目 录

1 ARP ····· 1-1
1.1 ARP简介 ····· 1-1
1.1.1 ARP报文结构 ····· 1-1
1.1.2 ARP地址解析过程 ····· 1-1
1.1.3 ARP表项类型 ····· 1-2
1.2 ARP配置任务简介 ····· 1-3
1.3 手工添加静态ARP表项 ····· 1-4
1.3.1 手工添加短静态ARP表项 ····· 1-4
1.3.2 手工添加长静态ARP表项 ····· 1-4
1.4 配置动态ARP表项的相关功能 ····· 1-4
1.4.1 配置设备学习动态ARP表项的最大数目 ····· 1-4
1.4.2 配置接口学习动态ARP表项的最大数目 ····· 1-5
1.4.3 配置动态ARP表项的老化时间 ····· 1-5
1.4.4 开启动态ARP表项的检查功能 ····· 1-6
1.5 开启在地址借用的接口学习不同网段ARP表项的功能 ····· 1-6
1.6 开启ARP日志信息功能 ····· 1-7
1.7 ARP显示和维护 ····· 1-7
1.8 ARP典型配置举例 ····· 1-8
1.8.1 长静态ARP表项配置举例 ····· 1-8
1.8.2 短静态ARP表项配置举例 ····· 1-9
2 免费ARP ····· 2-1
2.1 免费ARP简介 ····· 2-1
2.1.1 IP地址冲突检测 ····· 2-1
2.1.2 免费ARP报文学习 ····· 2-1
2.1.3 定时发送免费ARP ····· 2-1
2.2 免费ARP配置任务简介 ····· 2-2
2.3 开启源IP地址冲突提示功能 ····· 2-2
2.4 开启免费ARP报文学习功能 ····· 2-3
2.5 开启定时发送免费ARP功能 ····· 2-3
2.6 开启设备收到非同一网段ARP请求时发送免费ARP报文功能 ····· 2-3
2.7 配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔 ····· 2-4

3 代理ARP ····· 3-1
3.1 代理ARP简介 ····· 3-1
3.2 开启普通代理ARP功能 ····· 3-1
3.3 开启本地代理ARP功能 ····· 3-1
3.4 代理ARP显示和维护 ····· 3-2
3.5 普通代理ARP典型配置举例 ····· 3-2
3.5.1 普通代理ARP基本组网配置举例 ····· 3-2
4 ARP Snooping ····· 4-1
4.1 ARP Snooping简介 ····· 4-1
4.1.1 ARP Snooping表项建立机制 ····· 4-1
4.1.2 ARP Snooping表项老化机制 ····· 4-1
4.1.3 ARP Snooping表项冲突处理机制 ····· 4-1
4.2 ARP Snooping与硬件适配关系 ····· 4-1
4.3 开启ARP Snooping功能 ····· 4-2
4.4 ARP Snooping显示和维护 ····· 4-3
5 ARP快速应答 ····· 5-1
5.1 ARP快速应答简介 ····· 5-1
5.2 ARP快速应答与硬件适配关系 ····· 5-1
5.3 开启ARP快速应答功能 ····· 5-2
5.4 ARP快速应答典型配置举例 ····· 5-3
5.4.1 ARP快速应答基本组网配置举例 ····· 5-3
6 即插即用网关 ····· 6-1
6.1 即插即用网关简介 ····· 6-1
6.2 即插即用网关配置准备 ····· 6-1
6.3 开启即插即用网关功能 ····· 6-1
6.4 即插即用网关显示和维护 ····· 6-1
6.5 即插即用网关典型配置举例 ····· 6-2
6.5.1 即插即用网关基本组网配置举例 ····· 6-2
7 ARP泛洪抑制 ····· 7-1
7.1 ARP泛洪抑制简介 ····· 7-1
7.2 ARP泛洪抑制与硬件适配关系 ····· 7-1
7.3 开启ARP泛洪抑制功能 ····· 7-2
7.4 ARP泛洪抑制显示和维护 ····· 7-3
7.5 ARP泛洪抑制典型配置举例 ····· 7-3
7.5.1 ARP泛洪抑制基本组网配置举例 ····· 7-3

8 ARP直连路由通告 8-1
8.1 ARP直连路由通告简介 8-1
8.1.1 工作机制 8-1
8.1.2 L2VPN接入L3VPN组网应用 8-1
8.2 开启ARP直连路由通告功能 8-1

1 ARP

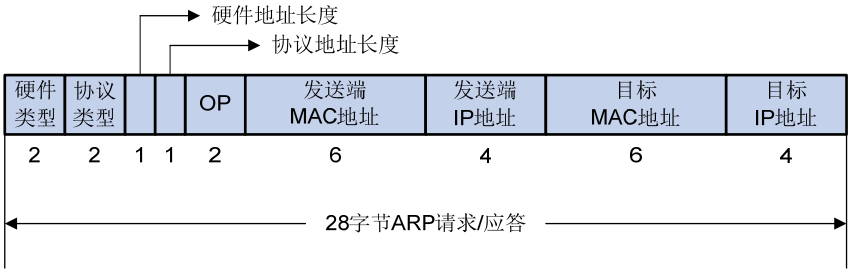
1.1 ARP简介

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。在网络中，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），由于 IP 数据报必须封装成帧才能通过物理网络发送，因此还需要知道对方的物理地址，所以设备上需要存在一个从 IP 地址到物理地址的映射关系。ARP 就是实现这个功能的协议。

1.1.1 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 1-1 所示。

图1-1 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。

1.1.2 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 图 1-2 所示，具体的地址解析过程如下：

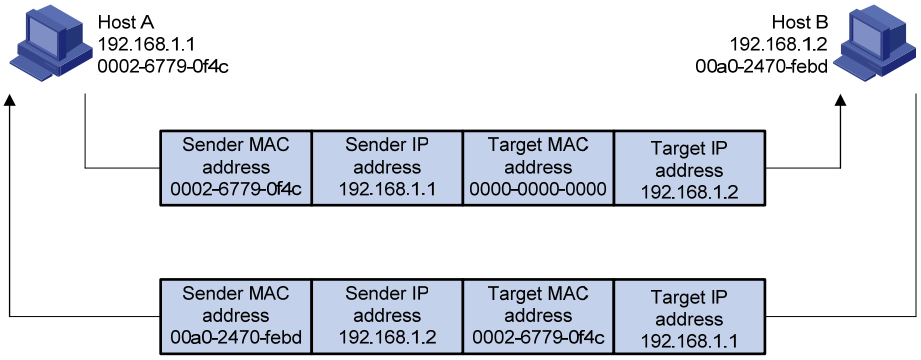
(1) 主机 A 首先查看自己的 ARP 表，确定其中是否包含有主机 B 对应的 ARP 表项。如果找到了对应的 MAC 地址，则主机 A 直接利用 ARP 表中的 MAC 地址，对 IP 数据报进行帧封装，并将 IP 数据报发送给主机 B。

(2) 如果主机 A 在 ARP 表中找不到对应的 MAC 地址，则将缓存该 IP 数据报，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 数据报进行封装后发送出去。

图1-2 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。

1.1.3 ARP表项类型

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 地址和 MAC 地址映射关系的表项，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、静态 ARP 表项、OpenFlow ARP 表项和 Rule ARP 表项。

1. 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、接口状态 down 时，系统会删除相应的动态 ARP 表项。

2. 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、长静态 ARP 表项。

- 长静态 ARP 表项可以直接用于报文转发，除了包括 IP 地址和 MAC 地址外，还需要包括以下两种表项内容之一：
  - 该 ARP 表项所在 VLAN 和出接口；
  - 该 ARP 表项的入接口和出接口对应关系。
- 短静态 ARP 表项只包括 IP 地址和 MAC 地址。

  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，需要对表项进行解析：当要发送 IP 数据报时，设备先发送 ARP 请求报文，如果收到的响应报文中的发送端 IP 地址和发送端 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，此时，该短静态 ARP 表项由未解析状态变为解析状态，之后就可以用于报文转发。

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。

3. OpenFlow ARP表项

OpenFlow ARP 表项由 OpenFlow 添加，不会被老化，不能通过 ARP 报文更新。可以直接用于转发报文。关于 OpenFlow 的介绍，请参见“OpenFlow 配置指导”中的“OpenFlow”。

4. Rule ARP表项

Rule ARP 表项不会被老化，不能通过 ARP 报文更新，可以被静态 ARP 表项覆盖，可以直接用于转发报文。Rule ARP 表项可由如下特性添加：

- Portal，Portal 的详细介绍请参见“安全配置指导”中的“Portal”。
- VXLAN，VXLAN 的详细介绍请参见“VXLAN 配置指导”中的“VXLAN”。

1.2 ARP配置任务简介

本节中的所有配置均为可选，请根据实际情况选择配置。

- 手工添加静态ARP表项
  - 手工添加短静态ARP表项
  - 手工添加长静态ARP表项
- 配置动态ARP表项的相关功能
  - 配置设备学习动态ARP表项的最大数目
  - 配置接口学习动态ARP表项的最大数目
  - 配置动态ARP表项的老化时间
  - 开启动态ARP表项的检查功能
- 开启在地址借用的接口学习不同网段ARP表项的功能
- 开启ARP日志信息功能

1.3 手工添加静态ARP表项

静态 ARP 表项在设备正常工作期间一直有效。

1.3.1 手工添加短静态ARP表项

1. 配置限制和指导

对于已经解析的短静态 ARP 表项，会由于外部事件，比如解析到的出接口状态 down 或设备的 ARP 表项所对应的 VLAN 或 VLAN 接口被删除等原因，恢复到未解析状态。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 手工添加短静态 ARP 表项。

arp static *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]

1.3.2 手工添加长静态ARP表项

1. 功能简介

长静态 ARP 表项根据设备的当前状态可能处于有效或无效两种状态。处于无效状态的原因可能是该 ARP 表项中的 IP 地址与本地 IP 地址冲突或设备上没有与该 ARP 表项中的 IP 地址在同一网段的接口地址等原因。处于无效状态的长静态 ARP 表项不能指导报文转发。当长静态 ARP 表项所对应的 VLAN 或 VLAN 接口被删除时，该 ARP 表项会被删除。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 手工添加长静态 ARP 表项。

arp static *ip-address mac-address* [*vlan-id interface-type interface-number* | *interface-type interface-number interface-type interface-number* | **vsi-interface** *vsi-interface-id* **tunnel** *number* **vsi** *vsi-name*] [**vpn-instance** *vpn-instance-name*]

1.4 配置动态ARP表项的相关功能

1.4.1 配置设备学习动态ARP表项的最大数目

1. 功能简介

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止用户占用过多的 ARP 资源，可以通过设置设备学习动态 ARP 表项的最大数目来进行限制。当设备学习动态 ARP 表项的数目达到所设置的值时，该设备上将不再学习动态 ARP 表项。

当本命令配置的动态 ARP 表项的最大数目小于设备当前已经学到的动态 ARP 表项数目，已学到的动态 ARP 表项不会被直接删除，用户可以通过执行 **reset arp dynamic** 命令直接清除动态 ARP 表项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置设备允许学习动态 ARP 表项的最大数目。

（独立运行模式）

arp max-learning-number *max-number*

（IRF 模式）

arp max-learning-number *max-number* **slot** *slot-number*

缺省情况下，设备允许学习的动态 ARP 表项的最大数目为 4096。

当配置设备允许学习动态 ARP 表项的最大数目为 0 时，表示禁止本设备学习动态 ARP 表项。

1.4.2 配置接口学习动态ARP表项的最大数目

1. 功能简介

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止部分接口下的用户占用过多的 ARP 资源，可以通过设置接口学习动态 ARP 表项的最大数目来进行限制。当接口学习动态 ARP 表项的数目达到所设置的值时，该接口将不再学习动态 ARP 表项。

如果二层接口及其所属的 VLAN 接口都配置了允许学习动态 ARP 表项的最大数目，则只有二层接口及 VLAN 接口上的动态 ARP 表项数目都没有超过各自配置的最大值时，才会学习 ARP 表项。

设备各接口学习的动态 ARP 表项之和不会超过该设备学习动态 ARP 表项的最大数目。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口允许学习动态 ARP 表项的最大数目。

arp max-learning-num *max-number*

缺省情况下，设备允许学习动态 ARP 表项的最大数目为 4096。

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

1.4.3 配置动态ARP表项的老化时间

1. 功能简介

为适应网络的变化，ARP 表需要不断更新。ARP 表中的动态 ARP 表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将从 ARP 表中删除，这个生存周期被称作老化时间。如果在到达老化时间前记录被刷新，则重新计算老化时间。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置动态 ARP 表项的老化时间。

arp timer aging *aging-time*

缺省情况下，动态 ARP 表项的老化时间为 20 分钟。

1.4.4 开启动态ARP表项的检查功能

1. 功能简介

动态 ARP 表项检查功能可以控制设备上是否可以学习 ARP 报文中的发送端 MAC 地址为组播 MAC 的动态 ARP 表项。

- 开启 ARP 表项的检查功能后，设备上不能学习 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也不能手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。
- 关闭 ARP 表项的检查功能后，设备可以学习以太网源 MAC 地址为单播 MAC 且 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也可以手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启动态 ARP 表项的检查功能。

arp check enable

缺省情况下，动态 ARP 表项的检查功能处于开启状态。

1.5 开启在地址借用的接口学习不同网段ARP表项的功能

1. 功能简介

在某些组网环境中，当配置某个接口借用指定接口 IP 地址后，由于借到的地址所在的网段和对端接口的地址可能处于不同网段，导致接口收到不同网段的 ARP 报文时无法学习到 ARP 表项。配置本功能后，可以使接口收到不在同一网段的 ARP 报文后学习对应的 ARP 表项，保证该接口和对端可以通信。

关闭本功能后，配置了地址借用功能的接口不再学习不同网段的 ARP 表项，已经学到的 ARP 表项老化后删除。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置本接口借用指定接口的 IP 地址。

ip address unnumbered interface *interface-type interface-number*

缺省情况下，本接口未借用其它接口的 IP 地址。

(4) 开启在地址借用的接口学习不同网段 ARP 表项的功能。

arp ip-unnumbered learning enable

缺省情况下，在地址借用的接口学习不同网段 ARP 表项的功能处于关闭状态。

1.6 开启ARP日志信息功能

1. 功能简介

ARP 日志可以方便管理员定位问题和解决问题，对处理 ARP 报文的信息进行的记录。例如，ARP 日志可以记录如下事件：

- 设备未使能 ARP 代理功能时收到目的 IP 不是设备接口 IP 地址、VRRP 备份组中的虚拟 IP 地址或 NAT 转换的外部网络地址；
- 收到的 ARP 报文中源地址和接收接口 IP 地址、VRRP 备份组中的虚拟 IP 地址或 NAT 转换的外部网络地址冲突，且此报文不是 ARP 请求报文等。

设备生成的 ARP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 ARP 日志信息功能。

arp check log enable

缺省情况下，ARP 日志信息功能处于关闭状态。

1.7 ARP显示和维护

提示

清除 ARP 表项，将取消 IP 地址和 MAC 地址的映射关系，可能导致无法正常通信。清除前请务必仔细确认。

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 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 表项。

表1-1 ARP 显示和维护

操作	命令
显示ARP表项	（独立运行模式） **display arp** [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**] （IRF模式） **display arp** [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
显示指定IP地址的ARP表项	（独立运行模式） **display arp** *ip-address* [**verbose**] （IRF模式）

操作	命令
	display arp *ip-address* [**slot** *slot-number*] [**verbose**]
显示动态ARP表项的老化时间	**display arp timer aging**
显示指定VPN实例的ARP表项	**display arp vpn-instance** *vpn-instance-name* [**count** | **verbose**]
清除ARP表项	（独立运行模式） **reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** } （IRF模式） **reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

1.8 ARP典型配置举例

1.8.1 长静态ARP表项配置举例

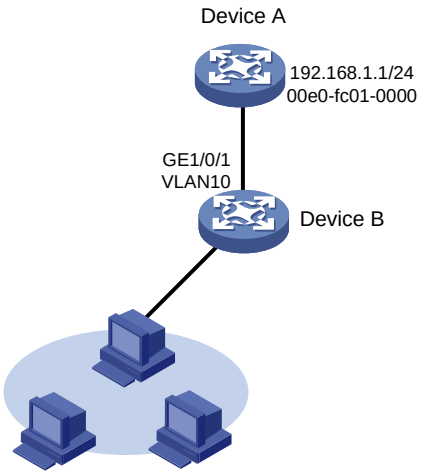
1. 组网需求

- Device B 连接主机，通过接口 GigabitEthernet1/0/1 连接 Device A。接口 GigabitEthernet1/0/1 属于 VLAN 10。
- Device A 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-0000。

为了增加 Device B 和 Device A 通信的安全性，可以在 Device B 上为 Device A 配置一条静态 ARP 表项，从而防止攻击报文修改此表项的 IP 地址和 MAC 地址的映射关系。

2. 组网图

图1-3 长静态 ARP 表项配置组网图



3. 配置步骤

在 Device B 上进行下列配置。

创建 VLAN 10。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

将接口 GigabitEthernet1/0/1 加入到 VLAN 10 中。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
```

创建接口 Vlan-interface10，并配置 IP 地址。

```
[DeviceB] interface vlan-interface 10
[DeviceB-vlan-interface10] ip address 192.168.1.2 8
[DeviceB-vlan-interface10] quit
```

配置一条长静态 ARP 表项，IP 地址为 192.168.1.1，对应的 MAC 地址为 00e0-fc01-0000，此条 ARP 表项对应的出接口为属于 VLAN 10 的接口 GigabitEthernet1/0/1。

```
[DeviceB] arp static 192.168.1.1 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

4. 验证配置

查看长静态 ARP 表项信息。

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP address       MAC address    SVLAN/VSI Interface/Link ID        Aging Type
192.168.1.1      00e0-fc01-0000 10        GE1/0/1                  --    S
```

1.8.2 短静态ARP表项配置举例

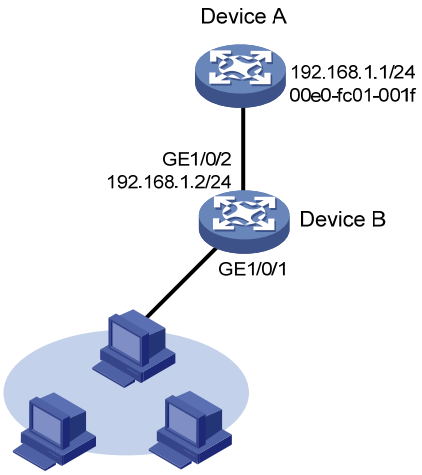
1. 组网需求

- Device B 通过接口 GigabitEthernet1/0/1 连接主机，通过接口 GigabitEthernet1/0/2 连接 Device A。
- Device A 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-001f。

网络管理员需要通过某种方法来防止恶意用户对 Device B 进行 ARP 攻击，增加 Device B 和 Device A 通信的安全性。如果 Device A 的 IP 地址和 MAC 地址是固定的，则可以通过在 Device B 上配置静态 ARP 表项的方法，防止恶意用户进行 ARP 攻击。

2. 组网图

图1-4 短静态 ARP 表项配置组网图



3. 配置步骤

在 Device B 上进行下列配置。

在接口 GigabitEthernet1/0/2 配置 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 192.168.1.2 24
[DeviceB-GigabitEthernet1/0/2] quit
```

配置一条短静态 ARP 表项，IP 地址是 192.168.1.1，对应的 MAC 地址是 00e0-fc01-001f。

```
[DeviceB] arp static 192.168.1.1 00e0-fc01-001f
```

4. 验证配置

查看短静态 ARP 表项信息。

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP address       MAC address    SVLAN/VSI Interface/Link ID        Aging Type
192.168.1.1      00e0-fc01-001f --        --                       --    S
```

2 免费ARP

2.1 免费ARP简介

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 地址都是本机的 IP 地址。设备通过对外发送免费 ARP 报文来确定其他设备的 IP 地址是否与本机的 IP 地址冲突，并实现在设备硬件地址改变时通知其它设备更新 ARP 表项。

2.1.1 IP地址冲突检测

设备接口获取到 IP 地址时可以在接口所在局域网内广播发送免费 ARP 报文。如果设备收到 ARP 应答报文，表示局域网中存在与该设备 IP 地址相同的设备，则设备不会使用此 IP 地址，并打印日志提示管理员修改该 IP 地址。如果设备未收到 ARP 应答报文，表示局域网中不存在与该设备 IP 地址相同的设备，则设备可以正常使用 IP 地址。

2.1.2 免费ARP报文学习

开启了免费 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（发送端 IP 地址、发送端 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 报文中的发送端 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。

2.1.3 定时发送免费ARP

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：

- 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。

  为了降低这种仿冒网关的 ARP 攻击所带来的影响，可以在网关的接口上开启定时发送免费 ARP 功能。开启该功能后，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。

- 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开启定时发送免费 ARP 功能。启用该功能后，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。

- 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，从而确保网络中不会存在 IP 地址与 Master 路由器 VRRP 虚拟 IP 地址相同的设备。免费 ARP 报文中的发送端 MAC 为 VRRP 虚拟路由器对应的虚拟 MAC 地址。关于 VRRP 的详细介绍，请参见“可靠性配置指导”中的“VRRP”。

- 及时更新模糊的 Dot1q/QinQ 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的 Dot1q/QinQ 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的 Dot1q/QinQ 终结 VLAN 内设备的 MAC 地址表项，可以在三层以太网子接口上开启定时发送免费 ARP 功能。开启该功能后，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，各个模糊的 Dot1q/QinQ 终结 VLAN 内设备上可以及时更新为正确的 MAC 地址表项。关于 VLAN 模糊的 Dot1q/QinQ 终结的详细介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 终结”。

2.2 免费ARP配置任务简介

本节中的所有配置均为可选，请根据实际情况选择配置。当以下功能均未开启时，免费 ARP 的冲突地址检测功能仍然生效。

- 开启源IP地址冲突提示功能
- 开启免费ARP报文学习功能
- 开启定时发送免费ARP功能
- 开启设备收到非同一网段ARP请求时发送免费ARP报文功能
- 配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔

2.3 开启源IP地址冲突提示功能

1. 功能简介

设备接收到其它设备发送的 ARP 报文后，如果发现报文中的源 IP 地址和自己的 IP 地址相同，该设备会根据当前源 IP 地址冲突提示功能的状态，进行如下处理：

- 如果源 IP 地址冲突提示功能处于关闭状态时，设备发送一个免费 ARP 报文确认是否冲突，只有收到对应的 ARP 应答后才提示存在 IP 地址冲突。
- 如果源 IP 地址冲突提示功能处于开启状态时，设备立刻提示存在 IP 地址冲突。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启源 IP 地址冲突提示功能。

arp ip-conflict log prompt

缺省情况下，源 IP 地址冲突提示功能处于关闭状态。

2.4 开启免费ARP报文学习功能

(1) 进入系统视图。

system-view

(2) 开启免费 ARP 报文学习功能。

gratuitous-arp-learning enable

缺省情况下，免费 ARP 报文的学习功能处于开启状态。

2.5 开启定时发送免费ARP功能

1. 配置限制和指导

- 设备最多允许同时在 1024 个接口上开启定时发送免费 ARP 功能。
- 开启定时发送免费 ARP 功能后，只有当接口链路状态 up 并且配置 IP 地址后，此功能才真正生效。
- 如果修改了免费 ARP 报文的发送时间间隔，则在下一个发送时间间隔才能生效。
- 如果同时在很多接口下开启定时发送免费 ARP 功能，或者每个接口有大量的从 IP 地址，又或者是两种情况共存的同时又配置很小的发送时间间隔，那么免费 ARP 报文的实际发送时间间隔可能会远远高于用户设定的时间间隔。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启定时发送免费 ARP 功能。

arp send-gratuitous-arp [**interval** *interval*]

缺省情况下，定时发送免费 ARP 功能处于关闭状态。

2.6 开启设备收到非同一网段ARP请求时发送免费ARP报文功能

(1) 进入系统视图。

system-view

(2) 开启设备收到非同一网段 ARP 请求时发送免费 ARP 报文功能。

gratuitous-arp-sending enable

缺省情况下，设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能处于关闭状态。

2.7 配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔

1. 功能简介

当设备的MAC地址发生变化后，设备会通过免费ARP报文将修改后的MAC地址通告给其他设备。由于目前免费ARP报文没有重传机制，其他设备可能无法收到免费ARP报文。为了解决这个问题，用户可以配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔，保证其他设备可以收到该免费ARP报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置当接口MAC地址变化时，重新发送免费ARP报文的次数和时间间隔

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

缺省情况下，当设备的接口MAC地址变化时，该接口只会发送一次免费ARP报文。

3 代理ARP

3.1 代理ARP简介

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 的应用场景为：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 的应用场景为：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。

3.2 开启普通代理ARP功能

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

普通代理 ARP 功能可在 VLAN 接口视图/三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图下进行配置。

(3) 开启普通代理 ARP 功能。

proxy-arp enable

缺省情况下，普通代理 ARP 功能处于关闭状态。

3.3 开启本地代理ARP功能

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

本地代理 ARP 功能可在 VLAN 接口视图/三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图下进行配置。

(3) 开启本地代理 ARP 功能。

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

缺省情况下，本地代理 ARP 功能处于关闭状态。

3.4 代理ARP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代理 ARP 的运行情况，查看显示信息验证配置的效果。

表3-1 代理 ARP 显示和维护

操作	命令
显示本地代理ARP的状态	**display local-proxy-arp** [**interface** *interface-type interface-number*]
显示普通代理ARP的状态	**display proxy-arp** [**interface** *interface-type interface-number*]

3.5 普通代理ARP典型配置举例

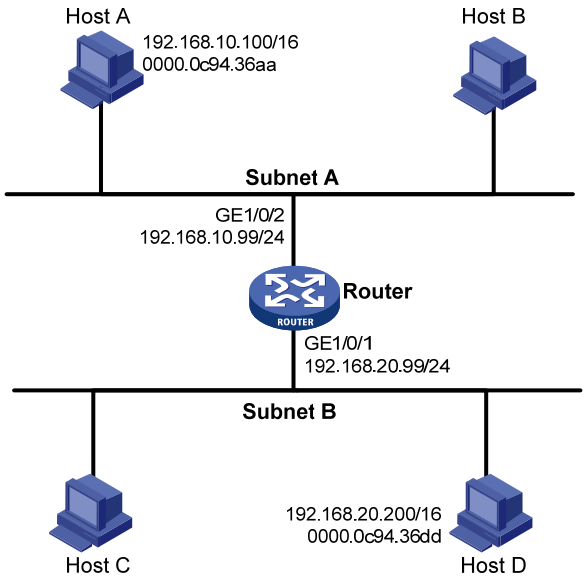
3.5.1 普通代理ARP基本组网配置举例

1. 组网需求

- Host A 的 IP 地址是 192.168.10.100/16，所在局域网的网络号为 192.168.0.0/16。
- Host D 的 IP 地址是 192.168.20.200/16，所在局域网的网络号为 192.168.0.0/16。
- Host A 和 Host D 互相认为处于同一子网，但实际却被设备 Router 分在两个不同的子网。
- Host A 和 Host D 没有配置缺省网关，要求在设备 Router 上开启普通代理 ARP 功能，使处在两个子网的 Host A 和 Host D 能互通。

2. 组网图

图3-1 配置普通代理 ARP 组网图



3. 配置步骤

配置接口 GigabitEthernet1/0/2 的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 192.168.10.99 255.255.255.0
```

开启接口 GigabitEthernet1/0/2 的代理 ARP 功能。

```
[Router-GigabitEthernet1/0/2] proxy-arp enable
[Router-GigabitEthernet1/0/2] quit
```

配置接口 GigabitEthernet1/0/1 的 IP 地址。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.20.99 255.255.255.0
```

开启接口 GigabitEthernet1/0/1 的普通代理 ARP 功能。

```
[Router-GigabitEthernet1/0/1] proxy-arp enable
[Router-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，Host A 和 Host D 可以互相 ping 通。

4 ARP Snooping

4.1 ARP Snooping简介

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（MAC-Forced Forwarding，MAC 强制转发等使用。关于 MFF 的详细介绍，请参见“安全配置指导”中的“MFF”。

4.1.1 ARP Snooping表项建立机制

设备上在一个 VLAN 中启用 ARP Snooping 后，该 VLAN 内接收的 ARP 报文都会被上送到 CPU。CPU 对上送的 ARP 报文进行分析，获取 ARP 报文的发送端 IP 地址、发送端 MAC 地址、VLAN 和入端口信息，建立记录用户信息的 ARP Snooping 表项。

4.1.2 ARP Snooping表项老化机制

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 12 分钟内没有收到 ARP 更新报文，设备会向外主动发送一个 ARP 请求进行探测；若 ARP Snooping 表项自最后一次更新后 15 分钟时，还没有收到 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。当收到发送端 IP 地址和发送端 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。

4.1.3 ARP Snooping表项冲突处理机制

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 1 分钟后删除此表项。

4.2 ARP Snooping与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	不支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持

型号	说明
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	不支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	不支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	说明
MSR810-W-WiNet/810-LM-WiNet	支持
MSR830-4LM-WiNet	不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet	不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet	不支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	MSR2600-6-WiNet：不支持 MSR2600-10-X1-WiNet：支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	不支持
MSR3610-IE-XS	不支持

4.3 开启ARP Snooping功能

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 开启 ARP Snooping 功能。

arp snooping enable

缺省情况下，ARP Snooping 功能处于关闭状态。

4.4 ARP Snooping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 Snooping 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 Snooping 表中的表项。

表4-1 ARP Snooping 显示和维护

操作	命令
显示ARP Snooping表项	（独立运行模式） **display arp snooping** [**vlan** *vlan-id*] [**count**] **display arp snooping ip** *ip-address* （IRF模式） **display arp snooping** [**vlan** *vlan-id*] [**slot** *slot-number*] [**count**] **display arp snooping ip** *ip-address* [**slot** *slot-number*]
清除ARP Snooping表项	**reset arp snooping** [**ip** *ip-address* | **vlan** *vlan-id*]

5 ARP快速应答

5.1 ARP快速应答简介

ARP 快速应答功能根据设备上生成的 IP Source Guard 表项或者 ARP Snooping 表项包含的信息，在指定的 VLAN 内，对 ARP 请求进行应答，从而减少 ARP 广播报文。关于 IP Source Guard 的详细介绍，请参见“安全配置指导”中的“IP Source Guard”。

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 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 接口的 IP 地址，则根据报文中的目的 IP 地址查找 IP Source Guard 表项：

- 如果查找成功，当接口是以太网接口时，当查找到的表项的接口和收到请求报文的接口一致，不进行应答，否则立即进行应答。
- 如果查找失败且设备开启了 ARP Snooping，则继续查找 ARP Snooping 表项，如果查找成功，当接口是以太网接口时，当查找到的表项的接口和收到请求报文的接口一致，不进行应答，否则立即进行应答。
- 如果两个表均查找失败，则向指定 VLAN 内除收到请求报文的接口外的其他接口转发该请求报文或将报文交于其他特性处理。

5.2 ARP快速应答与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	不支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	不支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	不支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	不支持

型号	说明
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	说明
MSR810-W-WiNet、MSR810-LM-WiNet	不支持
MSR830-4LM-WiNet	不支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	不支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	不支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	MSR2600-6-WiNet：不支持 MSR2600-10-X1-WiNet：支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	不支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	不支持
MSR3620-XS	支持
MSR3610-I-XS	不支持
MSR3610-IE-XS	不支持

5.3 开启ARP快速应答功能

1. 配置限制和指导

为了提高 ARP 快速应答的应答几率，可以在应用 ARP 快速应答功能的场合同时开启 ARP Snooping 功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 VLAN 视图。

vlan *vlan-id*

(3) 开启 ARP 快速应答功能。

arp fast-reply enable

缺省情况下，ARP 快速应答功能处于关闭状态。

5.4 ARP快速应答典型配置举例

5.4.1 ARP快速应答基本组网配置举例

1. 组网需求

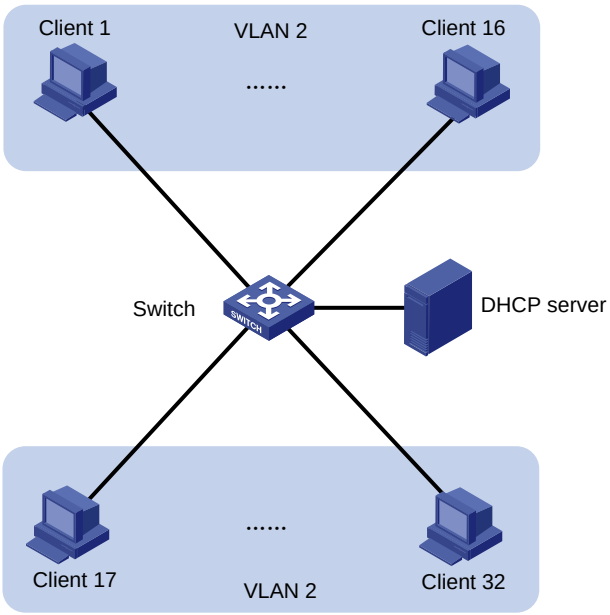
Client 1～Client 32 通过 Switch 接入网络，所有客户端接入 VLAN 为 VLAN 2。

当 Client 1 需要访问 Client 32 时，Client 1 发送 ARP 请求报文，ARP 请求报文在 Switch 上被复制其他所有接口上发送（除了与 Client 1 直连的接口），在设备上具有多个接口的情况下，这种复制的广播会占用接口资源。

为减少对接口资源的占用，可以在 VLAN 2 上开启 ARP 快速应答。启用 ARP 快速应答，当 Client 32 通过 DHCP 服务器获得 IP 地址后，Client 1 需要访问 Client 32 时，ARP 请求报文可以在 Switch 上得到应答，而 Switch 不会再对报文进行广播，从而减少了对接口资源的占用。

2. 组网图

图5-1 开启 ARP 快速应答组网图



3. 配置步骤

(1) 开启 Switch 上 VLAN2 开启 ARP Snooping 功能。

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] arp snooping enable
```

(2) 开启 Switch 上 VLAN 2 开启 ARP 快速应答功能。

```
[Switch-vlan2] arp fast-reply enable
```

```
[Switch-vlan2] quit
```

6 即插即用网关

6.1 即插即用网关简介

即插即用网关功能主要用于屏蔽设备 IP 地址和本地网段地址的差异，以实现设备在不改变现有 IP 配置的情况下，即可通过网关连接外网。

在网关上开启了即插即用网关功能后，虽然设备的 IP 地址和网关接口地址不在同一网段，网关收到设备发送的 ARP 请求后，仍然会以网关的 MAC 地址应答该 ARP 请求。从设备处收到报文时，网关会为设备分配一个与接口 IP 地址同网段的代理 IP 地址，并把报文中的源 IP 地址替换成代理 IP 地址。网关收到目的为设备的应答报文后，会把报文中的目的 IP 地址由分配的代理 IP 地址替换回用户 IP 地址。这样，就可以保证设备可以正常访问外网。

6.2 即插即用网关配置准备

在设备上开启即插即用网关功能前，需要先完成以下操作：

(1) 在设备的下行接口上配置一个主 IP 地址和掩码。即插即用网关功能会根据主 IP 地址和掩码生成与主 IP 地址同网段的代理 IP 地址。

(2) 配置 **reset arp** 命令清除接口上所有的 ARP 表项。

(3) 在设备上配置 NAT 功能，即在设备上创建 NAT 池并添加地址组成员，在设备的上行口配置出方向动态地址转换等。关于 NAT 的相关介绍请参考“三层技术-IP 业务配置指导”中的“NAT”。

6.3 开启即插即用网关功能

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

指定的接口应为网关设备的下行接口。接口类型可以是三层以太网接口、三层以太网子接口。

(3) 开启即插即用网关功能。

arp pnp

缺省情况下，接口的即插即用功能处于关闭状态。

6.4 即插即用网关显示和维护

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即插即用网关特性的运行情况，通过查看显示信息验证配置的效果。

表6-1 即插即用网关显示和维护

操作	命令
显示设备的即插即用网关用户信	**display arp pnp** [**interface** *interface-type*

操作	命令
息	*interface-number*]

6.5 即插即用网关典型配置举例

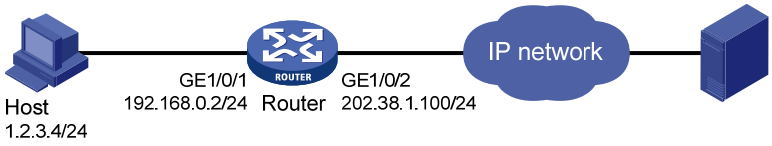
6.5.1 即插即用网关基本组网配置举例

1. 组网需求

用户入住宾馆，需要用自己携带的电脑访问服务器，用户电脑的 IP 地址为：1.2.3.4/24，宾馆网关 Router 的接口 GigabitEthernet1/0/1 的 IP 地址为 192.168.0.2/24，接口 GigabitEthernet1/0/2 的 IP 地址为 202.38.1.100/24。现在需要实现用户的电脑 IP 地址不做任何修改即可访问服务器。

2. 组网图

图6-1 开启即插即用网关组网图



3. 配置步骤

(1) 配置 NAT

配置各设备的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.0.2 24
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 202.38.1.100 24
[Router-GigabitEthernet1/0/2] quit
```

配置 ACL2000，仅允许对 192.168.0.0/24 网段用户的报文进行地址转换。

```
[Router] acl basic 2000
[Router-acl-ipv4-basic-2000] rule permit source 192.168.0.0 0.0.0.255
[Router-acl-ipv4 basic-2000] quit
```

配置地址组 1，并添加地址组成员地址 202.38.1.100。

```
[Router] nat address-group 1
[Router-nat-address-group-1] address 202.38.1.100 202.38.1.100
[Router-nat-address-group-1] quit
```

在接口 GigabitEthernet1/0/2 上配置出方向动态地址转换，允许对匹配 ACL 2000 的报文使用地址组 1 中的地址进行地址转换，且在转换的时候使用 TCP/UDP 的端口信息。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] nat outbound 2000 address-group 1
```

(2) 开启即插即用网关功能

在接口 GigabitEthernet1/0/1 上开启即插即用网关功能。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] arp pnp
[Router-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，在 Router 上执行 **display arp pnp** 命令可以查询到设备的即插即用网关的用户表项。

以接口 GigabitEthernet1/0/1 为例

```
[Router] display arp pnp interface gigabitethernet 1/0/1
Total number of entries : 1
Agent IP address   User IP address   MAC address      Interface   Aging
192.168.0.3        1.2.3.4          00e0-fc00-0001   GE1/0/1     10
```

可以看出 Router 为 IP 地址 1.2.3.4 的用户分配的代理 IP 地址为 192.168.0.3。

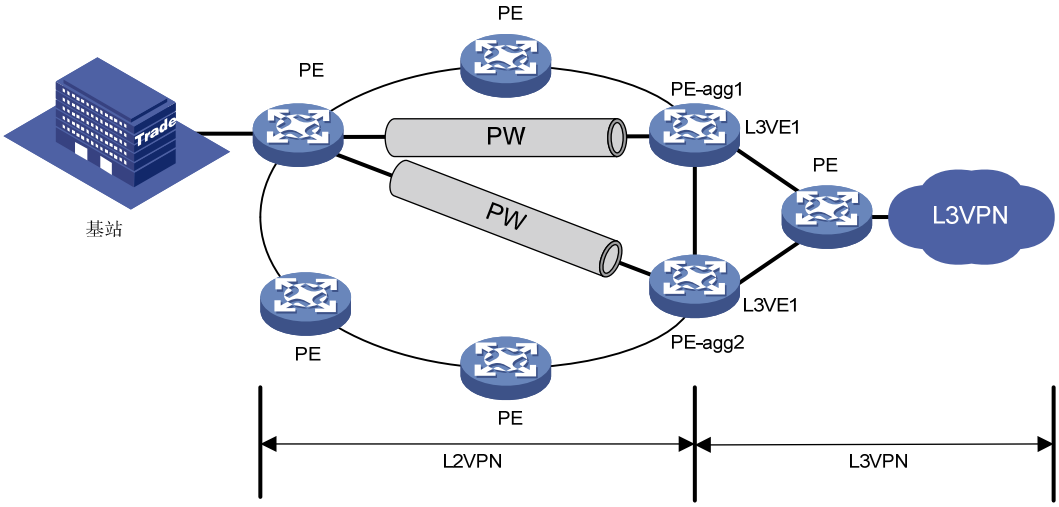
7 ARP泛洪抑制

7.1 ARP泛洪抑制简介

如 图 7-1 所示，基站、PE和PE-agg建立L2VPN连接。这时，在PE设备上开启ARP泛洪抑制功能，PE就能够侦听经过它的ARP报文。当基站或PE-Agg再次发起ARP解析时，PE可以对ARP请求进行代答，从而可以抑制设备发起ARP解析时引起的网络泛洪。

PE 还可以固定的时间间隔以免费 ARP 报文的形式，向基站和 PE-agg 设备推送 ARP 泛洪抑制表项信息。

图7-1 ARP 泛洪抑制组网图



7.2 ARP泛洪抑制与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	支持

型号	说明
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	不支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	说明
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	不支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	不支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	不支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

7.3 开启ARP泛洪抑制功能

(1) 进入系统视图。

system-view

(2) （可选）开启主动推送 ARP 泛洪抑制表项功能，并配置推送时间间隔。

arp suppression push interval *interval*

缺省情况下，主动推送 ARP 泛洪抑制表项功能处于关闭状态。

(3) 创建一个交叉连接组，并进入交叉连接组视图。

xconnect-group *group-name*

关于 **xconnect-group** 命令的详细介绍，请参见“MPLS 命令参考”中的“MPLS L2VPN”。

(4) 创建交叉连接，进入交叉连接视图。

connection *connection-name*

关于 **connection** 命令的详细介绍，请参见“MPLS 命令参考”中的“MPLS L2VPN”。

(5) 开启 ARP 泛洪抑制功能。

arp suppression enable

缺省情况下，ARP 泛洪抑制功能处于关闭状态。

7.4 ARP泛洪抑制显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以查看 ARP 泛洪抑制配置后的运行情况，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 泛洪抑制表中的表项。

表7-1 ARP 泛洪抑制显示和维护

操作	命令
显示ARP泛洪抑制表项	（独立运行模式） **display arp suppression xconnect-group** [**name** *group-name*] [**count**] （IRF模式） **display arp suppression xconnect-group** [**name** *group-name*] [**slot** *slot-number*] [**count**]
清除ARP泛洪抑制表项	**reset arp suppression xconnect-group** [**name** *group-name*]

7.5 ARP泛洪抑制典型配置举例

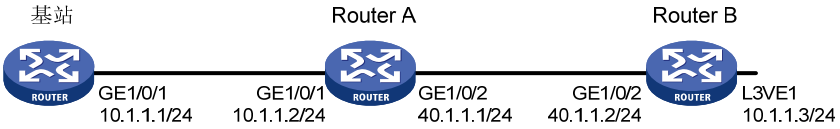
7.5.1 ARP泛洪抑制基本组网配置举例

1. 组网需求

基站、Router A 和 Router B 之间由 L2VPN 连接，基站设备与 Router B 设备的 L3VE 口之间路由可达。为了减少网络中的 ARP 报文数，开启 ARP 泛洪抑制功能，Router A 不再转发 ARP 请求报文，而是代答基站请求 Router B 信息的 ARP 报文。

2. 组网图

图7-2 开启 ARP 泛洪抑制组网图



3. 配置步骤

(1) 配置 IP 地址和路由

请按照组网图配置各接口的 IP 地址，并且配置路由保证基站设备和 Router B 设备的 L3VE 口之间路由可达。具体配置过程略。

(2) 开启泛洪抑制功能

在 Router A 上创建交叉连接组 vpna，在该交叉连接组内创建名称为 svc 的交叉连接。在该交叉连接视图下配置泛洪抑制功能。

```
<RouterA> system-view
[RouterA] xconnect-group vpna
[RouterA-xcg-vpna] connection svc
[RouterA-xcg-vpna-svc] arp suppression enable
```

4. 验证配置

清除基站的 ARP 表项，从基站 ping Router B 的 L3VE 口，ping 通后在 Router A 上查看泛洪抑制表项

```
[RouterA-xcg-vpna-svc] display arp suppression xconnect-group
IP address      MAC address     Xconnect-group       Connection           Aging
10.1.1.1        00e0-fc04-582c  vpna                 svc                  25
10.1.1.3        0023-89b7-0861  vpna                 svc                  25
```

打开 Router B 的 ARP 调试开关，清除基站的 ARP 表项，从基站 ping Router B 的 L3VE 口，在 Router B 上看不到 ARP 解析的过程。

8 ARP直连路由通告

8.1 ARP直连路由通告简介

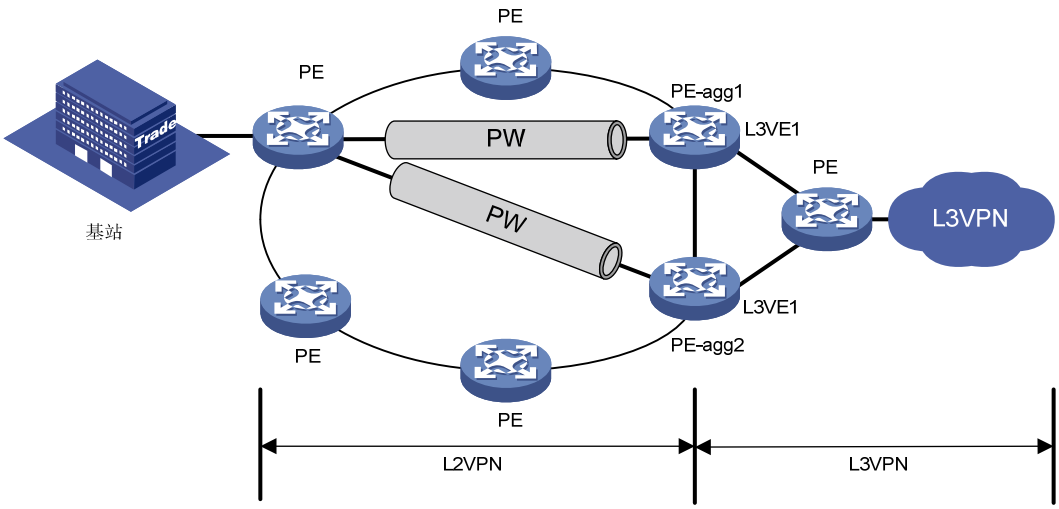
8.1.1 工作机制

ARP 直连路由通告功能用于使设备从 ARP 表中学到对应的直连路由信息，以便其他路由协议发布该直连路由或指导报文转发。

8.1.2 L2VPN接入L3VPN组网应用

如 图 8-1 所示，基站设备、PE分别与PE-agg1、PE-agg2 建立L2VPN连接。在PE-agg1 和PE-agg2 上开启ARP直连路由通告功能，这两台设备才能将基站的主机路由对L3VPN内的PE设备发布。这时，该PE设备到基站设备上会生成经过PE-agg1 和PE-agg2 的两条等价路由，PE发往基站设备的流量同时经过PE-agg1 和PE-agg2。如果PE-agg1 设备发生故障，从PE发往基站设备的流量能快速地完全切换到由PE-agg2 转发。

图8-1 ARP 直连路由通告功能组网图



关于“L2VPN 接入 L3VPN”功能的详细介绍，请参见“MPLS 配置指导”中的“L2VPN 接入 L3VPN 或 IP 骨干网”。

8.2 开启ARP直连路由通告功能

(1) 进入系统视图。

system-view

(2) 进入 L3VE 接口视图。

interface ve-l3vpn *interface-number*

(3) 开启 ARP 直连路由通告功能。

arp route-direct advertise

缺省情况下，ARP 直连路由通告功能处于关闭状态。