链滴

转载：36 张图详解计算机网络知识点

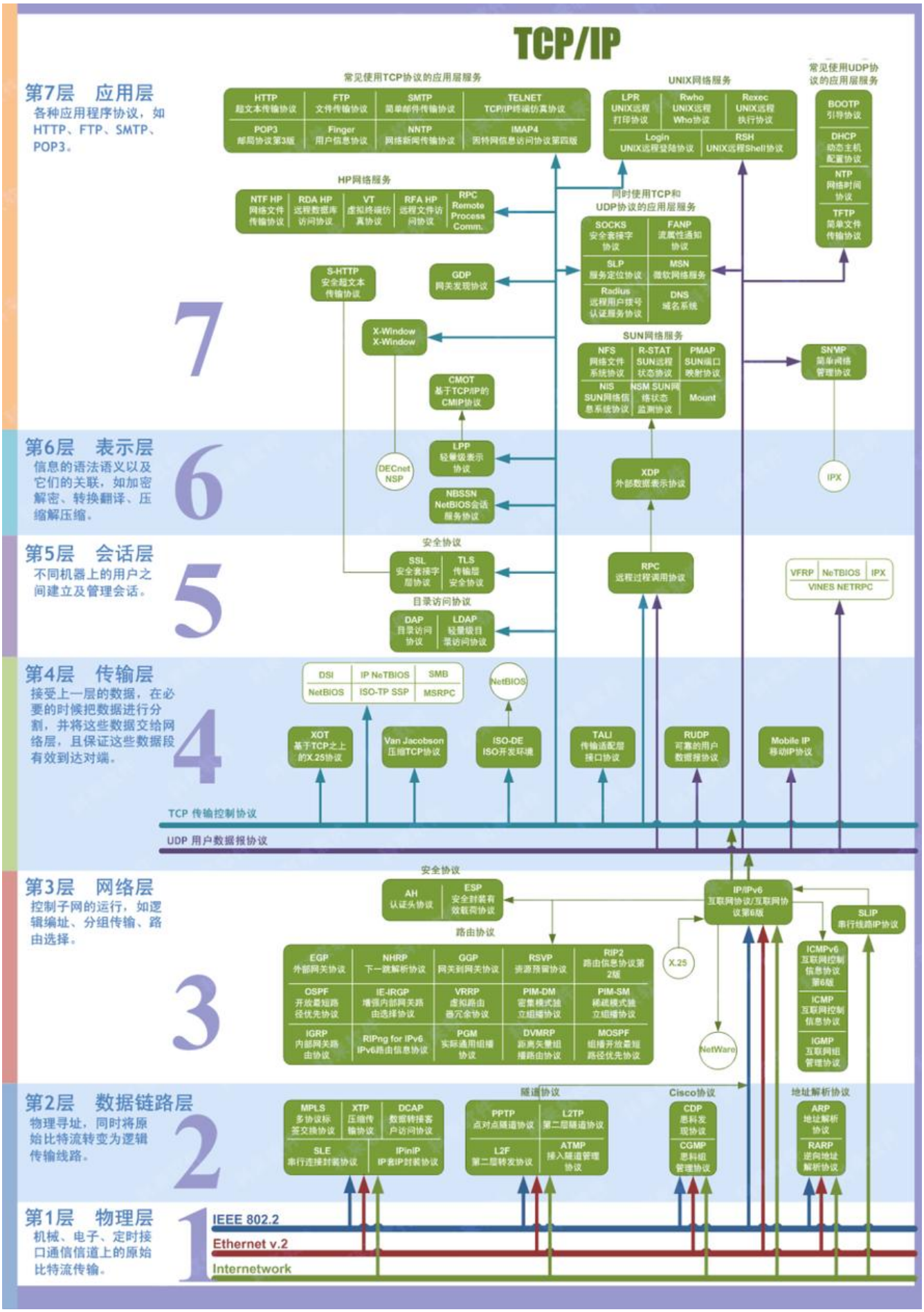
作者：WongKai42817

原文链接：https://ld246.com/article/1640274724095

来源网站：链滴

公众号

一、计算机网络概述



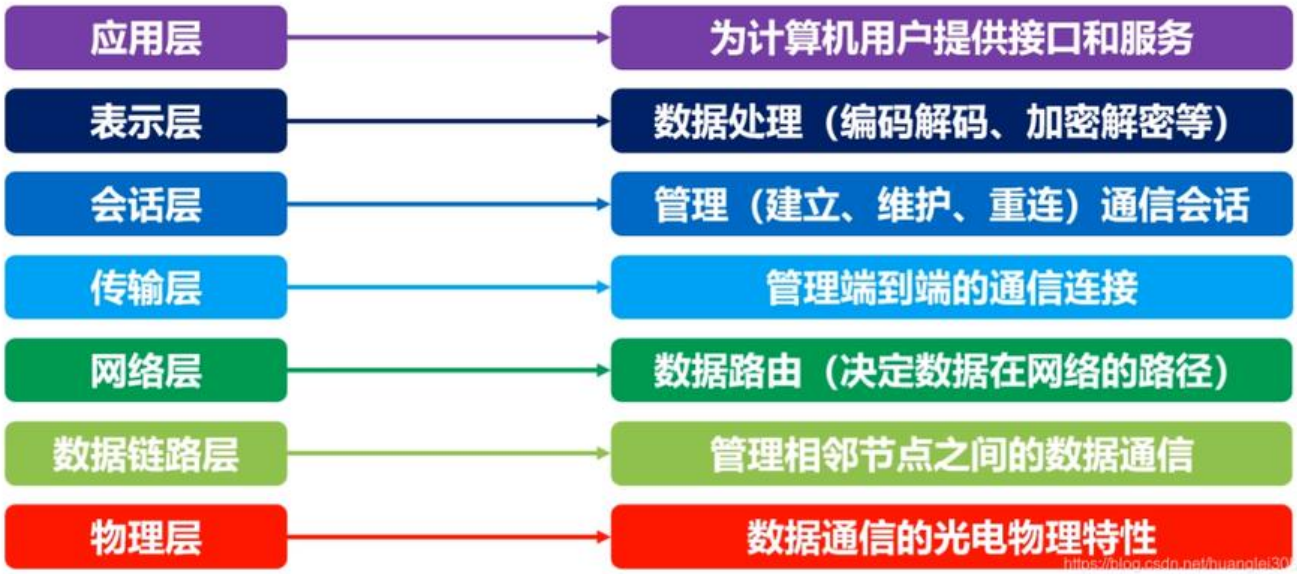
原文链接：转载：36 张图详解计算机网络知识点

1.1 计算机网络的分类

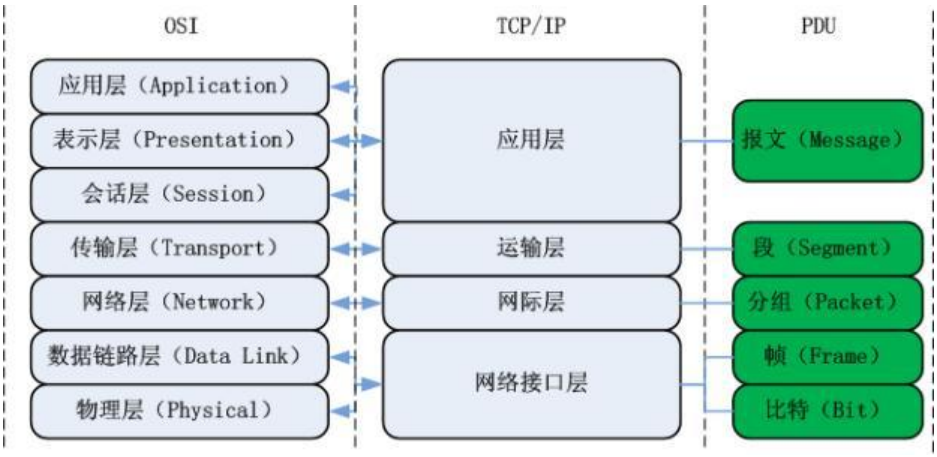
按照网络的作用范围：广域网（WAN）、城域网（MAN）、局域网（LAN）；

按照网络使用者：公用网络、专用网络。

1.2 计算机网络的层次结构



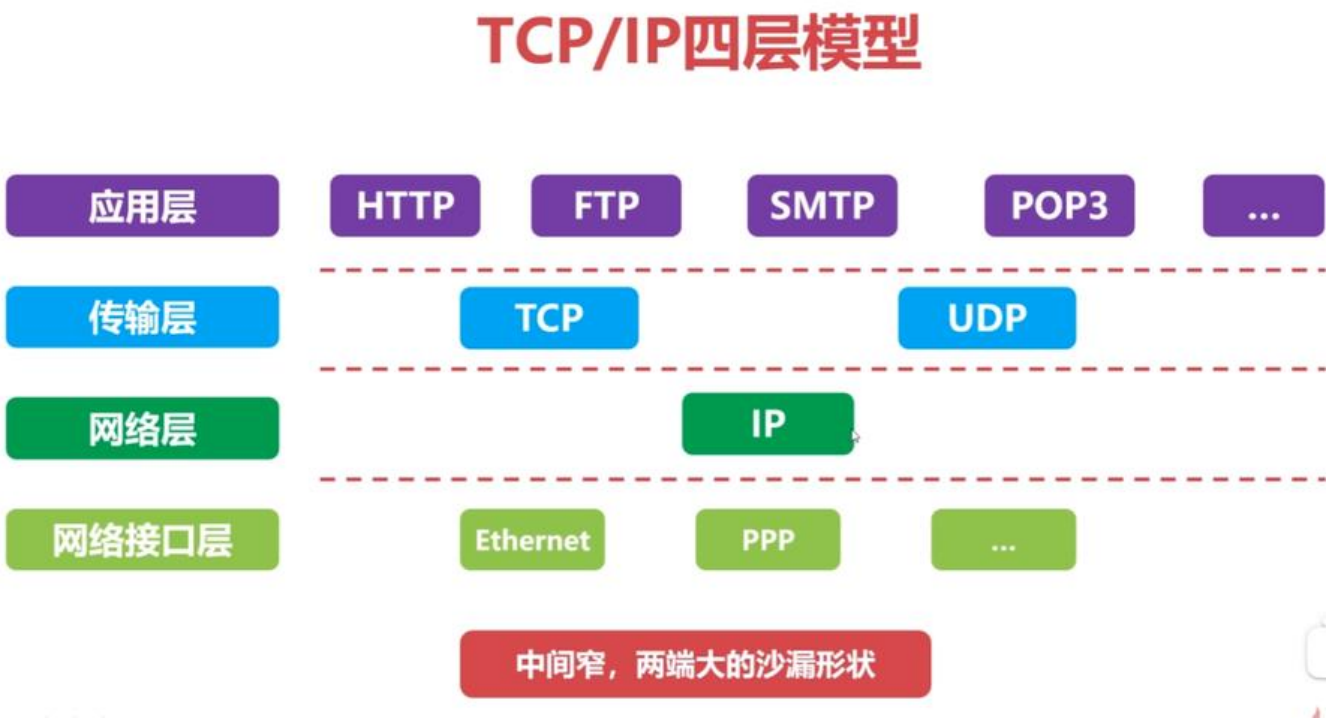
TCP/IP 四层模型与 OSI 体系结构对比：



1.3 层次结构设计的基本原则

- 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。

原文链接：转载：36 张图详解计算机网络知识点



1.4 计算机网络的性能指标

速率：bps=bit/s 时延：发送时延、传播时延、排队时延、处理时延 往返时间 RTT：数据报文在端到通信中的来回一次的时间。

二、物理层

物理层的作用：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。

物理层设备：

- 中继器【Repeater，也叫放大器】：同一局域网的再生信号；两端口的网段必须同一协议；5-4-3程：10BASE-5 以太网中，最多串联 4 个中继器，5 段中只能有 3 个连接主机；
- 集线器：同一局域网的再生、放大信号（多端口的中继器）；半双工，不能隔离冲突域也不能隔离播域。

信道的基本概念：信道是往一个方向传输信息的媒体，一条通信电路包含一个发送信道和一个接受信。

- 单工通信信道：只能一个方向通信，没有反方向反馈的信道；
- 半双工通信信道：双方都可以发送和接受信息，但不能同时发送也不能同时接收；
- 全双工通信信道：双方都可以同时发送和接收。

三、数据链路层

3.1 数据链路层概述

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。

该层的作用包括：**物理地址寻址、数据的成帧、流量控制、数据的检错、重发**等。

有关数据链路层的重要知识点：

- 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；
- 主要的协议：以太网协议；
- 两个重要设备名称：网桥和交换机。

封装成帧：“帧” 是**数据链路层**数据的基本单位：

透明传输：“透明” 是指即使控制字符在帧数据中，但是要当做不存在去处理。即在控制字符前加上义字符 ESC。

3.2 数据链路层的差错监测

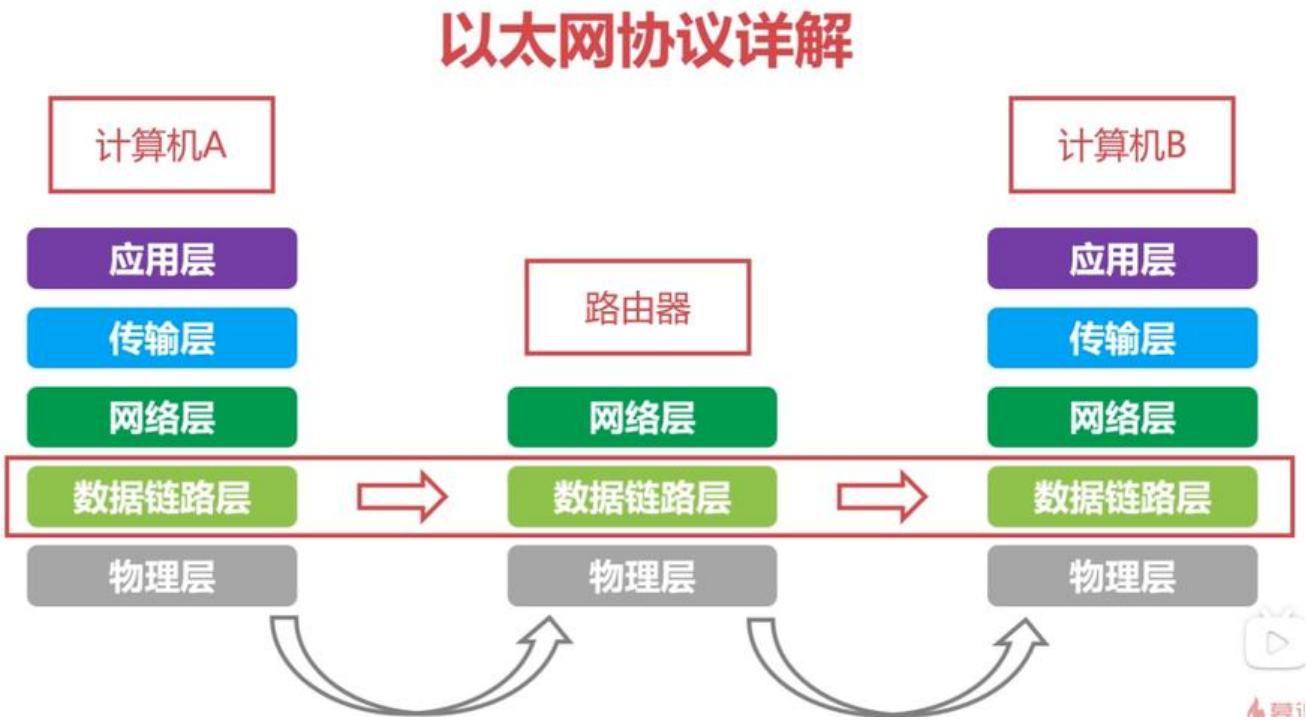
差错检测：奇偶校验码、循环冗余校验码 CRC

- 奇偶校验码–局限性：当出错两位时，检测不到错误。
- 循环冗余检验码：根据传输或保存的数据而产生固定位数校验码。

3.3 最大传输单元 MTU

最大传输单元 MTU(Maximum Transmission Unit)，数据链路层的数据帧不是无限大的，数据帧长受 MTU 限制.

路径 MTU：由链路中 MTU 的最小值决定。



3.4 以太网协议详解

MAC 地址：每一个设备都拥有唯一的 MAC 地址，共 48 位，使用十六进制表示。

以太网协议：是一种使用广泛的局域网技术，是一种应用于数据链路层的协议，使用以太网可以完成邻设备的数据帧传输：

目的地址	源地址	类型	帧数据	CRC
6	6	2	46~1500	4

局域网分类：

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：

- 类型：标识上层协议（2 字节）
- 目的地址和源地址：MAC 地址（每个 6 字节）
- 数据：封装的上层协议的分组（46~1500 字节）
- CRC：循环冗余码（4 字节）
- 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）

- MAC 地址长度为 6 字节，48 位；
- MAC 地址具有唯一性，每个网络适配器对应一个 MAC 地址；
- 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；
- MAC 广播地址：FF-FF-FF-FF-FF-FF。

四、网络层

网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括寻址和路由选择、连接的建立、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，数据交换单位报文。

网络层中涉及众多的协议，其中包括最重要的协议，也是 TCP/IP 的核心协议——IP 协议。IP 协议非简单，仅仅提供不可靠、无连接的传送服务。IP 协议的主要功能有：无连接数据报传输、数据报路由择和差错控制。

与 IP 协议配套使用实现其功能的还有地址解析协议 ARP、逆地址解析协议 RARP、因特网报文协议 IMP、因特网组管理协议 IGMP。具体的协议我们会在接下来的部分进行总结，有关网络层的重点为：

1、网络层负责对子网间的数据包进行路由选择。此外，网络层还可以实现拥塞控制、网际互连等功；2、基本数据单位为 IP 数据报；3、包含的主要协议：

- IP 协议（Internet Protocol，因特网互联协议）；
- ICMP 协议（Internet Control Message Protocol，因特网控制报文协议）；
- ARP 协议（Address Resolution Protocol，地址解析协议）；
- RARP 协议（Reverse Address Resolution Protocol，逆地址解析协议）。

4、重要的设备：路由器。

路由器相关协议

4.1 IP 协议详解

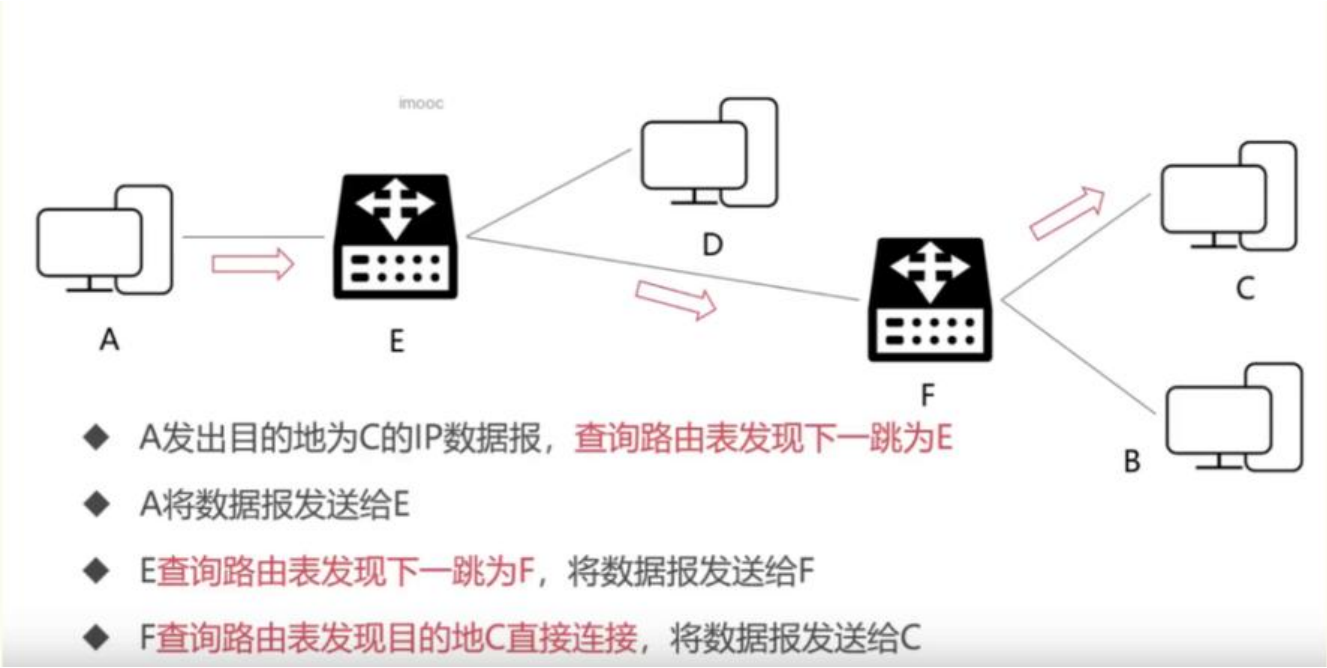
IP 网际协议是 Internet 网络层最核心的协议。虚拟互联网络的产生：实际的计算机网络错综复杂；理设备通过使用 IP 协议，屏蔽了物理网络之间的差异；当网络中主机使用 IP 协议连接时，无需关注络细节，于是形成了虚拟网络。

原文链接：转载：36 张图详解计算机网络知识点

IP 协议使得复杂的实际网络变为一个虚拟互联的网络；并且解决了在虚拟网络中数据报传输路径的问
。

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。

4.2 IP 协议的转发流程



4.3 IP 地址的子网划分

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

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）

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。

	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

4.4 网络地址转换 NAT 技术

用于多个主机通过一个公有 IP 访问访问互联网的私有网络中，减缓了 IP 地址的消耗，但是增加了网通信的复杂度。

NAT 工作原理：

从内网出去的 IP 数据报，将其 IP 地址替换为 NAT 服务器拥有的合法的公共 IP 地址，并将替换关系录到 NAT 转换表中；

从公共互联网返回的 IP 数据报，依据其目的的 IP 地址检索 NAT 转换表，并利用检索到的内部私有 IP 地址替换目的 IP 地址，然后将 IP 数据报转发到内部网络。

4.5 ARP 协议与 RARP 协议

地址解析协议 ARP（Address Resolution Protocol）：为网卡（网络适配器）的 IP 地址到对应的硬地址提供动态映射。可以把网络层 32 位地址转化为数据链路层 MAC48 位地址。

ARP 是即插即用的，一个 ARP 表是自动建立的，不需要系统管理员来配置。

IP地址	MAC地址
192.168.83.254	00-50-56-e0-33-40
192.168.83.255	01-00-5e-00-00-16
224.0.0.251	01-00-5e-00-00-fc
239.1.2.3	01-00-5e-40-98-8f
255.255.255.255	01-00-5e-7f-ff-fa

RARP(Reverse Address Resolution Protocol) 协议指逆地址解析协议，可以把数据链路层 MAC48 地址转化为网络层 32 位地址。

4.6 ICMP 协议详解

网际控制报文协议（Internet Control Message Protocol），可以报告错误信息或者异常情况，ICMP 报文封装在 IP 数据报当中。

ICMP 协议的应用：

- Ping 应用：网络故障的排查；
- Traceroute 应用：可以探测 IP 数据报在网络中走过的路径。

4.7 网络层的路由概述

关于路由算法的要求：正确的完整的、在计算上应该尽可能是简单的、可以适应网络中的变化、稳定公平的。

自治系统 AS：指处于一个管理机构下的网络设备群，AS 内部网络自治管理，对外提供一个或多出入口，其中自治系统内部的路由协议为内部网关协议，如 RIP、OSPF 等；自治系统外部的路由协为外部网关协议，如 BGP。

静态路由：人工配置，难度和复杂度高；

动态路由：

- 链路状态路由选择算法 LS：向所有隔壁路由发送信息收敛快；全局式路由选择算法，每个路由器计路由时，需构建整个网络拓扑图；利用 Dijkstra 算法求源端到目的端网络的最短路径；Dijkstra(迪杰特拉) 算法
- 距离 - 向量路由选择算法 DV：向所有隔壁路由发送信息收敛慢、会存在回路；基础是 Bellman-Fod 方程（简称 B-F 方程）；

4.8 内部网关路由协议之 RIP 协议

路由信息协议 RIP(Routing Information Protocol)【应用层】，基于距离 - 向量的路由选择算法，小的 AS（自治系统），适合小型网络；RIP 报文，封装进 UDP 数据报。

RIP 协议特性：

- RIP 在度量路径时采用的是跳数（每个路由器维护自身到其他每个路由器的距离记录）；
- RIP 的费用定义在源路由器和目的子网之间；
- RIP 被限制的网络直径不超过 15 跳；

- 和隔壁交换所有的信息，30 主动一次（广播）。

4.9 内部网关路由协议之 OSPF 协议

开放最短路径优先协议 OSPF(Open Shortest Path First)【网络层】，基于链路状态的路由选择算法即 Dijkstra 算法），较大规模的 AS，适合大型网络，直接封装在 IP 数据报传输。

OSPF 协议优点：

- 安全；
- 支持多条相同费用路径；
- 支持区别化费用度量；
- 支持单播路由和多播路由；
- 分层路由。

RIP 与 OSPF 的对比（路由算法决定其性质）：

RIP协议	OSPF协议
从邻居看网络	整个网络的拓扑
在路由器之间累加距离	Dijkstra算法计算最短路径
频繁、周期更新，收敛很慢	状态变化更新，收敛很快
路由间拷贝路由信息	路由间传递链路状态，自行计算路径

4.10 外部网关路由协议之 BGP 协议

BGP（Border Gateway Protocol）边际网关协议【应用层】：是运行在 AS 之间的一种协议，寻找一好路由：首次交换全部信息，以后只交换变化的部分，BGP 封装进 TCP 报文段.

五、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相应的端口。

有关网络层的重点：

- 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

制问题；

- 包含的主要协议：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）；
- 重要设备：网关。

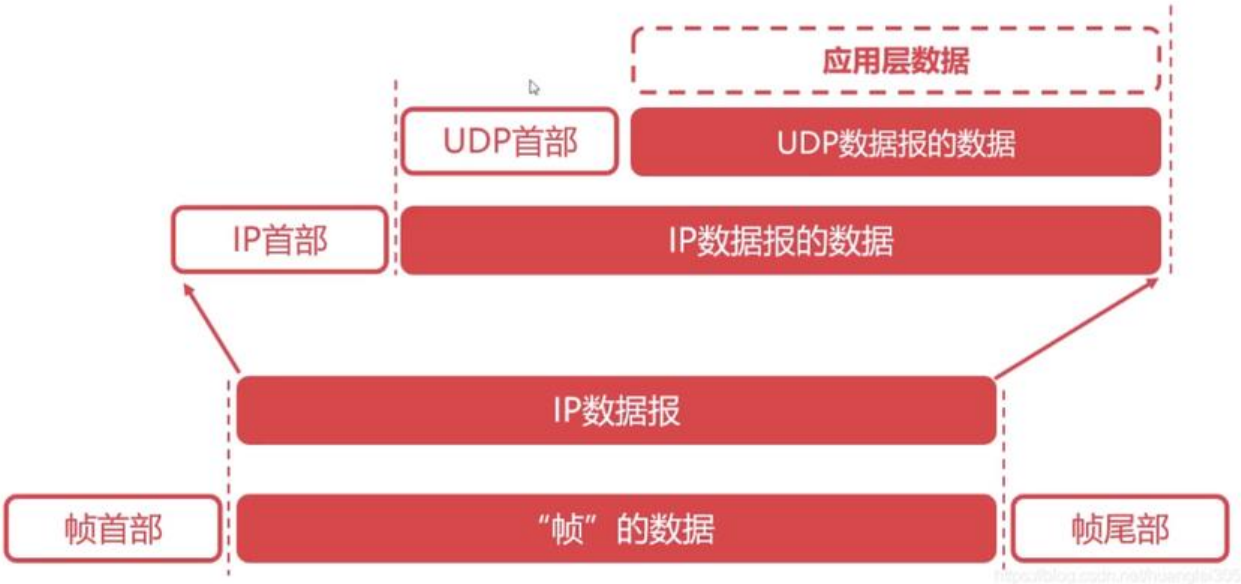
◆ 使用端口(Port)来标记不同的网络进程

◆ 端口(Port)使用16比特位表示(0~65535)

FTP	HTTP	HTTPS	DNS	TELNET
21	80	443	53	23

5.1 UDP 协议详解

UDP(User Datagram Protocol: 用户数据报协议)，是一个非常简单的协议。



UDP 协议的特点：

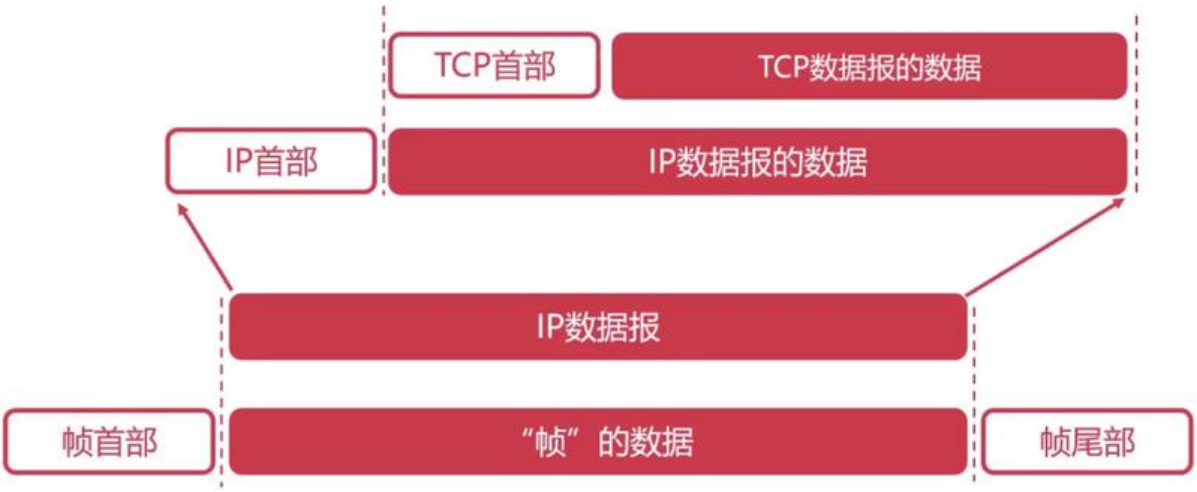
- UDP 是无连接协议；
- UDP 不能保证可靠的交付数据；
- UDP 是面向报文传输的；
- UDP 没有拥塞控制；
- UDP 首部开销很小。

UDP 数据报结构：

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

5.2 TCP 协议详解

TCP(Transmission Control Protocol: 传输控制协议)，是计算机网络中非常复杂的一个协议。



TCP 协议的功能：

- 对应用层报文进行分段和重组；
- 面向应用层实现复用与分解；
- 实现端到端的流量控制；
- 拥塞控制；
- 传输层寻址；
- 对收到的报文进行差错检测（首部和数据部分都检错）；
- 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）；

5.2.1 TCP 报文段结构：

最大报文段长度：报文段中封装的应用层数据的最大长度。

原文链接：转载：36 张图详解计算机网络知识点

TCP 首部：

- 序号字段：TCP 的序号是对每个应用层数据的每个字节进行编号
- 确认序号字段：期望从对方接收数据的字节序号，即该序号对应的字节尚未收到。用 ack_seq 标识；
- TCP 段的首部长度最短是 20B ，最长为 60 字节。但是长度必须为 4B 的整数倍

TCP 标记的作用：

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

5.3 可靠传输的基本原理

基本原理：

- 不可靠传输信道在数据传输中可能发生的情况：比特差错、乱序、重传、丢失
- 基于不可靠信道实现可靠数据传输采取的措施：

差错检测：利用编码实现数据包传输过程中的比特差错检测 确认：接收方向发送方反馈接收状态 重：发送方重新发送接收方没有正确接收的数据 序号：确保数据按序提交 计时器：解决数据丢失问题；

停止等待协议：是最简单的可靠传输协议，但是该协议对信道的利用率不高。

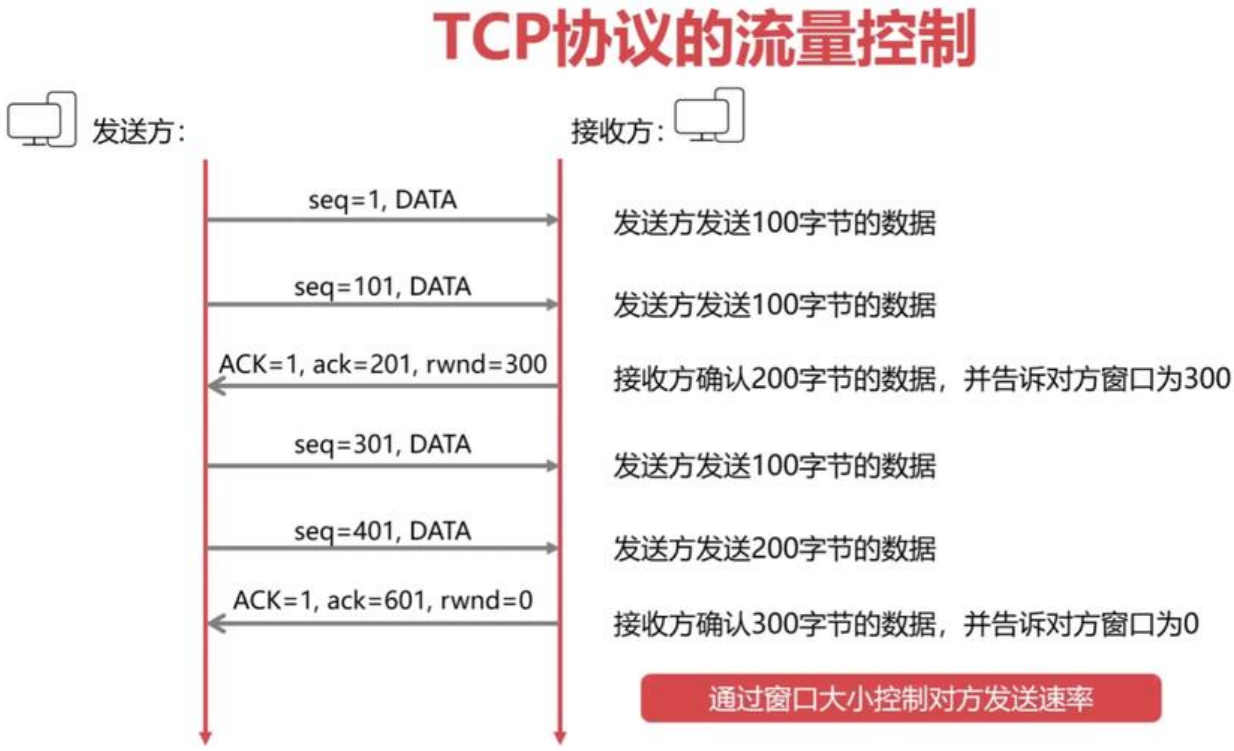
连续 ARQ(Automatic Repeat reQuest：自动重传请求) 协议：滑动窗口 + 累计确认，大幅提高了道的利用率。

5.3.1TCP 协议的可靠传输

基于连续 ARQ 协议，在某些情况下，重传的效率并不高，会重复传输部分已经成功接收的字节。

5.3.2 TCP 协议的流量控制

流量控制：让发送方发送速率不要太快，TCP 协议使用滑动窗口实现流量控制。

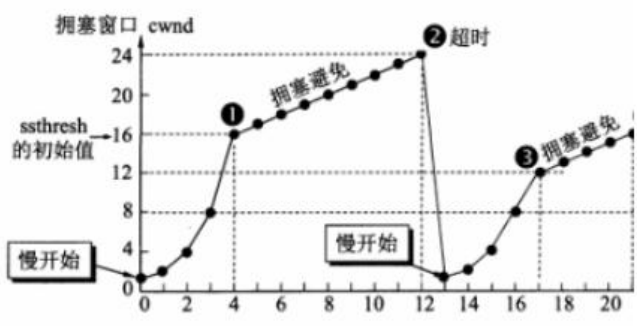


5.4 TCP 协议的拥塞控制

拥塞控制与流量控制的区别：流量控制考虑点对点的通信量的控制，而拥塞控制考虑整个网络，是全性的考虑。拥塞控制的方法：慢启动算法 + 拥塞避免算法。

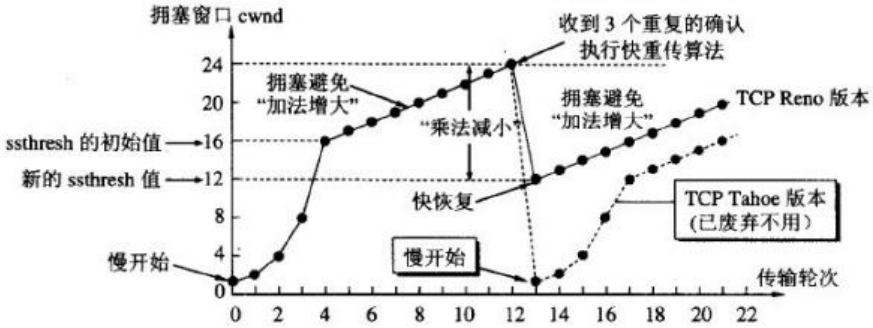
慢开始和拥塞避免：

- 【慢开始】拥塞窗口从 1 指数增长；
- 到达阈值时进入【拥塞避免】，变成 + 1 增长；
- 【超时】，阈值变为当前 cwnd 的一半（不能 < 2）；
- 再从【慢开始】，拥塞窗口从 1 指数增长。



快重传和快恢复：

- 发送方连续收到 3 个冗余 ACK，执行【快重传】，不必等计时器超时；
- 执行【快恢复】，阈值变为当前 cwnd 的一半（不能 < 2），并从此新的 ssthresh 点进入【拥塞免】。



5.5 TCP 连接的三次握手（重要）

TCP 三次握手使用指令：

TCP标记

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

面试常客：为什么需要三次握手?

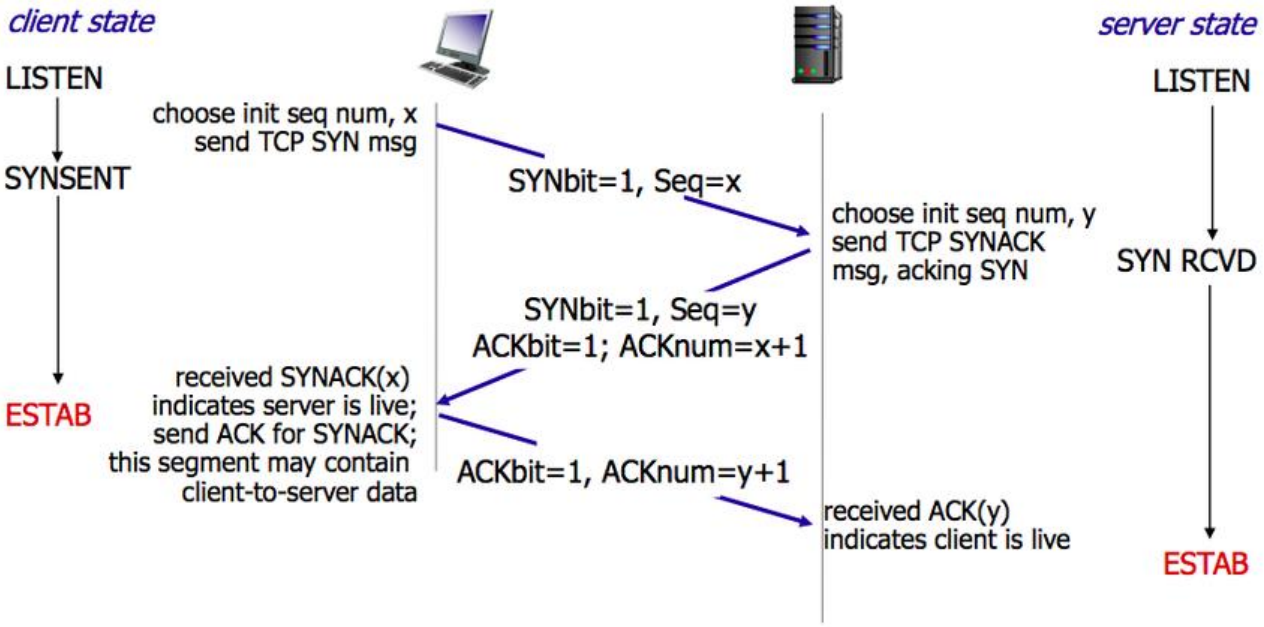
- 第一次握手：客户发送请求，此时服务器知道客户能发；
- 第二次握手：服务器发送确认，此时客户知道服务器能发能收；
- 第三次握手：客户发送确认，此时服务器知道客户能收。

建立连接（三次握手）：

第一次：客户向服务器发送连接请求段，建立连接请求控制段（SYN=1），表示传输的报文段的一个数据字节的序列号是 x，此序列号代表整个报文段的序号（seq=x）；客户端进入 SYN_SEND 同步发送状态）；

第二次：服务器发回确认报文段，同意建立新连接的确认段（SYN=1），确认序号字段有效（AC=1），服务器告诉客户端报文段序号是 y（seq=y），表示服务器已经收到客户端序号为 x 的报文段准备接受客户端序列号为 x+1 的报文段（ack_seq=x+1）；服务器由 LISTEN 进入 SYN_RCVD （步收到状态）；

第三次：客户对服务器的同一连接进行确认. 确认序号字段有效 (ACK=1), 客户此次的报文段的序号是 x+1(seq=x+1), 客户期望接受服务器序列号为 y+1 的报文段 (ack_seq=y+1); 当客户发送 ack，客户端进入 ESTABLISHED 状态; 当服务收到客户发送的 ack 后，也进入 ESTABLISHED 状态; 第次握手可携带数据;



5.6 TCP 连接的四次挥手（重要）

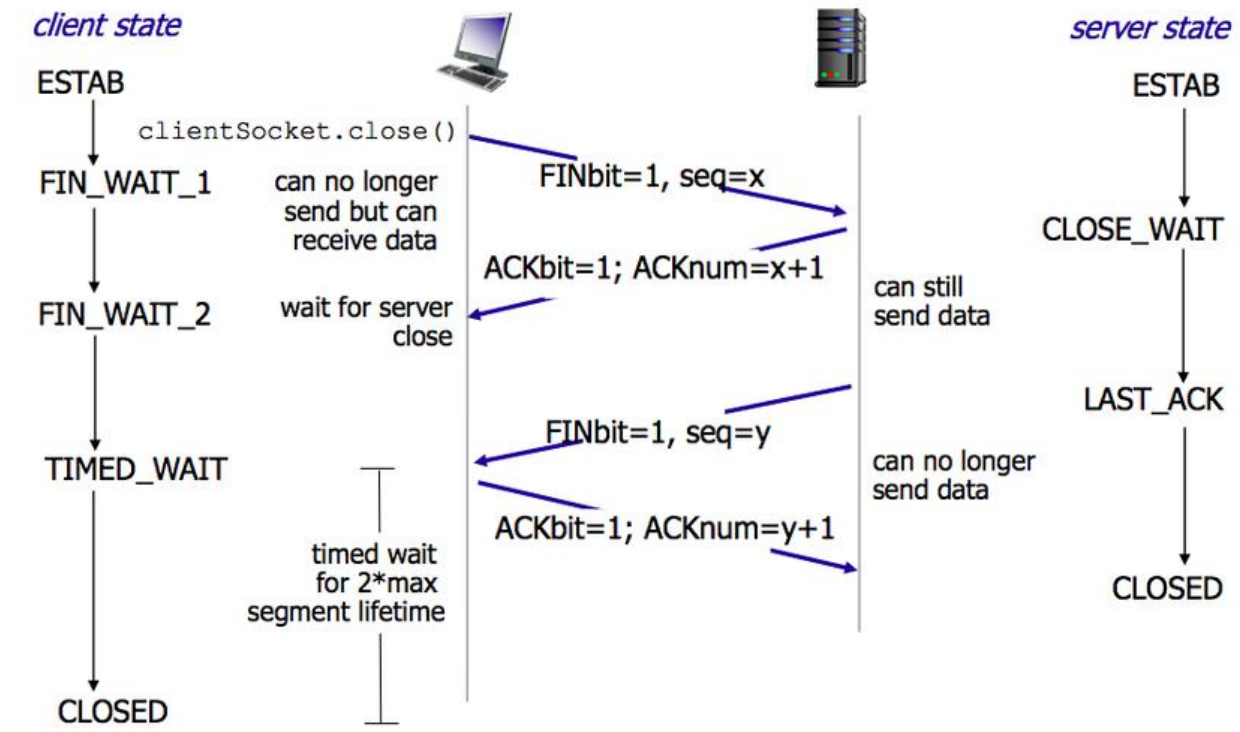
释放连接（四次挥手）

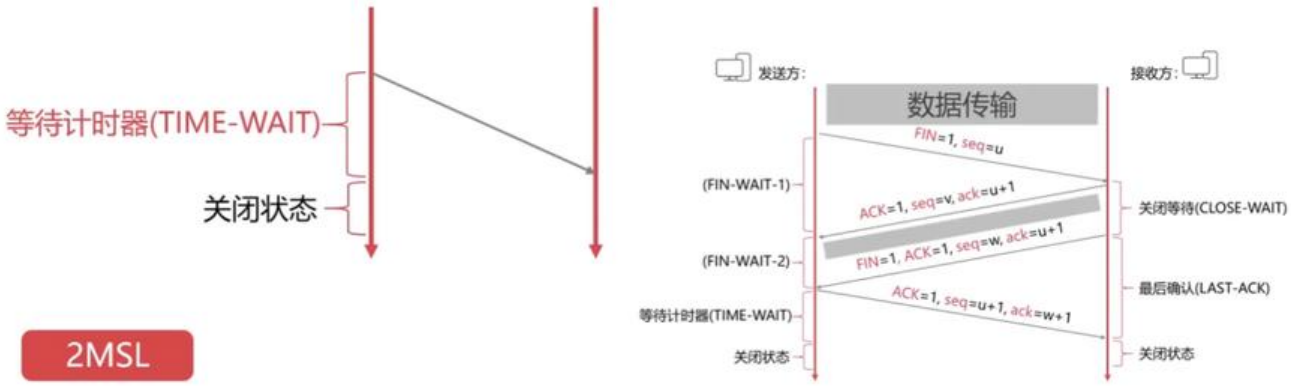
第一次：客户向服务器发送释放连接报文段，发送端数据发送完毕，请求释放连接（FIN=1），输的第一个数据字节的序号是 x（seq=x）；客户端状态由 ESTABLISHED 进入 FIN_WAIT_1（终止待 1 状态）；

第二次：服务器向客户发送确认段，确认字号段有效（ACK=1），服务器传输的数据序号是 y（sq=y），服务器期望接收客户数据序号为 x+1（ack_seq=x+1）；服务器状态由 ESTABLISHED 进入 LOSE_WAIT（关闭等待）；客户端收到 ACK 段后，由 FIN_WAIT_1 进入 FIN_WAIT_2；

第三次：服务器向客户发送释放连接报文段，请求释放连接（FIN=1），确认字号段有效（ACK=），表示服务器期望接收客户数据序号为 x+1（ack_seq=x+1）；表示自己传输的第一个字节序号是+1（seq=y+1）；服务器状态由 CLOSE_WAIT 进入 LAST_ACK （最后确认状态）；

第四次：客户向服务器发送确认段，确认字号段有效（ACK=1），表示客户传输的数据序号是 x+（seq=x+1），表示客户期望接收服务器数据序号为 y+1+1（ack_seq=y+1+1）；客户端状态由 FI_WAIT_2 进入 TIME_WAIT，等待 2MSL 时间，进入 CLOSED 状态；服务器在收到最后一次 ACK，由 LAST_ACK 进入 CLOSED；





MSL(Max Segment Lifetime): 最长报文段寿命

MSL建议设置为2分钟

为什么需要等待 2MSL?

- 最后一个报文没有确认;
- 确保发送方的 ACK 可以到达接收方;
- 2MSL 时间内没有收到，则接收方会重发;
- 确保当前连接的所有报文都已经过期。

六、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。应用层重点:

- 数据传输基本单位为报文；
- 包含的主要协议：FTP（文件传送协议）、Telnet（远程登录协议）、DNS（域名解析协议）、SMP（邮件传送协议），POP3 协议（邮局协议），HTTP 协议（Hyper Text Transfer Protocol）。

6.1 DNS 详解

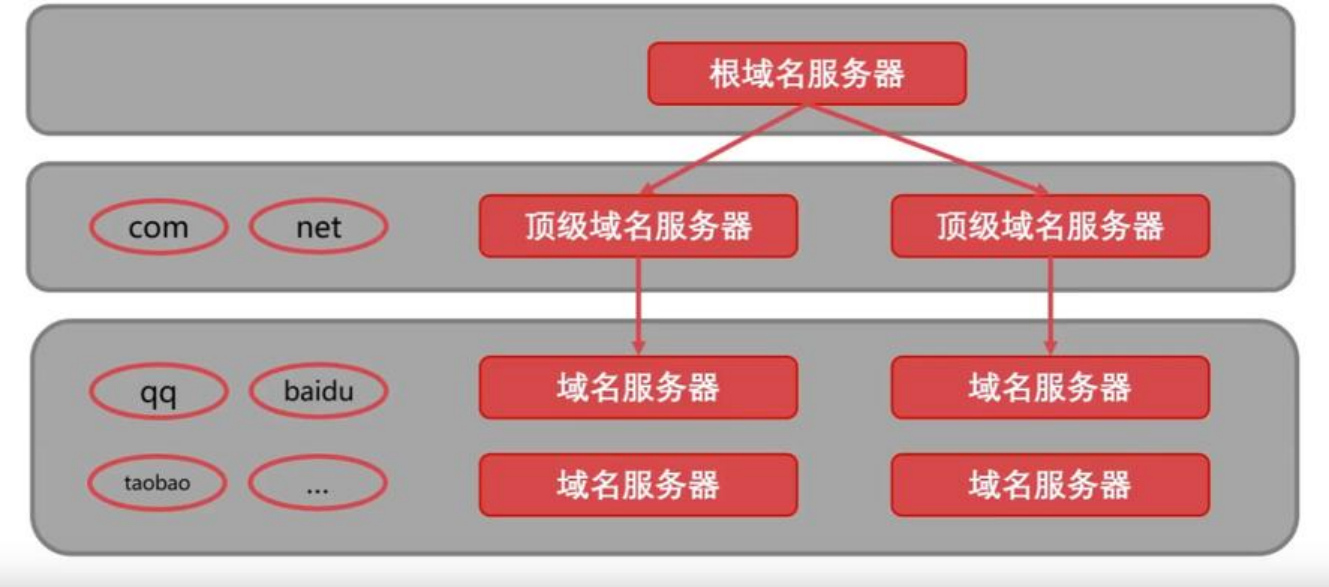
DNS（Domain Name System: 域名系统）【C/S，UDP，端口 53】：解决 IP 地址复杂难以记忆的题, 存储并完成自己所管辖范围内主机的 域名 到 IP 地址的映射。

域名解析的顺序：

- 【1】浏览器缓存，
- 【2】找本机的 hosts 文件，
- 【3】路由缓存，
- 【4】找 DNS 服务器（本地域名、顶级域名、根域名）-> 迭代解析、递归查询。

IP—>DNS 服务—> 便于记忆的域名

域名由点、字母和数字组成，分为顶级域（com，cn，net，gov，org）、二级域（baidu,taobao,qq alibaba）、三级域（www）(12-2-0852)



6.2 DHCP 协议详解

DHCP（Dynamic Configuration Protocol: 动态主机设置协议）：是一个局域网协议，是应用 UDP 协议的应用层协议。作用：为临时接入局域网的用户自动分配 IP 地址。

6.3 HTTP 协议详解

文件传输协议（FTP）：控制连接（端口 21）：传输控制信息（连接、传输请求），以 7 位 ASCII 的格式。整个会话期间一直打开。

HTTP（HyperText Transfer Protocol: 超文本传输协议）【TCP，端口 80】：是可靠的数据传输协

，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。

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

6.3.1 HTTP 工作的结构

6.3.2 HTTPS 协议详解

HTTPS(Secure) 是安全的 HTTP 协议，端口号 443。基于 HTTP 协议，通过 SSL 或 TLS 提供加密处数据、验证对方身份以及数据完整性保护。

原文链接

https://blog.csdn.net/Royalic/article/details/119985591