Dynamic Host Configuration Working Group
INTERNET DRAFT

Rich Woundy
Kim Kinnear
Cisco Systems

March 2002
Expires September 2002

DHCP Lease Query
<draft-ietf-dhc-leasequery-03.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

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.

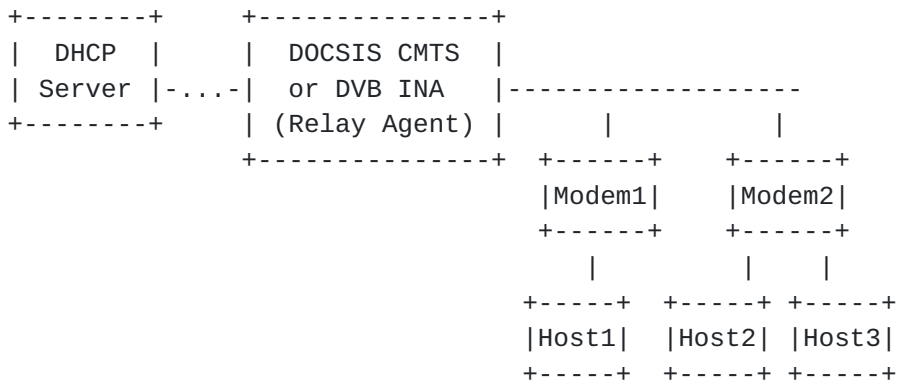


Figure 1: Cable Environment for DHCPLEASEQUERY

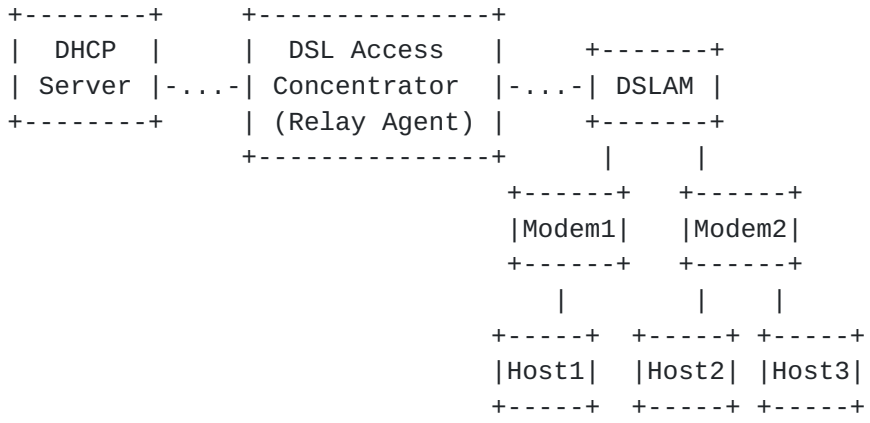


Figure 2: DSL Environment for DHCPLEASEQUERY

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, DHCPACTIVE or DHCPUNKNOWN message. The DHCPACTIVE 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".

- "reservation"

  At times it is convenient for an administrator to assign a fixed IP address to a particular DHCP client. The DHCP server must be

configured with this DHCP client to IP address mapping, typically using the MAC address as the way to identify the client. The DHCP client to IP address mapping, configured in the DHCP server, is called a reservation for the purposes of this document.

- o "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.

- o "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.

- o "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.

- o "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 [RFC 3046]) 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].

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 as a 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 or a Client-identifier option (option 61) appearing in the options area. In this case, the DHCP server SHOULD return an IP address in the "ciaddr" if it has any record of the client described by the Client-identifier or MAC address. In the absence of specific configuration information to the contrary (see Section 6.4) it MUST be the IP address most recently used by the client described by the MAC address or Client-identifier option (or the client described by both, if both appear).

The DHCP servers that implement this protocol always send a response to the DHCPLEASEQUERY message: either a DHCPKNOWN, DHCPACTIVE or DHCPUNKNOWN (or in some cases, DHCPUNIMPLEMENTED). The reasons why a DHCPKNOWN, DHCPACTIVE or DHCPUNKNOWN message might be generated are explained in the specific query regimes, below. Servers which do not support the DHCPLEASEQUERY message SHOULD (and are expected to) drop the DHCPLEASEQUERY message silently, although they MAY respond with a DHCPUNIMPLEMENTED message. The DHCPLEASEQUERY message can support three query regimes:

- Query by IP address:

  For this query, the "ciaddr" field MUST contain an IP address. It MUST NOT contain a MAC address or Client-identifier option (option 61). The DHCP server will return any information that it has on the most recent client to have been allocated that IP address. Any server which supports the DHCPLEASEQUERY message MUST support query by IP address.

  The DHCP server replies to the DHCPLEASEQUERY message with a DHCPKNOWN or DHCPACTIVE 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".

- Query by MAC address:

  For this query, the "ciaddr" field MUST be zero and there MUST be a MAC address is specified in the "htype", "hlen", and "chaddr" fields. There MUST NOT be a Client-identifier option (option 61) in the packet. The DHCP server looks up all IP addresses for which clients with this MAC address are the most recent user. In contrast to the query by IP address, there may be multiple IP addresses which show the client specified by the MAC address as having been the most recent user. The DHCP server places the IP address most recently accessed by a DHCP client with this MAC address (unless specifically configured otherwise, see Section 6.4) in the "ciaddr" field, and returns other information associated with that IP 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 a single Requested IP address option (option 50) [RFC 2132] with multiple IP addresses in it. A server which implements the DHCPLEASEQUERY message SHOULD implement this capability. If it does not, it MUST respond with a DHCPUNIMPLEMENTED message when it receives a query by MAC address.

  The DHCP server replies to the DHCPLEASEQUERY message with a DHCPKNOWN or DHCPACTIVE message if the MAC address corresponds to a DHCP client which was the most recent user of an IP address controlled by this DHCP server. The server replies with a DHCPUNKNOWN message if the MAC address does not correspond to such an IP address.

- Query by Client-identifier option:

  For this query, the "ciaddr" field MUST be zero, there MUST be a Client-identifier option (option 61) in the packet and there MUST NOT be a MAC address in the packet (i.e., the hlen, htype, and chaddr MUST all be zero). The DHCP server looks up all IP addresses for which a client with this Client-identifier is the most recent user. In contrast to the query by IP address, there may be multiple IP addresses which show the client specified by this Client-identifier as having been the most recent user. The DHCP server places the IP address most recently accessed by a DHCP client with this Client-identifier (unless specifically configured otherwise, see Section 6.4) in the "ciaddr" field, and returns other information associated with that IP 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 Client-identifier in a single Requested IP address option (option 50) containing multiple IP addresses. A server which implements the DHCPLEASEQUERY message SHOULD

implement this capability. If it does not, it MUST respond with a DHCPUNIMPLEMENTED message when it received a query by Client-identifier option address.

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 or DHCPACTIVE 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 Parameter Request List (option 55) 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

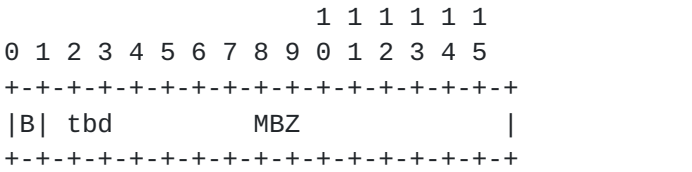
6.1. Definitions required for DHCPLEASEQUERY processing

The operation of the DHCPLEASEQUERY message requires the definition of the following new and extended values for the DHCP packet beyond those defined by [RFC 2131] and [RFC 2132]. See also Section 8, IANA considerations.

1. The message type option (option 53) from [RFC 2132] requires five new values: The DHCPLEASEQUERY message itself and its three possible responses DHCPKNOWN, DHCPACTIVE, DHCPUNKNOWN, and DHCPUNIMPLEMENTED. 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
TBD	DHCPACTIVE
TBD	DHCPUNIMPLEMENTED

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

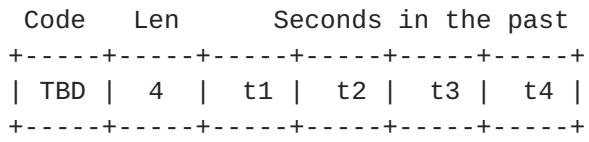
3. There is one new option defined which can be used to return important information in a DHCPKNOWN response to a DHCPLEASE-QUERY message -- the client-last-transaction-time.

client-last-transaction-time

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

This MUST NOT be an absolute time. This MUST NOT be an absolute number of seconds since Jan 1, 1970. Instead, this MUST be an integer number of seconds in the past from the time the DHCPKNOWN message is sent that the client last dealt with this server about this IP address. In the same way that the IP Address Lease Time option (option 51) encodes a lease time which is a number of seconds into the future from the time the message was sent, this option encodes a value which is a number of seconds into the past from when the message was sent.

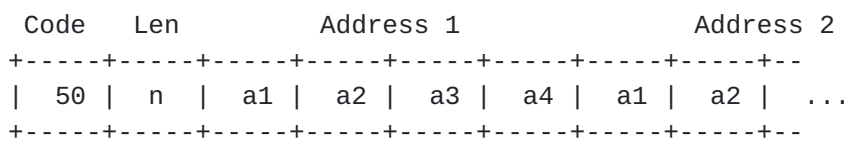
The code for the this option is TBD. The length of the this option is 4 octets.



4. The Requested IP Address option is extended to allow for multiple IP addresses in the option.

This option is used to return all of the IP addresses associated with the DHCP client specified in a particular DHCPLEASEQUERY message.

The code for this option is 50, and its minimum length is 4 and its maximum length MUST be a multiple of 4.



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 requester (i.e. the access concentrator). The giaddr is independent of the "ciaddr" field 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 requester. The interesting options are likely to include the IP Address Lease Time option (option 51) and the Relay Agent Information option (option 82).

- The Reservation bit in the "flags" field of the DHCP packet (see [RFC 2131] and Section 6.1 of this document) is not used when sending a DHCPLEASEQUERY message.

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" field MUST be set to the IP address of the lease to be queried.

  The Client-identifier 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" field MUST be set to zero.

  The Client-identifier option (option 61) MUST NOT appear in the packet.

- Query by Client-identifier option:

  There MUST be a Client-identifier option (option 61) in the

DHCPLEASEQUERY message.

The "ciaddr" field MUST be set to zero.

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

The access concentrator SHOULD ensure that the "ciaddr" field mentioned in the DHCPLEASEQUERY message (if a query by IP address) is a local subnet 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 DHCPLEASEQUERY message MUST have exactly one of: a non-zero ciaddr, a non-zero "htype"/"hlen"/"chaddr", or a Client-identifier.

The DHCP server which receives a DHCPLEASEQUERY message MUST base its response on the particular data item used in the query.

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

There are four possible responses to a DHCPLEASEQUERY message:

- DHCPKNOWN

  The DHCPKNOWN message indicates that the server knows about the IP address or client specified in the DHCPLEASEQUERY message, but there is no currently active lease for the IP address returned in the "ciaddr" field of the DHCPKNOWN message. The R (reservation) bit MAY be set in the case where there is a reservation for this IP address by the client returned in the DHCPKNOWN message, allowing the access concentrator to consider a reservation equivalent to a currently active lease on the IP address.

  The server MUST respond with a DHCPKNOWN message if this server

has information about the IP address or client in question, but that there is no active lease for the IP address or client specified in the query. If the query was by IP address, then the DHCPKNOWN message indicates that this server manages this IP address. If there is a reservation for this IP address, then the DHCP server MUST set the R (reservation) bit in the "flags" field of the DHCP packet, and the DHCP server MUST return whatever client information is known in the DHCPKNOWN message.

In the case where a client was specified either by Client-identifier or MAC address, then the DHCPKNOWN message indicates that the client is known to the DHCP server, and was the most recent client associated with a particular IP address. In the case where the client specified has a reservation for the IP address returned in the ciaddr, the R (reservation) bit is set in the "flags" field of the DHCP packet.

o DHCPUNKNOWN

The DHCPKNOWN message indicates that the server knows nothing about the IP address or client specified in the DHCPLEASEQUERY message.

The server MUST response with a DHCPKNOWN message when this server has no information about the IP address or client specified in the DHCPLEASEQUERY message.

When responding with a DHCPUNKNOWN, the DHCP server SHOULD NOT include other DHCP options in the response. The R (reservation) bit MUST NOT be set in the "flags" field of the DHCP packet.

o DHCPACTIVE

The DHCPACTIVE message indicates that the server not only knows about the IP address and client specified in the DHCPACTIVE message but also that there is an active lease by that client for that IP address.

In some cases, the DHCP server MAY be configured to return a DHCPACTIVE message when there is no active lease but when there is a reservation by the specified client for the IP address in the "ciaddr" field of the DHCPACTIVE message. A server would be so configured when it was desired that the access concentrator would allow access to IP addresses which are not DHCP clients. In this case the DHCP server SHOULD NOT place an IP Address Lease Time (option 51) in the DHCPACTIVE message, allowing the access concentrator to determine that this is a DHCPACTIVE message for an IP address without a currently active lease.

The server MUST respond with a DHCPACTIVE message when the IP address returned in the "ciaddr" field is currently leased. If the client returned in the DHCPACTIVE message has a reservation for that IP address recorded in the DHCP server, then the R (reservation) bit MUST be set in the "flags" field of the DHCP packet.

- DHCPUNIMPLEMENTED

  The DHCPUNIMPLEMENTED message indicates that the particular form of DHCPLEASEQUERY used is not implemented in this DHCP server. It may mean that the DHCPLEASEQUERY message as a whole is not implemented by this DHCP server although it is usually used to indicate that a query by Client-identifier or MAC address is not implemented by a DHCP server that otherwise supports a DHCPLEASEQUERY by IP address.

Since the response to a DHCPLEASEQUERY request can only contain full information about one IP address -- the one that appears in the "ciaddr" field -- determination of which IP address to which to respond is a key issue. (Of course, the values of additional IP addresses for which a client has a lease may also be returned in multiple Requested IP address options (option 50). This is the only information returned not directly associated with the IP address in the "ciaddr" field.)

6.4.1. Determining the IP address to which to respond

In the event that an IP address appears in the "ciaddr" field of a DHCPLEASEQUERY message, if that IP address is one managed by the DHCP server, then that IP address MUST be set in the "ciaddr" field of a DHCPKNOWN message.

If the IP address is not managed by the DHCP server, then a DHCPUNKNOWN message must be returned.

If the "ciaddr" field of the DHCPLEASEQUERY is zero, then the DHCPLEASEQUERY message is a query by Client-identifier or MAC address. In this case, the client's identity is any client which has proffered an identical Client-identifier option (if the Client-identifier option appears in the DHCPLEASEQUERY message), or an identical MAC address (if the MAC address fields in the DHCPLEASEQUERY message are non-zero). This client matching approach will, for the purposes of this section, be described as "Client-identifier or MAC address".

The Reservations bit (the R bit) has no meaning in the DHCPLEASEQUERY message and is used only to indicate the existence of a reservation

in a DHCPKNOWN or DHCPACTIVE message.

If the "ciaddr" field is zero in a DHCPLEASEQUERY message, then the IP address placed in the "ciaddr" field of the DHCPKNOWN or DHCPACTIVE message MUST be that of an IP address for which the client that most recently used the IP address matches the Client-identifier or MAC address specified in the DHCPLEASEQUERY message.

If there is only a single IP address which fulfills this criteria, then it MUST be placed in the "ciaddr" field of the DHCPKNOWN or DHCPACTIVE message.

In the case where more than one IP has been accessed by the client specified by the MAC address or Client-identifier option, then the DHCP server MUST return the IP address returned to the client in the most recent transaction with the client unless the DHCP server has been configured by the server administrator to use some other preference mechanism.

If, after all of the above processing, no value is set in the "ciaddr" field of the DHCPKNOWN or DHCPACTIVE message, then a DHCPUNKNOWN message MUST be returned instead.

6.4.2. **Building a DHCPKNOWN or DHCPACTIVE message once the "ciaddr"** field is set

Once the "ciaddr" field of the DHCPKNOWN or DHCPACTIVE message is set, the rest of the processing largely involves returning information about the IP address specified in the "ciaddr" field.

If the IP address in the "ciaddr" field of the DHCPKNOWN or DHCPACTIVE message is currently leased by the client specified in the Client-identifier or MAC address returned in the DHCPKNOWN or DHCPACTIVE message, then the message MUST be a DHCPACTIVE message, otherwise it MUST be a DHCPKNOWN message.

It MAY be possible to configure a DHCP server to return a DHCPACTIVE message even though the IP address specified in the "ciaddr" field is not currently leased if there is a reservation for that IP address by the client specified in the Client-identifier or MAC address fields of the DHCPACTIVE message. In this case, there MUST NOT be an IP Address Lease Time option (option 51) in the packet.

The R (reservation) bit must be set in the "flags" field if the IP address in the "ciaddr" field is reserved for the client returned in the MAC address or Client-identifier option.

The IP address in the "ciaddr" field of the DHCPKNOWN or DHCPACTIVE

message MUST be one for which this server is responsible (or a DHCPUNKNOWN message would be have already been returned early in the processing described in the previous section).

The MAC address of the DHCPKNOWN or DHCPACTIVE message MUST be set from the client associated with the IP address in the "ciaddr" field of the DHCPKNOWN message. This may be derived from a real DHCP client or from reservation information configured into the DHCP server.

If the Client-identifier option (option 61) is specified in the Parameter Request List option (option 55), then the Client-identifier (if any) of the client associated with the IP address in the "ciaddr" field SHOULD be returned in the DHCPKNOWN or DHCPACTIVE message. This may be derived from a real DHPC client, or from reservation information configured into the DHCP server.

In the case where more than one IP has been accessed by the client specified by the MAC address and/or Client-identifier option, then the list of all of the IP addresses SHOULD be returned as multiple Requested IP address options (option 50), if that option was requested as part of the Parameter Request List 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 requester (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.

If there is no currently valid lease on the IP address in the "ciaddr" field, and if the R bit is set in the DHCPLEASEQUERY and in the DHCPKNOWN messages (i.e., if the sender of the DHCPLEASEQUERY message requested reservation information, and the "ciaddr" in the DHCPKNOWN message was derived from reservation information), then the DHCP server MAY synthesize an IP Address Lease Time option for the DHCPKNOWN message if configured to do so. Typically the value of this option would itself be a configuration parameter of the DHCP server.

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 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.

The DHCPKNOWN or DHCPACTIVE 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 or DHCPACTIVE option values. The values of the options that were returned to the DHCP client would generally be preferred, but in the absence of those, options that were sent in DHCP client requests would be acceptable.

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 (option 82) values to the secondary server via the DHCP Failover BNDUPD messages.

6.4.3. Sending a DHCPKNOWN, DHCPACTIVE, or DHCPUNKNOWN message

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

6.5. Receiving a DHCPKNOWN, DHCPACTIVE, or DHCPUNKNOWN Message

When a DHCPACTIVE message is received in response to the DHCPLEASEQUERY message 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 DHCPACTIVE 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 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.

If the R (reservation) bit is set in the "flags" field of the DHCPKNOWN message, it means that a reservation exists in the DHCP server for the IP address and associated client. The access concentrator MAY be configured to allow the client access even though no currently outstanding lease is in place for this

In either case, when a DHCPKNOWN or DHCPACTIVE 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" field of the DHCPLEASEQUERY message. If there is no IP address in the "ciaddr" field of the DHCPLEASEQUERY message, then a DHCPUNKNOWN message means that the DHCP server does not have definitive information concerning the any DHCP client specified in the "hlen", "htype", and "chaddr" fields or the Client-identifier 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" field with a DHCPUNKNOWN.

When a DHCPUNIMPLEMENTED message is received by an access concentrator, it means that the particular aspect of DHCPLEASEQUERY processing requested is not implemented in the responding server. It may or may not be the case that other aspects of DHCPLEASEQUERY processing are not implemented in that server.

6.6. Receiving 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, DHCPACTIVE 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 DHCPLEASE-QUERY 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 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.

In practice this approach would probably best be handled by a per-server timer that backs off exponentially to once a minute, and a per-message backoff timer that also backs off to once a minute. The per-server timer would start off expired, and in the expired state only one DHCPLEASEQUERY message would be queued for the associated server. This DHCPLEASEQUERY message would be sent with the backoff quickly moving to once a minute until a DHCPACTIVE, DHCPKNOWN, or DHCPUNKNOWN message reply was received. Whenever one of these messages is received, the per-server timer is reset, and whenever the per-server timer has not expired, more than one individual DHCPLEASE-QUERY messages can be outstanding to the DHCP server at one time. It is recommended that this number be limited to a relatively small number, for example, 100 or 200, to avoid swamping the DHCP server. Each of these messages should have its own per-message retry timer. This would retransmit each message and backoff as discussed above. In the event the per-server timer goes off, then all outstanding messages SHOULD be dropped except for a single DHCPLEASEQUERY message which is used to poll the server until such time as another DHCPACTIVE, DHCPKNOWN, or DHCPUNKNOWN message is received.

6.7. Using the DHCPLEASEQUERY message in a failover environment

When using 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.

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 [RFC 3118]. 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. Alternatively, use of IPsec would also be a way to ensure security between the relay agent and the DHCP server.

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 cacheing (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. IANA Considerations

IANA has assigned seven values for this document. See Section 6.1 for details. There are five new messages types, which are the value of the message type option (option 53) from [RFC 2132]. The value for DHCPLEASEQUERY is TBD, the value for DHCPKNOWN is TBD, the value for DHCPACTIVE is TBD, the value for DHCPUNKNOWN is TBD and the value for DHCPUNIMPLEMENTED is TBD. There is a new bit defined for the "flags" field of the DHCP packet (see Section 1, Figure 1 and Table 1 of [RFC 2131]). The flag is called "R: RESERVATION flag", and its

value is TBD. Finally, there is one new DHCP option defined, which is the client-last-transaction-time option, and its option code is TBD.

9. 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.

10. 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.

[RFC 3118] Droms, R., Arbaugh, W., "Authentication for DHCP Messages", RFC 3118, June 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/.

[DHCPMIB] Hibbs, R., Waters, G., "Dynamic Host Configuration Protocol (DHCP) Server MIB", draft-ietf-dhc-server-mib-06.txt, February 2002.

[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-10.txt, January 2002.

11. Author's information

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

Phone: (978) 497-8000

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

12. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this

specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

13. Full Copyright Statement