TCP/IP 分析

Andrew Huang< bluedrum@163.com>

内容:

协议概论

协议(protocol)就是通讯双方都要遵守的一系列规则,是一个抽象规定,人类的语言交流就是一个典型的协议系统,在这个例子里,语法就是协议.它本身就是抽象的.当然你写成书面表达,就叫协议文本.协议的发送是由人类发声器官,如声带来产生,协议的接收是由人类听觉器官---耳朵来接用,并由大脑来理解.协议的传输介质是两人之间的空气.协议的编码是由发声器官加载在声波上传送的.

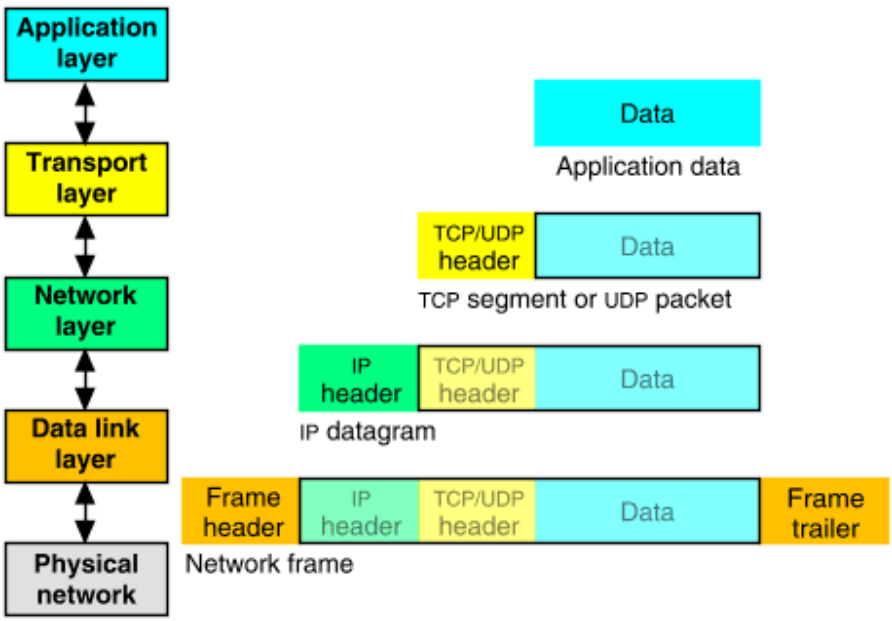
同样一种协议,可以由不同裁体来传输,一句话除了用声音来传输外,人类还发明的书写方式来传输.到后来,技术进步,人类可以通过旗语,信号灯,电报以及现代互联网的 E-mail.来传输.这样不同实现方法就是不同协议.作用基本上只有一个,就是传达信息.

同样,在我们这节讨论的网络系统里,也是一种协议系统.以常见的局域网系统为例,协议的发送和接收设备是网卡,连接网卡是网线.在局域网上传输都是以太网传输协议.

我们也知道网络协议是分层的.象 TCP/IP ,就分为物理层,数据链路层和网络层等结构,在编程上,每一层协议是由单独的模块来实现的.第一层协议模块,只与上一层和下一层协议打交道.这个结构非常象一个栈(stack)结构,即一个协议架在另一个协议之上.这有一个术语来专门描述,协议栈(Protocol Stack),只要任何具有多层协议框架并有序叠在一起都可以用协议栈来称呼.如 TCP/IP 协议栈.蓝牙协议栈,GSM 协议栈等.

TCP/IP 协议栈

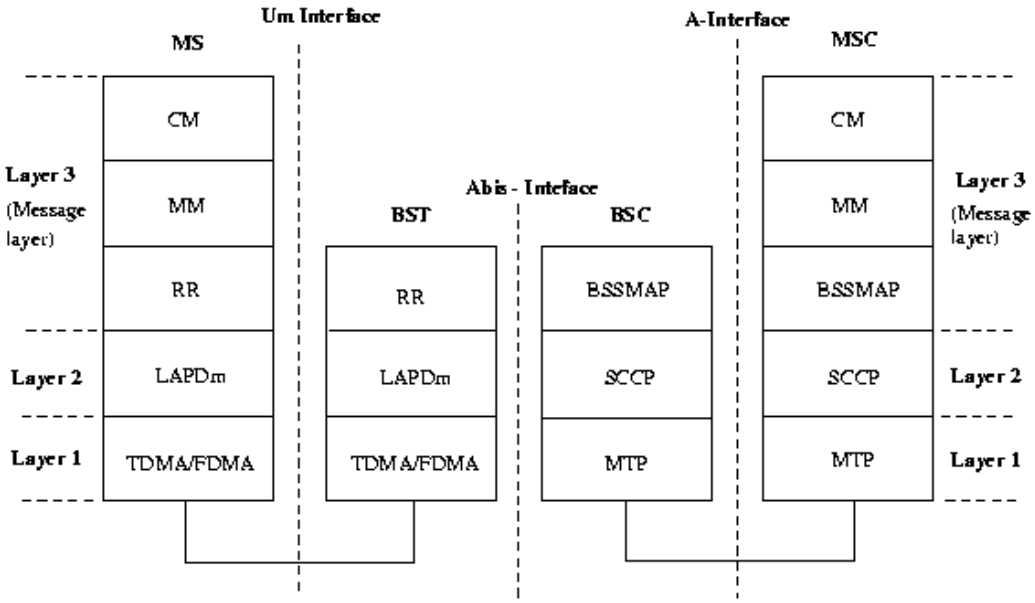
下图是典型的 TCP/IP 五层协议栈,其中网络层是 IP 协议.



GSM 协议栈

下图是典型 GSM 协议栈结构,layer1(物理层)采用 TDMA/FDMA 协议,layer2(数据链路层)采用 LAPD,layer3(消息层)用来处理 GSM 信号协议.分为三个独立子协议.

- Radio Resource management (RR)
- Mobility Management (MM) and
- Connection Management (CM).



FTP

下面,以大家比较熟悉**FTP**为例来解释**TCP/IP**协议栈的运作.

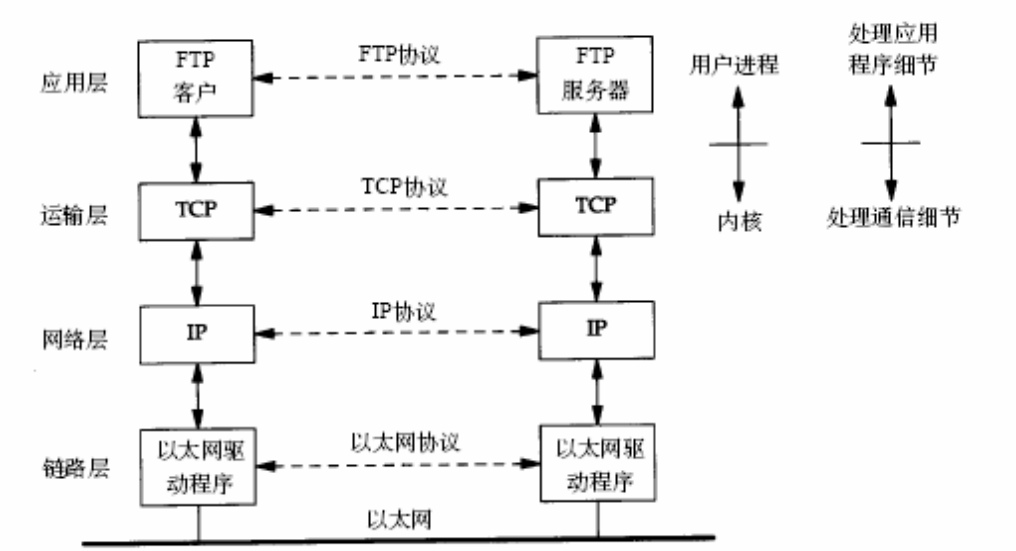
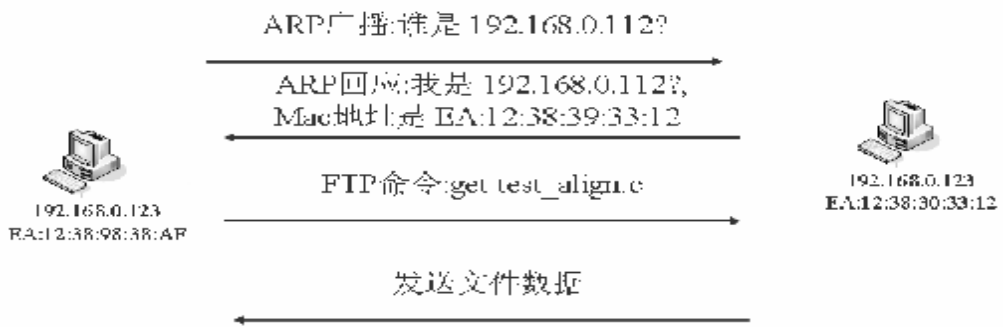
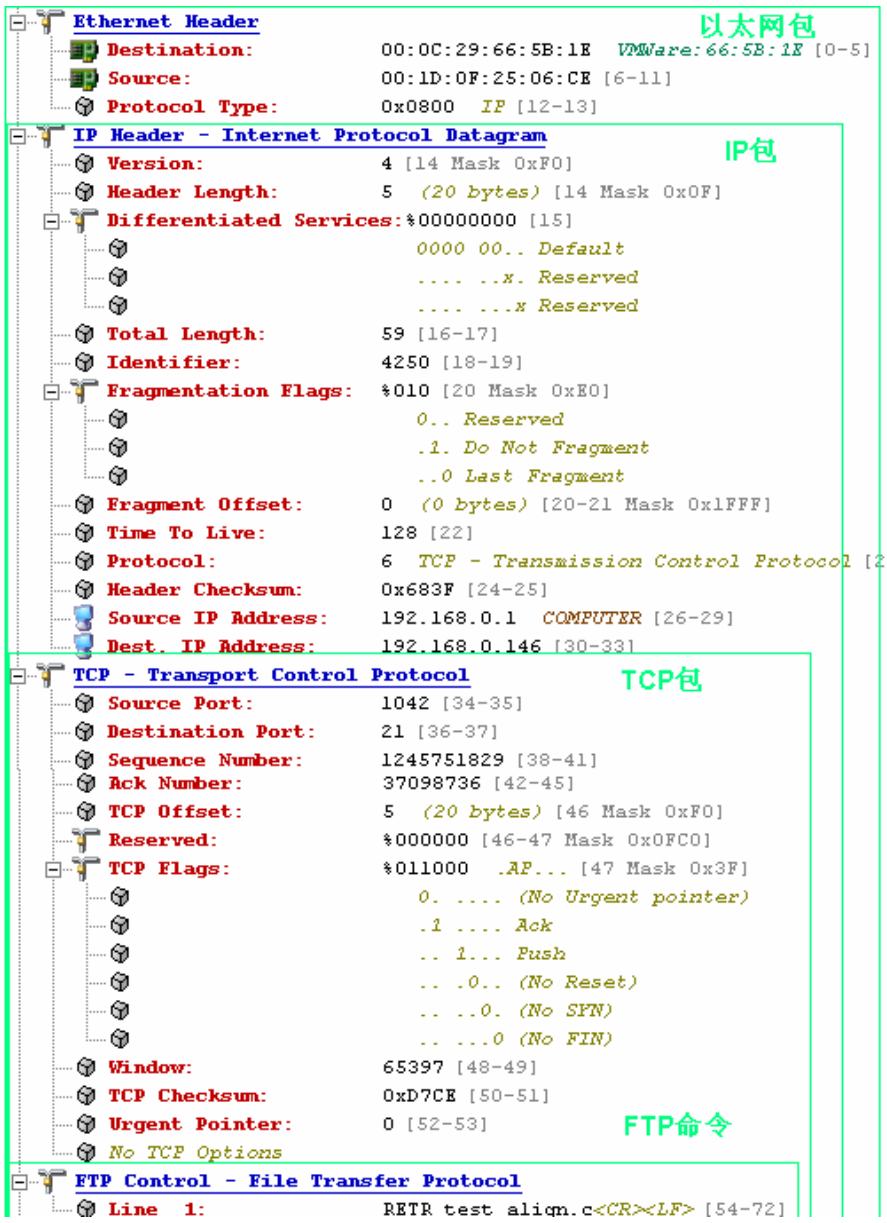


图1-2 局域网上运行FTP的两台主机

- 当ip地址为192.168.0.123的机器运行ftp 192.168.0.132 命令





ARP: 地址解析协议

ARP：地址解析协议

- 每个以太网对应一个硬件地址,称为mac地址.理论是全球唯一的.由IEEE 进行分配
- 在以太网上传输数据以太网包都是通过mac的地址来定位的.IP包则包含以太网包的数据段里
- 因此在以太网网卡之间传输IP包之前,必须先知道对方的mac地址, A R P为I P地址到对应的硬件地址之间提供动态映射。之所以用动态这个词是因为这个过程是自动完成的，一般应用程序用户或系统管理员不必关心。

- RARP（逆地址解析协议）。是ARP的反向操作
- 用arp命令可以手动进行arp各种操作

arp 命令

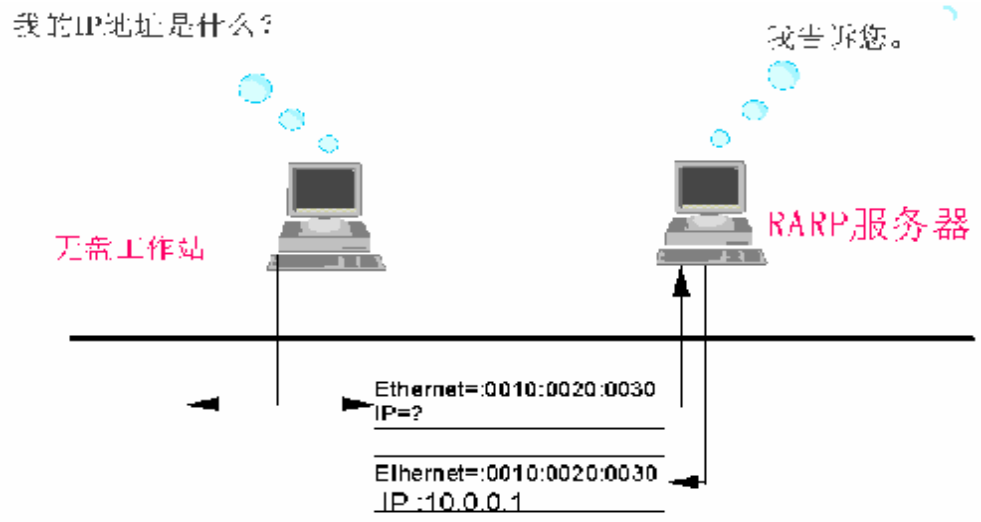
- 可以显示IP与Mac地址的对照表.
  - **Windows** 下运行 **arp –a**

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.0.1 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.0.28          00-30-18-00-56-20     dynamic
  192.168.0.46          00-14-78-44-0a-84     dynamic
  192.168.0.54          00-e0-4c-77-62-66     dynamic
  192.168.0.146         00-0c-29-66-5b-1e     dynamic
  192.168.0.199         00-1e-c9-06-be-a4     dynamic
  192.168.0.234         00-03-0d-8b-bc-9e     dynamic
```

  - **Linux** 下运行**arp**

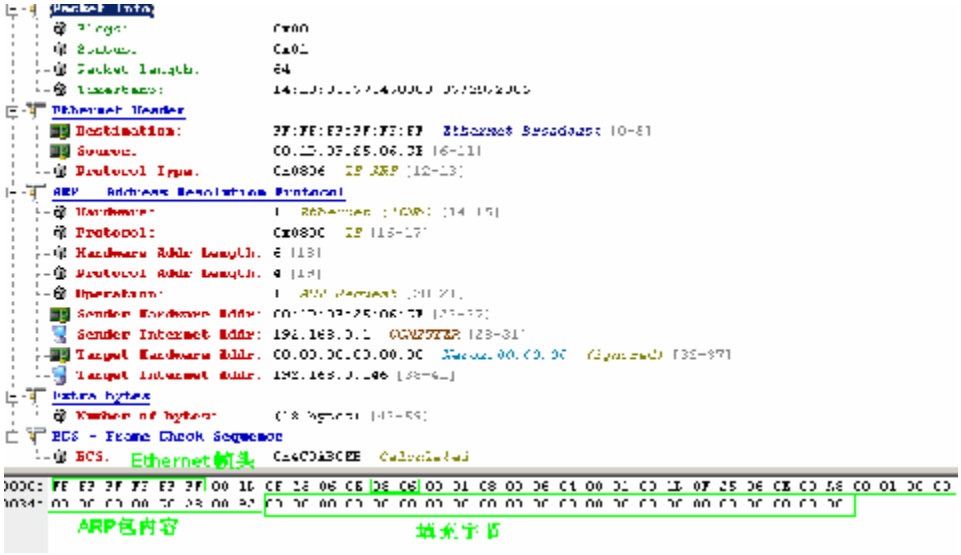
```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.0.1 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.0.28          00-30-18-00-56-20     dynamic
  192.168.0.46          00-14-78-44-0a-84     dynamic
  192.168.0.54          00-e0-4c-77-62-66     dynamic
  192.168.0.146         00-0c-29-66-5b-1e     dynamic
  192.168.0.199         00-1e-c9-06-be-a4     dynamic
  192.168.0.234         00-03-0d-8b-bc-9e     dynamic
```

RARP 协议



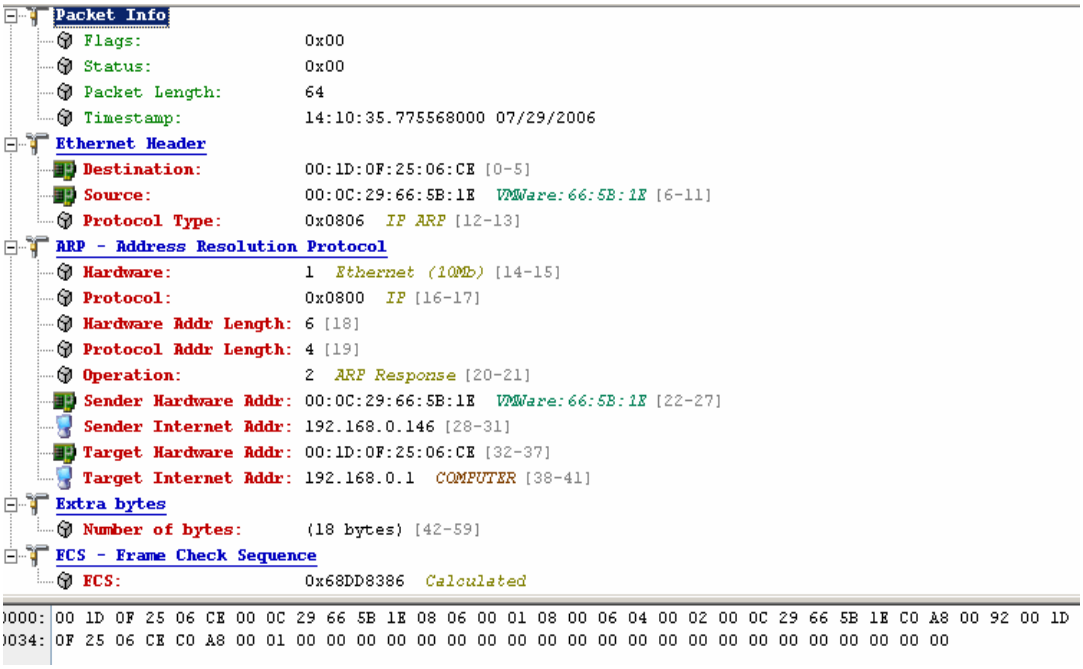
ARP请求,实例

- ARP的以太网协议类型是0x0806



ARP 响应实例

- 从包分析结果得知,IP为192.168.0.146的机器把自己的Mac地址 00:1D:0F:25:06:CE 放在响应包内发回给 00:0C:29:66:5B:1E



FTP 协议

- FTP是另一个常见的应用程序。它是用于文件传输的 Internet标准。我们必须分清文件传送（file transfer）和文件存取(file access)之间的区别，前者是 FTP提供的，后者是如 NFS等应用系统提供的。由 FTP提供的文件传送是将一个完整的文件从一个系统复制到另一个系统中。要使用 FTP，就需要有登录服务器的注册帐号，或者通过允

许匿名F T P的服务器来使用FTP首先是一个FTP包,是一个文本协议.

- 然后封装在TCP里,然后封装在IP包里,然后在以太网帧里发送

FTP介绍

- F T P与我们已描述的另一种应用不同，它采用两个 T C P连接来传输一个文件。
  - 1) 控制连接以通常的客户服务器方式建立。服务器以被动方式打开众所周知的用于F T P的端口（2 1），等待客户的连接。客户则以主动方式打开 T C P端口2 1，来建立连接。控制连接始终等待客户与服务器之间的通信。该连接将命令从客户传给服务器，并传回服务器的应答。由于命令通常是由用户键入的，所以I P对控制连接的服务类型就是“最大限度地减小迟延”。
  - 2) 每当一个文件在客户与服务器之间传输时，就创建一个数据连接。（其他时间也可以创建，后面我们将说到）。由于该连接用于传输目的，所以I P对数据连接的服务特点就是“最大限度提高吞吐量”。

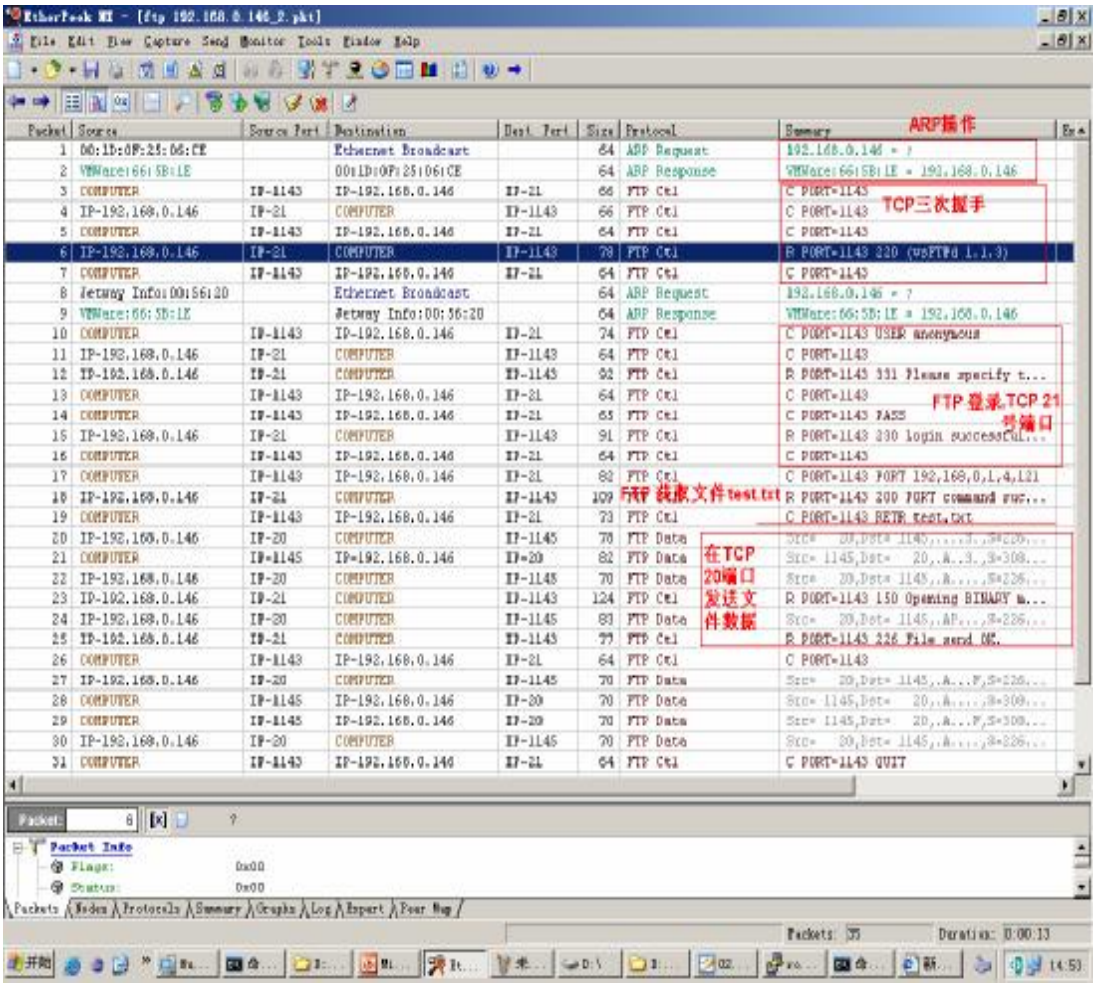
FTP 命令

- 命令和应答在客户和服务器的控制连接上以 NVT ASCII码形式传送。这就要求在每行结尾都要返回C R、L F对（也就是每个命令或每个应答）。
- 这些命令都是3或4个字节的大写A S C I I字符，其中一些带选项参数。从客户向服务器发送的F T P命令超过3 0种。
  - 在FTP命令行输入help可以查看所有命令

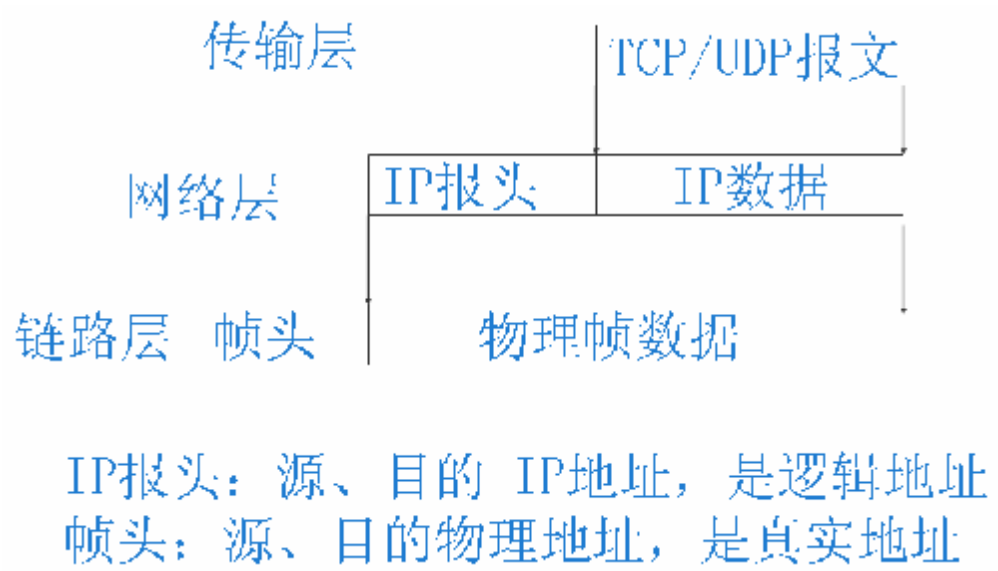
命　令	说　明
ABOR	放弃先前的FTP命令和数据传输
LIST *filelist*	列表显示文件或目录
PASS *password*	服务器上的口令
PORT *n1,n2,n3,n4,n5,n6*	客户端IP地址（*n1.n2.n3.n4*）和端口（*n5*×256+*n6*）
QUIT	从服务器注销
RETR *filename*	检索（取）一个文件
STOR *filename*	存储（放）一个文件
SYST	服务器返回系统类型
TYPE *type*	说明文件类型：A表示ASCII码，I表示图像
USER *username*	服务器上用户名

本次测试所有命令序列

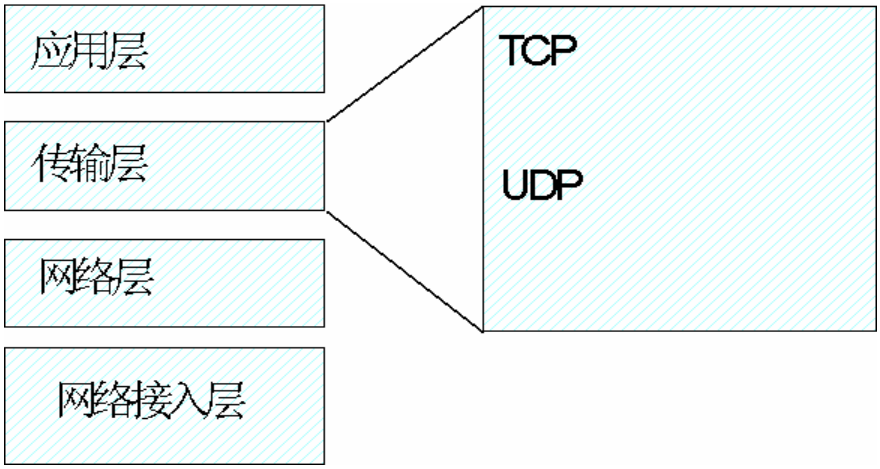
```
C:\Documents and Settings\Administrator>ftp 192.168.0.146
Connected to 192.168.0.146.
220 (vsFTPd 1.1.3)
User (192.168.0.146:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful. Have fun.
ftp> get test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for test.txt (13 bytes).
226 File send OK.
ftp: 13 bytes received in 0.00Seconds 13000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```



应用包的封装



传输层协议概述

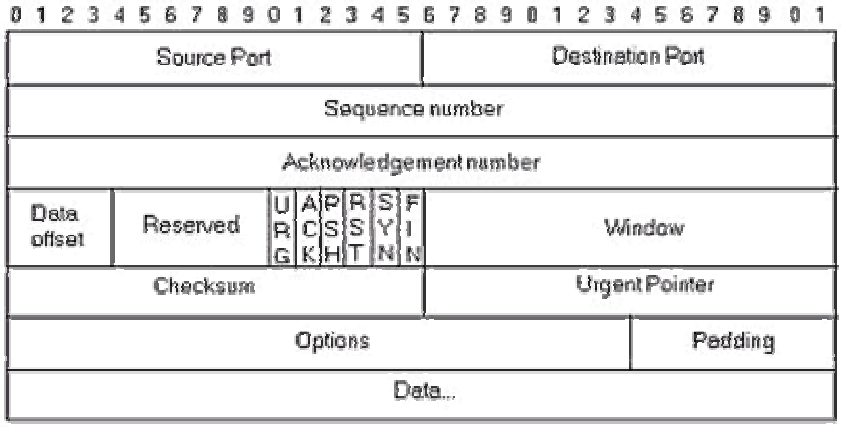


TCP(传输控制协议)

- TCP协议主为了在主机间实现高可靠性的包交换传输协议。
- TCP利用协议栈内部包检测和重传机制在不可靠的IP网络上建立一个可靠的传输的通道.
- TCP相对于UDP,需要一些处理,对服务器要求较高
- 很多协议是建立于TCP之上,如HTTP,FTP,POP3,SMTP(两个E-mail协议)

TCP包头

每个 TCP 的包头都一个定长的结构,比 UDP 要复杂的得多.



TCP Header

TCP的三次握手

相对于 UDP 协议,TCP 是建立一个连接的过程,因此在建立连接和折除连接,有固定步骤.这一些步骤是由 TCP/IP 协议栈的自动完成的.建立连接需要三次交互完成,称为三次握手(three-way handshake).拆除连接需要四次交互,称为四次挥手.

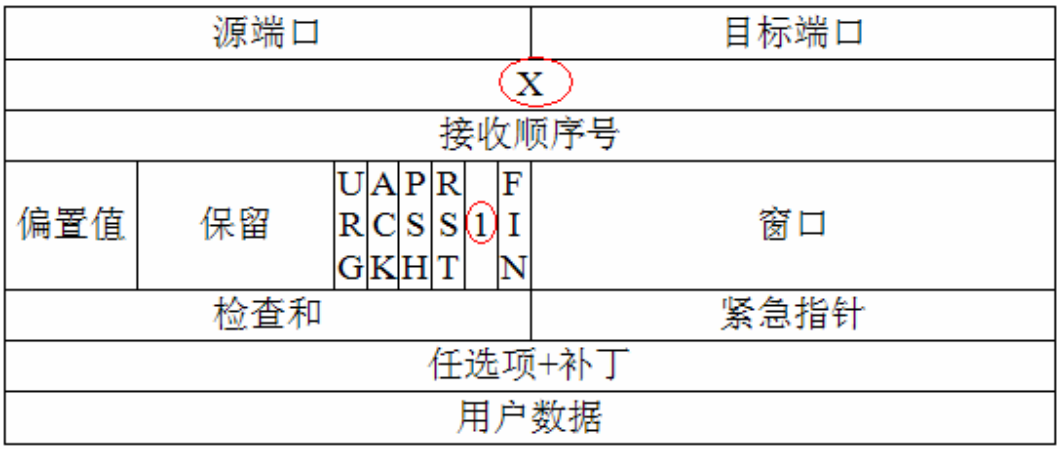
应用层 SOCKET 开发者接触不到这个流程.因此无需了解这些流程也能编写出不错 SOCKET 程序来,但是应际工作中,面试网络相关开发工作,招聘者特别喜欢问三次握手的问题.他

们认为可以通过三次握手的理解来判断出面试者对网络知识的掌握.

因此这里,比较详细分析三次握手的情况.

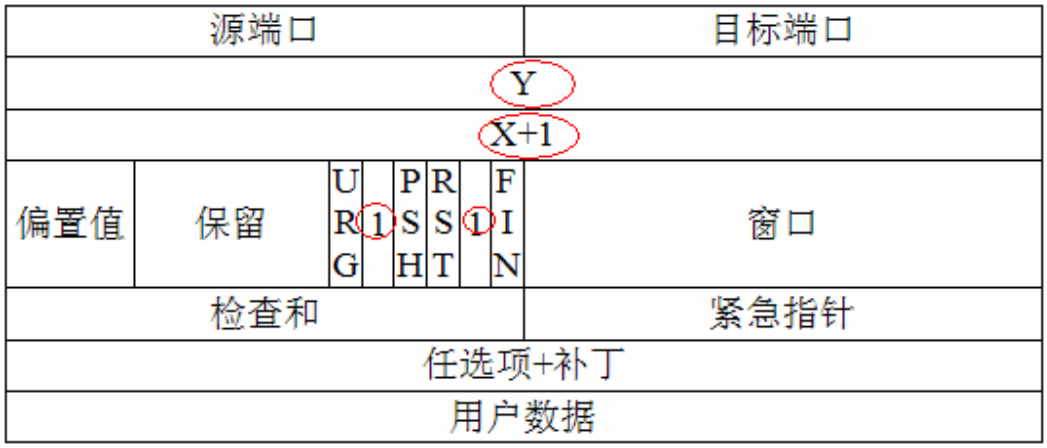
I 第一次握手:

客户端发送一个 TCP 的 SYN 标志位置 1 的包指明客户打算连接的服务器的端口，以及初始序号 X,保存在包头的序列号(Sequence Number)字段里。



I 第二次握手:

服务器发回确认包(ACK)应答。即 SYN 标志位和 ACK 标志位均为 1 同时，将确认序号(Acknowledgement Number)设置为客户的 I S N 加 1 以.即 X+1。



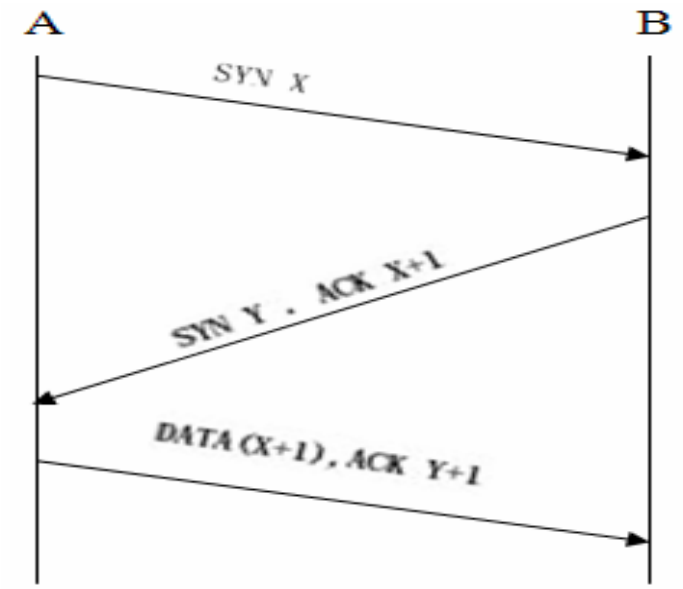
I 第三次握手.

客户端再次发送确认包(ACK) SYN 标志位为 0,ACK 标志位为 1.并且把服务器发来 ACK 的序号字段+1,放在确定字段中发送给对方.并且在数据段放写 ISN 的+1

源端口								目标端口
发送顺序号								
Y+1								
偏置值	保留	URG	1	PSH	RST	SYN	FIN	窗口
检查和								紧急指针
任选项+补丁								
DATA（X+1）								

这三个报文段完成连接的建立。这个过程也称为三次握手（ three-way handshake）。

TCP的三次握手图解



TCP 三次握手的问题

TCP 握手三部分协议依赖于双方合作完成握手,但如果是客户端是一个故意想破坏服务器的黑客的终端.它往往可以用利用握手来进行一种特殊攻击.SYN 洪水攻击(SYN Flooding)

SYN Flooding 思路就是服务完成第二次握手后,客户端故意不发送第三握手的 SYN 包.这样服务器在无限等待.等待时会占用一定服务器资源.当这种客户端到达一定数量时,服务器就会因为资源不够用而停止响应.这是一种典型的 DDOS 攻击.较新的 TCP 服务器采用超时来判断这种情况,到一定时间,比如 50ms,客户端不发来第三次握手的包,服务器自动释放客户端占用资源.

UDP：用户数据报协议

- UDP协议是英文User Datagram Protocol的缩写，即用户数据报协议.

- UDP只是IP协议简单的封装,对数据的完整性等控制均由应用程序控制.因此具有响应速度快的的特点,合适于每次传输数据量小的应用.
- 很多大型网络应用均采用UDP来传输.
  - QQ,VOIP(网络电话),视频会议,网络游戏

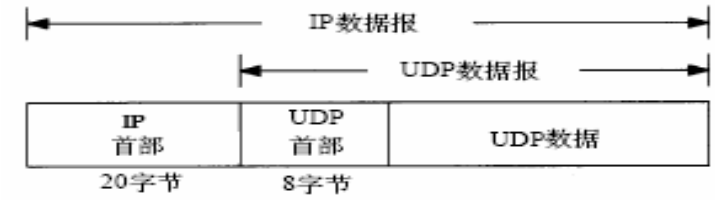
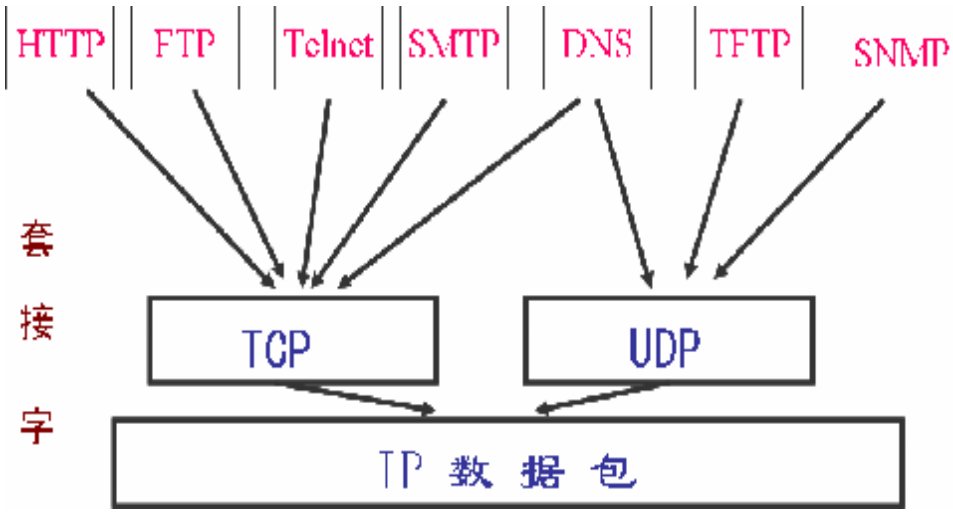


图11-1 UDP封装

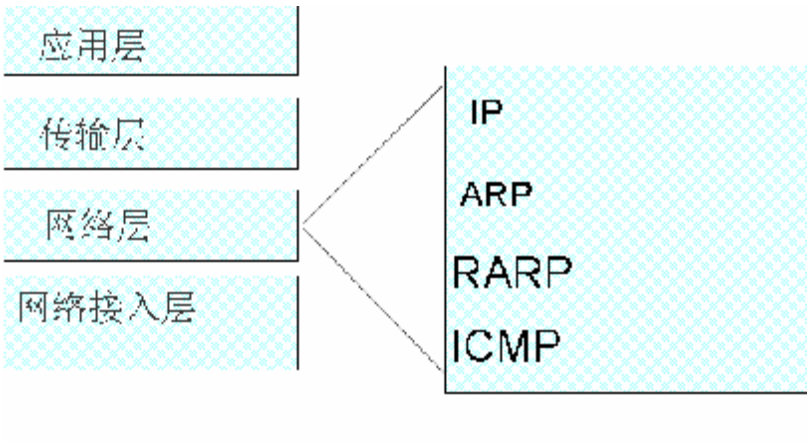
TCP/UDP端口

- 在同一IP上通常会有多个应用.为了让远程的IP上的应用找到对应的服务,TCP/IP协议栈定义端口的概念.
- 端口号的范围从0到65535 ,TCP和UDP是分开的,即两个协议端口互不相干
- 较低端的端口(范围从0到1023)通常都被一些特定协议使用.如21端口分配给FTP服务，25端口分配给SMTP（简单邮件传输协议）服务，80端口分配给HTTP服务，135端口分配给RPC（远程过程调用）服务
- 较高端的端口用户可以自由使用.
- 可以把端口看成是一个在TCP/IP协议栈里面创建的IP包队列.发往远程的包和从这个端口包都放在这个队列里

端 口 号



互联层协议概述



IP包头

版本	报文长度	服务类型	总 长 度	
标 示 符			标志	片 偏 移
生存时间		协 议	报 头 校 验 和	
源 IP 地 址				
目 的 IP 地 址				
IP 选 项				

练习题

- 1.IP协议层是否有端口概念?
- 2.截包软件是否能判断出是不同Socket发来连接?是否能从所截的包看一个TCP是哪一个Socket发出来?
- 手动捕获 TCP 连接时的,三次握手的过程,并且能识别各个阶段的含义