NGN AND INTERNET: FROM COEXISTENCE TO INTEGRATION

Kenji Rikitake[*], *Koji Nakao*[*⋆]

[*]Network Security Incident Response Group,
National Institute of Information and Communications Technology (NICT)
4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795 Japan
[⋆]Information Security Fellow, KDDI Corporation
Garden Air Tower, 10-10, Iidabashi 3-chome, Chiyoda-ku, Tokyo 102-8460, Japan

ABSTRACT

NGN has been on the implementation phase, primarily focused on the replacement of PSTN. NGN carriers try to differentiate NGN from the current Internet for the service quality and reliability. Users of the current Internet, however, expect the early integration of NGN and the Internet, as Internet services have already been deployed into the society and daily life. In this paper, we address the interoperability, management, and security issues for the future integration of NGN and Internet, such as the usage of IPv4 and IPv6 (IPv6 migration), DNS operation, updating end-user equipments and Internet connectivity over NGN. We also propose and evaluate a future model of multi-network connection of NGN networks and the Internet.

Index Terms— NGN and Internet integration; IPv6 migration; DNS operation on NGN; End-user terminal update; Internet connectivity over NGN

1. INTRODUCTION

Next Generation Network (NGN) has been on the implementation phase, primarily focused on a replacement of PSTN. In Japan, the largest national telecom carrier NTT group has announced to start NGN services in March 2008 [1]. NTT has also released a set of documents on the preliminary interface condition and service specification for connecting to their NGN networks [2].

The primary target for NGN is to replace the existing PSTN and ISDN, by introducing highly-reliable networks based on Internet Protocol (IP) and the related technologies. For example, telephone signaling network will be replaced by Session Initiation Protocol (SIP) [3], and the voice transmission will use connectionless protocols such as Realtime Transfer Protocol (RTP) [4].

The *current Internet* is a set of multiple networks which are arbitrarily connected together in various Internet exchanges (IXes), under multitude of bilateral and multilateral agreements between individual Internet Service Providers (ISPs). Some ISPs own the physical links while some use the links provided by the others. Forwarding data between different ISPs are controlled by the policy-based routing protocol, such as Border Gateway Protocol (BGP) [5].

While the current Internet allows open and diverse connectivities as an inter-network of multiple ISPs, the routing has become too complex and a high-cost task for each router. Routing between ISPs are only controlled by the forwarding path between the Autonomous Systems (ASes), a set of multiple IP networks representing an ISP, since BGP is a path-vector routing protocol based on policies and rule-sets.

As the number of networks connected to the current Internet increases rapidly, the minimal service conditions between two arbitrary networks get worse with higher latency of packets, instability of multi-ISP routes, and the financial and social conditions of transit ISPs and IXes.

Another NGN's perspective is to provide a *reliable* set of services which have already been commercialized on the current Internet, under the control of single management entity, such as a telecom carrier company, which is a completely different management model from the current Internet. NGN networks will introduce prioritized packet forwarding based of Differentiated Services (DiffServ) [6, 7] by using the priority field in each IP packet and with strict priority queueing strategy, so that it can provide real-time services such as telephony and video multicast with no interruption by other services with less real-time demands, such as email and Web.

From the current Internet points of view, however, NGN's advantage and goals are still vague and ambiguous. NGN will provide Point-to-Point Protocol over Ethernet (PPPoE) [8] access links, which is the de-facto standard for broadband Mbps-class end-user access links to existing ISPs. However, the direct packet-level reachability and interconnectivity with the current Internet and NGN are still unclear, according to the NGN design and implementation documents. In other words, NGN networks are still just another set of private networks, unless they have direct connectivity to the current Internet. Figure 1 shows the relationship between the NGN networks and the current Internet, which NGN acts only as the access links for Internet and the internal proprietary services.

Since NGN is an Internet-technology-based network, it is expected that NGN will not stay long just coexisting with the current Internet, staying on playing the role of the last-one-

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/

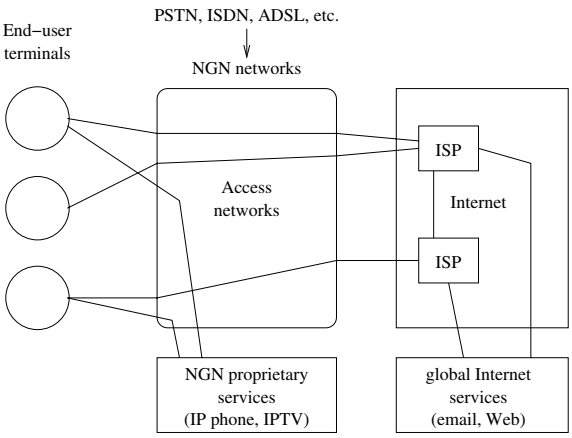


Fig. 1. NGN coexisting with Internet as the access links, while providing the proprietary services.

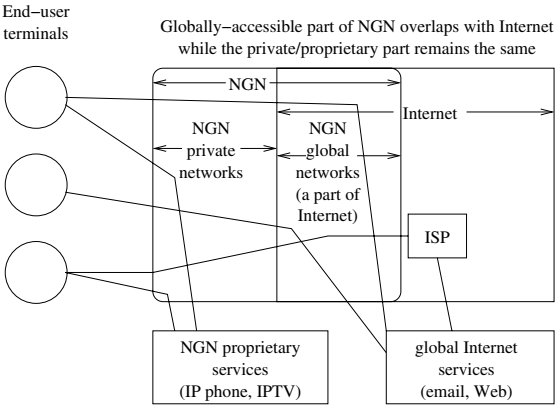


Fig. 2. NGN integrated as a part of global Internet and connected without external ISPs.

mile access network for the current Internet users. This has already been done by existing PSTN, ISDN, mobile terminals, and other carrier networks. NGN should go beyond to become an integrated part of global Internet networks, if NGN carriers want to replace the existing last-one-mile access technologies. Figure 2 shows an example of the future NGN which becomes an essential part of the Internet, while preserving the proprietary services on the private networks as well.

Preparation of connecting and integrating NGN to the current Internet should be planned ahead as a set of design and implementation policies; otherwise the vast investment of replacing existing carrier networks by NGN technologies will only result in reinventing another Internet of very limited connectivity.

In this paper, we address the interoperability, management, and security issues for the future integration of NGN and Internet, based on the seamless routing between the NGN networks and the current Internet networks. We focus on the operational issues of the current Internet networks which will directly affect the NGN network design policies now and in the near future, including the address space, DNS, and the direct IP-level connectivity of NGN and the Internet, which are not well-addressed in NGN-GSI Release 1 documents [9].

In later sections, in relation to the above considerations, we further discuss the technical issues on handling IP version 4 (IPv4) [10, 11, 12] and IP version 6 (IPv6) [13, 14, 15] in Section 2, and the Domain Name System (DNS) issues in Section 3. We also address the issues and problems to solve remote updating issues of the customer equipments in Section 4. Then we propose and evaluate a future model of multi-network connection of NGN networks and the Internet in Section 5. We summarize and conclude the paper in Section 6.

2. IPV4 AND IPV6 ISSUES

2.1. NGN and IP protocol versions

NGN is largely dependent on IPv4 and IPv6 and the functionalities. NGN implementations are focused toward IPv6, though existing IPv4 SIP devices will also be connected, so in the advanced regions where NGN is built on IPv6 from the very beginning will not face the IPv4-related problems within the internal network.

IPv6 is, however, technologically completely independent and different protocol suite from IPv4. Since the current Internet is mostly running on the IPv4 network, the interoperability issues between IPv4 and IPv6 should not be ignored, especially for providing external services between NGN networks and the current Internet. For the developing regions, building NGN over IPv4 is still a viable option to reduce the overall cost, so NGN carriers should consider the scalability of IPv4-based NGN as well as the IPv6-based one, for a tentative network design. Migration from IPv4 to IPv6, however, is equivalent to build a new network of IPv6 and to switch over from the IPv4 network, so the migration cost should be carefully estimated.

2.2. IPv4 address spaces and service transparency

IP phone services, including the video and audio streams, do not necessarily require IPv4 and some implementations are built upon IPv6. Existing global IP phone services are mostly on IPv4, however, due to the wide availability of IPv4 over the world.

If NGN networks want to connect with the existing IP phone services, NGN carriers have to obtain a portion of IPv4 address space dedicated for their services, and provide a protocol conversion using Application Level Gateways (ALGs), such as those for DNS [16].

IPv4 has been suffering from the address exhaustion issues. Experts in Internet registries predict the unassigned unicast global Internet address blocks will be used up by the year 2010 or 2011 [17, 18]. Within two or three years, IPv4 address space will become rather expensive and scarce re-

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/

sources than now, due to the exhaustion and trading incentives of allocated-but-unused IPv4 address spaces.

NGN carriers will have difficulties on providing external services if they fail to allocate adequate IPv4 global address blocks. For example, only 65536 source port numbers is assignable for each IPv4 address. If an NGN network want to serve 1 million simultaneous TCP connections through Network Address Translation (NAT) [19], it has to have at least 16 addresses dedicated for the outgoing services.

The address limitation problem also arises even in the private address space of IPv4 as defined in RFC1918 [20]. Under RFC1918, the number of terminals connectable to the private address space calculated by simply summing up the subnetwork spaces is approximately 17.9 million, which will not be sufficient for large-scale economic regions. Those regions should immediately employ IPv6 for their NGN networks from the very beginning.

For IPv4, NAT and ALG pairs and narrow subnetting within the private address spaces will increase the number of connectable terminals, by allowing address duplicates between them, though multiple NATs may cause confusion of addresses and related security issues by increasing ambiguity of binding IPv4 addresses to actual terminals. Connecting multiple IPv4 networks using NATs is strongly discouraged for this reason.

2.3. Carrier IPv6 networks separated from the current Internet

To preserve direct connectivity between millions of terminals, introducing IPv6 is the only solution. The current usage of IPv6 by telecom carriers, however, is restricted to those which are *not* provided by the current IPv4 Internet.

For example, NTT's Flets IPv6 services [21], a set of carrier-internal IPv6 network services, include IP phone, video streaming, video on demand (VOD) , multicast and Virtual Private Networks (VPNs) between internal nodes. While these services are adding important values to serve the customer's needs, they are proprietary and will not be extended outside of the carrier network.

NTT's Flets IPv6 routing is strictly limited within the carrier, though the end-point terminals must be aware of the IPv6 connectivity if the users want to use the provided services (Fig. 3). If the users want to use *both* the IPv6 and IPv4 connectivities simultaneously, and if an external service is provided both over the IPv6 and IPv4, a problem will arise; the external service is not reachable through the IPv6 so the users have to wait for the completion of the fallback sequence to IPv4.

Allocating global IPv6 addresses to the end-user terminals is a simple and practical solution to solve this separation issue (Fig. 4). IPv6 assumes and allows multiple address allocation for a single network interface, which means a point of connection, so each terminal can be assigned multiple IPv6 addresses and can join multiple networks. NGN carriers can serve their proprietary services within the private network,

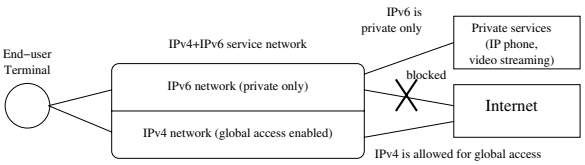


Fig. 3. A dual-protocol network with global IPv4 access and the private-only IPv6 services.

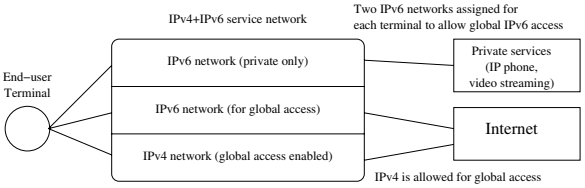


Fig. 4. A dual-protocol network with global IPv4 and IPv6 access, and the private-only IPv6 services.

while allowing the terminals to communicate using another network addresses.

2.4. External connectivity depending on PPPoE

NTT's preliminary NGN service specification only provides PPPoE as the only external connectivity feature for the NGN network, as IP Connectivity Access Networks (IP-CANs). This only allows NGN to be a link-layer medium for an external ISP, while the ISP service is not necessarily directly provided by the NGN carrier.

The choice of an ISP by users should be respected for the current Internet access, and the IP-CAN functionality is essential for NGN networks to be an immediate substitute of the legacy telecom carrier networks. Allowing *only* IP-CAN access based on PPPoE and *not* providing direct IP-level access from NGN networks to the current Internet, however, may cause inefficiency on the traffic processing, such as congestion of traffics between the user terminals and the PPPoE gateway devices, links between the existing ISP and the NGN networks, and the authentication servers and clients to authorize the PPPoE connections.

In the current pre-NGN broadband links which did not assign IP addresses to the endpoints, the two-level structure of the broadband access links and ISPs handling IP services was making sense and logical. For the coming era of NGN, however, all NGN network components, and many of the end-user terminals are technically capable to directly handle IP packets by themselves. Depending external connectivities solely on PPPoE is superfluous and nothing but adding inefficiency to the NGN networks. IP-packet-level direct connectivity between NGN and Internet should be seriously considered for a simpler and robust network, which will result in high performance and reliability.

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/
This article represents the opinion of the authors, and does not imply any endorsement of said opinion by the organizer of the conference.

3. DNS ISSUES

DNS [22, 23, 24] is an essential part of IP protocol suite, and also plays an important role on NGN. For example, ENUM (an acronym from Telephone Number Mapping) [25] defines the lookup method from E.164 telephone numbers through `e164.arpa` domain name space, and finding out the connecting method as describes in DNS Naming Authority Pointer (NAPTR) Resource Records (RRs) [26, 27].

DNS has many interoperability issues, however, in the dual-stack environment of IPv4 and IPv6. The current DNS does not have an established authentication mechanism either, and that contributes to the fraudulent attacks by redirecting traffics to unauthorized or illegal hosts from a legitimate domain name.

3.1. IPv4 and IPv6 DNS service coexistence requirement

DNS has been built on an assumption that the access method is only via IPv4. For example, the number of Root Zone servers (13) is defined by the 512-byte size limit of DNS UDP payload and the DNS A RR, representing an IPv4 address for a domain name. If IPv6 addresses should be also placed on the Root Zone, the DNS AAAA RRs [28] have to share the limited space with the A RRs, so the number of servers in a DNS answer packet for a Root Zone should be reduced. This will cause the DNS less robust and more prone to denial-of-service (DoS) attacks. EDNS0 [29], a DNS protocol extension to enable larger UDP payloads, has been gaining popularity among major implementations such as BIND [30], but is still not considered to be the standard throughout the current Internet.

Introduction of IPv6 also requires another condition to *all* the DNS servers to make them accessible in both IPv4 *and* IPv6 networks. During the transition phase from an IPv4 network to an IPv6 network, the entire DNS system components have to be operational on both networks, to prevent unresolvable domain names. This issue becomes further complicated due to the DNS protocol that DNS authoritative servers cannot be specified directly by the IP addresses, but by the server hostnames (NS RRs). A DNS resolver cannot determine whether a DNS server provides the service on a network unless trying to resolve the server hostname again to a set of IPv4 or IPv6 addresses.

In the current Internet, very few DNS authoritative servers provide IPv6 accessibility, so DNS accessibility through IPv4 is almost mandatory for IPv6 hosts [31]. Using IPv6-to-IPv4 DNS proxies will relax the IPv4 accessibility requirement, with the cost of externalizing the protocol conversion between IPv6 and IPv4. Transition from IPv4 to IPv6 is generally not easy, due to the fundamental differences between the two network protocols [32].

The coexistence requirements explained above are also the same in an NGN network, so long as DNS is used for providing a mandatory service such as ENUM. If an NGN network which only uses IPv6 and does not use IPv4 were built, the *internal* requirement of supporting IPv4 DNS would be eliminated, but the interoperability issues with other Internet networks still remain.

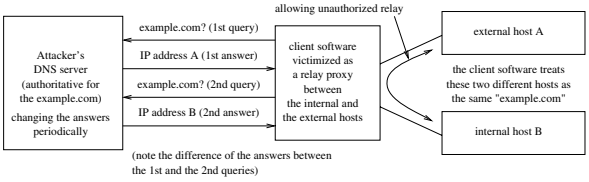


Fig. 5. DNS rebinding attack, by answering two different IP addresses to the same hostname.

3.2. Securing DNS resources and private namespaces

DNS itself does not have the authentication mechanism, and a source of various frauds using false domain names and the redirection to false domain servers. DNSSEC [33, 34, 35], a cryptographic authentication scheme with the chain of trust reflecting the domain name hierarchy and the zone delegation, has been gaining popularity among Top-level Domain (TLD) registrars.

DNSSEC requires all RRs to be signed with the administrator, and the signing path is traceable to the trust anchor which is the root of the signing delegation tree, so the resolver can verify whether a received RR is authenticated or not.

NTT's preliminary NGN service specification, however, does not mandate the use of DNSSEC. While this may reduce the processing burden of NGN service and customer equipments, this will become a vulnerability when a malicious service provider over NGN starts to distribute false DNS information.

If NGN depends on the DNS-based technology such as ENUM, introduction of DNSSEC is an essential measure to be taken as soon as possible. Deployment of private DNSSEC zones for an NGN network should be consistent with the global zones, even though the scope of the private domain names should be within the access-control perimeter of the NGN network, and the private zones should have their own trust anchor.

3.3. DNS access control for private networks

Building a DNS for a private network is traditionally considered as constructing an isolated DNS tree from the global Internet. This is not sufficient, however, to guarantee the namespace isolation under the modern environment of Web browsers and plugins, based on hostname authentication.

DNS rebinding attack [36] is an emerging method to force Web programs running on hostname-based authentication to accept multiple IP addresses for a hostname, so that contents of a host within the private address space is accessible from external hosts by using the programs as the proxy.

Figure 5 shows the attack scheme; an attacker who has the control of a domain namespace forces a remote program to authenticate two or more addresses for a hostname under the

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/
This article represents the opinion of the authors, and does not imply any endorsement of said opinion by the organizer of the conference.

domain, by periodically changing the address RRs bound to the hostname. This vulnerability is based on the weak assumption that a hostname is always representing the same host, which is the current access control model on JavaScript, Java, Flash and other Web application plugins.

One of the fundamental solution to prevent the DNS rebinding attack for a private network including NGN is to filter out DNS address RRs pointing *internal* IP addresses for an *external* name by a mandatory screening program such as `dnswall` [37], presumably placed for all of the DNS cache programs for the private network. Unfortunately DNSSEC will not prevent this problem so long as it accepts the zone signature of the attacker's domain.

NGN's core competence is the higher reliability than the current Internet by ensuring and limiting the services running within the network. Strict perimeter control of the internal and external resources, including IP addresses and DNS zones, should be enforced as much as possible.

4. REMOTE UPDATES OF CUSTOMER EQUIPMENTS

Supporting the autoconfiguration is an essential part of modern computer networks. Autoconfiguration includes remotely updating the software and firmware of connected devices, and providing the dynamically-configurable information such as the default router and DNS server addresses.

Being able to remotely update customer equipments is an essential functionality for network-connected products. Automatic updating of software and firmware has become a core functionality of security-aware application programs and systems. Performing remote updates of customer equipments is a fundamental function of an NGN network, and may cause a serious trouble if failed.

Providing important updates such as those fixing vulnerabilities is essential for keeping the entire network secure. Updating through a server-client connection, however, may cause severe congestion and processing load to the distribution server of the update information. For example, Microsoft's Windows operating system have the long history of update failures and congestions [38], due to the large install base on diversed user environments. NGN carriers should expect the similar congestion and should prevent it by a careful planning.

Performing updates on a program may introduce bugs on another program and render it unusable. For example, Skype IP phone service was disrupted on August 2007 [39] by a Microsoft routing update to the Windows operating system. The components of NGN terminals, including the hardware, software and firmware, should be fully tested to avoid the inter-dependency between running programs.

Performing updates for NGN terminals should be carefully designed to avoid congestions on a certain period of a day or a week, and should minimize the requirement of user assistance as possible.

Updating customer equipments requires the boot-up address and protocol information of the server which each terminal connects for the updating data. Modern IP networks introduce autoconfiguration capabilities. For example, NTT's preliminary NGN service specification includes the usage of Dynamic Host Configuration Protocol (DHCP) for IPv4 [40] and the DHCPv6 for IPv6 [41] to provide boot-up information to the terminals. In this case, the most direct way to provide the boot-up information for the remote updating is to include the data as DHCP/DHCPv6 options [42, 43], since maintaining the quality of the end-user terminals is mandatory to ensure the security of NGN networks.

5. INTEGRATING NGN BY MULTI-NETWORK CONNECTION TO INTERNET

5.1. Inter-connection technologies between NGN and IPv6 Internet

Internet connectivity over NGN is the most expected service of NGN, since many of the potential NGN users have presumably been accustomed to the current Internet environment and services. NGN uses IPv6 as the base protocol suite, so it is highly plausible for the users to assume that they can reach the IPv6 Internet as well as the IPv4 Internet.

The inter-connection technology of NGN and the IPv6 Internet, however, is not well-defined yet. For example, NTT West does not define how the company provide the IPv6 connectivity in their preliminary service specification document [2]. In Section 2.3, we have described the situation of the private-only IPv6 services which NTT West provides as of March 2008.

Reaching to the IPv6 Internet can be accomplished by the following two methodologies:

- operating multiple IPv6 networks of different cover ranges and services within an NGN network, each represented by the own IPv6 network prefix; and
- providing IP-CAN for the IPv6 Internet as well as for the IPv4 Internet, such as IPv6 over PPP [44], explicitly forming tunnels between each terminal and the router for the IPv6 Internet.

In later sections, we explain the advantages and issues to be resolved for operating multiple IPv6 networks within an NGN network. IP-CAN for the IPv6 Internet has the same issues as in the case of the IPv4 Internet, which has previously been described in Section 2.4.

5.2. Connectivity by assignment of multiple network prefixes to NGN terminals

Assignment of multiple addresses on an IP network interface has already been a common practice for the current IPv4 Internet, such as for providing virtual hosting services on the same physical computer. On IPv6, the assignment will be even much easier, since each terminal can have multiple network addresses assigned on the upper 64-bit part of the IPv6

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/

address, while preserving the uniqueness by using the EUI-64 address on the lower 64 bits [45].

The freedom of address assignment on IPv6 will practically enable *all* NGN terminals to simultaneously join multiple IPv6 networks, including the private one with the proprietary services, and the global one with the Internet services. The NGN carriers can control the membership of each terminal for each IPv6 network of different scopes by the DHCPv6 prefix assignment options for authenticating each terminal, and providing explicit routing information for each IPv6 network.

The IPv6 multiple address assignment procedure explained above is a complicated task comparing to the traditional IPv4 network management practice, where each terminal is only allowed to have one IPv4 address. This task is also required, however, when an NGN carrier explores the usability of IPv6 multicasting by choosing the members of each multicast group, as a technical requirement.

We also believe that relying only to IP-CAN for providing external Internet connectivity is not sufficient to satisfy the user's demand although the NGN Release 1 expects to provide the IP-CAN capability as a connectivity to the existing ISPs, regarding the following possibly expected results after NGN carriers start providing the services:

- NGN networks will connect millions of terminals and will possibly cause congestion for the links between NGN and ISP networks;
- NGN is IP-based, so IP-CAN services are inevitably IP-over-IP, which are superfluous and inefficient, especially for IPv6 which results in carrying overlaying IPv6 packets over another set of IPv6 packets; and
- NGN authorized users may want to use the proprietary services out of the home NGN network, from other NGN networks or from the Internet, such as roaming services of IP phone services between different NGN carriers.

NGN networks will firstly form its own inter-connection networks to maintain the quality of services (QoS) including the packet loss rate and latency. Since the current Internet does not guarantee the QoS characteristics at all, inter-network IP connections between NGN networks should be peer-to-peer and in a mesh topology. As NGN proceeds to replace the PSTN and ISDN services, it is expected that the interconnection points between NGN networks will resemble the IXes, since the points perform the exactly same functions as IXes, namely exchanging IP packets and the routing information.

Extending these NGN exchange points into IXes including NGN inter-network traffics (Fig. 6 will result in advantages listed as follows:

- Enabling direct IP packet exchange between NGN networks and the Internet networks, which may shorten the latency and improve the packet loss rate;

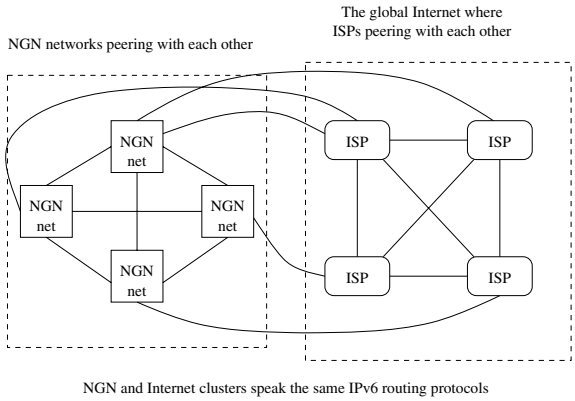


Fig. 6. NGN network exchange and Internet exchange connected with each other.

- ISPs may use NGN networks in transit for a long-haul link, as a backup between the peer ISPs, only by specifying the routes; and
- A part of NGN networks can be resold for an ISP, which will allow services such as Mobile Virtual Network Operators (MVNOs) on NGN, as the MVNOs currently do with the current mobile phone networks.

5.3. Issues to be resolved on operating IPv6 networks with multiple prefixes

Extending an NGN network from a private IPv6 network to a set of multiple IPv6 networks with different scopes will introduce the following issues to be solved:

Address allocation: prefixes for private IPv6 networks should not be duplicated between multiple NGN carriers. While each carrier can arbitrarily choose the address prefix for the internal use by introducing Unique Local Addresses (ULA) [46], the mathematical possibility of ULA space collision is non-zero, so the arbitration of address space usage has to be performed between the inter-connected private networks. Using a globally-unique address space is a workaround, but that will introduce another source of routing complexity, not only wasting the address space, which is still finite for IPv6.

Routing complexity: the computational complexity of calculating optimal peer-to-peer routes is $O(n^2)$ when the number of routes in a network is n. Adding IPv6 networks in an NGN network will raise the processing burden of routers in the network and may reduce the availability. For example, NTT East has an incident of 7-hour disruption of the IPv6-based network services on May 15, 2007, which had 10000 routes inside, due to 2000 failed routers of 4000 routers in total [47]. A single router's failure caused the network-wide dynamic route recalculation and exceeded the processing capacity of the failed routers. This problem may even be much worse on the global Internet, as the number of global Internet routes are $\simeq$ 254000 for IPv4 and $\simeq$ 1200 for IPv6 as of March 2008 [48], steadily increasing.

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/
This article represents the opinion of the authors, and does not imply any endorsement of said opinion by the organizer of the conference.

Policy enforcement of address scopes: In either case of using multiple prefixes or that of IP-CAN for IPv6, policy enforcement to the terminals of an NGN network will be a complex procedure. Address scope control for each terminal should be performed with a combined configuration of the DHCPv6 database, the routing table of the border routers between the private and global IPv6 networks, and the routing configuration for each terminal. For the IP-CAN access control, the connected ISP or NGN carrier should authenticate each connection request, such as that of PPPoE. A detailed definition of NGN network components and procedures for the policy enforcement, similar to the standard profiles for U.S. Military networks [49] and the local network protection procedure for the IPv6 Internet [50], should be formalized as a part of NGN recommendations.

6. CONCLUSIONS

In this paper, we discussed the interoperability, management and security issues of NGN, focused on the IPv4 and IPv6 address management and routing, DNS operation, and remote updates of customer equipments. We also proposed an integration plan of NGN networks, by taking the advantage of NGN terminals to simultaneously join multiple IPv6 networks.

We understand the primary motivation of NGN is the replacement of the legacy telecom carrier networks, with the inexpensive equipments available for the Internet protocols. The first generation NGN networks going to be provided in 2008 will still have an aspect of the field experimentation of the commercial IPv6 private network, and the replacement of legacy telephone service with IP phone services.

The current Internet over IPv4, however, will become incapable of accepting users within a few years due to the address space exhaustion. Many Internet users expect NGN to be better than the current Internet and ensuring access to the existing Internet services. NGN carriers therefore should take advantage of providing IPv6 global Internet services as well as the proprietary value-added ones, so that they will succeed the prosperity of the current Internet and truly become the Next Generation Network.

7. REFERENCES

[1] NTT West, "Press release of application for approval of NGN commercial services," originally written in Japanese, October 25, 2007, http://www.ntt-west.co.jp/news/0710/071025b.html.

[2] NTT West, "Interface Conditions of Next Generation Network," Oct. 2007, originally written in Japanese, http://www.ntt-west.co.jp/open/ngn/interface.html.

[3] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," June 2002, RFC3261.

[4] H. Schulzrinne and S. Casner and R. Frederick and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," July 2003, RFC3550.

[5] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," January 2006, RFC4271.

[6] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W . Weiss, "An Architecture for Differentiated Service," December 1998, RFC2475.

[7] D. Grossman, "New Terminology and Clarifications for Diffserv," April 2002, RFC3260.

[8] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)," February 1999, RFC2516.

[9] ITU-T, "Next Generation Network Global Standards Initiative (NGN-GSI) Release I," 2005, http://www.itu.int/ITU-T/ngn/release1.html.

[10] J. Postel, "Internet Protocol," 1981, RFC791 (also STD5).

[11] J. Postel, "Internet Control Message Protocol," 1981, RFC792 (also STD5).

[12] R. Braden (Editor), "Requirements for Internet Hosts – Communication Layers," 1989, RFC1122.

[13] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) specification," 1998, RFC2460.

[14] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," December 1998, RFC2461.

[15] Susan Thomson and Thomas Narten, "IPv6 Stateless Address Autoconfiguration," 1998, RFC2462.

[16] P. Srisuresh, G. Tsirtsis, P. Akkiraju, and A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)," September 1999, RFC2694.

[17] G. Huston, "IPv4 Unallocated Address Space Exhaustion," Oct. 2007, presentation at RIPE 55 Meeting, Amsterdam, Netherlands, http://www.ripe.net/ripe/meetings/ripe-55/presentations/huston-ipv4.pdf.

[18] Ministry of Internal Affairs and Communications, Japan, "Minutes of the 2nd meeting of the survey and research group for smooth IPv6 migration of Internet," Oct. 2007, originally written in Japanese, http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/ipv6/071016_2.html.

[19] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations ," August 1999, RFC2663.

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/
This article represents the opinion of the authors, and does not imply any endorsement of said opinion by the organizer of the conference.

[20] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, "Address Allocation for Private Internets," February 1996, RFC1918.

[21] NTT West, "Service description of NTT Flets v6 Appli," originally written in Japanese, http://flets-w.com/v6ap/tokuchou/index.html.

[22] P. V. Mockapetris, "Domain names – concepts and facilities," 1987, RFC1034 (also STD13).

[23] P. V. Mockapetris, "Domain names – implementation and specification," 1987, RFC1035 (also STD13).

[24] R. Braden (Editor), "Requirements for Internet Hosts – Application and Support," 1989, RFC1123.

[25] Patrik Faltstrom and Michael Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)," 2004, RFC3761.

[26] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS," Oct. 2002, RFC3401.

[27] M. Mealling, "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm," Oct. 2002, RFC3402.

[28] S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, "DNS extensions to support IP version 6," 2003, RFC3596.

[29] P. Vixie, "Extension Mechanisms for DNS (EDNS0)," 1999, RFC2671.

[30] Internet Software Consortium, "BIND," http://www.isc.org/bind/.

[31] A. Durand, J. Ihren, and P. Savola, "Operational Considerations and Issues with IPv6 DNS," April 2006, RFC4472.

[32] R. Bush, "IPv6 Transition and Operational Reality," Oct. 2007, presentation at RIPE 55 Meeting, Amsterdam, Netherlands, http://www.ripe.net/ripe/meetings/ripe-55/presentations/bush-ipv6-transition.pdf.

[33] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," Mar. 2005, RFC4033.

[34] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Resource Records for the DNS Security Extensions," Mar. 2005, RFC4034.

[35] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Protocol Modifications for the DNS Security Extensions," Mar. 2005, RFC4035.

[36] C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh, "Protecting Browsers from DNS Rebinding Attacks," in *Proceedings of the 14th ACM conference on Computer and Communications Security (CCS 2007)*. ACM, Oct. 2007, http://crypto.stanford.edu/dns/dns-rebinding.pdf.

[37] Google, "dnswall," http://code.google.com/p/google-dnswall/.

[38] Microsoft, "You receive an access violation error and the system may appear to become unresponsive when you try to install an update from Windows Update or from Microsoft Update," http://support.microsoft.com/kb/927891/.

[39] Villu Arak, "What happened on August 16," Aug. 2007, August 17, 2007, on Skype's Heartbeat blog, http://heartbeat.skype.com/2007/08/what_happened_on_august_16.html.

[40] R. Droms, "Dynamic Host Configuration Protocol," 1997, RFC2131.

[41] R. Droms (Editor), J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," 2003, RFC3315.

[42] Internet Assigned Numbers Authority (IANA), "DHCP and BOOTP Parameters," http://www.iana.org/assignments/bootp-dhcp-parameters.

[43] Internet Assigned Numbers Authority (IANA), "DHCPv6 and DHCPv6 options," http://www.iana.org/assignments/dhcpv6-parameters.

[44] S.Varada, D. Haskins, and E. Allen, "IP Version 6 over PPP," September 2007, RFC5072.

[45] M. Crawford, "Transmission of IPv6 Packets over Ethernet Networks," December 1998, RFC2464.

[46] R. Hinden and B. Haberman, "Unique Local IPv6 Unicast Addresses," October 2005, RFC4193.

[47] S. Munakata, *NTT no Jibaku – Unknown Facts about NGN Project (originally written in Japanese)*, pp. 18–32, Nikkei BP, 2008, ISBN-13: 978-4-8222-1079-3.

[48] G. Huston, "BGP Analysis Reports – BGP Table Data," http://bgp.potaroo.net/index-bgp.html.

[49] DISR IPv6 Standards Technical Working Group, "Dod IPv6 Standard Profiles for IPv6 Capable Products Version 2.0," 1 August 2007, http://www.nav6tf.org/documents/DISR_IPv6_Product_Profile_v20_FINAL_Aug07_ITSC_Approved.zip.

[50] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, and E. Klein, "Local Network Protection for IPv6," May 2007, RFC4864.

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/
This article represents the opinion of the authors, and does not imply any endorsement of said opinion by the organizer of the conference.

ITU-T Kaleidoscope Conference
Innovations in NGN

NGN AND INTERNET: FROM COEXISTENCE TO INTEGRATION

Kenji Rikitake
NICT, Japan
rikitake@nict.go.jp

Geneva, 12-13 May 2008

Paper accepted for presentation (Poster Session P06)
at the ITU-T "Innovations in NGN" Kaleidoscope Conference, Geneva 12-13 May 2008, http://itu.int/ITU-T/uni/kaleidoscope/

NGN AND INTERNET: FROM COEXISTENCE TO INTEGRATION

Kenji Rikitake, Koji Nakao

Network Security Incident Response Group,
National Institute of Communications and Information Technology (NICT), Japan
Contact e-mail: rikitake@nict.go.jp
ITU-T Innovations in NGN: 13 May 2008, Geneva, Switzerland

NGN status in Japan

NTT has started their NGN service called *Flets Hikari Next* since April 2008, including:

- Diffserv-based QoS to guarantee minimum bandwidth and low packet-loss
- Terminal device authentication
- IPv6 *private network* services such as:
  - IP telephony
  - VPN and wide-area Ethernet
  - Multicasting (e.g., for IPTV)

Other examples:

- KDDI's *Ultra 3G* fixed-mobile convergence
- Softbank's merger with Vodafone

Our concerns

- *Is NGN just another private IPv6 network without global reachability?*
- *Can NGN keep itself isolated from the IPv6 global Internet forever?*
- *How NGN carriers interconnect with each other?*

Examples on NTT's NGN:

- NTT has already provided best-effort-based Internet services and links *before NGN*: NGN services may be superfluous
- The IP-CAN feature is only provided for the IPv4 global Internet, *not for IPv6*
- Current NGN services are all physically restricted in the private network

Security issues on NGN and the global IPv6 Internet integration

NGN needs stronger terminal authentication.

NGN is based on Internet technologies. *Everything can be connected* as an NGN end-user terminal by the attackers. IPv6 and MAC address-based terminal device authentication with DHCPv6 does not necessarily defend the end-node subsystems. Stronger authentication methods, such as tamper-proof terminal identification devices and protocols, should be introduced to prevent connection of unauthorized devices.

NGN needs standardized update methods.

Remote software update capability should be an essential part of NGN terminal devices to automatically fix the vulnerabilities. The number of NGN terminals is large, so the update procedure itself should not crash or fail even if the update requests from the terminals to the network are congested.

NGN components should be robust enough as if they were connected to the global Internet.

Cross-network vulnerabilities has already been exploited on the devices connected to the IPv4 and the IPv6 networks. While current NGN is considered as a private IPv6 network, it has been widely exposed to the IPv4 public Internet and the connected devices can be attacked using IPv4. NGN devices could be exploited to attack existing IPv4 hosts.

NGN carriers should be ready to assign multiple IPv6 prefixes to the terminals.

IPv6 assumes each terminal has multiple addresses for each interface as a basic capability. For interconnecting NGN carriers, representing access scopes using individual prefixes is the most straightforward method to implement the access control policy to the terminals. While IP-CAN service for IPv6 is another possible choice, policy-based routing is simpler to implement across the entire network, and is more efficient.

NGN carriers should be capable to handle massive number of external IP routes.

As of March 2008, the number of IPv4 Internet routes are 254,000, and IPv6 Internet has already 1200 routes [1]. While NGN networks can be designed to simplify and minimize the route recalculation, unnecessary routing complexity may cause service disruption at any time. In the case of NTT East on May 2007 [2], a single router's failure caused recalculation and overloaded other routers.

[1] Geoff Huston, *BGP Analysis Reports – BGP Table Data*, `http://bgp.potaroo.net/index-bgp.html`

[2] NTT East, the final press release on the disruption of Flets and Hikari Denwa services, May 16, 2007, `http://www.ntt-east.co.jp/release/0705/070516b.html`

End users want Internet connectivities *through NGN with IPv6*

NGN cannot stay private forever.

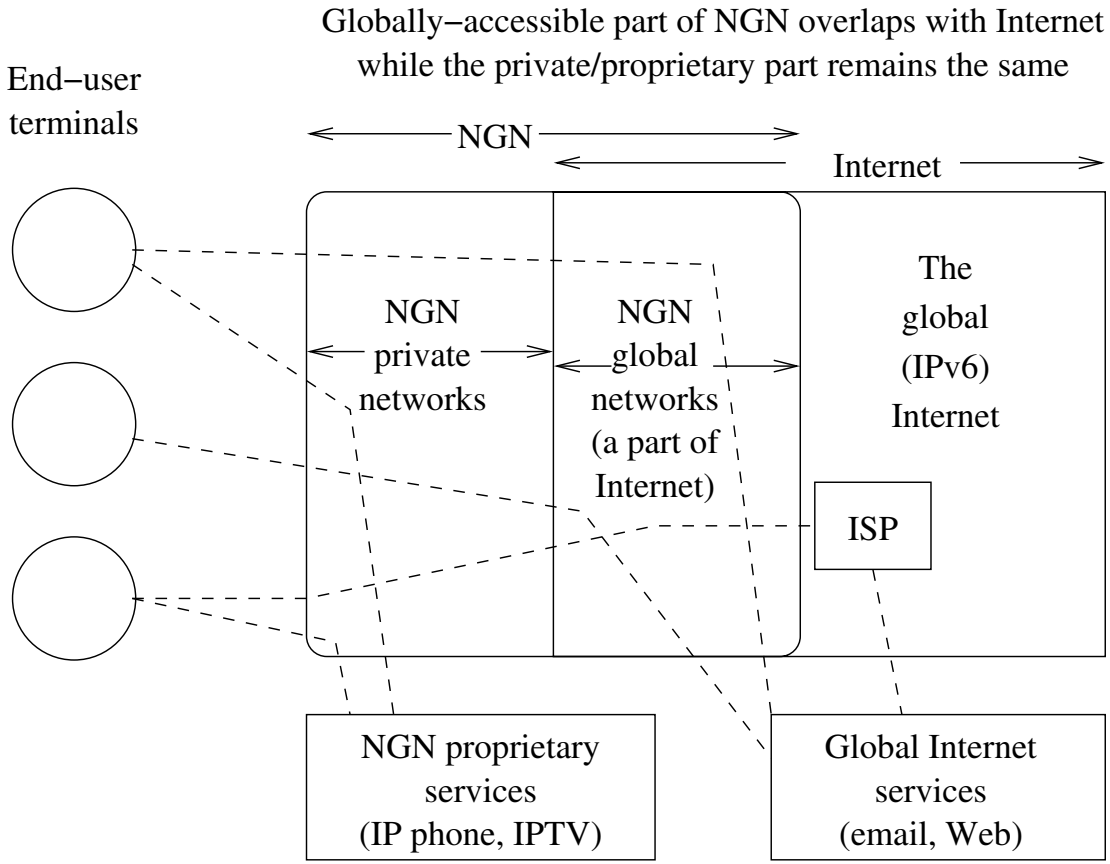
The end users of NGN do not want another closed network; many of them believe NGN will *integrate* and even *replace* the Internet.

NGN cannot be isolated from the IPv6 global Internet.

NGN is based on *Internet* technologies. NGN should go beyond from the state of coexistence with the current Internet as the last-one-mile link; NGN should be *part of* the Internet to maximize the usability not only from the NGN users but also from the Internet users.

NGN carriers must be ready for inter-connecting each other.

NGN is not just another Internet service; it will replace the existing PSTN, ISDN, and mobile services. Interconnection between multiple NGN carriers with different security and accounting policies is inevitable.



NGN should be integrated as a part of global Internet, connected without external ISPs.

End users want more transparent and seamless access to the Internet through NGN, as Internet migrates from IPv4 to IPv6.

Multi-prefix connectivity helps NGN integration to IPv6 Internet