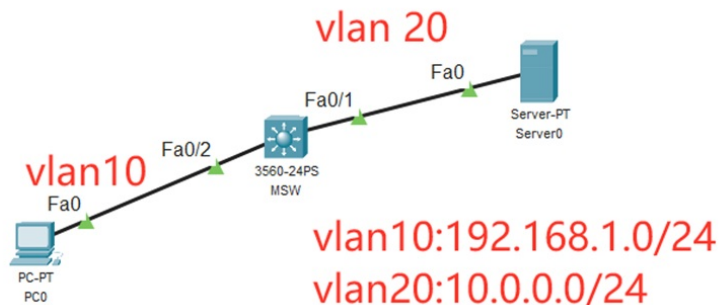


组网及说明



本案例采用思科模拟器来模拟思科交换机tacacs典型组网配置案例，在本案例中，服务器作为AAA服务器，MSW交换机作为AAA客户端，采用tacacs协议来实现交换机的安全登录管理。

配置步骤

1. 按照网络拓扑图配置IP地址。
2. 在MSW开启SSH功能，SSH账号为weijianing，密码weijianing
3. 在MSW配置tacacs
4. 在服务器开启AAA功能，并创建tacacs账号，账号为james，密码james
5. 在AAA服务器正常时，使用tacacs账号才能登录MSW
6. 在AAA服务器故障时，使用MSW的本地账号才能登录MSW

配置关键点

MSW:

```
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)#vlan 20
```

```
MSW(config-vlan)#exit
```

```
MSW(config)#int f 0/1
```

```
MSW(config-if)#sw mo acc
```

```
MSW(config-if)#sw acc vlan 20
```

```
MSW(config-if)#exit
```

```
MSW(config)#int f 0/2
```

```
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)#int vlan 20
```

```
MSW(config-if)#ip address 10.0.0.1 255.255.255.0
```

```
MSW(config-if)#no shutdown
```

```
MSW(config-if)#exit
```

```
MSW(config)#ip routing
```

```
MSW(config)#ip domain name h3c.com
```

MSW(config)#enable secret weijianing

MSW(config)#aaa new-model

MSW(config)#crypto key generate rsa

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

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

MSW(config)#

MSW(config)#ip ssh version 2

MSW(config)#ip ssh time-out 30

MSW(config)#ip ssh authentication-retries 5

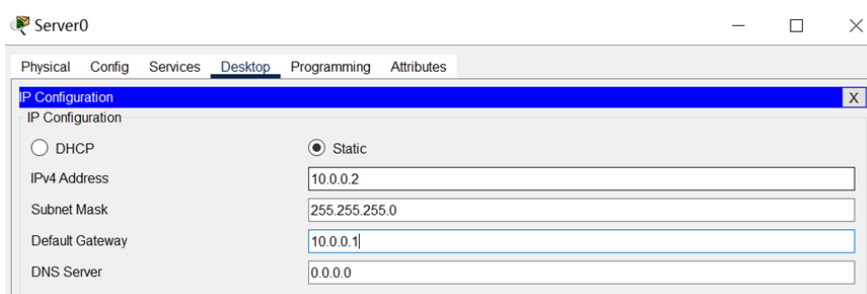
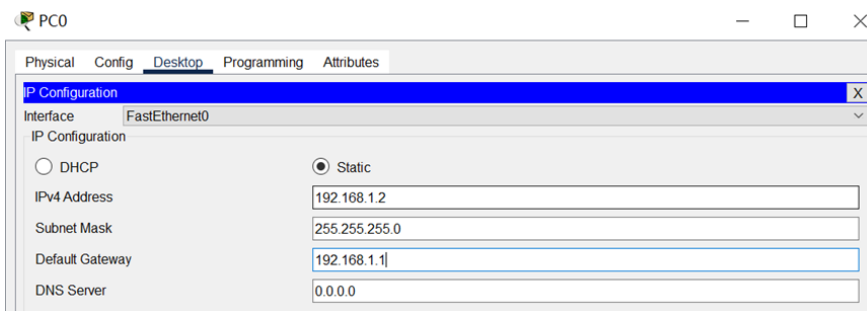
MSW(config)#username weijianing password weijianing

MSW(config)#line vty 0 4

MSW(config-line)#transport input ssh

MSW(config-line)#exit

PC和服务器填写IP地址，且能相互PING通。



Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time=7ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>
```

```
MSW(config)#aaa authentication login default group tacacs+ local
MSW(config)#tacacs-server host 10.0.0.2
MSW(config)#tacacs-server key james
MSW(config)#line vty 0 4
MSW(config-line)#login authentication default
MSW(config-line)#exit
```

在服务器上启用AAA功能，并创建tacacs账号和密码

Server0

Physical Config Services Desktop Programming Attributes

AAA

Service On Off Radius Port

Network Configuration

Client Name Client IP

Secret ServerType

	Client Name	Client IP	Server Type	Key	
1	MSW	10.0.0.1	Tacacs	james	Add

Save

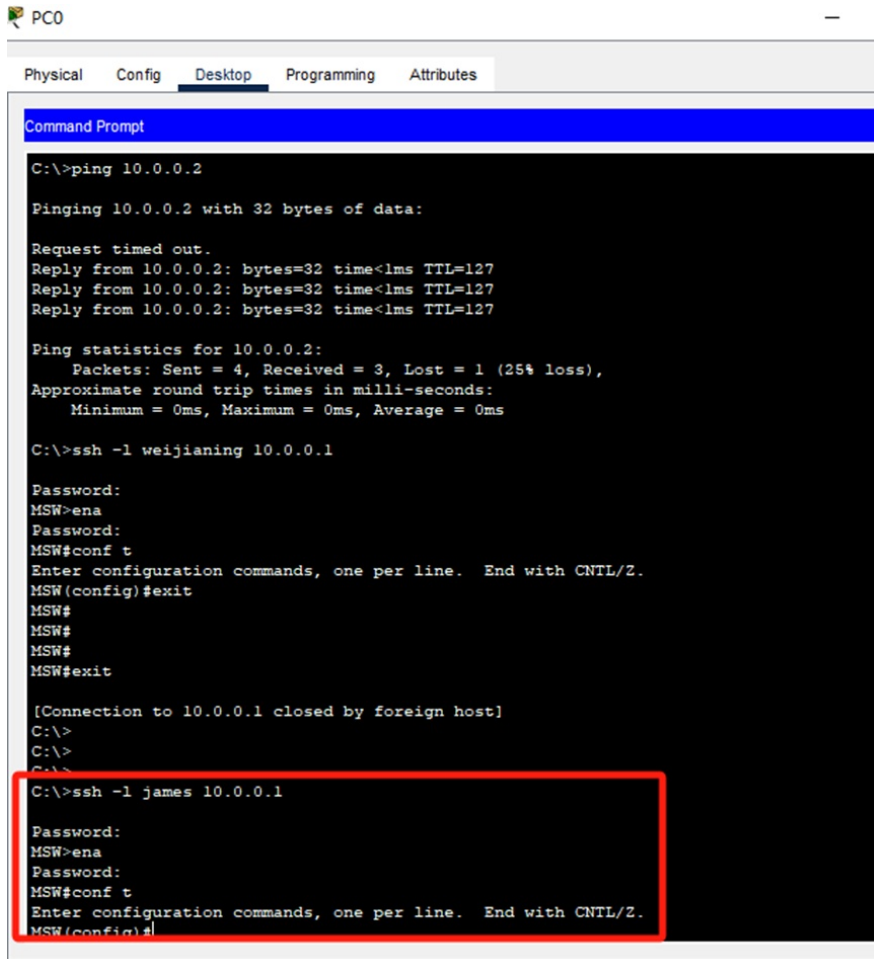
Remove

User Setup

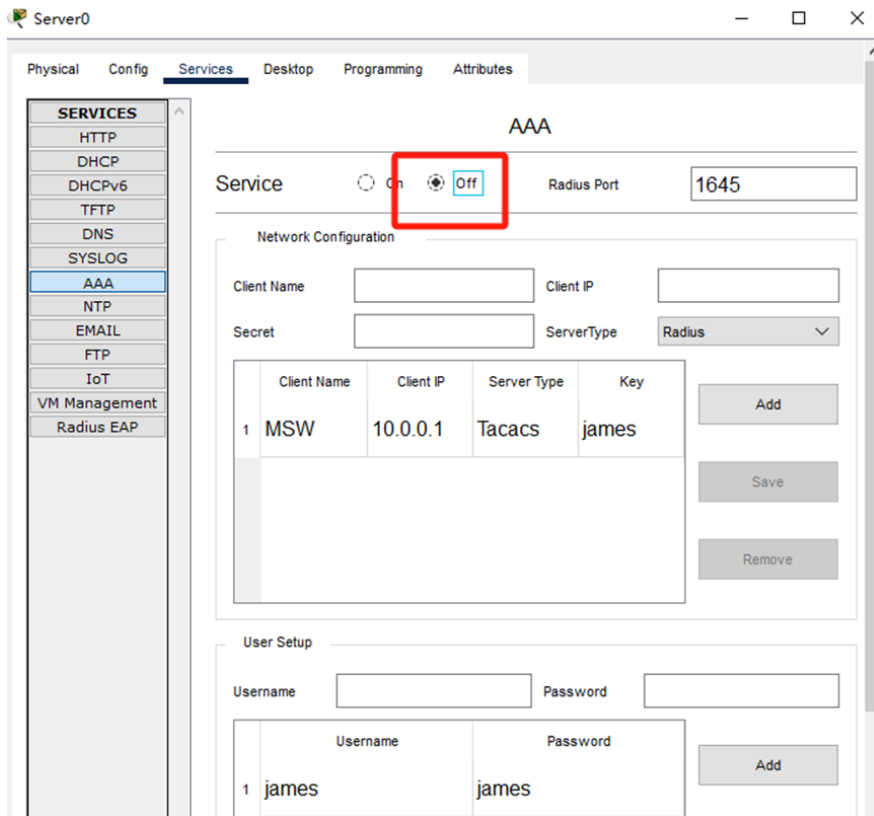
Username Password

	Username	Password	
1	james	james	Add

在PC使用tacacs账号james能SSH登录MSW

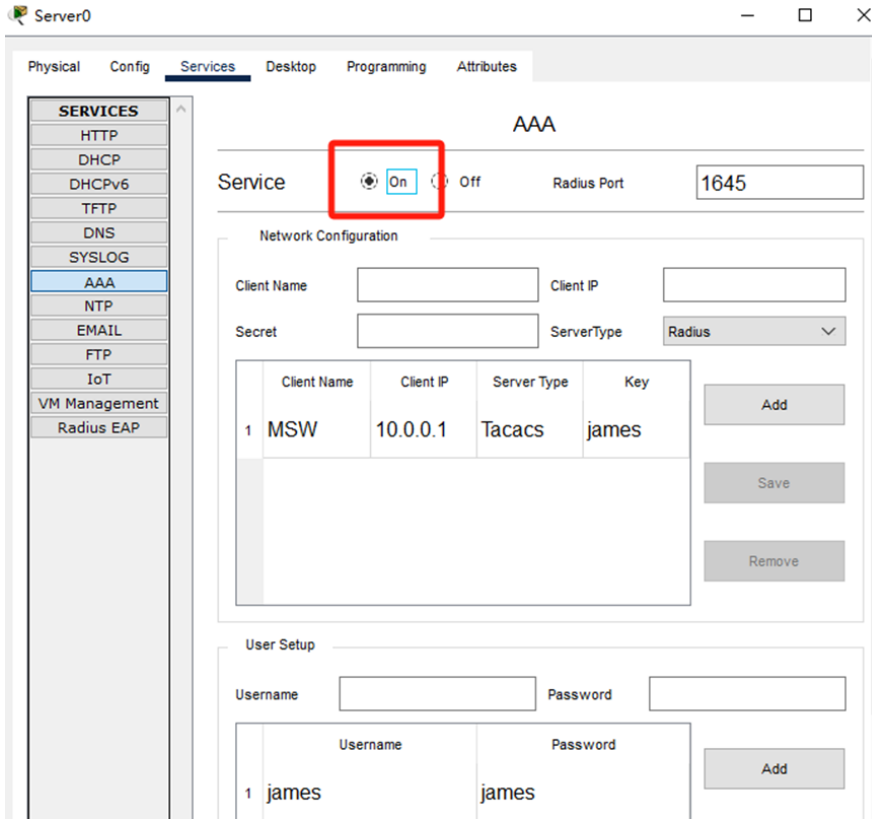


关闭AAA服务器的AAA功能，MSW无法用tacacs账号james登录，但是还能用本地账号weijianing登录。



```
C:\>ssh -l weijianing 10.0.0.1
Password:
MSW>ena
Password:
MSW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MSW(config)#
```

重新开启AAA服务器的AAA功能，使用tacacs账号james可以恢复对MSW的登录。



```
[Connection to 10.0.0.1 closed by foreign host]
C:\>ssh -l james 10.0.0.1
Password:
MSW>ena
Password:
MSW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MSW(config)#
```

至此，思科交换机tacacs典型组网配置案例已完成。