Independent Submission
Request for Comments: 7849
Category: Informational
ISSN: 2070-1721

D. Binet
M. Boucadair
Orange
A. Vizdal
Deutsche Telekom AG
G. Chen
China Mobile
N. Heatley
EE
R. Chandler
eircom | meteor
D. Michaud
Rogers Communications
D. Lopez
Telefonica I+D
W. Haeffner
Vodafone

May 2016

An IPv6 Profile for 3GPP Mobile Devices

Abstract

This document defines a profile that is a superset of the connection to IPv6 cellular networks defined in the IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts document. This document defines a profile that is a superset of the connections to IPv6 cellular networks defined in "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts" (RFC 7066).

Both mobile hosts and mobile devices with the capability to share their 3GPP mobile connectivity are in scope.

IESG Note

The consensus-based IETF description of IPv6 functionality for cellular hosts is described in RFC 7066.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

IPv6 deployment in 3GPP mobile networks is the only viable 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 lack of availability of working IPv6 implementation in mobile devices (e.g., Section 3.3 of [OECD]).

[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 services should be considered.

This document fills this void. Concretely, this document lists means to ensure IPv4 service over an IPv6-only connectivity given the adoption rate of this model by mobile operators. Those operators require that no service degradation is experienced by customers serviced with an IPv6-only model compared to the level of service of customers with legacy IPv4-only devices.

This document defines an IPv6 profile for mobile devices listing specifications produced by various Standards Developing Organizations (including 3GPP, IETF, and the Global System for Mobile Communications Association (GSMA)). The objectives of this effort are as follows:

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 packet core architectures such as General Packet Radio Service (GPRS) or Evolved Packet Core (EPC).

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. Inform vendors 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 release details, the reader may refer to Section 6.2 of [RFC6459]. More details can be found at [R3GPP].

Some of the features listed in this profile document could require that dedicated functions be activated 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]. IPv6-only considerations in mobile networks are further discussed in [RFC6342].

This document is organized as follows:

- Section 2 lists generic recommendations, including functionalities to provide IPv4 service over an IPv6-only connectivity.
- Section 3 enumerates a set of recommendations for cellular devices with Local Area Network (LAN) capabilities (e.g., Customer Edge (CE) routers with cellular access link, dongles with tethering features).
- Section 4 identifies a set of advanced recommendations to fulfill requirements of critical services such as VoLTE (Voice over LTE).

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 that can be connected to 3GPP mobile networks.
- 3GPP cellular device (or "cellular device" for short): refers to a cellular host that supports the capability to share its 3GPP mobile connectivity.
- IPv4 service continuity: denotes the features used to provide access to IPv4-only services to customers serviced with an IPv6-only connectivity. A typical example of IPv4 service continuity technique is Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers (NAT64) [RFC6146].

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 Equipment (UE) such as a mobile telephone or a CE router. 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.

The machine-to-machine (M2M) devices profile is out of scope.

This document is structured to provide the generic IPv6 recommendations that are valid for all nodes, whatever their function (e.g., host or CE router) 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 CE router or broadband dongles).

The recommendations listed below are valid for both 3GPP GPRS and 3GPP Evolved Packet System (EPS). For EPS, the term "PDN-Connection" is used instead of PDP-Context. 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 and EPC, that require features to ensure IPv4 service delivery over an IPv6-only transport in addition to the base IPv6 service. Moreover, this profile also covers cellular CE routers that are used in various mobile broadband deployments. 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 an IPv6 prefix towards the 3GPP cellular device. In particular, Maximum Transmission Unit (MTU) communication via Router Advertisement (RA) 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 larger prefixes 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.

The use of address-family-dependent Application Programming Interfaces (APIs) or hard-coded IPv4 address literals may lead to broken applications when IPv6 connectivity is in use. As such, means to minimize broken applications when the cellular host is attached to an IPv6-only network should be encouraged. Particularly, (1) name resolution libraries (e.g., [RFC3596]) must support both IPv4 and IPv6; (2) applications must be independent of the underlying IP address family; and (3) applications relying upon Uniform Resource Identifiers (URIs) must follow [RFC3986] and its updates. Note, some IETF specifications (e.g., SIP [RFC3261]) contains broken IPv6 Augmented Backus-Naur Form (ABNF) and rules to compare URIs with embedded IPv6 addresses; fixes (e.g., [RFC5954]) must be used instead.

The recommendations included in each section are listed in a priority order.

This document is not a standard, and conformance with it is not required in order to claim conformance with IETF standards for IPv6. Compliance with this profile does not require the support of all enclosed items. Obviously, the support of the full set of features may not be required in some deployment contexts. However, the authors believe that not supporting relevant features included in this profile (e.g., Customer-Side Translator (CLAT) [RFC6877]) may lead to a degraded level of service.

2. Connectivity Recommendations

This section identifies the main connectivity recommendations to be followed by a cellular host to attach to a network using IPv6 in addition to what is defined in [RFC6434] and [RFC7066]. 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. These recommendations apply also for cellular devices (see Section 3).

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].

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], and [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 request 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., a cellular host with LAN capabilities as discussed in Section 3):

* 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 of the other address family in addition to the one already activated for a given Access Point Name (APN). The purpose of initiating a second PDP-Context is to achieve dual-stack connectivity by means of two PDP-Contexts.

* If the subscription data or network configuration 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 network informs the cellular host about allowed Packet Data Protocol (PDP) types by means of Session Management (SM) cause codes. In particular, the following cause codes can be returned:

* cause #50 "PDP type IPv4 only allowed" - This cause code is used by the network to indicate that only PDP type IPv4 is allowed for the requested Public Data Network (PDN) connectivity.

* cause #51 "PDP type IPv6 only allowed" - This cause code is used by the network to indicate that only PDP type IPv6 is allowed for the requested PDN connectivity.

* cause #52 "single address bearers only allowed" - This cause code is used by the network to indicate that the requested PDN connectivity is accepted with the restriction that only single IP version bearers are allowed.

The text above focuses on the specification (an excerpt from [TS.23060], [TS.23401], and [TS.24008]) that explains the behavior for requesting IPv6-related PDP-Context(s).

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

The 3GPP network communicates parameters by means of the protocol configuration options information element when activating, modifying, or deactivating a PDP-Context. PCO is a convenient method to inform the cellular host about various services, including DNS server information. It does not require additional protocol to be supported by the cellular host 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 (TFTs) [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

The purpose of this recommendation is to guarantee for a deterministic behavior to be followed by all cellular hosts when the DNS information is received in various channels.

C_REC#6: Because of potential operational deficiencies to be experienced in some roaming situations, the cellular host must be able to be configured with a home PDP-Context type(s) and a roaming PDP-Context type(s). The purpose 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.

A detailed analysis of roaming failure cases is included in [RFC7445].

The configuration can be either local to the device or be managed dynamically using, for example, Open Mobile Alliance (OMA) management. The support of dynamic means is encouraged.

C_REC#7: In order to ensure IPv4 service continuity in an IPv6-only deployment context, the cellular host should support a method to learn PREFIX64(s).

In the context of NAT64, IPv6-enabled applications relying on address referrals will fail because an IPv6-only client will not be able to make use of an IPv4 address received in a referral. This feature allows for solving the referral problem (because an IPv6-enabled application can construct IPv4-embedded IPv6 addresses [RFC6052]) and, also, for distinguishing between IPv4-converted IPv6 addresses and native IPv6 addresses.

In other words, this feature contributes to offload both the CLAT module and NAT64 devices. Refer to Section 3 of [RFC7051] for an inventory of the issues related to the discovery of PREFIX64(s).

In environments based on the Port Control Protocol (PCP), 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#8: In order to ensure IPv4 service continuity in an IPv6-only deployment context, the cellular host should implement the CLAT [RFC6877] function in compliance with [RFC6052], [RFC6145], and [RFC6146].

The CLAT function in the cellular host allows for IPv4-only application and IPv4 referrals to work on an IPv6-only connectivity. The more applications are address family independent, the less the CLAT function is solicited. The CLAT function requires a NAT64 capability [RFC6146] in the network.

The cellular host should only invoke CLAT in the absence of IPv4 connectivity on the cellular side, i.e., when the network does not assign an IPv4 address on the

cellular interface. Note, NAT64 assumes an IPv6-only mode [RFC6146].

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

CLAT and/or NAT64 do not interfere with native IPv6 communications.

CLAT may not be required in some contexts, e.g., if other solutions such as Bump-in-the-Host (BIH) [RFC6535] are supported.

The cellular device can act as a CE router connecting various IP hosts on a LAN segment; this is also the case with using WLAN (Wireless LAN) tethering or a WLAN hotspot from the cellular device. Some of these IP hosts can be dual-stack, others are IPv6-only or IPv4-only. IPv6-only connectivity on the cellular device does not allow IPv4-only sessions to be established for hosts connected on the LAN segment of the cellular device. IPv4 session establishment initiated from hosts located on the LAN segment side and destined for IPv4 nodes must be maintained. A solution is to integrate the CLAT function to the LAN segment in the cellular device.

C_REC#9: The cellular host may 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, (2) network conditions with regard to the support of specific PDP types (e.g., IPv4v6 PDP-Context is not supported), (3) IPv4 sunset objectives, (4) subscription data, etc.

Note, a cellular host changing its connection between an IPv6-specific APN and an IPv4-specific APN will interrupt related network connections. This may be considered as a brokenness situation by some applications.

The configuration can be either local to the device or be managed dynamically using, for example, OMA management. The support of dynamic means is encouraged.

3. Recommendations for Cellular Devices with LAN Capabilities

This section focuses on cellular devices (e.g., CE routers, smartphones, or dongles with tethering features) that provide IP connectivity to other devices connected to them. In this 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: For deployments that require that the same /64 prefix be shared, the cellular device should support [RFC7278] to enable sharing a /64 prefix between the LAN and the WAN interfaces. The WAN interface is the one towards the Gateway GPRS Support Node (GGSN) / Packet Data Network Gateway (PGW).

Prefix Delegation (refer to L_REC#2) is the target solution for distributing prefixes in the LAN side but, because the device may attach to earlier 3GPP release networks, a means to share a /64 prefix is also recommended [RFC7278].

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

L_REC#2: The cellular device must support Prefix Delegation capabilities [RFC3633] and must support the 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 broadband 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 larger prefixes (other than /64s) 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 the 3GPP link allocated using the Stateless Address Autoconfiguration (SLAAC) mechanism and

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

Note that the 3GPP network architecture requires both the WAN 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 compliance with [RFC3633] (e.g., halving the delegated prefix and assigning the WAN prefix out of the first half and the prefix to be delegated to the terminal from the second half).

Because Prefix Delegation capabilities may not be available in some attached networks, L_REC#1 is strongly recommended to accommodate early deployments.

L_REC#3: The cellular CE router must be compliant with the requirements specified in [RFC7084].

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

Note, this profile does not require IPv4 service continuity techniques listed in Section 4.4 of [RFC7084] because those are specific to fixed networks. IPv4 service continuity techniques specific to the mobile networks are included in this profile.

This recommendation does not apply to handsets with tethering capabilities; it is specific to cellular CE routers in order to ensure the same IPv6 functional parity for both fixed and cellular CE routers. Note, modern CE routers are designed with advanced functions such as link aggregation that consists in optimizing the network usage by aggregating the connectivity resources offered via various interfaces (e.g., Digital Subscriber Line (DSL), LTE, WLAN, etc.) or offloading the traffic via a subset of interfaces. Ensuring IPv6 feature parity among these interface types is important for the sake of specification efficiency, service design simplification, and validation effort optimization.

L_REC#4: If an RA MTU is advertised from the 3GPP network, the cellular device should send RAs to the downstream attached LAN devices with the same MTU as seen on the mobile interface.

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 tunnels that use the GPRS Tunneling Protocol (GTP).

[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. More details about link MTU considerations can be found in Annex C of [TS.23060].

4. Advanced Recommendations

This section identifies a set of advanced recommendations to fulfill requirements of critical services such as VoLTE. These recommendations apply for mobile hosts, including mobile devices.

A_REC#1: The cellular host must support the RObust Header Compression (ROHC) RTP Profile (0x0001) and the 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.

The "RTP/UDP/IP" ROHC profile (0x0001) to compress RTP packets and the "UDP/IP" ROHC profile (0x0002) to compress Real-time Transport Control Protocol (RTCP) packets are required for VoLTE by Section 4.1 of IR.92.7.0 [IR92]. Note, [IR92] indicates that the host must be able to apply the compression to packets that are carried over the voice-media-dedicated radio bearer.

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 keep-alive 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., NAT64 and/or IPv6 Firewalls), PCP can be used by the cellular host to control network-based NAT64 and IPv6 Firewall functions that 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 (which 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.).

Deploying PCP allows cellular hosts to manage protocols that convey IP addresses and/or port numbers (see Section 2.2 of [RFC6889]) without requiring Application Level Gateways (ALGs) to be enabled at the network side (e.g., NAT64). Avoiding soliciting ALGs makes it easier to develop a service without any adherence with the underlying transport network.

A_REC#3: In order for host-based validation of DNS Security Extensions (DNSSEC) to continue to function in an IPv6-only connectivity 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#7.

[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 a native IPv6 connection over a connection established through translation devices (e.g., NAT44 and NAT64).

When both IPv4 and IPv6 DNS servers are configured, a dual-stack host must first contact its IPv6 DNS server. This preference allows it to offload IPv4-only DNS servers.

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

5. Security Considerations

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

In the case of cellular CE routers, compliance with L_REC#3 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 the IETF makes 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 that preserve privacy. The activation of the 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 4).

6. References

6.1. Normative References

[IR92] GSMA, "IMS Profile for Voice and SMS", Official Document IR.92 - IMS Profile for Voice and SMS, V7.0, March 2013, <http://www.gsma.com/newsroom/wp-content/uploads/2013/04/IR.92-v7.0.pdf>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, DOI 10.17487/RFC3596, October 2003, <http://www.rfc-editor.org/info/rfc3596>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <http://www.rfc-editor.org/info/rfc3633>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC5795] Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, DOI 10.17487/RFC5795, March 2010, <http://www.rfc-editor.org/info/rfc5795>.

[RFC5954] Gurbani, V., Ed., Carpenter, B., Ed., and B. Tate, Ed., "Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261", RFC 5954, DOI 10.17487/RFC5954, August 2010, <http://www.rfc-editor.org/info/rfc5954>.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <http://www.rfc-editor.org/info/rfc6052>.

[RFC6603] Korhonen, J., Ed., Savolainen, T., Krishnan, S., and O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", RFC 6603, DOI 10.17487/RFC6603, May 2012, <http://www.rfc-editor.org/info/rfc6603>.

[RFC7066] Korhonen, J., Ed., Arkko, J., Ed., Savolainen, T., and S. Krishnan, "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts", RFC 7066, DOI 10.17487/RFC7066, November 2013, <http://www.rfc-editor.org/info/rfc7066>.

[TS.23060] 3GPP, "General Packet Radio Service (GPRS); Service description; Stage 2", 3GPP TS 23.060 13.6.0, March 2016, <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", 3GPP TS 23.401 13.6.1, March 2016, <http://www.3gpp.org/DynaReport/23401.htm>.

[TS.24008] 3GPP, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3", 3GPP TS 24.008 13.5.0, March 2016, <http://www.3gpp.org/DynaReport/24008.htm>.

6.2. Informative References

[OECD] Organisation for Economic Co-operation and Development (OECD), "The Economics of the Transition to Internet Protocol version 6 (IPv6)", DOI 10.1787/5jxt46d07bhc-en, November 2014, <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP%282014%293/FINAL&docLanguage=En>.

[Power] Haverinen, H., Siren, J., and P. Eronen, "Energy Consumption of Always-On Applications in WCDMA Networks", Proceedings of IEEE 65: Vehicular Technology Conference, VTC2007-Spring, pp 964-968, DOI 10.1109/VETECS.2007.207, April 2007, <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4212635>.

[R3GPP] 3GPP, "The Mobile Broadband Standard: Releases", 2016, <http://www.3gpp.org/specifications/67-releases>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, DOI 10.17487/RFC3948, January 2005, <http://www.rfc-editor.org/info/rfc3948>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <http://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <http://www.rfc-editor.org/info/rfc4035>.

[RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, DOI 10.17487/RFC6092, January 2011, <http://www.rfc-editor.org/info/rfc6092>.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, DOI 10.17487/RFC6145, April 2011, <http://www.rfc-editor.org/info/rfc6145>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <http://www.rfc-editor.org/info/rfc6146>.

[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, DOI 10.17487/RFC6147, April 2011, <http://www.rfc-editor.org/info/rfc6147>.

[RFC6342] Koodli, R., "Mobile Networks Considerations for IPv6 Deployment", RFC 6342, DOI 10.17487/RFC6342, August 2011, <http://www.rfc-editor.org/info/rfc6342>.

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, DOI 10.17487/RFC6434, December 2011, <http://www.rfc-editor.org/info/rfc6434>.

[RFC6459] Korhonen, J., Ed., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, DOI 10.17487/RFC6459, January 2012, <http://www.rfc-editor.org/info/rfc6459>.

[RFC6535] Huang, B., Deng, H., and T. Savolainen, "Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)", RFC 6535, DOI 10.17487/RFC6535, February 2012, <http://www.rfc-editor.org/info/rfc6535>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <http://www.rfc-editor.org/info/rfc6724>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <http://www.rfc-editor.org/info/rfc6877>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <http://www.rfc-editor.org/info/rfc6887>.

[RFC6889] Penno, R., Saxena, T., Boucadair, M., and S. Sivakumar, "Analysis of Stateful 64 Translation", RFC 6889, DOI 10.17487/RFC6889, April 2013, <http://www.rfc-editor.org/info/rfc6889>.

[RFC7050] Savolainen, T., Korhonen, J., and D. Wing, "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis", RFC 7050, DOI 10.17487/RFC7050, November 2013, <http://www.rfc-editor.org/info/rfc7050>.

[RFC7051] Korhonen, J., Ed. and T. Savolainen, Ed., "Analysis of Solution Proposals for Hosts to Learn NAT64 Prefix", RFC 7051, DOI 10.17487/RFC7051, November 2013, <http://www.rfc-editor.org/info/rfc7051>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <http://www.rfc-editor.org/info/rfc7084>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <http://www.rfc-editor.org/info/rfc7217>.

[RFC7225] Boucadair, M., "Discovering NAT64 IPv6 Prefixes Using the Port Control Protocol (PCP)", RFC 7225, DOI 10.17487/RFC7225, May 2014, <http://www.rfc-editor.org/info/rfc7225>.

[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, DOI 10.17487/RFC7278, June 2014, <http://www.rfc-editor.org/info/rfc7278>.

[RFC7335] Byrne, C., "IPv4 Service Continuity Prefix", RFC 7335, DOI 10.17487/RFC7335, August 2014, <http://www.rfc-editor.org/info/rfc7335>.

[RFC7445] Chen, G., Deng, H., Michaud, D., Korhonen, J., and M. Boucadair, "Analysis of Failure Cases in IPv6 Roaming Scenarios", RFC 7445, DOI 10.17487/RFC7445, March 2015, <http://www.rfc-editor.org/info/rfc7445>.

[TS.23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.401 13.5.0, March 2016, <http://www.3gpp.org/DynaReport/23402.htm>.

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, B. Stark, and A. Petrescu for the discussion in the v6ops mailing list and for the comments.

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, F. Baker, L.M. Contreras Murillo, and M. Abrahamsson for their detailed reviews and comments.

Authors' Addresses

David Binet
Orange
Rennes
France

Email: david.binet@orange.com

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Ales Vizdal
Deutsche Telekom AG
Tomickova 2144/1
Prague, 148 00
Czech Republic

Email: Ales.Vizdal@T-Mobile.cz

Gang Chen
China Mobile
29, Jinrong Avenue
Xicheng District, Beijing 100033
China

Email: phdgang@gmail.com, chengang@chinamobile.com

Nick Heatley
EE
The Point, 37 North Wharf Road,
London W2 1AG
United Kingdom

Email: nick.heatley@ee.co.uk

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

Email: ross@eircom.net

Dave Michaud
Rogers Communications
8200 Dixie Rd.
Brampton, ON L6T 0C1
Canada

Email: dave.michaud@rci.rogers.com

Diego R. Lopez
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid 28006
Spain

Phone: +34 913 129 041
Email: diego.r.lopez@telefonica.com

Walter Haeffner
Vodafone D2 GmbH
Ferdinand-Braun-Platz 1
Duesseldorf 40549
Germany

Email: walter.haeffner@vodafone.com