目 录

1 ARP攻击防御配置

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
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	1.5
	配置 ARP 主动确认功能		可选 建议在网关设备上配置本功能	1.6
	配置授权 ARP 功能		可选 建议在网关设备上配置本功能	1.7
	配置 ARP Detection 功能		可选 建议在接入设备上配置本功能	1.8
	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	1.9
	配置 ARP 网关保护功能		可选 建议在接入设备上配置本功能	1.10

配置任务		说明	详细配置
	配置 ARP 过滤保护功能	可选 建议在接入设备上配置本功能	1.11

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：

- 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，如果网络中某主机向设备某端口连续发送目标 IP 地址不能解析的 IP 报文，当每 5 秒内由此主机发出 IP 报文触发的 ARP 请求报文的流量超过设置的阈值，那么对于由此主机发出的 IP 报文，设备不允许其触发 ARP 请求，直至 5 秒后再处理，从而避免了恶意攻击所造成的危害。
- 如果发送攻击报文的源不固定，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，使得设备在一段时间内将去往该地址的报文直接丢弃。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**	-
使能 ARP 源抑制功能	**arp source-suppression enable**	必选 缺省情况下，关闭 ARP 源抑制功能
配置 ARP 源抑制的阈值	**arp source-suppression limit** *limit-value*	可选 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**	-

操作	命令	说明
使能 ARP 黑洞路由功能	**arp resolving-route enable**	必选 缺省情况下，关闭 ARP 黑洞路由功能

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 源抑制显示和维护

操作	命令
显示 ARP 源抑制的配置信息	**display arp source-suppression** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.3.4 ARP防止IP报文攻击配置举例

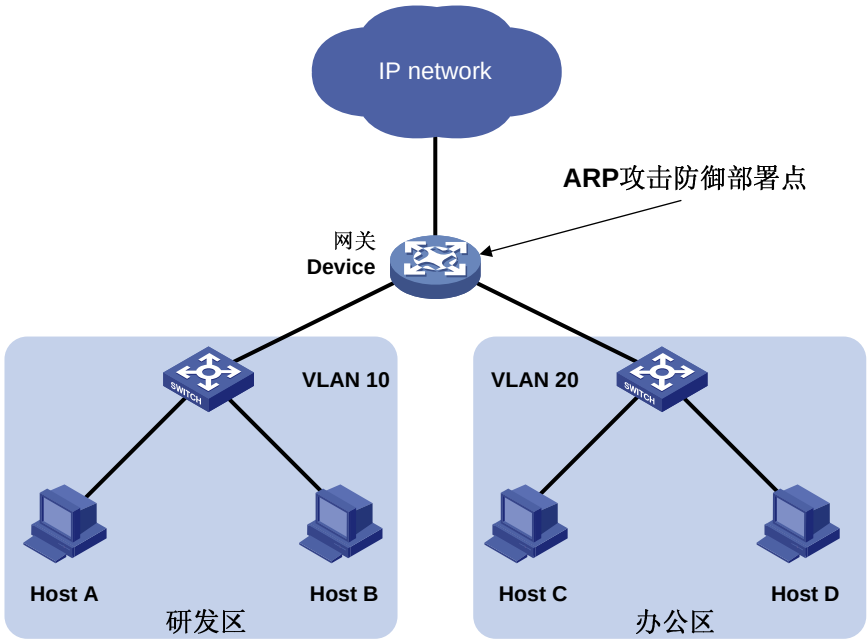
1. 组网需求

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：

- 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。

否则采用 ARP 黑洞路由功能，在 Device 上配置 ARP 黑洞路由功能。

4. 配置步骤

(1) 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。

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

(2) 配置 ARP 黑洞路由功能

使能 ARP 黑洞路由功能。

```
<Device> system-view
[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，这个时候可以启用 ARP 报文限速功能来控制上送 CPU 的 ARP 报文的速率。

推荐用户在配置了 ARP Detection、ARP Snooping、ARP 快速应答、MFF，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（在系统视图下配置限速）

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**	-
开启 ARP 报文限速功能（集中式设备）	**arp rate-limit** { **disable** | **rate** *pps* **drop** }	必选 缺省情况下，开启 ARP 报文限速功能，限速速率为 5～8192pps
开启 ARP 报文限速功能（分布式设备）	**arp rate-limit** { **disable** | **rate** *pps* **drop** } [**slot** *slot-number*]	必选 缺省情况下，开启 ARP 报文限速功能，限速速率为 5～8192pps

1.5 配置ARP报文源MAC地址一致性检查功能

1.5.1 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。

1.5.2 配置ARP报文源MAC地址一致性检查功能

表1-6 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 anti-attack valid-check enable**	必选 缺省情况下，关闭 ARP 报文源 MAC 地址一致性检查功能

1.6 配置ARP主动确认功能

1.6.1 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。

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。关于工作原理的详细介绍请参见“ARP 攻击防范技术白皮书”。

1.6.2 配置ARP主动确认功能

表1-7 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 anti-attack active-ack enable**	必选 缺省情况下，关闭 ARP 主动确认功能

1.7 配置授权ARP功能

说明

- 本特性目前仅支持三层以太网接口。
- 关于 DHCP 服务器的介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”。
- 关于 DHCP 中继的介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。

1.7.1 授权ARP功能简介

所谓授权 ARP（Authorized ARP），就是根据 DHCP 服务器生成的租约或者 DHCP 中继生成的安全表项同步生成 ARP 表项。

使能接口的授权 ARP 功能后：

- 系统会启动接口下授权 ARP 表项的老化探测功能，可以检测用户的非正常下线；
- 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。

说明

静态 ARP 表项可以覆盖授权 ARP 表项，授权 ARP 表项可以覆盖动态 ARP 表项，但是授权 ARP 表项不能覆盖静态 ARP 表项，动态 ARP 表项不能覆盖授权 ARP 表项。

1.7.2 配置授权ARP功能

表1-8 配置授权 ARP 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 DHCP 服务器（DHCP 中继）支持授权 ARP 功能	**dhcp update arp**	必选 缺省情况下，DHCP 服务器（DHCP 中继）不支持授权 ARP 功能
使能授权 ARP 功能	**arp authorized enable**	必选 缺省情况下，接口下没有使能授权 ARP 功能
配置授权 ARP 表项的老化时间	**arp authorized time-out** *seconds*	可选 缺省情况下，接口下授权 ARP 表项的老化时间为 1200 秒

说明

如果 DHCP 服务器（DHCP 中继）不支持授权 ARP 功能，当配置了 **arp authorized enable** 命令后，只是会禁止该接口学习动态 ARP 表项，不会同步生成授权 ARP 表项。

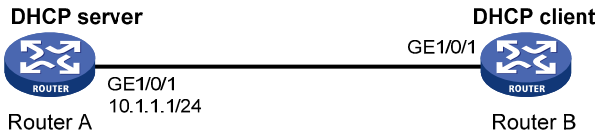
1.7.3 授权ARP功能在DHCP服务器上的典型配置举例

1. 组网需求

- Router 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 GigabitEthernet1/0/1 上启用授权 ARP 功能对客户端进行老化探测，并保证客户端的合法性。
- Router 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1-2 授权 ARP 功能典型配置组网图



3. 配置步骤

(1) 配置 Router A

配置接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
```

使能 DHCP 服务。

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

进入三层以太网接口视图。

```
[RouterA] interface gigabitethernet 1/0/1
```

使能 DHCP 同步 ARP 表项功能。

```
[RouterA-GigabitEthernet1/0/1] dhcp update arp
```

使能接口授权 ARP 功能。

```
[RouterA-GigabitEthernet1/0/1] arp authorized enable
```

配置接口下授权 ARP 的老化时间。

```
[RouterA-GigabitEthernet1/0/1] arp authorized time-out 120
[RouterA-GigabitEthernet1/0/1] quit
```

(2) 配置 Router B

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address dhcp-alloc
[RouterB-GigabitEthernet1/0/1] quit
```

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

```
[RouterA] display arp all
                Type: S-Static    D-Dynamic    A-Authorized
IP Address       MAC Address      VLAN ID  Interface          Aging  Type
10.1.1.2         0012-3f86-e94c   N/A      GE1/0/1            2      A
```

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

此后，Router B 与 Router 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。

如果 Router B 非正常下线（比如，异常断电），待老化时间过后，Router A 将删除相应的授权 ARP 表项。

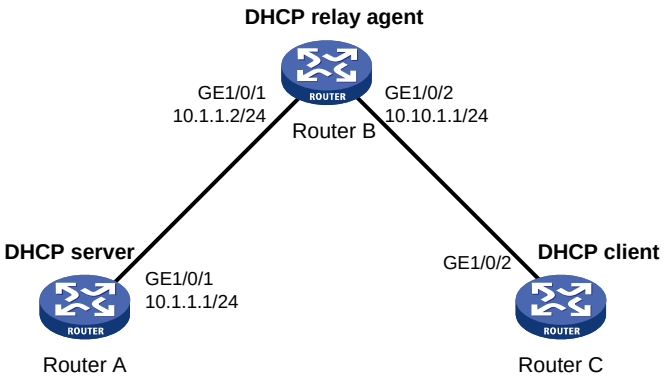
1.7.4 授权ARP功能在DHCP中继上的典型配置举例

1. 组网需求

- Router 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。
- Router B 是 DHCP 中继，通过在接口 GigabitEthernet1/0/2 上启用授权 ARP 功能对客户端进行老化探测，并保证客户端的合法性。
- Router 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1-3 授权 ARP 功能典型配置组网图



3. 配置步骤

(1) 配置 Router A

配置接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
```

使能 DHCP 服务。

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

(2) 配置 Router B

使能 DHCP 服务。

```
<RouterB> system-view
[RouterB] dhcp enable
```

配置接口的 IP 地址。

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ip address 10.10.1.1 24
```

配置 GigabitEthernet1/0/2 接口工作在 DHCP 中继模式。

```
[RouterB-GigabitEthernet1/0/2] dhcp select relay
[RouterB-GigabitEthernet1/0/2] quit
```

配置 DHCP 服务器的地址。

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

配置 GigabitEthernet1/0/2 接口对应 DHCP 服务器组 1。

```
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] dhcp relay server-select 1
```

使能 DHCP 同步 ARP 表项功能。

```
[RouterB-GigabitEthernet1/0/2] dhcp update arp
```

使能接口授权 ARP 功能。

```
[RouterB-GigabitEthernet1/0/2] arp authorized enable
```

配置接口下授权 ARP 的老化时间。

```
[RouterB-GigabitEthernet1/0/2] arp authorized time-out 120
[RouterB-GigabitEthernet1/0/2] quit
```

(3) 配置 Router C

```
<RouterC> system-view
[RouterC] ip route-static 10.1.1.0 24 10.10.1.1
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] ip address dhcp-alloc
[RouterC-GigabitEthernet1/0/2] quit
```

(4) Router C 获得 Router A 分配的 IP 后，在 Router B 查看授权 ARP 信息。

```
[RouterB] display arp all
                Type: S-Static    D-Dynamic    A-Authorized
IP Address       MAC Address     VLAN ID  Interface          Aging Type
10.10.1.2        0012-3f86-e94c  N/A      GE1/0/2             2     A
```

从以上信息可以获知 Router A 为 Router C 动态分配的 IP 地址为 10.10.1.2。

此后，Router C 与 Router 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。

如果 Router C 非正常下线（比如，异常断电），待老化时间过后，Router B 将删除相应的授权 ARP 表项。

1.8 配置ARP Detection功能

说明

本特性仅在 SAP 板工作在二层模式时支持。

1.8.1 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：ARP 报文有效性检查、用户合法性检查、ARP 报文强制转发。

1. ARP报文有效性检查

对于 ARP 信任端口，不进行报文有效性检查；对于 ARP 非信任端口，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。

- 对于源 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；
- 对于目的 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，无效的报文需要被丢弃；
- 对于 IP 地址检查模式，会检查 ARP 报文中的源 IP 和目的 IP 地址，全 0、全 1、或者组播 IP 地址都是不合法的，需要丢弃。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。

2. 用户合法性检查

对于 ARP 信任端口，不进行用户合法性检查；对于 ARP 非信任端口，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 所在端口上的合法用户，包括基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 安全表项的检查、基于 802.1X 安全表项的检查和 OUI MAC 地址的检查。

(1) 首先进行基于 IP Source Guard 静态绑定表项检查。如果找到了对应源 IP 地址和源 MAC 地址的静态绑定表项，认为该 ARP 报文合法，进行转发。如果找到了对应源 IP 地址的静态绑定表项但源 MAC 地址不符，认为该 ARP 报文非法，进行丢弃。如果没有找到对应源 IP 地址的静态绑定表项，继续进行 DHCP Snooping 安全表项、802.1X 安全表项和 OUI MAC 地址检查。

(2) 在基于 IP Source Guard 静态绑定表项检查之后进行基于 DHCP Snooping 安全表项、802.1X 安全表项和 OUI MAC 地址检查，只要符合三者中任何一个，就认为该 ARP 报文合法，进行

转发。其中，OUI MAC 地址检查指的是，只要 ARP 报文的源 MAC 地址为 OUI MAC 地址，并且使能了 Voice VLAN 功能，就认为是合法报文，检查通过。

(3) 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。

说明

- IP Source Guard 静态绑定表项通过 **user-bind** 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”。
- 802.1X 安全表项通过 802.1X 功能产生，详细介绍请参见“安全配置指导”中的“802.1X”。

3. ARP报文强制转发

对于从 ARP 信任端口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任端口接收到的、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，通过信任端口进行转发；
- 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 应答报文通过信任端口进行转发。

1.8.2 配置ARP Detection功能

说明

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. 配置ARP报文有效性检查功能

表1-9 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**	必选 缺省情况下，关闭 ARP Detection 功能
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** } *	必选 缺省情况下，关闭 ARP 报文的有效性检查功能
进入以太网接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
将不需要进行 ARP 报文有效性检查的端口配置为 ARP 信任端口	**arp detection trust**	可选 缺省情况下，端口为 ARP 非信任端口

2. 配置用户合法性检查功能

表1-10 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**	必选 缺省情况下，关闭 ARP Detection 功能。即不进行用户合法性检查
退回系统视图	**quit**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
将不需要进行用户合法性检查的端口配置为 ARP 信任端口	**arp detection trust**	可选 缺省情况下，端口为 ARP 非信任端口

说明

- 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、DHCP Snooping 功能、802.1X 功能三者之一，否则所有从 ARP 非信任端口收到的 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。

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1-11 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**	必选 缺省情况下，ARP 报文强制转发功能处于关闭状态

1.8.3 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1-12 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** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
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*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除 ARP Detection 的统计信息	**reset arp detection statistics** [**interface** *interface-type interface-number*]

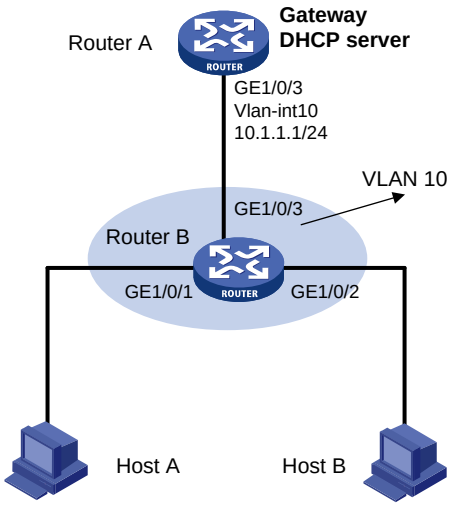
1.8.4 用户合法性检查和报文有效性检查配置举例

1. 组网需求

- Router 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。
- Router 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。

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) 配置组网图中所有端口属于 VLAN 及 Router A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Router A

配置 DHCP 地址池 0。

```
<RouterA> system-view
[RouterA] dhcp enable
[RouterA] dhcp server ip-pool 0
[RouterA-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 Router B

配置 DHCP Snooping 功能。

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

使能 ARP Detection 功能，对用户合法性进行检查。

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

端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。

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

在端口 GigabitEthernet1/0/2 上配置 IP Source Guard 静态绑定表项。

```
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] user-bind ip-address 10.1.1.6 mac-address 0001-0203-0607
vlan 10
[RouterB-GigabitEthernet1/0/2] quit
```

配置进行报文有效性检查。

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

完成上述配置后，对于端口 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。

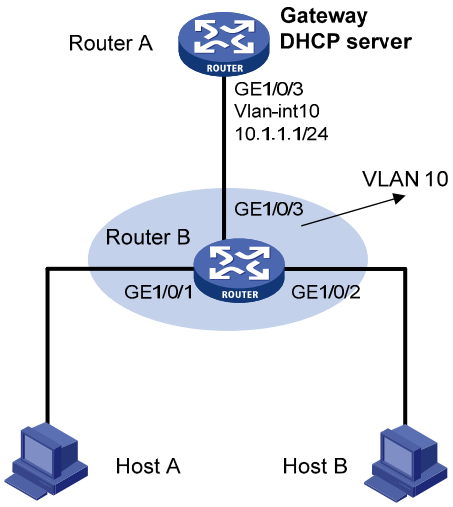
1.8.5 用户合法性检查配置举例

1. 组网需求

- Router A 是 DHCP 服务器；Router B 是支持 802.1X 的设备，在 VLAN 10 内启用 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1-5 配置用户合法性检查组网图



3. 配置步骤

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

(2) 配置 DHCP 服务器 Router A

配置 DHCP 地址池 0。

```
<RouterA> system-view
[RouterA] dhcp enable
[RouterA] dhcp server ip-pool 0
[RouterA-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 Router B

配置 dot1x 功能。

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

添加本地接入用户。

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

使能 ARP Detection 功能，对用户合法性进行检查。

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

端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。

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

完成上述配置后，对于端口 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。

1.8.6 ARP报文强制转发配置举例

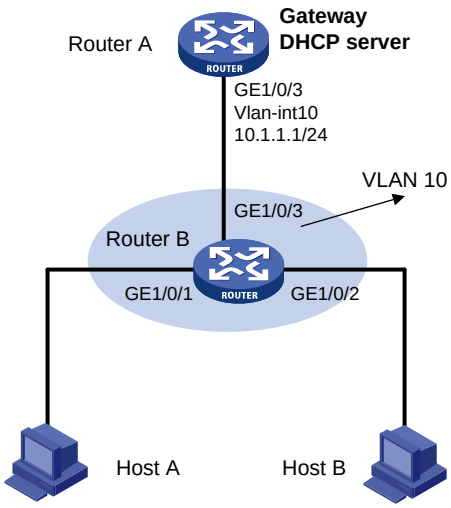
1. 组网需求

- Router 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 Router B 上端口隔离，但是均和网关 Router A 相通，GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 均属于 VLAN 10。
- Router 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：Router 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) 配置组网图中所有端口属于 VLAN 及 Router A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Router A

配置 DHCP 地址池 0。

```
<RouterA> system-view
[RouterA] dhcp enable
[RouterA] dhcp server ip-pool 0
[RouterA-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 Router B

配置 DHCP Snooping 功能。

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

使能 ARP Detection 功能，对用户合法性进行检查。

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

端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。

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

在端口 GigabitEthernet1/0/2 上配置 IP Source Guard 静态绑定表项。

```
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] user-bind ip-address 10.1.1.6 mac-address 0001-0203-0607
vlan 10
[RouterB-GigabitEthernet1/0/2] quit
```

配置进行报文有效性检查。

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

配置端口隔离。

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

完成上述配置后，对于端口 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 Router 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。

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

此时，Host A 发往 Router A 的合法 ARP 广播请求报文只能通过信任端口 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。

1.9 配置ARP自动扫描、固化功能

1.9.1 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，可以有效的防止攻击者修改 ARP 表项。

说明

推荐在网吧这种环境稳定的小型网络中使用这两个功能。

1.9.2 配置ARP自动扫描、固化功能

表1-13 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*]	必选
退回系统视图	**quit**	-
配置 ARP 固化功能	**arp fixup**	必选

说明

- 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。
- 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。
- 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。
- 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。

1.10 配置ARP网关保护功能

1.10.1 ARP网关保护功能简介

在设备上不与网关相连的端口上配置此功能，可以防止伪造网关攻击。

在端口配置此功能后，当端口收到 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。

1.10.2 配置ARP网关保护功能

表1-14 配置 ARP 网关保护功能

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*	必选 缺省情况下，ARP 网关保护功能处于关闭状态


说明

- 每个端口最多支持配置 8 个被保护的网关 IP 地址。
- 不能在同一端口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection、MFF、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。

1.10.3 ARP网关保护功能配置举例

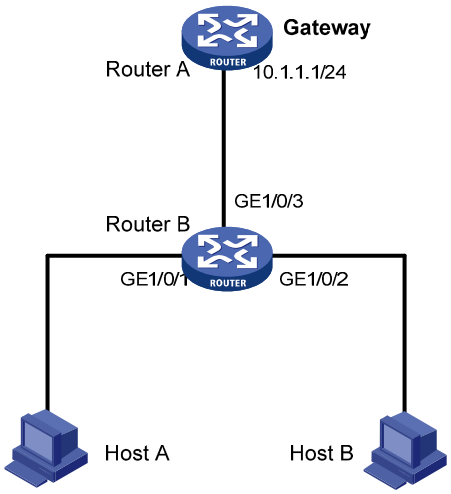
1. 组网需求

与 Router B 相连的 Host B 进行了仿造网关 Router A（IP 地址为 10.1.1.1）的 ARP 攻击，导致与 Router B 相连的设备与网关 Router 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 Router B 上配置 ARP 网关保护功能。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-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。

1.11 配置ARP过滤保护功能

1.11.1 ARP过滤保护功能简介

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

在端口配置此功能后，当端口收到 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。

1.11.2 配置ARP过滤保护功能

表1-15 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视图	**interface** *interface-type interface-number*	-

操作	命令	说明
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*	必选 缺省情况下，ARP 过滤保护功能处于关闭状态

说明

- 每个端口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。
- 不能在同一端口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection、MFF、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。

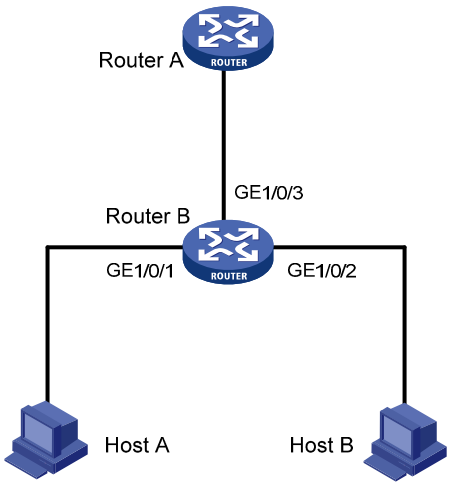
1.11.3 ARP过滤保护功能配置举例

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 Router B 的 GigabitEthernet1/0/1、GigabitEthernet1/0/2 端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 Router B 的 ARP 过滤保护功能。

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

```
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

完成上述配置后，端口 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；端口 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。