International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.4064

(09/2020)

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

Testing specifications – Testing specifications for IMT-2020 and IoT

Interoperability testing requirements for a virtualized broadband network gateway

Recommendation ITU-T Q.4064

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**
PROTOCOLS AND SIGNALLING FOR P2P COMMUNICATIONS	Q.4100–Q.4139
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.4064

Interoperability testing requirements for a virtualized broadband network gateway

Summary

Recommendation ITU-T Q.4064 specifies virtualized broadband network gateway (vBNG) interoperability testing requirements. As a background, Recommendation ITU-T Q.4064 gives an overview of the vBNG and its interoperability testing, which includes, but is not limited to, the definition, characteristics and general capabilities of vBNG. Use cases of a vBNG are provided in an appendix. Based on an analysis of the vBNG capabilities involved in use cases, the corresponding requirements for vBNG interoperability testing are introduced.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.4064	2020-09-29	11	11.1002/1000/14418

Keywords

Interoperability, requirements, testing, virtual BNG.

* 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	2
4	Abbreviations and acronyms	2
5	Conventions	4
6	Overview of vBNG	4
6.1	Concept of vBNG	4
6.2	Framework of vBNG	5
7	IOPT framework of vBNG	6
8	IOPT requirements of vBNG	7
8.1	IOPT requirements between vBNG and CPE/vCPE	7
8.2	IOPT requirements between vBNG and BNG/vBNG/PE	9
8.3	IOPT requirements between vBNG and management system	10
Appendix I – Typical use cases of vBNG		12
I.1	PPPoE access use case	12
I.2	IPoE access use case	14
I.3	VPN service use case	16
I.4	Multicast service use case	18
I.5	SR use case	20
I.6	Network management use case	21
Bibliography		23

Recommendation ITU-T Q.4064

Interoperability testing requirements for a virtualized broadband network gateway

1 Scope

This Recommendation gives:

1) an overview of the virtualized broadband network gateway (vBNG) comprising:
   a) the concept of vBNG, including its definition, characteristics and general capabilities,
   b) the framework for vBNG, which consists of control and data planes;
2) an interoperability testing (IOPT) framework for vBNG based on its the target areas;
3) IOPT requirements for vBNG.

NOTE – The IOPT requirements of vBNG should include those derived from analysis of typical use cases, which should address the need to verify cloud-related vBNG capabilities.

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 Q.3315] Recommendation ITU-T Q.3315 (2015), *Signalling requirements for flexible network service combination on broadband network gateway*.

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

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 broadband network gateway (BNG) [ITU-T Q.3315]: The access point to the provider's IP network for wireline broadband services.

3.1.2 cloud service customer (CSC) [b-ITU-T Y.3502]: A party which is in a business relationship for the purpose of using cloud services.

3.1.3 cloud service provider (CSP) [b-ITU-T Y.3502]: A party which makes cloud services available.

3.1.4 network virtualization [ITU-T Y.3011]: A technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of

multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource.

3.1.5 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.6 cloud interoperability [ITU-T Q.4040]: The capability to interact between CSCs and CSPs or between different CSPs, 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 virtualized broadband network gateway (vBNG): A virtualized solution of a broadband network gateway, attained by using virtualization technologies, which is responsible for user access and traffic forwarding to realize broadband services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

6VPE	Internet protocol version 6 Virtual private network Provider Edge
AAA	Authentication, Authorization and Accounting
ACK	Acknowledgement
ACL	Access Control List
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
BGP-FS	BGP-Flow Specification
BNG	Broadband Network Gateway
BSS	Business Support System
CHAP	Challenge Handshake Authentication Protocol
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CVLAN	Customer Virtual Local Area Network
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DPI	Deep Packet Inspection
DNS	Domain Name System
DoS	Denial of service
FW	Firewall

GRE	Generic Routing Encapsulation
HQoS	Hierarchical Quality of Service
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IOPT	Interoperability Testing
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPoE	IP over Ethernet
IPvn	Internet Protocol version n
IPTV	Internet Protocol Television
ISIS	Intermediate System-Intermediate System
ITMS	Integrated Terminal Management System
L2TP	Layer 2 Tunnelling Protocol
LCP	Link Control Protocol
MAC	Media Access Control
MANO	Management and Orchestration
MLD	Multicast Listener Discovery
MPLS	Multi-Protocol Label Switching
MSDP	Multicast Source Discovery Protocol
MTU	Maximum Transmission Unit
MVPN	Multicast Virtual Private Network
NAS-Port-ID	Network Access Server Port Identifier
NAT	Network Address Translation
NCP	Network Control Protocol
NFVO	Network Function Virtualization Orchestration
NP	Network Processor
OSPF	Open Shortest Path First
OSS	Operation Support System
PAP	Password Authentication Protocol
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
QinQ	802.1Q-in-802.1Q
QoS	Quality of Service

RADIUS	Remote Authentication Dial-In User Service
SFC	Service Function Chain
SID	Segment Identifier
SNMP	Simple Network Management Protocol
SR	Segment Routing
SR-TE	Segment Routing-Traffic Engineering
SVLAN	Service Virtual Local Area Network
TCP	Transmission Control Protocol
TE	Traffic Engineering
UDP	User Datagram Protocol
URPF	Unicast Reverse Path Forwarding
VAS	Value-Added Service
vBNG	virtualized Broadband Network Gateway
vCPE	virtual Customer Premises Equipment
VIM	Virtual Infrastructure Manager
VLL	Virtual Leased Line
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNFM	Virtual Network Function Manager
VPLS	Virtual Private Local area network Service
VPN	Virtual Private Network
VxLAN	Virtual extensible Local Area Network
WAN	Wide Area Network

5 Conventions

The keywords "is required" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document 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 Overview of vBNG

6.1 Concept of vBNG

A broadband network gateway (BNG) is defined as the access point to a provider's Internet protocol (IP) network for wireline broadband services [ITU-T Q.3315]. vBNG is the virtualization of a BNG by using virtualization technologies, which include network virtualization [ITU-T Y.3011] and compute virtualization technologies. Virtualization technologies aggregate multiple resources, which can be distributed in different equipment in a provider and appear as a single resource. vBNG should meet the signalling requirements between a vBNG and service platform for flexible network service combination on the BNG specified in [ITU-T Q.3315], and the on-demand service based on flexible function provision.

NOTE – The service platform acts as an intermediate layer between the network services and the BNG.

Cloud computing is defined in clause 3.1.5. As a virtualized network element, vBNG can be deployed in a scalable and elastic pool of shared physical or virtual resources, and can provide self-service and administration based on the management system, such as management and orchestration (MANO). vBNG belongs to cloud computing, and its IOPT is a kind of cloud IOPT. Compared to BNG, the characteristics of vBNG can be summarized as follows.

– vBNG can provide such service functions as VNF, so it should provide compatibility for a network function virtualization platform.

– vBNG can provide service functions on demand and customized functions for specific requirements such as deep packet inspection (DPI), firewall (FW) and service function chain (SFC) functions.

– vBNG can provide flexible extensibility of a logical isolated partition to improve service capabilities. One example is that vBNG can extend a data plane by adding forwarding equipment both in virtualized and traditional forms to improve bandwidth.

vBNG usually provides both layer 2 (L2) and layer 3 (L3) network functions. For L2 network functions, it includes user access services and L2 virtual private network (VPN) services, such as a virtual private local area network service (VPLS) and virtual leased line (VLL). For L3 network functions, it refers to routing and multi-protocol label switching (MPLS) services, such as L3 VPN services.

vBNG often interacts with customer premises equipment/virtual customer premises equipment (CPE/vCPE) to provide user access services, and interacts with BNG/vBNG/provider edge (PE) to realize L3 network functions and L2 VPN service. In order to realize the control and management functions of network and service, a vBNG should also interact with a management system such as an operation support system/business support system (OSS/BSS) and MANO.

6.2 Framework of vBNG

The framework of vBNG in this Recommendation is shown in Figure 6-1. It consists of control and data planes.

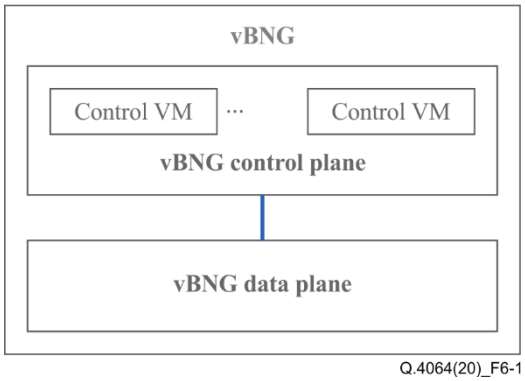


Figure 6-1 – The framework of vBNG

The vBNG control plane is responsible for user access management, user management, address management, authentication management, service management, etc. The vBNG data plane is responsible for packet forwarding.

NOTE 1 – User access management establishes connections with users, including point-to-point protocol over Ethernet (PPPoE), IP over Ethernet (IPoE).

NOTE 2 – User management is responsible for the unified management of user authority, status and business information, such as accounting information.

NOTE 3 – Address management realizes unified allocation and management of user address and service address based on local or external address pools.

NOTE 4 – Authentication management achieves user authentication, which can be implemented locally or remotely. Remotely, vBNG is used as authentication agent by interacting with authentication, authorization and accounting (AAA) systems to realize authentication. Locally, vBNG acts as authentication server to provide the authentication function.

NOTE 5 – Service management is responsible for management of Internet access, L2 or L3 VPN, multicast services, etc.

The vBNG control plane is responsible for functions that need flexible programming of network function and elastic computing capacity, so the control plane is usually deployed as virtual machines (VMs). The vBNG data plane sometimes needs low forwarding capacity when carrying low traffic services like an integrated terminal management system (ITMS), while sometimes it requires high forwarding performance for large capacity and low latency when carrying heavy traffic and delay-sensitive services such as video and Internet protocol television (IPTV). According to the different application scenarios, there are a few kinds of implementation mode for data planes, including equipment based on the central processing unit (CPU), application specific integrated circuit (ASIC) and network processor (NP) chips.

NOTE 6 – Network equipment carried by CPU chips, such as a router deployed on an x86 server, can provide flexible deployment of network functions for more open architecture. A VM is deployed on shared physical resources based on virtualization technology, thus a VM can flexibly expand of functions and performance. Based on the preceding advantages, a vBNG control plane is usually deployed as a VM to flexibly program network function and elastic computing capacity.

7 IOPT framework of vBNG

According to the framework and overview of cloud computing IOPT in [ITU-T Q.4040], which consists of interaction between cloud service customer-cloud service provider (CSC-CSP), CSP-CSP and CSP-management system corresponding to three different target areas, there also are three target areas of vBNG IOPT.

– Target area A: dealing with the interaction between vBNG and access users to provide user access services.

  NOTE 1 – One example of target area A interaction is PPPoE or IPoE access service.

– Target area B: dealing with the interaction between vBNG and BNG/vBNG/PE to provide network services.

  NOTE 2 – One example of target area B interaction is VPN service.

– Target area C: dealing with the interaction between vBNG and a management entity to provide operation- and business-supporting capabilities.

  NOTE 3 – One example of target area C interaction is AAA service.

Based on these three target areas, The IOPT framework of vBNG is as shown in Figure 7-1.

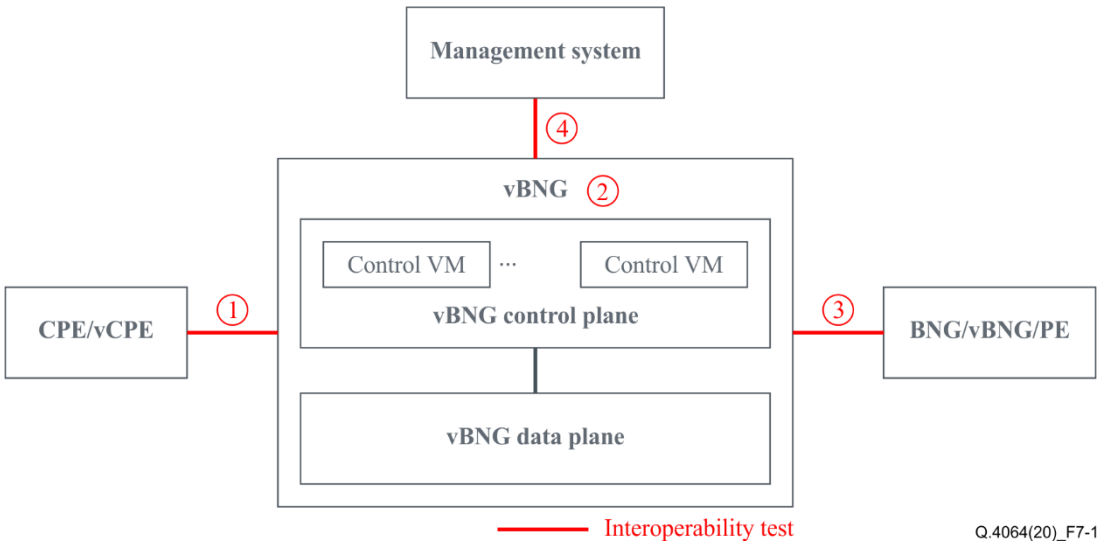


Figure 7-1 – The IOPT architecture of vBNG

The test entities include CPE/vCPE, vBNG, BNG/vBNG/PE and a management system.

1) CPE/vCPE: Equipment deployed on the customer side by service providers to provide wide area network (WAN) services, such as border gateways, network address translation (NAT), and other value-added services (VASs) to customers, especially enterprise customers.

2) vBNG: The IOPT subject.

3) BNG/vBNG/PE: The network device deployed on the WAN side to provide network services, such as those for routing, MPLS and VPN. In the IOPT framework, this entity is peer network equipment interacting with the vBNG under test.

4) Management system: The management system includes the service and operation management system such as OSS/BSS and MANO. It mainly provides device, network and service management functions, including billing management, performance management, fault management, configuration management and security management.

NOTE 4 – The MANO system includes network function virtualization orchestration (NFVO), virtual network function manager (VNFM) and virtual infrastructure manager (VIM).

The IOPT between those entities includes the IOPT of vBNG-CPE/vCPE, vBNG-BNG/vBNG/PE and vBNG-management system.

– vBNG-CPE/vCPE: The IOPT between a vBNG and CPE/vCPE, including verification that user access and authentication functions can be provided through interaction between vBNG and CPE/vCPE.

– vBNG-BNG/vBNG/PE: The IOPT between a vBNG and BNG/vBNG/PE, including verification that routing and tunnel functions can be established between vBNG-BNG/vBNG/PE.

– vBNG-management system: The IOPT between a vBNG and management system, including verification that a vBNG can be managed by an OSS/BSS and MANO to support device management, service management and network management functions.

8 IOPT requirements of vBNG

8.1 IOPT requirements between vBNG and CPE/vCPE

According to different access modes of user and service, IOPT requirements between vBNG and CPE/vCPE include at least the following aspects.

– **PPPoE**: It is required that a vBNG support PPPoE service, including provision of a point-to-point protocol (PPP) connection with CPE/vCPE and allocation of an IP address for a user to access the Internet through CPE/vCPE [b-IETF RFC 2516]. The service should provide both IPv4 and IPv6 access functions.

– **IPoE**: It is required that vBNG support IPoE service, including provision of related access and control functions. The service should provide both IPv4 and IPv6 access functions.

NOTE 1 – Dedicated access service can also be involved in IPoE service, the dedicated access service can provide a fixed IP address to customer.

– **Multicast group management protocol**: It is required that vBNG support access and control functions of multicast users based on the Internet group management protocol (IGMP) [b-IETF RFC 3376] or multicast listener discovery (MLD) protocol [b-IETF RFC 3810]. The service should provide both IPv4 and IPv6 access functions.

– **NAT**: It is required that vBNG support 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 and external networks, and ensure the independence and privacy of the internal network.

– **QoS**: It is required that vBNG support quality of service (QoS) functions for grantee network and service demands, such as traffic classification, bandwidth guarantee, queue scheduling, congestion control and hierarchical quality of service (HQoS).

NOTE 2 – HQoS service refers to multilevel traffic scheduling, such as port, service virtual local area network (SVLAN), customer virtual local area network (CVLAN), and session.

– **VLAN**: It is required that vBNG support a virtual local area network (VLAN) function in order to create a partitioned and isolated broadcast domain at the data link layer.

– **QinQ** (802.1Q-in-802.1Q): It is required that vBNG support encapsulation of 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].

– **VAS**: It is recommended that vBNG support VASs, such as FW and DPI.

NOTE 3 – VASs are premium features and add-ons to basic functions like user access; this kind of function can be deployed on demand.

– **ACL**: It is required that vBNG support an access control list (ACL) function to help to realize the packets filtering and forwarding control by permitting or denying the matched packets.

– **ARP**: It is required that vBNG support provision of an address resolution protocol (ARP) response to CPE/vCPE in order to shrink the ARP domain size and consequently reduce the number of APR broadcast packets that will cause ARP flooding when it is too large.

– **DNS**: It is recommended that vBNG support provision of a domain name system (DNS) function by creating a mapping between the domain name (host) and the address (IP).

– **Access redirection**: It is required that vBNG support redirecting users to a specific web page or IP address.

NOTE 4 – When a customer intends to access the Internet, the network provider can redirect the web page of the customer to a fixed site once the customer logged in, such as a welcome page.

– **MTU** (maximum transmission unit): It is required that vBNG support the limitation of the maximum frame size allowed through the port.

– **Port aggregation**: It is required that vBNG support a port aggregation function by logically using multiple independent links as a single link to achieve flexible high bandwidth and link redundancy.

– **Jumbo frame**: It is required that vBNG support jumbo frames to reduce the number of packets and the overhead of frame header processing.

– **Anti-DoS/DDoS**: It is required that vBNG support traffic restrictions and filtering for specific protocols (such as the transmission control protocol (TCP), user datagram protocol (UDP) and Internet control message protocol (ICMP)) to prevent denial of service or distributed denial of service (DoS/DDoS) attacks.

– **URPF**: It is required that vBNG support unicast reverse path forwarding (URPF) to prevent network attacks based on source address spoofing.

8.2 IOPT requirements between vBNG and BNG/vBNG/PE

According to the different routing protocol and tunnel protocol, the IOPT requirements between vBNG and BNG/vBNG/PE include at least the following aspects.

– **IGP routing protocols**: It is required that vBNG support the interior gateway protocol (IGP) for routing, including the open shortest path first (OSPF) [b-IETF RFC 2328], intermediate system-intermediate system (ISIS) [b-IETF RFC 1142] protocols. IGP can realize route discovery and path computing, and generate network topology based on the link state collection.

– **BGP routing protocol**: It is required that vBNG support aBGP routing protocol [b-IETF RFC 4273]. BGP is a dynamic routing protocol between AS, whose focus is not to find and calculate routes, but to choose the best route between AS and control the propagation of routes.

– **Multicast routing protocols**: It is required that vBNG support multicast routing protocols such as protocol independent multicast-dense mode (PIM-DM) [b-IETF RFC 3973], protocol independent multicast-sparse mode (PIM-SM) [b-IETF RFC 7761], multicast source discovery protocol (MSDP) [b-IETF RFC 3618], etc.

– **Static route**: It is required that vBNG support configuration of static routes to specific destinations defined by network prefix.

– **MPLS protocol**: It is required that vBNG support the MPLS protocol [b-IETF RFC 4364].

– **Tunnelling protocol**: It is required that vBNG support a tunnelling protocol in order to encapsulate frames with tunnel header, recognize and utilizes tunnel header information for forwarding, filtering and other functions, such as generic routing encapsulation (GRE), layer 2 tunnelling protocol (L2TP), L2 VPN and L3 VPN.

NOTE – VPN is a kind of tunnelling technology, including L2 VPN and L3 VPN services specifically, which include at least: VPLS, VLL, L2TP, MPLS VPN, multicast virtual private network (MVPN), IPv6 VPN provider edge (6VPE), virtual extensible local area network (VxLAN).

– **SR protocol**: It is required that vBNG support segment routing (SR) services to realize packet fast forwarding by encapsulation of segment labels such as node segment, prefix segment and adjacent segment in packet. The service includes MPLS-based SR and IPv6-based SR [b-IETF RFC 8402] [b-IETF RFC 8663] [b-IETF RFC 8754].

– **Policy-based routing**: It is required that vBNG support policy-based routing functions to control packet forwarding, including ACL and BGP-flow specification (BGP-FS).

– **MTU**: It is required that vBNG support limitation of the maximum frame size allowed through the ports.

– **QoS**: It is required that vBNG support QoS functions for grantee network and service demands, such as traffic classification, bandwidth guarantee, queue scheduling, congestion control and HQoS.

– **Port aggregation**: It is required that vBNG support a port aggregation function by logically using multiple independent links as a single link to achieve flexible high bandwidth and link redundancy.

– **Jumbo frame**: It is required that vBNG support jumbo frames to improve network throughput and efficiency.

– **Anti-DoS/DDoS**: It is required that vBNG support traffic restrictions and filtering for specific protocols (such as TCP, UDP and ICMP) to prevent DoS/DDoS attacks.

– **URPF**: It is required that vBNG support URPF to prevent network attacks based on source address spoofing.

8.3 IOPT requirements between vBNG and management system

The IOPT requirements between vBNG and management system include at least the following aspects,

– **AAA**: It is required that vBNG support AAA functions.

NOTE 1 – The authentication function refers to user identity verification, such as the remote authentication dial-in user service (RADIUS) protocol [b-IETF RFC 2865]. vBNG should support at least the password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP) algorithms.

NOTE 2 – The authorization is used to grant user specific permissions and provide relevant network service according to service demand, and is usually based on authentication results.

NOTE 3 – The accounting function is used to record the user's usage of various network services and provide the results to the billing system. vBNG should support multiple billing methods, including billing based on time and traffic.

– **DHCP**: It is required that vBNG support the dynamic host configuration protocol (DHCP) relay function. vBNG acts as DHCP relay, and interacts with a DHCP server to allocate addresses [b-IETF RFC 2131].

– **SNMP**: It is required that vBNG support a simple network management protocol (SNMP) function to manage network devices, including at least inspection of device information, modification of device parameter values, monitoring device status, automatic discovery of network faults and report generation.

– **Flow sampling**: It is required that vBNG support a flow-sampling function to monitor the traffic status.

– **Port mirror**: It is required that vBNG support a port mirror function to realize fault location, traffic analysis and traffic backup.

– **Alarm**: It is required that vBNG support an alarm function to report device and service fault information.

NOTE 4 – Faults are due to multiple causes, such as equipment failure, network connection failure and the exhaustion of a network resource.

– **Telemetry**: It is required that vBNG support a telemetry function to collect device and service information, including interface traffic, CPU utilization and bandwidth utilization, and upload it to a collection platform.

– **Virtualized resource management**: It is required that vBNG support virtualized resource management functions by a MANO system, including VNF orchestration based on VNF allocation on demand, lifecycle management of VNF, virtualization infrastructure management by virtual resource allocation, such as virtual computing, virtual storage and virtual network.

NOTE 5 – Virtualized resource management also includes the flexible expansion and contraction function of VNFs in vBNG. For example, the vBNG expands the user management VNF to meet service needs when the number of access users is too large.

– **Basic device configuration**: It is required that vBNG support basic device configuration through a management system, such as IP address configuration of the interface.

– **Service configuration**: It is required that the vBNG support service configuration through a management system to realize service function, such as L2 VPN and L3 VPN service.

Appendix I

Typical use cases of vBNG

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

This appendix identifies use cases of vBNG. Table I.1 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 the use case.
Abstract	Overview and features of the use case.
Description and illustration	Description of the use case and illustration to represent it. (A unified modelling language-like diagram is suggested to clarify 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 dependency may exist among different use cases, pre-conditions and post-conditions are introduced to help understand the relationships among use cases.
Post-conditions (optional)	Post-conditions describe conditions or use cases that are carried out after the termination of a currently described use case.
Requirements	The title of requirements derived from the use case.

I.1 PPPoE access use case

Table I.2 describes a PPPoE access use case.

Table I.2 – PPPoE access use case

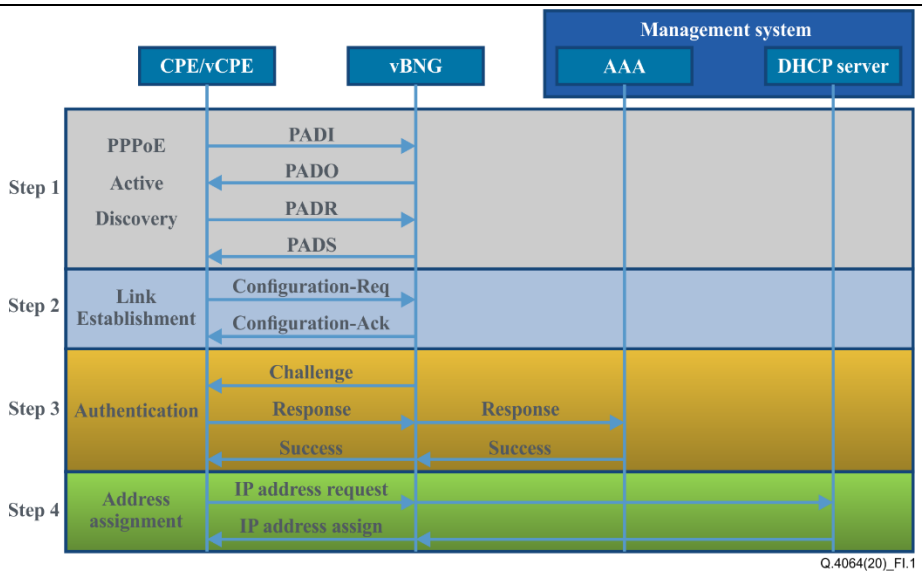
Use case	
Name	PPPoE access service
Abstract	vBNG interacts with CPE/vCPE to provide PPPoE access service to end user for Internet connection
Description and illustration	

Figure I.1 – PPPoE access process

Table I.2 – PPPoE access use case

Use case	
	The PPPoE access process can be divided into discovery and session phases. 1) Discovery phase vBNG establishes a PPPoE connection with CPE/vCPE and assigns a session ID to the user. In Figure I.1, the discovery phase is step 1. 2) Session phase The session phase includes three parts: link control protocol (LCP); authentication; and network control protocol (NCP) negotiation, corresponding to steps 2-4 in Figure I.1. a) Step 2: The LCP stage establishes a link connection. CPE/vCPE and vBNG establish a PPP connection and then negotiate LCP configuration parameters. Only after successful LCP negotiation, will the process come to the authentication or NCP stage, it is usually an Internet protocol control protocol (IPCP) negotiation. b) Step 3: The authentication stage is not necessary in the PPPoE protocol. However, for network security and user management, it is necessary that service providers do it. Authentication of vBNG is usually done in two ways: locally and remotely through an AAA system (such as a RADIUS server). In local authentication, the interaction is only between vBNG and CPE/vCPE. In remote authentication, which is based on an AAA system, the interaction of this function involves CPE/vCPE, vBNG and AAA system entities. Take RADIUS authentication for example, vBNG acts as authentication agent, converses and transmits the PPPoE authentication packet from CPE/vCPE, and the RADIUS packet from the RADIUS server. In addition, authentication algorithms mainly include PAP and CHAP etc. Only once the authentication succeeds can the IPCP negotiation phase start, otherwise PPPoE access fails. c) Step 4: The IPCP stage assigns an IP address. CPE/vCPE and vBNG negotiate the IP address and DNS information for the user through a PPPoE configuration packet. The address allocation mode can be done in two ways: by vBNG or by DHCP server. For address management purposes, service providers often choose the second method. After this stage, vBNG configures the network interface and sync user forwarding table, thus the user can access the Internet. NOTE – From the logical aspect, AAA and DHCP server functions lie within the management system scope. vBNG acts as a proxy to forward user access packets to the AAA and DHCP client.
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	The IOPT requirements between CPE/vCPE and vBNG include at least: – **PPPoE** (see clause 8.1) – **NAT** (see clause 8.1) – **QoS** (see clause 8.1) – **VLAN** (see clause 8.1) – **QinQ** (see clause 8.1) – **VAS** (see clause 8.1) – **ACL** (see clause 8.1) – **ARP** (see clause 8.1) – **DNS** (see clause 8.1) – **Access redirection** (see clause 8.1)

Table I.2 – PPPoE access use case

Use case	
	– **MTU** (see clause 8.1) – **Port aggregation** (see clause 8.1) – **Jumbo frame** (see clause 8.1) – **Anti-DoS/DDoS** (see clause 8.1) – **URPF** (see clause 8.1) The IOPT requirements between vBNG and management system include at least: – **AAA** (see clause 8.3) – **DHCP** (see clause 8.3)

I.2 IPoE access use case

Table I.3 – IPoE access use case

Use case	
Name	IPoE access service
Abstract	vBNG interacts with CPE/vCPE to provide IPoE access service to end user for Internet connection.
Description and illustration	The main purpose of IPoE access service is to obtain an IP address for the user to connect to the Internet. IPoE access service mainly includes IPoE user access, authentication and address allocation functions. IPoE access process comprises four steps: 1) user identification and authentication initiation; 2) identity authentication; 3) address allocation; 4) accounting. For 3), the DHCP dynamic address allocation method is used to allocate an address, and the IP address is released through the DHCP release protocol. The DHCP address allocation process includes the following four principal steps: 1) DHCP discovery; 2) DHCP offer; 3) DHCP request; 4) DHCP ACK (acknowledgement). See Figure I.2.

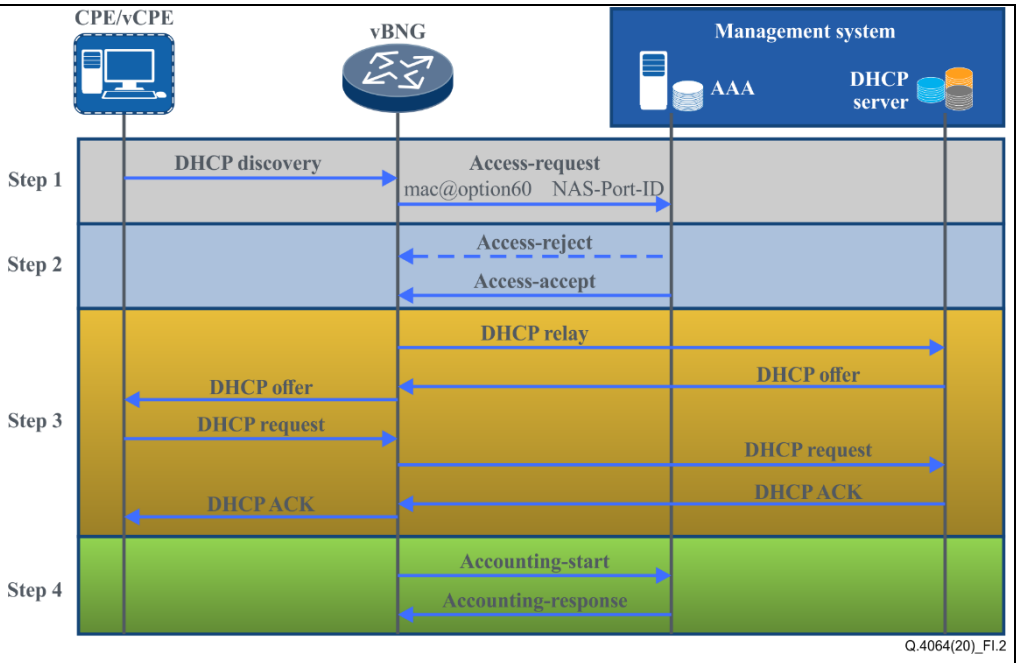


Figure I.2 – IPoE access process

The signalling interaction process of IPoE access service can be described as follows.

1) Step 1: user identification and authentication initiation
   a) User terminals or CPE initiate DHCP requests with the corresponding option 60 information (it usually uses a fixed media access control (MAC) address as username to initiate requests).
   b) Intermediate network devices label option 82 information according to relevant specifications.
   c) On receipt of a user request message, vBNG extracts the MAC address, option 60, option 82 information, and forms a username format: MAC@Option 60. It also converts option 82 information into network access server port identifier (NAS-Port-ID) information and sends it to RADIUS authentication.

      NOTE – Option 82 and option 60 are both DHCP options. Option 82, which is specified in [b-IETF RFC 3046], is a relay agent information option to identify user location by carrying relay agent information in the packet. Option 60, which is specified in [b-IETF RFC 2132] is used to report manufacturer and configuration information of a terminal.
2) Step 2: identity authentication

The RADIUS server returns a rejection message if authentication fails and vBNG terminates the user session.

If authentication succeeds, vBNG sends back the authenticated information with the relevant service policy attributes of the user.

3) Step 3: address allocation
   a) vBNG relays DHCP requests to the DHCP server for address allocation.
   b) DHCP server assigns corresponding addresses to users according to different service information.
   c) vBNG gets the user address and sends DHCP ACK information to the end user or CPE, and the user can surf the Internet.
4) Step 4: accounting
   a) vBNG sends an accounting start message to the AAA system.
   b) AAA system completes the relevant processing and sends a response message to vBNG.

Table I.3 – IPoE access use case

Use case	
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	The IOPT requirements between CPE/vCPE and vBNG include at least: – **IPoE** (see clause 8.1) – **NAT** (see clause 8.1) – **QoS** (see clause 8.1) – **VLAN** (see clause 8.1) – **QinQ** (see clause 8.1) – **VAS** (see clause 8.1) – **ACL** (see clause 8.1) – **ARP** (see clause 8.1) – **DNS** (see clause 8.1) – **Access redirection** (see clause 8.1) – **MTU** (see clause 8.1) – **Port aggregation** (see clause 8.1) – **Jumbo frame** (see clause 8.1) – **Anti-DoS/DDoS** (see clause 8.1) – **URPF** (see clause 8.1) The IOPT requirements between vBNG and management system include at least: – **AAA** (see clause 8.3) – **DHCP** (see clause 8.3)

I.3 VPN service use case

Table I.4 – VPN service use case

Use case	
Name	VPN service
Abstract	vBNG interacts with BNG/vBNG/PE to provide private communication over a public network for VPN service.
Description and illustration	VPN service consists of different types as described in clause 8.2, the realization principle of different VPN services also varies, but the idea is similar. In this clause, the MPLS VPN use case is taken as an example to make the description. MPLS VPN is the use of MPLS technology in the backbone of a broadband IP network to build an IP private network especially for enterprises, so as to achieve cross-regional, secure, high-speed, reliable communication for data, voice, image and video. See Figure I.3.

Table I.4 – VPN service use case

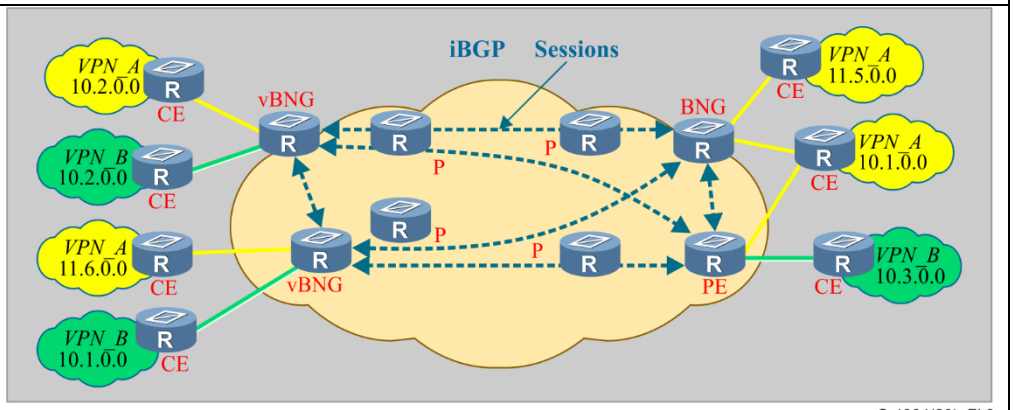
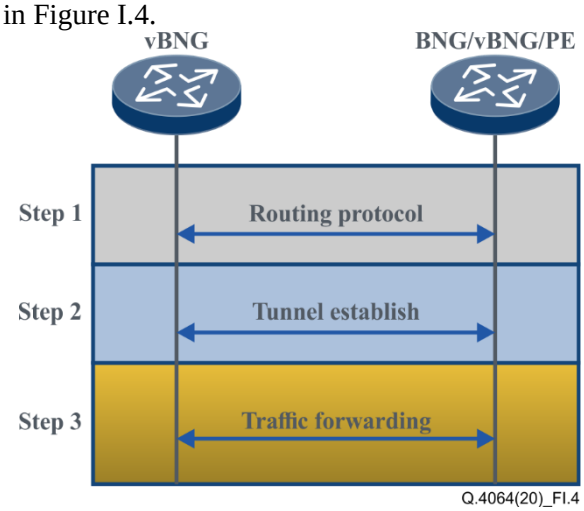
Use case	
	 Q.4064(20)_FI.3 **Figure I.3 – MPLS VPN service topology** VPN services are provided by vBNG and vBNG/BNG/PE. The process of VPN service is shown in Figure I.4.  Q.4064(20)_FI.4 **Figure I.4 – VPN service process** – Step 1: vBNG runs a routing protocol with BNG/vBNG/PE to establish an L3 network connection. – Step 2: vBNG and BNG/vBNG/PE establish a tunnel connection through a VPN instance. – Step 3: vBNG imports user traffic into the VPN tunnel. Users cannot feel the existence of public networks, just as they have independent network resources. NOTE – VPN service can be realized with QoS and traffic engineering (TE)
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	The IOPT requirements of a VPN service include the interaction between vBNG and BNG/vBNG/PE. The requirements are as follows. Requirements between vBNG and BNG/vBNG/PE include at least: – **IGP routing protocols** (see clause 8.2) – **BGP routing protocol** (see clause 8.2) – **Static route** (see clause 8.2) – **MPLS protocol** (see clause 8.2)

Table I.4 – VPN service use case

Use case	
	– **Tunnelling Protocol** (see clause 8.2) – **Policy-based routing** (see clause 8.2) – **MTU** (see clause 8.2) – **QoS** (see clause 8.2) – **Port aggregation** (see clause 8.2) – **Jumbo frame** (see clause 8.2) – **Anti-DoS/DDoS** (see clause 8.2) – **URPF** (see clause 8.2)

I.4 Multicast service use case

Table I.5 – Multicast service use case

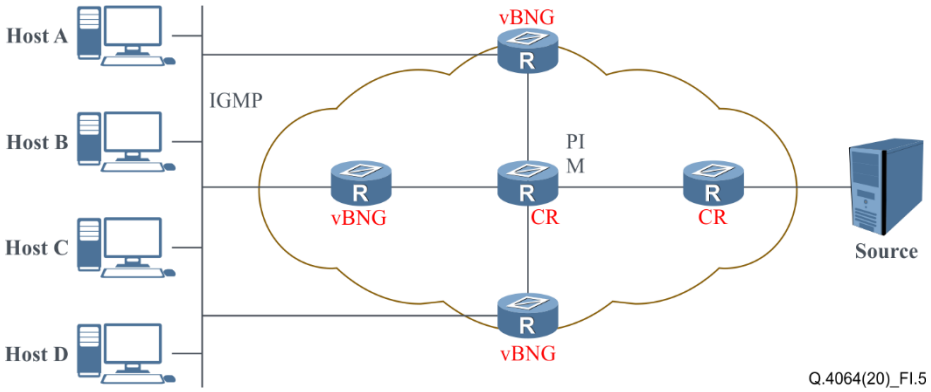
Use case	
Name	Multicast service use case
Abstract	vBNG interacts with CPE/vCPE to provide a multicast service to the end user.
Description and illustration	Multicast service is efficient data transmission from point to multi-point based on a multicast group management protocol (e.g., IGMP) and multicast routing protocol (e.g., PIM). A multicast service uses a multicast routing protocol to transfer information in a WAN and a multicast group management protocol to manage the multicast group. The typical multicast model is shown in Figure I.5, it consists of a user, vBNG and IP backbone network.  **Figure I.5 – Multicast service model** Multicast service is provided by CPE/vCPE, vBNG and vBNG/BNG/PE, the process of multicast service is as shown in Figure I.6.

Table I.5 – Multicast service use case

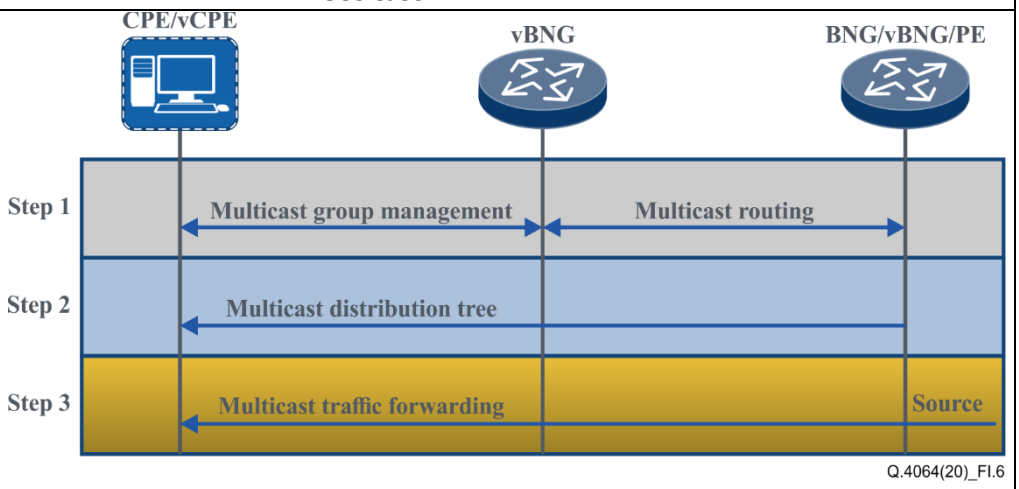
<table>
<tr><th colspan="2">Use case</th></tr>
<tr><td></td><td>


Figure I.6 – Multicast service process
1) Step 1: vBNG runs a multicast group management protocol to establish a multicast user connection by CPE/vCPE, and manages the multicast group. vBNG runs a multicast routing protocol between vBNG and BNG/vBNG/PE to realize multicast routing and forwarding.
2) Step 2: vBNG establishes the multicast routing table based on the multicast distribution tree.
3) Step 3: vBNG can replicate and forward multicast traffic to users through CPE/vCPE.
NOTE 1 – Multicast VPN should be supported.
NOTE 2 – L2 multicast should be supported.
</td></tr>
<tr><td>Pre-conditions (optional)</td><td>User already accesses the Internet through PPPoE or IPoE.</td></tr>
<tr><td>Post-conditions (optional)</td><td></td></tr>
<tr><td>Requirements</td><td>
The IOPT requirements of multicast service include interactions between: vBNG and BNG/vBNG/PE; and CPE/vCPE and vBNG.
The IOPT requirements between vBNG and BNG/vBNG/PE include at least:
– IGP routing protocols (see clause 8.2)
– BGP routing protocol (see clause 8.2)
– Multicast routing protocols (see clause 8.2)
– Policy based routing (see clause 8.2)
– MTU (see clause 8.2)
– QoS (see clause 8.2)
– Port aggregation (see clause 8.2)
– Jumbo frame (see clause 8.2)
– Anti-DoS/DDoS (see clause 8.2)
– URPF (see clause 8.2)
The IOPT requirements between vBNG and CPE/vCPE include at least:
– Multicast group management protocol (see clause 8.1)
– NAT (see clause 8.1)
– QoS (see clause 8.1)
– VLAN (see clause 8.1)
– QinQ (see clause 8.1)
– VAS (see clause 8.1)
</td></tr>
</table>

Table I.5 – Multicast service use case

Use case	
	– **ACL** (see clause 8.1) – **ARP** (see clause 8.1) – **DNS** (see clause 8.1) – **Access redirection** (see clause 8.1) – **MTU** (see clause 8.1) – **Port aggregation** (see clause 8.1) – **Jumbo frame** (see clause 8.1) – **Anti-DoS/DDoS** (see clause 8.1) – **URPF** (see clause 8.1)

I.5 SR use case

Table I.6 – SR use case

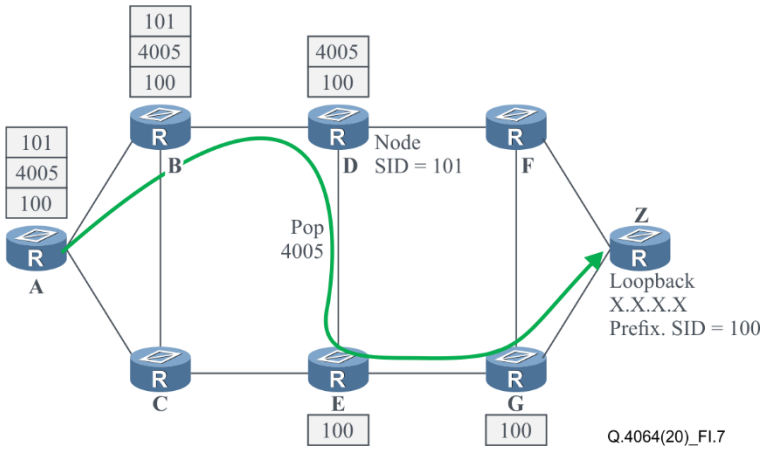
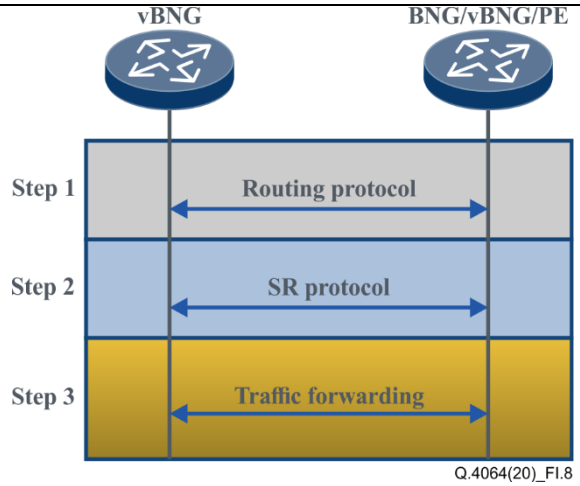
Use case	
Name	SR use case
Abstract	vBNG interacts with BNG/vBNG/PE to provide fast forwarding and traffic engineering functions over a public network by SR service.
Description and illustration	SR is a protocol whose design is based on the idea of source routing to forward packets. It divides the network path into segments and assigns a segment identifier (SID) to them and also to the forwarding nodes in the network. The forwarding path consists of a list of by ordered SIDs. NOTE – Source routing is the mechanism by which the traffic carries the transmission path in the packet at the head node. SR can be directly applied to the MPLS architecture without any changes in forwarding mechanism. The SID representing the segment is encoded as an MPLS label. The segment sequence is encoded as a label stack. The segment to be processed is at the top of the stack. After a segment is processed, the relevant tags are ejected from the tag stack. See Figure I.7.  **Figure I.7 – SR forward model based on node and adjacent SIDs** SR service is implemented by vBNG and vBNG/BNG/PE, the process of SR service is as shown in Figure I.8.

Table I.6 – SR use case

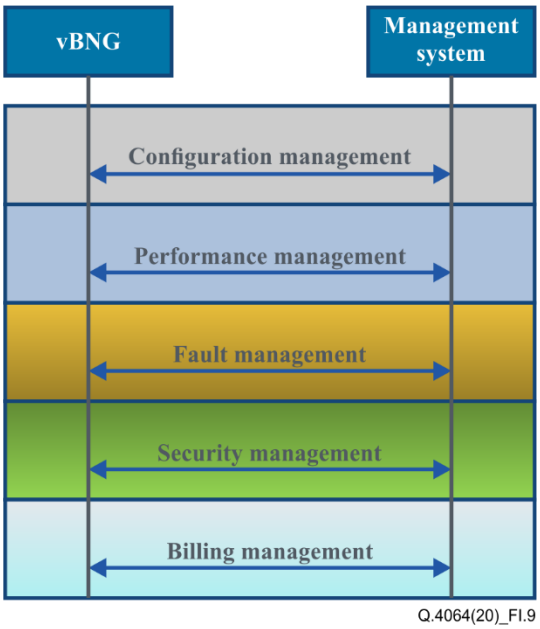
Use case	
	 **Figure I.8 – SR service process** – Step 1: vBNG and BNG/vBNG/PE run an IGP protocol to establish an L3 network connection. – Step 2: vBNG and BNG/vBNG/PE run an SR protocol; usually MPLS protocol is needed as basic. The SID is distributed by the controller or IGP protocol. Based on the routing table and SID, vBNG establishes the SR label forwarding table. – Step 3: vBNG and BNG/vBNG/PE forward SR traffic. NOTE – Segment routing-traffic engineering (SR-TE) controls the service path by labelling the path in the packet at the head node. The intermediate nodes do not need to retain the path information.
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	The IOPT requirements of SR service are mainly the interaction between vBNG and BNG/vBNG/PE. The IOPT requirements between vBNG and BNG/vBNG/PE include at least: – **IGP routing protocols** (see clause 8.2) – **BGP routing protocol** (see clause 8.2) – **Static route** (see clause 8.2) – **SR protocol** (see clause 8.2) – **Policy based routing** (see clause 8.2) – **MTU** (see clause 8.2) – **QoS** (see clause 8.2) – **Port aggregation** (see clause 8.2) – **Jumbo frame** (see clause 8.2) – **Anti-DoS/DDoS** (see clause 8.2) – **URPF** (see clause 8.2)

I.6 Network management use case

Table I.7 – Network management use case

Use case	
Name	Network management use case

Table I.7 – Network management use case

Use case	
Abstract	vBNG interacts with a management system to support its fault management, configuration management, performance management, security management and billing management functions.
Description and illustration	Network management includes the management of network equipment hardware, software and network services in order to monitor, test, configure, analyse, evaluate and control network resources, so that network operation status and service quality can be grasped in real time. When there is a network failure, operators can deal with it in time, so as to ensure the stable operation of the network system. vBNG interacts with management system to realize management functions as shown in Figure I.9.  **Figure I.9 – Network management functions**
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	The IOPT requirements of network management mainly refer to the interaction between vBNG and the management system. The IOPT requirements between vBNG and management system include at least: – **AAA** (see clause 8.3) – **DHCP** (see clause 8.3) – **SNMP** (see clause 8.3) – **Flow sampling** (see clause 8.3) – **Port mirror** (see clause 8.3) – **Telemetry** (see clause 8.3) – **Virtualized resource management** (see clause 8.3) – **Basic device configuration** (see clause 8.3) – **Service configuration** (see clause 8.3)

Bibliography

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-IEEE 802.1Q] IEEE 802.1Q-2018, *IEEE Standard for local and metropolitan area networks – Virtual bridged local area networks.*

[b-IETF RFC 1142] IETF RFC 1142 (1990), *OSI IS-IS intra-domain routing protocol*.

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic host configuration protocol.*

[b-IETF RFC 2132] IETF RFC 2132 (1997), *DHCP options and BOOTP vendor extensions.*

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

[b-IETF RFC 2516] IETF RFC 2516 (1999), *A method for transmitting PPP over Ethernet (PPPoE)*.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote authentication dial in user service (RADIUS).*

[b-IETF RFC 3046] IETF RFC 3046 (2001), *DHCP relay agent information option*.

[b-IETF RFC 3376] IETF RFC 3376 (2002), *Internet group management protocol, version 3*.

[b-IETF RFC 3618] IETF RFC 3618 (2003), *Multicast source discovery protocol (MSDP).*

[b-IETF RFC 3810] IETF RFC 3810 (2004), *Multicast listener discovery version 2 (MLDv2) for IPv6*.

[b-IETF RFC 3973] IETF RFC 3973 (2005), *Protocol independent multicast-dense mode (PIM-DM): Protocol specification (revised).*

[b-IETF RFC 4273] IETF RFC 4273 (2006), *Definitions of managed objects for BGP-4.*

[b-IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP virtual private networks (VPNs).*

[b-IETF RFC 7761] IETF RFC 7761 (2016), *Protocol independent multicast-sparse mode (PIM-SM): Protocol specification (Revised).*

[b-IETF RFC 8402] IETF RFC 8402 (2018), *Segment routing architecture.*

[b-IETF RFC 8663] IETF RFC 8663 (2019), *MPLS segment routing over IP*.

[b-IETF RFC 8754] IETF RFC 8754 (2020), *IPv6 segment routing header (SRH).*

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, 2020