目 录

1 IP Source Guard配置

1.1 IP Source Guard简介

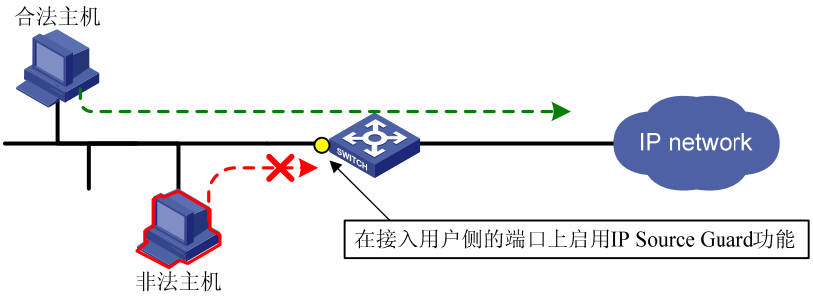
1.1.1 概述

通过在设备接入用户侧的端口上启用 IP Source Guard 功能，可以对端口收到的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了端口的安全性。

IP Source Guard 在端口上用于过滤报文的特征项包括：源 IP 地址、源 MAC 地址。这些特征项可单独或组合起来与端口进行绑定，形成绑定表项，具体包括：IP、MAC、IP＋MAC。

如 图 1-1 所示，配置了IP Source Guard的端口接收到报文后查找IP Source Guard绑定表项，如果报文中的特征项与绑定表项中记录的特征项匹配，则端口转发该报文，否则做丢弃处理。绑定功能是针对端口的，一个端口配置了绑定功能后，仅该端口被限制，其他端口不受该绑定影响。

图1-1 IP Source Guard 功能示意图



1.1.2 静态绑定表项

通过手工配置产生绑定表项来完成端口的控制功能，适用于局域网络中主机数较少且主机使用静态配置 IP 地址的情况，比如在接入某重要服务器的端口上配置绑定表项，仅允许该端口接收或者发送与该服务器通信的报文。

- IPv4 静态表项：使用手工配置的 IPv4 静态绑定表项来过滤端口收到的 IPv4 报文，或者与 ARP Detection 功能配合使用检查接入用户的合法性；
- IPv6 静态表项：使用手工配置的 IPv6 静态绑定表项来过滤端口收到的 IPv6 报文，或者与 ND Detection 功能配合使用检查接入用户的合法性。

说明

- ARP Detection 功能的详细介绍请参考“安全配置指导”中的“ARP 攻击防御”。
- ND Detection 功能的详细介绍请参考“安全配置指导”中的“ND 攻击防御”。

静态绑定表项又包括全局静态绑定表项和端口静态绑定表项两种类型，这两种绑定表项的作用范围不同。

1. 全局静态绑定表项

全局静态绑定表项是在系统视图下配置的绑定了 IP 地址和 MAC 地址的表项，这类表项在设备的所有端口上生效，允许端口正常转发 IP 地址和 MAC 地址均与全局静态绑定表项匹配的报文，其它报文是否可以被正常转发由端口上配置的静态绑定表项来决定。全局静态绑定表项适用于防御主机仿冒攻击，可有效过滤攻击者通过仿冒合法用户主机的 IP 地址或者 MAC 地址向设备发送的伪造 IP 报文。

2. 端口静态绑定表项

端口静态绑定是在端口上配置的绑定了 IP 地址、MAC 地址以及相关组合的表项，这类表项仅在当前端口上生效。只有端口收到的报文的 IP 地址、MAC 地址与端口上配置的绑定表项的各参数完全匹配时，报文才可以在该端口被正常转发，其它报文都不能被转发，该表项适用于检查端口上接入用户的合法性。

1.1.3 动态绑定表项

根据 DHCP 的相关表项动态生成绑定表项来完成端口控制功能，通常适用于局域网络中主机较多，并且采用 DHCP 进行动态主机配置的情况。其原理是每当 DHCP 为用户分配 IP 地址而生成一条 DHCP 表项时，端口绑定功能就相应地增加一条绑定表项以允许该用户访问网络。如果某个用户私自设置 IP 地址，则不会触发设备生成相应的 DHCP 表项，因此端口绑定功能也不会增加相应的访问规则来允许该用户访问网络。除此之外，IPv6 类型的动态绑定还支持自动获取 ND Snooping 表项。

- IPv4 动态绑定：根据 DHCP Snooping 表项或 DHCP Relay 表项动态生成绑定表项来过滤端口收到的 IPv4 报文；
- IPv6 动态绑定：根据 DHCPv6 Snooping 表项或 ND Snooping 表项动态生成绑定表项来过滤端口收到的 IPv6 报文。

说明

- DHCP Snooping 和 DHCP Relay 功能的详细介绍请参考“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- DHCPv6 Snooping 功能的详细介绍请参考“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。
- ND Snooping 功能的详细介绍请参考“三层技术-IP 业务配置指导”中的“IPv6 基础”。

1.2 配置IPv4绑定功能

说明

加入聚合组或加入业务环回组的端口上不能配置 IP Source Guard 功能，反之亦然。

1.2.1 配置IPv4 端口绑定功能

配置了 IPv4 端口绑定功能的端口，可利用配置的 IPv4 静态绑定表项和从 DHCP 模块获取的 IPv4 动态绑定表项对端口转发的报文进行过滤：

- IPv4 静态绑定表项的配置请参考“1.2.2 配置IPv4 静态绑定表项”。

- 在二层以太网端口上，IP Source Guard 可与 DHCP Snooping 配合，通过获取 IP 地址动态分配时产生的 DHCP Snooping 表项来生成动态绑定表项；
- 在 VLAN 接口上，IP Source Guard 可与 DHCP Relay 配合，通过获取 IP 地址跨网段动态分配时产生的 DHCP Relay 表项来生成动态绑定表项。

动态绑定表项中可能包含的内容有：MAC 地址、IP 地址、VLAN 信息、入端口信息及表项类型（DHCP Snooping 或 DHCP Relay），其中 MAC 地址、IP 地址和 VLAN 信息的包含情况由动态绑定配置决定。IP Source Guard 把这些动态绑定表项下发到端口后，可对端口上转发的报文进行过滤。

表1-1 配置 IPv4 端口绑定功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv4端口绑定功能	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	必选 缺省情况下，端口上未配置IPv4端口绑定功能

说明

- IPv4 端口绑定功能中所指的“接口”可以为二层以太网端口、VLAN 接口或端口组。
- 接口下的 IPv4 端口绑定功能可多次配置，最后一次的配置生效。
- 若要通过获取 DHCP 相关表项来生成动态绑定表项，请保证网络中的 DHCP Snooping 或 DHCP Relay 配置有效且工作正常，DHCP Snooping 配置的具体介绍请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”，DHCP Relay 配置的具体介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- 虽然 IP Source Guard 的动态表项是通过获取 DHCP 的相关表项而生成，但生成的 IP Source Guard 动态绑定表项数目并不与对应的 DHCP 表项数目保持一致，实际使用过程中，请以 IP Source Guard 实际生成的表项数目为准。

1.2.2 配置IPv4 静态绑定表项

IPv4 静态绑定表项包括全局IPv4 静态绑定表项和端口IPv4 静态绑定表项。IPv4 静态绑定表项只能在配置了IPv4 端口绑定功能的端口上生效，端口绑定功能的具体配置请参见“1.2.1 配置IPv4 端口绑定功能”。

静态绑定表项与端口绑定功能配合使用时，端口静态绑定表项和动态绑定表项的优先级高于全局静态绑定表项，即端口优先使用端口上的静态或动态绑定表项对收到的报文进行匹配，若匹配失败，再与全局静态绑定表项进行匹配。

1. 配置全局IPv4 静态绑定表项

全局静态绑定表项中定义了端口允许转发的报文的 IP 地址和 MAC 地址，对所有端口都生效。

表1-2 配置全局 IPv4 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置全局IPv4静态绑定表项	**ip source binding ip-address** *ip-address* **mac-address** *mac-address*	必选 缺省情况下，无全局IPv4静态绑定表项

2. 配置端口IPv4 静态绑定表项

表1-3 配置端口 IPv4 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置端口的IPv4静态绑定表项	**ip source binding** { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	必选 缺省情况下，端口上无IPv4静态绑定表项

说明

- 一个表项不能在同一个端口上重复绑定，但可以在不同端口上绑定。
- 当 IPv4 静态绑定表项与 IP Source Guard 功能配合时，静态绑定表项中的 VLAN 参数不作为过滤报文的特征项，VLAN 参数指定与否，不影响 IP Source Guard 功能对报文的过滤结果。
- 在 IPv4 静态绑定表项与 ARP Detection 功能配合时，静态绑定表项中必须指定 VLAN 参数，且该 VLAN 为使能 ARP Detection 功能的 VLAN，否则 ARP 报文将无法通过 IPv4 静态绑定表项的检查。关于 ARP Detection 功能的相关配置请参见“安全配置指导”中的“ARP 攻击防御”。
- 配置静态表项时，如果系统中已经存在相同内容的动态表项，则新添加的静态表项将会覆盖已有的动态表项。

1.2.3 配置IPv4 绑定表项数目的最大值

IPv4 绑定表项数目的最大值用于限制端口上允许添加的 IPv4 静态绑定表项和 IPv4 动态绑定表项的数量总和。当端口上的 IPv4 绑定表项数目达到指定的最大值时，端口将不再允许添加新的 IPv4 绑定表项。

表1-4 配置 IPv4 绑定表项数目的最大值

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置IPv4绑定表项数目的最大值	**ip verify source max-entries** *number*	可选 缺省情况下，S5500-EI系列以太网交换机的端口上IPv4绑定表项的最大值为1500，S5500-SI系列以太网交换机端口上IPv4绑定表项的最大值为640

说明

如果要配置的 IPv4 绑定表项数目的最大值小于当前端口上已存在的 IPv4 绑定表项总数，则该最大值可以配置成功，且原有的表项不受影响，但端口将不再允许新增 IPv4 绑定表项，除非端口上的 IPv4 绑定表项数目减少到小于此最大值。

1.3 配置IPv6绑定功能

说明

加入聚合组或加入业务环回组的端口上不能配置 IP Source Guard 功能，反之亦然。

1.3.1 配置IPv6 端口绑定功能

配置了 IPv6 端口绑定功能的端口，利用配置的 IPv6 静态绑定表项和从 DHCP 模块或 ND 模块获取的 IPv6 动态绑定表项对端口转发的报文进行过滤：

- IPv6 静态绑定表项的配置请参考“1.3.2 配置IPv6 静态绑定表项”。
- 在二层以太网端口上，IP Source Guard 可与 DHCPv6 Snooping 配合，通过获取 IPv6 地址动态分配时产生的 DHCPv6 Snooping 表项来生成动态绑定表项。
- 在二层以太网端口上，IP Source Guard 可与 ND Snooping 配合，通过获取动态产生的 ND Snooping 表项来生成动态绑定表项。

动态绑定表项中可能包含的内容有：MAC 地址、IPv6 地址、VLAN 信息、入端口信息及表项类型（DHCPv6 Snooping 或 ND Snooping），其中 MAC 地址、IPv6 地址和 VLAN 信息的包含情况由端口绑定配置决定。IP Source Guard 把这些动态绑定表项下发到端口后，可对端口上转发的报文进行过滤。

表1-5 配置 IPv6 端口绑定功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口或端口组视图	**interface** *interface-type interface-number*	-
配置IPv6端口绑定功能	**ipv6 verify source** { **ipv6-address** | **ipv6-address mac-address** | **mac-address** }	必选 缺省情况下，端口上未配置IPv6端口绑定功能

说明

- 若要通过获取 DHCP 或 ND 相关表项来生成动态绑定表项，请保证网络中的 DHCPv6 Snooping 或 ND Snooping 配置有效且工作正常，配置的具体介绍请分别参见“三层技术-IP 业务配置指导”中的“DHCPv6”和“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- IPv6 端口绑定功能可多次配置，最后一次的配置生效。
- 若设备上同时配置了 ND Snooping 和 DHCPv6 Snooping，通常会首先生成 DHCPv6 Snooping 表项，因此 IP Source Guard 会使用先生成的 DHCPv6 Snooping 表项来过滤端口报文。
- 虽然 IP Source Guard 的动态表项是通过获取 DHCP 的相关表项而生成，但生成的 IP Source Guard 动态绑定表项数目并不与对应的 DHCP 表项数目保持一致，实际使用过程中，请以 IP Source Guard 实际生成的表项数目为准。

1.3.2 配置IPv6 静态绑定表项

IPv6 静态绑定功能包括全局IPv6 静态绑定功能和端口IPv6 静态绑定功能。IPv6 静态绑定表项只能在配置了IPv6 端口绑定功能的端口上生效，端口绑定功能的具体配置请参见“1.3.1 配置IPv6 端口绑定功能”。

IPv6 静态绑定表项与 IPv6 端口绑定功能配合使用时，端口 IPv6 静态绑定表项和 IPv6 动态绑定表项的优先级高于全局 IPv6 静态绑定表项，即端口优先使用端口上的 IPv6 静态或动态绑定表项对收到的报文进行匹配，若匹配失败，再与全局 IPv6 静态绑定表项进行匹配。

1. 配置全局IPv6 静态绑定表项

全局 IPv6 静态绑定表项中定义了端口允许转发的报文的 IP 地址和 MAC 地址，对所有端口都生效。

表1-6 配置全局 IPv6 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-
配置全局IPv6静态绑定表项	**ipv6 source binding ipv6-address** *ipv6-address* **mac-address** *mac-address*	必选 缺省情况下，无全局IPv6静态绑定表项

2. 配置端口IPv6 静态绑定表项

表1-7 配置端口 IPv6 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置端口的IPv6静态绑定表项	**ipv6 source binding** { **ipv6-address** *ipv6-address* | **ipv6-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	必选 缺省情况下，端口上无IPv6静态绑定表项

说明

- 同一个表项不能在同一个端口上重复绑定，但可以在不同端口上绑定。
- 绑定表项中的 MAC 地址不能为全 0、全 F（广播 MAC）和组播 MAC。绑定表项中的 IPv6 地址必须为单播地址，不能为全 0 地址、组播地址、环回地址。
- 当 IPv6 静态绑定表项与 IP Source Guard 功能配合时，静态绑定表项中的 VLAN 参数不作为过滤报文的特征项，VLAN 参数指定与否，不影响 IP Source Guard 功能对报文的过滤结果。
- 在与 ND Detection 功能配合时，绑定表项中必须指定 VLAN 参数，且该 VLAN 为使能 ND Detection 功能的 VLAN，否则 ND 报文将无法通过 IPv6 静态绑定表项的检查。关于 ND Detection 功能的相关配置请参见“安全配置指导”中的“ND 攻击防御”。
- 配置静态表项时，如果系统中已经存在相同内容的动态表项，则新添加的静态表项将会覆盖已有的动态表项。

1.3.3 配置IPv6 绑定表项数目的最大值

IPv6 绑定表项数目的最大值用于限制端口上允许添加的 IPv6 静态绑定表项和 IPv6 动态绑定表项的数量总和。当端口上的 IPv6 绑定表项数目达到指定的最大值时，端口将不再允许添加新的 IPv6 绑定表项。

表1-8 配置 IPv6 绑定表项数目的最大值

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置IPv6绑定表项数目的最大值	**ipv6 verify source max-entries** *number*	可选 缺省情况下，S5500-EI系列以太网交换机的端口上IPv6绑定表项的最大值为1500，S5500-SI系列以太网交换机端口上IPv6绑定表项的最大值为640

说明

如果要配置的 IPv6 绑定表项数目的最大值小于当前端口上已存在的 IPv6 绑定表项总数，则该最大值可以配置成功，且原有的表项不受影响，但端口将不再允许新增 IPv6 绑定表项，除非端口上的 IPv6 绑定表项数目减少到小于最大值。

1.4 IP Source Guard显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IP Source Guard 的运行情况，通过查看显示信息验证配置的效果。

表1-9 IP Source Guard 显示和维护（IPv4）

操作	命令
显示静态绑定表项信息	**display ip source binding static** [**interface** *interface-type interface-number* | **ip-address** *ip-address* **| mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示绑定表项信息	**display ip source binding** [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

表1-10 IP Source Guard 显示和维护（IPv6）

操作	命令
显示IPv6静态绑定表项信息	**display ipv6 source binding static** [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* **| mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPv6绑定表项信息	**display ipv6 source binding** [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.5 IP Source Guard典型配置举例

1.5.1 IPv4 静态绑定表项配置举例

1. 组网需求

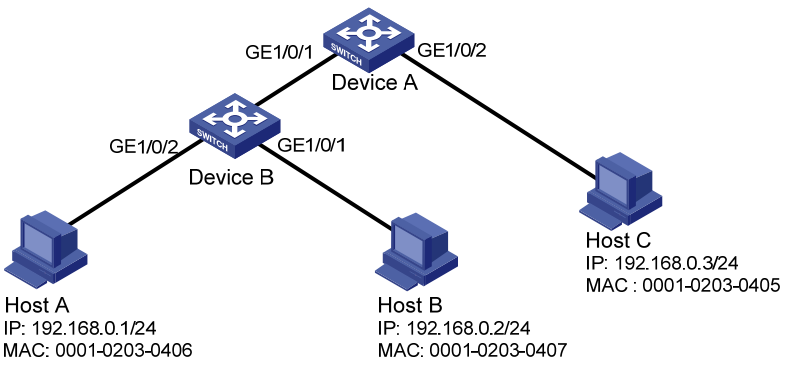
如 图 1-2 所示，Host A与Host B分别与Device B的端口GigabitEthernet1/0/2、GigabitEthernet1/0/1相连；Host C与Device A的端口GigabitEthernet1/0/2 相连。Device B接到Device A的端口GigabitEthernet1/0/1 上。各主机均使用静态配置的IP地址。

通过在 Device A 和 Device B 上配置 IPv4 静态绑定表项，可以满足以下各项应用需求：

- Device A 的端口 GigabitEthernet1/0/2 上只允许 Host C 发送的 IP 报文通过。
- Device A 的端口 GigabitEthernet1/0/1 上只允许 Host A 发送的 IP 报文通过。
- Device B 的端口 GigabitEthernet1/0/2 上只允许 Host A 发送的 IP 报文通过。
- Device B 的端口 GigabitEthernet1/0/1 上只允许使用 IP 地址 192.168.0.2/24 的主机发送的 IP 报文通过，即允许 Host B 更换网卡后仍然可以使用该 IP 地址与 Host A 互通。

2. 组网图

图1-2 配置静态绑定表项组网图



3. 配置步骤

(1) 配置 Device A

在端口 GigabitEthernet1/0/2 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0405、IP 地址为 192.168.0.3 的 Host C 发送的 IP 报文通过端口 GigabitEthernet1/0/2。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
[DeviceA-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/1 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的 Host A 发送的 IP 报文通过端口 GigabitEthernet1/0/1。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

在端口 GigabitEthernet1/0/2 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet1/0/2
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的 Host A 发送的 IP 报文通过端口 GigabitEthernet1/0/2。

```
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
[DeviceB-GigabitEthernet1/0/2] quit
```

在 GigabitEthernet1/0/1 上配置 IPv4 端口绑定功能，绑定源 IP 地址。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip verify source ip-address
```

配置 IPv4 静态绑定表项，只允许 IP 地址为 192.168.0.2 的主机发送的 IP 报文通过端口 GigabitEthernet1/0/1。

```
[DeviceB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2
[DeviceB-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

在 Device A 上显示 IPv4 静态绑定表项配置成功。

```
[DeviceA] display ip source binding static
Total entries found: 2
 MAC Address       IP Address       VLAN   Interface            Type
 0001-0203-0405    192.168.0.3      N/A    GE1/0/2              Static
 0001-0203-0406    192.168.0.1      N/A    GE1/0/1              Static
```

在 Device B 上显示 IPv4 静态绑定表项配置成功。

```
[DeviceB] display ip source binding static
Total entries found: 2
 MAC Address       IP Address       VLAN   Interface            Type
```

```
0001-0203-0406    192.168.0.1      N/A    GE1/0/2              Static
N/A               192.168.0.2      N/A    GE1/0/1              Static
```

1.5.2 与DHCP Snooping配合的IPv4 端口绑定功能配置举例

1. 组网需求

Device 通过端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别与客户端 Host 和 DHCP server 相连。

具体应用需求如下：

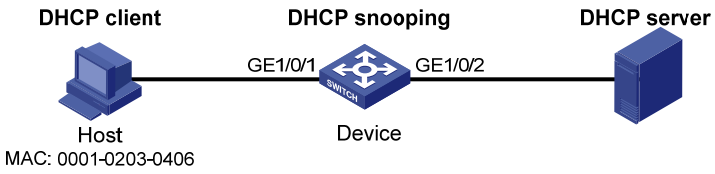
- Host 通过 DHCP server 获取 IP 地址。
- Device 上使能 DHCP Snooping 功能，记录 Host 的 DHCP Snooping 表项。
- 在端口 GigabitEthernet1/0/1 上启用 IPv4 端口绑定功能，利用记录的 DHCP Snooping 表项过滤端口转发的报文，仅允许通过 DHCP server 动态获取 IP 地址的客户端可以接入网络。

说明

DHCP server 的具体配置请参考“三层技术-IP 业务配置指导”中的“DHCP 服务器”。

2. 组网图

图1-3 配置与 DHCP Snooping 配合的 IPv4 端口绑定功能组网图



3. 配置步骤

(1) 配置 DHCP Snooping

开启 DHCP Snooping 功能。

```
<Device> system-view
[Device] dhcp-snooping
```

设置与 DHCP server 相连的端口 GigabitEthernet1/0/2 为信任端口。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] dhcp-snooping trust
[Device-GigabitEthernet1/0/2] quit
```

(2) 配置 IPv4 端口绑定功能

配置端口 GigabitEthernet1/0/1 的 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip verify source ip-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

显示端口 GigabitEthernet1/0/1 上的绑定表项信息。

```
[Device] display ip source binding
Total entries found: 1
 MAC Address       IP Address       VLAN   Interface            Type
 0001-0203-0406    192.168.0.1      1      GE1/0/1              DHCP-SNP
```

显示 DHCP Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 获取的动态表项一致。

```
[Device] display dhcp-snooping
 DHCP snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static , R--Recovering
 Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
 ==== =============== ============== ============ ==== ===== =================
 D    192.168.0.1     0001-0203-0406 86335        1    N/A   GigabitEthernet1/0/1
---   1 dhcp-snooping item(s) found   ---
```

从以上显示信息可以看出，端口 GigabitEthernet1/0/1 在配置 IPv4 端口绑定功能之后根据获取的 DHCP Snooping 表项产生了端口绑定表项。

1.5.3 与DHCP Relay配合的IPv4 端口绑定功能配置举例

1. 组网需求

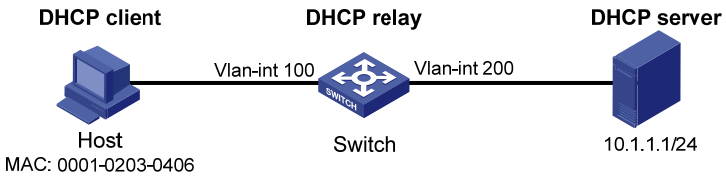
Switch 通过接口 Vlan-interface100 和 Vlan-interface200 分别与客户端 Host 和 DHCP server 相连。Switch 上使能 DHCP Relay 功能。

具体应用需求如下：

- Host（MAC 地址为 0001-0203-0406）通过 DHCP relay 从 DHCP server 上获取 IP 地址。
- 在接口 Vlan-interface100 上启用 IPv4 端口绑定功能，利用 Switch 上生成的 DHCP Relay 表项过滤端口转发的报文，仅允许通过 DHCP server 动态获取 IP 地址的客户端可以接入网络。

2. 组网图

图1-4 配置端口绑定功能组网图



3. 配置步骤

(1) 配置 IPv4 端口绑定功能

配置各接口的 IP 地址（略）。

在接口 Vlan-interface100 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<Switch> system-view
[Switch] vlan 100
[Switch-Vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip verify source ip-address mac-address
[Switch-Vlan-interface100] quit
```

(2) 配置 DHCP Relay

使能 DHCP 服务。

```
[Switch] dhcp enable
```

配置 DHCP 服务器的地址。

```
[Switch] dhcp relay server-group 1 ip 10.1.1.1
```

配置接口 Vlan-interface100 工作在 DHCP 中继模式。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] dhcp select relay
```

配置接口 Vlan-interface100 对应服务器组 1。

```
[Switch-Vlan-interface100] dhcp relay server-select 1
[Switch-Vlan-interface100] quit
```

4. 验证配置结果

显示生成的 IPv4 绑定表项信息。

```
[Switch] display ip source binding
Total entries found: 1
 MAC Address       IP Address      VLAN   Interface             Type
 0001-0203-0406    192.168.0.1     100    Vlan100               DHCP-RLY
```

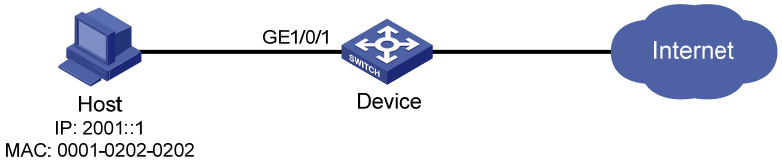
1.5.4 IPv6 静态绑定表项配置举例

1. 组网需求

IPv6 客户端通过 Device 的端口 GigabitEthernet1/0/1 接入网络。要求在 Device 上配置 IPv6 静态绑定表项，使得端口 GigabitEthernet1/0/1 上只允许 Host（MAC 地址为 0001-0202-0202、IPv6 地址为 2001::1）发送的 IPv6 报文通过。

2. 组网图

图1-5 配置 IPv6 静态绑定表项组网图



3. 配置步骤

在端口 GigabitEthernet1/0/1 上配置 IPv6 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<Device> system-view
[Device] interface gigabitethernet1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

在端口 GigabitEthernet1/0/1 上配置 IPv6 静态绑定表项，绑定源 IP 地址和 MAC 地址，只允许 IPv6 地址为 2001::1 且 MAC 地址为 00-01-02-02-02-02 的 IPv6 报文通过。

```
[Device-GigabitEthernet1/0/1] ipv6 source binding ipv6-address 2001::1 mac-address
0001-0202-0202
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

在 Device 上显示 IPv6 静态绑定表项配置成功。

```
[Device] display ipv6 source binding static
Total entries found: 1
 MAC Address         IP Address         VLAN   Interface             Type
 0001-0202-0202      2001::1            N/A    GE1/0/1               Static-IPv6
```

1.5.5 与DHCPv6 Snooping配合的IPv6 端口绑定功能配置举例

1. 组网需求

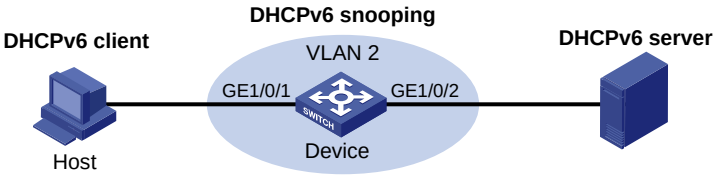
DHCPv6 客户端通过 Device 的端口 GigabitEthernet1/0/1 接入网络，通过 DHCPv6 server 获取 IPv6 地址。

具体应用需求如下：

- Device 上使能 DHCPv6 Snooping 功能，保证客户端从合法的服务器获取 IP 地址，且记录客户端 IPv6 地址及 MAC 地址的绑定关系。
- 在端口 GigabitEthernet1/0/1 上启用 IPv6 动态绑定功能，利用动态获取的 DHCPv6 Snooping 表项过滤端口转发的报文，只允许通过 DHCPv6 server 动态获取 IP 地址的客户端接入网络。

2. 组网图

图1-6 配置与 DHCPv6 Snooping 配合的 IPv6 端口绑定功能组网图



3. 配置步骤

(1) 配置 DHCPv6 Snooping

全局使能 DHCPv6 Snooping 功能。

```
<Device> system-view
[Device] ipv6 dhcp snooping enable
```

在 VLAN 2 内使能 DHCPv6 Snooping 功能。

```
[Device] vlan 2
[Device-vlan2] ipv6 dhcp snooping vlan enable
[Device] quit
```

配置端口 GigabitEthernet1/0/2 为信任端口。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
[Device-GigabitEthernet1/0/2] quit
```

(2) 配置 IPv6 动态绑定功能

配置端口 GigabitEthernet1/0/1 的 IPv6 动态绑定功能，绑定源 IP 地址和 MAC 地址。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

客户端通过 DHCPv6 server 成功获取 IP 地址之后，通过执行以下命令可查看到已生成的 IPv6 动态绑定表项信息。

```
[Device] display ipv6 source binding
Total entries found: 1
 MAC Address          IP Address        VLAN   Interface       Type
 040a-0000-0001       2001::1           2      GE1/0/1         DHCPv6-SNP
```

显示 DHCPv6 Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 生成的 IPv6 动态绑定表项一致。

```
[Device] display ipv6 dhcp snooping user-binding dynamic
IP Address                      MAC Address    Lease      VLAN Interface
=============================== ============== ========== ==== ==================
2001::1                         040a-0000-0001 286        2    GigabitEthernet1/0/1
---   1 DHCPv6 snooping item(s) found   ---
```

从以上显示信息可以看出，IP Source Guard 通过获取端口 GigabitEthernet1/0/1 上产生的 DHCPv6 Snooping 表项成功生成了 IPv6 动态绑定表项。

1.5.6 与ND Snooping配合的IPv6 端口绑定功能配置举例

1. 组网需求

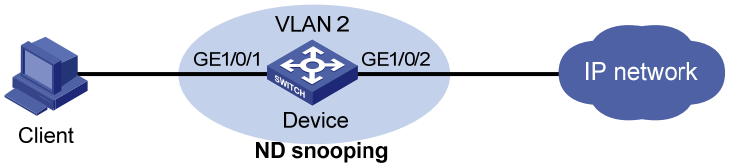
IPv6 客户端通过 Device 的端口 GigabitEthernet1/0/1 接入网络。

具体应用需求如下：

- Device 上使能 ND Snooping 功能，通过侦听 DAD NS 消息来建立 ND Snooping 表项。
- 在端口 GigabitEthernet1/0/1 上启用 IPv6 端口绑定功能，利用动态获取的 ND Snooping 表项过滤端口收到的报文，只允许合法获取 IPv6 地址的客户端可以接入网络。

2. 组网图

图1-7 配置与 ND Snooping 配合的 IPv6 端口绑定功能组网图



3. 配置步骤

(1) 配置 ND Snooping

在 VLAN 2 内使能 ND Snooping 功能。

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] ipv6 nd snooping enable
[Device-vlan2] quit
```

(2) 配置 IPv6 端口绑定功能

在端口 GigabitEthernet1/0/1 上配置 IPv6 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[Device] interface gigabitethernet1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

在 Device 上显示生成的 IPv6 绑定表项信息。

```
[Device] display ipv6 source binding
Total entries found: 1
 MAC Address          IP Address        VLAN   Interface       Type
 040a-0000-0001       2001::1           2      GE1/0/1         ND-SNP
```

显示 ND Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 获取的 IPv6 端口绑定表项一致。

```
[Device] display ipv6 nd snooping
IPv6 Address                  MAC Address     VID  Interface      Aging Status
2001::1                       040a-0000-0001  2    GE1/0/1        25     Bound
---- Total entries: 1 ----
```

从以上显示信息可以看出，IP Source Guard 通过获取端口 GigabitEthernet1/0/1 上产生的 ND Snooping 表项成功生成了 IPv6 动态绑定表项。

1.5.7 全局地址绑定配置举例

1. 组网需求

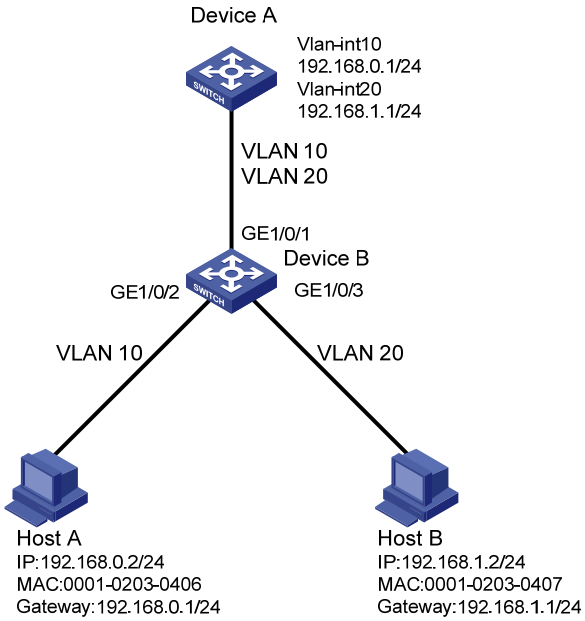
Device A 为汇聚设备，Device B 为接入设备，VLAN 10 中的 Host A 与 VLAN 20 中的 Host B 通过 Device A 进行通信。

具体应用需求如下：

- Device B 上阻止仿冒 Host A 和 Host B 的 IP 报文通过。
- Host A 和 Host B 之间的报文可在 Device B 上正常转发。

2. 组网图

图1-8 全局地址绑定典型配置组网图



3. 配置步骤

创建 VLAN 10，并将端口 GigabitEthernet1/0/2 加入 VLAN 10。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] port gigabitethernet1/0/2
[DeviceB-vlan10] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/3 加入 VLAN 20。

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet1/0/3
[DeviceB-vlan20] quit
```

将端口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，并允许 VLAN 10 和 VLAN 20 的报文通过。

```
[DeviceB] interface gigabitethernet1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

在端口 GigabitEthernet1/0/2 和端口 GigabitEthernet1/0/3 上分别配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[DeviceB] interface gigabitethernet1/0/2
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet1/0/3
[DeviceB-GigabitEthernet1/0/3] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/3] quit
```

配置全局静态绑定表项，阻止仿冒 Host A（IP 地址：192.168.0.2、MAC 地址：0001-0203-0406）和 Host B（IP 地址：192.168.1.2、MAC 地址：0001-0203-0407）的 IP 报文通过。

```
[DeviceB] ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0406
[DeviceB] ip source binding ip-address 192.168.1.2 mac-address 0001-0203-0407
```

4. 验证配置结果

在 Device 上显示配置的 IPv4 静态绑定表项信息。

```
[DeviceB] display ip source binding static
Total entries found: 2
 MAC Address       IP Address       VLAN   Interface           Type
 0001-0203-0406    192.168.0.2      N/A    N/A                 Static
 0001-0203-0407    192.168.1.2      N/A    N/A                 Static
```

以上配置完成后，Host A 和 Host B 能够成功 ping 通对方。

1.6 常见配置错误举例

1.6.1 静态绑定表项配置和端口绑定功能配置失败

1. 故障现象

在端口上配置静态绑定表项、配置端口绑定功能均失败。

2. 故障分析

IP Source Guard 功能不能在加入聚合组或加入业务环回组的端口上配置。

3. 处理过程

将端口退出已加入的聚合组或业务环回组。