DHCP Services

This chapter describes how to configure the DHCP server or DHCP relay and includes the following sections:

- Information About DHCP Services, page 17-1
- Licensing Requirements for DHCP, page 17-2
- Guidelines and Limitations, page 17-2
- Configuring DHCP Services, page 17-4
- Additional References, page 17-11
- Monitoring DHCP Services, page 17-11
- Feature History for DHCP Services, page 17-12

Information About DHCP Services

- Information About the DHCP Server, page 17-1
- Information About the DHCP Relay Agent, page 17-2

Information About the DHCP 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.

A client locates a DHCP server to request the assignment of configuration information using a reserved, link-scoped multicast address, which indicates that the client and server should be attached to the same link. However, in some cases where ease of management, economy, or scalability is the concern, we

recommend that you allow a DHCP client to send a message to a server that is not connected to the same link. The DHCP relay agent, which may reside on the client network, can relay messages between the client and server. The relay agent operation is transparent to the client.

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.

DHCP for IPv6 (DHCPv6) specified in RFC 3315 enables IPv6 DHCP servers to send configuration parameters such as network addresses or prefixes and DNS server addresses to IPv6 nodes (that is, DHCP clients). DHCPv6 uses the following multicast addresses:

- All_DHCP_Relay_Agents_and_Servers (FF02::1:2) is a link-scoped multicast address used by a client to communicate with neighboring (that is, on-link) relay agents and servers. All DHCPv6 servers and relay agents are members of this multicast group.
- The DHCPv6 relay service and server listen for messages on UDP port 547. The ASA DHCPv6 relay agent listens on both UDP port 547 and the All_DHCP_Relay_Agents_and_Servers multicast address.

Information 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.

You can remedy this situation by configuring the interface of your ASA that is receiving the broadcasts to forward DHCP requests to a DHCP server on another interface.

Licensing Requirements for DHCP

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

For all ASA models, the maximum number of DHCP client addresses varies depending on the license:

- If the limit is 10 hosts, the maximum available DHCP pool is 32 addresses.
- If the limit is 50 hosts, the maximum available DHCP pool is 128 addresses.
- If the number of hosts is unlimited, the maximum available DHCP pool is 256 addresses.

Guidelines and Limitations

Firewall Mode Guidelines

Supported in routed firewall mode.

DHCP server is supported in transparent firewall mode.

DHCP relay is NOT supported in transparent firewall mode.

Context Mode Guidelines

Supported in single and multiple context mode.

Failover Guidelines

Supports Active/Active and Active/Standby failover.

IPv6 Guidelines

Supports IPv6, except for interface-specific DHCP relay servers.

DHCP Server Guidelines

- The maximum available DHCP pool is 256 addresses.
- You can configure only one DHCP server on each interface of the ASA. 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 a DHCP client or DHCP relay service on an interface on which the server is enabled. Additionally, DHCP clients must be directly connected to the interface on which the server is enabled.
- The ASA does not support QIP DHCP servers for use with the DHCP proxy service.
- The relay agent cannot be enabled if the DHCP server is also enabled.
- The ASA DHCP server does not support BOOTP requests. In multiple context mode, you cannot enable the DHCP server or DHCP relay service on an interface that is used by more than one context.
- When it receives a DHCP request, the ASA sends a discovery message to the DHCP server. This message includes the IP address (within a subnetwork) that was configured with the **dhcp-network-scope** command in the group policy. If the server has an address pool that falls within that subnetwork, the server sends the offer message with the pool information to the IP address—not to the source IP address of the discovery message.
- When a client connects, the ASA sends a discovery message to all the servers in the server list. This message includes the IP address (within a subnetwork) that was configured with the **dhcp-network-scope** command in the group policy. The ASA selects the first offer received and drops the other offers. If the server has an address pool that falls within that subnetwork, the server sends the offer message with the pool information to the IP address—not to the source IP address of the discovery message. When the address needs to be renewed, it attempts to renew it with the lease server (the server from which the address was acquired). If the DHCP renew fails after a specified number of retries (four attempts), the ASA moves to the DHCP rebind phase after a predefined time period. During the rebind phase, the ASA simultaneously sends requests to all servers in the group. In a high availability environment, lease information is shared, so the other servers can acknowledge the lease and ASA will return to the bound state. During the rebind phase, if there is no response from any of the servers in the server list (after three retries), then the ASA will purge the entries.

  For example, if the server has a pool in the range of 209.165.200.225 to 209.165.200.254, mask 255.255.255.0, and the IP address specified by the **dhcp-network-scope** command is 209.165.200.1, the server sends that pool in the offer message to the ASA.

  The **dhcp-network-scope** command setting applies only to VPN users.

DHCP Relay Guidelines

- 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.
- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- When the DHCP relay service is enabled and more than one DHCP relay server is defined, the ASA forwards client requests to each defined DHCP relay server. Replies from the servers are also forwarded to the client until the client DHCP relay binding is removed. The binding is removed when the ASA receives any of the following DHCP messages: ACK, NACK, ICMP unreachable, or decline.
- You cannot enable DHCP relay service on an interface running as a DHCP proxy service. You must remove the VPN DHCP configuration first or an error message appears. This error occurs if both DHCP relay and DHCP proxy services are enabled. Make sure that either the DHCP relay or DHCP proxy service is enabled, but not both.
- DHCP relay services are not available in transparent firewall mode. You can, however, allow DHCP traffic through using an access list. To allow DHCP requests and replies through the ASA in transparent mode, you need to configure two access lists, one that allows DCHP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.
- 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.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context.
- The DHCP clients must be on different interfaces from the DHCP servers to which the ASA relays requests.

Configuring DHCP Services

- Configuring the DHCP Server, page 17-4
- Configuring the DHCP Relay Agent, page 17-8

Configuring the DHCP Server

This section describes how to configure a DHCP server provided by the ASA and includes the following topics:

- Enabling the DHCP Server, page 17-5
- Configuring DHCP Options, page 17-6

Enabling the DHCP Server

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

Detailed Steps

	Command	Purpose
Step 1	**dhcpd address** *ip_address if_name* **Example:** `ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside`	Creates a DHCP address pool. 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. The address pool must be on the same subnet as the ASA interface.
Step 2	**dhcpd dns** *dns1* [*dns2*] **Example:** `ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129`	(Optional) Specifies the IP address(es) of the DNS server(s).
Step 3	**dhcpd wins** *wins1* [*wins2*] **Example:** `ciscoasa(config)# dhcpd wins 209.165.201.5`	(Optional) Specifies the IP address(es) of the WINS server(s). You can specify up to two WINS servers.
Step 4	**dhcpd lease** *lease_length* **Example:** `ciscoasa(config)# dhcpd lease 3000`	(Optional) Changes 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.
Step 5	**dhcpd domain** *domain_name* **Example:** `ciscoasa(config)# dhcpd domain example.com`	(Optional) Configures the domain name.
Step 6	**dhcpd ping_timeout** *milliseconds* **Example:** `ciscoasa(config)# dhcpd ping timeout 20`	(Optional) Configures 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.
Step 7	**dhcpd option 3 ip** *gateway_ip* **Example:** `ciscoasa(config)# dhcpd option 3 ip 10.10.1.1`	Defines a default gateway that is sent to DHCP clients. If you do not use the **dhcpd option 3** command to define the default gateway, DHCP clients use the ASA interface IP address that is closest to the DHCP clients by default; the ASA does not use the management interface IP address. As a result, the DHCP ACK does not include this option.
Step 8	**dhcpd enable** *interface_name* **Example:** `ciscoasa(config)# dhcpd enable outside`	Enables the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface.

–

Configuring DHCP Options

The ASA supports the DHCP options listed in RFC 2132 to send information. This section includes the following topics:

- Options that Return an IP Address, page 17-6
- Options that Return a Text String, page 17-6
- Options that Return a Hexadecimal Value, page 17-6

Options that Return an IP Address

Command	Purpose
dhcpd option *code* **ip** *addr_1* [*addr_2*] **Example:** `ciscoasa(config)# dhcpd option 2 ip 10.10.1.1 10.10.1.2`	Configures a DHCP option that returns one or two IP addresses.

Options that Return a Text String

Command	Purpose
dhcpd option *code* **ascii** *text* **Example:** `ciscoasa(config)# dhcpd option 2 ascii examplestring`	Configures a DHCP option that returns a text string.

Options that Return a Hexadecimal Value

Command	Purpose
dhcpd option *code* **hex** *value* **Example:** `ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11`	Configures a DHCP option that returns a hexadecimal value.

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.

Table 17-1 shows the DHCP options that are not supported by the **dhcpd option** command.

Table 17-1 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

DHCP options 3, 66, and 150 are used to configure Cisco IP phones. For more information about configuring these options, see Using Cisco IP Phones with a DHCP Server, page 17-7.

Using Cisco IP Phones with a DHCP Server

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.

Note Cisco IP phones can also include DHCP option 3 in their requests, which 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.

To send information to use for any option number, enter the following command:

Command	Purpose
dhcpd option *number value* **Example:** `ciscoasa(config)# dhcpd option 2`	Provides information for DHCP requests that include an option number as specified in RFC 2132.

To send information to use for option 66, enter the following command:

Command	Purpose
dhcpd option 66 ascii *server_name* **Example:** `ciscoasa(config)# dhcpd option 66 ascii exampleserver`	Provides the IP address or name of a TFTP server for option 66.

To send information to use for option 150, enter the following command:

Command	Purpose
dhcpd option 150 ip *server_ip1* [*server_ip2*] **Example:** `ciscoasa(config)# dhcpd option 150 ip 10.10.1.1`	Provides the IP address or names of one or two TFTP servers for option 150. The *server_ip1* is the IP address or name of the primary TFTP server while *server_ip2* is the IP address or name of the secondary TFTP server. A maximum of two TFTP servers can be identified using option 150.

To send information to use for option 3, enter the following command:

Command	Purpose
dhcpd option 3 ip *router_ip1* **Example:** `ciscoasa(config)# dhcpd option 3 ip 10.10.1.1`	Sets the default route.

Configuring the DHCP Relay Agent

- Configuring the DHCPv4 Relay Agent, page 17-8
- Configuring the DHCPv6 Relay Agent, page 17-10

Configuring the DHCPv4 Relay Agent

When a DHCP request enters an interface, the DHCP servers to which the ASA relays the request depends on your configuration. You can 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.

Detailed Steps

	Command	Purpose
Step 1	Do one or both of the following:	

	For a global server:
	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`
		Specifies a global DHCP server IP address and the interface through which it is reachable.

	For an interface-specific server:
	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`
		Specifies 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. 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	**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`
		Enables the DHCP relay service on the interface connected to the DHCP clients. You can enable DHCP relay on multiple interfaces.

Step 3	**dhcprelay timeout** *seconds* **Example:** `ciscoasa(config)# dhcprelay timeout 25`	(Optional) Sets the number of seconds allowed for DHCP relay address handling.
Step 4	**dhcprelay setroute** *interface_name* **Example:** `ciscoasa(config)# dhcprelay setroute inside`	(Optional) Changes the first default router address in the packet sent from the DHCP server to the address of the ASA interface. 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) Do one of the following:	

Command	Purpose

interface *interface_id*
dhcprelay information trusted
 	
Example:
`ciscoasa(config)# interface gigabitethernet 0/0`
`ciscoasa(config-if)# dhcprelay information trusted`
	Specifies a DHCP client interface that you want to trust. 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.

dhcprelay information trust-all **Example:** `ciscoasa(config)# dhcprelay information trust-all`	Configures all client interfaces as trusted.

Configuring the DHCPv6 Relay Agent

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

Detailed Steps

	Command	Purpose
Step 1	**ipv6 dhcprelay server** *ipv6_address* [*interface*] **Example:** `ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701`	Specifies the IPv6 DHCP server destination address to which client messages are forwarded. 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	**ipv6 dhcprelay enable** *interface* **Example:** `ciscoasa(config)# ipv6 dhcprelay enable inside`	Enables DHCPv6 relay service on a client interface.
Step 3	**ipv6 dhcprelay timeout** *seconds* **Example:** `ciscoasa(config)# ipv6 dhcprelay timeout 25`	(Optional) Specifies 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. Valid values for the *seconds* argument range from 1 to 3600. The default is 60 seconds.

Additional References

For additional information related to implementing DHCPv6, see the following section:

- RFCs, page 17-11

RFCs

RFC	Title
2132	DHCP Options and BOOTP Vendor Extensions
2462	IPv6 Stateless Address Autoconfiguration
5510	DHCP for IPv6

Monitoring DHCP Services

To monitor DHCP, enter one or more of the following commands:

Command	Purpose
show running-config dhcpd	Shows the current DHCP configuration.
show running-config dhcprelay	Shows the current DHCP relay service status.
show ipv6 dhcprelay binding	Shows the relay binding entries that were created by the relay agent.
show ipv6 dhcprelay statistics	Shows DHCP relay agent statistics for IPv6.
clear config ipv6 dhcprelay	Clears the IPv6 DHCP relay configuration.

Feature History for DHCP Services

Table 17-2 each feature change and the platform release in which it was implemented.

Table 17-2 Feature History for DHCP Services

Feature Name	Releases	Description
DHCP	7.0(1)	The ASA can provide a DHCP server or DHCP relay services to DHCP clients attached to ASA interfaces. 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**.
DHCP for IPv6 (DHCPv6)	9.0(1)	Support for IPv6 was added. 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**.
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**.
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 rebind function	9.1(4)	During the DHCP rebind phase, the client now attempts to rebind to other DHCP servers in the tunnel group list. Prior to this release, the client did not rebind to an alternate server, when the DHCP lease fails to renew. There is no change to the CLI.