

计算机网络与安全实践

实验指导手册

基于 GNS3 的组网实验

华中科技大学网络空间安全学院

二零二四年十月

目 录

第一章 实验目标和内容	1
1.1 实验目的	1
1.2 实验环境	1
1.3 实验要求	2
1.4 实验内容（基本部分）	3
1.5 实验内容（综合部分）	4
第二章 GNS3 软件包概览	6
2.1 总述	6
2.2 拓扑图设计	6
2.3 设备的配置与测试	7
2.3 网络拓扑的打开与保存	13
第三章 锐捷路由器部分命令列表	14
3.1 常用命令	14
3.2 配置 IP 地址	15
3.3 广域网协议设置	15
第四章 示例	16
4.1 交换机配置	16
4.2 路由器配置	18
4.3 简单的排错	20

第一章 实验目标和内容

1.1 实验目的

- ◇ 了解 IP 协议、网络层协议和数据链路层协议的工作原理及机制
- ◇ 掌握 IP 地址的规划方法
- ◇ 掌握路由协议的配置方法
- ◇ 掌握路由器及二/三层交换机的配置方法
- ◇ 了解 VLAN 的划分原理
- ◇ 掌握访问控制的配置方法

1.2 实验环境

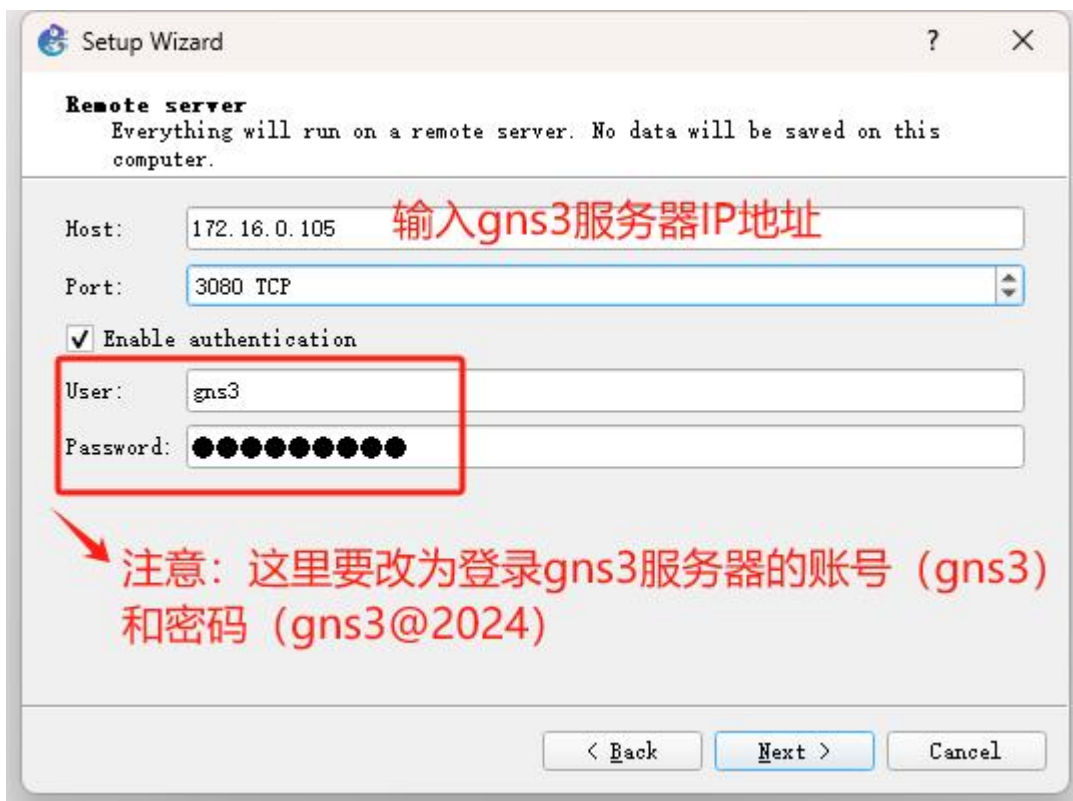
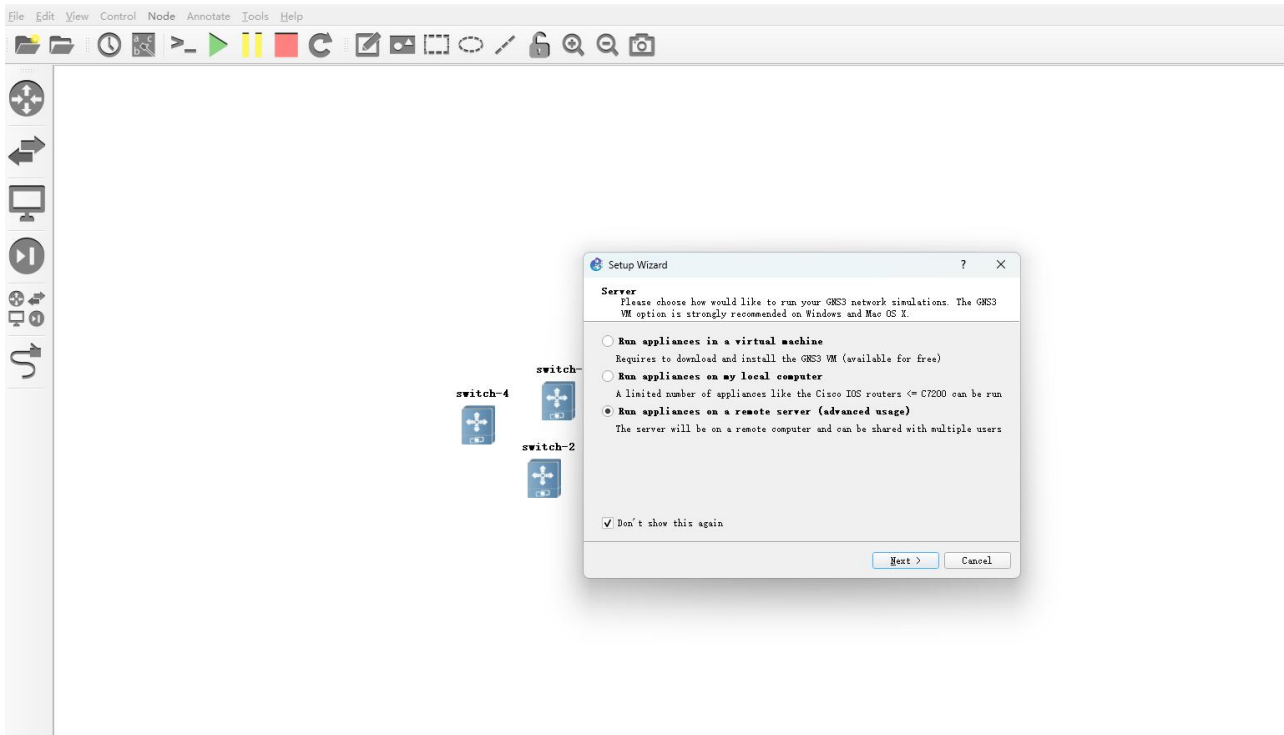
实验使用 GNS3 客户端（v2.2.49 版本）、以及 VMCourse 分级通关综合实践平台（已部署 GNS3 服务器），也可以将 GNS3 服务器部署在本地 VMware 上（提供 gns3server 镜像文件），实验需要使用的锐捷路由器、交换机等设备均已部署在 GNS3 服务器上。

在分级通关综合实践平台进入该课程实验环境，申请实例并连接进入虚拟机。通过 ip add 命令查看 GNS3 服务器 IP 地址（GNS3 服务器账号：gns3，密码：gns3@2024），客户端需要输入 GNS3 服务器的 IP 地址进行连接。输入“sudo gns3server”命令启动 GNS3 服务器，等待客户端连接。

```
ubuntu@gns3-server:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether fa:ef:94:58:d8:00 brd ff:ff:ff:ff:ff:ff
    inet 172.17.8.27/16 brd 172.17.255.255 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fd2d:541c:8d51:0:f8ef:94ff:fe58:d800/64 scope global mngtnpaddr noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::f8ef:94ff:fe58:d800/64 scope link
        valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:b0:28:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:b0:28:ae brd ff:ff:ff:ff:ff:ff
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:99:0b:0f:a5 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

如果输入 ip add 后，发现没有获取到 ip 地址，此时输入“sudo dhclient”，再重新查看地址即可；如果输入 ip add 后，发现已有和其他同学重复的 ip 地址，删除掉这个重复的 ip 地址（ip addr del ip dev 网卡接口），再使用命令“sudo dhclient”获取新的 ip 地址即可。

接着在 GNS3 客户端点击工具栏中的“Help->Setup Wizard”，选择“Run appliances on a remote server(advanced usage)”，输入刚查看的 GNS3 Server 的 IP 地址，端口选择“3080 TCP”，输入 GNS3 服务器账号：gns3，GNS3 服务器密码：gns3@2024，点击下一步即可连接 GNS3 服务器（注意：应把服务器启动之后客户端再连接）。



1.3 实验要求

- ✧ 熟悉 GNS3 仿真软件。
- ✧ 利用 GNS3 仿真软件完成实验内容。
- ✧ 提交实验设计报告纸质档和电子档。
- ✧ 基于自己的实验设计报告，通过实验课的上机实验，演示给实验指导教师检查。

1.4 实验内容（基本部分）

本部分实验为基础部分的实验，分为两项内容，每项实验内容在最终的评价中占比 30%，本部分实验将使用两张拓扑结构图配合完成实验，如图 1.1 和 1.2 所示。

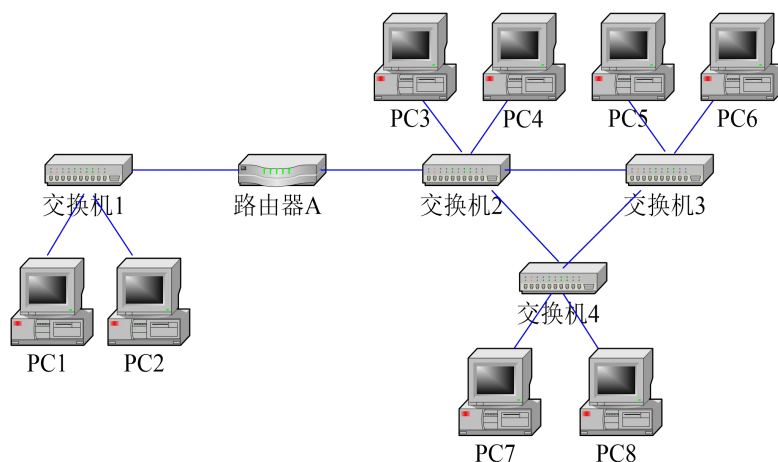


图 1.1

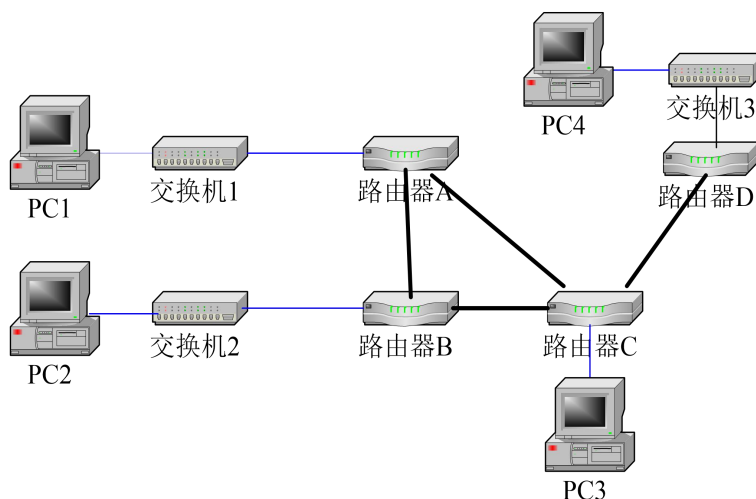


图 1.2

第一项实验——IP 地址规划与 Vlan 分配实验：

✧ 使用仿真软件描述网络拓扑图 1.1。

✧ 基本内容 1

- 将 PC1、PC2 设置在同一个网段，子网地址是：192.168.0.0/24；
- 将 PC3~PC8 设置在同一个网段，子网地址是：192.168.1.0/24；
- 配置路由器，使得两个子网的各 PC 机之间可以自由通信。

✧ 基本内容 2

- 将 PC1、PC2 设置在同一个网段，子网地址是：192.168.0.0/24；
- 将 PC3、PC5、PC7 设置在同一个网段，子网地址是：192.168.1.0/24；
- 将 PC4、PC6、PC8 设置在同一个网段，子网地址是：192.168.2.0/24；
- 配置交换机 1、2、3、4，使得 PC1、PC2 属于 Vlan2，PC3、PC5、PC7 属于 Vlan3，PC4、PC6、PC8 属于 Vlan4；
- 测试各 PC 之间的连通性，并结合所学理论知识进行分析；

- 配置路由器，使得拓扑图上的各 PC 机之间可以自由通信，结合所学理论对你的路由器配置过程进行详细说明。

第二项实验——路由器配置实验

- ✧ 使用仿真软件描述网络拓扑图 1.2
- ✧ 基本内容 1
 - 将 PC1 设置在 192.168.1.0/24 网段；
 - 将 PC2 设置在 192.168.2.0/24 网段；
 - 将 PC3 设置在 192.168.3.0/24 网段；
 - 将 PC4 设置在 192.168.4.0/24 网段
 - 设置路由器端口的 IP 地址
 - 在路由器上配置 OSPF 协议，使各 PC 机能互相访问
- ✧ 基本内容 2（选做）
 - 在基本内容 1 或者 2 的基础上，对路由器 1 进行访问控制配置，使得 PC1 无法访问其它 PC，也不能被其它 PC 机访问。
 - 在基本内容 1 或者 2 的基础上，对路由器 1 进行访问控制配置，使得 PC1 不能访问 PC2，但能访问其它 PC 机

1.5 实验内容（综合部分）

本部分实验为综合部分的实验，在最终的评价中占比 40%。

实验背景：

某企业有公司总部，另有两个分公司，两个分公司共用前缀为 192.168.1.0/24 的地址块，准备将该企业连入网络。分公司 1 有 100 名员工；分公司 2 有 120 名员工；财务部门有 20 名工作人员，单独使用前缀为 192.168.2.0/24 地址块中的地址。两个分公司通过汇聚交换机接入总部核心交换机，总部财务部门通过接入交换机接入总部。公司另有 FTP 服务器、DNS 服务器、HTTP 服务器直接接入核心交换机，服务器网段使用前缀为 192.168.3.0/24 地址块中的地址。核心交换机通过路由器接入互联网，路由器的接口地址可以使用 172.0.12.0/24 地址块中的地址，此网段有 100 台主机连接到路由器。

表 1 该公司各种子网的主机数

子网分类	主机数	VLAN ID
分公司 1	100	2
分公司 2	120	3
财务部门	20	4
服务器	20	5

实验任务要求：

（1）基本任务

- ✧ 根据背景描述，设计该公司的网络拓扑结构图，每种类型的交换机只需要画出一台，每个子网只需要画出

一台主机（不需要考虑设备冗余备份问题）。

- ✧ 对全网的 IP 地址进行合理的分配，并在 GNS3 绘制的网络拓扑结构图上对各类设备进行配置（配置 VLAN、路由、IP 地址等），并测试是否满足组网需求，如有无法满足之处，请结合理论给出解释和说明。

（2）进阶任务（完成即可加分）

- ✧ 财务部门只能访问服务器，不能访问其他网段。
- ✧ 两个分公司不能访问财务部门，其余都可以访问。
- ✧ 在分公司 1 和分公司 2 的客户端上分别配置 FTP 客户端（使用 Kali 系统终端）和 HTTP 客户端，并对 FTP 服务器、HTTP 服务器和 DNS 服务器进行相关配置。FTP 客户端能访问 FTP 服务器，能够实现上传、下载文件功能。HTTP 客户端能通过域名访问 HTTP 服务器，并能正常访问网页。

第二章 GNS3 软件包概览

2.1 总述

GNS3 是一款具有图形化界面可以运行在多平台的网络虚拟软件，用于模拟、配置、测试虚拟和真实网络并对其进行故障排除。用户可以在软件的图形用户界面上直接使用拖曳方法建立网络拓扑，并可提供数据包在网络中行进の詳細处理过程，观察网络实时运行情况。可以学习 IOS 的配置、锻炼故障排查能力。

本章内容基于 2.2.49 版本的 GNS3 进行介绍。

2.2 拓扑图设计

2.2.1 设备的选择

GNS3 软件的主界面如图 2.1 所示。



图 2.1 GNS3 的主界面

在界面的左侧区域，为设备工具栏，这里有许多种类的硬件设备，从上到下分别为路由器、交换机、终端设备、安全设备、所有设备、以及连线。点击设备直接拖动到工作区即可使用。

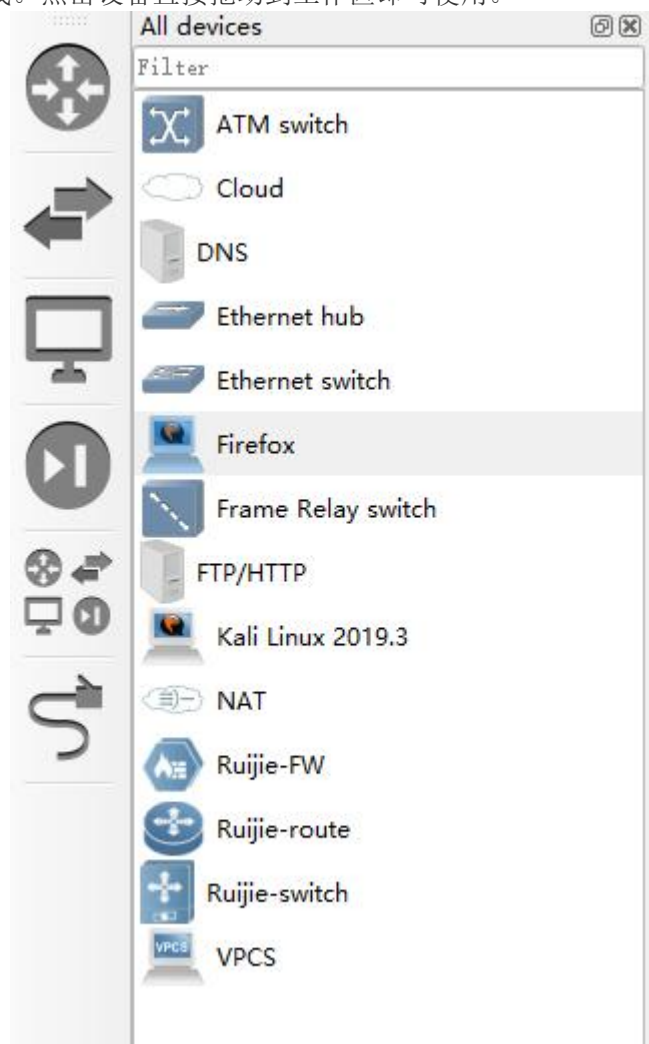


图 2.2 GNS3 的设备列表

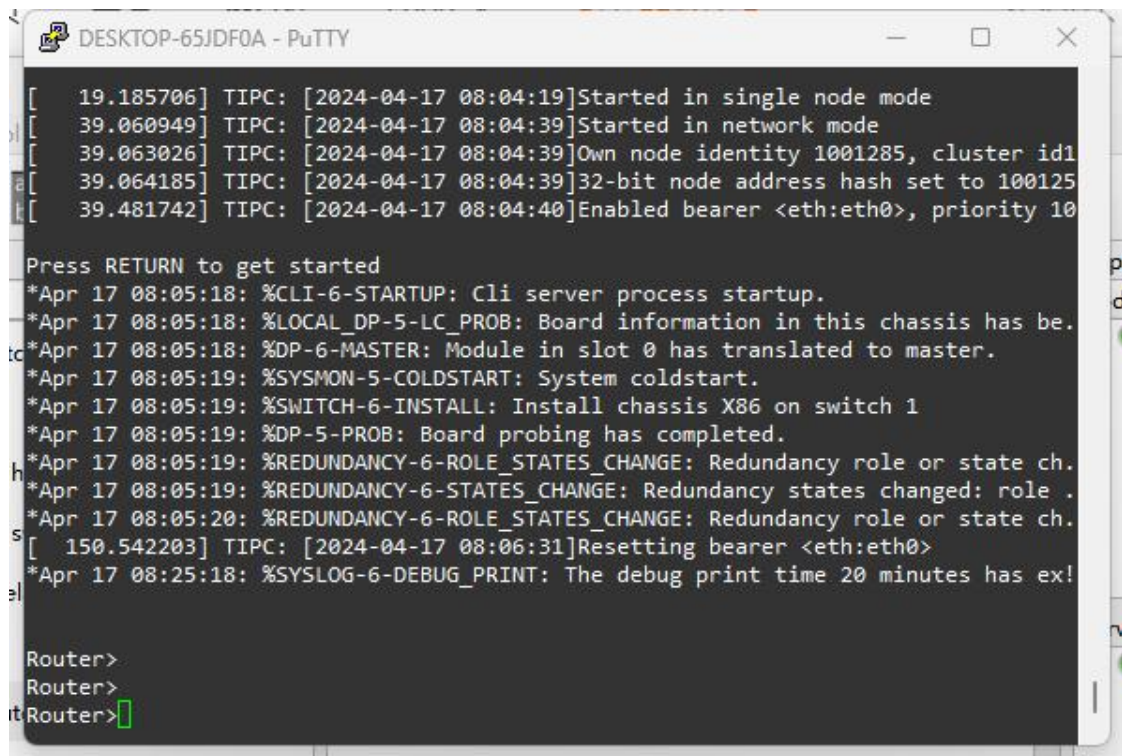
设备列表中列出了网络拓扑结构设计软件中可以使用的网络设备列表，并可供绘制拓扑结构图时使用。GNS3 服务器上导入了锐捷交换机、路由器、防火墙镜像，因此，在绘制网络拓扑结构图中，优先使用锐捷路由器和锐捷交换机来完成实验。为了实现清晰的配置过程和配置效果，有两个原则需要注意：（1）以够用为度，即：尽量选择一个简单的、接口数较少的路由器；（2）面向实际，即：尽可能的按照实际网络的情况进行设备选择。

另外，在 GNS3 服务器上已事先导入制作好的 FTP/HTTP 服务器和 DNS 服务器。FTP/HTTP 服务器既可以提供 FTP 服务，也可以提供 Nginx 服务。同时还导入了 Firefox 客户端和 Kali 客户端，请注意，Firefox 客户端只能实现下载功能，无法上传文件，在选用 FTP 客户端时，尽量选择 Kali 系统客户端。

2.3 设备的配置与测试

2.3.1 路由器/交换机添加网络配置

设备连接好以后，需要为设备添加网络配置。对于路由器、交换机设备，采用命令行来配置。将设备拖拽到工作区后，右击双击设备，点击“start”启动设备，随后回车进入命令行配置界面。



```
DESKTOP-65JDF0A - PuTTY

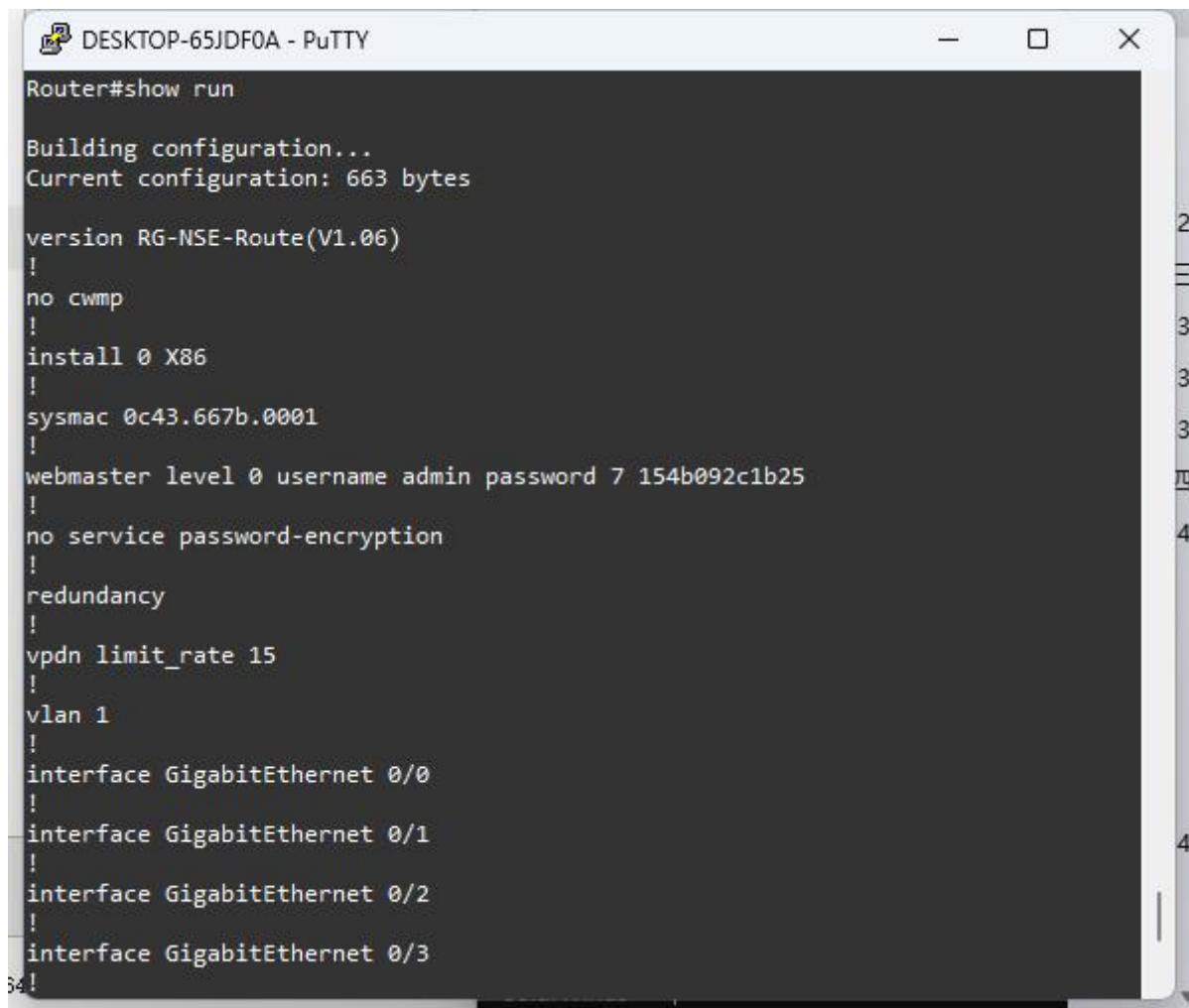
[ 19.185706] TIPC: [2024-04-17 08:04:19]Started in single node mode
[ 39.060949] TIPC: [2024-04-17 08:04:39]Started in network mode
[ 39.063026] TIPC: [2024-04-17 08:04:39]Own node identity 1001285, cluster id1
[ 39.064185] TIPC: [2024-04-17 08:04:39]32-bit node address hash set to 100125
[ 39.481742] TIPC: [2024-04-17 08:04:40]Enabled bearer <eth:eth0>, priority 10

Press RETURN to get started
*Apr 17 08:05:18: %CLI-6-STARTUP: Cli server process startup.
*Apr 17 08:05:18: %LOCAL_DP-5-LC_PROB: Board information in this chassis has be.
*Apr 17 08:05:18: %DP-6-MASTER: Module in slot 0 has translated to master.
*Apr 17 08:05:19: %SYSMON-5-COLDSTART: System coldstart.
*Apr 17 08:05:19: %SWITCH-6-INSTALL: Install chassis X86 on switch 1
*Apr 17 08:05:19: %DP-5-PROB: Board probing has completed.
*Apr 17 08:05:19: %REDUNDANCY-6-ROLE_STATES_CHANGE: Redundancy role or state ch.
*Apr 17 08:05:19: %REDUNDANCY-6-STATES_CHANGE: Redundancy states changed: role .
*Apr 17 08:05:20: %REDUNDANCY-6-ROLE_STATES_CHANGE: Redundancy role or state ch.
[ 150.542203] TIPC: [2024-04-17 08:06:31]Resetting bearer <eth:eth0>
*Apr 17 08:25:18: %SYSLOG-6-DEBUG_PRINT: The debug print time 20 minutes has ex!

Router>
Router>
Router>
```

图 2.3 路由器命令行配置界面

图 2.3 为路由器命令行配置界面。通过 show run 命令显示路由器配置信息，如图 2.4 所示。锐捷路由器的部分命令使用方法具体见第三章。



```
DESKTOP-65JDF0A - PuTTY

Router#show run

Building configuration...
Current configuration: 663 bytes

version RG-NSE-Route(V1.06)
!
no cwm
!
install 0 X86
!
sysmac 0c43.667b.0001
!
webmaster level 0 username admin password 7 154b092c1b25
!
no service password-encryption
!
redundancy
!
vpdn limit_rate 15
!
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
```

图 2.4 命令行显示路由器配置信息

2.3.2 终端添加网络配置

Firefox 客户端设备启动后，双击进入图形化界面对终端设备配置 IP 地址和网关，点击“Apply”即可。如图 2.5 所示。

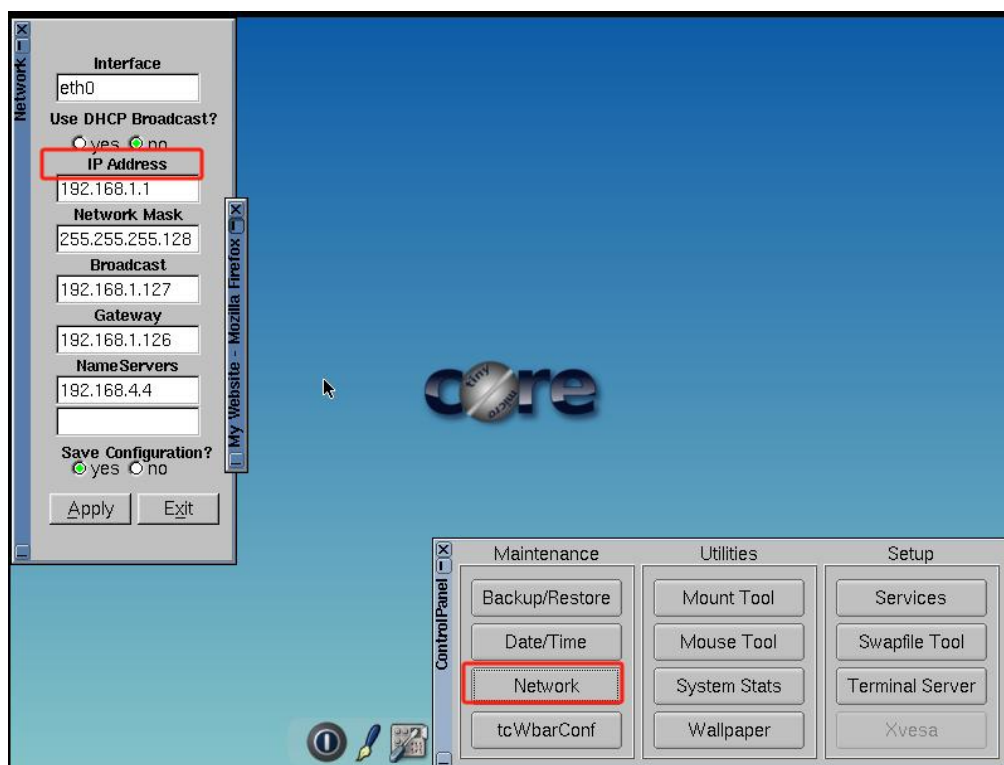
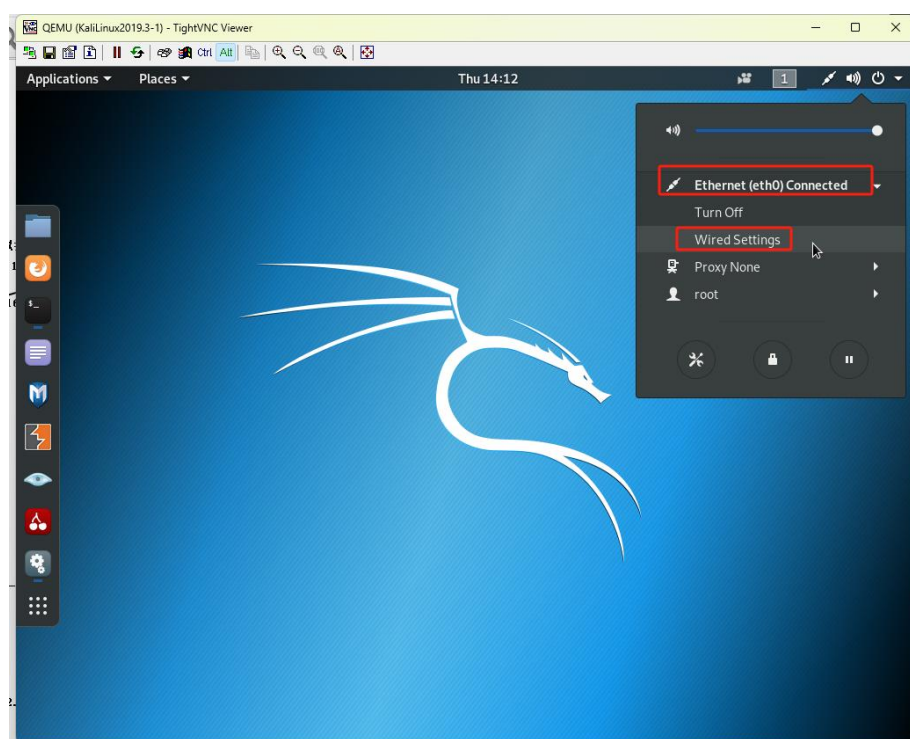


图 2.5 Firefox 终端图形化界面配置 IP 地址和网关

Kali 系统终端启动进入界面后，点击进入网络设置，配置好 IP 地址和网关等之后，点击“Apply”并重启网卡即可。



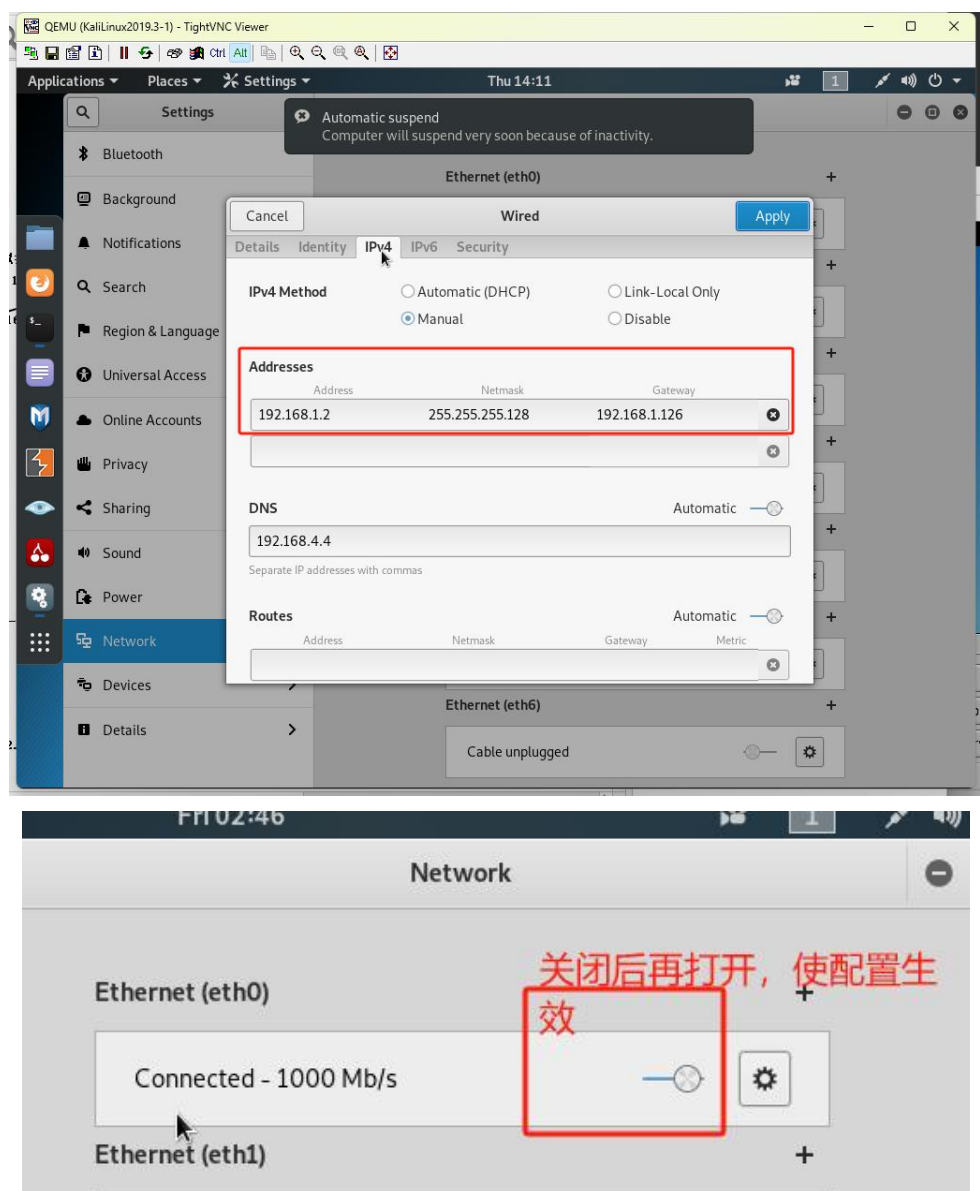


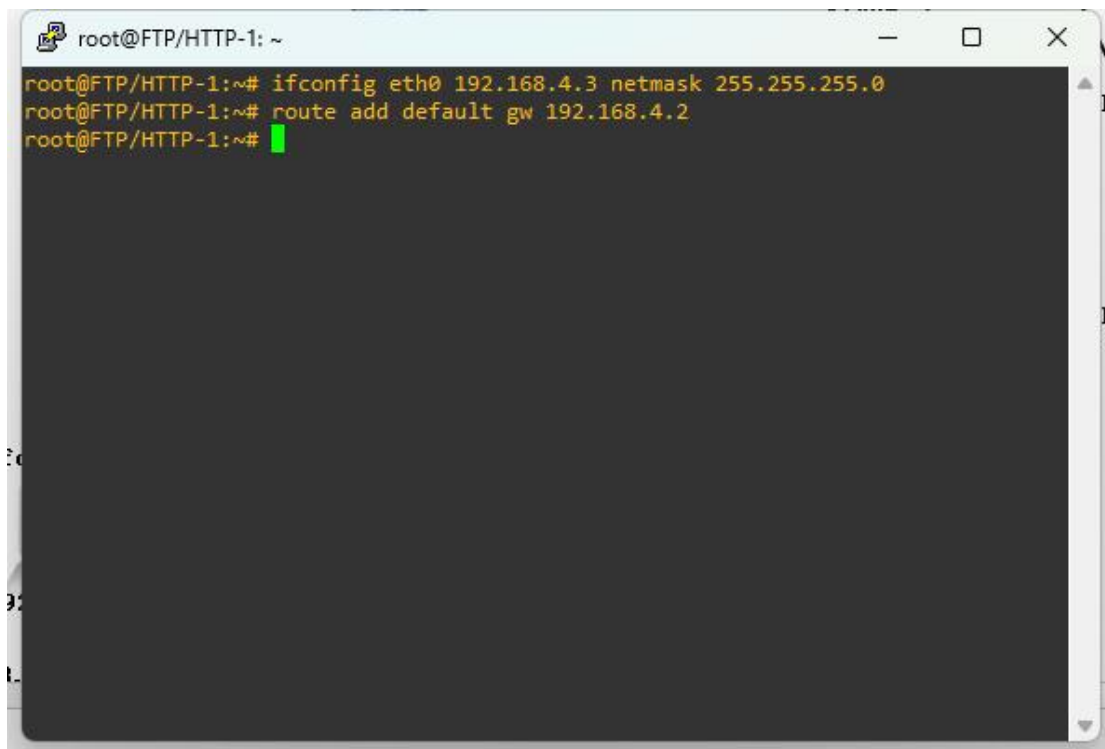
图 2.6 Kali 系统终端网络配置

在 kali 客户端和 firefox 客户端可以利用 ping 命令测试连通性，tracert 命令来测试网络的路由转发路径。

2.3.3 服务器端添加网络配置

(1) 服务器端网络配置

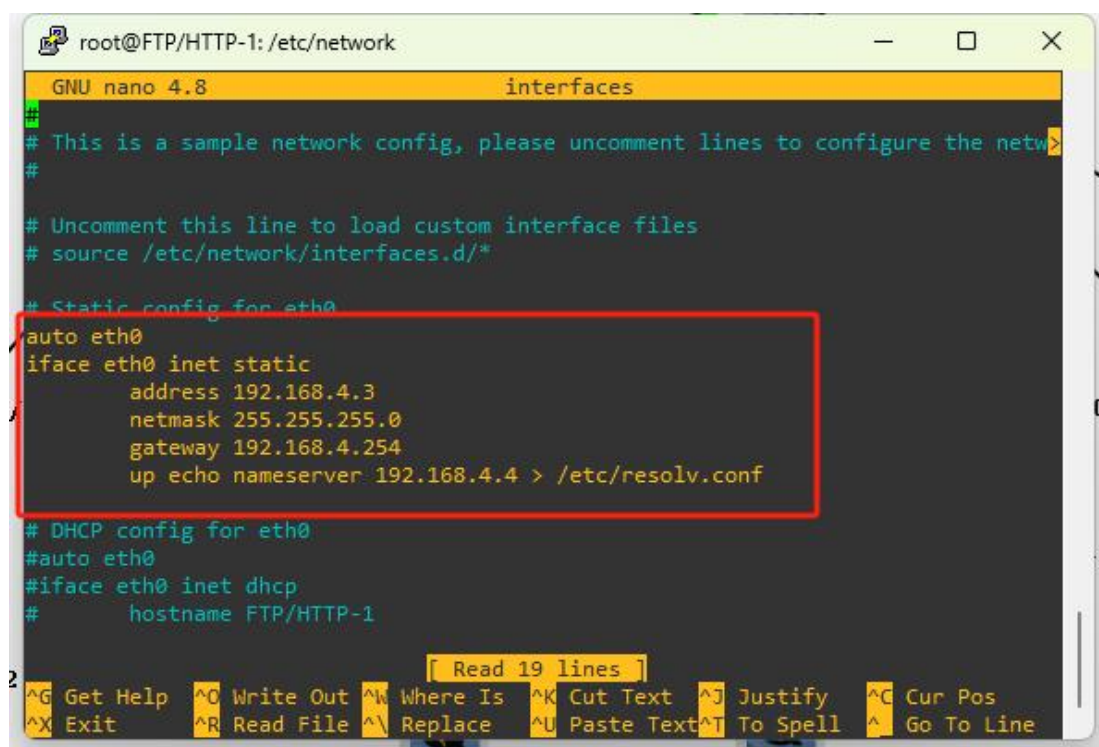
双击服务器打开命令行界面，使用 ifconfig 命令配置服务器 ip 地址，使用 “route add default gw” 命令配置网关。这种使用命令行进行网络配置的方式在设备关机后配置会失效，因此更推荐通过修改配置文件的方式对服务器网络进行配置。

A terminal window titled 'root@FTP/HTTP-1: ~' showing three commands being executed: 'ifconfig eth0 192.168.4.3 netmask 255.255.255.0', 'route add default gw 192.168.4.2', and a prompt 'root@FTP/HTTP-1:~#'.

```
root@FTP/HTTP-1: ~
root@FTP/HTTP-1:~# ifconfig eth0 192.168.4.3 netmask 255.255.255.0
root@FTP/HTTP-1:~# route add default gw 192.168.4.2
root@FTP/HTTP-1:~#
```

图 2.7 使用命令行对服务器进行 IP 地址配置（不推荐）

使用 nano 打开/etc/network 目录下的 interfaces 文件后，编辑修改服务器的 IP 地址等信息，完成修改后保存文件退出，网络配置即可生效。

A terminal window titled 'root@FTP/HTTP-1: /etc/network' showing the nano 4.8 editor editing the 'interfaces' file. The file content includes comments and configuration for eth0. A red box highlights the static configuration for eth0. The bottom of the window shows nano editor shortcuts.

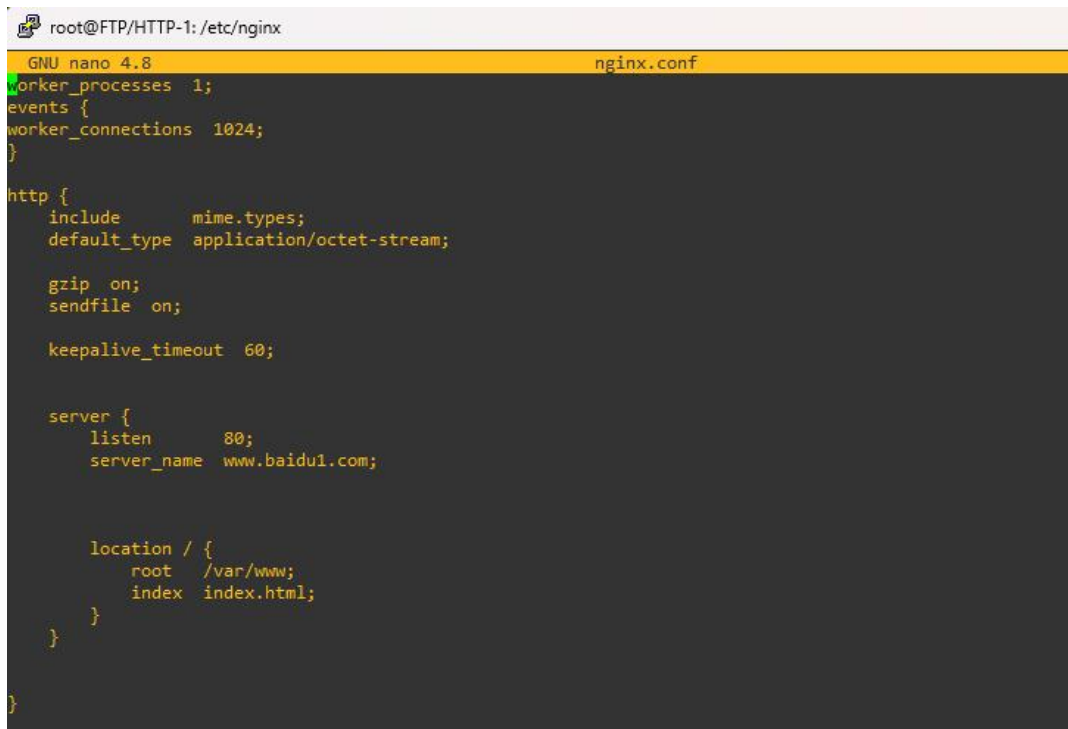
```
root@FTP/HTTP-1: /etc/network
GNU nano 4.8 interfaces
# This is a sample network config, please uncomment lines to configure the network
#
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*
# Static config for eth0
auto eth0
iface eth0 inet static
    address 192.168.4.3
    netmask 255.255.255.0
    gateway 192.168.4.254
    up echo nameserver 192.168.4.4 > /etc/resolv.conf
# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
#    hostname FTP/HTTP-1

[ Read 19 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

图 2.8 修改配置文件进行网络配置（推荐）

(2) HTTP 服务器配置

HTTP 服务器使用的是 Nginx 镜像，使用 nano 命令打开/etc/nginx 目录下的 nginx.conf 进行服务器配置。修改 server 地址块的监听端口以及监听地址，和对应的网页文件，为客户端提供 HTTP 服务。



```
root@FTP/HTTP-1: /etc/nginx
GNU nano 4.8 nginx.conf
worker_processes 1;
events {
    worker_connections 1024;
}

http {
    include mime.types;
    default_type application/octet-stream;

    gzip on;
    sendfile on;

    keepalive_timeout 60;

    server {
        listen 80;
        server_name www.baidu1.com;

        location / {
            root /var/www;
            index index.html;
        }
    }
}
```

图 2.9 nginx 配置文件

(3) DNS 服务器配置

打开 /etc 目录下的 hosts 文件，在文件后面添加对应关系（ip 地址和域名），重启 DNS 服务器生效（只能对本网段提供服务）。如果要从 DNS 服务器所在的子网以外的子网为 DNS 请求提供服务，需要进行以下配置：

1. nano 编辑/etc/init.d/dnsmasq;
2. 找到 DNSMASQ_OPTS="\$DNsmasq_OPTS --local-service" 行；
3. 注释该行并在另一行中添加 DNSMASQ_OPTS="";
4. 使用 “service dnsmasq restart” 命令重新启动 dnsmasq 服务；

这样就可以对所有网段的客户端提供 DNS 服务。

(4) FTP 服务器配置及使用

FTP 服务器无需配置，双击进入命令行即可使用。以下列举了一些常用的 FTP 命令。

1.连接到 FTP 服务器

通过使用 FTP 服务器的 IP 或仅通过服务器的名称来启动连接。

```
ftp [ IP of FTP Server ]
```

2.列出服务器上的文件

```
ftp> ls
```

显示远程 FTP 服务器当前目录下的所有可用文件和目录。

3.切换 FTP 服务器目录

cd 命令允许用户在 FTP 服务器内的目录之间切换。

```
ftp> cd /etc
```

cdup 命令向上移动目录级别，类似于命令“cd ..”。

```
ftp> cdup
```

4.从 FTP 服务器下载文件

```
ftp> get test.zip
```

上面的命令从远程 FTP 服务器的当前目录复制 `test.zip` 文件。该文件将存储在本地当前工作目录中。

5. 上传文件到 FTP 服务器

```
ftp> put TEST.zip
```

此命令会将 `TEST.zip` 文件从本当前工作目录复制到远程服务器的当前目录。

2.3 网络拓扑的打开与保存

文件菜单组包含了如下菜单项：

- 新建：绘制一个新的网络拓扑结构图
- 打开：打开一个磁盘上已存在的网络拓扑结构图工程文件。
- 保存/另存为/：将当前正在绘制的网络拓扑结构图工程文件存储到磁盘上。
- 退出：退出网络拓扑结构图设计软件。

第三章 锐捷路由器部分命令列表

3.1 常用命令

1. 改变命令状态

任务	命令
进入特权命令状态	enable
退出特权命令状态	disable
进入全局设置状态	config terminal
退出全局设置状态	end
进入端口设置状态	interface <i>type slot/number</i>
进入子端口设置状态	interface <i>type number.subinterface</i> [point-to-point multipoint]
进入路由设置状态	router <i>protocol</i>
退出局部设置状态	exit

3. 显示命令

任务	命令
查看版本及引导信息	show version
查看运行设置	show running-config
显示端口信息	show interface <i>type slot/number</i>
显示路由信息	show ip route

4. 网络命令

任务	命令
登录远程主机	telnet <i>hostname IP address</i>
网络侦测	ping <i>hostname IP address</i>
路由跟踪	trace <i>hostname IP address</i>

5. 基本设置命令

任务	命令
全局设置	config terminal
设置访问用户及密码	username <i>username</i> password <i>password</i>
设置特权密码	enable secret <i>password</i>
设置路由器名	hostname <i>name</i>
启动 IP 路由	ip routing
端口设置	interface <i>type slot/number</i>
设置 IP 地址	ip address <i>address subnet-mask</i>
激活端口	no shutdown

3.2 配置 IP 地址

任务	命令
接口设置	interface type slot/number
为接口设置 IP 地址	ip address ip-address mask

3.3 广域网协议设置

1. HDLC 配置命令

任务	命令
设置 HDLC 封装	encapsulation hdlc
指定 HDLC 协议的 keepalive 时间 间隔和最大超时次数	keepalive seconds/retries

2. OSPF 协议

任务	命令
指定使用 OSPF 协议	router ospf <i>process-id</i> ¹
指定与该路由器相连的网络	network <i>address wildcard-mask</i> area <i>area-id</i> ²
指定与该路由器相邻的节点地址	neighbor <i>ip-address</i>

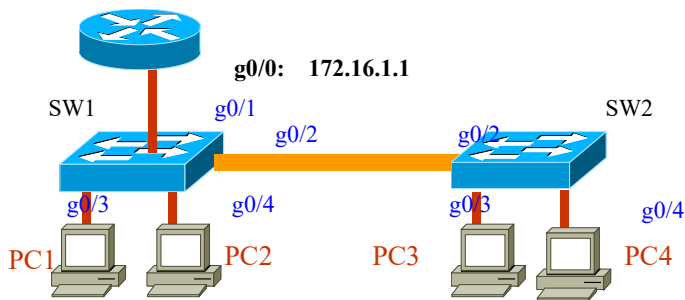
3. 访问控制

任务	命令
设置访问表项目	access-list <i>list</i> {permit deny} <i>address</i> <i>mask</i>
设置队列表中队列的大小	queue-list <i>list-number</i> queue <i>queue-number</i> byte-count <i>byte-count-number</i>
使用指定的访问表	ip access-group <i>list</i> {in out}

第四章 示例

4.1 交换机配置

4.1.1 网络拓扑图



4.1.2 设备选型和 IP 地址规划

设备名	设备型号	接口	IP 地址	掩码
router1	RG-RSR50-X	g0/0	172.16.1.1	255.255.255.0
switch1	RG-S7800C-X			
switch2	RG-S7800C-X			
PC1			172.16.2.21	255.255.255.0
PC2			172.16.3.22	255.255.255.0
PC3			172.16.2.23	255.255.255.0
PC4			172.16.3.24	255.255.255.0

4.1.3 实验目标

- PC1 与 PC3 能互相访问，PC2 与 PC4 能互相访问
- PC1、PC3 与 PC2、PC4 之间不能互相访问

4.1.4 VLAN 划分

鉴于两个交换机为同类型交换机，下述操作在两个交换机上都要进行，手册中仅说明一个交换机上的操作。

1. 在交换机上创建两个 VLAN，分比为 VLAN 2 和 VLAN 3

```
Switch# config terminal //进入配置模式
```

```
Switch(config)# vlan 2 //在交换机上添加 vlan2
```

```
Switch(config-vlan)# exit //退出 vlan2，回到配置模式
```

```
Switch(config)# vlan 3 //在交换机上添加 vlan3
```

Switch(config-vlan)# **exit** //退出 vlan3，回到配置模式

2. 将 3 号端口和 4 号端口分别分配到 VLAN 2 和 VLAN 3 中

Switch# **config terminal** //进入配置模式

Switch(config)# **interface g0/3** //配置 g0/3 端口

Switch(config-if-GigabitEthernet 0/3)# **switchport mode access** //指定该端口为访问链路

Switch(config-if-GigabitEthernet 0/3)# **switchport access vlan 2** //将 3 号端口分配到 VLAN 2

Switch(config-if-GigabitEthernet 0/3)# **exit**

Switch(config)# **interface g0/4** //配置 g0/4 端口

Switch(config-if-GigabitEthernet 0/4)# **switchport mode access** //指定该端口为访问链路

Switch(config-if-GigabitEthernet 0/4)# **switchport access vlan 3** //将 4 号端口分配到 VLAN 3

Switch(config-if-GigabitEthernet 0/4)#**CTRL-C** //CTRL-C 退出端口配置

Switch# **show vlan**

（此时可测试 PC1 和 PC2 能否互相访问，并分析原因）

输入命令 show vlan 查看创建成功的 vlan 信息，包括 vlan id、vlan 名称、状态等信息。

3. 配置两个交换机之间的 trunk 链路（两端都要配置）

Switch(config)# **interface g0/2**

Switch(config-if-GigabitEthernet 0/2)# **switchport mode trunk** //配置为 trunk 模式

Switch(config-if-GigabitEthernet 0/2)# **switchport trunk allowed vlan only 2,3** //配置 trunk 口许可 vlan2,3

Switch(config-if-GigabitEthernet 0/2)#**CTRL-C** //CTRL-C 退出端口配置

4.1.5 VLAN 之间的路由配置

1. 由于路由器仅通过接口 g0/0 与交换机相连，而该接口实际上连接了两个 VLAN，因此为了联通两个 VLAN，需要在两个 vlan 各自创建两个虚拟端口 172.16.2.1 和 172.16.3.1，分别作为 vlan 2 和 vlan 3 内 PC 的网关。

Switch(config)# **ip routing** //即使之前已启用 IP 路由，此步骤也可确保已激活该项。

2. 创建 vlan 2 和 vlan 3:

Switch# **conf t** //注意此处进入 config 模式

Switch(config)# **vlan 2**

Switch(config)# **vlan 3**

Switch(config-vlan)# **exit**

3. 创建 vlan 虚拟端口并保持端口打开

Switch(config)# **interface vlan 2**

Switch(config-if-VLAN 2)# **ip address 172.16.2.1 255.255.255.0**

Switch(config-if-VLAN 2)# **exit**

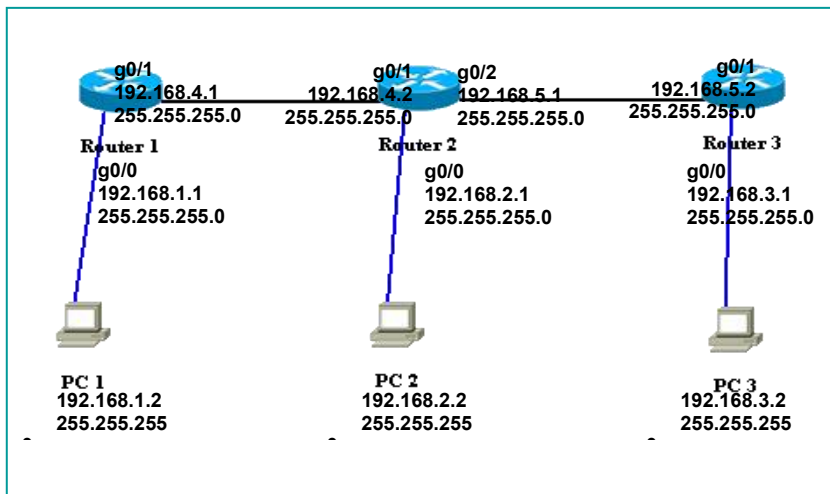
Switch(config)# **interface vlan 3**

Switch(config-if-VLAN 3)# **ip address 172.16.3.1 255.255.255.0**

4. 至此，vlan 2 和 vlan 3 实现互通。

4.2 路由器配置

4.2.1 网络拓扑图



4.2.2 实验目标

- 分别为各路由器配置 OSPF 协议，使得 PC1、PC2、PC3 可以互访。
- 对 Router 1 配置 ACL，使得 PC1 无法访问其它网段

4.2.3 OSPF 协议配置

路由器 Router1 的配置

```
Router>
Router>enable //进入超级用户模式
Router#conf t //进入全局配置模式
Router(config)#interface g0/0 //指定以太网端口 g0/0
Router(config-if-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0 //配置 g0/0 接口地址
Router(config-if) #int g0/1 //配置 g0/1 接口
Router(config-if-GigabitEthernet 0/1)#ip address 192.168.4.1 255.255.255.0
Router(config-if-GigabitEthernet 0/1)#CTRL-C //CTRL-C 退出端口配置
Router#show ip route //查看路由设置
```

路由器 Router2 的配置

```
Router>
Router>enable //进入超级用户模式
Router#conf t //进入全局配置模式
Router(config)#interface g0/0 //指定以太网口 g0/0
Router(config-if-GigabitEthernet 0/0)#ip address 192.168.2.1 255.255.255.0 //配置 g0/0 接口地址
Router(config-if-GigabitEthernet 0/0)#interface g0/1 //指定以太网串口 g0/1
Router(config-if-GigabitEthernet 0/1)#ip address 192.168.4.2 255.255.255.0 //配置 g0/1 接口地址
Router(config-if-GigabitEthernet 0/1) #int g0/2 //配置 g0/2 接口
Router(config-if-GigabitEthernet 0/2)#ip address 192.168.5.1 255.255.255.0
Router(config-if-GigabitEthernet 0/2)#CTRL-C //CTRL-C 退出端口配置
Router#show ip route //查看路由设置
```

路由器 Router3 的配置

```
Router>
```

```

Router>enable //进入超级用户模式
Router#conf t //进入全局配置模式
Router(config)#interface g0/0 //指定以太网口 g0/0
Router(config-if-GigabitEthernet 0/0)#ip address 192.168.3.1 255.255.255.0 //配置 g0/0 接口地址
Router(config-if-GigabitEthernet 0/0) #int g0/1 //配置 g0/1 接口
Router(config-if-GigabitEthernet 0/1)#ip address 192.168.5.2 255.255.255.0
Router(config-if-GigabitEthernet 0/1)#CTRL-C //CTRL-C 退出端口配置
Router#show ip route //查看路由设置

```

在路由器 Router1 上配置 OSPF 协议

```

Router#conf t //进入全局配置模式
Router(config)#router ospf 1 //选择 ospf 协议
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
//0.0.0.255 是翻转掩码，0 和 1 设置刚好和子网掩码相反
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#end
Router#write

```

在路由器 Router2 上配置 OSPF 协议

```

Router#conf t //进入全局配置模式
Router(config)#router ospf 50 //选择 ospf 协议，进程号为 50
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#end
Router#write

```

在路由器 Router3 上配置 OSPF 协议

```

Router#conf t //进入全局配置模式
Router(config)#router ospf 51
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#end
Router#write

```

4.2.4 ACL 配置

在路由器 Router1 上建立访问控制列表，使得 PC1 无法访问其它网段

```

Router#conf t
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Router1(config-if)#access-list 10 permit any
Router1(config-if)#interface g0/0
Router1(config-if-GigabitEthernet 0/0)#ip access-group 10 in

```

4.3 简单的排错

4.3.1 使用 Ping 测试连接

Ping 命令有助于验证 IP 级的连通性。进行故障排除时，可以使用 ping 向目标主机名或 IP 地址发送 ICMP 回显请求。需要验证主机能否连接到 TCP/IP 网络和网络资源时，使用 ping 命令。也可以使用 ping 命令将网络硬件问题和不兼容配置隔离开来。

使用格式：ping [-t] [-a] [-n count] [-l size]

参数介绍：

- t 让用户所在的主机不断向目标主机发送数据
- a 以 IP 地址格式来显示目标主机的网络地址
- n count 指定要 ping 多少次，具体次数由后面的 count 来指定
- l size 指定发送到目标主机的数据包的大小

4.3.2 使用 ifconfig 和 route 查看配置

在进行网络问题排除时，先检查出现问题的 VPC 上的 TCP/IP 配置。可以使用 show 命令获得主机配置信息，包括 IP 地址、子网掩码和默认网关。

4.3.3 traceroute

主要功能：判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间

参数介绍：

4.1.3 traceroute

执行 traceroute 命令，可以显示用于测试的数据包从源地址到目的地址所经过的所有网关。

traceroute [vrf vrf-name | ip] [ip-address [probe number] [source source] [timeout seconds] [ttl minimum maximum]]

参数说明

参数	描述
vrf-name	VRF 名字
ip-address	指定 IPv4 地址。
number	指定发送的探测的数量
source	指定源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址。
seconds	指定超时时间
minimum maximum	指定最小和最大 TTL 值

4.3.4 检查 IP 和网关的设置

留意 PC 端口的 IP、掩码以及网关是否正确，否则将导致 ping 不通。