International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.4043

(07/2019)

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

Testing specifications – Testing specifications for Cloud computing

Interoperability testing requirements of a virtual switch

Recommendation ITU-T Q.4043

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
TESTING SPECIFICATIONS	Q.3900–Q.4099
Testing specifications for next generation networks	Q.3900–Q.3999
Testing specifications for SIP-IMS	Q.4000–Q.4039
Testing specifications for Cloud computing	**Q.4040–Q.4059**
Testing specifications for IMT-2020 and IoT	Q.4060–Q.4099
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

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

Recommendation ITU-T Q.4043

Interoperability testing requirements of a virtual switch

Summary

Recommendation ITU-T Q.4043 specifies virtual switch (vswitch) interoperability testing requirements. This Recommendation introduces an overview of a vswitch and vswitch interoperability testing . This includes, but is not limited to, the definition, characteristics and general capabilities of vswitches, as well as an overview of interoperability testing of vswitches. The description of cloud-related use cases of vswitches, given in the appendix, describes the related interaction processes. Based on an analysis of involved vswitch capabilities in cloud-related use cases, the corresponding derived requirements of a vswitch's interoperability testing are introduced.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.4043	2019-07-29	11	11.1002/1000/13979

Keywords

Interoperability, requirements, testing, virtual switch.

* 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
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	1
4	Abbreviations and acronyms	1
5	Conventions	3
6	Concept of a virtual switch	3
7	Overview of virtual switch interoperability testing	4
8	IOPT requirements of a virtual switch	5
	8.1 IOPT requirements between a virtual switch and a VM	5
	8.2 IOPT requirements between a virtual switch and other network equipment	7
	8.3 IOPT requirements for control plane coordination aspect	8
	8.4 IOPT requirements between a virtual switch and computing virtualization	8
Appendix I – Typical use cases of a virtual switch		9
	I.1 Virtual switch use cases on network connectivity	9
	I.2 Virtual switch use cases on network security	11
	I.3 Virtual switch use cases on QoS	12
	I.4 Virtual switch use cases on tunnelling	13
	I.5 Virtual switch use cases on control plane coordination	14
	I.6 Virtual switch use cases on reference points	15
	I.7 Virtual switch use cases on computing virtualization compatibility	16
Bibliography		17

Recommendation ITU-T Q.4043

Interoperability testing requirements of a virtual switch

1 Scope

This Recommendation covers the following:

– conceptual overview of a virtual switch;

– overview of interoperability testing of a virtual switch;

– interoperability testing requirements of a virtual switch.

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*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud interoperability [b-ITU-T Q.4040]: The capability to interact between CSCs and CSPs or between different CPSs, including the ability of CSCs to interact with cloud services and exchange information, the ability for one cloud service to work with other cloud services, and the ability for CSCs to interact with the cloud service management facilities of the CSPs.

3.1.2 cloud interoperability testing [b-ITU-T Q.4040]: Verifying functions and interaction that realize the cloud interoperability.

3.1.3 interoperability [b-ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 virtual switch: Resource abstraction and control function abstracting physical network resources to offer virtual network capabilities.

3.2.2 virtual switch user: Entity (e.g., a person or a program) that uses or operates a virtual switch.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ARP Address Resolution Protocol

AS Autonomous System

BGP	Border Gateway Protocol
DDOS	Distributed Denial of Service
DOS	Denial of Service
EGP	Exterior Gateway Protocol
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
ID	Identifier
IGP	Interior Gateway Protocol
IOPT	Interoperability Testing
IP	Internet Protocol
IS-IS	Intermediate System-to-Intermediate System
L2	Layer 2
LAN	Local Area Network
MAC	Media Access Control
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NFV	Network Function Virtualization
NIC	Network Interface Card
NSH	Network Service Header
NVGRE	Network Virtualization using Generic Routing Encapsulation
OSPF	Open Shortest Path First
OVSDB	OpenvSwitch Database
QoS	Quality of Service
RIP	Routing Information Protocol
SDN	Software Defined Network
SF	Service Function
SFC	Service Function Chaining
SFF	Service Function Forwarder
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
STT	Stateless Transport Tunneling
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function

VS Virtual switch

VSU Virtual switch user

VXLAN Virtual Extensible LAN

5 Conventions

In this Recommendation:

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

6 Concept of a virtual switch

A virtual switch, which belongs to the resource abstraction and control function, abstracts physical network resources to enable a cloud service provider to offer virtual network capabilities for a virtual machine (VM) with capabilities of rapid elasticity, resource pooling and on-demand self-service. A virtual switch is a software implementation, which can be deployed as a part of hypervisor or as a VM. As shown in Figure 6-1, a virtual switch provides network access to the VM through the VM's virtual network interface cards (NICs), as well as network access to physical hosts though the physical NIC which is used as the uplink port of the virtual switch.

NOTE 1 – A virtual switch only refers to the virtual switch used to provide connectivity for VMs in virtualized environments. Some variant implementations of a virtual switch can be used in other technical areas, such as containers, and are beyond the scope of this Recommendation.

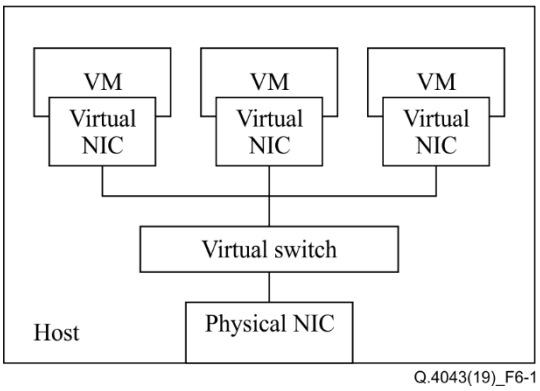


Figure 6-1 – Overview of a virtual switch

Compared to physical switches, virtual switches have the following key characteristics:

– need to provide the compatibility for computing virtualization platforms;

– can be deployed without changing the hardware environment;

– convenient to deploy new functions through software upgrades.

Virtual switches mainly implement layer 2 (L2) network switching to meet the L2 connectivity requirements between VMs, including L2 network connectivity with VMs on the same host, and L2 network connectivity between VMs on different hosts. Virtual switches also provide additional functions for connectivity between VMs, such as virtual local area networks (LANs), traffic filtering, etc.

Virtual switches are basic components of the resource layer in high-level architecture of software defined networks (SDNs) defined in [ITU-T Y.3300]. Through a tunnelling function, a virtual switch

creates virtual networks decoupled from physical network. A virtual switch provides L2 network switching and layer 3 (L3) Internet protocol (IP) routing for VMs, while providing capabilities related to network isolation, quality of service (QoS) and network operation and maintenance. The virtual switch could run on mainstream server virtualization platforms. Virtual switches are basic components of an infrastructure network domain in a high-level network function virtualization (NFV) framework defined in [b-ETSI NFV-INF 003]. It provides basic network forwarding functions and advanced network functions for a VNF such as service function chain (SFC) support.

NOTE 2 – SFC, defined in [b-IETF RFC 7498], is one of the key functions of a virtual switch for NFV. In SFC networks, virtual switches can serve as classifiers and as a service function forwarder (SFF) or SFF proxy nodes, which can forward or terminate network service header (NSH) [b-IETF RFC 8300] messages for service function (SF) and provide end-to-end NSH forwarding capabilities. [b-IETF RFC 7665].

7 Overview of virtual switch interoperability testing

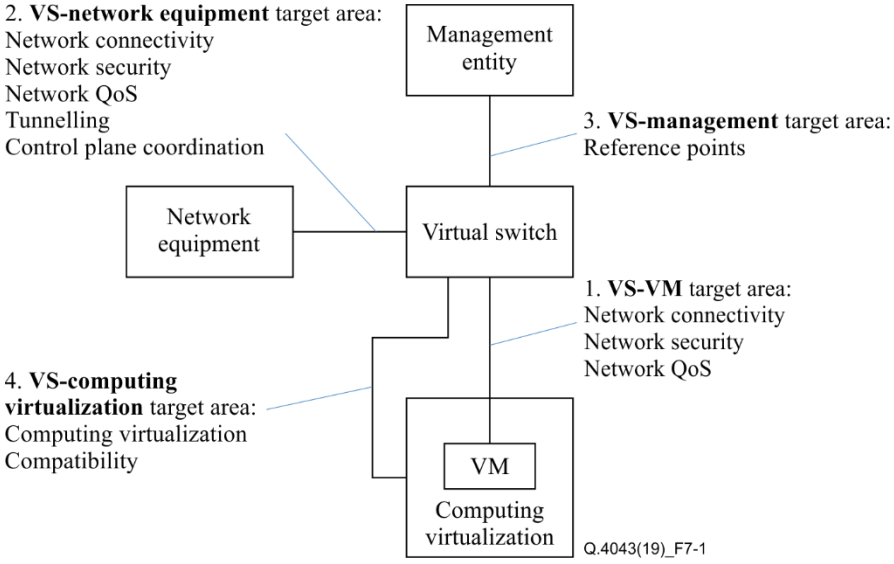


Figure 7-1 – Target areas of virtual switch interoperability

Interoperability testing of a virtual switch is to verify that the virtual switch can interact with other entities as expected. As shown in Figure 7-1, according to the way a virtual switch works, there are four different target areas that need to be considered in interoperability testing (IOPT) of virtual switch as follows:

– Target area 1: "**virtual switch – VM**", dealing with interaction between virtual switch and VM;

– Target area 2: "**virtual switch – network equipment**", dealing with interaction between virtual switch and other network equipment;

– Target area 3: "**virtual switch – management entity**", dealing with interaction between virtual switch and management entity;

– Target area 4: "**virtual switch – computing virtualization**", dealing with interaction between virtual switch and computing virtualization.

As shown in Figure 7-1, for each target area, the IOPT should verify that the virtual switch provides specific relevant capabilities, which can be classified into the following categories:

– **network connectivity**: The capabilities to provide access for VMs at multiple levels of the network including link layer, network layer and transport layer. Verification of network connectivity capabilities should be considered in target area 1 and 2;

– **network security**: Multi-level network security protection through the detection and processing of packet header information of each layer network to prevent spoofed traffic,

dangerous traffic, distributed denial of service (DDOS) attacks and other threats. Verification of network security capability should be considered in target area 1 and 2;

– **network QoS**: Control and manage capabilities of network resources by traffic classification, rate limiting, bandwidth grantee. Verification of network QoS capabilities should be considered in target area 1 and 2;

– **tunnelling**: End-to-end tunnel encapsulation capabilities to enable network communication independent of the underlying layer and provide logical isolated networks. Verification of tunneling capability should be considered in target area 2;

NOTE – Tunnelling can be realized base on different protocols, such as virtual extensible local area network (VXLAN), multi-protocol label switching (MPLS) over generic routing encapsulation (GRE), stateless transport tunnelling (STT), network virtualization using generic routing encapsulation (NVGRE).

– **control plane coordination**: Cooperation with other network equipment on control plane to enable automated multi-device collaboration, such as distributed traffic processing logic, automated complex networking, etc. Additional logic centralized controllers are the usual implementation for control plane coordination. Verification of control plane coordination capability should be considered in target area 2;

– **reference points**: Conceptual points at the conjunction of virtual switch and management entities. Verification of reference points should be considered in target area 3;

– **computing virtualization compatibility**: The capability of virtual switch supporting deployment on computing virtualization and cooperation with computing virtualization. Verification of computing virtualization compatibility should be considered in target area 4.

8 IOPT requirements of a virtual switch

Clauses 8.1 to 8.4 provide the IOPT requirements for a virtual switch.

8.1 IOPT requirements between a virtual switch and a VM

Clauses 8.1.1 to 8.1.3 give the IOPT requirements between a virtual switch and a virtual machine.

8.1.1 IOPT requirements for network connectivity aspect

The IOPT requirements for the network connectivity aspect are given as follows:

– **data frame forwarding**: It is required that a virtual switch provides data frame forwarding function, which forwards data frames from virtual ports base on address information in data frames;

NOTE – For received frames with broadcast, multicast, and unknown unicast media access control (MAC) addresses, virtual switch floods the frames to each other ports in the same broadcast domain.

– **VLAN**: It is required that a virtual switch provides VLAN function in order to create partitioned and isolated broadcast domain in a computer network at the data link layer;

– **MTU**: It is recommended that virtual switch limits the maximum frame size allowed through the ports;

– **port aggregation**: It is recommended that a virtual switch logically uses multiple independent links as a single link to achieve flexible high bandwidth and link redundancy;

– **jumbo frame**: It is recommended that a virtual switch recognise and forward jumbo frames to reduce the number of packets and the overhead of frame header processing;

– **IP protocol**: It is required that a virtual switch supports the IP protocol [b-IETF RFC 791] and functions related to the IP protocol, including IP packet forwarding, IP subnetting [b-IETF RFC 950], IP broadcast [b-IETF RFC 922], and classless inter-domain routing (CIDR) [b-IETF RFC 4632];

– **transport protocol**: It is required that a virtual switch supports the transmission control protocol (TCP) protocol and the user datagram protocol (UDP) protocol;

– **ARP proxy**: It is recommended that a virtual switch provides address resolution protocol (ARP) response to VMs in order to reduce ARP broadcast packet in the broadcast domain;

– **forwarding acceleration**: It is recommended that a virtual switch supports forwarding acceleration in order to meet high forwarding performance of VNF;

– **ethernet interface**: It is recommended that a virtual switch supports Ethernet interface, including 10 Mbps Ethernet interface, 100 Mbps fast Ethernet interface, gigabit Ethernet interface, 10 G Ethernet interface, 40 G Ethernet interface and 100 G Ethernet interface;

– **Ethernet auto-negotiation**: It is recommended that a virtual switch supports a port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection;

– **STP**: It is recommended that a virtual switch implements spanning tree protocol (STP) protocols [b-IEEE Std 802.1D];

– **QinQ**: It is recommended that a virtual switch supports to encapsulate the private network VLAN tag in the public network VLAN so that the packet can be forwarded with two VLAN tags [b-IEEE 802.1q];

– **ICMP**: It is recommended that a virtual switch supports sending Internet message control protocol (ICMP) destination unreachable messages and can choose a code that is closest to the reason for unreachable [b-IETF RFC 792] [b-IETF RFC 1122];

– **IGMP**: It is recommended that a virtual switch supports the Internet group management protocol (IGMP) v2 [b-IETF RFC 3376];

– **IGP**: It is recommended that a virtual switch supports interior gateway protocol (IGP) to distribute routing information within a specific autonomous system (AS), such as open shortest path first (OSFP) [b-IETF RFC 2328], Intermediate System to Intermediate System (IS-IS) [b-IETF RFC 1142] and [b-IETF RFC 1195], and routing information protocol (RIP) [b-IETF RFC 2453];

– **EGP**: It is recommended that a virtual switch supports exterior gateway protocol (EGP) to distribute routing information between autonomous systems (ASs), such as border gateway protocol version 4 (BGP-4) [b-IETF RFC 4271];

– **static route**: It is recommended that a virtual switch supports to define static routes to specific destinations defined by network prefix;

– **routing policy**: It is recommended that a virtual switch supports routing policy with route filtering and attributes setting to control traffic forwarding;

– **NAT**: It is recommended that a virtual switch supports network address translation (NAT) by converting the internal network address (possibly a private address) to an external network address in order to complete the communication between the internal network and the external network, and ensure the independence and privacy of the internal network;

8.1.2 IOPT requirements for network security aspect

The IOPT requirements for the network security aspect are given as follows:

– **traffic filtering**: It is recommended that a virtual switch filter each port's traffic according to specific filtering rules;

NOTE 1 – The virtual switch supports various packet header information based filtering rules, including MAC address, IP address, TCP/UDP port.

– **anti-MAC spoofing**: It is recommended that a virtual switch allow only incoming and outgoing frames with specific MAC addresses. Frames with unexpected MAC addresses will be blocked;

– **security group**: It is recommended that a virtual switch supports security group which is a group of traffic filtering rules in order to simplify management;

NOTE 2 – Security group is provided as a function of virtual switch for SDN scenario in order to realize network isolation and access controlling by controller. Once the virtual port is associated with the security group, the internal and external traffic of the VM would be fileted with security group's rules. The security group can distinguish the traffic according to protocol, port and state to prevent the attack of unknown protocol and illegal traffic. Only traffic that meets the rules is allowed to be forward.

– **network security**: It is recommended that a virtual switch provides network layer-based security protection and supports network protection for IPv4, IPv6 and dual stacks, such as preventing a request for an IP from the source, limiting the number of concurrent requests generated by each source IP address;

– **ACL**: It is recommended that a virtual switch support IPv4, IPv6 and dual stack access control lists (ACLs), based on quintuple (source/destination IP address, source/destination port, protocol type);

– **Anti-DOS/DDOS**: It is recommended that a virtual switch supports traffic restrictions and filtering for specific protocols (e.g., TCP, UDP, ICMP) to prevent denial of service (DOS)/DDOS attacks.

8.1.3 IOPT requirements for QoS aspect

The IOPT requirements for the QoS aspect are given as follows:

– **traffic classification**: It is recommended that a virtual switch can assign a QoS priority tag in the header of the frame for a specified virtual port;

– **rate limiting**: It is recommended that a virtual switch limits the uplink or downlink rate of specified virtual port and flow to specific value.

8.2 IOPT requirements between a virtual switch and other network equipment

IOPT requirements for network connectivity aspect, network security aspect and network QoS aspect are given in clauses 8.1.1, 8.1.2 and 8.1.3 respectively.

8.2.1 IOPT requirements for tunnelling aspect

– **tunnelling protocol**: It is required that a virtual switch supports a tunnel protocol in order to encapsulate frames with tunnel header, recognise and utilizes tunnel header information for forwarding, filtering and other functions;

– **bridging tunnelling-based network and VLAN network**: A virtual switch bridges specified tunnelling based network and VLAN network by maintaining the tunnelling identifier (ID) and VLAN ID mapping, and also frames encapsulating and forwarding.

8.2.2 IOPT requirements for control plane coordination aspect

– **distributed virtual switch**: It is recommended that a virtual switch supports distributed virtual switch that extends virtual switch's ports and management across multiple servers;

NOTE – A VM remain connected to the same network as it migrates among multiple hosts connecting to same distributed virtual switch.

– **distributed routing**: It is recommended that a virtual switch supports distributed routing function in order to perform L3 routing at virtual switch without another router;

– **service function chain**: It is recommended that a virtual switch supports service function chain, including service function chain related encapsulation recognition, service classification as a service chain (SC) and service function forwarding as an SFF.

8.3 IOPT requirements for control plane coordination aspect

Clause 8.3.1 provides the IOPT requirements for the reference point aspect.

8.3.1 IOPT requirements for reference point aspect

The IOPT requirements for the reference point aspect are given as follows:

– **reference points for network functions**: It is recommended that a virtual switch provides reference points for network functions, including VLAN, QoS, speed limit, anti MAC spoofing, maximum transmission unit (MTU), port aggregation, jumbo frame;

– **reference points for network operation**: It is recommended that a virtual switch provides operational reference points for network operation configuration and network operation data receiving, including port traffic monitoring, port status monitoring, port mirroring, port traffic statistics, traffic alarm, fault alarm, running log;

– **reference points' format**: It is recommended that a virtual switch's reference points are implemented according to industry specifications;

NOTE – Examples of virtual switch reference point industry specifications are OpenFlow protocol, open vswitch database management protocol (OVSDB) protocol and simple network management protocol (SNMP).

– **change configuration remotely**: It is recommended that a virtual switch provides ability to change the configuration remotely and associated authorization mechanism.

8.4 IOPT requirements between a virtual switch and computing virtualization

Clause 8.4.1 provides the IOPT requirements for the computing virtualization aspect.

8.4.1 IOPT requirements for computing virtualization compatibility aspect

The IOPT requirements for the computing virtualization aspect are given as follows:

– **deploy on server virtualization platform**: It is recommended that a virtual switch supports deployment on mainstream implementations of computing virtualization technology;

– **accessing VM's virtual port**: It is recommended that a virtual switch supports accessing of VM's virtual ports while maintaining the isolation of each port;

– **VM status awareness**: It is recommended that a virtual switch be aware of the status (start, stop, migrated, etc.) of the VM's on the computing virtualization platform so that can adjust the network configuration according to the VMs' status;

– **monitoring resource allocation**: It is recommended that a virtual switch monitor resource allocation information of computing virtualization platform.

Appendix I

Typical use cases of a virtual switch

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

This appendix identifies use cases of a virtual switch. The table below shows the template used for the description of the use cases.

Table I.1 – Template for the description of a use case

Use case	
Name	Title of use case
Abstract	Overview and features of use case
Figure	Figure to present the use case. (A UML-like diagram is suggested for clarifying relations between roles)
Pre-conditions (optional)	Pre-conditions represent the necessary conditions or use cases that should be achieved before starting the described use case. NOTE – As dependencies may exist among different use cases, pre-conditions and post-conditions are introduced to help understand the relationships among use cases.
Post-conditions (optional)	As the same for pre-condition, the post-condition describes conditions or use cases that will be carried out after the termination of a currently described use case.
Requirements	The title of requirements derived from the use case.

I.1 Virtual switch use cases on network connectivity

Table I.2 – Virtual switch use case on network connectivity

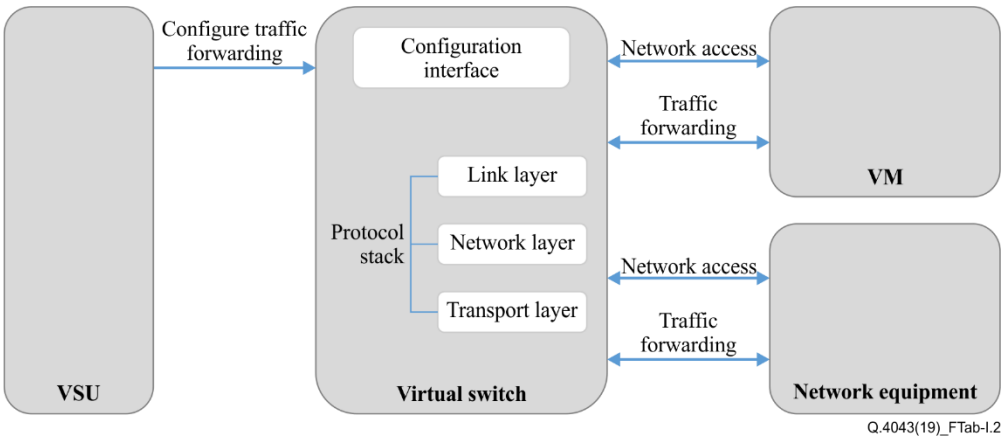
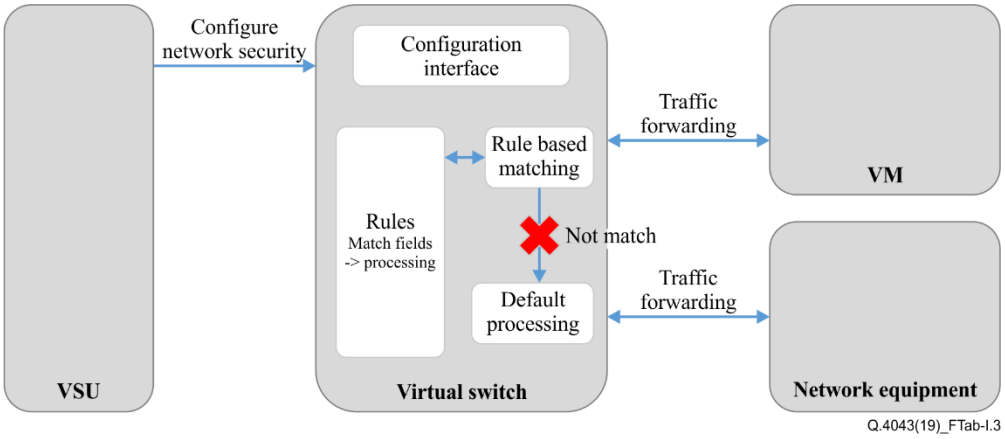
Use case	
Name	Virtual switch use case on network connectivity
Abstract	Virtual switch provides network connectivity capabilities to VM and network equipment
Figure	

Table I.2 – Virtual switch use case on network connectivity

Pre-conditions (optional)	
Post-conditions (optional)	
Description	Virtual switch user (VSU) login the configuration interface of virtual switch for configure traffic forwarding. VSU configure virtual switch to provide basic network connections for VM or network devices, including those deployed in the form of virtual machines, by configuration interface. Virtual switch can be configured to provide network connection for different layers of network connection, such as link layer (port type, MTU, STP, VLAN, QinQ, jumbo frame), network layer (ARP, IP, NAT, routing protocol) and transport layer (TCP). VM or network devices and virtual switches achieve network access through network access negotiation. Virtual switch forwards traffic between VM or network devices at different layers of network.
Requirements	– Data frame forwarding (See clause 8.1.1) – VLAN (See clause 8.1.1) – MTU (See clause 8.1.1) – Port aggregation (See clause 8.1.1) – Jumbo frame (See clause 8.1.1) – IP protocol (See clause 8.1.1) – Transport protocol (See clause 8.1.1) – ARP proxy (See clause 8.1.1) – Forwarding acceleration (See clause 8.1.1) – Ethernet interface (See clause 8.1.1) – Ethernet auto-negotiation (See clause 8.1.1) – STP (See clause 8.1.1) – QinQ (See clause 8.1.1) – ICMP (See clause 8.1.1) – IGMP (See clause 8.1.1) – IGP (See clause 8.1.1) – EGP (See clause 8.1.1) – Static route (See clause 8.1.1) – Route policy (See clause 8.1.1) – NAT (See clause 8.1.1)

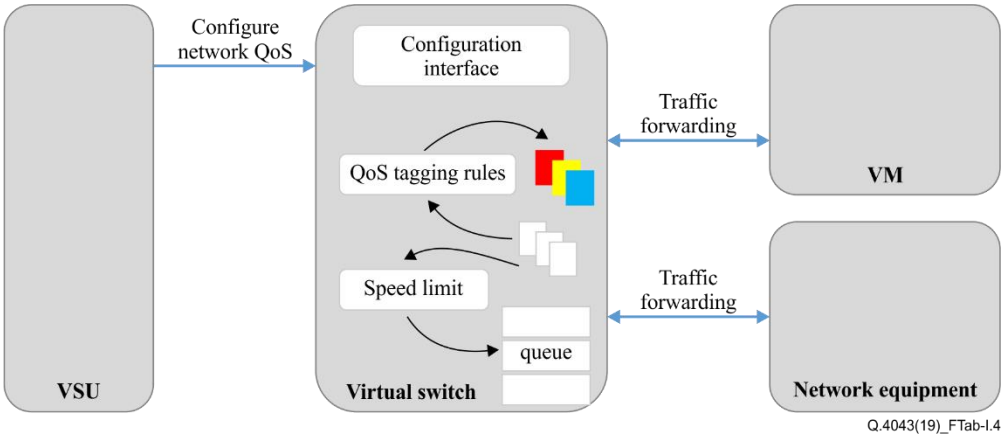
I.2 Virtual switch use cases on network security

Table I.3 – Virtual switch use case on network security

Use case	
Name	Virtual switch use case on network security
Abstract	Virtual switch provides network security capabilities to VM and network equipment
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Description	VSU login the configuration interface of virtual switch for network security. VSU configure virtual switch to provide network security capabilities for VM or network devices, including those deployed in the form of virtual machines, by configuration interface. Virtual switch can be configured to provide different security related capabilities, such as traffic filtering, anti mac spoofing, security group, network security and ACL. Virtual switch analyze incoming packets and process them accordingly according to security rules.
Requirements	– Traffic filtering (See clause 8.1.2) – Anti MAC spoofing (See clause 8.1.2) – Security group (See clause 8.1.2) – Network security (See clause 8.1.2) – ACL (See clause 8.1.2) – Anti-DOS/DDOS (See clause 8.1.2)

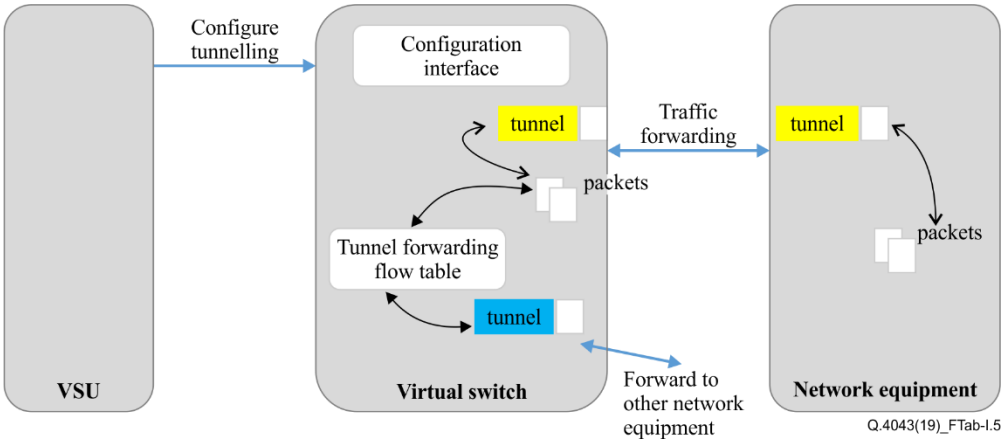
I.3 Virtual switch use cases on QoS

Table I.4 –Virtual switch use case on QoS

Use case	
Name	Virtual switch use case on QoS
Abstract	Virtual switch provides network QoS capabilities to VM and network equipment
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Description	VSU login the configuration interface of virtual switch for network QoS. VSU configure virtual switch to provide network QoS capabilities for VM or network devices, including those deployed in the form of virtual machines, by configuration interface. The virtual switch can be configured to classify the traffic of ports. Rate limiting can be configured for a specified port of the virtual switch. For traffic classification, the virtual switch assigns specified a QoS priority tag for received packets before forwarding. For rate limiting, the virtual switch limits the forwarding speed according to the configuration by putting the packets into queues with different priorities.
Requirements	– Traffic classification (See clause 8.1.3) – Rate limiting (See clause 8.1.3)

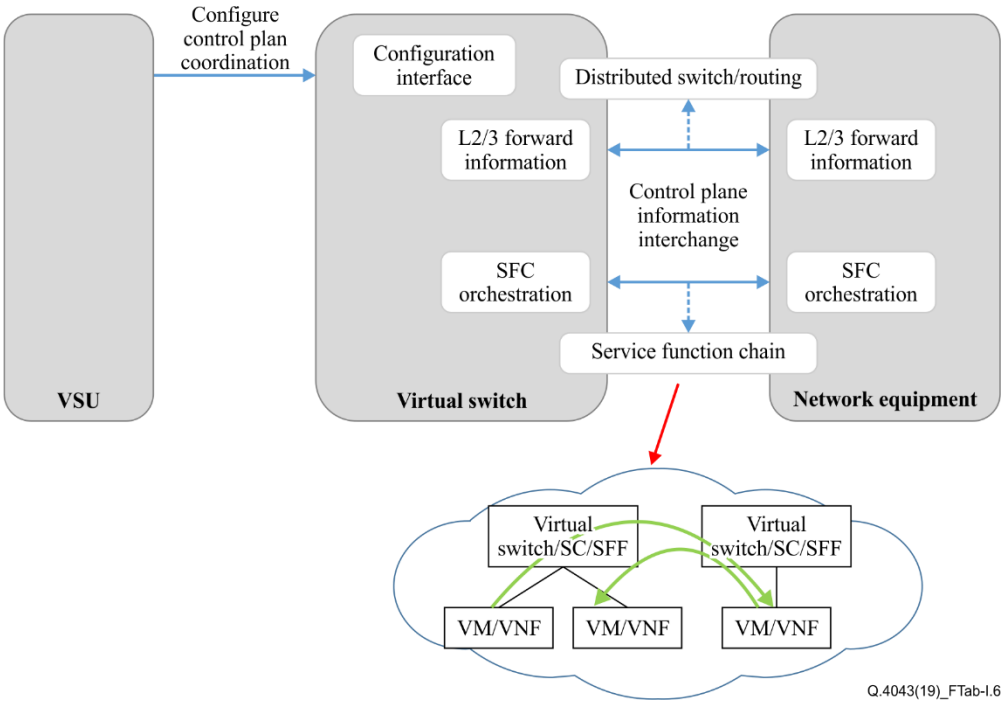
I.4 Virtual switch use cases on tunnelling

Table I.5 – Virtual switch use case on tunnelling

Use case	
Name	Virtual switch use case on tunnelling
Abstract	Virtual switch provides tunnelling capabilities between virtual switch and other network equipment.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Description	VSU login the configuration interface of virtual switch for tunnelling. VSU configure virtual switch to provide tunnelling for network equipment, including those deployed in the form of virtual machines, by configuration interface. Virtual switch can be configured to provide tunnel between virtual switch and network equipment. The virtual switch also can be configured to provide bridging between tunnelling based network and VLAN network. Virtual switch forwarding network traffic between network equipment through tunnel. Virtual switch supports tunnelling protocol including recognise and utilizes tunnel header information for forwarding, filtering and other functions. Virtual switch bridge network traffic between tunnelling based network and VLAN network.
Requirements	– Tunnelling protocol (See clause 8.2.1) – Bridging tunnelling based network and VLAN network (See clause 8.2.1)

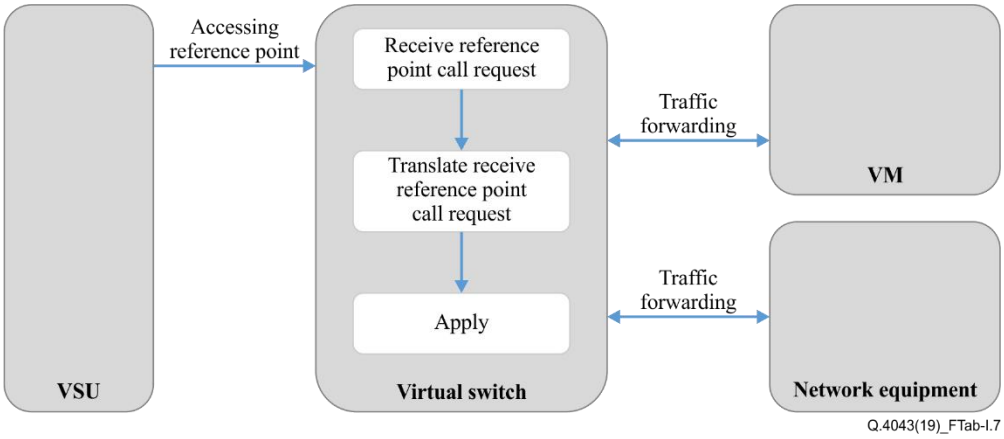
I.5 Virtual switch use cases on control plane coordination

Table I.6 – Virtual switch use case on control plane coordination

Use case	
Name	Virtual switch use case on control plane coordination
Abstract	Virtual switch performs control plane coordination between virtual switch and other network equipment.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Description	VSU login the configuration interface of virtual switch for control plan coordination. VSU configure virtual switch to interchange control plane information with other network equipment to achieve distributed switch/routing and service function chain. For distributed switch/routing, Virtual machines migrating between different switches can achieve consistent forwarding capabilities without additional configuration modifications For service function chaining, virtual switch act as SC to classify services and act as SFF to forward packets to specify next hop VM/VNF.
Requirements	– Distributed virtual switch (See clause 8.2.2) – Distributed routing (See clause 8.2.2) – Service function chain (See clause 8.2.2)

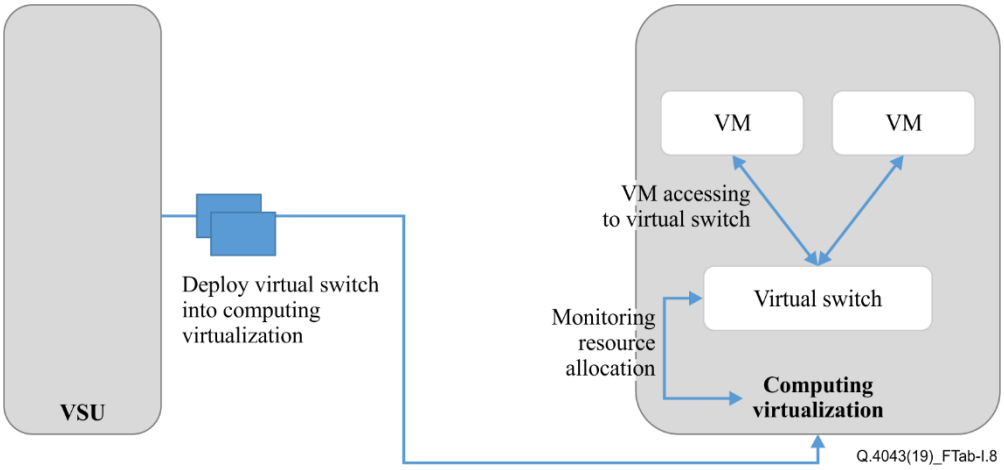
I.6 Virtual switch use cases on reference points

Table I.7 – Virtual switch use case on reference points

Use case	
Name	Virtual switch use case on reference points
Abstract	VSU uses and operates virtual switch through the virtual switch's reference points.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Description	VSU uses and operates virtual switch through the virtual switch's reference points which are implemented according to industry specifications. Through the reference points, VSU can: • manages and monitors virtual switch, including port traffic monitoring, port status monitoring, port mirroring, port traffic statistics, traffic alarm, fault alarm, running log. • utilizes reference points of virtual switch to configure network functions and obtaining/receiving monitoring data, log and alarm.
Requirements	– Reference points for network functions (See clause 8.3.1) – Reference points for network operation (See clause 8.3.1) – Reference points' format (See clause 8.3.1)

I.7 Virtual switch use cases on computing virtualization compatibility

Table I.8 – Virtual switch use cases on computing virtualization compatibility

Use case	
Name	Virtual switch use cases on computing virtualization compatibility
Abstract	Virtual switch provide compatibility for computing virtualization platform.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Description	VSU deploy virtual switch on computing virtualization platform. The deployment can be achieved in different way, such as to deploy as an embedded component of hypervisor, or deploy as a VM. Virtual switch provide accessing for the VMs. Virtual switch monitor computing virtualization platform's resource allocation.
Requirements	– Deploy on server virtualization platform (See clause 8.4.1) – Accessing VM's virtual port (See clause 8.4.1) – VM status awareness (See clause 8.4.1) – Monitoring resource allocation (See clause 8.4.1)

Bibliography

[b-ITU-T Q.4040] Recommendation ITU-T Q.4040 (2016), *The framework and overview of cloud computing interoperability testing*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ETSI NFV-INF 003] ETSI GS NFV-INF 003 V1.1.1 (2014), *Network Functions Virtualisation (NFV); Infrastructure; Compute Domain*.

[b-IEEE Std 802.1D] IEEE Std 802.1D (2004), *Standard for Local and Metropolitan Area-Media Access*.

[b-IEEE Std 802.1q] IEEE Std 802.1q (2014), *802.1Q - Virtual LANs*.

[b-IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[b-IETF RFC 792] IETF RFC 792 (1981), *INTERNET CONTROL MESSAGE PROTOCOL*.

[b-IETF RFC 950] IETF RFC 950 (1985), *Internet Standard Subnetting Procedure*.

[b-IETF RFC 922] IETF RFC 922 (1984), *Broadcasting Internet Datagrams in the Presence of Subnets*.

[b-IETF RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts -- Communication Layers*.

[b-IETF RFC 1142] IETF RFC 1142 (1990), *OSI IS-IS Intra-domain Routing Protocol*.

[b IETF RFC 1195] IETF RFC 1195 (1990), *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.

[b-IETF RFC 2328] IETF RFC 2328 (1998), *OSPF Version 2*.

[b-IETF RFC 2453] IETF RFC 2453 (1998), *RIP Version 2*.

[b-IETF RFC 3376] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

[b-IETF RFC 4632] IETF RFC 4632 (2006), *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*.

[b-IETF RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4)*.

[b-IETF RFC 7498] IETF RFC 7498 (2015), *Problem Statement for Service Function Chaining*.

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

[b-IETF RFC 8300] IETF RFC 8300 (2018), *Network Service Header (NSH)*.

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, 2019