should be based on functional requirements which are derived from the corresponding use cases or scenarios. Therefore, it is required to develop this Supplement with the following steps:

Step 1: Signalling scenarios and their derived functional requirements (clause 6);

Step 2: Signalling models with FEs and their mutual interaction, which are based on the functional requirements derived in Step 1 (clauses 7 and 8);

Step 3: Signalling protocol procedures for typical signalling scenarios (clause 9).

As a new paradigm, SDN mainly focuses on separation of control and forwarding. It consists of a series of existing and emerging technologies and can be utilized in many different scenarios, such as cloud computing, data centres, operators' IP carrier network, broadband access network, wireless network, network security, etc. Each SDN-applied scenario has its dedicated solution and different functional requirements. Therefore, the FEs and their reference points in a SDN high-level framework have dedicated descriptions and requirements in different scenarios, respectively.

Bibliography

[b-ETSI NFV ISG] ETSI NFV ISG, *Network Functions Virtualization*, http://portal.etsi.org/portal/server.pt/community/NFV.

[b-IEEE 802.21] IEEE 802.21 (2008), *IEEE Standard for Local and metropolitan area networks – Media Independent Handover Services.*

[b-ONF] Open Networking Foundation, *OpenFlow/Software-Defined Networking (SDN)*, https://www.opennetworking.org/.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016