DHCPv4 Vendor-specific Message
<draft-volz-dhc-dhcpv4-vendor-message-00.txt>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 8, 2009.

Abstract

This document requests a vendor-specific DHCPv4 message assignment. This message can be used for vendor specific and experimental purposes.
1. Introduction

The DHCPv4 [RFC2131] protocol specifies a mechanism for the assignment of addresses and configuration information to nodes. The protocol provides for 256 possible message codes, of which a small number are assigned ([DHCPv4Params]). Each of the assigned message codes have specific purposes. New message codes are assigned through IETF Standards Action.

There may be a need for vendors of DHCPv4 clients, relay agents, or servers to experiment with new capabilities that require new messages to be exchanged between these elements. Thus, this document defines the format for and requests that a new message code be reserved for vendor-specific and experimental purposes.

2. Terminology

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 [RFC2119].

3. Vendor-specific Message

The vendor-specific message may be exchanged between clients, relay agents, and/or servers and allows multiple vendors to make use of the message for completely different and independent purposes.

Clients and servers MAY chose to support this message; those that do not, MUST discard the message. Relay agents SHOULD relay these messages as they would other DHCPv4 messages unless the relay agent understands the specific message and knows that the message was directed at it.

Applications using these messages MUST NOT assume that all DHCPv4 clients, relay agents, and servers support them and MUST use good networking practices when transmitting and retransmitting these messages. For some applications, it may be appropriate to use Vendor-Identifying Vendor Options [RFC3925] in a standard DHCPv4 exchange to negotiate whether the end-points support the vendor-specific message.

A vendor-specific message is constructed by placing the Vendor-Specific Message number (254) into the DHCP Message Type option [RFC2132] and including the Vendor Message Option defined below. A Vendor-Specific Message that does not contain the Vendor Message Option MUST be ignored. A Vendor Message Option in a DHCPv4 message
other than the Vendor-Specific Message MUST be ignored.

The format of the Vendor Message Option is shown below:

```
  1 1 1 1 1 1
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
  +-----------------------------+
  | option-code    | option-len |
  +-----------------------------+
  | enterprise-number          |
  +-----------------------------+
  /  vendor-message-data  /  ~
  ~  ...  ~
  +-----------------------------+
```

- **option-code**          OPTION_VENDOR_MESSAGE (TBD)
- **option-len**           4 plus the length of the vendor-message-data.
- **enterprise-number**    The vendor’s 32-bit Enterprise Number as registered with [EID], in network octet order.
- **vendor-message-data**  Vendor specific data (of length option-len - 4 octets).

The contents and format of the vendor-message-data field is up to the vendor.

Clients, relay agents, and/or servers supporting the Vendor Message Option MUST support [RFC3396].

Note: Vendor-Identifying Vendor Options [RFC3925] are not used to convey the vendor identification (enterprise-number) for the vendor-specific message as the message may contain instances of those options for other reasons.

4. Security Considerations

The Security Considerations of [RFC2131] apply.

This new message does potentially open up new avenues of attacking clients, relay agents, or servers. The exact nature of these attacks will depend on what functions and capabilities the message exposes and are thus not possible to describe in this document. Clients and
servers that have no use for these messages SHOULD discard them and thus the threat is no different than before this message was assigned.

Vendors using this new message should use the DHCPv4 security mechanisms (such as [RFC3118] as appropriate) and carefully consider the security implications of the functions and capabilities exposed.

5. IANA Considerations

IANA is requested to assign DHCPv4 Message type 254 to the Vendor-specific Message in the registry maintained in [DHCPv4Params]:

254 VENDOR-SPECIFIC

IANA is requested to assign a DHCPv4 option number to the Vendor Message Option in the registry maintained in [DHCPv4Params]:

TBD OPTION_VENDOR_MESSAGE

6. References

6.1. Normative References


6.2. Informative References


[RFC3925] Littlefield, J., "Vendor-Identifying Vendor Options for


Author’s Address

Bernard Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA  01719
USA

Phone: +1 978 936 0000
Email: volz@cisco.com
Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.