目 录

1 IP Source Guard

1.1 IP Source Guard简介

1.1.1 概述

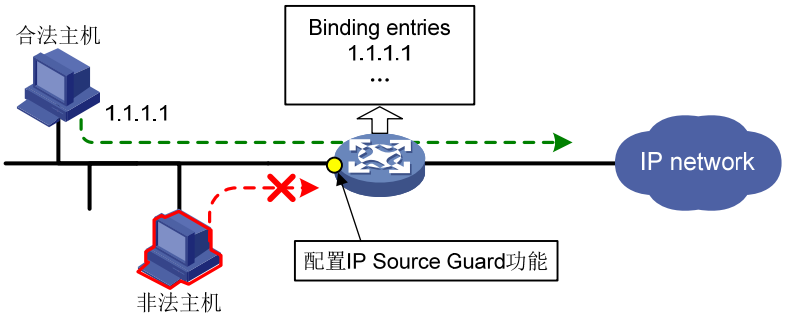
IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

如 图 1-1 所示，配置了IP Source Guard功能的接口接收到用户报文后，首先查找与该接口绑定的表项（简称为绑定表项），如果报文的信息与某绑定表项匹配，则转发该报文；若匹配失败，则查看是否配置了全局静态绑定表项，如果配置了此类表项，且报文的信息与表项匹配，则转发该报文，否则丢弃该报文。IP Source Guard可以根据报文的源IP地址、源MAC地址和VLAN标签对报文进行过滤。报文的这些特征项可单独或组合起来与接口进行绑定，形成如下几类绑定表项：

- IP 绑定表项
- MAC 绑定表项
- IP＋MAC 绑定表项
- IP＋VLAN 绑定表项
- MAC＋VLAN 绑定表项
- IP＋MAC＋VLAN 绑定表项

IP Source Guard 绑定表项可以通过手工配置和动态获取两种方式生成。

图1-1 IP Source Guard 功能示意图



说明

- IP Source Guard 的绑定功能是针对接口的，一个接口配置了绑定功能后，仅对该接口接收的报文进行限制，其它接口不受影响。
- 全局IP Source Guard表项仅支持IP+MAC静态绑定表项。全局静态绑定表项的详细介绍，请参见“1.1.2 静态配置绑定表项”

1.1.2 静态配置绑定表项

静态配置绑定表项是指通过命令行手工配置绑定表项，该方式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接口上配置绑定表项，仅允许该接口接收与该服务器通信的报文。

IPv4 静态绑定表项用于过滤接口收到的 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 静态绑定表项用于过滤接口收到的 IPv6 报文，或者与 ND Detection 功能配合使用检查接入用户的合法性。ARP Detection 功能的详细介绍请参见“安全配置指导”中的“ARP 攻击防御”。ND Detection 功能的详细介绍请参见“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接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。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. 接口静态绑定表项

端口静态绑定是在端口上配置的绑定了 IP 地址、MAC 地址、VLAN 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、VLAN 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 动态获取绑定表项

动态获取绑定表项是指通过获取其它模块生成的用户信息来生成绑定表项。目前，可为 IP Source Guard 提供表项信息的模块包括 ARP Snooping、802.1X、DHCP Snooping、DHCPv6 Snooping、DHCP 中继、DHCPv6 中继和 DHCP 服务器、ND Snooping 模块。

这种动态获取绑定表项的方式，通常适用于局域网络中主机较多的情况。以主机使用 DHCP 动态获取 IP 地址的情况为例，其原理是每当局域网内的主机通过 DHCP 服务器获取到 IP 地址时，DHCP 服务器会生成一条 DHCP 服务器表项，DHCP 中继会生成一条 DHCP 中继表项，DHCP Snooping 会生成一条 DHCP Snooping 表项。IP Source Guard 可以根据以上任何一条表项相应地增加一条 IP Source Guard 绑定表项来判断是否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，IP Source Guard 也不会增加相应的绑定表项，因此该用户的报文将会被丢弃。

1. IPv4 动态绑定功能

在配置了 IPv4 动态绑定功能的接口上，IP Source Guard 通过与不同的模块配合动态生成绑定表项：

- 在二层以太网端口上，IP Source Guard 可与 DHCP Snooping 配合，通过主机动态获取 IP 地址时产生的 DHCP Snooping 表项来生成动态绑定表项，并用于过滤报文。
- 在三层以太网接口或 VLAN 接口上，IP Source Guard 可与 DHCP 中继配合，通过主机跨网段获取 IP 地址时产生的 DHCP 中继表项来生成动态绑定表项，并用于过滤报文。
- 在二层以太网端口上，IP Source Guard 可与 802.1X 配合，通过获取认证用户的信息来生成动态绑定表项，并用于过滤报文。

- 在二层以太网端口上，IP Source Guard 可与 ARP Snooping 配合，通过获取的 ARP Snooping 表项来生成动态绑定表项，并用于过滤报文。
- 在三层以太网接口或 VLAN 接口上，IP Source Guard 可与 DHCP 服务器配合，通过 DHCP 服务器为主机动态分配 IP 地址时记录的用户信息来生成动态绑定表项，用于配合其它模块（例如授权 ARP）提供相关的安全服务，而不直接用于过滤报文。

802.1X 功能的详细介绍请参见“安全配置指导”中的“802.1X”。DHCP Snooping 功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。ARP Snooping 功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“ARP”。DHCP 中继功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。DHCP 服务器功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”。

2. IPv6 动态绑定功能

在配置了 IPv6 动态绑定功能的接口上，IP Source Guard 通过与不同模块配合动态生成绑定表项：

- 在二层以太网端口上，IP Source Guard 可与 DHCPv6 Snooping 配合，通过主机动态获取 IP 地址时产生的 DHCPv6 Snooping 表项来生成动态绑定表项，并用于过滤报文。
- 在三层以太网接口或 VLAN 接口上，IP Source Guard 可与 DHCPv6 中继配合，通过主机跨网段获取 IPv6 地址时产生的 DHCPv6 中继表项来生成动态绑定表项，并用于过滤报文。
- 在二层以太网端口上，IP Source Guard 可与 802.1X 配合，通过获取认证用户的信息来生成动态绑定表项，并用于过滤报文。
- 在二层以太网端口上，IP Source Guard 可与 ND Snooping 配合，通过获取的 ND Snooping 表项来生成动态绑定表项，并用于过滤报文。

802.1X 功能的详细介绍请参见“安全配置指导”中的“802.1X”。DHCPv6 Snooping 功能的详细介绍请参见“三层技术-IP 业务配置指导”的“DHCPv6 Snooping”。ND Snooping 功能的详细介绍请参见“三层技术-IP 业务配置指导”的“IPv6 基础”。DHCPv6 中继功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6 中继”。

1.2 IP Source Guard配置任务简介

表1-1 IPv4 绑定功能配置任务简介

配置任务	说明	详细配置
配置IPv4接口绑定功能	必选	1.3.1
配置IPv4静态绑定表项	可选	1.3.2
配置IP Source Guard免过滤条件	可选	1.3.3

表1-2 IPv6 绑定功能配置任务简介

配置任务	说明	详细配置
配置IPv6接口绑定功能	必选	1.4.1
配置IPv6静态绑定表项	可选	1.4.2

1.3 配置IPv4绑定功能

1.3.1 配置IPv4 接口绑定功能

配置了 IPv4 接口绑定功能的接口，将打开根据绑定表项过滤报文的开关，并利用配置的 IPv4 静态绑定表项和从其它模块获取的 IPv4 动态绑定表项对接口转发的报文进行过滤或者配合其它模块提供相关的安全服务。

(1) IPv4 静态绑定表项中指定的信息均用于IP Source Guard过滤接口收到的报文，具体配置请参考“1.3.2 配置IPv4 静态绑定表项”。

(2) IPv4 动态绑定表项中可能包含的内容有：MAC 地址、IP 地址、VLAN 信息、入接口信息及表项类型（DHCP Snooping、DHCP 中继等）。IP Source Guard 依据该表项中的哪些信息过滤接口收到的报文，由 IPv4 接口绑定配置决定：

- 若接口上配置动态绑定功能时绑定了源 IP 地址和 MAC 地址，则只有接口上收到的报文的源 IPv4 地址和源 MAC 地址都与某动态绑定表项匹配，该报文才能被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 IP 地址，则只有该接口收到的报文的源 IPv4 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 MAC 地址，则只有该接口收到的报文的源 MAC 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃。

要实现 IPv4 动态绑定功能，请保证网络中的 DHCP Snooping、DHCP 中继、ARP Snooping、802.1X 或 DHCP 服务器配置有效且工作正常。

表1-3 配置 IPv4 接口绑定功能

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*	可支持二层以太网端口/三层以太网接口VLAN接口
开启IPv4接口绑定功能	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	缺省情况下，接口的IPv4接口绑定功能处于关闭状态 IPv4接口绑定功能可多次配置，最后一次的配置生效

1.3.2 配置IPv4 静态绑定表项

IPv4 静态绑定表项包括全局的 IPv4 静态绑定表项和接口的 IPv4 静态绑定表项。

接口的 IPv4 静态绑定表项和动态绑定表项的优先级高于全局的 IPv4 静态绑定表项，即接口优先使用本接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，再与全局的静态绑定表项进行匹配。

1. 配置全局的IPv4 静态绑定表项

全局的 IPv4 静态绑定表项中定义了接口允许转发的报文的 IP 地址和 MAC 地址，对设备的所有接口都生效。

表1-4 配置全局的 IPv4 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-
配置全局的IPv4静态绑定表项	**ip source binding ip-address** *ip-address* **mac-address** *mac-address*	缺省情况下，未配置全局IPv4静态绑定表项

2. 配置接口的IPv4 静态绑定表项

表1-5 配置接口的 IPv4 静态绑定表项

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*	可支持二层以太网端口/三层以太网接口VLAN接口
配置接口的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*]	缺省情况下，接口上未配置IPv4静态绑定表项 **vlan** *vlan-id*参数仅在二层以太网接口视图下支持 在与ARP Detection功能配合时，绑定表项中必须指定IP、MAC和VLAN参数，且该VLAN为使能ARP Detection功能的VLAN，否则ARP报文将无法通过接口的IPv4静态绑定表项的检查。

说明

同一个表项不能在同一个接口上重复绑定，但可以在不同的接口上绑定。

1.3.3 配置IP Source Guard免过滤条件

缺省情况下，在接口上配置了 IPv4 绑定功能后，接口上会丢弃所有无绑定表项的 IPv4 报文。为避免特定用户的报文由于没有匹配的绑定表项而被丢弃，可配置 IP Source Guard 免过滤条件，允许接口直接放行匹配上免过滤条件的 IPv4 报文。

表1-6 配置 IP Source Guard 免过滤条件

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置IP Source Guard免过滤条件	**ip verify source exclude vlan** *start-vlan-id* [to *end-vlan-id*]	缺省情况下，未配置免过滤**条件** 可以通过**多次执行本命令**，**配置多个**IP Source Guard免过滤VLAN，但不同命令中的VLAN范围**不能重叠**

1.4 配置IPv6绑定功能

1.4.1 配置IPv6 接口绑定功能

配置了 IPv6 接口绑定功能的接口，将打开根据绑定表项过滤报文的开关，并利用配置的 IPv6 静态绑定表项和从其他模块获取的 IPv6 动态绑定表项对接口转发的报文进行过滤。

(1) IPv6 静态绑定表项中指定的信息均用于IP Source Guard过滤接口收到的报文，具体配置请参考“1.4.2 配置IPv6 静态绑定表项”。

(2) IPv6 动态绑定表项中可能包含的信息有：MAC 地址、IP 地址、VLAN 信息、入接口信息及表项类型（DHCPv6 Snooping、DHCPv6 Relay 等）。IP Source Guard 依据该表项中的哪些信息过滤接口收到的报文，由 IPv6 接口绑定配置决定：

- 若接口上配置动态绑定功能时绑定了源 IP 地址和 MAC 地址，则只有接口上收到的报文的源 IPv6 地址和源 MAC 地址都与某动态绑定表项匹配，该报文才能被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 IP 地址，则只有该接口收到的报文的源 IPv6 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 MAC 地址，则只有该接口收到的报文的源 MAC 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃。

要实现 IPv6 动态绑定功能，请保证网络中的 DHCPv6 Snooping、DHCPv6 Relay、802.1X 或 ND Snooping 配置有效且工作正常。

表1-7 配置 IPv6 接口绑定功能

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*	可支持二层以太网端口/三层以太网接口/VLAN接口
配置IPv6接口绑定功能	**ipv6 verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	缺省情况下，接口的IPv6接口绑定功能处于关闭状态 IPv6接口绑定功能可多次配置，最后一次的配置生效。

1.4.2 配置IPv6 静态绑定表项

IPv6 静态绑定功能包括全局的 IPv6 静态绑定功能和接口的 IPv6 静态绑定功能。

接口的 IPv6 静态绑定表项和 IPv6 动态绑定表项的优先级高于全局的 IPv6 静态绑定表项，即接口优先使用本接口上的 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，再与全局的 IPv6 静态绑定表项进行匹配。

1. 配置全局的IPv6 静态绑定表项

全局的 IPv6 静态绑定表项中定义了接口允许转发的报文的 IPv6 地址和 MAC 地址，对设备的所有接口都生效。

表1-8 配置全局的 IPv6 静态绑定表项

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

2. 配置接口的IPv6 静态绑定表项

表1-9 配置接口的 IPv6 静态绑定表项

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*	可支持二层以太网端口/三层以太网接口/VLAN接口
配置接口的IPv6静态绑定表项	**ipv6 source binding** { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	缺省情况下，未配置接口上IPv6静态绑定表项 **vlan** *vlan-id*参数仅在二层以太网接口视图下支持 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报文将无法通过接口的IPv6静态绑定表项的检查

说明

同一表项不能在同一个接口上重复绑定，但可以在不同接口上绑定。

1.5 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1-10 IP Source Guard 显示和维护（IPv4）

操作	命令
显示IPv4绑定表项信息	**display ip source binding** [**static** | [**arp-snooping** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]
显示IP Source Guard免过滤条件生效情况	**display ip verify source excluded** [**vlan** *start-vlan-id* [**to** *end-vlan-id*]] [**slot** *slot-number*]

表1-11 IP Source Guard 显示和维护（IPv6）

操作	命令
显示IPv6绑定表项信息	**display ipv6 source binding** [**static** | [**dhcpv6-relay** | **dhcpv6-snooping** | **dot1x** | **nd-snooping**] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

1.6 IP Source Guard典型配置举例

1.6.1 IPv4 静态绑定表项配置举例

1. 组网需求

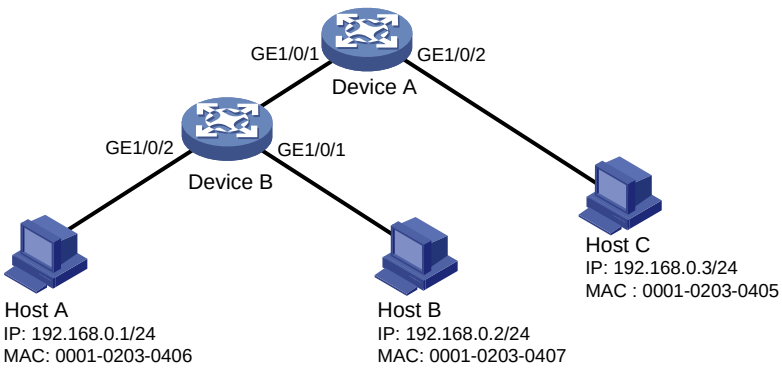
如 图 1-2 所示，Host A、Host B分别与Device B的接口GigabitEthernet1/0/2、GigabitEthernet1/0/1相连；Host C与Device A的接口GigabitEthernet1/0/2 相连。Device B接到Device A的接口GigabitEthernet1/0/1 上。各主机均使用静态配置的IP地址。

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

- Device A 的接口 GigabitEthernet1/0/2 上只允许 Host C 发送的 IP 报文通过。
- Device A 的接口 GigabitEthernet1/0/1 上只允许 Host A 发送的 IP 报文通过。
- Device B 上的所有接口都允许 Host A 发送的 IP 报文通过。
- Device B 的接口 GigabitEthernet1/0/1 上允许 Host B 发送的 IP 报文通过。

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

配置各接口的 IP 地址（略）。

在接口 GigabitEthernet1/0/2 上开启 IPv4 接口绑定功能，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，在 Device A 的 GigabitEthernet1/0/2 上只允许 MAC 地址为 0001-0203-0405、IP 地址为 192.168.0.3 的数据终端 Host C 发送的 IP 报文通过。

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

在接口 GigabitEthernet1/0/1 上开启 IPv4 接口绑定功能，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
```

配置在 Device A 的 GigabitEthernet1/0/1 上只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。

```
[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

配置各接口的 IP 地址（略）。

在接口 GigabitEthernet1/0/2 上开启 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

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

配置 IPv4 静态绑定表项，在 Device B 上的所有接口都允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。

```
[DeviceB] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

在接口 GigabitEthernet1/0/1 上开启 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

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

配置 IPv4 静态绑定表项，在 Device B 的 GigabitEthernet1/0/1 上允许 MAC 地址为 0001-0203-0407 的数据终端 Host B 发送的 IP 报文通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip source binding mac-address 0001-0203-0407
[DeviceB-GigabitEthernet1/0/1] quit
```

4. 验证配置

在 Device A 上显示 IPv4 静态绑定表项，可以看出以上配置成功。

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

```
192.168.0.3     0001-0203-0406 GE1/0/1                  N/A  Static
```

在 Device B 上显示 IPv4 静态绑定表项，可以看出以上配置成功。

```
<DeviceB> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 N/A                     N/A  Static
N/A             0001-0203-0407 GE1/0/1                 N/A  Static
```

1.6.2 与DHCP Snooping配合的IPv4 动态绑定功能配置举例

1. 组网需求

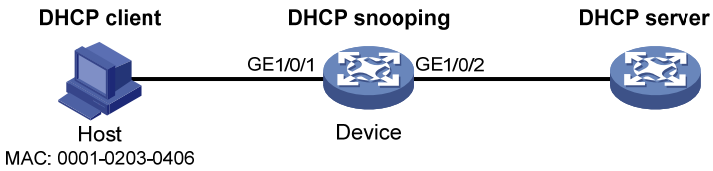
DHCP 客户端通过 Device 的接口 GigabitEthernet1/0/1 接入网络，通过 DHCP 服务器获取 IPv4 地址。

具体应用需求如下：

- Device 上使能 DHCP 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 IPv4 地址及 MAC 地址的绑定关系。
- 在接口 GigabitEthernet1/0/1 上启用 IPv4 动态绑定功能，利用动态生成的 DHCP Snooping 表项过滤接口接收的报文，只允许通过 DHCP 服务器动态获取 IP 地址的客户端接入网络。DHCP 服务器的具体配置请参见“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 动态绑定功能组网图



3. 配置步骤

(1) 配置 DHCP Snooping

配置各接口的 IP 地址（略）。

开启 DHCP Snooping 功能。

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

设置与 DHCP 服务器相连的接口 GigabitEthernet1/0/2 为信任接口。

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

(2) 配置 IPv4 接口绑定功能

开启接口 GigabitEthernet1/0/1 的 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址，并启用接口的 DHCP Snooping 表项记录功能。

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

```
[Device-GigabitEthernet1/0/1] dhcp snooping binding record
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置

显示接口 GigabitEthernet1/0/1 从 DHCP Snooping 获取的动态表项。

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

从以上显示信息可以看出，接口 GigabitEthernet1/0/1 在配置 IPv4 接口绑定功能之后根据 DHCP Snooping 表项产生了动态绑定表项。

1.6.3 与DHCP中继配合的IPv4 动态绑定功能配置举例

1. 组网需求

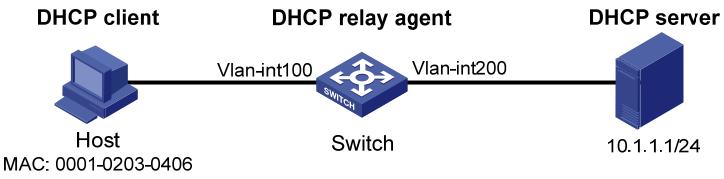
Switch 通过接口 Vlan-interface100 和 Vlan-interface200 分别与客户端 Host 和 DHCP 服务器相连。Switch 上使能 DHCP 中继功能。

具体应用需求如下：

- Host 通过 DHCP 中继从 DHCP 服务器上获取 IP 地址。
- 在接口 Vlan-interface100 上启用 IPv4 动态绑定功能，利用 Switch 上生成的 DHCP 中继表项，过滤接口接收的报文。

2. 组网图

图1-4 配置动态绑定功能组网图



3. 配置步骤

(1) 配置 IPv4 动态绑定功能

配置各接口的 IP 地址（略）。

在接口 Vlan-interface100 上开启 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

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

(2) 配置 DHCP 中继

开启 DHCP 服务。

```
[Switch] dhcp enable
```

开启 DHCP 中继用户地址表项记录功能。

```
[Switch] dhcp relay client-information record
```

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
```

指定 DHCP 服务器的地址。

```
[Switch-Vlan-interface100] dhcp relay server-address 10.1.1.1
[Switch-Vlan-interface100] quit
```

4. 验证配置

显示生成的 IPv4 动态绑定表项信息。

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

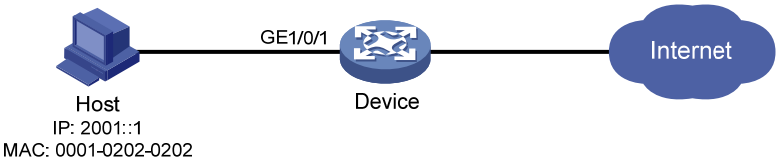
1.6.4 IPv6 静态绑定表项配置举例

1. 组网需求

IPv6 客户端通过 Device 的接口 GigabitEthernet1/0/1 接入网络。要求在 Device 上配置 IPv6 静态绑定表项，使得接口 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

在接口 GigabitEthernet1/0/1 上开启 IPv6 接口绑定功能，绑定源 IP 地址和 MAC 地址。

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

在接口 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 ip-address 2001::1 mac-address
0001-0202-0202
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置

在 Device 上显示 IPv6 静态绑定表项，可以看出以上配置成功。

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

1.6.5 与DHCPv6 Snooping配合的IPv6 动态绑定表项配置举例

1. 组网需求

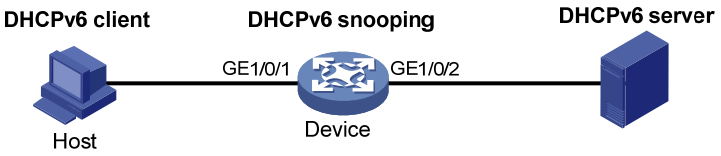
DHCPv6 客户端通过 Device 的接口 GigabitEthernet1/0/1 接入网络，通过 DHCPv6 服务器获取 IPv6 地址。

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。
- 在接口 GigabitEthernet1/0/1 上启用 IPv6 动态绑定功能，利用动态生成的 DHCPv6 Snooping 表项过滤接口接收的报文，只允许通过 DHCPv6 服务器动态获取 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 动态绑定功能组网图



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
```

配置接口 GigabitEthernet1/0/2 为信任接口。

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

(2) 配置 IPv6 接口绑定功能

开启接口 GigabitEthernet1/0/1 的 IPv6 接口绑定功能，绑定源 IP 地址和 MAC 地址，并启用接口的 DHCPv6 Snooping 表项记录功能。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
[Device-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置

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 dhcpv6-snooping
Total entries found: 1
IPv6 Address         MAC Address    Interface              VLAN Type
2001::1              040a-0000-0001 GE1/0/1                1    DHCPv6 snooping
```

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

1.6.6 与DHCPv6 中继配合的IPv6 动态绑定功能配置举例

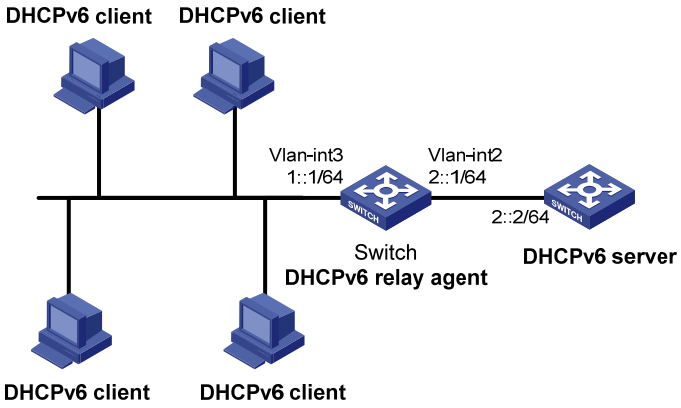
1. 组网需求

Switch 通过接口 Vlan-interface3 和 Vlan-interface2 分别与客户端和 DHCPv6 服务器相连。通过在 Switch 上使能 DHCPv6 中继功能，实现如下需求：

- 客户端通过 DHCPv6 中继从 DHCPv6 服务器上获取 IPv6 地址。
- 在接口 Vlan-interface3 上启用 IPv6 动态绑定功能，利用 Switch 上生成的 DHCPv6 中继表项，过滤接口接收的报文。

2. 组网图

图1-7 配置与 DHCPv6 中继配合的 IPv6 动态绑定功能组网图



3. 配置步骤

(1) 配置 DHCPv6 中继

创建 VLAN、将接口加入到 VLAN，并配置 VLAN 接口的 IPv6 地址（略）。

配置接口 Vlan-interface3 工作在 DHCPv6 中继模式。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ipv6 dhcp select relay
```

开启 DHCPv6 中继用户地址表项记录功能。

```
[Switch-Vlan-interface3] ipv6 dhcp relay client-information record
```

指定 DHCPv6 服务器的地址。

```
[Switch-Vlan-interface3] ipv6 dhcp relay server-address 2::2
[Switch-Vlan-interface3] quit
```

在接口 Vlan-interface3 上开启 IPv6 接口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<Switch> system-view
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ipv6 verify source ip-address mac-address
[Switch-Vlan-interface3] quit
```

4. 验证配置

显示生成的 IPv6 动态绑定表项信息。

```
[Switch] display ipv6 source binding dhcpv6-relay
Total entries found: 1
IP Address      MAC Address    Interface               VLAN Type
1::2            0001-0203-0406 Vlan3                   3    DHCPv6 relay
```