INTAREA Working Group
Internet-Draft
Intended status: Informational
Expires: August 18, 2014

M. Boucadair, Ed.
D. Binet
S. Durel
B. Chatras
France Telecom
T. Reddy
Cisco
B. Williams
Akamai, Inc.
L. Xue
Huawei

February 14, 2014

# Host Identification: Use Cases
# draft-boucadair-intarea-host-identifier-scenarios-04

Abstract

This document describes a set of scenarios in which host identification is required.

Status of This Memo

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

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

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

This Internet-Draft will expire on August 18, 2014.

Table of Contents



## 1. Introduction

The ultimate goal of this document is to enumerate scenarios which encounter the issue of uniquely identifying a host among those sharing the same IP address. Examples of encountered issues are:

- Blacklist a misbehaving host without impacting all hosts sharing the same IP address.
- Enforce a per-subscriber/per-UE policy (e.g., limit access to the service based on some counters such as volume-based service offering); enforcing the policy will have impact on all hosts sharing the same IP address.
- If invoking a service has failed (e.g., wrong login/password), all hosts sharing the same IP address may not be able to access that service.
- Need to correlate between the internal address:port and external address:port to generate and therefore to enforce policies.

It is out of scope of this document to list all the encountered issues as this is already covered in [RFC6269].

The generic concept of host identifier, denoted as HOST_ID, is defined in [I-D.ietf-intarea-nat-reveal-analysis].

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

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

The following use cases are identified so far:

(1) Section 3.1: Carrier Grade NAT (CGN)
(2) Section 3.2: A+P (e.g., MAP )
(3) Section 3.3: Application Proxies
(4) Section 3.4: Provider Wi-Fi
(5) Section 3.5: Policy and Charging Architectures
(6) Section 3.6: Cellular Networks
(7) Section 3.7: Femtocells
(8) Section 3.8: Overlay Networks (e.g., CDNs)
(9) Section 3.9: Emergency Calls
(10) Section 3.10: Traffic Detection Function
(11) Section 3.11: Fixed and Mobile Network Convergence

## 2. Scope

It is out of scope of this document to argue in favor or against the use cases listed in the following sub-sections. The goal is to identify scenarios the authors are aware of and which share the same issue of host identification.

This document does not include any solution-specific discussion. This document can be used as a tool to design solution(s) mitigating the encountered issues. Having a generic solution which would solve the issues encountered in these use cases is preferred over designing a solution for each use case. Describing the use case allows to identify what is common between the use cases and then would help during the solution design phase.

The first version of the document does not elaborate whether explicit authentication is enabled or not.

## 3. Use Cases

### 3.1. Use Case 1: CGN

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

1. NAT44 ( [I-D.ietf-behave-lsn-requirements], [I-D.tsou-stateless-nat44])

2. DS-Lite NAT44 [RFC6333]

3. NAT64 [RFC6146]

4. NPTv6 [RFC6296]

As discussed in [I-D.ietf-intarea-nat-reveal-analysis], remote servers are not able to distinguish between hosts sharing the same IP address (Figure 1).

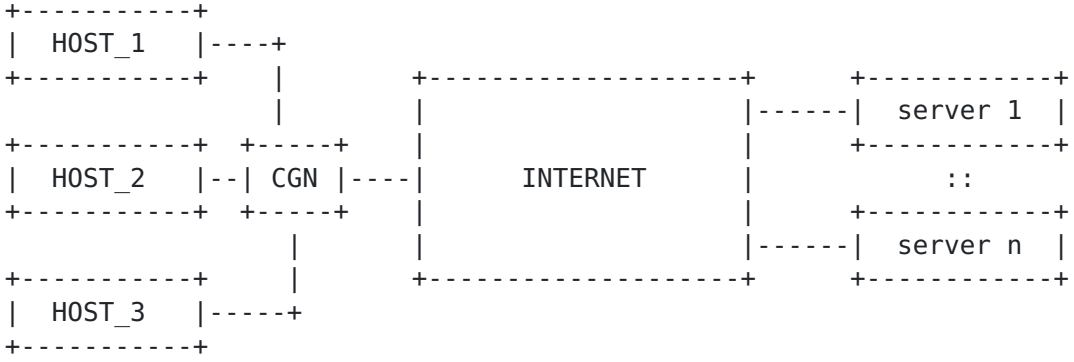



Figure 1: CGN: Architecture Example

### 3.2. Use Case 2: A+P

A+P [RFC6346][I-D.ietf-softwire-map][I-D.cui-softwire-b4-translated-ds-lite] denotes a flavor of address sharing solutions which does not require any additional NAT function 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 PRR (Port Range Router, [RFC6346]) is needed (Figure 2).

Similar to the CGN case, the same issue to identify hosts sharing the same IP address is encountered by remote servers.

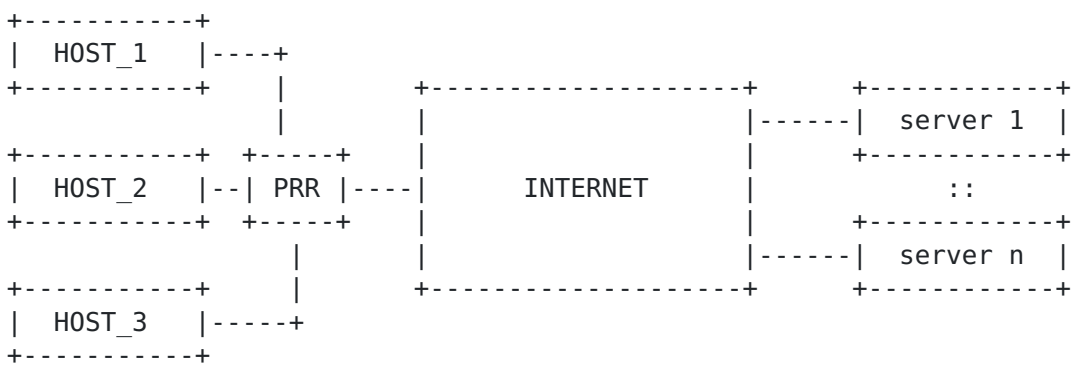



Figure 2: A+P: Architecture Example

## 3.3. Use Case 3: Application Proxies

This scenario is similar to the CGN scenario. 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.

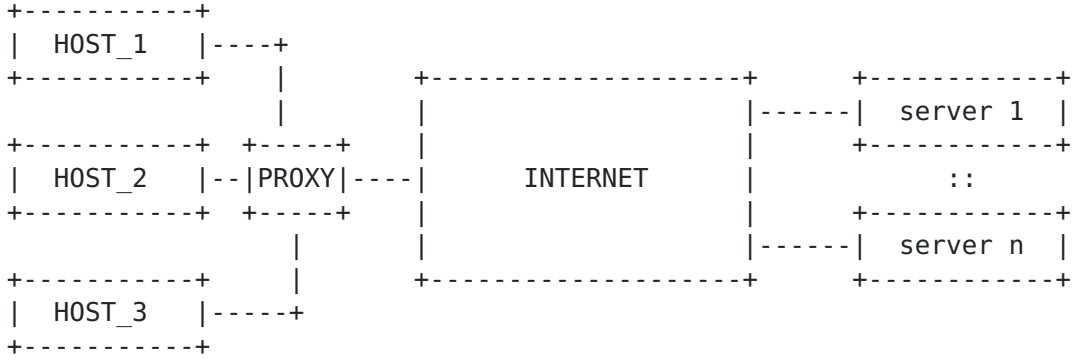



Figure 3: Proxy: Overview

## 3.4. Use Case 4: Open Wi-Fi or Provider Wi-Fi

In the context of Provider Wi-Fi, a dedicated SSID can be configured and advertised by the RG (Residential Gateway) 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 which will be responsible to intercept all the traffic issued from visiting terminals (see Figure 4). 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 3.1, 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 form a visiting terminal are translated using the public IP address assigned to the RG (see Figure 5). 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 apply some policies such as: accounting, DSCP remarking, black list, etc.

   * Similar to the CGN case Section 3.1, 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]).

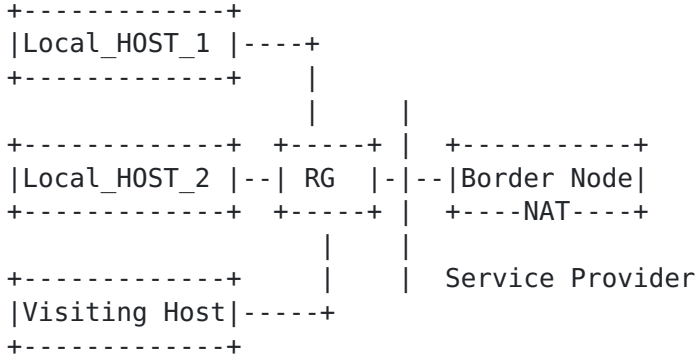



Figure 4: NAT enforced in a Service Provider's Node

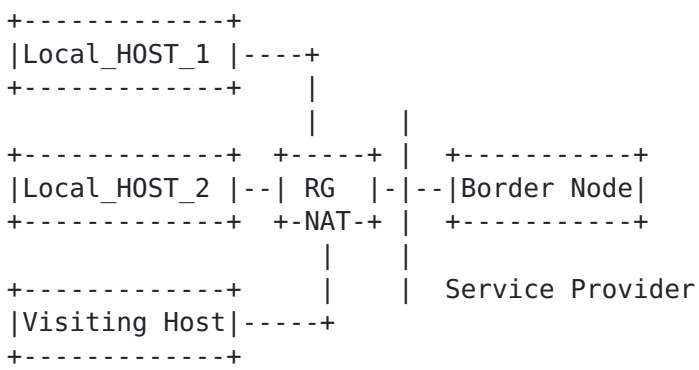



Figure 5: NAT located in the RG

## 3.5. Use Case 5: Policy and Charging Control Architecture

This issue is related to the framework defined in [TS23.203] when a NAT is located between the PCEF (Policy and Charging Enforcement Function) and the AF (Application Function) as shown in Figure 6.

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

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

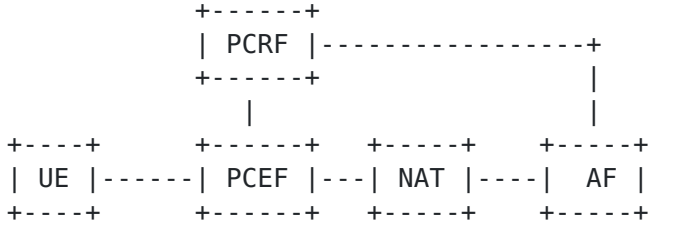



Figure 6: NAT located between AF and PCEF

This scenario can be generalized as follows (Figure 7):

- Policy Enforcement Point (PEP, [RFC2753])

o Policy Decision Point (PDP, [RFC2753])

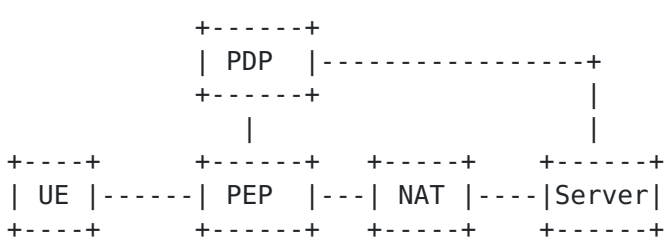



Figure 7: NAT located between PEP and Server

A similar issue is encountered when the NAT is located before the PEP function (see Figure 8):

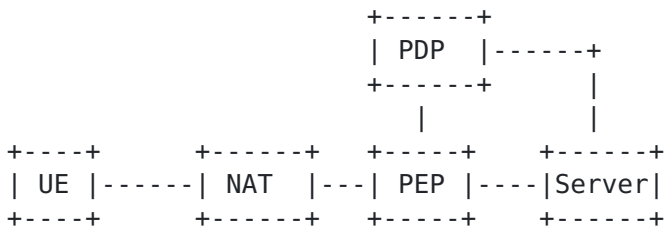



Figure 8: NAT located before PEP

## 3.6. Use Case 6: Cellular Networks

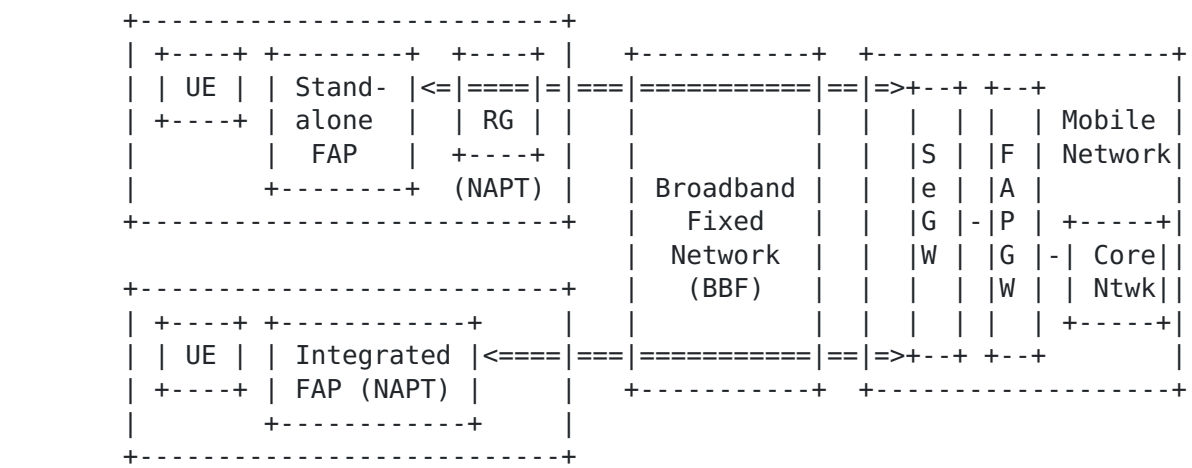
Cellular operators allocate private IPv4 addresses to mobile terminals and deploy NAT44 function, generally co-located with firewalls, to access to public IP services. The NAT function is located at the boundaries of the PLMN (Public Land Mobile Network). IPv6-only strategy, consisting in allocating 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 very similar to those mentioned in Figure 1 and Section 3.5. This issue is particularly encountered if policies are to be applied on the Gi interface: a private IP address is 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.

## 3.7. Use Case 7: Femtocells

This issue is discussed in [I-D.so-ipsecme-ikev2-cpext]. This use case can be seen as a combination of the use cases described in Section 3.4 and Section 3.5.

The reference architecture, originally provided in [I-D.so-ipsecme-ikev2-cpext], is shown in Figure 8.




<=====> IPsec tunnel
CoreNtwk Core Network
FAPGW FAP Gateway
SeGW Security Gateway

Figure 9: Femtocell: Overall Architecture

UE is connected to the FAP at the residential gateway (RG), routed back to 3GPP Evolved Packet Core (EPC). UE is assigned IPv4 address by the Mobile Network. Mobile operator's FAP leverages the IPSec IKEv2 to interconnect FAP with the SeGW over the 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 the mobile operator to pass 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 be ready to serve its mobile devices.

- determine the FAP's pubic 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.

- o determine the corresponding FAP's public IPv4 address associated with the UE's inner-IPv4 address which is assigned by the mobile network to identify the mobile UE to allow 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.

SecGW would have the complete knowledge of such mapping, but the reasons for unable to use SecGW for this purpose is explained in "Problem Statements" (section 2 of [I-D.so-ipsecme-ikev2-cpext]).

This use case makes use of PCRF/BPCF but it is valid in other deployment scenarios making use of 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.

## 3.8. Use Case 8: 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 10). 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.

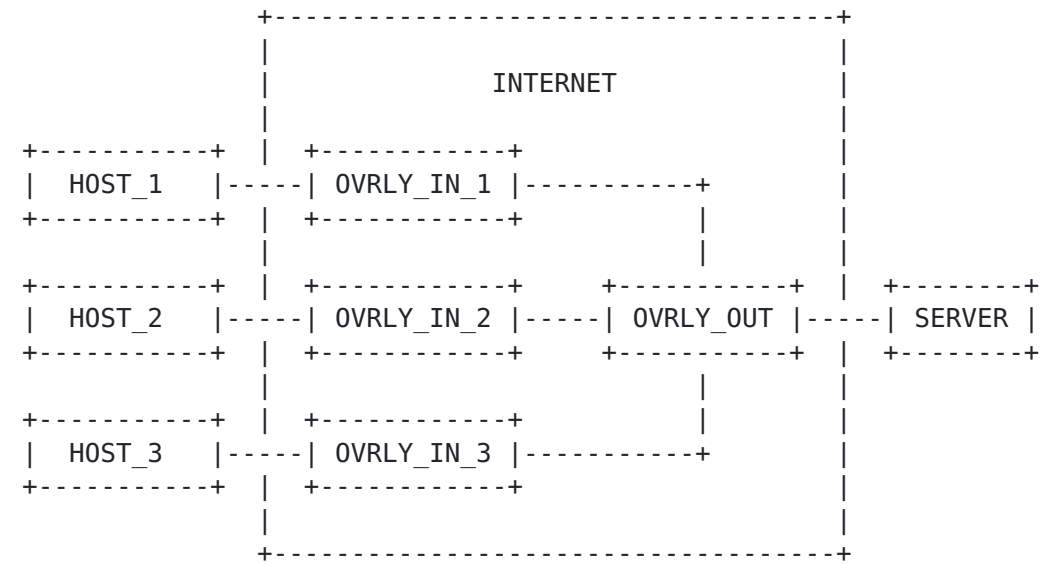



Figure 10: Overlay Network

Data transport using an overlay network requires network address translation for both the source and destination addresses in such a

way that the public IP addresses of the true endpoint machines involved in data transport are invisible to each other (see Figure 11). In other words, the true sender and receiver use two completely different pairs of source and destination addresses to identify the connection on the sending and receiving networks.

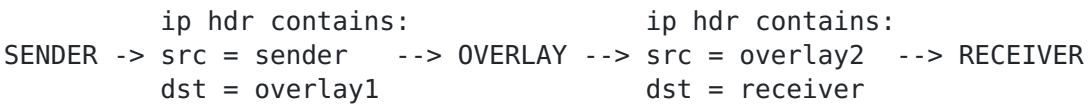



Figure 11: NAT operations in an Overlay Network

This scenario is similar to the CGN (Section 3.1) and proxy (Section 3.3) scenarios. 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.

More details about this use case are provided in [I-D.williams-overlaypath-ip-tcp-rfc].

## 3.9. Use Case 9: 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 PSAPs (Public Safety Answering Points, [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 look-up 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 look-up 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 or if the emergency call is established over a VPN tunnel (e.g., an employee remotely connected to a company 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 identity the NAT or the address assigned to the caller equipment by the VSP (i.e., the address inside 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 setup an emergency call regardless of the actual call control protocol used between the user and the VSP (e.g., SIP [RFC3261], 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 layers protocols.

## 3.10. Use Case 10: Traffic Detection Function

Operators expect that the traffic subject to the packet inspection is routed via the Traffic Detection Function (TDF) function as 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 NA(P)T which may be deployed into the RG in fixed broadband network, shown in Figure 12. As a result, additional mechanisms are needed to enable this requirement.

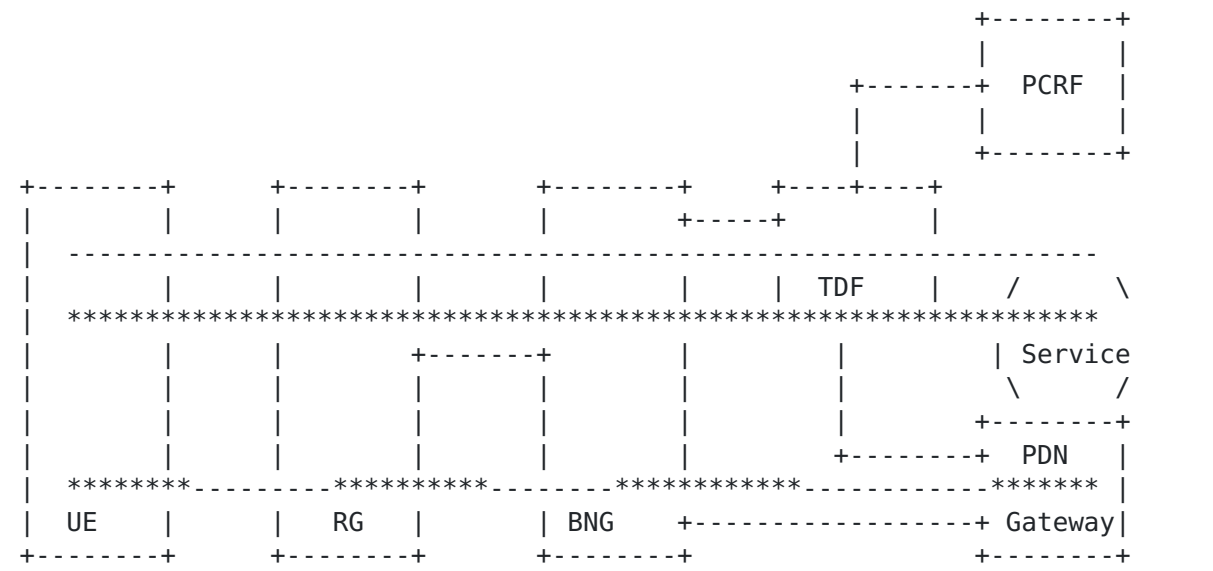



Figure 12: UE's Traffic Routed with TDF

## 3.11. Use Case 11: Fixed and Mobile Network Convergence

In the Fixed and Mobile network convergence (FMC) scenario, the fixed broadband network must partner with the mobile network to perform authorisation, authentication, and accounting (AAA) and acquire the policies for the mobile terminals attaching to the fixed broadband network, shown in Figure 13.

A UE is connected to the RG, routed back to the mobile network. The mobile operator's PCRF needs to maintain the interconnect with the Broadband Policy Control Function (BPCF) in the BBF network for PCC (Section 3.5). The hosts (i.e. UEs) attaching to fixed broadband network with a NA(P)T deployed should be identified. Based on the UE identification, the BPCF to deploy policy rules in the fixed broadband network can acquire the associated policy rules of the identified UE from the PCRF in the mobile network. But in the fixed broadband network, private IPv4 address is supported. The similar requirements are raised in this use case as Figure 9.

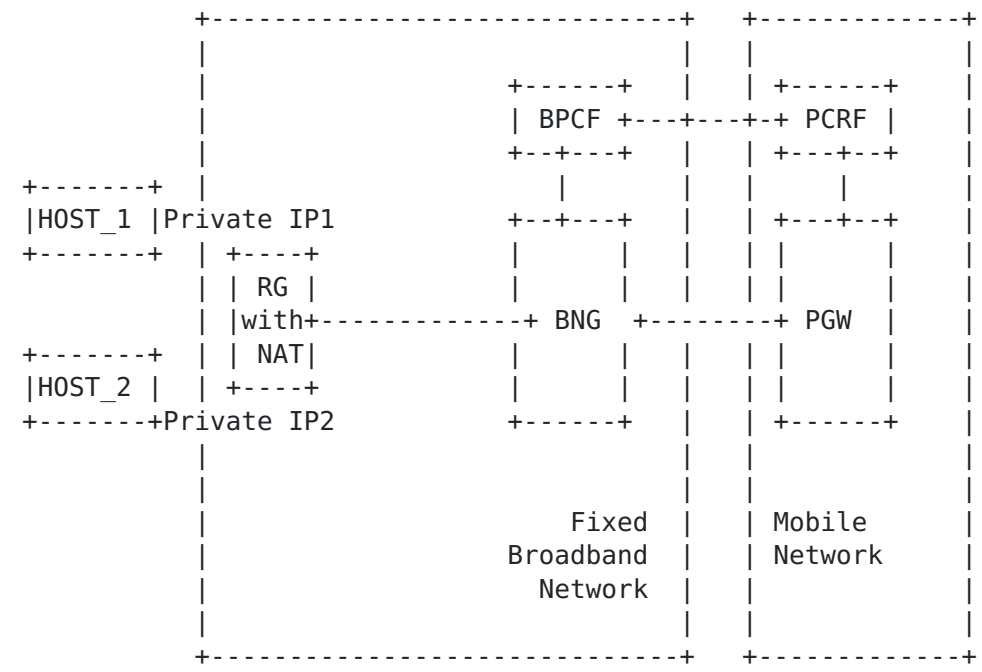



Figure 13: Fixed and Mobile Network Convergence

In IPv6 network, the similar issues exists when the IPv6 prefix is sharing between multiple UEs attaching to the RG. More details about the IPv6 prefix sharing issues are provided in[I-D.sarikaya-fmc-prefix-sharing-usecase].

## 4. Discussion

This section is to be completed.

### 4.1. HOST_ID Requirements

Below is listed as set of requirements to be used to characterize each use case (discussed in Section 3):

REQ#1: HOST_ID MUST be set by a trusted device. Receiver using HOST_ID MUST be able to validate that HOST_ID is set by a trusted device. Receiver MUST detect HOST_ID set by rogue devices and discard HOST_ID (i.e. not use HOST_ID for policy enforcement).

REQ#2: Trusted Device that generates HOST_ID MUST strip HOST_ID received from the host or HOST_ID set by any other downstream devices.

REQ#3: Receiver that enforces policy based on HOST_ID MUST strip HOST_ID before sending it upstream

REQ#4: Host SHOULD be permitted to set HOST_ID

REQ#5: HOST_ID MUST be provided in all the IP packets

REQ#6: HOST_ID MUST be provided in-line (i.e. Multiplexed) with the transport protocol

REQ#7: HOST_ID MUST be provided using out-of-band mechanism

REQ#8: HOST_ID MUST be provided either using in-line or out-of-band mechanism

REQ#9: HOST_ID MUST be encrypted so that other devices cannot glean the HOST_ID information, that could result in identity leakage.

REQ#10: HOST_ID MUST be conveyed for consumption within a single administrative domain.

REQ#11: HOST_ID MUST be conveyed across multiple administrative domain. In other words, the producer and consumer of HOST_ID are in different administrative domains.

REQ#12: Connection-oriented protocols (e.g., TCP or SCTP) MUST convey HOST_ID.

REQ#13: Connection-less protocols (e.g., UDP) MUST convey HOST_ID.

REQ#14: The entire IPv6/IPv4 address MUST be conveyed in the HOST_ID

REQ#15: 16-bit value representing a host hint is sufficient to be conveyed in the HOST_ID

REQ#16: HOST_ID propagation MUST be supported for IPv4-only.

REQ#17: HOST_ID propagation MUST be supported for IPv4 and IPv6.

REQ#18: Receiver MUST use HOST_ID to enforce policies like QoS.

REQ#19: Receiver uses HOST_ID only for Accounting and debugging purposes.

REQ#20: Receiver MUST use HOST_ID to achieve specific traffic treatment like TDF.

REQ#21: HOST_ID MUST be recongnized by different operators.

Once this list is stabilized, each use case will be checked against these requirements.

## 4.2. Synthesis

The following table shows whether each use case is valid for IPv4/ IPv6 and if it is to be applied within one single administrative domain or not. This table will be completed.

| Use Case | IPv4 | IPv6 | | Single Administrative Domain |
|---|---|---|---|---|
| | | Client | Server | |
| CGN | Yes | Yes(1) | No | No |
| A+P | Yes | No | No | No |
| Application Proxy | Yes | Yes(2) | Yes(2) | No |
| Provider Wi-Fi | Yes | No | No | Yes |
| PCC | Yes | Yes(1) | No | Yes |
| Femtocells | Yes | No | No | No |
| Cellular Networks | Yes | Yes(1) | No | Yes |
| Overlay Networks | Yes | Yes(3) | Yes(3) | No |
| Emergency Calls | Yes | Yes | Yes | No |
| TDF | Yes | Yes | No | Yes |
| FMC | Yes | Yes(1) | No | No |

Notes:
(1) e.g., NAT64
(2) A proxy can use IPv6 for the communication leg with the server or the application client.
(3) This use case is a combination of CGN and Application Proxies.

## 5. Security Considerations

This document does not define an architecture nor a protocol; as such it does not raise any security concern.

## 6. IANA Considerations

This document does not require any action from IANA.

## 7. Acknowledgments

Many thanks to F. Klamm for the review.

Figure 8 and part of the text in Section 3.7 are inspired from [I-D.so-ipsecme-ikev2-cpext].

## 8. Informative References

[I-D.cui-softwire-b4-translated-ds-lite]
Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture", draft-cui-softwire-b4-translated-ds-lite-11 (work in progress), February 2013.

[I-D.ietf-behave-lsn-requirements]
Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", draft-ietf-behave-lsn-requirements-10 (work in progress), December 2012.

[I-D.ietf-intarea-nat-reveal-analysis]
Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Solution Candidates to Reveal a Host Identifier (HOST_ID) in Shared Address Deployments", draft-ietf-intarea-nat-reveal-analysis-10 (work in progress), April 2013.

[I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, "Mapping of Address and Port with Encapsulation (MAP)", draft-ietf-softwire-map-10 (work in progress), January 2014.

[I-D.sarikaya-fmc-prefix-sharing-usecase]
Sarikaya, B., Spini, M., and D. DH, "IPv6 Prefix Sharing Problem Use Case", draft-sarikaya-fmc-prefix-sharing-usecase-01 (work in progress), February 2013.

[I-D.so-ipsecme-ikev2-cpext]
So, T., "IKEv2 Configuration Payload Extension for Private IPv4 Support for Fixed Mobile Convergence", draft-so-ipsecme-ikev2-cpext-02 (work in progress), June 2012.

[I-D.tsou-stateless-nat44]
Tsou, T., Liu, W., Perreault, S., Penno, R., and M. Chen, "Stateless IPv4 Network Address Translation", draft-tsou-stateless-nat44-02 (work in progress), October 2012.

[I-D.williams-overlaypath-ip-tcp-rfc]
Williams, B., "Overlay Path Option for IP and TCP", draft-williams-overlaypath-ip-tcp-rfc-04 (work in progress), June 2013.

[RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, January 2000.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC5456] Spencer, M., Capouch, B., Guy, E., Miller, F., and K. Shumard, "IAX: Inter-Asterisk eXchange Version 2", RFC 5456, February 2010.

[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.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

[RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

[RFC6346] Bush, R., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", RFC 6346, August 2011.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

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

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

Authors' Addresses

Mohamed Boucadair (editor)
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

David Binet
France Telecom
Rennes
France

Email: david.binet@orange.com

Sophie Durel
France Telecom
Rennes
France

Email: sophie.durel@orange.com

Bruno Chatras
France Telecom
Paris
France

Email: bruno.chatras@orange.com

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

Email: tireddy@cisco.com

Brandon Williams
Akamai, Inc.
Cambridge MA
USA

Email: brandon.williams@akamai.com

Li Xue
Huawei
Beijing
China

Email: xueli@huawei.com