

数据链路层

主要作用是加强物理层传输原始比特流的功能，将物理层提供的可能出错的物理连接改造为逻辑上无差错的数据链路

✧ 封装成帧

把比特组合成帧为单位传输，是为了在出错时只重发出错的帧，而不必重发全部数据。

组帧时，既要加首部，也要加尾部。因为接受端收到的是一串比特流，，没有首部和尾部不能正确区分帧的。而IP数据包只有头部和身体

帧定界的方法：字符技术法，字符填充的首尾定界符法

✧ 透明传输

如果数据中恰好出现与帧界定符相同的比特组合，则会被误认为传输结束，透明传输就是要解决这个问题。更确切地说，透明传输就是不管所传数据是什么样的比特组合，都能在链路上传送。

✧ 流量控制

流量控制就是限制发送方的数据流量，使其发送速率不超过接收方的接受能力。

对于数据链路层来说，控制的是相邻两节点之间数据链路上的流量，而对于传输层来说，控制的是从源端到目的端之间的流量。

流量控制的基本方式是由接受方控制发送方发送数据的速率。常见的方式有两种：停等协议和滑动窗口协议。

✧ 差错控制

位错：指帧中的某些位出现了差错，通常通过CRC循环冗余校验方式发现位错，通过自动重传请求ARQ方式来重传出错的帧。

帧错：指帧的重复，丢失，失序。在数据链路层引入定时器和编号机制，能保证每一帧最终都能有且仅有一次正确地交付给目的节点。

差错控制方法：奇偶校验码，循环冗余码

✧ 可靠传输

通常使用确认和超时重传两种机制来完成，实际的有线网络的链路层很少采用可靠传输，一般都交给传输层。

✧ 介质访问控制

为使用介质的每个节点隔离来自同一信道上其他节点所传送的信号，以协调活动节点的传输。常见的方法有：信道划分介质访问控制，随机访问介质访问控制，轮询访问介质访问控制。

信道划分介质访问控制（静态划分信道）

频分多路复用 FDM

时分多路复用 TDM

波分多路复用 WDM

码分多路复用 CDM

随机访问介质访问控制（动态划分信道）

纯ALOHA协议

时隙ALOHA协议

CSMA协议（载波侦听多路访问 Carrier Sense Multiple Access）每个站点发送数据前先侦听一下共用信道

CSMA/CD协议（Collision Detection）碰撞检测。碰撞检测就是边发送边侦听

轮询访问介质访问方式（动态划分信道）

令牌传递协议：一个令牌在各节点之间以某个固定次序交换

✧ 局域网

局域网的特性主要由三个要素决定：拓扑结构（星形结构，环形结构，总线型结构），传输介质（双绞线，铜缆，光纤），介质访问控制方式（CSMA/CD，令牌总线，令牌环）。

以太网与IEEE802.3

以太网描述了物理层，数据链路层和MAC子层的实现方法

以太网采用总线形拓扑结构

MAC层使用CSMA/CD

以太网采用无连接的工作方式，不对数据帧进行编号，尽最大努力交付数据

wifi与IEEE802.11 针对无线局域网

使用星形拓扑，其中心称为接入点 AP

MAC层使用CSMA/CA

✧ 广域网

物理空间范围很广的长距离网络，需要考虑通信容量必须足够大，以便支持日益增长的通信量。

网络层

网络层向上只提供简单灵活的，无连接的，尽最大努力交付的数据包服务。

异构网络互联：互联数以百万计的网络，提供不同的寻址方案，不同的网路接入机制，不同的差错处理方法

路由选择与分组转发：不同的路由选择机制（确定某一条路径），分组转发(将IP数据包从合适的端口转发出去)

拥塞控制：在通信子网中，因出现过量的分组引起网络性能下降的现象称为拥塞，拥塞控制就是避免通信子网中的拥塞现象。是一个全局性问题，涉及网络中的所有主机，路由器及导致网络传输能力下降的所有因素。

✧ 路由算法

静态路由算法：管理员手动配置路由信息，网络发生变化后，在手动改变。

动态路由算法：距离-向量路由算法（RIP），链路状态路由算法（OSPF）。

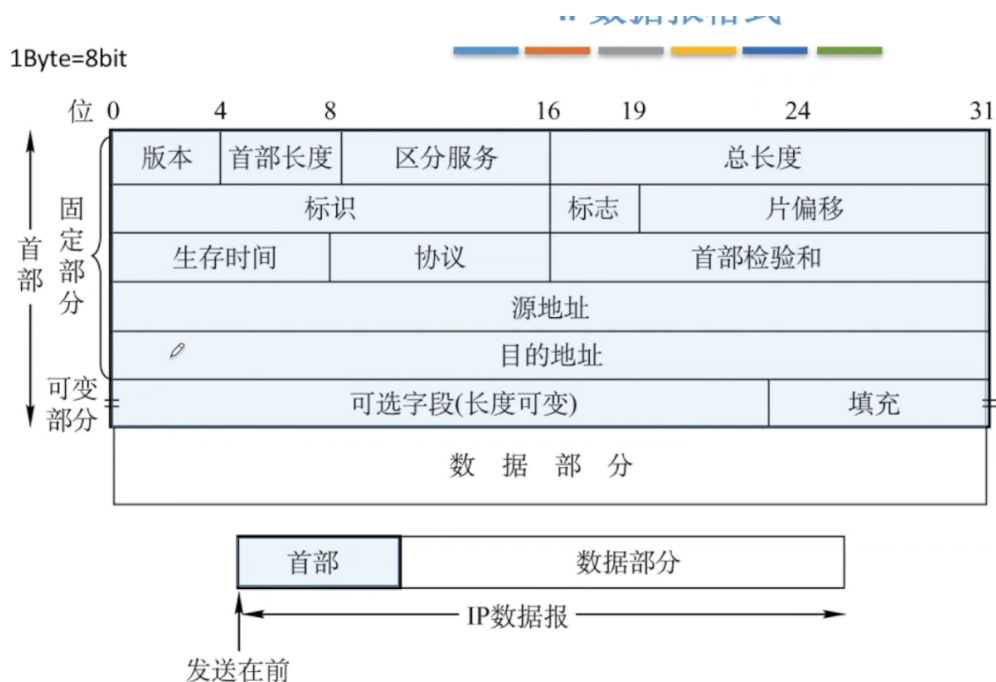
距离-向量路由算法

所有节点都定期地将它们的整个路由选择表传送给所有与之相连的节点。路由选择表包含：每条路径的目的地，路径的代价

链路状态路由算法

* IPv4

IP数据包



版本: 一般为4

首部长度: 单位为4B, 常用20B, 即不用任何可选字段

总长度: 单位为B, 最大为65535B, 但是由于MTU的限制, 达不到

生存时间: TTL 每转发一次减一, 变为0时丢弃分组

数据包分片

根据数据链路层的MTU的值进行分片, 以太网MTU=1500B

广域网MTU=576B

地址结构

网络号+主机号

分为ABCDE五类

A 1-126

B 128-192

C 192-223

D 224-039

E 240-255

主机号全为0是网络本身

主机号全为1是广播地址

127.0.0.0表示主机本身

网络地址转换

NAT Network Address Translation

将专用网络地址转换为公用地址,从而对外隐藏内部管理的IP地址,使得专用网只需要一个IP地址就能与因特网联通.大大节省了IP地址的消耗

NAT路由器工作在传输层,需查看数据包的端口号,然后进行地址转化,把私有IP:Port转化为公有IP:Port.

但是普通路由器并不改变源IP地址和目的IP地址

子网划分

二级IP地址变为三级IP地址

网络号 子网号 主机号

子网掩码

子网掩码和IP地址 AND运算 得到网络地址

CIDR

Classless Inter-Domain Routing 无类域间路由

消除传统ABC类地址以及子网划分的概念

网络前缀,主机号

斜线记法 128.14.32.5/20: 掩码为20个1,12个0

ARP协议

地址解析协议 Address Resolution Protocol

完成IP地址到MAC地址的映射

ICMP

Internet Control Message Protocol 网际控制报文协议

为了提高IP数据包的交付成功的机会,在网络层使用ICMP来让主机或路由器报告差错和异常情况.

一共有五种:

终点不可达

源点抑制

时间超过:TTL为0

参数问题

改变路由(重定向)

* IPV6

* IP组播

传输层

✧ UDP协议

User Datagram Protocol

复用 分用 差错校验

无连接,数据报首部小8B

1:1 1:m m:1 m:n

常用于一次性传输少量数据,例如DNS,DHCP;或者多媒体应用

报文格式

源端口 目的端口

长度 校验和

都是2B

校验

计算校验和时,要加上12B的伪首部

✧ TCP协议

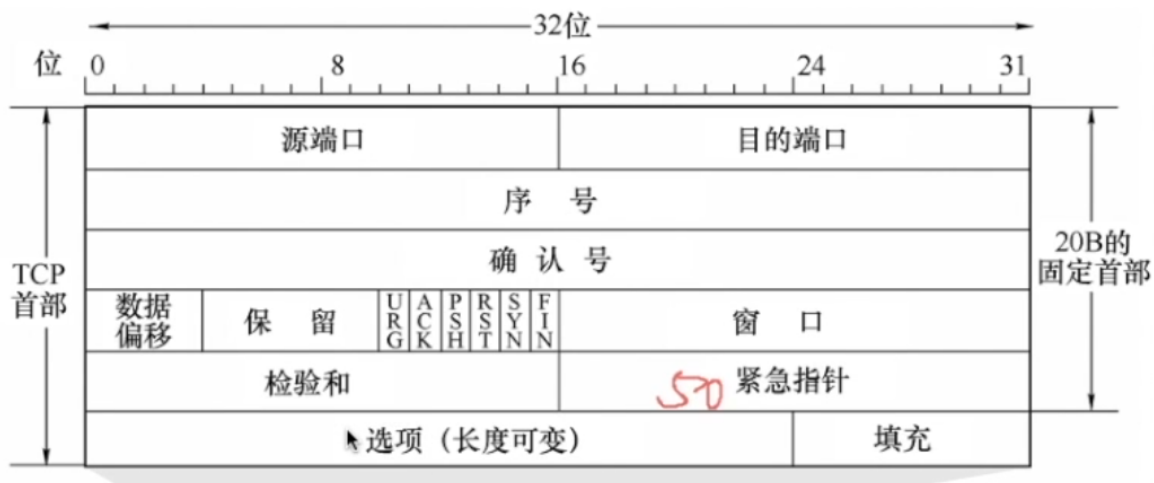
Transmission Control Protocol

不丢不重,可靠有序。

全双工点对点通信

传送字节流byte stream, 每个字节都有序号

TCP报文段



20B的固定首部，还是40B的可选长度，最大60B

2个字节的端口号

序号：本报文段所发送数据的第一个字节的序号

确认号：期望收到对方下一个报文段的第一个字节的编号。

数据偏移：即TCP首部长度，单位为4B

URG紧急位：尽快发送，不要再缓存中排队

ACK确认位：在连接建立后所有传送的报文段都必须把ACK置为1

SYN同步位：表明是一个连接请求/连接接受报文

FIN终止位：发送方数据已发完，要求释放连接

TCP连接

连接建立，数据传送，连接释放

三次握手 建立TCP连接

客户端的TCP首先向服务器发送连接建立请求报文段，其中SYN=1，同时假设初始序号seq=x。

然后，服务器的TCP收到连接后，如果同意建立连接，则向客户端发送确认，并为该TCP连接分配缓存和变量，在确认报文段中，SYN=1，ACK=1，确认号ack=x+1，seq=y，这些链接报文本身不携带数据，但要消耗一个序号。

最后，客户端收到确认报文后，还要向服务器给出确认，并为该TCP连接分配缓存和变量， $ACK=y$ ，序号为 $seq=x+1$ ，确认号 $ack=y+1$

四次挥手 释放TCP连接

可靠传输

TCP在不可靠，尽最大努力交付的IP层的基础上建立一种可靠的数据传输服务。

校验

序号 给字节流的每个字节都编序号

确认 使用报文中的确认号来进行确认；发送缓存区会存储那些已发送却没有收到确认的报文段，以便需要时重传。

重传：1.超时：每个报文段都有一个计时器，计时器为0还没收到确认就重传，计时器的值一般为一个平均RTT。2.冗余ACK：超时重传周期太长，对于失序的报文段，会发送冗余的ACK说明自己期待的报文段序号，

流量控制

端到端的流量控制，使用滑动窗口机制，并且滑动窗口大小可以变化，而数据链路层的滑动窗口不可以。

拥塞控制

防止过多的数据注入网络，保证网络中的路由器和链路不过载

慢开始(发送窗口刚开始很小,然后指数增大)和拥塞避免(达到一定阈值后,cwnd缓慢增大,一次加一,线性增长,发生超时重传后,就减为1)

快重传(冗余ACK)和快恢复(拥塞时,发送窗口减半,而不是减为1)

应用层

DNS

Domain Name System

域名系统

使用UDP数据报

主机向本地域名服务器进行查询,如果查询不到,则本地域名服务器可以:

递归查询,迭代查询

DHCP

基于UDP

给主机动态分配IP地址

FTP

SMTP

HTTP
