DHCPv6 Options Support

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 bea 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:

```
(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

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

	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 .example.example.com infinite-lifetime
```

Use the **no ipv6 nd ra dns search list name** command to delete a single DNS search list under an interface. Use the **no ipv6 nd ra dns search list** command to delete all DNS search lists 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	**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 5	**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 6	**ipv6 nd ra dns search list** *list-name* [**infinite-lifetime**] **Example:** `Device(config-if)# ipv6 nd ra dns search list example.example.com infinite-lifetime`	Configures the DNS search list. You can specify the life time of the search list.

Step 7	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

What to do next

Use the **show ipv6 nd idb interface** command to verify the DNS search list configuration based on IPv6 RA options:

```
Device# show ipv6 nd idb interface gigabitEthernet 0/2/0/0 detail location 0/2/CPU0

Mon Jul 4 14:28:53.422 IST

ifname: Gi0/2/0/0, ifh: 0x01000300, iftype: 15, VI-type: 0, Pseudo IDB: FALSE
vrf-id: 0x60000000, table-id: 0xe0800000
Mac Addr: 02d1.1e2b.0baf, size: 6, VLan tag set: FALSE
```

```
Media Name: ether, Media Encap: 0x1 (ARPA)
Mac Length: 6, Media Header Len: 14, Media Proto: 0xdd86
Current Encap: 0x1 (ARPA), Mcast Encap : 0x1 (ARPA)

IPV6 Interface: Enabled, IPV6: Enabled, MPLS: Disabled
Link local address: 2001::d1:1eff:fe2b:baf, Global Addr count: 1
Global Addresses:1::1(0x2),
Default Prefix Address: ::, Prefix Addr Count: 3,
Prefix addresses: 1::(0x401), 2001:db8:e8:1011::(0x4), 2001:db8:e8:1011::(0x4)

RA Specific Route Count: 1,
RA Specific Route : Address 3:: Prefix Length 116 Lifetime 1112 Preference Low

RA DNS Search List Count: 3,
RA DNS Search List : Name example.example.com Lifetime 240
RA DNS Search List : Name example1.example1.com Lifetime 240
RA DNS Search List : Name example2.example2.com Lifetime 4294967295
```

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)
```

Troubleshooting DNS Search Lists

Recursive DNS servers and DNS search lists are sent as part of RA messages. Run the IPv6 ND traces to debug any particular issue related to a DNS servers and DNS search lists:

```
Device# show ipv6 nd trace location 0/2/CPU0

Jun 30 20:07:03.508 nd/fevent 0/2/CPU0 t26702 Sending RA to ff02::1 on GigabitEthernet0/2/0/0
 (0x1000300)
Jun 30 20:07:03.508 nd/fevent 0/2/CPU0 t26702 hoplimit 64 lifetime 9000 reachable 0 retrans
 0
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 1::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 2592000 pref 604800
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 2002:4898:e8:1011::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 2002:4899:e8:1011::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra specific route address 3:: lifetime 1112
preference Low
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 5::6 lifetime 240 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 5::5 lifetime 240 part
 of same ra dns server option
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 4::4 lifetime 4294967295
 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example.example.com
lifetime 240 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example1.example1.com
 lifetime 240 part of
same ra dns search list option
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example2.example2.com
 lifetime 4294967295 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_send_ra: sending RA paksize=320, plen=280
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_pak_send: size=320, ifh
GigabitEthernet0/2/0/0 (0x1000300) ,
priority=2 to ipv6-io
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_pak_send: sending pak=0x60c07d8b with NO
FVS set, size=320,
ifh GigabitEthernet0/2/0/0 (0x1000300) to ipv6-io
```

Additional References for DHCPv6 Options Support

Standards and RFCs

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

Feature History for DHCPv6 Options Support

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.11.1	CAPWAP Access Controller DHCPv6 Option-52	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	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	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.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.