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

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 DCHP 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 5.

Enable the DHCPv4 Server

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

Procedure

Step 1 Choose **Configuration** > **Device Management** > **DHCP** > **DHCP Server**.

Step 2 Choose an interface, then click **Edit**.

In transparent mode, choose a bridge group member interface.

a) Check the **Enable DHCP Server** check box to enable the DHCP server on the selected interface.

b) Enter the range of IP addresses from lowest to highest that is used by the DHCP server in the **DHCP Address Pool** field. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.

c) Set the following in the **Optional Parameters** area:

- The DNS servers (1 and 2) configured for the interface.
- The WINS servers (primary and secondary) configured for the interface.
- The domain name of the interface.
- The time in milliseconds that the ASA will wait for an ICMP ping response on the interface.
- The duration of time that the DHCP server configured on the interface allows DHCP clients to use an assigned IP address.
- The interface on a DHCP client that provides DNS, WINS, and domain name information for automatic configuration if the ASA is acting as a DHCP client on a specified interface (usually outside).
- Click **Advanced** to display the **Advanced DHCP Options** dialog box to configure more DHCP options. See Configure Advanced DHCPv4 Options, on page 5 for more information.

d) Check the **Update DNS Clients** check box in the **Dynamic Settings for DHCP Server** area to specify that in addition to the default action of updating the client PTR resource records, the selected DHCP server should also perform the following update actions:

- Check the **Update Both Records** check box to specify that the DHCP server should update both the A and PTR RRs.
- Check the **Override Client Settings** check box to specify that DHCP server actions should override any update actions requested by the DHCP client.

e) Click **OK** to close the **Edit DHCP Server** dialog box.

Step 3 (Optional) (Routed mode) Check the **Enable Auto-configuration from interface** check box in the **Global DHCP Options** area below the DHCP Server table to enable DHCP auto configuration only if the ASA is acting as a DHCP client on a specified interface (usually outside).

DHCP auto configuration enables the DHCP Server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that is running on the specified interface. If information obtained through auto configuration is also specified manually in the **Global DHCP Options** area, the manually specified information takes precedence over the discovered information.

Step 4 Choose the auto-configuration interface from the drop-down list.

Step 5 Check the **Allow VPN override** check box to override the interface DHCP or PPPoE client WINS parameter with the VPN client parameter.

Step 6 Enter the IP address of the primary DNS server for a DHCP client in the **DNS Server 1** field.

Step 7 Enter the IP address of the alternate DNS server for a DHCP client in the **DNS Server 2** field.

Step 8 Enter the DNS domain name for DHCP clients (for example, example.com) in the **Domain Name** field.

Step 9 Enter the amount of time, in seconds, in the **Lease Length** field that the client may use its allocated IP address before the lease expires. Valid values range from 300 to 1048575 seconds. The default value is 3600 seconds (1 hour).

Step 10 Enter the IP address of the primary WINS server for a DHCP client in the **Primary WINS Server** field.

Step 11 Enter the IP address of the alternate WINS server for a DHCP client in the **Secondary WINS Server** field.

Step 12 To avoid address conflicts, the ASA sends two ICMP ping packets to an address before assigning that address to a DHCP client. enter the amount of time, in milliseconds, in the **Ping Timeout** field that the ASA waits to time out a DHCP ping attempt. Valid values range from 10 to 10000 milliseconds. The default value is 50 milliseconds.

Step 13 Click **Advanced** to display the **Configuring Advanced DHCP Options** dialog box to specify additional DHCP options and their parameters. For more information, see Configure Advanced DHCPv4 Options, on page 5.

Step 14 You configure the DDNS update settings for the DHCP server in the **Dynamic DNS Settings for DHCP Server** area. Check the **Update DNS Clients** check box to specify that, in addition to the default action of updating the client PTR resource records, the selected DHCP server should also perform the following update actions:

- Check the **Update Both Records** check box to specify that the DHCP server should update both the A and PTR RRs.
- Check the **Override Client Settings** check box to specify that the DHCP server actions should override any update actions requested by the DHCP client.

Step 15 Click **Apply** to save your changes.

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 Choose **Configuration** > **Device Management** > **DHCP** > **DHCP Server**, then click **Advanced**.

Step 2 Choose the option code from the drop-down list.

Step 3 Choose the options that you want to configure. Some options are standard. For standard options, the option name is shown in parentheses after the option number and the option parameters are limited to those supported by the option. For all other options, only the option number is shown and you must choose the appropriate parameters to supply with the option. For example, if you choose DHCP Option 2 (Time Offset), you can only enter a hexadecimal value for the option. For all other DHCP options, all of the option value types are available and you must choose the appropriate one.

Step 4 Specify the type of information that the option returns to the DHCP client in the **Option Data** area. For standard DHCP options, only the supported option value type is available. For all other DHCP options, all of the option value types are available. Click **Add** to add the option to the DHCP option list. Click **Delete** to remove the option from the DHCP option list.

- Click **IP Address** to indicate that an IP address is returned to the DHCP client. You can specify up to two IP addresses. IP Address 1 and IP Address 2 indicate an IP address in dotted-decimal notation.

  Note The name of the associated IP address fields can change based on the DHCP option that you chose. For example, if you choose DHCP Option 3 (Router), the fields names change to Router 1 and Router 2.

- Click **ASCII** to specify that an ASCII value is returned to the DHCP client. Enter an ASCII character string in the **Data** field. The string cannot include spaces.

  Note The name of the associated Data field can change based on the DHCP option that you chose. For example, if you choose DHCP Option 14 (Merit Dump File), the associated Data field names change to File Name.

- Click **Hex** to specify that a hexadecimal value is returned to the DHCP client. Enter a hexadecimal string with an even number of digits and no spaces in the **Data** field. You do not need to use a 0x prefix.

  Note The name of the associated Data field can change based on the DHCP option you chose. For example, if you choose DHCP Option 2 (Time Offset), the associated Data field becomes the Offset field.

Step 5 Click **OK** to close the **Advanced DHCP Options** dialog box.

Step 6 Click **Apply** to save your changes.

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.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **DHCP** > **DHCP Relay**.

Step 2 Check the check boxes for the services you want for each interface in the **DHCP Relay Agent** area.

- **IPv4 > DHCP Relay Enabled**.
- **IPv4 > Set Route**— Changes the default gateway address in the DHCP message from the server to that of the ASA interface that is closest to the DHCP client, which relayed the original DHCP request. 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.
- **IPv6 > DHCP Relay Enabled**.
- **Trusted Interface**—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. You can alternatively trust all interfaces by checking the **Set dhcp relay information as trusted on all interfaces** check box.

Step 3 Add one or more DHCP servers to which DHCP requests are relayed in the **Global DHCP Relay Servers** area,

a) Click **Add**. The **Add Global DHCP Relay Server** dialog box appears.
b) Enter the IPv4 or IPv6 address of the DHCP server in the **DHCP Server** field.
c) Choose the interface to which the specified DHCP server is attached from the **Interface** drop-down list.
d) Click **OK**.

The newly added global DHCP relay server appears in the **Global DHCP Relay Servers** list.

Step 4 (Optional) In the **IPv4 Timeout** field, enter the amount of time, in seconds, allowed for DHCPv4 address handling. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.

Step 5 (Optional) In the **IPv6 Timeout** field, enter the amount of time, in seconds, allowed for DHCPv6 address handling. Valid values range from 1 to 3600 seconds. The default value is 60 seconds.

Step 6 In the **DHCP Relay Interface Servers** area, add one or more interface-specific DHCP servers to which DHCP requests on a given interface are relayed:

a) Click **Add**. The **Add DHCP Relay Server** dialog box appears.
b) From the **Interface** drop-down list, choose the interface connected to the DHCP clients. Note that you do not specify the egress interface for the requests, as for a Global DHCP Server; instead, the ASA uses the routing table to determine the egress interface.
c) In the **Server to** field, enter the IPv4 address of the DHCP server, and click **Add**. The server is added to the right-hand list. Add up to 4 servers, if available out of the overall maximum. IPv6 is not supported for interface-specific servers.
d) Click **OK**.

The newly added interface DHCP relay servers appear in the **DHCP Relay Interface Servers** list.

Step 7 To configure all interfaces as trusted interfaces, check the **Set dhcp relay information as trusted on all interfaces** check box. You can alternatively trust individual interfaces.

Step 8 Click **Apply** to save your settings.

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 Choose **Configuration** > **Device Management** > **DNS** > **Dynamic DNS**.

Step 2 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) In the **Update Methods** area, click **Add**.
b) Specify a **Name** for this method.
c) (Optional) Configure the **Update Interval** between DNS requests. 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**.
d) Under **Records to Update**, specify the standard DDNS records that you want the ASA to update.

This setting only affects the records you want to update directly from the ASA; to determine the records you want the DHCP server to update, configure the DHCP client settings per interface or globally. See Step Step 3, on page 9.

- **Both (PTR and A records)**—Sets the ASA to update both A and PTR RRs. Use this option for static or PPPoE IP addressing.
- **A records only**—Sets the ASA to update the A RR only. Use this option if you want the DHCP server to update the PTR RR.

e) Click **OK**.
f) Assign this method to the interface in Step Step 3, on page 9.

Step 3 Configure interface settings for DDNS, including setting the update method, DHCP client settings, and the hostname for this interface.

a) In the **Dynamic DNS Interface Settings** area, click **Add**.
b) Choose the **Interface** from the drop-down list.
c) Choose the **Method Name** that you created in the **Update Methods** area.

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

d) Set the **Hostname** for this interface.

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).

e) Configure the **DHCP Server Record Updates** to determine which records you want the DHCP server to update.

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 on the main **Dynamic DNS** page. The per-interface settings take precedence over the global settings.

- **Default (PTR Records)**—Requests that the DHCP server perform the PTR RR update. This setting works in conjunction with a DDNS update method with **A Records** enabled.
- **Both (PTR Records and A Records)**—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.
- **None**—Requests the DHCP server not to perform updates. This setting works in conjunction with a DDNS update method with **Both A and PTR Records** enabled.

f) Click **OK**.

Step 4 Click **Apply** to save your changes, or click **Reset** to discard them and enter new ones.

Monitoring DHCP and DDNS Services

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

Monitoring DHCP Services

- **Monitoring > Interfaces > DHCP > DHCP Client Lease Information**.

  This pane displays configured DHCP client IP addresses.

- **Monitoring > Interfaces > DHCP > DHCP Server Table**

  This pane displays configured dynamic DHCP client IP addresses.

- **Monitoring > Interfaces > DHCP > DHCP Statistics**

  This pane displays DHCPv4 message types, counters, values, directions, messages received, and messages sent.

- **Monitoring > Interfaces > DHCP > IPV6 DHCP Relay Statistics**

  This pane displays DHCPv6 Relay message types, counters, values, directions, messages received, and messages sent.

- **Monitoring > Interfaces > DHCP > IPV6 DHCP Relay Binding**

  This pane displays DHCPv6 Relay bindings.

Monitoring DDNS Status

See the following command for monitoring DDNS status. Enter the commands on **Tools > Command Line Interface**.

- **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. We introduced the following screens: DHCPv6 monitoring Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics, Monitoring > Interfaces > DHCP > IPV6 DHCP Binding.
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 modify any ASDM screens.
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 modify any ASDM screens.
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 modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.
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 modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.

Feature Name	Platform Releases	Description
DHCP relay for IPv6 (DHCPv6)	9.0(1)	DHCP relay support for IPv6 was added. We modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.
DDNS	7.0(1)	We introduced this feature. We introduced the following screens: Configuration > Device Management> DNS > DNS Client. Configuration > Device Management > DNS > Dynamic DNS.
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 screens: Configuration > Device Management > DHCP > DHCP Relay. Configuration > Device Management > DHCP > DHCP Server.