IPv6

Transition Considerations for

LTE and Evolved Packet Core

February 2009

Table of Contents

1. EXECUTIVE SUMMARY

As the wireless networks grow and evolve, the dependency on IP addresses becomes a vital ingredient to rolling out services. At the same time IPv4 addresses are being depleted, always-on services (SIP-based applications) are already being deployed at an increasing rate; hence, the urgency to move to IPv6 continues to be a major issue for operators and vendors in the wireless industry.

The purpose of this paper is to build on the IPv6 recommendations presented in the first iteration of 3G Americas IPv6 White Paper published in 2008. The focus of this paper includes common areas of interest that will affect interoperability and other appropriate issues. This paper covers the following areas:

- The evolution to the Evolved Packet Core
- Assess impact of IPv6 to existing Voice Core
- Ensure network Security during transition to IPv6

2. INTRODUCTION

The Evolved Packet Core is the mobility core solution associated with the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), which was formally known as Long Term Evolution (LTE). EPC and E-UTRAN are defined by 3GPP's Release 8 specifications, in particular [1], [2] and [3]. The combination of E-UTRAN and EPC is called Evolved Packet System (EPS).

2.1 EPS ARCHITECTURE

The EPS architecture is depicted in the following figure.

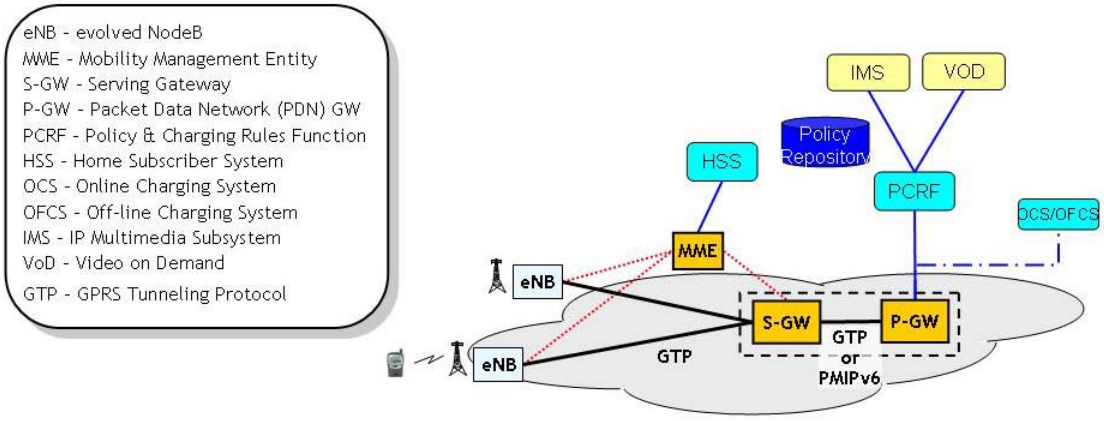

Figure 1: Evolved Packet System

E-UTRAN introduces a new radio interface technology. A base station that supports this radio interface technology is called Evolved NodeB (eNB).

The EPC architecture consists of a Mobility Management Entity (MME) and two gateways, the Serving Gateway (SGW) and the Packet Data Network Gateway (PDN GW or P-GW).

The MME is responsible for control plane functions: authentication, mobility management, paging and signaling security. Many of the functions and protocols supported by the MME are similar to those supported by SGSNs in UMTS deployments. In contrast to the SGSN, the MME solely deals with control protocols. User plane traffic flows directly between the eNB and the gateways.

The two gateways may be combined in a single network element. In the case that S-GW and P-GW are separate network elements, there are two options for the protocol used between them: GPRS Tunneling Protocol (GTP) and Proxy Mobile IP v6 (PMIPv6).

2.1.1 SIMULTANEOUS DUAL STACK SUPPORT

Similar to the concept of PDP Context, which is defined in 3GPP's R7 specifications, the R8 specifications identify EPS bearers. An EPS bearer is a logical connection between a UE and a gateway, associated with a specific QoS Class. An EPS bearer can carry multiple Service Data Flows (SDF), as long as these SDFs belong to the same QoS class

In contrast to the PDP Context definition in 3GPP R7, an EPS bearer can carry both native IPv4 and IPv6 traffic. Therefore, a UE can support simultaneously an IPv4 and an IPv6 stack while being connected through a single EPS bearer.

In a previous 3G Americas whitepaper on IPv6 ([4]), it was argued that in UMTS deployments, support of simultaneous dual-stack was impractical, because the number of PDP Context that would need to be setup would be unacceptably high. Since EPC allows both IPv4 and IPv6 traffic on a single EPS bearer, support of simultaneous dual stack in EPC does not suffer from the same problem.

Of course, allocating both IPv6 and IPv4 addresses to a device does not solve the problem of IPv4 exhaustion. A service provider may therefore decide to assign only IPv6 addresses to certain devices, even when the device is able to support IPv4 and IPv6 simultaneously. In that case, NAT-PT (see RFC 2766) or IPv6-toIPv4 http-proxy functionality may be required to connect these IPv6-only devices with legacy IPv4 end-points. Such a decision needs careful consideration and the issues identified in RFC 4966 ("NAT-PT Issues Analysis") need to be taken into account.

Note that the 3GPP R8 specs also provide updates to UMTS specifications. An R8-based UMTS network can carry both IPv4 and IPv6 traffic over a single PDP Context.

2.1.2 ADDRESS ASSIGNMENT MECHANISMS

A User Equipment device (UE) obtains an IP address in one of two ways:

- as part of the attachment procedure
- via s separate assignment procedure, such as DHCP or IPv6 Stateless Address Autoconfiguration

The attachment procedure is depicted in the following figure:

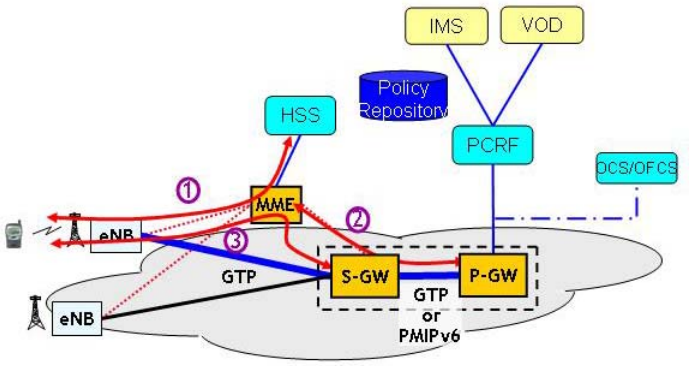

Figure 2: Attachment procedure

The attachment procedure consists of the following steps:

1. The User Equipment (UE) requests attachment by sending a message to the MME. This is followed by an authentication procedure that involves the HSS. As part of this procedure, the HSS sends subscription data associated with the user to the MME.

2. The MME is, with a few exceptions, responsible for selecting the Serving and PDN Gateways that will be used for this UE. It sends a request for the establishment of the *default bearer* to the S-GW, which forwards it to the P-GW. This message exchange results in the establishment of a GTP tunnel or a Mobile IP tunnel segment between S-GW and P-GW. This segment remains up, as long as the user is attached, even when the UE enters the idle state.

3. As a last step, the MME orchestrates the establishment of the GTP tunnel segment between S-GW and eNB and the (default) radio bearer between eNB and UE. The bearer between S-GW and UE is torn down whenever the UE goes to idle state. If the S-GW receives IP packets destined for the UE while it is in idle state, the S-GW triggers the MME which starts a paging procedure.

In the case IP address assignment is part of the attachment procedure, the P-GW allocates an IP address to the UE as part of step 2. This address is conveyed to the UE in the GTP control messages that are used to establish the EPS bearer in step 3.

Once a default bearer is established (with or without IP address assignment), the UE can perform DHCP or IPv6 Stateless Address Autoconfiguration (SLAAC) to obtain an IP address. Thus, for example, a UE could obtain an IPv4 address as part of the attachment procedure and an IPv6 address through an additional IPv6 SLAAC procedure.

2.1.3 EVOLVING PACKET CORE TO EPC AND IPV6

Introduction of LTE requires new or upgraded NodeBs and new mobility gateways in the core network. Many service providers, however, will gradually upgrade their networks to LTE. Therefore, LTE and UMTS (and previous technologies) will be deployed simultaneously.

The following figure shows how LTE and UMTS networks interface.

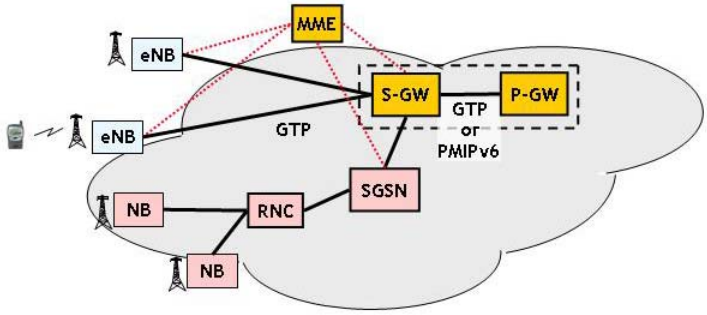

Figure 3: Combined LTE and UMTS network architecture

When a UE, after attaching through an LTE radio link, moves out of the reach of LTE eNBs, it may have to fall back to UMTS. The handover to UMTS is orchestrated by the MME, which interfaces with the target SGSN. The PDP Context is routed via the SGSN to the S-GW to which the UE was previously connected.

If the UE is a dual-stack device with its IPv4 and IPv6 stack simultaneously active, a handover may have impact on its operations. If the UE is handed over to an R8-compliant UMTS network, there are no consequences, as the R8 PDP Context can carry both IPv4 and IPv6 traffic. However, if the UE is handed over to an R7-compliant UMTS network (which is the more likely scenario), this does not work, since an R7 PDP Context carries either IPv4 traffic or IPv6 traffic, but not both.

3GPP standards specify a one-to-one mapping between EPS bearers and PDP contexts. This implies that an operator either needs to upgrade all SGSNs (connected to the EPC) to Rel-8, or disable dual-stack operation over the EPS network. In the latter case, a UE that requests dual-stack operation at attachment to the EPS network will only receive a single-stack bearer, say for IPv4, and it will subsequently need to initiate a second bearer establishment towards the same APN for IPv6.

3. VOICE CORE NETWORK

Voice telephony services in a 3GPP network are traditionally provided by a Mobile-services Switching Centre (and supporting infrastructure) and/or an IP Multimedia System.

As the name implies, IP Multimedia Subsystems (IMS) rely heavily on IP protocol. Per 3GPPP standards, IMS equipment should be deployed using IPv6 thereby avoiding the need for a future IPv4 to IPV6 migration.

Whereas new IMS equipment will typically be deployed with IPv6, existing voice core equipment will still be utilizing IPv4. Since the MSC is at the heart of any existing 3GPP voice core, this section focuses on the use of IP in the Mobile-services Switching Centre (MSC). As part of the MSC discussion, IP interfaces to subtending voice core network elements are also covered.

3.1 IP ADDRESS USAGE IN THE DISTRIBUTED MSC

The Mobile-services Switching Centre (MSC) performs all CS domain switching and signalling functions for GSM and UMTS mobile stations located in a specific geographical area. The MSC can be implemented in an integrated platform or in two distinct physical entities.

When divided into two physical entities the MSC consists of an MSC Server, handling only signalling, and a MGW, handling user data. This architecture of dividing the signalling server from the data plane is sometimes referred to as a distributed MSC.

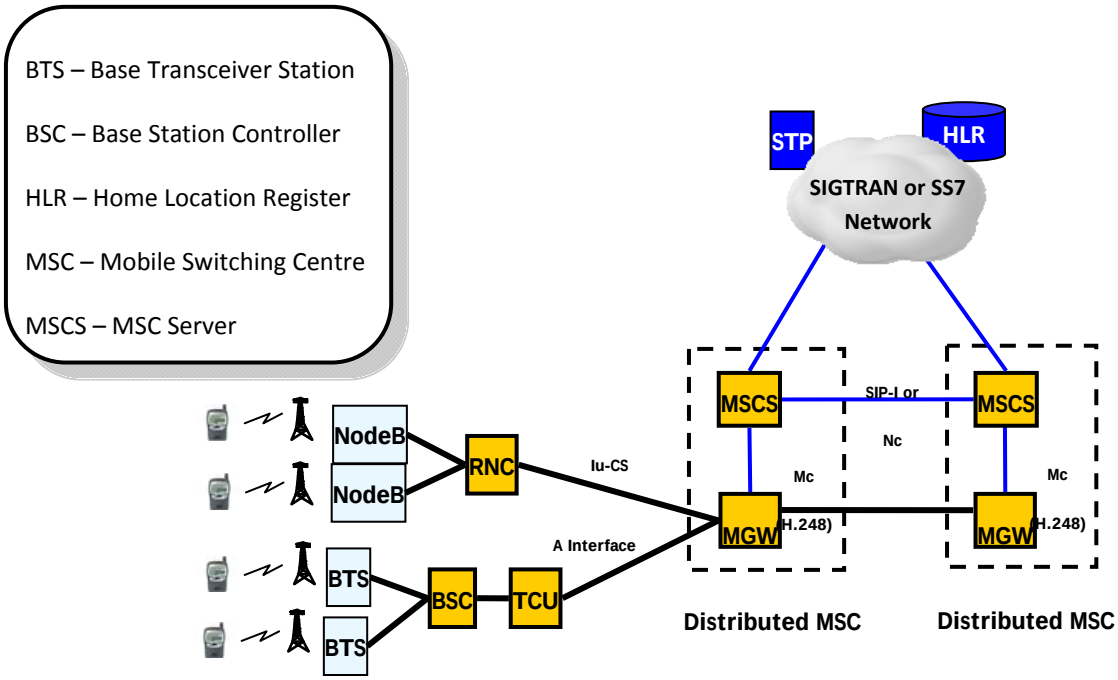

Figure 4. GSM/UMTS Voice Core with a Distributed MSC

Dependent on the vendor implementation, the distributed MSC may be enhanced to function in an IMS environment as a Telephony Application Server (TAS), MGCF/IM-MGW, IM-SSF, MRF, MSC enhanced for ICS, MSC enhanced for SRVCC etc., or may be extended to service SIP user equipment directly.

For interconnect, a distributed MSC will typically utilize a mix of packet or cell based protocols including IP and/or ATM. Since IP interfaces in a distributed MSC environment are generally a superset of an integrated MSC, this paper assumes a distributed MSC as the reference point.

Every instance of an IP address must be considered when migrating from IPv4 to IPv6 or operating in a dual-stack environment. The following sub-sections identify where IP addresses are typically utilized within the distributed MSC.

3.1.1 MSC TO SS7 NETWORK – SIGTRAN

In a GSM, UMTS, or 4G network, the MSC may connect to other SSPs, STPs, or SCPs (such as the HLR) via a traditional SS7 protocol stack or via SIGTRAN.

SIGTRAN, as defined in RFC 2719 and RFC 4166, is a set of protocols that allow circuit switch telephony messages, such as Media Gateway control and SS7 messages, to be reliably transported over an IP network. SIGTRAN consists of three components: a standard IP layer, an SCTP layer, and user adaptation layer(s).

When migrating networks from IPv4 to IPv6, all three of the SIGTRAN components must be considered. Components above SIGTRAN are also relevant when migrating from IPv4 to IPv6; however, discussion for upper layer signaling components is reserved for subsequent sections.

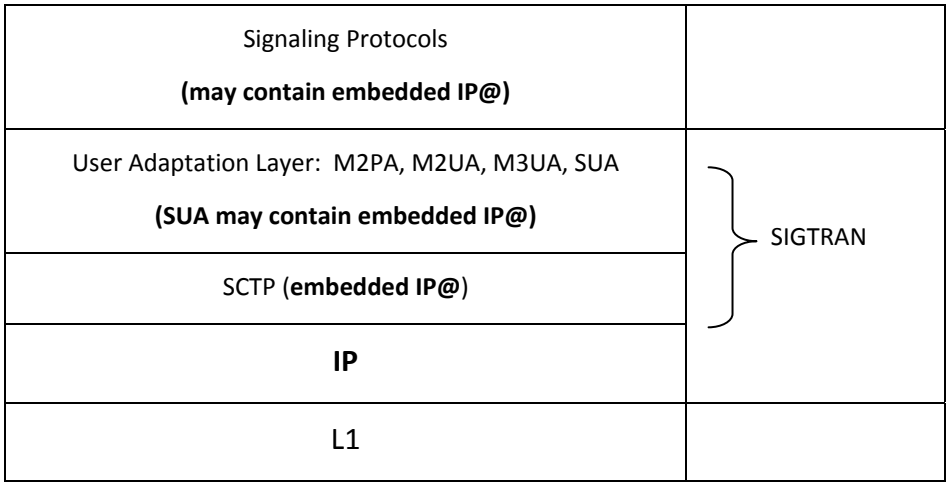

Figure 5.

3.1.1.1 SCTP

To meet the performance requirements of a telephony network in an IP environment, SIGTRAN uses the SCTP protocol defined in RFC 3257. SCTP is a connection oriented protocol that offers multiple services including: Multi-homing, Multi-streaming, Heart-beat, among others.

When migrating from IPv4 to IPv6, of particular note is SCTP's multi-homing service. Multi-homing allows an association to support multiple IP addresses at a given end point. The use of more than one IP address at an end point increases network robustness by providing an alternate path for re-transmissions or allowing re-routing of packets during failure scenarios.

As part of SCTP's multi-homing service, SCTP control packets carry embedded IP addresses during the connection setup process. This allows the end points to exchange IP address lists.

Although SCTP's multi-homing service can provide increased network resiliency, the embedded IP addresses exchanged during connection setup complicate the use of a NAT-PT and the potential inter-working between IPv4 and IPv6 network elements.

As discussed in RFC 4966 section 2.6 [5], use of NAT-PT with SCTP should generally be avoided.

3.1.1.1 USER ADAPTATION (UA) LAYERS

Above the SCTP layer, SIGTRAN offers multiple user adaptation layers including: M2PA, M2UA, M3UA and SUA. The user adaptation layers mimic the services of the lower layers of SS7 and ISDN.

Among the adaptation layers, M3UA and SUA are IP aware and require special attention when migrating from IPv4 to IPv6.

3.1.1.2.1 M3UA

M3UA is defined in RFC 4666. M3UA is IP aware in that it translates point codes to IP addresses and vice versa using a Routing Key. However, M3UA does not exchange IP address information within any of its messages. Rather, M3UA relies on point codes to identify end points and defines boundaries between itself and MTP3, SCTP, and Layer Management.

Because M3UA does not exchange IP address information within any of its defined messages, address translators will operate transparently within the network with respect to M3UA – there is no need for an application layer gateway for M3UA. Still, IPv4 and IPv6 must be considered at the M3UA end points: at the IP protocol port and within the M3UA software.

3.1.1.2.2 SUA

SUA is defined in RFC 3868. SUA supports both connectionless and connection oriented operations. SUA may determine the next hop IP address based on Global Title information (e.g. E.164 number), IP address or pointcode contained in the called party address. Accordingly, some SUA messages such as

CLDT (Connectionless Data Transfer), CLDR (Connectionless Data Response), Connection Request (CORE), Connection Refused (COREF), and COAK (Connection Acknowledge) may embed IP address information as a parameter.

3.1.2 MSC SERVER TO MEDIA GATEWAY – MC INTERFACE

In a distributed MSC environment, the MSC Server uses H.248 on the Mc interface to control a Media Gateway. When planning a migration from IPv4 to IPv6 on the Mc interface, a minimum of three layers must be considered: the network/transport layer, the SCTP layer, and the H.248 layer.

3.1.2.1 NETWORK/TRANSPORT LAYER

At the network/transport layer, the 3GPP standards allow for the following Mc interface options:

1.) A mixed IP & ATM connection –H.248/M3UA/SCTP/IP/AAL5/ATM as an example

2.) A pure IP connection -- H.248/M3UA/SCTP/IP with M3UA as an optional layer.

3.) A pure ATM connection -- H.248/MTP3b/SSCF/SSCOP/AAL5/ATM

The first two interface options both utilize IP and must be considered when migrating from IPv4 and IPv6. The third option involves no IP addressing and is therefore excluded from this paper.

In the first two options, the Mc interface IP connections may be either IPv4 or IPv6. The diagram below provides a protocol stack for the Mc interface in the "pure IP" connection and "mixed IP & ATM" connection cases. Note that the M3UA layer is an optional layer in the "pure IP" case. [3GPP TS 29.232 V4.17.0 (2007-06) – page 11].

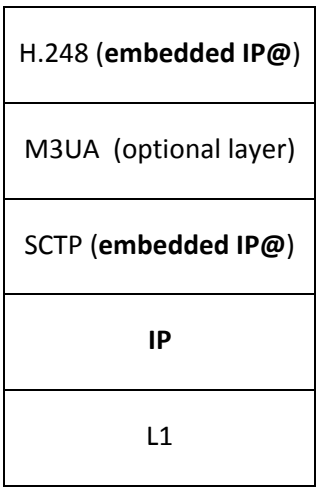

Figure 6.

3.1.2.2 SCTP AND M3UA

The Mc interface uses the SCTP protocol and may optionally use the M3UA layer as discussed in section 6.1.1. The SCTP layer embeds IP addresses during connection setup which complicates the use of NAT-PT for IPv4 to IPv6 migrations. For more information on SCTP and M3UA refer to section 6.1.1.

3.1.2.2 H.248 LAYER

Above the network/transport and SCTP layers, and within H.248 layer, IP addresses are also embedded.

For example, during a call setup across an IP backbone, the MSC server will send an H.248 Add request to the local MGW to create a context. The local MGW responds to the MSC server with an H.248 Reply message. Inside the Reply message is the local descriptor which contains the local MGW's bearer IP address. The local descriptor makes the MSC server aware of the IP termination point for which it must direct the incoming IP media stream.

Similarly, the remote MGW provides its bearer IP address to its controlling MSC server within the H.248 messaging. This IP address (part of the "Remote Descriptor") is relayed to the local MGW. The local MGW uses this Remote Descriptor IP to appropriately address the outgoing media stream.

This exchange of IP addresses within the H.248 layer allows for the dynamic switching of VoIP packets between MGW contexts.

As mentioned in the example above, H.248 commands may specify an IPv4 or IPv6 address anywhere a Local, Remote and/or a LocalControl Descriptor are utilized [ITU-T Rec. H.248.1 (09/2005) – Annex C].

3.1.2.3 H.248.37

Because H.248 messaging between the call server and MGW effectively relays IP address information between MGWs, H.248 by itself does not allow for NAPT traversal between MGWs. To overcome this limitation, H.248.37 was developed.

H.248.37 allows the MSC Server to instruct a MGW to latch to an address provided by an incoming Internet Protocol (IP) application data stream rather than the address provided by the call/bearer control. This enables the MGW to open a pinhole for data flow. It also allows the MGW to ignore the RemoteDescriptor MGW IP address information provided in the H.248 messaging.

When the NAPT parameter on a termination/stream is set to LATCH, the MGW ignores the IP addresses received in the RemoteDescriptor. Instead, the MGW will use the source address and source port from the incoming media stream (i.e., from the other termination) as the destination address and destination port of the outgoing application data.

Ignoring the RemoteDescriptor IP addresses in the H.248 messaging, makes IP address translation within the network transparent to basic MGW operations. Thus, H.248.37 could be used to allow interworking of an IPv4 MGW with an IPv6 MGW, allow two IPv4 MGW's to communicate across an IPv6 backbone, and/or help facilitate an IPv4 to IPv6 migration. Still, H.248.37 has a serious limitation as discussed below.

H.248.37 assumes that the media stream has *already* been established and VoIP traffic is *already* flowing between MGWs. For H.248.37 and NAT-PT to be effective in allowing interworking of IPv4 to IPv6 capable MGWs, the media stream must first be established with an IP address provided in the H.248 messaging. This implies that either the call server includes an Application Level Gateway Control Function (ALGCF) to control a dynamic NAT [6], or it implies that static address translation is used between the MGWs.

3.1.3 MSC TO RNC FOR UMTS ACCESS SUPPORT – IU-CS INTERFACE

The UMTS access network is connected to the MSC via the Iu-CS interface. Standards allow for Iu-CS to be transported over ATM or IP. With either transport option, Iu-CS over IP or Iu-CS over ATM, the Iu-CS interface can be logically divided into three areas:

1. Control Plane
2. Bearer Control Plane
3. Bearer (or User) Plane

3.1.3.1 IU-CS CONTROL PLANE

The Iu-CS control plane carries RANAP signaling between the UTRAN and MSCS.

3.1.3.2 IU-CS OVER IP

For the Iu-CS over IP control plane, three layers must be considered when migrating from IPv4 to IPv6: the network/transport layer, the SCTP layer, and the RANAP layer. Notice the protocol stack shown in the figure below (3GPP TS 25.412 section 5.2.3).

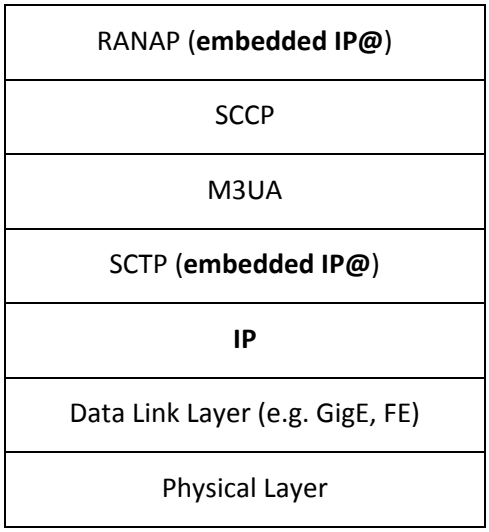

Figure 7.

As discussed in section 6.1.1, SCTP offers a multi-homing service which provides redundancy between two SCTP endpoints. As part of multi-homing, SCTP messages exchange IP transport layer addresses during connection setup [8].

In the RANAP layer, transport layer IP address are exchanged between the RNC and MGW using the Prepare_IP_Transport procedure.

In the Prepare_IP_Transport procedure, the MSC server requests the MGW to provide IP Transport Address and an Iu UDP Port and provides the MGW with the bearer characteristics. After the MGW has replied with the IP address and UDP Port, the MSC server requests access bearer assignment using the provided IP address and UDP Port in accordance with 3GPP TS 25.413.

The IP addresses and UDP Ports of the MGW and the RNC are exchanged via the RANAP procedures. If the bearer transport is IP and IuUP mode is Transparent, when the MSC receives the RANAP RAB assignment response it sends the RNC IP address and UDP Port to the MGW Access bearer termination using the Modify_IP_Transport_Address procedure.

If the bearer transport is IP and IuUP mode is Support, the MGW uses the source IP address and UDP Port of the IuUP Init packet received from the radio access network as the destination address for subsequent downlink packets. The RNC is already aware of the MGW IP address because the Call Server provides the RNC the Media Gateway's IP address in the RAB Assignment Request message.

3.1.3.3 IU-CS OVER ATM

In the Iu-CS over ATM configuration, the control plane uses broadband SS7 signaling which does not require IP.

It should be noted however that some vendors, in particular those who have an all-IP MSC server, may convert M3UA/IP to broadband SS7 in a Signaling Gateway (SGW) or MGW. Because this type of implementation is vendor specific, IPv4 to IPv6 migration concerns should be worked directly with the vendor for the Iu-CS over ATM interface.

3.1.3.4 IU-CS BEARER CONTROL PLANE

The bearer control plane is only applicable for Iu-CS over ATM, and does not need to be considered when planning an IPv4 to IPv6 migration.

3.1.3.5 IU-CS BEARER (OR USER) PLANE

The Iu-CS bearer can utilize ATM or IP at the transport layer. In an ATM configuration, the bearer is transported over AAL2 virtual circuit connections. In an IP configuration, bearer is transported over RTP/UDP/IP [9].

A protocol stack of the Iu-CS Bearer using IP transport is provided below.

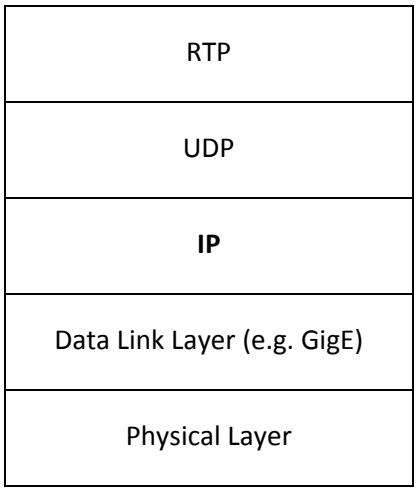

Figure 8.

MSC to TCU/BSC for GSM Access support – A Interface

At the time of the writing of this document, standards for A-interface over IP standards were still being developed by 3GPP. Previously, the A- interface implementation did not utilize or support IP. A-Interface is therefore excluded from this paper.

3.1.4 MSC TO MSC INTERFACES

3.1.4.1 BICC ARCHITECTURE

Bearer Independent Call Control (BICC) is a signaling protocol used to support narrowband ISDN service independent of the bearer technology and signaling message transport technology used.

BICC was developed to be interoperable with any type of bearer, such as ATM, IP, and TDM. The following section focuses on BICC when used in an IP network.

Three interfaces are defined in a BICC architecture:

Nb – MGW to MGW

Mc -- (G)MSC Server to MGW

Nc – MSC Server to (G)MSC Server

3.1.4.2 NB INTERFACE

The Nb interface transports bearer information between MGWs. The 3GPP standards support TDM, IP, and ATM transport on the Nb interface. The protocol stack of the Nb interface using IP transport is provided below:

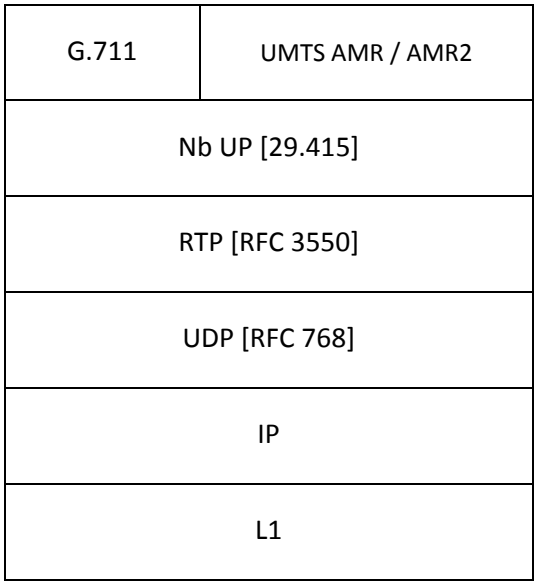

Figure 9.

3.1.4.3 TUNNELING ACROSS THE MC AND NC INTERFACES

Because BICC is "Bearer Independent" it utilizes other protocols for exchanging media stream characteristics.

In an ATM network, BICC uses ALCAP/Q.2630 signaling for bearer control of Nb. The ATM bearer control is carried directly between MGWs alongside the bearer traffic.

In IP networks, the IP bearer control is not carried directly between MGWs alongside the bearer traffic. Nb bearer control is tunneled between MGWs via the Mc and Nc interfaces using IPBCP (IP Bearer Control Protocol – Q.1970). The figure below illustrates the path for IPBCP.

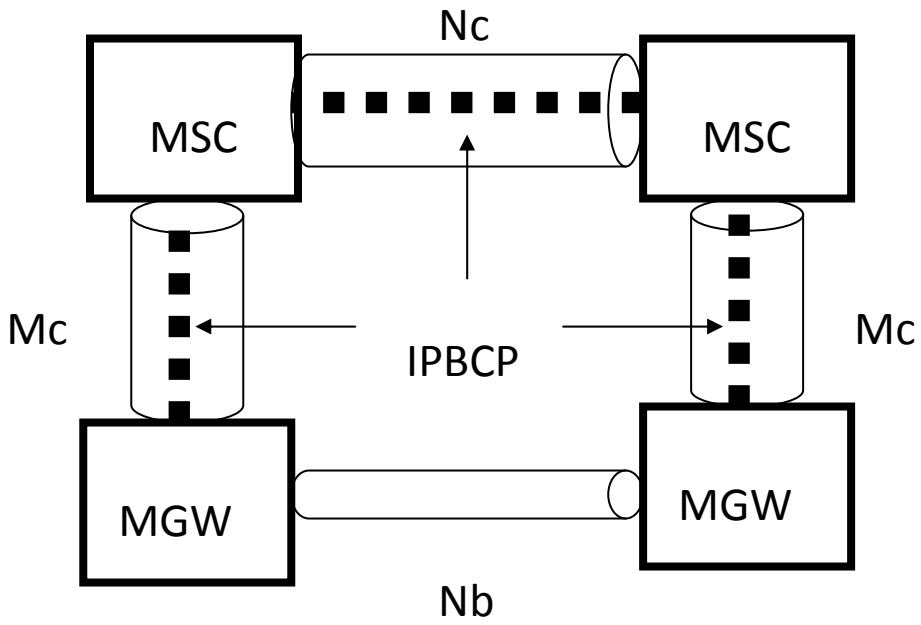

Figure 10.

IPBCP protocol allows the establishment and modification of IP bearers on the MGWs. IPBCP exchanges media characteristics such as port numbers and IP addresses of the source and sink of a media stream. The exchange of information with IPBCP is done during BICC call establishment and after a call has been established. IPBCP uses a subset of the Session Description Protocol (SDP) defined in 3GPP 29.414 to encode the information.

Although the transport layers for the Mc and Nc interfaces may consist of various protocols, the figure below provides the protocol stack for IPBCP when IP is the transport type.

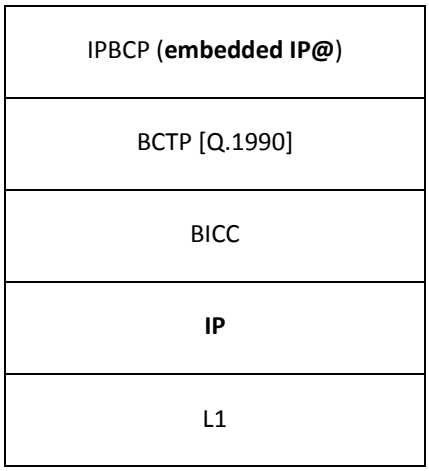

Figure 11.

3.1.5 SIP-I

SIP-I is an extension of the SIP protocol. SIP-I is used to transport ISUP messages across a SIP network as attachments to the SIP messages.

Similar to BICC, SIP-I provides a mechanism by which two MSCs can be connected over an IP network. Though BICC was the first protocol standardized by 3GPP for inter-MSC Voice over IP connectivity, BICC is limited to operation in a GSM/UMTS environment. Thus, many operators have opted to use SIP-I for MSC interconnect.

To exchange media stream information between MGWs, SIP-I utilizes the Session Description Protocol (SDP).

3.2 MIGRATING THE VOICE CORE FROM IPV4 AND IPV6

As described in the preceding section, migration of the voice core from IPv4 to IPv6 is a complex activity requiring consideration of numerous protocols and layers above the IP network layer.

One of the primary drivers for a migration from IPv4 to IPv6 is to alleviate IP address consumption. Since the majority of IP addresses are consumed by end user devices, and a full migration of the voice core from IPv4 to IPv6 is highly complex, in most cases it will not be feasible to migrate an operators' entire 3GPP voice core to IPv6. Instead, it is much more probable that a migration of IPv4 to IPv6 within the voice core will only be targeted at specific interfaces.

For example, an operator may opt to leave all Iu-CS/IP and *intra*-call server MGW to MGW traffic as IPv4 while making all *inter*-call server MGW to MGW traffic IPv6. This type of architecture would allow the network operator to only require dual stack capable MGWs on the network bound (vs. access) interfaces and would avoid the need for an IPv6 capable RNC.

4. IMPACT OF THE INTRODUCTION OF IPV6 ON SECURITY IN UMTS

IPv6 currently has relatively limited deployments, thus few vulnerabilities have been exploited. As adoption expands, like in IPv4, attacks on the protocol will emerge unless sufficiently protected. IPv6 security issues have implications directly for the IP layer, and indirectly for application support and the link layer. And these security issues can be examined with respect to end-to-end security, end-to-gateway and gateway-to-gateway connections. The implementation of IPv6 requires extensions to the existing security policy as well as introducing new security policies specific to IPv6. The security concerns (threats and vulnerabilities) and specific solutions comprise those issues common to IPv4 and IPv6, those security issues specific to the transition to IPv6, and those specific to IPv6. IPv6 must be managed to provide an equivalent level of security as is provided for IPv4.

The following sub-section provides a concise summary of security issues related to IPv6. Sections 0 and 0 provide an overview of how these issues impact or do not impact 3GPP and LTE.

4.1 IPV6 SECURITY ISSUES OVERVIEW

4.1.1 SECURITY ISSUES COMMON TO IPV4 AND IPV6

Many security issues and solutions common in IPv4 implementations project forward into IPv6.

Firewalls are required to be updated to support firewall rules specific to IPv6, as well as updates for SSH (Secure Shell protocol for remote login/file transfer).

IPsec, AH (authentication header) and ESP (encapsulating security payload) function essentially the same for both IPv4 and IPv6. IPsec can be used to support the routing protocols, Routing Information Protocol (RIP) & Open Shortest Path First (OSPFv3), if required. The Virtual Private Network (VPN) model in use must be updated to add IPv6 support. The IPv6 configuration in IKEv2 is still being worked on in the IETF and currently is defined with limitations with respect to IKEv2 and IPv6 functionality. Refer to IETF draft, *IPv6 Configuration in IKEv2*.

For Domain Name System (DNS) and DNSSEC the same security concerns apply to IPv6 as IPv4. There is no new impact to Transport Layer Security (TLS) functionality with the introduction of IPv6. Application-layer attacks have the same vulnerabilities. No new security concerns for Border Gateway Protocol (BGP) are introduced with IPv6.

Updates are required to support IPv6 for: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

With respect to the benefits of Network Address Translation (NAT), IPv6 provides alternative mechanisms. NAT is often used to perform the tasks of a firewall by establishing dynamic state for connections to protect against unauthorized, ingress traffic, and also to perform topology hiding. NAT should not be used as a substitute for a firewall. NAT is not invulnerable and once compromised it is easy for attackers to scan the private address space on the inside of the NAT for open ports. It

should also be noted that NAT complicates the use of IPsec for end-to-end encryption. For example, there is additional overhead required to support UDP encapsulation and NAT keep-alive messaging.

IPv6 provides several mechanisms to support topology hiding. The size of a single IPv6 subnet makes ping sweeps and port scanning for network vulnerabilities unprofitable. Simply assigning multiple IPv6 addresses to a host, difficult in IPv4 due to the limited address space and on some hosts not supported, can aid in concealing the nodes in the internal network. Unique Local IPv6 Unicast Addressing can be used for address allocation within a site - this traffic is for communication within a site and should never be routed outside the internal network. Untraceable IPv6 addressing (random prefix allocation within a subnet) can be used to conceal the size and topology of the network, as opposed to sequential numbering within a subnet, commonly employed in IPv4 due to the limited number of available addresses.

Refer to Local Network Protection for IPv6 (RFC 4864), for a more complete understanding.

4.1.2 SECURITY ISSUES INVOLVED IN TRANSITION TO IPV6

The introduction of IPv6 has impacts on security relating to the transition mechanisms of dual-stack, tunneling, and translation.

Dual-stack

Active IPv4-only networks may already be vulnerable to IPv6 attacks if IPv6-capable devices (dual-stack) are included. The security policy should determine whether IPv6 packets in the IPv4-only network should be blocked as IP-in-IP packets (41 in protocol field of IPv4 header) that may be concealing IPv6-in-IPv4 attacks.

Refer to RFC 4942, *IPv6 Transition/Coexistence Security Considerations*, for a complete description of issues with supporting a dual-stack environment.

Tunneling

There are several tunneling mechanisms proposed to allow IPv6 traffic to traverse IPv4-only networks. Some are based on static configuration and some support automatic tunneling. In general, static tunneling is more secure than automatic tunneling, but does not scale well. Tunneling mechanisms that are constructed using IP-in-IP, as 6in4 static or 6to4 automatic tunneling, cannot traverse a NAT when port translation is required (NAPT). Many of the automatic tunneling mechanisms, as 6to4, ISATAP and Teredo, use embedded IPv4 addresses within the 128-bits of the IPv6 address.

Depending upon the tunneling mechanisms employed, filtering may be required at firewalls to block IP-in-IP or IPv6 addresses with embedded IPv4 addresses. Embedded addressing may introduce vulnerabilities that are able to traverse firewalls.

Refer to IPv6 Operations and Softwires IETF working groups for additional RFCs and drafts on IPv6 security mechanisms related to tunneling, www.ietf.org.

Translation

Refer to IETF draft, *A Comparison of Proposals to Replace NAT-PT*, for current status of possible co-existence mechanisms.

Refer to the following reports for a more complete understanding of IPv6 security issues:

- *North American IPv6 Task Force (NAv6TF) Technology Report*, http://www.6journal.org/archive/00000287/01/nav6tf.analysis_ipv6_features_and_usability.pdf
- *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation*, http://www.seanconvery.com/v6-v4-threats.pdf

4.1.3 SECURITY ISSUES SPECIFIC TO IPV6

IPv6 address selection algorithm (source and destination) security has impacts with respect to ingress filtering and attempts at session hijacking. This concern also applies for dual-stack nodes and tunneling environments.

IPv6 privacy extensions, which are used to vary the Interface Identify by the end node, can be used to thwart device profiling.

New firewall rules for IPv6 are required to support policy for ICMPv6 and IPv6 extension headers: which ICMP messages to allow or deny, e.g., Packet Too Large for PMTU, which extension headers to allow or deny, e.g., deny Routing Header Type 0, whether to allow Routing Header Type 2 for MIPv6 Route Optimization. Refer to RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls* and RFC 4942, *IPv6 Transition/Coexistence Security Considerations*.

IPv6 stateless address auto-configuration uses new ICMP messages in Router Advertisements (RA)/Router Solicitations (RS) and Neighbor Advertisements (NA)/Neighbor Solicitations (NS) that assist an IPv6 node in constructing an IPv6 address. New vulnerabilities are introduced if the link is compromised. NA/NS and RA/RS can be protected using a link-level security mechanism, as, for example, the Secure Neighbor Protocol (SEND) and Cryptographically Generated Addresses (CGA) to determine whether a router on the link is a trusted router. However, deployment of CGA may be limited due to Intellectual Property Rights issues and some technical concerns. Refer to the IETF working group, Cga & Send maintenance (csi) for current status.

Certain IPv6 addresses should be filtered at the firewall, for example: IPv6 loopback, IPv4-mapped address, unique local address, site local address, certain multicast addresses. The IPv6 use of multicast addressing introduces the potential for new vulnerabilities. Certain resources internal to the network are identifiable by multicast addressing. These addresses should be filtered at the

network boundary, depending upon their scope. These addresses also introduce the potential for DoS attacks. Also, IPv6 anycast addresses, such as Mobile IPv6 Home Agent anycast or Subnet-Router anycast, can potentially be used in DoS attacks.

IPsec support is built-in to IPv6, which will allow for more instances of end-to-end encryption, consistent with the design of IPv6 to move more of the responsibility for the session to the end users. However, end-user encryption makes execution of IDS more difficult. In general, consistent with the design of IPv6, some level of security may be moved down to the end nodes, either for encryption or at the application level. Security may be transitioned from a perimeter model to a distributed model.

Performance considerations of IPv6 security mechanisms must be balanced against risk.

MIPv6

Several security issues/mechanisms are introduced with MIPv6.

IPsec can be used to secure communication between the mobile node and the home agent. As an alternative to IPsec, securing of binding updates and binding acknowledgements can be performed using MIPv6 signaling messaging between the Mobile Node (MN) and the Home Agent (HA). Refer to RFC 4285.

In MIPv6, packet loss due to egress filtering at the access router is prevented by placing the IPv6 mobile node's care-of address in the external IP header when in a foreign network.

Dynamic Home Agent Address Discovery relies upon special ICMP messaging, which is required to pass through the network firewalls.

Route optimization allows the mobile node and the correspondent node to communicate directly (rather than via the home agent), without pre-arranged security associations. Additional messaging is required to perform return routability for route optimization. In route optimization, a mobile node reveals its care-of address (current point of attachment) to the correspondent node. The care-of address can be traceable to a particular location. It is a concern that a mobile user's location can be compromised when route optimization is used.

Hierarchical MIPv6 can be used to mitigate location privacy issues with route optimization.

Issues with Mobile IPv6 security have considerable implications for end users and the network, and is too large a topic to due justice to here. Refer to the IETF Mobility EXTensions for IPv6 (mext) working group related RFCs for additional information.

Security Support Tools

Additional considerations include the status of common, security support tools: *Nessus* (vulnerability scanner), *Nmap* (port scanner), *Wireshark* (packet analyzer), *netcat* (packet read/write), *hping* (packet generator), *Snort* (packet sniffer), to list only few of the open source and commercial products which all have varying levels of support for IPv6. The Status of commercial firewalls, IDS and IPS to support IPv6 is not mature. Refer to National Institute of Standards and Technology (NIST) report, *Firewall Design Considerations for IPv6*.

4.2 OVERVIEW OF UMTS SECURITY AND IPV6

4.2.1 IPV6 IMPACTS TO UMTS END-USER SECURITY

In Packet Date Protocol (PDP) Context activation using IPv6 stateless address auto-configuration, the Gateway GPRS Support Node (GGSN) assigns both an IPv6 Interface Identifier and /64 prefix to the Mobile Station (MS). The prefix is unique within its scope. The GGSN and MS are the only nodes on the local link, thus Duplicate Address Detection is not required. The MS is authenticated by the network and the PDP Context is tunneled within the network. The need for additional security measures, such as SEND and CGA are not required for the PDP Context within the 3GPP network.

The GGSN acts as an anchor for the PDP Context, eliminating the need for MIPv6, prior to release 8 (LTE).

3GPP supports IPv6 privacy extensions for the PDP Address. The PDP Context is identified by the IPv6 prefix at the Serving GPRS Support Node (SGSN) and GGSN and not by the full 128-bit PDP Address.

For IMS, the GGSN provides the address of the P-CSCF to the MS for Proxy Discovery. The MS, GGSN and P-CSCF must support the same IP version. The MS point of attachment is at the external interface of the GGSN. IMS relies upon SIP signaling between end user and P-CSCF IMS. SIP signaling is protected by IPsec or TLS. This protection is independent of the Access Network protection mechanisms.

For IMS security, refer to IMS TS 33.203. For IPv4-IPv6 inter-working scenarios, refer to 3GPP TS 23.981.

4.2.2 IPV6 IMPACTS TO UMTS PACKET NETWORK SECURITY

Security protection is specified for GTP control traffic. Protection of user traffic is considered outside the scope of the standards.

TS 32.210 describes the minimum security features in support of data integrity, origin authentication, anti-replay protection, and confidentiality. 3GPP Network Domain Security provides hop-by-hop protection, which allows for separate security policies depending upon whether a link is intra-domain

or inter-domain and whether between trusted or un-trusted domains. Security Gateways are stationed at the network boundary - all traffic between security domains is via a Security Gateway. Authentication and integrity protection are mandatory between two security domains and encryption using ESP in tunnel mode is optional. Protection of traffic within the Security Domain is optional.

Firewalls at network boundaries are required to protect against unauthorized traffic.

The IMS network topology can be hidden by encrypting the IMS network element IP addresses in SIP messages.

Refer to TS 33.102, 33.203, 33.210 and 33.310 for details of Network Domain Security and TS 33.234 for WLAN inter-working security.

4.3 IPV6 IMPACTS ON LTE SECURITY IMPLEMENTATION

The LTE specification supports a flat-IP network based upon TCP/IP protocols. General security and end-user privacy principles for the EPS are specified in TS 22.278. LTE-specific security is detailed in TS 33.203, 33.401, 33,402 and 33.178.

The LTE UE supports dual-stack, which may use simultaneous IPv4 and IPv6 addresses, over an EPS Bearer (MIP between S-GW and P-GW) or PDP Context (GTP tunneling).

LTE supports inter-working between 3GPP EPS and UTRAN, WLAN, CDMA, WIMAX and GERAN. Secure hand-over is supported between EPS and non-EPS access networks. This incurs additional complexity with respect to security to support mobility, key transfer and algorithm negotiation, DS-MIPv6 or PMIPv6, and support for IPv4 private addressing.

4.4 IPV6 SECURITY RECOMMENDATIONS

It is obvious but significant to stress the importance of training and planning for the adoption of IPv6 with respect to security. Once a security policy is established, it is necessary to stay current and vigilant with security vulnerabilities and with IPv6-specific updates and vulnerabilities, as IPv6 continues to be adopted.

Not all security support is equal - know the capabilities/limitations of hosts and routers in network: IPv6 stack support, privacy extensions, IPsec, and filtering capabilities.

Determine a balance across risk, overhead and performance of security mechanisms.

5. CONCLUSIONS

The growth of always-on always-reachable services and the depletion of IPv4 addresses are two key drivers moving carriers to consider transitioning to IPv6. IPv4 will coexist with IPv6 for several years; therefore, transition mechanisms and coexistence techniques will be used as the carriers' transition to IPv6.

Carriers evolving their networks to LTE should consider making IPv6 a requirement from day 1. Since LTE EPC does not support a Circuit Switched Core as part of the 3GPP standard, native support for voice will be supported by the IMS core. Because the transition to IMS-based VoIP will likely take several years, it is critical for the carriers to understand the impacts of IPv6 on the existing Voice Core and signaling infrastructure. Lastly, it is absolutely critical that the transition to IPv6 consider network security.

6. ACKNOWLEDGEMENTS

The mission of 3G Americas is to promote and facilitate the seamless deployment throughout the Americas of the GSM family of technologies, including LTE. 3G Americas' Board of Governor members include Alcatel-Lucent, AT&T (USA), Cable & Wireless (West Indies), Ericsson, Gemalto, HP, Huawei, Motorola, Nokia Siemens Networks, Nortel Networks, Openwave, Research In Motion (RIM), Rogers Wireless (Canada), T-Mobile USA, Telcel (Mexico), Telefonica and Texas Instruments.

We would like to recognize the significant project leadership and important contributions of Paul Smith of AT&T as well as the other member companies from 3G Americas' Board of Governors who participated in the development of this white paper.

7. REFERENCES

[1] GPRS enhancements for E-UTRAN access (Release 8); 3GPP TS 23.401; in progress

[2] Architecture Enhancements for non-3GPP accesses (Release 8); 3GPP TS 23.402; in progress

[3] Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), 3GPP TS 36.300; in progress

[4] Transitioning to IPv6; 3G Americas; February 2008

8. GLOSSARY

AAA	Authentication, Authorization and Accounting
ALG	Application-Level Gateway
APN	Access Point Name
CDR	Call Detail Record
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EMS	Element Management System
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Number Authority
ICE	Interactive Connectivity Establishment
IMS	IP Multimedia Subsystem
ICID	IMS Charging Identity
NAT	Network Address Translation
NOC	Network Operation Center
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDP	Packet Data Protocol
QoS	Quality-of-Service
RAB	Radio Access Bearer
RAN	Radio Access Network
RIM	Research in Motion
RIR	Regional Internet Registry
RNC	Radio Network Controller
RTCP	Real-Time Control Protocol
RTP	Real-Time Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SLAAC	Stateless Address Auto-Configuration
SIP	Session Initiation Protocol
SGSN	Serving GPRS Support Node
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URI	Universal Resource Identifier
VPN	Virtual Private Network