DHC Working Group P. Kurapati
Internet-Draft R. Desetti
Expires: July 17, 2009 B. Joshi
Infosys Technologies Ltd.
January 13, 2009

DHCPv4 Leasequery by relay agent remote ID
draft-ietf-dhc-leasequery-by-remote-id-01.txt

Status of this Memo

Copyright Notice

Abstract

Some Relay Agents extract lease information from the DHCP message exchanged between the client and DHCP server. This lease information is used by relay agents for various purposes like antispoofing, prevention of flooding. RFC 4388 defines a mechanism for relay agents to retrieve the lease information from the DHCP server as and when this information is lost. Existing leasequery mechanism is data driven which means that a relay agent can initiate the leasequery only when it starts receiving data from/to the clients. In certain scenarios, this model is not scalable. This document first looks at issues in existing mechanism and then proposes a new query type, query by remote ID, to address these issues.

Table of Contents

1. Introduction

DHCP relay agents snoop DHCP messages and append relay agent information option before relaying it to the configured DHCP Servers. In this process, some relay agents also glean the lease information sent by the server and maintain this locally. This information is used for prevention of spoofing attempts from the clients and also sometimes used to install routing information. When relay agent reboots, this information is lost. RFC 4388 [RFC4388] has defined a mechanism to retrieve this lease information from the DHCP server. The existing query types defined by RFC 4388 [RFC4388] are data driven. When client initiates data, based on the source MAC/IP address, relay agent can query the server about the lease information. These mechanisms do not scale well when there are thousands of clients connected to the relay agent. In data driven model, DHCP Leasequery does not provide all the active Lease informations associated with a given connection/circuit [consolidated information] which will result into an inefficient anti-spoofing. It also has to contend with considerable resources for negative caching specially under spoof attacks.

We need a mechanism for relay agent to retrieve the consolidated lease information for a given connection/circuit before traffic is initiated by the clients.

```
              +--------+
              |  DHCP  |     +--------------+
              | Server |-...-|    DSLAM     |
              |        |     |  Relay Agent |
              +--------+     +--------------+
                                |        |
                            +------+   +------+
                            |Modem1|   |Modem2|
                            +------+   +------+
                               |        |    |
                            +-----+  +-----+ +-----+
                            |Host1|  |Host2| |Host3|
                            +-----+  +-----+ +-----+
```

Figure 1

For example, when a DSLAM acting as a Relay Agent is rebooted, it should query the server for the lease information for all the connections/circuits. Also, as shown in the above figure, there could be multiple clients on one DSL circuit. Relay agent should get the lease information of all the clients connected to a DSL circuit. This is possible by introducing a new query type based on the Remote Id sub-option of Relay Agent Information option. This document talks

about the motivation for the new query type and the method to do the same.

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 [RFC2119].

This document uses the following terms:

o "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.

o "DHCP client"

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

o "DHCP relay agent"

A DHCP relay agent is a third-party agent that transfers Bootstrap Protocol (BOOTP) and DHCP messages between clients and servers residing on different subnets, per RFC951[RFC951] and RFC1542[RFC1542].

o "DHCP server"

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

o "downstream"

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

o "fast path"

Data transfer which happens through Network Processor or an ASIC which are programmed to forward the data at very high speeds.

o "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 following fields: hardware type "htype", hardware length "hlen", and client hardware address "chaddr".

- "slow path"

Data transfer which happens through the control plane. Typically this has very limited buffers to store data and the speeds are very low compared to fast path data transfer.

- "upstream"

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

3. Motivation

Consider a typical access concentrator (e.g., DSLAM) working also as a DHCP relay agent. "Fast path" and "slow path" generally exist in most networking boxes. Fast path processing is done in network processor or an ASIC (Application Specific Integrated Circuit). Slow path processing is done in a normal processor. As much as possible, regular data handling code should be in fast path. Slow path processing should be reduced as it may become a bottleneck.

For an access concentrator having multiple access ports, multiple IP addresses may be assigned using DHCP to a single port and the number of clients on a port may be unknown. The access concentrator may also not know the network portions of the IP addresses that are assigned to its DHCP clients.

The access concentrator gleans IP address or other information for antispoofing and for other purposes from DHCP negotiations. The antispoofing itself is done in fast path. Access concentrator keeps track of only one list of IP addresses: list of IP addresses that are assigned by DHCP server. Traffic for all other IP addresses is dropped. If client starts its data transfer after its DHCP negotiations are gleaned by access concentrator, no legitimate packets will be dropped because of antispoofing. In other words, antispoofing is effective (no legitimate packets are dropped and all spoofed packets are dropped) and efficient (antispoofing is done in fast path). The intention is to achieve similar effective and efficient antispoofing in the lease query scenario also when an access concentrator loses its gleaned information (for example, because of reboot).

After a deep analysis, we found that the three existing query types supported by RFC 4388[RFC4388] do not provide effective and efficient antispoofing for the above scenario and a new mechanism is required.

The existing query types

- necessitate a data driven approach: the lease queries can only be done when access concentrator receives data. That results in increased outage time for clients.

- result in excessive negative caching consuming lot of resources under a spoofing attack.

- result in antispoofing being done in slow path instead of fast path.

The deeper analysis, which led to the above conclusions, itself

appears as an Appendix to this document.

4. Design Goals

The goal of this document is to provide a lightweight mechanism for access concentrator to retrieve lease information available in the DHCP server. The mechanism SHOULD also support an access concentrator to retrieve consolidated lease information for a connection/circuit.

4.1. Information Acquisition before Data Starts

Existing data driven approach by RFC 4388 [RFC4388] means that the lease queries can only be done when access concentrator receives data. If an approach exists to initiate lease queries even before the calls come up, then it will be more effective. For antispoofing, packets need to be dropped until it gets the lease information from DHCP server. If access concentrator finishes the lease queries before it start receiving data, then there is no need to drop legitimate packets. So, effectively outage time may be reduced. The lease queries should help in retrieving lease information even before the data starts flowing and should be independent of data traffic.

4.2. Lessen Negative Caching

If lease queries result in negative caches, then that puts additional overhead on access concentrator. The negative caches not only consume precious resources they also need to be managed. Hence they should be avoided as much as possible. The lease queries should reduce the need for negative caching as far as possible.

4.3. Antispoofing in 'Fast Path'

If Antispoofing is not done in fast path, it will become a bottleneck and may lead to denial of service of access concentrator. The lease queries should make it possible to do antispoofing in fast path.

5. Protocol Overview

RFC 3046 [RFC3046] defines two sub-options for Relay Agent Information option. Sub-option 1 corresponds to circuit ID which identifies the local circuit of the access concentrator. This sub-option is unique to the relay agent. Sub-option 2 corresponds to remote ID which identifies the remote host end of the circuit. This is globally unique in the network.

This document defines a new query type based on remote ID sub-option. Suppose that the access concentrator (e.g., DSLAM) lost the lease information when it was rebooted. When the access concentrator comes up, it would initiate a DHCPLEASEQUERY message for each connection/ circuit containing the Relay Agent Information option [RFC3046] with sub-option remote ID. DHCP server must return an IP address in the ciaddr if it has any record of the client described by the remote ID. In the absence of specific configuration information to the contrary, it SHOULD be the IP address with the latest client-last-transaction-time associated with the client described by the remote ID. The DHCP servers that implement this document always send a response (DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE, or DHCPLEASEUNKNOWN) to the DHCPLEASEQUERY message. The reasons why a DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE, or DHCPLEASEUNKNOWN message might be generated are explained in the specific query regimes below. Servers that do not implement the DHCPLEASEQUERY based on remote ID message SHOULD simply not respond.

The query regime is described below:

o Query by Agent Remote ID sub-option:

For this query, the requester supplies only a option 82 which will include only an Agent Remote ID sub-option in the DHCPLEASEQUERY message. The DHCP server will return any information that it has on the IP address most recently accessed by a client with that Agent Remote ID. In addition, it SHOULD supply any additional IP addresses that have been associated with Agent Remote ID in different subnets. Information about these bindings can then be found using the Query by IP Address, as described in RFC 4388[RFC4388].

The DHCP server MUST reply with a DHCPLEASEACTIVE message if the Agent Remote ID in the DHCPLEASEQUERY message currently has an active lease on an IP address in this DHCP server. The server MUST reply with a DHCPLEASEUNASSIGNED if it has information of the said remote ID but no lease is assigned for the same. The server MAY keep track of the remote ID values for which it has currently active leases as well as any which it has served in the past but for which it has no currently active leases. The server MUST reply with a

DHCPLEASEUNKNOWN message if it has no information of the said remote ID.

6. Protocol Details

In this section, DHCPLEASEQUERY message refers to DHCPLEASEQUERY message with query by remote ID.

6.1. 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 RFC2131[RFC2131], and uses message number 10 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 the return address of the DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE, or DHCPLEASEUNKNOWN message from the DHCP server. Note that this use of the giaddr is consistent with the definition of giaddr in RFC2131[RFC2131], where the giaddr is always used as the return address of the DHCP response message. In some (but not all) contexts in RFC 2131, the giaddr is used as the "key" to access the appropriate address pool.

- The Parameter Request List option (option 55) SHOULD be set to the options of interest to the requester. It MUST include the Relay Agent Information option (option 82). The other interesting options are likely to include the IP Address Lease Time option (option 51), and possibly the Vendor class identifier option (option 60). In the absence of a Parameter Request List option, the server SHOULD return the same options it would return for a DHCPREQUEST message that didn't contain a DHCPLEASEQUERY message, which includes those mandated by Section 4.3.1 of [RFC2131] as well as any options that the server was configured to always return to a client.

Additional details concerning different query types are

- Query by Agent Remote ID sub-option:

  * There MUST be a Relay Agent Information option (option 82) with only Agent Remote ID sub-option (sub-option 2) in the DHCPLEASEQUERY message.

  * The "ciaddr" field MUST be set to zero.

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

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

The DHCPLEASEQUERY message SHOULD be sent to a DHCP server which is known to possess authoritative information concerning the remote ID. 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 remote ID, it SHOULD be sent to all DHCP servers configured for the associated relay agent (if any are known).

6.2. Receiving the DHCPLEASEQUERY Message

A DHCPLEASEQUERY message MUST have a non-zero giaddr. The DHCPLEASEQUERY message MUST have a zero ciaddr, a zero htype/hlen/chaddr, and no Client-identifier option. The DHCPLEASEQUERY message MUST have a relay agent option 82 with only remote ID sub-option.

6.3. Responding to the DHCPLEASEQUERY Message

There are three possible responses to a DHCPLEASEQUERY message:

o DHCPLEASEUNASSIGNED

The server MUST respond with a DHCPLEASEUNASSIGNED message if this server has information about the remote ID, but there is no associated active lease. The DHCPLEASEUNASSIGNED indicates that the server manages the IP address allocation for the given remote ID, but there is no currently active lease.

o DHCPLEASEUNKNOWN

The DHCPLEASEUNKNOWN message indicates that the client specified in the DHCPLEASEQUERY message is not managed by the server.

o DHCPLEASEACTIVE

The DHCPLEASEACTIVE message indicates that the server not only knows the client specified in the DHCPLEASEQUERY message, but also knows that there is an active lease for that client.

6.4. Determining the IP address to be used in response

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 about which to respond is a key issue. Of course, the values of additional IP addresses for which a client has a lease must also be returned in the

associated-ip option (RFC 4388[RFC4388], Section 6.1, #3). This is the only information returned not directly associated with the IP address in the "ciaddr" field.

The client's identity is any client that has proffered an identical Agent Remote ID (if the option 82 with Agent Remote ID sub-option appears in DHCPLEASEQUERY message). This client matching approach will, for the purposes of this section, be described as "remote ID".

The IP address placed in the "ciaddr" field of a DHCPLEASEACTIVE message MUST be the IP address with the latest client-last-transaction-time associated with the client described by the remote ID specified in the DHCPLEASEQUERY message.

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

In the case where more than one IP address has been accessed by the client specified by the Remote ID, 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.

6.5. Building a DHCPLEASEUNASSIGNED, DHCPLEASEUNKNOWN, or DHCPLEASEACTIVE Messages

DHCPLEASEUNASSIGNED and DHCPLEASEUNKNOWN messages are created alike except for message type. DHCP server MUST echo the received Option 82 available in DHCPLEASEQUERY in the response. No other options are returned for these messages. With that the processing for a DHCPLEASEUNASSIGNED or DHCPLEASEUNKNOWN message is complete.

For the DHCPLEASEACTIVE message, the rest of the processing largely involves returning information about the IP address specified in the "ciaddr" field.

The MAC address of the DHCPLEASEACTIVE message MUST be set to the values that identify the client associated with the IP address in the "ciaddr" field of the DHCPLEASEACTIVE message.

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 DHCPLEASEACTIVE message.

In the case where more than one IP address has been involved in a DHCP message exchange with the client specified by the Agent Remote

ID, then the list of all those IP addresses MUST be returned in the associated-ip option, whether or not 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 then the DHCP server MUST return this option in the DHCPLEASEACTIVE message with its value equal to the time remaining until 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. DHCP server SHOULD return these options (when requested) with the remaining time until renewal or rebinding, respectively.

The information contained in the most recent Relay Agent Information option received from the relay agent associated with this IP address MUST be included in the DHCPLEASEACTIVE message.

The DHCPLEASEACTIVE 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 and that are acceptable to return based on the list of "non-sensitive options", discussed below.

DHCP servers SHOULD be configurable with a list of "non-sensitive options" that can be returned to the access concentrator when specified in the Parameter Request List of the DHCPLEASEQUERY message. Any option not on this list SHOULD NOT be returned to an access concentrator, even if requested by that access concentrator.

The DHCP server uses information from its lease binding database to supply the DHCPLEASEACTIVE 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 some cases, the Relay Agent Information option in an incoming DHCPREQUEST packet is used to help determine the options returned to the DHCP client that sent the DHCPREQUEST. When responding to a DHCPLEASEQUERY message, the DHCP server MUST use the saved Relay Agent Information option just like it did when responding to the DHCP client in order to determine the values of any options requested by the DHCPLEASEQUERY message. The goal is to return the same option values to the DHCPLEASEQUERY as those that were returned to the DHCPDISCOVER or DHCPREQUEST from the DHCP client (unless otherwise specified, above).

In the event that two servers are cooperating to provide a high-availability DHCP server, as supported by [RFC2131], they would have to communicate some information about IP address bindings to each other. In order to properly support the DHCPLEASEQUERY message, these servers MUST ensure that they communicate the Relay Agent Information option information to each other in addition to any other IP address binding information.

6.6. Sending a DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE, or DHCPLEASEUNKNOWN Message

The server expects a giaddr in the DHCPLEASEQUERY message, and unicasts the DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE, or DHCPLEASEUNKNOWN message to the giaddr.

6.7. Receiving a DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE, or DHCPLEASEUNKNOWN Message

When a DHCPLEASEACTIVE 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 DHCPLEASEACTIVE as well as Relay Agent Information option information included in the packet to refresh its location information for this IP address. An access concentrator is likely to query by IP address for all the IP addresses specified in the associated-ip option in the response, if any, at this point in time.

When a DHCPLEASEUNASSIGNED message is received in response to the DHCPLEASEQUERY message, it means that there is no currently active lease associated with the client specified by remote ID in the DHCP server, but that this server does in fact manage the IP address allocation for the client specified by remote ID. In this case, the access concentrator SHOULD cache this information for later use.

When a DHCPLEASEUNKNOWN message is received by an access concentrator that has sent out a DHCPLEASEQUERY message, it means that the DHCP server does not have definitive information concerning the DHCP client specified in the Agent Remote ID sub-option of the DHCPLEASEQUERY message. The access concentrator SHOULD cache this information, but only for a relatively short lifetime, approximately 5 minutes. Having cached this information, the access concentrator SHOULD only infrequently direct a DHCPLEASEQUERY message to a DHCP server that responded to a DHCPLEASEQUERY message with a DHCPLEASEUNKNOWN.

6.8. Receiving No Response to the DHCPLEASEQUERY Message

When an access concentrator receives no response to a DHCPLEASEQUERY message, it should be handled in the same manner as suggested in RFC 4388 [RFC4388].

6.9. Lease Binding Data Storage Requirements

Implementation Note:

To generate replies for a lease query by remote-id effeciently, a DHCP server should index the lease binding data structures using remote-id.

6.10. Using the DHCPLEASEQUERY Message with Multiple DHCP Servers

This scenario should be handled in the same way it is done in RFC 4388 [RFC4388].

7. RFC 4388 Considerations

This document is compatible with RFC 4388 [RFC4388] based implementations which means that a client which supports this extension can work with a server not supporting this document provided it uses RFC 4388 [RFC4388] defined query types. Also, a server supporting this document can work with a client not supporting this query type. However, there are some changes that this document proposes with respect to RFC 4388 [RFC4388]. Implementors extending RFC 4388 [RFC4388] implementation to support this document, should take note of the following points:

- RFC 4388 [RFC4388] suggests that a DHCPLEASEUNASSIGNED is returned only in the case of 'query by IP address'. All other query types will have a return message of either DHCPLEASEACTIVE or DHCPLEASEUNKNOWN'. This document proposes that DHCPLEASEUNASSIGNED can be returned for the query by remote ID.

- There may be cases where a query by IP address/MAC address/Client Identifier has an option 82 containing remote ID. In that case, the query will still be recognized as query by IP address/MAC address/Client Identifier as specified by RFC 4388 [RFC4388].

- Section 6.4 of RFC 4388 [RFC4388] suggests that a DHCPLEASEUNKNOWN MUST NOT have any other option present. But for a query by remote ID, option 82 MUST be present in the reply.

8. Security Considerations

This document does not introduce any new security concerns beyond those specified in the original leasequery protocol RFC 4388 [RFC4388] specifications.

9. IANA Considerations

This document does not introduce any new namespaces for the IANA to manage.

10. Acknowledgments

Copious amounts of text in this document are derived from RFC 4388 [RFC4388]. Kim kinnear provided valuable feedback on this document.

11. References

11.1. Normative Reference

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4388] Woundy, R. and K. Kinnear, "Dynamic Host Configuration Protocol (DHCP) Leasequery", RFC 4388, February 2006.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

11.2. Informative Reference

[RFC951] Croft, B. and J. Gilmore, "Bootstrap Protocol (BOOTP)", RFC 951, September 1985.

[RFC1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993.

[RFC2132] Droms, R. and S. Alexander, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

Appendix A. Why a New Leasequery is Required?

The three existing query types supported by RFC 4388 do not provide effective and efficient antispoofing for the above scenario.

- Query by Client Identifier

Query by Client Identifier is not possible because to use that access concentrator need to glean client identifier also but the whole issue is that we need leasequeries because the gleaned information was lost. On the other hand, we can query by client identifier when client sends a DHCP request, but then there may not be any need for lease query as such -- regular gleaning may be enough.

- Query by IP Address

RFC 4388 suggests that it is preferable to use Query by IP Address when getting downstream traffic.

Query by IP address is not very useful in downstream traffic because downstream traffic may not exist for the clients on a access port. (In most Internet applications, downstream traffic exists only when a client sends upstream traffic). In other words, the client will be denied service until it gets downstream traffic, which may never come.

Query by IP address may be used for upstream traffic. Then whenever an upstream packet comes whose IP address is unknown to the access concentrator, a lease query may be initiated. A related question is what to do with that upstream traffic itself until lease query response comes? If the traffic is dropped, we may be dropping legitimate traffic. If the traffic is forwarded, we may be forwarding spoofed packets. Once the lease response comes, subsequent traffic is handled depending on the response. If a DHCPLEASEACTIVE response comes, access concentrator will accept the traffic. If a DHCPLEASEUNASSIGNED response comes, access concentrator will drop the traffic corresponding to the IP address. If a DHCPLEASEUNKNOWN response comes, access concentrator may drop the traffic corresponding to the IP address but will have to periodically send the lease query for that IP address again (additional overhead). The process is triggered whenever an unknown IP address comes.

Note that access concentrator needs to keep track of 4 lists of IP addresses: (1) List of IP addresses for which it got DHCPLEASEACTIVE responses; (2) List of IP addresses for which it got DHCPLEASEUNASSIGNED responses; (3) List of IP addresses for which it got DHCPLEASEUNKNOWN responses; (4) All other IP addresses.

This approach may be acceptable if only legitimate traffic is received. Consider the case when someone sends packets that uses spoofed IP addresses. In that case, lease response will be DHCPLEASEUNASSIGNED or DHCPLEASEUNKNOWN. RFC 4388 suggests usage of negative caching in this regard (which involves additional resources).

In a spoofing type of attack, negative caching information may grow considerably if attacker varies the source IP address. For each such new source IP address, traffic will come to slow path, a new lease query needs to be initiated, response will be processed, and negative caching to be done. That will mean using many resources for negative caching.

RFC 4388 suggests that if the access concentrator knows the network portion of the IP addresses that are assigned to its clients, then some amount of antispoofing can be done in fast path and some lease queries may be avoided. But as indicated before, that information may not always be available to access concentrators.

Effectively, antispoofing support involves considerable slow path processing and considerable resources tied for negative caching.

RFC 4388 says that DHCP server should be protected from being flooded with too many leasequery requests and access concentrator also should not send too many lease query messages at a time. This would mean that legitimate clients may be excessively delayed getting their information in the face of antispoofing attacks.

It is concluded that antispoofing is neither effective nor efficient with this query type.

o Query by MAC Address

Query by MAC address can also be used similar to query by IP address described above. Indeed, query by MAC address may be better than query by IP address in one sense because of the possible presence of associated-ip option in lease responses (Note that associated-ip option does not appear in responses for query by IP address). With associated-ip option, access concentrator can get information not only about the IP address/MAC address that triggered the lease query but also about other IP addresses that are associated with the original MAC address. That way, when traffic that uses the other IP addresses comes along, access concentrator is already prepared to deal with them.

Although, query by MAC address is better than query by IP address in the above respect, it has a specific problem which is not shared by

query by IP address. For a query by MAC address, only two types of responses are possible: DHCPLEASEUNKNOWN and DHCPLEASEACTIVE; DHCPLEASEUNASSIGNED is not supported. This is particularly troublesome when a DHCP server indeed has definitive information that no IP addresses are associated with the specified MAC address in the leasequery, but it is forced to respond with DHCPLEASEUNKNOWN instead of DHCPLEASEUNASSIGNED. As we have seen above, unlike DHCPLEASEUNASSIGNED, DHCPLEASEUNKNOWN requires periodic querying with DHCP server, an additional overhead.

Moreover, query by MAC address also shares all other issues we discussed above for query by IP address.

We conclude that existing lease query types are not appropriate to achieve effective and efficient antispoofing.

Authors' Addresses

Pavan Kurapati
Infosys Technologies Ltd.
44 Electronics City, Hosur Road
Bangalore 560 100
India

Email: pavan_kurapati@infosys.com
URI: http://www.infosys.com/

D.T.V Ramakrishna Rao
Infosys Technologies Ltd.
44 Electronics City, Hosur Road
Bangalore 560 100
India

Email: ramakrishnadtv@infosys.com
URI: http://www.infosys.com/

Bharat Joshi
Infosys Technologies Ltd.
44 Electronics City, Hosur Road
Bangalore 560 100
India

Email: bharat_joshi@infosys.com
URI: http://www.infosys.com/