DHCPV6 Working Group

Internet Draft

Intended status: Informational

Expires: April 2009

October 25, 2008

Ruth Li Intel Corporation Vincent Zimmer Intel Corporation Dong Wei Hewlett-Packard Kathryn Hampton Hewlett-Packard Phil Doragh Hewlett-Packard Richard Chan Dell Dave Thaler Microsoft Fiona Jensen Apple

DHCPv6 Remote Boot Options draft-zimmer-dhc-dhcpv6-remote-boot-options-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.

This document may not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

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."

Expires April 25, 2009

[Page 1]

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/lid-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 April 27, 2009.

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 [UEF122]. 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.	Introduction3
2.	DHCPv6 Options4
	Error! Bookmark not defined.
	2.1. Root Path Option
	2.2. Server Address Option (former option 54 in DHCPv4)Error!
	Bookmark not defined.
	2.3. Boot File Name Option (former option 67 in DHCPv4)4
	2.4. Boot File Size Option (former option 13 in DHCPv4)5
	2.5. Client System Architecture Type Option (former option 93).5
	2.6. Client Network Interface Identifier Option
	2.7. iSNS Option Definition (former option 83) [rfc4174]7
	2.8. SLP Directory Agent Option Definition (former option
	78)[rfc2610]8
	2.9. SLP Service Scope Option Definition (former option 79)
	[rfc2610]8
3.	Security Considerations8
4.	IANA Considerations9
5.	Acknowledgments9
6.	References10
	6.1. Normative References10
	6.2. Informative References11

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.

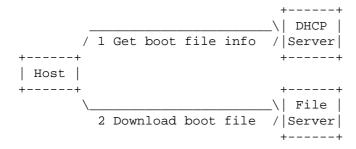


Figure 1: Network Boot Sequence

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. The options in this list support both PXE and iSCSI. The PXEspecific options include Client System Architecture type, Client Network Interface Identifier Option,

The iSCSI-specific options include iSNS and SLP. The Root Path, Boot File Name, and Boot File Size options are shared by both iSCSI and PXE.

2.2. 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.

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 2 3 4 5 6 7 8 9 0														
+-														
OPTION_ROOT_PATH option-len														
+-														
. root-disk-pathname (variable length) .														
•														
+-+-+-+-+-+-+-+-+-	+-+-+-+-+-+-+-	+-+-+-+-+-+-+-+	-+-+-+											
option-code	OPTION_ROOT_PATH (TB	D1).												
option-len	Length of Root Path	Name in octets.												
root-disk-pathname	An option field str	ing as specified in												
	[RFC4173] section 5													

2.3. Boot File Name Option (former option 67 in DHCPv4)

This option specifies the path-name that contains the client's boot file name. The path is formatted as a character string consisting of characters from the NVT ASCII character set.

0		1	2	3
0 1 2 3	3 4 5 6 7 8	9 0 1 2 3 4 5	5 6 7 8 9 0 1 2 3 4 5	6 7 8 9 0 1
+-+-+-	-+-+-+-+-	+-+-+-+-+-	-+-+-+-+-+-+-+-+-+	+-+-+-+

Zimmer

Expires April 27, 2009

[Page 4]

_		option-len
+-+-+-+-+-+	-+	-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+++
. B	oot File Name (variable leng	rth) .
+-+-+-+-+-+-+	-+	-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++++
option-code	OPTION_BOOT_FILE_NAME (TBD3)	
option-len	Length in octets of the Boot	File Name.
Boot File Name	XXX to be filled in	

2.4. Boot File Size Option (former option 13 in DHCPv4)

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

This option goes beyond the Boot File Size Option defined for DHCPv4 in [RFC2132] section 3.15. This is consistent with new pre-OS technologies like UEFI [UEFI22] that use the PE/COFF specification and allow for boot loaded images that are up to 4Gbytes in size.

0	1	2		3										
0 1 2 3 4 5 6	5 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_	BOOT_FILE_SIZE	optio	n-len											
+-														
File Size														
+-+-+-+-+-	-+-+-+-+-+-		+-+-+-+-	+-+-+										
option-code	OPTION_BOOT_FILE_S	SIZE (TBD4).												
option-len	4													
File Size	The length in 512-	octet blocks of	the boot image	age for the										
	client.													

2.5. Client System Architecture Type Option (former option 93)

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:

Ü	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_CLIENT_ARCH_TYPE option-len													
+-													
. Client System	Architecture Ty	pe (variable leng	gth) .										
•			•										
+-+-+-+-+-+-+	-+-+-+-+-+-	+-+-+-+-+-	+-+-+-+-+-+-+										
option-code		OPTION_CLIENT_ARCH_TYPE (TBD).											
option-len		XXX to be fil	led in										
a1 . a													
Client System Arc	hitecture Type	XXX to be fil:	led in										

Octet "n" gives the number of octets containing "architecture types"(not including the code and len fields). It MUST be an even number equal to one. Clients that support more than one architecture type WILL describe the instruction that the UEFI or BIOS runs within in their initial DHCP and PXE boot server packets. Octets "n1" and "n2" encode a 16-bit architecture type identifier that describes the pre-boot runtime environment(s) of the client machine.

dd		Type	Architecture	Name
tbd##	Inte	el x86P0	C	
tbd##	NEC	/PC98		
tbd##	EFI	Itaniur	n	
tbd##	DEC	Alpha		
tbd##	Arc	x86		
tbd##	Inte	el Lean	Client	
tbd##	x86-6	54PC		
tbd##	EFI	BC		
tbd##	EFI	ARM		

Zimmer

Expires April 27, 2009

[Page 6]

tbd## EFI x86-64 tbd## EFI IA32

2.6. 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:

Minor

0	1	2	3										
0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5	5 6 7 8 9 0 1 2	3 4 5 6 7 8 9 0 1										
+-+-+-+-+-+	-+-+-+-+-+-+-+-+-	-+-+-+-+-+-+-+	-+-+-+-+-+-+-+										
01	PTION_NII	opti	on-len										
+-+-+-+-+	-+-+-+-+-+-+-+-+	-+-+-+-+-+-+-+	-+-+-+-+-+-+-+										
Type	Major	Minor											
+-+-+-+-+-+	-+-+-+-+-+-+-+-+-	-+-+-+-+-+-+-+	-+-+										
option-code option-len	OPTION_NII (TBD)												
Туре	Type As specified in [RFC4578] section 2.2.												
Major	As specified	in [RFC4578] se	ction 2.2.										

As specified in [RFC4578] section 2.2.

2.7. iSNS Option Definition (former option 83) [rfc4174]

Zimmer Expires April 27, 2009 [Page 7]

+-
Additional Secondary iSNS Servers
+-

2.8. SLP Directory Agent Option Definition (former option 78)[rfc2610]

0	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	_				
+-+		+	-+	+	+-+	+	+	+-+	- - +	-	+	+	+	- - +	+	+	+	+	+	+	-	+	 -	+	-		+	+	+	+	+-	+				
		od	le	=	OF	T	101	v 5	SLE	e t	bc	l##				Le	eng	gtl	n				ľ	Mar	nda	ato	ory	Y					a1			Ī
+-+		+	-+	+	+-+	+	+	+-+	+-+	- - +	+	+	+		+	-	+	- +	+	+	-	+	-	+	-		+	+	+	+ – .	+-	.+				
			a2	2							а	13							á	a 4																
+-+		+	-+	+	+-+	+	+	+	- - +	+ - +	+	+	+	+ – +	+ - -		+	+	+	+ - -	- -	+	 -	+ – -	⊢ – -		+	+	+	+	+-	+				

2.9. SLP Service Scope Option Definition (former option 79) [rfc2610]

```
1
                 2
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 SLP SERVICE | Length | Mandatory | <Scope List>...
```

option-code OPTION_SLP_SERVICE (TBD).

option-len See RFC2610

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

Zimmer Expires April 27, 2009 [Page 8] 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

TBD

5. Acknowledgments

The authors would like to thank Phil Doragh and Anil Kumar Reddy Sirigiri from Hewlett-Packard. We would also like to thank Joe Calhoun and Jason Jin from Intel Corporation. We would also like to thank Thomas Narten from IBM.

6. References

6.1. Normative References

- [PECOFF] Microsoft Portable Executable and Common Object File Format, Revision 8.1, March 27, 2008 http://www.microsoft.com/whdc/system/platform/firmware/PECO FF.mspx
- [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
- [RFC4578] Johnston, M. and Venaas, S. "Dynamic Host Configuration Protocol (DHCP) Options for the Intel Preboot eXecution Environment (PXE)", RFC 4578, November 2006.
- [RFC2610] C. Perkins, E. Guttman, "DHCP Options for Service Location Protocol", RFC2610, June 1999.
- [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: 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

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 Statement

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

Zimmer

Expires April 27, 2009

[Page 11]

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.

Opens:

- . Restrict arch types to 1
- . Relationship to draft-ietf-dhc-dhcpv6-opt-netboot-00.txt?