IPv6 Operations (V6OPS)
Internet-Draft
Obsoletes: 3316 (if approved)
Intended status: Informational
Expires: March 19, 2014

J. Korhonen, Ed.
Renesas Mobile
J. Arkko, Ed.
Ericsson
T. Savolainen
Nokia
S. Krishnan
Ericsson

September 15, 2013

IPv6 for 3GPP Cellular Hosts
draft-ietf-v6ops-rfc3316bis-06.txt

Abstract

As the deployment of third and fourth generation cellular networks progresses, a large number of cellular hosts are being connected to the Internet. Standardization organizations have made Internet Protocol version 6 (IPv6) mandatory in their specifications. However, the concept of IPv6 covers many aspects and numerous specifications. In addition, the characteristics of cellular links in terms of bandwidth, cost and delay put special requirements on how IPv6 is used. This document considers IPv6 for cellular hosts that attach to the General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), or Evolved Packet System (EPS) networks (Hereafter collectively referred to as 3GPP networks). This document also lists out specific IPv6 functionalities that need to be implemented in addition what is already prescribed in the IPv6 Node Requirements document. It also discusses some issues related to the use of these components when operating in these networks. This document obsoletes RFC 3316.

This Internet-Draft will expire on March 19, 2014.

Copyright Notice

Table of Contents

1. Introduction

Technologies such as GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunications System), Evolved Packet System (EPS), CDMA2000 (Code Division Multiple Access 2000) and eHRPD (Enhanced High Rate Packet Data) are making it possible for cellular hosts to have an always-on connection to the Internet. IPv6 [RFC2460] has become essential to such networks as the number of cellular hosts is increasing rapidly. Standardization organizations working with cellular technologies have recognized this and made IPv6 mandatory in their specifications.

Support for IPv6 and the introduction of UMTS started with 3GPP Release-99 networks and hosts. For the detailed description of IPv6 in 3GPP networks including the Evolved Packet System, see [RFC6459].

1.1. Scope of this Document

For the purpose of this document, a cellular interface is considered to be the interface to a cellular access network based on the following standards: 3GPP GPRS and UMTS Release-99, Release-4 to Release-11, and EPS Release-8 to Release-11 as well as future UMTS or EPS releases. A cellular host is considered to be a host with such a cellular interface.

This document complements the IPv6 node requirements [RFC6434] in places where clarifications are needed with discussion on the use of these selected IPv6 specifications when operating over a cellular interface. Such a specification is necessary in order to enable the optimal use of IPv6 in a cellular network environment. The description is made from a cellular host point of view. Complementary access technologies may be supported by the cellular host, but those are not discussed in detail. Important considerations are given in order to eliminate unnecessary user confusion over configuration options, ensure interoperability and to provide an easy reference for those who are implementing IPv6 in a cellular host. It is necessary to ensure that cellular hosts are good citizens of the Internet.

This document is informational in its nature, and it is not intended to replace, update, or contradict any IPv6 standards documents or the IPv6 node requirements [RFC6434].

This document is primarily targeted to the implementers of cellular hosts that will be used with the cellular networks listed in the scope. The document provides guidance on which IPv6 related specifications are to be implemented in such cellular hosts. Parts of this document may also apply to other cellular link types, but

this document does not provide any detailed analysis on other link types. This document should not be used as a definitive list of IPv6 functionalies for cellular links other than those listed above. Future changes in 3GPP networks that impact host implementations may result in updates to this document.

There are different ways to implement cellular hosts:

- The host can be a "closed" device with optimized built-in applications, with no possibility to add or download applications that can have IP communications. An example of such a host is a very simple form of a mobile phone.
- The host can be an open device, e.g., a "smart phone" where it is possible to download applications to expand the functionality of the device.
- The cellular radio modem part can be separated from the host IP stack with an interface. One example of such host is a laptop computer that uses a USB cellular modem for the cellular access.

If a cellular host has additional IP capable interfaces, (such as Ethernet, WLAN, Bluetooth, etc.) then there may be additional requirements for the device, beyond what is discussed in this document. Additionally, this document does not make any recommendations on the functionality required on laptop computers having a cellular interface such as an embedded modem or a USB modem stick, other than recommending link specific behavior on the cellular link.

This document discusses IPv6 functionality as of the time when this document has been written. Ongoing work on IPv6 may affect what is required of future hosts.

Transition mechanisms used by cellular hosts are not in the scope of this document and are left for further study. The primary transition mechanism supported by the 3GPP is dual-stack [RFC4213]. Dual-stack capable bearer support has been added to GPRS starting from the 3GPP Release-9 and to EPS starting from the Release-8 [RFC6459], whereas the earlier 3GPP releases required multiple single IP version bearers to support dual-stack.

1.2. Abbreviations

2G Second Generation Mobile Telecommunications, such as GSM and GPRS technologies.

3G	Third Generation Mobile Telecommunications, such as UMTS technology.
4G	Fourth Generation Mobile Telecommunications, such as LTE technology.
3GPP	3rd Generation Partnership Project. Throughout the document, the term 3GPP (3rd Generation Partnership Project) networks refers to architectures standardized by 3GPP, in Second, Third and Fourth Generation releases: 99, 4, and 5, as well as future releases.
APN	Access Point Name. The APN is a logical name referring to a GGSN and/or a PGW, and an external network.
EPC	Evolved Packet Core.
EPS	Evolved Packet System.
ESP	Encapsulating Security Payload
GGSN	Gateway GPRS Support Node (a default router for 3GPP IPv6 cellular hosts in GPRS).
GPRS	General Packet Radio Service.
LTE	Long Term Evolution.
MT	Mobile Terminal, for example, a mobile phone handset.
MTU	Maximum Transmission Unit.
PDN	Packet Data Network.
PDP	Packet Data Protocol.
PGW	Packet Data Network Gateway (the default router for 3GPP IPv6 cellular hosts in EPS).
SGW	Serving Gateway. The user plane equivalent of an SGSN in EPS (and the default router for 3GPP IPv6 cellular hosts when using PMIPv6).
TE	Terminal Equipment, for example, a laptop attached through a 3GPP handset.
UMTS	Universal Mobile Telecommunications System.
WLAN	Wireless Local Area Network.

1.3. Cellular Host IPv6 Features

This document lists IPv6 features for cellular hosts that are split into three groups.

Basic IP

In this group, a list of the basic IPv6 features essential for cellular hosts are described.

IP Security

In this group, the IP Security related parts are described.

Mobility

In this group, IP layer mobility issues are described.

2. Basic IP

For most parts refer to the IPv6 Node Requirements document [RFC6434].

2.1. Internet Protocol Version 6

The Internet Protocol Version 6 (IPv6) is specified in [RFC2460]. This specification is a mandatory part of IPv6. A cellular host must conform to the generic IPv6 Host Requirements [RFC6434], unless specifically pointed out otherwise in this document.

2.2. Neighbor Discovery in 3GPP Networks

A cellular host must support Neighbor Solicitation and Neighbor Advertisement messages [RFC4861]. Some further notes on how these are applied in the particular type of an interface can be useful, however:

In 3GPP networks, some Neighbor Discovery messages can be unnecessary in certain cases. GPRS, UMTS and EPS links resemble a point-to-point link; hence, the cellular host's only neighbor on the cellular link is the default router that is already known through Router Discovery. The cellular host always solicits for routers when the cellular interface is brought up (as described in [RFC4861], Section 6.3.7).

There are no link layer addresses on the 3GPP cellular link technology. Therefore, address resolution and next-hop determination are not needed. If the cellular host still attempts to do the address resolution e.g., for the default router, it must be understood that the GGSN/PGW may not even answer the address resolution Neighbor Solicitations. And even if it does, the Neighbor Advertisement is unlikely to contain the Target link-layer address option as there are no link-layer addresses on the 3GPP cellular link technology.

The cellular host must support Neighbor Unreachability Detection (NUD) as specified in [RFC4861]. Note that the link-layer address considerations above also apply to the NUD. The NUD triggered Neighbor Advertisement is also unlikely to contain the Target link-layer address option as there are no link-layer addresses. The cellular host should also be prepared for a router (i.e., GGSN/PGW) initiated NUD. However, it is unlikely a router to host NUD should

ever take place on a GPRS, UMTS and EPS links. See Appendix A for more discussion on the router to host NUD.

In 3GPP networks, it is desirable to reduce any additional periodic signaling. Therefore, the cellular host should include a mechanism in upper layer protocols to provide reachability confirmations when two-way IP layer reachability can be confirmed (see [RFC4861], Section 7.3.1). These confirmations would allow the suppression of NUD-related messages in most cases.

Host TCP implementation should provide reachability confirmation in the manner explained in [RFC4861], Section 7.3.1.

The widespread use of UDP in 3GPP networks poses a problem for providing reachability confirmation. As UDP itself is unable to provide such confirmation, applications running on top of UDP should provide the confirmation where possible. In particular, when UDP is used for transporting DNS, the DNS response should be used as a basis for reachability confirmation. Similarly, when UDP is used to transport RTP [RFC3550], the RTCP protocol [RFC3550] feedback should be used as a basis for the reachability confirmation. If an RTCP packet is received with a reception report block indicating some packets have gone through, then packets are reaching the peer. If they have reached the peer, they have also reached the neighbor.

When UDP is used for transporting SIP [RFC3261], responses to SIP requests should be used as the confirmation that packets sent to the peer are reaching it. When the cellular host is acting as the server side SIP node, no such confirmation is generally available. However, a host may interpret the receipt of a SIP ACK request as confirmation that the previously sent response to a SIP INVITE request has reached the peer.

2.3. Stateless Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration is defined in [RFC4862]. This specification is a mandatory part of IPv6 and also the only mandatory method to configure an IPv6 address in a 3GPP cellular host.

A cellular host in a 3GPP network must process a Router Advertisement as stated in [RFC4862]. The Router Advertisement contains a maximum of one prefix information option with lifetimes set to infinite (both valid and preferred lifetimes). The advertised prefix cannot ever be used for on-link determination (see [RFC6459], Section 5.2) and the lifetime of the advertised prefix is tied to the PDP Context/PDN Connection lifetime. Keeping the forward compatibility in mind there is no reason for the 3GPP cellular host to have 3GPP specific

handling of the prefix information option(s) although 3GPP specifications state that the Router Advertisement may contain a maximum of one prefix information option and the lifetimes are set to infinite.

Hosts in 3GPP networks can set DupAddrDetectTransmits equal to zero, as each assigned prefix is unique within its scope when advertised using the 3GPP IPv6 Stateless Address Autoconfiguration. In addition, the default router (GGSN/PGW) will not configure any addresses on its interfaces based on prefixes advertised to IPv6 cellular hosts on those interfaces. Thus, the host is not required to perform Duplicate Address Detection on the cellular interface.

Furthermore, the GGSN/PGW will provide the cellular host with an interface identifier that must be used for link-local address configuration. The link-local address configured from this interface identifier is guaranteed not to collide with the link-local address that the GGSN/PGW uses. Thus, the cellular host is not required to perform Duplicate Address Detection for the link-local address on the cellular interface.

See Appendix A for more details on 3GPP IPv6 Stateless Address Autoconfiguration.

2.4. IP version 6 over PPP

A cellular host in a 3GPP network that supports PPP [RFC1661] on the interface between the MT and the TE, must support the IPv6CP [RFC5072] interface identifier option. This option is needed to be able to connect other devices to the Internet using a PPP link between the cellular device (MT, e.g., a USB dongle) and other devices (TE, e.g., a laptop). The MT performs the PDP Context activation based on a request from the TE. This results in an interface identifier being suggested by the MT to the TE, using the IPv6CP option. To avoid any duplication in link-local addresses between the TE and the GGSN/PGW, the MT must always reject other suggested interface identifiers by the TE. This results in the TE always using the interface identifier suggested by the GGSN/PGW for its link-local address.

The rejection of interface identifiers suggested by the TE is only done for creation of link-local addresses, according to 3GPP specifications. The use of privacy addresses [RFC4941] or similar technologies for unique local IPv6 unicast addresses (ULA) [RFC4193] and global addresses is not affected by the above procedure.

2.5. Multicast Listener Discovery (MLD) for IPv6

Within 3GPP networks, hosts connect to their default routers (GGSN/PGW) via point-to-point links. Moreover, there are exactly two IP devices connected to the point-to-point link, and no attempt is made (at the link-layer) to suppress the forwarding of multicast traffic. Consequently, sending MLD reports for link-local addresses in a 3GPP environment is not necessary, although sending those cause no harm or interoperability issues. Refer Section 5.10 of [RFC6434] for MLD usage for multicast group knowledge that is not link-local.

2.6. Privacy Extensions for Address Configuration in IPv6

Privacy Extensions for Stateless Address Autoconfiguration [RFC4941] or other similar technologies may be supported by a cellular host. Privacy in general, is important for the Internet. In 3GPP networks the lifetime of an address assignment depends on many factors such as radio coverage, device status and user preferences. As a result also the prefix the cellular host uses is a subject to frequent changes.

Refer to Section 7 for a discussion of the benefits of privacy extensions in a 3GPP network.

2.7. Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

As of 3GPP Release-11 The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315] is neither required nor supported for address autoconfiguration. The IPv6 stateless autoconfiguration still remains the only mandatory address configuration method. However, DHCPv6 may be useful for other configuration needs on a cellular host. e.g. Stateless DHCPv6 [RFC3736] may be used to configure DNS and SIP server addresses, and DHCPv6 prefix delegation [RFC3633] may be used to delegate a prefix to the cellular host for use on its downstream non-cellular links.

2.8. DHCPv6 Prefix Delegation

Starting from Release-10 DHCPv6 Prefix Delegation was added as an optional feature to the 3GPP system architecture [RFC3633]. The prefix delegation model defined for Release-10 requires that the /64 IPv6 prefix assigned to the cellular host on the 3GPP link must aggregate with the shorter delegated IPv6 prefix. The cellular host should implement the Prefix Exclude Option for DHCPv6 Prefix Delegation [RFC6603] (see [RFC6459], Section 5.3 for further discussion).

2.9. Router preferences and more specific routes

The cellular host should implement the Default Router Preferences and More-Specific Routes extension to Router Advertisement messages [RFC4191]. These options may be useful for cellular hosts that also have additional interfaces on which IPv6 is used.

2.10. Neighbor Discovery and additional host configuration

The DNS server configuration is learned from the 3GPP link layer signaling. However, the cellular host should also implement the IPv6 Router Advertisement Options for DNS Configuration [RFC6106]. DHCPv6 is still optional for cellular hosts, and learning the DNS server addresses from the link layer signaling can be cumbersome when the MT and the TE are separated using other techniques than PPP interface.

The cellular host should also honor the MTU option in the Router Advertisement (see [RFC4861], Section 4.6.4). 3GPP system architecture uses extensive tunneling in its packet core network below the 3GPP link and this may lead to packet fragmentation issues. Therefore, the GGSN/PGW may propose a MTU to the cellular host that takes the additional tunneling overhead into account.

3. IP Security

IPsec [RFC4301] is a fundamental but not mandatory part of IPv6. Refer to the IPv6 Node Requirements Section 11 of [RFC6434] for the security requirements that also apply to cellular hosts.

3.1. Extension header considerations

The support for the Routing Header Type 0 (RH0) has been deprecated [RFC5095]. Therefore, the cellular host should as a default setting follow the RH0 processing described in Section 3 of [RFC5095].

IPv6 packet fragmentation has known security concerns. The cellular host must follow the handling of overlapping fragments as described in [RFC5722] and the cellular host must not fragment any neighbor discovery messages as described in [RFC6980].

4. Mobility

For the purposes of this document, IP mobility is not relevant. The movement of cellular hosts within 3GPP networks is handled by link layer mechanisms in majority of cases. 3GPP Release-8 introduced the dual-stack Mobile IPv6 (DSMIPv6) for a client based mobility

[RFC5555]. Client based IP mobility is optional in 3GPP architecture.

5. IANA Considerations

This document has no IANA actions.

6. Acknowledgements

The authors would like to thank the original authors for their grounding work on this documents: Gerben Kuijpers, John Loughney, Hesham Soliman and Juha Wiljakka.

The original [RFC3316] document was based on the results of a team that included Peter Hedman and Pertti Suomela in addition to the authors. Peter and Pertti have contributed both text and their IPv6 experience to this document.

The authors would like to thank Jim Bound, Brian Carpenter, Steve Deering, Bob Hinden, Keith Moore, Thomas Narten, Erik Nordmark, Michael Thomas, Margaret Wasserman and others at the IPv6 WG mailing list for their comments and input.

We would also like to thank David DeCamp, Karim El Malki, Markus Isomaki, Petter Johnsen, Janne Rinne, Jonne Soininen, Vlad Stirbu and Shabnam Sultana for their comments and input in preparation of this document.

For the revised version of the [RFC3316] the authors would like thank Dave Thaler, Ales Vizdal, Gang Chen, Ray Hunter, Charlie Kaufman, Owen DeLong and Alexey Melnikov for their comments, reviews and inputs.

7. Security Considerations

This document does not specify any new protocols or functionalities, and as such, it does not introduce any new security vulnerabilities. However, specific profiles of IPv6 functionality are proposed for different situations, and vulnerabilities may open or close depending on which functionality is included and what is not. There are also aspects of the cellular environment that make certain types of vulnerabilities more severe. The following issues are discussed:

- The suggested limitations (Section 3.1) in the processing of extension headers limits also exposure to Denial-of-Service (DoS) attacks through cellular hosts.
- IPv6 addressing privacy [RFC4941] or similar technology may be used in cellular hosts. However, it should be noted that in the 3GPP model, the network would assign a new prefix, in most cases, to hosts in roaming situations and typically, also when the cellular hosts activate a PDP Context or a PDN Connection. 3GPP devices must not use interface identifiers that are unique to the device, so the only difference in address between to 3GPP devices using SLAAC is in the prefix. This means that 3GPP networks will already provide a limited form of addressing privacy, and no global tracking of a single host is possible through its address. On the other hand, since a GGSN/PGW's coverage area is expected to be very large when compared to currently deployed default routers (no handovers between GGSN/PGWs are possible), a cellular host can keep a prefix for a long time. Hence, IPv6 addressing privacy can be used for additional privacy during the time the host is on and in the same area. The privacy features can also be used to e.g., make different transport sessions appear to come from different IP addresses. However, it is not clear that these additional efforts confuse potential observers any further, as they could monitor only the network prefix part.
- The use and recommendations of various security services such as IPsec or TLS [RFC5246] in the connection of typical applications that also apply to cellular hosts are discussed in Section 11 of [RFC6434].
- The airtime used by cellular hosts is expensive. In some cases, users are billed according to the amount of data they transfer to and from their host. It is crucial for both the network and the users that the airtime is used correctly and no extra charges are applied to users due to misbehaving third parties. The cellular links also have a limited capacity, which means that they may not necessarily be able to accommodate more traffic than what the user selected, such as a multimedia call. Additional traffic might interfere with the service level experienced by the user. While Quality of Service mechanisms mitigate these problems to an extent, it is still apparent that DoS aspects may be highlighted in the cellular environment. It is possible for existing DoS attacks that use for instance packet amplification to be substantially more damaging in this environment. How these attacks can be protected against is still an area of further study. It is also often easy to fill the cellular link and queues on both sides with additional or large packets.
- Within some service provider networks, it is possible to buy a prepaid cellular subscription without presenting personal identification. Attackers that wish to remain unidentified could leverage this. Note that while the user hasn't been identified,

the equipment still is; the operators can follow the identity of the device and block it from further use. The operators must have procedures in place to take notice of third party complaints regarding the use of their customers' devices. It may also be necessary for the operators to have attack detection tools that enable them to efficiently detect attacks launched from the cellular hosts.

- Cellular devices that have local network interfaces (such as WLAN or Bluetooth) may be used to launch attacks through them, unless the local interfaces are secured in an appropriate manner. Therefore, local network interfaces should have access control to prevent others from using the cellular host as an intermediary.
- The 3GPP link model mitigates most of the known IPv6 on-link and neighbor cache targeted attacks (see Section 2.2 and Appendix A).
- Advice for implementations in the face of Neighbor Discovery DoS attacks may be useful in some environments [RFC6583].
- Section 9 of [RFC6459] discusses further some recent concerns related to cellular hosts security.

8. References

8.1. Normative references

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

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, December 2009.

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

[RFC6980] Gont, F., "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery", RFC 6980, August 2013.

8.2. Informative references

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[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.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3316] Arkko, J., Kuijpers, G., Soliman, H., Loughney, J., and J. Wiljakka, "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts", RFC 3316, April 2003.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

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

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC5072] Varada, S., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

[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.

[RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, March 2012.

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

[TS.23060] 3GPP, "General Packet Radio Service (GPRS); Service description; Stage 2", 3GPP TS 23.060 11.5.0, March 2013.

[TS.23401] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 11.5.0, March 2013.

[TS.23402] 3GPP, "Architectural enhancements for non-3GPP accesses", 3GPP TS 23.402 11.6.0, March 2013.

[TS.29061] 3GPP, "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)", 3GPP TS 29.061 11.4.0, March 2013.

Appendix A. Cellular Host IPv6 Addressing in the 3GPP Model

The appendix aims to very briefly describe the 3GPP IPv6 addressing model for 2G (GPRS), 3G (UMTS) and 4G (EPS) cellular networks from Release-99 onwards. More information for 2G and 3G can be found from 3GPP Technical Specifications [TS.23060] and [TS.29061]. The equivalent documentation for 4G can be found from 3GPP Technical

Specifications [TS.23401], [TS.23402] and [TS.29061].

There are two possibilities to allocate the address for an IPv6 node: stateless and stateful autoconfiguration. The stateful address allocation mechanism needs a DHCP server to allocate the address for the IPv6 node. On the other hand, the stateless autoconfiguration procedure does not need any external entity involved in the address autoconfiguration (apart from the GGSN/PGW). At the time of writing this document, the IPv6 stateless address autoconfiguration mechanism is still the only mandatory and supported address configuration method for the cellular 3GPP link.

In order to support the standard IPv6 stateless address autoconfiguration mechanism as recommended by the IETF, the GGSN/PGW shall assign a single /64 IPv6 prefix that is unique within its scope to each primary PDP Context or PDN Connection that uses IPv6 stateless address autoconfiguration. This avoids the necessity to perform Duplicate Address Detection (DAD) at the network level for any address built by the mobile host. The GGSN/PGW always provides an interface identifier to the mobile host. The Mobile host uses the interface identifier provided by the GGSN/PGW to generate its link-local address. The GGSN/PGW provides the cellular host with the interface identifier, usually in a random manner. It must ensure the uniqueness of such identifier on the link (i.e., no collisions between its own link-local address and the cellular host's).

In addition, the GGSN/PGW will not use any of the prefixes assigned to cellular hosts to generate any of its own addresses. This use of the interface identifier, combined with the fact that each PDP Context or PDN Connection is allocated a unique prefix, will eliminate the need for DAD messages over the air interface, and consequently reduces inefficient use of radio resources. Furthermore, the allocation of a prefix to each PDP Context or PDN Connection will allow hosts to implement the Privacy Extensions in [RFC4941] without the need for further DAD messages.

In practice, the GGSN/PGW only needs to route all traffic destined to the cellular host that falls under the prefix assigned to it. This implies the GGSN/PGW may implement a minimal neighbor discovery protocol subset; since, due the point-to-point link model and the absence of link-layer addressing the address resolution can be entirely statically configured per PDP Context or PDN Connection, and there is no need to defend any other address than the link-local address for very unlikely duplicates. This has also an additional effect on a router to host NUD. There is really no need for it, since from the GGSN/PGW point of view it does not need to care for a single address, just routes the whole prefix to the cellular host. However, the cellular host must be prepared for the unlikely event of

receiving a NUD against its link-local address. It should be noted that the 3GPP specifications at the time of writing this document are silent what should happen if the router to host NUD fails.

See Sections 5 of [RFC6459] for further discussion on 3GPP address allocation and link model.

Appendix B. Changes to RFC 3316

- Clarified that [RFC4941] or similar technologies instead of plain [RFC4941] may be used for privacy purposes (as stated in [RFC6459]).
- Clarified that MLD for link-local addresses is not necessary but doing it causes no harm (instead of saying it may not be needed in some cases).
- Clarified that a cellular host should not do any changes in its stack to meet the 3GPP link restriction on the RA PIO options.
- Clarified that a cellular host should not do any changes in its stack to meet the infinite prefix lifetime requirement the 3GPP link has.
- Clarified that the prefix lifetime is tied to the PDP Context/PDN Connection lifetime.
- Clarified explicitly that a NUD from the gateway side to the UE's link-local address is possible.
- Added references to 3GPP specifications.
- Additional clarification on NUD on 3GPP cellular links.
- Added an explicit note that the prefix on the link is /64.
- Clarified that DHCPv6 ([RFC3315]) is not used at all for address autoconfiguration.
- Removal of all sections that can be directly found from [RFC6434].
- Clarifications to 3GPP link model and how Neighbor Discovery works on it.
- Addition of [RFC4191] recommendations.
- Addition of DHCPv6-based Prefix Delegation recommendations.
- Addition of [RFC6106] recommendations.
- Addition of [RFC5555] regarding client based mobility.
- Addition of Router Advertisement MTU option handling.
- Addition of Evolved Packet System text.
- Clarification on the primary 3GPP IPv6 transition mechanism.
- Addition of [RFC5095] that deprecates the RH0.
- Addition of [RFC5722] and [RFC6980] regarding the IPv6 fragmentation handling.
- Addition of [RFC6583] for Neighbor Discovery denial-of-service attack considerations.
- Made the PPP IPv6CP [RFC5072] support text conditional.

Authors' Addresses

Jouni Korhonen (editor)
Renesas Mobile
Porkkalankatu 24
FIN-00180 Helsinki
Finland

Email: jouni.nospam@gmail.com

Jari Arkko (editor)
Ericsson
Jorvas 02420
Finland

Email: jari.arkko@piuha.net

Teemu Savolainen
Nokia
Hermiankatu 12 D
FI-33720 Tampere
FINLAND

Email: teemu.savolainen@nokia.com

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com