目 录

ARP

ARP 作用

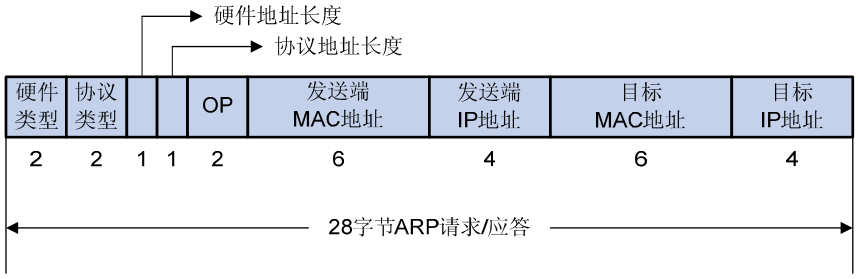
ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

在局域网中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报文必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。APR 就是实现这个功能的协议。

ARP 报文结构

ARP报文分为ARP请求和ARP应答报文，报文格式如 图 1所示。

图 1 ARP 报文结构



- 硬件类型：表示硬件地址的类型。它的值为 1 表示以太网地址；
- 协议类型：表示要映射的协议地址类型。它的值为 0x0800 即表示 IP 地址；
- 硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 6 和 4；
- 操作类型（OP）：1 表示 ARP 请求，2 表示 ARP 应答；
- 发送端 MAC 地址：发送方设备的硬件地址；
- 发送端 IP 地址：发送方设备的 IP 地址；
- 目标 MAC 地址：接收方设备的硬件地址。
- 目标 IP 地址：接收方设备的 IP 地址。

ARP 地址解析过程

假设主机A和B在同一个网段，主机A要向主机B发送信息。如 (4)图 2所示，具体的地址解析过程如下：

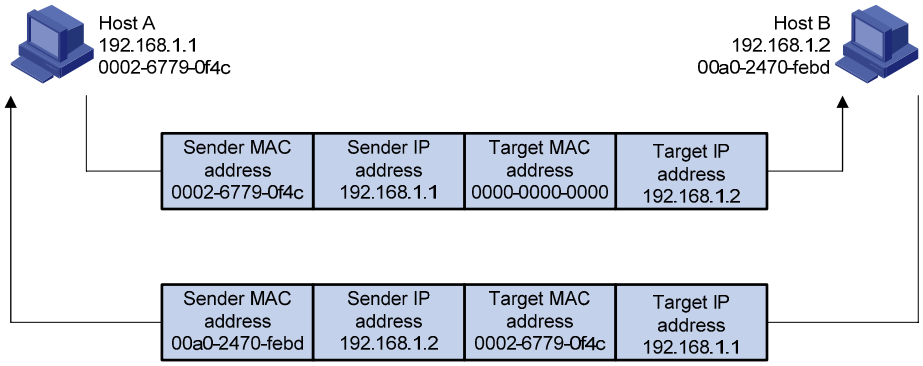
(1) 主机 A 首先查看自己的 ARP 表，确定其中是否包含有主机 B 对应的 ARP 表项。如果找到了对应的 MAC 地址，则主机 A 直接利用 ARP 表中的 MAC 地址，对 IP 数据包进行帧封装，并将数据包发送给主机 B。

(2) 如果主机 A 在 ARP 表中找不到对应的 MAC 地址，则将缓存该数据报文，然后以广播方式发送一个 ARP 请求报文。ARP 请求报文中的发送端 IP 地址和发送端 MAC 地址为主机 A 的 IP 地址和 MAC 地址，目标 IP 地址和目标 MAC 地址为主机 B 的 IP 地址和全 0 的 MAC 地址。由于 ARP 请求报文以广播方式发送，该网段上的所有主机都可以接收到该请求，但只有被请求的主机（即主机 B）会对该请求进行处理。

(3) 主机 B 比较自己的 IP 地址和 ARP 请求报文中的目标 IP 地址，当两者相同时进行如下处理：将 ARP 请求报文中的发送端（即主机 A）的 IP 地址和 MAC 地址存入自己的 ARP 表中。之后以单播方式发送 ARP 响应报文给主机 A，其中包含了自己的 MAC 地址。

(4) 主机 A 收到 ARP 响应报文后，将主机 B 的 MAC 地址加入到自己的 ARP 表中以用于后续报文的转发，同时将 IP 数据包进行封装后发送出去。

图 2 ARP 地址解析过程



当主机 A 和主机 B 不在同一网段时，主机 A 就会先向网关发出 ARP 请求，ARP 请求报文中的目标 IP 地址为网关的 IP 地址。当主机 A 从收到的响应报文中获得网关的 MAC 地址后，将报文封装并发给网关。如果网关没有主机 B 的 ARP 表项，网关会广播 ARP 请求，目标 IP 地址为主机 B 的 IP 地址，当网关从收到的响应报文中获得主机 B 的 MAC 地址后，就可以将报文发给主机 B；如果网关已经有主机 B 的 ARP 表项，网关直接把报文发给主机 B。

ARP 表

设备通过 ARP 解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址到 MAC 地址的映射表项，以用于后续到同一目的地报文的转发。

ARP 表项分为动态 ARP 表项和静态 ARP 表项。

动态 ARP 表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口 down 时会删除相应的动态 ARP 表项。

静态 ARP 表项

静态 ARP 表项通过手工配置和维护，不会被老化，不会被动态 ARP 表项覆盖。

配置静态 ARP 表项可以增加通信的安全性。静态 ARP 表项可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

静态 ARP 表项分为短静态 ARP 表项和长静态 ARP 表项。

- 在配置长静态 ARP 表项时，除了配置 IP 地址和 MAC 地址项外，还必须配置该 ARP 表项所在 VLAN 和出接口。长静态 ARP 表项可以直接用于报文转发。
- 在配置短静态 ARP 表项时，只需要配置 IP 地址和 MAC 地址项。如果出接口是三层以太网接口，短静态 ARP 表项可以直接用于报文转发；如果出接口是 VLAN 虚接口，短静态 ARP 表项不能直接用于报文转发，当要发送 IP 数据包时，先发送 ARP 请求报文，如果收到的响应报文中的源 IP 地址和源 MAC 地址与所配置的 IP 地址和 MAC 地址相同，则将接收 ARP 响应报文的接口加入该静态 ARP 表项中，之后就可以用于 IP 数据包的转发。

说明

- 一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。
- 当希望设备和指定用户只能使用某个固定的 IP 地址和 MAC 地址通信时，可以配置短静态 ARP 表项，当进一步希望限定这个用户只在某 VLAN 内的某个特定接口上连接时就可以配置长静态 ARP 表项。

免费 ARP

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 IP 地址都是本机 IP 地址，报文源 MAC 地址是本机 MAC 地址，报文的目的 MAC 地址是广播地址。

设备通过对外发送免费 ARP 报文来实现以下功能：

- 确定其它设备的 IP 地址是否与本机的 IP 地址冲突。当其它设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。
- 设备改变了硬件地址，通过发送免费 ARP 报文通知其它设备更新 ARP 表项。

免费 ARP 报文学习功能的作用

使能了免费 ARP 报文学习功能后，设备会根据收到的免费 ARP 报文中携带的信息（源 IP 地址、源 MAC 地址）对自身维护的 ARP 表进行修改。设备先判断 ARP 表中是否存在与此免费 ARP 报文源 IP 地址对应的 ARP 表项：

- 如果没有对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息新建 ARP 表项；
- 如果存在对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息更新对应的 ARP 表项。

关闭免费 ARP 报文学习功能后，设备不会根据收到的免费 ARP 报文来新建 ARP 表项，但是会更新已存在的对应 ARP 表项。如果用户不希望通过免费 ARP 报文来新建 ARP 表项，可以关闭免费 ARP 报文学习功能，以节省 ARP 表项资源。

定时发送免费 ARP 功能的作用

定时发送免费 ARP 功能可以及时通知下行设备更新 ARP 表项或者 MAC 地址表项，主要应用场景如下：

(1) 防止仿冒网关的 ARP 攻击

如果攻击者仿冒网关发送免费 ARP 报文，就可以欺骗同网段内的其它主机，使得被欺骗的主机访问网关的流量，被重定向到一个错误的 MAC 地址，导致其它主机用户无法正常访问网络。

为了尽量避免这种仿冒网关的 ARP 攻击，可以在网关的接口上使能定时发送免费 ARP 功能。使能该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，每台主机都可以学习到正确的网关，从而正常访问网络。

(2) 防止主机 ARP 表项老化

在实际环境中，当网络负载较大或接收端主机的 CPU 占用率较高时，可能存在 ARP 报文被丢弃或主机无法及时处理接收到的 ARP 报文等现象。这种情况下，接收端主机的动态 ARP 表项会因超时而被老化，在其重新学习到发送设备的 ARP 表项之前，二者之间的流量就会发生中断。

为了解决上述问题，可以在网关的接口上使能定时发送免费 ARP 功能。使能该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，接收端主机可以及时更新 ARP 映射表，从而防止了上述流量中断现象。

(3) 防止 VRRP 虚拟 IP 地址冲突

当网络中存在 VRRP 备份组时，需要由 VRRP 备份组的 Master 路由器周期性的向网络内的主机发送免费 ARP 报文，使主机更新本地 ARP 地址表，确保网络中不会存在与 VRRP 虚拟 IP 地址相同的设备。

由于用户可以设定 VRRP 虚拟 IP 地址和 MAC 地址对应关系，因此有以下两种情况：

- 如果当前 VRRP 虚拟 IP 地址和虚拟 MAC 地址对应，则免费 ARP 报文中的源 MAC 地址为 VRRP 虚拟路由器对应的虚拟 MAC 地址。
- 如果当前 VRRP 虚拟 IP 地址和实际 MAC 地址对应，则免费 ARP 报文中的源 MAC 地址为 VRRP 备份组中 Master 路由器接口的 MAC 地址。

(4) 及时更新模糊终结 VLAN 内设备的 MAC 地址表

三层以太网子接口上同时配置了模糊终结多个 VLAN 和 VRRP 备份组时，为了避免发送过多的 VRRP 通告报文，需要关闭 VLAN 终结支持广播/组播功能，并配置 VRRP 控制 VLAN。此时，为了及时更新各个模糊终结 VLAN 内设备的 MAC 地址表项，可以在三层以太网子接口上使能定时发送免费 ARP 功能。使能该功能后，三层以太网子接口将按照配置的时间间隔周期性发送 VRRP 虚拟 IP 地址、接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，当 VRRP 主备状态切换时，各个模糊终结 VLAN 内设备上可以及时更新为正确的 MAC 地址表项。

代理 ARP

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP（Proxy ARP）。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

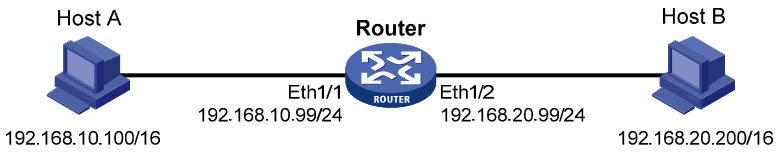
- 普通代理 ARP 的应用环境为：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP 的应用环境为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

普通代理 ARP

处于同一网段内的主机，当连接到设备的不同三层接口时，可以利用设备的代理 ARP 功能，通过三层转发实现互通。

代理ARP的典型应用环境如 图 3所示。设备Router通过两个三层接口Ethernet1/1 和Ethernet1/2 连接两个网络，两个三层接口的IP地址不在同一个网段，接口地址分别为 192.168.10.99/24、192.168.20.99/24。但是两个网络内的主机Host A和Host B的地址通过掩码的控制，既与相连设备的接口地址在同一网段，同时二者也处于同一个网段。

图 3 普通代理 ARP 的应用环境



在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IP 地址与本机的 IP 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 ARP 请求。但是，此时的两台主机处于不同的广播域中，Host B 无法收到 Host A 的 ARP 请求报文，当然也就无法应答。

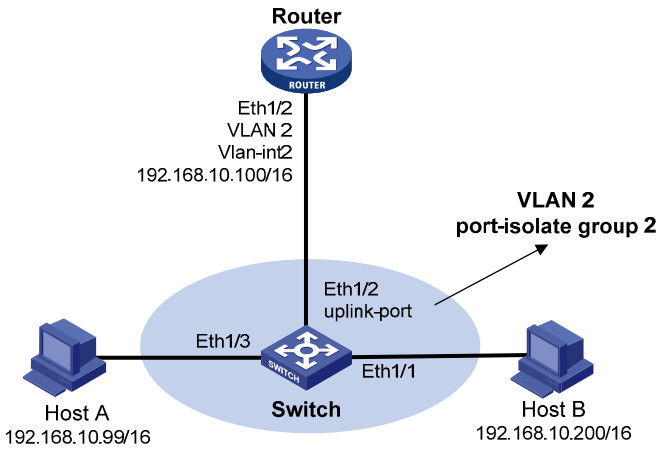
通过在 Router 上启用代理 ARP 功能，可以解决此问题。启用代理 ARP 后，Router 可以应答 Host A 的 ARP 请求。同时，Router 相当于 Host B 的代理，把从其他主机发送过来的报文转发给它。

代理 ARP 的优点是，它可以只被应用在一个设备上（此时该设备的作用相当于网关），不会影响到网络中其他设备的路由表。代理 ARP 功能可以在 IP 主机没有配置缺省网关或者 IP 主机没有任何路由能力的情况下使用。

本地代理 ARP

本地代理ARP的应用场景如 图 4所示。Host A和Host B属于同一个VLAN 2，但它们分别连接到被二层隔离的端口Ethernet1/3 和Ethernet1/1 上，通过在Router上启用本地代理ARP功能，可以实现Host A和Host B的三层互通。

图 4 本地代理 ARP 的应用环境



本地代理 ARP 可以在下列三种情况下实现主机之间的三层互通：

- 想要互通的主机分别连接到同一个 VLAN 中的不同二层隔离端口下；
- 使能 Super VLAN 功能后，想要互通的主机属于不同的 Sub VLAN；
- 使能 Isolate-user-vlan 功能后，想要互通的主机属于不同的 Secondary VLAN。

ARP Snooping

ARP Snooping 作用

ARP Snooping 功能是一个用于二层交换网络环境的特性，通过侦听 ARP 报文建立 ARP Snooping 表项，从而提供给 ARP 快速应答和 MFF 手动方式等使用。

ARP Snooping 工作机制

设备上的一个 VLAN 使能 ARP Snooping 后，该 VLAN 内所有端口接收的 ARP 报文会被重定向到 CPU。CPU 对重定向上送的 ARP 报文进行分析，获取 ARP 报文的源 IP 地址、源 MAC 地址、源 VLAN 和入端口信息，建立记录用户信息的 ARP Snooping 表项。

ARP Snooping 表项的老化时间为 25 分钟，有效时间为 15 分钟。如果一个 ARP Snooping 表项自最后一次更新后 15 分钟内没有收到 ARP 更新报文，则此表项开始进入失效状态，不再对外提供服务，其他特性查找此表项将会失败。当收到源 IP 地址和源 MAC 与已存在的 ARP Snooping 表项 IP 地址和 MAC 均相同的 ARP 报文时，此 ARP Snooping 表项进行更新，重新开始生效，并重新老化计时。当 ARP Snooping 表项达到老化时间后，则将此 ARP Snooping 表项删除。

如果 ARP Snooping 收到 ARP 报文时检查到相同 IP 的 ARP Snooping 表项已经存在，但是 MAC 地址发生了变化，则认为发生了攻击，此时 ARP Snooping 表项处于冲突状态，表项失效，不再对外提供服务，并在 25 分钟后删除此表项。

ARP 快速应答

ARP 快速应答作用

在无线产品组网中，AC 与 AP 会建立隧道连接，Client 通过 AP 连接到 AC，通过 AC，Client 可以与网关建立连接。当 Client 发起 ARP 广播请求时，需要通过 AC 向所有的 AP 复制 ARP 请求，这样会导致 ARP 广播占用隧道的大量资源，导致性能下降。为了减少 ARP 广播占用的隧道资源，可以在 AC 上启用 ARP 快速应答功能，减少 ARP 广播报文的影响。

ARP 快速应答功能就是根据 AC 设备收集的用户信息（用户信息可以是 DHCP Snooping 表项，也可以是 ARP Snooping 表项），在指定的 VLAN 内，尽可能的对 ARP 请求进行应答，从而减少 ARP 广播报文。

ARP 快速应答工作机制

ARP 快速应答的工作机制如下：

(1) 设备接收到 ARP 请求报文时，如果请求报文的目的 IP 地址是设备的 VLAN 虚接口的 IP 地址，则由 ARP 特性进行处理；

(2) 如果 ARP 请求报文的目的 IP 地址不是 VLAN 虚接口的 IP 地址，则根据报文中的目的 IP 地址查找 DHCP Snooping 表项：

- 如果查找成功，但是查找到的表项的接口和收到请求报文的接口一致，并且接口是以太网接口，则不进行应答，否则立即进行应答。
- 如果查找失败，则继续查找 ARP Snooping 表项，如果查找成功，但是查找到的表项的接口和收到请求报文的接口一致，并且接口是以太网接口，则不进行应答，否则立即进行应答。
- 如果两个表均查找失败，则直接转发请求报文或将报文交于其他特性处理。

ARP 攻击防御

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检测和解决。

下面将详细介绍一下这些技术的原理。

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。

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。

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 地址进行统计，在 5 秒内，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。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 存在攻击也不会被检测过滤。

只对上送 CPU 的 ARP 报文进行统计。

ARP 报文源 MAC 一致性检查功能简介

ARP 报文源 MAC 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。

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”。

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。

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。

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，一致认为有效，否则丢弃；
- 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。

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。

- 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。
- 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。
- 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。

ARP 报文强制转发

ARP 报文强制转发功能是将 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，按照一定的规则进行转发的防攻击功能，此功能不对 ARP 信任端口接收到的通过用户合法性检查的 ARP 报文进行限制。

对于从 ARP 非信任端口收到的已经通过用户合法性检查的合法 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。

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。

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。

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。

MFF

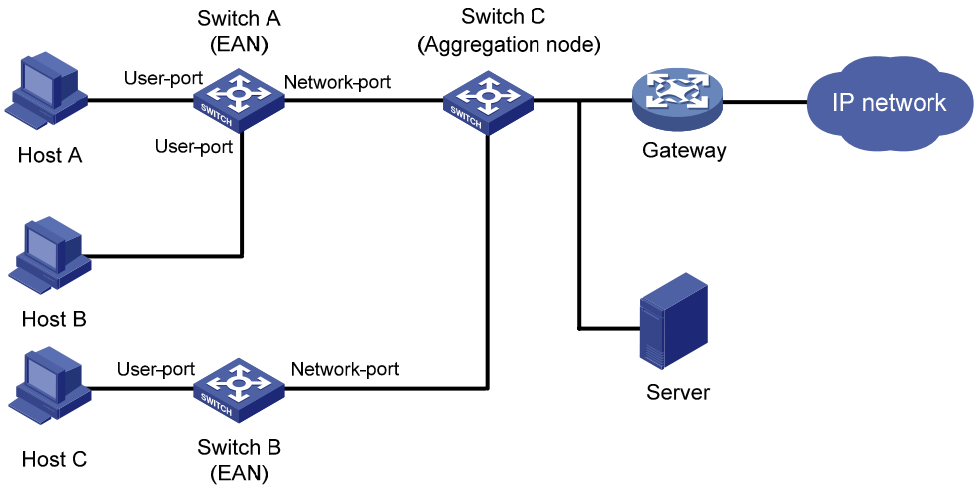
MFF 作用

在传统的以太网组网方案中，为了实现不同客户端主机之间的二层隔离和三层互通，通常采用在交换机上划分 VLAN 的方法。但是当彼此间需要二层隔离的用户较多时，这种方式会占用大量的 VLAN 资源；同时，为实现客户端之间三层互通，需要为每个 VLAN 规划不同的 IP 网段，并配置 VLAN 接口的 IP 地址，因此划分过多的 VLAN 会降低 IP 地址的分配效率。

为了改善这种现状，MAC-Forced Forwarding（下文统一用“MFF”替代）为同一广播域内实现客户端主机间的二层隔离和三层互通，提供了一种解决方案。

MFF 截获用户的 ARP 请求报文，通过 ARP 代答机制，回复网关 MAC 地址的 ARP 应答报文。通过这种方式，可以强制用户将所有流量（包括同一子网内的流量）发送到网关，使网关可以监控数据流量，防止用户之间的恶意攻击，能更好的保障网络部署的安全性。

图 5 应用组网图



如 图 5所示，Switch A和Switch B作为以太网接入节点（Ethernet Access Nodes，EAN），提供了客户端主机与汇聚节点（Switch C）之间的连接。在以太网接入节点上配置MFF功能，可以使客户端的数据报文交互全部通过网关转发，实现了客户端之间的三层互通，又保证了二层数据的隔离。

MFF 通常与 DHCP Snooping、ARP Snooping、IP Source Guard、ARP Detection、VLAN 映射等功能配合使用，在接入层交换机上实现客户端的流量过滤、二层隔离和三层互通，提高接入层网络的安全性。

MFF 端口角色

MFF 特性包括两种端口角色：用户端口及网络端口。

用户端口

MFF 的用户端口是指直接接入网络终端用户的端口。

用户端口上对于不同的报文处理如下：

- 允许组播报文和 DHCP 报文通过；
- 对于 ARP 报文则上送 CPU 进行处理；
- 若已经学习到网关 MAC 地址，则仅允许目的 MAC 地址为网关 MAC 地址的单播报文通过，其他报文都将被丢弃；若没有学习到网关 MAC 地址，目的 MAC 地址为网关 MAC 地址的单播报文也被丢弃。

网络端口

MFF 的网络端口是指连接其他网络设备如接入交换机、汇聚交换机或网关的端口。

网络端口上对于不同的报文处理如下：

- 允许组播报文和 DHCP 报文通过；
- 对于 ARP 报文则上送 CPU 进行处理；
- 拒绝其他广播报文通过。

MFF 运行模式

MFF 特性包括两种运行模式：手工方式和自动方式。

手工方式

手工方式应用于用户静态配置 IP 地址的场景中，这是因为在用户静态配置 IP 地址时，无法通过 DHCP 报文来获取网关信息。另外，在用户静态配置 IP 时，由于没有依据进行用户与网关的映射，因此仅维护缺省网关的 MAC 地址，即，一个 VLAN 下仅维护一个网关 MAC 地址。

使能了手工方式后，MFF 代答网关对用户的 ARP 请求，以及伪造 ARP 请求探测网关 MAC 的依据都是 ARP Snooping 表项。

若在 MFF 学习到缺省网关 MAC 地址后，收到来自网关的携带了与记录的 MAC 地址不同的源 MAC 地址的 ARP 报文，则需要更新记录的网关 MAC 地址。

自动方式

自动方式应用于用户通过 DHCP 协议动态获取 IP 地址的场景中。DHCP Snooping 功能通过侦听 DHCP ACK 报文，并解析其中的 Option 3 字段（Router IP）来获取网关 IP 地址。

在使能 MFF 自动方式时，每一个 DHCP Snooping 用户绑定表项都应该有相对应的唯一网关 IP 地址。若 DHCP ACK 报文携带多个网关 IP 地址，则只记录第一个。若学习到的用户绑定表项不包含网关 IP 地址，或者没有记录在用户绑定表项中，则自动方式会根据当前 VLAN 记录的第一个网关作为用户网关应答该用户的 ARP 请求，除非其请求的是一个已知的网关地址。

同时，针对每一个网关 IP 地址，从第一个与其对应的用户绑定表项中获取用户 IP 地址及 MAC 地址，封装并伪造 ARP 请求，用于探测网关的 MAC 地址。


说明

- 自动方式下，一个 VLAN 内最多可以学习并维护 20 个网关信息，超过此限制的网关不再学习及处理。网关 IP 获取之后不会进行更新，即网关信息一旦生成就不会老化，除非去使能 MFF。
- 若在 MFF 学习到网关 MAC 地址后，收到来自网关的 ARP 报文，携带了与记录 MAC 地址不同的源 MAC 地址，则需要更新记录的网关 MAC 地址。

MFF 工作机制

用户之间的三层互通是通过类似代理 ARP 的 ARP 代答机制保证。另外，这种代答机制也在一定程度上减少了网络侧和用户侧之间的广播报文数量。

针对 ARP 报文，MFF 具体进行以下处理：

- 代答用户 ARP 请求。替代网关给用户主机回应 ARP 报文，使用户之间的报文交互都通过网关进行三层转发。这里，用户主机的 ARP 请求，既包含对于网关的请求，也包含对于其他用户 IP 的 ARP 请求。
- 代答网关 ARP 请求。替代用户主机给网关回应 ARP 报文。如果网关请求的表项在 MFF 设备上存在，就根据表项进行代答。如果表项还没有建立，则转发请求。以便达到减少广播的目的。

- 转发用户主机和网关发来的 ARP 应答。
- 监听网络中的 ARP 报文。更新网关 IP 地址和 MAC 地址对应表并广播。