CAPWAP Access Controller DHCP Option
draft-ietf-capwap-dhc-ac-option-01

Status of this Memo

Abstract

   The Control And Provisioning of Wireless Access Points Protocol
   allows a Wireless Termination Point to use DHCP to discover the
   Access Controllers it is to connect to. This document describes the
   DHCP options to be used by the CAPWAP protocol.

Table of Contents

1. Introduction

The Control And Provisioning of Wireless Access Points Protocol
(CAPWAP) [I-D.ietf-capwap-protocol-specification] allows a Wireless
Termination Point (WTP) to use DHCP to discover the Access
Controllers (AC) it is to connect to.

Prior to the CAPWAP Discovery process, the WTP MAY use one of many
methods to identify the proper AC to establish a CAPWAP connection
with. One of these methods is through the DHCP protocol. This is
done through the CAPWAP AC DHCPv4 or CAPWAP AC DHCPv6 Option.

1.1. Conventions used in this document

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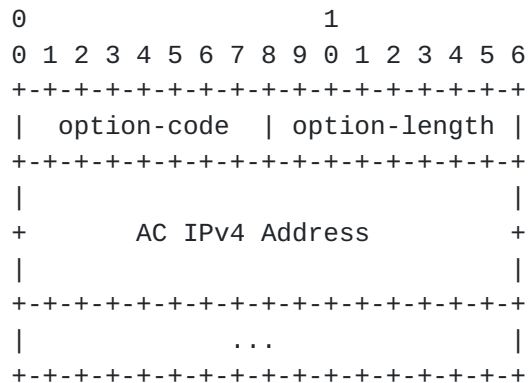document are to be interpreted as described in RFC 2119 [RFC2119].

1.2. Terminology

This document uses terminology defined in [RFC3753] and
[I-D.ietf-capwap-protocol-specification].

2. **CAPWAP AC DHCPv4 Option**

   This section defines a DHCPv4 option that carries a list of 32-bit
   (binary) IPv4 addresses indicating one or more CAPWAP AC available to
   the WTP.

   The DHCPv4 option for CAPWAP has the format shown in the following
   figure:

```
       0                   1
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |  option-code  | option-length |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                               |
       +        AC IPv4 Address        +
       |                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |             ...               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   option-code: OPTION_CAPWAP_AC_V4 (TBD)

   option-length: Length of the 'options' field in octets; MUST be a
      multiple of four (4).

   AC IPv4 Address: IPv4 address of a CAPWAP AC which the WTP may use.
      The ACs are listed in the order of preference for use by the WTP.

   A CAPWAP WTP, acting as a DHCPv4 client, SHOULD request the CAPWAP AC
   DHCPv4 Option in a Parameter Request List as described in [RFC2131]
   and [RFC2132].

   If configured with a (list of) CAPWAP AC address(es), a DHCPv4 server
   SHOULD send the client the CAPWAP AC DHCPv4 option, even if this
   option is not explicitly requested by the client.

   A CAPWAP WTP, acting as a DHCPv4 client, receiving the CAPWAP AC
   DHCPv4 option MAY use the (list of) IP address(es) to locate AC. The
   CAPWAP protocol [I-D.ietf-capwap-protocol-specification] provides
   guidance on the WTP's discovery process.

   The WTP, acting as a DHCPv4 client, SHOULD try the records in the
   order listed in the CAPWAP AC DHCPv4 option received from the DHCPv4
   server.

3. CAPWAP AC DHCPv6 Option

   This section defines a DHCPv6 option that carries a list of 128-bit
   (binary) IPv6 addresses indicating one or more CAPWAP AC available to
   the WTP.

   The DHCPv6 option for CAPWAP has the format shown in the following
   figure:

```
    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-code           |          option-length        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                      AC IPv6 Address                          +
   |                                                               |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                             ....                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   option-code: OPTION_CAPWAP_AC_V6 (TBD)

   option-length: Length of the 'options' field in octets; MUST be a
      multiple of sixteen (16).

   AC IPv6 Address: IPv6 address of a CAPWAP AC which the WTP may use.
      The ACs are listed in the order of preference for use by the WTP.

   A CAPWAP WTP, acting as a DHCPv6 client, SHOULD request the CAPWAP AC
   DHCPv6 Option in a Parameter Request List as described in [RFC2131]
   and [RFC2132].

   If configured with a (list of) CAPWAP AC address(es), a DHCPv6 server
   SHOULD send the client the CAPWAP AC DHCPv6 option, even if this
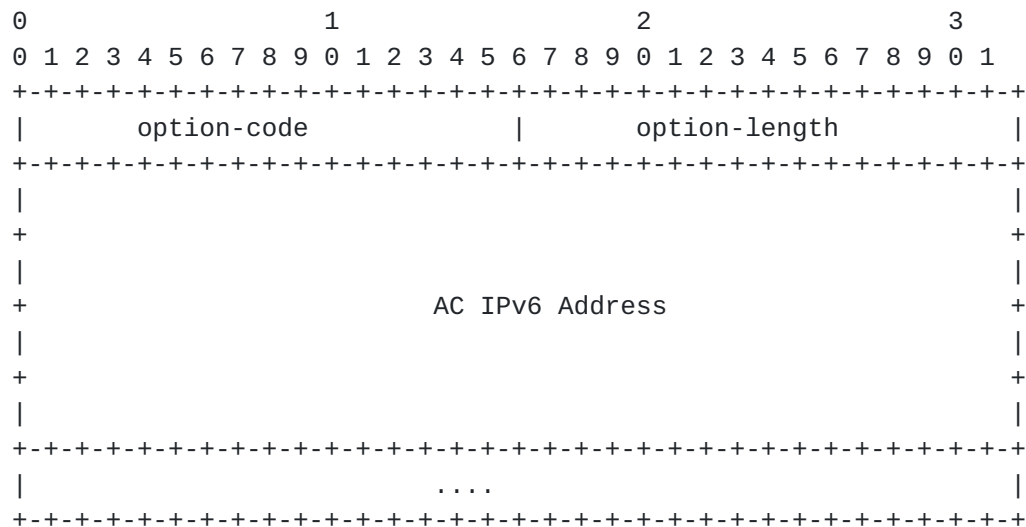   option is not explicitly requested by the client.

   A CAPWAP WTP, acting as a DHCPv6 client, receiving the CAPWAP AC
   DHCPv6 option MAY use the (list of) IP address(es) to locate AC. The
   CAPWAP protocol [I-D.ietf-capwap-protocol-specification] provides
   guidance on the WTP's discovery process.

   The WTP, acting as a DHCPv6 client, SHOULD try the records in the
   order listed in the CAPWAP AC DHCPv6 option received from the DHCPv6

server.

4. IANA Considerations

The following DHCPv4 option code for CAPWAP AC option MUST be assigned by IANA:

```
        Option Name            Value        Described in
        ------------------------------------------------
        OPTION_CAPWAP_AC_V4    TBD          Section 2
```

The following DHCPv6 option code for CAPWAP AC options MUST be assigned by IANA:

```
        Option Name            Value        Described in
        ------------------------------------------------
        OPTION_CAPWAP_AC_V6    TBD          Section 3
```

5. Security Considerations

   The security considerations in [RFC2131], [RFC2132] and [RFC3315]
   apply. If an adversary manages to modify the response from a DHCP
   server or insert its own response, a WTP could be led to contact a
   rogue CAPWAP AC, possibly one that then intercepts call requests or
   denies service. CAPWAP's use of DTLS MUST be used to authenticate
   the CAPWAP peers in the establishment of the session.

   In most of the networks, the DHCP exchange that delivers the options
   prior to network access authentication is neither integrity protected
   nor origin authenticated. Therefore, the options defined in this
   document are not the only methods used to determine which AC a WTP
   should connect to. The CAPWAP protocol
   [I-D.ietf-capwap-protocol-specification] defines other AC discovery
   procedures a WTP MAY utilize.

6. **Acknowledgements**

   The following individuals are acknowledged for their contributions to
   this protocol specification: Ralph Droms, Margaret Wasserman.

7. References

7.1. Normative References

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

   [RFC2131] Droms, R., "Dynamic Host Configuration Protocol",
              RFC 2131, March 1997.

   [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor
              Extensions", RFC 2132, March 1997.

   [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.

   [I-D.ietf-capwap-protocol-specification]
              Calhoun, P., "CAPWAP Protocol Specification",
              draft-ietf-capwap-protocol-specification-10 (work in
              progress), March 2008.

7.2. Informational References

   [RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology",
              RFC 3753, June 2004.

Author's Address

   Pat R. Calhoun
   Cisco Systems, Inc.
   170 West Tasman Drive
   San Jose, CA 95134

   Phone: +1 408-853-5269
   Email: pcalhoun@cisco.com

Full Copyright Statement

Intellectual Property