系列文章第一篇，主要是网络编程一些基础知识点。

计算机之间的通信要经过一系列复杂的过程，计算机之间通过传输介质、通信设施和网络通信协议互联，实现资源共享和数据传输。网络编程就是使用程序使互联网的两个（或多个）计算机之间进行数据传输。

同一台计算机不同程序之间、不同计算机之间通信，统一称为进程间通信。进程间通信有很多种方法，如

匿名管道(pipe)：父子进程间的通信

命名管道(fifo)：可以和无关联进程的通信

共享内存(shm)：可以和无关联进程的通信，需要自己处理进程同步，比如和信号量配合。

unix域套接字(unix socket)：可以和无关联进程的通信，使用socket接口。

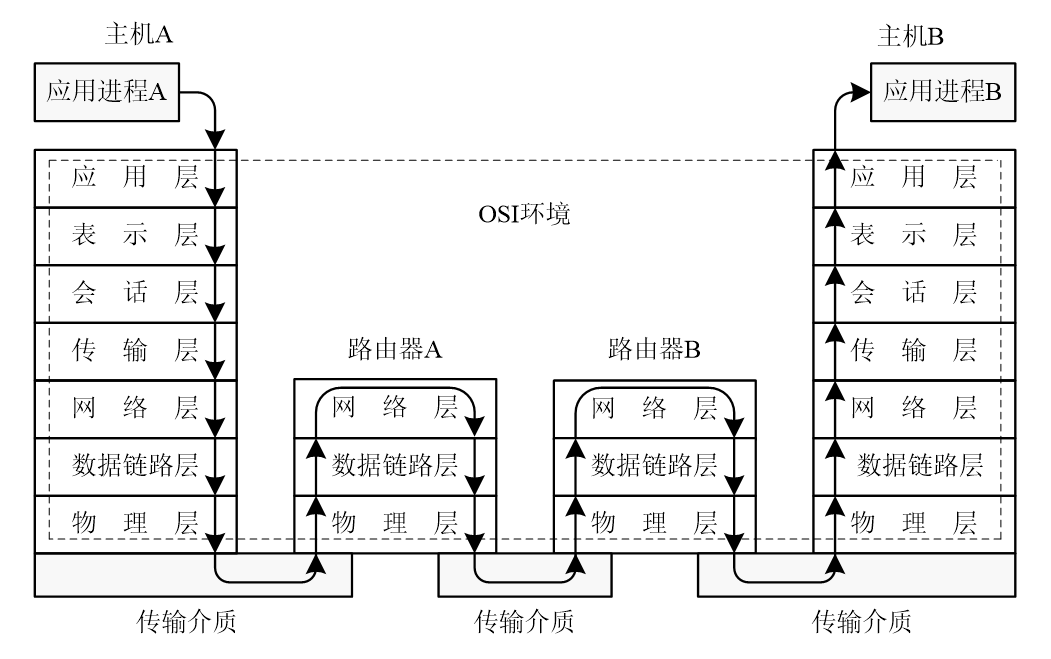
网域套接字(internet socket)：可以跨主机通信，使用socket接口。

等等

系列文章中主要以网域套接字(internet socket)编程，首先了解网络体系结构基本知识，计算机网络的层次模型，规划了两台计算机之间的物理逻辑和通信逻辑。

**一、OSI参考模型**

国际标准化组织ISO提出的，把网络通信的工作分为7层，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。



（1）物理层处于OSI的最底层，是开放系统的基础，它的功能主要是为计算机提供传送数据的通路以及传输数据。

（2）数据链路层的主要任务是实现计算机网络中相邻节点之间的可靠传输，把原始的、有差错的物理传输数据加上数据链路协议以后，构成逻辑上可靠的数据链路。

（3）网络层主要完成的功能主要包括路由选择、网络寻址、流量控制、拥塞控制、网络互连等。实现两个计算机节点之间的数据传输。

（4）传输层涉及源端节点到目的端节点之间可靠的信息传输。也就是说是采用TCP/IP还是采用UDP协议。他需要三次握手四次挥手。

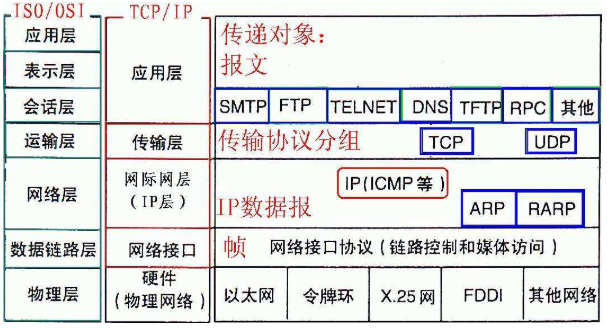
（5）会话层的主要功能是负责应用程序之间建立、维持和中断会话，提供单工、半双工和全双工3种不同的通信方式，使系统和服务之间有序地进行通信。

（6）表示层关心所传输数据信息的格式定义，其主要功能是把应用层提供的信息变换为能够共同理解的形式，提供字符代码、数据格式、控制信息格式、加密等的统一表示。

（7）应用层是直接为应用进程提供服务的。其作用是多个系统应用进程相互通信的同时，完成一系列业务处理所需的服务。

**二、TCP/IP参考模型**

采用4层的层级结构，每一层都呼叫它的下一层所提供的协议来完成自己的需求，这4个层次分别是：网络接口层、网络层（IP层）、传输层、应用层。



（1）网络接口层：对应着OSI参考模型的物理层和数据链路层

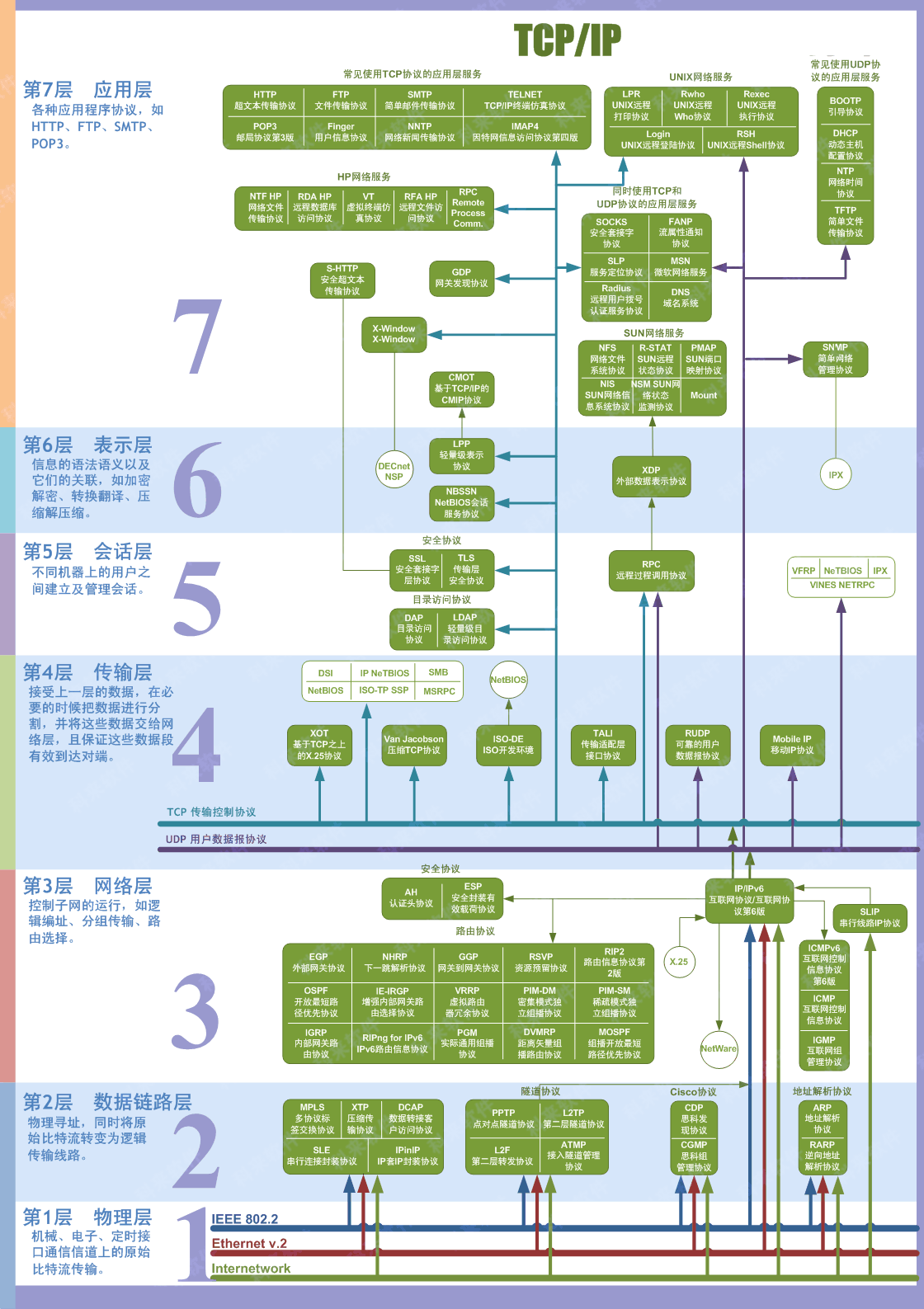
（2）网络层（IP层）：是整个TCP/IP协议栈的核心。它的功能是把分组数据发往目标网络或主机。可以完成将不同类型的网络（异构网）互连的任务。除此之外，还需要完成拥塞控制的功能。

（3）传输层（TCP层）：传输层负责在应用进程之间建立端到端的连接和可靠通信。TCP层涉及两个协议，TCP和UDP。TCP协议提供面向连接的服务，提供按字节流的有序、可靠传输，可以实现连接管理、差错控制、流量控制、拥塞控制等。也就是可靠传输；UDP协议提供无连接的服务，用于不需要或无法实现面向连接的网络应用中。也就是不可靠传输。

（4）应用层：为各种网络应用提供服务。

**三、网络协议**

OSI参考模型和TCP/IP模型在不同的层次中有许多不同的网络协议，如图所示：



有关TCP/IP协议簇中较常见的协议简单介绍

1. **应用层**
2. FTP

FTP（File Transfer Protocol，文件传输协议）是TCP/IP协议组中的协议之一，默认使用TCP端口中的20和21端口，其中20用于传输数据，21用于传输控制信息。

1. Telnet

Telnet协议是Internet远程登录服务的标准协议和主要方式，为用户提供了在本地计算机上完成远程主机工作的能力。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行要开始一个telnet会话，必须输入用户名和密码来登录服务器。协议端口为23。

1. SMTP

SMTP（Simple Mail Transfer Protocol）即简单邮件传输协议。是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议簇，帮助每台计算机在发送或中转信件时找到下一个目的地。协议端口为26。

1. DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议

使用UDP协议工作，主要给内部网络或网络服务供应商自动分配IP地址、给用户或者内部网络管理员作为对所有计算机作中央管理的手段。协议端口为67、68。

1. TFTP

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和服务器之间进行简单文件传输的协议。协议端口为69。

1. HTTP

超文本传输协议（HTTP，Hyper Text Transfer Protocol）是互联网上应用最广泛的一种网络协议。所有的www文件都必须遵守这个标准。设计HTTP最初的目的是为了提供一种发布和接收HTML页面的方法。协议端口：80/8080。

1. **传输层（主机到主机层协议）**
2. TCP协议

TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由IEEE的RFC 793定义。同步的。

1. UDP协议

UDP（User Datagram Protocol，用户数据报协议）是OSI（Open System Interconnection，开发式系统互联）参考模型中的一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务，IETF RFC 768是UDP的正式规范。异步的。

1. **网络层（因特网层协议）**
2. IP

IP协议是用于将多个包交换网络连接起来的，它在源地址和目的地址之间传送一种称之为数据包的东西，它还提供对数据大小的重新组装功能，以适应不同网络对包大小的要求。

1. ICMP

ICMP（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP 协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。

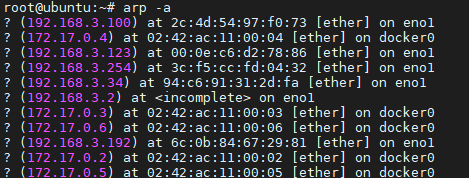
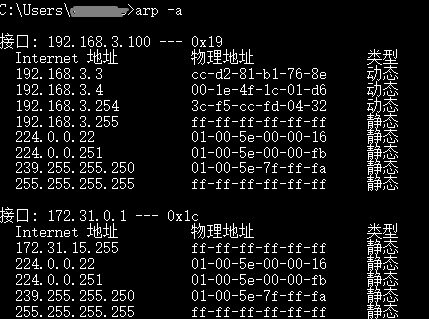
1. IGMP

IGMP（Internet Manage Protocol）Internet组管理协议。提供Internet网际多点传送的功能，即将一个ip包拷贝给多个host。

1. ARP

地址解析协议，即Address Resolution Protocol，是根据IP地址获取物理地址的一个TCP/IP协议。主要功能是将IPv4的地址解析为MAC地址、维护映射的缓存。

网络层对应的IP地址，是跨网段使用的。链路层地址对应的是MAC地址，是物理地址，是在局域网内使用的。

**四、IP地址、MAC地址、端口**

IP 是地址，有定位功能（网与网的通讯） （在逻辑上唯一标识一台电脑） （网络层）

MAC 是身份证，无定位功能（在子网干活） （在物理上唯一标识一台电脑） （链路层）

首先是如何查看ip地址的问题：

Windows：ipconfig

Linux：ifconfig 、ip addr

```

pi@test:~$ ip addr

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

inet6 ::1/128 scope host

valid\_lft forever preferred\_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc mq state UP group default qlen 1000

link/ether dc:a6:32:64:3f:1a brd ff:ff:ff:ff:ff:ff # MAC地址

inet 192.168.3.16/24 brd 192.168.3.255 scope global dynamic eth0 # IPV4地址

valid\_lft 72046sec preferred\_lft 61246sec

inet6 fe80::61c1:d6ac:e60d:99c9/64 scope link # IPV6地址

valid\_lft forever preferred\_lft forever

3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq state DOWN group default qlen 1000

link/ether dc:a6:32:64:3f:1b brd ff:ff:ff:ff:ff:ff

```

在利用TCP/IP协议族进行通信的时候，有三个比较关键的确认身份的信息：mac地址、IP地址和端口号。

* **IP地址** （基于计算机或路由器）在网络层的IP头部里，用于识别网络中互联的主机和路由器，其实主要是确认子网，通过子网掩码确认某个IP地址所在的子网，而后再在子网内部确认mac地址就能找到准确的用户了。
* **mac地址** （基于网卡或路由器）是在数据链路层包裹在以太网头部中的，它主要用来识别同一个链路中的不同计算机。Mac地址即网卡号，每块网卡出厂的时候，都有一个全世界独一无二的 MAC 地址，长度是 48 个二进制位，通常用 12 个十六进制数表示。
* **端口号** 在传输层包含在TCP/UDP头部中的，用于识别应用程序。一台主机上能运行多个程序，那么接收到的消息到底是哪个程序的呢？就需要端口号来确认。

端口号有两种：

* + 固定的端口号，是形如http,telnet,ftp等广为使用的应用协议所使用的端口号是固定的
  + 动态分配的端口号，这个时候服务端要确定监听端口号，接受服务的客户端没必要确定端口号

端口是应用层的概念，每个应用程序（进行网络通信）都占用自己的端口，端口号由传输层协议决定，因此不同传输协议可以使用相同的端口号，所以TCP和UDP可以使用同一个端口号。

端口号用16位2进制数来表示。取值范围0~65535，分为两种端口：0~1024为系统保留或作为系统应用程序占用，通常是固定的、广为人知的，例如FTP服务21、SSH服务的22、HTTP服务80/443；动态端口为剩下的1024~65535，为自己安装的应用程序或服务占用，MySQL的3306、Redis的6379，RTMP的1935。

MAC+IP+PORT完整唯一地确定数据包的发送和接收的端点。在发送端，一个完整的用户数据经过应用层（HTTP）封包、再经过传输层（TCP）封包、再经过网络层（IP）封包、再经过数据链路层（MAC）封包、最后有物理层转换为比特流发送出去，到达接收端后，进行反向传输接封包从而完成一次完成数据的交互。

参考：详解一次完整的数据包传输过程https://blog.csdn.net/u011563903/article/details/90116368