

802.1x配置

目 录

第 1 章 配置 802.1x.....	1
1.1 配置 802.1x任务列表	1
1.2 配置 802.1x任务	1
1.2.1 配置端口的 802.1x认证.....	1
1.2.2 配置 802.1x多主机端口认证.....	2
1.2.3 配置 802.1x身份认证请求的最大次数	2
1.2.4 配置 802.1x的重认证	3
1.2.5 控制 802.1x发送频率	3
1.2.6 配置 802.1x用户绑定	3
1.2.7 配置 802.1x端口的认证方法.....	3
1.2.8 选择 802.1x端口的认证类型	3
1.2.9 配置 802.1x记帐.....	4
1.2.10 配置 802.1x guest-vlan	4
1.2.11 禁止拥有多网卡的Supplicant.....	5
1.2.12 802.1x恢复默认配置	5
1.2.13 监控 802.1x认证配置和状态	5
1.3 配置 802.1x示例	5

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 身份认证请求的最大次数
- 配置 802.1x 的重认证
- 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 802.1x 记帐
- 配置 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，不需要在使用任何认证过程对端口进行认证，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协议控制方式。
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的认证方法。
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多主机端口认证

802.1x 的认证主要对单个主机用户进行认证，这时，交换机只允许一个用户进行认证、访问控制，其他用户是不能进行认证和访问的，除非前一个用户退出认证、访问过程；然而有时端口可能通过不支持 802.1x 的交换设备（例如 1108 交换机）与多个主机相连接，为了使这些主机用户都能访问，可以启动多主机端口访问功能。

将一个端口配置为 802.1x 的多主机认证后，交换机将对不同的台主机用户进行认证，当认证通过后，交换机将允许该主机通过交换机进行访问（使用主机的 MAC 进行控制），理论上 802.1x 对主机用户的数量是没有限制的，然而由于交换机对用户的认证控制是通过用户的 MAC 地址进行控制的，这时，主机用户的数量是就会受到交换机的 MAC 地址表大小的限制。

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 multiple-hosts	设置802.1x多主机端口认证。

1.2.3 配置 802.1x身份认证请求的最大次数

802.1x 开始认证时或重认证过程中，它会向客户主机发送身份认证请求，然而由于网络的原因造成报文的丢失或延时，这时就应该重新发送该请求报文，达到一定次数后，可以停止该认证请求，认为没有客户主机认证，认证失败。

根据不同的网络环境，更改身份认证请求的最大次数设置，以保证客户端与认证服务器间的认证通过。

配置身份认证请求的最大次数，可以在接口配置模式下使用下面一个或两个命令：

命令	目的
dot1x max-req count	配置身份认证请求的最大次数。

1.2.4 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进行认证，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。
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，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 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

1.2.10 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)}	在所有端口下打开 guest-vlan 功能

1.2.11 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。

1.2.12 802.1x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。

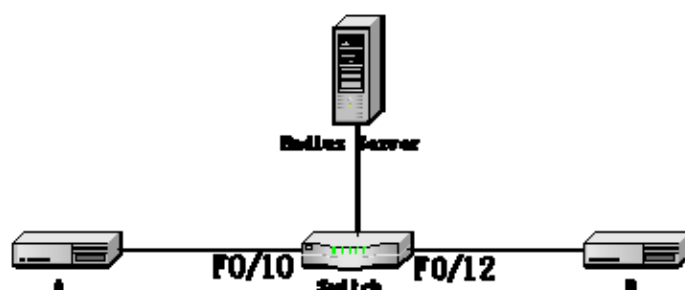
1.2.13 监控 802.1x认证配置和状态

为了监控 **802.1x** 认证配置和状态，决定那个 **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 ...}	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 F0/10 相连，Host B 与交换机的端口 F0/12 相连，radius-server host 的 ip 地址为 192.168.20.2，radius 的 key 为 TST；端口 F0/10

的认证使用远程的 **radius** 认证并且使用了用户绑定，端口 **F0/12** 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**。

全局的配置

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-F0/10 radius
aaa authentication dot1x TST-F0/12 local
interface VLAN1
 ip address 192.168.20.24 255.255.255.0
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

端口 F0/10 的配置

```
interface FastEthernet0/10
 dot1x port-control auto
 dot1x authentication method TST-F0/10
 dot1x user-permit radius-TST
```

端口 F0/12 的配置

```
interface FastEthernet0/12
 dot1x multiple-hosts
 dot1x port-control auto
 dot1x authentication method TST-F0/12
 dot1x authentication type eap
```