INTERNET-DRAFT
Intended Status: Standards Track
Expires: August 18, 2012

S. Sakane
Cisco Systems
M. Ishiyama
Toshiba Corp.

February 15, 2012

Kerberos Options for DHCPv6
draft-sakane-dhc-dhcpv6-kdc-option-14.txt

Abstract

This document defines new four options for the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) to carry configuration information related to the Kerberos protocol [RFC4120].

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Kerberos Version 5 [RFC4120] is an authentication system which is a trusted third-party authentication protocol. Each organization wishing to use the Kerberos protocol establishes its own "realm", and each client is assigned to that realm. At least one Key Distribution Center (KDC) is required for the operation of a Kerberos realm.

When a client wants to start communication with a Kerberos application server (which is another client of the KDC), and to be authenticated to that server, the client needs to acquire a credential from the KDC. In this process, the client presents both an identifier for itself, and the realm name to which the client itself belongs. After the client gets a credential from the KDC, the client presents it to the Kerberos application server. The server can authenticate the access from the client with this credential. Hence, the client needs to know at least one IP address for a KDC from which the client can get a credential before the client begins the communication with the Kerberos application server.

One use case for this specification is as follows. A public workstation for an unspecified several number of students in a college might not have any initial configuration for Kerberos. If there is a mechanism providing a realm name and a set of IP addresses for KDC instances, a student need only input a user identifier and a pass phrase into the workstation, and can then use the Kerberos authentication system.

To provide a set of IP addresses of the KDC, the Kerberos V5 specification [RFC4120] defines KDC discovery by utilizing DNS SRV records [RFC2782]. However, systems that do not employ the DNS, but do use DHCP, do exist, for example industrial systems. Some industrial systems don't use DNS because they have already had their own name spaces and their own name resolution systems, including pre-configured mapping tables for devices, rather than using FQDNs and DNS. And these systems would prefer not to employ DNS only for name resolution because adding a new server may bring a decrease in the reliability of the system, and increase the management cost of the system. (Details are described in Appendix A), For such an environment, another mechanism is required to provide a set of IP addresses for the KDC instances. For the PacketCable Architecture [PCARCH], the KDC Server Address sub-option for the DHCPv4 CableLabs Client Configuration option is defined in RFC 3634 [RFC3634]. However, a mechanism which does not depend on any external architecture is required for providing a realm name and a set of IPv6 addresses.

The Kerberos option for DHCPv6 defined by this document allows for

provision of a realm name and/or a list of IP addresses for KDC instances. The Kerberos option does not replace any of the previous methods, and this option does not interfere with those methods.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

It is assumed that the readers are familiar with the terms and concepts described in DHCPv6 [RFC3315].

3. Kerberos Options

The Kerberos options provide a set of configuration parameters for Kerberos. This document defines the options listed below.

    Kerberos Principal Name Option
    Kerberos Realm Name Option
    Kerberos Default Realm Name Option
    Kerberos KDC Option

This section describes the format of each option, and the usage of each field.

Except for the Kerberos KDC Option, none of these options may appear more than once in a DHCPv6 message.

3.1. Kerberos Principal Name Option

This option provides a principal name of the Kerberos system. It is intended that a DHCPv6 server determines a specific set of the configuration parameters of the Kerberos system for either a client or a Kerberos application server specified by the principal-name field.

The format of the Kerberos Principal Name option is:

```
    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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   OPTION_KRB_PRINCIPAL_NAME   |          option-len           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    :                                                               :
    :                         principal-name                        :
    :                        (variable length)                      :
    :                                                               :
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- option-code (16-bit): OPTION_KRB_PRINCIPAL_NAME (TBD by IANA)
- option-len (16-bit): length of the principal-name field.
- principal-name (variable): a client principal name. The encoding of the principal-name field MUST conform to "PrincipalName" defined in section 5.2.2 of RFC 4120 [RFC4120].

3.2. Kerberos Realm Name Option

This option provides a realm name for the Kerberos system. It is intended for DHCPv6 client use. This option informs a DHCPv6 server of which realm the client want to access, and a DHCPv6 server can determine what information should be sent to the client.

The format of the Kerberos Realm Name option is:

```
    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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     OPTION_KRB_REALM_NAME     |          option-len           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    :                                                               :
    :                           realm-name                          :
    :                        (variable length)                      :
    :                                                               :
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- option-code (16-bit): OPTION_KRB_REALM_NAME (TBD by IANA)
- option-len (16-bit): the length of the realm-name field in octets.
- realm-name (variable): a realm-name. The encoding of the realm-name field MUST conform to "Realm" which is defined in section

5.2.2 of RFC 4120 [RFC4120].

3.3. Kerberos Default Realm Name Option

This option provides a default realm name of the Kerberos system. Unlike the Kerberos Realm Name Option, it is intended for a DHCPv6 server to use, and specifies the default realm name to both clients and Kerberos application servers in the Kerberos system.

The option-code of this option is OPTION_KRB_DEFAULT_REALM_NAME. The format and the usage of each field are identical to the Kerberos Realm Name Option.

3.4. Kerberos KDC Option

This option provides a set of configuration information about a KDC.

The format of the Kerberos KDC Option is:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         OPTION_KRB_KDC        |          option-len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Priority            |            Weight             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Transport Type|          Port Number          |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               |
|                                                               |
|                                                               |
|                        KDC IPv6 address       +-+-+-+-+-+-+-+-+
|                                               |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               :
:                                                               :
:                           realm-name                          :
:                        (variable length)                      :
:                                                               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

o option-code (16-bit): OPTION_KRB_KDC (TBD by IANA)

o option-len (16-bit): 24-octet + the length of the realm-name field in octets.

o Priority (16-bit): see the description of Weight field.

o Weight (16-bit): both Priority and Weight provide a hint for the KDC server selection mechanism of a client. An implementer MUST follow the handling of the Priority and Weight values in the DNS SRV specification [RFC2782] for this usage.

o Transport Type (8-bit): The Transport Type specifies the transport for the Kerberos communication. The Kerberos specification [RFC4120] defines how to use both UDP and TCP for communication between clients and Kerberos application servers. The exchanges over TCP are described in [RFC5021]. The exchanges over TLS are described in [RFC6251].

   The transport type is defined in below.

Value	Transport Type
0	Reserved
1	UDP
2	TCP
3	TLS
4-254	Unassigned
255	Reserved

o Port Number (16-bit): a port number listened to by the KDC.

o KDC address (128-bit): an IPv6 address of the KDC.

4. Client Operation

This section describes the client behavior when the client requires configuration parameters for the Kerberos system, and when the client receives messages from the DHCPv6 server.

When the client requires configuration parameters for a Kerberos system while bootstrapping, the client SHOULD put the client principal name itself into the Kerberos Principal Name Option.

When the client requires specific information for a certain realm, the client SHOULD specify the realm name in the Kerberos Realm Name Option. When the client requires specific information related to a certain Kerberos application server of the Kerberos system, the client SHOULD put the principal name of the server into the Kerberos Principal Name Option.

More than one KDC Options MAY be presented in a DHCPv6 message of the Reply Message from the DHCP server. In this case, the client MUST use the addresses in the order of the value of the priority field in each Kerberos KDC Option. The value of the weight field might be considered simultaneously. For this usage, an implementer MUST refer to the DNS SRV specification [RFC2782].

The client MAY include any other options with data values as hints to the DHCP server as described in section 18.1.5 of RFC 3315 [RFC3315].

4.1. KDC discovery for a client

When a client is capable of using both the DNS method defined by section 7.2.3.2 of [RFC4120] and the DHCP method defined by this document, the method the client adopts depends on local policy. The administrator of the realm MUST define the method for the client before the client is installed into the environment.

When there are no criteria in the environment, and the client could get the Kerberos information from either the DNS server or the DHCP server, then the information from DNS SHOULD be preferred. The following is a recommendation of the behavior of the client in such environment where there is no criteria.

```
                           No Ans. or
           +------------+  DNS Info.  +-----------+ No Ans.
  Start --> | Ask DHCP(1)| ----------> | Ask DNS(3)| ------> Abort(4)
           +------------+             +-----------+
             /          \                        \
   Only KRB /            \ DNS and                \ KRB Info.
     Info. /              \ KRB Info.              \
          /                \                        \
         |                  |                        |
         |                  V                        |
         V     No Ans.  +-----------+  KRB Info.    V
  Adopt Info. <-------- | Ask DNS(6)| ---------> Adopt Info.
  from DHCP             +-----------+            from DNS
   (2), (7)                                      (5), (8)

     Abbreviations:
       Ans.: Answer
       Info.: Information
       KRB: Kerberos
```

1) Initially, the client asks both DNS and Kerberos information to the DHCP server.

2) If the client gets a response with Kerberos information from the DHCP server, the client adopts the information from the DHCP server.

3) As the result of (1), if the client gets either no answer or only a response with DNS information from the DHCP server, the client then asks Kerberos information from the DNS server.

4) If the client gets no answer from the DNS server, then the client will abort.

5) If the client gets Kerberos information from the DNS server, then the client adopts the information from the DNS server.

6) If, as the result of (1), if the client gets both DNS and Kerberos information from the DHCP server, then the client asks Kerberos information to the DNS server.

7) If the client gets no answer from the DNS server, the client adopts the Kerberos information from the DHCP server.

8) If, as the result of (6), the client gets Kerberos information from the DNS server, the client adopts the information instead of another from the DHCP server.

5. Server Operation

After the DHCPv6 server receives a message which is contained an Option Request Option, the information the server will provide depends on local policy. If there are no criteria on the server, the following operation is RECOMMENDED.

If the message from a client did not include any information which can be used to determine the correct configuration parameters for a specific client, the DHCP server SHOULD reply with at least the Default Realm Name Option.

6. IANA Considerations

IANA is requested to assign four option codes from the "DHCPv6 Options Codes" registry for the following:

OPTION_KRB_PRINCIPAL_NAME
OPTION_KRB_REALM_NAME
OPTION_KRB_DEFAULT_REALM_NAME
OPTION_KRB_KDC

IANA is requested to maintain a new number space of Kerberos Message Transport Type, located in the Kerberos Parameters Registry. The initial types are described in section 3.4.

IANA is requested to assign future types with an "IETF Consensus" policy as described in BCP 26. Future proposed types are to be referenced symbolically in the Internet-Drafts that describe them, and shall be assigned numeric codes by IANA when approved for publication as an RFC.

7. Security Considerations

The security considerations in RFC 3315 fully apply.

DHCPv6 messages can be altered undesirably. If an adversary modifies the response from a DHCPv6 server or inserts its own response, a client could be led to contact a rogue KDC that does not know the client access. Both cases are categorized as a kind of the Denial of Service (DoS) attack. However, such an incorrect KDC does not know the shared key between the client and a valid KDC. The incorrect KDC is not be able to proceed any further state of the client. Even when the client receives a response from such KDC, the client can know the fact that it has received an inappropriate message after it verifies the response with the shared key.

The considerable situation is that the support of an unconfigured workstation used by multiple users, which obtains its KDC information and default realm via DHCP. In such a scenario, the workstation may not have a host or other service key, and thus be unable to validate TGT's issued to users for the purposes of authorizing login. If this is the case, an altered DHCP response could result in the workstation talking to a rogue KDC which it will be unable to distinguish from a real KDC, and allowing access by unauthorized users.

In order to minimize potential vulnerabilities, a client SHOULD use DHCPv6 authentication as defined in section 21 of RFC 3315.

Sometimes, Kerberos information is manually configured into the client before the DHCPv6 process starts. Generally, manual configuration of the device SHOULD be preferred to configuration via the DHCP server.

8. Acknowledgments

The authors are very grateful to Nobuo Okabe and Shigeya Suzuki. They contributed the summary explaining why DNS is not appropriate to some industry networks, which is put as the appendix of this document. Ted Lemon gave us many suggestions to improve the specification in terms of the DHCP manner. Ken'ichi Kamada and Yukiyo Akisada contributed for the initial work of making this document. The authors also thank Jeffrey Hutzelman, Kazunori Miyazawa, Kensuke Hosoya, Nicolas Williams, Nobumichi Ozoe, Sam Hartman, and Stephen Farrell. They gave us valuable comments and suggestions for this document.

9. References

9.1. Normative References

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2782]
A. Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3315]
R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4120]
Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC5021]
Josefsson, S., "Extended Kerberos Version 5 Key Distribution Center (KDC) Exchanges over TCP", RFC 5021, August 2007.

[RFC6251]
Josefsson, S., "Using Kerberos Version 5 over the Transport Layer Security (TLS) Protocol", RFC 6251, May 2011.

9.2. Informative References

[PCARCH]
"PacketCable 1.0 Architecture Framework Technical Report", PKT-TR-ARCH-V01-991201, http://www.packetcable.com/downloads/specs/pkt-tr-arch-v01-991201.pdf

[RFC3634]
K. Luehrs, R. Woundy, J. Bevilacqua, N. Davoust, "Key Distribution Center (KDC) Server Address Sub-option for the Dynamic Host Configuration Protocol (DHCP) CableLabs Client Configuration (CCC) Option", RFC 3634, December 2003.

Appendix A. Why DNS is not acceptable in some environments

1. Summary

- This appendix describes reasons why DHCP-based KDC discovery is more suitable than DNS-based KDC discovery described in RFC4120 (= the RFC4120-way) for industrial systems.

- The main reason is that some industrial systems don't use DNS because they have already had their own name spaces and naming systems rather than FQDN and DNS.

- Fewer servers benefit industrial systems:
  1) Less messages simplifying the systems.
  2) Less servers contributing reliability, and reducing management cost.

- We understand that RFC4120 does not require DHCP for KDC discovery. However, we will have to solve DNS discovery when considering the RFC4120-way.
  And it is natural way to use DHCP for the purpose.

- DHCP-based KDC discovery is more efficient under those systems (=expecting not to use DNS).

2. Background (what are industrial systems?)

These systems can have a large number of devices, i.e. sensors and actuators, usually called field devices by which the systems control plants, factories, buildings, etc.

These field devices have the following features:
1) Their resources, e.g. processing capability, memory size, footprint, power consumption and user i/f, are limited even though they are physically large.
2) The field device is controlled as an I/O by a administrative device, usually called controller, with a legacy communication technology.
3) Security of the field devices has to date not been considered as they were regarded as being on I/O buses, not networks.

3. High-level goal and some requirements

3.1. IP and security can enhance industrial systems.

Our goal is to introduce the latest IP-based networking technology into field devices for enhancing the entire system.
1) Network architecture (=IP technology) can enhance the systems including the field devices.
2) Field devices will require security if connected to a network.

The field devices will not be I/O devices anymore.

3.2. Auto-configuration benefits industrial systems.

Auto-configuration will also be important for large systems like the industrial systems if introducing new technology or capabilities:

1) Reducing engineering cost when installing/configuring a large number of field devices over a large area. The size of a plant, the size of an industrial system and the number of field devices are growing.

   - An example of a single large process automation system: About 20000 field devices over 2km*2km area

     References:
      - http://www.process-worldwide.com/fachartikel/pw_fachartikel_2699276.html

   - An example of a distributed process automation systems: About 30000 field devices for 26 distributed sites over 30km*30km area.

     References:
      - http://www.mikrocentrum.nl/FilesPage/3462/Presentatie%20C3-1.pdf
      - http://www.nam.nl/home/Framework?siteId=nam-en&FC2=/nam-en/html/iwgen/algemeen/zzz_lhn.html&FC3=/nam-en/html/iwgen/algemeen/over_de_nam.html

   - An example of a single large building automation system: 170000 control points of 16500 field devices in 729,000 sq. meters (7.8 million sq. ft.) building complex.

     References:
      - http://www.echelon.com/company/press/2003/echelon_mori.htm

2) Reducing the chance of human error.

3) Making disaster-recovery easier.

3.3. Security mechanisms suited to resource-limited devices are necessary.

Kerberos-based security can be suited for resource-limited devices,

i.e. field devices, because of not requiring
public key cryptography (of course, when not using PKINIT).

4. Some industrial systems don't use DNS.

For field devices, there have been multiple technologies (see Section 6) which don't use DNS because of having already had their own name spaces and naming systems even though introducing IP (partially at this moment).

For example, "tag" is the common logical identifier for the process automation systems and Device ID is the common logical identifier for the building automation systems.
(You may think those names are not so abstracted, though....)

5. KDC discovery with DHCP is more suitable than with DNS.

If Kerberos is introduced into field devices,
auto-configuration will be achieved with the following steps:
1) Learning DNS address(es) by DHCP
2) Learning KDC address(es) by DNS based on RFC4120-way.
However, DNS will be used by kerberos-related part only.
Most application will not use DNS as described above.

If DHCP can advertise KDC-related information instead of DNS, there are the following advantages.
1) It can reduce messages handled by the field devices.
Consequently, it can reduce footprint of the field devices.
2) It can reduce the number of servers.
Consequently, it contribute to management cost of the systems.

6. References

There have been multiple technologies for field devices.
Examples:
- FOUNDATION Fieldbus (http://www.fieldbus.org/)
- PROFIBUS (http://www.profibus.com/)
- BACnet (http://www.bacnet.org/)
- LonWorks (http://www.echelon.co.jp/products/lonworks.html)
- Modbus (http://www.modbus.org/)

You can learn about communication technology of field devices with wikipedia:
- http://en.wikipedia.org/wiki/Fieldbus
- http://en.wikipedia.org/wiki/BACnet
- http://en.wikipedia.org/wiki/LonWorks

Authors' Addresses

Shoichi Sakane
Cisco Systems
2-1-1 Nishi-Shinjuku, Shinjuku-ku,
Tokyo 163-0409 Japan
E-mail: ssakane@cisco.com

Masahiro Ishiyama
Toshiba Corporation
1, komukai-toshiba-cho, Saiwai-ku,
Kawasaki 212-8582 Japan
E-mail: masahiro@isl.rdc.toshiba.co.jp