

## 403 Forbidden

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。 [点击这里下载CyberArticle](#)。注册  
版本不会显示该信息。 [删除广告](#)

# V5交换机802.1X+Radius认证配置 案例（命令行版）

## 目录

### [V5交换机802.1X+Radius认证配置案例（命令行版）](#)

#### [1 配置需求或说明](#)

##### [1.1 适用产品系列](#)

##### [1.2 配置需求及实现的效果](#)

#### [2 组网图](#)

#### [3 配置步骤](#)

##### [3.1 交换机VLAN及虚接口基本配置](#)

##### [3.2 配置RADIUS方案](#)

##### [3.3 配置认证域](#)

##### [3.4 配置802.1X认证](#)

##### [3.5 配置本地账户和密码（服务器无响应可用本地用户认证）](#)

##### [3.6 Radius服务器设置](#)

##### [3.7 配置客户端](#)

##### [3.8 实验结果验证](#)

# 1 配置需求或说明

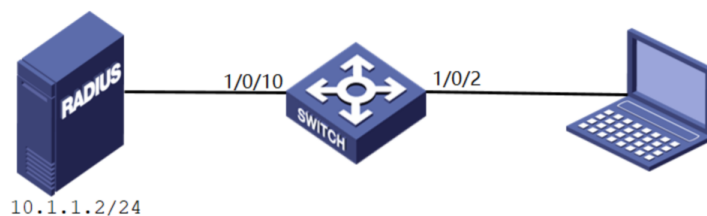
## 1.1 适用产品系列

本案例适用于如S5024PV2-EI等的V5交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comware V5、V7平台交换机分类说明”。

## 1.2 配置需求及实现的效果

电脑通过交换机的2口连入网络，设备对该端口接入的用户进行802.1X认证以控制其访问Internet，RADIUS服务器与交换机相连，其地址是10.1.1.2/24，RADIUS服务器作为认证计费服务器。认证时首先进行RADIUS认证，如果RADIUS服务器没有响应则进行本地认证。

# 2 组网图



# 3 配置步骤

## 3.1 交换机VLAN及虚接口基本配置

#进入交换机系统视图

```

<H3C>system-view
System View: return to User View with Ctrl+Z.
#创建vlan 1-2
[H3C]vlan 1 to 2
#配置vlan 1, vlan 2虚接口IP地址
[H3C]interface Vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.1.1
255.255.255.0
[H3C-Vlan-interface1]quit
[H3C]interface Vlan-interface 2
[H3C-Vlan-interface2] ip address 10.1.1.1
255.255.255.0
[H3C-Vlan-interface2]quit
#将端口分别划分到所属vlan, 端口2默认属于vlan 1, 端口10属于
vlan 2
[H3C] int Ethernet 1/0/10
[H3C-Ethernet1/0/10] port access vlan 2
[H3C-Ethernet1/0/10]quit
#配置到服务器的缺省路由
[H3C] ip route-static 0.0.0.0 0 10.1.1.2

```

## 3.2 配置RADIUS方案

```

#配置radius认证,配置radius服务器的IP地址、密钥
[H3C]radius scheme radius1
New Radius scheme
#配置RADIUS方案的主认证和主计费服务器及其通信密钥。
[H3C-radius-radius1]primary authentication
10.1.1.2 1812 key simple key
[H3C-radius-radius1]primary accounting 10.1.1.2
1813 key simple key

```

#配置发送给RADIUS服务器的用户名不携带ISP域名

```
[H3C-radius-radius1]user-name-format    without-
domain
```

```
[H3C-radius-radius1]qu
```

### 3.3 配置认证域

#创建名为a的ISP域并进入其视图

```
[H3C]domain a
```

#为dot1x用户配置AAA认证方法为RADIUS并采用local作为备选方案

```
[H3C-isp-a]authentication    lan-access    radius-
scheme radius1 local
```

#为dot1x用户配置AAA授权方法为RADIUS并采用local作为备选方案

```
[H3C-isp-a]authorization    lan-access    radius-
scheme radius1 local
```

#为dot1x用户配置AAA计费方法为RADIUS并采用local作为备选方案

```
[H3C-isp-a] accounting lan-access radius-scheme
radius1 local
```

```
[H3C-isp-a]qu
```

### 3.4 配置802.1X认证

#全局开启802.1X认证

```
[H3C]dot1x
```

```
802.1X is already enabled globally.
```

# Ethernet 1/0/2接口下开启802.1X认证

```
[H3C]int Ethernet 1/0/2
```

```
[H3C-Ethernet1/0/2]dot1x
```

```
802.1X is enabled on port Ethernet1/0/2
already.
```

```
#在以太网端口Ethernet1/0/2上配置802.1X用户使用强制认证域a
[H3C-Ethernet1/0/2]dot1x mandatory-domain a
[H3C-Ethernet1/0/2]qu
```

### 3.5 配置本地账户和密码（服务器无响应可用本地用户认证）

```
#创建本地用户h3c，密码为h3c，服务类型为lan-access
[H3C]local-user h3c
New local user added.
[H3C-luser-dot1x]password simple h3c
[H3C-luser-dot1x]service-type lan-access
[H3C-luser-dot1x]qu
#保存配置
[H3C]save force
```

### 3.6 Radius服务器设置

#下面以装有WinRadius软件的电脑（10.1.1.2/24）为例

- 1、 设置-数据库-自动配置ODBC-重启软件



- 2、 设置-系统，配置NAS密钥和交换机RADIUS方案的密钥一致，重启软件



- 3、 高级-创建RADIUS表，重启软件  
4、 操作-添加用户和账号

**添加账号**

用户名:

密码:

组名:

绑定地址:

请填写MAC地址或主叫号码来实现用户绑定。空白表示不绑定，0表示绑定到首次使用的地址。

预付金额:  分钱

到期日:

注意: yyyy/mm/dd表示到期日; 数字表示从第一次接入开始的有效天数; 空白表示永不过期。

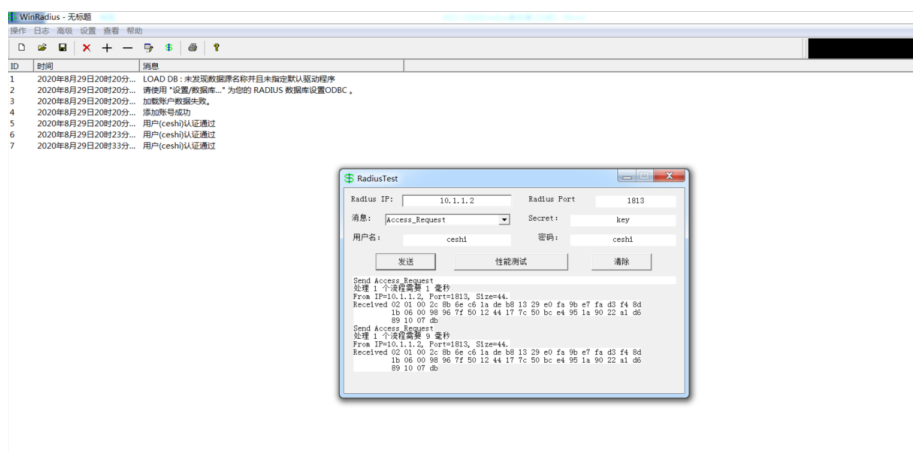
其它:

☐ 预付费用户 ☒ 后付费用户

计费方法:

备注:

可以利用软件Radius Test测试RADIUS服务器设置是否正确，在软件输入服务器地址，密钥，用户名和密码，点击发送，如下图所示提示用户（ceshi）认证通过。



### 3.7 配置客户端

#在客户端电脑上配置有线网卡的IPV4地址192.168.1.2/24，网关为192.168.1.1，安全INODE客户端软件，定制802.1X连接，输入用户名和密码是ceshi/ceshi



### 3.8 实验结果验证

将装有INODE客户端软件的电脑接入交换机的Ethernet 1/0/2，选择802.1X连接，输入正确的用户名和密码后点击连接，如下图802.1X认证通过





此时未进行802.1X认证的电脑可以ping通自己的网关

```
C:\Users\ASUS>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\ASUS>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

当交换机与服务器的接口断开连接，客户端向服务器认证无响应时可以用h3c/h3c的用户名和密码进行本地802.1X认证

