DHC Working Group
Internet Draft
Intended status: Informational
Expires: May 2009

November 3, 2008
Vincent Zimmer
Intel Corporation
Dave Thaler
Microsoft

DHCPv6 Remote Boot Options

draft-zimmer-dhc-dhcpv6-remote-boot-options-01.txt

Status of this Memo

Abstract

This document describes a means by which to support network boot of a bare-metal platform utilizing a pre-boot execution environment, such as the Unified Extensible Firmware Interface [UEFI22]. The problem being addressed is that the PXE [PXE21] and UEFI Specifications [UEFI22] only describe how to ascertain boot configuration options using DHCPv4 [RFC2131], not for DHCPv6 [RFC3315]. Similarly, iSCSI boot [RFC4173] does not specify how to discover boot device information in an DHCPv6 environment. This document will describe

how to ascertain this boot information in an IPv6 environment utilizing options in the DHCPv6 hand-off [RFC3315].

Table of Contents

1. Introduction

Many hosts today have the ability to boot an Operating System image (or "boot file") that is located on a server in the network. To do so, the host must begin with some functionality just sufficient to be able to get on the network and retrieve the boot file. As indicated in Figure 1, it is desirable to obtain from DHCP the information needed to locate the boot file, so that by the time the host is able to communicate on the network, it can immediately begin downloading the boot file.

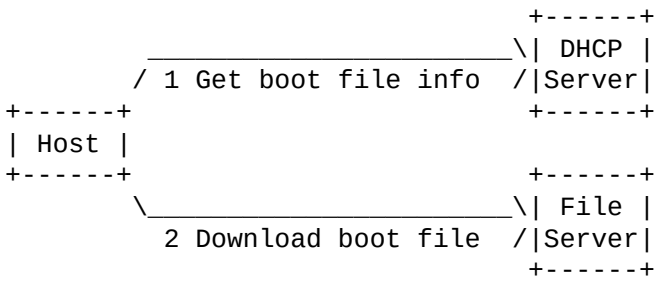


Figure 1: Network Boot Sequence

Two methods for downloading a boot file are specified today.

- o iSCSI: [RFC2132] specifies a DHCPv4 option for retrieving boot file information and [RFC4173] specifies how to download the boot file.

- o TFTP: [RFC2132] and [RFC4578] specify DHCPv4 options for retrieving boot file information and [RFC1350] specifies how to download the boot file.

The problem with both is that while the methods for downloading the boot files can work over either IPv4 or IPv6, the boot file info can only be obtained over DHCPv4. As a result, they do not support a network that only provides IPv6, nor do they support IPv6-only devices. To address this gap, this document specifies DHCPv6 options that provide parity with the DHCPv4 options.

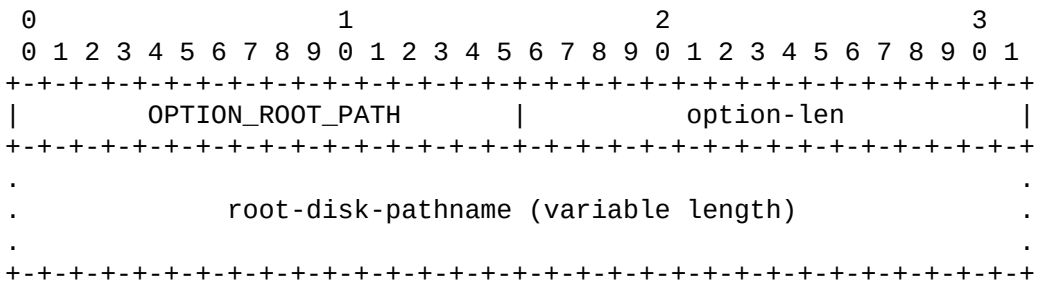
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. DHCPv6 Options

2.1. Root Path Option

The Root Path option specifies the path-name that contains the client's root disk. The path is formatted as a character string consisting of characters from the NVT ASCII character set.

This option provides parity with the Root Path Option defined for DHCPv4 in [RFC2132] section 3.19.



option-code OPTION_ROOT_PATH (TBD1).

option-len Length of Root Path Name in octets.

root-disk-pathname See below

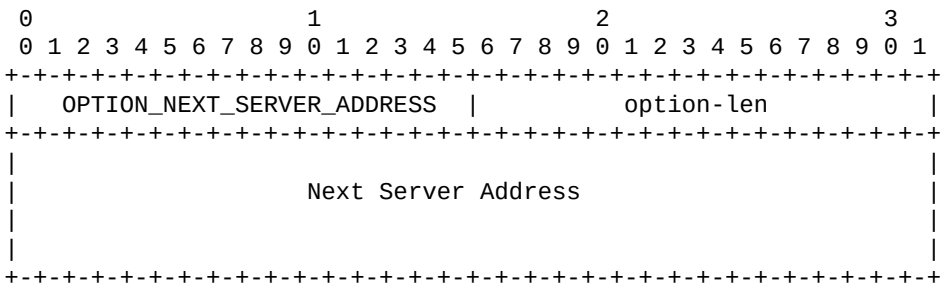
This NULL-terminated ASCII string is the URL (conforming to [RFC2396]) to a boot file. This string starts with the protocol which is used for downloading. Separated by '://', the hostname or IPv6 address of the server hosting the boot file (see also the note below), the path, file name and query parts of the URL follow. For iSCSI, the format of the URL is specified in [RFC4173] section 5.

2.2. Next Server Address Option

This option conveys the address of the server to use in the next step of the client's bootstrap process. A DHCP server may return its own address in this option, if the server is prepared to supply the next bootstrap service (e.g., delivery of an operating system executable image).

This option provides parity with the siaddr field in DHCPv4.

The format of the option is:



option-code OPTION_NEXT_SERVER_ADDRESS (TBD3).

option-len 16

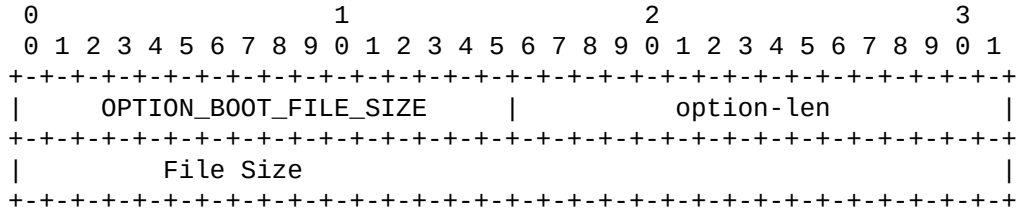
Next Server Address The IPv6 address or IPv4-mapped address of the next server

2.3. Boot File Size Option

This option specifies the length in 512-octet blocks of the default boot image for the client. The file length is specified as a 32-bit integer.

This option provides parity with the Boot File Size Option defined for DHCPv4 in [RFC2132] section 3.15.

The format of the option is:



option-code OPTION_BOOT_FILE_SIZE (TBD4).

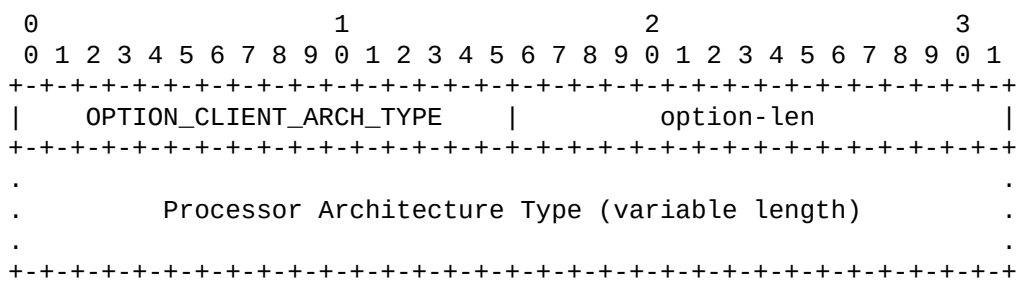
option-len 4

File Size The length in 512-octet blocks of the boot image for the client.

2.4. Client System Architecture Type Option

This option provides parity with the Client System Architecture Type Option defined for DHCPv4 in [RFC4578] section 2.1.

The format of the option is:



option-code OPTION_CLIENT_ARCH_TYPE (TBD5).

option-len See below.

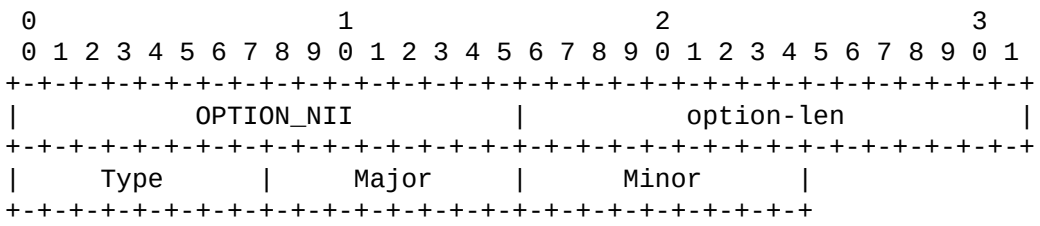
Processor Architecture Type	A list of one or more architecture types, as specified in [RFC4578] section 2.1.

2.5. Client Network Interface Identifier Option

The Client Network Interface Identifier option is sent by a DHCP client to a DHCP server to provide information about its level of Universal Network Device Interface (UNDI) support.

This option provides parity with the Client Network Interface Identifier Option defined for DHCPv4 in [RFC4578] section 2.2.

The format of the option is:



option-code OPTION_NII (TBD6).

option-len 3

Type As specified in [RFC4578] section 2.2.

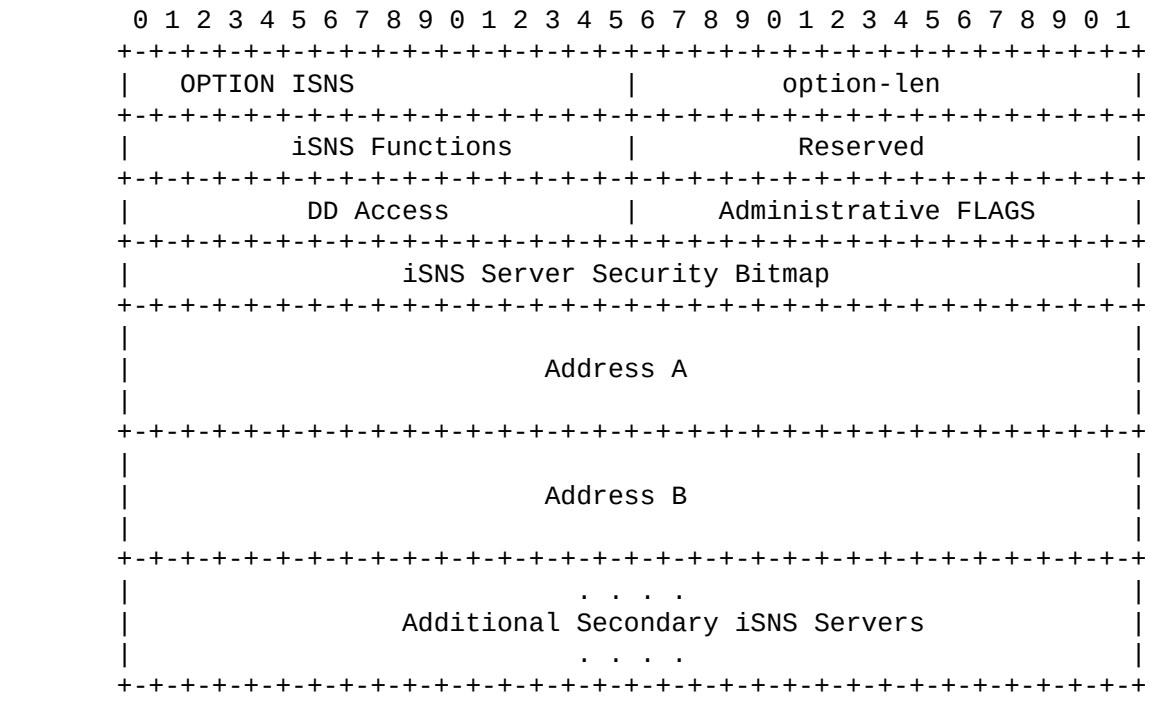
Major
As specified in [RFC4578] section 2.2.

Minor
As specified in [RFC4578] section 2.2.

2.6. iSNS Option

As specified in [RFC4173] section 6, iSCSI boot requires either iSNS or SLP support.

This option provides parity with the iSNS Option defined for DHCPv4 in [RFC4174] section 2.



option-code OPTION_ISNS (TBD7)

option-len 2

iSNS Functions As specified in [RFC4174] section 2.

Reserved MUST be set to zero

DD Access As specified in [RFC4174] section 2.

Administrative FLAGS As specified in [RFC4174] section 2.

iSNS Server Security Bitmap
As specified in [RFC4174] section 2.

Address A As specified in [RFC4174] section 2,
except that it contains an IPv6 address.

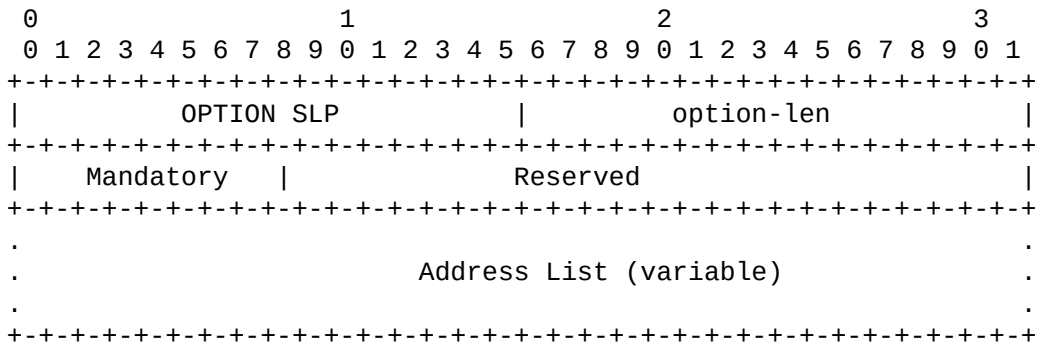
Address B As specified in [RFC4174] section 2,
except that it contains an IPv6 address.

Additional Secondary iSNS Servers
As specified in [RFC4174] section 2,
except that it contains IPv6 addresses.

2.7. SLP Directory Agent Option

As specified in [RFC4173] section 6, iSCSI boot requires either iSNS or SLP support.

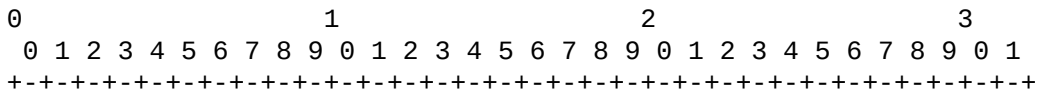
This option provides parity with the SLP Directory Agent Option defined for DHCPv4 in [RFC2610] section 3.

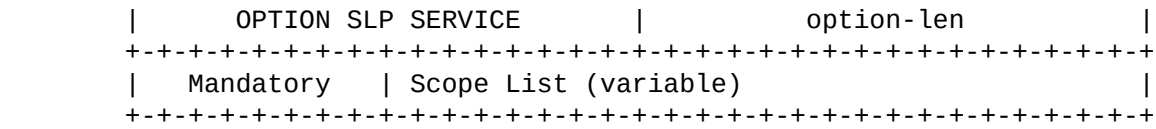


2.8. SLP Service Scope Option

As specified in [RFC4173] section 6, iSCSI boot requires either iSNS or SLP support.

This option provides parity with the SLP Directory Agent Option defined for DHCPv4 in [RFC2610] section 4.





option-code OPTION_SLP_SERVICE (TBD8)

option-len 2

Scope List As specified in [RFC2610] section 4

3. Security Considerations

If an adversary manages to modify the response from a DHCP server or insert its own response, a host could be led to contact a rogue file server, resulting in an attacker being able to run arbitrary code on the host. Consequently, a practical way to verify loaded boot images is to make sure that each host verifies the boot file to be executed using a mechanism of their choice.

In addition, some options contain information about a client's system architecture and may be of use to potential attackers.

See the security considerations in [RFC3315], [RFC4173], and [RFC4578] for more discussion. This document introduces no new concerns beyond the ones covered therein for IPv4.

4. IANA Considerations

This document introduces a new IANA registry for processor architecture types. The name of this registry shall be "Processor Architecture Type". Registry entries consist of a 16-bit integer recorded in decimal format, and a descriptive name. The initial values of this registry can be found in [RFC4578] section 2.1.

The assignment policy for values shall be Expert Review, and any requests for values must supply the descriptive name for the processor architecture type.

5. Acknowledgments

The authors would like to thank Ruth Li, Dong Wei, Kathryn Hampton, Phil Dorah, Richard Chan, and Fiona Jensen for discussions that led to this document.

6. References

6.1. Normative References

[PXE21] Henry, M. and M. Johnston, "Preboot Execution Environment (PXE) Specification", September 1999, http://www.pix.net/software/pxeboot/archive/pxespec.pdf

[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.

[RFC2610] C. Perkins, E. Guttman, "DHCP Options for Service Location Protocol," RFC2610, June 1999.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and Carney, M., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003.

[RFC4172] Monia, C., Tseng, J., and K. Gibbons, "The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service", RFC 4174, September 2005.

[RFC4173] Sarkar, P., Missimer, D. and Sapuntzakis, C., "Bootstrapping Clients using the Internet Small Computer System Interface (iSCSI) Protocol," RFC 4173, September 2005.

[RFC4174] Monia, C., Tseng, J., and K. Gibbons, "The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service", RFC 4174, September 2005.

[RFC4578] Johnston, M. and Venaas, S. "Dynamic Host Configuration Protocol (DHCP) Options for the Intel Preboot eXecution Environment (PXE)", RFC 4578, November 2006.

[UEFI22] Unified Extensible Firmware Interface Specification, Version 2.2, September 2008, http://www.uefi.org

6.2. Informative References

Author's Addresses

Vincent Zimmer
Intel
DP2-420
2800 Center Drive
DuPont, WA 98327

Phone: +1 253 371 5667
Email: vincent.zimmer@intel.com

Dave Thaler
Microsoft
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 703-8835
Email: dthaler@microsoft.com

Full Copyright Statement

Intellectual Property Statement

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.