Proposal of Functional Exchange Networking for Distributing Data Services across Multiple Network Generations

Shuichi Okamoto, Michiaki Hayashi, Nobutaka Matsumoto and Kosuke Nishimura
KDDI R&D Laboratories, Inc.
Saitama, Japan
e-mail: {okamoto, mc-hayashi, nb-matsumoto, nish}@kddilabs.jp

***Abstract*—Continuous evolutions of network management and control technologies are producing a variety of different network functions such as network-oriented authentication, cross-layer operation, administration and management, and session-based quality of service control. The continuous growth is also producing a byproduct that blocks the global distribution of data services because the evolved network functions are effective only within a single network domain. In short, the global network will have the network generations of conventional IP-based network, the next generation network, and the emerging future network. In order to achieve advanced network services utilizing evolved network functions across multiple network domains and generations, this paper proposes a network function exchange architecture. The proposed network function exchange intermediates the various differences related to control protocols, management information, and data format. A service scenario using the network function exchange and detailed architecture is described. Functional requirements of the exchange, a design of the universal interface protocol, and an operational procedure based on the design are described.**

Keywords-NGN; Future Network; Network Function Exchange; Multiple Network Generations

I. INTRODUCTION

Penetration of the cloud computing services and the Internet accessibility are driving the global distributions of the information and communication technology (ICT) services. The recent growth of emerging countries is the economical background to ICT globalization, and accordingly, activities of enterprises tend to go across borders. Indeed, various Internet applications have already been provided globally across multiple network operators, but they are usually provided with the best-effort quality. On the other hand, mission critical or bandwidth-sensitive ICT services cannot be globally achieved by best-effort quality. Today, the standardization of the next generation network (NGN) is enabling session-based quality of service (QoS) control even over all Internet protocol (IP) networks [1]. However, the capabilities achieved by the NGN are effective within the NGN operator, and achieving the capabilities across multiple network operators is unlikely since the NGN has not been widely rolled out yet. To accelerate the global distribution of the enterprise cloud services, various network functions, such as QoS or authentication interworking not only between conventional IP network and NGN but also between NGNs are required. So far, an attempt for global distribution of session initiation protocol (SIP) based services (typically the voice over IP (VoIP) service) has been made [2], however the service exchange technique cannot apply to non-SIP services including the cloud. For the limited scale of inter-operator network interworking businesses, the open access networking has been also discussed, where a common access operator is the hub for network service distribution [3, 4]. In addition, there was past activity for interworking among different types of networks [5], but the activity handled only single generation (i.e., IP network) and handled only single network function (i.e., QoS control).

Recently, a standardization of the future network (FN) as the next of NGN has been initiated [6], and an advance evaluation of the FN testbeds are also underway [7, 8]. FN will have additional functional capabilities, such as the network virtualization that enables secure isolation of user networks [9]. In the future, the global service distribution must transcend architectural barriers at the network borders of conventional IP networks, extended conventional IP network having the bandwidth broker [10] mechanism, NGN, and FN [11]. Not only a simple connectivity but also additional functions (e.g., QoS, authentication, charging) are required to be interworked between those network generations. The attendant issue of the interwork will be filling gaps regarding available functions between the network generations. In addition, depending on countries and operators, exchanging functions may face policy differences regarding, for example, the regulation of the data allocation and the business process of authentication and charging.

To achieve the network interworking, two typical models called the exchange model [12] and the private peering model [13] have been discussed. The exchange model has been employed for Internet exchange (IX) [12], and many networks are interconnected at the cost-effective concentrated exchange point. While the exchange model enables consolidation of interconnection points, the policy management (e.g., defining QoS class, authorization, and applied function itself) cannot be unified since each interconnecting provider has a different policy. On the other hand, in the private peering model, it is relatively easy to negotiate a universal policy and interworking functions at the interconnection point. But the private peering model is unlikely when the number of interconnected network increases, and thus the private peering model tends to require more interconnecting interfaces than the exchange model. Therefore, the exchange model is expected to be suitable for the service distribution in the large-scale global environments. However, there have not been discussions

 ISBN: 978-1-61208-148-9

regarding the suitable functional architecture for interworking various network functions among multiple network generations.

This paper proposes a network interworking architecture for the global-scale service environment across multiple network generations based on the network function exchange (NFE). This paper also proposes the functional design of the NFE and the design of the interworking interfaces. The structure of this paper is as follows. First, an example of the service scenario by utilizing proposed NFE is described in section 2. Section 3 describes the proposed functional architecture to achieve the exchange. Based on the functional design, technical issues that need to be resolved and the requirements to resolve the issues are identified in section 4. Next, detailed functions and interface design to fill the requirements are described in section 5. Finally, the proposed procedural design of the service distribution operations is described in section 6.

II. SERVICE SCENARIO

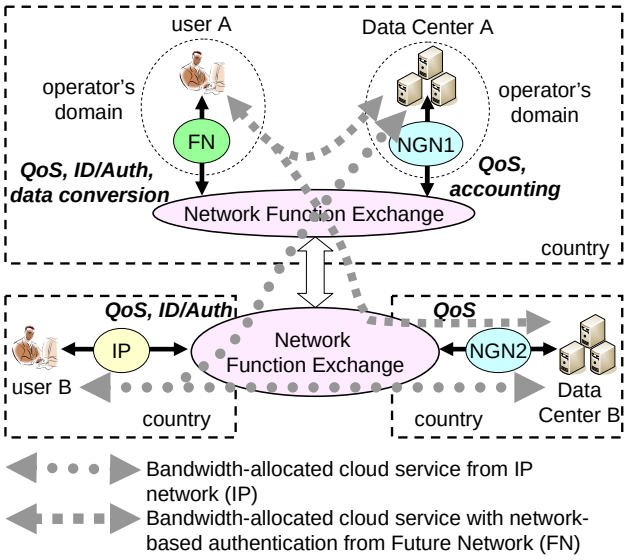

Figure 1. Example of advanced cloud service scenario by mediating functions among multiple network generations as well as multiple countries and operator's domains.

Fig. 1 shows an example scenario of a cloud computing service where the NFE intermediates the functions among multiple network generations owned by different countries and operators. The NFE is operated by an independent company dedicating NFE services, or operated by one of the network service operators providing FN, NGN or IP. The ***terms*** in Fig. 1 show examples of the major functional categories that are intermediated by the NFE. In this scenario, the intermediated functional categories are QoS control (e.g., bandwidth allocation, priority management, guarantee of latency and jitter), network-based identification and authentication (ID/Auth) (e.g., fixed-line or user-terminal based authorizations with the network operator-driven strict confirmation and proof of no-spoofing) and accounting. In addition, if the conversion of the data format or the control signal is necessary, the NFE makes the conversion. In this scenario, a data center A is connected to NGN1 which provides the QoS control and accounting functions. User A is connected to the FN that supports QoS control and ID/Auth functions. By intermediating the available functions of QoS control, ID/Auth and accounting between NGN1 and FN, the NFE provides a QoS-guaranteed cloud service with strict user authentication. The NFE knows the differences of protocols, data formats and functions between network generations, and has the translating/conversion functions. In this scenario for the cloud service between the data center A and the user A, when the NFE receives a request for network services across multiple network generations and domains from user A to data center A through the FN and NGN, the NFE identifies the detailed requested information such as the destination to be connected. The NFE intermediates the QoS control function with the translation of the control protocol to an understandable one in NGN1. The most important thing in this scenario is that the QoS control function is achieved across multiple network generations without any modifications to the current implementation of the control and management scheme on each network generation and domain.

In addition, in order to prevent spoofing, the NGN1 may ask the FN to provide the network-based authentication for identifying user A before providing the service. It is important that network-based authentication (i.e., ID/Auth) function is asked not directly to the user A but to the FN. The FN checks the subscriber information of user A and informs the result to the NGN1 through the NFE. If necessary, the NFE translates the ID/Auth information in order for the NGN1 to be able to understand. The NGN1 also requires the accounting to the user A, and the NFE asks the FN by proxy for the NGN1's request. This function is also translated in the NFE and then requested to the FN with the translation of the management protocol. In the same manner, the data center B connected by NGN2 which supports the QoS control function can also provide a QoS-guaranteed advanced cloud service with the user authentication for user B. Next, the user B connecting to conventional IP network that supports only the QoS control function can use the QoS-guaranteed cloud service without strict network-based user authentication using the data centers A and B. In such a scenario, the NFE can provide advanced services over multiple network generations, network operators and the limitation of country by intermediation of the various network functions.

 ISBN: 978-1-61208-148-9

III. PROPOSED ARCHITECTURE

A. Architectural Fundamentals

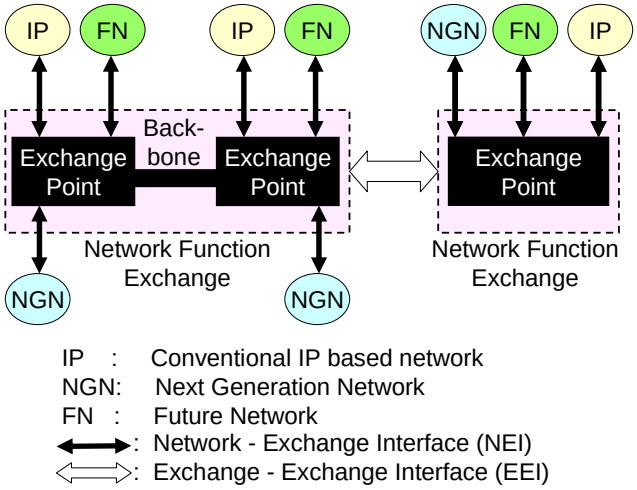

Figure 2. Basic topology of the proposed NFE

Fig. 2 shows the basic topology of the proposed NFE with two interconnection models bridging multiple generation networks. A NFE consists of more than one Exchange Point and a backbone link as optional. The backbone is required if one NFE needs to scale out by distributing the exchange point. If more than two exchange points are interconnected by the backbone link, the aggregated entity acts as an NFE for the distributed architecture. Various kinds of network generation (e.g., conventional IP network, NGN, and FN) are assumed to be interconnected to the exchange point through an interface called the network-exchange interface (NEI). All the data transition and the mediation of control information are transacted within the exchange point through the NEI. The most important characteristic of the exchange architecture is that the NEI is a unified single interface regardless of the network generation. The proposed design of the NEI is described in section 5. As indicated in section 2, the conversion of the data format and the control protocols between the different networks generations are carried out within the exchange point. Therefore, the exchange point provides not only simple data bridging, but also negotiating and brokering of network functions. If it is necessary to interwork between multiple NFEs, the exchange points are interconnected by the Exchange-Exchange Interface (EEI). The difference between the backbone link and the EEI is that the backbone link is a simple transport of control signals and data traffic, and EEI has a functional negotiation role but also a simple transport role.

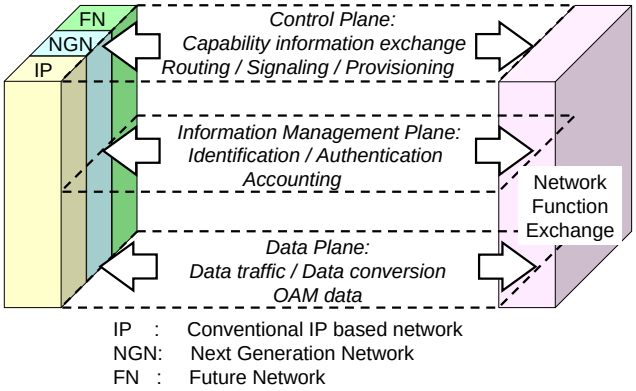

Figure 3. Proposed stratum model of the NFE architecture

The proposed stratum model of the NFE is shown in Fig. 3. The top of layer is the control plane where the supported functions of the network, routing, and reachability information are exchanged. In addition, the signaling information for establishing the QoS-managed path or for admission control is also exchanged in the control plane layer. The middle layer is the information management plane where information on authentication, accounting, network statistics, and operation and management (OAM) status is exchanged. The bottom layer is the data plane where all of the users' data traffic and OAM signals are exchanged. If the data structure or address information of one network generation's traffic must be converted into another generation's format, it is done via the data plane. The detailed data link layer, network layer or transport layer of FN has not been defined yet. Therefore, if the definition of FN will be completely different from the conventional IP or NGN, the Exchange Point must absorb the differences utilizing the data plane. The backbone includes these triple layers within it as a simple link interconnecting multiple exchange points, and delivers the information and data to each exchange point.

B. Architectural Comparison

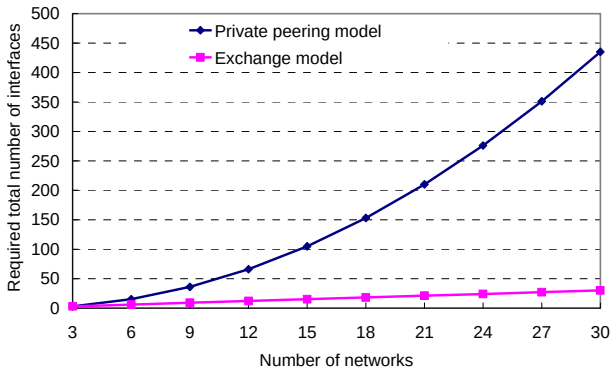

Figure 4. Comparison chart of required number of interfaces for interconnection

Fig. 4 shows a comparison of the required number of interconnection interfaces between the private peering model

 ISBN: 978-1-61208-148-9

and the proposed exchange model in the case of fully meshed interconnection among networks that can be conventional IP, NGN or FN. In the private peering model, when the number of interconnecting networks is *n*, the total number of interfaces can be calculated by an equation of the number of *2*-combinations from *n* elements, ${}_nC_2$. As the result, the total number of required interfaces increases at $O(n^2)$. Hence, when the number of interconnecting networks is 15, the total number of required interfaces is more than 100. Considering service provision on a global scale, it is no longer scalable. On the other hand, in the proposed architecture, a network only has to have an interconnection interface connected to the NFE, regardless of the total number of other interconnecting networks. As a result, the total number of interfaces increases on a linear scale of $O(n)$. In addition, considering the redundancy, many more interfaces are required for a full mesh model. However, the definition of the interface may be much more complicated than the full mesh model, and the NFE must play many advanced roles in order to achieve the proposed architecture. The detailed design is described in section 4.

IV. TECHNICAL ISSUES AND REQUIREMENTS

With the intermediation of network functions, a newly deployed function in one network must also be available to the other interconnecting networks. This means that any network of any generations must be indirectly but continuously upgraded based on functional demand or the plan of the network. In addition, interoperability issues must be partially resolved by emulating some of the functions implemented in the advanced network side. In order to achieve the above requirements in the control plane, each network must report the list of available functions exposed to the NFE. This concept is similar to the capability information exchange or discovery in the link-layer discovery protocol (LLDP) [14] and the link management protocol (LMP) [15], but those protocols can handle only link-layer capabilities. As for routing or signaling protocols, it is important for existing networks, such as the conventional IP and NGN, to reduce the impact on implementing additional interface protocols in order to ensure interoperability. Therefore, interface protocols used in the current networks should be continuously applicable for the NEI as much as possible. Absorbing protocol differences or converting the data format must be performed by the NFE. Even if the same interface protocols are used in interconnecting networks, the meanings or definitions of used parameters may be different and that results in failure of interworking routing or signaling operations. In order to prevent such failures, the introduction of common meanings and definitions within the same context parameters are required. Additionally, if conversion of the data format or addresses is necessary on the exchange point, additional latency and jitter caused by the exchanging operations are desirably required for consideration in the control plane.

As for the protocols and handled information regarding ID/Auth, accounting, and OAM control exchanged using the information management plane, there are few discussions and standardization activities for the functional exchange. Especially for the ID/Auth function, contexts and granularities of the information, such as the identifier (e.g., user account) and the locator (e.g., IP address), should be coupled beyond the network generations. In order to bridge the different ID/Auth protocols, universal hi-level schemes to exchange information should be defined as applicable to multiple network generations. Standardizing the high-level scheme aims to reduce the implementation impacts on all of the network generations, while standardizing new ID/Auth protocols or choosing one existing protocol has huge impacts on existing networks to be interconnected. The proposed high-level scheme is described in section 5. The approach of the ID/Auth functional exchange is expected to be applicable for the accounting function, since the accounting operation is tightly coupled with the ID/Auth information. Regarding the regulation policy of data allocation, configuring the data cache has legal constraints depending on the situations of each country. To address this constraint, the capability of disclosing location information for each exchange point or caching area is effective within the functional exchange. If multiple NFEs are involved, the capability of determining NFE for the conversion is required on EEI in order to avoid duplicated capability allocation and to balance the functional load.

V. DETAILED FUNCTIONS AND INTERFACES DESIGN

A. Functions Provided by Each Network Generation and Applicable Protocols

Table 1 shows the proposed list of typical network functions and shows the eligible protocols for each function. The category of Table.1 shows the major types of functions and the function name represents the specific function belonging to each category. These categories of network functions listed in Table I are already-available ones in current NGN or IP (i.e., QoS path control, ID/Authentication, Accounting, OAM, and Conversion) and a new function available in the FN (i.e., Virtualization/Separation). Eligible protocols for each function are shown in the applicable protocols field in Table 1 per the network generation. Fields represented as "New" in " Applicable Protocols" column means that the protocol needs to be newly defined. As for the "Conversion" row, there are needs for converting between different addressing such as IPv4 and IPv6, and for converting between different transports such as Ethernet and SONET/SDH.

TABLE I. LIST OF PROPOSED FUNCTIONS AND APPLICABLE PROTOCOLS AT EACH NETWORK GENERATION

Function		**Applicable Protocols**		
Category (plane)	**Function Name**	**FN**	**NGN**	**IP**
QoS path (Control)	Bandwidth allocation	New	SIP, Ri, RSVP	RSVP, SIP
	Priority	New	RSVP	RSVP
	Delay	New	New	New
	Jitter	New	New	New

Function		Applicable Protocols		
Category (plane)	**Function Name**	**FN**	**NGN**	**IP**
ID/Authentication (Information management)	Identification	New	New	New
	Authentication	New	Radius	Radius
Virtualization/Separation (Control)	Establish of virtualized/separated slice, participant management	New	New, L2TP, MPLS, GMPLS, VLAN	New,L2TP MPLS, GMPLS, VLAN
	Address conversion	New	New	New
Accounting (Information management)	Accounting	New	Radius	Radius
OAM (Control, Information management)	End to end quality Reachability	New	New	New, LMP
	End to end delay	New	New	New, LMP
	End to end jitter	New	New	New, LMP
Conversion (Data)	Data/format conversion (address, data, codec, IPv4-IPv6, etc)	-	6rd, DS-lite	6rd, DS-lite

B. Design of the Interface Protocols

As a basis of the protocol, a design of the control commands required for each function is proposed. Commands for each interface protocol are assumed to be performed in the control plane or the information management plane, and the commands are designed so that the typical operations of each categorized function in Table 1 can be covered as much as possible as well as the exchange of functional capability information described in section 4. In terms of the data conversion function in Table 1, it is a capability within the data plane, and thus specific commands are not introduced.

First, four commands are proposed to cover the exchange of functional capability information described in section 4.

- Functional capability data base (DB) creation
- Functional capability DB update
- Functional capability DB deletion
- Functional capability DB ack

The functional capability DB creation command is used when the new network is attached to the NFE so that a new functional capability database has to be created. The functional capability DB contains both the availability information of each network function and the routing/reachability information. The functional capability DB update command is used when current functional capability information is changed in supporting of new function. The functional capability DB deletion is used when a network is removed from the NFE. Functional capability DB ack is sent by NFE in order to notify that the NFE surely receives the command (the functional capability DB creation or update or deletion) to the FN, NGN and IP. The functional capability DB contains the area information where the required network function is available.

Second, five commands are proposed to cover the typical QoS functions.

- QoS path creation
- QoS path deletion.
- QoS path modification
- QoS path confirm/provisioning
- QoS path ack/nack

The QoS path creation command is used when new QoS guaranteed (bandwidth allocation, priority control, delay control and jitter control) path wants to be setup, and it contains the parameters of the QoS (e.g., bandwidth in Mbits per second) and path information (e.g., ingress, egress and transit points) to be created. The QoS path deletion command is used when the already setup QoS guaranteed path wants to be deleted. The QoS path modification command is used when the already setup the QoS guaranteed path wants to be modified. The most important factor of this command is that the availability of target path must be kept without any disruption of data traffic. If the modification cannot be achieved without the data disruption by a technology such as the “make before break”, the network providers have to notify that they have no functional availability of the QoS path modification by using the functional capability DB messages. The QoS path confirm/provisioning command is used when the required commands (creation, deletion, modification) are really operated. In the QoS path ack/nack command, Ack is used to report that the sent command (QoS path creation or deletion or modification or confirm/provisioning) is received by the opposite network or NFE. Nack is used to show the refusal of the received command and the reason to the opposite network or NFE.

Next, three commands are proposed to cover the typical ID/Auth functions.

- ID/Auth request
- ID/Auth reply
- ID/Auth ack/nack

The ID/Auth request command is used when ID/Auth information is required from one network or NFE to another NFE or network. The ID/Auth reply command is used when one network or the NFE reply with the ID/Auth information to another NFE or network. In the ID/Auth ack/nack command, Ack is used to report that the sent command (request or reply) is received by the opposite network or NFE. Nack is used to show the refusal of the received command and the reason to the opposite network or NFE.

As for the accounting function, four commands are proposed to cover the typical operations.

- Accounting request
- Accounting reply
- Accounting confirm/provisioning
- Accounting ack/nack

The accounting request command is used when charging is required from one network or NFE to another NFE or network. As the parameter, detailed information such as the cost is included in this command. The accounting reply command is used when replying with the received accounting request command, such as “accept” or “not

 ISBN: 978-1-61208-148-9

accept." The accounting confirm/provisioning command is used when the real charging transaction is done. In the accounting ack/nack command, Ack is used to report that the sent command (request or reply or confirm/provisioning) is received by the opposite network or NFE. Nack is used to show the refusal of received command the reason to the opposite network or NFE.

To cover the OAM function, five commands are proposed.

- OAM path creation
- OAM path deletion
- OAM path modification
- OAM path confirm/provisioning
- OAM path ack/nack

The OAM path creation command is used when the OAM function is newly required. The OAM path deletion command is used when the coexisting OAM path is deleted. The OAM path modification command is used when the coexisting OAM path is modified. The OAM path confirm/provisioning command is used when the required commands (creation, deletion, modification) are really operated. In the OAM path ack/nack command, Ack is used to report that the sent command (creation or deletion or modification or confirm/provisioning) is received by the opposite network or NFE. Nack is used to show the refusal of received command and the reason to the opposite network or NFE.

Finally, five commands are proposed to cover the typical virtualization functions.

- Virtualized/separated slice creation
- Virtualized/separated slice deletion
- Virtualized/separated slice modification
- Virtualized/separated slice confirm/provisioning
- Virtualized/separated slice ack/nack

The virtualized/separated slice creation command is used when the virtualized/separated slice or layer is newly required. The virtualized/separated slice deletion command is used when the coexisting slice or layer is deleted. The virtualized/separated slice modification command is used when the coexisting slice or layer is modified. The virtualized/separated slice confirm/provisioning command is used when the required commands (creation, deletion, modification) are really operated. In the virtualized/separated slice ack/nack command, Ack is used to report that the sent command (the virtualized/separated slice creation or deletion or modification or confirm/provisioning) is received by the opposite network or NFE. Nack is used to show the refusal of received command and the reason to the opposite network or NFE.

VI. PROCEDURE FOR THE SERVICE DISTRIBUTION

All of the services are achieved using the combination of the functions defined in Table 1 and the commands defined in section 5. For instance, the procedure for the global cloud service scenario of exchanging the secure bandwidth allocation functions is represented in Fig. 5. In this service example, following three functions are utilized.

- QoS: bandwidth allocation (QoS path)
- Identification/Authentication (ID/Auth)
- Accounting

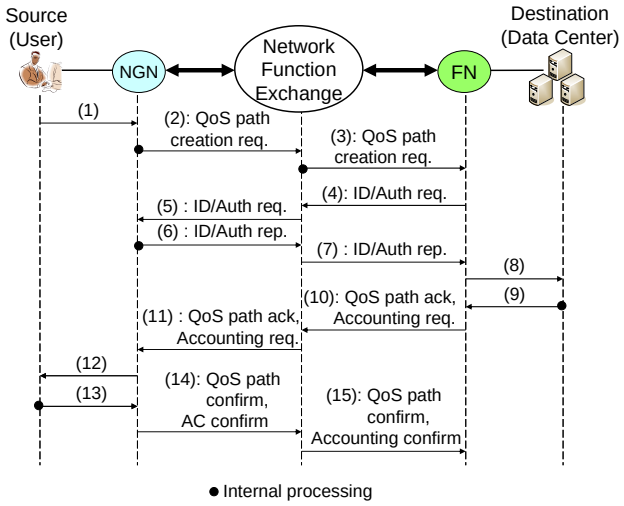

Figure 5. Example procedure of global cloud service scenario with exchanging the secure bandwidth allocation functions

The step-by-step procedure in Fig. 5 is explained below. It is on the premise that user knows the destination information as IP address, domain name or a kind of aliases representing the service name.

(1) The user sends a service request command for bandwidth allocation between the user and the data center to the NGN.

(2) The NGN confirms the availability of the bandwidth resources between the user and the NFE, and then sends the QoS path creation command to the NFE.

(3) The NFE confirms the functional capability of the FN belonging to the data center, and then sends the QoS path creation command to the FN. If the FN does not support the requested function, the NFE sends the QoS path nack command to the NGN and operation ends.

(4) In order to authenticate the requesting user, the FN sends the ID/Auth request command to the NFE.

(5) The NFE forwards the ID/Auth request command to the NGN. As the basic service policy using the network-based ID/Auth functions, the data center and the content provider must clearly specify the utilization to the user. Thus the confirmation process or privacy protection scheme must be prepared to the user.

(6) The NGN checks the identity of the requested user and then sends the ID/Auth reply command to the NFE.

(7) The NFE forwards the ID/Auth reply command with the requested user's identity information to the FN.

(8) The FN asks the data center's approval to create a bandwidth-allocated path to the requested user.

(9) The data center confirms and approves the user by the ID/Auth information.

(10) The FN sends both the QoS ack command and the accounting request command to the NFE.

(11) The NFE forwards both QoS ack command and the accounting request command to the NGN.

(12) The NGN asks for approval from the user.

 ISBN: 978-1-61208-148-9

(13) If the user agrees the details of service contents with accounting/charging information, he sends the final confirmation to the NGN. The final confirmation message is the trigger of actual service provisioning.
(14) The NGN sends both the QoS path confirmation command and an accounting confirmation command to the NFE. In addition, the NGN provisions the bandwidth-allocated path between the user and the NFE.
(15) The NFE sends both the QoS path confirmation command and the accounting confirmation command to the FN. In addition, the FN and NFE provision the bandwidth-allocated path between the NFE and the data center. Finally, the NFE bridges the bandwidth-allocated paths.

VII. DISCUSSION

The proposed architecture has advantages in reducing the number of interconnecting interfaces and also simplifying implementation of functional interworking scheme. However, those advantages are only effective for the network service providers which operate a single generation network and want to interconnect to different network generations for wider service distribution. However, there are some remaining issues regarding complicated implementation of functional interworking scheme especially for NFE provider. First, NFE has to know the detailed functional capability information of each network as well as the routing information, and to determine the availability of services from that information. For the further study, the scalability about the number of connecting networks should be done from this viewpoint. Second, the scalability of protocol and data conversion functions [16] in an NFE has to be considered.

VIII. CONCLUSION

In order to achieve global distribution of data services utilizing various network functions across multiple network generations and domains, a functional interworking architecture of NFE is proposed. The architectural fundamentals and design of the NFE with a triple layer structure of the control plane, the information management plane and the data plane are proposed. With the detailed functional description, the universal control commands between the NFE and each network generation is proposed to intermediate the various functions. Finally, the utilization of proposed commands is identified with a secure bandwidth-reserved cloud service scenario.

ACKNOWLEDGMENT

The authors wish to thank Hideaki Tanaka, Yasuyuki Nakajima and Shigeyuki Akiba who gave us insightful comments and suggestions for this evaluation.

REFERENCES

[1] ITU-T Recommendation Y.2012, “Functional Requirements and Architecture of Next Generation Networks,” April, 2010.

[2] GSM Association, “Inter-Service Provider IP Backbone Guidelines,” Official Document: IR.34, June, 2008.

[3] M. Forzati, C. P. Larsen, and C. Mattsson, “Open Access Networks, the Swedish Experience,” in Proceedings of ICTON 2010, pp. 1-4, July, 2010.

[4] M. Hayashi et al., “Design of Network Resource Federation towards Future Open Access Networking,” in Proceedings of The Seventh Advanced International Conference on Telecommunications (AICT), March, 2011.

[5] G. Cortese et al., “Cadenus: creation and deployment of end-user services in premium IP networks,” IEEE Communication Magazine, pp. 54-60, vol. 41, 2003.

[6] D. Matsubara and M. K. Shin, “Draft Deliverable on Future Networks: Design Goals and Promising Technologies,” ITU-T Focus Group on Future Network, December, 2010.

[7] L. Peterson et al., “GENI Design Principles,” GDD-06-08, August, 2006.

[8] S. Avéssta, “FIREworks,” D2.7 Draft Cooperation Concept, FIREworks consortium, 2009.

[9] S. Meier et al. “Provisioning and Operation of Virtual Networks,” Electronic Communications of the EASST, Kommunikation in Verteilten Systemen 2011, 37, March, 2011.

[10] K. Nichols, V. Jacobson, and L. Zhang, “A Two-bit Differentiated Services Architecture for the Internet,” RFC 2638, July, 1999.

[11] R. Dutta et al, “The Silo architecture for services integration, control, and optimization for the future internet,” In Communications, 2007. ICC '07. IEEE International Conference on, pp 1899-1904, June, 2007.

[12] S. Moore, “Evolution of the Internet,” in Proceedings of Electro/94 International Conference, pp. 263-265, 1994.

[13] R. Dewan, M. Freimer, and P. Gundepudi, “Interconnection Agreements between Competing Internet Service Providers,” in Proceedings of 33rd System Science, pp. 1-7, vol. 1, January, 2000.

[14] Link Layer Discovery Protocol (LLDP), IEEE 802.1AB.

[15] J. Lang et al., “Link Management Protocol,” RFC4204, IETF, October, 2005.

[16] R. Bless and C.Werle, “Network Virtualization From A Signaling Perspective,”Commnications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on., pp. 14-18, June, 2009.

 ISBN: 978-1-61208-148-9