CHAPTER 7

Configuring DHCP and Dynamic DNS Services

This chapter describes how to configure the DHCP server and dynamic DNS (DDNS) update methods.

This chapter includes the following topics:

Configuring DHCP Services

This section includes the following topics:

Information about DHCP

DHCP provides network configuration parameters, such as IP addresses, to DHCP clients. The ASA can provide a DHCP server or DHCP relay services to DHCP clients attached to ASA interfaces. The DHCP server provides network configuration parameters directly to DHCP clients. DHCP relay passes DHCP requests received on one interface to an external DHCP server located behind a different interface.

Licensing Requirements for DHCP

Table 7-1 lists the license requirements for DHCP.

Table 7-1 License Requirements

Model	License Requirement
All models	Base License.

For the Cisco ASA 5505 Adaptive Security Appliance, the maximum number of DHCP client addresses varies depending on the license:

- If the Host limit is 10 hosts, we limit the DHCP pool to 32 addresses.
- If the Host limit is 50 hosts, we limit the DHCP pool to 128 addresses.
- If the Host limit is unlimited, we limit the DHCP pool to 256 addresses.

Note By default the Cisco ASA 5505 Adaptive Security Appliance comes with a 10-user license.

Guidelines and Limitations

Use the following guidelines to configure the DHCP server:

- You can configure a DHCP server on each interface of the ASA. Each interface can have its own pool of addresses to draw from. 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 services 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 relay agent cannot be enabled if the DHCP server is also enabled.
- The ASA does not support QIP DHCP servers for use with DHCP Proxy.
- When it receives a DHCP request, the security appliance sends a *discovery* message to the DHCP server. This message includes the IP address (within a subnetwork) configured with the **dhcp-network-scope** command in the group policy. If the server has an address pool that falls within that subnetwork, it sends the *offer* message with the pool information to the IP address—not to the source IP address of the discovery message.
- For example, if the server has a pool of the range 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 security appliance.
- You can add up to four DHCP relay servers per interface; however, there is a limit of ten DHCP relay servers total that can be configured on the ASA. You must add at least one **dhcprelay server** command to the ASA configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured

Configuring a DHCP Server

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

Enabling the DHCP Server

The ASA can act as a DHCP server. DHCP is a protocol that supplies network settings to hosts including the host IP address, the default gateway, and a DNS server.

Note The ASA DHCP server does not support BOOTP requests. In multiple context mode, you cannot enable the DHCP server or DHCP relay on an interface that is used by more than one context.

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

Enter the following command to define the address pool:

	Command	Purpose
Step 1	**dhcpd address** *ip_address-ip_address interface_name* **Example:** `hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside`	Create a DHCP address pool. The ASA assigns a client one of the addresses from this pool to use for a given length 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:** `hostname(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:** `hostname(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:** `hostname(config)# dhcpd lease 3000`	(Optional) Change the lease length to be granted to the client. This lease equals the amount of time (in seconds) the client can use its allocated IP address before the lease expires. Enter a value between 0 to 1,048,575. The default value is 3600 seconds.
Step 5	**dhcpd domain** *domain_name* **Example:** `hostname(config)# dhcpd domain example.com`	(Optional) Configures the domain name.
Step 6	**dhcpd ping_timeout** *milliseconds*	(Optional) Configures the DHCP ping timeout value. To avoid address conflicts, the ASA sends two ICMP ping packets to an address before assigning that address to a DHCP client. This command specifies the timeout value for those packets.
Step 7	**dhcpd option 3 ip** *gateway_ip*	(Transparent Firewall Mode) Defines a default gateway that is sent to DHCP clients. If you do not use the DHCP option 3 to define the default gateway, DHCP clients use the IP address of the management interface. The management interface does not route traffic.
Step 8	**dhcpd enable** *interface_name*	Enables the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface

Configuring DHCP Options

You can configure the ASA to send information for the DHCP options listed in RFC 2132. The DHCP options fall into one of three categories:

The ASA supports all three categories of DHCP options. To configure a DHCP option, do one of the following:

Options that return an IP address

Command	Purpose
dhcpd option *code* **ip** *addr_1* [*addr_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*	Configures a DHCP option that returns a text string.

Options that return a hexadecimal value

Command	Purpose
dhcpd option *code* **hex** *value*	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 as expecting a single-digit, hexadecimal value. For more information about the option codes and their associated types and expected values, refer to RFC 2132.

Table 7-2 shows the DHCP options that are not supported by the **dhcpd option** command.

Table 7-2 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

Table 7-2 Unsupported DHCP Options

Option Code	Description
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

Specific options, DHCP option 3, 66, and 150, are used to configure Cisco IP Phones. See the "Using Cisco IP Phones with a DHCP Server" section on page 7-5 topic for more information about configuring those options.

Using Cisco IP Phones with a DHCP Server

Enterprises with small branch offices that implement a Cisco IP Telephony Voice over IP solution typically implement Cisco CallManager at a central office to control Cisco IP Phones at small branch offices. This implementation allows centralized call processing, reduces the equipment required, and eliminates the administration of additional Cisco CallManager and other servers at branch offices.

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.

Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route.

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

You can configure the ASA to send information for most options listed in RFC 2132. The following example shows the syntax for any option number, as well as the syntax for commonly-used options 66, 150, and 3:

Command	Purpose
dhcpd option *number value*	Provides information for DHCP requests that include an option number as specified in RFC-2132

Command	Purpose
dhcpd option 66 ascii *server_name*	Provides the IP address or name of a TFTP server for option 66

Command	Purpose
dhcpd option 150 ip *server_ip1* [*server_ip2*]	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.

Command	Purpose
dhcpd option 3 ip *router_ip1*	Sets the default route

Configuring DHCP Relay Services

A DHCP relay agent allows the ASA to forward DHCP requests from clients to a router connected to a different interface.

The following restrictions apply to the use of the DHCP relay agent:

- The relay agent cannot be enabled if the DHCP server feature is also enabled.
- DHCP clients must be directly connected to the ASA and cannot send requests through another relay agent or a router.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context.
- DHCP Relay services are not available in transparent firewall mode. A ASA in transparent firewall mode only allows ARP traffic through; all other traffic requires 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.
- When DHCP relay is enabled and more than one DHCP relay server is defined, the security appliance 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 security appliance receives any of the following DHCP messages: ACK, NACK, or decline.

Note You cannot enable DHCP Relay on an interface running DHCP Proxy. You must Remove VPN DHCP configuration first or you will see an error message. This error happens if both DHCP relay and DHCP proxy are enabled. Ensure that either DHCP relay or DHCP proxy are enabled, but not both.

To enable DHCP relay, perform the following steps:

	Command	Purpose
Step 1	**dhcprelay server** *ip_address if_name* **Example:** `hostname(config)# dhcprelay server 201.168.200.4`	Set the IP address of a DHCP server on a different interface from the DHCP client. You can use this command up to 4 times to identify up to 4 servers.
Step 2	**dhcprelay enable** *interface* **Example:** `hostname(config)# dhcprelay enable inside`	Enables DHCP relay on the interface connected to the clients.
Step 3	**dhcprelay timeout** *seconds*	(Optional) Set the number of seconds allowed for relay address negotiation.
Step 4	**dhcprelay setroute** *interface_name* **Example:** `hostname(config)# dhcprelay setroute inside`	(Optional) Change 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.

Feature History for DHCP

Table 7-3 lists the release history for this feature.

Table 7-3 Feature History for DHCP

Feature Name	Releases	Feature Information
DHCP	7.0(1)	This feature was introduced.

Configuring DDNS Services

This section includes the following topics:

Information about DDNS

DDNS update integrates DNS with DHCP. The two protocols are complementary: DHCP centralizes and automates IP address allocation; DDNS update automatically records the association between assigned addresses and hostnames at pre-defined intervals. DDNS allows frequently changing address-hostname

associations to be updated frequently. Mobile hosts, for example, can then move freely on a network without user or administrator intervention. DDNS provides the necessary dynamic updating and synchronizing of the name to address and address to name mappings on the DNS server.

Licensing Requirements For DDNS

Table 7-4 lists the license requirements for DDNS.

Table 7-4 License Requirements

Model	License Requirement
All models	Base License.

Configuring DDNS

This section describes examples for configuring the ASA to support Dynamic DNS. DDNS update integrates DNS with DHCP. The two protocols are complementary—DHCP centralizes and automates IP address allocation, while dynamic DNS update automatically records the association between assigned addresses and hostnames. When you use DHCP and dynamic DNS update, this configures a host automatically for network access whenever it attaches to the IP network. You can locate and reach the host using its permanent, unique DNS hostname. Mobile hosts, for example, can move freely without user or administrator intervention.

DDNS provides address and domain name mappings so hosts can find each other even though their DHCP-assigned IP addresses change frequently. The DDNS name and address mappings are held on the DHCP server in two resource records: the A RR contains the name to IP address mapping while the PTR RR maps addresses to names. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

The two most common DDNS update configurations are:

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

In general, the DHCP server maintains DNS PTR RRs on behalf of clients. Clients may be configured to perform all desired DNS updates. The server may be configured to honor these updates or not. To update the PTR RR, the DHCP server must know the Fully Qualified Domain Name of the client. The client provides an FQDN to the server using a DHCP option called Client FQDN.

Configuration Examples for DDNS

The following examples present these common scenarios:

- Example 1: Client Updates Both A and PTR RRs for Static IP Addresses, page 7-9
- Example 2: Client Updates Both A and PTR RRs; DHCP Server Honors Client Update Request; FQDN Provided Through Configuration, page 7-9
- Example 3: Client Includes FQDN Option Instructing Server Not to Update Either RR; Server Overrides Client and Updates Both RRs., page 7-10
- Example 4: Client Asks Server To Perform Both Updates; Server Configured to Update PTR RR Only; Honors Client Request and Updates Both A and PTR RR, page 7-10

Example 1: Client Updates Both A and PTR RRs for Static IP Addresses

The following example configures the client to request that it update both A and PTR resource records for static IP addresses. To configure this example, perform the following steps:

Step 1 To define a DDNS update method called ddns-2 that requests that the client update both the A and PTR RRs, enter the following commands:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

Step 2 To associate the method ddns-2 with the eth1 interface, enter the following commands:

```
hostname(DDNS-update-method)# interface eth1
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname asa.example.com
```

Step 3 To configure a static IP address for eth1, enter the following commands:

```
hostname(config-if)# ip address 10.0.0.40 255.255.255.0
```

Example 2: Client Updates Both A and PTR RRs; DHCP Server Honors Client Update Request; FQDN Provided Through Configuration

The following example configures 1) the DHCP client to request that it update both the A and PTR RRs, and 2) the DHCP server to honor the requests. To configure this example, perform the following steps:

Step 1 To configure the DHCP client to request that the DHCP server perform no updates, enter the following command:

```
hostname(config)# dhcp-client update dns server none
```

Step 2 To create a DDNS update method named ddns-2 on the DHCP client that requests that the client perform both A and PTR updates, enter the following commands:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

Step 3 To associate the method named ddns-2 with the ASA interface named Ethernet0, and enable DHCP on the interface, enter the following commands:

```
hostname(DDNS-update-method)# interface Ethernet0
hostname(if-config)# ddns update ddns-2
hostname(if-config)# ddns update hostname asa.example.com
hostname(if-config)# ip address dhcp
```

Step 4 To configure the DHCP server, enter the following command:

```
hostname(if-config)# dhcpd update dns
```

Example 3: Client Includes FQDN Option Instructing Server Not to Update Either RR; Server Overrides Client and Updates Both RRs.

The following example configures the DHCP client to include the FQDN option instructing the DHCP server not to update either the A or PTR updates. The example also configures the server to override the client request. As a result, the client backs off without performing any updates.

To configure this scenario, perform the following steps:

Step 1 To configure the update method named ddns-2 to request that it make both A and PTR RR updates, enter the following commands:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

Step 2 To assign the DDNS update method named ddns-2 on interface Ethernet0 and provide the client hostname (asa), enter the following commands:

```
hostname(DDNS-update-method)# interface Ethernet0
hostname(if-config)# ddns update ddns-2
hostname(if-config)# ddns update hostname asa.example.com
```

Step 3 To enable the DHCP client feature on the interface, enter the following commands:

```
hostname(if-config)# dhcp client update dns server none
hostname(if-config)# ip address dhcp
```

Step 4 To configure the DHCP server to override the client update requests, enter the following command:

```
hostname(if-config)# dhcpd update dns both override
```

Example 4: Client Asks Server To Perform Both Updates; Server Configured to Update PTR RR Only; Honors Client Request and Updates Both A and PTR RR

The following example configures the server to perform only PTR RR updates by default. However, the server honors the client request that it perform both A and PTR updates. The server also forms the FQDN by appending the domain name (example.com) to the hostname provided by the client (asa).

To configure this scenario, perform the following steps:

Step 1 To configure the DHCP client on interface Ethernet0, enter the following commands:

```
hostname(config)# interface Ethernet0
hostname(config-if)# dhcp client update dns both
hostname(config-if)# ddns update hostname asa
```

Step 2 To configure the DHCP server, enter the following commands:

```
hostname(config-if)# dhcpd update dns
hostname(config-if)# dhcpd domain example.com
```

Example 5: Client Updates A RR; Server Updates PTR RR

The following example configures the client to update the A resource record and the server to update the PTR records. Also, the client uses the domain name from the DHCP server to form the FQDN.

To configure this scenario, perform the following steps:

Step 1 To define the DDNS update method named ddns-2, enter the following commands:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns
```

Step 2 To configure the DHCP client for interface Ethernet0 and assign the update method to the interface, enter the following commands:

```
hostname(DDNS-update-method)# interface Ethernet0
hostname(config-if)# dhcp client update dns
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname asa
```

Step 3 To configure the DHCP server, enter the following commands:

```
hostname(config-if)# dhcpd update dns
hostname(config-if)# dhcpd domain example.com
```

Feature History for DDNS

Table 7-5 lists the release history for this feature.

Table 7-5 Feature History for DDNS

Feature Name	Releases	Feature Information
DHCP	7.0(1)	This feature was introduced.
DDNS	7.0(1)	This feature was introduced.