NETEXT WG
Internet-Draft
Intended status: Informational
Expires: August 25, 2012

S. Gundavelli
M. Grayson
Cisco
Y. Lee
Comcast
H. Deng
China Mobile
H. Yokota
KDDI Lab

February 22, 2012

Multiple APN Support for Trusted Wireless LAN Access
draft-gundavelli-netext-multiple-apn-pmipv6-01.txt

Abstract

This specification defines a mechanism for extending multiple APN/ home-network support for a mobile node.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 25, 2012.

Table of Contents

1. Introduction

Mobile Operators are expanding their network coverage by integrating various access technology domains. Proxy Mobile IPv6 [RFC5213] is one of the key protocol interface for integrating these access networks and building a common IP mobility architecture. For example, the Trusted non-3GPP Access interface based on Proxy Mobile IPv6 [TS23402] interface, 3GPP S2a PMIPv6, specified by the 3GPP system architecture, provides the needed protocol glue across different access systems.

The 3GPP system architecture supports the concept of an Access Point Name (APN). An APN can identify a particular routing domain and can be used by 3GPP operators to segment user traffic. APNs are included in the session establishment signaling sent by 3GPP User Equipments (UEs), identifying which routing domain they want to be connected to. Furthermore, 3GPP has defined a system architecture which supports the ability of a single UE to have simultaneous connectivity to a plurality of APNs, and be allocated multiple IPv4 addresses and/or IPv6 prefixes from the network.

When the S2a protocol interface based on Proxy Mobile IPv6 is used, the system architecture is restricted in that the mobile access gateway can establish bindings with a single APN/home network at any point of time. There is a limitation with respect to simultaneous, multiple APN access. This limitation is due to the lack of semantics for allowing multiple IPv4 address assignment over DHCP to a given interface of a mobile node. In IEEE 802.11-based Wireless LAN networks, the mobile node can only be assigned a single IPv4 address to the Wireless LAN interface. This essentially forces the mobile access gateway to establish only a single mobility session with any one home network/APN and assign a single IPv4 address to the mobile node.

This limitation of single, simultaneous, APN/home-network access from WLAN network, at any point of time, is proving to be a major hindrance. Mobile operators have deployed application specific APN's for many years and those networks are operational. For example, APNs have been defined to specifically support IP Multimedia Subsystem (IMS) based SIP services. It is critical for the mobile operator to ensure access to these APN's/home networks in a consistent way, irrespective of the access technology domain to which they are connected. It is in the interest of the operator to enable the mobile user to activate multiple applications hosted in different APN's and allow access from the WLAN access network. Therefore, there is a need to allow multiple APN access from WLAN access network. The proper approach to solving this problem is to force the mobile operator to move away from the model of building application

specific APN's/home-networks and consolidate them into a single home-network. There is also the other approach of building virtualized connection model (PDN Connection) on the Wireless LAN interface and make it appear like a 3G interface and enable similar access semantics. However, this has a huge impact on the mobile terminal and is not easy to achieve such radical change any time in the foreseeable future.

This document specifies an alternative approach for addressing this limitation. The mobile access gateway by supporting this approach can enable access to multiple APN/home networks, simultaneously. The specified approach does not require any changes to the mobile node, or to the Proxy Mobile IPv6 protocol interface. This approach is specific to IPv4 sessions. For IPv6, the mobile access gateway has the ability to project multiple IPv6 prefixes obtained from different home networks, and carry them in the Router Advertisement messages that it sends to the mobile node. The mobile node can potentially use Stateless Auto-configuration approaches for obtaining multiple IP addresses for the interface. This capability in conjunction with Prefix Coloring scheme, allows the mobile node to use the source address based on the application type, and hence has a solution for multiple APN access. There are clearly better ways to solve this problem for IPv6 and with the goal not to create NAT66 requirement, this specification therefore limits the scope of this document to IPv4-only sessions.

2. Conventions and Terminology

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in the base Proxy Mobile IPv6 specifications [RFC5213] , [RFC5844], [RFC6459], [RFC5149] and [RFC6089]. Additionally, this document uses the following abbreviations:

Access Point Name (APN)

Its the name of a packet data network. This APN concept was first introduced in GPRS by 3GPP to enable legacy Intelligent Networking (IN) approaches to be applied to the newly deployed IP packet data services. In roaming deployments, the APN construct was visible to the visited network and allowed legacy IN charging solutions to be supported. Defining an application specific APN then allowed application charging to be supported.

3. Solution Overview

Figure 2 illustrates the scenario where the mobile access gateway in the access network has established PMIPv6 bindings for the attached mobile node on multiple local mobility anchors, simultaneously.

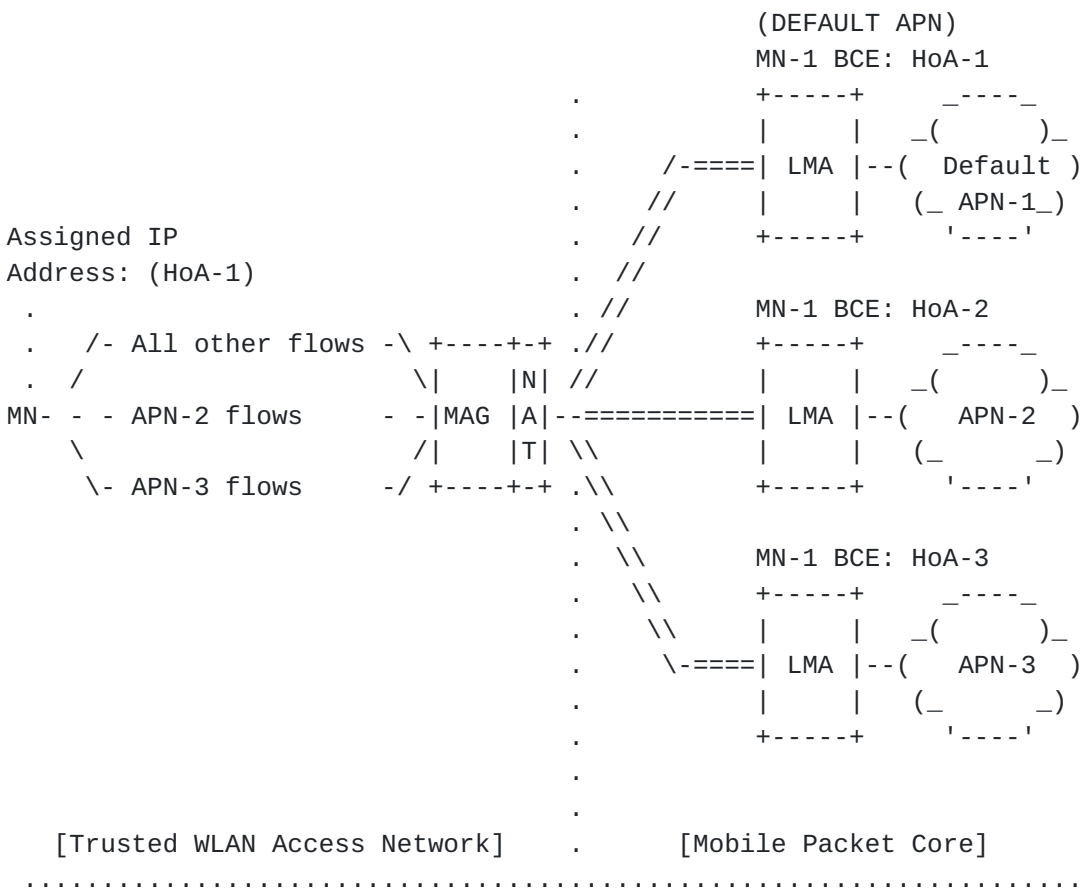


Figure 1: Multiple APN Support for Trusted WLAN Access

The mobile access gateway on detecting a new mobile node on its access link establishes bindings with the mobile node's home network

(default APN). The obtained IP address from this default APN is assigned to the WLAN interface of the mobile node over DHCP. The mobile access gateway also obtains the mobile node's policy profile, which identifies all the home networks/APN's to which the mobile node belongs. It also has knowledge on the applications hosted in the home network and the associated IP flow selectors.

The mobile node after obtaining the IPv4 address on the WLAN interface, activates all the applications and starts sending IP packets using the obtained IPv4 address. The IP flow selectors installed on the mobile access gateway identifies those application and initiates the Proxy Mobile IPv6 signaling with the respective local mobility anchor. The mobile access gateway can also choose to establish connections to all the APN's allowed for that mobile node prior to detecting any application specific flows. It maintains BUL entries for each of the sessions. However, except for the IPv4 address and the related configuration from the default APN/home network, the mobile node is not delivered any other IPv4 address from the other APN's.

The mobile access gateway installs the NAT translation rules on an APN basis. This essentially allows the mobile node's IP flows using the source address assigned by the default-APN/home network to an address assigned by the home network to which the application flows are associated to. For example, an RTP/SIP packet from the mobile node with the source address from the default APN, will get translated to the source address assigned by the LMA in the SIP APN.

IP packets from the mobile node and from the correspondent node, will be translated to use the IP address assigned by the respective APN. The translated packets are forwarded through the home network.

3.1. Potential Limitations and Workarounds

The approach specified in this document have some known limitations and can only be enabled when some assumptions are met. These limitations and the related considerations are specified in this section.

1. The mobile node is assigned a DNS server from the default-APN and all the DNS traffic will be routed to the DNS server in the default home-network. DNS is a global name space and generally there should not be any issues with DNS name resolutions for services in the other home networks. However, if a given APN/ home-network (other than the default home-network) is hosting private DNS name space, the DNS resolution requests initiated by the mobile node will always end up in the default home-network and those resolutions will be incorrect. There are clearly

approaches to deal with this problem.

* There are two potential approaches to deal with this problem. These approaches are outside the scope of this document, but few points related to those approaches are presented for further study. In both the cases, the mobile access gateway has the assumed capability to recover DNS information provisioned for that home network (or obtained using Protocol Configuration options related to primary and secondary DNS server addresses, when using 3GPP S2a interface).

* In one approach, the mobile access gateway can maintain the different DNS server configurations for the different home-networks, and create a single ordered list of DNS servers and provide it to the mobile node as part of the DHCP configuration message. Such an approach assumes that the mobile access gateway has chosen to establish connections to all the APN's allowed for that mobile node prior to detecting any application specific flows.

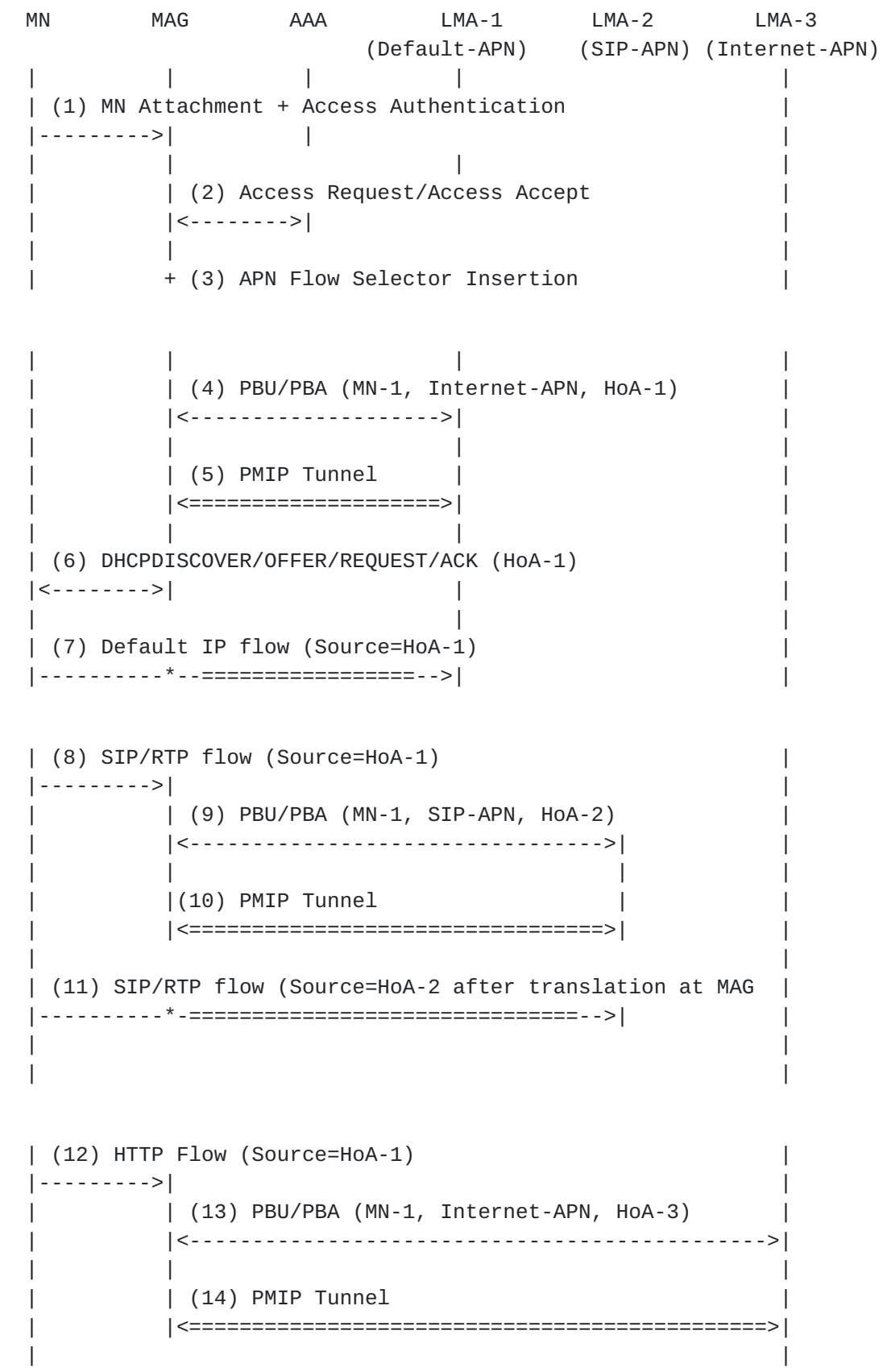
* Alternatively, the mobile access gateway can store the recovered DNS server information and only provide its own IP address as DNS server to the client. The MAG is then operable to receive DNS requests from clients and to determine to which DNS server to proxy the request. The mobile access gateway may use preference information or requested realm to select a DNS server. If the selected DNS server returns an error with unknown realm, the mobile access gateway may subsequently select an alternative DNS server.

2. If the configured APN's/home-networks are hosting a set of applications and if those applications have no unique traffic selectors that the mobile access gateway can apply and identify the IP packets in an unambiguous way, this approach will not work.

   * There is no workaround for this limitation. In such deployments, those APN's/home-networks hosting applications with no unique traffic selectors have to be excluded from multiple home network support.

4. Operational Details

Figure 2 explains the operational sequence of the Proxy Mobile IPv6 signaling message exchange between the mobile access gateway and the local mobility anchor when supporting multiple IPv4 home address support.


MN
MAG
AAA
LMA-1
(Default-APN)
LMA-2
(SIP-APN)
LMA-3
(Internet-APN)
(1) MN Attachment + Access Authentication
(2) Access Request/Access Accept
(3) APN Flow Selector Insertion
(4) PBU/PBA (MN-1, Internet-APN, HoA-1)
(5) PMIP Tunnel
(6) DHCPDISCOVER/OFFER/REQUEST/ACK (HoA-1)
(7) Default IP flow (Source=HoA-1)
(8) SIP/RTP flow (Source=HoA-1)
(9) PBU/PBA (MN-1, SIP-APN, HoA-2)
(10) PMIP Tunnel
(11) SIP/RTP flow (Source=HoA-2 after translation at MAG
(12) HTTP Flow (Source=HoA-1)
(13) PBU/PBA (MN-1, Internet-APN, HoA-3)
(14) PMIP Tunnel

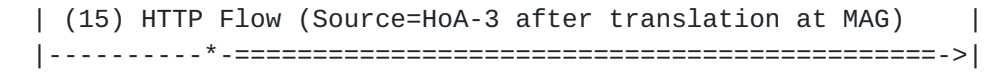


Figure 2: Exchange of IP Traffic Offload Selectors

- Step-1: The mobile node (MN1) attaches to the access link and completes the access authentication. Based on the interworking between the access authentication function (such as EAP Authenticator, or by virtue of being in the AAA path), the mobile access gateway learns the authenticated identity and the link-layer address of the mobile node.

- Step-2: The mobile access gateway obtains the mobile node's policy profile, which includes the list of home networks (APN's/Local mobility anchors that that the mobile node is allowed to access). It also includes the IP flow selectors for identifying the application traffic associated with each of those home networks.

- Step-3: The mobile access gateway installs the Policy Based Routing rules for detecting the application traffic associated with different home networks. For example, HTTP packets will be associated with the home network serving the Internet APN (LMA-3), SIP/RTP packets will be associated with the home network serving SIP APN (LMA-2), and all other IP flows will be associated with the default home APN (LMA-1). The mobile access gateway can complete the Proxy Mobile IPv6 signaling with different home networks based on the traffic detect function, or it may complete the signaling with all the home networks right after the mobile node's attachment to the access link.

- Step-4 to Step-7: The mobile access gateway completes the Proxy Mobile IPv6 signaling with the local mobility anchor (LMA-1) serving the default home APN. This is as specified in [RFC5213] and [RFC5844]. The obtained IPv4 address (HoA-1) is delivered to the mobile node over DHCPv4. This is the only IPv4 address from the home network that is assigned to the mobile node. The mobile node uses this IPv4 address as the source address with all of its applications when using the attached access technology. The mobile access gateway tunnels all the application traffic, except the application traffic associated with the other home networks, through the established Proxy Mobile IPv6 tunnel. These IP flows will not be subjected to any NAT translation treatment.

- Step-8 to Step-11: The mobile node launches a SIP application and initiates the SIP signaling. The traffic detect function on the mobile access gateway identifies this application traffic and determines that this application traffic needs to be routed to the

home network serving the SIP APN. The mobile access gateway completes the needed Proxy Mobile IPv6 signaling with the local mobility anchor (LMA-2) and obtains an IPv4 address (HoA-2) for the mobile node. It also inserts a NAT translation rule, which essentially identifies the application traffic associated with SIP and translates it to use the IP address assigned by that home network. "Application Traffic: SIP/RTP, NAT Internal IPv4 Address: HoA-1, NAT External IPv4 Address: HoA-2.

- Step-12 to Step-15: The mobile node launches a Web browser application and opens a URL link. The traffic detect function on the mobile access gateway identifies this HTTP application traffic and determines that this application traffic needs to be routed to the home network serving the Internet APN. The mobile access gateway completes the needed Proxy Mobile IPv6 signaling with the local mobility anchor (LMA-2) and obtains an IPv4 address for the mobile node. It also inserts a NAT translation rule, which essentially identifies the application traffic associated with HTTP and translates it to use the IP address assigned by that home network. "Application Traffic: Internet, NAT Internal IPv4 Address: HoA-1, NAT External IPv4 Address: HoA-3.

- The IP traffic from the mobile node belonging to different applications will now get NAT translated to use the IPv4 address assigned by the respective home network and will be routed through that network correctly. However, the application traffic belonging to the default home network (APN) does not require any NAT translation. The home network can correctly apply application specific charging, or other policy functions on the mobile node's IP traffic.

5. IANA Considerations

This document does not require any IANA actions.

6. Security Considerations

This specification does not define any new protocol extensions and therefore does not identify any specific issues on the protocol security.

When multiple APN (home network) support is enabled, per this specification, the mobile node's IP flows belonging to different applications selectively get NAT translated and it essentially introduces certain vulnerabilities which are common to any NAT deployment. These vulnerabilities and the related considerations

have been well documented in the NAT specification [RFC2663]. There are no additional considerations above and beyond what is already documented by the NAT specifications and which are unique to the approach specified in this document.

7. Acknowledgements

The authors would like to first thank 3GPP body for creating the APN concept and the associated issues for WLAN access, thus making this technical work relevant, without which the document would not have existed.

The authors would also like to thank Ivan Centeno on the importance of this use-case and the need to address this issue. Finally, the authors would like to thank Kent Leung, Rajesh Pazhyannur, Eric Hamel, Sanjay Kumar and Radhakrishna C, on the reviews related to this approach and specifically the discussions related to Split DNS, importance of requiring home-networks with non-overlapping applications.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

8.2. Informative References

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC5149] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", RFC 5149, February 2008.

[RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012.

[TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 2010.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Mark Grayson
Cisco
11 New Square Park
Bedfont Lakes, FELTHAM TW14 8HA
ENGLAND

Email: mgrayson@cisco.com

Yiu L. Lee
Comcast
One Comcast Center
Philadelphia, PA 19103
U.S.A.

Email: yiu_lee@cable.comcast.com
URI: http://www.comcast.com

Hui Deng
China Mobile
53A,Xibianmennei Ave.
Xuanwu District, Beijing 100053
China

Email: denghui02@gmail.com

Hidetoshi Yokota
KDDI Lab
2-1-15 Ohara
Saitama, Fujimino 356-8502
Japan

Email: yokota@kddilabs.jp