H3C 交换机 常见配置问题 FAQ

资料版本：6W102-20220630

目 录

1 登录设备 1
1.1 通过 Console 口连接设备，为什么配置终端无显示或显示乱码？ 1
1.2 如何恢复 Console 口密码？ 1
1.3 如何修改 web 登录密码？ 6
2 用户权限 7
2.1 为什么无法执行某些命令或提示配置权限不足？ 7
3 设备管理 7
3.1 对于支持可插拔风扇模块的设备，开机后 SYS 灯红色常亮该如何解决？ 7
3.2 风扇模块没有正确安装会引起什么故障？ 8
3.3 BIDI 型号的光模块能否与其他光模块混合使用？ 8
3.4 为什么以太网端口正常的情况下，设备上的对应的以太网端口指示灯不亮？ 8
3.5 新增 ACL 时提示资源不足，可能的原因有哪些？ 9
3.6 交换机未运行业务，但 CPU 使用率高，如何解决？ 9
4 IRF 9
4.1 将物理端口与 IRF 端口绑定时提示需要先将端口 shutdown，如何解决？ 9
4.2 将物理端口与 IRF 端口绑定时失败，如何解决？ 10
4.3 将物理端口与 IRF 端口绑定时提示某些端口为一组需要将这些端口全部关闭，如何解决？ 11
4.4 使用 undo shutdown 命令开启端口时提示需要将一组端口全部与 IRF 端口绑定或全部取消绑定，如何解决？ 12
4.5 完成 IRF 成员编号、IRF 物理端口等配置，重启设备后没有形成 IRF，是什么原因？ 12
4.6 执行 irf-port-configuration active 命令激活 IRF 物理端口的配置之后，设备提示由于 XX 配置不一致无法形成 IRF，如何处理？ 13
4.7 框式交换机是否支持 IRF 环形连接拓扑？ 14
4.8 IRF 重启后为什么有配置丢失？ 14
4.9 LACP MAD 检测采用的组网有何要求？ 15
4.10 BFD MAD 检测 VLAN 有何限制及注意事项？ 15
5 MAC 地址表 16
5.1 为什么设备无法转发源 MAC 地址是 VLAN 接口的 MAC 地址的流量？ 16
6 接口与聚合 16
6.1 电口或光口互连是否应该设置强制双工和速率？ 16
6.2 Combo 口为什么不 UP？ 17
6.3 聚合接口和成员接口的配置有哪些要求？ 17
6.4 聚合链路两端如何选择聚合模式？ 18

6.5 如何处理链路聚合负载分担不均匀的问题？ 18
6.6 使用链路聚合如何与服务器互通？ 19
7 DRNI 19
7.1 DRNI 组网中管理 IP 地址互访不通如何处理？ 19
7.2 DRNI+VRRP 组网中，单挂接入 DR 设备时，如何避免同一 ICMP 报文被 DR 主设备收到两次？ 19
8 VLAN 19
8.1 为什么部分 VLAN 无法通过 Trunk 端口？ 19
8.2 如何正确配置允许指定 VLAN 或全部 VLAN 通过 Trunk 端口？ 20
8.3 为什么设备获取不到 IP Phone 的 MAC 地址？ 20
8.4 如何限制广播域的范围？ 21
8.5 错误配置接口链路类型导致无法正常通信怎么办？ 21
8.6 在 Voice VLAN 中出现除语音数据之外的业务数据丢失情况怎么办？ 21
8.7 如何选择端口的 Voice VLAN 工作模式？ 21
9 生成树 23
9.1 什么情况下需要配置生成树边缘端口？ 23
9.2 在生成树拓扑中，不同的设备可以配置不同的生成树工作模式吗？ 23
9.3 开启生成树协议后，可通过哪些方法维持网络拓扑的稳定？ 23
9.4 设备频繁收到 TC 报文时该如何操作？ 24
9.5 开启生成树协议后，如何避免对其他网络造成不良影响？ 25
10 环路检测 26
10.1 如何选择环路检测时间间隔？ 26
10.2 环路检测和生成树功能可以同时配置吗？ 26
11 镜像 26
11.1 希望为本地端口镜像组配置多于一个目的端口，但部分设备不支持加入第二个目的端口怎么处理？ 26
11.2 配置二层远程端口镜像后，为什么与镜像无关的端口有异常的流量增加？ 27
11.3 配置镜像组的源端口失败，可能的原因有哪些？ 27
11.4 为什么配置远程镜像 VLAN 的 VLAN 接口可能导致镜像功能异常？ 27
12 DHCP 27
12.1 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？ 27
12.2 指定接口引用不存在的 DHCP 策略会怎样？ 28
12.3 地址池 IP 网段范围规划小了会发生什么？ 28
12.4 配置 DHCP Snooping 之后，下挂用户无法获取 IP 地址 28
12.5 私网客户端申请 IP 地址时，作为 DHCP 服务器的 V5 设备和 V7 设备配置上有何不同？ 29
12.6 配置 DHCP 服务器或 DHCP 中继生效的前提是什么? 29
12.7 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？ 29

12.8 重新指定地址池动态分配的 IP 地址范围时，应该注意什么？ ····· 29
12.9 DHCP Snooping 的信任端口和非信任端口设置在什么位置上？ ····· 29
12.10 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 或不与已有 IP 地址的设备发生地址冲突？ ····· 29
12.11 为什么在 DHCP snooping 组网下，DHCP 服务器的部分地址无法分配？ ····· 30
13 IP 业务 ····· 30
13.1 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？ ····· 30
13.2 为什么会出现网页打不开，但是能 Ping 通对方 IP 地址的情况？ ····· 30
13.3 反复出现通过 Telnet 登录上设备后又断开的情况是什么原因？ ····· 31
13.4 IP 地址冲突会导致出现什么故障？ ····· 31
13.5 设备 Ping 网关地址有丢包，可以从哪些方面排查？ ····· 31
13.6 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？ ····· 31
13.7 二层交换机如何配置 IP 地址？ ····· 32
13.8 配置静态 ARP 表项时需要注意哪些地方？ ····· 32
14 接入认证 ····· 32
14.1 接入用户认证时，按照什么顺序选择认证域？ ····· 32
14.2 如何修改或删除缺省的 ISP 域？ ····· 33
14.3 本地用户没有配置服务类型会导致认证失败吗？常用服务类型有哪些？ ····· 33
14.4 RADIUS 认证时为什么需要配置 nas-ip？ ····· 34
14.5 802.1X 在线用户握手功能的应用场景和注意事项有哪些？ ····· 34
14.6 在线用户握手安全功能有哪些使用限制？ ····· 35
14.7 什么情况下需要开启在线握手成功报文功能？ ····· 35
14.8 配置设备端和服务端的认证、授权、计费时需要注意什么？ ····· 35
14.9 什么情况下需要配置允许 MAC 迁移功能？ ····· 35
14.10 如何配置和查看 802.1X 用户使用的强制认证域？ ····· 36
14.11 当前 ISP 域中未指定具体授权方法的情况下，缺省授权方法是什么？如何配置缺省授权？ ····· 36
14.12 使用 iNode 客户端作为 802.1X 客户端时，iNode 该如何配置？ ····· 36
14.13 端口安全模式分为哪两类？配置之前，端口需要满足什么条件？ ····· 39
14.14 802.1X 环境如何实现终端免认证？ ····· 40
14.15 设备对 RADIUS 15 号属性的检查方式该如何配置？ ····· 40
14.16 对 802.1X 用户进行周期性重认证时，设备按什么顺序为其选择重认证时间间隔？ ····· 41
14.17 802.1X 的 Free IP 功能是否可以与端口安全同时开启？ ····· 41
14.18 802.1X 的 Free IP 功能是否可以与 MAC 地址认证同时开启？ ····· 41
14.19 为什么在接入设备上强制 Portal 用户下线失败？ ····· 41
14.20 什么情况需要配置认证触发功能？ ····· 42

14.21 什么情况下端口会加入 Critical VLAN？ ····· 42
14.22 端口安全允许的最大用户接入数有何限制？ ····· 42
14.23 同一端口下，同时进行 MAC 地址认证的终端过多时，重新认证时间间隔该如何设置？ ····· 43
14.24 IP Source Guard 动态绑定表项可以来源于哪些功能模块？ ····· 43
14.25 配置了 IP Source Guard 静态绑定表项，为什么绑定功能不生效？ ····· 43
14.26 Portal HTTPS 重定向为什么不生效？ ····· 43
14.27 为什么需要配置 RADIUS 报文的共享密钥？ ····· 44
14.28 配置 AAA 时如果没有计费服务器，需要配置当前 ISP 域的计费方法吗？ ····· 44
14.29 在 ISP 域下，若配置 AAA 认证/授权/计费方法使用的 RADIUS 方案不存在，AAA 认证/授权/计费方法会生效吗？ ····· 44
14.30 在实际应用场景中，若需要通过 iMC 服务器下发安全 ACL，应该如何配置？ ····· 44
14.31 802.1X 在线用户较多时，用户重认证周期过长该如何解决？ ····· 45
14.32 如何解决设备因无法感知 802.1X 认证用户离线导致用户再次上线失败？ ····· 45
14.33 配置 802.1X Guest VLAN 功能前有哪些配置准备？ ····· 45
14.34 端口接入控制方式为 Port-based 时可以配置单播触发功能吗？ ····· 45
14.35 如何配置 MAC 地址认证用户使用的账号格式？ ····· 46
14.36 开启 802.1X 或 MAC 地址认证对端口安全功能有何影响？ ····· 46
14.37 如何修改端口安全模式？ ····· 46
15 路由 ····· 46
15.1 路由配置不完整或配置错误会导致网络出现哪些故障，如何进行排查？ ····· 46
15.2 在同一设备上配置的 VPN 网段和公网网段相同，会冲突吗？ ····· 47
15.3 策略路由配置错误导致 Ping 不通故障如何排查？ ····· 47
15.4 静态路由的出接口没 UP 会导致 Ping 不通吗？ ····· 48
15.5 终端设备如果未配置网关，会导致通信故障吗？ ····· 48
15.6 为什么配置的备份静态路由未及时生效？ ····· 48
15.7 为什么配置了静态路由关联 track 项，却无法通过 track 关联的检测模块及时检测链路故障？ ····· 49
15.8 BGP 邻居关系未建立的常见原因有哪些？如果处理此类故障？ ····· 49
15.9 怎么查看和配置等价路由条数？ ····· 50
15.10 不同 VRF 或公网与 VRF 如何通过三层接口实现互访？ ····· 50
15.11 设备配置前缀大于 64 位的 IPv6 路由后为什么不生效？ ····· 50
15.12 部署 OSPF 后，为什么无法建立邻居关系？ ····· 51
16 组播 ····· 51
16.1 组播组网，接入设备配置二层组播后，为什么网络卡顿、延迟高？ ····· 51
16.2 组播组网，二层接入设备配置了 IGMP Snooping 和 IGMP Snooping drop-unknown 功能后，为什么组播转发表项异常？ ····· 52
16.3 什么情况下需要配置查询器？是否可以配置多个查询器？ ····· 52

16.4 同一 PIM 域内，配置三层组播功能后，三层组播流量不通？ ····· 53
17 安全 ····· 54
17.1 为什么配置了密码控制却不生效？ ····· 54
17.2 设备作为 SSH 服务器，为什么配置了 NTP 后登录不上设备？ ····· 54
17.3 为什么无法修改设备密码？ ····· 55
17.4 设备作为 SSH 服务器，什么情况下需要修改认证超时时间？ ····· 55
17.5 设备作为 SSH 客户端，如何删除本地文件中的指定服务器公钥？ ····· 55
17.6 为什么启用了 SSH 服务器功能后，客户端连接到设备时提示连接中断？ ····· 55
18 ACL 和 QoS ····· 56
18.1 QoS 策略流分类中配置了多条匹配规则，为什么没有一条规则能够匹配到相应的流量呢？ ····· 56
18.2 应用 ACL 进行报文过滤、禁止某 IP 地址段的主机发出的报文通过，为什么不生效呢？ ····· 56
18.3 在 VLAN 接口上应用 ACL 进行报文过滤，对二层转发报文不生效。 ····· 56
18.4 为什么报文命中 IP Source Guard 表项，但却无法转发呢？ ····· 56
18.5 ACL 规则的匹配顺序是怎么样的？ ····· 56
19 可靠性 ····· 58
19.1 修改了 VRRP 备份组的 VRRP 使用版本后，VRRP 为什么失效了？ ····· 58
19.2 VRRP 备份组网，当 Master 设备上行链路状态 down 后，备份组为什么没有切换？ ····· 58
19.3 配置 VRRP 与 Track 联动监视 Master 设备上行链路状态，Track 状态变为 Negative 时，为什么 VRRP 备份组中的主备未进行切换？ ····· 58
19.4 支持拨码开关的 IE 系列交换机，配置 RRPP 相关功能并保存配置，设备重启后 RRPP 配置丢失是什么原因？ ····· 59
20 网络管理与监控 ····· 59
20.1 PoE 端口无法正常供电的常见原因有哪些？ ····· 59
20.2 为什么 NMS 对设备的远程管理和操作出现异常？ ····· 60
20.3 设置本地时钟作为参考时钟会影响 NTP 客户端和服务器进行时间同步吗？ ····· 61
20.4 配置客户端/服务器模式下的 NTP，服务器端的时钟层数是否要小于客户端的时钟层数？ ····· 61
20.5 NTP 客户端/服务器时间不同步，时间相差若干小时的原因是什么？ ····· 61
20.6 什么情况下需要配置 PTP 接口角色才能实现 PTP 时间同步，有哪些配置限制？ ····· 61
20.7 为什么无法通过云平台（绿洲云）远程管理设备？ ····· 62
20.8 设备产生的日志信息过多，如何处理？ ····· 62
21 VXLAN ····· 63
21.1 为什么设备上无法配置 VXLAN 特性相关的命令？ ····· 63

说明

本文为交换机产品通用性内容，部分特性或功能存在产品支持差异。产品对各特性和功能的支持情况请参考产品的配置指导。

1 登录设备

1.1 通过Console口连接设备，为什么配置终端无显示或显示乱码？

设备上电后，通过 Console 口连接的配置终端无显示信息或显示乱码，首先应检查：电源是否正常；以及配置口（Console 口）电缆是否正确连接。如果以上检查未发现问题，很可能是配置电缆有问题或者终端参数的设置错误，请确认终端的参数设置：

- 波特率：9600
- 数据位：8
- 停止位：1
- 奇偶校验：无
- 流量控制：无

确认终端参数设置正确但故障无法解决时，请更换配置电缆进行替换测试。

1.2 如何恢复Console口密码？

说明

建议优先使用方法一恢复 Console 口密码，如果忘记所有登录设备的密码，再使用其他方法。

1. 方法一：通过 Stelnet/telnet 登录设备修改 Console 口密码。

(1) 通过 Stelnet/telnet 登录设备。

(2) 进入系统视图。

```
system-view
```

(3) 进入 AUX 用户线或 AUX 用户线类视图。

- 进入 AUX 用户线视图。

  line aux *first-number* [*last-number*]

- 进入 AUX 用户线类视图。

  line class aux

(4) 设置登录用户的认证方式为密码认证。

```
authentication-mode password
```

(5) 设置认证密码。

set authentication password { **hash** | **simple** } *password*

(6) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

2. 方法二：通过 bootware 菜单选择跳过配置文件启动后手工修改 console 口密码。

说明

不同产品的 bootware 页面可能有所不同，此处以 S5130 系列以太网交换机为例。

(1) 通过 console 口连接设备后将设备重新启动。

(2) 设备重启时按下 Ctrl+B 进入 bootware 菜单，选择跳过当前配置启动，如图 1-1 所示。

图1-1 进入 bootware 菜单并跳过当前配置启动

```
Press Ctrl+B to access EXTENDED BOOT MENU...0

Password recovery capability is enabled.

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright

Enter your choice(0-8): 7
The current setting will run with current configuration file when reboot.
Are you sure you want to skip current configuration file when reboot? Yes or No
(Y/N):Y
Setting...Done.
```

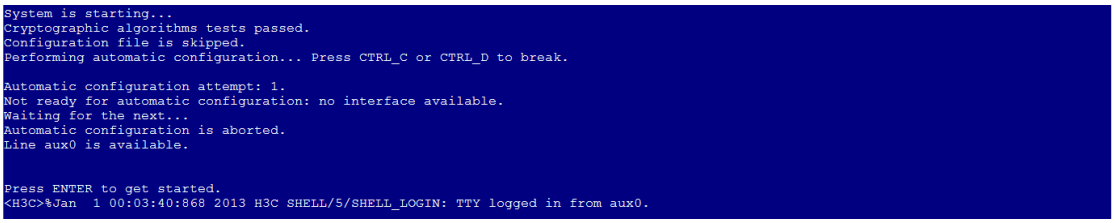
(3) 选择 Reboot 重启设备，如图 1-2 所示。

图1-2 重启设备

```
Enter your choice(0-8): 7
The current setting will run with current configuration file when reboot.
Are you sure you want to skip current configuration file when reboot? Yes or No
(Y/N):Y
Setting...Done.

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright

Enter your choice(0-8): 0
Starting......
Press Ctrl+D to access BASIC BOOT MENU
```

(4) 设备重启时按下 Ctrl+C 或 Ctrl+D 跳过自动配置，如图 1-3 所示。

图1-3 跳过自动配置



(5) 按下 Enter 键成功跳过配置文件启动。

(6) 查看配置文件内容。

```
more startup.cfg
```

(7) 将配置文件全部选中后复制粘贴到本地，如图 1-4 与图 1-5 所示

图1-4 导出配置文件（一）

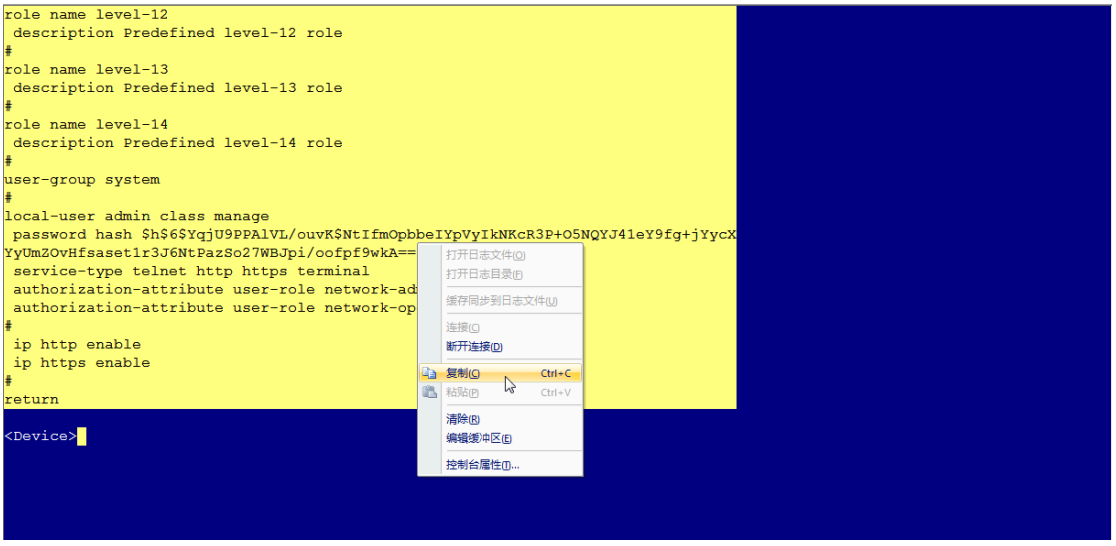


图1-5 导出配置文件（二）

```
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash $h$6$YqjU9PPAlVL/ouvK$NtIfmOpbbeIYpVyIkNKcR3P+O5NQYJ41eY9fg+jYycX
YyUmZOvHfsaset1r3J6NtPazSo27WBJpi/oofpf9wkA==
 service-type telnet http https terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ip http enable
 ip https enable
#
return
```

(8) 修改配置文件，配置新密码为 hello12345，如图 1-6 所示

图1-6 配置新密码

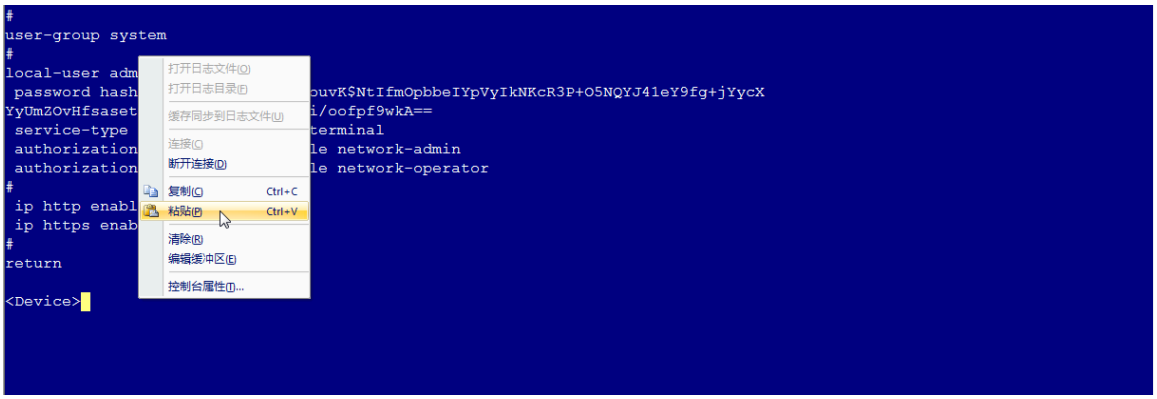
```
description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password simple hello12345
 service-type telnet http https terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ip http enable
 ip https enable
#
return
```

(9) 进入系统视图。

system-view

(10) 将修改后的配置文件复制粘贴到设备，如图 1-7 所示。

图1-7 导入配置文件



(11) 保存配置。

save

(12) 重启设备。

Reboot

3. 方法三：通过 bootware 菜单选择跳过配置文件启动后配置回滚。

(1) 通过方法二跳过配置文件启动后进入系统视图。

system-view

(2) 将当前配置回滚至默认配置文件 startup.cfg 中的配置状态

configuration replace file *startup.cfg*

(3) 输入 N，选择不保存当前配置。

(4) 等待配置回滚完成后进入系统视图。

system-view

(5) 进入 AUX 用户线或 AUX 用户线类视图。

- 进入 AUX 用户线视图。

  line aux *first-number* [*last-number*]

- 进入 AUX 用户线类视图。

  line class aux

(6) 设置登录用户的认证方式为密码认证。

authentication-mode password

(7) 设置认证密码。

set authentication password { **hash** | **simple** } *password*

(8) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

4. 方法四：通过 bootware 菜单选择跳过配置文件启动后将设备恢复出厂设置。

注意

此操作会清空设备所有配置，请确保当前业务不会受到影响时再进行。

(1) 通过方法二跳过配置文件启动后保存当前空配置。

save

(2) 重启设备。

reboot

1.3 如何修改web登录密码？

可以通过 Console 口、Stelnet/telnet 等方式登录设备后设置新的 web 登录密码。

(1) 通过 Console 口、Stelnet/telnet 等方式登录设备。

(2) 进入系统视图。

system-view

(3) 进入用于 Web 登录的本地用户视图。

local-user *user-name*

(4) 修改用户的密码。

Password [{ **hash** | **simple** } *password*]

2 用户权限

2.1 为什么无法执行某些命令或提示配置权限不足？

可能是当前用户角色的权限不足，请使用具有 network-admin 角色的用户登录设备再次尝试。

3 设备管理

3.1 对于支持可插拔风扇模块的设备，开机后SYS灯红色常亮该如何解决？

说明

不同产品的指示灯情况有所不同，此处以 S5560X-EI 系列以太网交换机为例，各产品的具体情况请参考对应的安装指导。

支持可插拔风扇模块的设备，若风扇模块正常，但风扇模块的实际风道风向与设备期望的风扇模块的风道风向不一致，则设备系统指示灯（SYS 灯）异常（红色常亮），但风扇模块的指示灯正常（黄色常亮），此时风扇运行噪音通常比较大，设备会打印风扇告警的日志信息。

风扇模块的实际风道方向，由所选风扇模块的型号决定。通常有：端口侧进风、电源侧出风或电源侧进风、端口侧出风两种。可查看对应的风扇手册了解；也可以通过在设备上执行 **display fan** 命令，查看字段“Airflow Direction”（风扇模块的实际风道方向）了解。

设备期望的风扇模块的风道方向，支持通过命令行进行配置，并可通过执行 **display fan** 命令，查看字段“Prefer Airflow Direction”（期望的风扇模块的风道方向）了解。

```
<Sysname> display fan
 Slot 1:
 Fan 1:
 State    : Normal
 Airflow Direction: Port-to-power
 Prefer Airflow Direction: Port-to-power
```

当二者不一致时，可通过系统视图下的 **fan prefer-direction** 命令调整设备期望的风道方向，使其与风扇模块的实际风道方向一致。

- 指定参数 **port-to-power**，表示期望风道方向为端口侧进风，电源侧出风。

- 指定参数 **power-to-port**，表示期望风道方向为电源侧进风，端口侧出风。

需要注意的是：设备上电后，是否检查风扇模块的实际风道风向与设备期望的风扇模块的风道风向一致，与产品和软件版本有关。各产品的具体情况请参考安装指导。

3.2 风扇模块没有正确安装会引起什么故障？

当风扇模块没有正确安装时，可能引起的故障包括但不限于：设备上电后无法启动、设备低负载运行但风扇声音很大、设备自动关机、设备温度过高、打印报错日志等。以下情况属于风扇模块没有正确安装：

- 风扇模块没有插到位或松动
- 安装的风扇模块不是适配的型号
- 没有安装风扇模块或仅安装一个风扇模块
- 安装的 2 个风扇模块的型号不同（风道风向不一致）
- 风扇实际的风道风向与期望的风道风向不一致

设备出现以上故障且用户发现风扇模块没有正确安装时，应及时重新安装风扇模块，确保设备安装两个适配的、相同型号的风扇模块，保证风扇模块插到位，并将期望的风道风向和风扇模块实际的风道风向配置成一致。

3.3 BIDI型号的光模块能否与其他光模块混合使用？

不可以，BIDI 型号的光模块必须成对使用。例如 SFP-XG-LX-SM1270-BIDI 必须和 SFP-XG-LX-SM1330-BIDI 成对使用，否则光模块无法正常工作。关于设备支持的 BIDI 光模块型号及可以成对使用的型号，请查看设备的硬件安装指导。

3.4 为什么以太网端口正常的情况下，设备上的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：

- 设备是 PoE 机型
  - 当端口模式指示灯呈绿色闪烁状态时，此时设备的端口处于 PoE 模式。在这种模式下，若设备端口未使能 PoE 功能，端口的指示灯是不亮的。
  - 当端口模式指示灯呈黄色闪烁状态时，此时设备的端口处于 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。
- 设备是非 PoE 机型
  - 当端口模式指示灯呈黄色闪烁状态时，此时设备的端口处于 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。

说明

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。

3.5 新增ACL时提示资源不足，可能的原因有哪些？

原因一：当前设备已达到 ACL 资源上限，请使用 display qos-acl resource 命令查看 acl 资源是否用尽，若用尽，请删除无用的 ACL 规则、QoS 策略、策略路由等无关业务确保设备有足够的内存进行 ACL 新增。

原因二：设备达到了缺省内存告警门限，请使用 display memory 命令查看设备的内存使用情况，并通过释放内存来确保有足够的内存空间新增 ACL。

原因三：误将内存告警门限配置得过低，导致设备异常认为达到了资源上限。可使用 **display memory-threshold** 命令来查看内存告警门限的相关信息，并使用 **undo memory-threshold** 命令用来恢复门限值缺省情况，保证设备剩余内存不在门限告警范围内即可正常创建 acl。有关设备内存告警门限的配置请查看产品配套资料“基础配置”中的“设备管理”。

如果上述方法不能解决您的问题，请联系 H3C 技术支持。

3.6 交换机未运行业务，但CPU使用率高，如何解决？

请先使用 **display process cpu** 命令显示设备所有进程的 CPU 使用率信息，若发现是 TMTH 进程的 CPU 使用率过高，可通过如下方式排查：TMTH 进程是端口训练进程，如果接口接了网线或者光模块但是对端无设备连接，设备会不断训练端口让其处于 up 状态，占用 CPU。请排查下是否有将插入模块和网线但是未接终端的接口情况，如果有，请先将这些端口手动 **shutdown** 之后再使用 display cpu-usage 命令查看 CPU 利用率信息，确保 CPU 使用率恢复正常。

如果上述方法不能解决您的问题，请联系 H3C 技术支持。

4 IRF

4.1 将物理端口与IRF端口绑定时提示需要先将端口shutdown，如何解决？

将物理端口与 IRF 端口绑定时提示需要先将端口 **shutdown**，输出类似如下提示（提示仅为示例，不同设备输出的提示信息可能有所区别）。

```
<Sysname> system-view
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
Please shutdown the current interface first.
```

以如上设备显示为例，配置 IRF 物理端口的过程如下：

(1) 进入端口 Ten-GigabitEthernet1/0/1 视图，执行 **shutdown** 命令关闭端口；

(2) 进入 IRF1/1 端口配置端口 Ten-GigabitEthernet1/0/1 与 IRF1/1 端口绑定；

(3) 再次进入端口 Ten-GigabitEthernet1/0/1 视图，执行 **undo shutdown** 命令开启端口。

(4) 完成全部物理端口绑定后，执行 **save** 命令保存配置。

(5) 执行 **irf-port-configuration active** 命令激活 IRF 物理端口配置。

```
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[Sysname-irf-port1/1] quit
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 5 commands and d
eletes 1 commands.
If you want to see the configuration differences, please cancel this operation,
and then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
[Sysname] irf-port-configuration active
```

此步骤仅包含 IRF 物理端口的配置过程，IRF 的全部配置过程请查看“虚拟化技术配置指导”中的“IRF”。

4.2 将物理端口与IRF端口绑定时失败，如何解决？

几个出现概率较高的原因为：

(1) 指定端口不支持作 IRF 物理端口。请查看配置指导确定该端口是否支持作 IRF 物理端口，选择支持作 IRF 物理端口的接口进行绑定。

(2) IRF 物理端口没有工作在最高速率下。部分产品要求 IRF 物理端口必须工作在最高速率下（拆分接口工作在拆分后的最高速率下即可）。对于有此要求的产品和端口，请更换对端端口或端口连接介质使 IRF 物理端口工作在最高速率下。

(3) IRF 物理端口的分组使用限制。

部分设备上存在端口分组，同一个 IRF 端口仅能绑定同一组的物理端口。产品对 IRF 物理端口的具体要求请参见“虚拟化技术配置指导”中的“IRF”或安装指导。

如果上述方法不能解决您的问题，请联系 H3C 技术支持。

4.3 将物理端口与IRF端口绑定时提示某些端口为一组需要将这些端口全部关闭，如何解决？

将物理端口与 IRF 端口绑定时提示某些端口为一组需要将这些端口全部关闭，输出类似如下提示（提示仅为示例，不同设备输出的提示信息可能有所区别）。

```
<Sysname> system-view
[Sysname]irf-port 1/2
[Sysname-irf-port1/2]port group interface Twenty-FiveGigE 1/0/13:1
Check failed for reason:
 Twenty-FiveGigE1/0/13:2, Twenty-FiveGigE1/0/13:3 and Twenty-FiveGigE1/0/13:4 be
long to a port group, Please shutdown all of them before changing the working mo
de.
```

某些设备上存在 IRF 物理端口按组使用限制，即一组端口必须全部作为普通业务端口或全部作为 IRF 物理端口，在这些设备上将物理端口与 IRF 端口绑定时，如果系统判断有同组端口处于 UP 状态，则不允许绑定，需要将同组端口全部配置 **shutdown** 关闭后才允许绑定。哪些端口属于同一组可以查看显示信息或者配置指导。

以如上设备显示为例，配置 IRF 物理端口的过程如下：

(1) 进入 Twenty-FiveGigE1/0/13:1、Twenty-FiveGigE1/0/13:2、Twenty-FiveGigE1/0/13:3、Twenty-FiveGigE1/0/13:4 端口组视图，执行 **shutdown** 命令关闭端口；

(2) 进入 IRF1/2 端口视图，配置端口 Twenty-FiveGigE1/0/13:1 与 IRF1/2 端口绑定；

(3) 再次进入端口 Twenty-FiveGigE1/0/13:1 视图，执行 **undo shutdown** 命令开启端口。同组端口中，其他未与 IRF 端口绑定的物理端口不允许开启。

(4) 完成全部物理端口绑定后，执行 **save** 命令保存配置。

(5) 执行 **irf-port-configuration active** 命令激活 IRF 物理端口配置。

```
[Sysname] interface range twenty-fivegige 1/0/13:1 twenty-fivegige 1/0/13:2 twenty-fivegige
1/0/13:3 twenty-fivegige 1/0/13:4
[Sysname-if-range] shutdown
[Sysname-if-range] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface twenty-fivegige 1/0/13:1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[Sysname-irf-port1/2] quit
[Sysname-Twenty-FiveGigE1/0/13:1] undo shutdown
[Sysname-Twenty-FiveGigE1/0/13:1] quit
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 5 commands and d
eletes 1 commands.
If you want to see the configuration differences, please cancel this operation,
```

```
and then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
[Sysname] irf-port-configuration active
```

此步骤仅包含 IRF 物理端口的配置过程，IRF 的全部配置过程请查看“虚拟化技术配置指导”中的“IRF”。

如果上述方法不能解决您的问题，请联系 H3C 技术支持。

4.4 使用undo shutdown命令开启端口时提示需要将一组端口全部与IRF端口绑定或全部取消绑定，如何解决？

使用 **undo shutdown** 命令开启端口时提示需要将一组端口全部与 IRF 端口绑定或全部取消绑定，输出类似如下提示（提示仅为示例，不同设备输出的提示信息可能有所区别）。

```
<Sysname> system-view
[Sysname] interface Twenty-FiveGigE 1/0/13:2
[Sysname-Twenty-FiveGigE1/0/13:2] undo shutdown
Bind all interfaces in the same group to IRF ports or cancel the bindings on all
 of them.
```

某些设备上存在 IRF 物理端口按组使用限制，即一组端口必须全部作为普通业务端口或全部作为 IRF 物理端口。在这些设备上使用 **undo shutdown** 命令开启端口时，如果系统判断有同组端口已经与 IRF 端口绑定，则不允许开启该端口，需要将该端口与 IRF 端口绑定或将同组端口全部与 IRF 端口解除绑定后才允许开启。在 IRF 端口执行 **display this** 命令可以查看已经与 IRF 端口绑定的物理端口，也可以通过配置指导查看 IRF 物理端口分组信息。

如果上述方法不能解决您的问题，请联系 H3C 技术支持。

4.5 完成IRF成员编号、IRF物理端口等配置，重启设备后没有形成IRF，是什么原因？

请确认是否进行了保存配置的操作。

盒式设备建议 IRF 的配置顺序如下：

- 进行物理端口与 IRF 端口绑定等配置；
- 执行 **save** 命令保存配置；
- 执行 **irf-port-configuration active** 命令激活 IRF 物理端口配置；
- 连接各成员设备间的 IRF 物理端口。

框式设备建议 IRF 的配置顺序如下：

- 进行物理端口与 IRF 端口绑定等配置；
- 执行 **save** 命令保存配置；
- 连接各成员设备间的 IRF 物理端口；
- 切换到 IRF 模式。

无法形成 IRF 的原因较多，忘记保存配置为容易疏忽、出现概率较高的一条。更多 IRF 无法形成的原因请查看故障处理手册。

4.6 执行irf-port-configuration active命令激活IRF物理端口的配置之后，设备提示由于XX配置不一致无法形成IRF，如何处理？

多台设备组成 IRF 时，部分涉及设备工作模式和资源使用的配置要求各成员设备配置相同，常见的有如下项目（不同产品上要求的项目和配置命令可能不同，产品的具体要求请参见“虚拟化技术配置指导”中的“IRF”）：

- 系统工作模式（通过 **system-working-mode** 命令配置）；
- 硬件资源模式（通过 **hardware-resource switch-mode** 命令配置或 **switch-mode** 命令配置）；
- 设备的聚合能力（通过 **link-aggregation capability** 命令配置）；
- 等价路由模式（通过 **ecmp mode** 命令配置）；
- 等价路由最大条数（通过 **max-ecmp-num** 命令配置）；
- 前缀大于 64 位的 IPv6 路由功能（通过 **hardware-resource routing-mode ipv6-128** 命令配置）；
- VXLAN 硬件资源模式（通过 **hardware-resource vxlan** 命令配置）。

如果设备在加入 IRF 的过程中检测到要求配置一致的项目与邻居成员设备不同，则无法加入 IRF。例如，执行 **irf-port-configuration active** 命令激活 IRF 物理端口的配置之后设备输出如下提示信息：

```
[Sysname]irf-port-configuration a
[Sysname]irf-port-configuration active
[Sysname]%Jan 14 20:53:07:484 2013 H3C STM/6/STM_LINK_UP: IRF port 2 came up.

The max-ecmp-num and switch-mode settings should be the same across devices in an IRF fabric.
The local max-ecmp-num setting is 8, and the local switch-mode setting is VXLAN. Please check
the settings on the neighbor device connected to IRF-port 2.
%Jan 14 20:53:07:864 2013 H3C STM/3/STM_SOMER_CHECK: Neighbor of IRF port 2 can't be stacked.
%Jan 14 20:53:08:088 2013 H3C STM/3/STM_LINK_DOWN: IRF port 2 went down.
```

此时，请根据提示信息修改本设备配置或其他成员设备配置，使相关配置一致。不同设备上提示信息的描述可能不同，本文以上述显示信息提示的情况为例介绍：

(1) 查看本成员设备提示信息。提示信息显示所有成员设备等价路由最大条数配置和硬件资源模式的配置需要相同。本端等价路由最大条数为 8，硬件资源模式为 VXLAN。设备检测到等价路由最大条数配置或硬件资源模式的配置与 IRF-port 2 连接的邻居成员设备不一致。

(2) 查看 IRF-port 2 连接的邻居成员设备等价路由条数和硬件资源模式。

```
[Sysname] display switch-mode status
     Switch-mode in use: NORMAL MODE(default).
     Switch-mode for next reboot: NORMAL MODE(default).
[Sysname]display max-ecmp-num
  Max-ECMP-Num in use: 8
  Max-ECMP-Num at the next reboot: 8
```

IRF-port 2 连接的邻居成员设备等价路由条数为 8，硬件资源模式为 NORMAL，硬件资源模式配置与本设备不同。

(3) 修改本设备或邻居成员设备硬件资源模式配置使二者一致。如果修改邻居成员设备配置，则需要确认 IRF 中是否还有其他成员设备，如有需要一并修改。请注意：修改后需要保存配置并重启设备，方能使配置生效。本文以修改本设备配置为例：

```
[Sysname]switch-mode ?
  0  NORMAL MODE(default)
  1  VXLAN MODE
  2  802.1BR MODE
  3  MPLS MODE
  4  MPLS-IRF MODE

[Sysname]switch-mode 0
Reboot device to make the configuration take effect.
[Sysname]
<Sysname>reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/test.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/test.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait........
```

4.7 框式交换机是否支持IRF环形连接拓扑？

对于仅支持两台设备组成 IRF 的框式交换机，不支持 IRF 环形连接拓扑。

对于最多支持四台设备组成 IRF 的框式交换机，使用三台或四台设备组建 IRF 时，可以支持环形连接拓扑。

交换机支持的 IRF 成员设备数量和连接拓扑请查看产品配套“虚拟化技术配置指导”中的“IRF”。

4.8 IRF重启后为什么有配置丢失？

常见原因有如下几种：

- IRF 重启前，修改了配置，但是没有保存。
- 在 IRF 上保存配置时，从设备正在重启，此时保存的配置文件中没有包含从设备的配置。当从设备启动完成并加入 IRF 后，无法从主设备的配置文件中恢复配置，导致从设备上的配置丢失。
- IRF 的软件版本升级后有部分软件功能不支持，相关功能的配置会丢失。
- 对于分布式交换机，如果设备长期不上电，可能会导致主控板上的 NVRAM 供电不足，NVRAM 中记录的设备启动配置文件路径信息丢失。此时，设备会以空配置的方式启动，设备上原有的

配置丢失。这种情况可以通过设备启动后查看系统时间是否准确进行判断，如果系统时间显示和之前配置的不匹配，则可以确认是主控板上 NVRAM 供电不足，请联系技术支持更换主控板上的电池。

4.9 LACP MAD检测采用的组网有何要求？

LACP MAD 适用于 IRF 使用聚合链路和上行设备或下行设备连接，组网通常要求：

- 每个成员设备都需要连接到中间设备。
- 成员设备连接中间设备的链路务必加入动态聚合组。
- 中间设备需要支持扩展 LACP 报文，即中间设备需要采用 H3C 设备。

4.10 BFD MAD检测VLAN有何限制及注意事项？

BFD MAD 检测 VLAN 通常有如下使用限制和注意事项：

- 不允许在 Vlan-interface1 接口上开启 BFD MAD 检测功能。
- 如果使用中间设备，需要进行如下配置：
  - 在 IRF 设备和中间设备上，创建专用于 BFD MAD 检测的 VLAN。
  - 在 IRF 设备和中间设备上，将用于 BFD MAD 检测的物理接口添加到 BFD MAD 检测专用 VLAN 中。
  - 在 IRF 设备上，创建 BFD MAD 检测 VLAN 的 VLAN 接口。
- 如果网络中存在多个 IRF，在配置 BFD MAD 时，各 IRF 必须使用不同的 VLAN 作为 BFD MAD 检测专用 VLAN。
- 用于 BFD MAD 检测的 VLAN 接口对应的 VLAN 中只能包含 BFD MAD 检测链路上的端口，请不要将其它端口加入该 VLAN。当某个业务端口需要使用 **port trunk permit vlan all** 命令允许所有 VLAN 通过时，请使用 **undo port trunk permit** 命令将用于 BFD MAD 的 VLAN 排除。

 注意

如下产品创建 VSI 虚接口后，部分 VLAN 接口不能作为用于 BFD MAD 检测的 VLAN 接口：

- 对于 S5560X-EI、S5500V2-EI、ES5500C、MS4520V2 系列交换机，编号为 3581~4092 的 VLAN 接口不能作为用于 BFD MAD 检测的 VLAN 接口。
- 对于 S6520X-SI、S6520-SI、MS4600 系列交换机，编号为 3581~4092 的 VLAN 接口不能作为用于 BFD MAD 检测的 VLAN 接口。
- 对于 S6520X-EI 系列交换机，编号为 3069~4092 的 VLAN 接口不能作为用于 BFD MAD 检测的 VLAN 接口。
- 对于 S6520X-HI、S5560X-HI、S5000-EI 系列交换机，编号为 2045~4092 的 VLAN 接口不能作为用于 BFD MAD 检测的 VLAN 接口。
- 对于 S6813&S6812 系列交换机，编号为 2045~4092 的 VLAN 接口不能作为用于 BFD MAD 检测的 VLAN 接口。

- IRF 设备使用 BFD MAD 检测功能时，请务必注意：开启 BFD 检测功能的 VLAN 接口只能专用于 BFD 检测，不允许运行其他业务。
  - 开启 BFD 检测功能的 VLAN 接口只能配置 mad bfd enable 和 mad ip address 命令。如果用户配置了其它业务，可能会影响该业务以及 BFD 检测功能的运行。
  - BFD MAD 检测功能与生成树功能互斥，在开启了 BFD MAD 检测功能的 VLAN 接口对应 VLAN 内的端口上，请不要开启生成树协议。

5 MAC 地址表

5.1 为什么设备无法转发源MAC地址是VLAN接口的MAC地址的流量？

报文入接口与静态 MAC 地址表项匹配检查功能处于开启状态时，设备会将接收到的报文的源 MAC 地址与静态 MAC 地址表项进行匹配。如果存在 MAC 地址与报文的源 MAC 相同的表项，但表项的出接口不是接收报文的端口，设备会丢弃该报文。对于源 MAC 地址是 VLAN 接口的 MAC 地址的流量，需要在对应 VLAN 所在的二层接口上关闭报文入接口与静态 MAC 地址表项匹配检查功能才能转发该流量。请客户按以下配置步骤在对应 VLAN 所在的二层接口上关闭该功能。

配置步骤：

(1) 进入系统视图。

system-view

(2) 进入二层以太网接口视图。

interface *interface-type interface-number*

(3) 在接口上关闭报文入接口与静态 MAC 地址表项匹配检查功能。

undo mac-address static source-check enable

缺省情况下，接口上的报文入接口与静态 MAC 地址表项匹配检查功能处于开启状态。

说明

对于不支持 **undo mac-address static source-check enable** 命令的产品（如 S12500X-AF/S12500F-AF/S6890），则不涉及此问题。

6 接口与聚合

6.1 电口或光口互连是否应该设置强制双工和速率？

电口具有很好的自协商能力，一般都能自协商成功，所以不要设置强制双工和速率。

光口自协商能力比电口稍差，极少部分光口会出现自协商不成功的现象，所以大部分光口在开局时候都被设置强制双工和速率。这样不加分析的设置强制双工和速率，会掩盖一些问题，需要注意查看端口信息中有没有错包。是否光衰过大，必要时要用光功率仪进行测试，确实是否需要更换光纤等。

电口或光口的协商机制可以遵循以下 2 个原则：

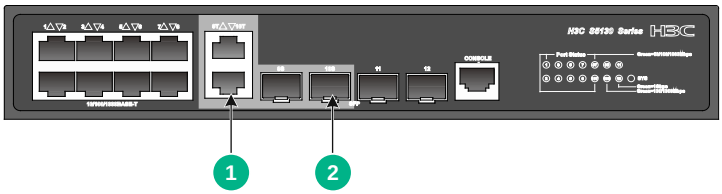
- 除非有特别的理由，双方均采用自协商方式。如果端口没有 UP，可以查看安装手册确认端口有无需要强制速率和双工的要求，如有相关描述，请按要求配置。
- 双方方式必须一致，要么双方都是自协商方式，要么双方都设置强制双工和速率，不允许一端自协商，一端设置强制双工和速率，也不允许只设置双工方式而不设置速率，同样也不允许只设置速率而不设置双工方式。

6.2 Combo口为什么不UP？

Combo 接口是一个逻辑接口，一个 Combo 接口物理上对应设备面板上一个电口和一个光口。电口与其对应的光口是光电复用关系，两者不能同时工作（当激活其中的一个接口时，另一个接口就自动处于禁用状态），用户可根据组网需求选择使用电口或光口。

- 请根据设备面板上的标识了解设备 Combo 接口的编号。例如，下图中设备前面板上的最后 2 个 10/100/1000BASE-T 自适应以太网端口和前 2 个 SFP 口（端口编号为 9、10）组成了 Combo 接口。

图6-1 前面板 Combo 接口示意图



(1): 10/100/1000BASE-T自适应以太网端口	(2): SFP口

- 通过 **display interface** 命令查看该 Combo 接口信息，如果显示信息中包含“Media type is twisted pair”，则表示电口处于激活状态，否则，则表示光口处于激活状态。
- 使用 **combo enable** { **copper** | **fiber** }命令激活 Combo 接口中的电口或者光口。

6.3 聚合接口和成员接口的配置有哪些要求？

接口加入聚合组前，有以下两种情况，不同产品要求不同，请以设备实际情况为准：

- 接口加入聚合组前，如果接口上的属性类配置和聚合接口不同，则该接口不能加入聚合组。
- 接口加入聚合组前，如果接口上的属性类配置和聚合接口不同，则该接口可以加入聚合组，但会处于非选中状态。

接口加入聚合组后，有以下两种情况，不同产品要求不同，请以设备实际情况为准：

- 接口加入聚合组后，不能修改接口的属性类配置。
- 接口加入聚合组后，可以修改接口的属性类配置，但会导致接口变为非选中状态。

处于非选中状态下的成员端口不能参与数据的转发，有关成员端口状态的详细介绍请参见各产品“二层技术—以太网交换配置指导”中的“以太网链路聚合”。

属性类配置包含的配置内容如表 6-1 所示。

表6-1 属性类配置的内容

配置项	内容
端口隔离	端口是否加入隔离组、端口所属的端口隔离组
QinQ配置	端口的QinQ功能开启/关闭状态、VLAN Tag的TPID值、VLAN透传。
VLAN映射	端口上配置的各种VLAN映射关系。
VLAN配置	端口上允许通过的VLAN、端口缺省VLAN、端口的链路类型（即Trunk、Hybrid、Access类型）、端口的工作模式（即promiscuous、trunk promiscuous、host、trunk secondary模式）、基于IP子网的VLAN配置、基于协议的VLAN配置、VLAN报文是否带Tag配置。

接口加入聚合组时，还存在如下限制：

- 不要将镜像反射端口加入聚合组。
- PEX 二层聚合组的成员端口必须是同一 PEX 上的接口或同一 PEX 组中同一层的不同 PEX 上的接口。同时必须使用同系列的 PEX 设备进行链路聚合。有关 PEX 的详细介绍请参见各产品“虚拟化技术配置指导”。

6.4 聚合链路两端如何选择聚合模式？

链路聚合分为静态聚合和动态聚合两种模式，聚合链路的两端应配置相同的聚合模式。对于不同模式的聚合组，其选中端口存在如下限制：

- 对于静态聚合模式，用户需要保证在同一链路两端端口的选中/非选中状态的一致性，否则聚合功能无法正常使用。
- 对于动态聚合模式：
  - 聚合链路两端的设备会自动协商同一链路两端的端口在各自聚合组内的选中/非选中状态，用户只需保证本端聚合在一起的端口的对端也同样聚合在一起，聚合功能即可正常使用。
  - 如果聚合链路一端使用半自动动态聚合方式，则链路另外一端使用手工动态聚合方式。

6.5 如何处理链路聚合负载分担不均匀的问题？

针对不同的业务场景，对应的负载分担方式也是不同的。当出现链路聚合负载分担不均匀的问题时，可以进行如下尝试改善负载分担不均的问题：

- 调整负载分担类型

  可通过系统视图下的 **link-aggregation global load-sharing mode** 命令调整全局的负载分担类型；部分交换机还可以通过聚合接口视图下的 **link-aggregation load-sharing mode** 命令调整聚合接口的负载分担类型。具体支持的负载分担类型以产品实际情况为准。

  针对不同业务流量，调整负载分担类型：
  - 对于 IP 报文，可以基于源 IP 地址或目的 IP 地址进行负载分担。
  - 对于二层报文，可以基于源 MAC 地址或目的 MAC 地址进行负载分担。
- 关闭本地优先转发功能

跨 IRF 成员设备聚合场景中，可以使用 **undo link-aggregation load-sharing mode local-first** 命令关闭本地优先转发功能。

需要注意，跨 IRF 成员设备流量不能过大，否则可能影响 IRF 系统稳定。

6.6 使用链路聚合如何与服务器互通？

与服务器对接时，需要在聚合接口下使用 **lacp edge-port** 命令将聚合接口配置为聚合边缘接口。该场景下聚合接口需要工作在动态聚合模式。

在服务器未配置动态聚合模式时，该服务器与网络设备间的链路可以形成备份，使该聚合组内的所有成员端口都作为普通物理口转发报文，从而保证终端设备与网络设备间的多条链路可以相互备份，增加可靠性。在服务器完成动态聚合模式配置时，其聚合成员端口正常发送 LACP 报文后，网络设备上符合选中条件的聚合成员端口会自动被选中，从而使聚合链路恢复正常工作。

7 DRNI

7.1 DRNI组网中管理IP地址互访不通如何处理？

DRNI 组网中需要进行以下部署：

- 需要在系统视图下或 IPP 口下配置 **undo mac-address static source-check enable** 命令，关闭报文入接口与静态 MAC 地址表项匹配检查功能。
- DR 接口仅允许业务流量所在 VLAN 通过。
- DRNI 主备设备均与上行设备连接，实现冗余备份。

7.2 DRNI+VRRP组网中，单挂接入DR设备时，如何避免同一ICMP报文被DR主设备收到两次？

在 DRNI+VRRP 组网场景中，需要 DR 设备上任意一个 DR 接口允许特定的 VLAN 通过，该特定 VLAN 为配置 VRID 的 VLAN 接口对应的 VLAN。

8 VLAN

8.1 为什么部分VLAN无法通过Trunk端口？

部分 VLAN 无法通过 Trunk 端口，可能是用户未将相应的 VLAN 加入到 Trunk 端口。此外，本端设备 Trunk 端口的缺省 VLAN ID 和相连的对端设备的 Trunk 端口的缺省 VLAN ID 必须一致，否则报文将不能转发。出现该问题时，可以通过 **display vlan** 命令来查看相应的 VLAN 是否加入了 Trunk 端口。若未加入，可以在接口视图下通过 **port trunk permit vlan** 命令设置相应的 VLAN 加入 Trunk 口，同时通过 **port trunk pvid** 命令正确配置 Trunk 端口的 PVID。

8.2 如何正确配置允许指定VLAN或全部VLAN通过Trunk端口？

基于 Trunk 端口的 VLAN 只能在接口视图下配置，正确配置步骤如下：

(1) 进入系统视图。

system-view

(2) 进入接口视图。

- 进入二层以太网接口视图。

  interface *interface-type interface-number*

- 进入二层聚合接口视图。

  interface bridge-aggregation *interface-number*

(3) 配置端口的链路类型为 Trunk 类型。

port link-type trunk

缺省情况下，端口的链路类型为 Access 类型。

(4) 允许指定的 VLAN 或全部 VLAN 通过当前 Trunk 端口。

port trunk permit vlan { *vlan-id-list* | **all** }

缺省情况下，Trunk 端口只允许 VLAN 1 的报文通过。

(5) 配置 Trunk 端口的 PVID。

port trunk pvid vlan *vlan-id*

缺省情况下，Trunk 端口的 PVID 为 VLAN 1。

建议用户谨慎使用 **port trunk permit vlan all** 命令，以防止未授权 VLAN 的用户通过该端口访问受限资源。

8.3 为什么设备获取不到IP Phone的MAC地址？

设备获取不到 IP Phone 的 MAC 地址，可能是该话机不在设备缺省的 OUI 地址中，请客户按以下配置步骤预先配置话机的 OUI 地址，然后执行 **display voice-vlan mac-address** 命令查看，确保表项中存在该话机。

配置步骤：

(1) 进入系统视图。

system-view

(2) 配置 Voice VLAN 识别的 OUI 地址。

voice-vlan mac-address *oui* **mask** *oui-mask* [**description** *text*]

Voice VLAN 启动后将有缺省的 OUI 地址。有关缺省 OUI 地址的详细介绍，请参见各产品“二层技术-以太网交换配置指导”中的“VLAN”。

在配置 Voice VLAN 的 OUI 时：

- OUI 地址不能是广播地址或者组播地址，也不能是全 0 的地址。
- OUI 地址是 **mac-address** 和 **oui-mask** 参数相与的结果。
- 设备最多支持配置 OUI 地址个数以具体产品实际规格为准。

8.4 如何限制广播域的范围？

可以通过划分设备所属 VLAN，将广播报文限制在同一个 VLAN 内，有效地限制广播域的范围。交换机可支持的 VLAN 划分方式包括：基于端口、MAC 地址、IP 子网、协议方式来划分 VLAN。不同设备支持的具体情况，请参考各系列交换机“二层技术-以太网交换配置指导”中的“VLAN 配置”部分。

8.5 错误配置接口链路类型导致无法正常通信怎么办？

首先要正确区分三种端口的链路类型：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。一般用于和不能识别 VLAN Tag 的用户终端设备相连，或者不需要区分不同 VLAN 成员时使用。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。

然后根据接口转发报文时是否需要携带 VLAN tag 或是否允许转发多个 VLAN 的报文，使用 **port link-type** 命令将错误的接口类型切换为正确的接口类型。

切换接口类型应注意：

- Trunk 端口不能直接切换为 Hybrid 端口，只能先将 Trunk 端口配置为 Access 端口，再配置为 Hybrid 端口。
- Hybrid 端口不能直接切换为 Trunk 端口，只能先将 Hybrid 端口配置为 Access 端口，再配置为 Trunk 端口。

8.6 在Voice VLAN中出现除语音数据之外的业务数据丢失情况怎么办？

在 Voice VLAN 中发生业务数据丢失情况时，请执行 **undo voice-vlan security enable** 命令关闭 Voice VLAN 的安全模式。在安全模式下，设备将对每一个要进入 Voice VLAN 传输的报文进行源 MAC 地址匹配检查，对于不能匹配 OUI 地址的报文，将其丢弃。因此建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。如确有此需要，请确认 Voice VLAN 的安全模式已关闭，否则业务数据会被丢弃。

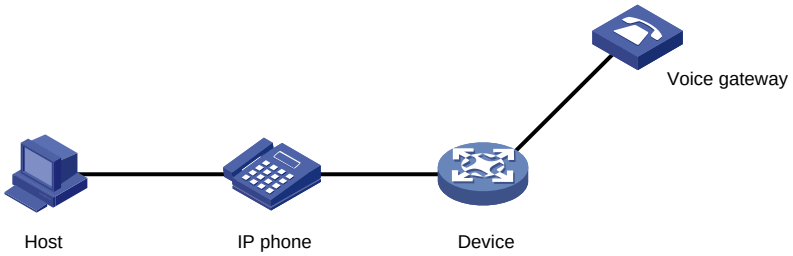
8.7 如何选择端口的Voice VLAN工作模式？

根据端口加入 Voice VLAN 的不同方式，可以将 Voice VLAN 的工作模式分为自动模式和手动模式，选择方式如下。

1. 自动模式

自动模式适用于主机和 IP 电话串联接入（端口同时传输语音数据和普通业务数据）的组网方式，如图 8-1 所示。

图8-1 主机与 IP 电话串联接入组网图



2. 手动模式

手动模式适用于 IP 电话单独接入（端口仅传输语音报文）的组网方式，如图 8-2 所示。该组网方式可以使该端口专用于传输语音数据，最大限度避免业务数据对语音数据传输的影响。单独接入适用于 IP 电话发出 Untagged 语音报文的情况，不同类型端口支持 Untagged 语音数据配置要求，如表 8-1 所示。

图8-2 IP 电话单独接入组网图

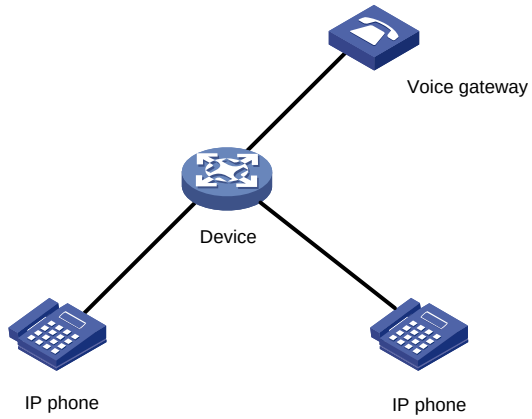


表8-1 不同类型端口支持 Untagged 语音数据配置要求

Voice VLAN 工作模式	端口类型	是否支持 Untagged 语音数据	配置要求
手动模式	Access	支持	端口加入Voice VLAN
	Trunk	支持	PVID必须为Voice VLAN，且接入端口允许PVID通过
	Hybrid	支持	PVID必须为Voice VLAN，且允许PVID的报文不带VLAN Tag通过

9 生成树

9.1 什么情况下需要配置生成树边缘端口？

与交换机连接的用户侧设备（如服务器等）无需运行生成树协议。若交换机上与这些设备相连的端口使能了生成树协议，则该端口的物理状态可能频繁震荡，在 Up/Down 上不停跳转；或生成树拓扑变化时端口角色需要计算，导致该端口一段时间后才能进入转发状态等问题；这对一些需要高链路稳定性或低转发延迟的业务是不可接受的。为了避免上述问题，需要将与用户侧设备连接的端口配置为边缘端口。边缘端口状态变为 Up 后可以快速进入转发状态，并且不会发送 TC 报文，也不会对其他运行了生成树协议的网络造成影响。

9.2 在生成树拓扑中，不同的设备可以配置不同的生成树工作模式吗？

H3C 设备在运行生成树协议时，不同的设备间的不同生成树工作模式可以互相兼容。其中：

- MSTP 模式可以兼容 RSTP 模式和 STP 模式，RSTP 模式可以兼容 STP 模式。
- 对于 Access 端口，PVST 模式在任意 VLAN 中都能与其他模式互相兼容；对于 Trunk 端口或 Hybrid 端口，PVST 模式仅在缺省 VLAN 中能与其他模式互相兼容。

若设备的对端设备为其他产商设备，建议对端设备与 H3C 设备使用同一种工作模式，以避免因产商差异而出现的不兼容问题。

9.3 开启生成树协议后，可通过哪些方法维持网络拓扑的稳定？

在使能了生成树协议的网络中，生成树计算后阻塞的部分二层通路，可能导致下行终端获取不到地址或获取地址慢、部分业务流量不通等问题，此时可通过下列方法尝试维护生成树的拓扑稳定，以保障正常的二层通路：

(1) 根桥保护

在一些组网环境中，用户指定的根桥设备因为未进行过根桥保护的相关配置，导致新设备加入组网时，成为新的根桥，引发生成树拓扑重新收敛和网络的震荡。

可通过下列方法避免其他设备的抢根：

- 设备的优先级参与生成树计算，数值越小表示优先级越高，用户可配置 **stp priority** 命令，直接将指定的设备优先级设置为 0 或值较小的优先级，以达到指定设备成为生成树根桥的目的。
- 通过配置 **stp root primary** 命令，用户可指定设备为生成树的根桥。需要注意的是，当设备一旦被配置为根桥之后，便不能再修改该设备的优先级。
- 设备被选举为根桥后，开启根保护功能。在接口视图下配置 **stp root-protection** 命令后，此接口在所有 MSTI 上的端口角色只能为指定端口。一旦该端口收到某 MSTI 优先级更高的 BPDU，立即将该 MSTI 端口设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在 2 倍的 Forward Delay 时间（缺省情况下 Forward Delay 时间为 15 秒）内没有收到更优的 BPDU 时，端口会恢复原来的正常状态。根保护功能，可以避免因错误配置或恶性攻击导致的生成树拓扑不合法的变动。

(2) 配置边缘端口和 BPDU 保护

对于接入层设备，接入端口一般直接与用户终端（如 PC）或文件服务器相连，此时接入端口应被设置为边缘端口以实现这些端口的快速迁移。正常情况下，接入端口不应该与用户终端交互生成树协议的 BPDU 报文，如果收到 BPDU 报文可能会引起网络拓扑结构的变化，造成网路震荡。

生成树协议提供了 BPDU 保护功能来解决这类问题：在全局或接口视图下配置 **stp bpdu-protection** 命令后，如果边缘端口收到了 BPDU，系统就将这些端口关闭，同时通知用户这些端口已被生成树协议关闭。被关闭的端口在经过一定时间间隔之后将被重新激活，这个时间间隔可通过 **shutdown-interval** 命令配置。

(3) 配置环路保护

下游设备依靠不断接收上游设备发送的 BPDU 来维持根端口和其他阻塞端口的状态。如果出现了链路拥塞或者单项链路故障，这些端口会收不到上游设备的 BPDU，此时下游设备会重新选择端口角色，导致下游设备的根端口转变为指定端口，而阻塞端口会迁移到转发状态，导致交换网络中产生环路。

在下游设备的根端口和替换端口上通过 **stp loop-protection** 命令配置环路保护功能后，可以抑制上述环路的产生。在开启了环路保护功能的端口上，其所有 MSTI 的初始状态均为 Discarding 状态：如果该端口收到了 BPDU，这些 MSTI 可以进行正常的状态迁移；否则，这些 MSTI 将一直处于 Discarding 状态以避免环路的产生。

需要注意的是，无需在与用户终端相连的端口上配置环路保护功能，否则该端口会因一直处于 Discarding 状态而无法正常转发用户报文。

(4) 配置防 TC-BPDU 攻击保护功能

在遭受到 TC-BPDU 恶意攻击行为时，设备会频繁地刷新转发地址表项。此类攻击给设备带来了很大负担，随时威胁着网络的稳定性。此时可以开启防 TC-BPDU 攻击保护功能，以避免频繁地刷新转发地址表项。该功能的描述如下：

- 在系统视图下执行 **stp tc-protection** 命令，可以开启防 TC-BPDU 攻击保护功能。
- 在系统视图下执行 **stp tc-protection threshold** *number* 命令，可以配置在单位时间（固定为十秒）内，设备收到 TC-BPDU 后立即刷新转发地址表项的最高次数。
- 开启本功能后，如果设备在单位时间（固定为十秒）内收到 TC-BPDU 的次数大于 *number* 次，那么该设备在这段时间之内将只进行 *number* 次刷新转发地址表项的操作，而对于超出 *number* 次的那些 TC-BPDU，设备会在这段时间过后再统一进行一次地址表项刷新的操作。

9.4 设备频繁收到TC报文时该如何操作？

设备收到 TC 报文后会进行如下两个操作：

(1) TC 报文所在的实例触发 MAC 地址删除及重新学习。

在 MAC 地址删除重新学习过程中，会产生未知单播流量导致网络中流量泛洪。

(2) TC 报文所在的实例触发 ARP 探测。

ARP 探测会导致 ARP 广播报文在网络中泛洪，增加设备负担。

如果设备频繁收到 TC 报文，就会频繁进行如上两种操作，会对网络中的设备产生冲击，因此要尽量避免这种情况。一般可按照如下步骤进行排查解决：

(1) 确定网络中频繁产生 TC 报文的设备。

分析设备日志信息，确定是哪个端口频繁收到 TC 报文。确定端口后，进一步排查与该端口对接设备的日志信息，继续分析是该设备产生的还是其下一级设备产生的 TC 报文。采用逐级排查的方式确认是哪台设备产生的 TC 报文。

注意

PVST 模式下端口收到 TC 报文后，默认不打印日志信息。可通过配置 **stp log enable tc** 命令配置在 PVST 模式下设备检测或接收到 TC 报文时打印日志信息功能。

(2) 确定设备频繁产生 TC 报文的原因。

设备开启生成树协议的情况下，如果端口 UP/DOWN，则会产生 TC 报文。即如果存在端口频繁 UP/DOWN 的情况，便会频繁产生 TC 报文。

(3) 消除 TC 报文。

如果设备上存在端口频繁 UP/DOWN，则分析定位端口 UP/DOWN 的原因并解决，即可消除设备频繁产生 TC 报文的情况。

如果暂时无法排查出频繁产生 TC 报文的原因或无法解决端口 UP/DOWN 问题，可以按照如下方式进行临时规避：

(1) 如果该端口对接的是终端设备，可配置端口为边缘端口（通过 **stp edged-port** 命令配置）。端口配置为边缘端口后，该端口 UP/DOWN 时，不再产生 TC 报文。

(2) 如果该端口对接的是非终端设备，可通过如下两种方式进行临时规避：

- 开启 TC-BPDU 传播限制功能（通过 **stp tc-restriction** 命令开启，缺省情况下处于关闭状态）。当开启了端口的 TC-BPDU 传播限制功能之后，该端口将不再向其它端口传播 TC-BPDU，也不删除本机的转发地址表项。
- 开启防 TC-BPDU 攻击保护功能（通过 **stp tc-protection** 命令开启，缺省情况下处于开启状态），并通过配置收到 TC-BPDU 后立即刷新转发地址表项的最高次数来控制刷新频率（通过 **stp tc-protection threshold** 命令配置，缺省情况为在单位时间（固定为十秒）内，设备收到 TC-BPDU 后立即刷新转发地址表项的最高次数为 6）。

9.5 开启生成树协议后，如何避免对其他网络造成不良影响？

与其他网络相连的边缘设备开启生成树功能后，会通过相连的端口发送 BPDU 报文至外部，引发其他网络重新计算生成树，造成网络震荡。此时通过配置 BPDU 过滤功能，可以使端口不再发送 BPDU 报文，以免对其他网络造成不良影响。请客户按以下配置步骤开启边缘端口的 BPDU 过滤功能。

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置端口的 BPDU 过滤功能。

stp port bpdu-filter { disable | enable }

10 环路检测

10.1 如何选择环路检测时间间隔？

设备以一定的时间间隔发送环路检测报文来确定是否存在环路，这个时间间隔就称为环路检测的时间间隔。同时这个时间间隔决定了环路检测在 Block 模式和 No-learning 模式下的端口恢复正常转发状态的速度：时间间隔越小，端口的恢复速度越快，环路检测的灵敏度越高，占用设备的系统资源越多；时间间隔越大，端口的恢复速度越慢，环路检测的灵敏度越低，占用设备的系统资源越小。请用户根据设备实际情况及组网的二层防环需求，灵活配置环路检测时间间隔。

同时需要注意的是，环路检测在 Shutdown 模式下，被关闭的端口的恢复不受环路检测时间间隔的影响，而是在 **shutdown-interval** 命令配置的端口状态检测定时器超时后，端口自动恢复为 UP 状态。

10.2 环路检测和生成树功能可以同时配置吗？

不建议同时配置，因为环路检测和生成树都具有二层防环功能，如果两者同时配置，可能其中一者在另一者计算出环路之前就已经消除了环路，造成环路检测功能不生效或生成树功能不生效等问题。

11 镜像

11.1 希望为本地端口镜像组配置多于一个目的端口，但部分设备不支持加入第二个目的端口怎么处理？

部分设备上，本地端口镜像组支持配置多个目的端口。

部分设备上，本地端口镜像组不支持配置多个目的端口，为镜像组配置第二个目的接口时输出类似如下提示信息：

```
<Sysname> system-view
[Sysname] mirroring-group 1 monitor-port HundredGigE 1/0/26
Mirroring group 1 already has a monitor port.
```

对于本地端口镜像组不支持配置多个目的接口的设备，可以使用远程镜像 VLAN 实现本地镜像组支持多个目的端口。

该方式利用二层远程端口镜像中镜像报文在远程镜像 VLAN 中广播发送的原理实现。具体实现方式为：

(1) 在本地设备上创建远程源镜像组、远程镜像 VLAN 和反射端口，并将本设备上连接监测设备的多个端口加入该 VLAN。

(2) 镜像报文在远程镜像 VLAN 中广播时即可从这些端口中发送出去，实现将镜像报文发送到多个目的端口。

具体配置方式请参见“网络管理和监控配置指导”中的“镜像”。

11.2 配置二层远程端口镜像后，为什么与镜像无关的端口有异常的流量增加？

查看这些端口是否加入到了远程镜像 VLAN 中，如是，请将与镜像无关的端口从远程镜像 VLAN 中删除。远程镜像 VLAN 需要专用，不要用作其他用途，也不要将镜像无关端口加入远程镜像 VLAN。

11.3 配置镜像组的源端口失败，可能的原因有哪些？

最常见的原因为接口类型支持情况限制和一个接口允许加入的聚合组数量限制。

请确认该接口是否支持配置为镜像源接口，特别是聚合接口、VLAN 接口等全局接口。VLAN 接口一般不支持作为镜像源接口，请配置 VLAN 中的物理端口作为镜像源接口。聚合接口是否支持作为镜像源接口与设备型号有关，请查询产品“网络管理和监控配置指导”和“网络管理和监控命令参考”中的“镜像”。

一个接口可以作为镜像源加入的镜像组数目受设备支持情况限制：

- 部分设备上：一个接口仅支持作为一个镜像组的源端口，将该接口配置为第二个镜像组的源接口时输出类似如下提示信息，表示该接口已经配置为其他镜像组的源端口：

  ```
  <Sysname> system-view
  [sysname] mirroring-group 2 mirroring-port ten-gigabitethernet 1/0/1 both
  ten-gigabitethernet 1/0/1 is a mirroring port of mirroring group 1.
  ```

- 部分设备上：一个接口作为单向源端口最多可以加入四个镜像组，作为双向源端口最多可以加入两个镜像组，或者以一个双向源端口和两个单向源端口的形式加入三个镜像组。请查看接口作为镜像源端口的配置是否已超过数量限制。

镜像的配置较复杂，如果上述方法不能解决您的问题请联系技术支持。

11.4 为什么配置远程镜像VLAN的VLAN接口可能导致镜像功能异常？

如果远程镜像 VLAN 配置了对应的 VLAN 接口，当镜像报文的目的 MAC 地址正好是 VLAN 接口的 MAC 地址时，报文只进行三层转发，不会从镜像目的端口发出。建议不要配置远程镜像 VLAN 的 VLAN 接口。

12 DHCP

12.1 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**] }

需要注意的是，配置静态绑定时，必须确保绑定的 MAC 地址与实际用户的 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。）。

12.2 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，则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 地址和其他参数分配会失败。

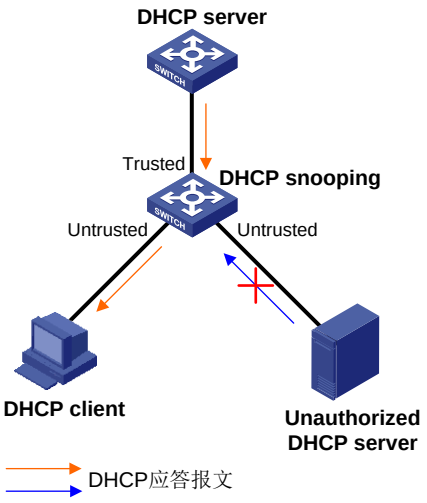
12.3 地址池IP网段范围规划小了会发生什么？

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。

12.4 配置DHCP Snooping之后，下挂用户无法获取IP地址

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。如图 12-1，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。

图12-1 信任端口和非信任端口



12.5 私网客户端申请IP地址时，作为DHCP服务器的V5设备和V7设备配置上有何不同？

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。但当 V7 设备作为 DHCP 服务器时，需要在相应地址池中配置绑定对应的 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，原因是 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相应的 VPN 私网，这样服务器就可以更好的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。

12.6 配置DHCP服务器或DHCP中继生效的前提是什么？

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。

12.7 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（例如 IP Source Guard）打算利用这些表项信息，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，不同产品系列支持开启 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。

12.8 重新指定地址池动态分配的IP地址范围时，应该注意什么？

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。

12.9 DHCP Snooping的信任端口和非信任端口设置在什么位置上？

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 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。

12.10 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得固定 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。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> system-view
[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
```

如果网络中的设备（如网关、FTP 服务器）已占用了 DHCP 服务器的地址池中的 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。请在作为 DHCP 服务器的设备的系统视图下，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 for**bidden-ip** 命令配置地址池中不参与自动分配的 IP 地址。

12.11 为什么在DHCP snooping组网下，DHCP服务器的部分地址无法分配？

DHCP Snooping 会记录客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息，并生成绑定表。一些安全特性会利用此绑定表实现相应的安全功能，如 IP Source Guard。

当 DHCP Snooping 设备上已经存在绑定表，且有 MAC 地址相同的客户端上线申请 IP 地址时，由于相关安全特性，设备无法区分是合法用户还是非法用户仿冒合法用户，所以 DHCP Snooping 设备不会修改已有的绑定表，从而导致客户端无法获得 IP 地址。可以通过删除 DHCP Snooping 设备上的绑定表解决。

13 IP 业务

13.1 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 均配置了缺省的管理 IP 地址。用户通过设备铭牌标签上打印的管理 IP 信息，可以获取该地址，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。请管理员通过 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。

13.2 为什么会出现网页打不开，但是能Ping通对方IP地址的情况？

对方的 IP 地址能够 Ping 通，说明设备之间的路由可达且链路是连通的，报文能够正常收发。那么这时候出现网页打不开或者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 1460）。

13.3 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。

13.4 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：

- 无法 Ping 通其他设备或无法被其他设备 Ping 通
- 无法登录 Web 管理界面或登录后闪退
- Telnet 连接设备时断时连
- 使用 FTP、TFTP 等方式传输文件时异常断开

13.5 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；如果不一致，则有可能是 IP 地址问题，需要进行第(2)、(3)步的排查。

(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。例如局域网内有其他网络设备的 IP 地址与设备或网关的 IP 地址冲突的情况，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) 当以上原因都不存在时，可以在 Ping 报文沿途的设备上通过抓包工具和流量统计等手段定位丢包的位置，从而进一步确定故障原因。

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

- 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。

13.7 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 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 接口 10 配置 IP 地址 192.168.1.2/24 为例：

创建 VLAN 10。

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

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
[Switch-GigabitEthernet1/0/1] quit
```

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
```

13.8 配置静态ARP表项时需要注意哪些地方？

- 确保静态 ARP 表项的 IP 地址和 MAC 地址是正确的对应关系。
- 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。
- 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。

14 接入认证

14.1 接入用户认证时，按照什么顺序选择认证域？

接入用户认证时，设备将按照如下先后顺序为其选择认证域：

(1) 接入模块指定的认证域：

- 对于 802.1X 认证用户，是指通过 **dot1x mandatory-domain** 命令，在端口上指定的 802.1X 用户使用的强制认证域；
- 对于 MAC 地址认证用户，是指通过 **mac-authentication domain** 命令，在端口上或全局指定的 MAC 地址认证域，其中端口上指定的认证域优先级高于全局指定的认证域。
- 对于 Portal 地址认证用户，是指通过 **portal domain** 或 **portal ipv6 domain** 命令在端口上指定的 IPv4 Portal 用户或 IPv6 Portal 用户的认证域；

(2) 用户名“*userid@domain-name*”中携带的 ISP 域“*domain-name*”；

(3) 设备系统缺省的 ISP 域（通过 **display domain** 命令的 Default domain name 可查看）

如果根据以上原则决定的认证域在设备上不存在，但设备上通过 **domain if-unknown** 命令为未知域名的用户指定了 ISP 域，则最终使用该指定的 ISP 域认证，否则，用户将无法认证。

14.2 如何修改或删除缺省的ISP域？

修改缺省 ISP 域的方法为：

(1) 执行命令 **display domain**，并通过“Default domain name”字段的显示信息查看当前的缺省 ISP 域；

(2) 通过 **domain** *isp-name* 命令，进入当前缺省的 ISP 域视图；使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域。

(3) 通过 **domain** *isp-name* 命令，创建新的 ISP 域，并进入其视图；使用命令 **domain default enable** 将新创建的 ISP 域设置为缺省的 ISP 域。

删除缺省 ISP 域，需要注意的是：

- 一个 ISP 域被配置为缺省的 ISP 域后，将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 系统缺省存在的 system 域只能被修改，不能被删除。

14.3 本地用户没有配置服务类型会导致认证失败吗？常用服务类型有哪些？

AAA 支持的本地认证方式是指：认证过程在接入设备上完成。这时用户信息（包括用户名、密码和服务类型等各种属性）也需要配置在接入设备上，我们称之为配置本地用户。配置本地用户包括创建一个本地用户并进入本地用户视图，然后在本地用户视图下配置密码和相应的用户属性。

服务类型是指用户可使用的网络服务类型，该属性是本地认证的检测项，如果没有用户可以使用的服务类型，则该用户无法通过认证。

缺省情况下，本地用户不能使用任何服务类型。在本地用户视图下，通过 **service-type** 命令设置用户可以使用的服务类型，多次执行该命令，可以设置用户使用多种服务类型。常见的服务类型包括：

- **ftp**：指定用户可以使用 FTP 服务。
- **http**：指定用户可以使用 HTTP 服务。
- **https**：指定用户可以使用 HTTPS 服务。
- **lan-access**：指定用户可以使用 lan-access 服务。主要指以太网接入，比如用户可以通过 802.1X 认证、MAC 地址认证接入。
- **portal**：指定用户可以使用 Portal 服务。
- **ssh**：指定用户可以使用 SSH 服务。
- **telnet**：指定用户可以使用 Telnet 服务。
- **terminal**：指定用户可以使用 terminal 服务（即从 Console 口登录）。

14.4 RADIUS认证时为什么需要配置nas-ip？

RADIUS服务器通过IP地址来标识接入设备，并根据收到的RADIUS报文的源IP地址（即NAS-IP）是否与服务器所管理的接入设备的IP地址匹配，来决定是否处理来自该接入设备的认证或计费请求。

为保证认证和计费报文可被服务器正常接收并处理，接入设备上发送RADIUS报文使用的源IP地址必须与RADIUS服务器上指定的接入设备的IP地址保持一致。

缺省情况下，未指定发送RADIUS报文使用的源IP地址，设备将使用到达RADIUS服务器的路由出接口的主IPv4地址或IPv6地址作为发送RADIUS报文的源IP地址。如果接入设备上发送RADIUS报文使用的源IP地址与RADIUS服务器上指定的接入设备的IP地址不一致，可采用**nas-ip**命令进行配置。

在接入设备上配置设备发送RADIUS报文使用的源IP地址（即NAS-IP）的方法有：

- RADIUS方案视图下，通过如下命令配置NAS-IP，只对本RADIUS方案有效；且优先级高于系统视图下的配置。

  nas-ip { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }
- 系统视图下，通过如下命令配置NAS-IP，对所有RADIUS方案有效；

  radius nas-ip { **interface** *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

配置NAS-IP的注意事项：

- 通过指定接口配置NAS-IP和通过指定IP来配置NAS-IP的方式不可同时使用，后配置的生效。
- 为避免物理接口故障时从服务器返回的报文不可达，可使用Loopback接口地址为发送RADIUS报文使用的源IP地址。

14.5 802.1X在线用户握手功能的应用场景和注意事项有哪些？

802.1X在线用户握手功能是指：802.1X用户在线期间，设备通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。具体的说，通过**dot1x handshake**命令开启设备的在线用户握手功能后，设备会根据**dot1x timer handshake-period**命令设置的时间间隔，向在线用户发送握手请求报文（EAP-Request/Identity），以定期检测用户的在线情况。如果设备连续多次（通过命令**dot1x retry**设置）没有收到客户端的应答报文（EAP-Response/Identity），则将用户置为下线状态。开启802.1X在线用户握手功能，可以防止802.1X用户因为异常原因下线而设备无法感知。

802.1X在线握手功能的注意事项如下：

- 部分802.1X客户端不支持与设备进行握手报文的交互，建议在这种情况下，执行命令**undo dot1x handshake**关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 设备在线用户过多，资源不够，需要适当增加握手时间间隔（通过命令**dot1x timer handshake-period**设置）和向接入用户发送认证请求报文的最大次数（通过命令**dot1x retry**设置），重新进行认证尝试。

14.6 在线用户握手安全功能有哪些使用限制？

开启在线用户握手安全功能（可执行 **dot1x handshake secure** 命令来开启）后，可以防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。

需要注意的是：

只有设备上的在线用户握手功能处于开启状态时，安全握手功能才会生效。

本功能仅能在 iNode 客户端和 iMC 服务器配合使用的组网环境中生效。

14.7 什么情况下需要开启在线握手成功报文功能？

端口上开启在线用户握手功能（可执行 **dot1x handshake** 命令来开启）后，缺省情况下，设备收到该端口上 802.1X 在线用户的在线握手应答报文（EAP-Response/Identity 报文）后，则认为该用户在线，并不给客户端回应在线握手成功报文（EAP-Success 报文）。但是，有些 802.1X 客户端如果没有收到设备回应的在线握手成功报文（EAP-Success 报文），就会自动下线。为了避免这种情况发生，需要在端口上配置 **dot1x handshake reply enable** 命令来开启发送在线握手成功报文功能。

只有当 802.1X 客户端需要收到在线握手成功报文时，才需要开启此功能。

14.8 配置设备端和服务端的认证、授权、计费时需要注意什么？

配置认证、授权、计费时，需保证设备端与服务器的配置一致，否则会导致用户上线失败。常见的例如以下情况均会导致上线失败：

- 远端服务器侧已配置用户授权 vlan 为 vlan name，但设备并不存在这个 name，导致授权失败。
- 设备上与 IMC 配置的授权密码不一致，会导致无法上线。
- 接入设备上配置的 Portal 密钥和 Portal 认证服务器上配置的密钥不一致，导致 Portal 认证服务器报文验证出错，Portal 认证服务器拒绝弹出认证页面。在 Portal 认证服务器视图下使用 **display this** 命令查看接入设备上是否配置了 Portal 认证服务器密钥，若没有配置密钥，请补充配置；若配置了密钥，请在 Portal 认证服务器视图中使用 **ip** 或 **ipv6** 命令修改密钥，或者在 Portal 认证服务器上查看对应接入设备的密钥并修改密钥，直至两者的密钥设置一致。

14.9 什么情况下需要配置允许MAC迁移功能？

允许 MAC 迁移功能是指，允许在线的 802.1X 用户、MAC 地址认证用户或 Web 认证用户迁移到设备的其它端口上或迁移到同一端口下的其它 VLAN（指不同于上一次发起认证时所在的 VLAN）接入后可以重新认证上线。可以通过在接口下执行 **port-security mac-move permit** 命令用来开启允许 MAC 迁移功能。缺省情况下，允许 MAC 迁移功能处于关闭状态。

通常，不建议开启该功能，只有在用户漫游迁移需求的情况下建议开启此功能。

需要注意的是：

如果用户进行 MAC 地址迁移前，服务器在线用户数已达到上限，则用户 MAC 地址迁移不成功。

对于迁移到同一端口下的其它VLAN内接入的用户，MAC地址认证的多VLAN模式优先级高于MAC迁移功能。当开启端口的多 VLAN 模式（通过 **mac-authentication host-mode multi-vlan** 命令）后，设备直接允许用户在新的 VLAN 通过，无需再次认证。

14.10 如何配置和查看802.1X用户使用的强制认证域？

在端口上指定强制认证域为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

缺省情况下，未指定 802.1X 用户使用的强制认证域。在二层以太网接口视图或二层聚合接口视图（产品不支持二层聚合口除外）下，通过 **dot1x mandatory-domain** 命令可以指定端口上 802.1X 用户使用的强制认证域。通过 **display dot1x** 命令的“Mandatory auth domain”字段可以查看指定接口的 802.1X 强制认证域配置。

14.11 当前ISP域中未指定具体授权方法的情况下，缺省授权方法是什么？如何配置缺省授权？

每个接入用户都属于一个 ISP 域，如果用户所属的 ISP 域下未配置任何认证、授权、计费方法，系统将使用缺省的认证、授权、计费方法，分别为本地认证、本地授权和本地计费。以配置授权为例，缺省情况下，ISP 域的缺省授权方法为 **local**。在当前 ISP 域视图下，可以通过如下命令配置缺省的授权方法：

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

需要注意的是：

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme** *radius-scheme-name* **local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

14.12 使用iNode客户端作为802.1X客户端时，iNode该如何配置？

以 iNode PC 7.3 版本为例配置客户端如下：

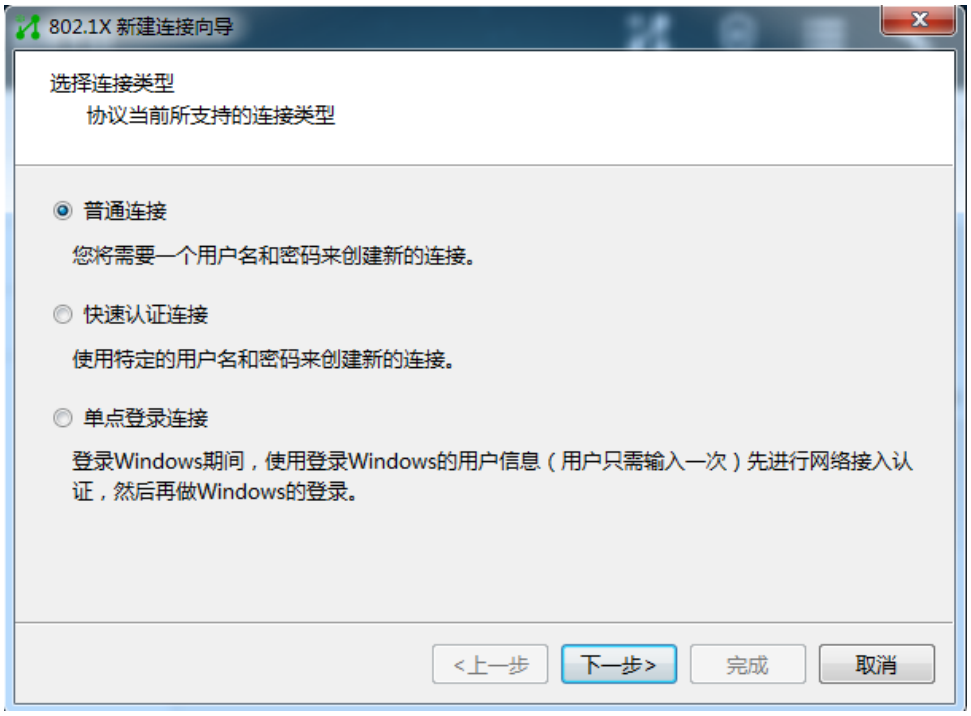
(1) 启动客户端

图14-1 iNode 客户端界面示意图

(2) 新建 802.1X 连接

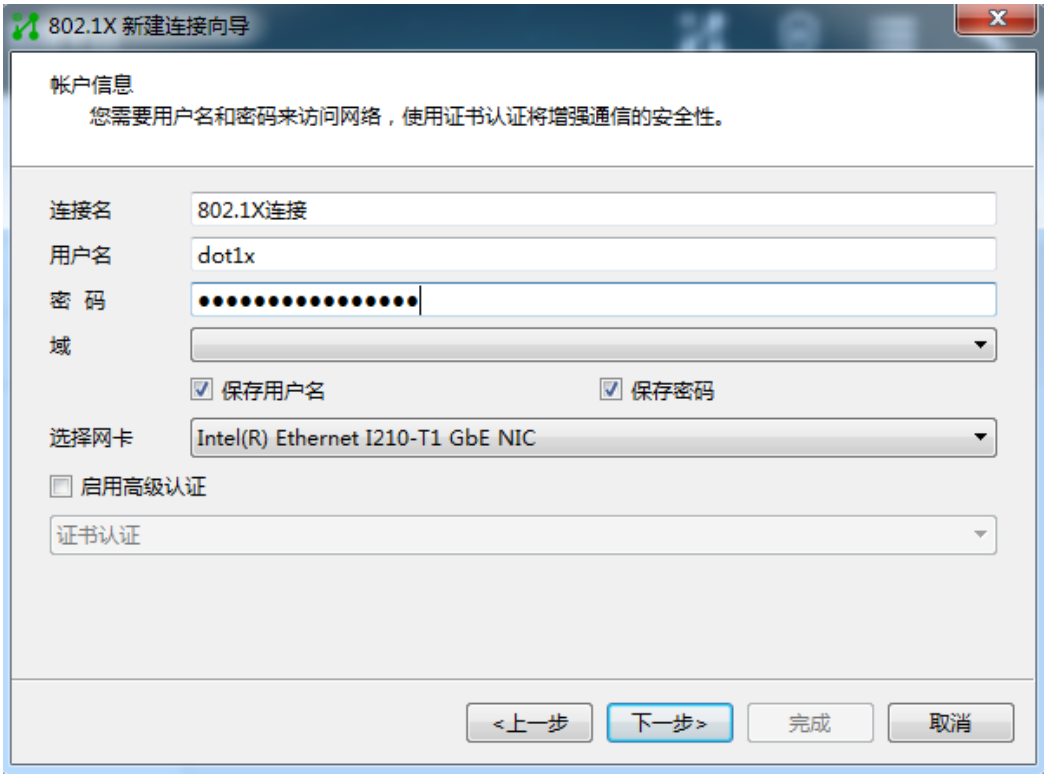
点击<新建>按钮，进入新建连接向导对话框。

图14-2 新建 802.1X 连接示意图



(3) 输入用户名和密码

图14-3 802.1X 用户名、密码配置示意图



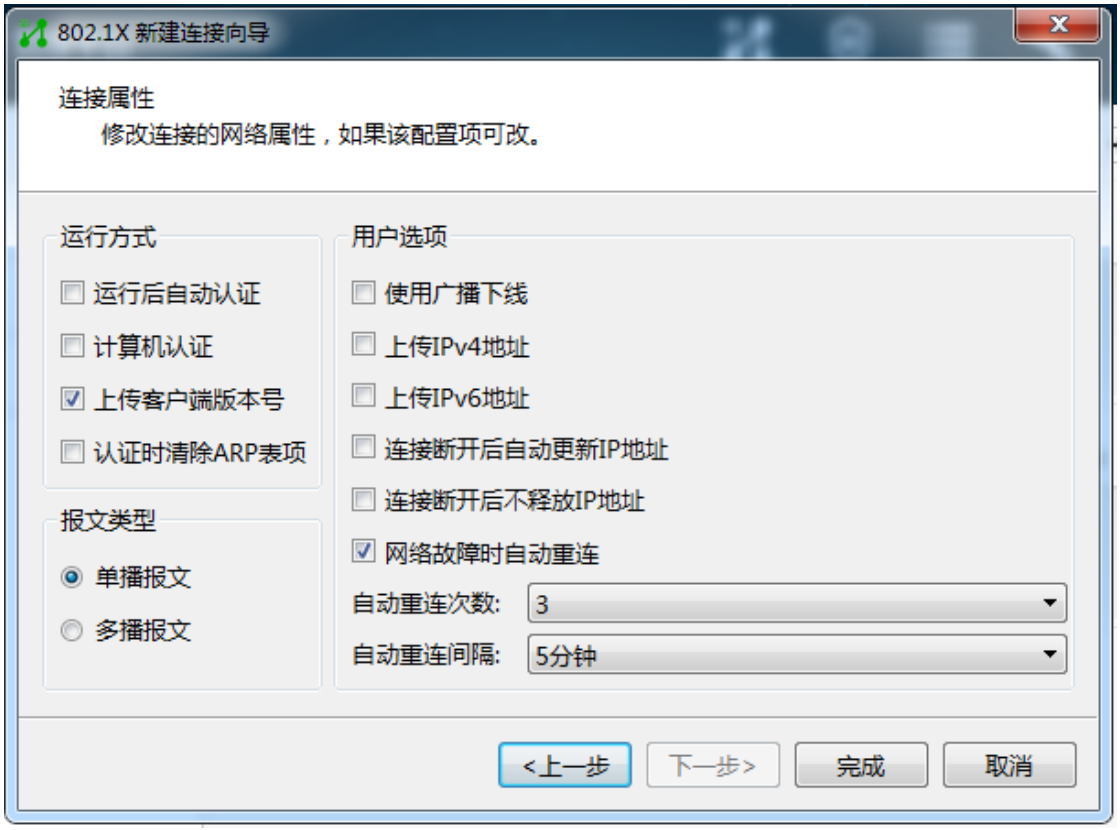
需要注意：iNode 认证连接的用户名、设备用于认证的域以及服务器的后缀三者密切相连，具体的配置关系参见下表。

表14-1 认证域配置关系表

iNode 认证连接的用户名	设备用于认证的 domian	设备配置的相关命令	iMC 中的服务后缀
X@Y	Y	with-domain	Y
		without-domain	无
X	Default domain (设备上指定的缺省域)	with-domain	Default domain
		without-domain	无

(4) 设置连接属性

图14-4 802.1X 连接属性配置示意图



需要注意的是：用户选项中如果选择了“上传客户端版本号”则客户端会对标准的认证协议进行扩展，在上传用户名的报文中添加客户端版本号来与 iMC 服务器配合进行认证。如果不选此项，则采用标准的 EAP 报文进行身份认证。

如果配置的认证方式为 RADIUS 认证失败转本地认证，由于本地认证不能对客户端上传的版本号进行识别，请不要勾选“上传客户端版本号”选项。

(5) 发起 802.1X 连接

完成新建连接后，点击 iNode 客户端的<连接>按钮，发起 802.1X 连接。

14.13 端口安全模式分为哪两类？配置之前，端口需要满足什么条件？

端口安全模式分为两大类：控制 MAC 学习类和认证类。缺省情况下，端口处于 noRestrictions 模式，此时该端口的安全功能关闭，端口处于不受端口安全限制的状态。通过 **port-security port-mode** 命令可以配置端口安全模式。

- 控制 MAC 学习类：无需认证，包括端口自动学习 MAC 地址和禁止 MAC 地址学习两种模式。
- 认证类：利用 MAC 地址认证和 802.1X 认证机制来实现，包括单独认证和组合认证等多种模式。

在配置端口安全模式之前，端口上首先需要满足以下条件：

- 802.1X 认证关闭。
- MAC 地址认证关闭。

- 端口未加入业务环回组。
- 对于 autoLearn 模式，还需要提前设置端口安全允许的最大安全 MAC 地址数。但是如果端口已经工作在 autoLearn 模式下，则无法更改端口安全允许的最大安全 MAC 地址数。

14.14 802.1X环境如何实现终端免认证？

开启 802.1X 功能的设备可以通过配置端口静态绑定 MAC 地址来实现终端免认证。缺省情况下，未配置任何 MAC 地址表项，可通过 **mac-address static** 命令配置静态 MAC 地址绑定端口。例如：需要实现免认证的终端的 MAC 地址为 0001-0001-0001，与交换机的端口 GE1/0/1 端口相连，GE1/0/1 端口属于 VLAN10，通过在系统视图下执行 mac-address static 0001-0001-0001 interface GigabitEthernet 1/0/1 vlan 10 命令，配置静态 MAC 地址绑定端口，从而实现免认证。

14.15 设备对RADIUS 15号属性的检查方式该如何配置？

RADIUS 15 号属性为 Login-Service 属性，该属性携带在 Access-Accept 报文中，由 RADIUS 服务器下发给设备，表示认证用户的业务类型，例如属性值 0 表示 Telnet 业务。设备检查用户登录时采用的业务类型与服务器下发的 Login-Service 属性所指定的业务类型是否一致，如果不一致则用户认证失败。由于 RFC 中并未定义 SSH、FTP 和 Terminal 这三种业务的 Login-Service 属性值，因此设备无法针对 SSH、FTP、Terminal 用户进行业务类型一致性检查，为了支持对这三种业务类型的检查，H3C 为 Login-Service 属性定义了下表所示的扩展取值。

表14-2 扩展的 Login-Service 属性值

属性值	描述
50	用户的业务类型为SSH
51	用户的业务类型为FTP
52	用户的业务类型为Terminal

可以通过配置设备对 RADIUS 15 号属性的检查方式，控制设备是否使用扩展的 Login-Service 属性值对用户进行业务类型一致性检查。

- 严格检查方式（**strict**）：设备使用标准属性值和扩展属性值对用户业务类型进行检查，对于 SSH、FTP、Terminal 用户，当 RADIUS 服务器下发的 Login-Service 属性值为对应的扩展取值时才能够通过认证。
- 松散检查方式（**loose**）：设备使用标准属性值对用户业务类型进行检查，对于 SSH、FTP、Terminal 用户，在 RADIUS 服务器下发的 Login-Service 属性值为 0（表示用户业务类型为 Telnet）时才能够通过认证。

在 RADIUS 方案视图下，通过执行 **attribute 15 check-mode { loose | strict }**命令用来配置对 RADIUS Attribute 15 的检查方式。

由于某些 RADIUS 服务器不支持自定义的属性，无法下发扩展的 Login-Service 属性，若要使用这类 RADIUS 服务器对 SSH、FTP、Terminal 用户进行认证，建议设备上对 RADIUS 15 号属性值采用松散检查方式。

14.16 对802.1X用户进行周期性重认证时，设备按什么顺序为其选择重认证时间间隔？

对 802.1X 用户进行周期性重认证时，设备将按照如下先后顺序为其选择重认证时间间隔：

(1) 服务器下发的重认证时间间隔；

(2) 通过接口视图下的 **dot1x timer reauth-period** 命令配置的周期性重认证定时器的值；

(3) 通过系统视图下的 **dot1x timer reauth-period** 命令配置的周期性重认证定时器的值；

(4) 设备缺省的周期性重认证定时器的值：3600 秒。

14.17 802.1X的Free IP功能是否可以与端口安全同时开启？

在 802.1X 的 EAD 快速部署方案中，可允许未通过认证的 802.1X 终端用户访问指定的 IP 地址段，该 IP 地址段中通常配置一个或多个特定服务器，用于提供 EAD 客户端的下载升级或者动态地址分配等服务。这种网段称为 Free IP，可通过 **dot1x ead-assistant free-ip** 命令进行配置。

由于端口安全特性不支持 802.1X 的 EAD 的快速部署功能，全局使能端口安全功能将会使 EAD 快速部署功能失效。如果接口下开启了端口安全，会导致配置 free-ip 不生效，建议删除。

14.18 802.1X的Free IP功能是否可以与MAC地址认证同时开启？

在 802.1X 的 EAD 快速部署方案中，可允许未通过认证的 802.1X 终端用户访问指定的 IP 地址段，该 IP 地址段中通常配置一个或多个特定服务器，用于提供 EAD 客户端的下载升级或者动态地址分配等服务。这种网段称为 Free IP，可通过 **dot1x ead-assistant free-ip** 命令进行配置。

部分设备上，EAD 快速部署功能和 MAC 地址认证功能互斥。

部分设备上，支持同时配置 EAD 快速部署辅助功能和 MAC 地址认证功能，需要注意的是：

- 同时开启 EAD 快速部署辅助功能和 MAC 地址认证功能时，MAC 地址认证用户认证失败后，该用户的 MAC 地址不会加入静默 MAC。若服务器上没有相关的用户信息，MAC 地址认证用户认证失败后，需要等 EAD 表项老化之后，才能再次触发认证。
- 开启 EAD 快速部署辅助功能与 MAC 地址认证的 Guest VLAN、Guest VSI 或 Critical VLAN、Critical VSI 功能不建议同时配置，否则可能导致 MAC 地址认证的 Guest VLAN、Guest VSI 或 Critical VLAN、Critical VSI 功能无法正常使用。
- 同时开启 EAD 快速部署辅助功能和 MAC 地址认证功能时，不建议同时配置 Web 认证或 IP Source Guard 功能，否则可能导致 Web 认证或 IP Source Guard 功能无法正常使用。
- 开启 EAD 快速部署辅助功能后，对于在使能 EAD 快速部署辅助功能之前就加入静默 MAC 的用户，需要等静默 MAC 老化后才能触发 EAD 快速部署功能。

14.19 为什么在接入设备上强制Portal用户下线失败？

在接入设备上使用 **portal delete-user** 命令强制用户下线时，由接入设备主动发送下线通知报文到 Portal 认证服务器，Portal 认证服务器会在指定的端口监听该报文（缺省为 50100），但是接入设备发送的下线通知报文的目的端口和 Portal 认证服务器真正的监听端口不一致，故 Portal 认证服务器无法收到下线通知报文，Portal 认证服务器上的用户无法下线。

当使用客户端的“断开”属性让用户下线时，由 Portal 认证服务器主动向接入设备发送下线请求，其源端口为 50100，接入设备的下线应答报文的目的端口使用请求报文的源端口，避免了其配置上的错误，使得 Portal 认证服务器可以收到下线应答报文，从而 Portal 认证服务器上的用户成功下线。

使用 **display portal server** 命令查看接入设备对应服务器的端口，并在系统视图中使用 **portal server** 命令修改服务器的端口，使其和 Portal 认证服务器上的监听端口一致。

14.20 什么情况需要配置认证触发功能？

对于不支持主动发送EAPOL-Start报文来发起802.1X认证的客户端，设备支持配置认证触发功能，即设备主动向该端口上的客户端发送认证请求来触发 802.1X 认证。设备提供了以下两种类型的认证触发功能：

- 组播触发功能：启用了该功能的端口会定期（间隔时间通过命令 **dot1x timer tx-period** 设置）向客户端组播发送 EAP-Request/Identity 报文来检测客户端并触发认证。
- 单播触发功能：当启用了该功能的端口收到源 MAC 地址未知的报文时，会主动向该 MAC 地址单播发送 EAP-Request/Identity 报文，若端口在指定的时间内（通过命令 **dot1x timer tx-period** 设置）没有收到客户端的响应，则重发该报文（重发次数通过命令 **dot1x retry** 设置）。

缺省情况下，组播触发功能处于开启状态，单播触发功能处于关闭状态。

建议组播触发功能和单播触发功能不要同时开启，以免认证报文重复发送。

14.21 什么情况下端口会加入Critical VLAN?

802.1X Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Critical VLAN。目前，只采用 RADIUS 认证方式的情况下，在所有 RADIUS 认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。

14.22 端口安全允许的最大用户接入数有何限制？

端口安全允许某个端口下有多个用户接入，但是允许的用户数不能超过规定的最大值。

配置端口允许的最大安全 MAC 地址数有两个作用：

- 控制端口允许接入网络的最大用户数。对于采用 802.1X、MAC 地址认证或者两者组合形式的认证类安全模式，端口允许的最大用户数取通过 **port-security max-mac-count** *max-count* [**vlan** [*vlan-id-list*]]命令配置的 *max-count* 值与相应模式下允许认证用户数 *max-number*（通过 **dot1x max-user** *max-number* 命令配置端口上最多允许同时接入的 802.1X 用户数，通过 **mac-authentication max-user** *max-number* 命令配置端口上最多允许同时接入的 MAC 地址认证用户数）的最小值；
- 控制 autoLearn 模式下端口能够添加的最大安全 MAC 地址数。如果配置了 **vlan** 关键字，但未指定具体的 *vlan-id-list* 时，可控制接口允许的每个 VLAN 内的最大安全 MAC 地址数；否则表示控制指定 *vlan-id-list* 内的最大安全 MAC 地址数。

14.23 同一端口下，同时进行MAC地址认证的终端过多时，重新认证时间间隔该如何设置？

用户被加入 Guest VLAN 或 Guest VSI 之后，设备将以指定的时间间隔对该用户定期发起重新认证，可通过 **mac-authentication guest-vlan re-authenticate** 命令开启 Guest VLAN 中用户的重新认证功能（通过 **mac-authentication guest-vsi re-authenticate** 命令开启 Guest VSI 中用户的重新认证功能），设备缺省开启 Guest VLAN 和 Guest VSI 中用户的重新认证功能。

当端口上同时进行认证的用户数大于 300 时，建议通过 **mac-authentication guest-vlan auth-period** 命令将设备对 Guest VLAN 中的用户进行重新认证的时间间隔（通过 **mac-authentication guest-vsi auth-period** 命令将设备对 Guest VSI 中的用户进行重新认证的时间间隔）设置为 30 秒以上。

14.24 IP Source Guard动态绑定表项可以来源于哪些功能模块？

IP Source Guard 功能通常配置在接入用户侧的接口上，通过手工配置或动态获取的表项对接口收到的报文进行过滤控制，以防止非法用户报文通过，从而限制了对网络资源的非法使用。

在通过 **ip verify source** 或 **ipv6 verify source** 命令配置了 IP Source Guard 动态绑定功能的接口上，IP Source Guard 可以通过与不同的模块配合生成 IP Source Guard 动态绑定表项。

表14-3 IP Source Guard 动态绑定功能信息表

接口类型	IPv4 表项来源模块	IPv6 表项来源模块
二层以太网接口	DHCP Snooping、ARP Snooping	DHCPv6 Snooping、ND Snooping
	802.1X	802.1X
三层以太网接口或VLAN接口	DHCP中继	DHCPv6中继、ND RA
	DHCP服务器	DHCPv6服务器

需要注意的是：要实现 IP Source Guard 动态绑定功能正常使用，请保证网络中的 802.1X、ARP Snooping 、DHCP Snooping、DHCP 中继、DHCP 服务器或 ND RA 配置有效且工作正常。

14.25 配置了IP Source Guard静态绑定表项，为什么绑定功能不生效？

在全局或接口视图下通过 **ip source binding** 命令，可配置 IP Source Guard 静态绑定表项。只有同时在接口下通过 **ip verify source** 命令配置 IPv4 接口绑定功能，才算打开根据绑定表项过滤报文的开关。这种情况下设备通过配置的 IPv4 静态绑定表项和从其它模块获取的 IPv4 动态绑定表项对接口转发的报文进行过滤或者配合其它模块提供相关的安全服务。

14.26 Portal HTTPS重定向为什么不生效？

HTTP 重定向是一种将用户的 HTTP/HTTPS 请求转到某个指定 URL 的方法，对 HTTP 请求报文，无需进行任何配置，设备即可进行重定向处理；对于 HTTPS 报文，必须配置对 HTTPS 报文进行重定向的内部侦听端口号，设备才会进行重定向。

缺省情况下，对 HTTPS 报文进行重定向的内部侦听端口号为 6654。为了避免端口号冲突导致服务不可用，需确保内部侦听端口号不是知名协议使用的端口号，且不能被其它基于 TCP 协议的服务占用（已被其他服务占用的 TCP 端口号可以通过 **display tcp** 命令查看）。可通过 **http-redirect https-port** 命令配置对 HTTPS 报文进行重定向的内部侦听端口号。

14.27 为什么需要配置RADIUS报文的共享密钥？

RADIUS 客户端与 RADIUS 服务器使用 MD5 算法并在共享密钥的参与下生成验证字，接受方根据收到报文中的验证字来判断对方报文的合法性。只有在共享密钥一致的情况下，彼此才能接收对方发来的报文并作出响应。

通常，在设备上配置 RADIUS 认证/计费服务器时应同时指定与主/备服务器交互的共享密钥，配置命令为 **primary accounting**、**primary authentication**、**secondary accounting**、**secondary authentication**。若通过上述命令指定服务器时未同时配置共享密钥，则需要通过在 RADIUS 方案视图下执行 **key** 命令来配置 RADIUS 报文的共享密钥。

需要注意的是：必须保证设备上设置的共享密钥与 RADIUS 服务器上的完全一致。

14.28 配置AAA时如果没有计费服务器，需要配置当前ISP域的计费方法吗？

ISP 域的缺省计费方法为 **local**，即本地计费。因此，即使没有指定远程计费服务器，也需要通过配置 **accounting default none** 命令将当前 ISP 域的缺省计费方法配置为不计费，否则会导致用户认证失败。

14.29 在ISP域下，若配置AAA认证/授权/计费方法使用的RADIUS方案不存在，AAA认证/授权/计费方法会生效吗？

在 ISP 域下，若配置 AAA 认证/授权/计费方法使用的 RADIUS 方案不存在，AAA 认证/授权/计费方法不会生效。可以执行 **display radius scheme** 命令查看 ISP 域下 AAA 认证/授权/计费方法中指定的 RADIUS 方案是否存在。例如如下配置：

```
[system]  domain aaa
[system-isp-aaa]authentication login radius-scheme bbb
[system-isp-aaa]display radius scheme bbb
The RADIUS scheme does not exist.
```

虽然为 login 用户配置的认证方法指定了 RADIUS 方案 bbb，但 RADIUS 方案 bbb 实际不存在，所以配置不生效。

14.30 在实际应用场景中，若需要通过iMC服务器下发安全ACL，应该如何配置？

在实际应用场景中，若需要通过 iMC 服务器下发安全 ACL，请在设备上通过 **radius session-control enable** 命令开启 RADIUS session control 功能，否则相关安全 ACL 无法生效。

iMC RADIUS 服务器使用 session control 报文向设备发送授权信息（例如授权 ACL/VLAN/用户组/VSI/黑洞 MAC）的动态修改请求以及断开连接请求。在使用 iMC RADIUS 服务器且服务器需要对用户授权信息进行动态修改或强制用户下线的情况下，必须开启 RADIUS session control 功能。

14.31 802.1X在线用户较多时，用户重认证周期过长该如何解决？

当 RADIUS 服务器从不可达变为可达时，处于 Critical VLAN 或 Critical VSI 中的用户也会再次发起认证，在设备上 802.1X 在线用户较多的情况下，如果通过 **dot1x server-recovery online-user-sync** 命令开启了 RADIUS 服务器变为可达后的 802.1X 在线用户信息同步功能，会因为同时进行认证的用户数量较大，而导致用户的上线时间变长。

可以执行 **undo dot1x server-recovery online-user-sync** 命令关闭 802.1X 在线用户信息同步功能，使重认证周期恢复正常。

14.32 如何解决设备因无法感知802.1X认证用户离线导致用户再次上线失败？

设备因无法感知 802.1X 认证用户离线导致用户再次上线失败，通常有如下几种方法可以解决：

- 执行 **dot1x offline-detect enable** 命令开启端口的 802.1X 认证下线检测功能，若设备在一个下线检测定时器间隔之内，未收到此端口下某 802.1X 在线用户的报文，则将切断该用户的连接，同时通知 RADIUS 服务器停止对此用户进行计费。
- 执行 **port-security traffic-statistics enable** 命令开启端口安全接入用户的流量统计功能，设备会根据 802.1X 认证用户的 MAC 地址统计流量信息，并将统计数据发送给计费服务器。部分产品不支持此方式。
- 执行 **port-security mac-move permit** 命令开启允许 MAC 迁移功能，如果用户从某一端口上线成功，则允许该在线用户在设备的其它端口上（无论该端口是否与当前端口属于同一 VLAN）发起认证。如果该用户在后接入的端口上认证成功，则当前端口会将该用户立即进行下线处理（不论用户在当前端口上通过哪种方式进行认证），保证该用户仅在一个端口上处于上线状态。

14.33 配置802.1X Guest VLAN功能前有哪些配置准备？

配置 802.1X Guest VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Guest VLAN 的 VLAN。
- 在接入控制方式为 MAC-based 的端口上，保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态。MAC VLAN 功能的具体配置请参见“二层技术-以太网交换配置指导”中的“VLAN”。

14.34 端口接入控制方式为Port-based时可以配置单播触发功能吗？

单播触发功能建议只在端口接入控制方式为 MAC-based 时配置；若在端口接入控制方式为 Port-based 时配置单播触发功能，可能会导致用户正常无法上线。

另外，建议组播触发功能和单播触发功能不要同时开启，以免认证报文重复发送。

14.35 如何配置MAC地址认证用户使用的账号格式？

开启 MAC 地址认证后，设备默认使用用户的 MAC 地址作为用户名和密码，其中字母为小写，且不带连字符“-”。可以通过执行 **mac-authentication user-name-format** 命令来配置 MAC 地址认证用户的账号格式。MAC 地址认证用户认证时，请确保使用的用户名格式符合配置的账户格式，否则，将导致认证失败。

需要注意的是：**mac-authentication mac-range-account** 命令（用来配置指定 MAC 地址范围的 MAC 地址认证用户名和密码）的优先级高于 **mac-authentication user-name-format** 命令。缺省情况下，未对指定 MAC 地址范围的 MAC 地址认证用户设置用户名和密码，MAC 地址认证用户采用 **mac-authentication user-name-format** 命令设置的用户名和密码接入设备。

14.36 开启802.1X或MAC地址认证对端口安全功能有何影响？

如果已全局开启了 802.1X 或 MAC 地址认证，则无法使能端口安全。

反之，如果开启了端口安全，则不能开启端口上的 802.1X 以及 MAC 地址认证，也不能修改 802.1X 端口接入控制方式和端口授权状态，它们只能随端口安全模式的改变由系统更改。

可以通过 **undo port-security enable** 命令关闭端口安全。但需要注意的是，在端口上有用户在线的情况下，关闭端口安全会导致在线用户下线。

执行使能或关闭端口安全的命令后，端口上的相关配置将会恢复为如下情况：

- 802.1X 端口接入控制方式恢复为 **macbased**；
- 802.1X 端口的授权状态恢复为 **auto**。

14.37 如何修改端口安全模式？

二层以太网接口或二层聚合接口视图下，通过执行 **port-security port-mode** 命令可配置端口安全模式。缺省情况下，端口处于 noRestrictions 模式，此时该端口的安全功能关闭，端口处于不受端口安全限制的状态。

当端口安全已经使能且当前端口安全模式不是 noRestrictions 时，若要改变端口安全模式，必须首先执行 **undo port-security port-mode** 命令恢复端口安全模式为 noRestrictions 模式；再重新配置为其它端口安全模式。

端口上有用户在线的情况下，端口安全模式无法改变。

端口安全模式与端口下的 802.1X 认证使能、端口接入控制方式、端口授权状态以及端口下的 MAC 地址认证使能配置互斥。

15 路由

15.1 路由配置不完整或配置错误会导致网络出现哪些故障，如何进行排查？

可能会出现的故障有：

- 交换机或主机设备跨网段 Ping 不通某个 IP 地址

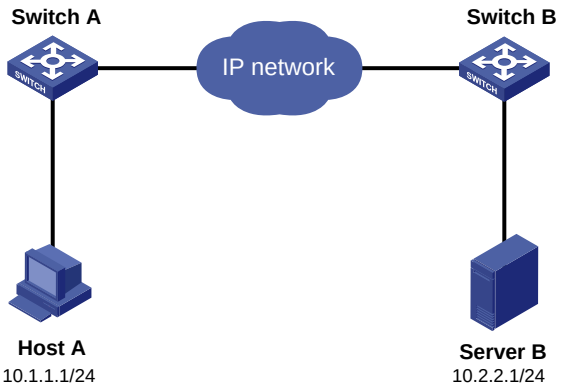
- 主机无法跨网段访问交换机设备的 web 页面
- 交换机直连网段的设备无法访问外部网络
- 交换机学习不到跨网段设备的 ARP 表项
- 交换机到达目的地址的路由单通，只能发送或只能接收数据包

在排查路由问题之前，需要确保网络中没有出现链路故障，并且各设备的 IP 地址配置正确、网段未发生冲突。

- 如果主机通过交换机无法访问其他网段的设备，则需要检查主机设备上是否配置了正确的网关地址。如果修改后仍无法访问，则需要继续检查交换机的路由配置。
- 如果交换机无法访问目的网络地址的设备，则需要检查交换机上有没有到达目的网络地址的路由，中间设备有没有到达源地址和目的网段地址的路由，以及目的设备有没有正确的回程路由。

如图 15-1 所示，当用户在 SwitchA 上配置了去往服务器 B 所在网段 10.2.2.0/24 的路由后，终端 A 还是无法与服务器 B 进行通信。

图15-1 三层通信示意图



一般情况下终端 A 和服务器 B 之间的通信是双向的，即不仅 SwitchA 上要有到 10.2.2.0/24 的路由，而且 SwitchB 上也要有到 10.1.1.0/24 的路由。因此，当用户在 SwitchA 上配置了去往服务器 B 所在网段 10.2.2.0/24 的路由后，还要在 SwitchB 上配置去往终端 A 所在的网段 10.1.1.0/24 的路由。在只有同时满足这两个条件，终端 A 才能与服务器 B 正常通信。

15.2 在同一设备上配置的VPN网段和公网网段相同，会冲突吗？

会因为网段冲突而导致网络故障。在同一设备上配置的 VPN 网段和公网网段相同，其他设备在转发报文时，优先选择直连路由的下一跳地址，而不是为 VPN 网段配置的静态路由下一跳，导致 ping 不通。需要将直连网段地址修改为其他网段的地址才可解决该问题。

15.3 策略路由配置错误导致Ping不通故障如何排查？

配置了策略路由后，满足一定条件的报文会优先通过策略路由执行指定的操作（例如设置报文的下一跳）。如果策略路由配置错误，可能会导致报文转发失败。

可通过如下步骤查看策略路由的配置，并作出相应的修改。

(1) 执行 **display ip policy-based-route** 命令，查看已经配置的策略。如果配置了策略路由，则继续执行下一步。

(2) 执行 **display ip policy-based-route setup** 命令，查看已经应用的策略路由信息，并分别通过如下命令查看具体类型的策略路由信息：

- 执行 **display ip policy-based-route local** 命令，查看本地策略路由的配置信息和统计信息
- 执行 **display ip policy-based-route interface** 命令，查看接口下转发策略路由的配置信息和统计信息
- 执行 **display ip policy-based-route apply** 命令，查看 VLAN 接口上应用的策略路由及其统计信息。
- 执行 **display ip policy-based-route global** 命令，查看全局策略路由的配置信息和统计信息
- 执行 **display ip policy-based-route egress interface** 命令，查看 VXLAN 隧道接口出方向策略路由的配置信息和统计信息。

(3) 如果策略路由的 **if-match** 子句配置了 ACL 匹配规则，可通过 **display acl** 命令查看 ACL 的配置和运行情况。

(4) 修改策略路由，保证设备间流量正常转发。

- 如果是策略路由的匹配规则或 apply 子句导致的流量不通，则需要修改策略路由的匹配规则或 **apply** 子句。
- 如果是策略路由应用的接口错误，则需要先取消对应接口的策略路由配置，再重新将策略路由应用到正确的接口上。
- 如果应用的全局策略路由或本地策略路由配置有误，则需要先取消对应的配置，再修改并重新应用策略路由。

15.4 静态路由的出接口没UP会导致Ping不通吗？

在配置静态路由时，指定的出接口需要为 UP 状态，否则静态路由不生效。

15.5 终端设备如果未配置网关，会导致通信故障吗？

会出现故障。如果组网环境中有多个网段，为实现终端设备跨网段互相通信，则终端设备需要配置网关，并且非直连的网关设备之间需要配置到达目的网段的路由。

15.6 为什么配置的备份静态路由未及时生效？

设备上配置了到达目的网段的主用静态路由和备用静态路由，当主用链路故障时，设备可能未及时检测到，备用链路的静态路由不能及时生效导致流量丢失。

建议配置静态路由关联 track 项，通过 track 联动 nqa 对主用链路进行检测。当主用链路发生故障时，设备能及时发现并撤销主用静态路由，启用备用静态路由指导报文转发，将链路故障的影响降到最低。

15.7 为什么配置了静态路由关联track项，却无法通过track关联的检测模块及时检测链路故障？

请按照如下顺序进行排查：

(1) 首先排查检测模块的配置是否正常，如果检查没问题，再进行下一步骤。

(2) 检查静态路由关联 track 项的配置是否成功。执行 **display current-configuration | include route-static** 命令查看静态路由的配置情况。在配置静态路由时，应严格按照各产品命令参考里的顺序配置各个参数，否则会配置失败。其中，**description** 参数后面不能配置其他参数，只能输入静态路由描述信息。

15.8 BGP邻居关系未建立的常见原因有哪些？如果处理此类故障？

本类故障的常见原因主要包括：

- BGP 报文转发不通
- ACL 过滤了 TCP 的 179 端口
- 配置的邻居的 AS 号错误
- 邻居的 IP 地址/IPv6 地址配置错误
- 未配置 **peer enable** 命令
- 用 Loopback 口建立邻居时没有配置 **peer connect-interface**
- 用非直连的 EBGP 邻居未配置 **peer ebgp-max-hop**
- **peer valid-ttl-hops** 配置错误
- 对端配置了 **peer ignore**
- 两端的地址族不匹配

故障处理步骤：

(1) 使用 **ping** 命令检查链路是否畅通。

(2) 检查路由表中是否存在到邻居的可用路由。

(3) 使用 **display tcp verbose** 命令或 **display ipv6 tcp verbose** 命令检查 TCP 连接是否正常。

(4) 检查是否配置了禁止 TCP 端口 179 的 ACL。

(5) 执行 **display current-configuration** 命令查看当前配置，检查邻居的 AS 号配置是否正确。

(6) 执行 **display bgp peer ipv4 unicast** 命令或 **display bgp peer ipv6 unicast** 命令检查邻居的 IP 地址/IPv6 地址是否正确。

(7) 如果使用 Loopback 接口，检查是否配置了 **peer connect-interface** 命令。

(8) 如果是物理上非直连的 EBGP 邻居，检查是否配置了 **peer ebgp-max-hop** 命令。

(9) 如果配置了 **peer ttl-security hops** 命令，请检查对端是否也配置了该命令，且保证双方配置的 *hop-count* 不小于两台设备实际需要经过的跳数。

(10) 检查两端设备是否配置了 **peer ignore**，如果想建立邻居关系，执行 **undo peer ignore** 命令即可。

(11) 请检查 BGP 会话两端的地址族能力是否匹配。例如，建立 BGP VPNv4 邻居时，需要两端都要在 BGP-VPNv4 地址族下配置命令 **peer enable**。

15.9 怎么查看和配置等价路由条数？

当到达同一目的地址的多条等价路由的条数超过了设备支持的最大条数时，新增的等价路由无法和已存在的等价路由一起形成负载分担。

通过如下命令可以查看系统当前支持的最大等价路由的条数：

- 执行 **display max-ecmp-num** 命令用来显示系统支持 IPv4 最大等价路由的条数。
- 执行 **display ipv6 max-ecmp-num** 命令用来显示系统支持 IPv6 最大等价路由的条数。

通过如下命令可以调整系统支持的最大等价路由的条数：

- 执行 **max-ecmp-num** 命令调整设备支持的最大 IPv4 等价路由的条数。
- 执行 **ipv6 max-ecmp-num** 命令用来配置系统支持 IPv6 最大等价路由的条数。

部分设备不支持配置系统支持的最大等价路由的条数，在这些设备上，可以通过各路由协议视图的 **maximum load-balancing** 命令取值范围查看路由协议支持的最大等价路由条数。需要注意的是，等价路由模式的配置可能会影响等价路由条数，通过 **ecmp mode** 命令可以调整等价路由模式。有关等价路由模式的详细介绍，请参见“IP 路由配置指导”中的“IP 路由基础”。

15.10 不同VRF或公网与VRF如何通过三层接口实现互访？

可通过多种方式实现不同 VRF 之间或公网与 VRF 之间通过三层接口实现互相访问：

- 配置静态路由实现三层接口路由互通：在执行 **ip route-static vpn-instance** 命令时，同时指定源和目的 VPN 实例，实现不同 VPN 实例下三层接口之间的路由互通；在执行 **ip route-static vpn-instance** 命令时，指定下一跳地址属于公网实例，实现公网与指定 VPN 实例的路由互通；在执行 **ip route-static** 命令时，同时指定下一跳地址属于 VPN 实例，实现公网与指定 VPN 实例的路由互通。
- 配置 BGP 路由协议实现三层接口路由互通：执行 **import-route** 命令引入不同 VPN 实例的 IGP 路由，实现三层接口路由互通。
- 配置路由信息引入功能实现三层接口路由互通：在 VPN 实例 IPv4 地址族视图下执行 **route-replicate** 命令，将公网或其他 VPN 实例的路由信息引入到指定 VPN 实例中；在公网实例 IPv4 地址族视图下执行 **route-replicate** 命令，将指定 VPN 实例的路由信息引入到公网中。

15.11 设备配置前缀大于64位的IPv6路由后为什么不生效？

部分产品需要通过指定命令行开启前缀大于 64 位的 IPv6 路由功能并重启设备后，前缀大于 64 位的 IPv6 路由才会生效。不同产品的开启命令行不同：

- 部分产品通过 **display switch-routing-mode status** 命令查看前缀大于 64 位的 IPv6 路由功能的配置情况。通过 **switch-routing-mode ipv6-128** 命令开启前缀大于 64 位的 IPv6 路由功能。

- 部分产品通过 **display hardware-resource routing-mode** 命令查看前缀大于 64 位的 IPv6 路由功能的配置情况。通过 **hardware-resource routing-mode ipv6-128** 命令开启前缀大于 64 位的 IPv6 路由功能。

15.12 部署OSPF后，为什么无法建立邻居关系？

OSPF 邻居无法建立的常见原因主要包括：

- 物理连接和下层协议故障
- 接口没有 up
- 两端 IP 地址不在同一网段
- Router ID 配置冲突
- 两端区域类型不一致
- 两端 OSPF 参数配置不一致

请尝试按照如下步骤排除故障：

(1) 使用 **display ospf interface** 命令查看 OSPF 接口的信息。如果接口状态为 Down，表明此接口没有发送和接收任何路由协议的报文，请检查接口是否 up。

(2) 检查物理连接及下层协议是否正常运行，可通过 **ping** 命令测试。若从本地路由器 Ping 对端路由器不通，则表明物理连接和下层协议有问题。

(3) 检查接口上配置的 OSPF 参数，必须保证与相邻路由器的参数一致，区域号相同，网段与掩码也必须一致（点到点与虚连接的网段与掩码可以不同）。如果配置了验证，需要保证：

- 如果使用 OSPF 区域验证，需要保证一个区域中所有路由器的验证模式和验证密码必须一致。如果引用 keychain 验证方式，必须使用 OSPF 能够支持的验证算法。
- 如果使用 OSPF 接口验证，需要保证同一网段的接口的验证字口令必须相同。如果引用 keychain 验证方式，必须使用 OSPF 能够支持的验证算法。

(4) 检查 OSPF 定时器，在同一接口上邻居失效时间应至少为 Hello 报文发送时间间隔的 4 倍。

(5) 如果是 NBMA 网络，则应该使用 **peer ip-address** 命令手工指定邻居。

(6) 如果网络类型为广播网或 NBMA，则至少有一个接口的路由器优先级大于零。

16 组播

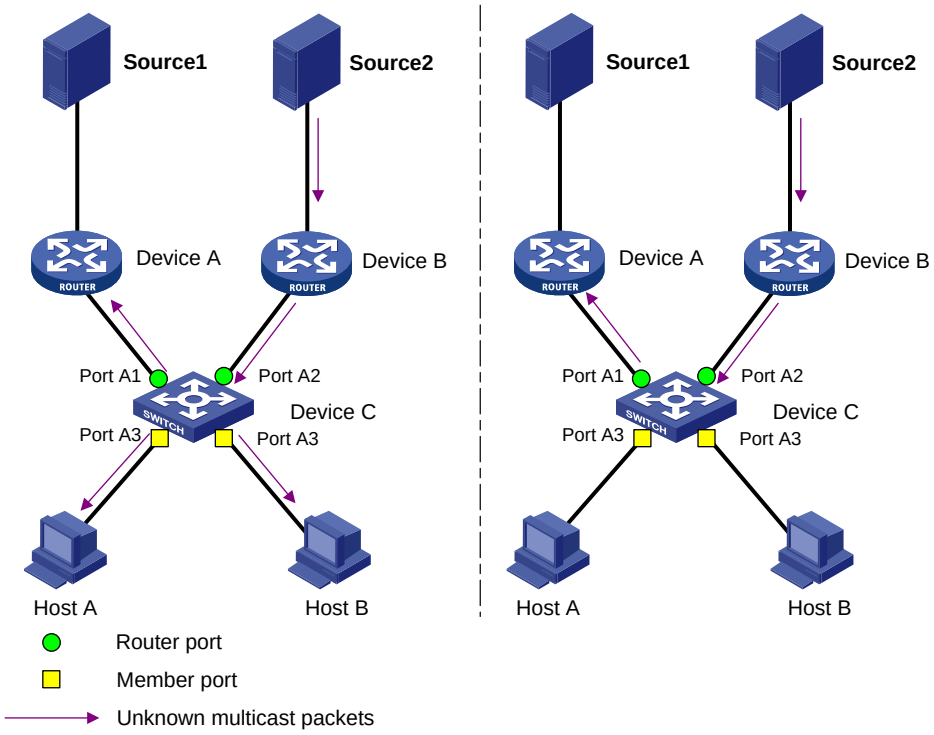
16.1 组播组网，接入设备配置二层组播后，为什么网络卡顿、延迟高？

需要配置未知组播数据报文丢弃功能。

当未配置丢弃未知组播数据报文功能时，二层设备收到未知组播数据报文时，会在未知组播数据报文所属的 VLAN/VSI 内广播该报文。当二层设备收到的大量未知组播报文时，网络中会充斥着大量的未知组播报文，从而导致网络卡顿、延迟高，如图 16-1 所示。

配置丢弃未知组播数据报文后，二层设备只向其路由器端口转发未知组播数据报文，不在 VLAN/VSI 内广播；如果二层设备没有路由器端口，未知组播数据报文会被丢弃，不再转发。

图16-1 配置丢弃未知组播数据报文功能前后的对比



16.2 组播组网，二层接入设备配置了IGMP Snooping和IGMP Snooping drop-unknown功能后，为什么组播转发表项异常？

需要将二层接入设备的 IGMP Snooping 版本配置为 3。

缺省情况下，二层设备开启 IGMP Snooping 功能后，设备上的 IGMP Snooping 版本为 2。当三层设备的 IGMP 版本和用户主机的 IGMP 版本为 3 时，二层设备收到用户主机发送的 IGMPv3 的成员关系报告报文后，无法处理 IGMPv3 的成员关系报文，将在 VLAN/VSI 内广播该报文。

将二层设备的 IGMP Snooping 版本修改为 3 后，IGMP Snooping 设备在收到 IGMP 成员关系报告报文时，二层设备将其通过 VLAN/VSI 内的所有路由器端口转发出去，从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做如下处理：

- 如果不存在该组播组所对应的转发表项，则创建转发表项，将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该组播组所对应的转发表项，但其出端口列表中不包含该端口，则将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该组播组所对应的转发表项，且其出端口列表中已包含该动态成员端口，则重置其老化定时器。

16.3 什么情况下需要配置查询器？是否可以配置多个查询器？

在运行了 IGMP 的组播网络中，会有一台三层组播设备充当 IGMP 查询器。该查询器负责发送 IGMP 查询报文，在网络层建立并维护组播转发表项，从而正常转发组播数据。

当组播组网中没有三层设备时，而二层设备不支持 IGMP。如果没有设备充当查询器，会导致无法建立组播转发表项。此时就需要在二层设备上开启 IGMP Snooping 查询器功能，从而能够在数据链路层建立并维护组播转发表项。

为了防止因单一IGMP Snooping查询器发生故障而引起组播业务中断，在同一网段、同一VLAN/VSI内可以配置多个查询器。但正常情况下，同一网段、同一 VLAN/VSI 内只需要一个查询器。过多的查询器会导致网络中充斥着大量的查询报文、组播接收者也会接收到多份同样的数据报文，导致网络非常拥塞。

通过在设备上开启 IGMP Snooping 查询器选举功能可以解决这个问题。选举出的 IGMP Snooping 查询器发生故障无法正常工作后，VLAN/VSI 内各设备会重新选举出新的 IGMP Snooping 查询器以保证组播业务正常转发。

16.4 同一PIM域内，配置三层组播功能后，三层组播流量不通？

本类故障的常见原因主要包括：

(1) 单播路由不通。

(2) 未开启 **multicast routing** 功能。

(3) 未正确配置 PIM 和 IGMP 功能。

(4) 对于 PIM-SM 或双向 PIM 网络，没有配置 RP 或 RP 信息不正确。

(5) 转发组播数据的接口上配置了组播边界。

(6) 对于 PIM-SM 或双向 PIM 网络，配置了错误的组播源过滤策略。

(7) 组播转发表项未生成。

问题定位过程如下：

(1) 检查组播转发路径上单播路由是否正常。使用 **ping** 命令检查组播源与组播接收者间的单播路由是否正常。若无法 ping 通，使用 **display ip routing-table** 命令查看路由表项是否存在到达组播源和组播接收者的路由。若没有，请先排查单播路由配置是否正确。若单播路由没有问题，请执行步骤（2）。

(2) 检查所有三层组播设备上是否开启了 **multicast routing** 功能。缺省情况下，**multicast routing** 功能处于关闭状态。在系统视图下，使用 **display this** 命令查看是否开启了 **multicast routing**。若所有三层组播设备上开启了 **multicast routing** 功能，请执行步骤（3）。

(3) 检查是否正确配置 PIM 和 IGMP 功能。在组播转发路径上，除连接组播接收者的端口上，均需要开启 PIM 功能；连接组播接收者的端口上，需要开启 IGMP 功能。在接口视图，使用 **display this** 命令查看当前端口上是否配置了 **igmp enable** 或者 **pim dm**、**pim sm**。若所有设备上正确配置 PIM 和 IGMP 功能：

a. 对于 PIM SM 或者双向 PIM 网络，请执行步骤（4）。

b. 对于 PIM DM 网络，请执行步骤（5）。

(4) 对于 PIM-SM 或双向 PIM，检查是否配置了 RP 且 RP 信息配置是否正确。在设备上使用 **display pim rp-info** 查看不同设备上的 RP 信息是否正确，主要检查如下字段：Scope、Group/MaskLen、RP address，确认服务于相同组播组的 RP 地址是否在相同、是否在相同的 PIM 域内。若 RP 信息不正确，请在所有设备上执行 **c-rp/static-rp** 命令将为某组播组服务的 RP 地址配置为一致，若 RP 信息配置正确，请执行步骤（5）。

(5) 检查组播转发路径上的接口是否配置了组播转发边界。在转发组播数据的接口上执行 **display this** 命令，查看接口的配置信息中是否配置 **multicast boundary** 命令。若存在，使用 **undo multicast boundary** 命令删除该配置。若不存在，请执行步骤（6）。

(6) 检查组播转发路径上是否配置了组播数据过滤器。在组播转发路径的设备上，进入 PIM 视图，使用 **display this** 命令查看是否配置了 **source-policy** 命令。若配置了，检查过滤策略是否正确。若过滤策略不正确，请删除该过滤器或者通过 **source-policy** 命令调整组播数据报文的源地址范围。若没有配置，请执行步骤（7）。

(7) 检查组播表项是否存在。

a. 通过 **display pim routing-table** 命令检查设备上 PIM 路由表项是否存在。对于连接组播接收者的设备，设备上应该存在（*，G）和（S，G）表项。对于没有连接接收者的 PIM 设备，设备上应该存在（S，G）表项。

b. 通过 **display multicast routing-table** 和 **display multicast fast-forwarding cache** 查看组播路由表和组播快速转发表是否存在。若这 2 个表项不存在，组播报文会转发失败。

c. 通过如上检查，若组播表项存在，组播数据仍然转发不通，请收集表项信息，然后请执行步骤（8）。

d. 若组播表项不存在，请执行步骤（8）。

(8) 请联系 H3C 技术支持人员。

17 安全

17.1 为什么配置了密码控制却不生效？

没有开启全局密码控制功能，需要先开启全局密码控制功能。

(1) 进入系统视图。

system-view

(2) 开启全局密码控制功能。

password-control enable

17.2 设备作为SSH服务器，为什么配置了NTP后登录不上设备？

检查设备是否开启了 password-control 功能，此功能开启后设备对密码的控制更加严格。在 password-control 功能开启时，密码存在老化时间，设备配置了 NTP 后系统时间发生改变，密码老化。此时可通过 console 口登录设备，关闭 password-control 功能即可。

(1) 进入系统视图。

system-view

(2) 关闭 password-control 功能。

undo password-control enable

系统时间修改完成后，如需使用 password-control 功能，可正常启用。关于 password-control 的详细描述请参见各产品“安全配置指导”中的“Password Control”。

17.3 为什么无法修改设备密码？

检查设备是否开启了password-control功能，此功能开启后密码更新的最小时间间隔功能默认开启。修改密码时，通常会看到设备提示Cannot change password until the update-wait time expires.此时可通过 **password-control update-interval** *interval* 命令修改密码更新的最小时间间隔。

17.4 设备作为SSH服务器，什么情况下需要修改认证超时时间？

缺省情况下，SSH用户的认证超时时间为60秒。

为了防止不法用户建立起 TCP 连接后，不进行接下来的认证而空占进程，妨碍其它合法用户的正常登录，可以设置认证超时时间，如果在规定的时间内没有完成认证就拒绝该连接。

如果认证超时时间设置过短，可能会造成SSH登录设备失败，设备返回Authentication timed out for x.x.x.x（用户实际IP地址），此时在系统视图下，使用 **ssh server authentication-timeout** 命令可调整认证超时时间。

17.5 设备作为SSH客户端，如何删除本地文件中的指定服务器公钥？

设备作为SSH客户端，在系统视图下执行 **delete ssh client server-public-key** 可以删除本地文件中的指定服务器公钥。

设备作为SSH客户端，登录SSH服务器后，在提示信息“Do you want to save the server public key?”后输入Y，设备会保存服务器公钥到本地文件。如果SSH客户端首次连接服务器后,服务器重新生成了公钥文件，会导致客户端的公钥文件与服务器不一致，SSH客户端登录服务器失败。通常会看到提示信息：The server's host key does not match the local cached key…这种情况下，可以通过 **delete ssh client server-public-key** 删除本地文件中的指定服务器公钥解决。

17.6 为什么启用了SSH服务器功能后，客户端连接到设备时提示连接中断？

执行 **ssh server enable** 命令开启设备Stelnet服务器功能并配置了相应的用户后，还需要配置Stelnet客户端登录时使用的VTY用户线。

(1) 进入系统视图。

system-view

(2) 进入VTY用户线视图。

line vty *number* [*ending-number*]

(3) 配置登录用户线的认证方式为scheme方式。

authentication-mode scheme

缺省情况下，用户线认证方式为 **password** 方式。

若没有配置用户线的认证方式为scheme方式，连接会自动中断，无法连接到设备。

18 ACL 和 QoS

18.1 QoS策略流分类中配置了多条匹配规则，为什么没有一条规则能够匹配到相应的流量呢？

请修改流分类规则之间的逻辑关系为 or。

当一个流分类中配置了多条 **if-match** 规则时，若指定流分类规则之间的逻辑关系为“and”时，数据包必须匹配全部规则才属于该类；若指定流分类规则之间的逻辑关系为“or”时，数据包只要匹配其中任何一个规则就属于该类。用户可通过 **traffic classifier** 命令修改各规则的逻辑关系。

18.2 应用ACL进行报文过滤、禁止某IP地址段的主机发出的报文通过，为什么不生效呢？

请检查 ACL **rule** 规则中 IP 地址的反掩码配置的是否正确。

使用 ACL 匹配报文的源或目的 IP 地址时，紧挨着 IP 地址后面输入的是反掩码，而不是掩码。

例如，如果您希望匹配 192.168.1.0/24 这个 IP 地址段的所有 IP 地址，您在 ACL 中使用 **rule** 命令配置的“IP 地址+反掩码”应为“**192.168.1.0 0.0.0.255**”。

18.3 在VLAN接口上应用ACL进行报文过滤，对二层转发报文不生效。

可通过如下两种方式之一解决：

- 请将 VLAN 接口上配置的报文过滤删除，然后在相应的二层以太网接口上重新配置。
- 对于支持 **packet-filter filter** 命令的设备，在 VLAN 接口视图下配置 **packet-filter filter all** 命令。此命令的缺省情况为 **packet-filter filter route**，即报文过滤仅对通过 VLAN 接口进行三层转发的报文生效。

18.4 为什么报文命中IP Source Guard表项，但却无法转发呢？

请执行以下命令，检查是否配置了报文过滤：

- **display packet-filter**
- **display acl**

若配置了报文过滤，请在报文过滤引用的 ACL 中配置软件统计规则。然后，使用 **display packet-filter statistics** 命令查看报文是否命中了报文过滤中的 deny 规则。

报文过滤优先级高于 IP Source Guard，所以当报文同时匹配报文过滤和 IP Source Guard 表项时，报文过滤优先生效。

18.5 ACL规则的匹配顺序是怎么样的？

当一个 ACL 中包含多条规则时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。ACL 的规则匹配顺序有以下两种：

- 配置顺序：按照规则编号由小到大进行匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，各类型 ACL 的“深度优先”排序法则如表 18-1 所示。

说明

可通过 **acl** 命令中的 **match-order { auto | config }** 参数指定规则的匹配顺序，**auto** 表示按照自动排序（即“深度优先”原则）的顺序进行规则匹配，**config** 表示按照配置顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。用户自定义 ACL 不支持本参数，其规则匹配顺序只能为配置顺序。

表18-1 各类型 ACL 的“深度优先”排序法则

ACL 类型	“深度优先”排序法则
IPv4基本ACL	**a** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **b** 如果 VPN 实例的包含情况相同，再比较源 IPv4 地址范围，较小者优先 **c** 如果源 IPv4 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv4高级ACL	**a** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **b** 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv4 承载的协议类型者优先 **c** 如果协议范围也相同，再比较源 IPv4 地址范围，较小者优先 **d** 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 **e** 如果目的 IPv4 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号的覆盖范围，较小者优先 **f** 如果四层端口号的覆盖范围无法比较，再比较配置的先后次序，先配置者优先
IPv6基本ACL	**a** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **b** 如果 VPN 实例的包含情况相同，再比较源 IPv6 地址范围，较小者优先 **c** 如果源 IPv6 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv6高级ACL	**a** 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 **b** 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv6 承载的协议类型者优先 **c** 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 **d** 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 **e** 如果目的 IPv6 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号的覆盖范围，较小者优先 **f** 如果四层端口号的覆盖范围无法比较，再比较配置的先后次序，先配置者优先
二层ACL	**a** 先比较源 MAC 地址范围，较小者优先 **b** 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 **c** 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少：“0”位越多，范围越小。通配符掩码（又称反向掩码）以点分十进制表示，并以二进制的“0”表示“匹配”，“1”表示“不关心”，这与子网掩码恰好相反，譬如子网掩码 255.255.255.0 对应的通配符掩码就是 0.0.0.255。此外，通配符掩码中的“0”或“1”可以是不连续的，这样可以更加灵活地进行匹配，譬如 0.255.0.255 就是一个合法的通配符掩码。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

19 可靠性

19.1 修改了VRRP备份组的VRRP使用版本后，VRRP为什么失效了？

VRRP 备份组中的所有设备上配置的 VRRP 版本必须一致。并且如果使用的是 VRRPv2 版本，则 VRRP 通告报文时间间隔也必须保持一致。

请在 VRRP 备份组中的所有设备上，通过执行 **display vrrp verbose** 命令，查看“Version”显示的当前 VRRP 备份组的 VRRP 版本，如果不一致，请执行 **vrrp version** 命令将版本修改一致。

如果版本均为 VRRPv2 版本，则继续通过执行 **display vrrp verbose** 命令，查看“Adver Timer”显示的当前配置的 VRRP 通告报文时间间隔，如果不一致，请执行 **vrrp vrid timer advertise** 命令将时间间隔修改一致。

19.2 VRRP备份组网，当Master设备上行链路状态down后，备份组为什么没有切换？

VRRP 自身并不具备链路状态检测能力，请在 VRRP 备份组的 Master 设备上，通过执行 **display vrrp verbose** 命令，查看“VRRP Track Information”是否关联了 Track 项。如果没有配置，请通过 **vrrp vrid track** 命令在 Master 设备上配置 VRRP 与 Track 联动、Track 与 NQA 或 BFD 联动，实现 VRRP Master 设备监视上行链路状态功能。

19.3 配置VRRP与Track联动监视Master设备上行链路状态，Track状态变为Negative时，为什么VRRP备份组中的主备未进行切换？

如果希望 Track 状态变为 Negative 时 VRRP 备份组进行主备切换，需要配置当被监视 Track 项的状态变为 Negative 时，Master 设备的优先级降低足够的数值，使得当前的 Master 设备的优先级不是组内优先级最高的设备，其它设备才会抢占成为新的 Master 设备。

请在 Master 设备上执行 **display vrrp verbose** 命令，查看“VRRP Track Information”中是否配置“Pri Reduced”，如果是配置“Weight Reduced”，则表示降低虚拟转发器的权重，请使用 **vrrp vrid track** 命令修改为降低 Master 设备的优先级。

如果配置了“Pri Reduced”，请继续查看 Master 设备的“Running Pri”（当前优先级）是否低于 VRRP 备份组中的其它设备，否则请使用 **vrrp vrid track** 命令加大“Pri Reduced”数值，使得 Master 设备降低优先级后低于其它设备的优先级。

19.4 支持拨码开关的IE系列交换机，配置RRPP相关功能并保存配置，设备重启后RRPP配置丢失是什么原因？

部分 IE 系列工业交换机支持两种 RRPP 配置方式：手工配置和通过拨码开关配置。

当拨码 4 置“ON”后，设备将进行如下配置：

(1) 创建 RRPP 域，设备的域 ID 为 domain 1。

(2) 指定主控制 VLAN 为 VLAN 4092，子控制 VLAN 为 VLAN 4093。

(3) 配置保护 VLAN 映射到 MSTP instance 0 上。

(4) 配置 RRPP 环和 RRPP 节点。设备为传输节点，并指定主端口和副端口。其中接入 RRPP 环的端口中，端口号小的作为主端口，端口号大的作为副端口。

(5) 激活 RRPP 域。

设备启动时，先轮询检测拨码开关的状态，当拨码开关处于“ON”时，设备自动完成以上配置。如果配置文件中的配置与拨码开关配置冲突，例如配置文件创建 RRPP domain 2，并指定其控制 VLAN 为 VLAN 4093，与 RRPP domain 1 子控制 VLAN 相同，则配置恢复失败。

为避免出现以上问题，如果需要同时使用拨码开关和手工配置，请确保手工配置内容与拨码开关配置不存在冲突。

20 网络管理与监控

20.1 PoE端口无法正常供电的常见原因有哪些？

如果出现设备开启 PoE 接口供电功能后 PoE 接口频繁 up/down、PoE 交换机只能给部分的 PD 正常供电或者 PoE 交换机端口模式指示灯不亮等现象，可能是由于以下原因引起的。

(1) 未开启接口 PoE 功能

确认设备电源、电缆正确连接的情况下，首先可以使用 **display poe interface** 命令查看设备 PoE 接口的供电状态。如果显示信息的 PoE Status 字段为 Disabled，则接口 PoE 功能是关闭状态，可以在 PoE 接口视图下执行命令 **poe enable** 来开启 PoE 功能。

(2) 未开启非标准 PD 检测功能

受电 PD 设备分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE 802.3af 和 IEEE 802.3at 标准的 PD 设备。如果是非标准 PD 供电，只有在开启非标准 PD 检测功能后，PSE 才对非标准 PD 供电。设备支持以下两种非标准 PD 检测功能的配置，使用任意一种配置方式均可开启该功能。

- 方法一：在系统视图下执行命令 **poe legacy enable pse** *pse-id* 开启 PSE 的非标准 PD 检测功能

- 方法二：在 PoE 接口视图下执行命令 **poe legacy enable** 开启 PoE 接口的非标准 PD 检测功能

(3) 未升级 PSE 固件

确认不是由上述 1、2 的原因导致 PoE 端口无法正常供电，该问题很可能是由于未升级 PSE 固件引起。

在进行在线升级操作前，请先联系 H3C 技术支持获取最新 PSE 固件版本文件。升级有以下两种模式：

- **refresh** 模式：在系统视图执行命令 **poe update full** *filename* [**pse** *pse-id*]（由于该模式升级过程简单快速，一般情况下推荐使用该模式来升级 PSE 固件。）
- **full** 模式：在系统视图执行命令 **poe update full** *filename* [**pse** *pse-id*]

需要注意的是，如果PSE固件的升级过程因设备重启而中断，重启完成后用**full**方式升级失败时，请将设备断电重启后再用 **full** 方式升级即可升级成功。

具体操作步骤，以采用 **refresh** 模式在线升级 PSE 4 固件为示例：

```
<Sysname> system-view
[Sysname] poe update refresh POE-168.bin pse 4
```

20.2 为什么NMS对设备的远程管理和操作出现异常？

NMS 和 Agent 能够建立 SNMP 连接后，很可能是由以下原因导致。

如果出现无法读取设备信息，NMS 对设备的远程管理和操作异常、NMS 无法收到设备发出的告警信息等异常情况。请按照以下顺序对配置进行排查：

1、确认版本一致。

请确认在 NMS 和 Agent 配置的 SNMP 版本是否一致。对此可以执行命令 **display snmp-agent sys-info** 查看设备配置的 SNMP 版本，如果 NMS 和 Agent 配置的 SNMP 版本不一致，可以在系统视图下执行命令执行命令 **snmp-agent sys-info version** 配置 SNMP 版本。

需要注意的是，设备运行于非 FIPS 模式时，支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本；设备运行于 FIPS 模式时，只支持 SNMPv3 版本。

2、确认团体名一致。

确保 NMS 和 Agent 使用的 SNMP 版本相同时，如果 NMS 仍不能读取到 Agent 的信息，可以执行命令**display snmp-agent community** 查看 SNMPv1 或 SNMPv2c 的团体名，如果 NMS 和 Agent 配置的团体名不一致，可以使用以下两种方式配置团体：

- 方法一：基于名称配置 SNMPv1/v2c 团体

  使用该方法直接执行命令创建团体有以下两种方式：

  - VACM 方式：在系统视图下执行命令 **snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *
  - RBAC 方式：在系统视图下执行命令 **snmp-agent community** [**simple** | **cipher**] *community-name* **user-role** *role-name* [**acl** { *ipv4-acl-number* | **name**

ipv4-acl-name } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

- 方法二：基于用户配置 SNMPv1/v2c 团体

  首先在系统视图下执行命令 **snmp-agent group** { **v1** | **v2c** } *group-name* [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { **ipv4-acl-number** | **name** *ipv4-acl-name* } | **acl ipv6** { **ipv6-acl-number** | **name** *ipv6-acl-name* }] *创建 SNMPv1/v2c 组；

  其次再执行命令 **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *创建 SNMPv1/v2c 用户。

以上两种团体配置方式，效果相同。如果采用第二种方式配置团体，创建的 SNMPv1/v2c 用户名相当于SNMPv1/v2c的团体名。如需删除SNMP团体，可以在系统视图下执行命令**undo snmp-agent community**。

20.3 设置本地时钟作为参考时钟会影响NTP客户端和服务器进行时间同步吗？

会影响。

实际网络中，通常将从权威时钟（如原子时钟）获得时间同步，并将其作为主时间服务器同步网络中其他设备的时钟，该情况不需要设置本地时钟作为参考时钟。

只有在某些特殊网络中，例如无法与外界通信的孤立网络，网络中的设备无法与权威时钟进行时间同步。此时，可以从该网络中选择一台时钟较为准确的设备，在系统视图下执行命令 **ntp-service refclock-master** [*ip-address*] [*stratum*]，指定该设备与本地时钟进行时间同步，即采用本地时钟作为参考时钟，使得设备的时钟处于同步状态。

请谨慎使用本配置，以免导致网络中设备的时间错误，影响 NTP 客户端和服务器进行时间同步。

20.4 配置客户端/服务器模式下的NTP，服务器端的时钟层数是否要小于客户端的时钟层数？

是。当 NTP 服务器端的时钟层数大于或等于客户端的时钟层数时，NTP 客户端将不会其进行时间同步。

20.5 NTP客户端/服务器时间不同步，时间相差若干小时的原因是什么？

客户端的夏令时、时区和服务器上的配置不一致。因为 NTP 客户端从服务器同步的是 UTC 时间，如果服务器上配置了夏令时、时区，请在客户端上执行 **clock timezone** 和 **clock summer-time** 命令，让客户端的夏令时、时区和服务器上的配置保持一致。

20.6 什么情况下需要配置PTP接口角色才能实现PTP时间同步，有哪些配置限制？

一般建议使用 BMC 协议自动协商 PTP 接口角色。

配置 PTP 接口角色适用于但不限于以下几种情况：

- 网络中只有少量 PTP 接口
- BMC 协议自动协商 PTP 接口角色失败，造成网络中有多个接口状态为 Master。

网络中是否有多个接口状态为 Master，可以执行命令 **display ptp interface brief** 查看接口的角色。请确保网络中只有一个接口状态为 Master 用于对外发布时间信息，如果有多个接口状态为 Master，可以在接口视图下执行命令 **ptp force-state** 命令强制修改 PTP 接口的角色。

配置限制

- 如果修改了 PTP 接口角色，则整个 PTP 域内的所有 PTP 接口均需手工执行命令 **ptp force-state** 命令配置角色，否则会导致 PTP 域内未配置角色的接口 PTP 功能不生效，域内时钟不能同步。
- 必须先配置 PTP 协议标准、时钟节点类型和 PTP 域后，才允许配置该命令。
- 一台设备上最多只允许配置一个从接口。

20.7 为什么无法通过云平台（绿洲云）远程管理设备？

请确认设备是否支持通过云平台远程管理设备，对于支持通过云平台远程管理的设备，请参考“网络管理和监控配置指导”中的“云平台连接”。

对于支持通过云平台远程管理的设备，若无法通过云平台远程管理设备，请排查是否配置了如下配置：

- 配置云平台服务器域名。可以通过 **display current-configuration** 命令查看设备是否配置了云平台服务器域名，如果未配置，则需要通过 **cloud-management server domain** *oasis.h3c.com* 命令配置设备连接的云平台服务器域名。
- 配置正确的域名解析，以便将云平台服务器的域名解析为正确的 IP 地址。
- 在云平台服务器上添加待管理设备的序列号。可以通过 **display device manuinfo** 命令查看设备序列号，将序列号添加到云平台上。

20.8 设备产生的日志信息过多，如何处理？

信息中心是设备的信息枢纽，它接收各模块生成的日志信息，能够按模块和等级将收到的日志信息输出到控制台、监视终端、日志主机等方向，为管理员监控设备运行情况和诊断网络故障提供了有力的支持。

但是如果设备在短时间内产生大量的日志信息，会造成 INFO 进程 CPU 使用率比较高，主要通过以下几种方法解决：

(1) 排查这些日志信息产生的原因：根据设备记录的日志信息内容，排查这些信息产生的原因，从根本上解决问题。例如：设备有大量端口的 UP/DOWN 信息输出，那么就要排查对应的端口是否有问题，端口 UP/DOWN 的问题解决后，日志信息就不再产生。

(2) 修改日志信息的输出级别：如果无法阻止日志信息的产生，可以修改日志信息的输出级别，使这些无用的信息不再向指定方向输出。例如：只允许 VLAN 模块信息级别为 notification 及以上的日志信息（即等级 0～5 的日志信息）输出到控制台，修改方法为：**info-center source vlan console level notification**。

(3) 禁止指定应用模块日志信息的输出：如果某个模块的日志信息管理员不需要关注，可以禁止该模块的日志信息输出到指定的方向。例如：禁止 Portal 模块信息输出到监视终端，修改方法为：**info-center source portal monitor deny**。

21 VXLAN

21.1 为什么设备上无法配置VXLAN特性相关的命令？

若设备上无法配置 VXLAN 特性相关的命令，请排查是否存在如下问题：

(1) 确认设备是否支持 VXLAN 特性。

(2) 部分设备上只有特定的工作模式下支持 VXLAN 特性，不同设备上工作模式的配置方式可能不同：

- 部分设备上：通过 **display switch-mode status** 命令查看设备是否处于 VXLAN 工作模式；若未处于 VXLAN 工作模式，则通过 **switch-mode** 命令将设备配置为 VXLAN 工作模式，并保存配置重启设备。
- 部分设备上：通过 **display system-working-mode** 命令查看设备的工作模式；若设备目前处于不支持 VXLAN 的工作模式，则需要通过 **system-working-mode** 命令将设备切换为支持 VXLAN 的工作模式，修改工作模式需要保存配置重启设备。

(3) 部分设备上不同的角色需要使用不同的硬件资源模式，如果硬件资源模式与配置不匹配，可能导致配置无法执行。通过 **display hardware-resource vxlan** 命令可以查看设备 VXLAN 的硬件资源模式；通过 **hardware-resource vxlan** 命令可以配置 VXLAN 的硬件资源模式，修改 VXLAN 的硬件资源模式需要保存配置并重启设备。

产品对 VXLAN 特性的具体要求请参见“VXLAN 配置指导”中的“VXLAN”。