DHCP for Mobile Networking with TCP/IP

Charles E. Perkins and Tangirala Jagannadh
IBM, T.J. Watson Research Center
Hawthorne, NY 10562

Abstract

Mobile-IP and the Dynamic Host Configuration Protocol(DHCP) are two protocols which are likely to be implemented together for use with wireless computers. We explore the ways that they can be used with in mobile computers.

These protocols interact in subtle ways, presenting a system architect with a variety of trade-offs that need careful analysis. We detail the important interactions and system design issues, and also explain the design and implementation of a new DHCP option for mobile computers. The difference between mobility and portability is explained; this paper only emphasizes approaches for mobility. We explore implementation issues that we have encountered.

1 Introduction

The capacity and processing power of handheld and laptop computers has continued to grow rapidly over the recent years. Moreover, battery operation and wireless communications devices are becoming standard features, especially infrared and radio frequency adapters ([1],[2]). Consequently, as never before computing resources are at our fingertips, unconstrained by cabling or power needs. People will soon almost always have powerful computers and convenient data paths available.

These fortunate circumstances will encourage mobile computer users to establish frequent connections to the resources of the Internet, and drive the deployment of mobile networking protocols. At the same time, the new market of Internet users, including mobile users, will be populated by many people who do not have the expertise nor desire to administer and configure their computers as has been up until now required to effectively communicate with other Internet hosts. Recognizing this, TCP/IP network engineers have begun deployment of the Dynamic Host Configuration Protocol(DHCP[5]). With DHCP, a new computer can obtain an IP([13]) address and perform all the necessary initializations to be hooked up to the Internet just as effectively as existing systems with statically allocated IP addresses.

However, receiving an IP address only allows a computer to be included in the address domain of the IP Internet routing infrastructure; it does not, a priori, enable anyone else to find the computer. DHCP is currently used in a way to allow computers to get addresses which are appropriate for their point of attachment, but that point of attachment traditionally has also identified the computer to the rest of the Internet. That effective identification arises because the IP address is, today, tightly bound to the fully qualified domain name ("DNS name" [8]) for hosts with Internet addresses. When the point of attachment can change frequently, but the effective identity of the computer is expected to remain the same, a conflict arises. And, in response to this need, there has recently been a great deal of work to enable the domain name of a computer to be automatically associated with different IP addresses over time([6]). One of the greatest difficulties in such dynamic DNS-based schemes is the possibility of allowing for impersonations. To avoid such attacks, additional and stringent security requirements have to be imposed on the mobile users by their DNS administration.

An alternative approach has been to enable mobile computers to interact with a routing infrastructure, so that the mobile computers can keep an unchanging "home address" for operating network connections with other computers, but on the other hand register a "foreign address" for use by the routing infrastructure. This approach has the disadvantage of requiring additional network entities to cooperate in providing service for the "home network", but does not require any DHCP service, nor dynamic DNS updates for the mobile computer's DNS name. An additional advantage is that movement by the computer is almost completely transparent to network applications. In contrast, the DHCP/DNS approach requires that applications on other computers interacting with the mobile host perform new name lookups every time it moves.

For the purposes of this paper, let us define that "mobility" is the capability of transacting continuous network traffic as long as there is a physical path available for the data, and by contrast define "portability" as just the ability to initiate network transactions whenever there is a physical data link available. Thus, a computer system which offers "mobility" also offers "portability". Portable computers are expected to be conveniently operated wherever they might be located, but network connections must be reinitialized whenever a movement occurs. Mobile computers, on the other hand, maintain network connections even during movements between different points of attachment (as long as there is actually a physical data link). Even if movement causes a temporary disconnect, as soon as a new data link can be established, a mobile computer will be able to resume all connections with nothing more than the penalty of some dropped packets. Fortunately, perhaps, there are many possible ways of combining available features that offer a wide range of intermediate capabilities between portability and mobility.

The mobile-IP protocol does nothing to alleviate the need for the initial IP address allocation and initialization steps for the mobile computer. The IETF working group has implicitly relied on the expected use of DHCP to solve this problem. The interactions of DHCP and mobile-IP in support of mobile computing (as opposed to merely supporting portable computers) form the subject of this paper. To give proper context to the discussion, we first briefly describe the operation of DHCP and mobile-IP.

We show that DHCP has to be explicitly augmented with a new option for the maintenance and allocation of IP addresses from appropriate home networks, replacing the current practice of allocating IP addresses dependent upon the current point of attachment for the mobile computer. We describe the use of the new DHCP option during the reboot sequence of the mobile client.

We mention the methods envisioned used by a mobile client wishing to use DHCP for obtaining temporary "care-of" addresses, as required for the operation of the mobile-IP protocol.

Afterwards, we detail the sequences of operations at boot time and later, between mobile nodes using DHCP and mobile-IP in various combinations. Lastly, we offer our conclusions and directions for future work.

2 DHCP Overview

DHCP was designed as a mostly compatible upgrade to the 'bootp'[4] protocol. Typical configuration details readily available from a DHCP server include an IP address usable by the client, a default router for that address, and the IP subnet mask associated with computers using the network on which the allocated IP address is presumed to reside. In addition, the client will often request the domain and DNS name associated with the new address. If the client has already been partially configured with such a name, then the client can specify that name as a hint to the DHCP server about what IP addresses might be preferred.

DHCP employs a simple client-server model. The model allows for arbitrary connections between multiple clients, multiple servers, and another entity known as a DHCP relay. Generally, clients wishing to obtain service will make a discovery broadcast. Any server wishing to satisfy the client's request will offer a set of configuration options to the client. The client will accept one of the offers, and the DHCP will then commit the transaction.

The DHCP relay is presumed to be a transparent provider of a data path between a client and a server; thus, a single DHCP server can respond to clients on many different subnets, simplifying equipment requirements and administrative overhead. A normal, non-mobile client gets the configuration data from the DHCP server by first discovering a suitable server. It does this by broadcasting to a local recipient, at a well known DHCP server UDP port number(67). The local recipient either satisfies the request if it is a DHCP server, or transmits it to a DHCP server if it is a relay. The interesting thing is how the DHCP server determines the subnet on which the client resides. The DHCP packet has a field called "giaddr". If the packet has been forwarded by the relay, then the relay sets the "giaddr" field to the address of the interface through which it has received the packet from the client. Thus the information about the client subnet has been preserved in the "giaddr" field. The DHCP server uses this to retrieve an address which belongs to the client subnet from its persistent database.

Although it is possible, and expected, that clients will interact with multiple DHCP servers, for the purposes of this paper we will usually presume that a client is interacting with a single DHCP server, through a DHCP relay. The number of entities attempting to provide service to the client will be of no importance; what is important is the order of operations between server and client.

3 Mobile-IP overview

With the goal of offering true mobile networking, a new draft protocol has been under development within the IETF[7]. This draft protocol, which we have implemented and tested, does indeed allow sessions to move along with the computer from one point of attachment to another. There are also additional features under development to allow packets to mobile computers to be routed along optimal paths, bypassing (if possible) the home agent, which maintains the virtual links between the home network and the current whereabouts of the mobile computers[11].

The mobile IP protocol begins with the premise that applications running on mobile clients should be able to operate without change, if the routing infrastructure can deliver packets to the mobile client regardless of its current location. Given the latter assumption, transparency results from the way that communication between Internet hosts is structured to depend fundamentally on their IP addresses. If the IP address remains the same as a computer moves, an application would never detect the movement.

IP addresses are traditionally associated with the location of the internet host, since that's usually defined by the structure of the address. The IP address is structured as a "network" number followed a "host" number, and Internet routers send packets to a router physically connected to the network associated with the network number of the destination. So, for instance, the IP address allocated by the DHCP server depends, given the current protocol options, on the location of the DHCP relay mediating the DHCP transactions for the client, since the relay's address defines the point of attachment of the client, and thus "defines" the location of the client.

The mobile-IP protocol resolves this problem by proposing a special new router called the "home agent". The home agent is considered to be the entry router for the "home network" containing a collection of mobile hosts. It will often happen that there

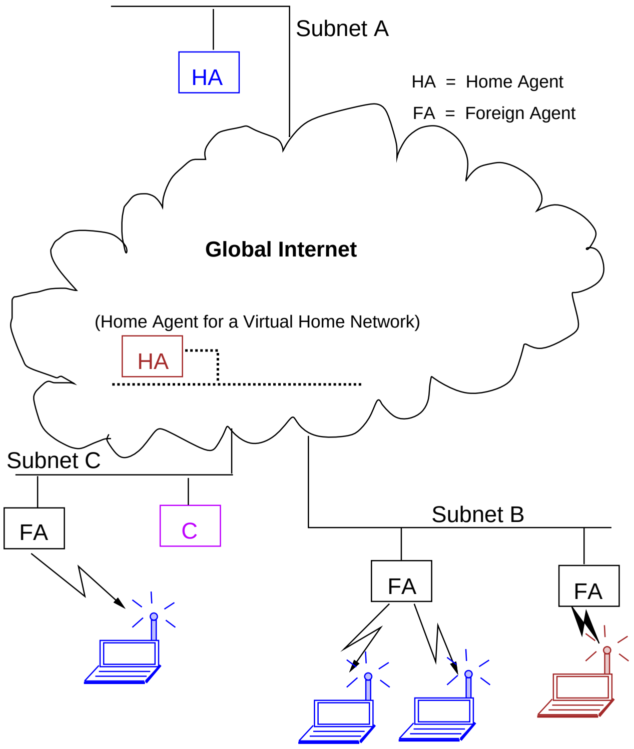

Figure 1: Mobile-IP entities

is no physical "home network", but nevertheless the home agent will attract packets targeted to its mobile hosts and make the appropriate arrangements for their delivery. The home agent is able to do this because whenever one of its mobile hosts changes its physical point of attachment to the Internet, it reports a new "care-of address" to the home agent. The association between a mobile node and its care-of address is known as a "binding", and should be thought of as a relatively long-lived cache entry. The home agent can deliver packets to its mobile host by delivering them to a current care-of address. The agent which receives packets addressed to the care-of address of a mobile host is known as a foreign agent. Once the foreign agent receives a packet meant for a mobile host, the foreign agent takes the necessary steps for completing the delivery of the packet to that mobile host.

Figure 1 is a picture of the basic setup.

The process by which the mobile host and its home agent agree on the current care-of address is known as registration. This registration process, mediated by the foreign agent, is performed whenever the mobile host moves to the area of service of a new foreign agent, or when the lifetime for the use of the current care-of address is in danger of expiring. It is of prime importance for the home agent to be able to trust the registration information sent to it by the mobile host; if a bad registration were accepted, the mobile host would be unable to obtain service from the Internet. For this reason, a mobile host and a home agent share a secret which they use to attach unforgeable signatures to registration data.

Suppose, now, that a registration has been completed, and the mobile node is accepting service from a foreign agent at a care-of address known to the mobile node's home agent. Packets targeted to the mobile node are attracted to the home agent, as configured by the local administration, possibly aided the by the operation of standard routing protocols to exchange route information among the routers in the local infrastructure surrounding the home network. In order for the home agent to deliver a packet to the mobile hosts, it encapsulates the packet and uses the care-of address as the new destination IP address of the packet. When the foreign agent receives the encapsulated packet, it decapsulates and finds the mobile user's IP address within. The decapsulated packet can then be delivered locally to the mobile user.

3.1 Triangle Routing

The basic mobile-IP routing paradigm. is fundamentally asymmetric. The mobile node itself doesn't have to make use of the home agent to send packets to a stationary Internet host, but that same host can only deliver packets to the mobile node with the assistance of the home agent. This asymmetry has been described as "triangle routing", as suggested by the diagram in figure 2. A solution to the triangle routing problem can be provided by the previously mentioned "route optimization" protocol[11].

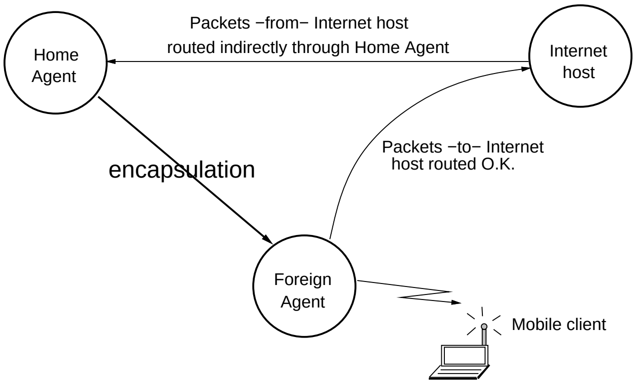
Packets −from− Internet host
routed indirectly through Home Agent
Home Agent
Internet host
encapsulation
Packets −to− Internet host routed O.K.
Foreign Agent
Mobile client

Figure 2: Mobile-IP entities, showing suboptimal path to mobile client

3.2 Authentic routing advice

Suppose, without any authentication, an Internet host accepts a directive regarding the current whereabouts of a mobile user. Then traffic directed towards that user could be hijacked by an agent sending false directives to that Internet host transmitting the packets. Thus it is of high importance to ensure that such routing directives can be authenticated by the recipient before use.

3.3 Smooth Handoffs

In order to avoid dropping any packets as a node migrates from one foreign agent to another, the previous foreign agent must be able to reliably receive information (a routing directive) about the new whereabouts of the mobile host. The foreign agents must authenticate these routing directives also. For this, the mobile host uses a different session-specific key for each foreign agent, and uses that key only for the purpose of validating the routing directive sent when movement occurs[9], [11]. Packets which continue to arrive at the previous foreign agent can then be forwarded to the new foreign agent. The mobile host arranges this with the cooperation of its new foreign agent, and provides smooth transitions from one area to another, when it is physically possible.

4 Mobile-IP and DHCP

Using mobile-IP with DHCP brings several new factors into play. In the first place, a mobile host may dynamically obtain a care-of address using DHCP([12]) instead of listening for service advertisements from a foreign agent. Such a mobile host would then have two addresses – a dynamic care-of address, and a long term home address. It would receive its packets encapsulated and addresses to its care-of address; it would encapsulate each packet and make sure that the result was a standard IP packet addressed to its home addressed, and then resume standard processing. Such a mobile host can be considered to be ”co-located” with its own, built-in foreign agent. This design results in a sort of ”highly-portable” mobile client. Later, in section 7, we consider the dual addressibility of the mobile client.

With this basic approach packets may be dropped during movements between service areas, but the usual method of employing TCP sessions will cause the retransmission of dropped packets. Even with TCP, however, dropped packets can cause users to be uncomfortable with the interactivity of their mobile nodes. The investigation by R. Caceres et al.([3]) shows that dropping packets substantially degrades the apparent performance of TCP connections; common transport protocols other than TCP are likely to be even more severely affected. If the home agent is far away or on the other side of a congested network, then the effects of dropped packets will be more noticeable because of the increased round-trip time measured by TCP. Consequently, we believe employing actual foreign agents on each subnet where mobility is supported will increase user satisfaction and avoid the pitfalls, known and unknown, associated with systemically unreliable data streams.

5 Home Address Option

Typical mobile users will not desire to perform any administrative tasks to configure their nodes before communicating via the Internet. Yet, DHCP as it is currently specified is unsuitable to satisfy the needs of mobile users employing mobile-IP. Current DHCP servers allocate IP addresses based on the identified location of the client, but for mobility we need to allocate a more permanent home address which is not necessarily associated with the client's current location. Moreover, it is reasonable for this home address to be accompanied by the address of a home agent which serves the associated home network. Upon discovery of a suitable home address and home agent, the DHCP client can then begin the subsequent process of registering its current location with the home agent, and then be able to move about with its newly allocated home address while maintaining its network connections.

Our solution is to introduce a new option([10]) so that a mobile client can request from via DHCP simultaneously a (mobile) home address and a new home agent address. The server would then reserve a pool of addresses for the mobile nodes. Since the home agent address depends on the home address in a well-defined way, and it is needed to allow the mobile client to register, the server can also deliver the home agent's address to the mobile node. The new option has been allocated option number 68, and can be interoperably implemented like any other option already in use conforming with the DHCP protocol standard. We also expect that the existence of this new DHCP option will result in an increased need for every foreign agent to implement ”smart” bridge or DHCP relay functionality for the convenience of the mobile users.

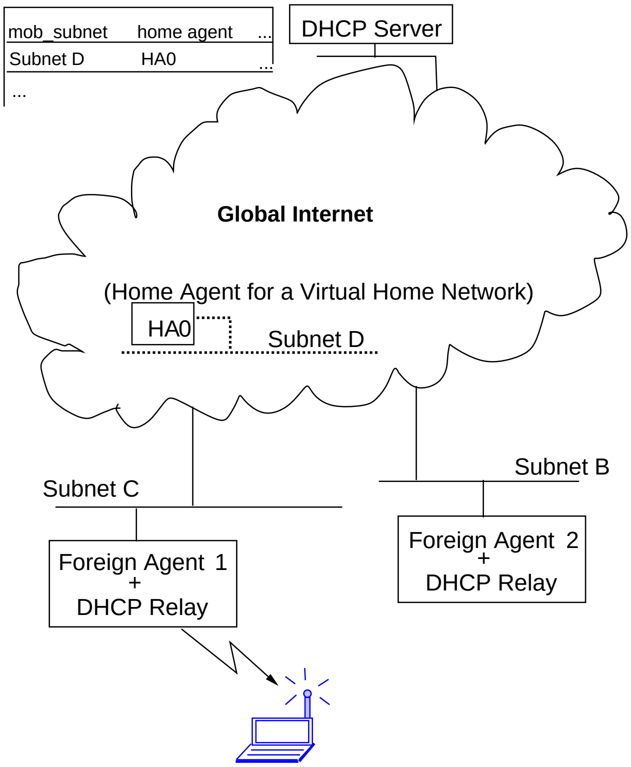

Figure 3: A mobile client getting a mobile home address

Figure 3 illustrates the operation of a mobile computer obtaining a mobile home address through a foreign agent which also acts as a DHCP relay. The mobile client is shown moving from foreign agent 1 to foreign agent 2, and both foreign agents are also able to relay DHCP transactions. The DHCP server is shown with its database containing a mobile subnet, associated with home agent HA0. The mobile node has contacted the DHCP server via the first DHCP relay, foreign agent 1, obtained a mobile home address, and registered foreign agent 1's care-of address with home agent HA0. When the mobile client moves to foreign agent 2, it will not need to contact the DHCP server again. It will have to register foreign agent 2's care-of address with home agent HA0.

Compared to the portable operation described in section 4, whereby the mobile client gets a care-of address from the nearby DHCP server, this method has the advantage that the DHCP allocated home address is useful in the service areas of other foreign agents, until the mobile DHCP client releases the home address. This method will also avert the problem of dropped packets discussed in the portable scenario, if as we expect foreign agents will facilitate smooth changes of network attachment point([9]).

The freedom with which mobile clients can obtain new home addresses may introduce a new phenomenon of stale entries at the associated home agents. Let us consider the following scenario. Suppose a mobile host receives a DHCP home address from a home agent ha1. After a mobile-IP registration, ha1 will have a binding for the mobile host. Suppose the mobile host moves, and a new home agent ha2 receives a registration with its new DHCP home address. The first binding at ha1 has become stale. The mobile node can solve this problem by de-registering with its previous home agent – that is, sending in a registration with a zero lifetime. The effects of this problem will be substantially reduced if the mobile node is able to update the relevant DNS databases each time it obtains a new home address. In that case, any other computer which needs to contact the mobile node will not attempt to make use of any stale home addresses.

5.1 New DHCP Option Implementation

For our implementation, the DHCP relay function is to reside at each foreign agent. To enable a mobile host to get an address on the home network and to let it get a home agent address, a new DHCP option, "Mobile Home Address" has been added to the DHCP code.

The configuration file of the DHCP server has been modified to reserve a pool of addresses for the mobile Home network in its persistent database and to associate with those reserved addresses, the address of a home agent. We have added a new keyword "mob_subnet" in our DHCP server configuration file which distinguishes a set of addresses as mobile subnet addresses. Each mob_subnet can have home agents associated with it; these home agents will be reported to mobile clients invoking the new option.

The following is a summary of the protocol exchanges between DHCP servers and clients wishing to get mobile home addresses.

1. To retrieve the above option or any other option of interest, a DHCP client must request the return of this information when a DHCPDISCOVER or DHCPREQUEST message is sent. The "Mobile Home Address" option is requested by including in a DHCPDISCOVER or DHCPREQUEST message the 'parameter request list' option containing option code (68).
2. When a server which has a pool of mobile home addresses in its repository finds the "Mobile Home Address" option in the 'parameter request list' in the received packet, it selects an address from its mobile addresses repository and returns that address in its DHCPOFFER. The server may also list the Home Agent address in the "Mobile Home Address" option.
3. When the client receives the DHCPOFFER with the new option, it sends out a DHCPREQUEST message again with the "Mobile Home Address" option included in the parameter request list.
4. When a server receives a DHCPREQUEST message, it commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client. The configuration parameters include the "Mobile Home Address" option with the home agent address filled. The "yiaddr" field in the DHCPACK messages is filled in with the selected mobile home network address.
5. The client receives the DHCPACK message with configuration parameters. The client performs a final check on the parameters (e.g., ARP for allocated network address). At this point, the client is configured.

If a client remembers and wishes to reuse a previously allocated mobile home network address, it adds the "Mobile Home Address" option in subsequent DHCPREQUEST renewal packets.

5.2 Format of the Option

```
Code Len    Home Agent Addresses
+----+----+ - -+ - -+ - -+ - -+ - -+
| 68 | n  | a1 | a2 | a3 | a4 | ...
+----+----+ - -+ - -+ - -+ - -+ - -+
```

Code 68

Length This is the length of the option excluding the two octets specifying the Code and the Length, which will usually be either 4 or 0 depending upon whether the home agent address is included.

home agent Zero or more IP addresses of home agents which can serve the mobile home address returned in DHCP's "yiaddr" field.

The client sets the "Home Agent Address" field to zero and the server selects one or more suitable servers depending on the home address chosen and returns this information in the "Home Agent Address". If the server wishes to return a home address without returning the home agent address, the length of the option is adjusted accordingly. Multiple home agents can be delivered to the mobile client for purposes of load balancing or fault tolerance.

6 Mobile client startup

As indicated previously, DHCP can be used to provide IP addresses for mobile clients which can be used in two different ways. IP addresses may be allocated to a mobile client via conventional mechanisms, for use by the client as the care-of address in its next mobile registration. The mobile client, however, may not even have any IP address at all; it then would request an IP address on a home network (a network with a home agent) for use as it moves from place to place. The allocation and use of these two addresses are logically distinct, and in operation there is little interaction between the procedures used by the mobile client to obtain them.

As indicated previously, additional system administration by the new users who will populate the mobile computing marketplace must be avoided. With that requirement in mind, we have designed our mobile computer client software so that the best operating mode available is selected from those outlined above. Any specific mode of operation can be selected by preconfiguration, but if no configuration has been selected we perform the following steps:

- When a mobile client reboots, it first must determine whether it has a home address. On Unix systems, the "hostname" command, or gethostname() system call, returns this information. If a DHCP home address is needed, the mobile node tries to contact a nearby server or relay to get it (section 5.1).
- The mobile client attempts to get a DHCP care-of address.
- Simultaneously the mobile node listens for advertisements
- If a DHCP care-of address is received, register with it
- Whenever an advertisement is received, then the mobile node registers with the care-of address
- If no advertisement is received and no configuration restrictions are in place, the mobile node solicits; if an advertisement is elicited, register...
- When the default router is no longer reachable, or when a lower-layer indication of a physical disconnection is obtained, start the process again

In this way, the mobile node will get the benefit of any foreign agent's services in the area if available, and otherwise will serve as its own foreign agent with the assistance of DHCP. Furthermore, if a mobile node gets a temporary care-of address via DHCP, and seconds later detects a agent advertisement from a foreign agent in the area, the mobile node will reregister using the newly available care-of address from the foreign agent. In this case, it is advisable for the mobile node to also release the temporary address it had obtained via DHCP for re-use by other clients. Starting the mobile-IP and DHCP operations occur in parallel minimizes the time a mobile client has to wait on reboot.

7 Multi-Homing

As a general statement, computers running mobile-IP offer mobility transparent to applications, and computers that get a location-dependent address from a DHCP server must be satisfied with portability. When mobile-IP nodes use DHCP for obtaining a care-of address, the finer modes of operation which are possible tend to impart some characteristics of portability into the general framework of mobility.

Note that a mobile client which has a DHCP care-of address must handle packets with two different IP addresses. The minimum requirement is that the mobile client receive packets delivered to its care-of address, and that it issue packets from its home address. If the mobile client issues packets from its care-of address, all the benefits of mobile-IP are already lost. If the mobile client is capable of true multi-homed operation, it still must issue all traffic from its home address instead of its care-of address.

The simplest operation provides that, if the mobile-IP node moves from one point of attachment to another and gets a new DHCP care-of address each time, it may essentially discard the previously used care-of address when its new registration has been completed. However, for smoothest operation, a mobile host getting its care-of addresses from DHCP should continue to accept packets addressed to its previous DHCP care-of address for while each time it moves and gets a new one.

A similar but more complicated phenomenon can occur when a mobile-IP node gets its home address from DHCP. If the node fails to renew its allocation of the home address, or if the node moves away from the service area of the DHCP server which granted it a DHCP home address, then that mobile node will have to take additional steps to receive packets from its previous home agent. At a minimum, the mobile node would have to accept packets from the previous address (assuming it is still valid, and perhaps even for a short while afterwards). This will probably imply that the mobile node would have to send a gratuitous registration request to its previous home agent so that the packets still coming to that home agent have a chance of arriving at the current whereabouts of the mobile node.

In the worst, and hopefully unlikely, case, a mobile node which is decapsulating its own packets at a DHCP-allocated care of address may want to receive packets addressed to four IP addresses; two different home addresses (one current, one previous), and two different care-of addresses. This unfortunate scenario would result from movement simultaneously across DHCP server boundaries which nevertheless have physically overlapping areas of service, for a mobile user obtaining both DHCP-allocated home addresses and care-of addresses. It remains to be seen whether mobile hosts in such situation, that do not field packets sent to multiple addresses, experience unacceptable breaks in service due to the dropped packets. Unfortunately for the network layer architect, the severity of the effects depends on the application.

8 Conclusions

We have investigated thoroughly the interactions of DHCP and mobile-IP as they may be applied to provide portability and mobility for users of new wireless systems. We have discovered that there are many combinations of features available using DHCP for certain required addresses with mobile-IP. Depending upon the capabilities built in to the mobile host, users can expect varying amounts of degradation from the pure mobile-IP model, when using DHCP.

The main candidates seem to be:

1. Rely on DHCP for a home address, and use it for as long as needed, using the mobile-IP protocol with foreign agents and smooth handoffs to provide satisfactory user convenience during the lifetime of the home address. Renew the lease on the home address when needed.

2. Rely on DHCP to allocate care-of addresses for use with mobile-IP registrations, and handle the effects of lost packets during transitions between subnets. Those who need transparent mobility will prefer movable computers which can accept packets addressed to multiple care-of addresses, to take care of overlaps, since there won't be any physical foreign agents to help out. However, the very fact that such systems can operate without the need for additional foreign agent entities on each subnet will make this an attractive choice for many.

3. Rely on DHCP for both home addresses and care-of addresses. The considerations of the previous two cases are both relevant here.

4. Rely on DHCP for an IP address valid only on the subnet on which the movable computer is located. This is the least expensive option, and has the least functionality. Network connections will need to be re-started whenever a new DHCP address is obtained.

The additional ease of configuration which can be provided by the use of DHCP will make the above choices much more attractive, even given the sometimes irritating loss of smoothness and increased need for packet retransmission. As outlined in the previous section, new implementations of multi-homed IP hosts may be indicated by the use of DHCP for addresses in overlapping areas of wireless service, to counteract the replacement of physical foreign agents by dynamic addressing functions in the mobile hosts themselves. Since there are real economic factors favoring the latter tradeoff, we expect to continue to investigate in much more detail the considerations of multi-homed movable computers.

Acknowledgements

Thanks to Mohamed Gouda for encouraging me to write this paper. Thanks also to Ralph Droms, of the Internet Engineering Task Force working group on DHCP, for reviewing an early draft.

References

[1] Serial Infrared Link Access Protocol (IrLAP), Version 1.0. Infrared Data Association, 1994.

[2] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Document P802.11/D1, Dec 1994.

[3] Ramon Caceres and Liviu Iftode. The Effects of Mobility on Reliable Transport Protocols. In *Proceedings of the 14th International Conference on Distributed Computing Systems*, June 1994.

[4] B. Croft and J. Gilmore. Bootstrap Protocol (BOOTP). RFC 951, September 1985.

[5] R. Droms. Dynamic Host Configuration Protocol. RFC 1541, October 1993.

[6] Donald E. Eastlake and Charles W. Kaufman. Domain Name System Protocol Security Extensions. Internet Draft – work in progress, January 1995.

[7] IETF Mobile-IP Working Group. ietf-draft-mobileip-protocol-08.txt. Internet Draft – work in progress, January 1995.

[8] P. Mockapetris. Domain Names - Concepts and Facilities. RFC 1034, November 1987.

[9] Charles Perkins, Andrew Myles, and David Johnson. The Internet Mobile Host Protocol (IMHP). In *Proceedings of INET'94/JENC5*, page 642, June 1994.

[10] Charles E. Perkins. DHCP Home Address option . draft-perkins-homeaddr-dhcpopt-00.txt – work in progress, March 1995.

[11] Charles E. Perkins and David B. Johnson. Route Optimization in Mobile-IP . Internet Draft – work in progress, January 1995.

[12] Charles E. Perkins and Kevin Luo. Using DHCP with Computers that Move. *Proceedings of the Ninth Annual IEEE Workshop on Computer Communications*, pages 56–59, October 1994.

[13] J. Postel. Internet Protocol. RFC 791, September 1981.