

DHCPv6 Based IPv6 Access Services

Last Updated: October 2011

This paper will discuss the basics of DHCPv6 and various implementation models to allow service providers to architect IPv6 access services using Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Classical access models have traditionally used PPP to provide IPv6 addressing services. In contrast, current NGN (Next Generation Networks) networks provide native IPv6 services without requiring PPP between the user and service provider. This paper extends the “IPv6 Access Services” whitepaper and highlights technology enhancements for deploying and provisioning PPP-less service provider access networks.

Managed IPv6 Access Services for Native IPv6 ISP Connectivity

DHCPv6 Technology Overview

IPv6 Internet Address Assignment Overview

IPv6 has been developed with Internet Address assignment dynamics in mind. Being aware that IPv6 Internet addresses are 128 bits in length and written in hexadecimals makes automation of address-assignment an important aspect within network design. These attributes make it inconvenient for a user to manually assign IPv6 addresses, as the format is not naturally intuitive to the human eye. To facilitate address assignment with little or no human intervention, several methods and technologies have been developed to automate the process of address and configuration parameter assignment to IPv6 hosts.

The various IPv6 address assignment methods are as follows:

1. **Manual Assignment**

An IPv6 address can be statically configured by a human operator. However, manual assignment is quite open to errors and operational overhead due to the 128 bit length and hexadecimal attributes of the addresses, although for router interfaces and static network elements and resources this can be an appropriate solution.

2. **Stateless Address Autoconfiguration (RFC2462)**

Stateless Address Autoconfiguration (SLAAC) is one of the most convenient methods to assign Internet addresses to IPv6 nodes. This method does not require any human intervention at all from an IPv6 user. If one wants to use IPv6 SLAAC on an IPv6 node, it is important that this IPv6 node is connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IPv6 nodes to configure themselves with IPv6 address and routing parameters, as specified in RFC2462, without further human intervention.

3. **Stateful DHCPv6**

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network

addresses, to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately, or in addition to the stateless autoconfiguration to obtain configuration parameters.

4. DHCPv6-PD

DHCPv6 Prefix Delegation (DHCPv6-PD) is an extension to DHCPv6, and is specified in RFC3633. Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. A practical example would be the stateful address assignment of "2001:db8::1" from a DHCPv6 server to a DHCPv6 client. DHCPv6-PD however is aimed at assigning complete subnets and other network and interface parameters from a DHCPv6-PD server to a DHCPv6-PD client. This means that instead of a single address assignment, DHCPv6-PD will assign a set of IPv6 "subnets". An example could be the assignment of "2001:db8::/60" from a DHCPv6-PD server to a DHCPv6-PD client. This will allow the DHCPv6-PD client (often a CPE device) to segment the received address IPv6 address space, and assign it dynamically to its IPv6 enabled interfaces.

5. Stateless DHCPv6

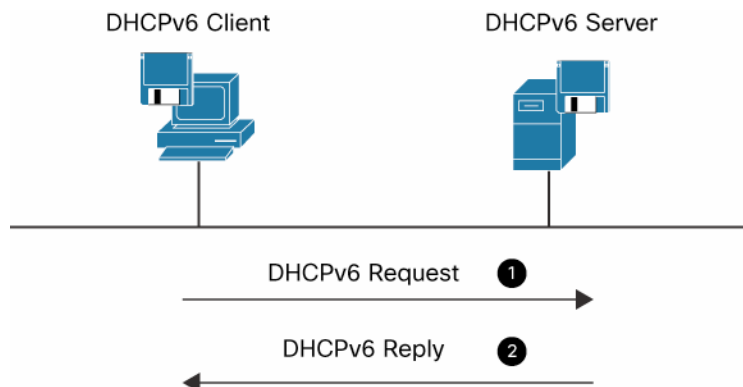
Stateless DHCPv6 is a combination of "stateless Address Autoconfiguration" and "Dynamic Host Configuration Protocol for IPv6" and is specified by RFC3736. When using stateless-DHCPv6, a device will use Stateless Address Auto-Configuration (SLAAC) to assign one or more IPv6 addresses to an interface, while it utilizes DHCPv6 to receive "additional parameters" which may not be available through SLAAC. For example, additional parameters could include information such as DNS or NTP server addresses, and are provided in a stateless manner by DHCPv6. Using stateless DHCPv6 means that the DHCPv6 server does not need to keep track of any state of assigned IPv6 addresses, and there is no need for state refreshment as result. On network media supporting a large number of hosts associated to a single DHCPv6 server, this could mean a significant reduction in DHCPv6 messages due to the reduced need for address state refreshments. From Cisco IOS 12.4(15)T onwards the client can also receive timing information, in addition to the "additional parameters" through DHCPv6. This timing information provides an indication to a host when it should refresh its DHCPv6 configuration data. This behavior (RFC4242) is particularly useful in unstable environments where changes are likely to occur.

Note that there is no requirement that a network use either stateless or stateful; in some cases both may be in use.

Introduction to DHCPv6

The basic DHCPv6 client-server concept is similar to DHCP for IPv4. If a client wishes to receive configuration parameters it will send out a request on the attached local network. A DHCPv6 server which is connected to this local network may reply back with the requested configuration parameters as demonstrated below:

Figure 1. : Basic DHCPv6 Principle



DHCPv6 technology was introduced in Cisco IOS since release 12.3(4)T and feature support has been adapted by many additional IOS releases. The Dynamic Host Configuration Protocol for IPv6 enables managed distribution of configuration parameters between a DHCPv6 Server and its clients. DHCPv6 offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility (e.g. DNS server, NTP server, etc.). DHCPv6 has been specified in RFC3315 and is the result of a clean new protocol architecture (for example DHCPv6 did not suffer from design restrictions mandated by legacy technology like BOOTP). As result DHCPv6 uses an architecture concept of "options" to carry additional parameters and information within DHCPv6 messages. These options are aligned in the TLV (Type-Length-Value) structure. Each Type and Length field has a length of 16 bits, with a variable length available for the Value field. Each option 'should' appear only once in the option area of the DHCPv6 messages, although the protocol standard does not restrict this aspect. Each option is also scoped, which means that some options can contain other options, in which case the options contained in that option have meaning only for the option they are contained in.

DHCPv6 Components

DUID (DHCP Unique Identifier)

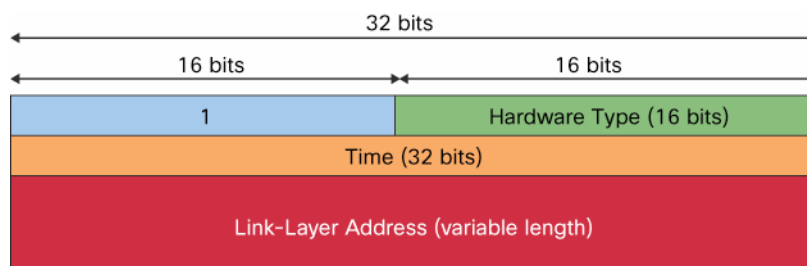
Each DHCPv6 component has a DUID (DHCPv6 Unique Identifier) which is used to identify the device when exchanging DHCPv6 messages. RFC3315 does not allow the use of the DUID for any other purpose. The DUID is carried as an DHCPv6 option, because its length could be variable and its availability is not required in all DHCPv6 messages. The DUID is designed to be unique around all DHCPv6 servers and clients, and must be stable for any specific client or server (for example a device DUID should not change as the result of changing some hardware in a device). A DUID can not be longer than 128 octets. At the moment there are three types of DUID defined:

- 1) Link-layer address plus time (DUID-LLT)
- 2) Vendor-assigned unique ID based on Enterprise Number
- 3) Link-layer address (DUID-LL)

Cisco uses a structure based on DUID-LLT (link-layer address plus time). The device uses the MAC address from the lowest numbered interface to form the DUID. The DUID of a Cisco router can be checked by executing the command 'show ipv6 dhcp' as shown below:

```
ecmd-1841-1#sho ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001001A2F875602
ecmd-1841-1#
```

The DUID-LLT field is constructed as follows:



The type of DUID-LLT consists of:

- Two octet type field containing the value 1

- Two octet hardware type code. The hardware type MUST be a valid hardware type assigned by the IANA as described in RFC 826. Ethernet uses hardware type 1 and 48-bit MAC address of the device as the link-layer address.
- Four octets containing a time value
- Link-layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated. The time value is the time that the DUID is generated, represented in seconds since midnight (UTC), January 1, 2000, modulo 2^{32} .

DHCPv6 Bindings

A DHCPv6 binding is based upon an IA (Identity Association) and is a construct through which a server and a client can identify, group, and manage a set of related IPv6 addresses.

A binding (or, client binding) is a group of server data records containing the information the server has about the addresses in an IA, or configuration information explicitly assigned to the client. A binding contains information about an IA and is indexed by the tuple <DUID, IA-type, IAID> (where IA-type is the type of address in the IA; for example, temporary, non-temporary or prefix delegation address; the IAID is a 32 bit number assigned by the DHCPv6 client). A binding contains configuration information for a client and is indexed by <DUID>. A single client can request multiple bindings (in single or multiple transactions), and each binding has one or more leases involved.

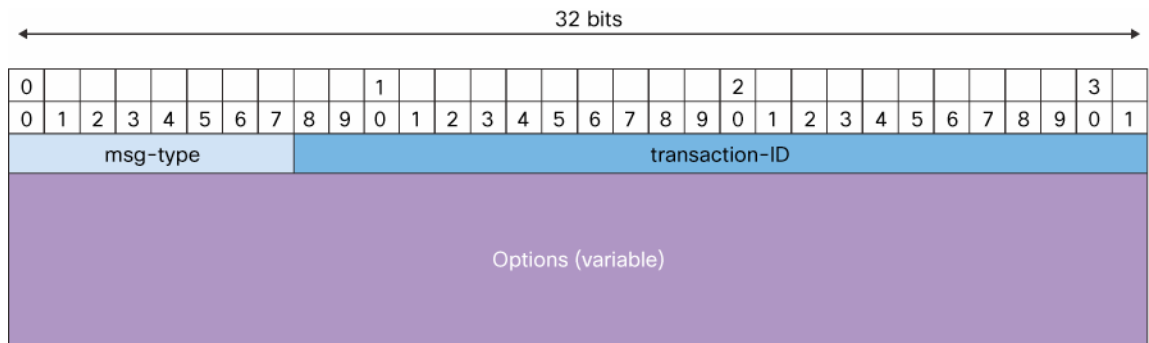
IPv6 Address Selection by an DHCPv6 Server

A server selects addresses to be assigned to an IA (Identity Association) according to the address assignment policies determined by the server administrator and the specific information the server determines about the client from some combination of the following sources:

- The link to which the client is attached. The client could be attached directly on-link or through a DHCPv6 relay.
- The client's DUID
- Other information supplied by the client
- Other information supplied by a relay agent

DHCPv6 Client/Server Messages

DHCPv6 messages are exchanged over UDP port 546 and 547. Clients listen for DHCP messages on UDP port 546 while servers and relay agents listen for DHCP messages on UDP port 547. The basic message format is as follows:



Client -> Server messages (msg-type):

Solicit, Request, Confirm, Renew, Rebind, Release, Decline, Information-Request

Server -> Client messages (msg-type):

Advertise, Reply, Reconfigure

Relay -> Relay/Server messages (msg-type):

Relay-Forw

Server/Relay -> Relay (msg-type):

Relay-Reply

To reduce the requirement for fixed fields, where potentially not all fields are always used, a flexible solution based upon DHCPv6 options is used to transport data, and all data is transported through dynamic usage of and selection options.

The following table shows a comparison between DHCPv6 and DHCPv4 message types.

DHCPv6 vs DHCPv4 Message Types

DHCPv6 Message Type	DHCPv4 Message Type
Solicit (1)	DHCPDISCOVER
Advertise (2)	DHCPOFFER
Request (3), Renew (5), Rebind (6)	DHCPREQUEST
Reply (7)	DHCPACK / DHCPNAK
Release (8)	DHCPRELEASE
Information-Request (11)	DHCPINFORM
Decline (9)	DHCPDECLINE
Confirm (4)	none
Reconfigure (10)	DHCPFORCERENEW
Relay-Forw (12), Relay-Reply (13)	none

SOLICIT (1)

A DHCPv6 client sends a Solicit message to locate DHCPv6 servers.

ADVERTISE (2)

A server sends an Advertise message to indicate that it is available for DHCP service, in response to a Solicit message received from a client.

REQUEST (3)

A client sends a Request message to request configuration parameters, including IP addresses or delegated prefixes, from a specific server.

CONFIRM (4)

A client sends a Confirm message to any available server to determine whether the addresses it was assigned are still appropriate to the link to which the client is connected. This could happen when the client

detects either a link-layer connectivity change or if it is powered on and one or more leases are still valid. The confirm message is used to confirm whether the client is still on the same link or whether it has been moved. The actual lease(s) are not validated; just the prefix portion of the addresses or delegated prefixes.

RENEW (5)

A client sends a Renew message to the server that originally provided the client's addresses and configuration parameters to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters.

REBIND (6)

A client sends a Rebind message to any available server to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters; this message is sent after a client receives no response to a Renew message.

REPLY (7)

A server sends a Reply message containing assigned addresses and configuration parameters in response to a Solicit, Request, Renew, Rebind message received from a client. A server sends a Reply message containing configuration parameters in response to an Information-request message. A server sends a Reply message in response to a Confirm message confirming or denying that the addresses assigned to the client are appropriate to the link to which the client is connected. A server sends a Reply message to acknowledge receipt of a Release or Decline message.

RELEASE (8)

A client sends a Release message to the server that assigned addresses to the client to indicate that the client will no longer use one or more of the assigned addresses.

DECLINE (9)

A client sends a Decline message to a server to indicate that the client has determined that one or more addresses assigned by the server are already in use on the link to which the client is connected.

RECONFIGURE (10)

A server sends a Reconfigure message to a client to inform the client that the server has new or updated configuration parameters, and that the client is to initiate a Renew/Reply or Information-request/Reply transaction with the server in order to receive the updated information.

INFORMATION-REQUEST (11)

A client sends an Information-request message to a server to request configuration parameters without the assignment of any IP addresses to the client.

RELAY-FORW (12)

A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent. The received message, either a client message or a Relay-forward message from another relay agent, is encapsulated in an option in the Relay-forward message.

RELAY-REPL (13)

A server sends a Relay-reply message to a relay agent containing a message that the relay agent delivers to a client. The Relay-reply message may be relayed by other relay agents for delivery to the destination

relay agent. The server encapsulates the client message as an option in the Relay-reply message, which the relay agent extracts and relays to the client.

DHCPv6 Options

Within DHCPv6, options are used to exchange parameter information between a server and a client. If a client wishes to request a specific option or set of parameters it must do this through an ORO option (Option Request Option). Cisco IOS only supports a limited set of options from the full list of options available at IANA (<http://www.iana.org/assignments/dhcpv6-parameters>). Options have a 16 bit option number and 16 bit option lengths. Some options will encapsulate other options for scoping purposes. A DHCPv6 relay will encapsulate client (or other relay) messages in a message option.

The following options are amongst others supported by Cisco IOS:

- Client Identifier option
 - The Client Identifier option is used to carry a DUID identifying a client between a client and a server
- Server Identifier option
 - The Server Identifier option is used to carry a DUID identifying a server between a client and a server
- Option Request option
 - The Option Request option is used to identify a list of options in a message between a client and a server.
- Preference option
 - The Preference option is sent by a server to a client to affect the selection of a server by the client
- Status Code Option
 - This option returns a status indication related to the DHCP message or option in which it appears
- Rapid Commit option
 - The Rapid Commit option is used to signal the use of the two message exchange for address assignment
- Identity Association for Prefix Delegation option (IA_PD option)
 - The IA_PD option is used to carry a prefix delegation identity association, the parameters associated with the IA_PD and the prefixes associated with it
- IA_PD Prefix option
 - The IA_PD Prefix option is used to specify IPv6 address prefixes associated with an IA_PD. The IA_PD Prefix option must be encapsulated in the IA_PD-options field of an IA_PD option.
- Domain Name Server option
 - The DNS Recursive Name Server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver MAY send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.
- Domain Search List option
 - The Domain Search List option specifies the domain search list the client is to use when resolving hostnames with DNS. This option does not apply to other name resolution mechanisms.
- Information Refresh Option

- The Information Refresh Option is used for specifying an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6. It is used with stateless DHCPv6 as there are no addresses or other entities with lifetimes that can tell the client when to contact the DHCPv6 server to refresh its configuration.
- Remote-id option
 - This option may be added by DHCPv6 relay agents that terminate switched or permanent circuits and have mechanisms to identify the remote host end of the circuit.

Not all options have been or will be standardized by the IETF. For these instances, a special option (VENDOR_OPTS Option) has been created which allows vendor specific options to be implemented. The SNMP-Enterprise-ID is used to identify the vendor. The data available in these options are completely up to the definition of the related vendor, however there is preference for the 16 bit options format. For example CableLabs is a vendor which utilizes a vendor specific option for DOCSIS3.0. The CableLabs enterprise-ID is 4491.

Some DHCPv6 options may encapsulate other options:

- IA_NA (Identity Association—Non-temporary Address) and IA_TA (Identity Association—Temporary Address) can encapsulate IAADDR (Identity Association Address)
- IA_PD (Identity Association—Prefix Delegation) can encapsulate IAPREFIX (Identity Association for prefixes)
- IAADDR and IAPREFIX could encapsulate address/prefix specific options (although none are presently specified by any IETF standard)
- Relay Message encapsulates relayed client or relayed messages. One message format is shared between Relay-Forward and Relay-Reply

Note: Full definition on these options can be found in RFC3315, which may be viewed at <http://www.ietf.org/rfc/rfc3315.txt>.

A note on IA_NA, IA_PD and IA_TA options:

- IAID is identity association for binding. It is a 32-bit value assigned by the client.
- IA_NA-options holds IAADDR options
- IA_PD is identical (except option code)
- IA_TA is similar, but has however no renewal (T1) or rebinding (T2) fields

An overview of the common DHCPv6 packet formats:

Figure 2. IA_NA Option (Identity Association - Non-temporary Address)

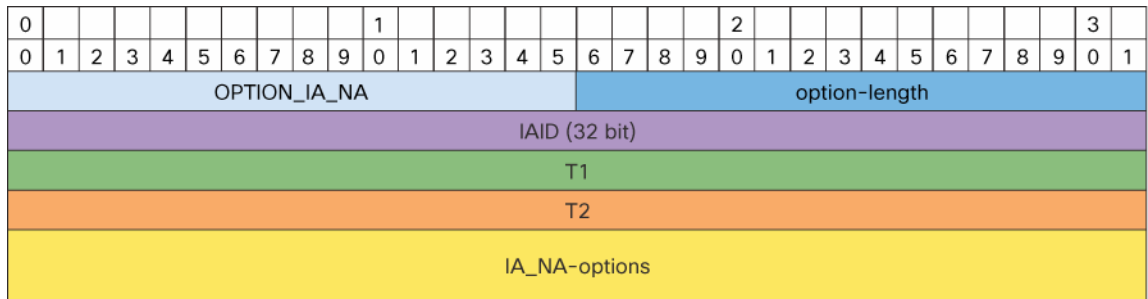


Figure 3. IAADDR Option (Identity Association Address)

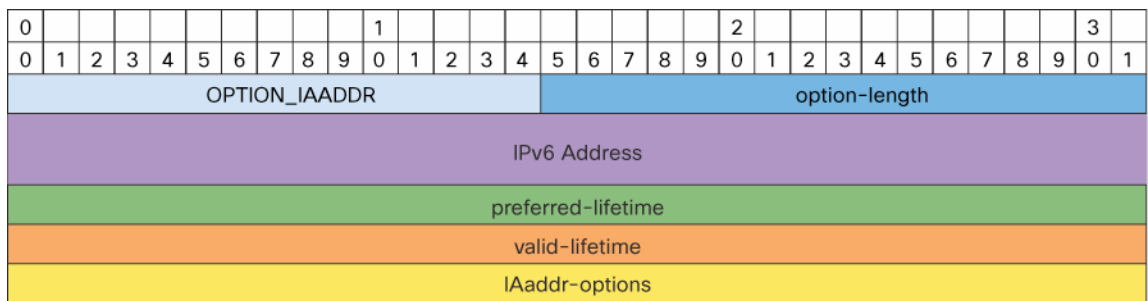


Figure 4. IAPREFIX Option (Identity Association for prefixes)

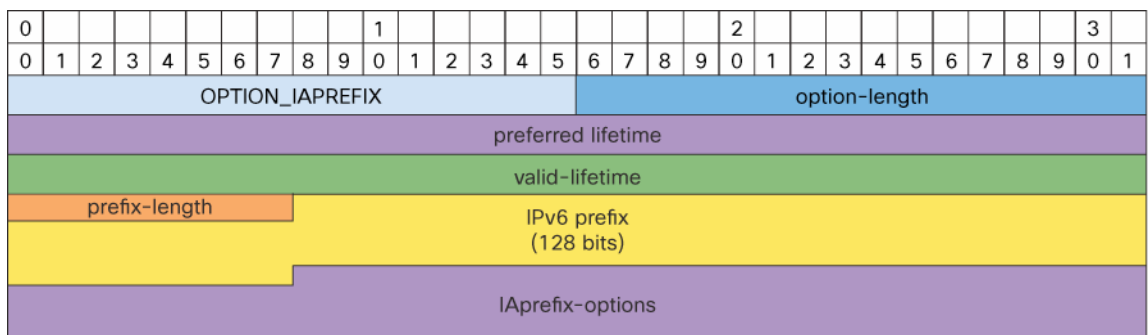
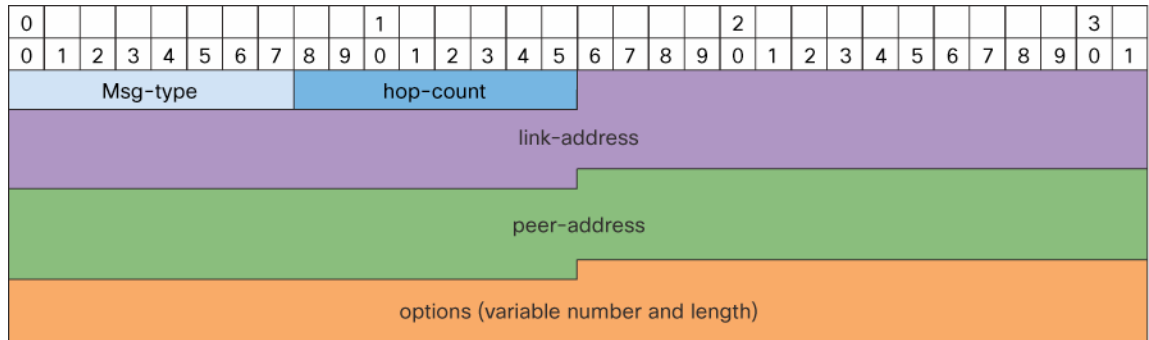


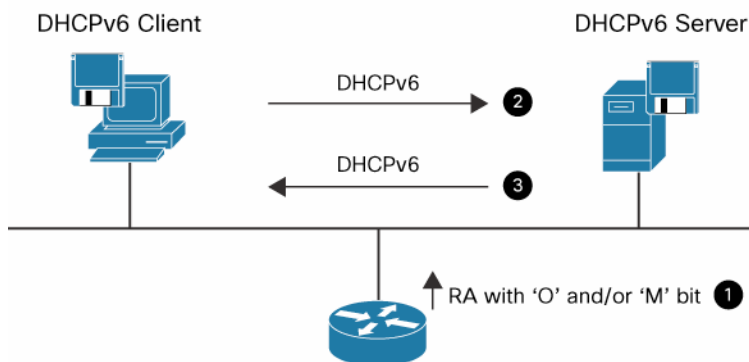
Figure 5. General Shared Relay Message Format



The entries within the shared Relay message format are defined as:

Relay-forward packet content	Relay-reply packet content
hop-count: Number of relay agents that have relayed this message. link-address: A global or unique local address that will be used by the server to identify the link on which the client is located. peer-address: The address of the client or relay agent from which the message to be relayed was received. Options: MUST include a "Relay Message option" and may include other options added by the relay agent (e.g. remote-id option).	hop-count: Copied from the Relay-forward message link-address: Copied from the Relay-forward message peer-address: Copied from the Relay-forward message options Options: MUST include a "Relay Message option" and may include other options

DHCPv6 Basic Operation



The traditional sequence of events is:

1. A router attached to a network will announce it as a router that is sending periodic RA's (Router Advertisements). If the router wishes the attached clients have to use DHCPv6 for acquiring an IPv6 address, it can signal that with setting the 'O' and 'M' bits in the Router Advertisement (RA). The two bits of importance within a Router Advertisement (RA) are:
 - a. M-bit: 1-bit "Managed address configuration" flag. When set, clients use DHCPv6 protocol for address configuration.
 - b. O-bit: 1-bit "Other stateful configuration" flag. When set, hosts use DHCPv6 to obtain 'other' (non-address) information.

2. On a client enabled with the DHCPv6 stack, the DHCP procedure is typically initiated when either the client receives a notification from the attached router to run DHCPv6 (by the 'O' and 'M' bits in the Router Advertisement (RA)), or if the client detects no directly connected routers. However, there's nothing to prohibit DHCPv6 to run always; it is just that it SHOULD be run if M or O bits are set.
3. A directly connected DHCPv6 server or client will reply to the request from the DHCPv6 client.

If however the client is a Cisco router trying to run DHCPv6-PD, then the parameters within the RA are not of critical importance to bootstrap the DHCPv6 process. In this case, the routers are manually configured to use DHCPv6. The DHCPv6-PD server can then decide to do Prefix Delegation with four messages, or it may proceed using only two messages, if rapid-commit is supported.

DHCPv6 clients and servers use UDP (ports 546/547) to exchange messages. The client will make use of Link Local addressing to send and receive DHCPv6 messages. DHCPv6 servers make use of the reserved link-local "ff02::1:2" (All DHCPv6 relay agents and servers) and site-local "ff05::1:3" (All DHCPv6 Servers) multicast addresses. A DHCP client transmits most messages to the reserved link-local "ff02::1:2" multicast address, so that the client does not need to be configured with the address or addresses of DHCP servers. However, in many situations the DHCP server will not be connected to a segment where its clients are connected. In these situations, a DHCP Relay Agent is used. The DHCP Relay agent must be connected to the segment of the client, and will relay the messages between the client and the server. The existence of a relay agent is transparent to the client. Cisco IOS routers can provide the function of DHCPv6 Relay Agent since release 12.3(11)T. Once a client has identified the existence of a DHCPv6 server it may start sending messages using unicast instead of multicast. The DHCPv6 Client-Server exchange can be completed by either a 2 or 4 message exchange which is described in the following section.

The next two examples introduce the fundamentals of the DHCPv6 two and four phase client and server negotiation. For documentation purposes the IA_PD option is used in this example related to Prefix Delegation (for example a CPE (Customer Premises Equipment) router acquiring IPv6 prefixes from the service provider DHCPv6 server). Later case-study examples will also be visualized with IA_PD options for prefix delegation. The identical same DHCPv6 2 or 4 phase negotiation can be used for IA_NA prefix configuration (for example when a host running a DHCPv6 client process wants to acquire IPv6 addresses and related information).

Client-server Exchanges Involving Two Messages

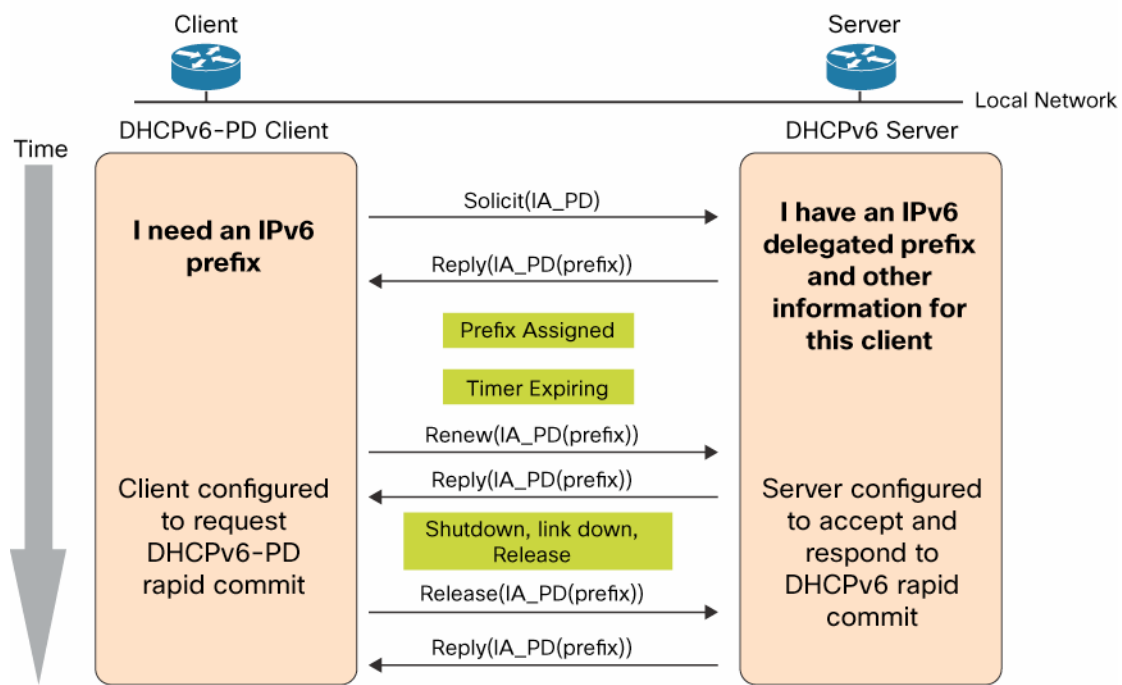
When a DHCP client does not need to have a DHCP server assign it IP addresses, the client can obtain configuration information such as a list of available DNS or NTP servers through a single message and reply exchange with a DHCP server. To obtain configuration information the client first sends an Information-Request message to ff02::1:2 (All Relay Agents and Servers). The server will respond with a Reply message containing the configuration information for the client.

This message exchange assumes that the client requires only configuration information and does not require the assignment of any IPv6 addresses. When a server has IPv6 addresses and other configuration information committed to a client, the client and server may be able to complete the exchange using only two messages, instead of four messages. In this case, the client sends a Solicit message to the ff02::1:2 requesting the assignment of prefixes and other configuration information. This message includes the Rapid Commit Option as an indication that the client is willing to accept an immediate Reply message from the server. A server that is willing to commit the assignment of addresses to the client immediately responds with a Reply message. The configuration information and the addresses in the Reply message are then immediately available for use by the

client. If a server is unwilling to allow the two message exchange, it responds as normal (this will be discussed later).

Each address assigned to the client has associated preferred and valid lifetimes specified by the server. To request an extension of the lifetimes assigned to an address, the client sends a Renew message to the server. The server sends a Reply message to the client with the new lifetimes, allowing the client to continue to use the address without interruption.

Figure 6. DHCPv6-PD Request Message Flows for Two Message Exchange



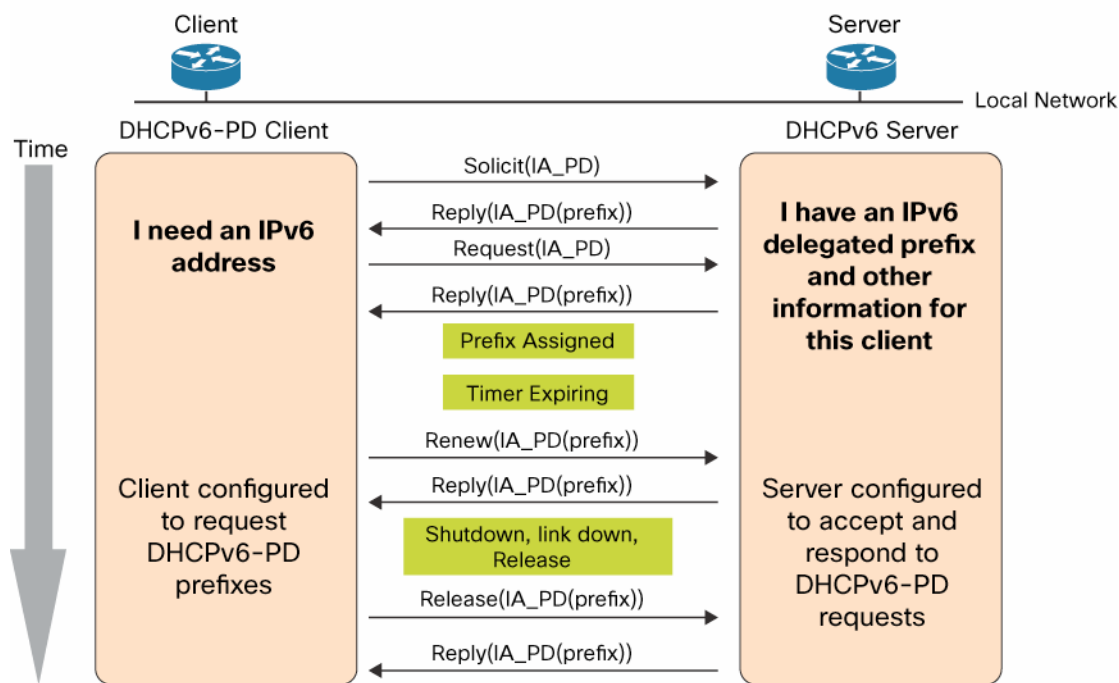
Client-server Exchanges Involving Four Messages

To request the assignment of one or more IPv6 addresses:

- A client first locates a DHCP server and then requests the assignment of addresses and other configuration information from the server. The client sends a Solicit message to the ff02::1:2 address to find available DHCP servers.
- Any server that can meet the client's requirements responds with an Advertise message.
- The client then chooses one of the servers and sends a Request message to the server asking for confirmed assignment of addresses and other configuration information.
- The server responds with a Reply message that contains the confirmed addresses and configuration.

In same manner as documented in previous section, the client sends a Renew message to the server to extend the lifetimes associated with its addresses, allowing the client to continue to use those addresses without interruption.

Figure 7. DHCPv6-PD Request Message Flows for Four Message Exchange

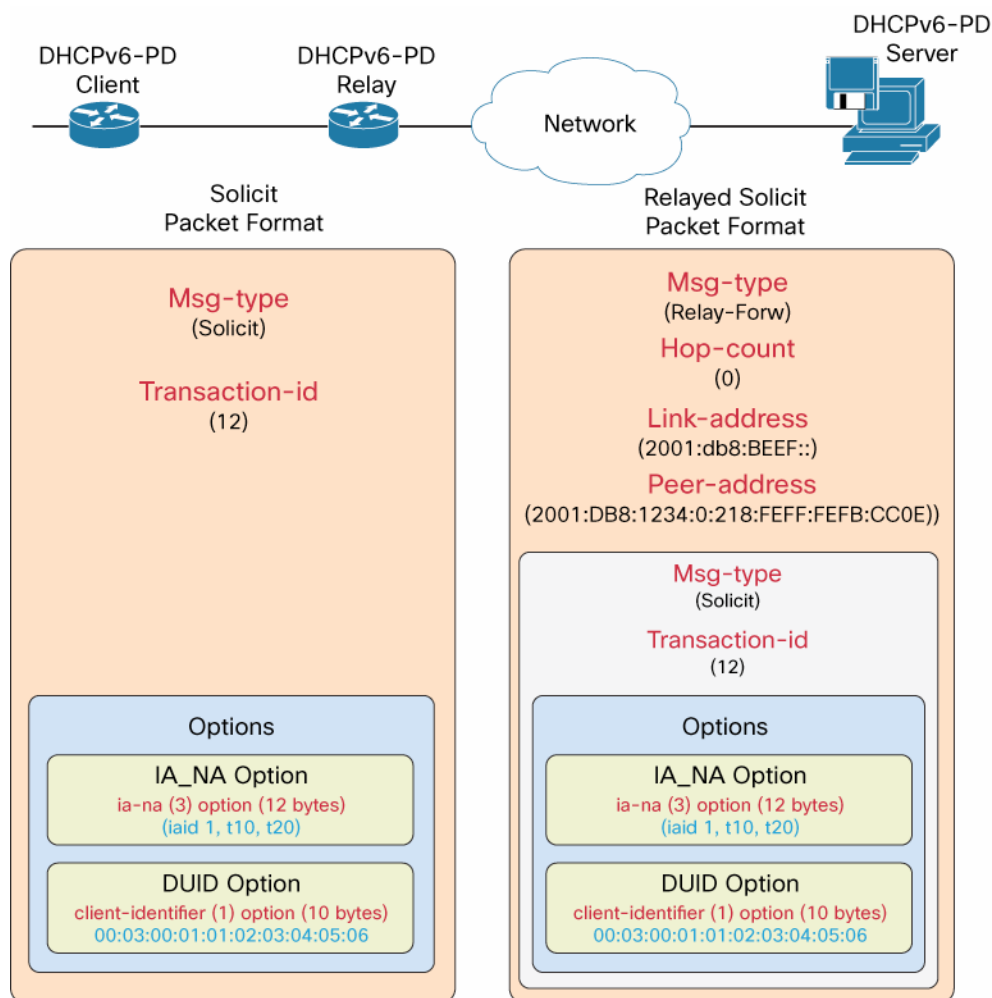


DHCPv6 Relay Messages

In many situations, the DHCPv6 server is not always directly connected to each and any potential client due to practical and network management reasons. It is however required to have an on-link presence of the DHCP server entity because DHCPv6 basic operation between client and server will use link-local communication. This entity can either be a DHCPv6 Server, or if a server is not present, it will be a DHCPv6 Relay Agent. A relay agent intercepts the link-local DHCPv6 messages and forwards these to a valid DHCPv6 server available within the networking infrastructure. When a relay agent "relays" messages it may be configured to with a list of destination addresses, which may include unicast addresses, the All_DHCP_Servers multicast address, or other addresses selected by the network administrator. If the relay agent relays messages to the All_DHCP_Servers multicast address or other multicast addresses, it sets the Hop Limit field to 32.

When a DHCPv6 server decides to respond to a relayed client message, it composes a reply with inclusion of information available within the relayed client message. In more detail, the server will copy some relay agent options (it will copy, for example, the Interface-Id option). The server will send the reply to the source address of the received packet on port 547 (relay port). This IPv6 source address is the address of the last relay agent within the potential chain of relay agents. The relay agent may now forward the packet onwards to either the next downstream relay-agent or directly to the actual DHCPv6 client if it is directly attached to the relay-agent. For the relay-agent to forward the reply it uses the 'peer-address' field in the received relay-reply as destination address, while the link-address and/or Interface-ID option determines the interface on which to forward the relayed message. The forwarded message is sent to port 547 (if encapsulated message is Relay-forw) otherwise port 546 is used.

Figure 8. Initial Solicit and Resulting Relayed Solicit Message



There may be a series of relay agents concatenated behind one another. The impact this will have is that for each relay agent there is an additional set of information embedded in the relayed DHCPv6 packet while encapsulating the original packet. This additional encapsulation (message-type, hop-count, link-address and peer-address) by the additional relay is similar to the previous diagram. This is in contrast with the behavior of what “ip helper address” is bringing to DHCPv4, where “ip helper address” can simply forward packets to a single IPv6 destination address.

The relay agent must be configured with a valid IPv6 address of the DHCPv6 server available within the network infrastructure (or the DHCPv6 server may be reachable via the site-local ff05::1:3 (All DHCPv6 Servers) multicast address). This can be done as demonstrated in the following example on a Cisco router functioning as a DHCPv6 Relay:

```
!
interface FastEthernet6/0
  ipv6 address 2001:DB8:BEEF::1/64
  ipv6 enable
```

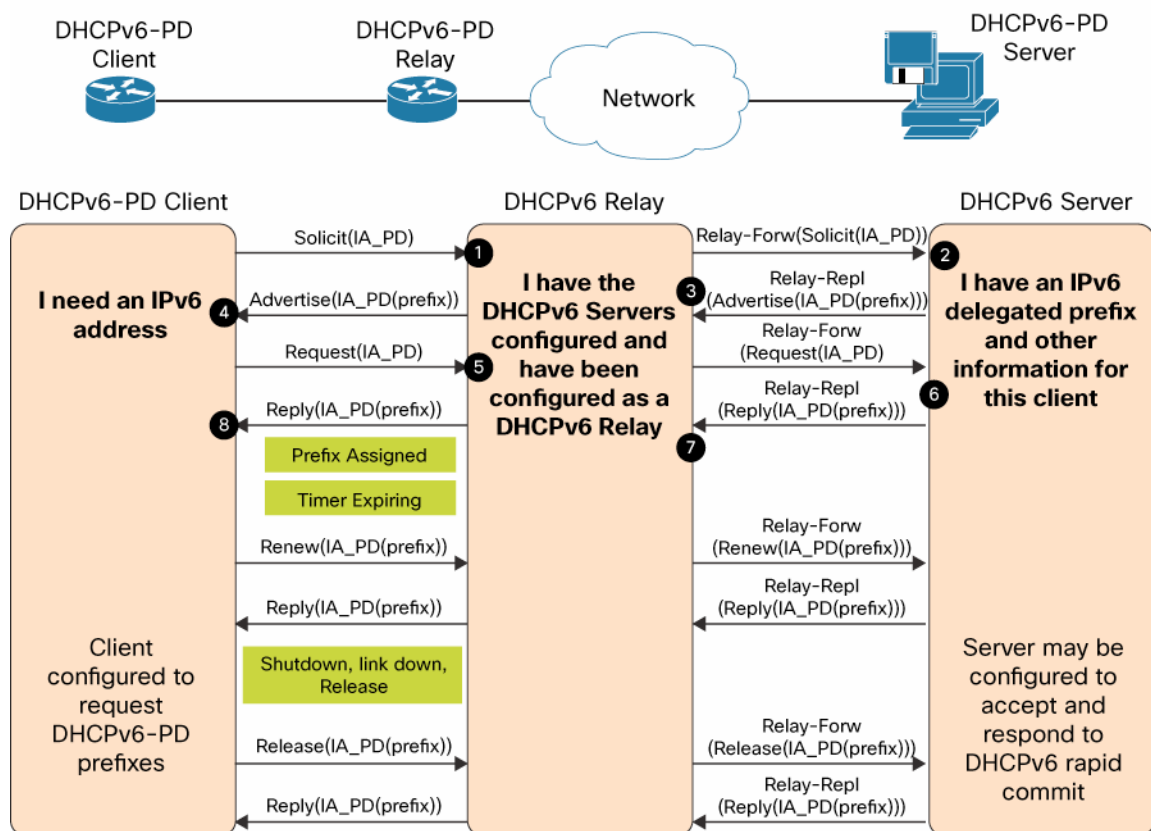
ipv6 dhcp relay destination 2001:DB8:1234:0:218:FEFF:FEFB:CC0E

!

Note: It is not required to configure this command on every router along the path between the client and server. It is ONLY required on the router functioning as the DHCPv6 relay agent.

When analyzing the packet exchange between the actual DHCPv6 client (in this example a DHCPv6-PD client is assumed), DHCPv6 relay agent, and DHCPv6 server, the following packet flow can be seen (assuming Client-Server exchange involves four messages):

Figure 9. Message Exchanged for Relay Based Implementation



The packet trace content from the above visualized packet IA_PD exchange is shown in the following output:

1- Solicit		2 – Relay-Forward Solicit	
IPv6 Header		IPv6 Header	
SourceAddress	fe80::200:ff:fe00:a2a2	SourceAddress	2001:db8:ffff:100:200:ff:fe00:a4a4
DestinationAddress	ff02::1:2	DestinationAddress	2001:db8:ffff:100:209:6bff:fea0:407a
DHCPv6 Solicit		DHCPv6 Relay-Forward	
Identifier	100	LinkAddr	2001:db8:ffff:101:200:ff:fe00:a5a5
Client ID option		PeerAddr	fe80::200:ff:fe00:a2a2
DHCPv6_DUID_LL_T_Ether		Interface ID option	
Type	1	Identifier	"gi 0/1"
HardwareType	1	Remote ID option	
Time	300000	Identifier	0x020a00000c00000202000000
LinkLayerAddress	00:00:00:00:a2:a2	Relay Message option	
IA_PD option		DHCPv6 Solicit	
Identifier	303030	Identifier	100
Time1	5000	Client ID option	
Time2	8000	DHCPv6_DUID_LL_T_Ether	
		Type	1
		HardwareType	1
		Time	300000
		LinkLayerAddress	00:00:00:00:a2:a2
		IA_PD option	
		Identifier	303030
		Time1	5000
		Time2	8000

3 – Relay-Reply Advertise	
IPv6 header	
SourceAddress	2001:db8:ffff:100:209:6bff:fea0:407a
DestinationAddress	2001:db8:ffff:100:200:ff:fe00:a4a4
DHCPv6 Relay-Reply	
LinkAddr	2001:db8:ffff:101:200:ff:fe00:a5a5
PeerAddr	fe80::200:ff:fe00:a2a2
Interface ID option	
Identifier	"gi 0/1"
Relay Message option	
DHCPv6 Advertise	
Identifier	100
Client ID option	
DHCPv6_DUID_LL_T_Ether	
Type	1
HardwareType	1
Time	300000
LinkLayerAddress	00:00:00:00:a2:a2
Server ID option	
DHCPv6_DUID_LL_T_Ether	
Type	1
HardwareType	1
Time	1138147733
LinkLayerAddress	00:02:8a:4b:02:d2
IA_PD option	
Identifier	303030
Time1	5400
Time2	8640
IA_Prefix option	
PreferredLifetime	10800
ValidLifetime	21600
PrefixLength	48
Prefix	3ffe:ffff:1000::
Server Preference option	
Preference	10

4 – Advertise

IPv6 Header
SourceAddress fe80::200:ff:fe00:a5a5
DestinationAddress fe80::200:ff:fe00:a2a2
DHCPv6 Advertise
Identifier 100
Client ID option
DHCPv6_DUID_LL_T_Ether
Type 1
HardwareType 1
Time 300000
LinkLayerAddress 00:00:00:00:a2:a2
Server ID option
DHCPv6_DUID_LL_T_Ether
Type 1
HardwareType 1
Time 1138147733
LinkLayerAddress 00:02:8a:4b:02:d2
IA_PD option
Identifier 303030
Time1 5400
Time2 8640
IA_Prefix option
PreferredLifetime 10800
ValidLifetime 21600
PrefixLength 48
Prefix 3ffe:ffff:1000::
Server Preference option
Preference 10

!"#\$%&'%(

!

IPv6 Header
SourceAddress fe80::200:ff:fe00:a2a2
DestinationAddress ff02::1:2
DHCPv6 Request
Identifier 100
Client ID option
DHCPv6_DUID_LL_T_Ether
Type 1
HardwareType 1
Time 300000
LinkLayerAddress 00:00:00:00:a2:a2
Server ID option
DHCPv6_DUID_LL_T_Ether
Type 1
HardwareType 1
Time 1138147733
LinkLayerAddress 00:02:8a:4b:02:d2
IA_PD option
Identifier 303030
Time1 5400
Time2 8640
IA_Prefix option
PreferredLifetime 10000
ValidLifetime 20000
PrefixLength 48
Prefix 3ffe:ffff:1000::

6 – Relay-Forward Request

IPv6 Header
SourceAddress 2001:db8:ffff:100:200:ff:fe00:a4a4
DestinationAddress 2001:db8:ffff:100:209:6bff:fea0:407a
DHCPv6 Relay-Forward
LinkAddr 2001:db8:ffff:101:200:ff:fe00:a5a5
PeerAddr fe80::200:ff:fe00:a2a2
Interface ID option
Identifier "gi 0/1"
Remote ID option
Identifier 0x020a00000c00000202000000
Relay Message option
DHCPv6 Request
Identifier 100
Client ID option
DHCPv6_DUID_LL_T_Ether
Type 1
HardwareType 1
Time 300000
LinkLayerAddress 00:00:00:00:a2:a2
Server ID option
DHCPv6_DUID_LL_T_Ether
Type 1
HardwareType 1
Time 1138147733
LinkLayerAddress 00:02:8a:4b:02:d2
IA_PD option
Identifier 303030
Time1 5400
Time2 8640
IA_Prefix option
PreferredLifetime 10000
ValidLifetime 20000
PrefixLength 48
Prefix 3ffe:ffff:1000::

7 – Relay-Reply Reply

```
IPv6 header
  SourceAddress      2001:db8:ffff:100:209:6bff:fea0:407a
  DestinationAddress 2001:db8:ffff:100:200:ff:fe00:a4a4
DHCPv6 Relay-Reply
  LinkAddr           2001:db8:ffff:101:200:ff:fe00:a5a5
  PeerAddr           fe80::200:ff:fe00:a2a2
  Interface ID option
    Identifier        "gi 0/1"
  Relay Message option
    DHCPv6 Reply
      Client ID option
        DHCPv6_DUID_LL_T_Ether
          Type         1
          HardwareType 1
          Time          300000
          LinkLayerAddress 00:00:00:00:a2:a2
      Server ID option
        DHCPv6_DUID_LL_T_Ether
          Type         1
          HardwareType 1
          Time          1138147733
          LinkLayerAddress 00:02:8a:4b:02:d2
      IA_PD option
        Identifier     303030
        Time1           5400
        Time2           8640
      IA_Prefix options
        PreferredLifetime 10800
        ValidLifetime     21600
        PrefixLength       48
        Prefix             3ffe:ffff:1000::
```

8 – Reply

```
IPv6 Header
  SourceAddress      fe80::209:6bff:fea0:407a
  DestinationAddress fe80::200:ff:fe00:a2a2
DHCPv6 Reply
  Client ID option
    DHCPv6_DUID_LL_T_Ether
      Type         1
      HardwareType 1
      Time          300000
      LinkLayerAddress 00:00:00:00:a2:a2
  Server ID option
    DHCPv6_DUID_LL_T_Ether
      Type         1
      HardwareType 1
      Time          1138147733
      LinkLayerAddress 00:02:8a:4b:02:d2
  IA_PD option
    Identifier     303030
    Time1           5400
    Time2           8640
  IA_Prefix options
    PreferredLifetime 10800
    ValidLifetime     21600
    PrefixLength       48
    Prefix             3ffe:ffff:1000::
```

Useful DHCPv6 Deployment Features and Options

Remote-id Option

Service provider DHCPv4 deployments make extensive use of Option 82 to help identify the subscriber and assign addresses. Similar needs arise when including DHCPv6 in large scale deployments. When a relay-agent is forwarding DHCPv6 client messages, it may insert additional parameters and options before relaying the message to a DHCPv6 server. A particular option of interest is the 'remote-id' option. This option will help the DHCPv6 server to identify the correct parameters to reply back to the DHCPv6 client. This option is the IPv6 counterpart of the IPv4 (DHCPv4) Relay Agent Option's Remote-ID sub-option as specified in [RFC 3046](#). A full definition of the IPv6 remote-id option is found at [RFC4649](#). This option is especially useful for an ISP because it allows the ISP to allocate a client prefix based upon an administrative identification, instead of a DUID or other parameter values.

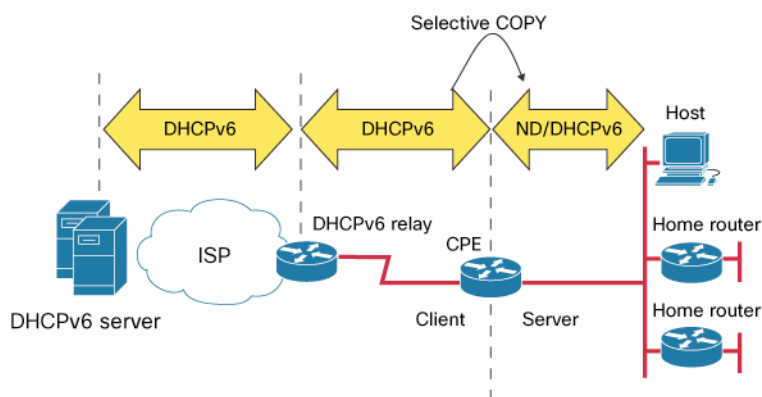
There is no direct show command on the router to show the assigned remote-id option added to a relayed DHCPv6 message. However, it can be found with "debug ipv6 dhcp relay" and "debug ipv6 dhcp detail" or it can be found on the DHCPv6 Server supporting the remote-id option for IPv6.

Information Refresh Time Option

This option is a useful aid when deploying DHCPv6 based services and is standardized by the IETF in RFC4242. The refresh option can specify an upper boundary for the length of time a client should wait before refreshing information retrieved from DHCP for IPv6. This option is used with stateless DHCP for IPv6, because there are no addresses or other entities with lifetimes that can tell the client when to contact the DHCP for IPv6 server to refresh its configuration and is supported from Cisco IOS 12.4(15)T onward.

Hierarchical DHCPv6

A home access router for an IPv6 enabled household can be both a DHCPv6 client and server. The client function will retrieve configuration parameters from the provider in stateful or stateless DHCPv6. In either case, the ISP side DHCPv6 server can provide configuration parameters such as DNS server addresses, domain names, NTP server, etc. to the DHCPv6 client on the IPv6 enabled household access router. These configuration parameters are traditionally specific to an ISP and may alter over time.



In addition to being a DHCPv6 client (towards the ISP), the access router can act as a DHCPv6 server towards the home network. For example, Neighbor Discovery followed by stateless or stateful DHCPv6 can occur on the link between access router and the home devices. In some cases, the information to be provided to the home network is the same information obtained from the ISP side DHCPv6 server. Because this information can be dynamically

changed, it makes sense to have the DHCPv6 server function on the access router inherit the received configuration parameters from the DHCPv6 server from the ISP. Therefore, the DHCP for IPv6 component on the CPE allows automatic importing of configuration parameters from the DHCP for IPv6 client to the DHCP for IPv6 server pool.

Deploying DHCPv6 Based Access Services

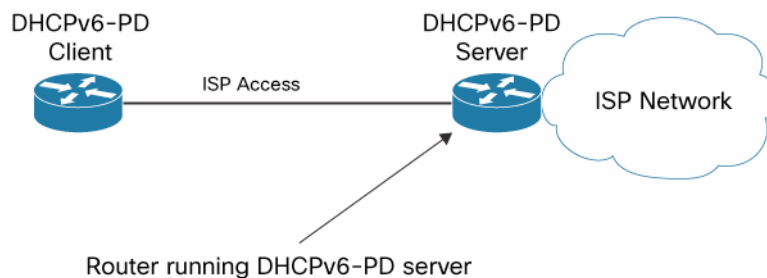
Introduction

Deploying DHCPv6 based access services can be achieved in a variety of manners. For the deployment models discussed in this paper, the assumed base requirement for a CPE is to receive an IPv6 address-range from its service provider while the local loop media used is Ethernet based. It is also assumed that the CPE's have support for DHCPv6-PD. This IPv6 address range can be used by the CPE to dynamically address the site and its interfaces.

When looking into the provisioning and deployment models of the DHCPv6-PD services, three main models can be identified:

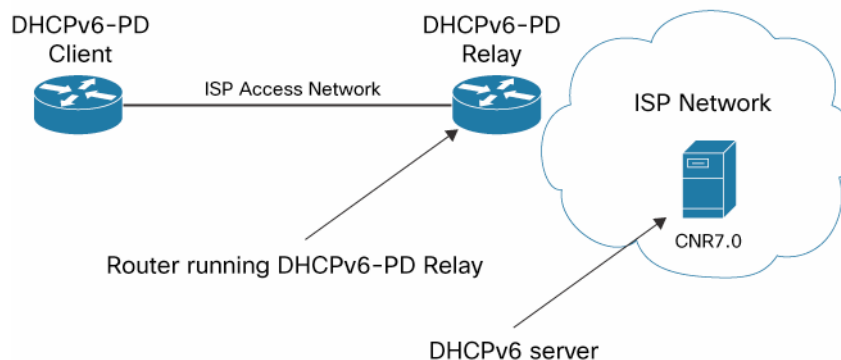
- **Deployment model 1:** DHCPv6-PD Server at the Service Provider Edge Router

This is maybe the simplest model, but can have its limits due to operational maintenance and provisioning overhead. With this deployment model the service provider edge router is directly delivering the DHCPv6-PD "server" service. This means that there is no need for an external DHCPv6 server beyond the service provider edge router, however, each ISP network edge router may need a unique DHCPv6-PD configuration with a configuration in place to assign IPv6 address space to each of its customers.



- **Deployment mode 2:** DHCPv6-PD Relay at the Provider Edge Router

This provisioning model is based around a centralized DHCPv6-server. In contrast with the first model, each ISP edge router will serve as a DHCPv6-relay agent. The required DHCPv6 configuration for this function on each of the DHCPv6 relay-agents can be quite simple and similar. The bulk of the DHCPv6 configuration, provisioning and tracking is done on the DHCPv6 server. CNR7.0 (Cisco Network Registrar 7.0) has in-depth support IPv6 technology. If this deployment model is used, then the ISP edge router will forward (known as Relaying) DHCPv6-PD messages between the DHCPv6-PD client and the DHCPv6-PD server.

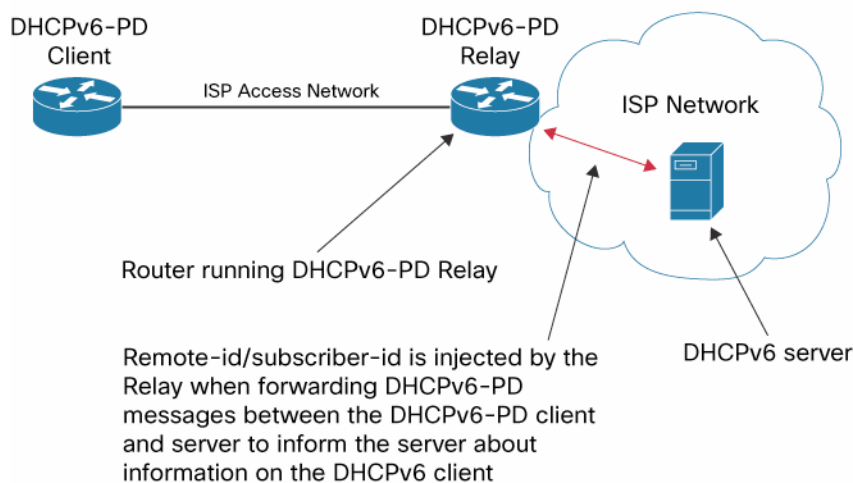


The principle of hierarchical DHCPv6 is powerful when hosts request additional information need beyond simply IPv6 addresses. A Cisco IOS CPE can be both a DHCPv6 Server and Client simultaneously. Through the DHCPv6 client, the CPE can learn parameters as domain name, DNS servers, SNTP servers, etc. from the central DHCPv6 server, and by acting as a DHCPv6 Server announce these parameters to a set of locally connected hosts. These hosts may utilize DHCPv6 to learn their IPv6 addresses, and in addition, use DHCPv6 to get information about the “other” parameters. This full process happens dynamically and without user intervention. In this case, the CPE DHCPv6 server functionality keeps track of the DHCPv6 client bindings and refreshes the bindings periodically. However, hosts may alternatively use SLAAC (Stateless Address Auto-Configuration), and get an IPv6 Address based upon the received CPE RA's (Router Advertisements), while using DHCPv6 to get the “other” parameters. With this design the CPE DHCPv6 server functionality does NOT need to keep track of the IPv6 to DHCPv6 client bindings, and there is no need to refresh the binding periodically. This is especially useful in situations with potential for a large amount of clients (wireless mobile phones connecting to the internet), or where bandwidth is an expensive resource.

- **Deployment model 3:** DHCPv6-PD Relay at the Provider Edge Router and DHCPv6 Remote-id Option

This third deployment model is quite similar to the previous model because the configuration, provisioning and tracking is done on a centralized DHCPv6 server. The difference is in the methodology on how IPv6 prefixes are assigned to the DHCPv6-clients. In the 2nd model, the assigned DHCPv6-PD addresses are based around the DUID (DHCPv6 Unique ID) and the location where the DHCPv6 client is accessing the service provider network. If an end-user changes his CPE device due to an upgrade or due a break/fix, then the provisioned address and tracking could become complicated because some parameters have changed at the customer side and the management system must accommodate that. In this last provisioning model, the assigned IPv6 address space is done based upon the remote-id options, which were injected by the DHCPv6-PD relay router. The remote-id gives the DHCPv6-server an indication to which service provider edge router any DHCPv6-client is connected and can simply, based upon these values, assign an IPv6 address-space. This has as benefit that IPv6 provisioning is completely independent of the DUID used by the DHCPv6-client, while at the same time the assigned IPv6 address is independent of the CPE used by the end-customer.

The remote-id is a value assigned automatically by the Cisco DHCPv6 relay.



DHCPv6-PD Client Configuration Consideration

The configuration for each of the DHCPv6-PD deployment models discussed are identical to each other. The configuration from the DHCPv6 client is fully independent and invisible from the DHCPv6-client perspective. During the DHCPv6 technology description both the client-server message exchanged were discussed with 2 and 4 messages. The client can be instructed through configuration to run DHCPv6 in either '2' or '4' messages. During the examples documented for each deployment model, the default of '4' messages is used, as it covers all steps of the DHCPv6 communication procedure. However for generating less messages for DHCPv6-PD, a '2' message exchange can be a better choice for implementation. The CPE utilized for this paper is a Cisco1841 ISR. For each of the deployment models the following Cisco IOS configuration is used on the CPE router:

```
!
hostname ecmd-1841-1
!
ipv6 unicast-routing
! Enable IPv6 Unicast Routing
ipv6 cef
! Enable IPv6 CEF switching
!
!
interface Loopback100
no ip address
ipv6 address PREFIX_1 ::1/64
! Configures the IPv6 address of the Loopback based upon the DHCPv6 received address
ipv6 enable
! enable IPv6 processing on this interface
!
interface FastEthernet0/0
description Link towards the Service Provider
```

```
ip address 11.11.11.1 255.255.255.252
```

```
speed 100
```

```
half-duplex
```

```
ipv6 address autoconfig default
```

! The IPv6 address is automatically learned and based upon the received Router Advertisement from its upstream Service Provider router. The 'default' keyword means that the CPE will learn the default route through the upstream routers RA (Router Advertisement) messages and install a default IPv6 route in the IPv6 routing table.

```
ipv6 enable
```

! enable IPv6 processing on this interface

```
ipv6 dhcp client pd PREFIX_1
```

! Enables IPv6 DHCPv6-PD on the CPE

!

This configuration has as usage to serve as demonstration of the DHCPv6-PD technology operation and can be used in a real DHCPv6 deployment. It is configuration which allows the CPE to be fully dynamic without additional user interaction. With this simple configuration, the CPE router will dynamically learn from the upstream 'DHCPv6 server' its delegated IPv6 address range and abstract it as "PREFIX_1". In the example below, the "PREFIX_1" stands for following delegated IPv6 prefix "2001:DB8:1::/48". It is seen that the server, in addition to an IPv6 address range, also provided information about both a DNS server (2001:DB8::1) and the domain name (ECMD.com), together with some timers related to the delegated prefix.

```
ecmd-1841-1#show ipv6 dhcp interface fast 0/0
```

```
FastEthernet0/0 is in client mode
```

```
State is OPEN
```

```
Renew will be sent in 3d10h
```

```
List of known servers:
```

```
Reachable via address: FE80::21A:A1FF:FE7A:46A8
```

```
DUID: 00030001001AA17A461B
```

```
Preference: 0
```

```
Configuration parameters:
```

```
IA PD: IA ID 0x00030001, T1 302400, T2 483840
```

```
Prefix: 2001:DB8:1::/48
```

```
preferred lifetime 604800, valid lifetime 2592000
```

```
expires at Feb 27 2008 10:59 AM (2587948 seconds)
```

```
DNS server: 2001:DB8::1
```

```
Domain name: ECMD.COM
```

```
Prefix name: PREFIX_1
```

```
Rapid-Commit: disabled
```

```
ecmd-1841-1#
```

From the above, the CPE DUID can be found (00030001001AA17A461B). This value is traditionally used by the DHCPv6 server to link the delegated IPv6 address with the CPE device. At the moment Rapid-Commit is disabled, this means that the CPE is using 4 messages to obtain its delegated IPv6 address range. If Rapid-Commit is supported by the DHCPv6 server, then this CPE can be enabled with appending the "rapid-commit" to the DHCPv6 prefix delegation command on the IOS based CPE:

```

!
interface FastEthernet0/0
ipv6 dhcp client pd PREFIX_1 rapid-commit
! Enables IPv6 DHCPv6-PD on the CPE with support for Rapid-Commit
!

```

In the current example, the upstream service provider supports DHCPv6-PD and has configured a global IPv6 address on the edge router connected to the CPE. With the shown CPE configuration, the following IPv6 addresses are seen on the router interfaces if the service provider runs DHCPv6-PD and announces RA's, which contain a global IPv6 address prefix:

```

ecmd-1841-1#show ipv6 interface brief
FastEthernet0/0                [up/up]
FE80::21A:2FFF:FE87:5602
2001:BEEF::21A:2FFF:FE87:5602
FastEthernet0/1                [up/up]
Serial0/0/0                    [administratively down/down]
Serial0/0/1                    [administratively down/down]
Serial0/0/2                    [administratively down/down]
Serial0/0/3                    [administratively down/down]
Loopback100                   [up/up]
FE80::21A:2FFF:FE87:5602
2001:DB8:1::1
ecmd-1841-1#

```

If the CPE has in addition to the loopback interface, a few interfaces with IPv6 capable hosts, then these interfaces can have a derived IPv6 address based upon the received "PREFIX_1". If for example, FastEthernet0/1 would have IPv6 capable hosts connected then the following configuration could be added to the CPE template so that these hosts can obtain IPv6 addresses, based upon the delegated "PREFIX_1". In this configuration is the "PREFIX_1" which stands for IPv6 prefix 2001:DB8:1::/48. With the below configuration snip, the following 16 bits "12AB:" written in hexadecimals, are appended to this IPv6 prefix to make the IPv6 address on FastEthernet0/1 as "2001:db8:1:12AB::1/64".

```

!
interface FastEthernet0/1
  description Connection to the local LAN segment
  no ip address
  ipv6 address PREFIX_1 :12AB::1/64
! Configures the IPv6 address of the Loopback based upon the DHCPv6 received address
  ipv6 enable
! enable IPv6 processing on this interface
!

```

If the IPv6 capable hosts attached on FastEthernet0/1 support DHCPv6 technology, then the configuration of the CPE can be further extended. When using a CPE running Cisco IOS, it is possible to use hierarchical DHCPv6.

This means that parameters the CPE learned through DHCPv6 from its upstream service provider can be relayed to the hosts running DHCPv6 clients, while attached to FastEthernet0/1 on the CPE.

The CPE configuration remains independent from any deployment model used at the service provider, and a simple and straightforward configuration can be used on the CPE.

Deployment Model 1: DHCPv6-PD Server at the Service Provider Edge Router

This deployment model has its usage where the organization or service provider trying to use DHCPv6-PD does not have a centralized DHCPv6 server. This deployment model has as consequence that all DHCPv6-PD server related configuration has to be made upon the router connected to the CPE device. The service provider edge router will have to decide which IPv6 prefix should be delegated to the CPE, and will have to keep track of the list of delegated prefixes.

For the example, the edge router used here is a Cisco 7200/NPE-G2.

```
!  
ipv6 unicast-routing  
ipv6 cef  
ipv6 dhcp pool ECMD_TEST  
prefix-delegation 2001:DB8:1::/48 00030001001A2F875602  
dns-server 2001:DB8::1  
domain-name ECMD.COM  
! Configuration of the available pool of prefixes linked to a DUID. It is  
important to know the DUID of the CPE so that correct mapping can be achieved  
!  
!  
interface FastEthernet6/0  
description Connection towards the CPE (to DHCPv6-PD Client)  
ip address 11.11.11.2 255.255.255.252  
duplex half  
ipv6 address 2001:BEEF::1/64  
ipv6 enable  
ipv6 dhcp server ECMD_TEST  
! This client will use the DHCPv6-PD pool "ECMD_TEST" to assign IPv6 prefixes to  
the CPE  
!
```

From the configuration, it can be seen that to map a certain IPv6 prefix to a CPE, the DUID of the CPE must be known. The structure of the DUID used by a Cisco router has been discussed earlier. On the CPE, the DUID can be retrieved by executing following show command:

```
ecmd-1841-1#sho ipv6 dhcp  
This device's DHCPv6 unique identifier(DUID): 00030001001A2F875602  
ecmd-1841-1#
```

The above example has the assumption that each CPE DUID is known to the service provider, which is not always a practical reality. An alternative solution is to configure on the service provider Edge Router a dedicated and unique DHCPv6 address pool used for Prefix Delegation, and this for each interface which has a CPE connected.

The following provides a possible configuration template when a service provider does not know the DUID from each CPE and would like use the service provider Edge Router as DHCPv6-PD server:

```
int FastEthernet3/0
ipv6 dhcp server SERV1
!
ipv6 dhcp pool SERV1
  prefix-delegation pool POULE
!
ipv6 local pool POULE 2001:DB8:1::/48 48
```

With the Router configuration shown the following debugging is seen on CPE and the router running DHCPv6-PD Server:

CPE: Sending 'Solicit'

```
*Jan 28 10:59:32.616: IPv6 DHCP: Sending SOLICIT to FF02::1:2 on FastEthernet0/0
*Jan 28 10:59:32.616: IPv6 DHCP: detailed packet contents
*Jan 28 10:59:32.616:   src FE80::21A:2FFF:FE87:5602
*Jan 28 10:59:32.616:   dst FF02::1:2 (FastEthernet0/0)
*Jan 28 10:59:32.616:   type SOLICIT(1), xid 3795614
*Jan 28 10:59:32.616:   option ELAPSED-TIME(8), len 2
*Jan 28 10:59:32.616:     elapsed-time 3122
*Jan 28 10:59:32.616:   option CLIENTID(1), len 10
*Jan 28 10:59:32.616:     00030001001A2F875602
*Jan 28 10:59:32.616:   option ORO(6), len 6
*Jan 28 10:59:32.616:     IA-PD,DNS-SERVERS,DOMAIN-LIST
*Jan 28 10:59:32.616:   option IA-PD(25), len 12
*Jan 28 10:59:32.616:     IAID 0x00030001, T1 0, T2 0
! Note: The CPE asks about the available DHCPv6 servers on the FastEthernet link
```

DHCPv6-PD Router: Receiving of 'Solicit'

```
Jan 28 02:18:55.612: IPv6 DHCP: Received SOLICIT from FE80::21A:2FFF:FE87:5602 on
FastEthernet6/0
Jan 28 02:18:55.612: IPv6 DHCP: detailed packet contents
Jan 28 02:18:55.612:   src FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)
Jan 28 02:18:55.612:   dst FF02::1:2
Jan 28 02:18:55.612:   type SOLICIT(1), xid 3795614
Jan 28 02:18:55.612:   option ELAPSED-TIME(8), len 2
Jan 28 02:18:55.612:     elapsed-time 3122
Jan 28 02:18:55.612:   option CLIENTID(1), len 10
Jan 28 02:18:55.612:     00030001001A2F875602
Jan 28 02:18:55.612:   option ORO(6), len 6
Jan 28 02:18:55.612:     IA-PD,DNS-SERVERS,DOMAIN-LIST
Jan 28 02:18:55.612:   option IA-PD(25), len 12
Jan 28 02:18:55.612:     IAID 0x00030001, T1 0, T2 0
! Note: The Solicit requests from the CPE arrives at the Service Provider router
configured as DHCPv6-PD server
```

DHCPv6-PD Router: Sending of 'Advertise'

Jan 28 02:18:55.612: IPv6 DHCP: Sending ADVERTISE to FE80::21A:2FFF:FE87:5602 on FastEthernet6/0

Jan 28 02:18:55.612: IPv6 DHCP: detailed packet contents

Jan 28 02:18:55.612: src FE80::21A:A1FF:FE7A:46A8

Jan 28 02:18:55.612: dst FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)

Jan 28 02:18:55.612: type ADVERTISE(2), xid 3795614

Jan 28 02:18:55.612: option SERVERID(2), len 10

Jan 28 02:18:55.612: 00030001001AA17A461B

Jan 28 02:18:55.612: option CLIENTID(1), len 10

Jan 28 02:18:55.612: 00030001001A2F875602

Jan 28 02:18:55.612: option DNS-SERVERS(23), len 16

Jan 28 02:18:55.612: 2001:DB8::1

Jan 28 02:18:55.612: option DOMAIN-LIST(24), len 10

Jan 28 02:18:55.612: ECMD.COM

Jan 28 02:18:55.612: option IA-PD(25), len 41

Jan 28 02:18:55.612: IAID 0x00030001, T1 302400, T2 483840

Jan 28 02:18:55.612: option IAPREFIX(26), len 25

Jan 28 02:18:55.612: preferred 604800, valid 2592000, prefix 2001:DB8:1::/48

! Note: The Service Provider edge router configured as DHCPv6-PD device replies to the solicit message from the CPE by announcing him as a valid DHCPv6-PD server for this CPE

CPE: Receiving of the 'Advertise'

*Jan 28 10:59:32.616: IPv6 DHCP: Received ADVERTISE from FE80::21A:A1FF:FE7A:46A8 on FastEthernet0/0

*Jan 28 10:59:32.620: IPv6 DHCP: detailed packet contents

*Jan 28 10:59:32.620: src FE80::21A:A1FF:FE7A:46A8 (FastEthernet0/0)

*Jan 28 10:59:32.620: dst FE80::21A:2FFF:FE87:5602

*Jan 28 10:59:32.620: type ADVERTISE(2), xid 3795614

*Jan 28 10:59:32.620: option SERVERID(2), len 10

*Jan 28 10:59:32.620: 00030001001AA17A461B

*Jan 28 10:59:32.620: option CLIENTID(1), len 10

*Jan 28 10:59:32.620: 00030001001A2F875602

*Jan 28 10:59:32.620: option DNS-SERVERS(23), len 16

*Jan 28 10:59:32.620: 2001:DB8::1

*Jan 28 10:59:32.620: option DOMAIN-LIST(24), len 10

*Jan 28 10:59:32.620: ECMD.COM

*Jan 28 10:59:32.620: option IA-PD(25), len 41

*Jan 28 10:59:32.620: IAID 0x00030001, T1 302400, T2 483840

*Jan 28 10:59:32.620: option IAPREFIX(26), len 25

*Jan 28 10:59:32.620: preferred 604800, valid 2592000, prefix 2001:DB8:1::/48

*Jan 28 10:59:32.620: IPv6 DHCP: Adding server FE80::21A:A1FF:FE7A:46A8

! Note: The CPE receives the 'Advertise' message from the DHCPv6-PD server. It will select from all replies it received (in this example there is only one

server configured, hence only one advertise is seen). The server it selects will be reflected in the next message the CPE will send out and will place within the body of the message the server it would like to use by means of the server-id

CPE: Sending the 'Request' Message

```
*Jan 28 10:59:32.620: IPv6 DHCP: Sending REQUEST to FF02::1:2 on FastEthernet0/0
*Jan 28 10:59:32.620: IPv6 DHCP: detailed packet contents
*Jan 28 10:59:32.620:   src FE80::21A:2FFF:FE87:5602
*Jan 28 10:59:32.620:   dst FF02::1:2 (FastEthernet0/0)
*Jan 28 10:59:32.620:   type REQUEST(3), xid 4016343
*Jan 28 10:59:32.620:   option ELAPSED-TIME(8), len 2
*Jan 28 10:59:32.620:     elapsed-time 0
*Jan 28 10:59:32.620:   option CLIENTID(1), len 10
*Jan 28 10:59:32.620:     00030001001A2F875602
*Jan 28 10:59:32.620:   option ORO(6), len 6
*Jan 28 10:59:32.620:     IA-PD,DNS-SERVERS,DOMAIN-LIST
*Jan 28 10:59:32.620:   option SERVERID(2), len 10
*Jan 28 10:59:32.620:     00030001001AA17A461B
*Jan 28 10:59:32.620:   option IA-PD(25), len 12
*Jan 28 10:59:32.620:     IAID 0x00030001, T1 0, T2 0
*Jan 28 10:59:32.624: IPv6 DHCP: DHCPv6 changes state from SOLICIT to REQUEST
(ADVERTISE_RECEIVED) on FastEthernet0/0
! The CPE is asking the DHCPv6-PD server with this message a bunch of parameters.
It asks these parameters from DHCPv6 server with server-id
'00030001001AA17A461B', which is in this example the 7200/NPE-G2 serving as
DHCPv6-PD server.
```

DHCPv6-PD Router: Receiving of the 'Request' message

```
Jan 28 02:18:55.620: IPv6 DHCP: Received REQUEST from FE80::21A:2FFF:FE87:5602 on
FastEthernet6/0
Jan 28 02:18:55.620: IPv6 DHCP: detailed packet contents
Jan 28 02:18:55.620:   src FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)
Jan 28 02:18:55.620:   dst FF02::1:2
Jan 28 02:18:55.620:   type REQUEST(3), xid 4016343
Jan 28 02:18:55.620:   option ELAPSED-TIME(8), len 2
Jan 28 02:18:55.620:     elapsed-time 0
Jan 28 02:18:55.620:   option CLIENTID(1), len 10
Jan 28 02:18:55.620:     00030001001A2F875602
Jan 28 02:18:55.620:   option ORO(6), len 6
Jan 28 02:18:55.620:     IA-PD,DNS-SERVERS,DOMAIN-LIST
Jan 28 02:18:55.620:   option SERVERID(2), len 10
Jan 28 02:18:55.620:     00030001001AA17A461B
Jan 28 02:18:55.620:   option IA-PD(25), len 12
Jan 28 02:18:55.620:     IAID 0x00030001, T1 0, T2 0
Jan 28 02:18:55.620: IPv6 DHCP: Creating binding for FE80::21A:2FFF:FE87:5602 in
pool ECMD_TEST
Jan 28 02:18:55.620: IPv6 DHCP: Allocating IA_PD 00030001 in binding for
FE80::21A:2FFF:FE87:5602
```

Jan 28 02:18:55.620: IPv6 DHCP: Allocating prefix 2001:DB8:1::/48 in binding for FE80::21A:2FFF:FE87:5602, IAID 00030001

! Note: From the moment the 7200/NPE-G2 serving as DHCPv6-PD server received the 'REQUEST' message from the CPE it will check its IPv6 pool and create a binding for the CPE based upon its DUID. It will also prepare the message (REPLY) for the CPE based upon this binding information

DHCPv6-PD Router: Installation of the route towards the CPE for the delegated prefix

Jan 28 02:18:55.620: IPv6RT0: static, Add 2001:DB8:1::/48 to table

Jan 28 02:18:55.620: IPv6RT0: static, Adding next-hop FE80::21A:2FFF:FE87:5602 over FastEthernet6/0 for 2001:DB8:1::/48, [1/0]

Jan 28 02:18:55.620: IPv6RT0: Event: 2001:DB8:1::/48, Add, owner static, previous None

! Note: If the Service Provider edge router made the binding between the CPE and its delegated prefix it will install automatically a static route for this delegated prefix into the routing table. The next-hop addresses used will be Link-Local.

DHCPv6-PD Router: Sending 'REPLY' message to CPE

Jan 28 02:18:55.620: IPv6 DHCP: Sending REPLY to FE80::21A:2FFF:FE87:5602 on FastEthernet6/0

Jan 28 02:18:55.620: IPv6 DHCP: detailed packet contents

Jan 28 02:18:55.620: src FE80::21A:A1FF:FE7A:46A8

Jan 28 02:18:55.620: dst FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)

Jan 28 02:18:55.620: type REPLY(7), xid 4016343

Jan 28 02:18:55.620: option SERVERID(2), len 10

Jan 28 02:18:55.620: 00030001001AA17A461B

Jan 28 02:18:55.620: option CLIENTID(1), len 10

Jan 28 02:18:55.620: 00030001001A2F875602

Jan 28 02:18:55.620: option DNS-SERVERS(23), len 16

Jan 28 02:18:55.620: 2001:DB8::1

Jan 28 02:18:55.620: option DOMAIN-LIST(24), len 10

Jan 28 02:18:55.620: ECMD.COM

Jan 28 02:18:55.620: option IA-PD(25), len 41

Jan 28 02:18:55.620: IAID 0x00030001, T1 302400, T2 483840

Jan 28 02:18:55.620: option IAPREFIX(26), len 25

Jan 28 02:18:55.620: preferred 604800, valid 2592000, prefix 2001:DB8:1::/48

! Note: With this message the DHCPv6-PD server lets the CPE know what the requested parameters are, including the delegated prefix "2001:DB8:1::/48".

CPE: Receiving of the 'REPLY' sent by the DHCPv6-PD server

*Jan 28 10:59:32.624: IPv6 DHCP: Received REPLY from FE80::21A:A1FF:FE7A:46A8 on FastEthernet0/0

*Jan 28 10:59:32.624: IPv6 DHCP: detailed packet contents

*Jan 28 10:59:32.624: src FE80::21A:A1FF:FE7A:46A8 (FastEthernet0/0)

*Jan 28 10:59:32.624: dst FE80::21A:2FFF:FE87:5602

*Jan 28 10:59:32.624: type REPLY(7), xid 4016343

*Jan 28 10:59:32.624: option SERVERID(2), len 10

```
*Jan 28 10:59:32.624:      00030001001AA17A461B
*Jan 28 10:59:32.624:      option CLIENTID(1), len 10
*Jan 28 10:59:32.624:      00030001001A2F875602
*Jan 28 10:59:32.624:      option DNS-SERVERS(23), len 16
*Jan 28 10:59:32.624:      2001:DB8::1
*Jan 28 10:59:32.624:      option DOMAIN-LIST(24), len 10
*Jan 28 10:59:32.624:      ECMD.COM
*Jan 28 10:59:32.624:      option IA-PD(25), len 41
*Jan 28 10:59:32.624:      IAID 0x00030001, T1 302400, T2 483840
*Jan 28 10:59:32.624:      option IAPREFIX(26), len 25
*Jan 28 10:59:32.624:      preferred 604800, valid 2592000, prefix
2001:DB8:1::/48
! Note: The CPE receives the 'REPLY' from the Service provider edge router
```

CPE: Action on the CPE following receiving of the 'REPLY'

```
*Jan 28 10:59:32.624: IPv6 DHCP: Processing options
*Jan 28 10:59:32.624: IPv6 DHCP: Adding prefix 2001:DB8:1::/48 to PREFIX_1
*Jan 28 10:59:32.628: IPv6 DHCP: T1 set to expire in 302400 seconds
*Jan 28 10:59:32.628: IPv6 DHCP: T2 set to expire in 483840 seconds
*Jan 28 10:59:32.628: IPv6 DHCP: Configuring DNS server 2001:DB8::1
*Jan 28 10:59:32.628: IPv6 DHCP: Configuring domain name ECMD.COM
*Jan 28 10:59:32.628: IPv6 DHCP: DHCPv6 changes state from REQUEST to OPEN
(REPLY_RECEIVED) on FastEthernet0/0
```

! Note: DHCPv6 process on the CPE is processing the content in greater detail and places the received prefix together with its attached parameters under the name "PREFIX_1"

CPE: Action on the CPE with respect to routing

```
*Jan 28 10:59:32.624: IPv6RT0: connected, Route add 2001:DB8:1::/64 [new]
*Jan 28 10:59:32.624: IPv6RT0: connected, Add 2001:DB8:1::/64 to table
*Jan 28 10:59:32.624: IPv6RT0: connected, Adding next-hop :: over Loopback100 for
2001:DB8:1::/64, [0/0]
*Jan 28 10:59:32.628: IPv6RT0: connected, Route add 2001:DB8:1::1/128 [new]
*Jan 28 10:59:32.628: IPv6RT0: connected, Add 2001:DB8:1::1/128 to table
*Jan 28 10:59:32.628: IPv6RT0: connected, Adding next-hop :: over Loopback100 for
2001:DB8:1::1/128, [0/0]
*Jan 28 10:59:32.628: IPv6RT0: static, Route add 2001:DB8:1::/48 [new]
*Jan 28 10:59:32.628: IPv6RT0: static, Add 2001:DB8:1::/48 to table
*Jan 28 10:59:32.628: IPv6RT0: static, Adding next-hop :: over Null0 for
2001:DB8:1::/48, [1/0]
*Jan 28 10:59:32.628: IPv6RT0: Event: 2001:DB8:1::/64, Add, owner connected,
previous None
*Jan 28 10:59:32.628: IPv6RT0: Event: 2001:DB8:1::1/128, Add, owner connected,
previous None
*Jan 28 10:59:32.628: IPv6RT0: Event: 2001:DB8:1::/48, Add, owner static,
previous None
```

! Note: Once the delegated prefix is allocated to "PREFIX_1" the CPE can start with dynamically configuring the IPv6 addresses for its interfaces. In addition it will add a routing in place to support these automatic generated prefixes.

From now onwards, the CPE is fully automated and has all routing needed installed for the correct routing of traffic and to support stateless auto-configuration of directly connected IPv6 hosts. To check the received prefixes on the CPE, the following command can be executed:

```
ecmd-1841-1#show ipv6 dhcp interface fast 0/0
FastEthernet0/0 is in client mode
State is OPEN
Renew will be sent in 3d10h
List of known servers:
  Reachable via address: FE80::21A:A1FF:FE7A:46A8
  DUID: 00030001001AA17A461B
  Preference: 0
Configuration parameters:
  IA PD: IA ID 0x00030001, T1 302400, T2 483840
  Prefix: 2001:DB8:1::/48
          preferred lifetime 604800, valid lifetime 2592000
          expires at Feb 27 2008 10:59 AM (2587948 seconds)
  DNS server: 2001:DB8::1
  Domain name: ECMD.COM
  Prefix name: PREFIX_1
  Rapid-Commit: disabled
ecmd-1841-1#
```

Deployment Model 2: DHCPv6-PD Relay at the Service Provider Edge Router

This model provides a highly scalable infrastructure, while the configuration upon the Edge Routers functioning as DHCPv6-Relay remains compact and straightforward. The configuration task on the Edge Router exists out activating the Relay functionality and enabling IPv6 routing. The following configuration snip can be a good base example template for the service provider Edge Router:

```
!
ipv6 unicast-routing
ipv6 cef
!
!
interface FastEthernet0/2
  description Lab backbone connection to CNR7.0 (to DHCPv6-PD Server)
  ip address 10.48.81.86 255.255.255.192
  speed 10
  duplex half
  ipv6 address 2001:DB8:1234::1/64
  ! The DHCPv6 Server is connected to this FastEthernet2/0
  !
interface FastEthernet6/0
  description Connection towards the CPE (to DHCPv6-PD Client)
  ip address 11.11.11.2 255.255.255.252
  duplex half
  ipv6 address 2001:BEEF::1/64
```

```
! Manually configured link-address
ipv6 enable
ipv6 dhcp relay destination 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
! Enabling DHCPv6-PD Relay services towards the connected CPE device
!
```

From the configuration example provided above, it is seen that the configuration on the DHCPv6_PD relay router is compact and simple to extend towards additional CPEs connected to this router. All configurations are done on the DHCPv6 server in a central location. In the above configuration FastEthernet6/0 has an IPv6 address configured. This is an optional configuration and may not always be the most convenient implementation for this deployment model. Often there will be no IPv6 address configured on the interface pointing toward the CPE. The decision however to either 'add' or 'not-add' an IPv6 address on the interface pointing to the CPE has consequences for the configuration of the DHCPv6 server (e.g. CNR7.0). This IPv6 address will, by the service provider Edge Router acting as DHCPv6 Relay Agent, be included in any relayed DHCPv6 messages as the "Link-address". It will indicate towards the DHCPv6 server where the CPE is connected, hence if this IPv6 is not configured, then the DHCPv6 Server must use another mechanism for this purpose.

When the CNR7.0 DHCPv6 server is utilized, then the following decision criteria is used to identify the correct delegated prefix the DHCPv6-client: CNR will use the source address of the relayed packet UNLESS it is a link-local address, in which case it will use the interface's addresses (preferring global unicast addresses, but it will use the interface's link-local as a last resort).

Based upon the base CPE configuration and the above Relay configuration, the following message exchanges are seen on CPE and DHCPv6-PD relay:

CPE: 'Solicit' sent from CPE -> DHCPv6-PD Relay

```
*Jan 28 15:08:26.175: IPv6 DHCP: Sending SOLICIT to FF02::1:2 on FastEthernet0/0
*Jan 28 15:08:26.175: IPv6 DHCP: detailed packet contents
*Jan 28 15:08:26.175:   src FE80::21A:2FFF:FE87:5602
*Jan 28 15:08:26.175:   dst FF02::1:2 (FastEthernet0/0)
*Jan 28 15:08:26.175:   type SOLICIT(1), xid 1363537
*Jan 28 15:08:26.175:   option ELAPSED-TIME(8), len 2
*Jan 28 15:08:26.175:     elapsed-time 3078
*Jan 28 15:08:26.175:   option CLIENTID(1), len 10
*Jan 28 15:08:26.175:     00030001001A2F875602
*Jan 28 15:08:26.175:   option ORO(6), len 6
*Jan 28 15:08:26.175:     IA-PD,DNS-SERVERS,DOMAIN-LIST
*Jan 28 15:08:26.175:   option IA-PD(25), len 12
*Jan 28 15:08:26.175:     IAID 0x00030001, T1 0, T2 0
```

! The CPE is totally not aware that there is an upstream connected relay. The message send out by the CPE is to inform about the connected DHCPv6 servers connected to its upstream interface

RELAY Agent: Received 'Solicit' from CPE

```
Jan 28 06:27:47.063: IPv6 DHCP: Received SOLICIT from FE80::21A:2FFF:FE87:5602 on
FastEthernet6/0
Jan 28 06:27:47.063: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.063:   src FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)
```

```
Jan 28 06:27:47.063: dst FF02::1:2
Jan 28 06:27:47.063: type SOLICIT(1), xid 1363537
Jan 28 06:27:47.063: option ELAPSED-TIME(8), len 2
Jan 28 06:27:47.063:     elapsed-time 3078
Jan 28 06:27:47.063: option CLIENTID(1), len 10
Jan 28 06:27:47.063:     00030001001A2F875602
Jan 28 06:27:47.063: option ORO(6), len 6
Jan 28 06:27:47.063:     IA-PD,DNS-SERVERS,DOMAIN-LIST
Jan 28 06:27:47.063: option IA-PD(25), len 12
Jan 28 06:27:47.063:     IAID 0x00030001, T1 0, T2 0
```

! The relay (the service provider edge router) is receiving the solicit from the connected CPE. The relay will take this solicit packet, and encapsulate it fully in a 'RELAY-FORW' message seen in the next debug capture.

Relay Agent: Encapsulating the received 'Solicit' and forward it onwards to the DHCPv6 server

```
Jan 28 06:27:47.063: IPv6 DHCP_RELAY: Relaying SOLICIT from
FE80::21A:2FFF:FE87:5602 on FastEthernet6/0
Jan 28 06:27:47.063: IPv6 DHCP_RELAY: to 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Jan 28 06:27:47.063: IPv6 DHCP: Sending RELAY-FORWARD to
2001:DB8:1234:0:218:FEFF:FEFB:CC0E on FastEthernet0/2
Jan 28 06:27:47.063: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.063:   src 2001:DB8:1234::1
Jan 28 06:27:47.063:   dst 2001:DB8:1234:0:218:FEFF:FEFB:CC0E (FastEthernet0/2)
Jan 28 06:27:47.063:   type RELAY-FORWARD(12), hop 0
Jan 28 06:27:47.063:   link 2001:BEEF::1
Jan 28 06:27:47.063:   peer FE80::21A:2FFF:FE87:5602
Jan 28 06:27:47.063:   option RELAY-MSG(9), len 50
Jan 28 06:27:47.063:       type SOLICIT(1), xid 1363537
Jan 28 06:27:47.063:       option ELAPSED-TIME(8), len 2
Jan 28 06:27:47.063:           elapsed-time 3078
Jan 28 06:27:47.063:       option CLIENTID(1), len 10
Jan 28 06:27:47.063:           00030001001A2F875602
Jan 28 06:27:47.063:       option ORO(6), len 6
Jan 28 06:27:47.063:           IA-PD,DNS-SERVERS,DOMAIN-LIST
Jan 28 06:27:47.063:       option IA-PD(25), len 12
Jan 28 06:27:47.063:           IAID 0x00030001, T1 0, T2 0
Jan 28 06:27:47.063:   option INTERFACE-ID(18), len 5
Jan 28 06:27:47.063:       0x4661362F30
Jan 28 06:27:47.063:   option UNKNOWN(37), len 22
```

! Note: The Solicit is fully encapsulated into a 'RELAY-FORW' message as a 'relay-msg' option. In addition the relay adds a few other options. The options added are identified above because they are placed in bold. The 'link' option informs the DHCPv6 server to which link the request is coming from. Based on this the DHCPv6 may make a decision on the IPv6 prefixes being exchanged.

DHCPv6 SERVER: receiving of the 'RELAY-FORW' message on the DHCPv6 server (CNR7.0)

```

01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: ----- RECEIVED -- R1 --
---
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> received 123
bytes from 2001:db8:1234::1, port 547
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> +- Start of
RELAY-FORW (12) message (123 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | hop-count
0,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | link-
address 2001:beef::1,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | peer-
address fe80::21a:2fff:fe87:5602
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | relay-message
(9) option (50 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | +- Start of
SOLICIT (1) message (50 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | |
transaction-id 1363537
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | elapsed-
time (8) option (2 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | 3078
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | client-
identifier (1) option (10 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | |
00:03:00:01:00:1a:2f:87:56:02
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | oro (6)
option (6 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | 25,23,24
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | ia-pd (25)
option (12 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | | (iaid
196609, t1 0, t2 0)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | +- End of
SOLICIT message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | interface-id
(18) option (5 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> |
46:61:36:2f:30
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | remote-id (37)
option (22 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> |
(enterprise-id 9,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> | remote-id
02:00:60:00:06:90:00:0a:00:03:00:01:00:1a:a1:7a:46:1b)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: -> +- End of RELAY-
FORW message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R1: ----- END OF RECEIVED -
- R1 -----
01/28/2008 16:06:54 name/dhcp/1 Activity Server 0 18173 Server received a relayed
SOLICIT from Client: DUID: 00:03:00:01:00:1a:2f:87:56:02 packet: R1 on network
interface ifIndex 4, device 'Local Area Connection 2', 2 in use.
! The DHCPv6 server receives the 'RELAY-FORW' message. It will investigate the
Solicit message and reply back to the relay with a 'RELAY-REPLY' message.

```

DHCPv6 SERVER: Sending of the 'RELAY-REPLY' message on the DHCPv6 server back to the Relay (CNR7.0)

```
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: ----- TRANSMITTED --
X67 -----
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      transmitted 162
bytes to 2001:db8:1234::1, port 547
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      +- Start of
RELAY-REPLY (13) message (162 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      hop-count
0,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      link-
address 2001:beef::1,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      peer-
address fe80::21a:2fff:fe87:5602
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      interface-id
(18) option (5 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |
46:61:36:2f:30
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      relay-message
(9) option (115 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      +- Start of
ADVVERTISE (2) message (115 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
transaction-id 1363537
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |      client-
identifier (1) option (10 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
00:03:00:01:00:1a:2f:87:56:02
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |      server-
identifier (2) option (14 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
00:01:00:01:46:84:cc:5e:00:18:fe:fb:cc:0f
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |      ia-pd (25)
option (41 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |      (iaid
196609, t1 3d12h, t2 5d14h24m)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
iaprefix (26) option (25 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
(preferred-lifetime 1w,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
valid-lifetime 2w,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
prefix-length 64,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
prefix 2001:db8:cafe::)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |      dns-
servers (23) option (16 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
2001:c00::23:2
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |      domain-
list (24) option (10 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      |      |
ecmd.com.
```

```
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      | +- End of
ADVERTISE message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: <-      +- End of RELAY-
REPLY message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X67: ----- END OF
TRANSMITTED -- X67 -----
01/28/2008 16:06:54 name/dhcp/1 Activity Protocol 0 18643 Server sent a relayed
ADVERTISE to Client: DUID: 00:03:00:01:00:1a:2f:87:56:02 packet: R1, OFFERED
2001:db8:cafe::/64 (2w/1w). 0 ms.

! Note: Because the DHCPv6 server received a 'Solicit' message from the CPE it
will reply back with an 'Advertise' message. The DHCPv6 server received this
'Solicit' encapsulated in a 'RELAY-FORW' message; hence the 'Advertise' will be
encapsulated also in a relay message. The message type is known as a 'RELAY-
REPLY' message.
```

RELAY Agent: Receiving from 'RELAY-REPLY' message on the Service provider edge router functioning as relay

```
Jan 28 06:27:47.067: IPv6 DHCP: Received RELAY-REPLY from
2001:DB8:1234:0:218:FEFF:FEFB:CC0E on FastEthernet0/2
Jan 28 06:27:47.067: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.067:   src 2001:DB8:1234:0:218:FEFF:FEFB:CC0E (FastEthernet0/2)
Jan 28 06:27:47.067:   dst 2001:DB8:1234::1
Jan 28 06:27:47.067:   type RELAY-REPLY(13), hop 0
Jan 28 06:27:47.067:   link 2001:BEEF::1
Jan 28 06:27:47.067:   peer FE80::21A:2FFF:FE87:5602
Jan 28 06:27:47.067:   option INTERFACE-ID(18), len 5
Jan 28 06:27:47.067:     0x4661362F30
Jan 28 06:27:47.067:   option RELAY-MSG(9), len 115
Jan 28 06:27:47.067:     type ADVERTISE(2), xid 1363537
Jan 28 06:27:47.067:     option CLIENTID(1), len 10
Jan 28 06:27:47.067:       00030001001A2F875602
Jan 28 06:27:47.067:     option SERVERID(2), len 14
Jan 28 06:27:47.067:       000100014684CC5E0018FEFBCC0F
Jan 28 06:27:47.067:     option IA-PD(25), len 41
Jan 28 06:27:47.067:       IAID 0x00030001, T1 302400, T2 483840
Jan 28 06:27:47.067:     option IAPREFIX(26), len 25
Jan 28 06:27:47.067:       preferred 604800, valid 1209600, prefix
2001:DB8:CAFE::/64
Jan 28 06:27:47.067:     option DNS-SERVERS(23), len 16
Jan 28 06:27:47.067:       2001:C00::23:2
Jan 28 06:27:47.067:     option DOMAIN-LIST(24), len 10
Jan 28 06:27:47.067:       ecmd.com
```

! Note: the DHCPv6 Relay router receives the 'Relay-reply' message from the DHCPv6 server and realizes it is a message not destined for itself, but for the downstream CPE router. The Service provider edge router will now de-capsulate the 'RELAY-REPLY' and forward the 'Advertise' message to the connected CPE router.

RELAY Agent: decapsulating the 'RELAY-REPLY' message and sending the 'Advertise' to the CPE

```
Jan 28 06:27:47.067: IPv6 DHCP_RELAY: Relaying RELAY-REPLY from
2001:DB8:1234:0:218:FEFF:FEFB:CC0E on FastEthernet0/2
```

```
Jan 28 06:27:47.067: IPv6 DHCP_RELAY: to FE80::21A:2FFF:FE87:5602 via
FastEthernet6/0
Jan 28 06:27:47.067: IPv6 DHCP: Sending ADVERTISE to FE80::21A:2FFF:FE87:5602 on
FastEthernet6/0
Jan 28 06:27:47.067: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.067:   src FE80::21A:A1FF:FE7A:46A8
Jan 28 06:27:47.067:   dst FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)
Jan 28 06:27:47.067:   type ADVERTISE(2), xid 1363537
Jan 28 06:27:47.067:   option CLIENTID(1), len 10
Jan 28 06:27:47.067:     00030001001A2F875602
Jan 28 06:27:47.067:   option SERVERID(2), len 14
Jan 28 06:27:47.067:     000100014684CC5E0018FEFBCC0F
Jan 28 06:27:47.067:   option IA-PD(25), len 41
Jan 28 06:27:47.067:     IAID 0x00030001, T1 302400, T2 483840
Jan 28 06:27:47.067:   option IAPREFIX(26), len 25
Jan 28 06:27:47.067:     preferred 604800, valid 1209600, prefix
2001:DB8:CAFE::/64
Jan 28 06:27:47.067:   option DNS-SERVERS(23), len 16
Jan 28 06:27:47.067:     2001:C00::23:2
Jan 28 06:27:47.067:   option DOMAIN-LIST(24), len 10
Jan 28 06:27:47.067:     ecmd.com
```

! Note: The 'Advertise' is forwarded to the CPE as a native 'Advertise' message without any Relay based encapsulation. The CPE will hence be fully non-aware of the existence of the Relay.

CPE: Receiving of the 'Advertise' message on the CPE

```
*Jan 28 15:08:26.179: IPv6 DHCP: Received ADVERTISE from FE80::21A:A1FF:FE7A:46A8
on FastEthernet0/0
*Jan 28 15:08:26.179: IPv6 DHCP: detailed packet contents
*Jan 28 15:08:26.179:   src FE80::21A:A1FF:FE7A:46A8 (FastEthernet0/0)
*Jan 28 15:08:26.179:   dst FE80::21A:2FFF:FE87:5602
*Jan 28 15:08:26.179:   type ADVERTISE(2), xid 1363537
*Jan 28 15:08:26.179:   option CLIENTID(1), len 10
*Jan 28 15:08:26.179:     00030001001A2F875602
*Jan 28 15:08:26.179:   option SERVERID(2), len 14
*Jan 28 15:08:26.179:     000100014684CC5E0018FEFBCC0F
*Jan 28 15:08:26.179:   option IA-PD(25), len 41
*Jan 28 15:08:26.183:     IAID 0x00030001, T1 302400, T2 483840
*Jan 28 15:08:26.183:   option IAPREFIX(26), len 25
*Jan 28 15:08:26.183:     preferred 604800, valid 1209600, prefix
2001:DB8:CAFE::/64
*Jan 28 15:08:26.183:   option DNS-SERVERS(23), len 16
*Jan 28 15:08:26.183:     2001:C00::23:2
*Jan 28 15:08:26.183:   option DOMAIN-LIST(24), len 10
*Jan 28 15:08:26.183:     ecmd.com
*Jan 28 15:08:26.183: IPv6 DHCP: Adding server FE80::21A:A1FF:FE7A:46A8
```

! Note: The CPE received as reply on its originally sent 'Solicit' message a set of available and active DHCPv6 servers. This list of available DHCPv6 servers are found within the 'Advertise' messages. In the above it can be seen that the CPE

recognizes "FE80::21A:A1FF:FE7A:46A8" as an available DHCPv6 server. It uses the IPv6 Link-local address of the received 'Advertise' message. Note that this address in the above example points to the DHCPv6-Relay agent, and not to the real DHCPv6 server (The CNR7.0). For the perspective of the CPE it appears as the Relay is the DHCPv6 server.

CPE: Sending of 'REQUEST' by the CPE to the DHCPv6 server

```
*Jan 28 15:08:26.183: IPv6 DHCP: Sending REQUEST to FF02::1:2 on FastEthernet0/0
*Jan 28 15:08:26.183: IPv6 DHCP: detailed packet contents
*Jan 28 15:08:26.183:   src FE80::21A:2FFF:FE87:5602
*Jan 28 15:08:26.183:   dst FF02::1:2 (FastEthernet0/0)
*Jan 28 15:08:26.183:   type REQUEST(3), xid 2172694
*Jan 28 15:08:26.183:   option ELAPSED-TIME(8), len 2
*Jan 28 15:08:26.183:     elapsed-time 0
*Jan 28 15:08:26.183:   option CLIENTID(1), len 10
*Jan 28 15:08:26.183:     00030001001A2F875602
*Jan 28 15:08:26.183:   option ORO(6), len 6
*Jan 28 15:08:26.183:     IA-PD,DNS-SERVERS,DOMAIN-LIST
*Jan 28 15:08:26.183:   option SERVERID(2), len 14
*Jan 28 15:08:26.183:     000100014684CC5E0018FEFBCC0F
*Jan 28 15:08:26.183:   option IA-PD(25), len 12
*Jan 28 15:08:26.183:     IAID 0x00030001, T1 0, T2 0
*Jan 28 15:08:26.183: IPv6 DHCP: DHCPv6 changes state from SOLICIT to REQUEST
(ADVERTISE_RECEIVED) on FastEthernet0/0
```

! Note: The CPE will choose one DHCPv6 server from the available list of DHCPv6 servers and send it a 'REQUEST' message. This communication happens with Link local addressing between the CPE (the DHCPv6-PD client) and the Service Provider edge router (DHCPv6-Relay agent). With this action the CPE expects to receive a delegated IPv6 prefix it can use to configure its interfaces

RELAY Agent: Receiving of the 'REQUEST' sent by the CPE

```
Jan 28 06:27:47.071: IPv6 DHCP: Received REQUEST from FE80::21A:2FFF:FE87:5602 on
FastEthernet6/0
Jan 28 06:27:47.071: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.071:   src FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)
Jan 28 06:27:47.071:   dst FF02::1:2
Jan 28 06:27:47.071:   type REQUEST(3), xid 2172694
Jan 28 06:27:47.071:   option ELAPSED-TIME(8), len 2
Jan 28 06:27:47.071:     elapsed-time 0
Jan 28 06:27:47.071:   option CLIENTID(1), len 10
Jan 28 06:27:47.071:     00030001001A2F875602
Jan 28 06:27:47.071:   option ORO(6), len 6
Jan 28 06:27:47.071:     IA-PD,DNS-SERVERS,DOMAIN-LIST
Jan 28 06:27:47.071:   option SERVERID(2), len 14
Jan 28 06:27:47.071:     000100014684CC5E0018FEFBCC0F
Jan 28 06:27:47.071:   option IA-PD(25), len 12
Jan 28 06:27:47.071:     IAID 0x00030001, T1 0, T2 0
```


! Note: The Service Provider edge router receives the 'REQUEST' sent by the CPE. The router is configured as a DHCPv6 relay and will encapsulate this packet in a 'RELAY-FORW' message and send it onwards to the DHCPv6 server.

Relay Agent: sending the 'RELAY-FORW' message with the initial 'REQUEST' included within the message body

```
Jan 28 06:27:47.071: IPv6 DHCP_RELAY: Relaying REQUEST from
FE80::21A:2FFF:FE87:5602 on FastEthernet6/0
Jan 28 06:27:47.071: IPv6 DHCP_RELAY: to 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Jan 28 06:27:47.071: IPv6 DHCP: Sending RELAY-FORWARD to
2001:DB8:1234:0:218:FEFF:FEFB:CC0E on FastEthernet0/2
Jan 28 06:27:47.071: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.071:   src 2001:DB8:1234::1
Jan 28 06:27:47.071:   dst 2001:DB8:1234:0:218:FEFF:FEFB:CC0E (FastEthernet0/2)
Jan 28 06:27:47.071:   type RELAY-FORWARD(12), hop 0
Jan 28 06:27:47.071:   link 2001:BEEF::1
Jan 28 06:27:47.071:   peer FE80::21A:2FFF:FE87:5602
Jan 28 06:27:47.071:   option RELAY-MSG(9), len 68
Jan 28 06:27:47.071:     type REQUEST(3), xid 2172694
Jan 28 06:27:47.071:     option ELAPSED-TIME(8), len 2
Jan 28 06:27:47.071:       elapsed-time 0
Jan 28 06:27:47.071:     option CLIENTID(1), len 10
Jan 28 06:27:47.071:       00030001001A2F875602
Jan 28 06:27:47.071:     option ORO(6), len 6
Jan 28 06:27:47.071:       IA-PD,DNS-SERVERS,DOMAIN-LIST
Jan 28 06:27:47.071:     option SERVERID(2), len 14
Jan 28 06:27:47.071:       000100014684CC5E0018FEFBCC0F
Jan 28 06:27:47.071:     option IA-PD(25), len 12
Jan 28 06:27:47.071:       IAID 0x00030001, T1 0, T2 0
Jan 28 06:27:47.071:     option INTERFACE-ID(18), len 5
Jan 28 06:27:47.071:       0x4661362F30
Jan 28 06:27:47.071:     option UNKNOWN(37), len 22
```

! Note: the original "REQUEST" message is included in the 'RELAY-FORW' message as an option. All data included in this option is identical as the within original 'REQUEST'. The communication between DHCPv6 server and the DHCPv6 Relay Agent happens over global IPv6 addresses, because there is no requirement to have a Relay Agent directly connected to the DHCPv6 server. What can be seen again is that the 'RELAY-FORW' message has a few additional DHCPv6 options included to inform the DHCPv6 server about the original requester. It will aid the DHCPv6 server to know who is requesting the IPv6 prefix and where it was requested.

DHCPv6 SERVER: Receiving of the 'RELAY-FORW' message sent by the DHCPv6 Relay Agent

```
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: ----- RECEIVED -- R2 --
---
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2:  ->  received 141
bytes from 2001:db8:1234::1, port 547
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2:  ->  +- Start of
RELAY-FORW (12) message (141 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2:  ->  |      hop-count
0,
```

```

01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | link-
address 2001:beef::1,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | peer-
address fe80::21a:2fff:fe87:5602
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | relay-message
(9) option (68 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | +- Start of
REQUEST (3) message (68 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | |
transaction-id 2172694
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | elapsed-
time (8) option (2 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | 0
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | client-
identifier (1) option (10 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | |
00:03:00:01:00:1a:2f:87:56:02
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | oro (6)
option (6 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | 25,23,24
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | server-
identifrier (2) option (14 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | |
00:01:00:01:46:84:cc:5e:00:18:fe:fb:cc:0f
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | ia-pd (25)
option (12 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | | (iaid
196609, t1 0, t2 0)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | +- End of
REQUEST message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | interface-id
(18) option (5 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> |
46:61:36:2f:30
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | remote-id (37)
option (22 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> |
(enterprise-id 9,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> | remote-id
02:00:60:00:06:90:00:0a:00:03:00:01:00:1a:a1:7a:46:1b)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: -> +- End of RELAY-
FORW message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 R2: ----- END OF RECEIVED -
- R2 -----
01/28/2008 16:06:54 name/dhcp/1 Activity Server 0 18173 Server received a relayed
REQUEST from Client: DUID: 00:03:00:01:00:1a:2f:87:56:02 packet: R2 on network
interface ifIndex 4, device 'Local Area Connection 2', 2 in use.

! Note: The DHCPv6 server received the 'RELAY-FORW' message and investigates the
information available within this packet. It sees that the requestor DUID (DHCPv6
Unique Identifier) is "00:03:00:01:00:1a:2f:87:56:02" and it will look at the
link-address "2001:beef::1". Based on these values it looks into its configuration
files and identifies an IPv6 prefix which can be delegated to the CPE with DUID
"00:03:00:01:00:1a:2f:87:56:02".

```


DHCPv6 SERVER: Sending of 'RELAY-REPLY' to the DHCPv6 Relay Agent as response to the initial 'RELAY-FORW'

```
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: ----- TRANSMITTED --
X68 -----
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      transmitted 162
bytes to 2001:db8:1234::1, port 547
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      +- Start of
RELAY-REPLY (13) message (162 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      hop-count
0,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      link-
address 2001:beef::1,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      peer-
address fe80::21a:2fff:fe87:5602
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      interface-id
(18) option (5 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |
46:61:36:2f:30
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      relay-message
(9) option (115 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      +- Start of
REPLY (7) message (115 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
transaction-id 2172694
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |      client-
identifier (1) option (10 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
00:03:00:01:00:1a:2f:87:56:02
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |      server-
identifier (2) option (14 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
00:01:00:01:46:84:cc:5e:00:18:fe:fb:cc:0f
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |      ia-pd (25)
option (41 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |      (iaid
196609, t1 3d12h, t2 5d14h24m)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
iaprefix (26) option (25 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
(preferred-lifetime 1w,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
valid-lifetime 2w,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
prefix-length 64,
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
prefix 2001:db8:cafe::)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |      dns-
servers (23) option (16 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
2001:c00::23:2
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |      domain-
list (24) option (10 bytes)
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      |      |
ecmd.com.
```

```
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      | +- End of
REPLY message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: <-      +- End of RELAY-
REPLY message
01/28/2008 16:06:54 name/dhcp/1 Info Protocol 0 04935 X68: ----- END OF
TRANSMITTED -- X68 -----
```

! Note: The DHCPv6 server found in its configuration that the prefix available for the CPE is '2001:DB8:CAFE::/64'. It will also add the lifetimes with this delegated prefix and DNS server in addition to the domain name 'ecmd.com'. This information is found in a DHCPv6 'REPLY' message which is carried as an option in the 'RELAY-REPLY' message send from the DHCPv6 Server to the DHCPv6 Relay Agent. Communication between the Server and relay agent happens between the global IPv6 addresses of both devices.

Relay Agent: Receiving of the 'RELAY-REPLY' message from the DHCPv6 Server

```
Jan 28 06:27:47.075: IPv6 DHCP: Received RELAY-REPLY from
2001:DB8:1234:0:218:FEFF:FEFB:CC0E on FastEthernet0/2
Jan 28 06:27:47.075: IPv6 DHCP: detailed packet contents
Jan 28 06:27:47.075:   src 2001:DB8:1234:0:218:FEFF:FEFB:CC0E (FastEthernet0/2)
Jan 28 06:27:47.075:   dst 2001:DB8:1234::1
Jan 28 06:27:47.075:   type RELAY-REPLY(13), hop 0
Jan 28 06:27:47.075:   link 2001:BEEF::1
Jan 28 06:27:47.075:   peer FE80::21A:2FFF:FE87:5602
Jan 28 06:27:47.075:   option INTERFACE-ID(18), len 5
Jan 28 06:27:47.075:     0x4661362F30
Jan 28 06:27:47.075:   option RELAY-MSG(9), len 115
Jan 28 06:27:47.075:     type REPLY(7), xid 2172694
Jan 28 06:27:47.075:     option CLIENTID(1), len 10
Jan 28 06:27:47.075:       00030001001A2F875602
Jan 28 06:27:47.075:     option SERVERID(2), len 14
Jan 28 06:27:47.075:       000100014684CC5E0018FEFBCC0F
Jan 28 06:27:47.075:     option IA-PD(25), len 41
Jan 28 06:27:47.075:       IAID 0x00030001, T1 302400, T2 483840
Jan 28 06:27:47.075:     option IAPREFIX(26), len 25
Jan 28 06:27:47.075:       preferred 604800, valid 1209600, prefix
2001:DB8:CAFE::/64
Jan 28 06:27:47.075:     option DNS-SERVERS(23), len 16
Jan 28 06:27:47.075:       2001:C00::23:2
Jan 28 06:27:47.075:     option DOMAIN-LIST(24), len 10
Jan 28 06:27:47.075:       ecmd.com
```

! Note: The Service provider edge router acting as a DHCPv6 Relay Agent receives the 'RELAY-REPLY' message and will investigate its content. Based on the content it discovers that a 'REPLY' message must be composed and sent onwards to the CPE.

Relay Agent: Adding dynamically static route entries pointing to the CPE for the delegated address space

```
Jan 28 06:27:47.075: IPv6 DHCP_RELAY: Relaying RELAY-REPLY from
2001:DB8:1234:0:218:FEFF:FEFB:CC0E on FastEthernet0/2
Jan 28 06:27:47.075: IPv6RT0: static, Add 2001:DB8:CAFE::/64 to table
```

Jan 28 06:27:47.075: IPv6RT0: static, Adding next-hop FE80::21A:2FFF:FE87:5602 over FastEthernet6/0 for 2001:DB8:CAFE::/64, [1/0]

Jan 28 06:27:47.075: IPv6 DHCP_RELAY: Route added: 2001:DB8:CAFE::/64 via FE80::21A:2FFF:FE87:5602 dist 1 lifetime 1209600

Jan 28 06:27:47.075: IPv6RT0: Event: 2001:DB8:CAFE::/64, Add, owner static, previous None

! Note: The Service Provider Edge router acting as a DHCPv6 relay agent installs based upon the content of the received 'RELAY-REPLY' message from the DHCPv6 Server a static route. This route entry will point the delegated IPv6 address range (2001:DB8:CAFE:0000::/64) to the Link Local IPv6 address of the directly connected CPE. This happens automatically on the Cisco IOS Relay agent without human interaction and without explicit configuration.

Relay Agent: Sending a 'REPLY' to the CPE router which is the final DHCPv6 Client

Jan 28 06:27:47.075: IPv6 DHCP_RELAY: to FE80::21A:2FFF:FE87:5602 via FastEthernet6/0

Jan 28 06:27:47.075: IPv6 DHCP: Sending REPLY to FE80::21A:2FFF:FE87:5602 on FastEthernet6/0

Jan 28 06:27:47.075: IPv6 DHCP: detailed packet contents

Jan 28 06:27:47.075: src FE80::21A:A1FF:FE7A:46A8

Jan 28 06:27:47.075: dst FE80::21A:2FFF:FE87:5602 (FastEthernet6/0)

Jan 28 06:27:47.075: type REPLY(7), xid 2172694

Jan 28 06:27:47.075: option CLIENTID(1), len 10

Jan 28 06:27:47.075: 00030001001A2F875602

Jan 28 06:27:47.075: option SERVERID(2), len 14

Jan 28 06:27:47.075: 000100014684CC5E0018FEFBCC0F

Jan 28 06:27:47.075: option IA-PD(25), len 41

Jan 28 06:27:47.075: IAID 0x00030001, T1 302400, T2 483840

Jan 28 06:27:47.075: option IAPREFIX(26), len 25

Jan 28 06:27:47.075: preferred 604800, valid 1209600, prefix 2001:DB8:CAFE::/64

Jan 28 06:27:47.075: option DNS-SERVERS(23), len 16

Jan 28 06:27:47.075: 2001:C00::23:2

Jan 28 06:27:47.075: option DOMAIN-LIST(24), len 10

Jan 28 06:27:47.075: ecmd.com

! Note: The Service Provider Edge router will send a DHCPv6 'REPLY' message to the CPE device. This 'REPLY' is composed from the information found in the 'RELAY-REPLY' message.

CPE: The CPE receives the 'REPLY' message from its upstream Service Provider edge route

*Jan 28 15:08:26.187: IPv6 DHCP: Received REPLY from FE80::21A:A1FF:FE7A:46A8 on FastEthernet0/0

*Jan 28 15:08:26.187: IPv6 DHCP: detailed packet contents

*Jan 28 15:08:26.187: src FE80::21A:A1FF:FE7A:46A8 (FastEthernet0/0)

*Jan 28 15:08:26.187: dst FE80::21A:2FFF:FE87:5602

*Jan 28 15:08:26.187: type REPLY(7), xid 2172694

*Jan 28 15:08:26.187: option CLIENTID(1), len 10

*Jan 28 15:08:26.187: 00030001001A2F875602

*Jan 28 15:08:26.187: option SERVERID(2), len 14

*Jan 28 15:08:26.187: 000100014684CC5E0018FEFBCC0F

```
*Jan 28 15:08:26.187: option IA-PD(25), len 41
*Jan 28 15:08:26.187: IAID 0x00030001, T1 302400, T2 483840
*Jan 28 15:08:26.191: option IAPREFIX(26), len 25
*Jan 28 15:08:26.191: preferred 604800, valid 1209600, prefix
2001:DB8:CAFE::/64
*Jan 28 15:08:26.191: option DNS-SERVERS(23), len 16
*Jan 28 15:08:26.191: 2001:C00::23:2
*Jan 28 15:08:26.191: option DOMAIN-LIST(24), len 10
*Jan 28 15:08:26.191: ecmd.com

! Note: The CPE receives the DHCPv6 'REPLY' message with embedded the delegated
prefix and accompanied information (DNS server, domain name, timers, etc...). Once
this information is received the CPE can start processing the information and
start dynamically configuring its interfaces and routing table.
```

CPE: Processing the 'REPLY' and dynamically configuring its interfaces with this information

```
*Jan 28 15:08:26.191: IPv6 DHCP: Processing options
*Jan 28 15:08:26.191: IPv6 DHCP: Adding prefix 2001:DB8:CAFE::/64 to PREFIX_1
*Jan 28 15:08:26.191: IPv6RT0: connected, Route add 2001:DB8:CAFE::/64 [new]
*Jan 28 15:08:26.191: IPv6RT0: connected, Add 2001:DB8:CAFE::/64 to table
*Jan 28 15:08:26.191: IPv6RT0: connected, Adding next-hop :: over Loopback100 for
2001:DB8:CAFE::/64, [0/0]
*Jan 28 15:08:26.191: IPv6RT0: connected, Route add 2001:DB8:CAFE::1/128 [new]
*Jan 28 15:08:26.191: IPv6RT0: connected, Add 2001:DB8:CAFE::1/128 to table
*Jan 28 15:08:26.191: IPv6RT0: connected, Adding next-hop :: over Loopback100 for
2001:DB8:CAFE::1/128, [0/0]
*Jan 28 15:08:26.191: IPv6RT0: static, Added backup for 2001:DB8:CAFE::/64,
distance 1
*Jan 28 15:08:26.191: IPv6 DHCP: T1 set to expire in 302400 seconds
*Jan 28 15:08:26.191: IPv6 DHCP: T2 set to expire in 483840 seconds
*Jan 28 15:08:26.191: IPv6 DHCP: Configuring DNS server 2001:C00::23:2
*Jan 28 15:08:26.191: IPv6 DHCP: Configuring domain name ecmd.com
*Jan 28 15:08:26.191: IPv6 DHCP: DHCPv6 changes state from REQUEST to OPEN
(REPLY_RECEIVED) on FastEthernet0/0
*Jan 28 15:08:26.195: IPv6RT0: Event: 2001:DB8:CAFE::/64, Add, owner connected,
previous None
*Jan 28 15:08:26.195: IPv6RT0: Event: 2001:DB8:CAFE::1/128, Add, owner connected,
previous None
*Jan 28 15:10:29.963: IPv6RT0: static, Route add ::/0 [new]
*Jan 28 15:10:29.963: IPv6RT0: static, Add ::/0 to table
*Jan 28 15:10:29.963: IPv6RT0: static, Adding next-hop FE80::21A:A1FF:FE7A:46A8
over FastEthernet0/0 for ::/0, [1/0]
*Jan 28 15:10:29.963: IPv6RT0: connected, Route add 2001:BEEF::/64 [new]
*Jan 28 15:10:29.963: IPv6RT0: connected, Add 2001:BEEF::/64 to table
*Jan 28 15:10:29.967: IPv6RT0: connected, Adding next-hop :: over FastEthernet0/0
for 2001:BEEF::/64, [0/0]
*Jan 28 15:10:29.967: IPv6RT0: Event: ::/0, Add, owner static, previous None
*Jan 28 15:10:29.967: IPv6RT0: Event: 2001:BEEF::/64, Add, owner connected,
previous None
```

```
*Jan 28 15:10:30.967: IPv6RT0: connected, Route add
2001:BEEF::21A:2FFF:FE87:5602/128 [new]
*Jan 28 15:10:30.967: IPv6RT0: connected, Add 2001:BEEF::21A:2FFF:FE87:5602/128
to table
*Jan 28 15:10:30.967: IPv6RT0: connected, Adding next-hop :: over FastEthernet0/0
for 2001:BEEF::21A:2FFF:FE87:5602/128, [0/0]
*Jan 28 15:10:30.967: IPv6RT0: Event: 2001:BEEF::21A:2FFF:FE87:5602/128, Add,
owner connected, previous None
! Note: The delegated prefix "2001:DB8:CAFE::/64" is added to the routing table
and based upon the router configuration also "loopback100" will receive an IPv6
address based upon this received IPv6 prefix, while inheriting the prefix timers
set by the DHCPv6 server (T1 and T2).
```

CPE: After DHCPv6-PD did the dynamic configuration of the interfaces

```
ecmd-1841-1#show ipv6 dhcp interface fastEthernet 0/0
```

FastEthernet0/0 is in client mode

State is OPEN

Renew will be sent in 17:30:30

List of known servers:

Reachable via address: FE80::21A:A1FF:FE7A:46A8

DUID: 000100014684CC5E0018FEFBCC0F

Preference: 0

Configuration parameters:

IA PD: IA ID 0x00030001, T1 302400, T2 483840

Prefix: 2001:DB8:CAFE::/64

preferred lifetime 604800, valid lifetime 1209600

expires at Feb 11 2008 03:08 PM (970231 seconds)

DNS server: 2001:C00::23:2

Domain name: ecmd.com

Prefix name: PREFIX_1

Rapid-Commit: disabled

```
ecmd-1841-1#show ipv6 interface brief
```

FastEthernet0/0 [up/up]

FE80::21A:2FFF:FE87:5602

2001:BEEF::21A:2FFF:FE87:5602

FastEthernet0/1 [up/up]

Serial0/0/0 [administratively down/down]

Serial0/0/1 [administratively down/down]

Serial0/0/2 [administratively down/down]

Serial0/0/3 [administratively down/down]

Loopback100 [up/up]

FE80::21A:2FFF:FE87:5602

2001:DB8:CAFE::1

! Note: The FastEthernet0/0 has both a global and a Link local address. The global address is seen on the router due to Stateless auto-configuration based upon RA (Router Advertisement) packets send by the upstream Service Provider router. The Loopback100 however is dynamically configured by DHCPv6-PD to the IPv6 address 2001:DB8:CAFE::1/64.

CPE: The routing table as seen on the CPE

ecmd-1841-1#**show ipv6 route**

IPv6 Routing Table - 6 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route, M - MIPv6

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

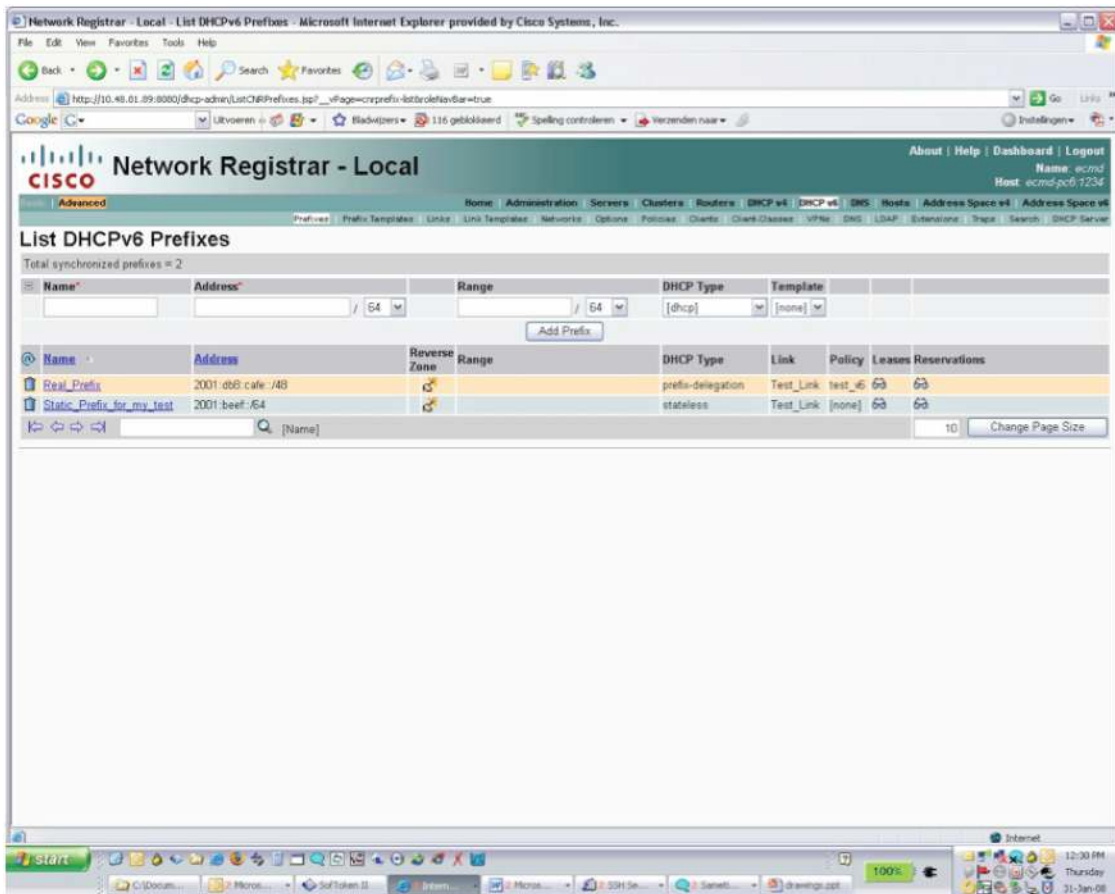
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

D - EIGRP, EX - EIGRP external

```
S  ::/0 [1/0]
    via FE80::21A:A1FF:FE7A:46A8, FastEthernet0/0
C  2001:DB8:CAFE::/64 [0/0]
    via ::, Loopback100
L  2001:DB8:CAFE::1/128 [0/0]
    via ::, Loopback100
C  2001:BEEF::/64 [0/0]
    via ::, FastEthernet0/0
L  2001:BEEF::21A:2FFF:FE87:5602/128 [0/0]
    via ::, FastEthernet0/0
L  FF00::/8 [0/0]
    via ::, Null0
```

The DHCPv6 Server used for the above test is the CNR7.0 (Cisco Network Registrar 7.0). The configuration for this test through the GUI can be observed below. Additionally, the DHCPv6-PD binding can be observed.



In the above example two entries have been configured:

Real_Prefix

The name has been randomly defined. For live deployments a meaningful name is recommended.

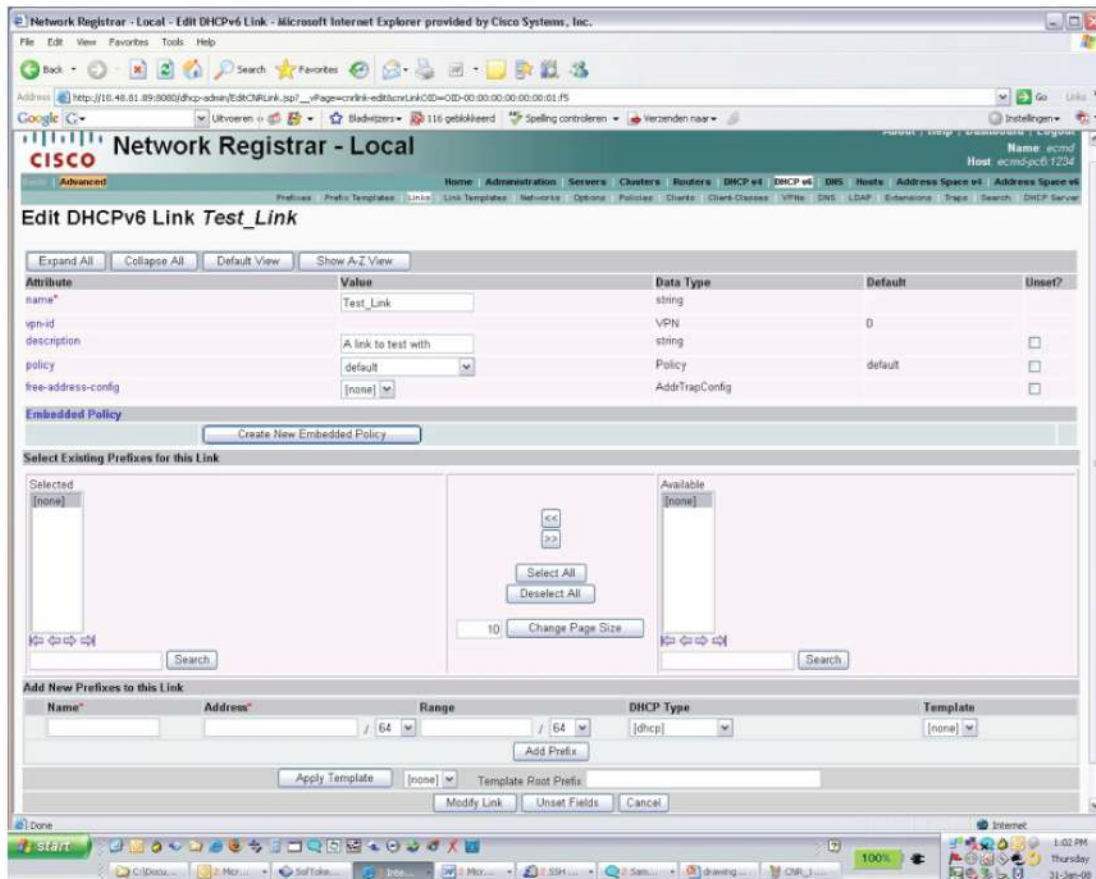
This entry carries the IPv6 prefixes used for Prefix Delegation. From the summary screen, it is seen that the prefix range is “2001:db8:cafe::/48” and that DHCP type is “Prefix-delegation”. The DHCPv6 configuration is for the Link “Test_Link”. The policy attached to this range of prefixes is “test-v6”. CNR allows for great flexibility and hierarchical policies, which it processes in a specific order to allow more specific policies (such as for a client) to override general policies (such as the system wide default policy).

Static_Prefix_for_my_test

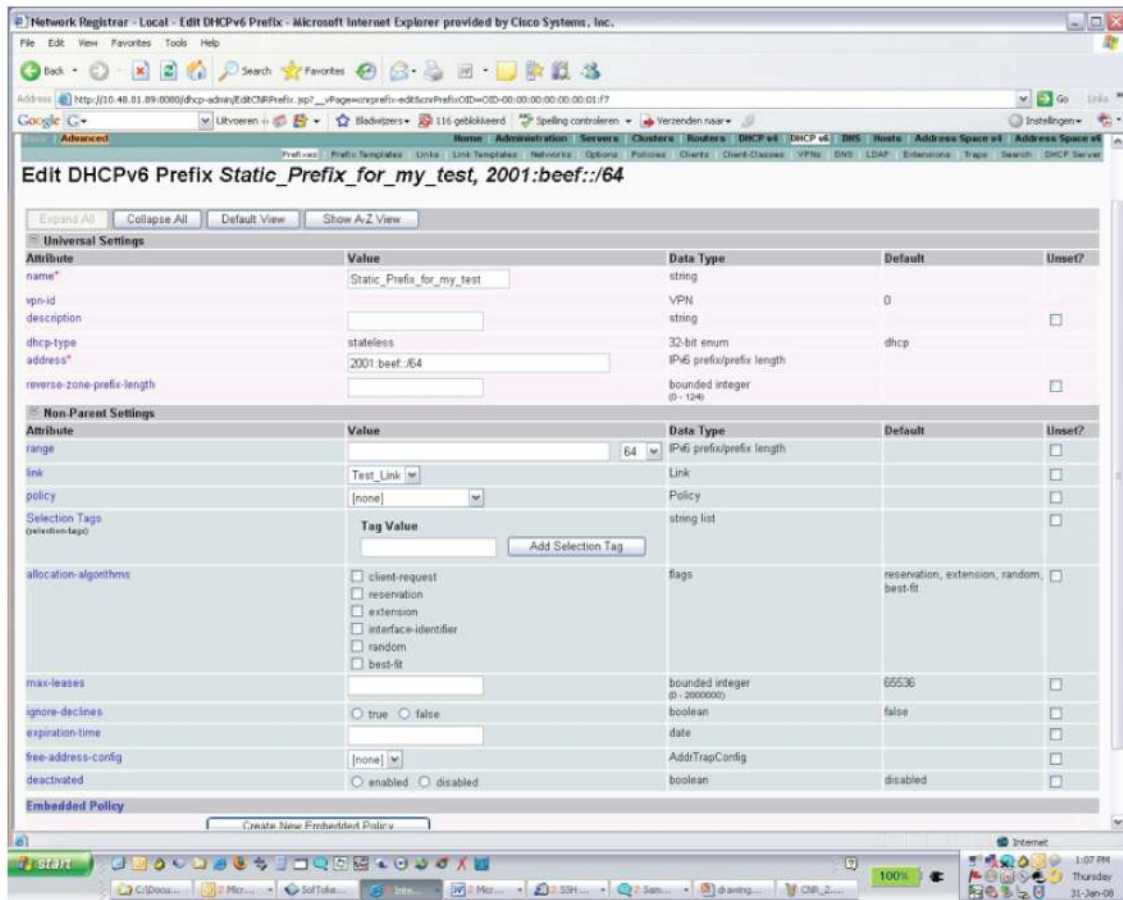
The name chosen has been randomly selected.

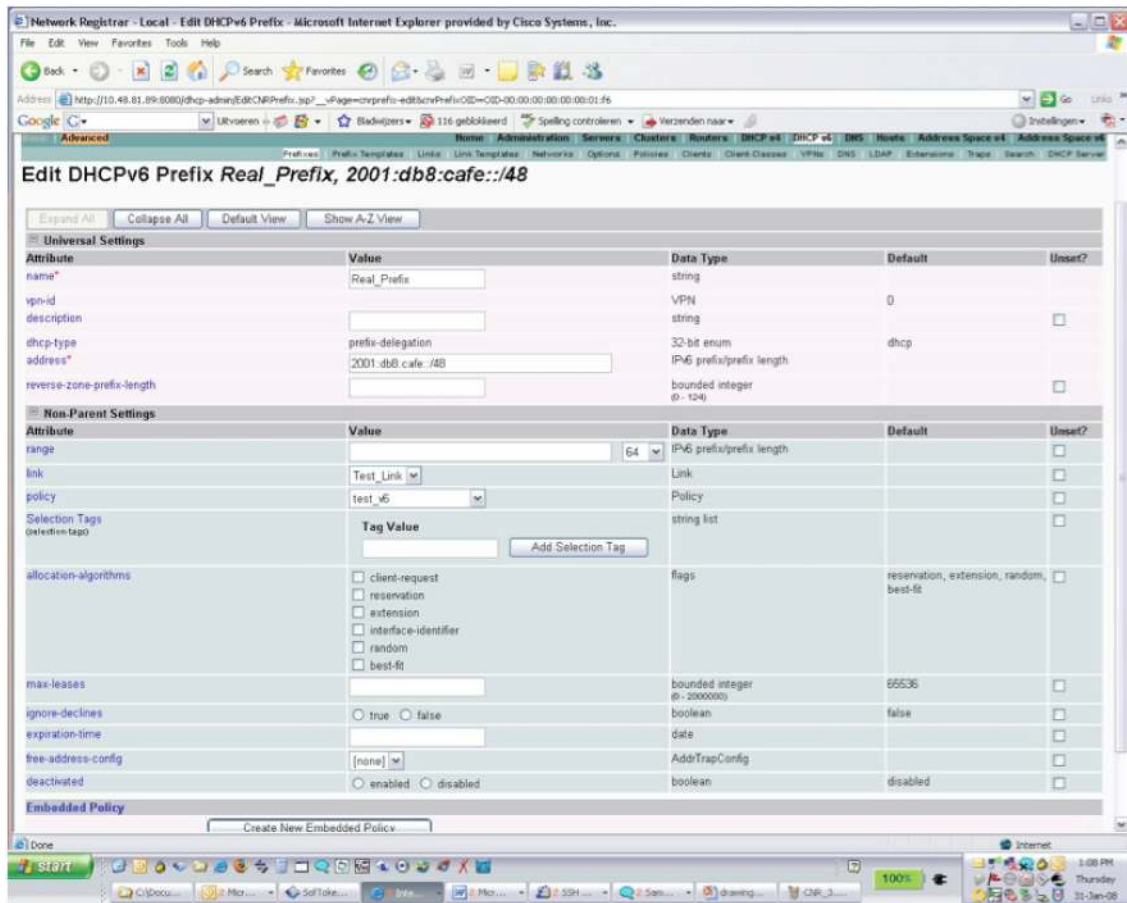
This entry is required to make a mapping between the used link and the delegated prefix. The DHCP type is “Stateless”. The value configured here is the link address “2001:beef::/64”. This entry provides the glue between the CPE and delegated prefix. If the DHCPv6 server received a DHCPv6 message for ‘Link’ entry of “2001:beef::/64”, then the DHCPv6 now realizes that it is for the ‘Link’ known by the CNR7.0 as “Test_Link” and that the prefixes it must assign are to be found under “Real_Prefix”. The CNR knows this because both the entry “Real_Prefix” and “Static_Prefix_for_my_test” have the same value “Test_Link” entry.

A look into the configuration for the 'Link' is shown below. For the configuration, just a name is created with all attributes left as default.

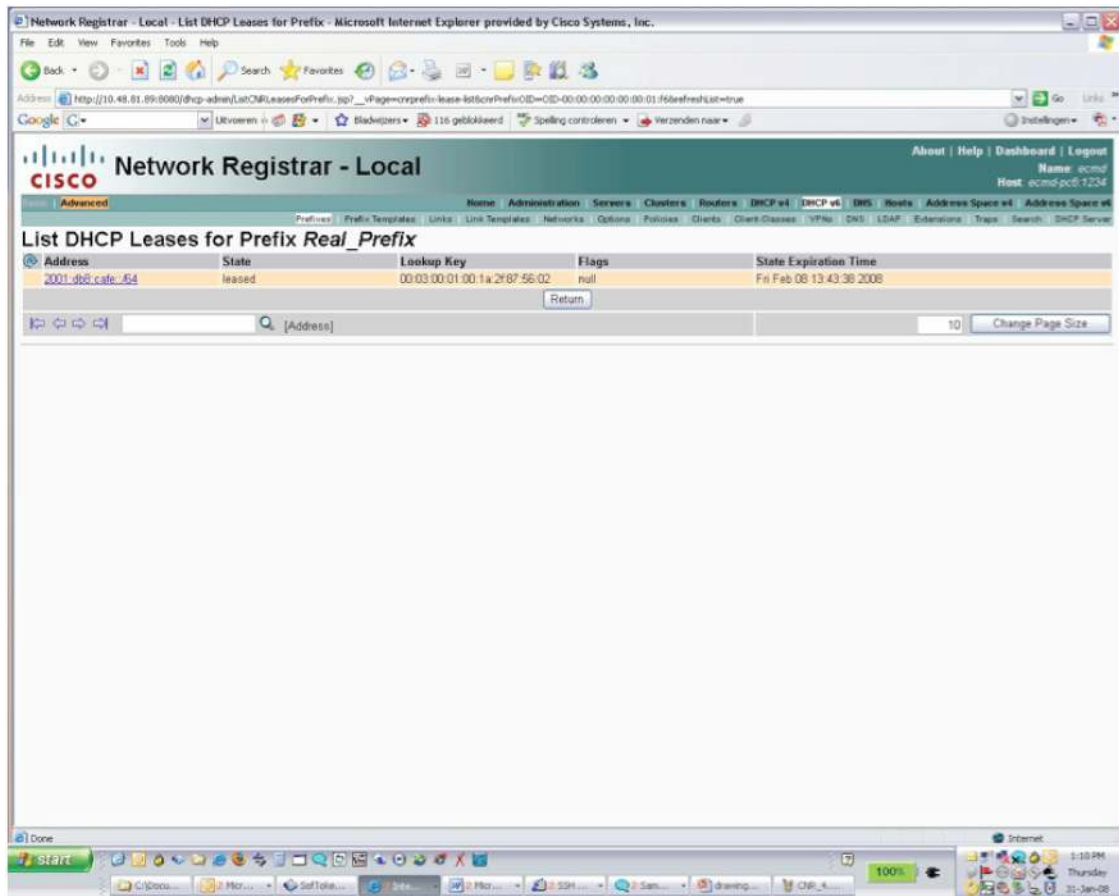


The configuration details of the prefixes discussed earlier are found in next two pictures:





An overview of the DHCPv6 leases on CNR7.0 is found in the below picture:



Deployment Model 3: DHCPv6-PD Relay at the Provider Edge Router and DHCPv6 remote-id Option
 This deployment model is from a packet exchange perspective identical to 'Deployment model 2'. The main difference is found in how the delegated prefix is identified. For deployment model 3, the delegated prefix is based at the server upon the 'remote-id' while deployment model 2 uses other mechanisms.

References

Cisco.com Web Site: <http://www.cisco.com/ipv6>

Cisco IPv6 Solutions:

http://www.cisco.com/en/US/technologies/collateral/tk648/tk872/tk373/technologies_white_paper_09186a00802219bc_ps6553_Products_White_Paper.html

Cisco IOS IPv6 Start Here: <http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-roadmap.html>

Cisco Network Registrar (log in required):

<http://www.cisco.com/en/US/partner/products/sw/netmgts/ps1982/index.html>

IANA, "Private Enterprise Numbers": <http://www.iana.org/assignments/enterprise-numbers>

RFC3315—Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

RFC3633—IPv6 Prefix Options for DHCPv6

RFC3646—DNS Configuration Options for DHCPv6

RFC4649—Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option

RFC4861—Neighbor Discovery for IP version 6 (IPv6)

RFC4862—IPv6 Stateless Address Autoconfiguration

RFC5007—DHCPv6 Leasequery



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA

C11-689821-00 10/11