Software School of Shandong University

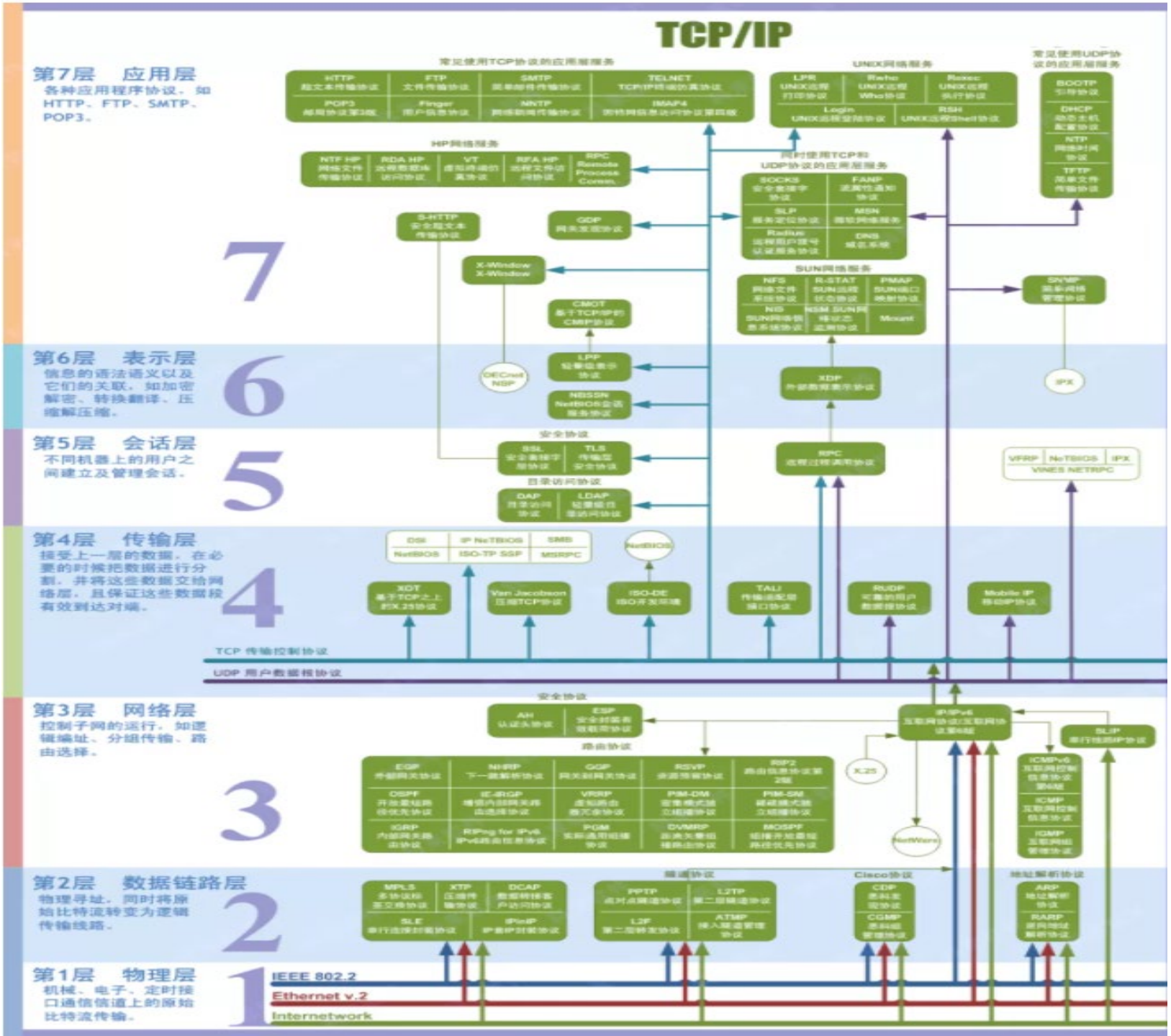
Security Protocols and Standards

--- PKI Principles and technology sd03031340

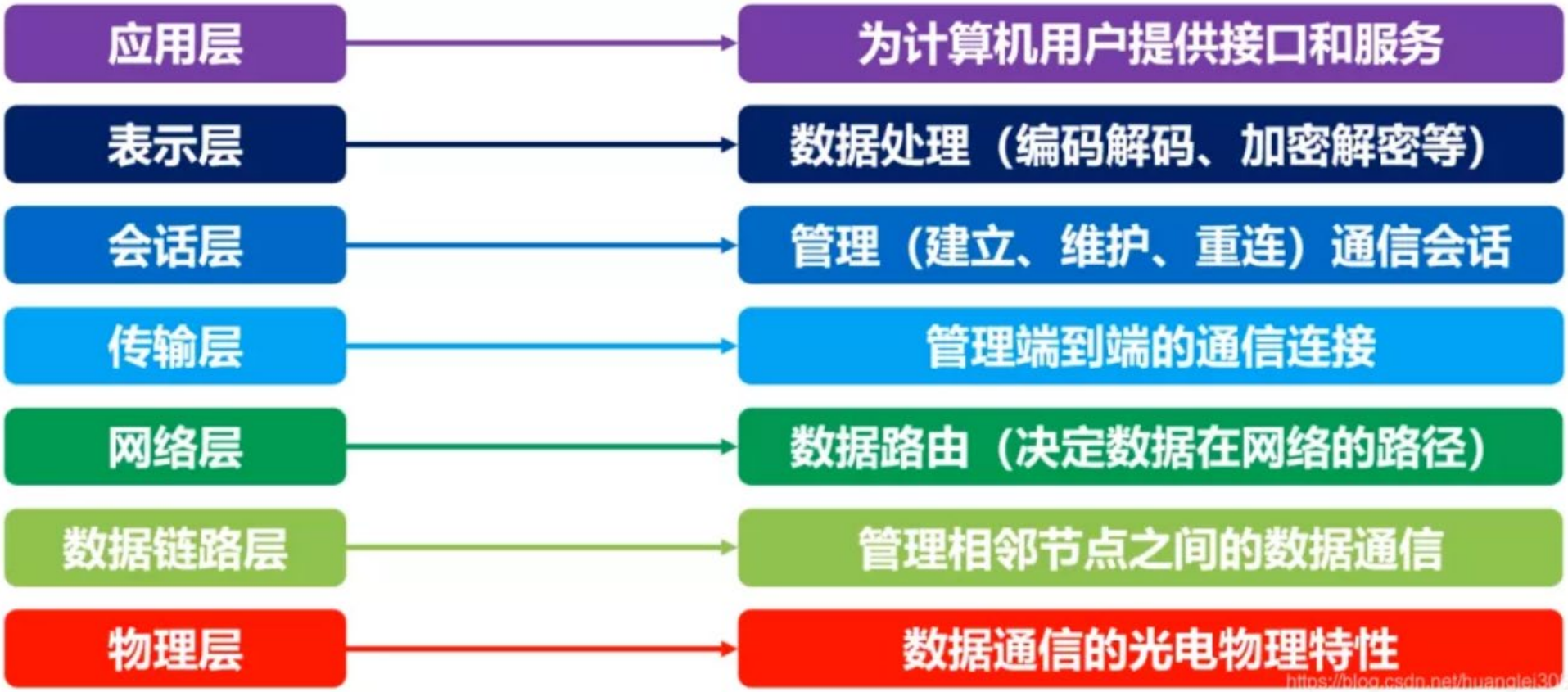
(Chapter 1 Review to Computer Network)

Instructor: AP&Dr. Hou Mengbo 侯孟波
Email: houmb AT sdu.edu.cn
Office: Information Security Research Office.
Office Rm: Office Building 421

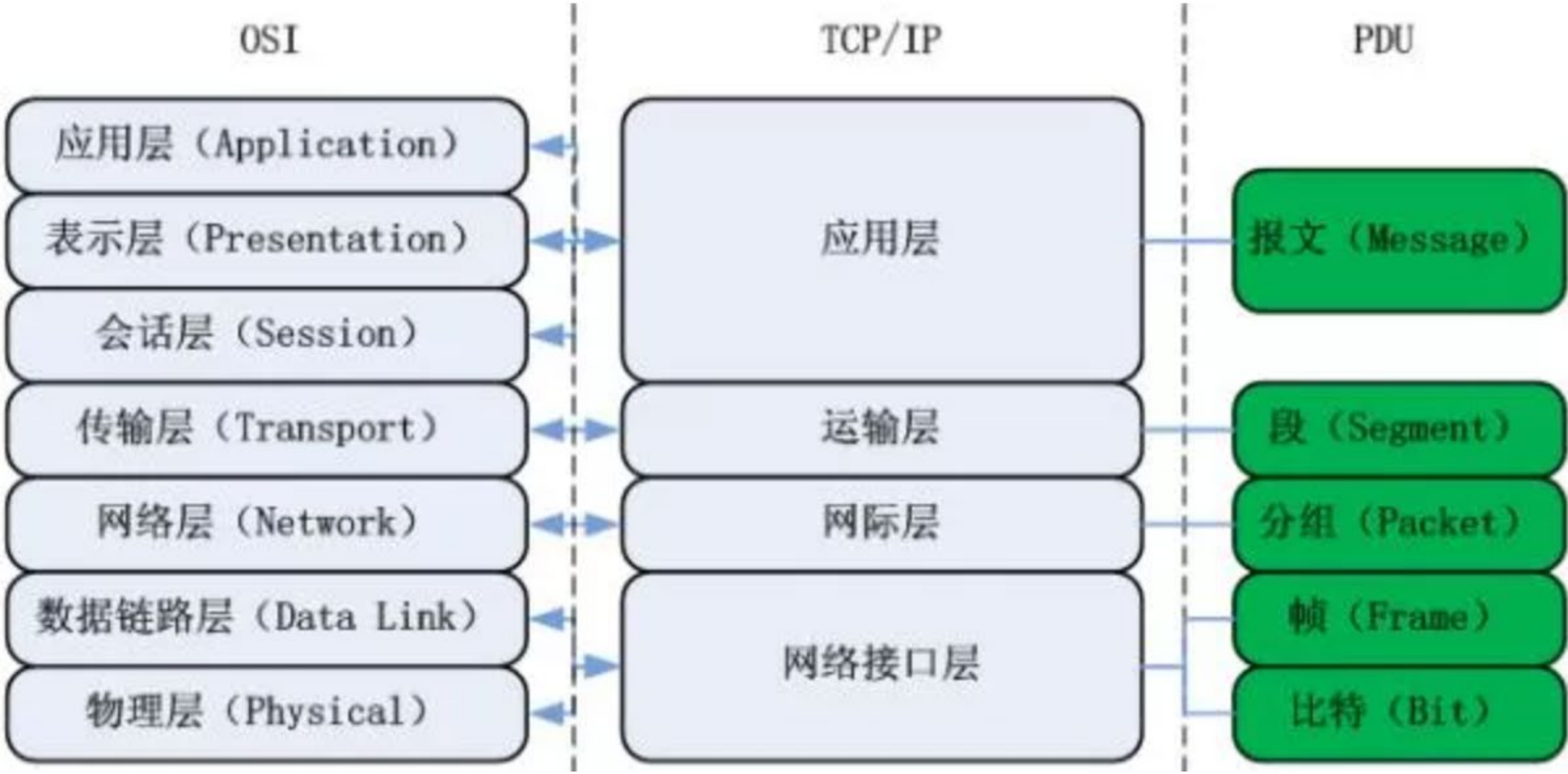
分层结构设计


TCP/IP
第7层 应用层
各种应用程序协议，如HTTP、FTP、SMTP、POP3。
第6层 表示层
信息的语法语义以及它们的关联，如加密解密、转换翻译、压缩解压缩。
第5层 会话层
不同机器上的用户之间建立及管理会话。
第4层 传输层
接受上一层的数据，在必要的时候把数据进行分割，并将这些数据交给网络层，且保证这些数据段有效到达对端。
第3层 网络层
控制子网的运行，如逻辑编址、分组传输、路由选择。
第2层 数据链路层
物理寻址，同时将原始比特流转变为逻辑传输线路。
第1层 物理层
机械、电子、定时接口通信信道上的原始比特流传输。
7
6
5
4
3
2
1
TCP 传输控制协议
UDP 用户数据报协议
IEEE 802.2
Ethernet v.2
Internetwork

计算机网络层次结构

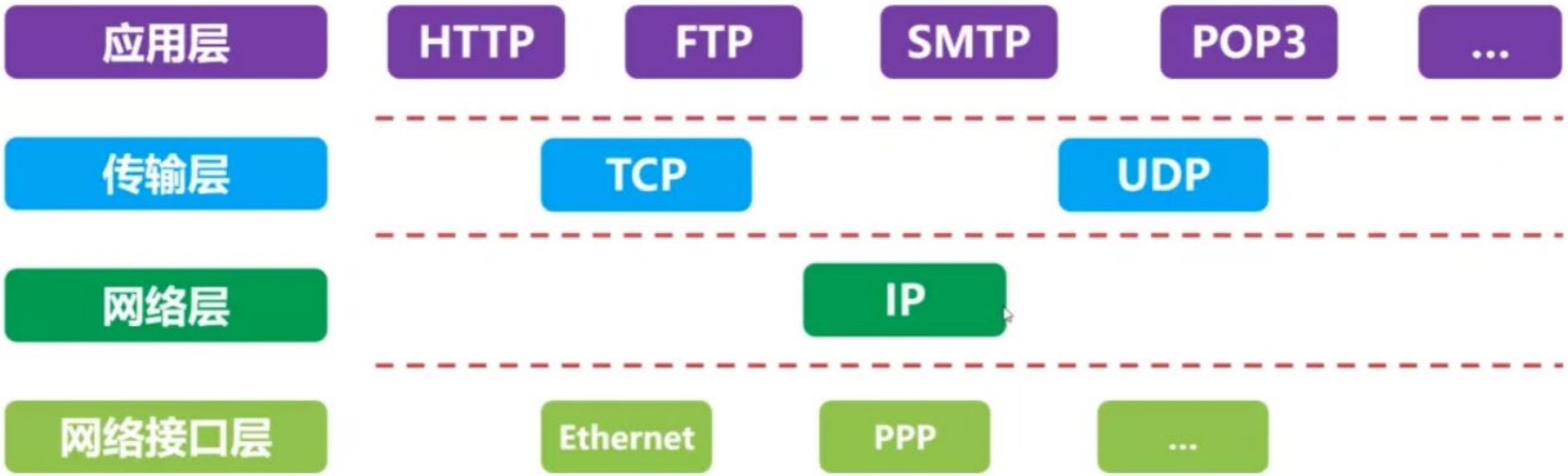

应用层
为计算机用户提供接口和服务
表示层
数据处理（编码解码、加密解密等）
会话层
管理（建立、维护、重连）通信会话
传输层
管理端到端的通信连接
网络层
数据路由（决定数据在网络的路径）
数据链路层
管理相邻节点之间的数据通信
物理层
数据通信的光电物理特性

TCP/IP四层模型与OSI体系结构对比



- 各层之间是相互独立的；
- 每一层需要有足够的灵活性；
- 各层之间完全解耦。

TCP/IP 四层结构



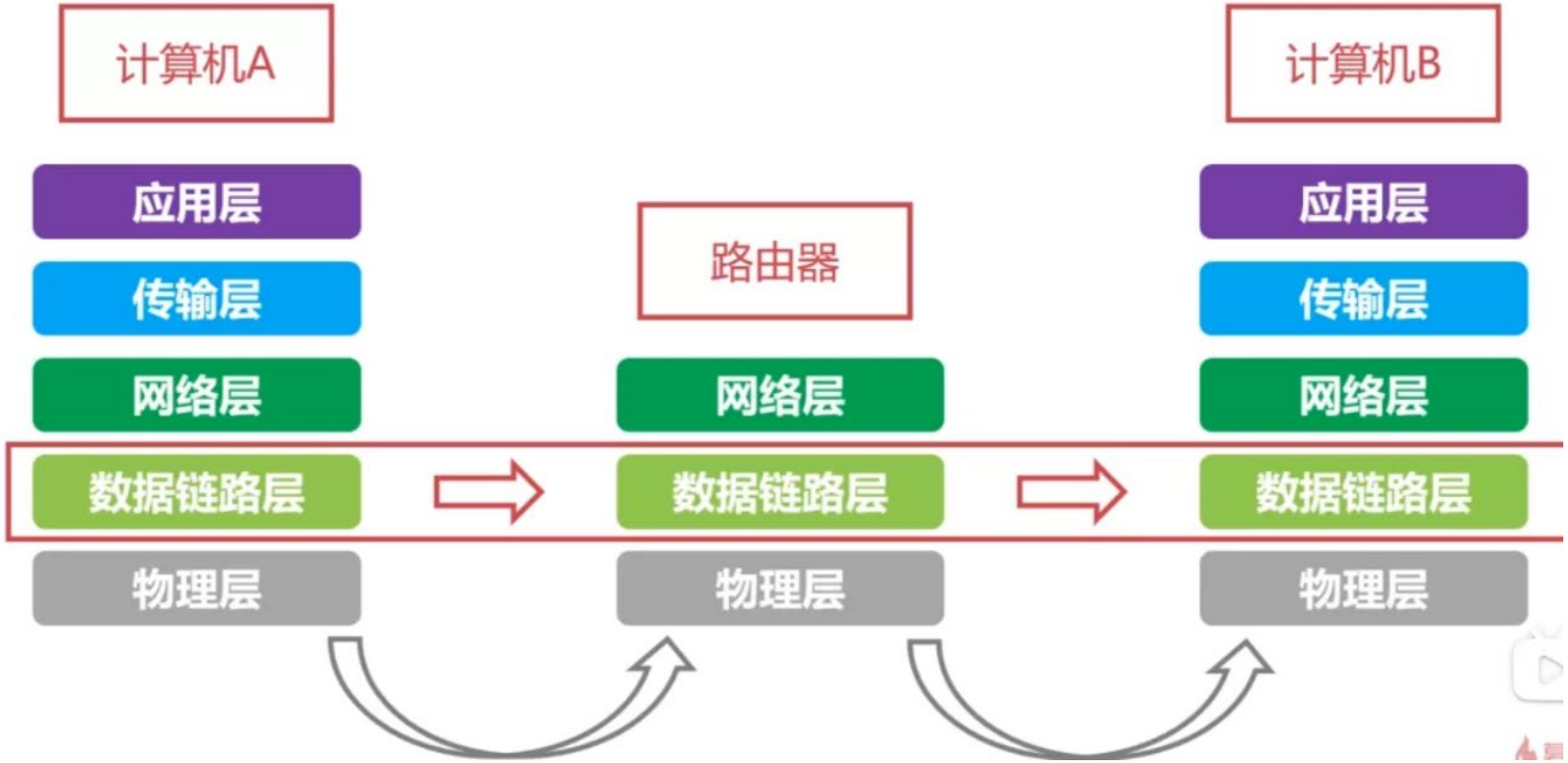
物理层

- 作用：连接不同的物理设备，传输比特流。该层为上层协议提供了一个传输数据的可靠的物理媒体。简单的说，物理层确保原始的数据可在各种物理媒体上传输。
- 设备：中继器、集线器
- 通信信道：单工、半双工、全双工

数据链路层

- 在物理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源自网络层来的数据可靠地传输到相邻节点的目标机网络层。数据链路层在不可靠的物理介质上提供可靠的传输。
- 作用：**物理地址寻址、数据的成帧、流量控制、数据的检错、重发**等。
- 知识点：
  - 数据链路层为网络层提供可靠的数据传输；
  - 基本数据单位为帧，长度受MTU限制；
  - 主要的协议：以太网协议；
  - 两个重要设备名称：网桥和交换机

以太网协议



MAC地址：每一个设备都拥有唯一的MAC地址，共48位。

目的地址	源地址	类型	帧数据	CRC
6	6	2	46~1500	4

Ethernet以太网IEEE802.3

- 以太网第一个广泛部署的高速局域网；以太网数据速率快；以太网硬件价格便宜，网络造价成本低

以太网帧结构：

1. 类型：标识上层协议（2字节）
2. 目的地址和源地址：MAC地址（每个6字节）
3. 数据：封装的上层协议的分组（46~1500字节）
4. CRC：循环冗余码（4字节）
5. 以太网最短帧：以太网帧最短64字节；以太网帧除了数据部分18字节；数据最短46字节；

MAC地址（物理地址、局域网地址）

1. MAC地址长度为6字节，48位；
2. MAC地址具有唯一性，每个网络适配器对应一个MAC地址；
3. 通常采用十六进制表示法，每个字节表示一个十六进制数，用 - 或 : 连接起来；
4. MAC广播地址：FF-FF-FF-FF-FF-FF。

网络层

- 实现两个**端系统**之间的数据透明传送。
- 功能：**寻址和路由选择、连接的建立、保持和终止**等。
- 数据交换技术是报文交换（基本上被**分组**所替代）：采用**储存转发**方式，数据交换单位是**报文**。
- **IP协议：**仅仅提供**不可靠、无连接**的传送服务。主要功能有：无连接数据报传输、数据报路由选择、拥塞控制、差错控制。基本数据单位为IP数据报。
- 配套协议
  - ARP（Address Resolution Protocol，地址解析协议）
  - RARP（Reverse Address Resolution Protocol，逆地址解析协议）
  - ICMP（Internet Control Message Protocol，因特网控制报文协议）
  - IGMP（ Internet Group Management Protocol ，因特网组管理协议）
- 设备： 路由器

路由器相关协议


网络层IP协议相关
IP协议
子网划分
简单路由过程
网络层其他协议
ARP协议与RARP协议
ICMP协议
IP的路由算法
路由的概述
内部网关路由协议
外部网关路由协议

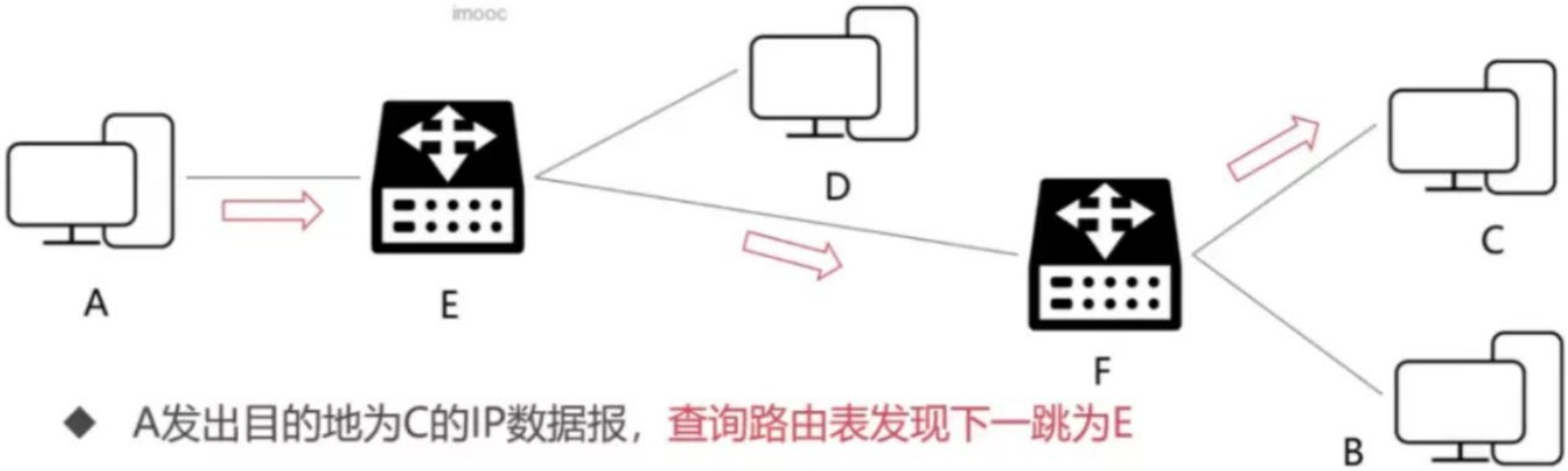
IP协议详解

- IP网际协议是 Internet 网络层最核心的协议。
- 实际的计算机网络错综复杂；物理设备通过使用IP协议，屏蔽了物理网络之间的差异；当网络中主机使用IP协议连接时，无需关注网络细节，于是形成了虚拟网络。

IP数据报

其中，版本指IP协议的版本，占4位，如IPv4和IPv6；首部位长度表示IP首部长度，占4位，最大数值位15；总长度表示IP数据报总长度，占16位，最大数值位65535；TTL表示IP数据报文在网络中的寿命，占8位；协议表明IP数据所携带的具体数据是什么协议的，如TCP、UDP。

IP协议转发流程



- A发出目的地为C的IP数据报，查询路由表发现下一跳为E
- A将数据报发送给E
- E查询路由表发现下一跳为F，将数据报发送给F
- F查询路由表发现目的地C直接连接，将数据报发送给C

IPV4地址的子网划分

xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

类	前缀长度	前缀	首字节
A	8位	0xxxxxxx	0-127
B	16位	10xxxxxx xxxxxxxx	128-191
C	24位	110xxxxx xxxxxxxx xxxxxxxx	192-223
D	不可用	1110xxxx xxxxxxxx xxxxxxxx xxxxxxxx	224-239
E	不可用	1111xxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx	240-255

	最小网络号	最大网络号	子网数量	最小主机号	最大主机号	主机数量
A	0(00000000)	127 (01111111)	2^7	0.0.0	255.255.255	2^24
B	128.0	191.255	2^14	0.0	255.255	2^16
C	192.0.0	223.255.255	2^21	0	255	2^8

A类（8网络号+24主机号）、B类（16网络号+16主机号）、C类（24网络号+8主机号）可以用于标识网络中的主机或路由器，D类地址作为组广播地址，E类是地址保留。

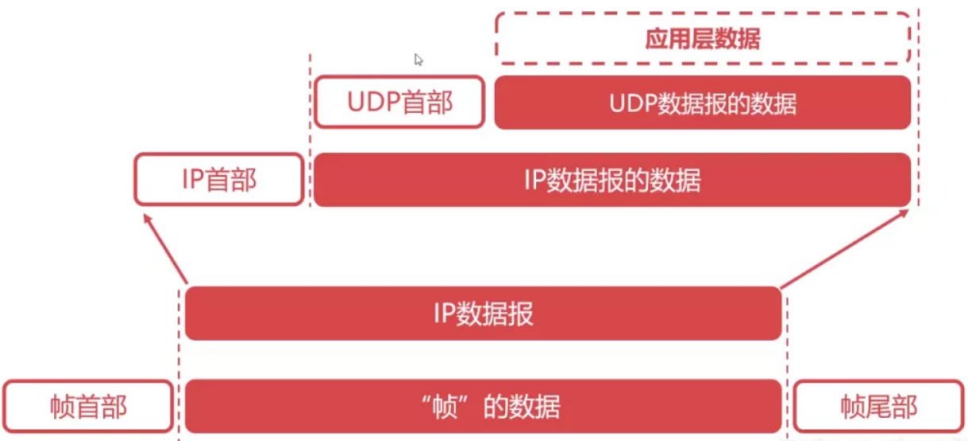
传输层

- 第一个端到端，即主机到主机的层次。传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的差错控制和流量控制问题。
- 传输层的任务是根据通信子网的特性，最佳的利用网络资源，为两个端系统的会话层之间，提供建立、维护和取消传输连接的功能，负责端到端的可靠数据传输。在这一层，信息传送的协议数据单元称为段或报文。
- 网络层只是根据网络地址将源结点发出的数据包传送到目的结点，而传输层则负责将数据可靠地传送到相应的端口。
- 传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输以及端到端的差错控制和流量控制问题；
- 主要协议：TCP协议（Transmission Control Protocol，传输控制协议）、UDP协议（User Datagram Protocol，用户数据报协议）；

- 使用端口(Port)来标记不同的网络进程
- 端口(Port)使用16比特位表示(0~65535)

FTP	HTTP	HTTPS	DNS	TELNET
21	80	443	53	23

UDP(User Datagram Protocol: 用户数据报协议)



首部:8B，四字段/2B【源端口 | 目的端口 | UDP长度 | 校验和】 数据字段：应用数据

特点：无连接、非可靠、面向报文、无拥塞控制、首部开销小

TCP(Transmission Control Protocol: 传输控制协议)

最大报文段长度：报文段中封装的应用层数据的最大长度。

16位源端口			16位目的端口
序号			
确认号			
数据偏移	保留字段	TCP标记	窗口
校验和			紧急指针
TCP选项（可选）			填充

固定20字节

TCP协议的功能：

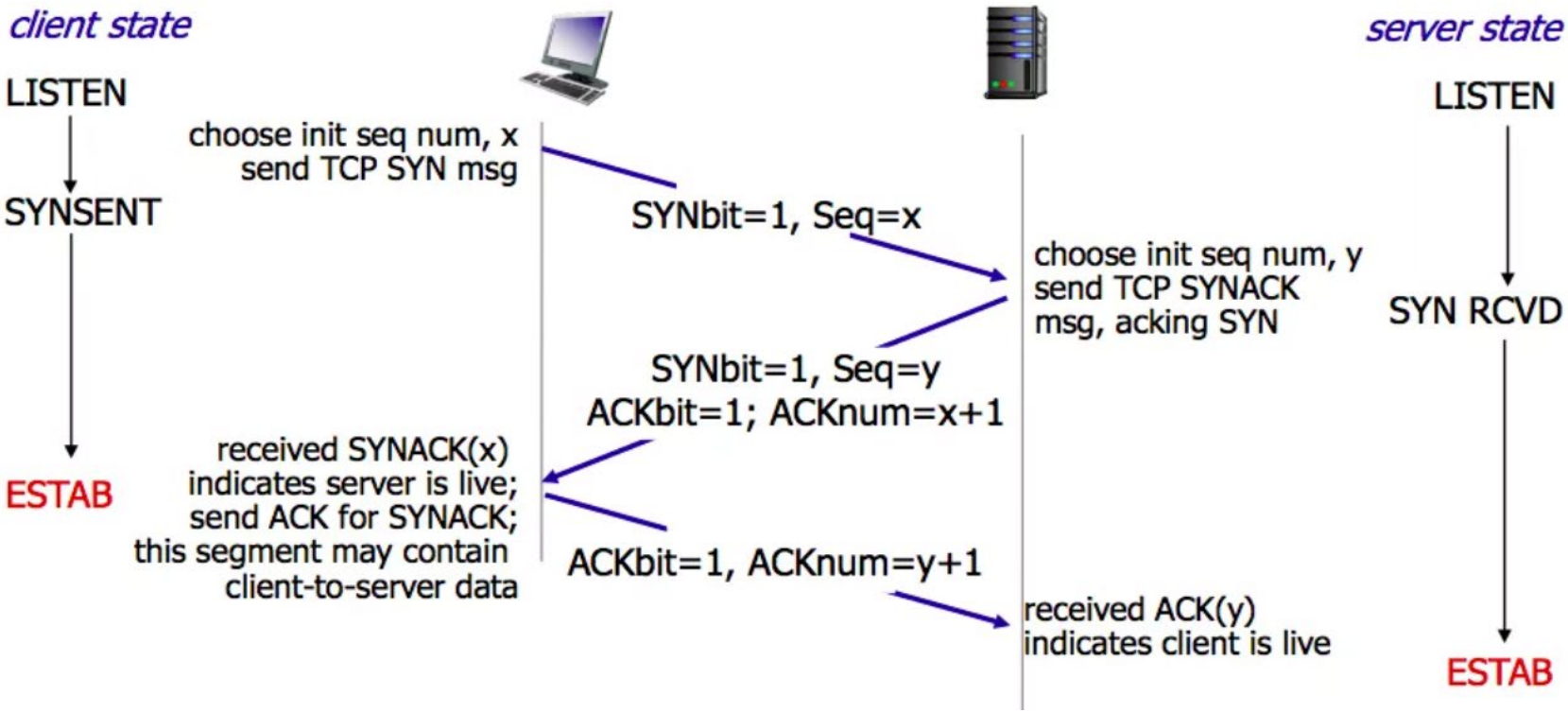
1.对应用层报文进行分段和重组；
2.面向应用层实现复用与分解；
3.实现端到端的流量控制；
4.拥塞控制；
5.传输层寻址；
6.对收到的报文进行差错检测（首部和数据部分都检错）；
7.实现进程间的端到端可靠数据传输控制。

TCP协议的特点：

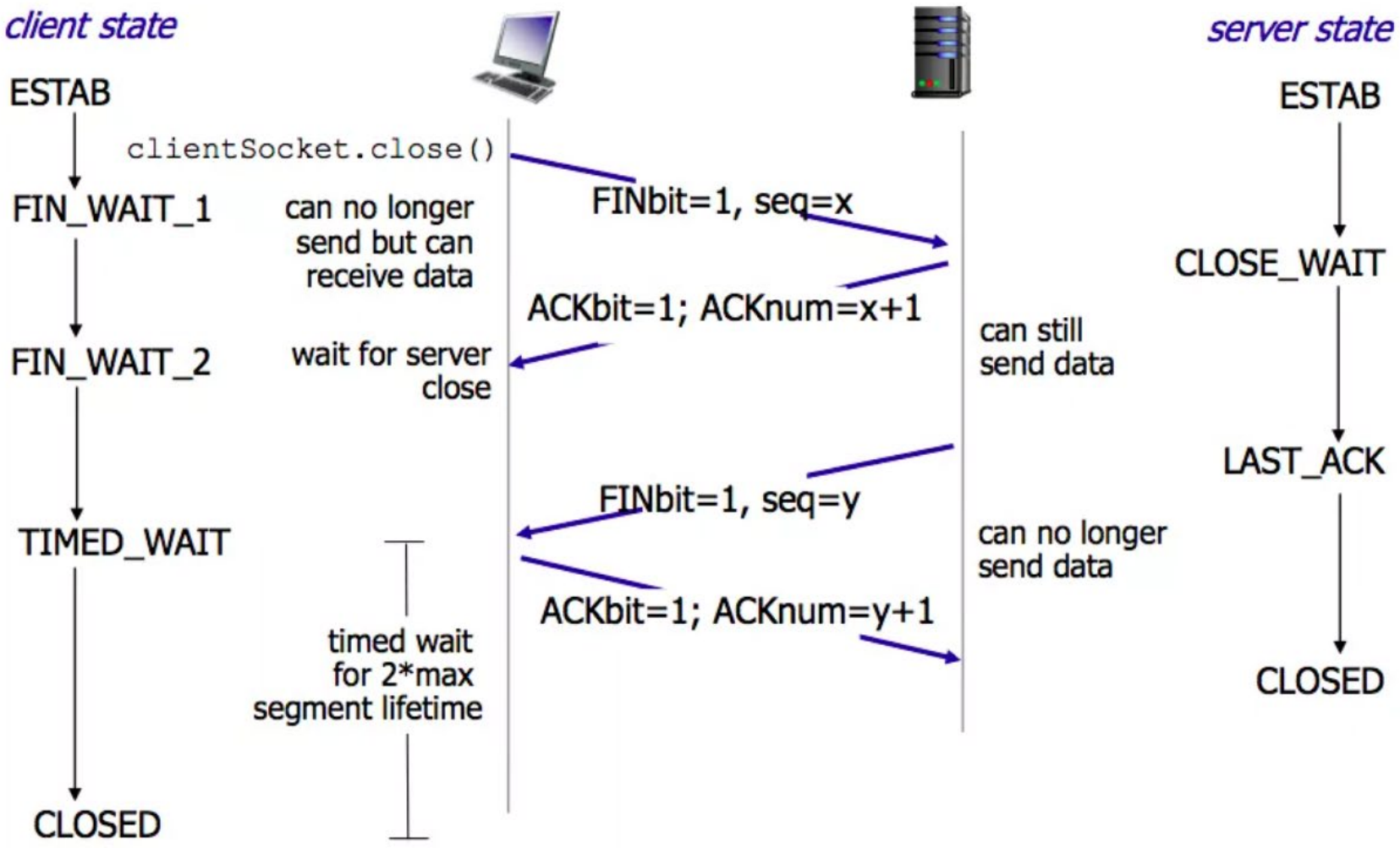
- TCP是面向连接的协议；
- TCP是面向字节流的协议；
- TCP的一个连接有两端，即点对点通信；
- TCP提供可靠的传输服务；
- TCP协议提供全双工通信（每条TCP连接只能一对一）；

TCP连接的三次握手

标记	含义
URG	Urgent: 紧急位，URG=1，表示紧急数据
ACK	Acknowledgement: 确认位，ACK=1，确认号才生效
PSH	Push: 推送位，PSH=1，尽快地把数据交付给应用层
RST	Reset: 重置位，RST=1，重新建立连接
SYN	Synchronization: 同步位，SYN=1 表示连接请求报文
FIN	Finish: 终止位，FIN=1 表示释放连接



TCP连接的四次挥手


client state
ESTAB
clientSocket.close()
FIN_WAIT_1
can no longer send but can receive data
FINbit=1, seq=x
ACKbit=1; ACKnum=x+1
FIN_WAIT_2
wait for server close
can still send data
FINbit=1, seq=y
TIMED_WAIT
can no longer send data
ACKbit=1; ACKnum=y+1
timed wait for 2*max segment lifetime
CLOSED
server state
ESTAB
CLOSE_WAIT
LAST_ACK
CLOSED

应用层

- 为操作系统或网络应用程序提供访问网络服务的接口
- 数据传输基本单位为报文;
- 主要协议:
  - FTP（文件传送协议）端口21
  - Telnet（远程登录协议）
  - DNS（域名解析协议）
  - DHCP（动态主机设置协议）
  - SMTP（邮件传送协议）
  - POP3协议（邮局协议）
  - HTTP协议（Hyper Text Transfer Protocol）端口80

HTTP协议

- 是可靠的数据传输协议，浏览器向服务器发收报文前，先建立TCP连接，HTTP使用TCP连接方式（HTTP自身无连接）。
- HTTP请求报文方式：
  - GET：请求指定的页面信息，并返回实体主体；
  - POST：向指定资源提交数据进行处理请求；
  - DELETE：请求服务器删除指定的页面；
  - HEAD：请求读取URL标识的信息的首部，只返回报文头；
  - OPETION：请求一些选项的信息；
  - PUT：在指明的URL下存储一个文档。
  - UPDATE：更新指定的服务端资源。

操作方式	数据位置	明文密文	数据安全	长度限制	应用场景
GET	HTTP包头	明文	不安全	长度较小	查询数据
POST	HTTP正文	可明可密	安全	支持较大数据传输	修改数据