EMU Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 January 2026

E. Lear
Cisco Systems, Inc.
A. Dekok
InkBridge Networks

5 July 2025

New TEAP TLV for Encapsulating DHCPv6 Options
draft-lear-teap-config-options-00

Abstract

This document defines a new Tunneled Extensible Authentication Protocol (TEAP) Type-Length-Value (TLV) to encapsulate DHCPv6 (Dynamic Host Configuration Protocol Version 6) options within TEAP authentication exchanges. This enhancement enables exchange of network configuration parameters after the authentication phase.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://elear.github.io/teap-config-options/main/draft-lear-teap-config-options.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-lear-teap-config-options/.

Discussion of this document takes place on the EMU WG Working Group mailing list (mailto:emu@ietf.org), which is archived at https://example.com/WG. Subscribe at https://www.ietf.org/mailman/listinfo/emu/.

Source for this draft and an issue tracker can be found at https://github.com/elear/draft-lear-teap-config-option.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

TEAP (Tunneled Extensible Authentication Protocol), defined in [I-D.ietf-emu-rfc7170bis], supports the use of Type-Length-Value (TLV) structures to exchange additional data during the authentication process. DHCPv6 [RFC8415] is widely used for configuration of network parameters. This document introduces a new TLV to encapsulate DHCPv6 options within TEAP messages.

[RFC9445] specifies a way to communicate DHCPv6 options to a RADIUS client. This memo specifies a means to communicate options end-to-end between the authentication server and the peer.

Not all DHCP communications will necessarily make sense in this context. For instance, an AAA server may only wish to send non-topological options, such as a definitions for a print server, or next hop configuration URL. It might not send next-hop router or IP address binding information.

Sending options in a protected and authenticated TLS tunnel also authenticates the options, and allows them to be transmitted securely from the authentication server to the peer. While [RFC8415], Section 20 provides for authentication of DHCP messages, this feature is not always used. Even if the DHCP messages are authenticated, there are still benefits to sending options inside of a protected TEAP session.

1.1. Use of both DHCPv6 and TEAP protocols

Because DHCPv6 is widely deployed, peers implementing this specification can expect to receive information via both TEAP and DHCPv6. Therefore, the possibility of a conflict arises. Clients are not in a good position to determine on their own which information is correct. Therefore, the following strategy is RECOMMENDED:

1. Peers receiving information only via DHCP will use that information.

2. Peers receiving DHCP information only via TEAP will use that information.

3. Peers receiving overlapping DHCPv6 options SHOULD select TEAP information since it is likely to be better authenticated and unchanged.

4. If conflicting information is received by the peer it SHOULD log the conflict as an error and MAY produce an exception.

In practice, these rules can be applied by a peer initializing a result option list by using the options which are received from TEAP, and then selectively adding options from DHCP. Before adding a DHCP option, the peer checks (by number) if the option already exists in the result option list. If no matching option exists, it is added. If a matching option exists, the values are compared, and a log message can be generated.

It is RECOMMENDED that conflict be avoided by having the DHCP server send options which control network behavior (address assignment, routes, etc). The TEAP server can then send options which require the peer to follow a particular policy. The detailed list of which options fall into which category is site-specific, and out of scope of this specification.

2. TEAP TLV for DHCPv6 Options

DHCPv6 options are carried within the DHCPv6-Options TLV. The TLV format is defined below.

Both the TEAP server and TEAP client MAY transmit this TLV during Phase 2, and it MAY be included in a Request Action frame. The Mandatory bit MUST not be set. If either side sends this TLV prior to Phase 2, an error TLV of 2002 (Unexpected TLVs Exchanged) be returned with a Result of Status=Failure. That is, the table in Section 4.3.1 of [I-D.ietf-emu-rfc7170bis] remains unchanged.

Thus this TLV MAY be used as follows:

Request	Response	Success	Failure	TLV
0-1	0-1	0-1	0	DHCPv6-Options

Table 1: When is this TLV Allowed

A TEAP peer or server receiving this TLV SHOULD NOT act on it until the other side has been sufficiently authenticated, but it is not an error to send this TLV in advance of such authentication. In this way, the TLV can be conveniently piggybacked as part of the authentication prior to a result or intermediate result being generated.

2.1. TLV Format

The DHCPv6-Options TLV follows the TEAP TLV format from [I-D.ietf-emu-rfc7170bis], Section 4.2.1, and is defined below:

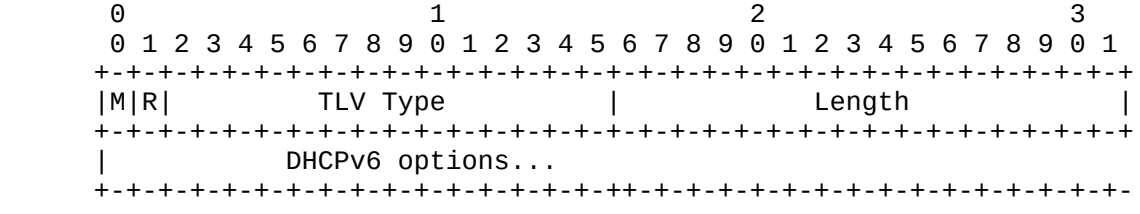

Figure 1: DHCP options TLV format

M

0 - Optional TLV

R

Reserved, set to zero (0)

TLV Type

TBD - DHCPv6 options

Length

>=2 octets

DHCPv6 options

This field MUST contain DHCPv6 options, as defined in {{RFC8415, Section 21.1}}.

2.1.1. DHCPv6 Option Encapsulation

The TLV Value field encapsulates DHCPv6 options exactly as they appear in DHCPv6 messages. There MUST NOT be more than one DHCPv6-Options TLV in a TEAP exchange. The TEAP TLV format is sufficient to carry any number of DHCPv6 options which may be needed.

A party which receives multiple DHCPv6-Options TLVs during a TEAP exchange SHOULD process only the first such option, and then ignore all remaining ones.

The format adheres to the standard DHCPv6 option encoding, ensuring compatibility with existing DHCPv6 implementations.

Encapsulating this option in the TLV would look as follows (in hexadecimal):

Type: 0xXXXX (TBD assigned by IANA)
Length: 0x0014
Value: 0x00170010FE8000000000000000000000000001

Where:

* Type = 0xXXXX (TBD assigned by IANA)

* Length = 0x0014 (20 bytes for the "Recursive DNS Servers" option, including addresses)

* Value = 0x00170010FE800000000000000000000000000001 (DHCPv6 Option 23 with an IPv6 address of FE80::1).

3. Security Considerations

Encapsulating DHCPv6 options within TEAP messages inherits the security guarantees of the TEAP protocol. Further details on mitigation strategies are discussed in [I-D.ietf-emu-rfc7170bis].

Sending DHCPv6 options withing a protected and authenticated TLS tunnel provides for additional authentication of those options, and for exchanging the options in a secure manner. While DHCPv6 provides for message authentication, that functionality is not always available.

This feature also enables better separation of responsibilities. A DHCPv6 server can simply manage address assignment and network configuration. The TEAP authentication server can then manage higher level network policies.

3.1. Additional Policy Decisions

DHCP clients can send options which indicate their desired network posture. An authentication server can then make policy decisions based on the options, such as placing the device into a different VLAN.

3.2. Captive Portals and Provisioning

TEAP provides for unauthenticated access for provisioning. The DHCPv6-Options TLV can be used within a provisioning network without issue.

4. IANA Considerations

IANA is requested to assign a new TEAP TLV type value for the DHCPv6 Options TLV from the TEAP TLV Type registry defined in [I-D.ietf-emu-rfc7170bis].

5. Acknowledgements

The authors hope to thank the members of the IETF EMU Working Group for their valuable input and contributions.

6. References

6.1. Normative References

[I-D.ietf-emu-rfc7170bis]
DeKok, A., "Tunnel Extensible Authentication Protocol (TEAP) Version 1", Work in Progress, Internet-Draft, draft-ietf-emu-rfc7170bis-22, 28 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-emu-rfc7170bis-22>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/rfc/rfc8415>.

6.2. Informative References

[RFC9445] Boucadair, M., Reddy.K, T., and A. DeKok, "RADIUS Extensions for DHCP-Configured Services", RFC 9445, DOI 10.17487/RFC9445, August 2023, <https://www.rfc-editor.org/rfc/rfc9445>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Eliot Lear
Cisco Systems, Inc.
Richtistrasse 7
CH-8304 Wallisellen
Switzerland
Phone: +41 44 878 9200
Email: lear@cisco.com

Alan Dekok
InkBridge Networks
Email: alan.dekok@inkbridge.io