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.

Information About DHCPv6 Options Support

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 bea maximum of 5 DNSSLs.

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:

```
(max ra interval) <= dns lifetime <= (2*(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

Cisco IOS XE Fuji 16.8.1a supports DHCPv6 Client Link-Layer Address Option (RFC 6939). It 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.

DHCPv6 Relay Agent

A DHCPv6 relay agent, which may reside on a client link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. The DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send messages to a DHCPv6 server that is not connected to the same link. IPv6 enable is required for IPv6 DHCP relay, even if the IPv6 address is configured.

How to Configure DHCPv6 Options Support

Configuring CAPWAP Access Points

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**capwap-ac address** *ipv6-address* **Example:** `Device(config-dhcpv6)# capwap-ac address 2001:DB8::1`	Configures CAPWAP access controller address.
Step 5	**end** **Example:** `Device(config-dhcpv6)# end`	Exits DHCPv6 pool configuration mode and returns to privileged EXEC mode.

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 lifetime infinite
```

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Device(config)# interface GigabitEthernet 0/2/0`	Configures an interface and enters interface configuration mode.
Step 4	**no switchport** **Example:** `Device(config-if)# no switchport`	For physical ports only, enters Layer 3 mode.
Step 5	**ipv6 nd prefix** *ipv6-prefix/prefix-length* **Example:** `Device(config-if)# ipv6 nd prefix 2001:DB8::1/64 1111 222`	Configures IPv6 prefixes that are included in IPv6 Neighbor Discovery (ND) router advertisements,
Step 7	**ipv6 nd ra lifetime** *seconds* **Example:** `Device(config-if)# ipv6 nd ra lifetime 9000`	Configures the device lifetime value in IPv6 router advertisements on an interface.
Step 7	**ipv6 nd ra dns-search-list domain** *domain-name* [**lifetime** [*lifetime-value* | **infinite**]] **Example:** `Device(config-if)# ipv6 nd ra dns-search-list domain example.example.com lifetime infinite`	Configures the DNS search list. You can specify the life time 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**
Step 8	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

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)
```

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 1: Feature Information for DHCPv6 Options Support

Feature Name	Release	Feature Information
CAPWAP Access Controller DHCPv6 Option-52	Cisco IOS XE Fuji 16.8.1a	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.
DHCPv6 Client Link-Layer Address Option	Cisco IOS XE Fuji 16.8.1a	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.
DNS Search List	Cisco IOS XE Fuji 16.8.1a	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.