

H3C S2000-EA 802.1x的典型配置

一、组网需求:

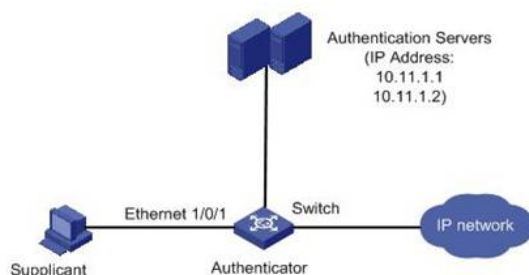
要求在各端口上对用户接入进行认证,以控制其访问Internet;接入控制模式要求是基于MAC地址的接入控制。

所有接入用户都属于一个缺省的域:aabbcc.net,该域最多可容纳30个用户;认证时,先进行RADIUS认证,如果RADIUS服务器没有响应再转而进行本地认证;计费时,如果RADIUS计费失败则切断用户连接使其下线;此外,接入时在用户名后不添加域名,正常连接时如果用户有超过20分钟流量持续小于2000Bytes的情况则切断其连接。

由两台RADIUS服务器组成的服务器组与交换机相连,其IP地址分别为10.11.1.1和10.11.1.2,前者作为主认证/备份计费服务器,后者作为备份认证/主计费服务器;设置系统与认证RADIUS服务器交互报文时的加密密码为"name"、与计费RADIUS服务器交互报文时的加密密码"money",设置系统在向RADIUS服务器发送报文后5秒钟内如果没有得到响应就向其重新发送报文,重复发送报文的次数总共为5次,设置系统每15分钟就向RADIUS服务器发送一次实时计费报文,指示系统从用户名中去掉用户域名后再将之传给RADIUS服务器。

本地802.1x接入用户的用户名为localuser,密码为localpass,使用明文输入,闲置切断功能处于打开状态。

二、组网图:



三、配置步骤:

开启全局802.1x特性。

```
<Sysname> system-view
```

System View: return to User View with Ctrl+Z.

```
[Sysname] dot1x
```

开启指定端口Ethernet 1/0/1的802.1x特性。

```
[Sysname] dot1x interface Ethernet 1/0/1
```

设置接入控制方式 (该命令可以不配置,因为端口的接入控制在缺省情况下就是基于MAC地址的)

.

```
[Sysname] dot1x port-method macbased interface Ethernet 1/0/1
```

创建RADIUS方案radius1并进入其视图。

```
[Sysname] radius scheme radius1
```

设置主认证/计费RADIUS服务器的IP地址。

```
[Sysname-radius-radius1] primary authentication 10.11.1.1
```

```
[Sysname-radius-radius1] primary accounting 10.11.1.2
```

设置备份认证/计费RADIUS服务器的IP地址。

```
[Sysname-radius-radius1] secondary authentication 10.11.1.2
```

```
[Sysname-radius-radius1] secondary accounting 10.11.1.1
```

设置系统与认证RADIUS服务器交互报文时的加密密码。

```
[Sysname-radius-radius1] key authentication name
```

设置系统与计费RADIUS服务器交互报文时的加密密码。

```
[Sysname-radius-radius1] key accounting money
```

设置系统向RADIUS服务器重发报文的时间间隔与次数。

```
[Sysname-radius-radius1] timer 5
```

```
[Sysname-radius-radius1] retry 5
```

设置系统向RADIUS服务器发送实时计费报文的时间间隔。

```
[Sysname-radius-radius1] timer realtime-accounting 15
```

指示系统从用户名中去掉用户域名后再将之传给RADIUS服务器。

```
[Sysname-radius-radius1] user-name-format without-domain
```

```
[Sysname-radius-radius1] quit
```

创建域aabbcc.net并进入其视图。

```
[Sysname] domain aabbcc.net
# 指定radius1为该域用户的RADIUS方案, 若RADIUS服务器无效, 则使用本地认证方案。
[Sysname-isp-aabbcc.net] scheme radius-scheme radius1 local
# 设置该域最多可容纳30个用户。
[Sysname-isp-aabbcc.net] access-limit enable 30
# 启动闲置切断功能并设置相关参数。
[Sysname-isp-aabbcc.net] idle-cut enable 20 2000
[Sysname-isp-aabbcc.net] quit
# 配置域aabbcc.net为缺省用户域。
[Sysname] domain default enable aabbcc.net
# 添加本地接入用户。
[Sysname] local-user localuser
[Sysname-luser-localuser] service-type lan-access
[Sysname-luser-localuser] password simple localpass
```

四、配置关键点:

无.