DHCP Option for Proxy Server Configuration
draft-ietf-dhc-proxyserver-opt-01.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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 December 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

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 an 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 corporate firewall.

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

```
+---------------------------+    +-----------+
|                           |    |Remote HTTP|
|                           |    |Server     |
|+---------------------------+<--->+-----------+
| | HTTP                     |
| | Server                  |
|+---------------------------+    +-----------+
| |Clients                  |
| |Inside the Firewall      |
|+---------------------------+    +-----------+
| |Proxy Server             |
| |Firewall                 |
|+---------------------------+    +-----------+
| |FTP                      |
| |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 format of Proxy Server Configuration Entry can be either protocol/encoding/Address/port tuple or RDF [RDF-SYN] Metadata type. The minimum length is 8 octets.

The Proxy Server Configuration entry consists of a sequence of Protocol Type (p), Encoding (e), IP address and port.

```
|p |e |IP address |port |
+--+--+--+--+--+
```

The Protocol (p) and encoding (e) are on 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.
The encoding field (e) 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, and the 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:

```
+-------+-------+----------------------------------+
| RDF   | N     | RDF Metadata for the Proxy       |
+-------+-------+----------------------------------+
```
Internet-Draft    DHCP Option for Proxy Server Configuration   Dec 2004

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 entries specifies the sample format of the RDF 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:type>
    <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:type>
    <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.

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 DHCP protocol; this option does not create any additional risk of such attacks.

DHCP provides an authentication mechanism, as described in RFC 3118 [3], 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 Srinivas Reddy and Sridhar Ramamoorthy of Satyam InfoWay for their extended help in technical Queries.

9. Normative References


Informative References


Author’s Address

Senthil K Balasubramanian
Hewlett Packard
29 Cunningham Road,
Bangalore
India 560 052

Phone: +91 80 2205 3103
EMail: ksenthil@india.hp.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