一、绪论和传输介质

1、信号的能量形式

电的：双绞线、同轴电缆

光的：光纤、红外线、激光

电磁波（无线电波）：地面无线电、卫星

2、屏蔽与非屏蔽双绞线、同轴电缆

非屏蔽双绞线（Unshielded Twisted Pair）：柔韧性强，成本低

同轴电缆（Coaxial Cable）：屏蔽能力强，成本高

屏蔽双绞线（Shielded Twisted Pair）：折中

双绞线：

既能传输模拟信号，也能传输数字信号

通信距离一般为几到几十公里（距离太长，信号会衰减，需要用中继器整形和放大）

CAT-3，带宽16MHz，曾常用在10Mbps以太网络

CAT-5，带宽100MHz，常用在快速以太网（100Mbit/s）中

CAT-5e，带宽125MHz，常用在快速以太网（100Mbit/s）和吉比特以太网（1000Mbit/s）

同轴电缆：

按阻抗分为50Ω同轴电缆和75Ω同轴电缆

50Ω：基带同轴电缆（Baseband Coaxial Cable）

以10Mb/s传输基带信号的距离可达1km

用于以太网的标准：10Base2，10Base5

75Ω：宽带同轴电缆（Broadband Coaxial Cable）

频率可高达500MHz以上，传输距离可达100km

用于传输有线电视的模拟信号

分为多个信道（使用电缆调制技术，电视和数据可在一条电缆上混合传输）

3、单模与多模光纤

多模突变光纤：便宜，纤芯密度不变，覆层间突变

多模渐变光纤：纤维密度越接近边缘越大，减少反射

单模光纤：贵，直径小，长距离，高比特率

项目	单模光纤	多模光纤
距离	长	短
数据传输率	高	低
光源	激光	发光二极管
信号衰减	小	大
端接	较易	较难
造价	高	低

二、局域异步通信

1、RS232-C标准

电气特性

连线长度：小于50ft

电压范围：-15V~+15V

线路编码：负电压表示1，正电压表示0（来自电传机（Teleprinter）），
$0:[3V,15V];1:[-15V,-3V]$

机械特性

RS232-C并未定义连接器的物理特性，因此出现了DB-25，DB-15和DB-9（以上均为梯形口）等各种类型的连接器

2、串行与并行传输

串行（Serial）：同时只传输一位

并行（Parallel）：多位同时传输

3、同步与异步传输

同步（Synchronous）：连续发生，需事先约定有效数据的位置，两个数据项之间没有间隔

异步（Asynchronous）：在任意时间发生，两个数据项之间可以有任意的时延

4、单工、半双工和全双工传输

单工：单方向通信（只能发送**或**接受）

半双工：可双向通信，但**同一时间**只能单向通信

全双工：同一时刻可双向通信

5、DCE和DTE设备的概念

DCE：数据通讯设备

DTE：数据终端设备

以下为10Mbps以太网RJ-45接口，DCE和DTE的连线

DCE		DTE
接受正（R+）	Lead#1	发送正（T+）
接受负（R-）	Lead#2	发送负（T-）
发送正（T+）	Lead#3	接受正（R+）
未用	Lead#4	未用
未用	Lead#5	未用
发送负（T-）	Lead#6	接受负（R-）
未用	Lead#7	未用
未用	Lead#8	未用

在UDP上以100Mbps及以上的局域网将使用全部四对线

6、带宽、波特率和比特率

带宽（Bandwidth）

传统定义：某个信号所具有的频带宽度

新定义：该信号各种不同频率成分所占据的频率范围（特定信号通常由许多不同频率成分组成）

数字信道的带宽：

在信道上能够传送的数字信号的速率，即数据率或比特率

单位：b/s，或bps

根据香农理论，带宽也有时候被称为吞吐量

波特率（Baud）

带宽的单位：波特（也称波特率）

传输介质中信号变化的速率，每秒传输的符号数（真正的硬件不能瞬时改变电压，带宽有限）

仅在二进制环境下为bps

发送方和接收方硬件的波特率不同，将发生错误

接收方计时器每个位的等待时长不恰当

检测错误时，接收机多次测量每个比特的电压，并比较测量结果。如果电压都不一致，或停止位没有在预期时间发生时，接收器会报告错误，成为帧错误

7、奈奎斯特定理和香农定理的物理意义

奈奎斯特定理：

如果传输系统使用K个可能的电压值，带宽为B（半个周期），则最大数据率为$D = 2Blog_2K$

香农定理：

引入噪声的传输系统可以达到的最大数据速率为$C = Blog_2(1 + \frac{S}{N})$

其中S是平均信号功率，N是平均噪声功率，$-\frac{S}{N}$是信噪比，其中$10lg\frac{S}{N}$的单位为分贝（dB）

物理意义：

奈奎斯特定理鼓励工程师探讨如何对信号进行位编码，因为一个聪明的编码允许单位时间传递更多位

香农定理则告诉工程师再多的巧妙编码也难以克服限制通信系统中每秒可传输位数目的物理规律

三、远程通信

1、模拟信号，数字信号、模拟-数字信号转换

模拟信号：

时间连续，幅值离散

数字信号：

时间离散，幅值连续

模拟-数字信号转换

利用奈奎斯特定理，以大于信号带宽两倍的频率进行采样，则原来的模拟信号可以从采样样本中完全重建出来

2、编码和解码

编码：

将字符按照相应的编码类型转化成计算机能够识别的0-1序列（比特-能量）

解码：

将0-1序列按照相应的解码规则转化成人类能够识别的字符（能量-比特）

3、常用调制技术：调幅、调频、调相

调幅（Amplitude Modulation, AM）

更改振幅

调频（Frequency Modulation, FM）

更改频率

调相（Phase Shift modulation, PM）

更改相位

4、调制解调器（Modem）

调制器（Modulator）

执行调制功能的器件

解调器（Demodulator）

执行解调制功能的器件

5、复用与解复用、时分复用、频分复用、波分复用

复用（Multiplexing）

指多个信源的信息流组合在一条共享介质上传输

解复用（Demultiplexing）

指将信息流组合分隔回分开的信息流

频分多路复用（Frequency-Division Multiplexing, FDM）

载波带宽被划分为多种不同频带的子信道，每个子信道可以并行传送一路信号的一种多路复用技术

多个载波可以在同一时间通过同一导线不相互干扰

高吞吐量（throughput）

波分多路复用（Wave Division Multiplexing , WDM）

光的频率很高，习惯用波长表示光波，即光的FDM就是WDM

在一根光纤上发送多个光波

在接收端，光学棱镜用来分离频率

时分多路复用（Time-Division Multiplexing, TDM）

将时间划成等长的时分复用帧

每个用户在每一帧中占用固定序号的时隙

所有用户在不同时间占用相等的频带宽度

同步时分多路复用（Synchronous TDM）：每个用户依次、均匀地占用信道

统计时分多路复用（Statistical TDM）：使用时分多路复用系统传输数据时，由于计算机数据的突发性质，用户对分配的子信道的利用率一般是不高的，故通过动态按需分配共用信道的时隙，优化信道的利用率

四、差错控制

1、奇偶校验（Parity Check）的简单计算

发送方根据消息序列计算一个额外的位附加在原有消息序列后，称为奇偶位

接收方收到所有位后，校验并丢弃奇偶位

两种机制：奇和偶

奇校验中消息和校验位有奇数个1，偶校验有偶数个1

发送和接收方应该有相同的模式

2、Internet校验和的计算

把消息每16位作为一个整数计算和，若结果大于16位，则重复上述过程，最后取反

3、循环冗余校验码（Cyclic Redundancy Codes）

一种根据网络数据包或文件等数据产生简短固定位数校验码的哈希函数，主要用来检测或校验数据传输或保存后可能出现的错误

重要特征

任意消息字长

出色的错误检测

快速硬件实现（位移寄存器，异或门）

五、局域网分组与编址

1、交换技术：电路交换、报文交换、分组交换

分组交换（Packet Switching）

以分组为单位进行传输和交换的存储-转发交换方式

采用统计复用，多个来源争夺共享介质使用

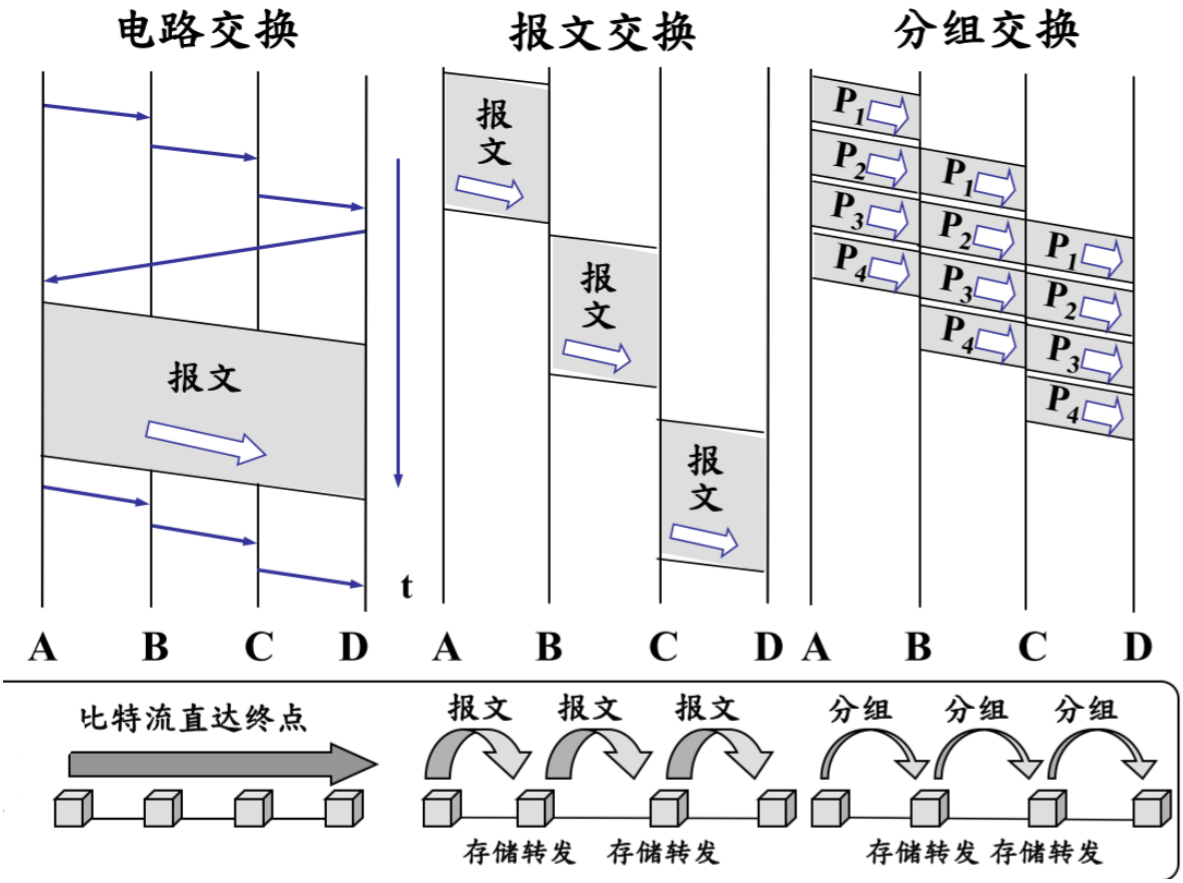
特点：异步，无需建立，性能各异

电路交换（Circuit Switching）

通信之前在通信双方之间建立一条被双方独占的物理通道

多个电路在共享介质上复用，形成虚拟通路

类似于电话技术：建立线路，线路交互，中止使用



2、网络接口卡（NIC）的作用

处理地址识别、CRC计算、帧识别、发送和接受帧（减小CPU的负荷）

3、MAC（Media Access Address）地址的构成

组织唯一标识（高24位）：

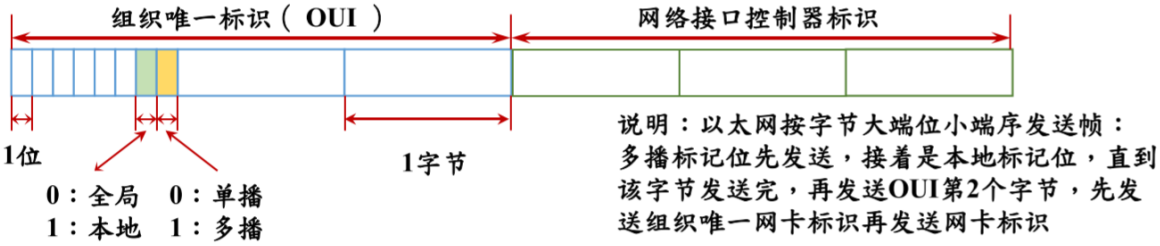
IEEE向厂家分配唯一标识（OUI）

第一个字节最低位为0表示单播，1表示多播和广播

第一个字节最低第二位为0表示全局网址，1表示局域网址

网卡标识符（低24位）

厂家自行分配



4、单播、广播、多播

单播（Unicast）

一对一

多播（Multicast）

一对多，特定地址

当一台计算机需要同时向多台计算机传输信息时使用广播

网上的所有设备的网卡拷贝数据帧，交给CPU处理，需要与否由CPU决定

广播（broadcast）

一对全体，48位全为1

5、帧结构（头部+载荷）、成帧

6、以太网的帧结构

七字节的前同步码：

56比特交替出现的的0和1

提醒系统有帧到来，以及使到来的帧与计时器同步

帧首界定符（SFD）：

1字节的10101011，标志帧的开始

目的地址：

6字节，目的物理地址

源地址：

6字节，源物理地址

类型：

2字节，标记了封装在帧中的数据类型

数据：

包含从上层来的数据，应在46~1500字节之间

若上层协议产生数据长度小于46字节，则将其填补到46字节

若数据长度超过1500字节，则必须将其进行分片

循环冗余校验：

4字节，CRC-32，用于差错检测

六、以太网、拓扑与无线技术

1、局域网拓扑：总线、星形、环形、网状

2、以太网介质访问控制策略（CSMA/CD）

3、其他网络类型的特点：LocalTalk、Token Ring、FDDI、ATM

4、网络技术的分类：个域网、局域网、城域网、广域网

5、WLAN基本概念：蓝牙、蜂窝网络、1~4G、GPS及其速率的大致量级

七、局域网的布线、拓扑、接口硬件

1、以太网的粗缆、细缆、双绞线布线

2、物理和逻辑拓扑

3、冲突域与广播域的概念

4、中继器、集线器、网桥

5、交换机、广播风暴与分布式生成树

八、远程数字连接技术、网络性能

1、Internet接入技术：上行与下行

2、接入技术：宽带与窄带、ISDN、ASDL、电缆调制解调器、无线、光纤

3、标准：数字电话标准（T、E）、干线标准（STC、OC、同步光网络）

4、各种网络接入技术与标准大致的速率量级

5、广域网技术的类型：虚电路、数据报、及各自的特点

6、不同类型的网络技术：APANET、PSTN、X.25、帧中继的特点

7、网络所有权：私有网络、公有网络的定义

8、网络的性能度量：时延、吞吐率、抖动

九、广域网技术与路由、协议系列

1、分组交换机的原理、存储与转发

2、广域网的概念和分层编址

3、路由工作表原理

4、路由器转发表、默认路径、下一站

5、网络协议分层的思想：网络互联、虚拟网络的概念

6、ISO/OSI网络协议的分层模型（七层）

7、TCP/IP协议栈（五层）

8、ISO/OSI和TCP/IP分层之间对应关系、数据基本单位、各层的分工作用

十、网际协议编址

1、IPV4编址方案

分类IP地址（1981~1993）：将IP地址空间分为五大类，是最基本的编址方法

子网划分（1985~）：主机号的部分位用于表示子网号，对分类地址方法的改进

无分类IP地址（1993~）：灵活调整网络大小

2、有类地址（A/B/C/D/E）、无分类和CIDR表示法

有类地址

根据最前的位内容来确定具体属于哪一类

类	位前缀	网络位	主机位	网络容量	网络中主机容量	起始地址	结束地址	子网掩码
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255	255.0.0.0
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255	255.255.0.0
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255	255.255.255.0
D	1110			多播地址		224.0.0.0	239.255.255.255	无
E	1111			保留地址		240.0.0.0	255.255.255.255	无

无分类和CIDR表示法

地址掩码（Address Masks）

用于指示IP地址中主机所在子网地址的位掩码

由连续的N位1和32 - N位0构成

作用：求取网络地址（网络号）

网络前缀 = (目的地址 & 网络掩码)

无类域间路由（Classless InterDomain Routing）

一般形式： ddd.ddd.ddd.ddd/m

d为网络号，m为掩码中1的个数（不一定是8的倍数）

3、子网划分和子网掩码

子网划分

从主机号借若干位作为子网号，主机号相应减少若干位

对外通讯和子网号无关，内部通讯和子网号有关

子网掩码（subnet mask）

使用子网掩码可以找出IP地址中的子网部分

路由器在和相邻路由器交换路由信息时，必须把自己所在的网络（子网）掩码告诉相邻路由器

若一个路由器连接在两个子网上，就拥有两个网络地址和两个子网掩码

4、特殊IP地址（本机、网络、环回、直接广播、有线广播）

名词	英文名词	规则	示例
网络地址	Network address	主机号全0	59.0.0.0
直接广播地址	Directed Broadcast Address	主机号全1	59.255.255.255
有限广播地址	Limited Broadcast Address	地址全1	255.255.255.255
本机地址	This Computer address	全0	0.0.0.0
回送地址	Loopback address	127.0.0.0/8	127.0.0.1

5、网络层的广播和多播

直接广播地址：主机号全为1，接收方为该网络号下的所有主机

有限广播地址：地址全为1（255.255.255.255），路由器不转发

6、多穴主机（Multi-Homed Hosts）

提高可靠性：如果一个网络失效（拥塞），主机仍可以通过第二连接到达互联网

多穴主机有多个IP地址，每个网络连接一个地址

有多重连接的原因：负载平衡和速度冗余提高网络可靠性

十一、数据报转发、支持协议和相关技术、IPv6

1、IPv4数据报格式中的各部分组成

版本：4bits（4或6）

报头长度：4bits，单位为4Bytes

服务类型：8bits，未实际使用

报文总长度：16bits（64KB）

标识：16bits，IP软件在存储器中的计数器在产生一个数据报时自增1，并赋值给标识字段，标识在分片时**复制**

分片标志：3bit，高到低分别为：无意义、不分片、还有分片

片偏移：13bits，分片在原始报文的位置，单位为8Bytes

生存时间（TTL）：8bits，单位为秒，路由器减去在其环节所消耗时间，直至零丢弃

协议类型：8bits，可能取值为ICMP、IGMP、TCP、UDP、OSPF等，用于将数据交给上层软件

报头校验和：16bits，检验报头完整性（不包括数据部分）

源IP地址：32bits

目的IP地址：32bits

选项内容：1~40bits，用于支持排错、测量、安全等措施

填充部分：不定长，使报文头部为4Bytes的整数倍

2、MTU与分片、分片重组和收集

MTU：最大传输单元

数据链路层帧支持的最大传输字节数

当前链路MTU小于IP报文长时，分成较小分片传输

分片

路由器将数据报分成更小的碎片

原始数据报首部被复制成各数据报片首部，但必须要修改有关字段的值

标识：复制，保持初始标识不变

分片标志：MF（More Fragment）= 1表示后续还有分片，反之亦然；DF（Don't Fragment）= 1表示不允许分片，反之亦然；

片偏移量：表示当前分片在初始IP包中有效数据的偏移位置（单位：8Bytes）

每个分片使用IP数据报格式，并独立发送

各片尽可能大（但不超过MTU），尽量少分片

分片（除了最后一片）应使得后续片偏移量为8的整数倍

分片重组（Reassembly）

可能有多次分片

所有分片重组在目标端进行，中间路由设备**不做**分片重组（减少中间节点的数据处理过程）

碎片可以再分片

分片收集

目标端对IP报文分片做重组时进行丢失判断

对于任意一个报文，在收集到第一个分片后设置一个等待的有限时间T-out，若经过T-out后还没有收到全部分片，则为超时

任意一个分片出错或丢失，则丢弃整个报文

3、IP封装、虚拟分组

封装（Encapsulation）

将IP数据报放入帧的载荷内，并加上帧头/尾

虚拟分组（Virtual Packet）

网络互联协议定义独立于底层硬件的“分组”格式

4、IP数据报转发原理、转发过程中的帧头、报文头的情况

通过计算（子网掩码 & 路由表中各条目的子网掩码），若按位与结果与该条目的网络号匹配，则下一条即为所求

最长前缀匹配（Longest Prefix Match）：若有多个条目能够匹配成功，则选用网络号最长的那个（网络掩码中1最多的）

通过以上方法选择下一跳后，通过物理网络发送

帧达到下一跳，接收方软件提取IP数据报并丢弃帧头/尾，若还需转发则重新封装

报文头一直不变

5、ARP协议作用、概念地址边界

ARP（Address Resolution Protocol，地址解析协议）协议的作用

将IP地址解析为MAC地址

方法：查表、相近形式计算、消息交换

使用ARP的四种典型情况：

主机 -> 本网主机：找到目的主机的MAC地址

主机 -> 另一网络上的主机：找到本网络上路由器的MAC地址

路由器 -> 本网主机：找到目的主机的MAC地址

路由器 -> 另一网络上的主机：找到另一路由器的MAC地址

概念地址边界

工作在IP地址和MAC地址之间（2.5层）

6、ICMP协议（ping、route、traceroute）工作原理

ICMP（Internet Control Message Protocol，Internet报文协议）工作机制

主机或路由器报告差错情况和提供有关异常情况的报告

ICMP报文作为IP层数据报的数据，加上数据报的首部，组成IP数据报发送出去

不发送ICMP差错报告报文的情况

原报文是ICMP差错报告报文

除了第一个分片以外的同一数据报片

地址为多播地址

地址为其它特殊地址（127.0.0.0、0.0.0.0等）

PING（Packet Internet Groper，因特网包探索器）

报文类型：ICMP回送请求和回送回复消息

把包含ICMP回送请求消息的IP数据报发送到指定的目的地

每当一个回送请求到达，ICMP软件必须发送一个回送应答

是应用层更直接使用网络层ICMP的例子（没有通过传输层的TCP/UDP）

traceroute

traceroute发送一系列数据报，等待每一个响应

如果TTL计数器达到0，则路由器丢弃数据报，并发送ICMP超时错误

traceroute不断增加TTL，直到该值足够大到数据报到达其最终目标

发送ICMP回送请求消息，目标主机将生成ICMP回送应答

将数据报发送给不存在的应用程序，目标主机将生成ICMP目的地无法到达的消息

route

打印本机路由表

7、DHCP协议作用

DHCP（动态主机配置协议）：从服务器获得IP地址（时分多路复用，轮流使用IP地址）

8、NAT和传输层NAT的工作原理、用于NAT的私有地址

NAT（网络地址转换）：将数据包中的IP源地址由站点替换为Internet，并且将IP目的地址由Internet替换为站点

传输层NAT（NAPT）：带端口号的NAT，端口号也参与转换（因为终究是追上的应用在上网）

私有地址：NAT内部的地址

9、IPv6编址方案、冒分十六进制表示法

地址空间：128位

冒分十六进制表示法

按16位一组，以冒号分隔每个组

每组内前导0可以不写

两个冒号表示连续出现两个以上的0（最多使用一次）

IPv4扩展到IPv6（在IPv4地址前加上::FFFF:0:0/96的前缀）

十二、传输层协议简介、用户数据报协议

1、端到端服务与虚拟连接的概念

端到端服务：网络通信本质是两个进程间的通信，不是主机间通信

虚拟连接：传输层隐藏了硬件拓扑、路由细节等，使应用程序直接调用其接口，建立一条虚拟的端到端的通信信道

2、端口号的作用与编号规则、应用层主要协议与端口号

作用：用于表示本机的不同进程

编号规则：熟知端口号（0 ~ 1023）、登记端口号（1024 ~ 49151）、客户端口号（49152 ~ 65535）

协议	传输层协议	端口号	作用
FTP（数据）	TCP	20	FTP数据传输
FTP（控制）	TCP	21	FTP控制命令传输
Telnet	TCP	23	终端远程登录
SMTP	TCP	25	发送电子邮件
HTTP	TCP	80	网页服务
POP3	TCP	110	接收电子邮件
IMAP	TCP	143	同步邮箱
HTTPS	TCP	443	加密网页服务
RDP	TCP	3389	Windows 远程桌面连接
DNS	TCP/UDP	53	域名解析
DHCP（源）	UDP	68	动态IP获取的客户端端口。
DHCP（目的）	UDP	67	动态IP获取的服务器端端口。

3、UDP的主要特点（无连接、尽力而为、轻量级）

UDP（User Datagram Protocol，用户数据报协议）

无连接：发送数据前不需要建立连接（连接：对状态/变量的保持，不是对网络的保持）

尽力而为：不保证可靠交付，同时也不使用拥塞控制

轻量级：首部开销小，只有8Bytes（16bits源地址、16bits目的地址、16bits长度、16bits校验和）

4、TCP、UDP的应用场景

UDP

常用于丢包损失不大、应用层可控制丢包的场景

面向简单事务：查询响应协议（域名系统、网络时间协议）、没有完整协议栈的引导（DHCP、TFTP）

提供数据报：构建其他协议（IP隧道、远程过程调用、网络文件系统）

大量客户端：流媒体应用（IPTV）

实时应用：建立在实时流的协议（IP语音、网络游戏）

单项沟通：服务发现和共享信息中的广播信息（广播时间或路由信息协议）

TCP

十三、传输控制协议

1、TCP的主要特点（面向连接、点对点、可靠、全双工、字节流）

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

面向连接：收发双方都保有一些状态的信息，使得通讯顺序进行

点对点：只允许一对一的通信

字节流：数据像水流一样源源不断地发出和接受

可靠：TCP保证接收到的数据一定是完整、可靠的

全双工：TCP在发送的同时可以接收

2、TCP段格式中的各部分组成

TCP报文头数据项（基本信息20B）

源端口号：16bits

目的端口号：16bits

发送数据序列号（报文段序号）：32bits

TCP将每一个**字节**按顺序编号

指的是本报文**第一个**字节的序号

确认序列号：32bits

期望收到**下一个**字节的序号，表示之前的字节都已经收到

报头长度：4bits，单位4Bytes

保留位：4bits

标识符：8bits

拥塞窗口下降

ECN回显

紧急指针：优先传输

ACK字段：确认号有效

数据前推：不等待缓存满，直接发送

连接复位：拒绝连接

序号同步：建立连接时用来同步信号

终止连接：数据已发送完毕，释放信号

滑动窗口缓冲区大小：16bits

校验和：16bits

紧急指针：16bits

选项字段（变长）：最大报文段长度、窗口扩大选项、时间戳等

3、TCP的基本工作原理（应答、超时、重传、窗口机制）

应答

接收方收到正确的报文后便发送确认消息，若多次收到相同的报文，则保留最后一次收到的报文，并且对每一个报文进行确认

超时重传

TCP每发送一个报文段，就设置一个计时器，在计时器设置的重传时间（RTO）到之前没有收到确认报文，就要重传该报文段（对重复收到的确认报文不予理睬）

第一次采集到RTT样本时，RTT_S就为采集到的RTT样本值，以后每收到一个RTT样本，就按以下公式计算一个新的RTT_S

$$RTT_S = (1-\alpha) \times RTT_S + \alpha \times RTT$$

推荐的α值为0.125

超时重传时间（Retransmission Time-Out）应略大于RTT_S

$RTO = RTT_S + 4 \times RTT_D$

RTT_D是RTT的偏差的加权平均值

第一次测量时，RTT_D值为RTT的一半，以后每收到一个RTT样本，就按以下公式计算一个新的RTT_D

$$RTT_D = (1-\beta) \times RTT_D + \beta \times |RTT_s - RTT|$$

推荐的β值为0.25

只要重传了报文，该报文的往返时间便不采用

RTO间每重传一次便乘二，不重传时回复

窗口机制

窗口内的分组都连续发送出去，不需要等待确认

逐一确认：每收到一个确认，窗口往前推移一格

累计确认：接收方收到几个分组后，对最后一个窗口进行确认

4、TCP的流量控制机制（滑动窗口）

根据接收方期望收到的序号 + 接收方给出的窗口值长度 - 1（即发送方的接收窗口前沿），发送方构造出自己的发送窗口

TCP标准强烈不赞成发送窗口前沿（离已发送最远的）向后收缩

发送窗口 - 已发送但尚未收到确认的字节 = 可用窗口（允许发送但尚未发送的字节）

接收方对于未按顺序收到的部分，先存下，等待缺少的数据到达

发送缓存：准备发送的数据、已发出但未收到确认的数据

接受缓存：按序到达但尚未被应用程序读取的数据、不按序到达的数据（TCP标准并未规定如何处理，这是常用做法）

发送方的发送窗口和接收方的接受窗口不一定一样大（有一定的时间滞后）

TCP要求接收方有累计确认功能，以减小传输开销

TCP为每一个链接设有一个持续计时器，只要一方收到对方的零窗口通知，就启动持续计时器，若计时器时间到，则发送一个零窗口探测报文段（仅携带1字节数据），而对方就在探测报文段给出现在的窗口值，若窗口值为0，收到报文段的一放就重新设置持续计时器，若不为0，则死锁的僵局被打破

不同机制控制TCP报文段发送：

缓存中存放的数据达到MSS（最大报文段长度）字节时，就组装成一个TCP报文段发送

发送方进程要求发送报文段即发送

发送方的计时器时限到了，就将当前已缓存数据装入报文段发送（不能大于MSS）

5、TCP的拥塞（congestion）控制（慢开始、拥塞避免、快重传、快恢复、随机早期检测）

慢开始：TCP初始化时，拥塞窗口置为1，发送方每收到**一个**对新报文的确认（不计算重传），就使cwnd（Congestion Window，拥塞窗口）加1，达到门限值（初始为16）改用拥塞避免算法

拥塞避免：把拥塞窗口控制为按线性规律增长，使网络**较不容易**拥塞

快重传和快恢复：要求接收方每收到一个失序的报文段后就立即发出重复确认（使发送方及早知道报文段有没有到达对方），发送方只要一连收到三个重复确认就应当立即重传对方尚未收到的报文段，并使cwnd减半，且执行拥塞避免算法

发送窗口的上限应为min(接收方窗口,拥塞窗口)，

随即早期检测RED（Random Early Detection）：使路由器队列维持两个参数，队列长度最小门限LH_{min}和最大门限LH_{max}，RED对每一个到达的数据报都先计算平均队列长度L_{AV}，从队首开始，在最小门限以内的便依次发送，在最大门限和最小门限之间的，以概率p丢弃（p线性增加），直至最大门限取到p_{max}，并且以后的都不发送

6、TCP的连接建立与解除（三次握手、四次挥手）

设A为客户端，B为服务器端

连接建立

A —— SNY = 1, seq = x ——> B

B —— SYN =1, ACK = 1, seq = y, ack = x + 1 ——> A（如果B同意建立连接）

A —— ACK = 1, seq = x + 1, ack = y + 1 ——> B（A的TCP通知上层应用进程，连接已经建立；B收到A的确认报文后，也通知上层应用进程TCP连接已经建立）

SYN：同步标记，ACK：确认标记，seq：发送数据序列号，ack：接收数据序列号

连接解除

数据传输结束后双方都可以释放连接

A —— FIN = 1, seq = u ——> B

B —— ACK = 1, seq = v, ack = u + 1 ——> A（TCP服务器进程通知高层应用进程，A到B的连接已经释放，TCP连接处于半关闭状态，若B发送数据，A仍要接受）

B —— FIN = 1, ACK = 1, seq = w, ack = u + 1 ——> A（B已经没有要向A发送的数据，应用进程便通知TCP释放连接）

A —— ACK = 1, seq = u + 1, ack = w + 1 ——> B（A经过2MSL（最长报文寿命）真正释放）

FIN：中止标记

7、传输层如何解决网络层存在的主要问题（丢包、重复、乱序）

丢包：确认信息、重传

重复：只保留最后一次收到的

乱序：缓存

十四、因特网路由与路由协议

1、静态路由与动态路由

静态路由选择策略（非自适应路由选择）：简单、开销较小，但不能及时适应网络的变化

动态路由选择策略（自适应路由选择）：能较好地适应网络状态的变化，但实现较复杂，开销较大

2、自治系统（AS）的概念

自治系统（Autonomous System）：在单一的技术管理下的一组路由器，尽管一个AS可能使用多种内部路由选择协议和度量，但重要的是一个AS对其它AS表现出的是一个单一的和一致的路由选择策略

3、内部网关协议（IGP）、外部网关协议（EGP）

内部网关协议（Interior Gateway Protocol）：在一个自治系统内部使用的路由选择协议

外部网关协议（External Gateway Protocol）：自治系统边界网关使用的路由选择协议

4、RIP协议、OSPF协议的工作原理和特点

路由信息协议（Routing Information Protocol，RIP）

工作原理是分布式的基于向量的路由选择协议（使用UDP报文）

网络中每个路由器维护从自己到其它网络的距离记录（最长距离为15，3min内没有收到相邻路由器的路由表便标记该路由器距离为16（不可达））；

特点：

仅与相邻的路由器交换信息

交换的信息是自己的路由表

按固定间隔时间交换里路由信息

路由器故障要较长时间才能传递给整个自治系统

开放最短路径优先（Open Shortest Path First，OSPF）

工作原理是分布式的链路状态协议（基于Dijkstra的最短路径算法），采用IP报文直接发送

特点：

使用洪泛法向本自治系统中的所有路由器发送信息

发送的信息是与本路由器相邻的所有路由器的链路状态（与哪些路由器相邻以及链路的度量（metric））

只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送信息

更新收敛得快

将自治系统划分成区域（因为每个路由器都知道自己区域内的完整区域信息），区域编号为32位，点分十进制表示

主干区域连通其它在下层的区域

多路径间的负载平衡：若到同一目的网络有多条相同代价的路径，则可将通信量分配给这几条路径

有五种报文分组（问候、数据库描述、链路状态请求、链路状态更新、链路状态确认）

每隔一段时间（如30min）要刷新一次数据库中的链路状态

5、BGP协议的工作原理和特点

每个自治系统选择至少一个路由器作为该自治系统的“BGP发言人”，在此基础上，不同自治系统的发言人之间建立TCP连接，并交换互相的“可达性”信息

BGP只是力求寻找一条能够到达目的地且比较好的路由，而并非寻找一条最佳路由

特点：

BGP协议交换路由信息的结点的数量级是自治系统数的量级

每一个系统中BGP发言人的数目很少，这样就使得自治系统之间的路由选择不会过于复杂

BGP支持CIDR，因此BGP的路由表也应当包括目的网络前缀、下一跳路由器、到达该目的网络所要经过的各个自治系统序列

BGP刚开始运行时，交换整个BGP路由表，但此后只用对更新部分进行交换

有四种报文格式（打开、更新、保活（确认邻站关系）、通知（发送检测到的差错））

十五、网络编程与Socket API

1、客户端-服务器端（C/S）交互模式工作原理

交互模式是一种分布式的应用结构计算，在任务或工作负载的资源或服务的提供者和服务请求者之间

客户端

主动打开、主动结束、一对一

服务器端

被动打开、响应请求、一对多

2、并发的概念

允许多个应用在同一时间执行的计算机系统

并发誓C-S交互模式的基础

3、Socket结构、半相关与全相关

结构：本地套接字地址（本地IP地址、本地端口号）、远程套接字地址（远程IP地址、远程端口号）、协议（TCP/UDP/原始IP）

半相关（half-association）：网络中用三元组（协议、本地地址、本地端口号）在全局唯一标志一个进程（连接的半部分）

相关（association）：网络中用五元组（协议、本地地址、本地端口号、远程地址、远程端口号）标识一个完整的网间通信

两个协议相同的半相关能够组成一个全相关

4、服务器与用户（硬件）、服务器端与客户端（软件）、二者区别

硬件：客户设备和服务器设备（需要有强大的硬件）

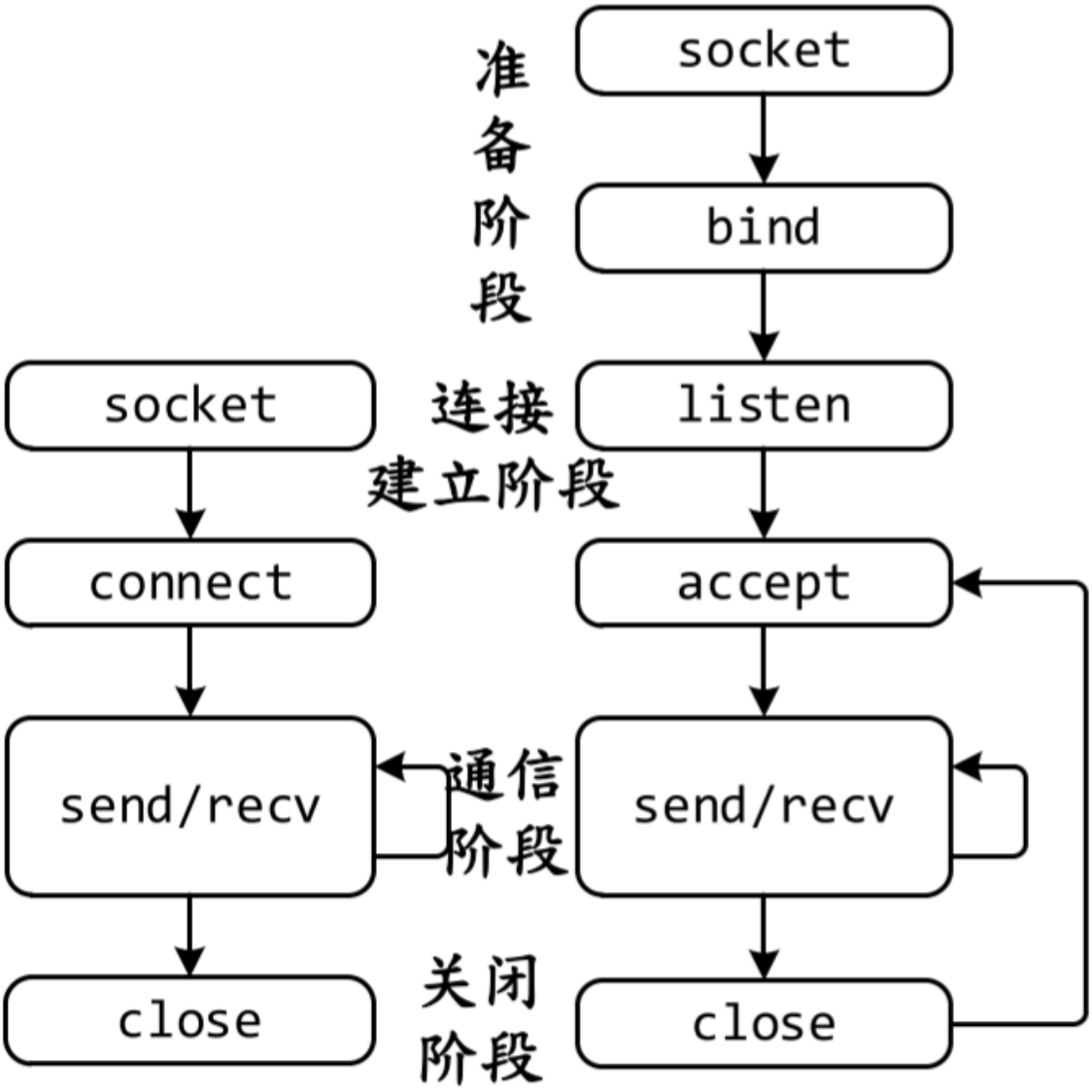
软件：客户端和服务器端是相对的，客户端可以是任意的应用程序；直接由客户调用（只执行一次会话）；主动与服务器接触；可以按需访问多个服务，但同时只能主动连接一个远程服务器，服务器端是提供服务的专门程序，可以同时处理多个远程客户端；系统启动时自调用，通过多个会话连续执行；在共享计算机上运行；被动地等待来自任意远程客户的联系；提供单一服务

区别：服务器是一个系统，响应计算机网络上的请求以提供或帮助提供网络服务；客户端是一个计算机硬件或软件服务器提供的服务的一块

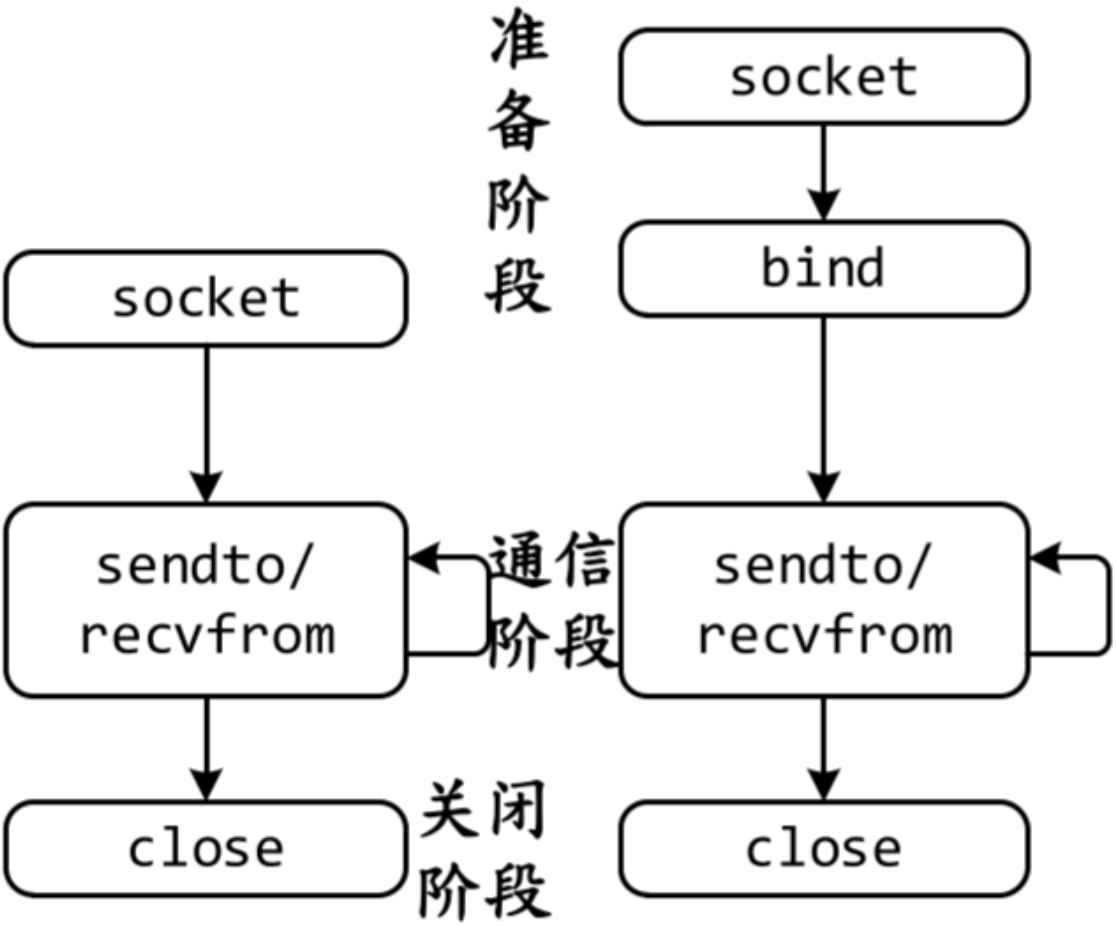
5、Socket API主要函数

Name	Used By	Meaning
accept	server	Accept an incoming connection
bind	server	Specify IP address and protocol port
close	either	Terminate communication
connect	client	Connect to a remote application
getpeername	server	Obtain client's IP address
getsockopt	server	Obtain current options for a socket
listen	server	Prepare socket for use by a server
recv	either	Receive incoming data or message
recvmsg	either	Receive data (message paradigm)
recvfrom	either	Receive a message and sender's addr.
send (write)	either	Send outgoing data or message
sendmsg	either	Send an outgoing message
sendto	either	Send a message (variant of sendmsg)
setsockopt	either	Change socket options
shutdown	either	Terminate a connection
socket	either	Create a socket for use by above

6、基于流模式的客户端、服务器端Socket API调用流程



7、基于报文模式的客户端、服务器端对Socket API调用流程



十六、传统的因特网应用

1、HTTP工作原理与过程、错误代码、URL、HTML文档

HTTP（HyperText Transfer Protocol，超文本传送协议）

原理：是万维网上能够可靠地交换文件的重要基础，可以使超文本的链接高效率地完成

过程：建立TCP连接，客户端发送HTTP请求报文、服务器端发送HTTP响应报文，释放TCP连接

URL（Uniform Resource Locator，统一资源定位符），每个文档在整个因特网范围内有唯一的标识符URL

错误代码：4XX表示客户的差错，5XX表示服务器的差错

HTML（HyperText Markup Language，超文本标记语言）文档：是一种可以用任何文本编辑器创建的ASCII码文件，定义了许多用于排版的命令

在浏览器输入网址并输入回车后发生的事件

浏览器分析超链指向页面的URL

浏览器向DNS请求解析网址的IP地址

域名系统解析出网址的IP地址

浏览器与服务器建立TCP连接

浏览器发出取文件命令

服务器给出响应，把文件发送给浏览器

TCP连接释放

浏览器显示文件中的所有文本

2、FTP工作原理与通信模式、主动和被动工作模式

TCP连接

文件传输协议（File Transfer Protocol，FTP）

提供交互式的访问，允许用户指明文件类型、格式，允许文件有存取权限

屏蔽计算机系统的细节，适合在异构网络中任意计算机之间传送文件

基于流的C/S模式，一个FTP服务器能够同时为多个客户端进程提供服务

由一个接受新的请求的主进程和若干个处理单个请求的从进程组成

使用两个端口号，端口21提供控制连接，端口20提供数据连接

主动模式：客户端主动提供端口号请求服务器端连接

被动模式：服务器端提供端口号使客户端连接（容易被冒用，但易于在NAT模式下是哟能够）

3、邮件传输协议（SMTP、POP3、IMAP4）的工作原理、MUA、MTA和MDA的定义

发件人 -- SMTP -->发送方服务器 -- SMTP --> 接收方服务器 -- POP3 --> 收件人

SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）

TCP连接，端口号：25（明文），465（SSL加密）

遵循流范式、使用文本控制信息、只传送文本消息、发送一个给定消息的副本、允许客户端列出用户，然后向列表中所有用户发送消息的单个副本（允许副本再发到多个目的地）

连接建立 -- 邮件传送 -- 连接释放

用命令在MTA客户端和MTA服务器端传输消息

命令格式：KEYWORD: INFO（关键字 + ": " + 信息）

响应（服务器端到客户端）：三位数的代码，后面可能有额外的文本信息

POP3（邮局协议）

TCP连接，端口号：110（明文），995（POP3S，SSL加密）

允许用户通过PC机动态地检索邮件服务器上的邮件

授权状态：验证用户名、密码

事务状态：检索邮件、删除（做删除标记）邮件等

更新状态（QUIT命令后）：删除标记邮件，关闭TCP连接，释放资源，会话结束

阅读邮件时可以不上网

IMAP4（Internet Mail Access Protocol，Internet邮件访问协议）

端口号143（明文），993（IMAPS，SSL加密）

三种工作模式：离线、在线和断连

不支持下载邮件**内容**，可以同时多个用户访问服务器

MUA（Mail User Agent，邮件用户代理）

帮助用户读取、编写、回复文件，再将这些信息转给MTA发送

MTA（Mail Transport Agent，邮件传输代理）

把邮件从一个服务器传到另一个服务器或邮件投递代理

MDA（Mail Delivery Agent，邮件投递代理）

将MTA接受的邮件，根据收件人地址投放到用户的邮箱里；在投放过程中，还可以进行邮件过滤、自动回复等功能

MIME（Multipurpose Internet Mail Extensions）

允许SMTP发送非ASCII数据的补充协议

在接收端服务器的SMTP接受ASCII数据后转换为原始数据

邮件性质：

Text：文本

Multipart：连接消息体的多个部分构成一个消息

Application：应用程序、二进制数据

Message：包装一个E-mail消息

Image：静态图片

Audio：音频

Video：动态影像数据、音视频

Base64编码

每6个二进制位解释成一个打印字符

0 - 25：A - Z；26 - 51：a - z；52 - 61：0 - 9；62：-；63：/

4、域名系统（DNS）工作原理

域名系统（Domain Name System，DNS）提供了将人类可读符号域名映射到**计算机地址**的服务

分布式：

名字到IP地址的解析由若干个域名服务器程序完成

域名服务器程序在专设的节点上运行，运行该程序的机器称为域名服务器

域名：因特网上的主机/路由器所具有的唯一的层次结构的名字

层次树状结构：由标号序列组成，各标点之间用点隔开

从后往前依次为：顶级域名-二级域名-三级域名.....

根域名服务器（13个IP地址）（Root Name Server，RNS）：是最重要的域名服务器，存储所有顶级域名服务器的地址信息

顶级域名服务器：管理在该顶级域名服务器注册的所有二级域名

权限域名服务器：负责一个区的域名服务器

本地域名服务器（Local Name Server，LNS）：主机发出DSN查询请求时，查询请求报文就发送给本地域名服务器，对域名系统非常重要

每台主机应该知道本地域名服务器的地址，每台LNS应该知道RNS的地址

查询路径：主机 --> 本地域名服务器 --> 根域名服务器 --> 顶级域名服务器 --> 权限域名服务器 --> 权限域名服务器 --> ...

迭代查询：当一个域名服务器无法得到本地域名服务器的IP地址时，返回本地域名服务器应查询的下一台域名服务器的IP地址

递归查询（较少）：当一个域名服务器无法得到本地域名服务器的IP地址时，以客户端的身份向下一台域名服务器查询

十七、高级专题

1、网络防火墙的基本常识

2、网络安全技术（加密、签名、访问控制、HTTPS、TLS等）的基本常识

3、虚拟专用网络（VPN）、万维网服务器的基本常识

4、对等计算（P2P）模式工作原理

5、内容缓存、Web均衡负载、网络架构的基本常识