Dynamic Host Configuration Working Group
INTERNET DRAFT

Rich Woundy
Kim Kinnear
Cisco Systems

July 2001
Expires January 2002

DHCP Lease Query
<draft-ietf-dhc-leasequery-02.txt>

Status of this Memo

Copyright Notice

Abstract

Access concentrators that act as DHCP relay agents need to determine the endpoint locations of IP addresses across public broadband access networks such as cable, DSL, and wireless networks. Because ARP broadcasts are undesirable in public networks, many access concentrator implementations "glean" location information from DHCP messages forwarded by its relay agent function. Unfortunately, the typical access concentrator loses its gleaned information when the access concentrator is rebooted or is replaced. This memo proposes that when gleaned DHCP information is not available, the access concentrator/relay agent obtains the location information directly

from the DHCP server(s) using a new, lightweight DHCPLEASEQUERY message.

1. Introduction

In many broadband access networks, the access concentrator needs to associate an IP address lease to the correct endpoint location, which includes knowledge of the host hardware address, the port or virtual circuit that leads to the host, and/or the hardware address of the intervening subscriber modem. This is particularly important when one or more IP subnets are shared among many ports, circuits, and modems. Representative cable and DSL environments are depicted in Figures 1 and 2 below.

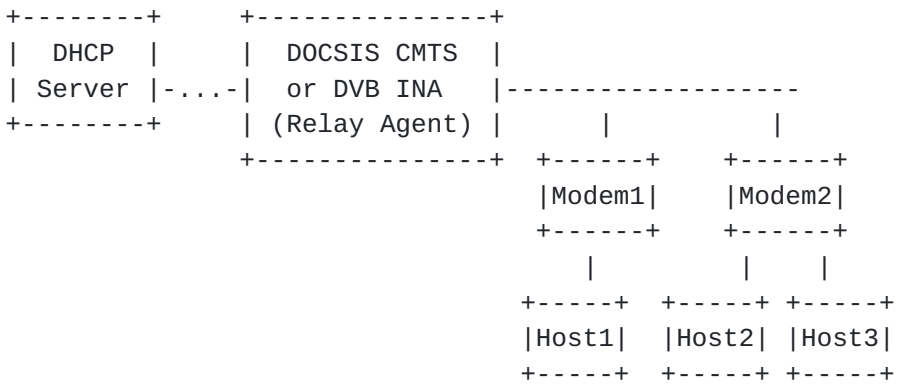


Figure 1: Cable Environment for DHCPLEASEQUERY

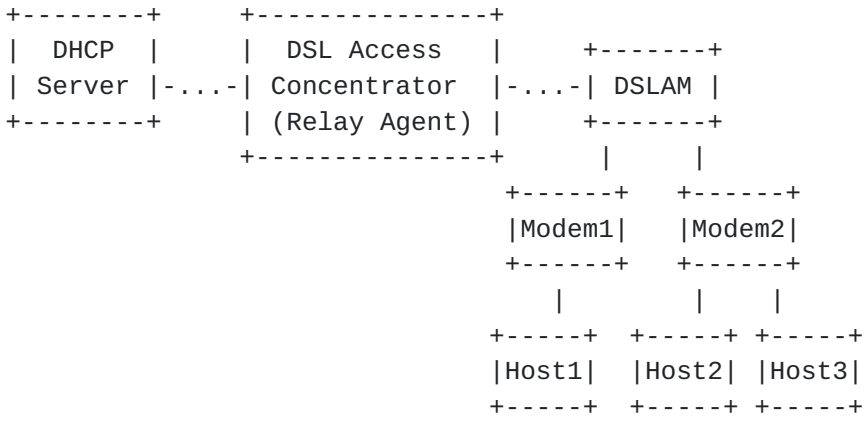


Figure 2: DSL Environment for DHCPLEASEQUERY

Knowledge of this location information benefits the access concentrator in several ways:

1. The access concentrator can forward traffic to the access network using the correct access network port, down the correct virtual circuit, through the correct modem, to the correct hardware address.

2. The access concentrator can perform IP source address verification of datagrams received from the access network. The verification may be based on the datagram source hardware address, the incoming access network port, the incoming virtual circuit, and/or the transmitting modem.

3. The access concentrator can encrypt datagrams which can only be decrypted by the correct modem, using mechanisms such as [BPI] or [BPI+].

The premise of this document is that the access concentrator obtains this location information primarily from "gleaning" information from DHCP server responses sent through the relay agent. When location information is not available from "gleaning", e.g. due to reboot, the access concentrator can query the DHCP server(s) for location information using the DHCPLEASEQUERY message. The DHCPLEASEQUERY mechanism is the focus of this document.

The DHCPLEASEQUERY message is a new DHCP message type transmitted from a DHCP relay agent to a DHCP server. The DHCPLEASEQUERY-aware relay agent sends the DHCPLEASEQUERY message when it needs to know the location of an IP endpoint. The DHCPLEASEQUERY-aware DHCP server replies with a DHCPKNOWN or DHCPUNKNOWN message. The DHCPKNOWN response to a DHCPLEASEQUERY message allows the relay agent to determine the IP endpoint location, and the remaining duration of the IP address lease.

2. 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 [RFC 2119].

This document uses the following terms:

- "access concentrator"

  An access concentrator is a router or switch at the broadband access provider's edge of a public broadband access network.

This document assumes that the access concentrator includes the DHCP relay agent functionality.

- "DHCP client"

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

- "DHCP relay agent"

  A DHCP relay agent is a third-party agent that transfers BOOTP and DHCP messages between clients and servers residing on different subnets, per [RFC 951] and [RFC 1542].

- "DHCP server"

  A DHCP server is an Internet host that returns configuration parameters to DHCP clients.

- "downstream"

  Downstream is the direction from the access concentrator towards the broadband subscriber.

- "gleaning"

  Gleaning is the extraction of location information from DHCP messages, as the messages are forwarded by the DHCP relay agent function.

- "location information"

  Location information is information needed by the access concentrator to forward traffic to a broadband-accessible host. This information includes knowledge of the host hardware address, the port or virtual circuit that leads to the host, and/or the hardware address of the intervening subscriber modem.

- "MAC address"

  In the context of a DHCP packet, a MAC address consists of the fields: hardware type "htype", hardware length "hlen", and client hardware address "chaddr".

- "primary DHCP server"

  The primary DHCP server in a DHCP Failover environment is configured to provide primary service to a set of DHCP clients for

a particular set of subnet address pools.

- "secondary DHCP server"

  The secondary DHCP server in a DHCP Failover environment is configured to act as backup to a primary server for a particular set of subnet address pools.

- "stable storage"

  Every DHCP server is assumed to have some form of what is called "stable storage". Stable storage is used to hold information concerning IP address bindings (among other things) so that this information is not lost in the event of a server failure which requires restart of the server.

- "upstream"

  Upstream is the direction from the broadband subscriber towards the access concentrator.

3. Background

The focus of this document is to enable access concentrators to send DHCPLEASEQUERY messages to DHCP servers, to obtain location information of broadband access network devices.

This document assumes that many access concentrators have an embedded DHCP relay agent functionality. Typical access concentrators include DOCSIS Cable Modem Termination Systems (CMTSs) [DOCSIS], DVB Interactive Network Adapters (INAs) [EUROMODEM], and DSL Access Concentrators.

The DHCPLEASEQUERY message is an optional extension to the DHCP protocol [RFC 2131]. Unlike previous DHCP message types, the DHCP relay agent originates and sends the DHCPLEASEQUERY message to the DHCP server, and processes the reply from the DHCP server (a DHCPKNOWN or DHCPUNKNOWN).

In a DHCP Failover environment [FAILOVER], the DHCPLEASEQUERY message can be sent to the primary or secondary DHCP server. In order for the secondary DHCP server to answer DHCPLEASEQUERY messages, the primary DHCP server must send "interesting options" (such as the relay-agent-information option) in Failover BNDUPD messages to the secondary DHCP server, as recommended by section 7.1.1 of [FAILOVER].

The DHCPLEASEQUERY message is a query message only, and does not

affect the state of the IP address or the binding information associated with it.

4. Design Goals

The core requirement of this document is to provide a lightweight mechanism for access concentrator implementations to obtain location information for broadband access network devices. The specifics of the broadband environment that drove the approach of this document follow.

4.1. Broadcast ARP is Undesirable

The access concentrator can transmit a broadcast ARP Request [RFC 826], and observe the origin and contents of the ARP Reply, to reconstruct the location information.

The ARP mechanism is undesirable for three reasons:

1. the burden on the access concentrator to transmit over multiple access ports and virtual circuits (assuming that IP subnets span multiple ports or virtual circuits),

2. the burden on the numerous subscriber hosts to receive and process the broadcast, and

3. the ease by which a malicious host can misrepresent itself as the IP endpoint.

4.2. SNMP and LDAP Client Functionality is Lacking

Access concentrator implementations typically do not have SNMP management client interfaces nor LDAP client interfaces (although they typically do include SNMP management agents). This is a primary reason why this document does not leverage the proposed DHCP Server MIB [DHCPMIB] nor leverage the proposed DHCP LDAP schema [DHCPSCHEMA].

4.3. DHCP Relay Agent Functionality is Common

Access concentrators commonly act as DHCP relay agents. Furthermore, many access concentrators already glean location information from DHCP server responses, as part of the relay agent function.

The gleaning mechanism as a technique to determine the IP addresses

valid for a particular downstream link is preferred over other mechanisms (ARP, SNMP, LDAP) because of the lack of additional network traffic, but sometimes gleaning information can be incomplete. The access concentrator usually cannot glean information from any DHCP unicast (i.e. non-relayed) messages due to performance reasons. Furthermore, the DHCP-gleaned location information often does not persist across access concentrator reboots (due to lack of stable storage), and almost never persists across concentrator replacements.

4.4. DHCP Servers Are Most Reliable Source of Location Information

DHCP servers are the most reliable source of location information for access concentrators, particularly when the location information is dynamic and not reproducible by algorithmic means (e.g. when a single IP subnet extends behind many broadband modems). DHCP servers participate in all IP lease transactions (and therefore in all location information updates) with DHCP clients, whereas access concentrators sometimes miss some important lease transactions.

In a DHCP Failover environment [FAILOVER], the access concentrator can query either the primary or secondary DHCP server, so that no one DHCP server is a single point of failure.

4.5. Minimal Additional Configuration is Required

Access concentrators can usually query the same set of DHCP servers used for forwarding by the relay agent, thus minimizing configuration requirements.

5. Protocol Overview

The access concentrator initiates all DHCPLEASEQUERY message conversations. This document assumes that the access concentrator gleans location information in its DHCP relay agent function. However, the location information is usually unavailable after the reboot or replacement of the access concentrator.

Suppose the access concentrator is a router, and further suppose that the router receives an IP datagram to forward downstream to the public broadband access network. If the location information for the downstream next hop is missing, the access concentrator sends one or more DHCPLEASEQUERY message(s), each containing the IP address of the downstream next hop in the "ciaddr" field.

An alternative approach is to send in a DHCPLEASEQUERY message with

the "ciaddr" field empty and the MAC address (i.e., "htype", "hlen", and "chaddr" fields) with a valid MAC address and/or a client-id option (option 61) appearing in the options area. In this case, the DHCP server SHOULD return an IP address in the "ciaddr". It MUST be the IP address most recently used by the client described by the MAC address or client-id option (or both, if both appear).

The DHCP servers that implement this protocol always sends a response to the DHCPLEASEQUERY message: either a DHCPKNOWN or DHCPUNKNOWN. The DHCP server replies to the DHCPLEASEQUERY message with a DHCPKNOWN message if the "ciaddr" corresponds to an IP address about which the server has definitive information (i.e., it is authorized to lease this IP address). The server replies with a DHCPUNKNOWN message if the server does not have definitive location information concerning the lease implied by the "ciaddr". Note that non-DHCPLEASEQUERY-literate DHCP servers SHOULD (and are expected to) drop the DHCPLEASEQUERY message silently. The DHCPLEASEQUERY message can support three different query regimes:

- o Query by IP address:

  For this query, the client passes in an IP address and the DHCP server the IP address and returns any information that it has on the most recent client to utilized that IP address. Any server which supports the DHCPLEASEQUERY message MUST support query by IP address. If an IP address appears in the "ciaddr" field, then the query MUST be by IP address regardless of the contents of the MAC address or client-id option (if any).

- o Query by MAC address:

  For this query, the MAC address is specified in the "htype", "hlen", and "chaddr" fields and no IP address is given in the "ciaddr" field. The DHCP server looks up all IP addresses for which clients with this MAC address are the most recent accessor. It returns information associated with the IP address most recently accessed by a DHCP client with this MAC address. If requested, the DHCP server SHOULD return information on all of the IP addresses it found to be associated with the DHCP client with the MAC address in multiple Requested IP address options (option 50) [RFC 2132]. A server which implements the DHCPLEASEQUERY message SHOULD implement this capability.

- o Query by client-id option:

  This query is similar to the query by MAC address, except that a client-id option is present in the DHCPLEASEQUERY packet. In this case, information on the IP address most recently accessed

by a client with the included client-id will be returned in the DHCPACK. If no MAC address is given in the DHCPLEASEQUERY request, then all IP addresses which have been accessed by any client with the included client-id SHOULD be returned in multiple Requested IP address options (option 50) [RFC 2132]. If a MAC address is present in the DHCP packet, then the client-id and the MAC address both must match the client information for an IP address for information about that IP address to be returned either in the "ciaddr" or in one of the Requested IP address options.

Generally, the query by IP address is likely to be the most efficient and widely implemented form of leasequery, and it SHOULD be used if at all possible. Use of the other two query formats SHOULD be minimized, as they can potentially place a large load on some servers.

The DHCPKNOWN message reply MUST always contain the IP address in the ciaddr field and SHOULD contains the physical address of the IP address lease owner in the "htype", "hlen", and "chaddr" fields. The dhcp-parameter-request option can be used to request specific options to be returned about the IP address in the ciaddr. The reply often contains the time until expiration of the lease, and the original contents of the Relay Agent Information option [RFC 3046]. The access concentrator uses the "chaddr" and Relay Agent Information option to construct location information, which can be cached on the access concentrator until lease expiration.

Any DHCP server which supports the DHCPLEASEQUERY message SHOULD save the information from the most recent Relay Agent Information option [RFC 3046] associated with every IP address which it serves. A server which implements DHCPLEASEQUERY SHOULD also save the information on the most recent vendor-class-identifier, option 60, associated with each IP address.

6. Protocol Details

6.1. Definitions required for DHCPLEASEQUERY processing

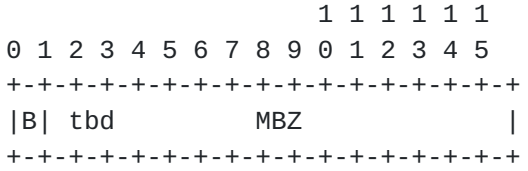
The operation of the DHCPLEASEQUERY message requires the definition of the following new values for the DHCP packet beyond those defined by [RFC 2131].

1. The message type option (option 53) from [RFC 2132] requires three new values: The DHCPLEASEQUERY message itself and its two responses DHCPKNOWN and DHCPUNKNOWN. The values of these message types are shown below in a reproduction of the table

from [RFC 2132]:

Value	Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM
TBD	DHCPLEASEQUERY
TBD	DHCPKNOWN
TBD	DHCPUNKNOWN

2. There is a new bit defined in the flags field of the DHCP packet (see Section 1, Figure 1 and Table 1 of [RFC 2131]). It is called the R: RESERVATION flag. The revised Figure 2 from [RFC 2131] is show here:



B: BROADCAST flag
R: RESERVATION FLAG

MBZ: MUST BE ZERO (reserved for future use)

Revised Figure 2 from RFC2131:
Format of the 'flags' field

3. There is one new option defined which can be used to return important information in a DHCPKNOWN response to a DHCPLEASE-QUERY message -- the client-last-transaction-time. See Section 6.8 for details.

The client-last-transaction-time is necessary in order to allow

an entity that receives multiple DHCPKNOWN messages from different DHCP servers to compare the results and extract the most recently used IP address from among the multiple replies.

6.2. Sending the DHCPLEASEQUERY Message

The DHCPLEASEQUERY message is typically sent by an access concentrator. The DHCPLEASEQUERY message uses the DHCP message format as described in [RFC 2131], and uses message number TBD in the DHCP Message Type option (option 53). The DHCPLEASEQUERY message has the following pertinent message contents:

- The giaddr MUST be set to the IP address of the requestor (i.e. the access concentrator). The giaddr is independent of the ciaddr to be searched -- it is simply the return address of for the DHCPKNOWN or DHCPUNKNOWN message from the DHCP server.

- The Parameter Request List SHOULD be set to the options of interest to the requestor. The interesting options are likely to include the IP Address Lease Time option (option 51) and the Relay Agent Information option (82).

- The Reservation bit in the "flags" field of the DHCP packet (see [RFC 2131] and Section 6.1 of this document) is used to specify if the response should include information encoded into reservations.

Additional details concerning different query types are:

- Query by IP address:

  The values of htype, hlen, and chaddr MUST be set to 0.

  The ciaddr MUST be set to the IP address of the lease to be queried.

  The client-id option (option 61) MUST NOT appear in the packet.

- Query by MAC address:

  The values of htype, hlen, and chaddr MUST be set to the value of the MAC address to search for.

  The ciaddr MUST be set to zero.

  The client-id option (option 61) MUST NOT appear in the packet.

- Query by client-id option:

There MUST be a client-id option (option 61) in the DHCPLEASE-QUERY message.

The ciaddr MUST be set to zero.

The values of htype, hlen, and chaddr MAY be set to the value of the MAC address to search for. In this case, the search MUST match both the values in the client-id option and the MAC address specified in the "htype", "hlen", or "chaddr".

The access concentrator SHOULD ensure that the ciaddr mentioned in the DHCPLEASEQUERY message (if a query by IP address) is a local sub-net of the interface specified for the client.

The DHCPLEASEQUERY message SHOULD be sent to a DHCP server which is known to possess authoritative information concerning the IP address. The DHCPLEASEQUERY message MAY be sent to more than one DHCP server, and in the absence of information concerning which DHCP server might possess authoritative information concerning the IP address, it SHOULD be sent to all DHCP servers configured for the associated relay agent (if any are known).

6.3. Receiving the DHCPLEASEQUERY Message

A DHCPLEASEQUERY message MUST have a non-zero giaddr. The DHCPLEASE-QUERY message MUST have at least one of: a non-zero ciaddr, a non-zero "htype"/"hlen"/"chaddr", or a client-id. It MAY have more than one.

The DHCP server which receives a DHCPLEASEQUERY message MUST base its response (if any) on the IP address represented by the ciaddr in the DHCPLEASEQUERY message if one is given.

If an IP address is not given, then the receiving DHCP server MUST base its response on the client-id and any MAC address contained in the "htype", "hlen", and "chaddr" fields of the DHCP packet.

The giaddr is used only for the destination address of any generated response and, while required, is not otherwise used in generating the response to the DHCPLEASEQUERY message.

6.4. Responding to the DHCPLEASEQUERY Message

The DHCP server MUST respond to a DHCPLEASEQUERY message with a DHCPKNOWN message if the ciaddr corresponds to an IP address which is managed by the DHCP server or if there is an IP address which has most recently been acccess by any DHCP client described by any client-id option and/or MAC address information in the "htype",

"hlen", and "chaddr" fields of the DHCPLEASEQUERY request.

In the event that an IP address appears in the "ciaddr" field, then the information returned should be about that IP address regardless of the values of the MAC address and/or client-id option.

If the Reservation bit is not set in the "flags" field of the DHCP packet (see [RFC 2131]), then the DHCP server SHOULD NOT respond to a DHCPLEASEQUERY message with a DHCPKNOWN if the "ciaddr" corresponds to an IP address about which the DHCP server has definitive information but which has no DHCP client information associated with it. As well, if the "ciaddr" does not contain an IP address and there is a MAC address or client-id in the DHCPLEASEQUERY request, if the Reservation bit is not set then the DHCP server SHOULD NOT respond with a DHCPKNOWN unless the client specified in the DHCPLEASEQUERY has accessed an IP address.

Conversely, if the Reservation bit is set in the "flags" field of the DHCP packet, then the DHCP server SHOULD respond with information contained in the reservation associated with either the IP address specified in the "ciaddr" or the client specified in the MAC adddress and/or client-id if there is no actual usage information concerning the association of the IP address or specified client.

If the DHCP server uses reservation information to fill in the information of a DHCPKNOWN message (other than using it to include an IP address in a Requested IP option), the DHCP server MUST set the Reservation bit in the "flags" field of the DHCPKNOWN message.

Thus, a DHCP server SHOULD, but doesn't have to implement reservation support if it implements support for the DHCPLEASEQUERY message, but if it does, it MUST set the Reservation bit in the "flags" field whenever the primary information it returns in the DHCPKNOWN message is based on a reservation.

The DHCP server MUST respond to the DHCPLEASEQUERY with a DHCPUNKNOWN if the DHCP server supports the DHCPLEASEQUERY message but does not have definitive information concerning the IP address in the ciaddr (if any) or if it does not have definitive information concerning the DHCP client specified in the "htype", "hlen", and "chaddr" fields or the client-id option. When responding with a DHCPUNKNOWN, the DHCP server SHOULD NOT include other DHCP options in the response.

A DHCP server which does not support the DHCPLEASEQUERY message MUST NOT respond to the DHCPLEASEQUERY message.

When responding to a DHCPLEASEQUERY message with a DHCPKNOWN:

- In the case where more than one IP has been accessed by the client specified by the MAC address and/or client-id option, then the IP address most recently the involved in a DHCP client message by that client SHOULD be used as the IP address to place into the "ciaddr". The DHCP server SHOULD be configurable to return other than the IP address with the most recent client-last-transaction-time, for instance the IP address with the longest lease time.

  In this case, all of the IP addresses which are recorded as having been accessed by this client should be returned in Requested IP address options (option 50) if that option is included in the dhcp-parameter-request-list option in the request. They should appear in order of increasing age of access in that option.

- If the IP Address Lease Time option (option 51) is specified in the Parameter Request List and if there is a currently valid lease for the IP address specified in the ciaddr, then the DHCP server MUST return this option in the DHCPKNOWN with its value equal to the time remaining until lease expiration. If there is no valid lease for the IP address, then the server MUST NOT return the IP Address Lease Time option (option 51). This allows the requestor (i.e. the access concentrator) to determine if there is currently a valid lease for the IP address as well as the time until the lease expiration.

  A request for the Renewal (T1) Time Value option or the Rebinding (T2) Time Value option in the Parameter Request List of the DHCPLEASEQUERY message MUST be handled like the IP Address Lease Time option is handled. If there is a valid lease, then the DHCP server SHOULD return these options (when requested) with the remaining time until renewal or rebinding, respectively. If there is not currently a valid lease for this IP address, the DHCP server MUST NOT return these options.

- If the DHCP server has information about the most recent device associated with the IP address specified in the ciaddr, then the DHCP server MUST encode the physical address of that device in the htype, hlen, and chaddr fields. Otherwise, the values of htype, hlen, and chaddr MUST be set to 0 in the DHCPKNOWN. If the IP Address Lease Time (option 51) is returned in the DHCPKNOWN (indicating a currently valid lease by some device for this IP address), the DHCP server MUST encode the physical address of the device which owns the lease in the htype, hlen, and chaddr fields.

- If the Relay Agent Information (option 82) is specified in the Parameter Request List and if the DHCP server has saved the

information contained in the most recent Relay Agent Information option, the DHCP server MUST include that information in a Relay Agent Information option in the DHCPKNOWN.

In environments with non-DHCP-enabled devices, when the DHCP server knows the network access information (perhaps through server configuration), the DHCP server MAY generate its own Relay Agent Information option value in the DHCPKNOWN; in such cases, the DHCP server MUST generate an option value that the access concentrator can process.

- The DHCPKNOWN message SHOULD include the values of all other options not specifically discussed above that were requested in the Parameter Request List of the DHCPLEASEQUERY message.

The DHCP server uses information from the lease binding database to supply the DHCPKNOWN option values.

In order to accommodate DHCPLEASEQUERY messages sent to a DHCP Failover secondary server [FAILOVER] when the primary server is down, the primary server MUST communicate the Relay Agent Information option (82) values to the secondary server via the DHCP Failover BNDUPD messages.

The server expects a giaddr in the DHCPLEASEQUERY message, and unicasts the DHCPKNOWN or DHCPUNKNOWN to the giaddr. If the giaddr field is zero, then the DHCP server does not reply to the DHCPLEASEQUERY message.

6.5. **Receiving a DHCPKNOWN or DHCPUNKNOWN response to the DHCPLEASEQUERY Message**

When a DHCPKNOWN message is received in response to the DHCPLEASEQUERY message and the DHCPKNOWN has an IP Address Lease Time option value that is non-zero, it means that there is a currently active lease for this IP address in this DHCP server. The access concentrator SHOULD use the information in the htype, hlen, and chaddr fields of the DHCPKNOWN as well as any Relay Agent Information option information included in the packet to refresh its location information for this IP address.

When a DHCPKNOWN message is received in response to the DHCPLEASEQUERY message and the DHCPKNOWN has no IP Address Lease Time option (though one was requested in the Parameter Request List), that means that there is no currently active lease for the IP address present in the DHCP server. In this case, the access concentrator SHOULD cache this information in order to prevent unacceptable loads on the access concentrator and the DHCP server in the face of a malicious or

seriously compromised device downstream of the access concentrator.

In either case, when a DHCPKNOWN message is received in response to a DHCPLEASEQUERY message, it means that the DHCP server which responded is a DHCP server which manages the IP address present in the ciaddr, and the Relay Agent SHOULD cache this information for later use.

When a DHCPUNKNOWN message is received by an access concentrator which has sent out a DHCPLEASEQUERY message, it means that the DHCP server contacted supports the DHCPLEASEQUERY message but that the DHCP server not have definitive information concerning the IP address contained in the ciaddr of the DHCPLEASEQUERY message. If there is no IP address in the ciaddr of the DHCPLEASEQUERY message, then a DHCPUNKNOWN message means that the DHCP server does not have definitive information concering the any DHCP client specified in the "hlen", "htype", and "chaddr" fields or the client-id option of the DHCPLEASEQUERY message.

The access concentrator SHOULD cache this information, and only infrequently direct a DHCPLEASEQUERY message to a DHCP server that responded to a DHCPLEASEQUERY message for a particular ciaddr with a DHCPUNKNOWN.

6.6. Receiving the no response to the DHCPLEASEQUERY Message

When an access concentrator receives no response to a DHCPLEASEQUERY message, there are several possible reasons:

- The DHCPLEASEQUERY or a corresponding DHCPKNOWN or DHCPUNKNOWN were lost during transmission or the DHCPLEASEQUERY arrived at the DHCP server but it was dropped because the server was too busy.

- The DHCP server doesn't support DHCPLEASEQUERY.

In the first of the cases above, a retransmission of the DHCPLEASEQUERY would be appropriate, but in the second of the two cases, a retransmission would not be appropriate. There is no way to tell these two cases apart (other than, perhaps, because of a DHCP server's response to other DHCPLEASEQUERY messages indicating that it supports the DHCPLEASEQUERY message).

An access concentrator which utilizes the DHCPLEASEQUERY message SHOULD attempt to resend DHCPLEASEQUERY messages to servers which do not respond to them using a backoff algorithm for the retry time that approximates an exponential backoff. The access concentrator SHOULD adjust the backoff approach such that DHCPLEASEQUERY messages do not arrive at a server which is not otherwise known to support the

DHCPLEASEQUERY message at a rate of not more than approximately one packet every 10 seconds, and yet (if the access concentrator needs to send DHCPLEASEQUERY messages) not less than one DHCPLEASEQUERY per minute.

6.7. Utilizing the DHCPLEASEQUERY message in a failover environment

When utilizing the DHCPLEASEQUERY message in an environment where multiple DHCP server may contain authoritative information about the same IP address (such as when failover [FAILOVER] is operating), there could be some difficulty in deciding which results are the most useful if two servers respond with DHCPKNOWN messages to the same query.

In this case, the client-last-transaction-time can be used to decide which server has more recent information concerning the IP address returned in the "ciaddr" field.

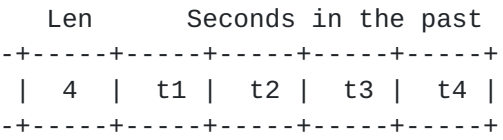
6.8. New option defined for responding to DHCPLEASEQUERY messages.

There is one new option defined for responding to DHCPLEASEQUERY messages: client-last-transaction time.

6.8.1. client-last-transaction-time

This option SHOULD record the time of the most recent access of the client. It is particularly useful when DHCPLEASEQUERY responses from two different DHCP servers need to be compared, although it can be useful in other situations. The value is a duration in seconds in the past from when this IP address was most recently the subject of communication between the client and the DHCP server.

The code for the this option is TBD. The length of the this option is 4 octets.



7. Security Considerations

Access concentrators that use DHCP gleaning, refreshed with DHCPLEASEQUERY messages, will maintain accurate location information. Location information accuracy ensures that the access concentrator can forward data traffic to the intended location in the broadband access network, can perform IP source address verification of

datagrams from the access network, and can encrypt traffic which can only be decrypted by the intended access modem (e.g. [BPI] and [BPI+]). As a result, the access concentrator does not need to depend on ARP broadcasts across the access network, which is susceptible to malicious hosts which masquerade as the intended IP endpoints. Thus, the DHCPLEASEQUERY message allows an access concentrator to provide considerably enhanced security.

DHCP servers SHOULD prevent exposure of location information (particularly the mapping of hardware address to IP address lease, which can be an invasion of broadband subscriber privacy) by leveraging DHCP authentication [DHCPAUTH]. With respect to authentication, the access concentrator acts as the "client". The use of "Authentication Protocol 0" (using simple unencoded authentication token(s) between the access concentrator and the DHCP server) is straightforward. The use of "Authentication Protocol 1" (using "delayed authentication") is under investigation, since it requires two message round trips.

Access concentrators SHOULD minimize potential denial of service attacks on the DHCP servers by minimizing the generation of DHCPLEASEQUERY messages. In particular, the access concentrator should employ negative caching (i.e. cache both DHCPKNOWN and DHCPUNKNOWN responses to DHCPLEASEQUERY messages) and ciaddr restriction (i.e. don't send a DHCPLEASEQUERY message with a ciaddr outside of the range of the attached broadband access networks). Together, these mechanisms limit the access concentrator to transmitting one DHCPLEASEQUERY message (excluding message retries) per legitimate broadband access network IP address after a reboot event.

8. Acknowledgments

Jim Forster, Joe Ng, Guenter Roeck, and Mark Stapp contributed greatly to the initial creation of the DHCPLEASEQUERY message.

Patrick Guelat suggested several improvements to support static IP addressing.

9. References

[RFC 826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", RFC 826, November 1982.

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

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

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

[RFC 2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC 2132] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC 3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[BPI] CableLabs, "Baseline Privacy Interface Specification", SP-BPI-I02-990319, March 1999, available at http://www.cablemodem.com/.

[BPI+] CableLabs, "Baseline Privacy Plus Interface Specification", SP-BPI+-I04-000407, April 2000, available at http://www.cablemodem.com/.

[DHCPAUTH] Droms, R., Arbaugh, W., "Authentication for DHCP Messages", draft-ietf-dhc-authentication-14.txt, July 2000.

[DHCPMIB] Hibbs, R., Waters, G., "Dynamic Host Configuration Protocol (DHCP) Server MIB", draft-ietf-dhc-server-mib-05.txt, November 2000.

[DHCPSCHEMA] Bennett, A., Volz, B., "DHCP Schema for LDAP", draft-ietf-dhc-schema-02.txt, March 2000.

[DOCSIS] CableLabs, "Data-Over-Cable Service Interface Specifications: Cable Modem Radio Frequency Interface Specification SP-RFI-I05-991105", November 1999.

[EUROMODEM] ECCA, "Technical Specification of a European Cable Modem for digital bi-directional communications via cable networks", Version 1.0, May 1999.

[FAILOVER] Droms, R., Kinnear, K., Stapp, M., Volz, B., Gonczi, S., Rabil, G., Dooley, M., Kapur, A., "DHCP Failover Protocol", draft-ietf-dhc-failover-09.txt, July 2001.

10. Author's information

Rich Woundy
Kim Kinnear
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824

Phone: (978) 244-8000

EMail: rwoundy@cisco.com
kkinnear@cisco.com

11. Full Copyright Statement