Network Working Group   Senthil K Balasubramanian
Internet-Draft   Intoto
Expires: March 2005   Michael Alexander
                                               Gustaf Neumann
                                               Wirtschaftsuniversitaet Wien
                                               October 2004

DHCP Option for Proxy Server Configuration
draft-ietf-dhc-proxyserver-opt-02.txt

Status of this Memo

Copyright Notice

Abstract

   This document defines a new Dynamic Host Configuration Protocol
   (DHCP) option, which can be used to configure the TCP/IP host's Proxy
   Server configuration for standard protocols like HTTP, FTP, NNTP,
   SOCKS, Gopher, SLL and etc. Proxy Server provides controlled and
   efficient access to the Internet by access control mechanism for
   different types of user requests and caching frequently accessed
   information (Web pages and possibly files that might have been
   downloaded using FTP and other protocols).

1. Terminologies Used

DHCP Client: A DHCP [RFC-2131] client is an Internet host that
         uses DHCP to obtain configuration information such as
         network address.

DHCP Server: A DHCP server [RFC-2131] is an Internet host that
         returns configuration parameters to DHCP clients.
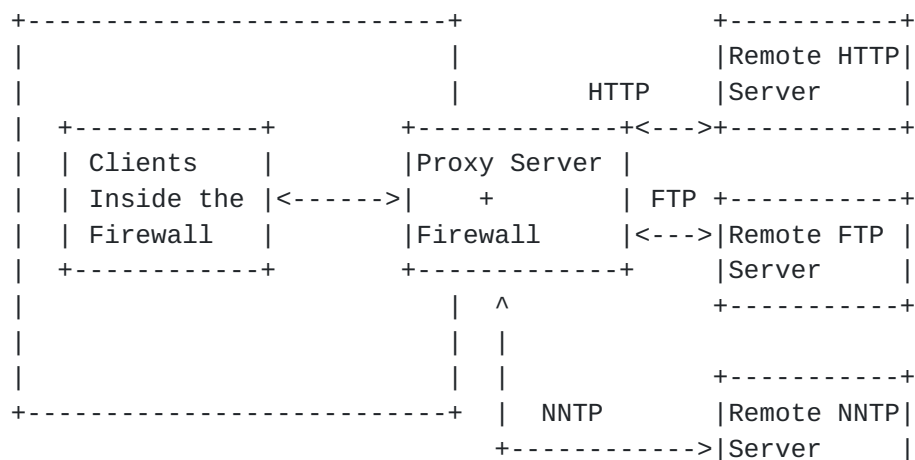
Proxy Server: In a enterprise network that connects to Internet,
         a proxy server is a server that acts as an intermediary
         between a workstation user and the Internet so that the
         enterprise can ensure security, administrative control,
         and caching service. A Proxy server MAY be associated
         with or part of a gateway server that separates the
         enterprise network from the outside network (Usually
         Internet) and a firewall server that protects the
         enterprise network from outside intrusion.

RDF:A language (Resource Description Framework [RDF-SYN]) for
         describing properties of web resources.

2. Introduction

The Dynamic Host Configuration Protocol [RFC-2131] provides a
framework for passing configuration information to hosts on a TCP/IP
network. This document describes a DHCP configuration option that
can be used to inform a DHCP client, the IP addresses of one or more
proxy services that are either available to it or that must be used
in order to access internet services, for example through a coporate
firewall.

The following diagram depicts the typical setup providing proxy
service to clients on a network that is protected by a firewall.

```
+---------------------------+                 +-----------+
|                           |                 |Remote HTTP|
|                           |        HTTP     |Server     |
|   +------------+        +-------------+<--->+-----------+
|   | Clients    |        |Proxy Server |
|   | Inside the |<------>|     +       | FTP +-----------+
|   | Firewall   |        |Firewall     |<--->|Remote FTP |
|   +------------+        +-------------+     |Server     |
|                           | ^               +-----------+
|                           | |
|                           | |               +-----------+
+---------------------------+ |   NNTP        |Remote NNTP|
                            +------------>|Server     |
```

```
                              +-----------+
```

The primary use of proxies is to allow access to the World Wide Web
from within a firewall. A proxy service typically runs on firewall
machine. It waits for a request from inside the firewall, forwards

the request to the remote server outside the firewall, reads the
response and then sends it back to the client. Usually, all the
clients use the same proxy within a given network, which helps in
efficient caching of documents that are requested by a number of
clients. This behavior makes proxies attractive to clients not
inside a firewall.

A proxy server increases the network security and user productivity
by content filtering and controlling both internal and external
access to information. Also, it provides several other
functionalities that are not discussed here.

3. Requirements 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 [RFC 2119].

4. Proxy Server Configuration Option

This document defines a new DHCP Option called the Proxy Server
Configuration Option. The format of the Proxy Server configuration
option is:

```
       Code     Len     Proxy Server Configuration Entry
      +-------+------+------+------+------+------+-....-+------+
      |  TBD  |  N   |  e1  |  e2  |  e3  |  e4  |      |  en  |
      +-------+------+------+------+------+------+-....-+------+
```

Code is TBD and will be assigned by IANA according to [RFC-2939].
The length N gives the total number of octets in the Proxy Server
Configuration entries.

The Proxy Server Configuration entry normally consists of a
sequence of Protocol Type (p), len (l), flag (f), IP
address and port. But it can also be a sequence of Protocol
Type (p), Len and RDF[RDF-SYN] metadata.

```
     +--+--+--+--+--+--+--+--+
     |p |l | f |IP address|port |
     +--+--+--+--+--+--+--+--+
```

The Protocol(p) is a two octet integer in network byte order,
length (l) and flag (f) are one octet each; each IP
address is four octets, and each port number is a two-octet
integer encoded in network byte order.

The protocol type(p) specifies the type of Protocol and MUST be
one of the following assigned numbers.

```
+------------------------------+
| protocol        |    Number   |
+------------------------------+
|    HTTP         |      80     |
+------------------------------+
|    FTP          |      21     |
+------------------------------+
|    NNTP         |     119     |
+------------------------------+
|    Gopher       |      70     |
+------------------------------+
|    SSL          |     TBD     |
+------------------------------+
|    SOCKS        |     1080    |
+------------------------------+
|    WAIS         |     210     |
+------------------------------+
|    IMAP         |     220     |
+------------------------------+
|    RDF          |     TBD     |
+------------------------------+
```

If the protocol type field is RDF[RDF-SYN], then it MUST be
followed by len (length of RDF metadata) and the actual RDF
metadata.

The length field (l) specifies the length of the Proxy Server
Configuration entry. If some new protocol is introduced in the
future and if some version of dhcpclient doesn't support, then
that particular entry can be ignored and process the following
Proxy Server Configuration Entry, if any.

The flag field (f) is by default 0. Otherwise, it can either
have "-" or "#".

If it is "-", then the entry becomes a destination address for
exclusion from forwarding to the proxy. If it is "#", then the proxy
requires authentication.

In cases where it makes sense to specify more than one proxy server
for a given protocol, these proxy servers MUST be specified as
additional IP addresses and ports within the same entry. The list is
ordered by precedence, with the most preferred proxy server appearing
first in the list, andthe least preferred proxy server appearing last
in the list. The DHCP client SHOULD honor this ordering.

More than one Proxy Server Configuration Entries MAY be specified in
the option. In that case, the list is ordered by precedence, with

the most preferred proxy server appearing first in the list, and the
least preferred proxy server appearing last in the list. The DHCP
client SHOULD honor this ordering.

The format of the Proxy Server Configuration using Metadata type is:


```
          p       Len         RDF Metadata for the Proxy
        +-------+------+----------------------------------+
        |  RDF  |  N   |            RDF                   |
        +-------+------+----------------------------------+
```

The RDF payload is freeform RDF metadata for describing proxy
properties. The length N gives the number of octets in the RDF
metadata field.

The following entry specifies the sample format of the RDF Meta
data field

HTTP proxy:

```
<?xml version="1.0"?>
<!DOCTYPE rdf:RDF [<!ENTITY xsd "http://www.w3.org/2001/XMLSchema#">]>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:dc="http://purl.org/dc/elements/1.1/">
<rdf:Description rdf:about="http://http-proxy.duke.edu:8080">
     <dc:title>License Gate Proxy</dc:title>
     <dc:creator>John Doe</dc:creator>
     <dc:publisher>Duke OIT</dc:publisher>
     <dc:subject>Offsite Campus Resource Access Proxy</dc:subject>
     <dc:type>Service</dc:subject>
     <dc:rights>Current Duke faculty, staff, and students</dc:rights>
     <dc:date>2004-06-15</dc:date>
</rdf:Description>
</rdf:RDF>
```

FTP proxy:

```
<?xml version="1.0"?>
<!DOCTYPE rdf:RDF [<!ENTITY xsd "http://www.w3.org/2001/XMLSchema#">]>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:dc="http://purl.org/dc/elements/1.1/">
<rdf:Description rdf:about="ftp://ftp-proxy.duke.edu:8080">
     <dc:title>License Gate FTP Proxy</dc:title>
     <dc:creator>John Doe</dc:creator>
     <dc:publisher>Duke OIT</dc:publisher>
     <dc:subject>Offsite Campus Resource Access Proxy</dc:subject>
     <dc:type>Service</dc:subject>
     <dc:rights>Current Duke faculty, staff, and students</dc:rights>
     <dc:date>2004-06-15</dc:date>
</rdf:Description>
</rdf:RDF>
```

As such there is no minimum length to specify a proxy using RDF
metadata. But the minimum sensible statement would be a literal
description of the proxy (<dc:title>License Gate Proxy</dc:title>)
giving a total of 418 characters including the overhead.

For example, with a description element of 60 characters, an URI of
80 characters plus a minimum XML/RDF syntax conformation/namespace
declaration of:

```
21 Octets <?xml version="1.0"?>
70 Octets <!DOCTYPE rdf:RDF [<!ENTITY xsd "http://www.w3.org/2001/
XMLSchema#">]>
64 Octets <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
45 Octets xmlns:dc="http://purl.org/dc/elements/1.1/">
109 Octets <rdf:Description rdf:about="..80 characters..">
81 Octets <dc:title>..60 characters..</dc:title>
18 Octets </rdf:Description>
10 Octets </rdf:RDF>
```

,the minimum length would be 418 octes.

5. Option Usage

The Proxy Server Configuration entries SHOULD not repeat the same
type of proxy entries. The port MUST be a valid TCP/UDP port.
If the length of the Proxy Server Configuration Option exceeds the
maximum permissible within a single option (255 octets), then the
option MUST be represented in the DHCP message as specified
in [RFC-3396].

The following example shows how an RDF version of proxy server
configuration entry of 400 octets is represented in the option.

```
 Code     Len   Proto   Len
+-------+------+------+------+------+------+-....-+------+
|  TBD  | 255  |  RDF |  253 | RDF Meta Data.............|
+-------+------+------+------+------+------+-....-+------+
 Code     Len   Proto   Len
+-------+------+------+------+------+------+-....-+------+
|  TBD  | 149  |  RDF |  147 | RDF Meta Data.............|
+-------+------+------+------+------+------+-....-+------+
```

The following example shows how the same RDF version of proxy
server configuration entry of 400 octets is represented in the
option along with a normal version (p|l|f|IP|port) of proxy
server configuration entry.

```
+---+---+----+-+-+-------------+----+---+---+...-+---+-----+
|TBD|255|HTTP|7|0|192.168.5.10 |8080|RDF|243| RDF Meta Data|
+---+---+----+-+-+-------------+----+---+---+...-+---+-----+


+-------+------+------+------+------+------+-....-+------+
|  TBD  | 159  |  RDF |  157 | RDF Meta Data.............|
+-------+------+------+------+------+------+-....-+------+
```

More than one RDF type of Proxy Server Configuration Entry MUST
not be sent in this option. This is because, the RDF Meta Data is
generally more than 255 octets and always require more than one
option of this type as per [RFC-3396]. However, more than one proxy
server configuration (FTP, HTTP, SOCKS) can be specified with the

same RDF Meta Data as follows

HTTP and FTP Proxy

```
<?xml version="1.0"?>
<!DOCTYPE rdf:RDF [<!ENTITY xsd "http://www.w3.org/2001/XMLSchema#">]>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:dc="http://purl.org/dc/elements/1.1/">
<rdf:Description rdf:about="ftp://ftp-proxy.duke.edu:8080">
    <dc:title>License Gate FTP Proxy</dc:title>
    <dc:creator>John Doe</dc:creator>
    <dc:publisher>Duke OIT</dc:publisher>
    <dc:subject>Offsite Campus Resource Access Proxy</dc:subject>
    <dc:type>Service</dc:subject>
    <dc:rights>Current Duke faculty, staff, and students</dc:rights>
    <dc:date>2004-06-15</dc:date>
</rdf:Description>
<rdf:Description rdf:about="http://http-proxy.duke.edu:8080">
    <dc:title>License Gate Proxy</dc:title>
    <dc:creator>John Doe</dc:creator>
    <dc:publisher>Duke OIT</dc:publisher>
    <dc:subject>Offsite Campus Resource Access Proxy</dc:subject>
    <dc:type>Service</dc:subject>
    <dc:rights>Current Duke faculty, staff, and students</dc:rights>
    <dc:date>2004-06-15</dc:date>
</rdf:Description>
</rdf:RDF>
```

6. Security Considerations

The DHCP Options defined here allow an intruder DHCP server to misdirect a client, causing it to access a nonexistent or malicious proxy server. This allows for a denial of service or man-in-the-middle attack. This is a well known property of the DCHP protocol; this option does not create any additional risk of such attacks.

DHCP provides an authentication mechanism, as described in [RFC-3118], which may be used if authentication is required.

7. IANA Considerations

IANA is requested to assign an option code to the Proxy Server Configuration Option and protocol numbers for the SSL and RDF protocol.

8. Acknowledgements

Thanks to the DHC Working Group for their time and input into the

specification. In particular, thanks to (in alphabetical order) Bernie Volz, Ralph Droms, Robert Elz, and Ted Lemon for their thorough review.

9. Normative References

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

[RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate
      Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC-3396] Lemon, T. and S. Cheshire, "Encoding Long DHCP Options",
      RFC 3396, November 2002.

10. Informative References

[RFC-3118] Droms, R. and W. Arbaugh, "Authentication for DHCP
      Messages", RFC 3118, June 2001.

[RFC-2939] Droms, R., "Procedures and IANA Guidelines for Definition
       of New DHCP Options and Message Types", BCP 43, RFC 2939,
       September 2000.

[RFC-2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H.,
      Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext
      Transfer Protocol -- HTTP/1.1" RFC 2616, June 1999.

[RFC-959] Postel, J. and J. Reynolds, "File Transfer Protocol
      (FTP)", STD 9, RFC 959, October 1985.

[RFC-1436] F. Anklesaria, M. McCahill, P. Lindner, D. Johnson,
      D. Torrey and B. Albert, "The Internet Gopher Protocol
      (a distributed document search and retrieval protocol)",
      RFC 1436, March 1993.

[RFC-977] Kantor, B and P. Lapsley, "Network News Transfer
      Protocol", RFC 977, February 1986.

[RFC-1928] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and
      L. Jones, "SOCKS Protocol V5", RFC 1928, April 1996.

[SSL2] Hickman, Kipp, "The SSL Protocol", Netscape Communications
      Corp., Feb 9, 1995.

[SSL3]   A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0
      Protocol", Netscape Communications Corp., Nov 18, 1996.

[RFC-1625] M. St. Pierre, J. Fullton, K. Gamiel, J. Goldman, B. Kahle,
      J. Kunze, H. Morris, F. Schiettecatte, "WAIS over Z39.50-1988",
      RFC 1625, June 1994.

[RDF-SYN] Becket, D. and B. McBride, Ed., "RDF/XML Syntax Specification",
          W3C REC-rdf-syntax, February 2004,
          <http://www.w3.org/TR/rdf-syntax-grammar/>.

Author's Address

   Senthil K Balasubramanian
   Intoto Software (I) Pvt Ltd
   C/o DBS Office Business Center
   Suite No.204, 31-A Cathedral Garden Road
   Chennai, India 600 034

   Phone: +91 44 2827 5191
   EMail: ksenthil@intotoinc.com

   Michael Alexander
   Wirtschaftsuniversitaet Wien
   Augasse 2-6
   A-1090 Vienna, Austria

   Phone: +43 31336 4467
   Email: malexand@wu-wien.ac.at

   Gustaf Neumann
   Wirtschaftsuniversitaet Wien
   Augasse 2-6
   A-1090 Vienna, Austria

   Phone: +43 31336 4671
   Email: neumann@wu-wien.ac.at

nnnn