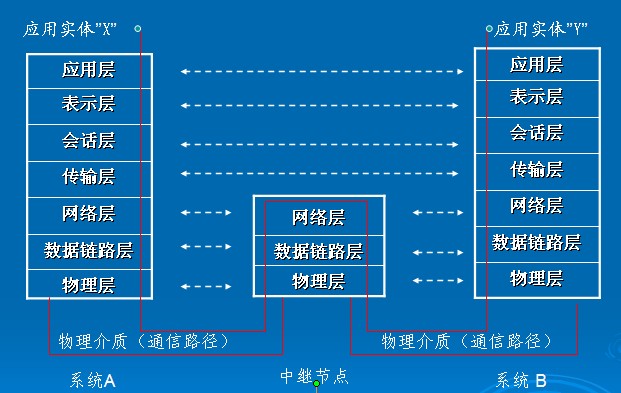
# OSI参考模型：

简记为：物数网传会表应（无数网银未必赢）



二、每层含义：

1、物理层：

   ①提供用于建立、保持和断开物理连接的机械、电气、功能和规程条件；

   ②提供数据流在物理介质上的传输手段，实现节点间的同步；

2、数据链路层：

①用于建立、维持和拆除链路连接，实现无差错传输的功能；

②在点到点或点到多点的链路上，保证报文的可靠传递；

③对相邻连接的通道进行差错控制、数据成帧、同步等控制；

3、网络层：

①主要功能是利用数据链路层所提供的功能，通过路由选择，实现两个系统之间的连接；

②规定了有关网络连接的建立、维持和拆除协议；

4、传输层：

①在系统之间实现数据的收发确认，进行端对端的传输控制；

②用于弥补各种通信网路的质量差异，对经过下三层之后仍然存在的传输差错再次进行纠错，进一步提高数据传输的可靠性；

5、会话层：

①按照应用进程之间的约定，按照正确的顺序收、发数据，进行各种形式的对话；

②接受处理和发送处理的逐个交替变换；

③在单方方向传送大量数据的情况下，给数据打上标记。如果出现通信意外，可以由打标记处重发；

6、表示层：

①主要功能是把应用层提供的信息内容变换为能够共同理解的形式；

②提供字符代码、数据格式、控制信息格式、加密等的统一表示；

③对应用层的信息内容进行形式变换，而不对其内容本身；

7、应用层：

①其功能是实现各应用进程之间的信息交换；

②具有一系列业务处理所需要的服务功能；

三、简记：



# TCP/IP的网络协议层次

对于网络[协议](http://cisco.chinaitlab.com/List_11.html)有所了解的朋友，相信都知道TCP IP网络[协议](http://cisco.chinaitlab.com/List_11.html)这个大户，那么对于TCP IP[协议](http://cisco.chinaitlab.com/List_11.html)来说，我们需要掌握的内容还真不少，这次我们则重点讲解一下协议栈的内容。我们知道，TCP IP网络协议栈分为应用层（Application）、传输层（Transport）、网络层（Network）和链路层（Link）四层。如下图所示。

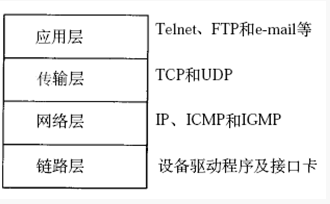
[](http://cisco.chinaitlab.com/UploadFiles_6776/201112/2011120513435446.png)

                                                                    图 TCP IP协议栈  
      
    两台计算机通过TCP IP协议通讯的过程如下所示

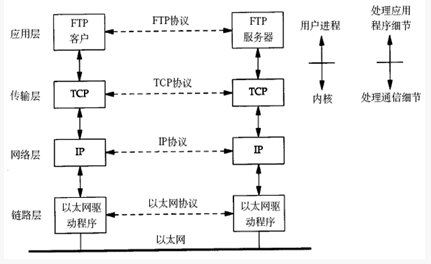
[](http://cisco.chinaitlab.com/UploadFiles_6776/201112/2011120513442336.png)

                                                                              图 TCP IP通讯过程  
      
    传输层及其以下的机制由内核提供，应用层由用户进程提供（后面将介绍如何使用socket API编写应用程序），应用程序对通讯数据的含义进行解释，而传输层及其以下处理通讯的细节，将数据从一台计算机通过一定的路径发送到另一台计算机。应用 层数据通过协议栈发到网络上时，每层协议都要加上一个数据首部（header），称为封装（Encapsulation），如下图所示

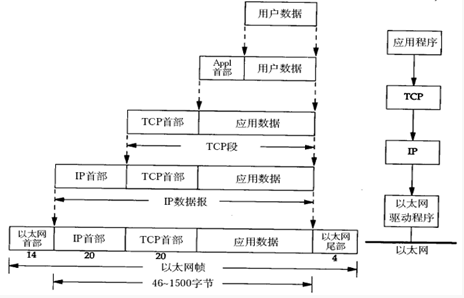
[](http://cisco.chinaitlab.com/UploadFiles_6776/201112/2011120513444891.png)

                                                                                图 TCP IP数据包的封装  
      
    不同的协议层对数据包有不同的称谓，在传输层叫做段（segment），在网络层叫做数据报（datagram），在链路层叫做帧（frame）。数据封装成帧后发到传输介质上，到达目的主机后每层协议再剥掉相应的首部，最后将应用层数据交给应用程序处理。  
      
    上图对应两台计算机在同一网段中的情况，如果两台计算机在不同的网段中，那么数据从一台计算机到另一台计算机传输过程中要经过一个或多个[路由](http://cisco.chinaitlab.com/List_6.html)器，如下图所示

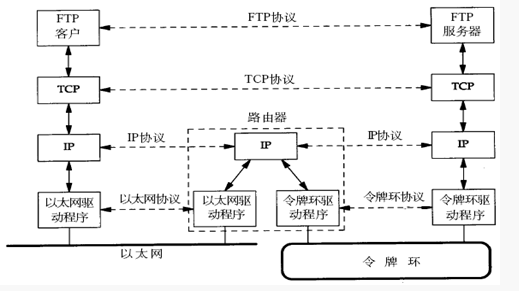
[](http://cisco.chinaitlab.com/UploadFiles_6776/201112/2011120513452470.png)

                                                                              图 跨路由器通讯过程  
      
    其实在链路层之下还有物理层，指的是电信号的传递方式，比如现在以太网通用的网线（双绞线）、早期以太网采用的的同轴电缆（现在主要用于有线电视）、光纤 等都属于物理层的概念。物理层的能力决定了最大传输速率、传输距离、抗干扰性等。集线器（Hub）是工作在物理层的[网络设备](http://network.chinaitlab.com/)，用于双绞线的连接和信号中继（将已衰减的信号再次放大使之传得更远）。

链路层有以太网、令牌环网等标准，链路层负责网卡设备的驱动、帧同步（就是说从网线上检测到什么信号算作新帧的开始）、冲突检测（如果检测到冲突就自动重发）、数据差错校验等工作。[交换](http://cisco.chinaitlab.com/List_7.html)机是工作在链路层的[网络设备](http://network.chinaitlab.com/)，可以在不同的链路层网络之间转发数据帧（比如十兆以太网和百兆以太网之间、以太网和令牌环网之间），由于不同链路层的帧格式不同，[交换](http://cisco.chinaitlab.com/List_7.html)机要将进来的数据包拆掉链路层首部重新封装之后再转发。  
      
    网络层的IP协议是构成Internet的基础。Internet上的主机通过IP地址来标识，Internet上有大量路由器负责根据IP地址选择合适 的路径转发数据包，数据包从Internet上的源主机到目的主机往往要经过十多个路由器。路由器是工作在第三层的网络设备，同时兼有交换机的功能，可以 在不同的链路层接口之间转发数据包，因此路由器需要将进来的数据包拆掉网络层和链路层两层首部并重新封装。IP协议不保证传输的可靠性，数据包在传输过程 中可能丢失，可靠性可以在上层协议或应用程序中提供支持。  
      
    网络层负责点到点（point-to-point）的传输（这里的"点"指主机或路由器），而传输层负责端到端（end-to-end）的传输（这里的" 端"指源主机和目的主机）。传输层可选择TCP或UDP协议。TCP是一种面向连接的、可靠的协议，有点像打电话，双方拿起电话互通身份之后就建立了连 接，然后说话就行了，这边说的话那边保证听得到，并且是按说话的顺序听到的，说完话挂机断开连接。也就是说TCP传输的双方需要首先建立连接，之后由 TCP协议保证数据收发的可靠性，丢失的数据包自动重发，上层应用程序收到的总是可靠的数据流，通讯之后关闭连接。UDP协议不面向连接，也不保证可靠 性，有点像寄信，写好信放到邮筒里，既不能保证信件在邮递过程中不会丢失，也不能保证信件是按顺序寄到目的地的。使用UDP协议的应用程序需要自己完成丢 包重发、消息排序等工作。  
      
    目的主机收到数据包后，如何经过各层协议栈最后到达应用程序呢？整个过程如下图所示

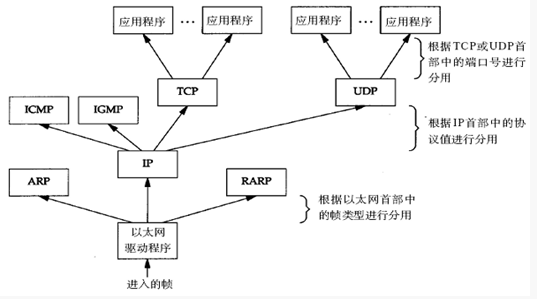
[](http://cisco.chinaitlab.com/UploadFiles_6776/201112/2011120513430354.png)

                                                                         图 Multiplexing过程  
      
    以太网驱动程序首先根据以太网首部中的"上层协议"字段确定该数据帧的有效载荷（payload,指除去协议首部之外实际传输的数据）是IP、ARP还是 RARP协议的数据报，然后交给相应的协议处理。假如是IP数据报，IP协议再根据IP首部中的"上层协议"字段确定该数据报的有效载荷是TCP、 UDP、ICMP还是IGMP,然后交给相应的协议处理。假如是TCP段或UDP段，TCP或UDP协议再根据TCP首部或UDP首部的"端口号"字段确 定应该将应用层数据交给哪个用户进程。IP地址是标识网络中不同主机的地址，而端口号就是同一台主机上标识不同进程的地址，IP地址和端口号合起来标识网 络中唯一的进程。  
      
    注意，虽然IP、ARP和RARP数据报都需要以太网驱动程序来封装成帧，但是从功能上划分，ARP和RARP属于链路层，IP属于网络层。虽然 ICMP、IGMP、TCP、UDP的数据都需要IP协议来封装成数据报，但是从功能上划分，ICMP、IGMP与IP同属于网络层，TCP和UDP属于 传输层。

# TCP通信时的安全性保证和是否增加校验

1. TCP协议是开放性的，就是说可以伪造协议。
2. 如果都严格的遵守协议，TCP的校验和基本上能满足要求，从数据的准确性来说是不需要的，TCP已经保证过了。
3. 但是不能排除数据被篡改，比如经常开机打开网页的时候会跳出电信的广告，这个就是数据插入，如果使用CRC MD5 SHA1等就有可能查出这种问题。实际应用的时候确实一般都加，尤其是游戏上。这主要是用来检测数据是否被人恶意篡改的。 如果你通过tcp传输的是转帐信息，crc，md5之类的还是远远不够的，至少也得1024的rsa签名才够。
4. 常用的办法

加密防止窃听，安全报文防止修改，hash来保证数据被假冒，签名保证数据不可抵赖CRC, MD5, SHA1, RSA