

ICS 33.030.30  
M 32



# 中华人民共和国通信行业标准

YD/T 3065-2016

## IPv6 地址编码与管理技术要求 基于 DHCPv6 的地址租约查询

Technical requirements for IPv6 address coding and management  
—DHCPv6 Leasequery

2016-04-05 发布

2016-07-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

    3.1 术语和定义.....1

    3.2 缩略语.....1

4 概述.....2

5 租约查询.....3

    5.1 消息和选项定义.....3

    5.2 消息验证.....6

    5.3 DHCPv6租约查询请求端行为.....7

    5.4 DHCPv6租约查询服务器行为.....8

    5.5 安全考量.....9

6 批量租约查询.....10

    6.1 概述.....10

    6.2 消息和选项的定义.....10

    6.3 请求端行为.....13

    6.4 服务器行为.....14

    6.5 安全考量.....16

参考文献.....17

## 前 言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国互联网络信息中心、互联网域名系统北京市工程研究中心有限公司、北龙中网（北京）科技有限责任公司、国家计算机网络应急技术处理协调中心、中国信息通信研究院。

本标准主要起草人：田野、马迪、邢志杰、卢文哲、钱炜烁、延志伟、周渊、马军锋。

# IPv6地址编码与管理技术要求

## 基于DHCPv6的地址租约查询

### 1 范围

本标准规定了一种可以用于从DHCPv6服务器端获取DHCPv6客户端的租约信息的交互租约查询方法，包括在DHCPv6租约查询请求端和服务端进行通信的数据格式及其交互逻辑的要求。

本标准适用于支持DHCPv6的设备。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2296-2011 IPv6 动态主机配置协议技术要求

### 3 术语、定义和缩略语

#### 3.1 术语和定义

下列术语和定义适用于本文件。

##### 3.1.1

**访问集中器 Access Concentrator**

在宽带服务提供商和公共宽带网络边界上的一个路由器或者交换机。在本标准中，假定访问集中器有DHCPv6中继代理的功能。

##### 3.1.2

**客户端 Client**

与DHCPv6服务器存在一个或多个连接的节点。该描述不包括发出租约查询请求的节点，除非它本身与DHCPv6服务器存在一个或多个连接。

##### 3.1.3

**收集 Gleaning**

从DHCPv6消息中获取位置信息的过程，在经由DHCP中继代理转发时执行。

##### 3.1.4

**位置信息 Location Information**

访问集中器收集的信息，用以将网络流量数据转发给宽带可连接的主机。这些数据包括了主机的硬件地址、连接到主机的端口或虚拟线路、和/或中间用户调制解调器的硬件地址。

##### 3.1.5

**请求端 Requestor**

向一个或多个DHCPv6服务器发送租约查询消息，以获取与DHCPv6服务器相连接的DHCPv6客户端的信息的节点。

#### 3.2 缩略语

下列缩略语适用于本文件。

## YD/T 3065-2016

## DHCP Dynamic Host Configuration Protocol 动态主机配置协议

## 4 概述

YD/T 2296-2011 中规定的 DHCPv6 []要求中规定了一种向一个 IPv6 节点分配 IPv6 地址和配置信息的机制。DHCPv6 中的前缀选项，规定了一种自动代理 IPv6 前缀和相关选项的机制。部署了 DHCPv6 的网络，可以使用程序化的方法来获取与 DHCPv6 服务器操作相关的数据。特别是，在理想状况下，使用 DHCPv6 能够获取有关 IPv6 地址和代理出的 IPv6 地址前缀的租约信息。例如，这种方法可以帮助网络边缘设备在网络中进行访问控制。这种能够以程序化的方式从 DHCPv6 服务器获取租约数据的能力，就称为租约查询。

本标准的侧重点在于对 DHCPv6 协议的扩展，以便相关设备以轻量和方便的方法，从 DHCPv6 服务器获取信息。该方法特别适用于那些已经能够支持 DHCPv6 消息的进程和设备。租约查询消息仅仅是一个查询消息，并不对 IPv6 地址或前缀，或者与之相关的绑定信息产生影响。

租约查询可以以下列查询方式进行：

## 1) 按 IPv6 地址查询

这种查询方式允许请求端向服务器请求，绑定了地址的或者被代理的地址前缀的客户端的租约信息。

## 2) 按客户端标识符查询

这种查询方式允许请求端向服务器请求在特定链路上的特定客户端，或一组与客户端存在连接的链路的租约信息。

在某些情况下，需要通过批量的 DHCPv6 地址租约查询来实现管理目的。一个批量租约查询客户端打开一个通向 DHCPv6 服务器的 TCP 连接，使用 DHCPv6 547 端口。这表明该租约查询客户端通过配置可以获得服务器的 IP 地址，并且具有可通过单播到达服务器的能力。批量租约查询没有指定中继。

在建立连接之后，请求端发送一条包含查询类型和它所感兴趣的连接数据的 LEASEQUERY 消息。服务器使用其中的查询类型和数据来鉴别相关的连接。为了支持某些查询类型，服务器可能需要保存额外的数据结构，用来根据特定的选项数据来定位连接（locate bindings）。服务器使用一条 LEASEQUERY-REPLY 消息作为回复，表明查询是成功还是失败。如果查询是成功的，服务器会把第一个客户端的连接数据也包含在 LEASEQUERY-REPLY 消息中。如果返回了多于一个的客户端的连接信息，则服务器会在一系列 LEASEQUERY-DATA 消息中发送额外的客户端连接信息。在服务器已经发送了至少一个客户端的连接信息的前提下，它会在发送完所有回复之后，发送一条 LEASEQUERY-DONE 消息。客户端可以再次利用建立的连接以发起额外的查询。TCP 连接的双方都可以在所有数据都发送完毕之后关闭该连接。

本标准包括了一种新的 DHCPv6 选项，即中继标识符(Relay-ID)选项。该选项包含一个 DUID(DHCP 唯一标识符)，用于标识一个 DHCPv6 中继代理。中继代理可以在它们发送的中继转发消息中加入这个选项。服务器可以保留中继标识符，并将其与以中继的客户端的名义建立的连接相关联。然后，中继可以通过在 LEASEQUERY 消息中使用中继标识符，恢复关于下游客户端的连接信息。

本标准还针对批量租约查询，定义了相关消息类型和查询类型：

## 1) 按中继标识符查询

这种查询方式要求服务器返回关于一个特定中继的连接；该中继由 Relay-ID 选项中携带的 DUID 来标识。



## 2) 按链路地址查询

该查询方式要求服务器返回一个特定网段中的连接；该网段的链路地址由查询消息中的链路地址字段（link-address field）来规定。

### 3) 按远程标识符查询

该查询方式要求服务器返回关于一个带有指定的远程标识符（Remote-ID[1]）的中继代理的连接。

## 5 租约查询

## 5.1 消息和选项定义

### 5.1.1 消息

LEASEQUERY (租约查询) 和 LEASEQUERY-REPLY (租约查询应答) 消息都使用在 YD/T 2296-2011 中描述的客户端/服务器消息格式。两条新的消息代码定义如下:

LEASEQUERY (14)——请求端可以发送 LEASEQUERY 消息到任何可用的 DHCPv6 服务器, 以获得其指定的客户端的租约信息。OPTION LO QUERY 中的选项组决定了该查询的性质。

LEASEQUERY-REPLY (15)——服务器通过发送包含指定客户端数据的 LEASEQUERY-REPLY 消息来响应 LEASEQUERY 消息。

### 5.1.2 查询选项

查询选项仅用在 LEASEQUERY 消息中，用来详细描述正在进行的查询。该选项的内容包含查询类型、链路地址（或 0::0）和其他该查询需要的数据。查询选项如图 1 所示。

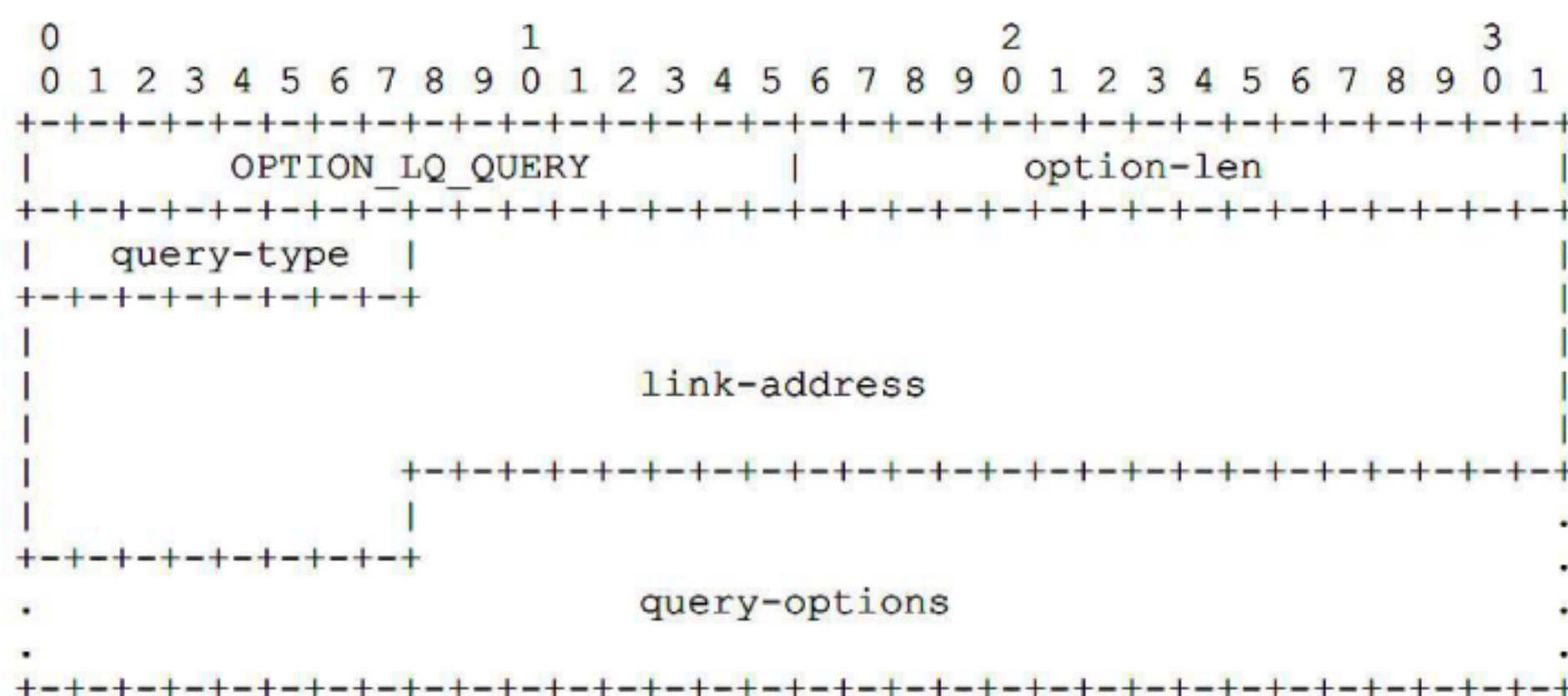


图 1 DHCPv6 租约查询选项格式

选项代码 (option-code): OPTION LQ QUERY (44)。

选项长度 (option-len): 17+查询选项组的长度。单位: 字节。

链路地址 (link-address): 一个提供给服务器用于标识该查询目标链路的全局地址, 如果未指定则使用 0::0。

查询类型 (query-type): 请求查询的类型。

查询选项组 (query-options): 与该查询相关的各个选项, 查询类型和必要的查询选项包括:

——按地址查询。

查询选项组中“必须”包含一个 `OPTION_IAADDR` 选项。如果 `OPTION_IAADDR` 选项中的地址空间不足，则在链路地址字段（link-address field），如果不是 `0::0`，规定目标客户端的链路地址。只有租用了



YD/T 3065-2016

特定地址或被指派了包含特定地址的前缀的客户端的信息被返回（如果相关信息可以获得）。

——按客户端标识符查询。

查询选项组中“必须”包含一个 `OPTION_CLIENTID` 选项。链路地址区域如果不是 `0::0`，则规定了目标客户端的链路地址。如果链路地址区域是 `0::0`，服务器“应该”搜索自身所有链路，以找到目标客户端。

查询选项组中还“可能”包含一个 `OPTION_ORO` 选项，用来指定请求端需要服务器返回的各个客户端的选项组。

如果服务器收到一条含有不支持的查询类型的 `OPTION_LQ_QUERY` 消息，服务器应该返回一个“未知查询类型”（UnknownQueryType）状态字。如果服务器收到合法的查询类型的消息，但该消息的查询选项组中缺失必要的选项，则服务器“应该”返回一个“查询格式错误”（MalformedQuery）状态字。

5.1.3 客户端数据选项

客户端数据选项用来在一条 `LEASEQUERY-REPLY` 消息中封装单一链路上的单一客户端的数据。客户端数据选项的格式如图 2 所示。

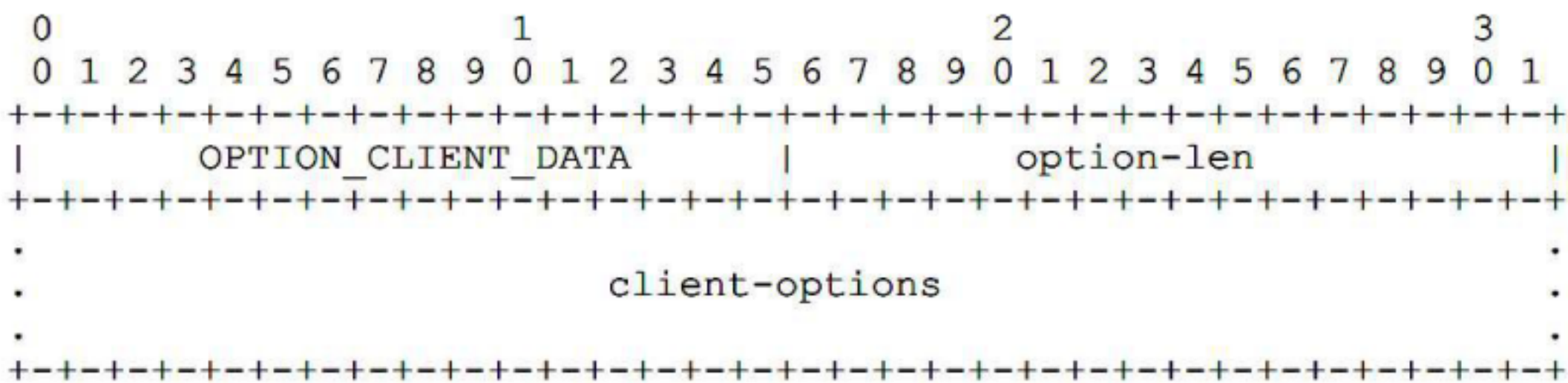


图 2 DHCPv6 客户端数据选项格式

选项代码（option-code）：`OPTION_CLIENT_DATA` (45)。

选项长度（option-len）：封装好的客户端选项组区域长度。单位：字节。

客户端选项组（client-options）：与客户端相关的各种选项。

封装好的客户端选项组包括客户端标识符选项（`OPTION_CLIENTID`）、链路地址选项（`OPTION_IAADDR`）、链路前缀选项（`OPTION_IAPREFIX`）、客户端最近事件处理时间选项（`OPTION_CLT_TIME`）以及其他针对特定客户端的特定选项，以及请求端在 `OPTION_LQ_QUERY` 的选项组中的 `OPTION_ORO` 选项中所请求的内容。服务器“必须”返回该链路上的客户端的全部赋值地址和指派的前缀。

5.1.4 客户端最近事务时间选项

客户端最近事务时间选项被封装在 `OPTION_CLIENT_DATA` 中，用来表示距离服务器上次与该客户端进行通信的时间，以秒为单位。客户端最近事件处理时间选项的格式如图 3 所示。

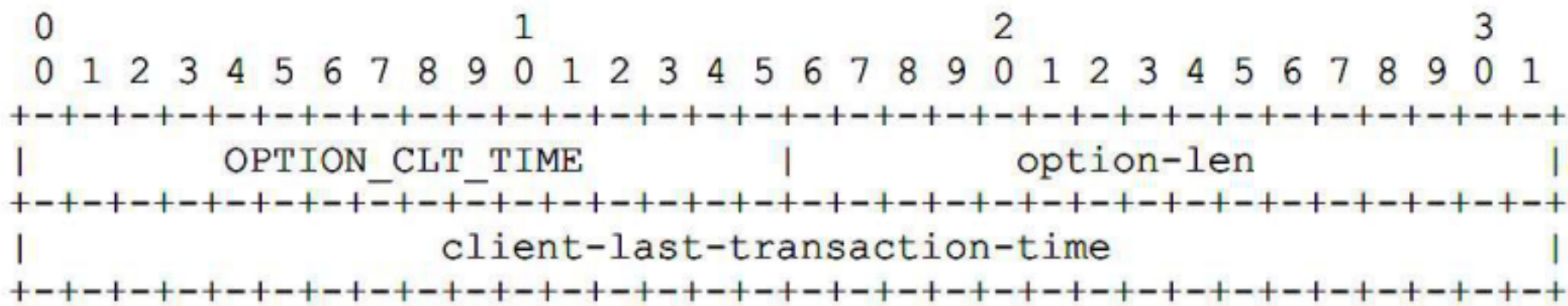


图 3 DHCPv6 客户端最近事件处理时间选项

选项代码（option-code）：`OPTION_CLT_TIME` (46)。



选项长度 (option-len): 4。  
客户端最近事件处理时间: 距离服务器上次与该客户端进行通信经历的时间, 以秒为单位。

5.1.5 中继数据选项

中继数据选项仅用在 LEASEQUERY-REPLY 消息当中, 用于提供客户端最近与服务器通信所用的中继代理的信息。中继数据选项的格式如图 4 所示。

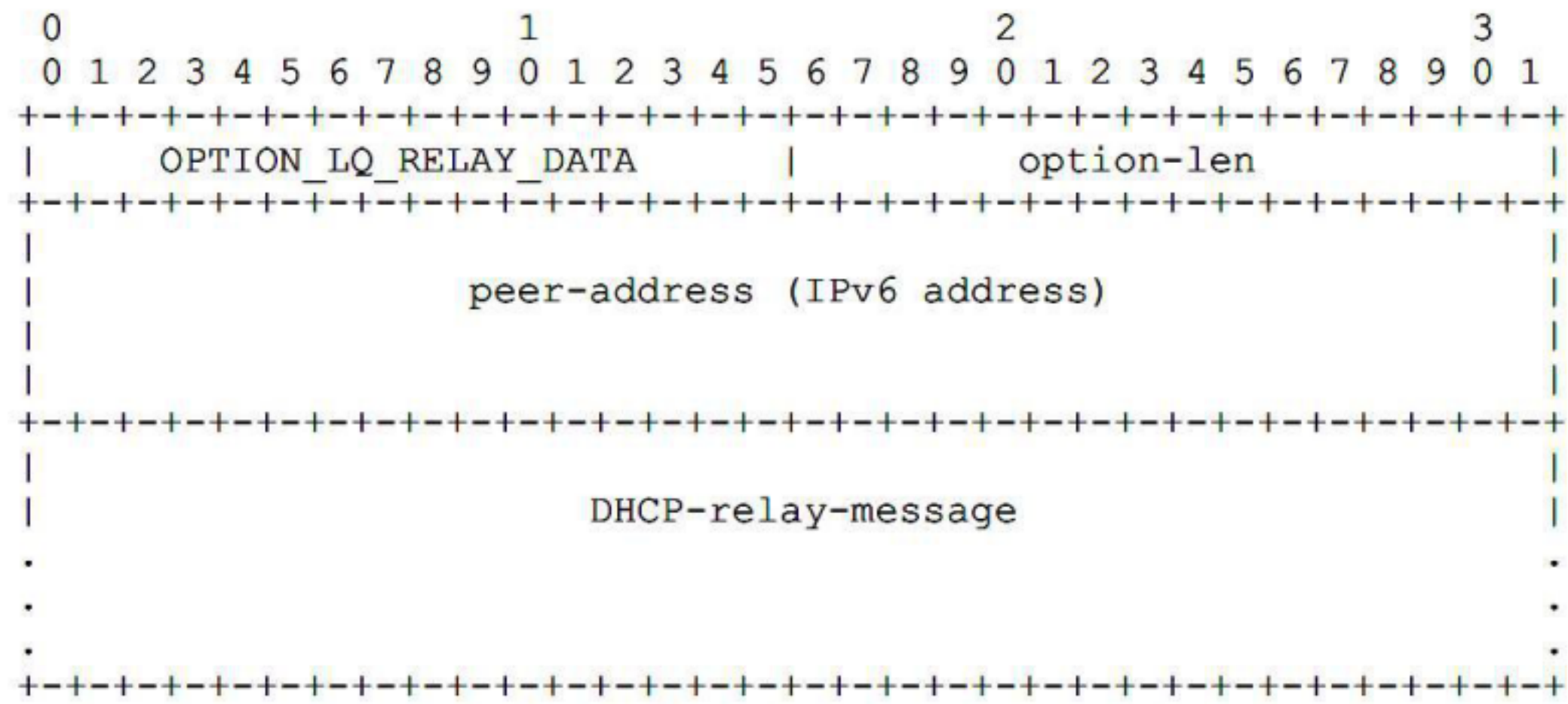


图 4 DHCPv6 中继数据选项格式

选项代码 (option-code): OPTION\_LQ\_RELAY\_DATA (47)。  
选项长度 (option-len): 16 +DHCP 中继信息长度。  
监视地址 (peer-address): 向服务器发送中继消息的源中继代理地址。  
DHCP 中继消息 (DHCP-relay-message): 最新的完整中继消息, 不包括服务器收到的客户端消息 (OPTION\_RELAY\_MSG)。

该选项被服务器用于返回完整的客户端中继代理信息。如果它不包含上述信息, 则“必须不能”作为返回值。其原因可能是该客户端直接与服务器通信 (不经过中继代理) 或者服务器未保存相关信息。

DHCP 中继消息如果被返回, 则它“必须”包含一个有效的 (有可能是反复变化的) RELAY-FORW 消息, 该消息是客户端最近发送给服务器的。但是, (最内部的) 包含客户端的消息的 OPTION\_RELAY\_MSG 选项“必须”被移除。该选项“应该”只在被 OPTION\_LQ\_QUERY 选项组中的 OPTION\_ORO 选项指定时才返回。

5.1.6 客户端链路选项

客户端链路选项仅在 LEASEQUERY-REPLY 消息中使用, 它标识一组与目标客户端有一个或多个连接的链路。该选项用来在未指定链路地址且目标客户端同时处于多个链路上的情况下响应一个查询。客户端链路选项的格式如图 5 所示。

选项代码 (option-code): OPTION\_LQ\_CLIENT\_LINK (48)。  
选项长度 (option-len): 链路列表的长度, 以字节为单位, 必须是 16 的倍数。  
链路地址 (link-address): 服务器用来标识目标客户端所在链路的全局地址。

当服务器响应一个根据客户端标识的查询时, 如果目标客户端同时处于多个链路上, 链路地址应被指定为 0::0。请求端可以对每个返回的链路地址再次重复查询, 以甄别返回的链路地址。如果目标客户端在一个单独链路上, 服务器“应该”在 OPTION\_CLIENT\_DATA 选项中返回客户端的数据。



YD/T 3065-2016

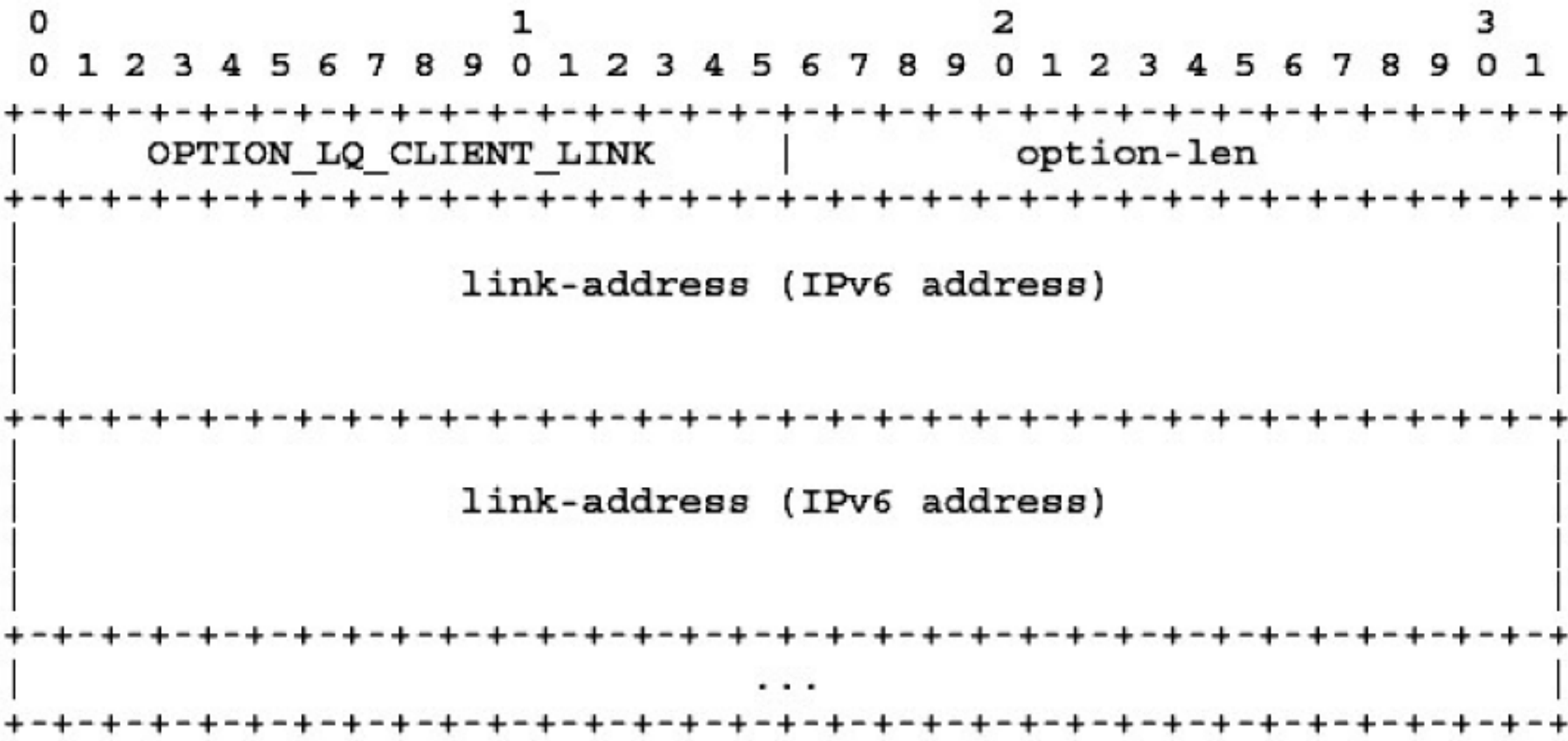


图 5 DHCPv6 客户端链路选项格式

5.1.7 状态字

本标准定义了新的状态字：

UnknownQueryType (7): 查询类别未知或者不被服务器支持。

MalformedQuery (8): 查询格式错误。举例来说，OPTION\_LQ\_QUERY 缺失了某项必要的选项。

NotConfigured (9): 服务器的配置文件中没有目标地址或链路。

NotAllowed (10): 服务器不允许请求端发起此次租约查询。

5.1.8 发送和重发参数

本条给出一个描述租约查询中的消息发送行为的表格。

参数	缺省值	描述
-----		
LQ_TIMEOUT	1 秒	初始租约查询超时时间
LQ_MAX_RT	10 秒	最大租约查询超时时间
LQ_MAX_RC	5	最大租约查询重试次数

5.2 消息验证

5.2.1 LEASEQUERY 消息

请求端和客户端“必须”丢弃任何接收到的 LEASEQUERY 消息。

满足下列任一条件时，服务器“必须”丢弃任何接收到的 LEASEQUERY 消息：

- 该消息中不包含 OPTION\_CLIENTID 选项；
- 该消息中包含 OPTION\_SERVERID 选项但是其内容与服务器的标识不符；
- 该消息中不包含 OPTION\_LQ\_QUERY 选项。

5.2.2 LEASEQUERY-REPLY 消息

满足下列任一条件时，请求端“必须”丢弃任何接收到的 LEASEQUERY-REPLY 消息：

- 该消息中不包含 OPTION\_SERVERID 选项；
- 该消息中不包含 OPTION\_CLIENTID 选项，或者 OPTION\_CLIENTID 选项的内容与请求端的

DUID 不符;

- 该消息中的“处理标识符”区与原消息中的值不符。

服务器和中继代理“必须”丢弃任何接收到的 LEASEQUERY-REPLY 消息。

### 5.3 DHCPv6 租约查询请求端行为

#### 5.3.1 概述

5.3 描述请求端如何向一个 DHCPv6 服务器发起一个租约数据检索。

#### 5.3.2 创建 LEASEQUERY 消息

请求端将 LEASEQUERY 消息的“消息类型”区置位。请求端生成一个处理标识符,并将其填入“处理标识符”区。

请求端“必须”包含一个 OPTION\_CLIENTID 选项以让服务器识别自己。

请求端“必须”包含一个 OPTION\_LQ\_QUERY 选项,并设置适合的查询类型、链路地址和查询选项组。

如果该租约查询请求希望获得特定服务器的响应、却又无法使用单播,则请求端“应该”包含一个 OPTION\_SERVERID 选项。

#### 5.3.3 LEASEQUERY 消息的传输

请求端“可能”被配置为使用一系列目标地址,这些地址“可能”包含单播地址、All\_DHCP\_Servers 多播地址或者其他被网络管理员选定的地址。如果请求端没有被明确的配置,它“可能”默认使用 All\_DHCP\_Servers 多播地址。

请求端“应该”向一个或多个已知拥有关于查询目标的权威信息的 DHCPv6 服务器发送 LEASEQUERY 消息。

如果缺乏可能拥有关于查询目标的权威信息的 DHCPv6 服务器的相关信息,请求端“应该”向所有已知的或经过配置的 DHCPv6 服务器发起查询。例如,请求端“可能”发送 LEASEQUERY 消息到 All\_DHCP\_Servers 多播地址。

请求端按 YD/T 2296-2011 第 14 章中描述的规则传输 LEASEQUERY 消息,使用下列参数:

IRT: LQ\_TIMEOUT  
MRT: LQ\_MAX\_RT  
MRC: LQ\_MAX\_RC  
MRD: 0

如果消息交互失败,请求端按请求端本地规则来执行行动。请求端可能执行的行动的例子包括:

- 从请求端已知服务器列表中选择另一服务器;
- 按照 All\_DHCP\_Servers 地址发送多播消息到多个服务器;
- 中止该请求。

#### 5.3.4 LEASEQUERY-REPLY 消息的接收

一个成功的 LEASEQUERY-REPLY 消息不包含 OPTION\_STATUS\_CODE 选项(或者 OPTION\_STATUS\_CODE 选项的内容为成功状态字)。以下是它的三种变体:

a) 如果一个服务器与目标客户端间相连,则该消息包含一个 OPTION\_CLIENT\_DATA 选项。请求端从 LEASEQUERY-REPLY 消息中提取客户端的数据并据此更新其信息数据库。如果 OPTION\_CLIENT\_DATA 选项中不包含 OPTION\_CLT\_TIME 选项,那么请求端“应该”丢弃该



OPTION\_CLIENT\_DATA 选项。

b) 如果服务器通过多条链路与目标客户端的相连, 则该消息包含一个 OPTION\_CLIENT\_LINK 选项。此时请求端需要向返回的每个链路地址再次发送 LEASEQUERY 消息, 以确定客户端的连接信息。

c) 如果该服务器与目标客户端之间没有连接, 则 OPTION\_CLIENT\_DATA 和 OPTION\_CLIENT\_LINK 选项都不会出现。

一条不成功的 LEASEQUERY-REPLY 消息是在 OPTION\_STATUS\_CODE 选项中包含错误代码的。按照不同的错误代码, 请求端可以尝试向不同的服务器发送请求 (例如 NotAllowed、NotConfigured, 和 UnknownQueryType), 尝试发送不同的或改正后的查询请求 (例如 UnknownQueryType 和 MalformedQuery), 或者终止该查询。

### 5.3.5 处理来自多个源的 DHCPv6 数据

请求端有可能从同一 DHCPv6 服务器接收关于同一客户端的, 响应不同类型 LEASEQUERY 消息的租约数据。如果一条 LEASEQUERY 消息发送给了多个服务器, 则请求端可能会从几个服务器接收到关于同一客户端的租约数据。本条描述了请求端如何处理从同一服务器得到的关于同一 DHCPv6 客户端的多个租约数据源。

从不同数据源得到客户端数据有可能是脱节的或者交叠的。脱节和交叠的情况会发生在来自同一服务器的数据或者来自不同服务器的数据之间。

如果来自两个数据源的关于同一客户端的数据有不同类型的值, 则称这些数据是“脱节”的。数据类型不同的例子是, 请求端从一个服务器收到一个 IPv6 地址租约, 而从另一个服务器收到一个前缀租约, 两份租约都是分配给同一个客户端的。数据的值不相符 (但都属于同一类型) 的例子是, 请求端从两个不同的服务器收到同一客户端的两个 IPv6 地址租约, 但是两份租约的 IPv6 地址不同。如果请求端从不同的数据源接收到脱节的客户端数据, 则“应该”将它们合并在一起。

如果来自两个不同数据源的同一客户端数据拥有相同的数据类型和数值, 则称这些数据是交叠的。数据交叠的例子是, 请求端从两个不同的服务器接收到一个相同的 IPv6 地址租约。交叠的客户端数据又称为冲突数据。

请求端“应该”使用 OPTION\_CLT\_TIME 选项来解决来自不同服务器的数据冲突, 且“应该”接受 OPTION\_CLT\_TIME 选项中最新的一个数据。

## 5.4 DHCPv6 租约查询服务器行为

### 5.4.1 概述

DHCPv6 服务器发送 LEASEQUERY-REPLY 消息, 以响应其接收到的合法的 LEASEQUERY 消息, 返回赋值地址、指派的前缀以及其他与此查询相匹配的其他信息。

### 5.4.2 LEASEQUERY 消息的接收

在合法的 LEASEQUERY 消息的回复中, DHCPv6 服务器找到目标客户端的位置, 收集该客户端上的数据, 构建并返回一个 LEASEQUERY-REPLY 消息。LEASEQUERY 消息不能用来分配、释放或更改连接或配置信息。

服务器通过将“信息类型 (msg-type)”字段置位来构建 LEASEQUERY-REPLY 信息, 并从 LEASEQUERY 消息中复制处理标识符到处理标识符区。

如果 OPTION\_LQ\_QUERY 选项中的查询类型是未知的或者是不支持的类型, 服务器则会增加一个

OPTION\_STATUS\_CODE 选项，并在其中填入 UnknownQueryType 状态字，然后发送 LEASEQUERY-REPLY 消息给请求端。如果查询选项组中不包含描述查询类型所必须的选项，服务器则会增加一个 OPTION\_STATUS\_CODE 选项，并在其中填入 MalformedQuery 状态字，然后发送 LEASEQUERY-REPLY 消息给请求端。

服务器也可能限定 LEASEQUERY 消息或某些查询类型来自特定的请求端。这种情况下，服务器“可能”丢弃该 LEASEQUERY 消息，也“可能”会增加一个 OPTION\_STATUS\_CODE 选项，并在其中填入 NotAllowed 状态字，然后发送 LEASEQUERY-REPLY 消息给请求端。

如果 OPTION\_LQ\_QUERY 选项指定了一个非零的链路地址，则服务器“必须”使用该地址来给目标客户端寻找适当的链路。对于按地址查询的情况来说，如果指定链路地址为 0::0，服务器则会使用 OPTION\_IAADDR 选项中的地址来给目标客户端寻找适当的链路。在上述两种情况下，如果服务器无法找到合适的链路，它“应该”返回一个 OPTION\_STATUS\_CODE 选项，并在其中填入 NotConfigured 状态字，然后发送 LEASEQUERY-REPLY 消息给请求端。

对于按客户端标识符查询的情况来说，如果指定链路地址为 0::0，服务器则“必须”在所有链路上查询目标客户端。如果目标客户端仅在一条链路上被发现，则服务器“应该”在 OPTION\_CLIENT\_DATA 选项中返回目标客户端的数据。如果目标客户端在多条链路上被发现，则服务器“必须”在 OPTION\_CLIENT\_LINK 选项中返回符合条件的链路的列表。此时，服务器“必须不”返回任何目标客户端数据。否则，服务器使用 OPTION\_LQ\_QUERY 选项中的数据来发起一个查询。该查询的结果可以是 0 或者是一个客户端，然后导致 0 或者一个 OPTION\_CLIENT\_DATA 选项被加入 LEASEQUERY-REPLY 消息中。

#### 5.4.3 构建客户端的 OPTION\_CLIENT\_DATA 选项

LEASEQUERY-REPLY 消息中的 OPTION\_CLIENT\_DATA 选项“必须”最少包含以下选项：

- 客户端标识符选项 (OPTION\_CLIENTID)
- 链路地址选项 (OPTION\_IAADDR) 和/或链路前缀选项 (OPTION\_IAPREFIX)
- 客户端最近事件处理时间选项 (OPTION\_CLT\_TIME)

根据目标客户端与链路间的连接类型不同，链路地址选项 (OPTION\_IAADDR) 或者链路前缀选项 (OPTION\_IAPREFIX) 会出现其一，或两个选项都出现。

OPTION\_CLIENT\_DATA 选项“应该”包含 LEASEQUERY 消息中 OPTION\_LQ\_QUERY 选项中的 OPTION\_ORO 所请求的那些选项。另外，基于“敏感选项组 (sensitive options)”列表来返回也是可以接受的，具体在下面讨论。

DHCPv6 服务器“应该”可以“按敏感选项组 (sensitive options)”列表来进行配置，当在 LEASEQUERY 消息中 OPTION\_LQ\_QUERY 选项中的 OPTION\_ORO 中被指定时，该列表必须不能被返回。该列表中的任何选项“必须不”能被返回给请求端，即使在被请求端请求的情况下。

#### 5.4.4 LEASEQUERY-REPLY 消息的传输

服务器按照 YD/T 2296-2011 中 17.2.3 的规定来发送 LEASEQUERY-REPLY 消息。

### 5.5 安全考量

普通的租约查询的请求端，应尽可能是连接集中器。使用 DHCPv6 收集、按 LEASEQUERY 消息的内容刷新的连接集中器，将能保持最准确的客户端/连接信息。这保证了连接集中器能够在宽带网络中转



发数据流量信息给其计划目的地，能够执行来自接入网络的数据报的 IPv6 源地址校验，还能够加密网络流量，仅让指定的调制解调器对其解密。因此，租约查询能力使连接集中器具有相对增强的安全性。

YD/T 2296-2011 的第 24 章规定了 DHCPv6 的大体安全威胁，这些威胁也对于 LEASEQUERY 消息也是等效的。YD/T 2296-2011 中第 21 章规定了中继代理与服务器之间，以及客户端与服务器之间的安全通信过程。如果请求端是一个连接集中器，YD/T 2296-2011 规定基于互联网协议的安全协议应被使用。其他类型的请求端本质上都是 DHCPv6 客户端。因此，YD/T 2296-2011 中 DHCPv6 身份验证是一种适宜安全处理 LEASEQUERY 和 LEASEQUERY-REPLY 消息的机制。鉴于在管理域中，租约查询请求端和服务器的数量相对较小，任何发布共享密钥带来的问题都会被弱化。

在实施上述措施的基础上，DHCPv6 服务器还应只与受信的 LEASEQUERY 请求端通信，这样应该能到达既定安全需求。

不是所有的网络流量都是由这些受信的请求端直接发起的。例如，受信的中继代理可以中继来自非受信请求端或者网络中其他地方的 LEASEQUERY 消息。因此，“应该”至少对网络边缘的中继代理（或者所有中继代理，除非其中继的 LEASEQUERY 消息是某些请求端所必需的）阻止上述操作。DHCPv6 服务器“可能”被配置成丢弃所有通过中继的 LEASEQUERY 的消息或者限制中继转播。

DHCPv6 服务器还“应该”具有限制 LEASEQUERY-REPLY 消息中的客户端信息返回租约查询请求端的能力，即使该请求端是受信的。

由于即使是受信的连接集中器也可能因为其外部活动的影响而生成 LEASEQUERY 请求，所以连接集中器“应该”通过最小化 LEASEQUERY 消息的生成来最小化对 DHCPv6 服务器的潜在“拒绝服务攻击（denial-of-service attack）”。需要特别说明的是，连接集中器“应该”使用“负缓存（negative caching）”（例如，缓存某个近期未能返回目标客户端数据的查询），并尽可能的使用地址限制（例如，不向超出宽带网络接入范围的地址发送 LEASEQUERY 消息）。总的来说，这些机制限制了连接集中器，在一次重新启动事件之后，发送 LEASEQUERY 消息（不包括重试的消息），每个合法的宽带连接地址一次。

数据包洪泛（Packet-flooding）式拒绝服务攻击（denial-of-service attack）可能导致处理资源耗尽，致使服务器不能向合法的和常规的 DHCPv6 客户端，以及合法的 DHCPv6 租约查询请求端提供服务、拒绝合法的 DHCPv6 客户端配置和合法的 DHCPv6 租约查询请求端的信息。如果仅仅与受信的租约查询请求端通信的情况下，上述攻击则不容易发生。在受信权错误下放，安全技术被放弃，或者甚至受信的请求端中存在漏洞的情况下，受攻击的可能性总是存在的。因此，防御数据包洪泛式拒绝服务攻击的技术总是不错的选择，如同早前提到的，这些技术同时提供不错的边缘安全性，并限制通过中继代理、其他网络部件甚至是服务器自身的 DHCPv6 网络流量。

有一种攻击作为租约查询请求端的连接集中器（而不是 DHCPv6 服务器）的方法是，建立一个意图向连接集中器提供错误租约或者路由信息恶意服务器，以阻挠 IPv6 源地址校验并阻止正确的路由。这种类型的攻击的威胁可以使用 YD/T 2296-2011 规定的互联网协议安全协议来抵御。

## 6 批量租约查询

### 6.1 概述

批量租约查询可以看作是已经存在的 UDP 租约查询协议的一个扩展。

### 6.2 消息和选项的定义

#### 6.2.1 面向 TCP 的消息帧



批量租约查询协议使用 TCP 以允许一个或多个 DHCPv6 消息在同一时间发送。接收器需要能够分辨每个消息的长度。包含消息长度的两个位组按网络字节顺序（network byte order），被预制在每条通过批量租约查询的 TCP 连接发送的 DHCPv6 消息中。两个位组的消息大小（message-size）作为每条 DHCPv6 消息的帧头。使用 TCP DHCPv6 消息的帧结构如图 6 所示。

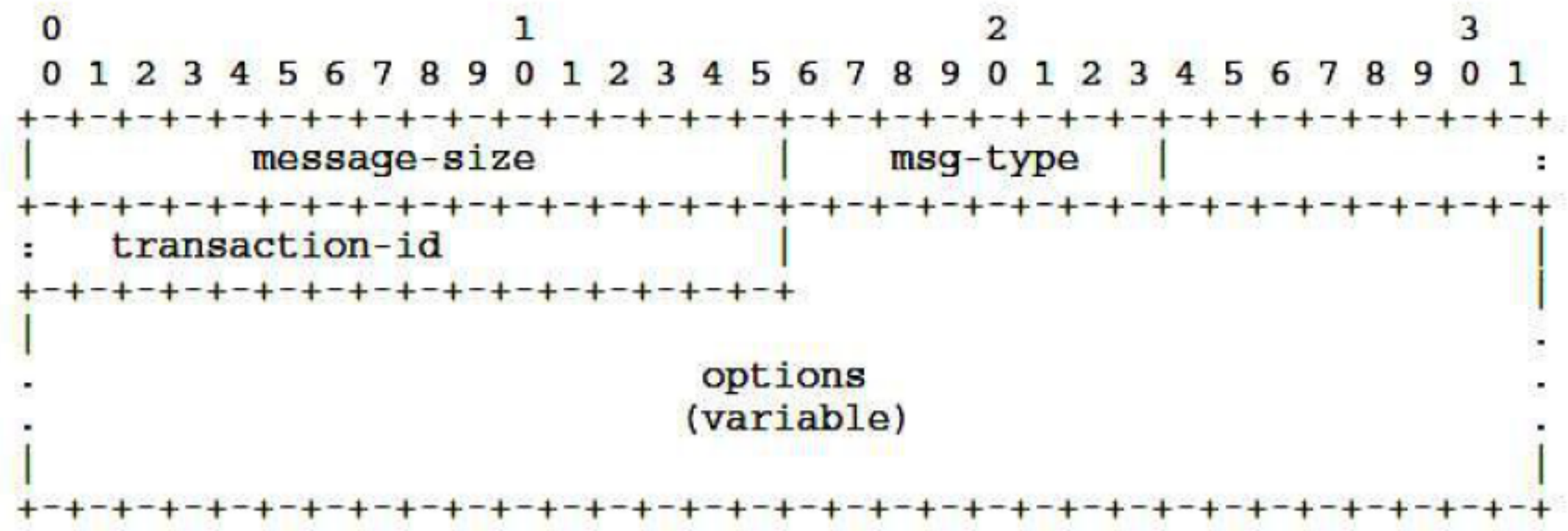


图 6 使用 TCP 承载的 DHCPv6 消息

消息大小（message-size）：消息中的字节数，以 16 位整数网络字节的顺序排列。

其他相关区域的内容见 YD/T 2296-2011。

### 6.2.2 消息

在批量租约查询交互中，单个 LEASEQUERY-REPLY 消息被用来表示一个查询是成功还是失败，同时承载不改变单一查询应答过程上下文的数据，比如服务器标识符和客户端标识符选项。如果一个查询是成功的，只“必须”有一个单一的 LEASEQUERY-REPLY 消息。如果服务器还返回了连接数据，LEASEQUERY-REPLY 消息还应在 OPTION\_CLIENT\_DATA 选项中包含第一个客户端的连接数据。

LEASEQUERY-DONE 消息——LEASEQUERY-DONE 消息承载关于单一 DHCPv6 客户端的租约数据和/或单一链路的前缀指派连接信息。使用该消息的目的是在多个连接数据被发送时减少多余数据。在发送 LEASEQUERY-DONE 消息之前“必须”发送 LEASEQUERY-REPLY 消息。LEASEQUERY-REPLY 消息承载查询的状态、租约查询的目标客户端标识符和服务器标识符选项，以及第一个客户端的连接数据和该查询是否成功。LEASEQUERY-DONE 消息“必须”“仅仅”用于回复一个成功的 LEASEQUERY 消息，而且仅当多于一个客户端的数据需要发送时使用。LEASEQUERY-DONE 消息中的处理标识符区“必须”与 LEASEQUERY 请求消息中的处理标识符区相匹配。服务器标识符、客户端标识符和 OPTION\_STATUS\_CODE 选项“不应该”包括在内，因为批量租约查询的回复中的数据必须是一个常量，并且应该在 LEASEQUERY-REPLY 消息中传输。

LEASEQUERY-DONE 消息——LEASEQUERY-DONE 消息表示一组与租约查询相关的消息的结束。LEASEQUERY-DONE 消息的处理标识符区“必须”与 LEASEQUERY 请求消息中的处理标识符区相匹配。该消息的出现是一系列回复消息结束的信号。单个 LEASEQUERY-DONE 消息“必须”在其他所有回复（一个成功的 LEASEQUERY-REPLY 消息以及 0 个或多个 LEASEQUERY-DONE 消息）后被发送，这些回复返回至少一个连接数据以响应一次成功的批量租约查询请求。服务器可能在开始发送 LEASEQUERY-REPLY 消息后，遇到错误的发生。在这种情况下，“应该”尝试发送一个带 OPTION\_STATUS\_CODE 选项的 LEASEQUERY-DONE 消息，用来向请求端表示错误的情况。其他的 DHCPv6 选项则“不应该”被包括在 LEASEQUERY-DONE 之内。



6.2.3 查询类型

DHCPv6 批量租约查询引入新的查询类型：按中继标识符查询（QUERY\_BY\_RELAY\_ID）、按链路地址查询（QUERY\_BY\_LINK\_ADDRESS）和按远程标识符查询（QUERY\_BY\_REMOTE\_ID）。这些查询方式是设计用来帮助中继代理在丢失部分或全部数据的状况下恢复数据的。

1) 按中继标识符查询（QUERY\_BY\_RELAY\_ID）

这种查询方式要求服务器返回关于一个特定中继 DUID 的连接。

按中继标识符查询：查询选项组“必须”包含一个 OPTION\_RELAY\_ID 选项。如果链路地址区域为 0::0，则该查询要求返还与指定中继 DUID 相关所有连接。如果链路地址区域被指定，该查询要求返还指定链路上的连接。

2) 按链路地址查询（QUERY\_BY\_LINK\_ADDRESS）

按照链路地址查询方式要求服务器返回一个由中继的中继转发（Relay-Forward）消息中的链路地址区域（link-address field）来规定的网段中的所有连接。

按链路地址查询：查询信息中的链路地址包含一个中继在中继转发信息中的链路地址区域中使用过的地址。服务器会尝试定位链路地址（link-address）所在的网段中的所有连接。

3) 按远程标识符查询（QUERY\_BY\_REMOTE\_ID）

该查询方式要求服务器返回，一个关于出现在中继的“中继转发消息”中的远程标识符（Remote-ID）选项的连接。其查询选项组中“必须”包含一个中继代理远程标识符选项。为了支持该查询类型，服务器需要记录从中继转发消息中找到最近的远程标识符选项值和与其相关的其他连接数据。

按远程标识符查询：查询选项组中“必须”包含一个中继代理远程标识符选项。如果服务器已经记录了远程标识符的值以及其连接，则用该选项的值标识的连接作为返回值。

6.2.4 中继标识符选项

中继标识符选项承载着 DHCP 唯一标识符（DUID）。中继代理“可能”将该选项包含在其发送的中继转发消息中。很明显，除非在该选项中包含了中继代理的信息，否则服务器不可能响应这个按中继标识符查询。中继“应该”能够为此目的生成一个 DUID 并稳定的存储起来。中继还“应该”允许该 DUID 的值是可配置的：这样做可以允许管理员在保持中继和已存在的 DHCPv6 连接之间关系不变的条件下，替换中继代理。

DHCPv6 服务器“可能”将从中继转发消息中截取的中继标识符选项与前缀指派和/或租约连接联系起来。这样做即可响应一个按中继标识符的租约查询。中继标识符选项的格式如图 7 所示。

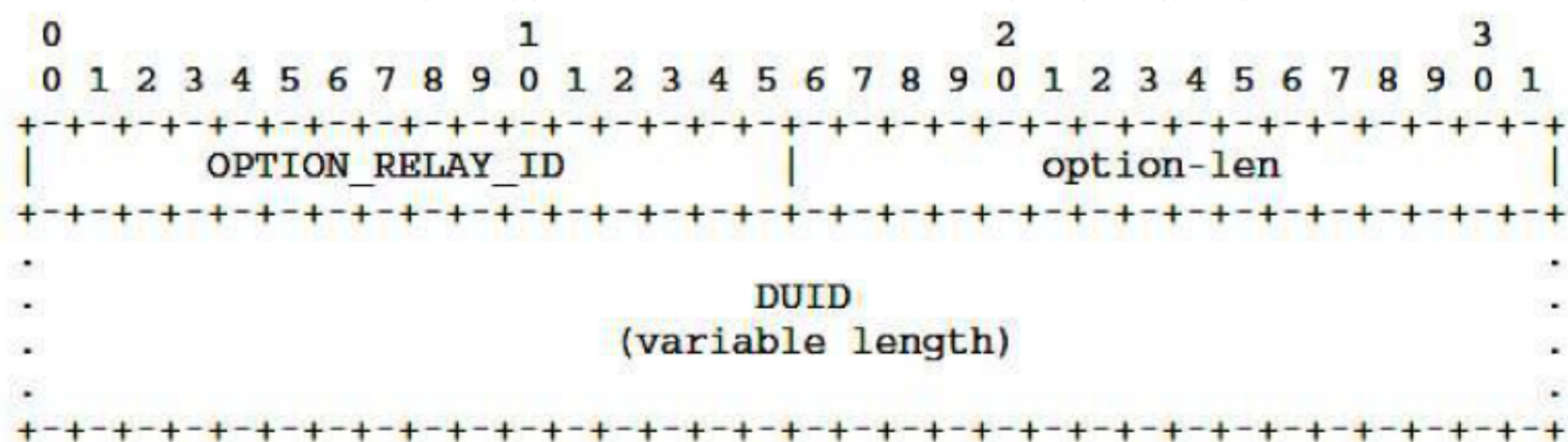


图 7 DHCPv6 中继标识符选项

选项代码（option-code）：OPTION\_RELAY\_ID。

选项长度（option-len）：DUID 的长度，以字节为单位。



DUID：中继代理的 DHCP 唯一标识符。

6.2.5 状态字

查询中止 (QueryTerminated)：表示服务器不能执行该查询或者因某些原因（应该在该消息的文本中被告知）在早期中止了该查询。这有可能是因为服务器的资源不足或者正被关闭。请求端可以在晚些时候重试查询，重试查询前至少应该等待一小段时间。注意，服务器在早期关闭连接的情况下，最好发送一个带有状态字的 LEASEQUERY-REPLY 或 LEASEQUERY-DONE 消息，以告知请求端发生的状况。

6.2.6 连接和传输参数

支持批量租约查询的 DHCPv6 服务器“应该”监听 DHCPv6 服务器 547 端口上的上行的 TCP 连接。具体实现中“可能”把监听的上行端口设置为可配置的，不过 547 端口“必须”设置为缺省值。客户端的具体实现“应该”与 547 端口建立 TCP 连接，“可能”把目标服务器端口设置为可配置的。

在本小节中提供了用于控制批量租约查询行为的参数表，具体实现中“可能”将这些数值设置为可配置的。不过，配置太小的超时时间可能会导致对本应用和其他网络流量的有害行为。因此，“不推荐”使用比缺省值更小的超时时间值。

参数	缺省值	描述
BULK_LQ_DATA_TIMEOUT	300 s	批量租约查询数据超时时间
BULK_LQ_MAX_CONNS	10	最大租约查询 TCP 连接数

6.3 请求端行为

6.3.1 连接和传输参数

请求端会尝试与 DHCPv6 服务器建立 TCP 连接，以初始化一个租约查询交互。如果该尝试失败，请求端“可能”会重试尝试。

6.3.2 发起查询

在连接建立之后，请求端构建一个租约查询消息。该查询可能是以任意先前定义的查询类型进行的，并包含选定的查询类型所要求的选项组和数据。

如果该 TCP 连接在请求端发送查询的过程中被阻断或不再处在可写状态，查询端“应该”准备好在超时时间 (BULK\_LQ\_DATA\_TIMEOUT) 后中止该连接，以允许请求端控制他们在放弃一个连接前想等待的时间，该时间独立于它们使用的 TCP 具体实现给出的通知。

6.3.3 处理回复

请求端尝试从 TCP 连接中获取 LEASEQUERY-REPLY 消息。如果该 TCP 连接停止传输返回数据（该连接不再处于可读状态），请求端“应该”准备好在超时时间 (BULK\_LQ\_DATA\_TIMEOUT) 后中止该连接，并“可能”在被配置为失败后重试时，开始重试过程。

请求端检验收到的 LEASEQUERY-REPLY 消息，并决定如何处理。不包含 OPTION\_CLIENT\_DATA 选项的，成功的回复表示目标服务器没有找到与查询匹配的连接。

注意：租约查询协议使用 OPTION\_CLIENT\_LINK 选项作为单一查询是否返回多个连接结果的指示器。对于批量租约查询来说，不使用 OPTION\_CLIENT\_LINK 选项，因此它一定不能出现在回复中。

成功的 LEASEQUERY-REPLY 消息返回的连接数据，包括一个 OPTION\_CLIENT\_DATA 选项，还可能包括其他额外选项。如果还有额外的连接需要返回，则会承载在 LEASEQUERY-DATA 信息中。每个



LEASEQUERY-DATA 信息包含一个 OPTION\_CLIENT\_DATA 选项, 以及可能的其他额外选项。不包含 OPTION\_CLIENT\_DATA 选项的 LEASEQUERY-DATA 信息“必须”被丢弃。

单个批量查询可以收到大量的回复。举例来说, 单个中继代理可能负责几千个客户端的指派前缀的路由。请求端“必须”准备好接收多个与 LEASEQUERY 消息的处理标识符相匹配的 LEASEQUERY-DATA 消息。

LEASEQUERY-DONE 消息结束一次成功的、至少返回一个连接信息的批量租约查询请求。一条没有任何连接信息的 LEASEQUERY-REPLY 消息“必须不”能跟随一条含有相同处理标识符的 LEASEQUERY-DONE 消息。在从服务器接收到 LEASEQUERY-DONE 消息之后, 请求端“可能”关闭其与该服务器间的 TCP 连接。如果 LEASEQUERY-DONE 消息中的处理标识符与 LEASEQUERY 消息中的不匹配, 客户端“必须”关闭该 TCP 连接。

在满足以下条件之一时, 批量租约查询的回复即告完成 (例如, 没有接收到更多的具有匹配处理标识符的消息):

- 如果接收到的 LEASEQUERY-REPLY 消息没有 OPTION\_CLIENT\_DATA 选项;
- 如果接收到的 LEASEQUERY-REPLY 消息包含 OPTION\_CLIENT\_DATA 选项, 然后接收到 LEASEQUERY-DONE 消息;
- TCP 连接被关闭。

#### 6.3.4 查询多个服务器

一个批量租约查询客户端“可能”被配置为尝试并行连接并查询多个 DHCPv6 服务器。

#### 6.3.5 向单一服务器进行多次查询

批量租约查询客户端可能需要进行多次查询以恢复连接信息。一个请求端“可能”使用单一连接来进行多次查询。每个查询“必须”有一个唯一的处理标识符。服务器“可能”同时处理几个查询, 进行上述操作的服务器“可能”在其发送的一系列回复中, 交错回复这些查询, 因此客户端操作需要清楚多个查询的回复信息可能是交叠在一起的。不能处理这些交叠在一起的回复 (基于处理标识符) 的客户端, “必须不”能同时发起多个查询。请求端应该清楚服务器并不必须并行处理这些查询, 而且服务器倾向于限制自身处理来自单一请求端的查询的速率。

#### 6.3.6 关闭连接

请求端“可能”在向服务器发送 LEASEQUERY 消息之后从自己这端关闭 TCP 连接。请求端也“可能”选择保留连接, 如果它还想发起额外的查询。这类客户端行为并不保证连接可以保持到发送完额外的查询: 服务器可能会根据自己的配置, 决定关闭连接。

### 6.4 服务器行为

#### 6.4.1 接受连接

采用 DHCPv6 批量租约查询的服务器监听上行的 TCP 连接。服务器“必须”能够限制同时接受的活跃连接数。BULK\_LQ\_MAX\_CONNS 的值必须有缺省值; 在具体实现中“可能”允许该数值可配置。

服务器“可能”限制特定客户端才能进行批量租约查询的连接和发送 LEASEQUERY 信息。那些不是来自允许的客户端的连接“应该”立即关闭, 以避免服务器的连接资源耗尽。服务器也“可能”限制某些客户端只能使用某几种查询方式。服务器“可能”以 NotAllowed 状态字来回复不允许的查询, 并且/或者关闭该连接。

如果在服务器接收一个连接或者读取一个查询的时候 TCP 连接被堵塞，服务器“应该”准备好在 BULK\_LQ\_DATA\_TIMEOUT 之后中止该连接。建议允许服务器控制其等待一个不活跃的连接的时间，独立于其所用 TCP 实现形式。

#### 6.4.2 构建回复

6.2.2 描述了在承载多个连接数据时 LEASEQUERY-REPLY 消息和 LEASEQUERY-DATA 消息的使用。TCP 帧结构和消息传输见 6.2。如果连接在服务器尝试发送回复信息时被阻塞，服务器“应该”准备好在 BULK\_LQ\_DATA\_TIMEOUT 之后中止该连接。

如果服务器在开始查询处理时遇到了错误，在发送任何回复之前，它“应该”发送一个在 OPTION\_STATUS\_CODE 选项中包含错误代码的 LEASEQUERY-REPLY 消息。这就向请求端表示不会有返回数据。如果服务器在查询处理过程中遇到了错误，已经发送了一条或多条回复消息，则服务器“应该”在其方向关闭连接，表示它无法完成查询的处理。

如果服务器没有找到任何满足查询的连接，它“应该”发送一条不含 OPTION\_STATUS\_CODE 选项且不含 OPTION\_CLIENT\_DATA 选项的 LEASEQUERY-REPLY 消息。否则，服务器在每条回复中发送一个连接的信息。第一条回复信息应该是 LEASEQUERY-REPLY 消息。连接数据承载在 OPTION\_CLIENT\_DATA 选项中。服务器在 LEASEQUERY-DATA 消息中返回随后的连接数据，这样可以避免多余的数据（例如请求端的客户端标识符）。

对于按中继标识符查询，服务器按查询的中继标识符与目标连接的关系来定位各个连接。为了给按中继标识符查询以有意义的回复，服务器必须能够在 DHCPv6 连接数据中保存这种联系。如果该查询的链路地址没有设置为 0::0，服务器只需回复在包含该地址的链路上的连接。如果链路地址不是 0::0 而且服务器找不到任何匹配的链路，服务器“应该”在返回的 LEASEQUERY-REPLY 消息中加入 NotConfigured 状态字。

对于按远程标识符查询，服务器按查询中的中继远程标识符来定位阈值相关联的各个连接。为了给按远程标识符查询以有意义的回复，服务器必须能够在连接数据库中保存这种联系。如果该查询的链路地址没有设置为 0::0，服务器只需回复在包含该地址的链路上的连接。如果链路地址不是 0::0 而且服务器找不到任何匹配的链路，服务器“应该”在返回的 LEASEQUERY-REPLY 消息中加入 NotConfigured 状态字。

服务器按 6.2.2 小节中规定，发送 LEASEQUERY-DONE 消息。

#### 6.4.3 多重查询或并行查询

如 6.3.5 节，如果请求端需要进行多重查询，请求端可能希望保持一个已存在的连接。服务器“可能”支持读取并处理来自单一连接的多重查询。服务器从一个连接读取的查询数量，“必须不”能大于服务器准备同时处理的查询数量。

这“可能”成为一个由管理员控制的特性。能够并行处理多个查询的服务器，“应该”提供限制允许同时处理的，来自单个请求端的，查询数量的配置项，以在多个请求端寻求该服务的情况下，控制资源的使用。

#### 6.4.4 关闭连接

在发送完响应一次查询的最后一条消息之后（一条 LEASEQUERY-REPLY 消息或者 LEASEQUERY-DONE 消息），服务器“可能”从服务器端关闭 TCP 连接。或者，服务器“可能”保持该连接

并等待来自对应客户端的额外查询。服务器“应该”准备好限制其保持的连接的数量，并“应该”准备好为了执行这一限制，关闭闲置的连接。

如果服务器在 TCP 连接上发送数据时遇到了错误，服务器“必须”从服务器端关闭此连接。如果服务器发现必须放弃一个正在处理的请求，服务器“必须”从服务器端关闭此 TCP 连接。服务器放弃一个正在处理的请求时，“可能”会尝试用 QueryTerminated 状态字来通知客户端。如果服务器检测到客户端关闭了连接，服务器“必须”在完成处理任意来自客户端的外部请求后，从服务器端关闭连接。

## 6.5 安全考量

TCP 连接的使用引入了一些额外的担心。尝试耗尽 DHCPv6 服务器可用的 TCP 连接资源的攻击，诸如 SYN 洪泛攻击，会危害服务器对合法的客户端提供服务的能力。恶意的客户端在成功建立连接之后，发送不合法的查询、不完整的查询或者根本不发送查询，也可能耗尽服务器的可用连接资源。建议服务器提供限制接入连接资源的配置项，用以限制来自一个客户端的接受的连接的数量和处理的查询的数量，并限制闲置的连接保持开启的时间长度。



## 参 考 文 献

- [1] IETF RFC4649,B. Volz, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option”, August 2006
- [2] IETF RFC5007,J. Brzozowski,“DHCPv6 Leasequery”,September 2007
- [3] IETF RFC5460,M. Stapp, “DHCPv6 Bulk Leasequery”,February 2009