

## 【交换机在江湖】第二十六章 IP与MAC一线牵之ARP

有木有因为不知如何查看ARP表而烦恼？

有木有因为不明白ARP表项从何而来而彷徨？

有木有因为不会配置静态ARP表项而惆怅？

有木有因为同一网段ARP学习不到而心烦意乱？

这个秋天就让小编来为您揭开ARP的朦胧面纱，ARP相关配置再也不愁啦~~~

我们首先回顾一下什么是ARP？江湖中人对ARP的描述是：闲窥江湖风云雨，IP、MAC一线牵。也就是说地址解析协议ARP（Address Resolution Protocol）实则是IP地址与MAC地址之间的桥梁，主要用于将IP地址解析为MAC地址。

无论是PC还是交换机上，都有一张ARP表，ARP表中保存着IP地址和MAC地址的映射关系。当PC或者交换机需要与网络中其他设备进行通信时，知道了对方的IP地址，还需要知道MAC地址以便将IP报文封装成帧才能通过物理网络发送，这时PC或者交换机可以通过查找ARP表知道对方IP地址对应的MAC地址。

下面就让小编带大家一起从以下几个方面来一步一步的了解ARP吧~

## 1 查看 ARP 表

交换机作为网关时，通过在网关上查看ARP表项，网络管理员可以查看下挂用户的IP地址、MAC地址和接口等信息。例如，当网络管理员知道某个用户的IP地址，想查询该用户的MAC地址时，可以通过查看ARP表项信息获取。

那我们如何查看设备上的ARP表呢？**display arp**就可以啦~

功能	命令行
想查看所有的ARP表项？	display arp all
想查看动态的ARP表项？	display arp dynamic
想查看静态的ARP表项？	display arp static
想查看某一网段的ARP表项？	display arp network x.x.x.x
想查看某一接口相关的ARP表项？	display arp interface xx
想查看某一VPN实例的ARP表项？	display arp vpn-instance xx
想查看某个具体IP地址的ARP表项？	display arp all   include x.x.x.x

举个例子，如下图所示，我们可以在交换机上执行命令**display arp network**查看172.16.0.0/16网段的ARP表项。ARP表项有S、I、D三种类型，这三种类型的ARP表项是怎么来的？怎么配置？小编待会儿给大家详细介绍。

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE	VPN-INSTANCE
172.16.10.3	0025-9efb-be55		S--	GE1/0/6	
172.16.20.3	0200-0000-00e8		S--	GE1/0/19	
172.16.10.1	0025-9ef4-abcd		I -	Vlanif100	
172.16.10.2	0025-9efb-be55	20	D-0	GE1/0/6	
			100/-		
172.16.20.1	0025-9ef4-abcd		I -	GE1/0/19	
172.16.20.2	0200-0000-00e8	18	D-0	GE1/0/19	
			100/-		
Total:6			Dynamic:2	Static:2	Interface:2

**S:静态ARP表项**  
IP地址和MAC地址之间固定的映射关系,不会被老化,也不会被动态ARP表项覆盖。

**I:接口本身的ARP表项**  
IP地址和MAC地址为接口本身的IP地址和MAC地址。

**D:动态ARP表项**  
根据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。

偶尔是不是还遇到过MAC ADDRESS字段显示为“**Incomplete**”的情况,不用迷惘,**Incomplete**表示这条ARP表项是一个临时ARP表项,即设备已经发送了ARP请求报文,但是还没有收到ARP应答。

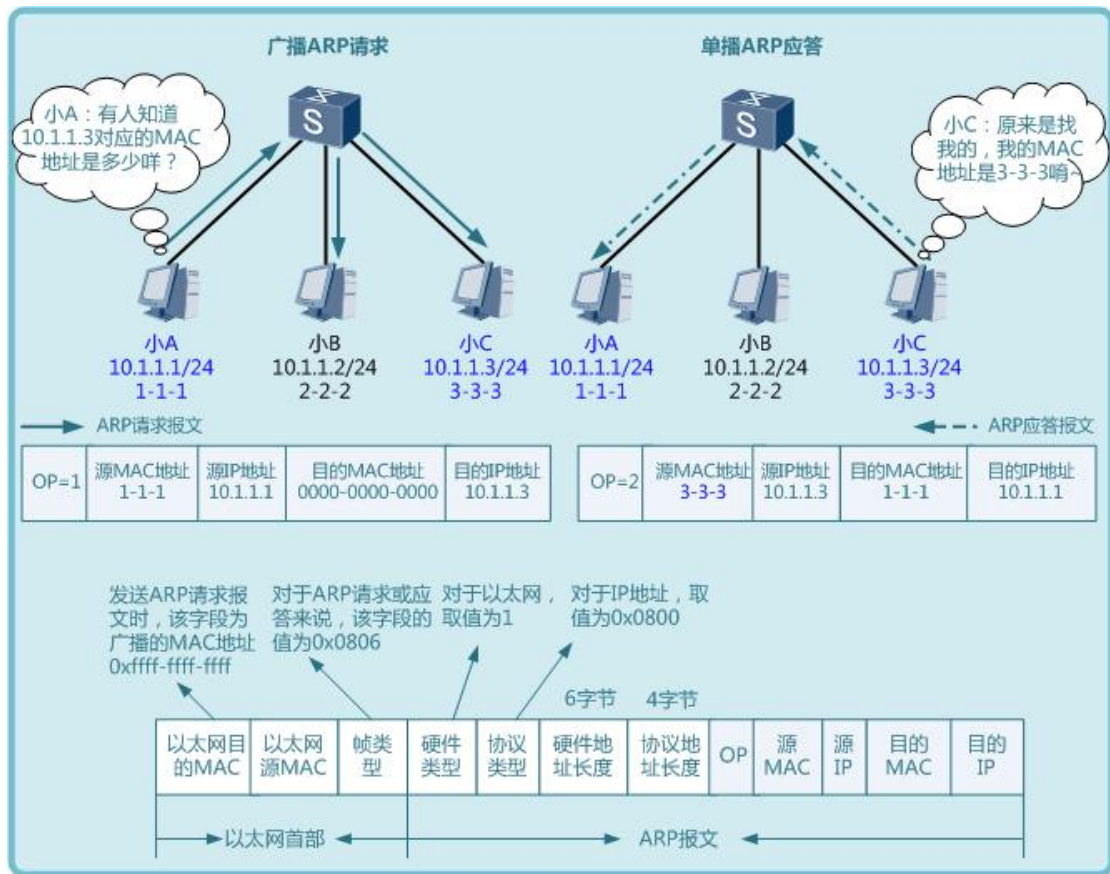
看了上面的ARP表,或许已经有细心的小伙伴发现:S和D类型的ARP表项中,为什么有的ARP表项没有VLAN信息,有的ARP表项有VLAN信息呢?哈哈,小编我就不卖关子了,是这样的:如果ARP表项没有VLAN信息,那么代表这条表项中的接口处于三层模式,是一个三层口;如果ARP表项有VLAN信息(并且表项中接口不是子接口时),那么代表这条表项中的接口处于二层模式,是一个二层口。

当然,如果你想删除设备上的ARP表项,可以通过执行**reset arp { all | dynamic xx | static xx | interface xx }**命令来实现。

刚刚小编给大家承诺过要介绍三种类型的ARP表项是如何来的。类型为I的ARP表项比较简单,只要在接口上配置了IP地址,设备上就会生成一条类型为I的ARP表项哦~类型为I的ARP表项不会老化,IP地址和MAC地址即为接口本身的IP地址和MAC地址。那另外两种类型的ARP表项呢?各位看官可要睁大你的眼睛哦~下面就介绍类型为D的ARP表项。

## 2 动态 ARP 表项学习

大多数情况下,设备可以通过ARP协议动态学习和更新ARP表项。设备是如何进行动态学习的呢?其实动态ARP主要是通过**广播ARP请求报文**和**单播ARP应答报文**这两个过程完成地址解析的。



例如小A和小C在一次聚会上互留了IP地址。如上图所示, 小A需要与小C进行通信时, 知道了小C的IP地址为10.1.1.3/24, 判断后发现与自己在同一网段10.1.1.0/24, 于是小A会广播发送一个ARP请求报文, 请求小C的MAC地址。

小C收到ARP请求报文后, 会单播发送一个ARP应答报文, 告诉对方自己的MAC地址是3-3-3。(在同一网段的小B也会收到ARP请求报文, 但是由于ARP请求报文中的目的IP地址不是小B的IP地址, 因此小B不会进行应答。)

小A收到ARP应答报文后, 就会在自己的ARP表中增加一条动态表项: IP地址10.1.1.3对应MAC地址3-3-3, 这样小A就可以与小C进行通信啦。怎样, 是不是觉得动态ARP学习很简单?

一方面由于ARP表的容量限制, 另一方面也为了保证动态ARP表项的准确性, PC或交换机会对学习到的动态ARP表项进行老化。交换机上动态ARP表项有一定的老化时间, 缺省值是20分钟, 一般建议使用缺省值。

设备上动态ARP表项到达老化时间后, 设备会发送老化探测报文(即ARP请求报文), 如果能收到ARP应答报文, 则更新该动态ARP表项, 本次老化探测结束; 如果超过设置的老化探测次数后仍没有收到ARP应答报文, 则删除该动态ARP表项, 本次老化探测结束。

好啦, 动态ARP表项的内容小编也介绍的差不多了, 是不是已经有小伙伴迫不及待的想知道S类型的ARP表项是怎么配置的呢?

### 3 静态 ARP 表项配置

对于网络中的重要设备，如服务器等，我们可以在交换机上配置静态ARP表项。这样可以避免交换机上重要设备IP地址对应的ARP表项被ARP攻击报文错误更新，从而保证用户与重要设备之间正常通信。

静态ARP表项不会老化，不会被动态ARP表项覆盖。用户可以通过手工方式配置静态ARP表项，下面小编就给大家举几个例子。

例如，网络中有一台重要的服务器，服务器的IP地址为172.16.10.2，MAC地址为0023-0045-0067。如果交换机与这台服务器相连的接口GE1/0/1处于二层模式，并加入VLAN100。这时可以在交换机上为服务器配置一条对应的ARP表项，具体配置如下。

```
<Quidway> system-view
[Quidway] vlan batch 100
[Quidway] interface vlanif 100
[Quidway-Vlanif100] ip address 172.16.10.1 24 //VLANIF 接口的 IP 地址需要与静态 ARP 表项中的 IP 地址（172.16.10.2）同网段。
[Quidway-Vlanif100] quit
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port link-type access
[Quidway-GigabitEthernet1/0/1] port default vlan 100 //接口 GigabitEthernet1/0/1 处于二层模式，需要加入 VLAN100。
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] arp static 172.16.10.2 0023-0045-0067 vid 100 interface gigabitethernet 1/0/1
```

还是上面的那台服务器，如果交换机与服务器相连的接口处于三层模式，这时在交换机上配置静态ARP表项，可以参考如下配置。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] undo portswitch
[Quidway-GigabitEthernet1/0/1] ip address 172.16.10.1 24 //GigabitEthernet1/0/1 的 IP 地址需要与静态 ARP 表项中的 IP 地址（172.16.10.2）同网段。
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] arp static 172.16.10.2 0023-0045-0067 interface gigabitethernet 1/0/2
```

当交换机采用多端口ARP方式与NLB服务器群集连接时，NLB服务器的群集IP地址为172.16.40.2，群集MAC地址为02bf-0045-0070。这时在交换机上配置对应的静态ARP表项时，可以参考如下配置。

```
<Quidway> system-view
[Quidway] arp static 172.16.40.2 02bf-0045-0070
```

对于出接口是以太网接口，并且以太网接口处于二层模式的情况，建议小伙伴们在配置静态ARP表项时尽量同时指定VLAN和出接口，否则可能导致业务流量不通。

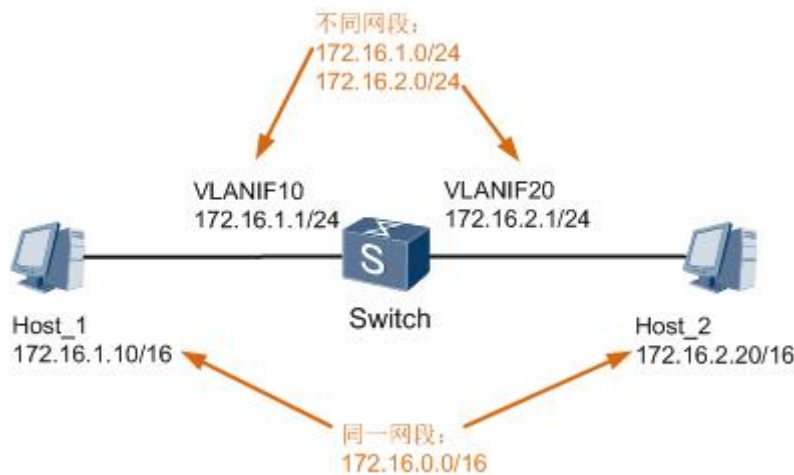
## 4 ARP 代理（即 Proxy ARP）

前面我们提到，主机进行动态ARP学习时，如果发现目的IP地址与自己在同一网段，会发送广播ARP请求报文进行ARP学习。但是呢，有些情况下两台主机虽然在同一网段，但不在同一广播域，目的主机是无法收到ARP请求报文的，因而也就无法成功学习到ARP表项。

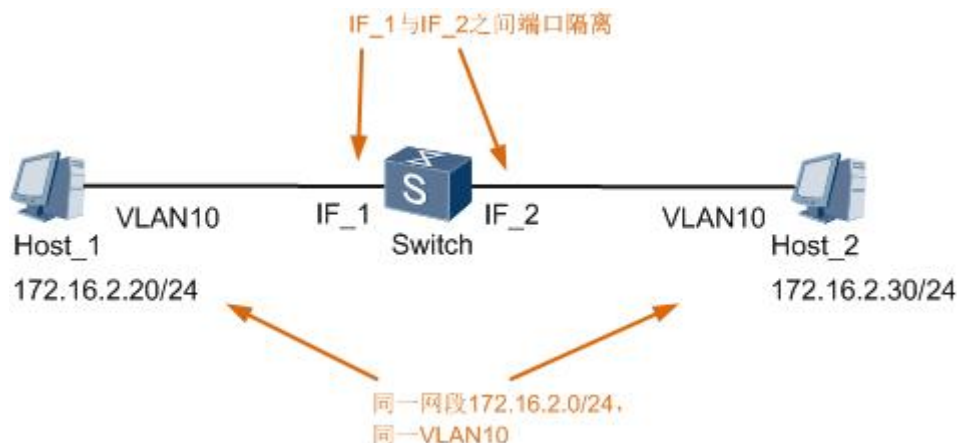
在连接两台主机的交换机上使能ARP代理后，交换机相当于一个中介，Host\_1发送ARP请求报文请求Host\_2的MAC地址的时候，交换机会将自己的MAC地址告诉Host\_1。这样Host\_1发给Host\_2的数据报文会先发给交换机，再由交换机转发给Host\_2。

例如下面的三种情况，我们就可以用到ARP代理。

**情况一：**需要互通的主机Host\_1与Host\_2（主机上没有配置缺省网关）处于相同的网段但不在同一物理网络（即不在同一广播域）。由于在不同的广播域，Host\_1发送的ARP请求报文Host\_2是收不到的，这时可以在交换机的VLANIF10和VLANIF20接口上使能**路由式Proxy ARP功能（arp-proxy enable）**，实现Host\_1与Host\_2之间的互通。

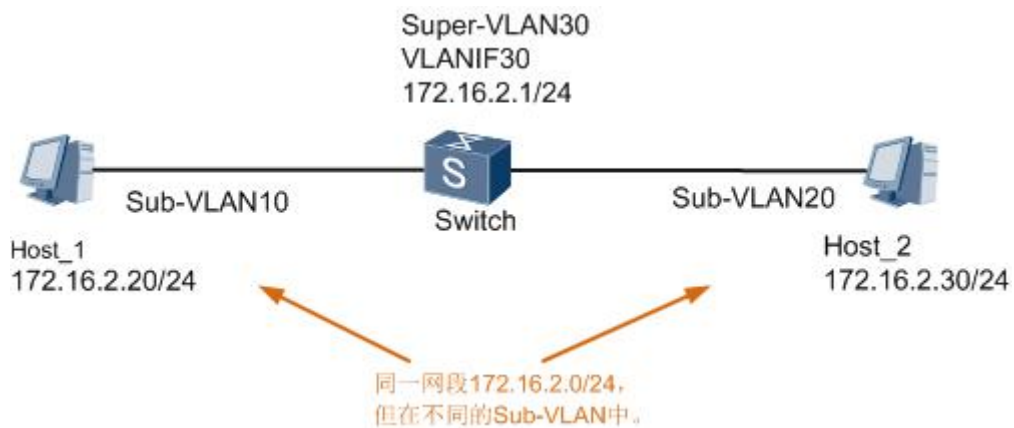


**情况二：**需要互通的主机Host\_1与Host\_2处于相同网段，并且属于相同VLAN，但是VLAN内接口IF\_1与IF\_2配置了端口隔离。由于IF\_1与IF\_2之间端口隔离，Host\_1发送的ARP请求报文Host\_2是收不到的，这时可以在Switch上关联了VLAN10的VLANIF接口上使能**VLAN内Proxy ARP功能（arp-proxy inner-sub-vlan-proxy enable）**，实现Host\_1与Host\_2之间的三层互通。





情况三：需要互通的主机Host\_1与Host\_2处于相同网段，但属于不同VLAN。由于不在同一VLAN，Host\_1发送的ARP请求报文Host\_2当然也是收不到的，这时可以在Switch上关联了VLAN10和VLAN20的VLANIF30接口上使能VLAN间Proxy ARP功能（**arp-proxy inter-sub-vlan-proxy enable**），实现Host\_1与Host\_2之间的三层互通。



ok，看到这里，是不是已经对ARP的基本功能有所了解了呢~