Independent Submission
Request for Comments: 7620
Category: Informational
ISSN: 2070-1721

M. Boucadair, Ed.
B. Chatras
Orange
T. Reddy
Cisco Systems
B. Williams
Akamai, Inc.
B. Sarikaya
Huawei
August 2015

Scenarios with Host Identification Complications

Abstract

This document describes a set of scenarios in which complications when identifying which policy to apply for a host are encountered. This problem is abstracted as "host identification". Describing these scenarios allows commonalities between scenarios to be identified, which is helpful during the solution design phase.

This document does not include any solution-specific discussions.

IESG Note

This document describes use cases where IP addresses are overloaded with both location and identity properties. Such semantic overloading is seen as a contributor to a variety of issues within the routing system [RFC4984]. Additionally, these use cases may be seen as a way to justify solutions that are not consistent with IETF Best Current Practices on protecting privacy [BCP160] [BCP188].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The goal of this document is to enumerate scenarios that encounter the issue of uniquely identifying a host among those sharing the same IP address. Within this document, a host can be any device directly connected to a network operated by a network provider, a Home Gateway, or a roaming device located behind a Home Gateway.

An exhaustive list of encountered issues for the Carrier-Grade NAT (CGN), Address plus Port (A+P), and application proxies scenarios are documented in [RFC6269]. In addition to those issues, some of the scenarios described in this document suffer from additional issues such as:

- Identifying which policy to enforce for a host (e.g., limit access to the service based on some counters such as volume-based service offerings); enforcing the policy will have an impact on all hosts sharing the same IP address.
- Needing to correlate between the internal address:port and external address:port to generate and therefore enforce policies.
- Querying a location server for the location of an emergency caller based on the source IP address.

The goal of this document is to identify scenarios the authors are aware of and that share the same complications in identifying which policy to apply for a host. This problem is abstracted as the host identification problem.

The analysis of the scenarios listed in this document indicates several root causes for the host identification issue:

1. Presence of address sharing (CGN, A+P, application proxies, etc.).
2. Use of tunnels between two administrative domains.
3. Combination of address sharing and presence of tunnels in the path.

Even if these scenarios share the same root causes, describing the scenario allows to identify what is common between the scenarios, and then this information would help during the solution design phase.

2. Scope

This document can be used as a tool to design a solution(s) that mitigates the encountered issues. Note, [RFC6967] focuses only on the CGN, A+P, and application proxies cases. The analysis in [RFC6967] may not be accurate for some of the scenarios that do not span multiple administrative domains (e.g., Section 10.1).

This document does not target means that would lead to exposing a host beyond what the original packet, issued from that host, would have already exposed. Such means are not desirable nor required to solve the issues encountered in the scenarios discussed in this document. The focus is exclusively on means to restore the information conveyed in the original packet issued by a given host. These means are intended to help in identifying which policy to apply for a given flow. These means may rely on some bits of the source IP address and/or port number(s) used by the host to issue packets.

To prevent side effects and misuses of such means on privacy, a solution specification document(s) should explain, in addition to what is already documented in [RFC6967], the following:

- To what extent the solution can be used to nullify the effect of using address sharing to preserve privacy (see, for example, [EFFOpenWireless]). Note, this concern can be mitigated if the address-sharing platform is under the responsibility of the host's owner and the host does not leak information that would interfere with the host's privacy protection tool.
- To what extent the solution can be used to expose privacy information beyond what the original packet would have already exposed. Note, the solutions discussed in [RFC6967] do not allow extra information to be revealed other than what is conveyed in the original packet.

This document covers both IPv4 and IPv6.

This document does not include any solution-specific discussions. In particular, the document does not elaborate whether explicit authentication is enabled or not.

This document does not discuss whether specific information is needed to be leaked in packets, whether this is achieved out of band, etc. Those considerations are out of scope.

3. Scenario 1: Carrier-Grade NAT (CGN)

Several flavors of stateful CGN have been defined. A non-exhaustive list is provided below:

1. IPv4-to-IPv4 NAT (NAT44) [RFC6888] [STATELESS-NAT44]
2. DS-Lite NAT44 [RFC6333]
3. Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers (NAT64) [RFC6146]

4. IPv6-to-IPv6 Network Prefix Translation (NPTv6) [RFC6296]

As discussed in [RFC6967], remote servers are not able to distinguish between hosts sharing the same IP address (Figure 1). As a reminder, remote servers rely on the source IP address for various purposes such as access control or abuse management. The loss of the host identification will lead to issues discussed in [RFC6269].

```
+-----------+
|  HOST_1   |----+
+-----------+    |        +--------------------+      +------------+
                 |        |                    |------|  Server 1  |
+-----------+  +-----+    |                    |      +------------+
|  HOST_2   |--| CGN |----|      INTERNET      |            ::
+-----------+  +-----+    |                    |      +------------+
                  |       |                    |------|  Server n  |
+-----------+     |       +--------------------+      +------------+
|  HOST_3   |-----+
+-----------+
```

Figure 1: CGN Reference Architecture

Some of the above-referenced CGN scenarios will be satisfied by eventual completion of the transition to IPv6 across the Internet (e.g., NAT64), but this is not true of all CGN scenarios (e.g., NPTv6 [RFC6296]) for which some of the issues discussed in [RFC6269] will be encountered (e.g., impact on geolocation).

Privacy-related considerations discussed in [RFC6967] apply for this scenario.

4. Scenario 2: Address plus Port (A+P)

A+P [RFC6346] [RFC7596] [RFC7597] denotes a flavor of address-sharing solutions that does not require any additional NAT function to be enabled in the service provider’s network. A+P assumes subscribers are assigned with the same IPv4 address together with a port set. Subscribers assigned with the same IPv4 address should be assigned non-overlapping port sets. Devices connected to an A+P-enabled network should be able to restrict the IPv4 source port to be within a configured range of ports. To forward incoming packets to the appropriate host, a dedicated entity called the Port-Range Router (PRR) [RFC6346] is needed (Figure 2).

Similar to the CGN case, remote servers rely on the source IP address for various purposes such as access control or abuse management. The loss of the host identification will lead to the issues discussed in

[RFC6269]. In particular, it will be impossible to identify hosts sharing the same IP address by remote servers.

```
   +-----------+
   |  HOST_1   |----+
   +-----------+    |        +--------------------+      +------------+
                    |        |                    |------|  Server 1  |
   +-----------+  +-----+    |                    |      +------------+
   |  HOST_2   |--| PRR |----|      INTERNET      |            ::
   +-----------+  +-----+    |                    |      +------------+
                     |       |                    |------|  Server n  |
   +-----------+     |       +--------------------+      +------------+
   |  HOST_3   |-----+
   +-----------+
```

Figure 2: A+P Reference Architecture

Privacy-related considerations discussed in [RFC6967] apply for this scenario.

5. Scenario 3: On-Premise Application Proxy Deployment

This scenario is similar to the CGN scenario (Section 3).

Remote servers are not able to distinguish hosts located behind the proxy. Applying policies on the perceived external IP address as received from the proxy will impact all hosts connected to that proxy.

Figure 3 illustrates a simple configuration involving a proxy. Note several (per-application) proxies may be deployed. This scenario is a typical deployment approach used within enterprise networks.

```
   +-----------+
   |  HOST_1   |----+
   +-----------+    |        +--------------------+      +------------+
                    |        |                    |------|  Server 1  |
   +-----------+  +-----+    |                    |      +------------+
   |  HOST_2   |--|Proxy|----|      INTERNET      |            ::
   +-----------+  +-----+    |                    |      +------------+
                     |       |                    |------|  Server n  |
   +-----------+     |       +--------------------+      +------------+
   |  HOST_3   |-----+
   +-----------+
```

Figure 3: Proxy Reference Architecture

The administrator of the proxy may have many reasons for wanting to proxy traffic - including caching, policy enforcement, malware scanning, reporting on network or user behavior for compliance, or security monitoring.

The same administrator may also wish to selectively hide or expose the internal host identity to servers. He/she may wish to hide the identity to protect end-user privacy or to reduce the ability of a rogue agent to learn the internal structure of the network. He/she may wish to allow upstream servers to identify hosts to enforce access policies (for example, on documents or online databases), to enable account identification (on subscription-based services) or to prevent spurious misidentification of high-traffic patterns as a DoS attack. Application-specific protocols exist for enabling such forwarding on some plaintext protocols (e.g., Forwarded headers on HTTP [RFC7239] or time-stamp-line headers in SMTP [RFC5321]).

Servers not receiving such notifications but wishing to perform host or user-specific processing are obliged to use other application-specific means of identification (e.g., cookies [RFC6265]).

Packets/connections must be received by the proxy regardless of the IP address family in use. The requirements of this scenario are not satisfied by eventual completion of the transition to IPv6 across the Internet. Complications will arise for both IPv4 and IPv6.

Privacy-related considerations discussed in [RFC6967] apply for this scenario.

6. Scenario 4: Distributed Proxy Deployment

This scenario is similar to the proxy deployment scenario (Section 5) with the same use cases. However, in this instance part of the functionality of the application proxy is located in a remote site. This may be desirable to reduce infrastructure and administration costs or because the hosts in question are mobile or roaming hosts tied to a particular administrative zone of control but not to a particular network.

In some cases, a distributed proxy is required to identify a host on whose behalf it is performing the caching, filtering, or other desired service - for example, to know which policies to enforce. Typically, IP addresses are used as a surrogate. However, in the presence of CGN, this identification becomes difficult. Alternative solutions include the use of cookies, which only work for HTTP traffic, tunnels, or proprietary extensions to existing protocols.

```
      +-----------+             +----------+
      |  HOST_1   |-------------|          |
      +-----------+             |          |   +-------+    +----------+
                                |          |   |       |----| Server 1 |
      +-----------+             |          |   |       |    +----------+
      |  HOST_2   |----+        | INTERNET |---| Proxy |         ::
      +-----------+  +-----+    |          |   |       |    +----------+
                     |Proxy|----|          |   |       |----| Server n |
      +-----------+  +-----+    |          |   +-------+    +----------+
      |  HOST_3   |----+        +----------+
      +-----------+
```

Figure 4: Distributed Proxy Reference Architecture (1)

```
       +-----------+         +---+         +---+  +----------+
       |  HOST_1   +---------+ I |         | I +--+ Server 1 |
       +-----------+         | N |  +---+  | N |  +----------+
                             | T |  | P |  | T |
       +-----------+  +---+  | E |  | r |  | E |  +----------+
       |  HOST_2   +--+ P |  | R +--+ o +--+ R +--+ Server 2 |
       +-----------+  | r |  | N |  | x |  | N |  +----------+
                      | o |--+ E |  | y |  | E |      ::
       +-----------+  | x |  | T |  +---+  | T |  +----------+
       |  HOST_3   +--+ y |  |   |         |   +--+ Server N |
       +-----------+  +---+  +---+         +---+  +----------+
```

Figure 5: Distributed Proxy Reference Architecture (2)

Packets/connections must be received by the proxy regardless of the IP address family in use. The requirements of this scenario are not satisfied by eventual completion of the transition to IPv6 across the Internet. Complications will arise for both IPv4 and IPv6.

If the proxy and the servers are under the responsibility of the same administrative entity (Figure 4), no privacy concerns are raised. Nevertheless, privacy-related considerations discussed in [RFC6967] apply if the proxy and the servers are not managed by the same administrative entity (Figure 5).

7. Scenario 5: Overlay Network

An overlay network is a network of machines distributed throughout multiple autonomous systems within the public Internet that can be used to improve the performance of data transport (see Figure 6). IP packets from the sender are delivered first to one of the machines that make up the overlay network. That machine then relays the IP packets to the receiver via one or more machines in the overlay network, applying various performance enhancement methods.

```
                    +------------------------------------+
                    |                                    |
                    |              INTERNET              |
                    |                                    |
     +-----------+  |  +------------+                    |
     |  HOST_1   |-----| OVRLY_IN_1 |-----------+        |
     +-----------+  |  +------------+           |        |
                    |                          |        |
     +-----------+  |  +------------+     +-----------+  |  +--------+
     |  HOST_2   |-----| OVRLY_IN_2 |-----| OVRLY_OUT |-----| Server |
     +-----------+  |  +------------+     +-----------+  |  +--------+
                    |                          |        |
     +-----------+  |  +------------+           |        |
     |  HOST_3   |-----| OVRLY_IN_3 |-----------+        |
     +-----------+  |  +------------+                    |
                    |                                    |
                    +------------------------------------+
```

Figure 6: Overlay Network Reference Architecture

Such overlay networks are used to improve the performance of content delivery [IEEE1344002]. Overlay networks are also used for peer-to-peer data transport [RFC5694], and they have been suggested for use in both improved scalability for the Internet routing infrastructure [RFC6179] and provisioning of security services (intrusion detection, anti-virus software, etc.) over the public Internet [IEEE101109].

In order for an overlay network to intercept packets and/or connections transparently via base Internet connectivity infrastructure, the overlay ingress and egress hosts (OVERLAY_IN and OVERLAY_OUT) must be reliably in path in both directions between the connection-initiating HOST and the SERVER. When this is not the case, packets may be routed around the overlay and sent directly to the receiving host, presumably without invoking some of the advanced service functions offered by the overlay.

For public overlay networks, where the ingress and/or egress hosts are on the public Internet, packet interception commonly uses network address translation for the source (SNAT) or destination (DNAT) addresses in such a way that the public IP addresses of the true endpoint hosts involved in the data transport are invisible to each other (see Figure 7). For example, the actual sender and receiver may use two completely different pairs of source and destination addresses to identify the connection on the sending and receiving networks in cases where both the ingress and egress hosts are on the public Internet.

```
          IP hdr contains:               IP hdr contains:
SENDER -> src = sender   --> OVERLAY --> src = overlay2  --> RECEIVER
          dst = overlay1                 dst = receiver
```

Figure 7: NAT Operations in an Overlay Network

In this scenario, the remote server is not able to distinguish among hosts using the overlay for transport. In addition, the remote server is not able to determine the overlay ingress point being used by the host, which can be useful for diagnosing host connectivity issues.

In some of the above-referenced scenarios, IP packets traverse the overlay network fundamentally unchanged, with the overlay network functioning much like a CGN (Section 3). In other cases, connection-oriented data flows (e.g., TCP) are terminated by the overlay in order to perform object caching and other such transport and application-layer optimizations, similar to the proxy scenario (Section 5). In both cases, address sharing is a requirement for packet/connection interception, which means that the requirements for this scenario are not satisfied by the eventual completion of the transition to IPv6 across the Internet.

More details about this scenario are provided in [OVERLAYPATH].

This scenario does not introduce privacy concerns since the identification of the host is local to a single administrative domain (i.e., Content Delivery Network (CDN) Overlay Network) or passed to a remote server to help forwarding back the response to the appropriate host. The host identification information is not publicly available nor can be disclosed to other hosts connected to the Internet.

8. Scenario 6: Policy and Charging Control Architecture (PCC)

This issue is related to the PCC framework defined by 3GPP in [TS23.203] when a NAT is located between the Policy and Charging Enforcement Function (PCEF) and the Application Function (AF) as shown in Figure 8.

The main issue is: PCEF, the Policy and Charging Rule Function (PCRF), and AF all receive information bound to the same User Equipment (UE) but without being able to correlate between the piece of data visible for each entity. Concretely,

- PCEF is aware of the International Mobile Subscriber Identity (IMSI) and an internal IP address assigned to the UE.

- AF receives an external IP address and port as assigned by the NAT function.

- PCRF is not able to correlate between the external IP address/port assigned by the NAT (received from the AF) and the internal IP address and IMSI of the UE (received from the PCEF).

```
               +------+
               | PCRF |-----------------+
               +------+                 |
                  |                     |
   +----+      +------+   +-----+    +-----+
   | UE |------| PCEF |---| NAT |----|  AF |
   +----+      +------+   +-----+    +-----+
```

Figure 8: NAT Located between AF and PCEF

This scenario can be generalized as follows (Figure 9):

- Policy Enforcement Point (PEP) [RFC2753]

- Policy Decision Point (PDP) [RFC2753]

```
               +------+
               | PDP  |-----------------+
               +------+                 |
                  |                     |
   +----+      +------+   +-----+    +------+
   | UE |------| PEP  |---| NAT |----|Server|
   +----+      +------+   +-----+    +------+
```

Figure 9: NAT Located between PEP and the Server

Note that an issue is encountered to enforce per-UE policies when the NAT is located before the PEP function (see Figure 10):

```
                          +------+
                          | PDP  |------+
                          +------+      |
                             |          |
   +----+      +------+   +-----+    +------+
   | UE |------| NAT  |---| PEP |----|Server|
   +----+      +------+   +-----+    +------+
```

Figure 10: NAT Located before PEP

This scenario does not introduce privacy concerns since the identification of the host is local to a single administrative domain and is meant to help identify which policy to select for a UE.

9. Scenario 7: Emergency Calls

Voice Service Providers (VSPs) operating under certain jurisdictions are required to route emergency calls from their subscribers and have to include information about the caller’s location in signaling messages they send towards Public Safety Answering Points (PSAPs) [RFC6443] via an Emergency Service Routing Proxy (ESRP) [RFC6443]. This information is used both for the determination of the correct PSAP and to reveal the caller’s location to the selected PSAP.

In many countries, regulation bodies require that this information be provided by the network rather than the user equipment, in which case the VSP needs to retrieve this information (by reference or by value) from the access network where the caller is attached.

This requires the VSP call server receiving an emergency call request to identify the relevant access network and to query a Location Information Server (LIS) in this network using a suitable lookup key. In the simplest case, the source IP address of the IP packet carrying the call request is used both for identifying the access network (thanks to a reverse DNS query) and as a lookup key to query the LIS. Obviously, the user-id as known by the VSP (e.g., telephone number or email-formatted URI) can’t be used as it is not known by the access network.

The above mechanism is broken when there is a NAT between the user and the VSP and/or if the emergency call is established over a VPN tunnel (e.g., an employee remotely connected to a company Voice over IP (VoIP) server through a tunnel wishes to make an emergency call). In such cases, the source IP address received by the VSP call server will identify the NAT or the address assigned to the caller equipment by the VSP (i.e., the address inside the tunnel). This is similar to the CGN case in (Section 3) and overlay network case (Section 7) and applies irrespective of the IP versions used on both sides of the NAT and/or inside and outside the tunnel.

Therefore, the VSP needs to receive an additional piece of information that can be used to both identify the access network where the caller is attached and query the LIS for his/her location. This would require the NAT or the tunnel endpoint to insert this extra information in the call requests delivered to the VSP call servers. For example, this extra information could be a combination of the local IP address assigned by the access network to the caller’s equipment with some form of identification of this access network.

However, because it shall be possible to set up an emergency call regardless of the actual call control protocol used between the user and the VSP (e.g., SIP [RFC3261], Inter-Asterisk eXchange (IAX) [RFC5456], tunneled over HTTP, or proprietary protocol, possibly encrypted), this extra information has to be conveyed outside the call request, in the header of lower-layer protocols.

Privacy-related considerations discussed in [RFC6967] apply for this scenario.

10. Other Deployment Scenarios

This section lists deployment scenarios that are variants of scenarios described in previous sections.

10.1. Open WLAN or Provider WLAN

In the context of Provider WLAN, a dedicated Service Set Identifier (SSID) can be configured and advertised by the Residential Gateway (RG) for visiting terminals. These visiting terminals can be mobile terminals, PCs, etc.

Several deployment scenarios are envisaged:

1. Deploy a dedicated node in the service provider’s network that will be responsible for intercepting all the traffic issued from visiting terminals (see Figure 11). This node may be co-located with a CGN function if private IPv4 addresses are assigned to visiting terminals. Similar to the CGN case discussed in Section 3, remote servers may not be able to distinguish visiting hosts sharing the same IP address (see [RFC6269]).

2. Unlike the previous deployment scenario, IPv4 addresses are managed by the RG without requiring any additional NAT to be deployed in the service provider’s network for handling traffic issued from visiting terminals. Concretely, a visiting terminal is assigned with a private IPv4 address from the IPv4 address pool managed by the RG. Packets issued from a visiting terminal are translated using the public IP address assigned to the RG (see Figure 12). This deployment scenario induces the following identification concerns:

- The provider is not able to distinguish the traffic belonging to the visiting terminal from the traffic of the subscriber owning the RG. This is needed to identify which policies are to be enforced such as: accounting, Differentiated Services Code Point (DSCP) remarking, black list, etc.

- Similar to the CGN case Section 3, a misbehaving visiting terminal is likely to have some impact on the experienced service by the subscriber owning the RG (e.g., some of the issues are discussed in [RFC6269]).

```
   +-------------+
   |Local_HOST_1 |----+
   +-------------+    |
                      |     |
   +-------------+  +-----+ |  +-----------+
   |Local_HOST_2 |--| RG  |-|--|Border Node|
   +-------------+  +-----+ |  +----NAT----+
                       |    |
   +-------------+     |    |  Service Provider
   |Visiting Host|-----+
   +-------------+
```

Figure 11: NAT Enforced in a Service Provider’s Node

```
   +-------------+
   |Local_HOST_1 |----+
   +-------------+    |
                      |     |
   +-------------+  +-----+ |  +-----------+
   |Local_HOST_2 |--| RG  |-|--|Border Node|
   +-------------+  +-NAT-+ |  +-----------+
                       |    |
   +-------------+     |    |  Service Provider
   |Visiting Host|-----+
   +-------------+
```

Figure 12: NAT Located in the RG

This scenario does not introduce privacy concerns since the identification of the host is local to a single administrative domain and is meant to help identify which policy to select for a visiting UE.

10.2. Cellular Networks

Cellular operators allocate private IPv4 addresses to mobile terminals and deploy NAT44 function, generally co-located with firewalls, to access public IP services. The NAT function is located at the boundaries of the Public Land Mobile Network (PLMN). IPv6-only strategy, consisting in allocating IPv6 prefixes only to mobile terminals, is considered by various operators. A NAT64 function is also considered in order to preserve IPv4 service continuity for these customers.

These NAT44 and NAT64 functions bring some issues that are very similar to those mentioned in Figure 1 and Section 8. These issues are particularly encountered if policies are to be applied on the Gi interface.

> Note: 3GPP defines the Gi interface as the reference point between the Gateway GPRS Support Node (GGSN) and an external Packet Domain Network (PDN). This interface reference point is called SGi in 4G networks (i.e., between the PDN Gateway and an external PDN).

Because private IP addresses are assigned to the mobile terminals, there is no correlation between the internal IP address and the external address:port assigned by the NAT function, etc.

Privacy-related considerations discussed in [RFC6967] apply for this scenario.

10.3. Femtocells

This scenario can be seen as a combination of the scenarios described in Sections 8 and 10.1.

The reference architecture is shown in Figure 13.

A Femto Access Point (FAP) is defined as a home base station used to graft a local (femto) cell within a user’s home to a mobile network.

```
   +---------------------------+
   | +----+ +--------+  +----+ |   +-----------+  +-------------------+
   | | UE | | Stand- |<=|====|=|===|===========|==|=>+--+ +--+        |
   | +----+ | Alone  |  | RG | |   |           |  |  |  | |  | Mobile |
   |        |  FAP   |  +----+ |   |           |  |  |S | |F | Network|
   |        +--------+  (NAPT) |   | Broadband |  |  |e | |A |        |
   +---------------------------+   |   Fixed   |  |  |G |-|P | +-----+|
                                   |   (BBF)   |  |  |W | |G |-| Core||
   +---------------------------+   |  Network  |  |  |  | |W | | Ntwk||
   | +----+ +------------+     |   |           |  |  |  | |  | +-----+|
   | | UE | | Integrated |<====|===|===========|==|=>+--+ +--+        |
   | +----+ | FAP (NAPT) |     |   +-----------+  +-------------------+
   |        +------------+     |
   +---------------------------+
```

<=====>	IPsec Tunnel
CoreNtwk	Core Network
FAPGW	FAP Gateway
NAPT	Network Address Port Translator
SeGW	Security Gateway

Figure 13: Femtocell Reference Architecture

UE is connected to the FAP at the RG, which is routed back to the 3GPP Evolved Packet Core (EPC). It is assumed that each UE is assigned an IPv4 address by the mobile network. A mobile operator’s FAP leverages the IPsec Internet Key Exchange Protocol Version 2 (IKEv2) to interconnect FAP with the SeGW over the Broadband Fixed (BBF) network. Both the FAP and the SeGW are managed by the mobile operator, which may be a different operator for the BBF network.

An investigated scenario is when the mobile operator passes on its mobile subscriber’s policies to the BBF to support traffic policy control. But most of today’s broadband fixed networks are relying on the private IPv4 addressing plan (+NAPT) to support its attached devices, including the mobile operator’s FAP. In this scenario, the mobile network needs to:

- determine the FAP’s public IPv4 address to identify the location of the FAP to ensure its legitimacy to operate on the license spectrum for a given mobile operator prior to the FAP being ready to serve its mobile devices.

- determine the FAP’s public IPv4 address together with the translated port number of the UDP header of the encapsulated IPsec tunnel for identifying the UE’s traffic at the fixed broadband network.

- determine the corresponding FAP’s public IPv4 address associated with the UE’s inner IPv4 address that is assigned by the mobile network to identify the mobile UE, which allows the PCRF to retrieve the special UE’s policy (e.g., QoS) to be passed onto the Broadband Policy Control Function (BPCF) at the BBF network.

SeGW would have the complete knowledge of such mapping, but the reasons for being unable to use SeGW for this purpose are explained in Section 2 of [IKEv2-CP-EXT].

This scenario involves PCRF/BPCF, but it is valid in other deployment scenarios making use of Authentication, Authorization, and Accounting (AAA) servers.

The issue of correlating the internal IP address and the public IP address is valid even if there is no NAT in the path.

This scenario does not introduce privacy concerns since the identification of the host is local to a single administrative domain and is meant to help identify which policy to select for a UE.

10.4. Traffic Detection Function (TDF)

Operators expect that the traffic subject to the packet inspection is routed via the Traffic Detection Function (TDF) as per the requirement specified in [TS29.212]; otherwise, the traffic may bypass the TDF. This assumption only holds if it is possible to identify individual UEs behind the Basic NAT or NAPT invoked in the RG connected to the fixed broadband network, as shown in Figure 14. As a result, additional mechanisms are needed to enable this requirement.

```
                                                              +--------+
                                                              |        |
                                                      +-------+  PCRF  |
                                                      |       |        |
                                                      |       +--------+
 +--------+      +--------+       +--------+     +----+----+
 |        |      |        |       |        +-----+         |
 |  ------------------------------------------------------------------
 |        |      |        |       |        |     |  TDF    |    /      \
 |  ****************************************************************** |
 +--------+      +--------+       +--------+     +----+----+   |       |
 |        |      |       +-------+        |         |         |Service|
 |        |      |        |       |        |         |          \      /
 |        |      |        |       |        |         |        +--------+
 |        |      |        |       |        |        +--------+  PDN   |
 |  >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> |
 |  UE    |      |   RG   |       | BNG    +------------------+ Gateway|
 +--------+      +--------+       +--------+                  +--------+

 Legend:
 ---------   3GPP UE User-Plane Traffic Offloaded subject to packet
             inspection

 *********   3GPP UE User-Plane Traffic Offloaded not subject to packet
             inspection

 >>>>>>>>>   3GPP UE User-Plane Traffic Home Routed

       BNG   Broadband Network Gateway
```

Figure 14: UE’s Traffic Routed with TDF

This scenario does not introduce privacy concerns since the identification of the host is local to a single administrative domain and is meant to help identify which policy to select for a UE.

10.5. Fixed and Mobile Network Convergence

In the Policy for Convergence of Fixed Mobile Convergence (FMC) scenario, the fixed broadband network must partner with the mobile network to acquire the policies for the terminals or hosts attaching to the fixed broadband network, shown in Figure 15, so that host-specific QoS and accounting policies can be applied.

A UE is connected to the RG, which is routed back to the mobile network. The mobile operator’s PCRF needs to maintain the interconnect with the BPCF in the BBF network for PCC (Section 8). The hosts (i.e., UEs) attaching to a fixed broadband network with a

Basic NAT or NAPT deployed should be identified. Based on the UE identification, the BPCF can acquire the associated policy rules of the identified UE from the PCRF in the mobile network so that it can enforce policy rules in the fixed broadband network. Note, this scenario assumes private IPv4 addresses are assigned in the fixed broadband network. Requirements similar to those in Section 10.3 are raised in this scenario.

```
                +------------------------------+   +-------------+
                |                              |   |             |
                |                   +------+   |   | +------+    |
                |                   | BPCF +---+---+-+ PCRF |    |
                |                   +--+---+   |   | +---+--+    |
     +-------+  |                      |       |   |     |       |
     |HOST_1 | Private IP1          +--+---+   |   | +---+--+    |
     +-------+  | +----+            |      |   |   | |      |    |
                | | RG |            |      |   |   | |      |    |
                | |with+-------------+ BNG  +--------+ PGW  |    |
     +-------+  | | NAT|            |      |   |   | |      |    |
     |HOST_2 |  | +----+            |      |   |   | |      |    |
     +-------+ Private IP2          +------+   |   | +------+    |
                |                              |   |             |
                |                              |   |             |
                |                       Fixed  |   | Mobile      |
                |                   Broadband  |   | Network     |
                |                     Network  |   |             |
                |                              |   |             |
                +------------------------------+   +-------------+
```

Figure 15: Reference Architecture for Policy for Convergence in Fixed and Mobile Network Convergence (1)

In an IPv6 network, similar issues exist when the IPv6 prefix is shared between multiple UEs attaching to the RG (see Figure 16). The case applies when RG is assigned a single prefix, the home network prefix, e.g., using DHCPv6 Prefix Delegation [RFC3633] with the edge router, and BNG acts as the Delegating Router (DR). RG uses the home network prefix in the address configuration using stateful (DHCPv6) or stateless address autoconfiguration (SLAAC) techniques.

```
                +------------------------------+   +-------------+
                |                              |   |             |
                |                              |   | +------+    |
                |                      +-------------+ PCRF |    |
                |                      |       |   | +---+--+    |
     +-------+  |                      |       |   |     |       |
     |HOST_1 |--+                   +--+---+   |   | +---+--+    |
     +-------+  | +----+            |      |   |   | |      |    |
                | | RG |            |      |   |   | |      |    |
                | |    +------------+ BNG  +---------+ PGW  |    |
     +-------+  | |    |            |      |   |   | |      |    |
     |HOST_2 |--+ +----+            |      |   |   | |      |    |
     +-------+  |                   +------+   |   | +------+    |
                |                              |   |             |
                |                              |   |             |
                |                       Fixed  |   | Mobile      |
                |                   Broadband  |   | Network     |
                |                     Network  |   |             |
                |                              |   |             |
                +------------------------------+   +-------------+
```

Figure 16: Reference Architecture for Policy for Convergence in Fixed and Mobile Network Convergence (2)

BNG acting as PCEF initiates an IP Connectivity Access Network (IP-CAN) session with the policy server, a.k.a. Policy and Charging Rules Function (PCRF), to receive the Quality of Service (QoS) parameters and charging rules. BNG provides the PCRF with the IPv6 prefix assigned to the host; in this case, it’s the home network prefix and an ID that has to be equal to the RG-specific home network line ID.

HOST_1 in Figure 16 creates a 128-bit IPv6 address using this prefix and adding its interface ID. Having completed the address configuration, the host can start communication with a remote host over the Internet. However, no specific IP-CAN session can be assigned to HOST_1, and consequently the QoS and accounting performed will be based on RG subscription.

Another host, e.g., HOST_2, attaches to the RG and also establishes an IPv6 address using the home network prefix. The edge router, or BNG, is not involved with this or any other such address assignments.

This leads to the case where no specific IP-CAN session/sub-session can be assigned to the hosts, HOST_1, HOST_2, etc., and consequently the QoS and accounting performed can only be based on RG subscription and is not host specific. Therefore, IPv6 prefix sharing in the Policy for Convergence scenario leads to similar issues as the address sharing as explained in the previous scenarios in this document.

11. Synthesis

The following table shows whether each scenario is valid for IPv4/IPv6 and if it is within one single administrative domain or spans multiple domains. The table also identifies the root cause of the identification issues.

The IPv6 column indicates for each scenario whether IPv6 is supported at the client's side and/or server's side.

Scenario	IPv4	IPv6		Single Domain	Root Cause	
		Client	Server		Address sharing	Tunneling
CGN	Yes	Yes(1)	No	No	Yes	No
A+P	Yes	No	No	No	Yes	No
Application Proxy	Yes	Yes	Yes	No	Yes	No
Distributed Proxy	Yes	Yes	Yes	Yes/No	Yes	No
Overlay Networks	Yes	Yes(2)	Yes(2)	No	Yes	No
PCC	Yes	Yes(1)	No	Yes	Yes	No
Emergency Calls	Yes	Yes	Yes	No	Yes	No
Provider WLAN	Yes	No	No	Yes	Yes	No
Cellular Networks	Yes	Yes(1)	No	Yes	Yes	No
Femtocells	Yes	No	No	No	Yes	Yes
TDF	Yes	Yes	No	Yes	Yes	No
FMC	Yes	Yes(1)	No	No	Yes	No

Notes:
(1) For example, NAT64
(2) This scenario is a combination of CGN and application proxies

Table 1: Synthesis

12. Privacy Considerations

Privacy-related considerations that apply to means to reveal a host identifier are discussed in [RFC6967]. This document does not introduce additional privacy issues than those discussed in [RFC6967].

None of the scenarios inventoried in this document aim at revealing a customer identifier, account identifier, profile identifier, etc.

Particularly, none of these scenarios are endorsing the functionality provided by the following proprietary headers (but not limited to) that are known to be used to leak subscription-related information: HTTP_MSISDN, HTTP_X_MSISDN, HTTP_X_UP_CALLING_LINE_ID, HTTP_X_NOKIA_MSISDN, HTTP_X_HTS_CLID, HTTP_X_MSP_CLID, HTTP_X_NX_CLID, HTTP__RAPMIN, HTTP_X_WAP_MSISDN, HTTP_COOKIE, HTTP_X_UP_LSID, HTTP_X_H3G_MSISDN, HTTP_X_JINNY_CID, HTTP_X_NETWORK_INFO, etc.

13. Security Considerations

This document does not define an architecture nor a protocol; as such it does not raise any security concerns. Security considerations that are related to the host identifier are discussed in [RFC6967].

14. Informative References

[BCP160] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, July 2011.

[BCP188] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014.

[EFFOpenWireless] EFF, "Open Wireless", 2014, <https://www.eff.org/issues/open-wireless>.

[IEEE101109] Salah, K., Calero, J., Zeadally, S., Almulla, S., and M. ZAaabi, "Using Cloud Computing to Implement a Security Overlay Network", IEEE Computer Society Digital Library, IEEE Security & Privacy, Vol. 11, Issue 1, pp. 44-53, DOI 10.1109/MSP.2012.88, Jan-Feb 2013.

[IEEE1344002] Byers, J., Considine, J., Mitzenmacher, M., and S. Rost, "Informed content delivery across adaptive overlay networks", IEEE/ACM Transactions on Networking, Vol. 12, Issue 5, pp. 767-780, DOI 10.1109/TNET.2004.836103, October 2004.

[IKEv2-CP-EXT] So, T., "IKEv2 Configuration Payload Extension for Private IPv4 Support for Fixed Mobile Convergence", Work in Progress, draft-so-ipsecme-ikev2-cpext-02, June 2012.

[OVERLAYPATH]
Williams, B., "Overlay Path Option for IP and TCP", Work in Progress, draft-williams-overlaypath-ip-tcp-rfc-04, June 2013.

[RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, DOI 10.17487/RFC2753, January 2000, <http://www.rfc-editor.org/info/rfc2753>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, DOI 10.17487/RFC3633, December 2003, <http://www.rfc-editor.org/info/rfc3633>.

[RFC4984] Meyer, D., Ed., Zhang, L., Ed., and K. Fall, Ed., "Report from the IAB Workshop on Routing and Addressing", RFC 4984, DOI 10.17487/RFC4984, September 2007, <http://www.rfc-editor.org/info/rfc4984>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC5456] Spencer, M., Capouch, B., Guy, E., Ed., Miller, F., and K. Shumard, "IAX: Inter-Asterisk eXchange Version 2", RFC 5456, DOI 10.17487/RFC5456, February 2010, <http://www.rfc-editor.org/info/rfc5456>.

[RFC5694] Camarillo, G., Ed. and IAB, "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, DOI 10.17487/RFC5694, November 2009, <http://www.rfc-editor.org/info/rfc5694>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <http://www.rfc-editor.org/info/rfc6146>.

[RFC6179] Templin, F., Ed., "The Internet Routing Overlay Network (IRON)", RFC 6179, DOI 10.17487/RFC6179, March 2011, <http://www.rfc-editor.org/info/rfc6179>.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011, <http://www.rfc-editor.org/info/rfc6265>.

[RFC6269] Ford, M., Ed., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, DOI 10.17487/RFC6269, June 2011, <http://www.rfc-editor.org/info/rfc6269>.

[RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, DOI 10.17487/RFC6296, June 2011, <http://www.rfc-editor.org/info/rfc6296>.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

[RFC6346] Bush, R., Ed., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", RFC 6346, DOI 10.17487/RFC6346, August 2011, <http://www.rfc-editor.org/info/rfc6346>.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, DOI 10.17487/RFC6443, December 2011, <http://www.rfc-editor.org/info/rfc6443>.

[RFC6888] Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, DOI 10.17487/RFC6888, April 2013, <http://www.rfc-editor.org/info/rfc6888>.

[RFC6967] Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Potential Solutions for Revealing a Host Identifier (HOST_ID) in Shared Address Deployments", RFC 6967, DOI 10.17487/RFC6967, June 2013, <http://www.rfc-editor.org/info/rfc6967>.

[RFC7239] Petersson, A. and M. Nilsson, "Forwarded HTTP Extension", RFC 7239, DOI 10.17487/RFC7239, June 2014, <http://www.rfc-editor.org/info/rfc7239>.

[RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596, July 2015, <http://www.rfc-editor.org/info/rfc7596>.

[RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <http://www.rfc-editor.org/info/rfc7597>.

[STATELESS-NAT44] Tsou, T., Liu, W., Perreault, S., Penno, R., and M. Chen, "Stateless IPv4 Network Address Translation", Work in Progress, draft-tsou-stateless-nat44-02, October 2012.

[TS23.203] 3GPP, "Policy and charging control architecture (Release 11)", 3GPP TS23.203, September 2012.

[TS29.212] 3GPP, "Policy and Charging Control (PCC); Reference points (Release 11)", 3GPP TS29.212, December 2013.

Acknowledgments

Many thanks to F. Klamm, D. Wing, D. von Hugo, G. Li, D. Liu, and Y. Lee for their review.

J. Touch, S. Farrel, and S. Moonesamy provided useful comments in the intarea mailing list.

Figure 8 and part of the text in Section 10.3 were inspired by [IKEv2-CP-EXT].

Contributors

Many thanks to the following people for contributing text and comments to the document:

- David Binet
- Sophie Durel
- Li Xue
- Richard Stewart Wheeldon

Authors' Addresses

Mohamed Boucadair (editor)
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Bruno Chatras
Orange
Paris
France

Email: bruno.chatras@orange.com

Tirumaleswar Reddy
Cisco Systems
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tireddy@cisco.com

Brandon Williams
Akamai, Inc.
Cambridge MA
United States

Email: brandon.williams@akamai.com

Behcet Sarikaya
Huawei
5340 Legacy Dr. Building 3,
Plano, TX 75024
United States

Email: sarikaya@ieee.org