交换机如何配置802.1X认证逃生

802.1X Radius AAA **Sakuray** 2023-02-04 发表

组网及说明

802.1x认证逃生可以分为两种情况，一是主服务器不可达转到备服务器，二是全部服务器不可达改用其他认证方式。

这里以radius方案为例，其他协议原理类似，具体请参考对应的配置手册

配置步骤

情况一：主服务器不可达转到备服务器

这里可以利用secondary的命令在radius scheme视图下配置备份的认证/计费服务器，以5130S-EI交换机为例，一个RADIUS方案中最多允许配置一个主认证服务器和16个从认证服务器。缺省情况下，当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为active的从服务器并与之交互。开启服务器负载分担功能后，设备会根据各服务器的权重以及服务器承载的用户负荷，按比例进行用户负荷分配并选择要交互的服务器。

典型配置如下：

创建RADIUS方案radius1并进入其视图。

[Device] radius scheme radius1

配置主认证/计费RADIUS服务器的IP地址。

[Device-radius-radius1] primary authentication 10.1.1.1

[Device-radius-radius1] primary accounting 10.1.1.1

配置备份认证/计费RADIUS服务器的IP地址。

[Device-radius-radius1] secondary authentication 10.1.1.2

[Device-radius-radius1] secondary accounting 10.1.1.2

情况二：改用其他认证方式

在认证ISP域中，可以选用多种认证/授权/计费的方法，在当前的认证/授权/计费方法无效时，会按照配置顺序尝试使用备选的方法完成认证。

例如，radius-scheme radius-scheme-name local none表示，先进行RADIUS认证，若RADIUS认证无效则进行本地认证，若本地认证也无效则不进行认证。远程认证无效是指，指定的认证方案不存在、认证报文发送失败或者服务器无响应。本地认证无效是指没有找到对应的本地用户配置。none表示不进行认证，对用户非常信任，不对其进行合法性检查，直接可以访问资源。

典型配置如下：

创建并进入名称为bbb的ISP域。

[SwitchA] domain bbb

为用户配置AAA认证方法为RADIUS认证/授权/计费，且均使用RADIUS方案 radius1。先进行RADIUS认证，若RADIUS认证无效则进行本地认证，若本地认证也无效则不进行认证。

[Device-isp-bbb] authentication lan-access radius-scheme radius1 local none

[Device-isp-bbb] authorization lan-access radius-scheme radius1 local none

[Device-isp-bbb] accounting lan-access radius-scheme radius1 local none

[Device-isp-bbb] quit

开启端口GigabitEthernet1/0/1的802.1X认证。

[SwitchA] interface gigabitethernet 1/0/1

[SwitchA-GigabitEthernet1/0/1] dot1x

指定端口上接入的802.1X用户使用认证域bbb。

[SwitchA-GigabitEthernet1/0/1] dot1x mandatory-domain bbb

[SwitchA-GigabitEthernet1/0/1] quit

开启全局802.1X认证。

[SwitchA] dot1x

配置关键点

除了上述两种逃生方式，802.1X还涉及两种VLAN：

802.1X Auth-Fail VLAN功能允许用户在认证失败的情况下访问某一特定VLAN中的资源，这个VLAN称之为Auth-Fail VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。根据端口的接入控制方式不同，Auth-Fail VLAN的生效情况有所不同。具体请参考设备的配置手册。

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。根据端口的接入控制方式不同，Critical VLAN的生效情况有所不同。具体请参考设备的配置手册。