Network Working Group
Request for Comments: 3316
Category: Informational

J. Arkko
G. Kuijpers
H. Soliman
Ericsson
J. Loughney
J. Wiljakka
Nokia

April 2003

Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

As the deployment of second and third generation cellular networks progresses, a large number of cellular hosts are being connected to the Internet. Standardization organizations are making 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), or Universal Mobile Telecommunications System (UMTS) networks. This document also lists basic components of IPv6 functionality and discusses some issues relating to the use of these components when operating in these networks.

Table of Contents

1 Introduction

Technologies such as GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunications System) and CDMA2000 (Code Division Multiple Access 2000) are making it possible for cellular hosts to have an always-on connection to the Internet. IPv6 becomes necessary, as it is expected that the number of such cellular hosts will increase rapidly. Standardization organizations working with cellular technologies have recognized this and are making IPv6 mandatory in their specifications.

Support for IPv6 and the introduction of UMTS starts with 3GPP Release 99 networks and hosts. IPv6 is specified as the only IP version supported for IP Multimedia Subsystem (IMS) starting from Release 5.

1.1 Scope of this Document

For the purposes 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, Release 5, as well as future UMTS releases. A cellular host is considered to be a host with such a cellular interface.

This document lists IPv6 specifications with discussion on the use of these specifications when operating over cellular interfaces. Such a specification is necessary in order for the optimal use of IPv6 in a cellular environment. The description is made from a cellular host point of view. Important considerations are given in order to eliminate unnecessary user confusion over configuration options, ensure interoperability and to provide an easy reference for those 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 nature, and it is not intended to replace, update, or contradict any IPv6 standards documents [RFC-2026].

The main audience of this document are: the implementers of cellular hosts that will be used with GPRS, 3GPP UMTS Release 99, Release 4, Release 5, or future releases of UMTS. The document provides guidance on which parts of IPv6 to implement in such cellular hosts. Parts of this document may also apply to other cellular link types, but no such detailed analysis has been done yet and is a topic of future work. This document should not be used as a definitive list

of IPv6 functionality for cellular links other than those listed above. Future changes in 3GPP networks that require changes in host implementations may result in updates to this document.

There are different ways to implement cellular hosts:

- The host can be a "closed 2G or 3G host" with a very compact size and optimized 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 2G or 3G host" with a compact size, but where it is possible to download applications; such as a PDA-type of phone.

If a cellular host has additional interfaces on which IP is used, (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 a PC card, other than recommending link specific behavior on the cellular link.

This document discusses IPv6 functionality as specified when this document has been written. Ongoing work on IPv6 may affect what is needed from future hosts. The reader should also be advised other relevant work exists for various other layers. Examples of this include the header compression work done in the IETF ROHC group, the analysis of the effects of error-prone links to performance in [RFC-3155], or the TCP work in [RFC-3481].

Transition mechanisms used by cellular hosts are not described in this document and are left for further study.

1.2 Abbreviations

2G	Second Generation Mobile Telecommunications, such as GSM and GPRS technologies.
3G	Third Generation Mobile Telecommunications, such as UMTS 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 and Third Generation releases: 99, 4, and 5, as well as future releases.
AH	Authentication Header
APN	Access Point Name. The APN is a logical name referring to a GGSN and an external network.

ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
IMS	IP Multimedia Subsystem
GGSN	Gateway GPRS Support Node (a default router for 3GPP IPv6 cellular hosts)
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
MT	Mobile Terminal, for example, a mobile phone handset.
MTU	Maximum Transmission Unit
PDP	Packet Data Protocol
SGSN	Serving GPRS Support Node
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 specification defines IPv6 features for cellular hosts in three groups.

Basic IP

In this group, basic parts of IPv6 are described.

IP Security

In this group, the IP Security parts are described.

Mobility

In this group, IP layer mobility issues are described.

2 Basic IP

2.1 RFC1981 - Path MTU Discovery for IP Version 6

Path MTU Discovery [RFC-1981] may be used. Cellular hosts with a link MTU larger than the minimum IPv6 link MTU (1280 octets) can use Path MTU Discovery in order to discover the real path MTU. The relative overhead of IPv6 headers is minimized through the use of longer packets, thus making better use of the available bandwidth.

The IPv6 specification [RFC-2460] states in Section 5 that "a minimal IPv6 implementation (e.g., in a boot ROM) may simply restrict itself to sending packets no larger than 1280 octets, and omit implementation of Path MTU Discovery."

If Path MTU Discovery is not implemented then the sending packet size is limited to 1280 octets (standard limit in [RFC-2460]). However, if this is done, the cellular host must be able to receive packets with size up to the link MTU before reassembly. This is because the node at the other side of the link has no way of knowing less than the MTU is accepted.

2.2 RFC3513 - IP Version 6 Addressing Architecture

The IPv6 Addressing Architecture [RFC-3513] is a mandatory part of IPv6.

2.3 RFC2460 - Internet Protocol Version 6

The Internet Protocol Version 6 is specified in [RFC-2460]. This specification is a mandatory part of IPv6.

By definition, a cellular host acts as a host, not as a router. Implementation requirements for a cellular router are not defined in this document.

Consequently, the cellular host must implement all non-router packet receive processing as described in RFC 2460. This includes the generation of ICMPv6 error reports, and the processing of at least the following extension headers:

- Hop-by-Hop Options header: at least the Pad1 and PadN options
- Destination Options header: at least the Pad1 and PadN options
- Routing (Type 0) header: final destination (host) processing only
- Fragment header
- AH and ESP headers (see also a discussion on the use of IPsec for various purposes in Section 3)
- The No Next Header value

Unrecognized options in Hop-by-Hop Options or Destination Options extensions must be processed as described in RFC 2460.

The cellular host must follow the packet transmission rules in RFC 2460.

The cellular host must always be able to receive and reassemble fragment headers. It will also need to be able to send a fragment header in cases where it communicates with an IPv4 host through a translator (see Section 5 of RFC2460).

Cellular hosts should only process routing headers when they are the final destination and return errors if the processing of the routing header requires them to forward the packet to another node. This will also ensure that the cellular hosts will not be inappropriately used as relays or components in Denial-of-Service (DoS) attacks. Acting as the destination involves the following: the cellular hosts must check the Segments Left field in the header, and proceed if it is zero or one and the next address is one of the host's addresses. If not, however, the host must implement error checks as specified in Section 4.4 of RFC 2460. There is no need for the host to send Routing Headers.

2.4 RFC2461 - Neighbor Discovery for IPv6

Neighbor Discovery is described in [RFC-2461]. This specification is a mandatory part of IPv6.

2.4.1 Neighbor Discovery in 3GPP Networks

A cellular host must support Neighbor Solicitation and Advertisement messages.

In GPRS and UMTS networks, some Neighbor Discovery messages can be unnecessary in certain cases. GPRS and UMTS 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. There are no link layer addresses. Therefore, address resolution and next-hop determination are not needed.

The cellular host must support neighbor unreachability detection as specified in [RFC-2461].

In GPRS and UMTS networks, it is very desirable to conserve bandwidth. Therefore, the cellular host should include a mechanism in upper layer protocols to provide reachability confirmation when two-way IP layer reachability can be confirmed (see RFC-2461, Section 7.3.1). These confirmations will allow the suppression of most NUD-related messages in most cases.

Host TCP implementation should provide reachability confirmation in the manner explained in RFC 2461, Section 7.3.1.

The common use of UDP in 3GPP networks poses a problem for providing reachability confirmation. UDP itself is unable to provide such confirmation. Applications running over UDP should provide the confirmation where possible. In particular, when UDP is used for transporting RTP, the RTCP protocol 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, 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.

2.5 RFC2462 - IPv6 Stateless Address Autoconfiguration

IPv6 Stateless Address Autoconfiguration is defined in [RFC-2462]. This specification is a mandatory part of IPv6.

2.5.1 Stateless Address Autoconfiguration in 3GPP Networks

A cellular host in a 3GPP network must process a Router Advertisement as stated in Section 2.4.

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

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

2.6 RFC2463 - Internet Control Message Protocol for the IPv6

The Internet Control Message Protocol for the IPv6 is defined [RFC-2463]. This specification is a mandatory part of IPv6. Currently, this work is being updated.

As per RFC 2463 Section 2, ICMPv6 requirements must be fully implemented by every IPv6 node. See also Section 3 for an explanation of the use of IPsec for protecting ICMPv6 communications.

2.7 RFC2472 - IP version 6 over PPP

IPv6 over PPP [RFC-2472] must be supported for cellular hosts that implement PPP.

2.7.1 IP version 6 over PPP in 3GPP Networks

A cellular host in a 3GPP network must support the IPv6CP 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) 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, 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 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 [RFC-3041] for site-local and global addresses is not affected by the above procedure. The above procedure is only concerned with assigning the interface identifier used for forming link-local addresses, and does not preclude TE from using other interface identifiers for addresses with larger scopes (i.e., site-local and global).

2.8 RFC2473 - Generic Packet Tunneling in IPv6 Specification

Generic Packet Tunneling [RFC-2473] may be supported if needed for transition mechanisms.

2.9 RFC2710 - Multicast Listener Discovery (MLD) for IPv6

Multicast Listener Discovery [RFC-2710] must be supported by cellular hosts.

MLD requires that MLD messages be sent for link-local multicast addresses (excluding the all-nodes address). The requirement that MLD be run even for link-local addresses aids layer-two devices (e.g., Ethernet bridges) that attempt to suppress the forwarding of link-layer multicast packets to portions of the layer-two network where there are no listeners. If MLD is used to announce the

presence of listeners for all IP multicast addresses (including link-local multicast addresses), layer 2 devices can snoop MLD messages to reliably determine which portions of a network IP multicast messages need to be forwarded to.

2.9.1 MLD in 3GPP Networks

Within 3GPP networks, hosts connect to their default routers (GGSN) 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 may not always be necessary.

MLD is needed for multicast group knowledge that is not link-local.

2.10 RFC2711 - IPv6 Router Alert Option

The Router Alert Option [RFC-2711] must be supported, and its use is required when MLD is used (see Section 2.9) or when RSVP [RFC-2205] is used.

2.11 RFC3041 - Privacy Extensions for Address Configuration in IPv6

Privacy Extensions for Stateless Address Autoconfiguration [RFC-3041] should be supported. RFC 3041, and privacy in general, is important for the Internet. Cellular hosts may use the temporary addresses as described in RFC 3041. However, the use of the Privacy Extension in an environment where IPv6 addresses are short-lived may not be necessary. At the time this document has been written, there is no experience on how long-lived cellular network address assignments (i.e., attachments to the network) are. The length of the address assignments depends upon many factors such as radio coverage, device status and user preferences. Additionally, the use of temporary address with IPsec may lead to more frequent renegotiation for the Security Associations.

Refer to Section 5 for a discussion of the benefits of privacy extensions in a 3GPP network.

2.12 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

The Dynamic Host Configuration Protocol for IPv6 [DHCPv6] may be used. DHCPv6 is not required for address autoconfiguration when IPv6 stateless autoconfiguration is used. However, DHCPv6 may be useful for other configuration needs on a cellular host.

2.13 RFC3484 - Default Address Selection for IPv6

Default Address Selection [RFC-3484] is needed for cellular hosts.

2.14 DNS

Cellular hosts should support DNS, as described in [RFC-1034], [RFC-1035], [RFC-1886], and [RFC-3152].

If DNS is used, a cellular host can perform DNS requests in the recursive mode, to limit signaling over the air interface. Both the iterative and the recursive approach should be supported, however, as the specifications require implementation of the iterative approach, and allow the recursive approach as an option. Furthermore, all DNS servers may not support recursive queries, and the security benefits of DNS Security cannot always be achieved with them.

3 IP Security

IPsec [RFC-2401] is a fundamental part of IPv6, and support for AH and ESP is described as mandatory in the specifications.

The first part of this section discusses the applicability of IP Security and other security mechanisms for common tasks in cellular hosts. The second part, Sections 3.1 to 3.13, lists the specifications related to IPsec and discusses the use of these parts of IPsec in a cellular context.

In general, the need to use a security mechanism depends on the intended application for it. Different security mechanisms are useful in different contexts, and have different limitations. Some applications require the use of TLS [RFC-2246], in some situations IPsec is used.

It is not realistic to list all possible services here, and it is expected that application protocol specifications have requirements on what security services they require. Note that cellular hosts able to download applications must be prepared to offer sufficient security services for these applications regardless of the needs of the initial set of applications in those hosts.

The following sections list specifications related to the IPsec functionality, and discuss their applicability in a cellular context. This discussion focuses on the use of IPsec. In some applications, a different set of protocols may need to be employed. In particular, the below discussion is not relevant for applications that use other security services than IPsec.

3.1 RFC2104 - HMAC: Keyed-Hashing for Message Authentication

This specification [RFC-2104] must be supported. It is referenced by RFC 2403 that describes how IPsec protects the integrity of packets.

3.2 RFC2401 - Security Architecture for the Internet Protocol

This specification [RFC-2401] must be supported.

3.3 RFC2402 - IP Authentication Header

This specification [RFC-2402] must be supported.

3.4 RFC2403 - The Use of HMAC-MD5-96 within ESP and AH

This specification [RFC-2403] must be supported.

3.5 RFC2404 - The Use of HMAC-SHA-96 within ESP and AH

This specification [RFC-2404] must be supported.

3.6 RFC2405 - The ESP DES-CBC Cipher Algorithm With Explicit IV

This specification [RFC-2405] may be supported. It is, however, recommended that stronger algorithms than DES be used. Algorithms, such as AES, are undergoing work in the IPsec working group. These new algorithms are useful, and should be supported as soon as their standardization is ready.

3.7 RFC2406 - IP Encapsulating Security Payload (ESP)

This specification [RFC-2406] must be supported.

3.8 RFC2407 - The Internet IP Security DoI for ISAKMP

Automatic key management, [RFC-2408] and [RFC-2409], is not a mandatory part of the IP Security Architecture. Note, however, that in the cellular environment the IP addresses of a host may change dynamically. For this reason the use of manually configured Security Associations is not practical, as the newest host address would have to be updated to the SA database of the peer as well.

Even so, it is not clear that all applications would use IKE for key management. For instance, hosts may use IPsec ESP [RFC-2406] for protecting SIP signaling in the IMS [3GPP-ACC] but provide authentication and key management through another mechanism such as UMTS AKA (Authentication and Key Agreement) [UMTS-AKA].

It is likely that several simplifying assumptions can be made in the cellular environment, with respect to the mandated parts of the IP Security DoI, ISAKMP, and IKE. Work on such simplifications would be useful, but is outside the scope of this document.

3.9 RFC2408 - The Internet Security Association and Key Management Protocol

This specification [RFC-2408] is optional according to the IPv6 specifications, but may be necessary in some applications, as described in Section 3.8.

3.10 RFC2409 - The Internet Key Exchange (IKE)

This specification [RFC-2409] is optional according to the IPv6 specifications, but may be necessary in some applications, as described in Section 3.8.

Interactions with the ICMPv6 packets and IPsec policies may cause unexpected behavior for IKE-based SA negotiation unless some special handling is performed in the implementations.

The ICMPv6 protocol provides many functions, which in IPv4 were either non-existent or provided by lower layers. For instance, IPv6 implements address resolution using an IP packet, ICMPv6 Neighbor Solicitation message. In contrast, IPv4 uses an ARP message at a lower layer.

The IPsec architecture has a Security Policy Database that specifies which traffic is protected, and how. It turns out that the specification of policies in the presence of ICMPv6 traffic is not easy. For instance, a simple policy of protecting all traffic between two hosts on the same network would trap even address resolution messages, leading to a situation where IKE can't establish a Security Association since in order to send the IKE UDP packets one would have had to send the Neighbor Solicitation Message, which would have required an SA.

In order to avoid this problem, Neighbor Solicitation, Neighbor Advertisement, Router Solicitation, and Router Advertisement messages must not lead to the use of IKE-based SA negotiation. The Redirect message should not lead to the use of IKE-based SA negotiation. Other ICMPv6 messages may use IKE-based SA negotiation as is desired in the Security Policy Data Base.

Note that the above limits the usefulness of IPsec in protecting all ICMPv6 communications. For instance, it may not be possible to protect the ICMPv6 traffic between a cellular host and its next hop

router. (Which may be hard in any case due to the need to establish a suitable public key infrastructure. Since roaming is allowed, this infrastructure would have to authenticate all hosts to all routers.)

3.11 RFC2410 - The NULL Encryption Algorithm & its Use With IPsec

This specification [RFC-2410] must be supported.

3.12 RFC2451 - The ESP CBC-Mode Cipher Algorithms

This specification [RFC-2451] must be supported if encryption algorithms other than DES are implemented, e.g., CAST-128, RC5, IDEA, Blowfish, 3DES.

4. Mobility

For the purposes of this document, IP mobility is not relevant. When Mobile IPv6 specification is approved, a future update to this document may address these issues, as there may be some effects on all IPv6 hosts due to Mobile IP. The movement of cellular hosts within 3GPP networks is handled by link layer mechanisms.

5. Security Considerations

This document does not specify any new protocols or functionality, 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 2.3) in the processing of routing headers limits also exposure to DoS attacks through cellular hosts.

- IPv6 addressing privacy [RFC3041] may be used in cellular hosts. However, it should be noted that in the 3GPP model, the network would assign new addresses, in most cases, to hosts in roaming situations and typically, also when the cellular hosts activate a PDP context. 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's coverage area is expected to be very large when compared to currently deployed default routers (no handovers between GGSNs are possible), a cellular host can keep an address 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 of various security services such as IPsec or TLS in the connection of typical applications in cellular hosts is discussed in Section 3 and recommendations are given there.

- Section 3 also discusses under what conditions it is possible to provide IPsec protection of e.g., ICMPv6 communications.

- 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 IrDA 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.

6. References

6.1. Normative

[RFC-1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC-1886] Thomson, S. and C. Huitema, "DNS Extensions to support IP version 6, RFC 1886, December 1995.

[RFC-1981] McCann, J., Mogul, J. and S. Deering, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[RFC-2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC-2104] Krawczyk, K., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC-2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC-2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC-2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC-2403] Madson, C., and R. Glenn, "The Use of HMAC-MD5 within ESP and AH", RFC 2403, November 1998.

[RFC-2404] Madson, C., and R. Glenn, "The Use of HMAC-SHA-1 within ESP and AH", RFC 2404, November 1998.

[RFC-2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[RFC-2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Protocol (ESP)", RFC 2406, November 1998.

[RFC-2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC-2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[RFC-2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC-2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC-2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

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

[RFC-2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC-2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC-2463] Conta, A. and S. Deering, "ICMP for the Internet Protocol Version 6 (IPv6)", RFC 2463, December 1998.

[RFC-2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC-2710] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC-2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.

[RFC-2874] Crawford, M. and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", RFC 2874, July 2000.

[RFC-3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC-3152] Bush, R., "Delegation of IP6.ARPA", BCP 49, RFC 3152, August 2001.

[RFC-3155] Dawkins, S., Montenegro, G., Kojo, M., Magret, V. and N. Vaidya, "End-to-end Performance Implications of Links with Errors", BCP 50, RFC 3155, August 2001.

[RFC-3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC-3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

6.2. Informative

[3GPP-ACC] 3GPP Technical Specification 3GPP TS 33.203, "Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services (Release 5)", 3rd Generation Partnership Project, March 2002.

[3GPP-IMS] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem - Stage 2; (3G TS 23.228)

[3GPP-IPv6] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects "Architectural requirements" (TS 23.221)

[DHCPv6] Bound, J., et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Work in progress.

[RFC-1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC-2529] Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC 2529, March 1999.

[RFC-2205] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC-3314] Wasserman, M., Editor, "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, RFC 3314, September 2002.

[RFC-3481] Inamura, H., Montenegro, G., Ludwig, R., Gurtov, A. and F. Khafizov, "TCP over Second (2.5G) and Third (3G) Generation Wireless Networks", BCP 71, RFC 3481, February 2003.

[UMTS-AKA] 3GPP Technical Specification 3GPP TS 33.102, "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 4)", 3rd Generation Partnership Project, December 2001.

7. Contributors

This document is 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.

8. Acknowledgements

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.

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) and 3G (UMTS) cellular networks from Release 99 onwards. More information can be found from 3GPP Technical Specification 23.060.

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).

In order to support the standard IPv6 stateless address autoconfiguration mechanism, as recommended by the IETF, the GGSN shall assign a prefix that is unique within its scope to each primary PDP context that uses IPv6 stateless address autoconfiguration. This avoids the necessity to perform Duplicate Address Detection at the network level for every address built by the mobile host. The GGSN always provides an Interface Identifier to the mobile host. The Mobile host uses the interface identifier provided by the GGSN to generate its link-local address. The GGSN 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 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 is allocated a unique prefix, will eliminate the need for DAD messages over the air interface, and consequently allows an efficient use of bandwidth. Furthermore, the allocation of a prefix to each PDP context will allow hosts to implement the privacy extensions in RFC 3041 without the need for further DAD messages.

Authors' Addresses

Jari Arkko
Ericsson
02420 Jorvas
Finland

EMail: jari.arkko@ericsson.com

Gerben Kuijpers
Ericsson
Skanderborgvej 232
DK-8260 Viby J
Denmark

EMail: gerben.a.kuijpers@ted.ericsson.se

John Loughney
Nokia Research Center
Itamerenkatu 11 - 13
FIN-00180 HELSINKI
Finland

EMail: john.loughney@nokia.com

Hesham Soliman
Ericsson Radio Systems AB
Torshamnsgatan 23, Kista, Stockholm
Sweden

EMail: hesham.soliman@era.ericsson.se

Juha Wiljakka
Nokia Mobile Phones
Sinitaival 5
FIN-33720 TAMPERE
Finland

EMail: juha.wiljakka@nokia.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.