Host Identification: Scenarios

draft-boucadair-intarea-host-identifier-scenarios-01
IETF 85-Atlanta, November 2012

M. Boucadair, S. Durel, D. Binet & T. Reddy
Background

• Host identification issue was raised in the BBF/3GPP FMC Workshop (November 2011)
  – “Encourage IETF work on mechanisms to enable identifying individual UEs behind NAT/RGs”

• Some progress was made in intarea WG
  – RFC 6269: listing issues encountered in address sharing context including implicit host identification (June 2011)
So, what is still missing?

• Solution specification?
  – A gap analysis is needed from the FMC community

• Is this issue specific to the so called FMC use case?

• This draft aims to provide a big picture overview of scenarios where the host identification issue is encountered
  – No solution-related discussion is included in the draft
Is this issue specific to the so called FMC use case?

- No
- 9 scenarios are identified so far:
  - CGN
  - A+P/MAP
  - Application Proxies
  - **UE behind a NATing RG**
  - **FAP behind a NATing RG**
  - Applying policies when a NAT is located in the boundary of the mobile network
  - Correlating between internal IP address:port and external IP address:port (PDP/PEP in NATed context)
  - Access to some cloud services when a NAT is in the path
  - Assign an IPv6 prefix to a host in the context of Provider Wi-Fi
The identified FMC case is deployment-specific

- Enforcing the NAT in the RG for a visiting UE will bring all the issues discussed in RFC6269 for the subscriber owning the RG
  - Is this acceptable for all service providers?
  - The main advantage is to leverage on the NAT in the RG and avoid introducing a CGN in the Provider’s network
  - Can be appropriate for community Wi-Fi service
The identified FMC case is deployment-specific

• If the NAT is not enforced in the RG but in the Service Provider’s network
  – The customer owning the RG is not impacted by a misbehaving visiting UE
  – Still, UEs sharing the same IP address will suffer from the same issues as for the CGN case

• In both case (NAT in RG or NAT in Service Provider’s network), the host identification is still problematic
Generalizing the Problem

• The host identification issue is valid for both IPv4 and IPv6
  – IPv4
    • The causes are address sharing, distinct administrative boundaries, use of tunnels, etc.
    • Mainly for applying policies: DSCP remarking, volume-based service offering, blacklist, etc.
    • Need to correlate between the external IP address and internal IP address
  – IPv6
    • For applying policies in the context of NPTv6
    • For assigning an IPv6 prefix in some contexts
Conclusions

• Host Identification is a valid technical problem
  – For both IPv4 and IPv6

• It is encountered in some FMC-related scenarios…but it is not specific to FMC

• *If the IETF has to conduct additional work on the host identification item, handling the issue with a big picture view is more valuable*
  – *Restricting it to FMC case is not encouraged*