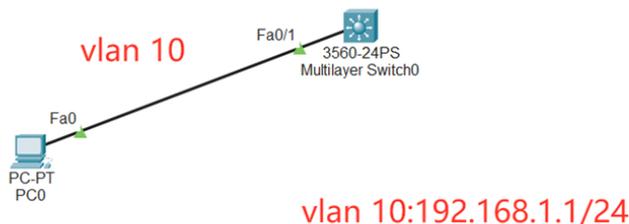


## 组网及说明



本案例采用思科模拟器的S3560交换机来模拟三权分立的典型组网配置，通过在S3560交换机配置SSH和三权分立，实现交换机的远程登录管理和用户权限的分配。

## 配置步骤

- 1、在交换机配置VLAN。
- 2、在交换机配置SSH。
- 3、创建用户admin，密码为admin，分配15级的管理员权限。
- 4、创建用户james，密码为james，分配0级的查看权限。
- 5、PC填写IP，能PING通交换机。
- 6、在PC上ssh登录交换机。
- 7、使用admin用户能进行配置
- 8、使用james用户仅能查看配置。

## 配置关键点

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hos MSW
MSW(config)#vlan 10
MSW(config-vlan)#exit
MSW(config)#int f 0/1
MSW(config-if)#sw mo acc
MSW(config-if)#sw acc vlan 10
MSW(config-if)#exit

MSW(config)#int vlan 10
MSW(config-if)#ip address 192.168.1.1 255.255.255.0
MSW(config-if)#no shutdown
MSW(config-if)#exit
MSW(config)#ip routing
```

SSH、三权分立配置关键点：

```
MSW(config)#username admin privilege 15 password 0 admin //创建用户名admin并配置密码，分配15级的管理员权限。
MSW(config)#username james privilege 0 password james //创建用户名james并配置密码，分配0级的查看权限。
MSW(config)#enable secret level 15 admin //配置特权密码，并分配15级的管理员权限。
```

MSW(config)#enable secret level 3 james //配置第二个特权密码，并分配3级的权限。

MSW(config)#aaa authentication login default local

MSW(config)#aaa authorization exec default local

MSW(config)# privilege exec level 3 sh run //指定3级权限登录时只能查看配置。

MSW(config)#ip domain name h3c.com //配置dns域名

MSW(config)#aaa new-model //使用本地数据库，模式为AAA

MSW(config)#crypto key generate rsa //创建密钥

The name for the keys will be: MSW.h3c.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024 //密钥长度配置为1024比特的长度

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

MSW(config)#ip ssh version 2 //配置ssh的版本为2

MSW(config)#ip ssh authentication-retries 5

MSW(config)#ip ssh time-out 60

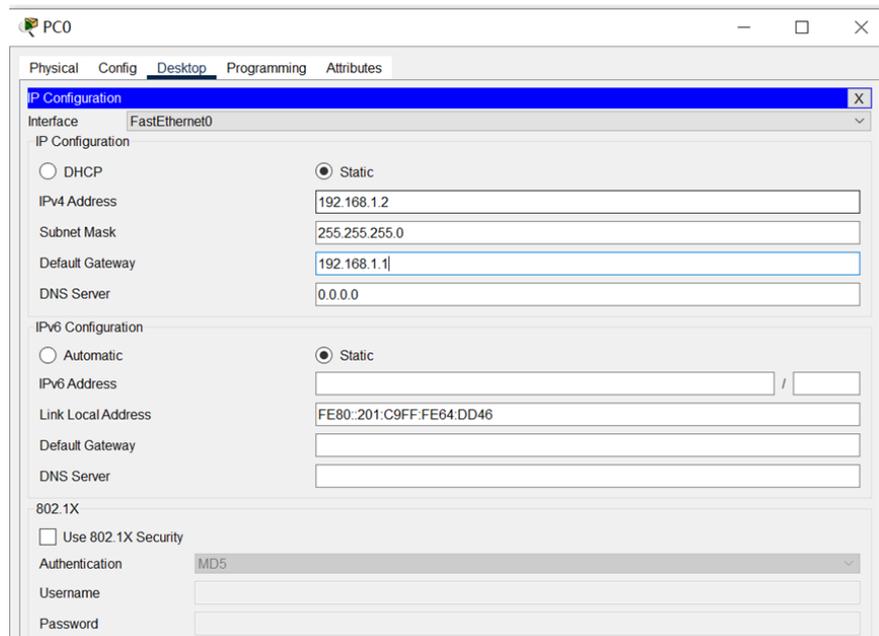
MSW(config)#line vty 0 4

MSW(config-line)#login

MSW(config-line)#transport input ssh

MSW(config-line)#exit

电脑填写IP地址:



电脑能PING通交换机

```

Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

电脑能使用admin用户SSH登录交换机，且能进入全局模式。

```

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l admin 192.168.1.1

Password:
MSW>ena
Password:
MSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MSW(config)#

```

Top

电脑能使用james用户SSH登录交换机

```

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l james 192.168.1.1

Password:
MSW>ena
MSW>enable 3
Password:
MSW#

```

但是无法进入全局模式

```

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l james 192.168.1.1

Password:
MSW>ena
MSW>enable 3
Password:
MSW#conf t
^
% Invalid input detected at '^' marker.
MSW#

```

可以查看配置：

## Command Prompt

```
tcp                Status of TCP connections
terminal          Display terminal configuration parameters
users            Display information about terminal lines
version          System hardware and software status
vlan            VTP VLAN status
vtp             Configure VLAN database
zone            Zone Information
zone-pair       Zone pair information
MSW#show ru
MSW#show running-config
MSW#exit

[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l james 192.168.1.1

Password:
MSW>ena
MSW>enable 3
Password:
MSW#conf t
^
% Invalid input detected at '^' marker.

MSW#sh
MSW#show run
MSW#show running-config
Building configuration...

Current configuration : 1891 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname MSW
!
!
enable secret level 3 5 $1$mERr$VMMaaCHP1JS/8WMKskOev.
enable secret 5 $1$mERr$VtBhull1N28cEp81kLqr0f/
!
!
!
!
!
aaa new-model
!
aaa authentication login default local
--More--
```

至此，思科交换机三权分立配置已完成。