Network Working Group   Anthony McAuley
INTERNET-DRAFT   Subir Das
Internet Engineering Task Force   Telcordia Technologies
draft-ietf-dhc-enhance-requirements-00.txt   Shinichi Baba
Date: March 8, 2000   Yasuro Shobatake
Expires: August, 2000   Toshiba America Research Inc.

Requirements for Extending DHCP into New Environments

Status of this memo

Abstract

The Dynamic Host Configuration Protocol (DHCP) provides a widely deployed framework for host registration and configuration [DHC]. DHCP, however, was designed only for fixed hosts on physically secure LANs. Other protocols fill some of the gap. PPP [PPP] is a good solution for many commercial service providers (where framing is needed). Mobile IP [MIP] is ideal for registering and configuring roaming users (when transparent address binding is needed). This still leaves many environments where there is no ideal solution, such as: roaming users who do not need transparent address binding (e.g., a mobile web browser), and commercial service providers who want to support home networking with multiple nodes. This draft proposes DHCP as the best protocol to meet these new needs, because it leave open how (and whether) to provide other functions, such as framing (e.g., PPP), locating (e.g., Mobile IP in co-located mode), inter-domain AAA (e.g., [AAAR]), or address distribution (e.g., [DAAP]). We describe and solicit feedback on seven new requirements that would be placed on DHCP to meet these needs.

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 they can be used across any wired or wireless access network.

1.1 Architecture

Figure 1 shows a high level functional architecture of a future IP-based network, with both a fixed and a roaming clients attaching to various wired or wireless Access Networks. We assume the client has at least one physical interface onto the access network, but can also have other physical and virtual interfaces. The access network, which may contain multiple Layer 2 nodes (such as hubs), connects to at least one Edge Router and Edge Agent (that may be co-located). The Regional Backbone connects all the Edge Routers in an administrative domain and the Global Internet interconnects all the regional networks.

We assume the network may need to change client configuration of even fixed nodes at any time, but that typically clients keep the same configuration (e.g., IP address) while they are within a given access network. Micro mobility within the access network is handled at Layer 2. Depending on how routing is done, the client may or may not need a new configuration when it moves to a new access network within the same domain (macro mobility) [CEL] [HAW]. We assume, however, that clients must be reconfigured when moving to a new domain (global mobility).

```
   . <---- DOMAIN 1 ----> .                    . <---- DOMAIN 2  ----> .
   .        +---------+   .  +--------------+  .    +---------+        .
   .        | Domain  |   .  | Inter-domain |  .    | Domain  |        .
   .        | Agent   |   .  | Agent        |  .    | Agent   |        .
   .        +---------+   .  +--------------+  .    +---------+        .
   .             |        .         |          .         |             .
   .           __|__      .       __|___       .       __|__           .
   .          /     \     .      /      \      .      /     \          .
   .         /       \    .     /        \     .     /       \         .
   .        / Regional\________/ Global   \_________/ Regional\        .
   .        \ Backbone/     .  \ Internet /  .      \ Backbone/        .
   .     ____\       /____   .  \        /  .    ____\       /____     .
   .    /     \_____/     \   .  \______/  .    /     \_____/     \    .
   .   /         |         \   .          .    /         |         \   .
   .  /          |          \   .        .    /          |          \  .
   .         +--------+          .       .          +--------+         .
   .      .. | Edge   | ..       .       .       .. | Edge   | ..      .
   .         | Router |          .       .          | Router |         .
   .         +--------+          .       .          +--------+         .
   .         .. |  | ..          .       .          .. |  | ..         .
   . +--------+ |  | +--------+  .       .  +--------+ |  | +--------+ .
   . | Edge   | |  | | Edge   |  .       .  | Edge   | |  | | Edge   | .
   . | Agent  | |  | | Agent  |  .       .  | Agent  | |  | | Agent  | .
   . +--------+ |  | +--------+  .       .  +--------+ |  | +--------+ .
   .  |         |  |         |   .       .   |         |  |         |  .
   .  | _____   |  |   _____ |   .       .   | _____   |  |   _____ |  .
   .  |/     \__|  |__/     \|   .       .   |/     \__|  |__/     \|  .
   .  /       \      /       \   .       .   /       \      /       \  .
   . / Access  \ .. / Access  \  .       .  / Access  \ .. / Access  \ .
   . \ Network /    \ Network /  .       .  \ Network /    \ Network / .
   .  \       /      \       /   .       .   \       /      \       /  .
   .   \_____/        \_____/    .       .    \_____/        \_____/   .
   .      |              |       .       .       |              |      .
          |              |                       |              |
     +---------+    +---------+      global          macro
```

```
   | Fixed    |    | Mobile   | ***************> *************>
   | Client   |    | Client   |     mobility          mobility
   +----------+    +----------+
```

Figure 1: Functional Network Architecture

Figure 1 is meant to be very general functional diagram. It does not, for example, specify where a Base Station (BS) is located. BSs could be within the access networks (Layer 2 BS) or in the Edge Router (IP BS). The Domain and Inter-Domain agents which perform functions such as registration and AAA, are shown as single boxes; but both could be implemented as multiple nodes (possibly in a hierarchical structure).

1.2 Functional Scope

The functions needed to support users' accessing IP-based networks vary, depending on network, user, and application characteristics. Some basic functions include:

- o Registration: Users indicate their presence and their requirements to a network (e.g., give a user name [NAI]).
- o Configuration: Networks adapt nodes to the particular network characteristics (e.g., give an IP address).
- o Framing: Indicates the start and end of packets in a data stream.
- o Compression: Compress RTP/UDP/TCP/IP header and data over an access network.
- o Dynamic Address Binding: Allows corresponding nodes to locate users and allows continuous communication as the user moves among networks.

This draft is concerned only with the first two functions, which we believe have a natural association (see Section 3.5). This draft considers only server based methods for registration and configuration within a single IP domain. The network servers are themselves configured with information such as an IP address pool; but, server configuration is beyond the scope of this draft. We assume each access network has at least one edge server (possibly co-located with the edge router), though it could be as simple as a relay agent.

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 Terminology

This document uses the following terms:

o "AAA"
  Authentication, authorization and accounting

o "BOOTP"
  The Bootstrap Protocol (BOOTP) [BOO1] [BOO2].

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 "Domain Agent"
An Internet node that provides a centralized service within a domain (e.g., DHCP server)

o "Edge Router"
An IP router connecting an IP subnet to other networks.

o "Edge Agnet"
An IP node (host or router) that is connected to an IP subnet and provides services (e.g., DHCP relay agent).

o "Inter-domain Agent"
An Internet node that provides services for a node anywhere in the Internet.

o "NAI"
Network Access Identifier of the form user@domain [NAI].

2 Registration and Configuration Protocols

There are several TCP/IP protocol choices for performing registration and configuration:

- o The Point-to-Point Protocol (PPP).
- o The Mobile IP protocol (MIP).
- o The Dynamic Host Configuration Protocol (DHCP).

2.1 PPP

Although its primary function is packet framing, PPP also provides well tested and widely deployed registration and configuration capabilities. PPP [PPP] clients sends registration information, such as login and password to an access concentrator on the Layer 2 network to which the client is connected. The access concentrator can then either directly configure the client or use the Layer 2 Tunneling Protocol [PPPL] to tunnel PPP packets to and from a server anywhere in the Internet. The powerful PPP registration and configuration capabilities are now even used when framing is not needed (e.g., PPPoE [PPPE]). The only cost is that it leaves some of the PPP framing overhead (2 bytes for framing, 2 bytes for CRC, up to 4 other bytes, and bit or byte stuffing overhead).

2.2 Mobile IP

Although its primary function is providing location service and continuous connectivity to roaming users, Mobile IP [MIP] [MIP6] also provides a flexible registration and configuration capabilities. The Mobile IP client sends registration information to a Foreign Agent [MIPA] [MIPC] [MIPD] [MIPN] [MIPS] [MIPT] on the Layer 2 network to which the client is connected. The Foreign Agent can then configure the client, after getting authorization from the user's Home Agent. The registration and configuration capabilities could be provided by Mobile IP for all roaming users, even when transparent binding is not needed (e.g., for web browsing) or may need alternative mechanisms (viz., SIP for real-time applications [SIP] [SIPM]). The only costs are: a) triangular routing, b) having to configure a permanent home address, and c) depending on a home network.

2.3 DHCP

DHCP provides a well tested and widely deployed framework for passing configuration information to hosts [DHC]. A DHCP client in a host broadcasts a DISCOVER control message to the access network. A server picks up the message and either a) returns an OFFER message (server) or b) relays the message to a central DHCP server. DHCP is

unique in that it:
 o Has no additional functions (e.g., framing or address binding).
 o Requires no client preconfiguration (e.g., for home addresses).
 o No overhead to data traffic (out-of-band signaling).
 o Allows nodes to go on and off without re-registration.
 o Allows a single network server per domain (using relay agents).

DHCP is likely to continue to gain in popularity with recent enhancements, such as Server fail-over [DHCF], Load balancing [DHCB], Dynamic updating of DNS [DHCD], LDAP database management [DHCL], and Authentication [DHCA].

2.4 Choice

PPP, Mobile IP and DHCP were designed for different environments. Thus, network designers select the registration and configuration protocol that best fits the types of access network and likely client applications. For example, networks using phone lines for access will typically use PPP; wireless providers supporting roaming TCP application, such as telnet and ftp, will use Mobile IP; and corporate networks will use DHCP.

The open question is what registration and configuration protocol will be used in environments that do not fit into the PPP, Mobile IP, or DHCP assumptions? Examples of these environments are:
 o Commercial service providers who want to support flexible home networking.
 o Roaming users who either do not need transparent binding (e.g., just web browsing) or prefer alternative mechanisms (e.g., SIP for real-time applications).

PPP, Mobile IP and DHCP could all be adapted to better some or all of these environments. This draft proposes DHCP as the best protocol to meet these new needs, because it leave open how (and whether) to provide other functions, such as framing (e.g., PPP), locating (e.g., Mobile IP in co-located mode), inter-domain AAA (e.g., [AAAR]), or address distribution (e.g., [DAAP]). We describe the new requirements that would be placed on DHCP in the next Section.

3. Requirements for Extending DHCP into New Environments

Though DHCP has many desirable features, the following requirements created by new environments are not fully met by DHCP:

- o R1 Rapid client configuration (milliseconds rather than seconds).
- o R2 Rapid client reconfiguration (independent of lease time).
- o R3 Efficient use of scarce wireless bandwidth.
- o R4 Allowing clients to be routers.
- o R5 Enhanced registration (e.g, user identification and security).
- o R6 Flexible proxies that can act as both relay or server.
- o R7 Allowing dynamic server and relay reconfiguration.

This section gives a brief description and motivation for each new requirement.

3.1 Rapid configuration

Configuration latency is critical to users roaming among wireless networks. A DHCP client accepts an OFFER by returning a REQUEST message to the server (which the server ACKS). The client, however, only configures its new address after checking that no other node on the subnet is using it. The DHCP specification [DHC] says a client SHOULD do ARP checking before an assigned address is used. This "in-line" checking results in long delay (typically 3-15 seconds) before communication can resume after a move; too long for many roaming users. While duplicate detection is desirable, it need not be part of the critical path. One possible alternative, for example, would be to have the server do ARP checking on addresses before they are requested.

The goal is to get configuration in milliseconds (bounded mostly by by the speed of the access link) rather than seconds.

3.2 Rapid reconfiguration

A recent draft [DHCR] has proposed a new DHCP FORCERENEW message that allows servers to force clients to immediately reconfigure. To enable rapid reconfiguration (e.g., when a roaming user moves into a new subnet or topology changes), clients must rapidly detect the server request. Today, DHCP clients typically go into sleep mode, not listening to DHCP messages until the lease is due for renewal. Clients can use external triggers, such as a layer 2 hand-off indication or an SNMP V3 request message, to jump DHCP into a new state. These triggers, however, may not always: a) be available, b) be standardized, c) have enough information. The information may help client to decide if it is in a new subnet or to get the location of a DHCP server (to prevent having to broadcast).

The goal is to be able to rapidly reconfigure DHCP clients, at any time, without relying on external triggers.

3.3 Bandwidth Efficiency

DHCP message overhead is considerably larger than needed, mainly because DHCP kept the same syntax as BOOTP [BOO1] [BOO2] [BOOD]. This was not a problem in the old paradigm where hosts connect to DHCP servers over high speed LANs; especially since DHCP overhead mainly occurs when a host first boots and DHCP adds nothing to normal packet communication overhead. The overhead is perhaps only a problem for roaming nodes using some wireless access networks. Depending on the size of the IP subnets, roaming users might need to reconfigure as fast as every few seconds. Depending on the speed and error rate of the wireless access networks, reducing DHCP message size could significantly improve bandwidth efficiency. (The error rate can be important since larger messages result in higher probability of loss, that increases latency and bandwidth needs.)

The goal is to minimize DHCP message size, by reducing the size of individual DHCP messages and possibly by reducing the total number of messages.

3.4 Clients as Routers

DHCP specification [DHC] says clients must be hosts and that it "is not intended for use in configuring routers." This was not a problem in the old paradigm, where routers were typically part of a hierarchical network that could be manually configured by a system's administrator. As the size and complexity of networks increase (e.g., with more small devices with low power wireless interfaces), routing functionality becomes desirable in places where manual configuration is not desirable. We are NOT proposing that DHCP be extended to simultaneously configure multiple router interfaces or to distribute address pools; only that DHCP could configure a single router interface over a subnet where there is a DHCP server (or relay). This would require no change in DHCP functionality; only a change in allowable application.

The goal is to allow DHCP to configure hosts and routers.

3.5 Enhanced Registration

Commercial service providers need a scalable way to identify and authenticate users. In addition they may need other registration information such as: a) the location of the client's AAA server (for inter-domain authentication [DHCZ], b) negotiate service requirements and costs, and c) trigger other services (possibly based on a user profile). Many of these features are now being defined for DHCP, but filling the missing needs would be helpful. We assume that DHCP itself only deals with intra-domain registration; a separate AAA protocol [AAAD] [AAAR] meets the inter-domain requirements.

The registration and configuration could be done in separate protocols; however we believe integrating the two functions is desirable. First, it reduces the latency, since it requires only one round trip from the client to the network. Second, it forces users to register before they can be configured. Clearly, devious users could still configure themselves, but now they cannot use

DHCP to do this.

The goal is to allow DHCP to meet the registration needs of diverse service providers.

3.6 DHCP Proxies

A DHCP client must either connect to a node acting as a DHCP server or connect to a DHCP relay. When a client first activates or moves into a new domain, DHCP message are best relayed to a central server (such as the Domain Agent in Figure 1); however, when users roaming among subnets within a domain DHCP message may best be handled locally. This would require no change in DHCP functionality; only a change in allowable application.

The goal is to allow a subnet proxy to act as both a relay and server, depending on a client's status.

3.7 Dynamically changing server (and relay) parameters

In some networks it may be desirable to dynamically change the preconfigured information in DHCP servers (and relay agents). For example, the address-pool may change if a topology change occurs [DAAP]. While DHCP should have nothing to do with updating address-pools, it should be able to handle dynamic changes in this information. If an external application changed the information, DHCP should gracefully handle the change (e.g., it may immediately update all its clients). This would require no change in DHCP protocol, only that: a) there is a common configuration framework (e.g., [DHCL]), and b) that DHCP servers and relay agents allow dynamic changes in preconfigured information.

The goal is to allow dynamic modification of DHCP server (and relay) configured parameters, such as the address-pool, by an external entity.

4 Discussion

The purpose of this draft is to stimulate discussion and solicit feedback on enhancing DHCP into new environments. These environments include roaming users who do not need transparent address binding (e.g., a mobile web browser) or commercial service providers whose access network provides framing (e.g., a cable access network). Given the large paradigm shift created by these new environments, it is an open question on how to achieve these changes. At the highest level we could slowly enhance DHCP, while maintaining backwards compatibility. A more radical approach would be the creation of a sister protocol such as DRCP [DRCP]. We have not given specific approaches or mechanisms here, except as examples, because we initially want to focus on the requirements.

5. Acknowledgments

The authors 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, S. Madhani, F. Vakil, P. Ramanathan, H. Sherry and R. Wolff) and Toshiba America Research Incorporated (T. Kodama). Also thanks to

Steve Gonczi of Process Software for his helpful suggestions.

The initial ideas came out of a project on complete network autoconfiguration within a domain [DAAP], funded by the U.S. Army Research Laboratory (ARL) under the Advanced Telecommunications and Information Distribution Research Program (ATIRP) Consortium.

6. References

[AAAD] P. Calhoun and A. Rubens, "DIAMETER Base Protocol," Internet draft, Work in Progress, Nov 1998.

[AAAR] C. Rigney, A. Rubens, W. Simpson, and S. Willens, "Remote Authentication Dial in User Service (RADIUS)," Request for Comments 2138, Apr 1997.

[BOO1] B. Croft & J. Gilmore, "Bootstrap Protocol (BOOTP)", RFC 951, Stanford and SUN Microsystems, September 1985.

[BOO2] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, Carnegie Mellon University, October 1993.

[BOOD] Droms, D., "Interoperation between DHCP and BOOTP", RFC 1534, Bucknell University, October 1993.

[CEL] Valko, A., Campbell, A. and Gomez, J.: "Cellular IP", Internet draft, <draft-valko-cellularip-00.txt>, Work in progress, November 1998.

[DAAP] A. McAuley and K. Manousakis, "Self-Configuring Networks." To appear Proc. of 4'th Advanced Telecommunications and Information Distribution Research (ATIRP) Conference, University of Maryland, March 2000.

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

[DHCA] R. Droms, W. Arbaugh, "Authentication for DHCP Messages", <draft-ietf-dhc-authentication-12.txt>, Work in progress, October 1999.

[DHCB] B. Volz, S. Gonczi, T. Lemon, R. Stevens, "DHC load balancing algorithm," <draft-ietf-dhc-loadb-00.txt>, Work in progress, October 1999.

[DHCD] Y. Rekhter, M. Stapp, "Interaction between DHCP and DNS," <draft-ietf-dhc-dhcp-dns-10.txt>, Work in progress, June 1999.

[DHCL] A. Bennett, B. Volz, A. Westerinen, "DHCP Schema for LDAP," <draft-ietf-dhc-schema-00.txt>, Work in progress, June 1999.

[DHCF] R. Droms, K. Kinnear, M. Stapp, B. Volz, S. Gonczi, G. Rabil, M. Dooley, A. Kapur, "DHCP Failover Protocol," <draft-ietf-dhc-failover-05.txt>, Work in progress, October 1999.

[DHCR] P. De Schrijver, Y. T'Joens, C. Hublet, "Dynamic host configuration : DHCP reconfigure extension," <draft-ietf-dhcpv4-reconfigure-01.txt>, Work in progress, March 2000.

[DHCZ] S. Das, A. McAuley, S.Baba, and Y.Shobatake, "Authentication, Authorization, and Accounting Requirements for Roaming Nodes using DHCP," <draft-ietf-dhc-aaa-reqs-00.txt>, Work in Progress, March 2000.

[DRCP] A. McAuley, S. Das, S.Baba, and Y.Shobatake, "Dynamic Registration and Configuration Protocol (DRCP)," <draft-itsumo-drcp-00.txt>, Work in Progress, October 1999.

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

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

[MIP6] D. Johnson and C. Perkins, "Mobility Support in IPv6," <draft-ietf-mobileip-ipv6-09.txt>, Work in Progress, Oct 1999.

[MIPA] S. Glass, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," <draft-ietf-mobileip-aaa-reqs-00.txt>, Work in progress, October 1999.

[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>, Work in progress, June 1999.

[MIPD] P. Calhoun and C.E. Perkins, "DIAMETER Mobile IP Extensions," Internet draft, Work in Progress, Nov 1998.

[MIPN] P. Calhoun and C.E. Perkins, "Mobile IP Network Access Identifier Extension," <draft-ietf-mobileip-mn-nai-05.txt> Work in progress, October 1999.

[MIPS] B. Patil, R. Narayanan & E. Qaddoura, "Security Requirements/ Implementaion Guidelines for Mobile IP using IP security" Internet draft, Work in Progress, June,1999.

[MIPT] Tom Hiller, et al. "3G Wireless Data Provider Architecture Using Mobile IP and AAA," <draft-hiller-3gwireless-00.txt>, Internet draft, Work in progress, October 1999.

[NAI] B. Aboba and M. A. Beadles, "The network access identifier," RFC 2486, January 1999.

[PPP] W. Simpson, "The Point to Point Protocol (PPP),: Internet STD 51, July 1994.

[PPPE] L. Mamakos, et al., "Method for Transmitting PPP Over Ethernet (PPPoE)," RFC 2516, February 1999.

[PPPL] W. Townsley, et al, "Layer Two Tunneling Protocol L2TP," RFC 2661, August 1999.

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

[SIP] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP:

Session Initiation Protocol," RFC 2543, March 1999.

[SIPM] E. Wedlund and H. Schulzrinne, "Mobility Support using SIP", Proc. of second ACM International Workshop on Wireless Mobile Multimedia (WOWMOM'99), pp 76-82, August, 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

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