Local Domain Name Discovery

draft-wang-dhc-ldn-option-00

Qin Wu

What’s the local domain name?

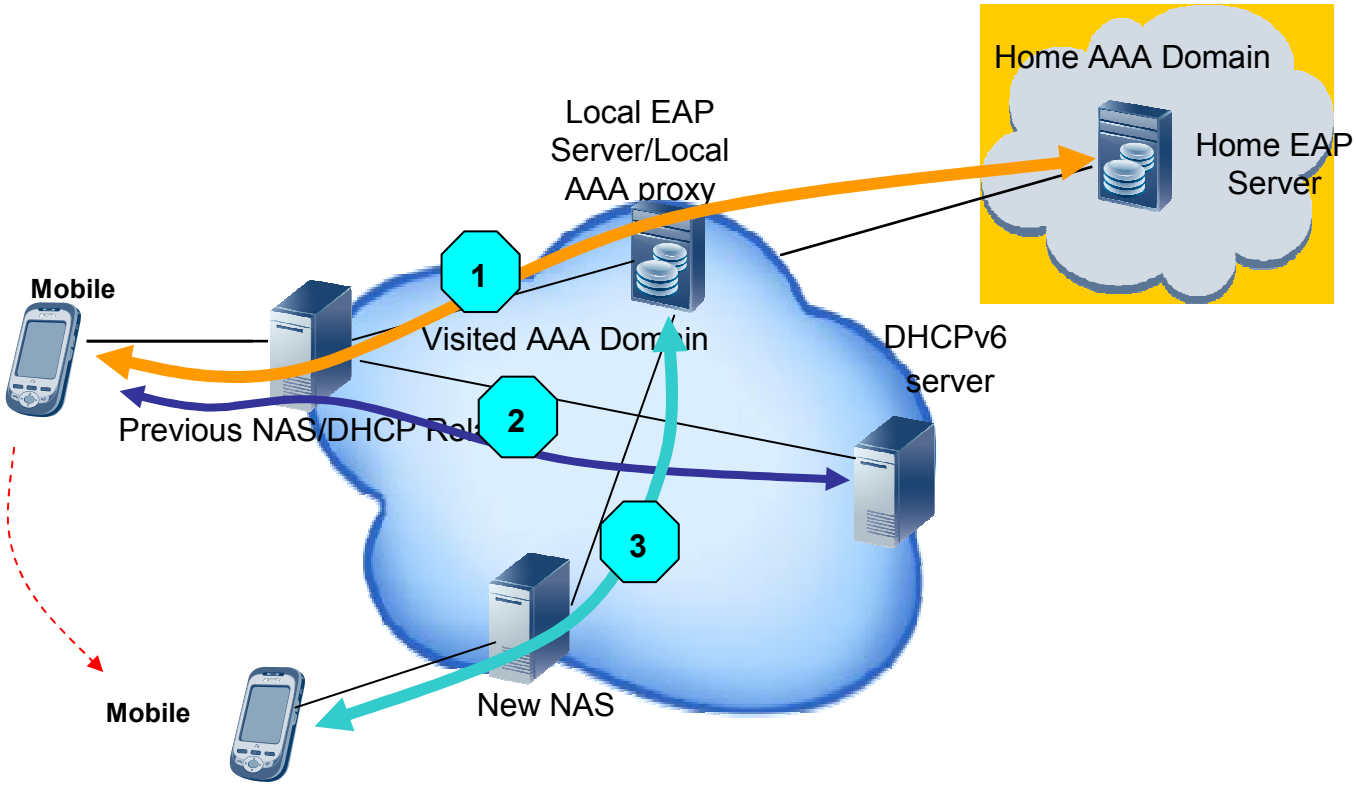
- The terms "home domain" and "local domain" are used to differentiate between the originating key management domain that performs the full EAP exchange with the peer and the local domain to which a peer may be attached at a given time.
  - The local domain name can be local EAP Re-authentication (ER) server name.
- The local domain name is utilized by the server and peer to derive domain special root key (DSRK, which is used as the EAP Re-authentication Root key).
- The local domain name MUST be available to the peer before the ER processing is initiated.

Reference: RFC5295, RFC5296.

Problem Statement and Motivation

- Problem Statement
  - As described in RFC5296, the peer could learn the domain name through the EAP-Initiate/Re-auth-Start message or via the lower-layer announcements.
    - The EAP-Initiate/Re-auth-Start message is sent at the beginning of the Re-auth processing. If the local domain name is learned at this time, the Re-auth processing will be delayed on consideration of time consumption that the peer derives the domain special root key and subsequent keys with the local domain name.
    - The lower-layer announcements can happen before the Re-auth processing. However, it is not specified anywhere.
- Motivation:
  - This document is intent to propose a media independent local domain name discovery mechanism, based on DHCP process.

Scenarios



1 **Full EAP authentication (Implicit bootstrapping) to push the local root Re-auth key to the local server**

2 **DHCP procedure to request local domain name**

3 **Local Re-authentication procedure to Re-authenticate the peer in the local domain**

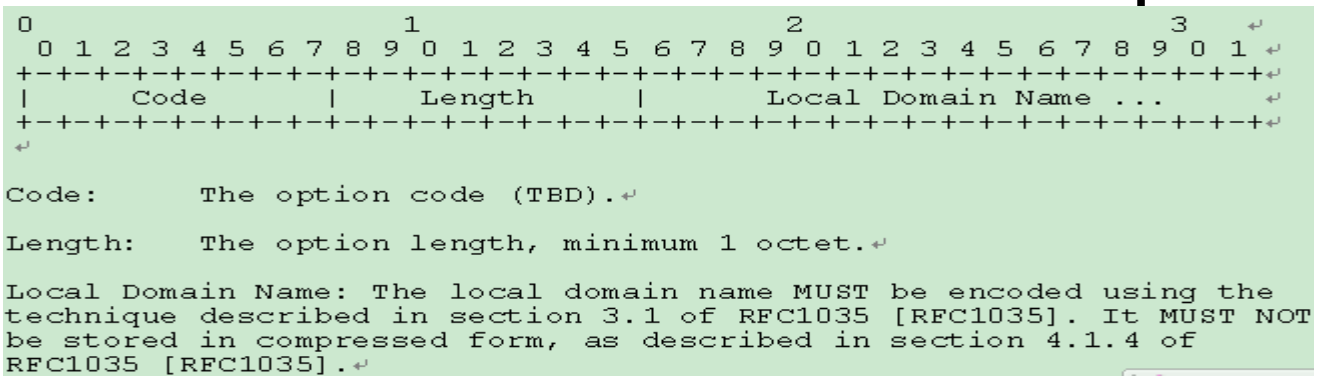
Proposal: DHCP based local domain name discovery

- Proposal 1:
  - The local domain name is configured in the DHCP server located in the local domain. The peer obtains the local domain name from the DHCP server.

- Proposal 2:
  - The local domain name has been conveyed to the NAS (DHCP Relay) from the AAA proxy located in the local domain. The peer obtains the local domain name using DHCP mechanism.

Format of Option

- DHCPv4 Local domain name option



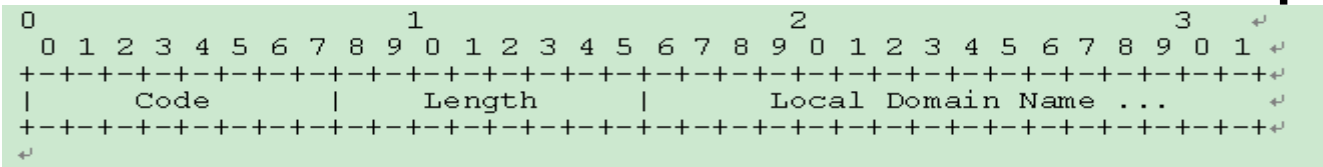
```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |    Length     |      Local Domain Name ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code: The option code (TBD).

Length: The option length, minimum 1 octet.

Local Domain Name: The local domain name MUST be encoded using the technique described in section 3.1 of RFC1035 [RFC1035]. It MUST NOT be stored in compressed form, as described in section 4.1.4 of RFC1035 [RFC1035].

- DHCPv4 local domain name sub-option



```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |    Length     |      Local Domain Name ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code: The option code (TBD).

Length: The option length, minimum 1 octet.

Local Domain Name: The local domain name MUST be encoded using the technique described in section 3.1 of RFC1035 [RFC1035]. It MUST NOT be stored in compressed form, as described in section 4.1.4 of RFC1035 [RFC1035].

Next Step

- Adopt it as WG work item?

Thanks

www.ietf.org