                      Kerberos Options for DHCPv6
                   draft-sakane-dhc-dhcpv6-kdc-option-18.txt

Abstract

   This document defines four new options for the Dynamic Host
   Configuration Protocol for IPv6 (DHCPv6). These options are used to
   carry coniguration information for Kerberos.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

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

   When a client wishes to communicate with, and be authenticated to, a
   Kerberos application server (also a client of the KDC), the client
   identifies itself, and its realm, to the KDC and acquires a
   credential from the KDC. The client then presents the credential to
   the Kerberos application server which can use the credential to
   authenticate the client. The client needs to know at least one IP
   address for a KDC in order to initiate this process.

   One example of the application of this protocol is as follows. A
   student might want to use a shared, public workstation, one that is
   not configured for Kerberos. If there is a mechanism for the
   workstation to obtain a realm name and IP address for a KDC, then a
   student need only input a user-id and pass phrase to be able to use
   Kerberos.

   The Kerberos V5 specification [RFC4120] defines the use of DNS SRV
   records [RFC2782] for KDC discovery. Some systems, such as
   industrial systems, do not use DNS. Such systems already have their
   own name spaces and their own name resolution systems, including pre-
   configured mapping tables for devices, and do not use Fully Qualified
   Domain Names. However, many of these systems do use DHCP.

   Adding a DNS server to such systems may decrease the reliability of
   the system and increase the management cost. In such an environment,
   another mechanism is needed to provide an IP address for the KDC.
   For the PacketCable Architecture [PCARCH], RFC 3634 [RFC3634] defines
   the KDC Server Address sub-option for the DHCPv4 CableLabs Client
   Configuration option. However, a mechanism is still needed to
   provide a realm name and an IPv6 address, one which does not depend
   on any external architecture.

   This document defines a Kerberos option for DHCPv6 which provides a
   realm name and/or a list of KDC IP addresses. This option does not
   replace or modify any of the existing methods for obtaining this
   information.

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], Kerberos V5 [RFC4120], and
DNS SRV [RFC2782].

3. **Kerberos Options**

   This document defines four DHCPv6 configuration parameters for
   Kerberos.

      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 in that option.

   These options except of the Kerberos KDC Option MUST NOT appear more
   than once in a DHCPv6 message.

3.1. **Kerberos Principal Name Option**

   The Kerberos Principal Name Option carries the name of a Kerberos
   principal. This is sent by the client to the DHCPv6 server which MAY
   use it to select a specific set of configuration parameters, either
   for a client or for a Kerberos application server.

   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)                      :
   :                                                               :
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

   o option-len (16-bit): length of the principal-name field.

   o principal-name (variable): a client principal name. The encoding
      of the principal-name field MUST conform to the definition of
      "PrincipalName" in section 5.2.2 of RFC 4120 [RFC4120].

3.2. Kerberos Realm Name Option

   The Kerberos Realm Name Option carries a Kerberos realm name. A
   DHCPv6 client uses this option to specify to a DHCPv6 server which
   realm the client wants to access.

   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)   :
      :   :
      +-+

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

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

   o   realm-name (variable): a realm-name. The encoding of the realm-
       name field MUST conform to the definition of "Realm" in section
       5.2.2 of RFC 4120 [RFC4120].

3.3. Kerberos Default Realm Name Option

   The Kerberos Default Realm Name Option is used to specify a default
   realm name for the Kerberos system. A DHCPv6 server uses this option
   to specify the default realm name to both clients and Kerberos
   application servers.

   The option-code of this option is OPTION_KRB_DEFAULT_REALM_NAME (TBD
   by IANA). The format and usage of the option-len and realm-name
   fields are identical to those for the Kerberos Realm Name Option.

3.4. Kerberos KDC Option

   The Kerberos KDC Option is used to provide 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)                     :
      :                                                              :
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
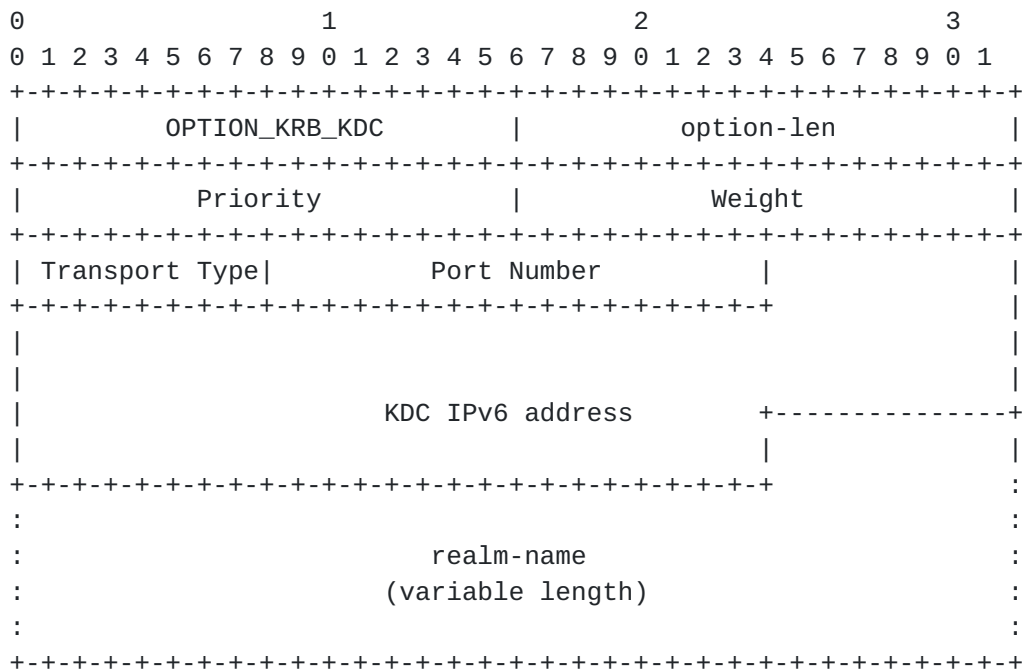
o option-code (16-bit): OPTION_KRB_KDC (TBD by IANA)

o option-len (16-bit): 23 + the length of the realm-name field in
   octets.

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

o Weight (16-bit): the Priority and Weight fields provide a hint to
   the client as to which KDC to select. The usage of the Priority
   and Weight values MUST follow the specification for DNS SRV
   [RFC2782].

o Transport Type (8-bit): The Transport Type specifies the transport
   protocol used for Kerberos. Kerberos [RFC4120] defines UDP and
   TCP transports. Exchanges over TCP are further described in
   [RFC5021] while the transport of Kerberos over TLS is 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): the port number on which the KDC listens.

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

   o realm-name (variable): the name of the realm for which the
      specified KDC provides service. The encoding of the realm- name
      field MUST conform to the definition of "Realm" in section 5.2.2
      of RFC 4120 [RFC4120].

4. **Client and Server Operation**

   This section describes the operations of client and server. It
   assumes that the client has been configured with a principal name.

   If a client requires a realm name, the client sends a DHCPv6 Option
   Request option (ORO) specifying the Kerberos Default Realm Name
   Option. The DHCPv6 server responds with a Reply message containing a
   Kerberos Default Realm Name Option.

   If a client requires configuration parameters for a KDC, the client
   sends a DHCPv6 ORO specifying the Kerberos KDC Option. The client
   MAY include a Kerberos Principal Name Option. The client MAY include
   a Kerberos Realm Name Option.

   The DHCPv6 server replies with one or more sets of configuration
   parameters for a Kerberos KDC. If the client has specified either a
   Kerberos Principal Name Option or a Kerberos Realm Name Option, then
   the DHCPv6 server MAY use those parameters to select specific sets of
   configuration parameters.

   Where the server replies with more than one set of configuration
   paramers, the usage of priority and weight fields by the client MUST
   follow the specification for DNS SRV [RFC2782].

   The client MAY include other options with data values as hints to the
   DHCPv6 server about parameter values the client would like to have
   returned; this is specified in section 18.1.5 of RFC 3315 [RFC3315].

4.1. **KDC discovery for a client**

   When a client implements both the DNS method defined by section
   7.2.3.2 of [RFC4120] and the DHCP method defined by this document,
   the choice of method is determined by local policy. The
   administrator of the realm usually defines the method as part of the
   configuration of the client before the client is installed.

   When no criteria have been specified and the client could get the
   Kerberos information from either the DNS server or the DHCPv6 server,
   then the information from DNS SHOULD be preferred.

5. 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 create a sub-registry of Kerberos Message
   Transport Type, under the Kerberos Parameters Registry. The initial
   entries are described in section 3.4.

   The assignment of future entries is by "IETF Review" policy as
   described in BCP 26 [RFC5226]. The RFC specifies the symbolic name
   of such entries which are assigned numeric codes by IANA once
   publication is approved.

6. Security Considerations

   The security considerations in RFC 3315 [RFC3315] apply.

   DHCPv6 messages can be modified in transit. If an adversary modifies
   the response from a DHCPv6 server or injects its own response, a
   client may be led into contacting a malicious KDC. Both cases are
   categorized as a Denial of Service (DoS) attack. However, a
   malicious KDC does not know the shared key and so is unable to
   proceed any further with the exchange. If a client receives a
   response from such a KDC, the client can use the shared key to detect
   that the message originates from a malicious KDC.

   A shared, unconfigured workstation may obtain its KDC information,
   and default realm, via DHCPv6. Such a workstation may not have a
   host or other service key, and thus be unable to validate the Ticket-
   Granting Ticket issued by the KDC. A modified DHCPv6 response would
   then result in the workstation talking to a malicious KDC and be
   unable to detect that has happened. This in turn could allow access
   by unauthorized users.

   To minimize potential vulnerabilities, a client SHOULD use DHCPv6
   authentication as defined in section 21 of RFC 3315 [RFC3315].

   Kerberos information may be manually configured into the client
   before requesting information from DHCPv6. Manual configuration of
   the device SHOULD be preferred to configuration via the DHCPv6
   server.

7. Acknowledgments

   The authors are very grateful to Nobuo Okabe and Shigeya Suzuki.
   They contributed the explanation as to why DNS is inappropriate for
   some industry networks. Ted Lemon made many suggestions to improve
   DHCP aspects of this specification. Ken'ichi Kamada and Yukiyo
   Akisada contributed to the initial work on this document. Tom Petch
   helped to improve the readability of this document. The authors also
   thank Jeffrey Hutzelman, Kazunori Miyazawa, Kensuke Hosoya, Nicolas
   Williams, Nobumichi Ozoe, Sam Hartman, and Stephen Farrell. They
   made valuable comments and suggestions.
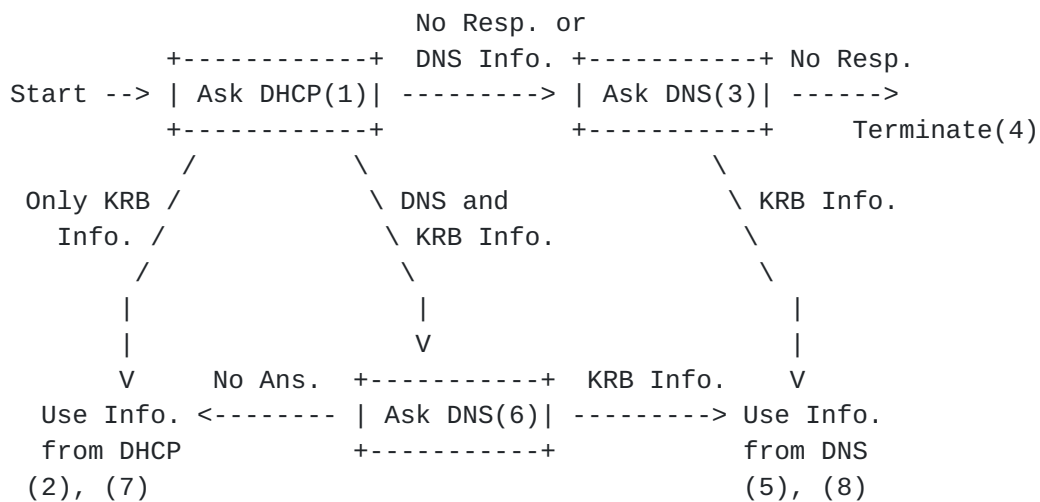
8. References

8.1. Normative References

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

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

[RFC3315]   Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,
            and 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.

[RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
            IANA Considerations Section in RFCs", BCP 26, RFC 5226,
            May 2008.

8.2. Informative References

[PCARCH]   CableLabs, "PacketCable 1.0 Architecture Framework
            Technical Report", December 1999, <http://
            www.packetcable.com/downloads/specs/
            pkt-tr-arch-v01-991201.pdf>.

[RFC3634]   Luehrs, K., Woundy, R., Bevilacqua, J., and 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.

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

Appendix A. An example of the operation of the client

   When no criteria have been specified and the client could get the
   Kerberos information from either the DNS server or the DHCPv6 server,
   then the information from DNS should be preferred. The following is
   an informational guide for the client in such an environment.

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


         Abbreviations:
           Resp.: Response
           Info.: Information
           KRB  : Kerberos
```

1) Initially, the client requests both DNS and Kerberos information
   from the DHCPv6 server.

2) If the DHCPv6 server replies with Kerberos information and not
   with DNS information, then the client uses that information.

3) If the DHCPv6 server does not reply or replies with only DNS
   information, then the client requests Kerberos information from
   the DNS server.

4) If the client gets no response or no Kerberos information from the
   DNS server, then the client terminates the process.

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

6) If, as the result of (1), the DHCPv6 server replies with both DNS
   and Kerberos information, then the client requests Kerberos
   information from the DNS server.

7) If the client gets no response from the DNS server, then the
   client uses the Kerberos information from the DHCPv6 server.

8) If, as the result of (6), the DNS server replies with Kerberos
   information, then the client uses the information from the DNS
   server and not that from the DHCPv6 server.

Authors' Addresses

    Shoichi Sakane
    Cisco Systems
    9-7-1 Akasaka
    Minato-ku, Tokyo 107-6227
    Japan

    Email: ssakane@cisco.com

    Masahiro Ishiyama
    Toshiba Corporation
    1, komukai-toshiba-cho, Saiwai-ku,
    Kawasaki, Kanagawa 212-8582
    Japan

    Email: masahiro.ishiyama@toshiba.co.jp