International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 41

(07/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Deployment models of service function chaining

ITU-T Y-series Recommendations – Supplement 41

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Supplement 41 to ITU-T Y-series Recommendations

Deployment models of service function chaining

Summary

Supplement 41 to the ITU-T Y-series Recommendations describes use cases and deployment models of service function chaining. This Supplement also specifies requirements in order to support service function chaining in IP-based fixed and mobile networks.

Service function chaining determines the requisite service functions (SFs), based on context information and selects a proper service function chain that consists of the requisite SFs providing specific treatment of packets. Therefore, service provisioning can be rapid and flexible with high manageability.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y Suppl. 41	2016-07-08	13	11.1002/1000/13021

Keywords

Service function, service function chain, service function chaining, service function path.

[*] 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 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/.

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Supplement 41 to ITU-T Y-series Recommendations

Deployment models of service function chaining

1 Scope

This Supplement explains the concept of service function chaining and presents required functionalities. It describes use cases and deployment models of service function chaining. It also specifies requirements in order to support service function chaining in IP-based fixed and mobile networks.

2 References

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.3043] Recommendation ITU-T Y.3043 (2013), *Smart ubiquitous networks - Context awareness framework.*

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

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 middlebox [b-IETF RFC 3234]: Any intermediary device performing functions other than the normal, standard functions of an IP router on the datagram path between a source host and destination host.

NOTE – Normal, standard IP routing functions (i.e., the route discovery and selection functions described in, and their equivalent for IPv6) are not considered to be network processing functions; a standard IP router is essentially transparent to IP packets.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 service function: A function, specifically representing network service function, that is responsible for specific treatment of received packets other than the normal, standard functions of an IP router (e.g., IP forwarding and routing functions) on the network path between a source host and destination host.

NOTE – The examples of service function are similar to, but not limited to that of a middlebox.

3.2.2 service function chain: A chain that defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification and/or policy.

3.2.3 service function chaining: A mechanism of building service function chains and forwarding packets/frames/flows through them.

3.2.4 service function path: A path that defines an ordered set of specific instantiations of service functions that packets and/or frames and/or flows must visit within a specific service function chain.

NOTE – A service function path is determined among the relevant service function paths within a specific service function chain, satisfying capacity and QoS requirements of service functions and their connecting links. There is typically a 1:n relationship between a service function chain and a service function path.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

3G	3rd Generation
4G	4th Generation
DPI	Deep Packet Inspection
FW	Firewall
HSS	Home Subscriber System
HTTP	Hypertext Transport Protocol
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IPS	Intrusion Prevention System
IPTV	Internet Protocol Television
L2	Layer 2
L3	Layer 3
LTE	Long Term Evolution
NAT	Network Address Translation
NF	Network Function
OSI	Open System Interconnection
PCRF	Policy Control and Repository Function
QoE	Quality of Experience
QoS	Quality of Service
RAT	Radio Access Technology
SF	Service Function
SFC	Service Function Chain
SFI	Service Function Instance
SFP	Service Function Path
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SNS	Social Networking Service
TCP	Transport Control Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VO	Video Optimizer
VoIP	Voice over Internet Protocol

VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network

5 Conventions

NOTE – This Supplement contains material that is supplementary to the ITU-T Y-series of Recommendations. As such, this Supplement is not required for the implementation of service function chaining.

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 prohibited from" 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 Supplement need not be present to claim conformance.

The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this Supplement can still be claimed even if this requirement is present.

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 Overview of service function chaining

This clause describes overview of service function chaining in terms of service functions and use cases.

6.1 Service functions

This clause introduces a various kind of service functions (SFs) and their roles, which is considered as an extension of middleboxes [b-IETF RFC 3234]. Until now, many kinds of middleboxes have been deployed in IP-based fixed and mobile networks in order to enhance the capabilities of the network. The middlebox performs numerous network processing functions, each providing a specific treatment of received packets. They range from security (e.g., firewall, intrusion detection system, traffic scrubber), traffic shaping (e.g., rate limiter, load balancer), dealing with address space exhaustion (e.g., network address translation) or improving the performance of network applications (e.g., traffic accelerator, cache, proxy). With the middlebox, the capability of a network can be quite enhanced in providing network services. The network services include examples such as voice/data, Internet access and a virtual private network [b-ETSI GS NFV 002].

However, most of these network services are implemented in costly, hard-to-modify, dedicated hardware, thus resulting in difficulty to rapidly deploy and easily adapt to new requirements. A service function is newly devised and extended from the middlebox with the help of virtualisation technology and can be realized in a virtual entity as well as a physical entity. Similarly to a middlebox, a service function performs a specific treatment of received packets at various layers of a protocol stack. The specific treatment of packet represents transformation, inspection and filtering.

The examples of service functions include, but are not limited to the following:

- Network address translation (NAT) replaces the source and/or destination IP addresses of packets that traverse the NAT service function. Typically, NAT is deployed to allow multiple end hosts to share a single IP address: hosts "behind" the NAT are assigned a private IP address, and their packets destined to the public Internet traverse NAT which replaces their internal, private address, with a shared public address.

- IP tunnel endpoints, including virtual private network endpoints, uses basic IP services to set up tunnels with their peer tunnel endpoints which might be anywhere in the Internet.
- Packet classifiers classify packets flowing through them according to policy and either select them for special treatment or mark them, in particular for differentiated services.
- TCP proxies modify the timing or action of the TCP protocol in flight for the purposes of enhancing performance.
- Load balancers provide one point of entry to a service, but forward traffic flows to one or more hosts that actually provide the service.
- Firewall (FW) functions filter traffic based on a set of predefined security rules defined by a network administrator. IP firewalls reject packets based purely on fields in the IP and Transport headers.
- Transcoders perform some type of on-the-fly conversion of application level data. Examples include the transcoding of existing web pages for display on hand-held wireless devices, and transcoding between various audio formats for interconnecting digital mobile phones with voice-over-IP services.

A service function chain (SFC) is intentionally devised to efficiently chain the requisite service functions in order of their execution. An SFC is, however, quite static and often tightly coupled to network topology and physical resources. It therefore makes it difficult for operators to introduce new or modify existing network services and/or service functions. Moreover, once an SFC is selected, it is not likely to be changeable to steer packets through that new service. Their shortcomings make it highly complicated to modify their configurations as well as to achieve automation.

6.2 Service function chaining

Service function chaining is intended to address the limitations of traditional SFs. This clause specifies the service function chaining that provides a mechanism to dynamically build SFCs and then make incoming packets forward through the SFC. With these dynamics, the SFC can rapidly and easily be generated and modified according to the service features carrying in packets. The concept of service function chaining is introduced in Figure 1. In this figure it is assumed that IP packets carrying both web and Internet protocol television (IPTV) service traffic separately traverse through corresponding SFCs. Each SFC consists of three SFs (e.g., FW, NAT, video optimizer (VO)) in order of their execution. All packets should be routed through all SFs regardless of their traffic characteristics before applying dynamic service function chaining, as shown with the solid line in Figure 1. In case packets carrying web traffic traverse their SFC, VO is definitely not necessary. In this respect, SFCs should be dynamically generated and selected, considering whether each packet should visit a specific SF or not. By applying dynamic service function chaining, packets carrying web traffic can traverse through a new SFC and thus bypass a VO as shown with the dotted line in Figure 1. The SFC therefore enables packets to be dynamically steered, considering on operator's policy and user preference.

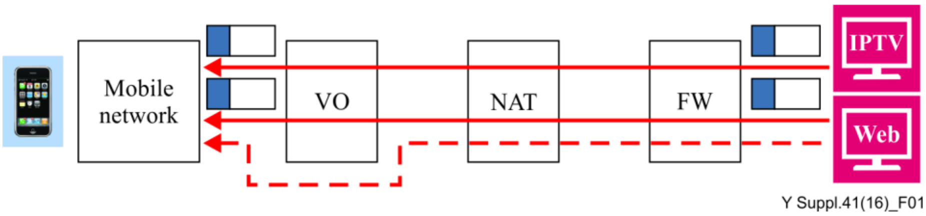

Figure 1 – The concept of service function chaining

The SFC can be provided by the combination of functions in data, control and management plane as shown in Figure 2. The scope of this supplement is limited to data plane and the roles of other planes are out of scope in this supplement.

- The data plane consists of classifiers and service functions. A classifier identifies and classifies traffic before forwarding it into the service function path. The path between classifiers and service functions is set up and managed by the control plane.
- The control plane includes policy controller, service function chain controller, service function path controller and user profile. First, the service function chain controller generates or selects a specific service function chain using a result of analysing incoming packets at the ingress classifier. The user profile stores user preference and subscription information. Therefore, an appropriate service function chain is allocated with referring to both. The service function path controller determines one among the relevant service function paths within the service function chain, satisfying capacity and QoS requirement of service functions and their connecting links and locating service functions in the network. Last, the policy controller is used to maintain SFC policy tables that represent forwarding paths. Software-defined networking is a candidate technology in control plane [ITU-T Y.3300].
- The management plane consists of service function chain manager, service function path manager and service function manager. They respectively manage the instantiation, maintenance and termination of service function.

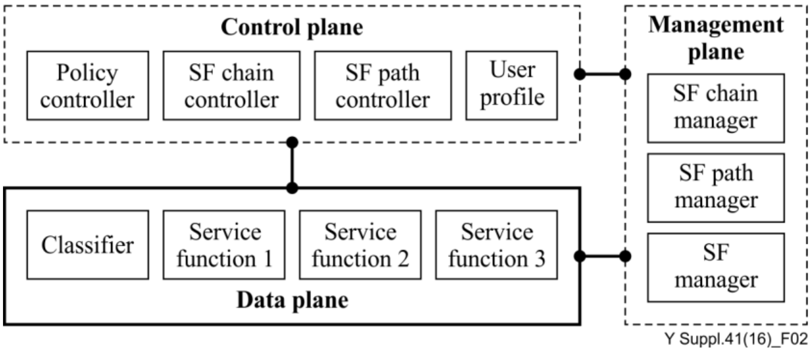

Figure 2 – The scope of this Supplement; data plane of service function chaining

6.3 Use cases

This clause describes three types of context information and use cases. These use cases can generally be categorized into three types, depending on context information [ITU-T Y.3043]; context information is independently retrieved from a result of packet inspections, network status and user subscriptions, but it is not limited to only this information. Moreover, many different use cases can be generated according to operator's policy and user preference, as well as in combination with the context information.

Below are examples of context information relating to packet inspections:

- Application type: session initiation protocol (SIP), simple mail transport protocol (SMTP), social networking service (SNS), voice over IP (VoIP), hypertext transport protocol (HTTP), etc.;
- Metadata: uniform resource locator (URL), file name, browser type, codec, international mobile subscriber identity (IMSI), etc.

The following show context information relating to user subscriptions:

- Value added service: Parent control, video optimization, anti-virus, etc.;
- Device type: smart phone, tablet, etc.

An example of the network status is:

- Radio access technology (RAT) type: 3G, 4G LTE, WiFi, etc.

A classifier identifies application type and metadata by inspecting the header and payload of an incoming packet. Based on the result of the packet inspection, the classifier basically selects the requisite service functions and determines a specific service function chain which includes all of these requisite service functions. Moreover, the classifier chooses more and different service functions, in conjunction with earlier chosen ones, by considering other information such as RAT type and user subscriptions. The user subscription may be retrieved from policy control and repository function (PCRF) or home subscriber system (HSS) [ITU-T Y.2012] in a mobile network environment. Overall, the selection of service functions depends on the network environments and their implementation.

As an example, it is assumed that a tablet is consuming a video streaming service within a 3G mobile network. The video optimizer would then apply an appropriate transcoding/translating scheme to the video stream in order to keep a certain quality of experience (QoE). In this use case, an SFC would be selected or generated to include the requisite service functions (e.g., video optimizer) by considering information retrieved from packet inspection, user subscriptions and network status. If the table now leaves the 3G network and moves to a 4G LTE network, the network has sufficient bandwidth and its conditions will be better such that a new SFC is selected as not to include video optimizer and packet can bypass the video optimizer through the SFC. In addition, when the user is willing to use a smart phone instead of the tablet, streams with different resolution will be more appropriate to the smart phone with its small screen in order to reduce network bandwidth consumption. The video optimizer therefore has to use another transcoding scheme and a new SFC will be allocated to the different use case. Furthermore, many different use cases can be generated with any combination of context information and involvement of relevant service functions such as intrusion prevention system (IPS), VO, transmission control protocol (TCP) proxy, HTTP proxy, uniform resource locator (URL) filter, etc.

7 Deployment models of service function chaining

This clause describes the deployment models of service function chaining in terms of service function chain and service function path.

The deployment model of SFC can be classified in consideration of both the roles and the capabilities of the involved SFs. An SFC enables the creation of composite network services by constructing an ordered set of service functions. In addition, an SFC can be fine-grained or coarse-grained, depending on the capabilities of the classification function in the ingress classifier. The classifier has the responsibility to identify and then classify packets in order to steer them through the proper SFC. The classification function can be deployed in either a single classifier or multiple service functions that include a classifier. Therefore, deployment models can be centralized or distributed within each SFC.

The deployment models of the SFC represent the capability and the deployment of classification function. In this regards, the model has three types; linear, recursive and branching models.

- Linear model is illustrated in Figure 3, where a classifier selects or generates either a coarse-grained SFC or a fine-grained SFC, depending on the capabilities of classification function. As shown in Figure 3, incoming packets should visit all SFs regardless of their executions when SFC 1 is selected by a classifier having limited capability. On the other hand, an ingress classifier with deep packet inspection capabilities can recognize that incoming packets do not contain any video traffic and select SFC 2 which does not include the video optimizer, namely SF 2, and thus, the video optimizer will not be executed.
- The recursive and branching models depend on the deployment of classification function (e.g., centralized or distributed) as shown in Figure 4 and Figure 5 respectively. For example, SFC 1 in Figure 4 is selected as a result of classification. Incoming packets visit SF 1 (e.g., intrusion detection system), which then detects malware in the packets. SF 1 then just decides

to stop following executions in SFC 1 because an anti-virus function does not exist in SFC 1. SF 1 cannot select a new SFC when it does not have the classification function. SF 1 only just steer the packets for the classifier to select other SFCs (e.g., SFC 2) when it itself cannot select a new SFC. On the other hand, Figure 5 shows a classification function existing in SF 1 as well. In this case, SF 1 selects a new SFC (e.g., SFC 2) and forward the packets through SFC 2.

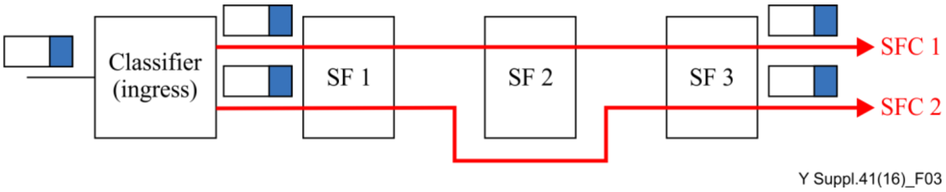

Figure 3 – Linear model of SFC

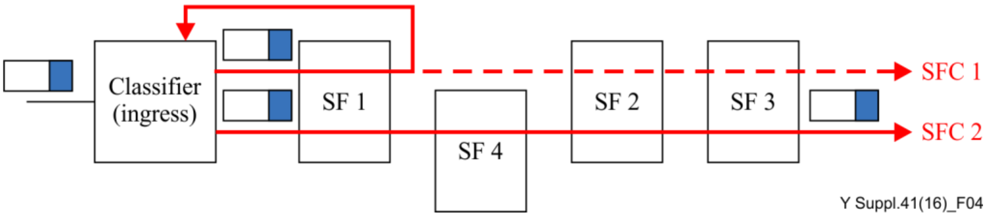

Figure 4 – Recursive model of SFC

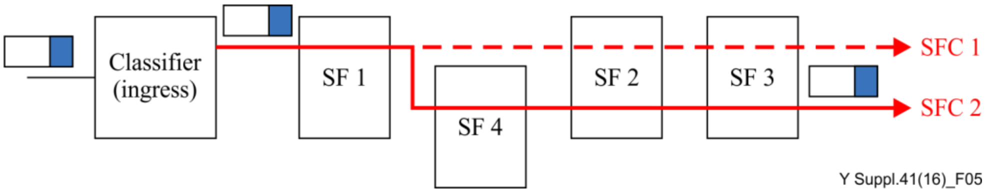

Figure 5 – Branching model of SFC

The service function path (SFP) is an ordered list of service function instances (SFIs) within a specific SFC; it represents an ordered list of abstracted SFs. An SFP is determined among the multiple relevant SFPs, satisfying the capacity availability and QoS requirement of service functions and their connecting links. There is therefore, typically a 1:n relationship between the SFC and SFP. The relationship between them is shown in Figure 6. This SFC example includes three service functions in abstracted level, such as VO-FW-NAT between ingress and egress classifier. The SFP definitively indicates the three service function instances that a packet must traverse. The SFP, for example VO_3-FW_2-NAT_1, would thus be determined among many service functions instances within the SFC.

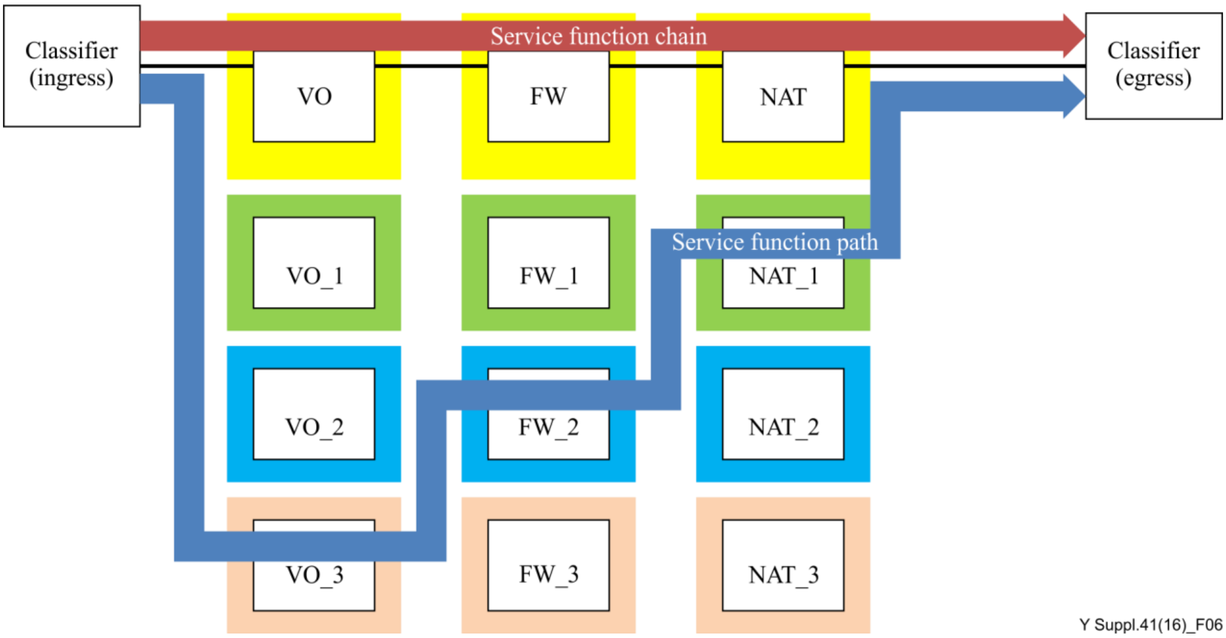

Figure 6 – Relationship between service function chain and service function path

The deployment model of SFP consists of a classifier, switch router and service functions as shown in Figures 7 and 8. The arrows in the figures represent the forwarding direction of packets in unidirection. The classifier on the left-hand side indicates an ingress node and the right-hand side indicates an egress node. The egress node is involved in the reverse direction of packets, thus it is ignored in the forwarding direction.

The deployment model of SFP can be classified into two: indirect and direct.

– Indirect model: A switch router has the packet forwarding information and table in order to provide the end-to-end path. In Figure 7, the table specifically includes segmented path information that is used for steering incoming packets into outgoing ports. There are three types of segmented paths including an ingress classifier and SFI 1, SFI 1 and SFI 2, and SFI 2 and an egress classifier (e.g., an outer network), respectively. This model can be deployed in network independently even though it may lead to increases in configuration complexity and modification difficulty. The candidate transport techniques for this indirect model will be VLAN, VXLAN, etc.

– Direct model: A switch router needs to provide end-to-end paths that packets traverse from an ingress to an egress classifier via SFI 1 and SFI 2. In Figure 8, the packet can carry end-to-end path information and thus the packet forwarding information and table are not necessary in switch router. It can alleviate the complexity and the difficulty of providing SFPs when SFIs are rapidly added or removed. Before forwarding packets, this model should consider the maximum size of packets carrying end-to-end path information. The candidate transport techniques for direct model will be IP source routing, etc.

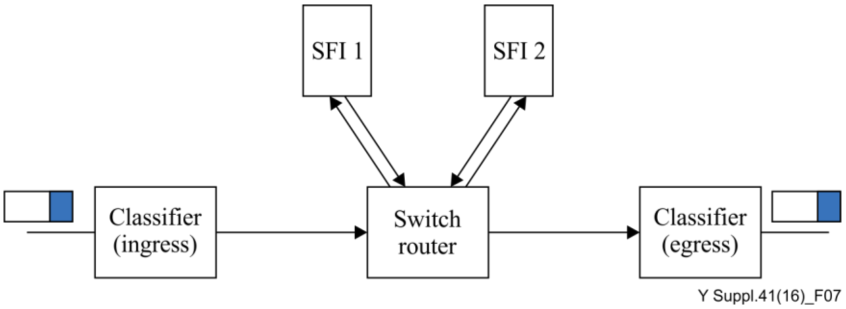

Figure 7 – Indirect model of SFP

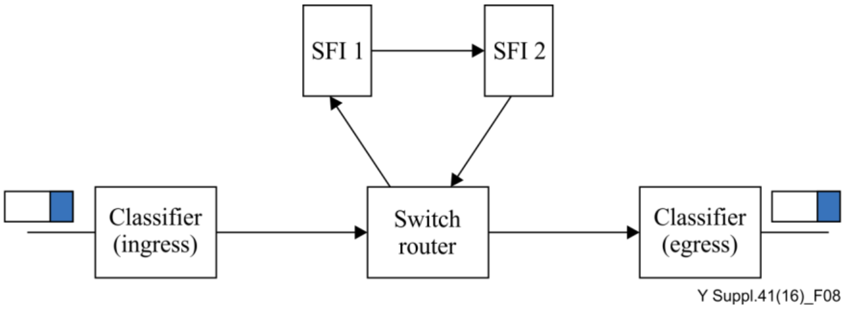

Figure 8 – Direct model of SFP

8 Requirements

NOTE 1 – This Supplement contains material that is supplementary to the ITU-T Y-series of Recommendations. As such, this Supplement is not required for the implementation of service function chaining.

Service functions in an SFC are required to represent either a physical entity or virtual entity, or a combination of them.

Service function instances in an SFP are required to be realized as either a physical entity or virtual entity, or as combination of them.

A service function chain is required to be independent of network topology.

A classifier is required to determine a specific service function chain with consideration of context information (e.g., packet inspection, user subscription and network status information).

A classifier is required to determine a specific SFP with considering the capacity and available resource of both SF instances and the links connecting them within the SFC.

A service function chain is required to represent a set of SFs in order of their execution.

A service function path is required to represent a set of SF instances in order of their execution within the SFC.

A service function path is recommended to support either direct model or indirect model in forwarding packets.

Service function chaining is required to support classifier to steer packets depending on operator's policy and network policy as well as available resource of SFs.

Service function chaining is recommended to support for classification function to determine new SFC and redirect packets through it after the first SFC is not valid.

Service function chaining is recommended to support automatic configuration and customization capabilities.

NOTE 2 – With support of automatic configuration and customization capabilities, deployment times and operational complexity can be decreased.

9 Security considerations

This Supplement is recognized as an enhancement of IP-based networks. Thus, it is assumed that security considerations in general, are based on the security of IP-based networks, especially as required to follow the security considerations identified by clauses 7 and 8 of [ITU-T Y.2701].

Appendix I

Standardization activities of service function chaining

As topology changes are frequently occurring and new service functions are more emerging, configuration of service function deployment will be complicated. In that sense, service function chaining is devised from some standardization bodies (e.g., Internet Engineering Task Force (IETF), Broadband Forum (BBF), 3rd Generation Partnership Project (3GPP)).

The European Telecommunications Standards Institute Industry Specification Group for Network Function Virtualization (ETSI ISG NFV) first introduced the concept of service function chain in the name of network function forwarding graph in [b-ETSI GS NFV 001], [b-ETSI GS NFV 002] and [b-ETSI GS NFV 003]. First, network service is introduced as a fundamental concept explaining service function chaining and is defined by a composition of network functions. A network function (NF) is the functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behaviour. A network function forwarding graph defines a graph of logical links connecting NF nodes for the purpose of describing traffic flow between these NFs and is almost same to an SFC. A simple network service can be implemented in an NFV environment using point to point links but a network function forwarding graph would be necessary to support a composite service with more complex structures. Second, the network forwarding path has very similar concept to the SFP and is defined as an ordered list of connection points forming a chain of NFs, along with policies associated to the list.

IETF service function chaining working group (SFC WG) also defined the service function chain as an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification [b-IETF RFC 7665]. In addition, SFP is introduced as a constrained specification of where packets assigned to a certain service function path must go. A service function path may be so constrained as to identify the exact locations of each network function instance.

The objective of [b-3GPP TR 22.808] is to study use cases and propose potential requirements for supporting traffic classification and service chain selection capabilities per operator's policy (e.g., based on user's profile, application type, RAN type, RAN status and flow direction) in order to realize efficient and flexible mobile service steering in the (S)Gi-LAN network. The term *flexible mobile service steering* is used to represent service function path instead.

Bibliography

[b-3GPP TR 22.808] 3GPP TR 22.808 (2015), *Study on Flexible Mobile Service Steering (FMSS).*

[b-ETSI GS NFV 001] ETSI GS NFV 001 (2013), *Network Functions Virtualisation (NFV); Use Cases*.

[b-ETSI GS NFV 002] ETSI GS NFV 002 (2014), *Network Functions Virtualisation (NFV); Architectural Framework.*

[b-ETSI GS NFV 003] ETSI GS NFV 003 (2014), *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV.*

[b-IETF RFC 3234] IETF RFC 3234 (2002), *Middleboxes: Taxonomy and Issues*.

[b-IETF RFC 7665] IETF RFC 7665 (2015), *Service Function Chaining (SFC) Architecture*.

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, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016