

ARP 安全技术白皮书

目 录

1 ARP 安全	1-1
1.1 介绍.....	1-1
1.2 原理描述.....	1-3
1.2.1 ARP 报文限速	1-3
1.2.2 ARP Miss 消息限速.....	1-5
1.2.3 免费 ARP 报文主动丢弃.....	1-7
1.2.4 ARP 表项严格学习	1-7
1.2.5 ARP 表项限制	1-8
1.2.6 ARP 表项固化	1-9
1.2.7 动态 ARP 检测	1-11
1.2.8 ARP 防网关冲突.....	1-12
1.2.9 发送免费 ARP 报文.....	1-13
1.2.10 ARP 报文合法性检查	1-14
1.2.11 DHCP 触发 ARP 学习	1-14
1.2.12 VPLS 网络中 ARP 代理	1-15
1.3 应用.....	1-15
1.3.1 ARP 安全综合功能典型应用	1-15
1.3.2 防止 ARP 中间人攻击典型应用	1-17
1.4 故障处理案例.....	1-19
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	1-19
1.4.2 ARP 报文攻击导致用户流量中断的故障处理案例	1-22
1.5 参考标准和协议.....	1-25

1 ARP 安全

关于本章

- 1.1 介绍
- 1.2 原理描述
- 1.3 应用
- 1.4 故障处理案例
- 1.5 参考标准和协议

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

1.2.2 ARP Miss 消息限速

1.2.3 免费 ARP 报文主动丢弃

1.2.4 ARP 表项严格学习

1.2.5 ARP 表项限制

1.2.6 ARP 表项固化

1.2.7 动态 ARP 检测

1.2.8 ARP 防网关冲突

1.2.9 发送免费 ARP 报文

1.2.10 ARP 报文合法性检查

1.2.11 DHCP 触发 ARP 学习

1.2.12 VPLS 网络中 ARP 代理

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 地址的 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，来确认广播域中是否有其他设备与自己的 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

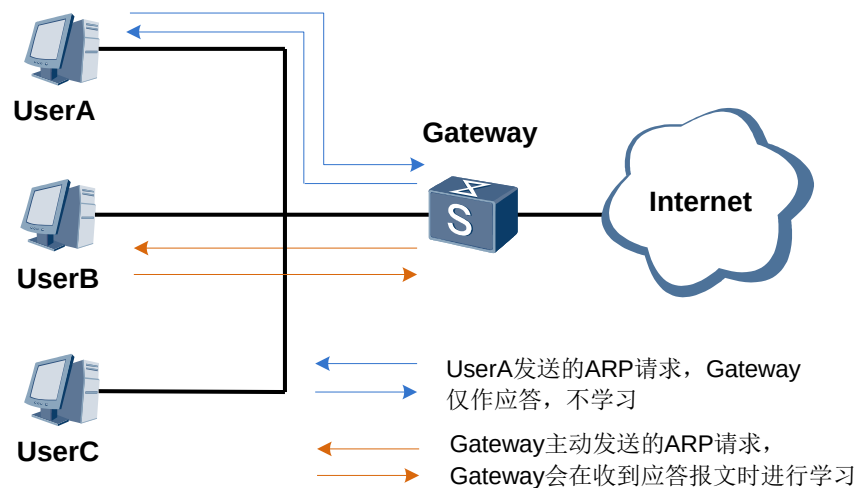
如果大量用户在同一时间段内向设备发送大量 ARP 报文，或者攻击者伪造正常用户的 ARP 报文发送给设备，则会造成下面的危害：

- 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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/418112124033006046>