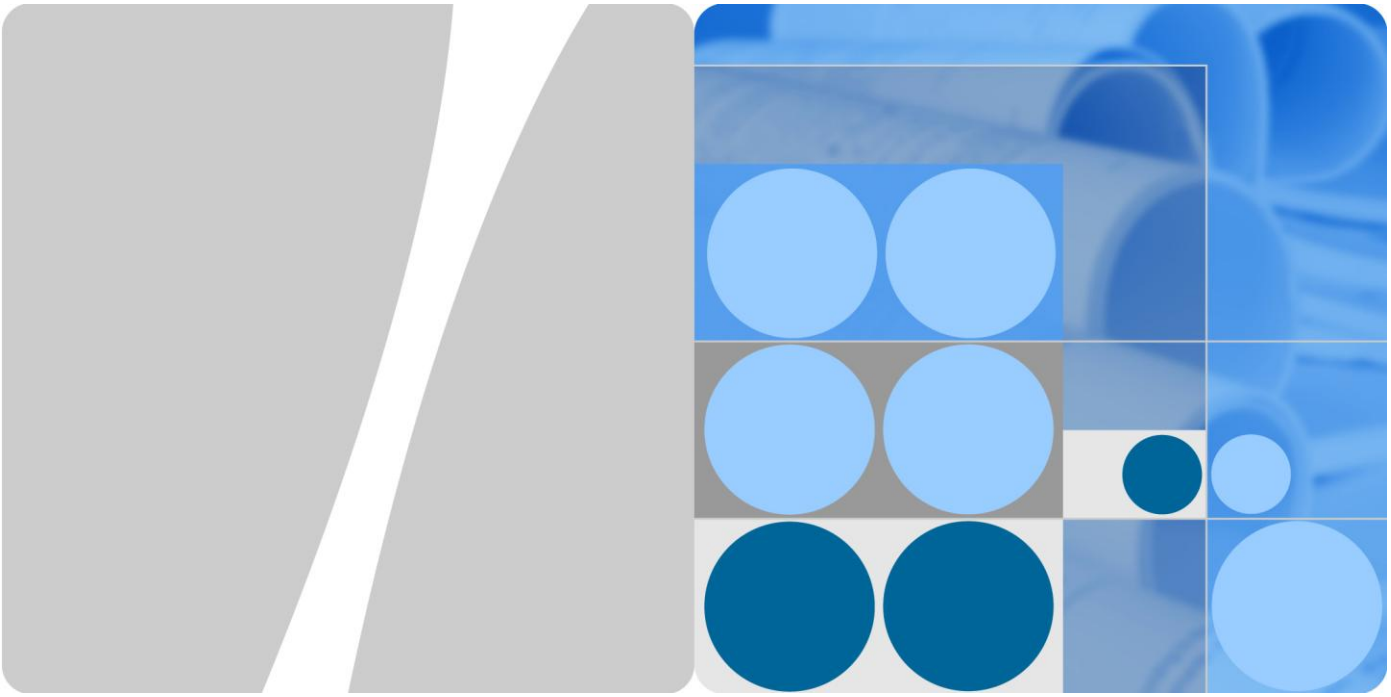


ARP 安全技术白皮书

文档版本 01

发布日期 2012-09-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目 录

1 ARP 安全

关于本章

1.1 介绍

定义

ARP（Address Resolution Protocol）安全是针对 ARP 攻击的一种安全特性，它通过一系列对 ARP 表项学习和 ARP 报文处理的限制、检查等措施来保证网络设备的安全性。ARP 安全特性不仅能够防范针对 ARP 协议的攻击，还可以防范网段扫描攻击等基于 ARP 协议的攻击。

目的

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，容易被攻击者利用。在网络中，常见的 ARP 攻击方式主要包括：

- ARP 泛洪攻击，也叫拒绝服务攻击（Denial of Service），主要存在这样两种场景：
  - 设备处理 ARP 报文和维护 ARP 表项都需要消耗系统资源，同时为了满足 ARP 表项查询效率的要求，一般设备都会对 ARP 表项规模有规格限制。攻击者就利用这一点，通过伪造大量源 IP 地址变化的 ARP 报文，使得设备 ARP 表项资源被无效的 ARP 条目耗尽，合法用户的 ARP 报文不能继续生成 ARP 条目，导致正常通信中断。
  - 攻击者利用工具扫描本网段主机或者进行跨网段扫描时，会向设备发送大量目标 IP 地址不能解析的 IP 报文，导致设备触发大量 ARP Miss 消息，生成并

下发大量临时 ARP 表项，并广播大量 ARP 请求报文以对目标 IP 地址进行解析，从而造成 CPU 负荷过重，这也是泛洪攻击的一种。

- ARP 欺骗攻击，是指攻击者通过发送伪造的 ARP 报文，恶意修改设备或网络内其他用户主机的 ARP 表项，造成用户或网络的报文通信异常。

ARP 攻击行为存在以下危害：

- 会造成网络连接不稳定，引发用户通信中断，导致严重的经济损失。
- 利用 ARP 欺骗截取用户报文，进而非法获取游戏、网银、文件服务等系统的帐号和口令，造成被攻击者重大利益损失。

为了避免上述 ARP 攻击行为造成的各种危害，ARP 安全特性针对不同的攻击类型提供了多种解决方案，具体如表 1-1 所示：

表1-1 ARP 安全针对不同攻击类型的解决方案

攻击类型	防攻击功能	部署设备
ARP 泛洪	ARP 报文限速	建议在网关设备上部署本功能
	ARP Miss 消息限速	建议在网关设备上部署本功能
	免费 ARP 报文主动丢弃	建议在网关设备上部署本功能
	ARP 表项严格学习	建议在网关设备上部署本功能
	ARP 表项限制	建议在网关设备上部署本功能
ARP 欺骗	ARP 表项固化	建议在网关设备上部署本功能
	动态 ARP 检测	建议在接入设备上部署本功能 说明 当网关设备上部署了 DHCP 触发 ARP 学习功能时，则需要在网关设备上部署本功能。
	ARP 防网关冲突	建议在网关设备上部署本功能
	免费 ARP 报文主动丢弃	建议在网关设备上部署本功能
	发送免费 ARP 报文	建议在网关设备上部署本功能
	ARP 报文合法性检查	建议在网关设备或接入设备上部署本功能
	ARP 表项严格学习	建议在网关设备上部署本功能
	DHCP 触发 ARP 学习	建议在网关设备上部署本功能
	VPLS 网络中 ARP 代理	建议在 PE 设备上部署本功能

受益

- 可以有效降低用户为保证网络正常运行和网络信息安全而产生的维护成本。
- 可以为用户提供更安全的网络环境和更稳定的网络服务。

1.2 原理描述

1.2.1 ARP 报文限速

如果设备对收到的大量 ARP 报文全部进行处理，可能导致 CPU 负荷过重而无法处理其他业务。因此，在处理之前，设备需要对 ARP 报文进行限速，以保护 CPU 资源。

设备提供了如下几类针对 ARP 报文的限速功能：

- **根据源 MAC 地址或源 IP 地址进行 ARP 报文限速**

  当设备检测到某一个用户在短时间内发送大量的 ARP 报文，可以针对该用户配置基于源 MAC 地址或源 IP 地址的 ARP 报文限速。在单位时间内，如果该用户的 ARP 报文数目超过设定阈值（ARP 报文限速值），则丢弃超出阈值部分的 ARP 报文。

  - 根据源 MAC 地址进行 ARP 报文限速：如果指定 MAC 地址，则针对指定源 MAC 地址的 ARP 报文根据限速值进行限速；如果不指定 MAC 地址，则针对每一个源 MAC 地址的 ARP 报文根据限速值进行限速。

  可以使用如下命令配置根据源 MAC 地址进行 ARP 报文限速：

  1. 配置对每一个 MAC 地址的 ARP 报文进行限速，每秒最多只允许同一个源 MAC 地址的 100 个 ARP 报文通过。

     ```
     [Quidway] arp speed-limit source-mac maximum 100
     ```

2. 配置对 MAC 地址为 0-0-1 的用户进行 ARP 报文限速，每秒最多只允许该 MAC 地址的 50 个 ARP 报文通过。

```
[Quidway] arp speed-limit source-mac 0-0-1 maximum 50
```

- 根据源 IP 地址进行 ARP 报文限速：如果指定 IP 地址，则针对指定源 IP 地址的 ARP 报文根据限速值进行限速；如果不指定 IP 地址，则针对每一个源 IP 地址的 ARP 报文根据限速值进行限速。

可以使用如下命令配置根据源 IP 地址进行 ARP 报文限速：

1. 配置对每一个源 IP 地址的 ARP 报文进行限速，每秒最多只允许同一个源 IP 地址的 100 个 ARP 报文通过。

```
[Quidway] arp speed-limit source-ip maximum 100
```

2. 配置对 IP 地址为 10.0.0.1 的用户进行 ARP 报文限速，每秒最多只允许该 IP 地址的 50 个 ARP 报文通过。

```
[Quidway] arp speed-limit source-ip 10.0.0.1 maximum 50
```

- **针对 Super VLAN 的 VLANIF 接口下的 ARP 报文限速**

当设备的 VLANIF 接口接收到触发 ARP Miss 消息的 IP 报文（关于 ARP Miss 消息的详细解释请参见 1.2.2 ARP Miss 消息限速）时，或者在设备的 VLANIF 接口上启用 ARP 代理功能之后，设备接收到目的 IP 符合代理条件且该 IP 对应的 ARP 条目不存在的 ARP 请求报文时，都会触发 Super VLAN 的 VLANIF 接口进行 ARP 学习。设备会将 ARP 请求报文在每个 Sub VLAN 下复制，如果该 Super VLAN 下配置了大量 Sub VLAN，那么设备将产生大量的 ARP 请求报文。为了避免 CPU 因复制、发送大量 ARP 请求报文而负担过重，设备支持 Super VLAN 的 VLANIF 接口下的 ARP 报文限速功能，以对该场景下设备发送的 ARP 请求报文进行流量控制。

可以使用如下命令在全局下配置 Super VLAN 的 VLANIF 接口下 ARP 请求报文的广播发送限制速率为 500pps：

```
[Quidway] arp speed-limit flood-rate 500
```

- **针对全局、VLAN 和接口的 ARP 报文限速**

设备支持在全局、VLAN 和接口下配置 ARP 报文的限速值和限速时间，有效顺序为接口优先，VLAN 其次，最后为全局。

另外，在接口下还可以指定阻塞 ARP 报文的时间段。如果设备的某个接口在 ARP 报文限速时间内接收到的 ARP 报文数目超过了设定阈值（ARP 报文限速值），则丢弃超出阈值部分的 ARP 报文，并在接下来的一段时间内（即阻塞 ARP 报文时间段）持续丢弃该接口下收到的所有 ARP 报文。

- 针对全局的 ARP 报文限速：在设备出现 ARP 攻击时，限制全局处理的 ARP 报文数量。
- 针对 VLAN 的 ARP 报文限速：在某个 VLAN 内的所有接口出现 ARP 攻击时，限制处理收到的该 VLAN 内的 ARP 报文数量，配置本功能可以保证不影响其他 VLAN 内所有接口的 ARP 学习。
- 针对接口的 ARP 报文限速：在某个接口出现 ARP 攻击时，限制处理该接口收到的 ARP 报文数量，配置本功能可以保证不影响其他接口的 ARP 学习。

可以使用如下命令配置针对全局、VLAN 和接口的 ARP 报文限速：

1. 全局下配置设备每秒最多允许 200 个 ARP 报文通过。

```
[Quidway] arp anti-attack rate-limit enable
[Quidway] arp anti-attack rate-limit 200
```

2. 配置设备每秒最多允许 200 个 VLAN100 的 ARP 报文通过。

```
[Quidway] vlan 100
[Quidway-vlan100] arp anti-attack rate-limit enable
[Quidway-vlan100] arp anti-attack rate-limit 200
```

3. 配置接口 GE1/0/1 在 10 秒钟内最多允许 200 个 ARP 报文通过，当 ARP 报文超过该限速值时，60 秒内持续丢弃该接口下的所有 ARP 报文。

```
[Quidway] interface gigabitethernet1/0/1
[Quidway-GigabitEthernet1/0/1] arp anti-attack rate-limit enable
[Quidway-GigabitEthernet1/0/1] arp anti-attack rate-limit 200 10 block
timer 60
```

1.2.2 ARP Miss 消息限速

如果网络中有用户向设备发送大量目标 IP 地址不能解析的 IP 报文（即路由表中存在该 IP 报文的目的 IP 对应的路由表项，但设备上没有该路由表项中下一跳对应的 ARP 表项），将导致设备触发大量的 ARP Miss 消息。这种触发 ARP Miss 消息的 IP 报文会被上送到主控板进行处理，设备会根据 ARP Miss 消息生成和下发大量临时 ARP 表项并向目的网段发送大量 ARP 请求报文，这样就增加了 CPU 的负担，同时加重了目的网段的负担。

为了避免这种 IP 报文攻击所带来的危害，设备提供了如下几类针对 ARP Miss 消息的限速功能：

- **根据源 IP 地址进行 ARP Miss 消息限速**

  当设备检测到某一源 IP 地址的 IP 报文在 1 秒内触发的 ARP Miss 消息数量超过了 ARP Miss 消息限速值，就认为此源 IP 地址存在攻击。

  此时如果设备对 ARP Miss 报文的处理方式是 block 方式，设备会丢弃超出限速值部分的 ARP Miss 消息，即丢弃触发这些 ARP Miss 消息的 ARP Miss 报文，并下发一条 ACL 来丢弃该源 IP 地址的后续所有 ARP Miss 报文；如果是 none-block 方式，设备只会通过软件限速的方式丢弃超出限速值部分的 ARP Miss 消息，即丢弃触发这些 ARP Miss 消息的 ARP Miss 报文。

  如果指定了 IP 地址，则针对指定源 IP 址的 ARP Miss 消息根据限速值进行限速；如果不指定 IP 地址，则针对每一个 IP 地址的 ARP Miss 消息根据限速值进行限速。

  可以使用如下命令配置根据源 IP 地址进行 ARP Miss 消息限速：

  1. 配置对每一个源 IP 地址的 ARP Miss 消息进行限速，允许设备每秒最多处理同一个源 IP 地址触发的 50 个 ARP Miss 消息。

     ```
     [Quidway] arp-miss speed-limit source-ip maximum 50
     ```

  2. 配置对 IP 地址为 10.0.0.1 的 ARP Miss 消息进行限速，允许设备每秒最多处理该 IP 地址触发的 100 个 ARP Miss 消息；对于其他 IP 地址，允许设备每秒最多处理同一个源 IP 地址触发的 50 个 ARP Miss 消息。

     ```
     [Quidway] arp-miss speed-limit source-ip maximum 50
     [Quidway] arp-miss speed-limit source-ip 10.0.0.1 maximum 100
     ```

- **针对全局、VLAN 和接口的 ARP Miss 消息限速**

  设备支持在全局、VLAN 和接口下配置 ARP Miss 消息限速，有效顺序为接口优先，VLAN 其次，最后为全局。

  - 针对全局的 ARP Miss 消息限速：在设备出现目标 IP 地址不能解析的 IP 报文攻击时，限制全局处理的 ARP Miss 消息数量。
  - 针对 VLAN 的 ARP Miss 消息限速：在某个 VLAN 内的所有接口出现目标 IP 地址不能解析的 IP 报文攻击时，限制处理该 VLAN 内报文触发的 ARP Miss 消息数量，配置本功能可以保证不影响其他 VLAN 内所有接口的 IP 报文转发。
  - 针对接口的 ARP Miss 消息限速：在某个接口出现目标 IP 地址不能解析的 IP 报文攻击时，限制处理该接口收到的报文触发的 ARP Miss 消息数量，配置本功能可以保证不影响其他接口的 IP 报文转发。

  可以使用如下命令配置针对全局、VLAN 和接口的 ARP Miss 消息限速：

  1. 全局下配置设备每秒最多允许处理 200 个 ARP Miss 消息。

     ```
     [Quidway] arp-miss anti-attack rate-limit enable
     [Quidway] arp-miss anti-attack rate-limit 200
     ```

  2. 配置设备每秒最多允许处理 200 个 VLAN100 的 IP 报文触发的 ARP Miss 消息。

     ```
     [Quidway] vlan 100
     [Quidway-vlan100] arp-miss anti-attack rate-limit enable
     [Quidway-vlan100] arp-miss anti-attack rate-limit 200
     ```

  3. 配置设备在 10 秒钟内最多允许处理 200 个从接口 GE1/0/1 上送的 IP 报文触发的 ARP Miss 消息。

     ```
     [Quidway] interface gigabitethernet1/0/1
     [Quidway-GigabitEthernet1/0/1] arp-miss anti-attack rate-limit enable
     [Quidway-GigabitEthernet1/0/1] arp-miss anti-attack rate-limit 200 10
     ```

- **通过设定临时 ARP 表项的老化时间控制 ARP Miss 消息的触发频率**

  当 IP 报文触发 ARP Miss 消息时，设备会根据 ARP Miss 消息生成临时 ARP 表项，并且向目的网段发送 ARP 请求报文。

  - 在临时 ARP 表项老化时间范围内，
  - 设备收到 ARP 应答报文前，匹配临时 ARP 表项的 IP 报文将被丢弃并且不会触发 ARP Miss 消息。
  - 设备收到 ARP 应答报文后，则生成正确的 ARP 表项来替换临时 ARP 表项。
  - 当老化时间超时后，设备会清除临时 ARP 表项。此时如果设备转发 IP 报文匹配不到对应的 ARP 表项，则会重新触发 ARP Miss 消息并生成临时 ARP 表项，如此循环重复。

  当判断设备受到攻击时，可以增大临时 ARP 表项的老化时间，减小设备 ARP Miss 消息的触发频率，从而减小攻击对设备的影响。

  可以使用如下命令配置接口 VLANIF 10 的临时 ARP 表项超时时间为 10 秒：

  ```
  [Quidway] interface vlanif 10
  [Quidway-Vlanif10] arp-fake expire-time 10
  ```

1.2.3 免费 ARP 报文主动丢弃

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的源 IP 地址和目地 IP 地址都是本机 IP 地址，源 MAC 地址是本机 MAC 地址，目的 MAC 地址是广播地址。当有新的用户主机接入网络时，该用户主机会以广播的方式发送免费 ARP 报文，来确认广播域中有无其他设备与自己的 IP 地址冲突；当用户主机改变了硬件地址时，为了能够在其他所有用户主机的 ARP 表项老化之前通告其硬件地址已经发生改变，该用户主机也会发送免费 ARP 报文。

由于发送免费 ARP 报文的用户主机并不需要经过身份验证，任何一个用户主机都可以发送免费 ARP 报文，这样就引入了两个问题：

- 如果网络中出现大量的免费 ARP 报文，设备会因为处理这些报文而导致 CPU 负荷过重，从而不能正常处理合法的 ARP 报文。
- 如果设备处理的免费 ARP 报文是攻击者伪造的，会造成设备错误地更新 ARP 表项，导致合法用户的通信流量发生中断。

参考以上问题描述，在确认攻击来自免费 ARP 报文之后，可以在网关设备上使能免费 ARP 报文主动丢弃功能，使网关设备直接丢弃免费 ARP 报文。

注意

当有主机更新了硬件地址并重新接入网络（如主机关机后更换了接口卡并重新启动，或双机热备份系统中主用设备发生故障，备用设备接管）时，如果设备开启了免费 ARP 报文主动丢弃功能，可能会导致其他网络设备因无法正常更新相应的 ARP 表项而无法与该主机建立正常通信。

可以使用如下命令使能免费 ARP 报文主动丢弃功能：

1. 全局使能免费 ARP 报文主动丢弃功能。

   ```
   [Quidway] arp anti-attack gratuitous-arp drop
   ```

2. 在接口 VLANIF10 下使能免费 ARP 报文主动丢弃功能。

   ```
   [Quidway] interface vlanif 10
   [Quidway-Vlanif10] arp anti-attack gratuitous-arp drop
   ```

1.2.4 ARP 表项严格学习

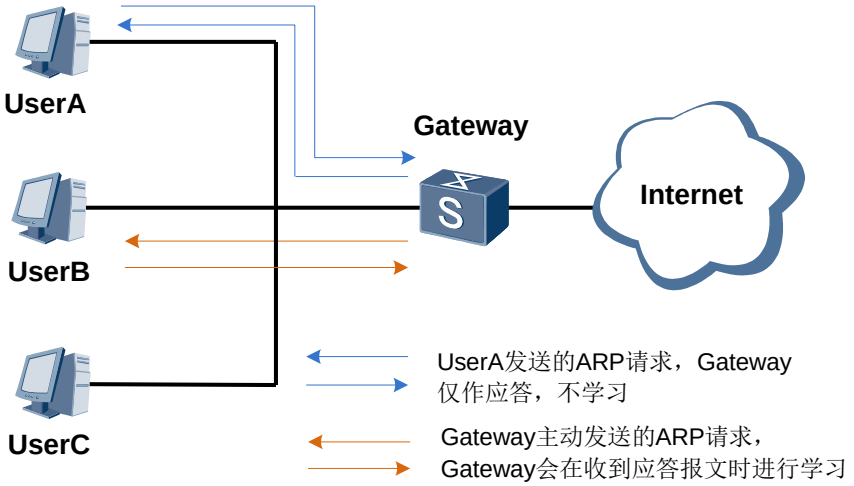
如果大量用户在同一时间段内向设备发送大量 ARP 报文，或者攻击者伪造正常用户的 ARP 报文发送给设备，则会造成下面的危害：

- 设备因处理大量 ARP 报文而导致 CPU 负荷过重，同时设备学习大量的 ARP 报文可能导致设备 ARP 表项资源被无效的 ARP 条目耗尽，造成合法用户的 ARP 报文不能继续生成 ARP 条目，进而导致用户无法正常通信。
- 伪造的 ARP 报文将错误地更新设备的 ARP 表项，导致用户无法正常通信。

为避免上述危害，可以在网关设备上部署 ARP 表项严格学习功能。

ARP 表项严格学习是指只有本设备主动发送的 ARP 请求报文的应答报文才能触发本设备学习 ARP，其他设备主动向本设备发送的 ARP 报文不能触发本设备学习 ARP，这样，可以拒绝大部分的 ARP 报文攻击。

图1-1 ARP 表项严格学习



如图 1-1 所示。通常情况下，当 UserA 向 Gateway 发送 ARP 请求报文后，Gateway 会向 UserA 回应 ARP 应答报文，并且添加或更新 UserA 对应的 ARP 表项。当 Gateway 配置 ARP 表项严格学习功能以后：

- 对于 Gateway 收到 UserA 发送来的 ARP 请求报文，Gateway 不添加也不更新 UserA 对应的 ARP 表项。如果该请求报文请求的是 Gateway 的 MAC 地址，那么 Gateway 会向 UserA 回应 ARP 应答报文。
- 如果 Gateway 向 UserB 发送 ARP 请求报文，待收到与该请求对应的 ARP 应答报文后，Gateway 会添加或更新 UserB 对应的 ARP 表项。

可以使用如下命令使能 ARP 表项严格学习功能：

1. 全局使能 ARP 表项严格学习功能。

```
[Quidway] arp learning strict
```

2. 使能接口 VLANIF10 的 ARP 表项严格学习功能。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp learning strict force-enable
```

1.2.5 ARP 表项限制

ARP 表项限制功能应用在网关设备上，可以限制设备的某个接口学习动态 ARP 表项的数目。默认状态下，接口可以学习的动态 ARP 表项数目规格与全局的 ARP 表项规格保持一致。当部署完 ARP 表项限制功能后，如果指定接口下的动态 ARP 表项达到了允许学习的最大数目，将不再允许该接口继续学习动态 ARP 表项，以保证当一个接口所接入的某一用户主机发起 ARP 攻击时不会导致整个设备的 ARP 表资源都被耗尽。

可以使用如下命令配置 ARP 表项限制功能：

1. 配置接口 VLANIF10 最多可以学习到 20 个动态 ARP 表项。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp-limit maximum 20
```

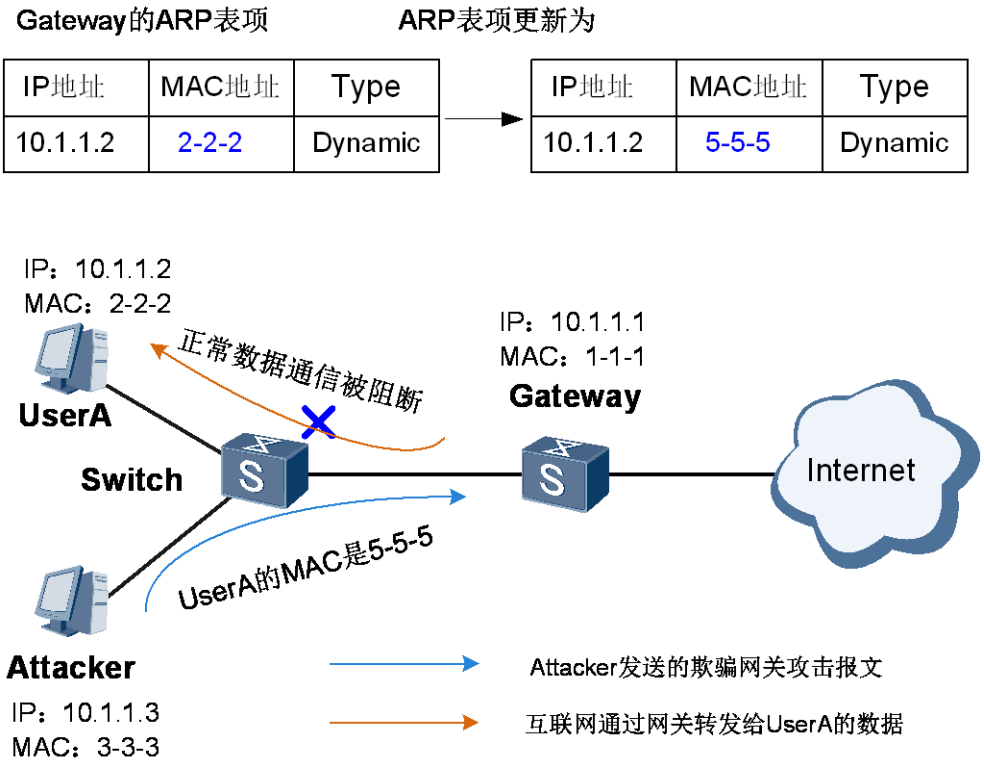
2. 配置接口 GE1/0/1 最多可以学习到 20 个 VLAN10 对应的动态 ARP 表项。

```
[Quidway] interface gigabitethernet1/0/1
[Quidway-GigabitEthernet1/0/1] arp-limit vlan 10 maximum 20
```

1.2.6 ARP 表项固化

如图 1-2 所示，Attacker 仿冒 UserA 向 Gateway 发送伪造的 ARP 报文，导致 Gateway 的 ARP 表中记录了错误的 UserA 地址映射关系，造成 UserA 接收不到正常的数据报文。

图1-2 欺骗网关攻击示意图



为了防御这种欺骗网关攻击，可以在网关设备上部署 ARP 表项固化功能。网关设备在第一次学习到 ARP 以后，不再允许用户更新此 ARP 表项或只能更新此 ARP 表项的部分信息，或者通过发送单播 ARP 请求报文的方式对更新 ARP 条目的报文进行合法性确认。

设备提供的三种 ARP 表项固化模式，如表 1-2 所示。

表1-2 ARP 表项固化模式介绍

固化模式	功能
fixed-all 模式	如果设备收到的 ARP 报文中的 MAC 地址、接口或 VLAN 信息和 ARP 表中的信息不匹配，则直接丢弃该 ARP 报文。此模式适用于静态配置 IP 地址，没有冗余链路的网络。
fixed-mac 模式	如果设备收到的 ARP 报文中的 MAC 地址与 ARP 表中对应条目的 MAC 地址不匹配，则直接丢弃该 ARP 报文；如果匹配，但是收到报文的接口或 VLAN 信息与 ARP 表中对应条目不匹配，则可以更新对应 ARP 条目中的接口和 VLAN 信息。此模式主要应用于用户接口需要进行切换的场景。
send-ack 模式	如果设备收到的 ARP 报文 A 涉及 ARP 表项 MAC 地址、接口或 VLAN 信息的修改，设备不会立即更新 ARP 表项，而是先向待更新的 ARP 表项现有 MAC 地址对应的用户发送一个单播的 ARP 请求报文进行确认。 • 如果在随后的 3 秒内设备收到 ARP 应答报文 B，且当前 ARP 条目中的 IP 地址、MAC 地址、接口和 VLAN 信息与 ARP 应答报文 B 的一致，则认为 ARP 报文 A 为攻击报文，不更新该 ARP 条目。 • 如果在随后的 3 秒内设备未收到 ARP 应答报文，或者收到 ARP 应答报文 B 与当前 ARP 条目中的 IP 地址、MAC 地址、接口和 VLAN 信息不一致，设备会再向刚才收到的 ARP 报文 A 对应的源 MAC 发送一个单播 ARP 请求报文。 - 如果在随后的 3 秒内收到 ARP 应答报文 C，且 ARP 报文 A 与 ARP 应答报文 C 的源 IP 地址、源 MAC 地址、接口和 VLAN 信息一致，则认为现有 ARP 条目已经无效且 ARP 报文 A 是可以更新该 ARP 条目的合法报文，并根据 ARP 报文 A 来更新该 ARP 条目。 - 如果在随后的 3 秒内未收到 ARP 应答报文，或者 ARP 报文 A 与收到的 ARP 应答报文 C 的源 IP 地址、源 MAC 地址、接口和 VLAN 信息不一致，则认为 ARP 报文 A 为攻击报文，设备会忽略收到的 ARP 报文 A，ARP 条目不会更新。 此模式适用于动态分配 IP 地址，有冗余链路的网络。

可以使用如下命令配置 ARP 表项固化功能：

1. 全局下使能 ARP 表项固化功能，指定固化模式为 fixed-mac 模式。

   ```
   [Quidway] arp anti-attack entry-check fixed-mac enable
   ```

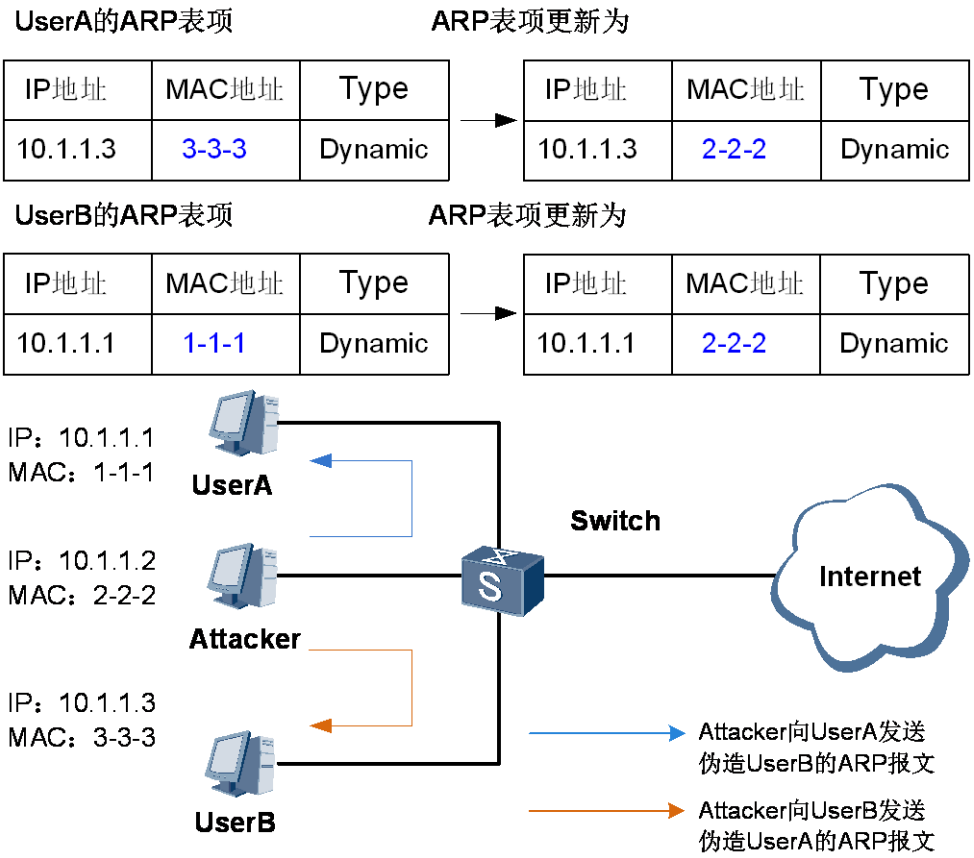
2. 在接口 VLANIF10 下使能 ARP 表项固化功能，指定固化模式为 send-ack 模式。

   ```
   [Quidway] interface vlanif 10
   [Quidway-Vlanif10] arp anti-attack entry-check send-ack enable
   ```

1.2.7 动态 ARP 检测

网络中针对 ARP 的攻击层出不穷，中间人攻击是常见的 ARP 欺骗攻击方式之一。

图1-3 中间人攻击



如图 1-3 所示，是中间人攻击的一个场景。攻击者主动向 UserA 发送伪造 UserB 的 ARP 报文，导致 UserA 的 ARP 表中记录了错误的 UserB 地址映射关系，攻击者可以轻易获取到 UserA 原本要发往 UserB 的数据；同样，攻击者也可以轻易获取到 UserB 原本要发往 UserA 的数据。这样，UserA 与 UserB 间的信息安全无法得到保障。

为了防御中间人攻击，可以在 Switch 上部署动态 ARP 检测功能。

动态 ARP 检测 DAI（Dynamic ARP Inspection）是利用 DHCP Snooping 绑定表来防御中间人攻击的。当设备收到 ARP 报文时，将此 ARP 报文对应的源 IP、源 MAC、VLAN 以及接口信息和 DHCP Snooping 绑定表的信息进行比较，如果信息匹配，说明发送该 ARP 报文的用户是合法用户，允许此用户的 ARP 报文通过，否则就认为是攻击，丢弃该 ARP 报文。

说明

动态 ARP 检测功能仅适用于 DHCP Snooping 场景。设备使能 DHCP Snooping 功能后，当 DHCP 用户上线时，设备会自动生成 DHCP Snooping 绑定表；对于静态配置 IP 地址的用户，设备不会生成 DHCP Snooping 绑定表，所以需要手动添加静态 DHCP Snooping 绑定表。

关于 DHCP Snooping 的详细介绍，请参见 DHCP Snooping 技术白皮书 中的描述。

当 Switch 上部署动态 ARP 检测功能后，如果攻击者连接到 Switch 并试图发送伪造的 ARP 报文，Switch 会根据 DHCP Snooping 绑定表检测到这种攻击行为，对该 ARP 报文进行丢弃处理。如果 Switch 上同时使能了动态 ARP 检测丢弃报文告警功能，则当 ARP 报文因不匹配 DHCP Snooping 绑定表而被丢弃的数量超过了告警阈值时，Switch 会发出告警通知管理员。

可以使用如下命令配置动态 ARP 检测功能：

1. 全局下使能动态 ARP 检测功能。

```
[Quidway] arp anti-attack check user-bind enable
```

2. 在 VLAN100 下使能动态 ARP 检测功能。

```
[Quidway] vlan 100
[Quidway-vlan100] arp anti-attack check user-bind enable
```

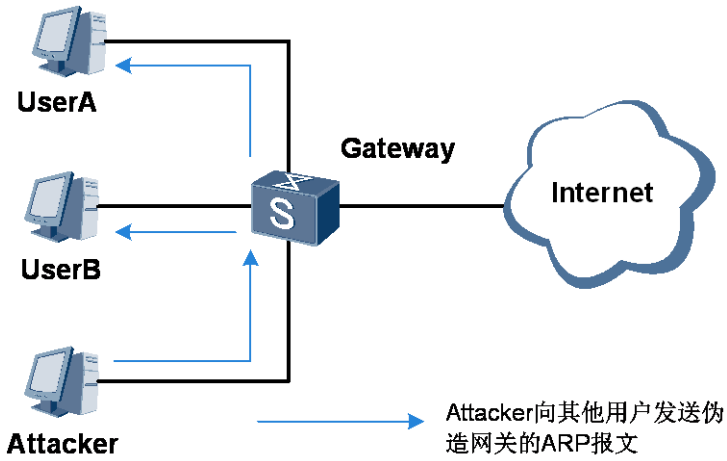
3. 在接口 GE1/0/1 下使能动态 ARP 检测功能以及动态 ARP 检测丢弃报文告警功能，并指定动态 ARP 检测丢弃报文告警阈值为 200。

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] arp anti-attack check user-bind enable
[Quidway-GigabitEthernet1/0/1] arp anti-attack check user-bind alarm
enable
[Quidway-GigabitEthernet1/0/1] arp anti-attack check user-bind alarm
threshold 200
```

1.2.8 ARP 防网关冲突

如图 1-4 所示，用户主机直接接入网关，Attacker 将伪造网关的 ARP 报文发送给 UserA 和 UserB，使 UserA 和 UserB 误以为攻击者即为网关。UserA 和 UserB 的 ARP 表中会记录错误的网关地址映射关系，这样就会把发往网关的流量均发送给了攻击者，攻击者可轻易窃听到 UserA 和 UserB 发送的数据内容。

图1-4 ARP 网关冲突



为了防范攻击者仿冒网关，可以在网关设备上使能 ARP 防网关冲突功能。当设备收到的 ARP 报文存在下列情况之一：

- ARP 报文的源 IP 地址与报文入接口对应的 VLANIF 接口的 IP 地址相同
- ARP 报文的源 IP 地址是入接口的虚拟 IP 地址，但 ARP 报文源 MAC 地址不是 VRRP 虚 MAC

说明

一个 VRRP 备份组，被当作一个共享局域网内主机的缺省网关，即虚拟交换机。一个虚拟交换机拥有一个 VRRP 虚 MAC，VRRP 虚 MAC 根据虚拟交换机 ID 生成，格式为：00-00-5E-00-01-{VRID}(VRRP)。当虚拟交换机回应 ARP 请求时，使用的是 VRRP 虚 MAC 地址，而不是接口的真实 MAC 地址。

设备就认为该 ARP 报文是与网关地址冲突的 ARP 报文，设备将生成 ARP 防攻击表项，并在后续一段时间内丢弃该接口收到的同 VLAN 以及同源 MAC 地址的 ARP 报文，这样可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。

可以使用如下命令全局使能 ARP 防网关冲突攻击功能：

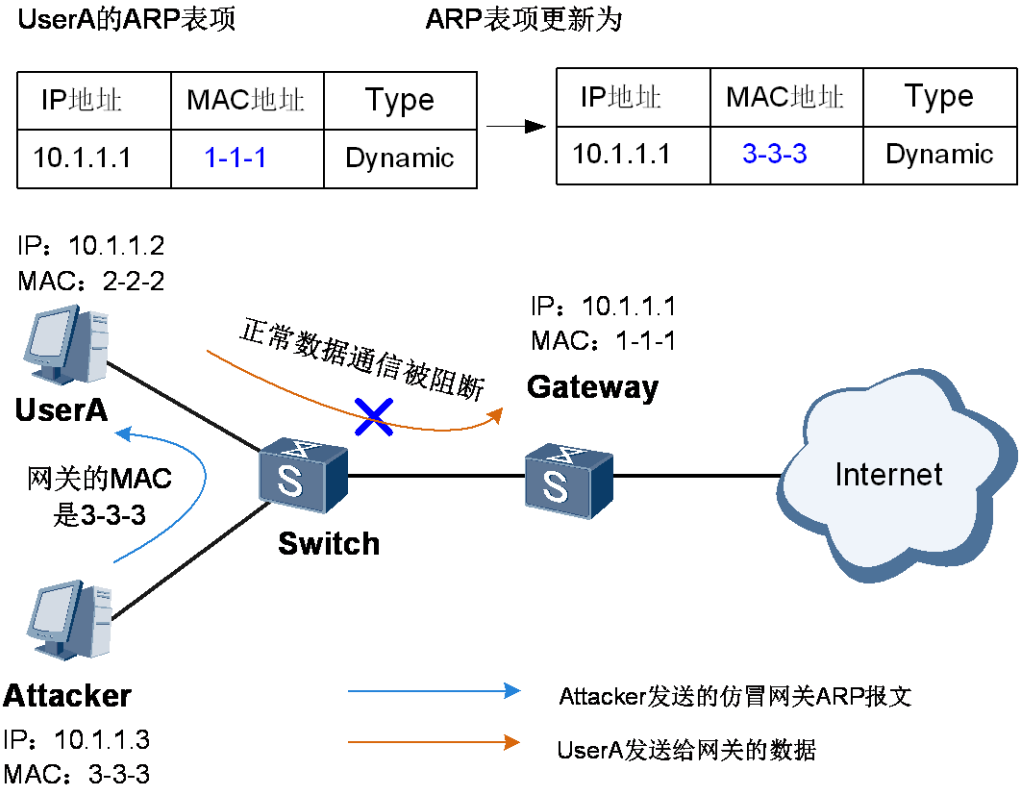
```
[Quidway] arp anti-attack gateway-duplicate enable
```

此时，还可以在设备上使能发送免费 ARP 报文功能，通过广播发送正确的免费 ARP 报文到所有用户，迅速将已经被攻击的用户记录的错误网关地址映射关系修改正确。

1.2.9 发送免费 ARP 报文

如图 1-5 所示，Attacker 仿冒网关向 UserA 发送了伪造的 ARP 报文，导致 UserA 的 ARP 表中记录了错误的网关地址映射关系，从而正常的数据不能被网关接收。

图1-5 仿冒网关攻击



为了避免上述危害，可以在网关设备上部署发送免费 ARP 报文功能，定期更新用户的 ARP 表项，使得用户 ARP 表项中记录的是正确的网关 MAC 地址。

可以使用如下命令配置发送免费 ARP 报文功能：

1. 全局使能发送免费 ARP 报文功能，并配置发送免费 ARP 报文的时间间隔为 100 秒。

```
[Quidway] arp gratuitous-arp send enable
[Quidway] arp gratuitous-arp send interval 100
```

2. 在接口 VLANIF10 下使能发送免费 ARP 报文功能，并配置发送免费 ARP 报文的时间间隔为 100 秒。

```
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp anti-attack gratuitous-arp drop
[Quidway-Vlanif10] arp gratuitous-arp send interval 100
```

1.2.10 ARP 报文合法性检查

ARP 报文合法性检查功能可以部署在接入设备或网关设备上，用来对 MAC 地址和 IP 地址不合法的报文进行过滤。设备支持以下三种可以任意组合的检查。

- 源 MAC 地址检查：设备会检查 ARP 报文中的源 MAC 地址和以太网数据帧首部中的源 MAC 地址是否一致，一致则认为合法，否则丢弃报文；
- 目的 MAC 地址检查：设备会检查 ARP 应答报文中的目的 MAC 地址是否和以太网数据帧首部中的目的 MAC 地址一致，一致则认为合法，否则丢弃报文；
- IP 地址检查：设备会检查 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。

可以使用如下命令使能 ARP 报文合法性检查功能，并指定 ARP 报文合法性检查时检查源 MAC 地址和目的 MAC 地址：

```
[Quidway] arp anti-attack packet-check sender-mac dst-mac
```

1.2.11 DHCP 触发 ARP 学习

在 DHCP 用户场景下，当 DHCP 用户数目很多时，设备进行大规模 ARP 表项的学习和老化会对设备性能和网络环境形成冲击。

为了避免此问题， 可以在网关设备上部署 DHCP 触发 ARP 学习功能。当 DHCP 服务器给用户分配了 IP 地址，网关设备会根据 VLANIF 接口上收到的 DHCP ACK 报文直接生成该用户的 ARP 表项。该功能生效的前提是使能 DHCP Snooping 功能。

可以使用如下命令在接口 VLANIF10 下使能 DHCP 触发 ARP 学习功能：

```
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
[Quidway] interface vlanif 10
[Quidway-Vlanif10] arp learning dhcp-trigger
```

网关设备上还可同时部署动态 ARP 检测功能，防止 DHCP 用户的 ARP 表项被伪造的 ARP 报文恶意修改。

1.2.12 VPLS 网络中 ARP 代理

在 VPLS 网络中，为了防止 PW（Pseudo Wire）侧的伪造 ARP 报文被广播到 AC（Attachment Circuit）侧形成 ARP 欺骗攻击，可以在 PE 设备上部署 VPLS 网络中的 ARP 代理功能，以及 VPLS 网络中的 DHCP Snooping 功能。

部署上述功能后，PW 侧的 ARP 报文将会被上送到主控板进行处理：

- 如果是 ARP 请求报文，并且报文的目的 IP 地址在 DHCP Snooping 绑定表中存在，则设备根据 DHCP Snooping 绑定表组装 ARP 应答报文直接回应 PW 侧的请求方。
- 如果不是 ARP 请求报文，或者 ARP 请求报文的目的 IP 地址不在 DHCP Snooping 绑定表中，则报文被正常转发。

可以使用如下命令使能设备在 VPLS 网络中的 ARP 代理功能：

```
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping over-vpls enable
[Quidway] arp over-vpls enable
```

1.3 应用

1.3.1 ARP 安全综合功能典型应用

如图 1-6 所示，Switch 作为网关通过接口 GE1/0/3 连接一台服务器，通过接口 GE1/0/1、GE1/0/2 连接 VLAN10 和 VLAN20 下的四个用户。网络中存在以下 ARP 威胁：

- 攻击者向 Switch 发送伪造的 ARP 报文、伪造的免费 ARP 报文进行 ARP 欺骗攻击，恶意修改 Switch 的 ARP 表项，造成其他用户无法正常接收数据报文。
- 攻击者发出大量目的 IP 地址不可达的 IP 报文进行 ARP 泛洪攻击，造成 Switch 的 CPU 负荷过重。
- 用户 User1 构造大量源 IP 地址变化 MAC 地址固定的 ARP 报文进行 ARP 泛洪攻击，造成 Switch 的 ARP 表资源被耗尽以及 CPU 繁忙，影响到正常业务的处理。
- 用户 User3 构造大量源 IP 地址固定的 ARP 报文进行 ARP 泛洪攻击，造成 Switch 的 CPU 繁忙，影响到正常业务的处理。

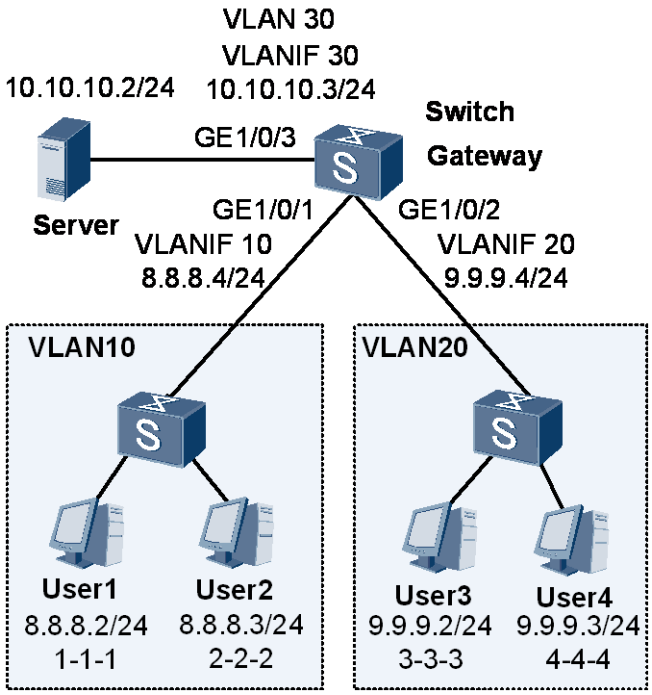
管理员希望能够防止上述 ARP 攻击行为，为用户提供更安全的网络环境和更稳定的网络服务。

采用如下思路在 Switch 上进行配置：

1. 配置 ARP 表项严格学习功能以及 ARP 表项固化功能，实现防止伪造的 ARP 报文错误地更新 Switch 的 ARP 表项。

2. 配置免费 ARP 报文主动丢弃功能，实现防止伪造的免费 ARP 报文错误地更新设备 ARP 表项。
3. 配置根据源 IP 地址进行 ARP Miss 消息限速，实现防止用户侧存在攻击者发出大量目的 IP 地址不可达的 IP 报文触发大量 ARP Miss 消息，形成 ARP 泛洪攻击。同时需要保证 Switch 可以正常处理服务器发出的大量此类报文，避免因丢弃服务器发出的大量此类报文而造成网络无法正常通信。
4. 配置基于接口的 ARP 表项限制以及根据源 MAC 地址进行 ARP 限速，实现防止 User1 发送的大量源 IP 地址变化 MAC 地址固定的 ARP 报文形成的 ARP 泛洪攻击，避免 Switch 的 ARP 表资源被耗尽，并避免 CPU 繁忙。
5. 配置根据源 IP 地址进行 ARP 限速，实现防止 User3 发送的大量源 IP 地址固定的 ARP 报文形成的 ARP 泛洪攻击，避免 Switch 的 CPU 繁忙。

图1-6 配置 ARP 安全功能组网图



Switch 的配置文件

```
#
sysname Switch
#
vlan batch 10 20 30
#
arp learning strict
#
arp-miss speed-limit source-ip 10.10.10.2 maximum 40
arp speed-limit source-ip 9.9.9.2 maximum 10
arp speed-limit source-mac 0001-0001-0001 maximum 10
arp anti-attack entry-check fixed-mac enable
```

```
arp anti-attack gratuitous-arp drop
#
arp-miss speed-limit source-ip maximum 20
#
interface Vlanif10
 ip address 8.8.8.4 255.255.255.0
#
interface Vlanif20
 ip address 9.9.9.4 255.255.255.0
#
interface Vlanif30
 ip address 10.10.10.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 arp-limit vlan 10 maximum 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
return
```

1.3.2 防止 ARP 中间人攻击典型应用

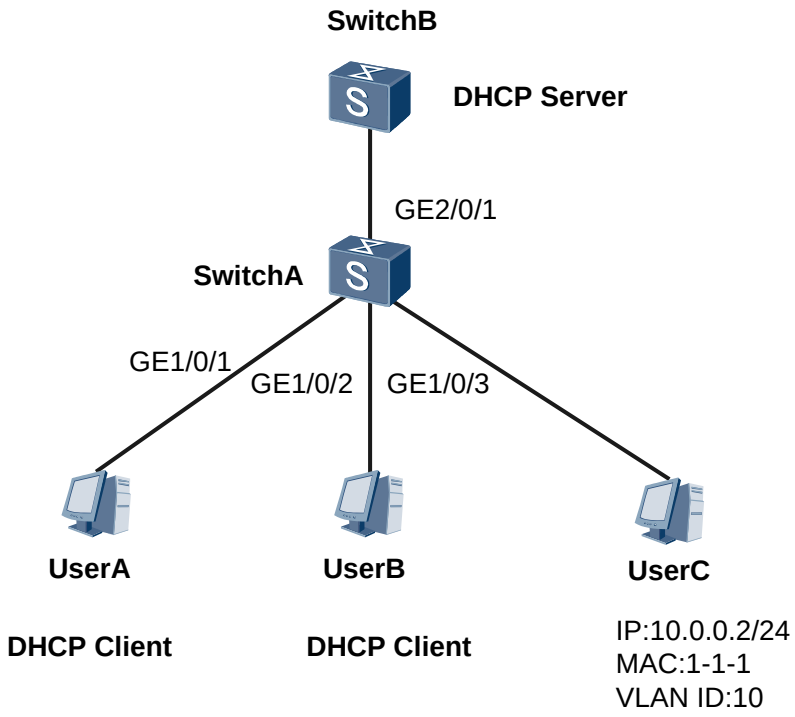
如图 1-7 所示，SwitchA 通过接口 GE2/0/1 连接 DHCP Server，通过接口 GE1/0/1、GE1/0/2 连接 DHCP 客户端 UserA 和 UserB，通过接口 GE1/0/3 连接静态配置 IP 地址的用户 UserC。SwitchA 的接口 GE1/0/1、GE1/0/2、GE1/0/3、GE2/0/1 都属于 VLAN10。

管理员希望能够防止 ARP 中间人攻击，避免合法用户的数据被中间人窃取，同时希望能够了解当前 ARP 中间人攻击的频率和范围。

采用如下思路在 SwitchA 上进行配置：

1. 使能动态 ARP 检测功能，使 SwitchA 对收到的 ARP 报文对应的源 IP、源 MAC、VLAN 以及接口信息进行 DHCP Snooping 绑定表匹配检查，实现防止 ARP 中间人攻击。
2. 使能动态 ARP 检测丢弃报文告警功能，使 SwitchA 开始统计丢弃的不匹配 DHCP Snooping 绑定表的 ARP 报文数量，并在丢弃数量超过告警阈值时能以告警的方式提醒管理员，这样可以使管理员根据告警信息以及报文丢弃计数来了解当前 ARP 中间人攻击的频率和范围。
3. 配置 DHCP Snooping 功能，并配置静态 DHCP Snooping 绑定表，使动态 ARP 检测功能生效。

图1-7 配置防止 ARP 中间人攻击组网图



SwitchA 的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface
GigabitEthernet1/0/3 vlan 10
#
vlan 10
 dhcp snooping enable
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet1/0/3
```

```
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 dhcp snooping trusted
#
return
```

1.4 故障处理案例

1.4.1 合法用户的 ARP 表项被修改导致合法用户的网络服务突然中断的故障处理案例

常见原因

本类故障的常见原因主要包括：

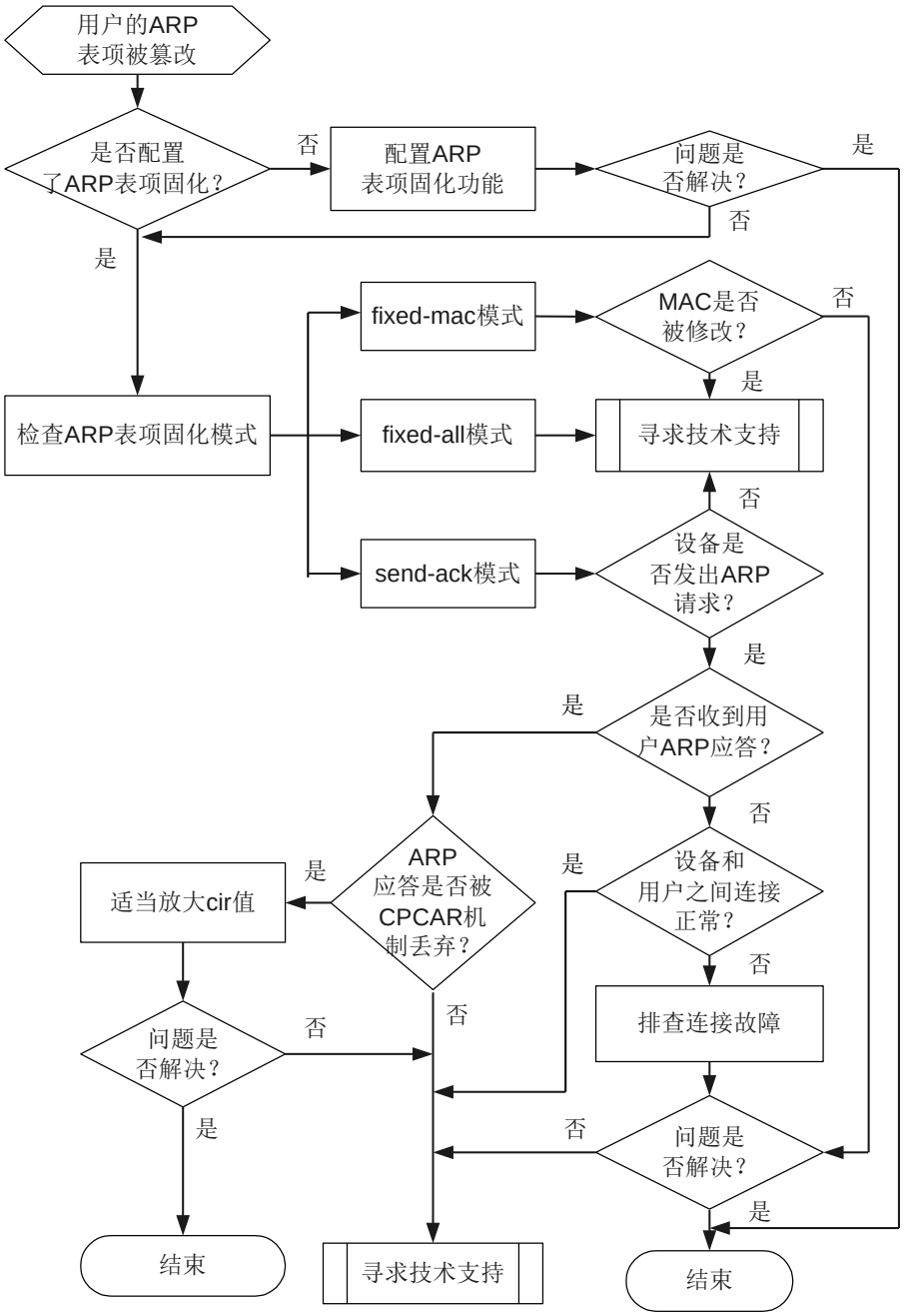
- 攻击者伪造合法用户的 ARP 报文修改合法用户的 ARP 表项

故障诊断流程

合法用户的网络服务突然中断，初步排查不是链路连接或路由问题。可能是攻击者通过伪造其他用户的 ARP 报文，篡改网关设备上的用户 ARP 表项，造成其他合法用户的网络服务中断。以下描述基于 ARP 表项被修改的处理流程。

详细处理流程如图 1-8 所示。

图1-8 合法用户 ARP 表项被修改故障诊断流程图



故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 在交换机上执行命令 **display arp anti-attack configuration entry-check** 查看 ARP 表项固化功能是否使能。

- 如果显示如下信息，则表示没有使能 ARP 表项固化功能。

```
ARP anti-attack entry-check mode: disabled
```

执行命令 **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable** 命令，使能该功能。

说明

在使能该功能前需要执行 **reset arp interface vlanif** *vlan-id* 命令清除用户所在接口下的已学到的攻击者 ARP 表项。

- 如果配置的 ARP 表项固化模式为 **send-ack**，请执行步骤 2。
- 如果配置的 ARP 表项固化模式为 **fixed-mac**，请执行步骤 3。
- 如果配置的 ARP 表项固化模式为 **fixed-all**，请直接执行步骤 4。

步骤 2 **send-ack** 模式下，执行以下子步骤继续排查。

1. 通过端口镜像抓取接入用户的接口上的报文，查看是否有对应的 ARP 交互过程。如果交换机没有发出 ARP 请求，请直接执行步骤 4。
2. 如果交换机发出了 ARP 请求，但没有收到用户的 ARP 应答，检查设备和用户之间网络连接是否正常。
3. 如果收到用户的 ARP 应答，执行 **display cpu-defend statistics packet-typearp-reply** 命令检查 ARP Reply 报文是否被丢弃。如果 ARP Reply 报文的“Drop”计数不断增加，可能是被 CPCAR 机制丢弃了。可以通过 **car** 命令适当放大 **cir** 值。
4. 如果执行完以上步骤后故障仍未排除，请执行步骤 4。

步骤 3 执行命令 **display arp all** | **include** *ip-address* 查看用户的 ARP 表项中哪些信息被修改。

如果是接口或 VLAN 信息被修改，在 **fixed-mac** 模式下认为是正常现象；如果是 MAC 地址被修改，则执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.2

相关日志

无

1.4.2 ARP 报文攻击导致用户流量中断的故障处理案例

常见原因

本类故障的常见原因主要包括：

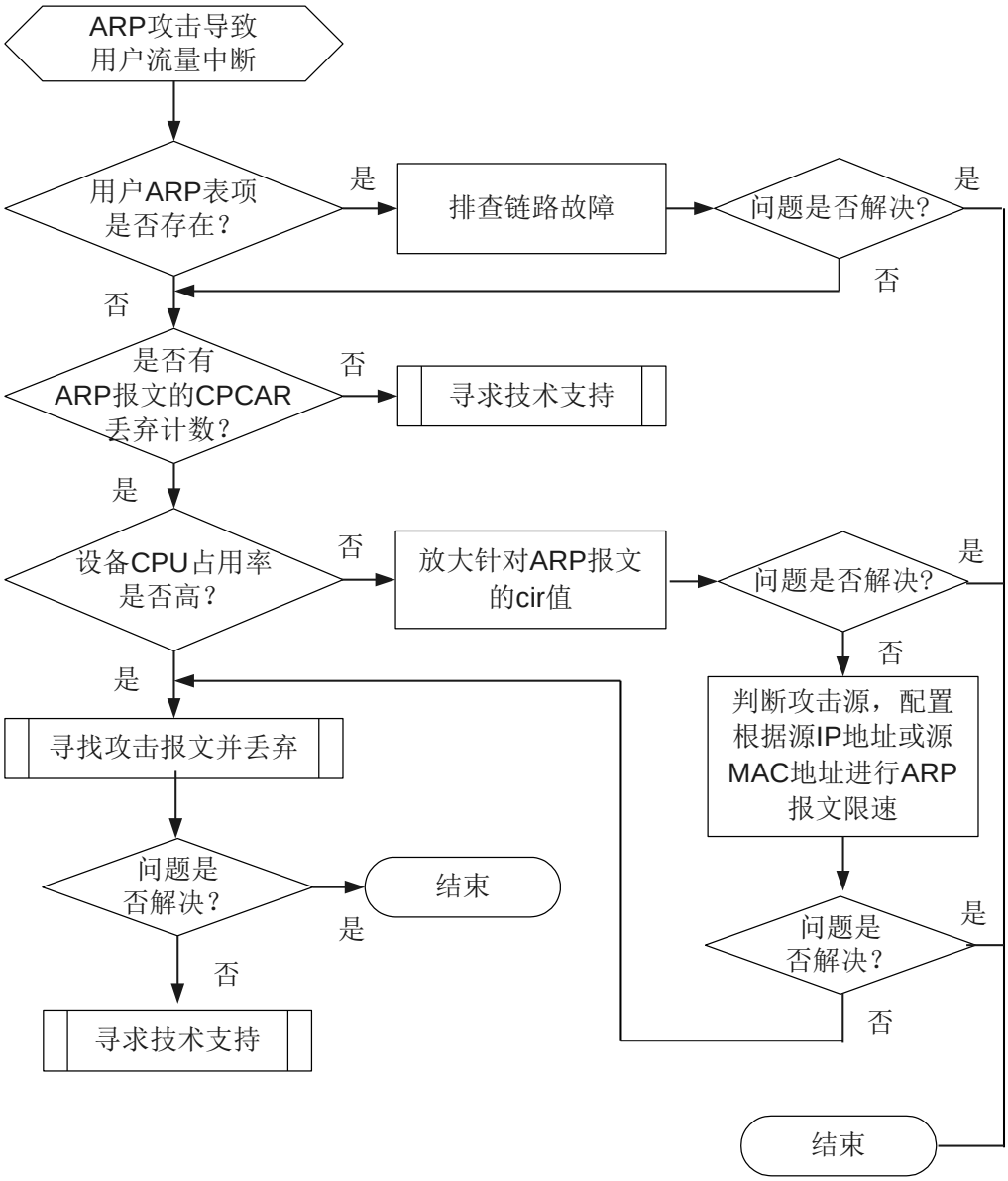
- 攻击者发送大量 ARP 请求，导致目的网段的负担加重。如果配置了三层接口，这些 ARP 报文还会送到 CPU 增加了 CPU 的负担，同时有可能导致合法用户流量中断，形成拒绝服务攻击。

故障诊断流程

交换机的 ARP 请求报文在上送 CPU 时有 CPCAR 机制进行限速，如果攻击者发送大量伪 ARP 请求，与合法用户的 ARP 请求报文共享 CPCAR 限制的带宽，就会导致合法的 ARP 请求报文被丢弃，从而导致用户流量中断。

详细处理流程如图 1-9 所示。

图1-9 ARP 报文攻击导致用户流量中断故障诊断流程图



故障处理步骤

说明

请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

操作步骤

步骤 1 执行命令 **display arp all** 查看用户的 ARP 表项是否存在。

- 如果 ARP 表项还在，表明学到了用户的 ARP 表项，用户流量中断可能是用户的连接闪断。检查并排除链路问题。
- 如果没有用户表项，执行步骤 2。

步骤 2 执行命令 **display cpu-defend statistics packet-type arp-request** 查看 ARP Request 报文的“Drop”计数是否增长。

- 如果计数为 0，设备没有丢弃 ARP Request 报文。请执行步骤 7。
- 如果有计数，表示设备收到的 ARP Request 报文由于超过了 CPCAR 的速率限制而被丢弃。执行步骤 3。

步骤 3 执行命令 **display cpu-usage**，查看主用主控板的 CPU 占用率信息。

- 如果 CPU 占用率正常，可能是相对 ARP 攻击报文规模较小的正常用户的 ARP 报文被 CPCAR 机制丢弃。请执行步骤 4。
- 如果 CPU 占用率较高（超过 70%），可能是相对 ARP 攻击报文规模较小的正常用户的 ARP 报文被 CPCAR 机制丢弃，但此时不能再放大 CPCAR 的限制值。请执行步骤 6。

步骤 4 执行命令 **car** 适当放大针对 ARP Request 报文的 CPCAR 的限制值。

car 命令应该在防攻击策略视图下执行，并应用该防攻击策略才能生效。

如果执行完以上步骤后，故障仍未排除或者故障已排除但是造成 CPU 占用率很高，请执行步骤 5。

步骤 5 在交换机与用户连接的接口上抓取报文，分析 ARP Request 报文的源地址，找出攻击者。

如果同一个源 MAC 或者源 IP 出现在很多 ARP Request 报文中，则交换机认为该地址对应的主机就是攻击源。

请根据实际网络状况，在系统视图下执行命令 **arp speed-limit source-ip** [*ip-address*] **maximum** *maximum*，逐步调小设备根据源 IP 地址进行 ARP 报文限速的限速值；或者执行命令 **arp speed-limit source-mac** [*mac-address*] **maximum** *maximum*，配置根据源 MAC 地址进行 ARP 报文限速。

缺省情况下，ARP 报文根据源 IP 地址限速功能已使能，每秒最多允许同一个源 IP 地址的 30 个 ARP 报文通过。如果超过该值，就对后来的 ARP Request 报文做丢弃处理。设备对每一个源 MAC 地址的 ARP 报文速率限制为 0，即不根据源 MAC 地址进行 ARP 报文限速。

如果根据源 IP 地址或源 MAC 地址进行 ARP 报文限速的限速值已经配置为较小的值（如 5pps），

- 故障仍未排除，请执行步骤 7。
- 故障已经排除但是 CPU 占用率仍然很高，则通过配置黑名单或黑洞 MAC 对攻击源的报文进行丢弃处理。之后如果 CPU 占用率仍然很高，请执行步骤 7。

步骤 6 在交换机与用户连接的接口上抓取报文，分析 ARP Request 报文的源地址，找出攻击者。

如果同一个源地址出现在很多 ARP Request 报文中，则交换机认为该地址就是攻击源。可以通过配置黑名单或黑洞 MAC 对其报文进行丢弃处理。

如果执行完以上步骤后故障仍未排除，请执行步骤 7。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.3
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.4
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.5
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.6
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.7
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.11

相关日志

无

1.5 参考标准和协议

本特性的参考资料清单如下：

文档	描述	备注
RFC826	Ethernet Address Resolution Protocol	-
RFC903	Reverse Address Resolution Protocol	-
RFC1027	Using ARP to Implement Transparent Subnet Gateways	-
RFC1042	Standard for the Transmission of IP Datagrams over IEEE 802 Networks	-