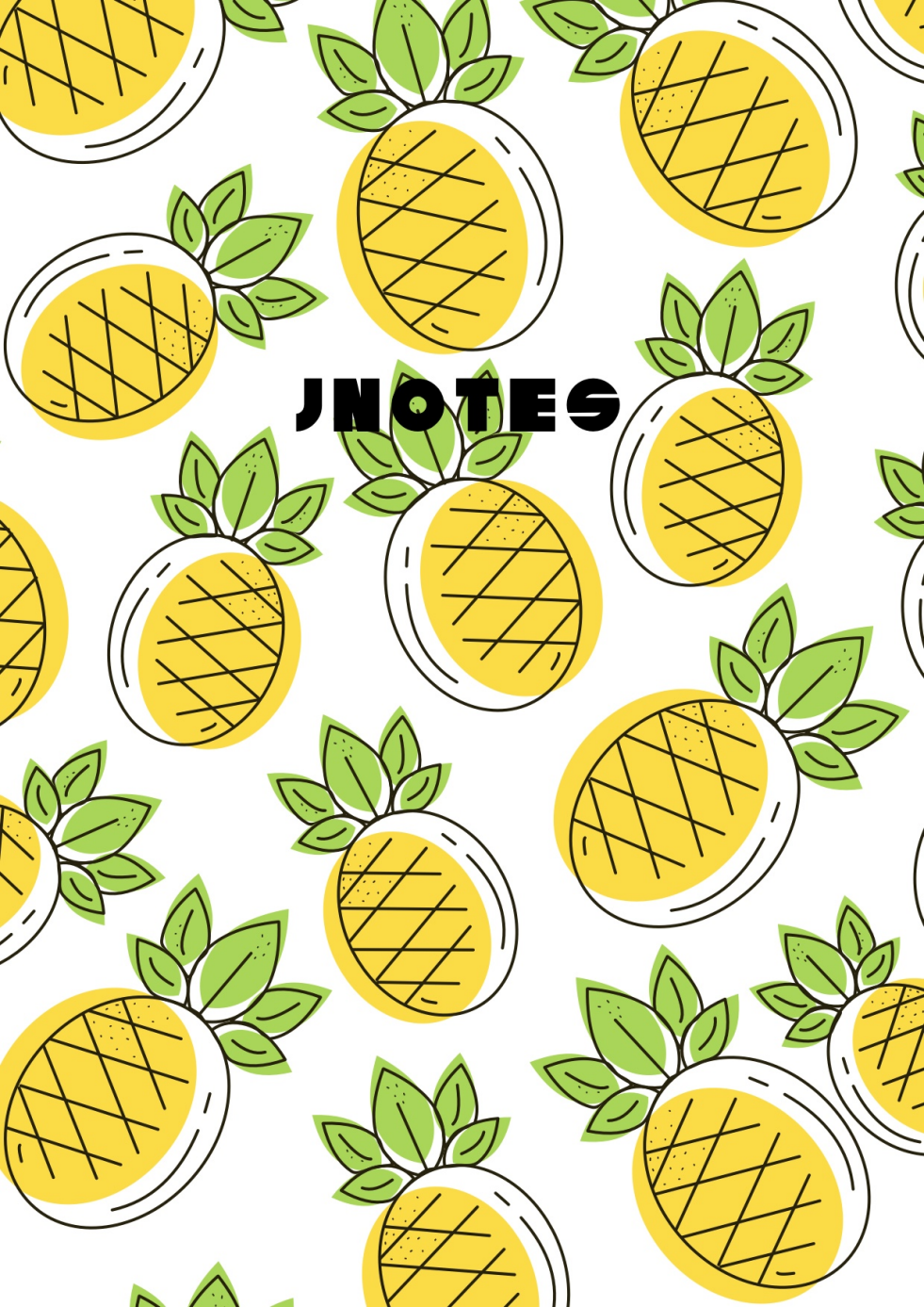

JNOTES

日期: /

计算机网络的分类:

1. 按分布范围分:

广域网(WAN)、城域网(MAN) → 企业、公网 数据链路层/交换机

局域网(LAN) 物理层/集线器

（广域网：存储交换机（分组交换技术） 网络层/路由器）

2. 传输技术分:

① 广播式网络 ② 点对点网络

3. 传输介质分:

① 有线网络 ② 无线网络

（有线网络 → 双绞线、同轴电缆、光纤）

4. 不同的拓扑结构:

① 星形 ② 树形 ③ 总线形 ④ 环形 ⑤ 网格形

（星形 → 交换机/集线器为中心，现今以太网物理星型）

5、服务对象分类:

① 公用网 ② 专用网

日期: /

计算机网络的性能指标.

1. 速率 单位时间内传送的数据量 手动理解能支持的最大比特率.

2. 带宽

① 通信: 频带宽度 (Hz)

② 计算机: 计算机网络的通信线路所能传送数据的能力. "最高数据率" (b/s)

3. 吞吐量: 实际到达的传输速率 (bps)

4. 时延: 数据从网络的一端传到另一端所需的时间. 由四个部分组成.

$D = d_{proc} + d_q + d_{trans} + d_{prop}$

处理~ 排队~

发送时延: $d_{trans} = \frac{L}{R}$ = 发送的数据量 / 信道带宽

传播时延: $d_{prop} = \frac{d}{v}$ = 信道长度 / 电磁波在信道上的传播速率

自由空间 3×10^8 m/s

铜线 2.3×10^8 m/s

光纤 2×10^8 m/s

往返时延: RTT. = 相当于传播时延的两倍 (重要概念)

$RTT = 2 \cdot d_{prop}$

5. 时延带宽积 = $d_{prop} \times$ 带宽 (链路中可容纳的比特数, 以b为单位的链路长度)

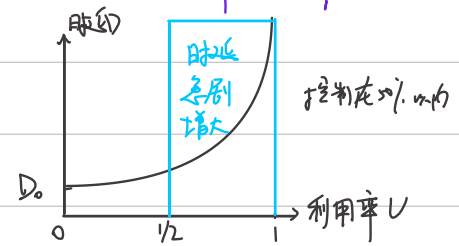
6. 利用率: 信道利用率 / 网络利用率. → 全网络的信道利用率加权平均

用于传输的时间比例

$D = \frac{D_0}{1-U}$

D_0: 网络空闲的时延 U: 数值在0到1之间

D: 网络当前的时延



日期:　　/

计算机网络的体系结构和模型

1)交换传送模块　2)通信服务模块　3)网络接入模块

协议明确：1) 数据的格式　2)同步问题

三要素：①语法　②语义　③同步

OSI模型		TCP/IP参考模型	
(7)应用层	用户服务平台	(4)应用层	应用程序
(6)表示层			
(5)会话层			
(4)传输层		(3)传输层	端对端
3)网络层		(2)互联网层	路由选择
2)数据链路层	网络服务平台	(1)网络接入层	端系统 与通信子网
1)物理层			

客户/服务器模式(C/S)：非对等作用和异步通信

客户 → 请求（主动请求）

服务器 → 提供服务

日期: /

面向连接服务和无连接服务

两个对等实体为进行通信而进行的一种约定

→折中：五层模型 应用层、传输层、网络层、数据链路层、物理层

一、OSI 七层模型总览表

层次	名称	主要功能	典型设备/协议	传输单位（PDU）
第7层	**应用层 (Application Layer)**	向用户直接提供网络服务，定义应用进程间通信方式，如文件传输、电子邮件、网页访问等。	HTTP、HTTPS、FTP、SMTP、POP3、DNS、DHCP、Telnet 等	数据（Data）或 消息（Message）
第6层	**表示层 (Presentation Layer)**	数据的表示、编码、压缩、加密/解密；确保不同系统间的表示一致。	JPEG、ASCII、SSL/TLS、MIME、加密协议	数据（Data）
第5层	**会话层 (Session Layer)**	管理通信会话，建立、维护、终止对话；提供同步、检查点、恢复。	RPC、NetBIOS、SQL 会话	数据（Data）
第4层	**传输层 (Transport Layer)**	提供端到端的进程通信：实现可靠传输、流量控制、差错控制；可面向连接（TCP）或无连接（UDP）。	**TCP、UDP**	段（Segment）（TCP）/ 数据报（Datagram）（UDP）
第3层	**网络层 (Network Layer)**	逻辑寻址与路由选择：负责数据包在不同网络间的转发与分片。	**IP（IPv4/IPv6）、ICMP、ARP、RIP、OSPF、BGP**、路由器	包（Packet）或 分组（Datagram）
第2层	**数据链路层 (Data Link Layer)**	在相邻节点之间提供**可靠帧传输**：成帧、差错检测、流量控制、介质访问控制（MAC）	以太网、**PPP、HDLC**、帧中继、**VLAN(802.1Q)**、交换机、桥接器	帧（Frame）
第1层	**物理层 (Physical Layer)**	负责比特的物理传输；定义电气特性、机械特性、信号、接口。	网线、光纤、集线器、调制解调器、收发器	比特（Bit）

(CSMA/CD)

一、TCP/IP 模型的基本结构

TCP/IP（Internet）体系结构是互联网的实际标准架构，通常分为 **四层**（有时也称"五层"，取决于教材是否把物理层单独列出）：

TCP/IP 层次	对应 OSI 层	主要功能	典型协议	传输单位（PDU）
应用层 (Application Layer)	OSI 第5–7层（会话层、表示层、应用层）	提供应用服务接口；实现进程间通信，如网页、邮件、文件传输等。	HTTP、HTTPS、DNS、FTP、SMTP、POP3、IMAP、Telnet、SSH、DHCP、SNMP	**数据 (Data)**
传输层 (Transport Layer)	OSI 第4层	提供端到端的可靠或不可靠通信；差错检测、流量控制、分段与重组。	**TCP、UDP、SCTP**	**段（Segment）或报文（Datagram）**
网络层 / 网际层 (Internet Layer)	OSI 第3层	提供逻辑寻址与路由选择，实现分组的转发与互联。	**IP（IPv4/IPv6）、ICMP、ARP、RARP、IGMP**	包（Packet）
网络接口层 (Network Access / Link Layer)	OSI 第1–2层	负责物理传输、帧封装、差错检测，与具体硬件接口；连接到实际链路。	以太网、Wi-Fi、**PPP、HDLC、ATM**、光纤信道	帧（Frame）/比特（Bit）

日期: /

传输方式:

1. 基带传输和频带传输. (是否搬移其频谱) →调制
   目的:适应信道频率特性.

2. 串行传输和并行传输. (按照其时空顺序)
   - 串行 → 依次,远距离,收发同步
   - 并行 → 同时,传输速度快,短距离

3. 异步传输和同步传输. (按照收发端实现同步的方式)
   - 异步 → 每个字符独立,靠起始位和停止位
   - 同步 → 时钟同步信号

4. 单工.半双工和全双工 (传送方向与时间)
   - 单工 → 一个指定方向
   - 半双工 → 两个方向但不能同时进行
   - 全双工 → 两个方向且同时进行

物理层: 在具体的物理媒体上提供"透明传输比特流的能力"

4个重要特性: 机械特性.电气特性.功能特性.规程特性

类型	英文名称	说明
1. 机械特性 (Mechanical Characteristics)	定义物理连接接口的形状、尺寸、引脚数、排列方式等机械结构。	👉 举例: RJ-45 网线接口有 8 个针脚; USB 插头、光纤接头的形状规格等。
2. 电气特性 (Electrical Characteristics)	规定信号电压、电流、阻抗、传输速率、信号电平等参数。	👉 举例: 逻辑"1"对应 +5V、"0"对应 0V; EIA RS-232C 接口定义了电压范围。
3. 功能特性 (Functional Characteristics)	说明各个信号线的用途以及各引脚在何种条件下承载何种信号。	👉 举例: 在串口通信中, TXD 为发送、RXD 为接收、RTS/CTS 用于流控。
4. 规程特性 (Procedural Characteristics)	规定不同功能线之间的工作时序与过程, 即信号交换的规则。	👉 举例: 发送端先置"请求发送"(RTS), 接收端应答"允许发送"(CTS), 之后才开始传输数据。

日期: /

数据链路层：同一链路之间提供可靠的数据传输服务

三个基本问题：①封装成帧 ②透明传输 ③差错检测

1. 封装成帧：在一段数据的前后分别添加首部和尾部构成一个帧

1) 字节填充法

使用一个特殊的字节来标志帧的开始和结束，称为帧首定界符

ESC 转义符

SOH、EOT（Start/end）

| DLE | STX | 数据 | DLE | ETX |

2) 比特填充法（常用）

使用一个特定的比特模式作为帧的起止标志，如：

标志（Flag）：01111110

总界，| Flag | 数据 | FCS | Flag |

在发送端检测出连续 5 个 "1" 时，自动插入一个 "0"（比特填充）

3) 字节计数法

在帧首部添加一个"长度字段"，指出该帧所含字节数（包括首部数据）

| 字节计数字段 | 数据（n字节） |

|←表示帧总长度→|

日期: /

2. 透明传输.

无论帧面数据部分中包含何种比特组合，接收方都能正确识别帧开始和结束，即不将任何比特误认为是控制信息

3. 差错检测

1) 奇偶校验法，添加一位校验位 (只能检测出奇数个比特错误)

偶校验：整个码组中(包括校验位)1的个数为偶数

奇 奇.

例：数据：1010001 (3个1 奇数)

偶校验：① → 10100011 (发送码)

奇 ：⓪ → 10100010 (发送码)

2) CRC 循环冗余校验

数据多项式：M(x)

生成 ~ ：G(x) (最高次为r)

余数 ~ ：R(x)

① M(x)补r个0 得到M'(x)

② G(x)与M'(x)模二除(异或)

③ 余数即为 CRC 校验码 R(x)

④ 发送码 = 原数据 + 余数

例：数据：1011 $G(x)=x^3+x^2+1$ = 1101

① 10111000

② 模二除(异或)

```
      1100
1101 / 10111000
       1101
       ----
       1100
       1101
       ----
        100   R(x)
```

发送码 = 10111000

日期: /

以太网:

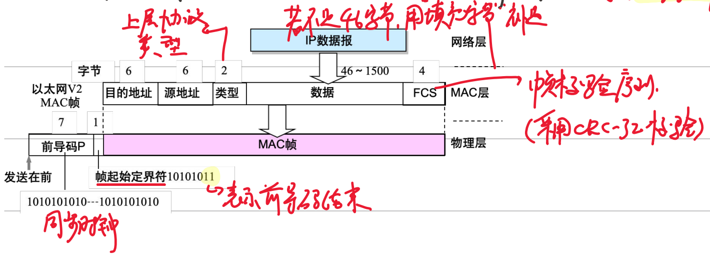
物理拓扑: 总线型

10 BASE-T

- 10 → 传输速率: 10Mb/s
- BASE → 基带传输
- T → 双绞线

有差错的帧 → 直接丢弃

以太网帧格式(MAC帧格式): 5个字段 (最少64字节)　64B　数据字段: ≥46B



无效的MAC帧: ① 帧的长度不是整数个字节 ② FCS检验出差错的帧
③ 数据字段长度不在46~1500字节之间

以太网采用的介质访问控制方式 → 多站点共享一个信道

CSMA/CD 载波监听多点接入/碰撞检测 → 边发送数据边检测总线上是否有碰撞的情况

发送前"监听": 若检测到其他节点正在发送,则等待信道空闲

概括: 先听后发,边发边听,冲突停止,随机延迟后重发。

端到端的往返时延 2τ 争用期　10Mb/s　512bit(64B) 最短有效帧长

重发帧所需时延: 截断二进制指数退避算法

日期: /

以太网标准命名格式:

<速率, BASE <传输介质或距离>

速率: Mbps 基带传输

例: 10BASE 5 10Mbps. 基带传输. 最大电缆长度为500米

② 1BASE 5 1Mbps ---

③ 10BASE-T 双绞线

局域网组成主要取决于 拓扑结构、传输媒体 信道访问控制方式

高速以太网 >10Mb/s

双绞线使用 RJ-45 水晶头. 长度不超过 100m

奈奎斯特定理（Nyquist） vs 香农定理（Shannon）对比表

项目	奈奎斯特定理（Nyquist Theorem）	香农定理（Shannon Theorem）
研究背景	理想**无噪声信道**，研究码元速率与带宽的关系	**有噪声信道**（高斯白噪声），研究信噪比与最大传输速率的关系
核心问题	在无噪声条件下，不产生码间串扰时的**最大数据传输速率**是多少?	在有噪声条件下，能**无差错传输信息**的最大理论速率是多少?
数学公式	$C = 2W \log_2 M$	$C = W \log_2(1 + \mathrm{SNR})$
参数含义	W：信道带宽（Hz） M：信号电平数（每码元状态数）	W：信道带宽（Hz） $\mathrm{SNR} = \frac{S}{N}$：信噪比（线性值）
假设条件	理想无噪声，仅受带宽与码间串扰限制	存在高斯白噪声（有噪声信道）
速率单位	比特每秒（bit/s）	比特每秒（bit/s）

日期: /

随机退后

k× 争用时 $k \in [0, 2^n - 1]$ n为第n次重生（最大n=10）

超过16次冲突→发送失败

CSMA/CD 适用场景：

10/10Base-5. 10Base-2. 10Base-T（半双工）

② 共享式集线器（HUB）局域网

③ 现代以太网（全双工）不再使用

集线器与交换机（扩展以太网）

HUB（物理层）　Switch（数据链路层）

对比项	集线器（Hub）	交换机（Switch）
工作原理	接收到信号后**放大再生**，并广播到所有端口	根据 **MAC 地址表**，**定向转发帧**
识别能力	不识别 MAC 地址，只看比特信号	能识别 MAC 地址，学习并维护 MAC 表
数据转发方式	广播（所有端口都收到）	单播（只发给目标端口）
冲突域	所有端口共享一个冲突域	每个端口独立一个冲突域
广播域	所有端口同属一个广播域	默认同一广播域（可通过 VLAN 划分）
全/半双工	仅支持 **半双工**	支持 **全双工**
传输速率	通常 10 Mb/s	10/100/1000 Mb/s 甚至更高
性能	冲突多，效率低	并行传输，效率高
智能性	无智能（纯信号中继）	具备帧缓存、学习与转发决策功能
典型应用	小型局域网、老式网络	现代局域网的核心设备

日期: /

二层交换机转发表自学习方法：学习 → 查找 → 转发 → 广播 → 老化。

MAC表

哪个主机连接在二层交换机的哪个端口上

<MAC地址，端口号，VLAN号，时间戳>

① 检查源 MAC 地址　不存在 → 新建条目
存在但不同 → 更新
同则更新时间戳

② 查找目的 MAC 地址：匹配 → 定向转发
不匹配 → 广播

③ 老化机制：（300s）未收到来自该源的帧，则删除条目

二层交换：点对点转发。

VLAN：Virtual LAN（虚拟局域网）

在二层交换机上逻辑划分多个广播域，不同的 VLAN 默认隔离，通过设备实现

主要用于划分广播域，提高网络安全性和管理效率

无线局域网的介质访问控制方法

CSMA/CA 协议（针对无线网络）

不能边发边听，所以不能冲突检测（CD）

→ 用 "CA" 避免冲突代替 CD

先听后发，先等随机时间再发，尽量避免冲突

日期: /

隐藏站：听不到 → 造成冲突　　Request/clear to send.

A－B－C

A后B发，C也想向B发。
因为C听不到A，则在B处冲突

解决方法：RTS/CTS握手机制
A发送的报文，先发送RTS，B回复CTS。
C听见CTS，则知道被占用，暂不发。

暴露站：听到一个以为忙

A－B－C－D

B听见AC
C听见BD

A听不到C　B听不到D

B向A发　C听到B的话，以为忙。
其实C向D发不会影响A。

RTS/CTS 握手机制

网络层：

网络层协议：

① IP协议：核心协议

② ICMP：网际控制报文协议：报告IP层错误，传递诊断信息　拥塞控制
1) ping：利用ICMP回送请求/应答检测连通性
2) tracert：利用了ICMP返回报文跟踪路径。

③ ARP：将IP地址 → MAC地址

④ RARP：将MAC地址 → IP地址

⑤ IGMP：网际组管理协议，用于管理主机加入/离开组播组

日期: /

网际协议 IPv4：

IPv4（Internet Protocol version 4） 是网络层的主要协议，负责实现**主机到主机的逻辑通信**。
它定义了 IP 地址格式、数据报格式以及分组转发机制，是整个 Internet 的基础。

📘 核心特征：

特性	说明
无连接（connectionless）	每个 IP 数据报独立传输，不建立连接
不可靠（unreliable）	不保证交付、顺序、无丢失（由 TCP 保证）
面向数据报（datagram）	每个分组独立路由
尽力而为（best-effort）	尽最大可能送达，但不保证成功

分类IP地址

IP地址定义为：{<网络号>, <主机号>}

A类 0 8比, 24bit　0~127　2^7-1

B类 10 16bit　16比　128~191　$2^{14}-1$

C类 110 24比　8比　192~223　IP地址表示方法：点分十进制 $2^{21}-1$

D类 1110 多播地址　224~239

E类 1111 保留为今后使用.　240~255

	有效网络数	可用主机数
	除全0.和回环127	除全0.全1
A类	-2	-2
其他	-1	-2

特别的IP地址：

网络号全0：本网络　全1：广播

网络号和主机号全1：对本网络进行广播

A类地址后127 用作回环测试

主机号全1：对本网络号的所有主机进行广播

日期: /

划分子网：<网络号，子网号，主机号>

子网掩码：用于区分IP地址中的网络部分和主机部分

网络号为1　主机为0

表示法：点分十进制.网络前缀(或斜线记法、记法)

(IP地址) AND (子网掩码) = 网络地址

默认子网掩码：

		网络前缀
A类：	255.0.0.0	/8
B类：	255.255.0.0	/16
C类：	255.255.255.0	/24

例：子网数：2^n-2 (n为借用的主机位数)

主机数：$2^{(32-n)}-2$ (n为子网掩码中'1'的个数)

IP：192.168.1.0/26 → 掩码 255.255.255.192

11 00 0000

子网号　主机号

子网数：$2^{(26-24)}-2=2$

主机数：$2^{(32-26)}-2=62$

变长子网划分(二叉树)

日期 /

目标主机

(逻辑地址)

实际传输(物理地址)

IP地址与MAC地址

三、MAC 地址 与 IP 地址的区别与关系

对比项目	MAC 地址	IP 地址
作用层次	数据链路层（物理标识）	网络层（逻辑标识）
长度	48 位（6 字节）	32 位
格式	十六进制（如 00-1A-2B-3C-4D-5E）	点分十进制（如 192.168.1.1）
分配方式	固化在网卡中，由厂家分配	由网络管理员或 DHCP 动态分配
是否可更改	一般不可（但可伪造）	可更改
作用范围	局域网内通信	端到端通信
对应关系	通过 **ARP 协议** 建立 IP→MAC 映射	

IP数据报的格式：首部+数据.

版本 — 4位 IP协议的版本.
- 0100 IPv4
- 0110 IPv6

首部长度 — 4位. 最大为60字节. 不是4字节的整数倍. 利用填充字段补齐

15个单位(4B/单位)

区分服务：8位. 前三位是优先级(0~7, 0最低)

D.T.R.C 有选择.

总长度：16位. 整个数据报长度. 最大64KB

不超过数据链路层最大传送单元(MTU)

超过则需分片

标志位(3位)：只有后两位有意义.

最低位MF (More~)	MF=0	后面无分片
	MF=1	有
次低位DF (Don't~)	DF=0	允许分片
	DF=1	不允许分片.

标识：同一数据报的所有分片有同样的标识

片偏移 — 13位：表示分片在原数据报中的位置 (以8字节为单位)

无分类编址. 可实现构造超网(路由聚合)

无分类域间路由选择 CIDR：IP地址 ::= {<网络前缀>, <主机号>}

例：136.48.32.8/20 表示前20位是网络地址

日期: /

ARP协议：将IP地址转换成MAC地址。（同一个局域网）

二、ARP 的工作原理（过程）

下面以主机 A 要与主机 B 通信为例：

1. 主机 A 知道目标主机 B 的 IP 地址（例如 192.168.1.2），但不知道它的 MAC 地址。
2. A 检查本地的 ARP 缓存表（ARP Cache），看是否已有对应记录。
   - 若有，则直接使用；
   - 若无，则执行下一步。
3. A 发送一条 ARP 请求广播帧，内容包括：

```
谁是 192.168.1.2？请告诉我你的 MAC 地址。
```

4. 局域网中所有主机都收到该广播请求，但只有 IP 地址为 192.168.1.2 的主机 B 会回复：

```
我是 192.168.1.2，我的 MAC 地址是 00-16-EA-12-34-56。
```

这是一条 ARP 响应（单播）帧。

5. A 收到响应后，将映射关系（192.168.1.2 → 00-16-EA-12-34-56）缓存到本地 ARP 表，以便下次直接使用。

请求：广播

应答：单播

网络地址（NAT）：将私有IP地址转换公网IP地址

IP层的分组转发机制：

网络层的基本功能：选路与转发

IP层负责：① 无连接的数据报传输服务 ② 分组选路与转发 ③ 分片与重组。

（数据在路由器内部加行为）

转发过程的步骤：（逐此转发）

（路径选择）

① 接收分组

② 提取目的IP地址（从头部读取目的地址字段）

③ 查路由表：寻找"最匹配"项目

④ 确定转发接口

⑤ 封装并转发

转发匹配规则——"最长前缀匹配"

选择网络前缀最长的（=又长又亲）

日期: /

用UDP

RIP协议：基于距离向量算法的动态路由协议

用于局域网或小型网络，帮助自动创建和更新路由表

↓ 到每个目的网络的跳数

对应的下一跳路由器

（每隔30s） 若180s未收到，认为该路由失效

定期广播自己的路由表给相邻路由器

报文有：①所有跳数加1 ②比较是否找到"更短的路径" ③多次广播直至全网收敛

度量：跳数。每经过一个路由器，跳数+1。最大为15，大于15视为不可达。

特点：好消息传播快，坏消息传播慢 → 路由环路问题

（但不说明RIP报文出错）

RIP的报文格式：命令字+多条路由项

首部占4个字节，每条路由项占20个字节，最多可包含25个路由项

一个RIP报文最大长度为 4+20×25=504 字节

日期: /

ICMP
- 差错报告报文
  - 终点不可达
  - 源点抑制
  - 超时
  - 重定向
- 询问报文
  - 回送请求回答（查看目的主机是否可达 ping命令）
  - 时间戳请求回答（跟踪路由 tracert）
    TTL=1 ↗

IPv6:

与IPv4区别
- ① 取消首部长度，固定为40字节
- ② 去除分片
- ③ 取消检验和

地址：16B 128位 ⟹ 零压缩，连续的0写成"::"

如何兼容：① 双协议栈 ② 隧道 ③ 首部转换

路由算法

① 和谁交换信息 ② 何时～ ③ 交换什么信息

RIP: ① 和相邻路由器交换 ② 定期 ③ 自身完整路由表 → （网络，跳数，下一跳）

更新：未出现的网络 / 出现过的网络：① 代价小 ② 对于同一个Net，同一个下一跳 要更新

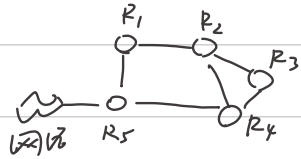
特点："好消息传得快，坏消息传得慢"

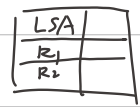
OSPF: ① "洪泛" 与网络里所有路由器交换 ② 链路状态发生改变

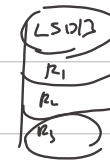
③ 交换链路状态（LS） 与哪些路由器相邻，相邻代价

日期: /

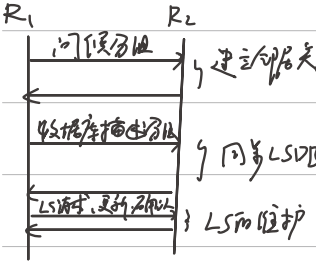
OSPF：流程：



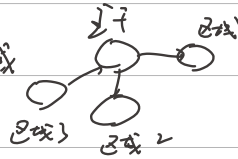




收敛，通过dijkstra算法找最短路径



细节：① 自主划分区域

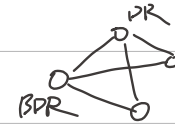


泛洪范围减小

② DR、BDR

泛洪次数减少

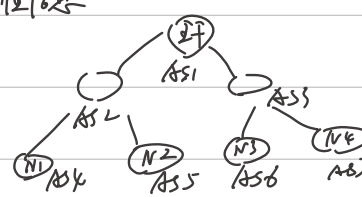
指定路由器、备选指定路由器



BGP：① 和BGP发言人交换信息

② 当网络信息发生变化时候，仅仅发生变化的那部分（增量更新）

③ 交换的是可达性信息



日期: /

BGP报文类型
- 打开报文 — 发送人 到建立关系 open
- 更新报文 — 发布/撤销 可达性信息 update
- 保活报文 — 确保连接 keepalive
- 通知报文 — 检测到差错 - 方要在关闭会话 notification

总结:

	RIP	OSPF	BGP
交换内容	完整路由表	相邻各路路状态	修改过的可达性信息
~对象	相邻路由器	所有路由器	BGP相邻发言人
~时机	(30s)定期	LS状态发生变化	网络发生变化
~方式	广播	洪泛	BGP会话
协议	UDP(应用层)	IP(网络层)	TCP(传输层)

IP组播(只可以用作目的地址,不能作为源地址)

单播  广播  组播 

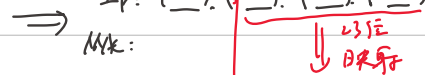
地址: D类 1110开头 224.0.0.0 ~ 239.255.255.255

工作协议: ① 只在本网络有意义 ② 何时发送: 有新主机加入/退出/更新.

IPv4 单播: ARP

IPv4 组播: 多播IP → 以太网多播MAC(因为规则)

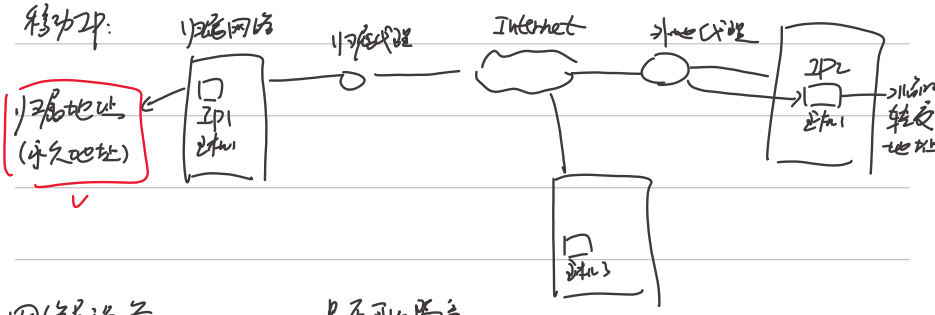
映射到MAC地址 ⟹ IP:  (32位)

MAC: 

第4个字节最高位固定为0。

日期: /

移动IP:



网络设备 是否可以隔离

层次	设备	冲突域	广播域
物理	中继器 集线器	否	否
数链	网桥 交换机	是	否
网络	路由器	是	是

日期: /

同一时间只能有一个设备发送数据到网络范围

对比记忆：

能收到同一个广播域的所有设备集合

设备	工作层	是否划分冲突域	是否划分广播域
集线器（Hub）	物理层	❌ 否	❌ 否
交换机（Switch）	数据链路层	✅ 是	❌ 否
路由器（Router）	网络层	✅ 是	✅ 是

使用VLAN可以实现广播域的隔离。

1 三种交换方式概念

(面向连接)

类型	传输单位	是否建立连接	是否存储转发	时延特性	典型应用
电路交换	比特流	✅ 是	❌ 否	建立前延迟，通信时延固定	电话网 打电话
报文交换	报文	❌ 否	✅ 是（整报文）	延时长且不定	电报网 寄信
分组交换	分组	❌ 否	✅ 是（分组级）	延时短但可变	计算机网络（Internet）

虚电路 → 面向连接，
数据报 → 无连接

微信/QQ

对比总结表

特点	电路交换	报文交换	分组交换
是否建立专用通路	✅ 是	❌ 否	❌ 否
是否存储转发	❌ 否	✅ 是（整份报文）	✅ 是（分组）
时延特性	固定且短	长且可变	较短但可变
实时性	强	弱	较强
典型应用	电话通信	早期电报	现代计算机网络（Internet）

日期: /

传输层:

1. 面向通信的最高层. 又是用户功能的最低层

2. 提供端到端的通信服务

3. 提供应用进程之间的逻辑通信

4. 复用/分用. 应用层不同进程的报文通过不同的端口向下交到传输层. 再往下交用网络层提供的服务

传输层的协议:

1. 用户数据报协议 UDP　　无连接. 不可靠传输　　一对一、一对多 多对一

2. 传输控制协议 TCP　　面向连接, 全双工可靠传输　　(不提供广播和多播)

传送的数据单位称为传输协议数据单元 (TPDU)

UDP → UDP用户数据报

TCP → TCP报文段 (segment)

传输层服务的两种类型:

1. 面向连接的传输服务.

三个阶段: 建立连接, 数据传输, 释放连接

2. 无连接的传输服务:

在传送数据前不必建立连接, 没有流控机制, 也不保证可靠交付

日期: /

传输层用协议端口号(简称端口)来标识进程

用一个16位的端口号进行标识,端口号只具有本地意义,仅标志本计算机应用层的各个进程与传输层之间交互之时的层间接口

端口号的两大类型

(1)服务器端使用的端口,又可以分为两类:

①熟知端口号: 0~1023 重要的应用程序

②登记端口号: 1024~49151

(2)客户端(临时端口号): 49152~65535

用户数据报协议 UDP.

在IP数据报服务之上增加了端口复用,分用和差错检测功能

主要特点: ①无连接 ②尽最大努力交付 ③面向报文. ④没有拥塞控制功能(实时) ⑤UDP首部简短(8字节). TCP(20字节)

(不合并也不拆分)

(在刃用时,不需要使用套接字)

UDP报文格式及伪首部:

首部(8字节)+数据

↓

4个字段×2字节

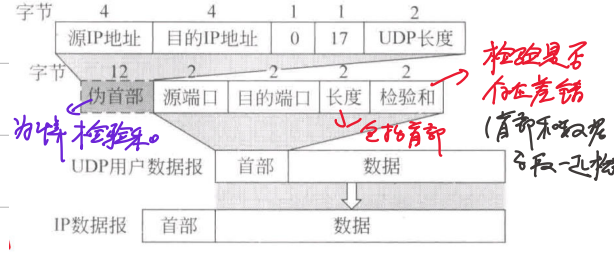


图 8-4 UDP 报文格式及伪首部

日期: /

TCP协议：传输控制协议

主要特点：①面向连接。三阶段：建立连接，数据传输，释放连接

②两个端点只能实现点一点通信 ③提供可靠交付的服务

④提供全双工通信 ⑤TCP是面向字节流

注：①TCP连接是点连接 ②根据窗口值和当前网络拥塞的程度来决定一个报文段包含多少个字节

每一条TCP连接有两个端点（套接字 socket）= IP地址：端口号

传输连接 = Socket1 · Socket2

TCP报文：

传送的数据单元：报文段（分为首部、数据两部分）

首部：固定20字节：20+4n（n≥2）

期望收到下一个报文段的第一个数据字节序号

图 8-6 TCP 报文段的格式

URG（紧急，=1 有高优先级

ACK（确认，建立连接后全置1

PSH（推送，=1 表示请求接收端的TCP立即将本报文送往应用层）

RST（复位，=1表示立即释放，而后再重建）

SYN（同步，起着序号同步的作用，当SYN=1，ACK=0，表示这是一个连接请求报文段）

同意建立连接 SYN=1，ACK=1

日期:　　/

FIN(终止，=1 表示发送的数据已完毕，并要求释放传输连接)

窗口(16位) 用于流控制 通常由接收方确定

检验和(16位)：范围：首部+数据. 计算时要在TCP报文段前面加上一个伪首部(12字节)

紧急指针(16位)：当URG=1时，表示紧急数据的末尾在报文段中位置

选项(最长可达40字节) MSS：数据字段的最大长度 (与接收窗口值无关)

填充：当选项长度不是32位的整数倍时，该字段用于补齐首部长度是4字节的整数倍

连续ARQ协议：ACK 1 表示确认0号帧，期望下一次得到1号帧

可靠传输：①面向字节流 ②确认机制—累积确认

① 重传 < 超时重传 / 冗余ACK

重传控制：① 检验出差错 ② 报文段丢失

TCP 采用重传的自适应算法.

一个报文段发出的时间和收到相应确认的时间 → 时间之差即为往返时间 RTT

TCP 保留一个加权平均往返时间 RTTS，公式如下：

新RTTS = (1−α)×旧的RTTS + α×新RTT样本 ($\alpha \in [0,1)$). RFC2988推荐的α值为 1/8

流量控制：　　真正的发送窗口值 = min(公告窗口值, 拥塞窗口值)

滑动窗口(单位：字节)　　发送方维持发送窗口

日期: /

拥塞控制：基于窗口的方法，维持了拥塞窗口 CWND

拥塞判断：① 重传定时超时 ② 收到三个相同的(重复)的 Ack

四种拥塞控制算法：慢启动 / 拥塞避免 / 快重传 / 快恢复 → 不执行慢启动

指数增加　线性增长/加法增大　3个重复确认

TCP 建立和释放连接的过程：

客户/服务器模式(c/s)：① 主动发起连接建立的应用进程称为客户 (client)

② 被动等待 …… 服务器 (server)

TCP 连接的建立：建立连接的过程称为"握手"需要在 client 和 server 之间交换三个 TCP 报文段，称为三报文握手("三次握手")

TCP 连接的释放：通信双方都可以释放连接，TCP 释放连接的过程也叫四报文握手("四次握手")

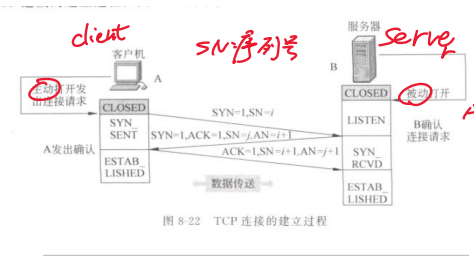


图 8-22 TCP 连接的建立过程

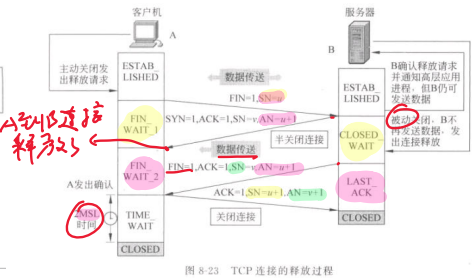


图 8-23 TCP 连接的释放过程

Question：1. 为什么三次握手：连接建立。4次？TCP是全双工

2. 为什么要有第三次握手：对自己同步确认

3. MSL (MAX segment Life time)

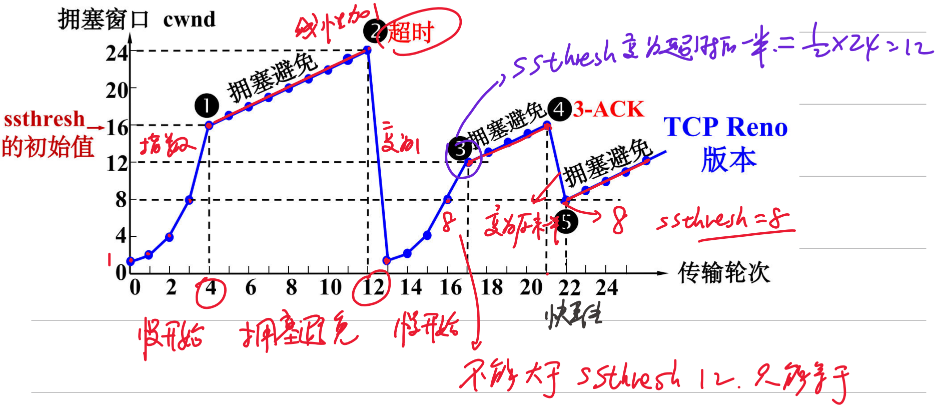
日期：　　/

拥塞控制算法：

三个核心：①轮次 n ②拥塞窗口 cwnd ③慢开始门限 ssthresh

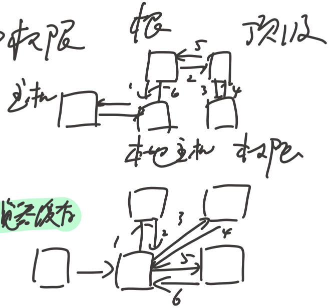
四个算法：①慢开始 ②拥塞避免 ③快重传 ④快恢复

3ACK：在数据传输过程中，有数据丢失



应用层

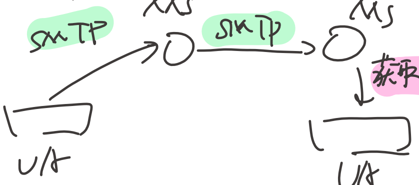
- 1 网络应用模型
  - C/S (客户端/服务器模型)
  - P2P (对等模型)
- DNS (Domain Name system)
  - 域名
    - 一对多 IP MAC.
    - 多域名对应一个IP
  - 分层结构: 根 → 顶级 → 权限
  - 域名解析过程
    - 递归
    - 迭代



主机: 操作系统/浏览器缓存

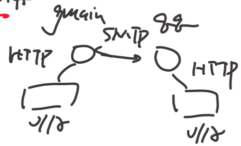
为减少根服务器压力, 我们在域名服务器之间采用迭代方式, 在主机和本地域名服务器之间采用递归方式

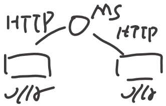
- 电子邮件
  - 连接建立
  - 邮件传送
  - 释放连接
  - 负责"发送"与"转发"



- POP3 → 下载并保存 / 下载并删除 (本地)
- IMAP → 在服务器端中被保存
- HTTP → 浏览器

MIME: 对于非ASCII码格式邮件, 先将其转换成7位ASCII码, 再用SMTP协议





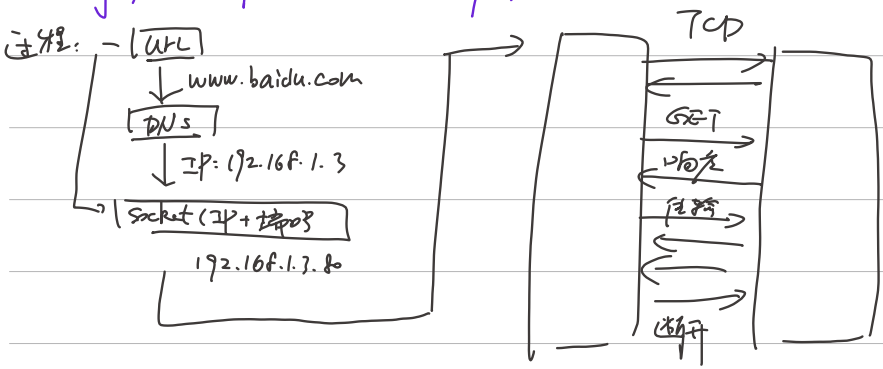
- WWW 万维网

日期: /

WWW 万维网

URL: http://www.baidu.com:80/index.html
协议 域名 端口 路径

DNS解析 → TCP连接 → HTTP请求/响应 → 浏览器可能还得解码渲染
client server



HTTP连接: 非持续访问 ⇒ 并行
持续 — 非流水
流水模式

状态码(3位数字):
1xx: 表示通知信息的
2xx: 成功
3xx: 重定向
4xx: 客户端错误
5xx: 服务器内部错误

UDP: DNS, TFTP, RIP, DHCP, IGMP
TCP: FTP, SMTP, POP3, HTTP

日期: /

DNS(Domain name system, 域名系统

分布式数据库系统　　域名 → IP地址

层次型命名机制　　最低级域名在前面, 最高级域名在最右边

顶级域名: ①国家顶级域名 ②通用顶级域名 ③基础结构域名(arpa) → 反向域名解析

倒置　根 → 顶级域名 → 一级 . .

区是一个域的子集, 区是域和根服务器管辖范围

为什么需要? DNS是分布式管理, 服务器不必管理域

域名查询: ①主机 → 本地域名服务器: 递归

②本地域名服务器 → 根: 迭代

总体: 高效(多级本地可缓存), 可靠(单点故障不致瘫痪), 分布(多服务器协作)

万维网: 分布式超媒体信息系统

工作模式: 客户/服务器模式(C/S)　浏览器/服务器模式(B/S)

统一资源定位符: URL　一般形式: <协议>://<主机>:<端口>/<路径>

<协议>: HTTP/FTP

<主机>: 域名

超文本传输协议: HTTP　核心

超文本标记语言: HTML

HTTP事务是无连接的, 但是在传输层使用TCP

日期: /

DHCP：动态主机配置协议

即插即用即连网 → 自动获取网络配置信息 （C/S模式）

端口号：DHCP熟知端口号：服务器 67，客户端 68

中继代理（Relay Agent）

Discover在本地网段广播，中继转发给服务器用单播

四步流程：DHCP DISCOVER（发现）→ DHCP OFFER（提供）→ DHCP REQUEST（请求）→ DHCP ACK（确认）

(data)

注：①可能收到多个offer ②客户选一个"request"

DHCP分配的IP是临时的，只在租赁时间内使用（租用期下）

socket 和 API

socket（套接字）：应用进程进行网络通信时的通信端点/地址+端口号

API（应用编程接口）：标准化的系统调用或库接口

日期: /

数据报分析：

TCP首部 20字节 UDP首部 8字节. 片偏移字段：单位为8字节.

例：1个UDP用户数据报的数据字段为6172字节.在经过路径传送使用以太网传送.请问应该划分为几个IP数据报片？说明每个数据报的数据字段长度和片偏移字段的值

UDP 首部：8个字节 6172+8=6200

IP将UDP报文部"数据"部分 IP首部：20个字节.

原始： 20+6200=6220个字节

MTU=1500字节.(标准：(1480字节数据+20字节首部))

8字节整数倍

6200÷1480 = 4…280 有5个IP分片. 前4个数据1480字节. 最后一个是280字节

分片	IP数据字段	IP总长	片偏移	MF	DF
1	1480	1500	0	1	0
2	1480	1500	185	1	0
3	1480	1500	370	1	0
4	1480	1500	555	1	0
5	280	300	740	0	0

日期: /

码分多址:

共有4个站进行码分多址CDMA通信. 4个站的码片序列为:

A. (-1 -1 -1 +1 +1 -1 +1 +1)　　B. (-1 -1 +1 -1 +1 +1 +1 -1)

C. (-1 +1 -1 +1 +1 +1 -1 -1)　　D. (-1 +1 -1 -1 -1 -1 +1 -1)

现收到的码片序列为 (-1 +1 -3 +1 -1 -3 +1 +1). 请问哪个站发送数据?

数据是0还是1?

进行乘运算: 1 → 发送1且发送数据为"1"

0 → 没有发送

-1 → 发送1且发送数据为"0"

路由表更新:

对发来路由表: 所有跳距+1, 下一跳站一

表中不存在的, 直接添加 若存在 { 下一跳不同. 跳距小时更新
下一跳相同. 无条件更新

日期: /

子网划分：网络号从主机号借位。

例：现在有一个C类网段 193.160.50.0，要将其划分为6个子网。

请问如何指定子网掩码？每个子网网络地址，广播地址分别是多少？

可分配主机地址范围是多少？

$2^n - 2 \geq 6 \quad n=3$

$24+3=27 \rightarrow$ 255.255.255.11100000

即 255.255.255.224

网络地址

193.160.50.001	32	
010	64	
011	96	
100	128	
101	160	
110	192	

广播地址：主机号全置1

193.160.50.00111111	63
010 11111	

可分配主机范围是 001 00001
001 11110

例：某单位分配到一个地址地址为14.24.74.0/24的地址块，该单位需要用到三个子网，他们对三个地址块的具体要求是：子网N1需要120个地址，N2需要60个，N3需要10个，请给出合理分配方案

先分地址块大的，再分小的

$2^n - 2 \geq 120$ n=7 主机号位数 8-7=1位 N1：/25

日期: /

14.24.74.0/25 子网N1地址块

$2^n-2 \geq 60$ $n \geq 6$ 借2位 14.24.74.128/26

$2^n-2 \geq 10$ $n \geq 4$ 借4位 14.24.74.196/28