常见问题答复集（四）

H3C交换机基础维护篇

精选Q&A

《常见问题答复集》第四期来啦！

本期主要内容：接入认证篇(上)

接入认证篇（上）

Q1 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

(1) 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。

(2) 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。

(3) 对于Portal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，可通过display domain命令查看default domain name

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。

Q2 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，通过default domain name字段的显示信息查看当前缺省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：

1. 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，然后才可以删除。

2. 系统缺省存在的system域只能被修改，不能被删除。

Q3 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。

Q4 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地址一致，来决定是否处理来自该接入设备的认证或计费请求。

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。

在接入设备上配置NAS-IP的方法有：

1. RADIUS方案视图下，通过命令nas-ip { *ipv4-address* | interface *interface-type interface-number* |ipv6 *ipv6-address* }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。

2. 系统视图下，通过命令radius nas-ip { interface *interface-type interface-number* | { *ipv4-address* | ipv6 *ipv6-address* } [vpn-instance *vpn-instance-name*] }配置NAS-IP，对所有RADIUS方案有效。

配置NAS-IP的注意事项：

1. 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。

2. 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。

Q5 什么是802.1x在线用户握手？如何开启在线用户握手功能？哪些相关场景可能导致认证失败？

802.1x用户在线期间，设备端会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。客户端收到握手报文后，向设备发送应答报文，表示用户仍然在线。可以通过开启设备的在线用户握手功能来实现这种监测。

一般情况下，只有当802.1X客户端需要收到在线握手成功报文时，才需要开启端口发送在线握手成功报文功能，但有些802.1X客户端如果没有收到设备回应的在线握手成功报文，就会自动下线。为了避免这种情况发生，需要在端口上通过dot1x handshake reply enable命令开启发送在线握手成功报文功能，该功能缺省关闭。

以下场景可能会导致802.1x认证失败：

1. 若客户端不支持握手报文交互过程，可能导致认证失败，需要执行命令undo dot1x handshake关闭在线握手功能。

2. 若客户端需要收到设备的握手成功报文，但设备未开启在线用户手功能可能导致认证失败，可通过dot1x handshake reply enable命令开启该功能。

3. 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。

Q6 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。

安全握手功能仅能在iNode客户端和iMC服务器配合使用的组网环境中生效。

Q7 在线握手成功报文功能有哪些使用限制？

端口上开启在线用户握手功能后，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，就会自动下线。为了避免这种情况发生，需要在端口上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。

Q8 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。常见的以下情况均会导致上线失败：

1. 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。

2. 设备上与IMC配置的授权密码不一致，会导致无法上线。

3. 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。

Q9 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，该功能关闭。

通常不建议开启该功能，只有在用户有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。

Q10 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（部分产品不支持二层聚合口）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。

Q11 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。

—— end ——