802.1x配置

目 录

第 1 章　配置 802.1x

1.1　配置802.1x任务列表

- 配置端口的 802.1x 认证
- 配置 802.1x 多主机端口认证
- 配置 802.1x 的重认证
- 配置 802.1x 的认证重试次数
- 配置 802.1x 发送频率
- 配置 802.1x 用户绑定
- 配置 802.1x 端口的认证方法
- 选择 802.1x 端口的认证类型
- 配置端口的 mab 认证
- 配置 802.1x 记账
- 配置 802.1x guest-vlan
- 禁止拥有多网卡的 Supplicant
- 802.1x 恢复默认配置
- 监控 802.1x 认证配置和状态

1.2　配置802.1x任务

1.2.1　配置端口的 802.1x 认证

802.1x 定义了三种端口的控制方式：强制认证通过、强制认证不通过和启动 802.1x 认证。

强制认证通过，表示端口已经认证通过，不需要再对端口进行认证，所有的用户都可以通过该端口进行数据访问控制；该模式是端口的默认模式。强制认证不通过，表示端口认证不通过，即使使用任何认证手段对端口进行认证，该端口都不会认证通过，所有的用户都无法通过该端口进行数据访问控制。

启动 802.1x 认证，即端口将运行 802.1x 认证协议，对访问该端口的用户进行 802.1x 认证，只有认证通过后用户都可以通过该端口进行数据访问控制。启动端口的 802.1x 的认证后还要配置 AAA 的认证方法。

在配置 802.1x 前，必须将 802.1x 功能使能，使用下面的命令可以使能 802.1x：

命令	目的
dot1x enable	使能802.1x功能 。

使用下面的命令可以启动 802.1x 认证：

命令	目的
dot1x port-control auto	配置端口为802.1x协议认证模式。
aaa authentication dot1x {default |list name} method	配置802.1x的AAA认证。

选择 802.1x 控制方式，可以在接口配置模式下使用下面的任意一个命令：

命令	目的
dot1x port-control auto	端口启动802.1x认证。
dot1x port-control force-authorized	端口强制认证通过。
dot1x port-control force-unauthorized	端口强制认证不通过。

1.2.2 配置 802.1x 多用户认证

802.1x 端口访问控制主要是对单个用户进行认证，其他用户不能同时进行认证和访问，除非前一个用户退出认证、访问过程。实际上，认证端口可能与多个用户相连接，为了使这些用户都能进行认证、访问，可以启动多用户认证功能。

多用户认证包含两种模式，一种是 multiple-hosts 模式：当用户进行认证时，只需要其中某一用户通过认证，就将端口置为 up 状态，其他用户无需认证也可以通过该端口进行访问；另一种是 multiple-auth 模式：交换机将对每个用户分别进行认证，每个用户认证之间互不影响。只要有一个用户认证成功，端口就 up，只有当所有的用户都认证失败，即认证端口下不存在认证成功的用户时，端口才 down。这样可以保证对每个用户分别认证，且一个用户认证失败不影响其他用户的正常访问权限。

注意：multi-auth 模式与 guest vlan 功能不能同时配置，与 mab 认证不能同时配置。修改端口的多用户认证模式后，会对端口下所有用户进行重新认证。

激活 802.1x 多主机端口认证，可以在接口配置模式下使用下面的任意一个命令：

命令	目的
dot1x authentication multiple-hosts	设置802.1x多主机端口访问模式。只需一个用户认证通过，端口就up。
dot1x authentication multiple-auth	设置802.1x多主机端口认证模式。每个用户认证之间互不影响。

1.2.3 配置 802.1x 的重认证

在认证通过后，为了保证认证客户端的合法性，间隔一段时间后还会向客户端发起认证，这时就需要启动重认证功能。

启动重认证功能，当端口认证通过以后，将会周期性的向主机进行认证请求。

配置重认证功能，可以使用下面的命令：

命令	目的
dot1x re-authentication	启动重认证功能。
dot1x timeout re-authperiod *time*	配置重认证的周期。

1.2.4 配置 802.1x 的认证重试次数

在认证失败之后，交换机会继续发送 request/ID 报文来发起认证，当超过该次数的认证后，客户机依然没有响应，认证将会被挂起。

配置重复认证次数的功能，可以使用下面的命令：

命令	目的
dot1x reauth-max *time*	配置重认证失败后的重试次数。

1.2.5 控制 802.1x 发送频率

802.1x 认证过程中，它会向客户主机发送数据报文，通过控制 802.1x 发送频率可以调节数据发送以保证客户主机的响应。

配置发送频率，可以使用下面的命令：

命令	目的
dot1x timeout tx-period *time*	设定802.1x报文发送频率。

1.2.6 配置 802.1x 用户绑定

802.1x 认证时，可以将用户与某一个端口进行绑定，保证端口访问的安全。启动 802.1x 用户绑定功能，可以在接口配置模式下使用下面的命令：

命令	目的
dot1x user-permit *xxxz*	配置端口下绑定的用户。

1.2.7 配置 802.1x 端口的认证方法

802.1x 认证时不同的端口可以使用不同的认证方法，缺省时，802.1x 认证使用 default 方法。

配置 802.1x 认证方法，可以在接口配置模式下使用下面的命令：

命令	目的
dot1x authentication method *yyy*	配置802.1x认证方法。

1.2.8 选择 802.1x 端口的认证类型

802.1x 认证时可以选择认证类型，该类型将决定 AAA 使用 Chap 或 Eap 认证(eap 认证支持 md5-challenge 和 eap-tls 方式)；使用 Chap 时 MD5 所需的 challenge 将在本地产生，而使用 Eap 时 challenge 将在认证服务器上产生；每一个端口只使用一种认证类型，默认情况下该类型使用全局配置的认证类型，当端口配置了认证类型时就一直使用该认证类型，除非使用 No 命令恢复到默认值。

eap-tls 采用电子证书作为认证凭证，遵循 tls(Translation Layer Security)中 handshake 协议规范，具有更好的安全性。

配置认证类型，可以在全局配置模式下使用下面的命令：

命令	目的
dot1x authen-type {chap|eap}	选择chap或eap。

也可以在接口配置模式下使用下面的命令：

命令	目的
dot1x authentication type {chap|eap}	选择chap或eap或使用全局下的配置类型。

1.2.9 配置端口的 mab 认证

当对端设备无法使用 802.1x 客户端软件时，交换机使用 Mab(MAC Authentication Bypass)认证方式，将对端设备的 mac 地址作为用户名和密码发往 radius 服务器进行认证。

注意：交换机上可以通过 dot1x mabformat 命令指定账号、密码格式，确保其与 radius 服务器上的设置一致。

开启 mab 功能后，如果对端设备既没有发送 eapol_start 报文，也没有响应 request_identity 报文，超时后，交换机认为对端设备不支持 802.1x 认证客户端，转而进入 mab 认证过程。交换机将获取到的设备的 mac 地址作为用户名和密码发送给 radius 服务器进行认证，如果在 radius 服务器上已经授权该 mac 地址，则认证成功，交换机允许用户通过该端口访问网络。

注意：开启 mab 认证时，不能同时配置 multi-auth 多主机认证模式。

开启 mab 认证，可以在接口配置模式下使用下面的命令：

命令	目的
dot1x mab	端口上开启mab认证功能。

可以在全局配置模式下使用下面的命令配置 mac 地址的格式：

命令	目的
dot1x mabformat{1|2|3|4|5|6}	可以选择格式1到格式6之间的六种mac地址格式中的一种。默认为格式1。

1.2.10 配置 802.1x 记帐

采用 dot1x 认证的同时，可以进行记帐，实现机制是，在 dot1x 认证通过后，判断是否在该认证接口下打开了记帐功能，如果是，则使用 AAA 接口发送记帐请求，在收到 AAA 模块的请求成功信息后，该接口才可以通过报文。

记帐方法可以采用 AAA 配置中各种记帐方法，相关内容请参考 AAA 配置。

为了保证记帐信息的准确性，在记帐开始后，dot1x 会周期性的使用 AAA 接口向 server 端发送 update 信息，但根据 AAA 配置的不同，AAA 模块决定是否真正发送该报文。

同时，请打开 dot1x 重认证功能，确保 supplicant 出现异常时，能够被交换机知晓。

为了打开 dot1x 记帐功能及配置记帐采用的方法，可以在接口配置模式下使用下面的命令：

命令	目的
dot1x accounting enable	打开802.1x记帐功能
dot1x accounting method {*method name***}**	配置记帐方法，缺省为default

1.2.11 配置 802.1x guest-vlan

Guest-vlan 功能可以在客户端没有响应时，给予相应端口有限的访问权限（例如下载客户端软件）。Guest-vlan 可以是系统中任何一个已配置的 vlan，如果配置的 guest-vlan 不满足该条件，则该端口无法进入该 guest-vlan。

注意：认证失败没有访问权限。

全局模式下打开 guest-vlan 功能，使用下面的命令：

命令	目的
dot1x guest-vlan	在所有端口下打开guest-vlan功能

初始时，每个端口的 guest-vlan id 为 0,此时即使打开了全局 guest-vlan 功能，也不起作用，只有在端口配置模式下，配置了 guest-vlan id 后，guest-vlan 才起作用。

端口模式下使用下面命令配置 guest-vlan id:

命令	目的
dot1x guest-vlan {id(1-4094)}	在端口下配置guest-vlan的Vlan id

1.2.12 禁止拥有多网卡的 Supplicant

禁止拥有多张网络适配器的 Supplicant 端，防止代理的发生。可以在端口配置模式下使用下面的命令：

命令	目的
dot1x forbid multi-network-adapter	禁止拥有多张网络适配器的Supplicant端。

1.2.13 802.1x 恢复默认配置

将所有的全局配置恢复到默认配置。可以在全局配置模式下使用下面的命令：

命令	目的
dot1x default	将所有的全局配置恢复到默认配置。

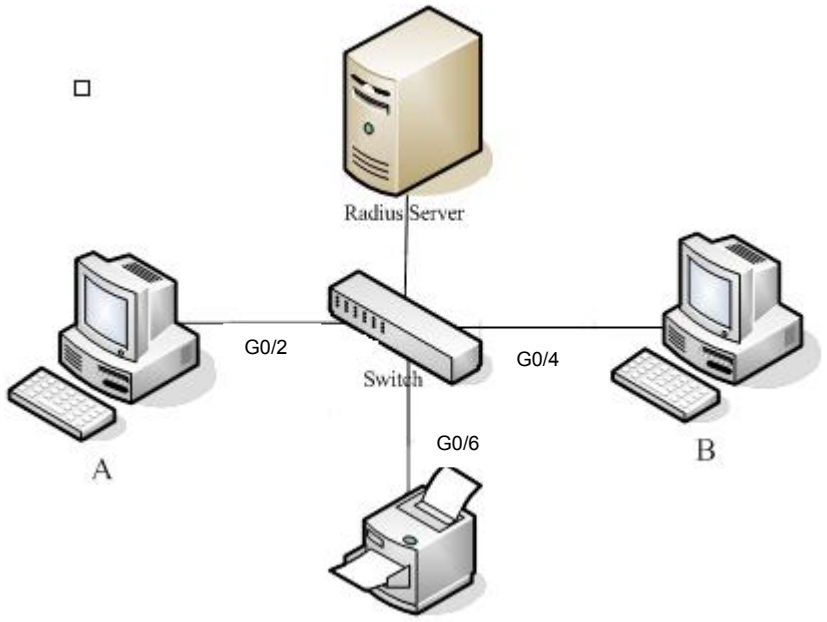
1.2.14 监控 802.1x 认证配置和状态

为了监控 802.1x 认证配置和状态，决定哪个 802.1x 参数需要调整，可以在管理模式下使用下面的命令：

命令	目的
show dot1x { *interface*|*statistics* }	802.1x认证配置和状态。

1.3 配置802.1x示例

连接如图：



Host A 与交换机的端口 G0/2 相连，Host B 与交换机的端口 G0/4 相连，Host C 与交换机的端口 G0/6 相连，radius-server host 的 ip 地址为 192.168.20.2，radius 的 key 为 TST；端口 G0/2 的认证使用远程的 radius 认证并且使用了用户绑定和开启记账功能和重认证功能，端口 G0/4 的认证使用本地认证没使用用户绑定，但用 eap 类型，并且启用了 Multi-hosts 和开启 guest-vlan 功能，端口 G0/6 使用 mab 认证，mac 地址格式为 AA:BB:CC:DD:EE:FF。

全局的配置

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
```

```
aaa authentication dot1x TST-G0/4 local
aaa authentication dot1x TST-G0/6 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
dot1x mabformat 2
dot1x guest-vlan
interface VLAN1
ip address 192.168.20.24 255.255.255.0
!
vlan 1-2
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

端口 G0/2 的配置

```
interface GigaEthernet0/2
 dot1x port-control auto
 dot1x authentication method TST-G0/2
 dot1x user-permit radius-TST
 dot1x accounting enable
 dot1x accounting method dot1x_acc
```

端口 G0/4 的配置

```
Interface GigaEthernet0/4
 dot1x authentication multiple-hosts
 dot1x port-control auto
 dot1x authentication method TST-G0/4
 dot1x guest-vlan 2
```

端口 G0/6 的配置

```
interface GigaEthernet0/6
 dot1x mab
 dot1x authentication method TST-G0/6
```