

**《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 {} 月 {} 日

**目录**

[实验01：网络相关进程与服务实验 2](#_Toc162560563)

[实验02：网络端口地址实验 9](#_Toc162560564)

[实验03：网络线的制作和测试实验 15](#_Toc162560565)

[实验04：基本网络测试工具及应用工具实验 19](#_Toc162560566)

[实验05：主机路由实验 36](#_Toc162560567)

[实验06：异步串口通信电缆制作实验 43](#_Toc162560568)

[实验07：异步串口通信收发实验 47](#_Toc162560569)

[实验08：IOS的基本操作（路由器的基本操作）实验 54](#_Toc162560570)

[实验09：VLAN配置实验 60](#_Toc162560571)

[实验10：静态路由配置实验 64](#_Toc162560572)

[实验11：蓝牙通信实验 74](#_Toc162560573)

[实验： 81](#_Toc162560574)

# 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】**

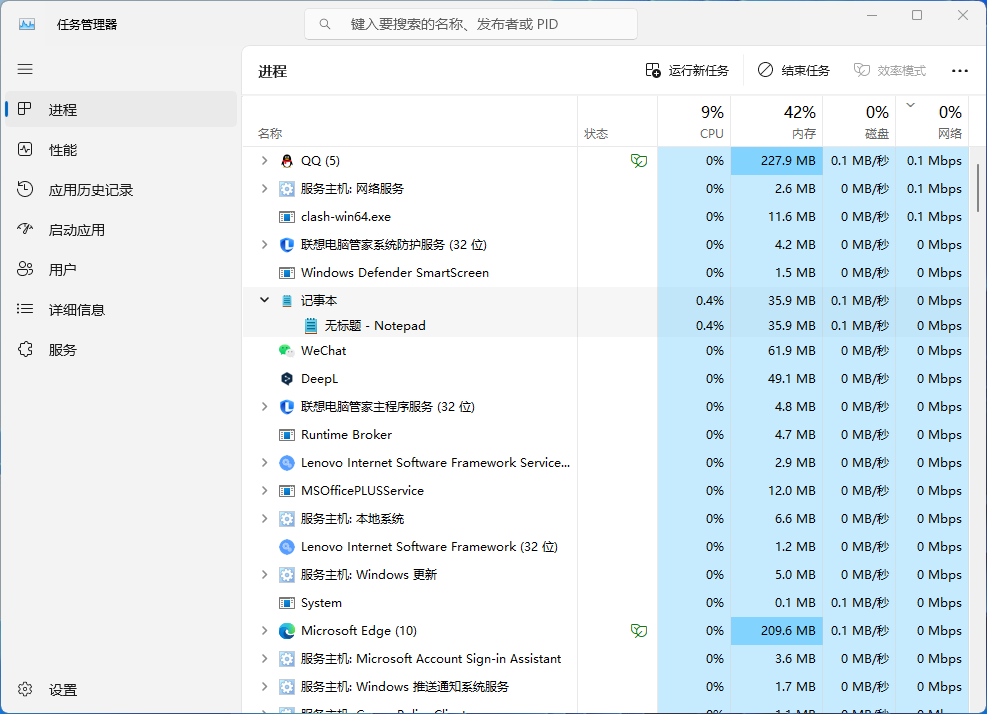
1. 操作系统：Windows 11
2. 网络环境：Wi-Fi连接
3. 应用程序：记事本、画图

**【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。



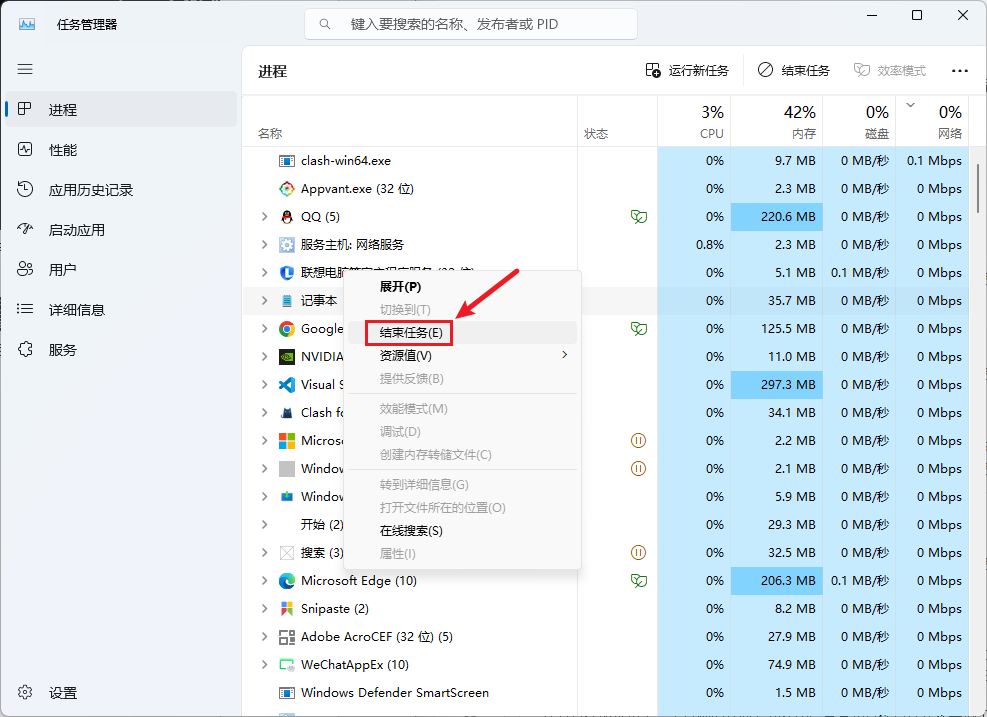
1. 在命令行通过中tasklist命令列出所有正在运行的进程。可以查看Notepad.exe的PID为26604。



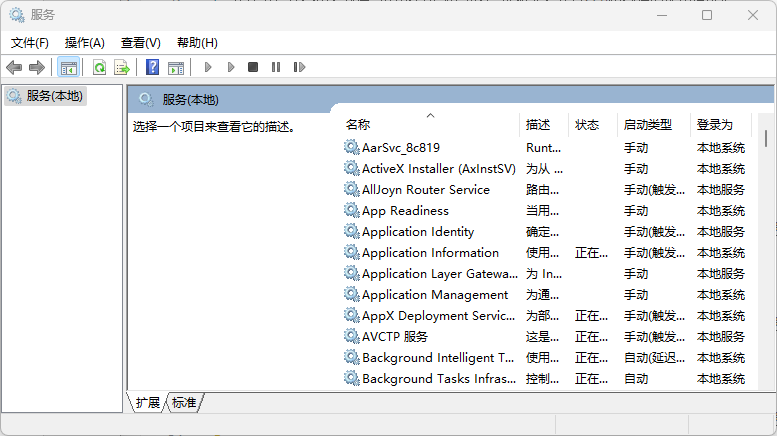
1. 在命令行通过中taskkill /PID 26604命令结束记事本应用程序的进程，可以观察记事本应用程序被关闭。



1. 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。



1. 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>

1. 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](http://www.tongji.edu.cn)发送的响应无效，错误代码为ERR\_SSL\_PROTOCOL\_ERROR”。



1. 在浏览器中输入[https://www.tongji.edu.cn:80](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](http://www.tongji.edu.cn)发送的响应无效，错误代码为ERR\_SSL\_PROTOCOL\_ERROR”。



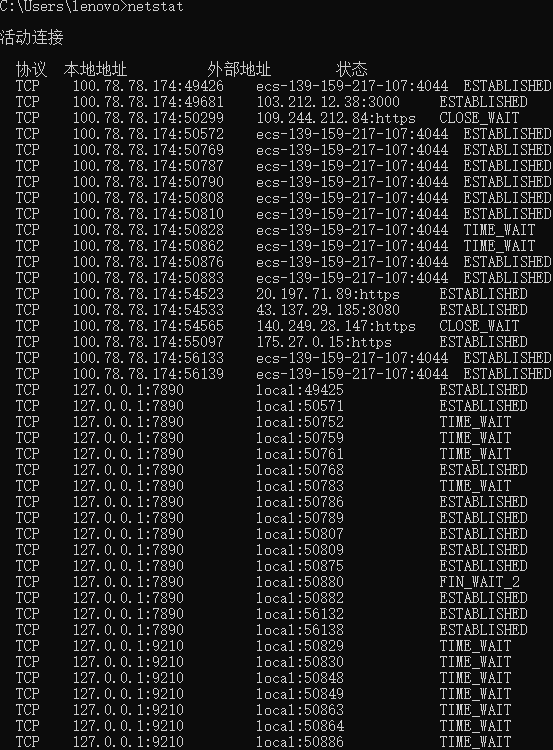
1. 在浏览器中输入<http://www.tongji.edu.cn:8080>并访问，显示“502 Bad Gateway”。



1. 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。



1. 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。



**【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>

1. 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。

1. 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。

1. 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。

1. 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。

1. 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。

1. 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。

1. 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。

1. 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 |

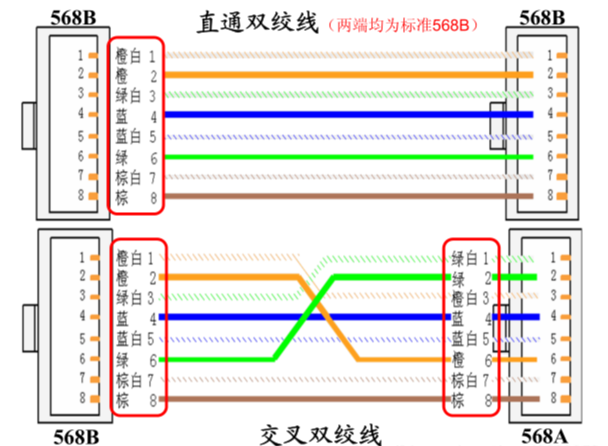
标准568B的线序如下：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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）。

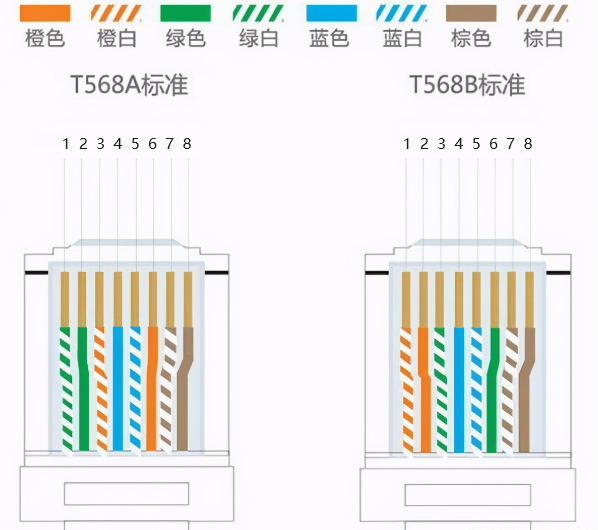
交叉线用于将计算机与计算机直接相连、交换机与交换机直接相连，也被用于计算机直接接入路由器的以太网口。根据568A标准和568B标准。



**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】**

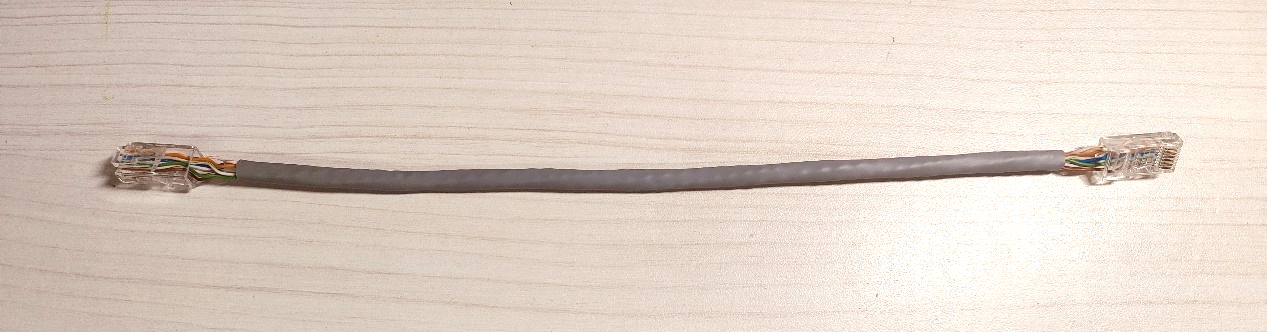
1. 双绞线
2. 水晶头（RJ-45接头）
3. 压线钳
4. 通断仪

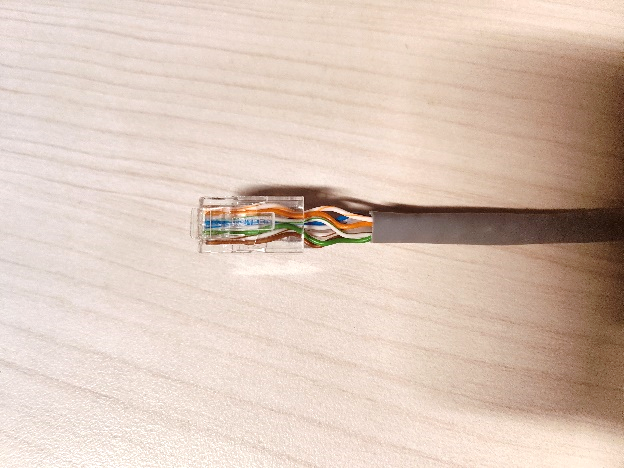
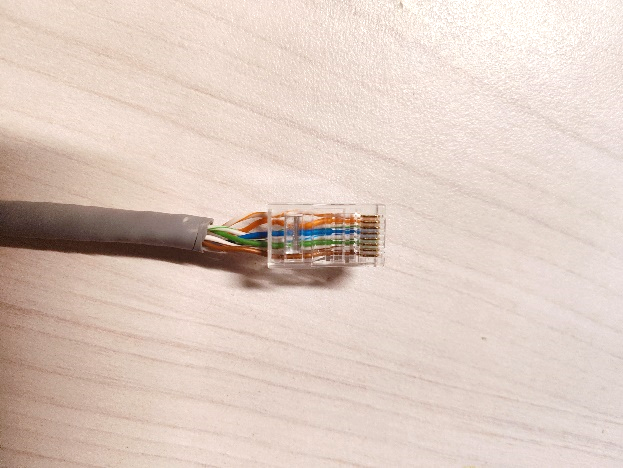
**【实验步骤】**

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】**

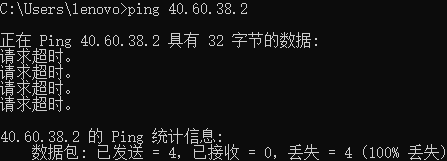
1. 操作系统：Windows 11
2. 网络环境：Wi-Fi连接

**【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】**

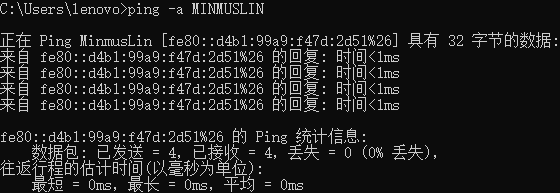
1. 使用ping 40.60.38.2命令测试网络是否通畅，结果显示网络不通畅。



1. 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。



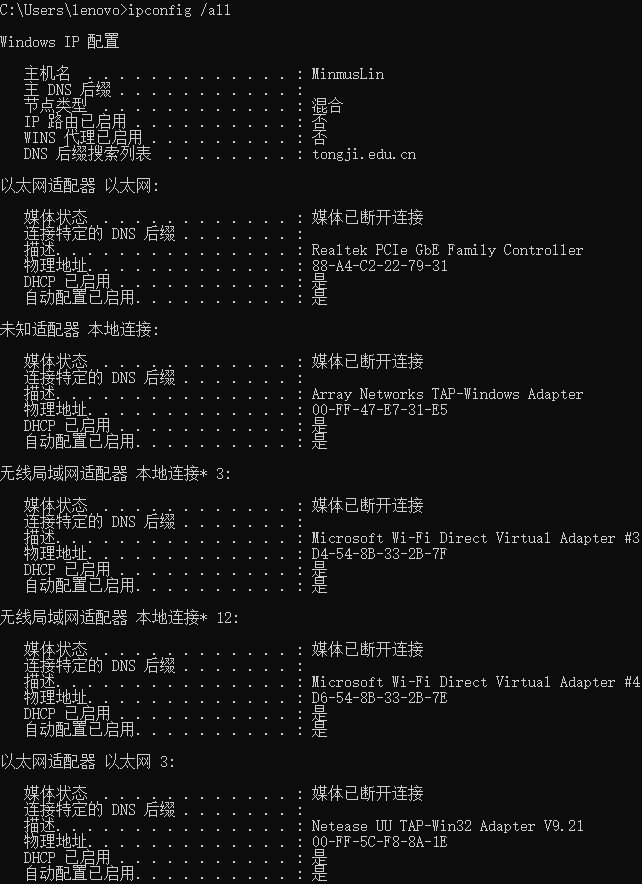
1. 使用ping -a MINMUSLIN命令获取计算机的IP地址。



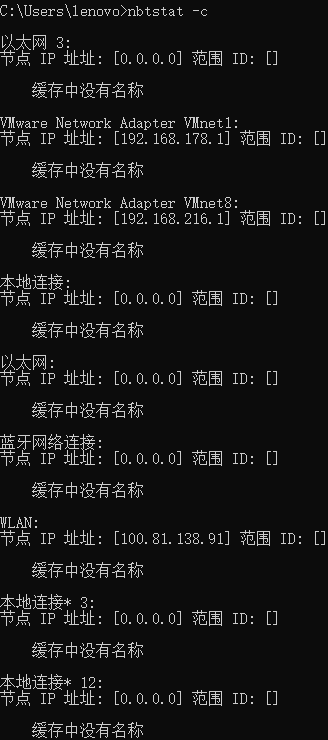
1. 使用ipconfig命令显示所有网络接口的IP地址、子网掩码和默认网关。



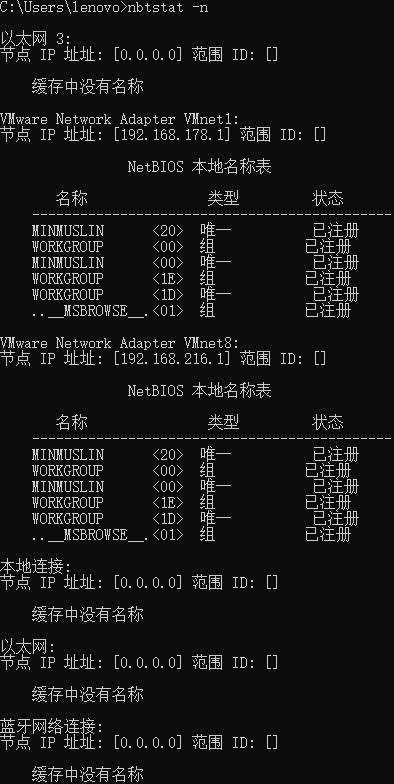
1. 使用ipconfig /all命令显示所有配置信息。



1. 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。



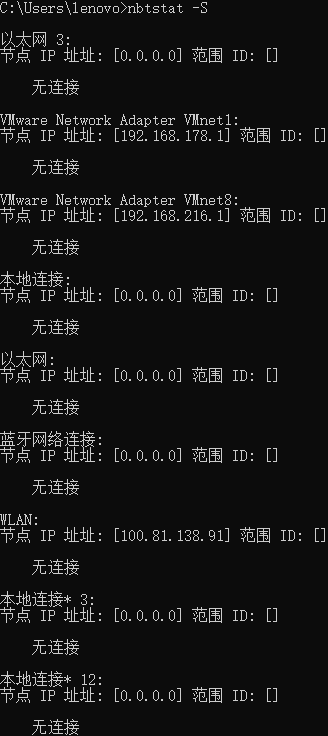
1. 使用nbtstat -n命令显示本地NetBIOS名称表。



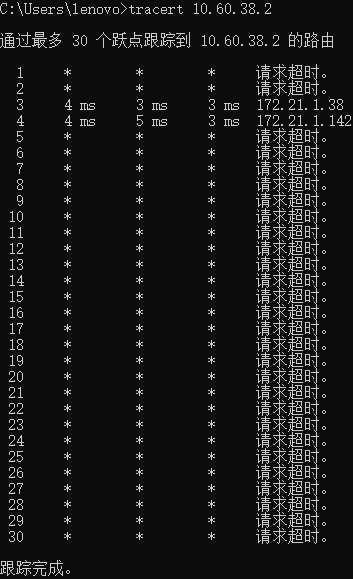
1. 使用nbtstat -r命令显示NetBIOS名称解析统计信息，包括成功的和失败的名称解析尝试。



1. 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。



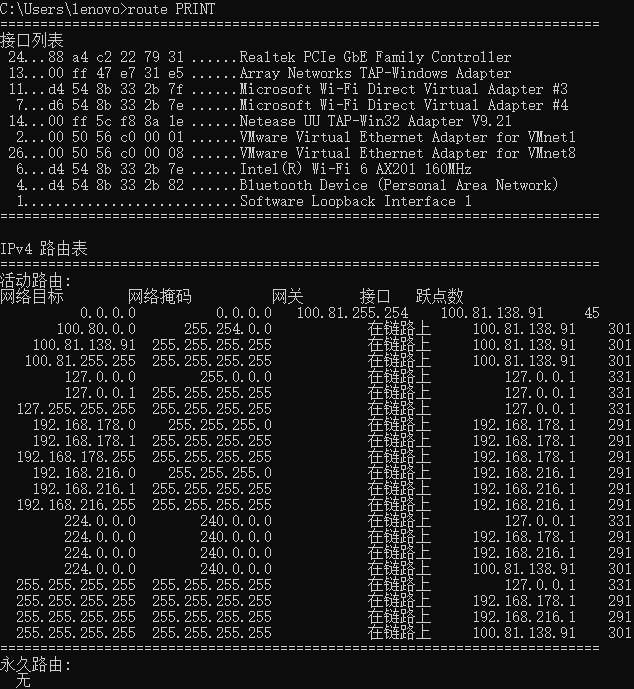
1. 使用tracert 10.60.38.2命令追踪数据包从执行该命令的设备到目的IP地址10.60.38.2的路由路径。

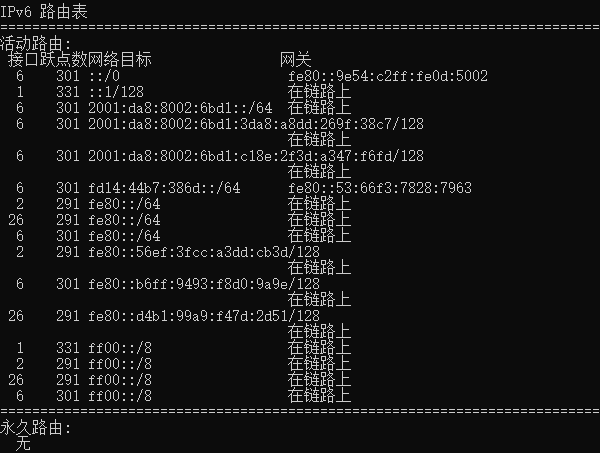


1. 使用net start命令显示已经启动的Windows服务。



1. 使用route PRINT命令显示当前的IP路由表。





1. 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。



1. 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。



1. 使用nslookup显示域名信息。



**【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】**

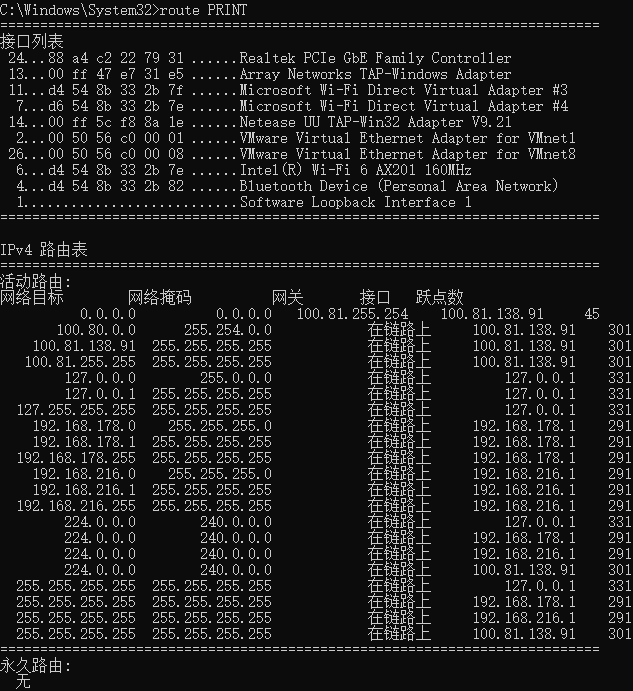
1. 打开命令提示符，注意要以管理员身份运行。
2. 使用route PRINT命令查看当前的路由表。
3. 记录显示的路由表项。
4. 使用route ADD命令添加新的路由。
5. 再次使用route PRINT命令，观察路由表的变化。
6. 使用route CHANGE命令尝试修改现有的路由。
7. 再次使用route PRINT命令，观察路由表的变化。
8. 使用route DELETE命令删除刚才添加的路由。
9. 再次使用route PRINT命令，观察路由表的变化。

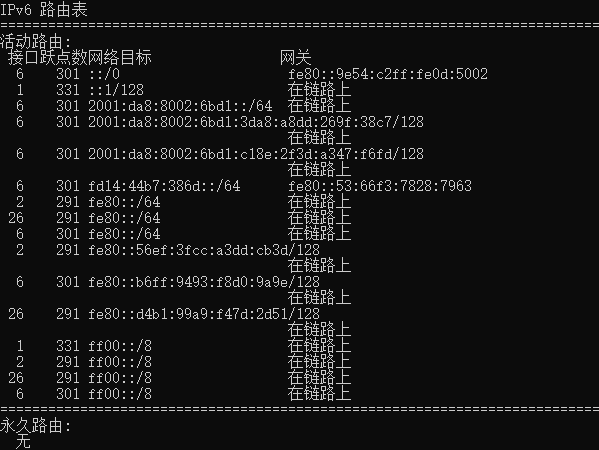
**【实验现象】**

1. 打开命令提示符，注意要以管理员身份运行。



1. 使用route PRINT命令查看当前的IPv4和IPv6路由表。

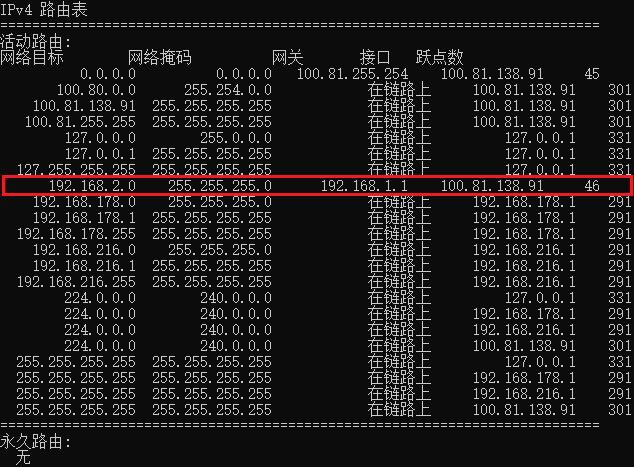




1. 记录显示的路由表项。
2. 使用route ADD 192.168.2.0 mask 255.255.255.0 192.168.1.1命令添加新的路由，使得所有前往192.168.2.0网络（子网掩码为255.255.255.0）的数据包都通过192.168.1.1网关转发。



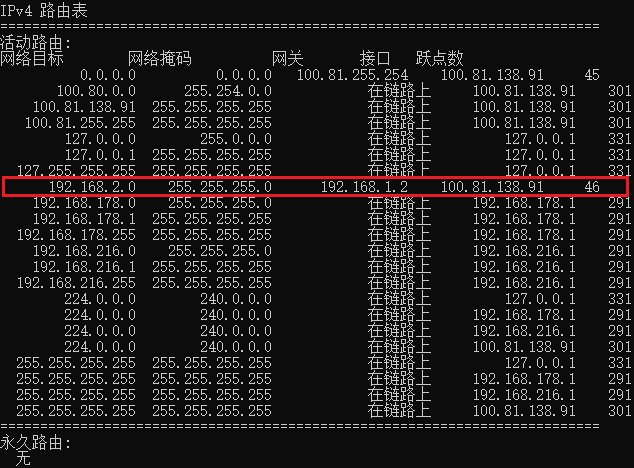
1. 再次使用route PRINT命令，观察路由表的变化，新的路由项出现在路由表中。



1. 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。



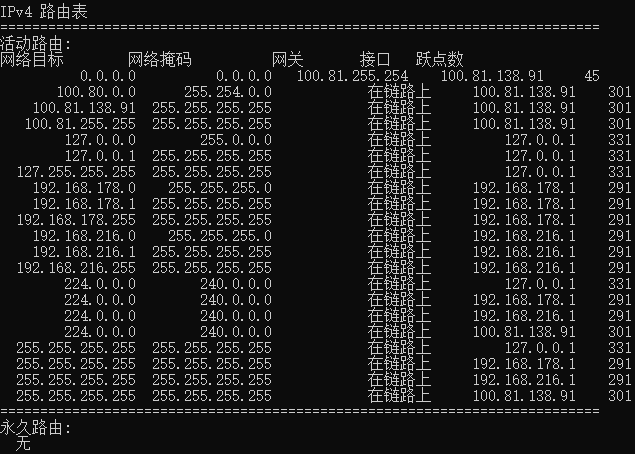
1. 再次使用route PRINT命令，观察路由表的变化，选定的路由项得到修改。



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



1. 再次使用route PRINT命令，观察相应的路由项从路由表中消失。



**【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。

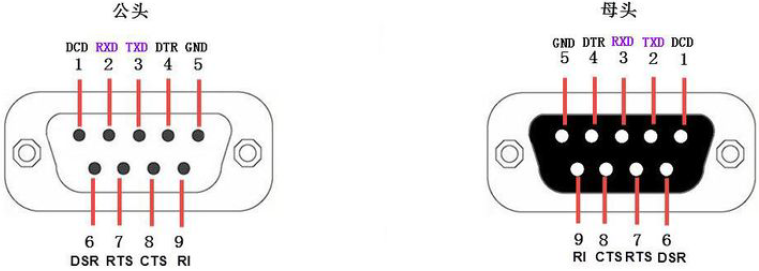
串口通信通过这两层的紧密协作，实现了设备间的高效、可靠通信。物理层确定了通信的物理和电子基础，而协议层则建立了共同的数据交流规则，使得不同设备之间能够顺畅地交换信息。这种分层的通信模型不仅适用于串口通信，也是现代通信技术中普遍采用的一个基本原则。

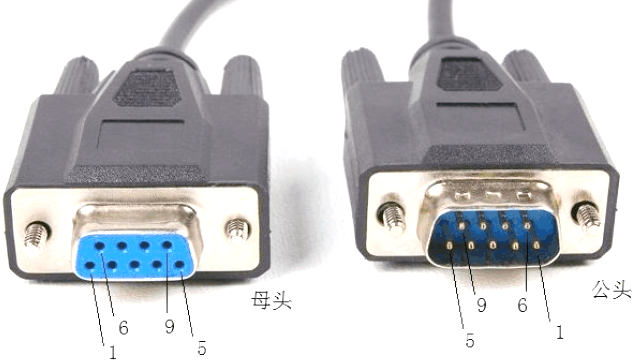
**二、串口通信标准**

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。

1. 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。
2. 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**

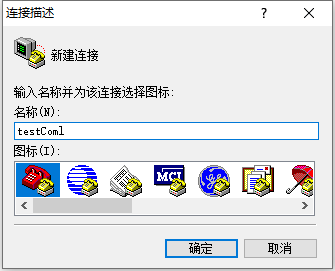
1. 信号电平：RS232接口采用负逻辑电平，其中-15V到-3V表示逻辑1，+15V到+3V表示逻辑0。电压值通常在7V左右。这种负逻辑电平的采用，对于确定数据传输中逻辑状态的识别具有重要意义​​。
2. 接口引脚：RS232接口标准定义了多个引脚用于不同的通信功能，例如DCD（载波检测）、RXD（接收数据）、TXD（发送数据）、DTR（数据终端准备好）、DSR（数据准备好）、RTS（请求发送）、CTS（清除发送）和RI（振铃提示）。这些引脚的设计使得串口通信能够支持复杂的控制信号交换，增强了通信的可靠性和灵活性​​。

**【实验设备】**

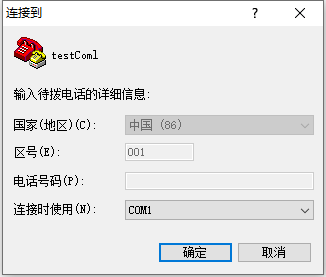
1. 装有Windows 10操作系统和超级终端应用程序的PC机两台
2. 串口线一条

**【实验步骤】**

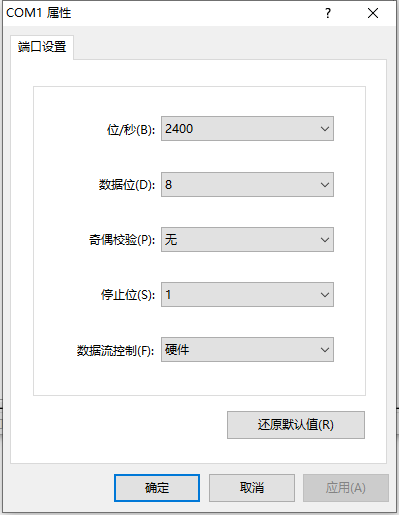
1. 使用串口线将两台装有Windows 10操作系统的PC机连接。
2. 在两台PC机上打开应用程序超级终端，并新建连接。



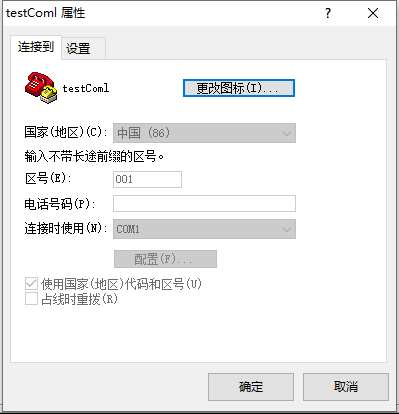
1. 在“连接到”窗口中，选择连接时使用“COM1”。

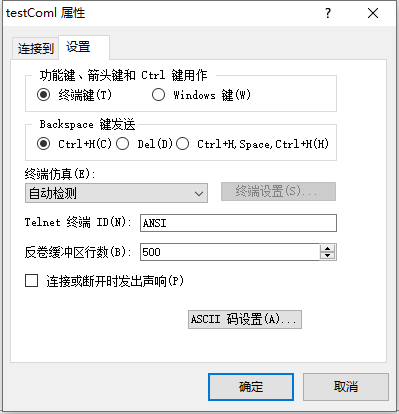


1. 在“COM1 属性”窗口中，进行如下设置。



1. 在“testComl 属性”窗口中，进行如下设置。



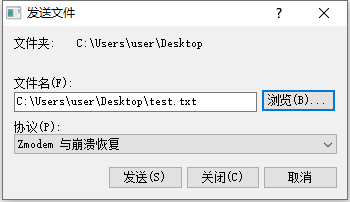


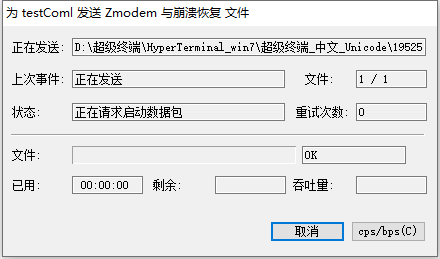
1. 点击“确定”，在超级终端“传送”选项卡中，分别选择“发送文件”、“接收文件”、“捕获文字”、“发送文本文件”，观察超级终端表现和文件传输特性。

**【实验现象】**

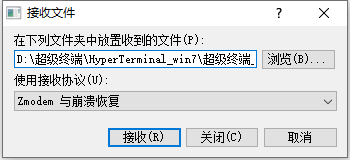
1. 当两台PC机的数据位设置为8位、奇偶校验设置一致（无论是奇校验、偶校验或无校验），以及停止位设置相同时， 发送文件、接收文件、捕获文字与发送文本文件均成功，即串口通信成功。这是因为数据位的一致性确保了双方能准确地解码对方发送的字符或命令；奇偶校验的一致性使得双方能同步地进行错误检测和纠正；而停止位的一致性则确保了双方能准确地识别字符或命令的结束，从而实现有效的数据传输。

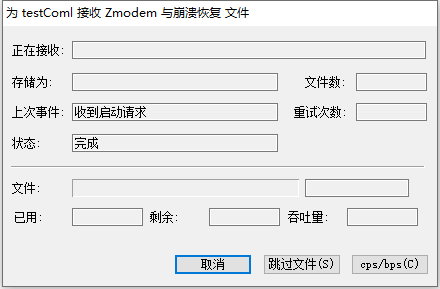
* “发送文件”实验现象



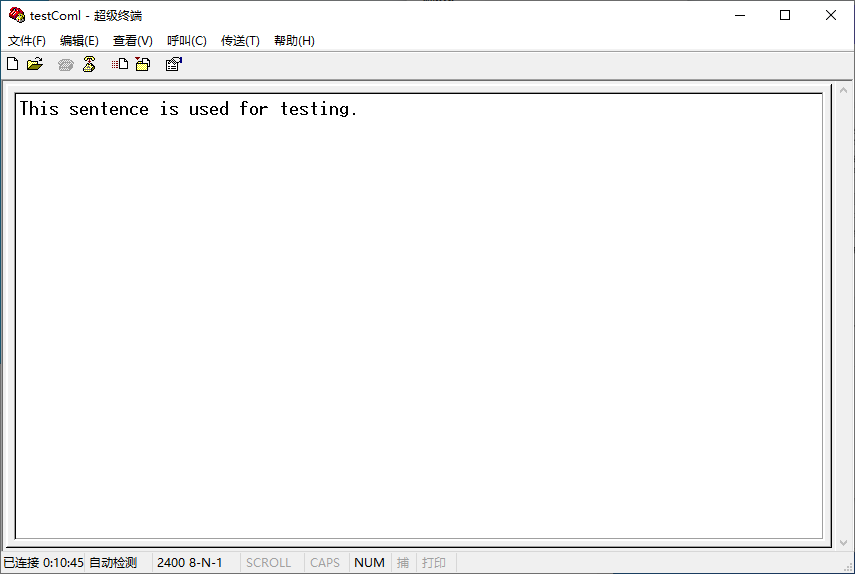


* “接受文件”实验现象





* “捕获文字”实验现象



* “发送文本文件”实验现象



1. 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**

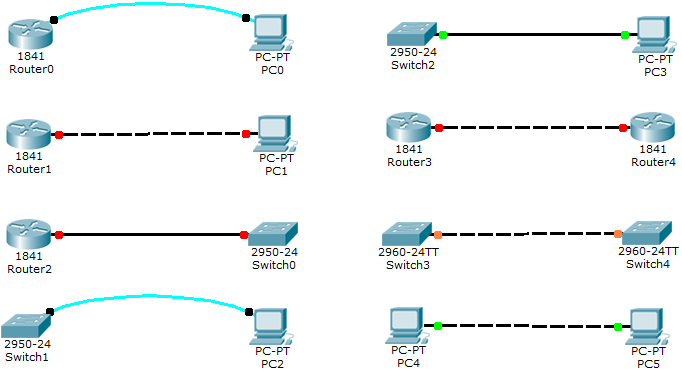
Setup模式：初次配置路由器时的简化模式。尽管它提供了一种配置路由器的方式，但通常推荐使用命令行界面（CLI）进行更详细的配置。

**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

**【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。

1. 学习IOS的启动过程和配置模式
2. 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。

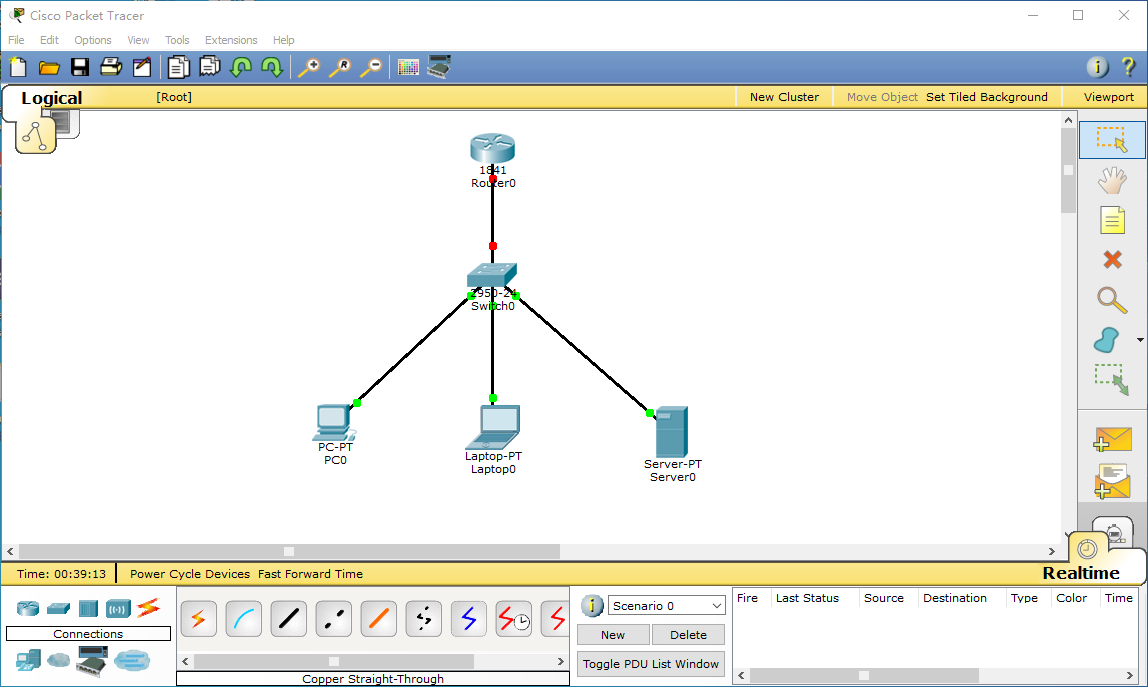
1. 接口操作

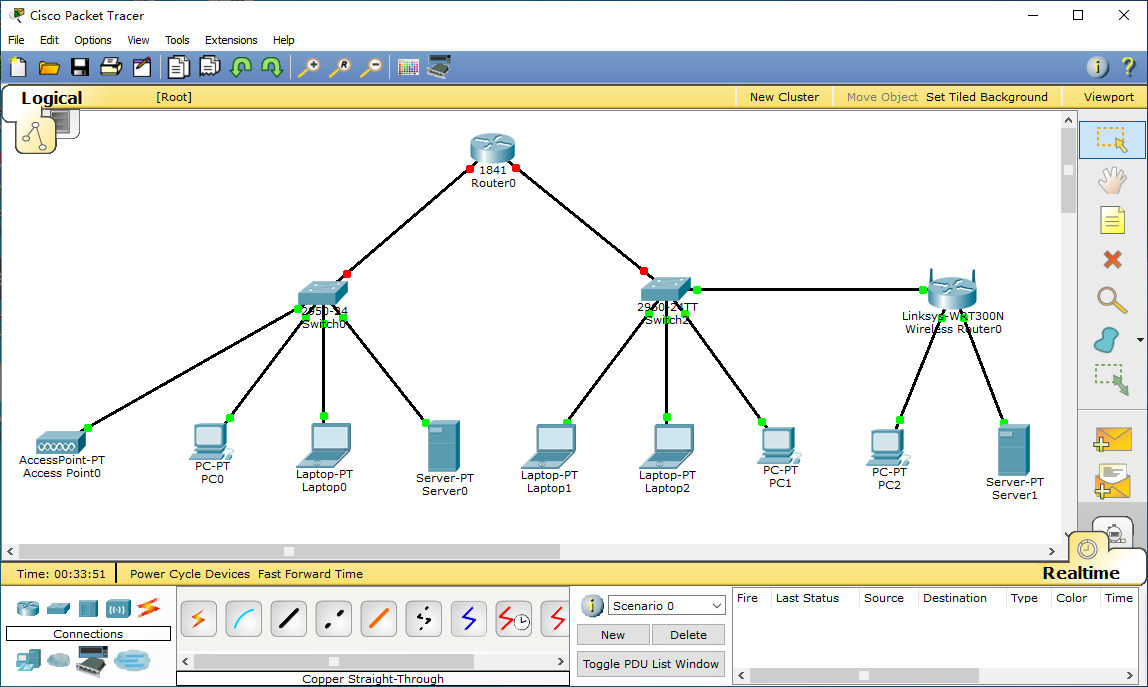
* 使用no shut命令启用接口。
* 使用end命令从任何配置模式返回到特权模式。

1. 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。

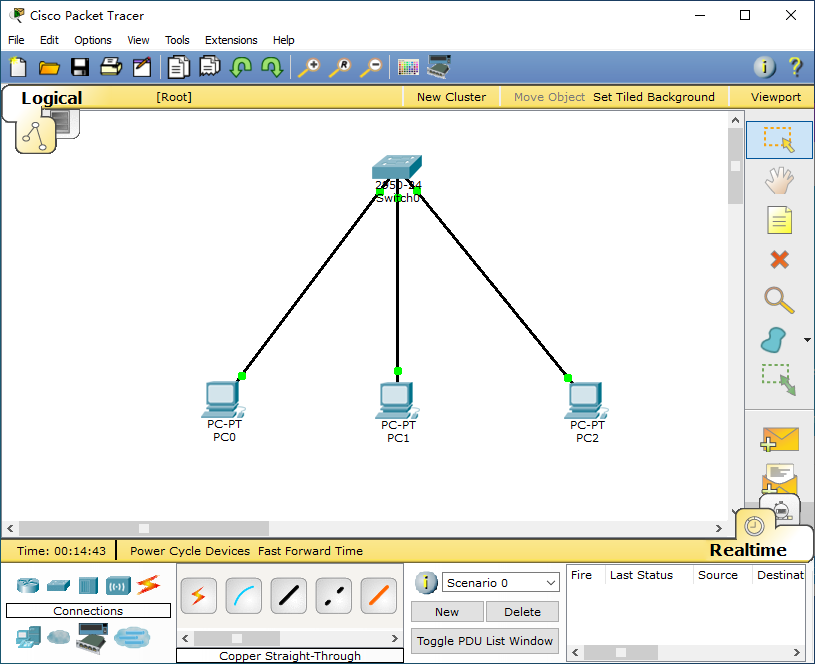
VLAN通过软件配置，而非物理连接，来划分网络。这允许网络管理员根据需要（例如部门、项目组或应用类型）灵活地组织设备，而不受物理位置的限制。在传统的局域网中，广播消息会发送给同一网络段内的所有设备，无论是否需要。VLAN技术可以将大的广播域划分成较小的片段，每个VLAN内部处理自己的广播流量，减少了不必要的广播传输，提高了网络的效率。VLAN之间的通信默认是隔离的。这意味着，不同VLAN的设备不会看到对方的数据，除非通过特定的路由配置允许这种通信。这种隔离增强了网络安全性，可以有效防止潜在的数据泄露和未授权访问。

**【实验设备】**

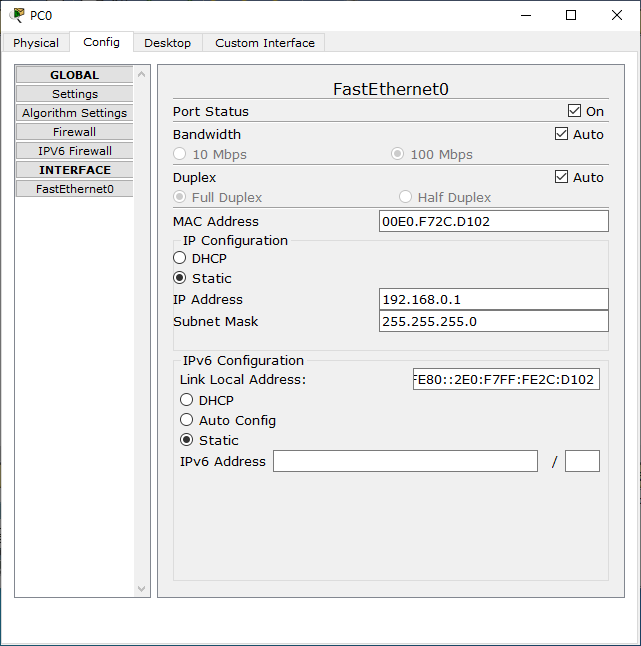
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer

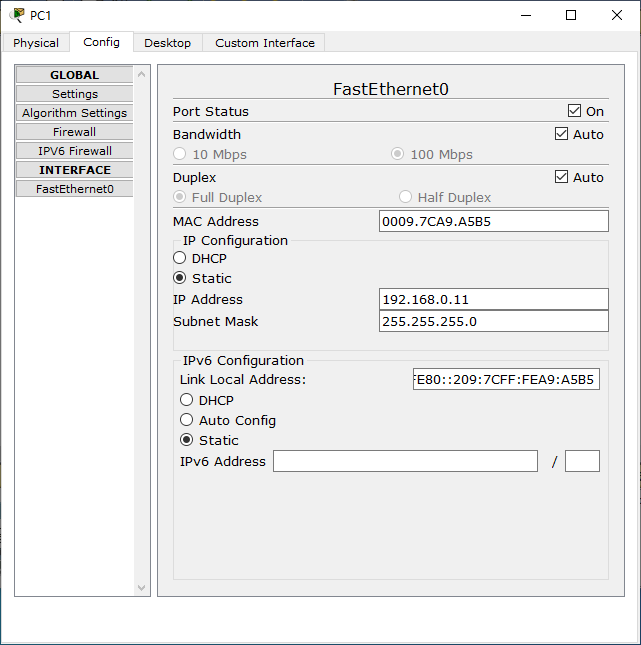
**【实验步骤】**

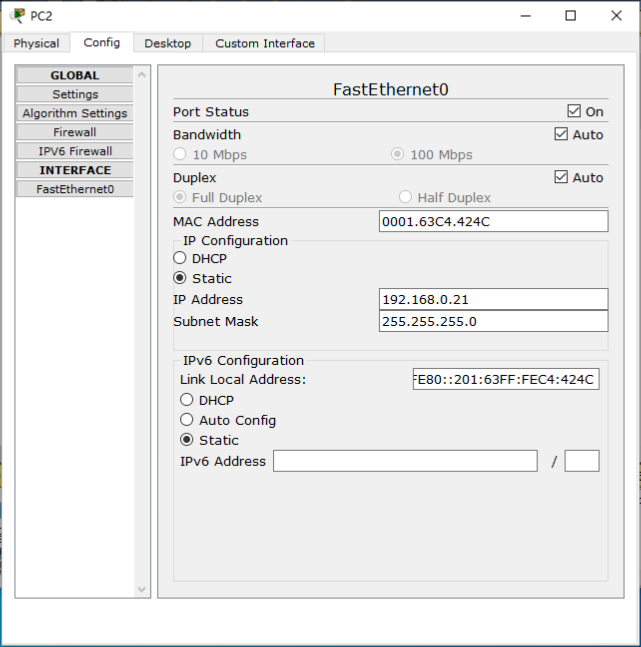
1. 启动Cisco Packet Tracer来模拟网络环境。
2. 连接设备。



1. 通过Config图形化界面为三台PC机配置IP及掩码。







1. 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

1. 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**

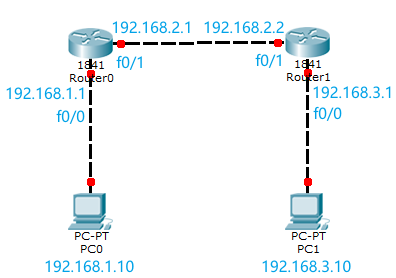
1. 设置IP地址和子网掩码：ip address [IP地址] [子网掩码]
2. 启用端口：No shutdown
3. 指定目标网段、子网掩码和下一跳地址：ip route [目标网段IP地址] [目标子网掩码] [下一跳地址]
4. 指定目标网段、子网掩码和送出接口：ip route [目标网段IP地址] [目标子网掩码] [接口]
5. 查看路由配置情况：show ip route

**【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

**【实验步骤】**

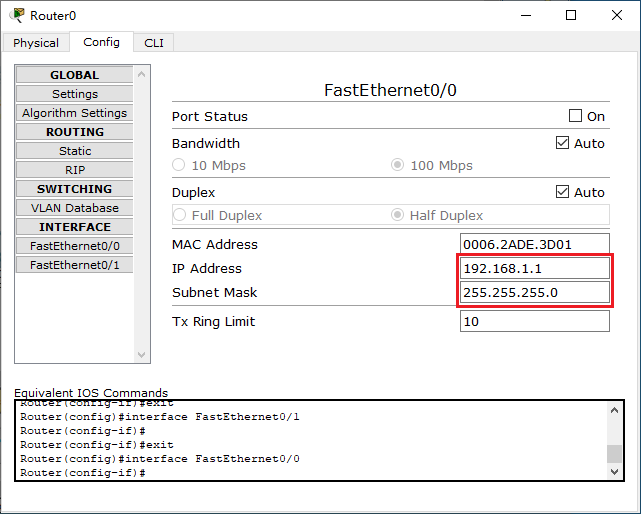
1. 启动Cisco Packet Tracer来模拟网络环境。
2. 按照如下拓扑图连接设备，子网掩码是255.255.255.0，PC0的网关是192.168.1.1，PC1的网关是192.168.3.1。

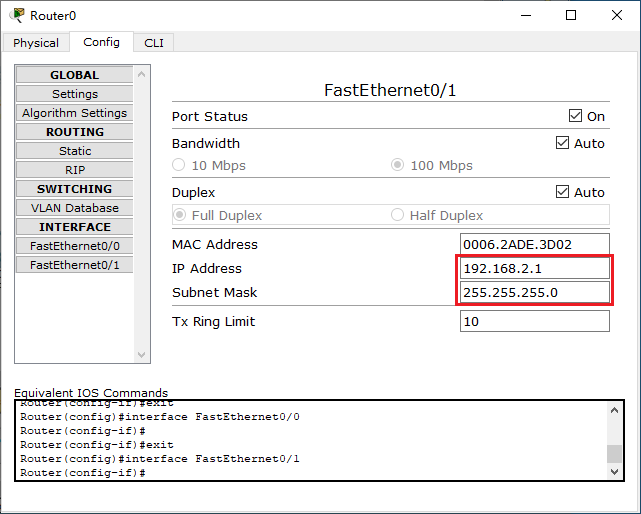


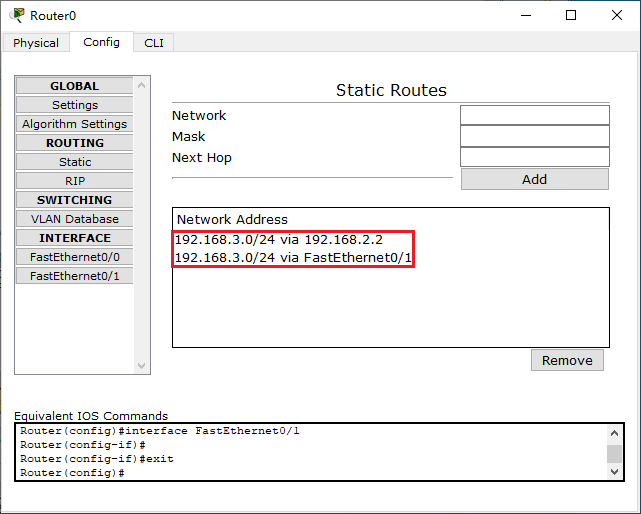
1. 配置路由器Router0。

* 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 |



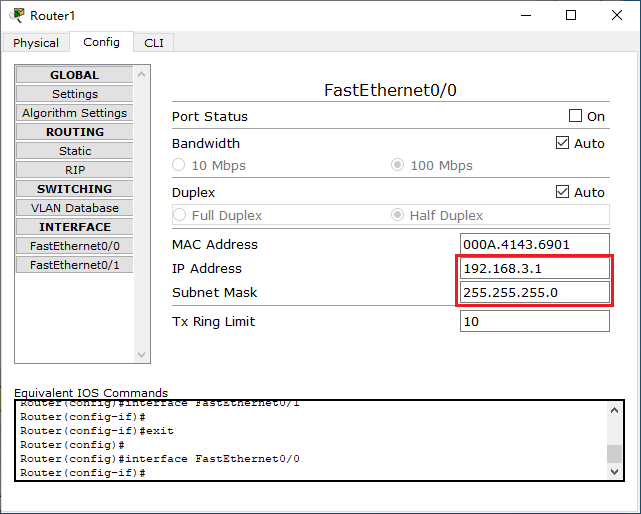


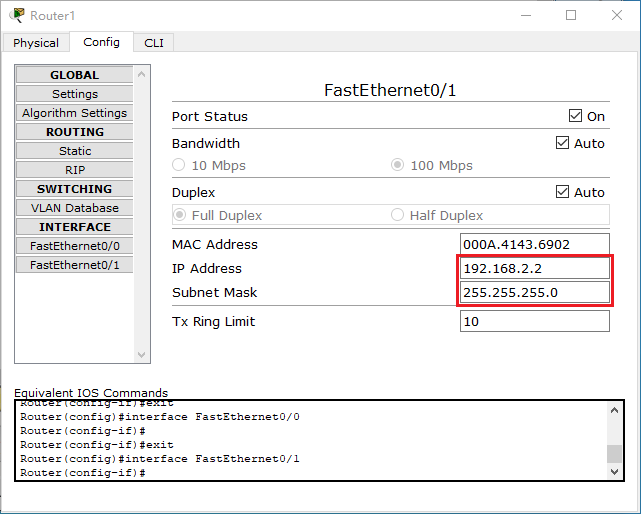


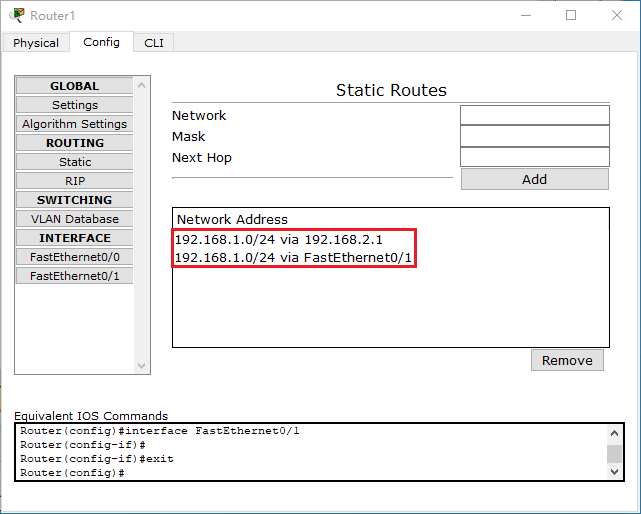
1. 配置路由器Router1。

* 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：

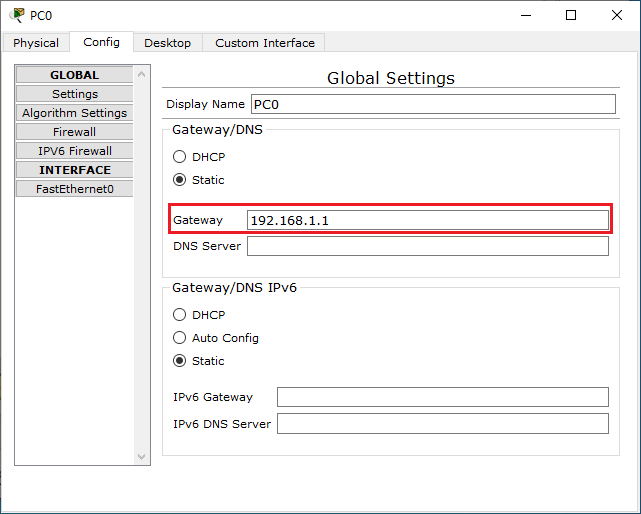
|  |
| --- |
| interface f0/0  ip address 192.168.3.1 255.255.255.0  no shutdown  interface f0/1  ip address 192.168.2.2 255.255.255.0  no shutdown  ip route 192.168.1.0 255.255.255.0 192.168.2.1  ip route 192.168.1.0 255.255.255.0 f0/1 |

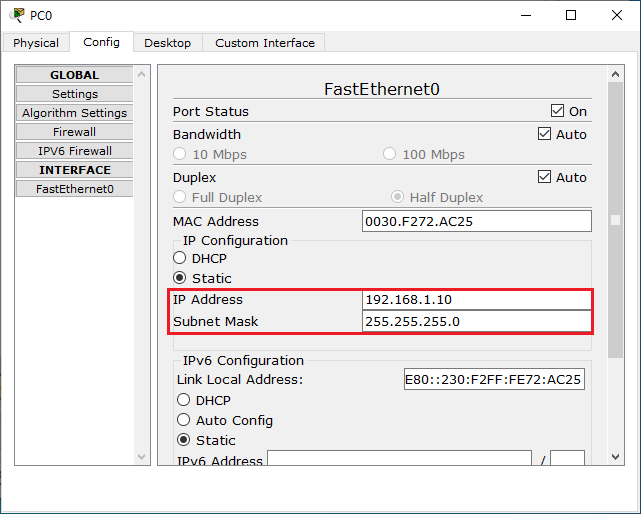




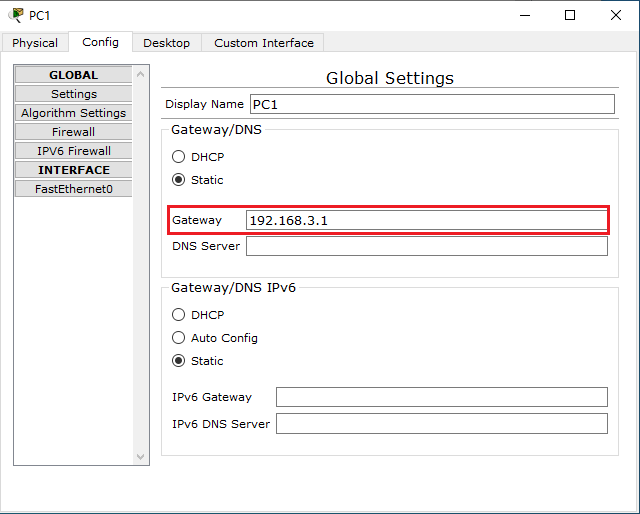


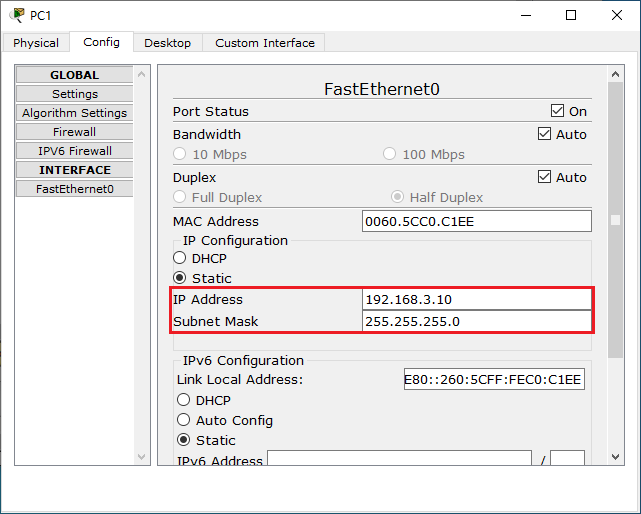
1. 配置PC0的网关、IP地址与子网掩码。





1. 配置PC1的网关、IP地址与子网掩码。





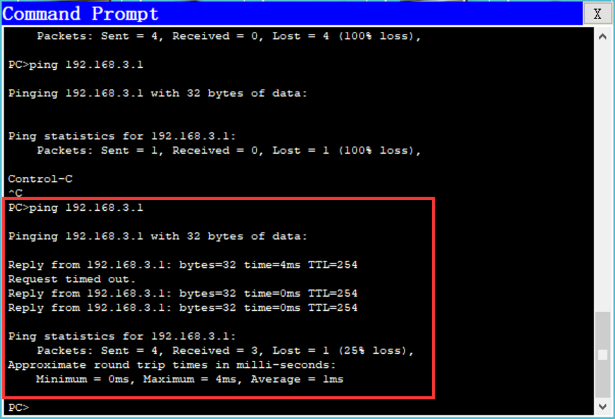
1. 测试PC0与PC1之间相互通信。

* 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。

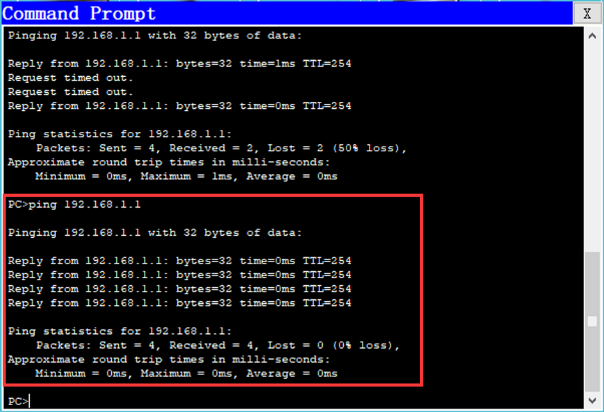
1. 在Route0与Route1的CLI中分别输入show ip route命令查看其对应的静态路由表。

**【实验现象】**

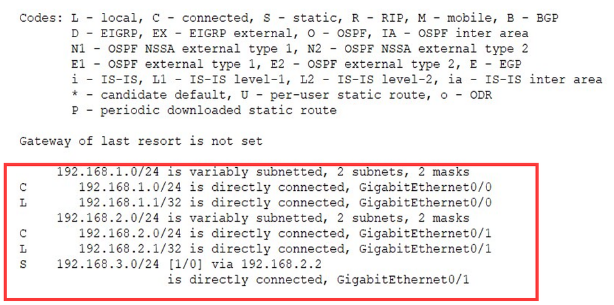
1. 在PC0的Prompt Terminal中输入ping 192.168.3.1命令接收PC1的消息。



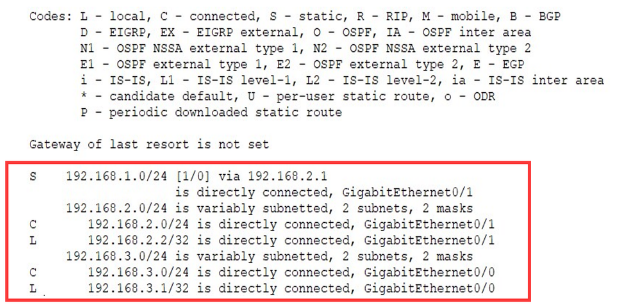
1. 在PC1的Prompt Terminal中输入ping 192.168.1.1命令接收PC0的消息。



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



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



**【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

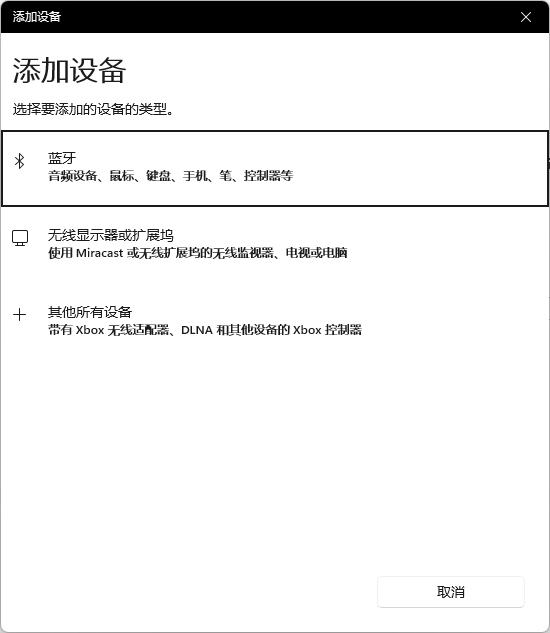
**【实验步骤】**

1. 打开电脑和手机的蓝牙功能。

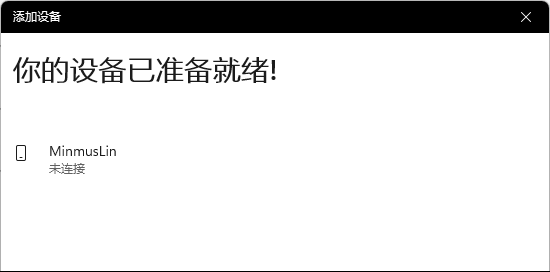


1. 在电脑上打开“设置”>“蓝牙和其他设备”>“设备”>“添加设备”>“蓝牙”，连接手机设备；也可以在手机上连接电脑。



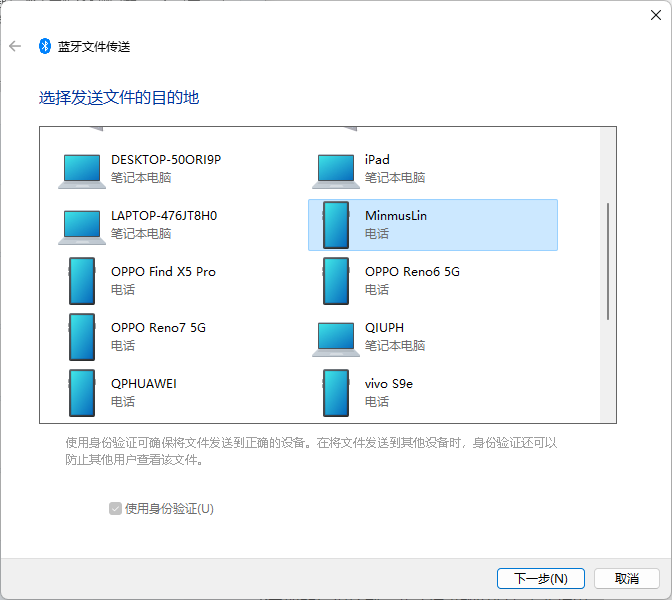






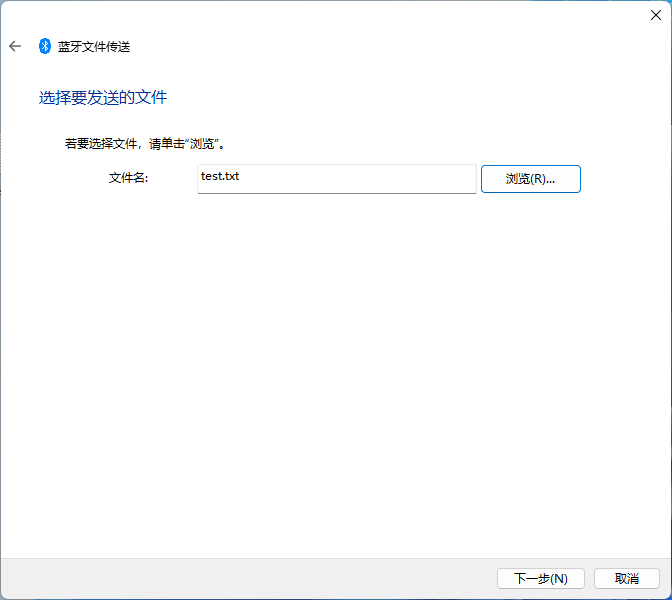
1. 在电脑上打开“设置”>“蓝牙和其他设备”>“设备”>“通过蓝牙发送或接收文件”>“发送文件”，选择手机设备，选择文件，将其发给手机。

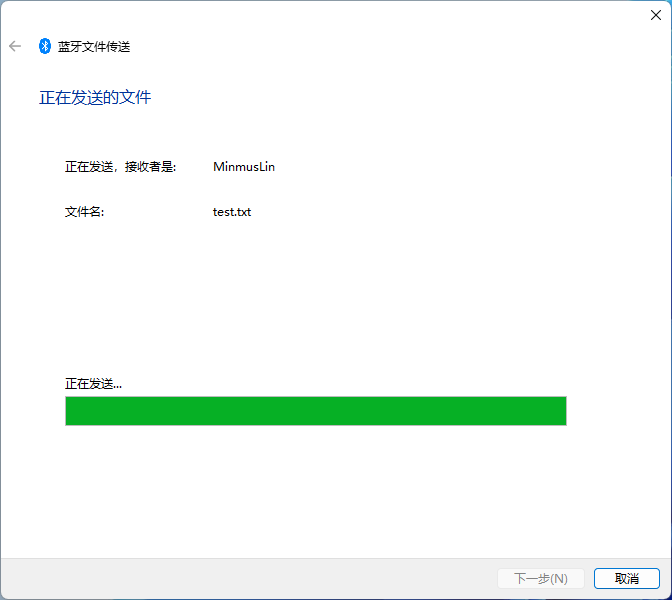




**【实验现象】**

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：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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// |

**【实验目的】**

**【实验原理】**

**【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：

**【实验步骤】**

**【实验现象】**

**【分析讨论】**