ARP 攻击防御技术白皮书

目 录

1 概述

1.1 产生背景

1.1.1 ARP 工作机制

ARP（Address Resolution Protocol，地址解析协议）协议是以太网等数据链路层的基础协议，负责完成 IP 地址到硬件地址的映射。工作过程简述如下：

(1) 当主机或者网络设备需要解析一个 IP 地址对应的 MAC 地址时，会广播发送 ARP 请求报文。

(2) 主机或者网络设备接收到 ARP 请求，如果 ARP 请求报文的目标 IP 地址是主机或者网络设备的 IP 地址，则会进行应答。同时，根据请求发送者的 IP 地址和 MAC 地址的对应关系建立 ARP 表项。

(3) 发起请求的主机或者网络设备接收到应答后，同样会将应答报文中发送者的 IP 地址和 MAC 地址的映射关系记录下来，生成 ARP 表项。

1.1.2 ARP 攻击类型介绍

从 ARP 工作机制可以看出，ARP 协议简单易用，但是却没有任何安全机制，攻击者可以发送伪造 ARP 报文对网络进行攻击。伪造 ARP 报文具有如下特征：

- 伪造的 ARP 报文中源 MAC 地址/目的 MAC 地址和以太网帧封装中的源 MAC 地址/目的 MAC 地址不一致。
- 伪造的 ARP 报文中源 IP 地址和源 MAC 地址的映射关系不是合法用户真实的映射关系。

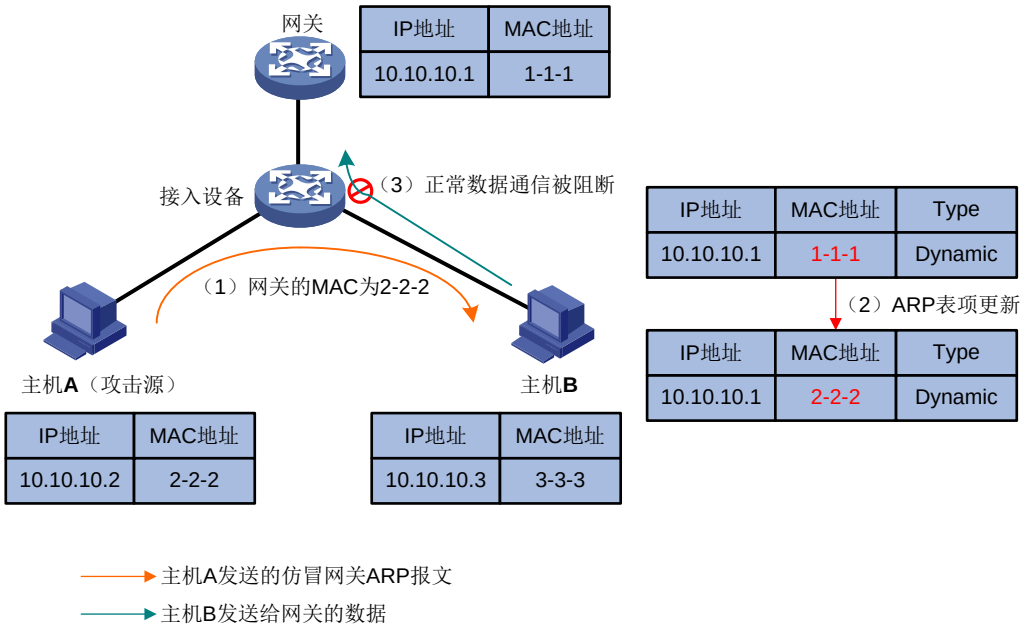
目前主要的 ARP 攻击方式有如下几类：

- 仿冒网关攻击
- 仿冒用户攻击（欺骗网关或者其他主机）
- 泛洪攻击

1. 仿冒网关攻击

如图 1 所示，因为主机 A 仿冒网关向主机 B 发送了伪造的网关 ARP 报文，导致主机 B 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 仿冒网关攻击示意图



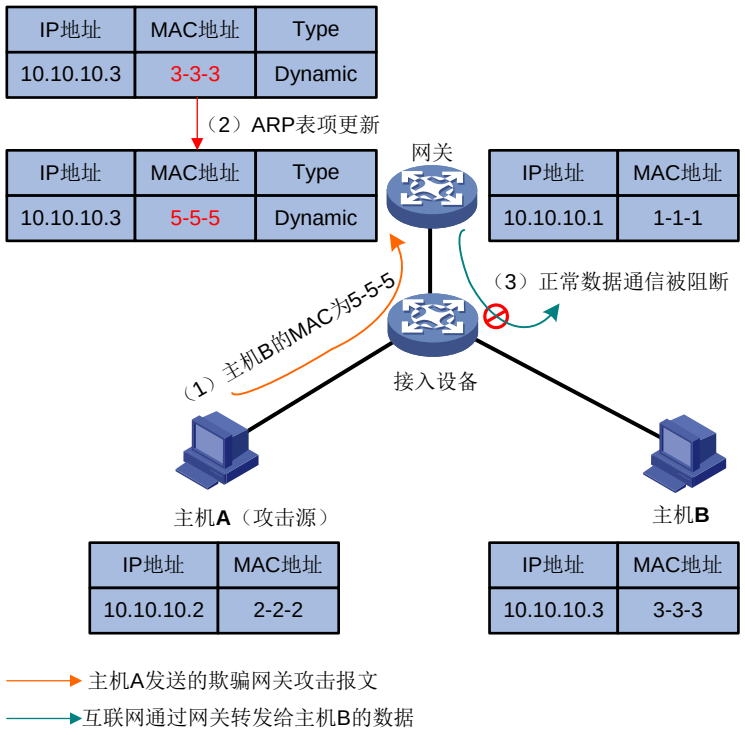
仿冒网关攻击是一种比较常见的攻击方式，如果攻击源发送的是广播 ARP 报文，或者根据其自身所掌握的局域网内主机的信息依次地发送攻击报文，就可能会导致整个局域网通信的中断，是 ARP 攻击中影响较为严重的一种。

2. 仿冒用户攻击

- 欺骗网关

  如图 2 所示，主机 A 仿冒主机 B 向网关发送了伪造的 ARP 报文，导致网关的 ARP 表中记录了错误的主机 B 地址映射关系，从而正常的数据报文不能正确地被主机 B 接收。

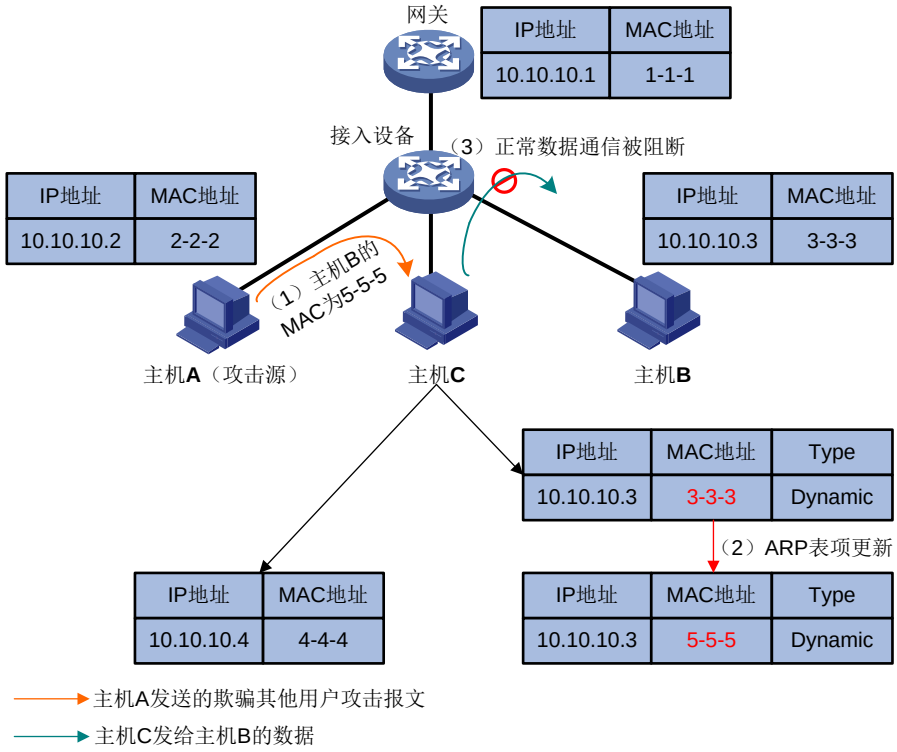
图2 欺骗网关攻击示意图



- 欺骗其他用户

  如图 3所示，主机 A 仿冒主机 B 向主机 C 发送了伪造的 ARP 报文，导致主机 C 的 ARP 表中记录了错误的主机 B 地址映射关系，从而正常的数据报文不能正确地被主机 B 接收。

图3 欺骗其他用户攻击示意图



3. ARP 泛洪攻击

网络设备在处理 ARP 报文时需要占用系统资源，同时因为系统内存和查找 ARP 表效率的要求，一般网络设备会限制 ARP 表的大小。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，使设备 ARP 表项溢出，合法用户的 ARP 报文不能生成有效的 ARP 表项，导致正常通信中断。另外，通过向设备发送大量目标 IP 地址不能解析的 IP 报文，使设备反复地对目标 IP 地址进行解析，导致 CPU 负荷过重，也是泛洪攻击的一种。

1.1.3 ARP 攻击的危害

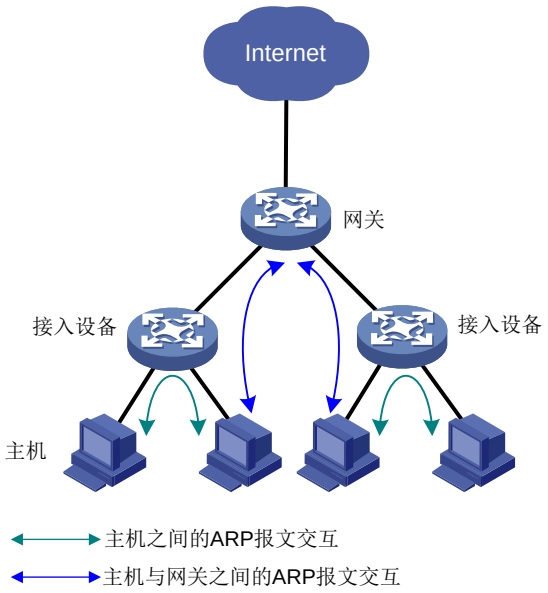
ARP 攻击是一种非常恶劣的网络攻击行为：

- 会造成网络不稳定，引发用户无法上网或者企业断网，导致重大生产事故。
- 利用 ARP 攻击可进一步实施攻击，非法获取游戏、网银、文件服务等系统的账号和口令，给被攻击者造成重大损失。

1.2 技术优点

针对上述网络中常见的 ARP 攻击行为，H3C 提供了完整的解决方案，可以避免客户网络受到 ARP 攻击。

图4 网络设备角色示意简图



如图 4 所示，ARP 攻击防范技术的思路是以设备角色为线索，通过分析二三层网络设备可能会面对的攻击类型，提供有效的防范措施。

- 攻击源一般来源于主机侧，因此接入设备在 ARP 攻击防御功能是一个关键控制点。
  - 通过建立正确的 ARP 映射关系、检测并过滤伪造的 ARP 报文，保证经过其转发的 ARP 报文正确合法。
  - 可抑制短时间内大量 ARP 报文的冲击。

  由于防范措施部署在接入设备，无需在网关上部署，因此可以减轻网关负担。
- 如果接入设备不支持 ARP 攻击防御功能，或者主机直接接入网关，则需要在网关上部署防御措施。
  - 通过建立正确的 ARP 表项，防止攻击者修改。
  - 可抑制短时间内大量 ARP 报文或者会触发 ARP 解析的 IP 报文的冲击。

  直接在网关上进行部署对接入设备的依赖较小，可以较好的支持现有网络，有效地保护用户设备。

2 接入设备 ARP 攻击防御技术实现

2.1 接入设备ARP攻击防御简介

接入设备可能受到的攻击类型为仿冒网关、仿冒用户和泛洪攻击。针对这三种攻击可以采用的防范措施为：

- 针对仿冒网关攻击

  对 ARP 报文的合法性进行检查，如果合法则进行后续处理，如果非法则丢弃报文。
  - ARP Detection 功能
  - ARP 过滤保护功能

- ARP 网关保护功能

- 针对仿冒用户攻击

  对 ARP 报文的合法性进行检查，如果合法则进行后续处理，如果非法则丢弃报文。

  - ARP Detection 功能
  - ARP 过滤保护功能

- 针对 ARP 泛洪攻击

  ARP 报文限速功能

2.2 ARP Detection功能

某 VLAN 内开启 ARP Detection 功能后，该 VLAN 内所有端口接收到的 ARP（请求与应答）报文将被重定向到 CPU 进行报文的用户合法性检查和报文有效性检查：如果认为该 ARP 报文合法，则进行转发；否则直接丢弃。

在 VXLAN 组网中，某 VSI 内开启 ARP Detection 功能后，该 VSI 下所有 AC 收到的 ARP 报文（请求与应答）报文将被重定向到 CPU 进行报文的用户合法性检查和报文有效性检查：如果认为该 ARP 报文合法，则进行转发；否则直接丢弃。

目前，ARP Detection 的三种具体实现机制如下：

- ARP 报文有效性检查
- 用户合法性检查
- ARP 报文强制转发

2.2.1 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，需要根据配置的检查模式对 MAC 地址和 IP 地址不合法的报文进行过滤：

- 源 MAC 地址的检查模式：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，一致认为报文有效，否则丢弃。
- 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：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。
- IP 地址检查模式：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。

2.2.2 用户合法性检查

用户合法性检查在 ARP 非信任端口或非信任 AC（Attachment Circuit，接入电路）上执行。对于 ARP 信任端口和信任 AC，不进行用户合法性检查。

ARP 非信任端口和非信任 AC 接收到 ARP 报文后，将 ARP 报文中的源 IP 地址和源 MAC 地址依次与用户合法性规则、用户表项（IP Source Guard 静态绑定表项、DHCP Snooping 表项、802.1X 安全表项）进行匹配，判断用户是否为所属 VLAN 所在接口上的合法用户、所属 VSI 所在 AC 上的合法用户。用户合法性检查的具体过程为：

(1) 如果找到与报文匹配的用户合法性规则，则按照该规则对报文进行处理。用户合法性规则以源 IP 地址范围、源 MAC 地址范围、报文的 VLAN ID 和 VSI 名称为匹配规则，对符合匹配规则的 ARP 报文进行转发或丢弃处理。

(2) 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。

(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。

上述过程中使用的 IP Source Guard 静态绑定表项由用户手工配置，DHCP Snooping 安全表项通过 DHCP Snooping 功能自动生成，802.1X 安全表项通过 802.1X 功能产生。其中，802.1X 用户使用支持将 IP 地址上传的客户端认证时，客户端会将 IP 地址上传至配置 ARP Detection 的设备，之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。

如果报文通过用户合法性检查，则对该报文进行二层转发。目的 IP 地址对应的 IP Source Guard 静态绑定表项、DHCP Snooping 表项和 802.1X 安全表项不影响报文的转发。

在用户在不同端口间来回迁移的场景下，可开启 ARP Detection 忽略端口匹配检查功能。开启 ARP Detection 忽略端口匹配检查功能后，ARP Detection 在根据表项进行用户合法性检查时，不会检查 ARP 报文入端口和表项中的端口是否匹配。

2.2.3 ARP 报文强制转发

ARP 报文强制转发基于非信任接口生效，对已经通过用户合法性检查的 ARP 报文进行处理：

- 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。

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。

2.2.4 ARP Detection 日志

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。

用户可以通过日志查看攻击情况。

2.3 ARP网关保护功能

ARP 网关保护功能在设备不与网关相连的端口上配置，可以防止仿冒网关攻击。

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；
- 如果不相同，认为此报文合法，继续进行后续处理。

2.4 ARP过滤保护功能

ARP 过滤保护功能用来限制接口上允许通过的 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。

2.5 ARP报文限速功能

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。在某个 VLAN 配置了 ARP Detection 功能后，设备会将该 VLAN 内所有接口收到的 ARP 报文重定向到 CPU 进行检查，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接口收到 ARP 报文的速率。

在接口上配置 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，超过限速部分的报文会被丢弃。设备还将进行如下操作：

- 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
- 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）。

3 网关设备 ARP 攻击防御技术实现

3.1 网关设备ARP攻击防御技术简介

网关设备可能受到的攻击类型为仿冒用户和泛洪攻击。针对这两种攻击可以采用的防范措施为：

- 针对仿冒用户攻击
  - 通过合法方式建立正确的 ARP 表项，并阻止攻击者修改
    - 授权 ARP 功能
    - ARP 自动扫描和固化功能
    - ARP 的 Keepalive 表项扫描
    - 配置静态 ARP 表项
  - 动态学习 ARP 表项前进行确认，保证学习到的是真实、正确的映射关系
    - ARP 主动确认功能
    - ARP 报文源 MAC 一致性检查功能
- 针对 ARP 泛洪攻击
  - 源 MAC 地址固定的 ARP 攻击检测功能
  - 指定源 MAC 地址的 ARP 报文限速功能

- 限制接口学习动态 ARP 表项的最大数目
- ARP 接口攻击抑制
- ARP 防 IP 报文攻击功能

3.2 授权ARP功能

授权 ARP 功能是指根据 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。该功能适用于采用 DHCP 协议动态分配主机 IP 地址的网络环境。

开启接口的授权 ARP 功能后：

- 只有静态 ARP 表项才可以覆盖授权 ARP 表项，授权 ARP 表项不会被 ARP 报文动态改写，因此保证了表项的正确性。
- 如果发送者冒用其它合法主机的 IP 地址发送 ARP 请求，因为 MAC 地址不是网关所记录的授权 ARP 表项中的合法 MAC 地址，伪造的 ARP 请求将不能得到应答，从而限制冒用合法 IP 地址的主机上网。
- 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。
- 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，及时删除对应的授权 ARP 表项。

3.3 ARP自动扫描和固化功能

ARP 自动扫描功能一般与 ARP 固化功能配合使用：

(1) 开启 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。

(2) 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。

推荐在网吧这种环境稳定的小型网络中使用这两个功能。

3.4 ARP的Keepalive表项扫描

在规模较大的组网环境中（比如园区网络），使用 ARP 自动扫描功能后，如果指定的扫描范围过大，会导致需要较长的时间才能扫描到异常下线的主机。开启 ARP 的 Keepalive 表项扫描后，系统可以通过 Keepalive 表项快速定位异常下线的主机，并在老化时间内对异常下线主机的状态进行监测。

用户上线后，系统会生成动态 ARP 表项和 IP Source Guard 绑定表项。开启本功能后，系统会根据这些表项建立状态为在线的 Keepalive 表项。用户下线后其 ARP 表项会被删除，对应的 Keepalive 表项的状态被置为离线。设备每隔一段时间会向处于离线状态的 Keepalive 表项对应的 IP 发送 ARP 请求报文，直到 Keepalive 表项的状态恢复成在线或离线状态的 Keepalive 表项被删除。处于离线状态的 Keepalive 表项在老化时间内没有恢复成在线便会被删除。

3.5 配置静态ARP表项

对于网络中重要的服务器等设备，可以将其 IP 地址和 MAC 地址的映射关系配置为静态 ARP 表项。这种静态映射关系不但不能被伪造的 ARP 报文动态改写，而且同样会限制对非法 ARP 请求的应答，从而保护服务器不受到攻击。

配置静态 ARP 表项虽然可以保护 ARP 表不被改写，但是配置工作量大，不适用于主机 IP 地址可能发生更改的网络环境，建议在比较小的网络里使用。

3.6 ARP主动确认功能

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 ARP 主动确认功能的严格模式后，新建 ARP 表项前，设备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，则解析成功后设备开启主动确认功能。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。

开启 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。

3.6.1 新建 ARP 表项前的主动确认

设备收到一个 ARP 报文时，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 ARP 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 ARP 表项。

3.6.2 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：

- 如果未超过 1 分钟，则设备不会对 ARP 表项进行更新。
- 如果已超过 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。

3.7 ARP报文源MAC一致性检查功能

ARP 报文源 MAC 一致性检查功能可以用来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。

配置本功能后，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。

3.8 源MAC地址固定的ARP攻击检测功能

当网关设备在短时间内收到同一个源发送的大量 ARP 报文时，就认定为发生了源 MAC 地址固定 ARP 攻击。

源 MAC 地址固定的 ARP 攻击检测功能根据 ARP 报文的源 MAC 地址进行统计，在一个探测周期内，如果收到同一源 MAC 地址的 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 日志信息功能的情况下，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，则会打印告警信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的模式为监控模式，则只打印告警信息，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，这样，即使该 MAC 地址发送大量 ARP 报文也不会被检测过滤。

3.9 指定源MAC地址的ARP报文限速功能

网络攻击者可能会构造大量 ARP 请求报文，向网络设备发起攻击。如果网关设备性能较低，收到大量 ARP 请求报文后，设备的 CPU 负担会过重，从而造成其他功能无法正常运行甚至设备瘫痪等问题。如果网络攻击者构造的 ARP 请求报文的源 MAC 地址相同，则可以限制指定源 MAC 地址的 ARP 请求报文的速率，丢弃超过限速部分的报文，从而减轻设备 CPU 的负担，避免 ARP 攻击。

3.10 限制接口学习动态ARP表项的最大数目

当指定接口下的动态 ARP 表项达到允许学习的最大数目后，将不允许学习动态 ARP 表项，以保证当一个接口所接入的某一台主机发起 ARP 攻击时不会导致整个设备的 ARP 表资源都被耗尽。

当配置接口学习动态 ARP 表项的最大数目为 0 时，表示禁止接口学习动态 ARP 表项。

3.11 ARP接口攻击抑制

为防止某个接口下非法用户构造大量 ARP 请求报文对设备进行 ARP 攻击，影响其它接口的 ARP 报文处理，设备会统计设备的三层接口上收到的 ARP 请求报文。在一个检测周期内，如果单个接口收到的 ARP 请求报文个数超过配置的 ARP 接口攻击抑制阈值，则认为该接口受到 ARP 攻击。确定受到 ARP 攻击后，设备会生成 ARP 接口攻击抑制表项，在 ARP 接口攻击抑制表项的抑制时间清零之前设备会限制被攻击的接口每秒钟接收 ARP 报文的速率，防止 ARP 攻击报文持续冲击 CPU。如果抑制时间内 ARP 收包个数大于或等于（表项抑制时间/检测周期）×抑制阈值，则抑制时间清零后设备将重置该表项的抑制时间。否则，设备删除该 ARP 接口攻击抑制表项，不再限制该接口接收 ARP 报文的速率。

3.12 ARP防IP报文攻击功能

如果网络中有主机通过向网关设备发送大量目标 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，设备提供了下列三个功能：

- 如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。

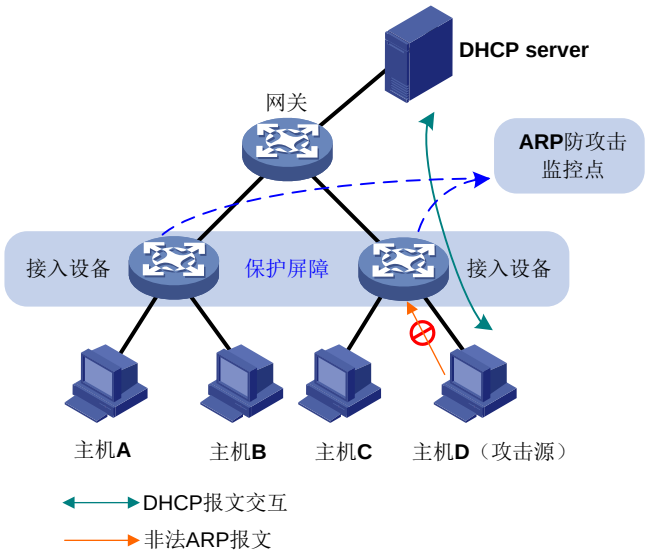
  开启该功能后，如果网络中某主机向设备某端口连续发送目标 IP 地址不能解析的 IP 报文，当每 5 秒内由此主机发出 IP 报文触发的 ARP 请求报文的流量超过设置的阈值，那么对于由此主机发出的 IP 报文，设备不允许其触发 ARP 请求，直至 5 秒后再处理，从而避免了恶意攻击所造成的危害。
- 如果发送攻击报文的源不固定，可以采用 ARP 黑洞路由功能。开启该功能后，一旦接收到目标 IP 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，使得设备在一段时间内将去往该地址的报文直接丢弃。黑洞路由老化之后，如果设备重新接收到目标 IP 地址不能解析的 IP 报文，将继续产生一个黑洞路由。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。
- 在网关开启发送端 IP 地址检查功能，手动限定 ARP 的学习范围。开启该功能后，如果指定 VLAN 内的 ARP 报文的发送端 IP 地址不在指定的源 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。

4 典型组网应用

4.1 监控部署方式

监控部署方式主要适用于动态接入用户居多的网络环境，如图 5 所示，网络内的主机通过 DHCP 服务器动态获取 IP 地址。

图5 监控方式部署组网图



在上述网络中，ARP 攻击防御的措施部署在接入设备上，网关设备和主机都无需另外进行攻击防御的配置。

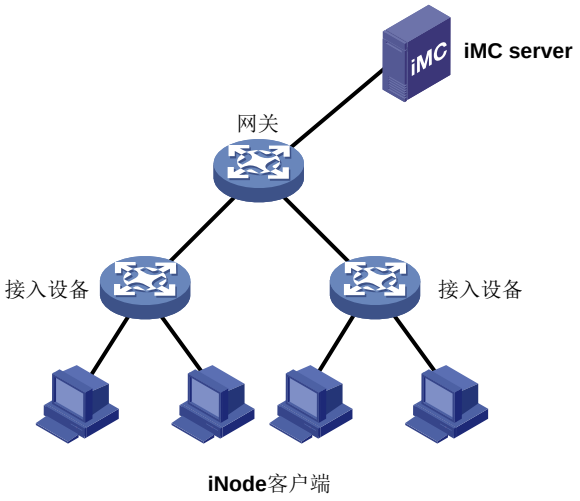
接入设备上运行的 ARP Detection 功能会根据 DHCP Snooping 的安全表项对通过本设备的 ARP 报文进行检查。如果用户侧主机的 ARP 报文中携带的发送者信息和 DHCP Snooping 安全表项的绑定信息不一致，报文将被认定为攻击报文并被丢弃。从而避免了网关或者其他主机的 ARP 表中记录错误的地址映射关系。

同时，建议在接入设备上配置 ARP 限速功能，防止 ARP 泛洪攻击。

4.2 认证部署方式

认证部署方式适合网络中采用接入认证的场景，如图 6 所示，接入设备通过与 H3C iMC（Intelligent Management Center，开放智能管理中枢）服务器、H3C iNode 客户端、网关的联动，全方面地防御 ARP 攻击。

图6 认证方式部署组网图



在上述组网中，iNode 客户端通过认证协议（802.1X 或 Portal）登录网络，iMC 服务器对客户端进行认证，接入设备绑定获取到的客户端的 IP+MAC 信息。ARP 攻击防御功能的措施部署在接入设备上：

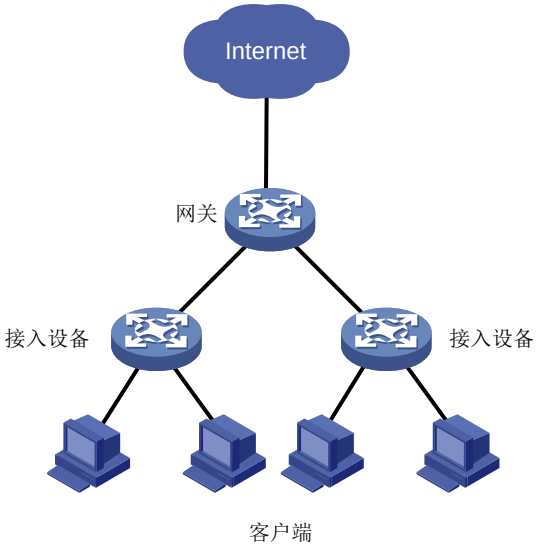
- 在接入设备的用户侧接口上开启 ARP 网关保护功能，可以防止伪造网关攻击；
- 在接入设备的网关侧接口上开启 ARP 过滤保护功能，可以防止伪造网关和伪造用户的攻击。

4.3 网吧等小型网络解决方案

在图 7 所示网吧等小型网络中，客户端比较稳定，不会经常新增或删除客户端。通过将 ARP 攻击防御技术部署在网关设备上，可防止用户私自修改客户端 IP 地址，使用户的网上行为有记录可循。

在本解决方案中，首先在网关上通过 ARP 自动扫描功能建立网吧等小型局域网内所有客户端的动态 ARP 表项，然后通过 ARP 固化功能将这些动态 ARP 表项转换为静态 ARP 表项。ARP 固化操作完成后，配置接口允许学习动态 ARP 表项的最大数目为 0，禁止接口学习动态 ARP 表项，即只允许和现有 ARP 表项一致的客户端才能访问 Internet。

图7 网吧等小型网络部署组网图



5 参考文献

- RFC 826：An Ethernet Address Resolution Protocol
- RFC 2131：Dynamic Host Configuration Protocol(DHCP)
- RFC 3046：DHCP Relay Agent Information Option