IPv6 in 3rd Generation Partnership Project (3GPP)
Evolved Packet System (EPS)

Abstract

   The use of cellular broadband for accessing the Internet and other
   data services via smartphones, tablets, and notebook/netbook
   computers has increased rapidly as a result of high-speed packet data
   networks such as HSPA, HSPA+, and now Long-Term Evolution (LTE) being
   deployed. Operators that have deployed networks based on 3rd
   Generation Partnership Project (3GPP) network architectures are
   facing IPv4 address shortages at the Internet registries and are
   feeling pressure to migrate to IPv6. This document describes the
   support for IPv6 in 3GPP network architectures.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   IPv6 support has been part of the 3rd Generation Partnership Project
   (3GPP) standards since the first release of the specifications
   (Release 99). This support extends to all radio access and packet-
   based system variants of the 3GPP architecture family. In addition,
   a lot of work has been invested by the industry to investigate
   different transition and deployment scenarios over the years.
   However, IPv6 deployment in commercial networks remains low. There
   are many factors that can be attributed to this lack of deployment.
   The most relevant factor is essentially the same as the reason for
   IPv6 not being deployed in other networks either, i.e., the lack of
   business and commercial incentives for deployment.

   3GPP network architectures have continued to evolve in the time since
   Release 99, which was finalized in early 2000. The most recent
   version of the 3GPP architecture, the Evolved Packet System (EPS) --
   commonly referred to as System Architecture Evolution (SAE), Long-
   Term Evolution (LTE), or Release-8 -- is a packet-centric
   architecture. In addition, the number of subscribers and devices
   using the 3GPP networks for Internet connectivity and data services
   has also increased phenomenally -- the number of mobile broadband
   subscribers has increased exponentially over the last couple of
   years.

   With subscriber growth projected to increase even further, and with
   recent depletion of available IPv4 address space by IANA, 3GPP
   operators and vendors are now in the process of identifying the
   scenarios and solutions needed to deploy IPv6.

   This document describes the establishment of IP connectivity in 3GPP
   network architectures, specifically in the context of IP bearers for
   3G General Packet Radio Service (GPRS) and for 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, 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 that have an IPv4-only stack will
   continue to be provided with IP connectivity to the Internet and
   services.

2. Devices that 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 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 Serving GPRS Support Node (SGSN) and the Gateway
GPRS Support Node (GGSN).

2. 3GPP Terminology and Concepts

2.1. Terminology

Access Point Name

    The Access Point Name (APN) is a Fully Qualified Domain Name
    (FQDN) and resolves to a set of gateways in an operator's network.
    The APNs are piggybacked on the administration of the DNS
    namespace.

Dual Address PDN/PDP Type

    The dual address Packet Data Network/Packet Data Protocol (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

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

Evolved Packet System

   The Evolved Packet System (EPS) is an evolution of the 3GPP GPRS
   system characterized by a higher-data-rate, lower-latency, packet-
   optimized system that supports multiple Radio Access Technologies
   (RATs). The EPS comprises the EPC together with the Evolved
   Universal Terrestrial Radio Access (E-UTRA) and the Evolved
   Universal Terrestrial Radio Access Network (E-UTRAN).

Evolved UTRAN

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

GPRS Tunnelling Protocol

   The GPRS Tunnelling Protocol (GTP) [TS.29060] [TS.29274]
   [TS.29281] is a tunnelling protocol defined by 3GPP. It is a
   network-based mobility protocol and is similar to Proxy Mobile
   IPv6 (PMIPv6) [RFC5213]. However, GTP also provides functionality
   beyond mobility, such as in-band signaling related to Quality of
   Service (QoS) and charging, among others.

GSM EDGE Radio Access Network

   The Global System for Mobile Communications (GSM) EDGE Radio
   Access Network (GERAN) is a communications network, commonly
   referred to as 2G or 2.5G, and consists of base stations and Base
   Station Controllers (BSCs), 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

   The Gateway GPRS Support Node (GGSN) is a gateway function in the
   GPRS that provides connectivity to the 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

   The General Packet Radio Service (GPRS) is a packet-oriented
   mobile data service available to users of the 2G and 3G cellular
   communication systems -- the GSM -- specified by 3GPP.

High-Speed Packet Access

   The High-Speed Packet Access (HSPA) and HSPA+ are enhanced
   versions of the Wideband Code Division Multiple Access (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 information related to call
   routing. All subscribers of an operator, and the subscribers'
   enabled services, are provisioned in the HLR.

Home Subscriber Server

   The Home Subscriber Server (HSS) is a database for a given
   subscriber and was 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

   The 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 the 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

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

Packet Data Network Gateway

   The Packet Data Network Gateway (PDN-GW) is a gateway function in
   the Evolved Packet System (EPS), which provides connectivity to
   the 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 User Equipment (UE) and a PDN using
   a specific 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 GPRS Support Node

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

   Serving Gateway

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

   Serving GPRS Support Node

      The Serving GPRS Support Node (SGSN) is a network element that is
      located between the radio access network (RAN) and the gateway
      (GGSN). A per-UE point-to-point (p2p) tunnel between the GGSN and
      SGSN transports the packets between the UE 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 an MT, for example, over the 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 that are hosts with the
      ability to obtain Internet connectivity via a 3GPP network. A MS
      is comprised of the Terminal Equipment (TE) and a Mobile Terminal
      (MT). The terms UE, MS, MN, and mobile are used interchangeably
      within this document.

   UMTS Terrestrial Radio Access Network

      The Universal Mobile Telecommunications System (UMTS) Terrestrial
      Radio Access Network (UTRAN) is a communications network, commonly
      referred to as 3G, and consists of NodeBs (3G base stations) and
      Radio Network Controllers (RNCs), which make up the UMTS radio
      access network. The UTRAN allows connectivity between the UE and
      the core network. The UTRAN is comprised of WCDMA, HSPA, and
      HSPA+ radio technologies.

   User Plane

      The user plane refers to data traffic and the required bearers for
      the data traffic. In practice, IP is the only data traffic
      protocol used in the 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. The 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 that do not provide Internet
   connectivity but rather provide connectivity to a closed network
   providing a set of the 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 illustrates the APN-based
   network connectivity concept.

```
                                                              .--.
                                                            _(.   )`.
                              .--.         +------------+  _(      PDN   `)_
                +---+       _(Core`.       |GW1         |====(   Internet   `)
                |RAN|      (    NW    )------|APN=internet|   ( `    .     )  )
 [UE]~~~~|RAN|----(`     .   )   )--+ +------------+     `--(_____)---'
  ^     +---+       `--(___.-'       |
  |                                   |                         .--.
  |                                   |     +----------+       _(.PDN`)
  |                                   +--|GW2         |      _(Operator`)_
  |                                      |APN=OpServ  |====(   Services    `)
 UE is attached                         +----------+   ( `    .      )  )
 to GW1 and GW2                                          `--(_____)---'
 simultaneously
```
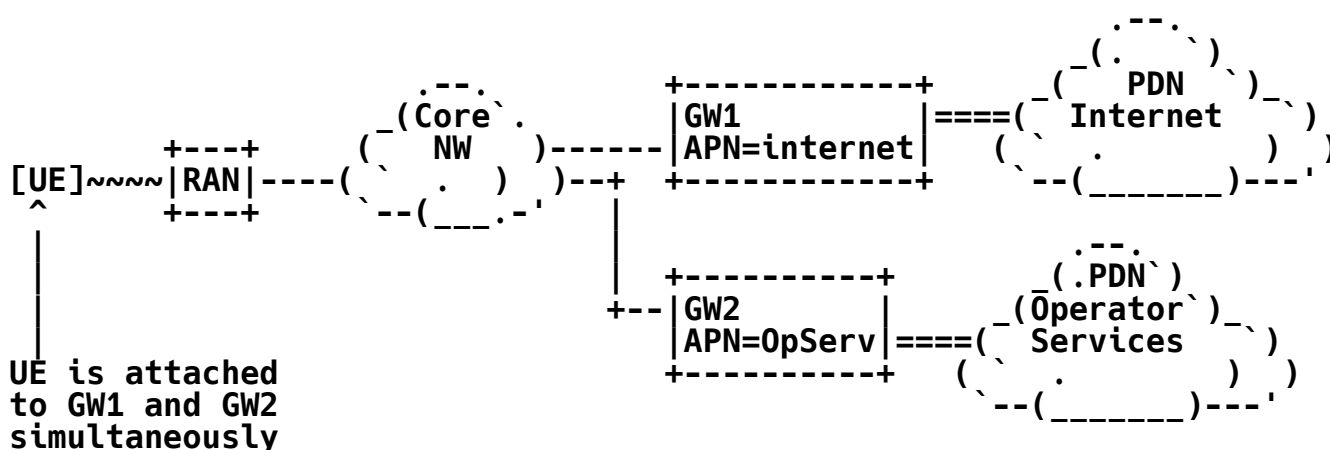
      Figure 1: User Equipment Attached to Multiple APNs Simultaneously

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 from R99 to
Release-7, and radio access technologies such as GSM (2G), EDGE (2G,
often referred to as 2.5G), WCDMA (3G), and HSPA(+) (3G, often
referred to 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.

```
              3G
              .--.
      Uu     _(    `.   Iu   +----+      +----+              .--.
  [UE]~~|~~~(   UTRAN  )--|---|SGSN|--|---|GGSN|--|----(    PDN  )
          (`  .   )  )       +----+  Gn +----+  Gi  (`  .   )  )
           --(___.-'          / |                    --(___.-'
                             /  |
              2G       Gb--  /   |
              .--.          /    |
             _(    `.      /     --Gp
  [UE]~~|~~~(   PDN  )__/       |
   Um  (`  .   )  )             .--.
        --(___.-'             _(.  `)
                            _( [GGSN] `)_
                           (    other    `)
                          (`  .  PLMN    )  )
                            --(_____)---'
```
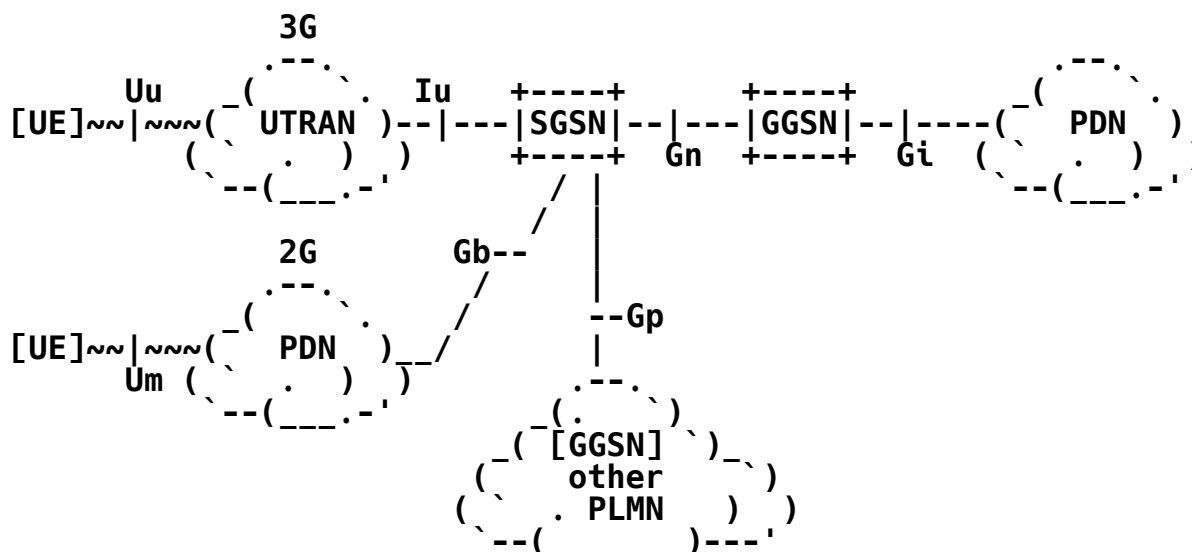
                Figure 2: Overview of the 2G/3G GPRS Logical Architecture

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

Gb: 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 Frame Relay or IP.

Iu: 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 the Radio
          Access Network Application Protocol (RANAP).

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

Uu/Um: 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 in 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, PDP Type IPv4v6
(dual-stack) as well.

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.

```
Y
|
| --+    _____   +---------+    .--.
|  |0_____PDPc1_____)|  APNx in |      (     `.
|  |                            |  GGSN /  |----(Internet)
|  |                            |  PDN-GW  |    ( `.   ) )
|UE|                            +---------+      `--(___.-'
|  |   _____   +---------+    .--.
|  |0_____PDPc2_____)|  APNy in |      _(Priv`.
+--+                       |  GGSN /  |-------(Network )
                           |  PDN-GW  |    ( `.   ) )
                           +---------+      `--(___.-'
```
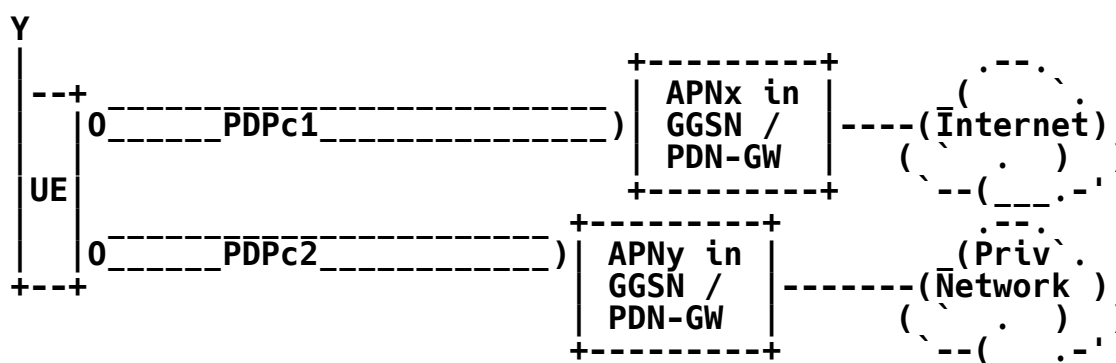
             Figure 3: PDP Contexts between the MS/UE and Gateway

   In the above figure, there are two PDP contexts at the MS/UE: the
   'PDPc1' PDP context, which is connected to APNx, provides 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 the MMS (Multimedia Messaging
   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 a 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 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, growth of
   traffic throughput, and control-signal processing.

```
                                                          +--------+
                                                          |   IP   |
                       S1-MME  +-------+  S11            |Services|
                   +----|----|  MME  |----|----+        +--------+
                   |         +-------+        |              |SGi
       +----+ LTE-Uu +-------+  S1-U           |         S5/  |
       |UE  |----|---|eNodeB |---|----------------| SGW   | S8 +-------+
       |    |======|=======|======================|======|======| PDN-GW |
       +----+      +-------+Dual-Stack EPS Bearer+------+      +-------+
```

                   Figure 4: EPS Architecture for 3GPP Access

   S5/S8:   Provides user-plane tunnelling and tunnel management between
             the 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 the
             PDN-GW and SGW are located inside one operator (i.e., a
             PLMN). The S8-interface is used if the PDN-GW and the SGW
             are located in different operator domains (i.e., a different
             PLMN).

   S11:   Reference point for the control-plane protocol between the
             MME and SGW, based on GTP-C (GTP control plane) and used,
             for example, during the establishment or modification of the
             default bearer.

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

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

   SGi: The interface between the PDN-GW and the PDN. The PDN 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). The 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., since
Release-8.

Each PDN connection has its own IP address/prefix assigned to it by
the PDN and anchored in the corresponding gateway. In the case of
the GTP-based S5/S8 interface, the PDN-GW is the first-hop router for
the UE, and in the 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
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 always provide low latency 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 connected to a PDN and
therefore do not get an IPv4 address and/or IPv6 prefix assigned
until they activate their first PDP context). This default bearer
will be allowed to carry all traffic that is not associated with a
dedicated bearer. Dedicated bearers are used to carry traffic for IP
flows that have been identified to require 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 Guaranteed Bit Rate (GBR) bearer if
dedicated network resources related to a 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 the eNodeB, and with no admission control.
However, the dedicated bearer can be either GBR or non-GBR. A GBR
bearer has a GBR and Maximum Bit Rate (MBR), while more than one
non-GBR bearer belonging to the same UE shares an Aggregate MBR

(AMBR). Non-GBR bearers can suffer packet loss under congestion,
while GBR bearers are immune to such losses as long as they honor the
contracted bit rates.

5. Address Management

5.1. IPv4 Address Configuration

The 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 on a 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-
dependent triggers to invoke the protocol.

5.2. IPv6 Address Configuration

IPv6 Stateless Address Autoconfiguration (SLAAC), as specified in
[RFC4861] and [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 that the
O-bit may be set to one in the Router Advertisement (RA) sent to
the UE.

The 3GPP network allocates each default bearer a unique /64 prefix,
and uses layer-2 signaling to suggest to the UE an Interface
Identifier that is guaranteed not to conflict with the 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, on using privacy extensions 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 Media Access Control (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 will configure exactly the same
link-local address as the GGSN/PDN-GW. The address collision may
then cause issues in IP connectivity -- for instance, the UE not
being able to forward any packets to the 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. Details of the 3GPP link-model and address
configuration are provided 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 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 the 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 the layer-2 connection is
also not possible. The lifetime of the /64 prefix is bound to the
lifetime of the 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 releases. However, the /64 prefix allocated for each
default bearer (and to the UE) may be shared to the local area
network by the UE implementing Neighbor Discovery proxy (ND proxy)
[RFC4389] functionality.

The 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 UE) 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 that the shorter 'delegated
prefix' cannot be given to the requesting router (i.e., the UE) as
such but has to be delivered by the delegating router (i.e., the
PDN-GW) in such a way that the /64 prefix allocated to the default
bearer is not part of the 'delegated prefix'. An option to exclude a
prefix from delegation [PD-EXCLUDE] prevents this problem.

5.4. IPv6 Neighbor Discovery Considerations

The 3GPP link between the UE and the next-hop router (e.g., the GGSN)
resembles a point-to-point (p2p) link, which has no link-layer
addresses [RFC3316], and this has not changed from the 2G/3G GPRS to
the 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 the 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 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 appear as an IEEE 802 interface/link to the
IP stack. This has a few known issues, especially when the IP stack
is made to believe that the underlying link has link-layer addresses.
First, the Neighbor Advertisement sent by a GGSN as a response to a
Neighbor Solicitation triggered by address resolution might not
contain a Target Link-Layer Address option (see Section 4.4 of
[RFC4861]). It is then 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 Neighbor Solicitation
messages triggered by address resolution (as Section 2.4.1 of
[RFC3316] is sometimes misinterpreted as saying that responding to
address resolution and next-hop determination is 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 IEEE 802 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 Figures 5 and 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.

```
   Y                                               .--.
   |                                             _(IPv4`.
   |---+              +---+     +---+          (`  PDN   )
   | D |~~~~~~~//-----|   |====|   |====(`   .   )  )
   | S |  IPv4 context| S |    | G |     `--(___.-'
   |   |              | G |    | G |        .--.
   | U |              | S |    | S |      _(IPv6`.
   | E |  IPv6 context| N |    | N |    (`  PDN   )
   |///|~~~~~~~//-----|   |====|(s)|====(`   .   )  )
   +---+              +---+     +---+     `--(___.-'
```
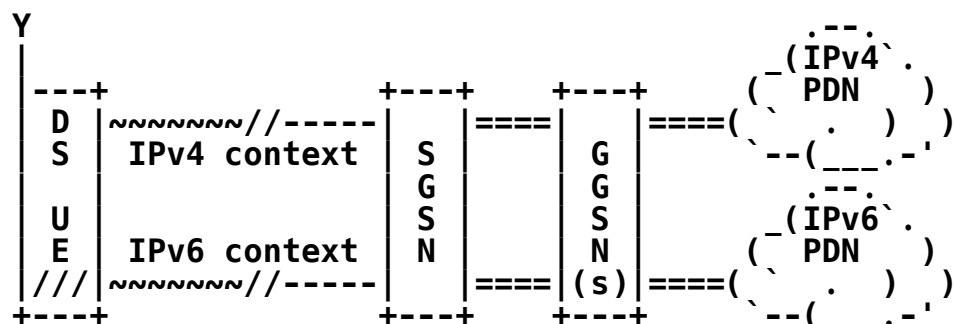
     Figure 5: Dual-Stack (DS) User Equipment Connecting to Both IPv4 and
       IPv6 Internet Using Parallel IPv4-Only and IPv6-Only PDP Contexts

```
   Y
   |
   |---+              +---+     +---+
   | D |~~~~~~~//-----|   |====|   |          .--.
   | S |  IPv4 context| S |    | G |        _( DS  `.
   |   |              | G |    | G |      (`  PDN   )
   | U |              | S |    | S |====(`   .   )  )
   | E |  IPv6 context| N |    | N |      `--(___.-'
   |///|~~~~~~~//-----|   |====|   |
   +---+              +---+     +---+
```
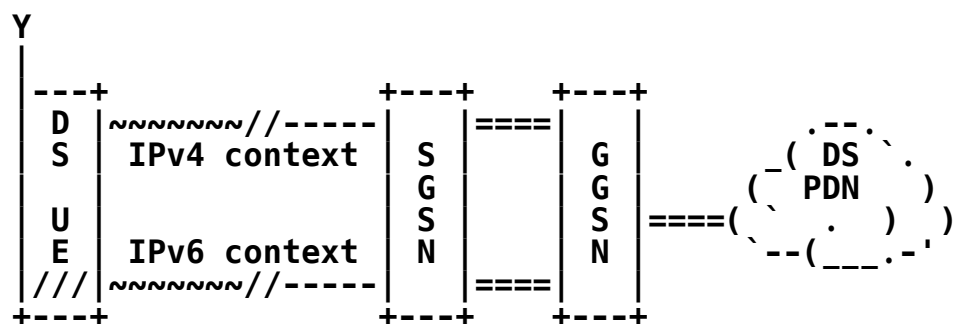
       Figure 6: Dual-Stack User Equipment Connecting to Dual-Stack Internet
                 Using Parallel IPv4-Only and IPv6-Only PDP Contexts

The approach of having parallel IPv4 and IPv6 types 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 Figure 6, the IPv4 and IPv6 PDP contexts are attached to
the same GGSN. While this is possible, the dual-stack 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 has 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 (IPv4v6) PDP contexts.

```
 Y
 |
 |---+                   +---+   +---+
 |   |                   |   |   | P |            .--.
 | D |                   |   |   | D |          _(  DS `.
 | S |    IPv4v6 (DS)    | S |   | N |         (  ` PDN   )
 |   |                   | G |   |   |       _(    .   )  )
 | U |~~~~~~~~//-----    | G |===| - |====(    .    )  )
 | E |                   | W |   | G |        `--(___.-'
 |///|   bearer          |   |   | W |
 |   |                   |   |   |   |
 +---+                   +---+   +---+
```
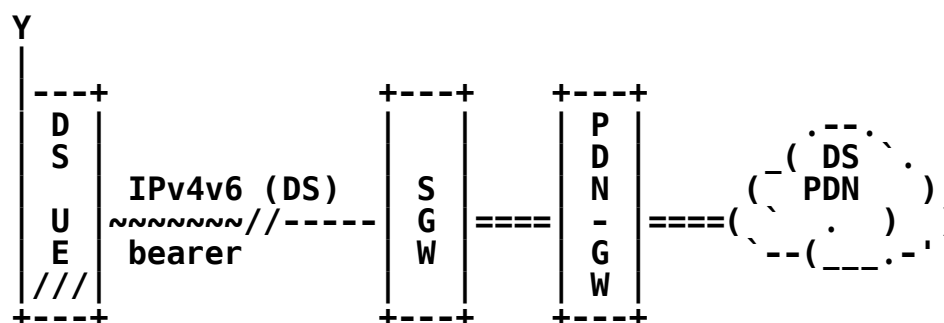
   **Figure 7: Dual-Stack User Equipment Connecting to Dual-Stack Internet
              Using a Single IPv4v6 PDN Connection**

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

1. For 2G/3G access to the 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 the GPRS core (SGSN/GGSN), starting with
    Release-9, there are three IP PDP Types: IPv4, IPv6, and IPv4v6.
    A minimum of one PDP context is needed to get dual-stack
    connectivity.

3. For 2G/3G access to the EPC (PDN-GW via S4-SGSN), starting with
    Release-8, there are three IP PDP Types: IPv4, IPv6, and IPv4v6
    (which gets mapped to the PDN connection type). A minimum of one
    PDP context is needed to get dual-stack connectivity.

4. For LTE (E-UTRAN) access to the EPC, starting with Release-8,
    there are three IP PDN Types: IPv4, IPv6, and IPv4v6. A minimum
    of 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
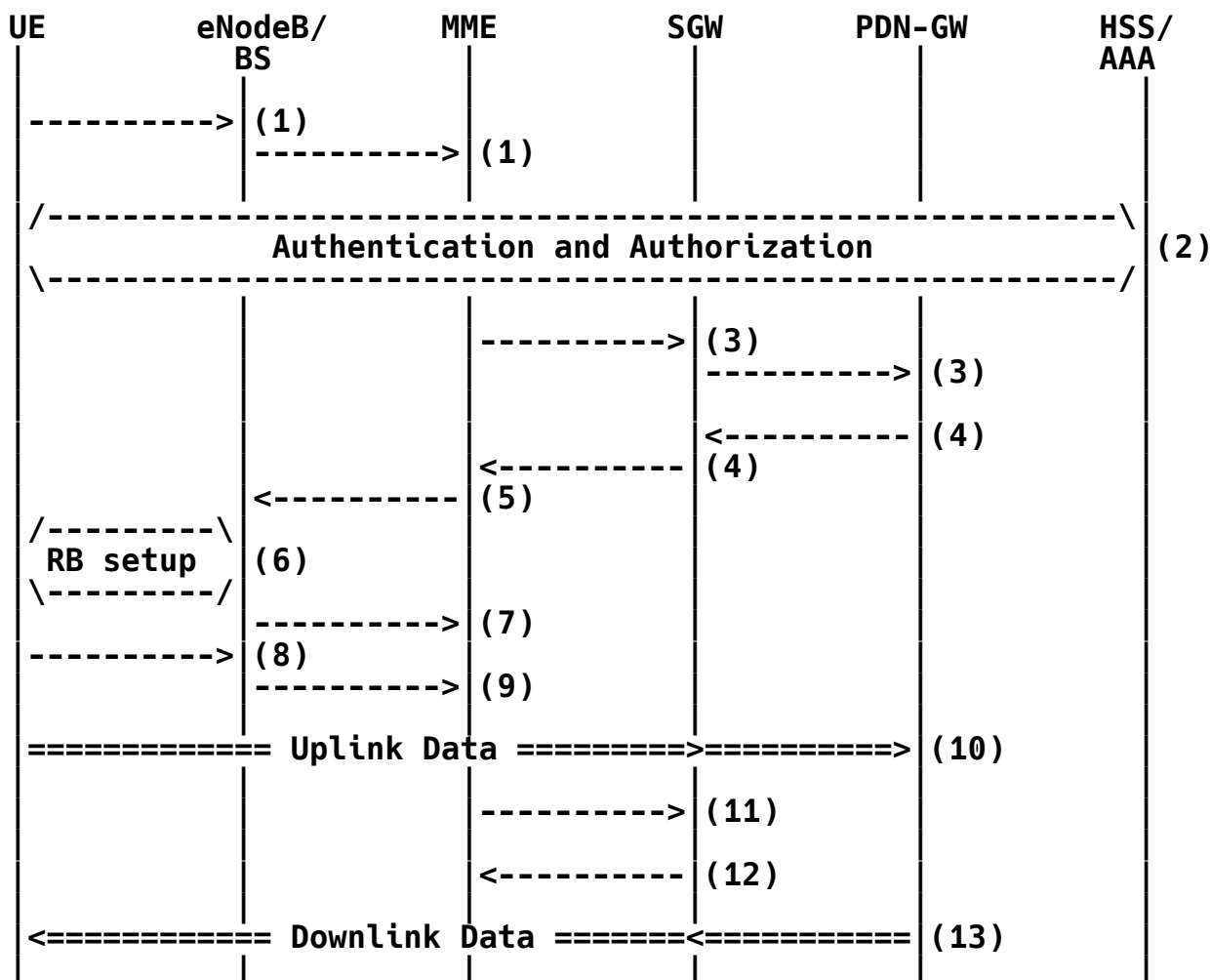   signaling involved in the establishment of a PDN connection.

```
    UE          eNodeB/        MME          SGW         PDN-GW        HSS/
                  BS                                                  AAA
    |             |             |            |             |           |
    | ---------->|(1)          |            |             |           |
    |             | ---------->|(1)          |             |          |
    |             |             |            |             |           |
    |/-----------------------------------------------------------------\
    <              Authentication and Authorization                     > (2)
    |\-----------------------------------------------------------------/
    |             |             |            |             |           |
    |             |             | --------->|(3)          |            |
    |             |             |            | ---------->|(3)         |
    |             |             |            |             |           |
    |             |             |            |<---------- |(4)         |
    |             |             |<---------- |(4)          |           |
    |             |<---------- |(5)          |             |           |
    |/----------\ |             |            |             |           |
    | RB setup   |(6)          |            |             |           |
    |\----------/ |             |            |             |           |
    |             | ---------->|(7)          |             |          |
    | ---------->|(8)          |            |             |           |
    |             | ---------->|(9)          |             |          |
    |             |             |            |             |           |
    |============ Uplink Data ========>==========> (10)    |           |
    |             |             |            |             |           |
    |             |             | --------->|(11)          |           |
    |             |             |            |             |           |
    |             |             |<---------- |(12)          |          |
    |             |             |            |             |           |
    |<=========== Downlink Data ======<=========== |(13)   |           |
    |             |             |            |             |           |
```

   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 base station (BS).
      The BS forwards this Attach request to the MME.

2.   Authentication of the UE with the Authentication, Authorization,
      and Accounting (AAA) server/HSS follows. If the UE is
      authorized to establish a data connection, the process continues
      with the following steps:

3.   The MME sends a "Create Session" request message to the SGW.
      The SGW forwards the Create Session request to the PDN-GW. The
      SGW knows the address of the PDN-GW to which it forwards the
      Create Session request 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 gets 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
      passes this previously allocated 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 step 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 a
      Create Session response message to the SGW from which the
      session request message was received. The SGW forwards the
      response to the corresponding MME that originated the request.

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

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

7.   The eNodeB sends an "Initial Context" response message to
      the MME.

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

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 PDN connection, i.e., the one that supports both IPv4 and IPv6
packets, is the default connection 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 the case of the 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 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 an S4-SGSN for the new dual-stack bearers. The chosen
   approach for mobility is as follows, in short: if a UE is allowed to
   do handovers between a Release-8 LTE network and a pre-Release-9
   2G/3G network without an S4-SGSN while having open PDN connections,
   only single-stack bearers are used. Essentially, this indicates the
   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 an 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 an 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 bearers. A Release-8 UE always requests 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 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 fall back to IPv4. A device that 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, the 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 the case of
Network Address Translation from IPv4 to IPv4 (NAT44), the number of
active NAT44-translated IPv4 connections can still be expected to
gradually decrease and thus give 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 that 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 between the 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 PDN context.
About 16 million UEs can be assigned a private IPv4 address that is
unique within a domain. However, for 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 connections 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 the EPC. Obvious deployment choices apply
also to the EPC:

1. Very large network deployments are partitioned, for example,
    based on geographical areas. This partitioning allows
    overlapping IPv4 address ranges to be assigned to UEs that are in
    different areas. Each area has its own pool of gateways that are
    dedicated to a certain overlapping IPv4 address range (also
    referred to as a zone). Standard NAT44 functionality allows for
    communication from the [RFC1918] private zone to the Internet.
    Communication between zones requires special arrangement, such as
    using intermediate gateways (e.g., a Back-to-Back User Agent
    (B2BUA) in the 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 on the order of 1 to 10
    million. Hence, all of 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 since 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 (at least from a routing perspective) to the
information 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 the user-plane
IP version. Furthermore, the design of the inter-operator roaming
networks is such that the user-plane and transport-network IP
addressing schemes are 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 are able to send and receive (tunneled) traffic within the
inter-operator roaming networks. Obviously, in order for 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 an 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 (see Section 6.1) for providing dual-stack capability may mean doubled resource usage in an operator's network. This is a major concern against providing dual-stack connectivity using techniques discussed in Section 6.1. Also, handovers between networks with different capabilities in terms of whether or not networks are capable of dual-stack service may prove difficult for users to comprehend and for applications/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 bearers to UEs in 3GPP networks. The IPv6-only bearer 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's capabilities) must first attempt to establish a dual-stack bearer and then possibly fall back to a single-stack bearer. A Release-8 (or later) UE with an IPv6-only stack can directly attempt to establish an IPv6-only bearer. The IPv6-only behavior is up to subscription provisioning or 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. The following are some operational aspects to consider for running a network with IPv6-only bearers:

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

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

o 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.

o Inter-operator roaming is another aspect that causes issues, at
   least during the ramp-up phase of the IPv6 deployment. If the
   visited network to which outbound roamers attach 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.

o If and when a UE using an IPv6-only bearer needs access to the
   IPv4 Internet/network, some type of translation from IPv6 to IPv4
   has to be deployed in the network. NAT64 (or 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 names 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:

   o 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 an S4-SGSN, but there is no
      definitive rule, as the deployed feature sets vary depending on
      implementations and licenses.

   o 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's point of view (note that
      the use of a visited-network GGSN/PDN-GW does not really exist
      today in commercial deployments 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:

   o Policy and Charging Control (PCC) [TS.23203] functionality and its
      rules, for example, could be used to cause bearer authorization to
      fail 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.

   o 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 a well-specified
   fallback mechanism from the UE's point of view.

8.6. Inter-RAT Handovers and IP Versions

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

   o The E-UTRAN IPv4v6 bearer has to map one to one to the UTRAN/GERAN
      IPv4v6 bearer.

   o The E-UTRAN IPv6 bearer has to map one to one to the UTRAN/GERAN
      IPv6 bearer.

   o The E-UTRAN IPv4 bearer has to map one to one to the UTRAN/GERAN
      IPv4 bearer.

   Other types of configurations are not standardized. The above rules
   essentially imply that the network migration has to be planned and
   subscriptions provisioned based on the lowest common denominator, if
   inter-RAT handovers are desired. For example, if some part of the
   UTRAN 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 the IPv4v6 PDP Type does not exist in
      an HLR and Mobile Application Part (MAP) [TS.29002] signaling
      prior to Release-9).

   o IPv6-only PDN Type.

o IPv4-only PDN Type.

o IPv4_or_IPv6 PDN Type (note that the IPv4_or_IPv6 PDP Type does
   not exist in an HLR or MAP signaling. However, an HLR may have
   multiple APN configurations of different PDN Types; these
   configurations would effectively achieve 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 of whether the UE operating system
IP stack is 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 where 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
network attachment signaling as to 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:

o (E)SM cause #50 "PDN/PDP type IPv4 only allowed".

o (E)SM cause #51 "PDN/PDP type IPv6 only allowed".

o (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, the response/cause codes that are used vary,
depending on the vendor, unfortunately.

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

o Requested and provisioned PDP/PDN Types match => requested.

o Requested IPv4v6 and provisioned IPv6 => IPv6, and a UE receives
   an indication that an IPv6-only bearer is allowed.

o Requested IPv4v6 and provisioned IPv4 => IPv4, and the UE receives
   an indication that an IPv4-only bearer is allowed.

   o 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.

   o 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 an MME/S4-SGSN) to affect the final
   selected PDP/PDN Type:

   o 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 in the bearer establishment signaling, then the UE
      would have received an indication that an IPv6-only or IPv4-only
      bearer is allowed.

   o 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 in the bearer establishment signaling, then the UE
      may have attempted to establish, based on the UE implementation, a
      parallel bearer of a different PDP/PDN Type.

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

9. Security Considerations

   This document does not introduce any security-related concerns.
   Section 5 of [RFC3316] already contains an in-depth discussion of
   IPv6-related security considerations in 3GPP networks prior to
   Release-8. This section discusses a 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 the operator's
   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 the operator's
deployment policy [TS.33401].

Several of the on-link and neighbor-discovery-related attacks can be
mitigated due to the nature of the 3GPP point-to-point link model,
and the fact that the UE and the first-hop router (PDN-GW/GGSN or
SGW) are 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 an International Mobile
Subscriber Identity (IMSI), as the source for the IPv6 address
Interface Identifier. This would be a privacy threat and would allow
tracking of subscribers. Therefore, the use of an IMSI (or any
identity defined by [TS.23003]) as the Interface Identifier is
prohibited [TS.23401]. However, there is no standardized method to
block such misbehaving UEs.

10. Summary and Conclusions

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 that capability.
With Release-8, 3GPP has specified a more optimal PDP context type
that 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 ability to fall back to IPv4. 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 current widely used applications and solutions for their
ability to operate over IPv6 PDN connections, an IPv6-only access
would cause disruptions.

11. 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, Paco Cortes, and Jari Arkko for their
reviews and comments on this document.

12. Informative References

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

[PD-EXCLUDE]   Korhonen, J., Ed., Savolainen, T., Krishnan, S., and O.
                Troan, "Prefix Exclude Option for DHCPv6-based Prefix
                Delegation", Work in Progress, December 2011.

[RFC1918]   Rekhter, Y., Moskowitz, B., Karrenberg, D., de 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., Ed., 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., Ed., 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 11.0.0, June 2011.

   [TS.23003]   3GPP, "Numbering, addressing and identification", 3GPP
                  TS 23.003 10.3.0, September 2011.

   [TS.23060]   3GPP, "General Packet Radio Service (GPRS); Service
                  description; Stage 2", 3GPP TS 23.060 8.14.0,
                  September 2011.

   [TS.23203]   3GPP, "Policy and charging control architecture", 3GPP
                  TS 23.203 8.12.0, June 2011.

   [TS.23401]   3GPP, "General Packet Radio Service (GPRS) enhancements
                  for Evolved Universal Terrestrial Radio Access Network
                  (E-UTRAN) access", 3GPP TS 23.401 10.5.0,
                  September 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;
                  Core network protocols; Stage 3", 3GPP
                  TS 24.008 8.14.0, June 2011.

   [TS.24301]   3GPP, "Non-Access-Stratum (NAS) protocol for Evolved
                  Packet System (EPS); Stage 3", 3GPP TS 24.301 8.10.0,
                  June 2011.

   [TS.29002]   3GPP, "Mobile Application Part (MAP) specification",
                  3GPP TS 29.002 9.6.0, September 2011.

   [TS.29060]   3GPP, "General Packet Radio Service (GPRS); GPRS
                  Tunnelling Protocol (GTP) across the Gn and Gp
                  interface", 3GPP TS 29.060 8.15.0, September 2011.

   [TS.29061]   3GPP, "Interworking between the Public Land Mobile
                  Network (PLMN) supporting packet based services and
                  Packet Data Networks (PDN)", 3GPP TS 29.061 8.8.0,
                  September 2011.

   [TS.29274]   3GPP, "3GPP Evolved Packet System (EPS); Evolved
                   General Packet Radio Service (GPRS) Tunnelling
                   Protocol for Control plane (GTPv2-C); Stage 3", 3GPP
                   TS 29.274 8.10.0, June 2011.

   [TS.29281]   3GPP, "General Packet Radio System (GPRS) Tunnelling
                   Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 10.3.0,
                   September 2011.

   [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 10.2.0,
                   September 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