International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3315

(01/2015)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

Signalling requirements for flexible network service combination on broadband network gateway

Recommendation ITU-T Q.3315

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

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.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	**Q.3300–Q.3369**
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for next generation networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3315

Signalling requirements for flexible network service combination on broadband network gateway

Summary

Recommendation ITU-T Q.3315 describes the signalling requirements, based on the service platform broadband network gateway (BNG) architecture, needed to achieve outstanding benefits like easy deployment of network services, fine grained network services, etc. This Recommendation covers the following three aspects for the signalling requirements:

1) network services combination/orchestration, i.e., the packet routes between network services

2) service configuration on the BNG

3) BNG resources, status and event notification to the service platform.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3315	2015-01-13	11	11.1002/1000/12417

Keywords

BNG, service chaining.

---

* 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

Introduction

Network services offered by carriers are far from adequate for the ever-changing requirements of Internet applications. As the key position to offer broadband network services, the broadband network gateway (BNG) should be able to support flexible service combination, new services introduction and provisioning. Carriers can then greatly improve their network service capability, bandwidth utilization and end user experience. Thus, the BNG will achieve the following outstanding benefits:

- easy deployment of network services, easing the strain of network updates;
- fine-grained network service handling and bandwidth utilization;
- greatly improved end user experience, based on the network services oriented to newly emerging network application techniques.

The service platform-BNG architecture is suitable for the feature requirements. The service platform is in charge of the BNG. Network services deploy on the service platform. The BNG acts according to the service platform's control information. The following three aspects are required for the features:

1) network services combination/orchestration, i.e., the packet routes between network services;
2) service configuration to the BNG;
3) BNG resources, status and event notification to the service platform.

Recommendation ITU-T Q.3315

Signalling requirements for flexible network service combination on broadband network gateway

1 Scope

This Recommendation describes the signalling requirements for the flexible network service combination on broadband network gateway (BNG). The signalling supports the service routing, service combination, service deployment and service provision on the BNG. This Recommendation focuses on the signalling between the service platform and BNG. Signalling above the service platform is out of scope of this Recommendation.

2 References

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 software-defined networking (SDN) [ITU-T Y.3300]: A set of techniques that enables users to directly program, orchestrate, control, and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 broadband network gateway (BNG): The access point to the provider's IP network for wireline broadband services.

3.2.2 chrysanthemum service route path: A route path in which every packet is transferred back to the original node from where it came when the network service handling is done.

3.2.3 hybrid service route path: A route path in which each packet is transferred either directly to the next network service for handling, or to the original node when the network service handling is done.

3.2.4 lily service route path: A route path in which each packet is transferred directly to the next node where network service is deployed for handling and it does not need to be transferred back to the original node.

3.2.5 service chaining: A technique of linking together simpler service-enabling elements in an intended order to create more complex services. The method of chaining may be composition, combination, etc.4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
A-RS-RSP	Automatic Resource Status Response
API	Application Programming Interface
BNG	Broadband Network Gateway
C-REQ	Configuration Request
C-RSP	Configuration Response
CHS-REQ	Chain Service Request
CHS-RSP	Chain Service Response
COA	Change of Authorization
CS-REQ	Create Service Request
CS-RSP	Create Service Response
DS-REQ	Delete Service Request
DS-RSP	Delete Service Response
MAC	Media Access Control
NMS	Network Management System
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RS-REQ	Resource Status Request
RS-RSP	Resource Status Response
SDK	Software Development Kit
SDN	Software-Defined Networking
SNMP	Simple Network Management Protocol
TLV	Type Length Value
UCHS-REQ	Unchain Service Request
UCHS-RSP	Unchain Service Response
US-REQ	Update Service Request
US-RSP	Update Service Response
VPN	Virtual Private 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 Architecture for the BNG with flexible network service combination

The BNG is divided into three layers, as depicted in Figure 1. The BNG is responsible for packet forwarding and policy enforcing, and keeps only the stable functions, such as routing process. The service platform acts as an intermediate layer between the network services and the BNG. The service platform provides application programming interfaces (APIs) for the network services deployed on it and delivers network service controls to the BNG. The frequently changing network services are decoupled from the BNG to the external service platform, and the frequently changing network services may be the ones that are related with service properties. Network service can be easily deployed on the service platform with the APIs provided by the service platform.

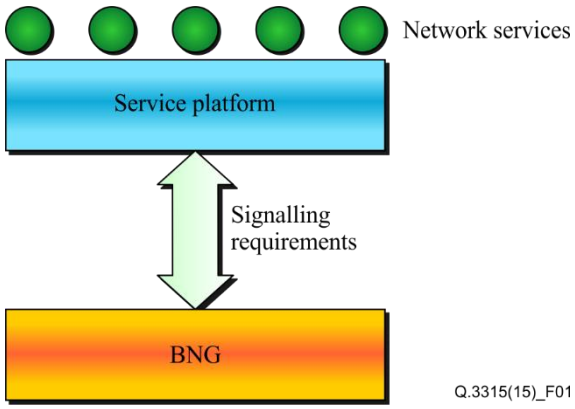

Figure 1 – Architecture for BNG with flexible network service combination

Network services control the BNG through the service platform and the BNG acts based on the action/commands from the network services. Packets will be processed in the intended sequence by the network services deployed on the service platform.

With this independent feature of the network services, the network services can be easily developed and deployed on the service platform. Moreover, the network services can be combined and chained flexibly to meet the service handlings on demand.

Signalling between the service platform and network services is not included in this Recommendation. Signalling between the service platform and the BNG is stressed in clause 7 and a concrete scenario of service and user awareness is illustrated in Annex D.

7 Signalling requirements of the BNG

7.1 Service route path, service combination and orchestration

The service platform should install the service route path to the BNG. Then packet(s) can be processed by the network services in the intended sequence. With the intended route path, service combination and orchestration on the BNG will be achieved.

The detailed scenarios and requirements are stated in Annex A.

7.1.1 Message types

As illustrated in Annex A, the service platform provides APIs/software development kits (SDKs). The services or the orchestration layer uses the APIs/SDKs for service chaining, service combination and orchestration. For the service management, the message types in Figure 2 should be followed.

As depicted in Figure 2, all the message interactions between the services platform and BNG are in request and response mode. The request messages may be for service creation, service deletion, service chaining, service unchaining and service updating. The response message contains the handling result of the corresponding requests and parameters to be returned to the service platform.

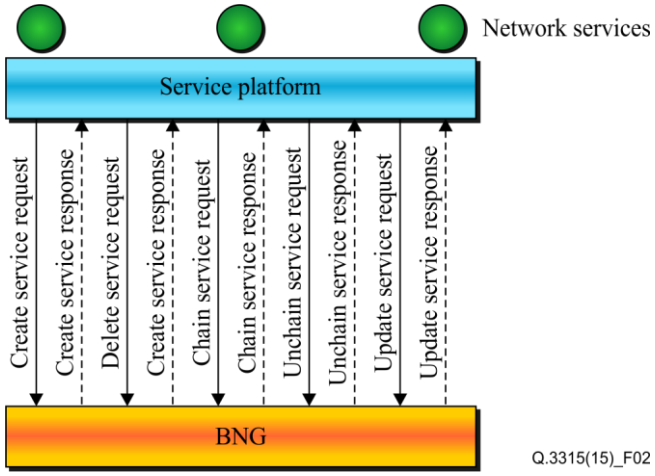

Figure 2 – Service management message types

Detailed descriptions of the message pairs are as follows:

1) Create service: used for setting up a service instance for a dedicated user flow. The functionalities of the service instance are specified by the parameters enclosed in the message. The response message for the create service shows the handling results, either success or failure. If it is successful, a service instance ID will be enclosed. The service instance ID can be used to fast index the service instance.

2) Delete service: used for deleting the service instance created by the create service message. The service instance can only be deleted when there is no flow steering into this service instance. The response message for the delete service message shows the handling result.

3) Chain service: used for steering the flow traffic across the service instances or the service nodes. Each service node can run multiple service instances with each one having its own service instance ID.

4) Unchain service: used for stopping the steering of flow traffic to the specified service.

5) Update service: used for updating the configurations of a specified service.

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

The signalling messages may be XML-based messages over (or carried by) TCP, UDP, SCTP, TLS, etc. All of the messages are in the message header and message body format.

The message header and message body format are described in Figure 3 as follows:

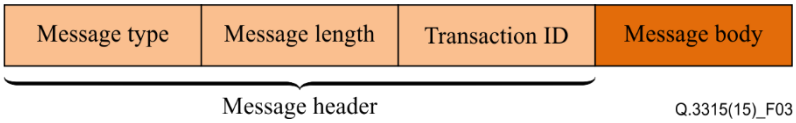

Figure 3 – Message composition

The message header field specifies the message types. The message body field contains the message contents.

The message header field should contain the following information:

1) Message type: uniquely specifies the type of the message;
2) Message length: specifies the length of the message body, which comes right after the message header;
3) Message transaction ID: generated by the sender of the message. If there is a response/reply message for the request message, the transaction IDs of the request and response/reply messages should be the same.

7.1.2 Message format

7.1.2.1 Create service request message and response message

The create service request (CS-REQ) message, indicated by the message type in the message header field, is sent by the services/service orchestrator to create a service instance.

Message format:

```
< CS-REQ-Message > ::= < Message header >
                       { Service-Platform-Id }
                       { BNG-Id }
                       { User-Id }
                      *{ Flow-Description }
                       { Service-Id}
                       { Service-Location }
                      *{ Service-Attribute }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `User-Id` uniquely identifies the user/application that created the service;
4) `Flow-Description` distinguishes the flows to be handled. This contains several fields from network flows. The flow description may be fields in the packet headers, and in some cases, the L4-7 information may be needed. There may be multiple flow descriptions items;
5) `Service-Id` uniquely identifies the service node, which provides the specified services;
6) `Service-Location` defines the location of the service node, so that the service platform can locate the service node;
7) `Service-Attribute` is used for the service attributes associated with the service node or the service instance. There may be multiple service attribute items.

The response message to the CS-REQ message is defined as the create service response (CS-RSP) message.

The CS-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform in response to the CS-REQ message.

Message format:

```
< CS-RSP-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                      { Result }
                     *{ Service-Instance-Id }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Result` shows the handling results of creating service instance;
4) `Service-Instance-Id` uniquely identifies the service instance created.

7.1.2.2 Delete service request message and response message

The delete service request (DS-REQ) message, indicated by the message type in the message header field, is sent by the services/service orchestrator to delete a service instance.

Message format:

```
< DS-REQ-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                      { Service-Instance-Id }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Service-Instance-Id` uniquely identifies the service instance to be deleted. The service instance is created by the CS-REQ message.

The response message to the DS-REQ message is defined as the delete service response (DS-RSP) message.

The DS-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform in response to the DS-REQ message. This message shows the handling results of the DS-REQ message.

Message Format:

```
< DS-RSP-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                      { Result }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Result` shows the handling result of deleting the service instance.

7.1.2.3 Chain service request message and response message

The chain service request (CHS-REQ) message, indicated by the message type in the message header field, is sent by the services/service orchestrator to chain up services, i.e., to steer flow traffic to the specified service handlers.

The CHS-REQ message may program the BNG to steer the traffic going out of its egress port to the ingress port of the service node. The service instance sends the flow through the egress port of the service node after the service instance handlings.

Message format:

```
< CHS-REQ-Message > ::= < Message Header >
                        { Service-Platform-Id }
                        { BNG-Id }
                        { User-Id }
                       *{ Flow-Description }
                        { Service-Id }
                        { Service-Location }
                        { Service-Instance-Id }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `User-Id` uniquely identifies the user/application that created the service;
4) `Flow-Description` distinguishes the flows to be handled. This contains several fields from network flows. The flow description may be fields in the packet headers, and in some cases, the L4-7 information may be needed. There may be multiple flow descriptions fields;
5) `Service-Id` uniquely identifies the service node that provides the specified services;
6) `Service-Location` defines the location of the service node, so that the service platform can locate the service node;
7) `Service-Instance-Id` is optional. If the service instance ID is not provided, it means that only one service instance is running in the service node.

The response message to the CHS-REQ message is defined as the chain service response (CHS-RSP) message.

The CHS-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform in response to the CHS-REQ message.

Message Format:

```
< CHS-RSP-Message > ::= < Message Header >
                        { Service-Platform-Id }
                        { BNG-Id }
                        { Result }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Result` shows the handling result of chaining up services.

7.1.2.4 Unchain service request message and response message

The unchain service request (UCHS-REQ) message, indicated by the message type in the message header field, is sent by the services/service orchestrator to unchain the service chains set up by CHS-REQ message, i.e., stopping steering flow traffic to the specified service handlers.

Message format:

```
< UCHS-REQ-Message > ::= < Message Header >
                        { Service-Platform-Id }
                        { BNG-Id }
                        { User-Id }
                       *{ Flow-Description }
                        { Service-Id }
                        { Service-Location }
                        { Service-Instance-Id}
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `User-Id` uniquely identifies the user/application that created this service;
4) `Flow-Description` distinguishes the flows to be handled. This contains several fields from network flows. The flow description may be fields in the packet headers, and in some cases, the L4-7 information may be needed. There may be multiple flow descriptions fields;
5) `Service-Id` uniquely identifies the service node that provides the specified services;
6) `Service-Location` defines the location of the service node, so that the service platform can locate the service node;
7) `Service-Instance-Id` is optional. If the service instance ID is not provided, it means only one service instance is running in the service node.

The response message to the UCHS-REQ message is defined as the unchain service response (UCHS-RSP) message.

The UCHS-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform in response to the UCHS-REQ message.

Message format:

```
< UCHS-RSP-Message > ::= < Message Header >
                        { Service-Platform-Id }
                        { BNG-Id }
                        { Result }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Result` shows the handling result of unchaining services.

7.1.2.5 Update service request message and response message

The update service request (US-REQ) message, indicated by the message type in the message header field, is sent by the services/service orchestrator to update the attributes of the service nodes or service instances.

Message format:

```
< US-REQ-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                      { Service-Id }
                      { Service-Location }
                      { Service-Instance-Id }
                     *{ Service-Attribute }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Service-Id` uniquely identifies the service node, which provides the specified services;
4) `Service-Location` defines the location of the service node, so that the service platform can locate the service node;
5) `Service-Instance-Id` is optional. If the service instance ID is not provided, it means only one service instance is running in the service node;
6) `Service-Attribute` is used for the service attributes associated with the service node or the service instance. There may be multiple service attribute items.

The response message to the US-REQ message is defined as the update service response (US-RSP) message.

The US-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform in response to the US-REQ message.

Message format:

```
< US-RSP-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                      { Result }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;
2) `BNG-Id` uniquely specifies the BNG element;
3) `Result` shows the handling result of updating service attributes.

7.2 Service configuration on the BNG

7.2.1 Message types

The service platform needs to configure the BNG. This is a basic requirement of the services, as well as the openness of the BNG functionalities and capabilities. The detailed scenarios and requirements are stated in Annex B.

The message types for the service configuration on the BNG are depicted in Figure 4.

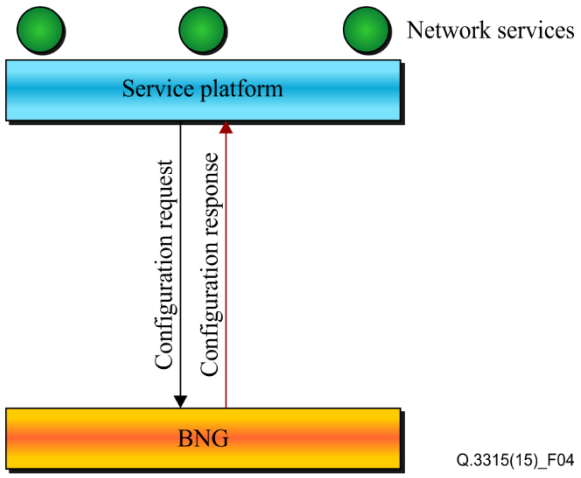

Figure 4 – Service configuration message types on BNG

As illustrated in Figure 4, services on the service platform may have multiple configurations on the BNG. The configuration message follows the request and response pairs, and the response message is optional.

For the two messages:

1) Configuration request: this message is used for conveying the service's configurations;

2) Configuration response: this message is used by the BNG for confirming the service's configurations. This message is optional. The services can configure the BNG to set its option.

The service configurations on the BNG are executed in the configuration request/response mode, and the response is optional. For the message mode, two message types are defined. The services use the configuration request (C-REQ) message to send the configurations to the BNG. The BNG sends the configuration response (C-RSP) message to notify the services whether the configuration(s) have/has been handled correctly or not.

The message composition of C-REQ and C-RSP is the same as clause 7.1.1, which is illustrated in Figure 3.

7.2.2 Message format

7.2.2.1 Network service configuration message

The network service configuration message is defined as the C-REQ message.

For either the static configurations or the runtime configurations, in the view of the message composition, there is no difference.

All of the service configurations from the service platform to the BNG follow the format of the C-REQ message.

The C-REQ message, indicated by the message type in the message header field, is sent by the services deployed on the service platform to configure the BNG.

Message format:

```
< C-REQ-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                     *{ Configuration-Type-Id }
                     *{ Configuration-Value }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;

2) `BNG-Id` uniquely specifies the BNG element;

3) `Configuration-Type-Id` uniquely specifies the type of each configuration within this C-REQ message;

4) `Configuration-Value` is a length variable field. This field contains the parameters for the configuration specified by the `Configuration-Type-Id`. If multiple configuration parameters are needed, the configuration value field is organized as type length values (TLVs). The TLVs are highly configuration type and content dependent.

7.2.2.2 Configuration response message

The configuration response message is defined as the C-RSP message.

The configuration message follows the C-REQ/C-RSP message mode, and the C-RSP message is optional.

By default, the BNG sends the C-RSP message to the service platform. The service platform can use the C-REQ message to set the BNG to send the C-RSP messages or not.

The C-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform to indicate whether this configuration is enforced to the BNG correctly or not.

Message format:

```
< C-RSP-Message > ::= < Message Header >
                      { Service-Platform-Id }
                      { BNG-Id }
                     *{ Configuration-Type-Id }
                     *{ Configuration-Result }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;

2) `BNG-Id` uniquely specifies the BNG element;

3) `Configuration-Type-Id` uniquely specifies the type of each configuration within this C-REQ message;

4) `Configuration-Result` is used to indicate the configuration result for the C-REQ message, which is specified by the other parameters in this message.

7.3 BNG resources, event and status notification to the service platform

The resources, events, status, network service status, etc. may need to be reported to the service platform.

Scenarios and requirements of BNG event and status notification to the service platform have been stressed in Annex C. As stated in Annex C, the three main types of events or statuses, such as resource notifications, failure or faults notifications, and statistics notifications should be reported to the service platform.

7.3.1 Message types

The network application or the service platform may need to know the resources in the BNG element. The enquiry of the BNG's resources is processed in the request and response mode. The service platform sends the resource status request (RS-REQ) message to the BNG and the BNG responds with the resource status response (RS-RSP) message.

In some cases, resource notifications or resource changes should be sent to the service platform automatically by the BNG. The RS-REQ message is used to indicate the resources to be automatically notified to the service platform. The BNG sends the automatic resource status response (A-RS-RSP) message to the service platform for the automatic resource notifications.

The three messages are illustrated in Figure 5.

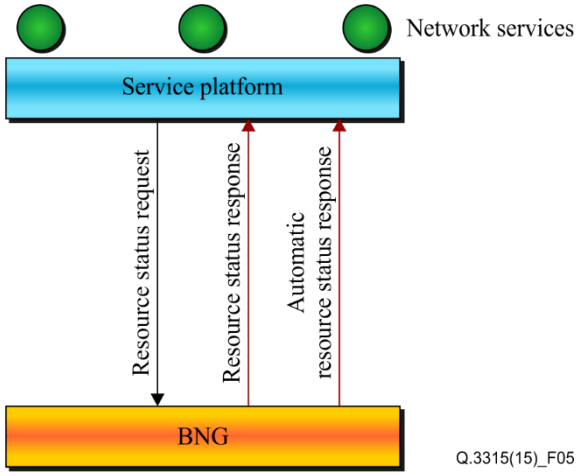

Figure 5 – Messages types for the BNG resource, events and status notifications

The message composition of RS-REQ, RS-RSP and A-RS-RSP is the same as clause 7.1.1, which is illustrated in Figure 3.

7.3.2 Message format

7.3.2.1 Resource status request message

The resource status request message is defined as the RS-REQ message.

The RS-REQ message, indicated by the message type in the message header field, is sent by the service platform to the BNG in order to get the resource status of the BNG.

Message format:

```
<RS-REQ-Message> ::= < Message Header >
                     { Service-Platform-Id }
                     { BNG-Id }
                    *{ Resource-Type-Id }
                    *[ Resource-Parameter-Id ]
                    *[ Auto-Resource-Type-Id ]
                    *[ Auto-Resource-Parameter-Id ]
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;

2) `BNG-Id` uniquely specifies the BNG element;

3) `Resource-Type-Id` uniquely specifies the type of resources enquired by the service platform;

4) `Resource-Parameter-Id` is optional. Some of the resources may need this ID to specify the intended resources. One possible example would be the port number (or ID) of the designated port;

5) `Auto-Resource-Type-Id` uniquely specifies the type of resources reported to the service platform by BNG. Auto means the BNG will automatically report the specified resources to the service platform in case of changes;

6) `Auto-Resource-Parameter-Id` is optional. Some of the resources may need this ID to specify the intended resources. One possible example would be the port number (or ID) of the designated port. Auto means the BNG will automatically report the specified resources to the service platform in case of changes.

7.3.2.2 Resource status response message

The resource status response message is defined as the RS-RSP message.

The RS-RSP message, indicated by the message type in the message header field, is sent by the BNG to the service platform in response to the RS-REQ message.

Message format:

```
<RS-RSP-Message> ::= < Message Header >
                     { Service-Platform-Id }
                     { BNG-Id }
                    *{ Resource-Type-Id }
                    *[ Resource-Parameter-Id ]
                    *{ Resource-Status-Value }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;

2) `BNG-Id` uniquely specifies the BNG element;

3) `Resource-Type-Id` uniquely specifies the type of resources enquired by the service platform;

4) `Resource-Parameter-Id` is optional. Some of the resources may need this ID to specify the intended resources. One possible example would be the port number (or ID) of the designated port;

5) `Resource-Status-Value` is used for describing the status of the resources specified by `Resource-Type-Id`.

7.3.2.3 Automatic resource status response message

The automatic resource status response message is defined as the A-RS-RSP message.

The A-RS-RSP message, indicated by the message type in the message header field, is automatically sent by the BNG to the service platform in order to notify resource notifications or resource changes.

Message format:

```
< A-RS-RSP-Message> ::= < Message Header >
                        { Service-Platform-Id }
                        { BNG-Id }
                       *{ Resource-Type-Id }
                       *[ Resource-Parameter-Id ]
                       *{ Resource-Status-Value }
```

Meanings and explanations:

1) `Service-Platform-Id` uniquely specifies the service platform;

2) `BNG-Id` uniquely specifies the BNG element;

3) `Resource-Type-Id` uniquely specifies the type of resources enquired by the service platform;

4) `Resource-Parameter-Id` is optional. Some of the resources may need this ID to specify the intended resources. One possible example would be the port number (or ID) of the designated port;

5) `Resource-Status-Value` is used for describing the status of the resources specified by `Resource-Type-Id`.

Annex A

Scenarios related to flexible network service combination on BNG

(This annex forms an integral part of this Recommendation)

A.1 Scenarios of the service route path

Network services are deployed on the service platform. A packet goes through the BNG and network service in the intended order for service handling. The intended order of the service handling is called the service route path. The service route path is mainly determined by the following key elements:

1) the relationship among the network services;

2) the interactions between the network service and BNG.

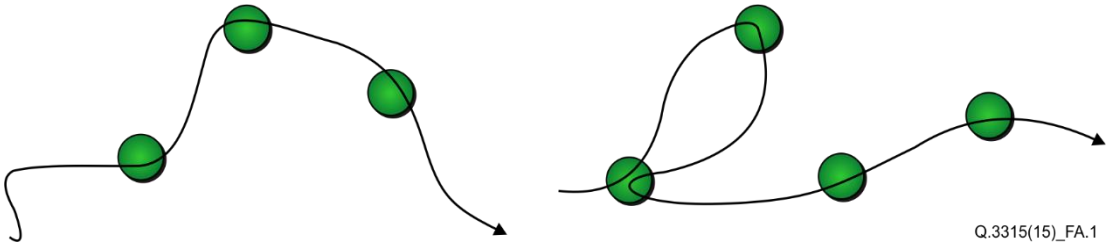

Figure A.1 – Example of packet processing by network services

As depicted in Figure A.1, the packets are processed by the network services one by one. The way the packet is switched to the next network service for processing should be standardized. Three service route path scenarios are introduced in this Annex.

A.1.1 Chrysanthemum service route path

To simplify the network service design, the decision of the network service processing order for a packet is determined by the BNG.

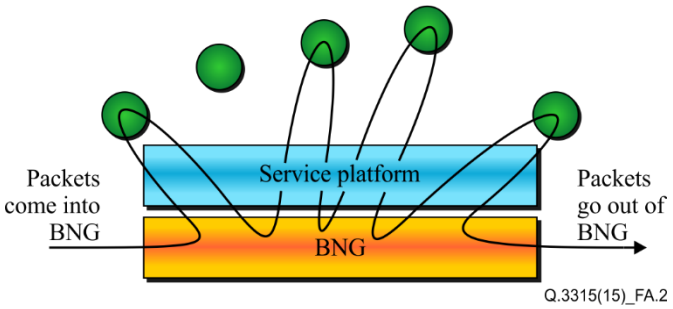

Figure A.2 – Scenario of Chrysanthemum service route path

As depicted in Figure A.2, the decision about which network service a packet should go to is made by the BNG. The decision is made only in a single node. Every packet goes back to the original node from where it came when the network service handling is done. As the service route path looks like the shape of a chrysanthemum, it is called the Chrysanthemum service route path.

In the Chrysanthemum service route path scenario, the network service does not need to know the next handling network services for the packet. Each network service only focuses on service specific handling and is not coupling with other network services.

The BNG as a central node chains all the network services.

One possible scenario of this kind of service route path is the video caching system. First, the video caching network service identifies the video caching server in which the intended video is cached.

Then this information associated with the packet is sent back to the BNG. Finally, the packet is redirected to the video caching server.

A.1.2 Lily service route path

Some network services are highly coupled with each other or have the ability to specify the next network service for this packet handling.

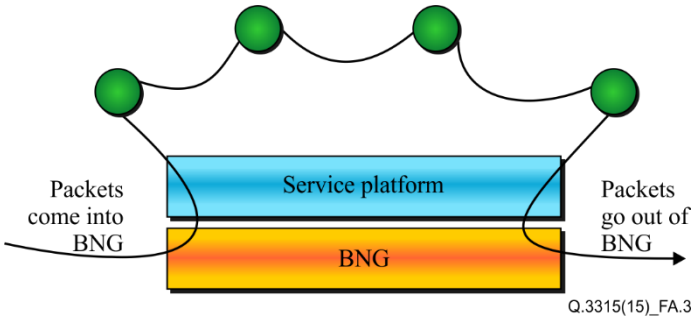

Figure A.3 – Scenario of Lily service route path

As depicted in Figure A.3, the decision about which network service a packet should go to is made by the network service itself. Each packet goes directly to the next network service for handling and it does not need to go back to the BNG. The packet should contain a certain flag for specifying the route path. As the service route path looks like the shape of a lily, it is called the Lily service route path.

In the Lily service route path scenario, each network service should have the ability to route a packet to the next destination. Certain message, information or metadata should be conveyed between network services.

The service route path is chained together by multiple network service nodes.

One possible scenario of this kind of service route path is the parental control network service. Suppose the parental control network service is composed of two smaller network work service entities, the URL filtering network service and the HTTP redirect network service. After the URL filtering network service's handling, the permit or deny information with the packet is handed directly to the HTTP redirect network service. With the permit or deny information, the HTTP redirect network service will make the judgement, and finally redirects the packet to the blocking page in case it is not permitted, otherwise to the web server specified.

A.1.3 Hybrid service route path

The hybrid service route path combines the Chrysanthemum service route path with the Lily service route path when needed.

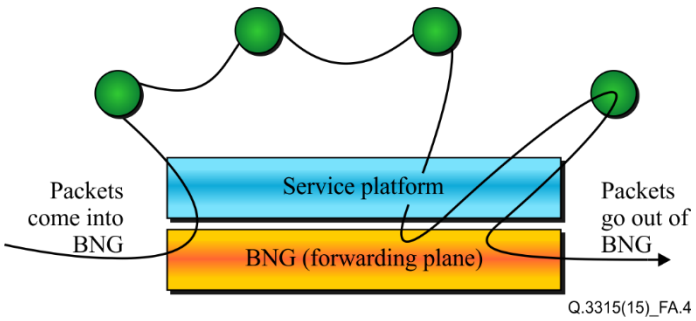

Figure A.4 – Scenario of Hybrid service route path

As depicted in Figure A.4, some network services can specify the next process destination of a packet and some network services need the BNG to specify the next processing destination of a packet. This

then becomes a hybrid service route path by combining the Lily service route path and Chrysanthemum service route path.

The service route path is chained together by the central node (i.e., BNG) and distributed to multiple network service nodes.

One possible scenario of this kind of service route path is a combination of the scenarios from clauses A.1.1 and A.1.2. When the parental control network service and video caching network service are deployed simultaneously, the hybrid service route path is needed.

A.2 Requirements of the network service combination

The service platform may consist of some basic network service handling entities, which are called service atoms. The service atom has its unique, integral and undivided network service functionality.

The service atoms within the service platform form the service atom base. By combing or linking one or more service atoms, a new network service will be created. The newly created network service may be viewed as a new service entity, which may be part of much more complicated network services. See Figure A.5.

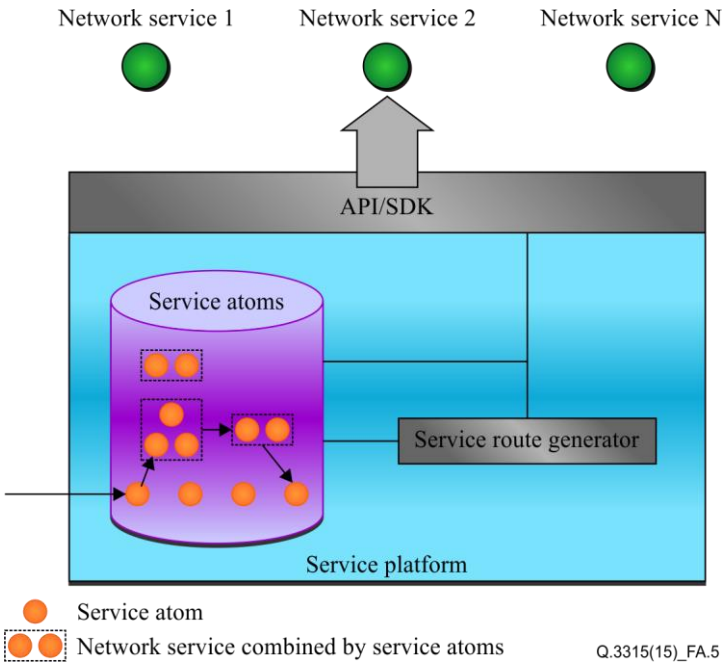

Figure A.5 – Service atoms in the service platform

The service atom or service atoms combined together provides open APIs or SDKs to the network services deployed on the service platform. Based on the APIs or SDKs, network services can easily use the already existing service handling routine provided by the service atoms. The network service may also combine its own handling with the service atoms, thus providing the intended service handling. With these features, an open environment is provided for the ease of network service provisioning. Eventually, new technologies, adoption requirements and fast-to-market requirements of network service will be satisfied.

Based on the network services request, the orchestrator in the service platform combines the service atoms to generate the service intended. The scenario of how the service atoms are combined or linked together is the same as the description in the previous clause, just like the way the network services are chained up, i.e., the service route path.

For the network service combination, three types are needed and described in the following clauses.

A.2.1 New network service creation

By combining or linking the service atoms, network service with intended functionalities will be generated. The network service creation request should provide the information about the service atoms needed and the service route path.

For the most part, one service atom may have more than one linkage to other service atoms. Then the service route path information should also include the linkage selection information, the condition, and next service atoms.

A.2.2 Network service modification

In some uncommon cases, the generated network services need some modifications. For example, adding/deleting some new features, changing the service handling sequences, etc.

For the modification information, the network service ID, added/deleted service atoms and service route path are all needed.

A.2.3 Network service deletion

If a network service is no longer needed, it should be deleted. Then the service atoms will be able to be released and reused.

For the deletion, only network service ID is needed.

Annex B

Scenarios and requirements of network service configuration on BNG

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

This annex describes some scenarios related to flexible network service combination on BNG.

B.1 Scenarios and requirements of the network service configuration on BNG

Network services all have different ways of packet handling. Different kinds of BNG functionalities are needed by different kinds of network services.

Through the service platform, the network services enforce the functionalities required on BNG. At the same time, the network services may also enforce their configuration on the service platform.

Most of the configurations fall into either the static configuration or the runtime configuration. The following two clauses elaborate these in detail.

B.1.1 Static network service configuration on BNG

Mostly, the static configurations needed by a network service are pre-installed on the BNG before the network service totally runs up. The static configurations mainly include the following:

1) Resource management:

   The resource includes physical resources as well as logical resources, which may be ports, queues, bandwidth, link-utilization, etc.

2) Network service handling configuration:

   The service platform may include some basic network service handling entities, which are called service atoms. For the network service composed of the service atoms, some rules/policies may be needed by the service atoms. Then the network service handling configuration is just for these. One possible example would be the URL filtering service atom, which is aimed to filter out and stop the forbidden URL visiting based on black/white URL lists. The default black/white URL lists are setup by the configuration. Some runtime configurations are also needed.

3) BNG behaviours management:

   The BNG may behave either in the legacy network forwarding manner or in the software defined-networking (SDN)/OpenFlow forwarding manner. Or the BNG may behave with both of the two, in the hybrid manner. This main behaviour should be configurable in all levels of granularities, such as per port, per line card, per chassis, entire network device, etc. Additional behaviours may include topology discovery enabling or disabling, link monitoring enabling or disabling, statistics enabling or disabling, etc. The BNG behaviour configuration should be able to enable or disable these functionalities.

The static configurations may be done in the following ways:

1) by the operators/managers of the networks services;
2) by the networks service itself at initialization stage;
3) by the combination of the operators/managers and network service itself.

B.1.2 Runtime network service configuration on BNG

The runtime configurations are highly network service type and runtime packet relative. Some of the runtime network service configurations are in the same range with the static configurations, the only difference is whether the configuration is pre-determined or not.

Runtime configuration scenarios may be one of the following:

1) Service route path configuration:

   Service atoms chain up the network services. Network services may extend or shrink service functions by adding or deleting service atoms based on user-defined requirements.

2) Packet handling action configuration:

   Network services may enforce different kinds of actions on the packet received. The actions may be dropping the packet, redirecting the packet to some service-handling servers, specifying the forwarding path of the packet, modifying some fields of the packet, etc.

3) Other configurations:

   This may overlap with the static configurations. The runtime configurations are not the predetermined defaults.

Annex C

Scenarios and requirements of BNG event and status notification to the service platform

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

C.1 Scenarios and requirements of BNG event and status notification to the service platform

Network services and the service platform have the requirement of knowing what is happening in the BNG. Based on the running status of the BNG, network services do their specific service handing.

The event and status notifications to the service platform may be reported in a reactive or proactive way. In the reactive way, only when the request from the service platform is received, will the BNG send the notifications. On the other hand, in the proactive way, the BNG keeps on sending the notification to the service platform whether it is requested or not.

The event and status notification are categorized into three types: resource notifications, failures/faults notifications, and statistics notifications. The following clauses elaborate each of these in detail.

C.1.1 Resource notifications

Resources within the BNG are composed of general resources of IT, such as CPU, RAM, storage, etc. As a network entity, BNG resources include ports, bandwidth between the BNG and service platform, capacity of forwarding rules, line-card forwarding speed, capacity of access users, etc.

Most of the time, these resources remain the same. Resource notification only needs to be reported to the service platform once.

These notifications properly fall into the reactive way.

C.1.2 Failure/faults notifications

The failure/faults are of all levels of BNG malfunctions, such as port down or up, link down or up, unsupported rules, exceeding the capacity, line-card dump, etc. All these events are essential to specific network services.

For example, the link down or up notifications are crucial to the network topology discovery service. Based on the notification, the topology can be closely in accordance with the real network topology.

The failure and faults should to be handled promptly, and then these notifications should be in the proactive way.

C.1.3 Statistics notifications

The BNG acts according to the actions from the service platform and network services. The BGN can be configured to do some statistics. The statistics may include port rate, bandwidths consumed, link utilization, current CPU usage, percentage of forwarding rules consumed, etc.

When the BNG receives the statistics requests, and in case this kind of statistics are enabled by the configuration, the statistics will be reported to the service platform or the network service.

The statistics notifications are sent to the service platform only when they are requested. This is the reactive way.

Annex D

Signalling requirements of service/user awareness and control

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

D.1 Introduction

Smart pipe is the evolution target for the telecom operators' network, as it can have more powerful control on network resources and provide differentiated services based on customers' demands. Based on smart pipe technology, operators can reduce network construction costs by efficiently utilizing their network resources and can increase their income by providing differentiated services for customers.

To build smart pipe, the key point is that the network can detect and differentiate services and users from network flows, and can then allocate appropriate network resources for different users/services based on some control policy. BNG is the important network device to perform service/user detection and control, as it is the access point of broadband users/services.

It is important to study how to apply service/user detection and control under such architecture and what are the corresponding signalling requirements.

D.2 Descriptions

BNG can provide the functions of user traffic analysis, service detection and dynamic control through the interface between BNG and the service platform. Through service/user detection, BNG can divide user traffic into different virtual pipes based on some criteria (e.g., service type, user type, TCP/IP port) and then allocate resources and provide static/dynamic quality of service (QoS) guarantee for these virtual pipes.

The BNG resources should not only include traditional QoS resources, but all the resources which are possibly allocated in a differentiated manner, so that the network can provide differentiated services to users according to users' demands.

The BNG resources might include (but are not limited to):

1) The resources in BNG, including:
   a) QoS queues and cache resources in line cards of BNG;
   b) port bandwidth resource;
   c) scheduling resources in switching queues of BNG;
   d) controllable and revisable resources related to network address translation (NAT)/deep packet inspection (DPI)/Firewall functions;
   e) tunneling control resources.
2) The resources in control plane of BNG, including:
   a) volume of routing table and virtual private network (VPN) routing table;
   b) user management related resources;
   c) volume of tunneling users;
   d) media access control (MAC) table volume of layer 2 (L2) switch and L2 VPN;
   e) bandwidth/number/priority of signalling session of network protocols.

The BNG can report the information of the above resource consumption situation to the service platform. The service platform allocates the appropriate resources to different users according to users' demands, resource consumption situations and the control policy. The allocation result can be distributed to the BNG through the control policy distribution/communication interface.

The functions and signalling requirements of BNG related to service/user detection/control may include:

1) User access and information reporting:
   a) user access function: BNG should support access of broadband users with point to point protocol over Ethernet (PPPoE), IP over Ethernet (IPoE), layer 2 tunnelling protocol (L2TP), L2VPN/layer 3 VPN (L3VPN), etc.;
   b) user information reporting to the service platform: BNG should support reporting of the information of user identification to the service platform. The service platform can save the user identification, which will be useful when performing service/user policy control.
2) Reporting of traffic statistics and BNG capability: BNG can calculate the statistics of different user/service traffic and report the information to the service platform. BNG should also report its capability, resources, and status to the service platform.
3) Policy control related communication interface:
   a) open communication interface: BNG should support multiple protocols to distribute control policy from the service platform, e.g., remote authentication dial in user service (RADIUS) change of authorization (COA), Diameter, simple network management protocol (SNMP), OpenFlow;
   b) supporting policy control protocol: BNG can interpret different policy control protocols and translate to control policies, which will be used for user/service control.

Figure D.1 shows the user/service control procedure. The BNG will report its traffic statistics, capability and status periodically to the service platform. After the user finishes the dial-up process between user and BNG, BNG will report the user identification information to the service platform. Then the service platform will distribute the initial control policy for that user to the BNG. The BNG will allocate the appropriate resources for the user and perform control. If the user demands to change its user/service policy (e.g., increasing priority to get QoS guarantee with more payment), it can send a request through some application (e.g., the portal provided by operator). The application can forward the request to the service platform. Then the service platform will update the control policy for that user/service and distribute the new policy to the BNG. Then the BNG will re-allocate the necessary resources and perform corresponding control.

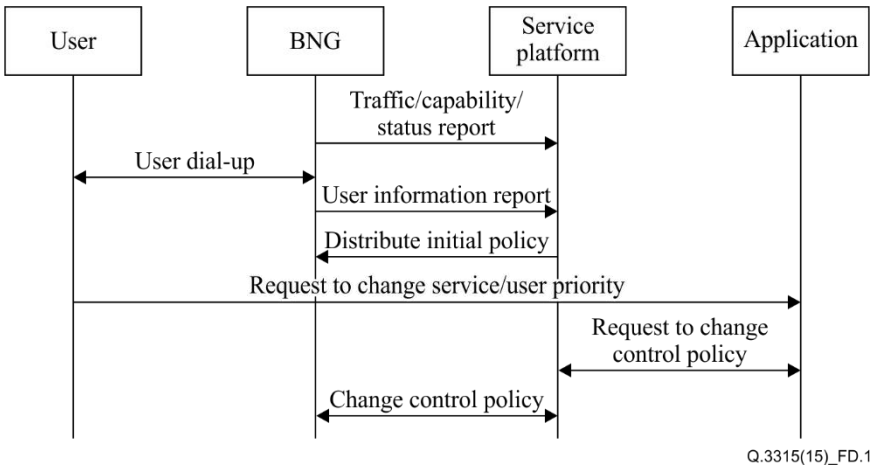

Figure D.1 – Service/user control procedure

Functions and signalling requirements related to service/user detection/control can be studied from the following perspectives, including:

1) user access and information reporting;
2) reporting of traffic statistics and BNG capability;

3) policy control related communication interface, etc.

D.2.1 Signalling requirements for user information report

The BNG can provide the functions of user traffic analysis, service detection and dynamic control through the interface between the BNG and the service platform. When the user finishes the dial-up process, the BNG will report the user identification information to the service platform. Then the service platform will distribute the initial control policy for that user to the BNG. The BNG will allocate the appropriate resources for the user and perform control.

For user information reports, the BNG usually needs to report BNG information and user identification information for BNG and user network information to the service platform:

1) The BNG information could include address information and BNG ID, which can be used to find the BNG by the service platform when it distributes the control policy;
2) The user network information is used to identify the user in the network. The user network information is known to the service/application. When the service/application wants to request policy control for a user, the service/application will send the user network information to the service platform, and the service platform will acquire the user identification information according to the user network information;
3) The user identification information for the BNG is used for policy control. The service platform will distribute the control policy with the user identification information to the BNG, then the BNG will perform control according to the user identification information.

The user network information could include:

1) user IP address or sub-network information;
2) public IP address and port range of NAT;
3) layer 2 information, e.g., MAC address;
4) user VPN information.

The user identification information could include:

1) user accounting ID information;
2) user IP address or sub-network information;
3) layer 2 information, e.g., MAC address;
4) user layer 2 or layer 3 VPN information;
5) user ID generated by BNG.

Most user network information and user identification information can be supported by current policy distribution protocols (e.g., RADIUS, Diameter, common open policy service (COPS)). However, some information might need to be supported by extending current protocols.

The following user related information could be considered to be included in the user information report from BNG to the service platform:

- user network information;
- user identification information (for BNG);
- BNG address information and BNG ID.

D.2.2 Requirements for traffic statistics and BNG capability reporting

The reported information should support accounting for users. The service platform and BNG should support the generation of accounting information and interact with authentication, authorization and accounting (AAA) servers through RADIUS or Diameter protocols. Accounting information can be generated based on user traffic volume or online time. The BNG needs to monitor the available traffic volume or online time for users. The service platform and the BNG also need to support smart

accounting functions, e.g., accounting according to QoS policy, application type, destination address, busy/idle time, and content type.

To support the above accounting functions, BNG needs to report all the user traffic information to the service platform, which can include user identification information, destination address, service type, content type, QoS policy, accumulated used traffic volume, online time, busy/idle time, etc.

The BNG needs to support reporting network or user traffic related events to the service platform. Such events can be pre-defined by the service platform. If the event is important, it also should be reported even if it is not subscribed. The BNG needs to report the events subscribed by the service platform, e.g., when user's accumulated online time or traffic is up to the threshold, or user's online time or traffic for visiting specific website is up to the threshold. BNG also needs to report network or user session related events, e.g., network abnormal situation, network congestion, and user offline.

D.2.3 Requirements for control policy distribution/communication interface

Usually the service platform can distribute the control policy to BNG through RADIUS COA, Diameter, COPS, or other more open protocols.

The control policy can include the following two parts:

1) target user, i.e., user identification information, which indicates the target user/flow for performing control;
2) execution policy, which indicates the detailed control action for the target user by the BNG. It is composed of two components. One is the mapping rule, which can filter the target user/service traffic from the network traffic. The other is the control action, which defines how to control the target user/flow.

When the BNG receives the control policy, the process is as follows:

1) finding the target user/service through the user identification information contained in the received control policy;
2) picking up the target traffic to form a virtual pipe according to the user identification information and the mapping rule contained in the control policy;
3) performing the control action on the virtual pipe according to the policy.

The control policy can be distributed in a static or dynamic way.

For the static configuration mechanism, the control policy can be pre-distributed to the BNG and statically configured. The target user of control policy for static configuration can be physical interface or virtual interface, one domain of authenticated users, tunnel, pseudowire (PW), and sessions.

For the dynamic policy configuration mechanism, the control policy can be distributed to the BNG dynamically in the runtime by the service platform. The distribution is through the policy control related communication interface, which can support RADIUS COA, Diameter, COPS, or other more open protocols.

All the control policies can be pre-installed in the BNG, so that the service platform can only distribute the name of the control policy and the target user identification information to the BNG. The BNG can acquire the policy content from BNG policy database according to the policy name.

If the policy control related communication interface can support more open protocols, the service platform can distribute the detailed content of the control policy to the BNG, and the BNG can generate the execution policy according to the received content of control policy. Then the BNG can find the target user/flow according to the user information, and perform execution control policy.

The dynamic distribution of control policy is usually triggered by some pre-defined conditions, which may include:

1) user trigger;

2) other device trigger;

3) network management system (NMS) trigger.

For user trigger, the operators can provide such pages/functions in the portal to allow users to order and modify the smart policy. When the user modifies the policy, the distribution of new control policy is automatically triggered by the service platform and distributed to the BNG.

The BNG can also provide smart user traffic monitoring function with some user traffic monitoring and analysis device, which can be line card/mode for service monitoring within the BNG. The BNG can monitor and analyse the real-time user traffic. When the user traffic meets the pre-defined condition, the BNG will notify the service platform. Then the service platform can push portal pages to the user side by the way of re-direction. The user can know the statistics of its service traffic and order/modify the pipe policy to enhance the service quality. After the user order/modify the control policy, the distribution of new control policy will be automatically triggered.

Other devices can also possibly trigger the modification of control policy. Suppose the BNG works together with individual CGN or DPI devices. When the CGN or DPI device finds user traffic abnormal, it can inform the service platform. The service platform can choose the appropriate control policy and distribute to the BNG. The user traffic might be limited, and the user will be notified through portal page pushing technology.

The service platform/BNG can also receive the configuration commands from the NMS through SNMP or other protocols, and the new control policy will be accordingly generated and distributed.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015