                   NetWare/IP Domain Name and Information

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

1.0 Abstract

   The Dynamic Host Configuration Protocol (DHCP) [RFC 2131] provides a
   framework for passing configuration information to hosts on a TCP/IP
   network. DHCP includes options for specific configuration parameters
   [RFC 2132]. This document defines options that carry NetWare/IP
   domain name and NetWare/IP sub-options to DHCP clients.

1.1 Requirements

   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 RFC 2119 [RFC 2119].

1.2 Terminology

   This document uses the following terms:

      o "DHCP client"

         A DHCP client is an Internet host using DHCP to obtain
         configuration parameters such as a network address.

   o "DHCP server"

      A DHCP server is an Internet host that returns configuration
      parameters to DHCP clients.

2. The NetWare/IP Domain Name option

   This option code is used to convey the NetWare/IP domain name used by
   the NetWare/IP product. The NetWare/IP Domain in the option is an NVT
   ASCII [RFC 854] string whose length is inferred from the option 'len'
   field.

   The code for this option is 62, and its maximum length is 255.

        Code Len   NetWare/IP Domain Name
       +-----+-----+------+------+------+-----
       | 62 | n | c1 | c2 | c3 | ...
       +-----+-----+------+------+------+-----

   The 'len' field gives the length of the NetWare/IP Domain Name.

3. The NetWare/IP Information option

   The NetWare/IP option code will be used to convey all the NetWare/IP
   related information except for the NetWare/IP domain name.

   The code for this option is 63, and its maximum length is 255. A
   number of NetWare/IP sub-options will be conveyed using this option
   code. The 'len' field for this option gives the length of the option
   data, which includes the sub-option code, length and data fields.

   Each sub-option contains in sequential order, a one byte sub-option
   code, a one byte length, and an optional multiple byte value field.
   The sub-option length gives the length of the value field for the
   sub-option. The example below illustrates the use of the 'len' and
   sub-option length fields in this option.

   One and only one of the following four sub-options must be the first
   sub-option to be present in option 63 encoding. Each of them is
   simply a type length pair with length set to zero.

   Sub-options:

   NWIP_DOES_NOT_EXIST (code 1)

      The responding DHCP server does not have any NetWare/IP
      information configured.

   NWIP_EXIST_IN_OPTIONS_AREA (code 2)

      All NetWare/IP information is present in the 'options' area of the
      DHCP response packet.

   NWIP_EXIST_IN_SNAME_FILE (code 3)

      All NetWare/IP information is present in the 'sname' and, if
      necessary, 'file' fields of the DHCP response packet. If used, the
      following DHCP server behavior is required: within the 'options'
      area, option 63 is present with its length field set to 2. The
      first byte of the value field is set to NWIP_EXIST_IN_SNAME_FILE
      tag and the second byte is set to zero. Both option 62 and option
      63 will be placed in the area covered by the sname and file
      fields. Option 62 is encoded normally. Option 63 is encoded with
      its tag, length and value. The value field does not contain any of
      the first four sub-options described herein.

   NWIP_EXIST_BUT_TOO_BIG (code 4)

      Neither 'options' area nor 'sname' field can accommodate the
      NetWare/IP information.

   If either NWIP_EXIST_IN_OPTIONS_AREA or NWIP_EXIST_IN_SNAME_FILE
   sub-options is set, one or more of the following sub-options may be
   present.

   NSQ_BROADCAST (code 5)

      Length is 1 and a value of 1 or 0. If the value is 1, the client
      SHOULD perform a NetWare Nearest Server Query to find out its
      nearest NetWare/IP server.

   PREFERRED_DSS (code 6)

      Length is (n * 4) and the value is an array of n IP addresses,
      each four bytes in length. The maximum number of addresses is 5
      and therefore the maximum length value is 20. The list contains
      the addresses of n NetWare Domain SAP/RIP Server (DSS).

   NEAREST_NWIP_SERVER (code 7)

      Length is (n * 4) and the value is an array of n IP addresses,
      each four bytes in length. The maximum number of addresses is 5
      and therefore the maximum length value is 20. The list contains
      the addresses of n Nearest NetWare/IP servers.

   AUTORETRIES (code 8)

      Length is 1 and the value is a one byte integer value indicating
      the number of times a NetWare/IP client should attempt to
      communicate with a given DSS server at startup.

   AUTORETRY_SECS (code 9)

      Length is 1 and the value is a one byte integer value indicating
      the amount of delay in seconds in between each NetWare/IP client
      attempt to communicate with a given DSS server at startup.

   NWIP_1_1 (code 10)

      Length is 1 and the value is 1 or 0. If the value is 1, the
      NetWare/IP client SHOULD support NetWare/IP Version 1.1
      compatibility. A NetWare/IP client only needs this compatibility
      if it will contact a NetWare/IP version 1.1 server.

   PRIMARY_DSS (code 11)

      Length of 4, and the value is a single IP address. This field
      identifies the Primary Domain SAP/RIP Service server (DSS) for
      this NetWare/IP domain. NetWare/IP administration utility uses
      this value as Primary DSS server when configuring a secondary DSS
      server.

   An example of option 63 encoding is provided below.

    Code   Len NetWare/IP General Info
    +-----+-----+----+----+
    | 63 | 11 | 2 | 0 |
    +-----+-----+----+----+
                NWIP_EXIST_IN_OPTIONS_AREA (length 0)

            +----+----+----+
            | 5 | 1 | 1 |
            +----+----+----+
             NSQ_BROADCAST_SERVER (length 1)
             value is YES

            +----+----+------------+
            | 7 | 4 | IP address |
            +----+----+------------+
             NEAREST_NWIP_SERVER (length 4)
             value is IP address of server

4. References

   [RFC 854] Postel, J. and J. Reynolds, "Telnet Protocol
   Specification", RFC 854, May 1983.

   [RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate
   Requirement Levels", RFC 2119, March 1997.

   [RFC 2131] Droms, R., "Dynamic Host Configuration Protocol", RFC
   2131, March 1997.

   [RFC 2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor
   Extensions", RFC 2132, 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 [RFC 2131].

   The NetWare/IP options can be used by unauthorized DHCP servers to
   misconfigure NetWare/IP clients with potentially disruptive
   information.

6. Authors' addresses

   Ralph Droms
   Computer Science Department
   323 Dana Engineering
   Bucknell University
   Lewisburg, PA 17837

   Phone: (717) 524-1145
   EMail: droms@bucknell.edu

   Kester Fong
   Information Access Division
   Novell Inc.
   SJF-8-265
   2010 Fortune Dr,
   San Jose, CA95131

   Phone:(408)-577-8959
   EMail: kfong@novell.com

7. Full Copyright Statement