Network Working Group
INTERNET-DRAFT
Internet Engineering Task Force
draft-itsumo-drcp-01.txt
Date: July 14, 2000
Expires: January 14, 2001

Anthony McAuley
Subir Das
Sunil Madhani
Telcordia Technologies
Shinichi Baba
Yasuro Shobatake
Toshiba America Research Inc.

Dynamic Registration and Configuration Protocol (DRCP)

Status of this memo

Abstract

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts [DHC]. DHCP was, however, designed for hosts on a fixed LAN, not for nodes roaming among commercial wireless networks. A Mobile IP [MIP] Foreign Agent gives some powerful plug and play capability for roaming hosts, especially when combined with some recent proposals [e.g., MIPA, MIPC, MIPD, MIPN, HAW, CEL, TIA]. Mobile IP functionality, however is not always needed and for some dynamic networks it may be undesirable to use Foreign Agents. This draft proposes a lightweight dynamic configuration protocol, called the Dynamic Registration and Configuration Protocol (DRCP). DRCP borrows heavily from DHCP and can switch to using DHCP protocol if only DHCP servers are present in the network; but adds features critical to roaming users. Most importantly, DRCP allows rapid configuration by moving address consistency checking from the critical path. Other new features

allow: a) clients to know when to get a new address independent of the layer-2 access technology, b) efficient use of scarce wireless bandwidth, c) clients to be routers, d) dynamic addition or deletion of address pools to any DRCP node, and e) message exchange without broadcast.

1. Introduction

Most future networks will use IP technology. To provide heterogeneity and flexibility, devices will likely access this IP-based network by directly sending IP packets. In such an environment it is natural to consider using IP-based protocols for user-network signaling, since it can be used across any wired or wireless access network.

The functions needed to support users' roaming among IP-based networks vary, depending on network, movement, and application characteristics. Three common functions are Registration, Configuration and Dynamic Address Binding. Registration allows roaming users to rapidly and automatically register their presence and their requirements with networks. Configuration allows networks to automatically configure roaming users to the particular network characteristics. Dynamic Binding allows corresponding nodes to locate roaming users and to allow continuous communication as the user moves among networks. This draft is concerned with the first two functions; it has nothing to say about dynamic binding, except that it should be a feature independent of the registration and configuration protocol. However, Dynamic Registration and Configuration Protocol does not mandate compulsory registration to the MN but it provides registration parameters to roaming users (such as local AAA server's address).

Alhough DRCP adds some new configuration capability, it has no other functions. DRCP may provide information about the location of a network registration, service negotiation, or mobility agent; but it must be combined with other protocols to perform these functions (e.g., use of Mobile IP protocol in co-located mode to register with a Home Agents). Furthermore, there are interesting possible application of DRCP, beyond the realm of configuring nodes roaming among a fixed infrastructure. An example of this is to combine DRCP with an address distribution protocol, such as DAAP [DAAP], to allow complete network autoconfiguration.

1.1 Architecture

Figure 1 shows an example of a high level functional architecture of a future IP-based network, with a roaming node attaching to various wired or wireless access networks. The access network may contain multiple hubs or base stations with at least one Edge Router and Controller (ERC) with connections to the rest of the network. We assume the mobile node keeps the same IP address anywhere within an access network, since micro mobility (e.g., among base stations) is

handled at layer 2. The mobile node may need, however, to get a new IP address when it moves to a new subnet (protocols such as HAWAII [HAW] or Cellular IP can be used [CEL] to allow node to keep their IP address within a single domain). The Regional Backbone connects all the edge router and controller in a single administrative domain and the global Internet interconnects all the regional networks.

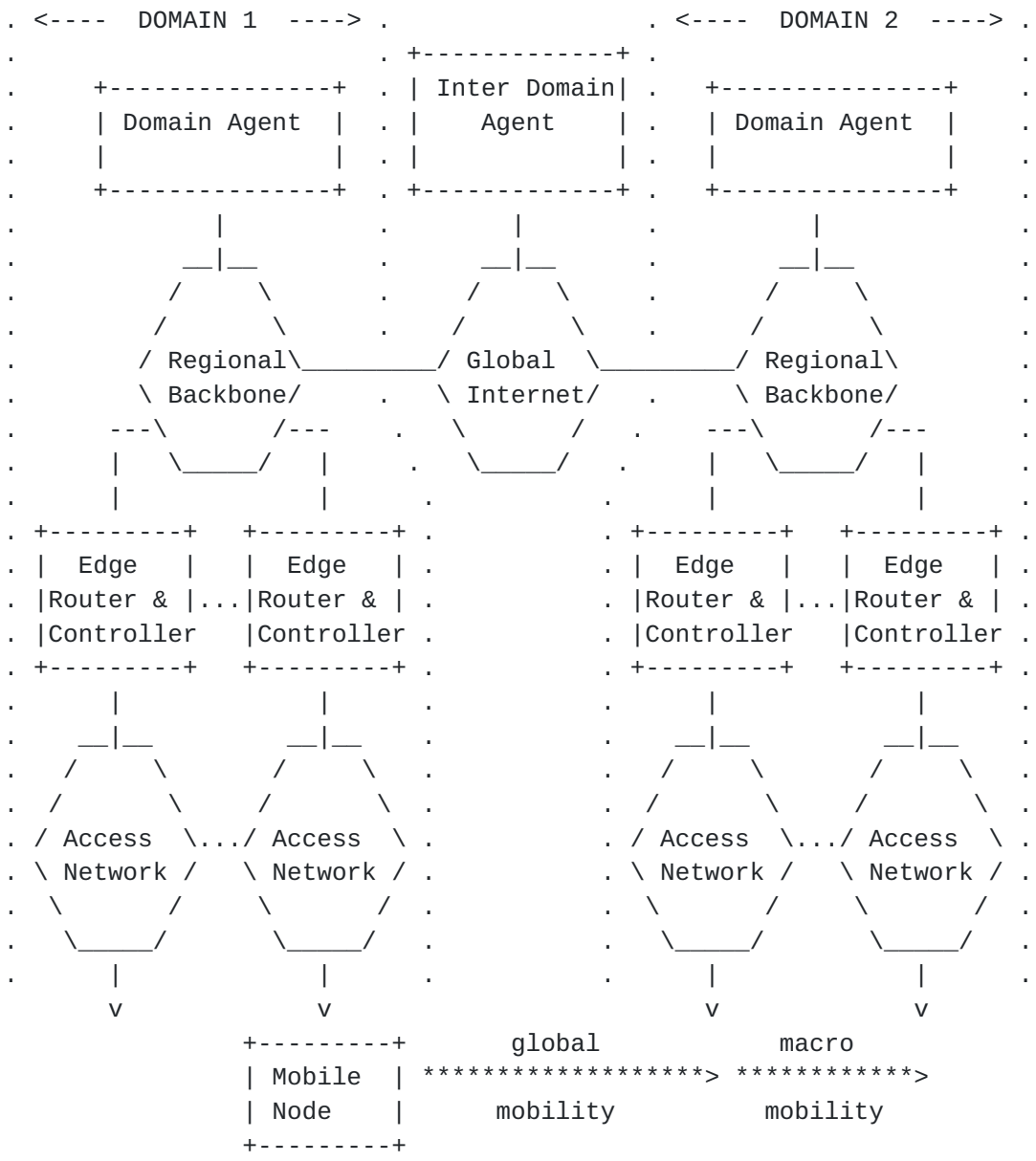


Figure 1: Example Functional Network Architecture for Supporting Universal Mobile Operation

1.2 DHCP Extensions

As discussed in the draft "Requirements for Extending DHCP into New Environments," [DHCR] the Dynamic Host Configuration Protocol (DHCP) represents the best and most flexible protocol for configuring nodes [DHC]. Recent proposals provide some enhancements to DHCP for

roaming users. For example there are proposals to adding authentication [DHCA], LDAP database management [DHCL], and dynamic updating of DNS [DHCD]. Unfortunately, these additions not only add to its complexity, they also leave some key configuration problems including:

o R1 Rapid client configuration (milliseconds rather than seconds).
o R2 Rapid client reconfiguration (independent of lease time or layer-2 access technology).
o R3 Efficient use of scarce wireless bandwidth.

- o R4 Allowing clients to be routers.
- o R5 Dynamic addition or deletion of address pools on any node.
- o R6 Message exchange without broadcast.

These six requirements are discussed in detail in [DHCR].

1.3 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 [REQ].

1.4 Overview

This draft proposes a light weight version of DHCP for roaming users, called the Dynamic Registration and Configuration Protocol (DRCP). DRCP adds many new features including rapid client configuration and efficient use of wireless bandwidth. Section 2 describes DRCP operations with client-server model while Section 3 presents the DRCP format.

1.5 Terminology

This document uses the following terms:

- o "DHCP"
  The Dynamic Host Configuration Protocol (DHCP) used to configure Internet hosts.

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

- o "DHCP relay agent"
  A relay agent is an Internet host that passes DHCP messages between DHCP clients and DHCP servers.

- o "DHCP server"
  A DHCP server is an Internet node that returns configuration parameters to DHCP clients.

- o "DRCP"
  The Dynamic Registration and Configuration Protocol (DRCP) used to configure nodes.

- o "DRCP client"
  A DRCP client is an Internet node (host or router) using DRCP to register with the network and obtain configuration parameters such as a network address.

- o "DRCP server"
  A DRCP server is an Internet node that owns a pool of IP addresses. The server can lease addresses from this pool to other DRCP nodes in its domain. Each domain running DRCP must have at

least one server, though there could be more in larger domains.

o "Edge Router and Controller"
An Edge Router and Controller (ERC) is an Internet node with a DRCP server that provides a centralized service to DRCP clients along with routing and other controlling functionalities.

o TBD = To Be Determined

2. Protocol Summary

The Dynamic Registration and Configuration Protocol (DRCP) uses many of the features found in DHCP. We require a new protocol, however, because DRCP's extended goals requires major enhancements to DHCP [DHCR].

2.1 DRCP Overview - Components

The Dynamic Registration and Configuration Protocol (DRCP) is based on a client-server model. Figure 2 shows how the client and server could map onto the network architecture shown in Figure 1. In general, however, the DRCP-server could be on any node in the subnet, not necessarily a router.

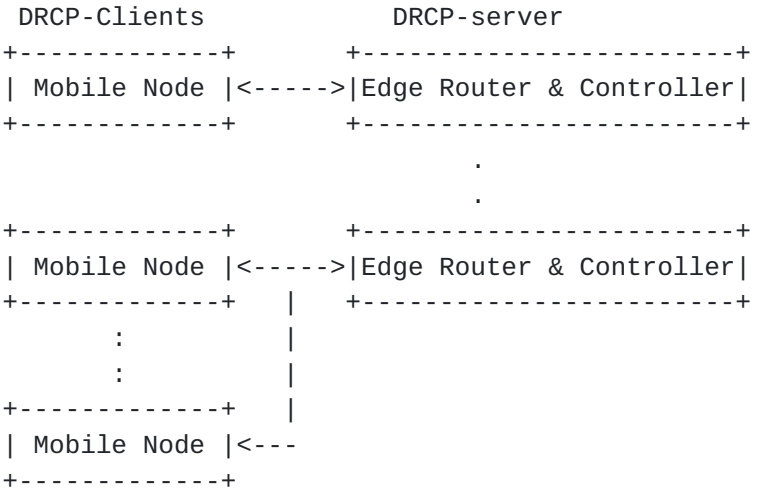


Figure 2 DRCP Client-Server model

The DRCP client-server model is similar to the client-server model of DHCP. There is, however, two subtle distinctions. First, any DRCP node (including client) can be on a router or host. The second distinction is that all DRCP nodes run the same program. The only

thing that makes a DRCP node a server is that it has configuration information, including an address pool and other configuration parameters to be used on an interface. A DRCP server must configure its own interface using the configuration information for that subnet. As we will show this allows for more flexible and robust operation.

2.2 DRCP Messages

DRCP messages have the same basic semantics as those used in DHCP. For example, the DHCPOFFER [DHC] has the same basic functions (and name) as DRCP_OFFER. New messages are needed in order to minimize message size (see Section 3). Like DHCP, DRCP uses UDP as its transport protocol. There are two types of DRCP signaling messages running on three different UDP ports:

a) All messages from a client are sent to the `DRCP_SERVER_PORT' port (number TBD).
b) All messages from a server are sent to the `DRCP_CLIENT_PORT' port (number TBD), except the DRCP_ADVERTISMENT.
c) DRCP_ADVERTISMENT messages from a server are sent to the `DRCP_ADVERTISEMENT_PORT' port (number TBD) on the client.

Figure 3 shows a general architecture for DRCP operation on a local subnet. In general a subnet requires only one server (as shown in Figure 2); however, we show the more general with redundant servers.

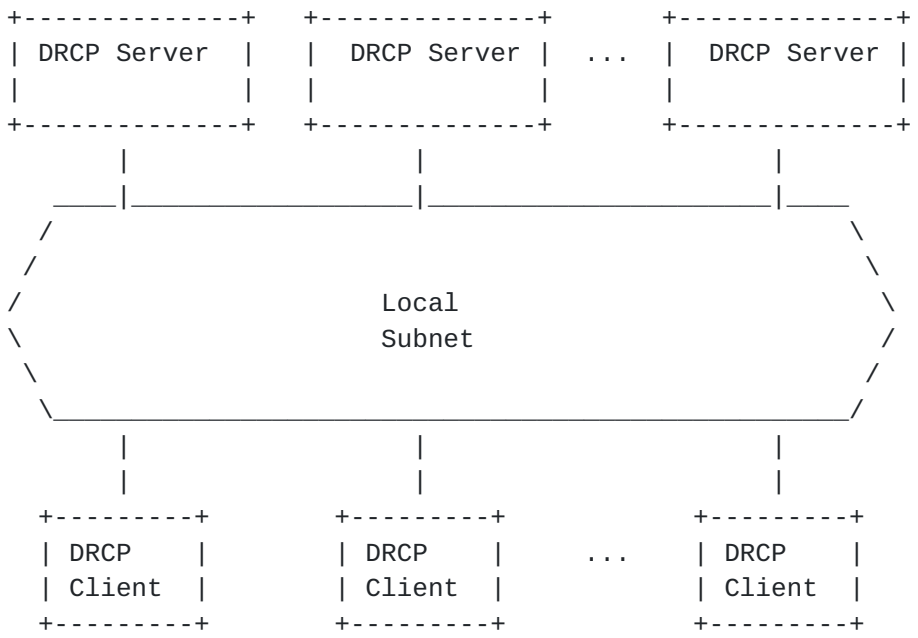


Figure 3 DRCP Node configuration on a Local Subnet

2.2.1 Messages from DRCP client

o DRCP_DISCOVER:
Registration message sent by a DRCP-client on its local subnet to request a new address and other configuration parameters. While a DHCPDISCOVER message must be broadcast [DHC], a DRCP_DISCOVER message may be broadcast or unicast depending whether the client knows the address of a DRCP Server (e.g., from a

DRCP_ADVERTISEMENT].

- DRCP_REQUEST:
  Registration message sent by a DRCP-client on its local subnet to request extending the lease on an address.

- DRCP_INFORM:
  Registration message sent by a DRCP-client on its local subnet to request new configuration parameters. This could be used, for example, if the client already has an externally configured network

address.

- o DRCP_DECLINE:
  Registration message sent by a DRCP-client on its local subnet to request a different address, either because the one assigned is not acceptable (e.g., it is already in use by another client) or because the client has moved to a new subnet.

- o DRCP_RELEASE:
  De-registration message sent by a DRCP-client on its local subnet to relinquish a network address and cancel remaining lease.

- o DRCP_ACCEPT
  Registration message sent by a DRCP-client on its local subnet in response to an OFFER from servers. The client accepts offered parameters from one server and implicitly declining offers from all others.

2.2.2 Messages from a DRCP server

- o DRCP_OFFER:
  Configuration message sent back to client on the same subnet where the DRCP server node received a DRCP_DISCOVER message.

- o DRCP_ACK:
  Configuration message broadcast by a Server on its local subnet in response to a DRCP_ACCEPT.

- o DRCP_NAK
  Message sent to a client or clients (may be broadcast) to tell them not to use an address or other service they requested. (e.g., when a client is using a wrong address).

- o DRCP_ADVERTISEMENT:
  Server periodically broadcasts (or unicast in response to a client using an incorrect address) the network information (such as Server IP address or Network address). Listening to this, client can understand the subnet change.

2.3 Basic Operation

A DRCP node is initially assumed only to know which of its interfaces is configuring using DRCP. If there are multiple interfaces, each interface may be configured in a different way. One interface may be configured by DRCP, another using a locally stored address, and a third as a DHCP-client. After boot-up, however, any interface

configured as a DRCP interface listens to messages on DRCP_ADVERTISMENT_PORT. During any message exchange a transaction id is used between the client and server and they must match for a given exchange.

2.3.1 Basic DRCP Client Operation

If a DRCP interface does not have a local address pool it becomes a

DRCP client. The client first broadcasts a DRCP_DISCOVER message (similar to a DHCPDISCOVER message) to the DRCP_SERVER_PORT. If it gets no response after DRCP_RETX_TIMEOUT, then it resends the DRCP_DISCOVER message. This process repeats for up to DRCP_RETX_MAX retransmissions.

If an unconfigured DRCP client receives a DRCP_ADVERTISEMENT message (on the DRCP_ADVERTISEMENT_PORT), then it will change to a unicast state, so the next DRCP_DISCOVER message will be unicast to the source address of the DRCP_ADVERTISEMENT.

If the client receives a DRCP_OFFER message, then it can immediately configure its interface with that address. There is no requirement to do check (e.g., using ARP) for others using the same address (as there is in DHCP).

After getting an address the client may periodically send out DRCP_REQUEST messages to renew the lease. These message are retransmitted until acknowledged by a DHCP_ACK message.

If a configured DRCP client receives a DRCP_ADVERTISEMENT message (on the DRCP_ADVERTISEMENT_PORT), then it will check if it can still use the same IP address. If it cannot use the same IP address, then the client must unicast a new DRCP_DISCOVER message in order to get a new address. This helps to detect the subnet change. It happens only when a client moves to a new subnet.

2.3.2 Basic DRCP Server Operation

If a DRCP interface has a local configuration information (including an address pool) for that interface, then it becomes a DRCP server. The DRCP server must first use the first address from the address pool to configure its own interface. It can then use the rest of the address pool to allocate individual addresses directly to clients on the same subnet as that interface.

The server may send periodic DRCP_ADVERTISEMENT messages (on the DRCP_ADVERTISMENT_PORT) every DRCP_ADVERTISMENT_PERIOD time.

The server listens for DHCP_DISCOVER broadcast or unicast to the DRCP_SERVER_PORT. If it gets a DHCP_DISCOVER message, then the DRCP server can immediately send a DRCP_OFFER message with valid IP address and other configuration parameters from its configuration information. The DRCP_OFFER will be resent every DRCP_OFFER_PERIOD for up to DRCP_SERVER_MAX retransmissions, or until it receives a DRCP_ACCEPT or DRCP_DECLINE from the client.

2.4. Example Applications

This section considers the operation of DRCP in the type of network shown in Figure 1.

2.4.1 Client Moves into a New Domain

If a client has just been rebooted or moves to a new domain, then there may be a flow of messages such as that shown below.

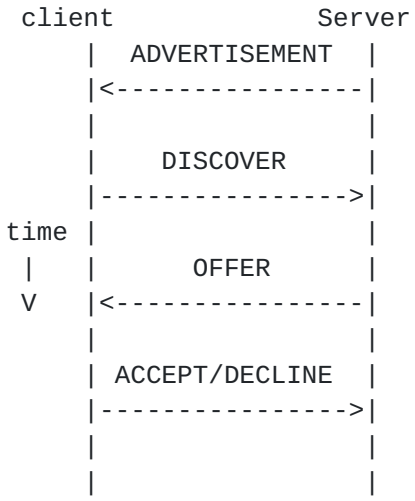


Figure 4 DRCP Client Moves into a New Domain/Subnet

The figure above shows the server initiates periodic ADVERTISEMENT messages. Upon receiving the ADVERTISEMENT message, the client transmits and retransmits the DISCOVER message until it gets an OFFER message or the timer expires. The server transmits and retransmits the OFFER message until it gets an ACCEPT or DECLINE message or timer expires.

One key difference from DHCP is that there is no ACK message from the server (and the client accepts with an ACCEPT rather than a REQUEST message). A second key difference is that we assume the configuration can be used as soon as the OFFER is received (duplicate detection is handled in the background).

2.4.2 Client Renews/Release existing lease

If a DRCP client wants to renew or release its lease, then there will be a flow of DRCP messages such as that shown below.

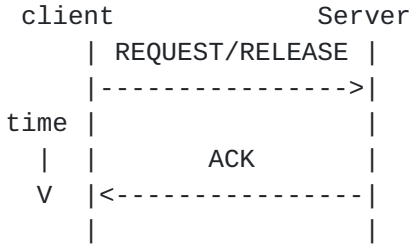


Figure 5 Extending the lease within a domain

The server sends an ACK message in response to the REQUEST/RELEASE.

2.4.3 **Client** Re-negotiates an OFFER

If a DRCP client does not like an OFFER, then it can request a new

offering using message flow as shown below.

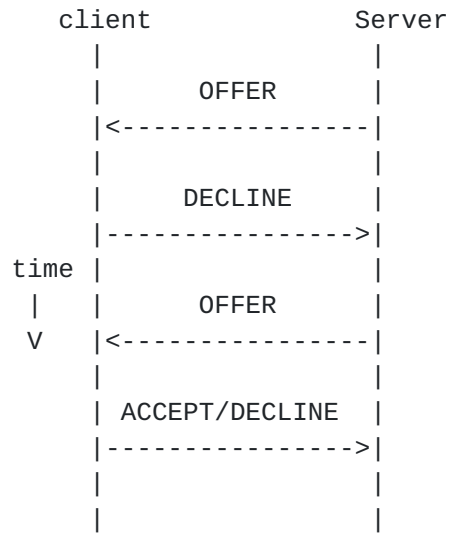


Figure 6 DRCP Client Re-negotiating an OFFER

Upon receiving the DECLINE message the DRCP server can either do nothing or can send a new OFFER message. In response to the new OFFER message, the client can either decline again (send another DECLINE message) or accept (send an ACCEPT message).

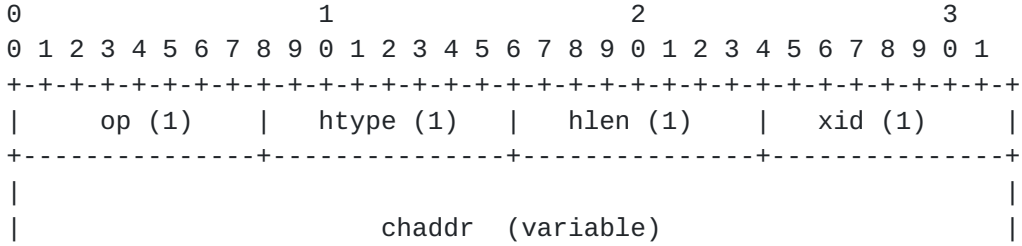
3. DRCP Message Format

All DRCP messages are sent in UDP/IP packets to special DRCP ports and are 32-bit aligned.

3.1 Common Header Format

3.1.1 Common Header for Message from the Client

All DRCP message from the client (to the DRCP_SERVER_PORT) have the same general format (size shown in braces):



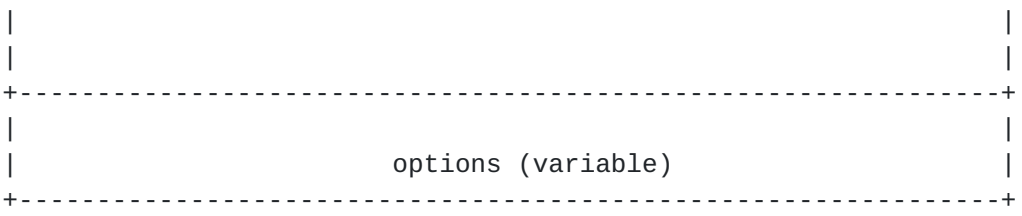


Figure 8 Format of a DRCP client message

The various fileds are See Section 3.2 for details):

FIELD	OCTETS	DESCRIPTION
op	1	Message OpCode.
htype	1	Hardware address type.
hlen	1	Hardware address length in bytes.
xid	1	Transaction ID.
chaddr	var.	Client hardware address (e.g 16 bytes for 802.X)
options	var.	Optional parameters field.

3.1.2 Common Header for Message from the Server

All DRCP message from the server (to the DRCP_CLIENT_PORT) have the same geenral format (except a DRCP_ADVERTISEMENT):

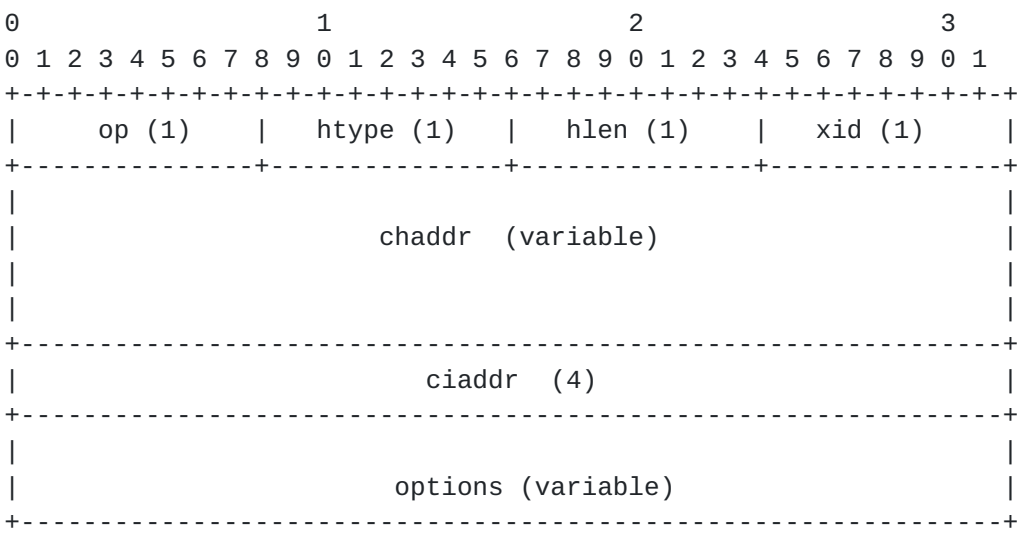


Figure 8 Format of a DRCP client message

The fileds are the same as for the client except that it includes

FIELD	OCTETS	DESCRIPTION
ciaddr	4	Client IP address

3.1.3 DRCP_ADVERTIEMENT

The format of the DRCP_ADVERTISEMENT is under review.

3.2 Common Header Content

3.2.1 OpCode

The opcode field consists of version number (ver), message type (mtype) and broadcast(B) flag as shown in figure 9.

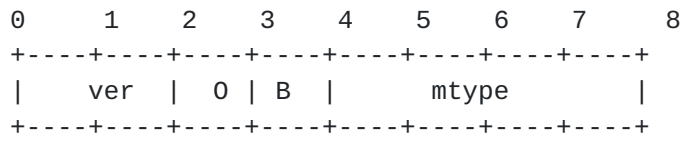


Figure 9 Op Code Field

FIELD	BITS	DESCRIPTION
ver	2	Version Number. Currentlty 001 (binary).
O	1	Options Flag (`1` if at least one option is present).
B	1	BroadCast Flag. Similar to DHCP broadcast flag.
mtype	4	Message type.

Possible values for Message types are

Message Value	Message Type
0 0 0 1	DRCP_DISCOVER
0 0 1 0	DRCP_REQUEST
0 0 1 1	DRCP_INFORM
0 1 0 0	DRCP_ACCEPT
0 1 0 1	DRCP_DECLINE
0 1 1 1	DRCP_RELEASE
1 0 0 1	DRCP_OFFER
1 0 1 0	DRCP_ACK
1 0 1 1	DRCP_NAK
1 1 1 1	DRCP_ADVERTISEMENT

3.2.2 Htype

See ARP section in "Assigned Numbers" RFC. For example: Htype = '1' means it is a 10mb ethernet.

3.2.3 Hlen

Length of chaddr field in bytes. For example Hlen is set to '6' for 10mbps ethernet.

3.2.4 Xid

A random number chosen by the client. It is used by the client and server to associate messages and responses between a client and a server.

3.2.5 Ciaddr

The IP address assigned to a client by a server.

3.3 Options

All information, other than what is in the common header, must be included as options. All options have a common 4 byte header shown below:

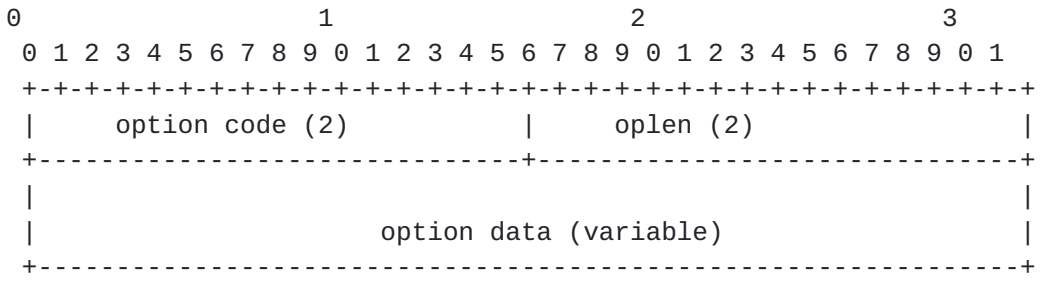


Figure 11 Format of Option field

FIELD	OCTETS	DESCRIPTION
option code	2	Defines the code of the option field. Same as in DHCP options
oplen	2	Length of the option data following
option data	var	Option data

4. DRCP Interface Messages

DRCP has the feature that its configuration information can be changed dynamically. This section contains the API to DRCP that allows users or other processes to interact with DRCP. However, the APIs and other features are TBD.

5. Security Considerations

DRCP is built directly on UDP and IP which are inherently insecure. IPsec and other security protocols can not be used since the client does not have any IP address. However, client-server authentication to provide for authetication of the source and contents of DRCP messages are under review.

6. Acknowledgments

The authors wish to acknowledge the contributions of other members of the ITSUMO (Internet Technologies Supporting Universal Mobile Operation) team from Telcordia (P. Agrawal, J.C. Chen, A. Dutta, D. Famolari, F. Vakil, P. Ramanathan, H. Sherry and R. Wolff) and Toshiba America Research Incorporated (T. Kodama).

Some of the initial ideas of DRCP came out of a project on complete

autoconfiguration within a domain, funded by the U.S. Army Research Laboratory (ARL) under the Advanced Telecommunications and Information Distribution Research Program (ATIRP) Consortium.

6. References

[CEL] A. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turanyi and A.

Valko, "Cellular IP", Internet draft, <draft-ietf-mobileip-cellularip-00.txt>, January 2000, Work in progress.

[DAAP] A. McAuley and K. Manousakis, "Self-Configuring Networks", To appear in Proceedings of MILCOM2000, October 2000.

[DHC] R. Droms, `` Dynamic Host Configuration Protocol,'' Request for Comments 2131, Mar 1997.

[DHCA] R. Droms, "Authentication for DHCP Messages", <draft-ietf-dhc- authentication-14.txt>, July 2000 Work in progress.

[DHCD] Y. Rekhter, M. Stapp, "Interaction between DHCP and DNS," <draft-ietf-dhc-dhcp-dns-12.txt>, March 2000, Work in progress.

[DHCL] A. Bennett, B. Volz, A. Westerinen, " DHCP Schema for LDAP," <draft-ietf-dhc-schema-02.txt>, March 2000, Work in progress.

[DHCR] A. Mcauley, S. Das, S. Baba and Y. Shobatake, "Requirements for Extending DHCP into New Environments", <draft-ietf-dhc-enhance -requirements-00.txt>, March 2000, Work in progress.

[HAW] R. Ramjee, T. La Porta, S. Thuel and K. Varadhan: "IP micro- mobility support using HAWAII", <draft-ramjee-micro-mobility-hawaii-00.txt>, June 1999, Work in progress.

[MIP] Perkins, C., Editor: "IP Mobility Support", RFC 2002, October 1996.

[MIPA] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements,"<draft-ietf-mobileip-aaa-reqs-04.txt>, June 2000. Work in progress

[MIPC] E. Gustafsson, A. Jonsson, E. Hubbard, J. Malmkvist, A. Roos, "Requirements on Mobile IP from a Cellular Perspective," <draft-ietf-mobileip-cellular-requirements-01.txt>, June 1999. Work in progress.

[MIPD] P. R. Calhoun and C.E. Perkins, "DIAMETER Mobile IP Extensions", Internet draft, <draft-calhon-diameter-mobileip-09.txt>, July 2000, Work in

Progress.

[MIPN] P. Calhoun and C.E. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

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

[TIA] Tom Hiller, et al. "3G Wireless Data Provider Architecture

Using Mobile IP and AAA," draft-hiller-3gwireless-00.txt, March 1999.

7. Authors' Addresses

Anthony J. McAuley
MCC 1C235B, Telcordia
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4698
email: mcauley@research.telcordia.com

Subir Das
MCC 1D210R, Telcordia
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4959
email: subir@research.telcordia.com

Sunil Madhani
MCC 1B246B, Telcordia
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 5162
email: sunil@research.telcordia.com

Shinichi Baba
Toshiba America Research Inc.
P.O. Box 136 Convent Station, NJ 07961-0136
Phone: +1 973 829 4759
email: sbaba@tari.toshiba.com

Yasuro Shobatake
Toshiba America Research Inc.
P.O. Box 136 Convent Station, NJ 07961-0136
Phone: +1 973 829 3951
email: yasuro.shobatake@toshiba.co.jp