International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3713

(03/2017)

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

Signalling requirements and protocols for SDN – Resource control protocols

Signalling requirements for broadband network gateway pool

Recommendation ITU-T Q.3713

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
Resource control protocols	**Q.3710–Q.3739**
TESTING SPECIFICATIONS	Q.3900–Q.4099

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

Recommendation ITU-T Q.3713

Signalling requirements for broadband network gateway pool

Summary

Recommendation ITU-T Q.3713 describes the scenarios, architecture and signalling for broadband network gateway (BNG) pool in order to achieve the following outstanding benefits: high reliability for broadband access services, resource sharing and load balancing among multiple BNG devices which composed a pool, simplified operation administration and maintenance (OAM) and reduction of operational expenditure (OPEX) and capital expenditure (CAPEX).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3713	2017-03-29	11	11.1002/1000/13247

Keywords

Broadband network gateway, BNG, pool.

* 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

Recommendation ITU-T Q.3713

Signalling requirements for broadband network gateway pool

1 Scope

This Recommendation describes the scenarios, the architecture and the networking method for BNG pool. It specifies signalling requirements and procedures between the controller and BNG devices. Signalling between the controller and the application is outside the scope of this Recommendation.

2 References

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

[ITU-T Q.3711] Recommendation ITU-T Q.3711 (2016), *Signalling requirements for software-defined broadband access network.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BNG	Broadband Network Gateway
CAPEX	Capital Expenditure
IP	Internet Protocol
IPTV	Internet Protocol Television
MAC	Media Access Control
NETCONF	Network Configuration Protocol
OAM	Operation Administration and Maintenance
OLT	Optical Line Terminal
OPEX	Operational Expenditure
OTN	Optical Transport Network
QoS	Quality of Service

SBAN Software-defined Broadband Access Network

SNMP Simple Network Management Protocol

VLAN Virtual Local Area Network

5 Conventions

In this Recommendation:

The keywords "is required to" 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.

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

6 Introduction of BNG pool

With the fast development of broadband service/network, higher requirements for BNG are needed. This includes addressing the following problems when deploying BNG in current carrier networks:

– As BNGs are usually deployed individually, according to its geographical region, there is usually no redundancy/protection function deployed among multiple BNG devices. As a result, the high reliability requirement for high value services, e.g., Internet protocol television (IPTV), customer leased-line services cannot be met.

– Given its low reliability, BNGs are not allowed to serve a large number of users simultaneously so as to avoid interrupting users' service. This leads to excessive waste of BNG resources.

– Resource utilization in BNGs is significantly different depending on its deployment location, carried services, etc., which may also lead to the waste of BNG resources.

– The individual deployment of BNG increases the complexity of BNG OAM.

– Given the high requirements regarding the BNG deployment environment (e.g., the power supply, transmission resources), the individual deployment of BNGs would increase the CAPEX.

A BNG pool architecture is proposed to solve the problems described above. In this architecture, BNG devices will be deployed in a moderately centralized manner. A BNG pool is composed of multiple BNG devices located in a central office or multiple central offices which are geographically adjacent to each other. Using BNG pool architecture has the following advantages:

– The BNG devices in one pool can provide the backup protection for each other, which can achieve the high reliability to meet the requirements of high value services.

– The BNG devices in one pool can provide resource sharing and load balancing, which can improve the overall resource utilization.

– The BNG pool can be maintained and operated as a whole, which can simplify the OAM.

– Moderately centralized deployment of BNG devices can reduce the demand for central office, which can greatly reduce the CAPEX.

Note that the hot-standby technology has been deployed to ensure the reliability of BNG. However, this technology is based on a totally distributed approach, which makes it complicated to configure, monitor, manage and coordinate the BNG devices. This will place high pressure on the BNG control plane. The BNG pool architecture is based on a centralized control mode, which facilitates centralized/unified coordination and scheduling, and helps achieve load balancing among the BNG devices. Under the control of a centralized controller, the pressure on control plane of the BNG can be alleviated, unified OAM for BNG devices can be achieved and differentiated requirements from the applications can be satisfied through open application programming interfaces (APIs).

7 Architecture of the BNG pool

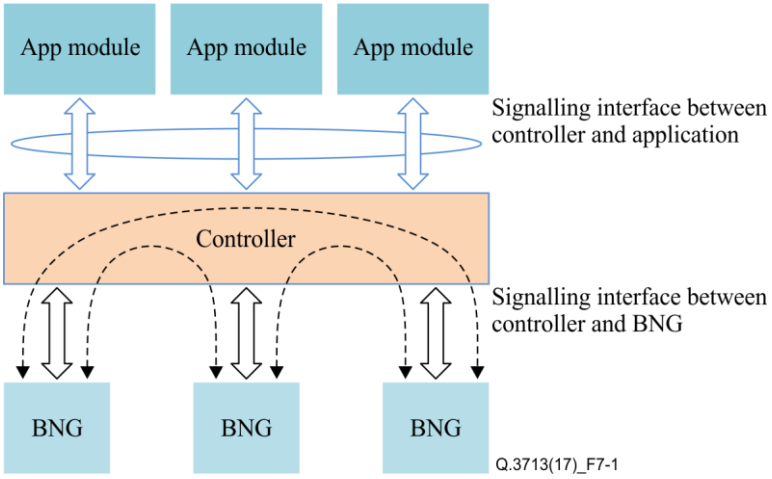

Figure 7-1 – The architecture of the BNG pool

The architecture of the BNG pool, which is required to be kept aligned with the software-defined broadband access network (SBAN) model defined in [ITU-T Q.3711], is divided into three layers, as shown in Figure 7-1. The BNG is responsible for the packet forwarding, policy enforcing and route processing, etc. The controller performs central control and coordination among multiple BNG devices which belong to the same BNG pool. Services can be easily configured based on the application modules with the northbound APIs provided by the controller.

The controller is in charge of the BNG pool, and the BNG devices forward data packets, provide the backup protection for each other and realize the load balancing among members of the BNG pool based on the actions/commands from the controller. The application interface defined by the controller is open for the upper application developers, which can satisfy the application requirements, for example, providing differentiated quality of service (QoS) for specific services/users.

The detailed signalling between the application and the controller is not included in this Recommendation. The signalling between the controller and the BNG is described in clause 8.

8 Signalling requirements for the BNG pool

As the hub node, the controller establishes the star-like control connections with each member of the BNG pool. To realize the high reliability and load balancing in the BNG pool, the following signalling requirements between the controller and the member of the BNG pool is recommended to be specified.

No new protocol is specified here, and the signalling can be implemented with existing protocols with possible extension.

8.1 Signalling for membership management and configuration of the BNG pool

The controller is in charge of the membership management for the BNG pool. The membership management functions include adding a new member, deleting an old member, and monitoring the status of each member of the BNG pool.

Figure 8-1 illustrates the signalling flow of the membership management and configuration between the controller and the BNG device.

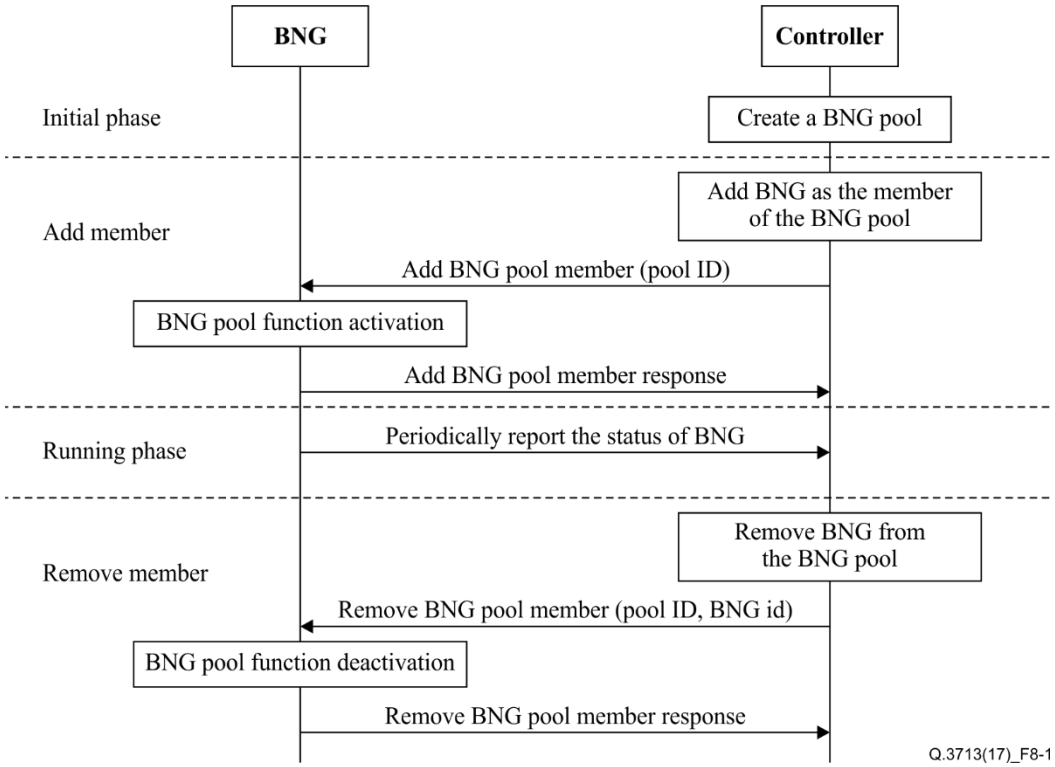

Figure 8-1 – The membership management and configuration procedure

At the initial phase, the controller creates a BNG pool after receiving an external request. The request could be issued from the operator, or one application module, etc. The detailed signalling between the controller and the application is not included in this Recommendation.

For membership management, the controller sets up a membership relation by adding a BNG device into the BNG pool. The message of adding a BNG pool member is generated and sent to the BNG device by the controller. A pool ID is carried in this message to identify the BNG pool. With receipt of the message, the BNG gets the information of membership and enables the corresponding BNG pool functions.

The BNG device is recommended to notify its status to the controller used for the functions of the load balancing, the fault protection, etc. This notification is recommended to be periodically sent, and the controller knows the status of all members in the BNG pool.

The procedure of removing members from the BNG pool is similar to the procedure of adding members.

The controller is also in charge of the management of the IP address pool in the BNG pool. This IP address pool is located in the BNG, and used for allocating IP addresses to the dial-up users.

When a BNG device becomes a member of the BNG pool at the initial phase, or when the address pool of BNG devices is about to run out and the number of online users reaches the upper limit of the address pool at the running phase, the BNG applies for new IP addresses from the controller.

When the number of online users is much less than the address number of the address pool, the BNG releases parts of IP addresses to improve the utilization of IP address resource.

Figure 8-2 illustrates the address management procedure in the BNG pool.

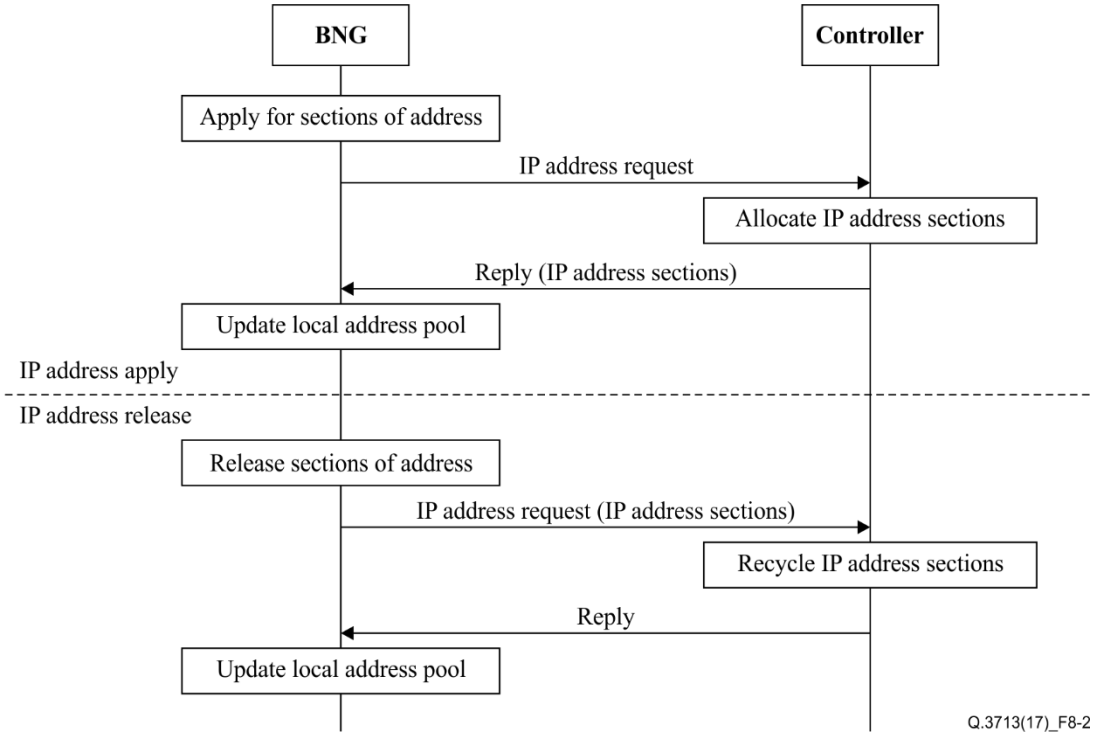

Figure 8-2 – The address pool management procedure

Each BNG device in the BNG pool detects the utilization of the local address pool. If the number of addresses in the local address pool is inadequate, the BNG generates an IP address request message and sends it to the controller to apply for new IP address sections. The controller then allocates IP address sections, and returns the response message with the allocated IP address sections to the BNG. On the contrary, if the IP addresses in the local address pool are used inefficiently, the BNG releases part of the unused IP addresses. Hence, the unused IP addresses in a BNG can be reused by other BNG and the IP address utilization ratio is improved correspondingly. The BNG generates the IP address request message and sends it to the controller to release unused IP addresses. The controller recycles the released IP addresses, and responds with the confirmation message to inform success or failure.

As described in Appendix I, the access requests from different users are recommended to be distributed among BNG devices of the BNG pool to achieve load balancing with the granularity of user group. The user group information can be extracted from the user access request or reply messages. The controller is required to allocate a different IP address block for every user group, otherwise, it might cause a routing problem. For example, in the case when the access requests from user group 1 are assigned to device BNG1 of BNG pool1 as described in Figure A.1, if the same IP address block is divided into two parts, one part is assigned to user group 1, and the other part is assigned to user group 2. So, when packets are switched between BNG1 and BNG2, this will cause the router in the IP core network not to know how to set up the next hop in the routing entry for this IP address block to forward downstream packets. The above problem can be avoided by allocating different IP address block for different user groups.

As described in clause 8.5, if a backup BNG takes over a faulty BNG based on the protection policy, the corresponding user traffic will be transferred seamlessly to the backup BNG. In order to achieve this, the destination media access control (MAC) address of packets sent from users is required to

remain unchanged, regardless of whether it is the primary BNG or the backup BNG. If the destination MAC address is set to the real MAC address of the primary BNG, the packets coming from users will be discarded by the backup BNG during the procedure of protection switch. Allocating a virtualized gateway MAC address to both the primary and backup BNG can solve this problem. The controller is in charge of managing virtualized MAC addresses and allocating virtual MAC addresses to the BNG by using the reply message.

There have been a variety of protocols between the controller and the network device, such as network configuration protocol (NETCONF), Openflow, simple network management protocol (SNMP), etc. The BNG device could be managed, configured and controlled by the controller through such protocols. The details of those existing protocols are beyond the scope of this Recommendation.

8.2 Signalling for the notification of BNG status/information

The BNG is recommended to notify its own status to the controller, which may include the load situation, the fault information (e.g., link/port/card failure), etc. The controller is recommended to be aware of the detailed status of each member of the BNG pool. Based on the BNG real-time status, it is possible to perform fault protection and load balancing. The BNG is recommended to also report some key information to the controller, such as the topology information.

As depicted in Figure 8-1, each BNG reports real-time load situation to the controller during the running phase. After receiving user access requests, the controller will decide which BNG in the BNG pool can provide service. If the real-time load of one BNG reaches the maximum threshold, the controller will dispatch the traffic from new users or a part of online users of this BNG to other BNGs. This load balancing procedure is illustrated in clause 8.5.

Each BNG also reports the topology information to the controller in the initial phase or in the running phase when the network topology changes, as depicted in Figure 8-1. The topology information is recommended to include (not limited):

– BNG identification;
– Board/Line card;
– Link;
– Interface.

8.3 Signalling for fault monitoring and notification

To realize the high reliability, signalling for the fault monitoring and notification is required between the controller and the member of the BNG pool, thus the failure can be detected as soon as possible.

In active mode, each BNG member will notify fault information to the controller when a failure occurs in the running phase as depicted in Figure 8-1. Then the controller will choose another BNG in the BNG pool to take over the services carried by the fault BNG.

In passive mode, the controller monitors the real-time status of each member of the BNG pool. When a BNG is out of service, the controller can detect the failure quickly through the monitoring mechanism. Then it will decide which BNG in the BNG pool can take over the service carried by the fault BNG.

The fault protection procedure is illustrated in clause 8.5.

8.4 Signalling for synchronization of user session information among BNGs

To realize hot-standby protection for a link/port/card/device failure and a user seamless migration, users' session information (including user IP/MAC, accounting information, etc.) of one BNG is recommended to be synchronized to its backup BNG. Optionally, such information can be transferred via the controller.

The controller is in charge of maintaining the relationship between the primary and hot-standby BNG, and assigning it to BNGs. Each BNG synchronizes its user session information to its backup BNG in a real-time manner. These synchronization information is recommended to include (not limited):

– user session, such as IP/MAC, a PPPoE session ID;

– account information;

– IP address sections;

– user group, such as a physical interface, a logical sub-interface, virtual local area network (VLAN) and MAC.

8.5 Signalling for user traffic scheduling among BNGs

To realize fault protection and load balancing, the controller is recommended to forward the corresponding user session information to the target BNG and inform the BNG to enable the user session information in its forwarding plane, thus the BNG can take over the corresponding user traffic.

The controller collects the load information of each BNG of the BNG pool in the running phase as depicted in Figure 8-1. It assigns the BNG with lower load to serve the new access users. This balances the load of each BNG in the BNG pool.

Figure 8-3 illustrates the load balancing procedure of the BNG pool.

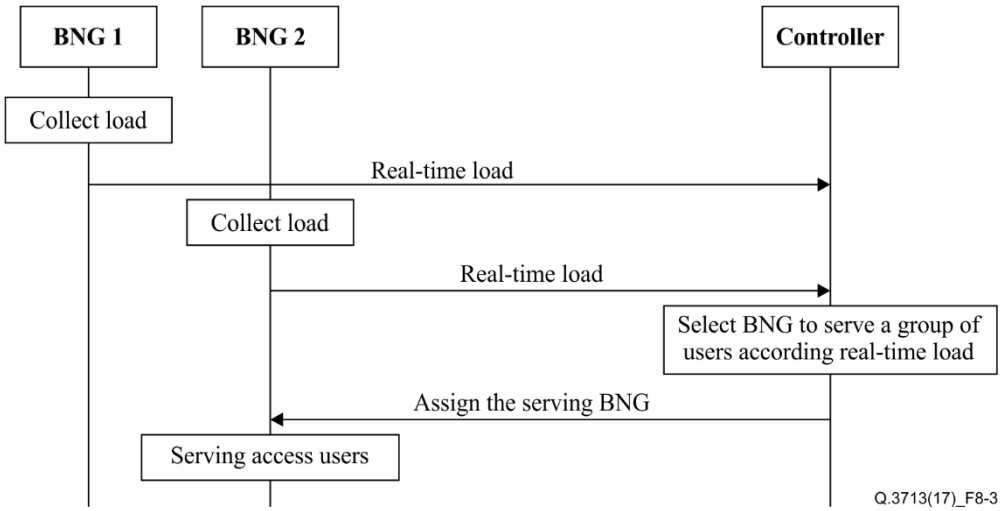

Figure 8-3 – The load balancing procedure

Each BNG in the BNG pool periodically collects and reports the load information to the controller. The controller obtains and analyses the load status of every member in the BNG pool, decides which BNG to serve the new coming users and then configures it. In this way, each BNG serves a part of the overall users to realize the traffic load balancing among all the members of the BNG pool. The controller is responsible for traffic allocation among all BNGs in the BNG pool to realize load balancing.

When the controller receives a fault report as described in clause 8.3, it becomes aware that a fault occurred in a BNG, and will select a normal operation BNG device from the BNG pool to take over the faulty one.

Figure 8-4 illustrates the fault protection procedure of the BNG pool.

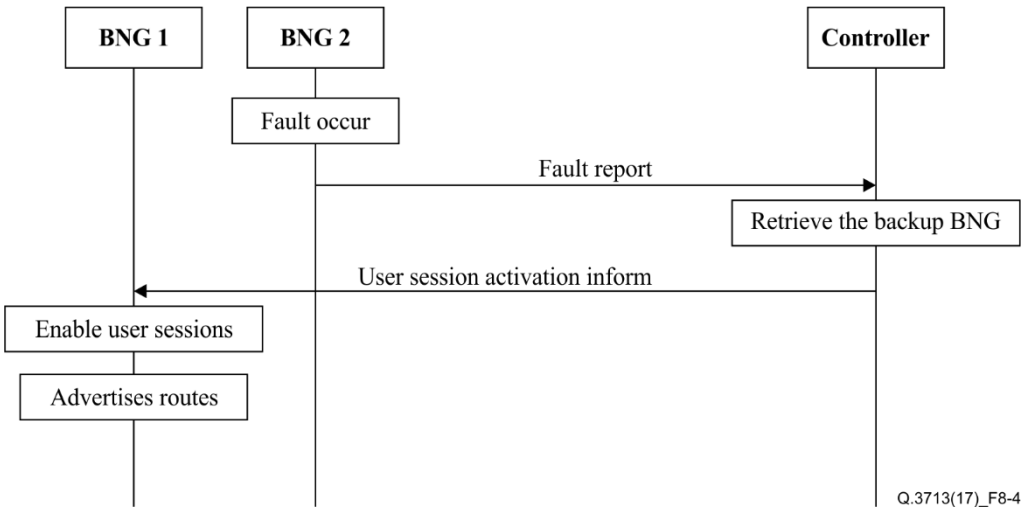

Figure 8-4 – The fault protection procedure

Each BNG in the BNG pool monitors its status and detects its faults. It reports the fault information to the controller as soon as possible when a fault occurs. The controller receives the fault report and retrieves the backup BNG. It then informs the backup BNG to enable the user session information in the forwarding plane. The backup BNG starts to work for these affected users, and advertises corresponding routes based on the IP address section that allocated by the controller as described in clause 8.1.

The fault BNG will synchronize its user session to the backup BNG. The synchronization is performed in a real-time manner so it assures that the fault protection does not break the service of online users. More details of the synchronization is described in clause 8.4.

Annex A

The scenarios related to BNG pool

(This annex forms an integral part of this Recommendation.)

This annex describes the scenarios related to the BNG pool.

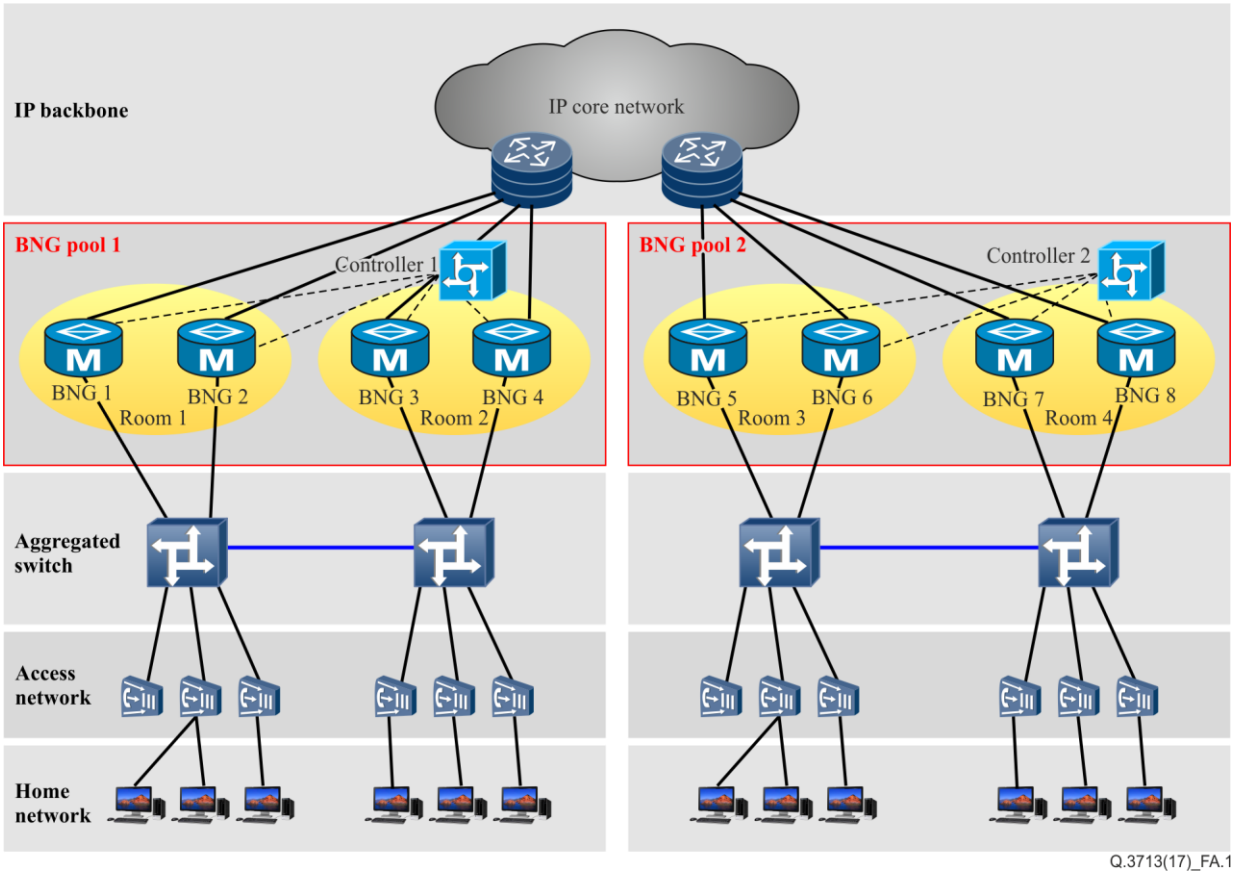

Figure A.1 – The scenario of BNG pool

As shown in Figure A.1, the BNG pool is composed of one controller and multiple BNG devices. Multiple BNG devices can be located in the same central office or different central offices, which are inter-connected by the underlay L2 network. BNG devices are deployed in a moderately centralized manner.

The controller acts as the centralized control unit of the BNG pool.

1) It manages the membership of the BNG pool and maintains the state of each member of the BNG pool.
2) It monitors the real-time load of each member of the BNG pool. Based on the overall load of the BNG pool, it realizes the load balancing among the members in the BNG pool.
3) It monitors the real-time state of each member of the BNG pool. It allocates BNG devices/ports into different backup groups and helps to synchronize the user access information among BNG devices within one backup group. Hence, the backup protection among the members in the BNG pool is realized.
4) It can configure each member of the BNG pool, and it is possible to perform OAM as a whole in the BNG pool.

5) It can receive the requirement from the application and provide differentiated functions for specific services/users.

The BNG devices act as the distributed unit to provide a variety of services and functions.

1) It provides broadband access services to users under the control of the controller.
2) It reports its own status/events/user session information to the controller.
3) It provides the backup service for other members of the BNG pool belonging to the same backup group under the control of the controller.

When the user accesses the broadband service through a member of the BNG pool and the corresponding port of the member is failed, the user's services can be transferred to another member of the BNG pool without awareness of the user. The members of the BNG pool can realize the resource sharing and load balancing.

With the BNG pool, it may have the following functions/benefits:

1) Simplifying the OAM.

   In the current network, user data (IP address, VLAN etc.) are planned in the unit of one BNG, which increases the complexity of the OAM. Whereas, with the BNG pool, user data can be planned and allocated in the unit of one BNG pool, which will greatly reduce the complexity of the OAM.

2) Achieving higher reliability and availability.

   It is possible for the members of the BNG pool to provide backup services among members of the BNG pool.

3) Achieving higher scalability.

   A BNG pool has the ability to provide the flexible resource extension to meet the increasing demands compared with the traditional single-rack mode. It can also improve the efficiency of physical resources due to the support of much more broadband users to access network.

4) Achieving the load balancing.

   The access requests of users can be distributed among members of the BNG pool with the granularity of user group. The granularity of user group is flexible, and can be based on the physical interface, the logical sub-interface, the VLAN, the MAC address, etc.

5) Saving the power consumption.

   When the network load is very low (e.g., at mid-night), on-line user's services can be centralized and migrated to one or a few members of the BNG pool. Other members of the BNG pool can be set in the sleeping mode. This can greatly save the power consumption.

Appendix I

The networking methods of BNG pool

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

This appendix describes the possible networking methods for members of the BNG pool.

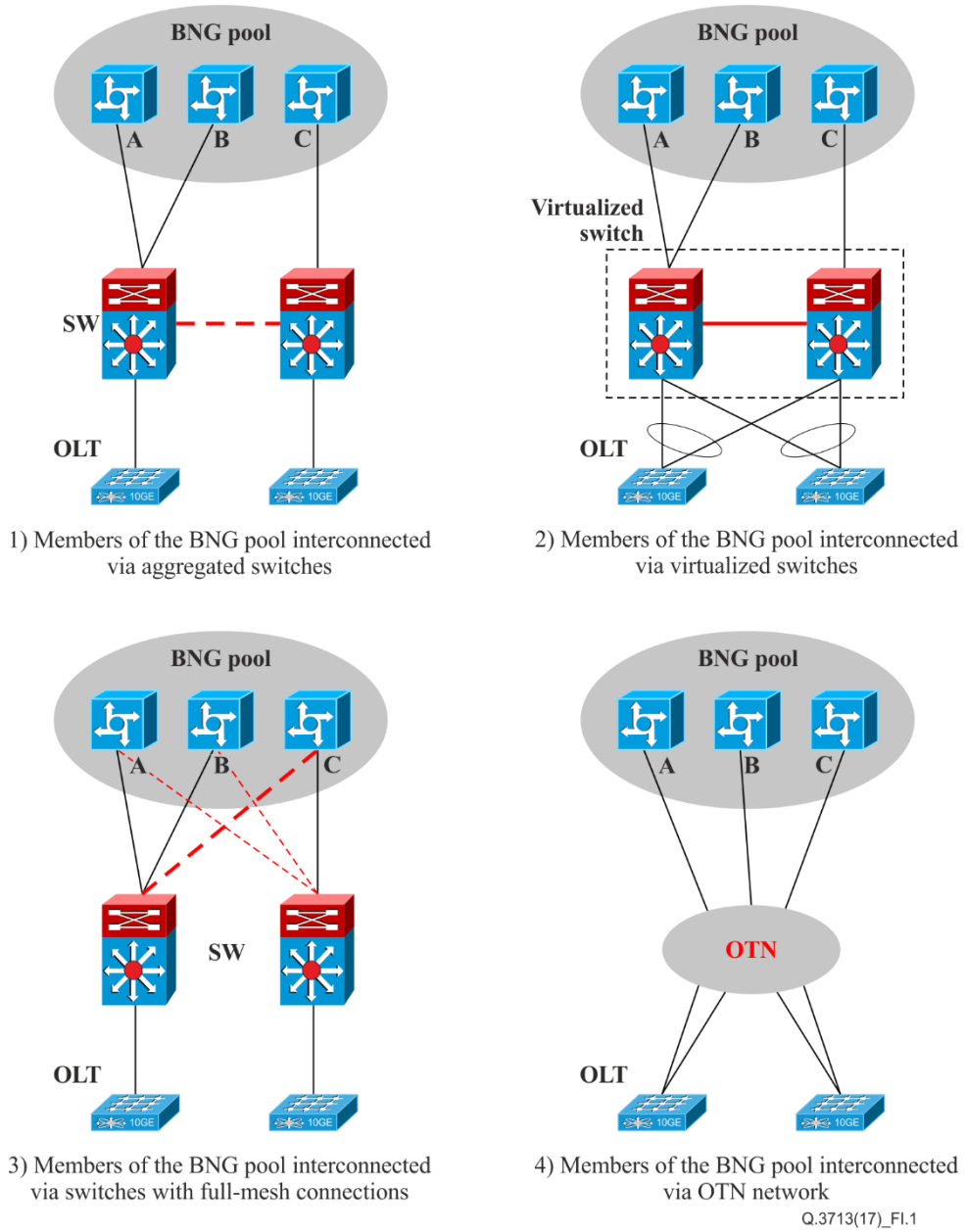

Figure I.1 – The networking methods for members of the BNG pool

The BNG pool is composed of multiple BNG devices from the same central office or different central offices. Members of the BNG pool are inter-connected by the underlay L2 network. The networking methods for members of the BNG pool can be classified by the following four types:

– Inter-connection via aggregated switches. The aggregated switches form an underlay layer 2 network by inter-connecting each other, and members of the BNG pool establish connections among them via the underlay layer 2 network. This networking method requires transmission resources among the aggregated switches.

– Inter-connection via virtualized switches. Multiple aggregated switches can be inter-connected and stacked into one virtualized switch. The optical line terminal (OLT) connects every physical switch directly, which forms a virtual trunk. Compared to the last scenario, multiple physical aggregated switches are virtualized into a logical switch and form a logical network topology.
– Inter-connection via switches with full-mesh connections. Each aggregated switch needs one link to connect each member of the BNG pool. This networking method will increase CAPEX, and require more transmission resources. However, such a full-mesh network topology does exist in the current carrier network.
– Inter-connection via the optical transport network (OTN). When the OTN is deployed between the BNG layer and the OLT layer, it will be an ideal networking method for the BNG pool. This mode can greatly reduce the consumption of transmission resources and device ports, and is the trend for the future network.

Of the above networking methods, the networking method based on the virtualized switch is recommended currently, since it has the advantages of the simplified logical network topology and OAM for aggregated switches. When the OTN network is deployed in the metro area in the near future, the networking method based on metro-OTN is recommended, since it can greatly reduce the consumption of transmission resources and device ports. However, other networking methods can also be considered based on the practical network resources.

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, 2017