5

DHCP FOR IPv6 (DHCPv6)

For those devices that obtain IPv6 addresses dynamically, two main strategies are available to automate this address assignment process: client based or network server based. In Chapter 2, we introduced the concept of client-based address assignment in the form of address autoconfiguration, a process whereby a client can determine its location based on router advertisements and automatically calculate its interface identifier to derive an address. However, if during the requisite process of duplicate address detection, the host determines that its autoconfigured address is already in use, it must rederive another address or await manual intervention.

Network server-based address assignment such as DHCP enables a host to announce its presence in requesting an IP address, among other parameters, from a server in the IP network. DHCP for IPv6 addresses is referred to as DHCPv6 and is defined in RFC 3315 (68). As defined, DHCPv6 is not integrated with DHCP for IPv4. This means that DHCPv6 will support IPv6 addresses and configurations only, not additionally IPv4 addresses and parameters. It is left to future development to define this should demand dictate.

IP Address Management: Principles and Practice, by Timothy Rooney

5.1 DHCP COMPARISON: IPv4 VERSUS IPv6*

DHCPv6 uses different message types and packet formatting than DHCP for IPv4, but is similar in many ways. Table 5.1 highlights these similarities and differences.

TABLE 5.1. Comparison of DHCP for IPv4 and IPv6

Feature	DHCP for IPv4	DHCPv6
Destination IP address of initial client message	Broadcast (255.255.255.255)	Multicast to link-scoped address: All-DHCP-Agents address (FF02::1:2)
DHCP Relay support	Yes by configuring DHCP server addresses in each relay agent	Yes either by configuring DHCP server addresses in each relay agent or using the All_DHCP_Servers site-scoped multicast address (FF05::1:3)
Relay agent forwarding	Same message type code, but inserts giaddr and unicasts to DHCP server(s)	Encapsulates client message in RELAY-FORW to DHCP server(s) and RELAY-REPL from server(s)
Message to locate server to obtain IP address and configuration	DHCPDISCOVER	SOLICIT
Server message to engage client	DHCPOFFER	ADVERTISE
Client message to accept parameters	DHCPREQUEST	REQUEST
Server acknowledgment of lease binding	DHCPACK	REPLY
Client message to leasing DHCP server to extend lease	DHCPREQUEST (unicast)	RENEW (unicast)
Client message to any DHCP server to extend lease	DHCPREQUEST (broadcast)	REBIND (multicast)
Client message to relinquish a lease	DHCPRELEASE	RELEASE
Client message to indicate that an offered IP address is already in use	DHCPDECLINE	DECLINE
Server message to instruct client to obtain a new configuration	DHCPFORCERENEW	RECONFIGURE
Request IP configuration only, not address	DHCPINFORM	INFORMATION-REQUEST

* Initial sections of this chapter are based on Chapter 3 of Ref. 11.

5.2 DHCPv6 ADDRESS ASSIGNMENT

When a device initializes on an IPv6 subnet, it will listen for or solicit a router advertisement to determine if DHCPv6 services are available for the subnet. Recall from our discussion about neighbor discovery in Chapter 2 that the M bit within the router advertisement informs subnet devices that DHCPv6 services are available for address and parameter assignment; the O bit indicates that DHCPv6 services are available for parameter setting but not for address assignment. The DHCPv6 process begins with a client issuing a SOLICIT message, in essence requesting a "bid" from DHCP servers that can provide an IP address on the particular subnet to which the client is connected. Instead of broadcasting this initial packet as in IPv4, the SOLICIT message is sent by the client to the All_Relay_Agents_and_Servers multicast address, FF02::1:2. Note that the scope field on this multicast address, highlighted in bold (FF0**2**::1:2), applies to link local scope.

DHCPv6 servers on this subnet will receive the SOLICIT packet directly and may respond with an ADVERTISE packet, indicating a preference value. The preference value is intended to enable the client to select the server advertising the highest preference as configured by administrators. The server will also indicate if it has no addresses available on the subnet. The ADVERTISE packet will be unicast to the client if the SOLICIT had been received directly using the client's source IP address from the SOLICIT packet (most likely the client's link local address).

The client analyzes the advertisements received, and selects a server from which to request an IP address, typically with the highest preference, and issues a REQUEST message to the server. The server will then record the address assignment and reply to the client with a REPLY message as shown in Figure 5.1.

Any routers on the link configured as relay agents receiving the SOLICIT packet from a DHCPv6 client will relay the packet to one or more DHCPv6 servers. IPv6 relay agents do not require configuration of DHCP Relay addresses as in the IPv4 case, though they may enable such configuration. Instead of simply forwarding the packet to one or more DHCP servers as in IPv4, IPv6 relay agents encapsulate the original SOLICIT packet within a RELAY-FORW packet. This packet is then sent to configured DHCP servers or via multicast to the scoped All-DHCP-Servers multicast address (FF05::1:3). Analogous to the IPv4 DHCP GIAddr parameter, the link address field of the RELAY-FORW packet indicates the link on which the client requesting an IP address currently resides. This process is illustrated in Figure 5.2. This information is used by the DHCPv6 server in assigning an appropriate IP address for this link. The

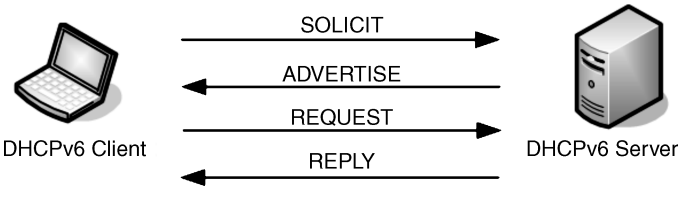

Figure 5.1. DHCPv6 address assignment.

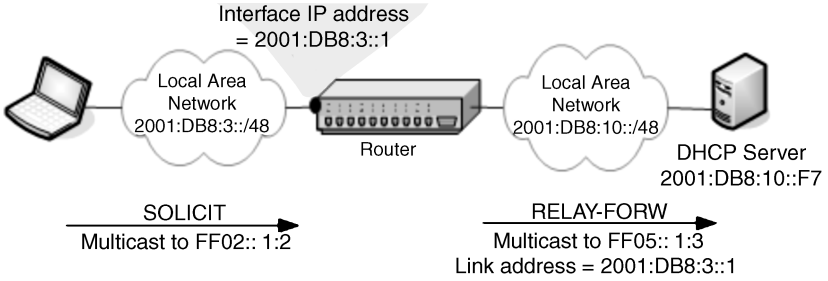

Figure 5.2. DHCPv6 Relay (11).

DHCPv6 server encapsulates its ADVERTISE message in a RELAY-REPL packet and unicasts it to the corresponding relay agent.

When the client receives a Reply packet to confirm the address assignment, the client must perform duplicate address detection to ensure no other device is already using the IP address due to autoconfiguration or manual configuration. If another device is using the assigned IP address, the client would send a Decline message to the DHCP server, indicating that the address is in use. The client can then reinitiate the DHCP process to obtain a different IP address.

In addition to the four-packet exchange outlined above, DHCPv6 features a rapid commit option. This halves the messaging requirements by enabling the server to simply REPLY to a SOLICIT packet. The client would include the rapid commit option in its SOLICIT message. Servers responding with an address assignment would issue a REPLY packet directly, also including the rapid commit option. Note that each server responding will assume that the address it assigned is leased, so rapid commit should be used either with short lease times or for support by a limited number of servers if normally there are many serving the same subnet.

As in IPv6 autoconfiguration described in Chapter 2, each nontemporary* IPv6 address assigned via DHCP has a preferred lifetime and a valid lifetime. After the preferred lifetime expires, the address is considered valid but deprecated. No new IP communications sessions should utilize the address while deprecated.

5.3 DHCPv6 PREFIX DELEGATION

DHCPv6 is not only used to assign individual IP addresses and/or associated IP configuration information to hosts but can also be used to delegate entire networks to requesting router devices. This form of delegation via DHCPv6 is called *prefix delegation*. This original motivation for prefix delegation arose from broadband service providers seeking to automate the process of delegating IPv6 subnets (e.g., /48 to /64 networks) to broadband subscribers in a hierarchical manner. A requesting router device at the edge of the service provider network, facing subscribers, would issue a request for address space via the DHCPv6 protocol to a delegating router. Note the terminology: this

* A temporary address is a short nonrenewable address.

is intended to be an inter-router protocol though a DHCPv6 server could perform the functions of the delegating router.

The prefix delegation process utilizes the same basic DHCPv6 message flow described above for address assignment per Figure 5.1: Solicit, Advertisement, Request, and Reply. Additional information within the corresponding DHCPv6 messages is used to determine an appropriate network for delegation. Like IP addresses, prefixes have preferred and valid lifetimes. The requesting router can request a lifetime extension via the DHCPv6 Renew and Rebind messages.

5.4 DHCPv6 SUPPORT OF ADDRESS AUTOCONFIGURATION

When we discussed IPv6 autoconfiguration in Chapter 2, we defined three types of autoconfiguration:

- *Stateless*. This process is "stateless" in that it does not depend on the state or availability of external assignment mechanisms, for example, DHCPv6.
- *Stateful*. The stateful process relies solely on external address assignment mechanism such as DHCPv6.
- *Combination Stateless and Stateful*. This process involves a form of stateless address autoconfiguration used in conjunction with stateful configuration of additional IP parameters.

This third combined form of autoconfiguration leverages DHCPv6 not for IPv6 address assignment, but for assignment of additional parameters, encoded as DHCPv6 options. The client can request configuration parameters via the Information-Request message, indicating which option parameter values it is seeking. A server(s) that is able to supply the desired configuration parameters will respond with a Reply message with the corresponding option parameters.

5.4.1 DHCPv6 Message Types

The following message types have been defined for DHCPv6:

- SOLICIT—message type = 1—issued by a client to locate DHCPv6 servers.
- ADVERTISE—message type = 2—issued by a server in response to a Solicit message to indicate availability of the server for DHCP service.
- REQUEST—message type = 3—issued by the client to request IP addresses and configuration parameters from a particular DHCPv6 server.
- CONFIRM—message type = 4—issued by a client to any available server to verify that the addresses assigned to it are still appropriate to its current subnet location.
- RENEW—message type = 5—issued by a client to the server from which it received its IP address to extend or renew its IP address lifetime and to update other parameters.

- REBIND—message type = 6—issued by a client to all available servers to extend its IP address lifetime and to update other parameters. This is sent after receiving no response from a prior RENEW message.
- REPLY—message type = 7—issued by a server to supply IP address and/or configuration parameters to a client in response to Solicit, Request, Renew, or Rebind messages. The server also issues this message type to clients desiring to confirm their configurations via the Confirm message and to acknowledge receipt of Release and Decline messages from clients.
- RELEASE—message type = 8—issued by a client to the server from which it received its IP address to relinquish the IP address. The client must then cease use of the IP address.
- DECLINE—message type = 9—issued by a client to inform a server that one or more addresses assigned by the server are already in use on the link on which the client resides.
- RECONFIGURE—message type = 10—issued by a server to instruct a client to reinitialize as the server has new or updated configuration parameters for the client. The client must then issue a Renew or Information-Request as instructed by the server to obtain the updated or new information.
- INFORMATION-REQUEST—message type = 11—issued by the client to obtain configuration parameters other than IP addresses from a server.
- RELAY-FORW—message type = 12—issued by a relay agent to a server or set of servers directly or via another agent to encapsulate a client-initiated or relay agent-initiated message.
- RELAY-REPL—message type = 13—issued by a server in reply to RELAY-FORW to a relay agent encapsulating a message destined for a client, which is encoded as an option within the RELAY-REPL message. The relay agent may pass the message directly or via other relay agents to the client.
- LEASEQUERY—message type = 14—issued by a device such as an access concentrator or relay agent to request lease binding information from the DHCP server for a particular client IPv6 address, DUID, relay agent, link address, or remote identifier. The IPv6 client DUID queries are for individual device lease queries, whereas the other query types facilitate bulk lease query of multiple client lease states. Bulk lease query for IPv4 is under development within the IETF.
- LEASEQUERY-REPLY—message type = 15—issued by a server to the querying device in response to a LEASEQUERY message with the lease binding information relevant to the query.
- LEASEQUERY-DONE—message type = 16—issued by a server to the querying device indicating the end of a result of a Bulk LeaseQuery.
- LEASEQUERY–DATA—message type = 17—issued by a server to the querying device to encapsulate a single DHCPv6 client's lease information when more than one client's data is provided in such results.

Figure 5.3. DHCPv6 packet format (68).

5.4.2 DHCPv6 Packet Format

The DHCPv6 packet format is very simple (Figure 5.3). It consists of an 8-bit message type, 24-bit transaction ID, and a variable-length options field. That's it! Information regarding identification and configuration of the client is placed within the options field.

However, when a relay agent is in the path between the client and the server, the relay agent modifies the message, yielding a common format for both forwarded and reply messages, as shown in Figure 5.4:

- 8-bit message type
- 8-bit hop count or the number of relay agents that have relayed this message, incremented by each along the path
- 128-bit link-address—the IPv6 address that is used by the server to identify the link on which the client is located (similar to the giaddr concept)
- 128-bit peer address—the IPv6 address of the client or relay agent from which the message to be relayed was received
- Variable length options field, including the relay message option that includes the DHCPv6 message being relayed between the client and the server

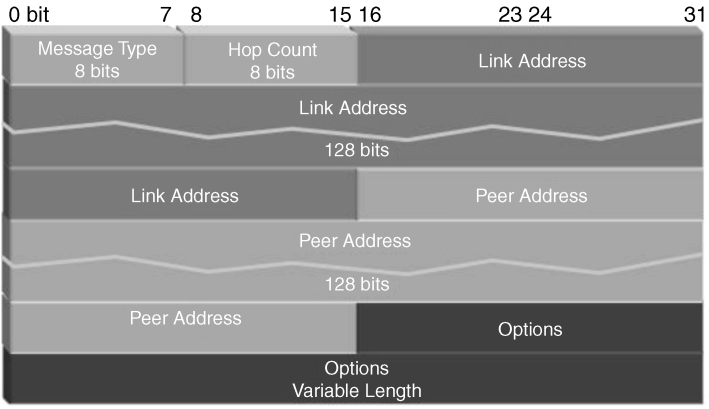

Figure 5.4. DHCP Relay packet format (68).

5.5 DEVICE UNIQUE IDENTIFIERS

Like DHCPv4, a DHCPv6 server must track the availability and assignment of IP addresses within its configured address pools and identify requestors and holders of IP addresses. DHCPv6 utilizes the Device Unique Identifier (DUID) to identify clients. DUIDs are used not only for servers to identify clients but also for clients to identify servers. The DUID is analogous to the client-identifier concept in that DUIDs are intended to be globally unique for a device, not an interface. DUIDs should not change over time, even if the device undergoes changes in hardware. DUIDs are constructed in various manners automatically by IPv6 nodes. They consist of a two-octet type code followed by a variable number of octets based on the type. The following DUID-type codes are defined as follows:

- Type = 1—link layer address plus time (DUID-LLT)
- Type = 2—vendor-assigned unique ID based on Enterprise Number (DUID-EN)
- Type = 3—link layer-based DUID (DUID-LL)

For those based on link layer address, they are to be used for *all* device interfaces, even if the hardware from which the link layer address was obtained is removed. The DUID is a device identifier, not an interface identifier.

5.5.1 DUID-LLT

The DUID-link layer address plus time format is shown in Figure 5.5. The DUID type is "1". The hardware type is the IANA-assigned value for the hardware type of the interface (see http://www.iana.org/assignments/arp-parameters for a complete list). The time field follows and represents the time that the DUID was created in seconds since midnight UTC, January 1, 2000, modulo 2^{32}. Then the hardware address of the selected interface comprises the link layer address field.

This DUID is formed by a device by selecting one interface for the use of its link layer type and address. The DUID should be stored in persistent storage on the device. The link layer address must be globally unique for its corresponding hardware type. This same DUID is then associated with each interface on the device during

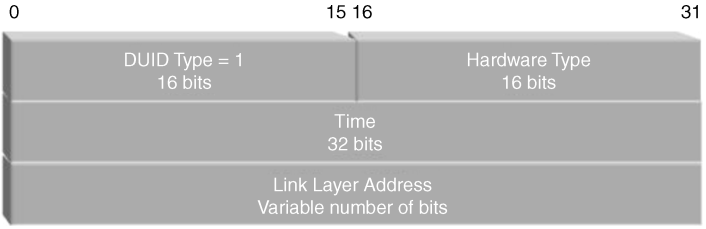

Figure 5.5. Link layer address plus time formatted DUID (68).

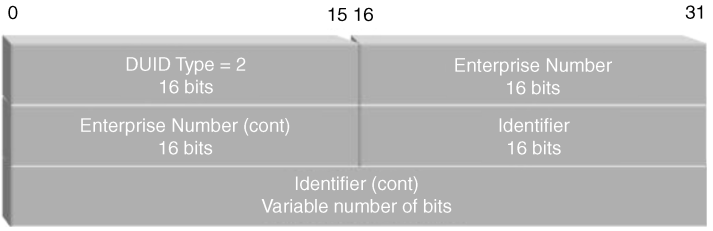

Figure 5.6. Enterprise number formatted DUID (68).

communications with the DHCP server, even if the interface upon which derivation of the DUID was based is removed. However, should the interface be removed and placed in another device, the time component of this DUID format should provide a high degree of likelihood that the DUID formulated by the new device using the same interface card will differ, should that device so choose to base its DUID on the same interface address. The DUID-LLT format is recommended for those devices that have persistent storage for storing the DUID.

5.5.2 DUID-EN

The Enterprise Number-based DUID format is assigned to the device by the vendor (Figure 5.6). The DUID consists of the DUID type "2", the Enterprise Number as assigned by IANA (see http://www.iana.org/assignments/enterprise-numbers) to the device vendor much as Ethernet interface prefixes are assigned to vendors by the IEEE. The EN is then followed by a vendor-unique identifier assigned by the vendor. This DUID must be stored in persistent storage on the device.

5.5.3 DUID-LL

The link layer address-based DUID is very similar to DUID-LLT, with the omission of the time field. The DUID Type is '3' (Figure 5.7). The hardware type is the IANA-assigned value for the hardware type of the interface (see http://www.iana.org/assignments/arp-parameters for complete list), and the link layer address field follows. Like the other forms of DUIDs, a common DUID should be associated with each

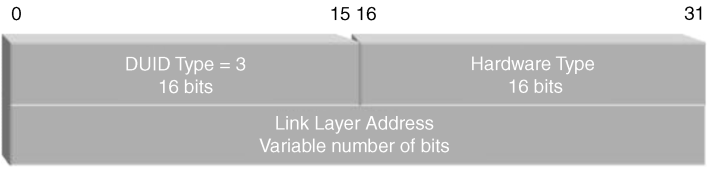

Figure 5.7. Link layer address formatted DUID (68).

interface on the device. This form of DUID is recommended for those devices that do not have persistent storage capabilities for the DUID value.

5.6 IDENTITY ASSOCIATIONS

While DUIDs are associated with all interfaces of a device and IP addresses are assigned to interfaces, you may be wondering how the device and server identify particular interfaces for a given DUID. The concept of the identity association (IA) provides this linkage between a DHCPv6 server and a client interface for individual address assignment. IAs are differentiated by type between those for temporary addresses (IA_TA), which are short-leased, nonrenewable addresses, those for nontemporary addresses (IA_NA), and those for prefix delegation (IA_PD).

Temporary address assignments assuage privacy concerns associated with auto-configured addresses based on hardware addresses (i.e., modified EUI-64 interface IDs), which do not change over time. The concern is that a given interface ID within an IPv6 address does not change unless the underlying hardware interface changes. Thus, even if the network upon which a device is connected changes from day to day, the interface ID does not. The ability to track the location of a device and thus its user becomes relatively easy, thus the concern with privacy. The use of short-lived, non-renewable address assignments via DHCPv6 using temporary addresses is one means to address this concern. Please see RFC 3041 for more background on this privacy issue.

For individual address assignment, temporary or nontemporary, each client interface has an IA, identified by an IA identifier (IAID). The IAID is represented as four octets in client–server DHCPv6 communications and is chosen by the client. The IAID must be unique among all IAIDs associated with the client and must be stored persistently across client reboots or consistently derivable upon each reboot. The client specifies its DUID and IAID for which an address is being requested from the DHCPv6 server. The DHCPv6 server assigns an IPv6 address to the IAID, along with the corresponding T1 (renew) and T2 (reboot) timer values.

IA_PDs are not necessarily associated with a device interface. Recall that the requesting router is using DHCPv6 to obtain an IPv6 network delegation. The requesting router must derive one or more IA_PDs for use within DHCPv6, and it must be persistent across reboots or consistently derivable.

5.7 DHCPv6 OPTIONS

DHCPv6 options are used to convey information relevant to the associated DHCP message, including DUIDs and IAs. Options are listed within the DHCPv6 message and have the general format as shown in Figure 5.8.

The currently defined set of DHCPv6 options are given in Table 5.2. Note that certain options may be nested, such as those associated with an IA.

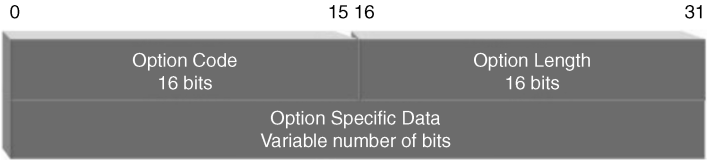

Figure 5.8. DHCPv6 options format (68).

TABLE 5.2. DHCPv6 Options

Code	Name	Meaning	Reference
1	OPTION_CLIENTID	Client identifier (DUID of client)	RFC 3315 (68)
2	OPTION_SERVERID	Server identifier (DUID of server)	RFC 3315 (68)
3	OPTION_IA_NA	Identity association for nontemporary addresses—includes the IAID, T1 time, T2 time, and additional options for the IA for nontemporary addresses	RFC 3315 (68)
4	OPTION_IA_TA	Identity association for temporary addresses—includes the IAID and additional options for this IA for temporary addresses	RFC 3315 (68)
5	OPTION_IAADDR	IA address option—specifies IPv6 addresses and associated preferred lifetime, valid lifetime, and options associated with an IA_NA or IA_TA. As such, this option may only appear as an option to the DHCPv6 message option OPTION_IA_TA or OPTION_IA_NA	RFC 3315 (68)
6	OPTION_ORO	Option request option—used by clients to list option codes for which values are requested or by servers in a Reconfigure message to indicate which options the client should request in its subsequent Renew or Information-Request message	RFC 3315 (68)
7	OPTION_PREFERENCE	Preference setting by the server to facilitate client selection of DHCP server	RFC 3315 (68)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
8	OPTION_ELAPSED_TIME	The amount of time since the client began the current DHCP transaction in hundredths of a second. Clients are required to use this option	RFC 3315 (68)
9	OPTION_RELAY_MSG	The DHCP message being relayed by a relay agent	RFC 3315 (68)
10	Unassigned		
11	OPTION_AUTH	Authentication information for use in reliably identifying the source of a DHCP message and to verify message integrity	RFC 3315 (68)
12	OPTION_UNICAST	Server unicast option indicates the IP address to which the client may unicast messages to this server	RFC 3315 (68)
13	OPTION_STATUS_CODE	Status code option indicates a 2-byte status code and variable length status message. This option may be used as a DHCP message option or as an option within another DHCP message option	RFC 3315 (68)
14	OPTION_RAPID_COMMIT	Rapid commit option enables a client to request a direct reply with an IP address and parameters, bypassing the Advertise and Request messages	RFC3315 (68)
15	OPTION_USER_CLASS	User class option—analogous to user class in DHCPv4 in assisting the server in making address assignment decisions	RFC 3315 (68)
16	OPTION_VENDOR_CLASS	Vendor class option—analogous to vendor class in DHCPv4 in conveying the vendor or manufacturer of the device or interface to assist the server in making address assignment decisions. The vendor class option includes the IANA-assigned Enterprise Number for the vendor	RFC 3315 (68)

(continued)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
17	OPTION_VENDOR_ OPTS	Vendor-specific information—this option includes the IANA-assigned Enterprise Number as well as one or more options, each defined with option code, length, and value	RFC 3315(68)
18	OPTION_ INTERFACE_ID	Interface ID option—used by relay agents to convey the agent's interface ID on which the client message was received. This option may only appear in RELAY-FORW messages, and when it does, it is copied by the server to the RELAY-REPL message	RFC 3315 (68)
19	OPTION_RECONF_MSG	Reconfigure message option for use in the Reconfigure message to inform the client which message type to use to reconfigure; either Renew or Information-Request	RFC 3315 (68)
20	OPTION_RECONF_ ACCEPT	Reconfigure accept option—the client uses this option if it is willing to accept Reconfigure messages from the server	RFC 3315 (68)
21	OPTION_SIP_ SERVER_D	SIP servers domain names option listing domain names of the SIP outbound proxy servers that the client can use	RFC 3319 (69)
22	OPTION_SIP_ SERVER_A	SIP servers IPv6 address list option lists the IPv6 addresses of the SIP outbound proxy servers that the client can use	RFC 3319 (69)
23	OPTION_DNS_SERVERS	DNS recursive name server option—lists IPv6 address(es) of DNS recursive name servers to which DNS queries may be sent by the client resolver in order of preference	RFC 3646 (70)
24	OPTION_DOMAIN_LIST	Domain search list option—provides a domain search list for client use when resolving hostnames via DNS	RFC 3646 (70)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
25	OPTION_IA_PD	Identity association for prefix delegation—includes the IAID, T1 time, T2 time, and additional options for the IA_PD, including the associated prefix(es) defined as option code 26	RFC 3633 (71)
26	OPTION_IAPREFIX	IA_PD Prefix option—specifies the IPv6 prefixes associated with the IA_PD, along with associated options and preferred and valid lifetimes. This option may only appear as an option to the DHCPv6 message option OPTION_IA_PD. The prefix is specified with an 8-bit prefix length and a 128-bit IPv6 prefix	RFC 3633 (71)
27	OPTION_NIS_SERVERS	Network information service (NIS) servers—ordered list of NIS servers by IPv6 address available to the client	RFC 3898 (72)
28	OPTION_NISP_SERVERS	Network information service v2 (NIS +) servers—ordered list of NIS + servers by IPv6 address available to the client	RFC 3898 (72)
29	OPTION_NIS_ DOMAIN_NAME	Network information service domain name—NIS domain name to be used by the client	RFC 3898 (72)
30	OPTION_NISP_ DOMAIN_NAME	Network information service v2 (NIS +) domain name—NIS + domain name to be used by the client	RFC 3898 (72)
31	OPTION_SNTP_ SERVERS	Simple Network Time Protocol (SNTP) servers—ordered list of SNTP servers by IPv6 address available to the client	RFC 4075 (73)
32	OPTION_ INFORMATION_ REFRESH_TIME	Information refresh option—specifies the upper bound of the number or seconds from the current time that a client should wait before refreshing information received from the DHCPv6 server, particularly for stateless DHCPv6 scenarios	RFC 4242 (74)

(continued)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
33	OPTION_BCMCS_SERVER_D	Broadcast and multicast service (BCMCS) domain name list—list of one or more FQDNs corresponding to BCMCS server(s) (BCMCS is used in 3G wireless networks to enable mobiles to receive broadcast and multicast services.)	RFC 4280 (46)
34	OPTION_BCMCS_SERVER_A	Broadcast and multicast service IPv6 address list—list of one or more IPv6 address(es) corresponding to BCMCS server(s). (BCMCS is used in 3G wireless networks to enable mobiles to receive broadcast and multicast services)	RFC 4280 (46)
35	Unassigned		
36	OPTION_GEOCONF_CIVIC	Geographical location in civic (e.g., postal) format. This option can be provided by the server to relate the location of the server, the closest network element (e.g., router) to the client, or the client itself. The location information includes an ISO 3166 country code (US, DE, JP, etc.) and country-specific location information such as state, province, county, city, block, group of streets, and more	RFC 4776 (51)
37	OPTION_REMOTE_ID	Relay agent remote ID option—remote identity inserted by the relay agent in RELAY-FORW message to the DHCPv6 server. This is useful in service provider environments where the "edge" device facing the subscriber device inserts an identifier for the subscriber connection prior to relaying to the DHCPv6 server	RFC 4649 (75)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
38	OPTION_ SUBSCRIBER_ID	Relay agent subscriber ID option—subscriber identity inserted by the relay agent in RELAY-FORW message to the DHCPv6 server. This is useful in service provider environments where the "edge" device facing the subscriber device inserts an identifier for the subscriber from which the message originated, prior to relaying to the DHCPv6 server	RFC 4580 (76)
39	OPTION_CLIENT_ FQDN	FQDN option—indicates whether the client or the DHCP server should update DNS with the AAAA record corresponding to the assigned IPv6 address and the FQDN provided in this option. The DHCP server always updates the PTR record	RFC 4704 (77)
40	OPTION_PANA_AGENT	This option provides one or more IPv6 address(es) associated with PANA (Protocol for Carrying Authentication for Network Access) Authentication Agents that a client can use	RFC 5192 (62)
41	OPTION_NEW_POSIX_ TIMEZONE	Time zone (TZ) to be used by the client in IEEE 1003.1 format (POSIX—portable operating system interface). This format enables textual representation of time zone and daylight savings time information	RFC 4833 (52)
42	OPTION_NEW_TZDB_ TIMEZONE	Time zone database entry referred to by entry name. The client must have a copy of the TZ database, which it queries for the corresponding entry to determine its time zone	RFC 4833 (52)

(continued)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
43	OPTION_ERO	Relay agent echo request option—used by relay agents in the RELAY_FORW message to request that the DHCPv6 server echo back certain requested relay agent options, even if not supported on the server (DHCPv4 servers always echo back relay agent option (82) information, but this is not required in DHCPv6, hence this option for relay agents requiring such echo back.)	RFC 4994 (78)
44	OPTION_LQ_QUERY	The query option is used in the LEASEQUERY message to identify the query information being requested. This option includes the query type (by IA address or client ID option), link address to which the query applies, and query options	RFC 5007 (79)
45	OPTION_CLIENT_DATA	Client data—this option contains the query response information for the requested client data within a LEASEQUERY-REPLY message. At a minimum, this option includes the client identifier (OPTION_CLIENTID), the IA address or prefix (OPTION_IAADDR and/or OPTION_IAPREFIX), and client last transaction time (OPTION_CLT_TIME)	RFC 5007 (79)
46	OPTION_CLT_TIME	Client last transaction time—indicates the number of seconds since the server last communicated with the client referenced by the lease query. This option is encapsulated within the OPTION_CLIENT_DATA option within a LEASEQUERY-REPLY message	RFC 5007 (79)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
47	OPTION_LQ_ RELAY_ DATA	Relay data—used in a LEASEQUERY-REPLY message to provide the relay agent information associated with the client information requested. This option includes the relay agent address from which the client's relay information was received along with the complete relayed message	RFC 5007 (79)
48	OPTION_LQ_ CLIENT_ LINK	Client link—identifies one or more links on which the queried client has DHCPv6 bindings. The queried client can be identified by address or client ID	RFC 5007 (79)
49	OPTION_MIP6_HNINF	Mobile IPv6 home network information—used by the client to identify its target home network to the server (in an Information Request message)	draft-ietf-mip6-hiopt-17.txt (80)
50	OPTION_MIP6_RELAY	Mobile IPv6 relay agent—used by a relay agent to identify home network information via a RELAY-FORW message	draft-ietf-mip6-hiopt-17.txt (80)
51	OPTION_V6_LOST	Location to Service Translation (LoST) server domain name; LoST protocol maps service identifiers and location information to service URLs	RFC 5223 (63)
52	OPTION_CAPWAP_ AC_ V6	Control and provisioning of wireless access points (CAPWAP) access controller IPv6 address(es) to which the client may connect	RFC 5417 (64)
53	OPTION_RELAY_ID	DHCPv6 Bulk LeaseQuery—requests lease and prefix delegation bindings for a specified relay agent identified by its DUID in this option	RFC 5460 (81)

(continued)

TABLE 5.2. DHCPv6 Options (*Continued*)

Code	Name	Meaning	Reference
54	OPTION-IPv6_ Addresss-MoS	List of IPv6 address(es) for servers providing particular types of IEEE 802.21 Mobility Services (MoS)	RFC 5678 (65)
55	OPTION-IPv6_ FQDN-MoS	List of FQDN(s) for servers providing particular types of IEEE 802.21 Mobility Services	RFC 5678 (65)
56	OPTION_NTP_SERVER	Network Time Protocol (NTP) and Simple NTP (SNTP) server address(es) and/or domain names	RFC 5908 (180)
57	OPTION_F6_ACCESS_ DOMAIN	Domain name of the Location Information Server (LIS) on this access network	draft-ietf-geopriv-lis-discovery-15 (178)
58	OPTION_SIP_UA_ CS_LIST	Session Initiation Protocol (SIP) user agent configuration	draft-lawrence-sipforum-user-agent-config-03 (179)
59	OPT_BOOTFILE_URL	URL of client boot file	draft-dhc-dhcpv6-opt-netboot-10 (181)
60	OPT_BOOTFILE_PARAM	Client bootfile parameters	draft-dhc-dhcpv6-opt-netboot-10 (181)
61	OPTION_CLIENT_ ARCH_TYPE	Client system architecture	draft-dhc-dhcpv6-opt-netboot-10 (181)
62	OPTION_NII	Client network interface for universal network device interface (UNDI) support	draft-dhc-dhcpv6-opt-netboot-10 (181)
63–255	Unassigned		