14 常见 ARP 操作

关于本章

介绍ARP的常见操作。

14.1 查看 ARP 表项

在日常维护工作中，用户可以在任意视图下执行**display arp**相关命令，查看设备上的ARP表项信息。

通过在网关设备上查看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。

当网关设备上没有学习到下挂用户的IP地址时，可以在网关设备上ping该网段的广播地址。例如网关的IP地址为10.10.10.1/24，在网关设备上ping 10.10.10.255，同一网段的用户会发送ARP应答报文，网关设备收到ARP应答报文后即能学习到用户的IP地址。

查看设备上172.16.0.0/16网段的ARP表项。

```
<HUAWEI> display arp network 172.16.0.0 16
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
```



```
--------------------------------------------------------------------------------

172.16.10.3     0025-9efb-be55            S--         GE1/0/6

100/-
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
--------------------------------------------------------------------------------

Total:6         Dynamic:2       Static:2     Interface:2
```

上述回显中，每行ARP表项的具体含义如下：

- IP地址为172.16.10.3，MAC地址为0025-9efb-be55，TYPE字段为S（代表该ARP表项为静态ARP表项）。这条静态ARP表项出接口为GE1/0/6，VLAN编号为100。
- IP地址为172.16.20.3，MAC地址为0200-0000-00e8，TYPE字段为S（代表该ARP表项为静态ARP表项）。这条静态ARP表项出接口为GE1/0/19。
- IP地址为172.16.10.1，MAC地址为0025-9ef4-abcd，TYPE字段为I（代表该ARP表项为接口本身的ARP表项）。这条ARP表项代表IP地址172.16.10.1是接口Vlanif100的IP地址。
- IP地址为172.16.10.2，MAC地址为0025-9efb-be55，TYPE字段为D（代表该ARP表项为动态ARP表项）。这条动态ARP表项是从接口GE1/0/6动态学习到的，VLAN编号为100，剩余存活时间为20分钟。
- IP地址为172.16.20.1，MAC地址为0025-9ef4-abcd，TYPE字段为I（代表该ARP表项为接口本身的ARP表项）。这条ARP表项代表IP地址172.16.20.1是接口GE1/0/19的IP地址。
- IP地址为172.16.20.2，MAC地址为0200-0000-00e8，TYPE字段为D（代表该ARP表项为动态ARP表项）。这条动态ARP表项是从接口GE1/0/19动态学习到的，剩余存活时间为18分钟。

说明

如果MAC ADDRESS字段显示为“Incomplete”，表示当前ARP表项为临时ARP表项。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。
- 在临时ARP表项老化超时后，设备会清除临时ARP表项。

相关信息

技术论坛

IP与MAC一线牵之ARP

视频

如何查询MAC和ARP表项

14.2 刷新 ARP 表项

当需要刷新设备上的ARP表项时，可以先清除设备上的ARP表项，这样设备会重新学习ARP表项。

注意

清除ARP表项后，将取消IP地址和MAC地址的映射关系，可能导致无法访问某些节点。清除前请务必仔细确认。

清除设备上所有的ARP表项。

说明

V200R009C00及后续版本设备不支持该功能。

```
<HUAWEI> reset arp all
```

清除设备上IP地址为172.16.10.1的动态ARP表项。

```
<HUAWEI> reset arp dynamic ip 172.16.10.1 //如果不指定IP地址，则删除设备上所有的动态ARP表项。
```

清除设备上所有的静态ARP表项。

```
<HUAWEI> reset arp static
Warning: This operation will reset all static ARP entries, and clear the configurations of all
static ARP, continue?[Y/N]:y
```

清除设备上IP地址为172.16.20.1，MAC地址为0023-0045-0067，出接口为GE1/0/1的静态ARP表项。

```
<HUAWEI> system-view
[HUAWEI] undo arp static 172.16.20.1 0023-0045-0067 interface gigabitethernet 1/0/1
```

清除设备上IP地址为172.16.20.1，从VLANIF100接口学习到的ARP表项。

```
<HUAWEI> reset arp interface vlanif 100 ip 172.16.20.1 //如果不指定IP地址，则删除设备上所有
VLANIF100接口学习到的ARP表项。
```

14.3 配置 ARP 老化时间

ARP老化时间仅对动态ARP表项生效，缺省值是20分钟。用户可以在系统视图或接口视图下执行命令**arp expire-time** *expire-time*，配置动态ARP表项的老化时间。ARP老化时间*expire-time*取值范围：框式交换机是60～62640，盒式交换机是30～62640，单位是秒。

如果只在系统视图下进行了配置，则对设备上所有接口学习到的动态ARP表项生效。如果在某接口视图和系统视图下同时进行了配置，则该接口学习到的动态ARP表项的老化时间与接口视图下的配置保持一致。

配置动态ARP表项的老化时间为1800秒。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp expire-time 1800
```


配置完成后可以在任意视图下执行命令**display current configuration | include arp**，查看设备上已配置的动态ARP表项的老化时间。

```
<HUAWEI> display current-configuration | include arp
arp expire-time 1800
```

14.4 配置静态 ARP 表项

静态ARP表项不会被老化，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，也可以通过自动扫描与固化方式批量配置静态ARP表项。

通过手工方式配置静态 ARP 表项

说明

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，建议用户尽量配置长静态ARP表项，即配置ARP表项时同时指定VLAN和出接口。

配置一条静态ARP表项，IP地址为172.16.10.2，MAC地址为0023-0045-0067，出接口GE1/0/1处于二层模式，此条ARP表项属于VLAN100。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-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。
[HUAWEI-Vlanif100] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port link-type trunk
[HUAWEI-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 //接口GigabitEthernet1/0/1处于二层模式，需要加入VLAN100。
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] arp static 172.16.10.2 0023-0045-0067 vid 100 interface gigabitethernet 1/0/1
```

配置一条静态ARP表项，IP地址为172.16.20.2，MAC地址为0023-0045-0068，出接口GE1/0/2处于三层模式。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/2
[HUAWEI-GigabitEthernet1/0/2] undo portswitch
[HUAWEI-GigabitEthernet1/0/2] ip address 172.16.20.1 24 //GigabitEthernet1/0/2的IP地址需要与静态ARP表项中的IP地址（172.16.20.2）同网段。
[HUAWEI-GigabitEthernet1/0/2] quit
[HUAWEI] arp static 172.16.20.2 0023-0045-0068 interface gigabitethernet 1/0/2
```

配置一条静态ARP表项，IP地址为172.16.30.2，MAC地址为0023-0045-0069，此静态ARP表项属于VPN实例vpn1。

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] arp static 172.16.30.2 0023-0045-0069 vpn-instance vpn1
```

配置一条静态ARP表项，IP地址为172.16.40.2，MAC地址为02bf-0045-0070。（例如设备采用多端口ARP方式与NLB服务器群集连接时，可以配置这种短静态的ARP表项。）

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


通过自动扫描与固化方式批量配置静态 ARP 表项

接口VLANIF103的IP地址为172.16.50.1/24，自动扫描该网段IP地址为172.16.50.2～172.16.50.4的ARP表项，并将学习到的ARP表项固化为静态ARP表项。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 103
[HUAWEI] interface vlanif 103
[HUAWEI-Vlanif103] ip address 172.16.50.1 24
[HUAWEI-Vlanif103] quit
[HUAWEI] interface gigabitethernet 1/0/3
[HUAWEI-GigabitEthernet1/0/3] port link-type trunk
[HUAWEI-GigabitEthernet1/0/3] port trunk allow-pass vlan 103
[HUAWEI-GigabitEthernet1/0/3] quit
[HUAWEI] display arp network 172.16.50.0 24
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
--------------------------------------------------------------------------------

172.16.50.1     00e0-0987-7895            I -
Vlanif103
--------------------------------------------------------------------------------

Total:1         Dynamic:0       Static:0     Interface:1
[HUAWEI] interface vlanif 103
[HUAWEI-Vlanif103] arp scan 172.16.50.2 to 172.16.50.4 //在接口VLANIF103上进行自动扫描，172.16.50.2～172.16.50.4与VLANIF103接口的IP地址172.16.50.1在同一网段，即ARP自动扫描区间的起始IP地址和结束IP地址必须与VLANIF接口的IP地址（主IP地址或者从IP地址）在同一网段。
Warning: This operation may take a long time, press CTRL+C to break. Continue?[Y/
N]:y
Processing...

Info: ARP scanning is completed.
[HUAWEI-Vlanif103] display arp network 172.16.50.0 24 //自动扫描后，查看ARP表项，设备新学习到3条动态ARP表项。
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
INSTANCE
                                          VLAN/
CEVLAN
--------------------------------------------------------------------------------

172.16.50.1     00e0-0987-7895            I -
Vlanif103
172.16.50.2     0200-0000-0212  20        D-0
GE1/0/3

103/-
172.16.50.3     0200-0000-0212  20        D-0
GE1/0/3

103/-
172.16.50.4     0200-0000-0212  20        D-0
GE1/0/3

103/-
--------------------------------------------------------------------------------

Total:4         Dynamic:3       Static:0     Interface:1
[HUAWEI-Vlanif103] arp fixup //在接口VLANIF103上进行固化，将学习的动态ARP表项固化为静态ARP表项。
Warning: This operation may generate configuration of static ARP, and take a long time, press CTRL
+C to break. Continue?[Y/N]:y
Processing...

Info: ARP fixup is completed.
[HUAWEI-Vlanif103] display arp network 172.16.50.0 24 //固化后，查看ARP表项，设备新学习到的3条动态ARP表项已经被固化为静态ARP表项。
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-
```



```
INSTANCE
                                        VLAN/
CEVLAN
--------------------------------------------------------------------------------

172.16.50.2     0200-0000-0212          S--         GE1/0/3

103/-
172.16.50.3     0200-0000-0212          S--         GE1/0/3

103/-
172.16.50.4     0200-0000-0212          S--         GE1/0/3

103/-
172.16.50.1     00e0-0987-7895          I -
Vlanif103
--------------------------------------------------------------------------------

Total:4         Dynamic:0       Static:3     Interface:1
```

14.5 配置 ARP 代理

Proxy ARP 分类

Proxy ARP分为路由式Proxy ARP、VLAN内Proxy ARP和VLAN间Proxy ARP，如表14-1所示。

表 14-1 Proxy ARP 方式

Proxy ARP方式	适用场景
路由式Proxy ARP	需要互通的主机（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）的场景。
VLAN内Proxy ARP	需要互通的主机处于相同网段，并且属于相同VLAN，但是VLAN内配置了端口隔离的场景。
VLAN间Proxy ARP	需要互通的主机处于相同网段，但属于不同VLAN的场景。

路由式 Proxy ARP

接口VLANIF100上配置IP地址为172.16.1.1/24，并使能路由式Proxy ARP功能。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.1.1 24
[HUAWEI-Vlanif100] arp-proxy enable
```

VLAN 内 Proxy ARP

接口VLANIF100上配置IP地址为172.16.1.1/24，并使能VLAN内Proxy ARP功能。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.1.1 24
[HUAWEI-Vlanif100] arp-proxy inner-sub-vlan-proxy enable
```


VLAN 间 Proxy ARP

接口VLANIF100上配置IP地址为172.16.1.1/24，并使能VLAN间Proxy ARP功能。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 172.16.1.1 24
[HUAWEI-Vlanif100] arp-proxy inter-sub-vlan-proxy enable
```

相关信息

技术论坛

IP与MAC一线牵之ARP

14.6 屏蔽基于源 IP 地址的 ARP Miss 告警

当某个源IP地址触发了ARP Miss告警，用户希望屏蔽此源IP地址的ARP Miss告警时，可以对这个IP地址的ARP Miss消息不进行限速。

说明

S1720GFR、S1720GW-E、S1720GWR-E、S1720X-E、S2720EI、S2750EI、S5710-C-LI、S5710-X-LI、S5700LI、S5700S-LI、S5720LI和S5720S-LI不支持该功能。

配置对IP地址为10.0.0.1的ARP Miss消息不进行限速。

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip 10.0.0.1 maximum 0
```

配置对所有源IP地址的ARP Miss消息不进行限速。

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip maximum 0
```

14.7 配置动态 ARP 检测（DAI）

动态ARP检测DAI（Dynamic ARP Inspection）功能主要用于防御中间人攻击的场景，避免设备上合法用户的ARP表项被攻击者发送的伪造ARP报文错误更新。

DAI功能是基于绑定表（DHCP动态和静态绑定表）对ARP报文进行匹配检查。

设备收到ARP报文时，将ARP报文对应的源IP地址、源MAC地址、接口、VLAN信息和绑定表的信息进行比较（比较的内容用户可以根据需要进行配置，例如可以只将ARP报文中的源IP地址和VLAN信息与绑定表的信息进行比较）：

- 如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过。
- 否则就认为是攻击，丢弃该ARP报文。

设备上配置DHCP Snooping功能，并在设备与用户侧相连的接口上使能DAI功能。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv4
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping enable //设备与用户侧相连的接口使能DHCP Snooping功能。
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/2
```



```
[HUAWEI-GigabitEthernet1/0/2] dhcp snooping trusted //设备与DHCP Server侧相连的接口配置为信任接口。如果DHCP Snooping功能部署在DHCP中继设备上，可以不配置信任接口。
[HUAWEI-GigabitEthernet1/0/2] quit
[HUAWEI] user-bind static ip-address 10.10.10.1 vlan 100 //对于静态配置IP地址的用户，在设备上配置静态绑定表。
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] arp anti-attack check user-bind enable //设备与用户侧相连的接口使能DAI功能。
[HUAWEI-GigabitEthernet1/0/1] quit
```

设备上配置DHCP Snooping功能，并在用户侧所属VLAN内使能DAI功能。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv4
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable //用户设备所属VLAN内使能DHCP Snooping功能。
[HUAWEI-vlan100] quit
[HUAWEI] vlan 200
[HUAWEI-vlan200] dhcp snooping enable
[HUAWEI-vlan200] dhcp snooping trusted interface gigabitethernet 1/0/2 //设备与DHCP Server侧相连的接口配置为信任接口。如果DHCP Snooping功能部署在DHCP中继设备上，可以不配置信任接口。
[HUAWEI-vlan200] quit
[HUAWEI] user-bind static ip-address 10.10.10.1 vlan 100 //对于静态配置IP地址的用户，在设备上配置静态绑定表。
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable //用户侧所属VLAN内使能DAI功能。
[HUAWEI-vlan100] quit
```

14.8 配置 ARP 防网关冲突

如果有攻击者仿冒网关，在局域网内发送源IP地址是网关IP地址的ARP报文，会导致局域网内其他用户主机的ARP表记录错误的网关地址映射关系。这样其他用户主机就会把发往网关的流量均发送给了攻击者，攻击者可轻易窃听到他们发送的数据内容，并且最终会造成这些用户主机无法访问网络。

为了防范攻击者仿冒网关，当用户主机直接接入网关时，可以在网关设备上使能ARP防网关冲突攻击功能。当设备收到的ARP报文存在下列情况之一：

- ARP报文的源IP地址与报文入接口对应的VLANIF接口的IP地址相同
- ARP报文的源IP地址是入接口的虚拟IP地址，但ARP报文源MAC地址不是VRRP虚MAC

设备就认为该ARP报文是与网关地址冲突的ARP报文，设备将生成ARP防攻击表项，并在后续一段时间内丢弃该接口收到的同VLAN以及同源MAC地址的ARP报文，这样就可以防止与网关地址冲突的ARP报文在VLAN内广播。

在网关设备上使能ARP防网关冲突攻击功能。缺省情况下设备上防网关冲突攻击功能处于未使能状态。

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack gateway-duplicate enable
```

