

Homenet Naming DHCP Options

draft-mglt-homenet-naming-architecture-dhc-options-00.txt

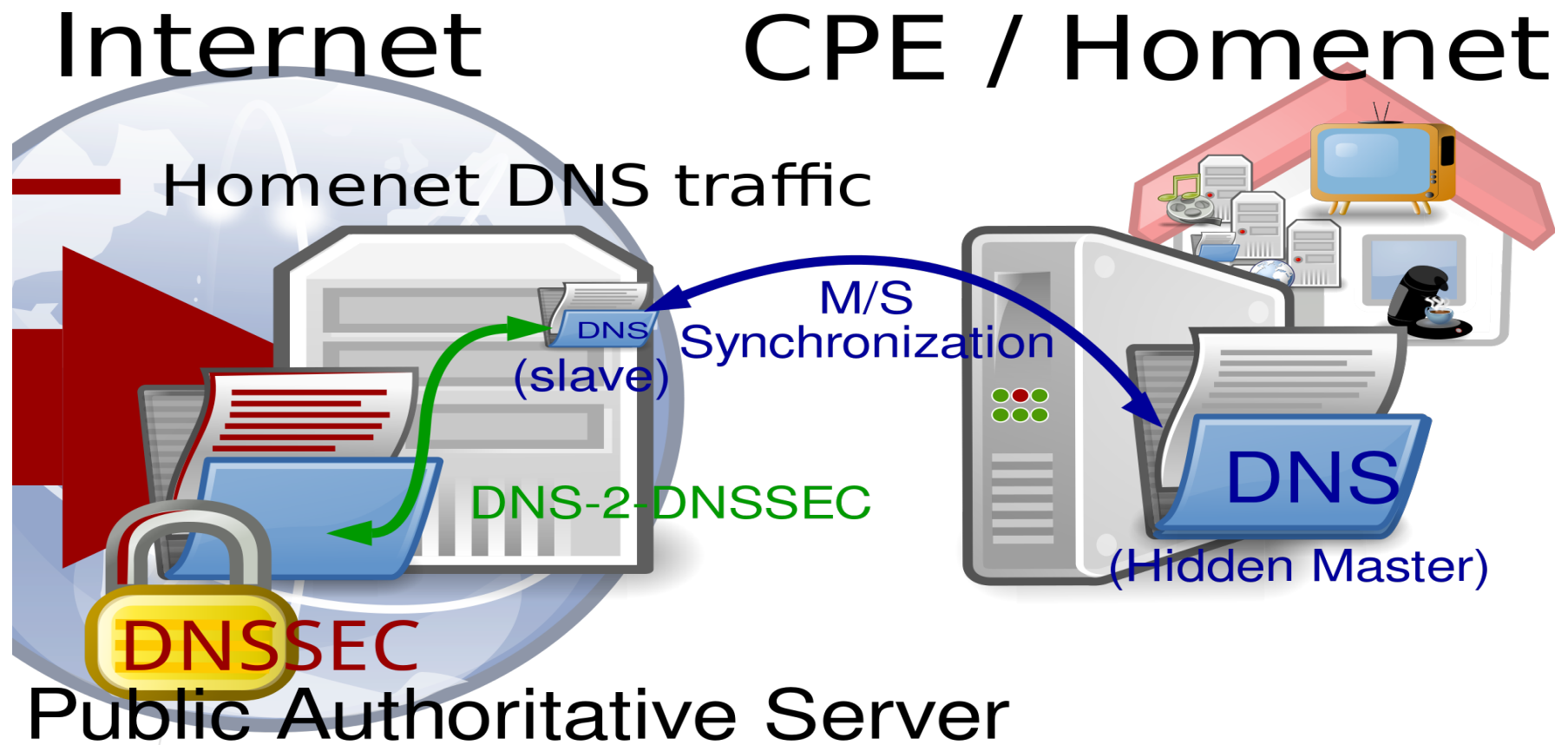
D. Migault, W. Cloetens, C. Griffiths, R. Weber

05/11/2013- IETF88- Vancouver

Table of Contents

- Architecture Description
- Setting the DNS Homenet DNS
- Uploading the DNS(SEC) Homenet Zone

Architecture Description



Architecture Description

The two operations consists in:

- Building the DNS Homenet Zone
 - ▶ Expected to be published on the Public Authoritative Masters

- Uploading the DNS Homenet Zone
 - ▶ To the Public Authoritative Name Server Set
 - ▶ via a secured channel

Architecture Description

We define one DHCP Option for those two operations:

- OPTION_ZONE_PUBLIC_MASTER, binding
 - ▶ Registered Domain
 - ▶ Public Authoritative Masters (FQDNs and IP addresses).

- OPTION_PUBLIC_MASTER_UPLOAD, binding
 - ▶ Public Authoritative Masters
 - ▶ Secure channels defined as
 - Protocol (NONE, TSIG, IPsec, SIG(0))
 - Security Credentials (PSK, ...)
 - Public Authoritative Name Server Set (IP addresses)

Setting the DNS Homenet Zone

```
$ORIGIN example.com
$TTL 1h

@ IN SOA public.autho.servers.example.net
      hostmaster.example.com. (
      2013120710 ; serial number of this zone file
      1d        ; slave refresh
      2h        ; slave retry time in case of a problem
      4w        ; slave expiration time
      1h        ; maximum caching time in case of failed
                ; lookups
      )

@ NS public.autho.servers.example.net

public.autho.servers.example.net A @IP1
public.autho.servers.example.net A @IP2
public.autho.servers.example.net AAAA @IP3
public.autho.servers.example.net AAAA @IP4
```

ZONE_PUBLIC_MASTER: Factorized

From DHCP option guide lines, we encapsulated the various options:

```
OPTION_ZONE_PUBLIC_MASTER_LIST      <- X OPTION_ZONE_PUBLIC_MASTER
- OPTION_ZONE_PUBLIC_MASTER
  - OPTION_REGISTERED_DOMAIN_NAME (list)
  - OPTION_MASTER                    <- X masters
    - MASTER_FQDN (Field)           <- single FQDN
    - OPTION_MASTER_IP4             <- X IP4
    - OPTION_MASTER_IP6
  - OPTION_MASTER
    - MASTER_FQDN (Field)
    - OPTION_MASTER_IP4
    - OPTION_MASTER_IP6
```

DHCP design questions:

- Can we assume that in IPv6 Home Networks the Master MUST be IP6
 - ▶ OPTION_MASTER_IP6 becomes a field
- Is 3 levels encapsulation fine?
- To reduce level encapsulation, one can have a list of (1 FQDN - 1 master)?

ZONE_PUBLIC_MASTER: Expanded

```
OPTION_ZONE_PUBLIC_MASTER_LIST
- OPTION_ZONE_PUBLIC_MASTER
  - REGISTERED_DOMAIN_NAME (field because single)
  - MASTER_FQDN (Field)
  - MASTER_IP6
  - OPTION_MASTER_IP4
```

Comparison between the Expanded Way and Factorized Way:

- Factorized optimize bandwidth
- Expanded is easy to develop
- Factorize does not make configuration harder:
 - ▶ Factorize-to-Expand function on the DHCP client
 - ▶ Expand-to-Factorize function on the Server side.

ZONE_PUBLIC_MASTER: Example

Suppose the CPE has 2 Registered Domains:

- mydomain.net
- mydomain.org

The CPE hosts these two domains on two different masters:

- master1.org
- master2.net

Every master has 2 IP4, 2 IP6

Do we agree that is a plausible use case?

ZONE_PUBLIC_MASTER: Example

Expanded way:

```
OPTION_ZONE_PUBLIC_MASTER_LIST
- OPTION_ZONE_PUBLIC_MASTER
  - REGISTERED_DOMAIN : mydomain.net
  - MASTER_FQDN : master1.org
  - MASTER_IP6
  - OPTION_MASTER_IP4
- OPTION_ZONE_PUBLIC_MASTER
  - REGISTERED_DOMAIN : mydomain.net
  - MASTER_FQDN : master2.org
  - MASTER_IP6
  - OPTION_MASTER_IP4
- OPTION_ZONE_PUBLIC_MASTER
  - REGISTERED_DOMAIN : mydomain.org
  - MASTER_FQDN : master1.org
  - MASTER_IP6
  - OPTION_MASTER_IP4
- OPTION_ZONE_PUBLIC_MASTER
  - REGISTERED_DOMAIN : mydomain.org
  - MASTER_FQDN master2.org
  - MASTER_IP6
  - OPTION_MASTER_IP4
```

Factorized way

```
OPTION_ZONE_PUBLIC_MASTER_LIST
- OPTION_ZONE_PUBLIC_MASTER
  - OPTION_REGISTERED_DOMAIN : mydomain.net
  - OPTION_MASTER mydomain.org
  - MASTER_FQDN : master1.org
  - MASTER_IP6
  - OPTION_IP4
- OPTION_MASTER
  - MASTER_FQDN : master2.org
  - MASTER_IP6
  - OPTION_IP4
```

- Factorized: [OPTION (7*4), IPs (2*4+2*32), FQDNs (#2*11+2*10)] # 150 B
- Expanded: 9*4 + (FQDN) 2*(#42) + (IPs) 2*(72) # 264 B (X 2)
- Difference increases with number of IP addresses, number of masters.

Uploading Zone

Public Authoritative Masters are bound Public Authoritative Name Server Set because:

- Each Public Authoritative Master is associated with a Public Authoritative Name Server Set

- A given DNS Homenet Zone MAY:
 - ▶ Have multiple Public Authoritative Masters
 - ▶ Need to upload on multiple Public Authoritative Name Server Sets

OPTION_PUBLIC_MASTER_UPLOAD

From DHCP option guide lines, we encapsulated the various options:

```
OPTION_PUBLIC_MASTER_UPLOAD_LIST <- X Public Masters
- OPTION_PUBLIC_MASTER_UPLOAD
  - SECURE_PROTOCOL (field)
  - OPTION_MASTER_FQDN_LIST (mandatory)
  - OPTION_PSK_CREDENTIAL
  - (future use Certificates, IDi)
  - OPTION_SERVER_SET_IP4
  - OPTION_SERVER_SET_IP6
```

DHCP design questions:

- Is 3 encapsulation fine?
- Can we assume that the SERVER MUST be able to be reached with IPv6?

PUBLIC_MASTER_UPLOAD: Example

Public Masters can be reached using IPsec or TSIG, using the same PSK If masters belong to different entities (ISP, third party)

```
OPTION PUBLIC_MASTER_UPLOAD_LIST <- X Public Masters
- OPTION_PUBLIC_MASTER_UPLOAD
  - SECURE_PROTOCOL (field) TSIG
  - OPTION_MASTER_FQDN_LIST master1.org
  - OPTION_PSK_CREDENTIAL (12 bytes) -> to be confirmed
  - OPTION_SERVER_SET_IP4
  - OPTION_SERVER_SET_IP6
- OPTION_PUBLIC_MASTER_UPLOAD
  - SECURE_PROTOCOL (field) IPsec
  - OPTION_MASTER_FQDN_LIST master2.org
  - OPTION_PSK_CREDENTIAL (12 bytes) -> To be confirmed
  - (future use Certificates, IDi) -> much more ;-)
```

PUBLIC_MASTER_UPLOAD: Example

If master1.org and master2.org belong to the same entities.

- A single Name Server Set is needed

```
OPTION PUBLIC_MASTER_UPLOAD_LIST <- X Public Masters
- OPTION_PUBLIC_MASTER_UPLOAD
  - SECURE_PROTOCOL (field) TSIG
  - OPTION_MASTER_FQDN_LIST master1.org, master2.org
  - OPTION_PSK_CREDENTIAL (12 bytes) -> to be confirmed
  - OPTION_SERVER_SET_IP4
  - OPTION_SERVER_SET_IP6
- OPTION_PUBLIC_MASTER_UPLOAD
  - SECURE_PROTOCOL (field) IPsec
  - OPTION_MASTER_FQDN_LIST master1.org, master2.org
  - OPTION_PSK_CREDENTIAL (12 bytes) -> To be confirmed
  - (future use Certificates, IDi) -> much more ;-)
```

We do not factorize SECURE_PROTOCOL to keep credential associated to ONE secure channel.

- Any suggestions?

Conclusion

Questions:

- Is IP6 an option or mandatory for masters and master server sets?
- Do we prefer the Expanded or Factorized or both options?
- Do people agree with these options ?

Thank you for your attention