

DHCP Continuation Option Code
<[draft-ietf-dhc-options-cont-00.txt](#)>

Status of this memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``[id-abstracts.txt](#)'' listing contained in the Internet-Drafts Shadow Directories on [ftp.is.co.za](#) (Africa), [nic.nordu.net](#) (Europe), [munnari.oz.au](#) (Pacific Rim), [ds.internic.net](#) (US East Coast), or [ftp.isi.edu](#) (US West Coast).

Abstract

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. Currently options are limited to an information size of 256 bytes because of the one-octet size of the length field. This document defines a new option that permits the continuation of the previous option information.

1. Introduction

The Dynamic Host Configuration Protocol (DHCP) [[1](#)] provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the 'options' field of the DHCP message. The data items themselves are also called "options."

Each option is assigned a one-octet option code and an one-octet size field. The one-octet size field limits the information contained in an option to 256 bytes. While there exist options that permit the use of the sname and file fields of the header, these options only add an additional 192 bytes when the fields are not in use. This document

describes a new DHCP option for continuing the information from the previous option. This option **MUST** not appear as the first option in a message. The option preceding this one **MUST** have a size of 256 bytes.

2. Definition of option [TBD]

Option code [TBD] indicates that the data contained in the option is a continuation of the previous option.

```

          Continuation
Code   Len  option code  Data...
+-----+-----+-----+-----+-----+-----+-----+-----+
| TBD | XXX | Continuation of previous option data
+-----+-----+-----+-----+-----+-----+-----+-----+

```

The example below shows how the option would work with a hypothetical authentication option that requires more than 255 bytes of information.

```

          Auth
Code   Len  option Data...
+-----+-----+-----+-----+-----+-----+-----+-----+
| 90 | 256 | 04 | d1    d2    d4    ... d255
+-----+-----+-----+-----+-----+-----+-----+-----+
Code   Len  Data...
+-----+-----+-----+-----+-----+-----+-----+-----+
| TBD | 20 | d257 d258 d259 d260 ... d276
+-----+-----+-----+-----+-----+-----+-----+-----+

```

4. References

- [1] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), Bucknell University, March 1997.
- [2] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), Lachman Associates, March 1997.

5. Security Considerations

DHCP currently provides no authentication or security mechanisms. Potential exposures to attack are discussed in [section 7](#) of the DHCP protocol specification [[1](#)]. One of the reasons for this definition is to provide support for the exchange of public key certificates are which usually larger than 256 bytes.

6. Author's Address

William A. Arbaugh
Angelos D. Keromytis
Distributed Systems Lab -- 102 Moore
Department of Computer and Information Sciences
University of Pennsylvania
200 South 33rd St.
Philadelphia, PA. 19104-6389

Email: {waa, angelos}@dsl.cis.upenn.edu