常见问题答复集（七）

H3C交换机基础维护篇

精选Q&A

《常见问题答复集》第七期来啦！

本期主要内容：安全篇、ACL和QoS篇、可靠性篇、网络管理与监控篇。

安全篇

Q1 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

Q2 设备作为SSH服务器，为什么配置了NTP后登录不上设备？

需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。

Q3 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。

Q4 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。

Q5 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。

ACL和QoS篇

Q1 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？

请执行display traffic classifier命令检查流分类的规则关系是否为“or”，如果不是，请改为“or”。

当一个流分类中配置了多条if-match规则时，各条规则之间的关系是“与”还是“或”，是由traffic classifier *classifier-name* [operator { and | or }]命令中的“and”和“or”决定的，缺省情况下是“and”

“and”表示流量必须匹配流分类中的所有规则，才表示流量命中该流分类；而“or”表示流量只要匹配流分类中的任意一条规则，就表示流量命中该流分类。

Q2 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”。

Q3 在VLAN接口上应用ACL进行报文过滤，为什么对二层转发报文不生效？

可通过如下两种方式之一解决：

1. 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。

2. 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。

Q4 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：

1. display packet-filter

2. 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。

可靠性篇

Q1 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。

Q2 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。

Q3 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。

Q4 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。

(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，接入RRPP环的端口中，端口号小的为主端口，端口号大的为副端口。

(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。

网络管理与监控篇

Q1 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。

Q2 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客户端将不会进行时间同步。

Q3 NTP客户端/服务器时间不同步，时间相差八个小时的原因是什么？

因为没有配置北京时区，请执行命令clock timezone beijing配置北京时区。

Q4 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：

1. 网络中只有少量PTP接口。

2. 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：

1. 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。

2. 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。

3. 一台设备上最多只允许配置一个从接口。

—— end ——

H3C Service

扫码关注我们哦