

# 第四讲

计算机网络原理实验

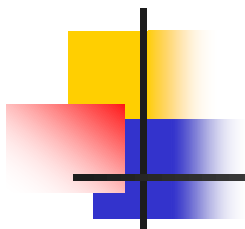
---

李勇军

# 本节实验内容

- 实验内容1： ICMP协议分析与验证
  - 实验七（P280）
  - 实验第8章： P242-P255
- 实验内容2： FTP客户端编程实验
  - 实验八： P283





- 实验内容1： ICMP协议分析与验证
  - 实验七（P280）
  - 实验第8章（P242–P255）



# 实验内容1: ICMP协议分析与验证

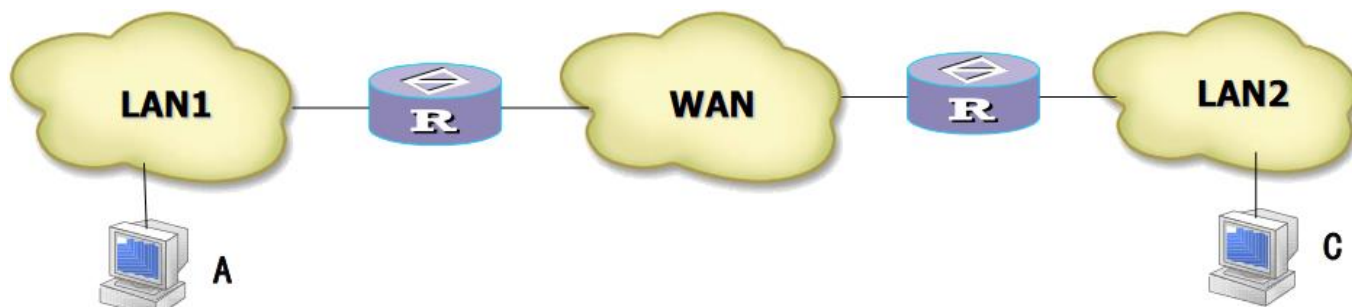
---

- 1、实验要求
  - 两个同学一组；
  - 提交文档：实验报告
- 2、实验环境
  - WIN XP
  - VC++, VISUAL STUDIO, PYTHON等

# 实验内容1: ICMP协议分析与验证

## ■ 3、实验目的

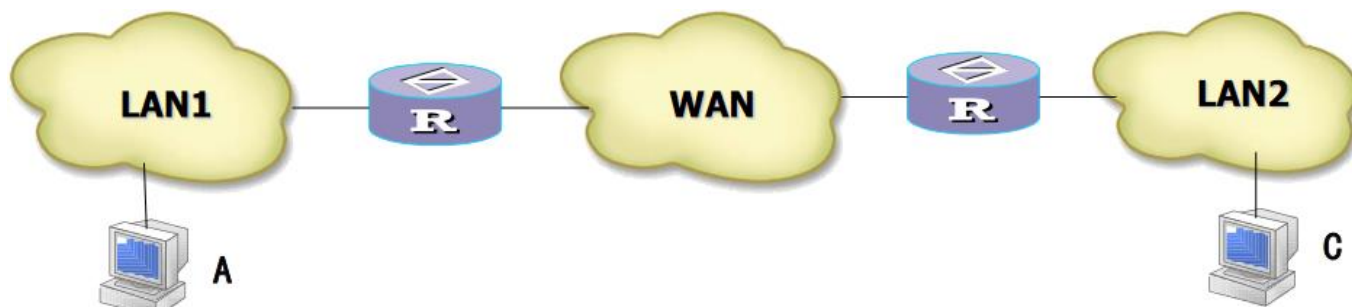
- (1) 在分析ping命令实现实例代码基础上, 理解该命令的实现原理; 通过构造并发送ICMP ECHO 请求报文, 在目标计算机上对ICMP ECHO 请求报文实施接收和解析, 深刻理解ICMP协议的工作原理。



# 实验内容1: ICMP协议分析与验证

## ■ 3、实验目的

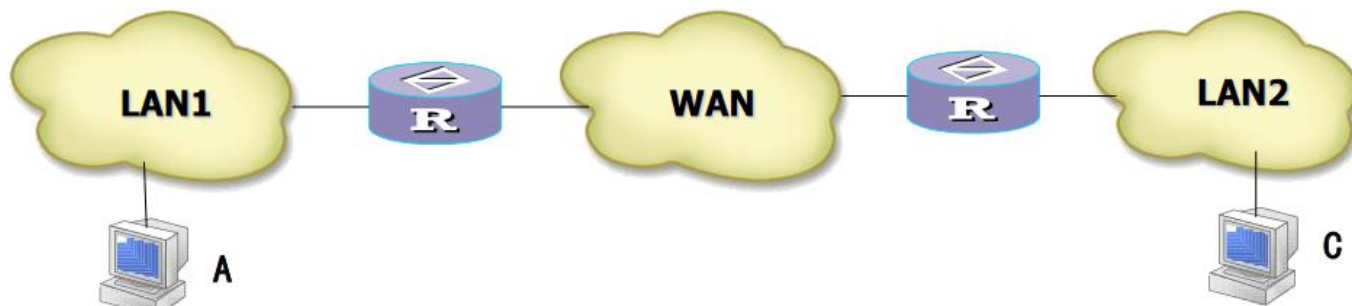
- (1) 在分析ping命令实现实例代码基础上, 理解该命令的实现原理; 通过构造并发送ICMP ECHO 请求报文, 在目标计算机上对ICMP ECHO 请求报文实施接收和解析, 深刻理解ICMP协议的工作原理。



# 实验内容1: ICMP协议分析与验证

## ■ 4、实验内容

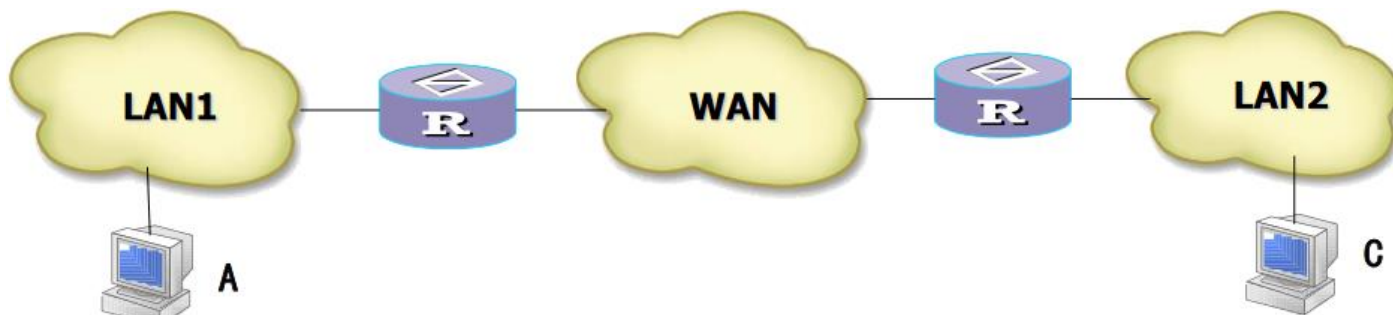
- (1) 分析ping命令实现的实例代码。
- (2) 在发送端构造ICMP ECHO请求报文并发送给接收端。
- (3) 在接收端接收ICMP ECHO请求报文并解析与显示首部各个字段的值。



# 实验内容1: ICMP协议分析与验证

## ■ 4、实验步骤

- (1) 分析ping命令实现的实例代码，并总结分析其实现原理和工作流程。
- (2) 在发送端构造ICMP ECHO请求报文并发送给接收端。
- (3) 在接收端接收ICMP ECHO请求报文，并解析其ICMP报文首部各个字段，在屏幕上显示解析结果。





# 实验内容1: ICMP协议分析与验证

## ■ 5、思考题

- 设计一个tracert命令（分析设计原理），根据IP数据报通信的特点，分析利用该命令获取的发送端到目的端的路径信息是否正确。若利用该命令可以获取发送端网络的网关IP地址（可通过抓包获取发送端网络网关的MAC地址），则分析利用该命令是否可以获取目的端所在网络的网关的IP和MAC地址，并解释原因。

```
C:\Users\Administrator>tracert /?
```

```
用法: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
        [-R] [-S srcaddr] [-4] [-6] target_name
```

选项:

-d	不将地址解析成主机名。
-h maximum_hops	搜索目标的最大跃点数。
-j host-list	与主机列表一起的松散源路由<仅适用于 IPv4>。
-w timeout	等待每个回复的超时时间<以毫秒为单位>。
-R	跟踪往返行程路径<仅适用于 IPv6>。
-S srcaddr	要使用的源地址<仅适用于 IPv6>。
-4	强制使用 IPv4。
-6	强制使用 IPv6。

```
C:\Users\Administrator>tracert www.nwpu.edu.cn
```

通过最多 30 个跃点跟踪  
到 www.nwpu.edu.cn [222.24.192.45] 的路由:

	<1 毫秒	<1 毫秒	<1 毫秒	
1				192.168.1.1
2	5 ms	1 ms	1 ms	10.164.0.1
3	2 ms	2 ms	2 ms	172.20.128.5
4	2 ms	2 ms	2 ms	222.24.254.1
5	*	*	*	请求超时。
6	3 ms	3 ms	2 ms	222.24.254.73
7	2 ms	1 ms	1 ms	222.24.254.66
8	5 ms	3 ms	3 ms	222.24.254.69
9	2 ms	4 ms	1 ms	192.168.141.3
10	2 ms	2 ms	1 ms	jiaowu.nwpu.edu.cn [222.24.192.45]

跟踪完成。

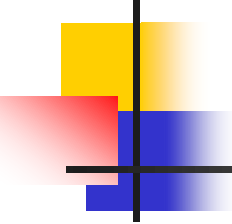


# 实验内容1: ICMP协议分析与验证

---

## ■ 6、实验助教检查点

- (1) 利用Wireshark抓包工具，捕获发送端发送的第一个ICMP ECHO请求报文报文，分析IP报文首部，ICMP报文首部各个字段的含义。
- (2) 利用Wireshark抓包工具，捕获接收端接收的第一个ICMP ECHO请求报文报文，分析IP报文首部，ICMP报文首部各个字段的含义，检查第一个ICMP ECHO请求报文是否与发送的ICMP ECHO请求报文完全一致，IP报文首部是否有变化。

- 
- 
- 实验内容2：FTP客户端编程实验
    - 教材-实验八：P283



# 实验内容2: FTP客户端多进程编程

---

## ■ 1、实验目的

- 通过设计和实现一个**FTP**客户端系统，深刻理解**FTP**协议工作原理，重点掌握**FTP**协议设计与实现中控制连接和数据连接建立过程，两个连接通信模式特点。

## ■ 2、实验内容

- （1）**FTP**客户端系统的设计，理解**FTP**协议中数据连接建立两种方式区别：被动模式和主动模式；
- （2）**FTP**客户端系统的实现，涉及控制连接、数据连接建立；通过在控制连接传输命令，数据连接传输数据，利用多进程编程，实现一个**FTP**客户端系统。



# 实验内容2: FTP客户端多进程编程

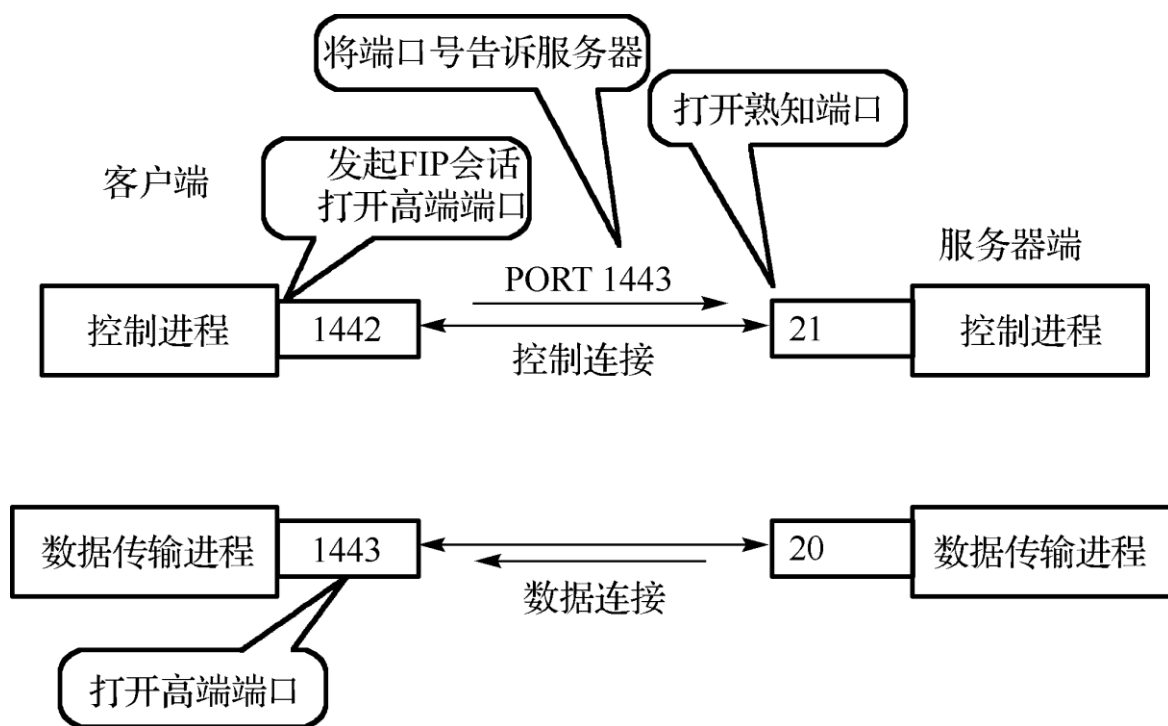
---

## ■ 3、实验要求

- (1) 每名学生独立完成实验内容和实验报告。
  - (2) 理解**FTP**协议中数据连接建立两种方式（被动模式和主动模式）的区别。
  - (3) 掌握控制连接和数据连接的建立方法和通信特点。
  - (4) 掌握多进程编程方法。
- 
- 提交文档：实验报告

# 实验内容2: FTP客户端多进程编程

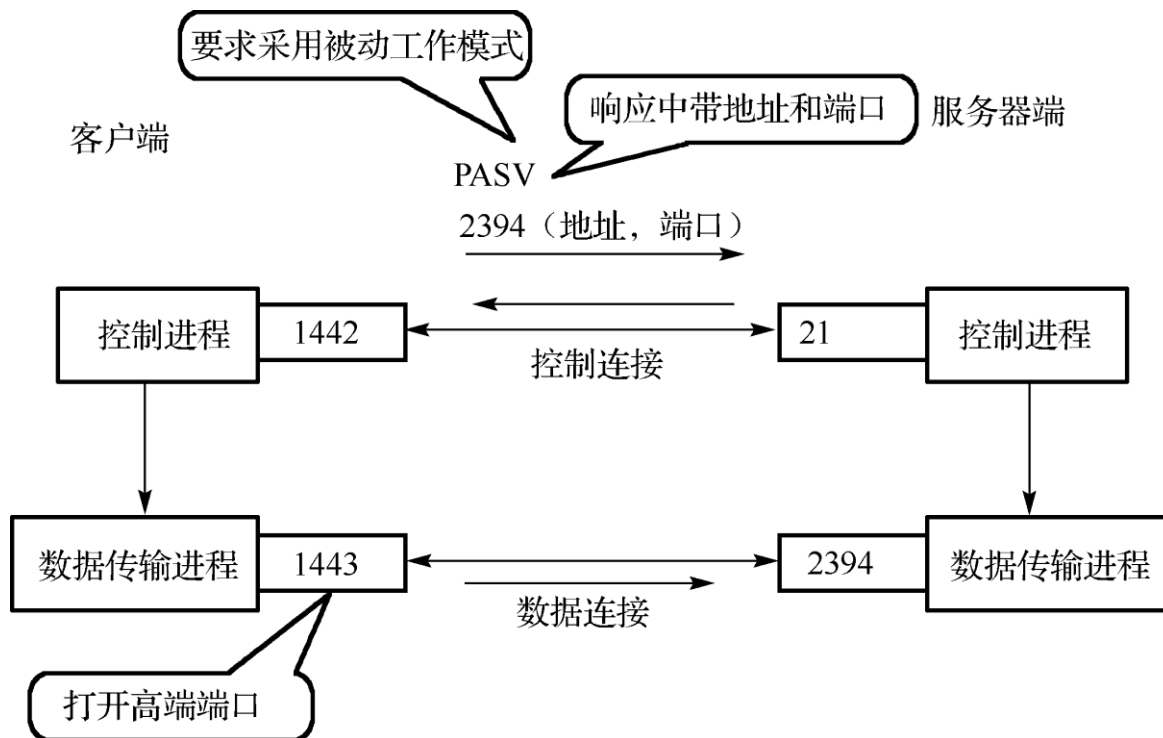
## 4、FTP数据连接建立方式（主动模式、被动模式）



FTP协议主动工作模式流程

# 实验内容2: FTP客户端多进程编程

## 4、FTP数据连接建立方式（主动模式、**被动模式**）



FTP协议被动工作模式流程



# 实验内容2: FTP客户端多进程编程

---

## ■ 5、实验步骤（FTP协议的设计和工作流程）

- （1）首先FTP客户端和服务器之间建立控制连接。
- （2）FTP客户端通过控制连接向服务器发送账号信息（用户名+密码），进行身份认证。
- （3）FTP客户端通过控制连接向服务器发送passiv命令，说明采用被动模式建立数据连接。
- （4）FTP客户端与服务器之间通过被动模式建立数据连接。
- （5）FTP客户端向服务器发送dir命令，服务器对该命令进行处理，并向客户端发送处理结果；
- （6）FTP客户端接收服务器发送来的处理结果（获得服务器当前目录下的列表信息），并在屏幕上显示。
- （7）释放数据连接。
- （8）FTP客户端向服务器发送quit命令，并释放控制连接。
- （9）通信结束。





# 实验内容2: FTP客户端多进程编程

---

## ■ 6、助教检查点

- （1）利用抓包工具获取passiv模式设置过程，以及数据连接建立过程，分析被动模式与主动模式在建立数据连接过程中有何不同？
- （2）利用抓包工具分析本次执行dir命令的通信流程，在数据连接上FTP服务器发送给FTP客户端数据字节个数是多少？



# 实验报告

---

- 按照格式要求，撰写2次实验的报告，并发送至指定的邮箱。
  - 2个报告放在一个文件中，按照统一要求命名
  - 实验报告雷同者均为0分
  - 截至日期为12月9日