

《未来互联网综合专题研究》

Cisco Packet Tracer 实验指南

谭立状

山东省计算中心（国家超级计算济南中心）



齐鲁工业大学(山东省科学院)
QILU UNIVERSITY OF TECHNOLOGY SHANDONG ACADEMY OF SCIENCES



计算机科学与技术学部
FACULTY OF COMPUTER SCIENCE AND TECHNOLOGY



山东省计算中心
SHANDONG COMPUTER SCIENCE CENTER



国家超级计算济南中心
NATIONAL SUPERCOMPUTER CENTER IN JINAN

目录

实验一：Cisco Packet Tracer 介绍及安装.....	1
实验二：Cisco Packet Tracer 界面及图标介绍.....	5
实验三：Cisco Packet Tracer 基本连通测试实验.....	12
实验四：交换机基本配置及带内带外管理实验.....	14
实验五：交换机 VLAN 划分实验	18
实验六：三层交换机基本配置	21
实验七：利用三层交换机实现 VLAN 间路由.....	23
实验八：路由器基本配置	27
实验九：路由器静态路由配置	30
实验十：路由器 RIP 动态路由配置.....	33
实验十一：路由器 OSPF 动态路由配置	37
实验十二：路由器综合路由配置	41
实验十三：标准 IP 访问控制列表配置	45
实验十四：网络地址转换 NAT 配置	48
实验十五：IP 分析实验.....	51
实验十六：IPv6 RIPng 动态路由配置	56
实验十七：应用层及传输层协议（DNS、UDP、TCP、HTTP、FTP）分析	61

实验一：Cisco Packet Tracer 介绍及安装

1.1 什么是 Cisco Packet Tracer

Cisco Packet Tracer（简称 CPT 或 PT）是由 Cisco 公司发布的一个辅助学习工具，为学习思科网络课程的初学者去设计、配置、排除网络故障提供了网络模拟环境。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的详细处理过程，观察网络实时运行情况。可以学习 IOS（网际网操作系统，Internet work Operating System）的配置、锻炼故障排查能力。

Cisco 对 Cisco Packet Tracer 的官方介绍及定位：Cisco Packet Tracer is a powerful network simulator that can be utilized in training for CCNA and CCNP certification exam by allowing students to create networks with an almost unlimited number of devices and to experience troubleshooting without having to buy real Cisco routers or switches.

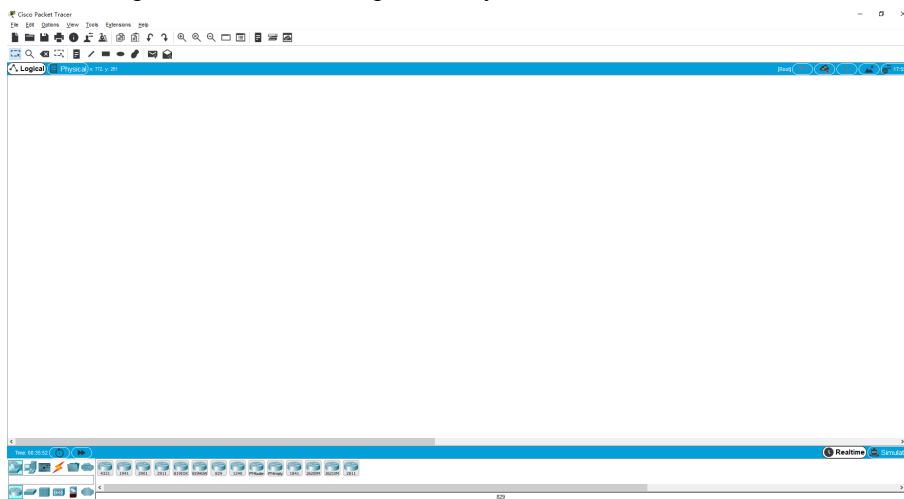


图 1-1 Cisco Packet Tracer 主界面

1.2 Cisco Packet Tracer 安装

1. 通过官方下载途径下载安装：

<https://www.packettracernetwork.com/download/download-packet-tracer.html>

*当前最新版本为 7.2.1，下载安装注意区分 32bit 和 64bit 软件。

2. 安装完成后，首次使用需使用邮箱进行注册。不注册账户则无法使用 Cisco Packet Tracer。账号注册可在 <https://www.netacad.com/en/one-step-self-enroll?p-p-id=onestepenrollmentportlet-WAR-studentenrollmentportlet&p-p-lifecycle=0&-onestepenrollmentportlet-WAR-studentenrollmentportlet-courseId=575428&-onestepenrollmentportlet-WAR-studentenrollmentportlet-language=en-US> 完成。

*注意区分思科账户和思科网校账户，这是两个账户，使用 Cisco Packet Tracer 需要思科网校账户而非思科账户。

3. 若不习惯英文软件，可以选择汉化，但不建议汉化。汉化方法：

找到文件安装目录下的 languages 文件夹，将汉化语言插件 chinese.ptl 复制到该文件夹内。打开 Cisco Packet Tracer，点击选项 Options->首选项 Preferences->Interface->Translator->选中 chinese.ptl->Change Language。然后重新启动 Cisco Packet Tracer。

4. Cisco Packet Tracer 还支持 Android 和 IOS 8.0+操作系统。可以搜索 Packet Tracer Mobile 并下载使用。

1.3 安装过程

1. 进入安装程序主界面，点击 next;
2. 选择接受协议，点击 next;
3. 选择安装目录，点击 next;
4. 修改文件夹，点击 next;
5. 出现创建桌面图标与快速启动图标复选框，选择后点击 next;
6. 完成安装。

1.4 Cisco Packet Tracer 功能及特点

(1) 支持多协议模型：支持常用协议 HTTP、DNS、TFTP、Telnet、TCP、UDP、Single Area OSPF、DTP、VTP、和 STP，同时支持 IP、Ethernet、ARP、wireless、CDP、Frame Relay、PPP、HDLC、inter-VLAN routing 和 ICMP 等协议模型。

(2) 支持大量的设备仿真模型：路由器、交换机、无线网络设备、服务器、各种连接电缆和终端等，这些设备是基于 CISCO 公司 还能仿真各种模块，在实际实验设备中是无法配置整齐的。提供图型化和终端两种配置方法。各设备模型有可视化的外观仿真。

(3) 支持逻辑空间和物理空间的设计模式：逻辑空间模式用于进行逻辑拓扑结构的实现；物理空间模式支持构建城市，楼宇、办公室、配线间等虚拟设置

(4) 可视化的数据报表示工具：配置有一个全局网络探测器，可以显示仿真数据报的传送路线，并显示各种模式，前进后退，或一步步执行。

(5) 数据报传输采用实时模式和仿真模式，实时模式与实际传输过程一样，仿真模式通过可视化模式显示数据报的传输过程，使用户能对抽象的数据的传送具体化。

1.5 Cisco Packet Tracer 学习资料

1. 51CTO 学院视频课程：

<http://edu.51cto.com/course/10369.html>

2. Cisco 官方视频课程：

<https://www.netacad.com/courses/packet-tracer>

3. 技术论坛实验资料：

<https://blog.csdn.net/al-assad/article/details/70255987>

*除此之外的任意 CCNA 课程书籍、视频、实验材料均可参考使用。

1.6 类似的仿真工具

1. GNS3

GNS3 是一款具有图形化界面可以运行在多平台（包括 Windows, Linux, and MacOS 等）的网络虚拟软件。Cisco 网络设备管理员或是想要通过 CCNA, CCNP, CCIE 等 Cisco 认证考试的相关人士可以通过它来完成相关的实验模拟操作。同时它也可以用于虚拟体验 Cisco 网际操作系统 IOS 或者是检验将要在真实的路由器上部署实施的相关配置。

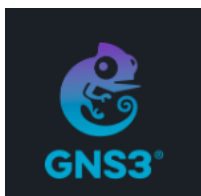


图 1-2 GNS3 图标

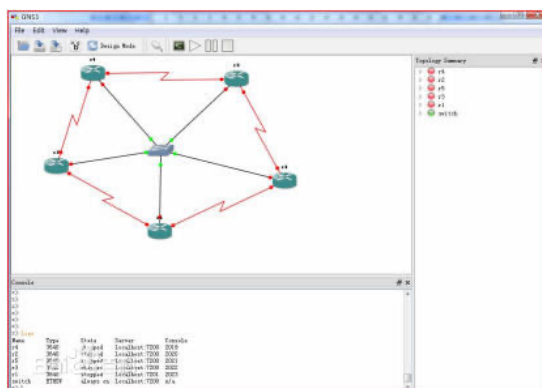


图 1-3 GNS3 主界面

2. eNSP

eNSP (Enterprise Network Simulation Platform) 是一款由华为提供的免费的、可扩展的、图形化操作的网络仿真工具平台，主要对企业网络路由器、交换机进行软件仿真，完美呈现真实设备实景，支持大型网络模拟，让广大用户有机会在没有真实设备的情况下能够模拟演练，学习网络技术。



图 1-4 eNSP 主界面

3. IOU

Cisco IOU，又名 IOU on Linux，作为 Web-IOU 的前身，是思科公司测试 IOU 时使用的模拟器，并且消耗资源很小。该模拟器在 NA 阶段不常用，在 NP、IE 阶段频繁使用。

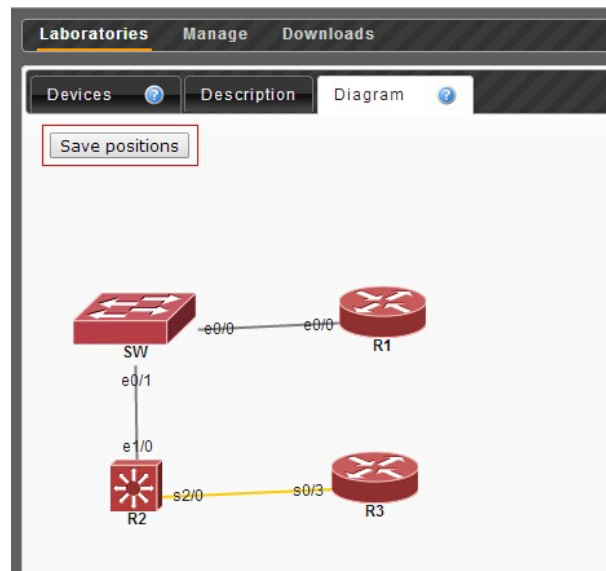


图 1-5 IOU-WEB 主界面

实验二：Cisco Packet Tracer 界面及图标介绍

2.1 Cisco Packet Tracer 界面介绍

Cisco Packet Tracer 主界面从上至下、从左至右依次为菜单栏、主工具栏、常用工具栏、逻辑/物理工作区栏、工作区、实时/模拟转换栏、网络设备栏、设备类型栏、特定设备库、用户数据包窗口等。

图 2-1 Cisco Packet Tracer 主界面栏目介绍

序号	栏目名	功能
1	菜单栏	此栏中有文件、选项和帮助按钮，我们在此可以找到一些基本的命令如打开、保存、打印和选项设置，还可以访问活动向导。
2	主工具栏	此栏提供了文件按钮中命令的快捷方式，我们还可以点击右边的网络信息按钮，为当前网络添加说明信息。
3	常用工具栏	此栏提供了常用的工作区工具包括：选择、整体移动、备注、删除、查看、添加简单数据包和添加复杂数据包等。
4	逻辑/物理工作区转换栏	我们可以通过此栏中的按钮完成逻辑工作区和物理工作区之间转换。
5	工作区	此区域中我们可以创建网络拓扑，监视模拟过程查看各种信息和统计数据。
6	实时/模拟转换栏	我们可以通过此栏中的按钮完成实时模式和模拟模式之间转换。
7	网络设备库	该库包括设备类型库和特定设备库。
8	设备类型库	此库包含不同类型的设备如路由器、交换机、HUB、无线设备、连线、终端设备和网云等。
9	特定设备库	此库包含不同设备类型中不同型号的设备，它随着设备类型库的选择级联显示。
10	用户数据包窗口	此窗口管理用户添加的数据包。

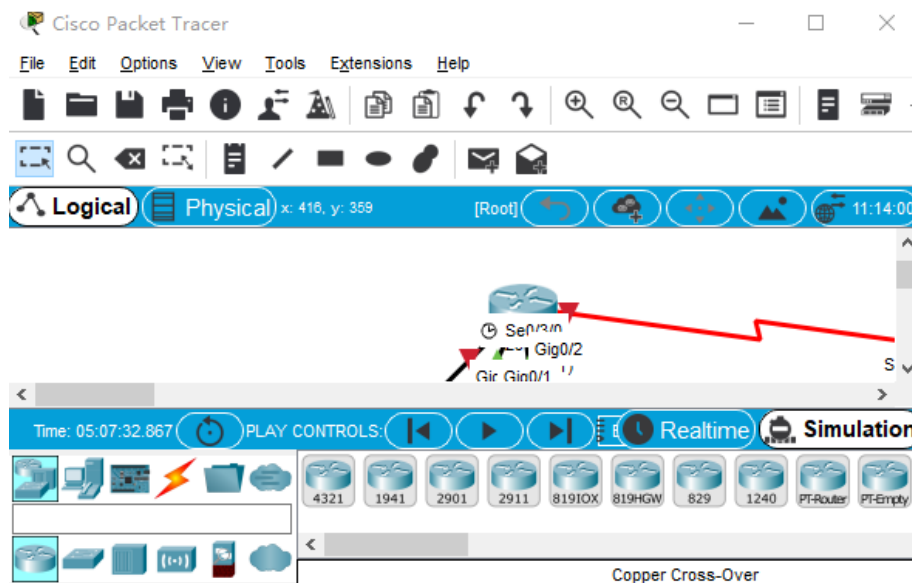


图 2-1 Cisco Packet Tracer 主界面

2.2 Cisco Packet Tracer 图标介绍

Cisco Packet Tracer 主界面的左下角放置有各种设备及链路图标，用户可自行拖拽图标至空白面板中，实现设备及链路的添加。

*注意，在选中设备并添加至工作区过程中，可按 ctrl 键+左键点击实现批量添加。也可选中已添加设备使用 ctrl+c 和 ctrl+v 实现设备复制粘贴。

表 2-2 常用工具栏图标

图标	名称及含义
	Select (Esc) 选定/取消 拖动选定设备
	Move layout (M) 移动画布
	Place note (N) 放置书签\贴便条
	Delete (Delete) 删除
	Inspect (I) 插入
	Resize Shape (Alt+R) 调整形状大小
	Add Simple PDU (P) 添加简单协议数据单元
	Add Complex PDU (C) 添加复杂协议数据单元

表 2-3 实时/模拟转换栏图标


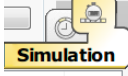
图标	名称及含义
	Realtime Mode (Shift+R) 实时模式 可以操作
	Simulation Mode (Shift+S) 模拟模式 显示过程

表 2-4 网络设备栏图标









图标	名称（快捷键）
	Routers 路由器 (Ctrl+Alt+R)
	Switches 交换机 (Ctrl+Alt+S)
	Hubs 集线器 (Ctrl+Alt+U)
	Wireless Devices 无线设备 (Ctrl+Alt+W)
	Connections 通讯链路 (Ctrl+Alt+O)
	End Devices 终端设备 (Ctrl+Alt+V)
	Custom Made Devices 定制设备 (Ctrl+Alt+T)
	Multiuser Connection 多用户连接器 (Ctrl+Alt+N)

表 2-5 链路图标

图标	名称
	Automatically Choose Connection Type 自动选择链路
	Console 配置线
	Copper Straight-Through 直连线
	Copper Croos-Over 交叉线
	Fiber 光纤
	Phone 电话线

	Coaxial 同轴电缆
	Serial DCE (Data Communication Equipment, 数据通讯设备) 串口线
	Serial DTE (Data Terminal Equipment, 数据终端设备) 串口线

2.3 Cisco Packet Tracer 设备配置栏

2.3.1 PC 设备

单击已添加到工作区的 PC 设备图标，显示如下：

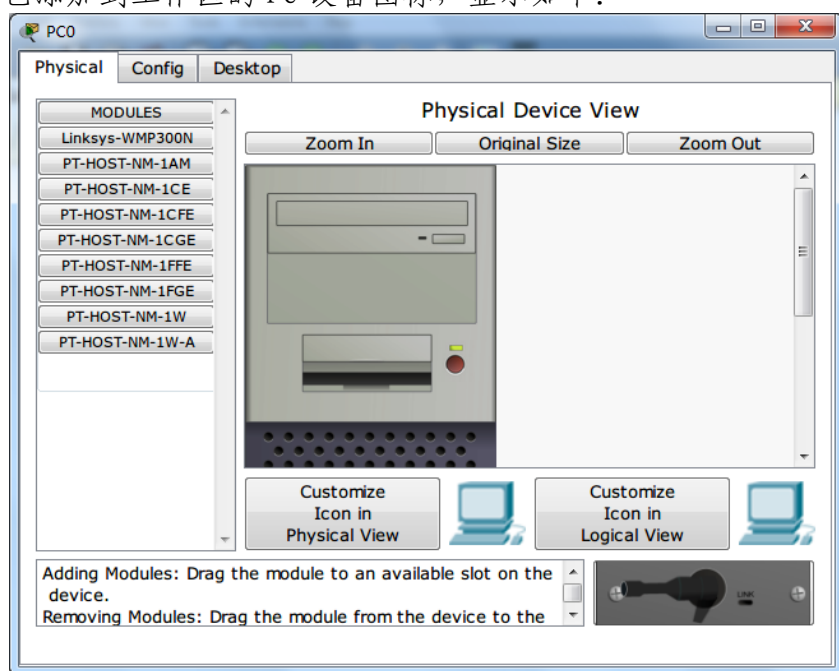


图 2-2 PC 设备配置栏-1

各部分含义如下：

Physical: 硬件

Config: 配置信息

Desktop: 桌面，包含 IP 地址、VPN、浏览器等常用功能的配置

Modules: 模块，拖动到右图的黑块（插口）即可使用

Physical Device View: 物理设备视图

Zoom In: （聚焦）放大

Original Size: （原始大小）复原

Zoom Out: （散焦）缩小

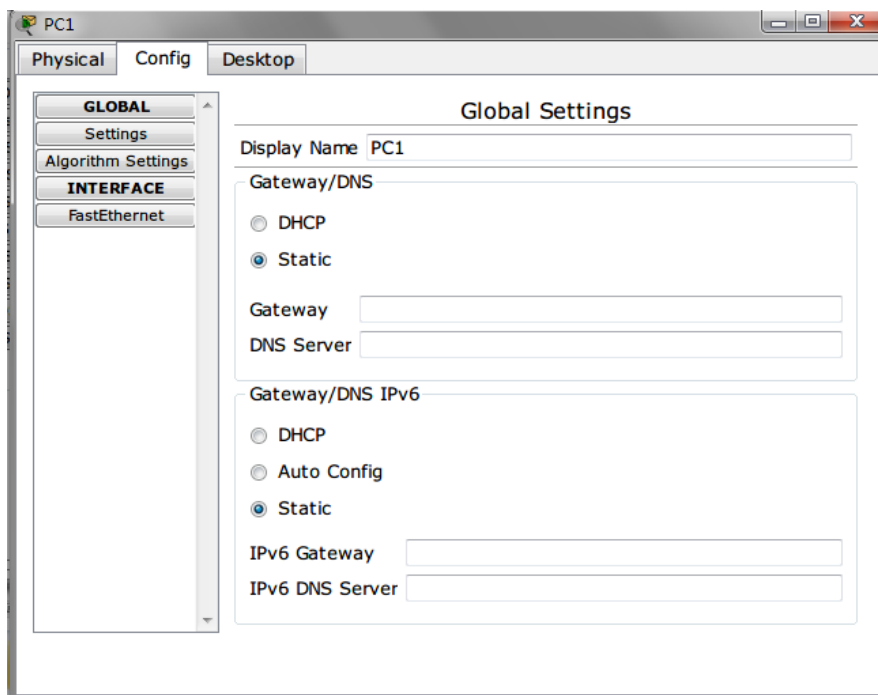


图 2-3 PC 设备配置栏-2

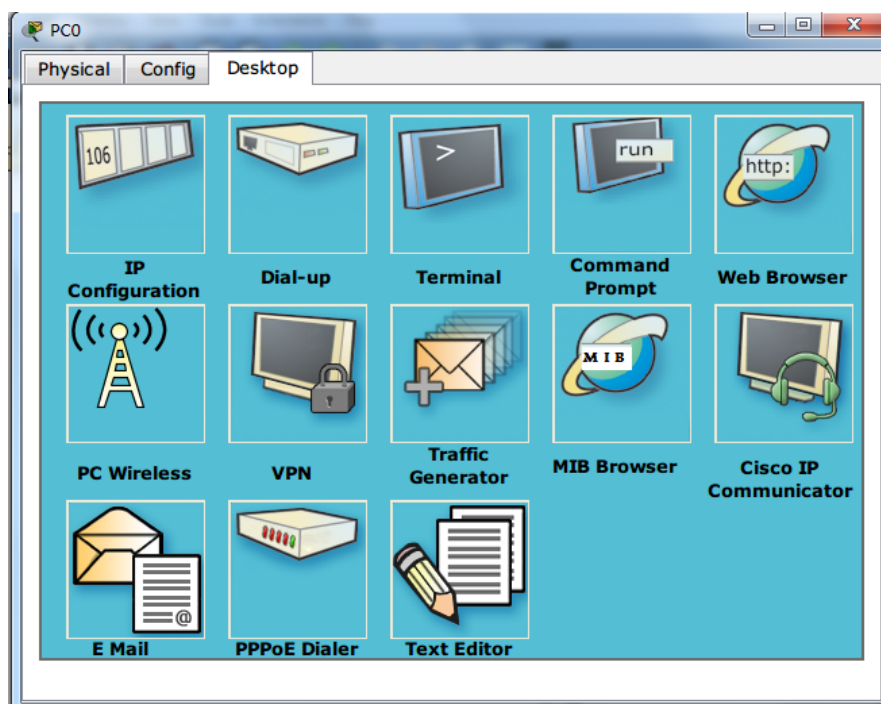


图 2-4 PC 设备配置栏-3

2.3.2 路由器设备

路由器配置

“Physical” 选项卡：主要用于配置设备接口模块，选择左侧的模块，将其拖动到右侧设备插槽即可（在添加或删除模块时，必须保持设备开关处于关闭状态）。

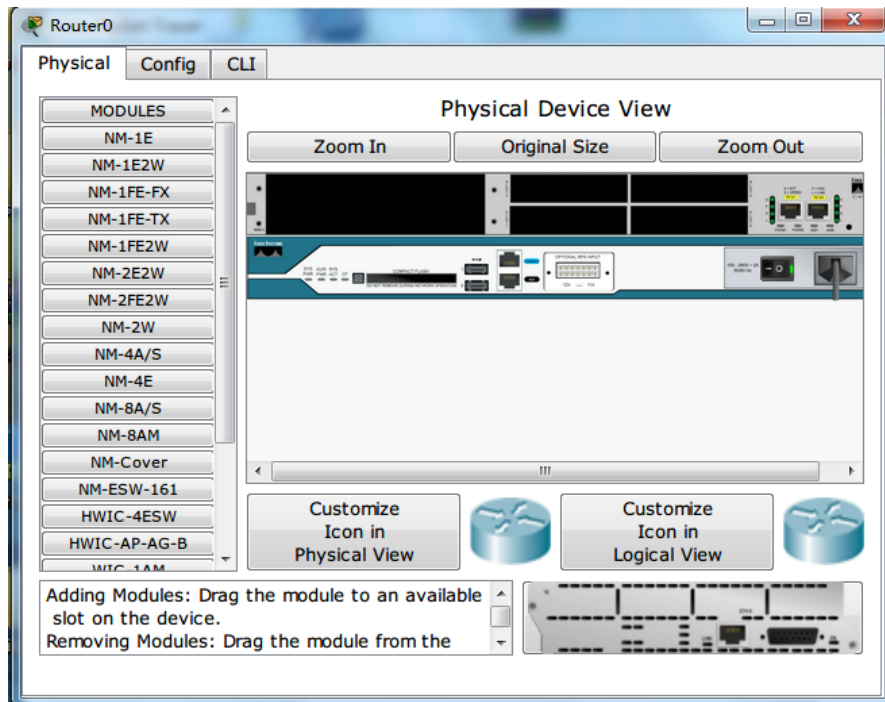


图 2-5 路由器配置-1

“Config” 选项卡: 主要用于图形化配置路由器的基本参数和配置文件的相关操作。

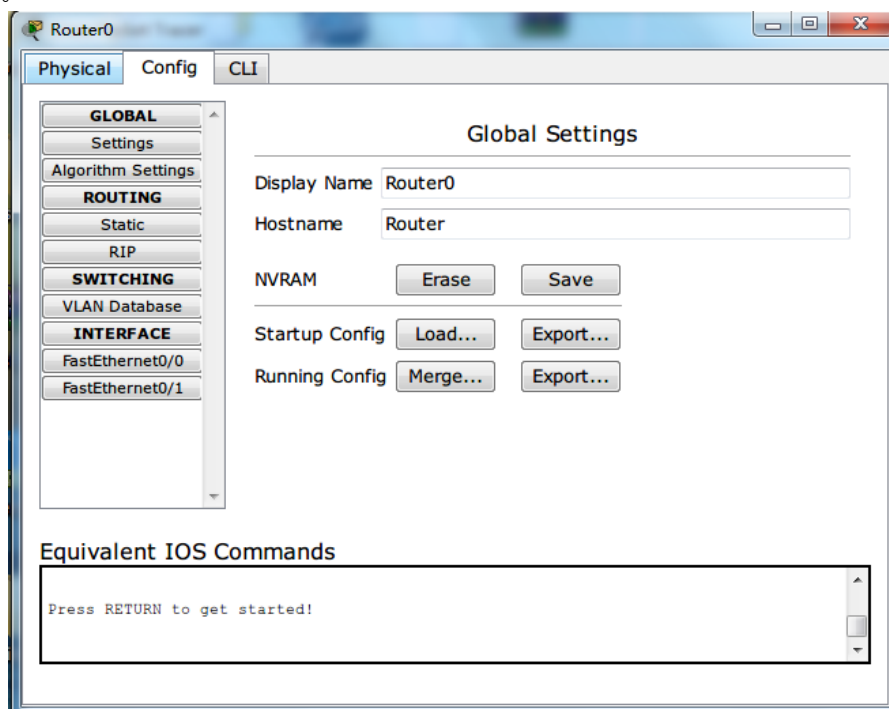


图 2-6 路由器配置-2

“CLI” 选项卡: CLI 命令行模拟真实设备的仿真界面, 可以在此对设备进行所需要的配置操作。

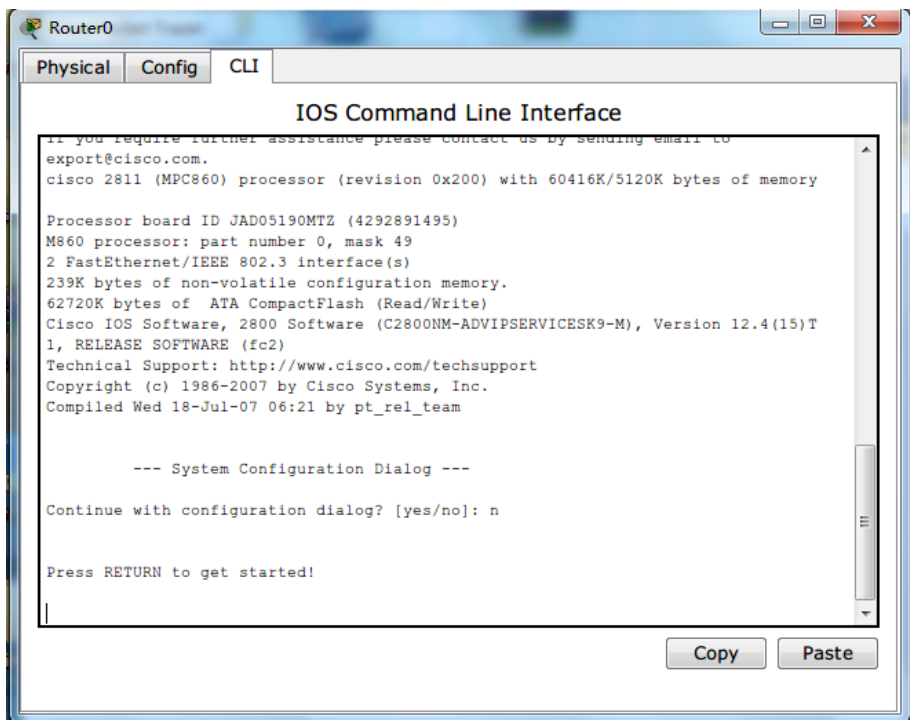


图 2-7 路由器配置-3

2.4 线缆两端颜色含义

线缆两端的圆点不同颜色有助于用户进行连通性的故障排除，其不同颜色对应的含义如下：

表 2-6 线缆两端颜色

链路圆点状态	含义
亮绿色	物理连接准备就绪，但还没有 Line Protocol Status 指示
闪烁绿色	连接激活
红色	物理连接不通，没有信号
黄色	交换机端口处于“阻塞状态”

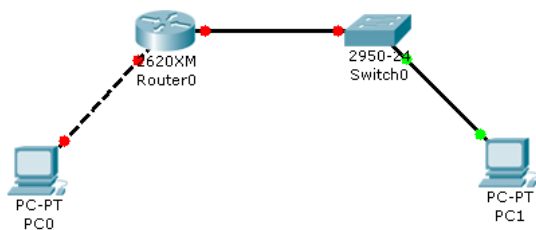


图 2-8 设备连接实例

实验三：Cisco Packet Tracer 基本连通测试实验

3.1 实验目的

掌握 Cisco Packet Tracer 基本使用方法，包括拓扑搭建、线缆连接、路由器配置命令、IP 地址配置及线路测试。

3.2 实验内容

搭建包含两台 PC 机和一台路由器的网络拓扑，选择合适线缆，主机互 Ping 成功。

3.3 实验拓扑

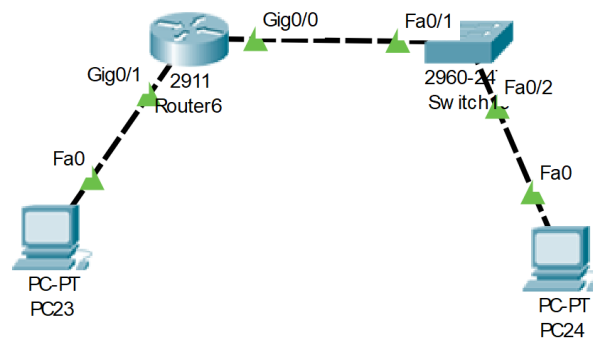


图 3-1 拓扑图

3.4 实验设备

路由器-2911 一台
交换机-2960 一台
PC 机两台
线缆 3 根

3.5 注意事项

线缆选择要正确，同层用交叉线，不同层用直通线。

3.6 实验过程

(1) 如实验拓扑图所示搭建网络拓扑，所有链路均显示绿色状态则表示链路互通。

(2) 路由器配置：

```
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router#config
Router(config)#inter g0/1
```

```
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#interface g0/0
Router(config-if)#ip add 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
```

(3) PC 机配置

配置 PC23 主机 IP 地址为 10.0.0.2，网关为 10.0.0.1；配置 PC24 主机 IP 地址为 11.0.0.2，网关为 11.0.0.1。

(4) 单击 PC23，选择 Desktop 中的命令提示符，输入 “ping 11.0.0.2”。显示结果如图 3-2 所示，则完成实验。

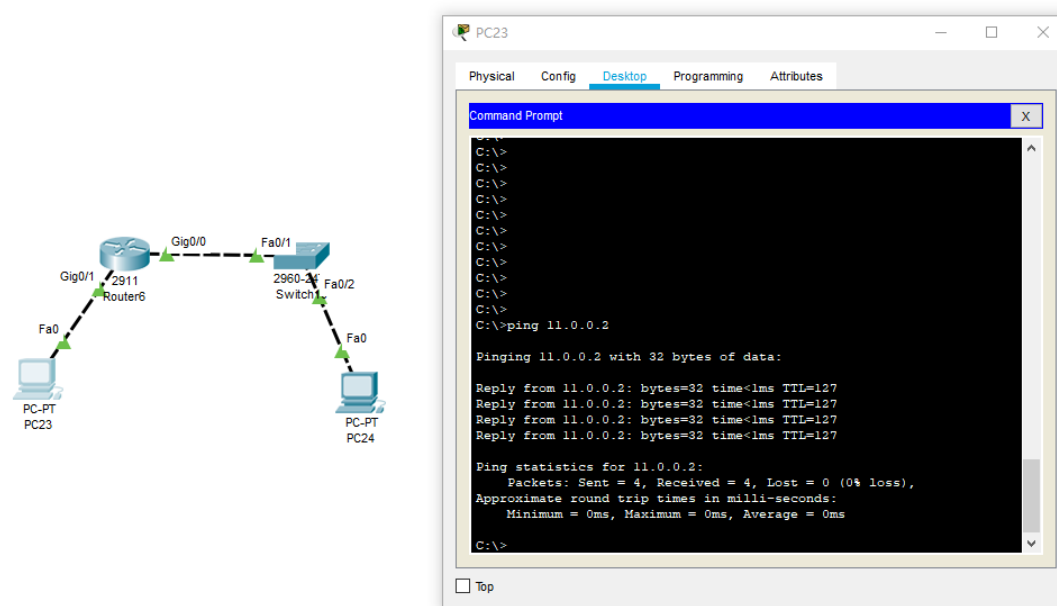


图 3-2 ping 命令结果

实验四：交换机基本配置及带内带外管理实验

4.1 实验目的

掌握交换机基本信息的配置管理。
了解交换机带内管理和带外管理。
掌握交换机配置的主要命令。

4.2 实验背景

某公司新进一批交换机，在投入网络以后要进行初始配置与管理，你作为网络管理员，对交换机进行端口的配置与管理。第一次在设备机房对交换机进行了初次配置后，你希望以后在办公室或出差时也可以对设备进行远程管理。

4.3 实验内容

- (1) 练习配置 Cisco 交换机的常用命令；
- (2) 总结常用的 show 命令。

4.4 技术原理

(1) 交换机的管理方式基本分为两种：带内管理和带外管理。通过交换机的 Console 端口管理交换机属于带外管理；这种管理方式不占用交换机的网络端口，第一次配置交换机必须利用 Console 端口进行配置。通过 Telnet、拨号等方式属于带内管理。

(2) 交换机的命令行操作模式主要包括：

- 用户模式 Switch>
- 特权模式 Switch#
- 全局配置模式 Switch(config)#
- 端口模式 Switch(config-if)#

(3) 交换机常用命令

- 进入特权模式(en)
- 进入全局配置模式(conf t)
- 进入交换机端口视图模式(int f0/1)
- 返回到上级模式(exit)
- 从全局以下模式返回到特权模式(end)
- 帮助信息(如?、co?、copy?)
- 命令简写(如 conf t)
- 命令自动补全(Tab)
- 快捷键(ctrl+c 中断测试, ctrl+z 退回到特权视图)
- Reload 重启。(在特权模式下)
- 修改交换机名称(hostname X)
- 配置交换机端口参数(speed, duplex)
- 查看交换机版本信息(show version)
- 查看当前生效的配置信息(show running-config)

- 查看保存在 NVRAM 中的启动配置信息 (show startup-config)
- 查看端口信息 Switch#show interface
- 查看交换机的 MAC 地址表 Switch#show mac-address-table
- 选择某个端口 Switch(config)# interface type mod/port (type 表示端口类型, 通常有 ethernet、Fastethernet、Gigabitethernet) (mod 表示端口所在的模块, port 表示在该模块中的编号) 例如 interface fastethernet0/1
- 选择多个端口 Switch(config)#interface type mod/startport-endport
- 设置端口通信速度 Switch(config-if)#speed [10/100/auto]
- 设置端口单双工模式 Switch(config-if)#duplex [half/full/auto]

(4) 配置交换机的管理 IP 地址 (计算机的 IP 地址与交换机管理 IP 地址在同一个网段)。

(5) 在 2 层交换机中, IP 地址仅用于远程登录管理交换机, 对于交换机的运行不是必需, 但是若没有配置管理 IP 地址, 则交换机只能采用控制端口 console 进行本地配置和管理。

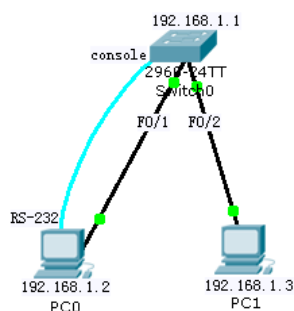
(6) 默认情况下, 交换机的所有端口均属于 VLAN1, VLAN1 是交换机自动创建和管理的。每个 VLAN 只有一个活动的管理地址, 因此对 2 层交换机设置管理地址之前, 首先应选择 VLAN1 接口, 然后再利用 IP address 配置命令设置管理 IP 地址。

(7) 为 telnet 用户配置用户名和登录口令:

- 设置进入特权模式的密码 switch(config)# enable password *****
- switch(config-line) 可以设置通过 console 端口连接设备及 Telnet 远程登录时所需的密码
- switch(config)# line console 0 表示配置控制台线路, 0 是控制台的线路编号
- switch(config-line)# login 用于打开登录认证功能
- switch(config-line)# password 5ijsj //设置进入控制台访问的密码

(8) 交换机、路由器中有很多密码, 设置对这些密码可以有效的提高设备的安全性。

4.5 实验拓扑



4.6 实验设备

交换机-2960 一台;

PC 机两台;

线缆 3 根。

4.7 实验步骤

- (1) 新建 Packet Tracer 拓扑图;
- (2) 利用 PC0 桌面选项卡中的超级终端对交换机进行基本配置;
- (3) 利用 PC0 桌面选项卡中的超级终端对交换机进行管理 IP 及 Telnet 配置;
- (4) 利用 PC1 桌面选项卡中的命令提示符对交换机进行管理配置。

4.8 实验内容

- (1) PC0 设置:

192.168.1.2

255.255.255.0

192.168.1.1

- (2) PC1 设置:

192.168.1.3

255.255.255.0

192.168.1.1

- (3) 通过 PC0 console 端口实现对交换机的管理

Switch>enable

Switch#conf t

Switch(config)#hostname S2960

S2960(config)#interface fa 0/1

S2960(config-if)#speed 100

S2960(config-if)#duplex full

S2960(config-if)#exit

同时将 PC 的网卡改成全双工模式, 100M 速率, 否则链路不通

S2960(config)#hostname switch

Switch(config)#exit

Switch#show version

Switch#show run

Switch#show interface

Switch#show mac-address-table

Switch#config t

Switch(config)#enable password cisco//激活特权模式密码为

cisco

Switch(config)#no enable password //取消特权模式密码

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#login

Switch(config-line)#no password//取消密码

(4) 通过 PC0 console 端口实现对交换机进行管理 IP 及 Telnet 配置:

```

Switch>En      //进入特权模式
Switch#conf t   //进入全局配置模式
Switch(config)#inter vlan 1 (默认交换机的所有端口都在 VLAN1 中) //
创建并进入 VLAN 1 的接口视图
Switch(config-if)#ip address 192.168.1.1 255.255.255.0 //在 VLAN
1 接口上配置交换机远程管理的 IP 地址
Switch(config-if)#no shutdown //开启接口
Switch(config-if)#exit //回到全局配置模式
Switch(config)#line vty 0 4    //进入远程登录用户管理视图, 0-4
个用户
Switch(config-line)#login //打开登录认证功能
Switch(config-line)#password 5ijsj //配置远程登录的密码为
5ijsj, 密码明码显示
Switch(config-line)#privilege level 3 //配置远程登录用户的权限
为最高级别权限 3
Switch(config-line)#end //退出到特权模式
Switch#show run //显示当前交换机配置情况

```

(5) 利用 PC1 桌面选项卡中的命令提示符对交换机进行管理配置。

PC0: 桌面选项卡中的 CMD, 命令提示符

```

ping 192.168.1.1 //成功以后, 再做下一步
telnet 192.168.1.1
输入 password: 5ijsj //登录成功, 进入用户模式
Switch>Enable //进入特权模式
Switch#

```

PC1: 桌面选项卡中的 CMD, 命令提示符

```

ping 192.168.1.1 //成功, 再做下一步
telnet 192.168.1.1
输入 password: 5ijsj
Switch>Enable //进入特权模式
Switch#

```

实验五：交换机 VLAN 划分实验

5.1 实验目标

理解虚拟 LAN (VLAN) 基本配置；
掌握一般交换机按端口划分 VLAN 的配置方法；
掌握 Tag VLAN 配置方法。

5.2 实验背景

某一公司内财务部、销售部的 PC 通过 2 台交换机实现通信；要求财务部和销售部的 PC 可以互通，但为了数据安全起见，销售部和财务部需要进行互相隔离，现要在交换机上做适当配置来实现这一目标。

5.3 技术原理

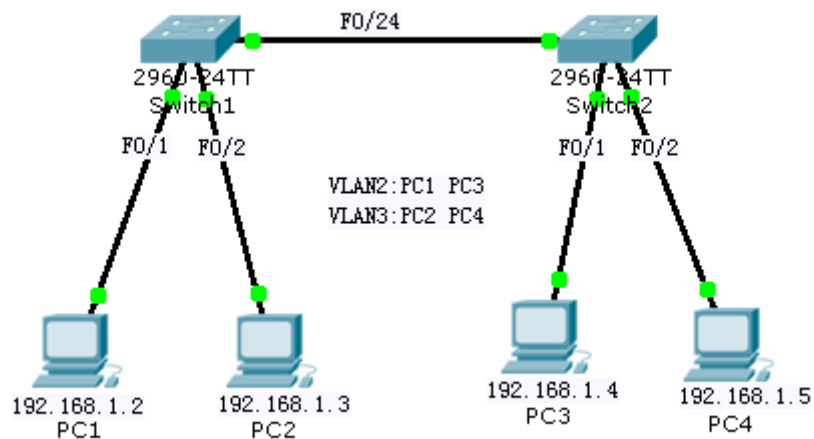
VLAN 是指在一个物理网段内。进行逻辑的划分，划分成若干个虚拟局域网，VLAN 做大的特性是不受物理位置的限制，可以进行灵活的划分。VLAN 具备了一个物理网段所具备的特性。相同 VLAN 内的主机可以相互直接通信，不同 VLAN 间的主机之间互相访问必须经路由设备进行转发，广播数据包只可以在本 VLAN 内进行广播，不能传输到其他 VLAN 中。

Port VLAN 是实现 VLAN 的方式之一，它利用交换机的端口进行 VLAN 的划分，一个端口只能属于一个 VLAN。

Tag VLAN 是基于交换机端口的另一种类型，主要用于是交换机的相同 Vlan 内的主机之间可以直接访问，同时对不同 Vlan 的主机进行隔离。Tag VLAN 遵循 IEEE802.1Q 协议的标准，在使用配置了 Tag VLAN 的端口进行数据传输时，需要在数据帧内添加 4 个字节的 802.1Q 标签信息，用于标示该数据帧属于哪个 VLAN，便于对端交换机接收到数据帧后进行准确的过滤。

5.4 实验设备及拓扑

Switch-2960 2 台；PC 4 台；直连线



5.5 实验步骤

- (1) 新建 Packet Tracer 拓扑图;
- (2) 划分 VLAN;
- (3) 将端口划分到相应 VLAN 中;
- (4) 设置 Tag VLAN Trunk 属性;
- (5) 测试

5.6 实验内容

PC1:

IP: 192.168.1.2
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC2:

IP: 192.168.1.3
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC3:

IP: 192.168.1.4
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC4:

IP: 192.168.1.5
Submark: 255.255.255.0
Gateway: 192.168.1.1

Switch1:

```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#inter fa 0/1
Switch(config-if)#switch access vlan 2
Switch(config-if)#exit
Switch(config)#inter fa 0/2
Switch(config-if)#switch access vlan 3
Switch(config-if)#exit
Switch(config)#inter fa 0/24
Switch(config-if)#switch mode trunk
Switch(config-if)#end
Switch#show vlan
```

Switch2:

```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#int fa 0/1
Switch(config-if)#switch access vlan 2
Switch(config-if)#exit
Switch(config)#int fa 0/2
Switch(config-if)#switch access vlan 3
Switch(config-if)#exit
Switch(config)#int fa 0/24
Switch(config-if)#switch mode trunk
Switch(config-if)#end
Switch#show vlan
```

5.7 实验结果

PC1 ping PC2 timeout

PC1 ping PC3 Reply

实验六：三层交换机基本配置

6.1 实验目标

理解三层交换机的基本原理；
掌握三层交换机物理端口开启路由功能的配置方法；

6.2 实验背景

公司现有 1 台三层交换机，要求你进行测试，该交换机的三层功能是否工作正常。

6.3 技术原理

(1) 开启路由功能

```
Switch(config)#ip routing
```

(2) 配置三层交换机端口的路由功能

```
Switch (config)#interface fastEthernet 0/5
```

```
Switch (config-if)#no switchport
```

```
Switch (config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Switch (config-if)#no shutdown
```

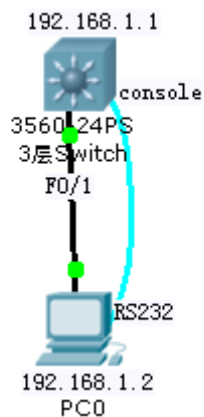
```
Switch (config-if)#end
```

(3) 如果是三层交换机的话，可以用到 no switchport 此命令。

(4) 三层交换机是带有三层路由功能的交换机，也就是这台交换机的端口既有三层路由功能，也具有二层交换功能。三层交换机端口默认为二层口，如果需要启用三层功能就需要在此端口输入 no switchport 命令。如果是二层交换机就不会用到 no switchport 命令。

6.4 实验设备及拓扑

交换机-3560 1 台，PC 1 台，直通线，配置线



6.5 实验内容

(1) PC0 设置:

192.168.1.2

255.255.255.0

(2) PC0 桌面上的终端

Switch>en

Switch#config t

Switch(config)#hostname S3550

S3550(config)#ip routing //开启路由功能

S3550(config)#interface fastEthernet 0/5

S3550(config-if)#no switchport //该端口启用三层路由功能

S3550(config-if)#ip address 192.168.5.1 255.255.255.0 //配置

IP 地址

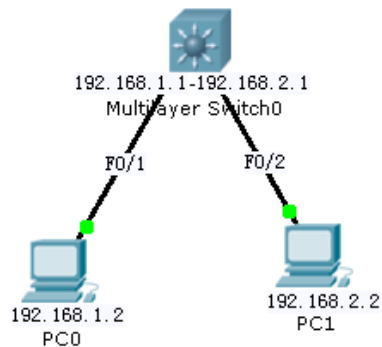
S3550(config-if)#no shutdown //开启端口

S3550(config-if)#end

S3550#

思考题:

利用三层交换机的路由功能固定 IP 地址的方法实现不同 vlan 之间联通?



实验七：利用三层交换机实现 VLAN 间路由

7.1 实验目标

掌握交换机 Tag VLAN 的配置；
掌握三层交换机基本配置方法；
掌握三层交换机 VLAN 路由的配置方法；
通过三层交换机实现 VLAN 间相互通信。

7.2 实验背景

某企业有两个主要部门，技术部和销售部，分处于不同的办公室，为了安全和便于管理对两个部门的主机进行了 VLAN 的划分，技术部和销售部分处于不同的 VLAN，先由于业务的需求需要销售部和技术部的主机能够相互访问，获得相应的资源，两个部门的交换机通过一台三层交换机进行了连接。

7.3 技术原理

三层交换机具备网络层的功能，实现 VLAN 相互访问的原理是：利用三层交换机的路由功能，通过识别数据包的 IP 地址，查找路由表进行选路转发，三层交换机利用直连路由可以实现不同 VLAN 之间的相互访问。三层交换机给接口配置 IP 地址。采用 SVI（交换虚拟接口）的方式实现 VLAN 间互连。SVI 是指为交换机中的 VLAN 创建虚拟接口，并且配置 IP 地址。

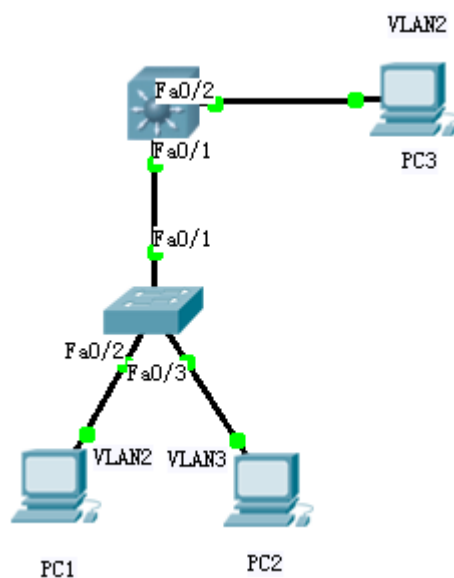
7.4 实验步骤

- (1) 新建 packet tracer 拓扑图
- (2) 在二层交换机上配置 VLAN2、VLAN3，分别将端口 2、端口 3 划分给 VLAN2、VLAN3。
- (3) 将二层交换机与三层交换机相连的端口 fa 0/1 都定义为 tag Vlan 模式。
- (4) 在三层交换机上配置 VLAN2、VLAN3，此时验证二层交换机 VLAN2、VLAN3 下的主机之间不能相互通信。
- (5) 设置三层交换机 VLAN 间的通信，创建 VLAN2、VLAN3 的虚接口，并配置虚接口 VLAN2、VLAN3 的 IP 地址。
- (6) 查看三层交换机路由表。
- (7) 将二层交换机 VLAN2、VLAN3 下的主机默认网关分别设置为相应虚拟接口的 IP 地址。
- (8) 验证二层交换机 VLAN2、VLAN3 下的主机之间可以相互通信。

首先在三层交换机上分别设置各 VLAN 的接口 IP 地址。三层交换机将 vlan 做为一种接口对待，就象路由器上的一样，再在各接入 VLAN 的计算机上设置与所属 VLAN 的网络地址一致的 IP 地址，并且把默认网关设置为该 VLAN 的接口地址。这样，所有的 VLAN 也可以互访了。

7.5 实验设备及拓扑

Switch-2960 1 台; Swithc-3560 1 台; PC 3 台; 直连线



7.5 实验过程

PC1:

IP: 192.168.1.2
Submark: 255.255.255.0
Gateway: 192.168.1.1

PC2:

IP: 192.168.2.2
Submark: 255.255.255.0
Gateway: 192.168.2.1

PC3:

IP: 192.168.1.3
Submark: 255.255.255.0
Gateway: 192.168.1.1

测试:

PC1 Ping PC3

Ping 192.168.1.3 reply

PC1 Ping PC2

Ping 192.168.2.2 timeout

S2960:

```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#int fa 0/2
```

```

Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa 0/3
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch#show vlan
S3560:
Switch>en
Switch#conf t
Switch(config)#vlan 2 //新建 vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3 //新建 vlan 3
Switch(config-vlan)#exit
Switch(config)#int fa 0/1 //进入 0 模块第 1 端口
Switch(config-if)#switchport trunk encapsulation dot1q //给
这个接口的 trunk 封装为 802.1Q 的帧格式
Switch(config-if)#switchport mode trunk //定义这个接口的工作
模式为 trunk
Switch(config-if)#exit
Switch(config)#int fa 0/2 //进入 0 模块第 2 端口
Switch(config-if)#switchport access vlan 2 //当前端口加入
vlan 2
Switch(config-if)#exit
Switch(config)#interface vlan 2 //进入 vlan2 虚拟接口
Switch(config-if)#ip address 192.168.1.1 255.255.255.0 //
配置 IP 地址
Switch(config-if)#no shutdown //开启该端口
Switch(config-if)#exit
Switch(config)#interface vlan 3
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip routing //开启路由功能
Switch#show ip route //显示路由表
Switch#show vlan //显示 vlan 信息

```

测试:

PC1 Ping PC3

Ping 192.168.1.3 reply

PC1 Ping PC2

Ping 192.168.2.2 reply

实验八：路由器基本配置

8.1 实验目标

掌握路由器几种常用配置方法；
掌握采用 Console 线缆配置路由器的方法；
掌握采用 Telnet 方式配置路由器的方法；
熟悉路由器不同的命令行操作模式以及各种模式之间的切换；
掌握路由器的基本配置命令；

8.2 实验背景

你是某公司新进的网管，公司要求你熟悉网络产品，首先要求你登录路由器，了解、掌握路由器的命令行操作；

作为网络管理员，你第一次在设备机房对路由器进行了初次配置后，希望以后在办公室或出差时也可以对设备进行远程管理，现要在路由器上做适当配置。

8.3 技术原理

路由器的管理方式基本分为两种：带内管理和带外管理。通过路由器的 Console 口管理路由器属于带外管理，不占用路由器的网络接口，其特点是需要使用配置线缆，近距离配置。第一次配置时必须利用 Console 端口进行配置。

8.4 实验步骤

- (1) 新建 packet tracer 拓扑图；
- (2) 用标准 console 线缆用于连接计算机的串口和路由器的 console 口上。在计算机上启用超级终端，并配置超级终端的参数，是计算机与路由器通过 console 接口建立连接；
- (3) 配置路由器的管理的 IP 地址，并为 Telnet 用户配置用户名和登录口令。配置计算机的 IP 地址（与路由器管理 IP 地址在同一个网段），通过网线将计算机和路由器相连，通过计算机 Telnet 到路由器上对交换机进行查看；
- (4) 更改路由器的主机名；
- (5) 擦除配置信息。保存配置信息，显示配置信息；
- (6) 显示当前配置信息；
- (7) 显示历史命令。

8.5 实验设备及拓扑

Router-2811 1 台；PC 1 台；交叉线；配置线



8.5 实验过程

PC:

IP: 192.168.1.2

Submask: 255.255.255.0

Gageway: 192.168.1.1

Router (不需做)

图形化: 界面开启 FastEthernet0/0 端口

命令行: rip 视图: router rip; ospf 视图: router ospf 1

PC 终端:

```
Router>en
```

```
Router #conf t
```

```
Router (config)#hostname R1
```

```
R1(config)#enable secret 123456 //设置特权模式密码
```

```
R1(config)#exit
```

```
R1#exit
```

```
R1>en
```

password: 此时输入密码, 输入的密码不显示

```
R1#conf t
```

```
R1(config)#line vty 0 4 //设置 telnet 远程登录密码
```

```
R1(config-line)#password 5ijsj
```

```
R1(config-line)#login
```

```
R1(config-line)#exit
```

```
R1(config)#interface fa 0/0 //进入路由器 0 模块第 0 端口
```

口配置相应的 IP 地址和子网掩码

```
R1(config-if)#ip address 192.168.1.1 255.255.255.0 //该端
```

```
R1(config-if)#no shut //开启端口
```

```
R1(config-if)#end
```

PC CMD;

```
Ipconfig /all    //查看本机 TCP/IP 配置情况（IP 地址、子网掩  
码、网关、MAC 地址）  
ping 192.168.1.1  
telnet 192.168.1.1    //远程登录到路由器上  
password: 5ijsj    //输入 telnet 密码  
en  
password: 123456    //输入特权模式密码  
show running    //显示路由器当前配置情况
```

实验九：路由器静态路由配置

9.1 实验目标

掌握静态路由的配置方法和技巧；
掌握通过静态路由方式实现网络的连通性；
熟悉广域网线缆的连接方式。

9.2 实验背景

学校有新旧两个校区，每个校区是一个独立的局域网，为了使新旧校区能够正常相互通讯，共享资源。每个校区出口利用一台路由器进行连接，两台路由器间学校申请了一条 2M 的 DDN 专线进行相连，要求做适当配置实现两个校区的正常相互访问。

9.3 技术原理

路由器属于网络层设备，能够根据 IP 包头的信息，选择一条最佳路径，将数据包转发出去。实现不同网段的主机之间的互相访问。路由器是根据路由表进行选路和转发的。而路由表里就是由一条条路由信息组成。

生成路由表主要有两种方法：手工配置和动态配置，即静态路由协议配置和动态路由协议配置。

静态路由是指有网络管理员手工配置的路由信息。

静态路由除了具有简单、高效、可靠的优点外，它的另一个好处是网络安全保密性高。

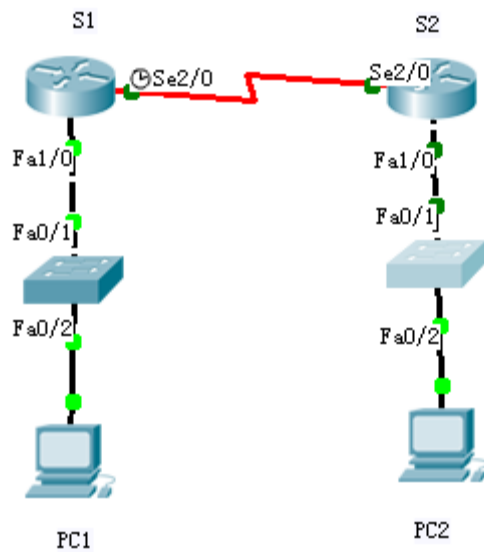
缺省路由可以看做是静态路由的一种特殊情况。当数据在查找路由表时，没有找到和目标相匹配的路由表项时，为数据指定路由。

9.4 实验步骤

- (1) 新建 packet tracer 拓扑图；
- (2) 在路由器 R1、R2 上配置接口的 IP 地址和 R1 串口上的时钟频率；
- (3) 查看路由器生成的直连路由；
- (4) 在路由器 R1、R2 上配置静态路由；
- (5) 验证 R1、R2 上的静态路由配置；
- (6) 将 PC1、PC2 主机默认网关分别设置为路由器接口 fa 1/0 的 IP 地址；
- (7) PC1、PC2 主机之间可以相互通信。

9.5 实验设备及拓扑

PC2 台；Router-PT 可扩展路由 2 台(Switch-2811 无 V.35 线接口)；Switch-2960 2 台；DCE 串口线；直连线；交叉线



9.6 实验过程

PC1

IP: 192.168.1.2
 Submask: 255.255.255.0
 Gateway: 192.168.1.1

PC2

IP: 192.168.2.2
 Submask: 255.255.255.0
 Gateway: 192.168.2.1

PC1 ping PC2

Ping 192.168.2.2 timeout

R1

```

en
conf t
hostname R1
int fa 1/0
no shut
ip address 192.168.1.1 255.255.255.0
exit
int serial 2/0
ip address 192.168.3.1 255.255.255.0
clock rate 64000 (必须配置时钟才可通信)

```

no shut

end

R2

en

```

conf t
hostname R2
int fa 1/0
ip address 192.168.2.1 255.255.255.0
no shut
exit
int serial 2/0
ip address 192.168.3.2 255.255.255.0
no shut
end

R1
en
conf t
ip route 192.168.2.0 255.255.255.0 192.168.3.2
end
show ip route

R2 25
en
conf t
ip route 192.168.1.0 255.255.255.0 192.168.3.1
end
show ip route

PC1 Ping PC2
Ping 192.168.2.2    reply

```

实验十：路由器 RIP 动态路由配置

10.1 实验目的

掌握 RIP 协议的配置方法；
掌握查看通过动态路由协议 RIP 学习产生的路由；
熟悉广域网线缆的连接方式。

10.2 实验背景

假设校园网通过一台三层交换机连到校园网出口路由器上，路由器再和校园外的另一台路由器连接。现要做适当配置，实现校园网内部主机与校园网外部主机之间的相互通信。为了简化网管的管理维护工作，学校决定采用 RIPv2 协议实现互通。

10.3 技术原理

RIP(Routing Information Protocols, 路由信息协议)是应用较早、使用较普遍的 IGP 内部网管协议，使用于小型同类网络，是距离矢量协议；

RIP 协议跳数作为衡量路径开销的，RIP 协议里规定最大跳数为 15；

RIP 协议有两个版本：RIPv1 和 RIPv2，RIPv1 属于有类路由协议，不支持 VLSM，以广播形式进行路由信息的更新，更新周期为 30 秒；RIPv2 属于无类路由协议，支持 VLSM，以组播形式进行路由更细。

10.4 实验步骤

建立建立 packet tracer 拓扑图

(1) 在本实验中的三层交换机上划分 VLAN10 和 VLAN20，其中 VLAN10 用于连接校园网主机，VLAN20 用于连接 R1。

(2) 路由器之间通过 V.35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000。

(3) 主机和交换机通过直连线，主机与路由器通过交叉线连接。

(4) 在 S3560 上配置 RIPv2 路由协议。

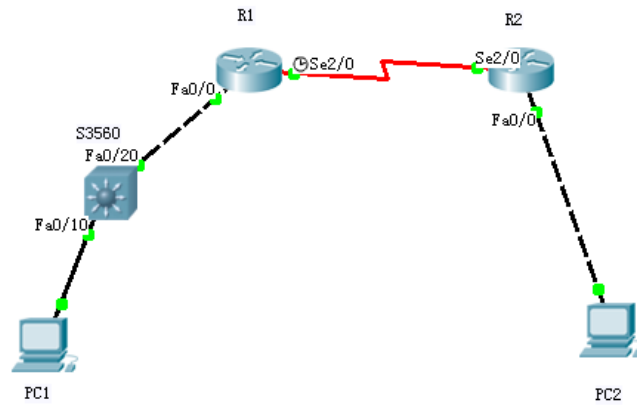
(5) 在路由器 R1、R2 上配置 RIPv2 路由协议。

(6) 将 PC1、PC2 主机默认网关设置为与直连网路设备接口 IP 地址。

(7) 验证 PC1、PC2 主机之间可以互相通信。

10.5 实验设备及拓扑图

PC 2 台；Switch-3560 1 台；Router-PT 2 台；直连线；交叉线；DCE 串口线



10.6 实验过程

PC1

IP: 192.168.1.2
 Submask: 255.255.255.0
 Gateway: 192.168.1.1

PC2

IP: 192.168.2.2
 Submask: 255.255.255.0
 Gateway: 192.168.2.1

S3560

```

en
conf t
hostname S3560
vlan 10
exit
vlan 20
exit
interface fa 0/10
switchport access vlan 10
exit
interface fa 0/20
switchport access valn 20
exit
end
show vlan

conf t
interface vlan 10
ip address 192.168.1.1 255.255.255.0
no shutdown
  
```

```
exit
interface vlan 20
ip address 192.168.3.1 255.255.255.0
no shutdown
end
show ip route
show runing
```

```
conf t
router rip
network 192.168.1.0
network 192.168.3.0
version 2
end
show ip route
```

R1

```
en
conf t
hostname R1
interface fa 0/0
no shutdown
ip address 192.168.3.2 255.255.255.0
exit
interface serial 2/0
no shutdown
ip address 192.168.4.1 255.255.255.0
clock rate 64000
end
show ip route
```

```
conf t
router rip
network 192.168.3.0
network 192.168.4.0
version 2
exit
```

R2

```
en
conf t
hostname R2
interface fa 0/0
no shutdown
```

```
ip address 192.168.2.1 255.255.255.0
exit
interface serial 2/0
no shutdown
ip address 192.168.4.2 255.255.255.0
end
show ip route
conf t
router rip
network 192.168.2.0
network 192.168.4.0
version 2
end
```

PC1 Ping PC2

Ping 192.168.2.2 reply

实验十一：路由器 OSPF 动态路由配置

11.1 实验目的

掌握 OSPF 协议的配置方法；
掌握查看通过动态路由协议 OSPF 学习产生的路由；
熟悉广域网线缆的连接方式。

11.2 实验背景

假设校园网通过一台三层交换机连到校园网出口路由器上，路由器再和校园外的另一台路由器连接。现要做适当配置，实现校园网内部主机与校园网外部主机之间的相互通信。为了简化网管的管理维护工作，学校决定采用 OSPF 协议实现互通。

11.3 技术原理

OSPF 开放式最短路径优先协议，是目前网路中应用最广泛的路由协议之一。属于内部网管路由协议，能够适应各种规模的网络环境，是典型的链路状态协议。OSPF 路由协议通过向全网扩散本设备的链路状态信息，使网络中每台设备最终同步一个具有全网链路状态的数据库，然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

11.4 实验步骤

新建 packet tracer 拓扑图。

(1) 在本实验中的三层交换机上划分 VLAN10 和 VLAN20，其中 VLAN10 用于连接校园网主机，VLAN20 用于连接 R1。

(2) 路由器之间通过 V35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000。

(3) 主机和交换机通过直连线，主机与路由器通过交叉线连接。

(4) 在 S3560 上配置 OSPF 路由协议。

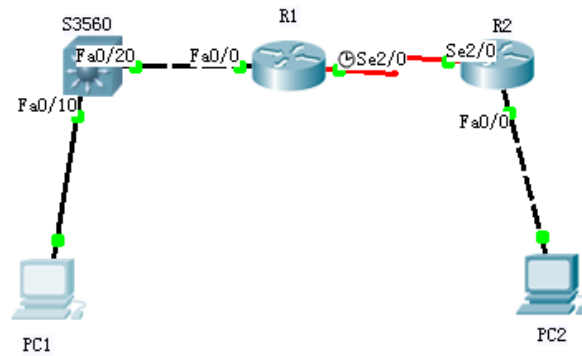
(5) 在路由器 R1、R2 上配置 OSPF 路由协议。

(6) 将 PC1、PC2 主机默认网关设置为与直连网路设备接口 IP 地址。

(7) 验证 PC1、PC2 主机之间可以互相通信。

11.5 实验设备及拓扑

PC 2 台；Switch-3560 1 台；Router-PT 2 台；直连线；交叉线；DCE 串口线



11.6 实验过程

PC1

IP: 192.168.1.2
 Submask: 255.255.255.0
 Gateway: 192.168.1.1

PC2

IP: 192.168.2.2
 Submask: 255.255.255.0
 Gateway: 192.168.2.1

S3560

```

en
conf t
hostname S3569
vlan 10
exit
vlan 20
interface fa 0/10
switchport access vlan 10
exit
int fa 0/20
switchport access valn 20
exit
interface valn 10
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
interface vlan 20
ip address 192.168.3.1 255.255.255.0
no shutdown
end
show ip route

```



```

conf t
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
end
show ip route

```

R1

```

en
conf t
hostname R1
interface fa 0/0
no shutdown
ip address 192.168.3.2 255.255.255.0
exit
interface serial 2/0
no shutdown
clock rate 64000
ip address 192.168.4.1 255.255.255.0
end
show ip route

```

```

conf t
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
end
show ip route

```

R2

```

en
conf t
hostname R2
interface fa 0/0
no shutdown
ip address 192.168.2.1 255.255.255.0
exit

```

```

interface serial 2/0
no shutdown
ip address 192.168.4.2 255.255.255.0
end
show ip route

```

```
conf t
router ospf 1
network 192.168.2.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
end
show ip route
```

实验十二：路由器综合路由配置

12.1 实验目标

掌握综合路由器的配置方法；
掌握查看通过路由重分布学习产生的路由；
熟悉广域网线缆的连接方式。

12.2 实验背景

假设某公司通过一台三层交换机连到公司出口路由器 R1 上，路由器 R1 再和公司外的另一台路由器 R2 连接。三层交换机与 R1 间运行 RIPV2 路由协议，R1 与 R2 间运行 OSPF 路由协议。现要做适当配置，实现公司内部主机与公司外部主机之间的相互通信。

12.3 技术原理

为了支持本设备能够运行多个路由协议进程，系统软件提供了路由信息从一个路由进程重分布到另一个路由进程的功能。比如你可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

要把路由从一个路由域分布到另一个路由域，并且进行控制路由重分布，在路由进程配置模式中执行以下命令：

```
redistribute protocol [metric metric] [metric-type metric-type] [match internal|external type|nssa-external type] [tag tag] [route-map route-map-name] [subnets]
```

12.4 实验步骤

新建 Packet Tracer 拓扑图

(1) PC 与交换机间用直连线连接；PC 与路由、路由与路由之间用交叉线连接。

(2) 在三层上划分 2 个 Vlan，运行 RIPV2 协议；R2 运行 OSPF 协议。

(3) 在路由器 R1 上左侧配置 RIPV2 路由协议；右侧配置 OSPF 协议。

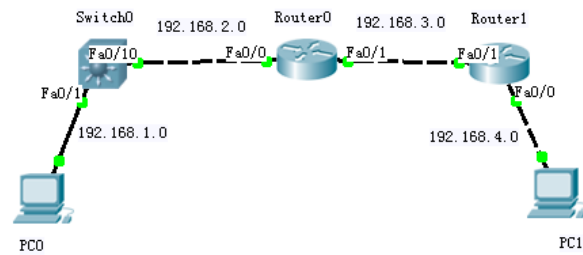
(4) 在 R1 路由进程中引入外部路由，进行路由重分布。

(5) 将 PC1、PC2 主机默认网关分别设置为与直接网络设备接口 IP 地址。

(6) 验证 PC1、PC2 主机之间可以互相通信；

12.5 实验设备及拓扑

Router-1841 2 台；Switch-3560 1 台；直通线；交叉线



12.6 实验过程

PC0

IP: 192.168.1.2
 Submask: 255.255.255.0
 Gageway: 192.168.1.1

PC1

IP: 192.168.4.2
 Submask: 255.255.255.0
 Gageway: 192.168.4.1

Switch0

```
en
conf t
vlan 2
exit
int fa 0/10
switchport access vlan 2
exit
int vlan 1
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
int vlan 2
ip address 192.168.2.1 225.255.255.0
no shutdown
end
show int vlan 1

conf t
router rip
network 192.168.1.0
network 192.168.2.0
version 2
```

Router0

```
en
conf t
host R1
```

```

inf fa 0/0
ip address 192.168.2.2 255.255.255.0
no shutdown
int fa 0/1
ip address 192.168.3.1 255.255.255.0
no shutdown
exit

router rip
network 192.168.2.0
version 2
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
Router1
en
conf t
host R2
int fa 0/1
ip address 192.168.3.2 255.255.255.0
no shutdown
int fa 0/0
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
end
show ip route
Router0
end
show ip route
show run
show ip route
ping 192.168.1.2 (success)
ping 192.168.4.2 (success)
PC0
ping 192.168.4.2 (Replay form 192.168.1.1: Destination host
unreachable)
Switch-3560
show ip rout (只有两条直连路由)
Router0
conf t
router rip

```

```
        redistribute ospf 1
        exit
        router ospf 1
        redistribute rip subnets
        end
Router1
    show ip route
PC0
    ping 192.168.4.2 (Replay form 192.168.4.2: bytes=32 time=125ms
TTL=125)
```

实验十三：标准 IP 访问控制列表配置

13.1 实验目标

理解标准 IP 访问控制列表的原理及功能；
掌握编号的标准 IP 访问控制列表的配置方法。

13.2 实验背景

你是公司的网络管理员，公司的经理部、财务部和销售部门分属于不同的 3 个网段，三部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部进行访问，但经理部可以对财务部进行访问。

PC1 代表经理部的主机、PC2 代表销售部的主机、PC3 代表财务部的主机。

13.3 技术原理

ACLs 的全称为接入控制列表 (Access Control Lists)，也称访问控制列表 (Access Lists)，俗称防火墙，在有的文档中还称包过滤。ACLs 通过定义一些规则对网络设备接口上的数据包文进行控制；允许通过或丢弃，从而提高网络可管理性和安全性；

IP ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表，编号范围为 1 ~ 99、1300 ~ 1999、100 ~ 199、2000 ~ 2699；

标准 IP 访问控制列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤；

扩展 IP 访问列表可以根据数据包的原 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤；

IP ACL 基于接口进行规则的应用，分为：入栈应用和出栈应用。

13.4 实验步骤

新建 Packet Tracer 拓扑图

(1) 路由器之间通过 V.35 电缆通过串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000；主机与路由器通过交叉线连接。

(2) 配置路由器接口 IP 地址。

(3) 在路由器上配置静态路由协议，让三台 PC 能够相互 Ping 通，因为只有互通的前提下才涉及到访问控制列表。

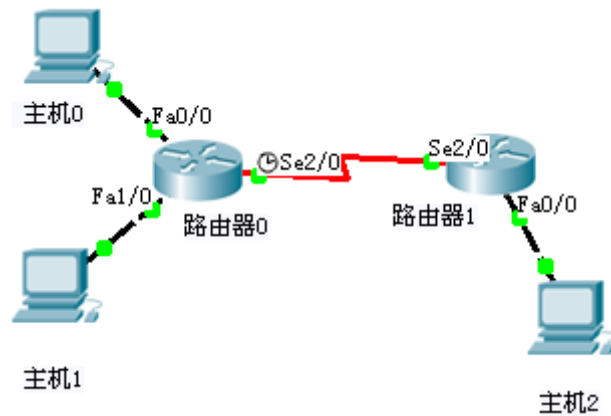
(4) 在 R1 上编号的 IP 标准访问控制

(5) 将标准 IP 访问控制应用到接口上。

(6) 验证主机之间的互通性。

13.5 实验设备及拓扑

PC 3 台；Router-PT 2 台；交叉线；DCE 串口线；



13.6 实验过程

PC0

IP: 172.16.1.2
 Submask: 255.255.255.0
 Gateway: 172.16.1.1

PC1

IP: 172.16.2.2
 Submask: 255.255.255.0
 Gateway: 172.16.2.1

PC2

IP: 172.16.4.2
 Submask: 255.255.255.0
 Gateway: 172.16.4.1

Router0

```

en
conf t
host R0
int fa 0/0
ip address 172.16.1.1 255.255.255.0
no shutdown
int fa 1/0
ip address 172.16.2.1 255.255.255.0
no shutdown
int s 2/0
ip address 172.16.3.1 255.255.255.0
no shutdown
clock rate 64000
  
```

Router1

```

en
conf t
host R1
  
```



```

    int s 2/0
    ip address 172.16.3.2 255.255.255.0
    no shutdown
    int fa 0/0
    ip address 172.16.4.1 255.255.255.0
    no shutdown
Router0
    exit
    ip route 172.16.4.0 255.255.255.0 172.16.3.2
Router1
    exit
    ip route 0.0.0.0 0.0.0.0 172.16.3.1
    end
    show ip route
PC0
    ping 172.16.4.2 (success)
PC1
    ping 172.16.4.2 (success)
Router0
    ip access-list standard 5ijsj
    permit 172.16.1.0 0.0.0.255
    deny 172.16.2.0 0.0.0.255 (如果有上面的 permit 默认跟一个 deny,
所以此命令可不写)
    conf t
    int s 2/0
    ip access-group 5ijsj out
    end
PC0
    ping 172.16.4.2 (success)
PC1
    ping 172.16.4.2 (Replay from 172.16.2.1: Destination host
unreachable)

```

实验十四：网络地址转换 NAT 配置

14.1 实验目标

理解 NAT 网络地址转换的原理及功能；
掌握静态 NAT 的配置，实现局域网访问互联网。

14.2 实验背景

你是某公司的网络管理员，欲发布公司的 WWW 服务。现要求将内网 Web 服务器 IP 地址映射为全局 IP 地址，实现外部网络可以访问公司内部 Web 服务器。

14.3 技术原理

网络地址转换 NAT (Network Address Translation)，被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

默认情况下，内部 IP 地址是无法被路由到外网的，内部主机 10.1.1.1 要与外部 Internet 通信，IP 包到达 NAT 路由器时，IP 包头的源地址 10.1.1.1 被替换成一个合法的外网 IP，并在 NAT 转发表中保存这条记录。当外部主机发送一个应答到内网时，NAT 路由器受到后，查看当前 NAT 转换表，用 10.1.1.1 替换掉这个外网地址。

NAT 将网络划分为内部网络和外部网络两部分，局域网主机利用 NAT 访问网络时，是将局域网内部的本地地址转换为全局地址（互联网合法的 IP 地址）后转发数据包；

NAT 分为两种类型：NAT（网络地址转换）和 NAPT（网络端口地址转换 IP 地址对应一个全局地址）。

静态 NAT：实现内部地址与外部地址一对一的映射。现实中，一般都用于服务器；

动态 NAT：定义一个地址池，自动映射，也是一对一的。现实中，用得比较少；

NAPT：使用不同的端口来映射多个内网 IP 地址到一个指定的外网 IP 地址，多对一。

14.4 实验步骤

新建 Packet Tracer 拓扑图

(1) R1 为公司出口路由器，其与外部路由器之间通过 V.35 电缆串口连接，DCE 端连接在 R1 上，配置其时钟频率 64000；

(2) 配置 PC 机、服务器及路由器接口 IP 地址；

(3) 在各路由器上配置静态路由协议，让 PC 间能相互 Ping 通；

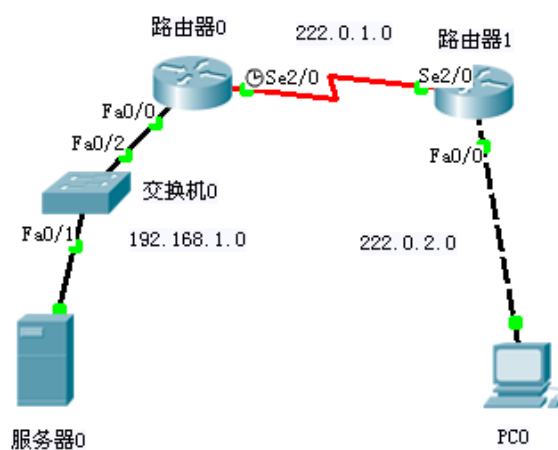
(4) 在 R1 上配置静态 NAT。

(5) 在 R1 上定义内外网络接口。

(6) 验证主机之间的互通性。

14.5 实验设备

PC 1 台； Server-PT 1 台； Switch-2950-24 1 台； Router-PT 2 台； 直连线； 交叉线； DCE 串口线。



14.6 实验设备

Server-PT

192.168.1.2
255.255.255.0
192.168.1.1

PC0

222.0.2.2
255.255.255.0
222.0.2.1

Router0

```
en
conf t
host R0
int fa 0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
int s 2/0
ip address 222.0.1.1 255.255.255.0
no shutdown
clock rate 64000
```

Router1

```
en
conf t
host R1
int s 2/0
ip address 222.0.1.2 255.255.255.0
```

```

no shut
int fa 0/0
ip address 222.0.2.1 255.255.255.0
no shutdown
Router0
exit;
ip route 222.0.2.0 255.255.255.0 222.0.1.2
Router1
exit
ip route 192.168.1.0 255.255.255.0 222.0.1.1
end
show ip route
PC0
CMD
ping 192.168.1.2 (success)
Web 浏览器
http://192.168.1.2 (success)
Router0
int fa 0/0
ip nat inside
int s 2/0
ip nat outside
exit
ip nat inside source static 192.168.1.2 222.0.1.3
end
show ip nat translations
PC0
Web 浏览器
http://222.0.1.3 (success)
Router0
show ip nat translations

```

实验十五：IP 分析实验

15.1 实验目的

熟悉 IP 的报文格式以及关键字段的含义；
掌握 IP 地址的分配方法；
理解路由器转发 IP 数据报的流程。

15.2 技术原理

(1) 什么是 IP 协议

IP 是英文 Internet Protocol（网际互连协议）的缩写，是 TCP/IP 体系中的网络层协议，目前常用的版本是 IPv4。设计 IP 协议的目的是提高网络的可扩展性：一是解决互联网问题，实现大规模、异构网络的互联互通；二是分割顶层网络应用和底层网络技术之间的耦合关系，以利于两者的独立发展。根据端到端的设计原则，IP 协议只为主机提供一种无连接、不可靠的、尽力而为的数据报传输服务。为了能适应异构网络，IP 强调适应性、简洁和可操作性，并在可靠性做了一定的牺牲。IP 不保证分组的交付时限和可靠性，所传送分组有可能出现丢失、重复、延迟或乱序等问题。IP 协议主要包含三方面内容：IP 编址方案、分组封装格式以及分组转发规则。

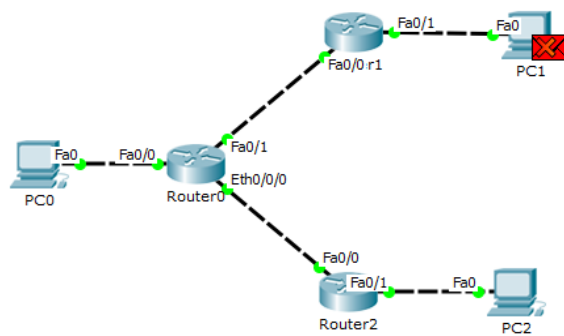
(2) IP 分组的转发规则

路由器仅根据网络地址进行转发。当 IP 数据包经由路由器转发时，如果目标网络与本路由器直接相连，则直接将数据包交付给目标主机，这称为直接交付；否则，路由器通过路由表查找路由信息，并将数据包转交给指明的下一跳路由器，这称为间接交付。路由器在间接交付中，若路由表中有到达目标网络的路由，则把数据报传送给路由表指明的下一跳路由器；如果没有路由，但路由表中有一个默认路由，则把数据报传送给指明的默认路由器；如果两者都没有，则丢弃数据包并报告错误。

(3) 什么是 IP 分片

一个 IP 包从源主机传输到目的主机可能需要经过多个不同的网络。由于各种物理网络的链路层都有一个最大传输单元 MTU 的限制，例如，以太网的 MTU 是 1500；因此，当路由器在转发 IP 包时，如果数据报的大小超过了出口链路的最大传输单元时，则会将该 IP 分组分解成很多足够小的片段，以便能够在目标链路上进行传输。这些 IP 分片重新封装一个 IP 包独立传输，并在到达目的主机时才会被重组起来。

15.3 实验拓扑



15.4 实验步骤

任务一：观察路由表

步骤 1：观察 Router0 的路由表

步骤 2：观察 Router1 的路由表

步骤 3：观察 Router2 的路由表

任务二：观察数据包的封装格式以及 TTL 字段的变化

步骤 1：初始化所有设备的 ARP 表信息

步骤 2：观察 IP 数据报的转发

任务三：观察路由器转发 IP 数据报的方式

步骤 1：初始化并观察各路由器的路由表

步骤 2：观察 PC0 到 PC2 的往返过程

步骤 3：观察 PC2 到 PC1 的往返过程

任务四：观察 IP 分片原理

步骤 1：产生需要分片的数据报

步骤 2：观察 IP 数据报的分片情况

任务一：观察数据包的封装以及字段变化

步骤 1：初始化所有设备的 ARP 表信息

步骤 2：观察 IP 数据报的转发

PDU Information at Device: Router0

OSI Model
Inbound PDU Details
Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0050.0F73.2D01		SRC MAC: 0001.9627.AD9B	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 28			
ID: 0x8		0x0		0x0		
TTL: 255		PRO: 0x1		CHKSUM		
SRC IP: 10.1.1.1						
DST IP: 10.1.3.1						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8		CODE: 0x0		CHECKSUM
ID: 0x9		SEQ NUMBER: 8		

PDU Information at Device: Router0

OSI Model
Inbound PDU Details
Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0001.96A5.8501		SRC MAC: 0001.9740.884A	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 28			
ID: 0x8		0x0		0x0		
TTL: 254		PRO: 0x1		CHKSUM		
SRC IP: 10.1.1.1						
DST IP: 10.1.3.1						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8		CODE: 0x0		CHECKSUM
ID: 0x9		SEQ NUMBER: 8		

任务二：观察路由器转发 IP 数据报的方式

步骤 1：初始化并观察各路由器的路由表

删除所有场景，打开 Router0、Router1 和 Router2 的路由表并比较三个路由表。

Routing Table for Router0				
Type	Network	Port	Next Hop IP	Metric
S	0.0.0.0/0	---	192.168.2.2	1/0
C	10.1.1.0/24	FastEthernet0/0	---	0/0
S	10.1.2.0/24	---	192.168.1.2	1/0
C	192.168.1.0/24	FastEthernet0/1	---	0/0
C	192.168.2.0/24	Ethernet0/0/0	---	0/0

Routing Table for Router1				
Type	Network	Port	Next Hop IP	Metric
S	10.1.1.0/24	---	192.168.1.1	1/0
C	10.1.2.0/24	FastEthernet0/1	---	0/0
C	192.168.1.0/24	FastEthernet0/0	---	0/0

Routing Table for Router2				
Type	Network	Port	Next Hop IP	Metric
S	10.1.1.1/32	---	192.168.2.1	1/0
S	10.1.2.0/24	---	192.168.2.1	1/0
C	10.1.3.0/24	FastEthernet0/1	---	0/0
C	192.168.2.0/24	FastEthernet0/0	---	0/0

步骤 2: 观察 PC0 到 PC2 的往返过程

单击 Add Simple PDU 按钮，然后分别单击 PC0 和 PC2。单击 Capture/Forward 按钮传送数据包。分别检查在 At Device （在设备）显示为 Router0 和 Router2 的数据包信息。在 Out Layers 中选择第三层。

PDU Information at Device: Router2

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: Router2 Source: PC0 Destination: PC2		
In Layers	Out Layers	
Layer7	Layer7	
Layer6	Layer6	
Layer5	Layer5	
Layer4	Layer4	
Layer3: IP Header Src. IP: 10.1.1.1, Dest. IP: 10.1.3.1 ICMP Message Type: 8	Layer3: IP Header Src. IP: 10.1.1.1, Dest. IP: 10.1.3.1 ICMP Message Type: 8	
Layer2: Ethernet II Header 0001.9740.884A >> 0001.96A5.8501	Layer2: Ethernet II Header 0001.96A5.8502 >> 0000.0CDC.6176	
Layer1: Port FastEthernet0/0	Layer1: Port(s): FastEthernet0/1	

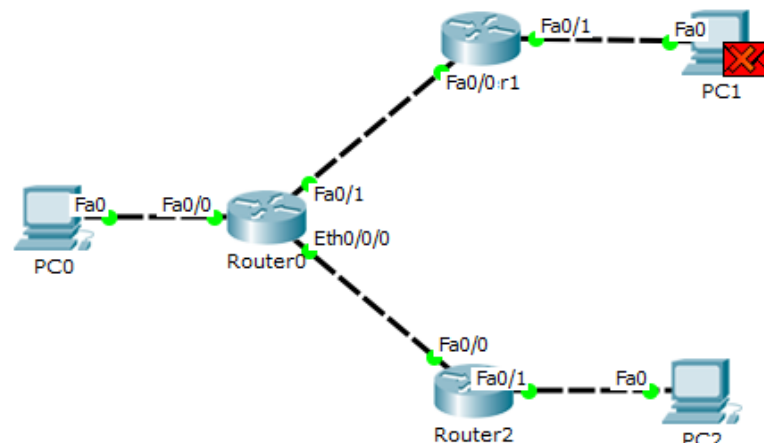
1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.

PDU Information at Device: Router0

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: Router0 Source: PC0 Destination: PC2		
In Layers	Out Layers	
Layer7	Layer7	
Layer6	Layer6	
Layer5	Layer5	
Layer4	Layer4	
Layer3: IP Header Src. IP: 10.1.1.1, Dest. IP: 10.1.3.1 ICMP Message Type: 8	Layer3: IP Header Src. IP: 10.1.1.1, Dest. IP: 10.1.3.1 ICMP Message Type: 8	
Layer2: Ethernet II Header 0001.9627.AD9B >> 0050.0F73.2D01	Layer2: Ethernet II Header 0001.9740.884A >> 0001.96A5.8501	
Layer1: Port FastEthernet0/0	Layer1: Port(s): Ethernet0/0/0	

1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.

步骤 3: 观察 PC2 到 PC1 的往返过程



任务三：观察 IP 分片原理

步骤 1:

Create Complex PDU

Source Settings

Source Device: PC0
Outgoing Port:
FastEthernet0 ☐ Auto Select Port

PDU Settings

Select Application: PING
Destination IP Address: 10.1.3.1
Source IP Address:
TTL: 32
TOS: 0
Sequence Number: 1
Size: 1500

Simulation Settings

☒ One Shot Time: 2 Seconds
☐ Periodic Interval: Seconds

Create PDU

步骤 2：观察 IP 数据包分片情况

PDU Information at Device: PC0

OSI Model

Outbound PDU Details

At Device: PC0
Source: PC0
Destination: 10.1.3.1

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3: IP Header Src. IP: 10.1.1.1, Dest. IP: 10.1.3.1
Layer2: Ethernet II Header 0001.9627.AD9B >> 0050.0F73.2D01
Layer 1: Port(s): FastEthernet0

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The device sets TTL in the packet header.
5. The destination IP address is not in the same subnet and is not the broadcast address.
6. The default gateway is set. The device sets the next-hop to default gateway.
7. Total length of the packet (1528 bytes) is greater than the IP MTU (1500 bytes). This datagram is fragmented.
8. The device sends an IP fragment with the FO 0, a payload length 1480 bytes, and a total length 1500 bytes.

Challenge Me << Previous Layer Next Layer >>

PDU Information at Device: PC0

OSI Model

Outbound PDU Details

At Device: PC0
Source: PC0
Destination: 10.1.3.1

In Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3: IP Header Src. IP: 10.1.1.1, Dest. IP: 10.1.3.1 ICMP Message Type: 8
Layer2: Ethernet II Header 0001.9627.AD9B >> 0050.0F73.2D01
Layer 1: Port(s):

1. The device sends an IP fragment with the FO 1480, a payload length 28 bytes, and a total length 48 bytes.

Challenge Me << Previous Layer Next Layer >>

15.5 思考题

- (1) 一个 IP 分组经路由器转发后，有哪些字段会发生变化？
- (2) TTL 会发生改变，源 MAC 地址和目的 MAC 地址
- (3) 为什么任务 3 中的两个分片的长度分别是 1500 和 48？
- (4) 因为发送的包的大小是 1500，封装它的 IP 数据报超出了以太网帧的负载上限，因此该 IP 报文被分拆为两个 ID 一样的分片，一个长度为 1500 字节，另一个为 48 字节。

55

实验十六：IPv6 RIPng 动态路由配置

16.1 实验目标

掌握 IPv6 RIPng 动态路由的基本原理；
学会配置 IPv6 RIPng 的基本方法。

16.2 技术原理

RIPng 与 RIPv2 类似，路由器在查询响应、周期更新、触发更新三种情况下会收到响应报文，接收报文的路由器根据响应报文判断是否对本地路由表进行更新。

基于距离矢量算法的路由协议会产生慢收敛和无限计数的问题而引发了路由的不一致。RIPng 使用与 RIPv2 类似的水平分割技术、毒性逆转技术、触发更新技术来解决这些问题，同时抑制广播风暴，减少路由信息数量。

RIPng 协议报文格式

RIPng 是基于 UDP 的协议，并且使用端口号 521 发送和接收数据报。RIPng 报文大致可分为两类：选路信息报文和用于请求信息的报文。

RIPng 中仍然使用固定的度量方式，即跳数，RIPng 的最大工作直径为 15 跳，16 即意味着目的地不可达。与 RIPv2 不同的是，RIPng 的下一跳字段是由一个单独的 RTE 指定的。

RIPng 和 RIPv1、RIPv2 的区别：

根据上面的介绍，应该看到 RIPng 的目标并不是创造一个全新的协议，而是对 RIP 进行必要的改造以使其适应 IPv6 的选路要求，因此 RIPng 的基本工作原理同 RIP 是一样的，其主要的变化在地址和报文格式方面，RIPng 与 RIPv1、RIPv2 的主要区别有以下几点：

(1) 地址版本。RIPv1、RIPv2 基于 IPv4，地址域只有 32bit，而 RIPng 基于 IPv6，使用的所有地址均为 128bit。

(2) 子网掩码和前缀长度。IPv6 的地址前缀有明确的含义，因此 RIPng 中不再有子网掩码的概念，取而代之的是前缀长度。同样也是由于使用了 IPv6 地址，RIPng 中也没有必要再区分网络路由、子网路由和主机路由。

(3) 对下一跳的表示。RIPv1 中没有下一跳的信息，接收端路由器把报文的源 IP 地址作为到目的网络路由的下一跳。RIPv2 中明确包含了下一跳信息，便于选择最优路由和防止出现选路环路及慢收敛。与 RIPv2 不同，为防止 RTE 过长，同时也是为了提高路由信息的传输效率，RIPng 中的下一跳字段是作为一个单独的 RTE 存在的。

(4) 报文长度。RIPv1、RIPv2 中对报文的长度均有限制，规定每个报文最多只能携带 25 个 RTE。而 RIPng 对报文长度、RTE 的数目都不作规定，报文的长度是由介质的 MTU 决定的。RIPng 对报文长度的处理，提高了网络对路由信息的传输效率。

(5) RIPng 使用 IPv6 的多播地址 FF02::9 收发路由更新报文。

16.3 实验拓扑

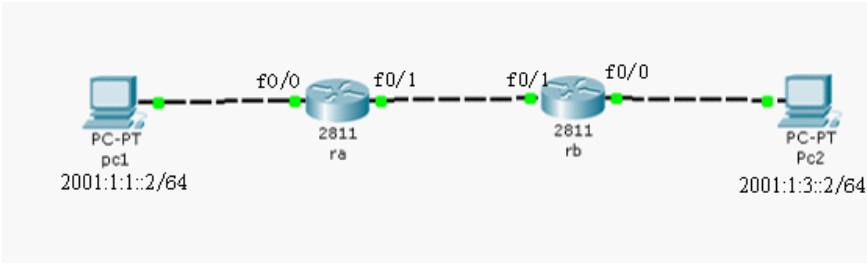


图 16-1 拓扑结构

16.4 IPv6 地址规划

表 16-1 IPv6 地址规划

PC1	2001: 1: 1: : 2/64	Rb f0/1	2001: 1: 2: : 2/64
Ra f0/0	2001: 1: 1: : 1/64	Rb f0/0	2001: 1: 3: : 1/64
Ra f0/1	2001: 1: 2: : 1/64	Pc2	2001: 1: 3: : 2/64

16.5 配置过程

(1) 步骤 1: 配置 PC 机的 IPv6 地址及默认网关

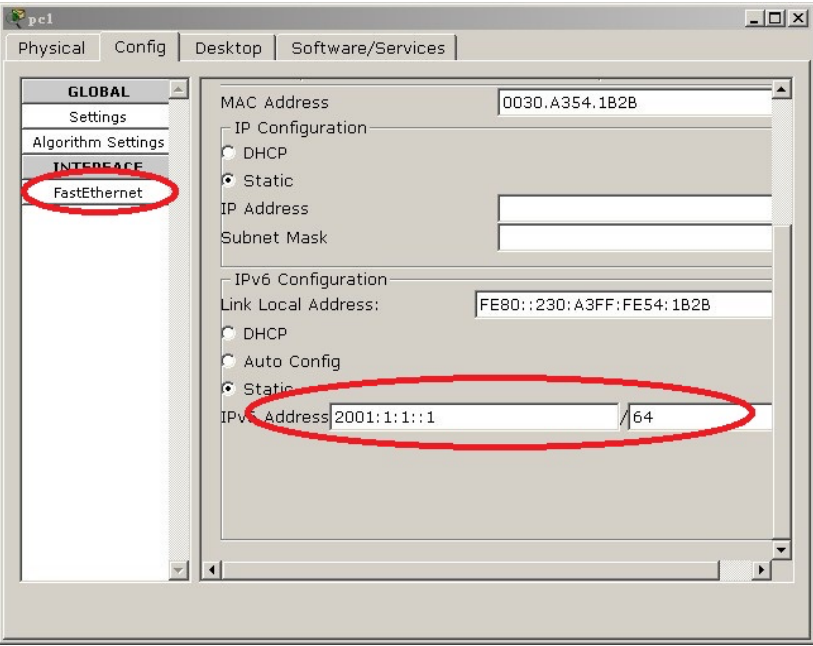


图 16-2 配置 IPv6 地址

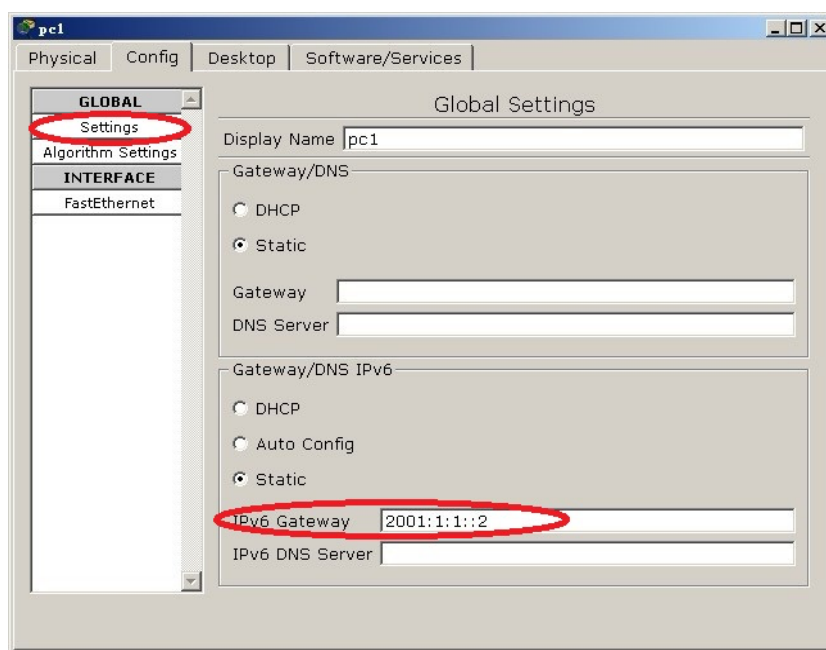


图 16-3 配置默认网关

(2) 步骤 2: 配置路由器 Ra

```
R1 (config)#ipv6 unicast-routing //启用 IPV6 单播服务
R1 (config)#ipv6 router rip 1 //启动 IPv6 RIPng 进程
R1 (config)#interface f0/0
R1 (config-if)#ipv6 address 2001:1:1::2/64
R1 (config-if)#ipv6 rip 1 enable //在接口上启用 RIPng
R1 (config-if)#no shutdown
R1 (config)#interface f0/1
R1 (config-if)#ipv6 address 2001:1:2::1/64
R1 (config-if)#ipv6 rip 1 enable
R1 (config-if)#no shutdown
```

(3) 步骤 3: 配置路由器 Rb

```
R2 (config)#ipv6 unicast-routing
R2 (config)#ipv6 router rip 1
R2 (config)#interface f0/0
R2 (config-if)#ipv6 address 2001:1:3::1/64
R2 (config-if)#ipv6 rip 1 enable
R2 (config-if)#no shutdown
R2 (config)#interface f0/1
R2 (config-if)#ipv6 address 2001:1:2::2/64
R2 (config-if)#ipv6 rip 1 enable
R2 (config-if)#no shutdown
```

(4) 步骤 4: 测试及抓包过程

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.001	rb	Pc2	ICMPv6	
	0.001	--	ra	ICMPv6	
	0.002	--	Pc2	ICMPv6	
	0.002	rb	ra	ICMPv6	
	0.002	--	Pc2	ICMPv6	
	0.002	--	Pc2	ICMPv6	
	0.002	rb	Pc2	ICMPv6	
	0.002	ra	pc1	ICMPv6	
	0.002	--	Pc2	ICMPv6	
	0.002	Pc2	rb	ICMPv6	

图 16-4 路由器使用 icmp 协议请求逻辑地址和物理地址

Vis.	Time (sec)	Last Device	At Device	Type	Info
	11.006	rb	Pc2	ICMPv6	
	13.017	--	ra	RIPv2	
	13.017	--	ra	RIPv2	
	13.018	ra	rb	RIPv2	
	13.018	ra	pc1	RIPv2	
	15.185	--	rb	RIPv2	
	15.185	--	rb	RIPv2	
	15.186	rb	ra	RIPv2	
	15.186	rb	Pc2	RIPv2	
	42.051	--	ra	RIPv2	

图 16-5 路由器使用 RIP 协议通信

(5) 步骤 5: 查看路由表

```

Ra#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
C   2001:1:1::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:1:1::1/128 [0/0]
    via ::, FastEthernet0/0
C   2001:1:2::/64 [0/0]
    via ::, FastEthernet0/1
L   2001:1:2::1/128 [0/0]
    via ::, FastEthernet0/1
R   2001:1:3::/64 [120/2]
    via FE80::200:CFF:FE71:C702, FastEthernet0/1
L   FF00::/8 [0/0]
    via ::, Null0

```

图 16-6 RA 路由表

```

Rb#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
R   2001:1:1::/64 [120/2]
    via FE80::201:63FF:FEA1:2402, FastEthernet0/1
C   2001:1:2::/64 [0/0]
    via ::, FastEthernet0/1
L   2001:1:2::2/128 [0/0]
    via ::, FastEthernet0/1
C   2001:1:3::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:1:3::1/128 [0/0]
    via ::, FastEthernet0/0
L   FF00::/8 [0/0]
    via ::, Null0

```

图 16-7 RB 路由表

实验十七：应用层及传输层协议（DNS、UDP、TCP、HTTP、FTP）分析

17.1 实验目的

通过本实验，熟悉 PacketTracer 的使用，学习在 PacketTracer 中仿真分析应用层和传输层协议，进一步加深对协议工作过程的理解。

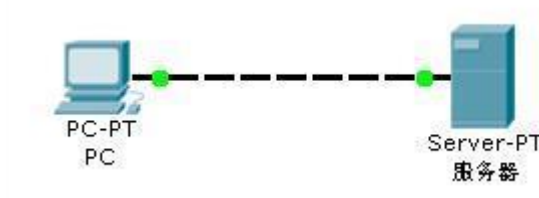
17.2 实验内容

任务 1：从 PC 使用 URL 捕获 Web 请求。

任务 2：从 PC 访问服务器的 HTTPS 服务，捕获数据包并分析。

任务 3：从 PC 访问服务器的 FTP 服务，捕获数据包并分析。

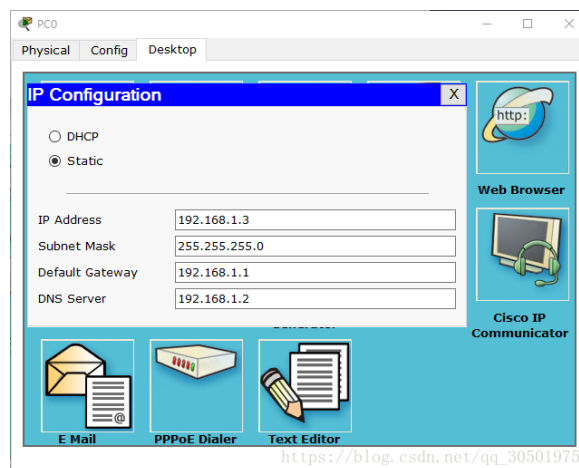
17.3 实验拓扑



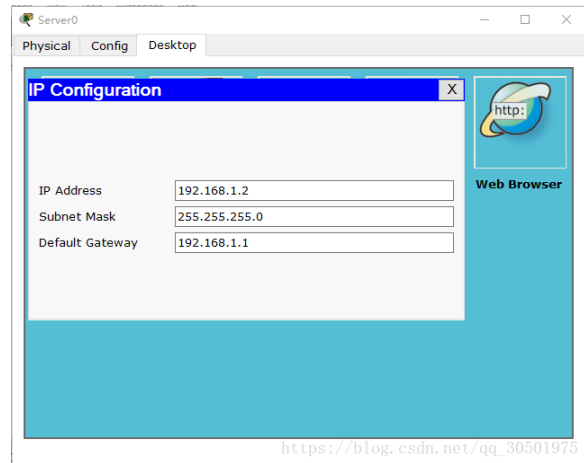
17.4 实验步骤

(1) 建立上述简单拓扑，并配置相关参数。

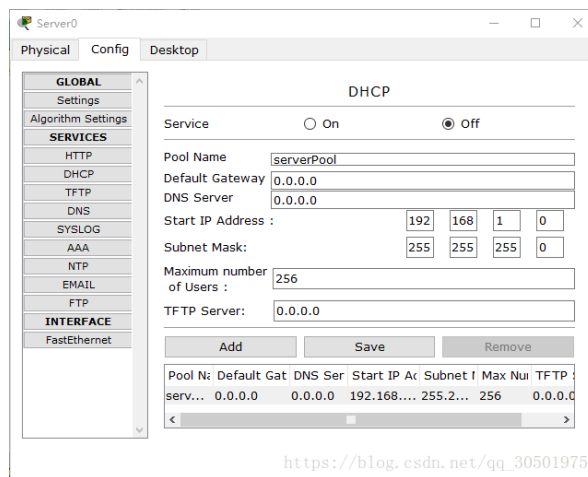
PC0:



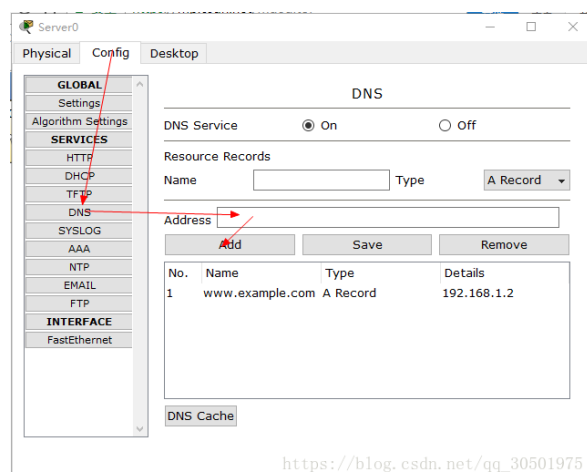
Server: 设置其 IP、DHCP 和 DNS 解析



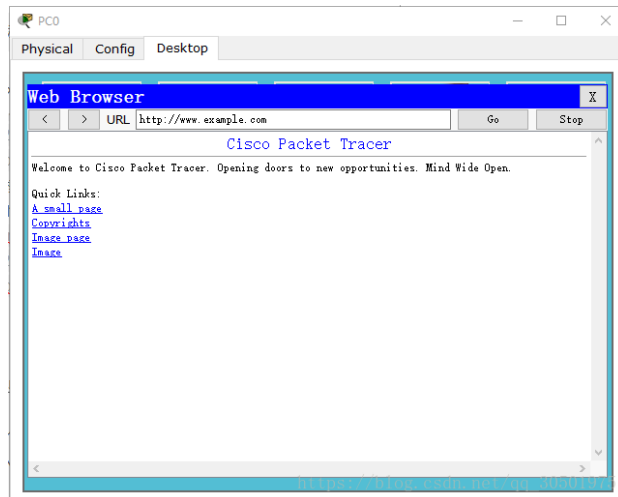
配置 DHCP, 将 Service 设置为 OFF, 使用静态分配 IP:



配置 DNS, 增加解析域名 www.example.com:



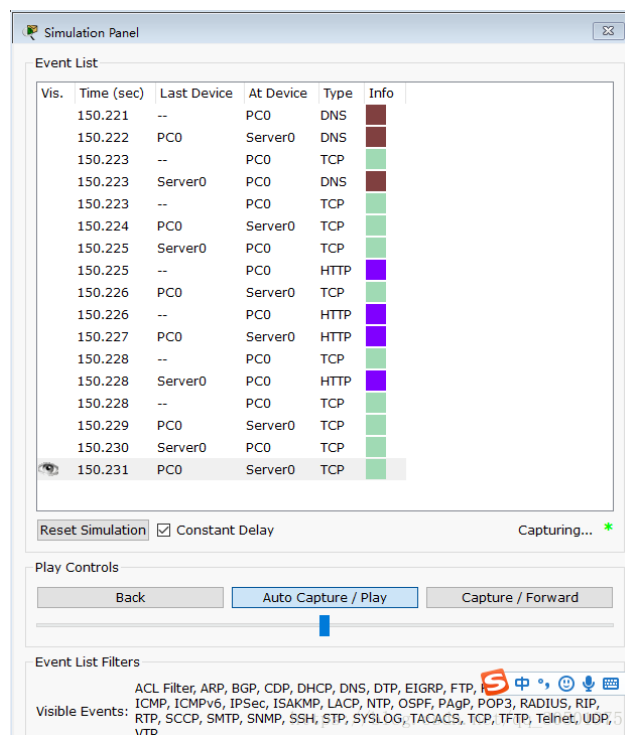
(3) 打开模拟模式, 单击主机, 进入 web browser, 输入 url, 点击 go:



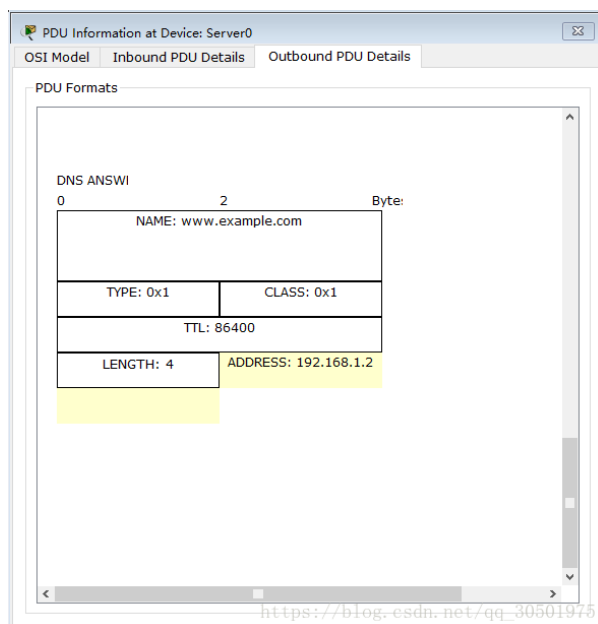
Event List 显示出刚抓的 DNS 包

Event List (事件列表) 中将会显示两个数据包：将 URL 解析为服务器 IP 地址所需的 DNS 请求，以及将服务器 IP 地址解析为其硬件 MAC 地址所需的 ARP 请求。

单击 Auto Capture/Play (自动捕获/播放) 按钮自动模拟和捕获事件。在拓扑图中可以动态看到 web 请求的模拟过程 (点击 show all 可以重新展示整个过程)：



点击第二个 DNS，可以看到返回了 IP 地址 192.168.1.2



对 DNS 协议的分析:

首先根据 www.example.com 的 URL 地址, 然后查询到了 IP 地址为 192.168.0.1 的目的地址, 将 URL 解析为服务器 IP 地址所需的 DNS 请求, 以及将服务器 IP 地址解析为其硬件 MAC 地址所需的 ARP 请求。

DNS 报文类型	源站点	目的站点	报文信息
DNS 请求报文	192.168.0.2	192.168.0.1	请求www.example.com的IP地址
DNS 应答报文	192.168.0.1	192.168.0.2	对192.168.0.1请求的回复, 将IP地址给它

其中在 TCP 协议中, 在开始建立连接阶段, 经历了 3 次握手; 在断开连接阶段, 经历了四次挥手。

Vis.	Time (sec)	Last Device	At Device	Type	Info
150.219	Server0	PC0	ARP		
150.219	--	PC0	DNS		
150.220	PC0	Server0	DNS		
150.221	--	PC0	TCP		
150.221	Server0	PC0	DNS		
150.221	--	PC0	TCP		
150.222	PC0	Server0	TCP		
150.223	Server0	PC0	TCP		
150.223	--	PC0	HTTP		
150.224	PC0	Server0	TCP		
150.224	--	PC0	HTTP		
150.225	PC0	Server0	HTTP		
150.226	--	PC0	TCP		
150.226	Server0	PC0	HTTP		
150.226	--	PC0	TCP		
150.227	PC0	Server0	TCP		
150.228	Server0	PC0	TCP		
150.229	PC0	Server0	TCP		

三次握手

四次挥手

Reset Simulation ☒ Constant Delay

Captured to: * 11868.258 s

Play Controls

Back Auto Capture / Play Capture / Forward

再打开一个 HTTP 请求: 可以看到请求的对象是一个图片。

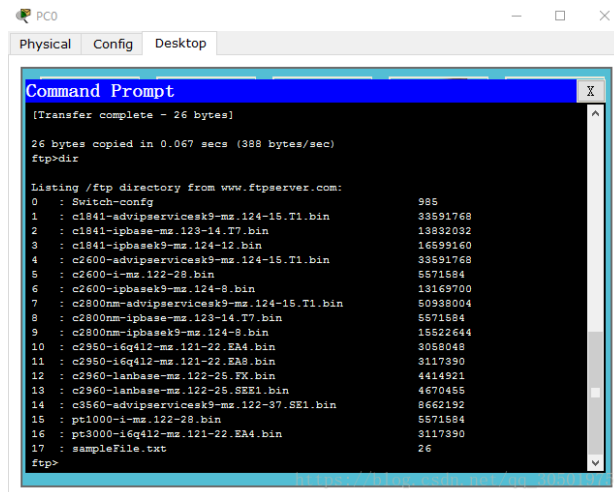
打开文件传送协议分析.pka。

点击 PC0, 打开 command prompt。

首先连接 FTP 服务器, 输入: ftp www.ftpserver.com。

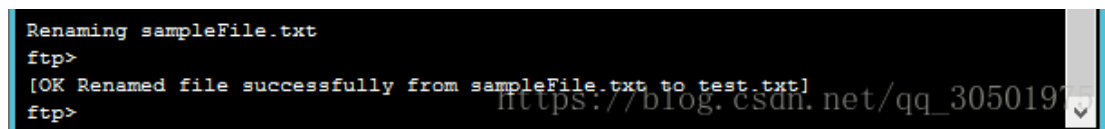
然后输入用户名: cisco, 密码: cisco, 进入 FTP prompt 界面。

获取服务器端全部文件列表: 在 command prompt 里面输入 dir, 可以看到服务器中所有文件的文件列表:



```
PC0
Physical Config Desktop
Command Prompt
[Transfer complete - 26 bytes]
26 bytes copied in 0.067 secs (388 bytes/sec)
ftp>dir
Listing /ftp directory from www.ftpserver.com:
0 : Switch-config 986
1 : c1841-advipservicesk9-ms.124-15.T1.bin 38591768
2 : c1841-ipbase-ms.123-14.T7.bin 13832032
3 : c1841-ipbasek9-ms.124-12.bin 16599160
4 : c2600-advipservicesk9-ms.124-15.T1.bin 33591768
5 : c2600-i-ms.122-28.bin 5571584
6 : c2600-ipbasek9-ms.124-8.bin 13169700
7 : c2800nm-advipservicesk9-ms.124-15.T1.bin 50938004
8 : c2800nm-ipbase-ms.123-14.T7.bin 5571584
9 : c2800nm-ipbasek9-ms.124-8.bin 15522644
10 : c2950-16q412-ms.121-22.EA4.bin 3058048
11 : c2950-16q412-ms.121-22.EA8.bin 3117390
12 : c2960-lanbase-ms.122-26.TX.bin 4414921
13 : c2960-lanbase-ms.122-26.SXE1.bin 4670455
14 : c3560-advipservicesk9-ms.122-37.SE1.bin 8662192
15 : pt1000-i-ms.122-28.bin 5571584
16 : pt3000-16q412-ms.121-22.EA4.bin 3117390
17 : sampleFile.txt 26
ftp>
```

测试重命名功能, 在 FTP prompt 输入: rename 例如这里我把 sampleFile.txt 文件重命名为: test.txt.



```
Renaming sampleFile.txt
ftp>
[OK Renamed file successfully from sampleFile.txt to test.txt]
ftp>
```

显示修改成功。

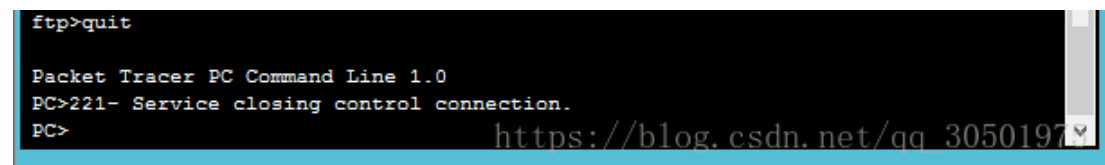
测试删除功能, 在 FTP prompt 输入: delete test.txt



```
ftp>delete test.txt
Deleting file test.txt from www.ftpserver.com: ftp>
[Deleted file test.txt successfully ]
ftp>
```

显示删除成功。

测试 FTP QUIT:



```
ftp>quit
Packet Tracer PC Command Line 1.0
PC>221- Service closing control connection.
PC>
```

成功退出 FTP, 回到 PC 界面。

总结: 完整一次传输过程包含四个 FTP。

连接并登陆 FTP 服务器的整个过程如下:

首先 PC0 输入 ftp www.ftpserver.com 发起连接; 收到服务器回复后;
紧接着输入账号: PC0 发出一个包含账号的 FTP 数据包;
然后服务器收到后, 发出一个账号已收到, 需要密码的 ftp 包;
收到后, PC0 再发出包含密码的 FTP 数据包;
服务器回复包含登陆成功的 FTP 数据包。