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."

   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 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 [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
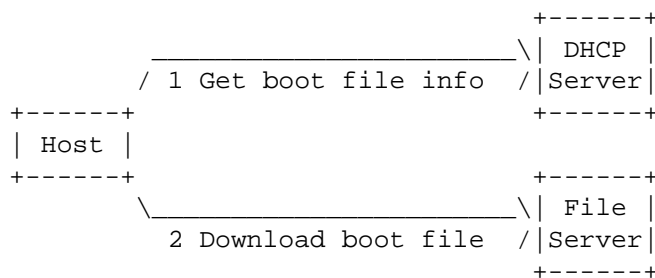   the boot file.

```
                                          +------+
                    _____\| DHCP |
                   / 1 Get boot file info  /|Server|
        +------+                            +------+
        | Host |
        +------+                            +------+
                   _____\| File |
                     2 Download boot file  /|Server|
                                            +------+
```

        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 PXE-
   specific 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        OPTION_ROOT_PATH        |          option-len           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   .                                                               .
   .            root-disk-pathname (variable length)               .
   .                                                               .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   option-code   OPTION_ROOT_PATH (TBD1).

   option-len   Length of Root Path Name in octets.

   root-disk-pathname An option field string 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 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_BOOT_FILE_NAME    |           option-len           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      .                                                               .
      .              Boot File Name (variable length)                .
      .                                                               .
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

      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 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     |           option-len          |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |          File Size                                            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

      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.

2.5. 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:

```
       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
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     OPTION_CLIENT_ARCH_TYPE    |          option-len           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      .                                                               .
      .  Client System Architecture Type (variable length)           .
      .                                                               .
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

      option-code                   OPTION_CLIENT_ARCH_TYPE (TBD).

      option-len                    XXX to be filled in

      Client System Architecture Type    XXX to be filled 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##     Intel x86PC

      tbd##     NEC/PC98

      tbd##     EFI Itanium

      tbd##     DEC Alpha

      tbd##     Arc x86

      tbd##     Intel Lean Client

      tbd##    x86-64PC

      tbd##     EFI BC

      tbd##     EFI ARM
```

        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:

```
         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
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |            OPTION_NII          |            option-len         |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |     Type      |     Major      |      Minor      |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        option-code   OPTION_NII (TBD).

        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.

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

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Code = OPTION ISNS tbd## |    Length      |      iSNS Functions      |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          DD Access         |     Administrative FLAGS      |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |              iSNS Server Security Bitmap             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     a1        |      a2       |      a3       |      a4       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     b1        |      b2       |      b3       |      b4       |
```

```
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                          . . . .                             |
     |                  Additional Secondary iSNS Servers           |
     |                          . . . .                             |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Code = OPTION SLP tbd## |    Length     |   Mandatory   |    a1      |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     a2        |      a3       |      a4       |     ...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |       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

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
              2005

   [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

Opens:

. Restrict arch types to 1

. Relationship to draft-ietf-dhc-dhcpv6-opt-netboot-00.txt?