

KDC option for DHCPv6

Shoichi Sakane

Yokogawa Electric Corporation

2008/03/10

Purpose and Goal of this presentation

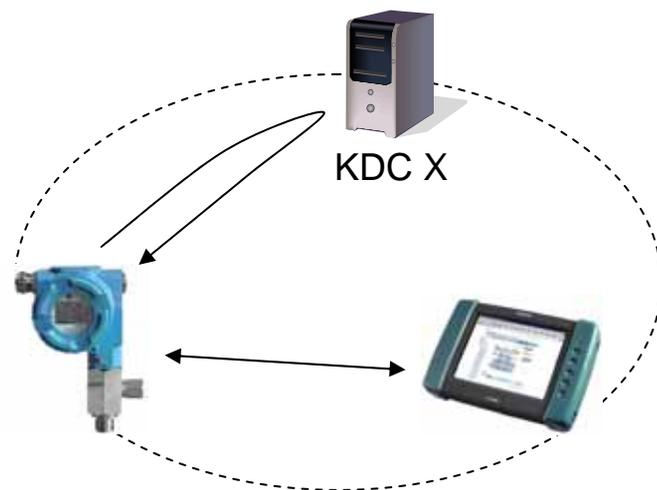
- I would like to standardize the KDC option for DHCPv6.
- First of all, I would like to get a consensus
 - #1. adding the KDC option as a DHCPv6 option.
 - #2. the way to implement it into a DHCPv6 option.

Background: IPv6 and Kerberos meet in the industry

- In the control and monitoring network of the industry, especially large plant network, there are lots of sensor devices like temperature, pressure, vibration and flow, and also lots of actuators.
- IPv6 is expected to reduce the management cost of IP address in that environment.
- On the other hand, the devices have several restrictions i.e. board size, memory size, power consumption and CPU power.
- All devices can not always use asymmetric key cryptography which we usually use.
- The Kerberos protocol is a de-facto standard for industry network security so that the authentication system can establish on even these devices.
- To exchange key information of IPsec between these devices for the secure communication, we standardized RFC4430 KINK protocol.

Background: Bootstrapping of Kerberos system

- The Kerberos protocol is a authentication system.
- The clients need to know some information of the KDC for bootstrapping, e.g. IP address of the KDC.
- To get the address, using DNS is recommended in RFC4120.
- However, in the industry environment,
- DNS can not always be used because
 - The networks typically are not constructed like the hierarchical network structure.
 - The network is basically discrete from each other.
 - The network is basically isolated from the Internet.
- Furthermore, some industry standard protocols assumes presence of DHCP.
 - If the discovering is realized by DHCP, the implementation cost would be saved.
- That is why the KDC option for DHCPv6 is required.



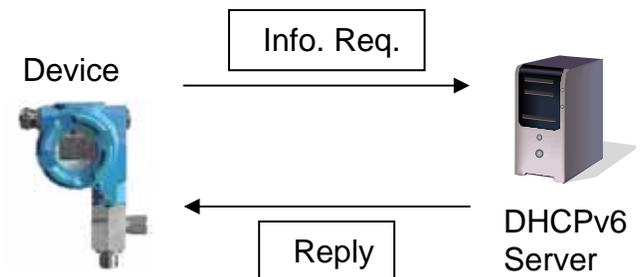
Requirement

- The Kerberos client has to get at least one IPv6 address of a KDC to which the client belongs from DHCPv6 server.

... Discovering client's KDC

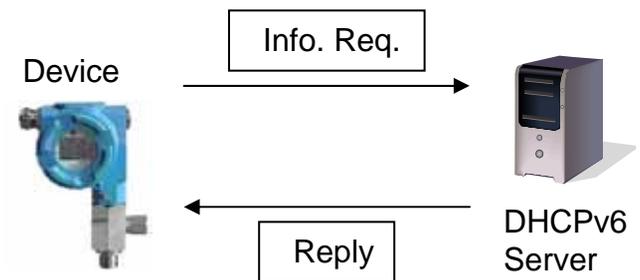
How to realize the discovering

- Simply using RFC3736 stateless DHCPv6.
- Adding a DHCPv6 option which contains the KDC information.



Requirement of the fields

- Request: Information-Request Message
 - Nothing, i.e. just specify an ORO.
 - Or with the Kerberos name of the client
- Response: Reply Message
 - IP addresses, and port number of the KDC
 - Realm name of the KDC
 - Service type of the Kerberos protocol



Current status

- Fundamental specification is described in *draft-sakane-dhc-dhcpv6-kdc-optoin-00.txt*
- There are some points to be considered.
 - Specification of the field of a principal name
 - Encoding method of a principal name
 - Type of the address family of a KDC
- A test implementation has been done.
 - But, with a vendor specific option.

Points to be considered

1. Specification of the field of a principal name
 - 1-1. DUID with new DUID type in another client identifier option
 - 1-2. DUID with new DUID type in a new option
e.g. principal name option
 - 1-3. A field in the KDC option ... I prefer it.
2. Encoding method of a principal name
 - 2-1. TLV in DHCP manner ... I prefer it.
 - 2-2. ASN.1 in Kerberos manner
3. Type of the address family of a KDC
 - 3-1. Only IPv6 address of the KDC ... I prefer it.
 - 3-2. IPv4 address could be provided ... Does it allowed ?

Further consideration

- What is the relationship of the KDC sub-option of the CCC option [RFC3634] ?
- In the cross-realm environment of Kerberos, another discovering is required to communicate with the peer.
 - It is required to get at least one IPv6 address of a KDC to which the peer belongs, before the client starts to talk to the peer.

Conclusion

- Basic specification is described in *draft-sakane-dhc-dhcpv6-kdc-optoin-00.txt*
- There are some points to be considered.
- A preliminary implementation exists.

Questions

- Would it be possible to add the KDC option to a DHCPv6 option, though there are some points to be considered ?

END of the presentation