同濟大學
TONGJI UNIVERSITY

# 《计算机网络实验》实验报告

| | |
|---|---|
| 课　程 | 计算机网络实验 |
| 课　号 | 42014706 |
| 姓　名 | 林继申 |
| 学　号 | 2250758 |
| 学　院 | 软件学院 |
| 专　业 | 软件工程 |
| 教　师 | 陈伟超 |

二〇二四 年 五 月 二十四 日

# 目录

实验 01：网络相关进程与服务实验 ..... 2
实验 02：网络端口地址实验 ..... 9
实验 03：网络线的制作和测试实验 ..... 15
实验 04：基本网络测试工具及应用工具实验 ..... 19
实验 05：主机路由实验 ..... 36
实验 06：异步串口通信电缆制作实验 ..... 43
实验 07：异步串口通信收发实验 ..... 47
实验 08：IOS 的基本操作（路由器的基本操作）实验 ..... 54
实验 09：VLAN 配置实验 ..... 60
实验 10：静态路由配置实验 ..... 64
实验 11：蓝牙通信实验 ..... 75
实验 12：局域网（以太网）实验 ..... 82
实验 13：RIP 路由配置实验 ..... 90
实验 14：NAT 网络地址转换实验 ..... 109
实验 15：帧中继（Frame Relay）配置实验 ..... 121
实验 16：ACL 访问控制实验 ..... 139
实验 17：OSPF 动态网络路由配置实验 ..... 151
实验 18：动态 IP 地址分配 DHCP 实验 ..... 163
实验 19：无线网络组网实验 ..... 176
实验 20：IP 电话实验 ..... 195
实验 21：以太网帧分析实验 ..... 209
实验 22：IP 数据包分析实验 ..... 235
实验 23：ARP 消息分析实验 ..... 247
实验 24：TCP 数据分析实验 ..... 259
实验 25：UDP 数据包分析实验 ..... 277
实验 26：DNS 实验 ..... 291
实验 27：组网技术实验 ..... 311

# 实验 01：网络相关进程与服务实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/02/29 |

**【实验目的】**

1. 理解操作系统中的进程管理：通过本实验，学习和理解 Windows 操作系统中任务管理器的功能和用途，包括进程管理、应用程序管理、服务管理及网络进程的监控。
2. 掌握任务管理器的使用：学会使用 Windows 任务管理器监控计算机的性能，包括 CPU 和内存使用情况，以及进程和应用程序的管理。
3. 学习进程管理命令：通过实际操作，掌握使用 tasklist、taskkill 和 tskill 命令对进程进行查看和管理的方法。
4. 了解网络进程的特点：通过实验，认识到网络进程与一般进程的区别，特别是在传输层开启端口号的特性，以及如何查看正在使用的端口号。
5. 熟悉 Windows 服务的管理：通过使用 services.msc 命令，了解 Windows 系统服务的管理界面，学习如何查看和管理操作系统中运行的服务。

**【实验原理】**

**一、Windows 任务管理进程**

Windows 任务管理器为用户提供了一种方便的方式来监控和管理正在运行的程序和进程。任务管理器可以打开用于监视计算机性能的关键指示器，使用户能够快速了解系统的整体健康状况。在“应用程序”选项卡中，用户可以看到所有当前运行的程序及其状态。“进程”选项卡显示了系统中所有正在运行的进程的详细列表，包括每个进程对 CPU 和内存资源的使用情况。任务管理器提供了一个深入的视角来观察运行中的进程如何影响计算机的性能。用户可以根据需要对这些进程进行排序，以便快速识别出最占资源的进程。用户能够通过任务管理器结束、切换或启动新的程序和进程。这提供了一种迅速处理不响应程序和调整正在运行应用的便捷方式。

**二、进程**

进程是操作系统中一个重要的概念，它表示计算机中正在执行的程序的实例。每个进程都拥有独立的地址空间和系统资源，包括内存、文件句柄和执行线程等。

进程作为系统资源分配和调度的基本单位，不仅包含了程序的执行状态信息，如程序计数器、寄存器和变量等，还涉及到 CPU 和内存的使用情况、页面错误和句柄计数等多种性能指标。操作系统通过进程管理机制，如任务创建、执行、挂起、终止等操作，协调各个进程之间的运行，确保系统资源的有效分配和使用，维持系统的稳定性和效率。

- tasklist 命令：这个命令用于展示在本地或远程计算机上运行的所有应用程序和服务列表，提供了每个进程的详细信息，包括进程 ID（PID）。
- taskkill 命令：taskkill 提供了一种机制来结束一个或多个任务或进程。用户可以根据进程 ID（PID）或程序的名称来指定需要结束的进程。
- tskill 命令：tskill 功能与 taskkill 相似，同样用于结束一个或多个进程。

**三、网络进程**

网络进程是指在网络通信中参与数据传输的进程，它们与一般的进程共享基础属性，如占用系统资源（CPU、内存等），但独特之处在于其能够开启一个或多个网络端口。这些端口作为通信通道，允许进程接收和发送网络数据。在客户端-服务器（C/S）或浏览器-服务器（B/S）架构中，客户端网络进程通常至少开启一个端口以接收服务器发送的数据或向服务器发送请求，而服务端网络进程可能开启至少两个端口，分别用于接收来自客户端的数据和向客户端发送数据。端口号的范围从 0 到 65535，其中 0 到 1023 通常被保留为系统或标准服务端口。通过特定命令，如在 Windows 环境下，用户可以查询哪些端口当前正在被使用，以及这些端口分别属于哪些进程，从而对网络通信过程有更清晰的了解和管理。

**四、服务**

服务（在 Windows 环境中通常称为 Windows 服务）是一种特殊类型的进程，主要设计用来在操作系统的后台执行，提供核心功能或支持其他程序和进程。与普通的应用程序不同，服务通常不需要用户交互，也不提供图形用户界面。它们在系统启动时自动开始，并且可以配置为持续运行，即使没有用户登录到系统也能执行其功能。这些服务负责处理多种系统级任务，如文件和打印共享、网络连接管理、用户认证等。Windows 服务可以通过事件日志记录其操作和错误信息，为系统管理员提供重要的诊断信息。

**【实验设备】**

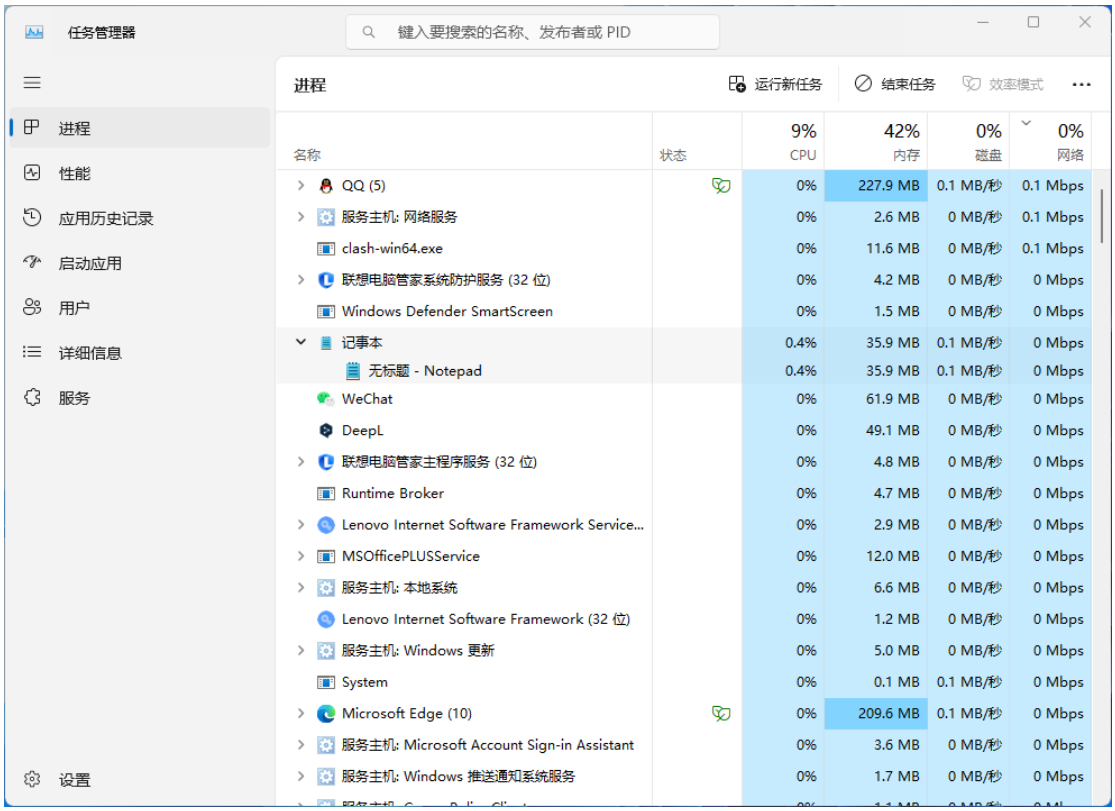
1. 操作系统：Windows 11
2. 网络环境：Wi-Fi 连接
3. 应用程序：记事本、画图

**【实验步骤】**

1. 启动并进入 Windows 环境，通过快捷键“Ctrl+Alt+Del”键选择“任务管理器”，或者右键点击任务栏，在快捷菜单选择“任务管理器”，或者通过命令 taskmgr 打开“任务管理器”。
2. 启动记事本应用程序。
3. 在任务管理器中，切换至“进程”选项卡，观察 CPU 和内存的使用情况。
4. 通过任务管理器和命令行工具（tasklist 命令、taskkill 命令等）查看和管理进程。
5. 通过命令 services.msc 查看系统服务。
6. 观察实验现象，记录观察到的进程、服务和相关参数。

**【实验现象】**

1. 在任务管理器“进程”选项卡中观察 CPU 和内存的使用情况，记事本应用程序在任务管理器“进程”选项卡中显示。



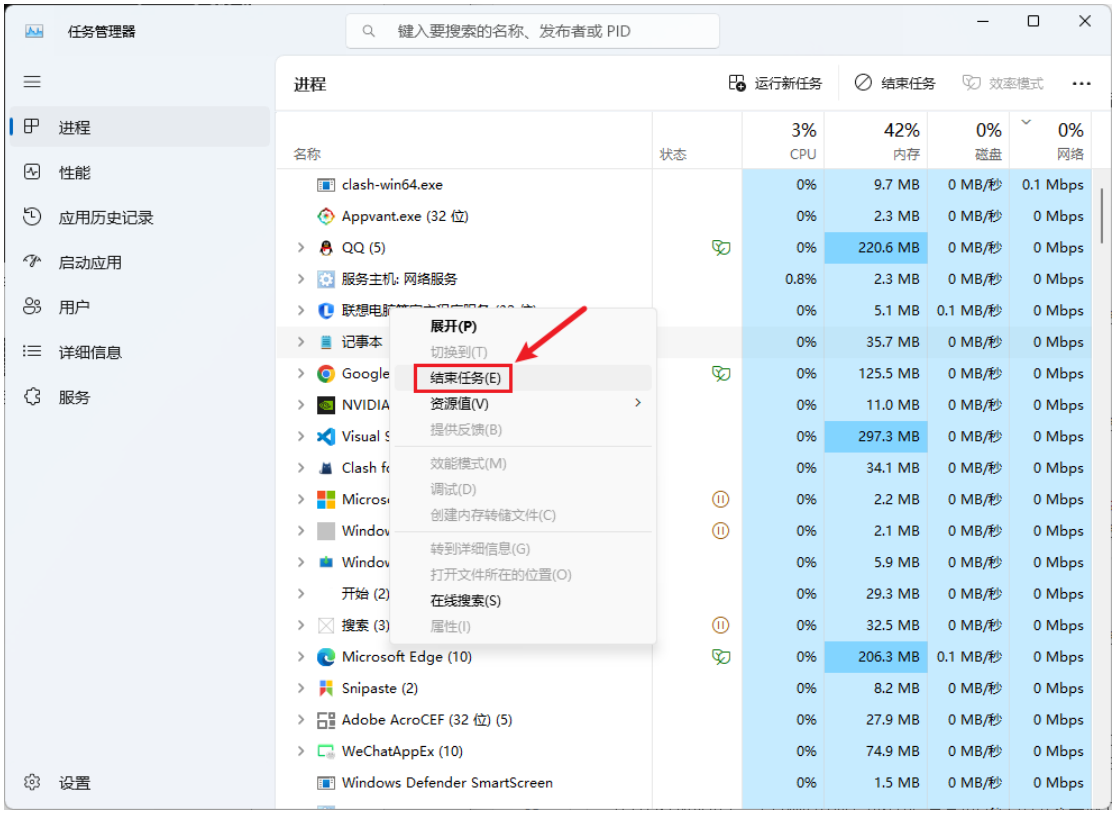
2. 在命令行通过中 tasklist 命令列出所有正在运行的进程。可以查看 Notepad.exe 的 PID 为 26604。

```
C:\Users\lenovo>tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      3,384 K
Registry                       216 Services                   0     30,488 K
smss.exe                       808 Services                   0        960 K
csrss.exe                     1124 Services                   0      6,296 K
wininit.exe                   1268 Services                   0      6,772 K
csrss.exe                     1280 Console                    1      6,888 K
services.exe                  1344 Services                   0      9,932 K
lsass.exe                     1372 Services                   0     22,812 K
svchost.exe                   1492 Services                   0     23,440 K
fontdrvhost.exe               1520 Services                   0      1,964 K
WUDFHost.exe                  1572 Services                   0     12,404 K
svchost.exe                   1624 Services                   0     15,816 K
svchost.exe                   1676 Services                   0      6,240 K
winlogon.exe                  1732 Console                    1      8,084 K
WUDFHost.exe                  1816 Services                   0      4,476 K
fontdrvhost.exe               1856 Console                    1     16,524 K
WUDFHost.exe                  1916 Services                   0      3,644 K
svchost.exe                   1988 Services                   0      2,980 K
dwm.exe                       2024 Console                    1    182,888 K
svchost.exe                   2036 Services                   0      4,968 K
svchost.exe                    916 Services                   0      8,156 K
svchost.exe                   1164 Services                   0     12,172 K
svchost.exe                   2084 Services                   0      8,228 K
svchost.exe                   2152 Services                   0     14,792 K
svchost.exe                   2192 Services                   0      7,136 K
svchost.exe                   2200 Services                   0      7,748 K
svchost.exe                   2212 Services                   0      7,824 K
svchost.exe                   2240 Services                   0     12,444 K
IntelCpHDCPSvc.exe            2368 Services                   0      3,712 K
svchost.exe                   2388 Services                   0     10,152 K
svchost.exe                   2396 Services                   0      6,988 K
svchost.exe                   2472 Services                   0      4,984 K
svchost.exe                   2488 Services                   0      5,312 K
svchost.exe                   2768 Services                   0      8,220 K
svchost.exe                   2860 Services                   0      7,856 K
svchost.exe                   2904 Services                   0      5,004 K
igfxCUIServiceN.exe           3008 Services                   0      7,892 K
svchost.exe                   3040 Services                   0     10,608 K
NVDisplay.Container.exe       3116 Services                   0     17,296 K
svchost.exe                   3128 Services                   0      5,936 K
svchost.exe                   3136 Services                   0      7,908 K
svchost.exe                   3296 Services                   0      7,260 K
svchost.exe                   3336 Services                   0     17,004 K
svchost.exe                   3420 Services                   0      5,808 K
svchost.exe                   3428 Services                   0     10,020 K
svchost.exe                   3508 Services                   0      8,892 K
svchost.exe                   3524 Services                   0     10,516 K
Memory Compression            3552 Services                   0    234,316 K
svchost.exe                   3608 Services                   0      8,284 K
WUDFHost.exe                  3704 Services                   0      9,372 K
svchost.exe                   3724 Services                   0     18,792 K
NVDisplay.Container.exe       3924 Console                    1     32,884 K
svchost.exe                   3944 Services                   0     23,500 K
svchost.exe                   4024 Services                   0      6,360 K
```

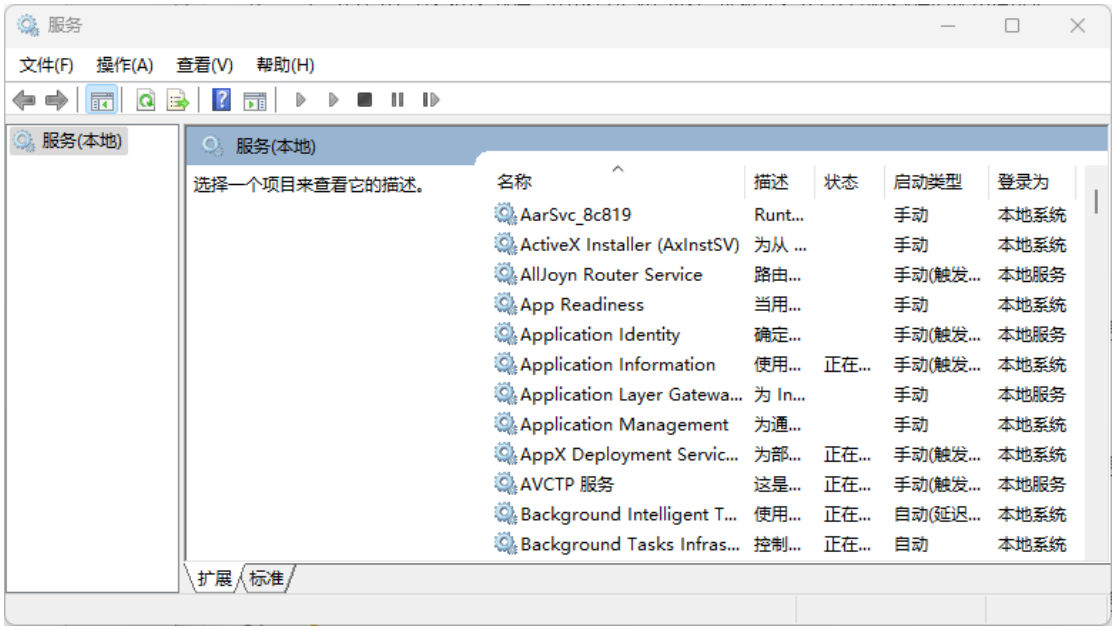
3. 在命令行通过中 taskkill /PID 26604 命令结束记事本应用程序的进程，可以观察记事本应用程序被关闭。

```
C:\Users\lenovo>taskkill /PID 26604
成功: 给进程发送了终止信号，进程的 PID 为 26604。
```

4. 在任务管理器通过中通过右键菜单选择“结束任务”结束记事本应用程序的进程，可以观察记事本应用程序被关闭。




5. 通过中 services.msc 命令列出所有的系统服务及其状态。



【分析讨论】

一、进程和网络进程的含义

- 进程：在操作系统中，进程是指一个执行中的程序。它不仅包含代码本身，还包括执行的当前活动、在内存中的数据、一个执行堆栈、至少一个执行序列（线程）以及其他用于操作系统书签的资源。简而言之，进程是系统进行资源分配和调度的基本单位，是应用程序在系统中的一次运行活动。
- 网络进程：网络进程在基本的进程属性上扩展，使其能够参与网络通信。这类进程通过开启一个或多个网络端口进行数据的发送和接收。网络进程的主要特点是其能够监听网络请求或向其他网络地址发送请求，常见于客户端-服务器（C/S）或浏览器-服务器（B/S）架构的应用中。网络进程至少需要开启一个端口号用于网络通信，使其在数据传输中扮演着至关重要的角色。

二、任务管理器的启动和使用

任务管理器是 Windows 操作系统中的一个系统监控工具，用于提供关于计算机性能及运行中程序的信息。可以通过快捷键 Ctrl+Alt+Del 并选择“任务管理器”，或者在任务栏上右键点击选择“任务管理器”来启动它，也可以通过命令 taskmgr 打开“任务管理器”。

三、图形界面方式和命令行方式显示有关服务

- 图形界面方式：用户可以通过运行 services.msc 命令打开服务管理控制台。这个图形界面显示了所有 Windows 服务的列表，包括每个服务的状态（如正在运行、已停止等），允许用户通过右键菜单进行启动、停止、暂停、恢复或重新启动服务等操作。
- 命令行方式：用户也可以通过命令行工具来管理服务。例如，使用 net start 和 net stop 命令分别启动和停止服务。对于更高级的服务管理，sc 命令提供了一套完整的服务控制功能，包括查询服务状态、配置服务启动类型等。

四、图形界面方式和命令行方式显示有关服务

- 图形界面方式：在任务管理器的“进程”选项卡中，用户可以查看到所有正在运行的进程及其资源使用情况。通过右键点击特定进程，用户可以选择“结束任务”来强制停止一个进程。
- 命令行方式：使用 tasklist 命令可以查看当前运行的所有进程及其 PID（进

程标识符)。taskkill 命令允许用户通过指定 PID 或进程名来结束一个或多个进程。如 taskkill /PID 1234 会结束 PID 为 1234 的进程。tskill 命令提供了类似 taskkill 的功能，也是用于结束进程。

# 实验 02：网络端口地址实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/02/29 |

**【实验目的】**

1. 深入理解网络进程与一般进程之间的基本相同属性和唯一不同的特性，特别是在开启传输端口号方面的差异。
2. 学习网络端口地址的重要性及其在网络通信中的作用，理解端口如何作为主机上某一进程的标识符，实现计算机间进程的通信。
3. 通过实际操作和观察，掌握如何在 Windows 操作系统下查看和分析网络端口的使用情况，包括使用命令行工具查看系统的网络连接和端口状态。
4. 识别和了解常用网络服务（如 HTTP、HTTPS、FTP 等）的默认端口号及其功能，加深对网络服务端口配置的理解。

**【实验原理】**

**一、网络端口地址**

网络端口地址是指在网络通信中，用于标识主机上特定进程的数字标签。这些端口号位于传输层，范围从 0 到 65535，其中 0 到 1023 号端口被划分为保留或系统端口号，通常被操作系统或特定的网络服务使用。端口地址的存在使得网络上的计算机可以同时运行多个网络服务，通过不同的端口号来区分不同的服务或进程，从而实现精准的数据传输和接收。

在客户端-服务器（C/S）或浏览器-服务器（B/S）架构的网络中，端口的使用是通信的基础。客户端网络进程通常至少开启一个端口号来发送或接收数据。而服务端网络进程则可能需要至少开启两个端口号，一个用于接收客户端发送的数据，另一个用于向客户端发送数据。这样的设计允许网络进程在进行数据交换时，能够明确数据的来源和目的地，确保数据传输的准确性和效率。

**二、网络端口地址划分示例**

- 端口 0-1023：系统端口，这些端口只有系统特许的进程才能使用。
- 端口 1024-65535：用户端口。
- 端口 1024-5000：临时端口，一般的应用程序使用 1024-4999 来进行通讯。
- 端口 5001-65535：服务器端口，用来给用户自定义端口。

## 三、常用的 TCP、UDP 相关端口号

- DHCP：服务器端的端口号是 67。
- DHCP：客户机端的端口号是 68。
- POP3：端口号是 110。POP3 接收协议，POP3 客户端使用 SMTP 向服务器发送邮件。
- SMTP：端口号是 25，SMTP 真正关心的不是邮件如何被传送，而只关心邮件是否能顺利到达目的地。
- Telnet：端口号是 23，测试端口号。
- FTP：端口号是 20 和 21。端口 20 用于数据的传输，端口 21 用于控制信息的传输，控制信息和数据能够同时传输，这是 FTP 的特殊之处。
- TFTP:端口号是 69,使用 UDP 的连接 TFTP(Trivial File Transfer Protocol,简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。
- UDP：端口号是 53，DNS 域名解析服务。
- TCP：端口号是 80，HTTP 超文本传输服务。
- TCP：端口号是 443，HTTPS 加密的超文本传输。

**【实验设备】**

1. 操作系统：Windows 11
2. 网络环境：Wi-Fi 连接
3. 应用程序：Google Chrome

**【实验步骤】**

1. 在浏览器中分别输入以下地址进行访问：
   - https://www.tongji.edu.cn:8080
   - https://www.tongji.edu.cn:80
   - http://www.tongji.edu.cn:8080
   - http://www.tongji.edu.cn:80
2. 在命令行中执行命令 netstat -ano，观察实验结果。

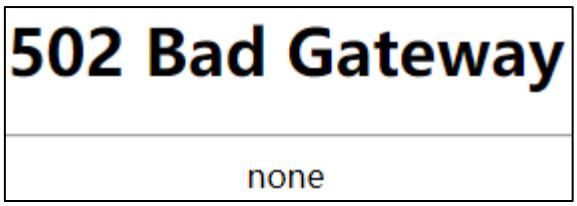
**【实验现象】**

1. 在浏览器中输入 https://www.tongji.edu.cn:8080 并访问，显示“此网站

无法提供安全连接，www.tongji.edu.cn 发送的响应无效，错误代码为 ERR_SSL_PROTOCOL_ERROR”。

2. 在浏览器中输入 https://www.tongji.edu.cn:80 并访问，显示“此网站无法提供安全连接，www.tongji.edu.cn 发送的响应无效，错误代码为 ERR_SSL_PROTOCOL_ERROR”。

3. 在浏览器中输入 http://www.tongji.edu.cn:8080 并访问，显示“502 Bad Gateway”。




4. 在浏览器中输入 http://www.tongji.edu.cn:80 并访问，正常显示同济大学官网内容。

5. 在命令行中执行命令 netstat -ano，观察到活动连接的协议、本地地址、外部地址和状态。

```
C:\Users\lenovo>netstat

活动连接

  协议  本地地址          外部地址        状态
  TCP    100.78.78.174:49426    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:49681    103.212.12.38:3000     ESTABLISHED
  TCP    100.78.78.174:50299    109.244.212.84:https   CLOSE_WAIT
  TCP    100.78.78.174:50572    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50769    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50787    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50790    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50808    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50810    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50828    ecs-139-159-217-107:4044  TIME_WAIT
  TCP    100.78.78.174:50862    ecs-139-159-217-107:4044  TIME_WAIT
  TCP    100.78.78.174:50876    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:50883    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:54523    20.197.71.89:https     ESTABLISHED
  TCP    100.78.78.174:54533    43.137.29.185:8080     ESTABLISHED
  TCP    100.78.78.174:54565    140.249.28.147:https   CLOSE_WAIT
  TCP    100.78.78.174:55097    175.27.0.15:https      ESTABLISHED
  TCP    100.78.78.174:56133    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    100.78.78.174:56139    ecs-139-159-217-107:4044  ESTABLISHED
  TCP    127.0.0.1:7890         local:49425            ESTABLISHED
  TCP    127.0.0.1:7890         local:50571            ESTABLISHED
  TCP    127.0.0.1:7890         local:50752            TIME_WAIT
  TCP    127.0.0.1:7890         local:50759            TIME_WAIT
  TCP    127.0.0.1:7890         local:50761            TIME_WAIT
  TCP    127.0.0.1:7890         local:50768            ESTABLISHED
  TCP    127.0.0.1:7890         local:50783            TIME_WAIT
  TCP    127.0.0.1:7890         local:50786            ESTABLISHED
  TCP    127.0.0.1:7890         local:50789            ESTABLISHED
  TCP    127.0.0.1:7890         local:50807            ESTABLISHED
  TCP    127.0.0.1:7890         local:50809            ESTABLISHED
  TCP    127.0.0.1:7890         local:50875            ESTABLISHED
  TCP    127.0.0.1:7890         local:50880            FIN_WAIT_2
```

【分析讨论】

## 一、实验内容记录

1. 在浏览器中分别输入以下地址进行访问：
   - https://www.tongji.edu.cn:8080
   - https://www.tongji.edu.cn:80
   - http://www.tongji.edu.cn:8080
   - http://www.tongji.edu.cn:80
2. 在命令行中执行命令 netstat -ano，观察实验结果。

## 二、相关端口号的使用举例

1. HTTP（超文本传输协议）
   - 端口号：80
   - 使用场景：这是最常见的网页浏览使用的端口。当你在浏览器中输入一个网址访问一个网站时，如果网址是以 http://开头，那么通信就是通过端口 80 进行的。
2. HTTPS（安全的超文本传输协议）
   - 端口号：443
   - 使用场景：用于安全的网页浏览。当网址以 https://开头时，表示网站使用了 SSL 或 TLS 加密，此时通信通过端口 443 进行。这种方式比 HTTP 更安全，因为它加密了传输的数据。
3. FTP（文件传输协议）
   - 端口号：20（数据传输）和 21（控制信息传输）
   - 使用场景：FTP 用于在网络上的计算机之间传输文件。端口 21 用于登录、命令和控制信息的传输，而端口 20 用于实际的文件数据传输。
4. SMTP（简单邮件传输协议）
   - 端口号：25
   - 使用场景：用于发送电子邮件。当你使用电子邮件客户端发送邮件时，邮件数据通过端口 25 发送到邮件服务器。
5. POP3（邮局协议第 3 版）
   - 端口号：110

- 使用场景：用于从邮件服务器接收电子邮件到本地电子邮件客户端。它允许电子邮件客户端下载服务器上的邮件。

6. DNS（域名系统）
   - 端口号：53
   - 使用场景：用于将域名（如 www.example.com）转换为与之对应的 IP 地址。这使得用户可以通过域名访问网站，而不需要记住复杂的 IP 地址。
7. DHCP（动态主机配置协议）
   - 服务器端口号：67
   - 客户机端口号：68
   - 使用场景： 在局域网中自动分配 IP 地址给设备。当一个设备连接到网络时，DHCP 服务器通过端口 67 分配 IP 地址，设备通过端口 68 接收。
8. Telnet
   - 端口号：23
   - 使用场景：用于远程登录到另一台计算机进行控制。虽然由于安全问题，现在已经被 SSH 所取代，但在某些老旧系统或设备中仍可能使用 Telnet。

# 实验 03：网络线的制作和测试实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/07 |

**【实验目的】**

1. 自行制作包括直通线和交叉线在内的网络双绞线。
2. 通过实践活动，掌握网络线的制作方法、测试技能以及使用相关工具（如 RJ-45 水晶头、压线钳和通断仪）的技巧。
3. 了解非屏蔽双绞线（Unshielded Twisted Pair, UTP）的基本结构和性能特点，以及其在网络中的应用。
4. 学习和理解 T568A 和 T568B 两种最常见的 RJ45 插头接线标准，包括每一对双绞线的颜色和位置规定。

**【实验原理】**

**一、双绞线**

非屏蔽双绞线（Unshielded Twisted Pair，简称 UTP）是在塑料绝缘外皮里面包裹着 8 根信号线，它们每 2 根为一对相互缠绕，形成总共 4 对。这种结构减少了电磁干扰，增强了信号传输的稳定性。

**二、T568A 和 T568B**

T568A 和 T568B 是最常见的 RJ45 插头接线标准，规定了每一对双绞线的颜色和位置。其中 1、2 用于发送，3、6 用于接收，4、5，7、8 是双向线。1、2 线必须是双绞，3、6 双绞，4、5 双绞，7、8 双绞。

标准 568A 的线序如下：

| 线序 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 颜色 | 白绿 | 绿 | 白橙 | 蓝 | 白蓝 | 橙 | 白棕 | 棕 |

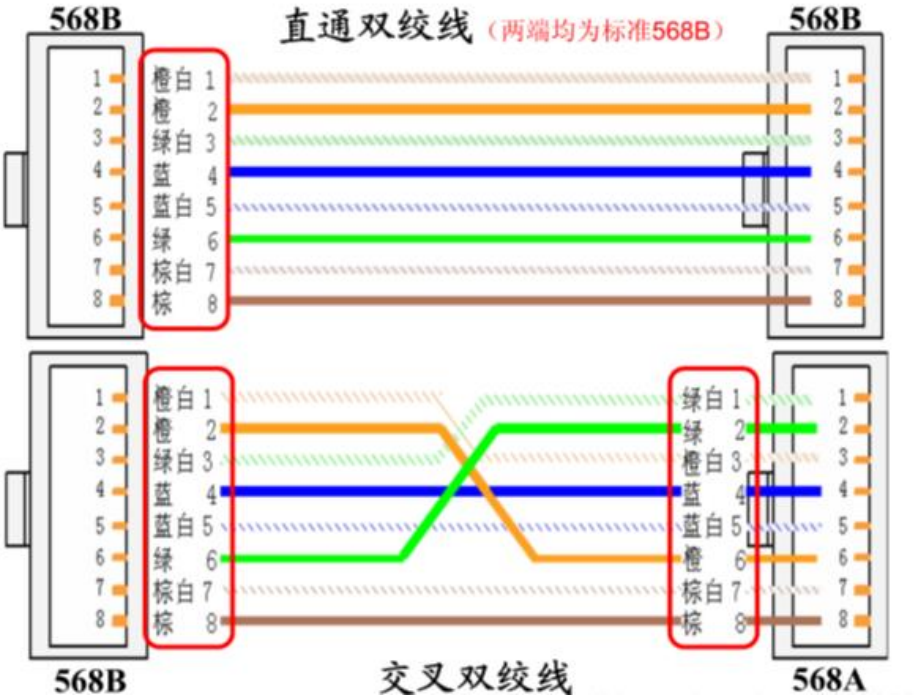
标准 568B 的线序如下：

| 线序 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 颜色 | 白橙 | 橙 | 白绿 | 蓝 | 白蓝 | 绿 | 白棕 | 棕 |

**三、直通线和交叉线的作用和线图**

直通线用于将计算机连入到交换机，或在结构化布线中由接线面板连到交换机等。根据 EIA/TIA 568-B 标准（又俗称为端接 B）。

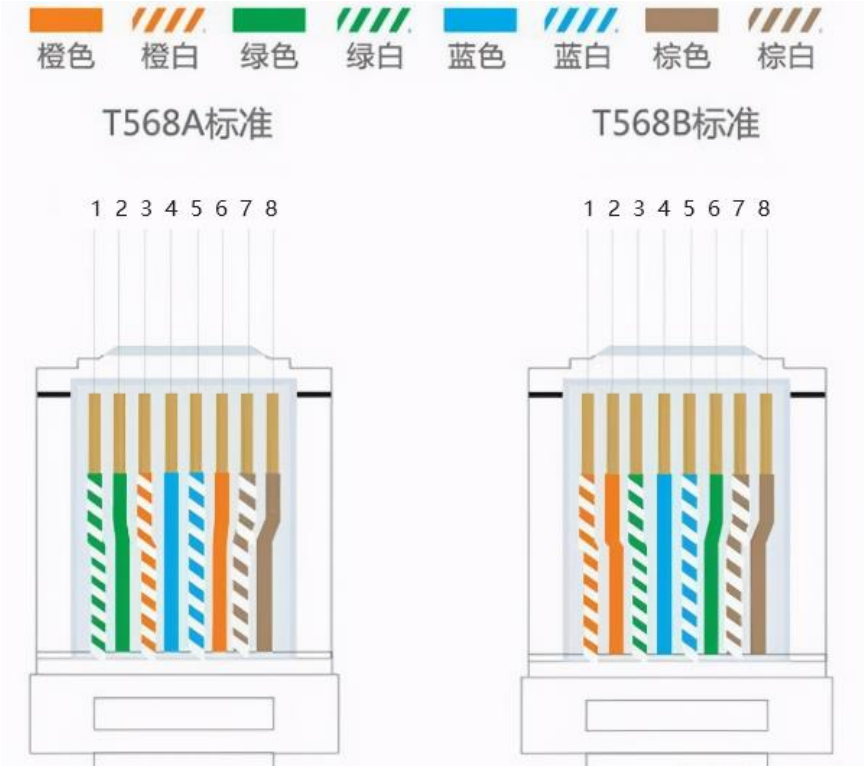
交叉线用于将计算机与计算机直接相连、交换机与交换机直接相连，也被用于计算机直接接入路由器的以太网口。根据 568A 标准和 568B 标准。




## 四、RJ-45 水晶头

双绞线的两端必须都安装 RJ-45 插头，以便插在网卡、集线器（Hub）或交换机（Switch）RJ-45 接口上。

水晶头接法如下：



**【实验设备】**

1. 双绞线
2. 水晶头（RJ-45 接头）
3. 压线钳
4. 通断仪

**【实验步骤】**

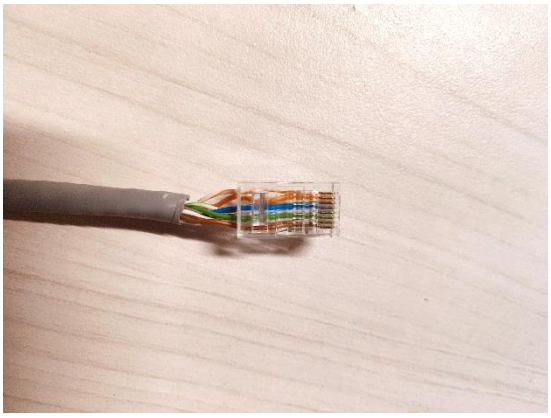
1. 工具准备。
2. 准备剥线：利用斜口剪下所需要的双绞线长度，至少 0.6 米，最多不超过 100 米。然后再利用双绞线剥线刀口将双绞线的外皮除去 2-3 厘米。
3. 抽取外套。
4. 拔线：将裸露的双绞线中的橙色对线拨向自己的左方，棕色对线拨向右方向，绿色对线拨向前方，蓝色对线拨向后方。
5. 按序号排好：小心的剥开每一对线，因为我们是遵循 EIA/TIA 568B 的标准（白橙-橙-白绿-蓝-白蓝-绿-白棕-棕）。
6. 排列整齐。
7. 剪断：将裸露出的双绞线用剪刀或斜口钳剪下只剩约 1.4 厘米的长度。
8. 准备放入插头。
9. 放入插头：最后再将双绞线的每一根线依序放入 RJ-45 接头的引脚内，第一只引脚内应该放白橙色的线，其余类推。确定双绞线的每根线是否按正确顺序放置，并查看每根线是否进入到水晶头的底部位置。
10. 准备压实。
11. 压紧：用 RJ-45 压线钳压接 RJ-45 接头，把水晶头里的八块小铜片压下去后，使每一块铜片的尖角都触到一根铜线。
12. 完成。
13. 制作另一端 RJ-45 接头。
14. 用通断仪测量。如果两组 1、2、3、4、5、6、7、8 指标灯对应的灯同时亮，则表示制作双绞线制作成功。

**【实验现象】**

1. 直通线测试：通断仪的指示灯 1-1、2-2、3-3、4-4、5-5、6-6、7-7、8-8 都

亮起，即直通线制作成功。

2. 交叉线测试：通断仪的指示灯 1-3、2-6、3-1、4-4、5-5、6-2、7-7、8-8 都亮起，即交叉线制作成功。



**【分析讨论】**

实验结果显示，通过遵循正确的线序（T568A 或 T568B）和使用适当的工具（如压线钳和通断仪），我们能够成功地制作出直通线和交叉线。

在实际网络环境中，直通线主要用于连接不同类型的网络设备（如计算机与交换机），而交叉线用于连接相同类型的设备（如计算机与计算机或交换机与交换机）。这两种线缆的正确制作和应用对于构建有效的网络连接至关重要。

通过亲手制作和测试网络线缆，能够将理论知识应用于实践，这种实践经验是极其宝贵的，有助于深化对计算机网络基础知识的理解。

# 实验 04：基本网络测试工具及应用工具实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/07 |

**【实验目的】**

1. 掌握基本网络测试工具的使用：熟悉并掌握操作系统中内置的网络测试工具的基本使用方法，如 Ping 命令、Ipconfig、Tracert、Net 命令等，这些工具虽然不能被视为专业级的测试软件，但对于日常网络故障的诊断与解决来说，它们是非常有效且便捷的手段。
2. 了解网络测试工具的应用场景：通过实际操作这些工具，理解各个工具的具体应用场景，例如，使用 Ping 命令检测网络连接的连通性，利用 Ipconfig 查看网络配置信息，通过 Tracert 命令追踪数据包的路由路径等。
3. 培养网络问题分析与解决能力：实验通过对各种网络命令的学习和实践，旨在培养分析和解决网络问题的能力。
4. 加深对 TCP/IP 协议的理解：通过使用这些基于 TCP/IP 协议的测试工具，可以加深对 TCP/IP 网络协议的理解，包括 IP 地址、子网掩码、默认网关等网络基本概念的实际应用。

**【实验原理】**

**一、Ping 命令**

Ping 命令是一个在各种操作系统中广泛使用的网络工具，用于测试网络连接。该命令通过发送 ICMP（Internet Control Message Protocol，互联网控制消息协议）Echo Request 消息给目标主机并等待 Echo Reply 消息来检查主机之间的连通性。它是诊断网络问题的首选工具之一，因为它不仅可以帮助确定两个节点之间是否存在通信路径，还能提供关于网络延迟和丢包率的信息。

主要参数说明：

- -t：持续 ping 目标主机，直到用户手动停止（使用 Control-C）。
- -a：解析地址到主机名。
- -n count：设置要发送的 Echo Request 消息数目，默认是 4。
- -l length：指定 ICMP 消息请求数据部分的字节大小，默认是 32 字节。最大值可达 65500 字节。

- -f：设置“不要分段”标志，告诉中间路由器不要分段 ICMP 数据包。
- -i ttl：设置生存时间 TTL（Time To Live），即数据包在网络中跳数的上限，帮助避免数据包在网络中无限循环。
- -v tos：设置服务类型（Type of Service），用于定义数据包的优先级。
- -r count：记录路由，存储经过的路由器地址，最多可记录 9 个。
- -s count：设置时间戳，记录每个跳的处理时间。
- -j host-list / -k host-list：通过指定的主机列表设置源路由，-j 允许路由分隔，-k 不允许。
- -w timeout：设置等待每次回复的超时时间（毫秒）。

使用场景：

- 网络连通性测试：验证本地主机与网络上另一台主机之间的连通性。
- 网络性能测量：通过观察 ping 回复的时间，可以评估网络延迟。
- 路由跟踪：通过修改 TTL 值，可以观察数据包通过网络到达目标的路径。
- 网络故障诊断：通过分析丢包情况和响应时间，可以帮助定位网络故障的位置。

## 二、Ipconfig 命令

ipconfig 是一个在 Windows 操作系统中常用的命令行工具，用于显示当前设备的网络配置信息，包括 IP 地址、子网掩码和默认网关等。该命令还可以刷新 DNS 解析缓存和重置 DHCP 配置等。ipconfig 是诊断网络问题和获取网络设置的重要工具，对网络管理员和终端用户都非常有用。

主要参数说明：

- 无参数：执行 ipconfig 命令而不带任何参数将显示所有网络接口的 IP 地址、子网掩码和默认网关。
- /all：显示所有配置信息，包括 DNS 服务器、DHCP 服务器、租约获取时间和过期时间等。
- /release：释放指定适配器的 IPv4 地址租约。如果不指定适配器名称，则会释放所有适配器的 IP 地址租约。
- /renew：更新指定适配器的 IPv4 地址租约。这通常用于从 DHCP 服务器获取新的 IP 地址。

- /flushdns：清除 DNS 解析缓存。这在更改 DNS 设置或排除 DNS 解析问题时非常有用。
- /displaydns：显示 DNS 解析缓存的内容，包括最近解析的域名及其 IP 地址。
- /registerdns：刷新所有 DHCP 租约并重新注册 DNS 名称。

使用场景：

- 查看网络配置：最基本的使用场景是查看设备的 IP 配置信息，包括 IP 地址、子网掩码、默认网关等，以便进行网络故障诊断或配置核对。
- 网络问题诊断：当遇到网络连接问题时，使用 ipconfig 检查 IP 地址是否正确分配，或者默认网关是否设置正确，是排除网络故障的第一步。
- 刷新 DNS 缓存：当网站的 IP 地址更改后，如果本地 DNS 缓存未更新，可能会导致无法访问该网站。使用/flushdns 参数可以清除 DNS 缓存，帮助解决访问问题。
- 更新 IP 地址：在使用动态主机配置协议（DHCP）环境中，如果需要更换设备的 IP 地址，可以使用/release 释放当前的 IP 地址，然后使用/renew 获取新的 IP 地址。
- 网络配置调试：在更改网络设置或进行网络优化时，可以使用 ipconfig 及其参数来验证更改的效果，确保网络配置正确应用。

## 三、Nbtstat 命令

nbtstat 是一个在 Windows 操作系统中用于诊断 NetBIOS（网络基本输入输出系统）名称解析问题的命令行工具。NetBIOS 是一种较旧的网络传输协议，主要用于小型网络和本地网络环境中的设备间通信。nbtstat 命令可以帮助网络管理员查看本地和远程机器的 NetBIOS 名称表，诊断网络连接问题。

主要参数说明：

- -a <名称>：显示一个远程机器的 NetBIOS 名称表，其中<名称>是远程计算机的 NetBIOS 名称。
- -A <IP 地址>：使用远程计算机的 IP 地址显示 NetBIOS 名称表。
- -c：显示 NetBIOS 名称缓存的内容，包括名称及其对应的 IP 地址。
- -n：显示本地 NetBIOS 名称表。

- -r：显示 NetBIOS 名称解析统计信息，包括成功的和失败的名称解析尝试。
- -R：清除 NetBIOS 名称缓存。
- -S：显示当前会话表，包括与远程计算机的 NetBIOS 会话。
- -s：与-S 类似，但也显示远程计算机的 IP 地址。

使用场景：

- 诊断 NetBIOS 名称解析问题：当网络上的设备通过 NetBIOS 名称无法相互识别或连接时，可以使用 nbtstat 来检查 NetBIOS 名称表和缓存，找出问题所在。
- 网络连接故障排除：通过查看本地和远程机器的 NetBIOS 会话表，可以帮助诊断连接失败的原因，如是否因为 NetBIOS 会话限制或其他网络问题。
- 查看 NetBIOS 统计信息：nbtstat 可以提供有关 NetBIOS 名称解析尝试的成功率和失败率的统计信息，有助于分析网络性能问题。
- 刷新 NetBIOS 名称缓存：在网络配置更改后，旧的 NetBIOS 名称记录可能仍保留在缓存中，使用-R 参数可以清除缓存，确保名称解析是最新的。
- 网络安全检查：通过查看会话表和 NetBIOS 名称，可以帮助识别未授权的设备试图连接到网络，或者存在的潜在安全威胁。

## 四、Tracert 命令

tracert（Trace Route）是一个在多种操作系统中可用的命令行工具，用于显示数据包从源计算机到目标计算机或设备在网络上的路径。它利用 Internet Control Message Protocol (ICMP)发送消息到目标设备，并记录每个路由器在路径上的跳数。每个跳的响应时间也被记录下来，从而帮助用户识别路径中可能的瓶颈或问题点。

主要参数说明：

- -d：不将地址解析成主机名，直接显示 IP 地址。
- -h maximum_hops:定义搜索目标设备的最大跳数。默认值通常为 30 跳。
- -j host-list：使用源路由选项沿指定的主机列表路径前进。
- -w timeout：设置每个响应的等待超时时间（毫秒）。

- -4：强制使用 IPv4。
- -6：强制使用 IPv6。

使用场景：

- 网络故障诊断：当用户无法访问特定网站或网络服务时，tracert 可以用来确定数据包在哪个网络跳发生了延迟或丢失，有助于定位故障点。
- 性能评估：通过测量到达每个跳的时间，tracert 可以帮助评估网络路径的性能，识别路径中可能的延迟点。
- 路由追踪：tracert 提供了一种方法来观察数据包在达到最终目标之前经过的路由器和设备，这对于理解网络拓扑结构非常有用。
- 网络安全分析：tracert 可以帮助识别数据包传输路径中未授权的或意外的路由器和交换机，这对于检测潜在的安全风险至关重要。
- ISP 连通性测试：当怀疑网络连接问题与 ISP（Internet Service Provider，互联网服务提供商）有关时，tracert 可以用来测试到 ISP 的连接质量，以及到达 ISP 之后的网络路径质量。

**五、Net 命令**

net 命令是 Windows 操作系统中一个非常强大的命令行工具，它用于执行与网络、共享资源、文件、打印作业和用户账户相关的各种任务。这个命令集合提供了一套广泛的网络和系统管理功能，使得管理员可以通过命令行接口快速配置和管理 Windows 网络环境。

主要参数说明：

- net user：管理用户账户。可以添加、删除、修改用户账户信息，例如密码、用户组、登录权限等。
- net view：显示网络上的计算机或设备列表，或者显示某台计算机上的共享资源。
- net share：创建、删除或管理共享资源。可以控制哪些文件夹在网络上共享以及它们的共享权限。
- net use：连接、断开与网络资源的连接，并显示网络连接的信息。这常用于映射网络驱动器和连接网络打印机。
- net localgroup：管理本地用户组，包括添加和删除用户组成员。

- net start/net stop：启动或停止 Windows 服务。
- net session：管理与本机建立的网络会话，可以查看活动的网络连接和断开这些连接。
- net statistics：显示网络服务的统计信息，如服务器或工作站服务。

使用场景：

- 用户和组管理：网络管理员可以使用 net user 和 net localgroup 命令来添加、删除或修改系统用户和用户组，包括重置密码、配置用户权限等。
- 网络资源管理：使用 net share 和 net use 命令来共享和访问网络上的文件夹和打印机，非常适合在企业环境中管理文件共享和网络打印服务。
- 服务管理：通过 net start 和 net stop 命令启动和停止 Windows 服务，这对于故障排除或系统配置调整非常有用。
- 网络诊断与管理：net view 和 net session 命令允许管理员查看网络上的计算机和资源以及管理网络会话，有助于网络维护和故障诊断。

**六、Route 命令**

route 命令是一个网络工具，用于查看和修改 IP 路由表。这个命令在各种操作系统中都有提供，包括 Windows、Linux 和 macOS，使网络管理员能够控制数据包从源地址到目的地址的路径。通过使用 route 命令，管理员可以指定特定的路径来优化网络流量，解决网络拥堵问题，或绕过故障的网络设备。

主要参数说明：

- add：添加一条新的路由规则到 IP 路由表中。
- delete：从 IP 路由表中删除一条路由规则。
- print：显示当前的 IP 路由表。
- -p：当添加路由时，使路由规则持久化。仅在 Windows 系统中有效，这意味着即使重启计算机路由规则也依然有效。

使用场景：

- 自定义网络流量路径：当网络管理员希望控制特定网络流量的路径时，可以通过添加自定义路由来实现。这在多网卡环境或多个网络连接存在时尤其有用。

- 网络故障诊断和规避：在网络设备或链接故障时，管理员可以临时更改路由表，将流量重新定向到备用路径，以保证网络的连通性和服务的可用性。
- 网络性能优化：通过合理配置路由规则，可以避免网络拥堵，优化网络性能。
- 安全控制：通过定义特定的路由规则，可以防止不安全的网络访问或限制访问特定网络资源。

## 七、Nslookup 命令

nslookup 是一个用于查询域名系统（DNS）以获取域名或 IP 地址映射的命令行工具。它对于网络管理员和普通用户来说都是诊断和解决 DNS 问题的重要工具。

主要参数说明：

- 无参数：在不带任何参数的情况下启动 nslookup 会进入交互式模式，用户可以连续执行多个查询。
- <域名>：直接查询一个域名来获取其对应的 IP 地址。
- <IP 地址>：查询哪个域名与该 IP 地址关联，进行反向 DNS 查找。
- -type=<查询类型>：指定查询类型，如 A、AAAA、MX、TXT 等。A 记录查询返回 IPv4 地址，AAAA 记录返回 IPv6 地址，MX 记录查询邮件交换服务器，TXT 记录通常包含了对域名的一些文本信息。
- -query=<查询类型>/-q=<查询类型>：同-type。
- -debug：显示查询过程中的详细技术信息。
- server <名称或 IP>：更改查询使用的 DNS 服务器。

使用场景：

- DNS 解析故障排查：当域名无法正确解析时，nslookup 可以帮助确定问题是否出在 DNS 解析上，通过比较不同 DNS 服务器的解析结果找出问题所在。
- 查看域名信息：nslookup 能查询特定域名的各类 DNS 记录，例如获取域名的邮件服务器(MX 记录)，用于邮件发送系统的配置。
- DNS 记录验证：在更改 DNS 记录，如更换网站的 IP 地址或更新邮件服务

器配置后，使用 nslookup 验证更改是否已正确生效。

- 反向 DNS 查找：通过输入 IP 地址查询关联的域名，这在识别访问网络服务的来源时非常有用。
- 测试 DNS 服务器性能：通过对比不同 DNS 服务器解析同一域名所用的时间，可以评估 DNS 服务器的响应速度。

八、Netsh 命令

netsh（Network Shell）命令是一个强大的命令行脚本工具，用于查看和修改 Windows 操作系统网络配置。它允许管理员配置几乎所有与网络相关的系统设置，包括网络接口、防火墙规则、路由策略、IP 地址配置、Wi-Fi 管理等。由于 netsh 能够导出和导入配置，它也常用于网络设置的备份和恢复。

主要参数说明：

- interface (int)：用于管理网络接口，可以配置 IP 地址、DHCP 设置等。
- firewall：用于配置 Windows 防火墙设置。
- http：管理 HTTP 协议相关设置，包括 SSL 配置。
- advfirewall：用于更高级的防火墙配置，比如入站和出站规则、安全策略等。
- wlan：管理无线网络配置，包括配置网络、显示可用网络列表等。
- dump：导出当前的网络配置到一个脚本文件。
- reset：重置网络配置到初始状态。

使用场景：

- 网络配置管理：netsh 命令可以配置网络接口的 IP 地址、子网掩码、默认网关等参数，非常适用于静态 IP 地址配置或切换不同网络配置的场景。
- 防火墙和安全策略配置：通过 netsh，管理员能够配置 Windows 防火墙的详细规则，包括允许或阻止特定端口、程序的网络访问权限。
- Wi-Fi 管理：netsh wlan 提供了一系列管理无线网络的命令，可以用来显示所有可用的无线网络、连接到无线网络、导出和导入无线网络配置。
- 故障排除和网络诊断：netsh 提供的诊断命令可以帮助分析和解决网络

连接问题，如重置网络接口、查看各种网络统计信息。

- 网络配置的备份和恢复：通过 netsh dump 命令，可以将当前的网络配置导出到一个脚本文件中，随后可以通过执行此脚本来恢复网络配置，这对于系统迁移和恢复非常有用。

## 九、Ftp 命令

FTP（File Transfer Protocol）是一种用于在网络上传输文件的协议，而 ftp 命令是一个基于命令行的客户端程序，用于连接到 FTP 服务器以上传、下载和管理文件。它是 Internet 上最早期的文件传输服务之一，支持在客户端和服务器之间进行交互式文件传输。

主要参数说明：

- open <hostname> [port]：连接到指定的 FTP 服务器，可选地指定端口（默认为 21）。
- user <username> [password]：登录到 FTP 服务器，可能会提示输入密码。
- ls [directory] [localfile]：列出远程目录的内容，可以将输出重定向到本地文件。
- cd <directory>：更改服务器上的当前目录。
- lcd <directory>：更改本地机的当前目录。
- get <remote-file> [local-file]：下载文件，可以指定本地文件名。
- put <local-file> [remote-file]：上传文件，可以指定远程文件名。
- mget <remote-files>：下载多个文件。
- mput <local-files>：上传多个文件。
- binary：设置二进制传输模式，用于传输非文本文件。
- ascii：设置 ASCII 传输模式，用于传输文本文件。
- quit：断开连接并退出 FTP 客户端。

使用场景：

- 文件上传：将本地文件或文件夹上传到远程服务器，用于网站更新、备份存储等。
- 文件下载：从 FTP 服务器下载文件或目录到本地，用于获取公开共享的

资源、软件更新包等。

- 网站管理：网站管理员经常使用 FTP 来部署新的网页内容或更新现有内容。
- 数据备份和恢复：通过 FTP 将重要数据备份到远端服务器，或从远端服务器恢复数据到本地。
- 文件共享：在需要共享大文件时，FTP 是一个传统但有效的选择。

## 十、Telnet 命令

telnet 命令是一个基于命令行的通信协议工具，用于远程登录到另一台计算机上。通过 telnet，用户可以在本地计算机上模拟终端，以访问远程服务器。它主要用于远程管理网络设备和服务器，或进行故障排除。尽管 telnet 因其不加密传输数据而逐渐被更安全的协议如 SSH（Secure Shell）所取代，但在某些特定环境和应用中，它仍然被使用。

主要参数说明：

- <hostname> 或 <IP 地址>：指定要连接的远程主机名称或 IP 地址。
- <port>：（可选）连接到远程主机的端口号，默认端口为 23。
- -l <username>：指定登录远程主机时使用的用户名。
- -a：自动登录，使用当前用户的用户名。
- -e <escape char>：设置退出 telnet 会话的转义字符，默认为 Ctrl+]。

使用场景：

- 远程设备管理：telnet 可以用于远程访问和管理网络设备，如路由器、交换机等，尤其是在这些设备尚未配置 SSH 访问时。
- 测试网络服务：通过 telnet 连接到特定的端口，可以测试网络服务（如 SMTP、HTTP、FTP 等）是否在运行，这对于网络管理员在进行故障排除时非常有用。
- 教育和学习：telnet 提供了一个简单的环境来学习网络协议和终端操作，对于网络和安全领域的学生来说，这是一个很好的学习工具。
- 旧式系统维护：在一些老旧的系统或设备中，telnet 可能是唯一可用的远程访问方法，因此在特定情况下，系统管理员可能需要使用它进行维护工作。

【实验设备】

1. 操作系统：Windows 11
2. 网络环境：Wi-Fi 连接

【实验步骤】

1. 测试 Ping 相关命令。
2. 测试 Ipconfig 相关命令。
3. 测试 Nbtstat 相关命令。
4. 测试 Tracert 相关命令。
5. 测试 Net 相关命令。
6. 测试 Route 相关命令。
7. 测试 Nslookup 相关命令。
8. 测试 Netsh 相关命令。
9. 测试 Ftp 相关命令。
10. 测试 Telnet 相关命令。

【实验现象】

1. 使用 ping 40.60.38.2 命令测试网络是否通畅，结果显示网络不通畅。

```
C:\Users\lenovo>ping 40.60.38.2

正在 Ping 40.60.38.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

40.60.38.2 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)
```

2. 使用 ping 10.60.41.1 命令测试网络是否通畅，结果显示网络通畅。

```
C:\Users\lenovo>ping 10.60.41.1

正在 Ping 10.60.41.1 具有 32 字节的数据:
来自 10.60.41.1 的回复: 字节=32 时间=3ms TTL=59
来自 10.60.41.1 的回复: 字节=32 时间=6ms TTL=59
来自 10.60.41.1 的回复: 字节=32 时间=4ms TTL=59
来自 10.60.41.1 的回复: 字节=32 时间=4ms TTL=59

10.60.41.1 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms，最长 = 6ms，平均 = 4ms
```

3. 使用 ping -a MINMUSLIN 命令获取计算机的 IP 地址。

```
C:\Users\lenovo>ping -a MINMUSLIN

正在 Ping MinmusLin [fe80::d4b1:99a9:f47d:2d51%26] 具有 32 字节的数据:
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms

fe80::d4b1:99a9:f47d:2d51%26 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

4. 使用 ipconfig 命令显示所有网络接口的 IP 地址、子网掩码和默认网关。

```
C:\Users\lenovo>ipconfig

Windows IP 配置


以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

未知适配器 本地连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 3:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 12:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 以太网 3:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::56ef:3fcc:a3dd:cb3d%2
   IPv4 地址 . . . . . . . . . . . . : 192.168.178.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

以太网适配器 VMware Network Adapter VMnet8:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::d4b1:99a9:f47d:2d51%26
   IPv4 地址 . . . . . . . . . . . . : 192.168.216.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
```

5. 使用 ipconfig /all 命令显示所有配置信息。

```
C:\Users\lenovo>ipconfig /all

Windows IP 配置

   主机名 . . . . . . . . . . . . . : MinmusLin
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表 . . . . . . . . . : tongji.edu.cn

以太网适配器 以太网:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   物理地址. . . . . . . . . . . . . : 88-A4-C2-22-79-31
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

未知适配器 本地连接:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Array Networks TAP-Windows Adapter
   物理地址. . . . . . . . . . . . . : 00-FF-47-E7-31-E5
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 本地连接* 3:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   物理地址. . . . . . . . . . . . . : D4-54-8B-33-2B-7F
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

无线局域网适配器 本地连接* 12:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   物理地址. . . . . . . . . . . . . : D6-54-8B-33-2B-7E
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 以太网 3:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Netease UU TAP-Win32 Adapter V9.21
   物理地址. . . . . . . . . . . . . : 00-FF-5C-F8-8A-1E
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
```

6. 使用 nbtstat -c 命令显示 NetBIOS 名称缓存的内容，包括名称及其对应的 IP 地址。

```
C:\Users\lenovo>nbtstat -c

以太网 3:
节点 IP 址址: [0.0.0.0] 范围 ID: []

    缓存中没有名称
```

7. 使用 nbtstat -n 命令显示本地 NetBIOS 名称表。

```
C:\Users\lenovo>nbtstat -n

以太网 3:
节点 IP 址址: [0.0.0.0] 范围 ID: []

    缓存中没有名称
```

8. 使用 nbtstat -r 命令显示 NetBIOS 名称解析统计信息，包括成功的和失败的名称解析尝试。

```
C:\Users\lenovo>nbtstat -r

    NetBIOS 名称解析和注册统计
    ----------------------------------------------------

    通过广播解析的      = 0
    通过名称服务器解析    = 0

    通过广播注册的    = 25
    通过名称服务器注册的 = 0
```

9. 使用 nbtstat -S 命令显示当前会话表,包括与远程计算机的 NetBIOS 会话。

```
C:\Users\lenovo>nbtstat -S

以太网 3:
节点 IP 址址: [0.0.0.0] 范围 ID: []

    无连接

VMware Network Adapter VMnet1:
节点 IP 址址: [192.168.178.1] 范围 ID: []

    无连接

VMware Network Adapter VMnet8:
节点 IP 址址: [192.168.216.1] 范围 ID: []

    无连接

本地连接:
节点 IP 址址: [0.0.0.0] 范围 ID: []

    无连接

以太网:
节点 IP 址址: [0.0.0.0] 范围 ID: []

    无连接
```

10. 使用 tracert 10.60.38.2 命令追踪数据包从执行该命令的设备到目的 IP 地址 10.60.38.2 的路由路径。

```
C:\Users\lenovo>tracert 10.60.38.2

通过最多 30 个跃点跟踪到 10.60.38.2 的路由

  1     *        *        *     请求超时。
  2     *        *        *     请求超时。
  3     4 ms     3 ms     3 ms  172.21.1.38
  4     4 ms     5 ms     3 ms  172.21.1.142
  5     *        *        *     请求超时。
  6     *        *        *     请求超时。
  7     *        *        *     请求超时。
  8     *        *        *     请求超时。
  9     *        *        *     请求超时。
 10     *        *        *     请求超时。
 11     *        *        *     请求超时。
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     *        *        *     请求超时。
 19     *        *        *     请求超时。
 20     *        *        *     请求超时。
 21     *        *        *     请求超时。
 22     *        *        *     请求超时。
 23     *        *        *     请求超时。
 24     *        *        *     请求超时。
 25     *        *        *     请求超时。
 26     *        *        *     请求超时。
 27     *        *        *     请求超时。
 28     *        *        *     请求超时。
 29     *        *        *     请求超时。
 30     *        *        *     请求超时。

跟踪完成。
```

11. 使用 net start 命令显示已经启动的 Windows 服务。

```
C:\Users\lenovo>net start
已经启动以下 Windows 服务:

   Application Information
   AppX Deployment Service (AppXSVC)
   AVCTP 服务
   Background Intelligent Transfer Service
   Background Tasks Infrastructure Service
   Base Filtering Engine
   BluetoothUserService_8be98
   cbdhsvc_8be98
   CDPUserSvc_8be98
   Clash Core Service
   CNG Key Isolation
   COM+ Event System
```

12. 使用 route PRINT 命令显示当前的 IP 路由表。

```
C:\Users\lenovo>route PRINT
===========================================================================
接口列表
 24...88 a4 c2 22 79 31 ......Realtek PCIe GbE Family Controller
 13...00 ff 47 e7 31 e5 ......Array Networks TAP-Windows Adapter
 11...d4 54 8b 33 2b 7f ......Microsoft Wi-Fi Direct Virtual Adapter #3
  7...d6 54 8b 33 2b 7e ......Microsoft Wi-Fi Direct Virtual Adapter #4
 14...00 ff 5c f8 8a 1e ......Netease UU TAP-Win32 Adapter V9.21
  2...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 26...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  6...d4 54 8b 33 2b 7e ......Intel(R) Wi-Fi 6 AX201 160MHz
  4...d4 54 8b 33 2b 82 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0   100.81.255.254    100.81.138.91     45
        100.80.0.0      255.254.0.0         在链路上     100.81.138.91    301
     100.81.138.91  255.255.255.255         在链路上     100.81.138.91    301
    100.81.255.255  255.255.255.255         在链路上     100.81.138.91    301
         127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
         127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
   127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
     192.168.178.0    255.255.255.0         在链路上     192.168.178.1    291
     192.168.178.1  255.255.255.255         在链路上     192.168.178.1    291
   192.168.178.255  255.255.255.255         在链路上     192.168.178.1    291
     192.168.216.0    255.255.255.0         在链路上     192.168.216.1    291
     192.168.216.1  255.255.255.255         在链路上     192.168.216.1    291
   192.168.216.255  255.255.255.255         在链路上     192.168.216.1    291
         224.0.0.0        240.0.0.0         在链路上         127.0.0.1    331
         224.0.0.0        240.0.0.0         在链路上     192.168.178.1    291
         224.0.0.0        240.0.0.0         在链路上     192.168.216.1    291
         224.0.0.0        240.0.0.0         在链路上     100.81.138.91    301
   255.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
   255.255.255.255  255.255.255.255         在链路上     192.168.178.1    291
   255.255.255.255  255.255.255.255         在链路上     192.168.216.1    291
   255.255.255.255  255.255.255.255         在链路上     100.81.138.91    301
===========================================================================
永久路由:
  无
```

```
IPv6 路由表
===========================================================================
活动路由:
 接口跃点数网络目标                 网关
  6    301 ::/0                     fe80::9e54:c2ff:fe0d:5002
  1    331 ::1/128                  在链路上
  6    301 2001:da8:8002:6bd1::/64  在链路上
  6    301 2001:da8:8002:6bd1:3da8:a8dd:269f:38c7/128
                                    在链路上
  6    301 2001:da8:8002:6bd1:c18e:2f3d:a347:f6fd/128
                                    在链路上
  6    301 fd14:44b7:386d::/64      fe80::53:66f3:7828:7963
  2    291 fe80::/64                在链路上
 26    291 fe80::/64                在链路上
  6    301 fe80::/64                在链路上
  2    291 fe80::56ef:3fcc:a3dd:cb3d/128
                                    在链路上
  6    301 fe80::b6ff:9493:f8d0:9a9e/128
                                    在链路上
 26    291 fe80::d4b1:99a9:f47d:2d51/128
                                    在链路上
  1    331 ff00::/8                 在链路上
  2    291 ff00::/8                 在链路上
 26    291 ff00::/8                 在链路上
  6    301 ff00::/8                 在链路上
===========================================================================
永久路由:
  无
```

13. 使用 route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 命令添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1 的路由。

```
(base) C:\Windows\System32>route add 10.41.0.0 mask 255.255.0.0 10.27.0.1
 操作完成!
```

14. 使用 route delete 10.41.0.0 mask 255.255.0.0 移除目的地为 10.41.0.0，子网掩码为 255.255.0.0 的路由。

```
(base) C:\Windows\System32>route delete 10.41.0.0 mask 255.255.0.0
 操作完成!
```

15. 使用 nslookup 显示域名信息。

```
C:\Users\lenovo>nslookup
默认服务器:  dnscache1.tongji.edu.cn
Address:  202.120.190.208
```

**【分析讨论】**

通过本次实验，我不仅掌握了各种基本网络测试工具的使用，还加深了对 TCP/IP 协议的理解。我学会了如何利用这些工具来诊断和解决网络问题，了解了它们在不同场景下的应用。此外，本次实验还提高了我分析和解决网络问题的能力，对于将来的网络管理和维护工作打下了坚实的基础。

# 实验 05：主机路由实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/14 |

**【实验目的】**

本实验旨在通过 Windows 系统的 Route 命令，掌握主机路由的基本概念和操作，进一步理解路由表的动态维护和数据包的转发机制。通过实验内容，学习如何使用 route 命令在 Windows 环境下进行路由表的查看、添加、修改和删除操作，从而深入理解网络路由的工作原理及其在数据包传输过程中的作用。实验的主要内容包括练习 route print 命令以显示当前的路由表项目，route add 命令添加新的路由项目，route change 命令修改数据的传输路由，以及 route delete 命令从路由表中删除路由。

**【实验原理】**

**一、路由**

路由（Routing）是指在网络中传输数据包从源头到目的地时，确定数据包传输的端到端路径的过程。路由主要在 OSI 参考模型的第三层——网络层上进行，其核心设备是路由器。路由器的任务是通过转发数据包来实现不同网络的互连。

在进行路由时，路由器通常会连接两个或多个逻辑网络，这些网络可以是 IP 子网或通过点到点协议标识的。路由器至少拥有一个物理端口。当路由器收到一个数据包时，它会根据数据包中的目的地网络层地址以及自己内部维护的路由表来决定该将数据包转发至哪个端口以及下一个跳转的地址，并重写数据包的链路层头部信息以实现数据包的正确转发。

路由器通过动态维护其路由表来反映当前网络的拓扑结构。这个动态维护过程通常涉及与网络中其他路由器交换路由信息和链路状态信息，从而使得路由器能够了解到达网络中各个目标地址的最佳路径，并在网络拓扑发生变化时更新这些路径信息。

虽然路由器可以支持多种网络协议，如 TCP/IP、IPX/SPX、AppleTalk 等，但在我国，绝大多数路由器运行的是 TCP/IP 协议。这是因为 TCP/IP 协议提供了一整套完善的网络通信协议，能够满足各种网络互联和数据传输的需求，成为了

全球网络通信的标准。

## 二、Route 命令

route 命令是一个网络工具，用于查看和修改 IP 路由表。这个命令在各种操作系统中都有提供，包括 Windows、Linux 和 macOS，使网络管理员能够控制数据包从源地址到目的地址的路径。通过使用 route 命令，管理员可以指定特定的路径来优化网络流量，解决网络拥堵问题，或绕过故障的网络设备。

主要参数说明：

- add：添加一条新的路由规则到 IP 路由表中。
- delete：从 IP 路由表中删除一条路由规则。
- print：显示当前的 IP 路由表。
- -p：当添加路由时，使路由规则持久化。仅在 Windows 系统中有效，这意味着即使重启计算机路由规则也依然有效。

使用场景：

- 自定义网络流量路径：当网络管理员希望控制特定网络流量的路径时，可以通过添加自定义路由来实现。这在多网卡环境或多个网络连接存在时尤其有用。
- 网络故障诊断和规避：在网络设备或链接故障时，管理员可以临时更改路由表，将流量重新定向到备用路径，以保证网络的连通性和服务的可用性。
- 网络性能优化：通过合理配置路由规则，可以避免网络拥堵，优化网络性能。
- 安全控制：通过定义特定的路由规则，可以防止不安全的网络访问或限制访问特定网络资源。

**【实验设备】**

1. 操作系统：Windows 11
2. 网络环境：局域网

**【实验步骤】**

1. 打开命令提示符，注意要以管理员身份运行。
2. 使用 route PRINT 命令查看当前的路由表。

3. 记录显示的路由表项。

4. 使用 route ADD 命令添加新的路由。

5. 再次使用 route PRINT 命令，观察路由表的变化。

6. 使用 route CHANGE 命令尝试修改现有的路由。

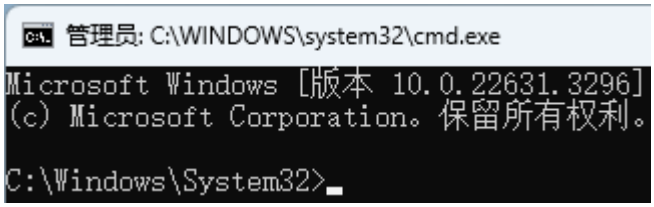
7. 再次使用 route PRINT 命令，观察路由表的变化。

8. 使用 route DELETE 命令删除刚才添加的路由。

9. 再次使用 route PRINT 命令，观察路由表的变化。

**【实验现象】**

1. 打开命令提示符，注意要以管理员身份运行。




2. 使用 route PRINT 命令查看当前的 IPv4 和 IPv6 路由表。

```
C:\Windows\System32>route PRINT
===========================================================================
接口列表
 24...88 a4 c2 22 79 31 ......Realtek PCIe GbE Family Controller
 13...00 ff 47 e7 31 e5 ......Array Networks TAP-Windows Adapter
 11...d4 54 8b 33 2b 7f ......Microsoft Wi-Fi Direct Virtual Adapter #3
  7...d6 54 8b 33 2b 7e ......Microsoft Wi-Fi Direct Virtual Adapter #4
 14...00 ff 5c f8 8a 1e ......Netease UU TAP-Win32 Adapter V9.21
  2...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 26...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  6...d4 54 8b 33 2b 7e ......Intel(R) Wi-Fi 6 AX201 160MHz
  4...d4 54 8b 33 2b 82 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0   100.81.255.254    100.81.138.91     45
        100.80.0.0      255.254.0.0         在链路上     100.81.138.91    301
     100.81.138.91  255.255.255.255         在链路上     100.81.138.91    301
    100.81.255.255  255.255.255.255         在链路上     100.81.138.91    301
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
     192.168.178.0    255.255.255.0         在链路上     192.168.178.1    291
     192.168.178.1  255.255.255.255         在链路上     192.168.178.1    291
   192.168.178.255  255.255.255.255         在链路上     192.168.178.1    291
     192.168.216.0    255.255.255.0         在链路上     192.168.216.1    291
     192.168.216.1  255.255.255.255         在链路上     192.168.216.1    291
   192.168.216.255  255.255.255.255         在链路上     192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上     192.168.178.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上     100.81.138.91    301
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上     192.168.178.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.216.1    291
  255.255.255.255  255.255.255.255         在链路上     100.81.138.91    301
===========================================================================
永久路由:
  无
```

```
IPv6 路由表
===========================================================================
活动路由:
 接口跃点数网络目标                    网关
  6    301 ::/0                        fe80::9e54:c2ff:fe0d:5002
  1    331 ::1/128                     在链路上
  6    301 2001:da8:8002:6bd1::/64     在链路上
  6    301 2001:da8:8002:6bd1:3da8:a8dd:269f:38c7/128
                                       在链路上
  6    301 2001:da8:8002:6bd1:c18e:2f3d:a347:f6fd/128
                                       在链路上
  6    301 fd14:44b7:386d::/64         fe80::53:66f3:7828:7963
  2    291 fe80::/64                   在链路上
 26    291 fe80::/64                   在链路上
  6    301 fe80::/64                   在链路上
  2    291 fe80::56ef:3fcc:a3dd:cb3d/128
                                       在链路上
  6    301 fe80::b6ff:9493:f8d0:9a9e/128
                                       在链路上
 26    291 fe80::d4b1:99a9:f47d:2d51/128
                                       在链路上
  1    331 ff00::/8                    在链路上
  2    291 ff00::/8                    在链路上
 26    291 ff00::/8                    在链路上
  6    301 ff00::/8                    在链路上
===========================================================================
永久路由:
  无
```

3. 记录显示的路由表项。

4. 使用 route ADD 192.168.2.0 mask 255.255.255.0 192.168.1.1 命令添加新的路由，使得所有前往 192.168.2.0 网络（子网掩码为 255.255.255.0）的数据包都通过 192.168.1.1 网关转发。

```
C:\Windows\System32>route ADD 192.168.2.0 mask 255.255.255.0 192.168.1.1
 操作完成!
```

5. 再次使用 route PRINT 命令，观察路由表的变化，新的路由项出现在路由表中。

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0   100.81.255.254    100.81.138.91     45
        100.80.0.0      255.254.0.0         在链路上     100.81.138.91    301
     100.81.138.91  255.255.255.255         在链路上     100.81.138.91    301
    100.81.255.255  255.255.255.255         在链路上     100.81.138.91    301
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
      192.168.2.0    255.255.255.0   192.168.1.1    100.81.138.91     46
     192.168.178.0    255.255.255.0         在链路上     192.168.178.1    291
     192.168.178.1  255.255.255.255         在链路上     192.168.178.1    291
   192.168.178.255  255.255.255.255         在链路上     192.168.178.1    291
     192.168.216.0    255.255.255.0         在链路上     192.168.216.1    291
     192.168.216.1  255.255.255.255         在链路上     192.168.216.1    291
   192.168.216.255  255.255.255.255         在链路上     192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上     192.168.178.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上     100.81.138.91    301
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上     192.168.178.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.216.1    291
  255.255.255.255  255.255.255.255         在链路上     100.81.138.91    301
===========================================================================
永久路由:
  无
```

6. 使用 route CHANGE 192.168.2.0 mask 255.255.255.0 192.168.1.2 命令尝试修改到 192.168.2.0 网络的路由，使数据包通过新的网关 192.168.1.2 转发。

```
C:\Windows\System32>route CHANGE 192.168.2.0 mask 255.255.255.0 192.168.1.2
 操作完成!
```

7. 再次使用 route PRINT 命令，观察路由表的变化，选定的路由项得到修改。

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0   100.81.255.254    100.81.138.91     45
       100.80.0.0      255.254.0.0         在链路上      100.81.138.91    301
   100.81.138.91  255.255.255.255         在链路上      100.81.138.91    301
  100.81.255.255  255.255.255.255         在链路上      100.81.138.91    301
        127.0.0.0        255.0.0.0         在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
      192.168.2.0    255.255.255.0   192.168.1.2    100.81.138.91     46
    192.168.178.0    255.255.255.0         在链路上      192.168.178.1    291
    192.168.178.1  255.255.255.255         在链路上      192.168.178.1    291
  192.168.178.255  255.255.255.255         在链路上      192.168.178.1    291
    192.168.216.0    255.255.255.0         在链路上      192.168.216.1    291
    192.168.216.1  255.255.255.255         在链路上      192.168.216.1    291
  192.168.216.255  255.255.255.255         在链路上      192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上          127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上      192.168.178.1    291
        224.0.0.0        240.0.0.0         在链路上      192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上      100.81.138.91    301
  255.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上      192.168.178.1    291
  255.255.255.255  255.255.255.255         在链路上      192.168.216.1    291
  255.255.255.255  255.255.255.255         在链路上      100.81.138.91    301
===========================================================================
永久路由:
  无
```

8. 使用 route DELETE 192.168.2.0 命令删除到 192.168.2.0 网络的路由。

```
C:\Windows\System32>route DELETE 192.168.2.0
 操作完成!
```

9. 再次使用 route PRINT 命令，观察相应的路由项从路由表中消失。

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0   100.81.255.254    100.81.138.91     45
       100.80.0.0      255.254.0.0         在链路上      100.81.138.91    301
   100.81.138.91  255.255.255.255         在链路上      100.81.138.91    301
  100.81.255.255  255.255.255.255         在链路上      100.81.138.91    301
        127.0.0.0        255.0.0.0         在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
    192.168.178.0    255.255.255.0         在链路上      192.168.178.1    291
    192.168.178.1  255.255.255.255         在链路上      192.168.178.1    291
  192.168.178.255  255.255.255.255         在链路上      192.168.178.1    291
    192.168.216.0    255.255.255.0         在链路上      192.168.216.1    291
    192.168.216.1  255.255.255.255         在链路上      192.168.216.1    291
  192.168.216.255  255.255.255.255         在链路上      192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上          127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上      192.168.178.1    291
        224.0.0.0        240.0.0.0         在链路上      192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上      100.81.138.91    301
  255.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上      192.168.178.1    291
  255.255.255.255  255.255.255.255         在链路上      192.168.216.1    291
  255.255.255.255  255.255.255.255         在链路上      100.81.138.91    301
===========================================================================
永久路由:
  无
```

【分析讨论】

一、实验内容记录

1. 打开命令提示符，注意要以管理员身份运行。使用 route PRINT 命令查看当前的 IPv4 和 IPv6 路由表。记录显示的路由表项。
2. 使用 route ADD 192.168.2.0 mask 255.255.255.0 192.168.1.1 命令添加新的路由，使得所有前往 192.168.2.0 网络（子网掩码为 255.255.255.0）的数据包都通过 192.168.1.1 网关转发。再次使用 route PRINT 命令，观察路由表的变化，新的路由项出现在路由表中。
3. 使用 route CHANGE 192.168.2.0 mask 255.255.255.0 192.168.1.2 命令尝试修改到 192.168.2.0 网络的路由，使数据包通过新的网关 192.168.1.2 转发。再次使用 route PRINT 命令，观察路由表的变化，选定的路由项得到修改。
4. 使用 route DELETE 192.168.2.0 命令删除到 192.168.2.0 网络的路由。再次使用 route PRINT 命令，观察相应的路由项从路由表中消失。

二、显示条目含义

1. 网络目标（Network Destination）：网络目标指的是目的地网络或主机的 IP 地址。这个字段定义了路由条目适用的目的地范围，可以是一个单一的 IP 地址（指向一个具体的设备）或一个网络地址（代表一个网络上的所有设备）。
2. 网络掩码（Netmask）：网络掩码与网络目标结合使用，用来指定目的地地址的范围。它通过掩码来区分 IP 地址中的网络部分和主机部分，从而定义了哪些 IP 地址属于同一个网络。例如，掩码 255.255.255.0 与网络地址 192.168.1.0 结合，表示 192.168.1.1 到 192.168.1.254 的所有 IP 地址都属于这个目标网络。
3. 网关（Gateway）：网关是指下一跳的路由器或其他转发设备的 IP 地址。对于目的地网络之外的数据包，网关是数据包被发送到，然后由其进一步转发到目的地的中间设备。
4. 接口（Interface）：接口是指本地主机上用于该路由的网络接口的 IP 地址。数据包将从这个接口出发，前往设置的网关或直接到达最终目的地。接口通常对应于物理或虚拟的网络适配器。

5. 跃点数（Metric）：跃点数是一个表示到达目的地所需成本的数值，它可以基于多种因素计算，如传输时间、距离、带宽等。在存在多条可用路径时，跃点数较低的路径通常会被选择为最佳路径。
6. 活动路由和永久路由：活动路由是当前有效并被使用的路由。而永久路由，不像活动路由在系统重启后会丢失，是在系统重启后依然有效的路由。永久路由需要通过特定的命令设置。
7. IPv4 和 IPv6 路由表：route PRINT 命令会显示 IPv4 和 IPv6 的路由表。尽管这两种协议在地址结构（IPv4 是 32 位，IPv6 是 128 位）和地址长度上有所不同，它们在路由原理上是相似的，都是通过路由表来指导数据包的转发。
8. 在链路上（On-link）：在链路上表示目的地可以直接通过本地接口到达，无需经过其他路由器。这通常用于表示该路由目的地是直接连接到本地网络的设备。

# 实验 06：异步串口通信电缆制作实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/14 |

**【实验目的】**

本实验旨在通过分析串口通信电缆，深入理解串口通信的基本原理和标准，包括物理连接、信号定义和通信协议。通过观察计算机的连接端口、分析串口线的结构和功能，以及实际操作中的问题解决，获得实践技能，并增强理论与实践结合的能力。此外，实验还旨在培养动手能力和解决实际问题的能力，为未来的电子和通信项目打下坚实的基础。

**【实验原理】**

**一、串口通信**

串口通信，或称串行通信（Serial Communication），是一种广泛应用于设备间的通讯方式。其主要特点是简单便捷，这使得大多数电子设备都采用了串口通信进行数据传输，特别是在设备调试过程中，经常利用串口通信来输出调试信息。在计算机科学中，通过将复杂问题分层处理来简化解决方案，串口通信也不例外，它主要分为物理层和协议层两个部分。

物理层负责定义通讯系统中的机械和电子特性，确保数据能够在物理媒介上成功传输。这涵盖了设备如何连接、信号的电子特性等基础设定，是实现通信的物质基础。

协议层则聚焦于通讯逻辑，规定了数据的打包、解包标准以及如何解释这些数据。它确保发送和接收双方能够以相同的方式理解和处理交换的信息，无论这些信息是通过何种物理手段传递的。

串口通信通过这两层的紧密协作，实现了设备间的高效、可靠通信。物理层确定了通信的物理和电子基础，而协议层则建立了共同的数据交流规则，使得不同设备之间能够顺畅地交换信息。这种分层的通信模型不仅适用于串口通信，也是现代通信技术中普遍采用的一个基本原则。

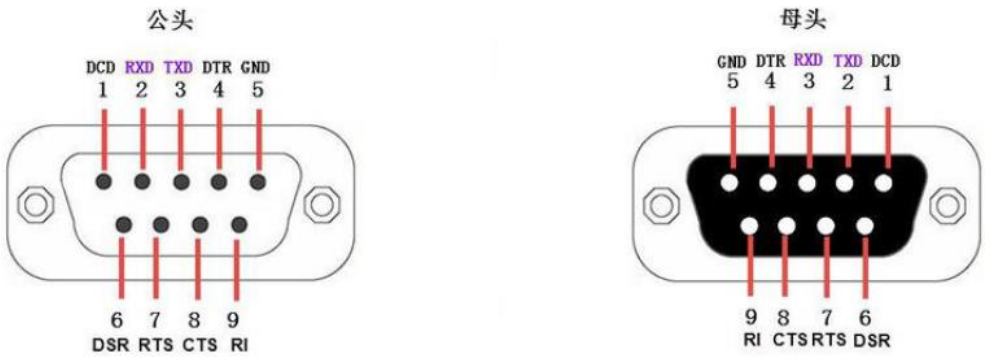
**二、串口通信标准**

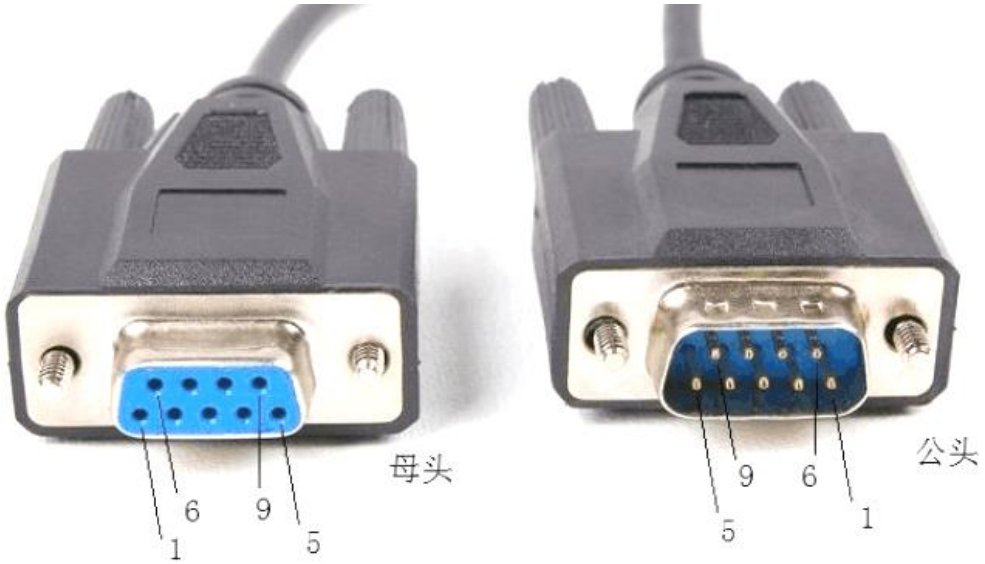
串口通信标准定义了串行通信中的物理接口、电信号特性、数据格式、通信速度等关键技术细节，确保了不同设备之间能够进行有效的数据交换。最常见的

串口通信标准包括 RS-232、RS-422、RS-485 等，其中 RS-232 是最广泛使用的一种标准。

RS-232 标准是最早的串行通信接口，主要用于计算机串行端口（COM 端口）和调制解调器之间的连接。它定义了一系列的信号线，包括数据发送（TX）、数据接收（RX）、地线（GND）等，并规定了电信号的电压水平，使得正电压表示二进制 0，负电压表示二进制 1。RS-232 通常支持的通信距离较短，最长不超过 15 米，适用于点对点的低速通信。

**三、串口连接（DB 连接端子——“D”型连接器）**




**四、串口协议**

串口协议是一种广泛使用的数据通信方式，特别是在嵌入式系统和计算机之间的低速数据交换中。串口通信允许设备通过串行接口进行数据传输，它遵循特定的协议规则来确保数据的正确传输。

1. 数据包格式：串口通讯的数据包由几个关键部分组成：启始位、主体数据（有效数据）、校验位（可选），以及停止位。

- 启始位：数据包的开始由一个逻辑 0 的数据位标识，表示数据传输的开始。
- 主体数据（有效数据）：紧随启始位之后的是要传输的主体数据，其长度通常被设定为 5、6、7 或 8 位。
- 校验位：位于有效数据之后，是一个可选部分，用于检测数据在传输过程中是否发生错误。常见的校验方法包括奇校验、偶校验、空格校验（0 校验）、标记校验（1 校验）和无校验。
- 停止位：数据包的结束由 0.5、1、1.5 或 2 个逻辑 1 的数据位表示，表示数据传输的结束。

2. 波特率（Baud Rate）：波特率是衡量数据传输速率的单位，代表每秒钟可以传输的码元数。在串口异步通信中，由于没有时钟信号，双方需要协商一致的波特率以便正确解码信号。常见的波特率有 4800、9600、115200 等。
3. 数据校验：数据校验是一种错误检测机制，旨在识别数据在传输过程中可能出现的错误。
   - 奇校验：要求有效数据加校验位中“1”的总数为奇数。
   - 偶校验：要求有效数据加校验位中“1”的总数为偶数。
   - 空格校验（0 校验）和标记校验（1 校验）：无论有效数据如何，校验位始终设定为“0”或“1”。

**【实验设备】**

1. 串口线

**【实验步骤】**

1. 观测计算机连接端口，尤其是 DB 连接器。
2. 查看串口连接线端子（公母头）及引脚编号对照前面信号定义。
3. 思考串口通信过程。
4. 由于实验条件所限（缺乏焊接设备，端子部件等），本实验不进行制作串口电缆。

**【分析讨论】**

**一、直通连接和交叉连接的不同**

直通连接（Straight-through connection）：直通连接线用于连接不同类型

的设备，例如将计算机连接到交换机或路由器。在这种连接中，一端的发送（Tx）针脚直接连接到另一端的接收（Rx）针脚，因此数据可以直接从一个设备传输到另一个设备。

交叉连接（Crossover connection）：交叉连接线用于连接两台相同类型的设备，如两台计算机或两台交换机。在这种连接中，一端的发送针脚连接到另一端的接收针脚，反之亦然。这意味着数据从一台设备的发送端传输到另一台设备的接收端，反之亦然，从而允许两个设备直接通信。

**二、两台 PC 连接需要直通连接线还是交叉连接线？**

现代网络设备，包括个人计算机和笔记本电脑，通常都支持自动协商功能，这意味着它们可以自动识别连接类型并相应地调整。因此，在大多数情况下，使用直通线即可。但是，在老旧的设备上，如果两台 PC 需要直接连接通信，通常需要使用交叉连接线。随着技术的发展，这一需求已大大减少。

**三、串口连接至少需要几根线？**

串口通信至少需要三根线：发送线（TX）、接收线（RX）和地线（GND）。发送线和接收线用于数据的双向传输，而地线用于提供参考电位，确保数据正确无误地传输。

**四、两个串口交叉线，每根串口线端子是一公一母，如需一根直通线，如何制作？**

要将两个串口的交叉连接线改造为一根直通线，需要确保一端的发送（TX）针脚连接到另一端的发送针脚，接收（RX）针脚连接到另一端的接收针脚，同时保持地线（GND）相连。如果每根线的端子分别是一公一母，可以按以下步骤操作：

1. 准备工作：准备线缆剥皮器和焊接工具。
2. 剪断线缆：将交叉线剪断，分别剥离两端的外皮，暴露内部的 TX、RX 和 GND 线。
3. 重新连接线缆：将一端的 TX 线连接到另一端的 TX 线，将一端的 RX 线连接到另一端的 RX 线，确保 GND 线也相连。
4. 焊接和绝缘：使用焊接工具将线焊接好后，使用绝缘胶带或热缩管对每个连接点进行绝缘处理，以避免短路。
5. 测试：在连接设备之前，先进行测试，确保所有连接正确无误。

# 实验 07：异步串口通信收发实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/14 |

**【实验目的】**

1. 深入了解串口与并口的工作原理和应用场景，包括它们的物理连接方式、通信协议、信号电平和数据传输速度。
2. 掌握串口和并口在数据传输中的优缺点，通过对比分析，了解它们在不同应用场景下的适用性。
3. 通过实际操作和观测，加深对串口通信特性和并口通信特性的理解，包括参数配置对数据传输速度、延迟和效率的影响。
4. 实践串口通信的配置和数据传输过程，包括硬件连接、软件配置、数据传输和参数调整，以及观测和记录实验现象和结果。
5. 分析和讨论实验过程中遇到的问题和现象，例如不同串口参数配置下的通信效果，以及使用不同软件进行通信的可行性和原理。

**【实验原理】**

**一、串口（Serial Port）**

1. 物理连接：在 PC 系统中，串口的物理连接方式主要有 9 针和 25 针两种。随着 PC 技术的发展，25 针的串口逐渐被淘汰，目前串口都采用 9 针的连接方式直接集成在主板上。一般的 PC 主板都提供两个串口：COM1 和 COM2。这些串口能够达到最高 115Kbps 的数据传输速度，而增强型串口如 ESP（Enhanced Serial Port）和 Super ESP（Super Enhanced Serial Port）则能达到 460Kbps 的数据传输速率。
2. 通信协议：串口通常使用 RS232 接口作为通信协议，由美国电子工业协会（EIA）于 1970 年制定。RS232 接口是一种用于串行二进制数据交换的技术标准，它规定了一个 25 个脚的 DB25 连接器，并对各种信号的电平进行了规定。随着时间的发展，出现了代替 DB25 的 DB9 接口。
3. 数据传输方式：串口采用串行传输方式，即一次只能传输一个数据位，这种方式虽然在速度上不如并行传输，但能用于比并行口更远距离的数据传输。

**二、并口（Parallel Port）**

1. 物理连接：并口通常使用 25 针的连接方式，也被称为 LPT 接口。并口的数据传输率比串口快 8 倍，标准并口的数据传输率为 1Mbps，通常用来连接打印机、扫描仪等。因此，并口又被称为打印口。
2. 数据传输方式：并口使用并行通信协议，允许多个数据位同时传输，这使得并口在数据传输速度上具有优势，适用于短距离高速数据传输。

**三、串口特性**

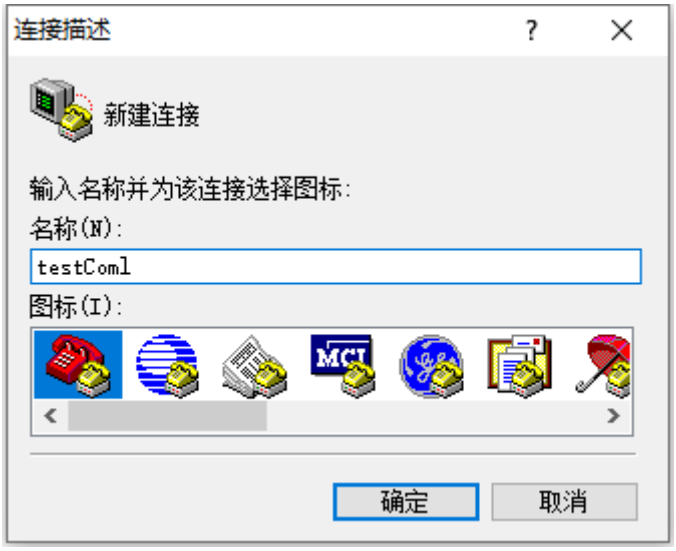
1. 信号电平：RS232 接口采用负逻辑电平，其中-15V 到-3V 表示逻辑 1，+15V 到+3V 表示逻辑 0。电压值通常在 7V 左右。这种负逻辑电平的采用，对于确定数据传输中逻辑状态的识别具有重要意义。
2. 接口引脚：RS232 接口标准定义了多个引脚用于不同的通信功能，例如 DCD（载波检测）、RXD（接收数据）、TXD（发送数据）、DTR（数据终端准备好）、DSR（数据准备好）、RTS（请求发送）、CTS（清除发送）和 RI（振铃提示）。这些引脚的设计使得串口通信能够支持复杂的控制信号交换，增强了通信的可靠性和灵活性。

**【实验设备】**

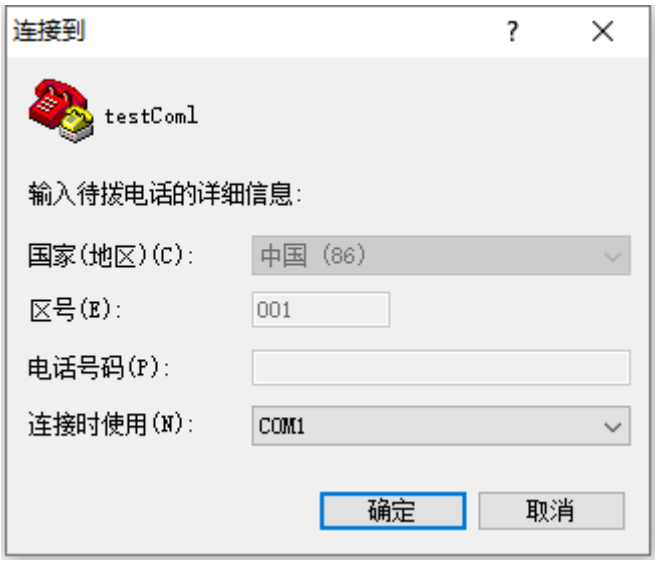
1. 装有 Windows 10 操作系统和超级终端应用程序的 PC 机两台
2. 串口线一条

**【实验步骤】**

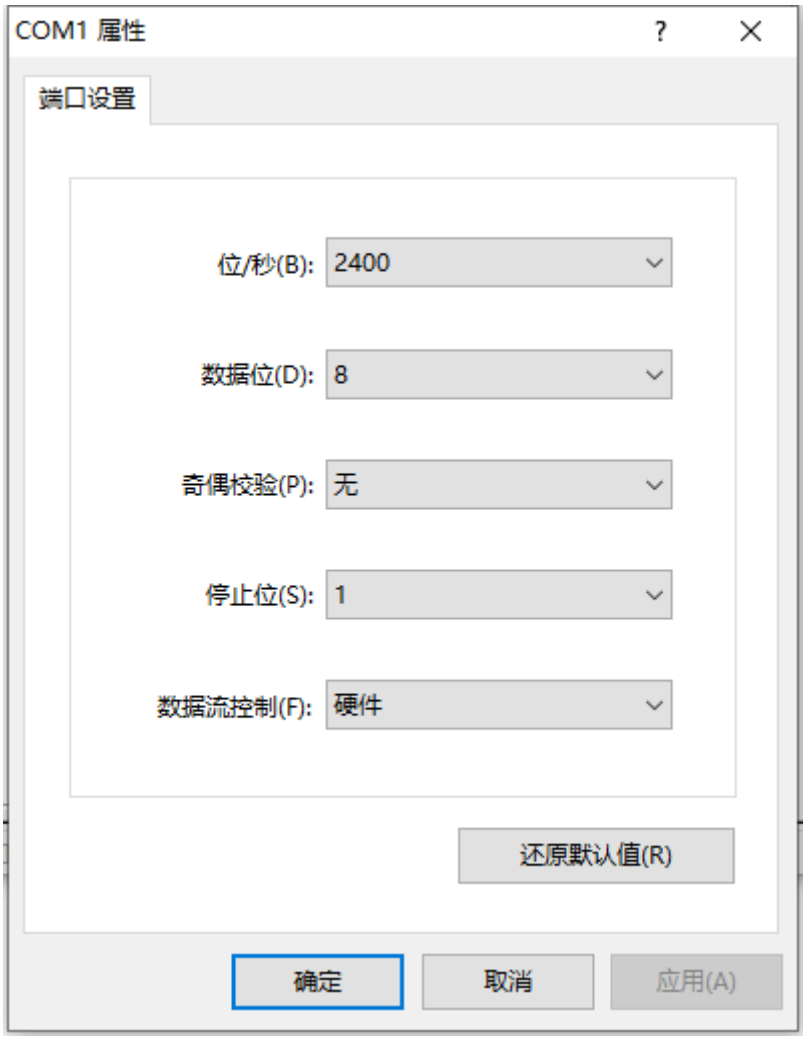
1. 使用串口线将两台装有 Windows 10 操作系统的 PC 机连接。
2. 在两台 PC 机上打开应用程序超级终端，并新建连接。



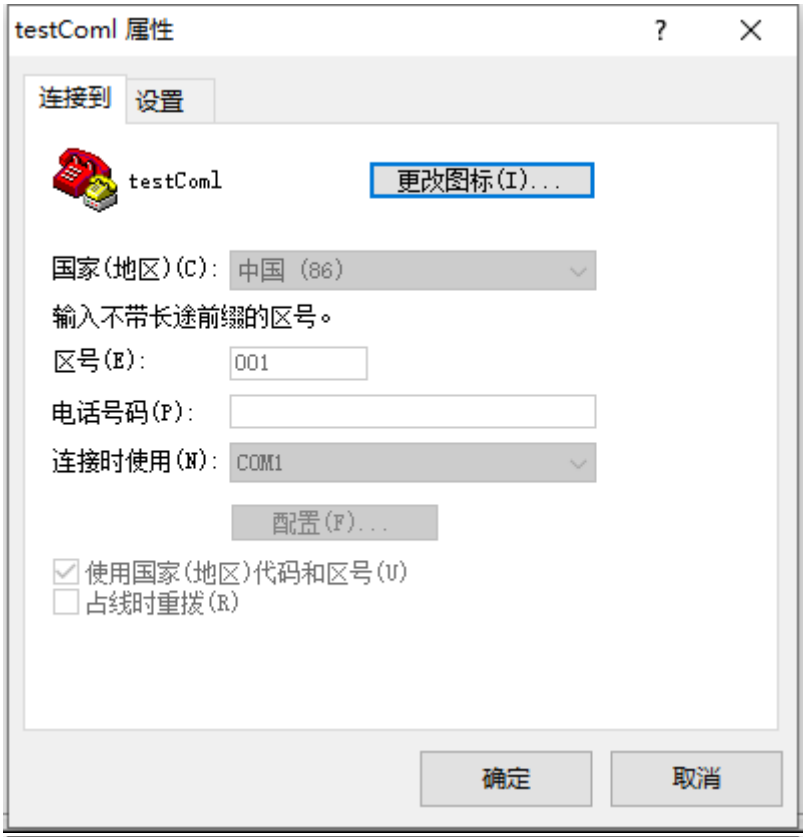
3. 在“连接到”窗口中，选择连接时使用“COM1”。

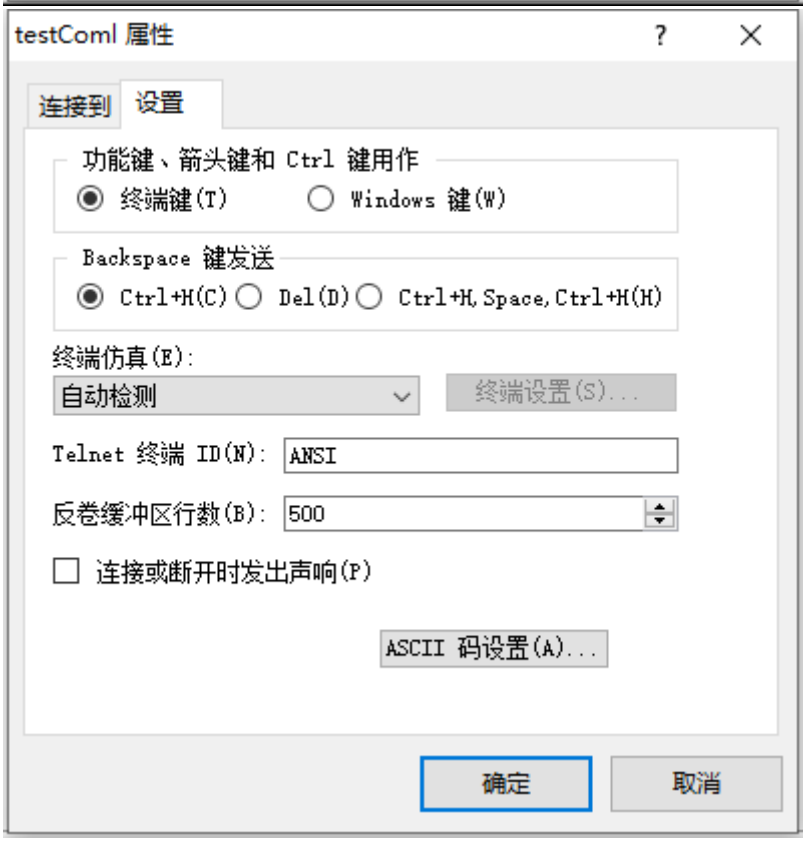



4. 在“COM1 属性”窗口中，进行如下设置。




5. 在“testCom1 属性”窗口中，进行如下设置。



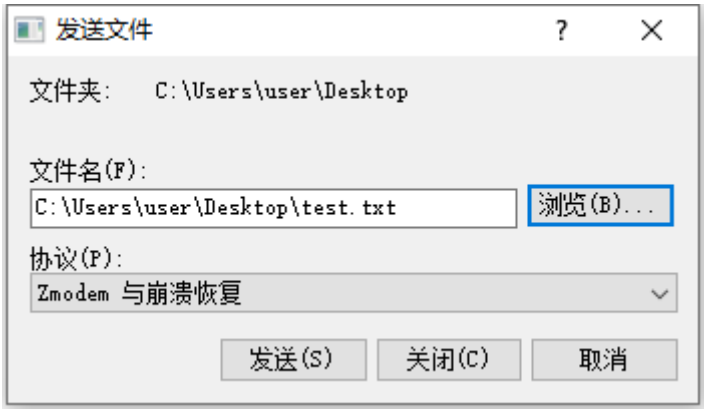



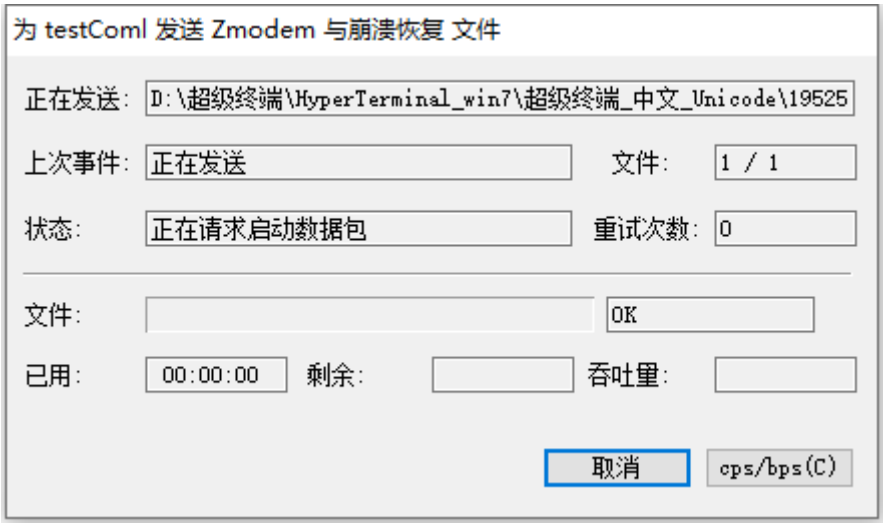

6. 点击“确定”，在超级终端“传送”选项卡中，分别选择“发送文件”、“接收文件”、“捕获文字”、“发送文本文件”，观察超级终端表现和文件传输特性。

**【实验现象】**

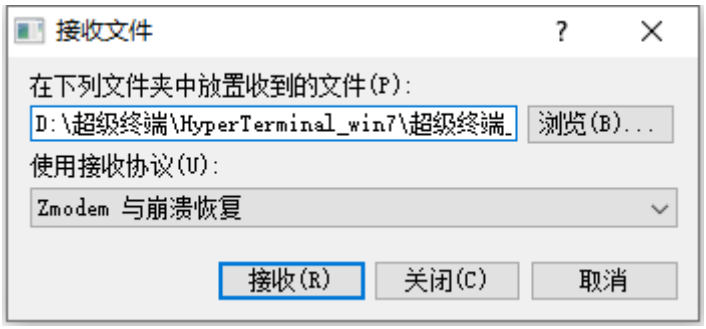
1. 当两台 PC 机的数据位设置为 8 位、奇偶校验设置一致（无论是奇校验、偶校验或无校验），以及停止位设置相同时， 发送文件、接收文件、捕获文字与发送文本文件均成功，即串口通信成功。这是因为数据位的一致性确保了双方能准确地解码对方发送的字符或命令；奇偶校验的一致性使得双方能同步地进行错误检测和纠正；而停止位的一致性则确保了双方能准确地识别字符或命令的结束，从而实现有效的数据传输。

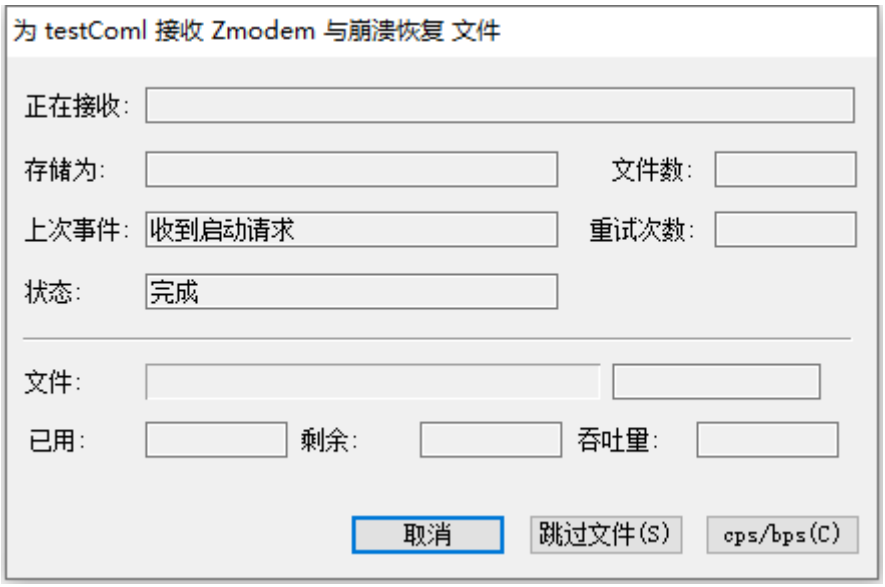
- “发送文件”实验现象



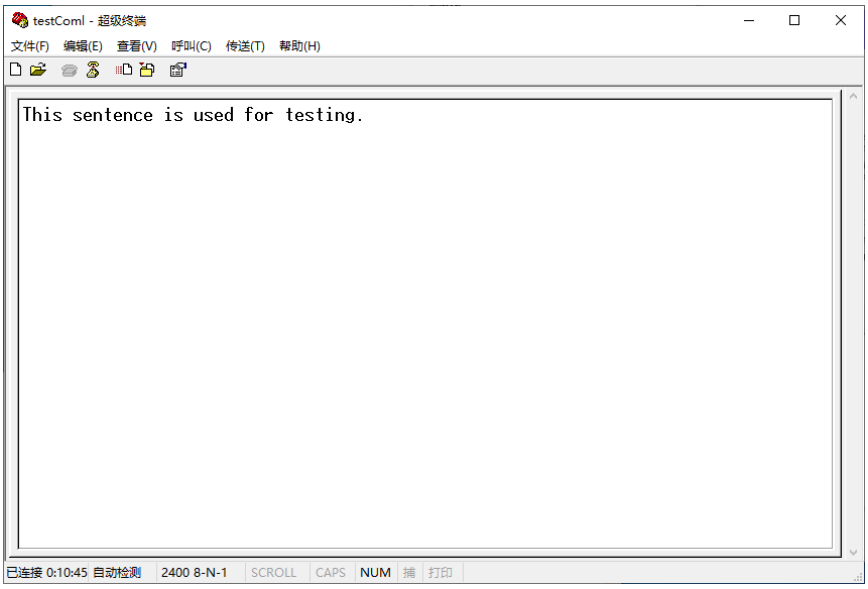




- “接受文件”实验现象

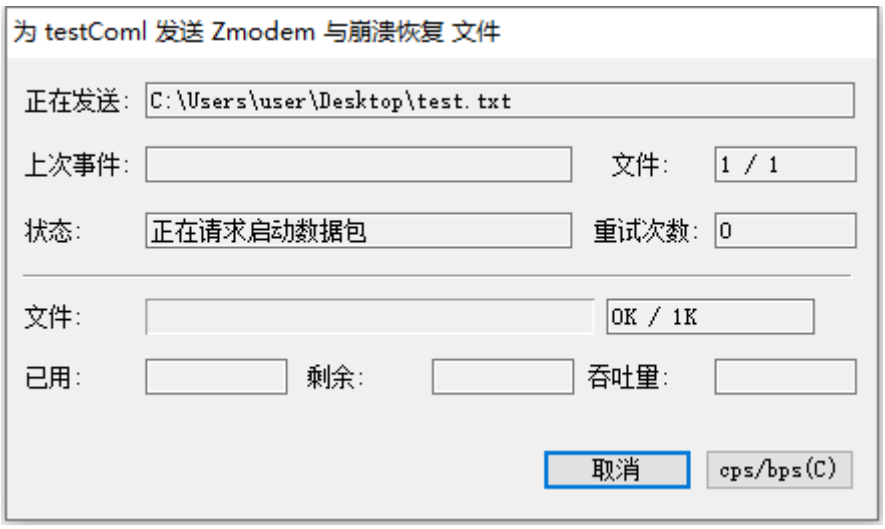





- “捕获文字”实验现象




- “发送文本文件”实验现象



2. 当两台 PC 机的上述三个条件（数据位、奇偶校验、停止位）有任何一个不一致时，串口通信失败。这是因为数据位的不匹配会导致接收端无法准确解码发送端的字符或命令，从而产生数据传输错误；奇偶校验的不一致会导致两台电脑无法同步进行错误检测和纠正，可能产生数据错误；而停止位的不匹配则会导致两台电脑无法准确识别字符或命令的结束，从而导致数据传输中断或错误。

**【分析讨论】**

**一、实验现象分析**

1. 成功的串口通信：当两台 PC 机的数据位、奇偶校验以及停止位设置一致时，实验能够成功进行，包括发送文件、接收文件、捕获文字和发送文本文件。这说明了串口通信的成功依赖于双方通信设置的一致性。
2. 串口通信失败的情况：当数据位、奇偶校验、或停止位中任何一个参数设置不一致时，串口通信失败。这种失败表明了参数设置的不匹配会直接影响数据的正确传输，导致通信中断或错误。

**二、实验讨论**

1. 本实验明确显示了进行串口通信前，双方必须确保通信参数的一致性。这不仅包括硬件连接的正确配置，还包括软件设置中的参数调整。因此，通信双方的预先协商和设置检查是保证数据传输成功的关键步骤。
2. 串口通信中奇偶校验的设置对于错误检测和纠正至关重要。本实验中，奇偶校验的一致性使得双方能够有效地进行错误检测和纠正，这表明在不可靠的传输媒介上进行通信时错误检测和纠正机制十分重要。
3. 虽然串口通信技术相对较老，但其在远距离通信、系统维护、以及设备控制等领域仍然具有应用价值。实验中观察到的现象和问题，如通信参数设置的一致性、错误检测和纠正，都是实际应用中需要考虑的重要因素。

# 实验 08：IOS 的基本操作（路由器的基本操作）实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/21 |

**【实验目的】**

1. 深入理解实验网络的物理组网原理：通过本实验学习网络中硬件设备如何通过物理介质（例如电缆）连接，并了解这些连接是如何构建一个功能完整的网络系统的。
2. 掌握设备间的连接策略及其作用：实验将介绍不同网络设备（如路由器和交换机）的功能，以及选择适当的物理介质（如双绞线、光纤）和拓扑结构（如总线、星形）的重要性。
3. 熟悉并掌握路由器操作系统 IOS 的基本操作：本实验的核心目标是熟悉 Cisco 路由器和交换机的核心软件—IOS（Internetwork Operating System），包括命令行接口（CLI）的使用、配置模式的理解、文件管理及故障排查工具的应用。
4. 确保未来的网络配置和管理工作能够高效地运用这些知识与技能：通过对 IOS 的基本操作的学习和实践，学生将能够在将来的网络工作中高效地使用这些技能进行网络配置和管理。

**【实验原理】**

**一、实验网络的物理组网原理**

1. 设备角色定义：网络中的每个设备都扮演着特定的角色，执行不同的功能。例如，路由器负责在不同网络之间转发数据包，而交换机则负责在同一个局域网内转发数据帧。
2. 物理介质选择：网络设备之间的连接依赖于物理介质，如双绞线、光纤或无线信号。每种介质具有其特定的传输速度、距离限制和适应环境。
3. 拓扑结构：网络的物理或逻辑布局，常见的拓扑结构包括总线、星形、环形和网状结构。拓扑结构影响了网络的性能和可靠性。

**二、路由器操作系统（IOS）的基本操作**

Cisco 的 IOS（Internetwork Operating System）是运行在 Cisco 路由器和交换机上的操作系统，类似于计算机上的 Windows 或 Linux 操作系统，但专门设

计用于网络设备。IOS 负责运载网络协议和功能，连接产生高速流量的设备，增加网络安全性，提供网络的可扩展性以简化网络的增长和解决冗余问题，以及可靠地连接网络资源。

1. 命令行接口（CLI）：IOS 的主操作环境，通过输入命令来查询信息或更改配置。
2. 配置模式：IOS 中存在多种配置模式，如全局配置模式、接口模式等，每种模式都有其特定的命令集，用于完成相应的配置任务。
3. 文件管理：IOS 允许对设备上的文件进行管理，包括配置文件和 IOS 映像文件的保存、备份和恢复。
4. 故障排查工具：IOS 提供了多种工具和命令（如 ping、traceroute 和 show 命令），以帮助管理员诊断和解决网络问题。

**三、IOS 配置方法**

配置 Cisco IOS 可以通过多种方式进行：

1. CONSOLE 口：使用 PC 的 COM 口直接连接到路由器的控制台口，用于本地配置。
2. MODEM 连接 aux 口：通过 MODEM 连接到辅助（aux）口，用于远程配置。
3. VTY 线路：通过网络使用 telnet 进行远程访问。
4. TFTP 下载配置文件：通过 TFTP 协议下载或上传配置文件。

一般情况下，最常用的配置方法是通过控制台口和 telnet。

**四、IOS 启动过程**

启动过程包括：

1. 加电自检（POST）：开机后进行硬件自检。
2. 载入 IOS：从闪存（flash memory）查找并加载 IOS 到 RAM 中。
3. 运行配置文件：在非易失性存储器（NVRAM）中查找启动配置文件（startup-config）。如果未找到任何启动配置文件，路由器将进入 setup 模式。

**五、IOS 引导和配置模式**

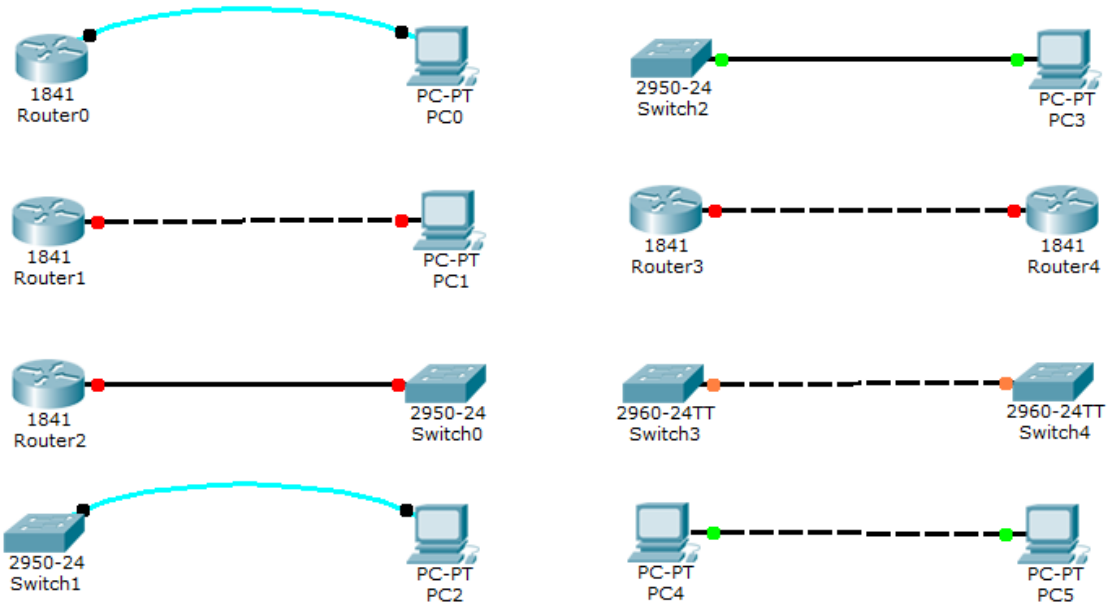
Setup 模式：初次配置路由器时的简化模式。尽管它提供了一种配置路由器的方式，但通常推荐使用命令行界面（CLI）进行更详细的配置。

## 六、路由器操作模式

1. 用户模式（>提示符）：提供有限的命令集，用于查看路由器状态。
2. 特权模式（#提示符）：通过输入 enable 从用户模式进入，提供查看和修改配置的能力。
3. 全局配置模式（(config)#提示符）：从特权模式通过 configure terminal 命令进入，用于修改路由器的全局设置。
4. 接口模式（(config-if)#提示符）：在全局配置模式下通过 interface 命令进入，用于配置特定接口。
5. 子接口配置模式（(config-subif)#提示符）：用于配置虚拟接口。
6. 线路配置模式（(config-line)#提示符）：用于配置控制台、telnet 和其他线路接口。
7. 路由配置模式（(config-router)#提示符）：用于配置路由协议。

## 七、连接基本原则

1. 同种类型的设备之间（如路由器到路由器）使用交叉线连接，而不同类型的设备（如路由器到交换机）使用直通线连接。
2. 路由器和 PC 属于数据终端设备（DTE），而交换机和 HUB 属于数据通信设备（DCE）。
3. 使用 RJ45 网络接头时，有两种标准制作方法（568A 和 568B），同一标准制作的是直通线，不同标准制作的是交叉线。



**【实验设备】**

1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

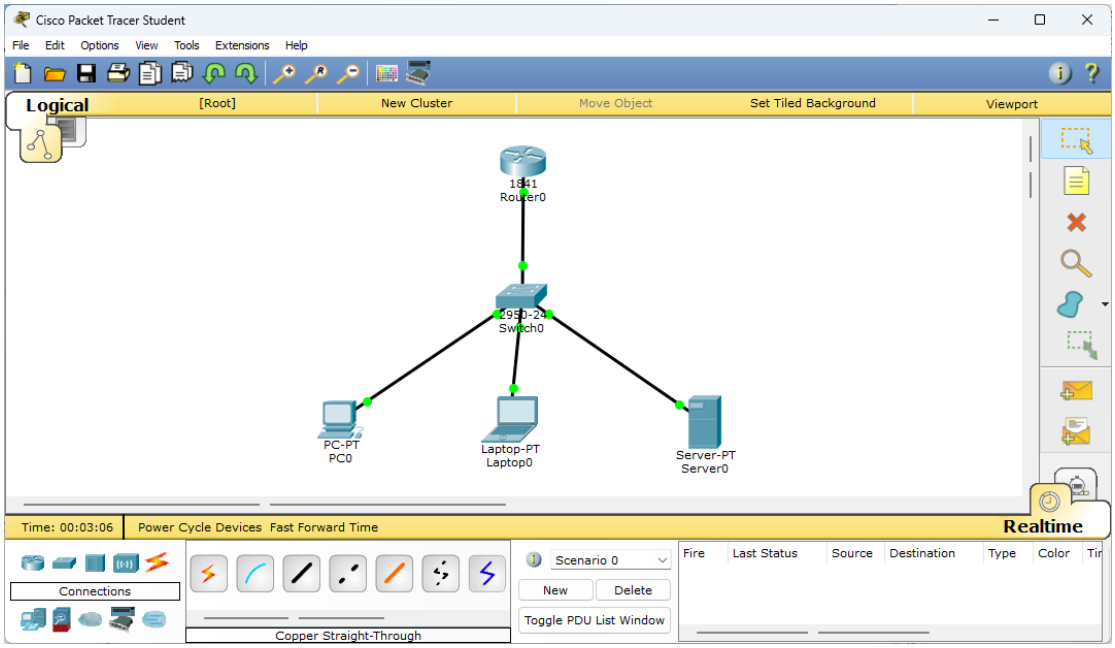
1. 启动 Cisco Packet Tracer，并使用软件提供的虚拟设备（如路由器、交换机、PC 等）来模拟网络环境。
2. 配置 IOS
   - 控制台配置：使用 USB 转串口线或直接的串口线将 PC 的 COM 口与路由器的 CONSOLE 口连接。使用终端仿真程序（如 PuTTY 或 Tera Term）通过控制台接口配置路由器。
   - MODEM 配置：通过 MODEM 连接到路由器的 aux 口进行远程配置。
   - Telnet 配置:使用 VTY 线路通过网络使用 telnet 命令远程访问路由器。
   - TFTP 配置：使用 TFTP 服务器下载或上传路由器的配置文件。
3. 学习 IOS 的启动过程和配置模式
4. 在路由器上配置不同的接口模式
   - 用户模式（查看状态）：直接进入 CLI 环境即处于用户模式。
   - 特权模式（查看配置和路由信息）：输入 enable 命令从用户模式切换到特权模式。
   - 全局配置模式（基本配置）：在特权模式下输入 configure terminal 进入。
   - 接口模式（配置接口）：例如配置以太网接口，使用 router(config)# interface ethernet 0。
   - 子接口配置模式：例如配置子接口，使用 router(config)#interface fastethernet 0/0.1。
   - 线路配置模式：例如配置 console 线，使用 line console 0 命令。
   - 路由配置模式：例如配置 RIP 协议，使用 router(config)#router rip 命令。
5. 接口操作

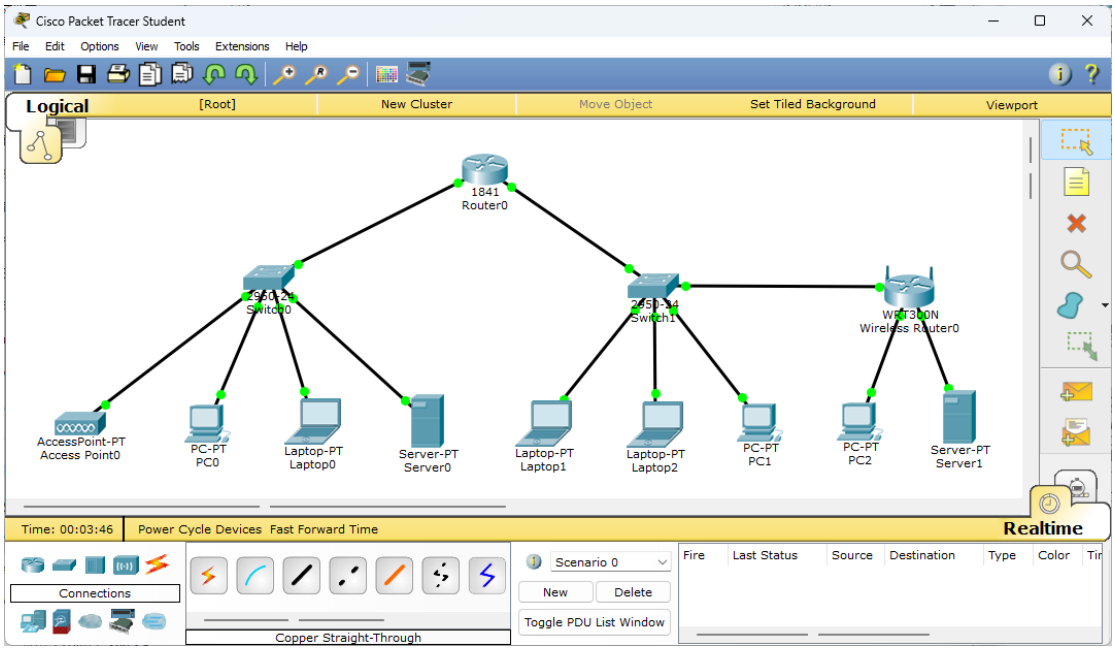
- 使用 no shut 命令启用接口。
- 使用 end 命令从任何配置模式返回到特权模式。

6. 连接路由器、交换机和 PC：遵循连接基本原则，使用直通线连接不同类型的设备（如路由器到交换机，PC 到交换机），使用交叉线连接同类型的设备（如路由器到 PC）。

**【实验现象】**

各项配置好后，绿灯亮起，使用 ping 命令可以接收到消息。




**【分析讨论】**

通过本实验，不仅深化了对网络物理组网原理的理解，也熟悉了 Cisco 路由器操作系统 IOS 的基本操作和配置模式。本实验突出了 IOS 为 Cisco 设备带来的强大配置和管理能力，展示了通过控制台、MODEM、Telnet、TFTP 等多样化配置方法来满足不同配置需求的重要性。同时，实验中的网络设备连接实践强调了在进行物理连接时需注意设备类型及线缆种类的选择，以确保网络连接的正确性和高效性。此外，通过使用 Cisco Packet Tracer 软件，本实验提供了一个模拟环境，使我们得以在不影响真实网络系统的条件下，练习和加深对 IOS 操作的理解。这样的模拟实践对于加强理论知识与实际操作技能的融合至关重要。

# 实验 09：VLAN 配置实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/21 |

**【实验目的】**

本次实验的目的是掌握 VLAN 的基本原理并了解如何在交换机上配置 VLAN，通过实验加深对 VLAN 的理解并掌握相关配置命令。实验涉及到虚拟局域网（VLAN）的配置，将地理位置上分散的主机集合到同一个局域网中，利用以太网交换机的软件特性进行逻辑上的分组，以形成独立的物理网络。此次实验旨在通过实际配置和测试，使学生能够熟练掌握 VLAN 的配置方法和原理。

**【实验原理】**

**VLAN 的原理**

VLAN（Virtual Local Area Network，虚拟局域网络）的原理基于通过软件将网络按逻辑分组的概念。VLAN 的实现使得不同地理位置的主机可以被分割到相同的 VLAN 内，即使它们连接在不同的物理交换机上。

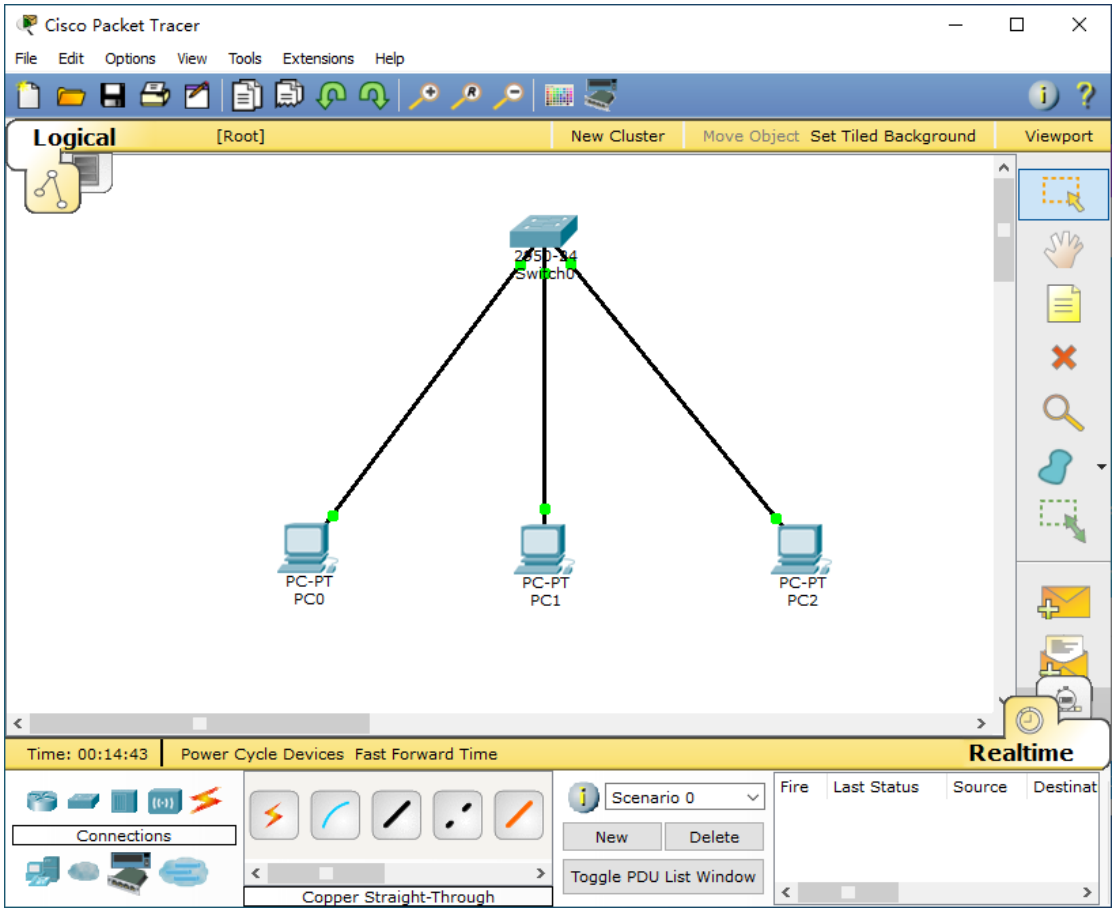
VLAN 通过软件配置，而非物理连接，来划分网络。这允许网络管理员根据需要（例如部门、项目组或应用类型）灵活地组织设备，而不受物理位置的限制。在传统的局域网中，广播消息会发送给同一网络段内的所有设备，无论是否需要。VLAN 技术可以将大的广播域划分成较小的片段，每个 VLAN 内部处理自己的广播流量，减少了不必要的广播传输，提高了网络的效率。VLAN 之间的通信默认是隔离的。这意味着，不同 VLAN 的设备不会看到对方的数据，除非通过特定的路由配置允许这种通信。这种隔离增强了网络安全性，可以有效防止潜在的数据泄露和未授权访问。

**【实验设备】**

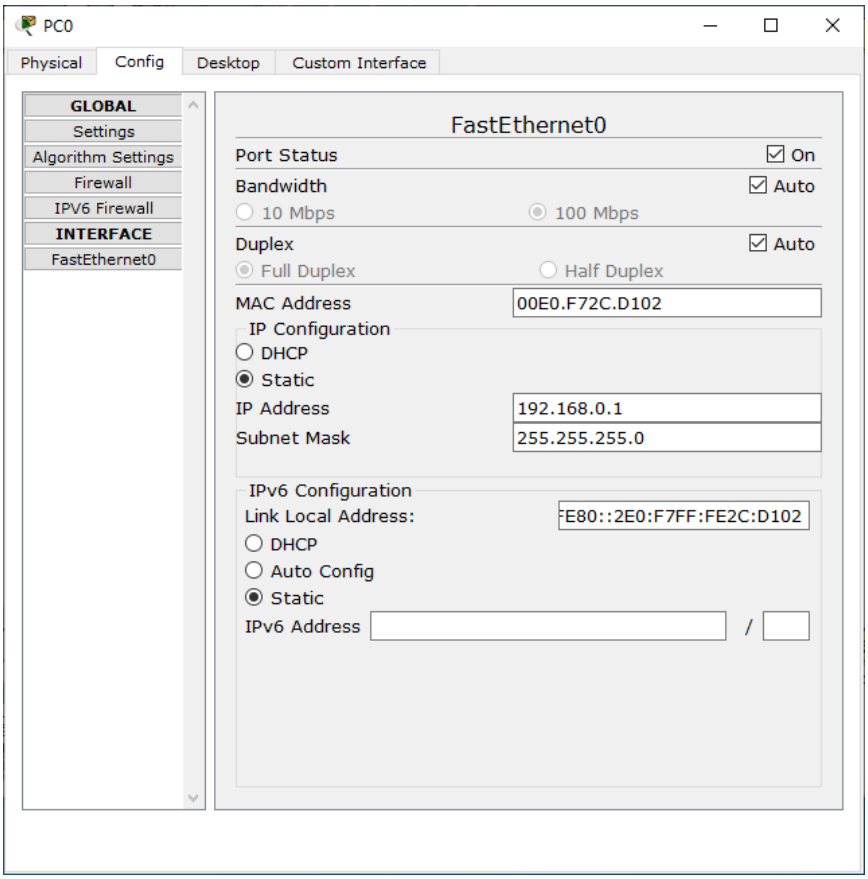
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

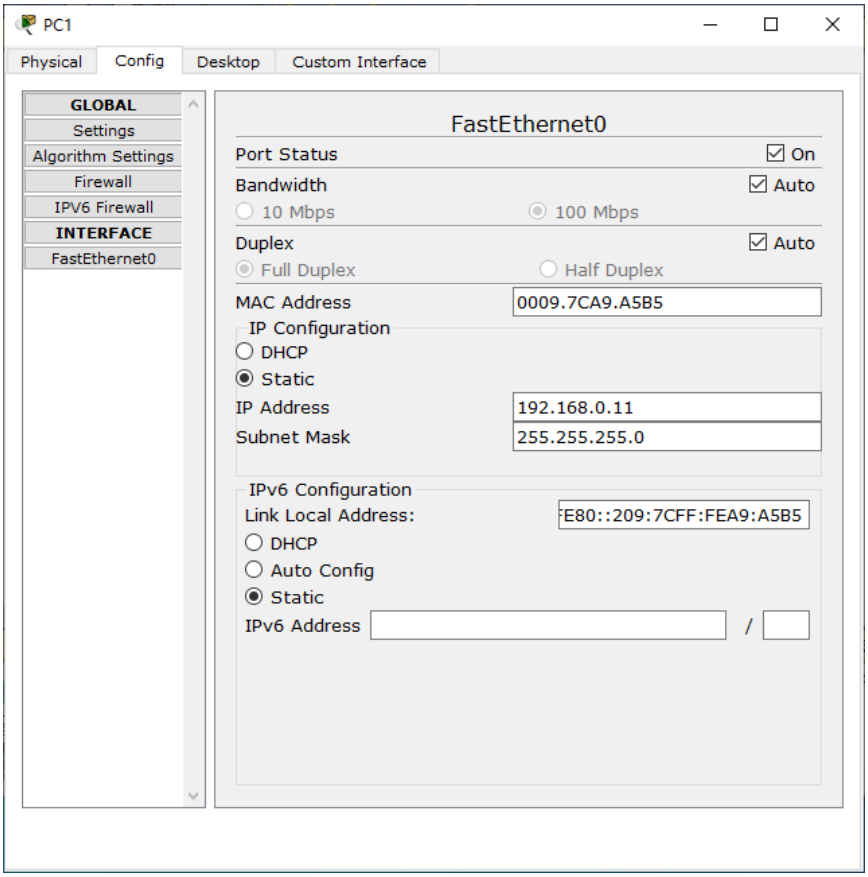
**【实验步骤】**

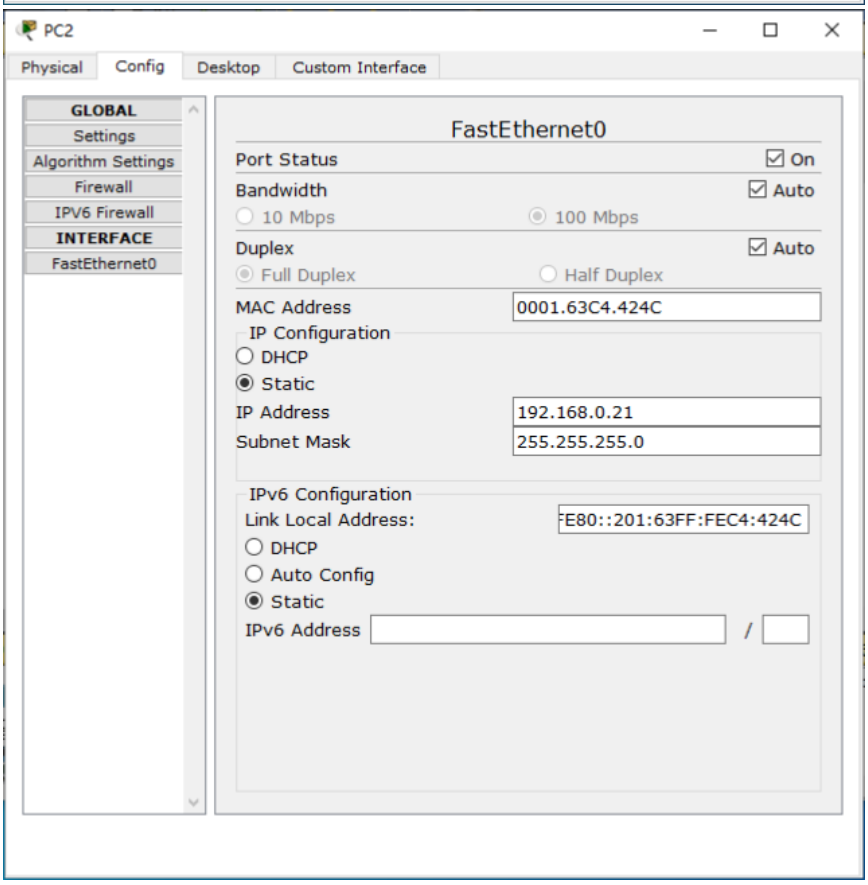
1. 启动 Cisco Packet Tracer 来模拟网络环境。
2. 连接设备。




3. 通过 Config 图形化界面为三台 PC 机配置 IP 及掩码。






4. 通过图形化界面，为 PC0/PC1/PC2 分别配置 VLAN10，VLAN20，VLAN30。

- PC0 配置：192.168.1.1 mask 255.255.255.0 F0/1 VLAN 10
- PC1 配置：192.168.1.11 mask 255.255.255.0 F0/2 VLAN 20
- PC2 配置：192.168.1.21 mask 255.255.255.0 F0/3 VLAN 30

5. 测试：PC0，PC1，PC2 之间相互 ping，查看并记录实验结果。

**【实验现象】**

用 PC0 分别 ping PC1、PC2，用 PC1 分别 ping PC0、PC2，用 PC2 分别 ping PC1、PC0，均请求失败。

**【分析讨论】**

在本次 VLAN 配置实验中，实验结果显示所有尝试在不同 VLAN 间的 ping 请求均失败，这与 VLAN 的基本原理和目的紧密相连。

VLAN 技术的核心在于通过逻辑上分组网络来实现隔离。每个 VLAN 形成了一个独立的广播域，限制了广播流量只在同一个 VLAN 内传播。这种隔离保证了不同 VLAN 间默认不允许直接通信，加强了网络的安全性和管理的灵活性。因此，即使 PC0、PC1 和 PC2 连接到同一交换机，它们被配置在不同的 VLAN（VLAN10、VLAN20、VLAN30）中导致它们之间无法直接通信。

实验中所有 ping 请求的失败正是 VLAN 隔离性原理的直接体现。这表明，在物理网络中成功创建了逻辑隔离，每个 VLAN 内部可以正常通信，但 VLAN 间的通信被默认阻断。这种行为符合 VLAN 设计的预期，验证了 VLAN 配置的正确性和功能的实现。

VLAN 通过将大的物理广播域划分为多个逻辑广播域，有效地减少了不必要的广播流量，提升了网络的性能和安全性。在这种配置下，每个 VLAN 内部的广播消息不会传播到其他 VLAN，这有助于控制广播风暴并保护网络不受未授权访问的影响。

确保实验的有效性和完整性需要仔细检查和确认每项配置。每台 PC 的 IP 地址、子网掩码和 VLAN 配置必须正确，交换机的 VLAN 配置需要准确无误，确保每个端口正确地分配到了对应的 VLAN。任何配置错误都可能导致通信失败或不符合预期的实验结果。

# 实验 10：静态路由配置实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/28 |

**【实验目的】**

1. 掌握静态路由的基本原理：通过本实验，深入理解静态路由的定义、工作机制以及如何在网络中应用。静态路由作为一种预设的、不随网络状况动态改变的路由选择方法，其稳定性和可靠性在特定场景下非常重要。
2. 学习静态路由的配置命令：实验的一个重要部分是通过实践学习和掌握在不同网络设备上配置静态路由的具体命令。这包括如何为路由器接口设置 IP 地址、启用端口、配置目标网段和下一跳地址等关键配置步骤。
3. 理解静态路由的优缺点：通过对比分析，了解静态路由相比于动态路由的优势和局限。例如，静态路由在网络安全性和可控性方面的优点，以及在大型或复杂网络环境中的局限性。
4. 实际操作静态路由的配置：通过在模拟或实际网络环境中配置静态路由，获得实际的操作经验。这不仅包括路由配置的步骤，还包括对配置结果的验证和问题排错。
5. 验证静态路由的通信功能：实验的最后一步是验证配置的静态路由是否能够成功地指导网络流量。通过测试网络中不同节点间的通信，学生可以直观地看到静态路由配置是否正确，以及它是如何影响数据包的传输路径的。

**【实验原理】**

**一、静态路由的原理**

静态路由是网络路由的一种基本形式，其中路由信息是由网络管理员手动配置的，而非通过动态路由协议自动发现和更新。这意味着，无论是指定数据包的转发路径还是定义目的地网络与下一跳地址的映射，都需要管理员直接介入。

在网络的拓扑结构或链路状态发生变化时，静态路由不会自动更新。任何必要的路由信息修改都需要管理员手动进行。静态路由通常适用于结构相对简单、稳定的网络环境，其中网络的拓扑结构较为固定，便于管理员理解和配置。

**二、静态路由的优缺点**

与动态路由相比，静态路由由于不需要路由器之间频繁交换路由信息，因而

能更好地保护网络的拓扑结构和地址信息不被外泄，从而提高网络的安全保密性。

在大型或复杂的网络环境中，维护静态路由表可能非常困难。网络管理员可能难以全面掌握网络的拓扑结构，且当网络结构或链路状态发生变化时，需要手动进行大量的调整，增加了管理的难度和复杂度。

**三、静态路由的配置命令**

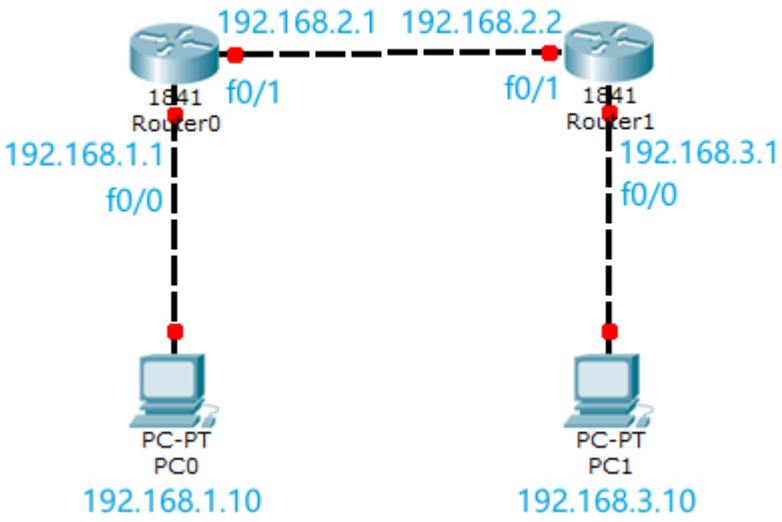
1. 设置 IP 地址和子网掩码：ip address [IP 地址] [子网掩码]
2. 启用端口：No shutdown
3. 指定目标网段、子网掩码和下一跳地址：ip route [目标网段 IP 地址] [目标子网掩码] [下一跳地址]
4. 指定目标网段、子网掩码和送出接口：ip route [目标网段 IP 地址] [目标子网掩码] [接口]
5. 查看路由配置情况：show ip route

**【实验设备】**

1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

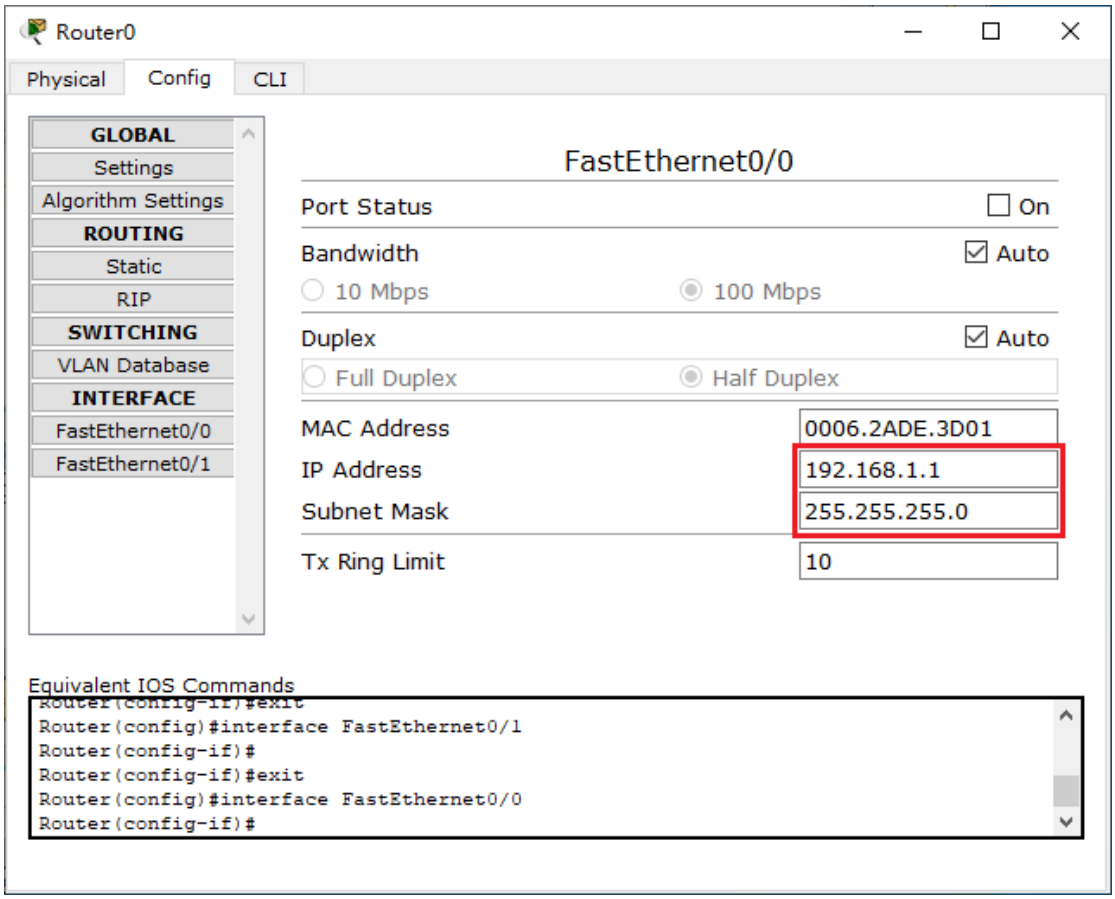
1. 启动 Cisco Packet Tracer 来模拟网络环境。
2. 按照如下拓扑图连接设备，子网掩码是 255.255.255.0，PC0 的网关是 192.168.1.1，PC1 的网关是 192.168.3.1。

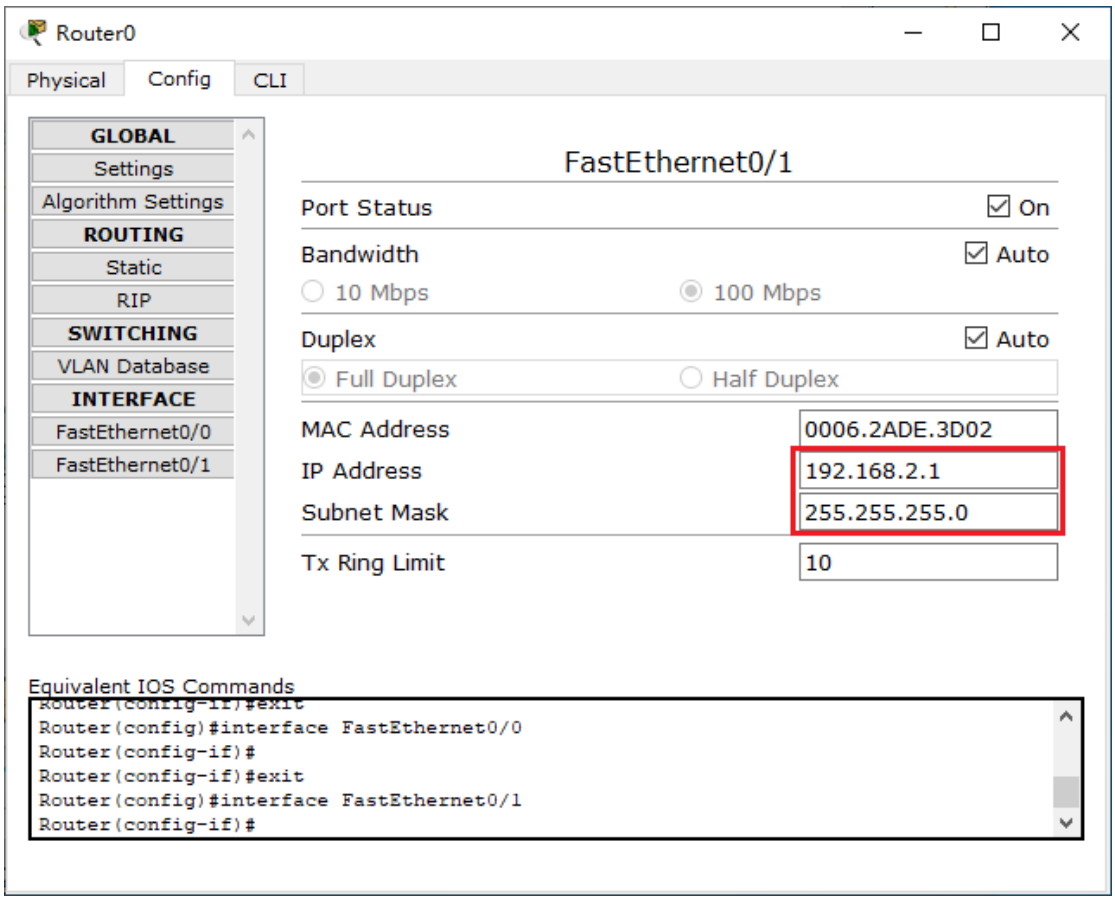


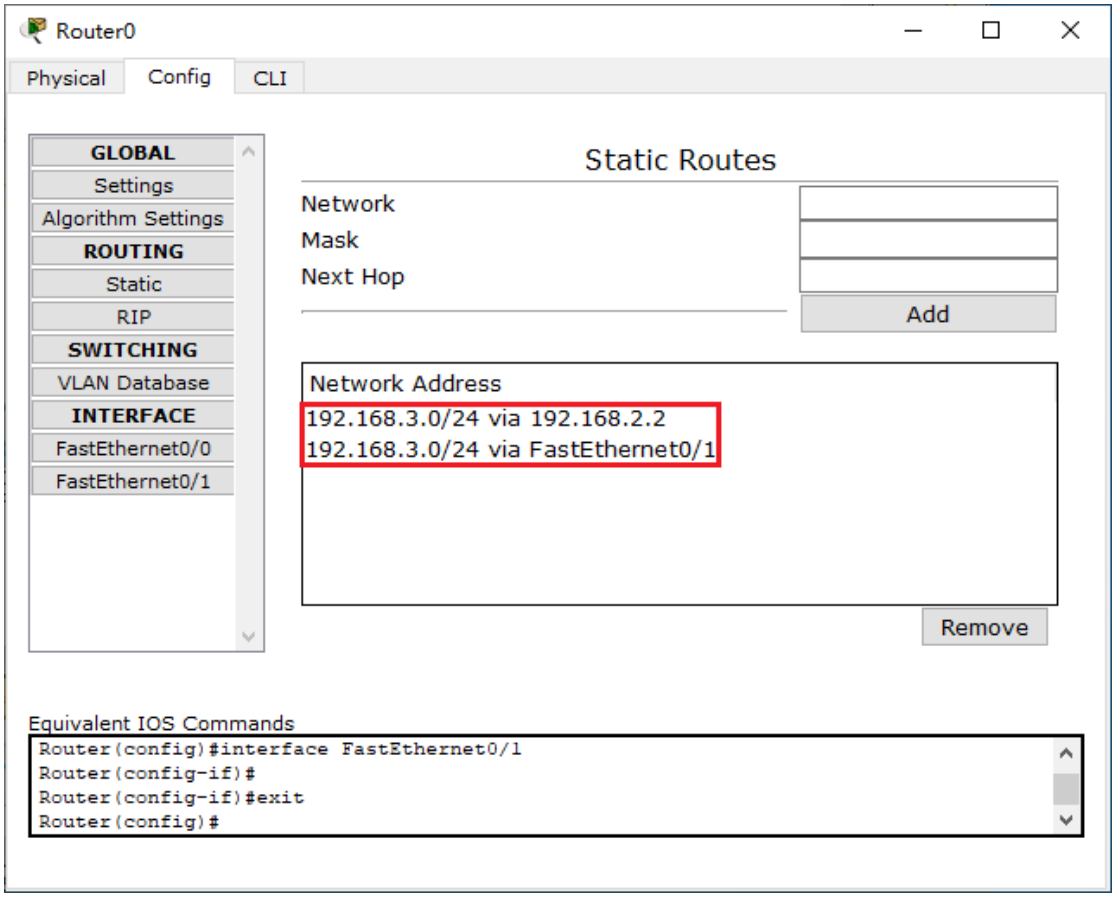
3. 配置路由器 Router0。

- FastEthernet0/0 接口配置 IP 地址为 192.168.1.1，子网掩码为 255.255.255.0。
- FastEthernet0/1 接口配置 IP 地址为 192.168.2.1，子网掩码为 255.255.255.0。
- 添加静态路由：要到达 192.168.3.0/24 网络应该通过 192.168.2.2，要到达 192.168.3.0/24 网络，应该通过 f0/1 接口。
- 也可以通过 CLI 窗口输入命令进行配置：

```
interface f0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
interface f0/1
ip address 192.168.2.1 255.255.255.0
no shutdown
ip route 192.168.3.0 255.255.255.0 192.168.2.2
ip route 192.168.3.0 255.255.255.0 f0/1
```



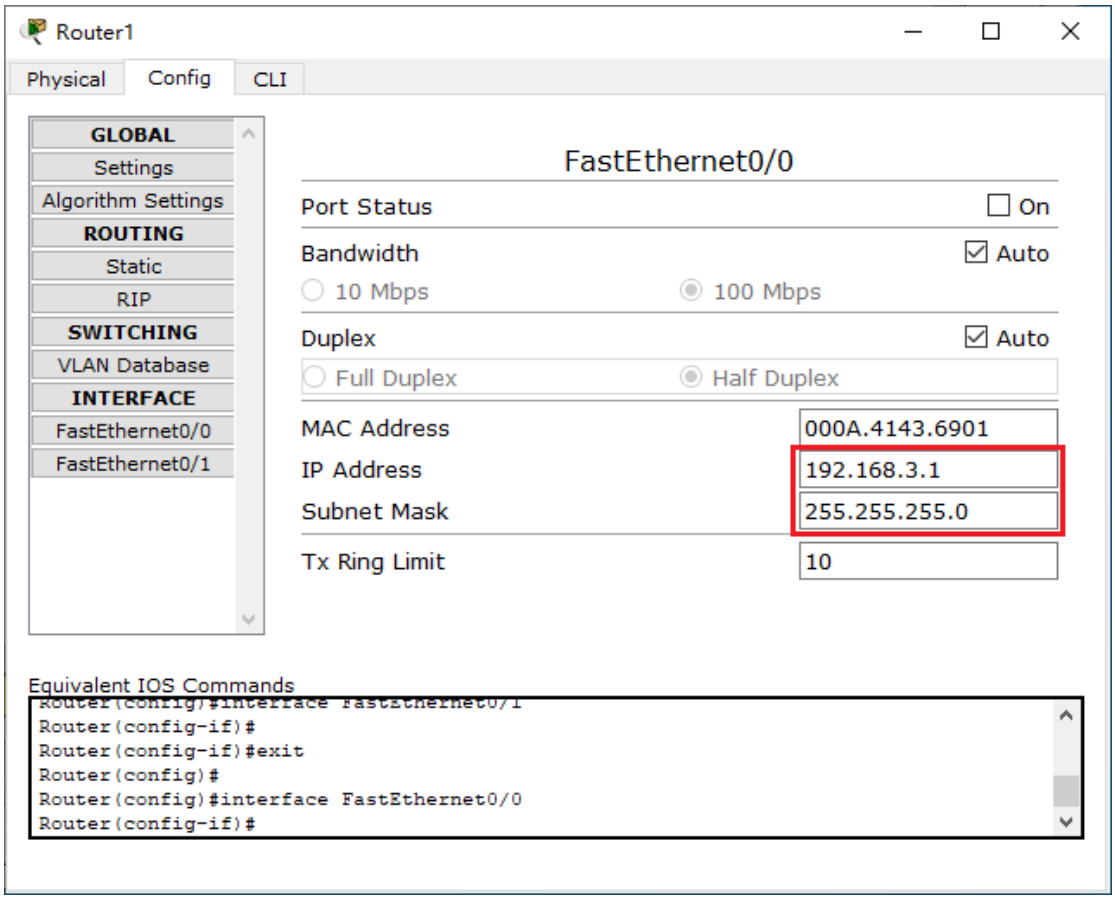

Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/1
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
0006.2ADE.3D02
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#

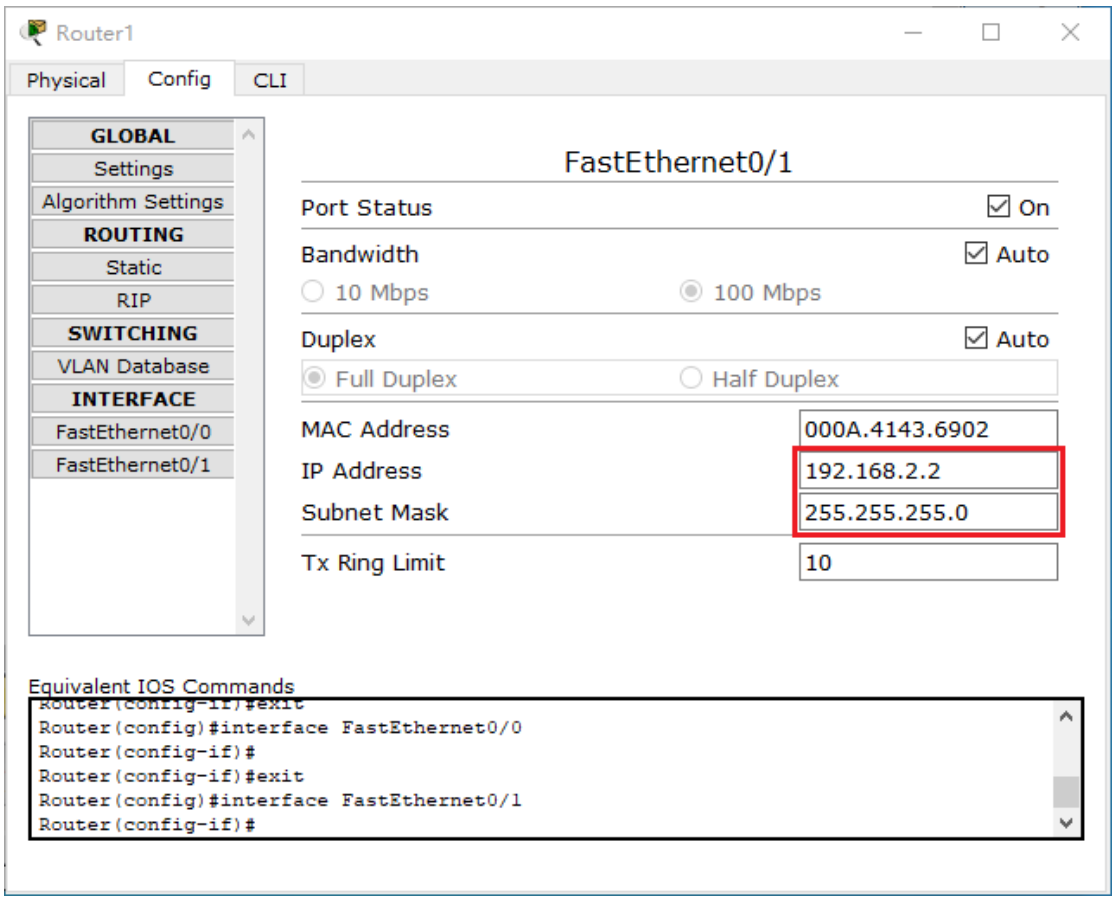

Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.3.0/24 via 192.168.2.2
192.168.3.0/24 via FastEthernet0/1
Remove
Equivalent IOS Commands
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#

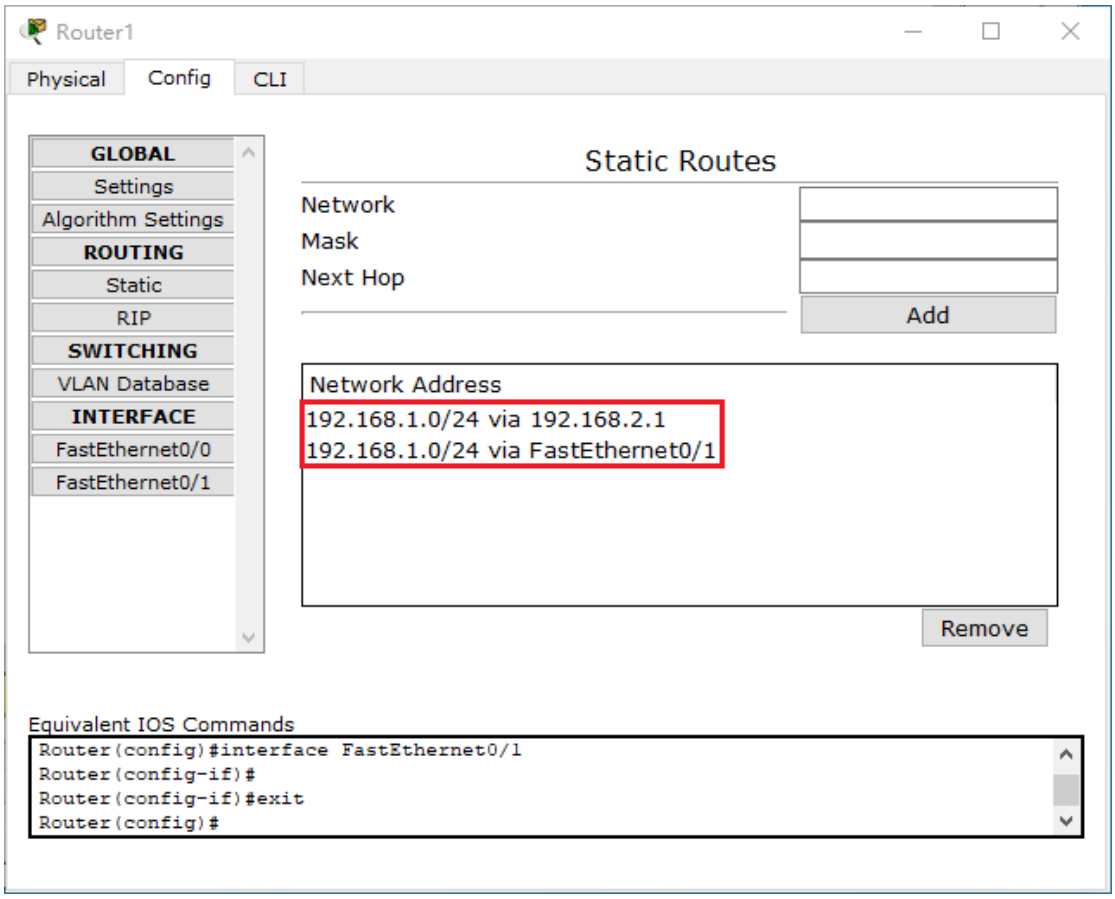
4. 配置路由器 Router1。

- FastEthernet0/0 接口配置 IP 地址为 192.168.3.1，子网掩码为 255.255.255.0。
- FastEthernet0/1 接口配置 IP 地址为 192.168.2.2，子网掩码为 255.255.255.0。
- 添加静态路由：要到达 192.168.1.0/24 网络应该通过 192.168.2.1，要到达 192.168.1.0/24 网络，应该通过 f0/1 接口。
- 也可以通过 CLI 窗口输入命令进行配置：

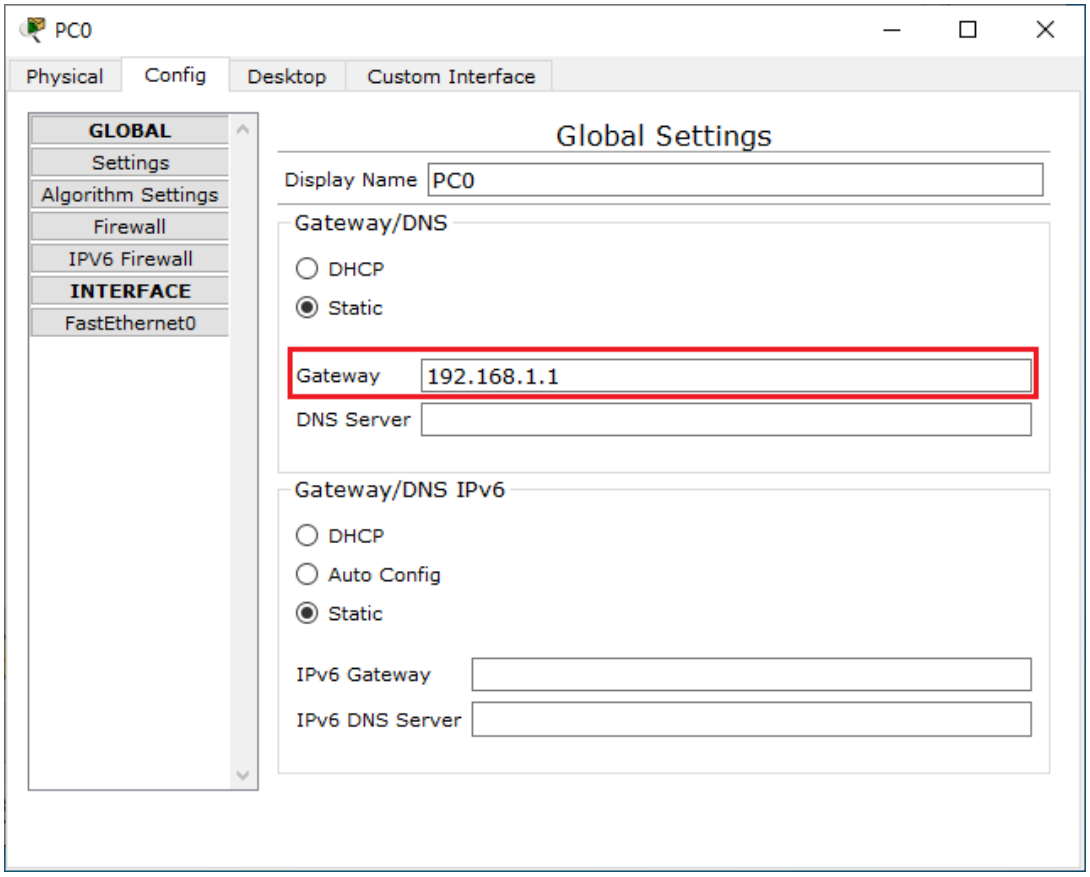
```
interface f0/0
ip address 192.168.3.1 255.255.255.0
no shutdown
interface f0/1
ip address 192.168.2.2 255.255.255.0
no shutdown
ip route 192.168.1.0 255.255.255.0 192.168.2.1
ip route 192.168.1.0 255.255.255.0 f0/1
```

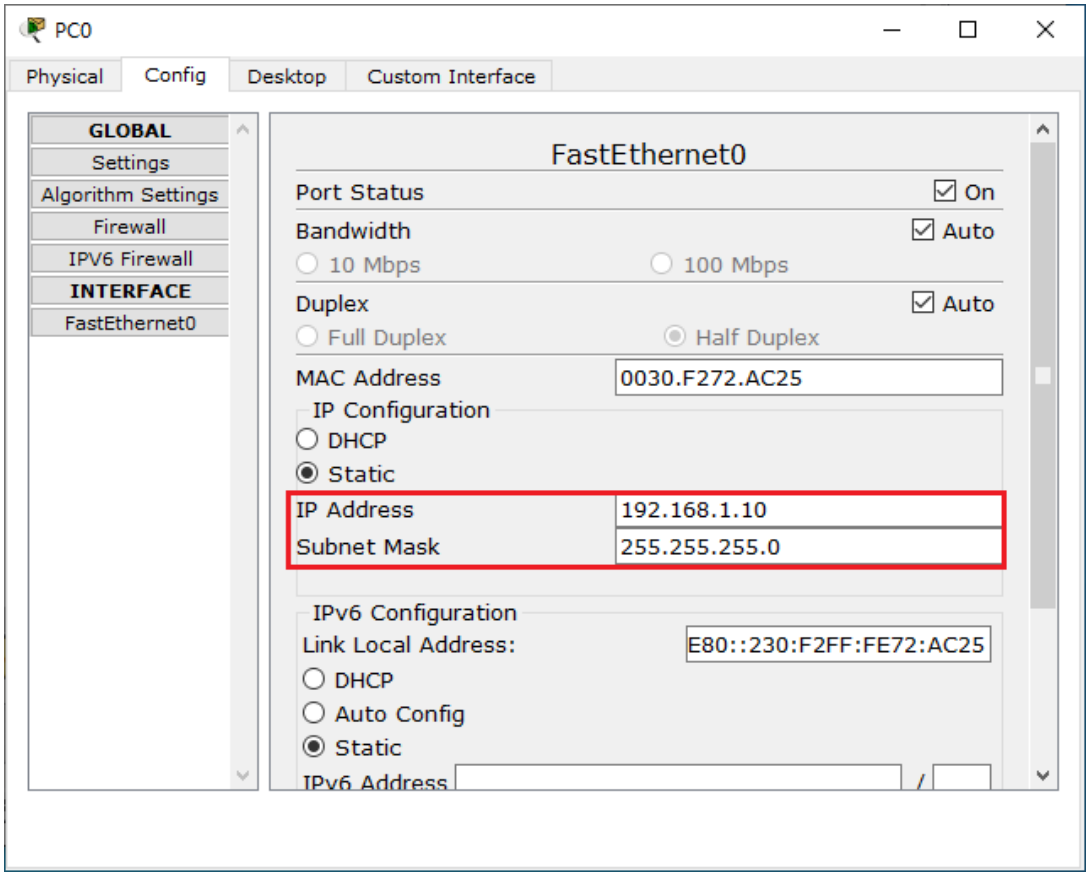



Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
FastEthernet0/1
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
000A.4143.6902
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#

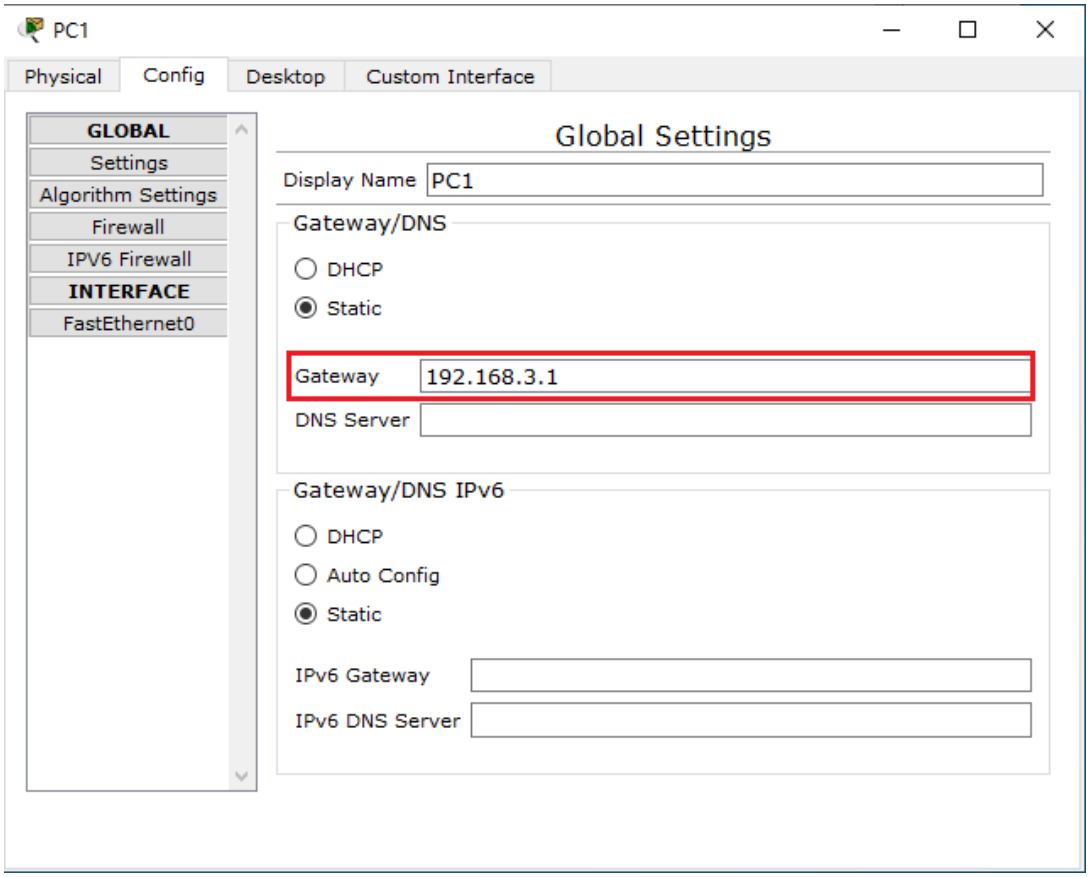

Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.1.0/24 via 192.168.2.1
192.168.1.0/24 via FastEthernet0/1
Remove
Equivalent IOS Commands
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#

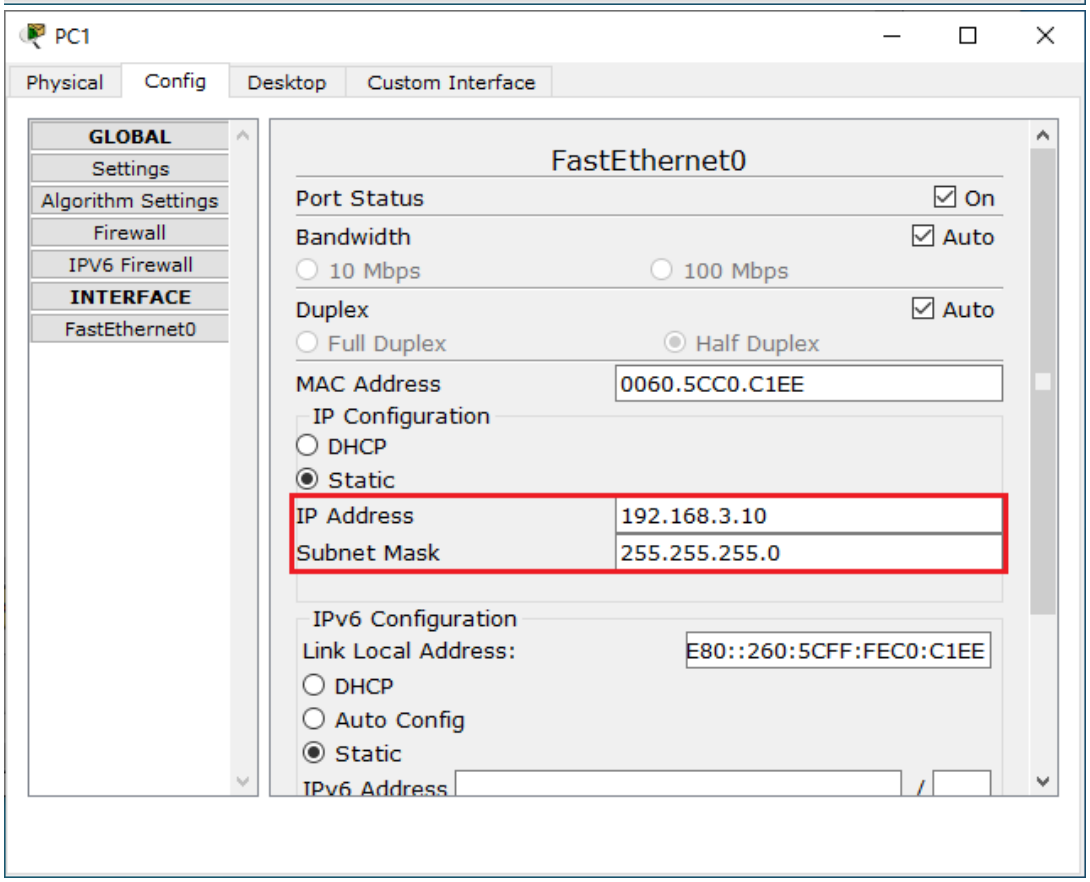
5. 配置 PC0 的网关、IP 地址与子网掩码。



6. 配置 PC1 的网关、IP 地址与子网掩码。



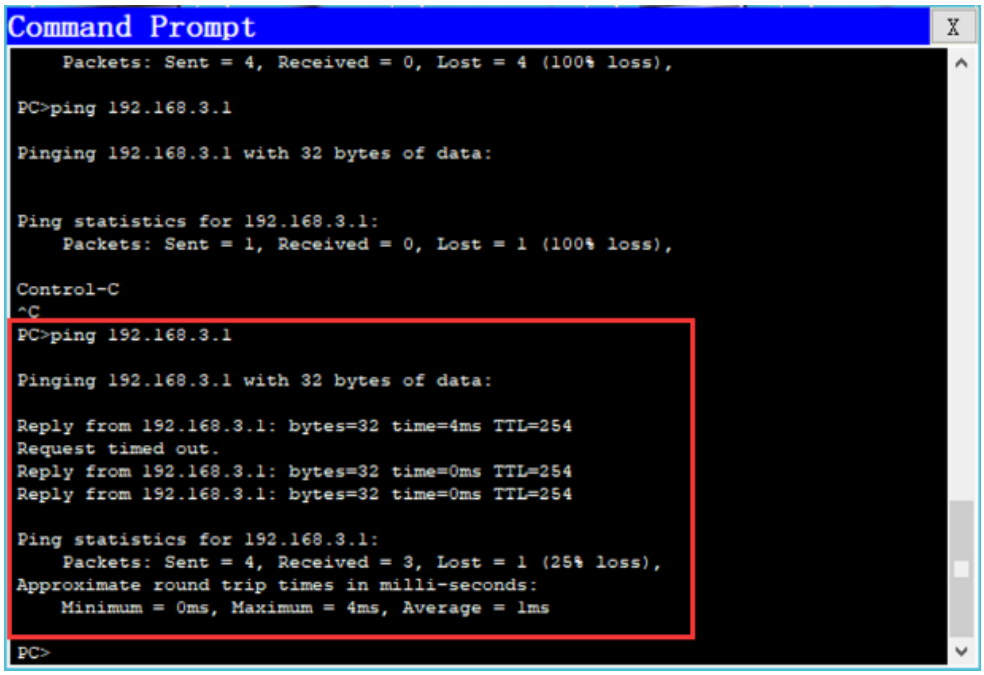
7. 测试 PC0 与 PC1 之间相互通信。

- 在 PC0 的 Prompt Terminal 输入 ping 192.168.3.1 命令接收 PC1 消息。
- 在 PC1 的 Prompt Terminal 输入 ping 192.168.1.1 命令接收 PC0 消息。

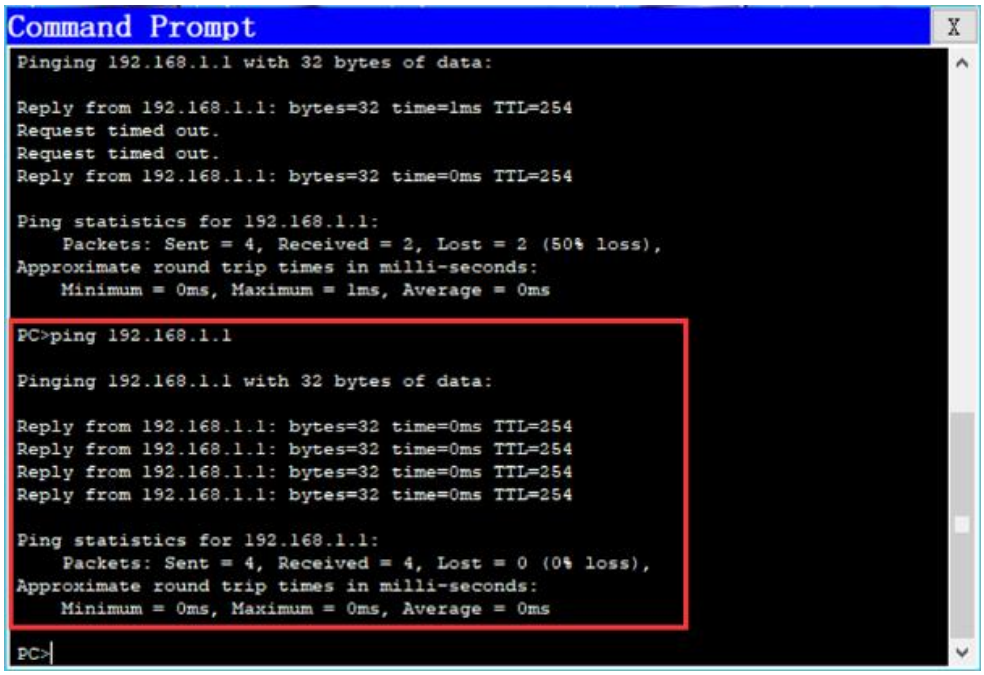
8. 在 Route0 与 Route1 的 CLI 中分别输入 show ip route 命令查看其对应的静态路由表。

**【实验现象】**

1. 在 PC0 的 Prompt Terminal 中输入 ping 192.168.3.1 命令接收 PC1 的消息。




2. 在 PC1 的 Prompt Terminal 中输入 ping 192.168.1.1 命令接收 PC0 的消息。



3. 在 Route0 的 CLI 中输入 show ip route 命令查看静态路由表。

```
Codes: L - local, C - connected, S - static, 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, 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

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1
S    192.168.3.0/24 [1/0] via 192.168.2.2
                    is directly connected, GigabitEthernet0/1
```

4. 在 Route1 的 CLI 中输入 show ip route 命令查看静态路由表。

```
Codes: L - local, C - connected, S - static, 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, 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

S    192.168.1.0/24 [1/0] via 192.168.2.1
                    is directly connected, GigabitEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.2/32 is directly connected, GigabitEthernet0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

**【分析讨论】**

本次实验的主要目标是通过配置静态路由来实现不同网络之间的通信。通过 Cisco Packet Tracer 软件，模拟了一个包含两个路由器和两台 PC 的网络环境。实验步骤包括为路由器和 PC 配置 IP 地址、子网掩码，以及配置静态路由规则来指定数据包的转发路径。

成功配置静态路由后，从 PC0 向 PC1 以及从 PC1 向 PC0 发送的 ping 命令均成功，这表明静态路由正确配置，数据包能够根据预定路由规则在网络中正确转发。通过执行 show ip route 命令观察到的静态路由表明确显示了目标网络、子网掩码以及下一跳地址或指定接口。

通过本次实验，我深刻理解了静态路由的工作原理和配置方法。静态路由的优点在于配置简单、稳定可靠，非常适合结构简单或网络拓扑变化不大的场景。然而，静态路由也有其局限性，主要表现在网络扩展或拓扑变化时，需要手动更新路由信息，管理维护成本较高。本次实验不仅加深了我对网络路由原理的理解，也提高了我的实践操作能力，为进一步学习网络技术打下了坚实的基础。

# 实验 11：蓝牙通信实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/03/28 |

**【实验目的】**

本次蓝牙通信实验旨在于深入探索并理解蓝牙技术的核心原理，以及该技术如何被应用于实现移动通信终端设备之间，以及这些设备与互联网之间的通信。本次实验将实现电脑与手机之间通过蓝牙技术进行文件传输，这对理解无线通信技术的工作原理至关重要。

**【实验原理】**

**蓝牙**

蓝牙技术是一种短距离无线通信技术，它极大地简化了移动通信终端设备之间的数据交换。这些设备包括掌上电脑、笔记本电脑和移动电话等。蓝牙技术的一个重要优势是能够简化这些设备与互联网之间的通信，使得数据传输变得更加迅速和高效。简而言之，蓝牙技术让我们能够在没有电缆的情况下连接到网络，并实现无线上网。

蓝牙技术的工作基于主从模式，这意味着在任何给定的蓝牙通信中，一方设备充当主设备（Master），另一方充当从设备（Slave）。通信过程中，主设备负责查找、发起配对并建立连接。一旦连接建立，双方即可进行数据传输。理论上，一个蓝牙主设备可以同时与多达七个从设备进行通信。

蓝牙设备具有角色切换的能力，意味着它们可以根据需要在主模式和从模式之间切换。大多数时间，一个设备可能处于从模式，等待其他主设备的连接请求。当有连接需求时，它可以切换到主模式，向其他设备发起连接。为了发起连接，主设备需要知道对方的蓝牙地址和配对密码。一旦配对成功，就可以直接发起呼叫和数据传输。

总的来说，蓝牙技术通过提供一种方便、无线的方式来连接和交换信息，极大地促进了现代移动设备的通信效率。它的应用范围广泛，从简单的耳机配对、文件传输到复杂的医疗设备和家用电器的远程控制，蓝牙技术都发挥着重要作用。

**【实验设备】**

1. 操作系统：Windows 11

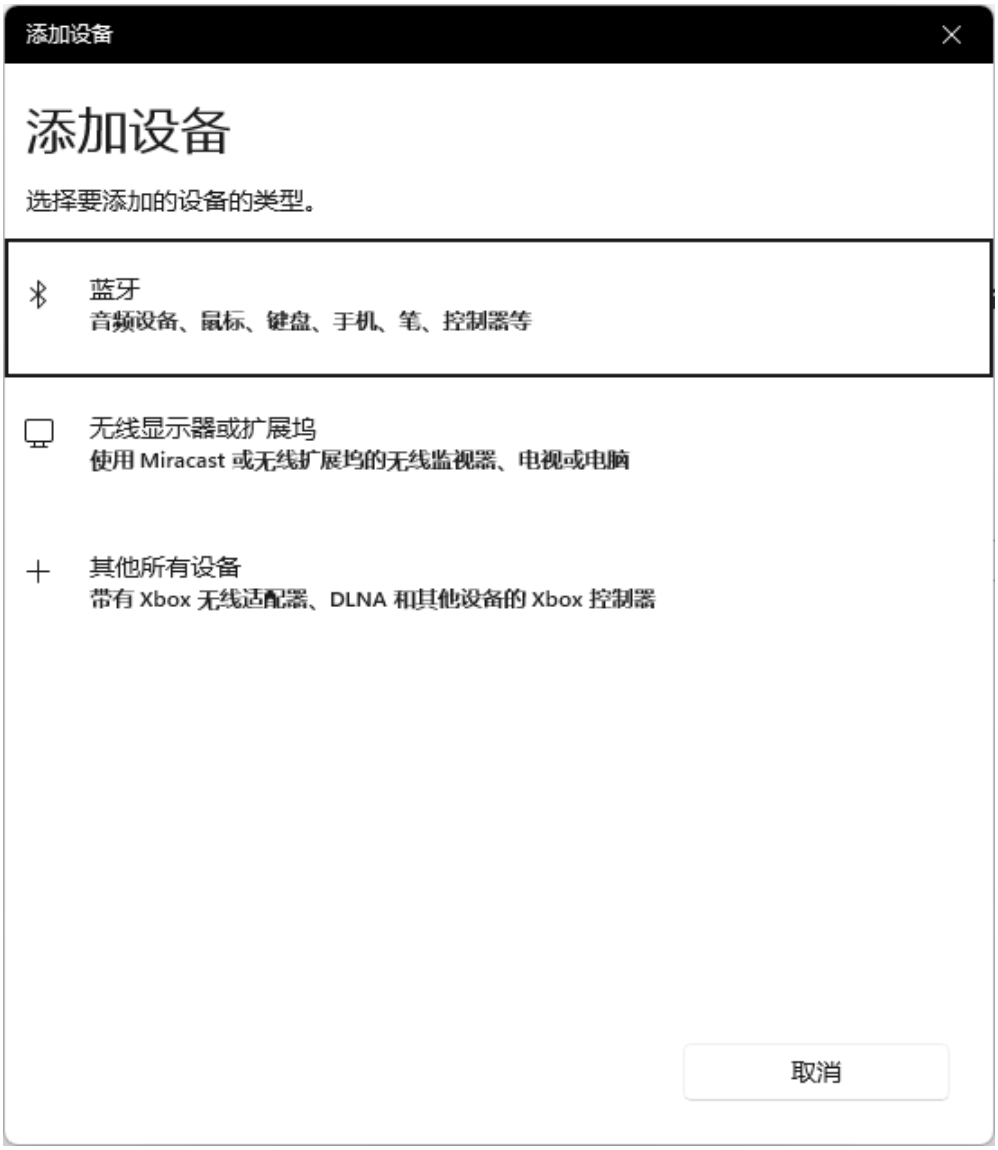
2. 网络环境：Wi-Fi 连接

3. IOS 设备和 Android 设备各一台

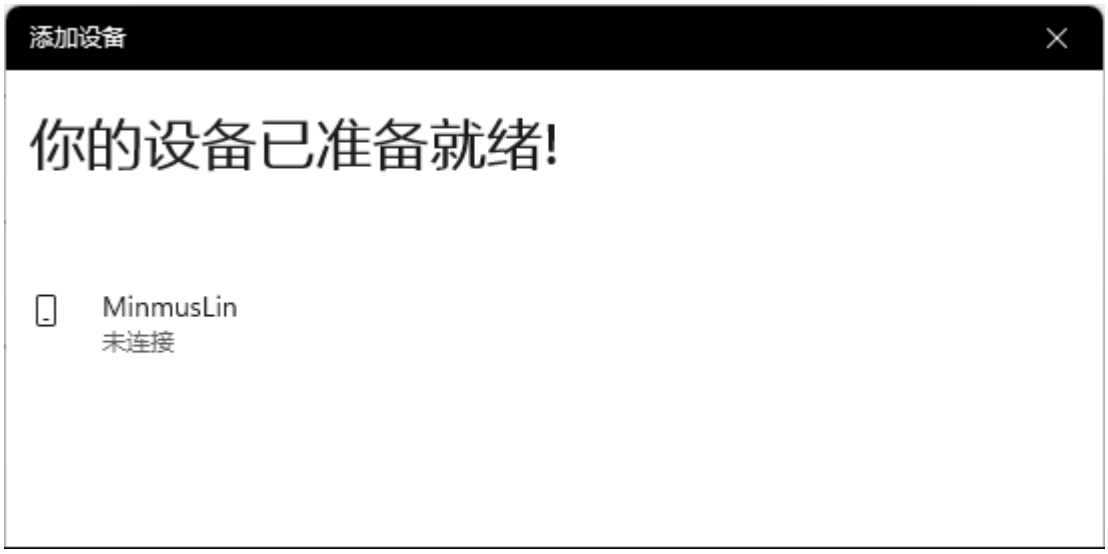
**【实验步骤】**

1. 打开电脑和手机的蓝牙功能。

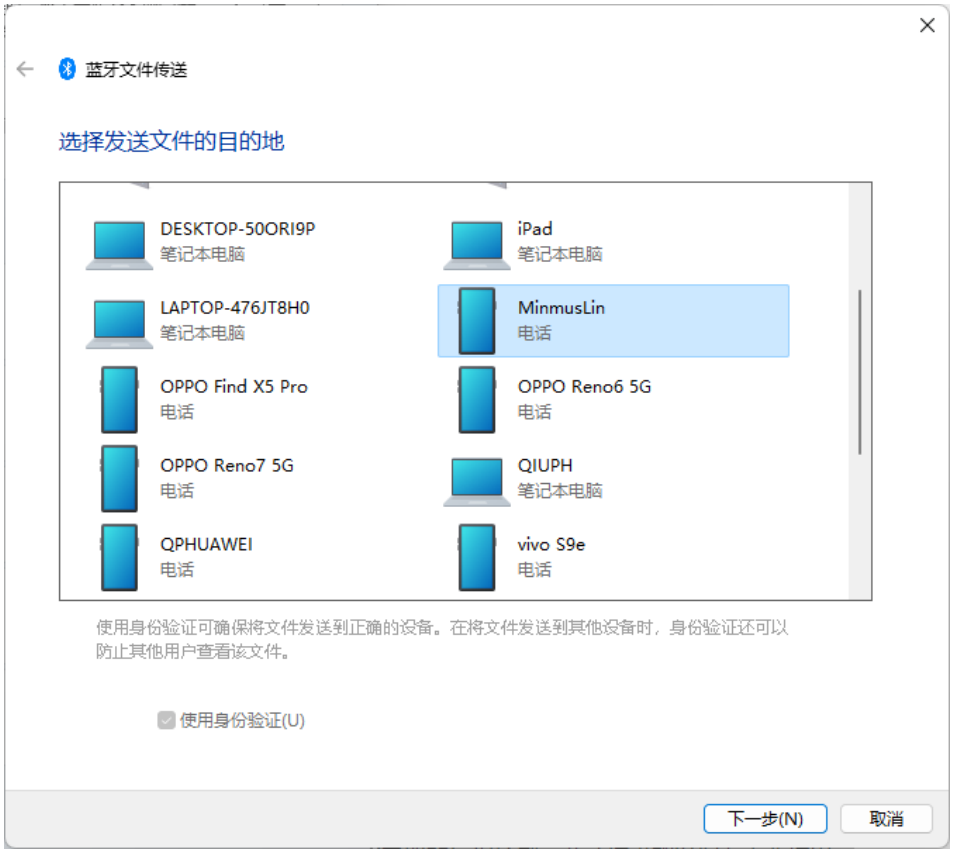
2. 在电脑上打开“设置”>“蓝牙和其他设备”>“设备”>“添加设备”>“蓝牙”，连接手机设备；也可以在手机上连接电脑。



添加设备
添加设备
确保你的设备已打开并可被发现。在下面选择要连接的设备。
QPHUAWEI
OPPO Reno7 5G
OPPO Reno6 5G
通信设备
MinmusLin
正在连接...
如果 MinmusLin 上的 PIN 与此 PIN 匹配，请按"连接"。
285741
连接
取消
139******15的nova 9
取消

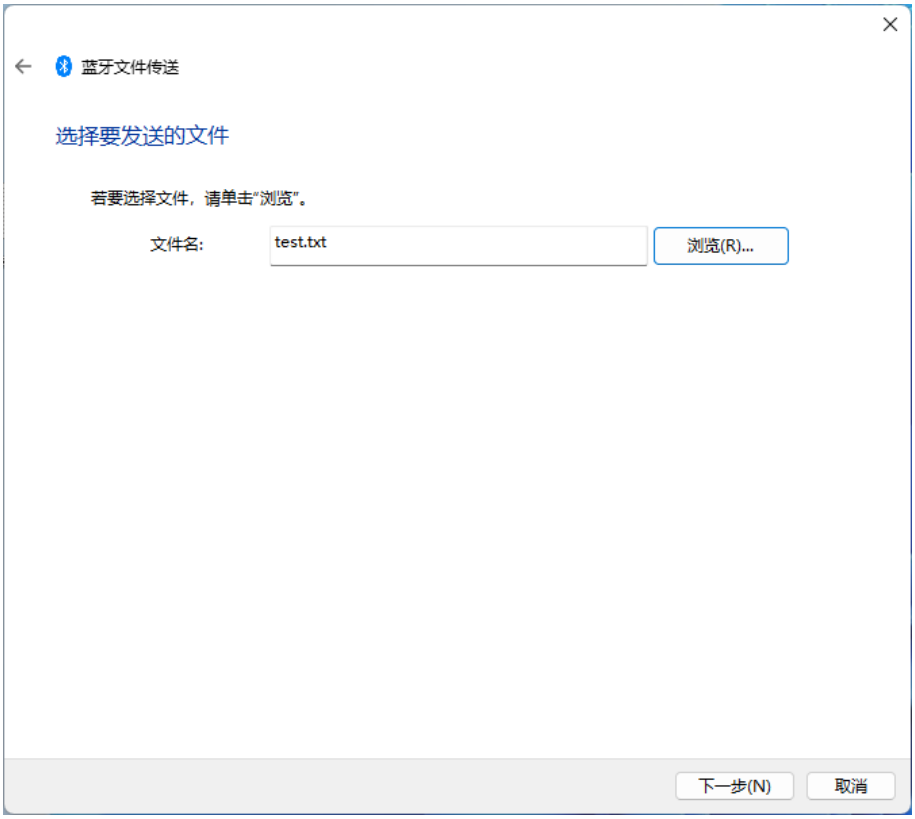

添加设备
你的设备已准备就绪!
MinmusLin
未连接

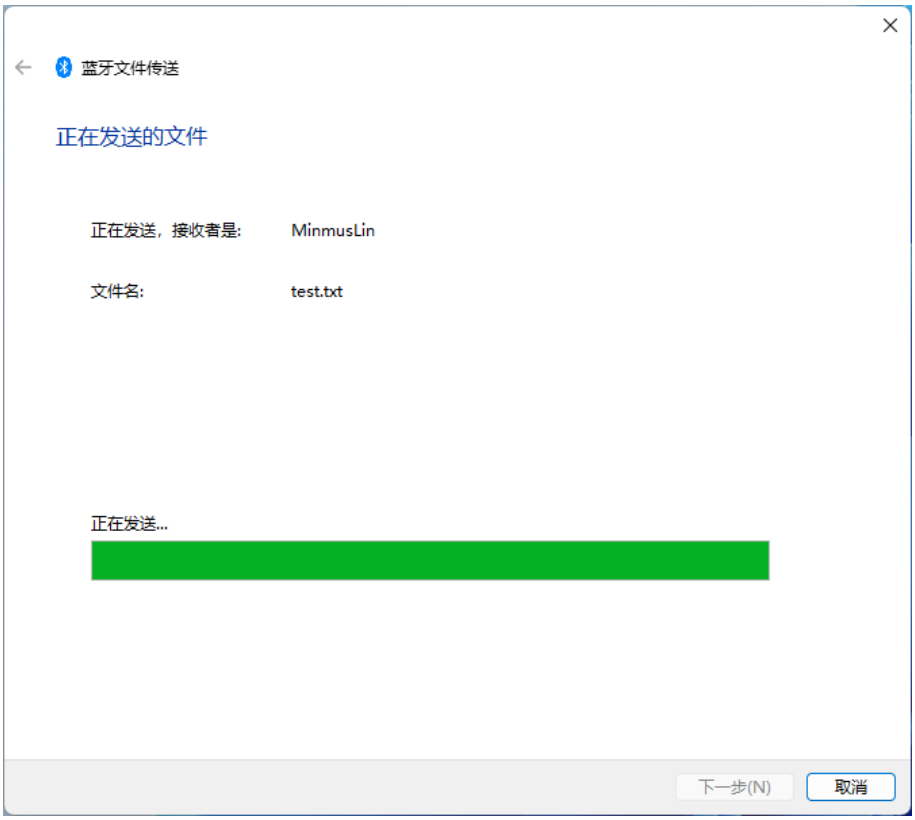
3. 在电脑上打开“设置”>“蓝牙和其他设备”>“设备”>“通过蓝牙发送或接收文件”>“发送文件”，选择手机设备，选择文件，将其发给手机。

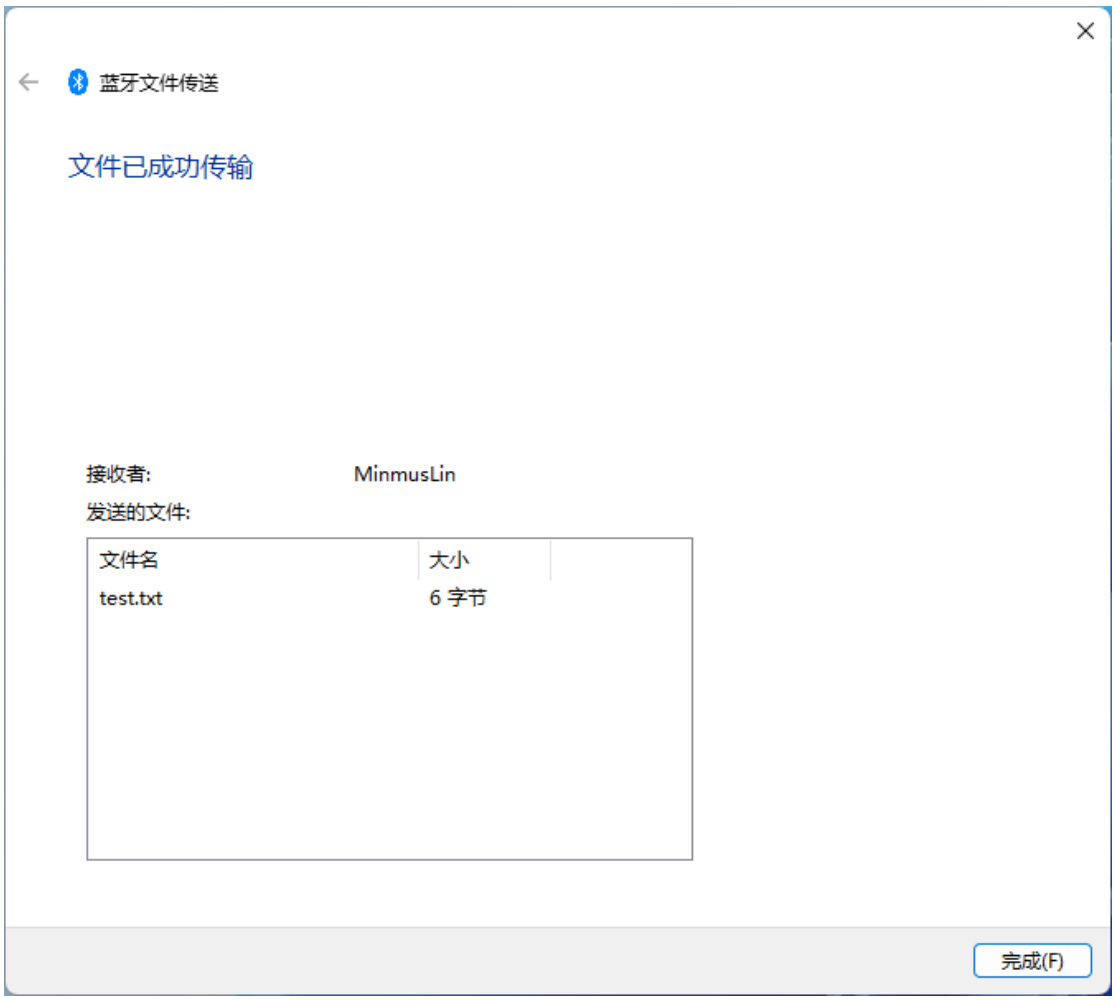


【实验现象】

1. 使用 IOS 设备进行文件传输，失败。
2. 使用 Android 设备进行文件传输，成功。






【分析讨论】

一、IOS 设备进行文件传输失败的原因

1. 严格的安全策略：Apple 对 IOS 设备的安全和隐私保护采取了较为严格的控制措施。这包括对通过蓝牙传输文件的限制，旨在防止潜在的安全威胁和数据泄露。iOS 设备通常不允许通过标准的文件传输协议与非 Apple 设备进行蓝牙文件共享，除非使用特定的应用或服务（如 AirDrop），这是 Apple 专为其设备生态系统设计的文件共享服务。
2. 限制的蓝牙配置文件：蓝牙技术中的配置文件定义了设备如何以及为何种目的相互通信。IOS 设备可能不支持或限制了文件传输配置文件（如文件传输协议（FTP）或对象推送配置文件（OPP）），这限制了其与非 Apple 设备的蓝牙文件传输能力。

二、Android 设备进行文件传输成功的原因

1. 开放的系统设计：相较于 IOS，Android 操作系统对用户和开发者提供了更

多的自由和控制权，包括蓝牙文件传输。Android 设备支持多种蓝牙配置文件，包括那些专门用于文件传输的配置文件。这使得 Android 设备能够更容易地与包括 Windows 电脑在内的其他设备通过蓝牙交换文件。

2. 广泛的兼容性：Android 设备设计为能够与多种不同设备和操作系统兼容，包括广泛支持各种蓝牙配置文件。这种兼容性使得 Android 设备能够成功地接收来自电脑的蓝牙文件传输请求。

# 实验 12：局域网（以太网）实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/11 |

**【实验目的】**

1. 深入理解局域网（以太网）的基本原理和组网技术，通过实际操作加强对局域网设计、配置与管理的认识。
2. 掌握局域网的基本概念，包括其定义、特点、组成部分，以及与其他网络类型的区别。
3. 学习和应用 Cisco2950 交换机在局域网中的配置和使用，包括端口的基本设置和网络设备的连接。
4. 理解 IP 地址配置的基本方法，包括终端 IP 地址的设置、子网掩码的应用以及子网规划的示例。
5. 通过使用 ipconfig 和 ping 命令，学习如何检查网络配置和进行网络连通性测试，以确保网络设备正确配置和有效通信。
6. 通过构建实际的网络拓扑结构，加深对局域网物理和逻辑结构的理解，以及网络设备之间的交互方式。

**【实验原理】**

**局域网原理**

局域网（Local Area Network, LAN）是一种计算机网络，专为小范围内，如学校、家庭、办公室或单一建筑内的网络通信设计。局域网的主要特点归纳如下：

- 有限的地理范围：局域网覆盖的区域相对较小，通常限于一个建筑物或一组紧密相连的建筑中。这与广域网（WAN）不同，后者可以跨越大的地理区域，甚至是全球。
- 高速数据传输：局域网提供高速的数据传输能力，其速度远高于通过电话线路或无线方式连接的广域网络。常见的局域网传输速度从 100Mbps 到 10Gbps 不等，依赖于所使用的技术和媒介。
- 稳定性和可靠性：由于局域网的封闭性和有限的地理范围，它们通常能提供较高的稳定性和可靠性。网络设备之间的物理连接减少了数据丢失和延迟的

可能性。

- 简易的网络框架：局域网结构相对简单，容易部署和管理。这种简易性使得局域网成为学校、企业和家庭等场所的理想选择。
- 封闭性：局域网通常是封闭的网络系统，仅供内部用户使用，这提供了更高的安全性和控制能力。管理员可以轻松管理谁可以访问网络以及他们可以访问网络的哪些部分。
- 组成部分：局域网主要由三大部分构成：
  - 计算机设备：包括连接到网络的所有终端用户设备，如个人计算机、笔记本电脑、服务器和打印机。
  - 网络连接设备：如交换机、路由器和集线器，这些设备负责数据包的路由和交换，确保数据正确地从一个设备传输到另一个设备。
  - 网络传输介质：局域网中数据传输使用的物理或无线介质，包括双绞线、光纤和无线电波等。

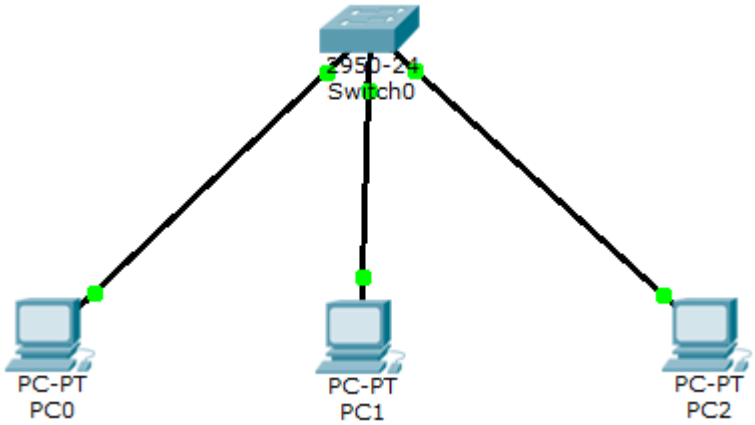
局域网的设计和实施要考虑到网络的扩展性、安全性、管理和成本效益，以满足用户的具体需求。随着技术的进步，局域网继续演化，提供更高的速度、更好的安全性和更广泛的应用。

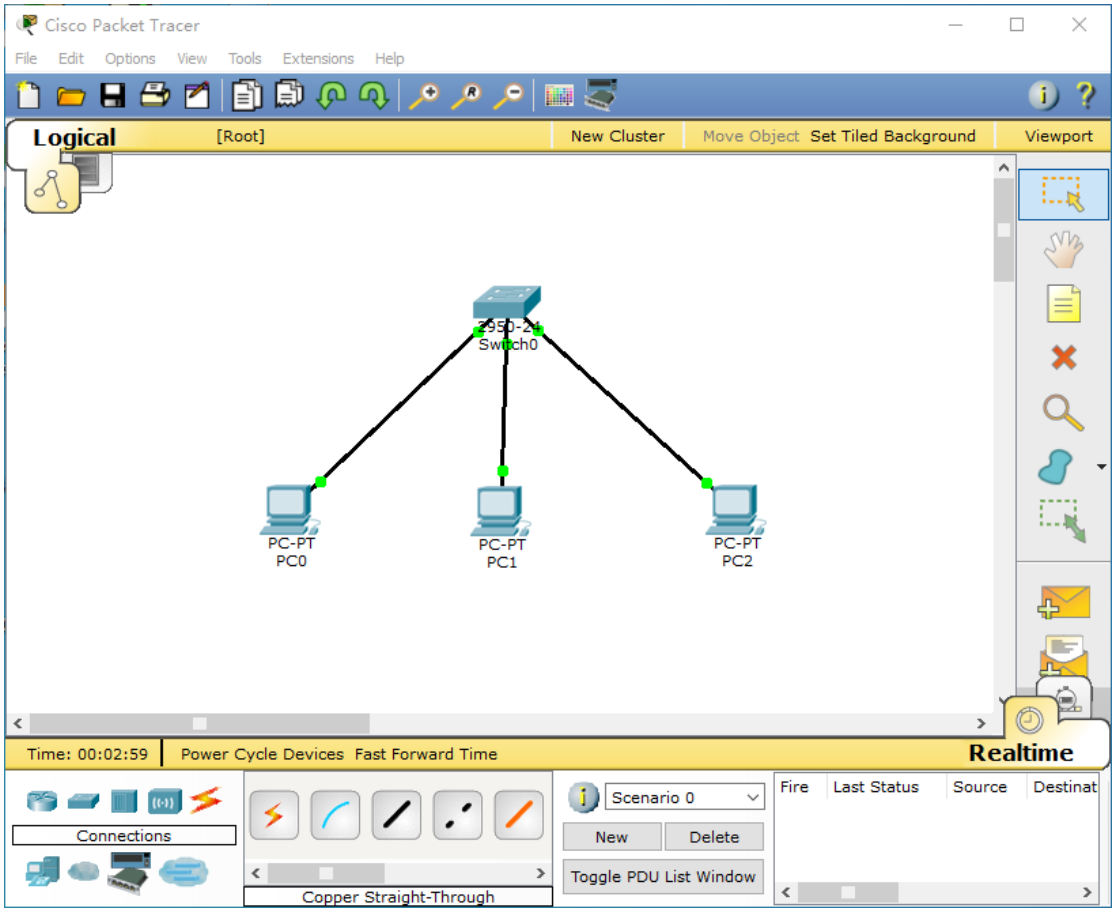
**【实验设备】**

1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

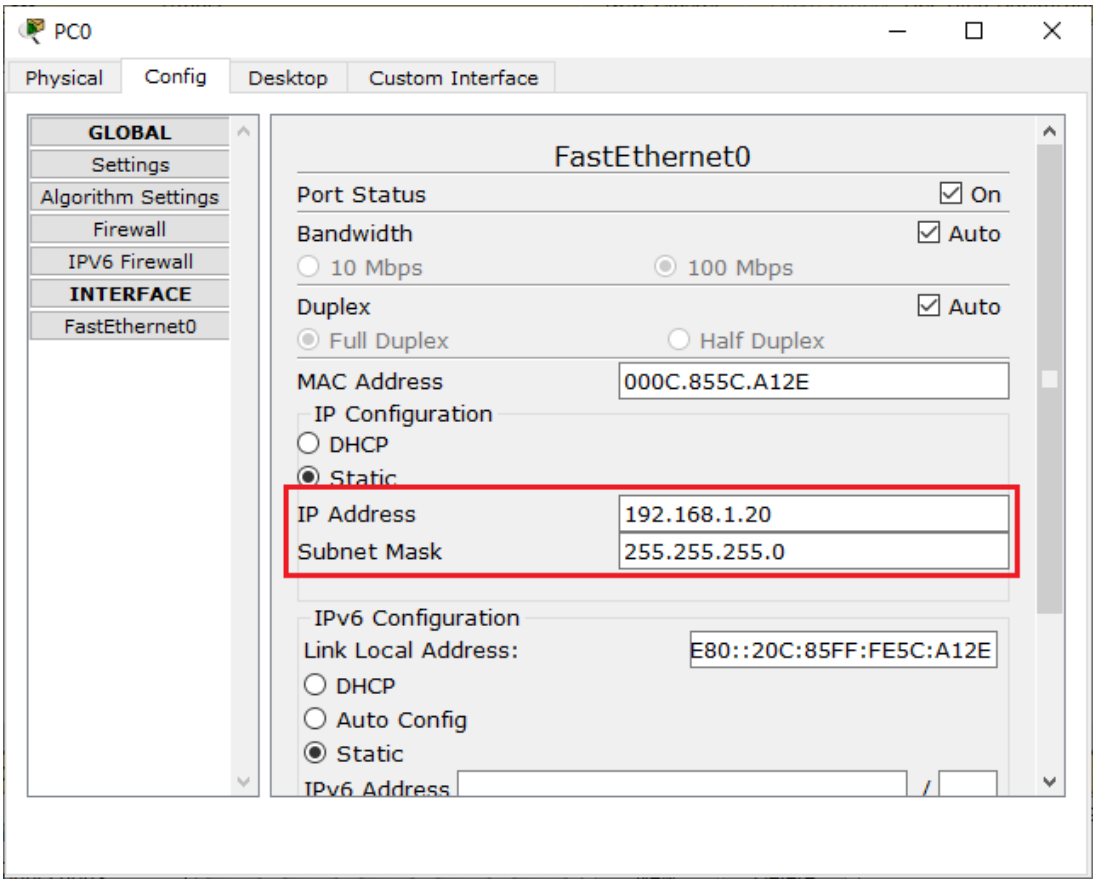
**【实验步骤】**

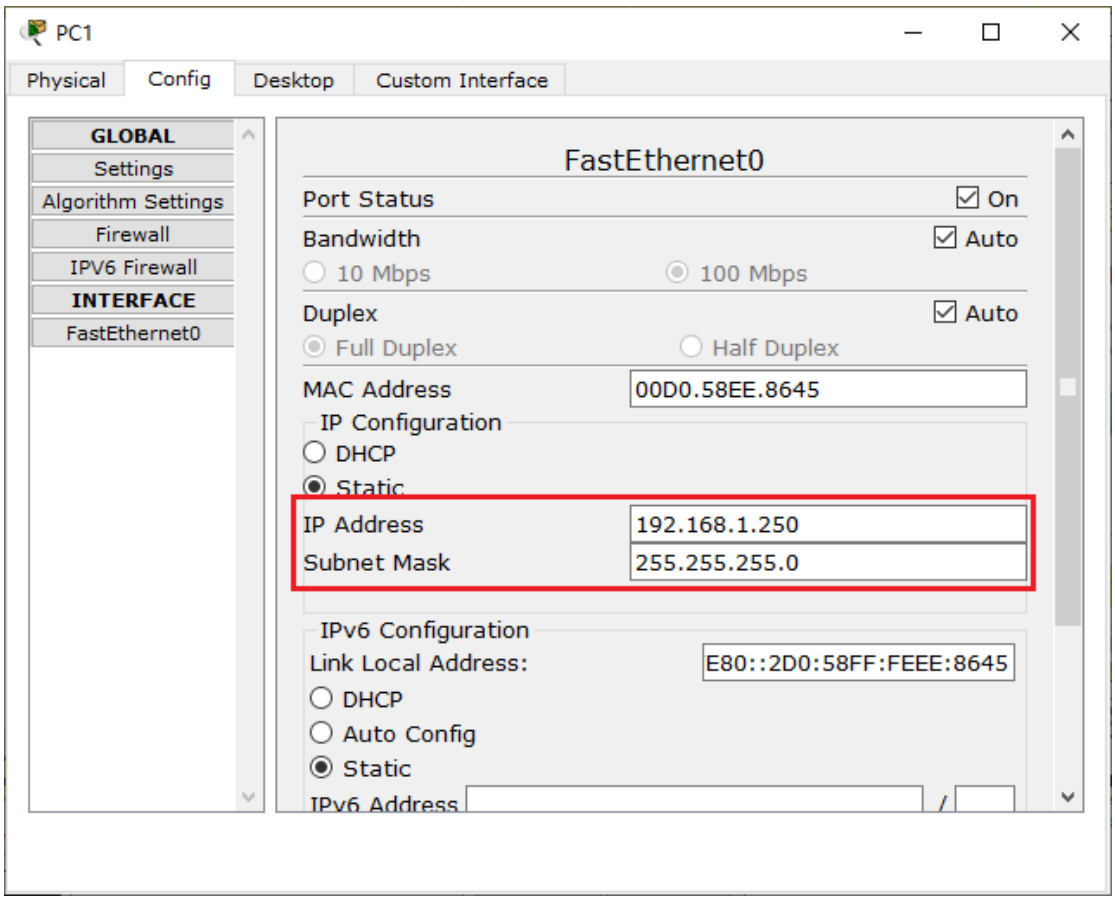
1. 启动 Cisco Packet Tracer，按照如下拓扑结构连接设备。

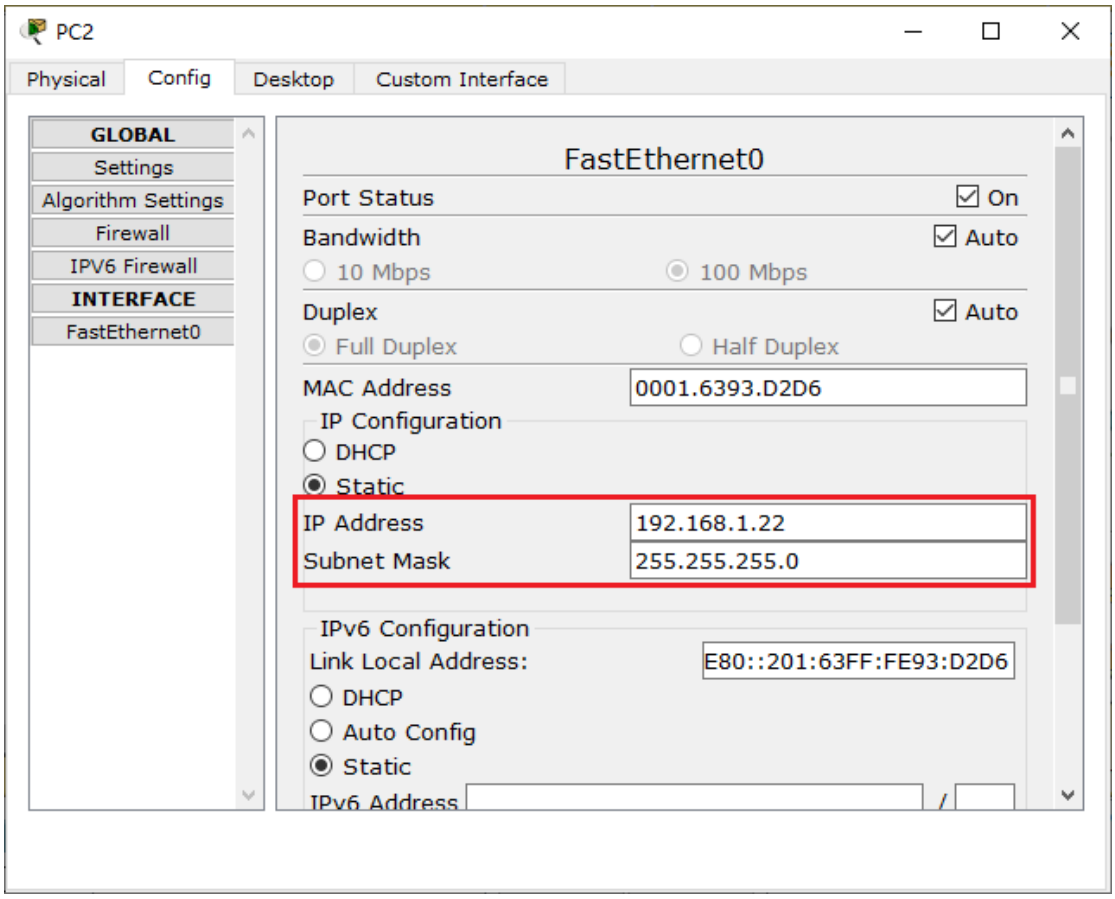





2. 为 PC0、PC1 和 PC2 分别配置 IP 地址和子网掩码。

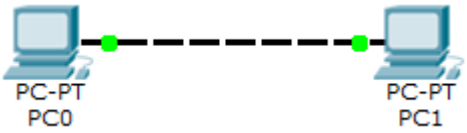


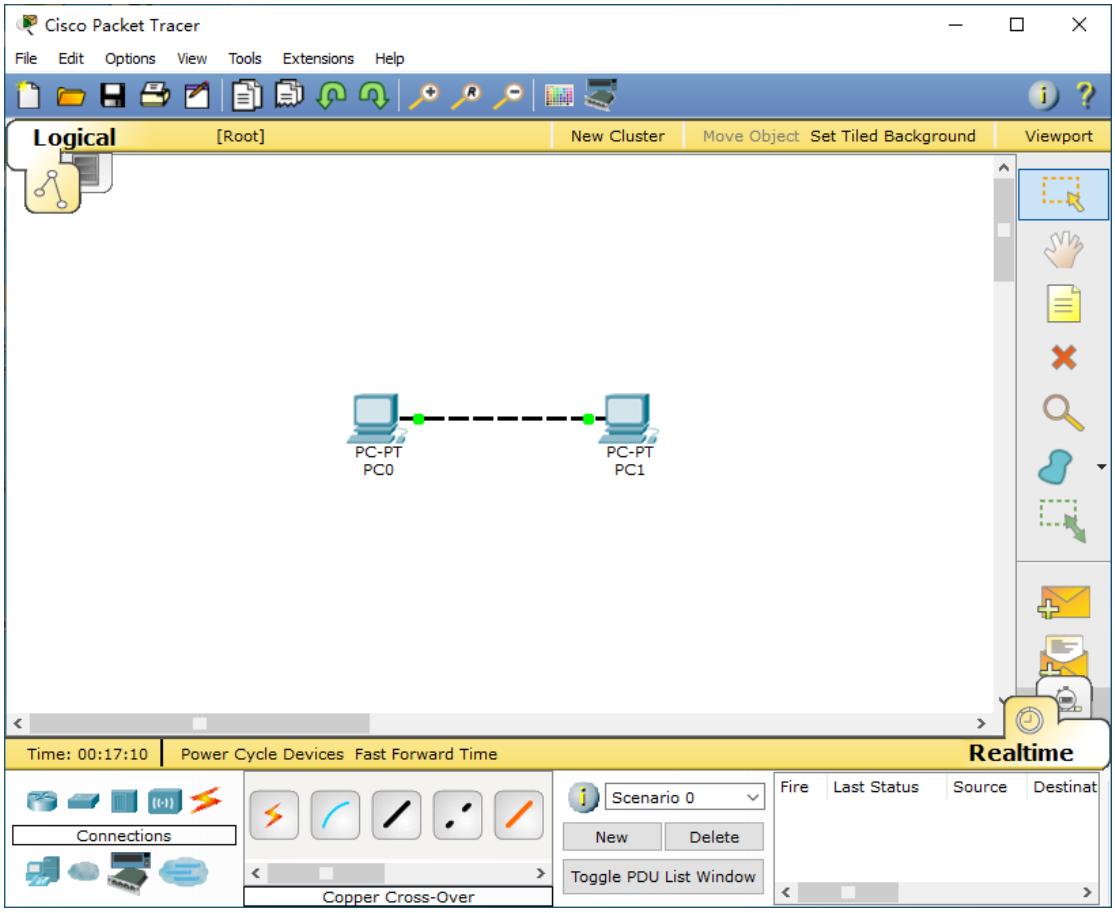

PC1
Physical
Config
Desktop
Custom Interface
GLOBAL
Settings
Algorithm Settings
Firewall
IPV6 Firewall
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
00D0.58EE.8645
IP Configuration
DHCP
Static
IP Address
192.168.1.250
Subnet Mask
255.255.255.0
IPv6 Configuration
Link Local Address:
E80::2D0:58FF:FEEE:8645
DHCP
Auto Config
Static
IPv6 Address


PC2
Physical
Config
Desktop
Custom Interface
GLOBAL
Settings
Algorithm Settings
Firewall
IPV6 Firewall
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
MAC Address
0001.6393.D2D6
IP Configuration
DHCP
Static
IP Address
192.168.1.22
Subnet Mask
255.255.255.0
IPv6 Configuration
Link Local Address:
E80::201:63FF:FE93:D2D6
DHCP
Auto Config
Static
IPv6 Address

3. 使用 ping 命令测试 PC0、PC1、PC2 之间的网络连通性，观察并记录实验结果。

4. 将两台终端连接，使用 ping 命令测试网络连通性，观察并记录实验结果。




**【实验现象】**

1. 用 PC0 分别 ping PC1、PC2，用 PC1 分别 ping PC0、PC2，用 PC2 分别 ping PC1、PC0，发现均请求成功，网络连通性测试成功。

   - PC0、PC1、PC2 的 ping 命令分别如下：

| |
|---|
| ping 192.168.1.250<br>ping 192.168.1.22 |
| ping 192.168.1.20<br>ping 192.168.1.22 |
| ping 192.168.1.20<br>ping 192.168.1.250 |

PC0

Physical | Config | Desktop | Custom Interface

Command Prompt

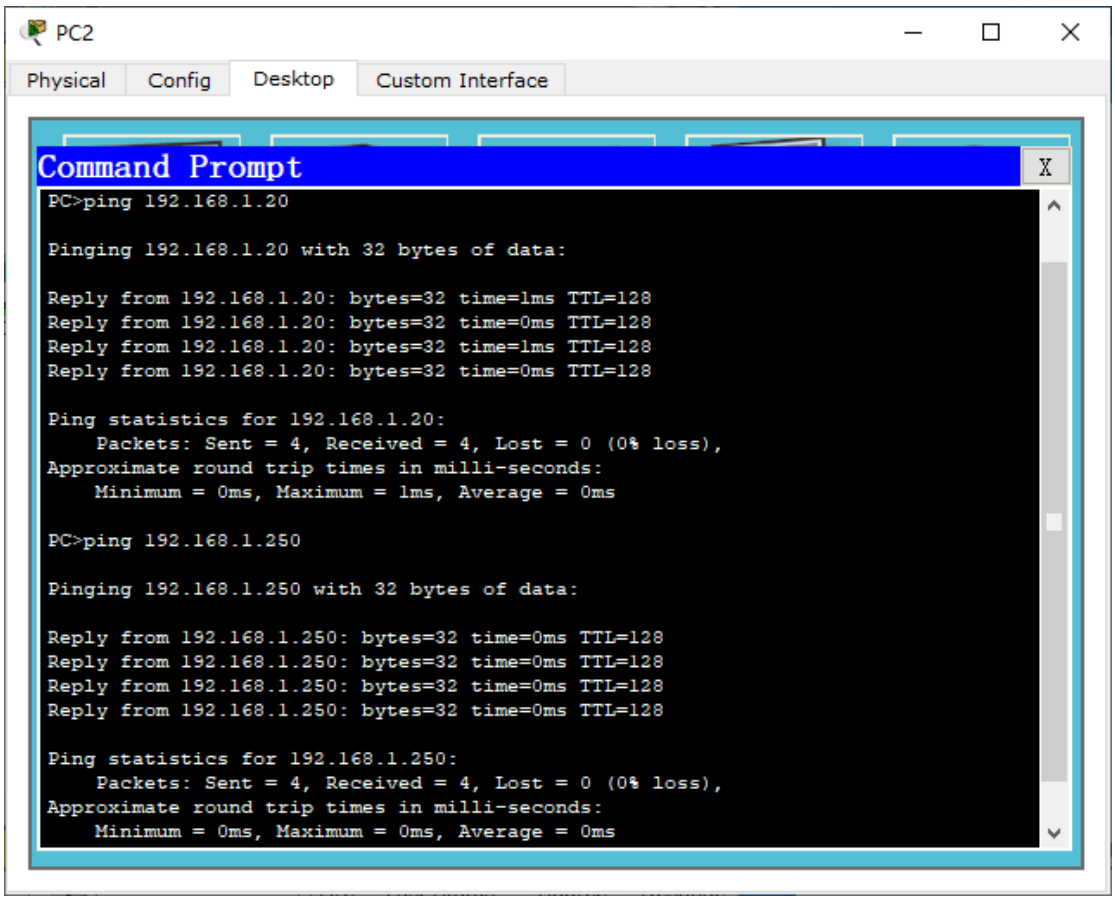
```
PC>ping 192.168.1.250

Pinging 192.168.1.250 with 32 bytes of data:

Reply from 192.168.1.250: bytes=32 time=1ms TTL=128
Reply from 192.168.1.250: bytes=32 time=0ms TTL=128
Reply from 192.168.1.250: bytes=32 time=0ms TTL=128
Reply from 192.168.1.250: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.1.22

Pinging 192.168.1.22 with 32 bytes of data:

Reply from 192.168.1.22: bytes=32 time=0ms TTL=128
Reply from 192.168.1.22: bytes=32 time=0ms TTL=128
Reply from 192.168.1.22: bytes=32 time=0ms TTL=128
Reply from 192.168.1.22: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1

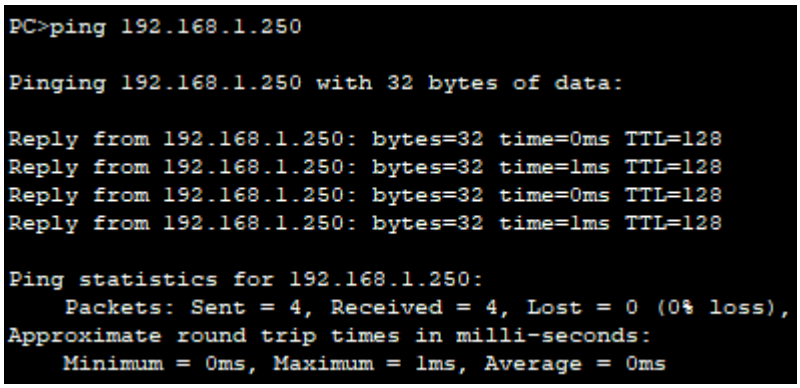
Physical | Config | Desktop | Custom Interface

Command Prompt

```
PC>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=0ms TTL=128
Reply from 192.168.1.20: bytes=32 time=0ms TTL=128
Reply from 192.168.1.20: bytes=32 time=0ms TTL=128
Reply from 192.168.1.20: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.22

Pinging 192.168.1.22 with 32 bytes of data:

Reply from 192.168.1.22: bytes=32 time=0ms TTL=128
Reply from 192.168.1.22: bytes=32 time=0ms TTL=128
Reply from 192.168.1.22: bytes=32 time=0ms TTL=128
Reply from 192.168.1.22: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```




2. 两台终端连接，使用 ping 命令测试网络连通性，发现请求成功，网络连通性测试成功。




**【分析讨论】**

实验结果表明，所有终端（PC0、PC1 和 PC2）之间的网络连通性良好，所有 ping 命令都成功执行，这证明了网络设置正确，各终端之间可以顺利通信。以下是对实验结果的具体分析与讨论：

1. IP 地址配置和子网掩码的正确性

IP 地址和子网掩码的配置对于局域网中的通信至关重要。在这个实验中，

每台 PC 的 IP 地址配置和子网掩码设置正确，能确保数据包在网络内正确路由。实验中各终端使用的是相同子网内的地址，这意味着不需要路由器就可以进行直接通信，这简化了数据传输过程。

2. 网络设备和连接的有效性

使用 Cisco Packet Tracer 模拟的网络环境，允许学生虚拟化实际网络设备的设置和连接。在实验中，正确的网络拓扑和物理连接是网络连通性成功的关键。此外，实验中使用的交换机模型（如 Cisco2950）能够有效地处理帧的传递和冲突管理，增强了网络的整体性能和稳定性。

3. 使用 ping 命令测试网络连通性

ping 命令是检查网络连通性的一个重要工具。它通过发送 ICMP 回显请求消息给目标地址，并等待回显回复来验证连接状态。成功的 ping 测试显示所有设备都可以接收和发送数据，这指示网络没有物理或逻辑错误。

4. 网络的稳定性和可靠性

局域网的封闭性和有限的地理范围通常提供较高的网络稳定性和可靠性。在这个实验中，由于所有操作均在同一个局域网内进行，网络稳定性和可靠性得到了证实。

# 实验 13：RIP 路由配置实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/11 |

**【实验目的】**

本次实验的目的是在一个配置了多台计算机和路由器的网络环境中，实现并验证 RIP（Routing Information Protocol）路由协议的功能和效果。RIP 是一种内部网关协议（IGP），主要应用于小型同类网络，它使用跳数作为衡量路径开销的指标。通过本实验，学生将学习如何规划网络地址和拓扑图，配置 PC 机、服务器及路由器的 IP 地址，并在路由器上配置 RIP 协议。实验的关键步骤包括检查 PC 间的连通性，配置 RIP 路由表，并最终验证配置后网络中主机之间的互通性。这将帮助学生理解路由协议在网络通信中的作用和重要性，以及如何在实际网络环境中部署和调试路由协议。

**【实验原理】**

**RIP 技术原理**

RIP（Routing Information Protocol，路由信息协议）是一种经典的内部网关协议（IGP），广泛应用于小型同类网络中。作为一种距离矢量路由协议，RIP 使用跳数来衡量到达目的网络的路径开销，其中规定的最大跳数限制为 15。跳数过多（超过 15 跳）的路由被认为是不可达的，这有助于防止路由循环。

RIP 具有两个主要的版本：

RIPv1：这是 RIP 的初版，属于有类路由协议。RIPv1 不支持可变长度子网掩码（VLSM），并且它通过广播的方式更新路由信息，每 30 秒更新一次。由于它是有类的，RIPv1 在处理不同大小的子网时存在限制，这在多子网环境中可能导致地址资源浪费。

RIPv2：作为 RIPv1 的改进版本，RIPv2 是一个无类路由协议，支持 VLSM，这使得它能更有效地使用 IP 地址空间，并适用于更复杂的网络结构。与 RIPv1 相比，RIPv2 采用组播地址（而非广播）来发送路由更新信息，这减少了网络上的广播风暴问题，提高了网络效率。

RIP 的工作机制基于距离矢量算法，路由器通过交换彼此的整个路由表来学习远程网络的存在和距离。每个路由器根据从邻居路由器接收到的信息，计算到

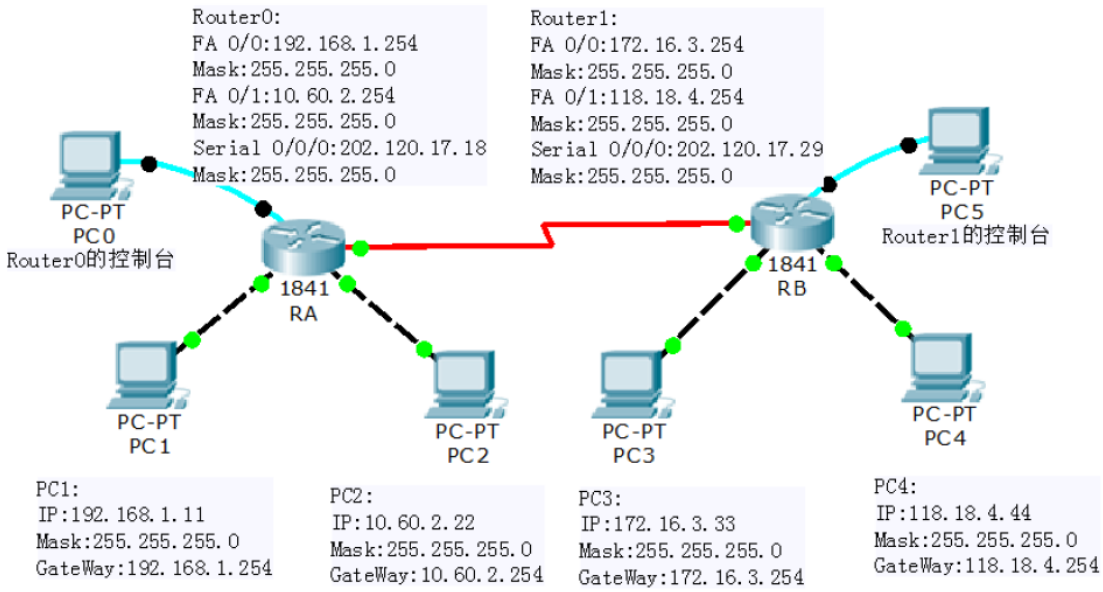
每个目的地的最短距离，并根据这些信息更新自己的路由表。

**【实验设备】**

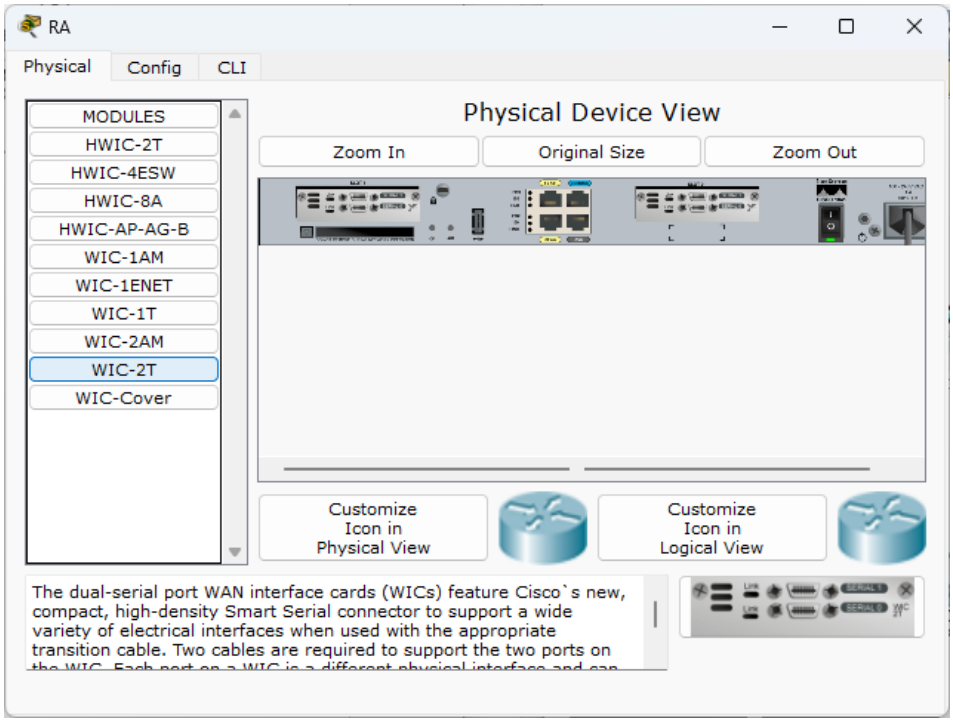
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

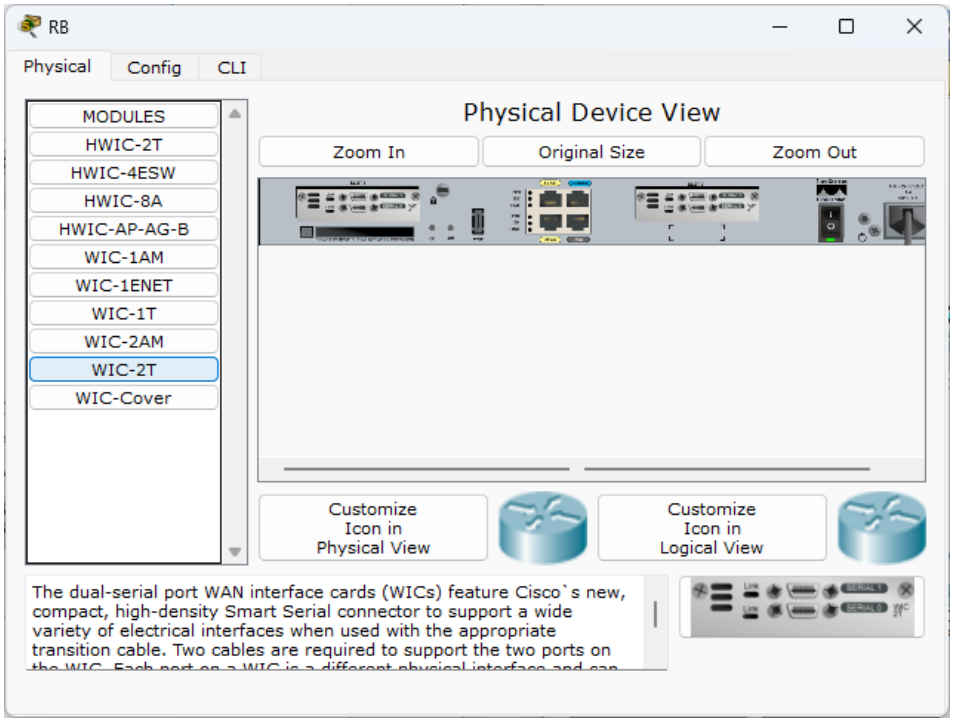
**【实验步骤】**

1. 规划网络地址及拓扑图。

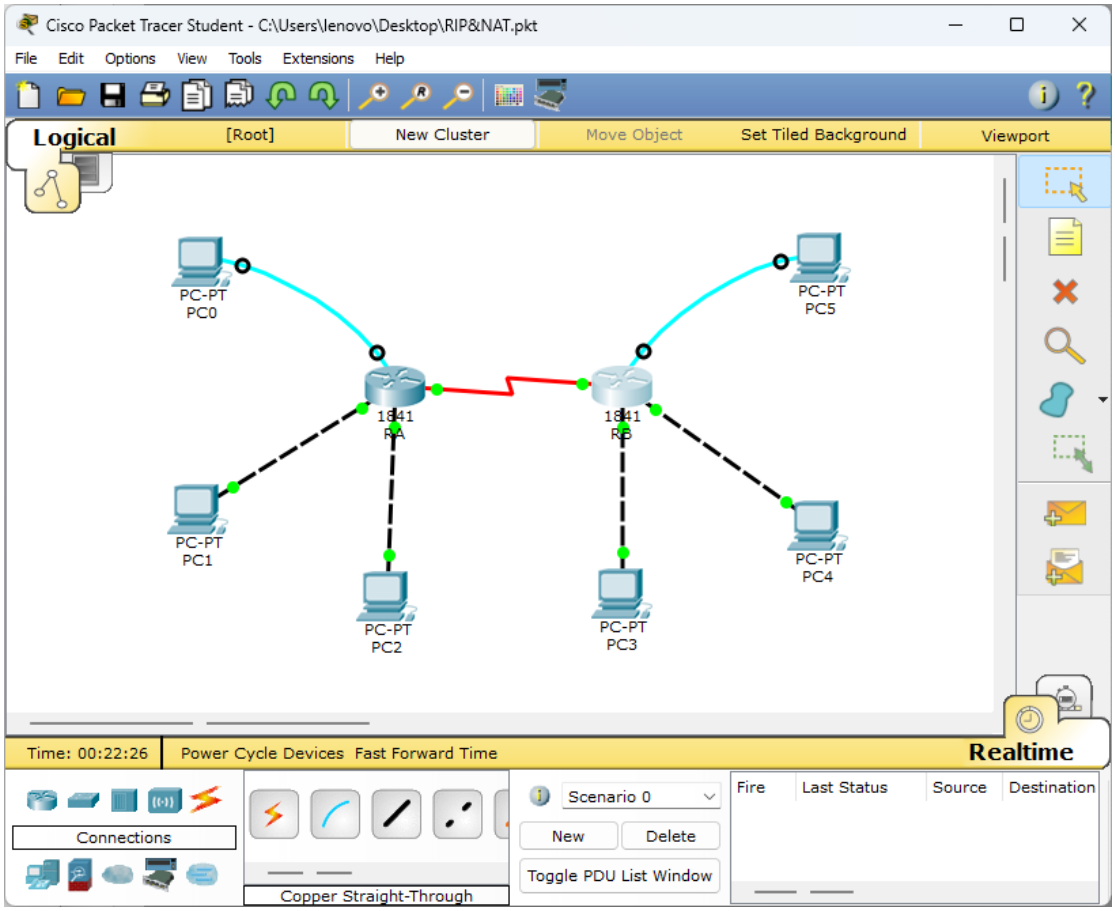



2. 在路由器 A 和路由器 B 中分别安装 WIC-2T，并重启设备。

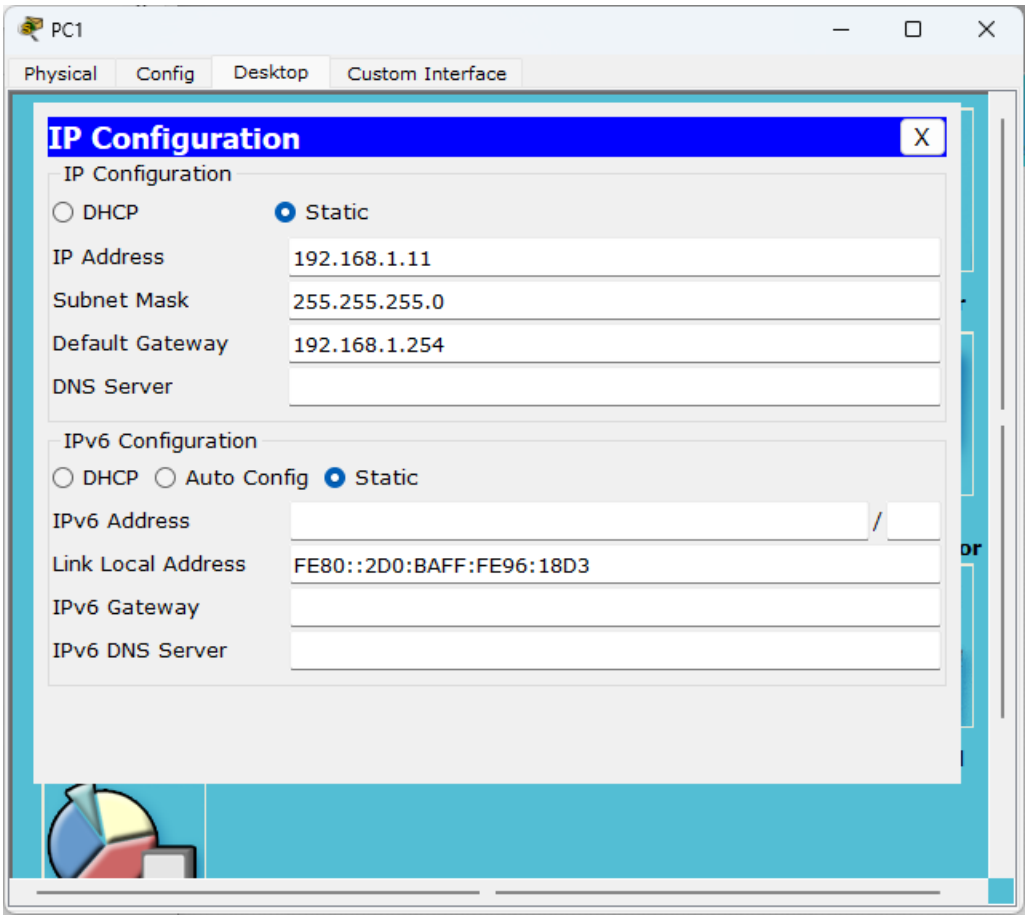


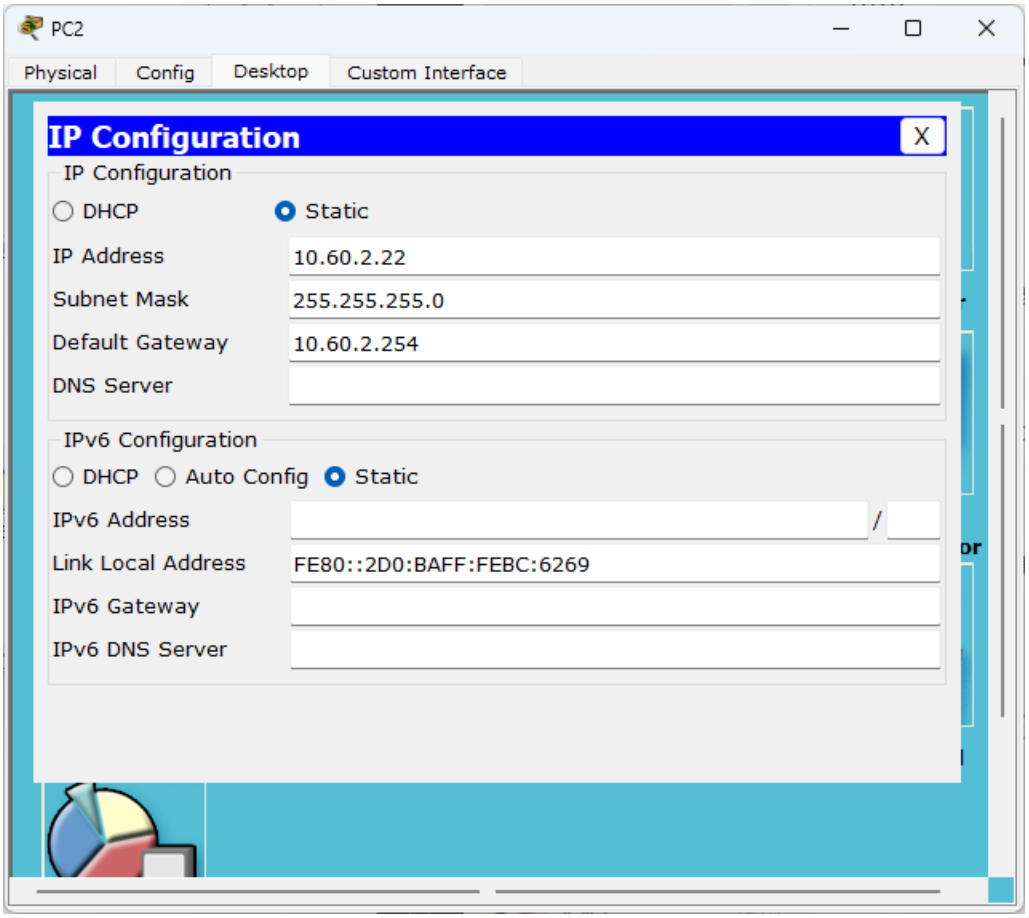


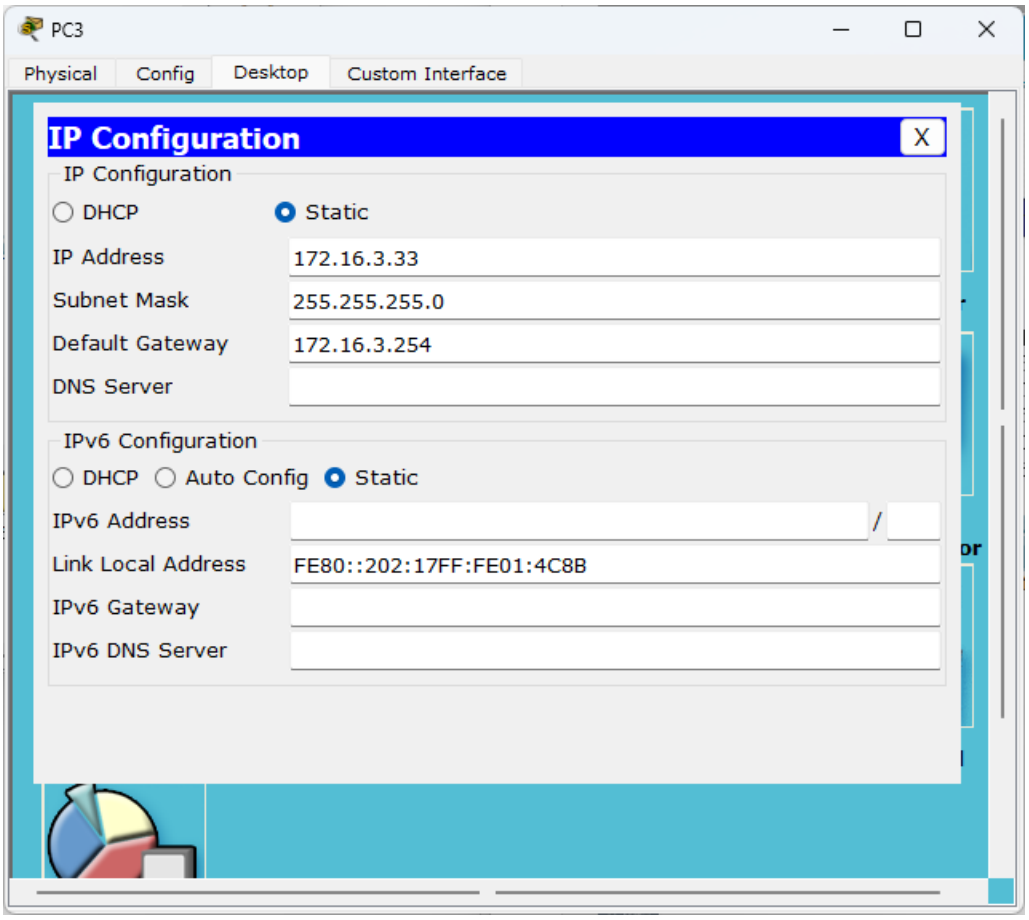

3. 启动 Cisco Packet Tracer，按照上述拓扑结构连接设备。

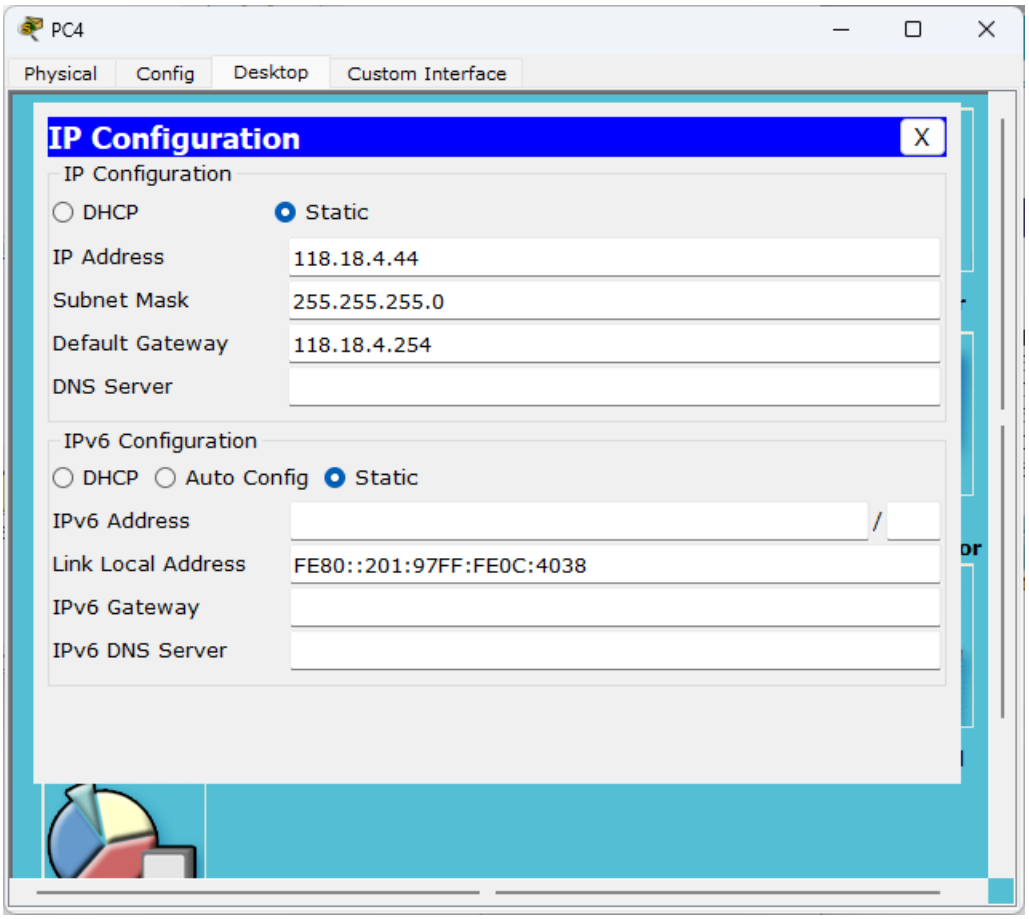



4. 配置 PC 机的 IP 地址、子网掩码和网关。


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE96:18D3
IPv6 Gateway
IPv6 DNS Server


PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.60.2.22
Subnet Mask
255.255.255.0
Default Gateway
10.60.2.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FEBC:6269
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
172.16.3.33
Subnet Mask
255.255.255.0
Default Gateway
172.16.3.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:17FF:FE01:4C8B
IPv6 Gateway
IPv6 DNS Server


PC4
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
118.18.4.44
Subnet Mask
255.255.255.0
Default Gateway
118.18.4.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE0C:4038
IPv6 Gateway
IPv6 DNS Server

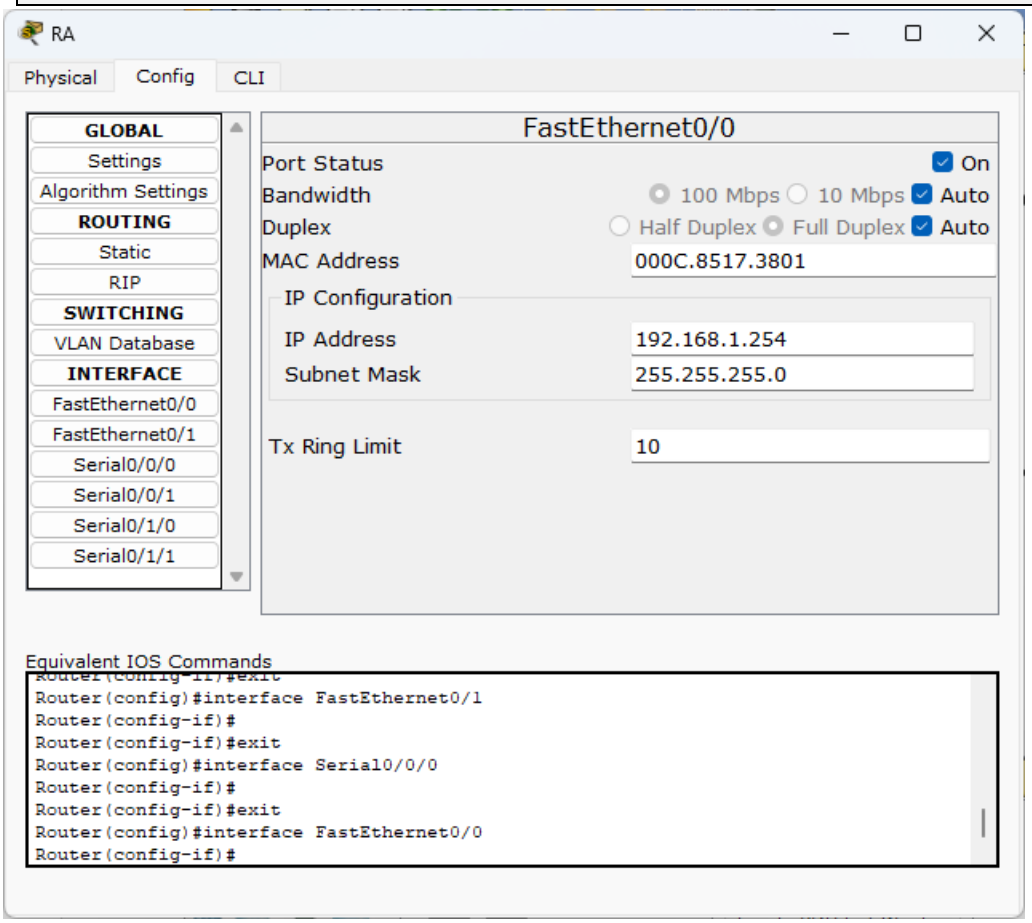
5. 配置路由器的端口地址和串口端口地址。

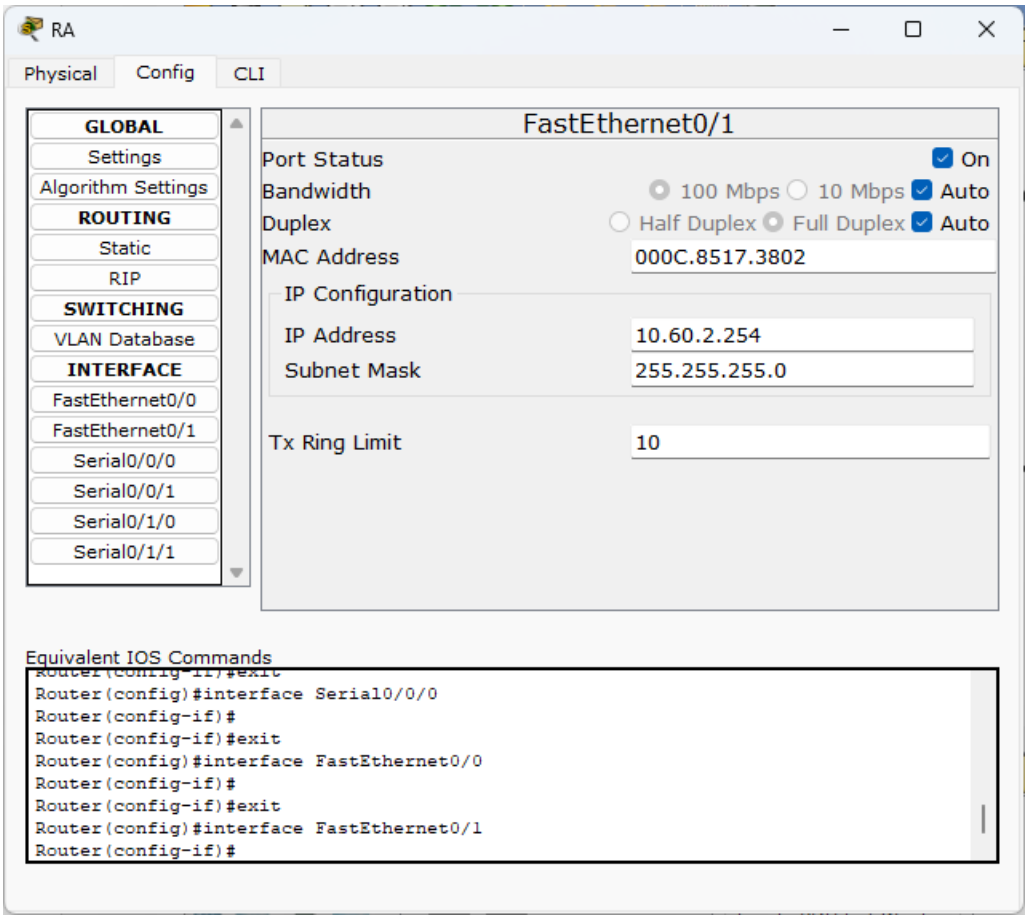
- 在路由器 A 的 CLI 中输入以下命令：

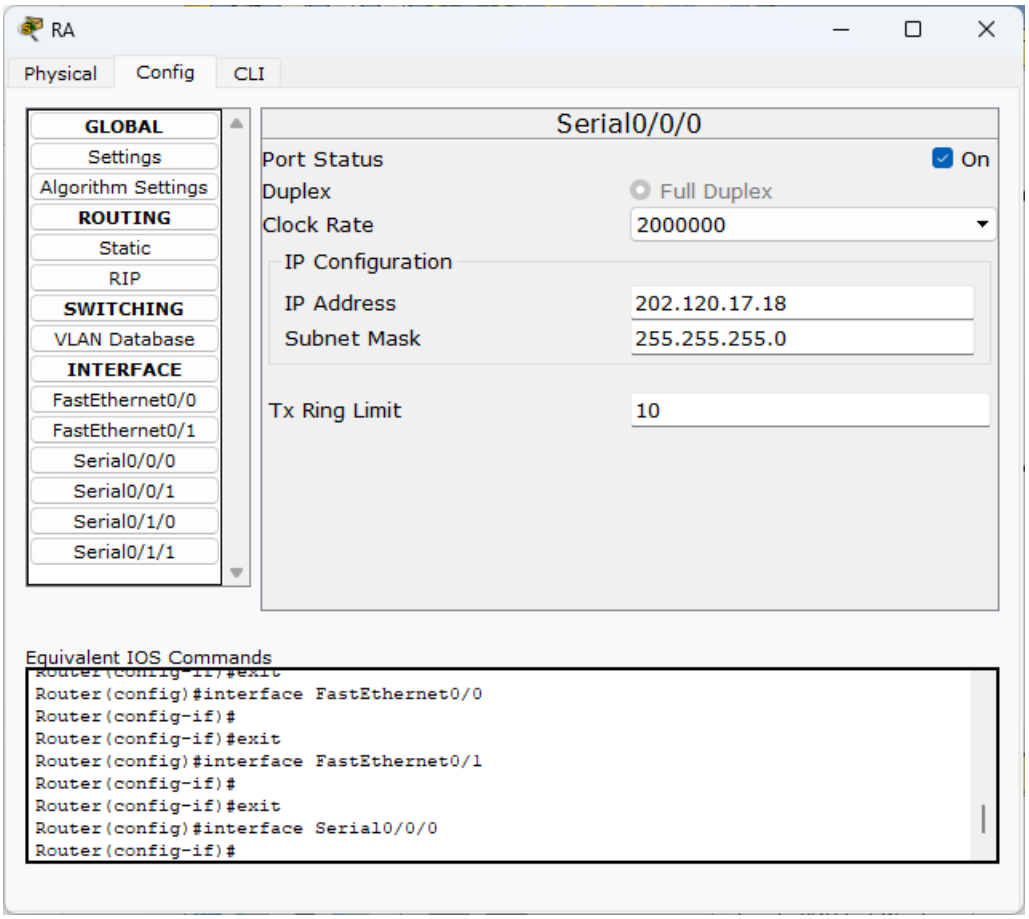
```
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.18 255.255.255.0
Clock rate 56000
```

- 在路由器 B 的 CLI 中输入以下命令：

```
interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.29 255.255.255.0
Clock rate 56000
```




RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8517.3802
IP Configuration
IP Address
10.60.2.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#


RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
202.120.17.18
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#

RB

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/0

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8101 |
| IP Configuration | |
| IP Address | 172.16.3.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

RB

Physical | Config | CLI

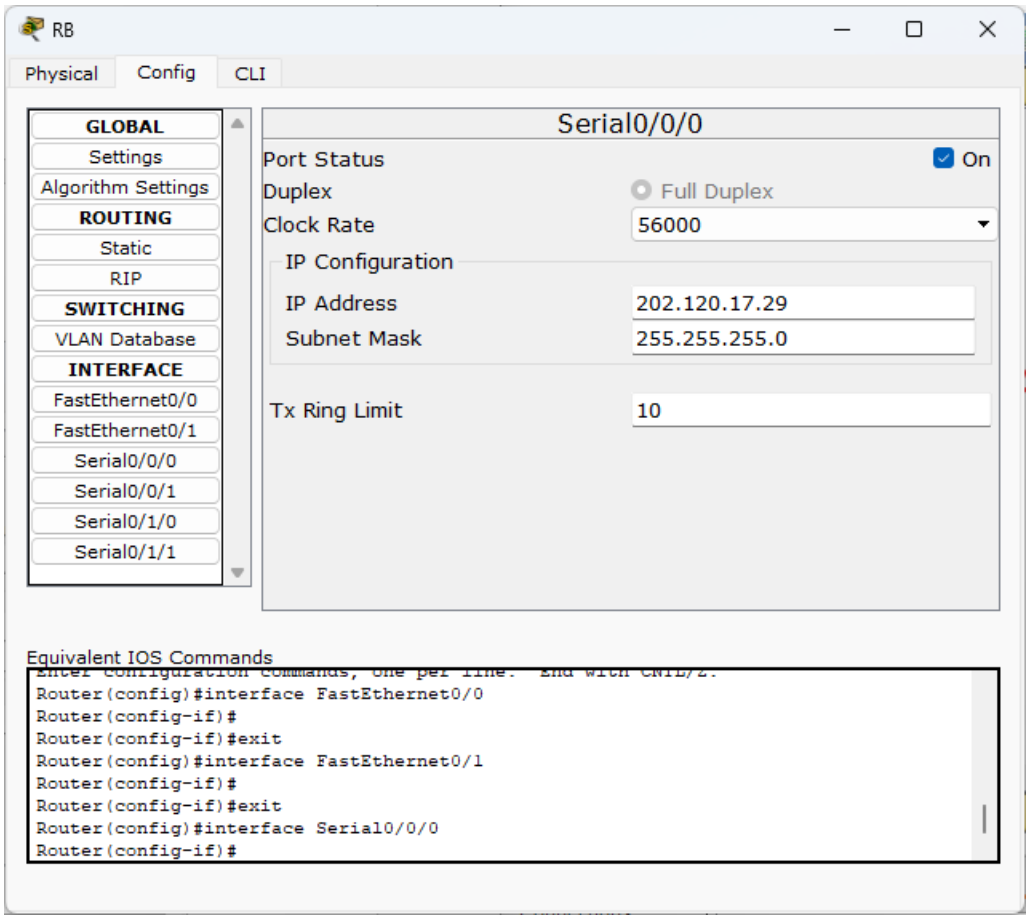
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/1

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8102 |
| IP Configuration | |
| IP Address | 118.18.4.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
```

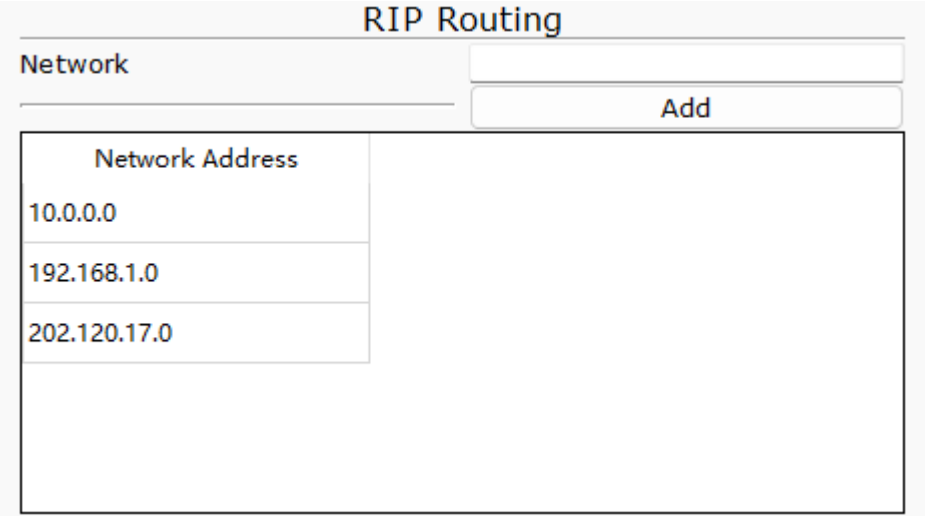



6. 几台 PC 机相互使用 ping 命令，观察实验结果。

7. 配置路由器 A 的 RIP 路由表。

- 在路由器 A 的 CLI 中输入以下命令：

```
router rip
network 192.168.1.11
network 10.60.2.22
network 202.120.17.18
```

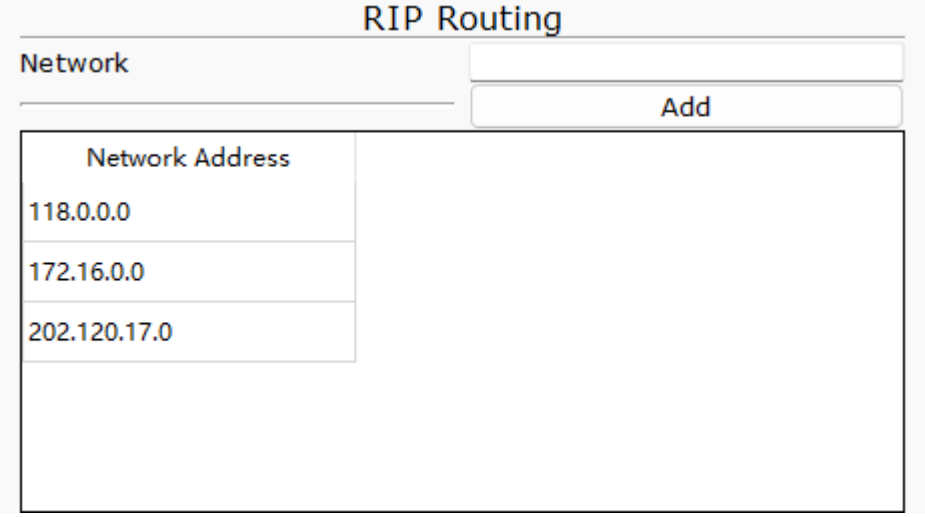


8. 几台 PC 机相互使用 ping 命令，观察实验结果。

9. 配置路由器 B 的 RIP 路由表。

- 在路由器 B 的 CLI 中输入以下命令：

```
router rip
network 172.16.3.33
network 118.18.4.44
network 202.120.17.29
```




10. 几台 PC 机相互使用 ping 命令，观察实验结果。

**【实验现象】**

1. 在配置路由器 A 和路由器 B 的 RIP 路由表之前，几台 PC 机相互使用 ping 命令。观察到如下实验现象：

   通过相同路由器连接的 PC 机之间相互 ping 成功。

   通过不同路由器连接的 PC 机之间相互 ping 失败。

- PC1 分别 ping PC2、PC3、PC4：

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- PC2 分别 ping PC1、PC3、PC4：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Request timed out.

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- PC3 分别 ping PC1、PC2、PC4：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Request timed out.
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
Reply from 118.18.4.44: bytes=32 time=1ms TTL=127
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC4 分别 ping PC1、PC2、PC3：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 172.16.3.33: bytes=32 time=1ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2. 在配置路由器 A 或路由器 B 的 RIP 路由表之后，几台 PC 机相互使用 ping 命令。观察到如下实验现象：

   通过相同路由器连接的 PC 机之间相互 ping 成功。

   通过不同路由器连接的 PC 机之间相互 ping 失败。

- PC1 分别 ping PC2、PC3、PC4：

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- PC2 分别 ping PC1、PC3、PC4：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Reply from 10.60.2.254: Destination host unreachable.
Request timed out.

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- PC3 分别 ping PC1、PC2、PC4：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.
Reply from 172.16.3.254: Destination host unreachable.

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Request timed out.
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
Reply from 118.18.4.44: bytes=32 time=1ms TTL=127
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC4 分别 ping PC1、PC2、PC3：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.
Reply from 118.18.4.254: Destination host unreachable.

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 172.16.3.33: bytes=32 time=1ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

3. 在配置路由器 A 和路由器 B 的 RIP 路由表之后，几台 PC 机相互使用 ping 命令。观察到如下实验现象：

   通过相同和不同路由器连接的 PC 机之间相互都 ping 成功。

- PC1 分别 ping PC2、PC3、PC4：

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 172.16.3.33: bytes=32 time=1ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Request timed out.
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
Reply from 118.18.4.44: bytes=32 time=1ms TTL=127
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC2 分别 ping PC1、PC3、PC4：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 172.16.3.33: bytes=32 time=1ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Request timed out.
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
Reply from 118.18.4.44: bytes=32 time=1ms TTL=127
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC3 分别 ping PC1、PC2、PC4：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Request timed out.
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
Reply from 118.18.4.44: bytes=32 time=1ms TTL=127
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC4 分别 ping PC1、PC2、PC3：

```
PC>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=0ms TTL=127
Reply from 192.168.1.11: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
PC>ping 10.60.2.22

Pinging 10.60.2.22 with 32 bytes of data:

Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127
Reply from 10.60.2.22: bytes=32 time=0ms TTL=127

Ping statistics for 10.60.2.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 172.16.3.33: bytes=32 time=1ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127
Reply from 172.16.3.33: bytes=32 time=0ms TTL=127

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

**【分析讨论】**

在未配置 RIP 之前，同一路由器下的 PC 机能够相互通信，而不同路由器连接的 PC 机间通信失败。这是因为在未配置 RIP 的情况下，路由器不具备将数据包传递到其他网络的路由信息。

在配置了一个路由器的 RIP 之后，尽管该路由器下的 PC 机之间可以正常通信，但是与另一个未配置 RIP 的路由器下的 PC 机间的通信仍然是失败的。这说明了仅部分配置 RIP 是不足以实现网络间全面互通的。

当两个路由器都配置了 RIP 之后，所有 PC 机无论是连接同一个路由器还是不同路由器，都能够相互成功地通信。这是因为 RIP 配置后，路由器之间能够交换各自的路由表，从而获得到达网络中任何部分的路由信息。此时，数据包可以根据这些路由信息被正确地传递到目的地。

# 实验 14：NAT 网络地址转换实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/11 |

**【实验目的】**

1. 理解 NAT 技术的基本原理：学习网络地址转换（NAT）如何解决 IP 地址不足的问题，并理解其如何提供额外的网络安全层，通过隐藏网络内部的计算机来防止外部攻击。
2. 掌握 NAT 配置步骤：通过实际配置 NAT，包括静态 NAT 和 NAPT（网络端口地址转换），深入理解 NAT 的配置流程和操作。
3. 应用 NAT 技术解决实际问题：通过配置和观察 NAT 操作，理解 NAT 在现实网络环境中的应用，如何有效地利用 NAT 技术管理和保护网络。
4. 提高网络配置技能：通过实际操作，提升配置网络地址、设备 IP 地址和静态路由的技能，增强对网络基础设施的理解和操作能力。
5. 观察和分析 NAT 效果：实验中通过观察 NAT 转换表和进行网络连通性测试，分析 NAT 配置的正确性和效果，加深对 NAT 工作机制的认识。

**【实验原理】**

**NAT 技术原理**

网络地址转换（NAT）是一种广泛应用的技术，主要用于解决 IP 地址不足的问题，并提供额外的网络安全保护。在大多数互联网接入场景中，尤其是家庭和小型企业网络，NAT 技术允许多个设备通过单一的公共 IP 地址接入互联网，从而节约了宝贵的 IP 资源。此外，NAT 提供了一层安全防护，通过隐藏内部网络的 IP 地址，从而防止外部直接访问内部网络设备。这种方法不仅保护了内部网络的隐私，也显著减少了外部攻击的风险。

NAT 的工作原理包括将内部网络的私有 IP 地址转换为公共 IP 地址，以及在必要时将公共 IP 地址转换回私有 IP 地址。这一过程涉及到修改经过 NAT 设备的数据包的 IP 地址信息。具体来说，当内部设备向互联网发送请求时，NAT 设备会替换这些请求的源 IP 地址为公共 IP 地址，并记录这一映射信息以供返回数据使用。当来自互联网的数据到达 NAT 设备时，NAT 会参考之前的映射记录，将数据包的目标地址从公共 IP 地址转换回原始的私有 IP 地址，确保数据正确送达内

部设备。

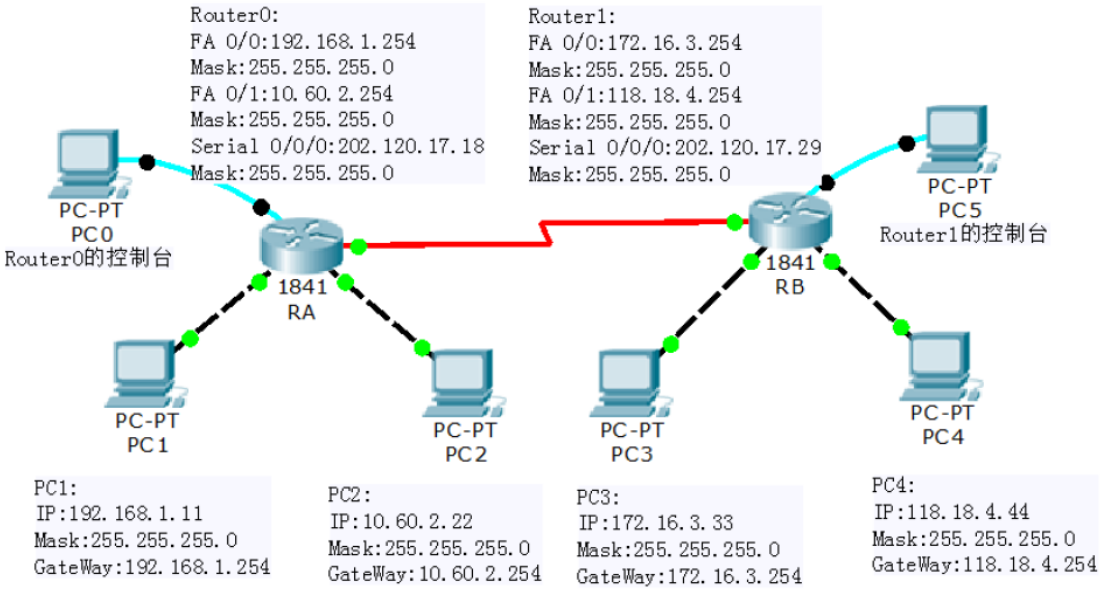
此外，NAT 可以分为静态 NAT、动态 NAT 和网络端口地址转换（NAPT）。静态 NAT 一对一地映射内部地址和外部地址，通常用于需要从外部网络直接访问的服务器。动态 NAT 则从地址池中分配地址，实现一对多的映射，但在现实应用中较少使用。NAPT 则是一种更为高效的方式，允许多个内部 IP 地址通过不同的端口映射到单一的外部 IP 地址上，这种方法在多设备共享单一出口的网络环境中尤其常见。这些技术的实现不仅提高了 IP 地址的使用效率，还增强了网络的安全性和灵活性。

**【实验设备】**

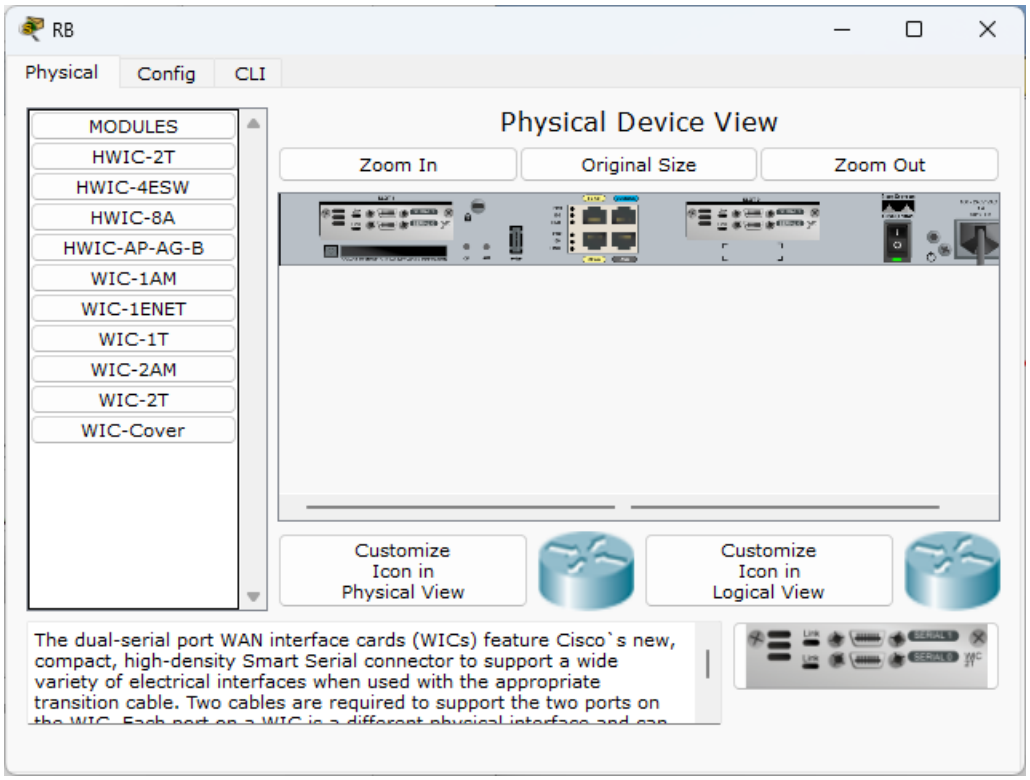
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

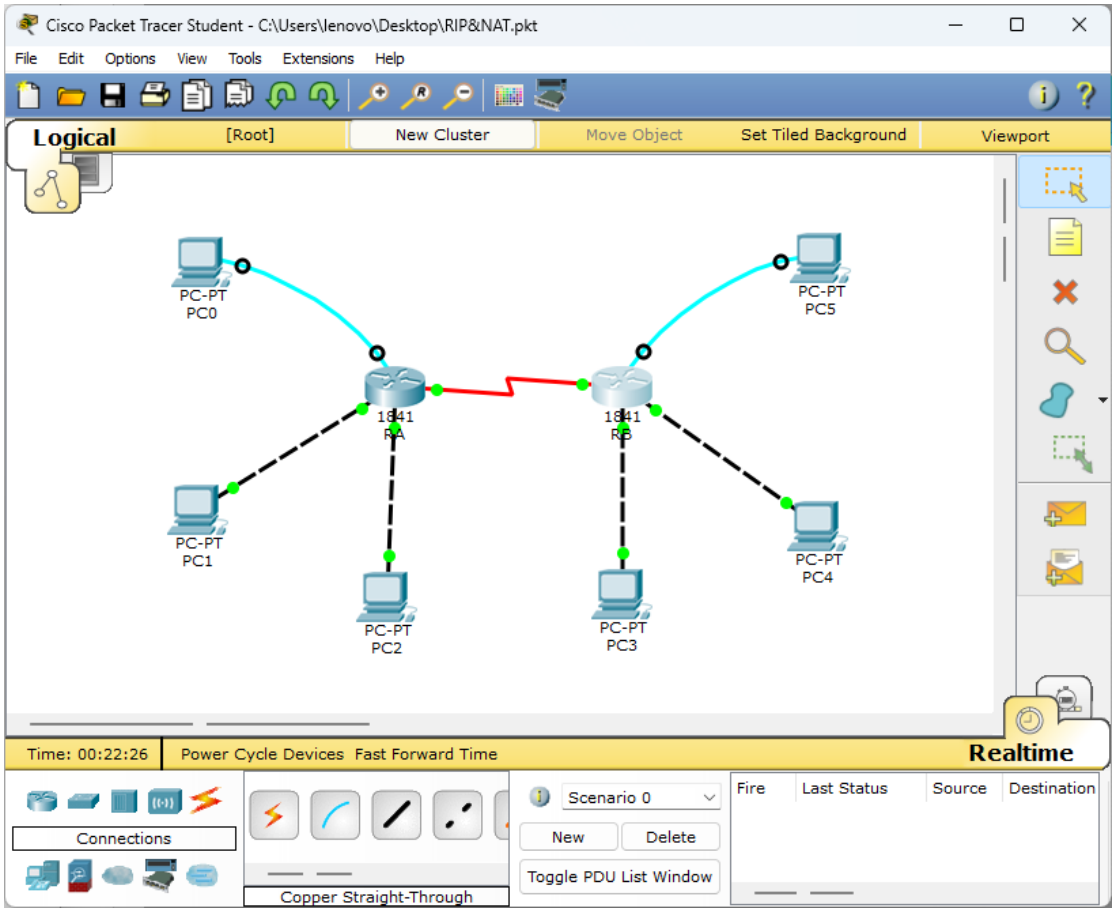
1. 规划网络地址及拓扑图。



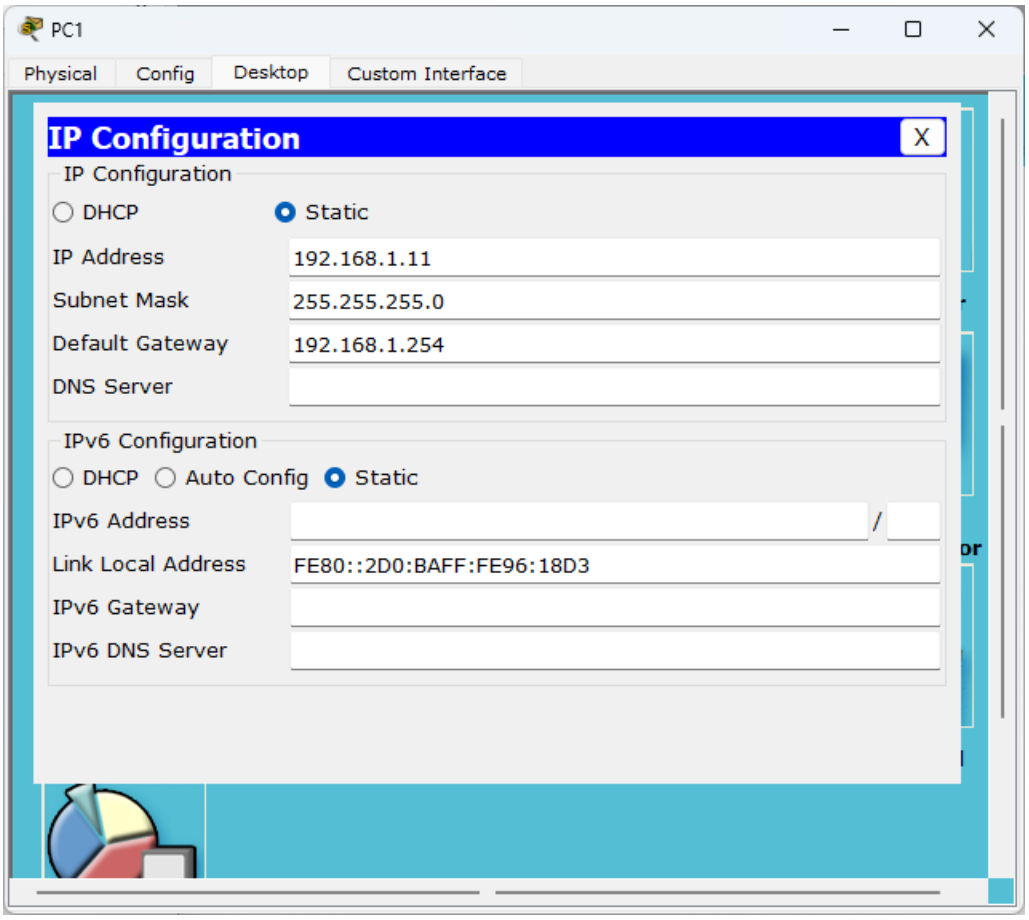

2. 在路由器 A 和路由器 B 中分别安装 WIC-2T，并重启设备。

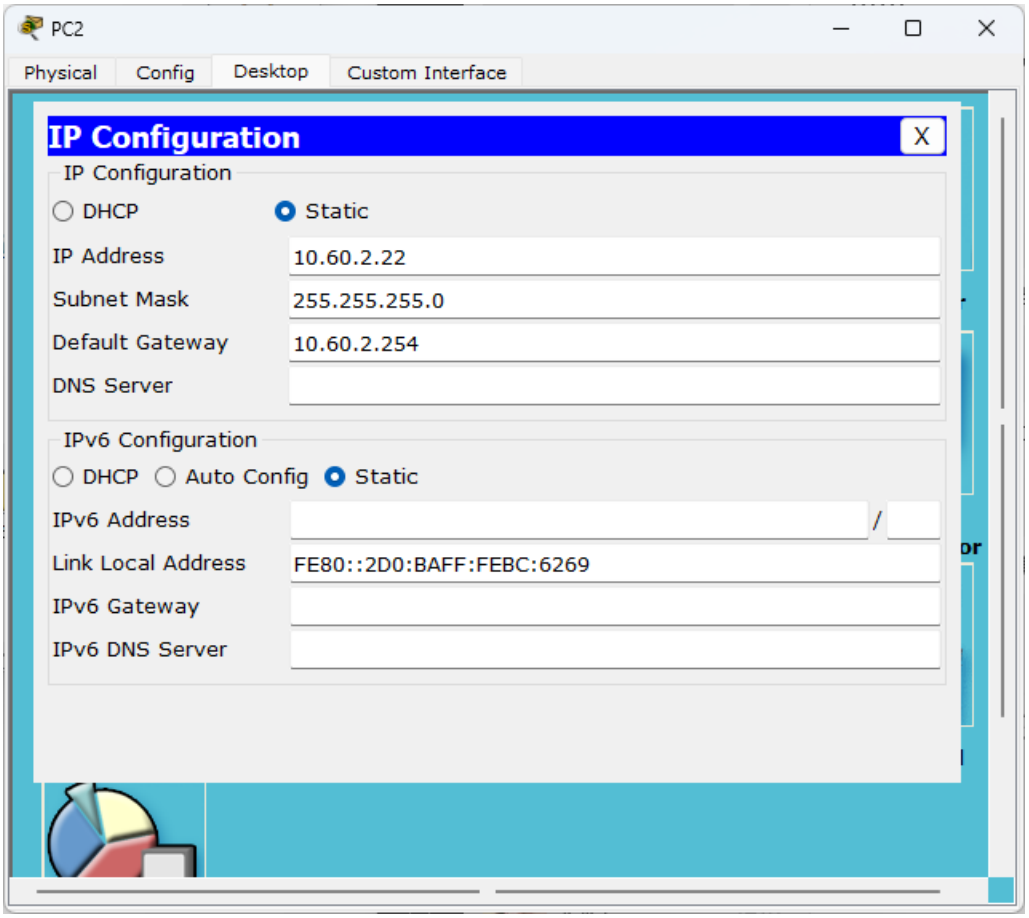


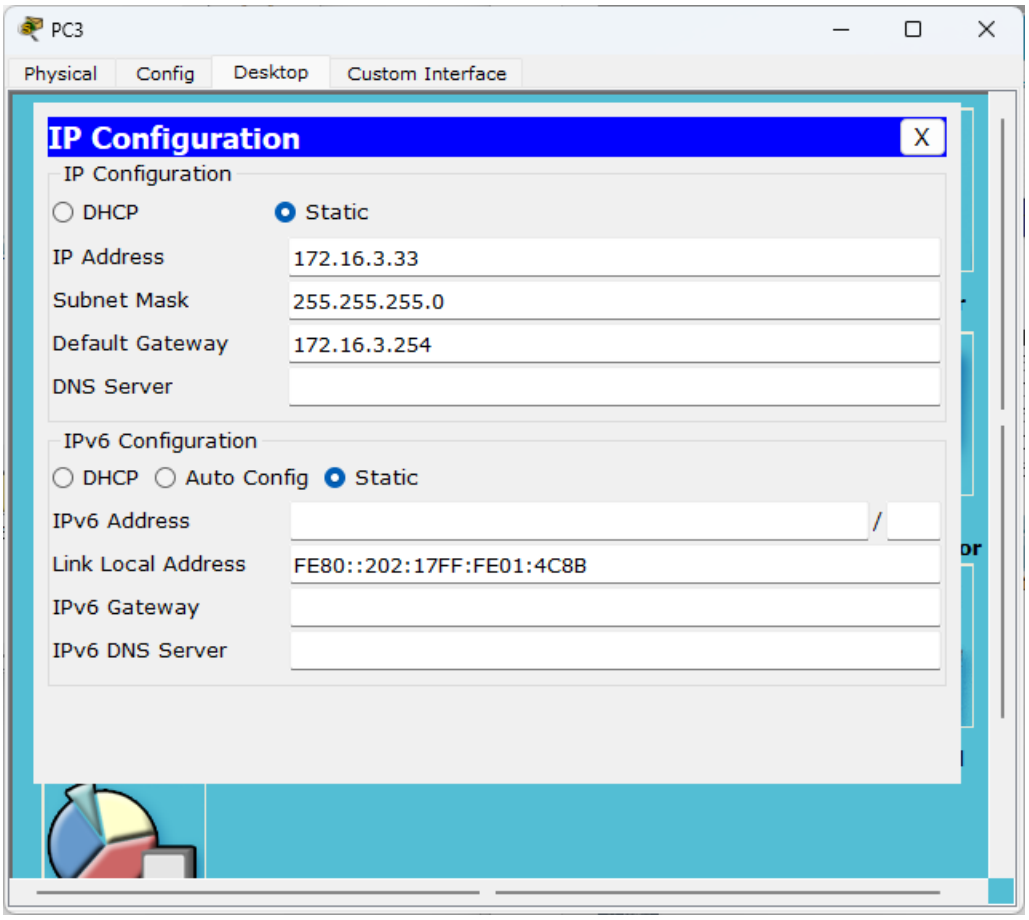

3. 启动 Cisco Packet Tracer，按照上述拓扑结构连接设备。

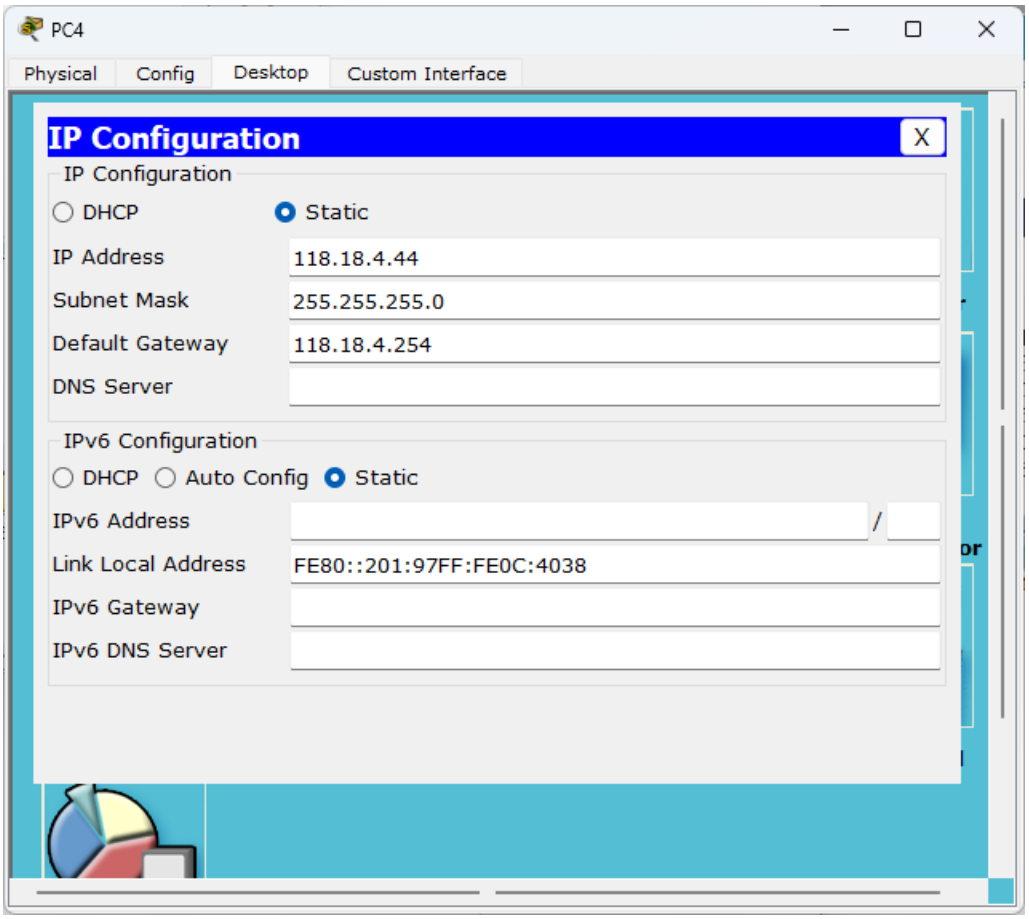



4. 配置 PC 机的 IP 地址、子网掩码和网关。


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE96:18D3
IPv6 Gateway
IPv6 DNS Server


PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.60.2.22
Subnet Mask
255.255.255.0
Default Gateway
10.60.2.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FEBC:6269
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
172.16.3.33
Subnet Mask
255.255.255.0
Default Gateway
172.16.3.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:17FF:FE01:4C8B
IPv6 Gateway
IPv6 DNS Server


PC4
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
118.18.4.44
Subnet Mask
255.255.255.0
Default Gateway
118.18.4.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE0C:4038
IPv6 Gateway
IPv6 DNS Server

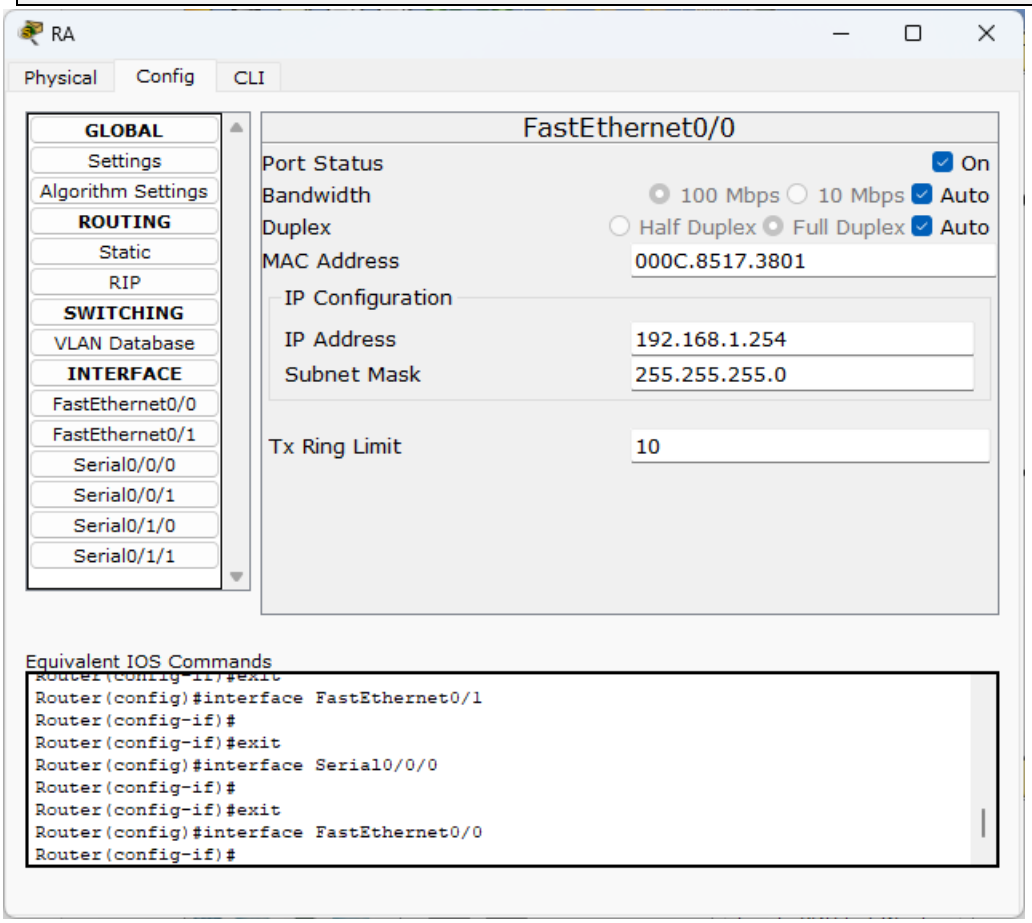
5. 配置路由器的端口地址和串口端口地址。

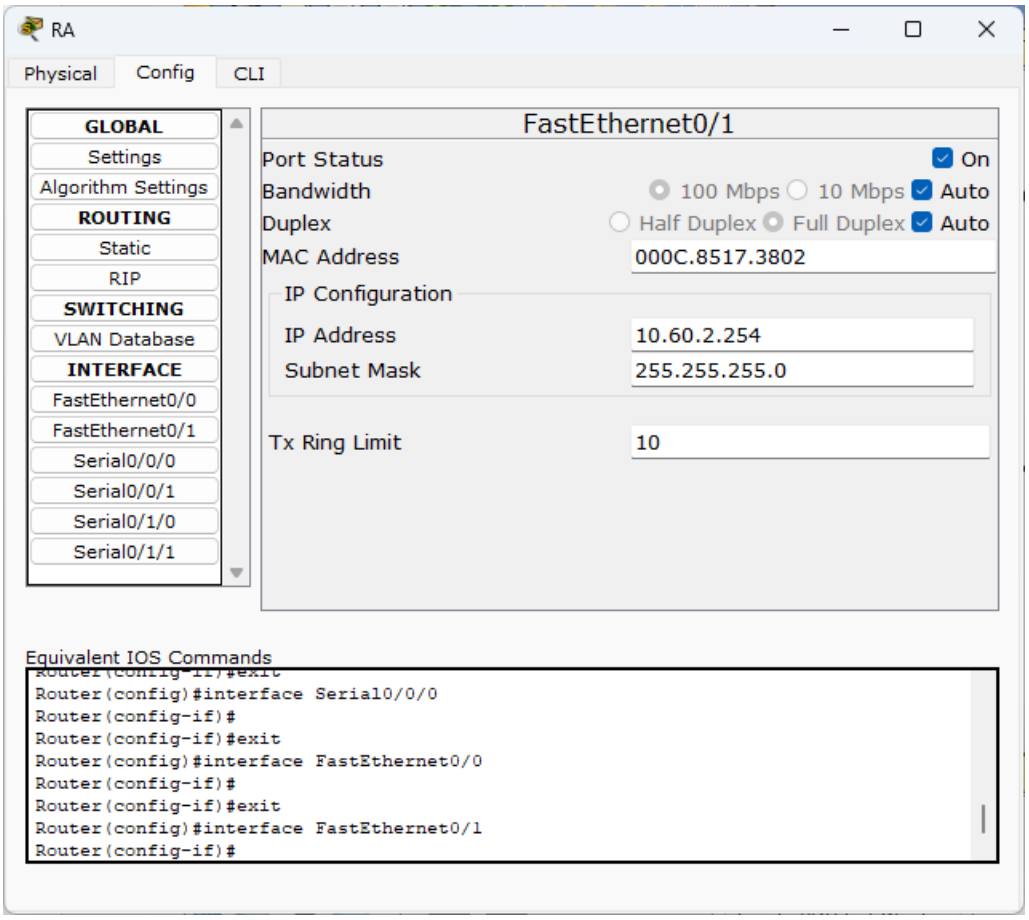
- 在路由器 A 的 CLI 中输入以下命令：

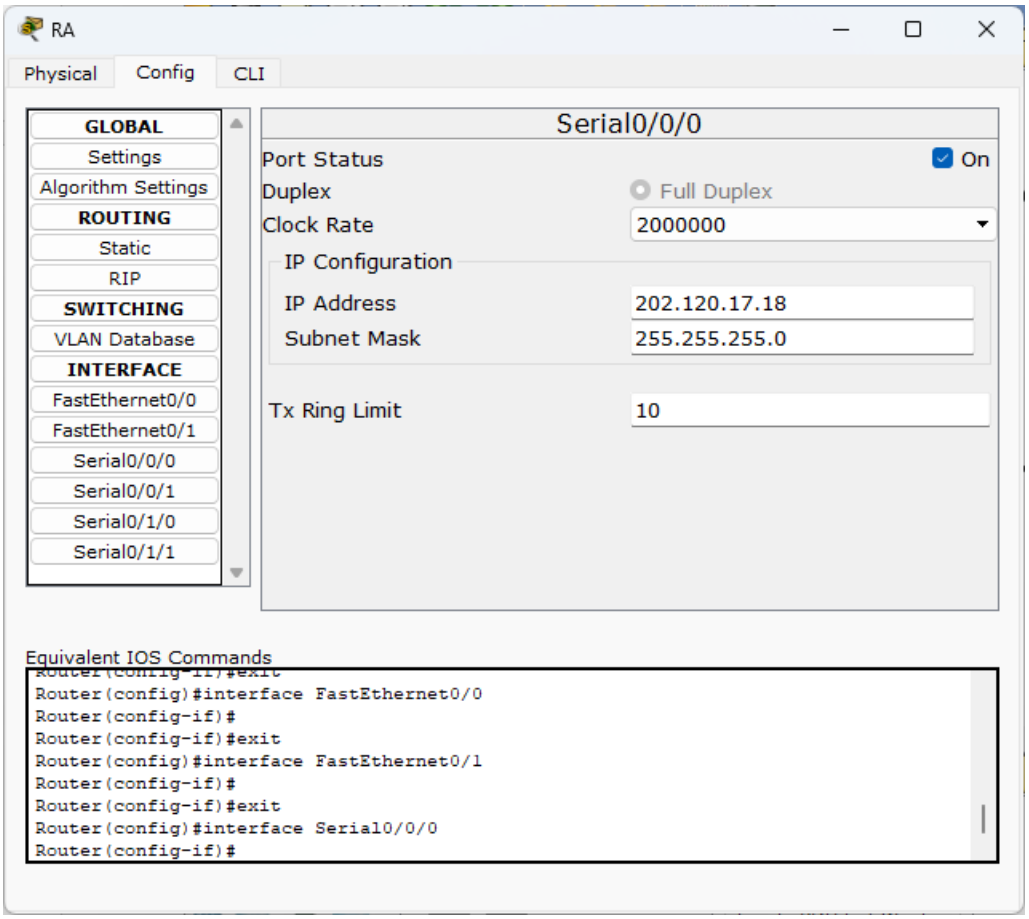
```
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.18 255.255.255.0
Clock rate 56000
```

- 在路由器 B 的 CLI 中输入以下命令：

```
interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.29 255.255.255.0
Clock rate 56000
```




RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8517.3802
IP Configuration
IP Address
10.60.2.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#


RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
202.120.17.18
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#

RB

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/0

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8101 |
| IP Configuration | |
| IP Address | 172.16.3.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

RB

Physical | Config | CLI

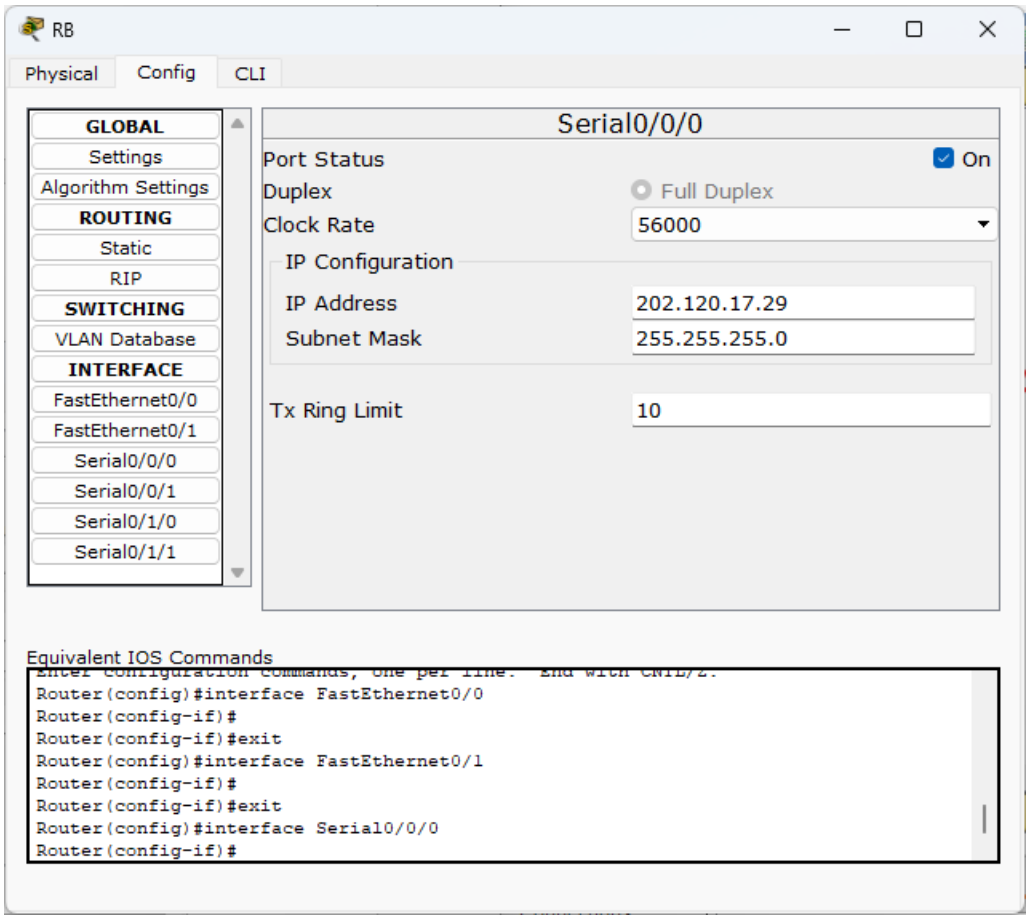
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/1

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8102 |
| IP Configuration | |
| IP Address | 118.18.4.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
```



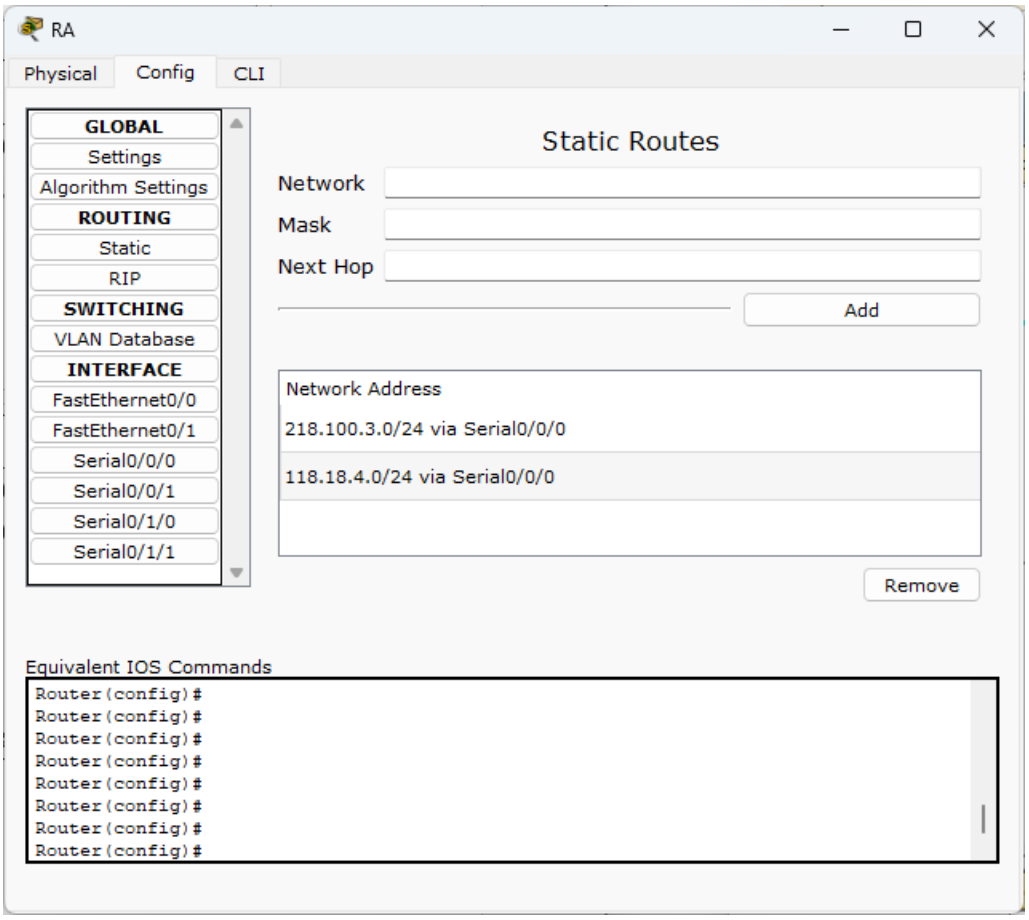

6. 配置路由器 A 和路由器 B 的静态路由表、NAT 出入口和 NAT 转换。

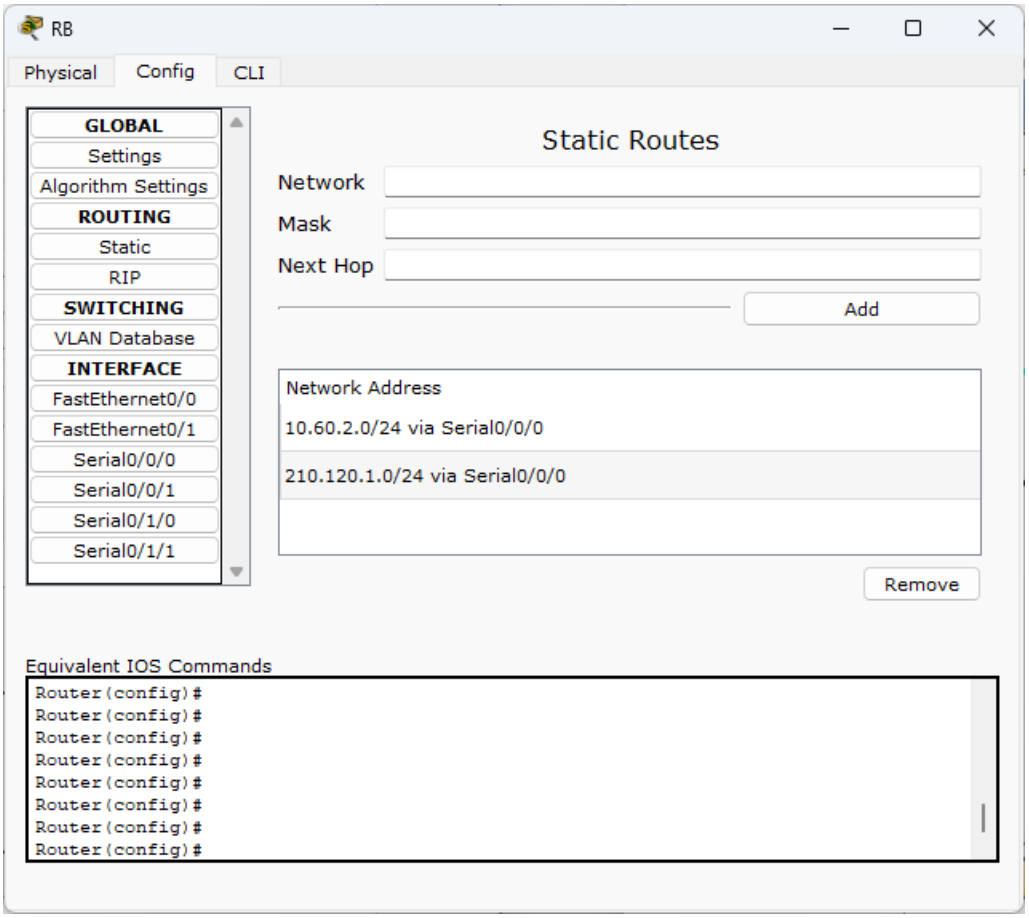
- 在路由器 A 的 CLI 中输入以下命令：

```
ip route 218.100.3.0 255.255.255.0 serial 0/0/0
ip route 118.18.4.0 255.255.255.0 serial 0/0/0
interface FastEthernet0/0
ip nat inside
interface Serial 0/0/0
ip nat outside
ip nat inside source static 192.168.1.11 210.120.1.11
```

- 在路由器 B 的 CLI 中输入以下命令：

```
ip route 10.60.2.0 255.255.255.0 serial 0/0/0
ip route 210.120.1.0 255.255.255.0 serial 0/0/0
interface FastEthernet0/0
ip nat inside
interface Serial 0/0/0
ip nat outside
ip nat inside source static 172.16.3.33 218.100.3.33
```


RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
218.100.3.0/24 via Serial0/0/0
118.18.4.0/24 via Serial0/0/0
Remove
Equivalent IOS Commands
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#


RB
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
10.60.2.0/24 via Serial0/0/0
210.120.1.0/24 via Serial0/0/0
Remove
Equivalent IOS Commands
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#

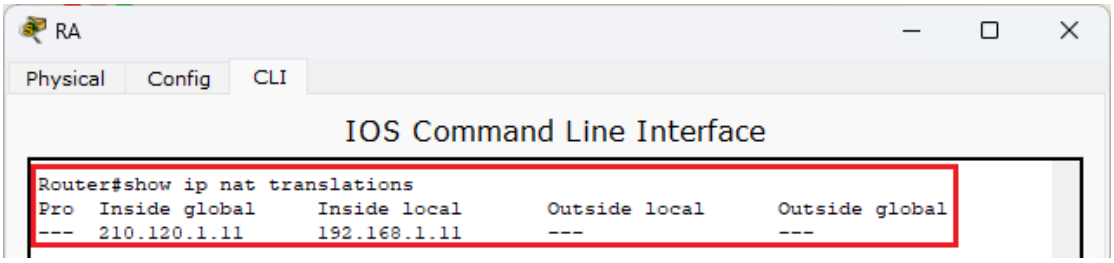
7. 在路由器 A 和路由器 B 的 CLI 中分别输入 show ip nat translations，观察实验结果。

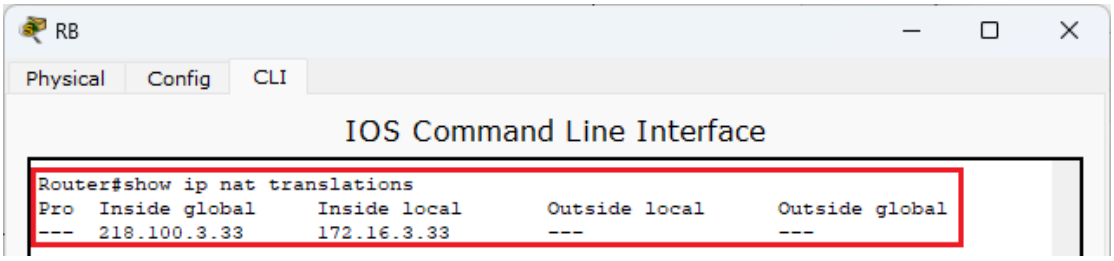
8. 在各自 PC 机分别进行以下 ping 测试，观察实验结果。

```
ping 192.168.1.11
ping 210.120.1.11
ping 10.60.2.22
ping 172.16.3.33
ping 218.100.3.33
ping 118.18.4.44
```

**【实验现象】**

1. 在路由器 A 和路由器 B 的 CLI 中分别输入 show ip nat translations，观察实验结果。




2. 在各自 PC 机分别进行以下 ping 测试，观察实验结果。

| ping 结果 | PC1 | PC2 | PC3 | PC4 |
|---|---|---|---|---|
| 192.168.1.11 | 成功 | 成功 | 失败 | 失败 |
| 210.120.1.11 | 失败 | 失败 | 成功 | 成功 |
| 10.60.2.22 | 成功 | 成功 | 成功 | 成功 |
| 172.16.3.33 | 失败 | 失败 | 成功 | 成功 |
| 218.100.3.33 | 成功 | 成功 | 失败 | 失败 |
| 118.18.4.44 | 成功 | 成功 | 成功 | 成功 |

**【分析讨论】**

在本次实验中，通过使用NAT（网络地址转换）技术，观察了四台PC在进行网络通信时的表现。NAT 技术不仅解决了 IP 地址不足的问题，还能够提供网络安全层，保护内部网络不被外部直接访问。以下是对实验结果的分析与讨论：

**一、NAT转换表**

在路由器A和路由器B的CLI中输入show ip nat translations命令，我们能够观察到 NAT 转换条目，显示了内部私有 IP 地址如何被映射到公共 IP 地址。这个转换表是NAT功能正常工作的关键，因为它保证了返回的数据能够正确地路由到发起请求的内部设备。

**二、Ping测试结果**

对本实验中的4个PC机的IP地址进行总结可以得到下表：

| IP地址 | 内部IP | 公共IP |
|---|---|---|
| PC1 | 192.168.1.11 | 210.120.1.11 |
| PC2 | 10.60.2.22 | |
| PC3 | 172.16.3.33 | 218.100.3.33 |
| PC4 | 118.18.4.44 | |

对内网 IP 地址的访问：同一网络内的 PC 能成功地互相访问对方的内部 IP 地址，而不同网络内的PC无法访问对方的内部IP地址。这表明NAT正常工作，阻止了不同网络间的直接内部IP访问，增加了网络的安全性。

对公网 IP 地址的访问：不同网络内的PC能成功访问对方的公共IP地址，而同一网络内的PC无法访问对方的公共IP地址。这显示了公共IP地址的可达性，允许跨网络的通信，同时还表明NAT的端口映射正常。

# 实验 15：帧中继（Frame Relay）配置实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/11 |

**【实验目的】**

本次实验的目的是学习和实践帧中继（Frame Relay）配置，这是一种重要的广域网（WAN）连接标准。实验的核心目标包括：

1. 理解帧中继技术的基础知识，包括其工作原理及关键技术概念，如虚电路（Virtual Circuits，VCs）、数据链路连接标识符（DLCI）以及逻辑链路控制和适配协议（LMI）类型。
2. 学习如何配置帧中继连接，包括设置路由器接口的封装类型、地址映射和 LMI 类型。
3. 实践帧中继的地址解析协议（ARP）和反向 ARP，通过动态和手动方式配置网络层地址和映射。
4. 验证配置的正确性和网络通信功能，通过在路由器间进行 ping 测试来检查接口之间的互通性。

**【实验原理】**

**帧中继（Frame Relay）技术**

1. 虚电路（Virtual Circuit, VC）
   - PVC（永久虚电路）：一旦建立，PVC 会持续存在，无需每次通信时重新建立，适用于常规和持续的数据传输需求。
   - SVC（交换虚电路）：为临时或需求驱动的通信提供服务，每次通信前需建立连接，通信结束后连接会断开，适用于不定期的数据交换。
2. 数据链路连接标识符（DLCI）
   - DLCI 是帧中继网络中分配给每条虚电路的唯一标识符，用于在一个物理链路上标记和区分不同的虚拟连接。
   - DLCI 不提供端到端的全局意义，其作用范围限定于单个链路。
3. 封装与映射
   - 帧中继协议允许数据封装，并使用 DLCI 进行路由，将每个数据帧映射到正确的虚电路。

- 地址映射可以通过动态或静态方式配置，动态地址映射依赖于帧中继地址解析协议（ARP），以动态学习网络中其他设备的地址。

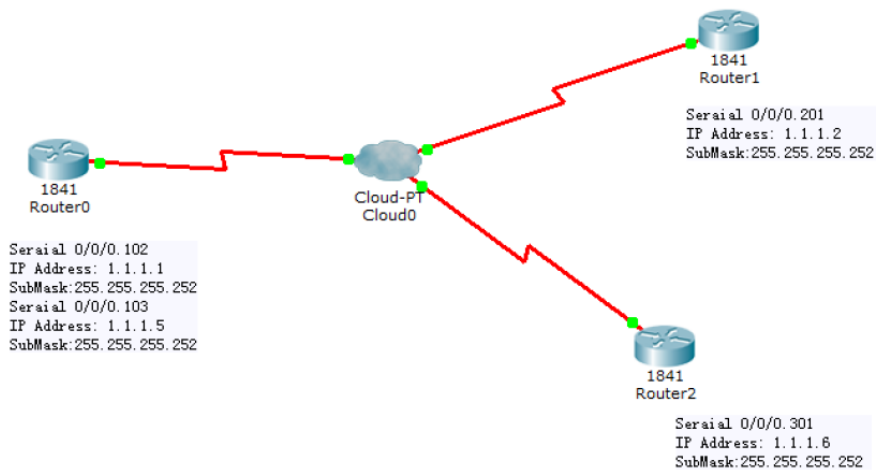
4. 逻辑链路控制和适配（LMI）
   - LMI 是一种信令协议，用于在帧中继交换机和连接的设备（如路由器）之间管理和维护虚电路的状态。
   - 提供几种类型的 LMI，包括 ITU-T Q.933 和 ANSI T1.617，以支持不同地区和设备的标准兼容性。
5. 性能与效率
   - 帧中继技术通过简化高性能数据传输和利用更可靠的网络基础设施（如光纤），以及减少传输中的错误校验负担（依靠高层协议进行错误处理），来提高传输效率。
6. 配置与应用
   - 帧中继配置过程包括设定适当的接口封装类型，配置必要的虚电路和DLCI，以及可选地实现路由协议或静态路由以确保数据正确路由。此外，交换机配置涉及到虚电路的创建和维护，以及确保通过正确的输出端口转发数据帧。

**【实验设备】**

1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

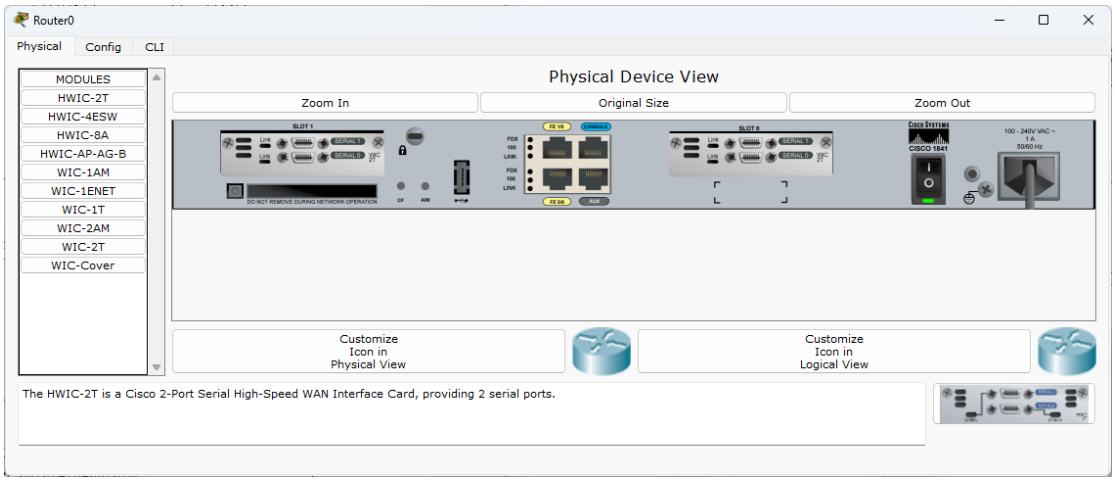
**【实验步骤】**

1. 规划网络地址及拓扑图。

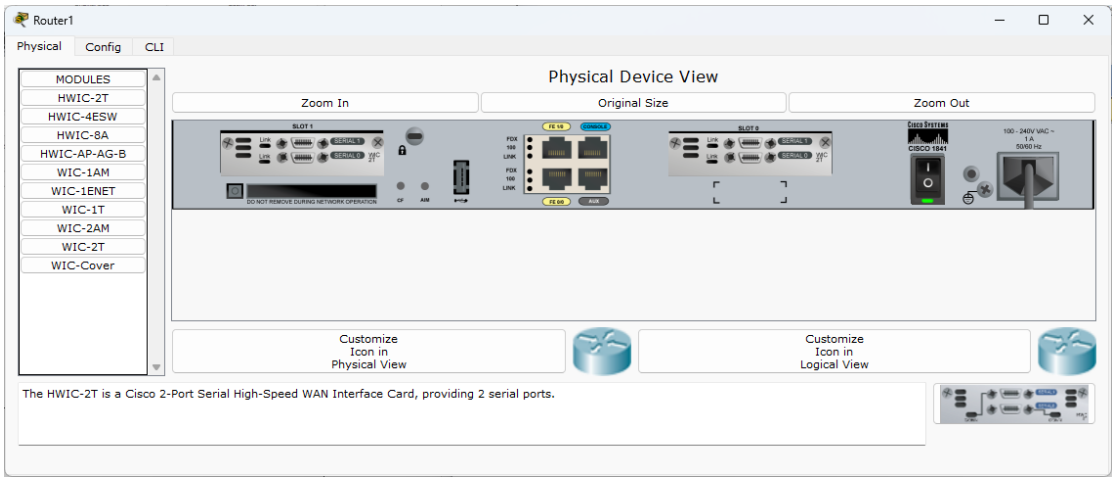


2. 在 Router0、Router1 和 Router2 中分别安装 WIC-2T，并重启设备。

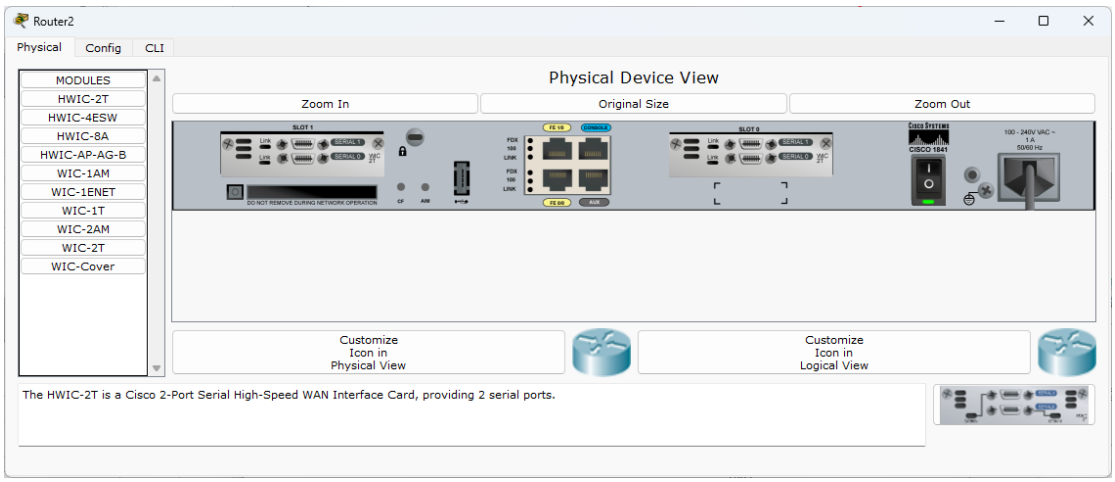
- 在 Router0 中安装 WIC-2T。



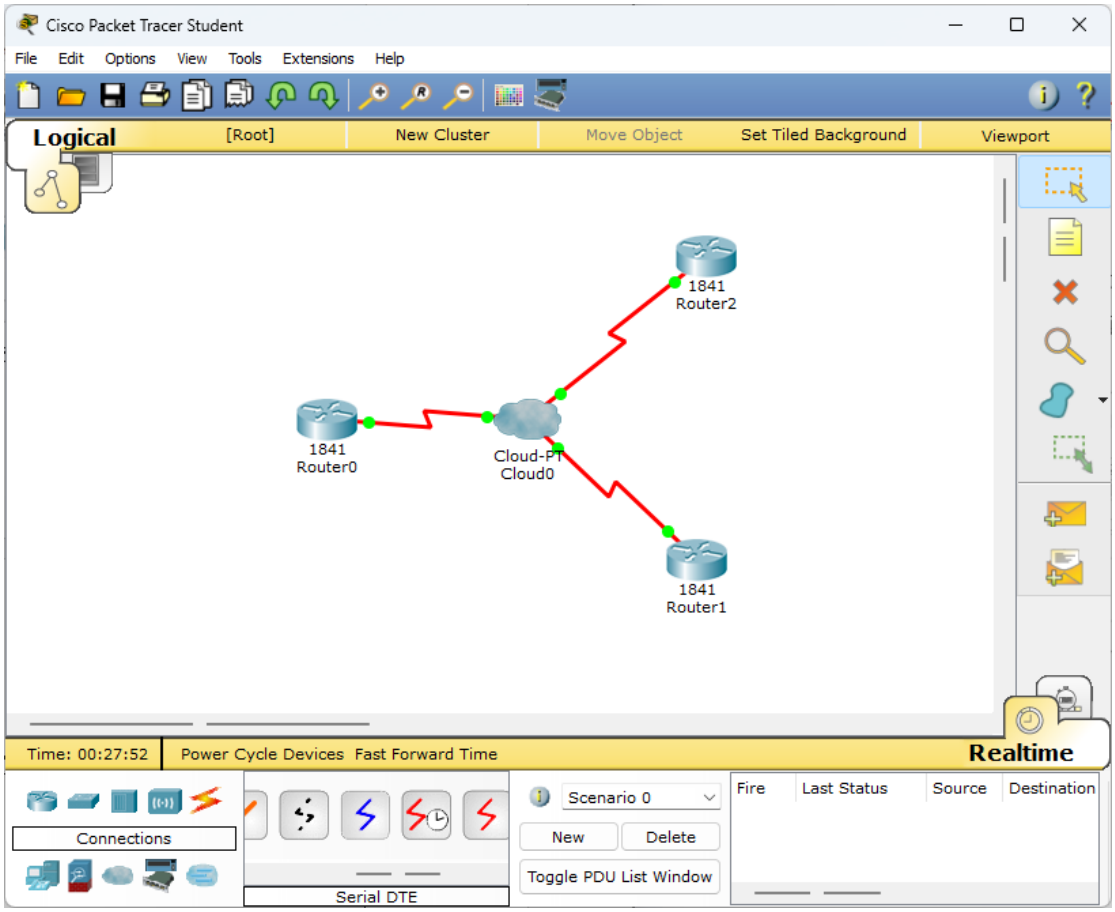

- 在 Router1 中安装 WIC-2T。



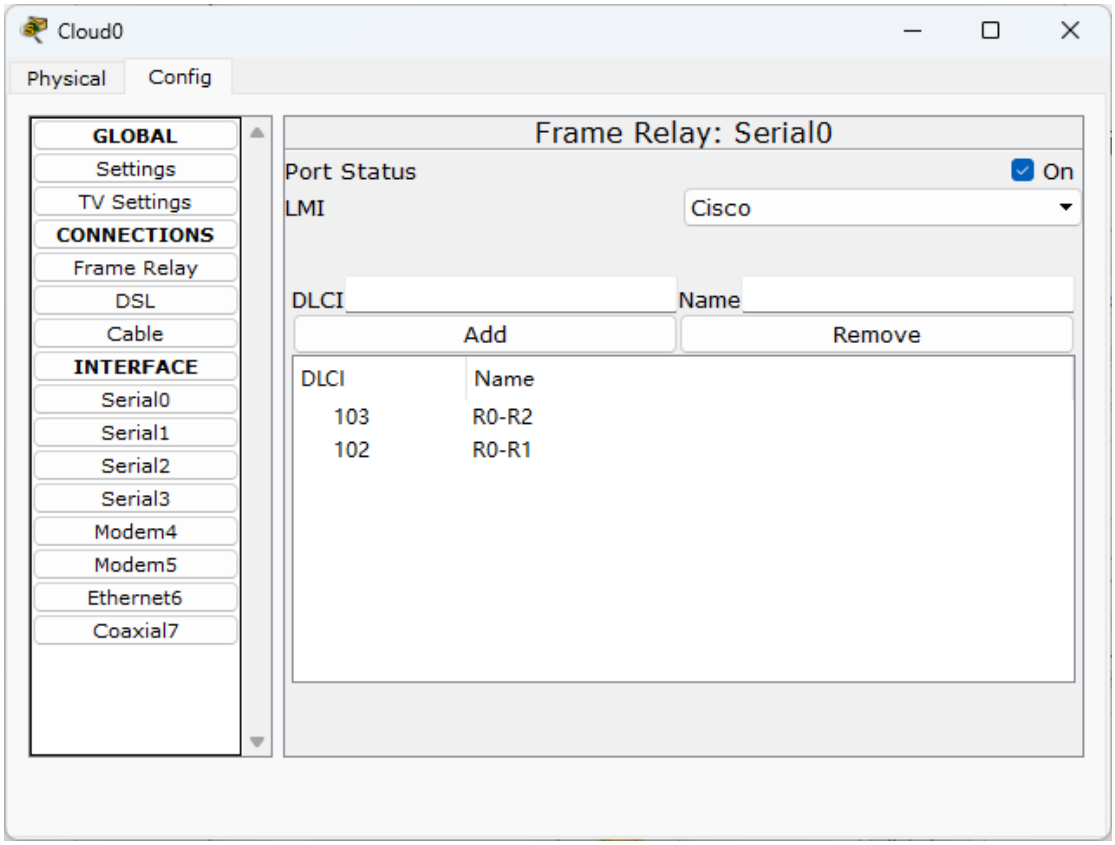

- 在 Router2 中安装 WIC-2T。

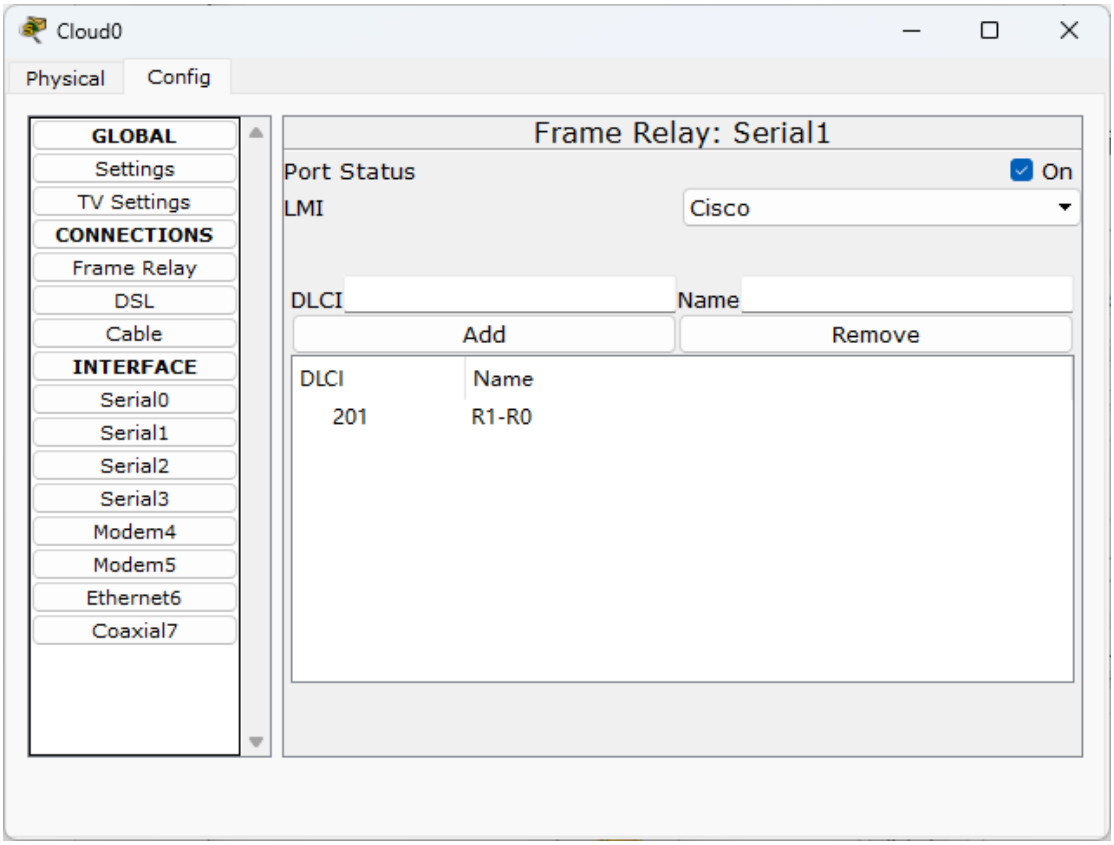


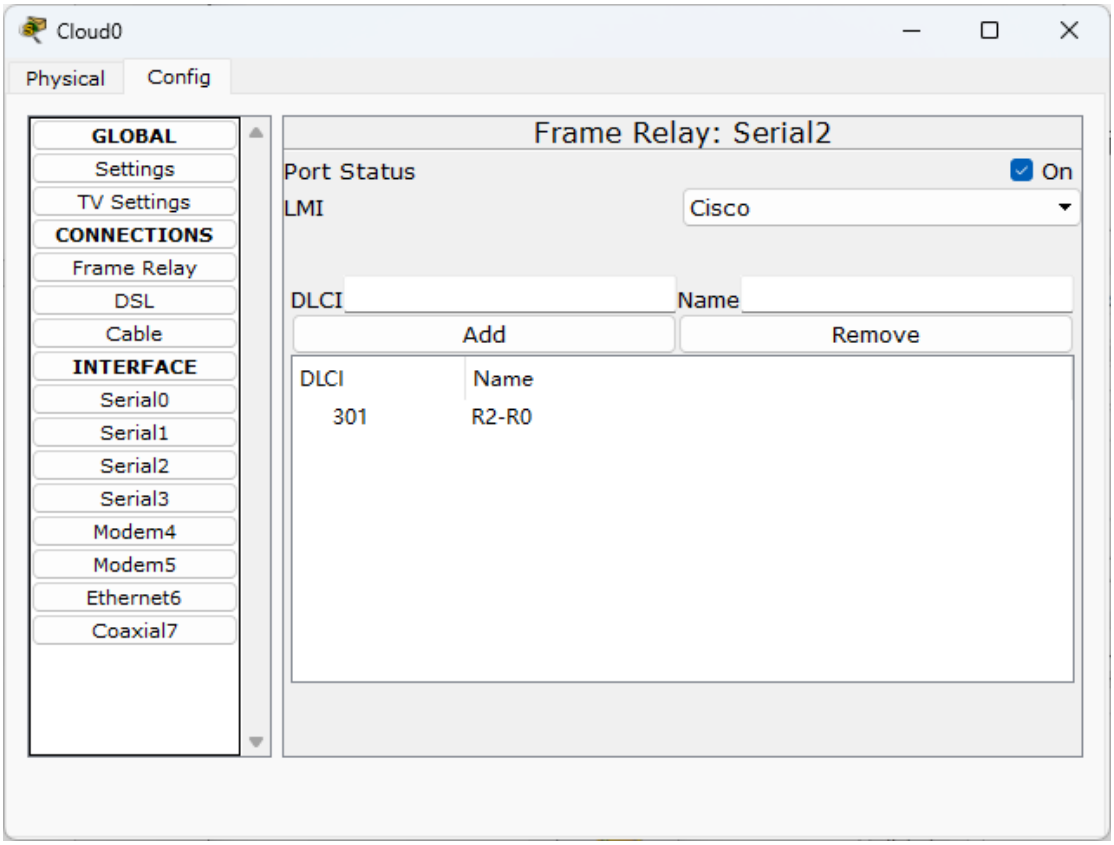

3. 启动 Cisco Packet Tracer，按照上述拓扑结构连接设备。

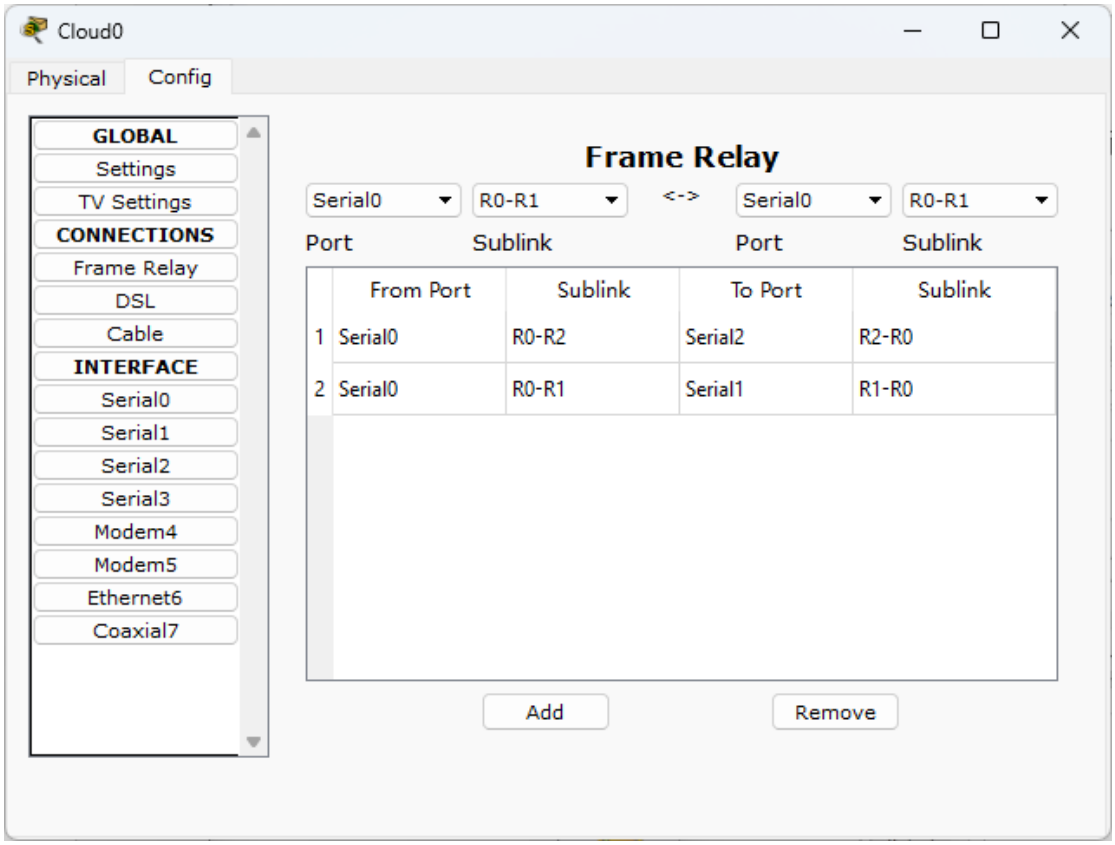



4. 进行帧中继交换机配置。




Cloud0
Physical
Config
GLOBAL
Settings
TV Settings
CONNECTIONS
Frame Relay
DSL
Cable
INTERFACE
Serial0
Serial1
Serial2
Serial3
Modem4
Modem5
Ethernet6
Coaxial7
Frame Relay: Serial1
Port Status
On
LMI
Cisco
DLCI
Name
Add
Remove
DLCI
Name
201
R1-R0


Cloud0
Physical
Config
GLOBAL
Settings
TV Settings
CONNECTIONS
Frame Relay
DSL
Cable
INTERFACE
Serial0
Serial1
Serial2
Serial3
Modem4
Modem5
Ethernet6
Coaxial7
Frame Relay: Serial2
Port Status
On
LMI
Cisco
DLCI
Name
Add
Remove
DLCI
Name
301
R2-R0




5. 在 Router0 的 CLI 中输入以下命令进行配置。

```
enable
configure terminal
interface Serial 0/0/0
no shutdown
encapsulation frame-relay
exit
interface Serial 0/0/0.102 point-to-point
ip address 1.1.1.1 255.255.255.252
frame-relay interface-dlci 102
exit
interface Serial 0/0/0.103 point-to-point
ip address 1.1.1.5 255.255.255.252
frame-relay interface-dlci 103
```

6. 在 Router1 的 CLI 中输入以下命令进行配置。

```
enable
configure terminal
interface Serial 0/0/0
```

```
no shutdown
encapsulation frame-relay
exit
interface Serial 0/0/0.201 point-to-point
ip address 1.1.1.2 255.255.255.252
frame-relay interface
frame-relay interface-dlci 201
```

7. 在 Router2 的 CLI 中输入以下命令进行配置。

```
enable
configure terminal
interface Serial 0/0/0
no shutdown
encapsulation frame-relay
exit
interface Serial 0/0/0.301 point-to-point
ip address 1.1.1.6 255.255.255.252
frame-relay interface-dlci 301
```

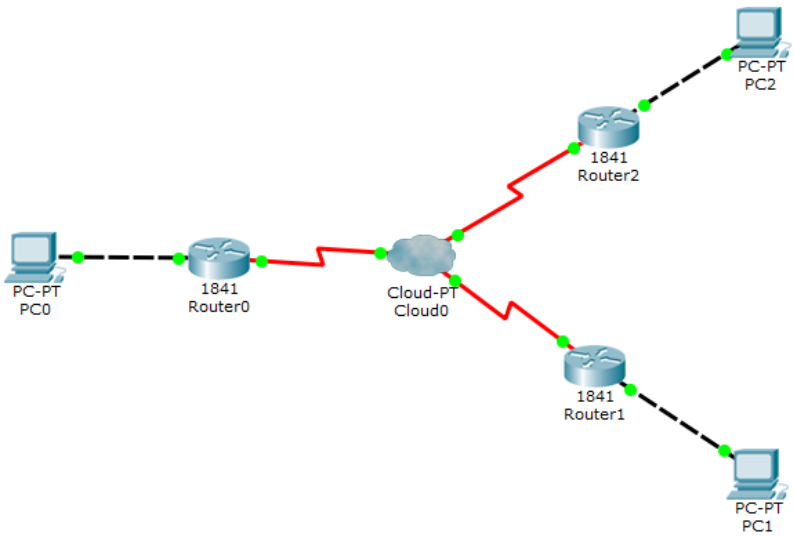
8. 为 Router1 和 Router2 配置静态路由之前检查接口间能否相互 ping 通。
9. 为 Router1 配置静态路由。

```
ip route 1.1.1.4 255.255.255.252 1.1.1.1
```

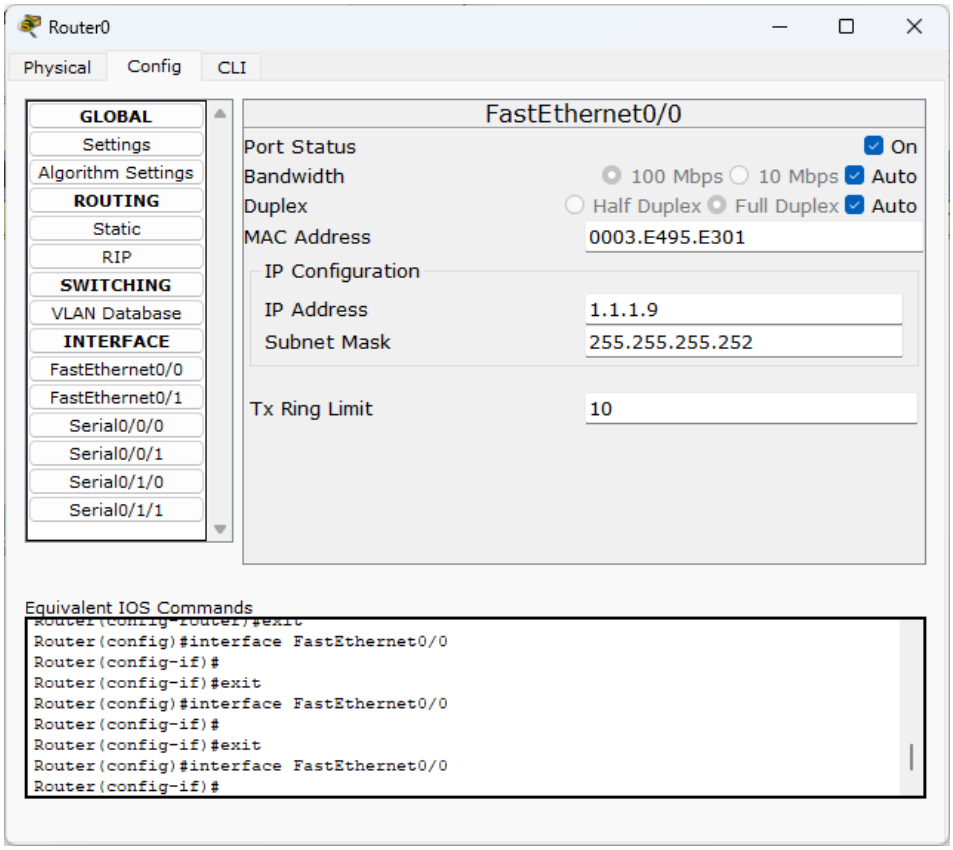
10. 为 Router2 配置静态路由。

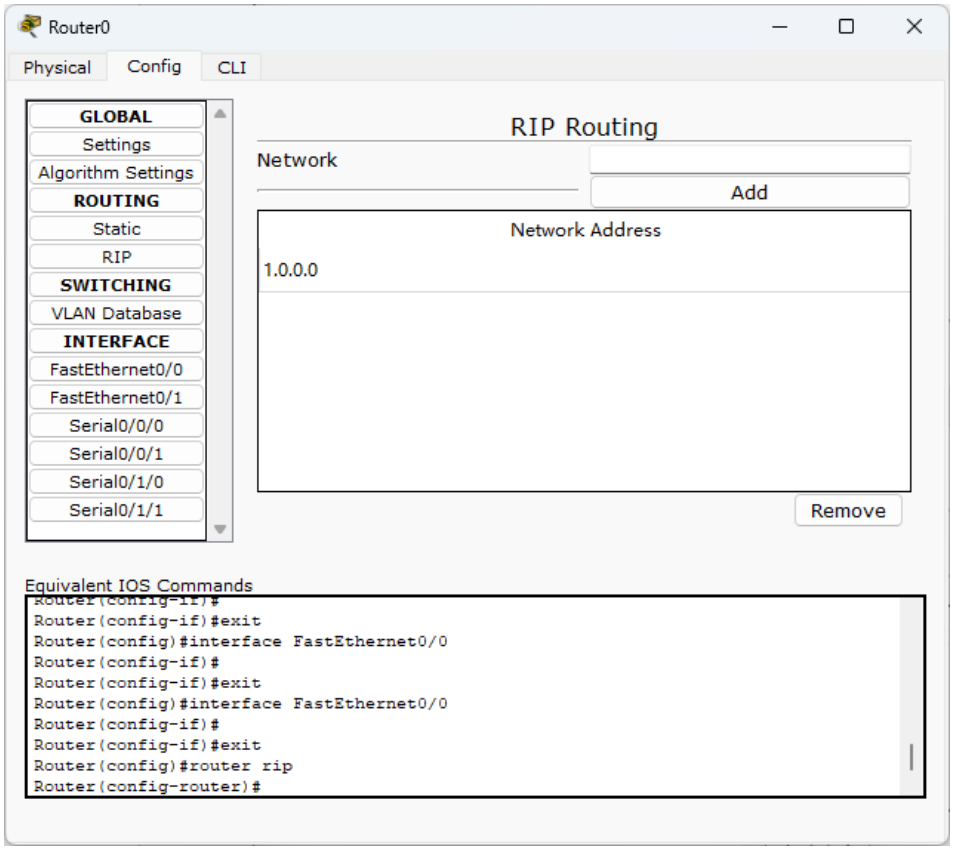
```
ip route 1.1.1.0 255.255.255.252 1.1.1.5
```

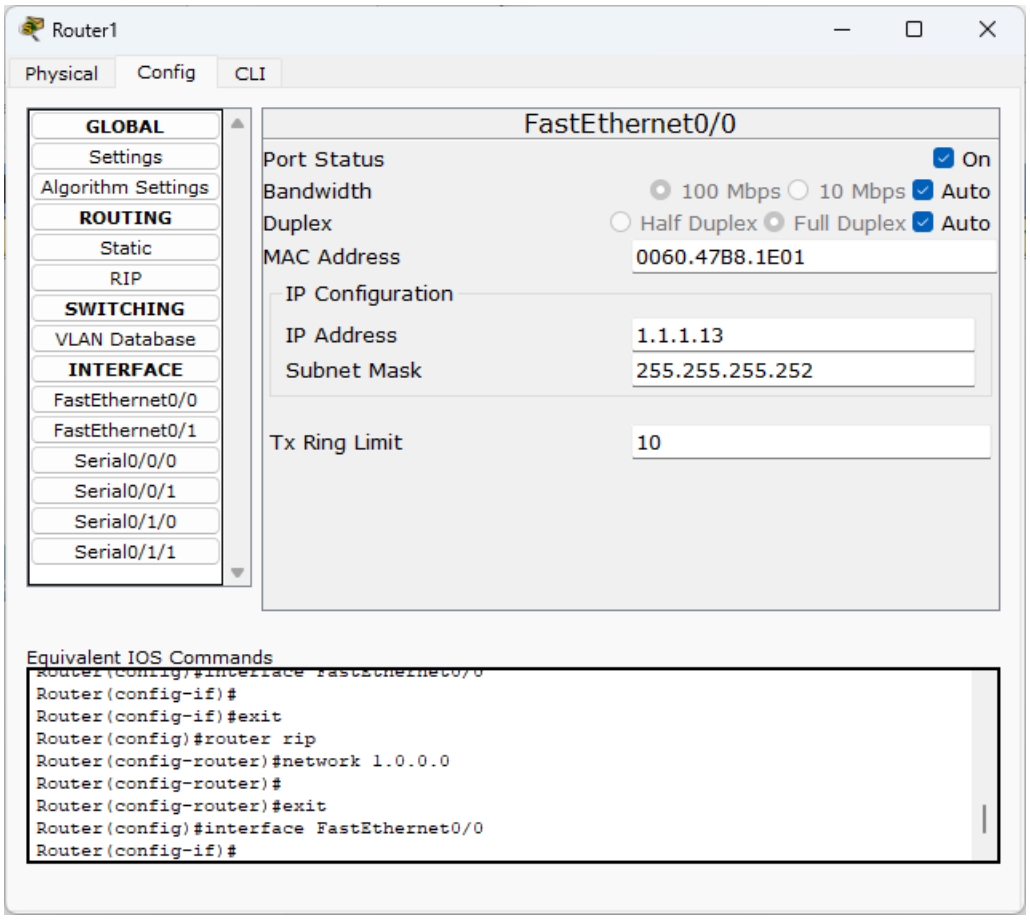
11. 为 Router1 和 Router2 配置静态路由之后检查接口间能否相互 ping 通。
12. 将三台 PC 机 PC1、PC2 和 PC3 分别连接至 Router0、Router1 和 Router2。

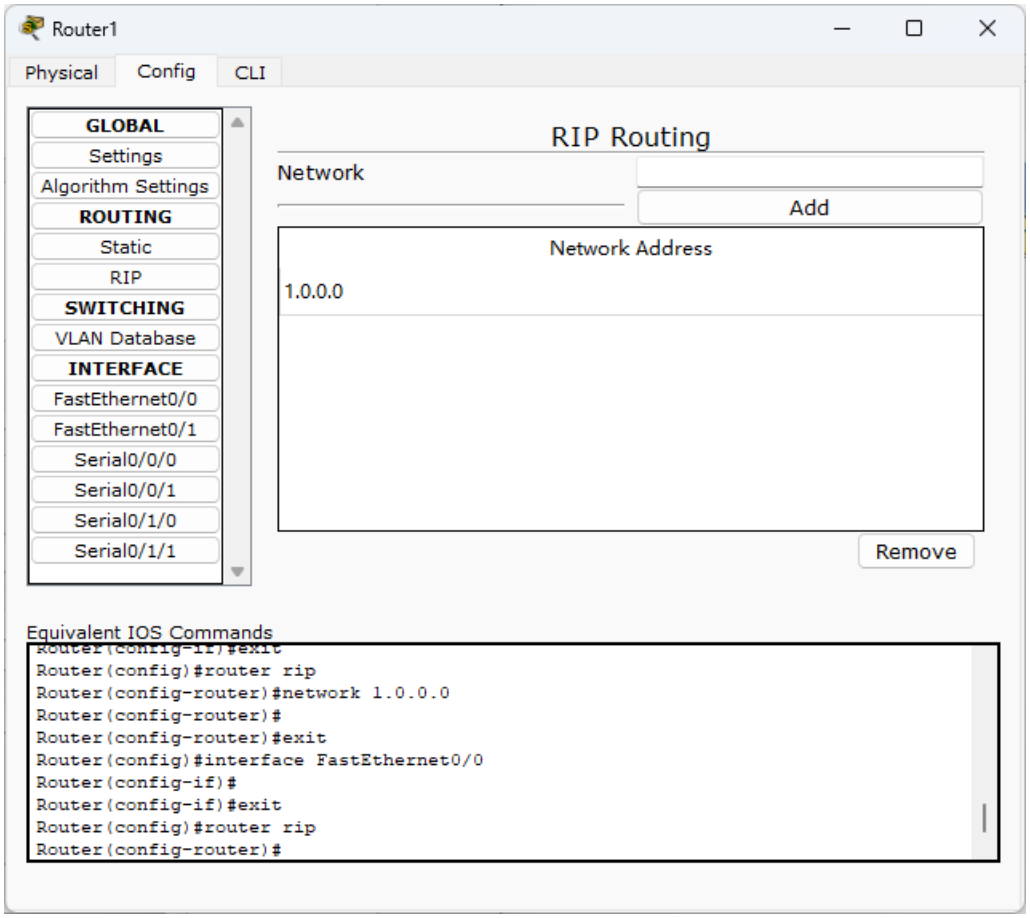


13. 分别配置 Router0、Router1 和 Router2 的 FastEthernet0/0 的 IP 地址和子网掩码，并在 RIP 路由协议中添加 1.0.0.0。




Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.47B8.1E01
IP Configuration
IP Address
1.1.1.13
Subnet Mask
255.255.255.252
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 1.0.0.0
Router(config-router)#
Router(config-router)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#


Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
1.0.0.0
Remove
Equivalent IOS Commands
Router(config)#router rip
Router(config-router)#network 1.0.0.0
Router(config-router)#
Router(config-router)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#

Router2

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/0

Port Status: On
Bandwidth: 100 Mbps, 10 Mbps, Auto
Duplex: Half Duplex, Full Duplex, Auto
MAC Address: 0001.C702.0501

IP Configuration
IP Address: 1.1.1.17
Subnet Mask: 255.255.255.252

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router(config-if)#ip address 1.1.1.17 255.255.255.252
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 1.0.0.0
Router(config-router)#
Router(config-router)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

Router2

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

RIP Routing

Network
Add

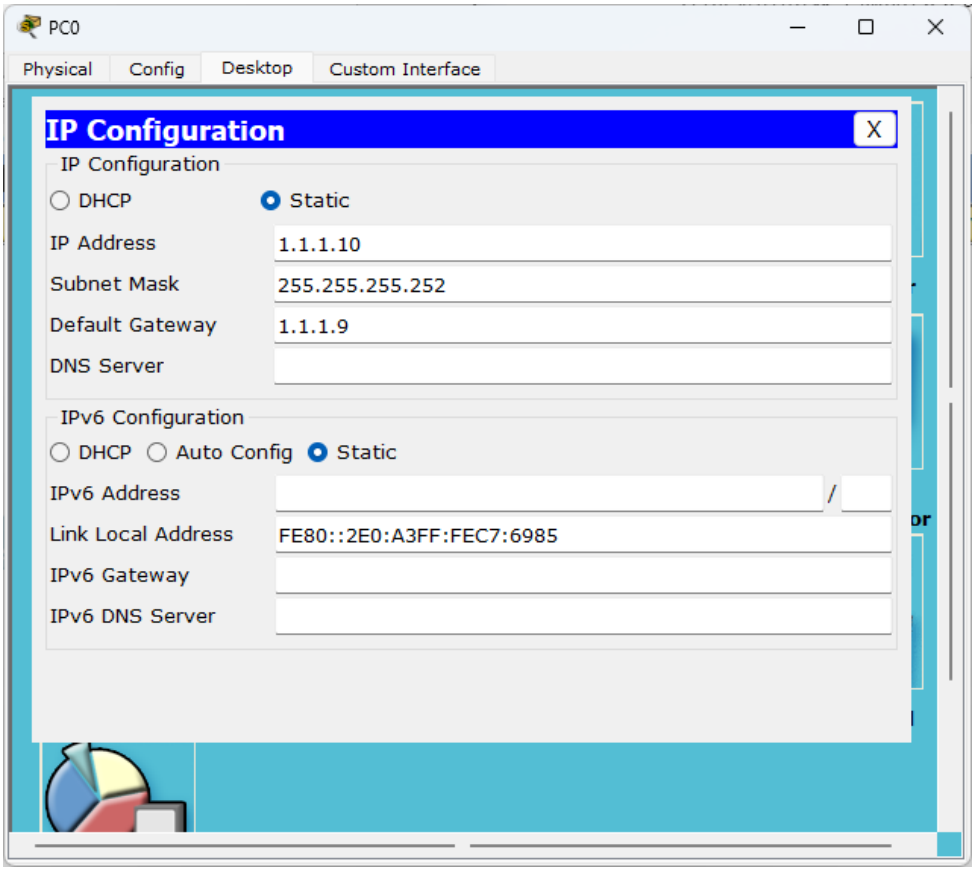
Network Address
1.0.0.0

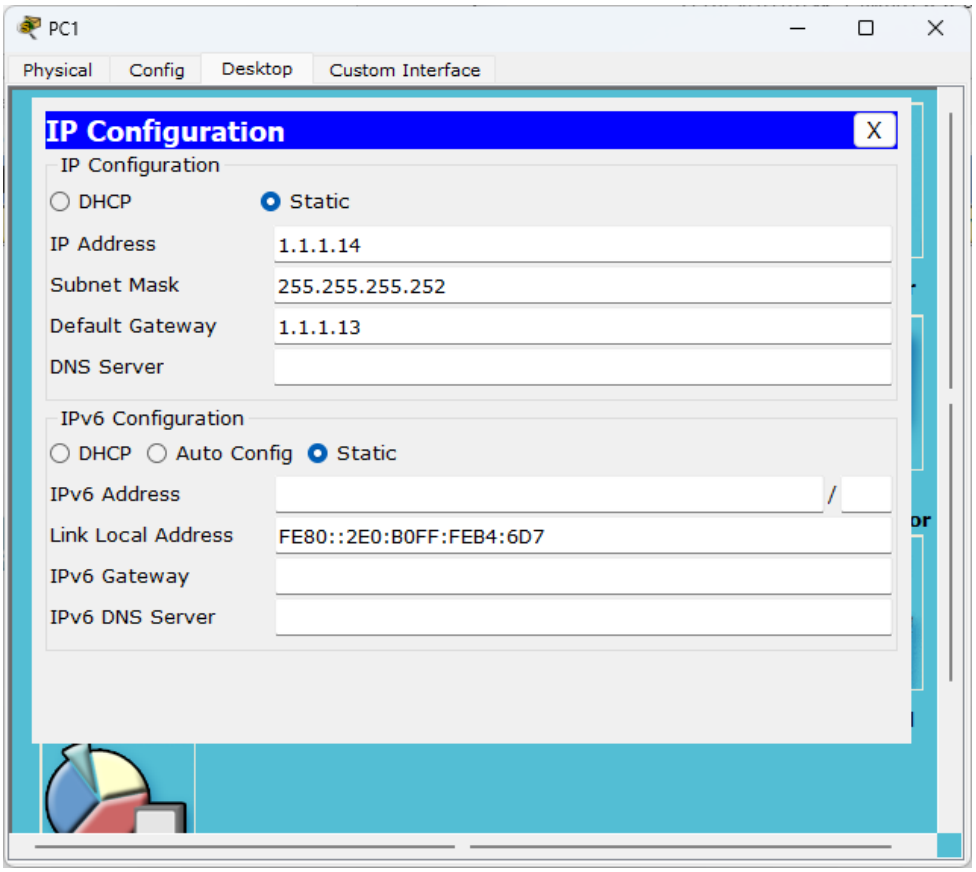
Remove

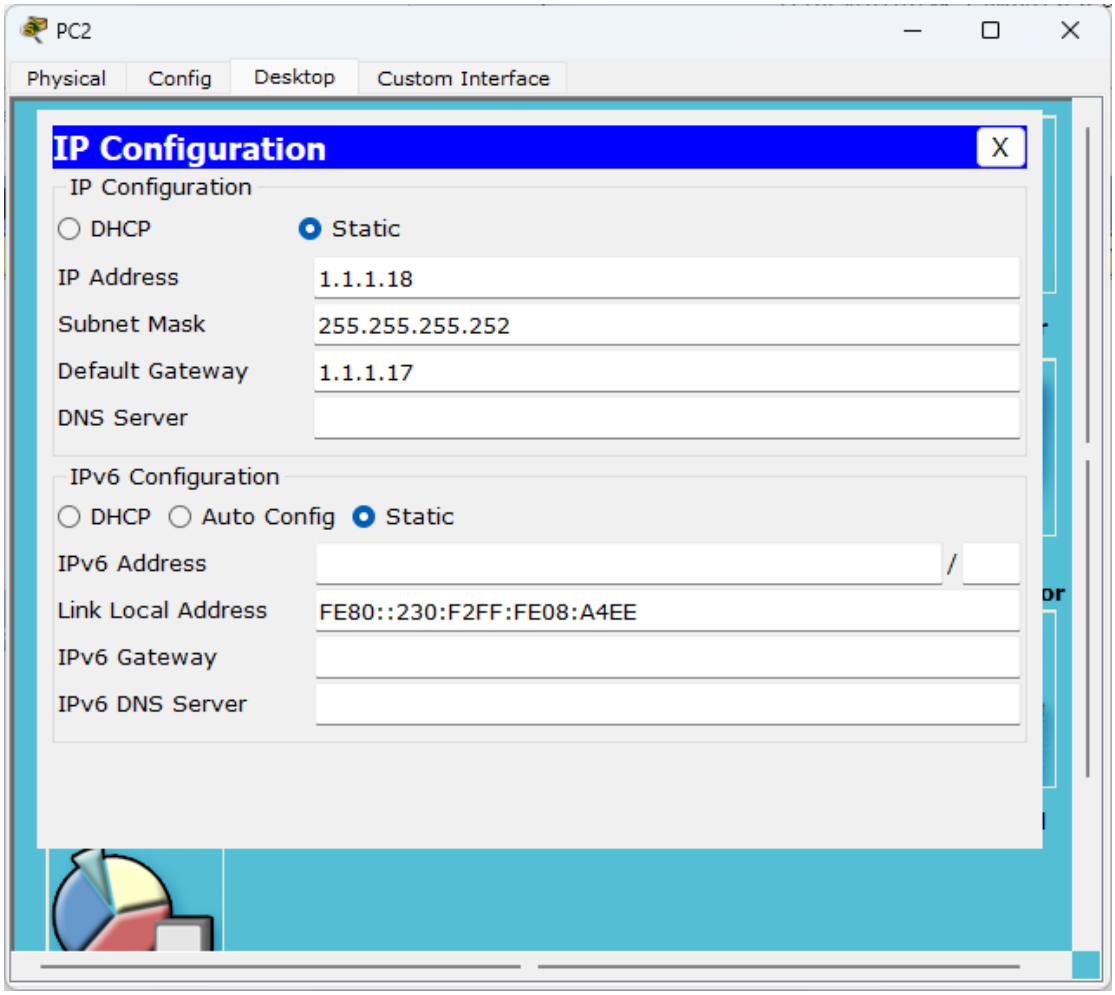
Equivalent IOS Commands

```
Router(config)#router rip
Router(config-router)#network 1.0.0.0
Router(config-router)#
Router(config-router)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#router rip
Router(config-router)#
```

14. 配置 PC0、PC1 和 PC2 的网关、IP 地址和子网掩码。



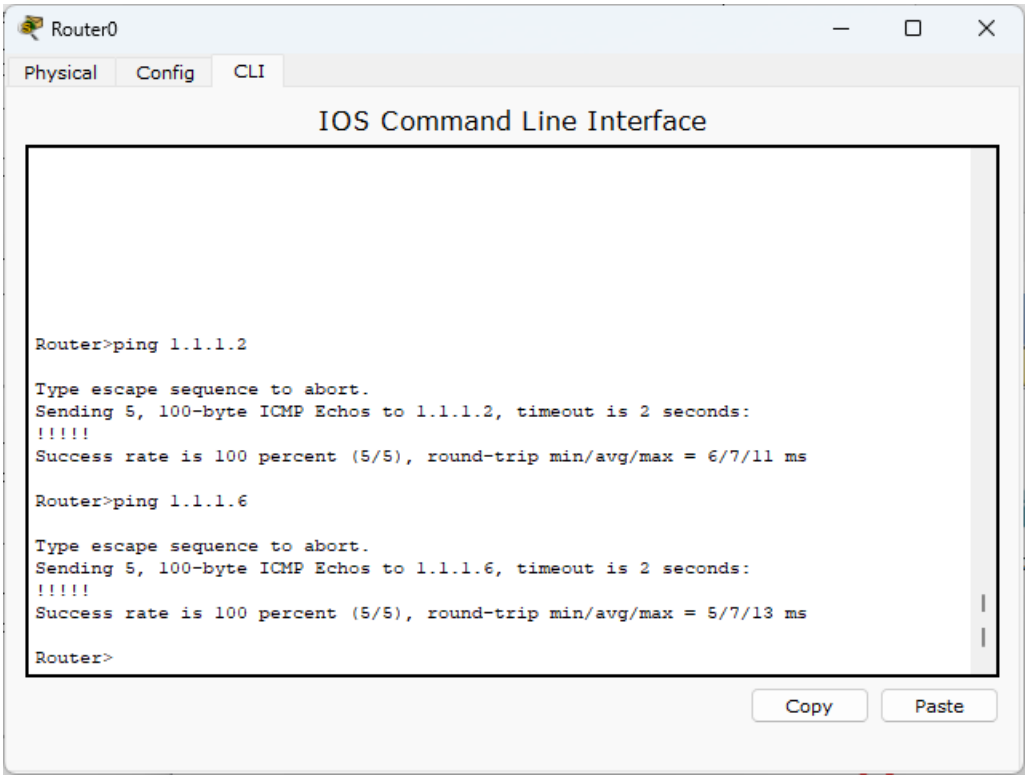


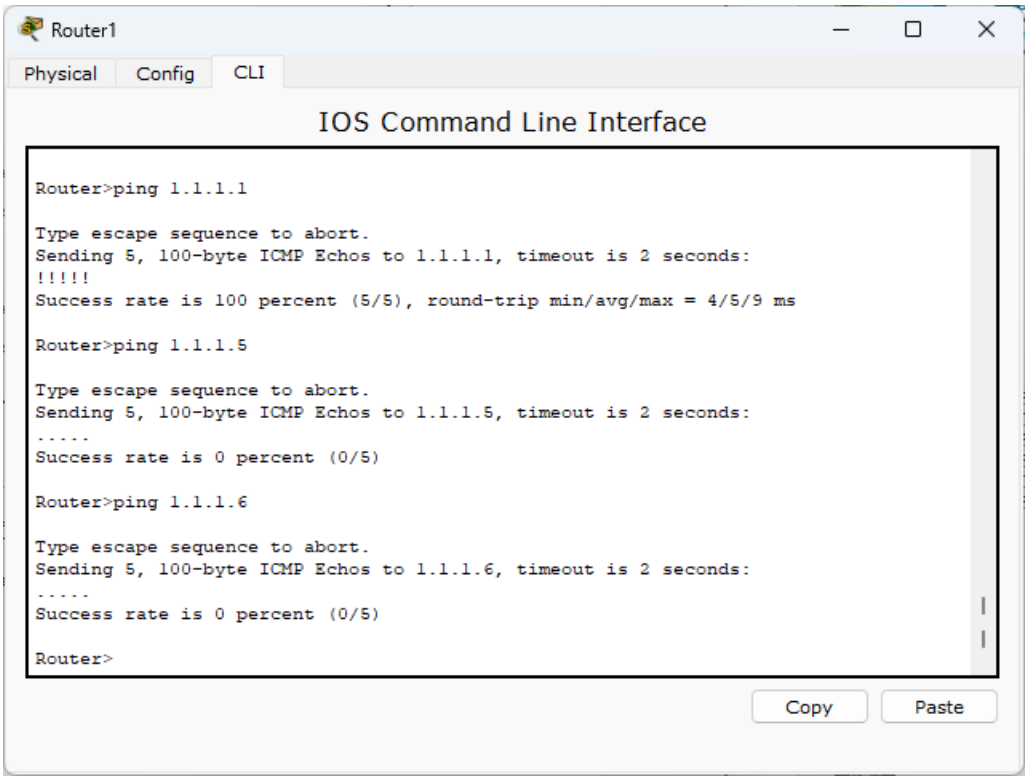

15. PC0、PC1 和 PC2 之间相互进行 ping 测试，观察实验结果。

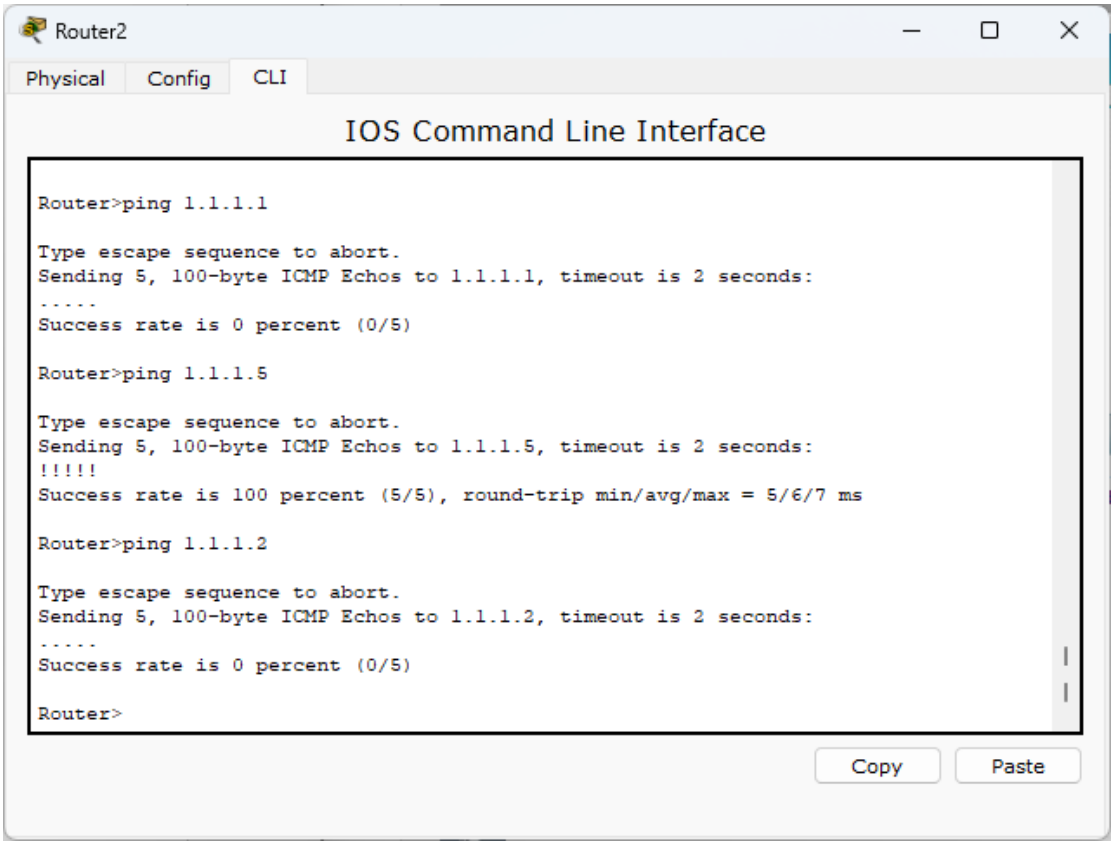
- PC0：
  - 网关：1.1.1.9
  - IP 地址：1.1.1.10
  - 子网掩码：255.255.255.252
- PC1：
  - 网关：1.1.1.13
  - IP 地址：1.1.1.14
  - 子网掩码：255.255.255.252
- PC2：
  - 网关：1.1.1.17
  - IP 地址：1.1.1.18
  - 子网掩码：255.255.255.252

【实验现象】

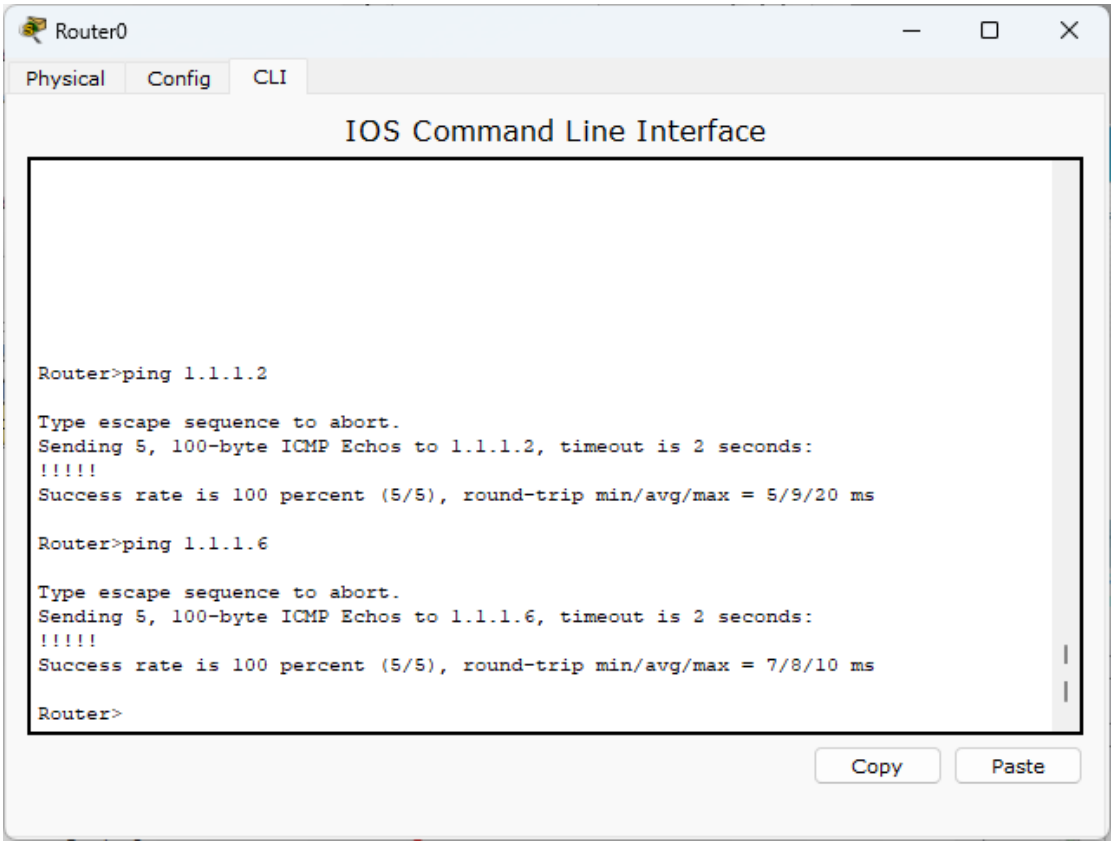
1. 为 Router1 和 Router2 配置静态路由之前检查接口间能否相互 ping 通。实验结果显示 Router0 分别与 Router1 和 Router2 之间能够相互 ping 通，但是 Router1 与 Router2 之间不能够 ping 通。

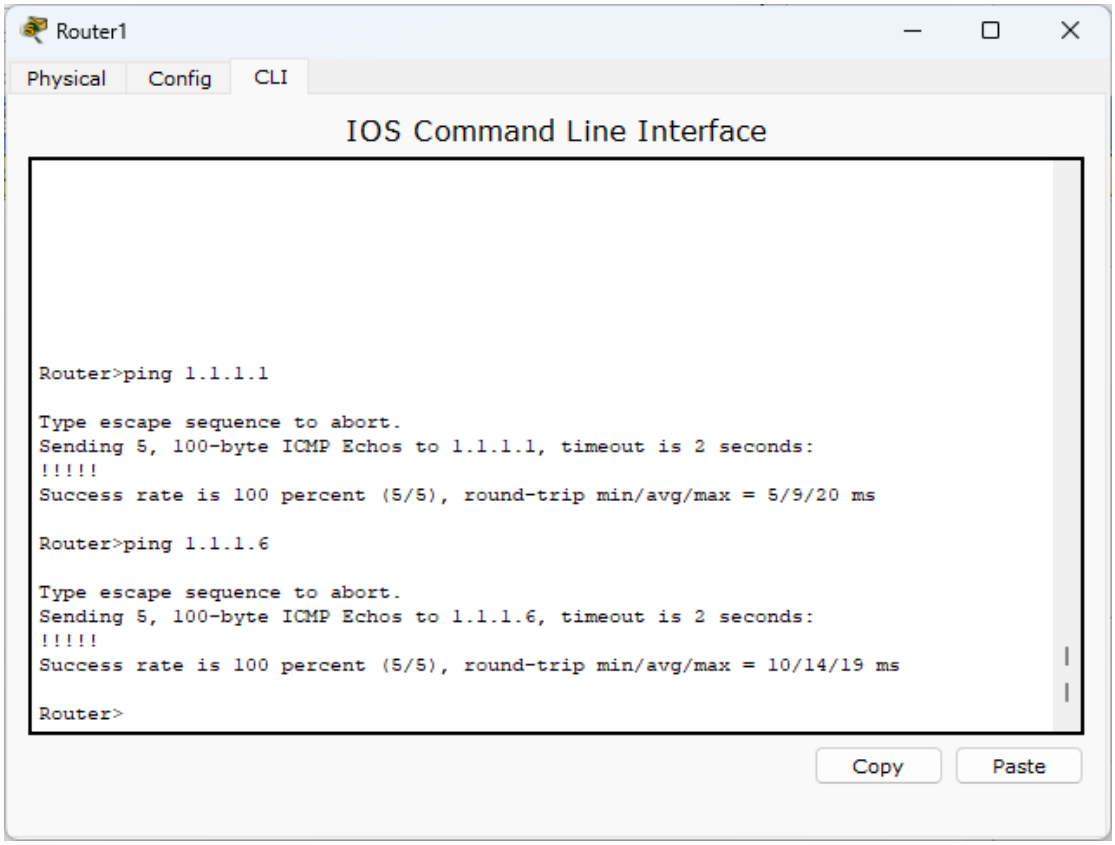


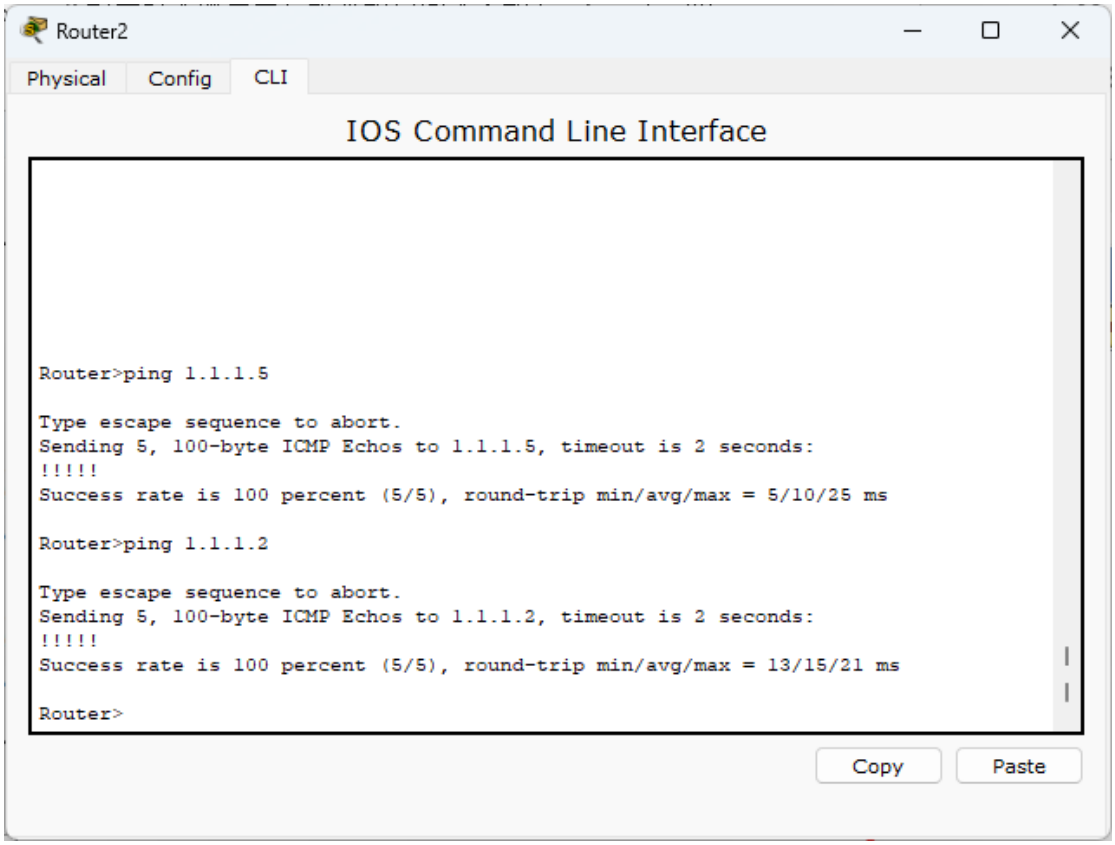






2. 为 Router1 和 Router2 配置静态路由之后检查接口间能否相互 ping 通。实验结果显示 Router0、Router1 和 Router2 之间能够相互 ping 通。






3. PC0、PC1 和 PC2 之间相互进行 ping 测试，均成功。

PC0

Physical | Config | Desktop | Custom Interface

Command Prompt

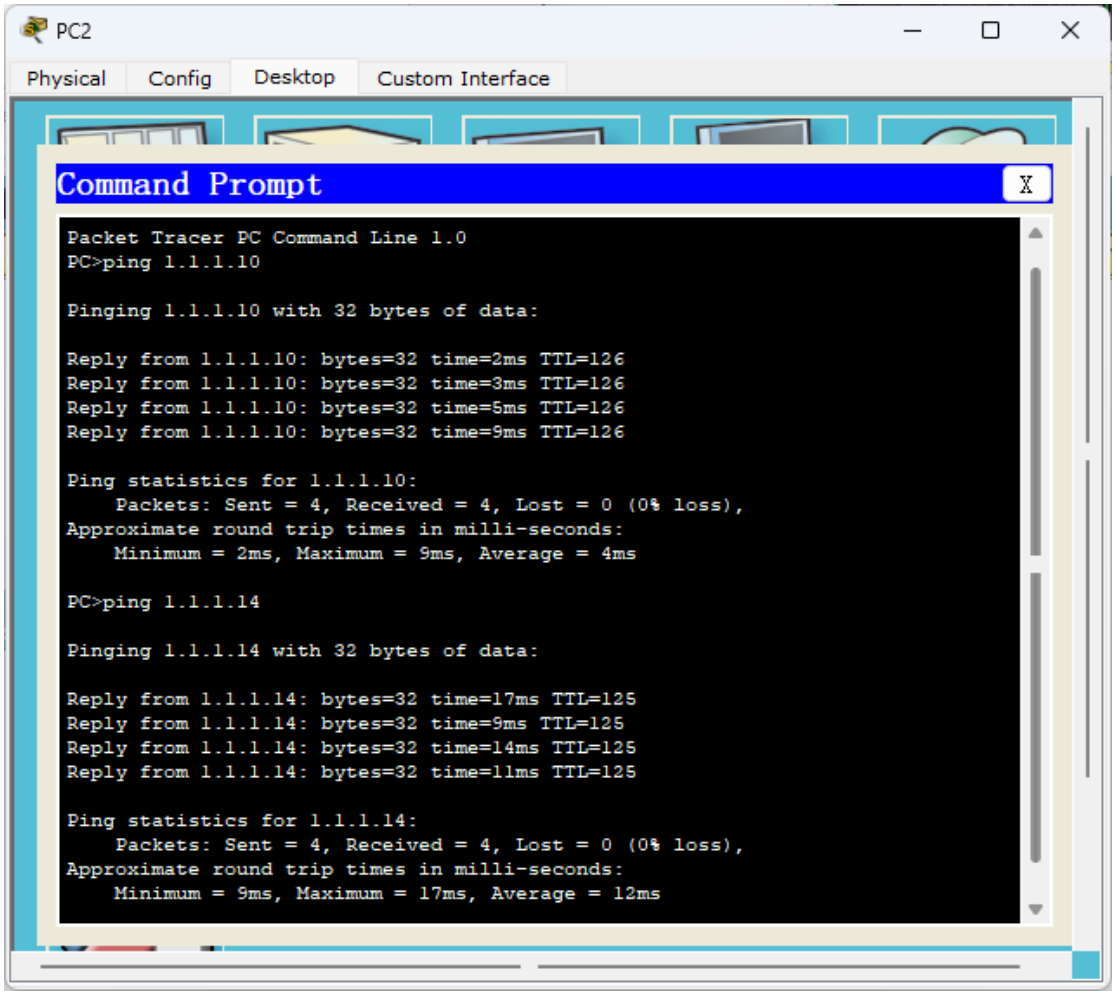
```
PC>ping 1.1.1.14

Pinging 1.1.1.14 with 32 bytes of data:

Reply from 1.1.1.14: bytes=32 time=9ms TTL=126
Reply from 1.1.1.14: bytes=32 time=9ms TTL=126
Reply from 1.1.1.14: bytes=32 time=6ms TTL=126
Reply from 1.1.1.14: bytes=32 time=8ms TTL=126

Ping statistics for 1.1.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 8ms

PC>ping 1.1.1.18

Pinging 1.1.1.18 with 32 bytes of data:

Reply from 1.1.1.18: bytes=32 time=8ms TTL=126
Reply from 1.1.1.18: bytes=32 time=7ms TTL=126
Reply from 1.1.1.18: bytes=32 time=6ms TTL=126
Reply from 1.1.1.18: bytes=32 time=9ms TTL=126

Ping statistics for 1.1.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 7ms
```

PC1

Physical | Config | Desktop | Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 1.1.1.10

Pinging 1.1.1.10 with 32 bytes of data:

Reply from 1.1.1.10: bytes=32 time=10ms TTL=126
Reply from 1.1.1.10: bytes=32 time=12ms TTL=126
Reply from 1.1.1.10: bytes=32 time=7ms TTL=126
Reply from 1.1.1.10: bytes=32 time=4ms TTL=126

Ping statistics for 1.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 12ms, Average = 8ms

PC>ping 1.1.1.18

Pinging 1.1.1.18 with 32 bytes of data:

Reply from 1.1.1.18: bytes=32 time=12ms TTL=125
Reply from 1.1.1.18: bytes=32 time=13ms TTL=125
Reply from 1.1.1.18: bytes=32 time=12ms TTL=125
Reply from 1.1.1.18: bytes=32 time=13ms TTL=125

Ping statistics for 1.1.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 13ms, Average = 12ms
```




**【分析讨论】**

**一、路由器间的通信连通性**

在配置静态路由之前，虽然 Router0 能够与 Router1 和 Router2 分别进行 ping 通，但 Router1 与 Router2 之间无法直接通信。这一现象指出，单独的帧中继配置无法解决跨不同网络的路由问题，必须通过适当的路由配置来确保端到端的通信连通性。静态路由的添加后，所有路由器之间的通信均恢复正常，验证了静态路由在指导数据包正确传输路径中的关键作用。

**二、帧中继的多路复用功能**

实验中，通过一个物理接口实现多个虚拟连接的配置展示了帧中继的多路复用能力。这种配置允许单个物理链路上运行多个虚拟电路，从而提高了网络资源的利用效率，并减少了所需的物理接口数量，显著降低了设备和管理成本。

**三、动态与静态地址映射的应用**

通过实践帧中继的地址解析协议（ARP）和反向 ARP，实验不仅强化了理论知

识，也展示了动态和静态地址映射在实际网络配置中的应用。动态地址映射允许设备在无需手动介入的情况下学习和更新网络地址，这对于大型动态网络环境尤为重要。

**四、PC 终端的网络连接测试**

连接 PC 机至各路由器并进行 ping 测试的步骤展示了端到端配置的正确性。所有 PC 机之间的成功通信表明了网络接口、IP 配置及路由配置的正确无误。此外，使用 RIP 动态路由协议进行的配置测试，验证了在更广泛的网络环境中，如何利用动态路由协议自动管理和更新路由信息。

# 实验 16：ACL 访问控制实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/18 |

**【实验目的】**

本实验旨在通过配置和应用接入控制列表（ACL）加深学生对网络安全和数据包过滤的理解。通过规划网络拓扑、设置设备 IP 和应用 ACL 规则，学生将实践如何控制网络流量，包括允许或拒绝特定的网络访问，以此提高对网络可管理性和安全性的认知和操作技能。

**【实验原理】**

**接入控制列表技术原理**

接入控制列表（Access Control Lists，简称 ACLs）是网络设备用于增强网络可管理性和安全性的关键技术。它们作为数据包过滤系统，根据定义的规则，控制数据报文在网络设备接口上的通过或阻断。这些规则可以是非常简单的，如基于源 IP 地址的标准 IP 访问列表，也可以是更复杂的，如扩展 IP 访问列表，后者不仅包括源 IP 地址，还包括目的 IP 地址、源端口号、目的端口号和使用的协议类型。

在 ACLs 的应用中，规则可以被设置为入栈应用或出栈应用，这意味着它们可以控制进入或离开接口的数据包。通过这种方式，ACLs 充当网络的“防火墙”，不仅可以防止未授权访问，还可以有效地管理和控制网络流量，保证网络的整体安全性和效率。

接入控制列表（ACLs）在网络安全架构中的运用不仅限于阻断非授权访问，它们还承担着网络监控和数据流量分析的重要角色。例如，通过记录接口上被拒绝或允许的数据包，ACLs 可以为网络管理员提供关键的安全日志信息，帮助识别潜在的安全威胁或不正常的流量模式。此外，ACLs 可以配置为时间基础的规则，允许在特定时间段内应用特定的访问控制策略，这种灵活性使得网络策略可以更加精确地匹配企业的运营需求。

在实际部署中，ACLs 的管理和维护要求网络管理员具备高度的精确度和前瞻性。错误配置的 ACLs 可能导致服务中断或数据泄露。因此，设计和实施 ACL 策略时，需要仔细规划并进行充分的测试，以确保它们不仅有效地执行预定的安

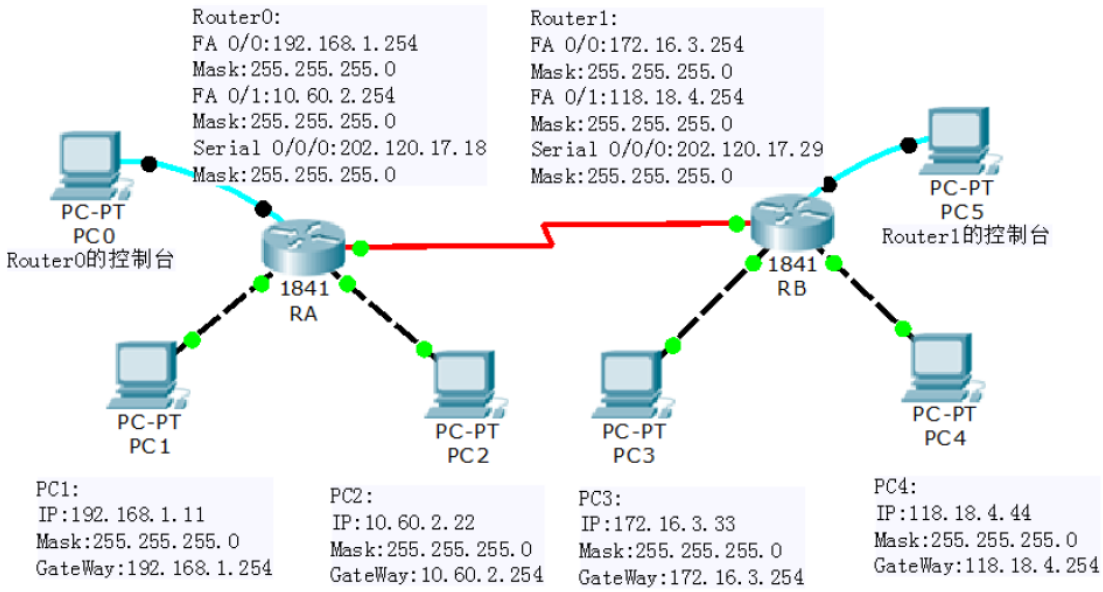
全策略，还要保持网络的最优性能。

**【实验设备】**

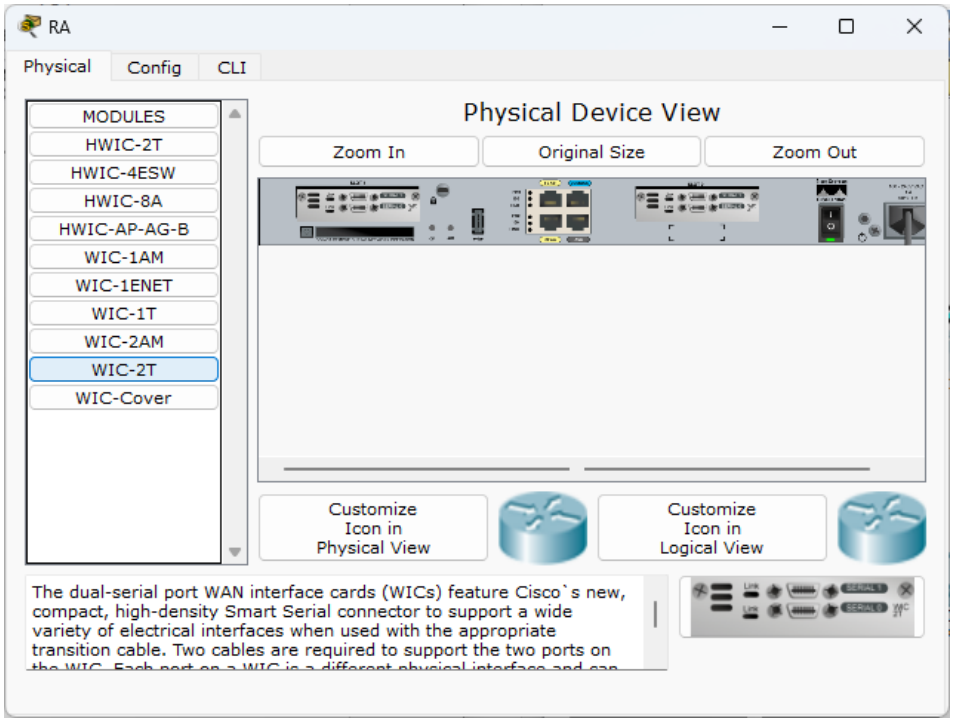
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

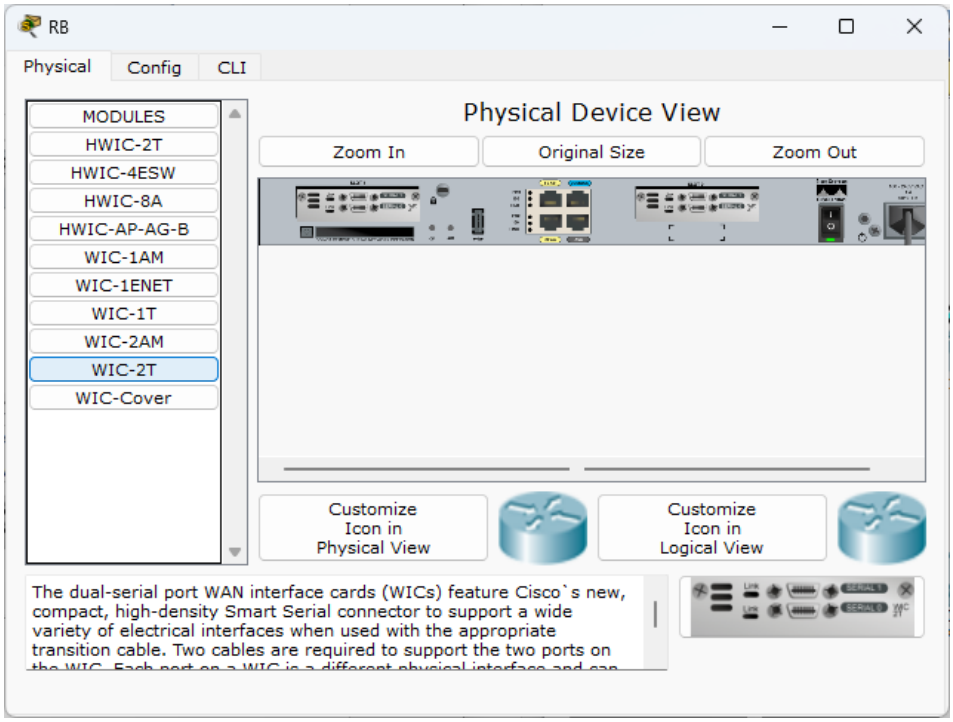
**【实验步骤】**

1. 规划网络地址及拓扑图。

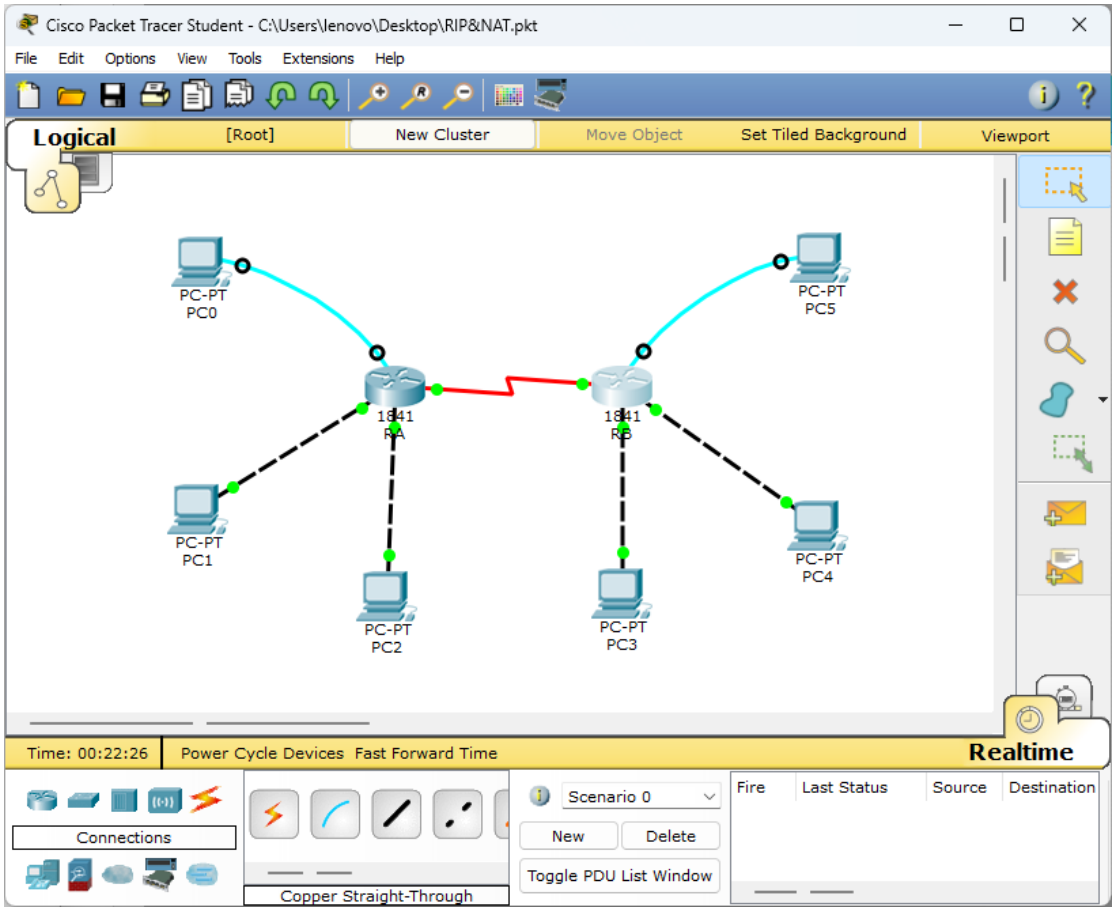



2. 在路由器 A 和路由器 B 中分别安装 WIC-2T，并重启设备。

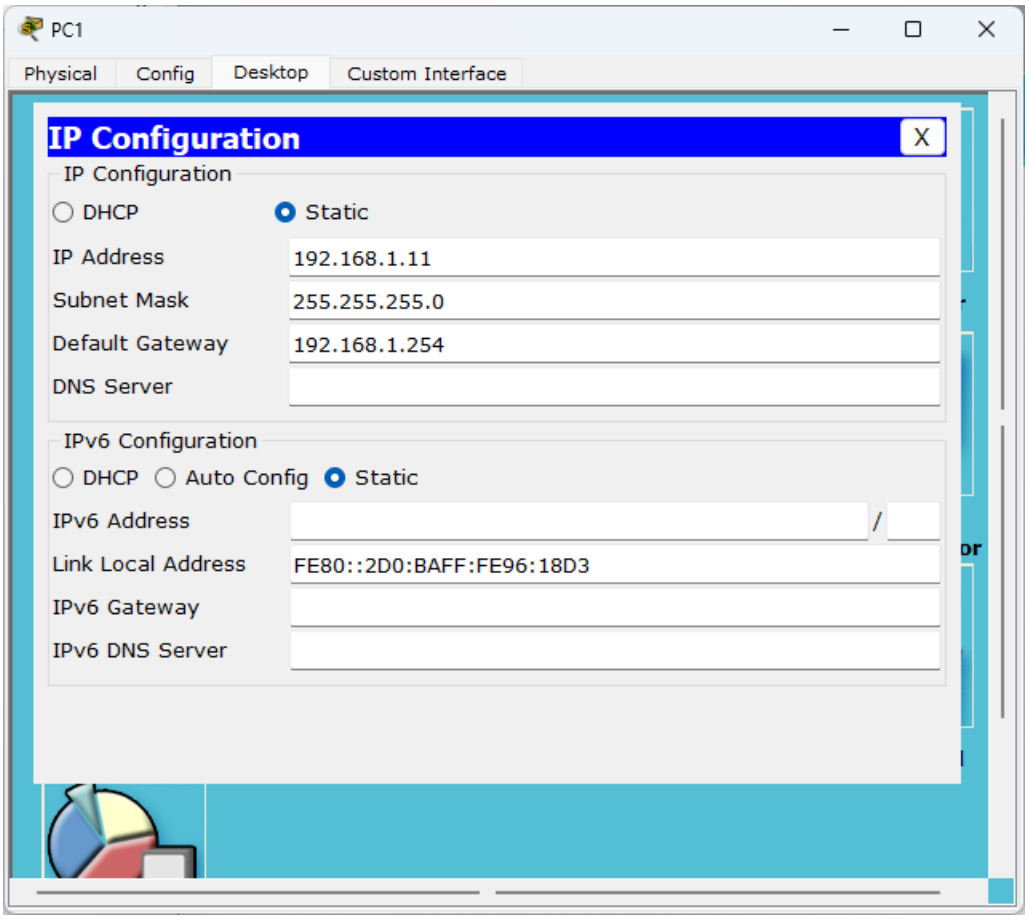


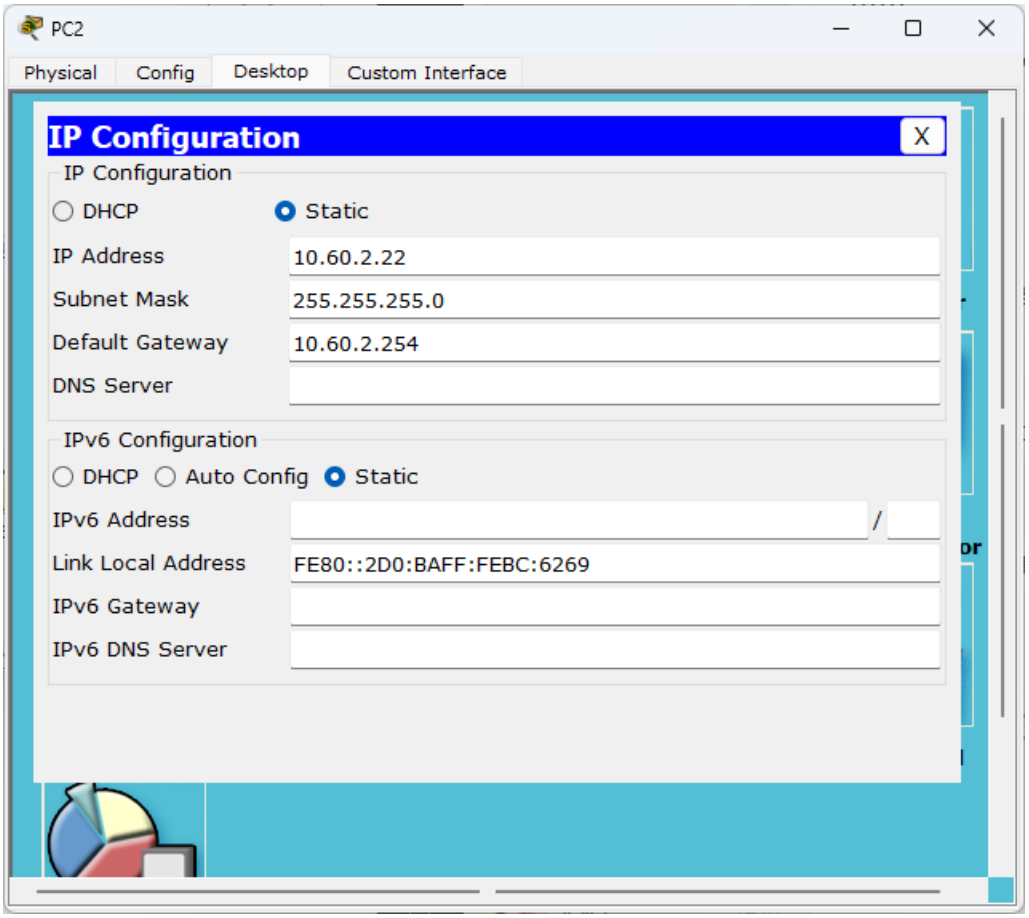


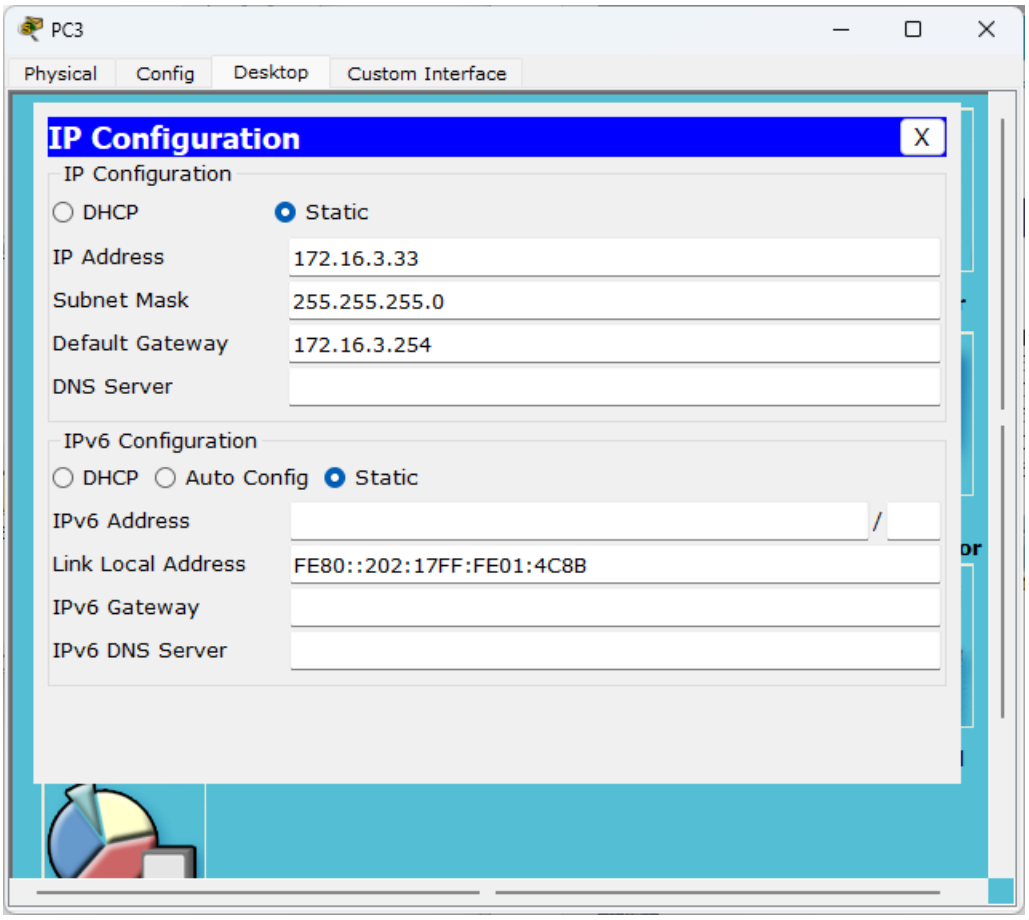

3. 启动 Cisco Packet Tracer，按照上述拓扑结构连接设备。

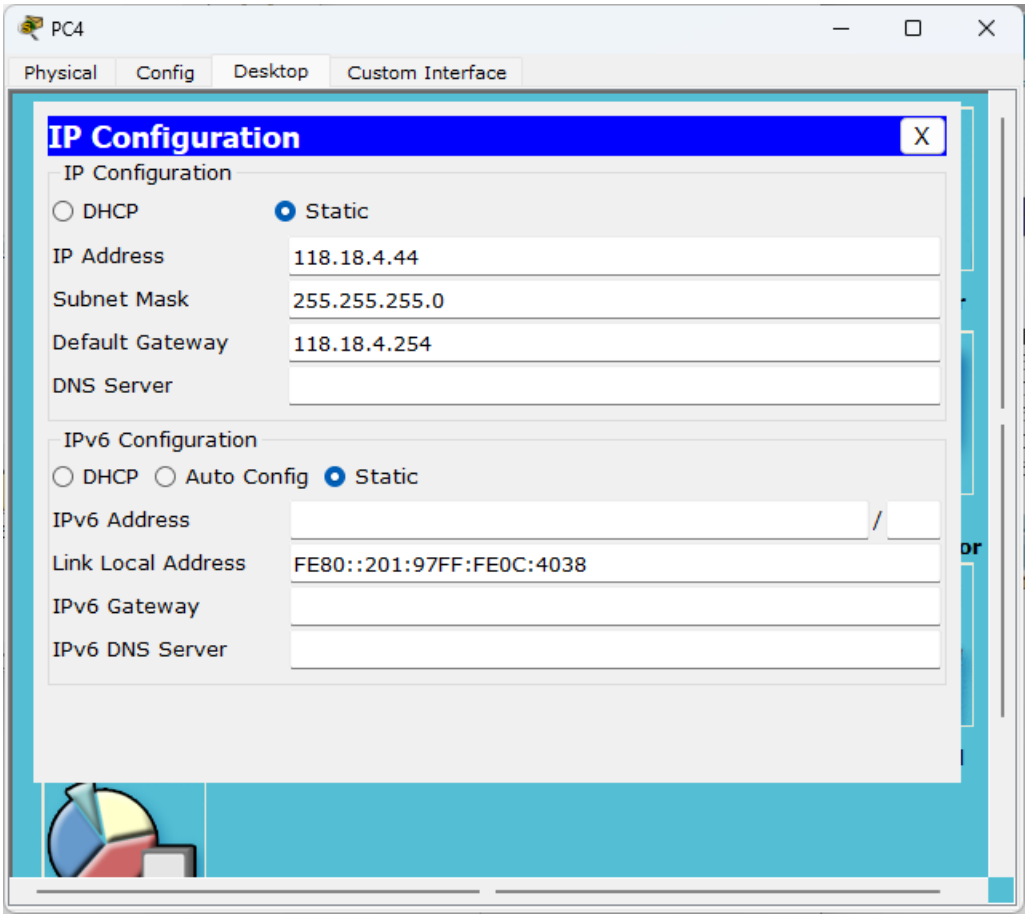



4. 配置 PC 机的 IP 地址、子网掩码和网关。


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE96:18D3
IPv6 Gateway
IPv6 DNS Server


PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.60.2.22
Subnet Mask
255.255.255.0
Default Gateway
10.60.2.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FEBC:6269
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
172.16.3.33
Subnet Mask
255.255.255.0
Default Gateway
172.16.3.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:17FF:FE01:4C8B
IPv6 Gateway
IPv6 DNS Server


PC4
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
118.18.4.44
Subnet Mask
255.255.255.0
Default Gateway
118.18.4.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE0C:4038
IPv6 Gateway
IPv6 DNS Server

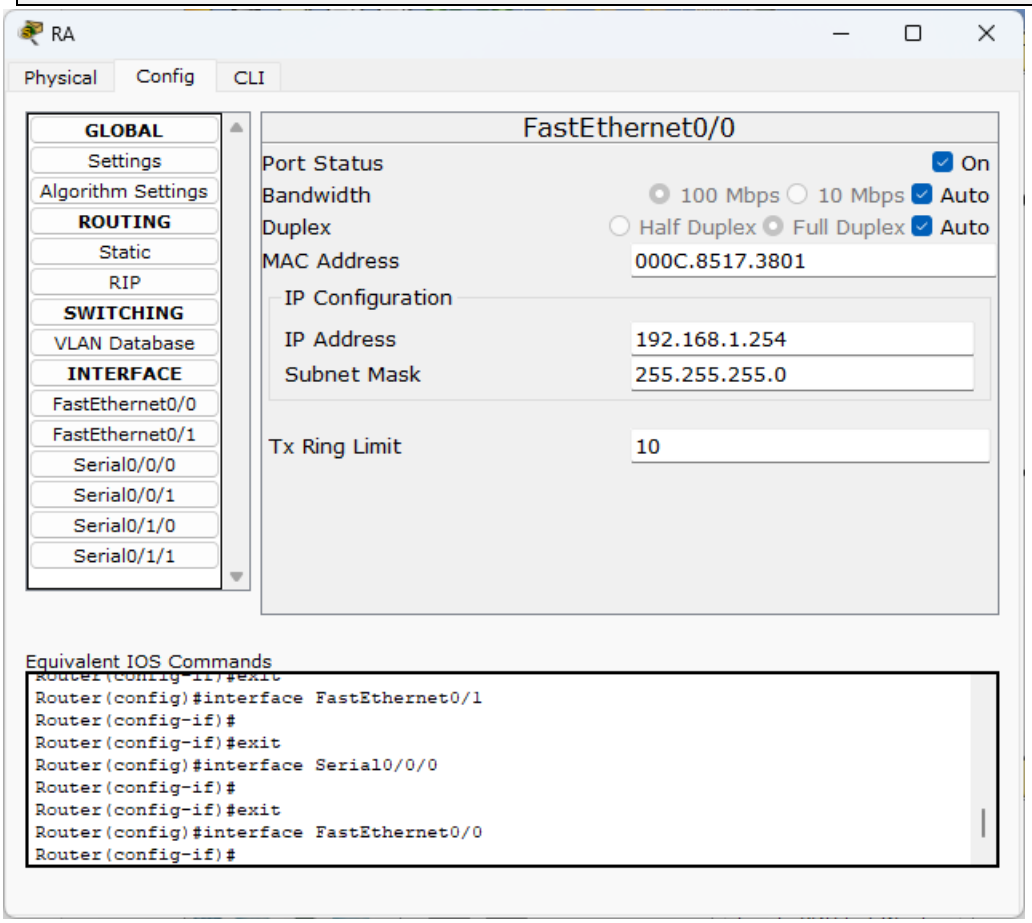
5. 配置路由器的端口地址和串口端口地址。

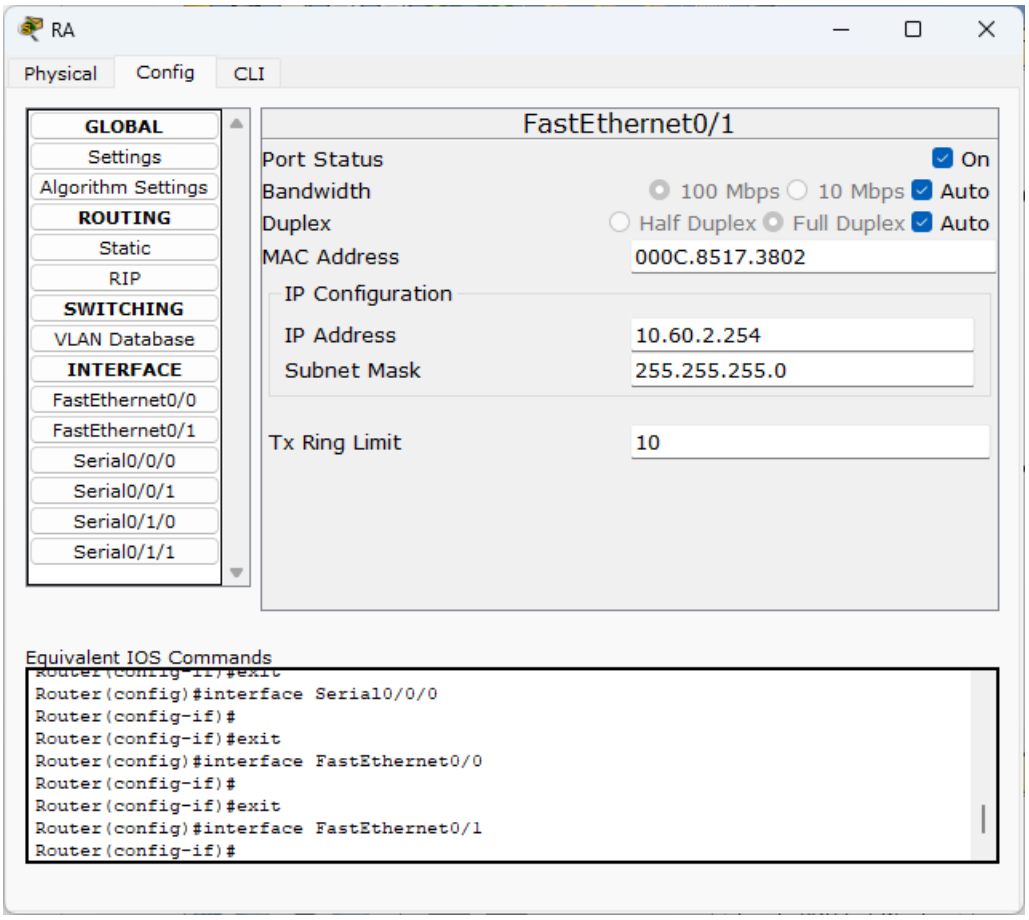
- 在路由器 A 的 CLI 中输入以下命令：

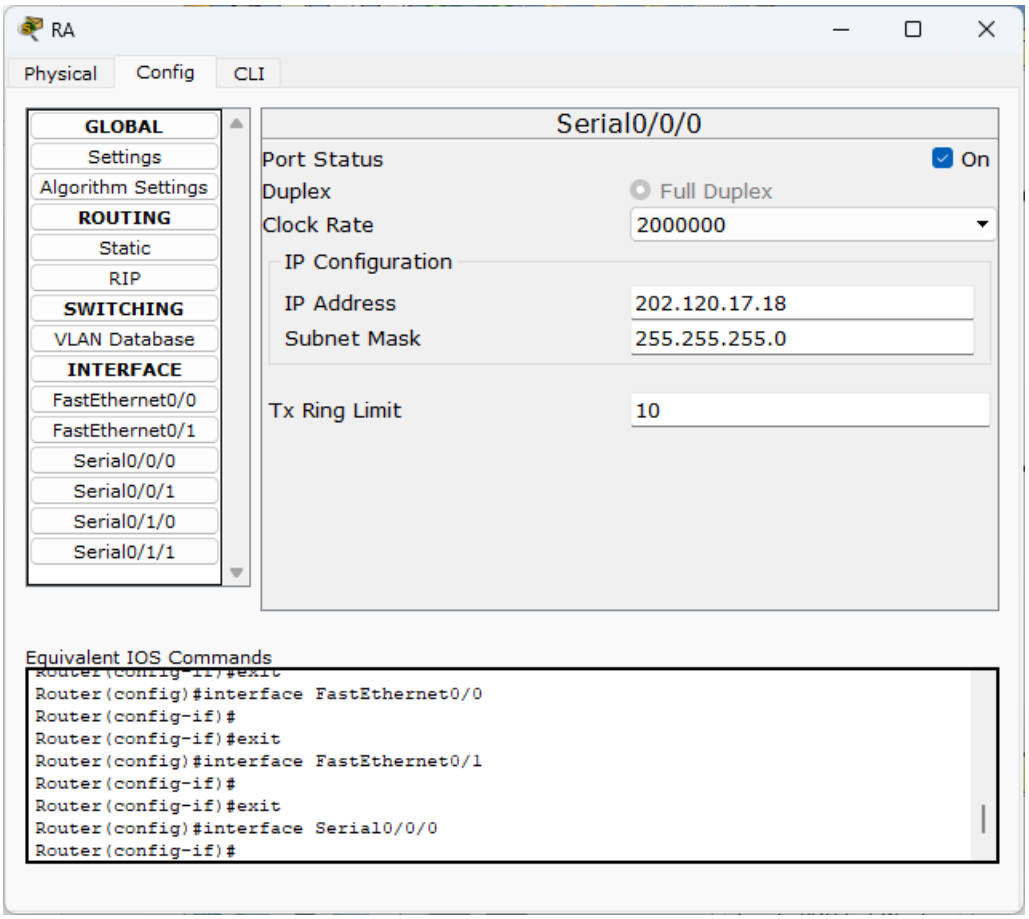
```
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.18 255.255.255.0
Clock rate 56000
```

- 在路由器 B 的 CLI 中输入以下命令：

```
interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.29 255.255.255.0
Clock rate 56000
```




RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8517.3802
IP Configuration
IP Address
10.60.2.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#


RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
202.120.17.18
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#

RB

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/0

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8101 |
| IP Configuration | |
| IP Address | 172.16.3.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

RB

Physical | Config | CLI

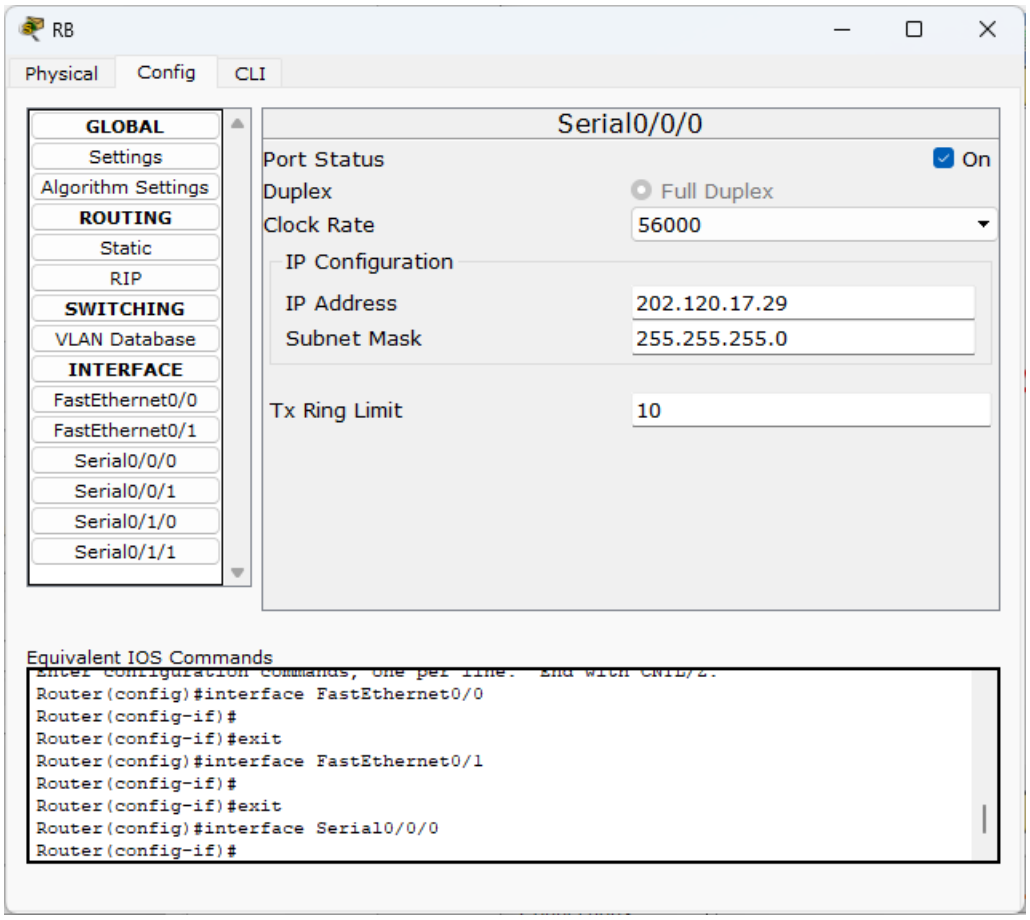
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/1

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8102 |
| IP Configuration | |
| IP Address | 118.18.4.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
```




6. 为 RA 配置静态路由。

```
ip route 172.16.3.0 255.255.255.0 Serial0/1/0
ip route 118.18.4.0 255.255.255.0 Serial0/1/0
```

7. 为 RouterB 配置静态路由。

```
ip route 192.168.1.0 255.255.255.0 Serial0/1/0
ip route 10.60.2.0 255.255.255.0 Serial0/1/0
```

8. 在配置 ACL 前，测试各 PC 机之间能否 ping 通及其互通性。

9. 为 RouterB 配置扩展 ACL 表并应用到端口。

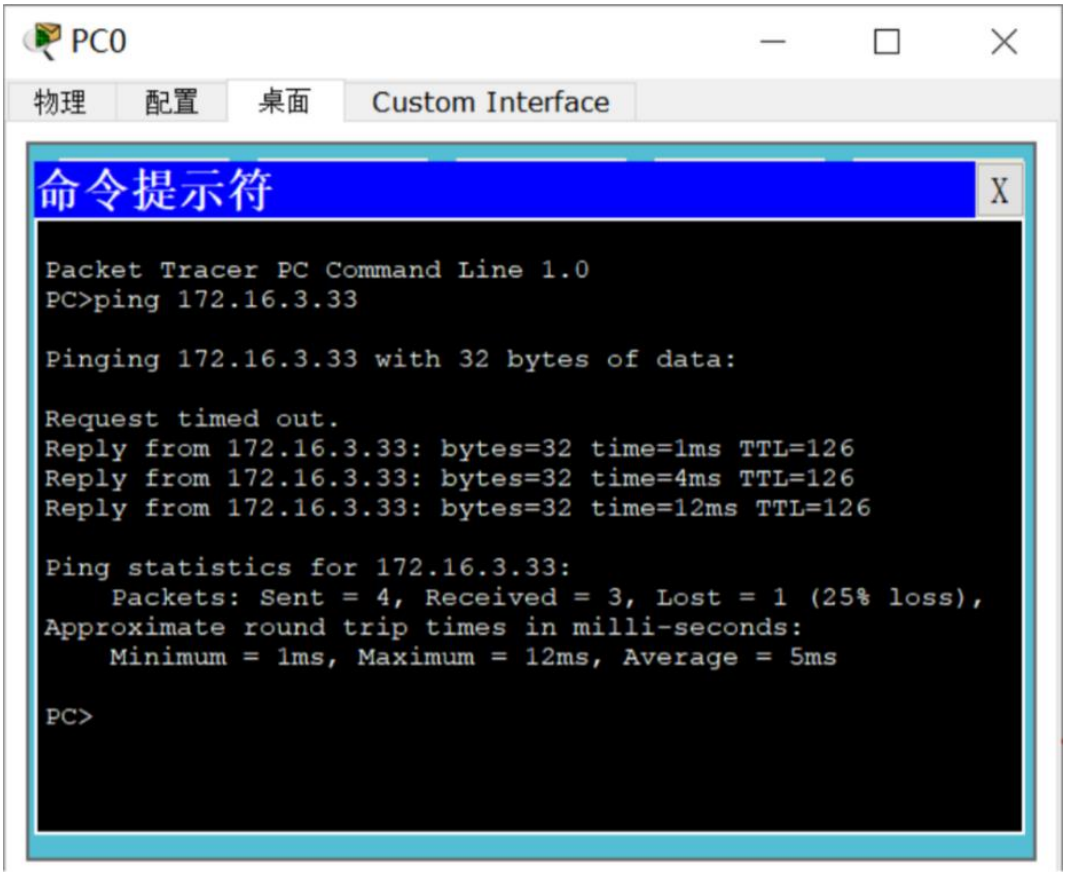
```
access-list 101 deny icmp host 192.168.1.11 host 172.16.3.33
access-list 101 permit tcp host 192.168.1.11 \
    host 172.16.3.33 eq www
interface Serial0/1/0
ip access-group 101 in
```

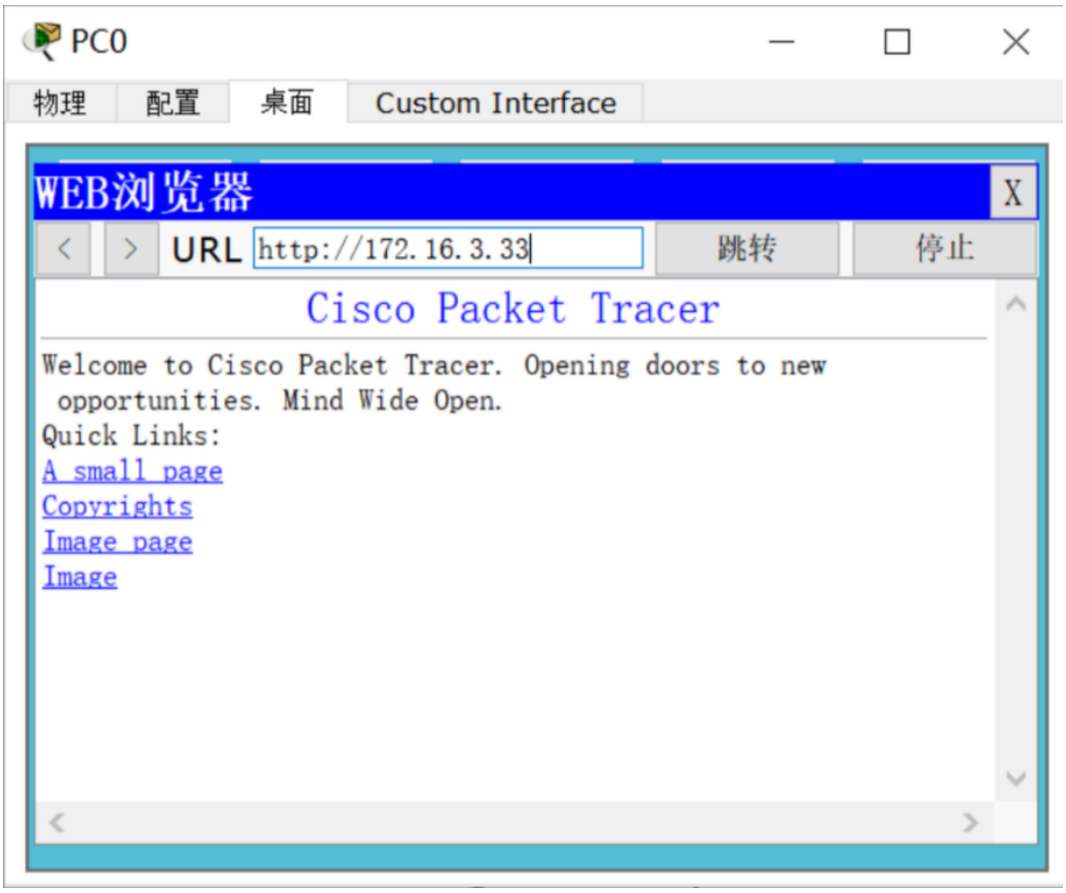
10. 在配置 ACL 后，测试各 PC 机之间能否 ping 通及其互通性。

**【实验现象】**

1. 在配置 ACL 前，测试各 PC 机之间能否 ping 通及其互通性。实验结果表明各

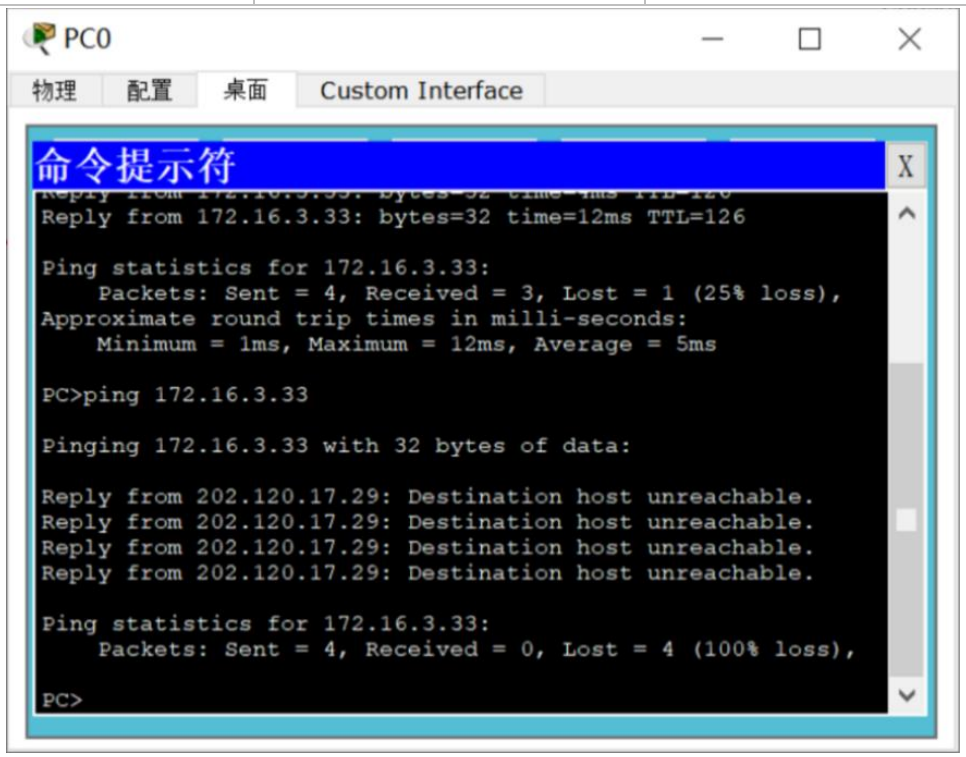
PC 机之间均访问成功。

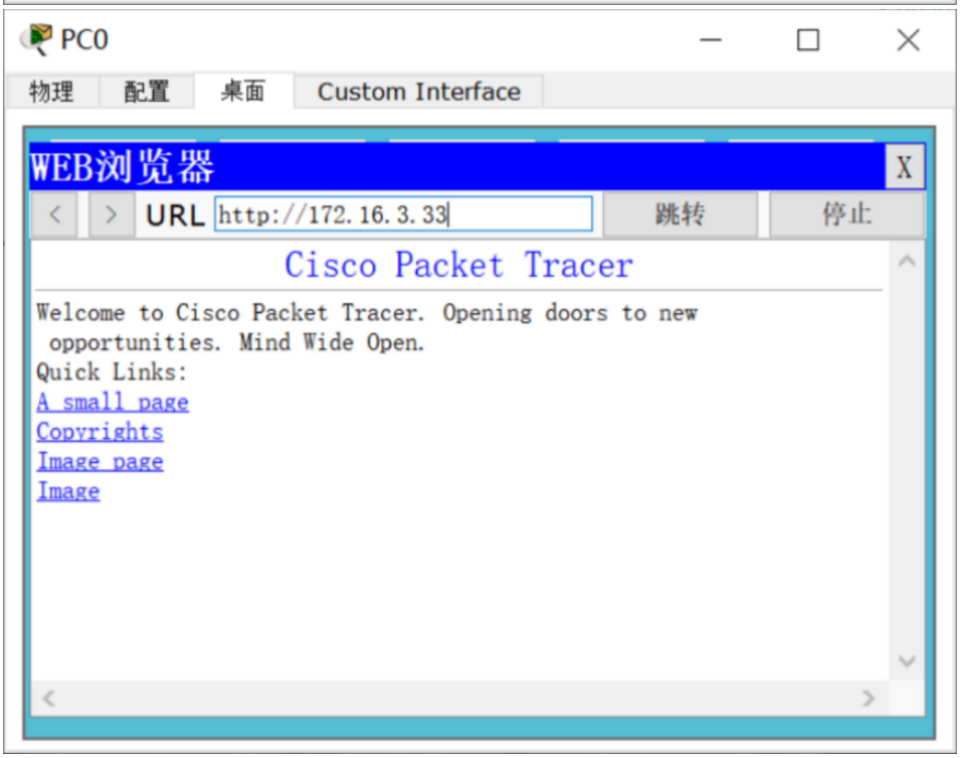

PC0
物理
配置
桌面
Custom Interface
命令提示符
X
Packet Tracer PC Command Line 1.0
PC>ping 172.16.3.33
Pinging 172.16.3.33 with 32 bytes of data:
Request timed out.
Reply from 172.16.3.33: bytes=32 time=1ms TTL=126
Reply from 172.16.3.33: bytes=32 time=4ms TTL=126
Reply from 172.16.3.33: bytes=32 time=12ms TTL=126
Ping statistics for 172.16.3.33:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 12ms, Average = 5ms
PC>


PC0
物理
配置
桌面
Custom Interface
WEB浏览器
X
URL
http://172.16.3.33
跳转
停止
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

2. 在配置 ACL 后，测试各 PC 机之间能否 ping 通及其互通性。

| PC | ping | http |
|---|---|---|
| PC0 | 失败 | 成功 |
| PC1 | 失败 | 失败 |
| PC2 | 成功 | 成功 |



【分析讨论】

实验结果清楚地展示了 ACL（接入控制列表）配置对路由器网络通信行为的直接影响。通过本次实验，可以观察到不同的 ACL 规则对网络数据包传输的控制效果，特别是如何影响网络中各个 PC 机的互通性。

一、PC0 的观察结果

PC0 可以成功发起 HTTP 请求，但不能成功执行 ping 操作。这个行为是 ACL 规则直接结果，其中明确拒绝了来自 PC0 的 ICMP 包（ping 使用 ICMP 协议），但允许了 TCP 协议下的 WWW 请求（HTTP 请求）。这种配置演示了 ACLs 如何细粒度地控制网络访问，允许特定类型的网络流量同时阻止其他类型，从而增强网络的安全性和特定服务的可用性。

二、PC1 的观察结果

PC1 的所有网络请求（包括 HTTP 和 ping）均失败。这表明 ACL 中可能存在更为严格的规则，完全阻断了从 PC1 出发的网络请求。这种情况可能是由于额外的 ACL 规则设置，或者 PC1 的网络配置本身存在问题导致无法通过 ACL 的检查。这也提示了 ACL 配置需要精确，错误的规则可能导致不必要的通信阻断。

三、PC2 的观察结果

PC2 在 ACL 配置前后均能成功执行 ping 和 HTTP 请求，表明它没有受到任何 ACL 规则的限制。这显示了 ACL 规则可以被设置为仅对网络中特定节点或通信类型生效，而不影响其他节点的正常通信。

# 实验 17：OSPF 动态网络路由配置实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/18 |

**【实验目的】**

本实验的主要目的是通过配置和验证 OSPF（开放最短路径优先）动态网络路由，来深入理解链路状态路由协议的工作机制。具体实验目的包括：

1. 掌握 OSPF 路由协议的基本工作原理，包括如何在自治系统内通过链路状态信息交换实现路由决策。
2. 学习如何在实际网络设备上配置 OSPF 协议，包括设置网络地址、端口配置和 OSPF 特定的参数。
3. 通过实验观察和验证网络中的路由器如何通过 OSPF 协议计算并更新路由表，以及如何处理网络拓扑的变化。
4. 验证配置后的网络中主机间的互通性，理解 OSPF 带来的路由优化效果。

**【实验原理】**

**OSPF（开放最短路径优先）技术原理**

OSPF 是一种链路状态的路由协议，主要用于同一个自治系统（AS）内。自治系统是指一组通过统一的路由政策或路由协议互相交换路由信息的网络。

1. 链路状态数据库（LSDB）：在 OSPF 中，每个路由器都会维护一个链路状态数据库。这个数据库包含了自治系统内所有链路的状态信息，如链路的可达性、带宽、延迟等。路由器使用这个数据库来计算到达网络中各个目的地的最佳路径。
2. 链路状态广告（LSA）：OSPF 路由器通过发送链路状态广告（LSA）来交换链路状态信息。LSA 是 OSPF 中用于广播和更新路由器之间链路状态的数据包。LSA 包含路由器的链接信息，包括邻接的路由器和连接成本，这些信息用来更新全局的链路状态数据库。
3. 区域分割：OSPF 允许将一个大的自治系统划分为多个较小的区域，每个区域内的 OSPF 路由器仅需维护本区域内的路由信息。这种区域划分可以减少路由更新导致的带宽消耗，提高路由计算的效率。
4. 与距离矢量协议的比较：与运行距离矢量协议（如 RIP）的路由器不同，OSPF

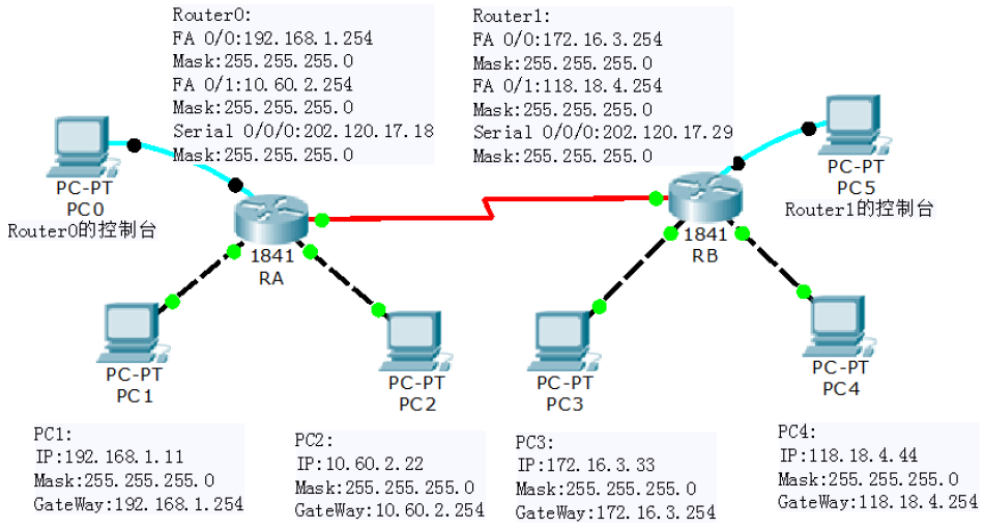
路由器不仅仅是将部分或全部的路由表传递给相邻的路由器，而是将链路状态信息传送给整个区域内的所有路由器。这种全面的信息交换使得 OSPF 能够更快地适应网络结构的变化，例如链路故障或是新链路的添加。

**【实验设备】**

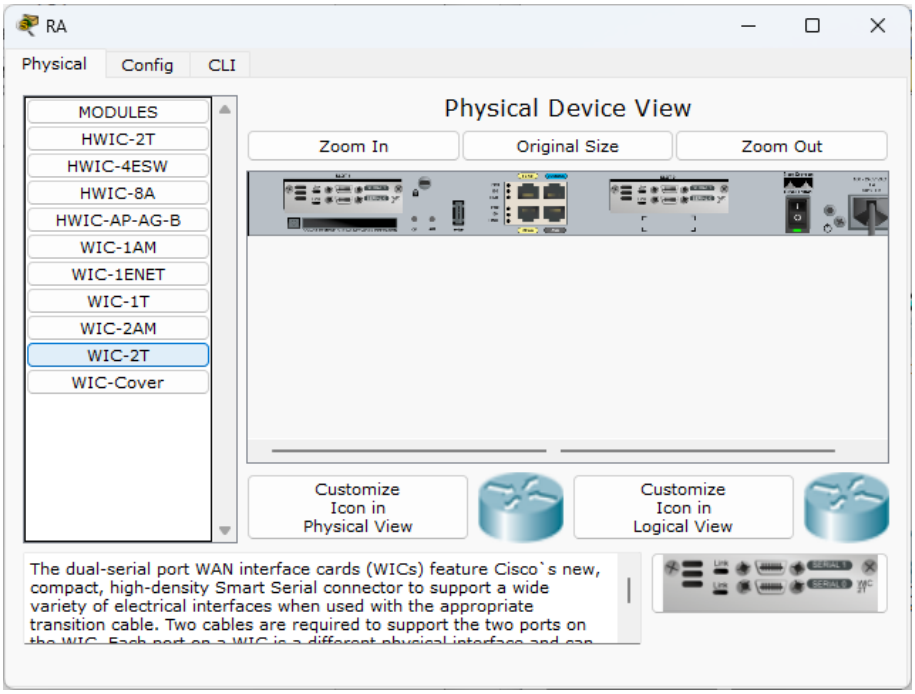
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

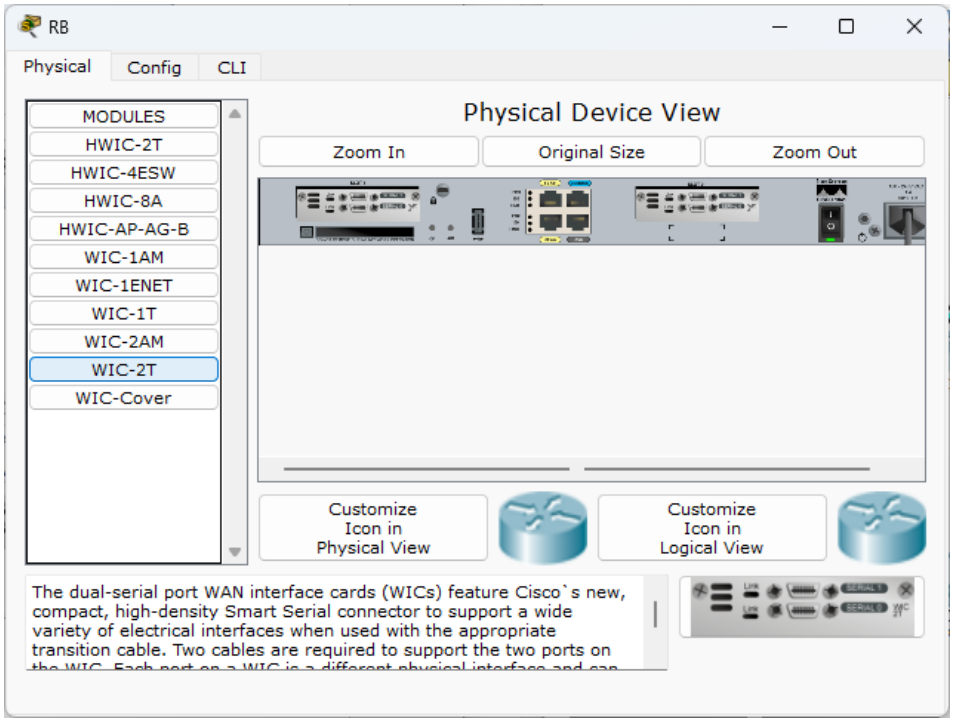
**【实验步骤】**

1. 规划网络地址及拓扑图。

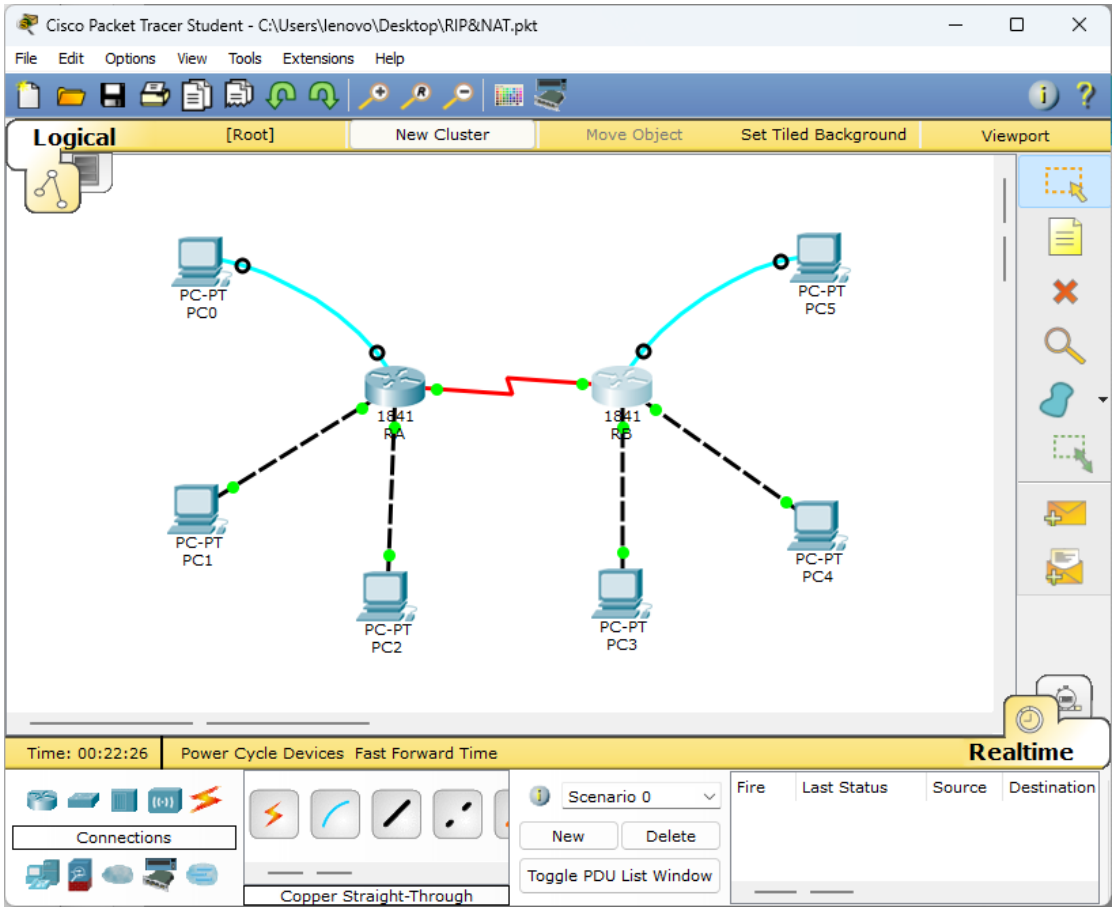



2. 在路由器 A 和路由器 B 中分别安装 WIC-2T，并重启设备。

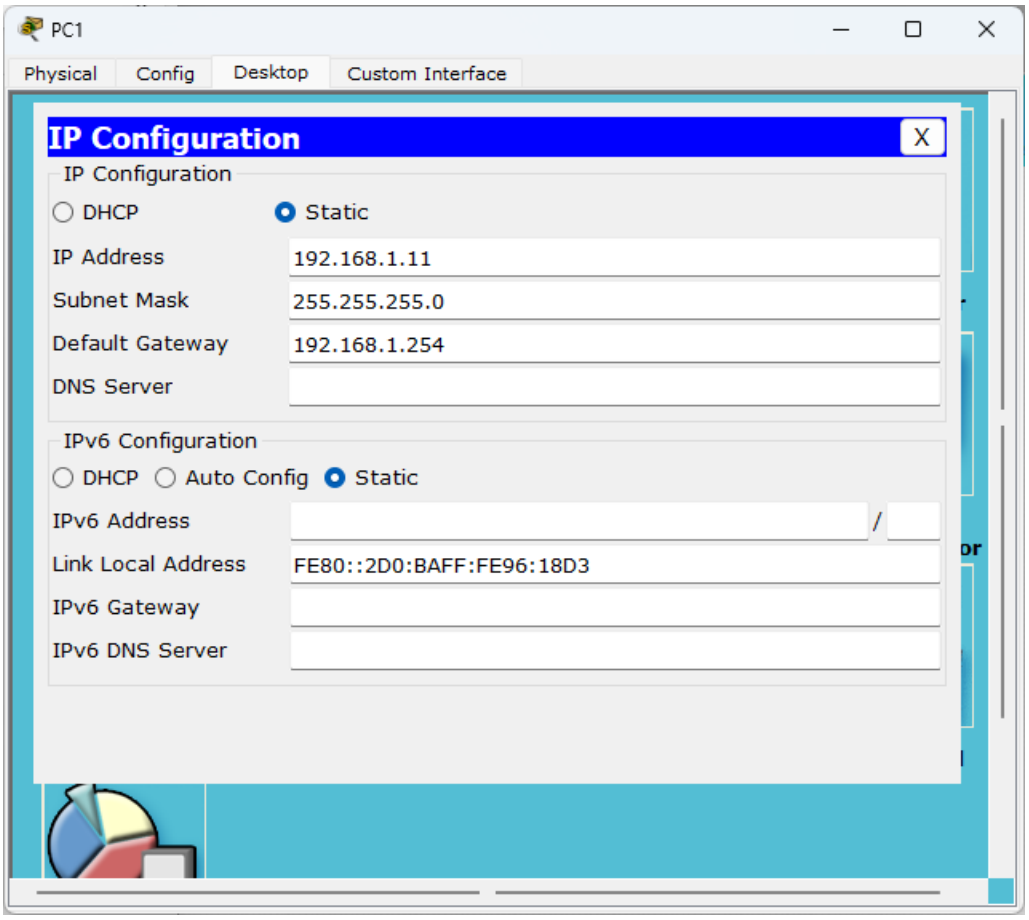


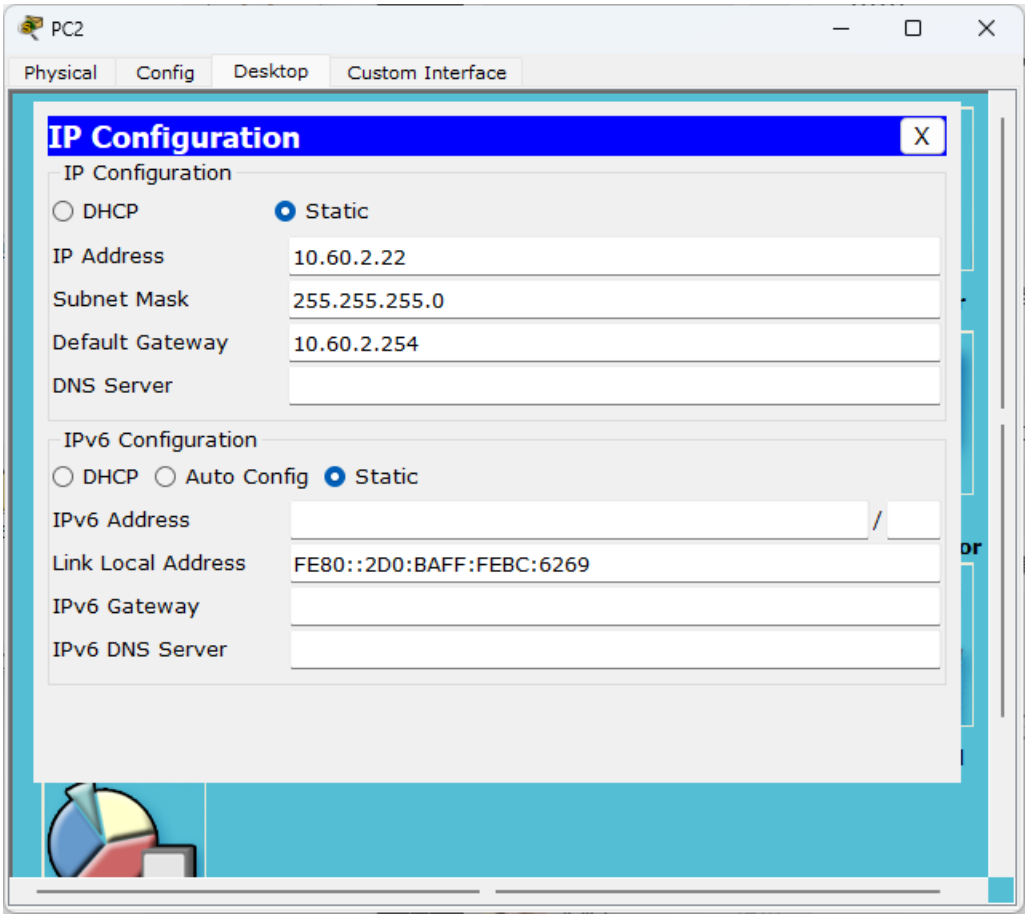


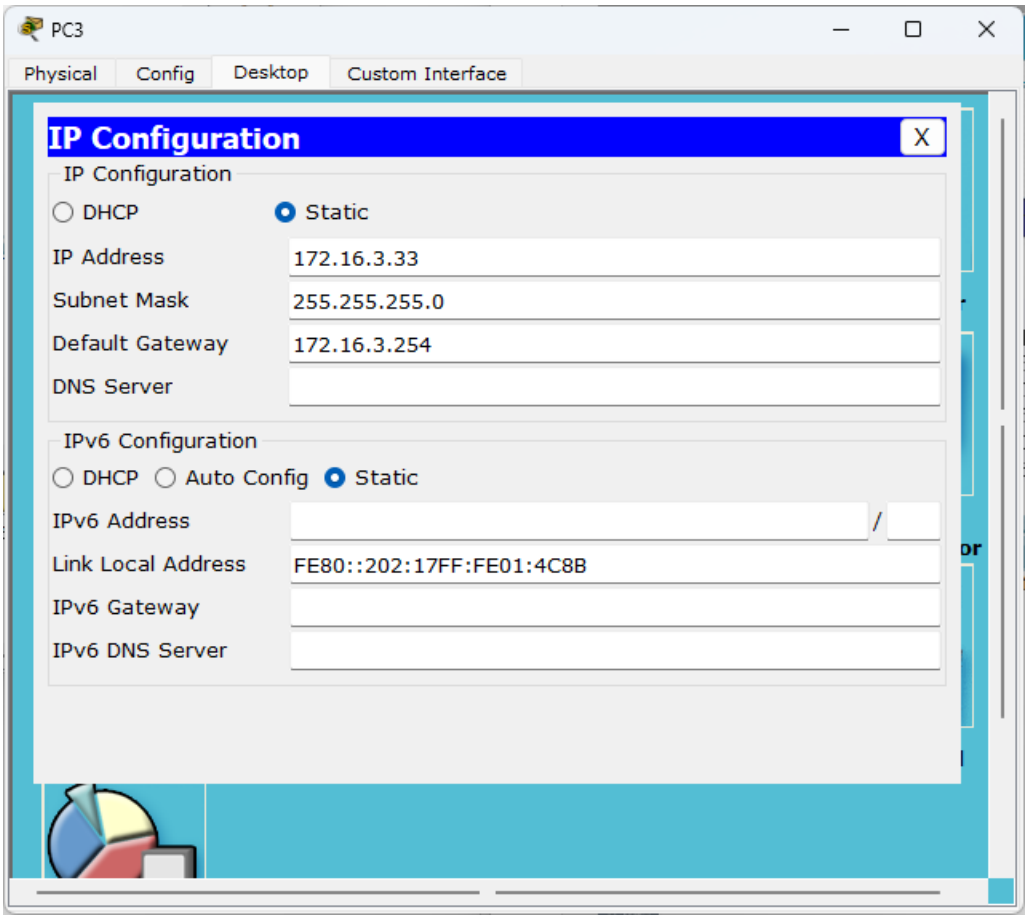

3. 启动 Cisco Packet Tracer，按照上述拓扑结构连接设备。

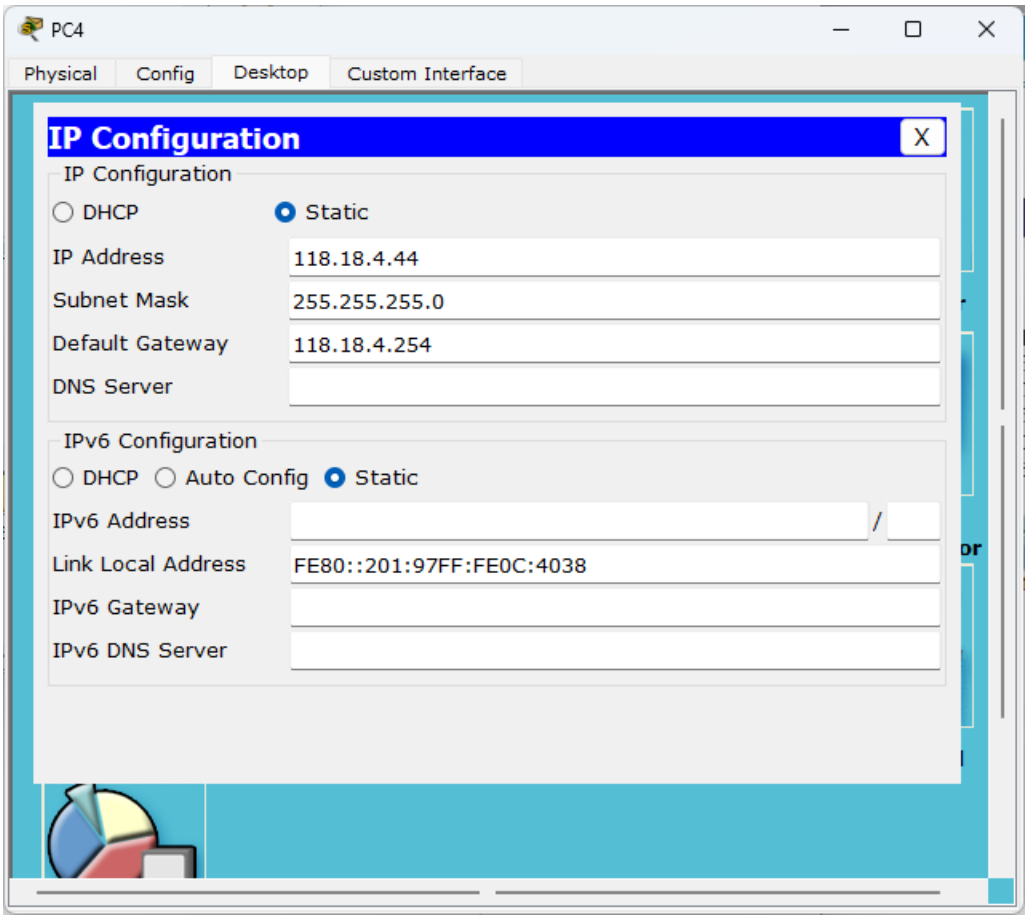



4. 配置 PC 机的 IP 地址、子网掩码和网关。


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE96:18D3
IPv6 Gateway
IPv6 DNS Server


PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.60.2.22
Subnet Mask
255.255.255.0
Default Gateway
10.60.2.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FEBC:6269
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
172.16.3.33
Subnet Mask
255.255.255.0
Default Gateway
172.16.3.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:17FF:FE01:4C8B
IPv6 Gateway
IPv6 DNS Server


PC4
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
118.18.4.44
Subnet Mask
255.255.255.0
Default Gateway
118.18.4.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE0C:4038
IPv6 Gateway
IPv6 DNS Server

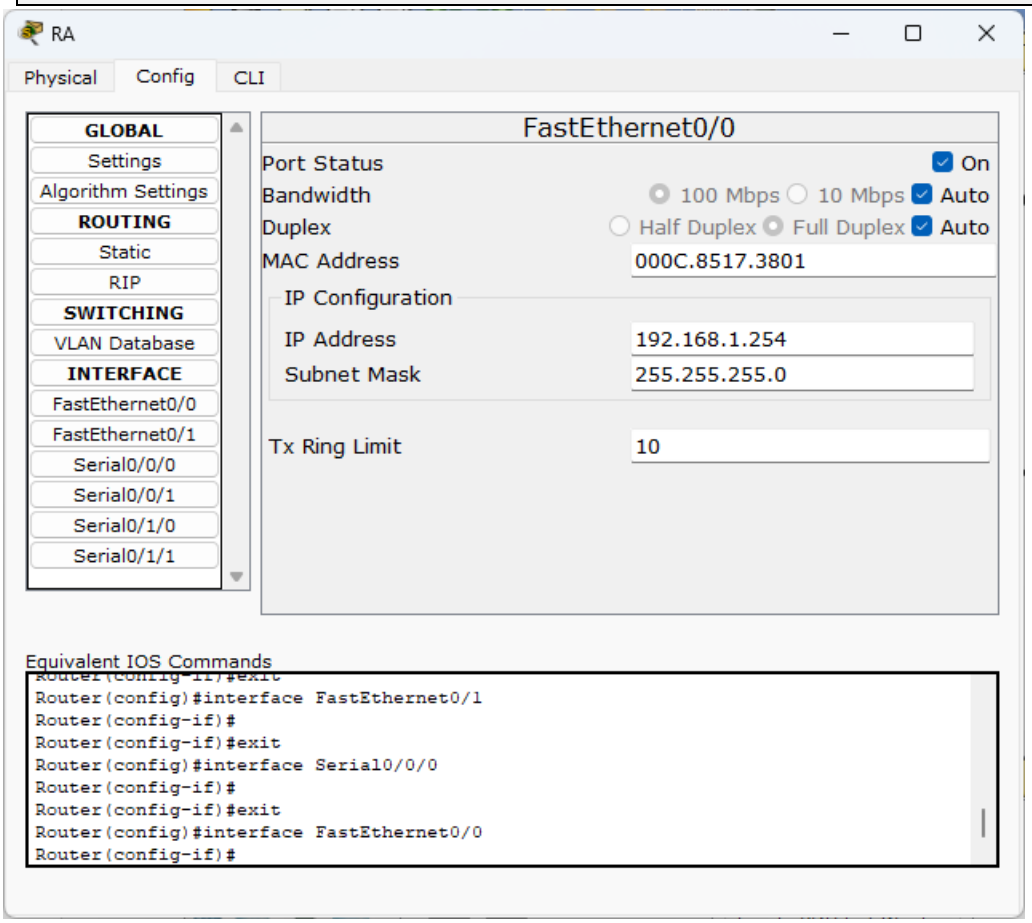
5. 配置路由器的端口地址和串口端口地址。

- 在路由器 A 的 CLI 中输入以下命令：

```
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.18 255.255.255.0
Clock rate 56000
```

- 在路由器 B 的 CLI 中输入以下命令：

```
interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.29 255.255.255.0
Clock rate 56000
```



RA

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/1

Port Status: On
Bandwidth: 100 Mbps, 10 Mbps, Auto
Duplex: Half Duplex, Full Duplex, Auto
MAC Address: 000C.8517.3802

IP Configuration
IP Address: 10.60.2.254
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
```

RA

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

Serial0/0/0

Port Status: On
Duplex: Full Duplex
Clock Rate: 2000000

IP Configuration
IP Address: 202.120.17.18
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
```

RB

Physical | Config | CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/0

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8101 |
| IP Configuration | |
| IP Address | 172.16.3.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

RB

Physical | Config | CLI

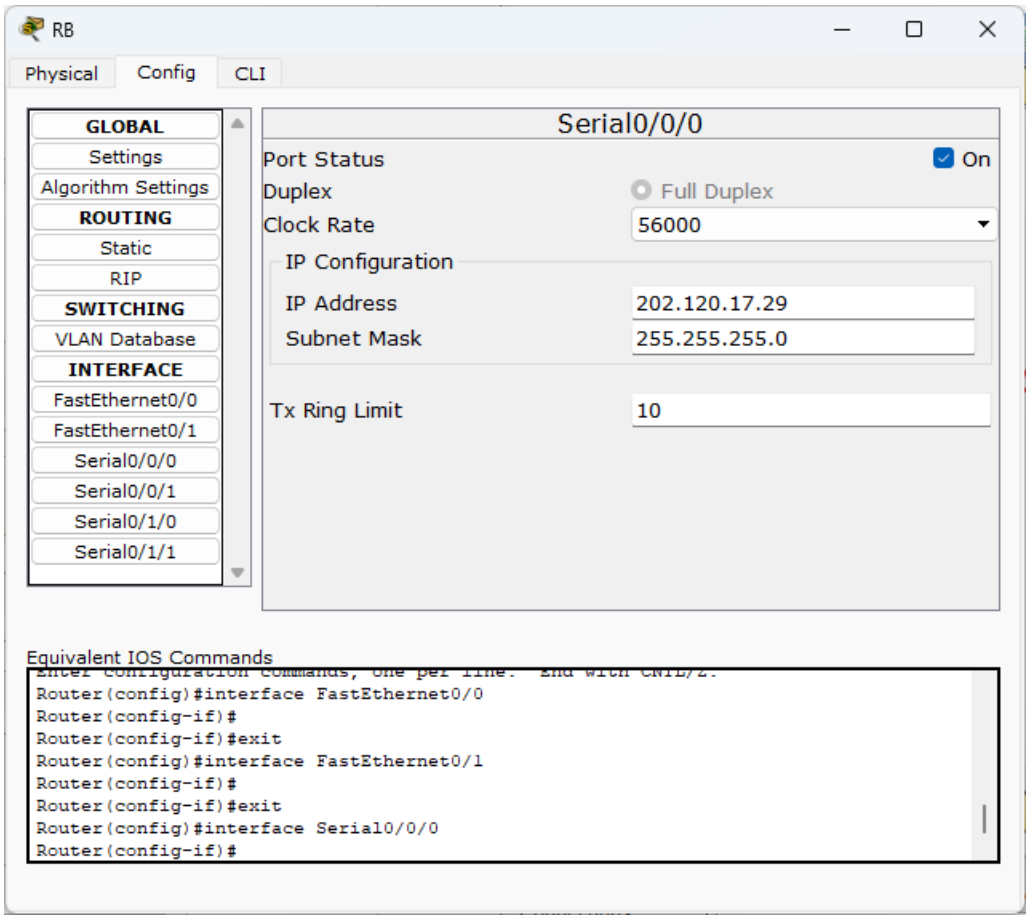
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1

FastEthernet0/1

| | |
|---|---|
| Port Status | On |
| Bandwidth | 100 Mbps 10 Mbps Auto |
| Duplex | Half Duplex Full Duplex Auto |
| MAC Address | 0009.7C5C.8102 |
| IP Configuration | |
| IP Address | 118.18.4.254 |
| Subnet Mask | 255.255.255.0 |
| Tx Ring Limit | 10 |

Equivalent IOS Commands

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
```




6. 在路由器 A 和 B 配置 OSPF 之前，测试各 PC 机之间能否 ping 通。

7. 为 RA 配置 OSPF 路由表。

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 10.60.2.0 0.0.0.255 area 0
network 202.120.17.0 0.0.0.255 area 0
```

8. 在路由器 A 或 B 配置 OSPF 之前，测试各 PC 机之间能否 ping 通。

9. 为 RB 配置 OSPF 路由表。

```
router ospf 1
network 172.16.3.0 0.0.0.255 area 0
network 118.18.4.0 0.0.0.255 area 0
network 202.120.17.0 0.0.0.255 area 0
```

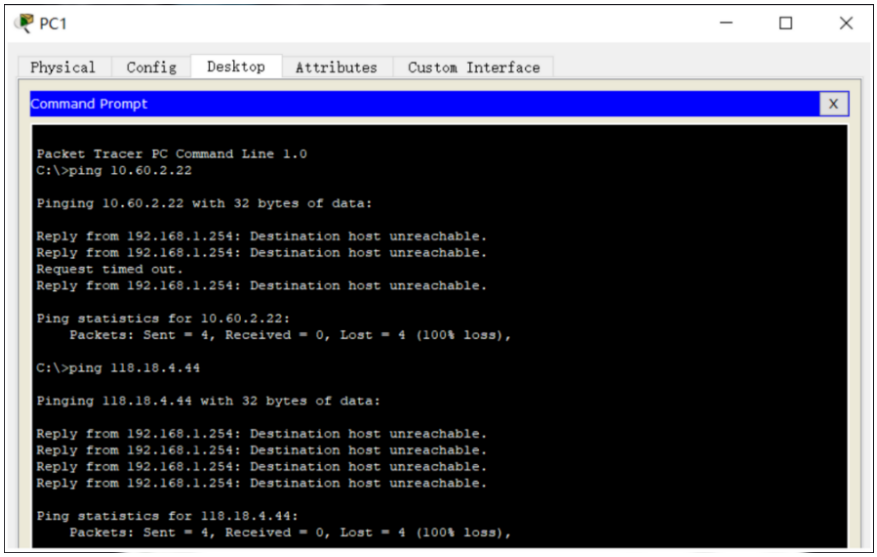
10. 在路由器 A 和 B 配置 OSPF 之前，测试各 PC 机之间能否 ping 通。

11. 通过 sh ip ospf neighbor，查看路由器的邻居。

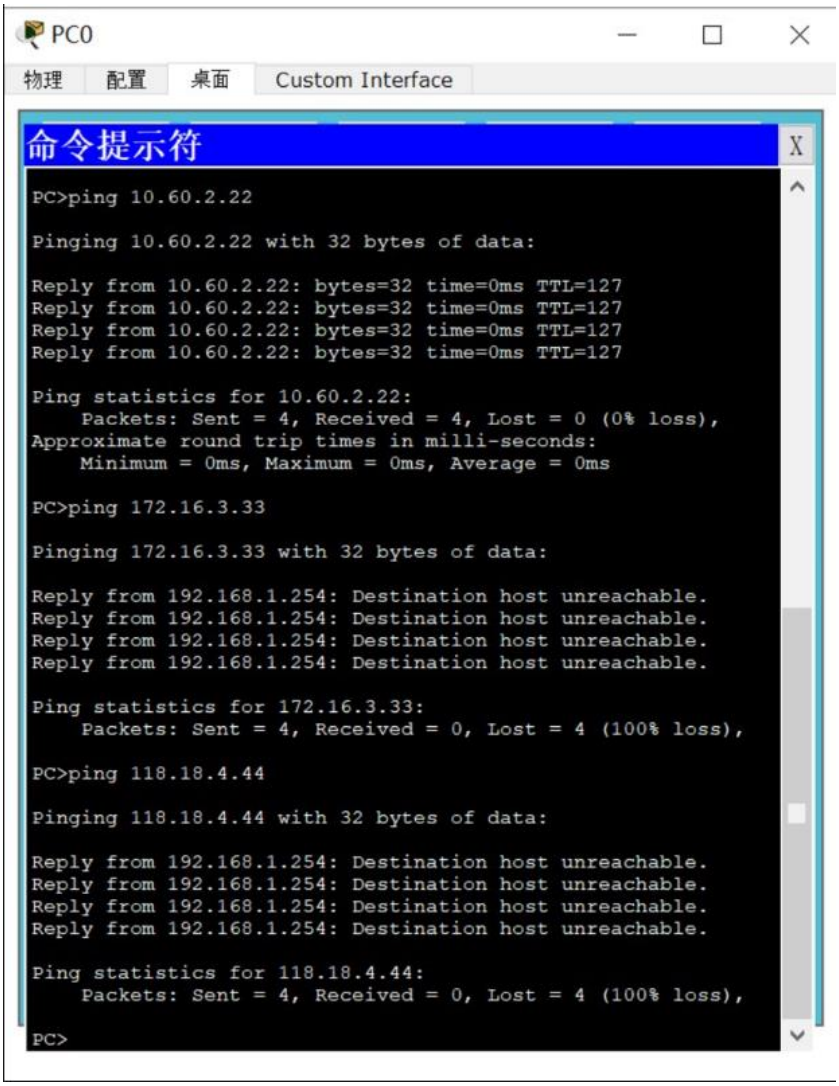
**【实验现象】**

1. 在路由器 A 和 B 配置 OSPF 之前，测试各 PC 机之间能否 ping 通。实验结果

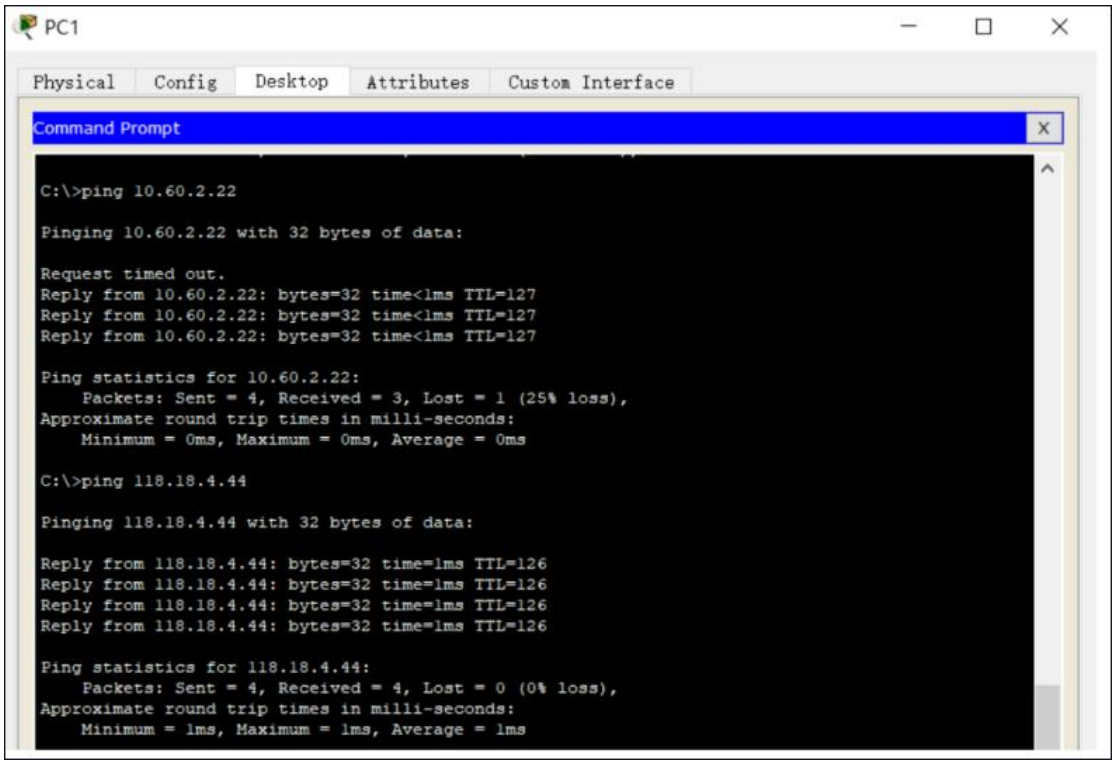
表明任意两个 PC 机之间不能 ping 通。




2. 在路由器 A 或 B 配置 OSPF 之前，测试各 PC 机之间能否 ping 通。实验结果表明路由器 A 的两个 PC 机之间能 ping 通，其他 PC 机之间不能 ping 通。



3. 在路由器 A 和 B 配置 OSPF 之前，测试各 PC 机之间能否 ping 通。实验结果表明任意两个 PC 机之间均能 ping 通。




4. 通过 sh ip ospf neighbor，查看路由器的邻居。

- 路由器 A 的邻居

```
%SYS-5-CONFIG_I: Configured from console by console

Router#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
202.120.17.29     0   FULL/  -        00:00:31    202.120.17.29   Serial0/0/0
```

- 路由器 B 的邻居

```
%SYS-5-CONFIG_I: Configured from console by console

Router#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
202.120.17.18     0   FULL/  -        00:00:32    202.120.17.18   Serial0/0/0
```

**【分析讨论】**

**一、实验结果分析**

通过实验前后的 ping 测试，可以观察到 OSPF 配置前后 PC 机之间互通情况的变化。特别是在配置 OSPF 后，原本无法通信的 PC 机（例如跨子网的 PC1 和

PC2）开始能够相互访问，显示了 OSPF 路由的有效性和自动路由计算的优势。

**二、子网配置问题**

PC1 和 PC2 即使连接到同一个路由器 RA，但由于它们位于不同的子网，因此在没有路由协议帮助路由器理解如何从一个子网到达另一个子网之前，它们不能直接通信。

PC1 的配置：IP 地址 192.168.1.11，子网掩码 255.255.255.0，网关 192.168.1.254。

PC2 的配置：IP 地址 10.60.2.22，子网掩码 255.255.255.0，网关 10.60.2.254。

**三、静态路由限制**

没有额外的路由配置，路由器 RA 不知道如何将从一个网络接口接收到的数据包转发到另一个网络接口。

# 实验 18：动态 IP 地址分配 DHCP 实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/25 |

**【实验目的】**

本次实验的主要目的是学习和掌握动态主机配置协议（DHCP）在大型局域网络环境中的应用。通过这个实验，学生将了解如何使用 DHCP 来集中管理和分配 IP 地址，使得网络环境中的主机可以动态地获取 IP 地址、网关地址、DNS 服务器地址等重要网络配置信息。这不仅可以提高地址的利用率，还可以减少配置错误，简化设备的配置和部署过程。实验包括规划网络地址和拓扑，配置路由器接口和 DHCP 服务，以及验证配置的正确性。通过这些步骤，学生将能够深入理解客户端/服务器模型下的地址动态分配机制，并实践如何设置和管理一个由 DHCP 控制的网络环境。

**【实验原理】**

**一、动态主机配置协议（DHCP）**

动态主机配置协议（DHCP，Dynamic Host Configuration Protocol）是一个广泛使用的网络协议，主要在大型局域网络环境中发挥作用。其核心目的是集中管理和自动分配 IP 地址，从而使网络中的设备（客户端）能够动态地获取必要的网络配置信息，例如 IP 地址、网关地址和 DNS 服务器地址。这种方式大大提高了 IP 地址的使用效率和网络管理的便捷性。

DHCP 基于客户端/服务器模型工作。在这种模型中：

- 服务器负责管理一个或多个 IP 地址池以及相关配置信息，如默认网关、DNS 服务器信息等。
- 客户端在启动时向网络广播寻找 DHCP 服务器，请求网络配置信息。

交互过程通常包括四个步骤，通常称为 DORA 过程：

1. 发现(Discovery)：客户端通过广播发送 DHCP 发现消息(DHCPDISCOVER)，寻找可用的 DHCP 服务器。
2. 提供（Offer）：DHCP 服务器响应发现请求，向客户端发送包含 IP 地址提供的 DHCP 提供消息（DHCPOFFER）。
3. 请求（Request）：客户端选择一个接收到的提供，并通过广播发送请求

消息（DHCPREQUEST），请求选定的 IP 地址和配置参数。

4. 确认（Acknowledgement）：DHCP 服务器确认这一请求，并发送确认消息（DHCPACK），包含 IP 地址以及其他配置信息。

DHCP 的通信是通过 UDP 协议实现的，客户端发送消息到服务器的 UDP 67 号端口，服务器则回应消息到客户端的 UDP 68 号端口。通过这种机制，DHCP 不仅简化了网络设备的配置过程，减少了配置错误，还使得网络管理员可以更加高效地管理网络地址分配和相关配置。

**二、DHCP 设备**

在基于动态主机配置协议（DHCP）的网络中，设备主要分为两类：DHCP 客户端和 DHCP 服务器。这两者共同在客户端/服务器（C/S）模式下运作，以实现网络配置的自动化和集中管理。

- DHCP 客户端

DHCP 客户端通常是连接到网络的设备，如个人电脑、智能手机或其他网络设备。这些客户端在启动时会自动向网络发送请求，寻找 DHCP 服务器以获取网络配置信息。主要好处包括：

1. 简化配置过程：自动从 DHCP 服务器获取 IP 地址、子网掩码、默认网关、DNS 服务器等信息，减少了手动配置的需要。
2. 减少错误：由于配置是自动完成的，所以减少了手动输入设置时可能发生的错误。
3. 集中管理：网络管理员可以集中管理 IP 地址和其他网络设置，易于追踪和修改，提高了网络管理的效率。

- DHCP 服务器

DHCP 服务器是配置和管理 IP 地址池及其他相关网络设置的中心设备。它响应来自客户端的请求，分配网络配置参数。服务器的主要职责包括：

1. 地址分配：控制 IP 地址范围（地址池），并根据网络需求动态分配给请求的客户端。
2. 配置管理：提供子网掩码、默认网关、DNS 设置等信息，确保网络设备能够正确访问网络资源。
3. 地址再利用：管理地址租用时间，当租期到期未被续租时，可以将 IP 地

址重新分配给其他请求的客户端。

**三、DHCP 配置方法**

配置动态主机配置协议(DHCP)主要涉及在 DHCP 服务器上设定一系列参数，以确保客户端可以自动获得正确的网络配置信息。以下是一个标准的路由器（作为 DHCP 服务器）的配置步骤：

1. 设置不可用的地址区间

   首先，定义哪些 IP 地址是不可用的，通常这些地址是为网络设备如路由器、打印机或服务器保留的固定 IP 地址。这样可以避免 DHCP 服务器分配已经手动设置的静态 IP 地址。

2. 建立地址池

   创建一个或多个地址池,每个池都有一个唯一标识符,比如 myleftnet。地址池包含了可以动态分配给客户端的 IP 地址范围。

3. 设置网络号和掩码

   为每个地址池指定网络号和子网掩码。这决定了该地址池中 IP 地址的网络部分和主机部分，从而确保分配的地址在正确的子网中。

4. 分配地址

   配置服务器以从地址池中选择未使用的地址自动分配给请求配置的客户端。这通常是基于先到先服务的策略。

5. 设置客户端的默认网关

   指定客户端应使用的默认网关地址。这通常是网络中的路由器地址，确保客户端能够访问本地网络外的目的地。

6. 设置域名服务器

   配置 DNS 服务器的地址，这是客户端解析域名所需的。提供 DNS 服务器地址允许客户端连接和解析网络中的其他系统和服务。

7. 设置其他相关选项

   除了基本的网络配置，还可以设置其他 DHCP 选项，如 NTP 服务器（网络时间协议），VoIP 配置，以及其他自定义的网络服务设置。

**【实验设备】**

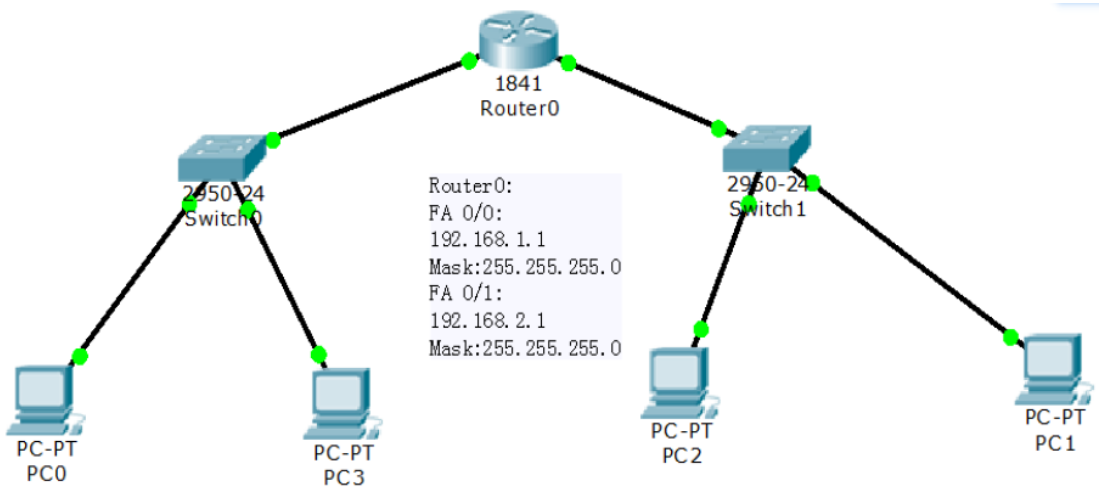
1. 操作系统：Windows 10

2. 网络环境：局域网

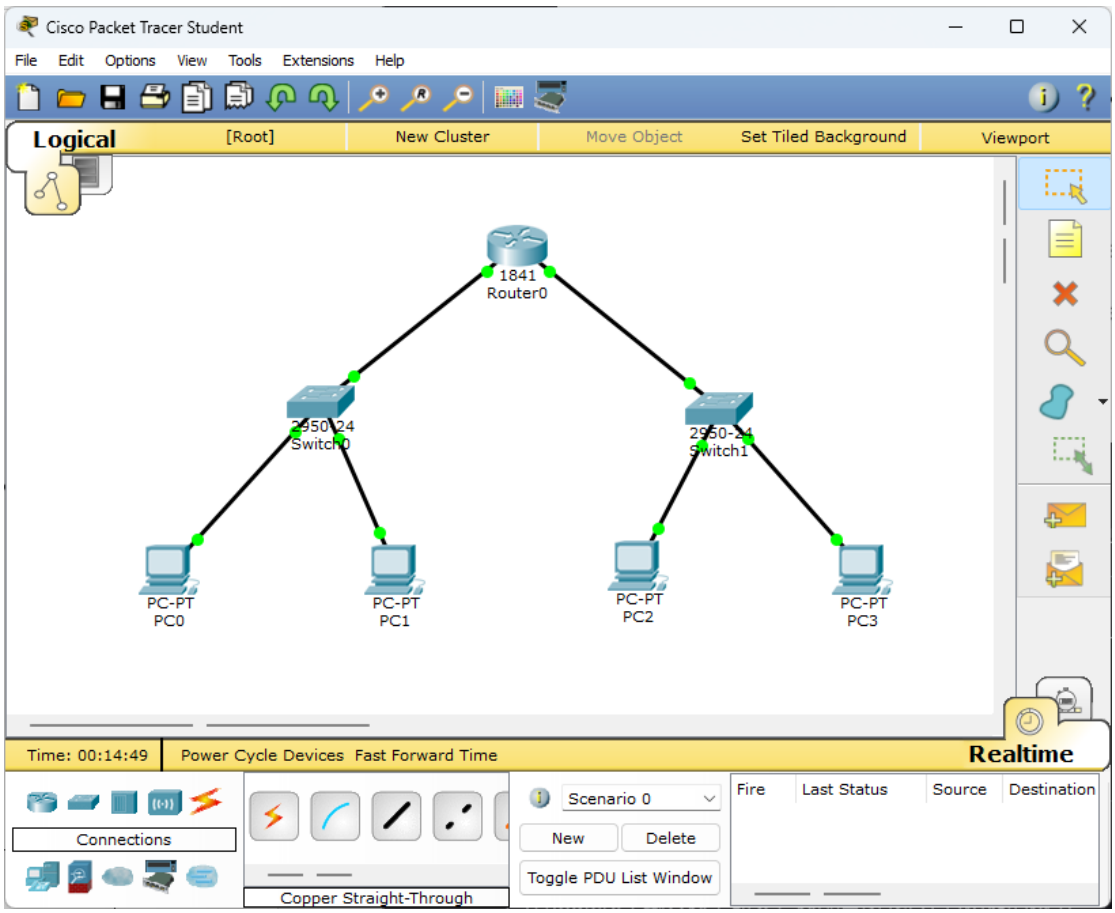
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。

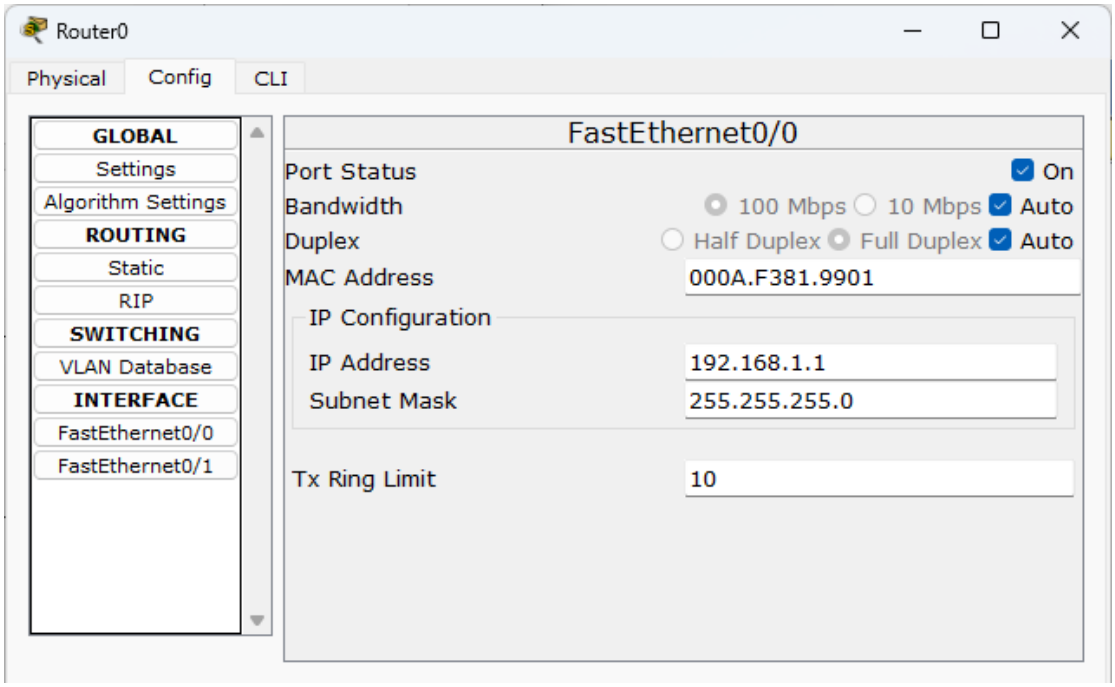


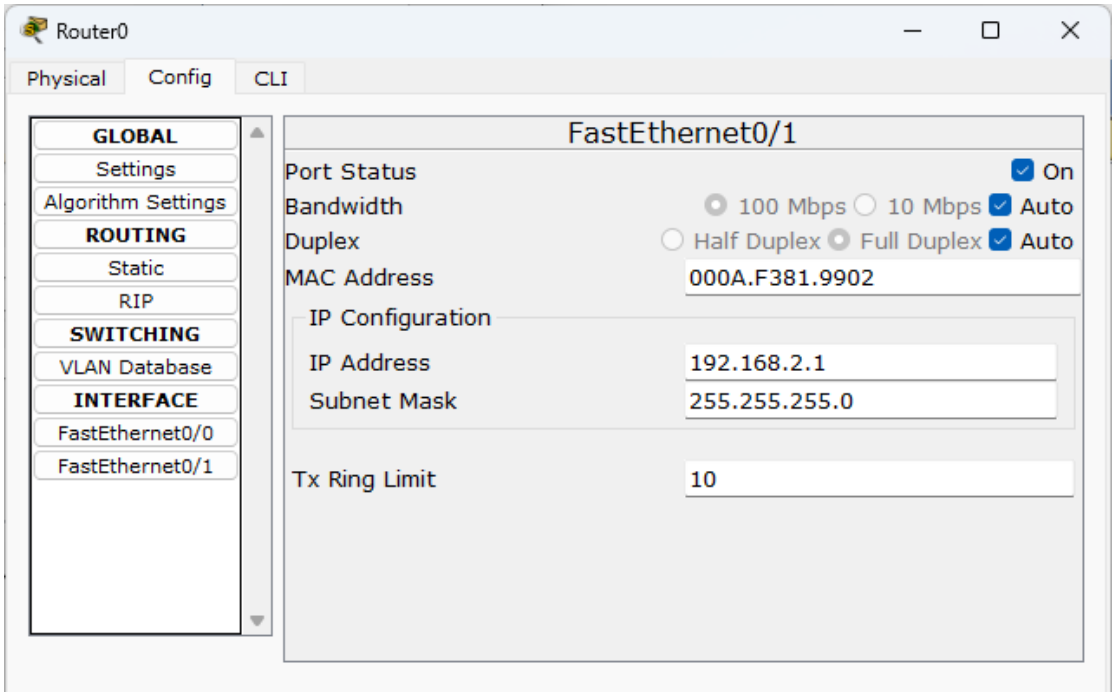

2. 启动 Cisco Packet Tracer，按照上图连接网络。




3. 配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```




4. 配置 DHCP 前查看各 PC IP 地址情况。

5. 在路由器 Router0 配置 DHCP。

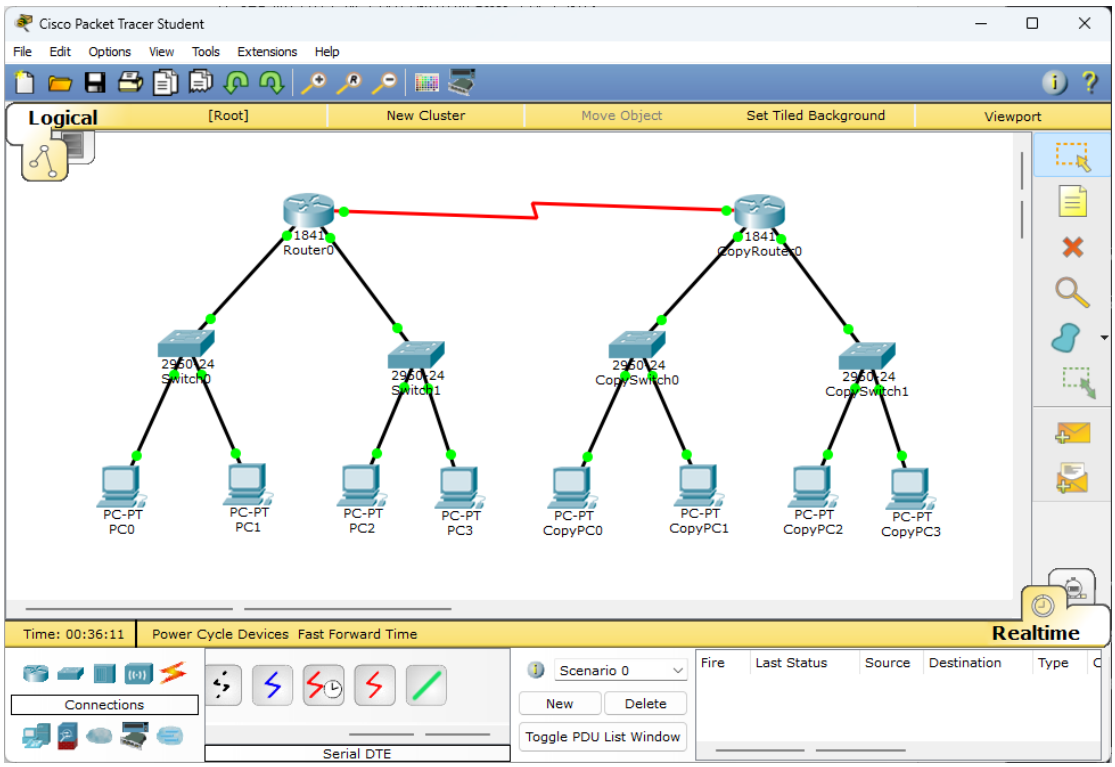
   - 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

6. 配置 DHCP 后查看各 PC IP 地址情况。
7. 两台路由器各自连接交换机，将路由器连接。在 Cisco Packet Tracer 中，按照下图连接网络。




8. 在路由器 CopyRouter0 配置 DHCP。
   - 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

```
ip dhcp excluded-address 192.168.3.0 192.168.3.10
```

```
ip dhcp pool myleftnet
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
option 150 ip 192.168.3.3
dns-server 192.168.3.2
```

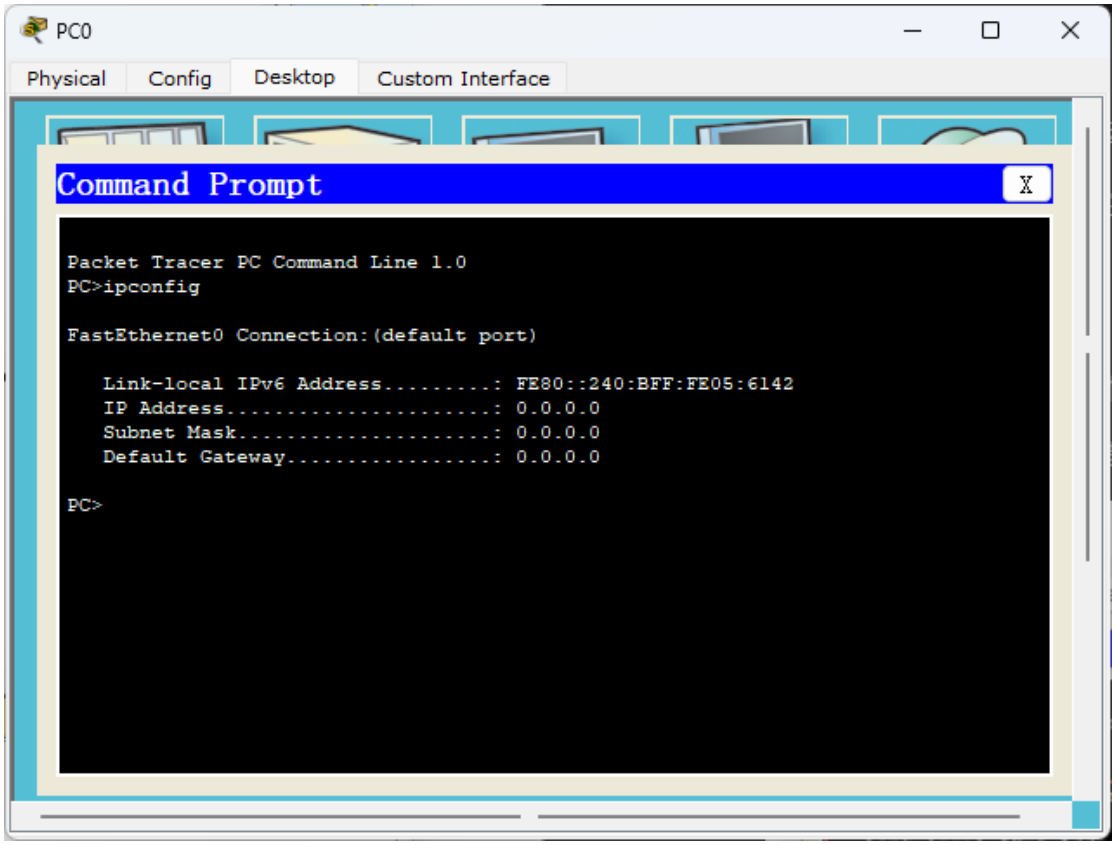
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

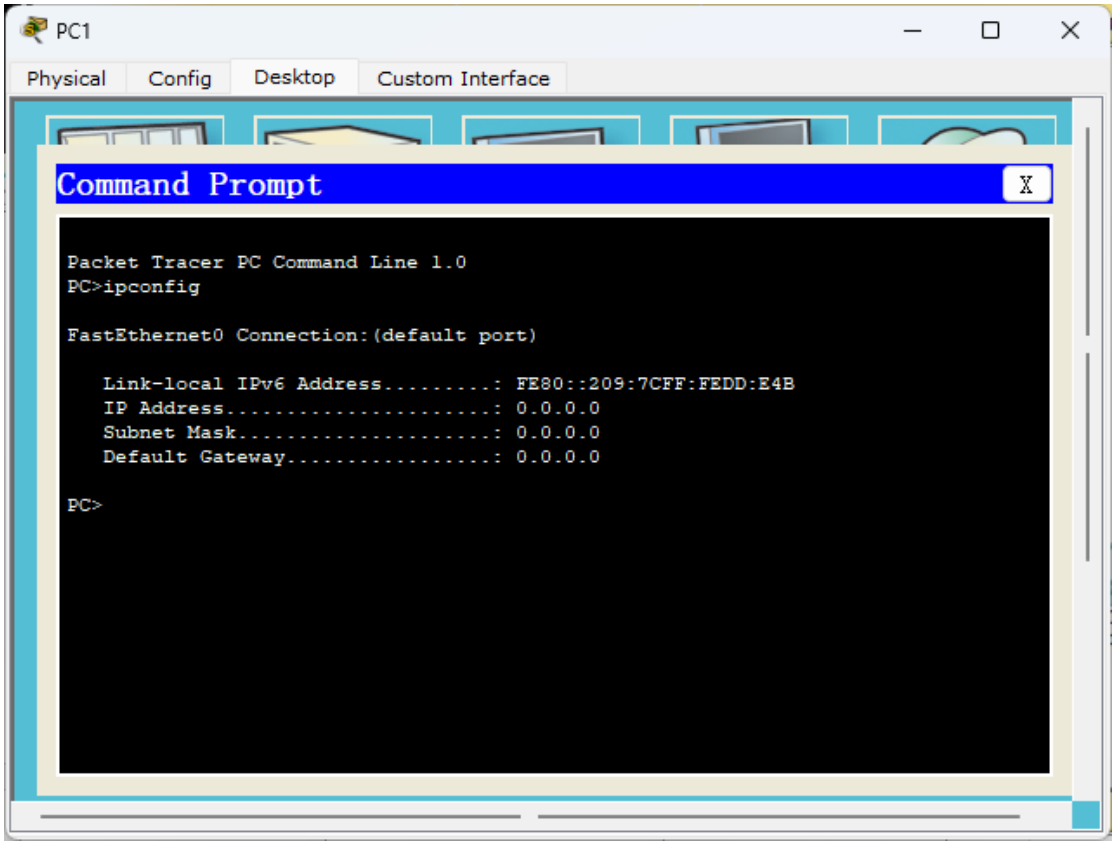
```
ip dhcp excluded-address 192.168.4.0 192.168.4.10
ip dhcp pool myrightnet
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
option 150 ip 192.168.4.3
dns-server 192.168.4.2
```

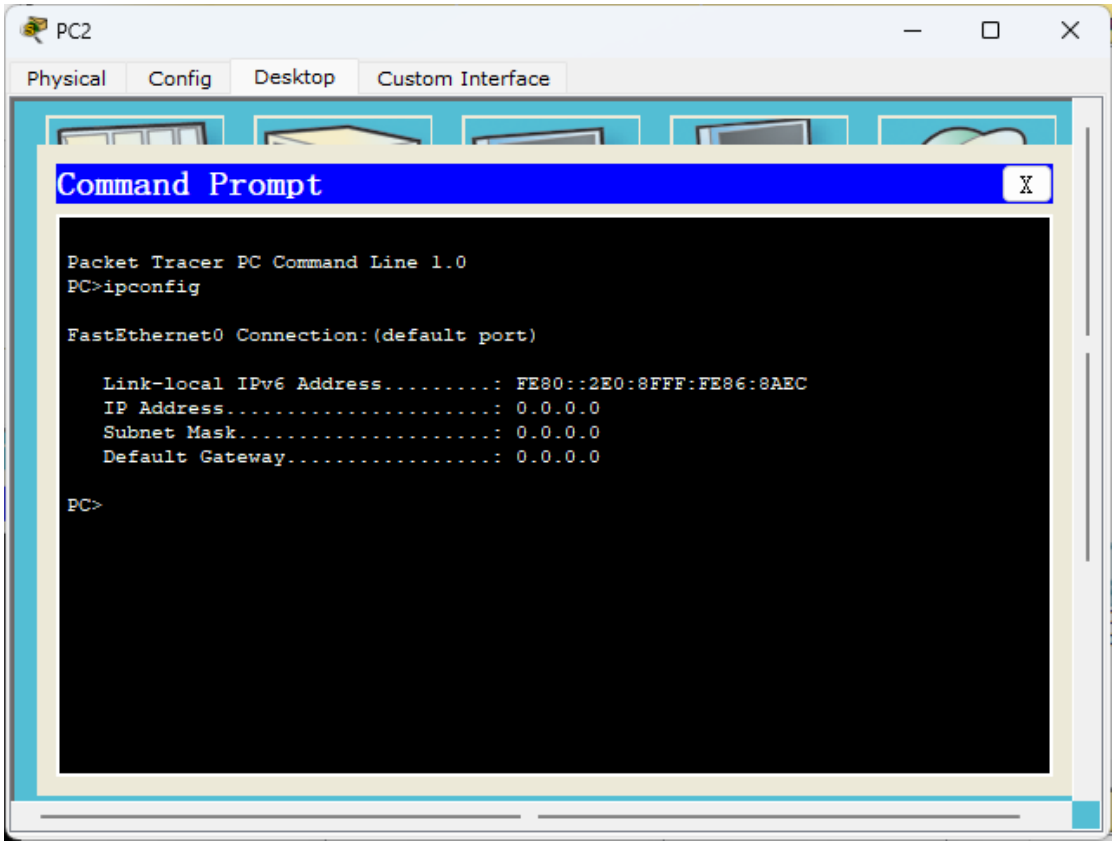
9. 根据 RIP 路由配置实验的方法对串口线进行配置。
10. 左右两边的 PC 机相互进行 ping 测试，观察并记录实验现象。

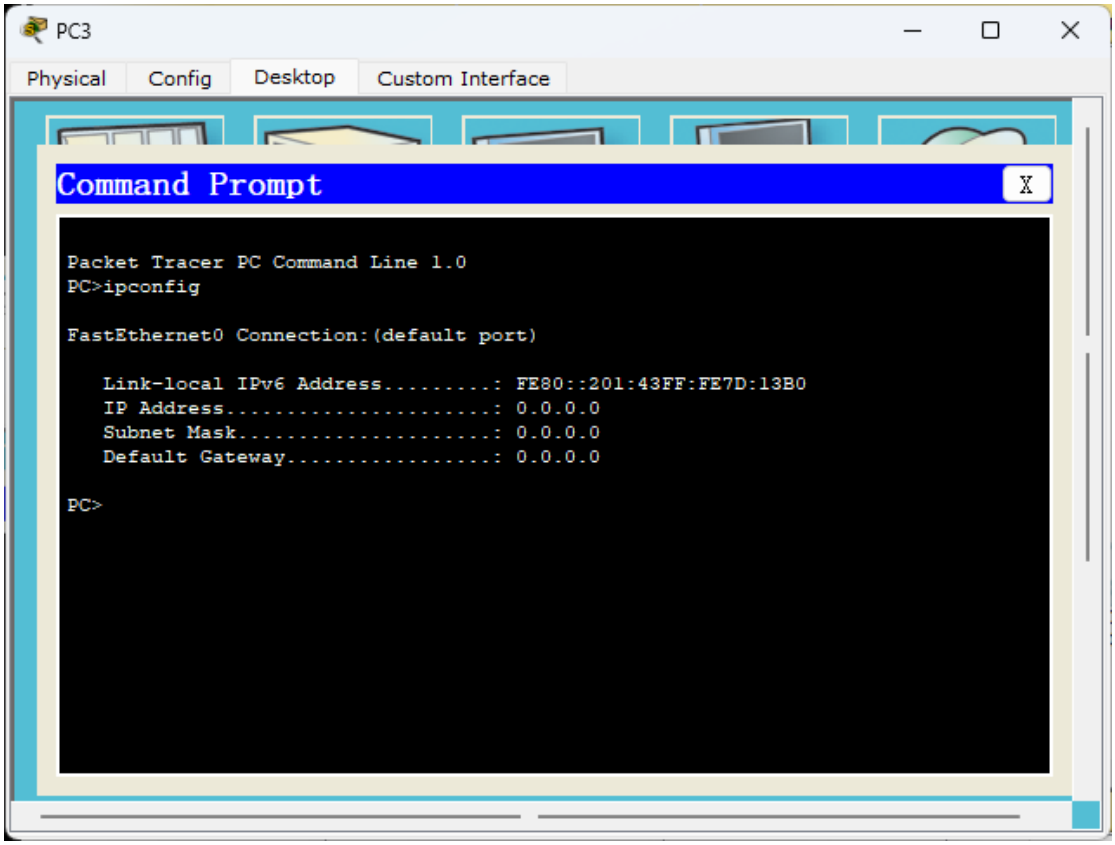
**【实验现象】**

1. 配置 DHCP 前查看各 PC IP 地址情况，各 PC 机的 IP 地址、子网掩码、默认网关均相同，为 0.0.0.0。




PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::209:7CFF:FEDD:E4B
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
PC>


PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::2E0:8FFF:FE86:8AEC
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
PC>




2. 配置 DHCP 后查看各 PC IP 地址情况。

- PC0：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::290:21FF:FEAD:CD14
   IP Address.......................: 192.168.1.12
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.1.1
```

- PC1：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::207:ECFF:FECE:EB7E
   IP Address.......................: 192.168.1.14
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.1.1
```

- PC2：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE48:E19B
   IP Address.......................: 192.168.2.12
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.2.1
```

- PC3：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::20C:CFFF:FEE5:5B6D
   IP Address......................: 192.168.2.14
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.2.1
```

| PC | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|
| PC0 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC1 | 192.168.1.14 | 255.255.255.0 | 192.168.1.1 |
| PC2 | 192.168.2.12 | 255.255.255.0 | 192.168.2.1 |
| PC3 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1 |

3. 配置 DHCP 后，左右两边的 PC 机相互进行 ping 测试，均成功。

- PC0 ping PC1、PC2、PC3：

```
Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.2.12 with 32 bytes of data:

Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 192.168.2.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.14: bytes=32 time=1ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC1 ping PC0、PC2、PC3：

```
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
Pinging 192.168.2.12 with 32 bytes of data:

Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 192.168.2.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.14: bytes=32 time=1ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC2 ping PC0、PC1、PC3：

```
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.2.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.14: bytes=32 time=1ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC3 ping PC0、PC1、PC2：

```
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.2.12 with 32 bytes of data:

Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**【分析讨论】**

**一、实验现象分析**

配置 DHCP 前：各 PC 机的 IP 地址、子网掩码、默认网关均为 0.0.0.0，表示在没有 DHCP 配置之前，这些 PC 机没有获得任何网络配置信息，因此无法进行网络通信。

配置 DHCP 后：通过 DHCP 服务，PC 机自动获得了 IP 地址、子网掩码和默认网关。这表明 DHCP 服务器成功地为客户端分配了网络配置，使它们具备了进行

网络通信的基本条件。

Ping 测试成功：配置 DHCP 后，左右两边的 PC 机可以相互进行 ping 测试，并且测试成功。这说明网络中的路由及网络配置正确，DHCP 分配的 IP 地址能够正确地在网络中路由和访问。

**二、实验结果分析**

DHCP 服务器的设置确保了各客户端能够自动、正确地获得 IP 配置，这减少了网络配置错误的可能性，并简化了网络管理。

成功的 ping 测试验证了网络连通性，显示 DHCP 分配的 IP 地址、网关和子网掩码的有效性，同时也测试了网络设备（如路由器和交换机）的配置正确性。

本实验还展示了网络的动态能力，即在增加新的客户端时，无需手动配置即可加入并正常工作于网络中。

# 实验 19：无线网络组网实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/28 |

**【实验目的】**

1. 理解无线网络基本原理：通过实验，学生可以深入了解无线网络的工作原理，包括无线信号的传输、接收和数据处理。
2. 熟悉无线网络配置：实验涉及无线路由器和接入点的配置，使学生能够掌握无线网络设备的设置和管理技能。
3. 实践网络规划与管理：通过规划网络地址和拓扑图，配置路由器和 DHCP 服务器，学生可以实践网络设计和管理的技能，理解网络地址分配和路由选择的重要性。
4. 掌握故障排查和网络测试方法：实验中包括使用 Ping 测试等工具来验证网络配置的正确性和网络连通性，提高学生的网络故障诊断和解决问题的能力。
5. 增强实际操作能力：通过亲手配置和测试实际设备，学生可以将理论知识应用到实践中，增强实际操作能力和解决实际问题的能力。

**【实验原理】**

**一、WIFI 简介**

Wi-Fi（无线保真，Wireless Fidelity）是目前广泛使用的一种无线网络技术，它通过无线电波将有线网络信号转换为无线信号，使支持 Wi-Fi 的设备如电脑、手机、PDA 等能够接收并连接网络。使用 Wi-Fi 的设备在无线信号覆盖范围内可以无需通过移动或联通的数据网络上网，从而节省数据流量费用。

Wi-Fi 技术包含在无线局域网（WLAN）的范畴内，其核心是确保设备之间的兼容性和互操作性。Wi-Fi 联盟（Wi-Fi Alliance）是一个维护和推广 Wi-Fi 标准的组织，负责对产品进行 Wi-Fi 认证以确保其符合 IEEE 802.11 系列的标准。这些标准定义了无线网络的通信协议，使得不同制造商生产的设备能够相互通信。

在 Wi-Fi 网络的架设中，通常需要无线网卡和接入点（AP，Access Point），也称为无线访问接入点或桥接器。AP 在网络中充当无线工作站与有线局域网络之间的桥梁，位于媒体存取控制层（MAC）。简单的无线网络可以不使用 AP，通过每台电脑装配无线网卡直接建立对等网络（peer-to-peer network），以分享网

络资源，其成本和复杂性远低于传统有线网络。

在 Wi-Fi 覆盖区域内，一个无线路由器可以为多个设备提供网络连接服务，如果连接到互联网线路，则该无线路由器也被称作热点（Hotspot），为周围设备提供互联网接入服务。通过这种方式，Wi-Fi 技术极大地方便了日常的网络使用，无论是在家庭、办公室还是公共场所。

**二、WIFI 协议**

Wi-Fi 的主要协议是 IEEE 802.11，这是一个定义无线局域网通信标准的系列，由电气和电子工程师协会（IEEE）制定。IEEE 802.11 规定了无线网络设备应如何进行通信以确保互操作性和兼容性。以下是一些关于 IEEE 802.11 标准中定义的主要任务和服务的介绍。

1. 分配系统的任务
   - 联接（Association）：联接是无线设备（如笔记本电脑、智能手机）与无线网络（通过接入点，AP）建立连接的过程。这是设备加入网络开始通信的首步。
   - 结束联接（Disassociation）：当设备需要断开与无线网络的连接时，进行的操作。这可能是由于移动到另一个网络覆盖区或关闭设备引起。
   - 分配（Distribution）：分配是指在网络内部路由数据包的过程，确保数据从源正确地发送到目的地。
   - 集成（Integration）：在使用多种网络技术时，如将无线网络与有线网络结合，集成服务负责不同网络类型之间的数据传递和转换。
   - 再联接（Reassociation）：再联接是在无线设备从一个接入点移动到另一个接入点时，重新建立网络连接的过程。这是实现无线网络中的漫游功能的关键。
2. 站点的任务
   - 鉴权（Authentication）：在无线设备可以加入网络之前，必须通过身份验证过程。这是安全机制的一部分，防止未授权的访问。
   - 结束鉴权（Deauthentication）：当需要终止设备的网络访问权限时，执行的操作，通常是因为安全问题。
   - 隐私（Privacy）：隐私任务涉及加密技术，用于保护用户数据免受未经

授权的访问和监听。

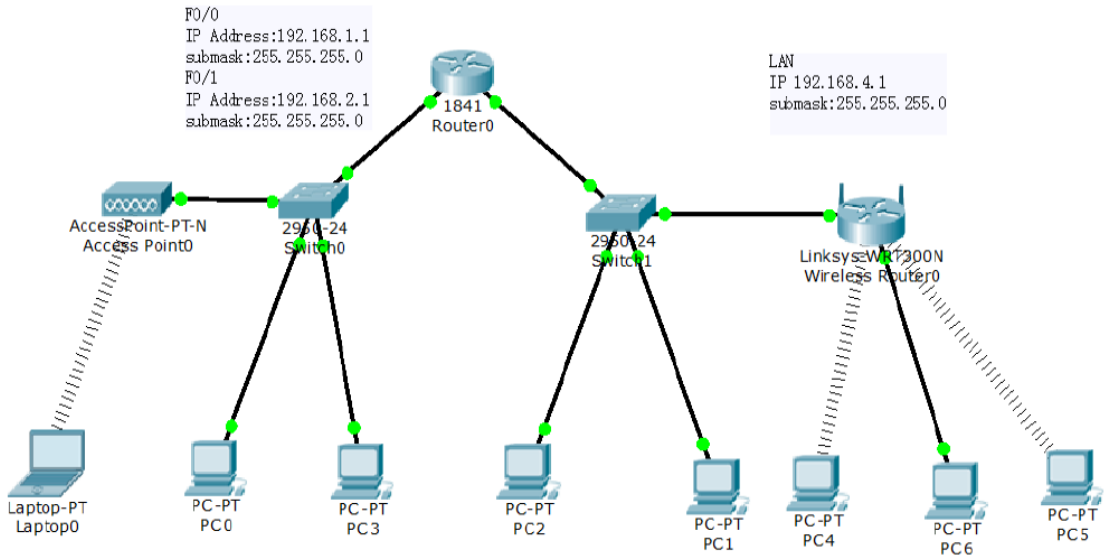
- MAC 数据传输（MSDU delivery）：MAC 子层数据单元（MSDU）传输是网络中进行数据帧传输的基本单位。这确保了有效和可靠的数据传输。

**【实验设备】**

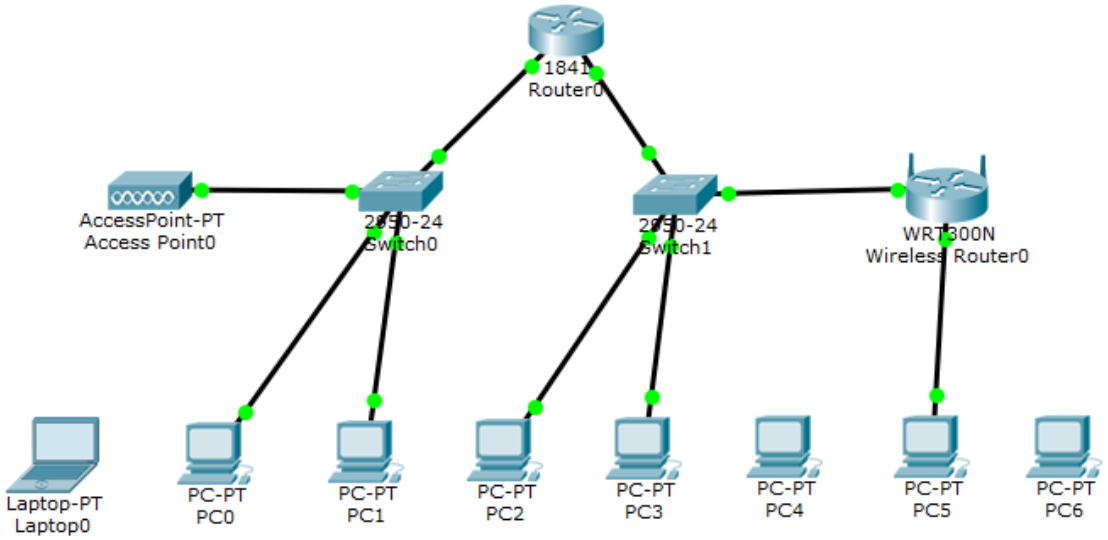
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。



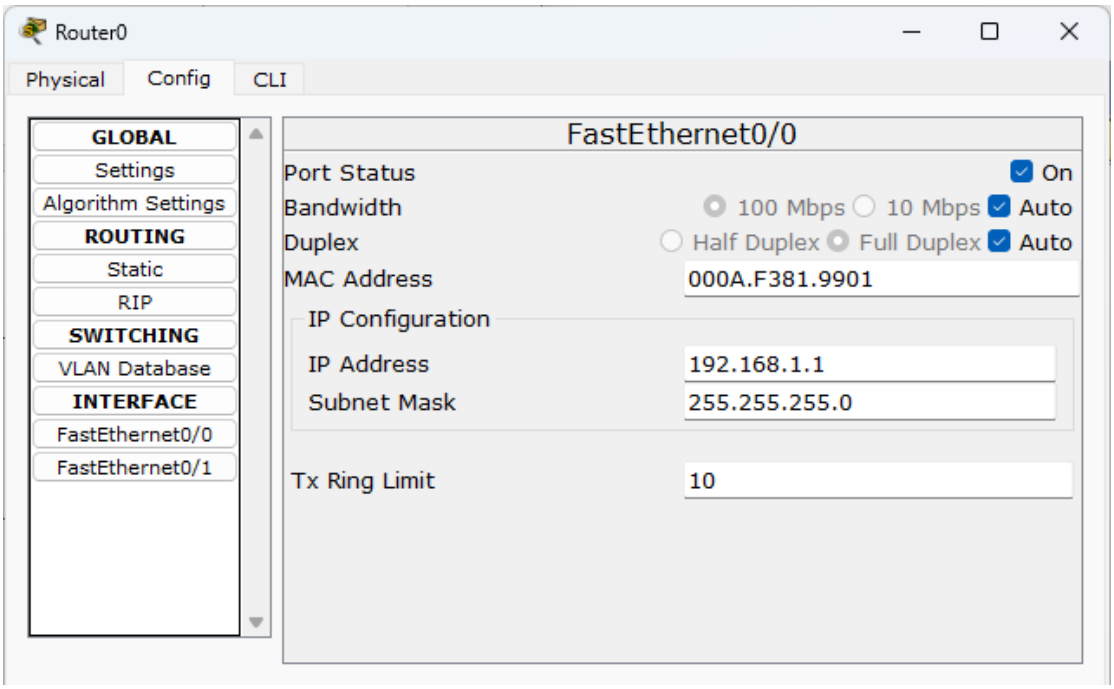

2. 启动 Cisco Packet Tracer，按照上图连接网络。

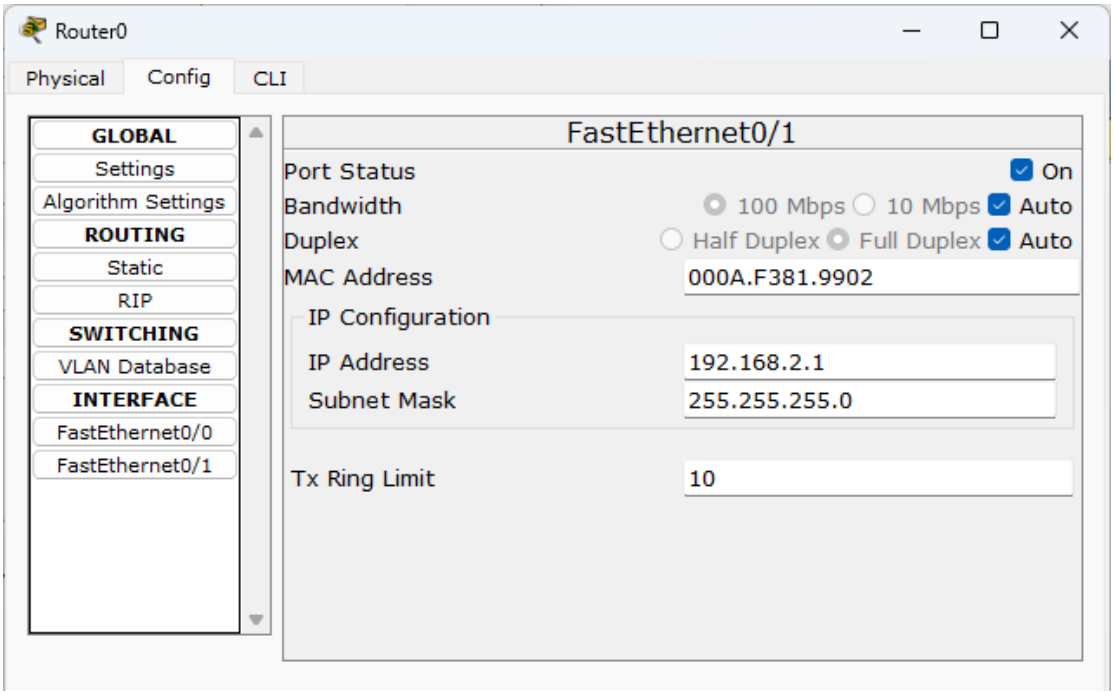



3. 配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也

可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```




4. 在路由器 Router0 配置 DHCP。

- 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

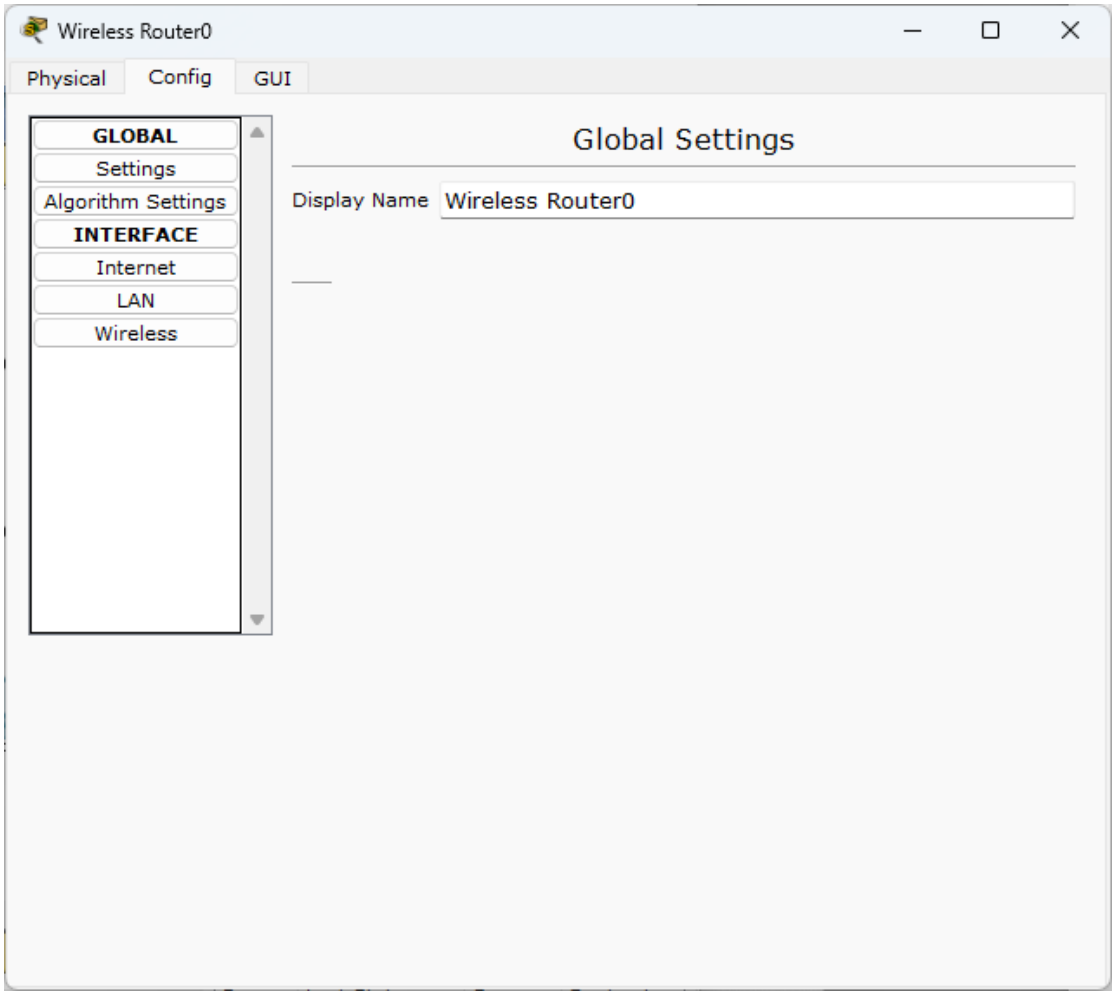
```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

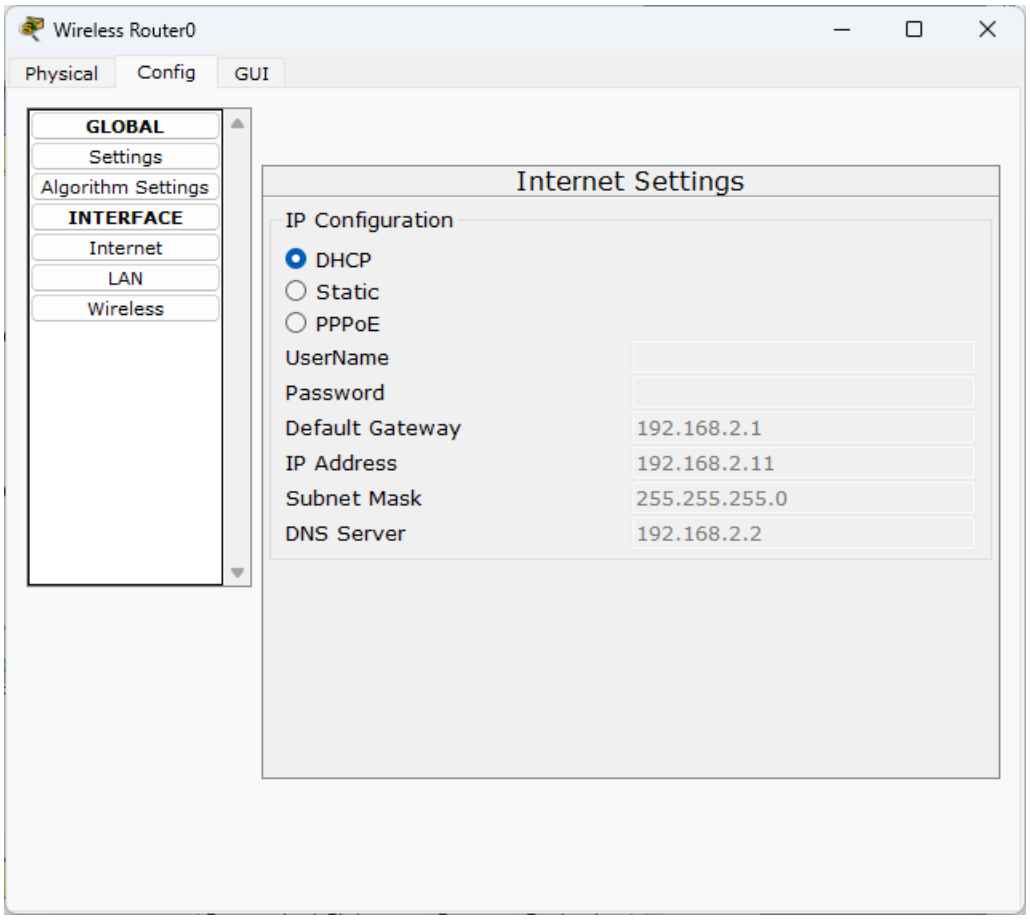
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

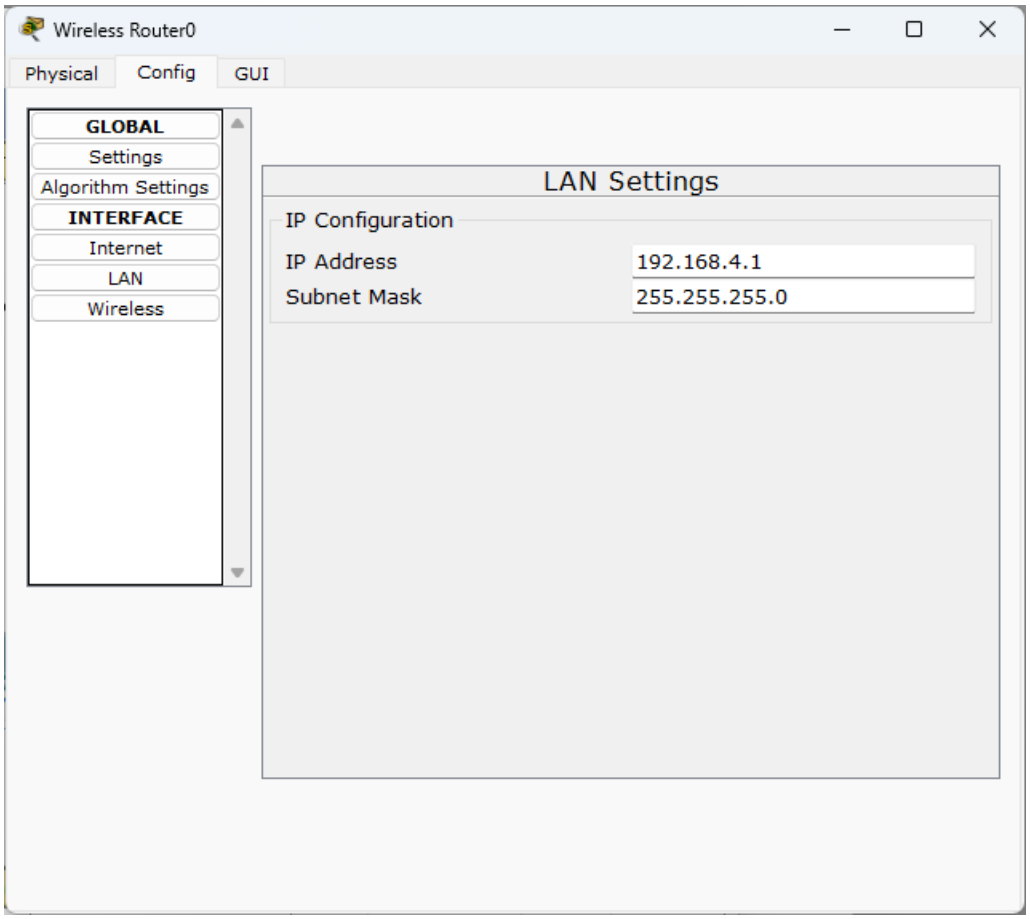
```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

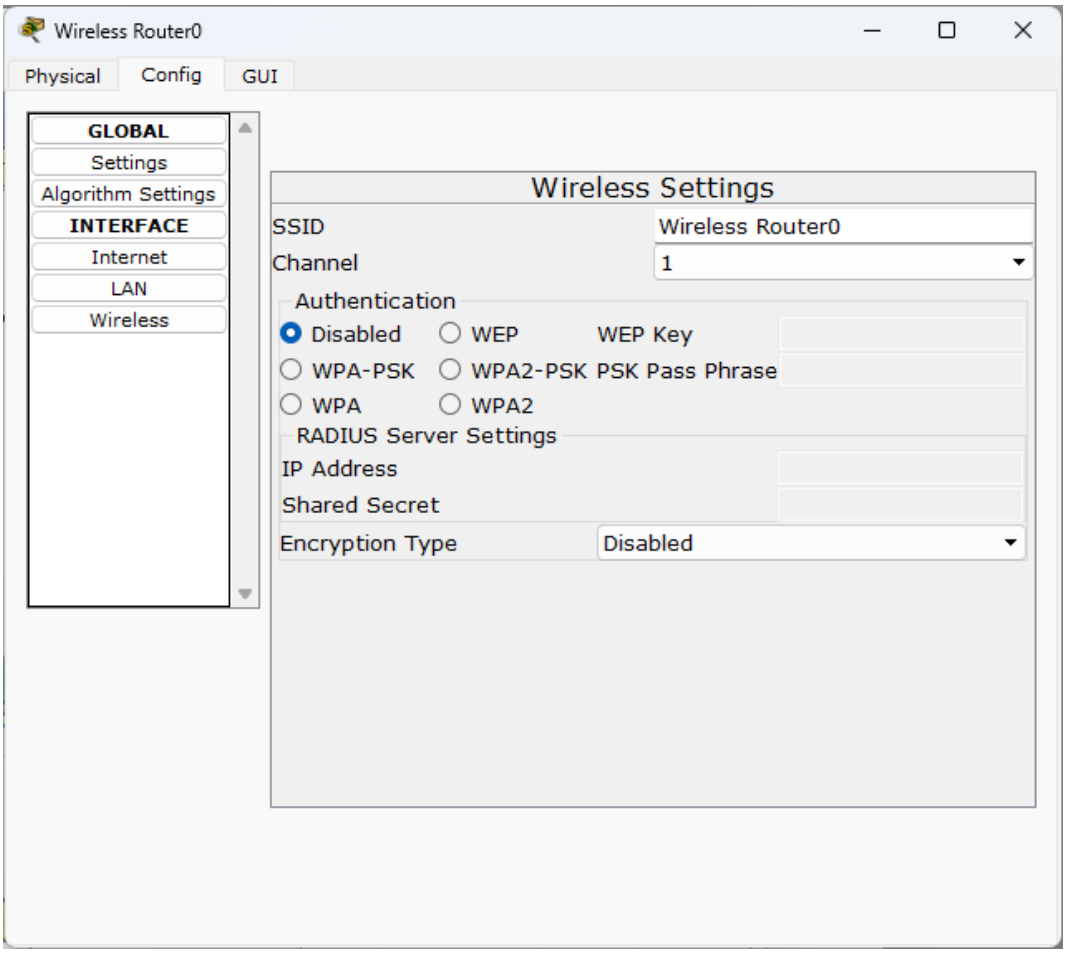
5. 验证主机之间的互通性。

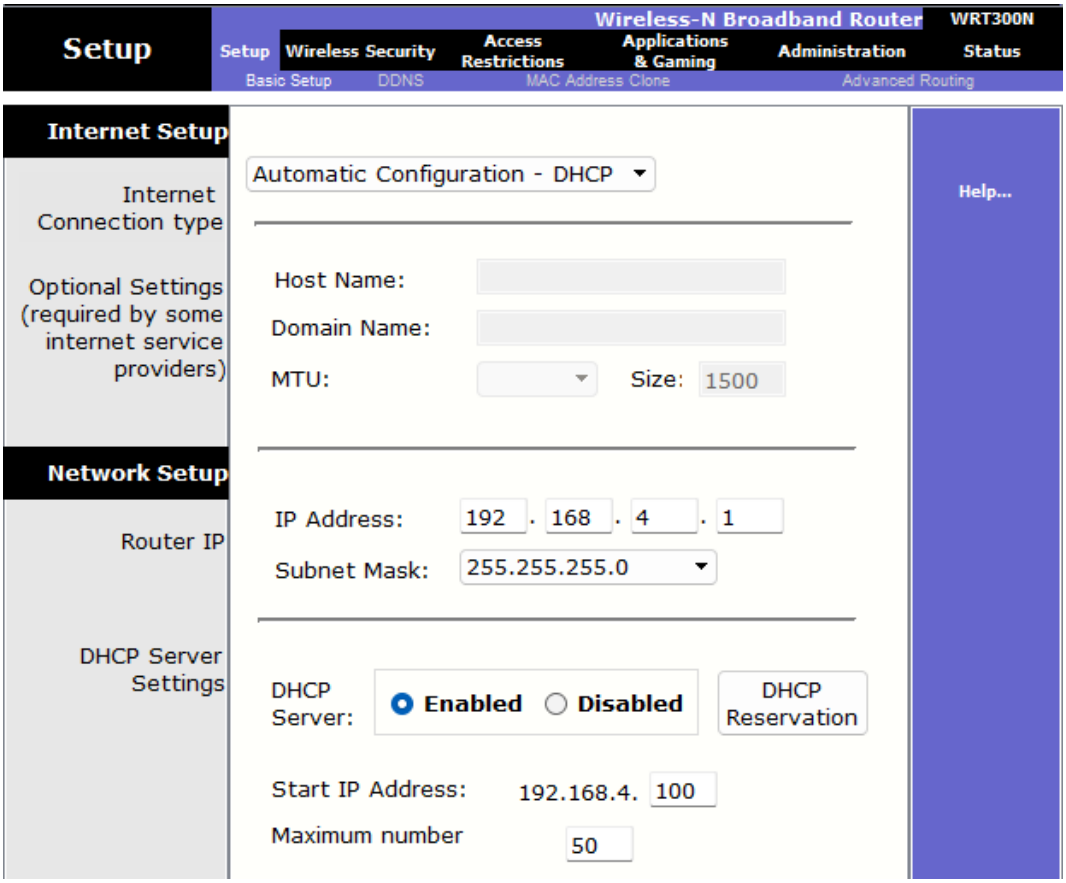
6. 配置 Wireless Router0。

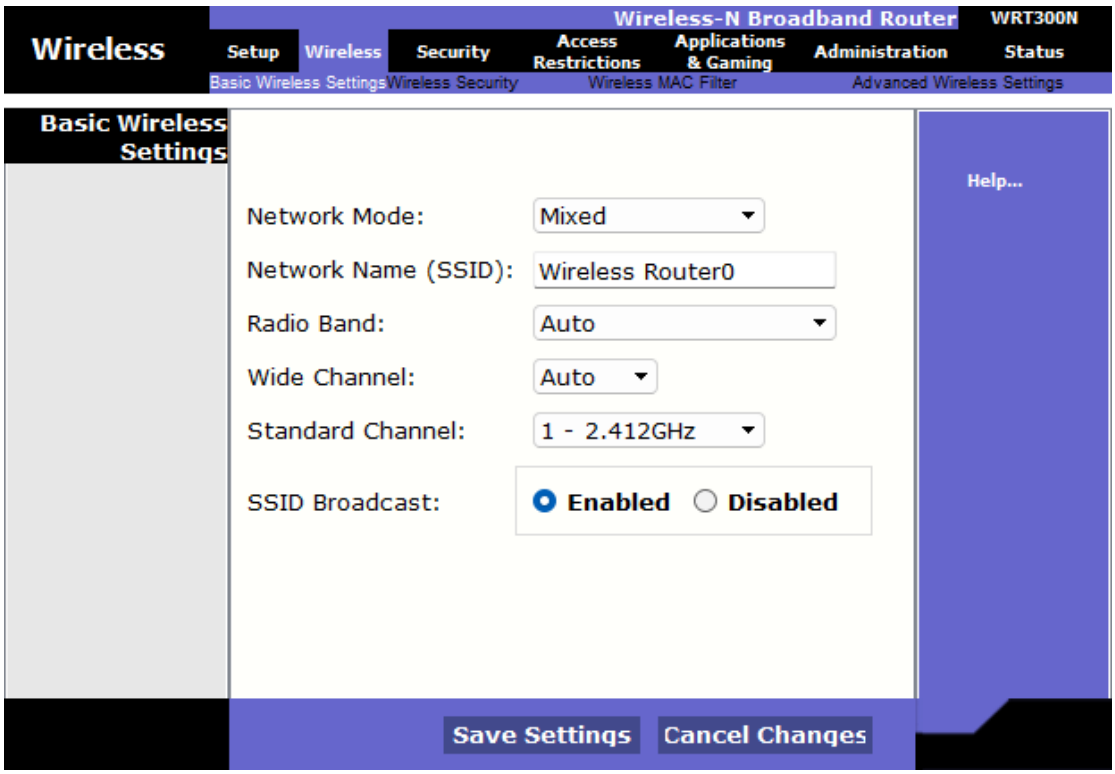



Wireless Router0
Physical
Config
GUI
GLOBAL
Settings
Algorithm Settings
INTERFACE
Internet
LAN
Wireless
Internet Settings
IP Configuration
DHCP
Static
PPPoE
UserName
Password
Default Gateway
192.168.2.1
IP Address
192.168.2.11
Subnet Mask
255.255.255.0
DNS Server
192.168.2.2

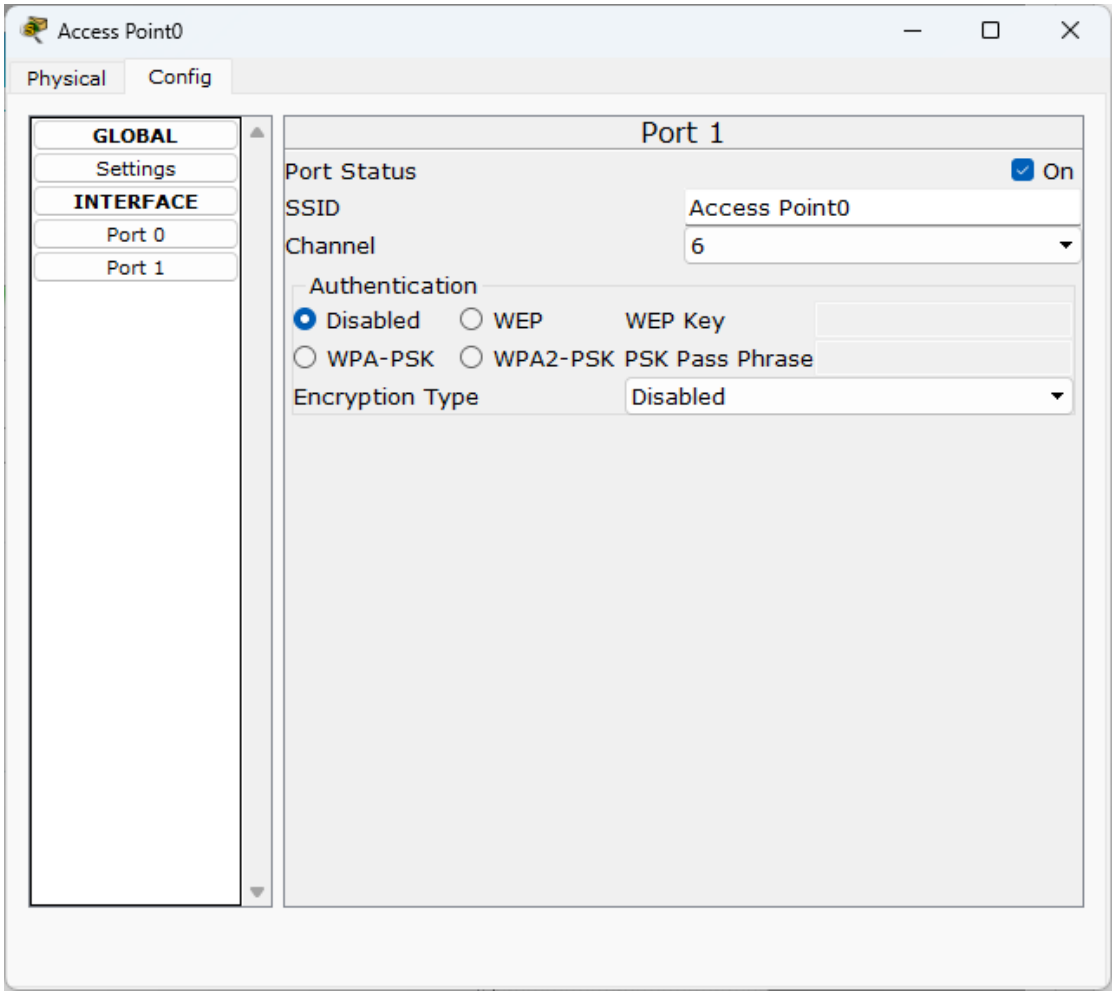

Wireless Router0
Physical
Config
GUI
GLOBAL
Settings
Algorithm Settings
INTERFACE
Internet
LAN
Wireless
LAN Settings
IP Configuration
IP Address
192.168.4.1
Subnet Mask
255.255.255.0


Wireless Router0
Physical
Config
GUI
GLOBAL
Settings
Algorithm Settings
INTERFACE
Internet
LAN
Wireless
Wireless Settings
SSID
Wireless Router0
Channel
1
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
WPA
WPA2
RADIUS Server Settings
IP Address
Shared Secret
Encryption Type
Disabled

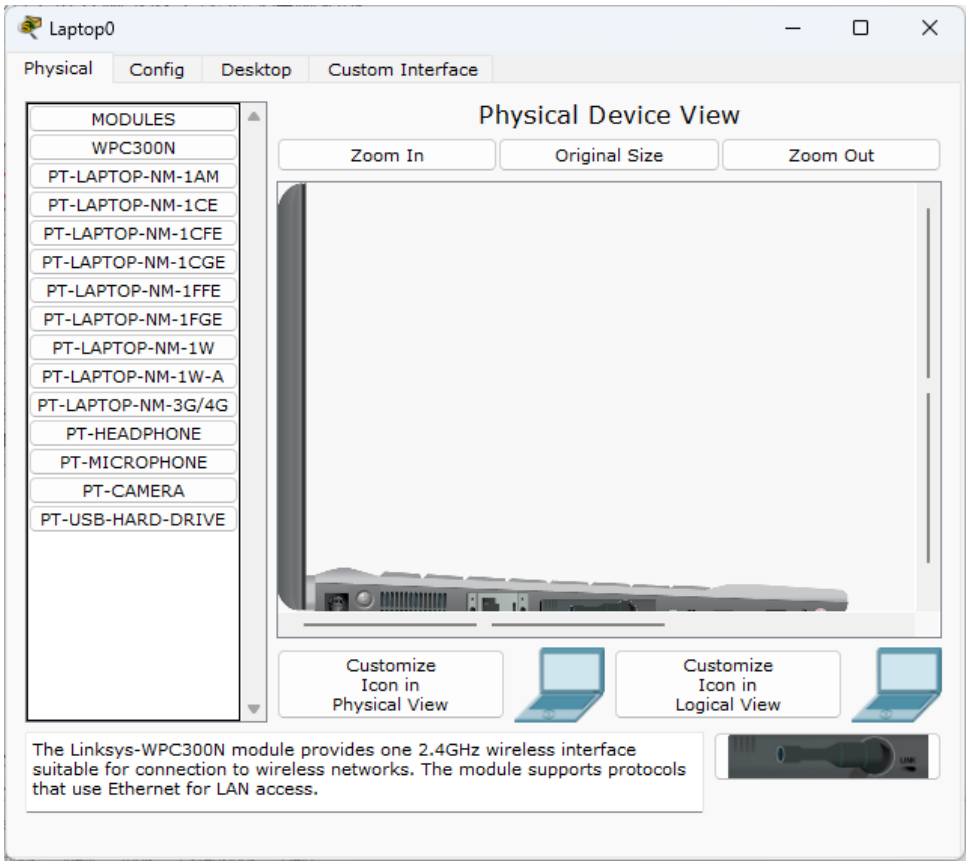

Setup
Wireless-N Broadband Router
WRT300N
Setup
Wireless Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
Internet Setup
Internet Connection type
Automatic Configuration - DHCP
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size:
1500
Help...
Network Setup
Router IP
IP Address:
192
168
4
1
Subnet Mask:
255.255.255.0
DHCP Server Settings
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address:
192.168.4.
100
Maximum number
50

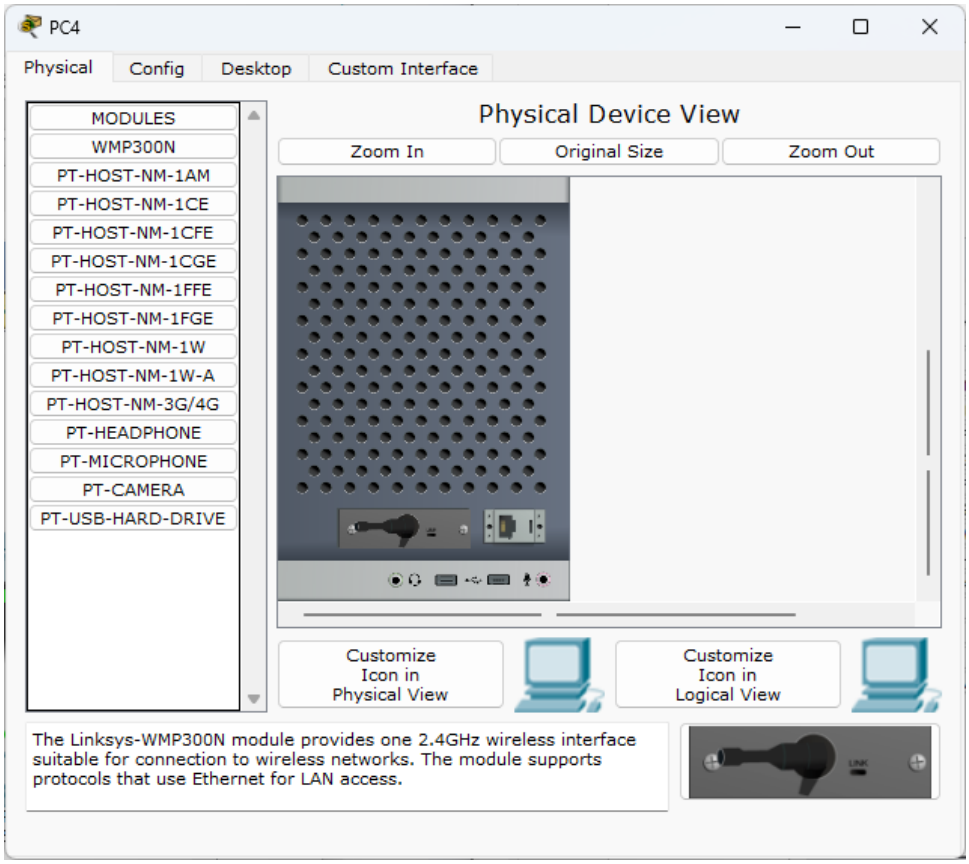


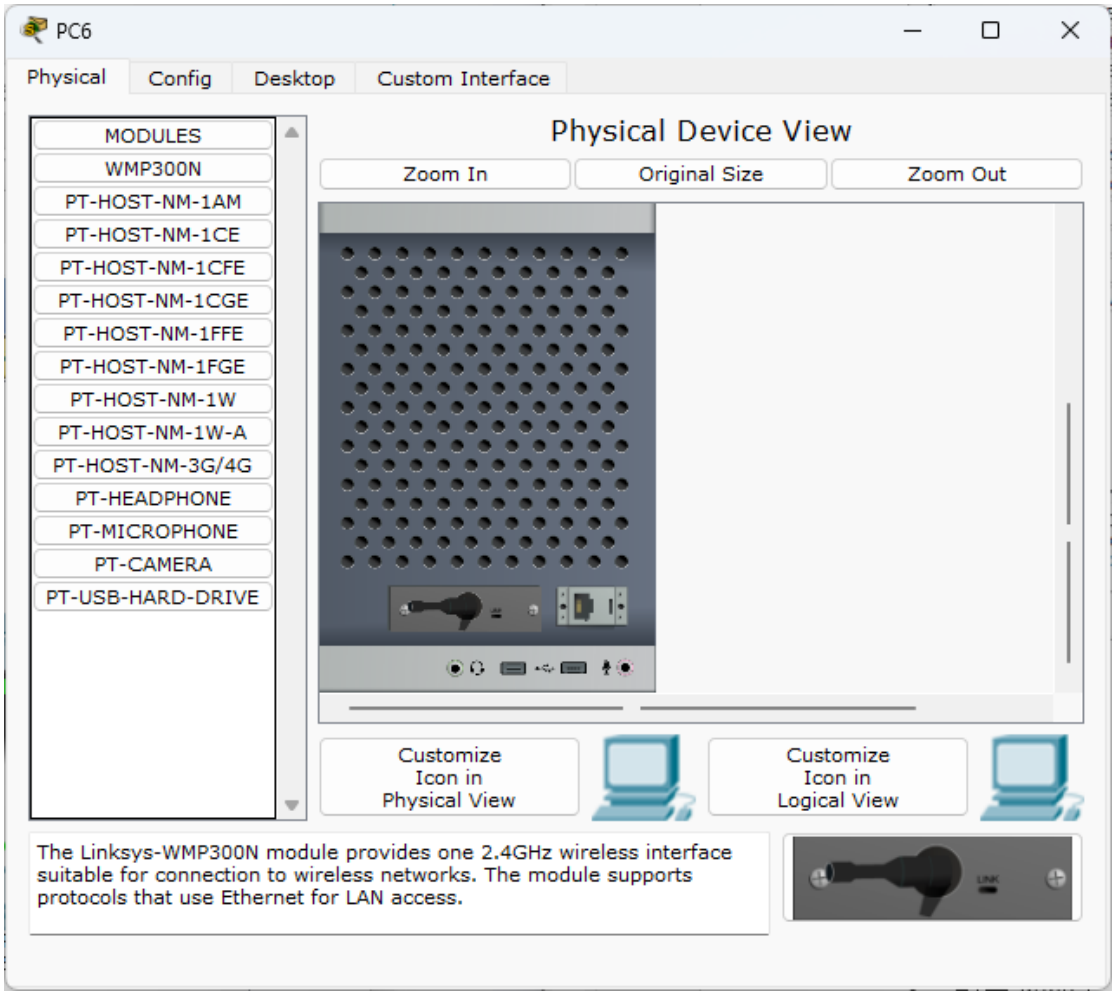

7. 配置 Access Point0。



8. 为 Laptop0、PC4、PC6 安装 WPC300N。

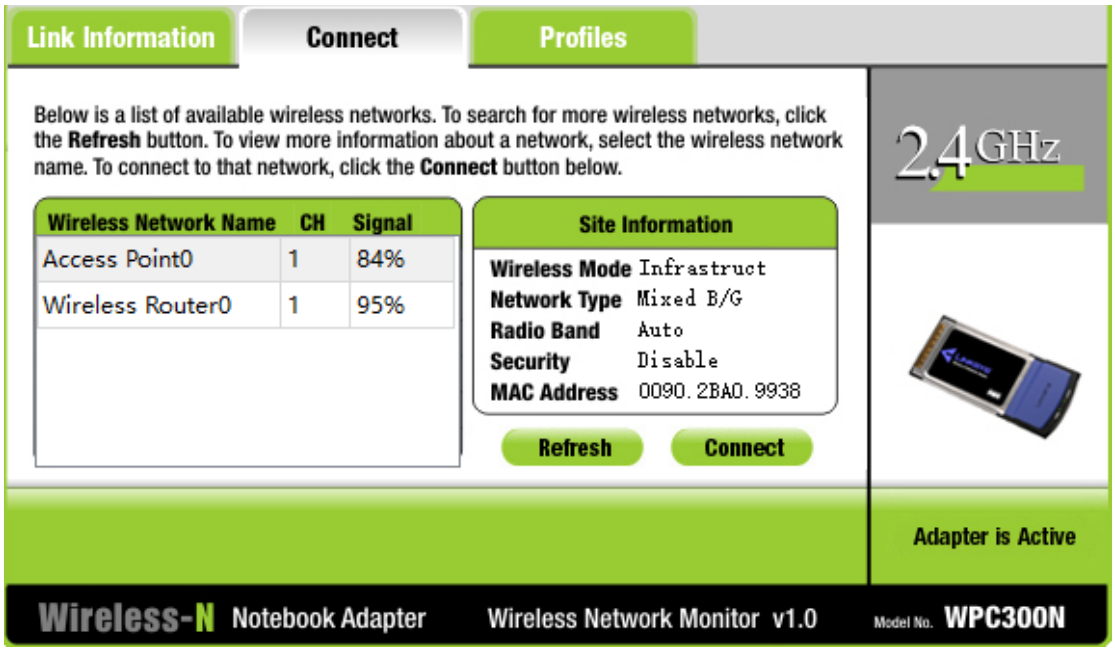


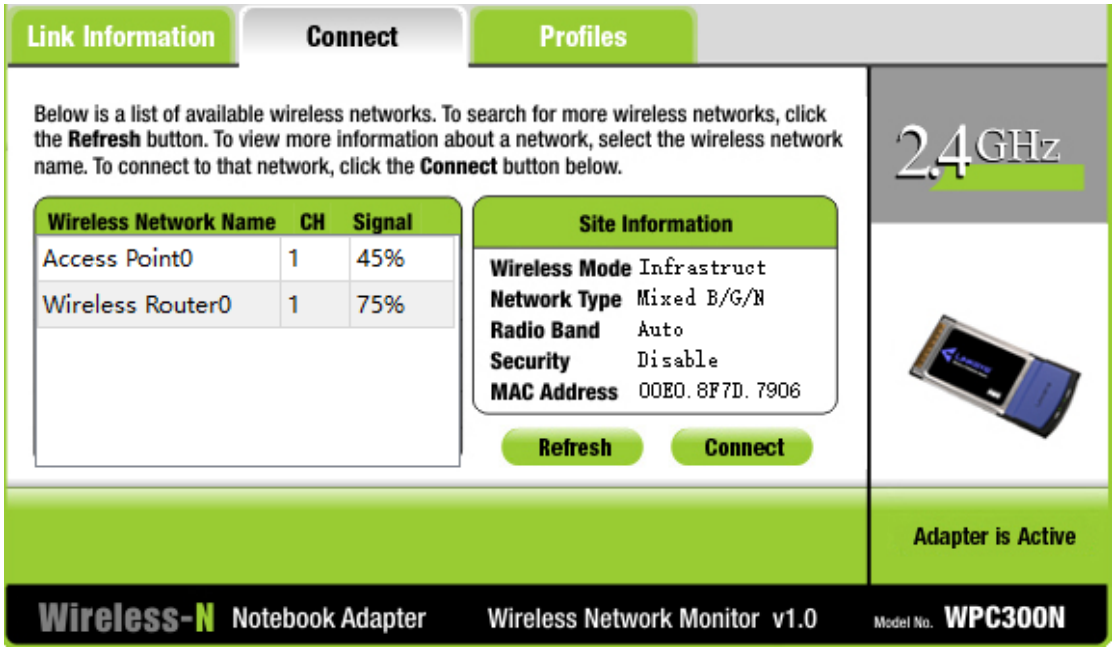



9. 在设备中打开“PC Wireless”。将 Laptop0 连接到 Access Point0 上，将 PC4、PC6 连接到 Wireless Router0 上。

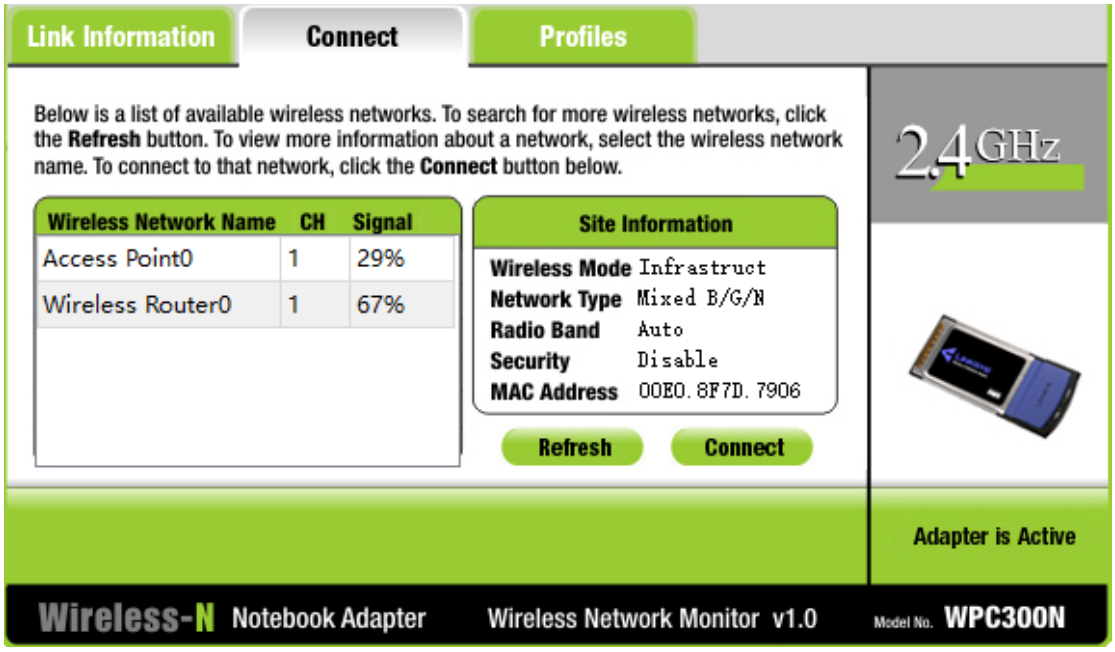
- 将 Laptop0 连接到 Access Point0 上。



- 将 PC4 连接到 Wireless Router0 上。




- 将 PC6 连接到 Wireless Router0 上。




10. Laptop0 连接到 Access Point0 上后，PC4、PC6 连接到 Wireless Router0 上后，可以观察到无线网络连接成功。

11. 配置无线路由器相关密码进行测试。

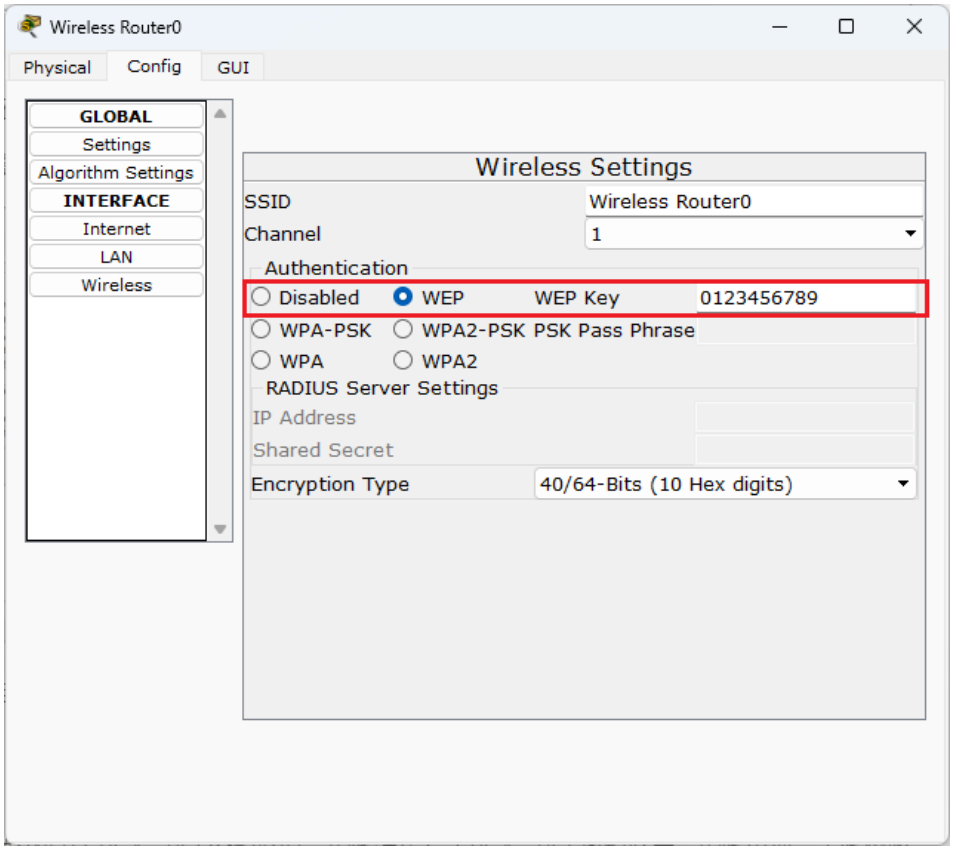
    11.1 为 Wireless Router0 配置 WEP 无线保护协议以及相应的密码。

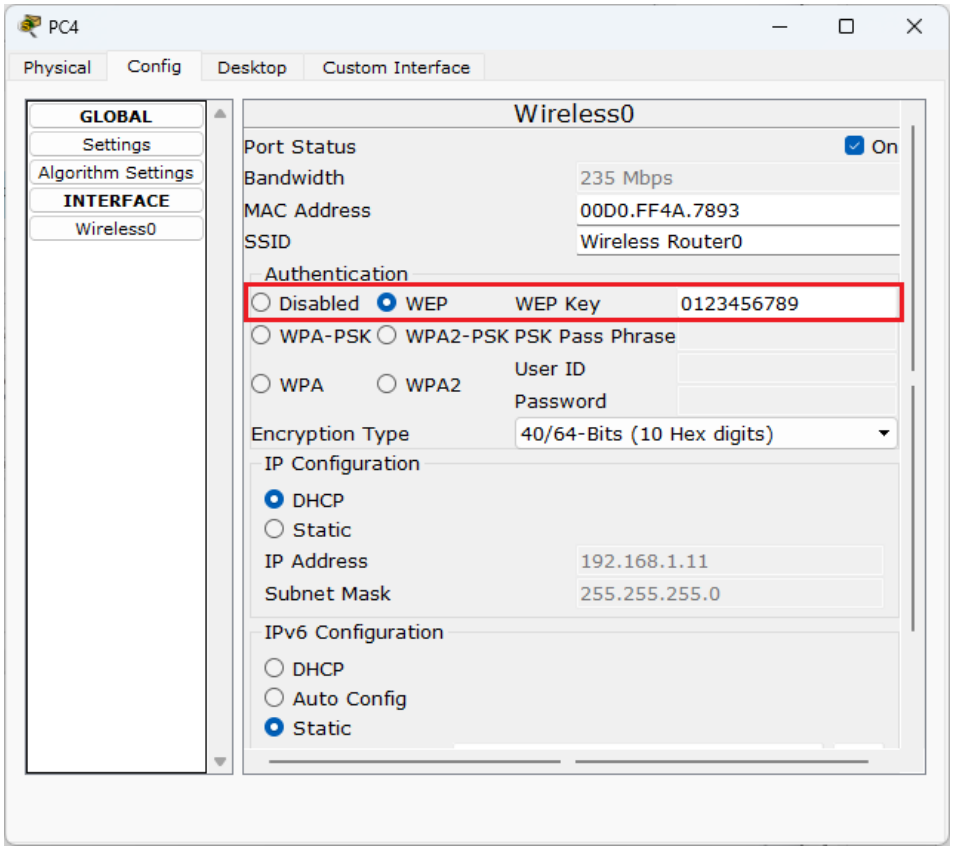
    11.2 为 PC4 配置 WEP 无线保护协议以及相应的密码。

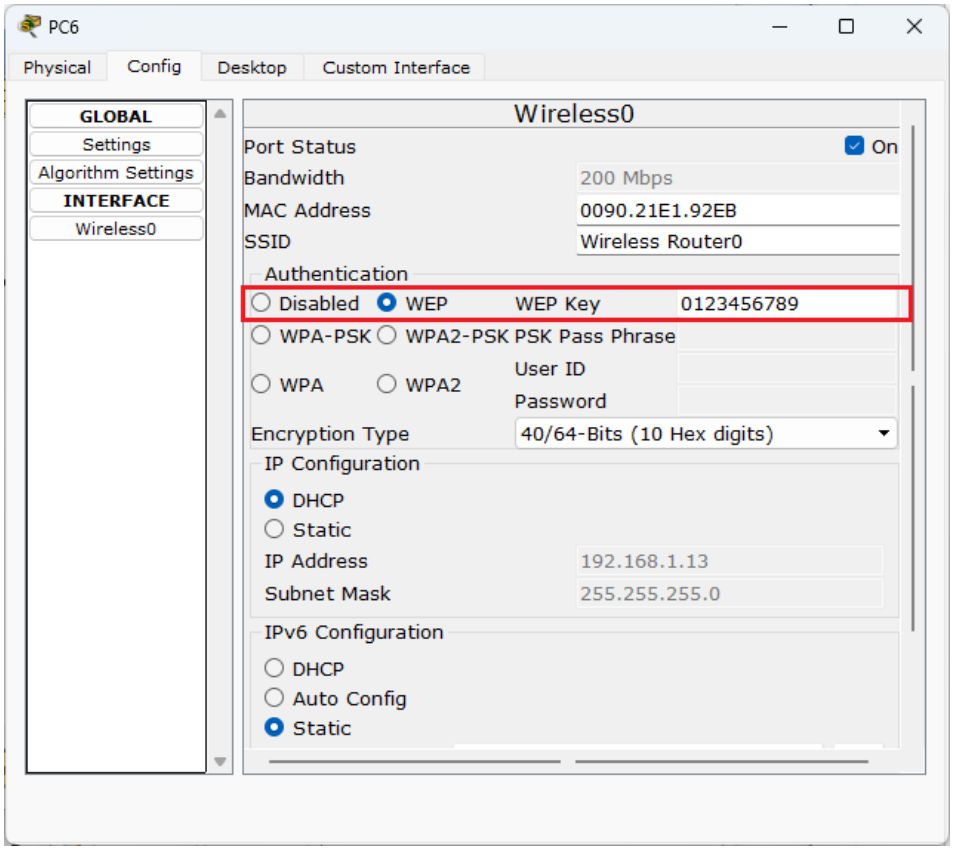
    11.3 将 PC4 连接到 Wireless Router0 上。

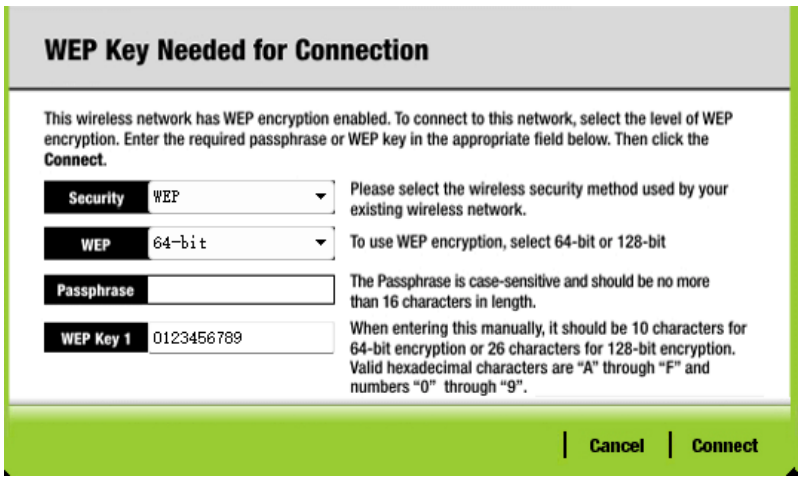
11.4 为 PC6 配置 WEP 无线保护协议以及相应的密码。

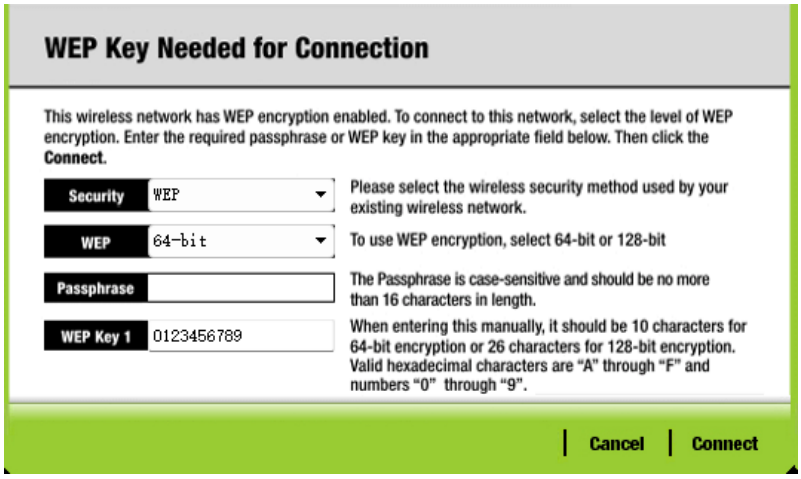
11.5 将 PC6 连接到 Wireless Router0 上。




PC6
Physical
Config
Desktop
Custom Interface
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Wireless0
Port Status
On
Bandwidth
200 Mbps
MAC Address
0090.21E1.92EB
SSID
Wireless Router0
Authentication
Disabled
WEP
WEP Key
0123456789
WPA-PSK
WPA2-PSK
PSK Pass Phrase
User ID
WPA
WPA2
Password
Encryption Type
40/64-Bits (10 Hex digits)
IP Configuration
DHCP
Static
IP Address
192.168.1.13
Subnet Mask
255.255.255.0
IPv6 Configuration
DHCP
Auto Config
Static


WEP Key Needed for Connection
This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then click the Connect.
Security
WEP
Please select the wireless security method used by your existing wireless network.
WEP
64-bit
To use WEP encryption, select 64-bit or 128-bit
Passphrase
The Passphrase is case-sensitive and should be no more than 16 characters in length.
WEP Key 1
0123456789
When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".
Cancel
Connect


WEP Key Needed for Connection
This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then click the Connect.
Security
WEP
Please select the wireless security method used by your existing wireless network.
WEP
64-bit
To use WEP encryption, select 64-bit or 128-bit
Passphrase
The Passphrase is case-sensitive and should be no more than 16 characters in length.
WEP Key 1
0123456789
When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".
Cancel
Connect

12. 观测各个 PC 机的连通情况（ping 测试）。

**【实验现象】**

1. 配置 DHCP 后，验证主机之间的互通性， 左右两边的 PC 机相互进行 ping 测试，均成功。

- PC0 ping PC1、PC2、PC3：

```
Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.2.12 with 32 bytes of data:

Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 192.168.2.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.14: bytes=32 time=1ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC1 ping PC0、PC2、PC3：

```
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
Pinging 192.168.2.12 with 32 bytes of data:

Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 192.168.2.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.14: bytes=32 time=1ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- PC2 ping PC0、PC1、PC3：

```
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

```
Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.2.14 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.14: bytes=32 time=1ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127
Reply from 192.168.2.14: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.14:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

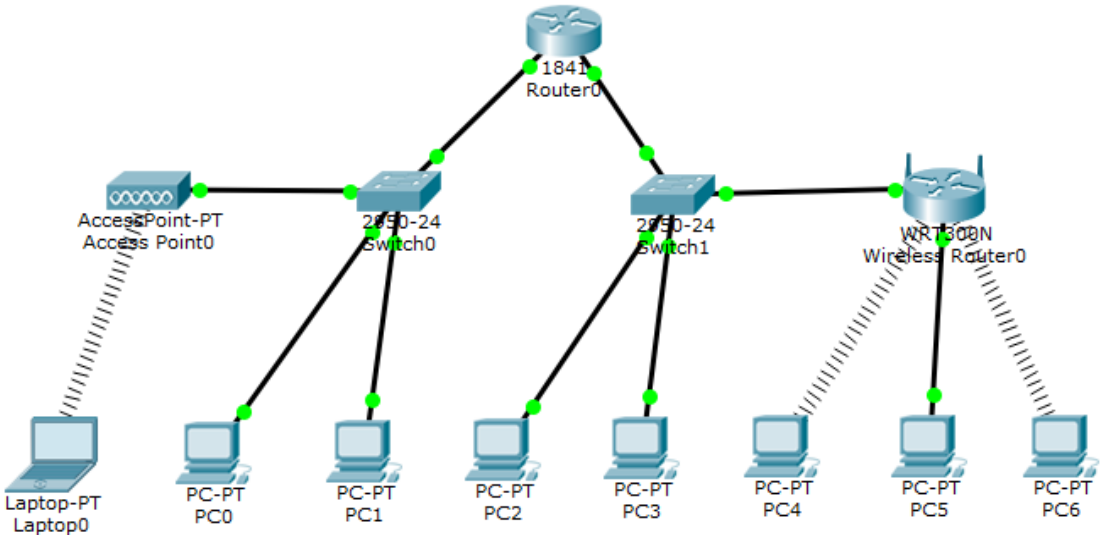
- PC3 ping PC0、PC1、PC2：

```
Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=3ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

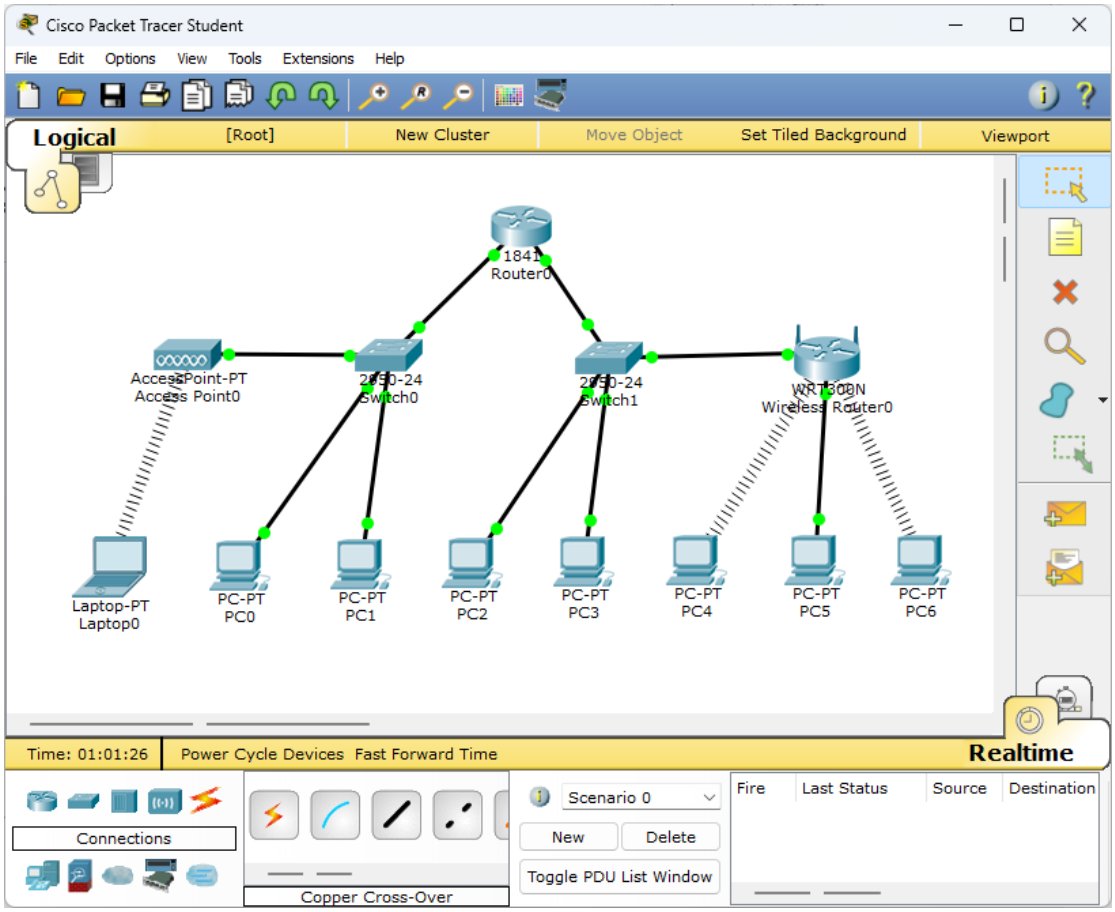
```
Pinging 192.168.1.14 with 32 bytes of data:

Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=0ms TTL=128
Reply from 192.168.1.14: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.2.12 with 32 bytes of data:

Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127
Reply from 192.168.2.12: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Laptop0 连接到 Access Point0 上后，PC4、PC6 连接到 Wireless Router0 上后，可以观察到无线网络连接成功。




3. 配置无线路由器相关密码进行测试，将 PC4 和 PC6 连接到 Wireless Router0 上，可以观察到无线网络连接成功。




4. 观测各个 PC 机的连通情况（ping 测试）。

- 外界 PC 机无法 ping 到通过无线网络连接的 PC 机。

```
Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- 通过无线网络连接的 PC 机可以 ping 到外界 PC 机。

```
Pinging 192.168.1.13 with 32 bytes of data:

Reply from 192.168.1.13: bytes=32 time=36ms TTL=128
Reply from 192.168.1.13: bytes=32 time=14ms TTL=128
Reply from 192.168.1.13: bytes=32 time=12ms TTL=128
Reply from 192.168.1.13: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 36ms, Average = 19ms
```

- 通过无线网络连接的 PC 机可以相互 ping。

```
Pinging 192.168.1.13 with 32 bytes of data:

Reply from 192.168.1.13: bytes=32 time=36ms TTL=128
Reply from 192.168.1.13: bytes=32 time=14ms TTL=128
Reply from 192.168.1.13: bytes=32 time=12ms TTL=128
Reply from 192.168.1.13: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 36ms, Average = 19ms
```

- 其他的 ping 命令均成功连通。

```
Pinging 192.168.1.13 with 32 bytes of data:

Reply from 192.168.1.13: bytes=32 time=36ms TTL=128
Reply from 192.168.1.13: bytes=32 time=14ms TTL=128
Reply from 192.168.1.13: bytes=32 time=12ms TTL=128
Reply from 192.168.1.13: bytes=32 time=15ms TTL=128

Ping statistics for 192.168.1.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 36ms, Average = 19ms
```

**【分析讨论】**

**一、如果再接入一台路由器如何配置**

当在现有网络中再接入一台路由器时，需要注意避免 IP 地址冲突，并保证正确的路由配置：

1. IP 地址选择：选择一个未被现有网络使用的 IP 段，如 192.168.5.x，确保不会与现有设备冲突。
2. 物理连接：使用串口线或以太网线将两台路由器连接起来。
3. 路由配置：在两台路由器上配置 OSPF 或其他动态路由协议，确保数据可以在新旧路由器之间正确路由。

**二、如果改为静态 IP 地址如何处理**

将网络配置改为使用静态 IP 地址时，需要手动设置每个设备的 IP 地址，并确保路由器与所有设备的网络设置相符：

1. IP 地址规划：为每个设备分配一个唯一的静态 IP 地址，确保地址在子网内并避免冲突。
2. 设备配置：在每个 PC、笔记本及无线设备上手动配置 IP 地址、子网掩码、默认网关及 DNS。
3. 无线设备配置：无线路由器和接入点也需要配置在正确的子网，若有多个子网，需确保主路由器有适当的路由设置以便跨子网通信。

## 三、外界 PC 机无法 ping 到通过无线网络连接的 PC 机的原因

无线路由器位于 192.168.4.0/24 子网，而 DHCP 服务器配置的是 192.168.2.0/24 子网，所以连接到无线路由器的设备无法正确路由，因为它们被分配到了错误的子网。

# 实验 20：IP 电话实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/09 |

**【实验目的】**

1. 理解 IP 电话的基本概念和工作原理：通过实验，学生可以了解 IP 电话（亦称网络电话或 VOIP 电话）是如何利用互联网技术来进行语音通信的。这包括了解语音信号是如何被数字化、压缩编码、通过网络传输、解压缩并还原为声音的基本过程。
2. 掌握 IP 电话的配置和设置：实验将指导学生学习如何配置 Cisco IP 电话和路由器，包括路由器的接口配置、DHCP 配置、电话服务配置等。这些技能是网络工程师在实际工作中常用到的技能。
3. 了解和实施 VOIP 相关的网络协议：学生将通过实验学习和实施多种 VOIP 相关协议，如 SIP（Session Initiation Protocol）和 RTP（Real-time Transport Protocol）。理解这些协议如何协同工作，支持 IP 电话系统的运行。
4. 网络设计与故障排除：学生将规划和设计一个小规模的 IP 电话网络，包括网络地址规划、电话号码配置以及 VLAN 配置。此外，通过实验中的问题解决，学生可以提升网络故障排查和解决问题的能力。
5. 实际操作能力的提升：通过对 Cisco 7960 IP 电话和路由器的实际配置操作，学生不仅能够将理论知识应用于实践，还能增强解决实际网络配置问题的能力。

**【实验原理】**

**一、IP 电话**

IP 电话，即网络电话或 VOIP 电话（Voice Over Internet Protocol），是一种通过互联网来实现语音通信的技术。与传统电话相比，IP 电话具有成本低廉和高度可扩展的特点。其工作原理主要包括以下几个步骤：

1. 声电转换：使用压电陶瓷或类似装置，将声波转换为电信号。
2. 量化采样：通过脉冲编码调制（PCM）等技术，将模拟电信号转换成数字信号。

3. 封包：数字化后的语音信号被组织成帧，按照国际电信联盟（ITU-T）的标准，封装到 RTP（实时传输协议）报文中，进一步封装到 UDP 和 IP 报文中。
4. 传输：通过 IP 网络将 IP 报文从源端发送到目的端。

在 IP 电话系统中，以下几个技术是关键：

- 话音编解码：转换声音与数字信号。
- 回声消除与抑制：改善通话质量，减少干扰。
- 时延控制：确保通话的实时性。
- 去抖动功能（De-jitter）：平滑数据传输，防止数据包到达时间差引起的通话不连贯。

此外，IP 电话支持多种协议，其中最常用的是 H.323 和 SIP（Session Initiation Protocol）。H.323 较旧，而 SIP 则因其灵活性和与 HTTP 的相似性而被广泛采用。SIP 主要负责电话的建立和释放，而实际的语音（及视频）数据则通过 RTP 协议传输。

IP 电话设备的例子包括 CISCO 7960，这是一款可以用于实验和商业用途的设备。通过这些设备，普通电话用户也可以通过网络进行通话，这通常需要通过一个语音网关来实现。

**二、IP 电话配置方法**

配置 Cisco IP 电话，特别是在使用 CISCO 7960 电话机和路由器 2811 配置 CME（Call Manager Express）的环境中，可以按照以下步骤进行：

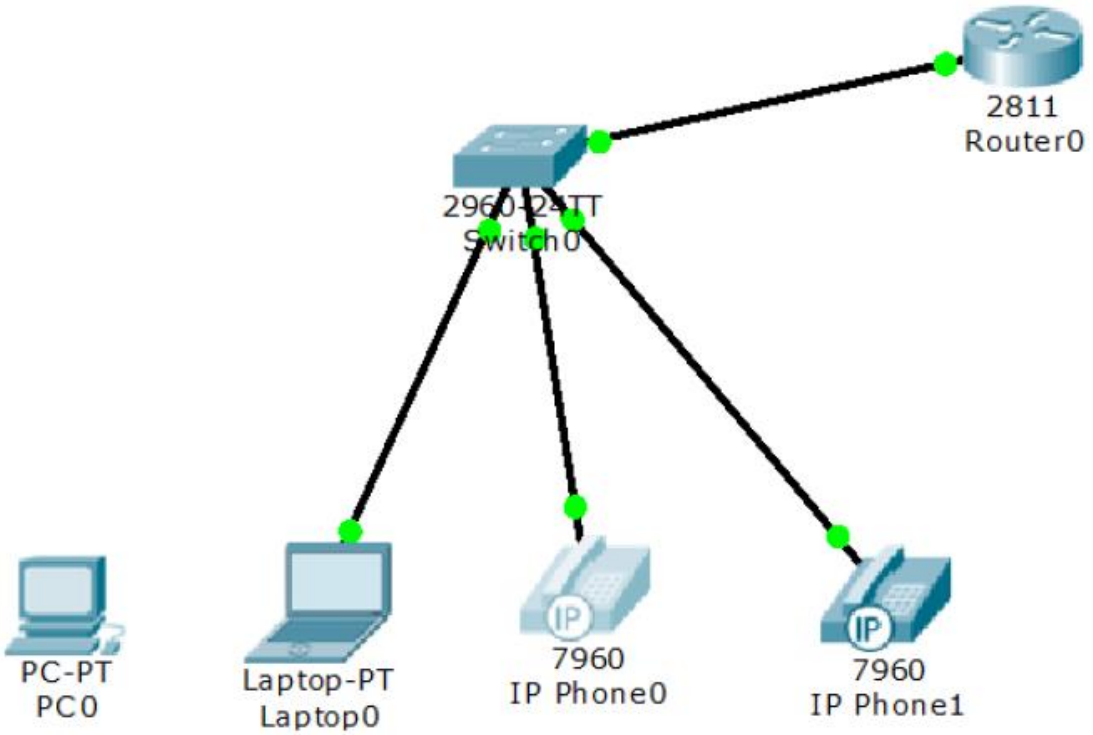
1. 路由器 2811 配置 CME。
2. 使用 Cisco 7960 电话。
3. 设置拨号位长等。
4. 连接 Cisco IP 电话等。

**【实验设备】**

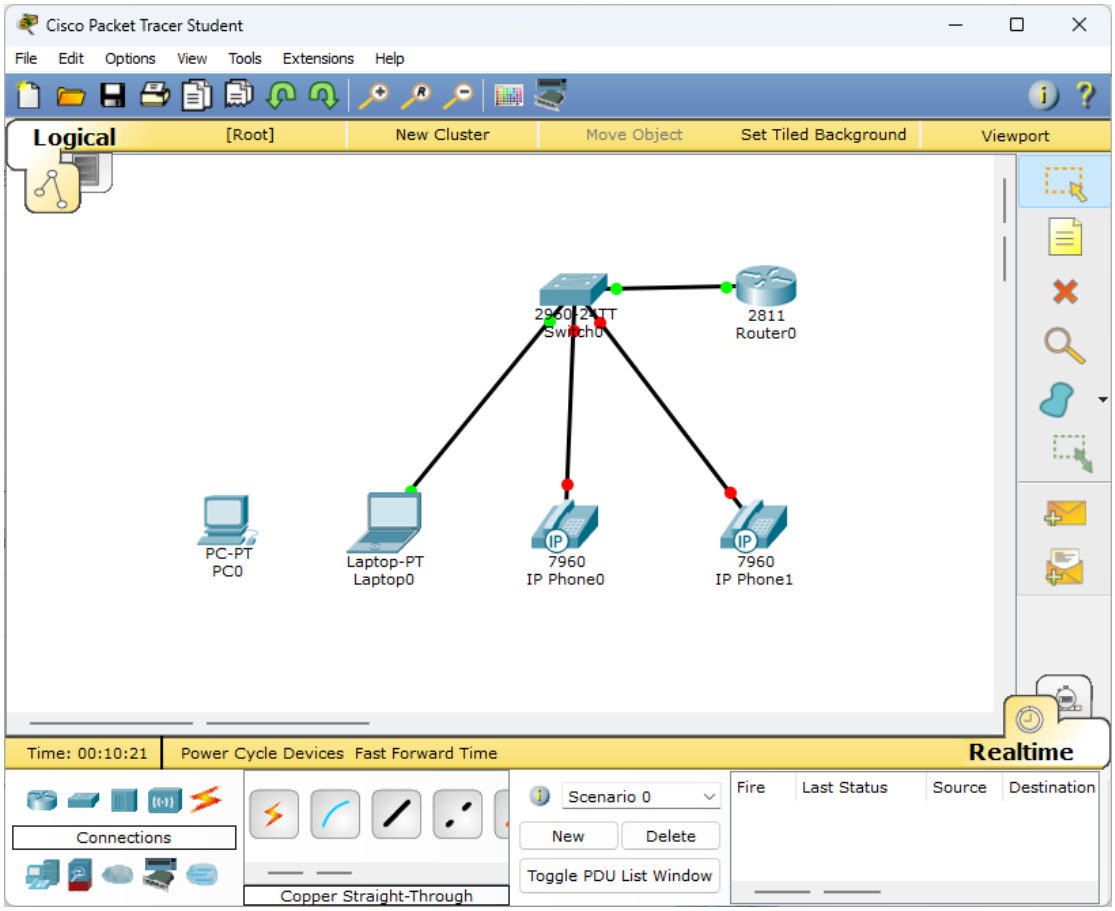
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

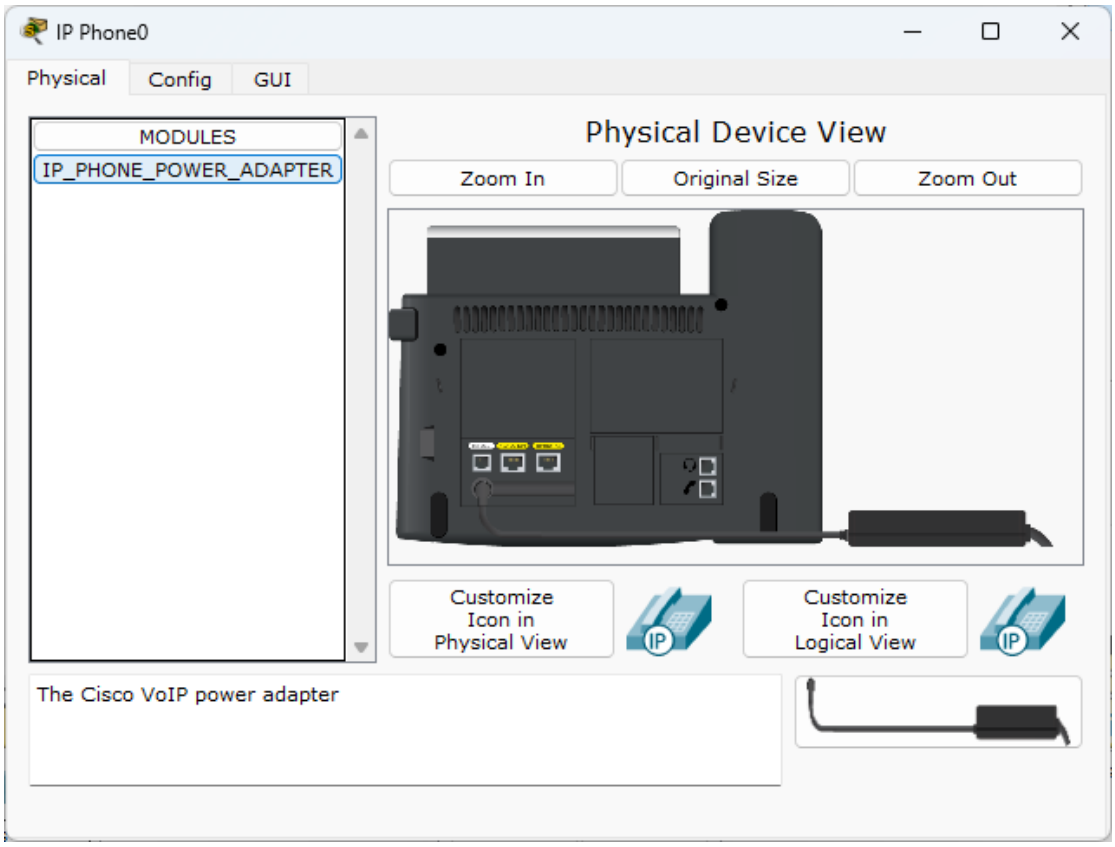
1. 规划网络地址及拓扑图。

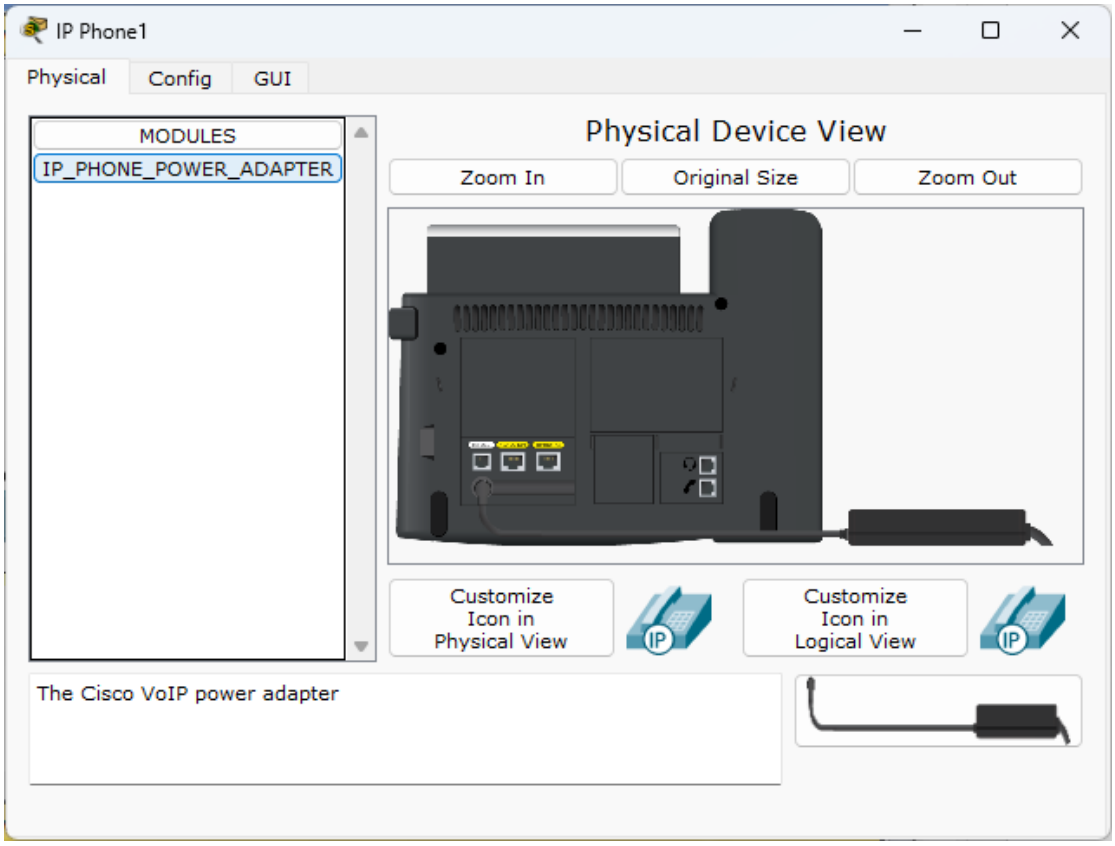


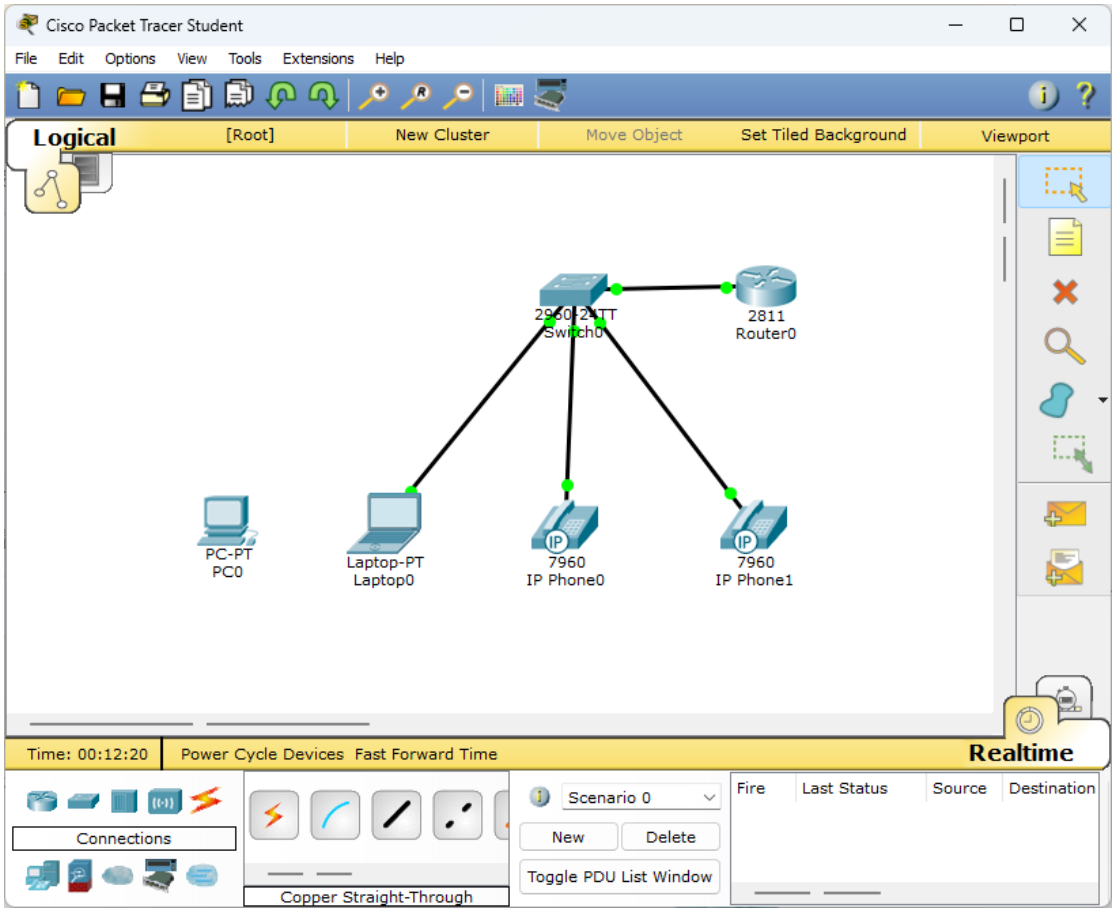

2. 启动 Cisco Packet Tracer，按照上图连接网络。



3. 将 7960 IP Phone0 和 7960 IP Phone1 安装 The Cisco VoIP power adapter，可以观察到连通成功。

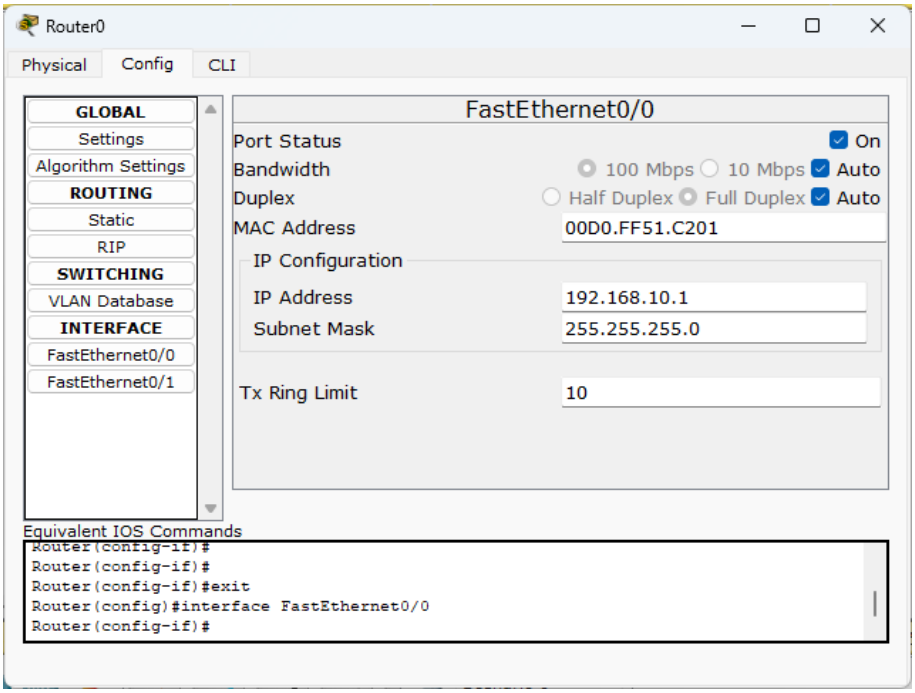





4. 配置路由器 Router0 接口。

```
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
```



5. 配置路由器 Router0 DHCP。

```
ip dhcp pool VOICE
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
option 150 ip 192.168.10.1
```

6. 配置路由器电话服务（CME）。

```
telephony-service
max-dn 5
max-ephones 5
ip source-address 192.168.10.1 port 2000
auto assign 4 to 6
auto assign 1 to 5
```

7. 配置交换机 VLAN。

```
interface range fa0/1 - 5
switchport mode access
switchport voice vlan 1
```

8. 连接一个 Cisco 7960，配置路由器中 IP 电话号码，并确认 IP 电话配置情况。

```
ephone-dn 1
number 54001
```

9. 配置上一步的 54001 就绪后，再连接一个 Cisco 7960，配置路由器中 IP 电话号码，并确认 IP 电话配置情况。

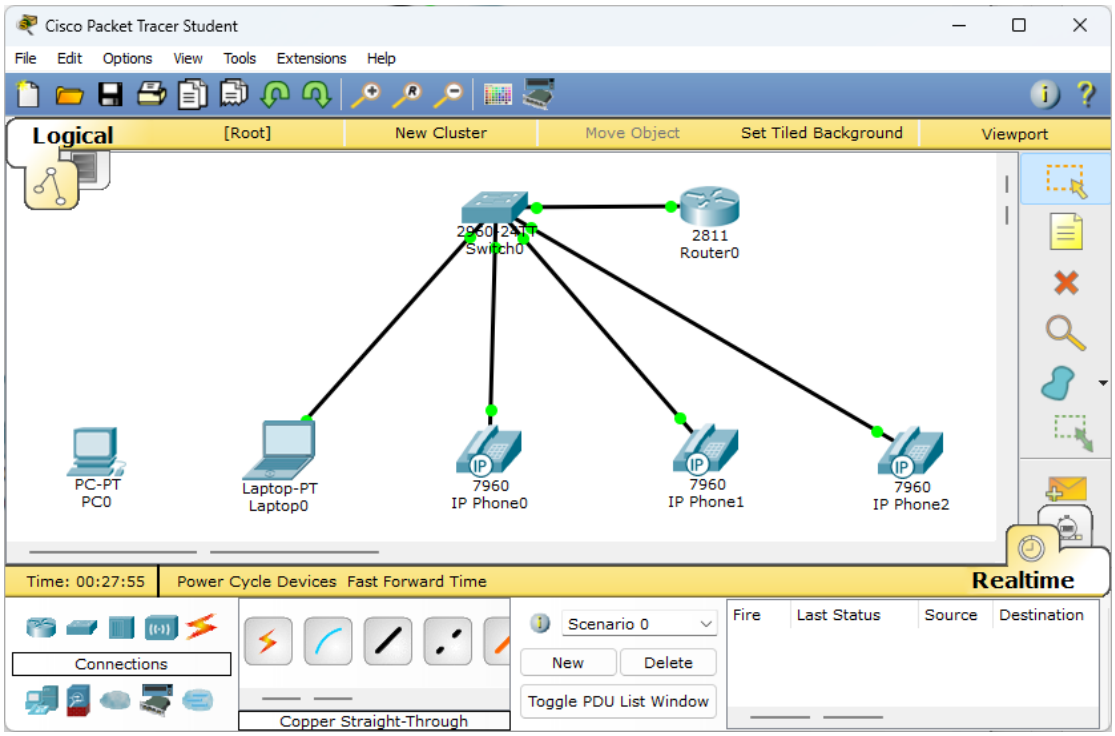
```
ephone-dn 2
number 54002
```

10. 检测两台话机拨号回铃情况。
11. 配置一台电脑，检测电脑与 IP 电话之间能否彼此呼叫。在电脑的 Cisco IP Communicator 中，输入电话号码，点击 Dial 按钮即可拨出电话。

```
ephone-dn 3
number 54004
```

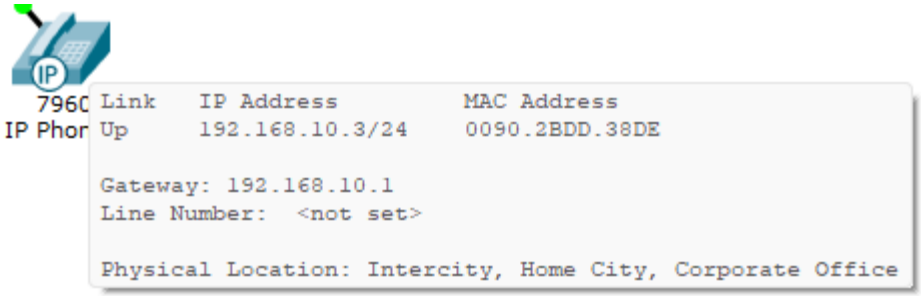
12. 增加一个 Cisco 7960，配置路由器中 IP 电话号码，检测话机之间拨号回铃情况。

```
ephone-dn 4
number 54004
```

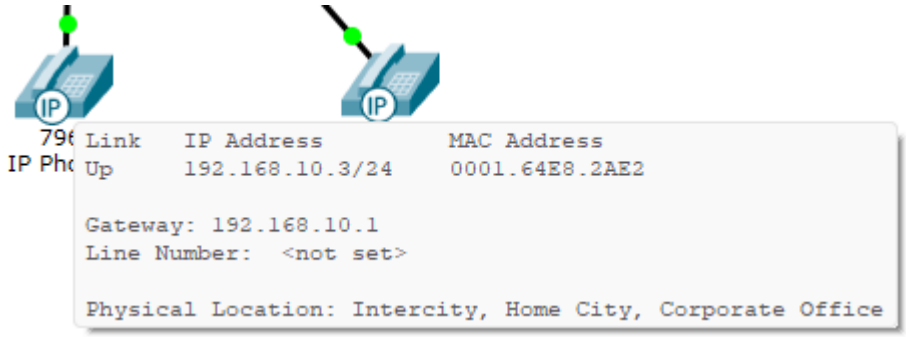



**【实验现象】**

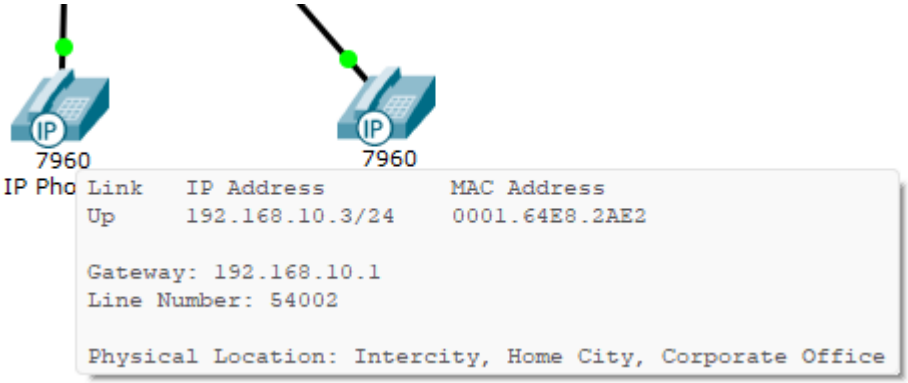
1. 在配置路由器中 IP 电话号码前，查看 IP 电话配置情况。



2. 连接一个 Cisco 7960，配置路由器中 IP 电话号码，并确认 IP 电话配置情况。

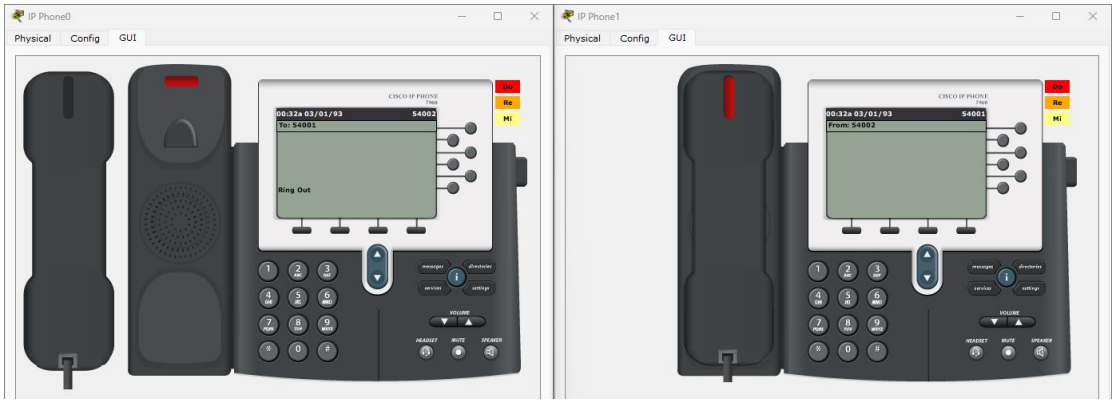


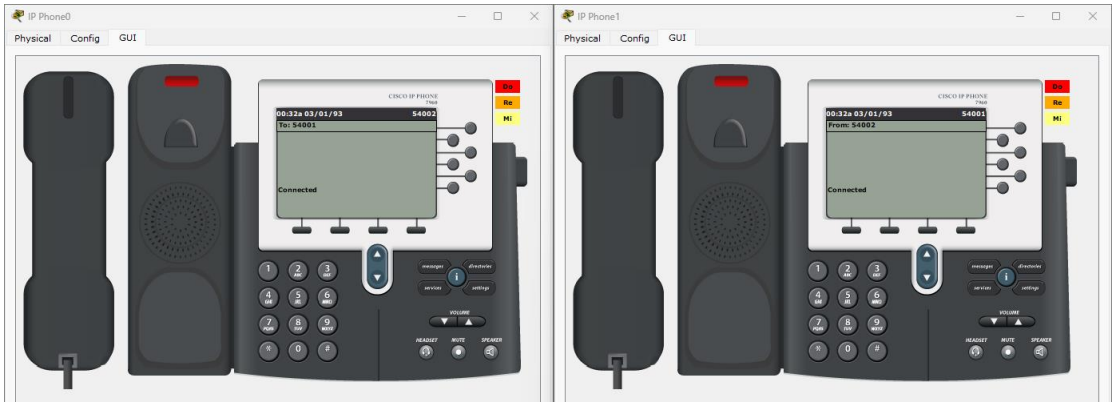
3. 配置上一步的 54001 就绪后，再连接一个 Cisco 7960，配置路由器中 IP 电话号码，并确认 IP 电话配置情况。



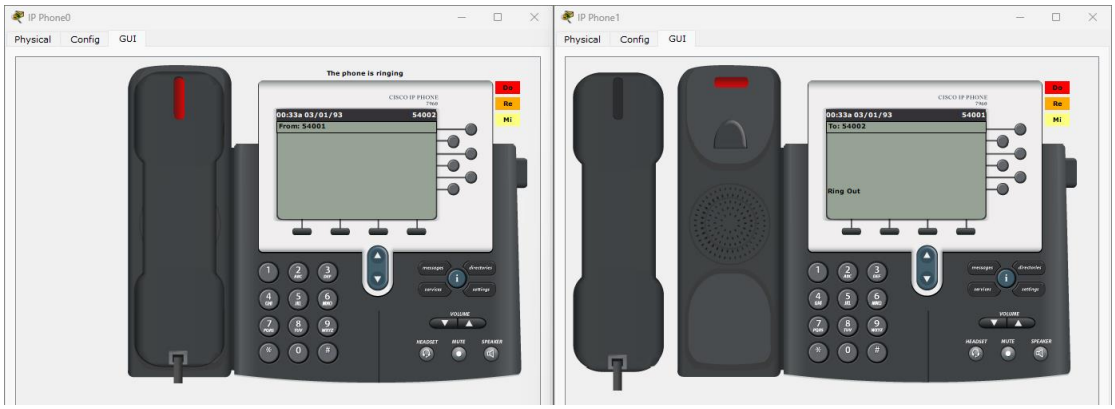
4. 检测两台话机拨号回铃情况。实验现象表明两台话机可以相互呼叫。

- 54001 拨打 54002：




- 54002 拨打 54001：



5. 配置一台电脑，检测电脑与 IP 电话之间能否彼此呼叫。在电脑的 Cisco IP Communicator 中，输入电话号码，点击 Dial 按钮即可拨出电话。实验现象

表明电脑与 IP 电话之间可以相互呼叫。

6. 增加一个 Cisco 7960，配置路由器中 IP 电话号码，检测话机之间拨号回铃情况。实验现象表明新增电话与原有电话之间可以相互呼叫。

- 54002 与 54004 互相呼叫：

- 54001 与 54004 互相呼叫：

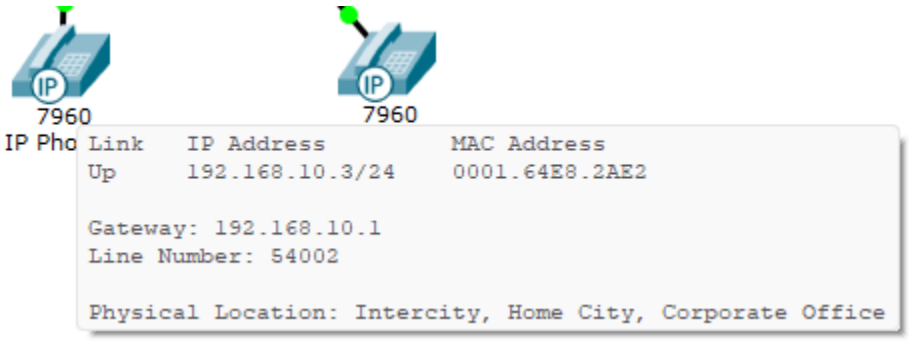
【分析讨论】

一、查看话机的 IP 地址

将鼠标悬停在话机上，在悬浮窗口上可以显示话机的详细信息，包括 IP 地址、物理地址、网关、电话号码等信息。

7960 IP Phone0、7960 IP Phone1、7960 IP Phone2 的详细信息如下：

| IP Phone | IP Address | MAC Mask | Gateway | Line Number |
|---|---|---|---|---|
| IP Phone0 | 192.168.10.3/24 | 0001.64E8.2AE2 | 192.168.10.1 | 54002 |
| IP Phone1 | 192.168.10.2/24 | 0090.2BDD.38DE | 192.168.10.1 | 54001 |
| IP Phone2 | 192.168.10.4/24 | 00D0.58DC.C90D | 192.168.10.1 | 54004 |



## 二、实验现象总结

1. IP 电话配置与连接测试：所有配置的 Cisco 7960 IP 电话均成功获取到 IP 地址，并能正确显示在界面上。这说明电话号码配置正确，并且电话之间能够顺利进行呼叫和接听。
2. 拨号回铃测试：电话之间的互相呼叫显示出良好的连接性。没有出现明显的通话延迟或其他问题，说明网络配置正确。
3. 电脑与 IP 电话互拨测试：使用 Cisco IP Communicator 软件的电脑能够与 IP 电话进行互拨，这表明软件电话的配置和网络整合良好。这也展示了 IP 电话系统的灵活性和与传统电脑设备的兼容性。

## 三、实验现象分析

1. IP 地址和网络配置：IP 电话获取的 IP 地址、网关和子网掩码均符合预期的网络配置，这表明 DHCP 服务器配置正确。VLAN 的正确配置确保了电话之间能够顺利进行呼叫和接听。
2. 电话服务（CME）配置：CME 的配置包括电话号码、最大端点数量的配置，这些都是确保电话系统功能正常的重要设置。
3. 协议的作用和表现：SIP 协议负责建立和终止通话，表现出良好的稳定性和可靠性。RTP 协议用于传输语音数据，由于没有出现丢包或显著延迟，表现出 RTP 性能良好。

# 实验 21：以太网帧分析实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/04/25 |

**【实验目的】**

1. 了解并识别 MAC 地址以及其在网络通信中的重要性。MAC 地址是网络设备的物理地址，对于网络中设备的识别和通信至关重要。
2. 使用 Wireshark 这一网络分析工具，抓取并分析 MAC 数据包。Wireshark 是一款强大的网络协议分析工具，能帮助学生理解网络通信过程中数据的传输和处理。
3. 深入理解以太网的数据帧结构，包括前导码、帧开始符、MAC 地址、以太类型字段等。
4. 观察并分析在使用 ICMP（如 ping 命令）数据包转发过程中 MAC 地址的变化情况，以加深对网络层与数据链路层交互作用的理解。

**【实验原理】**

**一、以太网**

以太网是一种广泛应用的计算机局域网技术，由 IEEE 的 IEEE 802.3 标准制定。这一标准涵盖了包括物理层连线、电子信号传输以及介质访问控制层协议的详细规定。因其高效和广泛的应用，以太网已成为当今最常见的局域网技术之一。

以太网有两种主要形式：经典以太网和交换式以太网。经典以太网是以太网的原始形式，其数据传输速率从 3 Mbps 到 10 Mbps 不等。而交换式以太网则支持更高的数据传输速率，包括 100 Mbps、1 Gbps（千兆以太网），甚至 10 Gbps（万兆以太网）。

在网络拓扑结构上，以太网从原来的总线型拓扑逐渐演变为星型拓扑。这种变化主要是通过使用交换机来实现的，目的是为了减少数据传输中的冲突，提高网络速度和效率。即使在物理结构上采用星型拓扑，以太网在逻辑上依然保留了总线型拓扑的特性，并使用了 CSMA/CD（载波侦听多路访问/碰撞检测）技术来管理数据传输。

以太网的每一个设备都有一个全球唯一的 48 位的 MAC 地址，这个地址由设备的制造商在制造时分配并烧录在网络接口卡上。MAC 地址的唯一性保证了网络

中的设备能够相互识别和通信。随着以太网技术的普及，许多设备制造商开始将以太网接口直接集成到计算机的主板中。

总体而言，以太网技术的普及和发展极大地促进了网络通信的效率和可靠性，使得网络设备的互联互通成为可能。

**二、MAC 地址**

MAC 地址，全称为媒体访问控制地址（Media Access Control address），是网络设备在制造过程中固化在网络接口卡（Network Interface Card, NIC）的唯一标识符。这个地址通常被存储在网卡的 EPROM（一种可编程读写的存储芯片）中，并可以通过特定程序进行修改。

MAC 地址共有 48 位，等同于 6 个字节，通常用十六进制表示，分为两部分：制造商标识符和设备标识符。例如，MAC 地址“00-16-EA-AE-3C-40”中，“00-16-EA”是由 IEEE（电气与电子工程师协会）分配给网络硬件制造商的 OUI（Organizationally Unique Identifier，组织唯一标识符），用于区分不同的制造商。“AE-3C-40”则是该制造商分配给具体网络产品的标识，代表了网卡或其他网络设备的系列号。

在 MAC 地址的编码中，最高有效字节的第二位（LSb，低第二位）称为 U/L 位（Universal/Local），用于表示地址是全球统一的还是局部使用的。如果此位为 0，表示地址是全局统一的；如果为 1，则表示地址是局部使用的。所有标准的 OUI 分配都将此位设置为 0。

此外，MAC 地址的最高有效字节的最低位（LSb，低第一位）用于指示地址是单播还是多播。如果此位为 0，表示是单播地址，用于单个设备；如果此位为 1，则表示是多播地址，用于多个设备。

MAC 地址的全球唯一性和这些结构特点使得在网络中每个设备都可以具有独一无二的身份，从而在数据传输过程中能够确保数据准确地发送至正确的目的地。

**三、MAC 数据包格式**

MAC 数据包格式，尤其是以太网环境下的 Ethernet II 帧结构，对于理解网络通信的基本机制至关重要。下面是对以太网帧的详细介绍，主要关注于 Ethernet II 帧格式，这是目前最常用的以太网数据包格式：

1. 帧间距：以太网帧之间需要有至少 12 字节的空闲线路状态码，也称为帧间隔，这有助于区分连续的数据帧，确保数据传输的清晰界限。
2. 以太帧类型：以太网支持多种帧类型，每种帧都有其特定的结构和最大传输单元（MTU）值。Ethernet II 帧（也称为 DIX 帧）是其中最常见的类型，直接支持 IP 协议等上层协议。
3. Ethernet II 帧格式：
   - 前导码和帧开始符：通常帧的开始有一个特定的前导码和帧开始符，用来标示帧的起始点。
   - 目标 MAC 地址和源 MAC 地址：每个 Ethernet II 帧都包含 6 字节的目标 MAC 地址和 6 字节的源 MAC 地址，分别指定帧的接收者和发送者。
   - 类型字段：紧随 MAC 地址后的是两字节的类型字段，用于指定帧中承载的数据类型。例如，0x0800 代表 IPv4 数据，0x0806 代表 ARP 请求，0x86DD 代表 IPv6 数据。
4. 长度与类型字段的区分：
   - 在早期的以太网版本中，这个字段被用来表示数据的长度，但在 Ethernet II 标准中，它被用作类型字段。
   - 如果该字段的值大于或等于 1536（0x0600），则解释为类型字段，表明帧是一个 Ethernet II 帧。
   - 如果该字段的值在 46 到 1500 字节之间（不包括 1500～1536 的未定义区域），则表示帧长度，并且帧遵循 IEEE 802.3 标准。
5. 数据和帧校验序列：类型字段后是数据负载，长度可变。每个帧的末尾包括一个 32 位的循环冗余校验码（CRC），用于检测传输过程中的错误。

这种结构的设计使得 Ethernet II 帧能够高效地支持多种网络协议，同时保持数据传输的准确性和可靠性，是网络通信中的基础设施之一。

802.3 以太网帧结构

| 前导码 | 帧开始符 | MAC 目标地址 | MAC 源地址 | 802.1Q 标签 (可选) | 以太类型 | 负载 | 冗余校验 | 帧间距 |
|---|---|---|---|---|---|---|---|---|
| 10101010 7个octet | 10101011 1个octet | 6 octets | 6 octets | (4 octets) | 2 octets | 46–1500 octets | 4 octets | 12 octets |
| | | 64–1522 octets | | | | | | |
| 72–1530 octets | | | | | | | | |
| 84–1542 octets | | | | | | | | |

**【实验设备】**

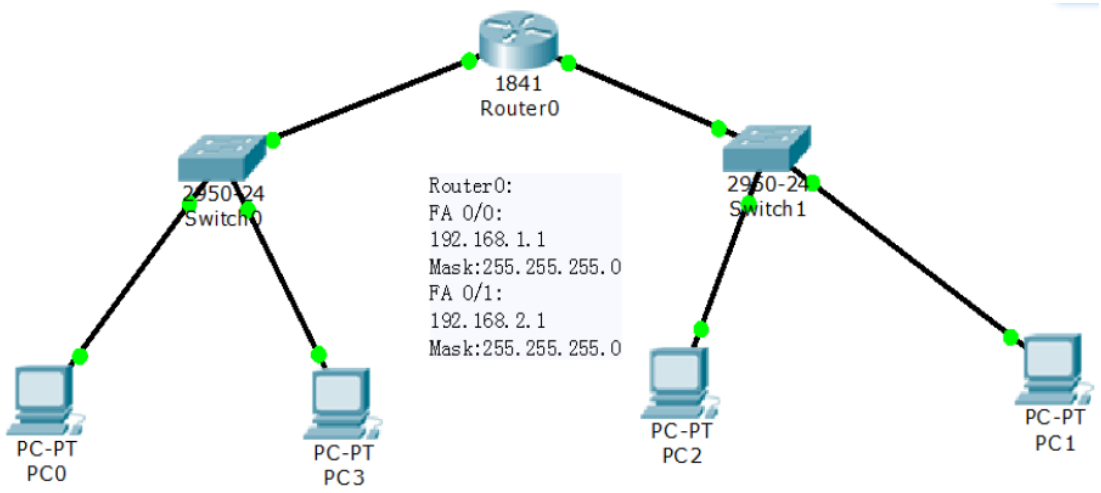
1. 操作系统：Windows 10

2. 网络环境：局域网

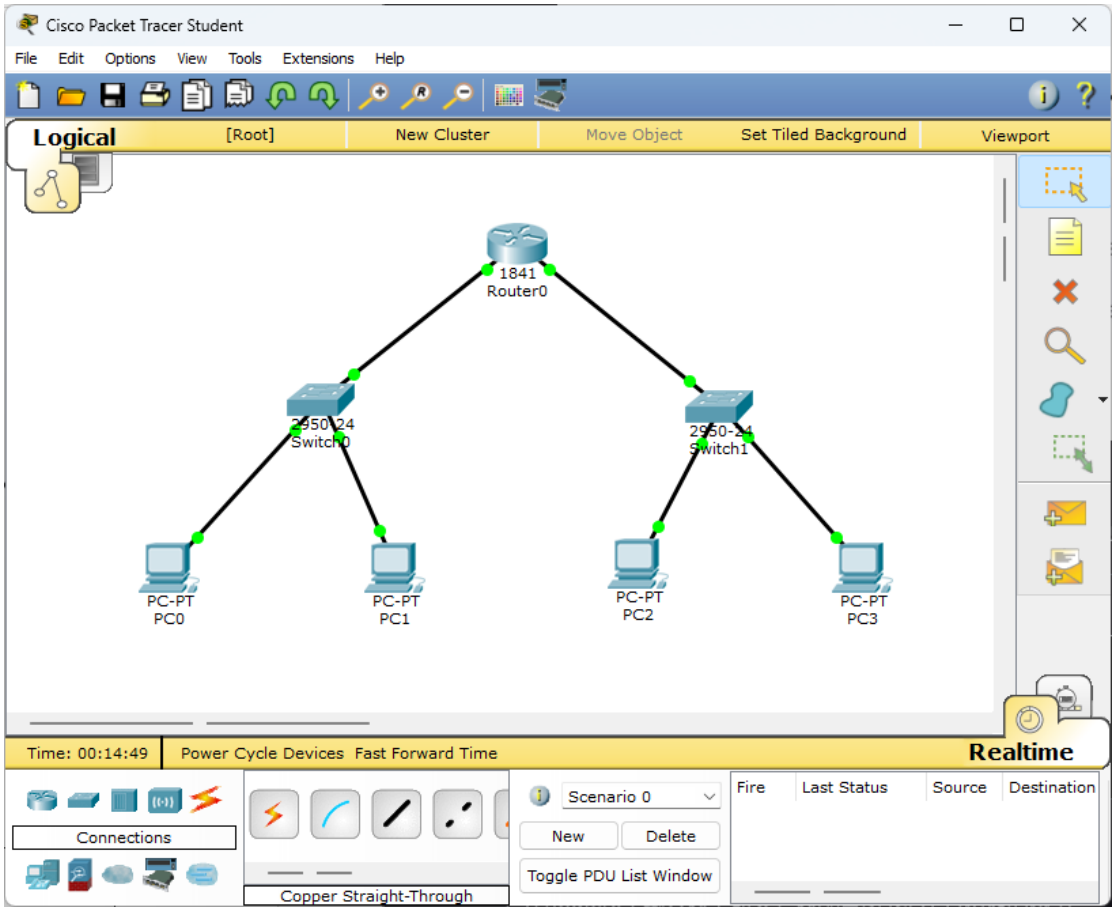
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。

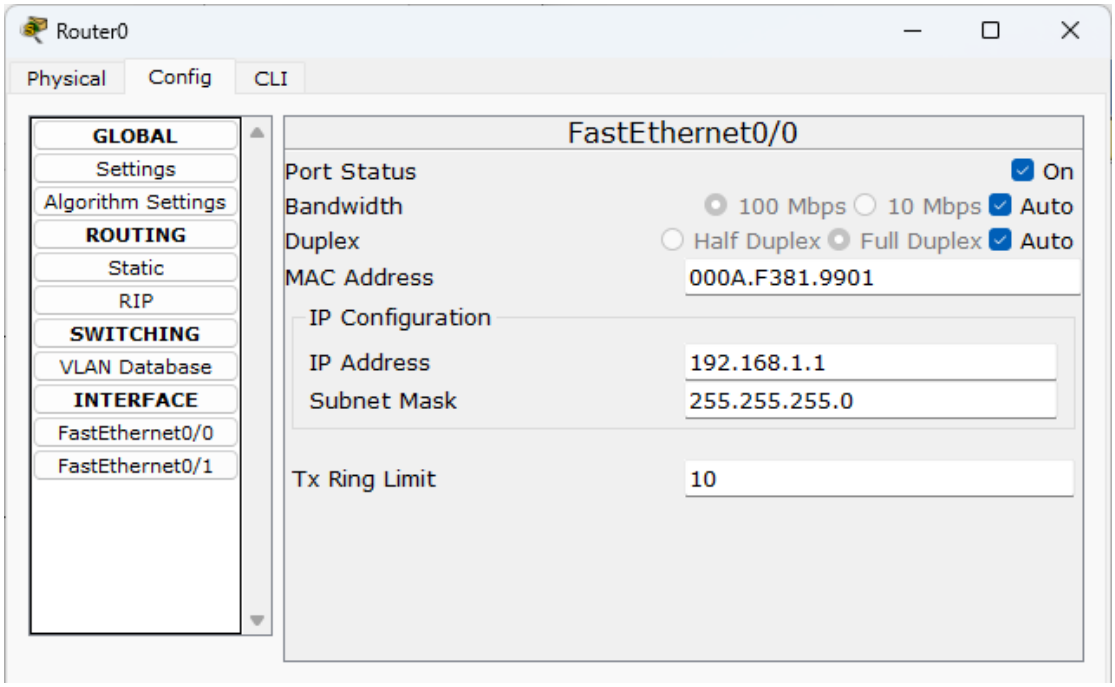


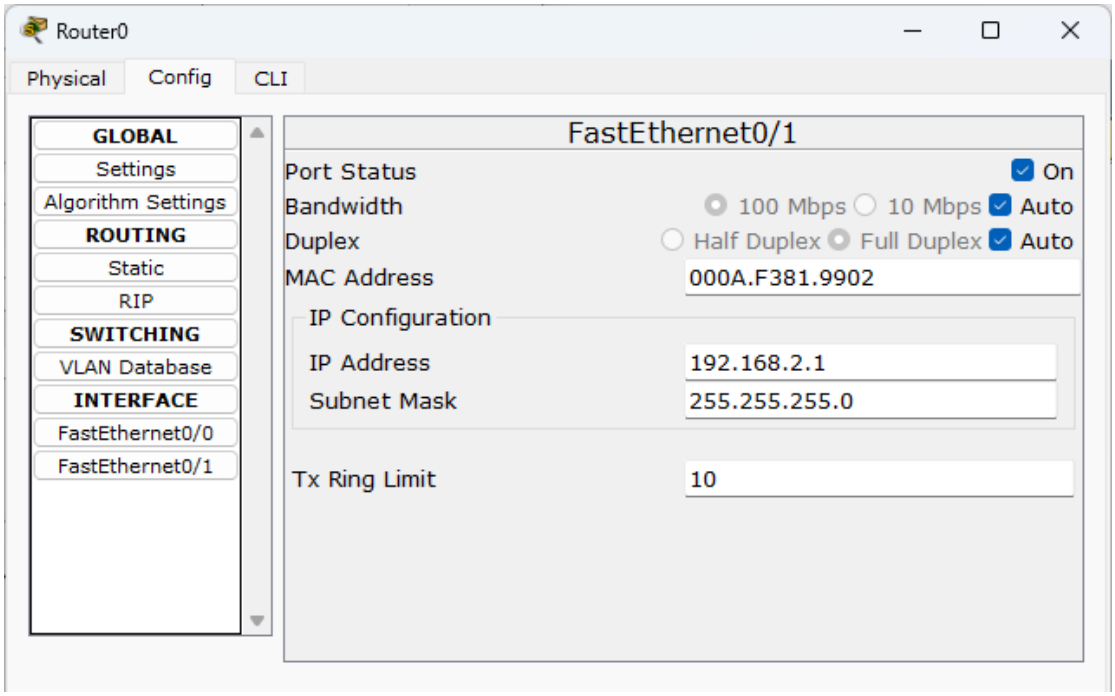

2. 启动 Cisco Packet Tracer，按照上图连接网络。




3. 配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```




4. 配置 DHCP 前查看各 PC IP 地址情况。

5. 在路由器 Router0 配置 DHCP。

   - 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

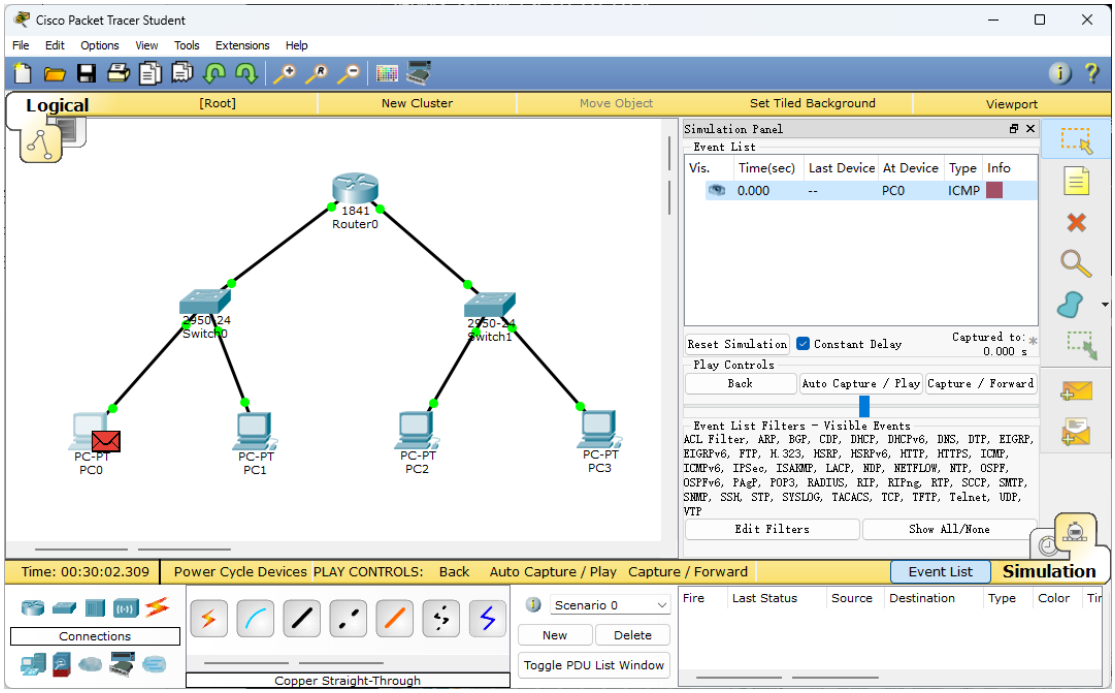
```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

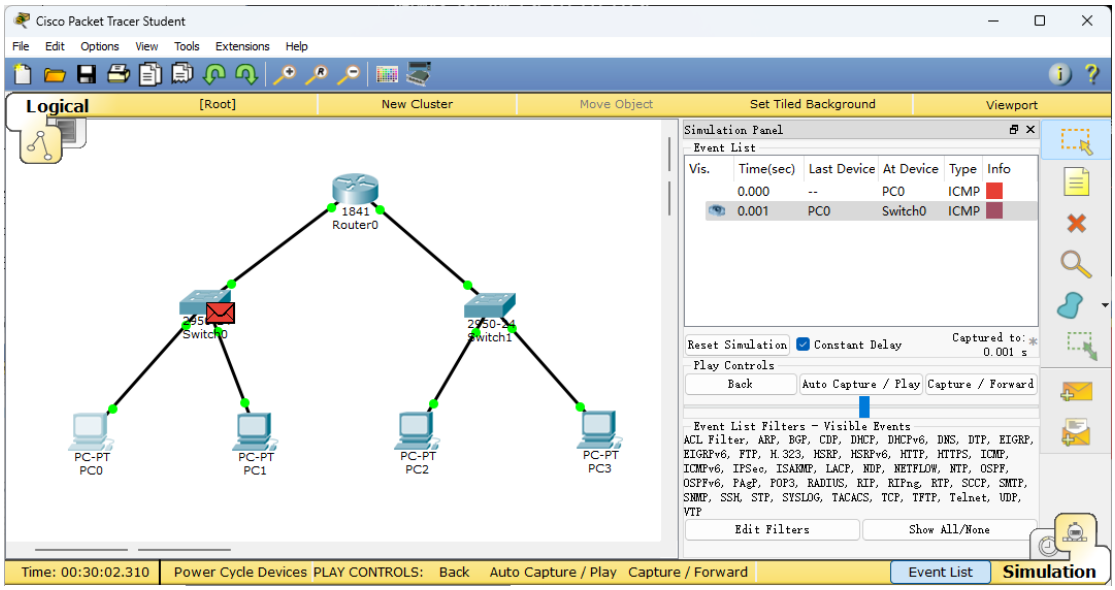
6. 配置 DHCP 后查看各 PC IP 地址情况。
7. 从 Realtime 模式切换至 Simulation 模式，模拟 ICMP（ping 命令）。

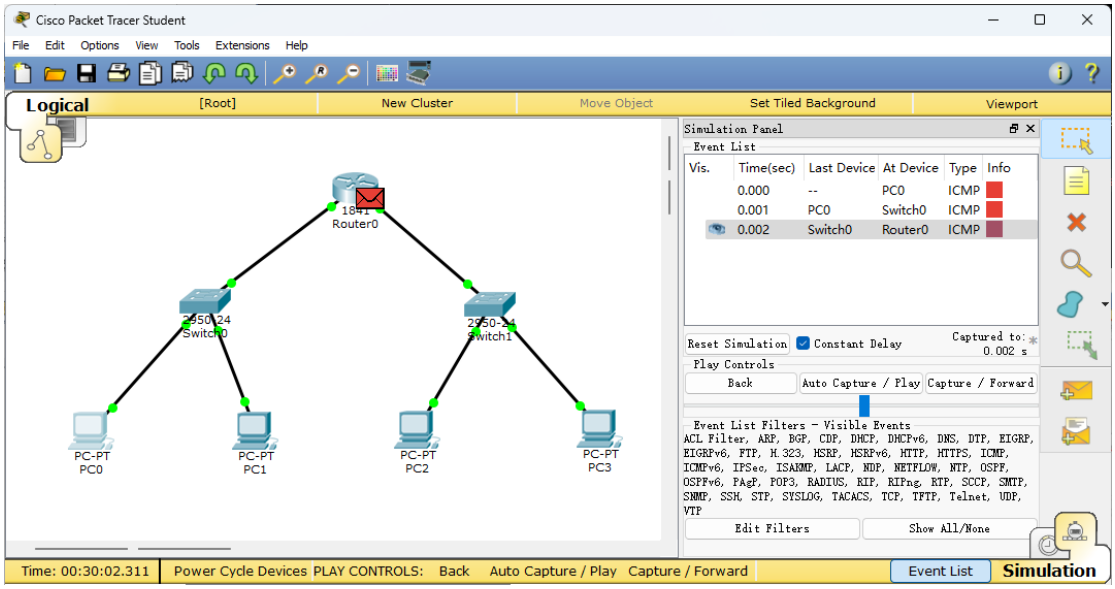
   7.1 在 PC0 的终端输入 ping 192.168.2.12 命令，即 ping PC2。

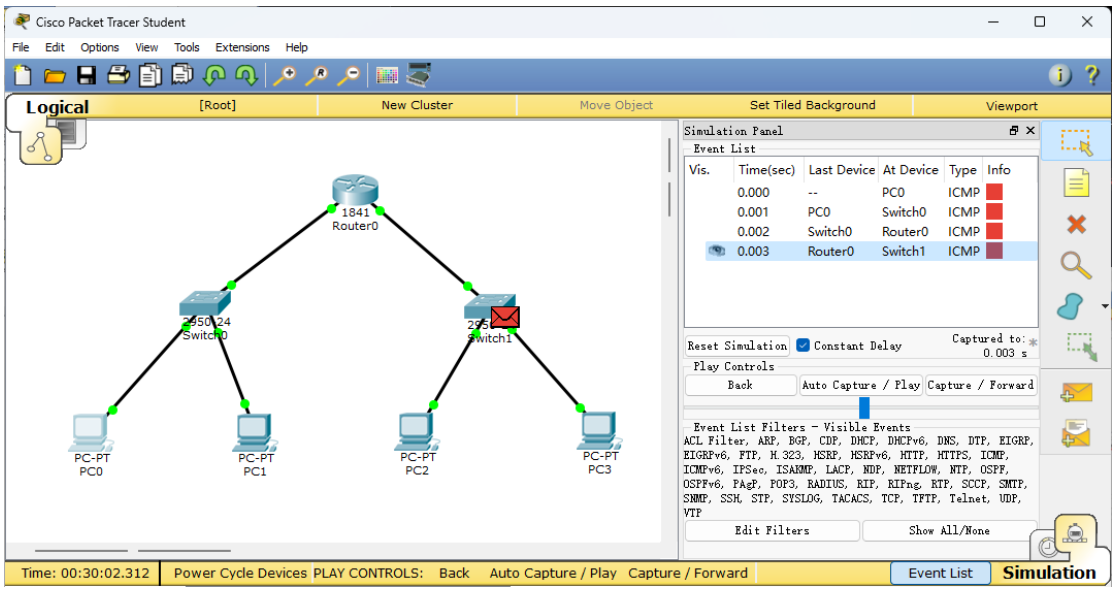
   7.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

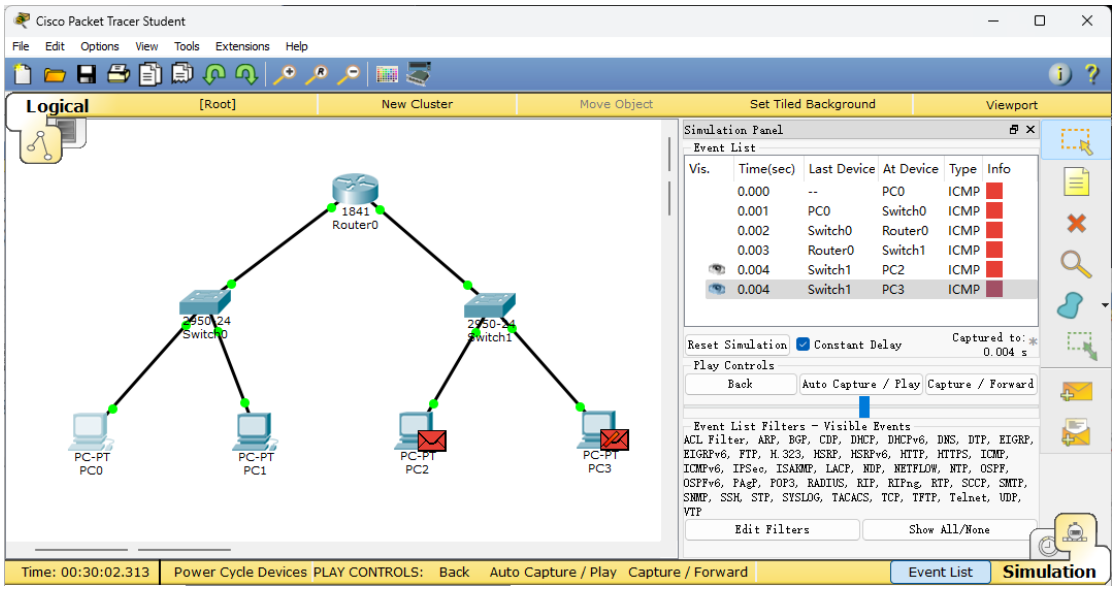
   7.3 在 Even List 中的 Info 栏可以查看相关信息。

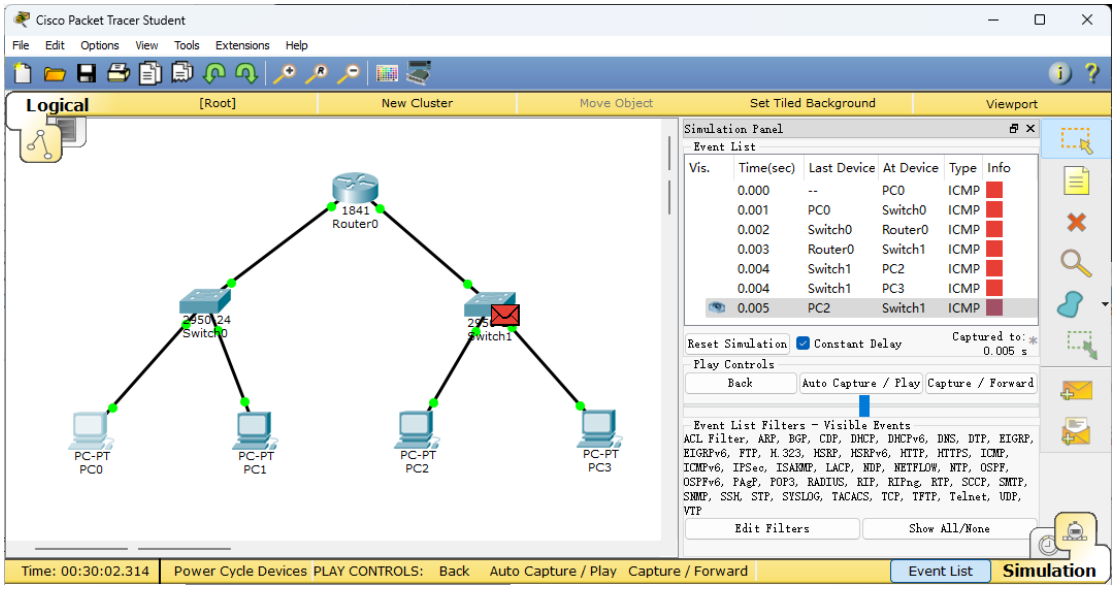


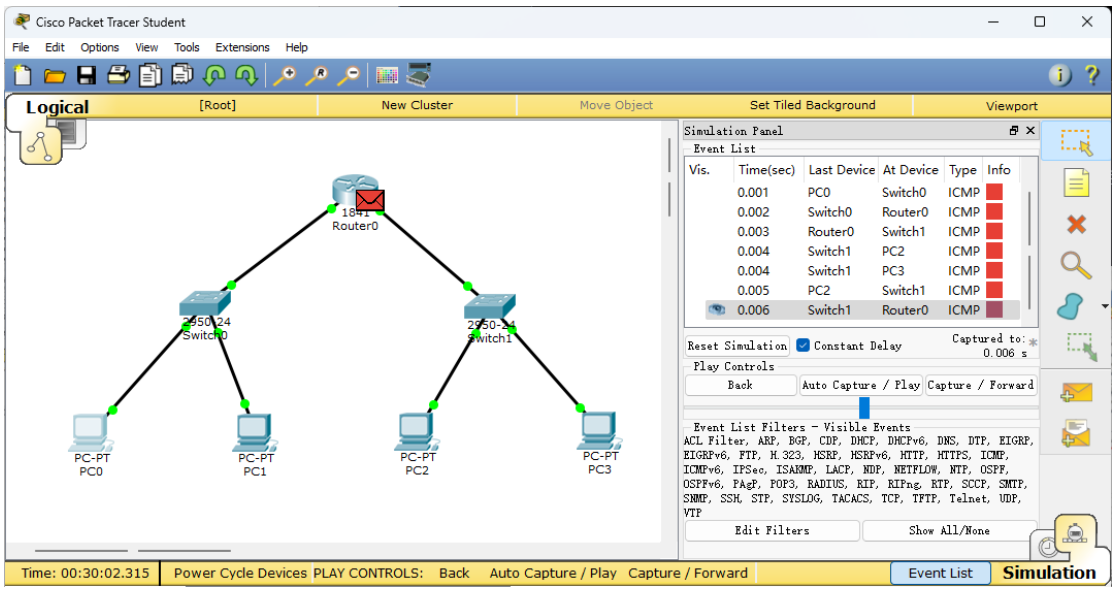

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
1841
Router0
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
Reset Simulation
Constant Delay
Captured to: 0.001 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:30:02.310
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation

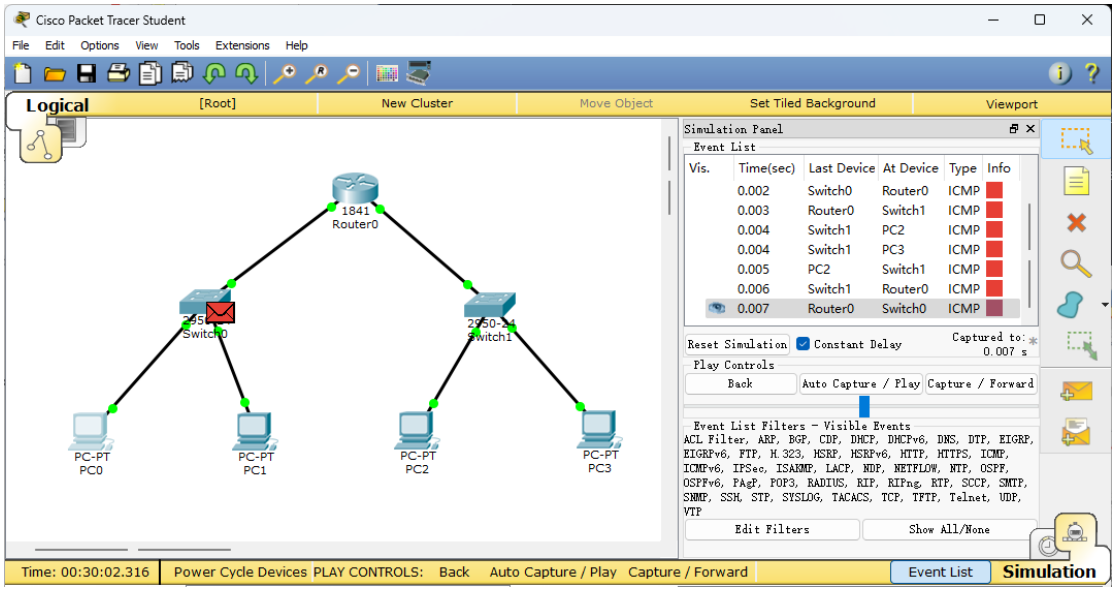

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
1841
Router0
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
Reset Simulation
Constant Delay
Captured to: 0.002 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:30:02.311
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation

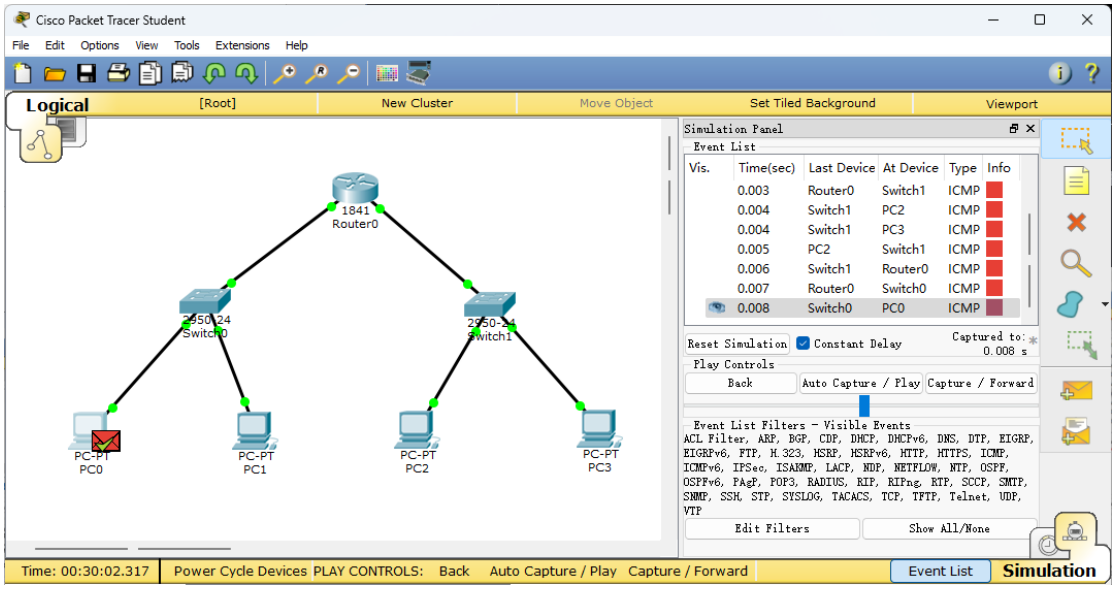

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
1841
Router0
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
Reset Simulation
Constant Delay
Captured to: 0.003 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:30:02.312
Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
1841
Router0
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
0.004 Switch1 PC2 ICMP
0.004 Switch1 PC3 ICMP
Reset Simulation
Constant Delay
Captured to: 0.004 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:30:02.313
Power Cycle Devices
PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
1841
Router0
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
0.004 Switch1 PC2 ICMP
0.004 Switch1 PC3 ICMP
0.005 PC2 Switch1 ICMP
Reset Simulation
Constant Delay
Captured to: 0.005 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:30:02.314
Power Cycle Devices
PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
1841
Router0
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
0.004 Switch1 PC2 ICMP
0.004 Switch1 PC3 ICMP
0.005 PC2 Switch1 ICMP
0.006 Switch1 Router0 ICMP
Reset Simulation
Constant Delay
Captured to: 0.006 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters
Show All/None
Time: 00:30:02.315
Power Cycle Devices
PLAY CONTROLS: Back Auto Capture / Play Capture / Forward
Event List
Simulation

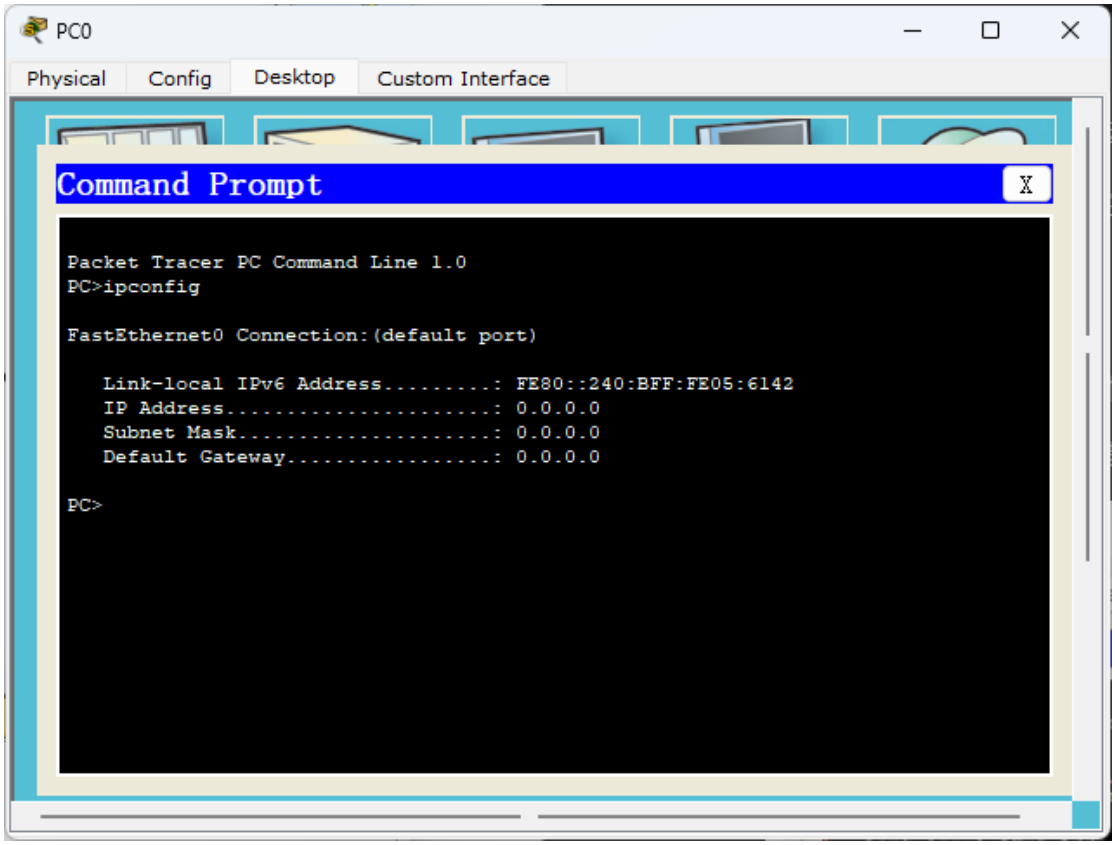


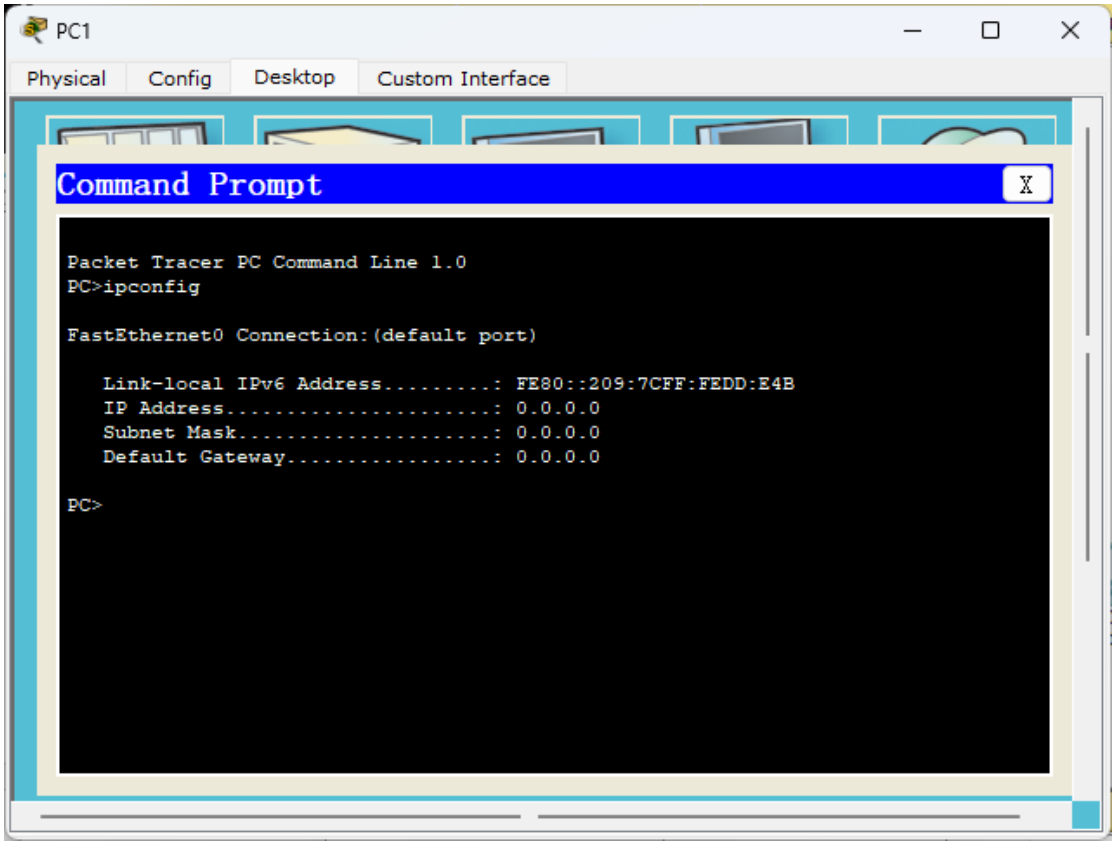



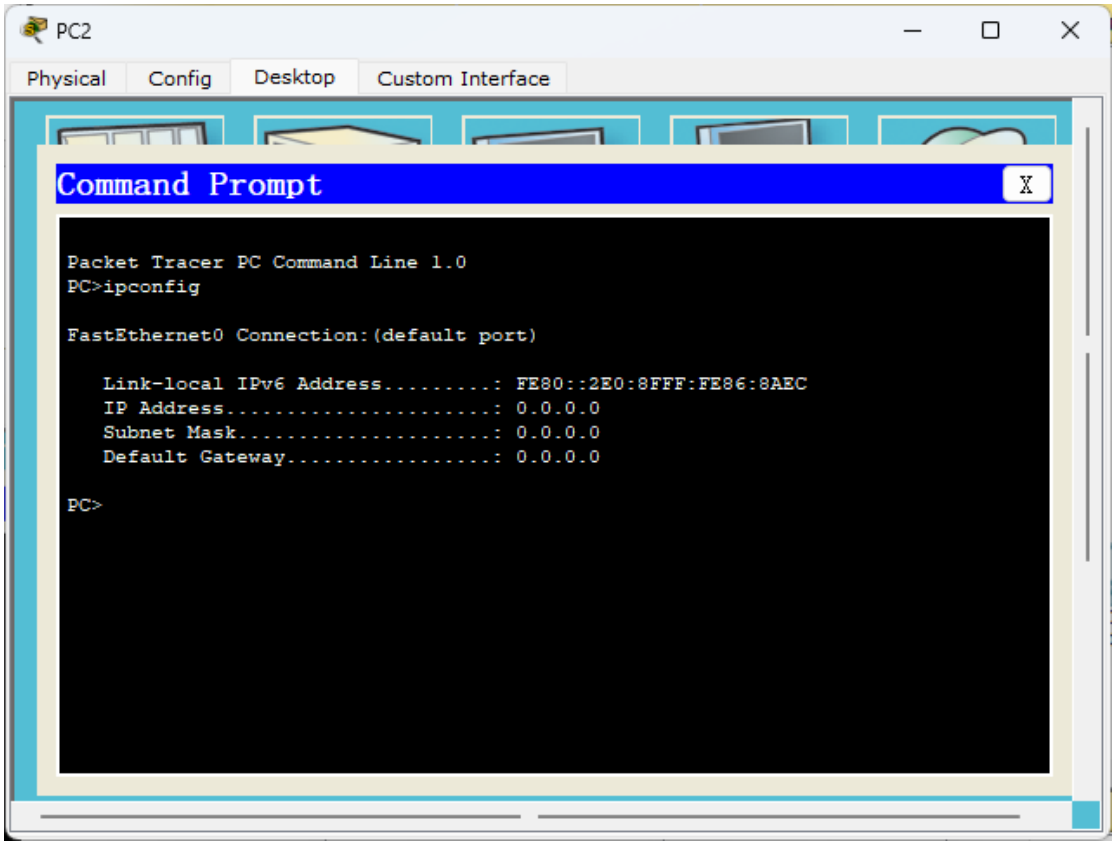

8. 本机命令提示符输入 ipconfig/all 命令，查看本机的 MAC 地址。
9. 安装 WireShark 软件并练习使用，并分析 MAC DIX V2 帧。
10. 用 WireShark 抓取 MAC 数据包，选用 WLAN 方式进行抓包。
11. 查看 MAC 数据包字段内容，并解读。
12. 分析在 Cisco Packet Tracer 中模拟 ICMP（ping 命令），ICMP 数据包转发过程中 MAC 地址变化情况。

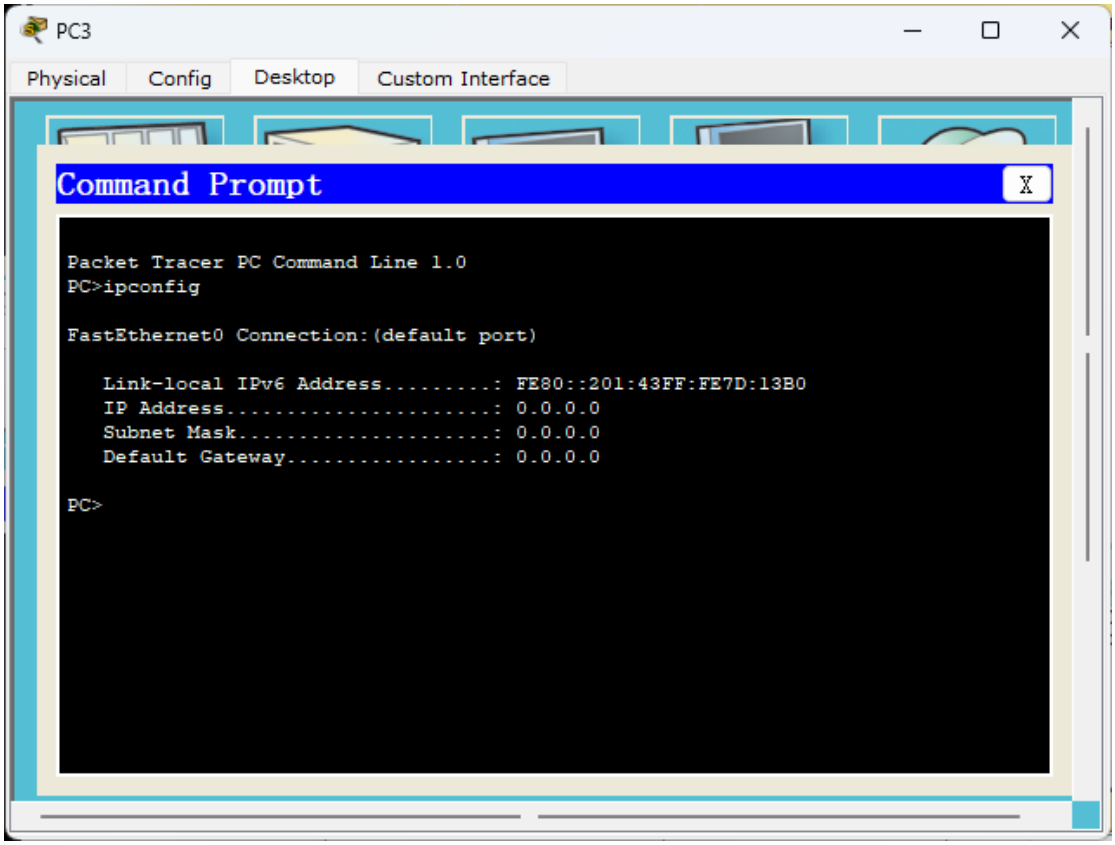
**【实验现象】**

1. 配置 DHCP 前查看各 PC IP 地址情况，各 PC 机的 IP 地址、子网掩码、默认网关均相同，为 0.0.0.0。


PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::240:BFF:FE05:6142
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
PC>


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::209:7CFF:FEDD:E4B
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
PC>




2. 配置 DHCP 后查看各 PC IP 地址情况。

- PC0：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::290:21FF:FEAD:CD14
   IP Address......................: 192.168.1.12
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.1.1
```

- PC1：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::207:ECFF:FECE:EB7E
   IP Address......................: 192.168.1.14
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.1.1
```

- PC2：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE48:E19B
   IP Address......................: 192.168.2.12
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.2.1
```

- PC3：

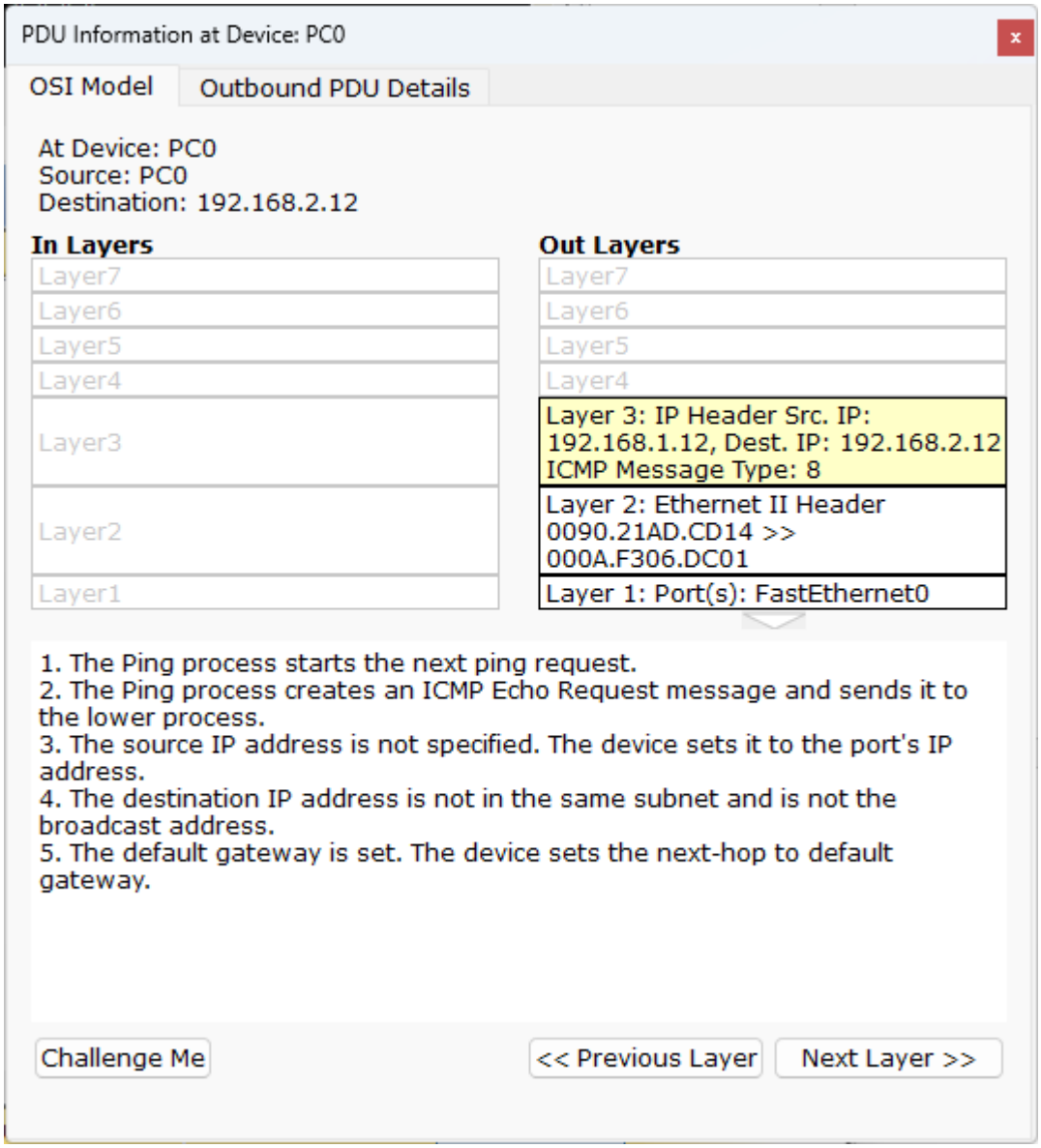
```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::20C:CFFF:FEE5:5B6D
   IP Address......................: 192.168.2.14
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.2.1
```

| PC | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|
| PC0 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC1 | 192.168.1.14 | 255.255.255.0 | 192.168.1.1 |
| PC2 | 192.168.2.12 | 255.255.255.0 | 192.168.2.1 |
| PC3 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1 |

3. 从 Realtime 模式切换至 Simulation 模式，模拟 ICMP（ping 命令），在 Even List 中的 Info 栏可以查看相关信息，这里分析前两个 Event 的相关数据。

| Vis. | Time(sec) | Last Device | At Device | Type | Info |
|---|---|---|---|---|---|
| | 0.000 | -- | PC0 | ICMP | |
| | 0.001 | PC0 | Switch0 | ICMP | |
| | 0.002 | Switch0 | Router0 | ICMP | |

3.1 PDU Information at Device: PC0（OSI Model）




这张图展示了在使用 Cisco Packet Tracer 进行网络模拟时，一个 ICMP 回显请求的数据包细节。它是根据 OSI 模型来组织的，图中包含了出站 PDU（协议数据单元）的详细信息。在 OSI 模型的不同层次上，可以看到如下信息：

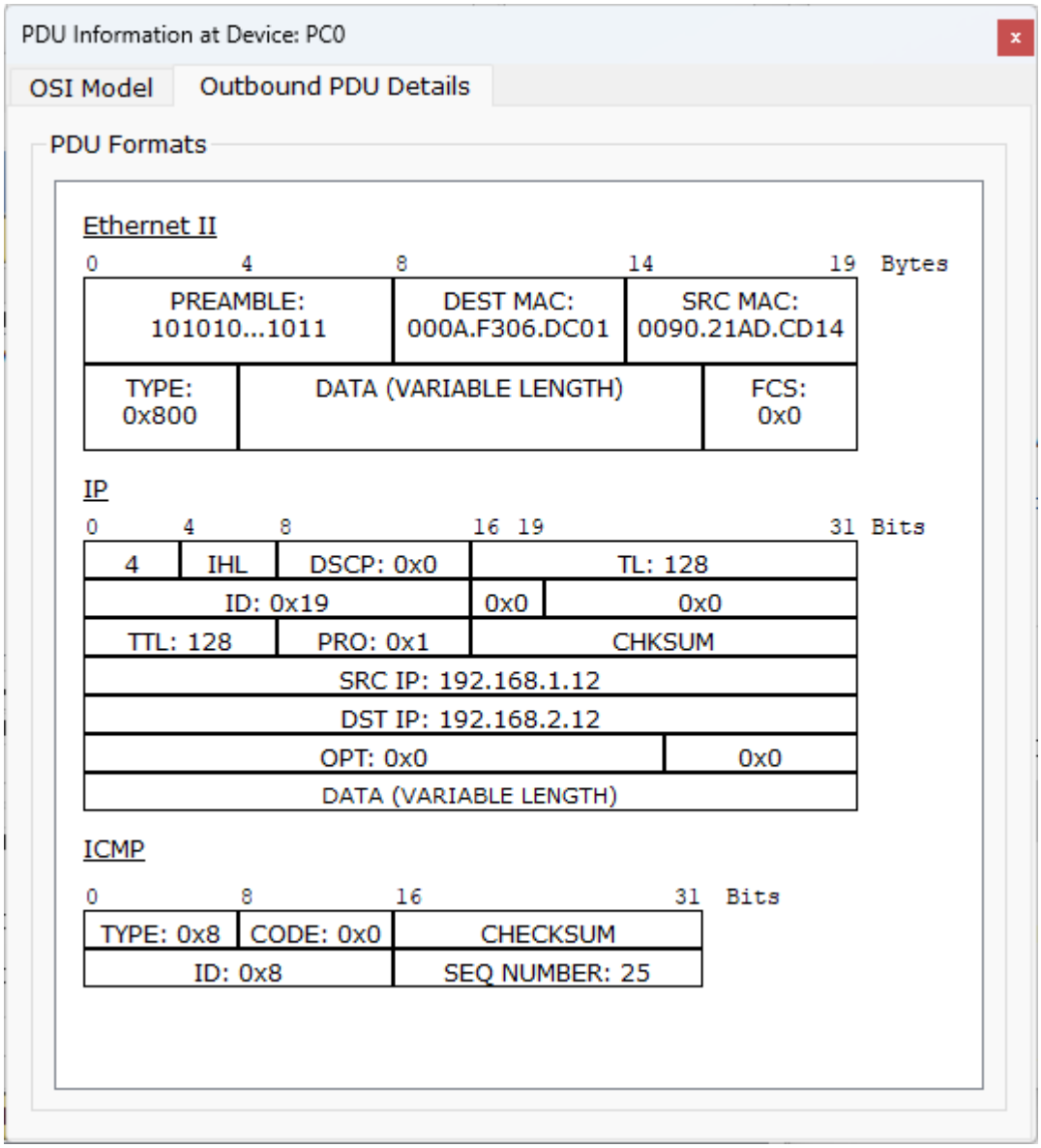
- 源地址（Source）和目的地址（Destination）被设置为 192.168.2.12。
- 出站层（Out Layers）显示数据包是如何从应用层（Layer 7）通过各个网络层逐步构建的，包括 IP 头信息（Layer 3），以及 Ethernet II 头信息（Layer 2），最后是物理层端口信息（Layer 1）。
- 在 Layer 3，我们可以看到源 IP（Src. IP）和目的 IP（Dest. IP）以及 ICMP 消息类型为 8，这是回显请求的类型。

- Layer 2 展示了以太网头信息，其中包含了 MAC 地址。
- Layer 1 指的是使用的物理端口，这里是 FastEthernet0。

屏幕底部列出的 1 至 5 点描述了 ping 过程中发生的步骤：

- Ping 过程启动下一个 ping 请求。
- Ping 过程创建了一个 ICMP 回显请求消息，并将其发送给较低层的处理过程。
- 源 IP 地址未指定，设备将其设置为端口的 IP 地址。
- 目的 IP 地址不在同一子网中，也不是广播地址。
- 已设置默认网关。设备将下一跳设置为默认网关。

3.2 PDU Information at Device: PC0（Outbound PDU Details）



这张图显示了Cisco Packet Tracer模拟中，一个ICMP数据包的出站PDU（协议数据单元)细节,涵盖了三个不同的网络层的格式:以太网II、IP和ICMP。

以太网II（Ethernet II）：

- 前导码（Preamble）：101010...1011，用于同步。
- 目的MAC地址（DEST MAC）：000A.F306.DC01。
- 源MAC地址（SRC MAC）：0090.21AD.CD14。
- 类型（Type）：0x800，表示载荷是一个IP数据包。
- 数据（Data）：可变长度，包含了封装的IP数据包。
- 帧检验序列（FCS）：0x0，用于错误检测。

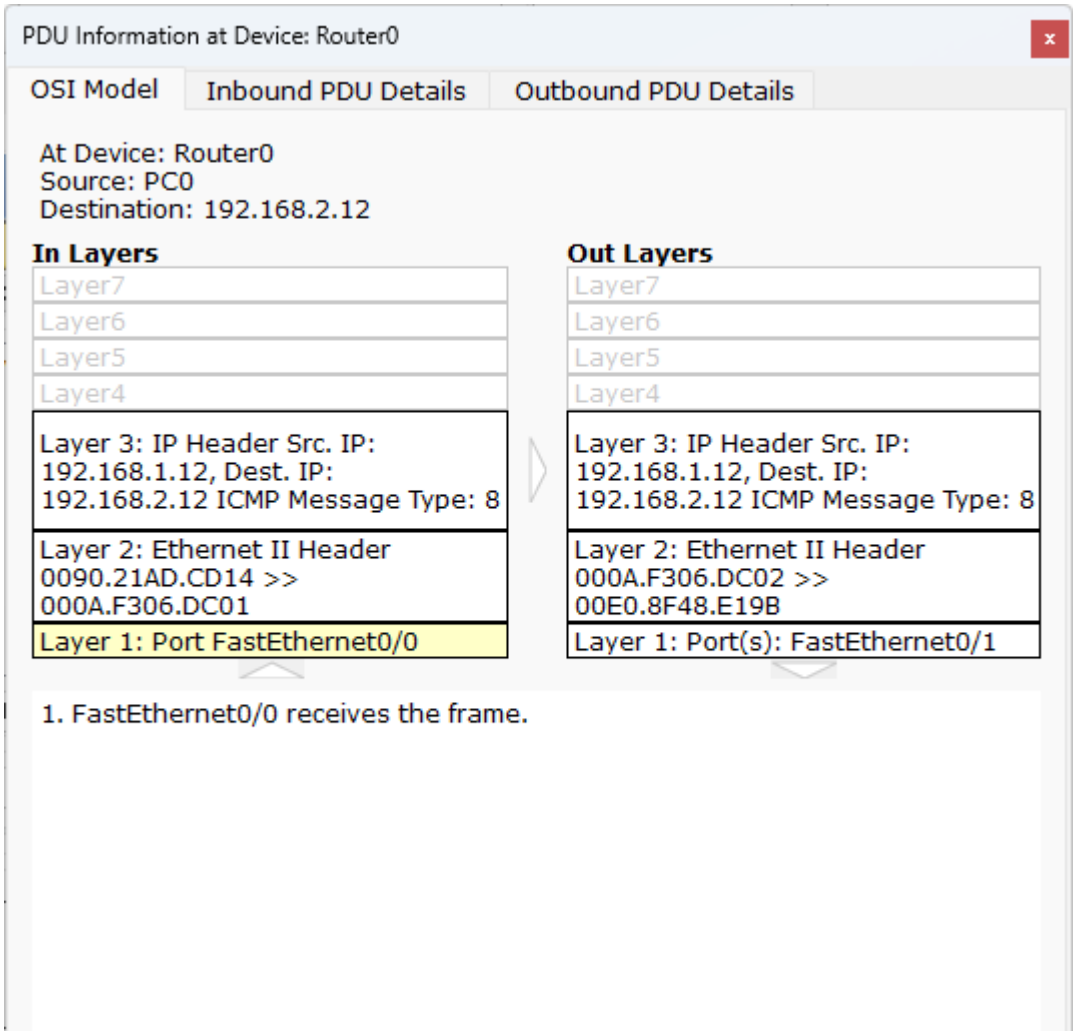
IP：

- 版本（Version）：4，表示IPv4。
- 头长度（IHL - Internet Header Length）：表示IP头部的长度。
- 差分服务代码点（DSCP）：0x0，表示数据包的服务质量。
- 总长度（TL - Total Length）：128字节。
- 标识（ID）：0x19，一个唯一标识符。
- 标志和片偏移(Flags and Fragment Offset)：0x0，相关于数据包分段。
- 生存时间（TTL - Time To Live）：128，数据包在网络中的生存时间。
- 协议（PRO）：0x1，表示承载的是ICMP数据。
- 头部校验和（Checksum）：用于错误检测。
- 源IP地址（SRC IP）：192.168.1.12。
- 目的IP地址（DST IP）：192.168.2.12。
- 选项（Options, OPT）：0x0，通常用于调试和网络测试。

ICMP：

- 类型（Type）：0x8，表示这是一个回显请求（通常用于ping）。
- 代码（Code）：0x0，具体化了类型。
- 校验和（Checksum）：用于错误检测。
- 标识符（ID）：0x8，用于标识回显请求。
- 序列号（Sequence Number, SEQ NUMBER）：25，用于标记发送的回显请求序列。

3.3 PDU Information at Device: Router0（OSI Model）




这张图是 Cisco Packet Tracer 中，一个路由器设备（Router0）的 ICMP 数据包的 PDU（协议数据单元）信息。这些信息反映了数据包在网络中的移动，从它进入路由器（入站 PDU 细节），到它从路由器出去（出站 PDU 细节）。

入站 PDU 细节（Inbound PDU Details）：

- 在设备：Router0
- 源地址（Source）：PC0
- 目的地址（Destination）：192.168.2.12

入站层（In Layers）信息显示数据包是如何被路由器接收的：

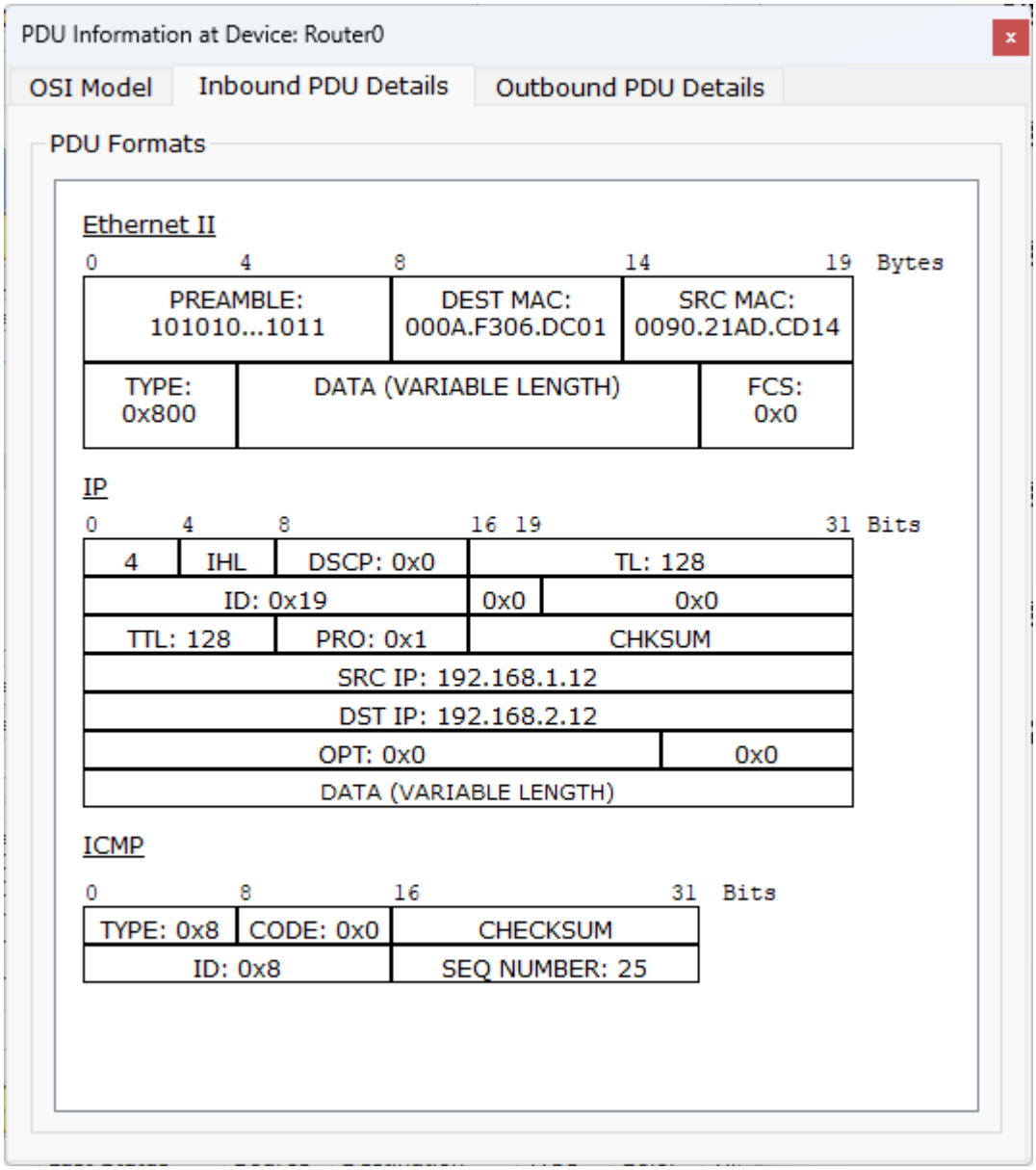
- Layer 3：IP 头信息显示源 IP 为 192.168.1.12，目的 IP 为 192.168.2.12，ICMP 消息类型为 8（回显请求）。
- Layer 2：以太网 II 头信息展示源 MAC 地址为 0090.21AD.CD14，目的 MAC 地址为 000A.F306.DC01。

- Layer 1：表明该数据包是通过端口 FastEthernet0/0 进入路由器的。
- 出站 PDU 细节（Outbound PDU Details）

出站层（Out Layers）信息显示数据包在经过路由器处理后如何出站：

- Layer 3：IP 头部信息不变，仍然显示源 IP 为 192.168.1.12 和目的 IP 为 192.168.2.12，ICMP 消息类型仍为 8。
- Layer 2：以太网 II 头信息此时展示的源 MAC 地址变为路由器的源 MAC 地址 000A.F306.DC02，而目的 MAC 地址变为另一个 MAC 地址（可能是下一个跳转目标的 MAC 地址）00E0.8F48.E19B。
- Layer 1：数据包现在是通过端口 FastEthernet0/1 离开路由器的。

3.4 PDU Information at Device: Router0（Inbound PDU Details）



这张图显示了在Cisco Packet Tracer模拟环境中，路由器（Router0）上的 ICMP 数据包的入站 PDU（协议数据单元）细节。它提供了数据包的三个层次的信息：以太网 II 层，IP 层和 ICMP 层。

以太网 II（Ethernet II）：

- 前导码（Preamble）：101010...1011，用于帧的同步。
- 目的 MAC 地址（DEST MAC）：000A.F306.DC01，是路由器接口或下一个跳转的 MAC 地址。
- 源 MAC 地址（SRC MAC）：0090.21AD.CD14，是发送者的 MAC 地址。
- 类型（Type）：0x800，说明后面跟随的是一个 IP 协议的数据包。
- 数据（Data）：可变长度，承载了 IP 和 ICMP 层的信息。
- 帧检验序列（FCS）：0x0，用于检测帧在传输过程中的错误。

IP：

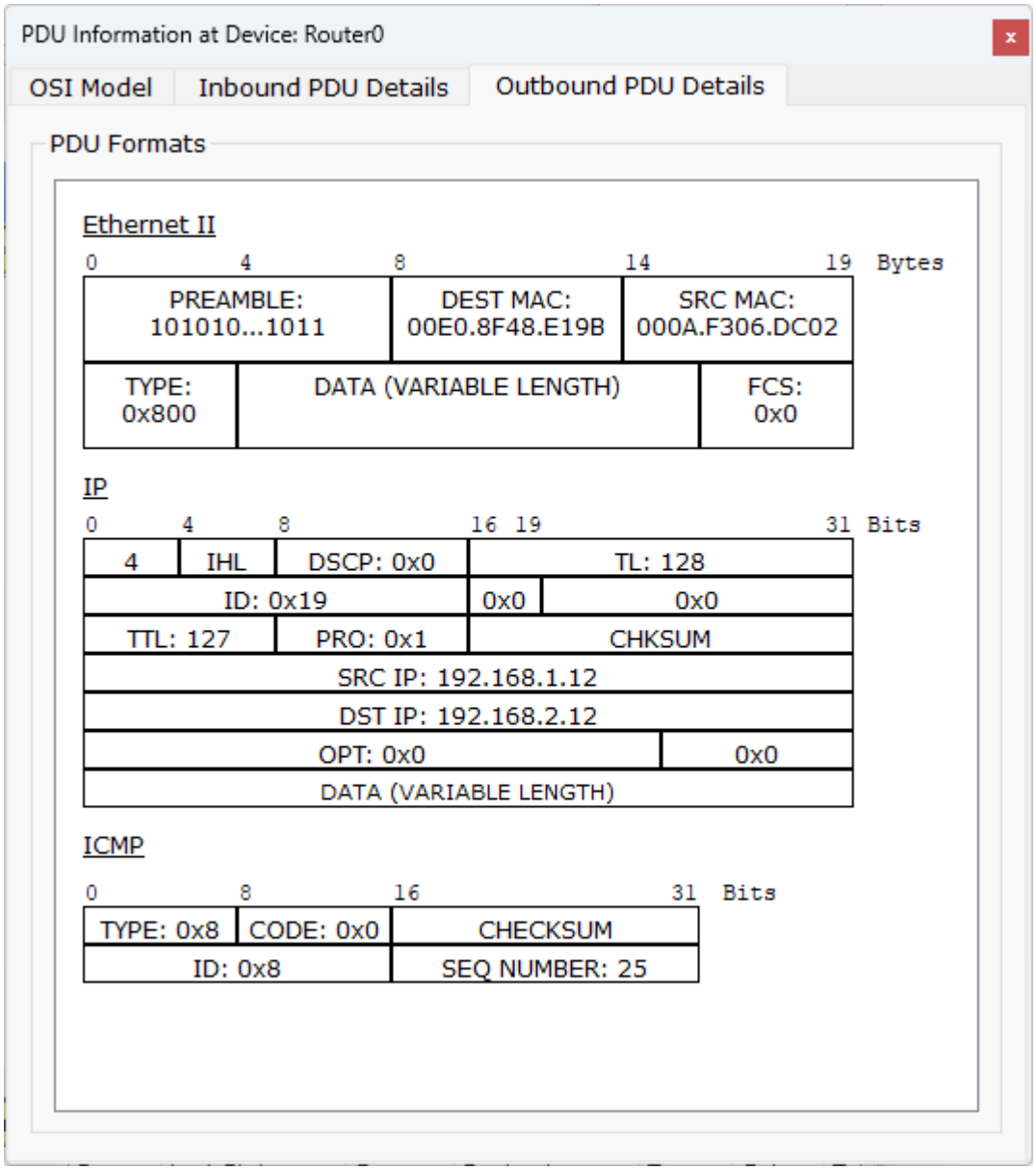
- 版本（Version）：4，指的是 IPv4。
- 头部长度（IHL - Internet Header Length）：通常表示 IP 头部的长度。
- 差分服务代码点（DSCP）：0x0，用于分类流量。
- 生存时间（TTL - Time To Live）：128，数据包可经过的最大路由器数目。
- 协议（Protocol）：0x1，表示这是 ICMP 协议。
- 总长度（Total Length, TL）：128 字节。
- 标识（Identification, ID）：0x19，用于唯一识别分组的序列号。
- 头部校验和（Checksum）：用于验证头部信息的正确性。
- 源 IP 地址（SRC IP）：192.168.1.12，发送者的 IP 地址。
- 目的 IP 地址（DST IP）：192.168.2.12，接收者的 IP 地址。
- 选项（Options, OPT）：0x0，可能用于各种 IP 功能，但在此为空。

ICMP：

- 类型（Type）：0x8，代表这是一个 ICMP 回显请求（ping 请求）。
- 代码（Code）：0x0，与特定的 ICMP 类型相关的附加信息。
- 校验和（Checksum）：用于确保 ICMP 消息的完整性。
- 标识符（Identifier, ID）：0x8，可能用于匹配请求与回复。

- 序列号（Sequence Number）：25，用于标记发送的 ICMP 请求的顺序。

3.5 PDU Information at Device: Router0（Outbound PDU Details）




这张图展示了 Cisco Packet Tracer 中，路由器（Router0）上的一个 ICMP 数据包的出站 PDU（协议数据单元）的详细信息。我们可以看到数据包的以太网 II 层，IP 层和 ICMP 层的信息，以及它们是如何准备离开路由器的。

以太网 II（Ethernet II）：

- 前导码（Preamble）：用于帧同步的二进制模式，这里以 101010...1011 展示。
- 目的 MAC 地址（DEST MAC）：00E0.8F48.E19B，指向的是下一跳或最终目的地址的硬件地址。

- 源 MAC 地址（SRC MAC）：000A.F306.DC02，代表路由器的发送接口的硬件地址。
- 类型（Type）：0x800，表明该帧是一个 IP 数据包。
- 数据（Data）：可变长度，携带 IP 数据包和其包含的 ICMP 消息。
- 帧检验序列（Frame Check Sequence, FCS）：0x0，用于错误检测（在实际网络中使用，但在模拟中可能不展示真实值）。

IP：

- 版本（Version）：4，指代 IPv4。
- 头部长度（Internet Header Length, IHL）：头部的字节长度。
- 差分服务代码点（Differentiated Services Code Point, DSCP）：0x0，用于指定数据包的服务类型。
- 总长度（Total Length, TL）：128 字节，表示整个 IP 数据包的长度。
- 标识（Identification, ID）：0x19，用于分片和重组的标识符。
- 生存时间（Time To Live, TTL）：127，每过一个路由器节点减 1。
- 协议（Protocol, PRO）：0x1，表示承载的是 ICMP 数据。
- 头部校验和（Checksum）：用于检测头部信息是否被更改。
- 源 IP 地址（Source IP, SRC IP）：192.168.1.12，发送 ICMP 请求的设备的 IP。
- 目的 IP 地址（Destination IP, DST IP）：192.168.2.12，接收 ICMP 请求的目的设备的 IP。

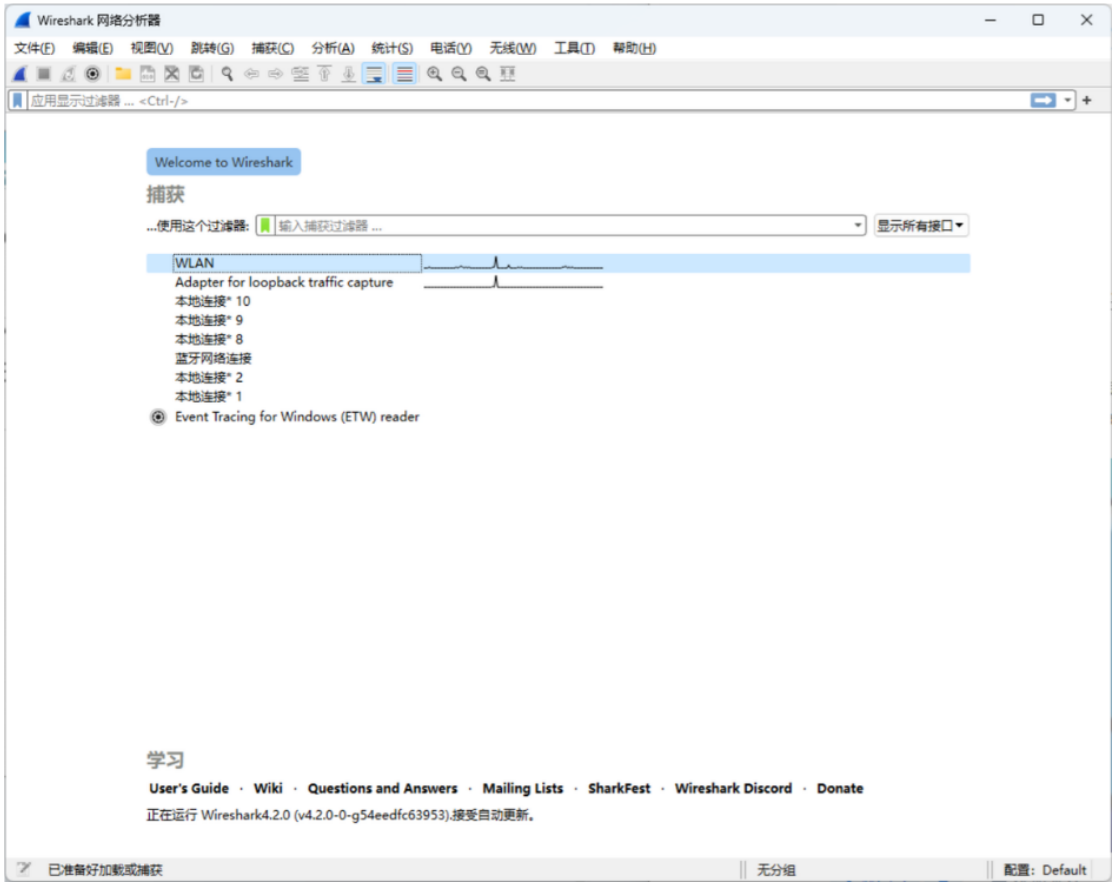
ICMP：

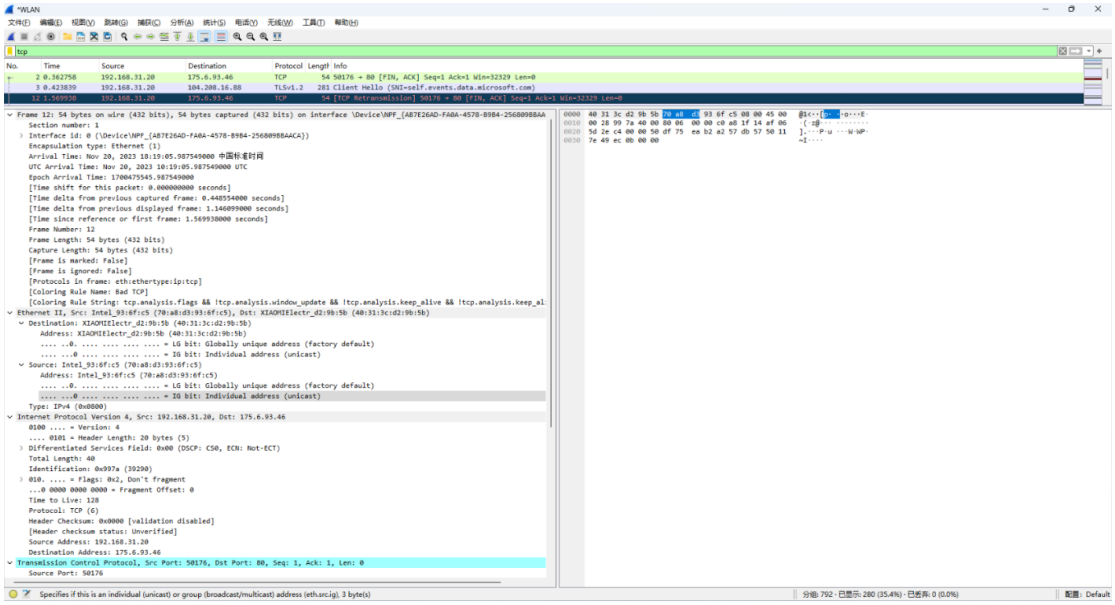
- 类型（Type）：0x8，代表 ICMP 回显请求，也就是 ping 请求。
- 代码（Code）：0x0，与 ICMP 类型相关的附加信息。
- 校验和（Checksum）：用于验证 ICMP 消息的完整性。
- 标识符（Identifier, ID）：0x8，可能用于将回显请求和回显应答匹配起来。
- 序列号（Sequence Number）：25，用于标记发送的 ICMP 请求的顺序。

4. 本机命令提示符输入 ipconfig/all 命令，查看本机的 MAC 地址，为 D4-54-8B-33-2B-7E。

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : tongji.edu.cn
   描述. . . . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   物理地址. . . . . . . . . . . . : D4-54-8B-33-2B-7E
   DHCP 已启用 . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . : 2001:da8:8002:6bd1:3da8:a8dd:269f:38c7(首选)
   临时 IPv6 地址. . . . . . . . . : 2001:da8:8002:6bd1:2928:8444:6090:5cad(首选)
   本地链接 IPv6 地址. . . . . . . : fe80::b6ff:9493:f8d0:9a9e%6(首选)
   IPv4 地址 . . . . . . . . . . . : 100.81.138.91(首选)
   子网掩码 . . . . . . . . . . . : 255.254.0.0
   获得租约的时间 . . . . . . . . : 2024年4月28日 18:43:28
   租约过期的时间 . . . . . . . . : 2024年4月28日 20:43:27
   默认网关. . . . . . . . . . . . : fe80::9e54:c2ff:fe0d:5002%6
                                     100.81.255.254
   DHCP 服务器 . . . . . . . . . . : 100.81.255.254
   DHCPv6 IAID . . . . . . . . . . : 64246923
   DHCPv6 客户端 DUID . . . . . . . : 00-01-00-01-29-5C-8A-6A-88-A4-C2-22-79-31
   DNS 服务器 . . . . . . . . . . : 202.120.190.208
                                     202.120.190.108
   TCPIP 上的 NetBIOS . . . . . . . : 已启用
```

5. 用 WireShark 抓取 MAC 数据包，选用 WLAN 方式进行抓包，查看 MAC 数据包字段内容，并解读。





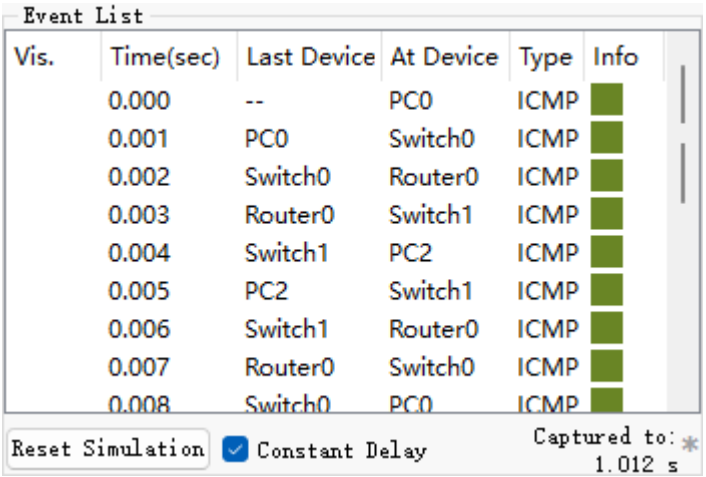

这张图来自 Wireshark，它捕获并详细展示了网络流量中的数据包信息。在这个特定的截图中，描述了一个 TCP 数据包，这个数据包包含了一个终止连接的请求（FIN 标志），并且确认了之前接收到的 TCP 段（ACK 标志）。下面是这些字段的解释以及包含的信息：

- 帧（Frame）：展示了该数据包在 Wireshark 捕获序列中的编号（第 12 个数据包），以及数据包的长度（54 字节）。它还告诉我们，数据包中包含了 Ethernet II、IP 和 TCP 这几个协议层。
- 以太网 II（Ethernet II）：
  - 目的 MAC 地址（Destination MAC Address）：一个唯一标识网络上接收设备物理地址的代码，这里是 XIAOMI 设备的地址（d2:9b:5b 结尾）。
  - 源 MAC 地址（Source MAC Address）：同样是一个唯一的代码，用于标识发送这个数据包的设备，这里是 IntelCor（93:6f:c5 结尾）。
  - 类型（Type）：表示这是一个 IPv4 协议的数据包（0x0800）。
- IPv4（Internet Protocol Version 4）：
  - 源 IP 地址（Source IP Address）：逻辑地址，标识发送数据包的设备，为 192.168.31.20。
  - 目的 IP 地址（Destination IP Address）：数据包的目的地逻辑地址，为 175.6.93.46。
  - 总长度（Total Length）：告诉我们整个 IP 数据包的长度。

- 生存时间（Time To Live, TTL）：设置为 128，这是数据包可以经过的最大路由器跳数，在到达目的地之前。

- TCP（Transmission Control Protocol）：
  - 源端口（Source Port）：本地端口号 50176，用于识别发送者的应用程序。
  - 目的端口（Destination Port）：端口号 80，通常用于 HTTP 服务。
  - 序列号（Sequence Number）：数据包的序列号为 1，用于确保数据按照发送顺序被接收。
  - 确认号（Acknowledgment Number）：确认号为 1，表示接收方已经正确接收到序列号为 1 的数据包，并期望下一个序列号。
  - 头部长度（Header Length）：TCP 头部长度为 20 字节，等于 5 个 32 位字。
  - 标志（Flags）：包含 FIN 和 ACK 标志，其中 FIN 表示发送方想要关闭连接，ACK 表示这是对先前收到数据包的确认。
  - 窗口大小（Window）：32329，表示接收方还可以接收多少字节的数据，这是 TCP 流量控制的一部分。
  - 校验和（Checksum）：0xec0b，这是一个检测数据包在传输过程中是否出错的数值。
  - 紧急指针（Urgent Pointer）：值为 0，表示没有紧急数据。

6. 分析在 Cisco Packet Tracer 中模拟 ICMP（ping 命令），ICMP 数据包转发过程中 MAC 地址变化情况。



- MAC 地址变化情况：

| Time(sec) | Last Device | At Device | Type | DEST MAC | SRC MAC |
|---|---|---|---|---|---|
| 0.000 | -- | PC0 | ICMP | 000A.F306.DC01 | 0090.21AD.CD14 |
| 0.001 | PC0 | Switch0 | ICMP | 000A.F306.DC01 | 0090.21AD.CD14 |
| 0.002 | Switch0 | Router0 | ICMP | 00E0.8F48.E19B | 000A.F306.DC02 |
| 0.003 | Router0 | Switch1 | ICMP | 00E0.8F48.E19B | 000A.F306.DC02 |
| 0.004 | Switch1 | PC2 | ICMP | 000A.F306.DC02 | 00E0.8F48.E19B |
| 0.005 | PC2 | Switch1 | ICMP | 000A.F306.DC02 | 00E0.8F48.E19B |
| 0.006 | Switch1 | Router0 | ICMP | 0090.21AD.CD14 | 000A.F306.DC01 |
| 0.007 | Router0 | Switch0 | ICMP | 0090.21AD.CD14 | 000A.F306.DC01 |
| 0.008 | Switch0 | PC0 | ICMP | 0090.21AD.CD14 | 000A.F306.DC01 |
| … | … | … | … | … | … |

- 起始 MAC 地址和目的 MAC 地址分析：

| Time (sec) | Last Device | At Device | Type | DEST MAC | SRC MAC |
|---|---|---|---|---|---|
| 0.000 | -- | PC0 | ICMP | Switch0 接口 MAC 地址 | PC0 MAC 地址 |
| 0.001 | PC0 | Switch0 | ICMP | Switch0 接口 MAC 地址 | PC0 MAC 地址 |
| 0.002 | Switch0 | Router0 | ICMP | Router0 MAC 地址 | Switch0 MAC 地址 |
| 0.003 | Router0 | Switch1 | ICMP | Switch1 接口 MAC 地址 | Router0 MAC 地址 |
| 0.004 | Switch1 | PC2 | ICMP | PC2 MAC 地址 | Switch1 接口 MAC 地址 |
| 0.005 | PC2 | Switch1 | ICMP | PC2 MAC 地址 | Switch1 接口 MAC 地址 |
| 0.006 | Switch1 | Router0 | ICMP | PC0 MAC 地址 | Switch0 接口 MAC 地址 |
| 0.007 | Router0 | Switch0 | ICMP | PC0 MAC 地址 | Switch0 接口 MAC 地址 |
| 0.008 | Switch0 | PC0 | ICMP | Switch0 接口 MAC 地址 | PC0 MAC 地址 |
| … | … | … | … | … | … |

**【分析讨论】**

**一、MAC 地址的重要性**

MAC 地址的不变性和唯一性保证了局域网内设备的可靠识别和数据链路层的准确通信。它是实现网络设备物理层寻址的关键，与 IP 地址相结合，实现了

从逻辑寻址到物理寻址的映射。

**二、ICMP 数据包转发中 MAC 地址的变化**

在实验中观察到，当 ICMP 数据包在内网中传输时，MAC 地址在通过路由器或交换机时会发生变化。这是因为：

- 在同一个子网内，交换机根据 MAC 地址表进行帧的转发。
- 而跨子网通信，路由器需要根据 IP 地址进行路由，然后将帧的目的 MAC 地址更改为下一跳的 MAC 地址或目的主机的 MAC 地址。

**三、ARP 的作用**

ARP 协议用于将网络层的 IP 地址解析成数据链路层的 MAC 地址。在本地子网内，如果主机需要知道另一个 IP 地址对应的 MAC 地址，它将广播一个 ARP 请求，询问哪台机器持有该 IP 地址。持有该 IP 地址的机器会以 ARP 响应的方式回复其 MAC 地址。

**四、MAC 地址与 IP 地址的联系与区别**

1. MAC 地址（Media Access Control Address）
   - 物理地址：MAC 地址通常被称为物理地址或硬件地址，因为它是固化在网络接口控制器硬件的。
   - 层次位置：它在 OSI 模型的数据链路层（第二层）使用。
   - 长度和格式：MAC 地址由 48 位组成，通常以六组两个十六进制数字表示（例如 00:1A:C2:7B:00:47）。
   - 分配方式：它由设备制造商分配，并通常不会改变。
   - 作用范围：在局域网内进行数据传输时使用，主要在同一个广播域内的设备之间传输帧。
   - 功能：它确保了帧能够在同一个网络段或局域网中正确地从一个物理设备传输到另一个物理设备。
2. IP 地址（Internet Protocol Address）
   - 逻辑地址：IP 地址是一个逻辑地址，与网络设备的位置有关。
   - 层次位置：它在 OSI 模型的网络层（第三层）使用。
   - 长度和格式：IPv4 地址由 32 位组成，分为 4 个 8 位的数字（例如 192.168.1.1），而 IPv6 地址由 128 位组成。

- 分配方式：IP 地址可以是静态分配的，也可以是通过动态主机配置协议（DHCP）动态分配的。
- 作用范围：它用于不同网络或广播域间的设备进行数据传输。
- 功能：IP 地址使设备能够在全球范围的互联网上找到彼此，并确保数据包能够从源头正确地路由到目的地。

3. MAC 地址与 IP 地址的联系
   - 相互转换：在局域网通信中，IP 地址需要转换为 MAC 地址以进行物理层传输，这通常通过 ARP 协议完成。
   - 配合使用：数据包从一个设备传输到另一个设备的过程中，同时使用 MAC 地址和 IP 地址，其中 IP 地址用于在网络间路由，MAC 地址用于在同一网络内的数据链路层传输。
   - 同一设备：在一台网络设备中，通常会同时配置有 MAC 地址和 IP 地址，两者共同工作确保数据包能够在网络中正确传输。

# 实验 22：IP 数据包分析实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/09 |

**【实验目的】**

1. 理解 IP 协议和数据包结构：学生将学习 IP 数据包的组成，包括首部和数据两部分的详细结构，了解各个字段的功能，例如版本、首部长度、总长度、标识、标志、片偏移、生存时间（TTL）、协议、首部校验和以及源地址和目的地址等。
2. 掌握 IP 数据包的封装和拆封过程：通过实验，学生将了解 IP 层是如何封装和拆封数据报来提供不可靠无连接的数据报传输服务的。
3. 学习 IP 数据包的传输和分片机制：实验中将介绍 IP 数据包在不同网络环境下的传输方式，以及如何处理数据报的分片和重组，特别是在跨越具有不同最大传输单元（MTU）值的网络时。
4. 使用网络分析工具进行数据包捕获和分析：学生将使用如 Wireshark 等网络分析工具，实际捕获和分析 IP 数据包。这不仅包括数据包的捕获，还包括如何读取和解释数据包中的信息。
5. 诊断网络问题和验证网络设计：通过对捕获的数据包进行分析，学生可以学习如何诊断网络中的问题，并验证网络设计和配置是否正确。
6. 实践网络安全和性能评估：学生将通过分析数据包来评估网络的安全性和性能，了解如何通过配置和优化来提高网络的效率和安全性。

**【实验原理】**

**一、IP 协议**

IP 协议（Internet Protocol）提供不可靠、无连接的数据报传输服务。IP 层提供的服务是通过对数据报进行封装和拆封实现的。IP 数据报的格式分为两个主要部分：报头和数据部分。报头部分包含确保数据正确传输所需的各种控制信息，而数据部分包括上层协议需要传输的数据。

1. IP 数据报文格式概览

IP 数据报由报头和数据两部分组成，报头用于携带传输控制信息，数据部分包含实际的传输数据。

2. 报头

报头的固定部分长度为 20 字节，是每个 IP 数据报文都包含的基础信息。可选字段的长度可变，可以根据需要包含更多的控制信息。

3. 报头的固定部分字段

- 版本：4 位，表示 IP 协议的版本号。常见的版本是 IPv4。
- 首部长度：4 位，指示报头的长度，单位为 4 字节。
- 区分服务：8 位，用于不同服务类型的需求。
- 总长度：16 位，表示整个数据报的长度，单位为字节。
- 标识：16 位，唯一标识一个数据报。
- 标志：3 位，控制数据报的分片行为。
- 片偏移：13 位，指示数据报在分片后的位置。
- 生存时间（TTL）：8 位，指示数据报在网络中的最大跳数。
- 协议：8 位，指示承载的数据使用的协议。
- 首部校验和：16 位，仅校验报头部分。
- 源地址和目的地址：各 4 字节，指示数据的源和目标。

4. 报头的可选部分

报头的可选字段长度可变，提供额外的传输控制、排错和安全选项，最大长度为 40 字节。

5. 报头校验

使用 16 位二进制反码求和算法，对报头部分进行校验。

6. 数据报分片

如果数据报的总长度超过网络的 MTU（最大传输单元），需要进行分片。每个分片都复制原数据报的报头，并修改相关字段以表示其位置和顺序。

7. 数据报的传输顺序

在传输时，数据按位序从高位到低位传输。

8. TOS（服务类型）

服务类型字段占用 8 位，设定了数据报的优先级、延迟、吞吐量和可靠性等特性。

9. 最大传输单元（MTU）

每个网络都有固定的 MTU，表示网络帧的最大长度。分片通常由路由器负责，以适应不同网络的 MTU。

10. 分片和重组

数据报被分片后，接收端主机会根据标识、标志和偏移量字段进行重组，恢复成原始数据报。

11. IP 选项

IP 选项字段用于控制数据报的传输过程，可设置传输路由、记录路径、时间戳等。常用的选项有：

- 源路由选择：严格或宽松地指定数据报的路径。
- 记录路由：记录数据报经过的路由器。
- 时间戳：记录数据报通过每个路由器的时间和地址。

**二、ARP 协议**

ARP（地址解析协议）是一种网络协议，用于在 IP 网络中将设备的 IP 地址转换为物理层的 MAC 地址，从而实现同一局域网中设备之间的通信。它通过广播 ARP 请求，目标设备回复其 MAC 地址，然后发送设备将此对应关系缓存，以便后续快速访问。ARP 对于以太网环境中的正常通信至关重要，但同时也易受 ARP 欺骗和缓存中毒等网络攻击的威胁。

ARP 消息的结构通常包括：

- 硬件类型：指定所用链路层协议，如以太网为 1。
- 协议类型：标识需要解析的上层协议，如 IPv4 为 0x0800。
- 硬件地址长度：表示 MAC 地址的长度。
- 协议地址长度：表示 IP 地址的长度。
- 操作码：指定 ARP 请求或回复（1 为请求，2 为回复）。
- 发送方 MAC 地址：发送设备的 MAC 地址。
- 发送方 IP 地址：发送设备的 IP 地址。
- 目标 MAC 地址：目标设备的 MAC 地址（请求时为空）。
- 目标 IP 地址：目标设备的 IP 地址。

**【实验设备】**

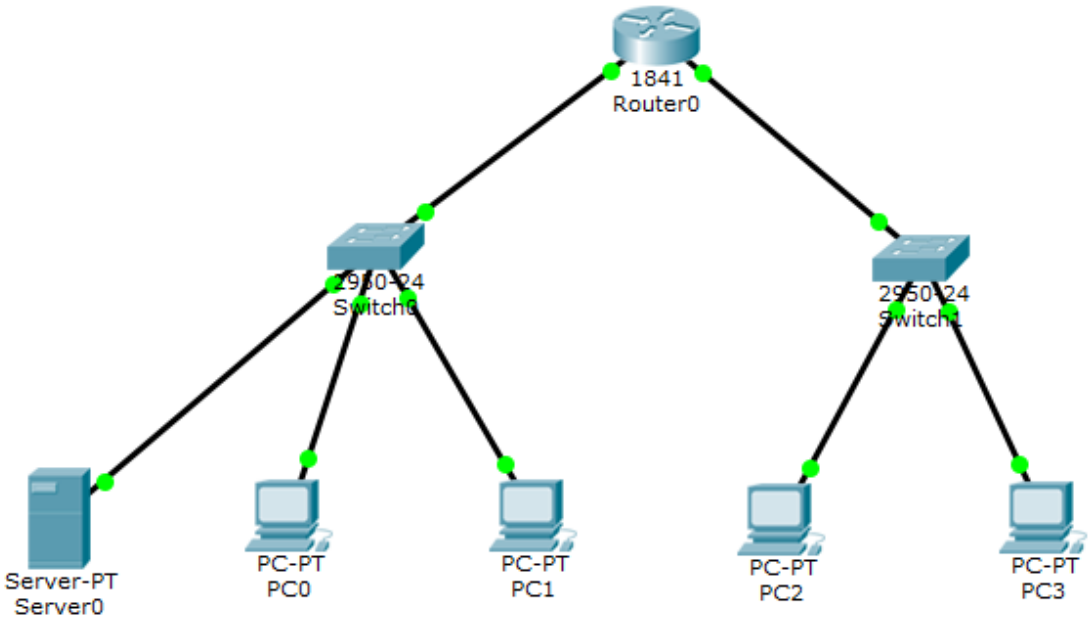
1. 操作系统：Windows 10

2. 网络环境：局域网

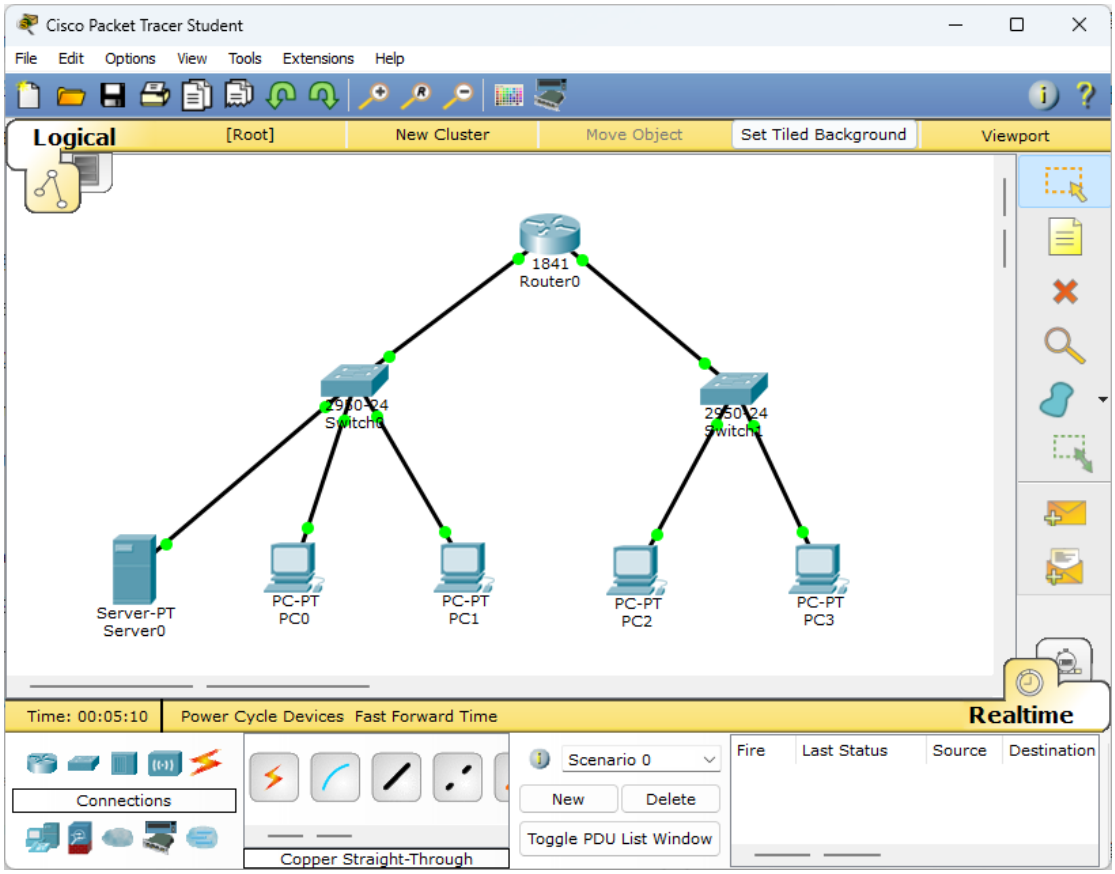
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

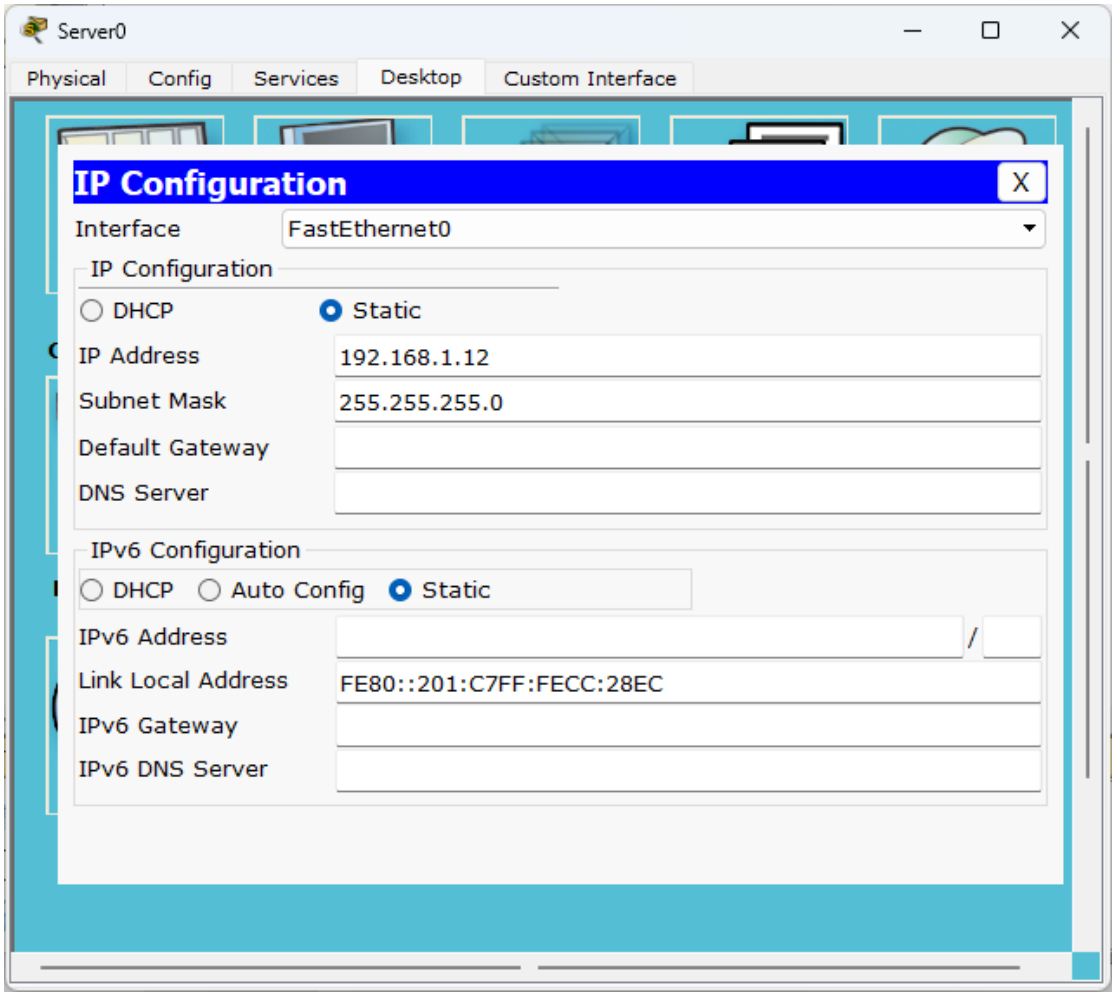
1. 规划网络地址及拓扑图。




2. 启动 Cisco Packet Tracer，按照上图连接网络，并参照先前实验进行配置。



3. 配置服务器，设置静态 IP 为 192.168.1.12，子网掩码为 255.255.255.0。

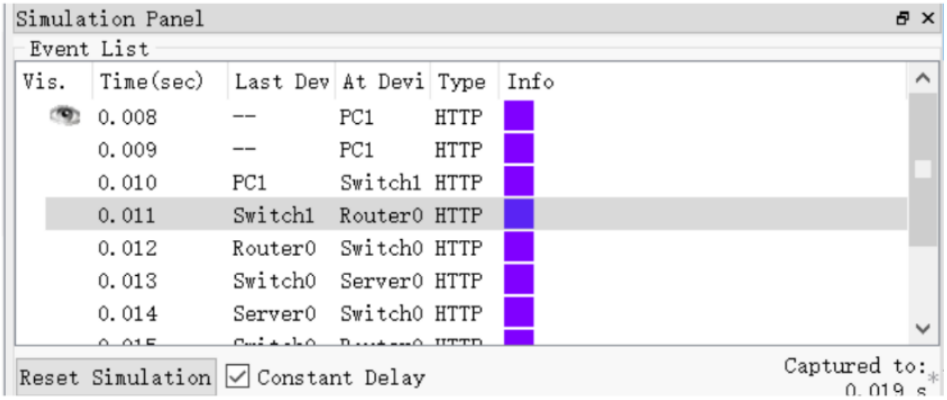


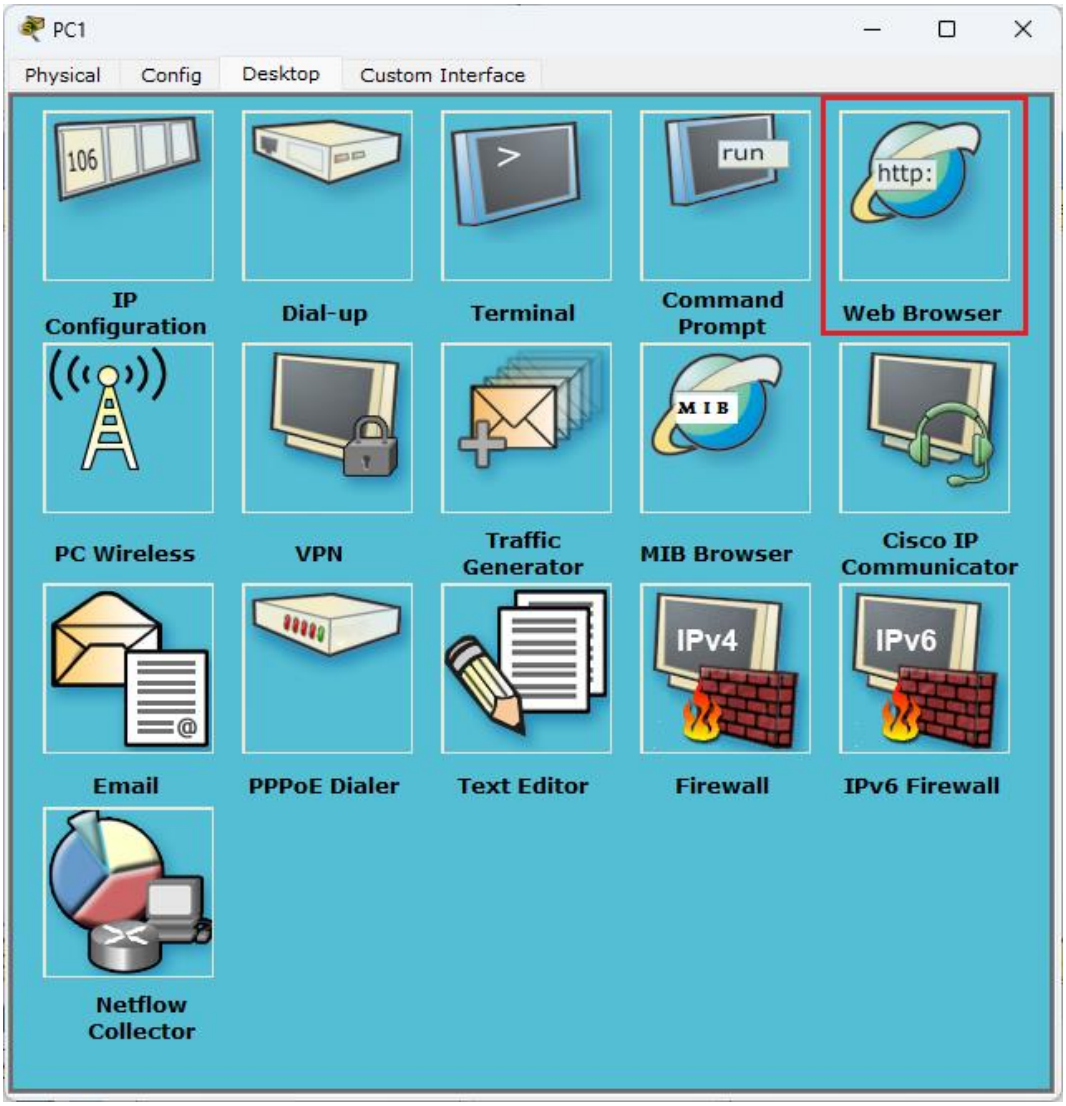

4. 从 Realtime 模式切换至 Simulation 模式。

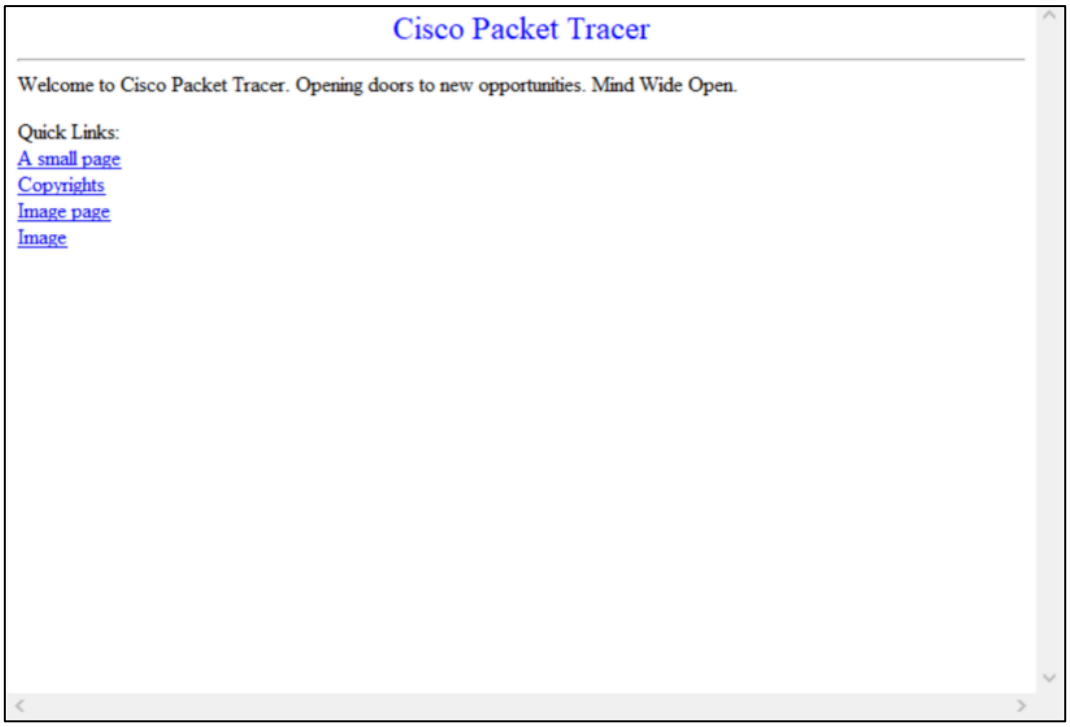
4.1 在 PC1 的 Web Browser 中输入服务器网址 http://192.163.1.12，产生 IP 数据报文。

4.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

4.3 在 Even List 中的 Info 栏可以查看相关信息。




PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
Dial-up
Terminal
Command Prompt
Web Browser
PC Wireless
VPN
Traffic Generator
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
Firewall
IPv6 Firewall
Netflow Collector


Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

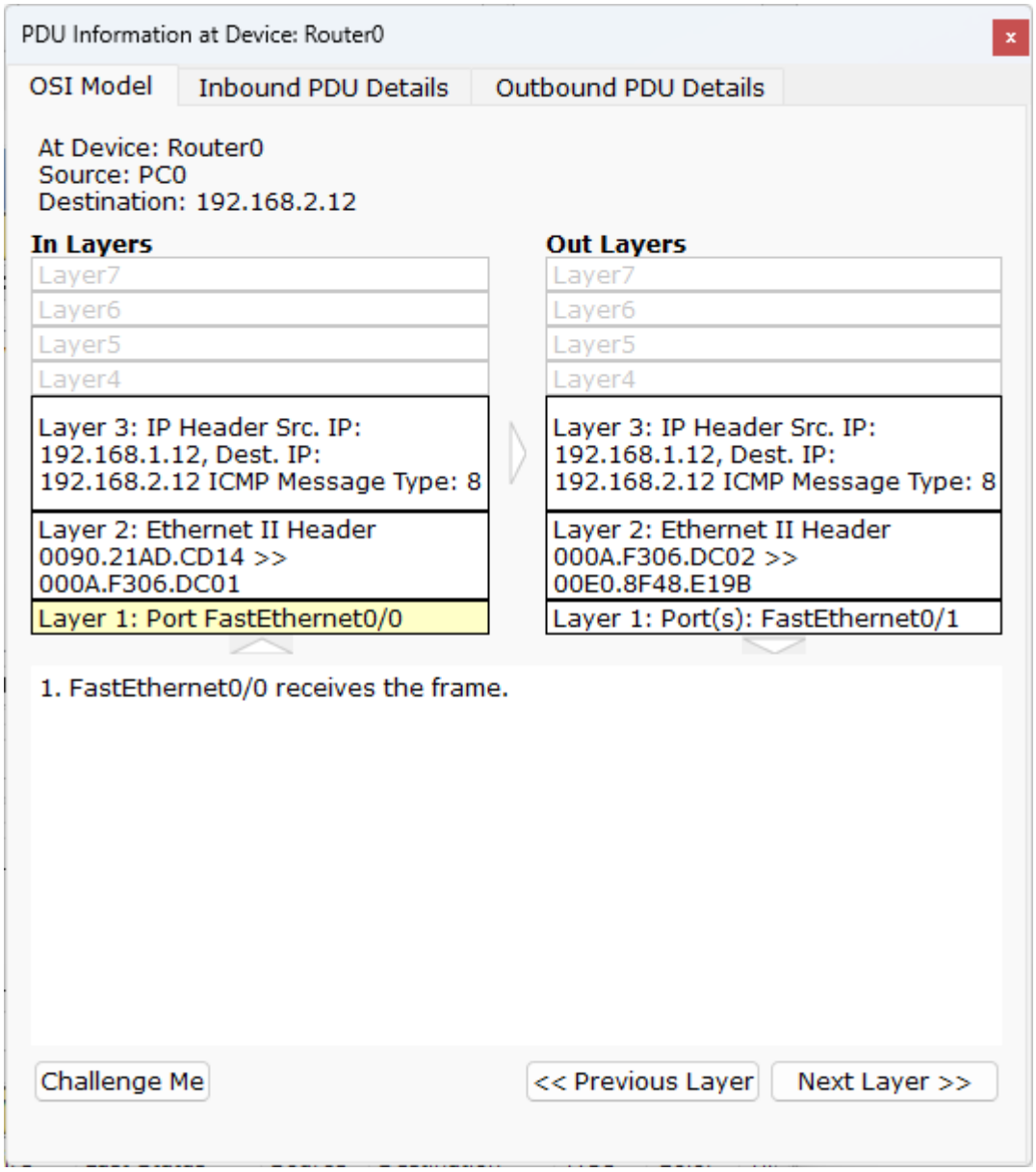
5. 分析 IP 数据报文。

6. 用 WireShark 抓取 IP 数据包，并解读。

**【实验现象】**

1. 从 Realtime 模式切换至 Simulation 模式，在 Even List 中的 Info 栏可以查看相关信息，这里对 Router0 的相关 Event 进行如下分析。

1.1 PDU Information at Device: Router0（OSI Model）




入站 PDU 细节（Inbound PDU Details）：

- 在设备：Router0
- 源地址（Source）：PC0
- 目的地址（Destination）：192.168.2.12

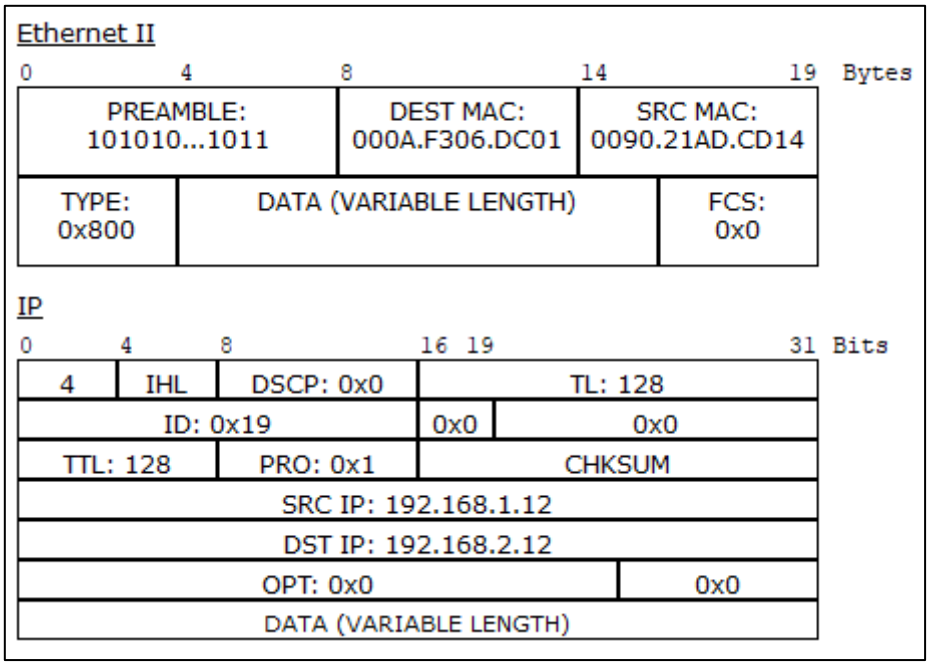
入站层（In Layers）信息显示数据包是如何被路由器接收的：

- Layer 3：IP 头信息显示源 IP 为 192.168.1.12，目的 IP 为 192.168.2.12。
- Layer 2：以太网 II 头信息展示源 MAC 地址为 0090.21AD.CD14，目的 MAC 地址为 000A.F306.DC01。
- Layer 1：表明该数据包是通过端口 FastEthernet0/0 进入路由器的。
- 出站 PDU 细节（Outbound PDU Details）

出站层（Out Layers）信息显示数据包在经过路由器处理后如何出站：

- Layer 3：IP 头部信息不变，仍然显示源 IP 为 192.168.1.12 和目的 IP 为 192.168.2.12。
- Layer 2：以太网 II 头信息此时展示的源 MAC 地址变为路由器的源 MAC 地址 000A.F306.DC02，而目的 MAC 地址变为另一个 MAC 地址（可能是下一个跳转目标的 MAC 地址）00E0.8F48.E19B。
- Layer 1：数据包现在是通过端口 FastEthernet0/1 离开路由器的。

1.2 PDU Information at Device: Router0（Inbound PDU Details）




以太网 II（Ethernet II）：

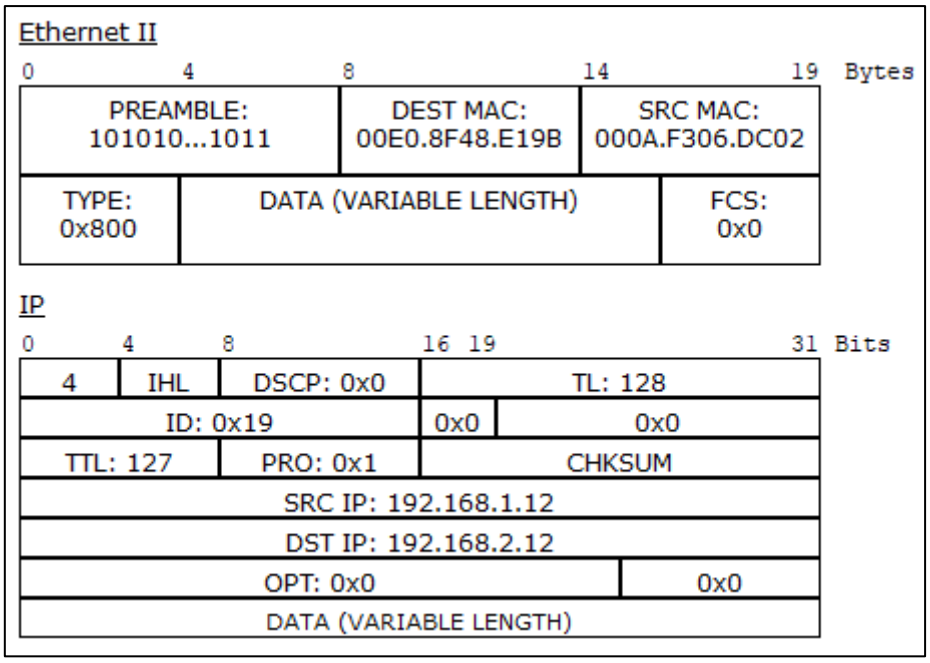
- 前导码（Preamble）：101010...1011，用于帧的同步。
- 目的 MAC 地址（DEST MAC）：000A.F306.DC01，是路由器接口或下一个跳转的 MAC 地址。
- 源 MAC 地址（SRC MAC）：0090.21AD.CD14，是发送者的 MAC 地址。

- 类型（Type）：0x800，说明后面跟随的是一个 IP 协议的数据包。
- 数据（Data）：可变长度。
- 帧检验序列（FCS）：0x0，用于检测帧在传输过程中的错误。

IP：

- 版本（Version）：4，指的是 IPv4。
- 头部长度（IHL - Internet Header Length）：通常表示 IP 头部的长度。
- 差分服务代码点（DSCP）：0x0，用于分类流量。
- 生存时间（TTL - Time To Live）：128，数据包可经过的最大路由器数目。
- 协议（Protocol）：0x1。
- 总长度（Total Length, TL）：128 字节。
- 标识（Identification, ID）：0x19，用于唯一识别分组的序列号。
- 头部校验和（Checksum）：用于验证头部信息的正确性。
- 源 IP 地址（SRC IP）：192.168.1.12，发送者的 IP 地址。
- 目的 IP 地址（DST IP）：192.168.2.12，接收者的 IP 地址。
- 选项（Options, OPT）：0x0，可能用于各种 IP 功能，但在此为空。

1.3 PDU Information at Device: Router0（Outbound PDU Details）




以太网 II（Ethernet II）：

- 前导码（Preamble）：用于帧同步的二进制模式，这里以 101010...1011

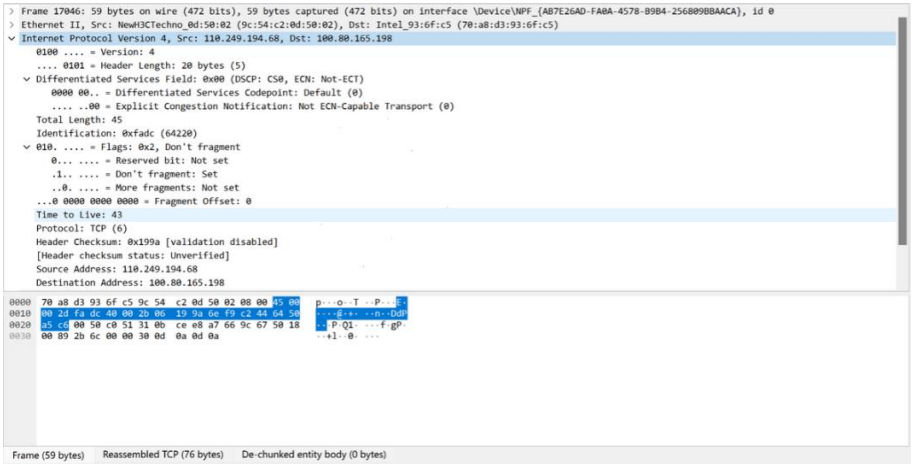
展示。

- 目的 MAC 地址（DEST MAC）：00E0.8F48.E19B，指向的是下一跳或最终目的地址的硬件地址。
- 源 MAC 地址（SRC MAC）：000A.F306.DC02，代表路由器的发送接口的硬件地址。
- 类型（Type）：0x800，表明该帧是一个 IP 数据包。
- 数据（Data）：可变长度。
- 帧检验序列（Frame Check Sequence, FCS）：0x0，用于错误检测（在实际网络中使用，但在模拟中可能不展示真实值）。

IP：

- 版本（Version）：4，指代 IPv4。
- 头部长度（Internet Header Length, IHL）：头部的字节长度。
- 差分服务代码点（Differentiated Services Code Point, DSCP）：0x0，用于指定数据包的服务类型。
- 总长度（Total Length, TL）：128 字节，表示整个 IP 数据包的长度。
- 标识（Identification, ID）：0x19，用于分片和重组的标识符。
- 生存时间（Time To Live, TTL）：127，每过一个路由器节点减 1。
- 协议（Protocol, PRO）：0x1。
- 头部校验和（Checksum）：用于检测头部信息是否被更改。
- 源 IP 地址（Source IP, SRC IP）：192.168.1.12。
- 目的 IP 地址（Destination IP, DST IP）：192.168.2.12。

2. 用 WireShark 抓取 IP 数据包，并解读如下：



- 版本 (Version): 4 - 这表明数据报使用的是 IPv4 协议。
- 首部长度 (Header Length): 20 字节（5 个 32 位字）- 这指示首部长度为 20 字节，不包含任何选项。
- 区分服务字段 (Differentiated Services Field, DSCP): 0x00 - 这表明没有设置特殊的区分服务或流量优先级。
- 总长度 (Total Length): 45 字节 - 这个字段指示整个 IP 数据报的长度（包括首部和数据）。但这似乎是截图中显示不全或误解的数值，因为 45 字节过小，不太可能仅包括首部和有效载荷。
- 标识 (Identification): 0xf4ac - 用于标识主机发送的每个数据报，关键用于数据报的分片和重组。
- 标志 (Flags): Don't Fragment (DF) - 这表示数据报不应被分片。
- 片偏移 (Fragment Offset): 0 - 表示该数据包是更大数据包的第一个片段或完整包。
- 生存时间 (Time to Live, TTL): 43 - 表示数据报可以在网络中的最大跳数。
- 协议 (Protocol): TCP (6) - 表明此数据报的上层协议是 TCP。
- 头部校验和 (Header Checksum): 用于检测在传输过程中首部信息是否出现错误。
- 源 IP 地址 (Source Address): 110.249.194.68 - 数据包的发送方地址。
- 目的 IP 地址 (Destination Address): 100.80.165.198 - 数据包的接收方地址。

**【分析讨论】**

**一、配置 Web 服务器并从客户端查看**

在配置了 Web 服务器并设置了静态 IP 地址之后，从客户端通过浏览器访问服务器网址能成功加载页面。这显示了 IP 地址和网络配置的正确性，以及 HTTP 协议在客户端和服务器之间如何工作。成功的页面加载证实了网络层到应用层的各个组件都被正确设置和协调工作。

**二、用 WireShark 抓取 IP 数据包**

使用 WireShark 捕获了在网络上传输的数据包。通过分析这些数据包，可以观察到 IP 头部的详细信息，包括但不限于源地址、目的地址、总长度、协议等。这有助于理解网络数据流动和协议的实际应用。WireShark 作为一个强大的网络分析工具，使我们能够实时捕获和分析网络交通，是网络管理和故障排除的关键工具。

**三、查看 IP 报文字段内容并解读**

实验详细解读了 IP 报文的各个字段，包括版本、首部长度、服务类型等。每个字段的解读不仅加深了对 IP 协议的理解，也揭示了数据包是如何根据不同的需求被处理和优先级分配的。特别是分片和重组机制的理解，对于处理跨网络数据传输至关重要。

**四、分析在 Packet Tracer 中 IP 报文情况**

通过使用 Packet Tracer，模拟了网络环境并观察了 IP 数据包在各网络设备间的传输过程。Packet Tracer 提供了一个动态的可视化界面，允许观察和跟踪数据包的每一步行为。通过详细的数据包信息，我们可以看到如何通过路由器和交换机处理和转发 IP 数据包，并且能够验证各种网络配置和协议的影响，比如 IP 路由、子网划分以及网络层的错误处理。

# 实验 23：ARP 消息分析实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/16 |

**【实验目的】**

1. 理解 ARP 协议的基本原理：学生将通过实验了解 ARP 协议的作用，即如何在以太网环境中将已知的 IP 地址转换为 MAC 地址。这涉及到 ARP 请求和响应消息的生成与处理。
2. 学习 ARP 消息的结构和字段内容：实验将指导学生详细了解 ARP 消息的格式，包括硬件类型、协议类型、硬件地址长度、协议地址长度、操作码、源硬件地址、源协议地址、目标硬件地址以及目标协议地址等字段。
3. 掌握 ARP 映射的静态与动态方式：学生将学习 ARP 协议中静态映射和动态映射的区别和应用场景，理解两者的优缺点以及适用环境。
4. 操作实践与网络工具应用：通过使用网络模拟工具如 Packet Tracer 和网络分析工具如 Wireshark，学生将实际操作 ARP 协议的配置和分析，包括抓取和解析 ARP 数据包。
5. 诊断和解决网络地址问题：通过分析 ARP 数据包，学生可以学习如何诊断网络中的地址解析问题，如 IP 地址和 MAC 地址不匹配、ARP 缓存中的脏数据等。
6. 提高网络安全意识：学生将探索 ARP 协议可能的安全漏洞，如 ARP 欺骗，并学习基本的防护措施。

**【实验原理】**

**一、ARP 协议的出现原因**

ARP（地址解析协议）是网络通信中的关键协议。在以太网中，通信依赖于设备的 MAC 地址，而不是 IP 地址。ARP 协议的主要作用是将已知的 IP 地址转换成目标设备的 MAC 地址，以确保数据能够正确传输。主机在进行通信时，需要先确定对方的 MAC 地址，这就是地址解析的过程，由 ARP 来完成。

**二、ARP 映射方式**

静态映射：管理员手动创建 ARP 表，将 IP 地址和 MAC 地址关联并保存在网络中每台机器上。这种方式有局限性，比如网络适配器的更换或移动电脑的迁移

可能导致物理地址的变化。因此，静态 ARP 表需要定期更新和维护，增加了操作的复杂性。

动态映射：每台主机只需知道对方的 IP 地址，即可使用 ARP 协议查找相应的 MAC 地址。ARP 协议是将 IP 地址映射为 MAC 地址，反向 ARP（RARP）则用于将 MAC 地址映射为 IP 地址。

**三、ARP 工作原理及流程**

请求：当一台主机想要发送数据给另一台主机时，它首先广播一个 ARP 请求，包含自身的 MAC 和 IP 地址以及目标设备的 IP 地址。由于此时不确定目标 MAC 地址，查询分组会在网络层中广播。

响应：局域网内的所有主机接收并处理这个 ARP 请求。如果某台主机的 IP 地址与请求中目标 IP 地址匹配，它会返回一个 ARP 响应，包含自身的 MAC 地址，以单播方式发送给请求主机。

**四、ARP 协议报文字段及抓包分析**

1. 报文格式
   - 硬件类型：标识运行 ARP 的网络类型，例如以太网为 1。
   - 协议类型：标识使用的协议，例如 IPv4 为 0800。
   - 硬件长度：表示物理地址的长度（以太网为 6 字节）。
   - 协议长度：表示逻辑地址的长度（IPv4 为 4 字节）。
   - 操作码：标识报文类型（1 为请求，2 为响应）。
   - 源硬件地址：发送方的 MAC 地址（以太网为 6 字节）。
   - 源逻辑地址：发送方的 IP 地址（IPv4 为 4 字节）。
   - 目标硬件地址：目标设备的 MAC 地址（请求时全 0，响应时 6 字节）。
   - 目标逻辑地址：目标设备的 IP 地址（IPv4 为 4 字节）。
2. 报文长度：ARP 报文总长度为 64 字节，包括以太网帧头和 ARP 数据。为了满足以太网最小帧长要求，报文中还添加填充字段。
3. CRC 字段：用于验证以太网帧的正确性。在填充完成后，通过算法计算的值会放入 CRC 字段，接收方可以验证数据包是否被修改。

**五、报文封装**

ARP 报文直接封装在数据链路帧中，以太网帧的类型字段标识此帧中携带的

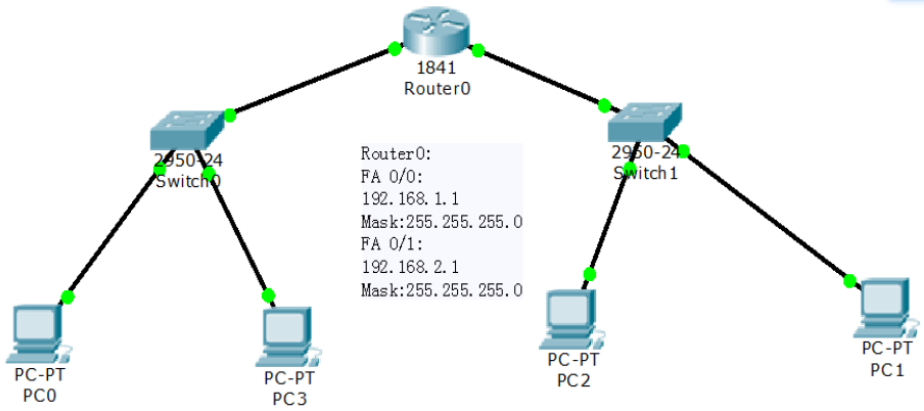
是 ARP 报文。

**【实验设备】**

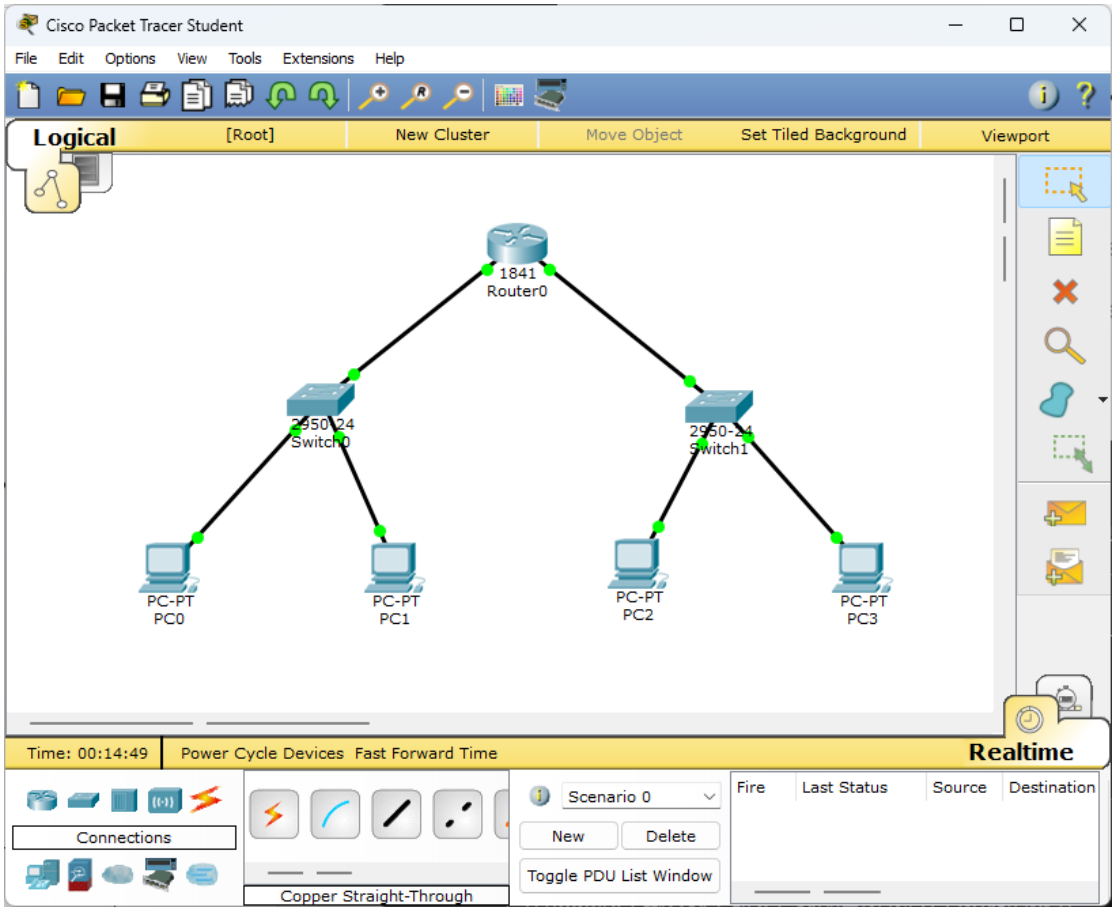
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。




2. 启动 Cisco Packet Tracer，按照上图连接网络，并参照先前实验进行配置。



3. 在 PC 机的命令行中输入如下命令，观察清除 ARP 前后当前主机的 ARP（地址解析协议）表内容。

```
arp -a
arp -d
arp -a
```

4. 在 Router 的 CLI 中输入如下命令，观察清除 ARP 前后当前路由的 ARP（地址解析协议）表内容。

```
show arp
clear arp-cache
show arp
```

5. 从 Realtime 模式切换至 Simulation 模式。

   5.1 在 PC1（192.168.2.13）的命令行中执行命令 ping 192.162.1.11（ping PC0）。

   5.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

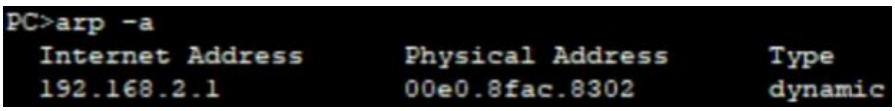
   5.3 在 Even List 中的 Info 栏可以查看相关信息。

6. 使用 WireShark 抓取 ARP 数据包，查看 ARP 报文字段内容，并解读。
7. 分析在 Packet Tracer 中 ARP 报文情况。
8. 查看本机的 ARP 内容。

**【实验现象】**

1. 在 PC 机的命令行中输入如下命令，显示当前主机的 ARP（地址解析协议）表内容。

```
arp -a
```




2. 在 PC 机的命令行中输入如下命令，清除当前主机的 ARP（地址解析协议）表内容。

```
arp -d
```

3. 在 PC 机的命令行中再次输入如下命令，显示当前主机的 ARP（地址解析协议）表内容。

```
arp -a
```

```
PC>arp -a
No ARP Entries Found
```

4. 在 Router 的 CLI 中输入如下命令，查看当前路由的 ARP（地址解析协议）表内容。

```
show arp
```

```
Router>show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -    0007.EC20.5201  ARPA   GigabitEthernet0/0
Internet  192.168.1.13           8    0060.5CD8.8C20  ARPA   GigabitEthernet0/0
Internet  192.168.2.1            -    0007.EC20.5202  ARPA   GigabitEthernet0/1
Internet  192.168.2.11           8    00D0.BC2C.850B  ARPA   GigabitEthernet0/1
Internet  192.168.2.12           7    0010.1123.C50E  ARPA   GigabitEthernet0/1
```

5. 在 Router 的 CLI 中输入如下命令，清除当前路由的 ARP（地址解析协议）表内容。

```
clear arp-cache
```

6. 在 Router 的 CLI 中再次输入如下命令，查看当前路由的 ARP（地址解析协议）表内容。

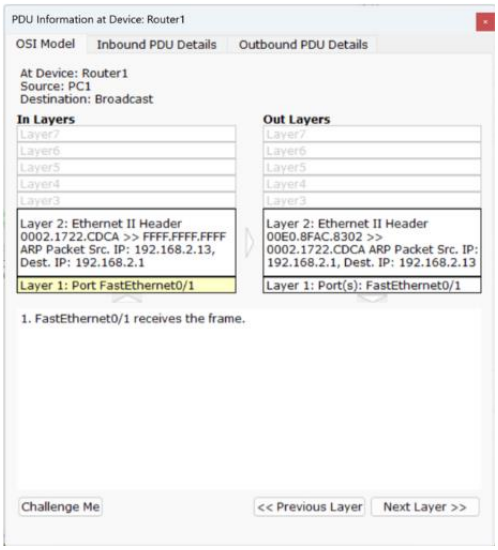
```
show arp
```

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.13           -    Incomplete      ARPA   GigabitEthernet0/0
Internet  192.168.2.11           -    Incomplete      ARPA   GigabitEthernet0/1
Internet  192.168.2.12           -    Incomplete      ARPA   GigabitEthernet0/1
Internet  192.168.1.1            -    0007.EC20.5201  ARPA   GigabitEthernet0/0
Internet  192.168.2.1            -    0007.EC20.5202  ARPA   GigabitEthernet0/1
```

**【分析讨论】**

**一、使用 WireShark 抓取 ARP 数据包，查看 ARP 报文字段内容，并解读**

1. PDU Information at Device: Router1（OSI Model）




这张图展示了一个典型的网络数据包在路由器处理中的入站和出站信息，特

别是针对 ARP（地址解析协议)请求的处理。这个图中详细地描述了 OSI 模型中的不同层级如何处理 ARP 请求和响应。

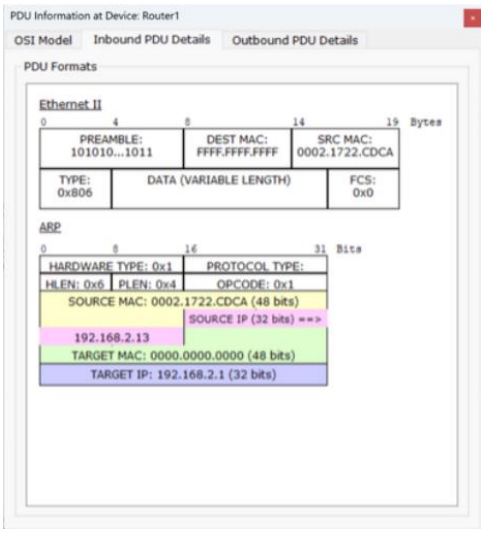
左侧（Inbound PDU Details)：

- At Device: Router1：显示该信息来自 Router1 设备。
- Source：PC1：数据包源自 PC1。
- Destination：Broadcast：这是一个广播包，目标是所有设备。
- Layers：
  - Layer 1：物理层，指出数据包通过 Router1 的 FastEthernet0/1 端口接收。
  - Layer 2：数据链路层，展示了 Ethernet II 帧头信息。源 MAC 地址为 0002.1722.CDCA，目标 MAC 地址为广播地址 FFFF.FFFF.FFFF。ARP 请求包的源 IP 为 192.168.2.13，目标 IP 为 192.168.2.1。

右侧（Outbound PDU Details)：

- 同样在 Router1 设备上显示出站的 PDU（协议数据单元）细节。
- Layers：
  - Layer 1：物理层，数据包通过相同的 FastEthernet0/1 端口发送出去。
  - Layer 2：数据链路层，显示了 Ethernet II 帧头信息。此时源 MAC 地址为 000E.8FAC.8302，目标 MAC 地址为 0002.1722.CDCA。ARP 响应的源 IP 为 192.168.2.1，目标 IP 为 192.168.2.13。

2. PDU Information at Device: Router1（Inbound PDU Details）



这张图详细展示了在Router1设备上接收的ARP请求的协议数据单元(PDU)的格式。具体内容分为Ethernet II帧格式和ARP协议部分，下面是各部分的详细解释：

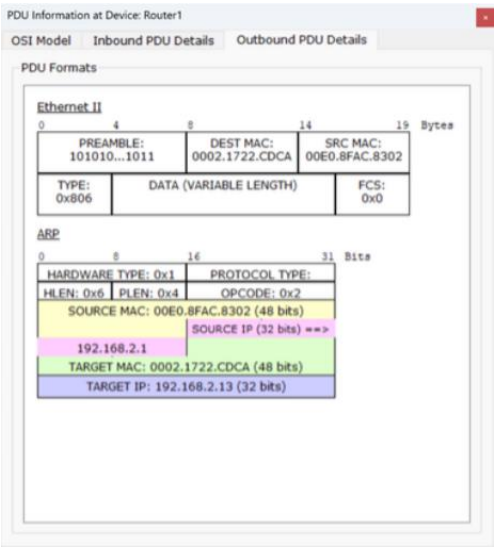
Ethernet II：

- Preamble（前导码）：起始部分为101010...1011，这部分用于同步网络设备之间的时钟频率，以确保数据的正确解读。
- Destination MAC（目标MAC地址）：为FFFF.FFFF.FFFF，这是一个广播地址，表示该ARP请求被发送到所有设备。
- Source MAC（源MAC地址）：为0002.1722.CDCA，这是发送该请求的设备的物理地址。
- Type（类型）：0x806，表示这个帧携带的数据是ARP协议的数据。
- Data（数据）：数据部分是可变长度的，包括ARP请求的具体内容。
- FCS（帧检验序列）：为0x0，用于错误检测的帧尾，虽然在此图示中显示为0，实际操作中由网络设备计算并添加。

ARP：

- Hardware Type（硬件类型）：0x1，表示这是以太网（Ethernet）。
- Protocol Type（协议类型）：0x0800，表示上层协议是IP。
- HLEN（硬件地址长度）：0x06，表示硬件地址（MAC地址）的长度为6字节。
- PLEN（协议地址长度）：0x04，表示协议地址（IP地址）的长度为4字节。
- Opcode（操作码）：0x01，表示这是一个ARP请求（请求MAC地址）。
- Source MAC Address：0002.1722.CDCA，请求方的物理地址。
- Source IP Address：192.168.2.13，请求方的IP地址。
- Target MAC Address：0000.0000.0000，目标方的MAC地址在请求时未知，因此全为0。
- Target IP Address：192.168.2.1，目标方的IP地址，即发送方希望获取MAC地址的IP地址。

3. PDU Information at Device: Router1（Outbound PDU Details）




这张图展示了从 Router1 发出的一个 ARP 响应的协议数据单元（PDU）的详细信息。这是对之前 ARP 请求的回应，具体内容如下：

Ethernet II：

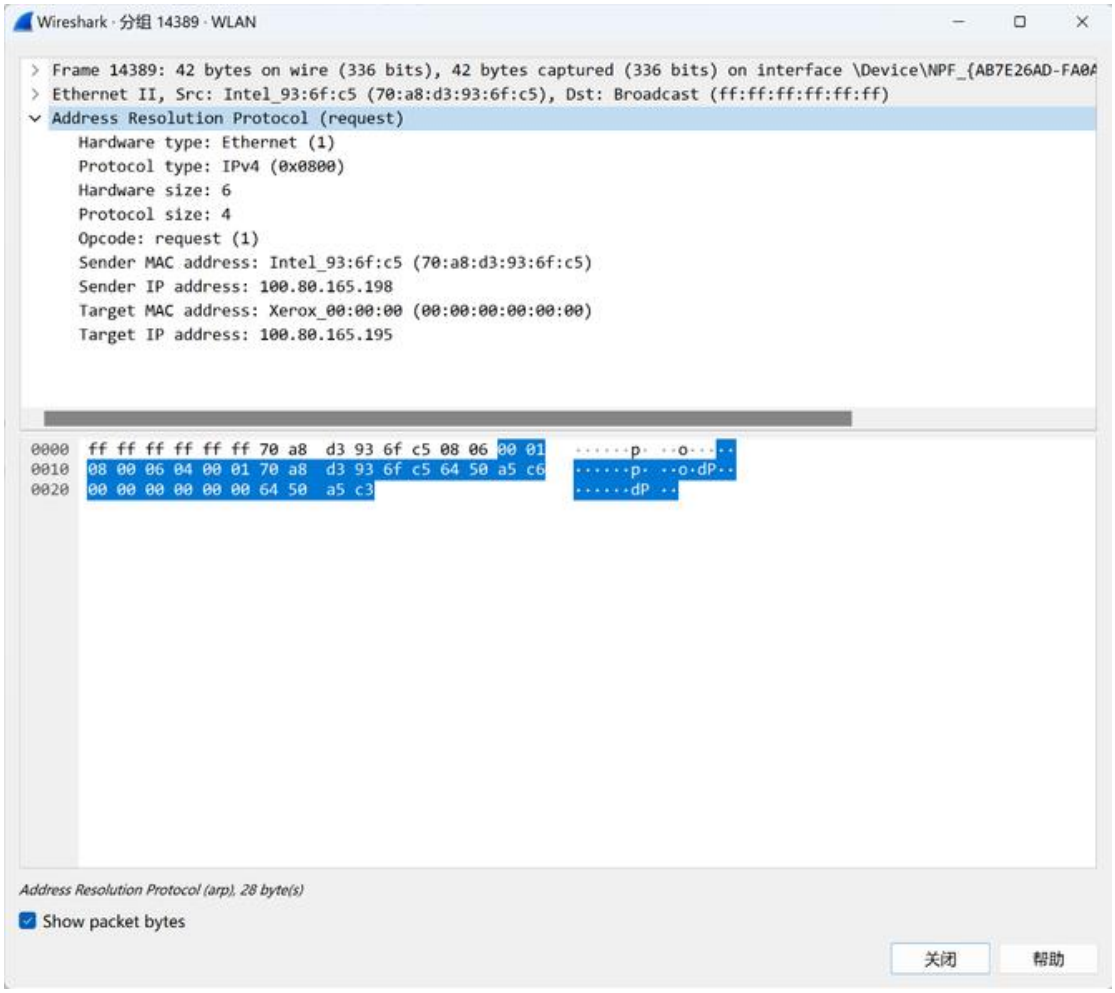
- Preamble（前导码）：为 101010...1011，用于时钟同步，以确保接收方能正确解析接下来的数据。
- Destination MAC（目标 MAC 地址）：为 0002.1722.CDCA，即发出 ARP 请求的设备的物理地址。
- Source MAC（源 MAC 地址）：为 00E0.8FAC.8302，即响应 ARP 请求的设备的物理地址。
- Type（类型）：0x806，指明这是一个 ARP 协议的数据包。
- Data（数据）：包含了 ARP 响应的详细内容。
- FCS（帧检验序列）：0x0，用于错误检测的帧尾，在此图中为示意，实际中会由设备计算并添加。

ARP：

- Hardware Type（硬件类型）：0x1，表示此 ARP 响应是针对以太网环境的。
- Protocol Type（协议类型）：0x0800，表示协议是 IP。
- HLEN（硬件地址长度）：0x06，表示硬件地址（MAC 地址）长度为 6 字节。
- PLEN（协议地址长度）：0x04，表示协议地址（IP 地址）长度为 4 字节。
- Opcode（操作码）：0x02，表示这是一个 ARP 响应。

- Source MAC Address：00E0.8FAC.8302，响应方的物理地址。
- Source IP Address：192.168.2.1，响应方的 IP 地址。
- Target MAC Address：0002.1722.CDCA，目标方（即请求方）的物理地址。
- Target IP Address：192.168.2.13，目标方的 IP 地址。

## 二、分析在 Packet Tracer 中 ARP 报文情况




下面对 Packet Tracer 中 ARP 报文情况进行分析：

Ethernet II：

- 源 MAC 地址：Intel_93:6f:c5（70:a8:d3:93:6f:c5）发送 ARP 请求的设备的物理地址。
- 目的 MAC 地址：Broadcast（ff:ff:ff:ff:ff:ff）表明这是一个广播消息，所有在网络上的设备都会接收这个包。
- 类型：0x0806 表示这个帧是 ARP 数据包。

ARP 报文：

- 硬件类型：1（Ethernet），这表明 ARP 请求是在以太网环境中使用的。
- 协议类型：0x0800（IPv4），这表明 ARP 请求是为了解析 IPv4 地址。
- 硬件地址长度：6，指出 MAC 地址使用 6 个字节。
- 协议地址长度：4，指出 IPv4 地址使用 4 个字节。
- 操作码：1（request），这表示此 ARP 包是一个请求包。
- 发送者 MAC 地址：Intel_93:6f:c5（70:a8:d3:93:6f:c5）同 Ethernet 头部的源地址。
- 发送者 IP 地址：100.80.165.198，发起 ARP 请求的设备的 IP 地址。
- 目标 MAC 地址：00:00:00:00:00:00，在请求时目标 MAC 地址未知，通常设置为全零。
- 目标 IP 地址：100.80.165.195，发起 ARP 请求的设备希望得到此 IP 地址的 MAC 地址。

**三、查看本机的 ARP 内容**

```
C:\Users\lenovo>arp -a

接口: 192.168.178.1 --- 0x2
  Internet 地址         物理地址              类型
  192.168.178.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 100.81.138.91 --- 0x6
  Internet 地址         物理地址              类型
  100.81.255.254        9c-54-c2-0d-50-02     动态
  100.81.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.216.1 --- 0x1b
  Internet 地址         物理地址              类型
  192.168.216.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

在 Windows 命令提示符中输入 arp -a，我们可以看到三个网络接口的 ARP

表信息。每个接口列出了与之相关联的 IP 地址、相应的物理地址（MAC 地址）和条目类型（静态或动态）。以下是各部分的具体解释：

1. 接口：192.168.178.1 --- 0x2
   - IP 地址 192.168.178.255：这是一个子网广播地址，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态，表示这个地址是用于广播消息到本地网络上的所有设备。
   - IP 地址 224.0.0.22，224.0.0.251，224.0.0.252：这些都是多播地址，对应的 MAC 地址以 01-00-5e 开头，根据多播 IP 到 MAC 地址映射的标准来设定，也都是静态条目。
   - IP 地址 239.255.255.250：同样是一个多播地址，用于特定的多播服务，如 SSDP（简单服务发现协议），MAC 地址同样为静态。
2. 接口：100.81.138.91 --- 0x6
   - IP 地址 100.81.255.254：这个地址可能是该接口的默认网关或者某个特定服务的地址，MAC 地址为 9c-54-c2-0d-50-02，标记为动态，表示这个地址是从网络上动态学习的。
   - IP 地址 100.81.255.255：这是该子网的广播地址，用于广播消息到这个特定子网的所有设备，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态。
   - 其余 IP 地址：包括多播地址和广播地址，与第一个接口的描述相同。
3. 接口：192.168.216.1 --- 0x1b
   - IP 地址 192.168.216.255：这是该子网的广播地址，用于广播消息到这个特定子网的所有设备，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态。
   - 其余 IP 地址：包括多播地址和广播地址，与前面的接口描述相同。

## 四、实验现象分析与讨论

1. ARP 表的初步观察

在使用 arp -a 命令查看 ARP 表时，可以看到本机已知的网络设备的 IP 地址和 MAC 地址列表。这显示了当前设备已经学习到的网络内部的 IP 到 MAC 地址映射。

2. 清除 ARP 缓存后的变化

执行 arp -d 清除 ARP 缓存后，再次使用 arp -a 查看 ARP 表时，表中内容减

少或显示为空。清除 ARP 缓存后，本机删除了所有动态学习的 IP 到 MAC 地址映射。这表明 ARP 缓存是动态的，设备通过网络通信实时更新这些信息。

3. ARP 缓存自动恢复

一段时间后，再次使用 arp -a 命令，发现 ARP 表已经重新填充了一些条目。这说明操作系统和网络设备在网络活动中自动重新学习了 IP 到 MAC 的映射这可能通过 ARP 请求和响应，或通常的网络交互过程自动完成。

4. 模拟 ARP 请求和响应

在 Cisco Packet Tracer 或 Wireshark 中模拟并抓取 ARP 数据包，观察到发送 ARP 请求后，接收到了 ARP 响应。这一现象验证了 ARP 协议的工作机制。请求被发送到广播地址，网络上所有设备均接收此请求，但只有 IP 地址匹配的设备才回应其 MAC 地址，这是典型的 ARP 查询流程。

# 实验 24：TCP 数据分析实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/16 |

**【实验目的】**

1. 理解 TCP 报文结构：学生将学习 TCP 报文段的各个字段，包括端口号、序号、确认号、数据偏移、控制位（如 SYN, ACK, FIN 等）、窗口大小、校验和、紧急指针等的作用和意义。
2. 掌握 TCP 的三次握手和四次挥手过程：通过实验，学生将详细了解 TCP 连接的建立和终止过程，即所谓的“三次握手”和“四次挥手”。这些知识对于理解网络通信的可靠性和效率至关重要。
3. 分析 TCP 的流量控制和拥塞控制机制：实验中，学生将观察和分析 TCP 如何通过窗口调整机制来进行流量控制，以及如何通过拥塞控制算法来响应网络中的拥塞情况。
4. 使用网络分析工具：学生将使用如 Wireshark 这类网络分析工具来捕获和分析 TCP 数据包。通过实际数据包的分析，学生可以更好地理解理论知识在实际网络通信中的应用。
5. 诊断网络问题：通过分析 TCP 数据段，学生能学习如何诊断网络中的问题，例如乱序数据包、丢包、重复确认等，并理解这些问题对网络性能的影响。
6. 实践和加深网络协议栈的理解：此实验不仅帮助学生加深对 TCP 协议的理解，还能够帮助他们了解更多关于网络层到应用层之间如何交互和协作的知识。

**【实验原理】**

**一、TCP 概述**

TCP（传输控制协议）是传输层的基于连接的协议，提供可靠的全双工数据传输。它通过序号和确认号机制确保数据按序传递且无损坏，并利用窗口机制进行流量控制，以及采用拥塞控制算法防止网络拥堵。虽然 TCP 需要在端系统中维护连接状态，带来一定的时间和空间开销，但其可靠性和数据完整性使其广泛应用于需要稳定传输的场景。相比之下，UDP 不维护连接状态，开销较小，适用于对传输速度要求高而对可靠性要求低的实时应用。

**二、TCP 的报文格式**

TCP 报文是 TCP 层传输的数据单元，也叫报文段。

<table>
<tr><td colspan="10">TCP报文</td></tr>
<tr><td colspan="8">源端口号16bit</td><td colspan="2">目的端口号16bit</td></tr>
<tr><td colspan="10">序号32bit</td></tr>
<tr><td colspan="10">确认号32bit</td></tr>
<tr><td>首部长度<br>4BIT</td><td>保留6BIT</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">接收窗口16bit</td></tr>
<tr><td colspan="8">检验和16bit</td><td colspan="2">紧急数据指针16bit</td></tr>
<tr><td colspan="10">选项(变长)</td></tr>
<tr><td colspan="10">用户数据变长</td></tr>
</table>

## 三、TCP 的报文字段

TCP 报文段由多个字段组成,每个字段在 TCP 传输过程中扮演着不同的角色。以下是这些字段的详细介绍：

1. 源端口：标识发送数据的应用进程，用于确定数据的返回地址。
2. 目的端口：标识接收数据的应用进程，指明接收方计算机上的应用程序接口。
3. 序号：表示报文段中的第一个字节的序号，确保数据按序到达。例如，如果报文段序号为 300，数据部分为 100 字节，则下一个报文段的序号为 400。
4. 确认号（ACK）：指示下一个期待收到的字节序号，表明之前的所有数据已正确接收。只有当 ACK 标志为 1 时才有效。
5. 数据偏移/首部长度：4 位字段，表示 TCP 报头的长度（以 32 位字为单位）。首部长度最大可为 60 字节。
6. 保留字段：为将来用途预留，一般置为 0。
7. 控制位：
   - URG：紧急指针标志，为 1 时表示紧急指针有效。
   - ACK：确认序号标志，为 1 时表示确认号有效。
   - PSH：Push 标志，为 1 表示接收方应尽快将报文段交给应用程序。
   - RST：重置连接标志，用于重置连接或拒绝非法的报文段。
   - SYN：同步序号标志，用于建立连接。
   - FIN：结束标志，用于释放连接。

8. 窗口：16 位字段，指示接收端的缓存大小，用于流量控制，最大值为 65535 字节。
9. 校验和：用于校验整个 TCP 报文段（包括头部和数据部分），确保数据完整性。
10. 紧急指针：在 URG 标志为 1 时有效，指示紧急数据的最后一个字节的序号。
11. 选项和填充：包含可选字段，如最大报文段大小（MSS）。选项字段的长度不定，需填充到 32 位整数倍。
12. 数据部分：可选字段，包含实际传输的数据。在连接建立和终止时，报文段仅包含 TCP 首部。

## 四、TCP 连接过程

TCP 连接过程包括“建立连接的三次握手”和“断开连接的四次挥手”，这两个过程确保了连接的可靠性和有序性。

### （一）三次握手（Three-way Handshake）

建立一个 TCP 连接时，需要客户端和服务器之间进行三次握手。其目的是建立 TCP 连接，并同步双方的序列号和确认号，同时交换窗口大小信息。

1. 第一次握手：
   - 客户端发送一个 SYN（同步序号）标志位为 1 的报文段，指明要连接的服务器端口和初始序列号 X。这个报文段表示客户端希望建立连接。
   - 服务器接收到这个报文段后，处于 SYN_RECEIVED 状态。
2. 第二次握手：
   - 服务器收到客户端的 SYN 报文后，回应一个 SYN 和 ACK（确认）标志位均为 1 的报文段。确认号为 X+1，表示服务器已经收到并确认了客户端的请求。
   - 这个报文段的初始序列号为 Y。
   - 客户端接收到这个报文段后，处于 SYN_ACK_RECEIVED 状态。
3. 第三次握手：
   - 客户端收到服务器的 SYN-ACK 报文后，再次发送一个 ACK 标志位为 1 的报文段，确认号为 Y+1，表示客户端已经收到服务器的确认。
   - 这个报文段的序列号为 X+1。

- 服务器接收到这个报文段后，连接进入 ESTABLISHED 状态，客户端也进入 ESTABLISHED 状态。

（二）四次挥手（Four-way Handshake）

断开一个 TCP 连接需要发送四个报文段，任何一方都可以主动发起断开连接的请求。

1. 第一次挥手：
   - 发起方（客户端或服务器）发送一个 FIN（结束）标志位为 1 的报文段，表示没有数据要发送了。
   - 对方接收到这个报文段后，处于 CLOSE_WAIT 状态。
2. 第二次挥手：
   - 接收方回应一个 ACK 标志位为 1 的报文段，确认号为发起方的序列号加 1。
   - 发起方接收到这个报文段后，处于 FIN_WAIT_2 状态。
3. 第三次挥手：
   - 接收方如果也没有数据要发送，发送一个 FIN 标志位为 1 的报文段，表示同意断开连接。
   - 发起方接收到这个报文段后，处于 TIME_WAIT 状态。
4. 第四次挥手：
   - 发起方回应一个 ACK 标志位为 1 的报文段，确认号为接收方的序列号加 1。
   - 接收方接收到这个报文段后，进入 CLOSED 状态。
   - 发起方等待一段时间后也进入 CLOSED 状态，确保对方接收到 ACK 后才彻底断开连接。

（三）SYN 攻击

在三次握手过程中，攻击者伪造大量不存在的 IP 地址发送 SYN 报文，服务器回复 SYN-ACK 报文并等待确认。由于源地址不存在，服务器需要不断重发，导致未连接队列被占用，正常请求被拒绝，系统性能下降甚至瘫痪。

**【实验设备】**

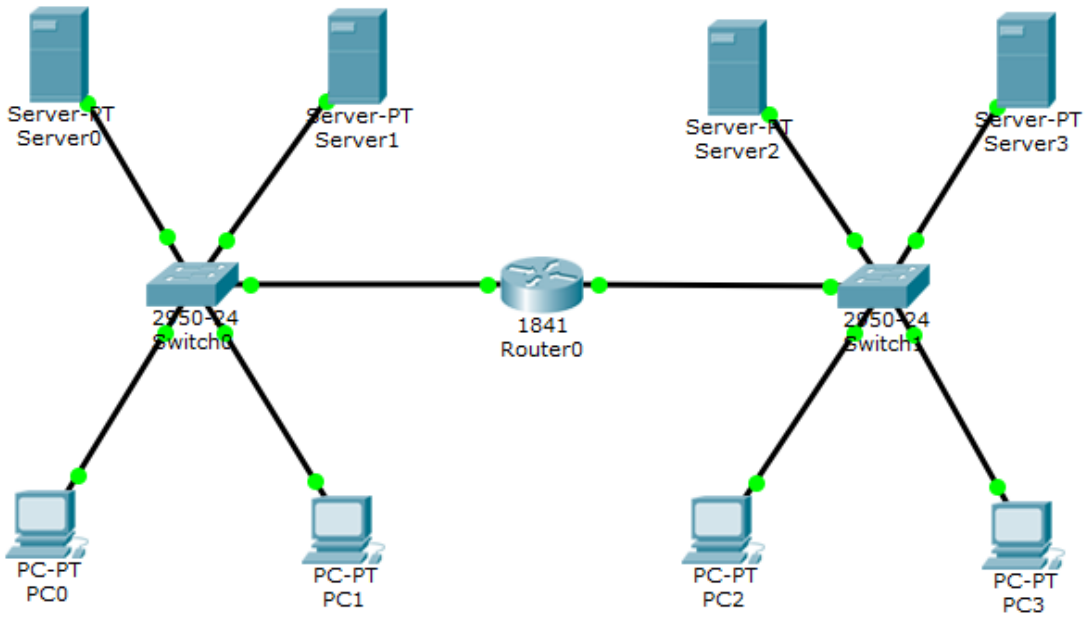
1. 操作系统：Windows 10

2. 网络环境：局域网

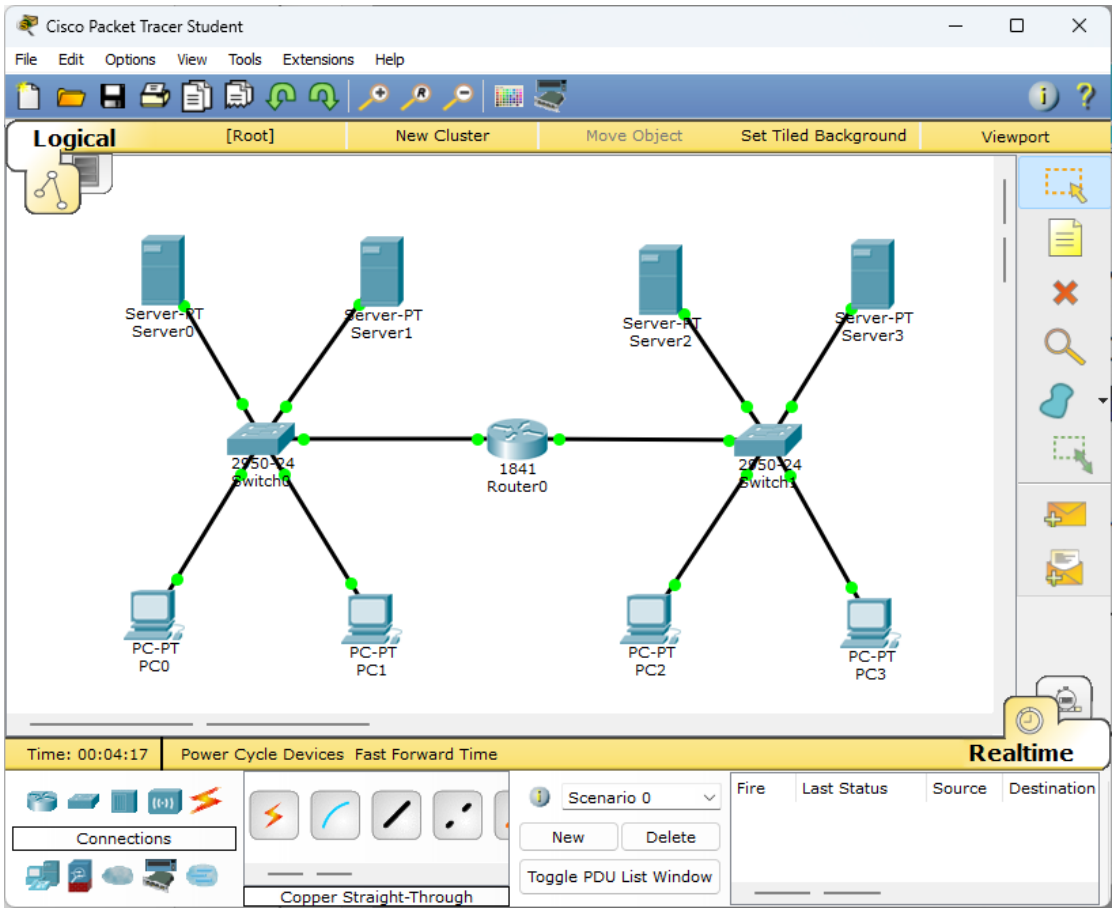
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。

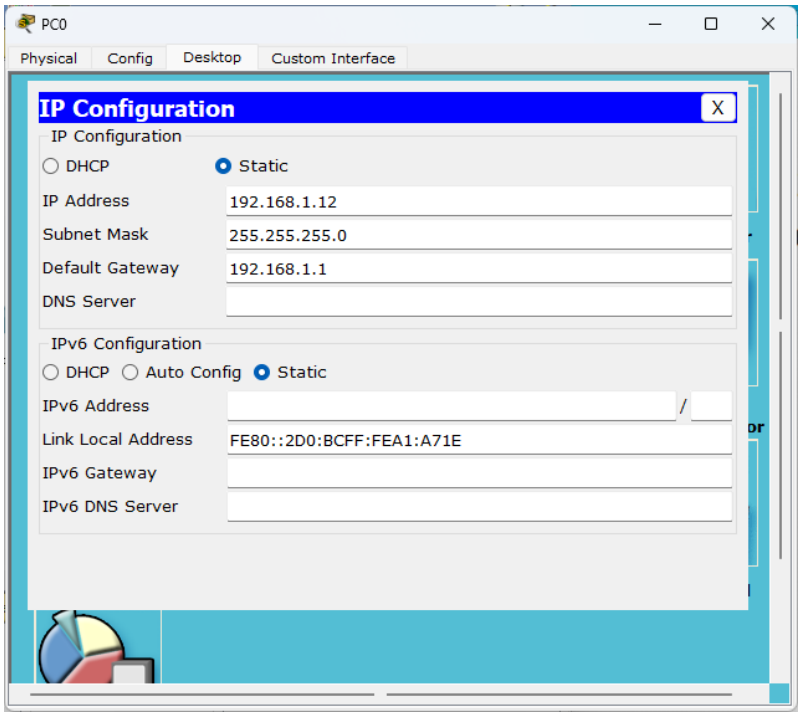


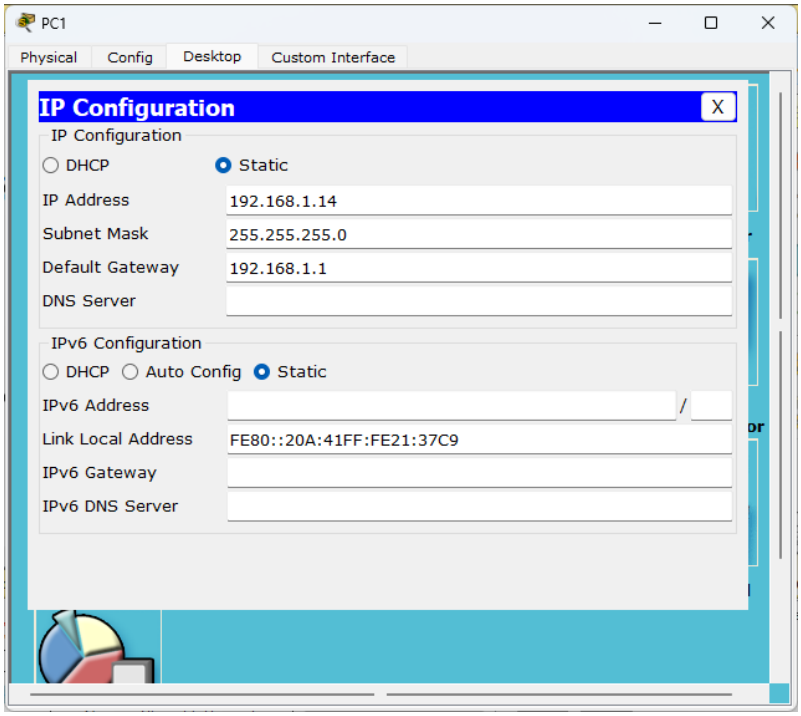

2. 启动 Cisco Packet Tracer，按照上图连接网络。

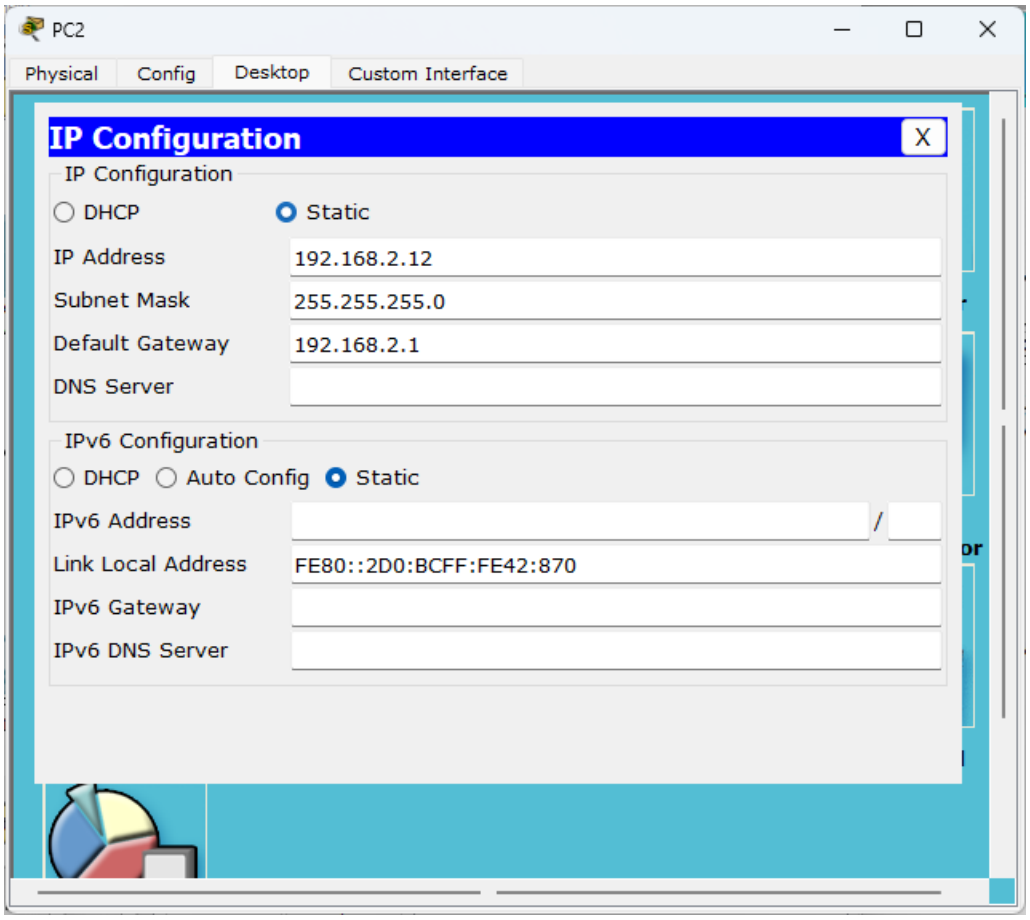


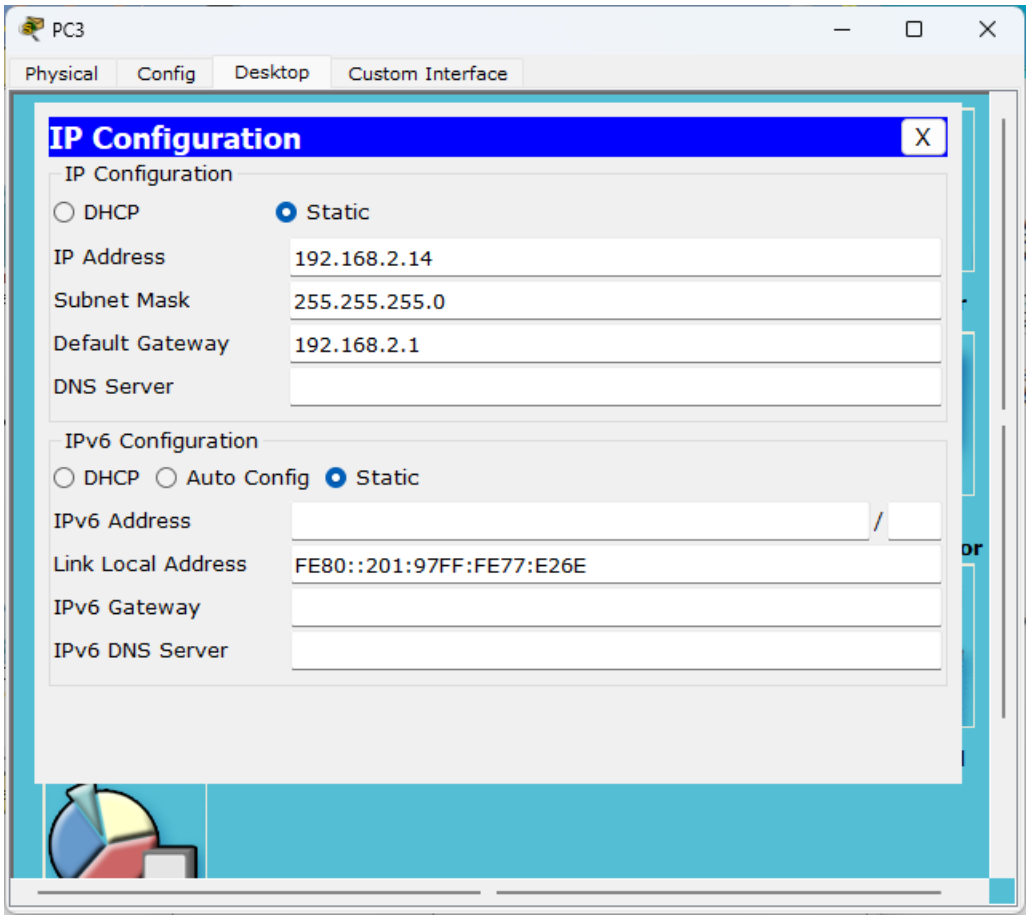
3. 为每台 PC 机配置如下静态 IP 地址、子网掩码和默认网关。

| PC | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|
| PC0 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC1 | 192.168.1.14 | 255.255.255.0 | 192.168.1.1 |
| PC2 | 192.168.2.12 | 255.255.255.0 | 192.168.2.1 |
| PC3 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1 |



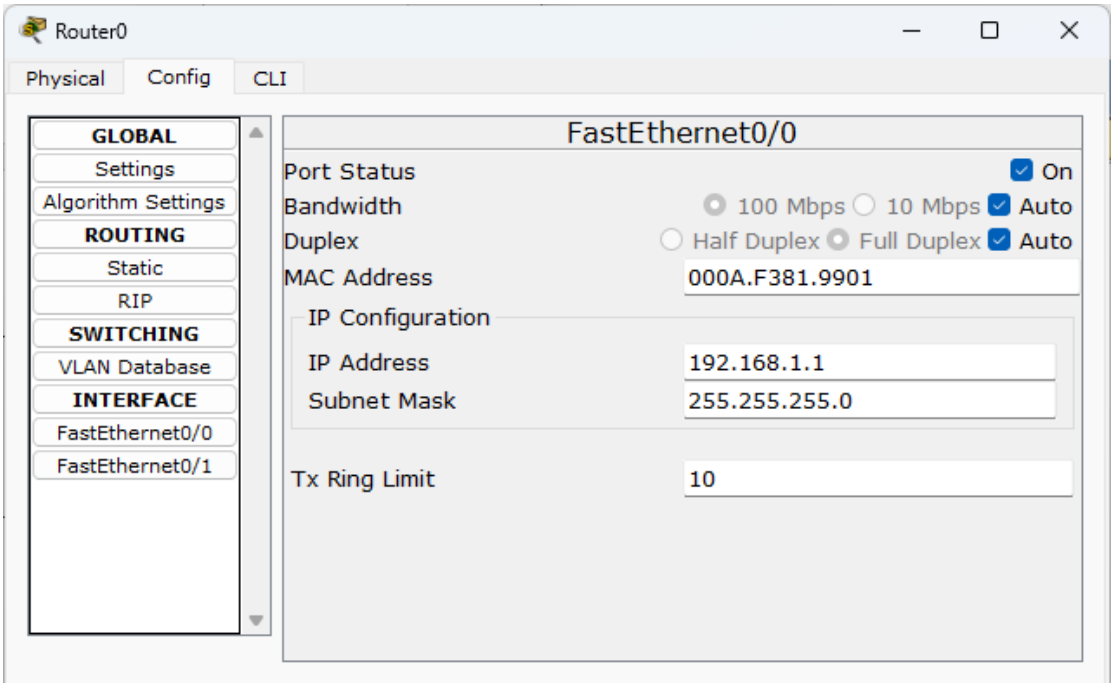



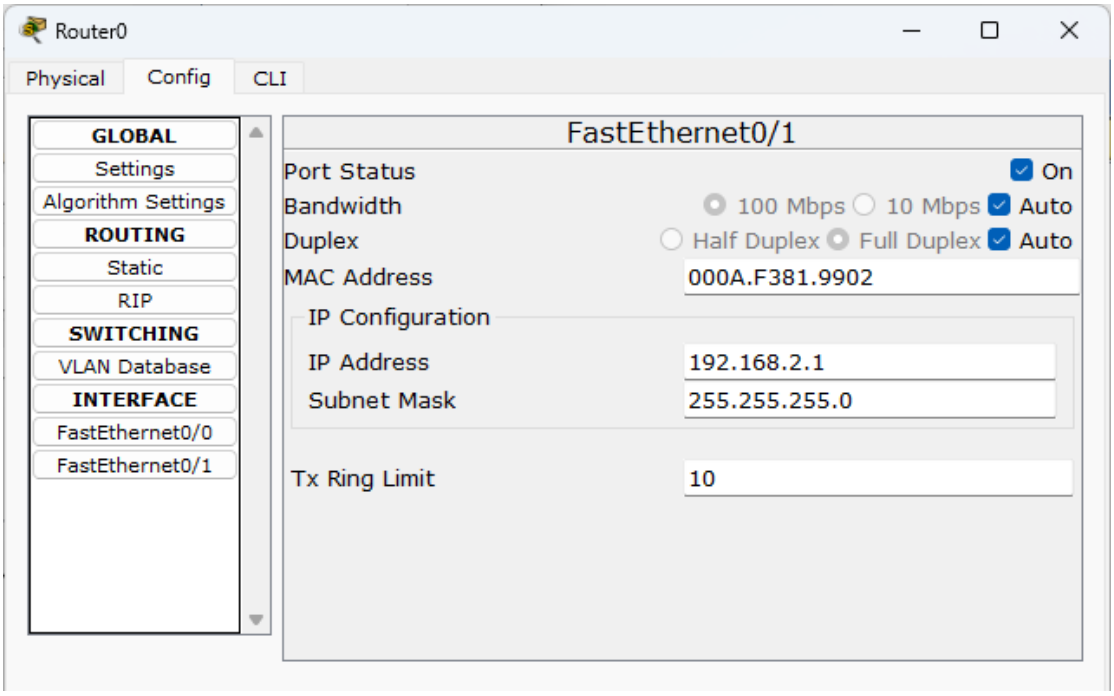

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE42:870
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE77:E26E
IPv6 Gateway
IPv6 DNS Server

4. 参照先前实验（实验 18：动态 IP 地址分配 DHCP 实验）配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```



5. 在路由器 Router0 配置 DHCP。

- 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

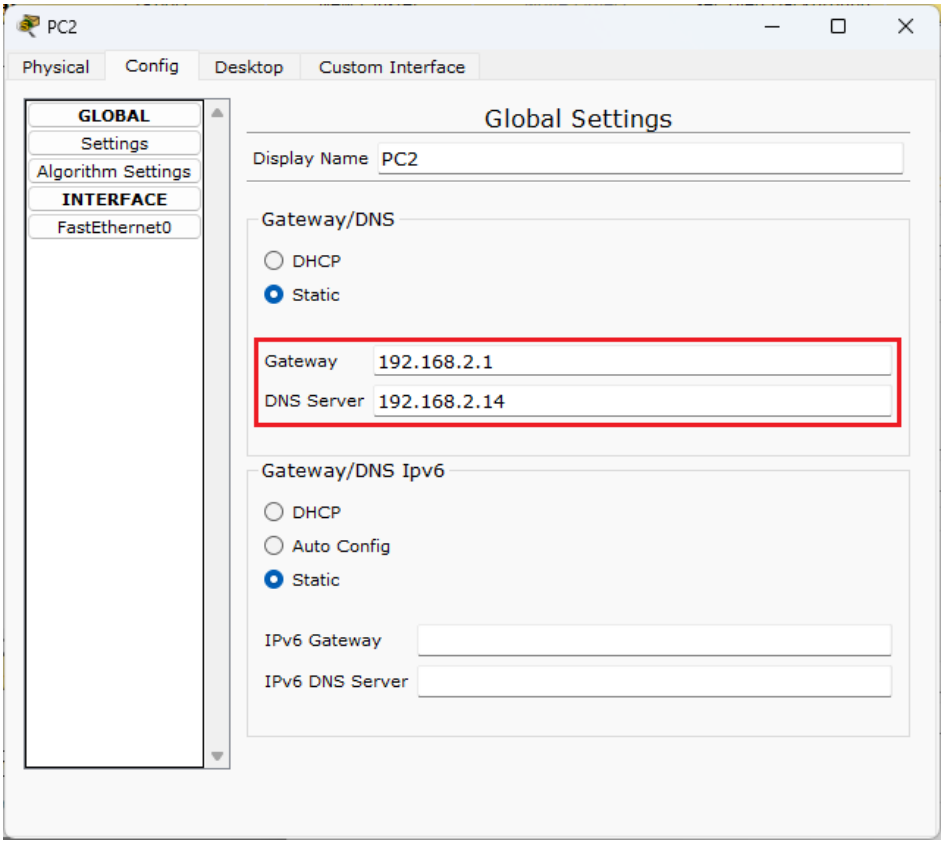
```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

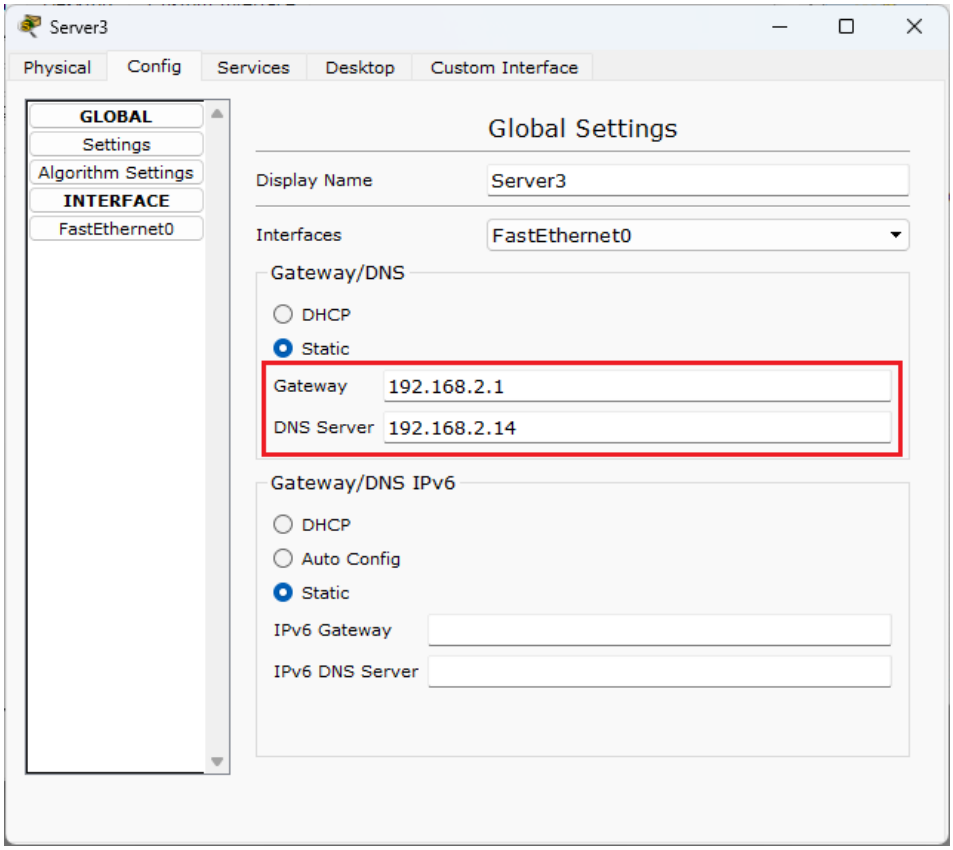
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

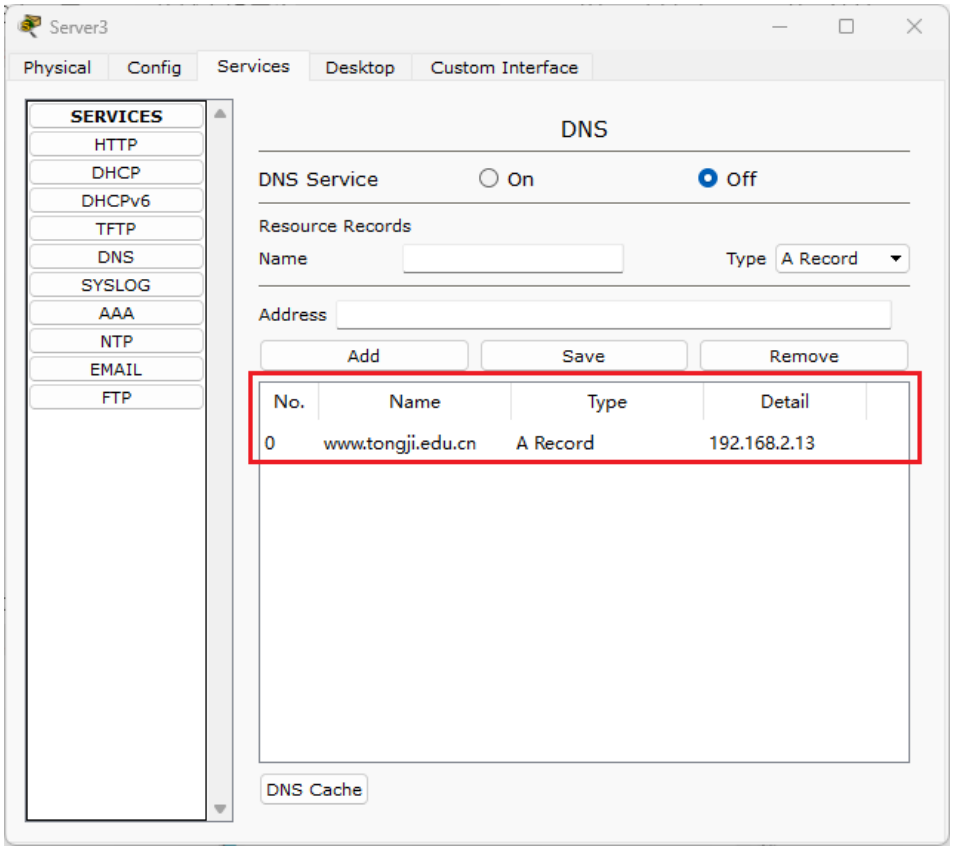
6. 配置 Server 的 Gateway 和 DNS Server。

7. 配置 PC2 的 DNS Server 为 192.168.2.14。设置 PC2 的 DNS Server 与 Server3 的 DNS Server 相同是为了能够通过 Server3 构建映射访问到 Server2。






8. 配置 Server3 的 Services，Name 设置为 www.tongji.edu.cn，Detail 设置为 Server2 的 IP 地址（192.168.2.13）。



9. 从 Realtime 模式切换至 Simulation 模式。

9.1 在 PC2 的 Web Browser 中输入 http://www.tongji.edu.cn，产生 TCP 数据报文。

9.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

9.3 在 Even List 中的 Info 栏可以查看相关信息。

10. 分析在 Packet Tracer 中 TCP 报文情况。

11. 用 WireShark 抓取 TCP 数据包，查看 TCP 报文字段内容，并解读。

12. 仔细研读 TCP 连接建立过程数据报文。

13. 仔细研读 TCP 拆链过程数据报文。

**【实验现象】**

1. 分析在 Packet Tracer 中 TCP 报文情况。

1.1 PDU Information at Device: Server2（OSI Model）

- 输入 PDU 详情（Switch2→Server2）
  - 源端口：1031
  - 目标端口：80（HTTP 服务）
  - 序列号：0
  - 确认号：0（此为建立连接时的 SYN 报文，序列号和确认号均为 0）
  - 源 IP 地址：192.168.2.11
  - 目的 IP 地址：192.168.2.13
  - 以太网 II 帧头：包含目标和源 MAC 地址（详细的 MAC 地址在描述中未提供）
  - TCP 控制位：SYN（由于是建立连接的 SYN 报文）
- 输出 PDU 详情（Server2→Switch2）
  - 源端口：80
  - 目标端口：1031
  - 序列号：0
  - 确认号：1（表示对第一阶段 SYN 请求的确认）
  - 源 IP 地址：192.168.2.13

- 目的 IP 地址：192.168.2.11
- TCP 控制位：SYN+ACK（表示对 SYN 的确认并请求对方也确认）

- 分析
  - SYN 报文（输入）：第一步的 SYN 报文用于初始化 TCP 连接，它从源端口 1031 发出，请求与目的端口 80（通常用于 HTTP 服务）的设备建立连接。这是三次握手过程中的第一步。
  - SYN+ACK 报文（输出）：服务器收到 SYN 后，回复一个 SYN+ACK 报文，确认收到（通过 ACK 序号为 1），并同时发送自己的 SYN 请求。这是握手过程的第二步，用来确认客户端的 SYN 并要求客户端确认服务器的连接请求。

1.2 PDU Information at Device: Server2（Inbound PDU Details）

- IP 层信息
  - TTL（Time To Live）：128，这表示该数据包在网络上的最大跳数。
  - 协议（PRO）：0x6，表示传输层协议为 TCP。
  - 源 IP（SRC IP）：192.168.2.11，数据包的起始地址。
  - 目的 IP（DST IP）：192.168.2.13，数据包的目标地址。
  - 校验和(CHECKSUM)：0x0，虽然这里显示为 0，实际情况应有一个计算值。

- 选项（OPT）和数据：这两项在此图中未展示具体值，数据长度为可变。

- TCP 层信息
  - 源端口（SRC PORT）：1031，标识发送端的端口。
  - 目标端口（DEST PORT）：80，通常用于 HTTP 服务的端口。
  - 序列号（SEQUENCE NUM）：0，用于标识从 TCP 源端发送的数据字节流的顺序号。
  - 确认号（ACK NUM）：0，用于确认收到对方发送的数据。
  - 偏移（OFF.）和保留（RES.）：TCP 头部的长度和保留位，通常用于控制标志。
  - SYN（同步序列号）：设置此标志表示这是一个连接建立请求。
  - 窗口（WINDOW）：控制从对方接收的数据量，此处未显示具体值。
  - 校验和（CHECKSUM）：0x0，用于检测数据在传输过程中的任何错误。
  - 紧急指针（URGENT POINTER）：当 URG 标志被设置时，表示这个字段是有效的，此处显示为未设置。
  - 选项（OPTION）和填充（PADDING）：TCP 头部可能包含的选项和为了字节对齐而添加的填充字节。

- 数据传输分析

- 这张图示例显示的是一个 TCP 初始化连接请求的 SYN 包。SYN 标志被设置表示请求建立连接。这是 TCP 三次握手过程中的第一步，用于同步序列号。接下来期待的是服务器响应一个 SYN-ACK 包，标志位 ACK 和 SYN 同时设置，表示确认并同意建立连接。

1.3 PDU Information at Device: Server2（Outbound PDU Details）

- IP 层信息
  - 版本号（Version）：4，表示这是 IPv4。
  - 首部长度（IHL - Internet Header Length）：表示 IP 头部的长度，单位为 32 位字（4 字节的倍数）。
  - 区分服务（DSCP）：0x0，表示没有特殊的区分服务。
  - 总长度（TL - Total Length）：44，表示整个 IP 数据包的长度（字节）。
  - 标识（ID）：0x88，一种标识，用于分片和重组。
  - 片偏移（Fragment Offset）：0x2，表示这个片段在原数据包中的位置。
  - 生存时间（TTL）：128，数据包在网络中的最大跳数。
  - 协议（PRO）：0x6，表示传输层协议为 TCP。
  - 校验和（CHECKSUM）：未显示具体值，用于检验 IP 头部的完整性。
  - 源 IP（SRC IP）：192.168.2.13，数据包的起始地址。
  - 目的 IP（DST IP）：192.168.2.11，数据包的目标地址。
  - 选项（OPT）和 数据：没有特殊选项，数据长度可变。
- TCP 层信息
  - 源端口（SRC PORT）：80，标识响应方的端口（HTTP 服务）。
  - 目标端口（DEST PORT）：1031，标识请求方的端口。
  - 序列号（SEQUENCE NUM）：0，用于标识从 TCP 源端发送的数据字节流的顺序号。
  - 确认号（ACK NUM）：1，用于确认收到对方发送的数据，这里的 1 表示确认收到了包含序列号为 0 的 SYN 报文。
  - 偏移（OFF.）和 保留（RES.）：TCP 头部的长度和保留位，通常用于控制标志。
  - SYN+ACK：设置这两个标志位表示响应连接请求并要求确认。

- 窗口（WINDOW）：控制从对方接收的数据量，此处未显示具体值。
- 校验和（CHECKSUM）：0x0，用于检测数据在传输过程中的任何错误。
- 紧急指针（URGENT POINTER）：当 URG 标志被设置时，表示这个字段是有效的，此处显示为未设置。
- 选项（OPTION）和 填充（PADDING）：TCP 头部可能包含的选项和为了字节对齐而添加的填充字节。

- 数据传输分析
  - 这个 SYN-ACK 报文是 TCP 三次握手过程中的第二步，用于确认之前收到的 SYN 请求，并要求对方确认本次连接的有效性。接下来期待的是客户端（源端口 1031）对此 SYN-ACK 的确认，发送一个仅设置 ACK 标志位的 TCP 报文，这将完成三次握手过程，建立 TCP 连接。

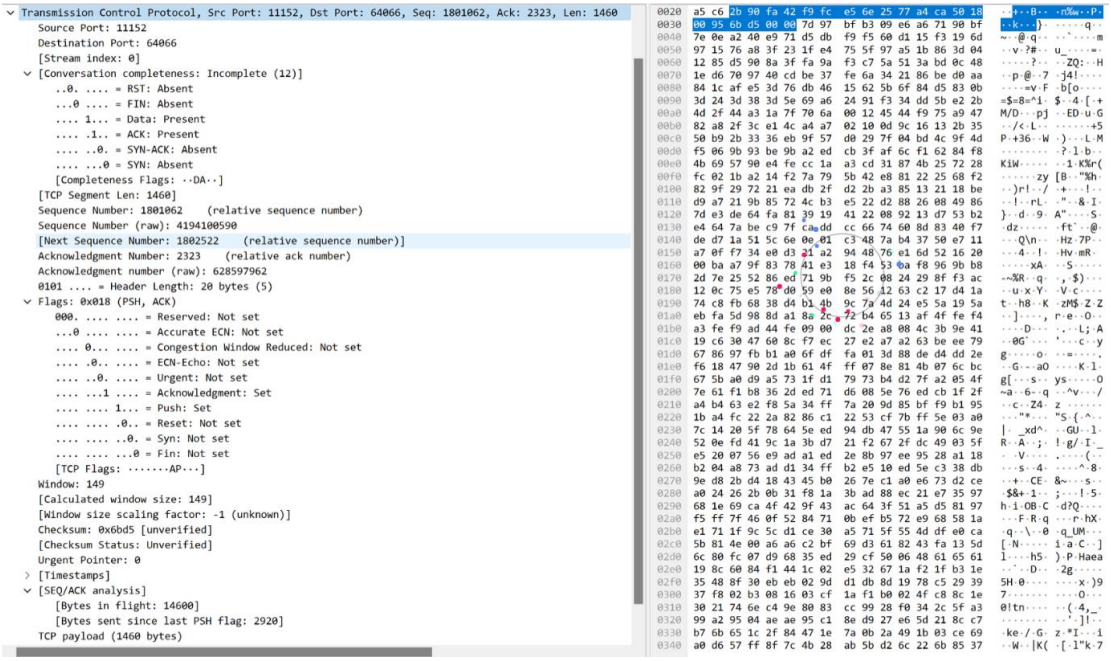
2. 仔细研读 TCP 连接建立过程数据报文。

- 主要 TCP 字段解析
  - 源端口号（Source Port）：11152，标识发送方的应用层端口。
  - 目的端口号（Destination Port）：64066，标识接收方的应用层端口。
  - 序列号（Sequence Number）：4194102590，这是此 TCP 段发送的数据的第一个字节的序列号。

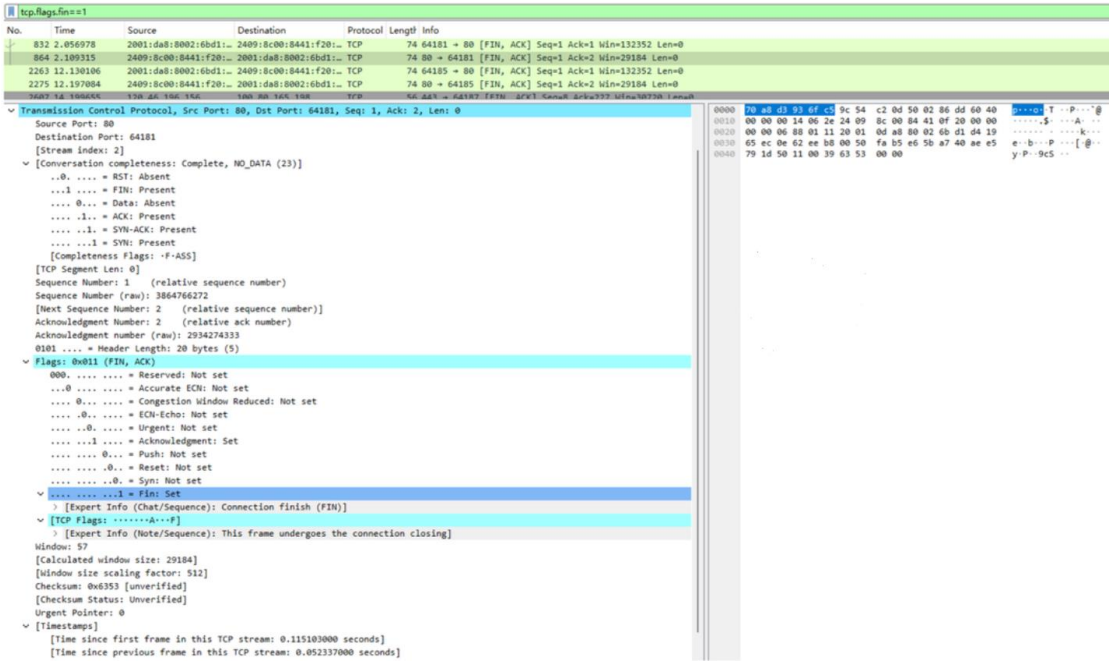
- 确认号（Acknowledgment Number）：2323，这表示接收方期待的下一个字节的序列号，确认了接收方已经成功接收的数据。
- 数据偏移（Header Length）：20 字节，指示 TCP 头部的长度，表明此 TCP 段没有包含额外的选项。
- 标志位（Flags）：PSH, ACK。PSH 标志位提示接收方应该立即将这些数据传递给应用层，而不是在缓冲区中等待更多的数据。ACK 标志位确认接收到的数据。
- 窗口大小（Window）：149，这表示接收方当前的接收窗口大小，告知发送方它还能接收多少字节的数据，用于流控制。
- 校验和（Checksum）：0x6bd5，用于验证接收到的数据在传输过程中是否出现错误。这个值是对整个 TCP 段（包括 TCP 伪头部，TCP 头部和数据）计算得出的。
- 紧急指针（Urgent Pointer）：0，由于 URG 标志没有设置，这个字段不被使用。

● 数据包分析

- 此数据包的 PSH 和 ACK 标志位被设置，表明这是一个在数据传输中间阶段的包，发送方不仅发送数据还确认之前接收的数据。ACK 标志常用于所有接收到数据的确认响应中，而 PSH 标志用于指示接收方应立即处理这些数据，这常见于需要快速响应的应用，如实时通信应用。



3. 仔细研读 TCP 拆链过程数据报文。




- 主要 TCP 字段解析
  - 源端口（Source Port）：80，通常用于 HTTP 服务的端口，表示发送方的端口。
  - 目的端口（Destination Port）：64181，表示接收方的端口。
  - 序列号（Sequence Number）：1，这是相对序列号，Wireshark 显示为 1，表示这是相对于 TCP 连接初始序列号的序列号。
  - 确认号（Acknowledgment Number）：293474333，这是相对确认号，表示接收方已经收到对方发送的数据直到这个序号。
  - 标志位（Flags）：FIN, ACK。FIN 标志用于通知接收方发送方已完成发送数据并希望建立终止连接，ACK 标志是对之前接收到的 TCP 段的确认。
  - 窗口大小（Window）：57，这指示接收方当前的接收窗口大小，告知发送方它还能接收多少字节的数据，这对于流量控制很重要。
  - 校验和（Checksum）：0x6353，用于验证接收到的数据在传输过程中的完整性和正确性。
  - 紧急指针（Urgent Pointer）：0，由于紧急标志(URG)未被设置，此字段不被使用。
- 连接拆除分析

  这个 TCP 段标志着一个 TCP 连接的结束阶段之一。当一个 TCP 连接准备关闭

时，一个端点会发送一个 FIN 标志位的段。这里，端口 80 发送了一个包含 FIN 和 ACK 标志的 TCP 段，目的是通知接收端（端口 64181），它已经完成了数据传输，并希望建立终止连接。

这种 FIN 和 ACK 的组合也是对接收端之前发送的任何未确认数据的确认。接下来的期待是接收端响应一个 ACK，确认这个 FIN 段，然后发送自己的 FIN 段，如果还有待发送的数据，则在此之后发送。最终，发送端将确认这个 FIN，从而完成四次挥手过程，彻底关闭连接。

**【分析讨论】**

**一、在 Packet Tracer 中 TCP 报文情况。**

在 Packet Tracer 模拟环境中，TCP 报文被详细模拟，展现了从 TCP 三次握手到四次挥手的全过程。通过模拟，可以观察到报文的发送和接收，以及在不同 TCP 状态转换时各种控制位的变化。

**二、TCP 报文字段内容。**

TCP 报文的字段结构包括源端口、目的端口、序列号、确认号、数据偏移、控制位、窗口、校验和、紧急指针等。这些字段合作确保了 TCP 的可靠传输，其中序列号和确认号为核心机制，支持数据的有序传送和重传机制。窗口大小字段则关系到流量控制，而控制位如 SYN、ACK、FIN 等则是连接管理的基础。

**三、TCP 连接建立过程数据报文。**

TCP 连接的建立过程，即三次握手，涉及 SYN 和 ACK 报文的交换。首先，客户端发送 SYN 报文请求建立连接；接着，服务器回应 SYN-ACK 报文；最后，客户端再发送 ACK 报文确认，完成连接建立。这个过程确保了双方的序列号和确认号能被正确同步，是建立可靠通信的基石。

**四、TCP 拆链过程数据报文**

TCP 连接的终止过程，即四次挥手，涉及 FIN 和 ACK 报文的交换。这个过程开始于发送方发送一个 FIN 报文，请求关闭连接。接收方确认这个 FIN 报文，并可能继续发送数据直到也发送 FIN 报文。发送方确认这个 FIN 后，连接终止。这一过程确保了双方数据的完整传输，即使在关闭连接时。

# 实验 25：UDP 数据包分析实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/23 |

**【实验目的】**

1. 了解 UDP 协议的特点：学生将学习 UDP 协议的无连接、不可靠传输和简单的错误检测机制。这包括理解 UDP 为什么比 TCP 有更少的时延，以及为什么在某些应用中（如实时视频、VoIP、DNS 查询等）更适合使用 UDP 而不是 TCP。
2. 分析 UDP 报文结构：通过实验，学生将了解 UDP 数据报的首部格式，包括源端口号、目的端口号、长度和校验和字段的作用。
3. 掌握如何使用网络分析工具：学生将使用工具如 Wireshark 来捕获和分析 UDP 数据包，这不仅包括识别基本的 UDP 流量，还包括深入理解数据包中的信息，如端口号、数据长度和可能的传输错误。
4. 学习 UDP 的实际应用：实验中，学生将配置和观察使用 UDP 协议的网络服务，例如 DNS 服务器。这有助于学生理解在实际网络环境中 UDP 的运用场景和行为。
5. 诊断网络问题：通过分析 UDP 通信过程中的数据包，学生可以学习如何诊断网络中的问题，例如丢包、端口不可达错误以及由校验和错误导致的数据包丢弃。
6. 评估 UDP 的性能和可靠性：学生将评估 UDP 协议在不同网络条件下的性能，理解 UDP 协议在高速网络传输中如何受到网络延迟和丢包的影响，并探索如何在应用层增加额外的机制来提高通信的可靠性。

**【实验原理】**

**一、UDP 概述**

UDP（用户数据报协议）是一种位于网络传输层的协议，它在 IP 的数据报服务之上增加了基本的服务功能，包括复用与分用服务以及差错检测。UDP 是一个简单的面向消息的传输协议，不像 TCP（传输控制协议）那样提供可靠性保证，也不进行连接管理。

**二、UDP 应用特点**

UDP（用户数据报协议）的应用特点主要体现在其设计和功能的简洁性以及

对于特定应用环境的适用性。以下是 UDP 的主要应用特点：

1. 无连接性：UDP 是一个无连接的协议，这意味着在数据传输前不需要建立连接，从而减少了通信的延迟。这种特性使得 UDP 非常适合需要快速数据传输的场景，例如 DNS 查询。
2. 简单的首部结构：UDP 的首部只有 8 字节，比 TCP 的 20 字节首部要小得多。这种简单的首部结构减少了数据传输的总开销，尤其是在传输小量数据时更为高效。
3. 尽最大努力的交付：UDP 不保证数据的可靠交付。它不会对丢失的数据包进行重传，也没有确认机制，这样可以避免在网络条件不佳时造成的延迟。
4. 无拥塞控制：UDP 没有内置的拥塞控制机制，因此它允许应用层更好地控制数据的发送时间和频率。这对于实时应用（如视频流、实时游戏）来说非常重要，因为这些应用更关注延迟而不是每个数据包的完整性。
5. 面向报文：UDP 是面向报文的，它保持应用层数据的边界。这意味着 UDP 一次发送一个完整的消息，并保持消息的完整性。应用层在接收时也必须一次性完整地接收整个消息，这简化了应用层的处理逻辑。
6. 适用于多种应用：
   - DNS：UDP 用于 DNS 查询，因为 DNS 请求通常很小，并且要求快速响应。
   - 实时应用：UDP 常用于实时应用，如 VOIP（语音通信）、实时视频会议和在线游戏，因为这些应用可以容忍一定的数据丢失，但对延迟非常敏感。
   - 多媒体流：流媒体传输等应用使用 UDP 来减少播放时的延迟。

总体来说，UDP 的设计哲学是提供快速、简单且灵活的传输服务，尽管这样的服务是不可靠的。这使得 UDP 在那些不需要或少需要可靠性但需求低延迟或高效率的场景中非常有用。

**三、UDP 报文格式**

UDP（用户数据报协议）报文的格式设计简单而高效，使其在网络中的处理非常快速。UDP 数据报整体分为首部和数据两部分，封装在 IP 数据报中进行传输。以下是 UDP 报文格式的详细介绍：

1. UDP 首部格式

UDP 首部固定长度为 8 字节，由以下四个字段各占两字节组成：

- 源端口号：这是发送方的端口号，用于接收方回复消息时指定返回的端口。如果发送方不需要回复，则可以将此字段设置为 0。
- 目的端口号：这是接收方的端口号，用于在目的地将数据报文正确地交付给相应的应用程序。
- 长度：这个字段指定了 UDP 首部和数据的总长度，最小值为 8 字节（即只有首部，没有数据）。
- 校验和：用于检测 UDP 数据报在传输过程中是否发生错误。如果设置为 0，则表示发送方没有计算校验和，接收方也不应进行校验。

2. 校验和计算

校验和的计算包括首部和数据两部分，以确保数据的完整性。为了进行校验和的计算，还需要在 UDP 数据报前临时添加一个 12 字节的伪首部。伪首部包括：

- 源 IP 地址（4 字节）
- 目的 IP 地址（4 字节）
- 保留字节（全 0，1 字节）
- 协议类型（1 字节，表示 UDP）
- UDP 长度（2 字节，与 UDP 首部中的长度字段相同）

伪首部不是 UDP 数据报的实际一部分，不会传送，只是在计算校验和时使用。校验和的计算方法是将整个 UDP 数据报（包括伪首部、首部和数据）视为 16 位的字序列，进行二进制反码求和。如果最后的求和结果为全 1，则表示数据在传输过程中没有错误；如果不是，则表明数据报在传输过程中出现了错误。

3. 错误处理

如果接收到的 UDP 数据报校验和不正确，表明数据报可能已损坏。接收方可以选择丢弃此数据报，或者可以选择接收但向应用层报告数据可能已损坏。此外，如果接收方发现目的端口号不存在，则会丢弃该数据报，并可能通过 ICMP 协议向发送方发送“端口不可达”错误消息。

通过这种设计，UDP 提供了一种快速但不保证可靠性的传输方式，适合对传输效率和低延迟有高要求的网络应用。

**【实验设备】**

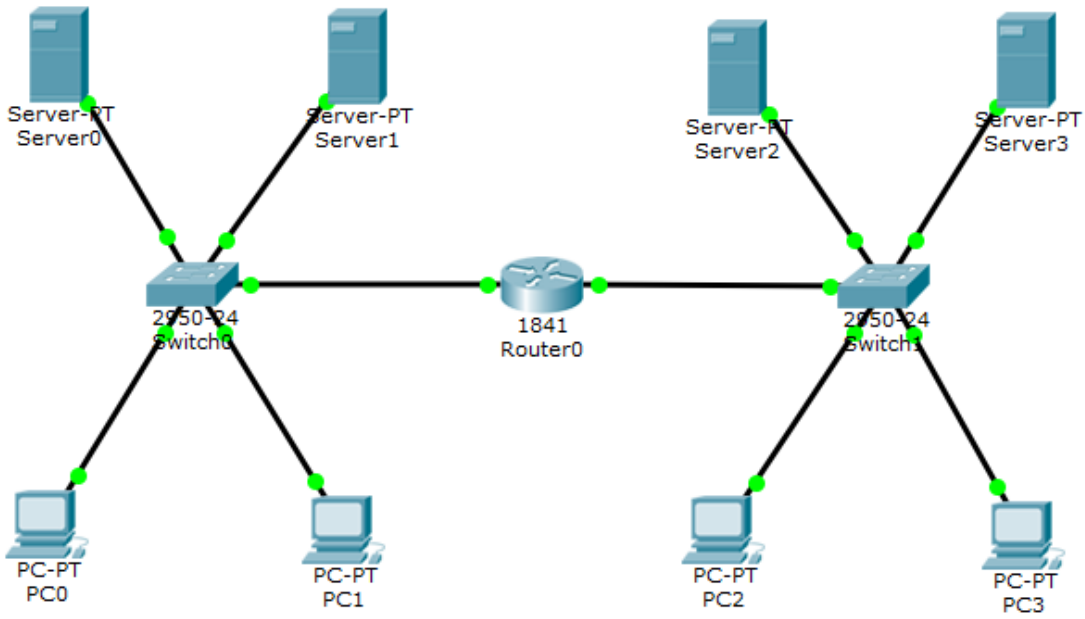
1. 操作系统：Windows 10

2. 网络环境：局域网

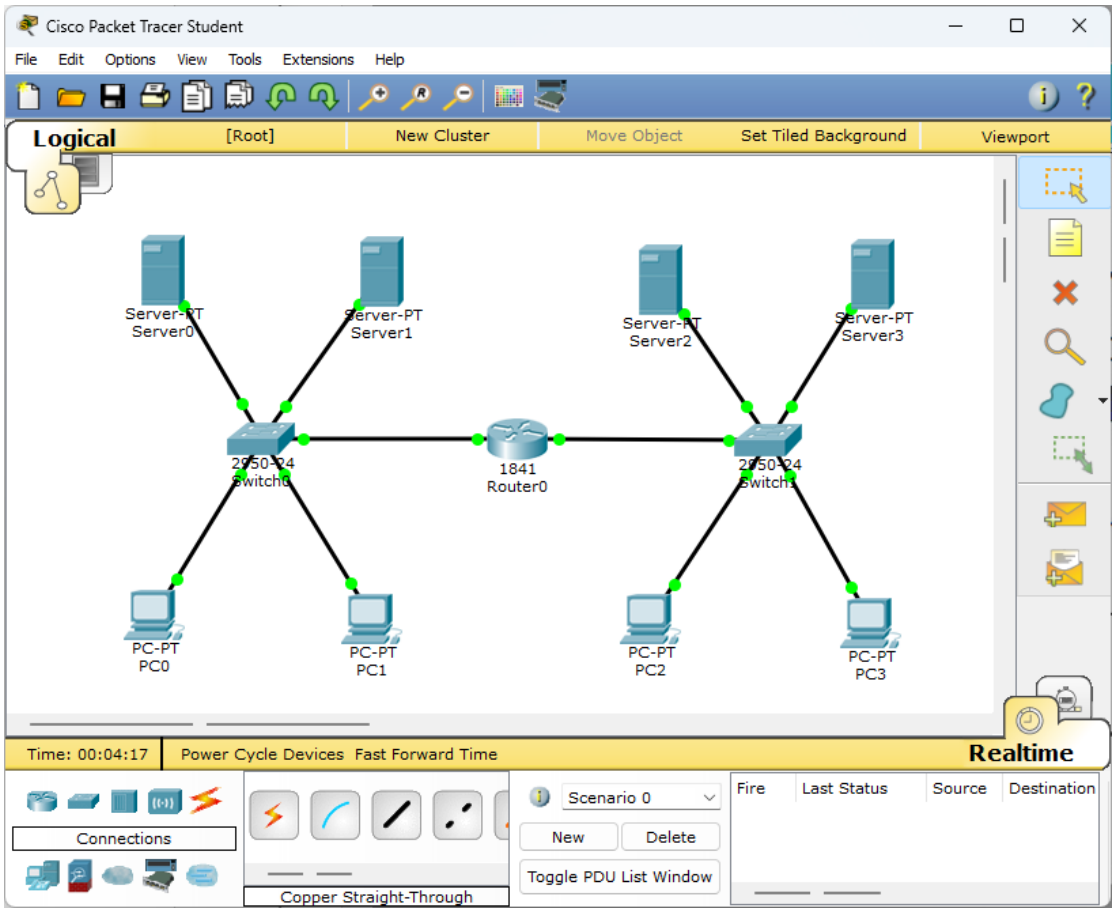
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。

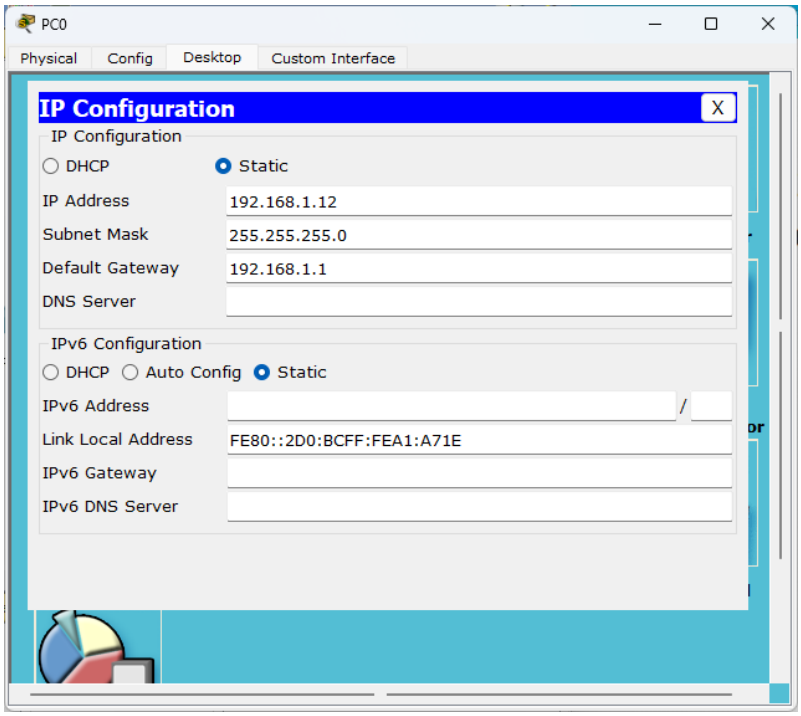


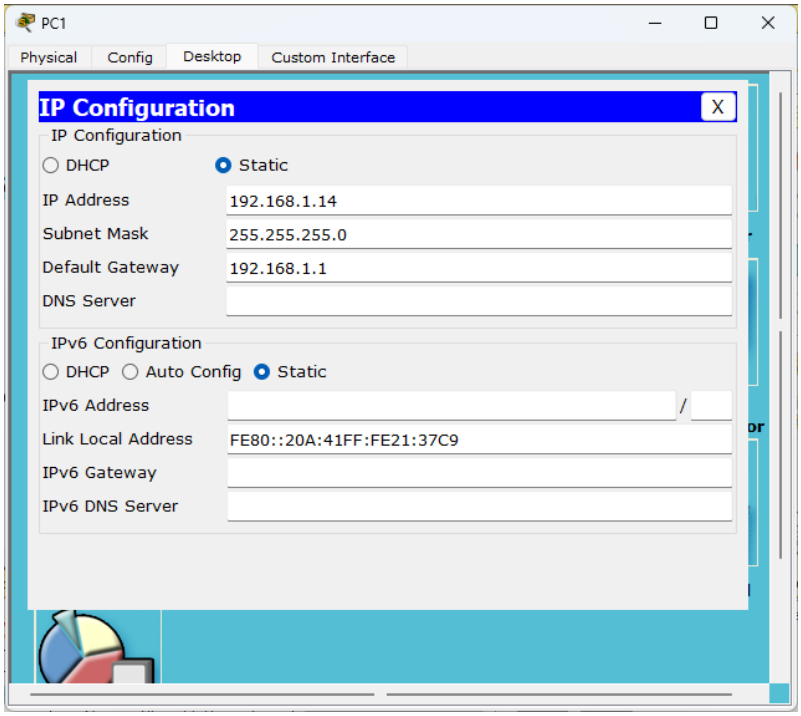

2. 启动 Cisco Packet Tracer，按照上图连接网络。

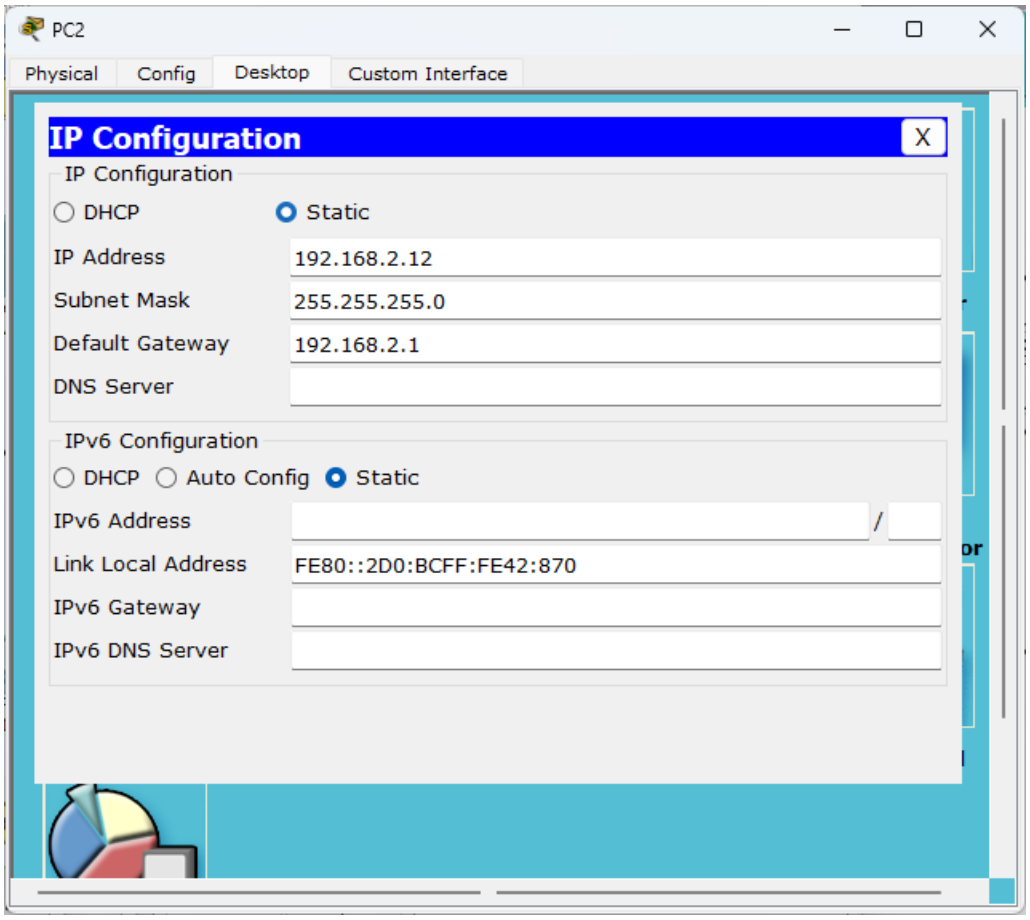


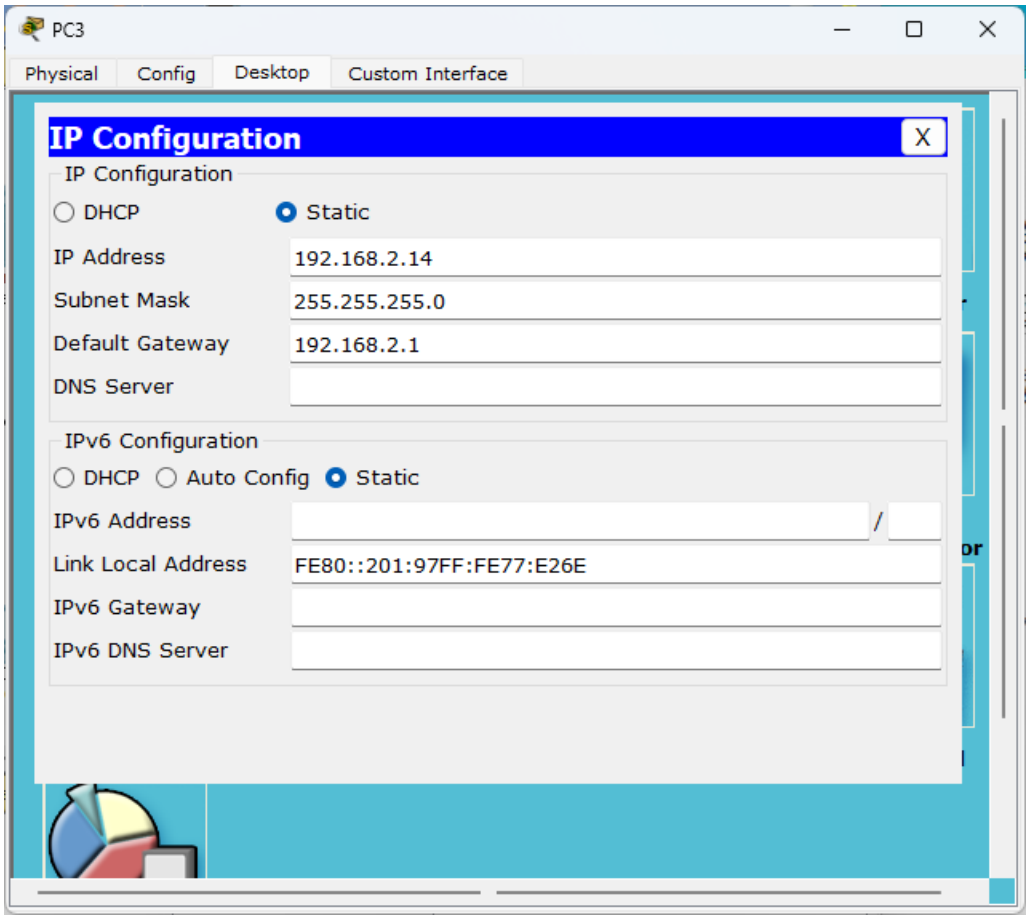
3. 为每台 PC 机配置如下静态 IP 地址、子网掩码和默认网关。

| PC | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|
| PC0 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC1 | 192.168.1.14 | 255.255.255.0 | 192.168.1.1 |
| PC2 | 192.168.2.12 | 255.255.255.0 | 192.168.2.1 |
| PC3 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1 |



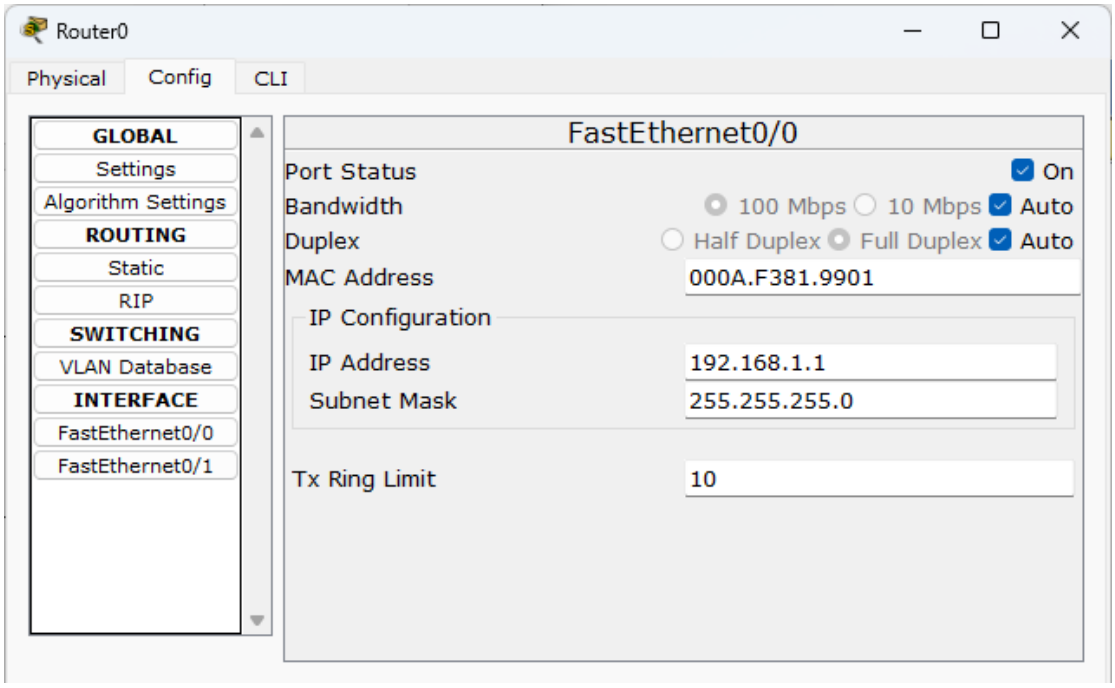



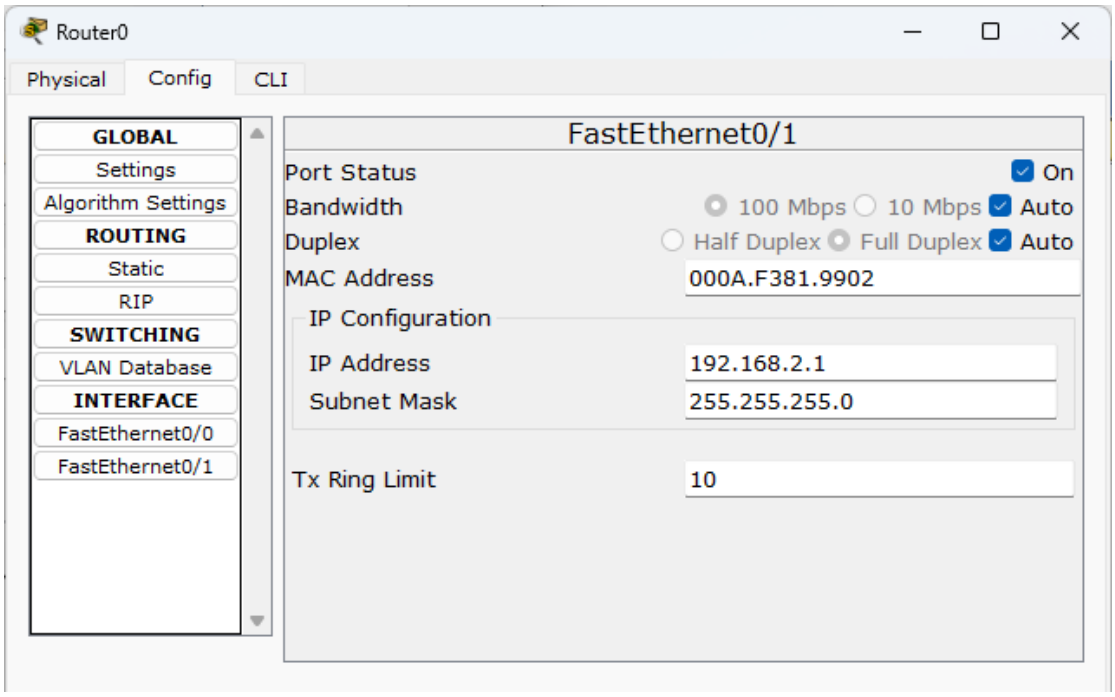

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE42:870
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE77:E26E
IPv6 Gateway
IPv6 DNS Server

4. 参照先前实验（实验 18：动态 IP 地址分配 DHCP 实验）配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```



5. 在路由器 Router0 配置 DHCP。

- 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

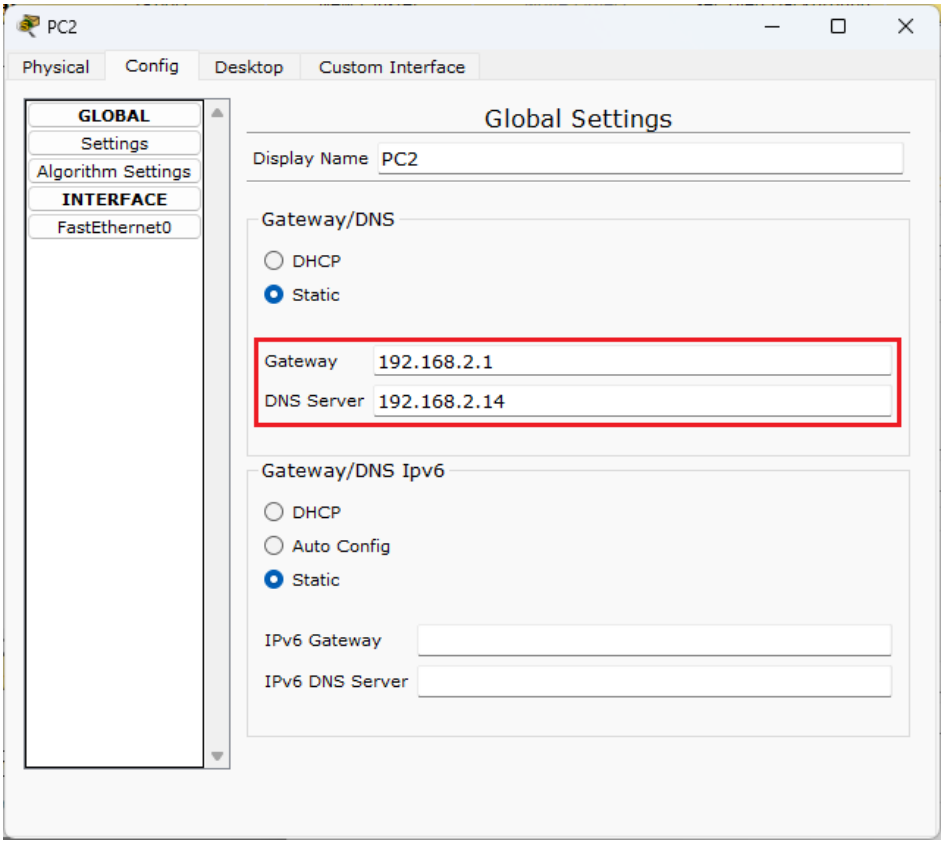
```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

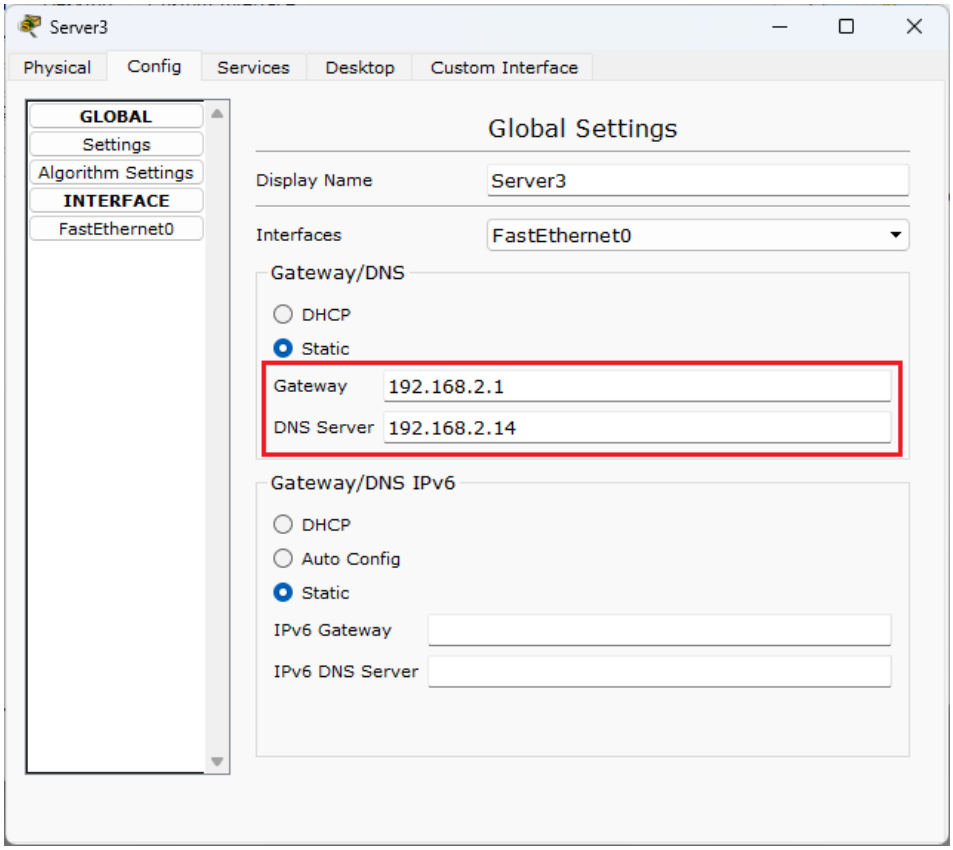
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

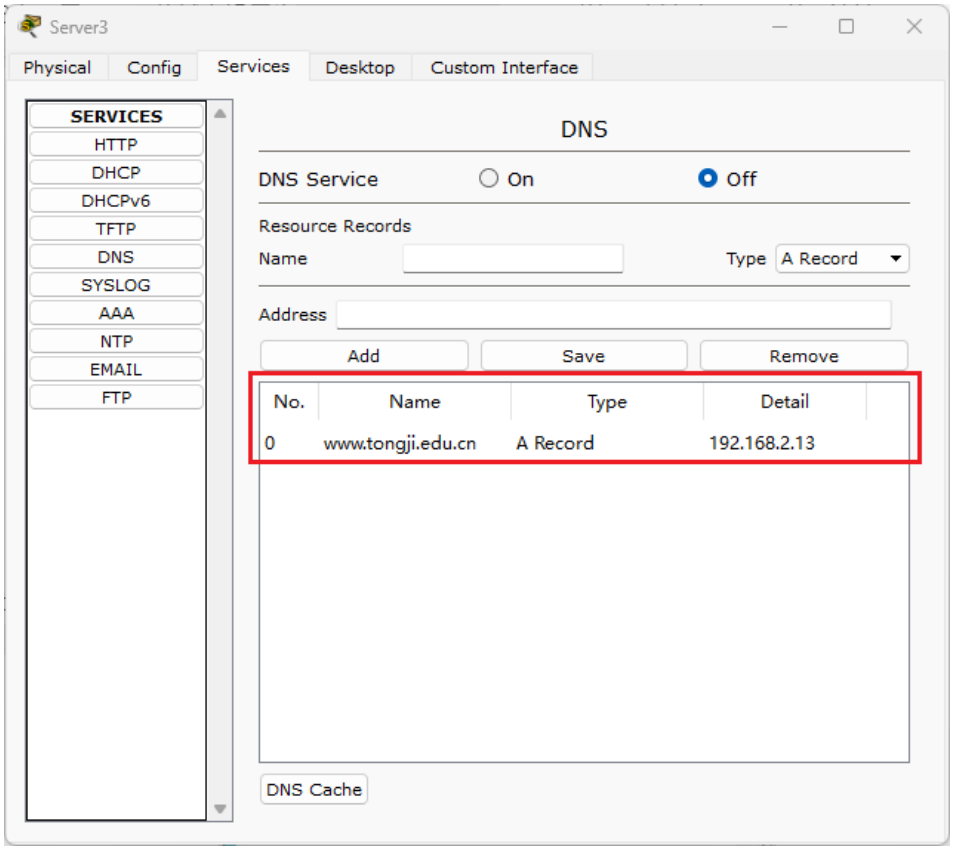
6. 配置 Server 的 Gateway 和 DNS Server。

7. 配置 PC2 的 DNS Server 为 192.168.2.14。设置 PC2 的 DNS Server 与 Server3 的 DNS Server 相同是为了能够通过 Server3 构建映射访问到 Server2。






8. 配置 Server3 的 Services，Name 设置为 www.tongji.edu.cn，Detail 设置为 Server2 的 IP 地址（192.168.2.13）。



9. 从 Realtime 模式切换至 Simulation 模式。

9.1 在 PC2 的 Web Browser 中输入 http://www.tongji.edu.cn，产生 UDP 数据流量，分析 UDP 数据报文。

9.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

9.3 在 Even List 中的 Info 栏可以查看相关信息。

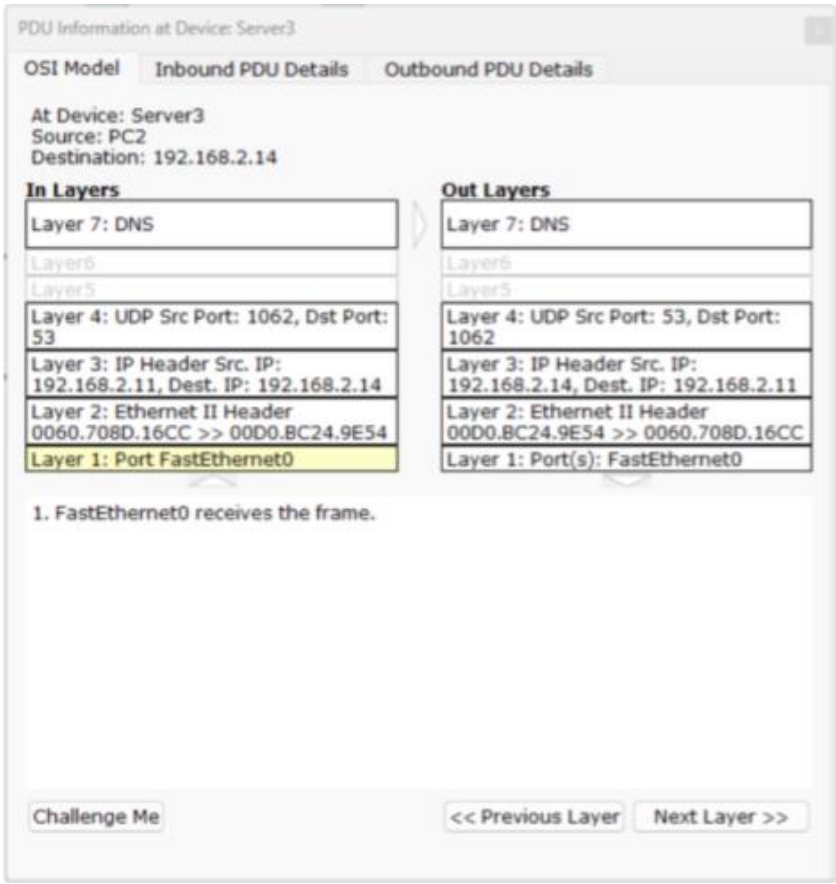
10. 分析在 Packet Tracer 中 UDP 报文情况。

11. 用 WireShark 抓取 UDP 数据包，查看 UDP 报文字段内容，并解读。

**【实验现象】**

1. 分析在 Packet Tracer 中 UDP 报文情况。

1.1 PDU Information at Device: Server3（OSI Model）




在 Packet Tracer 中，UDP 报文的详细情况如下：

- 输入 PDU 详情（Inbound PDU Details）
  - 源端口（Source Port）：53，表示这是一个来自 DNS 服务器的响应。
  - 目的端口（Destination Port）：1062，这是客户端的端口，用于接

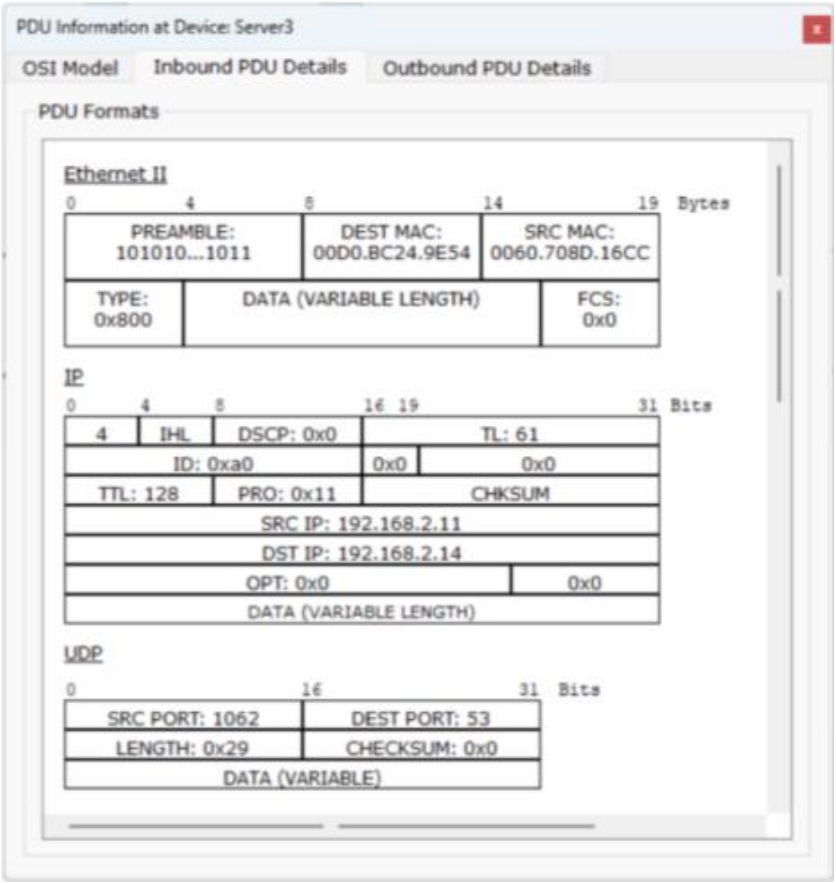
收 DNS 响应。

- 长度（Length）：0x29，这表示 UDP 报文的长度，包括首部和数据，十进制为 41 字节。
- 校验和（Checksum）：0x0，校验和用于错误检测，这里显示为 0，可能是在某些网络环境下不使用或者未被计算。

- 输出 PDU 详情（Outbound PDU Details）
  - 源端口（Source Port）：1062，客户端用于发送 DNS 查询的端口。
  - 目的端口（Destination Port）：53，目标是 DNS 服务器的标准端口。
  - 长度（Length）：0x48，报文长度，包括首部和数据，十进制为 72 字节。
  - 校验和（Checksum）：0x0，同上，校验和显示为 0。

这些信息展示了 UDP 数据包在发送和接收时的基本特征，输入和输出的 PDU（协议数据单元）提供了关于数据包移动和处理的详细信息。

1.2 PDU Information at Device: Server3（Inbound PDU Details）

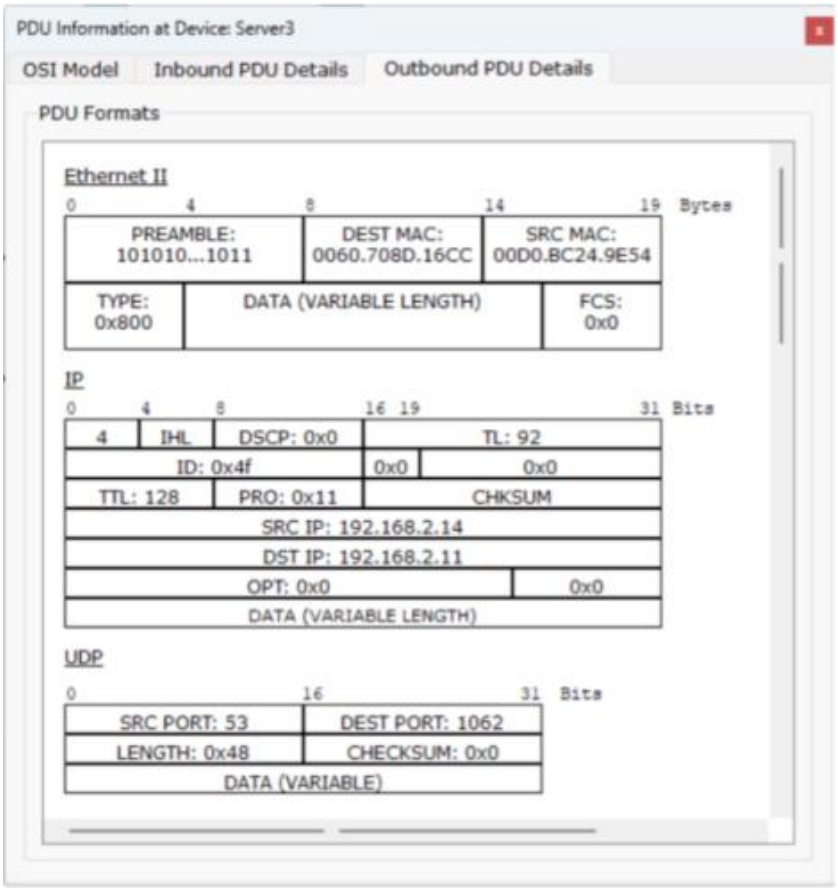



UDP 层：

- 源端口（SRC PORT）：1062，源端口号。
- 目的端口（DEST PORT）：53，DNS 服务的标准端口，表明这是一个 DNS 查询。
- 长度（LENGTH）：0x29，包括 UDP 首部和数据的总长度，十进制为 41 字节。
- 校验和（CHECKSUM）：0x0，可能未计算或不使用。

此图的信息可以帮助理解网络数据包是如何封装和在网络中传输的，以及如何通过不同的网络层来处理数据。每一层都对数据进行相应的封装，增加特定的首部信息，确保数据能正确地从源头传输到目的地。

1.3 PDU Information at Device: Server3（Outbound PDU Details）



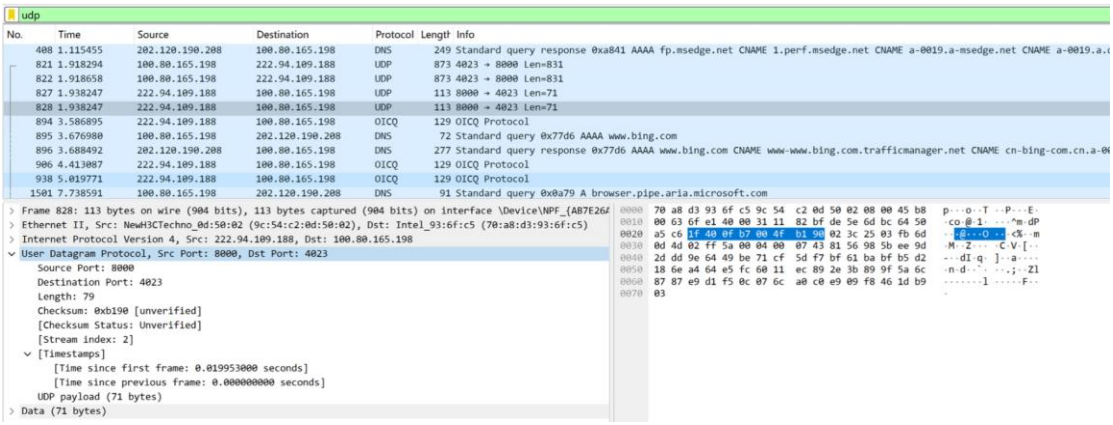

UDP 层：

- 源端口（SRC PORT）：53，表明这是从 DNS 服务器发出的响应。
- 目的端口（DEST PORT）：1062，客户端使用此端口接收 DNS 响应。
- 长度（LENGTH）：0x48，表示 UDP 数据报的总长度为 72 字节（包括首部和数据）。

- 校验和（CHECKSUM）：0x0，表示没有计算校验和，或者不进行校验。

这里的 UDP 数据报明确显示了一个从 DNS 服务器（端口 53）到客户端（端口 1062）的响应。长度字段表明整个 UDP 数据报，包括首部和数据的长度，而校验和字段的值为 0，可能是因为在特定的配置或环境中，校验和未被计算或者故意设置为 0 以避免校验过程。

2. 用 WireShark 抓取 UDP 数据包，查看 UDP 报文字段内容，并解读。




用 WireShark 抓取 UDP 数据包，查看 UDP 报文字段内容，并解读如下：

- 通用信息
  - 数据包编号：828。
  - 长度：113 bytes on wire（即物理层面的总字节数），904 bits。
- IP 协议信息
  - 源 IP 地址（Src IP）：222.94.109.188，发送此数据包的设备的 IP 地址。
  - 目的 IP 地址（Dst IP）：100.80.165.198，接收此 UDP 数据报的设备的 IP 地址。
  - 协议（Protocol）：UDP，表明这是一个 UDP 数据包。
  - 总长度（Total Length）：92 bytes，包括 IP 首部和数据。
- UDP 协议信息
  - 源端口（Source Port）：8000，发送数据报的应用程序端口号。
  - 目的端口（Destination Port）：4023，数据报应当被送达的应用程序端口号。
  - 长度（Length）：79，表示 UDP 数据报的总长度，包括 UDP 首部和数

据。

- 校验和（Checksum）：0xb190，校验和值用于错误检测，状态为“unverified”。

- 时间戳信息
  - 从首个数据包开始的时间：0.01995300 seconds，从会话开始到此数据包抓取的时间。
  - 从前一个数据包开始的时间：0.00000000 seconds，从上一个数据包到此数据包的间隔时间。
- 数据负载
  - UDP 负载长度：71 bytes，这是除 UDP 首部外的实际数据负载。

这些信息对于网络分析非常关键，可以帮助理解网络通信的动态过程、数据流的方向、通信双方的身份，以及数据包的结构。此外，MAC 地址、IP 地址、端口号等元素对于网络故障诊断、安全分析和网络性能优化都有重要作用。

**【分析讨论】**

**一、分析在 Packet Tracer 中 UDP 报文情况**

在本实验中，通过 Packet Tracer 模拟了 UDP 数据报的发送与接收过程，重点观察了 UDP 协议的无连接和简单首部特性。通过直观的网络仿真,理解 UDP 如何在不建立连接的情况下进行数据传输，以及这种传输方式如何减少通信延迟。在 DNS 查询这一特定应用案例中，观察到 UDP 首部的源端口和目的端口的设置，以及数据报文长度和校验和的具体应用。此部分的实验不仅加深了对 UDP 基础结构的认识，还提供了实际操作网络分析工具的机会，能够直观地看到协议在实际网络环境中的工作方式。

**二、用 WireShark 抓取 UDP 数据包并查看 UDP 报文字段内容**

使用 Wireshark 进行的数据捕获实验进一步加强对网络协议分析的实践技能。通过捕获实时网络流量，深入了解 UDP 数据包的传输细节，包括但不限于端口号的功能、数据长度的意义以及校验和的重要性。通过分析特定的 UDP 流量，如 DNS 响应和 VoIP 通信，得以观察和理解 UDP 在减少传输延迟和处理轻量级数据方面的有效性。此外，通过识别传输中可能的错误（如校验和错误）也能够掌握基本的网络问题诊断方法。

# 实验 26：DNS 实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/23 |

**【实验目的】**

DNS 实验的主要目的是通过分析 DNS（域名系统）的工作原理和过程，让学生理解和掌握如何将域名转换为 IP 地址的技术。实验将涉及到理解 DNS 的结构和功能，包括其层次数据库模式和分布式集群工作方式。此外，学生将通过实际操作，如使用 Packet Tracer 和 Wireshark 工具，来观察和分析 DNS 查询和响应的过程。这样的实验能够帮助学生深入了解网络协议的应用层面，以及 DNS 对于互联网通信的重要性。

**【实验原理】**

**一、DNS 概述**

DNS（Domain Name System，域名系统）是互联网的一个基础服务，作为将域名和 IP 地址相互映射的分布式数据库，允许用户通过使用容易记忆的域名来访问互联网资源，而不是复杂的数字 IP 地址。这种机制不仅大大简化了用户访问网络服务的方式，还对整个互联网的运行和管理起到了关键作用。

**二、DNS 过程**

DNS（域名系统）的核心任务是解析域名到相应的 IP 地址，使得其他应用层协议如 HTTP、SMTP、FTP 等可以使用这些 IP 地址进行网络通信。DNS 的过程是一个从用户设备到 DNS 服务器的多步骤查询流程，涉及本地客户端、DNS 缓存、根服务器、顶级域名服务器和权威域名服务器。以下详细描述了 DNS 解析的完整过程：

1. 用户端触发 DNS 查询
   - 用户在浏览器地址栏输入一个 URL，例如 http://www.baidu.com/。
   - 浏览器从 URL 中提取出域名 www.baidu.com，并将其传递给操作系统内部的 DNS 解析客户端。
2. 本地 DNS 客户端发起请求
   - DNS 客户端首先检查本地缓存是否已经有该域名的解析结果。如果有缓存结果，直接使用该 IP 地址完成后续操作。如果没有，客户端将向配置

的 DNS 服务器发送 DNS 查询请求。

3. DNS 解析过程
   - 递归查询：用户的 DNS 客户端通常配置有本地 ISP 的 DNS 服务器。该服务器会代表用户进行递归查询，即全权负责将查询一路跟进到得到答案。
   - 迭代查询：本地 DNS 服务器首先查询根 DNS 服务器，根服务器不会直接解析域名，而是指向负责该顶级域（如.com）的顶级域名服务器。
   - 本地 DNS 服务器接着向顶级域名服务器发出查询请求，顶级域名服务器再指向该二级域名（如 baidu.com）的权威 DNS 服务器。
   - 本地 DNS 服务器最后向权威 DNS 服务器查询具体的记录（如 A 记录，即 IPv4 地址），权威服务器返回域名对应的 IP 地址。
4. 接收 DNS 响应
   - 本地 DNS 服务器收到权威 DNS 服务器提供的 IP 地址后，会将该地址缓存（以减少未来对同一域名的查询时间），然后将解析结果返回给用户的 DNS 客户端。
5. 完成网络连接
   - 用户设备的 DNS 客户端接收到 IP 地址后，浏览器使用这个 IP 地址与目标 HTTP 服务器建立 TCP 连接，开始 Web 会话。

这一过程虽在描述中步骤繁多，但实际上通常在几毫秒到几秒钟内完成，取决于网络状况、服务器响应速度和查询路径的长度。DNS 系统的这种设计使得互联网能够以非常动态和分布式的方式运行，同时保持了对数十亿设备和服务的高效寻址能力。

**三、DNS 服务体系架构**

DNS（域名系统）是一个全球分布式的服务，其主要作用是将人类可读的主机名（如 www.google.com）转换为机器可读的 IP 地址（如 192.168.1.1）。这个系统的设计允许因特网用户通过域名访问网站，而不需要记忆复杂的数字地址。

1. 应用程序的调用：应用程序（例如 Web 浏览器或电子邮件客户端）需要解析域名时，会调用系统内置的 DNS 解析器。在 Unix-like 系统中，这通常是通过 gethostbyname()函数实现。
2. DNS 客户端查询：DNS 客户端（也称为解析器）向配置的 DNS 服务器发送 DNS

查询报文，这通常使用 UDP 协议，通过端口 53。

3. DNS 服务器：DNS 的服务器体系结构包括多层服务器。
   - 根 DNS 服务器：回答来自下级 DNS 服务器的关于顶级域（如.com、.net）的查询。
   - 顶级域 DNS 服务器（TLD）：管理域名注册服务，回答关于第二级域名的查询（如.google.com）。
   - 权威 DNS 服务器：提供最终的域名到 IP 地址的映射。如果权威服务器的数据没有在本地缓存，将由递归服务器查询获取。
4. 递归与缓存：DNS 查询可能涉及多个服务器，从根到顶级，再到权威服务器，直到获取到请求的 IP 地址。为减少延迟和网络负载，DNS 服务器会缓存查询结果，缓存的持续时间由域名的 TTL（生存时间）决定。

**四、DNS 分布式集群工作方式**

1. 分布式架构：为了避免单点故障和处理上亿台主机发出的 DNS 查询，DNS 采用分布式架构。
   - 可扩展性：分布式设计允许系统水平扩展，以应对持续增长的互联网设备和服务。
   - 容错性：多个服务器分散全球，每个层次的 DNS 服务器都有多个冗余选项，增加了整个系统的稳定性和可靠性。
   - 性能优化：通过地理分散的服务器，减少了用户与 DNS 服务器之间的距离，从而减少了查询的响应时间。
2. 避免集中式设计的问题：
   - 单点故障：集中式系统若出现故障，会影响全球的域名解析服务。
   - 通信容量和维护成本：集中式系统需要处理所有的 DNS 查询和更新操作，难以应对全球范围内的巨大流量和动态更新。

**五、DNS 域名**

1. 域名称和域命名空间
   - 域命名空间：DNS 的域名称形成了一个层次化的树状结构，这个结构被称为域命名空间。每个节点在这个树中代表一个域名的部分，节点从树的顶部（根域，通常表示为一个点"."）到具体的主机名。

- 完全限定域名（FQDN）：FQDN 是包括主机名在内的完整域名路径，它指定了从最高级的根域到具体主机的完整路径。例如，im.qq.com 是一个 FQDN，其中 im 是主机名，qq 是二级域名，com 是顶级域名。

2. DNS 域名称的类别

DNS 中的域名称可以根据其在域名空间中的位置和功能分类：

- 顶级域名（TLDs）：顶级域名位于 DNS 层次结构的最高层。这些通常分为两大类：
- 通用顶级域名（gTLDs）：如.com、.org、.net 等。
- 国家代码顶级域名（ccTLDs）：每个国家或地区具有特定的两字母代码，如.uk（英国）、.de（德国）等。
- 二级域名和子域名：位于顶级域名下面，例如在 example.com 中，example 是二级域名。子域名如 support.example.com 中的 support，用于进一步细分和组织网站的内容。

3. 域名资源记录（Resource Records, RR）

DNS 使用一系列的资源记录来描述域内的各种资源，这些记录包括：

- A 记录：将域名映射到 IPv4 地址。
- AAAA 记录：将域名映射到 IPv6 地址。
- NS 记录（Name Server）：指定该域名由哪个 DNS 服务器控制。
- MX 记录（Mail Exchange）：指定处理该域名邮件的邮件服务器。
- CNAME 记录（Canonical Name）：允许将一个域名解析到另一个域名，而不是一个 IP 地址。

## 六、DNS 服务工作过程

DNS 服务的工作过程是一个精妙而高效的系统，它涉及多个步骤和组件，以确保用户能够快速地将易记的域名转换为计算机能够理解的 IP 地址。这个过程分为递归查询和迭代查询两个主要部分。以下是详细介绍：

1. 客户端发起 DNS 查询：当用户在浏览器中输入一个域名如 www.qq.com 时，操作系统首先检查本地的 hosts 文件是否存在该域名的映射关系。如果存在，直接使用该映射完成域名解析。
2. 本地 DNS 解析器缓存查询：如果 hosts 文件中没有该域名的记录，操作系统

的 DNS 解析器将检查自己的缓存是否有这个网址的映射关系。如果缓存中有记录，直接返回这个 IP 地址。

3. 查询本地 DNS 服务器：如果本地缓存也没有找到相应的映射关系，DNS 解析器将向配置的本地 DNS 服务器发起查询。本地 DNS 服务器首先检查它自己的缓存，如果有缓存结果，即使这个结果不具有权威性，也会被返回给客户端以加快解析过程。
4. 递归与迭代查询：如果本地 DNS 服务器本身也无法解析该域名，它将进行以下操作之一：
   - 非转发模式：直接向根 DNS 服务器发起请求，根 DNS 服务器会指向负责该顶级域（如.com）的 TLD 服务器。本地 DNS 服务器然后向 TLD 服务器查询，获取更具体的权威 DNS 服务器地址（如 qq.com）。这个过程会继续，直至找到具体的 www.qq.com 的记录。
   - 转发模式：如果本地 DNS 服务器配置为转发模式，它将查询请求转发至上一级 DNS 服务器。如果上级服务器也无法解析，则请求可能被转发至更高级别的服务器或直接查询根 DNS 服务器。
5. 返回响应给客户端：无论是通过递归查询还是迭代查询，最终得到的解析结果都会被发送回原始请求的本地 DNS 服务器，然后由此服务器返回给客户端的 DNS 解析器，最后解析器将这一信息提供给浏览器或其他请求应用程序。
6. 缓存结果：为了提高效率，DNS 查询结果通常会在本地 DNS 服务器和客户端的 DNS 解析器中缓存一段时间，这样相同的查询在未来可以直接从缓存中获取答案，减少解析时间。

**七、DNS 域名解析顺序**

DNS 域名解析顺序是一个层次化和有序的查询过程，涉及从客户端到全球分布的服务器的多个步骤。这个解析顺序确保了域名能够高效且准确地被转换为对应的 IP 地址。以下是 DNS 域名解析的详细步骤：

1. 浏览器缓存：当用户在浏览器中输入一个域名时，浏览器首先检查自己的缓存，看是否已经存储了该域名的 IP 地址。如果找到了，就直接使用这个地址，这是最快的解析方式。
2. 系统缓存：如果浏览器缓存中没有找到域名的记录，解析器接下来会检查操

作系统的 DNS 缓存。系统缓存包括了之前解析过程中获取的域名记录，以及 hosts 文件中的静态指定。

3. 路由器缓存：如果系统缓存中也没有相应的记录，查询请求将转到网络路由器，许多家用路由器也会缓存 DNS 查询结果，以减少网络延迟和频繁的外网 DNS 查询。
4. ISP DNS 缓存：如果本地设备和路由器都无法解析域名，请求会被发送到 ISP 提供的 DNS 服务器。这些服务器拥有广泛的缓存，可能包含了所需的域名解析结果。
5. 根域名服务器：如果 ISP 的 DNS 服务器也无法解析，它会向根域名服务器发出查询。全球共有 13 台根域名服务器，它们知道所有顶级域名服务器的位置。
6. 顶级域名服务器（TLD 服务器）：根服务器会将查询指向负责该域名后缀（如.com、.net）的顶级域名服务器。顶级域名服务器管理着该后缀下所有域名的分配和解析。
7. 权威域名服务器：顶级域名服务器将查询指向负责该具体域名的权威域名服务器。权威服务器是最终存储域名对应 IP 地址记录的地方。
8. 缓存结果：一旦本地 DNS 服务器从权威服务器接收到 IP 地址，它将此结果缓存起来，用于加速未来的查询。然后，它将 IP 地址返回给发起请求的客户端。
9. 建立连接：客户端拿到 IP 地址后，便开始尝试与该地址对应的服务器建立网络连接，从而访问网站或服务。

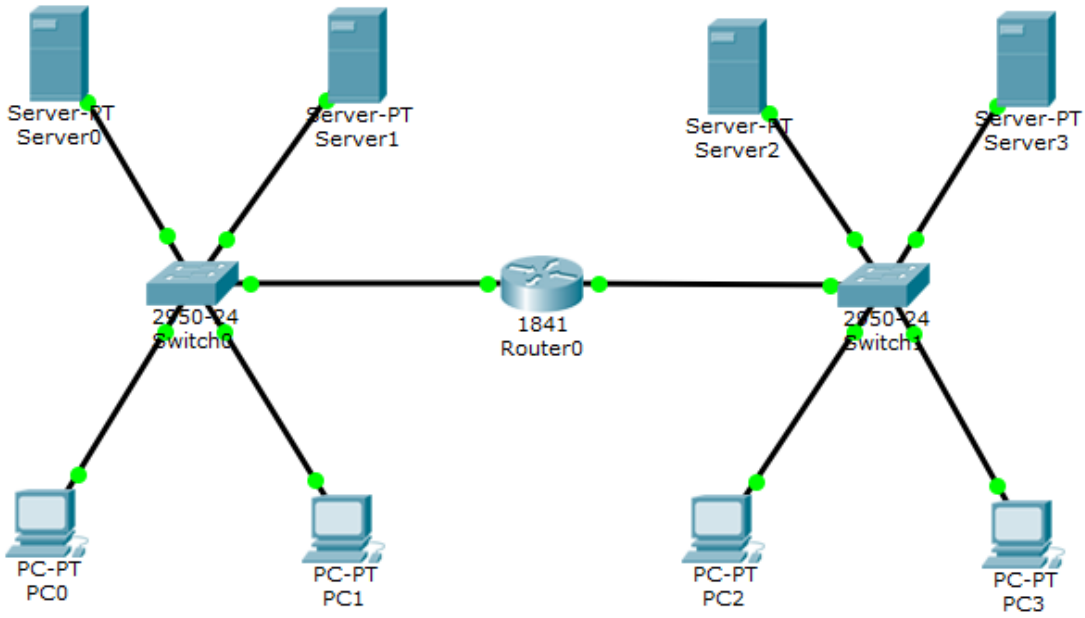
通过这个层次化和分布式的查询机制，DNS 能够在全球范围内提供快速、可靠的域名解析服务，支撑互联网的运作。每一步的缓存都旨在减少延迟，优化性能，同时确保数据的最新和准确性。

**【实验设备】**

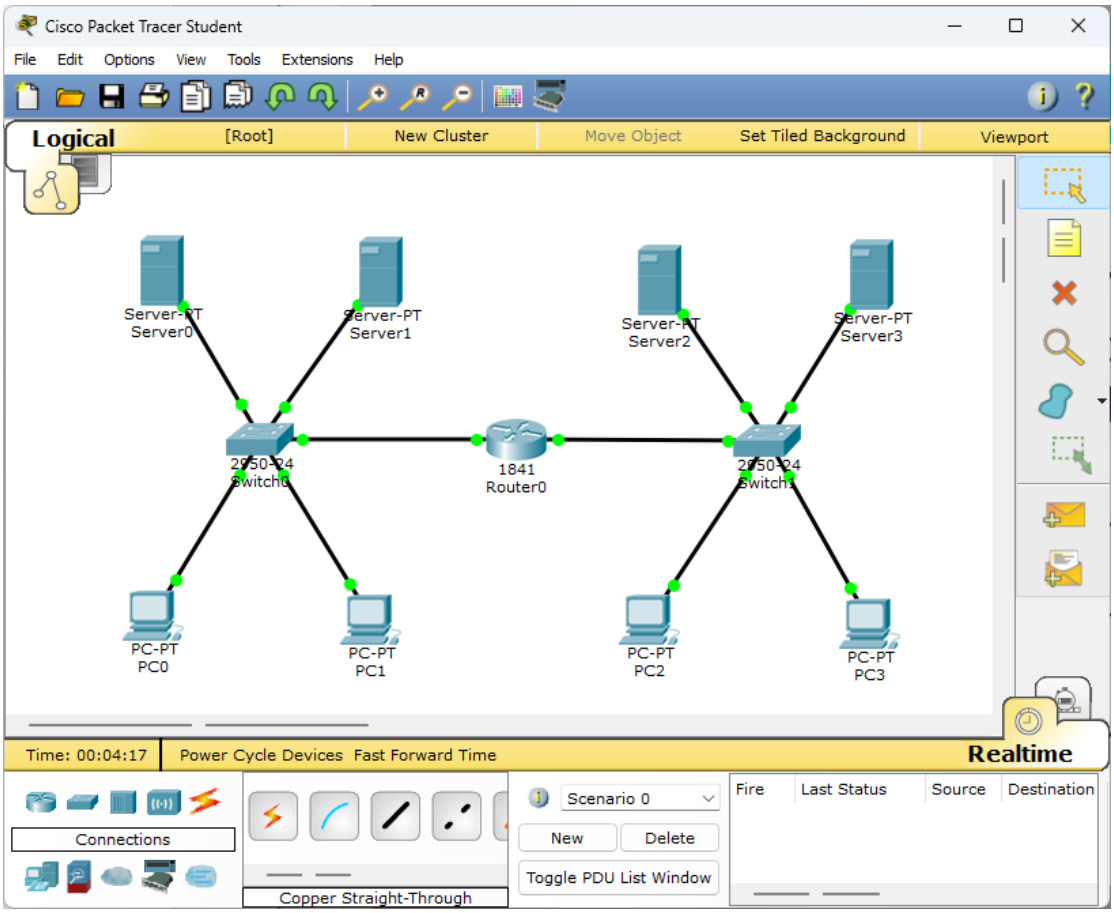
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

**【实验步骤】**

1. 规划网络地址及拓扑图。



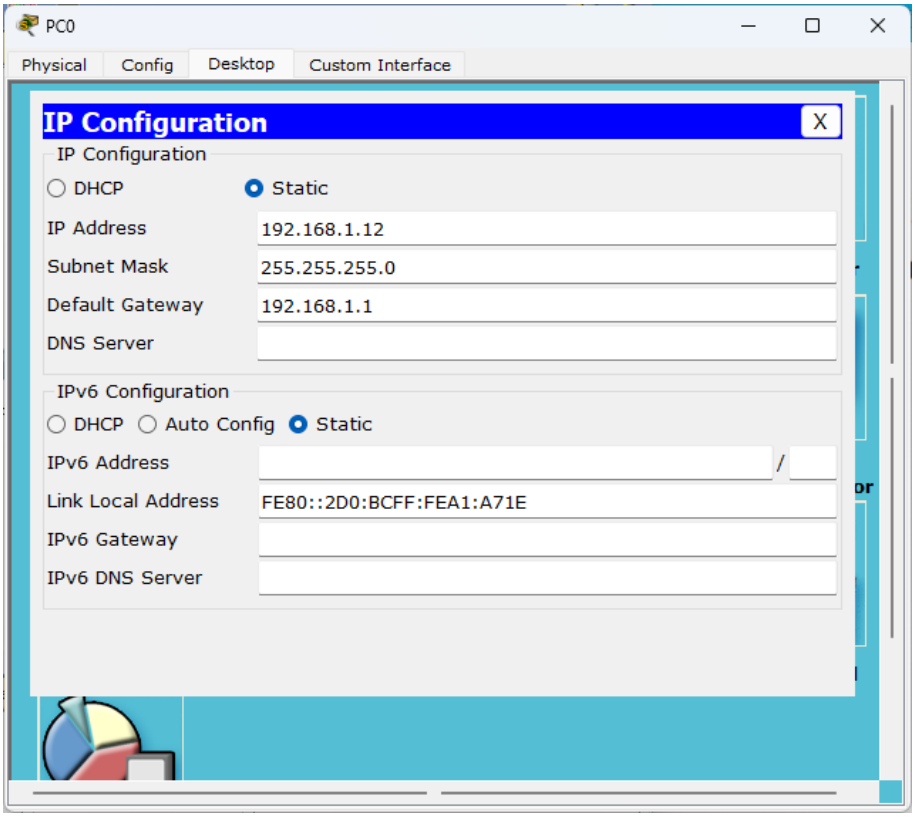

2. 启动 Cisco Packet Tracer，按照上图连接网络。

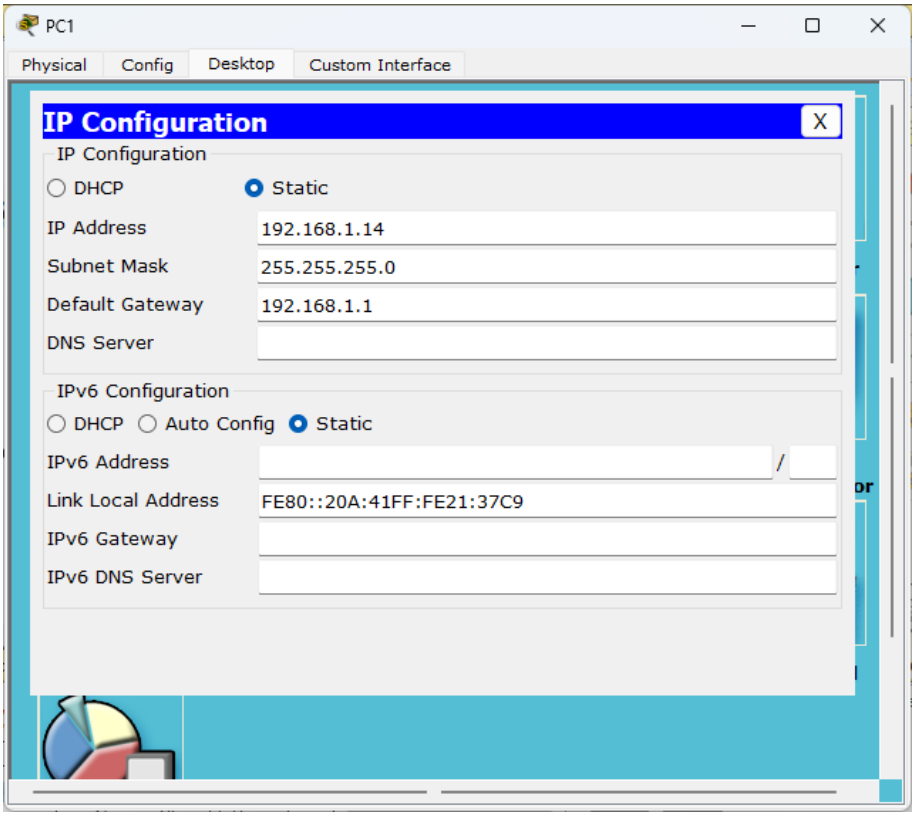


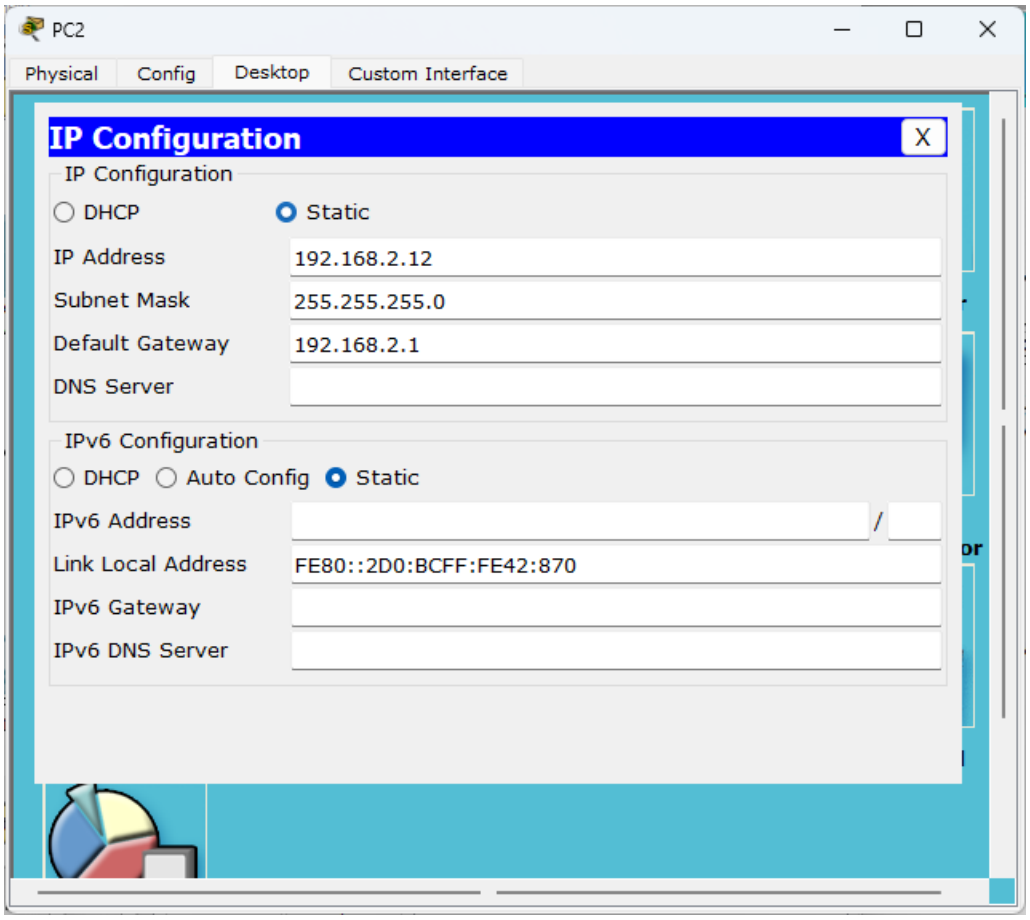

3. 为每台 PC 机配置如下静态 IP 地址、子网掩码和默认网关。

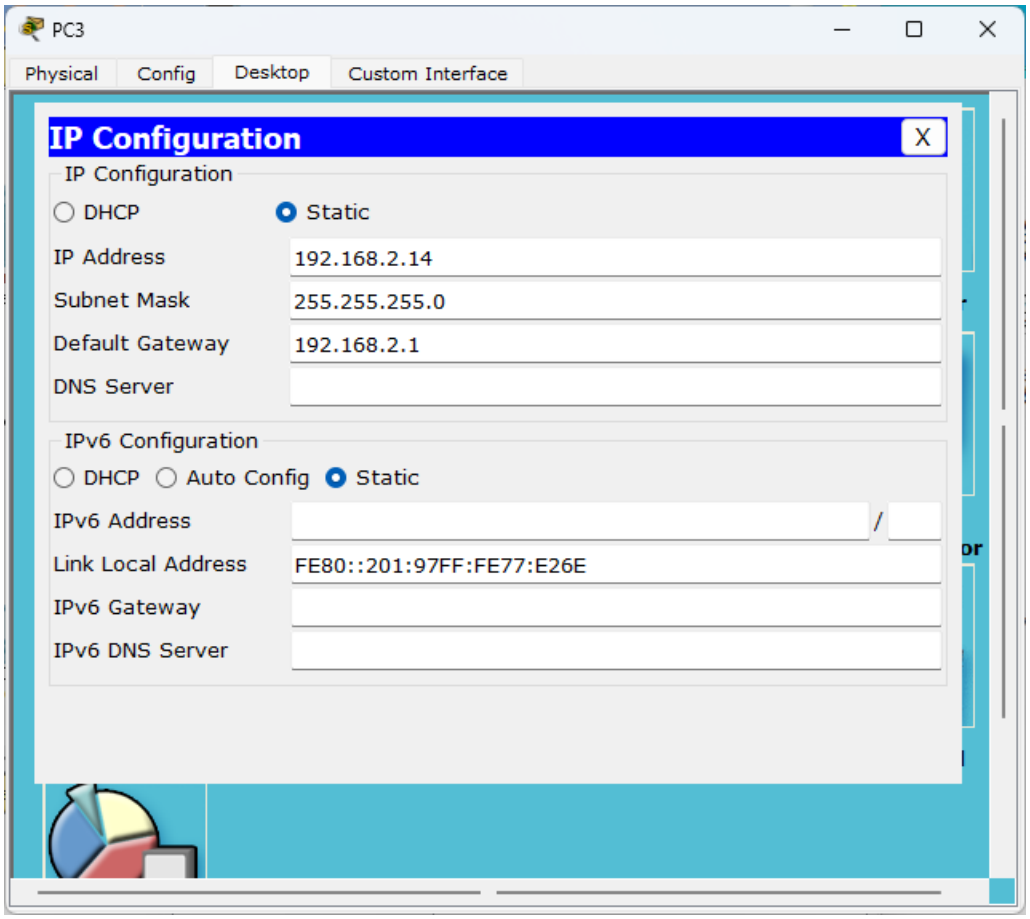
| PC | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|
| PC0 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |

| | | | |
|---|---|---|---|
| PC1 | 192.168.1.14 | 255.255.255.0 | 192.168.1.1 |
| PC2 | 192.168.2.12 | 255.255.255.0 | 192.168.2.1 |
| PC3 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1 |



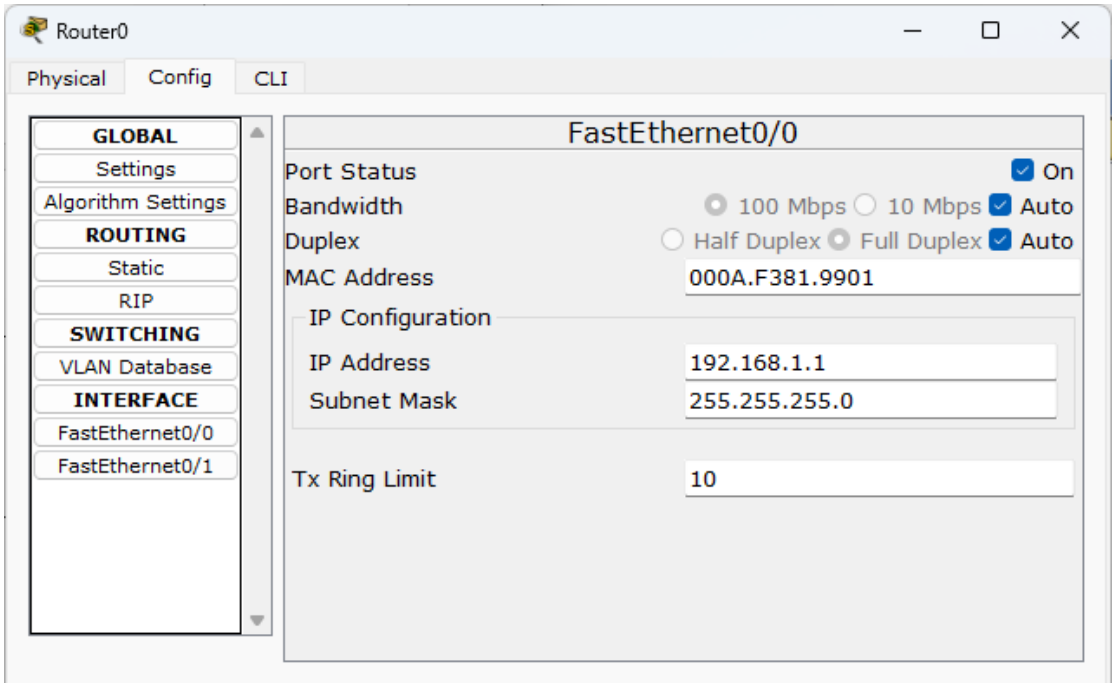



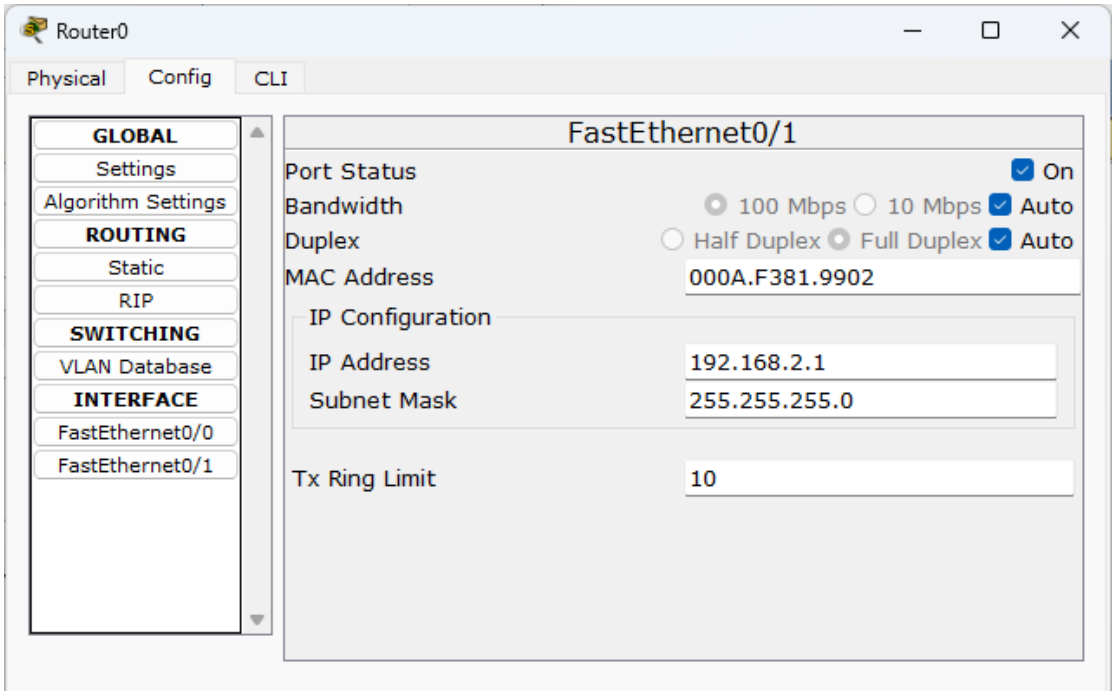

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE42:870
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE77:E26E
IPv6 Gateway
IPv6 DNS Server

4. 参照先前实验（实验 18：动态 IP 地址分配 DHCP 实验）配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```



5. 在路由器 Router0 配置 DHCP。

- 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

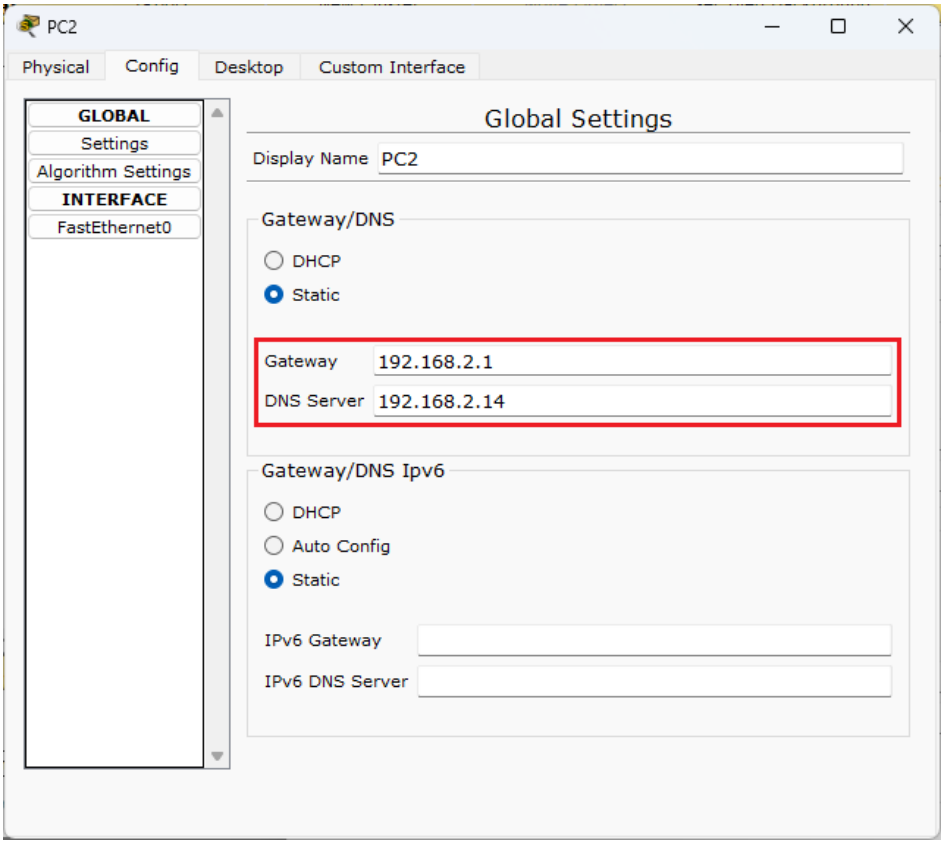
```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

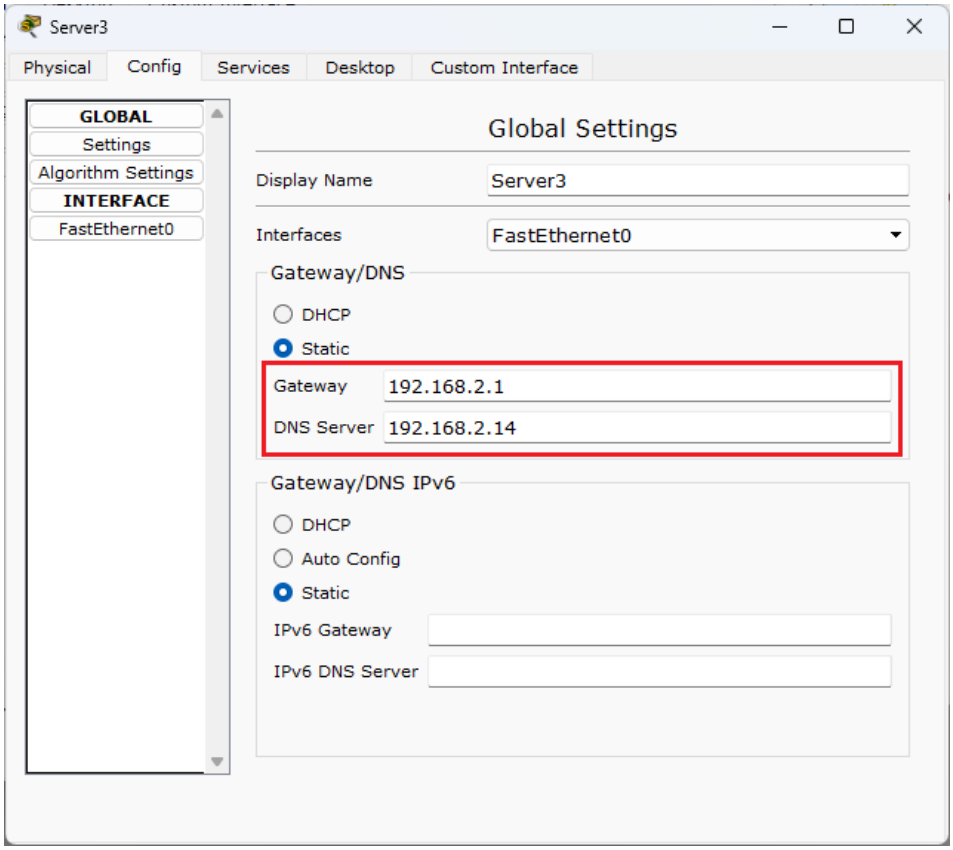
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

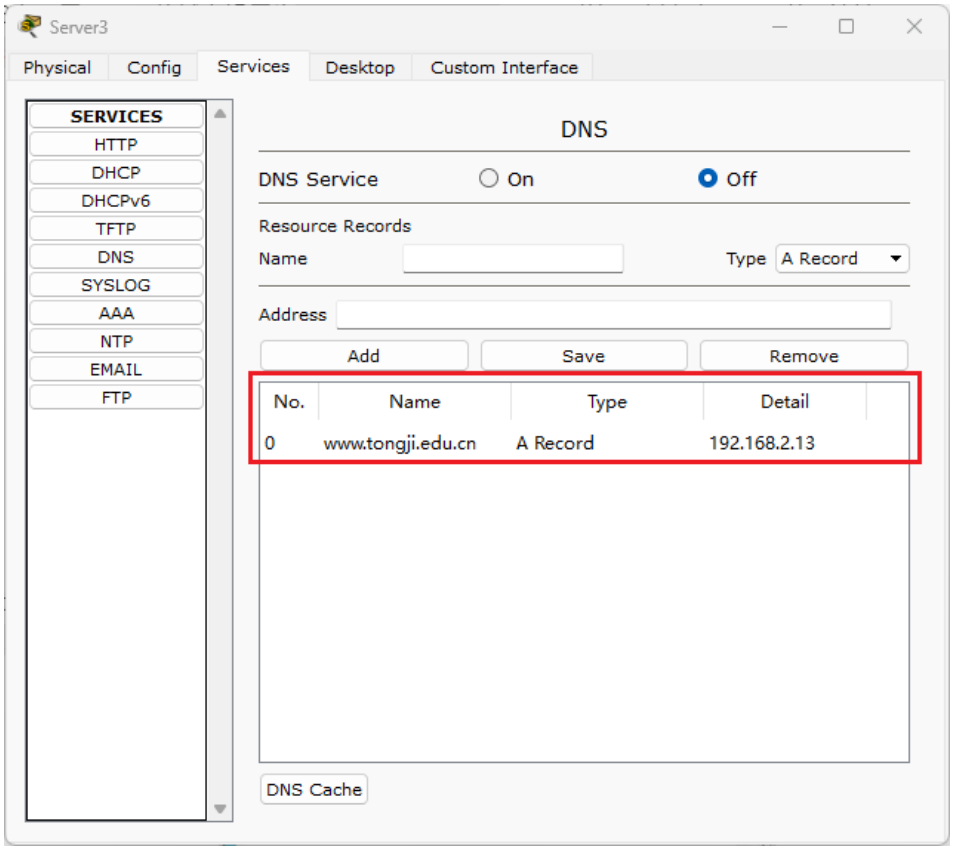
6. 配置 Server 的 Gateway 和 DNS Server。

7. 配置 PC2 的 DNS Server 为 192.168.2.14。设置 PC2 的 DNS Server 与 Server3 的 DNS Server 相同是为了能够通过 Server3 构建映射访问到 Server2。






8. 配置 Server3 的 Services，Name 设置为 www.tongji.edu.cn，Detail 设置为 Server2 的 IP 地址（192.168.2.13）。

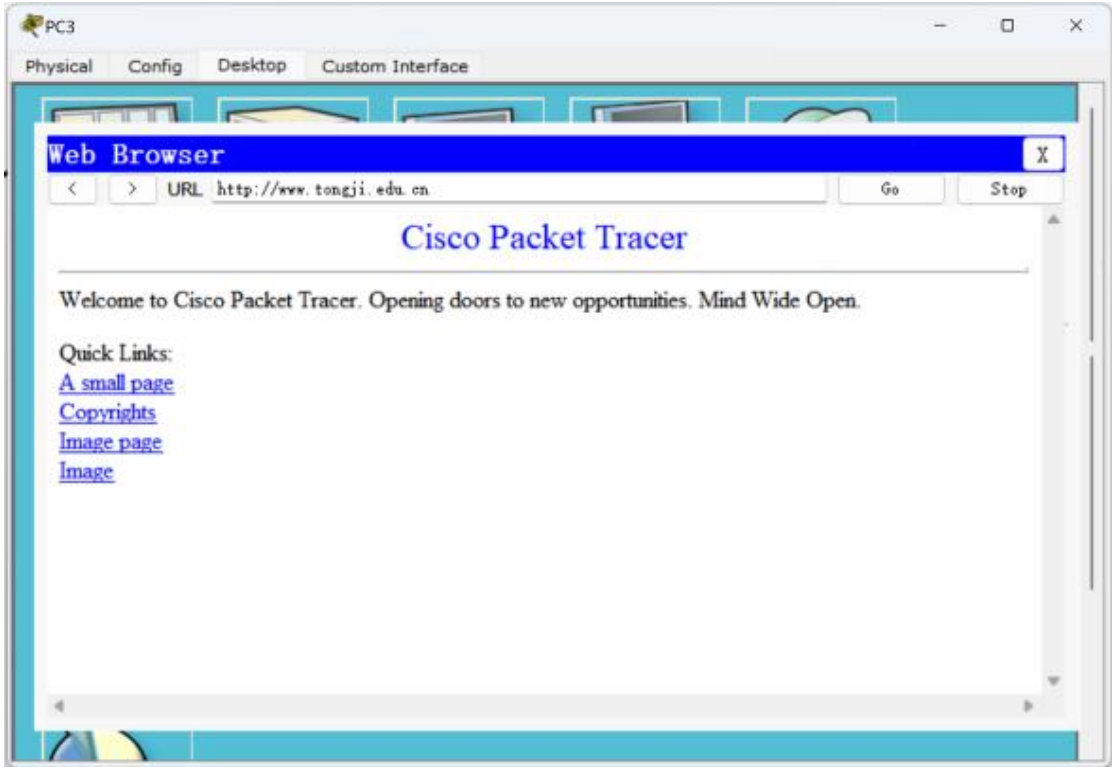


9. 从 Realtime 模式切换至 Simulation 模式。

9.1 在 PC3 的 Web Browser 中输入 http://www.tongji.edu.cn，产生 DNS 数据报文，分析 DNS 报文情况。

9.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

9.3 在 Even List 中的 Info 栏可以查看相关信息。




10. 分析在 Packet Tracer 中 DNS 报文情况。

11. 用 WireShark 抓取 DNS 数据包，查看 DNS 报文字段内容，并解读。

**【实验现象】**

1. 分析在 Packet Tracer 中 DNS 报文情况。

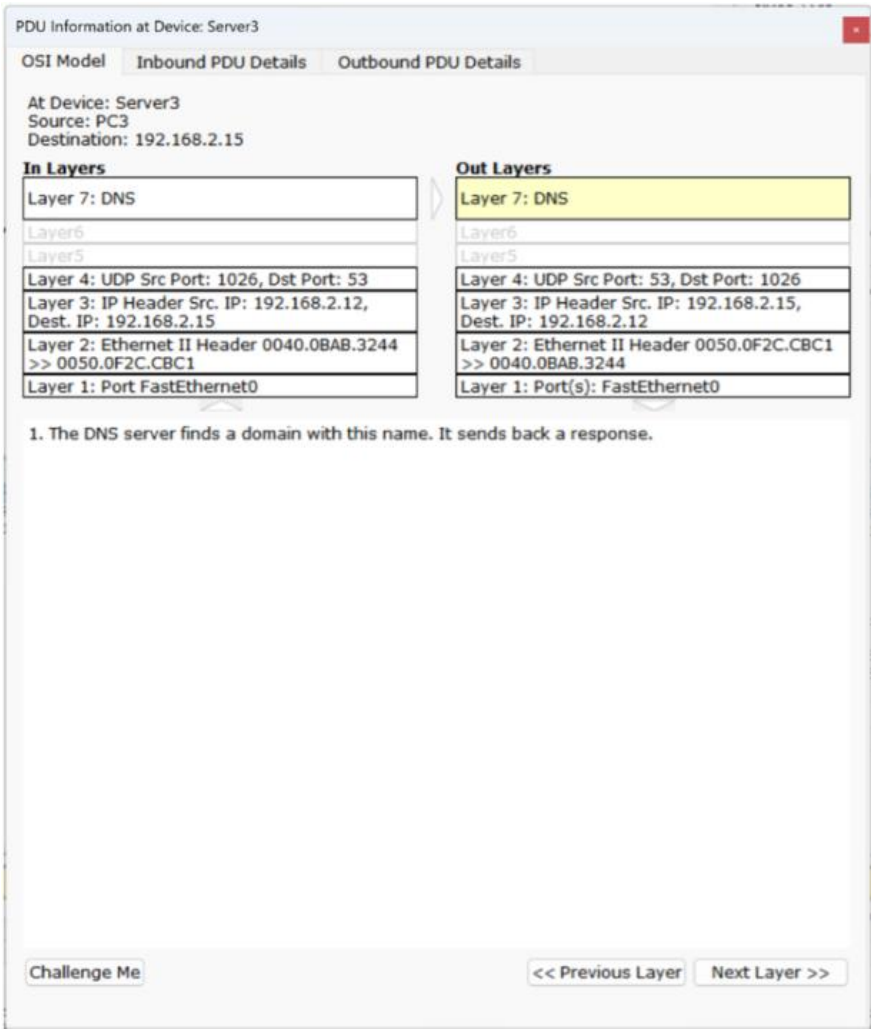
1.1 PDU Information at Device: Server3（OSI Model）

在这张 Packet Tracer 的截图中，我们可以看到 DNS 查询和响应的详细过程，涵盖了各层的信息。这个过程涉及从一个客户端(PC3)到 DNS 服务器(Server3)的 DNS 查询，以及服务器对该查询的响应。

- Inbound PDU Details（入站协议数据单元细节）
  - 源设备：PC3
  - 目的设备：Server3

- 源 IP 地址：192.168.2.12
- 目的 IP 地址：192.168.2.15

- 各层分析：
  - Layer 1（物理层）：Port FastEthernet0
  - Layer 2（数据链路层）：使用 Ethernet II 帧，源 MAC 地址为 0040.0BAB.3244，目的 MAC 地址为 0050.0F2C.CBC1。
  - Layer 3（网络层）：使用 IP 协议，源 IP 地址为 192.168.2.12，目的 IP 地址为 192.168.2.15。
  - Layer 4（传输层）：使用 UDP 协议，源端口 1026，目的端口 53（DNS 服务的标准端口）。
  - Layer 7（应用层）：DNS 层，此处未提供具体的 DNS 查询细节，但通常会包含所查询的域名等信息。




- Outbound PDU Details（出站协议数据单元细节）

- 源设备：Server3
- 目的设备：PC3
- 源 IP 地址：192.168.2.15
- 目的 IP 地址：192.168.2.12

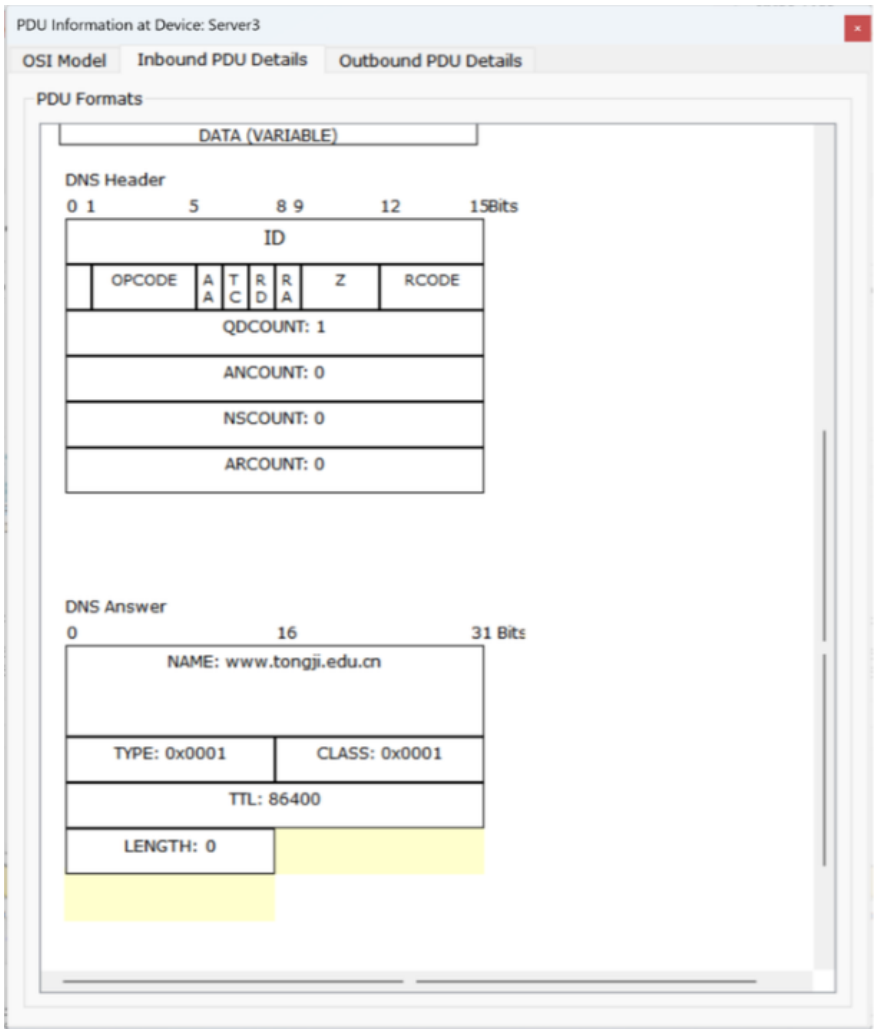
- 各层分析：
  - Layer 1 (物理层)：Port FastEthernet0
  - Layer 2 (数据链路层)：使用 Ethernet II 帧，源 MAC 地址为 0050.0F2C.CBC1，目的 MAC 地址为 0040.0BAB.3244。
  - Layer 3 (网络层)：使用 IP 协议，源 IP 地址为 192.168.2.15，目的 IP 地址为 192.168.2.12。
  - Layer 4 (传输层)：使用 UDP 协议，源端口 53，目的端口 1026。
  - Layer 7 (应用层)：DNS 层，说明 DNS 服务器已找到对应的域名，并发回响应。常见的 DNS 响应会包含请求的域名、解析到的 IP 地址、记录类型（如 A 记录，AAAA 记录等）、TTL 值等。

1.2 PDU Information at Device: Server3（Inbound PDU Details）

在这张图中，我们看到的是 Packet Tracer 模拟环境中一个 DNS 查询响应的详细 PDU（协议数据单元）信息。这个响应显示在设备 Server3 上的出站 PDU 细节。

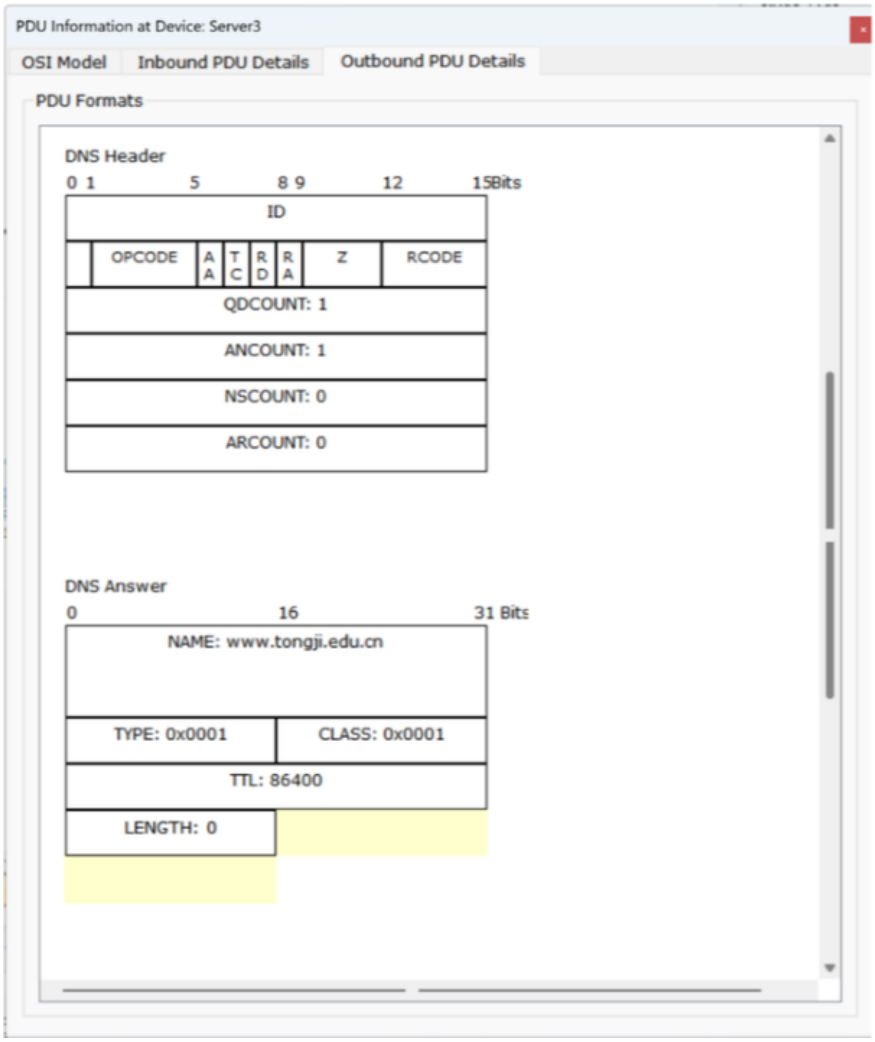
- DNS 头部
  - ID：事务 ID，用于匹配请求和响应。
  - OPCODE：操作码，用于指示查询的类型，这里默认为 0，表示标准查询。
  - AA（Authoritative Answer）：授权回答，此处应为 0，表示响应不是来自权威源。
  - TC（Truncated）：截断，标识消息是否被截断。
  - RD（Recursion Desired）：期望递归，请求希望得到一个递归响应。
  - RA（Recursion Available）：递归可用，服务器可以进行递归查询。
  - Z：保留位，必须为 0。
  - RCODE：响应码，指示查询的状态，此处应为 0，表示无错误。

- QDCOUNT：查询数量，这里为 1，表示一个查询请求。
- ANCOUNT：应答数量，此处为 0，表示没有应答资源记录。
- NSCOUNT：授权名称服务器计数，此处为 0。
- ARCOUNT：附加记录计数，此处也为 0。




- DNS 应答部分
  - NAME：请求的域名，www.tongji.edu.cn。
  - TYPE：查询类型，这里为 0x0001，即 A 记录，请求 IPv4 地址。
  - CLASS：类别，这里为 0x0001，即 IN，表示互联网。
  - TTL（Time To Live）：资源记录可以缓存的时间，这里为 86400 秒（24 小时）。
  - LENGTH：资源数据的长度，这里为 0，表示响应中没有包含实际的 IP 地址。这通常表明 DNS 查询没有成功找到请求的域名对应的 IP 地址，或者查询的记录不存在。

1.3 PDU Information at Device: Server3（Outbound PDU Details）




这张图展示的是在 Packet Tracer 中的一个 DNS 查询的响应。图中详细显示了 DNS 查询响应报文的结构，包括 DNS 头部和应答部分的具体内容。

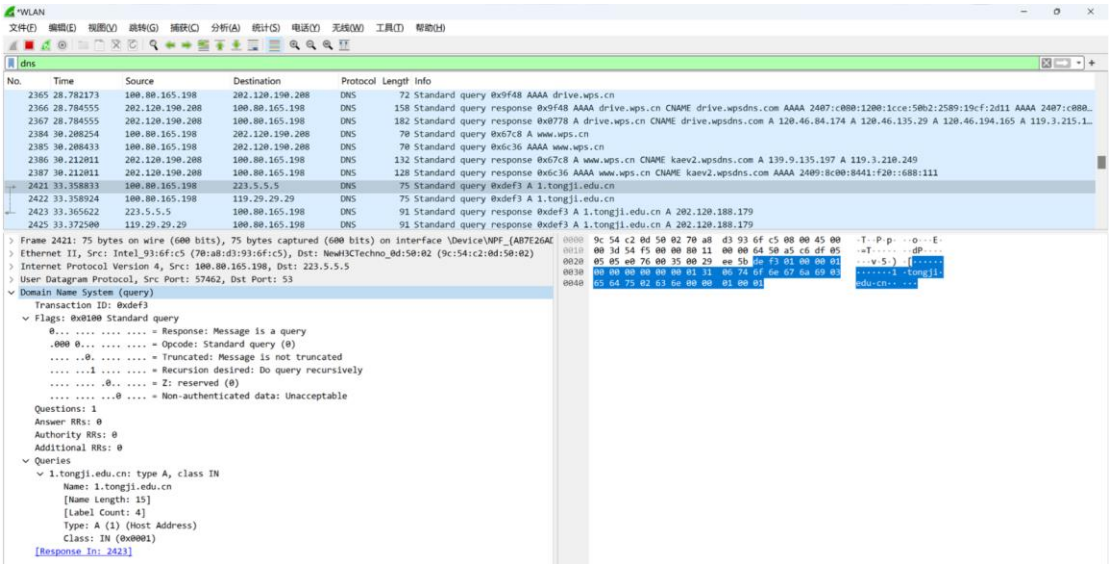
- DNS 头部
  - ID：用于匹配请求和响应的标识符。
  - Opcode：操作码，用于指示 DNS 查询的类型，这里为 0，表示标准查询。
  - AA (Authoritative Answer)：授权回答标志，这里没有具体显示是否设置，但通常用于表明响应是否来自拥有此记录权威的 DNS 服务器。
  - TC (Truncated)：截断标志，用于表明消息是否因过长而被截断，这里没有设置。
  - RD (Recursion Desired)：期望递归标志，通常在查询时设置，希

望 DNS 服务器进行完整的递归查询。

- RA (Recursion Available)：递归可用标志，表示服务器是否支持递归查询，这里没有设置。
- Z：保留字段，必须为 0。
- Rcode：响应代码，这里为 0，表示没有错误。
- QDCOUNT：查询计数，这里为 1，表示有一个查询请求。
- ANCOUNT：应答计数，这里为 1，表示有一个应答。
- NSCOUNT：授权名称服务器计数，这里为 0。
- ARCOUNT：附加记录计数，这里也为 0。

- DNS 应答部分
  - NAME：请求解析的域名，这里为 www.tongji.edu.cn。
  - TYPE：请求的类型，这里为 0x0001，表示是 A 记录查询，用于请求 IPv4 地址。
  - CLASS：类别，这里为 0x0001，通常表示 IN 类，即 Internet。
  - TTL (Time To Live)：DNS 记录的生存时间，这里为 86400 秒，表示该记录可以在 DNS 缓存中保留 24 小时。
  - LENGTH：数据长度，这里为 0，这通常意味着在响应中没有包含 IP 地址，可能是因为查找失败或请求的记录在 DNS 服务器上不存在。

2. 用 WireShark 抓取 DNS 数据包，查看 DNS 报文字段内容，并解读。




在这个 Wireshark 截图中，我们可以看到一个 DNS 查询过程的详细解析。这

份报文捕获展示了从某个设备对域名 1.tongji.edu.cn 进行 DNS 查询的详细过程。下面是报文字段详解：

- 事务 ID（Transaction ID）：0xd9ef3，这是由客户端生成的唯一 ID，用于匹配请求和响应。确保响应与请求对应。
- 标志（Flags）：0x0100，这是 DNS 报文的标志字段，具体细分如下：
  - QR（Query/Response）：0，表明这是一个查询请求。
  - Opcode: 0，标准查询。
  - AA（Authoritative Answer）：0，表明回答不是由权威 DNS 服务器直接提供。
  - TC（Truncated）：0，消息没有被截断。
  - RD（Recursion Desired）：1，客户端希望 DNS 服务器递归查询。
  - RA（Recursion Available）：0，响应中不显示是否支持递归。
- 计数器
  - 问题数（Questions）：1，指明了查询中包含的问题数量。
  - 回答资源记录数（Answer RRs）：0，响应中没有包含答案资源记录。
  - 授权资源记录数（Authority RRs）：0，响应中没有权威 DNS 服务器的信息。
  - 附加资源记录数（Additional RRs）：0，响应中没有附加资源记录。
- 查询（Queries）
  - 名称（Name）：查询的域名是 1.tongji.edu.cn。
  - 类型（Type）：A（1），请求的是 IPv4 地址的解析。
  - 类（Class）：IN（0x0001），表示查询属于互联网类别。
- 响应编号(Response In)：2423，指向 Wireshark 捕获中的具体一帧(2423 号帧)，在该帧中可以找到这个查询的响应。这表明响应与此查询相关联，可以在该帧中查看详细的响应信息。

这个 Wireshark 截图提供了关于一个 DNS 查询的详细技术视图。通过查看 DNS 查询和响应的详细信息能够诊断网络问题，如域名解析失败或延迟等。通过响应编号，我们可以进一步分析响应帧来获取更多关于未能解析域名的原因。

**【分析讨论】**

## 一、分析在 Packet Tracer 中 DNS 报文情况

在 Packet Tracer 的模拟环境中，DNS 报文的分析揭示了从客户端到 DNS 服务器的详细通信过程。通过配置和实施 DNS 查询，我们能够观察到以下现象：

- 网络配置：通过设定静态 IP 地址、子网掩码、默认网关以及 DNS 服务器，确保了网络内部各设备能够正确交换信息。
- DNS 查询过程：DNS 查询的捕获显示，客户端（如 PC3）向 DNS 服务器（如 Server3）发起请求，查询特定域名（例如 www.tongji.edu.cn）的 IP 地址。
- DNS 响应行为：服务器对 DNS 查询的响应揭示了是否成功找到相应的域名记录。在特定配置下，可以看到服务器是否能够返回正确的 IP 地址或者是否发生查询失败（如响应中的 LENGTH 字段为 0 时）。

此部分实验强调了 DNS 配置的正确性对网络服务可达性的重要性，同时也展示了在模拟环境中如何调试和解决网络配置问题。

## 二、用 WireShark 抓取 DNS 数据包并查看 DNS 报文字段内容

使用 WireShark 进行实时数据捕获进一步深化了对 DNS 查询机制的理解，具体包括：

- 详细的头部信息分析：事务 ID、Flags 和其他 DNS 协议特定字段的观察，提供了查询和响应匹配的方式，确保了数据通信的连贯性。
- 查询响应过程：WireShark 的捕获数据显示，查询如 1.tongji.edu.cn 的 DNS 请求，及其对应的响应或缺乏响应（例如响应中答案资源记录为 0），揭示了可能的配置错误或记录缺失。
- 故障诊断：分析响应编号如 2423 号帧，可以具体看到 DNS 响应的内容，进而判断 DNS 服务的健康状况以及可能的配置问题。

这一部分实验强调了实际网络环境中 DNS 查询的重要性，并展示了如何使用专业工具进行网络通信的故障诊断和性能分析。

# 实验 27：组网技术实验

| 姓名 | 学号 | 合作学生 | 指导教师 | 实验地点 | 实验时间 |
|---|---|---|---|---|---|
| 林继申 | 2250758 | 无 | 陈伟超 | 济事楼 330 | 2024/05/23 |

**【实验目的】**

本次组网技术实验的主要目的是学习和实现单臂路由，以促进不同虚拟局域网（VLAN）之间的互联互通。通过配置一个路由器接口上的子接口（逻辑接口），实验旨在实现原本相互隔离的 VLAN 之间的网络互通。这种设置特别适用于需要跨 VLAN 访问的场景，例如公司内不同部门之间的网络访问需求。具体包括：

1. 掌握单臂路由的概念和应用场景。
2. 学习如何配置路由器的子接口来处理不同 VLAN 的交流。
3. 理解并实现 VLAN 的配置和管理。
4. 通过实验设置，检验和分析网络的连通性，以及在特定场景下（如部门间需要通讯时）的网络表现。

**【实验原理】**

**一、单臂路由概述**

单臂路由，又称为 router-on-a-stick，是一种网络配置策略，通过在单一的物理路由器接口上配置多个虚拟的子接口来实现不同虚拟局域网（VLAN）之间的数据交换和互联互通。这种方法允许一台物理路由器利用单个接口来管理多个 VLAN 的流量，通过在物理接口上实现逻辑分割，使每个子接口都可以代表一个单独的 VLAN，并对应配置独立的 IP 路由策略。单臂路由的核心在于使用 802.1Q VLAN 标签技术，这项技术使得来自不同 VLAN 的数据包能够在同一物理接口上传输，而每个数据包的 VLAN 身份通过标签来识别和区分。这种配置方式非常适合那些硬件资源有限但需要处理多个网络分段的场合，例如小型企业或者分布式网络环境，因为它可以显著降低硬件成本，简化网络结构，同时提高网络的可扩展性和灵活性。

**二、单臂路由主要特点**

1. 逻辑子接口配置：在物理接口上创建多个子接口，每个子接口都有自己的 VLAN 标识（通过 802.1Q 标签）和 IP 地址。这样可以使得路由器理解来自不同 VLAN 的数据包，并根据配置进行正确的路由。

2. Trunk 链路：路由器与交换机之间的连接必须配置为 Trunk 模式，以便能够携带多个 VLAN 的数据包。Trunk 链路可以携带属于不同 VLAN 的所有数据包，每个数据包都带有 VLAN 标识。
3. 跨 VLAN 路由：通过配置单臂路由，可以使不同的 VLAN 间能够互相通信。例如，在一个企业环境中，不同部门可能位于不同的 VLAN，通常这些 VLAN 是相互隔离的以提高安全性。通过单臂路由，可以有选择性地允许特定 VLAN 之间的数据流动，如管理层需要访问多个部门的数据。

**三、单臂路由应用场景**

1. 企业网络：适用于需要成本效益的解决方案来实现 VLAN 间的路由，尤其是在小型或中型企业中。
2. 多租户环境：在提供 IT 服务的环境中，可以用单臂路由来隔离不同客户的网络，同时允许必要的通信。
3. 教育机构：学校可以使用单臂路由将教师、学生、行政等网络分开，同时允许行政访问需要的资源。

**四、单臂路由优缺点**

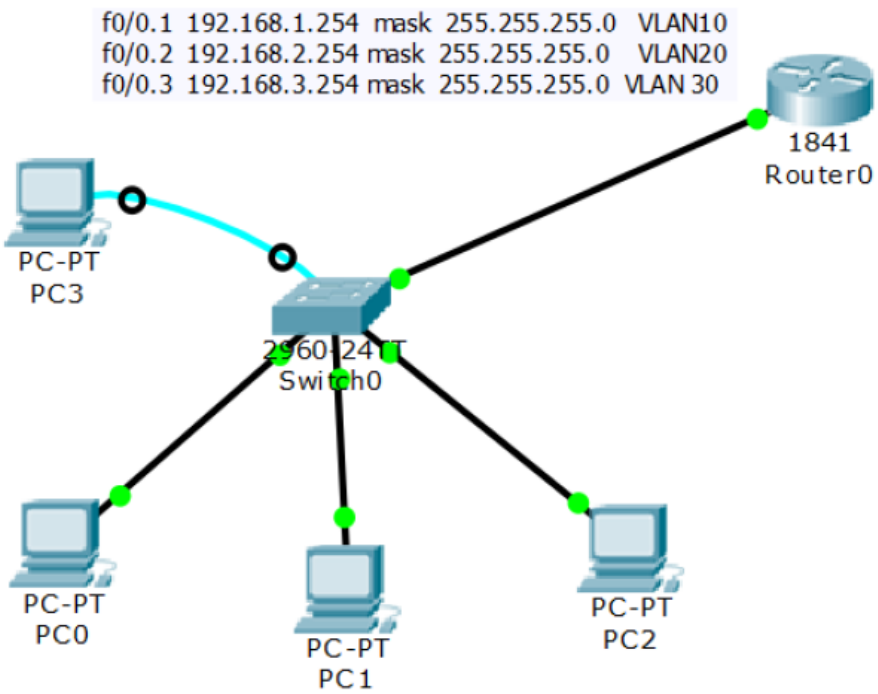
1. 优点
   - 成本效率：相比于为每个 VLAN 配置一个物理接口，单臂路由只需一个物理接口，减少了硬件成本。
   - 简化网络设计：简化了网络的物理布局，降低了管理复杂性。
2. 缺点
   - 带宽限制：所有 VLAN 的数据都通过同一个物理接口传输，可能会在高流量时段造成瓶颈。
   - 安全考虑：虽然有助于 VLAN 间的通信，但配置不当可能导致安全漏洞。

**【实验设备】**

1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

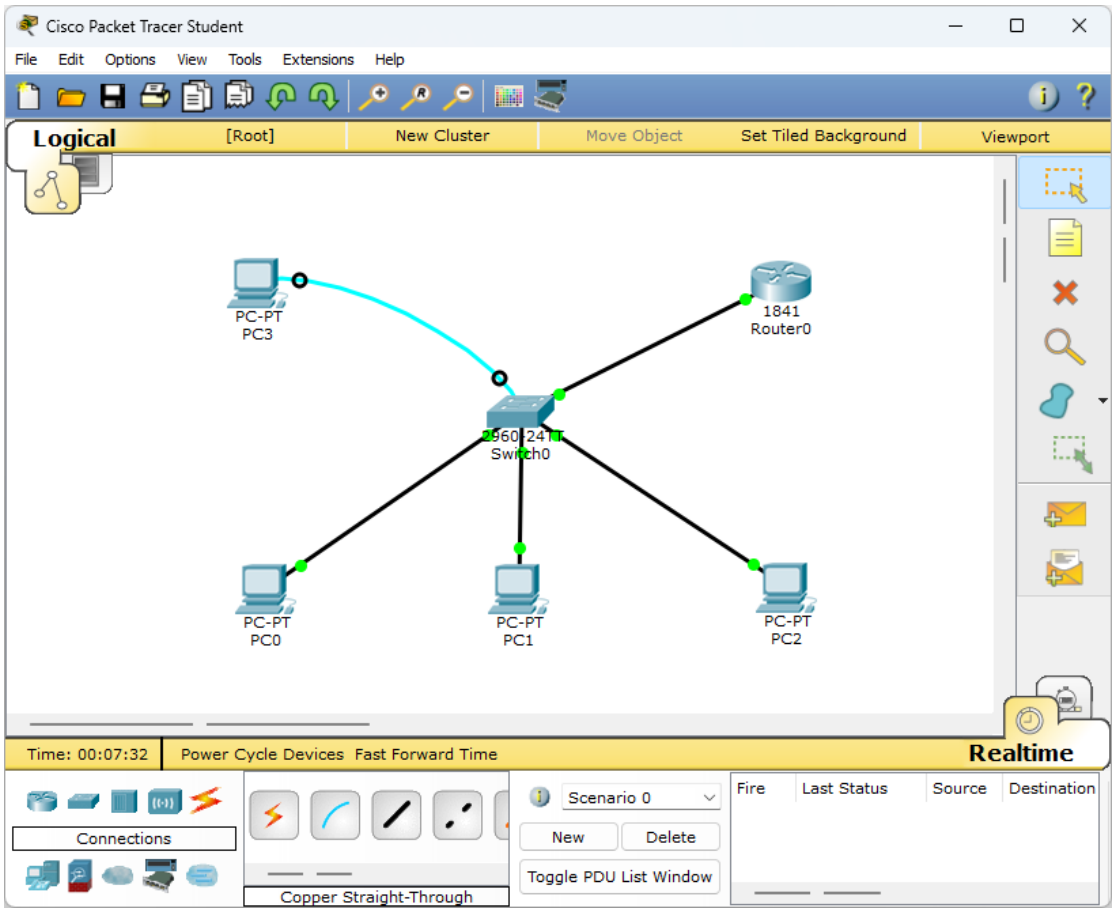
**【实验步骤】**

1. 规划网络地址及拓补图。

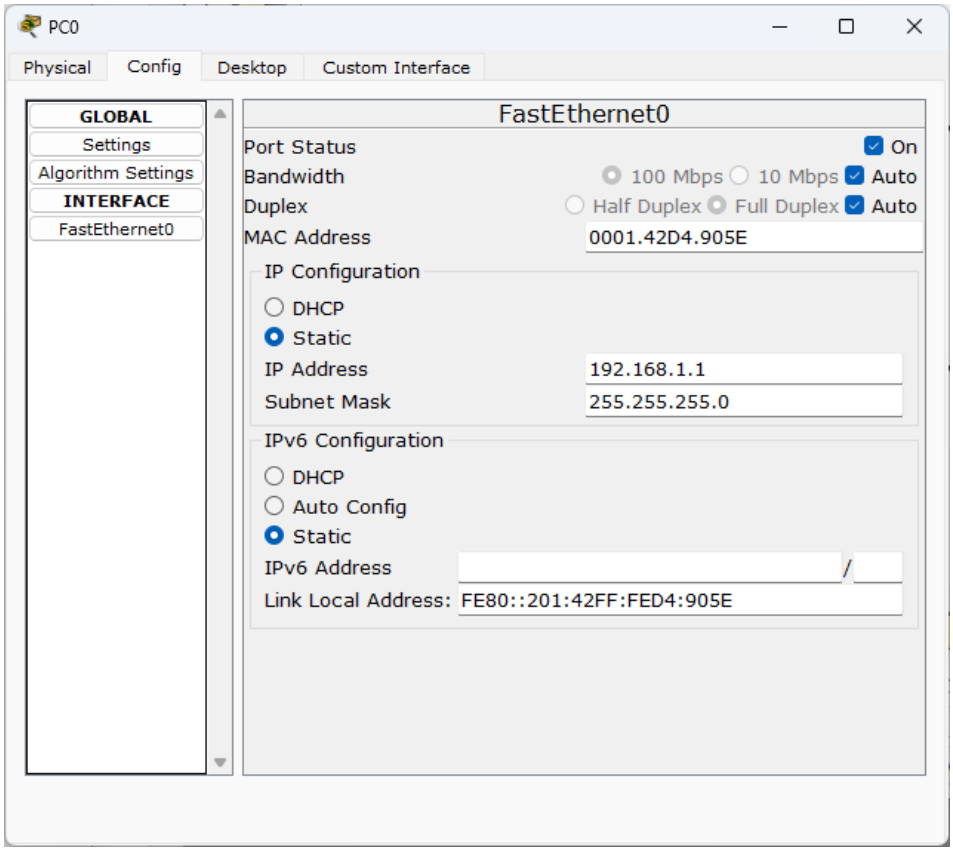


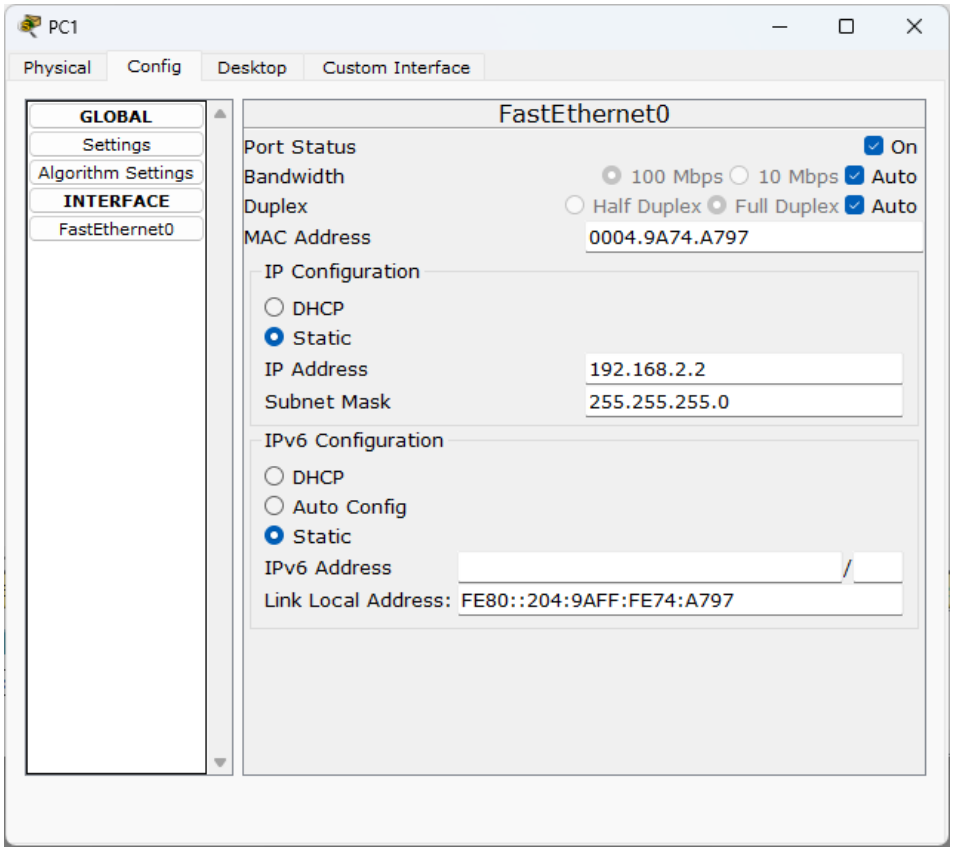

PC0 192.168.1.1 mask 255.255.255.0 F0/1 VLAN10
PC1 192.168.2.2 mask 255.255.255.0 F0/2 VLAN20
PC2 192.168.3.3 mask 255.255.255.0 F0/3 VLAN 30

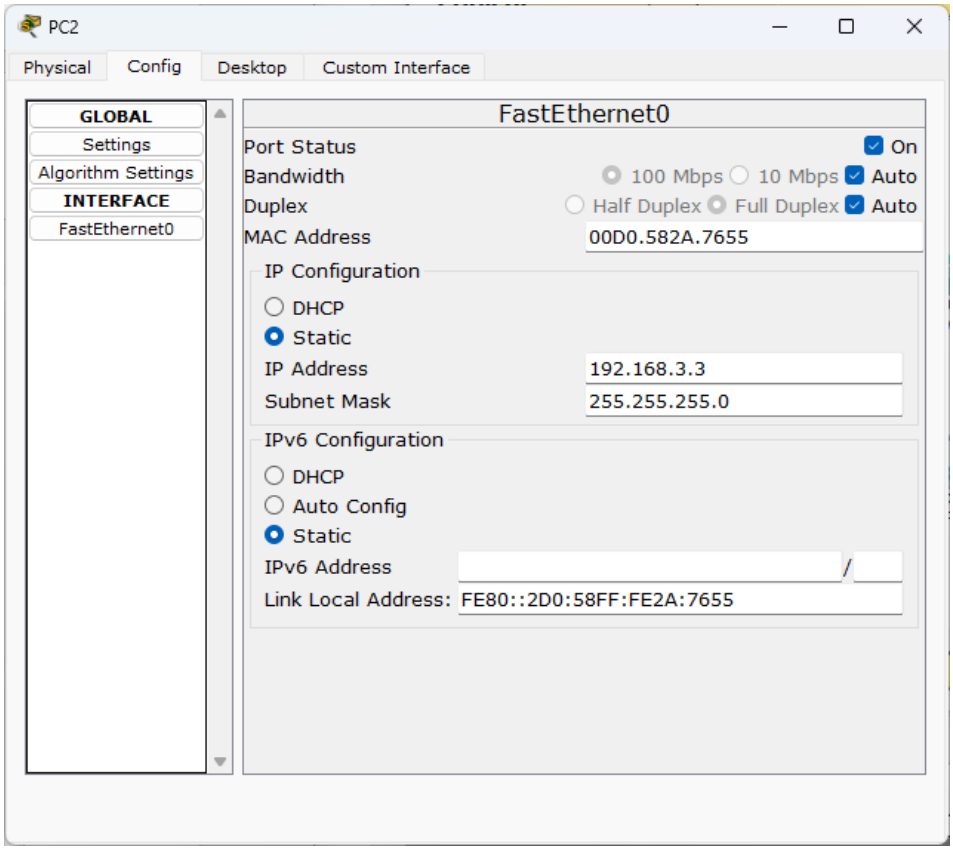
2. 启动 Cisco Packet Tracer 来模拟网络环境，并连接设备。



3. 通过 Config 图形化界面为三台 PC 机配置 IP 及掩码。

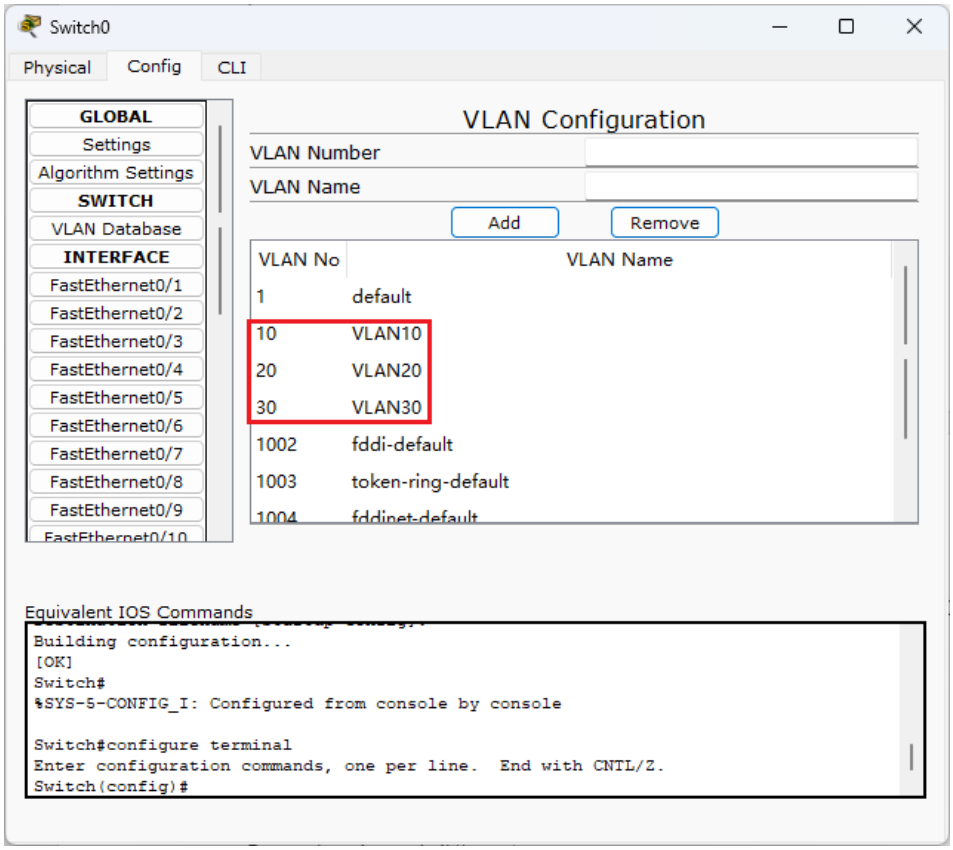


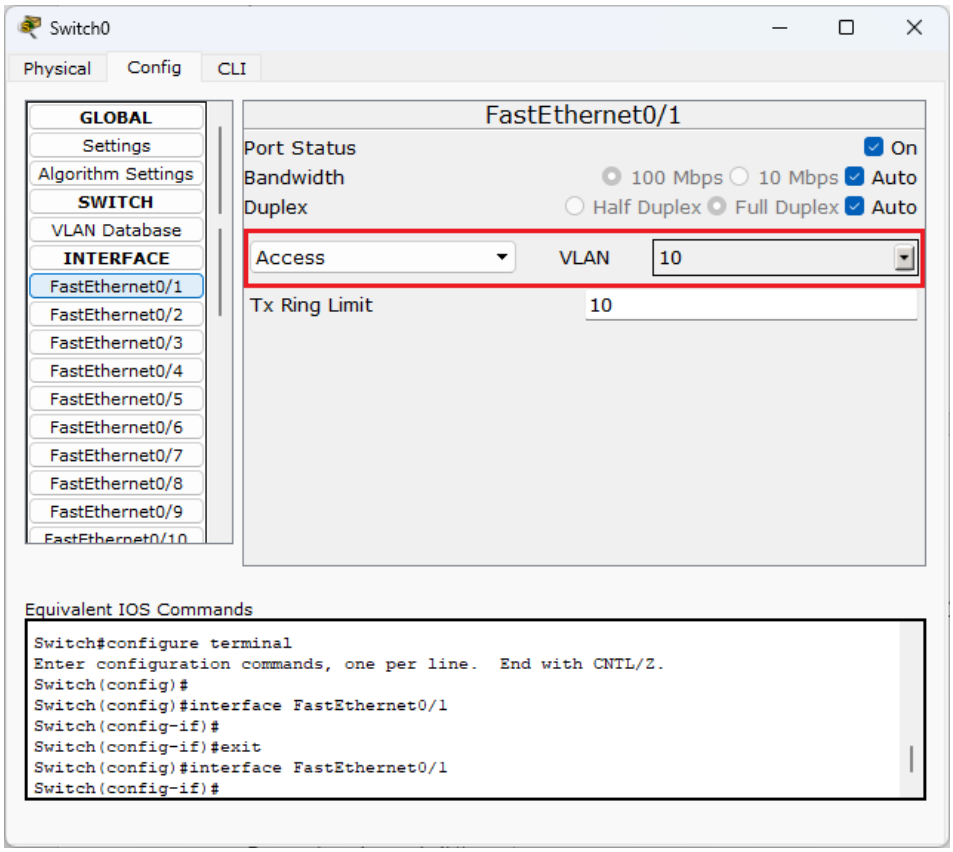



4. 在配置 VLAN 前测试 PC0，PC1，PC2 之间相互 ping，查看并记录实验结果。

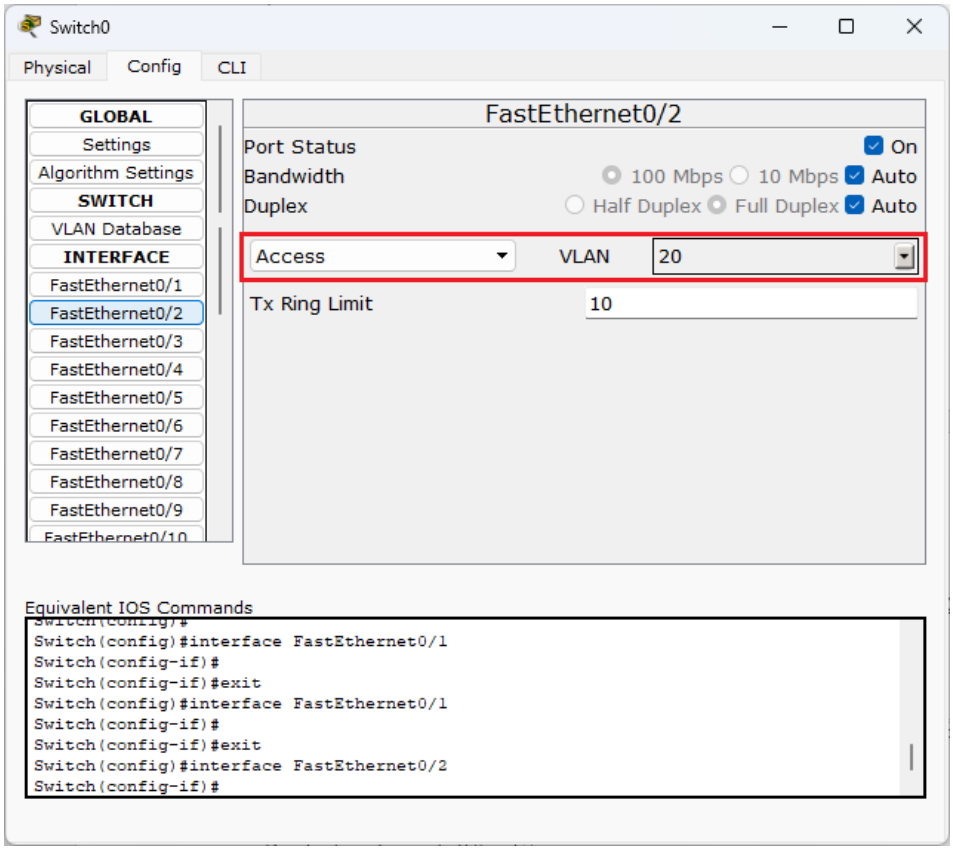
5. 通过图形化界面，为 PC0/PC1/PC2 分别配置 VLAN10，VLAN20，VLAN30。



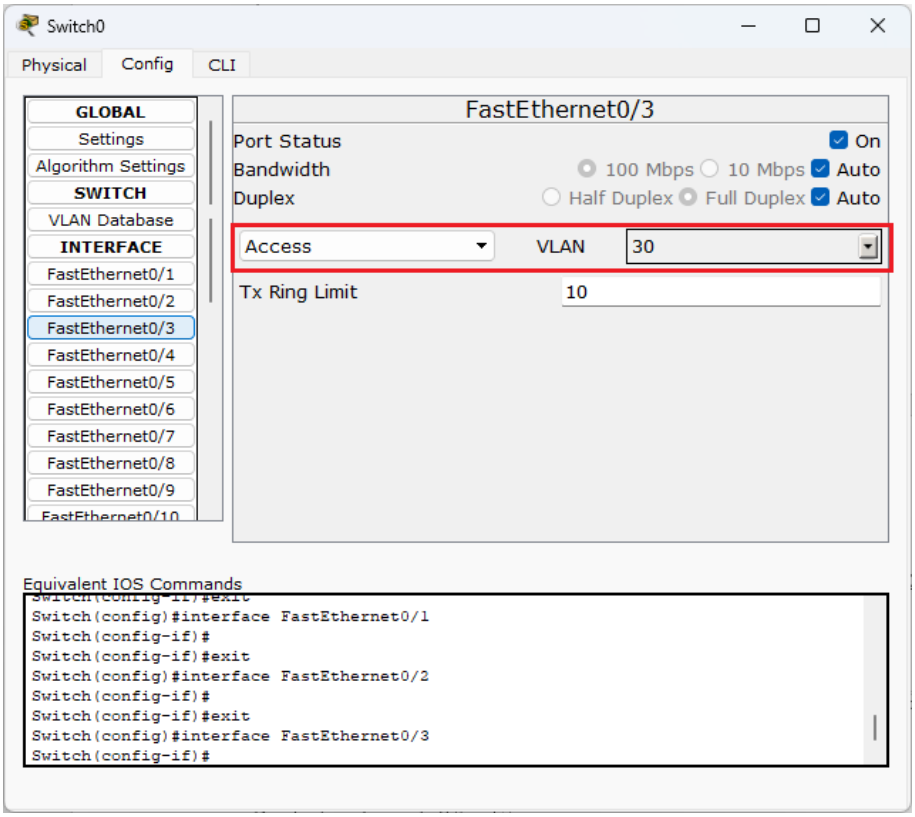
- PC0 配置：192.168.1.1 mask 255.255.255.0 F0/1 VLAN 10



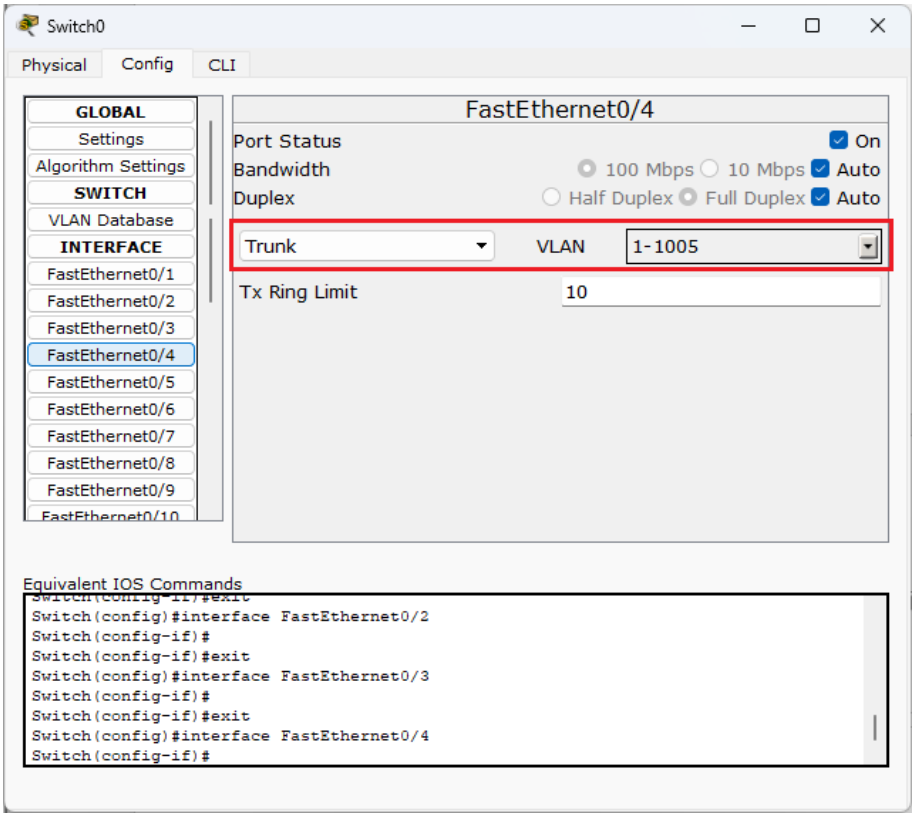

- PC1 配置：192.168.2.2 mask 255.255.255.0 F0/2 VLAN 20



- PC2 配置：192.168.3.3 mask 255.255.255.0 F0/3 VLAN 30




6. 在配置单臂路由前测试 PC0,PC1,PC2 之间相互 ping,查看并记录实验结果。
7. 配置交换机，将连接路由器的端口设置为 Trunk 模式，允许所有 VLAN 通过。



8. 在 Router0 的 CLI 中输入以下命令，配置单臂路由。

- 配置 VLAN10 的网关。

```
interface fa0/0.1
encapsulation dot1q 10
ip address 192.168.1.254 255.255.255.0
exit
```

- 配置 VLAN20 的网关。

```
interface fa0/0.2
encapsulation dot1q 20
ip address 192.168.2.254 255.255.255.0
exit
```

- 配置 VLAN30 的网关。

```
interface fa0/0.3
encapsulation dot1q 30
ip address 192.168.3.254 255.255.255.0
exit
```

9. 在配置单臂路由后测试 PC0,PC1,PC2 之间相互 ping,查看并记录实验结果。

**【实验现象】**

1. 在配置 VLAN 前，PC0，PC1，PC2 之间相互 ping，实验现象为：PC0、PC1、PC2 之间相互 ping 通，通信成功。
2. 在配置单臂路由前，PC0，PC1，PC2 之间相互 ping，实验现象为：用 PC0 分别 ping PC1、PC2，用 PC1 分别 ping PC0、PC2，用 PC2 分别 ping PC1、PC0. 均请求失败。
3. 在配置单臂路由后，PC0，PC1，PC2 之间相互 ping，实验现象为：PC0、PC1、PC2 之间相互 ping 通，通信成功。

**【分析讨论】**

**一、配置 VLAN 前的 Ping 测试**

在配置 VLAN 之前，PC0、PC1 和 PC2 位于同一个广播域内，没有进行 VLAN 划分。这意味着所有设备都在同一个网络中，可以自由地互相通信。因此，在实验现象中观察到 PC0、PC1、PC2 之间可以相互 ping 通且通信成功，这是因为在同一个 VLAN（或未划分 VLAN 时的默认 VLAN）中，所有设备都可以直接通过 MAC 地

址学习和 ARP 解析来发现对方的位置并进行通信。

**二、配置单臂路由前的 Ping 测试**

在对 PC0、PC1 和 PC2 配置不同的 VLAN 后（VLAN10, VLAN20, VLAN30），这三台 PC 机分别位于三个不同的广播域中。VLAN 的主要功能是进行网络隔离，使得不同 VLAN 的设备不能直接通信，除非通过路由器进行路由。由于在这一步中还没有配置单臂路由，路由器尚未对跨 VLAN 的数据包进行处理，因此 PC0、PC1 和 PC2 无法跨 VLAN 通信，导致实验现象中的 ping 请求失败。

**三、配置单臂路由后的 Ping 测试**

配置单臂路由后，路由器的每个子接口被配置为不同 VLAN 的网关。通过 802.1Q 标签技术，这些子接口可以正确地识别和处理来自不同 VLAN 的数据包。路由器为每个 VLAN 间提供了必要的路由功能，使得属于不同 VLAN 的 PC 机能够通过路由器相互通信。因此，在单臂路由配置完成后，PC0、PC1 和 PC2 能够成功进行跨 VLAN 的 ping 通信。这表明路由器正确地处理了 VLAN 间的路由需求，使得不同 VLAN 的设备可以根据需要安全地互联互通。

**四、简单组网设计**

**（一）组网设计需求**

某公司三个部门，每部门 20 人，每人一台 PC 机，每个部门在同一网段，部门内机器彼此可以互访，不同部门之间平时网络相互隔离，但三个部门的工作人员混在一起办公。假如年末，公司这三个部门之间网络需保持互通，以便网络互通“联欢”，请给出网络解决方案。

**（二）组网设计方案**

为满足三个部门内部互访及部门间隔离的需求，可以为每个部门设置独立的虚拟局域网（VLAN）。选择合适的私有地址空间和子网掩码，确保每个部门内足够的 IP 地址供分配，同时易于管理和扩展。

1. 给出网络规划、地址及掩码（内网地址）

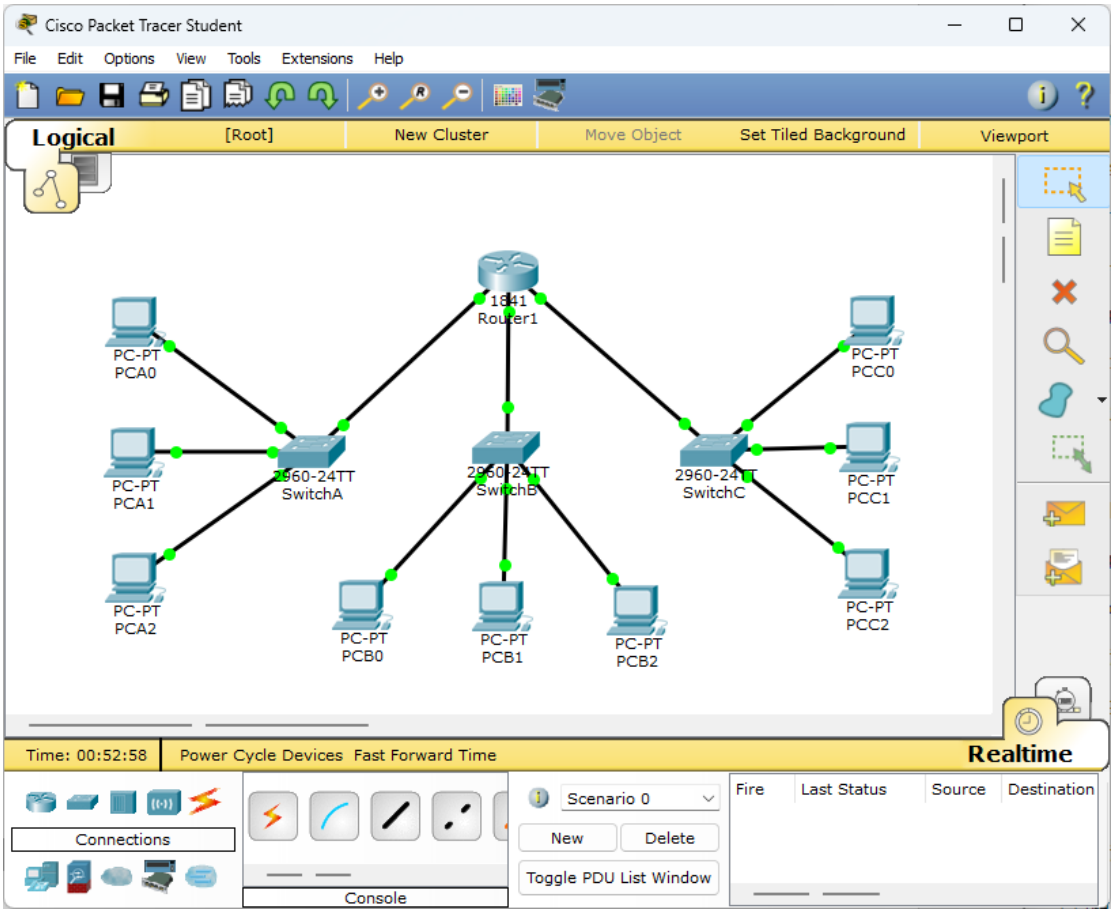
| 部门 | 部门 A | 部门 B | 部门 C |
|---|---|---|---|
| 网络地址 | 192.168.10.0/24 | 192.168.20.0/24 | 192.168.30.0/24 |
| 广播地址 | 192.168.10.255 | 192.168.20.255 | 192.168.30.255 |
| 可用地址 | 192.168.10.1 至 | 192.168.20.1 至 | 192.168.30.1 至 |

| | 192.168.10.254 | 192.168.20.254 | 192.168.30.254 |
|---|---|---|---|
| 子网掩码 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |

2. 规划硬件端口分配
   - 路由器：路由器配置三个子接口处理来自三个 VLAN 的数据。
     - fa0/0.10：VLAN10 的网关（192.168.10.254）
     - fa0/0.20：VLAN20 的网关（192.168.20.254）
     - fa0/0.30：VLAN30 的网关（192.168.30.254）
   - 交换机：配置为支持 Trunk 模式，连接路由器的 fa0/0 端口，确保所有 VLAN 数据能够通过一个物理接口传输。
   - PC 分配：每个部门分配 20 个端口，分别配置到对应的 VLAN。
3. 每个部门至少三个终端且配置（每部门三个为例）
   - 部门 A
     - PCA0：IP 192.168.10.1，掩码 255.255.255.0
     - PCA1：IP 192.168.10.2，掩码 255.255.255.0
     - PCA2：IP 192.168.10.3，掩码 255.255.255.0
   - 部门 B
     - PCB0：IP 192.168.20.1，掩码 255.255.255.0
     - PCB1：IP 192.168.20.2，掩码 255.255.255.0
     - PCB2：IP 192.168.20.3，掩码 255.255.255.0
   - 部门 C
     - PCC0：IP 192.168.30.1，掩码 255.255.255.0
     - PCC1：IP 192.168.30.2，掩码 255.255.255.0
     - PCC2：IP 192.168.30.3，掩码 255.255.255.0
4. 在模拟器配置

   使用 Cisco Packet Tracer 模拟器配置上述网络。包括路由器的子接口配置、交换机的 Trunk 配置、以及 PC 的静态 IP 配置。
5. 测试设备的连通性
   - VLAN 内连通性测试：在每个 VLAN 内部使用 ping 命令测试 PC 之间的连通性。

- VLAN 间连通性测试：初始配置下，VLAN 间不应通信，测试确认隔离性。




**（三）年末联欢网络互通解决方案**

为了在年末联欢时实现三个部门之间的网络互通，我们可以通过配置访问控制列表（ACL）来控制和管理 VLAN 间的流量。

1. 定义 ACL 规则

创建扩展 ACL 以允许每个 VLAN 内的主机访问其他两个 VLAN 的网络。需要为从每个 VLAN 到其他两个 VLAN 的通信分别创建一组规则。

- 部门 A 访问部门 B 和 C：

```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

- 部门 B 访问部门 A 和 C：

```
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.30.0
```

```
0.0.0.255
```

- 部门 C 访问部门 A 和 B：

```
access-list 103 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 103 permit ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

2. 应用 ACL 到路由器接口

将创建的 ACL 应用到路由器的相应子接口上，控制进出的数据包。对于每个子接口配置入站 ACL。

- 部门 A 访问部门 B 和 C：

```
interface fa0/0.10
ip access-group 101 in
```

- 部门 B 访问部门 A 和 C：

```
interface fa0/0.20
ip access-group 102 in
```

- 部门 C 访问部门 A 和 B：

```
interface fa0/0.30
ip access-group 103 in
```

3. 测试和验证

使用 ping 命令检查 ACL 规则是否正确实施，确保各部门能够相互访问，确保不影响部门内部的网络通信。

4. 临时性配置

记得在联欢活动结束后，移除对应的 ACL 设置，为联欢活动添加的特定规则，以保持原有的网络隔离策略。