ipv – ir

ipv4-prefix

要为映射地址和端口 (MAP) 域中的基本映射规则配置 IPv4 前缀，请在 MAP 域基本映射规则配置模式下使用 **ipv4-prefix** 命令。使用此命 **no**令的形式来删除前缀。

ipv4-prefix*ipv4_network_addressnetmask*
no ipv4-prefix*ipv4_network_addressnetmask*

Syntax Description

ipv4_network_addressnetmask	定义客户边缘 (CE) 设备的 IPv4 地址池的 IPv4 前缀。指定网络地址和子网掩码，例如 192.168.3.0 255.255.255.0。不能在不同 MAP 域中使用相同的 IPv4 前缀。

Command Default

无默认值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
MAP域基本映射规则配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.13(1)	引入了此命令。

使用指南

IPv4 前缀定义客户边缘 (CE) 设备的 IPv4 地址池。CE 设备首先将其 IPv4 地址转换为 IPv4 前缀定义的池中的地址（和端口号）。然后，MAP 会使用默认映射规则中的前缀将新地址转换为 IPv6 地址。

CR_Examples

以下示例创建一个名为 1 的 MAP-T 域，并为该域配置转换规则。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
```

```
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

命令	说明
basic-mapping-rule	配置 MAP 域的基本映射规则。
default-mapping-rule	配置 MAP 域的默认映射规则。
ipv4-prefix	为 MAP 域中的基本映射规则配置 IPv4 前缀。
ipv6-prefix	为 MAP 域中的基本映射规则配置 IPv6 前缀。
map-domain	配置映射地址和端口 (MAP) 域。
share-ratio	在 MAP 域中配置基本映射规则中的端口数。
showmap-domain	显示有关映射地址和端口 (MAP) 域的信息。
start-port	配置 MAP 域中基本映射规则的起始端口。

ipv6 address

要启用IPv6并在接口上配置IPv6地址（在路由模式下），或为网桥组或管理接口地址（透明模式）配置 IPv6 地址，请使用 **ipv6address** 命令。要删除 IPv6 地址，请使用此命 **no**令的形式。

ipv6
prefix{**autoconfig**[**autoconfig**[**defaulttrust**{**dhcp**|**ignore**}]|**dhcp**[**default**]|*ipv6_address*|*prefix_name ipv6_address*|*prefix_length*|*ipv6_address***linklocal**[**standby***ipv6_address*]}
no ipv6
prefix{**autoconfig**[**autoconfig**[**defaulttrust**{**dhcp**|**ignore**}]|**dhcp**[**default**]|*ipv6_address*|*prefix_name ipv6_address*|*prefix_length*|*ipv6_address***linklocal**[**standby***ipv6_address*]}

Syntax Description

autoconfig	在接口上启用无状态自动配置。在接口上启用无状态自动配置可根据路由器通告消息中收到的前缀配置 IPv6 地址。当启用无状态自动配置时，将根据修改后的EUI-64接口ID自动为接口生成链路本地地址。不支持透明防火墙模式。 注释 尽管RFC 4862规定配置为无状态自动配置的主机不会发送路由器通告消息，但在这种情况下 ASA 会发送路由器通告消息。查看抑制消息的 **ipv6ndsuppress-ra**命令。
cluster-pool*poolname*	（可选）对于 ASA 集群，设置 **ipv6localpool** 命令定义的集群地址池。参数定义的主集群 IP 地址仅属于当前主设备。每个集群成员都会从此池中收到一个本地 IP 地址。 您无法提前确定分配给每个单元的确切地址；要查看每个单元使用的地址，请输入 **showipv6localpool***poolname* 命令。每个集群成员在加入集群时都会分配到一个成员 ID。该 ID 决定了池中使用的本地 IP。
default	（可选）从路由器通告中获取默认路由。
defaulttrust	（可选）安装来自路由器通告的默认路由。
dhcp (autoconfig)	（可选）指定 ASA 仅使用来自可信来源（换句话说，来自提供 IPv6 地址的同一服务器）的路由器通告的默认路由。
dhcp	从 DHCPv6 服务器获取 IPv6 地址。
ignore	（可选）指定路由器通告可以来自另一个网络，这可能是一种更危险的方法。
ipv6_address/prefix_length	为接口分配全局地址。分配全局地址时，将为接口自动创建链路本地地址。

*ipv6_prefix/prefix_length***eui-64**	通过将指定的前缀与使用修改后的 EUI-64 格式从接口 MAC 地址生成的接口 ID 相结合，为接口分配全局地址。分配全局地址时，将为接口自动创建 链路本地地址。如果为 *+)* 参数指定的值大于 64 位，则前缀位优先于接口 ID。如果另一台主机正在使用指定的地址，系统将显示错误消息。 您不需要指定备用接口；接口 ID 将会自动生成。 修改后的 EUI-64 格式接口 ID 是通过在 48 位链路层 (MAC) 地址的高三个字节 (OUI 字段) 和低三个字节 (序列号) 之间插入十六进制数 FFFE 得出的。为确保所选地址来自唯一以太网以太网 MAC 地址，高顺序字节中的倒数第二位将反转（通用/本地位），以指示 48 位地址的唯一性。例如，MAC 地址为 00E0.B601.3B7A 的接口的 64 位接口 ID 为 02E0:B6FF:FE01:3B7A。
*ipv6_address***link-local**	仅手动配置链路本地地址。使用此命令指定的 *ipv6* 地址 会覆盖为接口自动生成的链路本地地址。链路本地地址由链路本地前缀 FE80::/64 和采用修改的 EUI-64 格式的接口 ID 组成。MAC 地址为 00E0.B601.3B7A 的接口的本地链路地址为 FE80::2E0:B6FF:FE01:3B7A。如果另一台主机正在使用指定的地址，系统将显示错误消息。
prefix_nameipv6_address/prefix_length	使用委托前缀。此功能要求 ASA 接口启用 DHCPv6 前缀委派客户端 (**ipv6dhcpclientpd**)。通常情况下，授权的前缀将为 /60 或更小，因此您可以将其作为多个 /64 网络的子网。如果希望连接的客户端支持 SLAAC，则 /64 是受支持的子网长度。您应指定可以完成 /60 子网的地址，例如 ::1:0:0:0:1。在地址前输入 ::，以免前缀小于 /60。例如，如果授权的前缀是 2001:Db8:1234:5670::/60，则分配给该接口的全局 IP 地址是 2001:DB8:1234:5671::1/64。在路由器通告中通告的前缀是 2001:DB8:1234:5671::/64。在本例中，如果前缀小于 /60，则前缀剩余的位将是 0，就如前导 :: 所指示的那样。例如，如果前缀是 2001:DB8:1234::/48，则 IPv6 地址将为 2001:DB8:1234::1:0:0:0:1/64。
standby*ipv6_address*	（可选）指定故障转移对中的辅助单元或故障转移组使用的接口地址。

Command Default 已禁用 IPv6。

Command Modes 下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。
8.2(2)	增加了对备用地址的支持。
8.4(1)	对于透明模式，添加了桥接组。您应为 BVI 设置 IP 地址，而不是全局设置。
9.0(1)	添加 **cluster-pool**关键字是为了支持 ASA 集群。
9.6(2)	添加了以下选项： • **autoconfigdefaulttrust**{**dhcp** | **ignore**} • **dhcp**[**default**] • *prefix_nameipv6_address/prefix_length*

使用指南

在接口上配置 IPv6 地址可在该接口上启用 IPv6；请参阅指定 IPv6 地址后，无需使用 **ipv6enable** 命令。

多上下文模式指南

在单情景路由防火墙模式下，每个接口地址必须位于唯一的子网上。在多情景模式下，如果此接口位于共享接口上，则每个 IP 地址必须唯一，但在同一子网上。如果接口是唯一的，则此 IP 地址可以在需要时由其他情景使用。

多情景模式不支持 DHCPv6 和前缀代理选项。

透明防火墙指南

透明模式仅支持手动设置 IPv6 地址。透明防火墙不参与 IP 路由。如果要设置 BVI 地址，则只需对 ASA 进行 IP 配置。需要此地址是因为 ASA 使用此地址作为源自 ASA 的流量（例如系统消息或与 AAA 服务器的通信）的源地址。您还可以使用此地址进行远程管理访问。此地址必须与上游和下游路由器位于同一子网上。对于多情景模式，在每个情景内设置管理 IP 地址。对于包含管理接口的型号，您还可以为此接口设置 IP 地址以进行管理。

故障转移指南

备用 IP 地址必须与主 IP 地址位于同一子网。

ASA 集群指南

只有在将集群接口模式配置为单个接口 (**cluster-interfacemodeindividual**) 后，您才能为单个接口设置集群池。唯一的例外情况是仅管理接口：

- 您始终可以将仅管理接口配置为单独的接口，即使在跨网以太网通道模式下也是如此。即使在透明防火墙模式下，管理接口也可以是单独的接口。
- 在跨网以太网通道模式下，如果将管理接口配置为单独接口，则无法为管理接口启用动态路由。您必须使用静态路由。

集群不支持 DHCPv6 和前缀委派选项。

CR_Examples

以下示例将 2001:0DB8:BA98::3210/64 分配为选定接口的全局地址，并将 2001:0DB8:BA98::3211 分配为备用设备上相应接口的地址：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

以下示例为所选接口自动分配 IPv6 地址：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

以下示例将 IPv6 前缀 2001:0DB8:BA98::/64 分配到所选接口，并在地址的低 64 位指定 EUI-64 接口 ID。如果此设备属于故障转移对，则无需指定 **standby** 关键字；备用地址将使用修改的 EUI-64 接口 ID 自动创建。

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

以下示例分配 FE80::260:3EFF:FE11:6670 作为所选接口的链路级地址：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

以下示例分配 FE80::260:3EFF:FE11:6670 作为故障转移对中主设备上所选接口的链路级地址，并分配 FE80::260:3EFF:FE11:6671 作为链路级地址已完成。

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

以下示例分配 ::1:0:0:0:1/64 作为完成指定前缀的地址：

```
ciscoasa(config)# interface gigabitethernet 0/5
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

Related Commands

命令	说明
debugipv6interface	显示 IPv6 接口的调试信息。
showipv6interface	显示为 IPv6 配置的接口的状态。

ipv6-address-pool

要指定用于向远程客户端分配地址的 IPv6 地址池列表，请在 tunnel-group general-attributes 配置模式下使用 **ipv6-address-pool** 命令。要消除 IPv6 地址池，请使用此命令的 **no** 形式。

ipv6-address-pool [（*interface_name*）] *ipv6_address_pool* [*...ipv6_address_pool6*]
no ipv6-address-pool [（*interface_name*）] *ipv6_address_pool* [*...ipv6_address_pool6*]

Syntax Description

interface_name	（可选）指定用于地址池的接口。
ipv6_address_pool	指定使用**ipv6localpool** 命令配置的地址池的名称。最多可以指定六个本地地址池。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Tunnel-group 隧道组常规属性配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

您可以输入多个命令，每个接口一个。如果未指定接口，则 命令指定所有未显式引用的接口的默认值。

group-policy **ipv6-address-pools** 命令中的 IPv6 地址池设置会覆盖 tunnel group**ipv6-address-pool** 命令中的 IPv6 地址池设置。

地址池的指定顺序非常重要。ASA 按照这些地址池在此命令中出现的顺序分配这些地址池中的地址。

CR_Examples

以下示例在 tunnel-group general-attributes 配置模式下输入，指定用于将 IPsec 远程访问隧道组测试的地址分配给远程客户端的 IPv6 地址池列表：

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
```

```
ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

Related Commands

命令	说明
ipv6-address-pools	配置组策略的IPv6地址池设置，这会覆盖隧道组的这些设置。
ipv6 local pool	配置用于 VPN 远程访问隧道的 IP 地址池。
clear configure tunnel-group	清除所有配置的隧道组。
show running-config tunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group	配置隧道组。

ipv6-address-pools

要指定最多包含六个 IPv6 地址池的列表（从中将地址分配给远程客户端），请在 group-policy 属性配置模式下使用**ipv6-address-pools**命令。要从组策略中删除属性并启用从其他组策略源继承，请使用此命令的 **no** 形式。

ipv6-address-pools value*ipv6_address_poll1*[*...ipv6_address_pool6*]
no ipv6-address-pools value*ipv6_address_poll1*[*...ipv6_address_pool6*]
ipv6-address-poolsnone
noipv6-address-poolsnone

Syntax Description

ipv6_address_pool	指定使用**ipv6localpool** 命令配置的最多六个 IPv6 地址池的名称。使用空格分隔 IPv6 地址池名称。
none	指定不配置 IPv6 地址池，并禁用从其他组策略源继承。
value	指定包含最多六个 IPv6 地址池的列表，要从中分配地址。

Command Default

默认情况下，未配置 IPv6 地址池属性。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略属性配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

使用指南

要配置 IPv6 地址池，请使用 **ipv6localpool** 命令。

在命令中指定池的顺**ipv6-address-pools**序很重要。ASA 按照这些地址池在此命令中出现的顺序分配这些地址池中的地址。

该 **ipv6-address-poolsnone** 命令禁止从其他策略源（例如 DefaultGrpPolicy）继承此属性。该命**ipv6-address-poolsnone**令从配置中删除该命令，恢复默认值，即允许继承。**noipv6-address-poolsnone**

CR_Examples

以下示例在 group-policy 属性配置模式下配置名为 firstipv6pool 的 IPv6 地址池用于向远程客户端分配地址，然后将该池与 GroupPolicy1 关联：

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# ipv6-address-pools value firstipv6pool
ciscoasa(config-group-policy)#
```

Related Commands

命令	说明
ipv6localpool	配置要用于 VPN 组策略的 IPv6 地址池。
clear configure group-policy	清除所有已配置的组策略。
show running-config group-policy	显示所有组策略或特定组策略的配置。

ipv6 dhcp client pd

要启用 DHCPv6 前缀委派客户端并命名在接口上获取的前缀，请在 **ipv6dhcpclientpd**接口配置模式下使用该命令。要禁用客户端，请使用此命 **no**令的形式。

ipv6 dhcp client pd*name*
no ipv6 dhcp client pd*name*

Syntax Description

name 设置此前缀的名称。name 最长为 200 个字符。在将 IP 地址分配给使用前缀 (**ipv6address***prefix_name*) 的接口时，将使用此名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.6(2)	我们引入了此命令。

使用指南

在一个或多个接口上启用 DHCPv6 前缀代理客户端。ASA 可获取一个或多个可设置子网和分配给内部网络的 IPv6 前缀。通常，在其上启用前缀代理客户端的接口使用 DHCPv6 地址客户端获取其 IP 地址，只有其他 ASA 接口才能使用代理前缀衍生的地址。

此功能不支持集群。

无法在仅管理接口上配置此功能。

CR_Examples

以下示例在 GigabitEthernet 0/0 上配置 DHCPv6 地址客户端和前缀代理客户端，然后在 GigabitEthernet 0/1 和 0/2 上分配包含该前缀的地址：

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 dhcp client pd hint

要提供一个或多个有关您希望接收的授权前缀的提示，请在接口配置模式下使用**ipv6dhcpclientpdhint**命令。要禁用客户端，请使用此命 **no**令的形式。

ipv6 dhcp client pd hint*ipv6_prefix/prefix_length*
no ipv6 dhcp client pd hint*ipv6_prefix/prefix_length*

Syntax Description

ipv6_prefix/prefix_length	指定要接收的 IPv6 前缀和长度。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.6(2)	我们引入了此命令。

使用指南

通常，您需要请求特定的前缀长度（例如 ::/60），或者如果您以前收到过特定前缀并希望确保在租用到期后重新获取该前缀，可以作为提示输入整个前缀。如果输入了多个提示（不同的前缀或长度），则由 DHCP 服务器来决定要尊重的提示或是否尊重提示。

CR_Examples

以下示例在 GigabitEthernet 0/0 上配置 DHCPv6 地址客户端和前缀代理客户端，然后在 GigabitEthernet 0/1 和 0/2 上分配包含该前缀的地址：

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。

命令	说明
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 dhcp pool

要配置 IPv6 DHCP 池以包含您希望 DHCPv6 服务器向无状态地址自动配置 (SLAAC) 客户端提供的信息，请在全局配置模式下使用 **ipv6dhcppool** 命令。要删除池，请使用此命 **no**令的形式。

ipv6 dhcp pool*pool_name*
no ipv6 dhcp pool*pool_name*

Syntax Description

pool_name	指定地址池。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
9.6(2)	我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA，使其在向 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。使用 **ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定此池名称。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。输入**ipv6dhcppool** 命令后，您可以配置一个或多个要提供给客户端的参数。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

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
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。

命令	说明
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 dhcprelay enable

要在接口上启用 DHCPv6 中继服务，请在全局配置模式下使用 **ipv6dhcprelayenable**命令。要禁用 DHCPv6 中继服务，请使用此命令的 **no** 形式。

ipv6 dhcprelay enable*interface*
no ipv6 dhcprelay enable*interface*

Syntax Description

接口	指定目标的输出接口。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

此命令允许您在接口上启用 DHCPv6 中继服务。启用服务后，来自接口上的客户端的传入 DHCPv6 消息（可能已由另一个中继代理中继）将通过所有已配置的传出消息转发到所有已配置的中继目标链接。对于多上下文模式，您不能在由多个上下文（即共享接口）使用的接口上启用 DHCP 中继服务。

CR_Examples

以下示例显示如何在 ASA 外部接口上为具有 IP 地址 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 的 DHCPv6 服务器配置 DHCPv6 中继代理。客户端请求来自 ASA 内部接口，绑定超时值为 90 秒。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

命令	说明
ipv6dhcprelayserver	指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

命令	说明
ipv6dhcprelaytimeout	设置允许 DHCPv6 服务器的响应通过中继绑定结构传递到 DHCPv6 客户端的时间量（以秒为单位）。

IPv6 dhcprelay 服务器

要指定客户端消息转发到的 IPv6 DHCP 服务器目标地址，请在 **ipv6dhcprelayserver** 全局配置模式下使用该命令。要删除 IPv6 DHCP 服务器目标地址，请使用此命令的 **no**形式。

ipv6 dhcprelay server*ipv6-address* [*interface*]
no ipv6 dhcprelay server*ipv6-address* [*interface*]

Syntax Description

接口	（可选）指定目标的输出接口。
ipv6-address	可以是链路范围的单播、多播、站点范围的单播或全局 IPV6 地址。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

此命令可让您指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。客户端消息通过输出接口所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。不允许将未指定、环回和本地节点组播地址用作中继目标。您可以为每个情景指定最多十个服务器。

CR_Examples

以下示例显示如何在 ASA 外部接口上为具有 IP 地址 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 的 DHCPv6 服务器配置 DHCPv6 中继代理。客户端请求来自 ASA 内部接口，绑定超时值为 90 秒。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

命令	说明
ipv6dhcprelayenable	在接口上启用 IPv6 DHCP 中继服务。

命令	说明
ipv6dhcprelaytimeout	设置允许 DHCPv6 服务器的响应通过中继绑定结构传递到 DHCPv6 客户端的时间量（以秒为单位）。

ipv6 dhcprelay timeout

如要设置从DHCPv6服务器到通过中继绑定结构将响应传递至客户端所允许的时间（以秒为单位），请在全局配置模式下使用 **ipv6dhcprelaytimeout**命令。要恢复默认设置，请使用此命 **no**令的形式。

ipv6dhcprelaytimeout*seconds*
noipv6dhcprelaytimeout*seconds*

Syntax Description

seconds	设置允许 DHCPv6 中继地址协商的秒数。有效值范围为 1 至 3600。

Command Default

默认值为 60 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

此命令允许您设置 DHCPv6 服务器的响应通过中继绑定结构传递到 DHCPv6 客户端的时间（以秒为单位）。

CR_Examples

以下示例显示如何在 ASA 外部接口上为具有 IP 地址 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 的 DHCPv6 服务器配置 DHCPv6 中继代理。客户端请求来自 ASA 内部接口，绑定超时值为 90 秒。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

命令	说明
ipv6dhcprelayserver	指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。
ipv6dhcprelayenable	指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

ipv6 dhcp server

对于结合前缀委派功能和无状态地址自动配置 (SLAAC) 功能的客户端，请在接口配置模式下使用 **ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器。要禁用 DHCP 服务器，请使用此命 **no**令的形式。

ipv6 dhcp server*pool_name*
no ipv6 dhcp server*pool_name*

Syntax Description

pool_name	设置使用 **ipv6dhcppool**命令配置的 IPv6 池的名称。此池包含您想提供给给定接口上客户端的信息。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.6(2)	我们引入了此命令。

使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA，使其在向 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。使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

CR_Examples

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
```

Related Commands

命令	说明
clearipv6dhcpstatistics	清除 DHCPv6 统计信息。
domain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的域名。
dns-server	配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。
import	使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。
ipv6address	启用 IPv6 并在接口上配置 IPv6 地址。
ipv6addressdhcp	使用 DHCPv6 获取接口的地址。
ipv6dhcpclientpd	使用授权前缀设置接口的地址。
ipv6 dhcp client pd hint	提供关于您想要接收的委托前缀的一个或多个提示。
ipv6dhcppool	创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。
ipv6dhcpserver	启用 DHCPv6 无状态服务器。
network	将 BGP 配置为通告从服务器接收的授权前缀。
nisaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。
nisdomain-name	配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。
nispaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。
nispdomain-name	配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。
showbgpipv6unicast	显示 IPv6 BGP 路由表中的条目。
showipv6dhcp	显示 DHCPv6 信息。
showipv6general-prefix	显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。
sipaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。
sipdomain-name	配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。
sntpaddress	配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。

ipv6 enable

要启用 IPv6 处理，而您尚未配置显式 IPv6 地址，请在全局配置模式下使用 **ipv6enable**命令。要禁用尚未配置明确 IPv6 地址的接口上的 IPv6 处理，请使用此 **no**命令的形式。

ipv6 enable
no ipv6 enable

Syntax Description

此命令没有任何参数或关键字。

Command Default

已禁用 IPv6。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	• 支持	—
全局配置	—	• 是	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

ipv6enable 命令会在接口上自动配置 IPv6 本地链路单播地址，同时还会启用接口以进行 IPv6 处理。

该 **noipv6enable**命令不会禁用配置了显式 IPv6 地址的接口上的 IPv6 处理。

CR_Examples

以下示例在所选接口上启用 IPv6 处理：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

Related Commands

命令	说明
ipv6address	为接口配置 IPv6 地址并在接口上启用 IPv6 处理。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 enforce-eui64

要强制在本地链路上的 IPv6 地址中使用修改后的 EUI-64 格式接口标识符，请在 **ipv6enforce-eui64** 全局配置模式下使用该命令。要禁用修改的 EUI-64 地址格式实施，请使用此命令的 **no** 形式。

ipv6 enforce-eui64*if_name*
no ipv6 enforce-eui64*if_name*

Syntax Description

if_name 指定要启用修改后的EUI-64地址格式强制执行的接口的名称（由命**nameif**令指定）。

Command Default

已禁用修改的 EUI-64 格式实施。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

当在接口上启用此命令时，将根据源 MAC 地址验证该接口上接收的 IPv6 数据包的源地址，以确保接口标识符使用修改后的 EUI-64 格式。如果 IPv6 数据包不使用修改后的 EUI-64 格式作为接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
%ASA-3-325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。从路由器背后的主机接收的数据包将无法通过地址格式验证，且会被丢弃，因为其源 MAC 地址将是路由器 MAC 地址，而不是主机 MAC 地址。

修改后的 EUI-64 格式接口标识符由 48 位链路层 (MAC) 地址派生而来，通过在链路层地址的高三个字节（OUI字段）和低三个字节（序列号）之间插入十六进制数FFFE。为确保所选地址来自唯一以太网以太网MAC地址，高顺序字节中的倒数第二位将反转（通用/本地位），以指示48位地址的唯一性。例如，MAC 地址为 00E0.B601.3B7A 的接口的 64 位接口 ID 为 02E0:B6FF:FE01:3B7A。

CR_Examples

以下示例为在内部接口上接收的 IPv6 地址启用 EUI-64 修改格式的实施：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

Related Commands

命令	说明
ipv6address	在接口上配置 IPv6 地址。
ipv6enable	在接口上启用 IPv6。

ipv6 icmp

要配置接口的ICMP访问规则，请在**ipv6icmp**全局配置模式下使用该命令。要删除ICMP访问规则，请使用此命 **no**令的形式。

ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host***ipv6-address*} [*icmp-type*] *if-name*
no ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host***ipv6-address*} [*icmp-type*] *if-name*

Syntax Description

any	指定任何 IPv6 地址的关键字。IPv6 前缀 ::/0 的缩写。
deny	阻止选定接口上的指定 ICMP 流量。
host	表示引用特定主机的地址。
icmp-type	指定由访问规则过滤的ICMP消息类型。该值可以是有效的ICMP类型编号（0至255）或以下 ICMP 类型文字之一： • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	应用访问规则的接口的名称，由 **nameif** 命令指定。
ipv6-address	向接口发送 ICMPv6 消息的主机的 IPv6 地址。
ipv6-prefix	向接口发送 ICMPv6 消息的 IPv6 网络。

permit	允许选定接口上的指定 ICMP 流量。
prefix-length	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。

Command Default

如果未定义 ICMP 访问规则，则允许所有 ICMP 流量。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

IPv6 中的 ICMP 功能与 IPv4 中的 ICMP 相同。ICMPv6 生成错误消息，例如 ICMP 目的地不可达消息以及信息性消息（例如 ICMP 回应请求和应答消息）。另外，IPv6中的ICMP数据包用于IPv6邻居发现过程和路径MTU发现。

启用 IPv6 的接口上允许的最小 MTU 为 1280 字节；但是，如果在接口上启用了 IPsec，则由于 IPsec 加密会产生开销，因此 MTU 值不应设置为低于 1380。将接口设置为低于 1380 字节可能会导致数据包丢失。

如果没有为接口定义 ICMP 规则，则允许所有 IPv6 ICMP 流量。

如果为接口定义了 ICMP 规则，则系统按照“匹配优先”的顺序处理这些规则，然后是隐式“拒绝所有”规则。例如，如果第一个匹配的规则是允许规则，将处理 ICMP 数据包。如果第一个匹配的规则是拒绝规则，或者 ICMP 数据包未与该接口上的任何规则匹配，则 ASA 将丢弃该 ICMP 数据包并生成一条系统日志消息。

因此，输入ICMP规则的顺序非常重要。如果输入一条拒绝来自特定网络的所有ICMP流量的规则，然后遵循该规则的是允许来自该网络上的特定主机的 ICMP 流量的规则，系统将永远不会处理主机规则。ICMP流量被网络规则阻止。但是，如果先输入主机规则，后输入网络规则，将允许主机ICMP流量，而阻止该网络中的所有其他 ICMP 流量。

ipv6icmp 命令为在 ASA 接口终止的 ICMP 流量配置访问规则。要配置传递 ICMP 流量的访问规则，请参阅**ipv6access-list**命令。

CR_Examples

以下示例拒绝所有 ping 请求并允许外部接口上的所有数据包过大消息（以支持路径 MTU 发现）：

```
ciscoasa(config)# ipv6 icmp deny any echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

以下示例允许主机 2000:0:0:4::2 或前缀 2001::/64 上的主机 ping 外部接口：

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

命令	说明
ipv6access-list	配置访问列表。

ipv6 local pool

要配置IPv6地址池，请在**ipv6localpool**全局配置模式下使用该命令。要删除池，请使用此命**no**令的形式。

ipv6 local pool*pool_nameipv6_address/prefix_lengthnumber_of_addresses*
no ipv6 local pool*pool_nameipv6_address/prefix_lengthnumber_of_addresses*

Syntax Description

ipv6_address	指定池的起始 IPv6 地址。
number_of_addresses	范围：1-16384。
pool_name	指定要分配给此IPv6地址池的名称。
prefix_length	范围：0-128。

Command Default

默认情况下，未配置 IPv6 本地地址池。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	已为**ipv6address**命令中的集群池添加了 IPv6 本地池，以支持 ASA 集群。

使用指南

对于 VPN，要分配 IPv6 本地池，请在隧道组中使用 **ipv6-local-pool** 命令或在组策略中使用 **ipv6-address-pools**命令（请注意此命令上的“s”）。组策略中的 ipv6-address-pools 设置覆盖隧道组中的 ipv6-address-pools 设置。

CR_Examples

以下示例配置名为 firstipv6pool 的 IPv6 地址池，以便用于向远程客户端分配地址：

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

Related Commands

命令	说明
ipv6-address-pool	将 IPv6 地址池与 VPN 隧道组策略关联。
ipv6-address-pools	将 IPv6 地址池与 VPN 组策略关联。
clear configure IPv6 local pool	清除所有已配置的 IPv6 本地池。
show running-config ipv6	显示 IPv6 的配置。

ipv6 nd dad attempts

要配置重复地址检测期间接口上连续发送的邻居请求消息的数量，请在接口配置模式下使用 **ipv6nddadattempts** 命令。要恢复到发送的重复地址检测消息的默认数量，请使用此命令的 **no** 形式。

ipv6 nd dad attempts值
no ipv6 nd dad attempts值

Syntax Description

value 介于 0 到 600 之间的数字。输入 0 将禁用指定接口上的重复地址检测。输入 1 配置单次传输，无后续传输。默认值为 1 条消息。

Command Default

默认尝试次数为 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

重复地址检测会在将新单播 IPv6 地址分配给接口之前验证其唯一性（在执行重复地址检测时，新地址保持暂定状态）。重复地址检测使用邻居请求消息来验证单播 IPv6 地址的唯一性。发送邻居请求消息的频率使用 **ipv6ndns-interval** 命令进行配置。

在管理上处于关闭状态的接口上，重复地址检测将被暂停。当接口处于管理性关闭状态时，单播 IPv6 地址将分配给设置为处于暂停状态的接口。

当接口恢复到管理性启用状态时，重复地址检测将在接口上自动重启。返回管理状态的接口将重新启动该接口上所有单播 IPv6 地址的重复地址检测。

注释 对接口的链路本地地址执行重复地址检测时，其他 IPv6 地址的状态仍会设置为暂定。对链路本地地址完成重复地址检测后，将对其余 IPv6 地址执行重复地址检测。

当重复地址检测识别到一个重复地址时，地址的状态设置为“重复”，并且不使用该地址。如果重复地址是接口的链路本地地址，则接口上会禁用 IPv6 数据包的处理，并发出类似以下内容的错误消息：

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

如果重复地址是接口的全局地址，则不会使用该地址，并会发出类似如下的错误消息：

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

当地址状态设置为 DUPLICATE 时，与重复地址相关的所有配置命令仍保持配置状态。

如果接口的链路本地地址发生变化，则会对新的链路本地地址执行重复地址检测，并重新生成与该接口关联的所有其他 IPv6 地址（仅对新的链路本地地址执行重复地址检测）。

CR_Examples

以下示例将配置为在对接口的暂定单播 IPv6 地址执行重复地址检测时，发送 5 条连续的邻居请求消息：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

以下示例在所选接口上禁用重复地址检测：

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

Related Commands

命令	说明
ipv6ndns-interval	配置接口上 IPv6 邻居请求传输之间的间隔。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd managed-config-flag

要将 ASA 配置为在 IPv6 路由器通告数据包中设置托管地址配置标志，请在接口配置模式下使用 **ipv6ndmanagedconfig-flag**命令。要恢复默认设置，请使用此命 **no**令的形式。

ipv6 nd managed-config-flag
no ipv6 managed-config-flag

Syntax Description

此命令没有任何参数或关键字。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

IPv6 自动配置客户端主机可使用此标志来指示其必须使用有状态地址配置协议 (DHCPv6) 来获取除派生的无状态自动配置地址之外的地址。

CR_Examples

以下示例在接口 GigabitEthernet 0/0 的 IPv6 路由器通告数据包中设置托管地址配置标志：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

Related Commands

命令	说明
ipv6ndother-config-flag	配置 ASA 以设置 IPv6 路由器通告数据包中的另一个配置标志。

ipv6 nd ns-interval

要配置接口上 IPv6 邻居请求重新传输之间的间隔，请在 **ipv6ndns-interval**接口配置模式下使用该命令。要恢复默认值，请使用此命 **no**令的形式。

ipv6 nd ns-interval值
no ipv6 nd ns-interval [*value*]

Syntax Description

value IPv6 邻居请求传输之间的间隔（以毫秒为单位）。有效值范围为 1000 至 3600000 毫秒。默认值为 1000 毫秒。

Command Default

邻居请求传输之间的默认间隔为 1000 毫秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

此值将包含在通过此接口发送的所有 IPv6 路由器通告中。

CR_Examples

以下示例为 GigabitEthernet 0/0 配置 9000 毫秒的 IPv6 邻居请求传输间隔：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

命令	说明
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd other-config-flag

要将 ASA 配置为在 IPv6 路由器通告数据包中设置 other config 标志，请在接口配置模式下使用 **ipv6ndother-config-flag**命令。要恢复默认设置，请使用此命 **no**令的形式。

ipv6 nd other-config-flag
no ipv6 other-config-flag

Syntax Description

此命令没有任何参数或关键字。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

IPv6 自动配置客户端主机可以使用此标志来指示它必须使用状态地址配置协议 (DHCPv6) 获取非地址配置信息，例如 DNS 服务器信息。

CR_Examples

以下示例在接口 GigabitEthernet 0/0 的 IPv6 路由器通告数据包中设置其他配置标志：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

Related Commands

命令	说明
ipv6ndmanaged-config-flag	配置 ASA 以在 IPv6 路由器通告数据包中设置托管地址配置标志。

ipv6 nd prefix

要配置 IPv6 路由器通告中包含的 IPv6 前缀，请在接口配置模式下使用 **ipv6ndprefix** 命令。要删除前缀，请使用此命 **no**令的形式。

ipv6 nd
prefix*ipv6-prefix*|*prefix-length*|**default**[[*valid-lifetimepreferred-lifetime*] | [**at***valid-datepreferred-date*] |**infinite**|**no-advertise**|**off-link**|**no-autoconfig**]
no ipv6 nd
prefix*ipv6-prefix*|*prefix-length*|**default**[[*valid-lifetimepreferred-lifetime*] | [**at***valid-datepreferred-date*] |**infinite**|**no-advertise**|**off-link**|**no-autoconfig**]

Syntax Description

at*valid-datepreferred-date*	生命周期和偏好到期的日期和时间。EXTEN 到达此指定的日期和时间之前，前缀均有效。日期以 date-valid *-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* 的形式表示。
default	已使用默认值。
infinite	（可选）有效的生命周期不会到期。
ipv6-prefix	路由器通告中包含的 IPv6 网络号。 此参数必须采用 RFC 2373 中记录的形式，其中地址以冒号之间的 16 位值以十六进制格式指定。
no-advertise	（可选）向本地链路上的主机指示指定的前缀不用于 IPv6 自动配置。对于 **default** 前缀，此设置仅适用于 on-link 前缀。除非您为特定 Off-link 前缀指定 **no-advertise**，否则系统仍将通告 Off-link 前缀。
no-autoconfig	（可选）向本地链路上的主机指示指定的前缀不能用于 IPv6 自动配置。
off-link	（可选）表示指定的前缀不用于链路上确定。
首选有效期限	指定 IPv6 前缀被宣传为首选的时间量（以秒为单位）。值的范围为 0 到 4294967295 秒。最大值代表无穷大，也可以使用 **infinite** 关键字指定。默认值为 604800 秒（7 天）。
prefix-length	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。
valid-lifetime	指定 IPv6 前缀被宣传为有效的时间量。值的范围为 0 到 4294967295 秒。最大值代表无穷大，也可以使用 **infinite** 关键字指定。默认值为 2592000 秒（30 天）。

Command Default

在发起 IPv6 路由器通告的接口上配置的所有前缀均采用 2592000 秒（30 天）的有效生命周期和 604800 秒（7 天）的首选生命周期进行通告，并同时设置“onlink”和“autoconfig”标志。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令允许控制每个前缀的各个参数，包括是否应通告该前缀。

默认情况下，使用该命令在接口上配置为地址的**ipv6address**前缀将在路由器通告中通告。如果您使用该命令配置要通告的 **ipv6ndprefix** 前缀，则仅通告这些前缀。

该关 **default**键字可用于为所有前缀设置默认参数。

可以设置日期来指定前缀的过期日期。实时倒计时有效有效期和首选有效期。到达到期日期时，将不再通告前缀。

当 onlink 为“on”（默认）时，指定的前缀将分配给链接。向包含指定前缀的此类地址发送流量的节点会将目标视为在链路上本地可访问。

当自动配置处于“开启”状态（默认）时，它向本地链路上的主机指示指定的前缀可用于 IPv6 自动配置。

CR_Examples

以下示例包含 IPv6 前缀 2001:200::/35，在指定接口上发出的路由器通告中，有效生命周期为 1000 秒，首选生命周期为 900 秒：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

命令	说明
ipv6address	配置 IPv6 地址并在接口上启用 IPv6 处理。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd ra-interval

要配置接口上IPv6路由器通告传输之间的间隔，请在**ipv6ndra-interval**接口配置模式下使用该命令。要恢复默认间隔，请使用此命 **no**令的形式。

ipv6 nd ra-interval [**msec**] *value*
no ipv6 nd ra-interval [[**msec**] *value*]

Syntax Description

msec	（可选）表示提供的值以毫秒为单位。如果不存在此关键字，则提供的值为秒。
value	IPv6 路由器通告传输之间的间隔。有效值范围为 3 至 1800 秒，或 500 至 1800000 毫秒（如果提供了关 **msec**键字）。默认值为 200 秒。

Command Default

200 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果使用该命令将 ASA 配置为默认路由器，则传输间隔应小于或等于 IPv6 路由器通告生存**ipv6ndra-lifetime**期。为防止与其他 IPv6 节点的同步，请将所用的实际值随机调整为指定值的 20% 以内。

CR_Examples

以下示例为所选接口配置 201 秒的 IPv6 路由器通告间隔：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

Related Commands

命令	说明
ipv6ndra-lifetime	配置 IPv6 路由器通告的有效期。
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd ra-lifetime

要在接口上配置IPv6路由器通告中的“路由器有效期”值，请在接口配置模式下使用**ipv6ndra-lifetime**命令。要恢复默认值，请使用此命 **no**令的形式。

ipv6 nd ra-lifetime秒
no ipv6 nd ra-lifetime[秒]

Syntax Description

seconds	ASA 作为此接口上的默认路由器的有效性。值的范围为 0 到 9000 秒。默认值为 1800 秒。0 表示 ASA 不应被视为所选接口上的默认路由器。

Command Default

1800秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

通过接口发送的所有 IPv6 路由器通告中都包含“路由器寿命”值。此值表示 ASA 作为此接口的默认路由器的益处。

将该值设置为非零值表示应将ASA视为此接口上的默认路由器。“路由器寿命”值的非零值不应小于路由器通告间隔。

将值设置为 0 表示 ASA 不应被视为此接口上的默认路由器。

CR_Examples

以下示例为所选接口配置 1801 秒的 IPv6 路由器通告有效期限：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

命令	说明
ipv6ndra-interval	配置接口上IPv6路由器通告传输之间的间隔。

命令	说明
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd reachable-time

要配置在发生可达性确认事件后远程 IPv6 节点被视为可达的时间量，请在 **ipv6ndreachable-time**接口配置模式下使用该命令。要恢复默认时间，请使用此命 **no**令的形式。

ipv6 nd reachable-time值
no ipv6 nd reachable-time [*value*]

Syntax Description

value 远程 IPv6 节点被视为可达的时间量（以毫秒为单位）。有效值范围为 0 至 3600000 毫秒。默认值为 0。

当 值 参数使用 0 时，可达时间将作为未确定时间发送。由接收设备来设置和跟踪可访问时间的值。

Command Default

零毫秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

配置的时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快；但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

要查看 ASA 使用的可访问时间（包括此命令设置为 0 时的实际值），请使用 **showipv6interface** 命令显示有关 IPv6 接口的信息，包括正在使用的 ND 可访问时间。

CR_Examples

以下示例为所选接口配置 1700000 毫秒的 IPv6 可访问时间：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

命令	说明
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 nd suppress-ra

要抑制 IPv6 路由器通告在 LAN 接口上的传输，请在接口配置模式下使用 **ipv6ndsuppress-ra** 命令。要在 LAN 接口上重新启用发送 IPv6 路由器通告传输，请使用此命令的 **no** 形式。

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Syntax Description

此命令没有任何参数或关键字。

Command Default

如果启用了 IPv6 单播路由，将在 LAN 接口上自动发送路由器通告。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

使用**noipv6ndsuppress-ra** 命令，可在非 LAN 接口类型（例如串行接口或隧道接口）上启用 IPv6 路由器通告传输。

CR_Examples

以下示例抑制所选接口上的 IPv6 路由器通告：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra
```

Related Commands

命令	说明
showipv6interface	显示为 IPv6 配置的接口的可用性状态。

ipv6 neighbor

要在 IPv6 邻居发现缓存中配置静态条目，请在全局配置模式下使用 **ipv6neighbor** 命令。要从邻居发现缓存中删除静态条目，请使用此命令的 **no** 形式。

ipv6 neighbor*ipv6_addressif_namemac_address*
no ipv6 neighbor*ipv6_addressif_name*[*mac_address*]

Syntax Description

if_name	由 **nameif** 命令指定的内部或外部接口名称。
ipv6_address	与本地数据链路地址对应的 IPv6 地址。
mac_address	本地数据线路（硬件 MAC）地址。

Command Default

静态条目不在 IPv6 邻居发现缓存中配置。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

该**ipv6neighbor**命令与该 **arp**命令类似。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。当使用该命令存储配置时，**copy**这些条目将存储在配置中。

使用该 **showipv6neighbor**命令查看 IPv6 邻居发现缓存中的静态条目。

该**clearipv6neighbors**命令将删除 IPv6 邻居发现缓存中除静态条目之外的所有条目。The **noipv6neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. 使用该命令禁用接口上的 **noipv6enable**IPv6 将会删除为该接口配置的所有 IPv6 邻居发现缓存条目，静态条目除外（条目的状态更改为 INCMP [Incomplete]）。

邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。

CR_Examples

以下示例将 IPv6 地址为 3001:1::45A 和 MAC 地址为 0002.7D1A.9472 的内部主机的一个静态条目添加到邻居发现缓存：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

命令	说明
clearipv6neighbors	删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。
showipv6neighbor	显示 IPv6 邻居缓存信息。

ipv6 ospf

要启用 IPv6 的 OSPFv3 接口配置，请在 **ipv6ospf**全局配置模式下使用该命令。要禁用用于 IPv6 的 OSPFv3 接口配置，请使用此命令的 **no** 形式。

ipv6
ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]
no ipv6
ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

Syntax Description

cost	显式指定在接口上发送数据包的成本。
database-filter	过滤发往 OSPFv3 接口的传出 LSA。
dead-interval秒	设置在邻居指示路由器已关闭之前不得看到 hello 数据包的时间段（以秒为单位）。该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。默认值是命令设置的间隔的 **ipv6ospfhello-interval**四倍。
flood-reduction	指定到接口的 LSA 泛洪减少量。
hello-interval秒	指定接口上发送 hello 数据包之间的间隔（以秒为单位）。该值必须对于特定网络上的所有节点都相同，并且范围可以是 1 至 65535。默认间隔对于以太网接口为 10 秒，对于非广播接口为 30 秒。
mtu-ignore	收到 DBD 数据包时禁用 OSPF MTU 不匹配检测。默认情况下，OSPF MTU 不匹配检测已启用。
neighbor	配置 OSPFv3 路由器与非广播网络的互连。
network	将 OSPF 网络类型设置为默认类型以外的类型，这取决于网络类型。
priority	设置路由器优先级，帮助确定网络的指定路由器。有效值范围为 0 到 255。
process-id	指定要启用的 OSPFv3 进程。有效值范围为 1 到 65535。
retransmit-interval 秒	指定属于该接口的邻接关系的 LSA 重新传输之间的时间（以秒为单位）。该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。
transmit-delay秒	设置在接口上发送链路状态更新数据包的预计时间（以秒为单位）。有效值的范围为 1 到 65535 秒。默认值为 1 秒。

Command Default

默认情况下，包含所有 IPv6 地址。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

您必须先启用 OSPFv3 路由进程，然后才能创建 OSPFv3 区域。

CR_Examples

以下示例启用 OSPFv3 接口配置：

```
ciscoasa(config)# ipv6 ospf 3
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf area

要为 IPv6 创建 OSPFv3 区域，请在全局配置模式下使用 **ipv6ospfarea** 命令。要禁用 IPv6 的 OSPFv3 区域配置，请使用此命令的 **no** 形式。

ipv6 ospf area [*area-num*] [**instance**]
no ipv6 ospf area [*area-num*] [**instance**]

Syntax Description

area-num	指定要启用的 OSPFv3 区域。
instance	指定要分配给接口的区域实例 ID。

Command Default

默认情况下，包含所有 IPv6 地址。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

您必须在每个接口上单独配置 OSPFv3 路由。接口只能有一个 OSPFv3 区域，并且 ASA 的 OSPFv3 仅支持每个接口一个实例。每个接口使用不同的区域实例 ID。区域实例 ID 仅影响 OSPF 数据包的接收，并适用于普通 OSPF 接口和虚拟链路。

CR_Examples

以下示例启用 OSPFv3 接口配置：

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf cost

要明确指定在接口上发送数据包的开销，请在接口配置模式下使用**ipv6ospfcost**命令。要将接口上发送数据包的成本重置为默认值，请使用此命令的 **no**形式。

ipv6 ospf cost*interface-cost*
no ipv6 ospf cost*interface-cost*

Syntax Description

interface-cost	指定表示链路状态度量的无符号整数值，范围从 1 到 65535。

Command Default

默认开销基于带宽。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可明确指定接口的数据包开销。

CR_Examples

以下示例将数据包开销设置为 65：

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf database-filter all out

要过滤发往 OSPFv3 接口的传出 LSA，请在 **ipv6ospfdatabse-filterallout** 接口配置模式下使用该命令。要恢复将 LSA 转发到接口，请使用此命令的 **no** 形式。

ipv6 ospf database-filter all out
no ipv6 ospf database-filter all out

Syntax Description

此命令没有任何参数或关键字。

Command Default

所有传出的 LSA 均会泛洪至该接口。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可以过滤发往 OSPFv3 接口的传出 LSA。

CR_Examples

以下示例将筛选到指定接口的传出 LSA：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf dead-interval

要设置在邻居声明路由器已关闭之前不得看到 hello 数据包的时间段，请在 **ipv6ospfdead-interval** 接口配置模式下使用该命令。要返回默认时间，请使用此命 **no**令的形式。

ipv6 ospf dead-interval秒
no ipv6 ospf dead-interval秒

Syntax Description

秒指定间隔（以秒为单位）。网络中的所有节点的值必须相同。有效值范围为 1 到 65535。

Command Default

默认值是命令设置的间隔的 **ipv6ospfhello-interval**四倍。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可指定在邻居通知路由器关闭之前，看不到呼叫数据包的时间间隔。

CR_Examples

以下示例将 dead 间隔设置为 60：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf encryption

要指定接口的加密类型，请在 **ipv6ospfencryption** 接口配置模式下使用该命令。要删除接口的加密类型，请使用此命令的 **no**形式。

ipv6 ospf
encryption{**ipsecspi***spi***esp***encryption-algorithm*[[*key-encryption-type*]*key*]*authentication-algorithm*[*key-encryption-type*]*key*|**null**}
no ipv6 ospf
encryption{**ipsecspi***spi***esp***encryption-algorithm*[[*key-encryption-type*]*key*]*authentication-algorithm*[*key-encryption-type*]*key*|**null**}

Syntax Description

authentication-algorithm	指定要使用的加密算法。有效值为以下值之一： • —**md5**启用消息摘要 5 (MD5)。 • —**sha1**启用 SHA-1。
加密算法-	指定与 ESP 一起使用的加密算法。。有效值包括以下值： • —**aes-cdc**启用 AES-CDC 加密。 • —**3des**启用 3DES 加密。 • —启**des**用 DES 加密。 • —**null**指定不加密的 ESP。
esp	指定封装安全有效载荷 (ESP)。
ipsec	指定 IP 安全协议。
key	指定在计算消息摘要时使用的数字。使用 MD5 身份验证时，密钥长度必须为 32 位十六进制数字（16 字节）。使用 SHA-1 身份验证时，密钥长度必须为 40 位十六进制数字（20 字节）。
key-encryption-type	（可选）指定密钥加密类型，可以是以下值之一： • **0**- 密钥未加密。 • —**7**密钥已加密。
null	覆盖区域身份验证。
spi*spi*	指定 安全策略索引 (SPI) 值。 *spi* 值必须为 256 到 4294967295 之间的数字，且须以十进制形式输入。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令指定接口的加密类型。

CR_Examples

以下示例在接口上启用 SHA-1 加密：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf flood-reduction

要指定到接口的 LSA 泛洪减少，请在接口配置模式下使用该 **ipv6ospfflood-reduction**命令。要取消对接口的 LSA 泛洪减少，请使用此命令的 **no**形式。

ipv6 ospf flood-reduction
no ipv6 ospf flood-reduction

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令指定到接口的 LSA 泛洪减少。

CR_Examples

以下示例启用减少到接口的 LSA 泛洪：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200vlan 200 nameif outside security-level
 100 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31  ipv6 address 3001::1/64
standby 3001::8 ipv6 address 6001::1/64 standby 6001::8 ipv6 enable ospf priority 255 ipv6
 ospf cost 100 ipv6 ospf 100 area 10 instance 200 ipv6 ospf flood reduction
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf hello-interval

要设置在邻居声明路由器已关闭之前不得看到 hello 数据包的时间段，请在 **ipv6ospfdead-interval** 接口配置模式下使用该命令。要返回默认时间，请使用此命 **no**令的形式。

ipv6 ospf dead-interval秒
no ipv6 ospf dead-interval秒

Syntax Description

秒指定间隔（以秒为单位）。网络中的所有节点的值必须相同。有效值范围为 1 到 65535。

Command Default

如果使用的是以太网，则默认间隔为 10 秒；如果使用的是非广播，则默认间隔为 30 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可指定在邻居通知路由器关闭之前，看不到呼叫数据包的时间间隔。

CR_Examples

以下示例将 dead 间隔设置为 60：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf mtu-ignore

要在 ASA 接收数据库描述符 (DBD) 数据包时禁用 OSPFv3 最大传输单元 (MTU) 不匹配检测，请在接口配置模式下使用 **ipv6ospfmtu-ignore**命令。要在 ASA 接收 DBD 数据包时将 MTU 不匹配检测重置为默认值，请使用此命令的 **no** 形式。

ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，OSPFv3 MTU 不匹配检测处于启用状态。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可在 ASA 接收 DBD 数据包时禁用 OSPFv3 MTU 不匹配检测。

CR_Examples

以下示例在 ASA 接收 DBD 数据包时禁用 OSPFv3 MTU 不匹配检测：

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6 ospf neighbor

要配置与非广播网络的 OSPFv3 路由器互连，请在接口配置模式下使用 **ipv6ospfneighbor** 命令。当达到最大数量（由邻居最大前缀命令设置）时，条目中**no**会出现字符串“PfxRcd”，邻居被关闭，连接处于空闲状态。

ipv6 ospf neighbor*ipv6-address*[**priority***number*][**poll-interval**秒][**cost***number*][**database-filter**]
no ipv6 ospf neighbor*ipv6-address*[**priority***number*][**poll-interval**秒][**cost***number*][**database-filter**]

Syntax Description

cost编号	（可选）以 1 到 65535 之间的整数形式为邻居分配开销。未配置特定开销的邻居会根据 **ipv6ospfcost** 命令采用接口的开销。
database-filter	（可选）过滤到 OSPF 邻居的传出链路状态通告 (LSA)。
ipv6-address	邻居的链路本地 IPv6 地址。此参数必须采用 RFC 2373 中记录的形式，其中地址以冒号之间的 16 位值以十六进制格式指定。
poll-interval 秒	（可选）表示轮询间隔时间（以秒为单位）的数字值。RFC 2328 建议将此值远大于呼叫间隔。默认值为 120 秒（两分钟）。此关键字不适用于点对多点接口。
priority编号	（可选）一个数字，表示与指定 IPv6 前缀关联的非广播邻居的路由器优先级值。默认值为 0。

Command Default

默认值取决于网络类型。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	•	•		—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令配置 OSPFv3 路由器与非广播网络的互连。

CR_Examples

以下示例配置 OSPFv3 邻居路由器：

```
ciscoasa(config)# interface serial 0
```

```
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6 ospf network

要将 OSPFv3 网络类型配置为默认类型以外的其他类型，请在接口配置模式下使用 **ipv6ospfnetwork** 命令。要返回默认类型，请使用此命 **no**令的形式。

ipv6 ospf network {**broadcast** | **point-to-pointnon-broadcast**}
no ipv6 ospf network {**broadcast** | **point-to-pointnon-broadcast**}

Syntax Description

广播	将网络类型设置为广播。
point-to-pointnon-broadcast	将网络类型设置为点对点非广播。

Command Default

默认值取决于网络类型。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可将 OSPFv3 网络类型配置为不同于默认值的类型。

CR_Examples

以下示例将 OSPFv3 网络设置为广播网络：

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6 ospf priority

要设置路由器优先级（这有助于为指定网络确定指定路由器），请在接口配置模式下使用**ipv6ospfpriority**命令。要返回默认值，请使用此**no**命令形式。

ipv6 ospf priority*number-value*
no ipv6 ospf priority*number-value*

Syntax Description

number-value	设置用于指定路由器优先级的数字值。有效值范围为0到255。

Command Default

默认优先级为 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可设置路由器的优先级。

CR_Examples

以下示例将路由器的优先级设置为 4：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfretransmit-interval	指定属于该接口的邻接关系的LSA 重新传输之间的时间。

ipv6 ospf retransmit-interval

要指定属于该接口的邻接关系的 LSA 重新传输之间的时间，请在 **ipv6ospfretransmit-interval** 接口配置模式下使用该命令。要返回默认值，请使用此**no**命令形式。

ipv6 ospf retransmit-interval秒
no ipv6 ospf retransmit-interval秒

Syntax Description

秒指定两次重新传输的间隔时间（以秒为单位）。该间隔必须大于所连接网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。

Command Default

默认值为 5 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令可以指定属于该接口的邻接关系的 LSA 重新传输之间的时间。

CR_Examples

以下示例将重新传输间隔设置为 8 秒：

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

Related Commands

命令	说明
ipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6 ospf transmit-delay

如要设置在接口上发送链路状态更新数据包所需的估计时间，请在接口配置模式下使用**ipv6ospftransmit-delay**命令。要返回默认值，请使用此**no**命令形式。

ipv6 ospf transmit-delay秒
no ipv6 ospf transmit-delay秒

Syntax Description

秒指定发送链路状态更新所需的时间（以秒为单位）。有效值的范围为 1 到 65535 秒。

Command Default

默认值为 1 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

使用此命令设置在接口上发送链路状态更新数据包所需的估计时间。

CR_Examples

以下示例将传输延迟设置为 3 秒：

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
ipv6ospfpriority	确定指定网络的指定路由器。

ipv6-prefix

要为映射地址和端口 (MAP) 域中的基本映射规则配置 IPv6 前缀，请在 MAP 域基本映射规则配置模式下使用 **ipv6-prefix** 命令。使用此命 **no**令的形式来删除前缀。

ipv6-prefix*ipv6_prefix/prefix_length*
no ipv6-prefix*ipv6_prefix/prefix_length*

Syntax Description

ipv6_prefix/prefix_length	IPv6 前缀定义客户边缘 (CE) 设备的 IPv6 地址的地址池。指定 IPv6 前缀和前缀长度，通常为 64，但不能小于 8。不能在不同 MAP 域中使用相同的 IPv6 前缀。

Command Default

无默认值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
MAP域基本映射规则配置模式	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.13(1)	引入了此命令。

使用指南

IPv6 前缀定义 CE 设备 IPv6 地址的地址池。只有当数据包的目标地址具有该前缀，源地址具有默认映射规则中定义的 IPv6 前缀，且在正确的端口范围内时，MAP 才会将 IPv6 数据包翻译回 IPv4。任何从其他地址发送到 CE 设备的 IPv6 数据包都会被简单地作为 IPv6 流量处理，而不会进行 MAP 转换。来自 MAP 源/目的池但端口超出范围的数据包会被直接丢弃。

CR_Examples

以下示例创建一个名为 1 的 MAP-T 域，并为该域配置转换规则。

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
```

```
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

命令	说明
basic-mapping-rule	配置 MAP 域的基本映射规则。
default-mapping-rule	配置 MAP 域的默认映射规则。
ipv4-prefix	为 MAP 域中的基本映射规则配置 IPv4 前缀。
ipv6-prefix	为 MAP 域中的基本映射规则配置 IPv6 前缀。
map-domain	配置映射地址和端口 (MAP) 域。
share-ratio	在 MAP 域中配置基本映射规则中的端口数。
showmap-domain	显示有关映射地址和端口 (MAP) 域的信息。
start-port	配置 MAP 域中基本映射规则的起始端口。

ipv6 prefix-list

要在 IPv6 前缀列表中创建条目，请在全局配置模式下使用 **ipv6prefix-list** 命令。要删除条目，请使用此命 **no**令的形式。

ipv6
prefix-list*list-name* [**seq***seq-number*] {**deny***ipv6-prefix* | *prefix-length* | **description***text*} [**ge***ge-value*] [**le***le-value*]
no ipv6 prefix-list*list-name*

Syntax Description

list-name	前缀列表的名称。 名称不能与现有访问列表相同。 注释 名称不能为“detail”或“summary”，因为它们是关键字。
seq*seq-number*	（可选）正在配置的前缀列表条目的序列号。
deny	拒绝符合条件的网络。
permit	允许符合条件的网络。
ipv6-prefix	向指定前缀列表分配的 IPv6 网络。 此参数必须采用 RFC 2373 中记录的形式，其中地址是用冒号分隔的十六进制 16 位值。
prefix-length	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。
description 文本、	前缀列表的说明，最长可以为 80 个字符。
ge*ge-value*	（可选）指定前缀长度大于或等于 *ipv6-prefix*/*prefix-length* 参数。它是长度范围（长度范围的“起始”部分）的最小值。
le*le-value*	（可选）指定小于或等于 *ipv6-prefix*/*prefix-length* 参数的前缀长度。它是一个长度范围（长度范围的“至”部分）的最大值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.3(2)	添加了此命令。

Related Commands

命令	说明
showipv6prefix-list	显示 IPv6 前缀列表。
showipv6route	显示 IPv6 路由表的当前内容。

ipv6 route

要将 IPv6 路由添加到 IPv6 路由表，请在 **ipv6route**全局配置模式下使用该命令。要删除 IPv6 默认路由，请使用此命 **no**令的形式。

ipv6 route*if_nameipv6-prefix* | *prefix-lengthipv6-address* [*management-distance* | **tunneled**]
no ipv6 route*if_nameipv6-prefix* | *prefix-lengthipv6-address* [*management-distance* | **tunneled**]

Syntax Description

administrative-distance	（可选）路由的管理距离。默认值为 1，这表示静态路由优先于任何其他类型的路由（连接路由除外）。
if_name	正在为其配置路由的接口的名称。
ipv6-address	可用于到达指定网络的下一跳的 IPv6 地址。
ipv6-prefix	作为静态路由目的地的 IPv6 网络。 此参数必须采用 RFC 2373 中记录的形式，其中地址以冒号之间的 16 位值以十六进制格式指定。
prefix-length	IPv6 前缀的长度。此值表示组成前缀网络部分的地址高位、连续位的数量。斜线 (/) 必须在前缀长度前。
tunneled	（可选）将路由指定为 VPN 流量的默认隧道网关。

Command Default

默认情况下，管理距离为 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.2(1)	添加了对透明防火墙模式的支持。

使用指南

使用命令查看IPv6 **showipv6route**路由表的内容。

您可以为隧道流量定义单独的默认路由以及标准默认路由。当您使用该 **tunneled**选项创建默认路由时，来自终止于ASA的隧道且无法使用学习或静态路由进行路由的所有流量都将发送到此路由。对于从隧道传出的流量，此路由将覆盖任何其他已配置或学习到的默认路由。

以下限制适用于带 **tunneled**选项的默认路由：

- 不要在隧道路由的出口接口上启用单播 RPF（**ipverifyreverse-path** 命令）。在隧道路由的传出接口上启用 uRPF 会导致会话失败。
- 不要在隧道路由的出口接口上启用 TCP 拦截。这样做会导致会话失败。
- 请勿使用 VoIP 检查引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP 或 SKINNY）、DNS 检查引擎或带有隧道路由的 DCE RPC 检查引擎。这些检测引擎会忽略隧道路由。

您不能使用该选项定义多个默认路由；不支持隧道流量的 **tunneled**ECMP。

CR_Examples

以下示例将网络 7fff::0/32 的数据包路由到位于 3FFE:1100:0:CC00::1 上的内部接口上的网络设备，管理距离为 110：

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

Related Commands

命令	说明
debugipv6route	显示IPv6路由表更新和路由缓存更新的调试消息。
showipv6route	显示 IPv6 路由表的当前内容。

ipv6 router ospf

要创建 OSPFv3 路由进程并进入 IPv6 路由器配置模式，请在 **ipv6routerospf** 全局配置模式下使用该命令。

ipv6 router ospf*process-id*

Syntax Description

process-id	指定内部标识，该标识是本地分配的，可以是 1 到 65535 之间的正整数。使用的号码是当您为 IPv6 路由进程启用 OSPFv3 时管理分配的号码。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

ipv6routerospf命令是用于在 ASA 上运行的 OSPFv3 路由进程的全局配置命令。输入 **ipv6routerospf** 命令后，命令提示符显示为 (config-rtr)#，表示您处于 IPv6 路由器配置模式。

使用 **noipv6routerospf**命令时，除非可选参数提供必要的信息，否则无需指定可选参数。**noipv6routerospf**命令终止由其 *process-id* 参数指定的 OSPFv3 路由进程。在 ASA 上本地分配 *process-id* 值。必须为每个 OSPFv3 路由进程分配唯一值。您最多可以使用两个进程。

在 IPv6 路由器配置模式下，使用 **ipv6routerospf** 命令，通过以下特定于 OSPFv3 的选项配置 OSPFv3 路由进程：

- —配**area**置 OSPFv3 区域参数。支持的参数包括从 0 到 4294967295 的十进制值区域 ID 和 的 IP 地址格式的区域 ID。 **A.B.C.D**
- —**default**将命令设置为其默认值。该 **originate**参数分发默认路由。
- —**default-information**控制默认信息的分发。
- —**distance**根据路由类型定义 OSPFv3 路由管理距离。支持的参数包括管理距离（值从 1 到 254）和 **ospf**OSPF 距离。

- 退出**exit**—IPv6 路由器配置模式。
- **lsa**— **ignore**当路由器接收到第 6 类多播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，抑制发送带有该参数的系统日志消息。
- —**log-adjacency-changes**配置路由器在 OSPFv3 邻居启动或关闭时发送系统日志消息。通过该**detail**参数，所有状态变化都会被记录下来。
- **passive-interface**- 使用以下参数抑制接口上的路由更新：
  - **GigabitEthernet**- 指定千兆以太网 IEEE 802.3z 接口。
  - —**Management**指定管理接口。
  - **Port-channel**- 指定接口的以太网通道。
  - —**Redundant**指定冗余接口。
  - —**default**抑制所有接口上的路由更新。
- —**redistribute**根据以下参数配置从一个路由域到另一个路由域的路由重新分配：
  - —**connected**指定连接的路线。
  - —**ospf**指定 OSPF 路由。
  - —指**static**定静态路由。
- —**router-id**使用以下参数为指定进程创建固定路由器 ID：
  - —**A.B.C.D**以 IP 地址格式指定 OSPF 路由器 ID。
  - —**cluster-pool**配置第 3 层集群时配置 IP 地址池。
- —**summary-prefix**配置 IPv6 地址摘要，有效值为 0 至 128。该 **X:X:X:X::X/**参数指定 IPv6 前缀。
- **timers**—使用以下参数调整路由计时器：
  - —指**lsa**定 OSPF LSA 计时器。
  - —**pacing**指定 OSPF 定步计时器。
  - —**throttle**指定 OSPF 节流计时器。

CR_Examples

以下示例启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式：

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

Related Commands

命令	说明
clearipv6ospf	删除 OSPFv3 路由进程中的所有 IPv6 设置。
debugospfv3	为 OSPFv3 路由进程故障排除提供调试信息。

ipv6-split-tunnel-policy

要设置 IPv6 分割隧道策略，请在 group-policy 配置模式下使用 **ipv6-split-tunnel-policy**命令。要从运行配置中删除 ipv6-split-tunnel-policy 属性，请使用此命令的 **no**形式。

ipv6-split-tunnel-policy { **tunnelall** | **tunnelspecified** | **excludespecified** }
no ipv6-split-tunnel-policy

Syntax Description

excludespecified	定义流量明文传输到的网络列表。对于想要访问本地网络上的设备（如打印机），而通过隧道连接到公司网络的用户来说，此功能非常有用。
ipv6-split-tunnel-policy	表示正在设置隧道流量规则。
tunnelall	指定流量不会被明文传送或流向 ASA 以外的任何其他目标。远程用户通过公司网络访问互联网，没有访问本地网络的权限。
tunnelspecified	通过隧道传送进出指定网络的所有流量。此选项可启用分割隧道。它允许您创建要通过隧道传送的地址的网络列表。发往所有其他地址的数据均以明文形式传输，并由远程用户的互联网服务提供商进行路由。

Command Default

IPv6 分割隧道默认为禁用状态，即 **tunnelall**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

IPv6 分割隧道主要是一种流量管理功能，而不是安全功能。事实上，为了获得最佳安全性，我们建议您不要启用 IPv6 拆分隧道。

这使得可以从另一个组策略继承 IPv6 分割隧道的值。

IPv6 分割隧道允许远程访问 VPN 客户端有条件地以加密形式将数据包定向到 IPsec 或 SSL IPv6 隧道，或者以明文形式定向到网络接口。启用 IPv6 分割隧道后，未绑定到 IPsec 或 SSL VPN 隧道终端另一端的目标的数据包不必加密，通过隧道发送，解密，然后路由到最终目标。

此命令将 IPv6 分割隧道策略应用于特定网络。

CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略设置仅为指定网络建立隧道的拆分隧道策略：

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-split-tunnel-policy tunnelspecified
```

Related Commands

命令	说明
split-tunnel-network-listnone	表示分割隧道不存在访问列表。所有流量都通过隧道传输。
split-tunnel-network-listvalue	标识 ASA 用于区分需要建立隧道和不需要建立隧道的网络的访问列表。

ipv6-vpn-address-assign

要指定向远程访问客户端分配 IPv6 地址的方法，请在 **ipv6-vpn-addr-assign**全局配置模式下使用该命令。要从配置中删除该属性，请使用此命令的 **no**版本。要从 ASA 中删除所有已配置的 VPN 地址分配方法，请使用此命令的 **no**版本。不带参数。

ipv6-vpn-addr-assign { **aaa** | **local** }
no ipv6-vpn-addr-assign { **aaa** | **local** }

Syntax Description

aaa	ASA 根据每个用户从外部或内部（本地）AAA（身份验证、授权和记帐）服务器检索地址。如果使用已配置 IP 地址的身份验证服务器，建议使用此方法。
local	ASA 会从内部配置的地址池中分配 IPv6 地址。

Command Default

默认情况下，会启用 AAA 和本地 VPN 地址分配选项。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.0(1)	添加了此命令。
9.5(2)	增加了多情景模式支持。

使用指南

ASA 可以使用 AAA 或本地方法为远程访问客户端分配 IPv6 地址。如果配置多个地址分配方法，ASA 将搜索每个选项，直到找到 IPv6 地址。

CR_Examples

以下示例显示如何配置 AAA 作为地址分配方法。

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

以下示例显示如何配置使用本地地址池作为地址分配方法。

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

Related Commands

命令	说明
ipv6localpool	配置要用于 VPN 组策略的 IPv6 地址池。
show running-config group-policy	显示所有组策略或特定组策略的配置。
vpn-addr-assign	指定为远程访问客户端分配 IPv4 地址的方法。

ipv6-vpn-filter

要指定用于 VPN 连接的 IPv6 ACL 的名称，请在 **ipv6-vpn-filter**策略组配置或用户名配置模式下使用该命令。要删除 ACL（包括通过发出命令创建的 **ipv6-vpn-filternone**空值），请使用此命令的 **no**形式。

ipv6-vpn-filter { **value***IPV6 ACL* 名称 | **none** }
no ipv6-vpn-filter

Syntax Description

none	指示没有访问列表。设置一个空值，从而禁止访问列表。防止从其他组策略继承访问列表。
value*IPV6 ACL* 名称	提供先前配置的访问列表的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略配置	• 是	—	• 是	—	—
用户名配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.0(1)	该 **ipv6-vpn-filter**命令已被弃用。使用 **vpn-filter** 命令来配置具有 IPv4 和 IPv6 条目的统一过滤器。仅当 **vpn-filter** 命令指定的访问列表中没有 IPv6 条目时，才会使用此 IPv6 过滤器。
9.1(4)	**ipv6-vpn-filter** 命令已禁用，仅允许使用该命令的“no”形式。使用 **vpn-filter** 命令为 IPv4 和 IPv6 条目配置统一过滤器。如果错误地使用此命令指定 IPv6 ACL，则连接将终止。

使用指南

无客户端 SSL VPN 不使用命令中定义的 **ipv6-vpn-filter**ACL。

no 选项允许从其他组策略继承值。为了防止继承值，请使 **ipv6-vpn-filternone**用命令。

您配置 ACL 来为此用户或组策略允许或拒绝各种类型的流量。然后，使用 **ipv6-vpn-filter** 命令以应用这些 ACL。

CR_Examples

以下示例显示如何设置一个过滤器，该过滤器为名为 FirstGroup 的组策略调用名为 ipv6_acl_vpn 的访问列表：

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-vpn-filter value ipv6_acl_vpn
```

Related Commands

命令	说明
access-list	创建访问列表，或使用可下载访问列表。
vpn-filter	指定要用于 VPN 连接的 IPv4 或 IPv6 ACL 的名称。

ip verify reverse-path

要启用单播 RPF，请在 **ipverifyreverse-path**全局配置模式下使用该命令。要禁用此功能，请使用此 **no**命令的形式。

ip verify reverse-path interface*interface_name*
no ip verify reverse-path interface*interface_name*

Syntax Description

interface_name	要在其上启用单播RPF的接口。

Command Default

默认情况下会禁用此功能。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

单播RPF根据路由表来确保所有数据包均有与正确的源接口匹配的源IP地址，从而避免IP欺骗（即数据包使用不正确的源 IP 地址以掩盖其真正来源）。

通常，ASA 在确定将数据包转发到何处时仅查看目标地址。单播 RPF 指示 ASA 也查看源地址；这就是它被称为反向路径转发的原因。对于您想要允许通过 ASA 的任何流量，ASA 路由表必须包含返回源地址的路由。有关详细信息，请参阅 RFC 2267。

例如，对于外部流量，ASA可以使用默认路由来满足单播RPF保护。如果流量从外部接口进入，并且路由表不知道源地址，则 ASA 使用默认路由将外部接口正确识别为源接口。

如果流量从路由表已知但与内部接口关联的地址进入外部接口，则ASA会丢弃该数据包。类似地，如果流量从未知源地址进入内部接口，ASA 会丢弃该数据包，因为匹配的路由（默认路由）指示的是外部接口。

单播 RPF 的实施过程如下：

- ICMP 数据包没有会话，因此要检查每个数据包。

- UDP 和 TCP 有会话，因此初始数据包要求反向路由查找。对于在会话期间到达的后续数据包，使用作为部分会话来维护的现有状态进行检查。检查非初始数据包以确保它们到达初始数据包使用的同一接口。

CR_Examples

以下示例在外部接口上启用单播 RPF：

```
ciscoasa(config)# ip verify reverse-path interface outside
```

Related Commands

命令	说明
clearconfigureipverifyreverse-path	使用命令清除配置 **ipverifyreverse-path**集。
clearipverifystatistics	清除单播 RPF 统计信息。
showipverifystatistics	显示单播 RPF 统计数据。
showrunning-configipverifyreverse-path	显示使用该命令设置的 **ipverifyreverse-path**配置。

ipv6 未编号

要从接口（例如，环回接口）借用或继承 IPv6 地址，请在接口配置模式下使用 **ipv6unnumbered** 命令。要停止从接口继承 IP 地址，请使用此命令的 **no**形式。

ipv6unnumbered *interface-name*
no ipv6 unnumbered

Syntax Description

interface-name	指定要继承 IPv6 地址的接口的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.19(1)	添加了此命令。

使用指南

`ipv6 unnumbered` 命令用于继承所选 `接口` 的 IPv6 地址，作为当前接口的地址。

CR_Examples

以下示例从环回接口借用 IPv6 地址，并将其用于 VTI 隧道接口：

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ipv6 unnumbered loopback1
```

Related Commands

命令	说明
ipunnumbered*interface-name*	继承指定接口的 IP 地址。
interfaceloopback*loopback-number*	创建环回接口。

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。