IETF 83 DHC WG Meeting

Security option extensions for DHCPv4

draft-bi-dhc-sec-option-01

Yang Cui
Huawei Technologies
Mar. 29, 2012 @Paris

Motivation

- To propose a new DHCP option, providing network configuration parameter for security
- Why DHCP?
  - configuration information is expected to be initialized at the early stage when it is connected to the network
  - DHCP is essential for users who want to connect to IP networks before they can communicate with other hosts

Background

- DHCP options:
  - configuration parameters and control information can be carried in DHCP options, such as defined in [RFC2132], [RFC3046], [RFC4030], etc.
- Security related parameters, not included
  - hard to guarantee the validity of information provided, even authentication [RFC3118] is deployed
  - DHCP solely is quite hard to provide security
  - how to guarantee the validity of DHCP option is out of scope

DHCP option

- However, DHCP has the capability to help set up security mechanism, at the very beginning a client connects to IP network, if

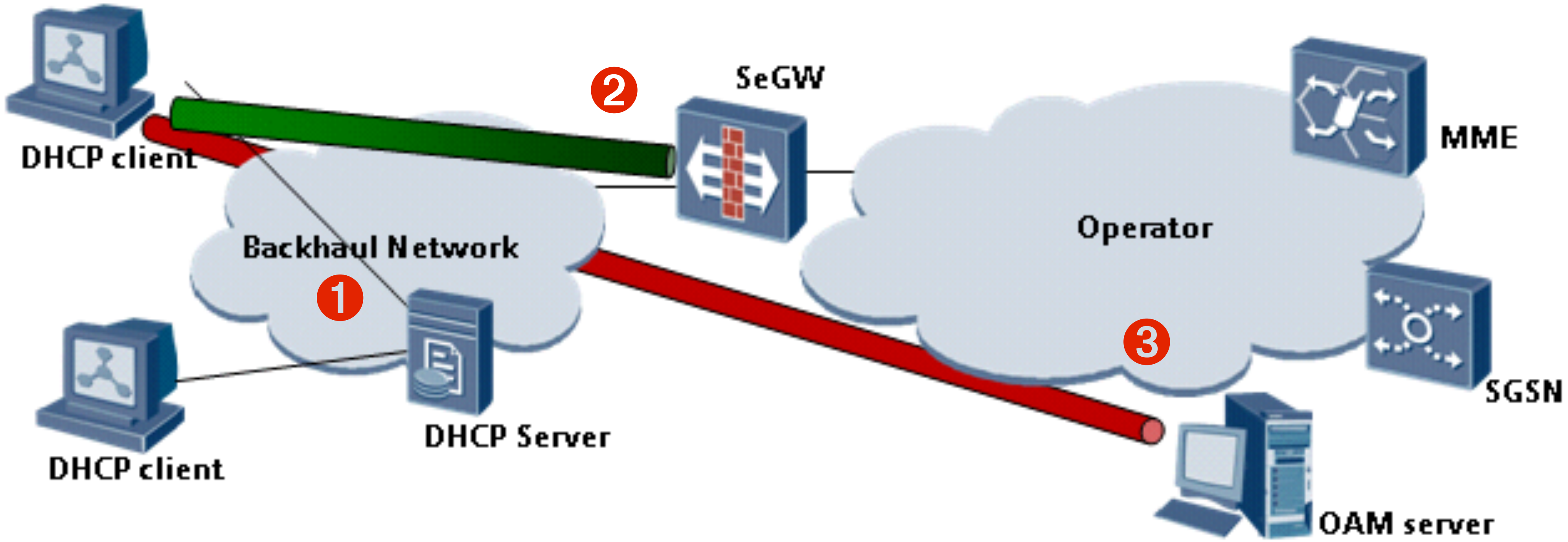
  1. the security does not depend on configuration information provisioned by DHCP option, for example, not contain any sensitive information to SA
  2. attackers do not benefit from manipulating DHCP option

A typical use case - self booting in 3GPP network

1. client connects to DHCP server to get IP address and network configuration, including IP addresses of SeGW (and PKI server, etc.) by a new DHCP option, automatically

2. client (with pre-installed vendor's certificate) connects to SeGW for mutual authentication and security mechanism setting up

3. client can connect to operator's core network by IPsec tunnel or TLS.

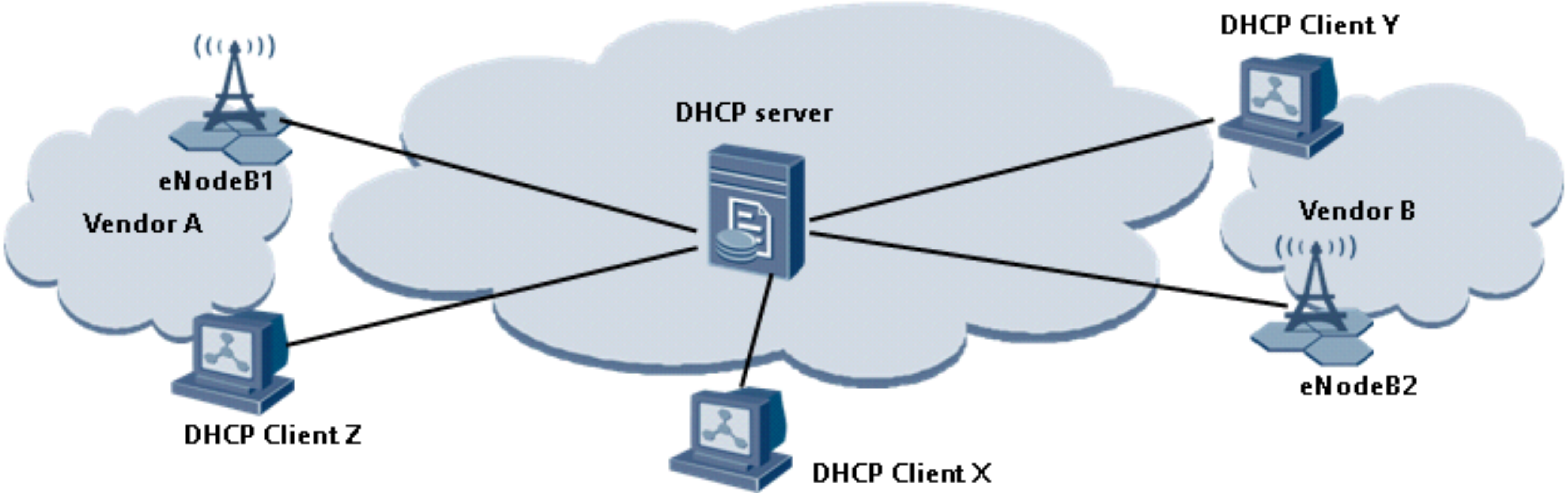


Analysis

- Client is pre-installed with vendor's certificates to have cross-certification with operator's network
- Security consideration
  - since DHCP server is not in administrative area, DHCP option could be manipulated.
  - but, a fake DHCP option cannot hurt the security between client and SeGW, because they have mutual authentication
  - attackers do not benefit, because security does not depend on DHCP option

Problem of previous solution

- Vendor-specific (option 43) does not give the dynamic capability to DHCP clients, because
  - bad interoperability
  - manual setting is necessary
  - fail the booting-up, since IP address of the SeGW (and PKI server) is a MUST for client



Proposal

- DHCP security configuration option, possibly includes the following minimum set for security
  - client IP address
  - SeGW IP address
  - PKI IP address
  - etc.

Data format

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  option-code  |  option-len   | C-IP Address   |   data-len1  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                    Client IP address Data                     |
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Se-GW ID     | data-len2   |      Security-GW ID Data        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                     Security-GW ID Data                       |
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  ACL policy   | data-len3   |      ACL Policy Data            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                     ACL Policy Data                           |
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  PKI IP Add   | data-len4   |      PKI IP Address Data        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                     PKI IP Address Data                       |
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              RSV                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              Private                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Finally...

- A new DHCP option itself does not guarantee the security, but provides a quick and dynamic way to allocate the security configuration parameter
- A standardized DHCP option could be a huge benefit to interoperability, instead of vendor-specific (option 43) solution
- To get further reviews and comments

Questions?