Internet Engineering Task Force (IETF)
Request for Comments: 7445
Category: Informational
ISSN: 2070-1721

G. Chen
H. Deng
China Mobile
D. Michaud
Rogers Communications
J. Korhonen
Broadcom Corporation
M. Boucadair
France Telecom

March 2015

Analysis of Failure Cases in IPv6 Roaming Scenarios

Abstract

This document identifies a set of failure cases that may be encountered by IPv6-enabled mobile customers in roaming scenarios. The analysis reveals that the failure causes include improper configurations, incomplete functionality support in equipment, and inconsistent IPv6 deployment strategies between the home and the visited networks.

Copyright Notice

Table of Contents

1. Introduction

Many mobile operators have deployed IPv6, or are about to, in their operational networks. A customer in such a network can be provided IPv6 connectivity if their User Equipment (UE) is IPv6 compliant. Operators may adopt various approaches to deploy IPv6 in mobile networks, such as the solutions described in [TR23.975]. Depending on network conditions, either dual-stack or IPv6-only deployment schemes can be enabled.

A detailed overview of IPv6 support in 3GPP architectures is provided in [RFC6459].

It has been observed and reported that a mobile subscriber roaming around a different operator’s areas may experience service disruption due to inconsistent configurations and incomplete functionality of equipment in the network. This document focuses on these issues.

1.1. Terminology

This document makes use of these terms:

- o Mobile networks refer to 3GPP mobile networks.

- o Mobile UE denotes a 3GPP device that can be connected to 3GPP mobile networks.

- o The Public Land Mobile Network (PLMN) is a network that is operated by a single administrative entity. 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 [RFC6459].

- o The Home Location Register (HLR) is a pre-Release 5 database (but is also used in real deployments of Release 5 and later) 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 [RFC6459].

- o 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 [RFC6459].

- o "HLR/HSS" is used collectively for the subscriber database unless referring to the failure case related to General Packet Radio Service (GPRS) Subscriber data from the HLR.

An overview of key 3GPP functional elements is documented in [RFC6459].

"Mobile device" and "mobile UE" are used interchangeably.

2. Background

2.1. Roaming Architecture: An Overview

Roaming occurs in two scenarios:

- o International roaming: a mobile UE enters a visited network operated by a different operator, where a different PLMN code is used. The UEs could, either in an automatic mode or in a manual mode, attach to the visited PLMN.

- o Intra-PLMN mobility: an operator may have one or multiple PLMN codes. A mobile UE could pre-configure the codes to identify the Home PLMN (HPLMN) or Equivalent HPLMN (EHPLMN). Intra-PLMN mobility allows the UE to move to a different area of HPLMN and EHPLMN. When the subscriber profile is not stored in the visited area, HLR/HSS in the Home area will transmit the profile to the Serving GPRS Support Node (SGSN) / Mobility Management Entity (MME) in the visited area so as to complete network attachment.

When a UE is turned on or is transferred via a handover to a visited network, the mobile device will scan all radio channels and find available PLMNs to attach to. The SGSN or the MME in the visited networks must contact the HLR or HSS to retrieve the subscriber profile.

Steering of roaming may also be used by the HPLMN to further restrict which of the available networks the UE may be attached to. Once the authentication and registration stage is completed, the Packet Data Protocol (PDP) or Packet Data Networks (PDN) activation and traffic flows may be operated differently according to the subscriber profile stored in the HLR or the HSS.

The following subsections describe two roaming modes: Home-routed traffic (Section 2.1.1) and Local breakout (Section 2.1.2).

2.1.1. Home Routed Mode

In this mode, the subscriber’s UE gets IP addresses from the home network. All traffic belonging to that UE is therefore routed to the home network (Figure 1).

GPRS roaming exchange (GRX) or Internetwork Packet Exchange (IPX) networks [IR.34] are likely to be invoked as the transit network to deliver the traffic. This is the main mode for international roaming of Internet data services to facilitate the charging process between the two involved operators.

```
 +------------------------------+            +-------------------------+
 |Visited Network               |            |Home Network             |
 |  +-----+       +----+---+    | (GRX/IPX)  |    +---------+ Traffic Flow
 |  | UE |=======>|SGSN/SGW|====================>|GGSN/PGW|============>
 |  +-----+       +----+---+    |            |    +---------+          |
 |                |MME |        |            |                         |
 |                +----+        | Signaling  |    +---------+          |
 |                   |-------------------------->|HLR/HSS |           |
 |                              |            |    +---------+          |
 +------------------------------+            +-------------------------+
```

Figure 1: Home Routed Traffic

2.1.2. Local Breakout Mode

In the local breakout mode, IP addresses are assigned by the visited network to a roaming mobile UE. Unlike the home routed mode, the traffic doesn’t have to traverse GRX/IPX; it is offloaded locally at a network node close to that device’s point of attachment in the visited network. This mode ensures a more optimized forwarding path for the delivery of packets belonging to a visiting UE (Figure 2).

```
     +-----------------------------+            +-----------------+
     |Visited Network              |            |Home Network     |
     |  +-----+       +---------+  | Signaling  |    +---------+  |
     |  | UE |=======>|SGSN/MME|-------------------->|HLR/HSS |  |
     |  +-----+       +---+-----+  | (GRX/IPX)  |    +---------+  |
     |                |SGW|        |            |                 |
     |                +---+        |            |                 |
     |                  ||         |            |                 |
     |              +---------+    |            |                 |
     |              |GGSN/PGW|     |            |                 |
     |              +---------+    |            |                 |
     |    Traffic Flow  ||         |            |                 |
     +------------------||---------+            +-----------------+
                        \/
```

Figure 2: Local Breakout

The international roaming of services based on the IP Multimedia Subsystem (IMS), e.g., Voice over LTE (VoLTE)[IR.92], is claimed to select the local breakout mode in [IR.65]. Data service roaming across different areas within an operator network might use local breakout mode in order to get more efficient traffic forwarding and also ease emergency services. The local breakout mode could also be applied to an operator's alliance for international roaming of data service.

EU Roaming Regulation III [EU-Roaming-III] involves local breakout mode allowing European subscribers roaming in European 2G/3G networks to have their Internet data routed directly to the Internet from their current Visited Public Land Mobile Network (VPLMN).

Specific local breakout-related configuration considerations are listed below:

- o Operators may add the APN-OI-Replacement flag defined in 3GPP [TS29.272] into the user's subscription data. The visited network indicates a local domain name to replace the user requested Access Point Name (APN). Consequently, the traffic would be steered to the visited network. Those functions are normally deployed for the intra-PLMN mobility cases.

- o Operators may also configure the VPLMN-Dynamic-Address-Allowed flag [TS29.272] in the user's profile to enable local breakout mode in VPLMNs.

- o 3GPP specified the Selected IP Traffic Offload (SIPTO) function [TS23.401] since Release 10 in order to get efficient route paths. It enables an operator to offload a portion of the traffic at a network node close to the UE's point of attachment to the network.

- o The Global System for Mobile Communications Association (GSMA) has defined Roaming Architecture for Voice over LTE with Local Breakout (RAVEL) [IR.65] as the IMS international roaming architecture. Local breakout mode has been adopted for the IMS roaming architecture.

2.2. Typical Roaming Scenarios

Three stages occur when a subscriber roams to a visited network and intends to invoke services:

- o Network attachment: this occurs when the UE enters a visited network. During the attachment phase, the visited network should authenticate the subscriber and make a location update to the HSS/HLR in the home network of the subscriber. Accordingly, the subscriber profile is offered from the HSS/HLR. The subscriber profile contains the allowed APNs, the allowed PDP/PDN Types, and rules regarding the routing of data sessions (i.e., home routed or local breakout mode) [TS29.272]. The SGSN/MME in the visited network can use this information to facilitate the subsequent PDP/PDN session creation.

- PDP/PDN context creation: this occurs after the subscriber’s UE has been successfully attached to the network. This stage is integrated with the attachment stage in the case of 4G, but is a separate process in 2G/3G. 3GPP specifies three types of PDP/PDN to describe connections: PDP/PDN Type IPv4, PDP/PDN Type IPv6, and PDP/PDN Type IPv4v6. When a subscriber creates a data session, their device requests a particular PDP/PDN Type. The allowed PDP/PDN Types for that subscriber are learned in the attachment stage. Hence, the SGSN and MME via the Serving Gateway (SGW) could initiate a PDP/PDN request to Gateway GSN (GGSN) / Packet Data Network Gateway (PGW) modulo subscription grants.

- Service requests: when the PDP/PDN context is created successfully, UEs may launch applications and request services based on the allocated IP addresses. The service traffic will be transmitted via the visited network.

Failures that occur at the attachment stage (Section 3) are independent of home routed and the local breakout modes. Most failure cases in the PDP/PDN context creation (Section 4) and in service requests (Section 5) occur in the local breakout mode.

3. Failure Case in the Network Attachment

3GPP specified PDP/PDN Type IPv4v6 in order to allow a UE to get both an IPv4 address and an IPv6 prefix within a single PDP/PDN bearer. This option is stored as a part of subscription data for a subscriber in the HLR/HSS. PDP/PDN Type IPv4v6 has been introduced at the inception of the Evolved Packet System (EPS) in 4G networks.

The nodes in 4G networks should present no issues with the handling of this PDN Type. However, the level of support varies in 2G/3G networks depending on the SGSN software version. In theory, S4-SGSN (i.e., an SGSN with S4 interface) has supported the PDP/PDN Type IPv4v6 since Release 8, and Gn-SGSN (i.e., the SGSN with Gn interface) has supported it since Release 9. In most cases, operators normally use Gn-SGSN to connect either GGSN in 3G or Packet Data Network Gateway (PGW) in 4G.

The MAP (Mobile Application Part) protocol, as defined in 3GPP [TS29.002], is used over the Gr interface between SGSN and HLR. The MAP Information Element (IE) "ext-pdp-Type" contains the IPv4v6 PDP Type that is conveyed to SGSN from the HLR within the Insert Subscriber Data (ISD) MAP operation. If the SGSN does not support the IPv4v6 PDP Type, it will not support the "ext-pdp-Type" IE; consequently, it must silently discard that IE and continue processing the rest of the ISD MAP message. An issue that has been observed is that multiple SGSNs are unable to correctly process a subscriber's data received in the Insert Subscriber Data Procedure [TS23.060]. As a consequence, it will likely discard the subscriber attach request. This is erroneous behavior due to the equipment not being compliant with 3GPP Release 9.

In order to avoid encountering this attach problem at a visited SGSN, both operators should make a comprehensive roaming agreement to support IPv6 and ensure that it aligns with the GSMA documents, e.g., [IR.33], [IR.88], and [IR.21]. Such an agreement requires the visited operator to get the necessary patch on all its SGSN nodes to support the "ext-pdp-Type" MAP IE sent by the HLR. To ensure data-session continuity in Radio Access Technology (RAT) handovers, the PDN Type sent by the HSS to the MME should be consistent with the PDP Type sent by the HLR to the Gn-SGSN. Where roaming agreements and visited SGSN nodes have not been updated, the HPLMN also has to make use of specific implementations (not standardized by 3GPP, discussed further in Section 6) in the HLR/HSS of the home network. That is, when the HLR/HSS receives an Update Location message from a visited SGSN not known to support dual-stack in a single bearer, subscription data allowing only PDP/PDN Type IPv4 or IPv6 will be sent to that SGSN in the Insert Subscriber Data procedure. This guarantees that the user profile is compatible with the visited SGSN/MME capability. In addition, HSS may not have to change if the PGW is aware of the subscriber's roaming status and only restricts the accepted PDN Type consistent with PDP Type sent by the HLR. For example, a AAA server may coordinate with the PGW to decide the allowed PDN Type.

Alternatively, HPLMNs without the non-standardized capability to suppress the sending of "ext-pdp-Type" by the HLR may have to remove this attribute from APNs with roaming service. PDN Type IPv4v6 must also be removed from the corresponding profile for the APN in the HSS. This will restrict their roaming UEs to only IPv4 or IPv6 PDP/PDN activation. This alternative has problems:

- The HPLMN cannot support dual-stack in a single bearer at home where the APN profile in the HLR/HSS is also used for roaming.

- The UE may set up separate parallel bearers for IPv4 and IPv6, where only single-stack IPv4 or IPv6 service is preferred by the operator.

4. Failure Cases in the PDP/PDN Creation

When a subscriber's UE succeeds in the attach stage, the IP allocation process takes place to retrieve IP addresses. In general, a PDP/PDN Type IPv4v6 request implicitly allows the network side to make several IP assignment options, including IPv4-only, IPv6-only, IPv4 and IPv6 in single PDP/PDN bearer, and IPv4 and IPv6 in separated PDP/PDN bearers.

A PDP/PDN Type IPv4 or IPv6 restricts the network side to only allocate the requested IP address family.

This section summarizes several failures in the Home Routed (HR) and Local Breakout (LBO) mode as shown in Table 1.

Case#	UE request	PDP/PDN IP Type permitted on GGSN/PGW	Mode
#1	IPv4v6	IPv4v6	HR
	IPv4v6	IPv4 or IPv6	LBO
#2	IPv6	IPv6	HR
#3	IPv4	IPv6	HR
#4	IPv6	IPv4	LBO

Table 1: Failure Cases in the PDP/PDN Creation

4.1. Case 1: Splitting Dual-Stack Bearer

Dual-stack capability is provided using separate PDP/PDN activation in the visited network that doesn't support PDP/PDN Type IPv4v6. That means only separate, parallel, single-stack IPv4 and IPv6 PDP/PDN connections are allowed to be initiated to separately allocate an IPv4 address and an IPv6 prefix. The SGSN does not support the Dual Address Bearer Flag (DAF) or does not set the DAF because the operator uses single addressing per bearer to support interworking with nodes of earlier releases. Regardless of home routed or local breakout mode, GGSN/PGW will change PDN/PDP Type to a single address PDP/PDN Type and return the Session Management (SM) Cause #52 "single address bearers only allowed" or SM Cause #28 "unknown PDP address or PDP type" as per [TS24.008] and [TS24.301] to the UE. In this case, the UE may make another PDP/PDN request with a single address PDP Type (IPv4 or IPv6) other than the one already activated.

This approach suffers from the following drawbacks:

- The parallel PDP/PDN activation would likely double PDP/PDN bearer resource on the network side and Radio Access Bearer (RAB) resource on the Radio Access Network (RAN) side. It also impacts the capacity of the GGSN/PGW, since only a certain amount of PDP/PDN activation is allowed on those nodes.

- Some networks may allow only one PDP/PDN to be alive for each subscriber. For example, an IPv6 PDP/PDN will be rejected if the subscriber has an active IPv4 PDP/PDN. Therefore, the subscriber would not be able to obtain the IPv6 connection in the visited network. It is even worse, as they may have a risk of losing all data connectivity if the IPv6 PDP gets rejected with a permanent error at the APN level and not an error specific to the PDP-Type IPv6 requested.

- Additional correlations between those two PDP/PDN contexts are required on the charging system.

- Policy and Charging Rules Function (PCRF) [TS29.212] / Policy and Charging Enforcement Function (PCEF) treats the IPv4 and IPv6 sessions as independent and performs different quality-of-service (QoS) policies. The subscriber may have an unstable experience due to different behaviors on each IP version connection.

- Mobile devices may have a limitation on the number of allowed simultaneous PDP/PDN contexts. Excessive PDP/PDN activations may result in service disruption.

In order to avoid the issue, the roaming agreement in the home routed mode should make sure the visited SGSN supports and sets the DAF. Since the PDP/PDN Type IPv4v6 is supported in the GGSN/PGW of the home network, it’s expected that the visited SGSN/MME could create a dual-stack bearer as the UE requested.

In the local breakout mode, the visited SGSN may only allow single IP version addressing. In this case, the DAF on the visited SGSN/MME has to be unset. One approach is to set a dedicated APN [TS23.003] profile to only request PDP/PDN Type IPv4 in the roaming network. Some operators may also consider not adopting the local breakout mode to avoid the risks.

4.2. Case 2: IPv6 PDP/PDN Unsupported

PDP/PDN Type IPv6 has good compatibility to visited networks during the network attachment. In order to support the IPv6-only visitors, SGSN/MME in the visited network is required to accept IPv6-only PDP/PDN activation requests and enable IPv6 on the user plane in the direction of the home network.

In some cases, IPv6-only visitors may still be subject to the SGSN capability in visited networks. This becomes especially risky if the home operator performs roaming steering targeted to an operator that doesn't allow IPv6. The visited SGSN may just directly reject the PDP context activation. Therefore, it's expected that the visited network is IPv6 roaming-friendly to enable the functions on SGSN/MME by default. Otherwise, operators may consider steering the roaming traffic to the IPv6-enabled visited network that has an IPv6 roaming agreement.

4.3. Case 3: Inappropriate Roaming APN Set

If IPv6 single stack with the home routed mode is deployed, the requested PDP/PDN Type should also be IPv6. Some implementations that support the roaming APN profile may set IPv4 as the default PDP/PDN Type, since the visited network is incapable of supporting PDP/PDN Types IPv4v6 (Section 4.1) and IPv6 (Section 4.2). The PDP/PDN request will fail because the APN in the home network only allows IPv6. Therefore, the roaming APNs have to be compliant with the home network configuration when home routed mode is adopted.

4.4. Case 4: Fallback Failure

In the local breakout mode, PDP/PDN Type IPv6 should have no issues to pass through the network attachment process, since 3GPP specified the PDP/PDN Type IPv6 as early as PDP/PDN Type IPv4. When a visitor requests PDP/PDN Type IPv6, the network should only return the expected IPv6 prefix. The UE may fail to get an IPv6 prefix if the visited network only allocates an IPv4 address. In this case, the visited network will reject the request and send the cause code to the UE.

A proper fallback scheme for PDP/PDN Type IPv6 is desirable; however, there is no standard way to specify this behavior. The roaming APN profile could help to address the issue by setting the PDP/PDN Type to IPv4. For instance, the Android system solves the issue by configuring the roaming protocol to IPv4 for the APN. It guarantees that UE will always initiate a PDP/PDN Type IPv4 in the roaming area.

5. Failure Cases in the Service Requests

After the successful network attachment and IP address allocation, applications could start to request service based on the activated PDP/PDN context. The service request may depend on specific IP family or network collaboration. If traffic is offloaded locally (Section 2.1.2), the visited network may not be able to accommodate the UE's service requests. This section describes the failures.

5.1. Lack of IPv6 Support in Applications

Operators may only allow IPv6 in the IMS APN. VoLTE [IR.92] and Rich Communication Suite (RCS) [RCC.07] use the APN to offer voice service for visitors. The IMS roaming in RAVEL architecture [IR.65] offloads voice and video traffic in the visited network; therefore, a dual-stack visitor can only be assigned with an IPv6 prefix but no IPv4 address. If the applications can't support IPv6, the service is likely to fail.

Translation-based methods, for example, 464XLAT [RFC6877] or Bump-in-the-Host (BIH) [RFC6535], may help to address the issue if there are IPv6 compatibility problems. The translation function could be enabled in an IPv6-only network and disabled in a dual-stack or IPv4 network; therefore, the IPv4 applications only get the translation in the IPv6 network and they perform normally in an IPv4 or dual-stack network.

5.2. 464XLAT Support

464XLAT [RFC6877] is proposed to address the IPv4 compatibility issue in an IPv6-only connectivity environment. The customer-side translator (CLAT) function on a mobile device is likely used in conjunction with a PDP/PDN IPv6 Type request and cooperates with a remote NAT64 [RFC6146] device.

464XLAT may use the mechanism defined in [RFC7050] or [RFC7225] to detect the presence of NAT64 devices and to learn the IPv6 prefix used for protocol translation [RFC6052].

In the local breakout approach, a UE with the 464XLAT function roaming on an IPv6 visited network may encounter various situations. For example, the visited network may not have deployed DNS64 [RFC6147] but only NAT64, or CLAT may not be able to discover the provider-side translator (PLAT) translation IPv6 prefix used as a destination of the PLAT. If the visited network doesn't have a NAT64 and DNS64 deployed, 464XLAT can't perform successfully due to the lack of PLAT collaboration. Even in the case of the presence of NAT64 and DNS64, a pre-configured PLAT IPv6 prefix in the CLAT may cause failure because it can't match the PLAT translation.

Considering the various network configurations, operators may turn off local breakout and use the home routed mode to perform 464XLAT. Alternatively, UE may support the different roaming profile configuration to adopt 464XLAT in the home network and use IPv4-only in the visited networks.

6. HLR/HSS User Profile Setting

A proper user profile configuration would provide a deterministic outcome to the PDP/PDN creation stage where dual-stack, IPv4-only, and IPv6-only connectivity requests may come from devices. The HLR/HSS may have to apply extra logic (not standardized by 3GPP) to achieve this. It is also desirable that the network be able to set up connectivity of any requested PDP/PDN context type.

The following are examples to illustrate the settings for the scenarios and the decision criteria to be applied when returning user profile information from the HLR to the visited SGSN.

```
user profile #1:

PDP-Context ::= SEQUENCE {
pdp-ContextId ContextId,
pdp-Type  PDP-Type-IPv4
  ....
ext-pdp-Type PDP-Type-IPv4v6
  ...
}


user profile #2:

PDP-Context ::= SEQUENCE {
pdp-ContextId ContextId,
pdp-Type  PDP-Type-IPv6
  ....
}
```

Scenario 1: Support of IPv6-Only, IPv4-Only, and Dual-Stack Devices

The full PDP-context parameters are referred to Section 17.7.1 ("Mobile Service data types") of [TS29.002]. User profiles #1 and #2 share the same "ContextId". The setting of user profile #1 enables IPv4-only and dual-stack devices to work. User profile #2 fulfills the request if the device asks for IPv6-only PDP context.

```
user profile #1:

PDP-Context ::= SEQUENCE {
pdp-ContextId ContextId,
pdp-Type  PDP-Type-IPv4
  ....
ext-pdp-Type PDP-Type-IPv4v6
  ...
}


user profile #2:

PDP-Context ::= SEQUENCE {
pdp-ContextId ContextId,
pdp-Type  PDP-Type-IPv4
  ....
}
```

Scenario 2: Support of Dual-Stack Devices with Pre-Release 9 Visited SGSN (vSGSN) Access

User profiles #1 and #2 share the same "ContextId". If a visited SGSN is identified as early as pre-Release 9, the HLR/HSS should only send user profile #2 to the visited SGSN.

7. Discussion

Several failure cases have been discussed in this document. It has been illustrated that the major problems happen at three stages: the initial network attachment, the PDP/PDN creation, and service requests.

In the network attachment stage, PDP/PDN Type IPv4v6 is the major concern to the visited pre-Release 9 SGSN. 3GPP didn't specify PDP/PDN Type IPv4v6 in the earlier releases. That PDP/PDN Type is supported in the newly built EPS network, but it isn't supported well in the third-generation network. Visited SGSNs may discard the subscriber's attach requests because the SGSN is unable to correctly process PDP/PDN Type IPv4v6. Operators may have to adopt temporary solutions unless all the interworking nodes (i.e., the SGSN) in the visited network have been upgraded to support the ext-PDP-Type feature.

In the PDP/PDN creation stage, support of PDP/PDN Types IPv4v6 and IPv6 on the visited SGSN is the major concern. It has been observed that single-stack IPv6 in the home routed mode is a viable approach to deploy IPv6. It is desirable that the visited SGSN have the ability to enable IPv6 on the user plane by default. For support of the PDP/PDN Type IPv4v6, it is suggested to set the DAF. As a complementary function, the implementation of a roaming APN configuration is useful to accommodate the visited network. However, it should consider roaming architecture and the permitted PDP/PDN Type to properly set the UE. Roaming APN in the home routed mode is recommended to align with home network profile setting. In the local breakout case, PDP/PDN Type IPv4 could be selected as a safe way to initiate PDP/PDN activation.

In the service requests stage, the failure cases mostly occur in the local breakout case. The visited network may not be able to satisfy the requested capability from applications or UEs. Operators may consider using home routed mode to avoid these problems. Several solutions, in either the network side or mobile device side, can also help to address the issue. For example,

- o 464XLAT could help IPv4 applications access IPv6 visited networks.

- o Networks can deploy a AAA server to coordinate the mobile device capability. Once the GGSN/PGW receives the session creation request, it will initiate a request to a AAA server in the home network via the RADIUS or Diameter protocol [TS29.061]. The request contains subscriber and visited network information, e.g., PDP/PDN Type, International Mobile Equipment Identity (IMEI), Software Version (SV) and visited SGSN/MME location code, etc. The AAA server could take mobile device capability and combine it with the visited network information to ultimately determine the type of session to be created, i.e., IPv4, IPv6, or IPv4v6.

8. Security Considerations

Although this document defines neither a new architecture nor a new protocol, the reader is encouraged to refer to [RFC6459] for a generic discussion on IPv6-related security considerations.

9. References

9.1. Normative References

[IR.21] Global System for Mobile Communications Association (GSMA), "Roaming Database, Structure and Updating Procedures", IR.21, Version 7.4, November 2013.

[IR.65] Global System for Mobile Communications Association (GSMA), "IMS Roaming and Interworking Guidelines", IR.65, Version 15.0, January 2015.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011, <http://www.rfc-editor.org/info/rfc6146>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011, <http://www.rfc-editor.org/info/rfc6147>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, April 2013, <http://www.rfc-editor.org/info/rfc6877>.

[TS23.060] 3GPP, "General Packet Radio Service (GPRS); Service description; Stage 2 v9.00", TS 23.060, March 2009.

[TS23.401] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access v9.00", TS 23.401, March 2009.

[TS29.002] 3GPP, "Mobile Application Part (MAP) specification v9.12.0", TS 29.002, December 2009.

[TS29.272] 3GPP, "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol v9.00", TS 29.272, September 2009.

9.2. Informative References

[EU-Roaming-III] Amdocs Inc., "Amdocs 2014 EU Roaming Regulation III Solution", July 2013, <http://www.amdocs.com/Products/Revenue-Management/Documents/amdocs-eu-roaming-regulation-III-solution.pdf>.

[IR.33] Global System for Mobile Communications Association (GSMA), "GPRS Roaming Guidelines", IR.33, Version 7.0, June 2014.

[IR.34] Global System for Mobile Communications Association (GSMA), "Guidelines for IPX Provider networks", IR.34 Version 11.0, January 2015.

[IR.88] Global System for Mobile Communications Association (GSMA), "LTE Roaming Guidelines", IR.88, Version 12.0, January 2015.

[IR.92] Global System for Mobile Communications Association (GSMA), "IMS Profile for Voice and SMS", IR.92, Version 7.1, January 2015.

[RCC.07] Global System for Mobile Communications Association (GSMA), "Rich Communication Suite 5.2 Advanced Communications Services and Client Specification", RCC.07, Version 5.0, May 2014.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010, <http://www.rfc-editor.org/info/rfc6052>.

[RFC6459] Korhonen, J., Ed., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012, <http://www.rfc-editor.org/info/rfc6459>.

[RFC6535] Huang, B., Deng, H., and T. Savolainen, "Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)", RFC 6535, February 2012, <http://www.rfc-editor.org/info/rfc6535>.

[RFC7050] Savolainen, T., Korhonen, J., and D. Wing, "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis", RFC 7050, November 2013, <http://www.rfc-editor.org/info/rfc7050>.

[RFC7225] Boucadair, M., "Discovering NAT64 IPv6 Prefixes Using the Port Control Protocol (PCP)", RFC 7225, May 2014, <http://www.rfc-editor.org/info/rfc7225>.

[TR23.975] 3GPP, "IPv6 migration guidelines", TR 23.975, June 2011.

[TS23.003] 3GPP, "Numbering, addressing and identification v9.0.0", TS 23.003, September 2009.

[TS24.008] 3GPP, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 v9.00", TS 24.008, September 2009.

[TS24.301] 3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) ; Stage 3 v9.00", TS 24.301, September 2009.

[TS29.061] 3GPP, "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) v9.14.0", TS 29.061, January 2015.

[TS29.212] 3GPP, "Policy and Charging Control (PCC); Reference points v9.0.0", TS 29.212, September 2009.

Acknowledgements

Many thanks to F. Baker and J. Brzozowski for their support.

This document is the result of the IETF v6ops IPv6-Roaming design team effort.

The authors would like to thank Mikael Abrahamsson, Victor Kuarsingh, Nick Heatley, Alexandru Petrescu, Tore Anderson, Cameron Byrne, Holger Metschulat, and Geir Egeland for their helpful discussions and comments.

The authors especially thank Fred Baker and Ross Chandler for their efforts and contributions that substantially improved the readability of the document.

Contributors

The following individual contributed to this document.

Vizdal Ales
Deutsche Telekom AG
Tomickova 2144/1
Prague 4, 149 00
Czech Republic

EMail: ales.vizdal@t-mobile.cz

Authors' Addresses

Gang Chen
China Mobile
53A,Xibianmennei Ave.,
Xicheng District,
Beijing 100053
China

EMail: phdgang@gmail.com, chengang@chinamobile.com

Hui Deng
China Mobile
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China

EMail: denghui@chinamobile.com

Dave Michaud
Rogers Communications
8200 Dixie Rd.
Brampton, ON L6T 0C1
Canada

EMail: dave.michaud@rci.rogers.com

Jouni Korhonen
Broadcom Corporation
3151 Zanker Rd.
San Jose, CA 95134
United States

EMail: jouni.nospam@gmail.com

Mohamed Boucadair
France Telecom
Rennes,
35000
France

EMail: mohamed.boucadair@orange.com