DHCP 和 DDNS 服务

本章介绍如何配置 DHCP 服务器和 DHCP 中继以及动态 DNS (DDNS) 更新方法。

- 关于 DHCP 和 DDNS 服务，第 1 页
- DHCP 和 DDNS 服务准则，第 3 页
- 配置 DHCP 服务器，第 5 页
- 配置 DHCP 中继代理，第 11 页
- 配置动态 DNS，第 14 页
- 监控 DHCP 和 DDNS 服务，第 19 页
- DHCP 和 DDNS 服务的历史记录，第 24 页

关于 DHCP 和 DDNS 服务

以下主题介绍 DHCP 服务器、DHCP 中继代理和 DDNS 更新。

关于 DHCPv4 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。ASA 可以为连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器。DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

DHCP 选项

DHCP 提供用于将配置信息传递至 TCP/IP 网络中主机的标准。配置参数在存储于 DHCP 消息的 Options 字段中的标记项目中携带，数据也称为选项。供应商信息也存储在 Options 中，并且所有供应商信息扩展均可用作 DHCP 选项。

例如，思科 IP 电话从 TFTP 服务器下载其配置。当思科 IP 电话启动时，如果其不让 IP 地址和 TFTP 服务器 IP 地址均得以预配置，则其将向 DHCP 服务器发送带有选项 150 或 66 的请求以获取此信息。

- DHCP 选项 150 提供 TFTP 服务器列表的 IP 地址。
- DHCP 选项 66 提供单一 TFTP 服务器的 IP 地址或主机名。

- DHCP 选项 3 设置默认路由。

单一请求可能同时包括选项 150 和 66。在此情况下，如在 ASA 上已配置这两个选项，则 ASA DHCP 服务器将在响应中为两个选项提供值。

您可以使用高级 DHCP 选项向 DHCP 客户端提供 DNS、WINS 和域名参数；DHCP 选项 15 用于 DNS 域名后缀。也可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器来发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

关于 DHCPv6 无状态服务器

对于结合前缀授权功能 (启用 IPv6 前缀授权客户端) 使用无状态地址自动配置 (SLAAC) 的客户端，可以来配置 ASA，以便在它们向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

关于 DHCP 中继代理

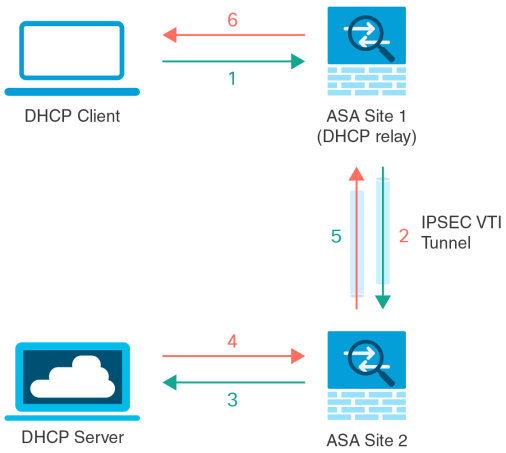
您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 ASA 进行转发，因为它不转发广播流量。DHCP 中继代理可用于配置用来接收广播的 ASA 的接口，以将 DHCP 请求转发至另一接口上的 DHCP 服务器。

VTI 上的 DHCP 中继服务器支持

您可以在 ASA 接口上配置 DHCP 中继代理，以在 DHCP 客户端和 DHCP 服务器之间接收和转发 DHCP 消息。但是，不支持通过逻辑接口转发消息的 DHCP 中继服务器。

下图显示了通过 VTI VPN 使用 DHCP 中继的 DHCP 客户端和 DHCP 服务器的发现过程。在 ASA 站点 1 的 VTI 接口上配置的 DHCP 中继代理从 DHCP 客户端接收 DHCPDISCOVER 数据包，并通过 VTI 隧道发送数据包。ASA 站点 2 将 DHCPDISCOVER 数据包转发到 DHCP 服务器。DHCP 服务器使用 DHCPOFFER 向 ASA 站点 2 进行回复。ASA 站点 2 将其转发到 DHCP 中继（ASA 站点 1），后者将其转发到 DHCP 客户端。

图 *1:* 通过 *VTI* 的 *DHCP* 中继服务器



DHCPREQUEST 和 DHCPACK/NACK 要求遵循相同的程序。

DHCP 和 DDNS 服务准则

本节介绍在配置 DHCP 和 DDNS 服务之前应检查的准则和限制。

情景模式

- 多情景模式下不支持 DHCPv6 无状态服务器。

防火墙模式

- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCP 中继。
- 在网桥组成员接口上的透明防火墙模式下，支持 DHCP 服务器。 在路由模式下，在 BVI 接口（而非网桥组成员接口）上支持 DHCP 服务器。BVI 必须具有名称，DHCP 服务器才能运行。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DDNS。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCPv6 无状态服务器。

集群

- 集群不支持 DHCPv6 无状态服务。

IPv6

支持 IPv6 用于 DHCP 无状态服务器和 DHCP 中继。

DHCPv4 服务器

- 最大可用 DHCP 池为 256 个地址。
- 您可以在具有名称和 IP 地址的任何接口（例如物理接口、子接口或路由模式下的 BVI）上配置 DHCP 服务器。
- 只能在每个接口上配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置（如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 如果某个接口也启用了 DHCP 服务器，则不能将该接口配置为 DHCP 客户端；您必须使用静态 IP 地址。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 您可以为接口保留 DHCP 地址。根据客户端的 MAC 地址，ASA 从地址池中将一个具体的 IP 地址分配给 DHCP 客户端。
- ASA 不支持 QIP DHCP 服务器与 DHCP 代理服务组合使用。
- DHCP 服务器不支持 BOOTP 请求。

DHCPv6 服务器

在已配置 DHCPv6 地址、前缀委派客户端或 DHCPv6 中继的接口上，无法配置 DHCPv6 无状态服务器。

DHCP 中继

- ，其中每个接口最多允许 4 台服务器。
- 最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的接口专用服务器。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下 DHCP 中继服务不可用。但是，可以通过使用访问规则允许 DHCP 流量通过。要允许 DHCP 请求和回复通过 ASA，需要配置两条访问规则，一条允许从内部接口到外部接口（UDP 目标端口 67）的 DCHP 请求，另一条允许来自其他方向（UDP 目标端口 68）的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 ASA 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，ASA支持来自另一个中继服务器的数据包。
- DHCP 客户端必须与 ASA 中继请求的 DHCP 服务器位于不同接口。
- 不能在流量区域内的接口上启用 DHCP 中继。

DDNS 服务

防火墙的 DDNS 仅支持 DynDNS 服务。因此，请确保使用以下语法中的更新 URL 配置 DDNS：

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

配置 DHCP 服务器

本部分介绍如何配置 ASA 提供的 DHCP 服务器。

过程

步骤 1 启用 DHCPv4 服务器，第 5 页。
步骤 2 配置高级 DHCPv4 选项，第 7 页。
步骤 3 配置 DHCPv6 无状态服务器，第 9 页。

启用 DHCPv4 服务器

要在 ASA 接口上启用 DHCP 服务器，请执行以下步骤：

过程

步骤 1 为接口创建一个 DHCP 地址池。ASA 会向客户端分配此池中的一个地址，以供给定时间段内使用。这些地址属于直接连接网络的本地未转换地址。

dhcpd address *ip_address_start-ip_address_end if_name*

示例：

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

该地址池必须与 ASA 接口位于同一子网中。在透明模式下，指定桥接组成员接口。在路由模式下，请指定一个路由接口或 BVI；不要指定桥接组成员接口。

步骤 2 （可选）（路由模式）自动配置从运行 DHCP 或 PPPoE 客户端的接口或从 VPN 服务器获取的 DNS、WINS 和域名值。

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

示例：

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

如果使用以下命令指定 DNS、WINS 或域名参数，则它们将覆盖自动配置获取的参数。

步骤 3 （可选）为客户端保留 DHCP 地址。根据客户端的 MAC 地址，ASA 从配置的地址池中将一个具体的 IP 地址分配给 DHCP 客户端。

dhcpd reserve-address *ip_address mac_address if_name*

示例：

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

保留的地址必须来自配置的地址池，并且地址池必须与ASA接口位于同一子网上。在透明模式下，指定桥接组成员接口。在路由模式下，请指定一个路由接口或 BVI；不要指定桥接组成员接口。

步骤 4 （可选）指定 DNS 服务器的 IP 地址。

dhcpd dns *dns1* [*dns2*]

示例：

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

步骤 5 （可选）指定 WINS 服务器的 IP 地址。最多可指定两台 WINS 服务器。

dhcpd wins *wins1* [*wins2*]

示例：

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

步骤 6 （可选）更改要授予客户端的租用时间。租用时间等于租赁到期之前客户端可以使用向其分配的 IP 地址的时间（以秒为单位）。输入一个介于 0 和 1,048,575 之间的值。默认值为 3600 秒。

dhcpd lease *lease_length*

示例：

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

步骤 7 （可选）配置域名。

dhcpd domain *domain_name*

示例：

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

步骤 8 （可选）配置 ICMP 数据包的 DHCP ping 超时值。为了避免地址冲突，ASA 在将某个地址分配至 DHCP 客户端之前会向该地址发送两个 ICMP ping 数据包。默认值为 50 毫秒。

dhcpd ping timeout *milliseconds*

示例：

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

步骤 9 定义被发送到 DHCP 客户端的默认网关。对于路由模式，如果未使用 **dhcpd option 3 ip** 命令，ASA 会作为默认网关发送启用 DHCP 服务器的接口 IP 地址。对于透明模式，如果要设置默认网关，必须设置 **dhcpd option 3 ip**；ASA 本身不能用作默认网关。

dhcpd option 3 ip *gateway_ip*

示例：

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

步骤 10 在 ASA 内启用 DHCP 后台守护程序，以在启用的接口上侦听 DHCP 客户端请求。

dhcpd enable *interface_name*

示例：

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

指定与 **dhcpd address** 范围相同的接口。

配置高级 DHCPv4 选项

ASA 支持 RFC 2132、RFC 2562 和 RFC 5510 中所列的 DHCP 选项以发送信息。所有 DHCP 选项 (1-255) 均受支持，但 1、12、50 – 54、58 – 59、61、67 和 82 除外。

过程

步骤 1 配置返回一个或两个 IP 地址的 DHCP 选项：

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

示例：

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

选项 150 可为一台或两台 TFTP 服务器提供 IP 地址或名称，以用于思科 IP 电话。选项 3 可为思科 IP 电话设置默认路由。

步骤 2 配置返回文本字符串的 DHCP 选项：

dhcpd option 代码**ascii**文本

示例：

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

选项 66 可提供 TFTP 服务器的 IP 地址或名称，以用于思科 IP 电话。

步骤 3 配置返回十六进制值的 DHCP 选项。

dhcpd option code hex 值

示例：

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

注释
ASA 不验证您提供的选项类型和值是否与 RFC 2132 中定义的选项代码的预期类型和值匹配。例如，可输入 **dhcpd option 46 ascii hello** 命令，尽管 RFC 2132 中定义的选项 46 期望一位数十六进制值，但 ASA 仍将接受配置。有关选项代码及其关联的类型和期望值的详细信息，请参阅 RFC 2132。

下表显示 **dhcpd option** 命令不支持的 DHCP 选项。

表 *1:* 不受支持的 ***DHCP*** 选项

选项代码	说明
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

配置 DHCPv6 无状态服务器

对于配合使用无状态地址自动配置 (SLAAC) 及前缀代理功能 (启用 IPv6 前缀授权客户端) 的客户端，可以将 ASA 配置为在客户端向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

开始之前

此功能仅支持单一路由模式。此功能不支持集群。

过程

步骤 1 配置包含您希望 DHCPv6 服务器提供的信息的 IPv6 DHCP 池：

ipv6 dhcp pool *pool_name*

示例：

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

如果需要，可以为每个接口配置单独的池，也可以在多个接口上使用相同的池。

步骤 2 配置以下要提供给客户端的一个或多个参数以响应 IR 消息：

dns-server *dns_ipv6_address*

domain-name *domain_name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

{[] [] [] [] [] [] [] [] []} **importdns-serverdomain-namenis addressnis domain-namenisp addressnisp domain-namesip addresssip domain-namesntp address**

示例：

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

import 命令使用 ASA 在前缀代理客户端接口上从 DHCPv6 服务器获取的一个或多个参数。您可以混合搭配手动配置的参数与导入的参数；但是手动配置的参数与使用 **import** 命令配置的参数不能相同。

步骤 3 对于您希望 ASA 在其上侦听 IR 消息的接口，进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

步骤 4 启用 DHCPv6 服务器：

ipv6 dhcp server *pool_name*

示例：

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

步骤 5 配置路由器通告以通知 SLAAC 客户端有关 DHCPv6 服务器的信息：

ipv6 nd other-config-flag

此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

示例

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

配置 DHCP 中继代理

在 DHCP 请求进入接口后，ASA 中继将请求转发到的 DHCP 服务器取决于您的配置。您可以配置以下类型的服务器：

- 接口专用 DHCP 服务器 - DHCP 请求进入特定接口后，ASA 仅向接口专用服务器中继请求。
- 全局 DHCP 服务器 - DHCP 请求进入未让接口专用服务器得以配置的接口后，ASA 将向所有全局服务器中继请求。如果接口有接口专用服务器，则将不使用全局服务器。

配置 DHCPv4 中继代理

当 DHCP 请求进入接口时，ASA 将向所有 DHCP 服务器中继该请求。

过程

步骤 1 执行以下两项操作或其中之一：

- 指定一个全局 DHCP 服务器 IP 地址及到达该地址所经过的接口。

  dhcprelay server *ip_address if_name*

  示例：

```
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
```

- 指定连接到 DHCP 客户端网络的接口 ID 以及要用于进入该接口的 DHCP 请求的 DHCP 服务器 IP 地址。

```
interface interface_id
  dhcprelay server ip_address
```

  示例：

```
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
```

  请注意，您没有使用全局 **dhcprelay server** 命令为这些请求指定出口接口；而 ASA 使用路由表确定出口接口。

步骤 2 在与 DHCP 客户端相连的接口上启用 DHCP 中继服务。您可以在多个接口上启用 DHCP 中继。

dhcprelay enable 接口

示例：

```
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
```

步骤 3 （可选）设置为 DHCP 中继地址处理预留的秒数。

dhcprelay timeout 秒

示例：

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

步骤 4 （可选）更改从 DHCP 服务器发送至 ASA 接口地址的数据包中的第一个默认路由器地址。

dhcprelay setroute *interface_name*

示例：

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

此操作允许客户端将其默认路由器设置为指向 ASA，即使 DHCP 服务器指定了其他路由器亦是如此。

如果数据包中没有默认的路由器选项，则 ASA 会添加一个包含接口地址的路由器选项。

步骤 5 （可选）将接口配置为受信任接口。执行以下操作之一：

- 指定您要信任的 DHCP 客户端接口：

  ```
  interface interface_id
    dhcprelay information trusted
  ```

  示例：

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

  您可以将接口配置为受信任接口以保留 DHCP Option 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 giaddr 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。

- 将所有客户端接口配置为受信任接口。

dhcprelay information trust-all

示例：

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

配置 DHCPv6 中继代理

当 DHCPv6 请求进入接口时，ASA 将向所有 DHCPv6 全局服务器中继该请求。

过程

步骤 1 指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

ipv6 dhcprelay server *ipv6_address* [*interface*]

示例：

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

ipv6-address 参数可以是链路范围的单播、组播、站点范围单播或全局 IPv6 地址。不允许将未指定、环回和本地节点组播地址用作中继目标。可选 *interface* 参数为目标指定输出接口。客户端消息通过输出接口连接的链路转发到目标地址。如果指定地址属于链路范围地址，则必须指定接口。

步骤 2 在接口上启用 DHCPv6 中继服务。

ipv6 dhcprelay enable 接口

示例：

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

步骤 3 （可选）指定响应通过中继地址处理中继绑定从 DHCPv6 服务器传递至 DHCPv6 客户端所允许的时间量（以秒为单位）。

ipv6 dhcprelay timeout 秒

示例：

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

seconds 参数的有效值范围为 1 到 3600。默认值为 60 秒。

配置动态 DNS

当接口使用 DHCP IP 寻址时，分配的 IP 地址可以在续约 DHCP 租用时更改。当需要使用完全限定域名 (FQDN) 访问接口时，更改 IP 地址可能导致 DNS 服务器资源记录 (RR) 失效。动态 DNS (DDNS) 提供一种机制，会在 IP 地址或主机名更改时更新 DNS RR。您还可以将 DDNS 用于静态或 PPPoE IP 寻址。

DDNS 在 DNS 服务器上更新以下 RR：A RR 包括名称到 IP 地址的映射，而 PTR RR 将地址映射到名称。

ASA 支持以下 DDNS 更新方法：

- 标准 DDNS，即标准 DDNS 更新方法由 RFC 2136 定义。

  通过此方法，ASA 和 DHCP 服务器使用 DNS 请求更新 DNS RR。ASA 或 DHCP 服务器向其本地 DNS 服务器发送 DNS 请求以获取有关主机名的信息，并根据响应确定拥有 RR 的主 DNS 服务器。然后，ASA 或 DHCP 服务器直接向主 DNS 服务器发送更新请求。请参阅以下典型场景。

  - ASA 更新 A RR，而 DHCP 服务器更新 PTR RR。

    通常情况下，ASA“拥有”A RR，而 DHCP 服务器“拥有”PTR RR，因此两个实体需要单独请求更新。当 IP 地址或主机名更改时，ASA 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 PTR RR 更新。

  - DHCP 服务器既更新 A，也更新 PTR RR。

    如果 ASA 无权更新 A RR，请使用此场景。当 IP 地址或主机名更改时，ASA 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 A 和 PTR RR 更新。

  您可以根据安全需求和主 DNS 服务器的要求配置不同的所有权。例如，对于静态地址，ASA 应拥有两个记录的更新。

- Web - Web 更新方法使用使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。

  使用此方法，当 IP 地址或主机名更改时，ASA 会直接向您拥有帐户的 DNS 提供商发送 HTTP 请求。

注释 BVI 或网桥组成员接口上不支持使用 DDNS。

开始之前

- 依次选择**配置** > **设备管理** > **DNS** > **DNS 客户端** 配置 DNS 服务器。请参阅 配置 DNS 服务器。
- 依次选择**配置** > **设备设置** > **设备名称/密码**，配置设备主机名和域名。请参阅 设置主机名、域名及启用密码和 Telnet 密码。如果未指定每个接口的主机名，则使用设备主机名。如果未指定 FQDN，则对于静态或 PPPoE IP 寻址，系统域名或 DNS 服务器域名将附加到主机名之前。

过程

步骤 1 标准 DDNS 方法：配置 DDNS 更新方法以启用来自 ASA 的 DNS 请求。

如果 DHCP 服务器将执行所有请求，则无需配置 DDNS 更新方法。

a) 创建更新方法。

ddns update method 名称

示例：

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

b) 指定标准 DDNS 方法。

ddns [**both**]

默认情况下，ASA 仅更新A RR。如果您希望 DHCP 服务器更新 PTR RR，请使用此设置。如果希望 ASA 更新 A 和 PTR RR，请指定 **both**。使用 **both** 关键字进行静态或 PPPoE IP 寻址。

示例：

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

c) （可选） 配置 DNS 请求之间的更新接口。

interval maximum *days hours minutes seconds*

默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置天数 (0-364)、小时、分钟和秒。

示例：

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

d) 将此方法与接口关联。请参阅 步骤 3，第 16 页。

步骤 2 Web 方法：配置 DDNS 更新方法，启用来自 ASA 的 HTTP 更新请求。

a) 创建更新方法。

ddns update method 名称

示例：

```
ciscoasa(config)# ddns update method web1
ciscoasa(DDNS-update-method)#
```

b) 指定引用身份名称以验证 ddns 服务器证书身份。ASA 尝试查找主机名匹配项。解析主机失败或未找到匹配项时，连接将终止。

示例：

```
ciscoasa(DDNS-update-method)# web reference-identity dyndns
```

c) 指定 Web 方法和更新 URL。

web update-url https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**

在输入问号 (？) 字符之前，请同时按 Ctrl + V 键。这样，你就可以输入“?”，软件也不会将“?”解释为帮助查询。

示例：

```
ciscoasa(DDNS-update-method)#
web update-url
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

d) （可选） 指定要更新的地址类型（IPv4 或 IPv6）。

默认情况下，ASA 更新所有 IPv4 和 IPv6 地址。如果要限制地址，请输入以下命令。

web update-type {**ipv4** | **ipv6** [**all**] | **both** [**all**]}

- **both all**-（默认）更新所有 IPv4 和 IPv6 地址。
- **both** - 更新 IPv4 地址和最新的 IPv6 地址。
- **ipv4** - 仅更新 IPv4 地址。
- **ipv6** - 仅更新最新的 IPv6 地址。
- **ipv6 all** - 更新所有 IPv6 地址。

示例：

```
ciscoasa(DDNS-update-method)# web update-type ipv4
```

e) （可选） 配置 DNS 请求之间的更新接口。

interval maximum *days hours minutes seconds*

默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置天数 (0-364)、小时、分钟和秒。

示例：

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

f) 将此方法与接口关联。请参阅 步骤 3，第 16 页。

g) DDNS 的 Web 类型方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参见第 步骤 4，第 18 页 步。

步骤 3 配置 DDNS 的接口设置，包括为此接口设置更新方法、DHCP 客户端设置和主机名。

a) 进入接口配置模式。

interface *id*

示例：

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

b) 分配一个更新方法。

ddns update 名称

标准 DDNS 方法：如果您希望 DHCP 服务器执行所有更新，则无需分配方法。Web 更新方法需要执行此命令。

示例：

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

c) 为该接口分配一个主机名。

ddns update hostname *hostname*

如果未设置主机名，则会使用设备主机名。如果未指定 FQDN，则会附加系统域名或 DNS 服务器组中的默认域（用于静态或 PPPoE IP 寻址），或附加来自 DHCP 服务器的域名（用于 DHCP IP 寻址）。

示例：

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

d) 标准 DDNS 方法：确定您希望 DHCP 服务器更新哪些记录。

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

ASA 将 DHCP 客户端请求发送到 DHCP 服务器。请注意，还必须将 DHCP 服务器配置为支持 DDNS。可以将该服务器配置为满足客户端请求，也可以覆盖客户端（在这种情况下，它将回复客户端，因此客户端也不会尝试执行服务器正在执行的更新）。即使客户端不请求 DDNS 更新，也可以将 DHCP 服务器配置为始终发送更新。

静态或 PPPoE IP 寻址，请忽略这些设置。

注释
您还可以使用 **dhcp-client update dns** 命令为所有接口全局设置这些值。每个接口的设置优先于全局设置。

- 默认（无关键字）- 请求 DHCP 服务器执行 PTR RR 更新。此设置与启用 **ddns** A 记录的 DDNS 更新方法配合使用。
- **server both** - 请求 DHCP 服务器同时执行 A 和 PTR RR 更新。此设置不需要将 DDNS 更新方法与接口关联。
- **server none** - 请求 DHCP 服务器不执行更新。此设置与启用 **ddns both** A 和 PTR 记录的 DDNS 更新方法配合使用。

示例：

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

步骤 4 DDNS 的 Web 方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参阅 配置信任点。

示例：

```
crypto ca trustpoint DDNS_Trustpoint
  enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

静态 IP 地址的标准 DDNS 方法

以下示例显示如何配置用于静态 IP 地址的标准 DDNS 方法。请注意，此场景中不配置 DHCP 客户端设置。

```
! 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
```

示例：标准 DDNS 方法；ASA 更新 A RR，DHCP 服务器更新 PTR RR

以下示例将 ASA 配置为更新 A RR，将 DHCP 服务器配置为更新 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
```

示例：标准 DDNS 方法；RR 没有 DHCP 服务器更新

以下示例将 ASA 配置为同时更新 A 和 PTR RR，同时请求 DHCP 服务器更新无 RR。

```
! 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
```

示例：标准 DDNS 方法；DHCP 服务器更新所有 RR

以下示例将 DHCP 客户端配置为请求 DHCP 服务器同时更新 A 和 PTR RR。由于服务器执行所有更新，因此不需要将更新方法与接口关联。

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

示例：Web 类型

以下示例配置 Web 类型方法。

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

监控 DHCP 和 DDNS 服务

本节介绍监控 DHCP 和 DDNS 服务的程序。

监控 DHCP 服务

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  此命令将显示当前 DHCP 服务器客户端绑定、状态和统计信息。

- **show dhcprelay** {**state** | **statistics**}

  此命令将显示 DHCP 中继状态和统计信息。

- **show ipv6 dhcprelay binding**

  此命令可显示中继代理创建的中继绑定条目。

- **show ipv6 dhcprelay statistics**

  此命令可显示 IPv6 的 DHCP 中继代理统计信息。

- **show ipv6 dhcp server statistics**

  此命令显示 DHCPv6 无状态服务器统计信息。以下示例显示了此命令提供的信息：

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]
- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface 命令用于显示所有接口的 DHCPv6 信息。如果接口配置用于 DHCPv6 无状态服务器配置（请参阅配置 DHCPv6 无状态服务器，第 9 页），则此命令将列出该服务器正在使用的 DHCPv6 池。如果接口包含 DHCPv6 地址客户端或前缀委派客户端配置，则此命令将显示各个客户端的状态，以及从该服务器收到的值。对于特定接口，可以显示 DHCP 服务器或客户端的消息统计信息。以下示例显示此命令提供的信息：

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
```

```
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                 preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

show ipv6 dhcp ha statistics 命令用于显示故障转移设备之间的事务处理统计信息，包括在DUID信息各个设备之间的同步次数。以下示例显示了此命令提供的信息。

在主用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

在备用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

故障排除 VTI 上的 DHCP 中继

如果 DHCP 客户端无法获取 IP 地址：

- 验证两个 ASA 站点中的隧道接口/ VTI配置。
- 使用 **show crypto ipsec sa** 命令验证站点之间传输的数据包：

  示例

```
ciscoasa(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cmap, seq num: 10, local addr: 192.168.2.111
access-list CSM_IPSEC_ACL_0 extended permit ip any4 any4
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.2.110
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

启用调试命令

启用 DHCP 中继调试可帮助您了解 DISCOVER/REQUEST 数据包是否已转发到 DHCP 中继服务器：

- **debug dhcprelay event 255**
- **debug dhcprelay packet 255**
- **debug dhcprelay error 255**

示例

```
ciscoasa(config)# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
DHCP: Received a BOOTREQUEST from interface 2 (size = 548)
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPRA: setting giaddr to 192.168.1.111. dhcpd_forward_request: request from xxxx.xxxx.xxxx
forwarded to 192.168.3.112.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on vti interface
DHCP: Received a BOOTREPLY from relay interface 5 (size = 300, xid = xxxxxxxxx) at 04:40:52
UTC Tue Sep 10 2019
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPD/RA: creating ARP entry (192.168.1.88, xxxx.xxxx.xxxx).
DHCPRA: Adding rule to allow client to respond using offered address 192.168.1.95
DHCPRA: forwarding reply to client xxxx.xxxx.xxxx.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
```

监控 DDNS 状态

请参阅以下用于监控 DDNS 状态的命令。

- **show ddns update** {**interface** *if_name* | **method** [*name*]}

  此命令显示 DDNS 更新状态。

  以下示例显示有关 DDNS 更新方法的详细信息：

  ```
  ciscoasa# show ddns update method ddns1

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

  以下示例显示有关 Web 更新方法的详细信息：

  ```
  ciscoasa# show ddns update method web1

  Dynamic DNS Update Method: web1
   Dynamic DNS updated via HTTP(s) protocols
    URL used to update record:
  https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
  ```

  以下示例显示有关 DDNS 接口的信息：

  ```
  ciscoasa# show ddns update interface outside

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

  以下示例显示 Web 类型更新成功：

  ```
  ciscoasa# show ddns update interface outside

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

  Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
  ```

```
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

以下示例显示 Web 类型故障：

```
ciscoasa# show ddns update interface outside

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

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

以下示例显示 DNS 服务器返回 Web 类型更新错误：

```
ciscoasa# show ddns update interface outside

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

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

以下示例显示，由于 IP 地址未配置或 DHCP 请求失败，尚未尝试 Web 更新，例如：

```
ciscoasa# show ddns update interface outside

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

Last Update Not attempted
```

DHCP 和 DDNS 服务的历史记录

功能名称	平台版本	说明
DDNS 支持 Web 更新方法	9.15(1)	您现在可以将接口配置为使用支持 Web 更新方法的 DDNS。 新增/修改的命令：**show ddns update interface**、**show ddns update method**、**web update-url**、**web update-type**
VTI 支持 DHCP 中继服务器	9.14(1)	现在，您可以在 VTI 上启用 DHCP 中继。 新增/修改的命令：**dhcprelay server** 。

功能名称	平台版本	说明
DHCP 预留	9.13(1)	ASA 支持 DHCP 预留。根据客户端的 MAC 地址从定义的地址池中将一个静态 IP 地址分配给 DHCP 客户端。 新增/修改的命令：**dhcpd reserve-address** 。
IPv6 DHCP	9.6(2)	ASA 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - ASA 从 DHCPv6 服务器获取指定的前缀。然后，ASA 可使用这些前缀来配置其他 ASA 接口地址，以使无状态地址自动配置 (SLAAC) 客户端可在同一网络上自动配置 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会向它们提供域名等其他信息。ASA 仅接受 IR 数据包，不向客户端分配地址。 添加或修改了以下命令：**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
DHCPv6 监控	9.4(1)	现在，可以监控适用于 IPv6 的 DHCP 统计信息和适用于 IPv6 的 DHCP 绑定。
DHCP 中继服务器验证 DHCP 服务器标识符是否存在应答	9.4(3)	如果 ASA DHCP 中继服务器收到来自错误的 DHCP 服务器的应答，现在它会验证该应答是否来自正确的服务器，然后对应答做出反应。未引入或修改任何命令。未修改任何 ASDM 屏幕。 未引入或修改任何命令。
DHCP 重新绑定功能	9.1(4)	在 DHCP 重新绑定阶段，客户端会尝试重新绑定到隧道组列表中的其他 DHCP 服务器。在此版本之前，当 DHCP 租约未能更新时，客户端不会重新绑定到备用服务器。 未引入或修改任何命令。
DHCP 受信任接口	9.1(2)	现可将接口配置为受信任接口，以保留 DHCP 选项 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 giaddr 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。 引入或修改了以下命令：**dhcprelay information trusted**、**dhcprelay information trust-all**、**show running-config dhcprelay**。

功能名称	平台版本	说明
每个接口的 DHCP 中继服务器（仅限 IPv4）	9.1(2)	现在可以配置单个接口的 DHCP 中继服务器，因此仅将进入指定接口的请求中继给为该接口指定的服务器。每接口 DHCP 中继不支持 IPv6。 引入或修改了以下命令：**dhcprelay server**（接口配置模式）、**clear configure dhcprelay**、**show running-config dhcprelay**。
适用于 IPv6 的 DHCP 中继 (DHCPv6)	9.0(1)	添加了 DHCP 中继对 IPv6 的支持。 引入了以下命令：**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** 和 **clear ipv6 dhcprelay statistics**。
DDNS	7.0(1)	引入了此功能。 添加了下列命令：**ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns** 和 **show running-config dns server-group**。
DHCP	7.0(1)	ASA 可向连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器或 DHCP 中继服务。 引入了以下命令： **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**和 **show running-config dhcprelay**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。