Network Working Group   Ye Gu, Microsoft
INTERNET DRAFT   Ramesh Vyaghrapuri, Microsoft
                                             Burcak Beser, 3Com
                                                  October 1998
                                             Expires April 1999

          DHCP Use of the User Class Option for Address Assignment
                   <**draft-ietf-dhc-useraddr-00.txt**>

Abstract

This document proposes a mechanism that DHCP clients can use optionally
to obtain their IP addresses from different address pools configured on
a DHCP server. A DHCP client can specify a class to which it belongs.
Based on the class, a DHCP server selects the appropriate address pool
to assign an address to the client.

1. Introduction

With the popularity and importance of the Internet growing, many
organizations and public carriers are deploying IP-based networks. An
IP network is a heterogeneous environment that supports various kinds
of devices, users and applications (which are referred to generically
as "users" in the rest of this document). Often IP network
administrators are faced with the need to provide different levels of
service quality or access privilege to different users.

In order for an IP network to implement differentiated services, it
needs a way to classify users. A simple solution to this is to use
source IP addresses for classification.

Under this scheme, network administrators first configure network

devices such as routers to recognize traffic from a particular source
IP address (or address range) and handle it specially to meet the
desired level of service. Next, they assign the IP address(es) to the
host(s) of the intended user(s) so that the user(s) will receive the
appropriate level(s) of service. They can configure the hosts manually
with these addresses. However, they cannot use DHCP [1] for address
assignment, even if they are already running a DHCP server in their
network. A current RFC-compliant DHCP server assigns IP addresses
based on the location of the DHCP Client in the network topology, not
the type of user it supports.

This document describes a simple extension of the DHCP protocol that
enables a DHCP server to assign IP addresses from different address
pools depending on the types of client from which it receive DHCP
requests. With this new extension, network administrators will be able
to use DHCP to hand out the appropriate addresses to users (assuming
that the user type maps to the client type).

An example intended usage is a corporate network subnet consisting of
different departments of users, such as Accounting, Legal, Staff etc.
It may be desirable to allocate logical address pools to each of the
departments so that network policies may be implemented easily on IP
address ranges; and this would facilitate providing differential
services, such as network reachability.

2. Definitions

Throughout this document, the words that are used to define the
significance of particular requirements are capitalized. These words
are:

   o "MUST"

     This word or the adjective "REQUIRED" means that the
     item is an absolute requirement of this specification.

   o "MUST NOT"

     This phrase means that the item is an absolute prohibition
     of this specification.

   o "SHOULD"

     This word or the adjective "RECOMMENDED" means that there
     may exist valid reasons in particular circumstances to
     ignore this item, but the full implications should be
     understood and the case carefully weighed before choosing a
     different course.

    o "SHOULD NOT"

       This phrase means that there may exist valid reasons in
       particular circumstances when the listed behavior is
       acceptable or even useful, but the full implications should
       be understood and the case carefully weighed before
       implementing any behavior described with this label.

    o "MAY"

       This word or the adjective "OPTIONAL" means that this item
       is truly optional. One vendor may choose to include the
       item because a particular marketplace requires it or because
       it enhances the product, for example; another vendor may
       omit the same item.

3. Schema Overview

The user class option [3] is used by a DHCP client to inform DHCP
servers about the category of system, user or application it
represents.

In the following section, it is assumed that the DHCP Client MAY send
multiple User Class options in the same message. (They may or may not
occur consequetively).

Each address pool on the DHCP Server MAY be configured with a set of
ALLOWED USER CLASSES, specifying the category of clients accepted by
the DHCP Server; and with a set of DISALLOWED USER CLASSES, specifying
the category of clients that must NOT be offered addresses from the
address pool.

4. Address Assignment

Whenever any DHCP client message is seen by the DHCP Server, it MUST do
the regular processing [1] and if the DHCP Server determines that the
Client is to be offered a new (or unbound)IP address, the following
procedure MUST be adopted:

If the client DHCP message does not contain any User Class options,
then the DHCP Server MUST attempt to choose an available address pool
which has both the ALLOWED and DISALLOWED USER CLASSES empty.   If no
such address pool is available, and if the DHCP Server has been
specifically configured to do so, it MUST attempt chose any available
address pool.

If the client DHCP Message contains any User Class options, then the
DHCP Server MUST attempt to choose an available address pool for which

the ALLOWED USER CLASSES set contains one of the user class options

present in the DHCP message; and for which none of the User Class
options present in the DHCP message are also present in the DISALLOWED
USER CLASSES set. If no such address pool is available, and if the
DHCP Server has been specifically configured to do so, it MUST attempt
to choose any address pool for which none of the User Class options
present in the DHCP message are also present in the DISALLOWED USER
CLASSES set.

If the DHCP Server is unable to find a suitable address pool, it MUST
NOT offer an IP address to the Client. It MAY indicate the condition
to the administrator.

5. Address Renewal

At renewal time, before the DHCP Server sends an DHCP ACK as per [1],
it MUST check to see if the address pool of the Client's IP address has
any of the User Class option values in the DHCP message of the Client
present in the DISALLOWED USER CLASSES set; or, if the ALLOWED USER
CLASSES set has none of the User Class option values in the DHCP
message, and the DHCP Server is NOT specifically configured to allow a
client whose user class options do not belong to either of the two sets
of USER CLASSES.   If either of the two checks above succeed, the DHCP
Server MUST send a DHCP NACK message to the client and remove the
binding information.   The DHCP Server MAY send an indication via the
MESSAGE option.

6. Security Considerations

DHCP currently provides no authentication or security mechanisms.
Potential exposures to attack are discussed is section 7 of the
protocol specification [1].

7. Acknowledgements

The authors would like to thank Munil Shah and Peter Ford for reviewing
this draft.

8. References

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March
1997.
[2] Alexander, S., and Droms R., "DHCP Options and BOOTP Vendor
Extensions", RFC 2132, March 1997.
[3] Stump, G., and Droms R., "The User Class Option for DHCP", Internet
Draft, November 1997.

[9](). **Author's Address**

    Ye Gu
    Microsoft Corporation
    One Microsoft Way
    Redmond, WA 98052

    Phone: 425 936 8601
    EMail: yegu@microsoft.com

    Ramesh Vyaghrapuri
    Microsoft Corporation
    One Microsoft Way
    Redmond, WA 98052

    Phone: 425 703 9581
    Email: rameshv@microsoft.com

    Burcak Beser
    3Com Corporation
    3800 Golf Road
    Rolling Meadows, IL

    Phone: 847 262 2195
    Email: Burcak_Beser@3com.com

    This document will expire in April 1999.