常见问题答复集（五）

H3C交换机基础维护篇

精选Q&A

《常见问题答复集》第五期来啦！

本期主要内容：接入认证篇(下）

接入认证篇

Q1 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：

1、802.1X认证关闭。

2、MAC地址认证关闭。

3、端口未加入业务环回组。

4、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。

Q2 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。

Q3 如何配置对RADIUS 15号属性的检查方式？

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。

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。

Q4 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。

Q5 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。

Q6 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。

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：

1、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。

2、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。

3、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。

4、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。

Q7 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50100监听该报文，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。

Q8 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没有收到客户端的响应，则重发该报文。

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。

Q9 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。

Q10 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：

1、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的最小值，可通过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。

2、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。

Q11 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设置为30秒以上，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。

—— end ——

扫码关注我们哦