

## 实验十六 DES-3526 配置 802.1x

### 一、产品简介：

DES-3526 10/100Mbps 可堆叠交换机应用了 D-Link 的最新单一 IP 管理技术。该机架安装交换机具有 24 个 10/100BASE-TX 端口和 2 个组合式 1000BASE-T/SFP 千兆端口，这样的设计可以提供更加安全及灵活的连接方式。DES-3526 交换机操作简便，易于管理，这些交换机组成的部门级访问层设备能和其他包括 L3 层核心交换机在内，支持 D-Link 独立 IP 管理技术的交换机堆叠和调试，和骨干网及中央高速服务器组成多层网络结构。

### 二、实验目的：

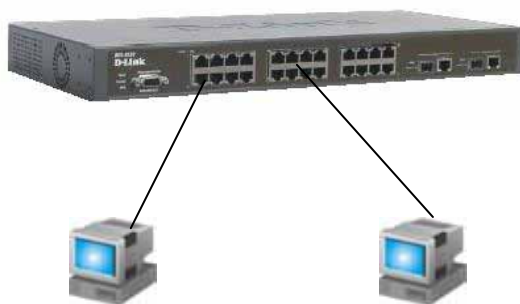
了解 DES-3526 配置 802.1x 的方法

### 三、实验环境要求：

#### 1、实验设备

- DES-3526 一台
- PC 两台
- 双绞线 若干

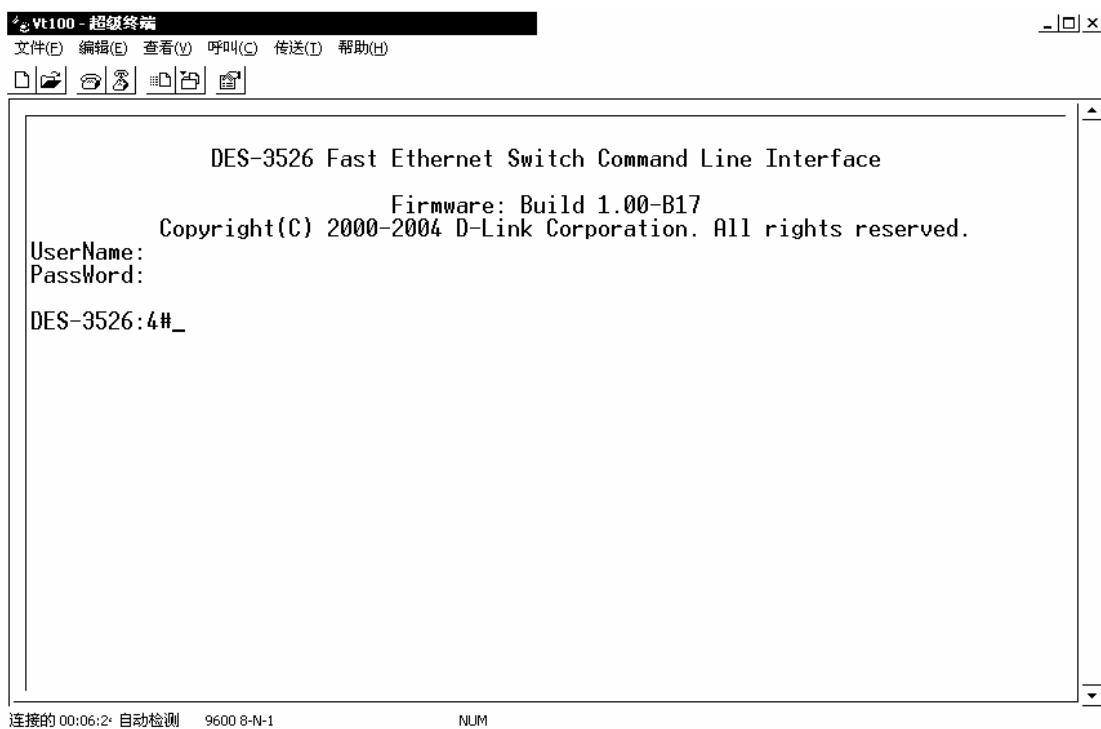
#### 2. 实验环境



### 四、实验步骤：

1) 把交换机的控制口和 PC 的串口相连，通过超级终端进入交换机的配置界面，

如下图：



- 2) 输入 `reset system` 命令，使交换机恢复出厂设置。交换机将自动重启。
- 3) 使用 “`config ipif System ipaddress 192.168.0.1/24`” 将交换机的 IP 地址修改为 192.168.0.1。
- 4) 首先使用 “`enable 802.1x`” 启用 802.1x 认证计费协议。得到交换机 “Success.” 的回应后，表示此时 802.1x 功能已经启用。此时可以指定需要认证的端口进行配置。

```
DES-3526:4#enable 802.1x
Command: enable 802.1x
Success.
```

- 5) 使用 “`config 802.1x capability ports 1 authenticator`” 将端口 1 设置为认证模式。

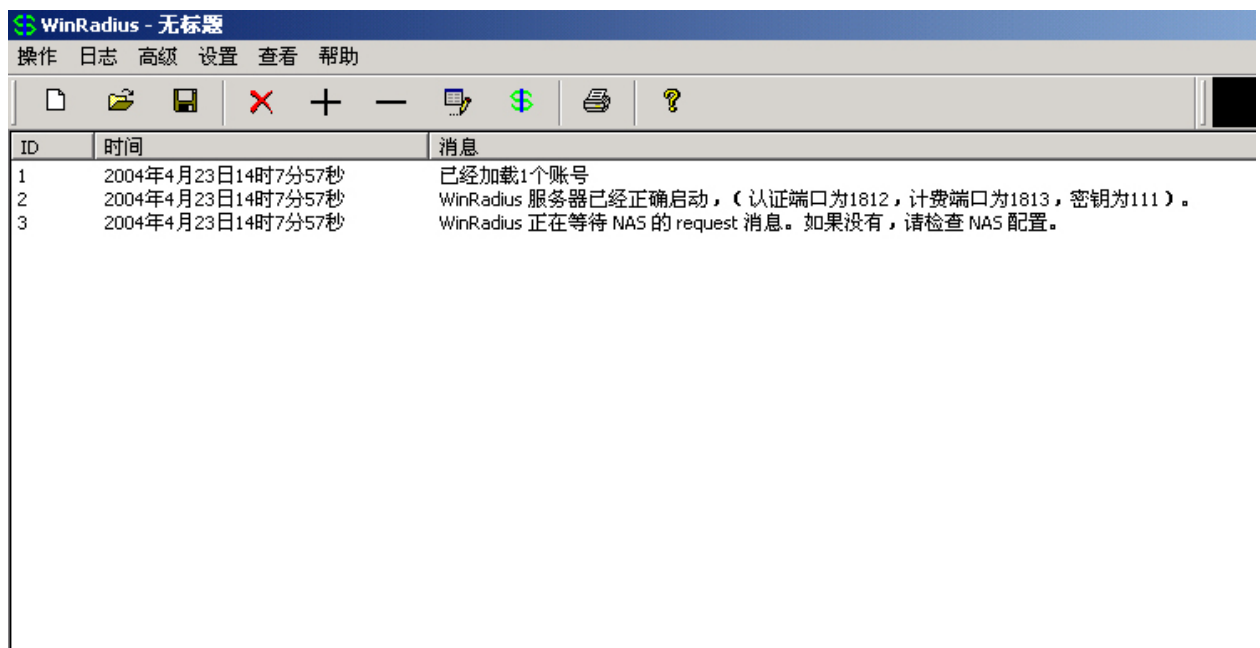
```
DES-3526:4#config 802.1x capability ports 1 authenticator
Command: config 802.1x capability ports 1 authenticator
Success.
```

- 6) 使用 “`config radius add 1 192.168.0.3 key 111 auth_port 1812 acct_port 1813`” 将 IP 地址为 192.168.0.3 的认证服务器添加到交换机，此时交换机接收到认证请求信息之后将把认证请求发送到这台认证服务器上。

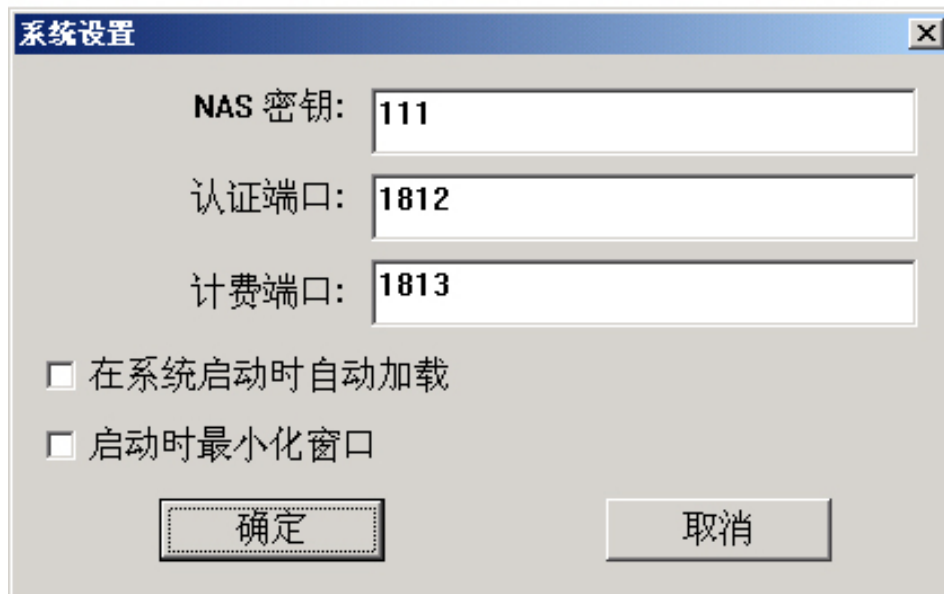
```
DES-3526:4#config radius add 1 192.168.0.3 key 111 auth_port 1812 acct_port 1813  
Command: config radius add 1 192.168.0.3 key 111 auth_port 1812 acct_port 1813  
Success.
```

命令中的参数“1”表示的是 RADIUS 服务器的序号；参数“111”是交换机和 RADIUS 服务器之间通信时的共享密钥，双方设置必须一致；“1812”和“1813”是 UDP 协议用的两个端口，“1812”是认证端口，“1813”是计费端口，这两个端口设置交换机和 RADIUS 双方也要一致。

7) 设置认证服务器。认证服务器有许多种，在此实验中我们采用 WinRadius 的免费版，此软件可以在网上下载，界面如图所示：



8) 单击“设置”按钮，在下拉菜单中选择“系统”，出现如下对话框：



系统设置

NAS 密钥: 111

认证端口: 1812

计费端口: 1813

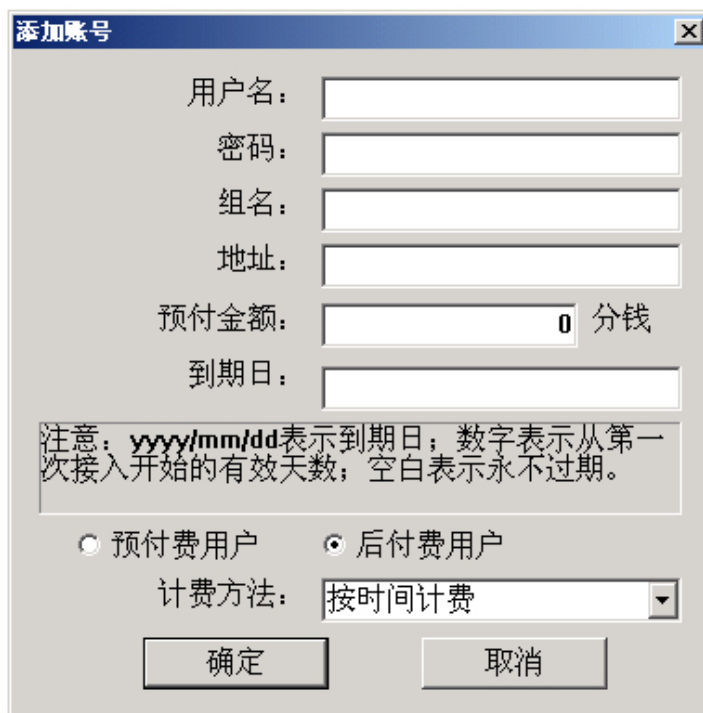
在系统启动时自动加载

启动时最小化窗口

确定 取消

设置完成后单击“确定”。

9) 单击“操作”按钮，在下拉菜单中选择“添加账号”出现如下对话框：



添加账号

用户名:

密码:

组名:

地址:

预付金额:  0 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。

预付费用户  后付费用户

计费方法: 按时间计费

确定 取消

10) 用户名和密码设为 dlink，选择“后付费用户”，单击“确定”。

11) WinRadius 将提醒“您修改了重要参数，请重新启动”，关闭并重新启动 WinRadius 软件。

12) 把 PC1 的 IP 地址设为 192.168.0.2/24，连接到端口 1，把装有 WinRadius 软件的 PC2 的 IP 地址设为 192.168.0.3/24，并连接到其它端口。

Note :

这样设置 IP 地址是为了保证服务器的 IP 地址和交换机的 IP 地址在同一网段，不需经由路由设备就可以相互通信。交换机的 IP 设置是必须的，因为在认证过程中交换机是认证代理，它必须和认证服务器及认证终端通信，所以要想认证成功，交换机、认证服务器、认证终端的 IP 地址必须在同一网段。

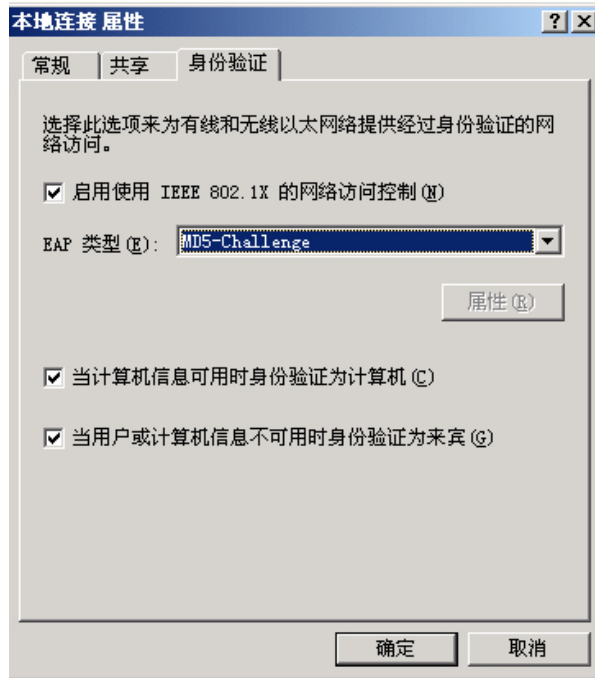
13) 此时输入 show 802.1x auth\_state 命令，查看认证情况：

```
DES-3226S:4#show 802.1x auth_state
Command: show 802.1x auth_state
```

Port	Auth PAE State	Backend State	Port Status
1	Connecting	Idle	Unauthorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized

此信息表明，端口 1 处于连接状态，但认证没通过，所以连接到端口 1 的 PC 不能进行正常通信。

14) 在 PC1 上启用 802.1x 认证客户端软件，用户名和密码都输入 dlink，进行认证。（注意：WindowsXP 系统自带认证软件，而 Windows2000 必须装有 SP4，或在 SP3 上打一个补丁才有此功能。Windows2000 系统装完相应补丁程序后，802.1x 认证服务默认是不启用的，所以要在“开始 - 控制面板 - 管理工具 - 服务”里启用“wireless configuration”服务，然后打开“网络连接属性”，按下图配置：



也可采用第三方 802.1x 客户端软件。)

15) Windows2000 下的认证画面如下：



16) 单击确定，如果认证成功，把鼠标指到 PC 右下角的网络连接图标上，会显示“身份验证成功”的提示。

17) 再次输入 `show 802.1x auth_state` 命令，查看交换机上的认证状态：

```
DES-3226S:4#show 802.1x auth_state  
Command: show 802.1x auth_state
```

Port	Auth PAE State	Backend State	Port Status
1	Authenticated	Idle	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized

此信息表明验证成功，此时 PC1 能正常通讯，可以用 PING 命令验证。

## 六、实验总结

802.1x 认证功能主要用在无线上网和小区宽带上网，需要注意的就是交换机的 IP 地址一定要配置正确，保证交换机和认证服务器的正常通讯。

## 七、实验完毕