

## 第3章

# 模拟器安装和使用

### 本章要点

- ◆ 了解 GNS3 软件安装必备的硬件环境和软件环境。
- ◆ 掌握模拟器 GNS3 上基本网络拓扑构建过程。

## 3.1 GNS3 模拟器简介

GNS3 模拟器是用来验证网络设计方案的。这款开源软件是一个图形化的网络模拟器,用于仿真模拟多种网络设备,如交换机、路由器、防火墙和入侵检测等。支持 Windows、Linux 和 Mac 的跨平台使用,开源性和跨平台使其被广泛使用,相较于软件 Cisco Packet Tracer,可以应对更加复杂的网络设计,并且支持网络安全设备的仿真实验。

GNS3 支持 Cisco 和非 Cisco 创建网络设计方案,可在项目中添加网络对象,模拟硬件设备的组合方案,保存项目后可以随时访问设计方案,具备跨多台计算机资源的分享能力,为网络方案设计提供了较好的灵活性。GNS3 为了适应不同用户的需求,集成了多种功能组件,如 Dynamips、Qemu 和 Wireshark 等程序,如表 3.1 所示。Dynamips 应用程序由法国人 Christophe Fillot 于 2005 年创建,GNS3 在 Dynamips 基础上,提供了友好的图形化操作界面,这是一个基于虚拟化技术的模拟器,用于模拟路由器和交换机等硬件设备。Dynamips 模拟器程序可以仿真 Cisco3600、3700 和 7200 等系列路由器硬件。通过 Dynamips 模拟器程序,使用 GNS3 模拟了网络插槽和广域网接口卡,实现了硬件设备的快速配置,如添加多个以太网接口卡、交换机模块、串口到设备中,为基本设备添加、删除内存等。Qemu 组件使 GNS3 软件可以支持网络安全设备模拟,如模拟防火墙、入侵检测系统和 Juniper 等。Wireshark 组件使 GNS3 软件可以支持对模拟器上网络设备之间的 IP 数据包进行捕获,从而可以对底层数据进行分析。因此,需要单独安装 WinPCAP、Npcap 和 Wireshark 等软件,否则该功能无法启用。

表 3.1 GNS3 组件说明

组 件	描 述
WinPCAP	将 GNS3 连接到外部,允许网络通信
Npcap	可替代 WinPCAP,解决 WinPCAP 的 Win10 问题,相对 WinPCAP 的测试少,可共存

续表

组 件	描 述
Wireshark	捕获、查看网络节点之间发送的网络流量
Dynamips	在本地 GNS3 运行 Cisco 路由器。如果只使用 GNS3 VM,则不需要勾选
QEMU 3.1.0 /0.11.0	一个计算机模拟器,如 Linux 系统,Qemu 0.11.0 安装时为了支持旧版 ASA 设备,推荐使用 GNS3 VM
VPCS	轻量级 PC 模拟器,支持 ping 和 traceroute 等命令
Cpulimit	避免 QEMU 百分百使用 CPU,如旧版本 ASA 设备
GNS3	必选项,GNS3 软件核心
TightVNC Viewer	图形化 VNC 客户端
Solar-Putty	新的默认控制台应用程序
Virt-viewer	推荐项,预装了 qemu-spice 的 Qemu VMs 的备用显示
Intel Hardware Acceleration Manager (HAXM)	仅适用于未使用 Hyper-V 的 Intel CPUs (启用 VT-X)的系统,用于 Android 模拟器硬件加速和 QEMU

## 3.2 GNS3 安装调试

### 3.2.1 GNS3 下载和配置要求

从 GNS3 官网或开源网站 GitHub 下载 GNS3 的所需版本,如图 3.1 所示,选择操作系统版本后执行下一步操作。本书实验采用 GNS3v0.8.6 版本的 GNS3 软件包,资源占用相对较少。新版本 GNS3 安装相对复杂,硬件要求高,资源消耗大,对软件包的依赖多,尤其是 Linux 系统。官网给出了最小硬件要求、推荐和最优硬件配置,操作系统要求 Windows 7 或者更高的版本,GNS3 软件安装的硬件基本需求是内存至少 4GB,推荐内存使用 16GB 至 32GB,CPU 使用 Core i7 或 i9,学生实验推荐使用实验版本。下面以 MacOS 版本 GNS3-2.2.25 为例,介绍安装过程、所需的组件和系统配置等操作。

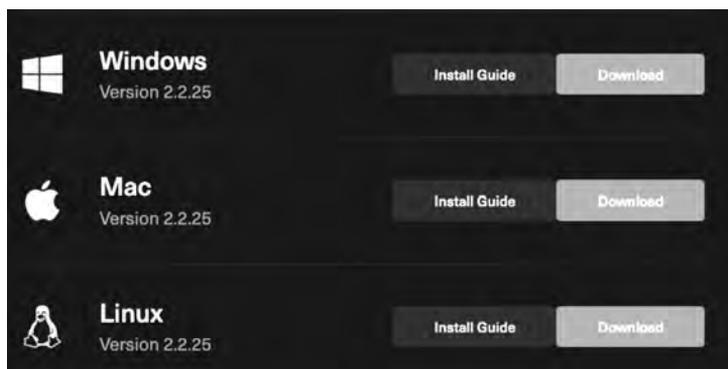


图 3.1 选择操作系统版本

## 3.2.2 安装 GNS3 及其组件

### 1. 安装 GNS3

GNS3 是款图形化界面工具,双击 GNS3 安装文件进行安装,Mac 版本的安装步骤简洁,如图 3.2 和图 3.3 所示拖动 APP 图标后,等待拷贝完成,如发现权限受限,则通过系统设置的安全和隐私功能,允许下载文件进行安装,并在安装完成后允许启动 GNS3 软件。



图 3.2 打开 GNS3 软件安装界面

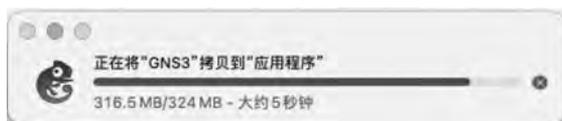


图 3.3 Mac 版本的安装界面

接着,进入安装软件初始页的界面、查看安装许可、选择安装路径,可按照如图 3.4、图 3.5 和图 3.6 所示的步骤进行操作。



图 3.4 安装向导初始页

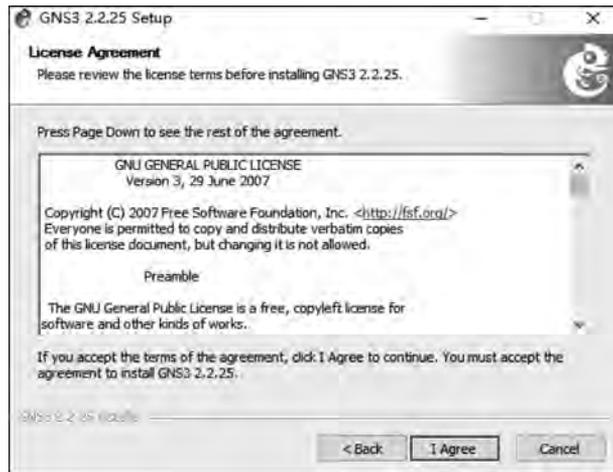


图 3.5 查看安装许可

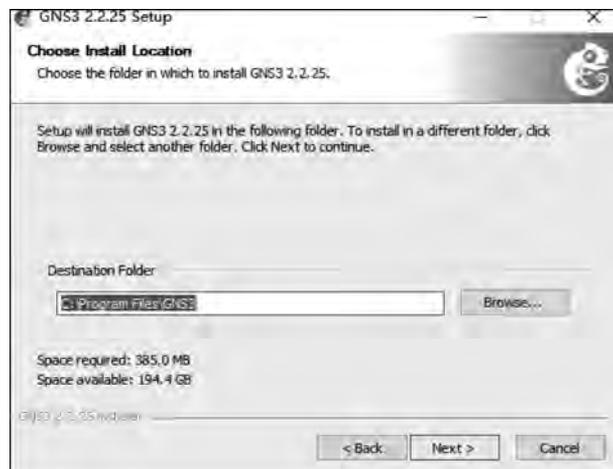


图 3.6 选择安装路径

## 2. 安装 GNS3 组件

GNS3 安装向导打开后,单击“Next”按钮,阅读许可协议信息并单击同意,继续单击“Next”按钮。提示安装 WinPCAP、Wireshark 等组件程序时,推荐不勾选,因为联网下载组件速度较慢,建议单独下载后安装速度更快。这样会提示 WinPACP 已经安装过了,取消安装组件,只安装 GNS3。

WinPCAP 是 Win32 平台抓包和网络分析的一个架构,软件与 Npcap 功能类似。Dynamips 用来创建使用思科路由器和交换机等组件,选择组件后单击“Next”按钮,如图 3.7 所示。

## 3. 添加 IOS 映像

安装完成后启动 GNS3,屏幕上会出现设置向导提示,提示用户需要三步设置便能够正常使用。这三步包括:(1)设置 IOS 映像文件路径;(2)检查 Dynamips 工作是否正常;

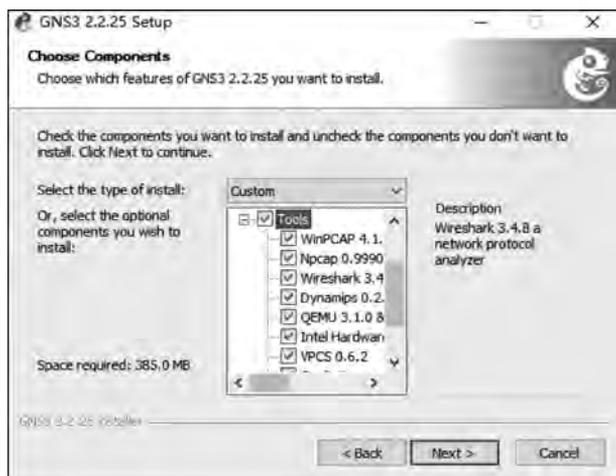


图 3.7 选择组件界面

(3) 设定 IOS 对应的 Idle-PC 值(后续实训内容再详细介绍)。

#### 4. 选择 GNS3 VM

默认安装其他 GNS3 插件,重复的可以勾掉。如图 3.8 所示,从 VMware Workstation、VMware ESXi、VirtualBox 和 Hyper-V 中任选一项。



图 3.8 GNS3 VM 选择界面

选择不同的安装软件版本,GNS3 的安装步骤基本相同,最后单击“Finish”按钮,就可以进入 GNS3 操作的主界面了,如图 3.9 所示,所有勾选组件安装完成。

### 3.2.3 配置 GNS3 环境

GNS3 通用配置界面如图 3.10 所示,第一个为工程目录,此目录用来存放工程的拓扑文件和配置信息;第二个为 OS 镜像目录,此目录用来存放各种系统镜像文件。这两个目



图 3.9 GNS3 安装完毕

录都可以自己设定,也可以选用系统默认的,这里使用系统默认的目录。

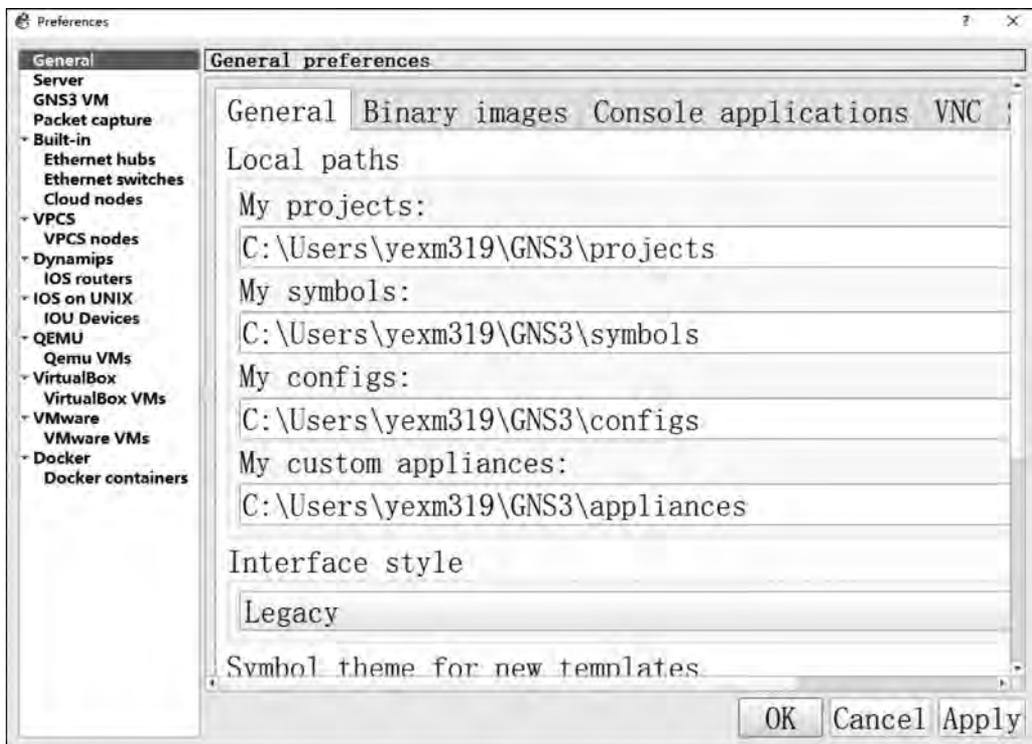


图 3.10 GNS3 通用配置界面

配置 IOS 文件路径,GNS3 需要使用 Cisco IOS 镜像文件来模拟路由器和交换机。支持的 IOS 平台包括 Cisco7200、3600 系列和 3700 系列 IOS。单击 GNS3 主界面的编辑菜单,选择菜单 IOS image and hypervisors。系统会弹出对话框,如图 3.11 所示,单击 IOS image 选项框的浏览选项,默认打开的目录是上面设置的 image 路径,也可以跳转到用户保

存镜像的路径,选定 IOS 文件打开。

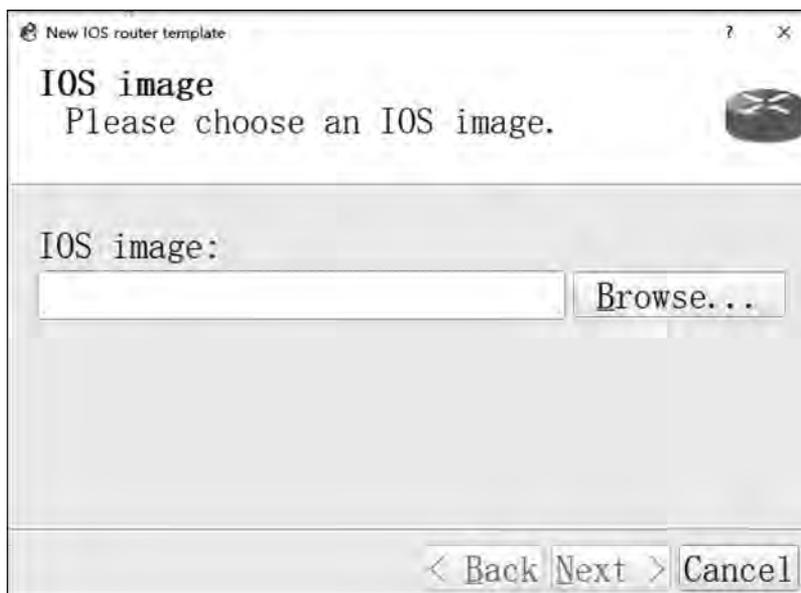


图 3.11 添加 IOS 镜像文件界面

该 IOS 文件就会出现在上面的镜像文件信息框中,也可以修改默认的镜像文件目录,要求目录是全英文路径。查看已经添加的模板信息,如图 3.12 和图 3.13 所示。

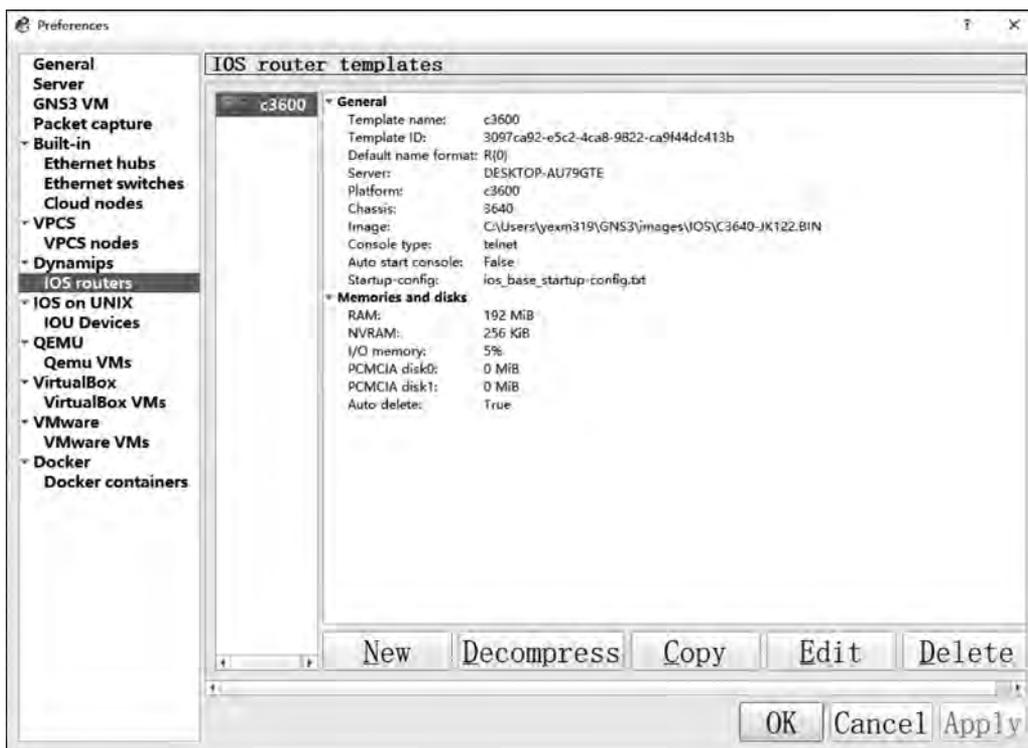


图 3.12 C3600 模板信息界面

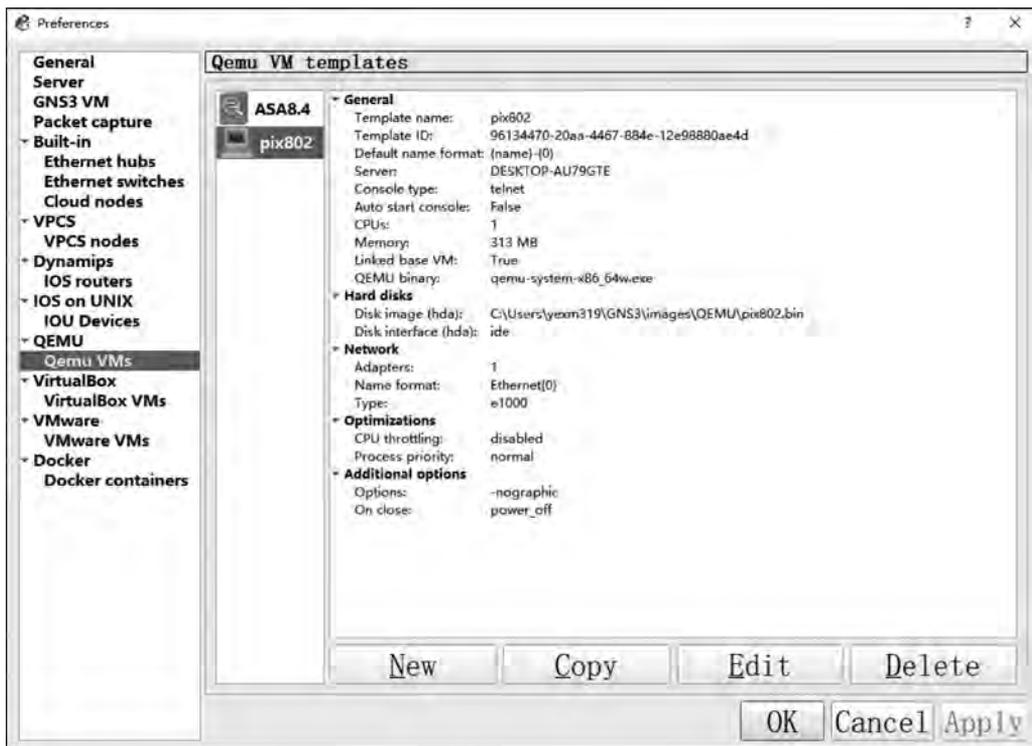


图 3.13 PIX 防火墙模板信息界面

### 3.2.4 配置 IOS 文件路径

配置 GNS3 基本参数,测试成功后,就能进行模拟 IOS 的实验。初始配置完成了,现在可以添加 IOS,以及进行 IDLE 计算,如图 3.14 和图 3.15 所示。GNS3 会自动识别此 IOS 文件的平台和型号,当模拟器开始运行时,通常要消耗主机较高的 CPU 使用率,有时甚至达到 100%,所以可通过参数优化来降低 GNS3 的硬件资源消耗,从而提高 GNS3 的运行效率,这里主要是设置 Idle-PC 值。GNS3 的一个优点是,系统可以判断出较优的 IDLE 值。Idle-PC 值是 GNS3 用于计算系统消耗的参数,这个参数会直接影响 GNS3 对主机 CPU 资源的占用率,较优的 Idle-PC 值可以将 CPU 占用率降低到 10% 以下,IDLE 值配置完毕以后,就可以直接进行实验了,如图 3.16 所示。

IDLE 值只需要计算一次,之后进行实验不用再进行 IDLE 值计算。单击“Idle-PC”按钮后,GNS3 会自动开始计算 IDLE 值,此过程可能会导致系统卡顿,直到出现下一个图,单击“Apply”或 OK 按钮来保存当前设置,关闭窗口后返回到 GNS3 的主界面。关于 IDLE 值的获取,很多路由器镜像文件同时提供了使用的最佳 IDLE 值以及相关配置参数,实验时可以直接使用。也可能出现部分主机无法计算出最佳 IDLE 值的情况,此时,通过配置路由器 IP 地址等命令后,再计算 IDLE 值来解决此问题。

为了便于使用,可以进入 Edit 菜单,选择 Preferences 菜单,将 GNS3 的 Language 配置为中文,然后需要重启 GNS3 生效,之后使用软件时就是中文界面。

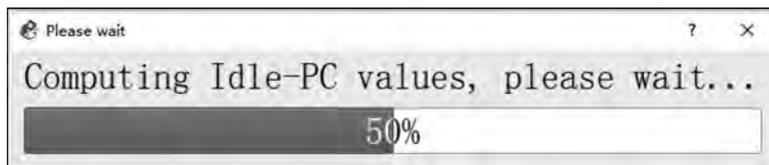


图 3.14 计算 Idle-PC 值

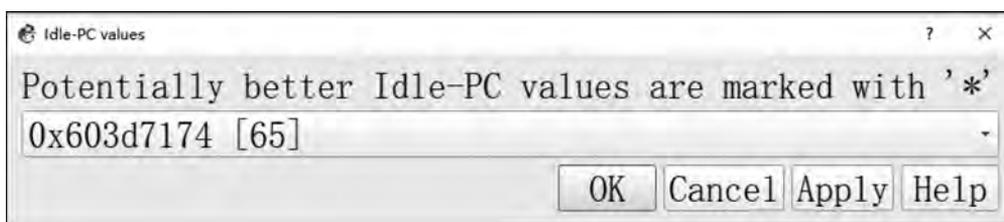


图 3.15 获得 Idle-PC 值

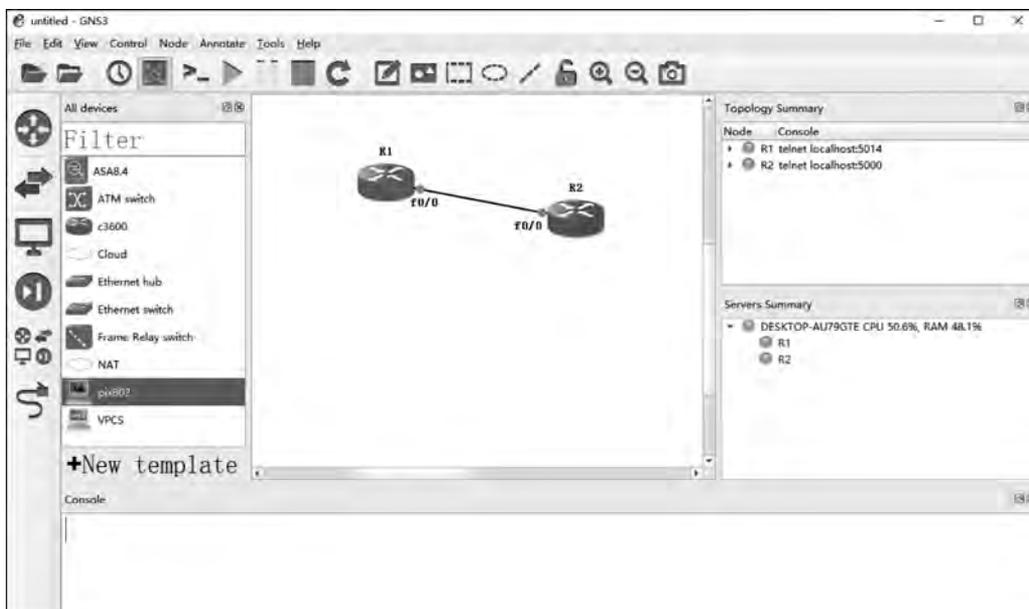


图 3.16 GNS3 网络拓扑图界面

### 3.3 GNS3 网络拓扑创建

在 GNS3 界面窗口有 3 个区域 4 个面板,包括左侧面板、右侧面板和中间区域,如图 3.17 所示。

(1) 左侧面板:列出了可用的节点类型(node)、各种设备如路由器、防火墙、以太网交换机等的图标,搭建拓扑时,从这里拖曳出设备。

(2) 右侧面板:提供抓包(Captures)信息和拓扑(Topology)汇总概要信息。

(3) 中间区域：包括两个面板，上面的面板是主要工作区，用于图形化显示拓扑结构；下面的面板是 Console 面板，用于连接到 Dynamips 程序的调试界面。

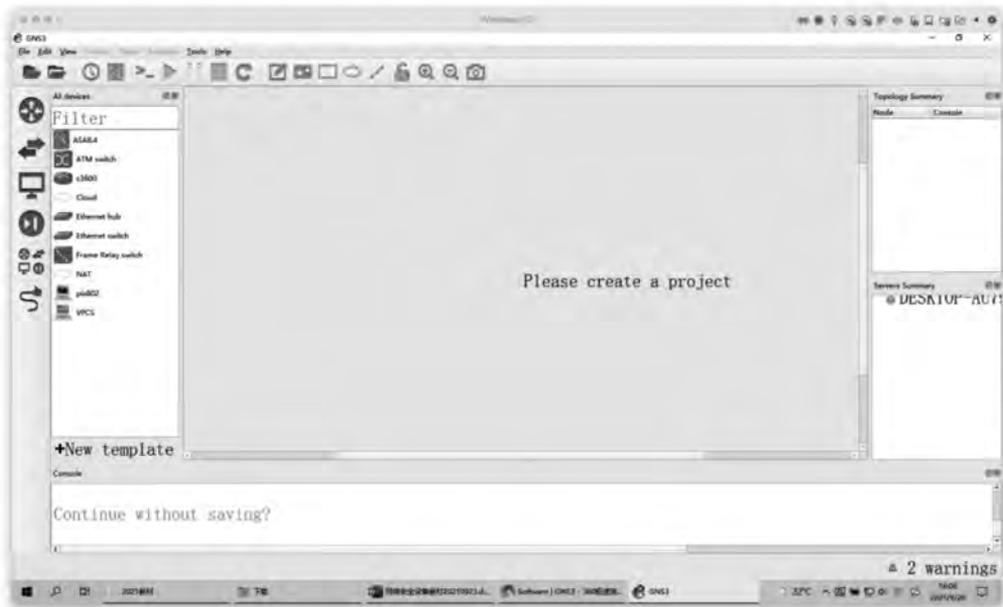


图 3.17 GNS3 软件主界面

配置一个路由器：从左侧面板拖动对应的路由器图标到中间的工作区，单击右键可以查看路由器的配置，还可以执行启动、停止、暂停和重启设备等操作，如图 3.18 所示。

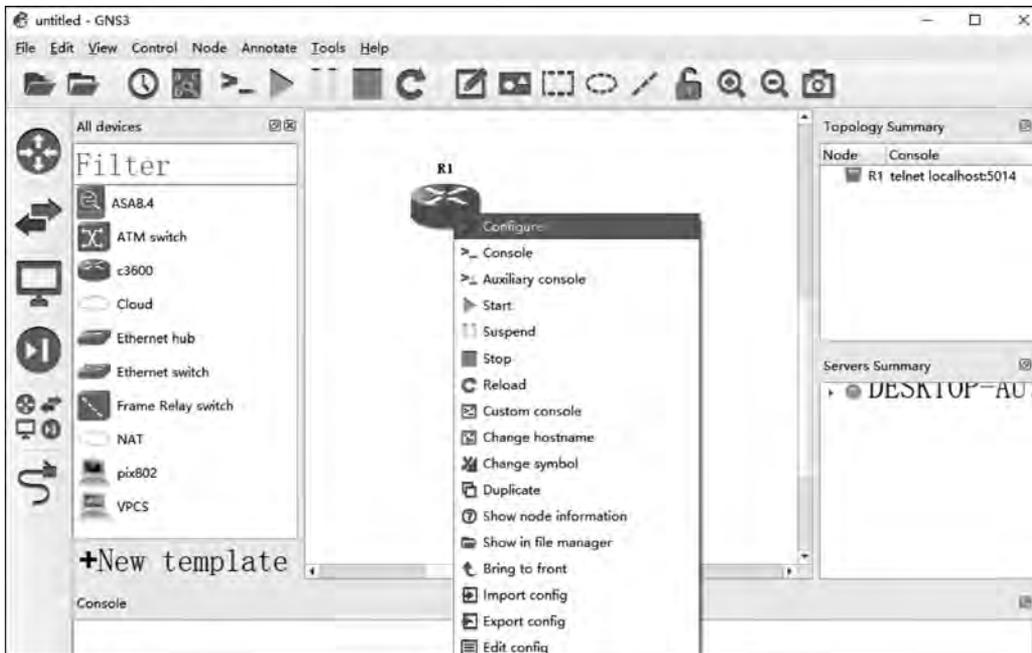


图 3.18 配置路由器

连接两台路由器：按照前面描述的操作方法，再从左侧面板拖出一台路由器，配置同样的接口模块。单击“连接线”来连接两台路由设备，再单击路由器 R1，会弹出已经配置的接口，选择路由器 R1 的接口 f0/0，再连接到路由器 R2 的接口 f0/0，如图 3.19 所示。

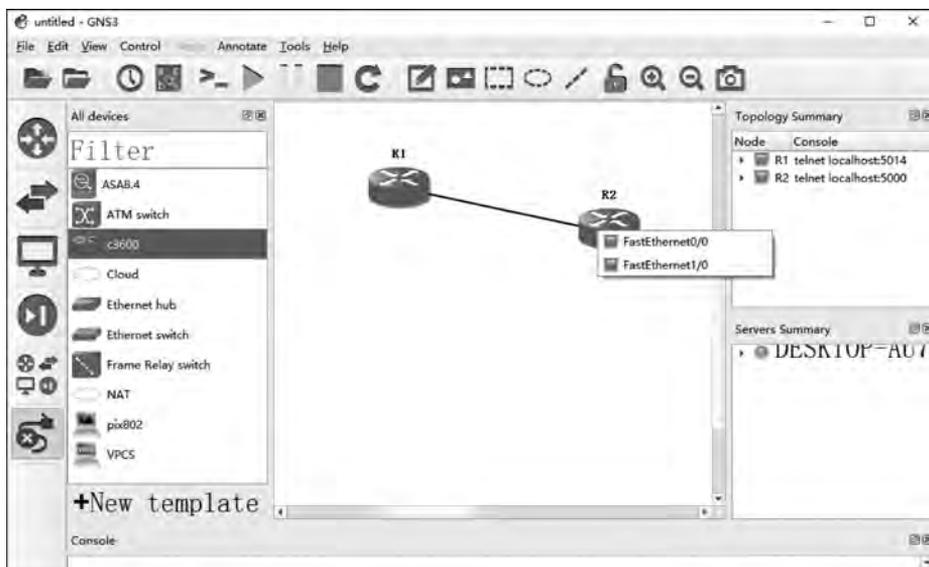


图 3.19 连接两台路由器

连接两台路由器之后，可以通过选择查看菜单的显示/隐藏接口标签 (Show/Hide interface labels) 菜单，这样就打开了显示接口名称的功能。尤其是当设备接口使用较多、配置较为复杂时，标签信息有助于规划、辨识模拟环境的接口连接关系，如图 3.20 所示。

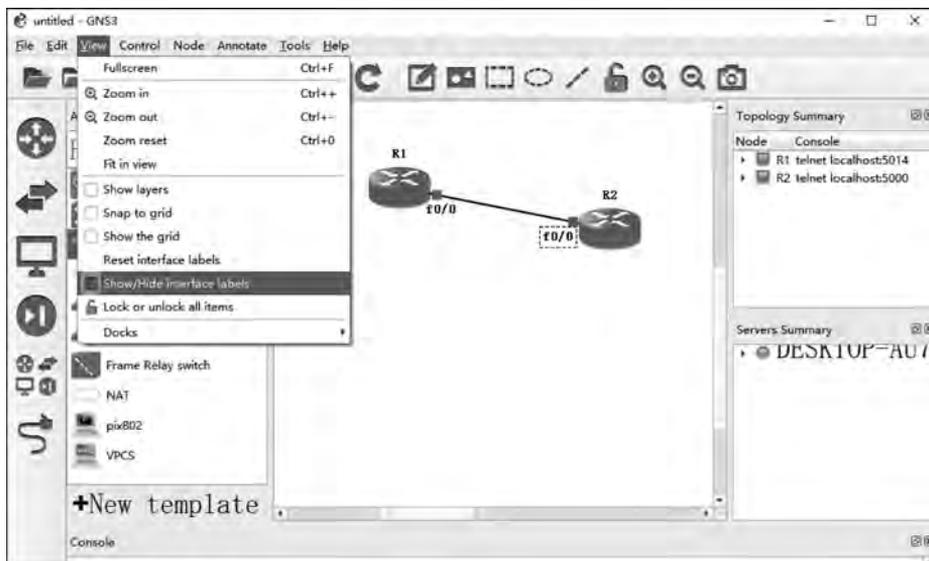


图 3.20 显示/隐藏接口标签

启动设备：启动 GNS3 中的路由器，并通过 SecureCRT 登录路由器。默认 GNS3 中连接线两端都是红色表示。将鼠标放在路由器上，并右键单击开启路由器，启动后所有的连接

线两端都变为绿色,如图 3.21 所示。

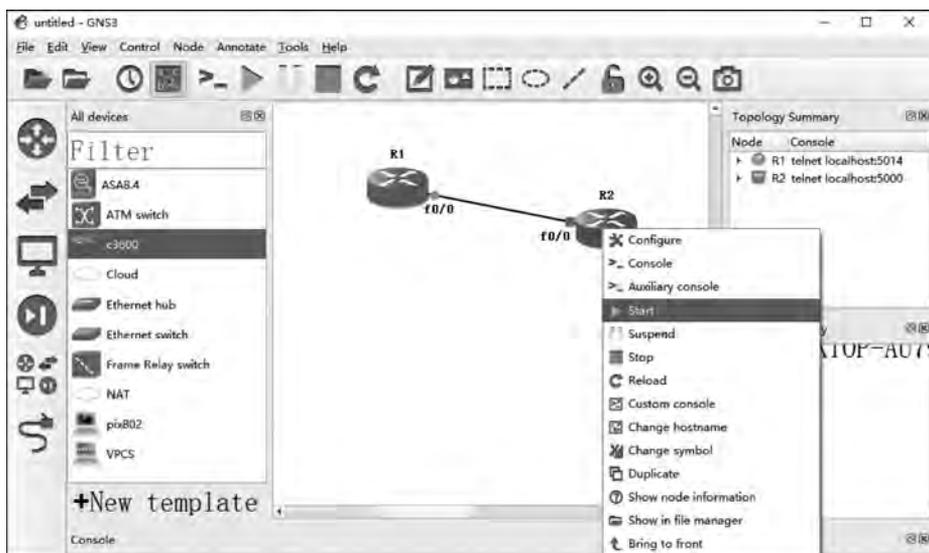


图 3.21 启动设备

通过 SecureCRT 管理设备:SecureCRT 软件连接设备,选择 Telnet 协议,本地主机的名称是 localhost 或者填写 127.0.0.1,端口号可查看右上角拓扑概要窗口,该窗口显示节点名称和 Console 信息。GNS3 的路由器 R1 的设备端口号为 5014,路由器 R2 的设备端口号为 5000,如图 3.22 所示。

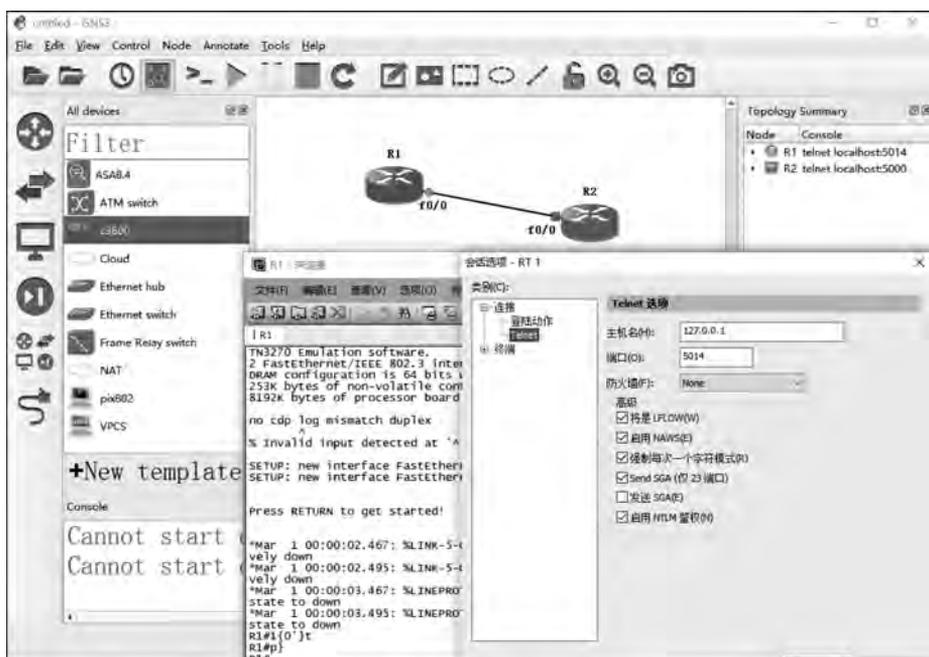


图 3.22 SecureCRT 命令管理配置界面

命令管理设备:GNS3 模拟器设备可以通过多种方式管理,使用 SecureCRT 进行命令调试是推荐方式,需要勾选、安装 SecureCRT 软件,并且配置正确的设备管理 Telnet 端口号,如图 3.23 所示。另一种方式如图 3.24 所示,可直接选中设备,右击,在弹出的快捷菜单中选择 Console 选项,直接进入控制台命令的管理界面,这种方式不需要配置主机名和通信端口的信息。

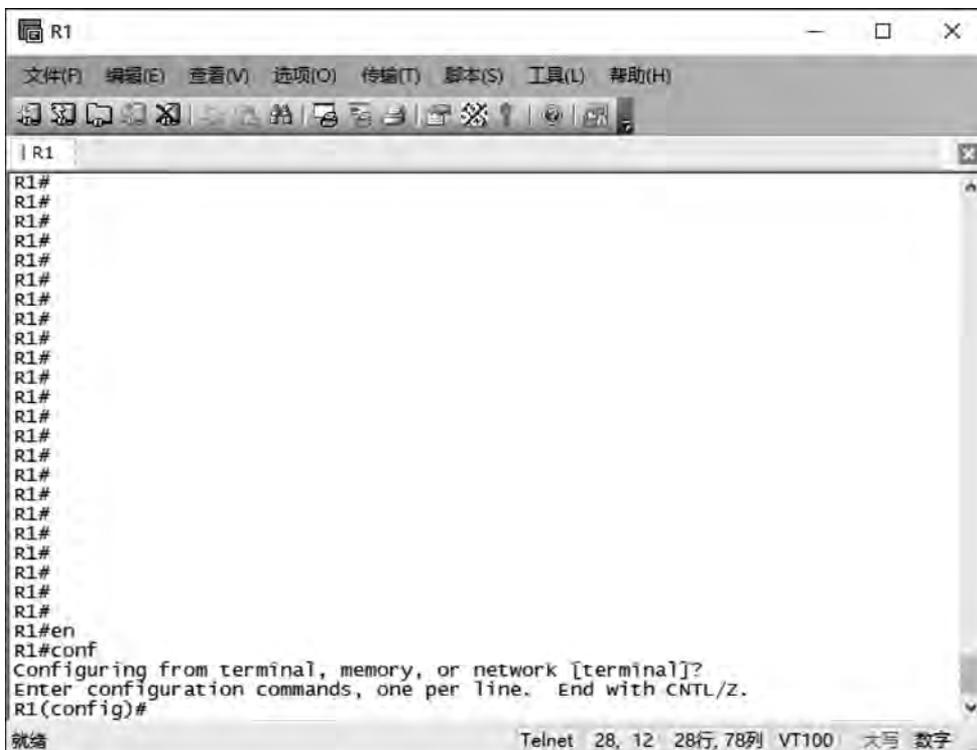


图 3.23 SecureCRT 控制台程序

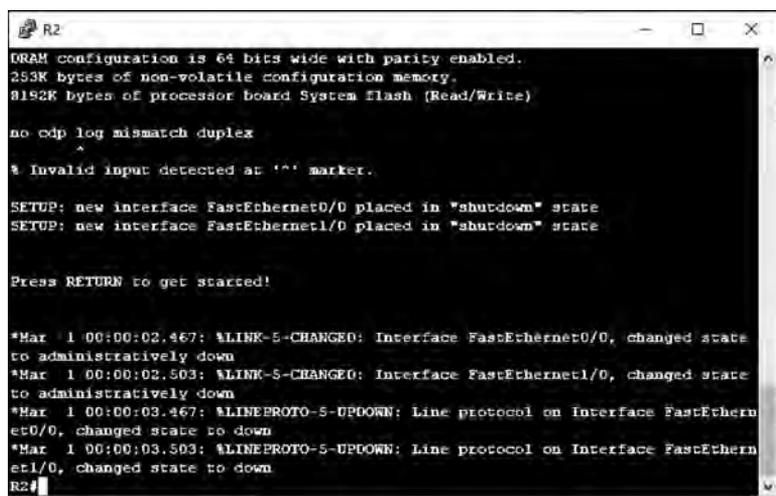


图 3.24 默认控制台程序

## 3.4 路由器桥接真机实训

### 3.4.1 实验目的与任务

#### 1. 实验目的

本实验为基础实验,主要目的是熟悉 GNS3 模拟器,配置路由器桥接真机或虚拟机,掌握路由器的配置命令和方法。本实验是后续综合实验防火墙日志配置和防火墙 AAA 配置的实验基础。本实验所需设备为路由器 2 台,网络连接线若干,PC 机或虚拟机 1 台。

#### 2. 实验任务

本实验主要任务如下:

- (1) 观察路由器接口硬件结构,掌握硬连线方法;
- (2) 掌握模拟器下路由器的配置,理解和配置路由器的基本命令,实现主机、虚拟机与路由器桥接;
- (3) 掌握查看路由器、真机网络配置信息的命令。

### 3.4.2 实验拓扑图和设备接口

根据实验任务规划设计实验的网络拓扑图,防火墙桥接真机实验拓扑图如图 3.25 所示。通过网络设备、路由器执行 ping 命令或 telnet 命令,发起位于防火墙不同安全区域网络设备的通信,验证防火墙功能是否配置正确。

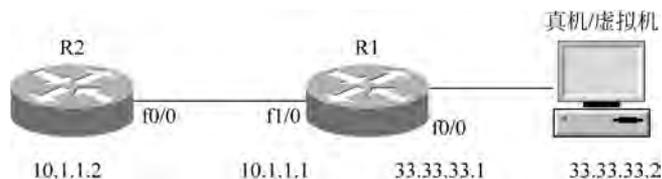


图 3.25 防火墙桥接真机实验拓扑图

根据实验任务,使用环回网卡来桥接真机,需要配置路由器和真机,配置网络参数后,使用命令 ping 测试,路由器 R2 和真机可以互通。根据实验任务和实验拓扑图,为每个网络设备及其接口规划相关配置,路由器 R1 的配置信息如表 3.2 所示。

表 3.2 路由器 R1 的配置信息

序 号	interface	IP Address
1	f0/0	33.33.33.1
2	f1/0	10.1.1.1

左端路由器 R2 的配置信息如表 3.3 所示。

表 3.3 路由器 R2 的配置信息

序 号	interface	IP Address
1	f0/0	10.1.1.2

真机的配置信息如表 3.4 所示。

表 3.4 真机的配置信息

序 号	interface	IP Address
1	环回网卡	33.33.33.2

### 3.4.3 实验步骤和命令

根据如图 3.25 所示实验拓扑设计,实现时需重点关注:桥接真机,先要系统安装环回网卡。配置路由器和真机、路由器和虚拟机的网络地址,设置 IP 地址属于同一子网,测试路由器 R2 和本计算机可以 ping 通,表示路由器和真机可以进行网络通信,桥接配置成功。

从控制面板进入高级网络配置界面,选择更改适配器选项,在网络连接的列表信息中,显示环回网卡已经安装成功,如图 3.26 所示。还要配置其 IPv4 地址等网络连接信息,如图 3.27 所示。



图 3.26 环回网卡安装成功



图 3.27 环回网卡的信息

本机还要创建静态路由,如图 3.28 所示,使用命令 `route add 10.1.1.0 mask 255.255.255.0 33.33.33.1` 设置主机静态路由,该命令指定主机到网段 10.1.1.0 的下一跳 IP 地址是 33.33.33.1。反之,删除该路由可使用命令 `route delete 10.1.1.0 mask 255.255.255.0 33.33.33.1`,还可以使用命令 `route print` 查验路由配置信息,具体操作如图 3.29 所示。

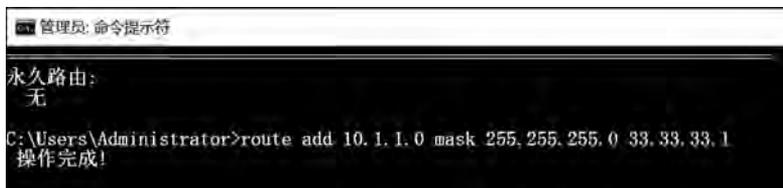


图 3.28 添加真机静态路由

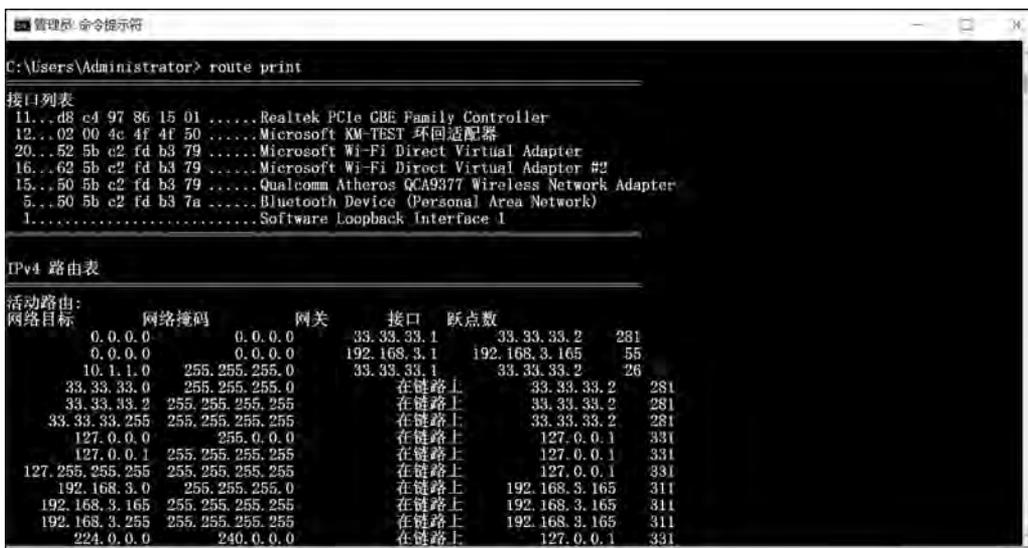


图 3.29 route print 显示真机路由

在 GNS3 模拟器中,按照实验网络拓扑图,以及本实训任务的接口规划,拖动对应网络设备图标并连接,再分别标注设备接口和 IP 地址等信息。完成上述工作后,启动网络设备执行配置命令,通过 `show` 命令查验设备配置是否正确,最后执行 `ping` 命令或 `telnet` 命令,验证设备之间的网络通信是否满足实验要求。

### 1. 路由器 R1 的配置

路由器 R1 的配置信息包括接口、路由配置,用于验证网络通信是否符合预期,命令如下所示:

```
R1 # EN
R1 # conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config) # int f0/0
R1(config-if) # ip add 33.33.33.1 255.255.255.0
```

```
R1(config-if) # no sh
R1(config-if) # end
R1 # show ip int br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          33.33.33.1      YES manual up          up
FastEthernet1/0          unassigned      YES unset  administratively down down
R1 # conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config) # int f1/0
R1(config-if) # ip add 10.1.1.1 255.255.255.0
R1(config-if) # no sh
R1(config-if) # end
R1 # show ip int br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          33.33.33.1      YES manual up          up
FastEthernet1/0          10.1.1.1        YES manual up          up
R1 # wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

## 2. 路由器 R2 的配置

路由器 R2 的配置信息包括接口、路由配置,用于验证网络通信是否符合预期,命令如下所示:

```
R2 # EN
R2 # conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config) # int f0/0
R2(config-if) # ip add 10.1.1.2 255.255.255.0
R2(config-if) # no sh
R2(config-if) # end
R2 # show ip int br
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          10.1.1.2        YES manual up          up
R2(config) # ip route 33.33.33.0 255.255.255.0 10.1.1.1
R2(config) # end
R2 # wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
00:03:20: %SYS-5-CONFIG_I: Configured from console by console
[confirm]
Building configuration...
[OK]
R2 # show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS - IS, su - IS - IS summary, L1 - IS - IS level - 1, L2 - IS - IS level - 2
       ia - IS - IS inter area, * - candidate default, U - per - user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
  33.0.0.0/24 is subnetted, 1 subnets
S       33.33.33.0 [1/0] via 10.1.1.1
  10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
```

## ★★本章小结★★

本章介绍了防火墙技术的实训环境安装和配置要点。实验使用了 GNS3 软件,并通过防火墙实训任务,进一步巩固和验证了防火墙技术和功能。并且比较了三个不同平台的安装过程,其中,安装配置到 Linux 最复杂,Windows 最易掌握,Mac 居中。

鉴于后续各个章节涉及的实验内容多,可能会出现看似命令配置正确却报错连连的情况,甚至安装相同实训配置步骤,却实验测试失败的情况。防火墙配置过程的常见错误总结为:配置命令前后顺序错误、遗漏命令、镜像版本错误等。

为了解决这些实训时遇到的问题,首先要理解每个实训任务,及其所对应的防火墙技术和原理,以及启用相应功能的步骤,最后才是决定实现上述防火墙的功能该使用哪些命令。每个实训任务都可以帮助读者更好地理解防火墙技术和验证防火墙镜像具备的功能。从简单的网络拓扑部署防火墙,引发读者思考复杂网络环境下,如何部署、发挥防火墙的功能。还可以通过 New project 重新配置解决。

因此,后续章节内容的学习,不仅仅是掌握命令的语法和使用场景,而是以防火墙常见的技术和功能为依托,实践实训任务。配置命令较少的基础实训任务,利于读者理解防火墙功能配置前后的流量穿越差异性。配置步骤和命令较多的复杂实训任务,利于帮助读者通过防火墙配置加深技术的理解。实训内容使用的命令越多,出错率越高,也正是通过配置、失败、排错的迭代过程,训练读者调试、排错和解决问题的能力,引发读者更多关于安全方案设计的思考和理解。

## 复习题

1. 对于 GNS3 的运行需要最小的内存配置是什么?
2. 如何修改镜像使用的内存大小?
3. 如何保存和加载工程的配置文件?