International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3740
(01/2018)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for SDN – Network signalling and signalling requirements for services

---

Signalling requirements for software-defined networking and network function virtualization-based central office services

Recommendation ITU-T Q.3740

ITU-T

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

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.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
Resource control protocols	Q.3710–Q.3739
Network signalling and signalling requirements for services	**Q.3740–Q.3779**
TESTING SPECIFICATIONS	Q.3900–Q.4099

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

Recommendation ITU-T Q.3740

Signalling requirements for software-defined networking and network function virtualization-based central office services

Summary

Recommendation ITU-T Q.3740 specifies the signalling requirements of an Si interface between a software-defined networking (SDN) controller and network function virtualization orchestration (NFVO) for SDN and central office (CO) services based on network function virtualization (NFV).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3740	2018-01-13	11	11.1002/1000/13486

Keywords

NFVO, SDN, Si interface, signalling requirements.

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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

Page

Recommendation ITU-T Q.3740

Signalling requirements for software-defined networking and network function virtualization-based central office services

1 Scope

This Recommendation specifies interface and signalling requirements of the Si interface between a software-defined networking (SDN) controller and network function virtualization orchestration (NFVO) based on the specific SDN-based central office (CO) services.

NOTE – This Recommendation focuses on the signalling requirement of the Si interface. The candidate protocols for the Si interface are outside the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[ITU-T Y.3302] Recommendation ITU-T Y.3302 (2017), *Functional architecture of software-defined networking*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 software-defined networking [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.

3.1.3 virtualized network function [b-ITU-T Y.3321]: A network function whose functional software is decoupled from hardware, and runs on virtual machine(s).

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 central office: The telephone building that is the origin of the outside loop plant.

NOTE – Based on the definition given in [b-ITU-T G.998.1].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AR Augmented Reality

BRAS	Broadband Remote Access Service
CO	Central Office
CoA	Change of Authorization
CGN	Carrier Grade Network address translation
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DPI	Deep Packet Inspection
ID	Identifier
IP	Internet Protocol
MAN	Management
MANO	Management and Orchestration
NAT	Network Address Translation
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVO	Network Function Virtualization Orchestration
NFVRS-REP	NFV-related Resource Scaling Response
NFVRS-REQ	NFV related Resource Scaling
OLT	Optical Line Terminal
PNF	Physical Network Function
PPPoE	Point-to-Point Protocol over Ethernet
QoS	Quality of Service
SCC-REP	Service Chain Creation Response
SCC-REQ	Service Chain Creation Request
SDN	Software-Defined Networking
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
vBRAS	virtual Broadband Remote Access Service
vCPE	virtual Customer Premises Equipment
VIM	Virtualized Infrastructure Management
VNF	Virtualized Network Function
VNFC-REP	VNF Creation Response
VNFC-REQ	VNF Creation Request
VNFFG	VNF Forwarding Graph
VNFL-REP	VNF List-related status Response
VNFL-REQ	VNF List-related status Request

VNFM	Virtualized Network Function Management
VNF-REP	VNF-related status Response
VNF-REQ	VNF-related status Request
vOLT	virtual Optical Line Terminal
VPN	Virtual Private Network
VR	Virtual Reality
XML	extensible Markup Language

5 Convention

In the body of this Recommendation and its appendixes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

{A}: indicates that the parameter A is mandatory;

*: indicates that the parameter may be multiple items.

6 Background

The CO is a common carrier switching centre in which trunks and loops are terminated and switched. Usually, it includes the access switches/optical line terminal (OLT) and network edge routers (BRAS), which cooperate to provide Internet access services to customers.

The CO, which now is equipped with SDN and network function virtualization (NFV) technologies, gains the capabilities of developing diverse Internet access services much more easily and faster. Figure 6-1 shows the functional architecture of CO, which is aligned with the high-level architecture of SDN specified in [ITU-T Y.3300] and [ITU-T Y.3302], including the physical broadband remote access service (BRAS), customer premises equipment (CPE), OLT, virtual broadband remote access service (vBRAS), virtual customer premises equipment (vCPE), virtual optical line terminal (vOLT). The SDN controller can communicate with NFVO via the Si interface, and they can perform network function management and service orchestration.

NOTE – The capabilities of NFVO are based on [b-ETSI GS NFV-MAN 001].

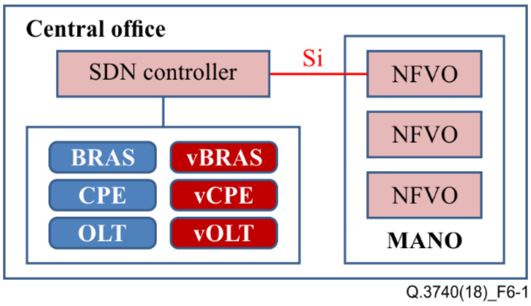

Figure 6-1 – Functional architecture of central office based on SDN and NFV technologies

The Si interface is that between the SDN controller and the NFVO. A message can be exchanged between these two functional entities over this interface in support of the following interface requirements:

– the SDN controller queries NFV-related resources from NFVO;

– when the SDN controller receives a service request from a customer, it requests NFVO to create a specific virtualized network function (VNF), which does not exist;
– when the existing VNF cannot satisfy the additional demands of the customer, the SDN controller requests NFVO to extend or shrink the virtual resources;
– according to the specific service, which requires the combined VNFs in a certain sequence, the SDN controller requests NFVO to create the service chain.

7 Signalling requirements for Si

7.1 Overview of signalling requirements

The messages over the Si interface are classified into the following four categories.

NOTE 1 – NFV-elated resources include VNF, service chain VNFG and network function virtualization infrastructure (NFVI), as well as resources such as central processing unit (CPU), memory and sessions.

Category 1: Status request

– VNF and VNF list request message and response message.

Category 2: VNF creation

– VNF creation message and response message.

Category 3: Resource scaling

– NFV-related resource extension/shrink message and response message.

Category 4: Service chain creation

– Service chain creation message and response message.

NOTE 2 – No transport protocol for the signalling messages is specified here. No message content format is specified here either.

The signalling messages may be XML-based messages over (or carried by) the transmission control protocol (TCP), user datagram protocol (UDP), stream control transmission protocol (SCTP), transport layer security (TLS), etc. All of the messages consist of the message header and the message body.

The message format is described in Figure 7-1.

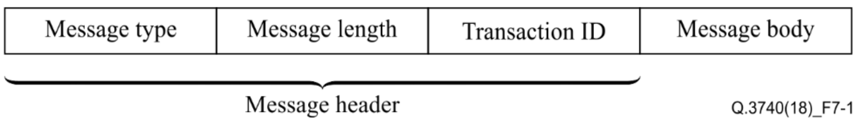

Figure 7-1 – Message composition

The message header field contains the following information.

– Message type: uniquely specifies the type of the message.
– Message length: specifies the length of the message body.
– Message transaction identifier (ID): generated by the sender of the message. If there is a response message for the request message, the transaction IDs of the request and response messages are the same.

The message body field contains the message contents.

7.2 Signalling requirements for status request

7.2.1 VNF list request message and response message

The VNF list-related status request (VNFL-REQ) message, indicated by the message type in the message header field, is sent by the SDN controller to the NFVO in order to get the VNF list resources.

Message format:

```
<VNFL-REQ-Message> ::= < Message Header >
```

The VNF list response (VNFL-REP) message, indicated by the message type in the message header field, is sent by the NFVO to the SDN controller in response to the VNFL-REQ message.

Message format:

```
<VNFL-REP-Message> ::= < Message Header >
                       *{VNF-Address}
                       *{VNF-Parameters}
```

VNF-Address uniquely specifies a VNF.

VNF-Parameters mean one or multiple parameters of the VNF mentioned in the foregoing. It includes, but not limited to:

– Available IPv4/IPv6 session uniquely specifies the available number of IPv4/IPv6 sessions;
– Available Service Specific Session uniquely specifies the available number of service specific sessions;
– Available CPU uniquely specifies the available CPU resources;
– Available Memory uniquely specifies the available memory resources;
– Available Bandwidth uniquely specifies the available bandwidth resources.

7.2.2 VNF request message and response message

The VNF-related status request (VNF-REQ) message, indicated by the message type in the message header field, is sent by the SDN controller to the NFVO in order to get the status of a specific VNF.

Message format:

```
<VNF-REQ-Message> ::= < Message Header >
                      {VNF-Address}
```

Meanings and explanations:

VNF-Address uniquely specifies a VNF.

The VNF-related status response (VNF-REP) message, indicated by the message type in the message header field, is sent by the NFVO to the SDN controller in response to the VNF-REQ message.

Message format:

```
<VNF-REP-Message> ::= < Message Header >
                      {VNF-Address}
                      *{VNF-Parameters}
```

VNF-Address uniquely specifies the VNF.

VNF-Parameters means one or multiple parameters of VNF. It includes, but is not limited to:

– Available IPv4/IPv6 session uniquely specifies the available number of IPv4/IPv6 sessions;

– Available service specific session uniquely specifies the available number of service specific sessions;
– Available CPU uniquely specifies the available CPU resources;
– Available Memory uniquely specifies the available memory resources
– Available Bandwidth uniquely specifies the available bandwidth resources.

7.3 Signalling requirements for VNF creation

The VNF creation request (VNFC-REQ) message, indicated by the message type in the message header field, is sent by the SDN controller to the NFVO.

Message format:

```
<VNFC-REQ -Message> ::= < Message Header >
                        { VNF-name}
                      * { Required-resource-parameters}
```

Meanings and explanations:

VNF-name uniquely specifies the VNF.

Required-resource-parameters uniquely specifies required resource parameters for the specific VNF, it indicates but not limited to:

– Required CPU uniquely specifies the CPU resources the VNF needed;
– Required Memory uniquely specifies the memory resources the VNF needed;
– Required Bandwidth uniquely specifies the bandwidth resources the VNF needed;
– Required Service Specific Resources uniquely specify resources needed for the VNF.

NOTE – For example, for the carrier grade network address translation (CGN) VNF, the specific resources needed are IPv4 and IPv6 session resources and IPv4 and IPv6 addresses.

The VNF creation response (VNFC-REP) message, indicated by the message type in the message header field, is sent by the NFVO to the SDN controller.

Message format:

```
<VNFC-REP-Message> ::= < Message Header >
                       { VNF-name}
                       {Instantiated-resources}
```

Meanings and explanations:

VNF-name uniquely specifies the name of VNF that is created.

Instantiated-resources uniquely specifies the VNF resources instantiated for the VNF, it indicates but is not limited to:

– Instantiated CPU uniquely specifies the CPU resources the VNF needs;
– Instantiated Memory uniquely specifies the memory resources the VNF needs;
– Instantiated Bandwidth uniquely specifies the bandwidth resources the VNF needs;
– Instantiated Service Specific Resources uniquely specify the resources needed for certain VNFs.

7.4 Signalling requirements for resource scaling

The NFV-related resource scaling request (NFVRS-REQ) message, indicated by the message type in the message header field, is sent by the SDN controller to the NFVO.

Message format:

```
<NFVRS-REQ-Message> ::= < Message Header >
                        *{ VNF-address}
                        *{required-resources}
```

Meanings and explanations:

NOTE – All the parameter values of this message could be positive or negative numbers. A positive number indicates resource extension; a negative number indicates resource shrink.

VNF address uniquely specifies the required VNF.

Required resources includes but is not limited to:

a) Required CPU resources uniquely specify the required CPU resource for scaling;

b) Required Memory resources uniquely specify the required memory for scaling;

c) Required Bandwidth uniquely specifies the required bandwidth for scaling;

d) Required Service specifies the service specific resources; it indicates but is not limited to:

   i) Required IPv4/IPv6_session uniquely specifies the required IPv4/IPv6 session for scaling,

   ii) Required IPv4/IPv6 addresses uniquely specifies the required IPv4/IPv6 address for scaling.

The NFV-related resource scaling response (NFVRS-REP) message, indicated by the message type in the message header field, is sent by the NFVO to the SDN controller in response to the NFVRS-REQ message.

Message format:

```
<NFVRS-REP-Message> ::= < Message Header >
                         *{ VNF-address }
                          *{scaled-resources}
```

Meanings and explanations:

VNF-address uniquely specifies the VNF that needs resource scaling.

Scaled-resources uniquely specifies the scaled resources, it indicates but is not limited to:

Scaled CPU uniquely specifies the scaled CPU resources for the VNF:

a) Scaled Memory uniquely specifies the scaled memory for the VNF;

b) Scaled Bandwidth uniquely specifies the scaled bandwidth for the VNF;

c) Scaled Service specific resources, indicates but is not limited to:

   i) Scaled IPv4/IPv6_session uniquely specifies the scaled IPv4/IPv6 session for scaling,

   ii) Scaled IPv4/IPv6 addresses uniquely specifies the scaled IPv4/IPv6 address for scaling.

7.5 Signalling requirements for service chain creation

The service chain creation request (SCC-REQ) message, indicated by the message type in the message header field, is sent by the SDN controller to NFVO in order to create the service chain.

When the SDN controller receives a service request from a customer, the SDN controller sends this message to NFVO to request NFVO to create a service chain.

Message format:

```
<SCC-REQ Message> ::= < Message Header >
                      {Service-Chain-ID}
                       {Required-VNF-forwarding-graph}
```

Meanings and explanations:

Service-Chain-ID uniquely specifies the identification of service chain in CO.

Required-VNF-forwarding-graph (VNFFG) specifies the VNFFG required by the specific service chain.

The service chain creation response (SCC-REP) message, indicated by the message type in the message header field, is sent by the NFVO to the SDN controller.

Message format:

```
<SCC-REP-Message> ::= < Message Header >
                      {Service-Chain-ID}
                      {Instantiated-VNF-forwarding-graph}
```

Service-Chain-ID uniquely specifies the identification of service chain in CO.

Instantiated VNFFG specifies the VNFFG instantiated for specific services.

Appendix I

Signalling scenarios

(This appendix does not form an integral part of this Recommendation.)

NOTE – This appendix describes the typical scenarios in the CO and indicates specific information exchanged between an SDN controller and NFVO. The physical device and virtual device coexist in the CO and the SDN controller should consider them as a whole.

I.1 Scenario 1: Traffic scheduling within the virtual broadband remote access service pool

The vBRAS pool can meet the real-time traffic demand by extending and shrinking the VNF and NFVI resources of vBRAS flexibly. One of the main targets of the vBRAS pool service is traffic scheduling, which means distributing the traffic among the vBRASs within the pool. Figure I.1 illustrates the signalling scenario of the point-to-point protocol over Ethernet (PPPoE) requests traffic scheduling within the vBRAS pool.

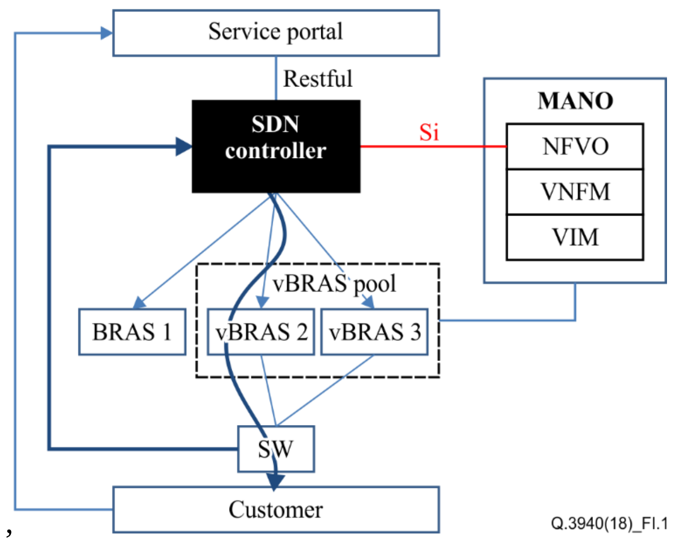

Figure I.1 – Point-to-point protocol over Ethernet requests traffic scheduling within the virtual broadband remote access service pool

The following stepwise approach illustrates the roles and responsibilities of the management and orchestration (MANO) and SDN controller entities.

1) Customer sends a network access request to the SDN controller through the service portal.
2) When the SDN controller receives the access request, it checks the resource statistics based on the customer ID and finds whether there are PPPOE-related resources available in the related BRAS or vBRAS to meet the requirement.
3) If one of the BRAS or vBRAS is available, the SDN controller sends the customer request to vBRAS1.
4) If no BRAS or vBRAS in the pool is available, the SDN controller will send the request to the NFVO.
5) NFVO interfaces with the virtualized network function management (VNFM) to configure and instantiate the vBRASs.
6) NFVO interconnects with the SDN controller to deliver the certain vBRAS parameters.
7) The SDN controller activates the vBRAS and goes to step 3).

The information transferred from the SDN controller to NFVO is:

– the required bandwidth;
– the required number of PPPoE session;
– the required number of Internet protocol (IP) address.

The information delivered from NFVO to the SDN controller when received the request includes:

– the available PPPoE sessions in specific vBRAS;
– the available public IP address and related ports scope in the specific vBRAS;
– the available bandwidth of each virtual interface and the remaining quality of service (QoS) queue in the specific vBRAS;
– the information of the instantiated vBRASs, e.g., vBRAS addresses or names.

BRAS/vBRAS are responsible for the control and management of customer access to the Internet. With increases in customer terminal numbers and traffic on the network, the carrier network is designed to have higher service capability.

I.2 Scenario 2: Dynamic bandwidth adjustment

This service is traditionally supported by a platform that has several shortcomings for service provision. The problem happens on change of authorizatio (CoA), the interface between platform and BRAS. It is only capable of carrying service name and leaves no room for more service parameters. In this case, service parameters need to be pre-configured in every BRAS in management (MAN). If the service has any change, the related service parameters have to be rewritten for every BRAS and create a lot of work for network administrators.

The SDN-based CO can utilize a programmable interface to convey flexible service parameters for customers in real time. Figure I.2 illustrates the detailed scenario.

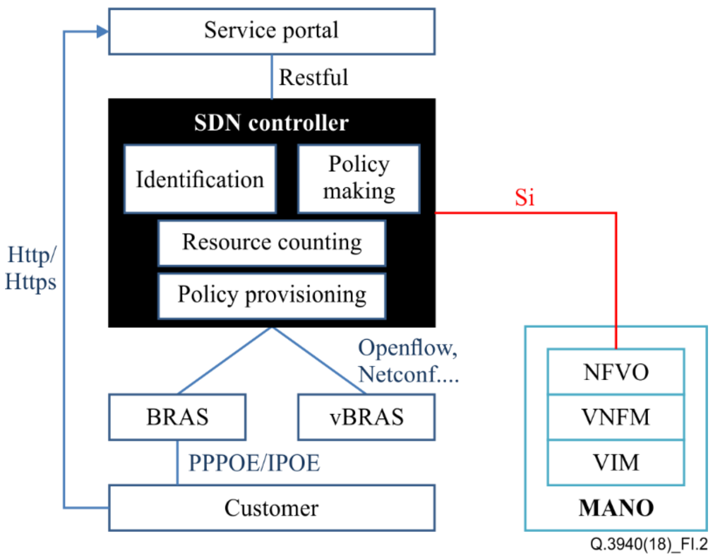

Figure I.2 – Dynamic bandwidth adjustment service scenario

The following stepwise approach illustrates the roles and responsibilities of the MANO and SDN controller entities.

a) Customer requests bandwidth adjustment service via a web portal. This request carries the bandwidth and timeframe parameters.

b) When the SDN controller receives the request, it checks the resource statistics based on the customer ID and finds whether there are available bandwidth resources in the BRAS or vBRAS for the customer to access the Internet to meet the requirement.

   i) If there is bandwidth available in this BRAS or vBRAS, the SDN controller reallocates the bandwidth to the specific customer ID.

   ii) If not, the SDN controller sends the request to the NFVO to allocate more bandwidth resources.

c) NFVO sends the parameter of the newly assigned bandwidth to the SDN controller.

The information transferred from the SDN controller to NFVO is:

– bandwidth;
– timeframe;
– customer ID;
– interface ID.

The information delivered from NFVO to SDN controller includes the following.

The bandwidth resources according to specific timeframe, customer ID and interface ID.

With the development of 4K (high-definition TV), augmented reality (AR) and virtual reality (VR) services, the bandwidth demand of users is increasing and varies over time. Bandwidth utilization will improve by adopting a dynamic bandwidth adjustment strategy.

I.3 Scenario 3: Service chain for enterprise

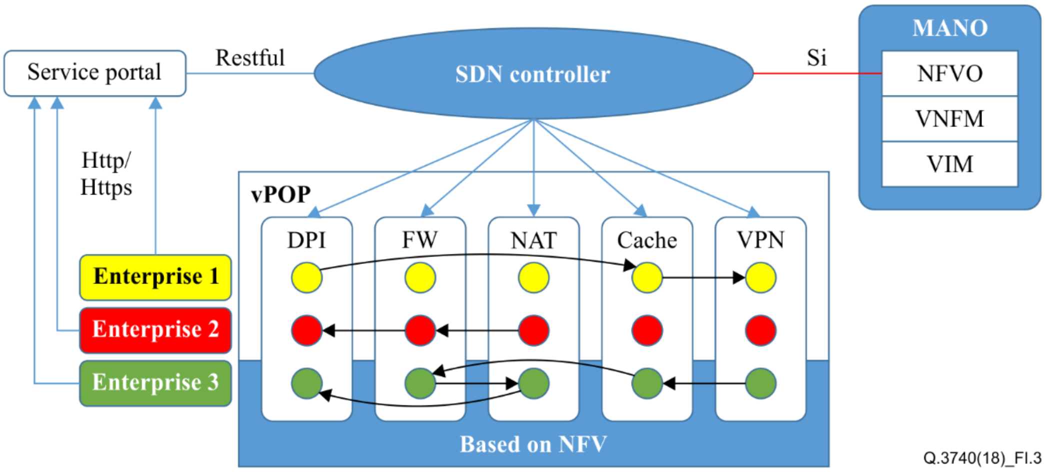

Figure I.3 – The service chain scenario for enterprises

As shown in Figure I.3, besides vBRAS, there can be several virtualized value-added service functions in the CO, e.g., deep packet inspection (DPI), network address translation (NAT), cache and firewall.

These functions serve a series of enterprise users. One function can be used by one or more enterprise users, and each enterprise user can select one or more functions according its service requirement. As shown in Figure I.3, there are three service chains, each chain serves an enterprise user and consists of a series of ordered functions.

– Enterprise 1: Pays close attention to intranet service, it needs DPI, NAT and virtual private network (VPN) functions.
– Enterprise 2: Pays close attention to Internet service, it needs DPI, firewall and NAT functions.

– Enterprise 3: All services are relevant, it needs DPI, NAT, firewall, cache and VPN functionality.

The following stepwise approach illustrates the roles and responsibilities of the MANO and SDN controller entities.

a) The enterprise customer requests service chaining service via a web portal.

b) This request triggers the SDN controller to make a list of all resources needed to deliver the service. The SDN controller also determines whether the request will be accepted, based on the real-time resource statistic [e.g. topologies and inventory of VNFs and physical network functions (PNFs)].

c) When the SDN controller receives the request, it checks the resource statistics based on the customer ID and finds whether there are available function resources (VNFs or PNFs) to meet the requirement.

    i) If there are function resources available in the CO, the SDN controller orchestrates and activates them to the specific customer ID.

    ii) If not, there are two kinds of situation.

        1) Within those functions, some of them are PNFs and others are VNFs. The SDN controller takes charge of orchestration and service functions allocation among PNFs and VNFs. It also activates and connects the VNFs instance by MANO.

        2) All the functions are VNFs, NFVO takes charge of orchestration. The SDN controller plays the role of activating the VNFs and connecting them.

The information transferred from the SDN controller to NFVO is:

– service chain ID;

– required VNFs and their related virtualized resources.

The information delivered from NFVO to SDN controller includes:

– service chain ID;

– forwarding graph;

– VNF information: CPU, storage, and session capacity;

– information about the instantiated VNFs, e.g. VNF address.

By deploying vCPE and value-added services in the CO, customers can select the services needed in the service chain to improve service allocation capability for their enterprises.

Bibliography

[b-ITU-T G.998.1] Recommendation ITU-T G.998.1 (2005), *ATM-based multi-pair bonding.*

[b-ITU-T Y.3321] Recommendation ITU-T Y.3321 (2015), *Requirements and capability framework for NICE implementation making use of software-defined networking technologies*.

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

[b-ETSI GS NFV-MAN 001] ETSI GS NFV-MAN 001 V1.1.1 (2014), *Network functions virtualisation (NFV); Management and orchestration.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018