



DHCP and DDNS Services

This chapter describes how to configure the DHCP server or DHCP relay as well as dynamic DNS (DDNS) update methods.

- [About DHCP and DDNS Services, on page 1](#)
- [Guidelines for DHCP and DDNS Services, on page 2](#)
- [Configure the DHCP Server, on page 3](#)
- [Configure the DHCP Relay Agent, on page 7](#)
- [Configure Dynamic DNS, on page 10](#)
- [Monitoring DHCP and DDNS Services, on page 14](#)
- [History for DHCP and DDNS Services, on page 15](#)

About DHCP and DDNS Services

The following topics describe the DHCP server, DHCP relay agent, and DDNS update.

About the DHCPv4 Server

DHCP provides network configuration parameters, such as IP addresses, to DHCP clients. The ASA can provide a DHCP server to DHCP clients attached to ASA interfaces. The DHCP server provides network configuration parameters directly to DHCP clients.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68; the DHCP server listens for messages on UDP port 67.

The DHCP server for IPv6 is not supported; you can, however, enable DHCP relay for IPv6 traffic.

DHCP Options

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. The configuration parameters are carried in tagged items that are stored in the Options field of the DHCP message and the data are also called options. Vendor information is also stored in Options, and all of the vendor information extensions can be used as DHCP options.

For example, Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address preconfigured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

- DHCP option 150 provides the IP addresses of a list of TFTP servers.

- DHCP option 66 gives the IP address or the hostname of a single TFTP server.
- DHCP option 3 sets the default route.

A single request might include both options 150 and 66. In this case, the ASA DHCP server provides values for both options in the response if they are already configured on the ASA.

You can use advanced DHCP options to provide DNS, WINS, and domain name parameters to DHCP clients; DHCP option 15 is used for the DNS domain suffix. You can also use the DHCP automatic configuration setting to obtain these values or define them manually. When you use more than one method to define this information, it is passed to DHCP clients in the following sequence:

1. Manually configured settings.
2. Advanced DHCP options settings.
3. DHCP automatic configuration settings.

For example, you can manually define the domain name that you want the DHCP clients to receive and then enable DHCP automatic configuration. Although DHCP automatic configuration discovers the domain together with the DNS and WINS servers, the manually defined domain name is passed to DHCP clients with the discovered DNS and WINS server names, because the domain name discovered by the DHCP automatic configuration process is superseded by the manually defined domain name.

About the DHCP Relay Agent

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers. DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the ASA because it does not forward broadcast traffic. The DHCP relay agent lets you configure the interface of the ASA that is receiving the broadcasts to forward DHCP requests to a DHCP server on another interface.

Guidelines for DHCP and DDNS Services

This section includes guidelines and limitations that you should check before configuring DHCP and DDNS services.

Firewall Mode

- DHCP Relay is not supported in transparent firewall mode.
- DHCP Server is supported in transparent firewall mode on a bridge group member interface.
- DDNS is not supported in transparent firewall mode.

IPv6

Does not support IPv6 for DHCP server; IPv6 for DHCP relay is supported.

DHCPv4 Server

- The maximum available DHCP pool is 256 addresses.
- You can configure only one DHCP server on each interface. Each interface can have its own pool of addresses to use. However the other DHCP settings, such as DNS servers, domain name, options, ping timeout, and WINS servers, are configured globally and used by the DHCP server on all interfaces.
- You cannot configure an interface as a DHCP client if that interface also has DHCP server enabled; you must use a static IP address.
- You cannot configure both a DHCP server and DHCP relay on the same device, even if you want to enable them on different interfaces; you can only configure one type of service.
- ASA does not support QIP DHCP servers for use with the DHCP proxy service.
- The DHCP server does not support BOOTP requests.

DHCP Relay

- You can configure a maximum of 10 DHCPv4 relay servers in single mode and per context, global and interface-specific servers combined, with a maximum of 4 servers per interface.
- You can configure a maximum of 10 DHCPv6 relay servers in single mode and per context. Interface-specific servers for IPv6 are not supported.
- You cannot configure both a DHCP server and DHCP relay on the same device, even if you want to enable them on different interfaces; you can only configure one type of service.
- DHCP relay services are not available in transparent firewall mode. You can, however, allow DHCP traffic through using an access rule. To allow DHCP requests and replies through the ASA, you need to configure two access rules, one that allows DHCP requests from the inside interface to the outside (UDP destination port 67), and one that allows the replies from the server in the other direction (UDP destination port 68).
- For IPv4, clients must be directly-connected to the ASA and cannot send requests through another relay agent or a router. For IPv6, the ASA supports packets from another relay server.
- The DHCP clients must be on different interfaces from the DHCP servers to which the ASA relays requests.
- You cannot enable DHCP Relay on an interface in a traffic zone.
- DHCP relay is not supported on Virtual Tunnel Interfaces (VTIs).

Configure the DHCP Server

This section describes how to configure a DHCP server provided by the ASA.

Procedure

-
- Step 1** [Enable the DHCPv4 Server, on page 4.](#)

Step 2 [Configure Advanced DHCPv4 Options, on page 6.](#)

Enable the DHCPv4 Server

To enable the DHCP server on an ASA interface, perform the following steps:

Procedure

Step 1 Create a DHCP address pool for an interface. The ASA assigns a client one of the addresses from this pool to use for a given period of time. These addresses are the local, untranslated addresses for the directly connected network.

dhcpcd address *ip_address_start-ip_address_end if_name*

Example:

```
ciscoasa(config)# dhcpcd address 10.0.1.101-10.0.1.110 inside
```

The address pool must be on the same subnet as the ASA interface. In transparent mode, specify a bridge group member interface.

Step 2 (Optional) (Routed mode) Automatically configure DNS, WINS, and domain name values obtained from an interface running a DHCP or PPPoE client, or from a VPN server.

dhcpcd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Example:

```
ciscoasa(config)# dhcpcd auto_config outside interface inside
```

If you specify DNS, WINS, or domain name parameters using the following commands, then they overwrite the parameters obtained by automatic configuration.

Step 3 (Optional) Reserve a DHCP address for a client. The ASA assigns a specific address from the configured address pool to a DHCP client based on the client's MAC address.

dhcpcd reserve-address *ip_address mac_address if_name*

Example:

```
ciscoasa(config)# dhcpcd reserve-address 10.0.1.109 030c.f142.4cde inside
```

The reserved address must come from the configured address pool, and the address pool must be on the same subnet as the ASA interface. In transparent mode, specify a bridge group member interface.

Step 4 (Optional) Specify the IP address(es) of the DNS server(s).

dhcpcd dns *dns1 [dns2]*

Example:

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

Step 5 (Optional) Specify the IP address(es) of the WINS server(s). You may specify up to two WINS servers.

```
dhcpd wins wins1 [wins2]
```

Example:

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

Step 6 (Optional) Change the lease length to be granted to the client. The lease length equals the amount of time in seconds that the client can use its allocated IP address before the lease expires. Enter a value from 0 to 1,048,575. The default value is 3600 seconds.

```
dhcpd lease lease_length
```

Example:

```
ciscoasa(config)# dhcpd lease 3000
```

Step 7 (Optional) Configure the domain name.

```
dhcpd domain domain_name
```

Example:

```
ciscoasa(config)# dhcpd domain example.com
```

Step 8 (Optional) Configure the DHCP ping timeout value for ICMP packets. To avoid address conflicts, the ASA sends two ICMP ping packets to an address before assigning that address to a DHCP client. The default is 50 milliseconds.

```
dhcpd ping timeout milliseconds
```

Example:

```
ciscoasa(config)# dhcpd ping timeout 20
```

Step 9 Define a default gateway that is sent to the DHCP clients. For routed mode, if you do not use the **dhcpd option 3 ip** command, then the ASA sends the DHCP server-enabled interface IP address as the default gateway. For transparent mode, you must set **dhcpd option 3 ip** if you want to set a default gateway; the ASA itself cannot act as the default gateway.

```
dhcpd option 3 ip gateway_ip
```

Example:

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

Step 10 Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface.

```
dhcpd enable interface_name
```

Example:

```
ciscoasa(config)# dhcpd enable inside
```

Specify the same interface as the **dhcpd address** range.

Configure Advanced DHCPv4 Options

The ASA supports the DHCP options listed in RFC 2132, RFC 2562, and RFC 5510 to send information. All DHCP options (1 through 255) are supported except for 1, 12, 50–54, 58–59, 61, 67, and 82.

Procedure

Step 1 Configure a DHCP option that returns one or two IP addresses:

```
dhcpd option code ip addr_1 [addr_2]
```

Example:

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

Option 150 provides the IP address or names of one or two TFTP servers for use with Cisco IP phones. Option 3 sets the default route for Cisco IP phones.

Step 2 Configure a DHCP option that returns a text string:

```
dhcpd option code ascii text
```

Example:

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

Option 66 provides the IP address or name of a TFTP server for use with Cisco IP phones.

Step 3 Configure a DHCP option that returns a hexadecimal value.

```
dhcpd option code hex value
```

Example:

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

Note The ASA does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter the **dhcpd option 46 ascii hello** command, and the ASA accepts the configuration, although option 46 is defined in RFC 2132 to expect a single-digit, hexadecimal value. For more information about option codes and their associated types and expected values, see RFC 2132.

The following table shows the DHCP options that are not supported by the **dhcpd option** command.

Table 1: Unsupported DHCP Options

Option Code	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Configure the DHCP Relay Agent

When a DHCP request enters an interface, the DHCP servers to which the ASA relays the request depends on your configuration. You may configure the following types of servers:

- Interface-specific DHCP servers—When a DHCP request enters a particular interface, then the ASA relays the request only to the interface-specific servers.
- Global DHCP servers—When a DHCP request enters an interface that does not have interface-specific servers configured, the ASA relays the request to all global servers. If the interface has interface-specific servers, then the global servers are not used.

Configure the DHCPv4 Relay Agent

When a DHCP request enters an interface, the ASA relays the request to the DHCP server.

Procedure

Step 1 Do one or both of the following:

- Specify a global DHCP server IP address and the interface through which it is reachable.

dhcprelay server *ip_address if_name*

Example:

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- Specify the interface ID connected to the DHCP client network, and the DHCP server IP address to be used for DHCP requests that enter that interface.

interface *interface_id*
dhcprelay server *ip_address*

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

Note that you do not specify the egress interface for the requests, as in the global **dhcprelay server** command; instead, the ASA uses the routing table to determine the egress interface.

Step 2 Enable the DHCP relay service on the interface connected to the DHCP clients. You can enable DHCP relay on multiple interfaces.

dhcprelay enable *interface*

Example:

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

Step 3 (Optional) Set the number of seconds allowed for DHCP relay address handling.

dhcprelay timeout *seconds*

Example:

```
ciscoasa(config)# dhcprelay timeout 25
```


- Step 4** (Optional) Change the first default router address in the packet sent from the DHCP server to the address of the ASA interface.

dhcprelay setroute *interface_name*

Example:

```
ciscoasa(config)# dhcprelay setroute inside
```

This action allows the client to set its default route to point to the ASA even if the DHCP server specifies a different router.

If there is no default router option in the packet, the ASA adds one containing the interface address.

- Step 5** (Optional) Configure interfaces as trusted interfaces. Do one of the following:

- Specify a DHCP client interface that you want to trust:

```
interface interface_id
  dhcprelay information trusted
```

Example:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

You can configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface.

- Configure all client interfaces as trusted:

dhcprelay information trust-all

Example:

```
ciscoasa(config)# dhcprelay information trust-all
```

Configure the DHCPv6 Relay Agent

When a DHCPv6 request enters an interface, the ASA relays the request to all DHCPv6 global servers.

Procedure

- Step 1** Specify the IPv6 DHCP server destination address to which client messages are forwarded.

ipv6 dhcprelay server *ipv6_address* [*interface*]

Example:

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

The *ipv6-address* argument can be a link-scoped unicast, multicast, site-scoped unicast, or global IPv6 address. Unspecified, loopback, and node-local multicast addresses are not allowed as the relay destination. The optional *interface* argument specifies the egress interface for a destination. Client messages are forwarded to the destination address through the link to which the egress interface is connected. If the specified address is a link-scoped address, then you must specify the interface.

Step 2 Enable DHCPv6 relay service on an interface.

ipv6 dhcprelay enable *interface*

Example:

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Step 3 (Optional) Specify the amount of time in seconds that is allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding for relay address handling.

ipv6 dhcprelay timeout *seconds*

Example:

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

Valid values for the *seconds* argument range from 1 to 3600. The default is 60 seconds.

Configure Dynamic DNS

When an interface uses DHCP IP addressing, the assigned IP address can change when the DHCP lease is renewed. When the interface needs to be reachable using a fully qualified domain name (FQDN), the IP address change can cause the DNS server resource records (RRs) to become stale. Dynamic DNS (DDNS) provides a mechanism to update DNS RRs whenever the IP address or hostname changes. You can also use DDNS for static or PPPoE IP addressing.

DDNS updates the following RRs on the DNS server: the A RR includes the name-to-IP address mapping, while the PTR RR maps addresses to names.

The ASA supports the DDNS update method is defined by RFC 2136. It does not support the Web update method. With this method, the ASA and the DHCP server use DNS requests to update the DNS RRs. The ASA or DHCP server sends a DNS request to its local DNS server for information about the hostname and, based on the response, determines the main DNS server that owns the RRs. The ASA or DHCP server then sends an update request directly to the main DNS server. See the following typical scenarios.

- The ASA updates the A RR, and the DHCP server updates the PTR RR.

Typically, the ASA "owns" the A RR, while the DHCP server "owns" the PTR RR, so both entities need to request updates separately. When the IP address or hostname changes, the ASA sends a DHCP request to the DHCP server to inform it that it needs to request a PTR RR update.

- The DHCP server updates both the A and PTR RR.

Use this scenario if the ASA does not have the authority to update the A RR. When the IP address or hostname changes, the ASA sends a DHCP request to the DHCP server to inform it that it needs to request an A and PTR RR update.

You can configure different ownership depending on your security needs and the requirements of the main DNS server. For example, for a static address, the ASA should own the updates for both records.



Note DDNS is not supported on the BVI or bridge group member interfaces.

Before you begin

- Configure a DNS server on **Configuration > Device Management > DNS > DNS Client**. See [Configure the DNS Server](#).
- Configure the device hostname and domain name on **Configuration > Device Setup > Device Name/Password**. See [Set the Hostname, Domain Name, and the Enable and Telnet Passwords](#). If you do not specify the hostname per interface, then the device hostname is used. If you do not specify an FQDN, then for static or PPPoE IP addressing, the system domain name or the DNS server domain name is appended to the hostname.

Procedure

Step 1 Configure a DDNS update method to enable DNS requests from the ASA.

You do not need to configure a DDNS update method if the DHCP server will perform all requests.

- a) Create an update method.

ddns update method *name*

Example:

```
ciscoasa(config)# ddns update method ddns1
ciscoasa(DDNS-update-method)#
```

- b) Specify the standard DDNS method.

ddns [**both**]

By default, the ASA updates the A RR only. Use this setting if you want the DHCP server to update the PTR RR. If you want the ASA to update both the A and PTR RR, specify **both**. Use the **both** keyword for static or PPPoE IP addressing.

Example:

```
ciscoasa(DDNS-update-method)# ddns
```

- c) (Optional) Configure the update interface between DNS requests.

interval maximum *days hours minutes seconds*

By default when all values are set to 0, update requests are sent whenever the IP address or hostname changes. To send requests regularly, set the *days* (0-364), *hours*, *minutes*, and *seconds*.

Example:

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

- d) Associate this method with an interface. See [Step 2, on page 12](#).

Step 2

Configure interface settings for DDNS, including setting the update method, DHCP client settings, and the hostname for this interface.

- a) Enter interface configuration mode.

interface *id*

Example:

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)#
```

- b) Assign an update method.

ddns update *name*

You do not need to assign a method if you want the DHCP server to perform all updates.

Example:

```
ciscoasa(config-if)# ddns update ddns1
```

- c) Assign a hostname for this interface.

ddns update hostname *hostname*

If you do not set the hostname, the device hostname is used. If you do not specify an FQDN, then the system domain name or the default domain from the DNS server group is appended (for static or PPPoE IP addressing) or the domain name from the DHCP server is appended (for DHCP IP addressing).

Example:

```
ciscoasa(config-if)# ddns update hostname asa1.example.com
```

- d) Determine which records you want the DHCP server to update.

dhcp client update dns [**server** {**both** | **none**}]

The ASA sends DHCP client requests to the DHCP server. Note that the DHCP server must also be configured to support DDNS. The server can be configured to honor the client requests, or it can override the client (in which case, it will reply to the client so the client does not also try to perform updates that the server is performing). Even if the client does not request DDNS updates, the DHCP server can be configured to send updates anyway.

For static or PPPoE IP addressing, these settings are ignored.

Note You can also set these values globally for all interfaces using the **dhcp-client update dns** command. The per-interface settings take precedence over the global settings.

- **Default (no keywords)**—Requests that the DHCP server perform the PTR RR update. This setting works in conjunction with a DDNS update method with **ddns A** Records enabled.
- **server both**—Requests that the DHCP server perform both A and PTR RR updates. This setting does not require a DDNS update method to be associated with the interface.
- **server none**—Requests the DHCP server not to perform updates. This setting works in conjunction with a DDNS update method with **ddns both** A and PTR records enabled.

Example:

```
ciscoasa(config-if)# ddns client update dns
```

Static IP Address

The following example shows how to configure the standard DDNS method for use with a static IP address. Note that you do not configure DHCP client settings for this scenario.

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
interface gigabitethernet1/1
  ip address 209.165.200.225
! Associate the method with the interface:
ddns update ddns-2
ddns update hostname asa1.example.com
```

Example:ASA Updates A RR and DHCP Server Updates PTR RR

The following example configures the ASA to update the A RR and the DHCP server to update the PTR RR.

```
! Define the DDNS method to update the A RR:
ddns update method ddns-1
  ddns
interface gigabitethernet1/1
  ip address dhcp
! Associate the method with the interface:
ddns update ddns-1
  ddns update hostname asa
! Set the client to update the A RR, and the server to update the PTR RR:
dhcp client update dns
```

Example: No DHCP Server Update of RRs

The following example configures the ASA to update both the A and PTR RR, while requesting the DHCP server to update no RRs.

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
```

```

! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update ddns-2
  ddns update hostname asa1.example.com
! Set the client to update both RRs, and the server to update none:
dhcp client update dns server none

```

Example: DHCP Server Updates all RRs

The following example configures the DHCP client to request that the DHCP server to update both the A and PTR RRs. Because the server performs all updates, you do not need to associated an update method with the interface.

```

interface gigabitethernet1/1
  ip address dhcp
  ddns update hostname asa
! Configure the DHCP server to update both RRs:
dhcp client update dns server both

```

Monitoring DHCP and DDNS Services

This section includes the procedures to monitor both DHCP and DDNS services.

Monitoring DHCP Services

- **show dhcpd {binding [IP_address] | state | statistics}**
This command shows the current DHCP server client binding, state, and statistics.
- **show dhcprelay {state | statistics}**
This command displays the DHCP relay status and statistics.
- **show ipv6 dhcprelay binding**
This command shows the relay binding entries that were created by the relay agent.
- **show ipv6 dhcprelay statistics**
This command shows DHCP relay agent statistics for IPv6.

Monitoring DDNS Status

See the following command for monitoring DDNS status.

- **show ddns update {interface if_name | method [name]}**
This command shows the DDNS update status.

The following example show details about the DDNS update method:

```
ciscoasa# show ddns update method ddns1
```

```
Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

The following example shows information about the DDNS interface:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
  test                    not available
```

History for DHCP and DDNS Services

Feature Name	Platform Releases	Description
DHCPv6 monitoring	9.4(1)	You can now monitor DHCP statistics for IPv6 and DHCP bindings for IPv6.
DHCP Relay server validates the DHCP Server identifier for replies	9.2(4)/ 9.3(3)	If the ASA DHCP relay server receives a reply from an incorrect DHCP server, it now verifies that the reply is from the correct server before acting on the reply. We did not introduce or modify any commands. We did not modify any ASDM screens. We did not introduce or modify any commands.
DHCP rebind function	9.1(4)	During the DHCP rebind phase, the client now tries to rebind to other DHCP servers in the tunnel group list. Before this release, the client did not rebind to an alternate server when the DHCP lease fails to renew. We did not introduce or modify any commands.
DHCP trusted interfaces	9.1(2)	You can now configure interfaces as trusted interfaces to preserve DHCP Option 82. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the ASA DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then the ASA will drop that packet by default. You can now preserve Option 82 and forward the packet by identifying an interface as a trusted interface. We introduced or modified the following commands: dhcprelay information trusted , dhcprelay information trust-all , show running-config dhcprelay .
DHCP relay servers per interface (IPv4 only)	9.1(2)	You can now configure DHCP relay servers per-interface, so requests that enter a given interface are relayed only to servers specified for that interface. IPv6 is not supported for per-interface DHCP relay. We introduced or modified the following commands: dhcprelay server (interface config mode), clear configure dhcprelay , show running-config dhcprelay .

Feature Name	Platform Releases	Description
DHCP relay for IPv6 (DHCPv6)	9.0(1)	<p>DHCP relay support for IPv6 was added.</p> <p>We introduced the following commands: ipv6 dhcprelay server, ipv6 dhcprelay enable, ipv6 dhcprelay timeout, clear config ipv6 dhcprelay, ipv6 nd managed-config-flag, ipv6 nd other-config-flag, debug ipv6 dhcp, debug ipv6 dhcprelay, show ipv6 dhcprelay binding, clear ipv6 dhcprelay binding, show ipv6 dhcprelay statistics, and clear ipv6 dhcprelay statistics.</p>
DDNS	7.0(1)	<p>We introduced this feature.</p> <p>We introduced the following commands: ddns, ddns update, dhcp client update dns, dhcpd update dns, show running-config ddns, and show running-config dns server-group.</p>
DHCP	7.0(1)	<p>The ASA can provide a DHCP server or DHCP relay services to DHCP clients attached to ASA interfaces.</p> <p>We introduced the following commands: dhcp client update dns, dhcpd address, dhcpd domain, dhcpd enable, dhcpd lease, dhcpd option, dhcpd ping timeout, dhcpd update dns, dhcpd wins, dhcp-network-scope, dhcprelay enable, dhcprelay server, dhcprelay setroute, dhcp-server, show running-config dhcpd, and show running-config dhcprelay.</p>