常见问题答复集（三）

H3C交换机基础维护篇

精选Q&A

《常见问题答复集》第三期来啦！

本期主要内容：DHCP篇 & IP业务篇

DHCP篇

Q1 在DHCP地址池视图下配置客户端MAC地址与IP地址的静态绑定，需要注意什么？

在DHCP地址池视图下执行命令static-bind ip-address *ip-address* [*mask-length* | mask *mask*] hardware-address *hardware-address* [ethernet | token-ring] }时需要注意，配置静态绑定时，必须确保绑定的MAC地址与用户实际的MAC地址保持一致，并且配置的MAC地址必须是有效的MAC地址。

MAC地址为4～39个字符的字符串，字符串中只能包括十六进制数和"-"，且形式为H-H-H…。除最后一个H表示2位或4位十六进制数外，其他均表示4位十六进制数。例如：aabb-cccc-dd为有效的客户端硬件地址，aabb-c-dddd和aabb-cc-dddd为无效的客户端硬件地址。

Q2 指定接口引用不存在的DHCP策略会怎样？

执行命令dhcp policy *policy-name*创建DHCP策略，并在指定接口下执行dhcp apply-policy *policy-name*命令引用该策略后，该接口接收到DHCP请求报文时，根据配置顺序逐个匹配DHCP策略中通过class ip-pool命令指定的DHCP用户类。如果接收DHCP请求报文的接口引用的DHCP策略不存在，或匹配的DHCP用户类关联的DHCP地址池不存在时，IP地址和其他参数会分配失败。

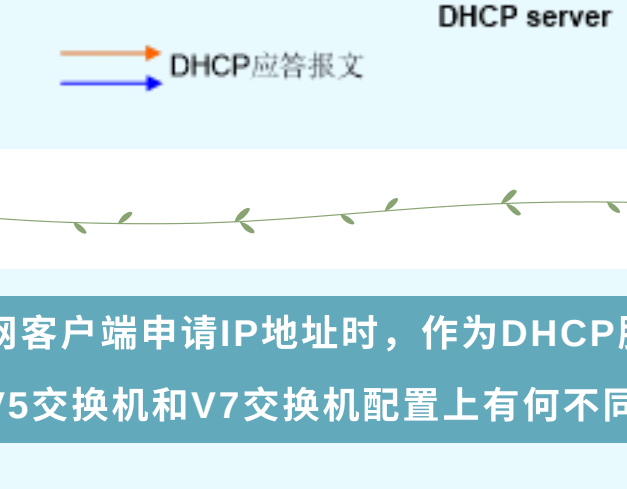
Q3 地址池IP网段范围规划小了会发生什么？

如果可供分配的IP网段范围过小，会导致动态分配的IP地址范围内没有空闲地址，DHCP服务器无法为剩余的DHCP客户端分配地址。因此建议用户合理规划IP网段范围，保证所有客户端都能获取到IP地址。

Q4 开启DHCP Snooping功能之后，下挂用户无法获取IP地址怎么办？

缺省情况下，在开启DHCP Snooping功能后，设备上所有支持DHCP Snooping功能的端口均为不信任端口。

如下图所示，需要通过dhcp snooping trust命令将连接DHCP服务器的端口设置为信任端口，并且设置的信任端口和与DHCP客户端相连的端口必须在同一个VLAN内，以便DHCP Snooping设备正常转发DHCP服务器的应答报文，保证DHCP客户端能够从合法的DHCP服务器获取IP地址。



Q5 私网客户端申请IP地址时，作为DHCP服务器的V5交换机和V7交换机配置上有何不同？

对于处于VPN私网中的客户端申请IP地址，若V5设备作为DHCP服务器，不需要在DHCP地址池下绑定VPN实例，客户端就可以获取到IP地址。

当V7设备作为DHCP服务器时，需要在相应地址池中配置绑定VPN实例。例如位于VPN实例abc中的客户端申请IP地址时，需要在DHCP服务器上对应的DHCP地址池视图下执行vpn-instance abc命令来绑定VPN实例abc。

DHCP服务器可以将网络划分成公网和VPN私网，未配置VPN属性的地址池被划分到公网，配置了VPN属性的地址池被划分到VPN私网，这样服务器就可以更好地选择合适的地址池来为客户端分配租约并且记录该客户端的状态信息。

Q6 配置DHCP服务器或DHCP中继生效的前提是？

只有在系统视图下执行dhcp enable命令后，DHCP服务器或DHCP中继配置才能生效。

Q7 设备记录DHCP客户端IP地址与MAC地址的对应关系，缺省是开启的吗？

缺省情况下，DHCP Snooping表项记录功能处于关闭状态，如果有其他特性如IP Source Guard等想要利用这些表项信息，可以在系统视图、VLAN视图、VSI视图或接口视图下执行dhcp snooping binding record命令生成DHCP Snooping安全表项。

需要注意的是，不同交换机产品支持开启DHCP snooping功能和表项记录功能的视图不同，请以设备实际情况为准。

Q8 重新指定地址池动态分配的IP地址范围时，应注意什么？

在DHCP地址池视图下，使用address range命令修改已存在的动态分配的IP地址范围时，新的IP地址范围需要覆盖之前该DHCP地址池已分配出去的IP地址，否则系统会提示配置错误。

如果用户仍然打算继续配置，需要使用reset dhcp server ip-in-use命令释放分配的地址租约后，再进行address range命令配置。

Q9 DHCP Snooping的信任端口和非信任端口应设置在什么位置？

网络中如果存在私自架设的非法DHCP服务器，可能导致DHCP客户端获取到错误的IP地址和网络配置参数，从而无法正常通信。为了使DHCP客户端能通过合法的DHCP服务器获取IP地址，DHCP Snooping安全机制允许将端口设置为信任端口和不信任端口。

在DHCP Snooping设备上指向DHCP服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，私自架设的伪DHCP服务器无法为DHCP客户端分配IP地址。

Q10 交换机作为DHCP服务器，如何配置才能使网络中的设备获得固定IP地址或不与已有IP地址的设备发生地址冲突？

交换机作为DHCP服务器为客户端分配IP地址，如果想让某客户端获取固定IP地址，而不是随机获取IP地址，可以在DHCP地址池视图下，使用static-bind ip-address命令配置该客户端的静态地址绑定。此后当客户端申请IP地址时，服务器会根据客户端的客户ID或MAC地址分配固定的IP地址。例如，在DHCP地址池0中配置为客户端ID为00aa-aabb的客户端，固定分配IP地址10.1.1.1/24：

```
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
client-identifier 00aa-aabb
```

如果网络中的其他设备已占用了DHCP服务器地址池中的IP地址，为避免DHCP服务器把这些IP地址分配出去，引起IP地址冲突，需要在作为DHCP服务器设备的系统视图下，使用dhcp server forbidden-ip命令配置全局不参与自动分配的IP地址；或在DHCP地址池视图下，使用forbidden-ip命令配置地址池中不参与自动分配的IP地址。

IP业务篇

Q1 为什么将两台交换机接入到同一个局域网，登录交换机的Web管理页面时会出现闪退？

目前，部分型号的交换机默认支持Web登录，且出厂时Vlan-interface1均配置了缺省管理IP地址。用户可通过设备铭牌标签上打印的信息获取该管理IP地址，该IP地址的掩码为255.255.255.0。

当多台缺省管理IP地址相同的以太网交换机接入同一局域网时，可能因IP地址冲突导致无法登录Web管理页面或登录后闪退。此时需由管理员通过Console口登录交换机，并在Vlan-interface1接口下通过ip address命令配置新的IP地址和掩码，注意新配置的IP地址应在该局域网的网段内，且与其他设备的IP地址不冲突。

Q2 为什么会出现网页打不开但是能Ping通对方IP地址的情况？

能够Ping通对方的IP地址，说明设备之间链路是连通的且路由是可达的，报文能够正常收发。那么这时候出现网页打不开或打开速度慢的原因有可能是链路拥塞、防火墙安全策略问题或TCP MSS值过小。

对于链路拥塞问题，可以通过配置QoS策略或者拥塞管理等方式来缓解。

对于防火墙安全策略问题，请检查已配置的防火墙策略是否过滤了Web服务。

对于TCP MSS值过小的问题，请使用tcp mss value命令将TCP MSS调整到一个合理的取值，通常取值为1460。

Q3 反复出现通过Telnet登录上设备后又断开的情况是什么原因？

物理链路时断时连、接口故障或者IP地址冲突都会导致Telnet登录上设备后又断开。

Q4 为什么以太网端口正常的情况下，设备上对应的以太网端口指示灯不亮？

在指示灯未损坏的情况下，若设备的前面板有端口状态指示灯模式切换按钮（MODE按钮），则有以下可能：

1. 设备是PoE机型：

(1) 当MODE灯呈绿色闪烁状态时，设备的端口处于PoE模式。在该模式下，若设备端口未使能PoE功能，端口指示灯是不亮的。

(2) 当MODE灯呈黄色闪烁状态时，设备的端口处于IRF模式。在这种模式下，端口状态指示灯绿色常亮表示设备的成员编号，其他灯灭。

2. 设备是非PoE机型

当MODE灯呈黄色闪烁状态时，设备的端口处于IRF模式。在这种模式下，端口状态指示灯绿色常亮表示设备的成员编号，其他灯灭。

需要说明的是，当端口处于IRF模式时，若设备的成员编号为n：对于S5560X-EI系列、S6520X-EI、S6520X-HI等系列，编号为n的端口状态指示灯绿色常亮，其它灯灭；对于S5130S-EI、S5130S-HI、S5560S-EI等系列，编号为1~n的端口状态指示灯绿色常亮，其他灯灭。关于端口状态指示灯模式切换按钮的介绍，请参见各产品安装指导里的指示灯介绍章节。

Q5 IP地址冲突会导致出现什么故障？

IP地址冲突，往往会导致网络设备之间无法正常通信。比较常见的故障现象有：

1. 无法Ping通其他设备或无法被其他设备Ping通

2. 无法登录Web管理界面或登录后闪退

3. Telnet连接设备时断时连

4. 使用FTP、TFTP等方式传输文件时异常断开

Q6 设备Ping网关地址有丢包，可以从哪些方面排查？

1. 检查设备是否正确学习到了网关IP地址对应的ARP表项，即执行display arp命令查看ARP表项中网关IP地址对应的MAC地址是否和实际网关MAC地址一致。如果一致，说明ARP表项正常，需要考虑是其他原因导致故障。

2. IP地址设置错误。例如子网掩码错误、设备的IP和网关的IP不在同一个网段等情况，重新配置设备正确的IP地址即可。

3. IP地址冲突。例如局域网内其他网络设备的IP地址与设备或网关的IP地址存在冲突，此时重新分配一个未占用的IP地址即可。

4. 链路故障。例如端口链路协议异常、接口物理故障、链路断开等情况，出现这种情况则需要对链路和接口进行故障排查。

5. 若以上各方面均正常，则建议在Ping报文沿途设备上通过抓包和流统等手段定位丢包位置，再具体分析丢包设备的问题。

Q7 两台主机的IP地址属于同一网段，但是被设备分割在不同的物理网络，如何实现两台主机之间的ARP报文正常通信？

可以在设备上配置代理ARP功能。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功能的设备就可以应答该请求，这个过程称作代理ARP。

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：

1. 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。在接口视图下执行proxy-arp enable命令即可开启普通代理ARP功能。

2. 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。在接口视图下执行local-proxy-arp enable [ip-range *start-ip-address* to *end-ip-address*]命令即可开启本地代理ARP功能。

Q8 二层交换机如何配置IP地址？

二层交换机的以太网端口无法配置IP地址，只能将端口绑定到某个VLAN下，再给该VLAN对应的VLAN虚接口配置IP地址。

以二层交换机的GigabitEthernet1/0/1端口加入VLAN 10，并将VLAN 10虚接口配置IP地址192.168.1.2/24为例：

```
创建VLAN 10
[Switch] vlan 10

将接口GigabitEthernet1/0/1加入到VLAN 10中
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port access vlan 10

创建接口Vlan-interface10，并配置IP地址
[Switch] interface vlan-interface 10
[Switch-vlan-interface10] ip address 192.168.1.2 24
```

Q9 配置静态ARP表项时需要注意哪些地方？

1. 确保静态ARP表项的IP地址和MAC地址是正确的对应关系。

2. 静态ARP表项不会被动态ARP表项更新。当发现网络中静态ARP表项关联的设备链路出现故障，或者更换了设备的接口，请及时手动更新静态ARP表项。

3. 静态ARP表项不会老化。当设备支持学习的ARP表项数量太低时，请尽可能减少静态ARP表项的数量，以免影响动态ARP表项的学习。如果静态ARP表项关联的设备或接口从网络中移除，请及时删除对应的静态ARP表项。

—— end ——