

# 校园网项目实验报告

## 一、题目

按拓扑图完成校园网设计项目，要求如下：

- (1) 所有主机可访问外网；
- (2) 主机可通过域名访问 Web 服务器，选做 FTP 服务器；
- (3) 为网络配置动态路由；
- (4) 教学楼主机通过 DHCP 自动获取地址，办公楼划分 VLAN；
- (5) 科技楼主机使用专用地址，需通过 NAT 来访问外网（选做）；
- (6) 无线局域网采用 AC+FIT AP 模式（选做）；
- (7) 为设备分配合适的 IP 地址和子网掩码，IP 地址的第二个字节使用学号的后两位；
- (8) 在已经配置过的交换机和路由器的用户视图下运行 save 命令以保存配置，然后在 eNSP 菜单中点击“保存”以保存拓扑，文件名为“学号姓名”，将文件压缩后提交（压缩文件名仍为“学号姓名”），同时需要提交报告。

## 二、网络规划

### 1. 基于 IP 子网划分 VLAN

- (1) LSW1 汇聚层交换机

端口号	端口类型	所属 VLAN	IP
GE 0/0/1	trunk	VLAN7	10.94.8.1
GE 0/0/2	trunk	VLAN1	10.94.1.1
GE 0/0/3	trunk	VLAN2	10.94.2.1

端口号	端口类型	所属 VLAN	IP
GE 0/0/4	trunk	VLAN3	10.94.3.1

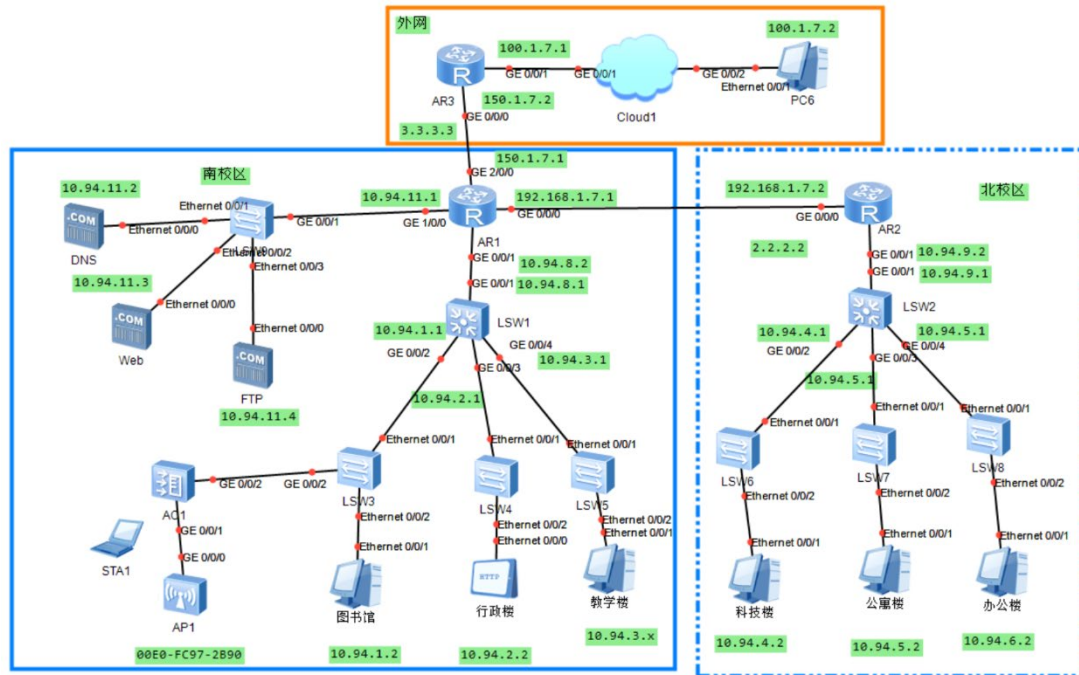
(2) LSW2 汇聚层交换机

端口号	端口类型	所属 VLAN	IP
GE 0/0/1	trunk	VLAN7	10.94.9.1
GE 0/0/2	trunk	VLAN1	10.94.4.1
GE 0/0/3	trunk	VLAN2	10.94.5.1
GE 0/0/4	trunk	VLAN3	10.94.6.1

(3) IP 地址规划

地址	IP 地址	网关
图书馆 PC1	10.94.1.2/24	10.94.1.1
行政楼（客户机）	10.94.2.2/24	10.94.2.2
教学楼 PC3	10.94.3.2/24	10.94.3.1
科技楼 PC4	10.94.4.2/24	10.94.4.1
公寓楼 PC5	10.94.5.2/24	10.94.5.1
办公楼 PC6	10.94.6.2/24	10.94.6.1
DNS 服务器	10.94.10.2/24	10.94.10.1
Web 服务器	10.94.10.3/24	10.94.10.1

2. 功能部署与网络拓扑图



### 三、配置 VLAN

#### 1. 配置三层交换机

以三层交换机 LSW3 为例：

1. `vlan batch 1`
2. `interface Ethernet 0/0/2`
3. `port link-type access`
4. `port default vlan 1`
5. `quit`
6. `interface e0/0/1`
7. `port link-type trunk`
8. `port trunk allow-pass vlan 1`
9. `quit`

#### 2. 配置二层交换机

以二层交换机 LSW1 为例：

(1) 进入配置模式

```
un in en
```

un 是缩写，用于解除设备的特权模式。

in 是进入全局配置模式。

en 是进入特权模式。

## (2) 创建 VLAN

```
vlan batch 1 2 3 7
```

创建 VLAN 1、2、3 和 7。这些 VLAN 将用于网络的不同部分。

## (3) 配置接口 GigabitEthernet0/0/2

```
1. int gi0/0/2
2. port link-type trunk
3. port trunk allow-pass vlan 1
```

进入接口 GigabitEthernet0/0/2 的配置模式。

将接口设置为 trunk 模式，允许它传输多个 VLAN 的数据。

允许 VLAN 1 通过这个 trunk 接口。

## (3) 配置接口 GigabitEthernet0/0/3

```
1. int gi0/0/3
2. port link-type trunk
3. port trunk allow-pass vlan 2
```

进入接口 GigabitEthernet0/0/3 的配置模式。

将接口设置为 trunk 模式。

允许 VLAN 2 通过这个 trunk 接口。

## (4) 配置接口 GigabitEthernet0/0/4

```
1. int gi0/0/4
2. port link-type trunk
3. port trunk allow-pass vlan 3
```

进入接口 GigabitEthernet0/0/4 的配置模式。

将接口设置为 trunk 模式。

允许 VLAN 3 通过这个 trunk 接口。

(5) 配置接口 GigabitEthernet0/0/1

```
1. int g0/0/1
2. port link-type access
3. port default vlan 1
4. port default vlan 2
5. port default vlan 3
6. port default vlan 7
```

进入接口 GigabitEthernet0/0/1 的配置模式。

将接口设置为 access 模式，即只能属于一个 VLAN。

依次将接口的默认 VLAN 设置为 1、2、3 和 7，这可能是配置中的一个错误，

通常一个接口只能属于一个 VLAN。

(6) 配置 VLAN 接口并分配 IP 地址

```
1. int vlanif 1
2. ip add 10.94.1.1 24
3. int vlanif 2
4. ip add 10.94.2.1 24
5. int vlanif 3
6. ip add 10.94.3.1 24
7. int vlanif 7
8. ip add 10.94.8.1 24
```

分别进入 VLAN 1、2、3 和 7 的逻辑接口配置模式。

为每个 VLAN 接口分配 IP 地址：

VLAN 1: 10.94.1.1/24

VLAN 2: 10.94.2.1/24

VLAN 3: 10.94.3.1/24

VLAN 7: 10.94.8.1/24

## (6) 配置静态路由

```
ip route-static 0.0.0.0 0 10.94.8.2
```

配置一条静态路由，目的地为 0.0.0.0/0（即所有网络），下一跳地址为 10.94.8.2。这通常用于指向默认网关。

该配置主要是为 LSW1 交换机设置不同的 VLAN，并为每个 VLAN 分配对应的 IP 地址。接口 Gi0/0/2、Gi0/0/3 和 Gi0/0/4 被配置为 trunk 模式，分别传输 VLAN 1、2 和 3 的数据。最后，通过配置静态路由，确保 LSW1 能通过网关 10.94.8.2 访问其他网络。

## 3.配置路由

以 R1 为例：

### (1) 创建 VLAN 7

```
vlan 7
```

创建 VLAN 7，这是用来划分网络广播域的虚拟局域网。

### (2) 配置接口 GigabitEthernet 0/0/1

```
1. int g0/0/1
2. ip add 10.94.8.2 24
```

进入接口 GigabitEthernet 0/0/1 的配置模式。

为该接口分配 IP 地址 10.94.8.2，子网掩码为 255.255.255.0。

这个接口连接到 LSW1，IP 地址 10.94.8.1 作为它的网关。

### (3) 配置接口 GigabitEthernet 0/0/0

```
1. int g0/0/0
2. ip add 192.168.7.1 24
```

进入接口 GigabitEthernet 0/0/0 的配置模式。

为该接口分配 IP 地址 192.168.7.1，子网掩码为 255.255.255.0。

这个接口可连接到其他设备（如 AR2），用于北校区的通信。

#### （4）配置接口 GigabitEthernet 2/0/0

```
1. int g2/0/0
2. ip add 150.1.7.1 24
```

进入接口 GigabitEthernet 2/0/0 的配置模式。

为该接口分配 IP 地址 150.1.7.1，子网掩码为 255.255.255.0。

这个接口用于连接到外部网络或其他子网。

#### （5）创建 VLAN 11

vlan 11

创建 VLAN 11，这是用来划分另一个网络广播域的虚拟局域网。

#### （6）配置接口 GigabitEthernet 1/0/0

```
1. int g1/0/0
2. ip add 10.94.11.1 24
```

进入接口 GigabitEthernet 1/0/0 的配置模式。

为该接口分配 IP 地址 10.94.11.1，子网掩码为 255.255.255.0。

这个接口可连接到南校区的设备。

#### （7）配置访问控制列表（ACL）2000

```
1. acl number 2000
2. rule 5 permit source 10.94.0.0 0.0.255.255
3. q
```

创建编号为 2000 的 ACL。

配置规则 5，允许源地址为 10.94.0.0/16 的流量通过。

ACL 通常用于流量过滤和安全策略。

#### (8) 配置静态路由

```
1. ip route-static 10.94.1.0 24 10.94.8.1
2. ip route-static 10.94.2.0 255.255.255.0 10.94.8.1
3. ip route-static 10.94.3.0 255.255.255.0 10.94.8.1
4. ip route-static 10.94.4.0 255.255.255.0 192.168.7.2
5. ip route-static 10.94.5.0 255.255.255.0 192.168.7.2
6. ip route-static 10.94.6.0 255.255.255.0 192.168.7.2
7. ip route-static 10.94.1.0 255.255.255.0 10.94.8.1
```

配置到各个子网的静态路由，使得 AR1 能够将流量正确转发到目标网络。

到 10.94.1.0/24 的路由通过 10.94.8.1

到 10.94.2.0/24 的路由通过 10.94.8.1

到 10.94.3.0/24 的路由通过 10.94.8.1

到 10.94.4.0/24 的路由通过 192.168.7.2

到 10.94.5.0/24 的路由通过 192.168.7.2

到 10.94.6.0/24 的路由通过 192.168.7.2

AR2 的路由表：

```
ip route-static 0.0.0.0 0.0.0.0 192.168.7.1
```

```
ip route-static 10.94.4.0 255.255.255.0 10.94.9.1
```

```
ip route-static 10.94.5.0 255.255.255.0 10.94.9.1
```

```
ip route-static 10.94.6.0 255.255.255.0 10.94.9.1
```

#### 4.配置主机 IP 地址

按照拓扑图，配置 ip 地址。

以图书馆为例：



图书馆

基础配置 | 命令行 | 组播 | UDP发包工具 | 串口

主机名:

MAC 地址:

**IPv4 配置**

☒ 静态 ☐ DHCP ☐ 自动获取 DNS 服务器地址

IP 地址:  DNS1:

子网掩码:  DNS2:

网关:

**IPv6 配置**

☒ 静态 ☐ DHCPv6

IPv6 地址:

前缀长度:

IPv6 网关:

应用

#### 四、教学楼开启 DHCP 服务

DHCP：动态主机配置协议，用来分配 IP 地址等网络参数，在路由器，核心交换机，Linux 等上面都可以配置 DHCP。

配置方式有：全局建立地址池方式，基于接口的方式，以及 DHCP 中继配置方式。

选用基于接口方式，在 LSW1 上配置：

1. `dhcp enable` #在 LSW1 上开启 dhcp 服务
2. `interface vlan 3`
3. `dhcp select interface`
4. `dhcp server dns-list 114.114.114.114 223.5.5.5`

测试 DHCP 服务：

将教学楼 IPv4 配置由静态 IP 改为 DHCP

**IPv4 配置**

☐ 静态 ☒ DHCP ☒ 自动获取 DNS 服务器地址

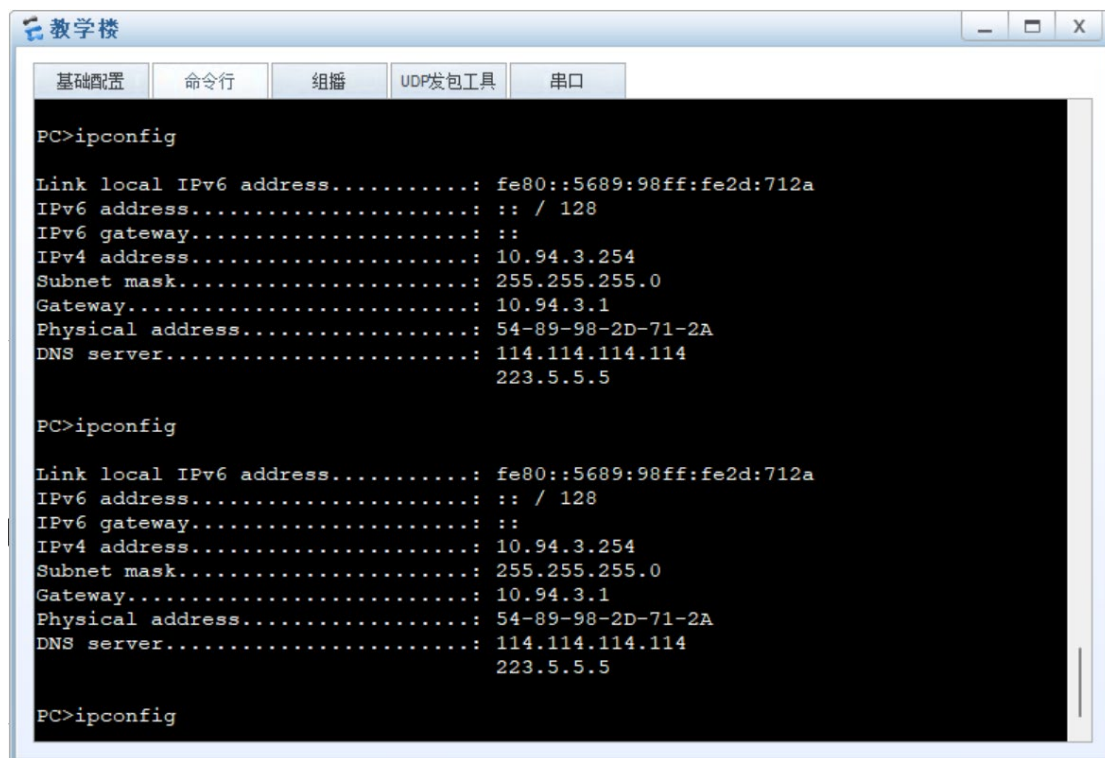
IP 地址:

子网掩码:

网关:

DNS1:

DNS2:



## 五、添加 Web 服务器和 DNS 服务器

为测试服务器是否正确运行，将行政楼换为客户端。

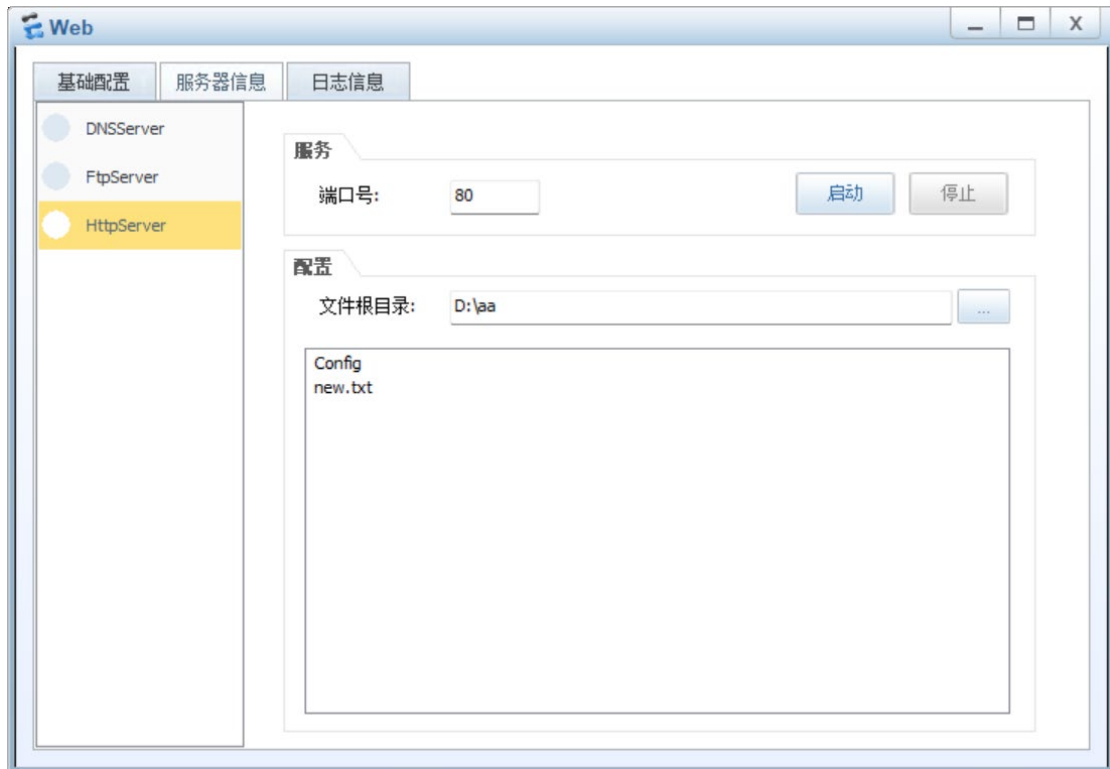
规划 IP：

设备	IP	网关	域名服务器
DNS 服务器	10.94.11.2/24	10.86.11.1	无
WEB 服务器	10.94.11.3/24	10.86.11.1	无
R1 路由器接口 E0/0/0	10.94.11.1/24	无	无
Client 客户机	10.94.2.2/24	10.94.2.1	10.94.11.2

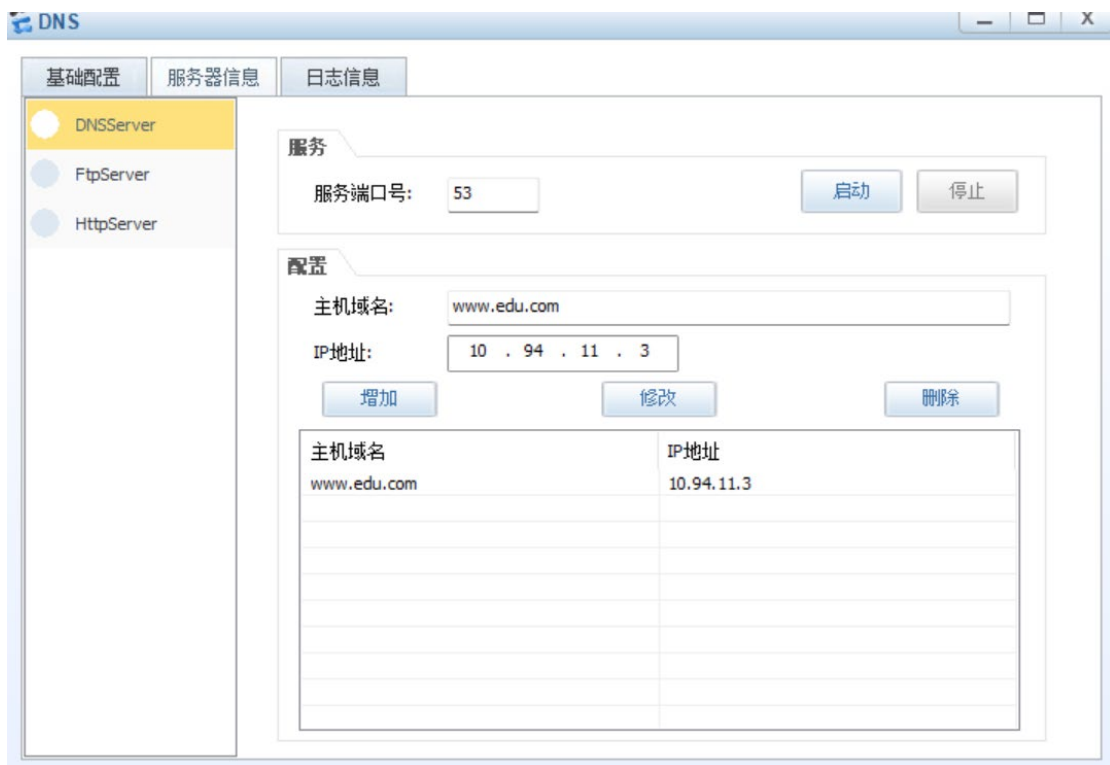
依照拓扑图添加 IP，在各个设备上设置 IP

### 1.搭建 WEB 服务

设置服务器如图：



## 2.在 DNS 服务器上选择 DNSServer



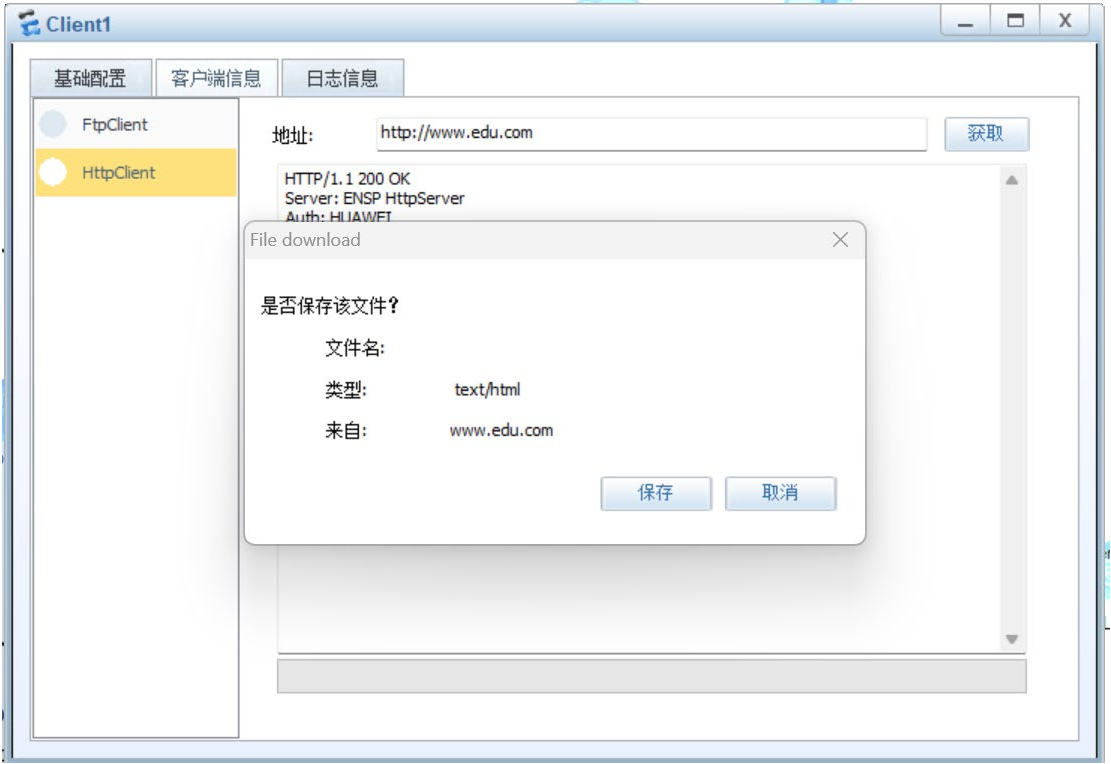
## 3. Cilent 客户机测试

PING 测试：目的 IPV4 分别为 web 服务器 ip 和 dns 服务器 ip，次数选择 5，点

击发送，测试成功。



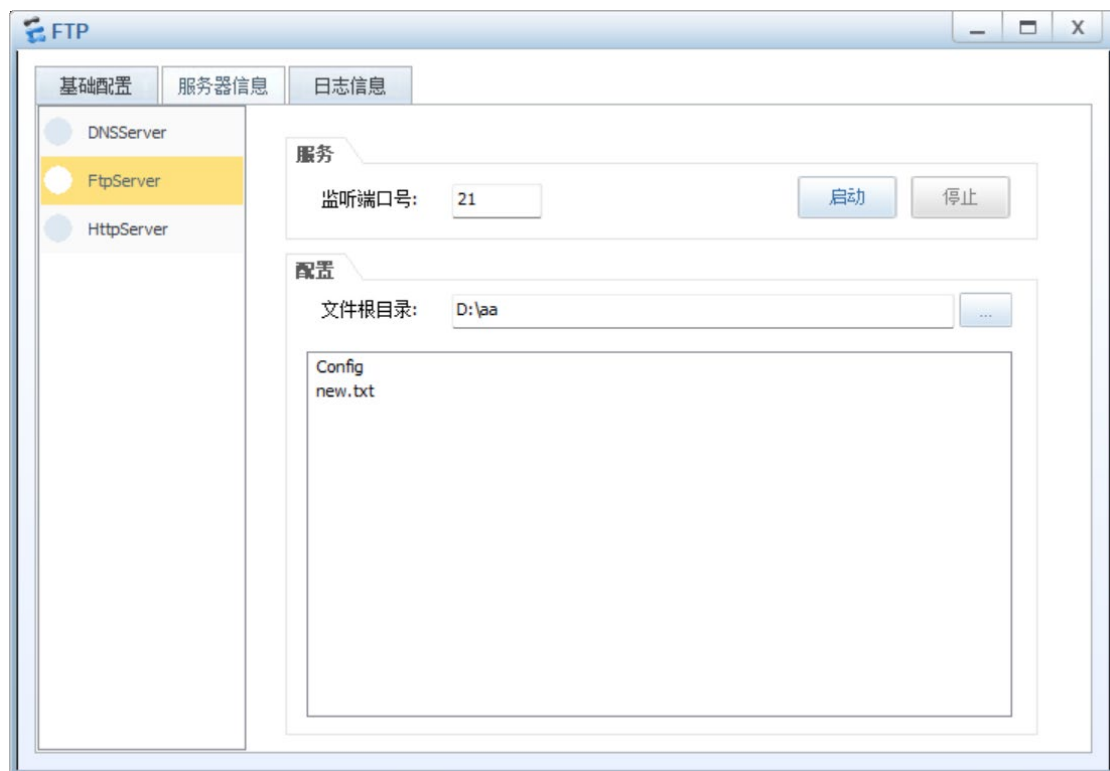
在客户端信息 HttpClient 中输入 www.edu.com,可以获取成功。



## 5.配置 FTP

在本地创建一个 FTP-Huawei 文件夹，然后再创建一个子文件夹 Config，再

在里面创建一个 test.txt 文件，在 Server1 上应用，并启动 FTP 服务。



在路由器 R1 上配置：

1. FTP 192.168.1.1 //连接ftp 服务器
2. ls //查看服务器文件夹状态
3. dir //查看详细的文件属性
4. cd Config //进入Config 文件夹
5. get test.txt //下载test.txt 文件到FTP 服务器
6. put test.txt new.txt //上传test.txt 到FTP 服务器，命名为new.txt
7. system-view //进入视图模式
8. ftp server enable //打开FTP 服务器功能
9. aaa
10. local-user ftp password cipher huawei //用户名为ftp，密码为huawei
11. local-user ftp ftp-directory flash: //设置文件夹目录为flash:
12. local-user ftp service-type ftp //服务类型为ftp
13. local-user ftp privilege level 15 //用户优先级为15

过程截图如下：

```

<Huawei>ftp 10.94.11.4
Trying 10.94.11.4 ...

Press CTRL+K to abort
Connected to 10.94.11.4.
220 FtpServerTry FtpD for free
User(10.94.11.4:(none)):XDU
331 Password required for XDU .
Enter password:
230 User XDU logged in , proceed

[Huawei-ftp]dir
200 Port command okay.
150 Opening ASCII NO-PRINT mode data connection for ls -l.
drwxrwxrwx 1 XDU nogroup 0 May 28 2024 Config
226 Transfer finished successfully. Data connection closed.
FTP: 66 byte(s) received in 0.200 second(s) 330.00byte(s)/sec.

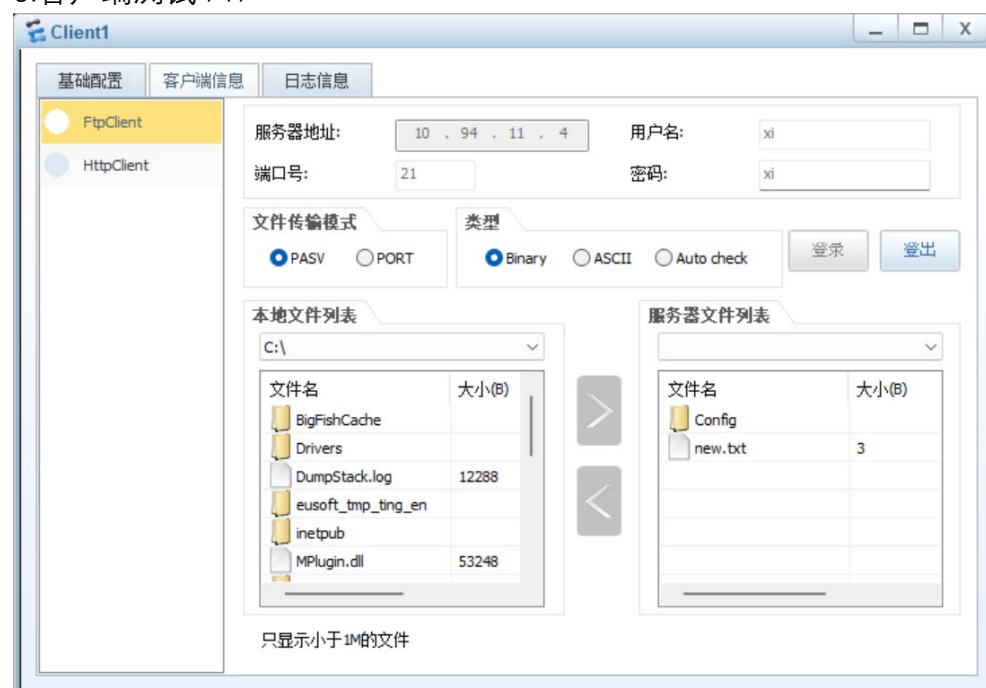
[Huawei-ftp]cd Config
250 "/Config" is current directory.

[Huawei-ftp]get test.txt
200 Port command okay.
150 Sending test.txt (0 bytes). Mode STREAM Type BINARY
226 Transfer finished successfully. Data connection closed.
FTP: 0 byte(s) received in 0.300 second(s) 0.00byte(s)/sec.

[Huawei-ftp]put test.txt new.txt
200 Port command okay.
150 Opening BINARY data connection for new.txt
226 Transfer finished successfully. Data connection closed.
FTP: 0 byte(s) received in 0.300 second(s) 0.00byte(s)/sec.
<Huawei>SYS
Enter system view, return user view with Ctrl+Z.
[Huawei]aaa
[Huawei-aaa]local-user xi password cipher xi
Info: Add a new user.
[Huawei-aaa]local-user xi ftp-directory flash:
[Huawei-aaa]local-user xi service-type ftp
[Huawei-aaa]local-user xi privilege level 15
[Huawei-aaa]

```

## 5.客户端测试 FTP



## 六、配置动态路由

R1 设置为整个校园网的出口，因此 g0/0/1 应设置为外网网段。

RIP 协议是一种内部网关协议（IGP），底层是贝尔曼福特算法，是一种动态路由选择协议，用于自治系统（AS）内的路由信息的传递。

### 1.配置 R1:

#### (1) 配置接口 GigabitEthernet 2/0/0

```
1. interface GigabitEthernet2/0/0
2. ip address 150.1.7.1 24
```

进入接口 GigabitEthernet 2/0/0 的配置模式。

为该接口分配 IP 地址 150.1.7.1，子网掩码为 255.255.255.0。

这个接口用于连接外部网络或其他子网，并作为出口接口。

#### (2) 配置 Loopback 接口 0

```
1. interface LoopBack 0
2. ip address 1.1.7.1 32
```

进入 Loopback 0 接口的配置模式。

为 Loopback 0 接口分配 IP 地址 1.1.7.1，子网掩码为 255.255.255.255 (/32)。

Loopback 接口是一种逻辑接口，通常用于路由协议的标识符或管理目的，因为它始终保持活动状态。

#### (3) 进入 RIP 配置模式

```
1. rip
2. version 2
3. network 192.168.7.0
4. network 1.0.0.0
5. network 10.0.0.0
6. network 150.0.0.0
```

## 7. undo summary

进入 RIP (Routing Information Protocol) 的配置模式。

设置 RIP 的版本为 2，RIP 版本 2 支持子网掩码信息的传递，增强了路由信息的传递能力。

使用 network 命令指定参与 RIP 路由的网络：

192.168.7.0：这个网络包括接口 GigabitEthernet 0/0/0。

1.0.0.0：包括 Loopback 0 接口。

10.0.0.0：可能包括其他内部网络。

150.0.0.0：包括接口 GigabitEthernet 2/0/0。

undo summary 命令禁用了 RIP 路由信息的自动汇总，确保精确的子网信息传递。

### (4) 配置静态路由

```
ip route-static 0.0.0.0 0 150.1.7.2
```

配置一条静态默认路由，目的地为 0.0.0.0/0（即所有网络），下一跳地址为 150.1.7.2。如果找不到匹配的具体路由，则将流量转发到 150.1.7.2。

这部分配置主要是为 AR1 配置外部连接和 RIP 路由协议。GigabitEthernet 2/0/0 接口用于连接到外部网络。Loopback 0 接口用于标识和管理目的。配置了 RIP 路由协议，使 AR1 可以与其他支持 RIP 的路由器交换路由信息。配置静态默认路由，确保流量可以转发到外部网络。

## 2.配置 R2

### (1) 配置 Loopback 接口 0

```
1. interface LoopBack 0
```



## 2. ip address 2.2.2.2 32

进入 Loopback 0 接口的配置模式。

为 Loopback 0 接口分配 IP 地址 2.2.2.2，子网掩码为 255.255.255.255 (/32)。

Loopback 接口是一种逻辑接口，通常用于路由协议的标识符或管理目的，因为它始终保持活动状态。

### (2) 进入 RIP 配置模式

```
1. rip
2. version 2
3. network 192.168.7.0
4. network 2.0.0.0
5. network 10.0.0.0
6. undo summary
```

进入 RIP (Routing Information Protocol) 的配置模式。

设置 RIP 的版本为 2，RIP 版本 2 支持子网掩码信息的传递，增强了路由信息的传递能力。

使用 network 命令指定参与 RIP 路由的网络：

192.168.7.0：这个网络包括接口连接到 192.168.7.x 网络，例如连接 AR1 的接口。

2.0.0.0：包括 Loopback 0 接口。

10.0.0.0：可能包括其他内部网络。

undo summary 命令禁用了 RIP 路由信息的自动汇总，确保精确的子网信息传递。

为 R2 配置一个 Loopback 接口，并启用 RIP 路由协议。Loopback 0 接口用于标识和管理目的，IP 地址为 2.2.2.2。配置了 RIP 路由协议，使 R2 可以与其他

支持 RIP 的路由器（如 AR1）交换路由信息。undo summary 确保了 RIP 不对网络信息进行自动汇总，从而传递更精确的子网信息。

### 3.配置 R3:

#### (1) 配置接口 GigabitEthernet 0/0/0

```
1. int gi0/0/0
2. ip address 150.1.7.2 24
```

进入接口 GigabitEthernet 0/0/0 的配置模式。

为该接口分配 IP 地址 150.1.7.2，子网掩码为 255.255.255.0。

这个接口连接到 AR1 的 GigabitEthernet 2/0/0 接口，用于与 AR1 进行通信。

#### (2) 配置 Loopback 接口 0

```
1. interface LoopBack 0
2. ip address 3.3.3.3 32
```

进入 Loopback 0 接口的配置模式。

为 Loopback 0 接口分配 IP 地址 3.3.3.3，子网掩码为 255.255.255.255 (/32)。

Loopback 接口是一种逻辑接口，通常用于路由协议的标识符或管理目的，因为它始终保持活动状态。

#### (3) 进入 RIP 配置模式

```
1. rip
2. version 2
3. network 150.0.0.0
4. network 3.0.0.0
```

进入 RIP（Routing Information Protocol）的配置模式。

设置 RIP 的版本为 2，RIP 版本 2 支持子网掩码信息的传递，增强了路由信息的

传递能力。

使用 network 命令指定参与 RIP 路由的网络：

150.0.0.0：包括接口 GigabitEthernet 0/0/0。

3.0.0.0：包括 Loopback 0 接口。

#### (4) 配置静态路由

```
ip route-static 10.94.0.0 16 150.1.7.1
```

配置一条静态路由，目的地为 10.94.0.0/16（即包括 10.94.x.x 的所有子网），下一跳地址为 150.1.7.1。如果目的地址在 10.94.0.0/16 子网中，则将流量转发到 150.1.7.1（AR1）。

#### (5) 配置接口 GigabitEthernet 0/0/1

```
1. int gi0/0/1
2. ip address 100.1.7.1 24
```

进入接口 GigabitEthernet 0/0/1 的配置模式。

为该接口分配 IP 地址 100.1.7.1，子网掩码为 255.255.255.0。

为 R3 配置外部连接、Loopback 接口和 RIP 路由协议。GigabitEthernet 0/0/0 接口用于与 AR1 进行通信，IP 地址为 150.1.7.2。Loopback 0 接口用于标识和管理目的，IP 地址为 3.3.3.3。配置了 RIP 路由协议，使 R3 可以与其他支持 RIP 的路由器交换路由信息。配置静态路由，确保 R3 能够将流量正确地引导到目标网络。GigabitEthernet 0/0/1 接口用于连接到外部网络或其他设备，IP 地址为 100.1.7.1。

#### 4.测试动态路由

dis ip ro 查看 R1 路由表：

```
[Huawei]display current-configuration
[V200R003C00]
#
board add 0/1 lGEC
board add 0/2 lGEC
#
snmp-agent local-engineid 800007DB0300000000000000
snmp-agent
#
clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
drop illegal-mac alarm
#
vlan batch 7 11
#
wlan ac-global carrier id other ac id 0
#
set cpu-usage threshold 80 restore 75
#
dhcp enable
#
acl number 2000
rule 5 permit source 10.94.0.0 0.0.255.255
acl number 2001
rule 5 permit source 10.94.1.0 0.0.0.255
acl number 2002
rule 5 permit source 10.94.2.0 0.0.0.255
acl number 2003
rule 5 permit source 10.94.3.0 0.0.0.255
acl number 2004
rule 5 permit source 10.94.4.0 0.0.0.255
acl number 2005
rule 5 permit source 10.94.5.0 0.0.0.255
acl number 2006
rule 5 permit source 10.94.6.0 0.0.0.255
#
ip pool vlan_3
gateway-list 10.94.3.1
network 10.94.3.0 mask 255.255.255.0
dns-list 119.29.29.29
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8br
local-user admin service-type http
#
```

```
firewall zone Local
priority 15
#
nat address-group 1 150.1.1.100 150.1.1.200
nat address-group 2 150.1.2.100 150.1.2.200
nat address-group 3 150.1.3.100 150.1.3.200
nat address-group 4 150.1.4.100 150.1.4.200
nat address-group 5 150.1.5.100 150.1.5.200
nat address-group 6 150.1.6.100 150.1.6.200
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface GigabitEthernet0/0/0
ip address 192.168.7.1 255.255.255.0
nat outbound 2001 address-group 1 no-pat
nat outbound 2002 address-group 2 no-pat
nat outbound 2003 address-group 3 no-pat
nat outbound 2004 address-group 4 no-pat
nat outbound 2005 address-group 5 no-pat
nat outbound 2006 address-group 6 no-pat
#
interface GigabitEthernet0/0/1
ip address 10.94.8.2 255.255.255.0
dhcp select global
#
interface GigabitEthernet1/0/0
ip address 10.94.11.1 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 150.1.7.1 255.255.255.0
#
interface NULL0
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
#
rip 1
#
rip 1
undo summary
version 2
network 192.168.7.0
network 1.0.0.0
network 10.0.0.0
network 150.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 10.94.8.1
ip route-static 0.0.0.0 0.0.0.0 150.1.7.2
ip route-static 10.94.1.0 255.255.255.0 10.94.8.1
ip route-static 10.94.2.0 255.255.255.0 10.94.8.1
ip route-static 10.94.3.0 255.255.255.0 10.94.8.1
ip route-static 10.94.4.0 255.255.255.0 192.168.7.2
ip route-static 10.94.5.0 255.255.255.0 192.168.7.2
ip route-static 10.94.6.0 255.255.255.0 192.168.7.2
#
user-interface con 0
authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

dis ip ro 查看 R2 路由表:

```
[Huawei]display current-configuration
[V200R003C00]
#
snmp-agent local-engineid 800007DB0300000000000000
snmp-agent
#
clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
drop illegal-mac alarm
#
vlan batch 7
#
wlan ac-global carrier id other ac id 0
#
set cpu-usage threshold 80 restore 75
#
acl number 2000
rule 5 permit source 10.94.0.0 0.0.255.255
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
local-user admin service-type http
#
firewall zone Local
priority 15
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface GigabitEthernet0/0/0
ip address 192.168.7.2 255.255.255.0
#
interface GigabitEthernet0/0/1
ip address 10.94.9.2 255.255.255.0
#
interface NULL0
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
#
rip 1
undo summary
version 2
network 192.168.7.0
network 2.0.0.0
network 10.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.7.1
ip route-static 10.94.4.0 255.255.255.0 10.94.9.1
ip route-static 10.94.5.0 255.255.255.0 10.94.9.1
ip route-static 10.94.6.0 255.255.255.0 10.94.9.1
#
user-interface con 0
authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
-----
```

10.94.6.2ping 100.1.7.2:

```
PC>tracert 100.1.7.2

tracert to 100.1.7.2, 8 hops max
(ICMP), press Ctrl+C to stop
 1  10.94.6.1    47 ms  31 ms  47 ms
 2  10.94.9.2    63 ms  62 ms  63 ms
 3  192.168.7.1  93 ms  63 ms  62 ms
 4  150.1.7.2    63 ms  62 ms  63 ms
 5  100.1.7.2    78 ms  94 ms  78 ms

PC5
```

基础配置	命令行	组播	UDP发包工具	串口
From 100.1.7.2: bytes=32 seq=3 ttl=124 time=78 ms				
From 100.1.7.2: bytes=32 seq=4 ttl=124 time=63 ms				
From 100.1.7.2: bytes=32 seq=5 ttl=124 time=78 ms				
--- 100.1.7.2 ping statistics ---				
5 packet(s) transmitted				
4 packet(s) received				
20.00% packet loss				
round-trip min/avg/max = 0/70/78 ms				
PC>ping 100.1.7.2				
Ping 100.1.7.2: 32 data bytes, Press Ctrl_C to break				
Request timeout!				
From 100.1.7.2: bytes=32 seq=2 ttl=124 time=78 ms				
From 100.1.7.2: bytes=32 seq=3 ttl=124 time=63 ms				
From 100.1.7.2: bytes=32 seq=4 ttl=124 time=94 ms				
From 100.1.7.2: bytes=32 seq=5 ttl=124 time=46 ms				
--- 100.1.7.2 ping statistics ---				
5 packet(s) transmitted				
4 packet(s) received				
20.00% packet loss				
round-trip min/avg/max = 0/70/94 ms				
PC>				

## 七、为科技楼配置 NAT

### 1.配置 AR1

#### (1) 配置 NAT 地址组

```
nat address-group 4 150.1.4.100 150.1.4.200
```

创建一个 NAT 地址组 4，地址范围从 150.1.4.100 到 150.1.4.200。

#### (2) 配置访问控制列表（ACL）2004

```
1. acl 2004
2. rule permit source 10.94.4.2 0.0.0.255
3. q
```

创建编号为 2004 的 ACL。

配置规则允许源地址为 10.94.4.2/24（即 10.94.4.2 到 10.94.4.255）的流量。

(3) 在接口 GigabitEthernet 0/0/0 上应用 NAT

```
1. interface GigabitEthernet0/0/0
2. nat outbound 2004 address-group 4 no-pat
3. q
```

进入接口 GigabitEthernet 0/0/0 的配置模式。

将 ACL 2004 中匹配的流量进行 NAT 转换，使用地址组 4 中的地址范围，并且不进行端口地址转换（no-pat）。

2.配置 AR2：

(1) 配置接口 GigabitEthernet 0/0/0

```
1. interface GigabitEthernet 0/0/0
2. ip address 192.168.7.2 255.255.255.0
```

进入接口 GigabitEthernet 0/0/0 的配置模式。

为该接口分配 IP 地址 192.168.7.2，子网掩码为 255.255.255.0。

这个接口连接到 AR1，IP 地址为 192.168.7.1。

(2) 配置接口 GigabitEthernet 0/0/1

```
1. interface GigabitEthernet 0/0/1
2. ip address 10.94.9.2 255.255.255.0
```

进入接口 GigabitEthernet 0/0/1 的配置模式。

为该接口分配 IP 地址 10.94.9.2，子网掩码为 255.255.255.0。

这个接口连接到北校区，IP 地址为 10.94.9.1。

(3) 配置 NAT 地址组

```
1. nat address-group 1 10.94.9.3 10.94.9.254
```

创建一个 NAT 地址组 1，地址范围从 10.94.9.3 到 10.94.9.254。

(4) 配置访问控制列表 (ACL) 2000

```
1. acl number 2000
2. rule 5 permit source 10.94.4.0 0.0.0.255
```

创建编号为 2000 的 ACL。

配置规则允许源地址为 10.94.4.0/24（即 10.94.4.x）的流量。

(5) 在接口 GigabitEthernet 0/0/0 上应用 NAT

```
1. interface GigabitEthernet 0/0/0
2. nat outbound 2000 address-group 1
```

进入接口 GigabitEthernet 0/0/0 的配置模式。

将 ACL 2000 中匹配的流量进行 NAT 转换，使用地址组 1 中的地址范围。

(6) 配置静态路由

```
ip route-static 0.0.0.0 0.0.0.0 10.94.9.1
```

配置一条默认静态路由，目的地为 0.0.0.0/0（即所有网络），下一跳地址为 10.94.9.1。如果找不到匹配的具体路由，则将流量转发到 10.94.9.1（北校区的网关）。

display nat address-group 查看地址池信息：

AR1:

```
[Huawei]display nat address-group

NAT Address-Group Information:
-----
Index      Start-address      End-address
-----
4          150.1.4.100        150.1.4.200
-----
Total : 1
```



AR2:

```
[Huawei]display nat address-group

NAT Address-Group Information:
-----
Index      Start-address      End-address
-----
1           10.94.9.3          10.94.9.254
-----
Total : 1
```

效果:

## I 地址隔离

通过在不同的路由器上配置不同的 NAT 地址组，可以有效隔离和管理不同网络段的流量。

AR1 的 NAT 地址组用于将特定内网段的流量转换为公共地址，以便访问外部网络。

AR2 的 NAT 地址组用于将另一个内网段的流量转换为其他内部地址，为了与特定的内部服务器或网络段进行通信。

## II 流量控制和安全

使用不同的 NAT 地址组可以更好地控制流量，确保不同的网络段和设备只能访问它们被允许访问的网络资源。这种配置有助于提高网络的安全性和管理性，通过限制和监控不同网络段之间的通信。

AR1 连接到某些外部服务或公共网络，而 AR2 主要处理内部网络段之间的通信和访问。

## 八、无线局域网 AC+FIT AP 模式

配置 AC 如下:

1. [AC6005]vlan batch 100 101 //100 为业务 VLAN
- 2.

```
3. [AC6005-vlan101]int g0/0/1
4.
5. [AC6005-GigabitEthernet0/0/1]port link-type trunk
6.
7. [AC6005-GigabitEthernet0/0/1]port trunk pvid vlan 101      //101 为管
   理 VLAN
8.
9. [AC6005-GigabitEthernet0/0/1]port trunk allow-pass vlan all
10.
11.[AC6005-GigabitEthernet0/0/1]quit
12.
13.[AC6005]int g0/0/2
14.
15.[AC6005-GigabitEthernet0/0/2]port link-type trunk
16.
17.[AC6005-GigabitEthernet0/0/2]port trunk allow-pass vlan all
18.
19.[AC6005-GigabitEthernet0/0/2]quit
20.
21.[AC6005]ip pool huawei      //创建 DHCP 地址池
22.
23.[AC6005-ip-pool-huawei]network 192.168.100.0 mask 24
24.
25.[AC6005-ip-pool-huawei]gateway-list 192.168.100.254
26.
27.[AC6005-ip-pool-huawei]dns-list 8.8.8.8
28.
29.[AC6005-ip-pool-huawei]quit
30.
31.[AC6005]dhcp enable      //启动 DHCP 服务
32.
33.[AC6005]int vlanif 100
34.
35.[AC6005-Vlanif100]ip add 192.168.100.1 24    //配置 VLAN 的虚拟接口地址
36.
37.[AC6005-Vlanif100]dhcp select global      //选择全局地址池给 DHCP 客
   户端使用
38.
39.[AC6005-Vlanif100]quit
40.
41.[AC6005]int vlanif 101      //管理 VLAN 接口
42.
43.[AC6005-Vlanif101]ip add 192.168.101.1 24
44.
```

```
45. [AC6005-Vlanif101]dhcp select interface //开启接口地址池的DHCP 服
    务器功能
46.
47. [AC6005-Vlanif101]quit
48.
49. [AC6005]capwap source int vlan101 //CAPWAP 隧道绑定端口
50.
51. [AC6005]wlan
52.
53. [AC6005-wlan-view]ap-group name ap //创建AP 组，以便将相同配置的
    AP 加入同一AP 组
54.
55. [AC6005-wlan-ap-group-ap]quit
56.
57. [AC6005-wlan-view]regulatory-domain-profile name domain //创建名为
    domain 的域管理模板
58.
59. [AC6005-wlan-regulate-domain-domain]country-code CN //城市代码
60.
61. [AC6005-wlan-regulate-domain-domain]quit
62.
63. [AC6005-wlan-view]ap-group name ap //进入新
    创建的AP 组
64.
65. [AC6005-wlan-ap-group-ap]regulatory-domain-profile name domain //调
    用刚才创建的模板
66.
67. [AC6005-wlan-regulate-domain-domain]quit
68.
69. //绑定AP 到AC 的AP 组中
70.
71. [AC6005-wlan-view]ap auth-mode mac-auth //AP 上线的方式
    是MAC 认证
72.
73. [AC6005-wlan-view]ap-id 0 ap-mac 00E0-FC4C-1860 //AP 的MAC 地址
    4 位为一组
74.
75. [AC6005-wlan-ap-0]ap-name area_1 //这个AP 的区域
    命名为area_1
76.
77. [AC6005-wlan-ap-0]ap-group ap // 将此AP 加入组
    ap
78.
```

```
79.Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]:y
80.
81.[AC6005-wlan-ap-0]quit
82.
83.display ap all
84.
85.[AC6005-wlan-view]security-profile name sec //调用安全模板
86.
87.[AC6005-wlan-sec-prof-sec]security wpa2 psk passphrase huawei@123 aes //认证方式和密码
88.
89.[AC6005-wlan-sec-prof-sec]quit
90.
91.
92.
93.[AC6005-wlan-view]ssid-profile name ssid //WLAN
   的名字
94.
95.[AC6005-wlan-ssid-prof-ssid]ssid huawei //配置
   SSID 名称为 huawei
96.
97.[AC6005-wlan-ssid-prof-ssid]quit
98.
99.
100.
101. [AC6005-wlan-view]vap-profile name vap //创建
    VAP 模板
102.
103. [AC6005-wlan-vap-prof-vap]forward-mode tunnel //配置
    隧道方式
104.
105. [AC6005-wlan-vap-prof-vap]service-vlan vlan-id 100 //
    业务 VLAN
106.
107. [AC6005-wlan-vap-prof-vap]security-profile sec
108.
109.
110.
111. [AC6005-wlan-vap-prof-vap]ssid-profile ssid //
    调用 SSID 模板
112.
```

```

113. [AC6005-wlan-vap-prof-vap]quit
114.
115. [AC6005-wlan-view]ap-group name ap //配置
    AP 组引用 VAP 模板
116.
117. [AC6005-wlan-ap-group-ap]vap-
    profile vap wlan 1 radio 0 //AP 射频0 使用 VAP WLAN 模板,0 为
    2.4GHz 射频, 1 为 5GHz 射频
118.
119. [AC6005-wlan-ap-group-ap]return
120.
121. display vap ssid huawei

```

```

<AC6005>display vap ssid huawei
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-----
AP ID AP name RfID WID BSSID Status Auth type STA SSID
-----
0 area_1 0 1 00E0-FC97-2B90 ON WPA2-PSK 0 huawei
-----
Total: 1

```

测试 SAT:



```

STA>ipconfig

Link local IPv6 address.....: ::
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.100.29
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.100.254
Physical address.....: 54-89-98-E2-4C-5E
DNS server.....: 8.8.8.8

```

连接成功!

## 九、设计心得

### 1. 网络分段和 VLAN 划分

VLAN 划分：通过 VLAN 将不同的部门和区域（如南校区、北校区和科技楼）分隔开来，有效地减少了广播域，提升了网络性能和安全性。

IP 地址规划：每个 VLAN 都有独立的 IP 地址段，便于管理和故障排查。例如，南校区使用 10.94.1.x 至 10.94.3.x，北校区使用 10.94.4.x 至 10.94.6.x。

### 2. 路由设计

静态路由与动态路由结合：使用静态路由来确保关键网络的确定性路由，同时使用 RIP 动态路由协议来简化路由表的维护和更新。

默认路由配置：在关键路由器上配置默认路由，确保未知流量能够正确转发至外部网络或其他子网。

### 3. NAT（网络地址转换）配置

专用地址转换：通过 NAT，将内部私有地址转换为公共地址，从而实现网络隔离和安全，同时节省公共 IP 地址的使用。比如，科技楼的地址转换为 150.1.4.100 到 150.1.4.200。

ACL 配合 NAT：利用 ACL 定义允许进行 NAT 转换的流量范围，增加了网络安全性。

### 4. 安全性设计

访问控制列表（ACL）：通过配置 ACL，控制流量进出不同的网络区域，防止未经授权的访问。

隔离关键网络：通过不同的 VLAN 和 ACL 配置，将关键网络（如管理网络、科研网络等）与普通用户网络隔离开来，防止内部威胁。

## 5. 网络拓扑

层次化设计：采用层次化的网络设计，包括核心层、汇聚层和接入层，简化了网络管理，提高了扩展性。

明确的拓扑结构：清晰的网络拓扑图有助于理解网络结构和配置，便于后续的维护和扩展。

这次项目实践让我收获良多，不仅锻炼了我对于专业知识的实践能力，熟悉基本软件的使用和调试，也让我对于计算机网络的知识更加明晰。

## 十、遇到的困难

1.eNSP 软件经常遇到启动问题和保存总是卡在 0%的情况导致需要从头开始配置，升级软件有所改善。

2.配置 NAT，动态路由时对于网段了解不熟悉导致多次配置完之后办公楼 ping 不同外网的 PC，但 10.94.4.2 可以，调整网段后有效解决。