EXHIBIT 1013

>

Network Working Group   R. Droms
Request for Comments: 1541   Bucknell University
Obsoletes: 1531   October 1993
Category: Standards Track

                 Dynamic Host Configuration Protocol

Status of this memo

   This RFC 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" for the standardization state and status
   of this protocol. Distribution of this memo is unlimited.

Abstract

   The Dynamic Host Configuration Protocol (DHCP) provides a framework
   for passing configuration information to hosts on a TCP/IP network.
   DHCP is based on the Bootstrap Protocol (BOOTP) [7], adding the
   capability of automatic allocation of reusable network addresses and
   additional configuration options [19]. DHCP captures the behavior of
   BOOTP relay agents [7, 23], and DHCP participants can interoperate
   with BOOTP participants [9]. Due to some errors introduced into RFC
   1531 in the editorial process, this memo is reissued as RFC 1541.

Table of Contents

file:///C:/Users/25474/AppData/Local/Temp/Low/GUK7JR2I.htm   12/17/2013

RFC 1541   Dynamic Host Configuration Protocol   October 1993

1. Introduction

    The Dynamic Host Configuration Protocol (DHCP) provides configuration
    parameters to Internet hosts. DHCP consists of two components: a
    protocol for delivering host-specific configuration parameters from a
    DHCP server to a host and a mechanism for allocation of network
    addresses to hosts.

    DHCP is built on a client-server model, where designated DHCP server
    hosts allocate network addresses and deliver configuration parameters
    to dynamically configured hosts. Throughout the remainder of this
    document, the term "server" refers to a host providing initialization

Droms   [Page 2]

RFC 1541   Dynamic Host Configuration Protocol   October 1993

    parameters through DHCP, and the term "client" refers to a host

requesting initialization parameters from a DHCP server.

A host should not act as a DHCP server unless explicitly configured
to do so by a system administrator. The diversity of hardware and
protocol implementations in the Internet would preclude reliable
operation if random hosts were allowed to respond to DHCP requests.
For example, IP requires the setting of many parameters within the
protocol implementation software. Because IP can be used on many
dissimilar kinds of network hardware, values for those parameters
cannot be guessed or assumed to have correct defaults. Also,
distributed address allocation schemes depend on a polling/defense
mechanism for discovery of addresses that are already in use. IP
hosts may not always be able to defend their network addresses, so
that such a distributed address allocation scheme cannot be
guaranteed to avoid allocation of duplicate network addresses.

DHCP supports three mechanisms for IP address allocation. In
"automatic allocation", DHCP assigns a permanent IP address to a
host. In "dynamic allocation", DHCP assigns an IP address to a host
for a limited period of time (or until the host explicitly
relinquishes the address). In "manual allocation", a host's IP
address is assigned by the network administrator, and DHCP is used
simply to convey the assigned address to the host. A particular
network will use one or more of these mechanisms, depending on the
policies of the network administrator.

Dynamic allocation is the only one of the three mechanisms that
allows automatic reuse of an address that is no longer needed by the
host to which it was assigned. Thus, dynamic allocation is
particularly useful for assigning an address to a host that will be
connected to the network only temporarily or for sharing a limited
pool of IP addresses among a group of hosts that do not need
permanent IP addresses. Dynamic allocation may also be a good choice
for assigning an IP address to a new host being permanently connected
to a network where IP addresses are sufficiently scarce that it is
important to reclaim them when old hosts are retired. Manual
allocation allows DHCP to be used to eliminate the error-prone
process of manually configuring hosts with IP addresses in
environments where (for whatever reasons) it is desirable to manage
IP address assignment outside of the DHCP mechanisms.

The format of DHCP messages is based on the format of BOOTP messages,
to capture the BOOTP relay agent behavior described as part of the
BOOTP specification [7, 23] and to allow interoperability of existing
BOOTP clients with DHCP servers. Using BOOTP relaying agents
eliminates the necessity of having a DHCP server on each physical
network segment.

Droms   [Page 3]

RFC 1541   Dynamic Host Configuration Protocol   October 1993

1.1 Related Work

There are several Internet protocols and related mechanisms that
address some parts of the dynamic host configuration problem. The
Reverse Address Resolution Protocol (RARP) [10] (through the

extensions defined in the Dynamic RARP (DRARP) [5]) explicitly
addresses the problem of network address discovery, and includes an
automatic IP address assignment mechanism. The Trivial File Transfer
Protocol (TFTP) [20] provides for transport of a boot image from a
boot server. The Internet Control Message Protocol (ICMP) [16]
provides for informing hosts of additional routers via "ICMP
redirect" messages. ICMP also can provide subnet mask information
through the "ICMP mask request" message and other information through
the (obsolete) "ICMP information request" message. Hosts can locate
routers through the ICMP router discovery mechanism [8].

BOOTP is a transport mechanism for a collection of configuration
information. BOOTP is also extensible, and official extensions [17]
have been defined for several configuration parameters. Morgan has
proposed extensions to BOOTP for dynamic IP address assignment [15].
The Network Information Protocol (NIP), used by the Athena project at
MIT, is a distributed mechanism for dynamic IP address assignment
[19]. The Resource Location Protocol RLP [1] provides for location
of higher level services. Sun Microsystems diskless workstations use
a boot procedure that employs RARP, TFTP and an RPC mechanism called
"bootparams" to deliver configuration information and operating
system code to diskless hosts. (Sun Microsystems, Sun Workstation
and SunOS are trademarks of Sun Microsystems, Inc.) Some Sun
networks also use DRARP and an auto-installation mechanism to
automate the configuration of new hosts in an existing network.

In other related work, the path minimum transmission unit (MTU)
discovery algorithm can determine the MTU of an arbitrary internet
path [14]. Comer and Droms have proposed the use of the Address
Resolution Protocol (ARP) as a transport protocol for resource
location and selection [6]. Finally, the Host Requirements RFCs [3,
4] mention specific requirements for host reconfiguration and suggest
a scenario for initial configuration of diskless hosts.

1.2 Problem definition and issues

DHCP is designed to supply hosts with the configuration parameters
defined in the Host Requirements RFCs. After obtaining parameters
via DHCP, a host should be able to exchange packets with any other
host in the Internet. The parameters supplied by DHCP are listed in
Appendix A.

Droms   [Page 4]

RFC 1541   Dynamic Host Configuration Protocol   October 1993

Not all of these parameters are required for a newly initialized
host. A client and server may negotiate for the transmission of only
those parameters required by the client or specific to a particular
subnet.

DHCP allows but does not require the configuration of host parameters
not directly related to the IP protocol. DHCP also does not address
registration of newly configured hosts with the Domain Name System
(DNS) [12, 13].

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.