Outsourcing Home Network Authoritative Naming Service

draft-mglt-homenet-front-end-naming-delegation-05.txt

D. Migault, W. Cloetens, C. Griffiths, R. Weber

24/03/2015- IETF92- Dallas

Change log of the 6th version

- Clarifying on handling different views:
  - ▸ How the CPE may be involved in the resolution and responds without necessarily requesting the Public Masters (and eventually the Hidden Master)
  - ▸ How to handle local scope resolution that is link-local, site- local and NAT IP addresses as well as Private domain names that the administrator does not want to publish outside the home network.
- Adding a Privacy Considerations Section
- Clarification on pro/cons outsourcing zone-signing
- Documenting how to handle reverse zones
- Adding reference to RFC 2308 (or the SOA)

Renumbering

We received some comments on renumbering

- Included in the next version

- Text has been sent on the ML

- ... and I am asking for feed back next slide

Renumbering: Problem Description

Impact of renumbering on HM/S synchronization:

- Hidden Master/Slave synchronization is performed by exchanging:
  - HM -> S: NOTIFY
  - S -> HM: SOA, IXFR/AXFR exchange
  - Note: In a HM/S architecture no additional entity is expected to interact.
- When renumbering occurs IP is updated
- So HM/S must inform each other of this change.

Renumbering: Problem Description

Use cases to consider are:

- HM or (not both) S being renumbered
- make-before-break / break-before-make renumbering

Scope:

- It can be done through DNS, or other layers SCTP, IPsec...
- The draft details how to perform it using DNS
- Limit the description for single interface used at a time
- Assume TSIG or SIG0 is used to secure HM/S channel

HM Renumbered make-before-break

Main steps are:

- 1. Update the DNS(SEC) Homenet Zone:

    - 1. With new IP addresses

    - (Optionally, make old and new IP addresses co-exist, only updates TTLs)

- 2. Synchronize the DNS(SEC) Homenet Zone

- 3. Update the sync channel

    - Eventually 2. and 3. may be merged in one step

How TTL of the Old IPs should be set regarding the time between announcement and roll-over should be documented.

HM Renumbered make-before-break

Protocol Details (merged 2. and 3):

- 1. HM -> S: NOTIFY protected with RRSIG/TSIG

- 2. S authenticate the NOTIFY
  - ▸ IP address is not needed for authentication.
  - ▸ NOTIFY and RRSIG has the DNS Homenet Zone

- 2. S checks the IP address has changed.
  - ▸ The IP can be in the IP header
  - ▸ The IP address can be in the edns-client-subnet

- 3. S -> HM: Performs a routability check to the new IP address with a protected SOA exchange
  - ▸ In case of IP header and edns-client-subnet mismatch you may perform 2 different routability check, start with the IP header.

- 4. S updates its configuration

HM Renumbered break-before-make

Perform as before.

- Devices may be partially unreachable for 2*TTL

S Renumbered make-before-break

Main steps are:

- 1. S informs the HM

- 2. HM performs an reachability check

- 3. HM updates its configuration

  - ‣ DNS(SEC) Homenet Zone does not need to be updated

S Renumbered make-before-break

Protocol Details:

- 1. S -> HM sends a protected SOA query with the new IP
  - The IP can be in the IP header
  - The IP address can be in the edns-client-subnet
- 2. HM authenticates the query
- 3. HM -> S performs a routability check with a protected SOA/NOTIFY exchange
  - NOTIFY is part of the sync process but triggers a SOA request from the HM.
  - SOA is recommended as it does not trigger any additional exchanges, but S is not supposed to receive SOA requests.
- 4. Updates the configuration
  - If multiple S renumber at the same time, Cryptographic keys are sufficient to identify the appropriated S.

S Renumbered break–before–make

Perform as before.

- There is no impact. If a NOTIFY occurs when the S is being renumbered, than retry should be performed until S responds with the new IP address.

Next

- We will submit the next version soon,
- I believe we have addressed most/all comments,

- Thank you to those that provided feed backs!

Thank you for your attention