Private IP addresses in Mobile IP

draft-petri-mobileip-pipe-00.txt

Bernhard Petri, Siemens
bernhard.petri@icn.siemens.de
1. Background:
   Private addresses in Mobile IP WG

1. Mobile IP charter:
   -> "Develop solutions for IPv4 private address spaces for the scenarios needed for deployment"

2. History:
   o Solutions for handling of IPv4 private addresses solicited already for several meetings
   o Some initial activities around June 99, but currently no WG draft available on this issue
   o Initial reviews showed some complexity of the problem, therefore:
     --> decision not to include handling of priv. addresses into the RFC2002-update (11/99)
     --> but to take this to the establishment a separate draft
1. Background: Mailing list discussions on private addressing in Mobile IP

- Discussions around Appendix of draft-ietf-mobileip-rfc2344-bis-01.txt: on: "Disparate Address Space Support"
  --> excellent outline of issues / problem space related to private addresses
  --> shows that problem applies more general to "overlapping address realms"

- Some mails on the need for "giving additional domain information" [Pete] for a private address, and on the need for an address "realm ID" [Gabriel] etc.

- Discussions on the cooperation with legacy RFC 2002 agents / nodes:
  --> re-use of an existing bit (T-bit), or definition of a new bit ("P-bit") within the Mobility Agent Advertisement Extension to indicate capability to support private addresses

- Discussions on whether solutions based on NAlS (RFC 2486) might be suitable
2. Problem statement - Handling of private addresses / disparate address realms

General: cf: draft-ietf-mobileip-rfc2344-bis-01.txt; Appendix

- if private addresses according to RFC 1918 are used, a receiving agent or mobile node will only detect that it is a private address, but will not know, to which address realm it belongs (unless a particular realm is preconfigured)
- similar problems for overlapping / non-routable corporate address ranges, even if not private

More specific:

- Corresponding node and mobile node are in disparate address spaces
- FA offers support of address realms different from the one it uses to communicate with HA e.g. since it advertise private COAs (Ma) or offers a VPN service (Mc)

[MC (or MA) Fa Fb Hb Hc Yc] (MN) ---------------- [FA] ---------------- [HA] ---------------- [Y]
Addr space A Addr space B Addr space C

draft-petri-mobileip-pipe-00.txt
2. Problem statement (continued): Handling of private addresses / disparate address realms

More specific examples:

Source: draft-ietf-mobileip-rfc2344-bis-01.txt; Appendix

- Mobile nodes with conflicting addresses (Mc = M and Md = M)

FA/HA in disparate address realms --> compound (IP-IP/GRE/...) tunnel with addr. transl /NAT
- particularly: HAs with private-only addresses
- particularly: FAs with private-only addresses
3. PIPE Solution Overview - What it does and what it doesn't provide ...

What PIPE provides for:

- An extension of IP-IP (RFC 2003) tunnels, allowing to handle private addresses by adding a kind of "address realm ID" for the inner IP addresses

  = the basis for a possible Mobile IP solution to handle private addresses, but not all detailed Mobile-IP extensions needed are outlined in the draft

What PIPE does **not** provide for:

- How to cooperate with existing RFC 2002 MIP agents/nodes (-> "P" bit discussion)

- Solution for other types of tunnels (GRE, L2TP, MPLS, ...)
  [expectation: easily extensible for other tunnel types; but not checked yet]

- Address translation / NAT functions for private addresses
3. PIPE Solution Overview - Tunnel Format for Private IP Encapsulation within IP

.. add (sel.+ realm-ID/VPN-ID) to RFC 2003 format:

+---------------------------+          +---------------------------+
|      Outer IP Header      |          |      Inner IP Header      |
| +------------------------+          | +------------------------+
| Sel. | VPN-OUI           |          | VPN index               |
| +------------------------+          | +------------------------+
|         VPN index         |          | Inner IP Header          |
| +------------------------+          | +------------------------+
|         IP Payload       |          | IP Payload              |
| +------------------------+          | +------------------------+
|                     ... |          |                     ...

Selector: indicates whether realm-ID / VPN-ID applies to source, dest. or both addr. of inner IP header.

VPN-ID / realm-ID:

more
3. PIPE Solution Overview -
Use of the VPN-ID (RFC 2685) as an address realm-ID

- 7-byte world-wide unique identification of networks (3-byte OUI + 4 byte index) +------------------------------------------+

- specified for various VPN purposes, particularly use of private addressing +------------------------------------------+

- derived from the structure of MAC addresses (3-byte OUI + 3-byte index), but extended index field to 4-bytes to allow for a possible 2+2 AS-number +index

- "OUI" (IEEE organizationally unique identifier) = world-wide unique company-ID [ more --> http://standards.ieee.org/regauth/oui/index.html ]
  e.g. of a network operator, company, service provider, IANA (0x00-00-5E), ...

- VPN index: index value for network or address realm, allocated by owner of VPN-OUI

| +--------------------+ 
| | 
| | VPN-OUI 
| +------------------------------------------+ 
| | 
| | VPN index 
| +------------------------------------------+ 

VPN-ID / realm-ID
### 3. PIPE Solution Overview - Example: packet travels from MN to HA (1)

priv. realm PR2  |  public IP (or PR4)  |  private realm PR3  
|----------------|---------------------|---------------------|
MN  -->  border gateway A  -->  border gateway B  -->  HA 
(BG A)  |  (BG B)             

Step 1 of 3: From MN to BG A:

- **Outer Header:**  
  - **Source Address:** MN(PR2)  
  - **Destination Address:** BG A(PR2)  
  - **Selector:** 0xE1 (explicitly indicated destination)  
  - **VPN-ID:** VPN-ID = PR 3

- **Inner Header:**  
  - **Source Address:** MN(PR2) = default  
  - **Destination Address:** HA(PR3)
3. PIPE Solution Overview -
Example: packet travels from MN to HA (2)

priv. realm PR2       public IP (or PR4)       private realm PR3
|                       |                       |
MN ---| border gateway A ---| border gateway B ---| HA
      (BG A)                   (BG B)

Step 2 of 3: From BG A to BG B:

Outer Header: Source Address: BG A (public IP or PR4)
      Destination Address: BG B (public IP or PR4)
Selector: 0xE3 (explicit source/dest realm, different)
VPN-ID: VPN-ID1 = PR 2
VPN-ID: VPN-ID2 = PR 3
Inner Header: Source Address: MN(PR2)
      Destination Address: HA(PR3)
3. PIPE Solution Overview -
Example: packet travels from MN to HA (3)

priv. realm PR2      public IP (or PR4)      private realm PR3
|                       |                       |
MN ---> border gateway A -------> border gateway B ---> HA
(BG A)                   (BG B)

Step 3 of 3: From BG B to HA:

Outer Header: Source Address: BG B (PR3)
               Destination Address: HA (PR3)
Selector:     0xE2 (explicitly indicated source)
VPN-ID:       VPN-ID = PR 2
Inner Header: Source Address: MN(PR2)
               Destination Address: HA(PR3) = default
4. PIPE - Private IP Encapsulation within IP:
Benefits

- outlines solution for the use of private addresses / disparate address realms for Mobile IP

- does not only care for simple cases (privately addressed MN), but for any type of combination of address realms (as illustrated in the example above) used for nodes and agents

- low administrative overhead involved to derive a realm-ID / VPN-ID, using either OUIs of operators or companies, or allocating realm-IDs from IANA's OUI (0x00-00-5E)

- low additional overhead for packets in the IP-IP tunnels
5. How to proceed -
Private Addresses in Mobile IP

- received messages to cooperate and work on a MIP WG framework / architecture document
  - -> sounds good
  - -> Appendix to draft-2344-bis looks like a good starting point

- additional work needed to specify how MIP nodes / agents supporting handling of private addresses communicate with existing RFC 2002 nodes / agents
  - -> advertisements, "P"-bit discussion
  - -> what else .. ?

- discussion to move PIPE towards an Experimental RFC for the time being, and possibly reconsider status later pending results of the 2 activities above