

H3C S9500交换机802.1X功能的配置

一、组网需求:

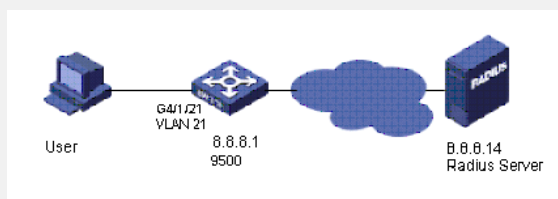
如下组网中,某用户的工作站与以太网交换机的端口G4/1/21相连接。交换机的管理者希望在各端口上对接入用户进行认证,以控制其访问Internet;接入控制模式要求是基于用户MAC地址或端口的接入控制。

所有AAA接入用户都属于一个缺省的域: H3C163.net;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。

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8.8.8.14和127.0.0.1,要求使用前者作为主认证/从计费服务器,使用本地作为从认证/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“h3c”、与计费RADIUS服务器交互报文时的加密密码“h3c”。

本地802.1x接入用户的用户名为localuser,密码为localpass,使用明文输入。

二、组网图



三、配置步骤:

软件版本: S9500交换机全系列软件版本

硬件版本: S9500交换机全系列硬件版本

1) 全局使能802.1X

```
[S9500]dot1x
```

2) 端口使能802.1X

```
[S9500]interface GigabitEthernet 4/1/21
```

```
[S9500-GigabitEthernet4/1/21]dot1x
```

3) 配置端口接入控制方式(端口的接入控制在缺省情况下是基于MAC地址的,下面列举基本MAC和基于端口两种方式)

基于MAC的方式

```
[S9500-GigabitEthernet4/1/21]dot1x port-method macbased
```

基于端口的方式

```
[S9500-GigabitEthernet4/1/21]dot1x port-method portbased
```

4) 配置802.1x用户的认证方法(该命令可以不配置,因为端口的认证方式在缺省情况下就是CHAP)

```
[S9500]dot1x authentication-method chap
```

5) 创建RADIUS方案radius1并进入其视图

```
[S9500] radius scheme radius1
```

6) 设置主认证/计费RADIUS服务器的IP地址

```
[S9500-radius-radius1] primary authentication 8.8.8.14
```

```
[S9500-radius-radius1] primary accounting 8.8.8.14
```

7) 设置从认证/计费RADIUS服务器的IP地址(本地)

```
[S9500-radius-radius1] secondary authentication 127.0.0.1 1645
```

```
[S9500-radius-radius1] secondary accounting 127.0.0.1 1646
```

8) 设置系统与认证RADIUS服务器交互报文时的加密密码

```
[S9500-radius-radius1] key authentication h3c
```

9) 设置系统与计费RADIUS服务器交互报文时的加密密码

```
[S9500-radius-radius1] key accounting h3c
```

10) 指示系统从用户名中去除用户域名后再将之传给RADIUS服务器

```
[S9500-radius-radius1] user-name-format without-domain
```

11) 创建用户域h3c163.net并进入其视图

```
[S9500] domain h3c163.net
```

12) 指定radius1为该域用户的RADIUS方案

```
[S9500-isp-h3c163.net] radius-scheme radius1
```

13) 设置本地radius的加密密码

```
[S9500]local-server nas-ip 127.0.0.1 key h3c
```

14) 添加本地接入用户

```
[S9500] local-user localuser
```

```
[S9500-luser-localuser] service-type lan-access
```

```
[S9500-luser-localuser] password simple localpass
```

四、配置关键点：

- 1) 设置本地Radius时需要指定认证和计费端口1645、1646，不能默认；
- 2) 本地的认证和计费密钥必须和远程服务器上的配置一致；
- 3) 只有在远程Radius无响应时才会转到本地认证。