V6OPS Working Group
Internet-Draft
Intended status: Informational
Expires: August 5, 2015

D. Binet
M. Boucadair
France Telecom
A. Vizdal
Deutsche Telekom AG
G. Chen
China Mobile
N. Heatley
EE
R. Chandler
eircom | meteor
February 1, 2015

An Internet Protocol Version 6 (IPv6) Profile for 3GPP Mobile Devices
draft-ietf-v6ops-mobile-device-profile-16

Abstract

This document defines a profile that is a superset of that of the connection to IPv6 cellular networks defined in the IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts document. This document defines an IPv6 profile that a number of operators recommend in order to connect 3GPP mobile devices to an IPv6-only or dual-stack wireless network (including 3GPP cellular network and IEEE 802.11 network).

Both hosts and devices with capability to share their WAN (Wide Area Network) connectivity are in scope.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

IPv6 deployment in 3GPP mobile networks is the only perennial solution to the exhaustion of IPv4 addresses in those networks. Several mobile operators have already deployed IPv6 [RFC2460] or are in the pre-deployment phase. One of the major hurdles as perceived by some mobile operators is the availability of non-broken IPv6 implementation in mobile devices.

[RFC7066] lists a set of features to be supported by cellular hosts to connect to 3GPP mobile networks. In the light of recent IPv6 production deployments, additional features to facilitate IPv6-only deployments while accessing IPv4-only service are to be considered.

This document defines an IPv6 profile for mobile devices listing specifications produced by various Standards Developing Organizations (in particular 3GPP and IETF). The objectives of this effort are:

1. List in one single document a comprehensive list of IPv6 features for a mobile device, including both IPv6-only and dual-stack mobile deployment contexts. These features cover various network types such as GPRS (General Packet Radio Service), EPC (Evolved Packet Core) or IEEE 802.11 network.

2. Help Operators with the detailed device requirement list preparation (to be exchanged with device suppliers). This is also a contribution to harmonize Operators' requirements towards device vendors.

3. Vendors to be aware of a set of features to allow for IPv6 connectivity and IPv4 service continuity (over an IPv6-only transport).

The recommendations do not include 3GPP release details. For more information on the 3GPP releases detail, the reader may refer to Section 6.2 of [RFC6459].

Some of the features listed in this profile document require to activate dedicated functions at the network side. It is out of scope of this document to list these network-side functions.

A detailed overview of IPv6 support in 3GPP architectures is provided in [RFC6459].

1.1. Terminology

This document makes use of the terms defined in [RFC6459]. In addition, the following terms are used:

- "3GPP cellular host" (or cellular host for short) denotes a 3GPP device which can be connected to 3GPP mobile networks or IEEE 802.11 networks.

- "3GPP cellular device" (or cellular device for short) refers to a cellular host which supports the capability to share its WAN (Wide Area Network) connectivity.

- "Cellular host" and "mobile host" are used interchangeably.

- "Cellular device" and "mobile device" are used interchangeably.

PREFIX64 denotes an IPv6 prefix used to build IPv4-converted IPv6 addresses [RFC6052].

1.2. Scope

A 3GPP mobile network can be used to connect various user equipments such as a mobile telephone, a CPE (Customer Premises Equipment) or a machine-to-machine (M2M) device. Because of this diversity of terminals, it is necessary to define a set of IPv6 functionalities valid for any node directly connecting to a 3GPP mobile network. This document describes these functionalities.

This document is structured to provide the generic IPv6 recommendations which are valid for all nodes, whatever their function (e.g., host or CPE) or service (e.g., Session Initiation Protocol (SIP, [RFC3261])) capability. The document also contains sections covering specific functionalities for devices providing some LAN functions (e.g., mobile CPE or broadband dongles).

The recommendations listed below are valid for both 3GPP GPRS and 3GPP EPS (Evolved Packet System) access. For EPS, PDN-Connection term is used instead of PDP-Context.

This document identifies also some WLAN-related IPv6 recommendations. Other non-3GPP accesses [TS.23402] are out of scope of this document.

This profile is a superset of that of the IPv6 profile for 3GPP Cellular Hosts [RFC7066], which is in turn a superset of IPv6 Node Requirements [RFC6434]. It targets cellular nodes, including GPRS, EPC (Evolved Packet Core) and IEEE 802.11 networks, that require features to ensure IPv4 service delivery over an IPv6-only transport in addition to the base IPv6 service. Moreover, this profile covers cellular CPEs that are used in various deployments to offer fixed-like services. Recommendations inspired from real deployment experiences (e.g., roaming) are included in this profile. Also, this profile sketches recommendations for the sake of deterministic behaviors of cellular devices when the same configuration information is received over several channels.

For conflicting recommendations in [RFC7066] and [RFC6434] (e.g., Neighbor Discovery Protocol), this profile adheres to [RFC7066]. Indeed, the support of Neighbor Discovery Protocol is mandatory in 3GPP cellular environment as it is the only way to convey IPv6 prefix towards the 3GPP cellular device. In particular, MTU (Maximum Transmission Unit) communication via Router Advertisement must be supported since many 3GPP networks do not have a standard MTU setting.

This profile uses a stronger language for the support of Prefix Delegation compared to [RFC7066]. The main motivation is that cellular networks are more and more perceived as an alternative to fixed networks for home IP-based services delivery; especially with the advent of smartphones and 3GPP data dongles. There is a need for an efficient mechanism to assign shorter prefix than /64 to cellular hosts so that each LAN segment can get its own /64 prefix and multi-link subnet issues to be avoided. The support of this functionality in both cellular and fixed networks is key for fixed-mobile convergence.

This document is not a standard, and conformance with it is not required in order to claim conformance with IETF standards for IPv6. The support of the full set of features may not be required in some deployment contexts. The authors believe that the support of a subset of the features included in this protocol may lead to degraded level of service in some deployment contexts.

2. Connectivity Recommendations

This section identifies the main connectivity recommendations to be followed by a cellular host to attach to a network using IPv6. Both dual-stack and IPv6-only deployment models are considered. IPv4 service continuity features are listed in this section because these are critical for Operators with an IPv6-only deployment model.

C_REC#1: In order to allow each operator to select their own strategy regarding IPv6 introduction, the cellular host must support both IPv6 and IPv4v6 PDP-Contexts [TS.23060]. Both IPv6 and IPv4v6 PDP-Contexts must be supported. IPv4, IPv6 or IPv4v6 PDP-Context request acceptance depends on the cellular network configuration.

C_REC#2: The cellular host must comply with the behavior defined in [TS.23060] [TS.23401] [TS.24008] for requesting a PDP-Context type. In particular, the cellular host must request by default an IPv6 PDP-Context if the cellular host is IPv6-only and requesting an IPv4v6 PDP-Context if the cellular host is dual-stack or when the cellular host is not aware of connectivity types requested by devices connected to it (e.g., cellular host with LAN capabilities as discussed in Section 4):

* If the requested IPv4v6 PDP-Context is not supported by the network, but IPv4 and IPv6 PDP types are allowed, then the cellular host will be configured with an IPv4 address or an IPv6 prefix by the network. It must initiate another PDP-Context activation in addition to

the one already activated for a given APN (Access Point Name).

* If the requested PDP type and subscription data allows only one IP address family (IPv4 or IPv6), the cellular host must not request a second PDP-Context to the same APN for the other IP address family.

The text above focuses on the specification part which explains the behavior for requesting IPv6-related PDP-Context(s). Understanding this behavior is important to avoid having broken IPv6 implementations in cellular devices.

C_REC#3: The cellular host must support the PCO (Protocol Configuration Options) [TS.24008] to retrieve the IPv6 address(es) of the Recursive DNS server(s).

In-band signaling is a convenient method to inform the cellular host about various services, including DNS server information. It does not require any specific protocol to be supported and it is already deployed in IPv4 cellular networks to convey such DNS information.

C_REC#4: The cellular host must support IPv6 aware Traffic Flow Templates (TFT) [TS.24008].

Traffic Flow Templates are employing a packet filter to couple an IP traffic with a PDP-Context. Thus a dedicated PDP-Context and radio resources can be provided by the cellular network for certain IP traffic.

C_REC#5: If the cellular host receives the DNS information in several channels for the same interface, the following preference order must be followed:

1. PCO

2. RA

3. DHCPv6

C_REC#6: The cellular host must be able to be configured to limit PDP type(s) for a given APN. The default mode is to allow all supported PDP types. Note, C_REC#2 discusses the default behavior for requesting PDP-Context type(s).

This feature is useful to drive the behavior of the UE to be aligned with: (1) service-specific constraints such as the use of IPv6-only for VoLTE (Voice over LTE), (2) network conditions with regards to the support of specific PDP types (e.g., IPv4v6 PDP-Context is not supported), (3) IPv4 sunset objectives, (4) subscription data, etc.

C_REC#7: Because of potential operational deficiencies to be experienced in some roaming situations, the cellular host must be able to be configured with a home IP profile and a roaming IP profile. The aim of the roaming profile is to limit the PDP type(s) requested by the cellular host when out of the home network. Note that distinct PDP type(s) and APN(s) can be configured for home and roaming cases.

C_REC#8: In order to ensure IPv4 service continuity in an IPv6-only deployment context, the cellular host should support a method to locally construct IPv4-embedded IPv6 addresses [RFC6052]. A method to learn PREFIX64 should be supported by the cellular host.

This solves the issue when applications use IPv4 referrals on IPv6-only access networks.

In PCP-based environments, cellular hosts should follow [RFC7225] to learn the IPv6 Prefix used by an upstream PCP-controlled NAT64 device. If PCP is not enabled, the cellular host should implement the method specified in [RFC7050] to retrieve the PREFIX64.

C_REC#9: In order to ensure IPv4 service continuity in an IPv6-only deployment context, the cellular host should implement the Customer Side Translator (CLAT, [RFC6877]) function which is compliant with [RFC6052][RFC6145][RFC6146].

CLAT function in the cellular host allows for IPv4-only application and IPv4-referals to work on an IPv6-only connectivity. CLAT function requires a NAT64 capability [RFC6146] in the core network.

The IPv4 Service Continuity Prefix used by CLAT is defined in [RFC7335].

2.1. WLAN Connectivity Recommendations

It is increasingly common for cellular hosts have a WLAN interface in addition to their cellular interface. These hosts are likely to be connected to private or public hotspots. Below are listed some generic recommendations:

W_REC#1: IPv6 must be supported on the WLAN interface. In particular, WLAN interface must behave properly when only an IPv6 connectivity is provided.

Some tests revealed that IPv4 configuration is required to enable IPv6-only connectivity. Indeed, some cellular handsets can access a WLAN IPv6-only network by configuring first a static IPv4 address. Once the device is connected to the network and the wlan0 interface got an IPv6 global address, the IPv4 address can be deleted from the configuration. This avoids the device to ask automatically for a DHCPv4 server, and allows to connect to IPv6-only networks. Failing to configure an IPv4 address on the interface must not prohibit using IPv6 on the same interface.

W_REC#2: If the device receives the DNS information in several channels for the same interface, the following preference order must be followed:

1. RA

2. DHCPv6

3. Advanced Recommendations

This section identifies a set of advanced recommendations to fulfill requirements of critical services such as VoLTE.

A_REC#1: The cellular host must support ROHC RTP Profile (0x0001) and ROHC UDP Profile (0x0002) for IPv6 ([RFC5795]). Other ROHC profiles may be supported.

Bandwidth in cellular networks must be optimized as much as possible. ROHC provides a solution to reduce bandwidth consumption and to reduce the impact of having bigger packet headers in IPv6 compared to IPv4.

"RTP/UDP/IP" ROHC profile (0x0001) to compress RTP packets and "UDP/IP" ROHC profile (0x0002) to compress RTCP packets are required for Voice over LTE (VoLTE) by

IR.92.4.0 section 4.1 [IR92]. Note, [IR92] indicates also the host must be able to apply the compression to packets that are carried over the radio bearer dedicated for the voice media.

A_REC#2: The cellular host should support PCP [RFC6887].

The support of PCP is seen as a driver to save battery consumption exacerbated by keepalive messages. PCP also gives the possibility of enabling incoming connections to the cellular device. Indeed, because several stateful devices may be deployed in wireless networks (e.g., NAT and/or Firewalls), PCP can be used by the cellular host to control network-based NAT and Firewall functions which will reduce per-application signaling and save battery consumption.

According to [Power], the consumption of a cellular device with a keep-alive interval equal to 20 seconds (that is the default value in [RFC3948] for example) is 29 mA (2G)/34 mA (3G). This consumption is reduced to 16 mA (2G)/24 mA (3G) when the interval is increased to 40 seconds, to 9.1 mA (2G)/16 mA (3G) if the interval is equal to 150 seconds, and to 7.3 mA (2G)/14 mA (3G) if the interval is equal to 180 seconds. When no keep-alive is issued, the consumption would be 5.2 mA (2G)/6.1 mA (3G). The impact of keepalive messages would be more severe if multiple applications are issuing those messages (e.g., SIP, IPsec, etc.).

A_REC#3: In order for host-based validation of DNS Security Extensions (DNSSEC) to continue to function in an IPv6-only with NAT64 deployment context, the cellular host should embed a DNS64 function ([RFC6147]).

This is called "DNS64 in stub-resolver mode" in [RFC6147].

As discussed in Section 5.5 of [RFC6147], a security-aware and validating host has to perform the DNS64 function locally.

Because synthetic AAAA records cannot be successfully validated in a host, learning the PREFIX64 used to construct IPv4-converted IPv6 addresses allows the use of DNSSEC [RFC4033] [RFC4034], [RFC4035]. Means to configure or discover a PREFIX64 are required on the cellular device as discussed in C_REC#8.

[RFC7051] discusses why a security-aware and validating host has to perform the DNS64 function locally and why it has to be able to learn the proper PREFIX64(s).

A_REC#4: When the cellular host is dual-stack connected (i.e., configured with an IPv4 address and IPv6 prefix), it should support means to prefer native IPv6 connection over connection established through translation devices (e.g., NAT44 and NAT64).

When both IPv4 and IPv6 DNS servers are configured, a dual-stack host must contact first its IPv6 DNS server.

Cellular hosts should follow the procedure specified in [RFC6724] for source address selection.

A_REC#5: The cellular host should support Happy Eyeballs procedure defined in [RFC6555].

4. Recommendations for Cellular Devices with LAN Capabilities

This section focuses on cellular devices (e.g., CPE, smartphones, or dongles with tethering features) which provide IP connectivity to other devices connected to them. In such case, all connected devices are sharing the same 2G, 3G or LTE connection. In addition to the generic recommendations listed in Section 2, these cellular devices have to meet the recommendations listed below.

L_REC#1: The cellular device must support Prefix Delegation capabilities [RFC3633] and must support Prefix Exclude Option for DHCPv6-based Prefix Delegation as defined in [RFC6603]. Particularly, it must behave as a Requesting Router.

Cellular networks are more and more perceived as an alternative to fixed networks for home IP-based services delivery; especially with the advent of smartphones and 3GPP data dongles. There is a need for an efficient mechanism to assign shorter prefix than /64 to cellular hosts so that each LAN segment can get its own /64 prefix and multi-link subnet issues to be avoided.

In case a prefix is delegated to a cellular host using DHCPv6, the cellular device will be configured with two prefixes:

(1) one for 3GPP link allocated using SLAAC mechanism and

(2) another one delegated for LANs acquired during Prefix Delegation operation.

Note that the 3GPP network architecture requires both the WAN (Wide Area Network) and the delegated prefix to be aggregatable, so the subscriber can be identified using a single prefix.

Without the Prefix Exclude Option, the delegating router (GGSN/PGW) will have to ensure [RFC3633] compliancy (e.g., halving the delegated prefix and assigning the WAN prefix out of the 1st half and the prefix to be delegated to the terminal from the 2nd half).

Because Prefix Delegation capabilities may not be available in some attached networks, L_REC#3 is strongly recommended to accommodate early deployments.

L_REC#2: The cellular CPE must be compliant with the requirements specified in [RFC7084].

There are several deployments, particularly in emerging countries, that relies on mobile networks to provide broadband services (e.g., customers are provided with mobile CPEs).

Note, this profile does not require IPv4 service continuity techniques listed in [RFC7084] because those are specific to fixed networks. IPv4 service continuity techniques specific to the mobile networks are included in this profile.

L_REC#3: For deployments requiring to share the same /64 prefix, the cellular device should support [RFC7278] to enable sharing a /64 prefix between the 3GPP interface towards the GGSN/PGW (WAN interface) and the LAN interfaces.

Prefix Delegation (refer to L_REC#1) is the target solution for distributing prefixes in the LAN side but, because the device may attach to earlier 3GPP release networks, a mean to share a /64 prefix is also recommended [RFC7278].

[RFC7278] must be invoked only if Prefix Delegation is not in use.

L_REC#4: In order to ensure IPv4 service continuity in an IPv6-only deployment context, the cellular device should support the Customer Side Translator (CLAT) [RFC6877].

Various IP devices are likely to be connected to cellular device, acting as a CPE. Some of these devices can be dual-stack, others are IPv6-only or IPv4-only. IPv6-only connectivity for cellular device does not allow IPv4-only sessions to be established for hosts connected on the LAN segment of cellular devices.

In order to allow IPv4 sessions establishment initiated from devices located on LAN segment side and target IPv4 nodes, a solution consists in integrating the CLAT function in the cellular device. As elaborated in Section 2, the CLAT function allows also IPv4 applications to continue running over an IPv6-only host.

The IPv4 Service Continuity Prefix used by CLAT is defined in [RFC7335].

L_REC#5: If a RA MTU is advertised from the 3GPP network, the cellular device should relay that upstream MTU information to the downstream attached LAN devices in RA.

Receiving and relaying RA MTU values facilitates a more harmonious functioning of the mobile core network where end nodes transmit packets that do not exceed the MTU size of the mobile network's GTP tunnels.

[TS.23060] indicates providing a link MTU value of 1358 octets to the 3GPP cellular device will prevent the IP layer fragmentation within the transport network between the cellular device and the GGSN/PGW.

5. APIs & Applications Recommendations

The use of address family dependent APIs (Application Programming Interfaces) or hard-coded IPv4 address literals may lead to broken applications when IPv6 connectivity is in use. This section identifies a set of recommendations aiming to minimize broken applications when the cellular device is attached to an IPv6 network.

APP_REC#1: Name resolution libraries must support both IPv4 and IPv6.

In particular, the cellular host must support [RFC3596].

APP_REC#2: Applications provided by the mobile device vendor must be independent of the underlying IP address family.

This means applications must be IP version agnostic.

APP_REC#3: Applications provided by the mobile device vendor that use Uniform Resource Identifiers (URIs) must follow [RFC3986] and its updates. For example, SIP applications must follow the correction defined in [RFC5954].

6. Security Considerations

The security considerations identified in [RFC7066] and [RFC6459] are to be taken into account.

In the case of cellular devices that provide LAN features, compliance with L_REC#2 entails compliance with [RFC7084], which in turn recommends compliance with Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service [RFC6092]. Therefore, the security considerations in Section 6 of [RFC6092] are relevant. In particular, it bears repeating here that the true impact of stateful filtering may be a reduction in security, and that IETF make no statement, expressed or implied, as to whether using the capabilities described in any of these documents ultimately improves security for any individual users or for the Internet community as a whole.

The cellular host must be able to generate IPv6 addresses which preserve privacy. The activation of privacy extension (e.g., using [RFC7217]) makes it more difficult to track a host over time when compared to using a permanent Interface Identifier. Tracking a host is still possible based on the first 64 bits of the IPv6 address. Means to prevent against such tracking issues may be enabled in the network side. Note, privacy extensions are required by regulatory bodies in some countries.

Host-based validation of DNSSEC is discussed in A_REC#3 (see Section 3).

7. IANA Considerations

This document does not require any action from IANA.

8. Acknowledgements

Many thanks to C. Byrne, H. Soliman, H. Singh, L. Colliti, T. Lemon, B. Sarikaya, M. Mawatari, M. Abrahamsson, P. Vickers, V.

Kuarsingh, E. Kline, S. Josefsson, A. Baryun, J. Woodyatt, T. Kossut, and B. Stark for the discussion in the v6ops mailing list.

Thanks to A. Farrel, B. Haberman and K. Moriarty for the comments during the IESG review.

Special thanks to T. Savolainen, J. Korhonen, J. Jaeggli, and F. Baker for their detailed reviews and comments.

9. References

9.1. Normative References

[IR92] GSMA, "IR.92.V4.0 - IMS Profile for Voice and SMS", March 2011, <http://www.gsma.com/newsroom/ir-92-v4-0-ims-profile-for-voice-and-sms>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC5795] Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, March 2010.

[RFC5954] Gurbani, V., Carpenter, B., and B. Tate, "Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261", RFC 5954, August 2010.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6603] Korhonen, J., Savolainen, T., Krishnan, S., and O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", RFC 6603, May 2012.

[RFC7066] Korhonen, J., Arkko, J., Savolainen, T., and S. Krishnan, "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts", RFC 7066, November 2013.

[TS.23060] 3GPP, "General Packet Radio Service (GPRS); Service description; Stage 2", September 2011, <http://www.3gpp.org/DynaReport/23060.htm>.

[TS.23401] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", September 2011, <http://www.3gpp.org/DynaReport/23401.htm>.

[TS.24008] 3GPP, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3", June 2011, <http://www.3gpp.org/DynaReport/24008.htm>.

9.2. Informative References

[Power] Haverinen, H., Siren, J., and P. Eronen, "Energy Consumption of Always-On Applications in WCDMA Networks", April 2007, <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4212635>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC6092] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.

[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.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", RFC 6555, April 2012.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, April 2013.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013.

[RFC7050] Savolainen, T., Korhonen, J., and D. Wing, "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis", RFC 7050, November 2013.

[RFC7051] Korhonen, J. and T. Savolainen, "Analysis of Solution Proposals for Hosts to Learn NAT64 Prefix", RFC 7051, November 2013.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, November 2013.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, April 2014.

[RFC7225] Boucadair, M., "Discovering NAT64 IPv6 Prefixes Using the Port Control Protocol (PCP)", RFC 7225, May 2014.

[RFC7278] Byrne, C., Drown, D., and A. Vizdal, "Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link", RFC 7278, June 2014.

[RFC7335] Byrne, C., "IPv4 Service Continuity Prefix", RFC 7335, August 2014.

[TS.23402] 3GPP, "Architecture enhancements for non-3GPP accesses", September 2011, <http://www.3gpp.org/DynaReport/23402.htm>.

Authors' Addresses

David Binet
France Telecom
Rennes
France

EMail: david.binet@orange.com

Mohamed Boucadair
France Telecom
Rennes 35000
France

EMail: mohamed.boucadair@orange.com

Ales Vizdal
Deutsche Telekom AG

EMail: ales.vizdal@t-mobile.cz

Gang Chen
China Mobile

EMail: phdgang@gmail.com

Nick Heatley
EE
The Point, 37 North Wharf Road,
London W2 1AG
U.K

EMail: nick.heatley@ee.co.uk

Ross Chandler
eircom | meteor
1HSQ
St. John's Road
Dublin 8
Ireland

EMail: ross@eircom.net