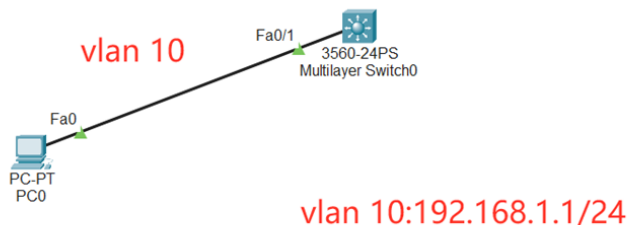


组网及说明



本案例采用思科模拟器的S3560交换机来模拟SSH的典型组网配置，通过在S3560交换机配置SSH，实现交换机的远程登录管理。同时为了确保交换机的安全登录，对SSH登录交换机进行IP限制。

配置步骤

- 1、在交换机配置VLAN。
- 2、在交换机配置SSH。
- 3、PC填写IP，能PING通交换机。
- 4、在PC上ssh登录交换机。
- 5、配置ACL，仅允许192.168.1.2的IP通过，并联动SSH，最终192.168.1.2的IP能SSH登录交换机，其他IP均无法SSH登录。

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配置关键点:

```
MSW(config)#username admin privilege 15 password 0 admin //创建用户名、密码
MSW(config)#enable secret admin //配置特权密码
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 //配置SSH重认证的次数为5次

MSW(config)#ip ssh time-out 60 //配置SSH登录的超时时间为60秒

MSW(config)#access-list 1 permit 192.168.1.2 0.0.0.0 //配置ACL，编号为1，允许192.168.1.2这个IP通过

MSW(config)#access-list 1 deny any //配置ACL，编号为1，拒绝所有通过

MSW(config)#line vty 0 4 //创建VTY 线路，前4个登录的用户需要使用该视图下配置的参数

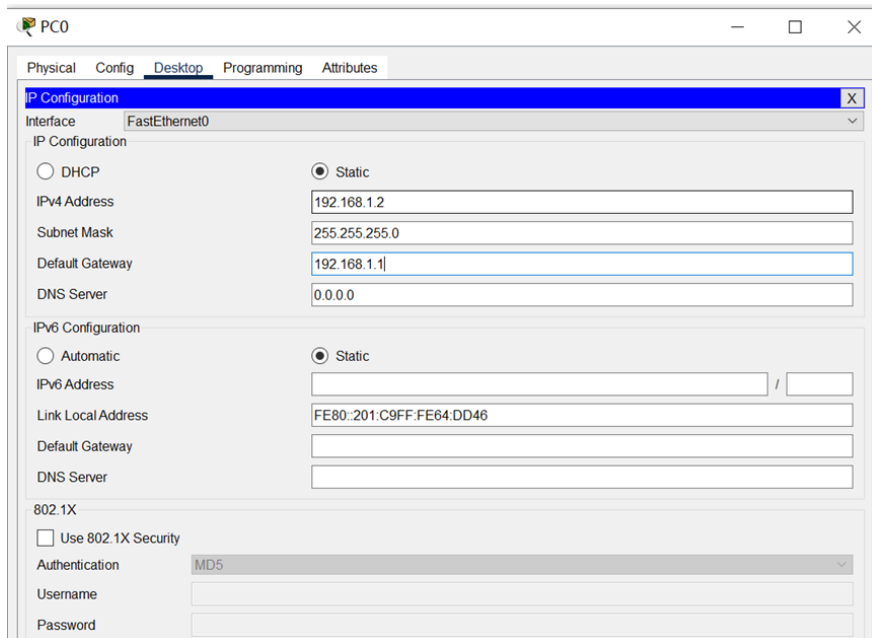
MSW(config-line)#login

MSW(config-line)#transport input ssh //登录的方式为SSH

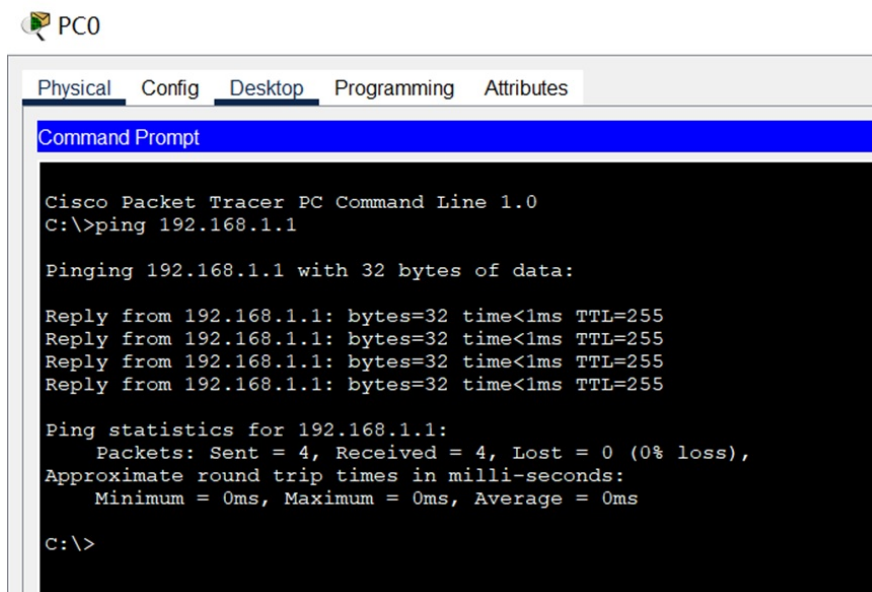
MSW(config-line)#access-class 1 in //调用ACL 1

MSW(config-line)#exit

电脑填写IP地址为192.168.1.2:



电脑能PING通交换机



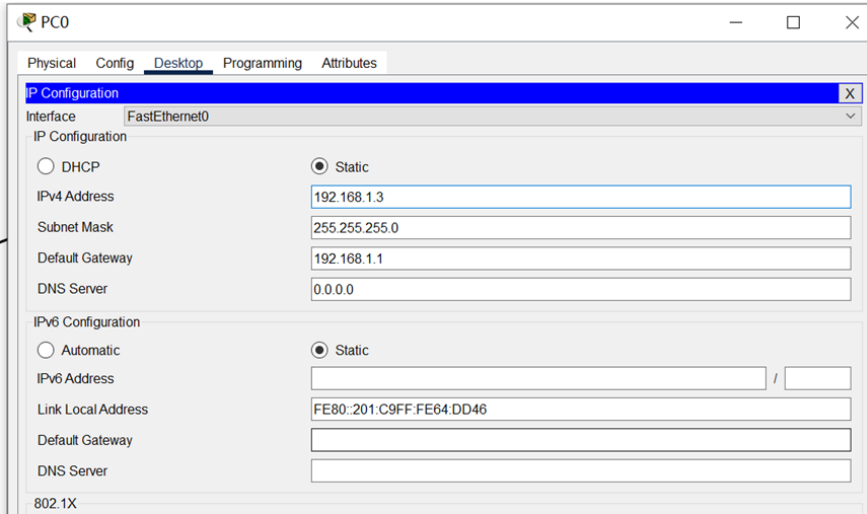
电脑能SSH登录交换机

```
[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

将电脑的IP修改为192.168.1.3



电脑能PING通交换机

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

Password:

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

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

Password:

Password:

Password:

MSW>
MSW#exit

[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)#

[Connection to 192.168.1.1 closed by foreign host]
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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
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:\>
```

但是无法SSH登录交换机

```
Physical Config Desktop Programming Attributes
Command Prompt
MSW>
MSW>ena
Password:
MSW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MSW(config)#exit
MSW#exit

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

Password:
Password:
Password:

MSW>
MSW>exit

[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)#

[Connection to 192.168.1.1 closed by foreign host]
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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
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:\>ssh -l admin 192.168.1.1

% Connection refused by remote host
C:\>
```

至此，思科交换机SSH登录IP限制的配置案例已完成。