

INTAREA Working Group
Internet-Draft
Intended status: Informational
Expires: April 14, 2013

M. Boucadair
D. Binet
S. Durel
France Telecom
October 11, 2012

HOST_ID: Use Cases
draft-boucadair-intarea-host-identifier-scenarios-00

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 April 14, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Scope	3
3.	Use Case 1: CGN	3
4.	Use Case 2: A+P	4
5.	Use Case 3: Application Proxies	5
6.	Use Case 4: Open Wi-Fi or Provider Wi-Fi	5
7.	Use Case 5: Policy and Charging Control Architecture	7
8.	Use Case 6: Cellular Networks	8
9.	Security Considerations	8
10.	IANA Considerations	8
11.	Informative References	8
	Authors' Addresses	9

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:

- o Blacklist a misbehaving host without impacting all hosts sharing the same IP address.
- o If a remote server enforces a policy to limit access to the service (based on some counters), the policy will have impact on all hosts sharing the same IP address.
- o If access to a service has failed (e.g., wrong login/passwd), all hosts sharing the same IP address may not be able to access that service.

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](#)].

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 Case 1: CGN

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

1. 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).

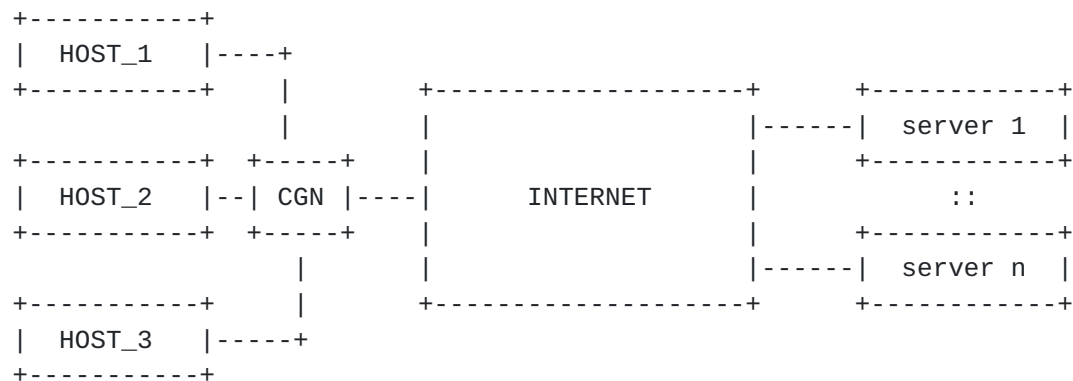


Figure 1

4. Use Case 2: A+P

A+P [[RFC6346](#)] 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 configure 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.

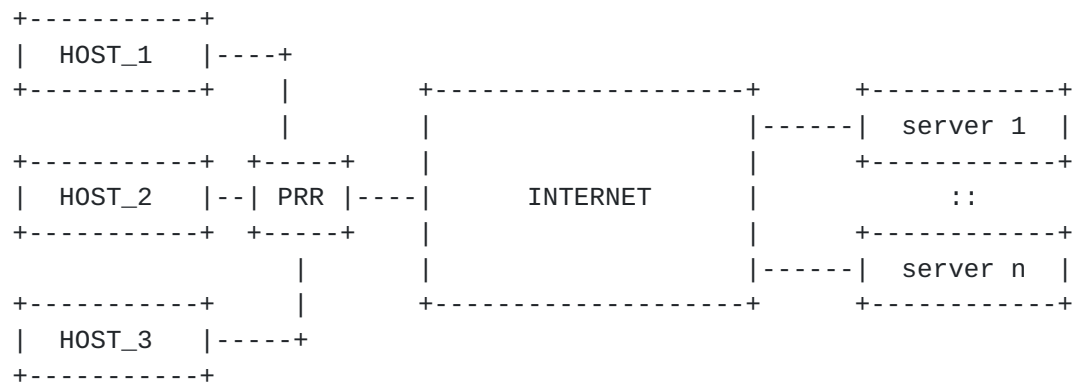


Figure 2

5. 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.

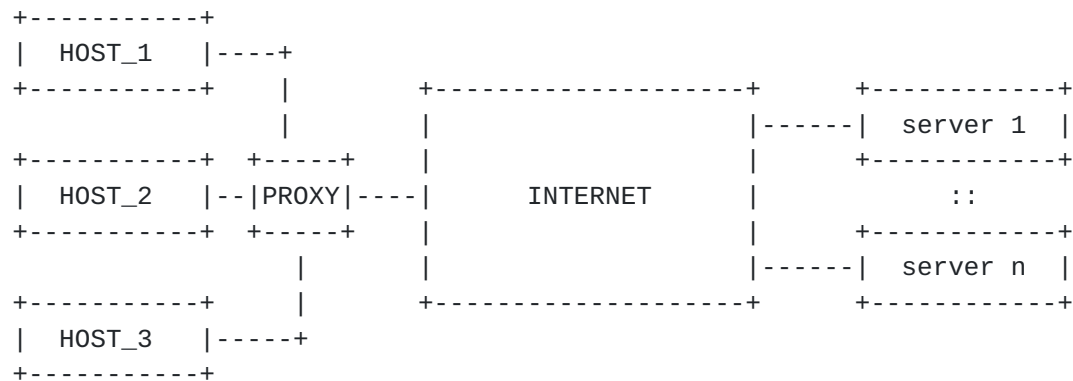


Figure 3

6. Use Case 4: Open Wi-Fi or Provider Wi-Fi

In the context of Provider Wi-Fi (also called Open Wi-Fi or FMC scenario), a dedicated SSID can be configured and advertised by a CPE 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](#), 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 CPE 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 pool managed by the CPE. Packets issued from a visiting terminal are translated using the public IP address assigned to the CPE (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 CPE. This is needed to apply some policies such as: accounting, 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 customer owning the CPE (e.g., some of the issues are discussed in [[RFC6269](#)]).

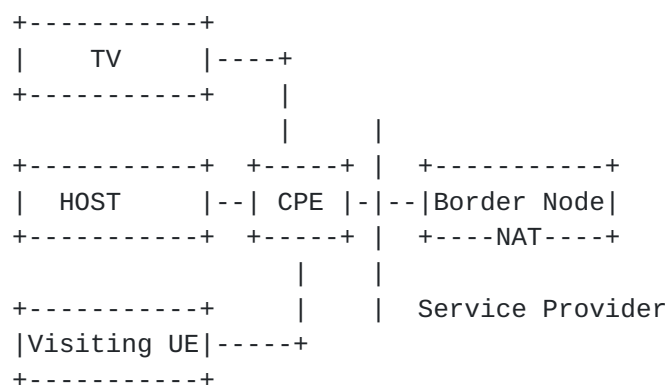


Figure 4

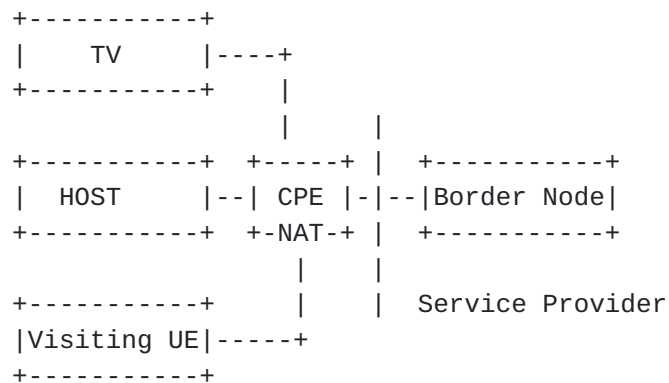


Figure 5

7. Use Case 5: Policy and Charging Control Architecture

This issue is related to the framework defined in [TS.23203] 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 but without being able to correlate between the piece of data visible for each entity. Concretely,

- o PCEF is aware of the IMSI (International Mobile Subscriber Identity) and an internal IP address assigned to the UE.
- o AF receives an external IP address and port as assigned by the NAT function.
- o 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.

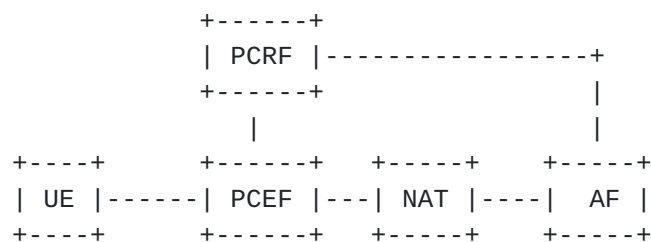


Figure 6

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

- o Policy Enforcement Point (PEP, [[RFC2753](#)])
- o Policy Decision Point (PDP, [[RFC2753](#)])

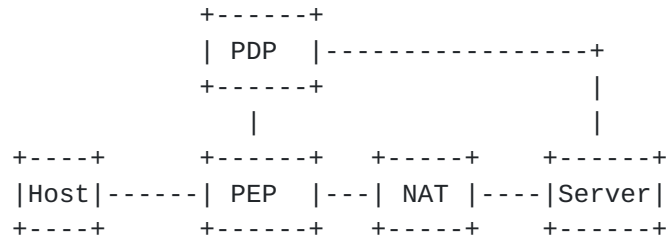


Figure 7

8. Use Case 6: Cellular Networks

Cellular operators allocate private IPv4 addresses to mobile customers 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. IPv6-only strategy, consisting in allocating IPv6 prefixes only to customers, 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 7](#). This issue is particularly encountered if policies are to be applied on the Gi interface: a private IP address may be assigned to several UEs, no correlation between the internal IP address and the address:port assigned by the NAT function, etc.

9. Security Considerations

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

10. IANA Considerations

This document does not require any action from IANA.

11. Informative References

[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-04](#) (work in progress), August 2012.

- [RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", [RFC 2753](#), January 2000.
- [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.
- [TS.23203] 3GPP, "Policy and charging control architecture", September 2012.

Authors' Addresses

Mohamed Boucadair
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

