Transitioning to IPv6

3G americas℠

March 2008

Executive Summary

As UMTS/HSPA and IMS networks are deployed, the wireless industry will continue to experience explosive growth. New always-on services will require the device to be always available. As a result of this, wireless service providers will require a substantial number of IP addresses to support such services.

At the same time, IPv4 addresses are being depleted at an extremely fast rate. They will cease to be available from the official registries within the next five years. When new IPv4 address blocks cease to be available, service providers will face increasing operational and capital expenses to survive as long as possible on a dwindling pool of IPv4 address.

Rather than wait for the inevitable, this report strongly recommends that service providers begin transitioning to IPv6 as soon as possible. Not only does IPv6 solve the address exhaustion problem, it will likely enable new services perhaps impossible in an IPv4 world.

This report analyzes in detail the impacts a wireless service provider faces when introducing IPv6. It investigates three use cases in detail: (a) a Video Share service; (b) Gaming services; and (c) a Blackberry service. Based on these use cases, it provides the following recommendations:

1. Develop a transitioning plan.

   This is the first order of business. Identify the IPv6 transitioning lead in the organization. Assess the readiness of existing equipment. Develop a transitioning plan.

2. Use a phased approach.

   For wireless service providers it is possible to start deployment of IPv6-capable mobile devices, while continuing to run IPv4 in most of the network. Introduction of IPv6-capable devices would require IPv6 support on GGSN, P-CSCF and application servers. In addition, many other systems will need to be IPv6-aware but would not have to run IPv6 themselves.

3. Develop a solution for IPv4-IPv6 interworking.

   One of the most important matters facing a wireless service provider is the assessment of how to support IPv4-IPv6 interworking. In general, it is preferred to use dual-stack mobile devices, in which the device uses IPv6 to communicate with IPv6 capable devices, and IPv4 otherwise. Due to the limitations in simultaneous PDP Contexts and Radio Access Bearers, however, this (simultaneous) dual-stack approach may not always be feasible in UMTS networks. In that case, translation is the preferred alternative.

4. Security Considerations.

   Over time, IPv4 networks have established a clear set of rules with respect to security. Introduction of IPv6 changes several networking aspects. Service providers and enterprises should carefully assess the impact of IPv6 and develop a new set of security policies.

Table of Contents

1 The need for IPv6

1.1 *IPv4 address exhaustion*

The exhaustion of IPv4 addresses was already foreseen before the Internet became a worldwide phenomenon. As early as 1990, the Internet Engineering Task Force started looking for a successor for IPv4 (see [3]). However, at the same time, other mechanisms, such as the use of Private Addresses, were introduced to stave off an immediate crisis. This caused some people to hope that perhaps the transition to IPv6 could be postponed indefinitely. A careful analysis of available data, however, shows that IPv4 address exhaustion is progressing unrelentingly and the most recent predictions are that in less than 5 years it will become impossible to receive new address blocks from official registries.

The "IPv4 Address Report" presents a thorough analysis of the expected depletion of IPv4 addresses (see [2]). It analyzes three stages of IP address usage:

1. Address blocks allocated by Internet Assigned Number Authority (IANA) to the Regional Internet Registries (RIRs)

2. Address blocks allocated by the RIRs to Internet Service Providers and other local entities

3. Addresses that appear in Internet routing tables

Extrapolating from existing data, the report anticipates that IANA will run out of addresses in May of 2011. The RIRs will run out of addresses in August of 2012.[1]

Based on its analysis of actual usage of IPv4 addresses, the IPv4 Address Report has found that not only do IANA and the RIRs allocate address blocks at an increasing pace, but the percentage of allocated addresses that are actually being used in the Internet is increasing as well.

When IANA and the RIRs run out of IPv4 addresses, many service providers will still have unallocated address blocks. However, to stave off total exhaustion as long as possible, service providers would have to fragment address pools in increasingly smaller sets and at times may have to reallocate addresses. Alternatively, service providers and enterprises could start trading unallocated address blocks. In either case, address management becomes an increasingly cumbersome and expensive procedure.

1.2 *Other advantages of IPv6*

The good news is that a transition to IPv6 is not merely a way to use a larger address pool. It has several other advantages. We will not describe these in detail, as they have been the subject of many other white papers. See, for example, [4] and [5] . Advantages of IPv6 include:

- Simplified header processing.
- Less fragmentation of the address space, leading to smaller routing tables.
- Built-in support for Mobile IP,
- Support for route optimization in Mobile IP.
- Support for address auto-configuration.
- Reduced dependency on translation devices.
- More sophisticated flow identification, potentially leading to improvements in QoS support.

[1] The IP Address Report is regularly updated. The quoted dates are from the report dated January 30, 2008.

Together, these features simplify network operations and user plane forwarding. It should be noted, though, that during the transition phase, in which both IPv4 and IPv6 are being deployed, operations as well as user plane forwarding will be more complex than in an IPv6 *or* IPv4-only world.

1.3 *IPv6 in standards*

In general, IPv6-related standards are extensive and mature. The first version of the IPv6 specification, RFC 1883, was published in 1995 ([6]). The original IPv6 Working Group in the IETF was recently closed because it had met all its targets.

For an overview of remaining issues and the standards organizations in which they are addressed, refer to ATIS reports on IPv6, [7] and [8].

1.4 *To transition to IPv6 or not?*

A critical question for many service providers is when to transition to IPv6. As pointed out in section 1.2, IPv6 has several benefits which will result in a simpler, more powerful and more efficient network. The sooner a service provider achieves these benefits, the sooner it will be at a competitive advantage compared to service providers who delay transition. The risks of delaying the transition are the following:

- Managing a dwindling IPv4 address space will become increasingly expensive. Address allocation requires careful planning; previously assigned address blocks may need to be recovered, which is a complex process; and the management of additional devices such as Network Address Translation (NAT) devices add to the cost.

- The service provider that delays transition to IPv6 may not be able to deliver the same services as service providers that have made the transition to IPv6. The ability to support always-on and peer-to-peer services is impaired when traffic has to traverse NAT devices. For example, always-on services require that a user is always reachable and therefore cannot share a pool of public addresses with other devices. This can be mitigated through address *and* port translation, but also that has its limitations.

- At some point, a service provider who has not made the transition to IPv6 may become unattractive as a roaming partner to service providers who have made the transition. The same may be true in retail/wholesale relationships.

On the other hand, transitioning to IPv6 at an early stage also has certain risks. The transitioning process is complex. It requires a significant investment in planning and training. During the transition period, the service provider must run both IPv4 and IPv6 systems concurrently, which leads to an increase in operational expenses. Furthermore, there is a risk of service interruption, customer dissatisfaction and penalties. All service providers will need to go through this, but an early adopter may run into problems which later adopters could avoid.

In the end, we believe that service providers don’t have the option to delay IPv6 introduction. The exhaustion of IPv4 addresses will force a transition to IPv6, and as pointed out in section 1.1, address exhaustion may become a reality within the next five years. From that point on, service providers will face an increase in operations cost, if not because of introduction of IPv6, then due to the complexity of running an IPv4-only network with a diminishing pool of addresses.

With careful planning, the risk of early adoption can be mitigated significantly. Later sections in this white paper provide suggestions for making the process as smooth as possible.

2 Transition Mechanisms

This section describes general (i.e. not UMTS-specific) mechanisms to start deploying IPv6 in networks that still require IPv4 support as well. Section 3 analyzes which mechanisms are best suited for UMTS deployments.

2.1 *Overview*

The transition to IPv6 is expected to be gradual and occur over several years. With this in mind, the Internet Engineering Task Force (IETF) has defined a wide range of transition mechanisms to allow smooth co-existence between IPv6 networks and legacy IPv4 networks.

Such mechanisms fall into three broad categories:

- Dual-stack (enables IPv4 and IPv6 to coexist in the same devices / networks).
- Tunneling (includes configured and automatic tunnels; encapsulating IPv6 packets in IPv4 packets and vice versa).
- Protocol Translation (enables an IPv6-only device to communicate with an IPv4-only device).

2.2 *Dual-Stack*

Dual-stack refers to an IP capable device (e.g. a host computer) supporting simultaneously both IPv4 and IPv6. This enables applications to communicate across either an IPv4 or IPv6 network. Typically, the preferred network is based on name lookup and application preference.

Dual-stack routers support both IPv4 and IPv6 routing protocols, and are able to forward both IPv4 and IPv6 packets. Many of the routers available today support this dual-stack capability. Dual-stack routers in conjunction with dual-stack application servers enable a gradual transition to IPv6, in which legacy IPv4 applications and devices can coexist with newly transitioned IPv6 applications on the same dual-stack network.

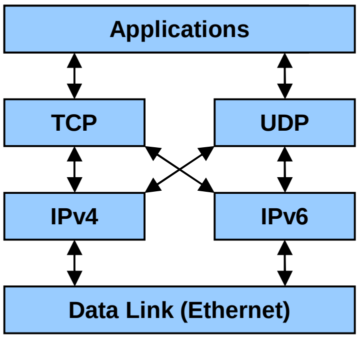


Figure 1: Dual-Stack Reference Architecture

Requiring all new IP-capable devices to support dual-stack is desirable in providing a flexible operational environment for transitioning to IPv6. Ideally, the IPv6 transition process would consist of two phases:

1. Replace all IPv4-only devices with dual-stack devices.
2. Once all devices support both IPv4 and IPv6, introduce IPv6-only devices.

However, it should be noted that dual-stack devices require IPv4 addresses and as such do not mitigate the IPV4 address exhaustion problem. It is therefore likely that service providers will have to start deploying IPv6-only devices before all IPv4-only devices have been converted to dual-stack support. Therefore, besides dual-stack, other transition mechanisms will be required.

2.3 *Tunneling*

Tunneling refers to a technique to encapsulate one version of IP in another so the packets can be sent over across a network that does not support the encapsulated IP version. This technique allows two IPv6 islands to communicate across an IPv4 network, or vice versa. Tunneling enables different parts of the network to transition to IPv6 at different times.

There are two main categories of tunneling: configured and automatic tunnels. Configured tunnels refer to a manually configured tunnel within the endpoint routers at each end of the tunnel. The end points are statically configured; hence, any changes to network numbering would require modification of tunnel endpoints. In contrast, automatic tunnels refer to a device dynamically creating its own tunnel to dual-stacked routers for sending IP packets within IP. The IPv6 Tunnel Broker (RFC 3053), 6to4 (RFC 3056), Teredo (Tunneling IPv6 over UDP through NATs) and ISATAP (Intra-site Automatic Tunnel Addressing Protocol) send IPv6 packets encapsulated in IPv4 and can be referenced as IPv6-over-IPv4 mechanisms while DSTM (Dual-Stack Transition Mechanism) sends IPv4 packets within IPv6 and can be referenced as IPv4-over IPv6 mechanism.

Security risks associated with automatic tunneling should be considered, prior to introducing automatic tunneling. For example, automatic tunneling could enable user-nodes to establish tunnels that bypass an enterprise's security mechanisms (e.g. firewalls, intrusion detection…) reducing the depth of security as well as allowing unsolicited traffic. Even though automatic tunneling provides an extremely flexible transition mechanism to move to IPv6, the risks associated with each transition mechanism should be analyzed. As discussed further in section 3, we do not recommend the use of automatic tunneling in the context of UMTS networks.

2.4 *Translation*

Translation refers to a method of translating one version of IP to another. This method does not depend on dual-stack for transition to IPv6, but rather enables devices on different versions of IP to communicate with each other through an intermediate Network Address Translation (NAT) device which performs protocol translation.

NAT is not transparent. Therefore, many applications have difficulty traversing NAT boundaries (e.g. SIP-based services or IPSec VPN). Likewise, NAT introduces additional complexity which impacts operational expense. NAT, also, requires specialized hardware to perform the translation function which impacts capital costs. Lastly, NAT obstructs the ability to perform bi-directional communication, global addressing, always-on systems, peer-to-peer networks, and push services – which are inherent to the design of IPv6.

NAT may be unavoidable, but should only be used as a last resort.

It should be noted, though, that NAT devices play a security role in IPv4 networks. Many enterprises have deployed RFC 1918 private IP addresses in combination with NAT to mitigate IPv4 address shortages. Since private addresses are unreachable from the Internet – Internet routers do not forward IP packets with a private address as destination address – the combination of NAT and private addresses hide the internals of enterprise networks from the rest of the Internet. When transitioning to IPv6 and removing previously used NAT devices, enterprises and operators should pay special attention to the impact on security and privacy. Section 4.4 discusses this further.

2.5 *IPv6-to-IPv4 HTTP Proxy*

One option an operator may consider is the use of an IPv6 Proxy Gateway for general web browsing. This dual stack Proxy Gateway would act as an intermediary between an IPv6 host or UE and a native IPv4 server accessed through the IPv4 Internet. This type of proxy may be limited to HTTP port 80 and long term may offer other functionality including caching, user authentication and content acceleration. This concept allows the operator to provide IPv4 Internet content while transitioning to IPv6 on the mobile user plane. There are considerations the operator must factor when deploying this type of service. The proxy must comply with the operator's security policies and provide proper levels of secure access when opening HTTP communication paths to Internet content. Performance and scalability will also need to be examined since IPv6 to IPv4 Gateways will likely be processor intensive since capabilities may initially be limited to software based solutions.

3 Use Cases

This section discusses three use cases and analyzes the impact of transitioning to IPv6.

3.1 *Video Share Use Case*

3.1.1 Introduction

Video-Share Calling consists of the establishment of a two-way circuit-switched voice call and a one-way packet-switched video stream. Using the video share service, a user can call a second user and subsequently begin sharing video content that is streamed to the second party.

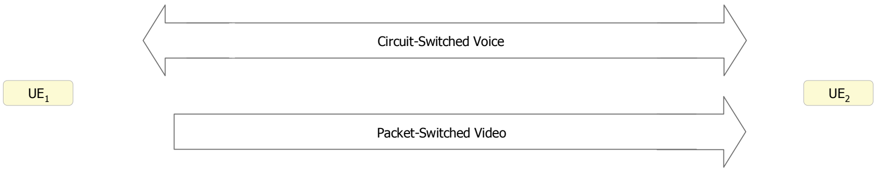


Figure 2*: *A voice call with simultaneous video sharing

For a UMTS subscriber, this use case involves procedures in the UMTS circuit-switched and packet-switched networks, as well as in the IMS core network.

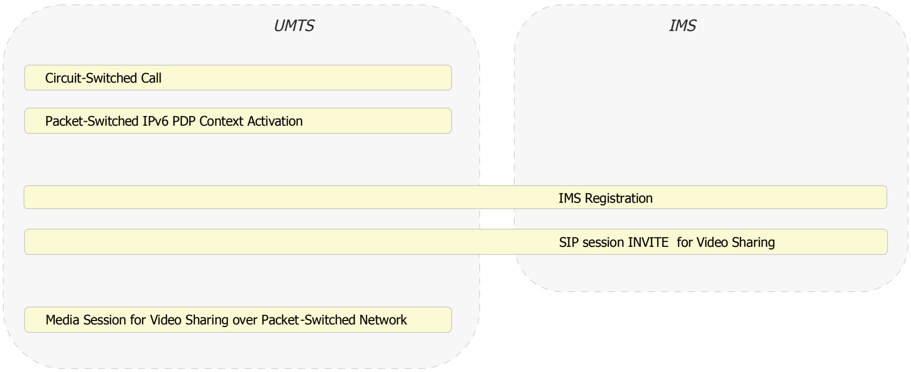

UMTS
IMS
Circuit-Switched Call
Packet-Switched IPv6 PDP Context Activation
IMS Registration
SIP session INVITE for Video Sharing
Media Session for Video Sharing over Packet-Switched Network

Figure 3: The impact of Video Share on UMTS and IMS

In the basic use case, the connection existsx between users within the same UMTS network, where both end users support IPv6. A video sharing client for this example is contained in each of the end users' devices.

The following sections provide detailed procedures for how a Video Share call is set up between two IPv6-enabled devices, both assumed to be in their Home Networks. Roaming is discussed in section 3.1.7; IPv6/IPv4 inter-working scenarios are discussed in section 3.1.9.

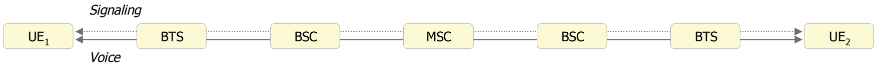


Figure 4: The Circuit-switched call is not impacted by IPv6

The circuit-switched portion of the call is set up and connected via an MSC. Figure 4 shows the network elements in the end-to-end path. This connection does not use an IP packet-switched network to establish connectivity between the end users, and therefore introduction of IPv6 has no impact on the related call control procedures. It is, however, possible that sections of the end-to-end path are transported over IP networks. For example, traffic between MSCs could be transported over an IP network. In that case, the network elements at the edges of those IP networks would be impacted by a transition to IPv6.

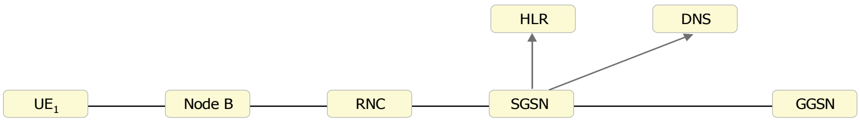


Figure 5: The packet-switched connection is impacted by IPv6

The video connection between the two users is set up over a packet-switched connection and is impacted by IPv6. Figure 5 shows several network elements that are in the path. This section addresses three aspects:

- Attachment.
- IP address assignment.
- IPv6 impact on Radio Access Network and Serving GPRS Support Node (SGSN).
- IPv6 impact on the IP transport network.
- IMS aspects.
- QoS and other policy-based actions.

3.1.2 Attachment

The GPRS attachment procedures are not impacted by IPv6.

3.1.3 IP address assignment

After successfully completing the GPRS attachment procedure, the User Equipment (UE) initiates PDP Context Activation by sending a request for an IPv6 PDP Context. The request includes an Access Point Name (APN). The APN is a reference point identifying an IP domain or service and maps to a GGSN. The APN determines which method is used to assign an IP address (PDP address) to the UE.

A UE is assigned a single IP (PDP) Address per Primary PDP Context. A Primary PDP Context may add multiple Secondary PDP Contexts that each share the same PDP address, but each Secondary PDP Context may support different levels of QoS. A UE may request additional Primary PDP contexts and these will each require the assigning of a different PDP address. For example, a UE may request a Primary PDP Context for IPv6 and another Primary PDP context for IPv4.

Address assignment can be static, via the HLR, or dynamic. If dynamic, it can be stateful (using DHCPv6) or stateless. The stateless mechanism is called IPv6 Stateless Address Auto-Configuration (SLAAC).

In the case of SLAAC, the Gateway GPRS Support Node (GGSN) allocates a 64-bit prefix, unique within its scope, to the UE. The GGSN provides the Interface Identifier to the UE for the IPv6 address. The UE uses this Interface Identifier to create its link-local address. The GGSN and the UE are the only two nodes on the link. This ensures that the Interface Identifier is unique on the link and IPv6 Duplicate Address Detection (DAD) is not required for the UE link-local address. IP address assignment using SLAAC is depicted in Figure 6.

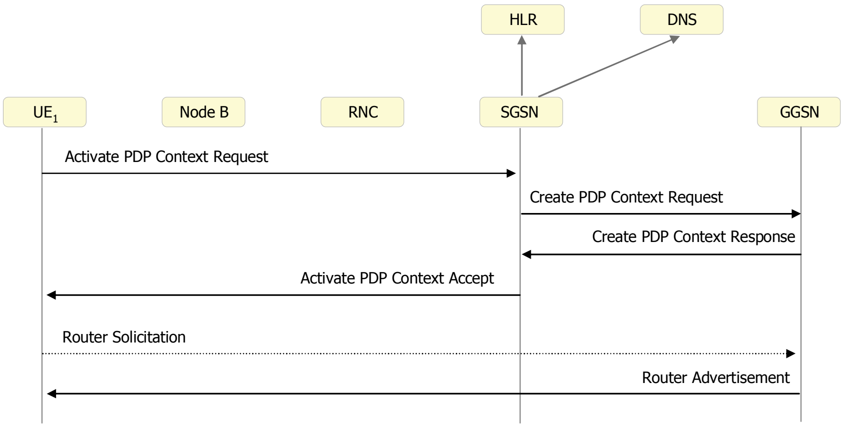

HLR
DNS
UE1
Node B
RNC
SGSN
GGSN
Activate PDP Context Request
Create PDP Context Request
Create PDP Context Response
Activate PDP Context Accept
Router Solicitation
Router Advertisement

Figure 6: IPv6 PDP Context Activation with SLAAC

The use of SLAAC enables *IPv6 Privacy Extensions*. Nodes may replace the Interface Identifier with a random value to create a temporary address. Interface Identifiers derived from a layer-2 address could be traceable to a particular device.

As this section shows, introduction of IPv6 requires that at a minimum UE and GGSN are IPv6 enabled. Depending on the IP address assignment method, the service provider may further need an IPv6-enabled HLR or DHCP server. In the case of HLR and DHCP server, it should be noted that they must be able to assign IPv6 addresses. The interfaces between HLR and GGSN and DHCP server and GGSN may be IPv4 based.

3.1.4 IPv6 impact on Radio Access Network and Serving GPRS Support Node (SGSN)

Figure 7 shows the UMTS user plane protocol stack. The figure shows that with respect to the IP layer seen by the UE, the GGSN is the first node that inspects and forwards the related IP packets. Between UE and GGSN, the IP traffic is tunneled. In other words, the intermediate nodes – NodeB, RNC and SGSN – do not inspect those IP packets. Instead, they base their forwarding decisions on the IP addresses in the header of the tunneling protocol.

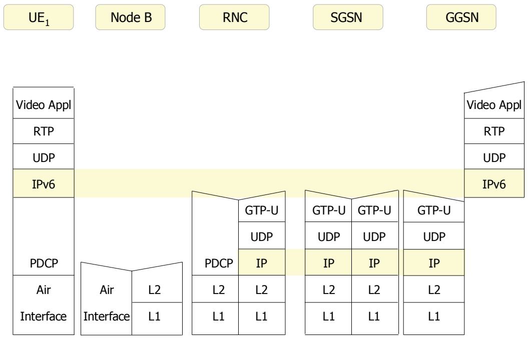


Figure 7: UMTS user plane protocol stack

The tunnel between UE and GGSN can be split in two. Between GGSN and RNC, via SGSN, GPRS Tunneling Protocol (GTP) is used. Between RNC and UE, a combination of protocols specifically designed for the Radio Access Network is used.

The GTP tunnels that exist across GGSN, SGSN and RNC are carried over IP. Therefore, the traffic exchanged between GGSN and SGSN or between SGSN and RNC can be routed through intermediate routers. These routers are completely independent of the UMTS network. In the context of this document, we refer to them as the *IP Transport Network*.

The UE and GGSN must support IPv6 (or dual-stack) interfaces. The SGSN and RNC are aware that the context is IPv6, but are not required to support IPv6 interfaces. They handle GPT-c, the control protocol associated with GTP, which, in the case of IPv6, has information elements (IE), such as the End User Address IE, which are different for IPv6 UEs than for IPv4 UEs. The NodeB is transparent to both GTP-u (the user-plane part of GTP) and GTP-c. Therefore, the NodeB does not require any modifications due to a transition to IPv6.

In some cases, the RNC performs IP header compression. In the case of introduction of IPv6, it should be verified whether the RNC is able to compress packets with an IPv6 header.

3.1.5 IPv6 impact on IP Transport Network

As shown in Figure 7, the IP layer that is visible to the UE (illustrated by the top yellow bar) is completely independent of the IP layer that connects RNCs, SGSNs and GGSNs (illustrated by the bottom yellow bar). Therefore, the interface on RNC and SGSN and the IP routers between them do not necessarily need to support IPv6, even if the UE and GGSN do.

3.1.6 IMS Aspects

All messaging between UE and IMS and between IMS components uses SIP except for:

- DNS queries (IPv6 AAAA) .
- Access to the HSS (which uses the Diameter protocol).

Registration

IMS Registration authenticates the user, allowing access to IMS services.

As part of PDP Context Activation, the UE performs Proxy Call Session Control Function (P-CSCF) discovery. The user’s Private User Identity, Public User Identity and Home Network Domain, required for IMS registration, are stored on the UE.

The P-CSCF binds the IMS Public User Identity to the IPv6 address found in the *contact* header of the SIP registration message. The P-CSCF also associates the UE with a Serving Call Session Control Function (S-CSCF). The UE can register one IP address (*contact* address) with a Private User Identity. There can be one or multiple Public User Identities related to a registration and a Public User Identity can be registered with multiple Private User Identities.

If an IMS user requires an additional Primary PDP Context, the user must register with a different Private User Identity and different IP address. This could be relevant in the case of a dual-stack user supporting both IPv4 and IPv6 addresses.

Registration is a two-stage process. The initial registration causes the S-CSCF to begin a challenge/response procedure to perform authentication. A Security Association is then established between the UE and P-CSCF. The Security Association is identified by the source and destination IP addresses (UE and P-CSCF). This process is shown in Figure 8.

The S-CSCF registers the Public User Identity of the UE. The S-CSCF authenticates the user and stores the URI and IP address of the P-CSCF, along with the IP address of the UE.

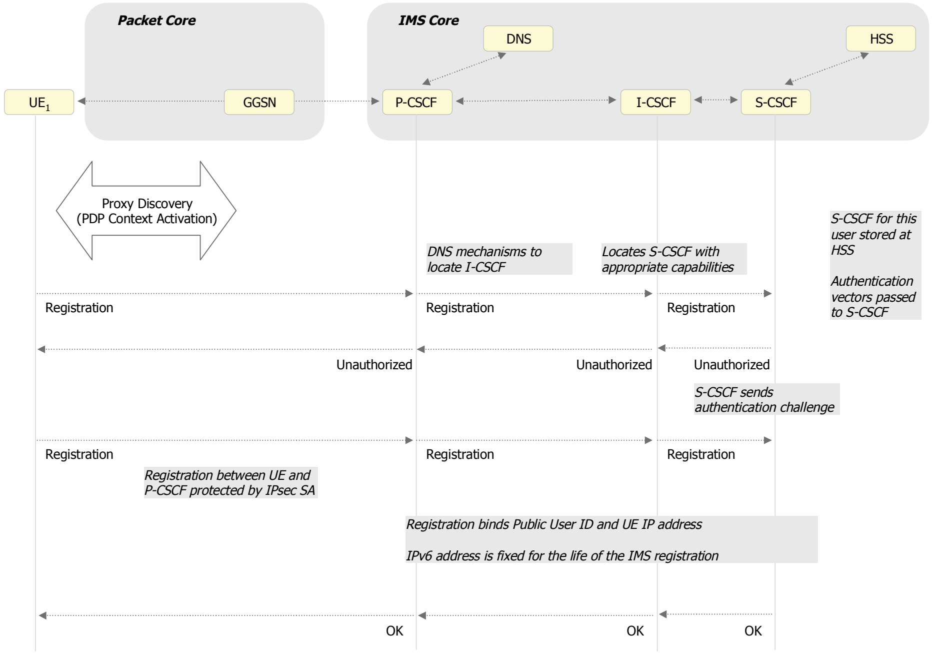

Packet Core
IMS Core
DNS
HSS
UE$_1$
GGSN
P-CSCF
I-CSCF
S-CSCF
Proxy Discovery
(PDP Context Activation)
DNS mechanisms to locate I-CSCF
Locates S-CSCF with appropriate capabilities
S-CSCF for this user stored at HSS
Authentication vectors passed to S-CSCF
Registration
Registration
Registration
Unauthorized
Unauthorized
Unauthorized
S-CSCF sends authentication challenge
Registration
Registration
Registration
Registration between UE and P-CSCF protected by IPsec SA
Registration binds Public User ID and UE IP address
IPv6 address is fixed for the life of the IMS registration
OK
OK
OK

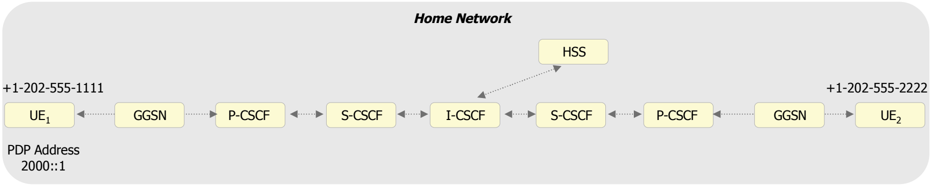
Figure 8: IMS Registration Procedure

Section 3.1.3 discussed the notion of IP Privacy Extensions. The mechanism works, because in the packet core, only IPv6 network prefix is significant. It should be noted that for IMS all 128 bits of the IPv6 address are significant. Any use of privacy extensions by an IMS UE will force a re-registration.

Video Sharing Session Setup

The SIP INVITE is used to establish a session between two IMS users. The following figure shows some of the fields in a sample INVITE. The SIP Via and Contact include the IP address to be used for signaling by the IMS originator. The SDP descriptors convey the session description information, including media (video, audio), and connection data (IP address to use for media).

In this use case, the SIP Request URI contains a TEL URI and the user for the TEL URI is another user in the IMS domain. The S-CSCF uses the ENUM DNS mechanism to determine the SIP URI for the destination.



```
INVITE tel:+1-202-555-2222 SIP/2.0
Via: SIP/2.0/UDP [2000::1]:5059;comp=sigcomp
...
Route: ,sip:pcscf.home.net:7531;1r;comp=sigcomp>, <sip:scscf.home.net;1r>
P-Preferred-
Identity: “User 1” <tel:+1-202-555-1111>
P-Access-Network-Info:  3GPP-UTRAN-TDD; utran-cell-id-3gpp=12345678CELL
Contact: <sip:[2000::1]:1357;comp=sigcomp
...
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321
Content-Type: application /sdp
...
o=- 123456 654321 IN IP6 2000::1
s=-
c=IN IP6 2000::1
t=0 0
m=video 3400 RTP/AVP 98 99
...
m=audio 3456 RTP/AVP 97 96
...
```

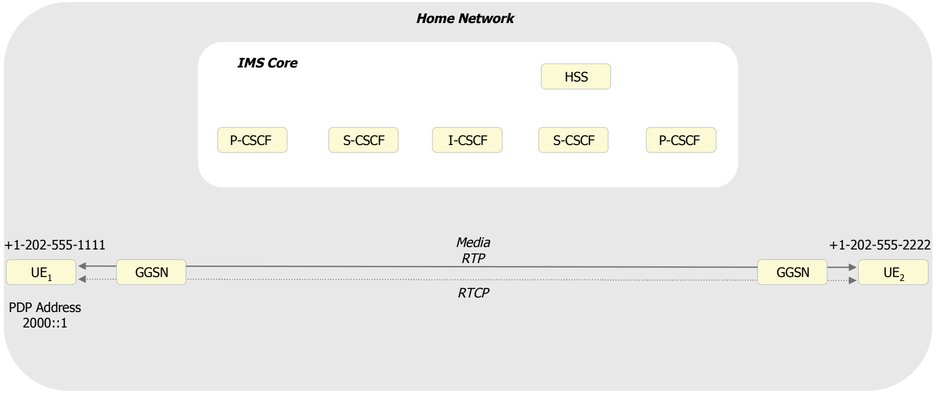
Figure 9: Session establishment

During exchange of messages in a SIP INVITE, both users request network resources. Resources are not allocated until session establishment is agreed upon. Users can request Secondary PDP contexts with different QoS from SIP signaling to support RTP media and RTCP signaling.

The ICID (IMS Charging Identity) contains IP-related parameters, extracted from the SDP descriptors. These are sent from the IMS core to the off-line or on-line charging entity, in the diameter ACR (Accounting Request).

Media Session for Video Sharing

SIP signaling flows through the IMS core. The media is routed between the source and destination, not via the IMS core.



Real-time IMS services, like video share and push to talk over cellular, may require predictable network quality over the network (e.g. jitter, delay, packet loss, etc.). To support these real-time services, 3GPP defined an end-to-end Quality of Service architecture (see next section). Further enhancements have been developed in the areas of QoS and policy control to support real-time services. For example, video share requires that a PDP context be established to stream video from one UE to the other. Initially, service providers could support this connectivity across a single primary PDP context with *best-effort* QoS. As service providers implement QoS capabilities, the video stream may be supported over a secondary PDP context mapped to a streaming class of service. RTP (Real-Time Protocol - media) and RTCP (Real-Time Control Protocol - signaling) use one, or possibly two, secondary PDP contexts. They use the same IP address as SIP signaling (which uses the Primary PDP Context), but support a different level of QoS. RTP and RTCP may be multiplexed over single RAB (Radio Access Bearer). However, multiplexing over a single RAB may have adverse impact on the user experience.

We conclude the IMS section with the following observations:

- The P-CSCF communicates directly with the UE. Service providers may opt to enable signaling compression in order to optimize the bandwidth between the UE and the P-CSCF. SIGCOMP (Signaling Compression) occurs between UE and the P-CSCF. Therefore, in the case of an IPv6 UE, the P-CSCF must support IPv6 interfaces.
- Specialized firewalls may be inline between the UE and the P-CSCF and provide SIP pin-hole security. These specialized firewalls must support both IPv4 and IPv6.
- All other IMS elements, such as the S-CSCF do not communicate directly with the UE. Therefore, they do not necessarily need to support IPv6 interfaces. However, many elements must be IPv6 aware. The S-CSCF, for example, acts on the SDP information, which, in the case of an IPv6 UE, contains IPv6 addresses.

3.1.7 QoS and other policy-based actions

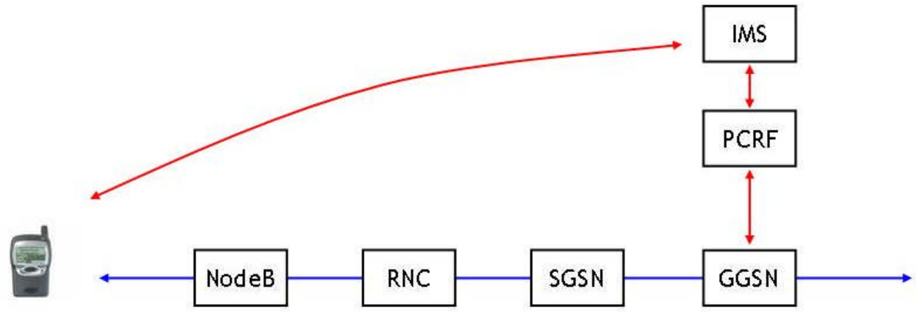


Figure 10: QoS support

Figure 10 shows the general model for QoS support. During session establishment, IMS determines the resources required for the session (for example, based on the codecs used for the media stream). It then requests resources from the Policy and Charging Rules Function (PCRF). The PCRF will determine, based on local policies whether or not to grant the request. If granted, it interfaces with the GGSN to push *policy enforcement rules*. Policy enforcement consists of one or more actions executed on the flow associated with the session. These actions are: gating (i.e. blocking the flow from going through), policing (rate limiting), QoS marking (to map the flow onto the desired service class) and charging.

In IPv4 networks, a media flow is typically identified through one or more of the following parameters: IP source address, IP destination address, Diffserv Code Point (DSCP), Protocol ID and UDP or TCP port numbers (source and destination).

In IPv6 networks, in particular in the GGSN, the flow identification implementation needs to be adapted. It must be based on IPv6 addresses instead of IPv4 addresses. The other parameters remain the same. IPv6, however, has introduced a new parameter - the Flow Label. At this point in time, it is not clear how the flow label will be used, but conceivably it would impact UE, IMS, PCRF and GGSN.

Without going into further detail, we point out that many other functions in the network will have to be IPv6 enabled. For example, Call Detail Records (CDRs) used for billing will refer to IPv6 addresses. Lawful Intercept may entail copying a target’s call content. The copying action will be based on IPv6 addresses.

In general, a transition to IPv6 will not require all network elements to support IPv6 on their external interfaces, but it will require IPv6 awareness.

3.1.8 Roaming

When a service provider starts the transition to IPv6, it will provide IPv6-capable devices to its subscribers and upgrade its infrastructure as described in the previous sections. The subscriber, however, may roam and enter networks that have not yet been upgraded for IPv6 support. Therefore, it is clear that during the initial years of IPv6 roll-out, all mobile devices must support both IPv4 and IPv6. When attaching to the Home Network, the UE will receive an IPv6 address, but when attaching to a visited network that does not support IPv6, it will receive an IPv4 address. The reason for assigning an IPv4 address is not due to limitations in the GGSN (after all, this section assumed that the home network supports IPv6) but due to the fact that the SGSN in the visited network may not be IPv6-enabled. If it would be certain that the visited network is IPv6-enabled, an IPv6 address could be assigned to the UE.

3.1.9 IPv6/IPv4 Inter-working

During the transition to IPv6, some end-user devices will have been upgraded to IPv6, but other devices will still support IPv4 only. This section discusses the case in which an IPv6-capable device needs to establish a connection with an IPv4-only device.

There are essentially three mechanisms to deal with heterogeneous UEs:

1. The IPv6-capable devices switches to IPv4 mode and establishes IPv4 connectivity.
2. The IPv6-capable devices establishes an additional IPv4 PDP Context and establishes IPv4 connectivity *simultaneously* with IPv6 connectivity.
3. The IPv6-capable device uses IPv6 to communicate. An intermediate device translates between IPv6 and IPv4,

The first solution is not feasible. It would entail the following procedure:

- The IPv6 UE tries to establish connectivity by sending a SIP INVITE to IMS.
- IMS (i.e. the S-CSCF of the destination node) discovers that the called party supports IPv4-only and issues an error message.
- The UE deletes the IPv6 PDP Context, establishes an IPv4 PDP Context; re-registers with IMS and then re-issues a SIP INVITE message using its IPv4 address.

This procedure will cause an unacceptable call setup delay and is therefore not recommended.

Rather then re-establishing a PDP Context, it seems better to support parallel PDP Contexts: one or more for IPv6 and one or more for IPv4. Under that assumption, there are several ways in which a UE can detect that the called party supports IPv4 only. It may wait until it receives an error message from IMS (as described above). However, it could also use ICE (Interactive Connectivity Establishment) and STUN (Session Traversal underneath NAT). The ICE solution allows a dual-stack node to offer both types of addresses in the SDP descriptors. In all cases, though, the UE needs both IPv6 and IPv4 PDP Contexts. The problem is that in UMTS networks, PDP Contexts and the associated Radio Access Bearers (RAB) are scarce. In the case of IMS services, a dual-stack device would need at least four: for IPv6 signaling, IPv6 media traffic, IPv4 signaling and IPv4 media traffic. Most NodeBs and RNCs do not support this.

Since both options of turning the UE to an IPv4 mode do not work well, the best solution is the use of NAT-PT (Network Address Translation - Protocol Translation) to translate the IP headers. This solution is similar to how NAT is used to translate between private and public addresses in IPv4 networks. In the case of IMS applications, not only translation of the IP headers in the media stream is required, but an ALG (Application-Level Gateway) is required as well to modify the IP-related fields in the SIP and SDP descriptors. ALGs could potentially be implemented as relays, acting as B2BUA (Back-to-Back User Agents).

As mentioned in section 2.4, the use of translation devices is in general not recommended. A service provider should therefore establish procedures that minimize the use of translation. For example, dual-stack devices attached to the home network should always adopt an IPv6 personality. It should not be allowed that one device registers with IPv6 while the other registers with IPv4, so that translation is required to connect the two.

That said, in the case a dual-stack device must interface with an IPv4-only device, we believe that translation is the best way to achieve this.

3.1.10 Conclusions of the Video Share Use Case

This section summarizes the main conclusions from the previous sections.

- IPv6 implementation can be introduced in a phased approach:

- IPv6 addressing can be introduced on UEs first, where it will have the greatest benefit in terms of mitigating IPv4 address exhaustion.
  - GGSN and P-CSCF must support IPv6. Other systems may need to be IPv6 aware, but do not necessarily need to support IPv6 interfaces.
  - IPv4 can continue to be used in the underlying transport network.
- To support roaming, UEs must be dual-stack. In the home network they will act as IPv6 UEs: in visited networks, they may act as IPv4 UEs, depending on the capabilities of the visited network.
- To enable interworking between an IPv6-capable device and a legacy IPv4-only device, it is recommended to introduce a translation function to translate between IPv6 and IPv4. This translation function also needs to act as an ALG, i.e. it must translate information in the SIP and SDP messages.

Note that the Video Share Use Case uses two interpretations of *dual stack*:

- *Sequential* dual stack support, in which case a UE sometimes operates in IPv6 mode and other times in IPv4 mode (e.g. when roaming).
- *Simultaneous* dual stack support, in which case a UE functions as both an IPv4 and an IPv6 end point simultaneously.

The use case demonstrates that sequential dual-stack support is required, while simultaneous dual-stack support is often not possible, due to limitations in the numbers of RABs that can be established.

3.2 *Gaming Use Case*

The gaming use case describes interactive games played by a mobile user. This section is less detailed than the previous one and focuses primarily on similarities and differences between the two use cases.

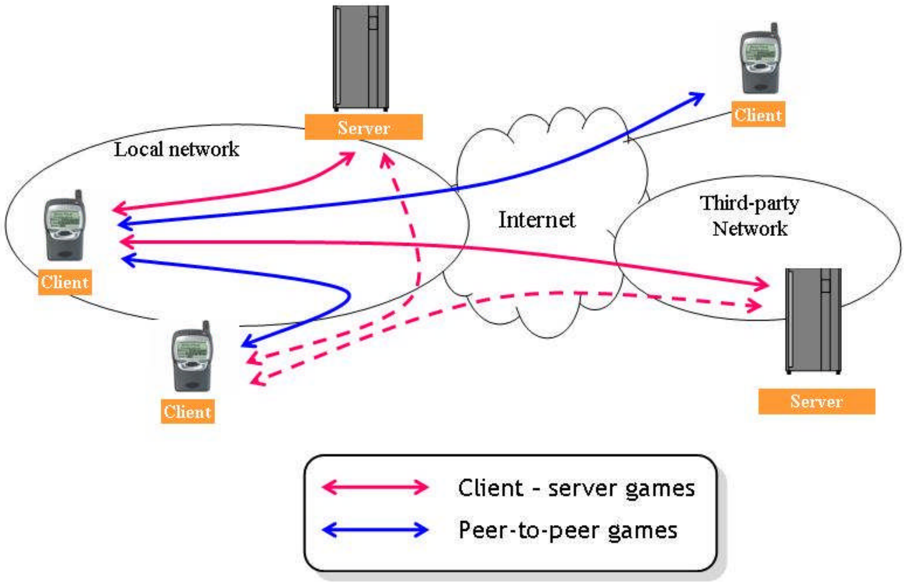
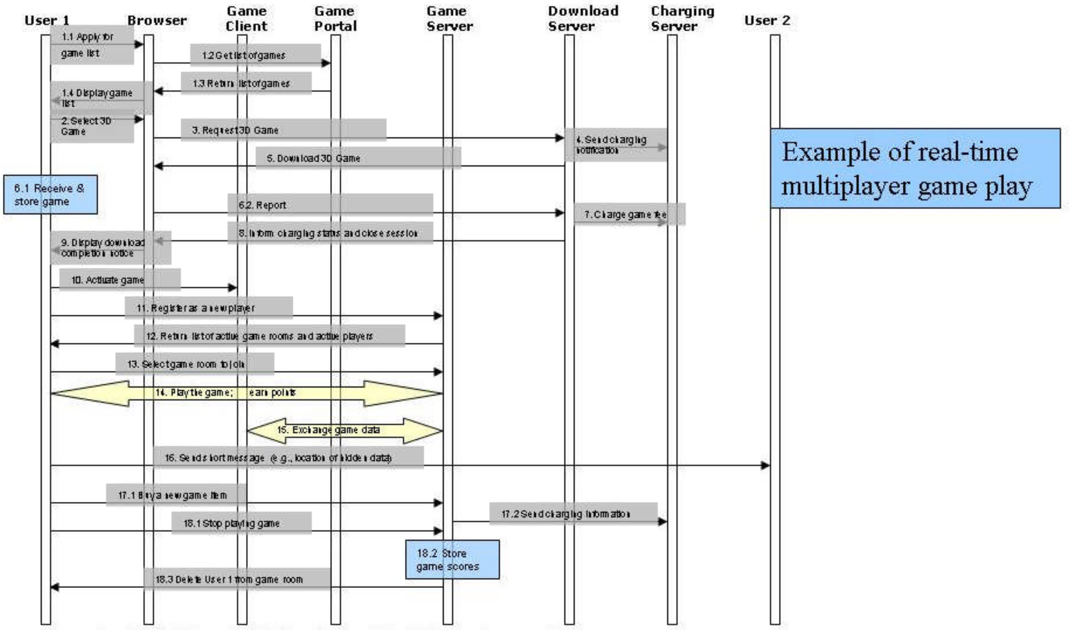


Figure 11: Several gaming options

Figure 11 shows multiple gaming scenarios:

- Client-server games, in which the user connects to a game server. The game server may be owned and operated by the user's wireless service provider, or by a third party provider. Furthermore, games may be single-user games, in which only one user interacts with the gaming server, or multi-user games in which multiple users participate in a single game on the gaming server.
- Peer-to-peer games in which users communicate directly with each other.

The vast majority of today's games are client-server games.


User 1
Browser
Game Client
Game Portal
Game Server
Download Server
Charging Server
User 2
1.1 Apply for game list
1.2 Get list of games
1.3 Return list of games
1.4 Display game list
2. Select 3D Game
3. Request 3D Game
4. Send charging notification
5. Download 3D Game
6.1 Receive & store game
6.2. Report
7. Charge game fee
8. Inform charging status and close session
9. Display download completion notice
10. Actuate game
11. Register as a new player
12. Return list of active game rooms and active players
13. Select game room to join
14. Play the game; earn points
15. Exchange game data
16. Send short message (e.g., location of hidden data)
17.1 Buy a new game item
17.2 Send charging information
18.1 Stop playing game
18.2 Store game scores
18.3 Delete User 1 from game room
Example of real-time multiplayer game play

Source: Open Mobile Alliance (OMA), Game Services WG, Architecture Document 1.0

Figure 12: A typical gaming call flow

Figure 12 shows a typical gaming call flow. The communication between user, portal and game server is based on http and https. In contrast to the Video Share use case, there is no separation between signaling flow and data flow.

When a service provider initiates the transition to IPv6 and starts deploying IPv6-capable mobile devices, it is fairly straightforward to upgrade gaming servers and portals under its control to IPv6 (or dual-stack). The situation is different for gaming servers and portals under control of third-party providers. It could be expected that many gaming providers will upgrade their infrastructure as soon as several large service providers begin IPv6 deployment, but in the beginning of the transition period, interfacing with IPv4-only gaming servers is likely to be required.

As there is no need for a separate signaling channel in gaming applications, the dual-stack approach would work. The UE would set up two PDP Contexts, one for IPv6 and one for IPv4. The default option would be the use of the IPv6 PDP Context, but when interfacing with an IPv4-only gaming server, the UE could fall back on the IPv4 PDP Context.

3.3 *Blackberry Use Case*

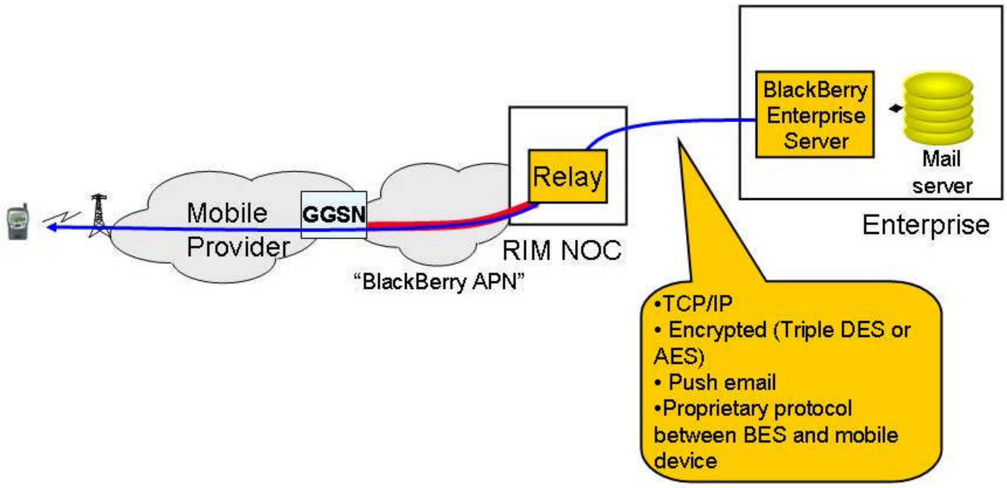

BlackBerry Enterprise Server
Mail server
Enterprise
Relay
RIM NOC
Mobile Provider
GGSN
"BlackBerry APN"
•TCP/IP
• Encrypted (Triple DES or AES)
• Push email
•Proprietary protocol between BES and mobile device

Figure 13: Blackberry architecture

The Blackberry use case is the most straightforward of the three use cases. To support email on mobile devices, mail is copied from the mail server of an enterprise onto a Blackberry Enterprise Server, from where it is forwarded to a relay function in the RIM Network Operations Center (NOC).

At attachment, the UE selects an APN that is associated with the Blackberry Services. After PDP Context Activation, the UE registers with the RIM NOC.

For IPv6-capable devices, the service provider will identify a special IPv6-Blackberry-APN. Via this APN, the UE will be able to connect to an IPv6 Relay Server.

It is to be expected that RIM NOCs will be IPv6-enabled before roll-out of IPv6-capable Blackberries begins. Therefore, it is unlikely that there is a need for IPv6-IPv4 interoperability.

4 Deployment Strategy / Recommendations

4.1 *Develop a transitioning plan*

The moment that service providers will not be able to acquire new IPv4 address blocks is rapidly approaching. As discussed in section 1.1, it could be as soon as 2012. The transition to IPv6 is inevitable. The transition to IPv6 will take several years, but the planning to transition to IPv6 should begin as soon as possible. Therefore, if service providers have not already started transitioning plans, it is strongly recommended to start soon.

The "IPv6 Transition Guidance" report, issued by Federal CIO Council Architecture and Infrastructure Committee ([9]) provides a useful blueprint. Among the recommended actions are:

- Identifying an IPv6 Transitioning lead within the organization
- Developing a transitioning plan
- Taking a complete inventory of IPv6-capable network elements, applications and end-user devices

Transition plans may vary widely from network to network; however, the transition plans should include the following sequence of activities - Assessment, Planning, and Deployment. Depending on the scale and complexity of the existing network infrastructure, a number of different detailed plans may be required. Some examples include: equipment inventory and upgrade capabilities and schedules, trials and testing vs. operational deployment, infrastructure vs. application rollout, and staff training and support.

Large wireless service providers will likely need to begin transition sooner than smaller service providers due to the sheer number of subscribers they must support. This places an additional burden of being early adopters to technologies and standards that are still maturing. One advantage that large service providers have as IPv6 pioneers is the ability to shape the industry to their benefit by being able to provide IPv6 development requirements to key suppliers and vendors.

4.2 *Use a phased approach*

As illustrated by the given use cases, wireless service providers have the option to start deploying IPv6-enabled devices while still running IPv4 on most network elements. In addition to the user devices, GGSN, P-CSCF and application servers should support IPv6 interfaces. Many other network elements need to be IPv6-aware but do not need to run IPv6 themselves. This latter point should not be underestimated. A large percentage of ancillary systems may need to be IPv6-aware, including DNS servers, DHCP servers, network management systems, billing systems, Lawful Intercept systems, etc.

The document does not mean to suggest that the only sensible transition scenario is one in which a service provider starts IPv6 transition with the deployment of IPv6-capable UEs, while upgrading the IP core infrastructure later. In fact, upgrading the core may be an easier task as many core routers already support IPv6. Therefore, upgrading the core before upgrading user devices and edge equipment is a valid transitioning plan.

It should be noted, though, that upgrading the IP core does not mitigate the IPv4 exhaustion problem, since new end-user devices and applications will still require IPv4 addresses. Also, in the absence of IPv6 hosts, the core may be able to route IPv6, but there will be no IPv6 traffic.

4.3 *Interworking mechanisms*

The biggest problem that a service provider will need to solve is the interworking between IPv6 devices and IPv4-only devices. As discussed in sections 2 and 3, a dual-stack approach is preferred because it maintains transparency between the two end-points. In the dual-stack approach, an IPv6 device will use IPv4 when interfacing with a device or application server that supports IPv4 only. However, as pointed out in the Video Share use case, the dual stack approach may not work well for mobile devices. In the case of IMS-based applications, the dual-stack approach may require four simultaneous PDP Contexts. On the other hand, for non-IMS-based applications such as gaming, the dual-stack approach may be feasible.

A service provider will need to develop a clear plan with respect to support of multiple PDP Contexts. This plan should take the following into account:

- Services the service provider is planning to support.
- QoS levels planned to be offered to subscribers.
- The ability of the existing RAN infrastructure to support multiple PDP Contexts and RABs.

Based on these, the service provider will be able to assess to what extent a dual-stack approach is feasible. The service provider should give careful consideration to an APN strategy in order to avoid overly complex RAB requirements. In the case a dual-stack approach is not feasible, translation is the recommended alternative.

4.4 *Security Considerations*

The transition to IPv6 requires special attention to security considerations. The security policies of individual companies typically address exposures and security mitigation techniques in the IPv4 environment. To this end, firewalls and intrusion detection systems have been implemented to protect an enterprise's network, host computer and data assets. However, with the introduction of dual-stack and IPv6, enterprises will need to assess security during and after the transition. As mentioned in section 2.3, automatic tunneling can bypass IPv4 safeguards. Therefore, transitional dual-stack security policies should be developed to address the many networking aspects that IPv6 introduces:

- Anycast addresses.
- Scoped addresses.
- New extension headers.
- Tunneling protocols.
- Transport headers and deep packet inspection.
- Privacy addresses.
- ICMP options.

5 Conclusions

This paper presented the following key points:

- The wireless industry continues to experience explosive growth.
- New always-on wireless services require always-available IP addresses.
- IPv4 addresses continue to deplete at a very rapid rate and are expected to exhaust as soon as 2012.
- IPv6 solves the IPv4 address depletion problem. In addition, IPv6 has several other benefits.
- Transitioning to IPv6 is a significant effort, but one that, at this point in time, can no longer be delayed. Transitioning to IPv6 will cost money, but failing to transition to IPv6 will also cost money (e.g. inability to scale services to be competitive in the industry).
- IPv4 to IPv6 transition is complex and suggested guidelines for implementation were provided.

To assist wireless service providers, this paper analyzed several use cases and laid out a series of recommendations that may help service providers initiate a smooth and successful IPv6 transitioning process.

6 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

7 References

[1] "The choice: IPv4 exhaustion or transition to IPv6", Jordi Palet, April 2006 http://www.ipv6tf.org/pdf/the_choice_ipv4_exhaustion_or_transition_to_ipv6_v4.4.pdf

[2] IPv4 address report, Report July 30 2007 http://www.potaroo.net/tools/ipv4/index.html

[3] "The Recommendation for the IP Next Generation Protocol", IETF RFC 1752, January 1995

[4] "IPv6 Forum Roadmap and Vision", version 6.0, IPv6 Forum, L. Ladid et al., 2006, http://www.ipv6forum.org/dl/forum/wwc_ipv6forum_roadmap_vision_2010.pdf

[5] "Analysis of IPv6 Features and Usability", version 1.0, North American IPv6 Task Force (NAv6TF) Technology Report, W. Eddy et al., September 2006, http://www.nav6tf.org/documents/nav6tf.analysis_ipv6_features_and_usability.pdf

[6] "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 1883, December 1995

[7] "ATIS Internet Protocol Version 6 (IPV6) Report & Recommendation", ATIS, May 2006, http://www.atis.org/tops/IPv6/ATIS_IPv6_Report_Recommendation_May2006-Final.pdf

[8] "ATIS Internet Protocol version 6 (IPv6) Task Force Report on IPv6 Transition Challenges", ATIS, July 2007, http://www.atis.org/IPv6TF_Report_Transition_Challenges_July_2007_Final.pdf

[9] "IPv6 Transition Guidance", Federal CIO Council Architecture and Infrastructure Committee, February 2006, http://www.cio.gov/documents/IPv6_Transition_Guidance.doc

8 Acknowledgements

The mission of 3G Americas is to promote and facilitate the seamless deployment throughout the Americas of GSM and its evolution to LTE. 3G Americas' Board of Governors members include Alcatel-Lucent, AT&T, Cable & Wireless, Ericsson, Gemalto, HP, Motorola, Nortel Networks, Nokia, Openwave, Research in Motion (RIM), Rogers (Canada), T-Mobile USA, Telcel (Mexico), Telefónica, and Texas Instruments.

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