目 录

1 ARP攻击防御

说明

设备支持两种运行模式：独立运行模式和 IRF 模式，缺省情况为独立运行模式。有关 IRF 模式的介绍，请参见“虚拟化技术配置指导”中的“IRF”。

1.1 ARP攻击防御简介

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。

- 攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表项不正确，从而对网络进行攻击。
- 攻击者通过向设备发送大量目标 IP 地址不能解析的 IP 报文，使得设备试图反复地对目标 IP 地址进行解析，导致 CPU 负荷过重及网络流量过大。
- 攻击者向设备发送大量 ARP 报文，对设备的 CPU 形成冲击。

关于 ARP 攻击报文的特点以及 ARP 攻击类型的详细介绍，请参见“ARP 攻击防范技术白皮书”。

目前 ARP 攻击和 ARP 病毒已经成为局域网安全的一大威胁，为了避免各种攻击带来的危害，设备提供了多种技术对攻击进行防范、检测和解决。

下面将详细介绍一下这些技术的原理以及配置。

1.2 ARP攻击防御配置任务简介

表1-1 ARP 攻击防御配置任务简介

配置任务			说明	详细配置
防止泛洪攻击	配置ARP防止IP报文攻击功能	配置ARP源抑制功能	可选 建议在网关设备上配置本功能	1.3
		配置ARP黑洞路由功能	可选 建议在网关设备上配置本功能	
	配置ARP报文限速功能		可选 建议在接入设备上配置本功能	1.4
	配置源MAC地址固定的ARP攻击检测功能		可选 建议在网关设备上配置本功能	1.5
防止仿冒用户、仿冒网关攻击	配置ARP报文源MAC地址一致性检查功能		可选 建议在网关设备上配置本功能	1.6
	配置ARP主动确认功能		可选 建议在网关设备上配置本功能	1.7

配置任务		说明	详细配置
	配置授权ARP功能	可选 建议在网关设备上配置本功能	1.8
	配置ARP Detection功能	可选 建议在接入设备上配置本功能	1.9
	配置ARP自动扫描、固化功能	可选 建议在网关设备上配置本功能	1.10
	配置ARP网关保护功能	可选 建议在接入设备上配置本功能	1.11
	配置ARP过滤保护功能	可选 建议在接入设备上配置本功能	1.12

1.3 配置ARP防止IP报文攻击功能

1.3.1 ARP防止IP报文攻击功能简介

如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下列两个功能：

- ARP 源抑制功能：如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。开启该功能后，如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。
- ARP 黑洞路由功能：无论发送攻击报文的源是否固定，都可以采用 ARP 黑洞路由功能。开启该功能后，一旦接收到目标 IP 地址未解析的 IP 报文，设备立即产生一个黑洞路由，去往该地址的报文将被丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。为了控制黑洞路由的存活时间，设备支持配置 ARP 黑洞路由探测时间间隔（t 秒）和发送探测报文的次数（n 次）。产生 ARP 黑洞路由后，设备会立即发送第一个探测报文（ARP 请求报文），之后每隔 t 秒发送一次探测报文，如果在黑洞路由老化时间（25 秒）内，对发送的探测报文中的目标 IP 地址的 MAC 地址 ARP 解析成功，则将此条黑洞路由转化为有效路由，并对报文进行转发；否则在黑洞路由老化时间到达后，设备删除该黑洞路由，此时如果发送的探测报文数未达到配置数，也将不再继续发送。后继，有报文触发则再次发起解析，解析成功则进行转发，不成功会立即产生一个 ARP 黑洞路由并重复上述过程。

1.3.2 配置ARP防止IP报文攻击功能

1. 配置ARP源抑制功能

表1-2 配置 ARP 源抑制功能

操作	命令	说明
进入系统视图	**system-view**	-
使能ARP源抑制功能	**arp source-suppression enable**	缺省情况下，ARP源抑制功能处于关闭状态
配置ARP源抑制的阈值	**arp source-suppression limit** *limit-value*	缺省情况下，ARP源抑制的阈值为10

2. 配置ARP黑洞路由功能

表1-3 配置 ARP 黑洞路由功能

操作	命令	说明
进入系统视图	**system-view**	-
使能ARP黑洞路由功能	**arp resolving-route enable**	缺省情况下，ARP黑洞路由功能处于开启状态
配置发送ARP黑洞路由探测报文的时间间隔	**arp resolving-route probe-interval** *time*	缺省情况下，发送ARP黑洞路由探测报文的时间间隔为1秒
配置发送ARP黑洞路由探测报文的次数	**arp resolving-route probe-count** *count*	缺省情况下，发送ARP黑洞路由探测报文的次数为1

1.3.3 ARP防止IP报文攻击显示和维护

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 ARP 源抑制的运行情况，通过查看显示信息验证配置的效果。

表1-4 ARP 防止 IP 报文攻击显示和维护

操作	命令
显示ARP源抑制的配置信息	**display arp source-suppression**

1.3.4 ARP防止IP报文攻击配置举例

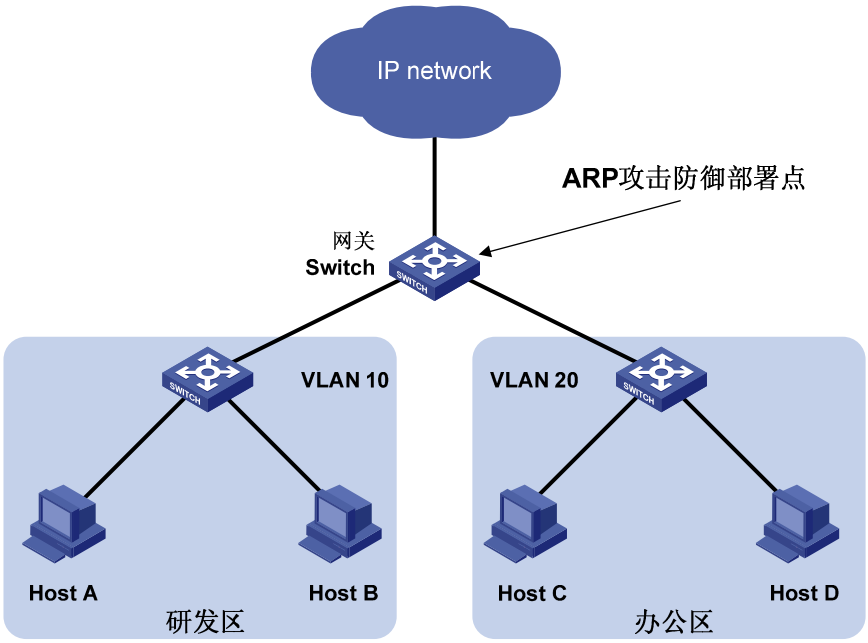
1. 组网需求

某局域网内存在两个区域：研发区和办公区，分别属于VLAN 10 和VLAN 20，通过接入交换机连接到网关Switch，如 图 1-1 所示。

网络管理员在监控网络时发现办公区存在大量 ARP 请求报文，通过分析认为存在 IP 泛洪攻击，为避免这种 IP 报文攻击所带来的危害，可采用 ARP 源抑制功能和 ARP 黑洞路由功能。

2. 组网图

图1-1 ARP 防止 IP 报文攻击配置组网图



3. 配置思路

对攻击报文进行分析，如果发送攻击报文的源地址是固定的，采用 ARP 源抑制功能。在 Switch 上做如下配置：

- 使能 ARP 源抑制功能；
- 配置 ARP 源抑制的阈值为 100，即当每 5 秒内的 ARP 请求报文的流量超过 100 后，对于由此 IP 地址发出的 IP 报文，设备不允许其触发 ARP 请求，直至 5 秒后再处理。

如果发送攻击报文的源地址是不固定的，则采用 ARP 黑洞路由功能，在 Switch 上配置 ARP 黑洞路由功能。

4. 配置步骤

- 配置 ARP 源抑制功能

使能 ARP 源抑制功能，并配置 ARP 源抑制的阈值为 100。

```
<Switch> system-view
[Switch] arp source-suppression enable
[Switch] arp source-suppression limit 100
```

- 配置 ARP 黑洞路由功能

使能 ARP 黑洞路由功能。

```
[Switch] arp resolving-route enable
```

1.4 配置ARP报文限速功能

1.4.1 ARP报文限速功能简介

ARP 报文限速功能是指对上送 CPU 的 ARP 报文进行限速，可以防止大量 ARP 报文对 CPU 进行冲击。例如，在配置了 ARP Detection 功能后，设备会将收到的 ARP 报文重定向到 CPU 进行检查，这样引入了新的问题：如果攻击者恶意构造大量 ARP 报文发往设备，会导致设备的 CPU 负担过重，从而造成其他功能无法正常运行甚至设备瘫痪，这个时候可以启用 ARP 报文限速功能来控制上送 CPU 的 ARP 报文的速率。

建议用户在配置了 ARP Detection、ARP Snooping、ARP 快速应答，或者发现有 ARP 泛洪攻击的情况下，使用 ARP 报文限速功能。

1.4.2 配置ARP报文限速功能

设备上配置 ARP 报文限速功能后，当接口上单位时间收到的 ARP 报文数量超过用户设定的限速值，设备处理方式如下：

- 当开启了 ARP 模块的告警功能后，设备将这个时间间隔内的超速峰值作为告警信息发送出去，生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关特性。有关告警信息的详细介绍请参见“网络管理和监控命令参考”中的 SNMP；
- 当开启了 ARP 限速日志功能后，设备将这个时间间隔内的超速峰值作为日志的速率值发送到设备的信息中心，通过设置信息中心的参数，最终决定日志报文的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）；

为防止过多的告警和日志信息干扰用户工作，用户可以设定信息的发送时间间隔。当用户设定的时间间隔超时时，设备执行发送告警或日志的操作。

表1-5 配置 ARP 报文限速功能

操作	命令	说明
进入系统视图	**system-view**	-
（可选）开启ARP模块的告警功能	**snmp-agent trap enable arp** [**rate-limit**]	缺省情况下，ARP模块的告警功能处于关闭状态
（可选）开启ARP报文限速日志功能	**arp rate-limit log enable**	缺省情况下，设备的ARP报文限速日志功能处于关闭状态
（可选）配置当设备收到的ARP报文速率超过用户设定的限速值时，设备发送告警或日志的时间间隔	**arp rate-limit log interval** *seconds*	缺省情况下，当设备收到的ARP报文速率超过用户设定的限速值时，设备发送告警或日志的时间间隔为60秒
进入二层以太网接口/二层聚合接口视图	**interface** *interface-type interface-number*	-
开启ARP报文限速功能	**arp rate-limit** [*pps*]	缺省情况下，ARP报文限速功能处于开启状态

说明

如果开启了 ARP 报文限速的告警和日志功能，并在二层聚合接口上开启了 ARP 报文限速功能，则只要聚合成员接口上的 ARP 报文速率超过用户设定的限速值，就会发送告警和日志信息。

1.5 配置源MAC地址固定的ARP攻击检测功能

1.5.1 源MAC地址固定的ARP攻击检测功能简介

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。

对于网关或一些重要的服务器，可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的 MAC 地址配置成保护 MAC 地址，这样，即使该设备存在攻击也不会被检测、过滤。

1.5.2 配置源MAC地址固定的ARP攻击检测功能

表1-6 配置源 MAC 地址固定的 ARP 攻击检测功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能源MAC地址固定的ARP攻击检测功能，并选择检查模式	**arp source-mac** { **filter** | **monitor** }	缺省情况下，源MAC地址固定的ARP攻击检测功能处于关闭状态
配置源MAC地址固定的ARP报文攻击检测的阈值	**arp source-mac threshold** *threshold-value*	缺省情况下，源MAC地址固定的ARP报文攻击检测阈值为30
配置源MAC地址固定的ARP攻击检测表项的老化时间	**arp source-mac aging-time** *time*	缺省情况下，源MAC地址固定的ARP攻击检测表项的老化时间为300秒，即5分钟
（可选）配置保护MAC地址	**arp source-mac exclude-mac** *mac-address*&<1-n>	缺省情况下，没有配置任何保护MAC地址 n的取值范围为1～64

说明

对于已添加到源 MAC 地址固定的 ARP 攻击检测表项中的 MAC 地址，在等待设置的老化时间后，会重新恢复成普通 MAC 地址。

1.5.3 源MAC地址固定的ARP攻击检测显示和维护

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源 MAC 地址固定的 ARP 攻击检测的运行情况，通过查看显示信息验证配置的效果。

表1-7 源 MAC 地址固定的 ARP 攻击检测显示和维护

操作	命令
显示检测到的源MAC地址固定的ARP攻击检测表项（独立运行模式）	**display arp source-mac** { **slot** *slot-number* | **interface** *interface-type interface-number* }
显示检测到的源MAC地址固定的ARP攻击检测表项（IRF模式）	**display arp source-mac** { **chassis** *chassis-number* **slot** *slot-number* | **interface** *interface-type interface-number* }

1.5.4 源MAC地址固定的ARP攻击检测功能配置举例

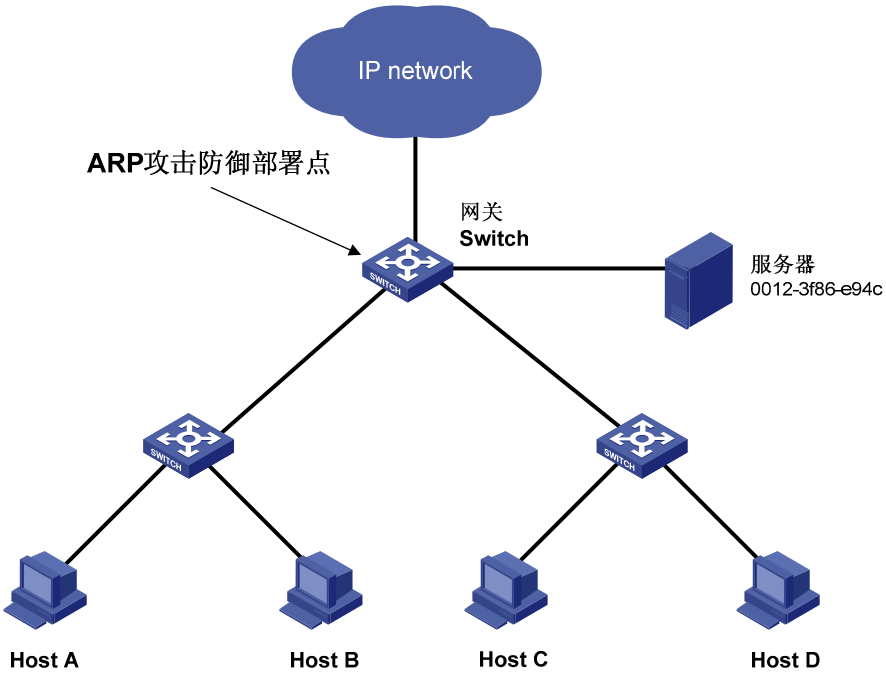
1. 组网需求

某局域网内客户端通过网关与外部网络通信，网络环境如 图 1-2 所示。

网络管理员希望能够防止因恶意用户对网关发送大量 ARP 报文，造成设备瘫痪，并导致其它用户无法正常地访问外部网络；同时，对于正常的大量 ARP 报文仍然会进行处理。

2. 组网图

图1-2 源 MAC 地址固定的 ARP 攻击检测功能配置组网图



3. 配置思路

如果恶意用户发送大量报文的源 MAC 地址是使用客户端合法的 MAC 地址，并且源 MAC 是固定的，可以在网关上进行如下配置：

- 使能源 MAC 固定 ARP 攻击检测功能，并选择过滤模式；
- 配置源 MAC 固定 ARP 报文攻击检测的阈值；
- 配置源 MAC 固定的 ARP 攻击检测表项的老化时间；
- 配置服务器的 MAC 为保护 MAC，使服务器可以发送大量 ARP 报文。

4. 配置步骤

使能源 MAC 固定 ARP 攻击检测功能，并选择过滤模式。

```
<Switch> system-view
[Switch] arp source-mac filter
```

配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。

```
[Switch] arp source-mac threshold 30
```

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
[Switch] arp source-mac aging-time 60
```

配置源 MAC 固定攻击检查的保护 MAC 地址为 0012-3f86-e94c。

```
[Switch] arp source-mac exclude-mac 0012-3f86-e94c
```

1.6 配置ARP报文源MAC地址一致性检查功能

1.6.1 ARP报文源MAC地址一致性检查功能简介

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同的 ARP 攻击。

配置本特性后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

1.6.2 配置ARP报文源MAC地址一致性检查功能

表1-8 配置 ARP 报文源 MAC 地址一致性检查功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能ARP报文源MAC地址一致性检查功能	**arp valid-check enable**	缺省情况下，ARP报文源MAC地址一致性检查功能处于关闭状态

1.7 配置ARP主动确认功能

1.7.1 ARP主动确认功能简介

启用 ARP 主动确认功能后，设备在新建或更新 ARP 表项前需进行主动确认。ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

未启用 ARP 主动确认功能时，设备收到一个 ARP 报文的处理过程如下：

- 如果设备的 ARP 表中没有与此 ARP 报文源 IP 地址对应的 ARP 表项，设备会根据 ARP 报文中携带的源 IP 地址、源 MAC 地址信息新建 ARP 表项。
- 如果设备的 ARP 表中存在与此 ARP 报文源 IP 地址对应的 ARP 表项，设备会根据 ARP 报文中携带的源 IP 地址、源 MAC 地址信息更新对应的 ARP 表项。

启用 ARP 主动确认功能后，设备在新建或更新 ARP 表项前需进行主动确认，防止产生错误的 ARP 表项。下面将详细介绍其工作原理。

1. 新建ARP表项前的主动确认

设备收到一个 ARP 报文，若当前设备 ARP 表中没有与此 ARP 报文源 IP 地址对应的 ARP 表项，设备会首先验证该 ARP 报文的真实性。设备会采用收到的 ARP 报文的源 IP 地址发送一个广播 ARP 请求报文，如果在随后的 3 秒内收到 ARP 应答报文，将对前期收到的 ARP 报文与此次收到的 ARP 应答报文进行比较（比较内容包括：源 IP 地址、源 MAC 地址、报文接收端口）。

- 如果两个报文一致，则认为收到的 ARP 报文为真实报文，并根据此报文在 ARP 表中新建对应的表项。
- 如果两个报文不一致，则认为收到的 ARP 报文为攻击报文，设备会忽略之前收到 ARP 报文，ARP 表中不会新建对应的表项。

2. 更新ARP表项前的主动确认

设备收到一个 ARP 报文（报文 A），若当前设备 ARP 表中已有与报文 A 源 IP 地址对应的 ARP 表项，但报文 A 携带的源 MAC 地址和现有 ARP 表项中的 MAC 地址不相同，设备就需要判断当前 ARP 表项的正确性以及报文 A 的真实性。

(1) 确定是否启动 ARP 表项正确性检查

为了避免短时间内多次收到来自同一源 IP 地址的 ARP 报文导致的 ARP 表项频繁更新，设备会首先判断该 ARP 表项的刷新时间是否超过 1 分钟。

- 如果没有超过 1 分钟，则设备不会对 ARP 表项进行更新。
- 如果已经超过 1 分钟，设备将启动当前 ARP 表项的正确性检查。

(2) 启动 ARP 表项的正确性检查

设备会向 ARP 表项对应的源发送一个单播 ARP 请求报文（报文的目的 IP 地址、目的 MAC 地址采用 ARP 表项中的 IP 地址、MAC 地址）。如果在随后的 5 秒内收到 ARP 应答报文（报文 B），将比较当前 ARP 表项中的 IP 地址、MAC 地址与报文 B 的源 IP 地址、源 MAC 地址是否一致。

- 如果一致，则认为报文 A 为攻击报文、ARP 表项不会更新。
- 如果不一致，设备将启动报文 A 的真实性检查。

(3) 启动报文 A 的真实性检查

设备会向报文 A 对应的源发送一个单播 ARP 请求报文（报文的目的 IP 地址、目的 MAC 地址采用报文 A 的源 IP 地址、源 MAC 地址）。如果在随后的 5 秒内收到 ARP 应答报文（报文 C），将比较报文 A 与报文 C 的源 IP 地址、源 MAC 地址是否一致。

- 如果一致，则认为报文 A 为真实报文，并根据报文 A 更新 ARP 表中对应表项。
- 如果不一致，则认为报文 A 为攻击报文，设备会忽略收到的报文 A，ARP 表项不会更新。

使能主动确认严格模式后，新建 ARP 表项前，ARP 主动确认功能会执行更严格的检查：

- 收到目标 IP 为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但不建立表项。
- 收到 ARP 应答报文时，需要确认本设备是否对该报文中源 IP 地址发起过 ARP 解析，若发起过解析，解析成功后设备启动主动确认功能，在主动确认流程成功完成后，设备建立该表项；若未发起过解析，设备直接丢弃该报文。

1.7.2 配置ARP主动确认功能

表1-9 配置 ARP 主动确认功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能ARP主动确认功能	**arp active-ack** [**strict**] **enable**	缺省情况下，ARP主动确认功能处于关闭状态

1.8 配置授权ARP功能

1.8.1 授权ARP功能简介

所谓授权 ARP（Authorized ARP），就是动态学习 ARP 的过程中，只有和 DHCP 服务器生成的租约或 DHCP 中继生成的安全表项一致的 ARP 报文才能够被学习。关于 DHCP 服务器和 DHCP 中继的介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”和“DHCP 中继”。

使能接口的授权 ARP 功能后，可以防止用户仿冒其他用户的 IP 地址或 MAC 地址对网络进行攻击，保证只有合法的用户才能使用网络资源，增加了网络的安全性。

1.8.2 配置授权ARP功能

表1-10 配置授权 ARP 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网接口/三层以太网子接口/三层聚合接口/三层聚合子接口视图/VLAN接口视图	**interface** *interface-type interface-number*	-
使能授权ARP功能	**arp authorized enable**	缺省情况下，接口下的授权ARP功能处于关闭状态

1.8.3 授权ARP功能在DHCP服务器上的典型配置举例

说明

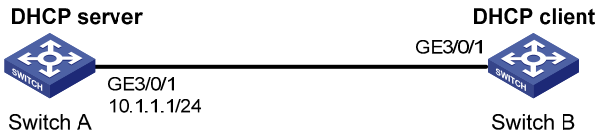
缺省情况下，以太网接口、VLAN 接口及聚合接口处于 DOWN 状态。如果要使这些接口能够正常工作，请先使用 **undo shutdown** 命令使接口状态处于 UP。

1. 组网需求

- Switch A 是 DHCP 服务器，为同一网段中的客户端动态分配 IP 地址，地址池网段为 10.1.1.0/24。通过在接口 GigabitEthernet3/0/1 上启用授权 ARP 功能来保证客户端的合法性。
- Switch B 是 DHCP 客户端，通过 DHCP 协议从 DHCP 服务器获取 IP 地址。

2. 组网图

图1-3 授权 ARP 功能典型配置组网图



3. 配置步骤

(1) 配置 Switch A

配置接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface GigabitEthernet 3/0/1
[SwitchA-GigabitEthernet3/0/1] ip address 10.1.1.1 24
[SwitchA-GigabitEthernet3/0/1] quit
```

使能 DHCP 服务。

```
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] quit
```

进入三层以太网接口视图。

```
[SwitchA] interface GigabitEthernet 3/0/1
```

使能接口授权 ARP 功能。

```
[SwitchA-GigabitEthernet3/0/1] port link-mode route
[SwitchA-GigabitEthernet3/0/1] arp authorized enable
[SwitchA-GigabitEthernet3/0/1] quit
```

(2) 配置 Switch B

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 3/0/1
[SwitchB-GigabitEthernet3/0/1] ip address dhcp-alloc
[SwitchB-GigabitEthernet3/0/1] quit
```

(3) Switch B 获得 Switch A 分配的 IP 后，在 Switch A 查看授权 ARP 信息。

```
[SwitchA] display arp all
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP Address       MAC Address     VLAN     Interface          Aging  Type
10.1.1.2         0012-3f86-e94c  N/A      GE3/0/1             20     D
```

从以上信息可以获知 Switch A 为 Switch B 动态分配的 IP 地址为 10.1.1.2。

此后，Switch B 与 Switch A 通信时采用的 IP 地址、MAC 地址等信息必须和授权 ARP 表项中的一致，否则将无法通信，保证了客户端的合法性。

1.8.4 授权ARP功能在DHCP中继上的典型配置举例

说明

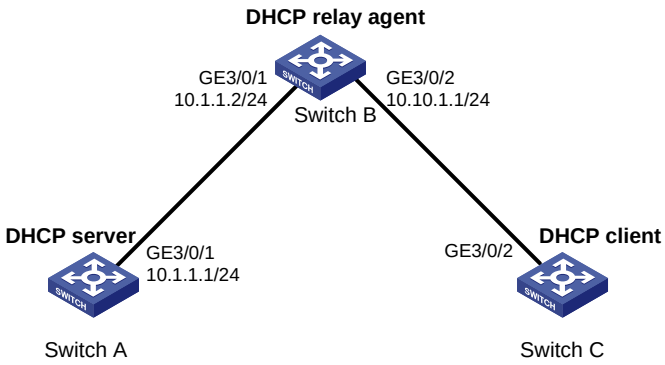
缺省情况下，以太网接口、VLAN 接口及聚合接口处于 DOWN 状态。如果要使这些接口能够正常工作，请先使用 **undo shutdown** 命令使接口状态处于 UP。

1. 组网需求

- Switch A 是 DHCP 服务器，为不同网段中的客户端动态分配 IP 地址，地址池网段为 10.10.1.0/24。
- Switch B 是 DHCP 中继，通过在接口 GigabitEthernet3/0/2 上启用授权 ARP 功能来保证客户端的合法性。
- Switch C 是 DHCP 客户端，通过 DHCP 中继从 DHCP 服务器获取 IP 地址。

2. 组网图

图1-4 授权 ARP 功能典型配置组网图



3. 配置步骤

(1) 配置 Switch A

配置接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface GigabitEthernet 3/0/1
[SwitchA-GigabitEthernet3/0/1] ip address 10.1.1.1 24
[SwitchA-GigabitEthernet3/0/1] quit
```

启用 DHCP 服务。

```
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-1] gateway-list 10.10.1.1
[SwitchA-dhcp-pool-1] quit
[SwitchA] ip route-static 10.10.1.0 24 10.1.1.2
```

(2) 配置 Switch B

启用 DHCP 服务。

```
<SwitchB> system-view
[SwitchB] dhcp enable
```
配置接口的 IP 地址。
```
[SwitchB] interface GigabitEthernet 3/0/1
[SwitchB-GigabitEthernet3/0/1] ip address 10.1.1.2 24
[SwitchB-GigabitEthernet3/0/1] quit
[SwitchB] interface GigabitEthernet 3/0/2
[SwitchB-GigabitEthernet3/0/2] ip address 10.10.1.1 24
```
配置 GigabitEthernet3/0/2 接口工作在 DHCP 中继模式。
```
[SwitchB-GigabitEthernet3/0/2] dhcp select relay
```
配置 DHCP 服务器的地址。
```
[SwitchB-GigabitEthernet3/0/2] dhcp relay server-address 10.1.1.1
```
启用接口授权 ARP 功能。
```
[SwitchB-GigabitEthernet3/0/1] port link-mode route
[SwitchB-GigabitEthernet3/0/2] arp authorized enable
[SwitchB-GigabitEthernet3/0/2] quit
```
开启 DHCP 中继用户地址表项记录功能。
```
[SwitchB] dhcp relay client-information record
```
(3) 配置 Switch C
```
<SwitchC> system-view
[SwitchC] ip route-static 10.1.1.0 24 10.10.1.1
[SwitchC] interface GigabitEthernet 3/0/2
[SwitchC-GigabitEthernet3/0/2] ip address dhcp-alloc
[SwitchC-GigabitEthernet3/0/2] quit
```
4. 验证配置

Switch C 获得 Switch A 分配的 IP 后，在 Switch B 查看授权 ARP 信息。
```
[SwitchB] display arp all
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP Address       MAC Address     VLAN     Interface          Aging Type
10.10.1.2        0012-3f86-e94c  N/A      GE3/0/2             20    D
```
从以上信息可以获知 Switch A 为 Switch C 动态分配的 IP 地址为 10.10.1.2。

此后，Switch C 与 Switch B 通信时采用的 IP 地址、MAC 地址等信息必须和授权 ARP 表项中的一致，否则将无法通信，保证了客户端的合法性。

1.9 配置ARP Detection功能

1.9.1 ARP Detection功能简介

ARP Detection 功能主要应用于接入设备上，对于合法用户的 ARP 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

ARP Detection 包含三个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转发。

1. 用户合法性检查

对于 ARP 信任接口，不进行用户合法性检查；对于 ARP 非信任接口，需要进行用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ARP 报文中源 IP 地址和源 MAC 地址检查用户是否是所属 VLAN 所在接口上的合法用户，包括基于 IP Source Guard 静态绑定表项的检查和基于 DHCP Snooping 表项的检查。只要符合其中的任何一个，就认为该 ARP 报文合法，进行转发。如果所有检查都没有找到匹配的表项，则认为是非法报文，直接丢弃。

IP Source Guard 静态绑定表项通过 **ip source binding** 命令生成，详细介绍请参见“安全配置指导”中的“IP Source Guard”。DHCP Snooping 安全表项通过 DHCP Snooping 功能自动生成，详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。

2. ARP报文有效性检查

对于 ARP 信任接口，不进行报文有效性检查；对于 ARP 非信任接口，需要根据配置对 MAC 地址和 IP 地址不合法的报文进行过滤。可以选择配置源 MAC 地址、目的 MAC 地址或 IP 地址检查模式。

- 源 MAC 地址的检查模式：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文；
- 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：会检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，需要被丢弃；
- IP 地址检查模式：会检查 ARP 报文中的源 IP 或目的 IP 地址，如全 1 或者组播 IP 地址都是不合法的，需要被丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

3. ARP报文强制转发

对于从 ARP 信任接口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任接口接收到的并且已经通过用户合法性检查的 ARP 报文的处理过程如下：

- 对于 ARP 请求报文，通过信任接口进行转发；
- 对于 ARP 应答报文，首先按照报文中的以太网目的 MAC 地址进行转发，若在 MAC 地址表中没有查到目的 MAC 地址对应的表项，则将此 ARP 应答报文通过信任接口进行转发。

说明

- ARP 报文强制转发功能不支持目的 MAC 地址为多端口 MAC 的情况。
- 如果既配置了报文有效性检查功能，又配置了用户合法性检查功能，那么先进行报文有效性检查，然后进行用户合法性检查。

1.9.2 配置ARP Detection功能

1. 配置用户合法性检查功能

配置用户合法性检查功能时，必须至少配置 IP Source Guard 静态绑定表项和 DHCP Snooping 功能检查二者之一，否则所有从 ARP 非信任接口收到的 ARP 报文都将被丢弃。

在配置 IP Source Guard 静态绑定表项时，必须指定 VLAN 参数，否则 ARP 报文将无法通过基于 IP Source Guard 静态绑定表项的检查。

表1-11 配置用户合法性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP Detection功能	**arp detection enable**	缺省情况下，ARP Detection功能处于关闭状态，即不进行用户合法性检查
退回系统视图	**quit**	-
进入二层以太网接口或者二层聚合接口视图	**interface** *interface-type interface-number*	-
（可选）将不需要进行用户合法性检查的接口配置为ARP信任接口	**arp detection trust**	缺省情况下，接口为ARP非信任接口

2. 配置ARP报文有效性检查功能

表1-12 配置 ARP 报文有效性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP Detection功能	**arp detection enable**	缺省情况下，ARP Detection功能处于关闭状态
退回系统视图	**quit**	-
使能ARP报文有效性检查功能	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	缺省情况下，对ARP报文的目的MAC地址或源MAC地址、IP地址的有效性检查功能处于关闭状态
进入二层以太网接口或者二层聚合接口视图	**interface** *interface-type interface-number*	-
（可选）将不需要进行ARP报文有效性检查的接口配置为ARP信任接口	**arp detection trust**	缺省情况下，接口为ARP非信任接口

3. 配置ARP报文强制转发功能

进行下面的配置之前，需要保证已经配置了用户合法性检查功能。

表1-13 配置 ARP 报文强制转发功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP报文强制转发功能	**arp restricted-forwarding enable**	缺省情况下，ARP报文强制转发功能处于关闭状态

1.9.3 ARP Detection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 ARP Detection 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **reset** 命令清除 ARP Detection 的统计信息。

表1-14 ARP Detection 显示和维护

操作	命令
显示使能了ARP Detection功能的VLAN	**display arp detection**
显示ARP Detection功能报文检查的丢弃计数的统计信息	**display arp detection statistics** [**interface** *interface-type interface-number*]
清除ARP Detection的统计信息	**reset arp detection statistics** [**interface** *interface-type interface-number*]

1.9.4 用户合法性检查和报文有效性检查配置举例

说明

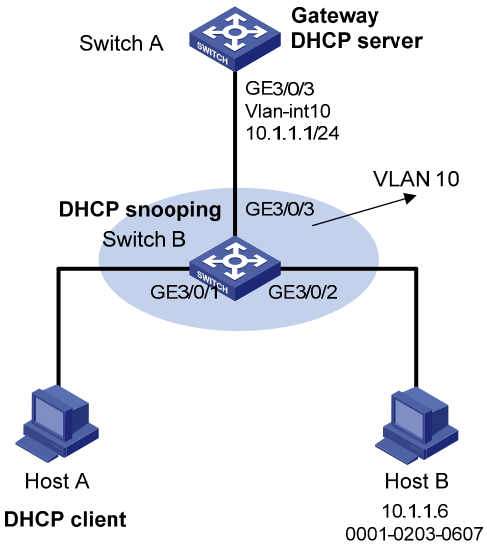
缺省情况下，以太网接口、VLAN 接口及聚合接口处于 DOWN 状态。如果要使这些接口能够正常工作，请先使用 **undo shutdown** 命令使接口状态处于 UP。

1. 组网需求

- Switch A 是 DHCP 服务器；
- Host A 是 DHCP 客户端；用户 Host B 的 IP 地址是 10.1.1.6，MAC 地址是 0001-0203-0607。
- Switch B 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端和用户进行用户合法性检查和报文有效性检查。

2. 组网图

图1-5 配置用户合法性检查和报文有效性检查组网图



3. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 及 Switch A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Switch A

配置 DHCP 地址池 0。

```
<SwitchA> system-view
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

(3) 配置 DHCP 客户端 Host A 和用户 Host B（略）

(4) 配置设备 Switch B

启用 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
[SwitchB] interface GigabitEthernet 3/0/3
[SwitchB-GigabitEthernet3/0/3] dhcp snooping trust
[SwitchB-GigabitEthernet3/0/3] quit
```

在接口 GigabitEthernet3/0/1 上启用 DHCP Snooping 表项记录功能。

```
[SwitchB] interface GigabitEthernet 3/0/1
[SwitchB-GigabitEthernet3/0/1] dhcp snooping binding record
[SwitchB-GigabitEthernet3/0/1] quit
```

使能 ARP Detection 功能，对用户合法性进行检查。

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
```

接口状态缺省为非信任状态，上行接口配置为信任状态，下行接口按缺省配置。

```
[SwitchB-vlan10] interface GigabitEthernet 3/0/3
```

```
[SwitchB-GigabitEthernet3/0/3] arp detection trust
[SwitchB-GigabitEthernet3/0/3] quit
```

在接口 GigabitEthernet3/0/2 上配置 IP Source Guard 静态绑定表项。

```
[SwitchB] interface GigabitEthernet 3/0/2
[SwitchB-GigabitEthernet3/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[SwitchB-GigabitEthernet3/0/2] quit
```

配置进行报文有效性检查。

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

完成上述配置后，对于接口 GigabitEthernet3/0/1 和 GigabitEthernet3/0/2 收到的 ARP 报文，先进行报文有效性检查，然后基于 IP Source Guard 静态绑定表项、DHCP Snooping 安全表项进行用户合法性检查。

1.9.5 ARP报文强制转发配置举例

说明

缺省情况下，以太网接口、VLAN 接口及聚合接口处于 DOWN 状态。如果要使这些接口能够正常工作，请先使用 **undo shutdown** 命令使接口状态处于 UP。

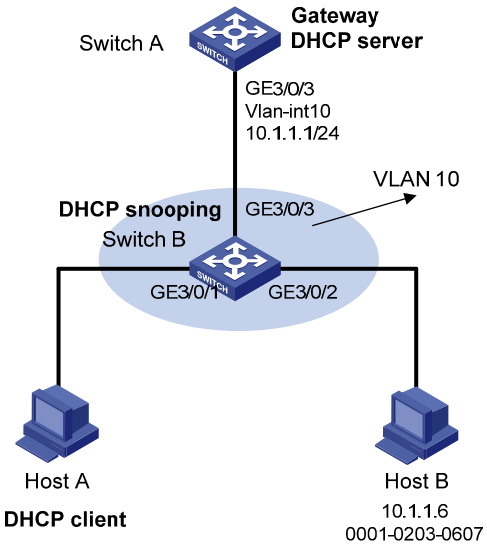
1. 组网需求

- Switch A 是 DHCP 服务器。
- Host A 是 DHCP 客户端；用户 Host B 的 IP 地址是 10.1.1.6，MAC 地址是 0001-0203-0607。
- Host A 和 Host B 在设备 Switch B 上端口隔离，但是均和网关 Switch A 相通，GigabitEthernet3/0/1、GigabitEthernet3/0/2、GigabitEthernet3/0/3 均属于 VLAN 10。
- Switch B 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端和用户进行保护，保证合法用户可以正常转发报文，否则丢弃。

要求：Switch B 在启用 ARP Detection 功能后，对于 ARP 广播请求报文仍然能够进行端口隔离。

2. 组网图

图1-6 配置 ARP 报文强制转发组网图



3. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 及 Switch A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Switch A

配置 DHCP 地址池 0。

```
<SwitchA> system-view
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

(3) 配置 DHCP 客户端 Host A 和用户 Host B（略）

(4) 配置设备 Switch B

配置 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
[SwitchB] interface GigabitEthernet 3/0/3
[SwitchB-GigabitEthernet3/0/3] dhcp snooping trust
[SwitchB-GigabitEthernet3/0/3] quit
```

使能 ARP Detection 功能，对用户合法性进行检查。

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
```

配置上行接口为信任状态，下行接口为缺省配置（非信任状态）。

```
[SwitchB-vlan10] interface GigabitEthernet 3/0/3
[SwitchB-GigabitEthernet3/0/3] arp detection trust
[SwitchB-GigabitEthernet3/0/3] quit
```

在接口 GigabitEthernet3/0/2 上配置 IP Source Guard 静态绑定表项。

```
[SwitchB] interface GigabitEthernet 3/0/2
```

```
[SwitchB-GigabitEthernet3/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[SwitchB-GigabitEthernet3/0/2] quit
```

配置进行报文有效性检查。

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

配置端口隔离。

```
[SwitchB] port-isolate group 1
[SwitchB] interface GigabitEthernet 3/0/1
[SwitchB-GigabitEthernet3/0/1] port-isolate enable group 1
[SwitchB-GigabitEthernet3/0/1] quit
[SwitchB] interface GigabitEthernet 3/0/2
[SwitchB-GigabitEthernet3/0/2] port-isolate enable group 1
[SwitchB-GigabitEthernet3/0/2] quit
```

完成上述配置后，对于接口 GigabitEthernet3/0/1 和 GigabitEthernet3/0/2 收到的 ARP 报文，先进行报文有效性检查，然后基于 IP Source Guard 静态绑定表项、DHCP Snooping 安全表项进行用户合法性检查。但是，Host A 发往 Switch A 的 ARP 广播请求报文，由于通过了用户合法性检查，所以能够被转发到 Host B，端口隔离功能失效。

配置 ARP 报文强制转发功能。

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp restricted-forwarding enable
[SwitchB-vlan10] quit
```

此时，Host A 发往 Switch A 的合法 ARP 广播请求报文只能通过信任接口 GigabitEthernet3/0/3 转发，不能被 Host B 接收到，端口隔离功能可以正常工作。

1.10 配置ARP自动扫描、固化功能

1.10.1 ARP自动扫描、固化功能简介

ARP 自动扫描功能一般与 ARP 固化功能配合使用：

- 启用 ARP 自动扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，从而建立动态 ARP 表项）。
- ARP 固化功能用来将当前的 ARP 动态表项（包括 ARP 自动扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效防止攻击者修改 ARP 表项。

说明

建议在网吧这种环境稳定的小型网络中使用这两个功能。

1.10.2 配置ARP自动扫描、固化功能

配置 ARP 自动扫描、固化功能时，需要注意：

- 对于已存在 ARP 表项的 IP 地址不进行扫描。
- 扫描操作可能比较耗时，用户可以通过<Ctrl_C>来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。

- 固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同。
- 固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。

表1-15 配置 ARP 自动扫描、固化功能

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*	-
启动ARP自动扫描功能	**arp scan** [*start-ip-address* **to** *end-ip-address*]	-
退回系统视图	**quit**	-
配置ARP固化功能	**arp fixup**	-

说明

- 通过 **arp fixup** 命令将当前的动态 ARP 表项转换为静态 ARP 表项后，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。
- 通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp** *ip-address* [*vpn-instance-name*] 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

1.11 配置ARP网关保护功能

1.11.1 ARP网关保护功能简介

在设备上不与网关相连的接口上配置此功能，可以防止伪造网关攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。

1.11.2 配置ARP网关保护功能

配置 ARP 网关保护功能，需要注意：

- 每个接口最多支持配置 8 个被保护的网关 IP 地址。
- 不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection、ARP Snooping 和 ARP 快速应答功能配合使用时，先进行本功能检查，本功能检查通过后才会进行其他配合功能的处理。

表1-16 配置 ARP 网关保护功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入二层以太网接口/二层聚合接口视图	**interface** *interface-type interface-number*	-
开启ARP网关保护功能，配置被保护的网关IP地址	**arp filter source** *ip-address*	缺省情况下，ARP网关保护功能处于关闭状态

1.11.3 ARP网关保护功能配置举例

说明

缺省情况下，以太网接口、VLAN 接口及聚合接口处于 DOWN 状态。如果要使这些接口能够正常工作，请先使用 **undo shutdown** 命令使接口状态处于 UP。

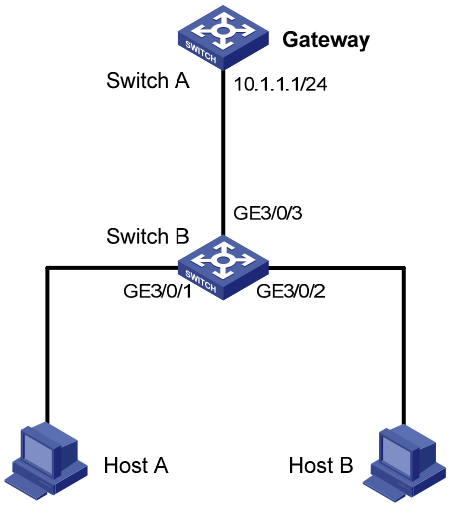
1. 组网需求

与 Switch B 相连的 Host B 进行了仿造网关 Switch A（IP 地址为 10.1.1.1）的 ARP 攻击，导致与 Switch B 相连的设备与网关 Switch A 通信时错误发往了 Host B。

要求：通过配置防止这种仿造网关攻击。

2. 组网图

图1-7 配置 ARP 网关保护功能组网图



3. 配置步骤

在 Switch B 上配置 ARP 网关保护功能。

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 3/0/1
[SwitchB-GigabitEthernet3/0/1] arp filter source 10.1.1.1
[SwitchB-GigabitEthernet3/0/1] quit
[SwitchB] interface GigabitEthernet 3/0/2
```

```
[SwitchB-GigabitEthernet3/0/2] arp filter source 10.1.1.1
```

完成上述配置后，对于 Host B 发送的伪造的源 IP 地址为网关 IP 地址的 ARP 报文将会被丢弃，不会再被转发。

1.12 配置ARP过滤保护功能

1.12.1 ARP过滤保护功能简介

本功能用来限制接口下允许通过的 ARP 报文，可以防止仿冒网关和仿冒用户的攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许通过的 IP 地址和 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理；
- 如果不相同，则认为此报文非法，将其丢弃。

1.12.2 配置ARP过滤保护功能

配置 ARP 过滤保护功能，需要注意：

- 每个接口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。
- 不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection、ARP Snooping 和 ARP 快速应答功能配合使用时，先进行本功能检查，本功能检查通过后才会进行其他配合功能的处理。

表1-17 配置 ARP 过滤保护功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口/二层聚合接口视图	**interface** *interface-type interface-number*	-
开启ARP过滤保护功能，配置允许通过的ARP报文的源IP地址和源MAC地址	**arp filter binding** *ip-address mac-address*	缺省情况下，ARP过滤保护功能处于关闭状态

1.12.3 ARP过滤保护功能配置举例

说明

缺省情况下，以太网接口、VLAN 接口及聚合接口处于 DOWN 状态。如果要使这些接口能够正常工作，请先使用 **undo shutdown** 命令使接口状态处于 UP。

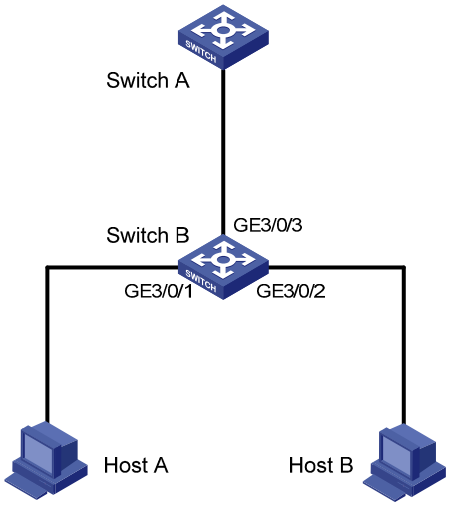
1. 组网需求

- Host A 的 IP 地址为 10.1.1.2，MAC 地址为 000f-e349-1233。
- Host B 的 IP 地址为 10.1.1.3，MAC 地址为 000f-e349-1234。

- 限制 Switch B 的 GigabitEthernet3/0/1、GigabitEthernet3/0/2 接口只允许指定用户接入，不允许其他用户接入。

2. 组网图

图1-8 配置 ARP 过滤保护功能组网图



3. 配置步骤

配置 Switch B 的 ARP 过滤保护功能。

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 3/0/1
[SwitchB-GigabitEthernet3/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[SwitchB-GigabitEthernet3/0/1] quit
[SwitchB] interface GigabitEthernet 3/0/2
[SwitchB-GigabitEthernet3/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

完成上述配置后，接口 GigabitEthernet3/0/1 收到 Host A 发出的源 IP 地址为 10.1.1.2、源 MAC 地址为 000f-e349-1233 的 ARP 报文将被允许通过，其他 ARP 报文将被丢弃；接口 GigabitEthernet3/0/2 收到 Host B 发出的源 IP 地址为 10.1.1.3、源 MAC 地址为 000f-e349-1234 的 ARP 报文将被允许通过，其他 ARP 报文将被丢弃。