**《网络工程与组网技术》**

**课程实验报告**

（2022学年）

实验名称 WEB访问、ACL与DNS解析

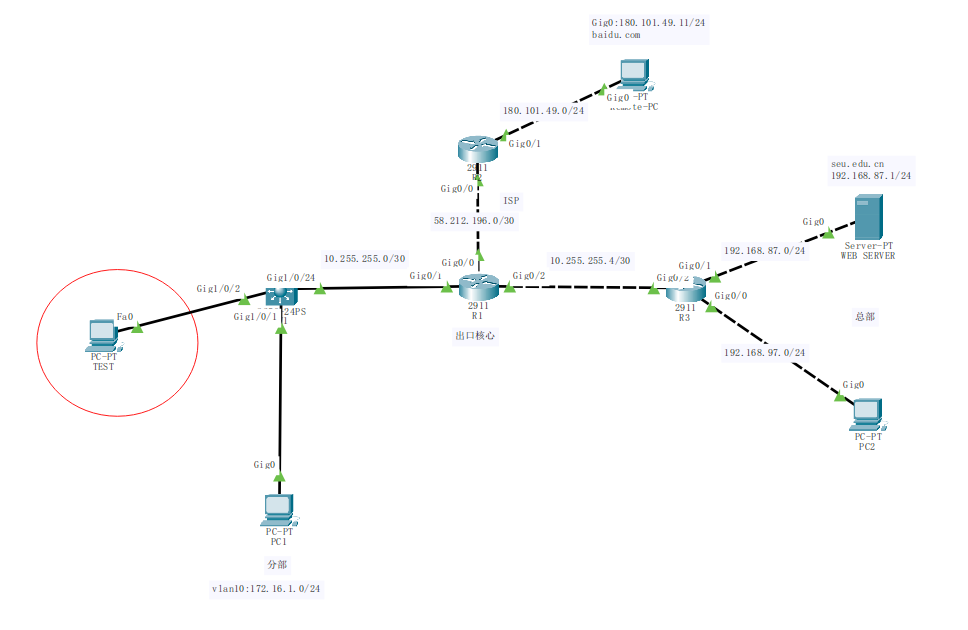
学 院

专业班级

学号姓名

2021年 8月17日

1. **实验说明**
2. 网络拓扑



（红圈中的主机是用于测试SW1的telnet功能所自行添加的，实验中不涉及）

1. 实验任务
2. IP配置

按照图中的 IP 地址规划，配置好对应设备的 IP 地址，PC 的 IP 所对应都的网关都设置为该段 IP 最后一个可 用地址。Remote-PC 上配置 IP 地址 180.101.49.11/24

**PC1配置：**

开启接口，ip地址为172.16.1.1，掩码为255.255.255.0，网关为172.16.1.254。

**PC2配置：**

开启接口，ip地址为192.168.97.1，掩码为255.255.255.0，网关为192.168.97.254。

**Remote-PC配置：**

开启接口，ip地址为180.101.49.11，掩码为255.255.255.0，网关为180.101.49.254。

**WEB\_SERVER配置：**

开启接口，ip地址为192.168.87.1，掩码为255.255.255.0，网关为192.168.87.254。

**R1配置：**

Router>en

Router#conf t

Router(config)#hostname R1

R1(config)#int Gig0/0 // R2（注释中写的是该接口所连接到的主机名称）

R1(config-if)#no shut

R1(config-if)#ip addr 58.212.196.2 255.255.255.252

R1(config-if)#exit

R1(config)#int Gig0/1 // SW1

R1(config-if)#no shut

R1(config-if)#ip addr 10.255.255.2 255.255.255.252

R1(config-if)#exit

R1(config)#int Gig0/2 // R3

R1(config-if)#no shut

R1(config-if)#ip addr 10.255.255.6 255.255.255.252

R1(config-if)#exit

**R2配置：**

Router>en

Router#conf t

Router(config)#hostname R2

R2 (config)#int Gig0/0 // R1

R2(config-if)#no shut

R2(config-if)#ip addr 58.212.196.1 255.255.255.252

R2(config-if)#exit

R2(config)#int Gig0/1 // Remote-PC

R2(config-if)#no shut

R2(config-if)#ip addr 180.101.49.1 255.255.255.0

R2(config-if)#exit

**R3配置：**

Router>en

Router#conf t

Router(config)#hostname R3

R3(config)#int Gig0/0 // PC2

R3(config-if)#no shut

R3(config-if)#ip addr 192.168.97.2 255.255.255.0

R3(config-if)#exit

R3(config-if)#int Gig0/1 // WEB\_SERVER

R3(config-if)#no shut

R3(config-if)#ip addr 192.168.87.2 255.255.255.0

R3(config-if)#exit

R3(config)#int Gig0/2 // R1

R3(config-if)#no shut

R3(config-if)#ip addr 10.255.255.5 255.255.255.252

R3(config-if)#exit

**SW1配置：**

Switch>en

Switch#conf t

Switch(config)#hostname SW1

SW1(config)#vlan 10

SW1(config-vlan)#int vlan 10

SW1(config-if)#no shut

SW1(config-if)#ip addr 172.16.1.254 255.255.255.0 // PC1网关

SW1(config-if)#exit

SW1(config)#int Gig1/0/1 // PC1

SW1(config-if)#no shut

SW1(config-if)#switchport acc

SW1(config-if)#switchport access vlan 10

SW1(config-if)#exit

SW1(config)#vlan 20

SW1(config-vlan)#int vlan 20

SW1(config-if)#no shut

SW1(config-if)#ip addr 10.255.255.1 255.255.255.252

SW1(config-if)#exit

SW1(config)#int Gig1/0/24 // R1

SW1(config-if)#no shut

SW1(config-if)#switchport access vlan 20

SW1(config-if)#exit

1. 路由配置

通过静态路由实现总部和分部互通（注意 R2 不向 R1 下发任何路由）。

需要在几个路由器中配置ip转发的下一跳路由，以R1为例：分部的网段是172.16.1.0/24，其他部门发往R1的报文需要需要经过R1，为R1配置到分部的报文的下一跳地址，应为SW1的接口Gig1/0/24，ip地址为10.255.255.0，在路由表中添加这一条目，从而实现多个网段的互通，其他路由器同理。

**R1配置：**

R1(config)#ip route 172.16.1.0 255.255.255.0 10.255.255.1 // ->分部PC1

R1(config)#ip route 192.168.87.0 255.255.255.0 10.255.255.5 // ->总部WEB\_SERVER

R1(config)#ip route 192.168.97.0 255.255.255.0 10.255.255.5 // ->总部PC2

**R3配置：**

R3(config)#ip route 0.0.0.0 0.0.0.0 10.255.255.6 // 默认路由

**SW1配置：**

SW1(config)#ip route 0.0.0.0 0.0.0.0 10.255.255.2 // 默认路由

此时分部与总部之间的各个主机可相互ping通，但到Remote-PC之间是不通的，因为R1中没有相关的路由表记录。

1. 网络地址转换

R1、R2 之间为运营商接入链路，R1 上配置 NAT，实现将 WEB-SERVER 地址的 80 端口映射到 R1 出 接口 IP 地址的 80 端口上，同时将 WEB-SERVER 地址的 53 端口映射到 R1 出接口 IP 地址的 53 端口 上，使得外网能访问 WEB-SERVER 上的 WEB 服务和 DNS 服务。

同时在 R1 上配置 NAT，使得总部分部的主机能够转换为 R1 与 R2 相连的出接口地址，访问到 Remote-PC。

**R1配置：**

R1(config)#ip route 0.0.0.0 0.0.0.0 58.212.196.1

R1(config)#access-list 1 permit 172.16.1.0 0.0.0.255 // ACL控制访问，末尾是反掩码

R1(config)#access-list 1 permit 192.168.87.0 0.0.0.255

R1(config)#access-list 1 permit 192.168.97.0 0.0.0.255

R1(config)#ip nat inside source static tcp 192.168.87.1 80 58.212.196.2 80 // 将WEB-SERVER的80端口映射到R1 Gig0/0的80端口

R1(config)#ip nat inside source static tcp 192.168.87.1 53 114.114.114.114 53 // tcp

R1(config)#ip nat inside source static udp 192.168.87.1 53 114.114.114.114 53 // udp

R1(config)#ip nat inside source list 1 interface Gig0/0 overload

R1(config-if)#int Gig0/0 // R2

R1(config-if)#ip nat outside // 外部接口

R1(config-if)#exit

R1(config-if)#int Gig0/1 // SW1

R1(config-if)#ip nat inside // 内部接口

R1(config-if)#exit

R1(config)#int Gig0/2 // R3

R1(config-if)#ip nat inside // 内部接口

R1(config-if)#exit

**R2配置：**

R2(config)#ip route 0.0.0.0 0.0.0.0 58.212.196.2 // R1作为默认路由

1. 设备管理

在 SW1 上开启 telnet 协议，设置 telnet 的密码为 dongda@2020,特权模式 enable 的密码为 dongda。

**SW1配置：**

SW1(config)#enable secret dongda // 设置特权模式密码为dongda

SW1(config)#line vty 0 4 // 开启控制台

SW1(config-line)#password dongda@2020 // 登录密码dongda@2020

SW1(config-line)#login

SW1(config-line)#transport input telnet

SW1(config-line)#exit

1. WEB访问

在 WEB\_SERVER 上开启 WEB 服务(WEB 服务已预配，无需配置)，让 PC 能访问到 WEB 服务器。

已经完成预配。

1. ACL

在 R1 配置扩展访问控制列表，要求禁止分部的 PC 访问 WEB\_SERVER 服务器，但是允许访问 WEB\_SERVER 的 DNS 服务。

在 R1 上配置扩展 ACL，禁止总部的 PC2 的 ICMP 流量访问分部的 172.16.1.0/24 网段。但是可以 telnet 到 SW1 的 172.16.1.254 网关地址。

**R1配置：**

R1(config)#access-list 100 permit udp 172.16.1.0 0.0.0.255 host 192.168.87.1 eq domain // 允许分部PC1的udp访问WEB\_SERVER

R1(config)#access-list 100 deny ip 172.16.1.0 0.0.0.255 host 192.168.87.1 // 拒绝分部PC1访问WEB\_SERVER

R1(config)#access-list 100 permit ip any any

R1(config)#access-list 101 deny icmp 192.168.97.0 0.0.0.255 172.16.1.0 0.0.0.255 // 拒绝总部PC2的icmp访问分部PC1

R1(config)#access-list 101 permit tcp 192.168.97.0 0.0.0.255 172.16.1.254 0.0.0.255 eq telnet //允许总部PC2的telnet访问分部SW1

R1(config)#access-list 101 permit ip any any

R1(config)#int Gig0/2 // R3

R1(config-if)#ip access-group 101 in

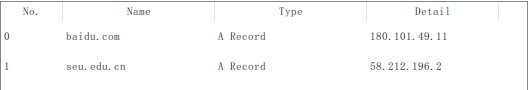
R1(config-if)#ip access-group 100 out

R1(config-if)#exit

1. DNS解析

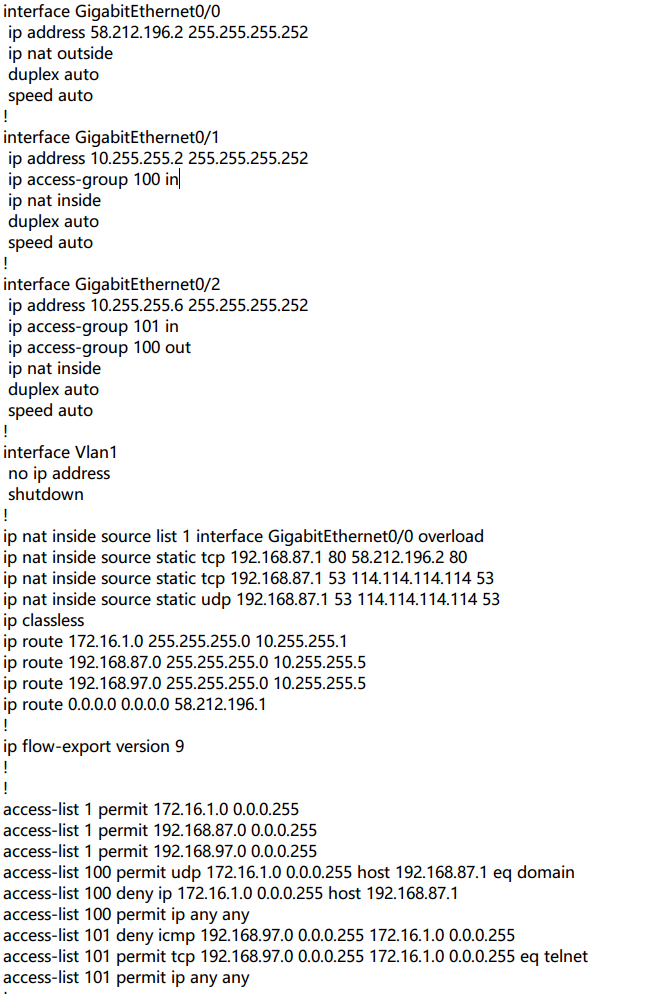
在 WEB\_SERVER 上配置 dns 服务(DNS 服务已预配，无需配置)，使得 Remote-PC 访问 seu.edu.cn 网址， 能访问 WEB\_SERVER，同时内网 ping baidu.com，可以访问到 180.101.49.11。

查看WEB\_SERVER的DNS配置，存在一条记录baidu.com – 180.101.49.11（Remote-PC），还有seu.edu.cn – 58.212.196.2（R2连接R1的接口）

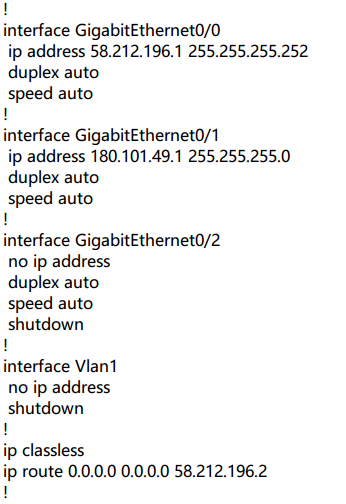


1. **网络节点配置**

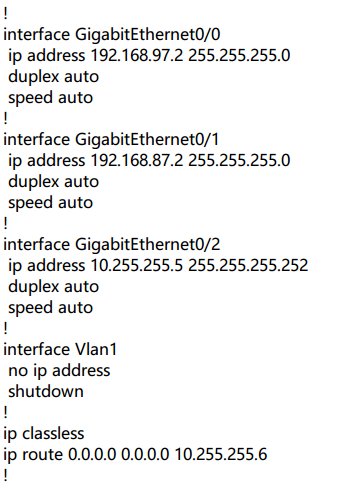
**R1部分配置文件：**



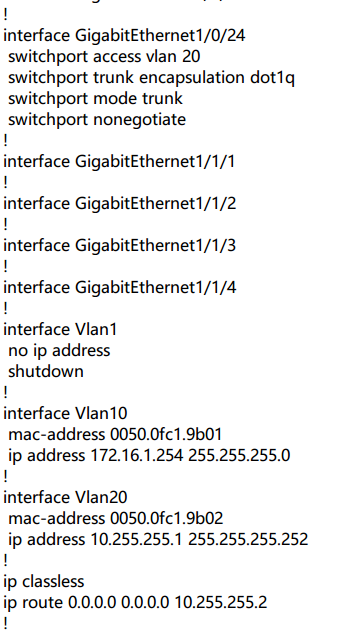
**R2部分配置文件：**



**R3部分配置文件：**

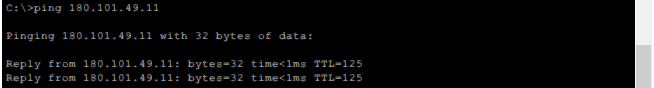


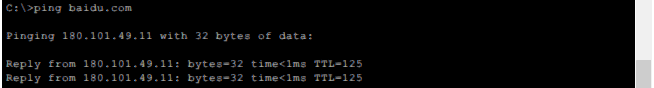
**SW1部分配置文件：**



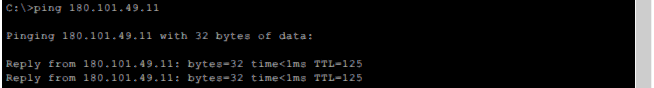
1. **功能测试**
2. 总部和分部 PC 可以 ping 通 Remote-PC 的 IP 地址和域名。

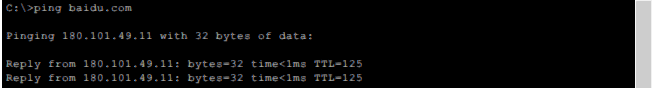
分部PC1（172.16.1.1）->Remote-PC（baidu.com 180.101.49.11）：





总部PC2(192.168.97.1) ->Remote-PC（seu.edu.cn 180.101.49.11）：

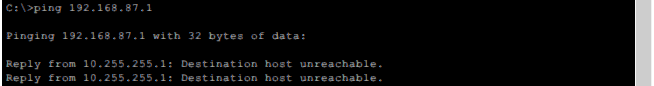




通过。

1. 测试分部的 PC 无法 ping 通总部 WEB\_SERVER。

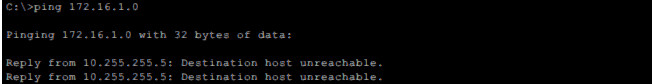
分部PC1（172.16.1.1）->WEB\_SERVER（192.168.87.1）：



主机不可达，符合流量控制要求。

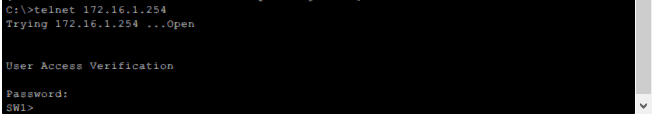
1. 测试总部 PC2 无法 ping 通分部 172.16.1.0/24 网段地址，但是可以 telnet 到 SW1 的 172.16.1.254 网关 地址。

总部PC2(192.168.97.1)->分部网段（172.16.1.0）：



主机不可达，符合流量控制要求。

总部PC2(192.168.97.1)输入telnet 172.16.1.254（SW1），输入登陆密码dongda@2020：



成功登录，符合要求。

1. 通过在 Remote-PC 上的浏览器测试 seu.edu.cn，看看是否可以访问到 WEB\_SERVER。

在Remote-PC中的网页浏览器中的地址栏输入seu.edu.cn访问东南大学主页：



成功访问，符合要求。