**《网络工程与组网技术》**

**课程实验报告**

（2022学年）

实验名称 6TO4隧道配置

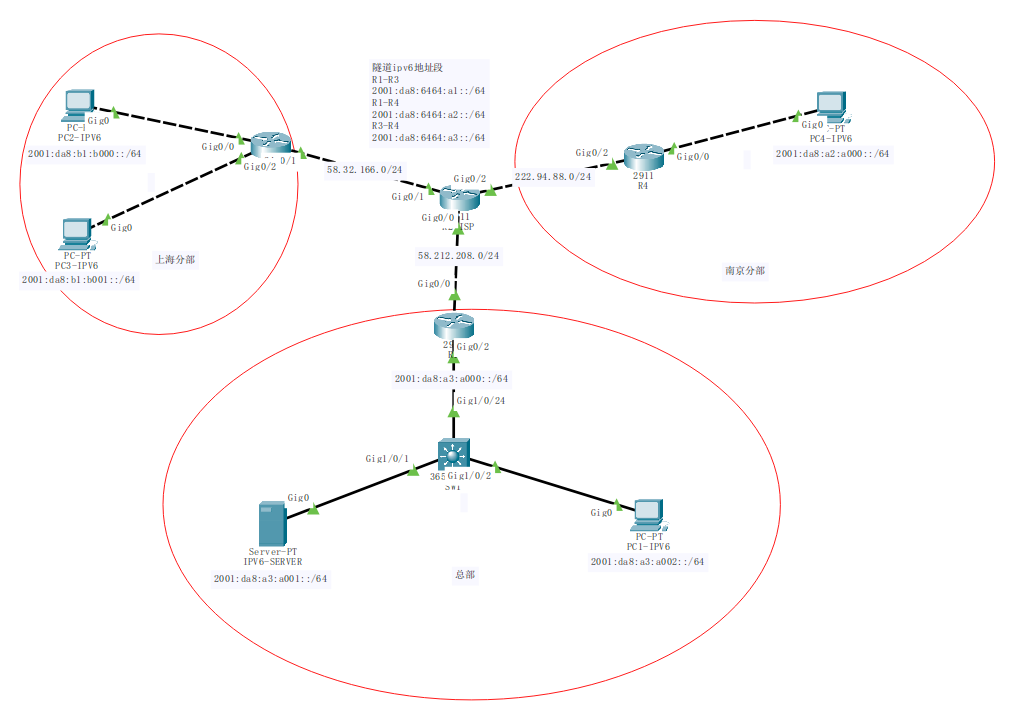
学 院

专业班级

学号姓名

2021年 8月22日

1. **实验说明**
2. 网络拓扑



1. 实验任务
2. IP配置

按照拓扑中 IP 标记配置 IP，上海分部、南京分部和总部的主机网关自定义；连接 R2 路由器接口的 IP 地址 配置成该段第二个可用地址。

* **IPv4配置：**

**R1配置：**

Router>en

Router#conf t

Router(config)#hostname R1

R1(config)#interface GigabitEthernet0/0 // 连接R2-ISP

R1(config-if)#no shut

R1(config-if)#ip addr 58.212.208.2 255.255.255.0

R1(config-if)#e

// IPv6接口在下面进行配置

**R2配置：**

R2-ISP>en

R2-ISP#conf t

R2-ISP(config)#interface GigabitEthernet0/0 // 连接R1

R2-ISP(config-if)#no shut

R2-ISP(config-if)#ip addr 58.212.208.1 255.255.255.0

R2-ISP(config-if)#e

R2-ISP(config)#interface GigabitEthernet0/1 // 连接R3

R2-ISP(config-if)#no shut

R2-ISP(config-if)#ip addr 58.32.166.1 255.255.255.0

R2-ISP(config-if)#e

R2-ISP(config)#interface GigabitEthernet0/2 // 连接R4

R2-ISP(config-if)#no shut

R2-ISP(config-if)#ip addr 222.94.88.1 255.255.255.0

R2-ISP(config-if)#e

**R3配置：**

Router>en

Router#conf t

Router(config)#hostname R3

R3(config)#interface GigabitEthernet0/1 // 连接R2-ISP

R3(config-if)#no shut

R3(config-if)#ip addr 58.32.166.2 255.255.255.0

R3(config-if)#e

// IPv6接口在下面进行配置

**R4配置：**

Router>en

Router#conf t

Router(config)#hostname R4

R4(config)#

R4(config)#interface GigabitEthernet0/2 // 连接R2-ISP

R4(config-if)#no shut

R4(config-if)#ip addr 222.94.88.2 255.255.255.0

R4(config-if)#e

* **IPv6配置：**

**SW1配置：**

Switch>en

Switch#conf t

Switch(config)#hostname SW1

SW1(config)#vlan 10 // 划分vlan 10

SW1(config-vlan)#name SERVER

SW1(config-vlan)#e

SW1(config)#int vlan 10

SW1(config-if)#ipv6 addr 2001:da8:a3:a001::2/64

SW1(config-if)#no shut

SW1(config-if)#e

SW1(config)#interface GigabitEthernet1/0/1 // 连接SERVER

SW1(config-if)#no shut

SW1(config-if)#switchport access vlan 10

SW1(config-if)#e

SW1(config)#vlan 20 // 划分vlan 20

SW1(config-vlan)#name PC1

SW1(config-vlan)#e

SW1(config)#int vlan 20

SW1(config-if)#ipv6 addr 2001:da8:a3:a002::2/64

SW1(config-if)#no shut

SW1(config-if)#e

SW1(config)#interface GigabitEthernet1/0/2 // 连接PC1

SW1(config-if)#no shut

SW1(config-if)#switchport access vlan 20

SW1(config-if)#e

SW1(config)#vlan 30 // 划分vlan 30

SW1(config-vlan)#name R2

SW1(config-vlan)#e

SW1(config)#int vlan 30

SW1(config-if)#ipv6 addr 2001:da8:a3:a000::2/64

SW1(config-if)#no shut

SW1(config-if)#e

SW1(config)#interface GigabitEthernet1/0/24 // 连接R2

SW1(config-if)#no shut

SW1(config-if)#switchport access vlan 30

SW1(config-if)#e

**R1配置：**

R1(config)#interface GigabitEthernet0/2 // 连接SW1

R1(config-if)#no shut

R1(config-if)#ipv6 addr 2001:da8:a3:a000::1/64

R1(config-if)#e

**R3配置：**

R3(config)#interface GigabitEthernet0/0 // 连接PC2

R3(config-if)#no shut

R3(config-if)#ipv6 addr 2001:da8:b1:b000::2/64

R3(config-if)#e

R3(config)#interface GigabitEthernet0/2 // 连接PC3

R3(config-if)#no shut

R3(config-if)#ipv6 addr 2001:da8:b1:b001::2/64

R3(config-if)#e

**R4配置：**

R4(config)#interface GigabitEthernet0/0 // 连接PC4

R4(config-if)#no shut

R4(config-if)#ipv6 addr 2001:da8:a2:a000::2/64

R4(config-if)#e

**PC1配置：**

IPv6地址：2001:DA8:A3:A002::1/64，网关：2001:DA8:A3:A002::2

**PC2配置：**

IPv6地址：2001:da8:b1:b000::1/64，网关：2001:da8:b1:b000::2

**PC3配置：**

IPv6地址：2001:da8:b1:b001::1/64，网关：2001:da8:b1:b001::2

**PC4配置：**

IPv6地址：2001:da8:a2:a000::1/64，网关：2001:da8:a2:a000::2

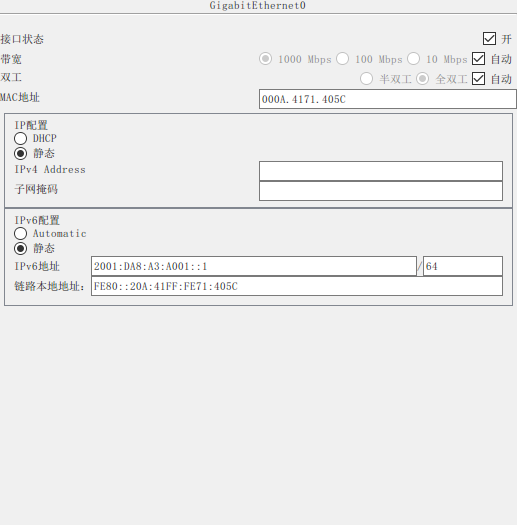
**SERVER配置：**

IPv6地址：2001:da8:a3:a001::1/64，网关：2001:da8:a3:a001::2

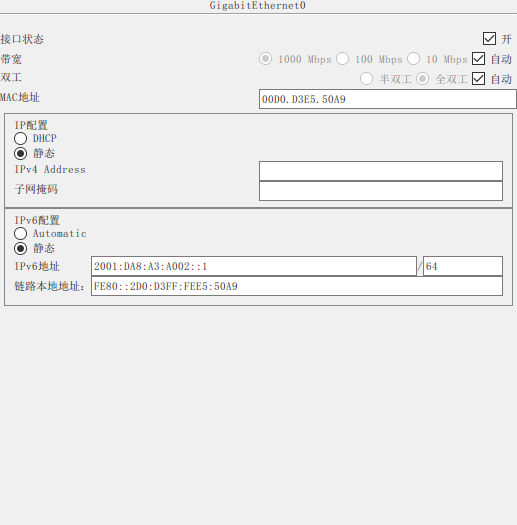
1. MAC地址绑定

SW1 上与 IPV6 服务器和 PC1 所连接接口配置 MAC 地址绑定，只允许对应主机接入。

查看SERVER的MAC地址为000A.4171.405C：



查看PC1的MAC地址为00D0.D3E5.50A9：



**SW1配置：**

SW1(config)#interface GigabitEthernet1/0/1 // 连接SERVER

SW1(config-if)#switchport port-security mac-address 000A.4171.405C

**Port-security not enabled on interface GigabitEthernet1/0/1.**

输入绑定MAC地址的命令后发出以上报错提示，查询后找到解决方案，需要先进入到access模式，启用安全绑定策略，然后再进行绑定等操作。

SW1(config-if)#switchport mode access // 进入access模式

SW1(config-if)#switchport port-security // 启用安全绑定策略

SW1(config-if)#switchport port-security mac-address 000A.4171.405C // 绑定SERVER的MAC地址

SW1(config-if)#switchport port-security maximum 1 // 设定端口最大连接数为1

SW1(config-if)#switchport port-security violation shut // 设定安全违规的处理方式为shutdown

SW1(config-if)#e

// 在另一连接PC1的端口上执行类似操作：

SW1(config)#interface GigabitEthernet1/0/2 // 连接PC1

SW1(config-if)#switchport mode access

SW1(config-if)#switchport port-security

SW1(config-if)#switchport port-security mac-address 00D0.D3E5.50A9 // PC1的MAC地址

SW1(config-if)#switchport port-security maximum 1

SW1(config-if)#switchport port-security violation shut

SW1(config-if)#e

1. 6TO4隧道配置

总部 R1 和上海分部、南京分部之间建立 GRE(6to4)隧道，实现总部 IPV6-server 可以和上海分部、南京分部 IPV6 网络互通，隧道所用 IPV6 地址段为拓扑图上标注的地址段。

**R1配置：**

R1(config)#int tunnel1 // 隧道1：R1-R3

R1(config-if)#no shut

R1(config-if)#ipv6 enable

R1(config-if)#ipv6 addr 2001:da8:6464:a1::1/64

R1(config-if)#tunnel source Gig0/0 **// 这里注意，在大部分教程中这里都会写为源接口的ip地址，但模拟器中并不支持这种写法，需要输入接口名称**

R1(config-if)#tunnel destination 58.32.166.2 // R3与R2-ISP连接的接口地址

R1(config-if)#tunnel mode ipv6ip // ipv6模式

R1(config-if)#e

R1(config)#int tunnel2 // 隧道2：R1-R4

R1(config-if)#no shut

R1(config-if)#ipv6 enable

R1(config-if)#ipv6 addr 2001:da8:6464:a2::1/64

R1(config-if)#tunnel source Gig0/0

R1(config-if)#tunnel destination 222.94.88.2 // R4与R2-ISP连接的接口地址

R1(config-if)#tunnel mode ipv6ip // ipv6模式

R1(config-if)#e

// 配置路由转发：

R1(config)#ip route 0.0.0.0 0.0.0.0 58.212.208.1 // 默认下一跳为R2-ISP

R1(config)#ipv6 unicast-routing

R1(config)#ipv6 route 2001:da8:b1:b000::/64 2001:da8:6464:a1::2

R1(config)#ipv6 route 2001:da8:b1:b001::/64 2001:da8:6464:a1::2 // 到上海分部网段的下一跳为tunnel1的R3接口

R1(config)#ipv6 route 2001:da8:a2:a000::/64 2001:da8:6464:a3::2 // 到南京分布网段的下一跳为tunnel3的R4接口

R1(config)#ipv6 route 2001:da8:a3:a001::/64 2001:da8:a3:a000::2

R1(config)#ipv6 route 2001:da8:a3:a002::/64 2001:da8:a3:a000::2 //到PC1和SERVER网段的下一跳为SW1

**R3配置：**

R3(config)#int tunnel1 // 隧道1：R1-R3

R3(config-if)#no shut

R3(config-if)#ipv6 enable

R3(config-if)#ipv6 addr 2001:da8:6464:a1::2/64

R3(config-if)#tunnel source Gig0/1

R3(config-if)#tunnel destination 58.212.208.2 // R1与R2-ISP连接的接口地址

R3(config-if)#tunnel mode ipv6ip

R3(config-if)#e

R3(config)#int tunnel3 // 隧道3：R3-R4

R3(config-if)#no shut

R3(config-if)#ipv6 enable

R3(config-if)#ipv6 addr 2001:da8:6464:a3::1/64

R3(config-if)#tunnel source Gig0/1

R3(config-if)#tunnel destination 222.94.88.2 // R4与R2-ISP连接的接口地址

R3(config-if)#tunnel mode ipv6ip

R3(config-if)#e

// 配置路由转发：

R3(config)#ip route 0.0.0.0 0.0.0.0 58.32.166.1 // 默认下一跳为R2-ISP

R3(config)#ipv6 unicast-routing

R3(config)#ipv6 route 2001:da8:a3:a000::/64 2001:da8:6464:a1::1

R3(config)#ipv6 route 2001:da8:a3:a001::/64 2001:da8:6464:a1::1

R3(config)#ipv6 route 2001:da8:a3:a002::/64 2001:da8:6464:a1::1 // 到总部网段的下一跳为tunnel1的R1接口

R3(config)#ipv6 route 2001:da8:a2:a000::/64 2001:da8:6464:a3::2 // 到南京分部网段的下一跳为tunnel3的R4接口

**R4配置：**

R4(config)#int tunnel2 // 隧道2：R1-R4

R4(config-if)#no shut

R4(config-if)#ipv6 enable

R4(config-if)#ipv6 addr 2001:da8:6464:a2::2/64

R4(config-if)#tunnel source Gig0/2

R4(config-if)#tunnel destination 58.212.208.2 // R1与R2-ISP相连的接口地址

R4(config-if)#tunnel mode ipv6ip

R4(config-if)#e

R4(config)#int tunnel3 // 隧道3：R1-R4

R4(config-if)#no shut

R4(config-if)#ipv6 enable

R4(config-if)#ipv6 addr 2001:da8:6464:a3::2/64

R4(config-if)#tunnel source Gig0/2

R4(config-if)#tunnel destination 58.32.166.2 // R3与R2-ISP相连的接口地址

R4(config-if)#tunne mode ipv6ip

R4(config-if)#e

// 配置路由转发：

R4(config)#ip route 0.0.0.0 0.0.0.0 222.94.88.1 // 默认下一跳为R2-ISP

R4(config)#ipv6 unicast-routing

R4(config)#ipv6 route 2001:da8:a3:a000::/64 2001:da8:6464:a2::1

R4(config)#ipv6 route 2001:da8:a3:a001::/64 2001:da8:6464:a2::1

R4(config)#ipv6 route 2001:da8:a3:a002::/64 2001:da8:6464:a2::1 // 到总部网段的下一跳为tunnel2的R1接口

R4(config)#ipv6 route 2001:da8:b1:b000::/64 2001:da8:6464:a3::1

R4(config)#ipv6 route 2001:da8:b1:b001::/64 2001:da8:6464:a3::1 // 到上海分部网段的下一跳为tunnel3的R3接口

**SW1配置：**

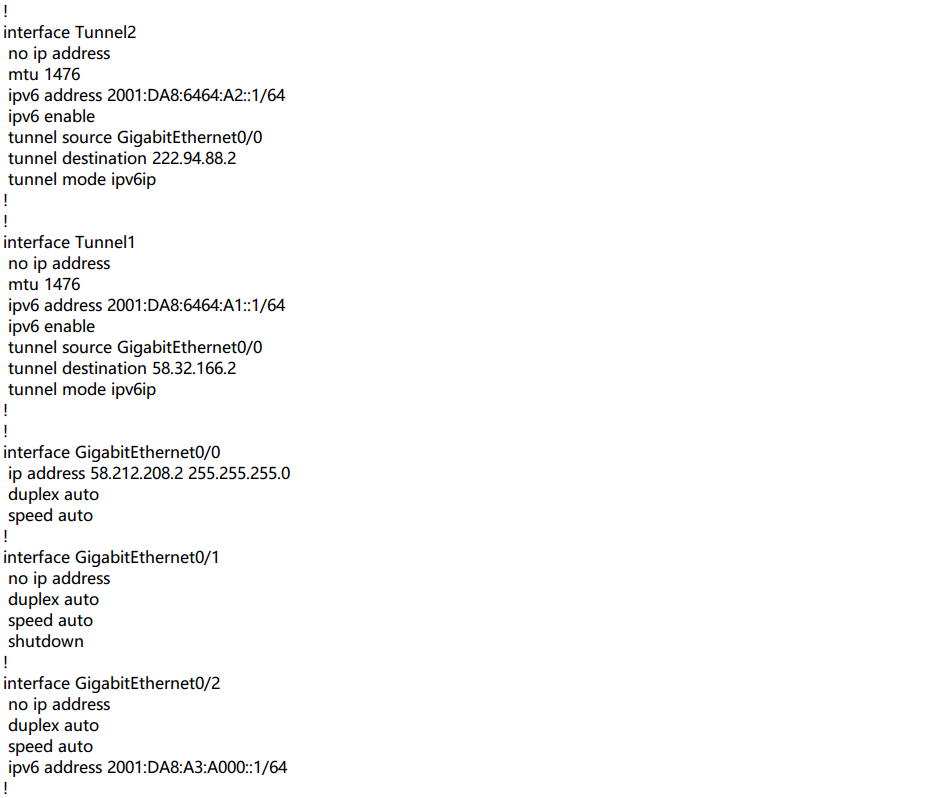
// 配置路由转发：

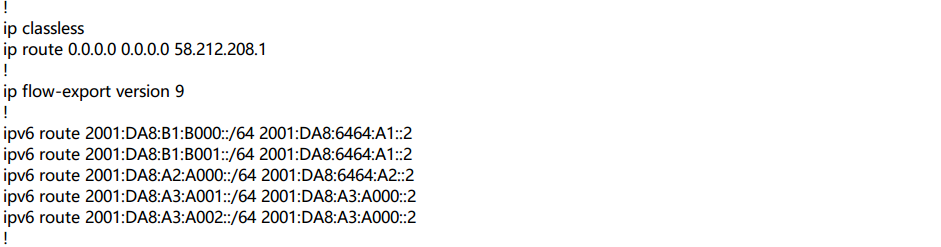
SW1(config)#ipv6 unicast-routing

SW1(config)#ipv6 route ::/0 2001:da8:a3:a000::1 // 默认下一跳为R1的Gig0/2接口

1. **网络节点配置**

* **R1部分配置文件信息：**



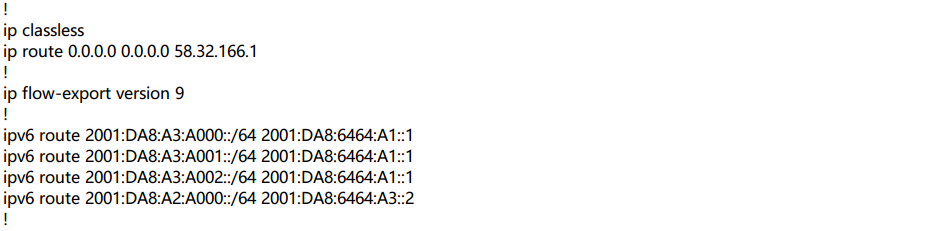


* **R2-ISP部分配置文件信息：**

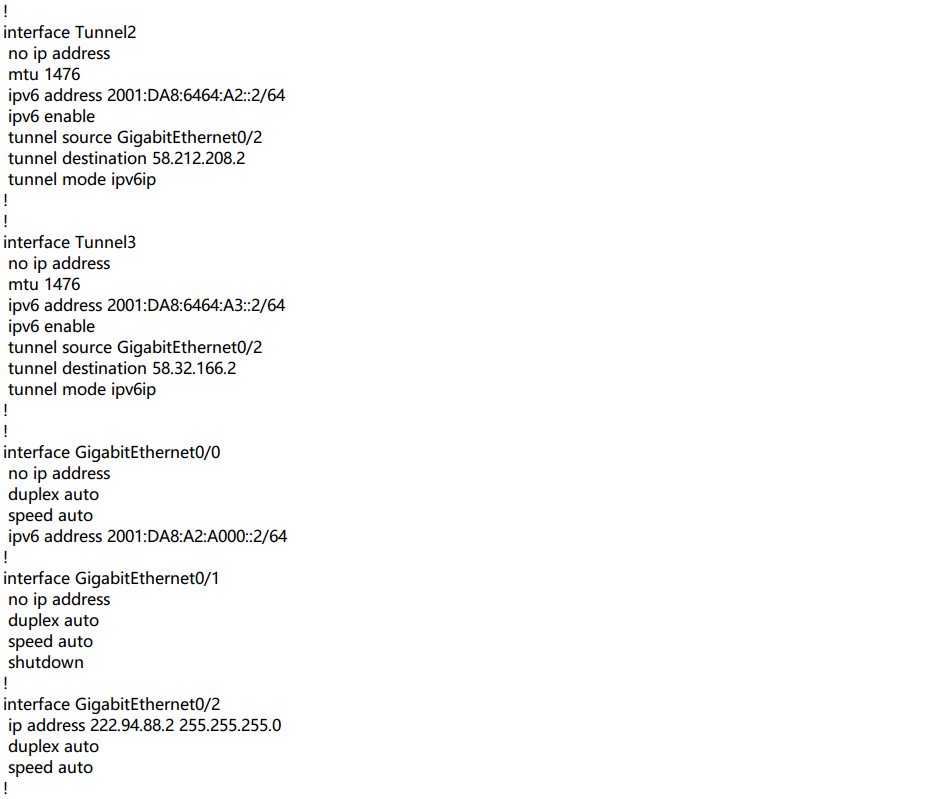


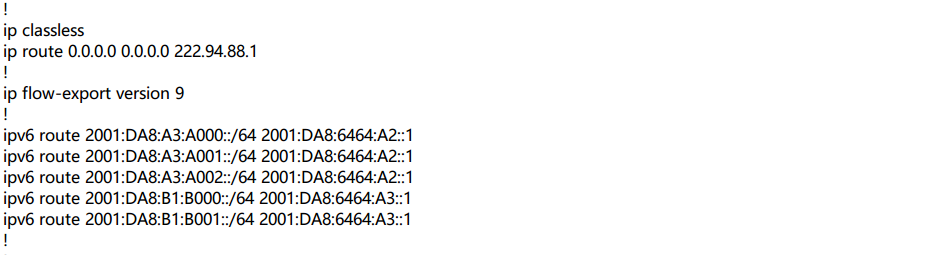
* **R3部分配置文件信息：**





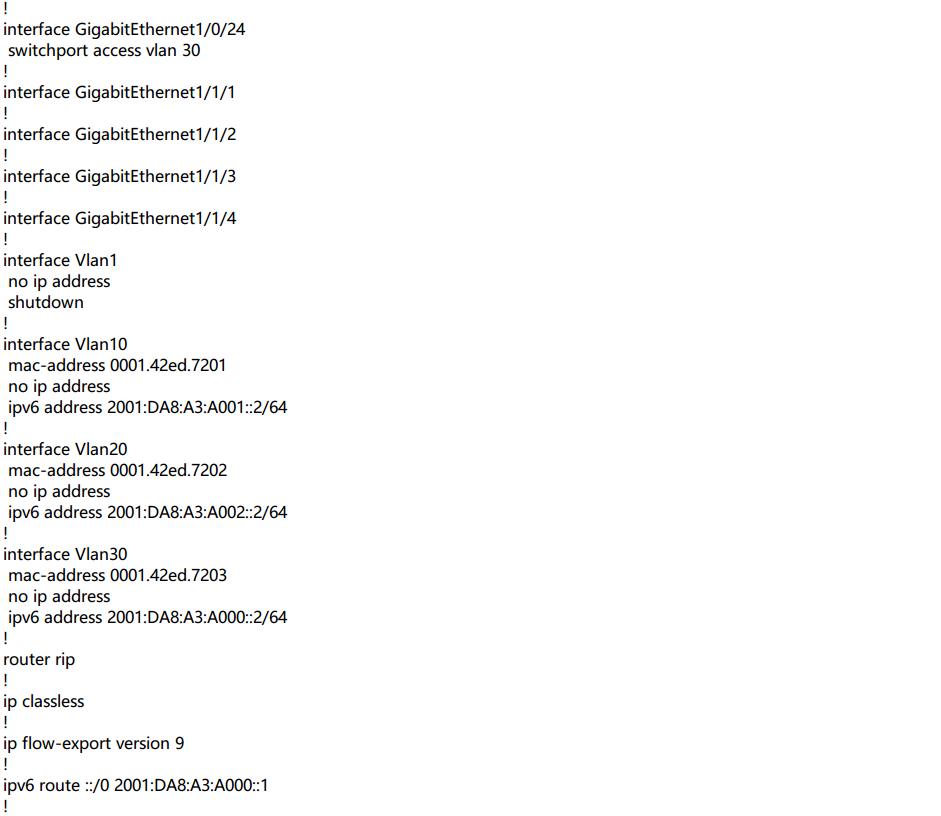
* **R4部分配置文件信息：**





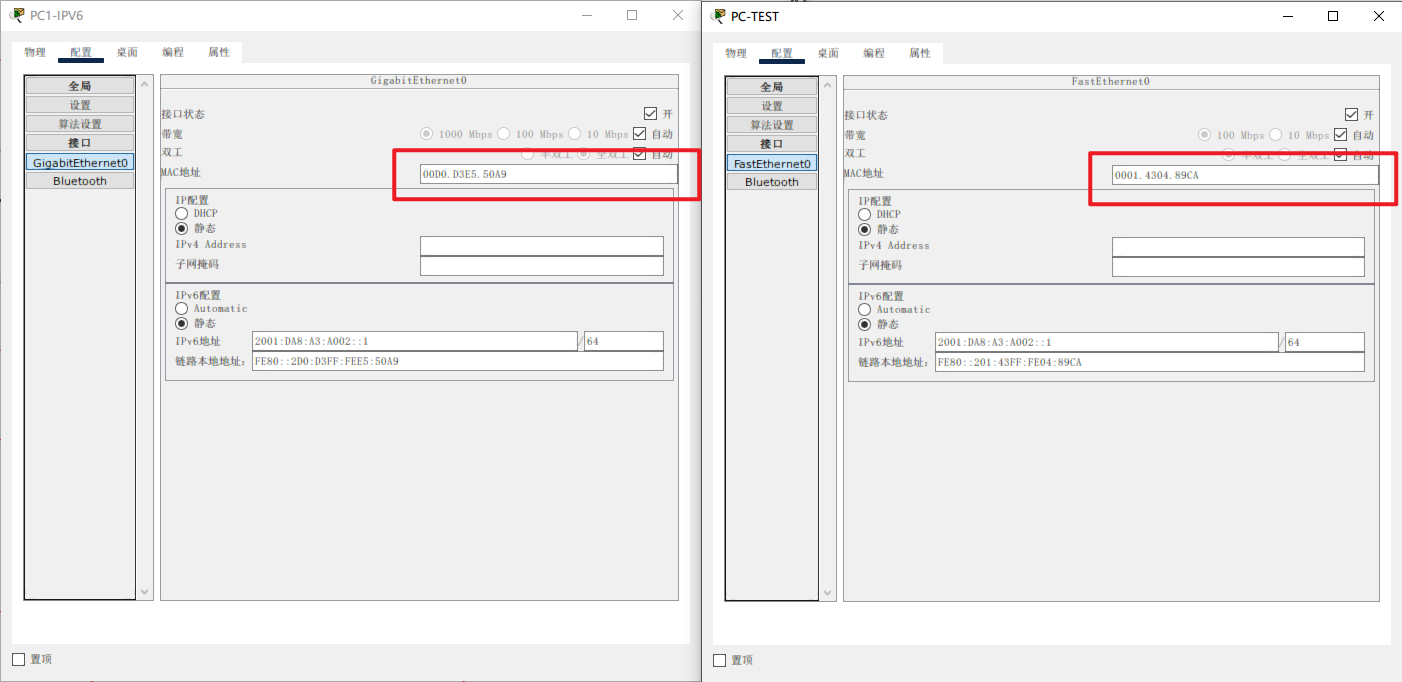
* **SW1部分配置文件信息：**



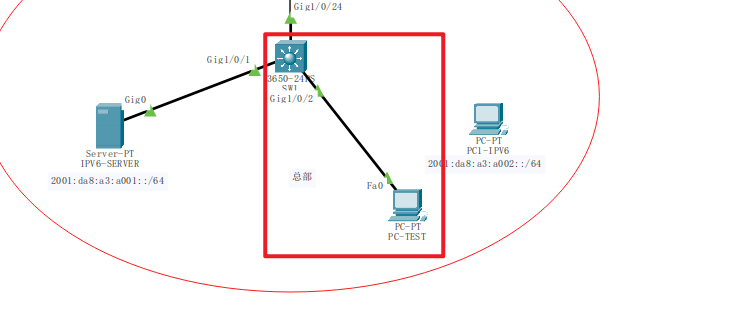


1. **功能测试**
2. 测试新建 VPC 接入 SW1 替换目前的 PC 是否能 ping 通 SW1 相对应 vlan 接口的 ip 地址。(请在所有实验 完成后再进行此步骤，否则网络会不通)。

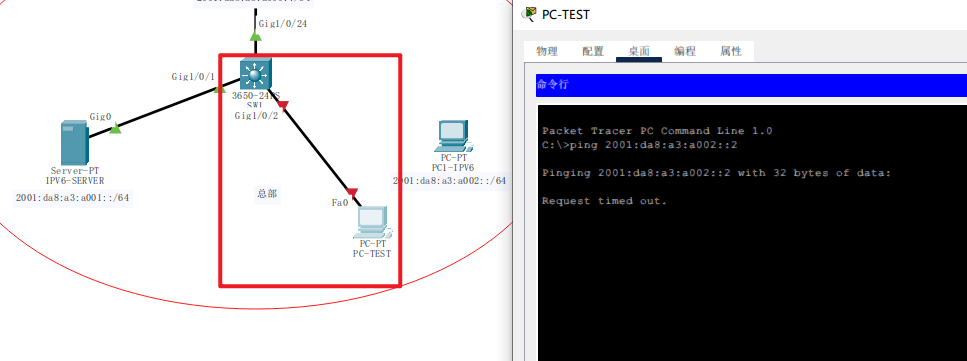
新建一台PC命名为PC-TEST，将IPv6地址和网关都配置为与PC1相同，MAC地址不改动，下图可以看到二者的MAC地址不相同：



将PC1从SW1上断开，将PC-TEST接入SW1（接口是PC1前面所使用的接口：Gig1/0/2）：



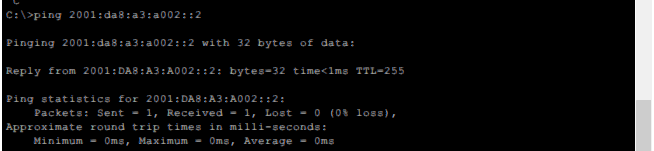
在PC-TEST命令行中输入ping 2001:da8:a3:a002::2（此地址是前面PC1所对应的vlan 20的接口地址），结果如下：



可以看到在命令行中显示请求超时，随即PC-TEST的相应端口Gig1/0/2自动关闭，这与前面在对SW1进行端口安全策略配置时的“switchport port-security violation shut”命令相符：



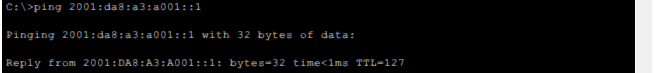
将接口重新开启后，断开与PC-TEST的连接，重新连接到PC1上，在PC1命令行中输入ping 2001:da8:a3:a002::2，成功ping通：



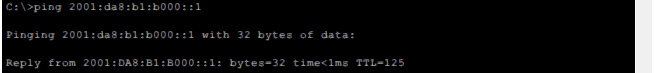
测试通过。

1. 测试总部与上海分部、南京分部之间的 IPV6 网络是否可以 ping通。

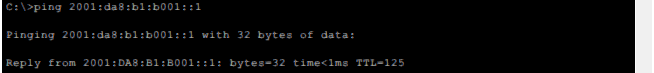
**总部PC1->总部SERVER（内部）：**



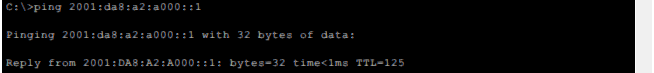
**总部PC1->上海分部PC2（tunnel 1）：**



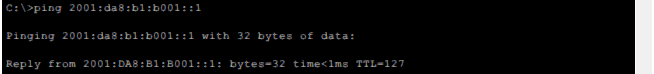
**总部PC1->上海分部PC3（tunnel 1）：**



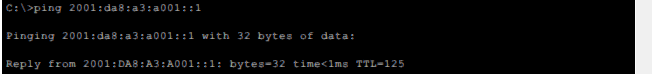
**总部PC1->南京分部PC4（tunnel 2）：**



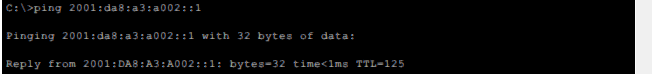
**上海分部PC2->上海分部PC3（内部）：**



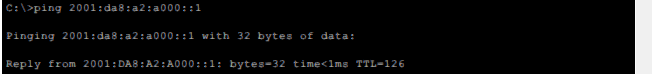
**上海分部PC2->总部SERVER（tunnel 1）：**



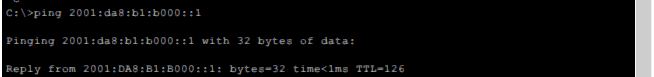
**上海分部PC2->总部PC1（tunnel 1）：**



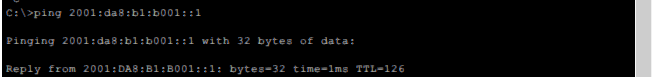
**上海分部PC2->南京分部PC4（tunnel 3）：**



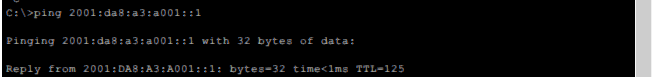
**南京分部PC4->上海分部PC2（tunnel 3）：**



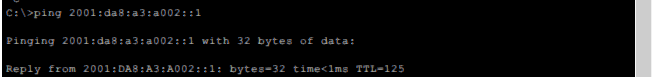
**南京分部PC4->上海分部PC3（tunnel 3）：**



**南京分部PC4->总部SERVER（tunnel 2）：**



**南京分部PC4->总部PC1（tunnel 2）：**



全部可通，测试通过。