Individual Submission
Internet-Draft
Intended status: Informational
Expires: April 2, 2012

J. Korhonen, Ed.
Nokia Siemens Networks
J. Soininen
Renesas Mobile
B. Patil
T. Savolainen
G. Bajko
Nokia
K. Iisakkila
Renesas Mobile

September 30, 2011

IPv6 in 3GPP Evolved Packet System
draft-ietf-v6ops-3gpp-eps-08

Abstract

Use of data services in smart phones and broadband services via HSPA and HSPA+, in particular Internet services, has increased rapidly and operators that have deployed networks based on 3GPP network architectures are facing IPv4 address shortages at the Internet registries and are feeling a pressure to migrate to IPv6. This document describes the support for IPv6 in 3GPP network architectures.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 2, 2012.

Table of Contents

1. Introduction

IPv6 has been specified in the 3rd Generation Partnership Project (3GPP) standards since the early architectures developed for R99 General Packet Radio Service (GPRS). However, the support for IPv6 in commercially deployed networks remains low. There are many factors that can be attributed to the lack of IPv6 deployment in 3GPP networks. The most relevant one is essentially the same as the reason for IPv6 not being deployed by other networks as well, i.e. the lack of business and commercial incentives for deployment. 3GPP network architectures have also evolved since 1999 (since R99). The most recent version of the 3GPP architecture, the Evolved Packet System (EPS), which is commonly referred to as SAE, LTE or Release-8, is a packet centric architecture. The number of subscribers and devices that are using the 3GPP networks for Internet connectivity and data services has also increased significantly. With the subscriber growth numbers projected to increase even further and the IPv4 addresses depletion problem looming in the near term, 3GPP operators and vendors have started the process of identifying the scenarios and solutions needed to transition to IPv6.

This document describes the establishment of IP connectivity in 3GPP network architectures, specifically in the context of IP bearers for 3GPP GPRS and for 3GPP EPS. It provides an overview of how IPv6 is supported as per the current set of 3GPP specifications. Some of the issues and concerns with respect to deployment and shortage of private IPv4 addresses within a single network domain are also discussed.

The IETF has specified a set of tools and mechanisms that can be utilized for transitioning to IPv6. In addition to operating dual-stack networks during the transition from IPv4 to IPv6 phase, the two alternative categories for the transition are encapsulation and translation. The IETF continues to specify additional solutions for enabling the transition based on the deployment scenarios and operator/ISP requirements. There is no single approach for transition to IPv6 that can meet the needs for all deployments and models. The 3GPP scenarios for transition, described in [TR.23975], can be addressed using transition mechanisms that are already available in the toolbox. The objective of transition to IPv6 in 3GPP networks is to ensure that:

1. Legacy devices and hosts which have an IPv4-only stack will continue to be provided with IP connectivity to the Internet and services,

2. Devices which are dual-stack can access the Internet either via IPv6 or IPv4. The choice of using IPv6 or IPv4 depends on the

capability of:

A. the application on the host,

B. the support for IPv4 and IPv6 bearers by the network and/or,

C. the capability of the server(s) and other end points.

3GPP networks are capable of providing a host with IPv4 and IPv6 connectivity today, albeit in many cases with upgrades to network elements such as the SGSN and GGSN.

2. 3GPP Terminology and Concepts

2.1. Terminology

Access Point Name

Access Point Name (APN) is a fully qualified domain name and resolves to a specific gateway in an operators network. The APNs are piggybacked on the administration of the DNS namespace.

Dual Address PDN/PDP Type

The Dual Address PDN/PDP Type (IPv4v6) is used in 3GPP context in many cases as a synonym for dual-stack i.e. a connection type capable of serving both IPv4 and IPv6 simultaneously.

Evolved Packet Core

Evolved Packet Core (EPC) is an evolution of the 3GPP GPRS system characterized by higher-data-rate, lower-latency, packet-optimized system. EPC comprises of subcomponents such as Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PDN-GW) and Home Subscriber Server (HSS).

Evolved Packet System

Evolved Packet System (EPS) is an evolution of the 3GPP GPRS system characterized by higher-data-rate, lower-latency, packet-optimized system that supports multiple Radio Access Technologies (RAT). The EPS comprises the Evolved Packet Core (EPC) together with the evolved radio access network (E-UTRA and E-UTRAN).

Evolved UTRAN

Evolved UTRAN (E-UTRAN) is communications network, sometimes referred to as 4G, and consists of eNodeBs (4G base station) which make up the E-UTRAN radio access network. The E-UTRAN allows connectivity between the User Equipment and the core network.

GPRS tunnelling protocol

GPRS Tunnelling Protocol (GTP) [TS.29060] [TS.29274] is a tunnelling protocol defined by 3GPP. It is a network based mobility protocol and similar to Proxy Mobile IPv6 (PMIPv6) [RFC5213]. However, GTP also provides functionality beyond mobility such as inband signaling related to Quality of Service (QoS) and charging among others.

GSM EDGE Radio Access Network

GSM EDGE Radio Access Network (GERAN) is communications network, commonly referred to as 2G or 2.5G, and consists of base stations and Base Station Controllers (BSC) which make up the GSM EDGE radio access network. The GERAN allows connectivity between the User Equipment and the core network.

Gateway GPRS Support Node

Gateway GPRS Support Node (GGSN) is a gateway function in GPRS, which provides connectivity to Internet or other PDNs. The host attaches to a GGSN identified by an APN assigned to it by an operator. The GGSN also serves as the topological anchor for addresses/prefixes assigned to the User Equipment.

General Packet Radio Service

General Packet Radio Service (GPRS) is a packet oriented mobile data service available to users of the 2G and 3G cellular communication systems Global System for Mobile communications (GSM), and specified by 3GPP.

High Speed Packet Access

The High Speed Packet Access (HSPA) and the Evolved High Speed Packet Access (HSPA+) are enhanced versions of the WCDMA and UTRAN, thus providing more data throughput and lower latencies.

Home Location Register

The Home Location Register (HLR) is a pre-Release-5 database (but is also used in Release-5 and later networks in real deployments) that contains subscriber data and call routing related information. Every subscriber of an operator including subscribers' enabled services are provisioned in the HLR.

Home Subscriber Server

The Home Subscriber Server (HSS) is a database for a given subscriber and got introduced in 3GPP Release-5. It is the entity containing the subscription-related information to support the network entities actually handling calls/sessions.

Mobility Management Entity

Mobility Management Entity (MME) is a network element that is responsible for control plane functionalities, including authentication, authorization, bearer management, layer-2 mobility, etc. The MME is essentially the control plane part of the SGSN in GPRS. The user plane traffic bypasses the MME.

Mobile Terminal

The Mobile Terminal (MT) is the modem and the radio part of the Mobile Station (MS).

Public Land Mobile Network

The Public Land Mobile Network (PLMN) is a network that is operated by a single administration. A PLMN (and therefore also an operator) is identified by the Mobile Country Code (MCC) and the Mobile Network Code (MNC). Each (telecommunications) operator providing mobile services has its own PLMN.

Policy and Charging Control

The Policy and Charging Control (PCC) framework is used for QoS policy and charging control. It has two main functions: flow based charging including online credit control, and policy control (e.g. gating control, QoS control and QoS signaling). It is optional to 3GPP EPS but needed if dynamic policy and charging control by means of PCC rules based on user and services are desired.

Packet Data Network

Packet Data Network (PDN) is a packet based network that either belongs to the operator or is an external network such as Internet and corporate intranet. The user eventually accesses services in one or more PDNs. The operator's packet core network are separated from packet data networks either by GGSNs or PDN Gateways (PDN-GW).

Packet Data Network Gateway

Packet Data Network Gateway (PDN-GW) is a gateway function in Evolved Packet System (EPS), which provides connectivity to Internet or other PDNs. The host attaches to a PDN-GW identified by an APN assigned to it by an operator. The PDN-GW also serves as the topological anchor for addresses/prefixes assigned to the User Equipment.

Packet Data Protocol Context

A Packet Data Protocol (PDP) Context is the equivalent of a virtual connection between the host and a gateway.

Packet Data Protocol Type

A Packet Data Protocol Type (PDP Type) identifies the used/allowed protocols within the PDP Context. Examples are IPv4, IPv6 and IPv4v6 (dual stack).

S4 Serving Gateway Support Node

S4 Serving Gateway Support Node (S4-SGSN) is a Release-8 (and onwards) compliant SGSN that connects 2G/3G radio access network to EPC via new Release-8 interfaces like S3, S4, and S6d.

Serving Gateway

Serving Gateway (SGW) is a gateway function in EPS, which terminates the interface towards E-UTRAN. The SGW is the Mobility Anchor point for layer-2 mobility (inter-eNodeB handovers). For each User Equipment connected with the EPS, at any given point of time, there is only one SGW. The SGW is essentially the user plane part of the GPRS' SGSN forwarding packets between a PDN-GW.

Serving Gateway Support Node

Serving Gateway Support Node (SGSN) is a network element that is located between the radio access network (RAN) and the gateway

(GGSN). A per User Equipment point to point (p2p) tunnel between the GGSN and SGSN transports the packets between the User Equipment and the gateway.

Terminal Equipment

The Terminal Equipment (TE) is any device/host connected to the Mobile Terminal (MT) offering services to the user. A TE may communicate to a MT, for example, over Point to Point Protocol (PPP).

UE, MS, MN and Mobile

The terms UE (User Equipment), MS (Mobile Station), MN (Mobile Node) and, mobile refer to the devices which are hosts with ability to obtain Internet connectivity via a 3GPP network. A MS comprises of a Terminal Equipment (TE) and a Mobile Terminal (MT). The terms UE, MS, MN and devices are used interchangeably within this document.

UMTS Terrestrial Radio Access Network

UMTS Terrestrial Radio Access Network (UTRAN) is communications network, commonly referred to as 3G, and consists of NodeBs (3G base station) and Radio Network Controllers (RNC) which make up the UMTS radio access network. The UTRAN allows connectivity between the User Equipment and the core network. UTRAN comprises of WCDMA, HSPA and HSPA+ radio technologies.

User Plane

Data traffic and the required bearers for the data traffic. In practice IP is the only data traffic protocol used in user plane.

Wideband Code Division Multiple Access

The Wideband Code Division Multiple Access (WCDMA) is the radio interface used in UMTS networks.

eNodeB

The eNodeB is a base station entity that supports the Long Term Evolution (LTE) air interface.

2.2. The concept of APN

The Access Point Name (APN) essentially refers to a gateway in the 3GPP network. The 'complete' APN is expressed in a form of a Fully Qualified Domain Name (FQDN) and also piggybacked on the administration of the DNS namespace, thus effectively allowing the discovery of gateways using the DNS. User Equipment (UE) can choose to attach to a specific gateway in the packet core. The gateway provides connectivity to the Packet Data Network (PDN) such as the Internet. An operator may also include gateways which do not provide Internet connectivity, rather a connectivity to closed network providing a set of operator's own services. A UE can be attached to one or more gateways simultaneously. The gateway in a 3GPP network is the GGSN or PDN-GW. Figure 1 below illustrates the APN-based network connectivity concept.

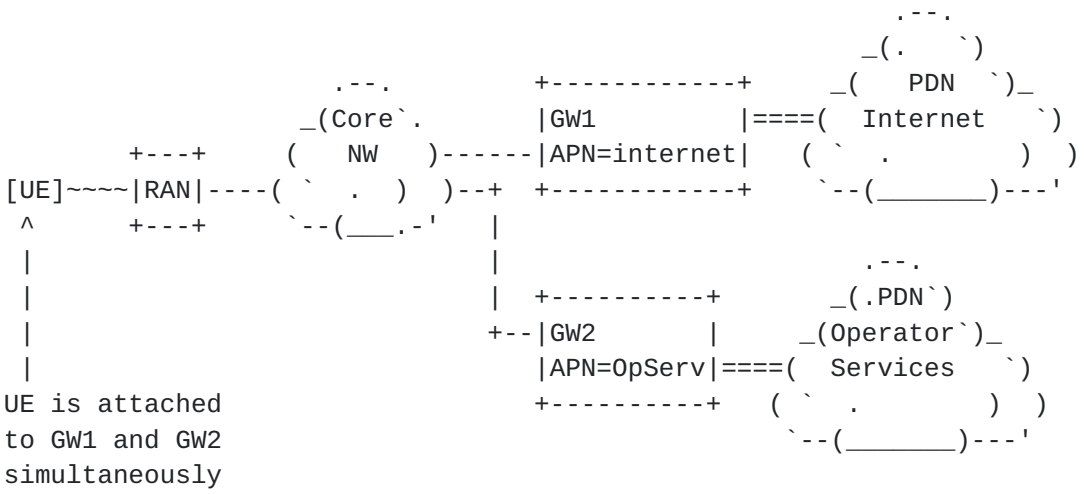

Figure 1: User Equipment attached to multiple APNs simultaneously

3. IP over 3GPP GPRS

3.1. Introduction to 3GPP GPRS

A simplified 2G/3G GPRS architecture is illustrated in Figure 2. This architecture basically covers the GPRS core network since R99 to Release-7, and radio access technologies such as GSM (2G), EDGE (2G, often referred as 2.5G), WCDMA (3G) and HSPA(+) (3G, often referred as 3.5G). The architecture shares obvious similarities with the Evolved Packet System (EPS) as will be seen in Section 4. Based on Gn/Gp interfaces, the GPRS core network functionality is logically implemented on two network nodes, the SGSN and the GGSN.

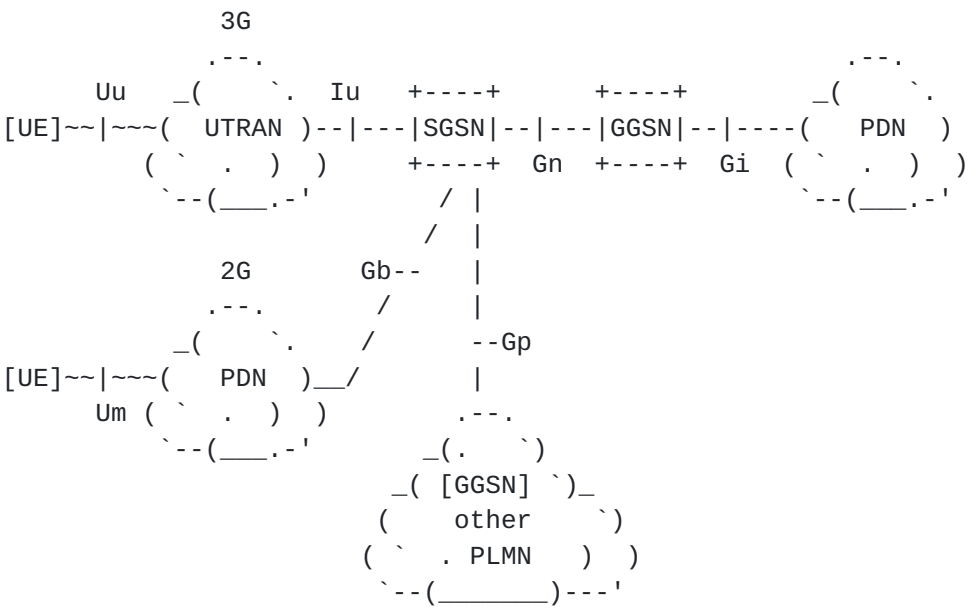

Figure 2: Overview of the 2G/3G GPRS Logical Architecture

Gn/Gp: These interfaces provide a network based mobility service for a UE and are used between a SGSN and a GGSN. The Gn interface is used when GGSN and SGSN are located inside one operator (i.e. PLMN). The Gp-interface is used if the GGSN and the SGSN are located in different operator domains (i.e. 'other' PLMN). GTP protocol is defined for the Gn/Gp interfaces (both GTP-C for the control plane and GTP-U for the user plane).

Gb: Is the Base Station System (BSS) to SGSN interface, which is used to carry information concerning packet data transmission and layer-2 mobility management. The Gb-interface is based on either on Frame Relay or IP.

Iu: Is the Radio Network System (RNS) to SGSN interface, which is used to carry information concerning packet data transmission and layer-2 mobility management. The user plane part of the Iu-interface (actually the Iu-PS) is based on GTP-U. The control plane part of the Iu-interface is based on Radio Access Network Application Protocol (RANAP).

Gi: It is the interface between the GGSN and a PDN. The PDN may be an operator external public or private packet data network or an intra-operator packet data network.

Uu/Um: Are either 2G or 3G radio interfaces between a UE and a respective radio access network.

The SGSN is responsible for the delivery of data packets from and to the UE within its geographical service area when a direct tunnel option is not used. If the direct tunnel is used, then the user plane goes directly between the RNC (in the RNS) and the GGSN. The control plane traffic always goes through the SGSN. For each UE connected with the GPRS, at any given point of time, there is only one SGSN.

3.2. PDP Context

A PDP (Packet Data Protocol) context is an association between a UE represented by one IPv4 address and/or one /64 IPv6 prefix and a PDN represented by an APN. Each PDN can be accessed via a gateway (typically a GGSN or PDN-GW). On the UE a PDP context is equivalent to a network interface. A UE may hence be attached to one or more gateways via separate connections, i.e. PDP contexts. 3GPP GPRS supports PDP Types IPv4, IPv6 and since Release-9 also PDP Type IPv4v6 (dual-stack).

Each primary PDP context has its own IPv4 address and/or one /64 IPv6 prefix assigned to it by the PDN and anchored in the corresponding gateway. The GGSN or PDN-GW is the first hop router for the UE. Applications on the UE use the appropriate network interface (PDP context) for connectivity to a specific PDN. Figure 3 represents a high level view of what a PDP context implies in 3GPP networks.

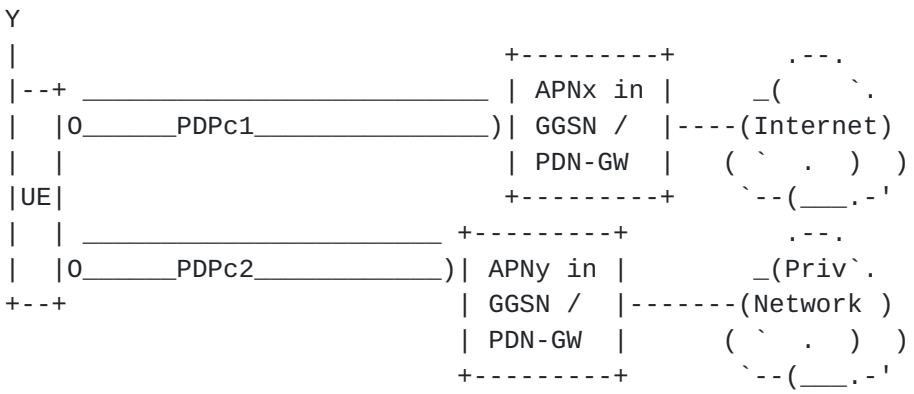

Figure 3: PDP contexts between the MS/UE and gateway

In the above figure there are two PDP contexts at the MS/UE (UE=User Equipment in 3GPP parlance). The 'PDPc1' PDP context that is connected to APNx provided Internet connectivity and the 'PDPc2' PDP context provides connectivity to a private IP network via APNy (as an example this network may include operator specific services such as

MMS (Multi media service). An application on the host such as a web browser would use the PDP context that provides Internet connectivity for accessing services on the Internet. An application such as MMS would use APNy in the figure above because the service is provided through the private network.

4. IP over 3GPP EPS

4.1. Introduction to 3GPP EPS

In its most basic form, the EPS architecture consists of only two nodes on the user plane, a base station and a core network Gateway (GW). The basic EPS architecture is illustrated in Figure 4. The functional split of gateways allows for operators to choose optimized topological locations of nodes within the network and enables various deployment models including the sharing of radio networks between different operators. This also allows independent scaling and growth of traffic throughput and control signal processing.

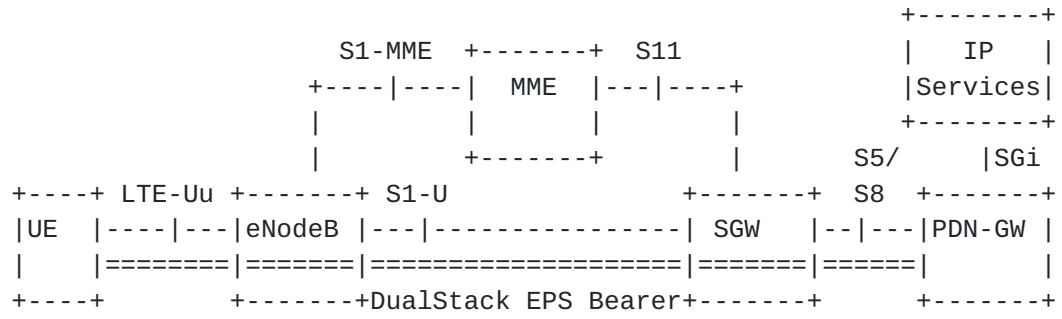

Figure 4: EPS Architecture for 3GPP Access

S5/S8: It provides user plane tunnelling and tunnel management between SGW and PDN-GW, using GTP (both GTP-U and GTP-C) or PMIPv6 [RFC5213][TS.23402] as the network based mobility management protocol. The S5 interface is used when PDN-GW and SGW are located inside one operator (i.e. PLMN). The S8-interface is used if the PDN-GW and the SGW are located in different operator domains (i.e. 'other' PLMN).

S1-U: Provides user plane tunnelling and inter eNodeB path switching during handover between eNodeB and SGW, using the GTP-U protocol (GTP user plane).

S1-MME: Reference point for the control plane protocol between eNodeB and MME.

SGi: It is the interface between the PDN-GW and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network.

4.2. PDN Connection

A PDN connection is an association between a UE represented by one IPv4 address and/or one /64 IPv6 prefix, and a PDN represented by an APN. The PDN connection is the EPC equivalent of the GPRS PDP context. Each PDN can be accessed via a gateway (a PDN-GW). PDN is responsible for the IP address/prefix allocation to the UE. On the UE a PDN connection is equivalent to a network interface. A UE may hence be attached to one or more gateways via separate connections, i.e. PDN connections. 3GPP EPS supports PDN Types IPv4, IPv6 and IPv4v6 (dual-stack) since the beginning of EPS i.e. Release-8.

Each PDN connection has its own IP address/prefix assigned to it by the PDN and anchored in the corresponding gateway. In case of GTP-based S5/S8 interface, the PDN-GW is the first hop router for the UE and in case of PMIPv6-based S5/S8 the SGW is the first hop router. Applications on the UE use the appropriate network interface (PDN connection) for connectivity.

4.3. EPS bearer model

The logical concept of a bearer has been defined to be an aggregate of one or more IP flows related to one or more services. An EPS bearer exists between the UE and the PDN-GW and is used to provide the same level of packet forwarding treatment to the aggregated IP flows constituting the bearer. Services with IP flows requiring a different packet forwarding treatment would therefore require more than one EPS bearer. The UE performs the binding of the uplink IP flows to the bearer while the PDN-GW performs this function for the downlink packets.

In order to provide low latency for always on connectivity, a default bearer will be provided at the time of startup and an IPv4 address and/or IPv6 prefix gets assigned to the UE (this is different from GPRS, where UEs are not automatically assigned with an IP address or prefix). This default bearer will be allowed to carry all traffic which is not associated with a dedicated bearer. Dedicated bearers are used to carry traffic for IP flows that have been identified to require a specific packet forwarding treatment. They may be established at the time of startup; for example, in the case of services that require always-on connectivity and better QoS than that provided by the default bearer. The default bearer and the dedicated bearer(s) associated to it share the same IP address(es)/prefix.

An EPS bearer is referred to as a GBR bearer if dedicated network resources related to a Guaranteed Bit Rate (GBR) value that is associated with the EPS bearer are permanently allocated (e.g. by an admission control function in the eNodeB) at bearer establishment/ modification. Otherwise, an EPS bearer is referred to as a non-GBR bearer. The default bearer is always non-GBR, with the resources for the IP flows not guaranteed at eNodeB, and with no admission control. However, the dedicated bearer can be either GBR or non-GBR. A GBR bearer has a Guaranteed Bit Rate (GBR) and Maximum Bit Rate (MBR) while more than one non-GBR bearer belonging to the same UE shares an Aggregate Maximum Bit Rate (AMBR). Non-GBR bearers can suffer packet loss under congestion while GBR bearers are immune to such losses.

5. Address Management

5.1. IPv4 Address Configuration

UE's IPv4 address configuration is always performed during PDP context/EPS bearer setup procedures (on layer-2). DHCPv4-based [RFC2131] address configuration is supported by the 3GPP specifications, but is not used in wide scale. The UE must always support address configuration as part of the bearer setup signaling, since DHCPv4 is optional for both UEs and networks.

The 3GPP standards also specify a 'deferred IPv4 address allocation' on a PMIPv6-based dual-stack IPv4v6 PDN connection at the time of connection establishment as described in Section 4.7.1 of [TS.23402]. This has the advantage of a single PDN Connection for IPv6 and IPv4 along with deferring IPv4 address allocation until an application needs it. The deferred address allocation is based on the use of DHCPv4 as well as appropriate UE side implementation dependant triggers to invoke the protocol.

5.2. IPv6 Address Configuration

IPv6 Stateless Address Autoconfiguration (SLAAC) as specified in [RFC4861][RFC4862] is the only supported address configuration mechanism. Stateful DHCPv6-based address configuration [RFC3315] is not supported by 3GPP specifications. On the other hand, Stateless DHCPv6-service to obtain other configuration information is supported [RFC3736]. This implies that the M-bit is always zero and the O-bit may be set to one in the Router Advertisement (RA) sent to the UE.

3GPP network allocates each default bearer a unique /64 prefix, and uses layer-2 signaling to suggest user equipment an Interface Identifier that is guaranteed not to conflict with gateway's Interface Identifier. The UE must configure its link-local address

using this Interface Identifier. The UE is allowed to use any Interface Identifier it wishes for the other addresses it configures. There is no restriction, for example, of using Privacy Extension for SLAAC [RFC4941] or other similar types of mechanisms. However, there are network drivers that fail to pass the Interface Identifier to the stack and instead synthesize their own Interface Identifier (usually a MAC address equivalent). If the UE skips the Duplicate Address Detection (DAD) and also has other issues with the Neighbor Discovery Protocol (see Section 5.4), then there is a small theoretical chance that the UE configures exactly the same link-local address as the GGSN/PDN-GW. The address collision may then cause issues in the IP connectivity, for instance, the UE not being able to forward any packets to uplink.

In the 3GPP link model the /64 prefix assigned to the UE cannot be used for on-link determination (because the L-bit in the Prefix Information Option (PIO) in the RA must always be set to zero). If the advertised prefix is used for SLAAC then the A-bit in the PIO must be set to one. The details of the 3GPP link-model and address configuration is described in Section 11.2.1.3.2a of [TS.29061]. More specifically, the GGSN/PDN-GW guarantees that the /64 prefix is unique for the UE. Therefore, there is no need to perform any Duplicate Address Detection (DAD) on addresses the UE creates (i.e., the 'DupAddrDetectTransmits' variable in the UE could be zero). The GGSN/PDN-GW is not allowed to generate any globally unique IPv6 addresses for itself using the /64 prefix assigned to the UE in the RA.

The current 3GPP architecture limits number of prefixes in each bearer to a single /64 prefix. If the UE finds more than one prefix in the RA, it only considers the first one and silently discards the others [TS.29061]. Therefore, multi-homing within a single bearer is not possible. Renumbering without closing layer-2 connection is also not possible. The lifetime of /64 prefix is bound to lifetime of layer-2 connection even if the advertised prefix lifetime is longer than the layer-2 connection lifetime.

5.3. Prefix Delegation

IPv6 prefix delegation is a part of Release-10 and is not covered by any earlier release. However, the /64 prefix allocated for each default bearer (and to the user equipment) may be shared to local area network by user equipment implementing Neighbor Discovery proxy (ND proxy) [RFC4389] functionality.

Release-10 prefix delegation uses the DHCPv6-based prefix delegation [RFC3633]. The model defined for Release-10 requires aggregatable prefixes, which means the /64 prefix allocated for the default bearer

(and to the user equipment) must be part of the shorter delegated prefix. DHCPv6 prefix delegation has an explicit limitation described in Section 12.1 of [RFC3633] that a prefix delegated to a requesting router cannot be used by the delegating router (i.e., the PDN-GW in this case). This implies the shorter 'delegated prefix' cannot be given to the requesting router (i.e. the user equipment) as such but has to be delivered by the delegating router (i.e. the PDN-GW) in such a way the /64 prefix allocated to the default bearer is not part of the 'delegated prefix'. An option to exclude a prefix from delegation [I-D.ietf-dhc-pd-exclude] prevents this problem.

5.4. IPv6 Neighbor Discovery Considerations

3GPP link between the UE and the next hop router (e.g. GGSN) resemble a point to point (p2p) link, which has no link-layer addresses [RFC3316] and this has not changed from 2G/3G GPRS to EPS. The UE IP stack has to take this into consideration. When the 3GPP PDP Context appears as a PPP interface/link to the UE, the IP stack is usually prepared to handle Neighbor Discovery protocol and the related Neighbor Cache state machine transitions in an appropriate way, even though Neighbor Discovery protocol messages contain no link layer address information. However, some operating systems discard Router Advertisements on their PPP interface/link as a default setting. This causes the SLAAC to fail when the 3GPP PDP Context gets established, thus stalling all IPv6 traffic.

Currently several operating systems and their network drivers can make the 3GPP PDP Context to appear as an IEEE802 interface/link to the IP stack. This has few known issues, especially when the IP stack is made to believe the underlying link has link-layer addresses. First, the Neighbor Advertisement sent by a GGSN as a response to an address resolution triggered Neighbor Solicitation may not contain a Target Link-Layer address option (as suggested in [RFC4861] Section 4.4). Then it is possible that the address resolution never completes when the UE tries to resolve the link-layer address of the GGSN, thus stalling all IPv6 traffic.

Second, the GGSN may simply discard all address resolution triggered Neighbor Solicitation messages (as sometimes misinterpreted from [RFC3316] Section 2.4.1 that responding to address resolution and next-hop determination are not needed). As a result the address resolution never completes when the UE tries to resolve the link-layer address of the GGSN, thus stalling all IPv6 traffic. There is little that can be done about this in the GGSN, assuming the Neighbor Discovery implementation already does the right thing. But the UE stacks must be able to handle address resolution in the manner that they have chosen to represent the interface. In other words, if they emulate IEEE802 type interfaces, they also need to process Neighbor

Discovery messages correctly.

6. 3GPP Dual-Stack Approach to IPv6

6.1. 3GPP Networks Prior to Release-8

3GPP standards prior to Release-8 provide IPv6 access for cellular devices with PDP contexts of type IPv6 [TS.23060]. For dual-stack access, a PDP context of type IPv6 is established in parallel to the PDP context of type IPv4, as shown in Figure 5 and Figure 6. For IPv4-only service, connections are created over the PDP context of type IPv4 and for IPv6-only service connections are created over the PDP context of type IPv6. The two PDP contexts of different type may use the same APN (and the gateway), however, this aspect is not explicitly defined in standards. Therefore, cellular device and gateway implementations from different vendors may have varying support for this functionality.

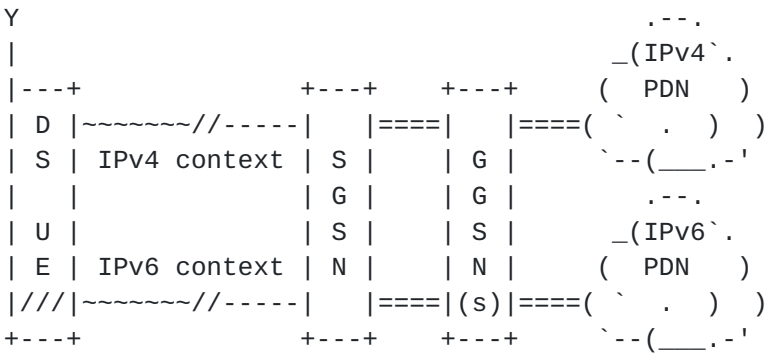

Figure 5: A dual-stack User Equipment connecting to both IPv4 and IPv6 Internet using parallel IPv4-only and IPv6-only PDP contexts

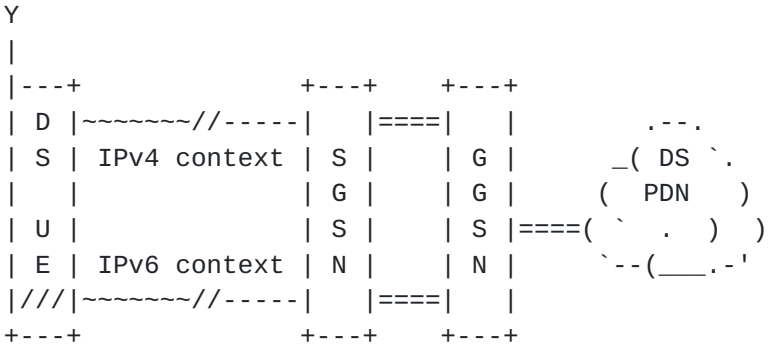

Figure 6: A dual-stack User Equipment connecting to dual-stack Internet using parallel IPv4-only and IPv6-only PDP contexts

The approach of having parallel IPv4 and IPv6 type of PDP contexts open is not optimal, because two PDP contexts require double the signaling and consume more network resources than a single PDP context. In the figure above the IPv4 and IPv6 PDP contexts are attached to the same GGSN. While this is possible, the dual-stack (DS) MS may be attached to different GGSNs in the scenario where one GGSN supports IPv4 PDN connectivity while another GGSN provides IPv6 PDN connectivity.

6.2. 3GPP Release-8 and -9 Networks

Since 3GPP Release-8, the powerful concept of a dual-stack type of PDN connection and EPS bearer have been introduced [TS.23401]. This enables parallel use of both IPv4 and IPv6 on a single bearer (IPv4v6), as illustrated in Figure 7, and makes dual stack simpler than in earlier 3GPP releases. As of Release-9, GPRS network nodes also support dual-stack type (IPv4v6) PDP contexts.

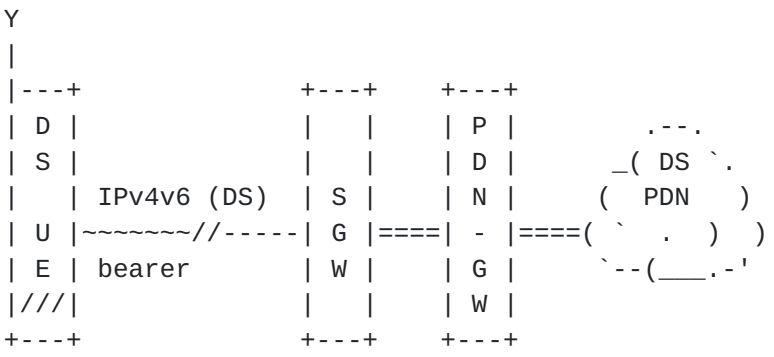

Figure 7: A dual-stack User Equipment connecting to dual-stack Internet using a single IPv4v6 type PDN connection

The following is a description of the various PDP contexts/PDN bearer types that are specified by 3GPP:

1. For 2G/3G access to GPRS core (SGSN/GGSN) pre-Release-9 there are two IP PDP Types, IPv4 and IPv6. Two PDP contexts are needed to get dual stack connectivity.

2. For 2G/3G access to GPRS core (SGSN/GGSN) from Release-9 there are three IP PDP Types, IPv4, IPv6 and IPv4v6. Minimum one PDP context is needed to get dual stack connectivity.

3. For 2G/3G access to EPC core (PDN-GW via S4-SGSN) from Release-8 there are three IP PDP Types, IPv4, IPv6 and IPv4v6 which gets mapped to PDN Connection type. Minimum one PDP Context is needed to get dual stack connectivity.

4. For LTE (E-UTRAN) access to EPC core from Release-8 there are three IP PDN Types, IPv4, IPv6 and IPv4v6. Minimum one PDN Connection is needed to get dual stack connectivity.

6.3. PDN Connection Establishment Process

The PDN connection establishment process is specified in detail in 3GPP specifications. Figure 8 illustrates the high level process and signaling involved in the establishment of a PDN connection.

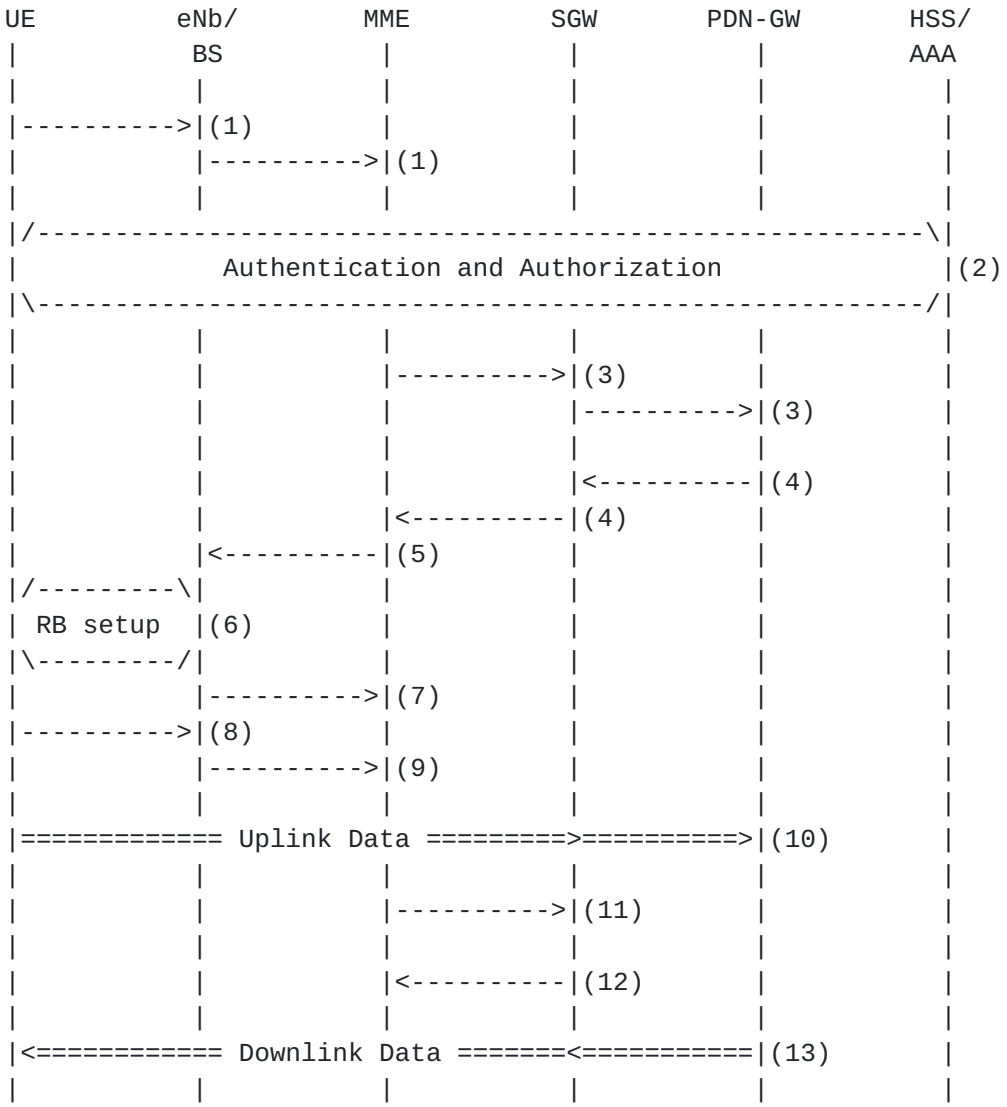

Figure 8: Simplified PDN connection setup procedure in Release-8

1. The UE (i.e the MS) requires a data connection and hence decides to establish a PDN connection with a PDN-GW. The UE sends an "Attach Request" (layer-2) to the BS. The BS forwards this attach request to the MME.

2. Authentication of the UE with the AAA server/HSS follows. If the UE is authorized for establishing a data connection, the following steps continue

3. The MME sends a "Create Session Request" message to the Serving-GW. The SGW forwards the create session request to the PDN-GW. The SGW knows the address of the PDN-GW to forward the create session request to as a result of this information having been obtained by the MME during the authentication/authorization phase.

   The UE IPv4 address and/or IPv6 prefix get assigned during this step. If a subscribed IPv4 address and/or IPv6 prefix is statically allocated for the UE for this APN, then the MME already passes the address information to the SGW and eventually to the PDN-GW in the "Create Session Request" message. Otherwise, the PDN-GW manages the address assignment to the UE (there is another variation to this where IPv4 address allocation is delayed until the UE initiates a DHCPv4 exchange but this is not discussed here).

4. The PDN-GW creates a PDN connection for the UE and sends "Create Session Response" message to the SGW from which the session request message was received from. The SGW forwards the response to the corresponding MME which originated the request.

5. The MME sends the "Attach Accept/Initial Context Setup request" message to the eNodeB/BS.

6. The radio bearer between the UE and the eNb is reconfigured based on the parameters received from the MME. (See note 1 below)

7. The eNb sends "Initial Context Response" message to the MME.

8. The UE sends a "Direct Transfer" message to the eNodeB which includes the Attach complete signal.

9. The eNodeB forwards the Attach complete message to the MME.

10. The UE can now start sending uplink packets to the PDN GW.

11. The MME sends a "Modify Bearer Request" message to the SGW.

12. The SGW responds with a "Modify Bearer Response" message. At this time the downlink connection is also ready.

13. The UE can now start receiving downlink packets, including possible SLAAC related IPv6 packets.

The type of PDN connection established between the UE and the PDN-GW can be any of the types described in the previous section. The dual-stack (DS) PDN connection, i.e the one which supports both IPv4 and IPv6 packets is the default one that will be established if no specific PDN connection type is specified by the UE in Release-8 networks.

Note 1: The UE receives the PDN Address Information Element [TS.24301] at the end of radio bearer setup messaging. This Information Element contains only the Interface Identifier of the IPv6 address. In a case of GPRS the PDP Address Information Element [TS.24008] would contain a complete IPv6 address. However, the UE must ignore the IPv6 prefix if it receives one in the message (see Section 11.2.1.3.2a of [TS.29061]).

6.4. Mobility of 3GPP IPv4v6 Type of Bearers

3GPP discussed at length various approaches to support mobility between a Release-8 LTE network and a pre-Release-9 2G/3G network without a S4-SGSN for the new dual-stack type of bearers. The chosen approach for mobility is as follows, in short: if a UE is allowed for doing handovers between a Release-8 LTE network and a pre-Release-9 2G/3G network without a S4-SGSN while having open PDN connections, only single stack bearers are used. Essentially this means following deployment options:

1. If a network knows a UE may do handovers between a Release-8 LTE network and a pre-Release-9 2G/3G network without a S4-SGSN, then the network is configured to provide only single stack bearers, even if the UE requests dual-stack bearers.

2. If the network knows the UE does handovers only between a Release-8 LTE network and a Release-9 2G/3G network or a pre-Release-9 network with a S4-SGSN, then the network is configured to provide the UE with dual-stack bearers on request. The same also applies for LTE-only deployments.

When a network operator and their roaming partners have upgraded their networks to Release-8, it is possible to use the new IPv4v6 dual-stack type of bearers. A Release-8 UE always requests for a dual-stack bearer, but accepts what is assigned by the network.

7. Dual-Stack Approach to IPv6 Transition in 3GPP Networks

3GPP networks can natively transport IPv4 and IPv6 packets between the UE and the gateway (GGSN or PDN-GW) as a result of establishing either a dual-stack PDP context or parallel IPv4 and IPv6 PDP contexts.

Current deployments of 3GPP networks primarily support IPv4-only. These networks can be upgraded to also support IPv6 PDP contexts. By doing so devices and applications that are IPv6 capable can start utilizing the IPv6 connectivity. This will also ensure that legacy devices and applications continue to work with no impact. As newer devices start using IPv6 connectivity, the demand for actively used IPv4 connections is expected to slowly decrease, helping operators with a transition to IPv6. With a dual-stack approach, there is always the potential to fallback to IPv4. A device which may be roaming in a network wherein IPv6 is not supported by the visited network could fall back to using IPv4 PDP contexts and hence the end user would at least get some connectivity. Unfortunately, dual-stack approach as such does not lower the number of used IPv4 addresses. Every dual-stack bearer still needs to be given an IPv4 address, private or public. This is a major concern with dual-stack bearers concerning IPv6 transition. However, if the majority of active IP communication has moved over to IPv6, then in case of Network Address Translation from IPv4 to IPv4 (NAT44) [RFC1918] IPv4 connections the number of active IPv4 connections can still be expected to gradually decrease and thus giving some level of relief regarding NAT44 function scalability.

As the networks evolve to support Release-8 EPS architecture and the dual-stack PDP contexts, newer devices will be able to leverage such capability and have a single bearer which supports both IPv4 and IPv6. Since IPv4 and IPv6 packets are carried as payload within GTP between the MS and the gateway (GGSN/PDN-GW) the transport network capability in terms of whether it supports IPv4 or IPv6 on the interfaces between the eNodeB and SGW or, SGW and PDN-GW is immaterial.

8. Deployment issues

8.1. Overlapping IPv4 Addresses

Given the shortage of globally routable public IPv4 addresses, operators tend to assign private IPv4 addresses [RFC1918] to UEs when they establish an IPv4-only PDP context or an IPv4v6 type PDN context. About 16 million UEs can be assigned a private IPv4 address that is unique within a domain. However, in case of many operators

the number of subscribers is greater than 16 million. The issue can be dealt with by assigning overlapping RFC 1918 IPv4 addresses to UEs. As a result the IPv4 address assigned to a UE within the context of a single operator realm would no longer be unique. This has the obvious and known issues of NATed IP connection in the Internet. Direct UE to UE connectivity becomes complicated, unless the UEs are within the same private address range pool and/or anchored to the same gateway, referrals using IP addresses will have issues and so forth. These are generic issues and not only a concern of the EPS. However, 3GPP as such does not have any mandatory language concerning NAT44 functionality in EPC. Obvious deployment choices apply also to EPC:

1. Very large network deployments are partitioned, for example, based on a geographical areas. This partitioning allows for overlapping IPv4 addresses ranges to be assigned to UEs that are in different areas. Each area has its own pool of gateways that are dedicated for a certain overlapping IPv4 address range (referred here later as a zone). Standard NAT44 functionality allows for communication from the [RFC1918] private zone to the Internet. Communication between zones require special arrangement, such as using intermediate gateways (e.g. Back to Back User Agent (B2BUA) in case of SIP).

2. A UE attaches to a gateway as part of the attach process. The number of UEs that a gateway supports is in the order of 1 to 10 million. Hence all the UEs assigned to a single gateway can be assigned private IPv4 addresses. Operators with large subscriber bases have multiple gateways and hence the same [RFC1918] IPv4 address space can be reused across gateways. The IPv4 address assigned to a UE is unique within the scope of a single gateway.

3. New services requiring direct connectivity between UEs should be built on IPv6. Possible existing IPv4-only services and applications requiring direct connectivity can be ported to IPv6.

8.2. IPv6 for transport

The various reference points of the 3GPP architecture such as S1-U, S5 and S8 are based on either GTP or PMIPv6. The underlying transport for these reference points can be IPv4 or IPv6. GTP has been able to operate over IPv6 transport (optionally) since R99 and PMIPv6 has supported IPv6 transport starting from its introduction in Release-8. The user plane traffic between the UE and the gateway can use either IPv4 or IPv6. These packets are essentially treated as payload by GTP/PMIPv6 and transported accordingly with no real attention paid to the information (at least from a routing perspective) contained in the IPv4 or IPv6 headers. The transport

links between the eNodeB and the SGW, and the link between the SGW and PDN-GW can be migrated to IPv6 without any direct implications to the architecture.

Currently, the inter-operator (for 3GPP technology) roaming networks are all IPv4-only (see Inter-PLMN Backbone Guidelines [GSMA.IR.34]). Eventually these roaming networks will also get migrated to IPv6, if there is a business reason for that. The migration period can be prolonged considerably because the 3GPP protocols always tunnel user plane traffic in the core network and as described earlier the transport network IP version is not in any way tied to user plane IP version. Furthermore, the design of the inter-operator roaming networks is such that the user plane and transport network IP addressing is completely separated from each other. The inter-operator roaming network itself is also completely separated from the Internet. Only those core network nodes that must be connected to the inter-operator roaming networks are actually visible there, and be able to send and receive (tunneled) traffic within the inter-operator roaming networks. Obviously, in order the roaming to work properly, the operators have to agree on supported protocol versions so that the visited network does not, for example, unnecessarily drop user plane IPv6 traffic.

8.3. Operational Aspects of Running Dual-Stack Networks

Operating dual-stack networks does imply cost and complexity to a certain extent. However these factors are mitigated by the assurance that legacy devices and services are unaffected and there is always a fallback to IPv4 in case of issues with the IPv6 deployment or network elements. The model also enables operators to develop operational experience and expertise in an incremental manner.

Running dual-stack networks requires the management of multiple IP address spaces. Tracking of UEs needs to be expanded since it can be identified by either an IPv4 address or IPv6 prefix. Network elements will also need to be dual-stack capable in order to support the dual-stack deployment model.

Deployment and migration cases described in Section 6.1 for providing dual-stack like capability may mean doubled resource usage in operator's network. This is a major concern against providing dual-stack like connectivity using techniques discussed in Section 6.1. Also handovers between networks with different capabilities in terms of networks being dual-stack like service capable or not, may turn out hard to comprehend for users and for application/services to cope with. These facts may add other than just technical concerns for operators when planning to roll out dual-stack service offerings.

8.4. Operational Aspects of Running a Network with IPv6-only Bearers

It is possible to allocate IPv6-only type bearers to UEs in 3GPP networks. IPv6-only bearer type has been part of the 3GPP specification since the beginning. In 3GPP Release-8 (and later) it was defined that a dual-stack UE (or when the radio equipment has no knowledge of the UE IP stack capabilities) must first attempt to establish a dual-stack bearer and then possibly fall back to single IP version bearer. A Release-8 (or later) UE with IPv6-only stack can directly attempt to establish an IPv6-only bearer. The IPv6-only behaviour is up to a subscription provisioning or a PDN-GW configuration, and the fallback scenarios do not necessarily cause additional signaling.

Although the bullets below introduce IPv6 to IPv4 address translation and specifically discuss NAT64 technology [RFC6144], the current 3GPP Release-8 architecture does not describe the use of address translation or NAT64. It is up to a specific deployment whether address translation is part of the network or not. Some operational aspects to consider for running a network with IPv6-only bearers:

- The UE must have an IPv6 capable stack and a radio interface capable of establishing an IPv6 PDP context or PDN connection.

- The GGSN/PDN-GW must be IPv6 capable in order to support IPv6 bearers. Furthermore, the SGSN/MME must allow the creation of PDP Type or PDN Type of IPv6.

- Many of the common applications are IP version agnostic and hence would work using an IPv6 bearer. However, applications that are IPv4 specific would not work.

- Inter-operator roaming is another aspect which causes issues, at least during the ramp up phase of the IPv6 deployment. If the visited network to which outbound roamers attach to does not support PDP/PDN Type IPv6, then there needs to be a fallback option. The fallback option in this specific case is mostly up to the UE to implement. Several cases are discussed in the following sections.

- If and when a UE using IPv6-only bearer needs to access to IPv4 Internet/network, a translation of some type from IPv6 to IPv4 has to be deployed in the network. NAT64 (and DNS64) is one solution that can be used for this purpose and works for a certain set of protocols (read TCP, UDP and ICMP, and when applications actually use DNS for resolving name to IP addresses).

8.5. Restricting Outbound IPv6 Roaming

Roaming was briefly touched upon in Sections 8.2 and 8.4. While there is interest in offering roaming service for IPv6 enabled UEs and subscriptions, not all visited networks are prepared for IPv6 outbound roamers:

- The visited network SGSN does not support the IPv6 PDP Context or IPv4v6 PDP Context types. These should mostly concern pre-Release-9 2G/3G networks without S4-SGSN but there is no definitive rule as the deployed feature sets vary depending on implementations and licenses.

- The visited network might not be commercially ready for IPv6 outbound roamers, while everything might work technically at the user plane level. This would lead to "revenue leakage" especially from the visited operator point of view (note that the use of visited network GGSN/PDN-GW does not really exist in commercial deployments today for data roaming).

It might be in the interest of operators to prohibit roaming selectively within specific visited networks until IPv6 roaming is in place. 3GPP does not specify a mechanism whereby IPv6 roaming is prohibited without also disabling IPv4 access and other packet services. The following options for disabling IPv6 access for roaming subscribers could be available in some network deployments:

- Using Policy and Charging Control (PCC) [TS.23203] functionality and its rules to fail, for example, the bearer authorization when a desired criteria is met. In this case that would be PDN/PDP Type IPv6/IPv4v6 and a specific visited network. The rules can be provisioned either in the home network or locally in the visited network.

- Some Home Location Register (HLR) and Home Subscriber Server (HSS) subscriber databases allow prohibiting roaming in a specific (visited) network for a specified PDN/PDP Type.

The obvious problems are that these solutions are not mandatory, are not unified across networks, and therefore also lack well-specified fall back mechanism from the UE point of view.

8.6. Inter-RAT Handovers and IP Versions

It is obvious that operators start incrementally deploy EPS along with the existing UTRAN/GERAN, handovers between different radio technologies (inter-RAT handovers) become inevitable. In case of inter-RAT handovers 3GPP supports the following IP addressing

scenarios:

- o E-UTRAN IPv4v6 bearer has to map one to one to UTRAN/GERAN IPv4v6 bearer.
- o E-UTRAN IPv6 bearer has to map one to one to UTRAN/GERAN IPv6 bearer.
- o E-UTRAN IPv4 bearer has to map one to one to UTRAN/GERAN IPv4 bearer.

Other types of configurations are not standardized. What the above rules essentially imply is that the network migration has to be planned and subscriptions provisioned based on the lowest common nominator, if inter-RAT handovers are desired. For example, if some part of the UTRAN network cannot serve anything but IPv4 bearers, then the E-UTRAN is also forced to provide only IPv4 bearers. Various combinations of subscriber provisioning regarding IP versions are discussed further in Section 8.7.

8.7. Provisioning of IPv6 Subscribers and Various Combinations During Initial Network Attachment

Subscribers' provisioned PDP/PDN Types have multiple configurations. The supported PDP/PDN Type is provisioned per each APN for every subscriber. The following PDN Types are possible in the HSS for a Release-8 subscription [TS.23401]:

- o IPv4v6 PDN Type (note that IPv4v6 PDP Type does not exist in a HLR and Mobile Application Part (MAP) [TS.29002] signaling prior Release-9).
- o IPv6-only PDN Type
- o IPv4-only PDN Type.
- o IPv4_or_IPv6 PDN Type (note that IPv4_or_IPv6 PDP Type does not exist in a HLR or MAP signaling. However, a HLR may have multiple APN configurations of different PDN Types, which effectively achieves the same functionality).

A Release-8 dual-stack UE must always attempt to establish a PDP/PDN Type IPv4v6 bearer. The same also applies when the modem part of the UE does not have exact knowledge whether the UE operating system IP stack is a dual-stack capable or not. A UE that is IPv6-only capable must attempt to establish a PDP/PDN Type IPv6 bearer. Last, a UE that is IPv4-only capable must attempt to establish a PDN/PDP Type IPv4 bearer.

In a case the PDP/PDN Type requested by a UE does not match what has been provisioned for the subscriber in the HSS (or HLR), the UE possibly falls back to a different PDP/PDN Type. The network (i.e. the MME or the S4-SGSN) is able to inform the UE during the network attachment signaling why it did not get the requested PDP/PDN Type. These response/cause codes are documented in [TS.24008] for requested PDP Types and [TS.24301] for requested PDN Types:

- (E)SM cause #50 "PDN/PDP type IPv4-only allowed".
- (E)SM cause #51 "PDN/PDP type IPv6-only allowed".
- (E)SM cause #52 "single address bearers only allowed".

The above response/cause codes apply to Release-8 and onwards. In pre-Release-8 networks used response/cause codes vary depending on the vendor, unfortunately.

Possible fall back cases when the network deploys MMEs and/or S4-SGSNs include (as documented in [TS.23401]):

- Requested and provisioned PDP/PDN Types match => requested.
- Requested IPv4v6 and provisioned IPv6 => IPv6 and a UE receives indication that IPv6-only bearer is allowed.
- Requested IPv4v6 and provisioned IPv4 => IPv4 and the UE receives indication that IPv4-only bearer is allowed.
- Requested IPv4v6 and provisioned IPv4_or_IPv6 => IPv4 or IPv6 is selected by the MME/S4-SGSN based on an unspecified criteria. The UE may then attempt to establish, based on the UE implementation, a parallel bearer of a different PDP/PDN Type.
- Other combinations cause the bearer establishment to fail.

In addition to PDP/PDN Types provisioned in the HSS, it is also possible for a PDN-GW (and a MME/S4-SGSN) to affect the final selected PDP/PDN Type:

- Requested IPv4v6 and configured IPv4 or IPv6 in the PDN-GW => IPv4 or IPv6. If the MME operator had included the "Dual Address Bearer Flag" into the bearer establishment signaling, then the UE receives an indication that IPv6-only or IPv4-only bearer is allowed.
- Requested IPv4v6 and configured IPv4 or IPv6 in the PDN-GW => IPv4 or IPv6. If the MME operator had not included the "Dual Address

Bearer Flag" into the bearer establishment signaling, then the UE may attempt to establish, based on the UE implementation, a parallel bearer of different PDP/PDN Type.

A SGSN that does not understand the requested PDP Type is supposed to handle the requested PDP Type as IPv4. If for some reason a MME does not understand the requested PDN Type, then the PDN Type is handled as IPv6.

9. IANA Considerations

This document has no requests to IANA.

10. Security Considerations

This document does not introduce any security related concerns. Section 5 of [RFC3316] already contains in depth discussion of IPv6 related security considerations in 3GPP networks prior Release-8. This section discusses few additional security concerns to take into consideration.

In 3GPP access the UE and the network always perform a mutual authentication during the network attachment [TS.33102][TS.33401]. Furthermore, each time a PDP Context/PDN Connection gets created, a new connection, a modification of an existing connection and an assignment of an IPv6 prefix or an IP address can be authorized against the PCC infrastructure [TS.23203] and/or PDN's AAA server.

The wireless part of the 3GPP link between the UE and the (e)NodeB as well as the signaling messages between the UE and the MME/SGSN can be protected depending on the regional regulation and operators' deployment policy. User plane traffic can be confidentiality protected. The control plane is always at least integrity and replay protected, and may also be confidentiality protected. The protection within the transmission part of the network depends on operators' deployment policy. [TS.33401]

Several of the on-link and neighbor discovery related attacks can be mitigated due the nature of 3GPP point to point link model, and the fact the UE and the first hop router (PGW/GGSN or SGW) being the only nodes on the link. For off-link IPv6 attacks the 3GPP EPS is as vulnerable as any IPv6 system.

There have also been concerns that the UE IP stack might use permanent subscriber identities, such as IMSI, as the source for IPv6 address Interface Identifier. This would be a privacy threat and

allow tracking of subscribers, and therefore use of IMSI (or any [TS.23003] defined identity) as the Interface Identifier is prohibited [TS.23401]. However, there is no standardized method to block such misbehaving UEs.

11. Summary and Conclusion

The 3GPP network architecture and specifications enable the establishment of IPv4 and IPv6 connections through the use of appropriate PDP context types. The current generation of deployed networks can support dual-stack connectivity if the packet core network elements such as the SGSN and GGSN have the capability. With Release-8, 3GPP has specified a more optimal PDP context type which enables the transport of IPv4 and IPv6 packets within a single PDP context between the UE and the gateway.

As devices and applications are upgraded to support IPv6 they can start leveraging the IPv6 connectivity provided by the networks while maintaining the fall back to IPv4 capability. Enabling IPv6 connectivity in the 3GPP networks by itself will provide some degree of relief to the IPv4 address space as many of the applications and services can start to work over IPv6. However without comprehensive testing of different applications and solutions that exist today and are widely used, for their ability to operate over IPv6 PDN connections, an IPv6-only access would cause disruptions.

12. Acknowledgements

The authors thank Shabnam Sultana, Sri Gundavelli, Hui Deng, Zhenqiang Li, Mikael Abrahamsson, James Woodyatt, Wes George, Martin Thomson, Russ Mundy, Cameron Byrne, Ales Vizdal, Frank Brockners, Adrian Farrel, Stephen Farrell, and Jari Arkko for their reviews and comments on this document.

13. Informative References

[GSMA.IR.34]
GSMA, "Inter-PLMN Backbone Guidelines", GSMA PRD IR.34.4.9, March 2010.

[I-D.ietf-dhc-pd-exclude]
Korhonen, J., Savolainen, T., Krishnan, S., and O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", draft-ietf-dhc-pd-exclude-03 (work in progress), August 2011.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

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

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

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

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

[RFC4389] Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, April 2006.

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

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

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

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.

[TR.23975] 3GPP, "IPv6 Migration Guidelines", 3GPP TR 23.975 1.1.1, June 2010.

[TS.23003]

3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 10.2.0, June 2011.

[TS.23060]
3GPP, "General Packet Radio Service (GPRS); Service description; Stage 2", 3GPP TS 23.060 8.8.0, March 2010.

[TS.23203]
3GPP, "Policy and charging control architecture (PCC)", 3GPP TS 23.203 8.11.0, September 2010.

[TS.23401]
3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 10.4.0, June 2011.

[TS.23402]
3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402 10.5.0, September 2011.

[TS.24008]
3GPP, "Mobile radio interface Layer 3 specification", 3GPP TS 24.008 8.12.0, December 2010.

[TS.24301]
3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)", 3GPP TS 24.301 8.8.0, December 2010.

[TS.29002]
3GPP, "Mobile Application Part (MAP) specification", 3GPP TS 29.002 9.5.0, June 2011.

[TS.29060]
3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", 3GPP TS 29.274 8.8.0, April 2010.

[TS.29061]
3GPP, "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)", 3GPP TS 29.061 8.5.0, April 2010.

[TS.29274]
3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)", 3GPP TS 29.060 8.11.0, December 2010.

[TS.33102]
3GPP, "3G Security; Security architecture", 3GPP TS 33.102 10.0.0, December 2010.

[TS.33401]
3GPP, "3GPP System Architecture Evolution (SAE); Security architecture", 3GPP TS 33.401 10.1.1, June 2011.

Authors' Addresses

Jouni Korhonen (editor)
Nokia Siemens Networks
Linnoitustie 6
FI-02600 Espoo
FINLAND

Email: jouni.nospam@gmail.com

Jonne Soininen
Renesas Mobile
Porkkalankatu 24
FI-00180 Helsinki
FINLAND

Email: jonne.soininen@renesasmobile.com

Basavaraj Patil
Nokia
6021 Connection drive
Irving, TX 75039
USA

Email: basavaraj.patil@nokia.com

Teemu Savolainen
Nokia
Hermiankatu 12 D
FI-33720 Tampere
FINLAND

Email: teemu.savolainen@nokia.com

Gabor Bajko
Nokia
323 Fairchild drive 6
Mountain view, CA 94043
USA

Email: gabor.bajko@nokia.com

Kaisu Iisakkila
Renesas Mobile
Porkkalankatu 24
FI-00180 Helsinki
FINLAND

Email: kaisu.iisakkila@renesasmobile.com