目 录

1 ARP攻击防御

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。

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

配置任务		说明	详细配置
	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
	配置ARP报文源IP地址检查功能配置	可选 建议在网关上配置本功能	1.13

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 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，并同时发起 ARP 主动探测，如果在黑洞路由老化时间内 ARP 解析成功，则设备马上删除此黑洞路由并开始转发去往该地址的报文，否则设备直接丢弃该报文。在删除黑洞路由之前，后续去往该地址的 IP 报文都将被直接丢弃。用户可以通过命令配置 ARP 请求报文的发送次数和发送时间间隔。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则进行转发，否则仍然产生一个黑洞路由将去往该地址的报文丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。

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**	-
开启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**	-
开启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
（可选）配置发送ARP请求报文的次数	**arp resolving-route probe-count** *count*	缺省情况下，发送ARP请求报文的次数为3次
（可选）配置发送ARP请求报文的时间间隔	**arp resolving-route probe-interval** *interval*	缺省情况下，发送ARP请求报文的时间间隔为1秒

说明

- 当用户配置的 ARP 主动探测总时长（发送次数×发送时间间隔）大于黑洞路由老化时间时，系统只会取小于等于该老化时间的最大值作为真正的探测总时长。
- 当发起 ARP 主动探测过程结束且生成的黑洞路由还未老化时，设备无法主动对黑洞路由对应的设备进行 ARP 解析，为了缓解该问题，用户可以配置较大的发送 ARP 请求报文次数。

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

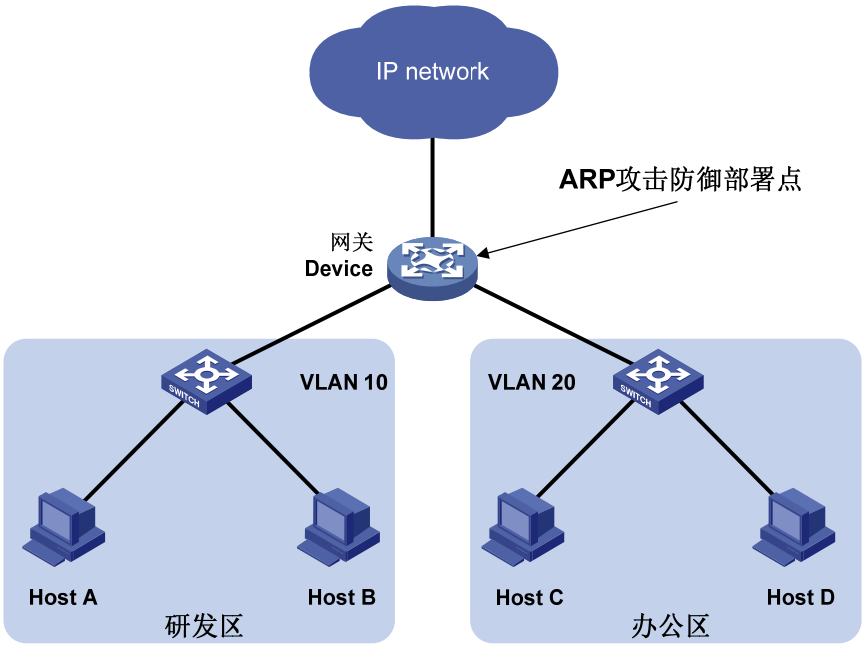
1. 组网需求

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Device，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 Device 上做如下配置：

- 开启 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 Device 上配置 ARP 黑洞路由功能。

4. 配置步骤

- 配置 ARP 源抑制功能

开启 ARP 源抑制功能，并配置 ARP 源抑制的阈值为 100。

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

- 配置 ARP 黑洞路由功能

开启 ARP 黑洞路由功能。

```
[Device] 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，这个时候可以配置 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，或者发现有 ARP 泛洪攻击的情况下，配置 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** *interval*	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/三层以太网接口/三层聚合接口视图	**interface** *interface-type interface-number*	-
开启ARP报文限速功能，并设置ARP报文限速速率	**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。当开启了 ARP 日志信息功能（配置 **arp check log enable** 命令），且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。关于 ARP 日志信息功能的详细描述，请参见“三层技术-IP 业务配置指导”中的“ARP”。

切换源 MAC 地址固定的 ARP 攻击检查模式时，如果从监控模式切换到过滤模式，过滤模式马上生效；如果从过滤模式切换到监控模式，已生成的攻击检测表项，到表项老化前还会继续按照过滤模式处理。

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或过滤。

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**	-
开启源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报文攻击检测的阈值为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*&<1-10>	缺省情况下，未配置任何保护MAC地址

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	**display arp source-mac** { **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

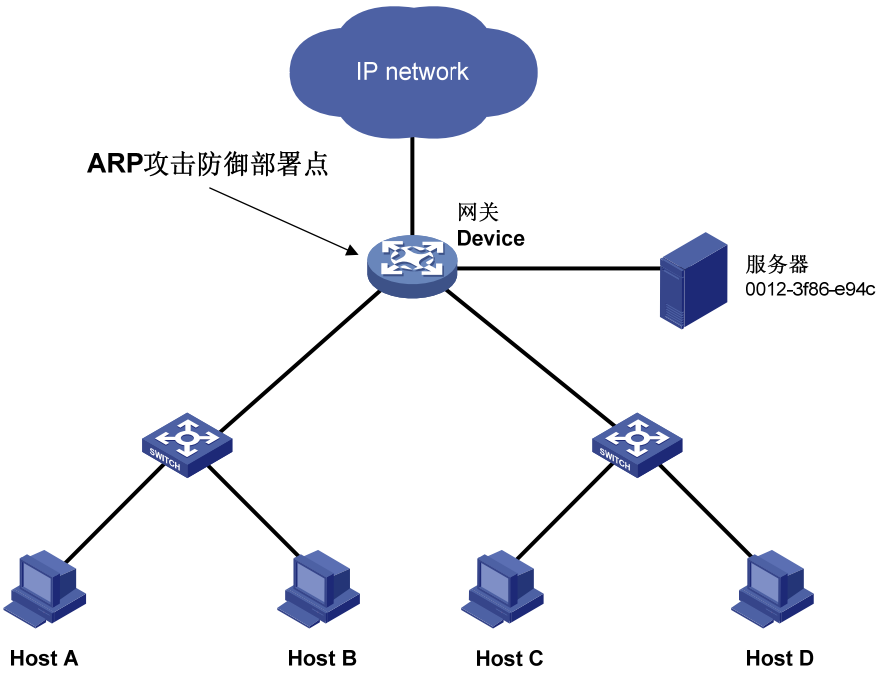
1. 组网需求

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：

- 开启源 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

开启源 MAC 固定 ARP 攻击检测功能，并选择过滤模式。

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

配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。

```
[Device] 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。

```
[Device] 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。

```
[Device] 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 开启ARP报文源MAC地址一致性检查功能

表1-8 开启 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**	-
开启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

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。

配置 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。

配置严格模式后，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 地址为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但不建立 ARP 表项；

- 收到 ARP 应答报文时，需要确认本设备是否对该报文中的源 IP 地址发起过 ARP 解析：若发起过解析，解析成功后则设备启动主动确认功能，主动确认流程成功完成后，设备可以建立该表项；若未发起过解析，则设备丢弃该报文。

1.7.2 开启ARP主动确认功能

表1-9 开启 ARP 主动确认功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
开启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

说明

在严格模式下，只有 ARP 黑洞路由功能处于开启状态，ARP 主动确认功能才能生效。

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”。

配置接口的授权 ARP 功能后，系统会禁止该接口学习动态 ARP 表项，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 开启授权ARP功能

表1-10 开启授权 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、三层聚合接口或VLAN接口视图	**interface** *interface-type interface-number*	-
开启授权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

1.9 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 包含四个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转发、ARP Detection 支持 VSI。

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，包括基于用户合法性规则检查、IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 表项的检查和基于 802.1X 安全表项的检查。设备收到 ARP 报文后，首先进行基于用户合法性规则检查，如果找到与报文匹配的规则，则按照该规则对报文进行处理；如果未找到与报文匹配的规则，则继续进行基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 表项的检查和基于 802.1X 安全表项的检查。只要符合三者中的任何一个，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”。

说明

802.1X 安全表项通过 802.1X 功能产生，802.1X 用户需要使用支持将 IP 地址上传的客户端，用户通过了 802.1X 认证并且将 IP 地址上传至配置 ARP Detection 的设备后，设备自动生成可用于 ARP Detection 的用户合法性检查的 802.1X 安全表项。802.1X 的详细介绍请参见“安全配置指导”中的“802.1X”。

---

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。

4. ARP Detection支持VSI

在 VXLAN 组网中，用户可以在 VTEP 设备上的 VSI 内配置用户合法性检查和 ARP 报文有效性检查。与 VLAN 内不同的是，在 VLAN 内，这两项检查针对的是 ARP 非信接口，而在 VSI 内，这两项检查均针对的是 ARP 非信任 AC。在 VXLAN 中，与 VSI 关联的以太网服务实例统称为 AC（Attachment Circuit，接入电路），详细介绍请参见“VXLAN”。

VSI 内的用户合法性检查和 ARP 报文有效性检查所依赖的安全表项和检查过程与 VLAN 环境下的相同。

1.9.2 配置限制和指导

- 配置用户合法性检查功能时，必须至少配置用户合法性规则或者 IP Source Guard 静态绑定表项、DHCP Snooping 功能和 802.1X 功能三者之一，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 IP、MAC 和 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。
- ARP Detection 功能与 ARP Snooping 功能不能同时配置，否则会导致 ARP Snooping 表项无法生成。

1.9.3 配置ARP Detection功能

1. 配置VLAN内用户合法性检查功能

表1-11 配置 VLAN 内用户合法性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置用户合法性检查规则	**arp detection rule** *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]	缺省情况下，未配置用户合法性检查规则
进入VLAN视图	**vlan** *vlan-id*	-

操作	命令	说明
开启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**	-
（可选）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VLAN内ARP报文有效性检查功能

表1-12 配置 VLAN 内 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*	-
开启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**	-
开启ARP报文有效性检查功能	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	缺省情况下，ARP报文有效性检查功能处于关闭状态
（可选）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. 配置在VLAN内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 VLAN 内 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*	-
开启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

1.9.4 配置VSI内ARP Detection功能

1. 配置VSI内用户合法性检查功能

表1-14 配置 VSI 内用户合法性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置用户合法性检查规则	**arp detection rule** *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]	缺省情况下，未配置用户合法性检查规则
进入VSI视图	**vsi** *vsi-name*	-
开启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**	-
（可选）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）进入以太网服务实例视图	**service-instance** *instance-id*	-
（可选）配置ARP信任AC	**arp detection trust**	缺省情况下，AC为ARP非信任服AC

2. 配置VSI内ARP报文有效性检查功能

表1-15 配置 VSI 内 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VSI视图	**vsi** *vsi-name*	-
开启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**	-
开启ARP报文有效性检查功能	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	缺省情况下，ARP报文有效性检查功能处于关闭状态
（可选）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）进入以太网服务实例视图	**service-instance** *instance-id*	-
（可选）配置ARP信任AC	**arp detection trust**	缺省情况下，AC为ARP非信任AC

1.9.5 配置ARP Detection日志功能

配置 ARP Detection 日志功能后，设备在检测到非法 ARP 报文时将生成检测日志，日志内容包括：

- 受到攻击的端口编号；

- 非法 ARP 报文的源 IP 地址；
- 丢弃的 ARP 报文总数。

表1-16 开启 ARP Detection 日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启ARP Detection日志功能	**arp detection log enable**	缺省情况下，ARP Detection日志功能处于关闭状态

1.9.6 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1-17 ARP Detection 显示和维护

操作	命令
显示开启了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* [**service-instance** *service-instance-id*]]
清除ARP Detection的统计信息	**reset arp detection statistics** [**interface** *interface-type interface-number* [**service-instance** *service-instance-id*]]

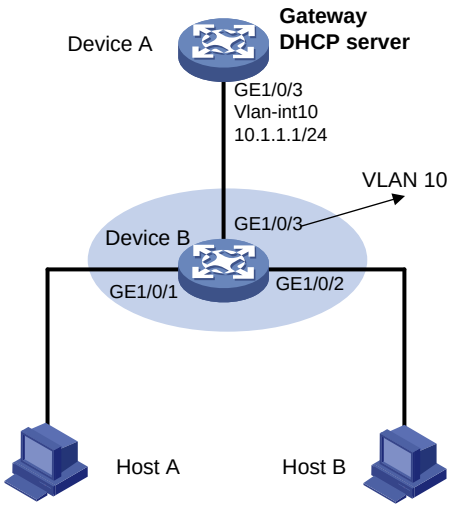
1.9.7 用户合法性检查配置举例

1. 组网需求

- Device A 是 DHCP 服务器；Device B 是支持 802.1X 的设备，在 VLAN 10 内配置 ARP Detection 功能，对认证客户端进行保护，保证合法用户可以正常转发报文，否则丢弃。
- Host A 和 Host B 是本地 802.1X 接入用户。

2. 组网图

图1-3 配置用户合法性检查组网图



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 Device A

配置 DHCP 地址池 0。

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

(3) 配置客户端 Host A 和 Host B（略），必须使用上传 IP 地址方式。

(4) 配置设备 Device B

配置 802.1X 功能。

```
<DeviceB> system-view
[DeviceB] dot1x
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dot1x
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dot1x
[DeviceB-GigabitEthernet1/0/2] quit
```

添加本地接入用户。

```
[DeviceB] local-user test
[DeviceB-luser-test] service-type lan-access
[DeviceB-luser-test] password simple test
[DeviceB-luser-test] quit
```

开启 ARP Detection 功能，对用户合法性进行检查。

```
[DeviceB] vlan 10
[DeviceB-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。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

完成上述配置后，对于接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的 ARP 报文，需基于 802.1X 安全表项进行用户合法性检查。

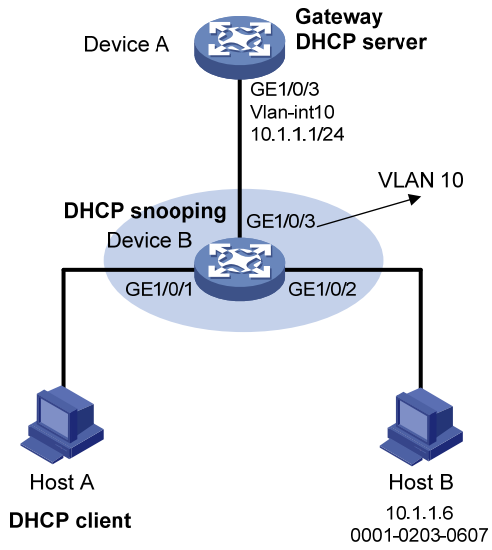
1.9.8 用户合法性检查和报文有效性检查配置举例

1. 组网需求

- Device 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。
- Device B 是 DHCP Snooping 设备，在 VLAN 10 内配置 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1-4 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 Device A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Device A

配置 DHCP 地址池 0。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-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 Device B

开启 DHCP Snooping 功能。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

在接口 GigabitEthernet1/0/1 上开启 DHCP Snooping 表项记录功能。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping binding record
[DeviceB-GigabitEthernet1/0/1] quit
```

开启 ARP Detection 功能，对用户合法性进行检查。

```
[DeviceB] vlan 10
[DeviceB-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。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

在接口 GigabitEthernet1/0/2 上配置 IP Source Guard 静态绑定表项。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

配置进行报文有效性检查。

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

完成上述配置后，对于接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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。

1.9.9 ARP报文强制转发配置举例

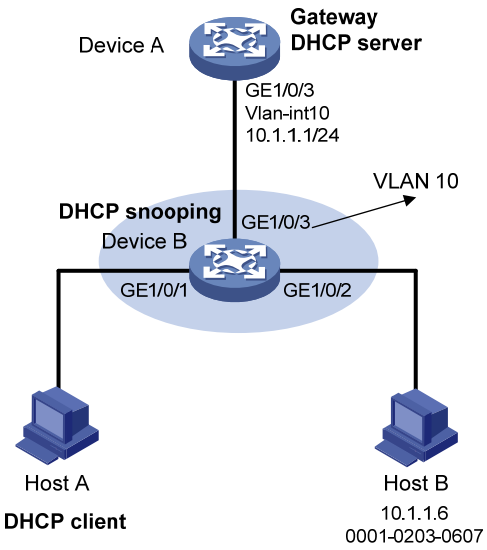
1. 组网需求

- Device 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 Device B 上端口隔离，但是均和网关 Device A 相通，GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 均属于 VLAN 10。
- Device B 是 DHCP Snooping 设备，在 VLAN 10 内开启 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：Device B 在开启 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1-5 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 Device A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Device A

配置 DHCP 地址池 0。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-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 Device B

开启 DHCP Snooping 功能。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

开启 ARP Detection 功能，对用户合法性进行检查。

```
[DeviceB] vlan 10
[DeviceB-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）。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

在接口 GigabitEthernet1/0/2 上配置 IP Source Guard 静态绑定表项。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

配置进行报文有效性检查。

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

配置端口隔离。

```
[DeviceB] port-isolate group 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port-isolate enable group 1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port-isolate enable group 1
[DeviceB-GigabitEthernet1/0/2] quit
```

完成上述配置后，对于接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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 Device 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。

开启 ARP 报文强制转发功能。

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

此时，Host A 发往 Device A 的合法 ARP 广播请求报文只能通过信任接口 GigabitEthernet1/0/3 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：

- 配置 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 开启ARP自动扫描、固化功能

开启 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1-18 开启 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*	-
开启ARP自动扫描功能	**arp scan** [*start-ip-address* **to** *end-ip-address*]	-
退回系统视图	**quit**	-
将设备上的动态ARP表项转化成静态ARP表项	**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* 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。

在接口上开启此功能后，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 开启ARP网关保护功能

开启 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 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1-19 开启 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

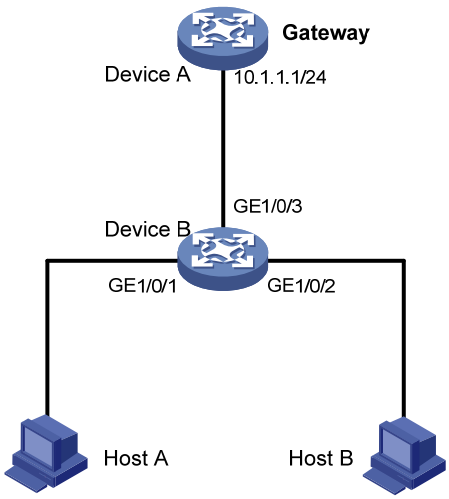
1. 组网需求

与 Device B 相连的 Host B 进行了仿造网关 Device A（IP 地址为 10.1.1.1）的 ARP 攻击，导致与 Device B 相连的设备与网关 Device 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1-6 配置 ARP 网关保护功能组网图



3. 配置步骤

在 Device B 上开启 ARP 网关保护功能。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] 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 开启ARP过滤保护功能

开启 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 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1-20 开启 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

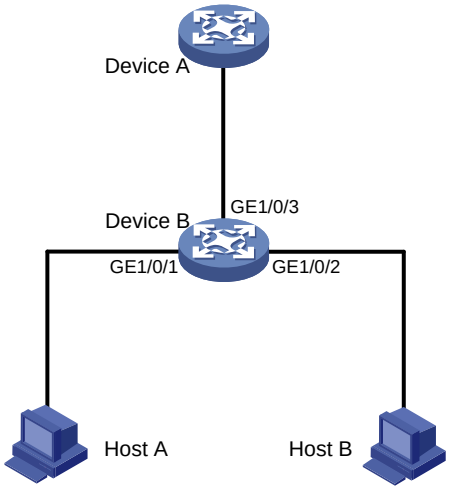
1.12.3 ARP过滤保护功能配置举例

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 Device B 的 GigabitEthernet1/0/1、GigabitEthernet1/0/2 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1-7 配置 ARP 过滤保护功能组网图



3. 配置步骤

开启 Device B 的 ARP 过滤保护功能。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

完成上述配置后，接口 GigabitEthernet1/0/1 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 GigabitEthernet1/0/2 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。

1.13 配置ARP报文源IP地址检查功能

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。如果指定 VLAN 内的 ARP 报文的 sender IP 不在指定源 IP 地址范围内，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

表1-21 配置 ARP 报文源 IP 地址检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
配置可接受的ARP报文中sender IP的地址范围	**arp sender-ip-range** *start-ip-address end-ip-address*	缺省情况下，未限制ARP报文中sender IP的地址范围

说明

- 当 Super VLAN 与 Sub VLAN 间建立映射关系时，本特性在 Sub VLAN 内配置。
- 如果 Primary VLAN 下配置了指定的 Secondary VLAN 间三层互通，则本特性需要配置在 Primary VLAN 中；如果 Primary VLAN 下未配置 Secondary VLAN 间三层互通，则本特性可以在 Primary VLAN 和 Secondary VLAN 中分别配置。