DHCPv6 Options Support

- Information About DHCPv6 Options Support, on page 1
- How to Configure DHCPv6 Options Support, on page 3
- Configuration Examples for DHCPv6 Options Support, on page 5
- Verifying DHCPv6 Options Support, on page 5
- Additional References for DHCPv6 Options Support, on page 6
- Feature Information for DHCPv6 Options Support, on page 6

Information About DHCPv6 Options Support

CAPWAP Access Controller DHCPv6 Option

The Control And Provisioning of Wireless Access Points (CAPWAP) protocol allows lightweight access points to use DHCPv6 to discover a wireless controller to which it can connect. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.

Wireless access points use the DHCPv6 option 52 (RFC 5417) to supply the IPv6 management interface addresses of the primary, secondary, and tertiary wireless controllers.

Both stateless and stateful DHCPv6 addressing modes are supported. In stateless mode, access points obtain IPv6 address using the Stateless Address AutoConfiguration (SLAAC), while additional network information (not obtained from router advertisements) is obtained from a DHCPv6 server. In stateful mode, access points obtain both IPv6 addressing and additional network information exclusively from the DHCPv6 server. In both modes, a DHCPv6 server is required to provide option 52 if Wireless Controller discovery using DHCPv6 is required.

When the MAX_PACKET_SIZE exceeds 15, and option 52 is configured, the DHCPv6 server does not send DHCP packets.

DNS Search List Option

DNS Search List (DNSSL) is a list of Domain Name System (DNS) suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names. The DNSSL option contains one or more domain names. All domain names share the same lifetime value, which is the maximum time in seconds over which this DNSSL may be used. If different lifetime values are required, multiple DNSSL options can be used. There can be a maximum of 5 DNSSLs.
DHCP messages with long DNSSL names are discarded by the device.

**Note**

If DNS information is available from multiple Router Advertisements (RAs) and/or from DHCP, the host must maintain an ordered list of this DNS information.

RFC 6106 specifies IPv6 Router Advertisement (RA) options to allow IPv6 routers to advertise a DNS Search List (DNSSL) to IPv6 hosts for an enhanced DNS configuration.

The DNS lifetime range should be between the maximum RA interval and twice the maximum RA interval, as displayed in the following example:

\[(\text{max ra interval}) \leq \text{dns lifetime} \leq (2*(\text{max ra interval}))\]

The maximum RA interval can have a value between 4 and 1800 seconds (the default is 240 seconds). The following example shows an out-of-range lifetime:

```
Device(config-if)# ipv6 nd ra dns-search-list sss.com 3600
! Lifetime configured out of range for the interface that has the default maximum RA interval.!
```

**DHCPv6 Client Link-Layer Address Option**

The DHCPv6 Client Link-Layer Address Option (RFC 6939) defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in DHCPv6 messages that are sent towards the server.

The Client Link-Layer Address option is only exchanged between relay agents and servers. DHCPv6 clients are not aware of the use of the Client Link-Layer Address option. The DHCPv6 client must not send the Client Link-Layer Address option, and must ignore the Client Link-Layer Address option if received.

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is carried in the client identifier and server identifier options. The DUID is unique across all DHCP clients and servers, and it is stable for any specific client or server. DHCPv6 uses DUIDs based on link-layer addresses for both the client and server identifier. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

**DHCP Relay Agent**

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces.
# How to Configure DHCPv6 Options Support

## Configuring CAPWAP Access Points

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 dhcp pool poolname</td>
<td>Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# ipv6 dhcp pool pool1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>capwap-ac address ipv6-address</td>
<td>Configures CAPWAP access controller address.</td>
</tr>
<tr>
<td>Example: Device(config-dhcpv6)# capwap-ac address 2001:DB8::1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
<td>Exits DHCPv6 pool configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-dhcpv6)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Configuring DNS Search List Using IPv6 Router Advertisement Options

### Note

The domain name configuration should follow RFC 1035. If not, the configuration will be rejected. For example, the following domain name configuration will result in an error:

```
Device(config-if)# ipv6 nd ra dns-search-list domain example.example.com infinite-lifetime
```

### Note

The `ipv6 nd ra dns-search-list domain` command can only be configured on physical interfaces that are configured as routed ports in layer 3 mode. This is done by running the `no switchport` command.
Use the `no ipv6 nd ra dns-search-list domain domain-name` command to delete a single DNS search list under an interface.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
Example:  
Device> enable |  
*Enter your password if prompted.* |
| 2    | configure terminal| Enters global configuration mode.  
Example:  
Device# configure terminal |
| 3    | interface interface-type interface-number | Configures an interface and enters interface configuration mode.  
Example:  
Device(config)# interface GigabitEthernet 0/2/0 |
| 4    | no switchport    | For physical ports only, enters Layer 3 mode.  
Example:  
Device(config-if)# no switchport |
| 5    | ipv6 nd prefix ipv6-prefix/prefix-length | Configures IPv6 prefixes that are included in IPv6 Neighbor Discovery (ND) router advertisements,  
Example:  
Device(config-if)# ipv6 nd prefix 2001:DB8::1/64 1111 222 |
| 6    | ipv6 nd ra lifetime seconds | Configures the device lifetime value in IPv6 router advertisements on an interface.  
Example:  
Device(config-if)# ipv6 nd ra lifetime 9000 |
| 7    | ipv6 nd ra dns-search-list domain domain-name [lifetime [lifetime-value | infinite ] ] | Configures the DNS search list. You can specify the lifetime of the search list.  
**Note** For releases earlier than Cisco IOS XE Giraltar 16.12.1, this command existed as `ipv6 nd ra dns search list list-name infinite-lifetime`  
Example:  
Device(config-if)# ipv6 nd ra dns-search-list domain example.example.com lifetime infinite |
| 8    | end               | Exits interface configuration mode and returns to privileged EXEC mode.  
Example:  
Device(config-if)# end |
Configuration Examples for DHCPv6 Options Support

Example: Configuring CAPWAP Access Points

The following example shows how to configure a CAPWAP access point:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1
Device(config-dhcpv6)# end
Device#
```

Verifying DHCPv6 Options Support

Verifying Option 52 Support

The following sample output from the `show ipv6 dhcp pool` command displays the DHCPv6 configuration pool information:

```
Device# show ipv6 dhcp pool
DHCPv6 pool: svr-p1
Static bindings:
  Binding for client 000300010002FCA5C01C
    IA PD: IA ID 00040002,
    Prefix: 2001:db8::3/72
    preferred lifetime 604800, valid lifetime 2592000
    IA PD: IA ID not specified; being used by 00040001
    Prefix: 2001:db8::1/72
    preferred lifetime 240, valid lifetime 54321
    Prefix: 2001:db8::2/72
    preferred lifetime 300, valid lifetime 54333
    Prefix: 2001:db8::3/72
    preferred lifetime 280, valid lifetime 51111
Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
DNS server: 1001::1
DNS server: 1001::2
CAPWAP-AC Controller address: 2001:DB8::1
Domain name: example1.com
Domain name: example2.com
Domain name: example3.com
Active clients: 2
```

The following example shows how to enable debugging for DHCPv6:

```
Device# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```
Additional References for DHCPv6 Options Support

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standards/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 6106</td>
<td>IPv6 Router Advertisement Options for DNS Configuration</td>
</tr>
<tr>
<td>RFC 54171</td>
<td>Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option</td>
</tr>
<tr>
<td>RFC 6939</td>
<td>Client Link-Layer Address Option in DHCPv6</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for DHCPv6 Options Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPWAP Access Controller DHCPv6 Option-52</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The CAPWAP protocol allows lightweight access points to use DHCPv6 to discover a Wireless Controller to which it can connect. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.</td>
</tr>
<tr>
<td>DHCPv6 Client Link-Layer Address Option</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The DHCPv6 Client Link-Layer Address Option (RFC 6939) defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages being sent towards the server.</td>
</tr>
<tr>
<td>DNS Search List</td>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>DNS Search List (DNSSL) is a list of Domain Name System (DNS) suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names. The DNSSL option contains one or more domain names.</td>
</tr>
<tr>
<td>DHCPv6 Relay Chaining and Route Insertion</td>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>DHCPv6 Relay Chaining and Route Insertion feature allows DHCPv6 messages to be relayed through multiple relay agents.</td>
</tr>
<tr>
<td>DHCPv6 Client Link-Layer Address Option - Command Changes</td>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>The syntax of <code>ipv6 nd ra dns-search-list domain</code> command was modified to <code>ipv6 nd ra dns-search-list domain</code>. The <code>show ipv6 nd ra dns-search-list</code> command was introduced.</td>
</tr>
<tr>
<td>IPv6 Support for RFC 6106 and RFC 5417</td>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>IPv6 support was introduced for Router Advertisement Options for DNS Configuration (RFC 6106), and Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option (RFC 5417).</td>
</tr>
</tbody>
</table>