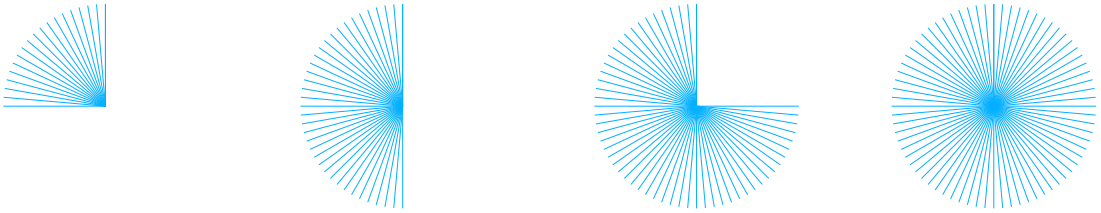
开课吧

计算机硕士

「高频考点」

计算机网络



考研

2016-2021年408统考-计算机网络考点分布									
		2016	2017	2018	2019	2020	2021	选择题	应用题
第一章	考点1-计算机网络的分层结构	33	33		33	33	33	5	
第二章	考点2 - 通信基础概念								
	考点3-奈氏准则/香农定理	34	34					2	
	考点4-编码与调制						34	1	
	考点5数据交换方式					34		1	
	考点6-物理层设备/传输介质			34	34	35		3	
第三章	考点7 -差错控制								
	考点8 - 流量控制/可靠传输/滑动窗口		47	36	35，36	36		4	1
	考点9-介质访问控制	36		35		37			
	考点10-局域网/广域网		35	37				2	
	考点11-链路层设备	35						1	
第四章	考点12-路由算法								
	考点13-1Pv4分组			47			36	1	1
	考点14-1Pv4地址与NAT	38			47	47		1	2
	考点15-子网掩码/子网划分	39	36		37		35	4	
	考点16-CIDR&路由聚合		38	38				2	
	考点17-ARP、 DHCP、ICMP协议								
	考点18-IPv6								
	考点19-路由协议: RIP、 OSPF、 BGP协议	37	37				37	3	
	考点20-IP组播								
	考点21-移动IP								
	考点22-网络层设备								
第五章	考点23-UDP协议/数据报			39			39	2	
	考点24-TCP报文段						39	1	
	考点25-TCP连接管理[必考]	41	39		38，39	39	38	5	1
	考点26-TCP可靠传输						40		
	考点27-TCP流量控制								
	考点28-TCP拥塞控制					38		1	
第六章	考点29-网络应用模型				40			1	
	考点30-域名解析	40				40	47	2	1
	考点31-文件传输协议FTP		40					1	
	考点32-电子邮件系统及相关协议			40				1	
	考点33-WWW与HTTP协议					47			1

编写人：李 超　审核人：于方泽　封面设计：乔宇、刘锦浩、郑悦

勘误信箱:

亲爱的开课吧学员你好，感谢您选择开课吧开启学习之旅。在使用这份学习资料时，希望你能感受到开课吧全体教职人员的用心。经过软件人工三审三校的资料难免有万分之三的概率出现小差错，我们设立勘误激励邮箱，感谢大家和小开共同成长。在使用本资料的同时，如您火眼金睛发现了小错误。可将资料的名称-页码带图反馈到本邮箱:

kaikeba0104@126.com。一经采纳小开感激不尽。

目　录

第一章 计算机网络体系结构

第二章 物理层

第三章 数据链路层

第四章 网络层

第五章 传输层

第六章 应用层

第一章 计算机网络体系结构

结构与模型

ISO/OSI 参考模型（七层）

自下而上：物理层(1)->数据链路层(2)->网络层(3)->运输层(4)->会话层(5)->表示层(6)->应用层(7)

TCP/IP 参考模型（四层）

自下而上：网际接口层(1)->网际层 IP(2)->运输层(TCP 或 UDP)(3)->应用层(4)

五层结构模型

自下而上：物理层(1)->数据链路层(2)->网络层(3)->运输层(4)->应用层(5)

第二章 物理层

奈奎斯特定理

具体的信道所能通过的频率范围总是有限的。所以信号中许多高频分量无法通过信道，所以在传输的过程中会衰减，导致在接收端收到的信号波形失去码元之间的清晰界限，以上现象是码间串扰。为了保证在不出现码间串扰的条件下的码元传输速率最大，提出了奈奎斯特定理。

公式：

$$C_{max} = f_{采样} \times \log_2 N = 2f \times \log_2 N\ (bit/s)$$

极限数据率：

$$理想低通信道下的极限数据传输速率 = 2W \log_2 W \quad (单位\ b/s)$$

结论：

任何信道中，码元传输速率是有上线的。若传输速率超过此上线，就会出现严重的码间串扰问题，使得接收端不可能完全正确认识码元。

信道的频带越宽(即通过的信号高频分量越多)。就可用更高的速率进行码元的有效传输。

奈氏准则给出了码元传输速率的限制，但并未对信息传输速率给出限制，即未对一个码元可以对应多少个二进制位给出限制。

香农定理

给出了带宽受限且有高斯白噪声干扰的信道的极限数据传输率，当用此速率进行传输时，可以做到不产生误差。

公式（引入信噪比后）：

$$信道的极限数据传输率 = W \times \log_2 (1 + S/N) \quad (单位\ b/s)$$

W 为信道的带宽，S 为信道所传输信号的平均功率，N 为信道内部的高斯噪声功率。S/N 为信噪比，及信号的平均功率与噪声的平均功率之比。

信噪比：

$$信噪比(dB) = 10\log_{10}(S/N) \quad (单位\ dB)$$

结论：

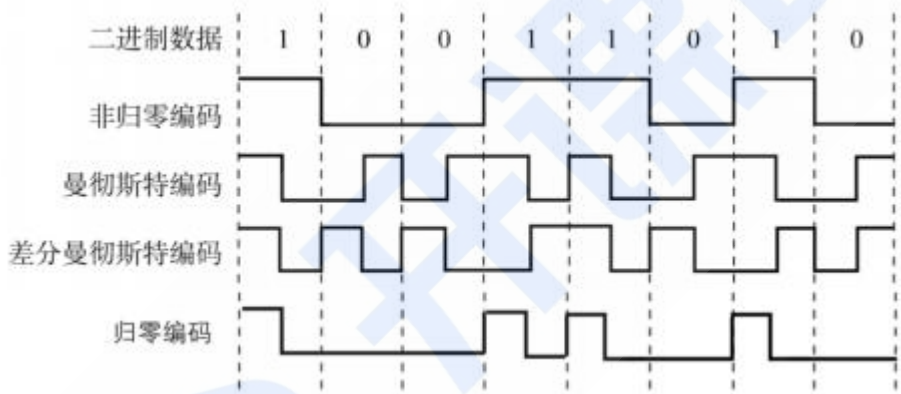
信道的带宽或信道中的信噪比越大，信息的极限传输速率越高。

对一定的传输带宽和一定的信噪比，信息传输速率的上限是确定的。

只要信息的传输速率低于信道的极限传输速率，就能找到某种方法来实现无差错的传输。

香农定理得出的是极限信息传输速率，实际信道能达到的传输速率要比它低不少。

编码与调制



非归零编码

高 1 低 0

曼彻斯特编码

将一个码元分成两个相等的间隔，前一个间隔为低电平后一个间隔为高电平表示码元 1；码元 0 则正好相反。也可以采用相反的规定。

差分曼彻斯特编码（同 1 异 0）

常用于局域网传输，其规则是：若码元为 1，则前半个码元的电平与上一个码元的后半个码元的电平相同，若为 0，则相反。

归零编码

信号电平在一个码元之内都要恢复到零的编码方式

传输介质

以太网比较常用的传输介质包括同轴电缆、双绞线和光纤三种，以 IEEE 802.3 委员会习惯用类似于 10Base-T 的方式进行命名。这种命名方式由三个部分组成：

（1）10：表示速率，单位是 Mb/s。

（2）Base：表示传输机制，Base 代表基带，Broad 代表宽带。

（3）T：传输介质，T 表示双绞线、F 表示光纤、数字代表铜缆的最大段长。

双绞线

是最常用的古老传输介质，它由两根采用一定规则并排绞合的、相互绝缘的铜导线组成。绞合可以减少对相邻导线的电磁干扰。位了进一步提高抗电磁干扰能力，可在双绞线的外面再加上一个由金属丝编织成的屏蔽层，这就是屏蔽双绞线(STP)。无屏蔽层的双绞线称为非屏蔽双绞线(UTP)。

同轴电缆

同轴电缆由内导体、绝缘层、网状编织屏蔽层和塑料外层构成，

光纤

光纤通信就是利用光导纤维(简称光纤)传递光脉冲来进行通信。有光脉冲表示 1，无光脉冲表示 0。可见光的频率约为 108MHz，因此光纤通信系统的带宽范围极大。光纤主要由纤心和包层构成，光波通过纤心进行传导，包层较纤心有较低的折射率。当光线从高折射率的介质射向低折射率的介质时，其折射角大于入射角。因此，如果入射角足够大，那么就会出现全反射，即光线碰到包层时会折射回纤心，这个过程不断重复，光也就沿着光纤传输下去。

无线传输介质

1）无线电波：无线电波具有较强的穿透能力，可以传输很长的距离，所以它被广泛应用于通信领域，如无线手机通信、计算机网络中的无线局域网(WLAN)等。

2）微波、红外线和激光：目前高带宽的无线通信主要使用三种技术：微波、红外线和激光。它们都需要发送方和接收方之间存在一条视线(Line-of-sight）通路，有很强的方向性，都沿直线传播，有时统称这三者为视线介质。

第三章 数据链路层

滑动窗口

滑动窗口有以下重要特性：

1）只有接收窗口向前滑动（同时接收方发送了确认帧）时，发送窗口才有可能（只有发送方收到确认帧后才一定）向前滑动；

2）从滑动窗口的概念看，停止-等待协议、后退况帧协议和选择重传协议只在发送窗口大小与接收窗口大小上有所差别：

停止−等待协议：发送窗口大小=1,接收窗口大小=1。

后退 N 帧协议：发送窗口大小＞1,接收窗口大小=1。

选择重传协议：发送窗口大小＞1，接收窗口大小＞1。

3）接收窗口的大小为 1 时，可保证帧的有序接收。

4）数据链路层的滑动窗口协议中，窗口的大小在传输过程中是固定的（注意与第 5 章传输层的滑动窗口协议的区别）。

介质访问控制

信道划分介质访问控制

信道划分介质访问控制将使用介质的每个设备与来自同一通信信道上的其他设备的通信隔 离开来，把时域和频域资源合理地分配给网络上的设备。

a）频分多路复用

b）时分多路复用

c）码分多路复用

码片、反码片、码片正交

d）波分多路复用

第四章 网络层

IP 协议

IP 数据报的格式

IP 数据报首部

IP 首部的部分重要字段含义如下：

a)版本。指 IP 的版本，目前广泛使用的版本号为 4。

b)首部长度。占 4 位。以 32 位为单位，最大值为 60B（15x4B）。最常用的首部长度是 20B， 此时不使用任何选项（即可选字段）。

c)总长度。占 16 位。指首部和数据之和的长度，单位为字节，因此数据报的最大长度为 216−1=65535B。以太网帧的最大传送单元（MTU）为 1500B，因此当一个 IP 数据报封装成帧时，数据报的总长度（首部加数据）一定不能超过下面数据链路层的 MTU 值。

d)标识。占 16 位。它是一个计数器，每产生一个数据报就加 1，并赋值给标识字段。但它并不是“序号”（因为 IP 是无连接服务）。当一个数据报的长度超过网络的 MTU 时，必须分片，此时每个数据报片都复制一次标识号，以便能正确重装成原来的数据报。

e)标志。占 3 位。标志字段的最低位为 MF，MF=1 表示后面还有分片，MF=0 表示最后一个分片。标志字段中间的一位是 DF，只有当 DF=0 时才允许分片。

f)片偏移。占 13 位。它指出较长的分组在分片后，某片在原分组中的相对位置。片偏移以 8 个字节为偏移单位，即每个分片的长度一定是 8B（64 位）的整数倍。

g)首部校验和。占 16 位。IP 数据报的首部校验和只校验分组的首部，而不校验数据部分。

h)生存时间(TTL)。占 8 位。数据报在网络中可通过的路由器输的最大值，标识分组在网络中的寿命，以确保分组不会永远在网络中循环。路由器在转发分组前，先把 TTL 减 1。若 TTL 被减为 0，则该分组必须丢弃。

i)协议。占 8 位。指出此分组携带的数据使用何种协议，即分组的数据部分应交给哪个传输层协议，如 TCP、UDP 等。其中值为 6 表示 TCP，值为 17 表示 UDP。

j)源地址字段。占 4B,标识发送方的 IP 地址。

k)目的地址字段。占 4B，标识接收方的 IP 地址。

2）IP 数据报分片

一个链路层数据报能承载的最大数据量称为最大传送单元（MTU）。因为 IP 数据报被封装在链路层数据报中，因此链路层的 MTU 严格地限制着 IP 数据报的长度，而且在 IP 数据报的源与目的地路径上的各段链路可能使用不同的链路层协议，有不同的 MTU。例如，以太网的 MTU 为 1500B,而许多广域网的 MTU 不超过 576B。当 IP 数据报的总长度大于链路 MTU 时，就需要将 1P 数据报中的数据分装在两个或多个较小的 IP 数据报中，这些较小的数据报称为片。

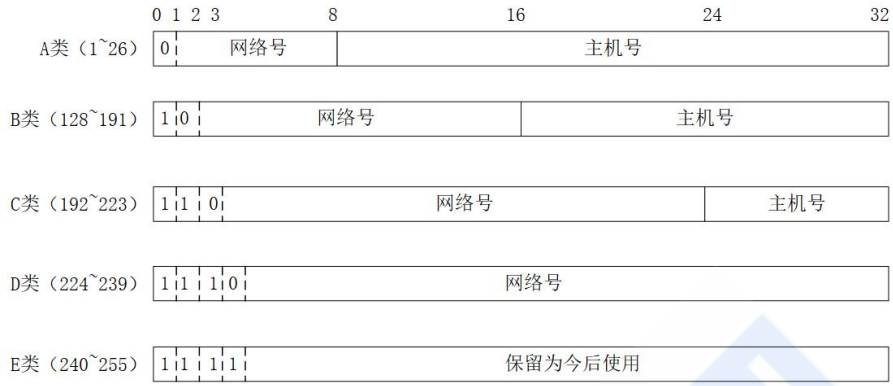
片在目的地的网络层被重新组装。目的主机使用 IP 首部中的标识、标志和片偏移字段来完成对片的重组。创建一个 IP 数据报时，源主机为该数据报加上一个标识号。当一个路由器需要将一个数据报分片时，形成的每个数据报（即片）都具有原始数据报的标识号。当目的主机收到来自同一发送主机的一批数据报时，它可以通过检查数据报的标识号来确定哪些数据报属于同一个原始数据报的片。IP 首部中的标志位有 3 比特，但只有后 2 比特有意义，分别是 MF 位（More Fragment）和 DF 位（Don't Fragment）。只有当 DF=0 时，该 IP 数据报才可以被分片。MF 则用来告知目的主机该 IP 数据报是否为原始数据报的最后一个片。当 MF=1 时，表示相应的原始数据报还有后续的片；当 MF=0 时，表示该数据报是相应原始数据报的最后一个片。目的主机在对片进行重组时，使用片偏移字段来确定片应放在原始 IP 数据报的哪个位置。

IPv4 地址与 NAT

IP 地址

连接到因特网上的每台主机（或路由器）都分配一个 32 比特的全球唯一标识符，即 IP 地址。传统的 IP 地址是分类的地址，分为 A、B、C、D、E 五类。

无论哪类 IP 地址，都由网络号和主机号两部分组成。即 IP 地址::={＜网络号＞，＜主机号＞}。其中网络号标志主机（或路由器）所连接到的网络。一个网络号在整个因特网范围内必须是唯一的。主机号标志该主机（或路由器）。一台主机号在它前面的网络号所指明的网络范围内必须是唯一的。由此可见，一个 IP 地址在整个因特网范围内是唯一的。



在各类 IP 地址中，有些 IP 地址具有特殊用途，不用做主机的 IP 地址：

a)主机号全为 0 表示本网络本身，如 202.98.174.0。

b)主机号全为 1 表示本网络的广播地址.又称直接广播地址.如 202.98.174.255。

c)127.0.0.0 保留为环路自检（Loopback Test）地址，此地址表示任意主机本身，目的地址为环回地址的 IP 数据报永远不会出现在任何网络上。

d)32 位全为 0，即 0.0.0.0 表示本网络上的本主机。

32 位全为 1，即 255.255.255.255 表示整个 TCP/IP 网络的广播地址，又称受限广播地址。 实际使用时，由于路由器对广播域的隔离，255.255.255.255 等效为本网络的广播地址。

网络地址转换（NAT）

网络地址转换（NAT）是指通过将专用网络地址（如 Intranet）转换为公用地址（如 Internet），从而对外隐藏内部管理的 IP 地址。它使得整个专用网只需要一个全球 IP 地址就可以与因特网连通，由于专用网本地 IP 地址是可重用的，所以 NAT 大大节省了 IP 地址的消耗。同时，它隐藏了内部网络结构，从而降低了内部网络受到攻击的风险。

此外，为了网络安全，划出了部分 IP 地址为私有 IP 地址。私有 IP 地址只用于 LAN，不用于 WAN 连接（因此私有 IP 地址不能直接用于 Internet，必须通过网关利用 NAT 把私有 IP 地址转换为 Internet 中合法的全球 IP 地址后才能用于 Internet），并且允许私有 IP 地址被 LAN 重复使用。这有效地解决了 IP 地址不足的问题。私有 IP 地址网段如下：

A 类：1 个 A 类网段，即 10.0.0.0～10.255.255.255。

B 类：16 个 B 类网段，即 172.16.0.0～172.31.255.255。

C 类：256 个 C 类网段，即 192.168.0.0～192.168.255.255。

子网掩码与子网划分

子网掩码

子网掩码是一个与 IP 地址相对应的、长 32bit 的二进制串，它由一串 1 和跟随的一串 0 组成。其中，1

对应于 IP 地址中的网络号及子网号，而 0 对应于主机号。计算机只需将 1P 地址和其对应的子网掩码逐位“与”（逻辑 AND 运算），就可得出相应子网的网络地址。

1）在使用子网掩码的情况下：

a)一台主机在设置 IP 地址信息的同时，必须设置子网掩码。

b)同属于一个子网的所有主机及路由器的相应端口，必须设置相同的子网掩码。

c)路由器的路由表中，所包含信息的主要内容必须有目的网络地址、子网掩码、下一跳地址。

2）使用子网掩码时路由器的分组转发算法如下：

d)从收到的分组的首部提取目的 IP 地址，记为 D。

e)先判断是否为直接交付。对路由器直接相连的网络逐个进行检查：用各网络的子网掩码和 D 逐位相“与”，看结果是否和相应的网络地址匹配。若匹配，则将分组直接交付，否则间接交付，执行步骤 3。

f)若路由表中有目的地址为 D 的特定主机路由，则将分组传送给路由表中所指明的下一跳 路由器；否则，执行 4。

g)对路由表中的每一行（目的网络地址、子网掩码、下一跳地址）中的子网掩码和逐位相“与”，其结果为 N。若况与该行的目的网络地址匹配，则将分组传送给该行指明的下一跳路由器；否则，执行步骤 5。

h)若路由表中有一个默认路由，则将分组传送给路由表中所指明的默认路由器；否则，执行步骤 6。

i)报告转发分组出错。

无分类域间路由选择（CIDR）

无分类域间路由选择是在变长子网掩码的基础上提出的一种消除传统 A、B、C 类网络划分，并且可以在软件的支持下实现超网构造的一种 IP 地址的划分方法。

1）CIDR 的主要特点如下：

a)消除了传统 A、B,C 类地址及划分子网的概念，因而可以更有效地分配 IPv4 的地址空间。CIDR 使用“网络前缀”的概念代替子网络的概念。因此，IP 地址的无分类两级编址为：IP：：={＜网络前缀〉，〈主机号＞}。

CIDR 还使用“斜线记法”（或称 CIDR 记法），即 IP 地址／网络前缀所占比特数。其中，网络前缀所占比特数对应于网络号的部分，等效于子网掩码中连续 1 的部分。

b)将网络前缀都相同的连续 IP 地址组成“CIDR 地址块”。一个 C1DR 地址块可以表示很多地址，这种地址的聚合称为路由聚合，或称构成超网。路由聚合使得路由表中的一个项目可以表示多个原来传统分类地址的路由，有利于减少路由器之间的路由选择信息的交换，从而提高网络性能。

c)CIDR 的优点在于网络前缀长度的灵活性。由于上层网络的前缀长度较短，因此相应的路由表的项目较少。而内部又可采用延长网络前缀的方法来灵活地划分子网。最长前缀匹配（最佳匹配）：使用 CIDR 时，路由表中的每个项目由“网络前缀”和“下一跳地址”组成。在查找路由表时可能会得到不止一个匹配结果。此时，应当从匹配结果中选择具有最长网络前缀的路由，因为网络前缀越长，其地址块就越小，因而路由就越具体。

CIDR 查找路由表的方法：为了更加有效地查找最长前缀匹配，通常将无分类编址的路由表存放在一种

层次的数据结构中，然后自上而下地按层次进行查找。这里最常用的数据结构就是二叉线索。

子网划分

1）子网划分的基本思路如下：

a）子网划分纯属一个单位内部的事情。单位对外仍然表现为没有划分子网的网络。

b）从主机号借用若干比特作为子网号，当然主机号也就相应减少了相同的比特。三级 IP 地址的结构如下：IP 地址={＜网络号＞，＜子网号＞，＜主机号＞}。

c）凡是从其他网络发送给本单位某台主机的 IP 数据报，仍然是根据 IP 数据报的目的网络号，先找到连接到本单位网络上的路由器。然后该路由器在收到 IP 数据报后，按目的网络号 和子网号找到目的子网。最后把 IP 数据报直接交付给目的主机。

2）注意

a)划分子网只是把 IP 地址的主机号这部分进行再划分，而不改变 IP 地址原来的网络号。因此，从一个 IP 地址本身或 IP 数据报的首部，无法判断源主机或目的主机所连接的网络是否进行了子网划分。

b)RFC950 规定，对分类的 IPv4 地址进行子网划分时，子网号不能为全 1 或全 0。但随着 CIDR 的广泛使用，现在全 1 和全 0 的子网号也可使用，但一定要谨慎使用，要弄清你的路由器所用的路由选择软件是否支持全 0 或全 1 的子网号。

c)不论是分类的 IPv4 地址还是 CIDR，其子网中的主机号为全 0 或全 1 的地址都不能被指派。子网中主机号全 0 的地址为子网的网络号，主机号全 1 的地址为子网的广播地址。

路由协议与算法

路由信息协议（RIP）

路由信息协议（Routing Information Protocol，RIP）是内部网关协议（IGP）中最先得到广泛应用的协议。R1P 是一种分布式的基于距离向撤的路由选择协议，其最大优点就是简单。

1）RIP 规定

a)网络中的每个路由器都要维护从它自身到其他每个目的网络的距离记录（因此这是一组离，称为距离向量）；

b)距离也称跳数（Hop Count），规定从一个路由器到直接连接网络的距离（跳数）为 1。而每经过一个路由器，距离（跳数）加 1；

c)RIP 认为好的路由就是它通过的路由器的数目少，即优先选择跳数少的路径

d)RIP 允许一条路径最多只能包含 15 个路由器（即最多允许 15 跳）。因此距离等于 16 时，它表示网络不可达。可见 RIP 只适用于小型互联网。距离向 i 路由可能会出现环路的情况，规定路径上的最高跳数的目的是为了防止数据报不断循环在环路上，减少网络拥塞的可能性；

e)RIP 默认在任意两个使用 RIP 的路由器之间每 30 秒广播一次 RIP 路由更新信息，以便自动建立并维护

路由表（动态维护）；

f)在 RIP 中不支持子网掩码的 RIP 广播，所以 RIP 中每个网络的子网掩码必须相同。但在新的 R1P2 中，支持变长子网掩码和 CIDR。

2）RIP 特点

a)仅和相邻路由器交换信息；

b)路由器交换的信息是当前路由器所知道的全部信息，即自己的路由表；

c)按固定的时间间隔交换路由信息，如每隔 30 秒。

3）距离向量算法

每个路由表项目都有三个关键数据：＜目的网络 N，距离 d，下一跳路由器义 X＞。对于每个相邻路由器发送过来的 RIP 报文，执行如下步骤：

a)对地址为 X 的相邻路由器发来的 RIP 报文，先修改此报文中的所有项目：把“下一跳”字段中的地址都改为 X，并把所有“距离”字段的值加 1；

b)对修改后的 RIP 报文中的每个项目，执行如下步骤：

①当原来的路由表中没有目的网络况时，把该项目添加到路由表中；

②当原来的路由表中有目的网络 M，且下一跳路由器的地址是 X 时，用收到的项目替换原路由表中的项目；

③当原来的路由表中有目的网络 N，且下一跳路由器的地址不是 X 时，如果收到的项目中的距离 d 小于路由表中的距离，那么就用收到的项目替换原路由表中的项目；否则什么也不做；

c)如果 180 秒（RIP 默认超时时间为 180 秒）还没有收到相邻路由器的更新路由表，那么把此相邻路由器记为不可达路由器，即把距离设置为 16（距离为 16 表示不可达）；

d)返回

RIP 最大的优点是实现简单、开销小、收敛过程较快。

RIP 的缺点如下：

a)R1P 限制了网络的规模，它能使用的最大距离为 15（16 表示不可达）

b)路由器之间交换的是路由器中的完整路由表，因此网络规模越大，开销也越大

c)网络出现故障时，会出现慢收敛现象（即需要较长时间才能将此信息传送到所有路由器），俗称“坏消息传得慢”，使更新过程的收敛时间长

开放最短路径优先(OSPF)

1）OSPF 协议的基本特点

OSPF 与 RIP 相比有以下 4 点主要区别：

a)OSPF 向本自治系统中的所有路由器发送信息，这里使用的方法是洪泛法。而 RIP 仅向自己相邻的几个路由器发送信息

b)发送的信息是与本路由器相邻的所有路由器的链路状态，但这只是路由器所知道的部分信息。“链路

状态"说明本路由器和哪些路由器相邻及该链路的"度量"（或代价）。而在 RIP 中，发送的信息是本路由器所知道的全部信息，即整个路由表

c)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此信息，并且更新过程收敛得快，不会出现 RIP"坏消息传得慢"的问题。而在 RIP 中，不管网络拓扑是否发生变化，路由器之间都会定期交换路由表的信息

d)OSPF 是网络层协议，它不使用 UDP 或 TCP，而直接用 IP 数据报传送（其 IP 数据报首 部的协议字段为 89）。而 RIP 是应用层协议，它在传输层使用 UDP。

2）OSPF 还有以下特点：

a)OSPF 对不同的链路可根据 IP 分组的不同服务类型（TOS）而设置成不同的代价。因此，OSPF 对于不同类型的业务可计算出不同的路由，十分灵活

b)如果到同一个目的网络有多条相同代价的路径，那么可以将通信量分配给这几条路径。 这称为多路径间的负载平衡

c)所有在 OSPF 路由器之间交换的分组都具有鉴别功能，因而保证了仅在可信赖的路由器 之间交换链路状态信息

d)支持可变长度的子网划分和无分类编址 CIDR

e)每个链路状态都带上一个 32 位的序号，序号越大，状态就越新

3）五种分组类型：

a)问候分组，用来发现和维持邻站的可达性

b)数据库描述分组，向邻站给出自己的链路状态数据库中的所有链路状态项目的摘要信息

c)链路状态请求分组，向对方请求发送某些链路状态项目的详细信息

d)链路状态更新分组，用洪泛法对全网更新链路状态

e)链路状态确认分组，对链路更新分组的确认

边界网关协议(BGP)

边界网关协议（BorderGatewayProtocol，BGP）是不同自治系统的路由器之间交换路由信息的协议，是一种外部网关协议。边界网关协议常用于互联网的网关之间。路由表包含已知路由器的列表、路由器能够达到的地址及到达每个路由器的路径的跳数。

内部网关协议主要设法使数据报在一个 AS 中尽可能有效地从源站传送到目的站。在一个 AS 内部不需要考虑其他方面的策略。然而 BGP 使用的环境却不同，主要原因如下：

a)因特网的规模太大，使得自治系统之间路由选择非常困难

b)对于自治系统之间的路由选择，要寻找最佳路由是很不现实的

c)自治系统之间的路由选择必须考虑有关策略

1）BGP 的特点如下：

a)BGP 交换路由信息的结点数量级是自治系统的数量级，要比这些自治系统中的网络数少很多

b)每个自治系统中 BGP 发言人（或边界路由器）的数目是很少的。这样就使得自治系统之间的路由选择不致过分复杂。

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

d)在 BGP 刚运行时，BGP 的邻站交换整个 BGP 路由表，但以后只需在发生变化时更新有 变化的部分。这样做对节省网络带宽和减少路由器的处理开销都有好处

2）BGP—4 共使用 4 种报文

a)打开（Open）报文。用来与相邻的另一个 BGP 发言人建立关系

b)更新（Update）报文。用来发送某一路由的信息，以及列出要撤销的多条路由

c)保活（Keepalive） 报文。用来确认打开报文并周期性地证实邻站关系。

d)通知（Notification）报文。用来发送检测到的差错。

<table>
<tr><td>协议</td><td>RIP</td><td>OSPF</td><td colspan="2">BGP</td></tr>
<tr><td>类型</td><td>内部</td><td>内部</td><td colspan="2">外部</td></tr>
<tr><td>路由算法</td><td>距离—向量</td><td>链路状态</td><td colspan="2">路径—向量</td></tr>
<tr><td>传递协议</td><td>UDP</td><td>IP</td><td colspan="2">TCP</td></tr>
<tr><td>路径选择</td><td>跳数最少</td><td>代价最低</td><td colspan="2">较好，非最佳</td></tr>
<tr><td>交换结点</td><td>和本结点相邻的路由器</td><td>网络中的所有路由器</td><td colspan="2">和本结点相邻的路由器</td></tr>
<tr><td rowspan="2">交换内容</td><td rowspan="2">当前本路由器知道的全部信息，即自己的路由表</td><td rowspan="2">与本路由器相邻的所有路由器的链路状态</td><td>首次</td><td>整个路由表</td></tr>
<tr><td>非首次</td><td>有变化的部分</td></tr>
</table>

第五章 传输层

UDP 数据报

UDP 的首部格式

UDP 数据报包含两部分： UDP 首部和用户数据，UDP 首部有 8B，由 4 个字段组成，每个字段的长度都是 2B，各字段意义如下：

1）源端口。源端口号。在需要对方回信时选用，不需要时可用全 0。

2）目的端口。目的端口号。这在终点交付报文时必须使用到。

3）长度。UDP 数据报的长度（包括首部和数据），其最小值是 8 （仅有首部）。

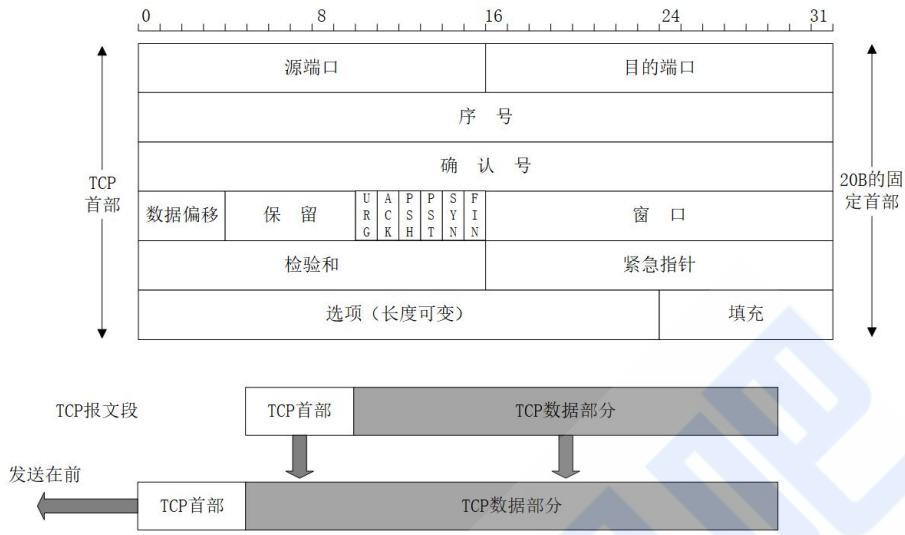
4）校验和。检测 UDP 数据报在传输中是否有错。有错就丢弃。该字段是可选的，当源主机不想计算校验和时，则直接令该字段为全 0。

TCP 报文段

TCP 传送的数据单元称为报文段。TCP 报文段既可以用来运载数据，又可以用来建立连接、释放连接和应答。一个 TCP 报文段分为 TCP 首部和数据两部分，整个 TCP 报文段作为 IP 数据报的数据部分封装在 IP 数据报中，如图 5.6 所示。其首部的前 20B 是固定的。TCP 报文段的首部最短为 20B，后面有 4N 字节是根据需要而增加的选项，通常长度为 4B 的整数倍。

TCP 的首部格式

TCP 的全部功能体现在其首部的各个字段中，各字段意义如下：



1）源端口和目的端口字段。各占 2B。端口是运输层与应用层的服务接口，运输层的复用和分用功能都要通过端口实现。

2）序号。占 4B，范围为 0~232−1，共 232 个序号。TCP 是面向字节流的（即 TCP 传送时是逐个字节传送的），所以 TCP 连接传送的数据流中的每个字节都按顺序编序。序号字段的值指的是本报文段所发送的数据的第一个字节的序号。

例如，一报文段的序号字段值是 301，而携带的数据共有 100B，表明本报文段的数据的最后一个字节的序号是 400，因此下一个报文段的数据序号应从 401 开始。

3）确认号。占 4B，是期望收到对方的下一个报文段的数据的第一个字节的序号。若确认号为 N，则表明到序号 N~ 1 为止的所有数据都已正确收到。 例如，B 正确收到了 A 发送过来的一个报文段，其序号字段是 501，而数据长度是 200B（序号 501～700），这表明 B 正确收到了 A 发送的到序号 700 为止的数据。因此 B 期望收到 A 的下一个数据序号是 701，于是 B 在发送给 A 的确认报文段中把确认号置为 701。

4）数据偏移（即首部长度）。占 4 位，这里不是 IP 数据报分片的那个数据偏移，而是表示首部长度，它指出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远。“ 数据偏移” 的单位是 32 位（以 4B 为计算单位）。因此当此字段的值为 15 时，达到 TCP 首部的最大长度 60 B。

5）保留。占 6 位，保留为今后使用，但目前应置为 0。

6）紧急位 URG。URG = 1 时，表明紧急指针字段有效。它告诉系统报文段中有紧急数据，应尽快传送（相当于高优先级的数据）。但 URG 需要和紧急指针配套使用，即数据从第一个字节到紧急指针所指字节就是紧急数据。

7）确认位 ACK。只有当 ACK = 1 时确认号字段才有效。当 ACK = 0 时，确认号无效。TCP 规定，在连接建立后所有传送的报文段都必须把 ACK 置 1。

8）推送位 PSH（Push）。接收 TCP 收到 PSH = 1 的报文段，就尽快地交付给接收应用进程，而不再等到整个缓存都填满后再向上交付。

9）复位位 RST（Reset）。RST=1 时，表明 TCP 连接中出现严重差错（如主机崩溃或其他原因），必须释放连接，然后再重新建立运输连接。

10）同步位 SYN。同步 SYN=1 表示这是一个连接请求或连接接收报文。 当 SYN= 1，ACK = 0 时，表明这是一个连接请求报文，对方若同意建立连接，则在响应报文中使用 SYN=1，ACK = 1。即 SYN=1 表示这是一个连接请求或连接接收报文。

11）终止位 FIN（Finish）。用来释放一个连接。FIN = 1 表明此报文段的发送方的数据已发送完毕，并要求释放传输连接。

12）窗口。占 2B，范围为 0~−1。它指出现在允许对方发送的数据量，接收方的数据缓存空间是有限的，因此用窗口值作为接收方让发送方设置其发送窗口的依据。 例如，假设确认号是 701，窗口字段是 1000 。这表明，从 701 号算起，发送此报文段的一方还有接收 1000 字节数据（字节序号为 701−1700）的接收缓存空间。

13）校验和。占 2B。校验和字段检验的范围包括首部和数据两部分。在计算校验和时，和 UDP 一样，要在 TCP 报文段的前面加上 12B 的伪首部（只需将 UDP 伪首部的第 4 个字段，即协议字段的 17 改成 6，其他的和 UDP 一样）。

14）紧急指针。占 2B。紧急指针仅在 URG = 1 时才有意义，它指出在本报文段中紧急数据共有多少字节急数据在本报文段数据的最前面）。

15）选项。长度可变。TCP 最初只规定了一种选项，即最大报文段长度（Maximum Segment Size，MSS）。MSS 是 TCP 报文段中的数据字段的最大长度（注意仅仅是数据字段）。

16）填充。这是为了使整个首部长度是 4B 的整数倍。

TCP 连接管理

TCP 是面向连接的协议，因此每个 TCP 连接都有三个阶段：连接建立、数据传送和连接释放。TCP 连接的管理就是使运输连接的建立和释放都能正常进行。

在 TCP 连接建立的过程中，要解决以下三个问题：

1） 要使每一方都能够确知对方的存在。

2） 要允许双方协商一些参数（如最大窗口值、是否使用窗口扩大选项、时间戳选项及服务质量等）。

3） 能够对运输实体资源（如缓存大小、连接表中的项目等）进行分配。

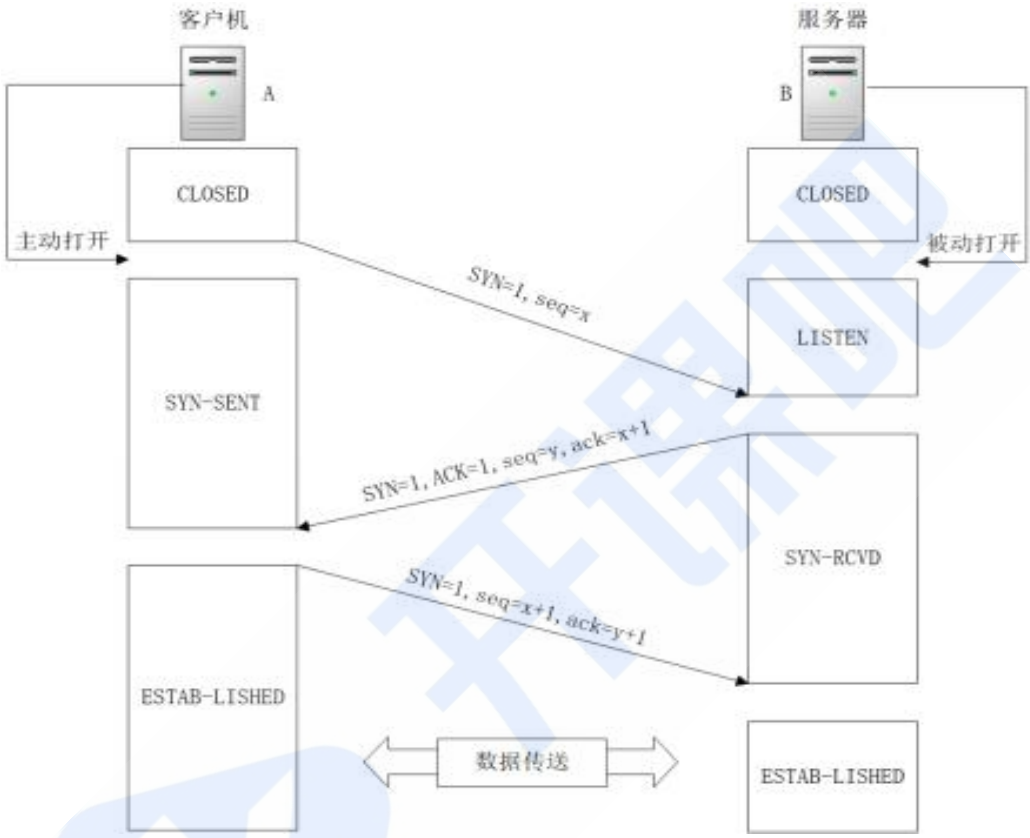
TCP 把连接作为最基本的抽象，每条 TCP 连接有两个端点，TCP 连接的端点不是主机，不是主机的 IP 地址，不是应用进程，也不是传输层的协议端口。TCP 连接的端口称为套接字（socket）或插口。

每条 TCP 连接唯一地被通信两端的两个端点（即两个套接字）确定。

TCP 连接的建立采用客户机/服务器方式。主动发起连接建立的应用进程称为客户机（Client ），而被动等待连接建立的应用进程称为服务器（Server）。

1．TCP 连接的建立

连接的建立经历以下 3 个步骤，通常称为三次握手，如图



连接建立前，服务器进程处于 LISTEN（收听）状态，等待客户的连接请求。

第一步： 客户机的 TCP 首先向服务器的 TCP 发送一个连接请求报文段。这个特殊报文段的首部中的同步位 SYN 置 1，同时选择一个初始序号 seq = x。TCP 规定，SYN 报文段不能携带数据，但要消耗掉一个序号。这时，TCP 客户进程进入 SYN—SENT（同步已发送）状态。

第二步： 服务器的 TCP 收到连接请求报文段后，如同意建立连接，则向客户机发回确认，并为该 TCP 连接分配缓存和变量。在确认报文段中，把 SYN 位和 ACK 位都置 1 ，确认号是 ack = x + 1，同时也为自己选择一个初始序号 seq = y。注意，确认报文段不携带数据，但也要消耗掉一个序号。这时，TCP 服务器进程进入 SYN—RCVD （同步收到）状态。 确认报文段同样不包含应用层数据。

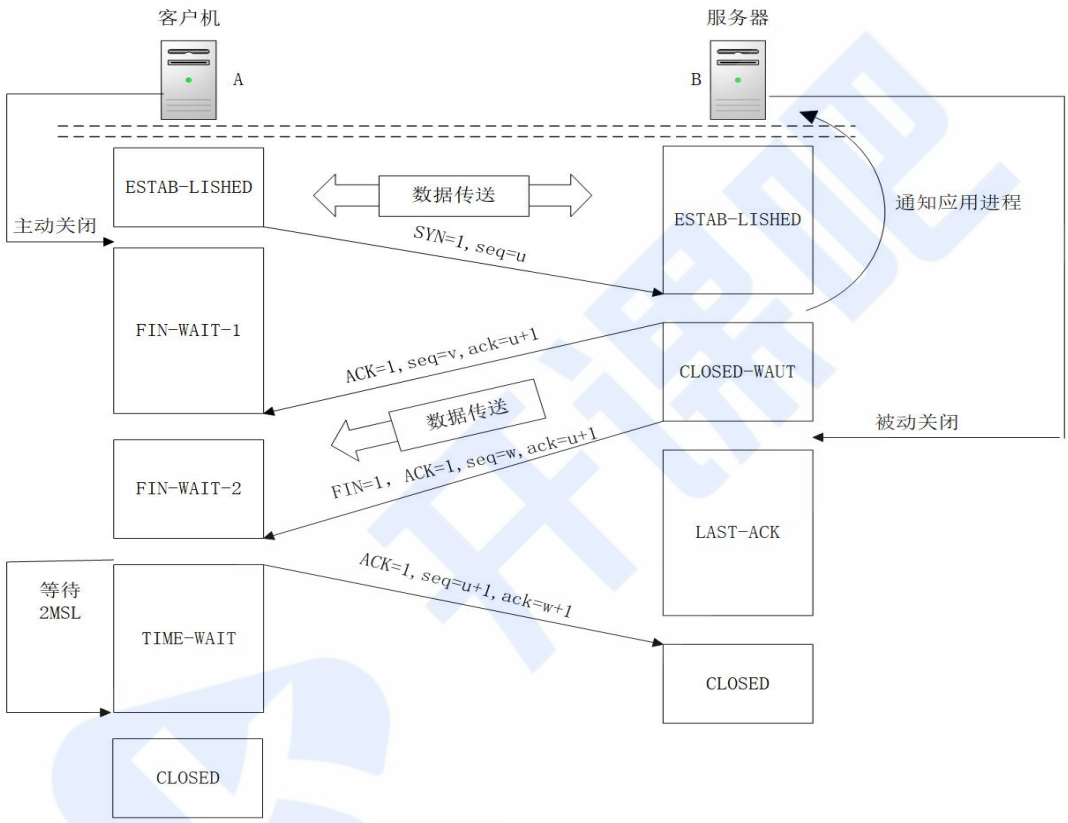
第三步： 当客户机收到确认报文段后，还要向服务器给出确认，并为该连接分配缓存和变量。确认报文段的 ACK 位置 1，确认号 ack = y + 1，序号 seq = x + 1。该报文段可以携带数据，若不携带数据则不消耗序号。这时，TCP 客户进程进入 ESTABLISHED （已建立连接）状态。

成功进行以上三步后，就建立了 TCP 连接，接下来就可以传送应用层数据。TCP 提供的是全双工通信，因此通信双方的应用进程在任何时候都能发送数据。

另外，值得注意的是，服务器端的资源是在完成第二次握手时分配的，而客户端的资源是在完成第三次握手时分配的，这就使得服务器易于受到 SYN 洪泛攻击。

2．TCP 连接的释放

天下没有不散的筵席，TCP 同样如此。参与 TCP 连接的两个进程中的任何一个都能终止该连接。TCP



连接释放的过程通常称为四次握手，如图

第一步： 客户机打算关闭连接时，向其 TCP 发送一个连接释放报文段，并停止发送数据，主动关闭 TCP 连接，该报文段的 终止位 FIN 置 1 ，seq ＝ u ，它等于前面已传送过的数据的最后一个字节的序号加 1，FIN 报文段即使不携带数据，也要消耗掉一个序号。这时，TCP 客户进程进入 FIN-WAIT-1（终止等待 1）状态。TCP 是全双工的，即可以想象为一条 TCP 连接上有两条数据通路。发送 FIN 的一端不能再发送数据，即关闭了其中一条数据通路，但对方还可以发送数据。

第二步： 服务器收到连接释放报文段后即发出确认，确认号是 ack ＝ u ＋ 1，序号 seq ＝ v ，等于它前面已传送过的数据的最后一个字节的序号加 1。然后服务器进入 CLOSE-WAIT（关闭等待）状态。此时，从客户机到服务器这个方向的连接就释放了，TCP 连接处于半关闭状态。但服务器若发送数据，客户机仍要接收，即从服务器到客户机这个方向的连接并未关闭。

第三步： 若服务器已经没有要向客户机发送的数据，就通知 TCP 释放连接，此时其发出 FIN = 1 的连接释放报文段。

第四步： 客户机收到连接释放报文段后，必须发出确认。把确认报文段中的却认为 ACK 置 1 ，确认号 ack = w + 1，序号 seq = u + 1。此时 TCP 连接还未释放，必须经过时间等待计时器设置的时间 2MSL（最长报文段寿命） 后，客户机才进入 CLOSED（连接关闭）状态。

对上述 TCP 连接建立和释放的总结如下：

1）连接建立。分为 3 步：

① SYN = 1，seq=x。

② SYN = 1，ACK = 1，seq = y，ack = x + 1。

③ ACK = 1，seq = x + 1，ack = y + 1。

2）释放连接。分为 4 步：

① FIN= 1，seq = u

② ACK = 1，seq = v，ack = u + 1。

③ FIN = 1，ACK = 1，seq = w，ack = u + 1。

④ ACK = 1，seq = u + 1，ack = w + 1。

选择题喜欢考查（关于连接和释放的题目，ACK、SYN、FIN 一定等于 1），请牢记。

TCP 拥塞控制

因特网建议标准定义了进行拥塞控制的 4 种算法：慢开始、拥塞避免、快重传、快恢复。

发送方在确定发送报文段的速率时，既要根据接收方的接收能力，又要从全局考虑不要使网络发生拥塞。因此，TCP 协议要求发送方维护以下两个窗口：

1）接收窗口 rwnd，接收方根据目前接收缓存大小所许诺的最新窗口值，反映接收方的容量。由接收方根据其放在 TCP 报文的首部的窗口字段通知发送方。

2）拥塞窗口 cwnd，发送方根据自己估算的网络拥塞程度而设置的窗口值，反映网络的当前容量。只要网络未出现拥塞，拥塞窗口就再增大一些，以便把更多的分组发送出去。但只要网络出现拥塞，拥塞窗口就减小一些,以减少注入网络的分组数。

发送窗口的上限值应取接收窗口 rwnd 和拥塞窗口 cwnd 中较小的一个，即

发送窗口的上限值 = min[rwnd，cwnd]

第六章 应用层

网络应用模型

客户/服务器模型（C/S 模型）

在客户/服务器（Client/Server，C/S）模型中，有一个总是打开的主机称为服务器，它服务于许多来

自其他称为客户机的主机请求。其工作流程如下：

1）服务器处于接收请求的状态。

2）客户机发出服务请求，并等待接收结果。

3）服务器收到请求后，分析请求，进行必要的处理，得到结果并发送给客户机。

客户程序必须知道服务器程序的地址，客户机上一般不需要特殊的硬件和复杂的操作系统，而服务器上运行的软件则是专门用来提供某种服务的程序，可同时处理多个远程或本地客户的要求。系统启动后即自动调用并一直不断地运行着，被动地等待并接收来自各地客户的请求。因此，服务器程序不需要知道客户程序的地址。

C/S 模型最主要的特征是：客户是服务请求方，服务器是服务提供方。

1）C/S 模型主要特点：

a)网络中各计算机的地位不平等，服务器可以通过对用户权限的限制来达到管理客户机的目的，使它们不能随意存储/删除数据，或进行其他受限的网络活动。整个网络的管理工 作由少数服务器担当，因此网络的管理非常集中和方便。

b)客户机相互之间不直接通信。

c)可扩展性不佳。受服务器硬件和网络带宽的限制，服务器支持的客户机数有限。

P2P 模型

P2P 模型的思想是整个网络中的传输内容不 再被保存在中心服务器上，每个结点都同时具有下载、上传的功能，其权利和义务都是大体对等的。

在 P2P 模型中，各计算机没有固定的客户和服务器划分。相反，任意一对计算机——称为对等方 (Peer)，直接相互通信。实际上，P2P 模型从本质上来看仍然使用客户/服务器方式，每个结点既作为客户访问其他结点的资源，也作为服务器提供资源给其他结点访问。当前比较流行的 P2P 应用 PPlive、Bittorrent 和电驴等。

1）P2P 模型的优点主要体现如下：

d)减轻了服务器的计算压力，消除了对某个服务器的完全依赖，可以将任务分配到各个结点上，因此大大提高了系统效率和资源利用率

e)多个客户机之间可以直接共享文档

f)可扩展性好，传统服务器有响应和带宽的限制，因此只能接受一定数量的请求

g)网络健壮性强，单个结点的失效不会影响其他部分的结点

2）P2P 模型也有缺点。

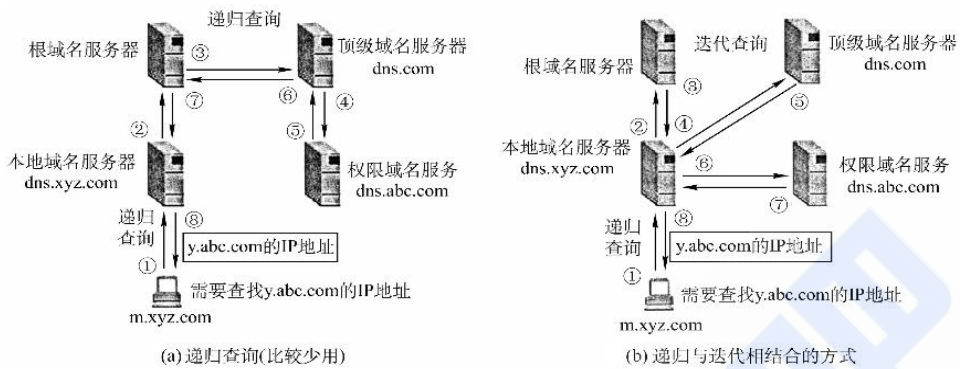
在获取服务的同时，还要给其他结点提供服务，因此会占用较多的内存，影响整机速度。

DNS 域名系统

域名系统概述

域名系统（Domain Name System，DNS）是因特网使用的命名系统，用来把便于人们记忆的具有特定

含义的主机名转换为便于机器处理的 IP 地址。相对于 IP 地址，人们更喜欢使用具有特定含义的字符串来标识因特网上的计算机。 值得注意的是，DNS 系统采用 C/S 模型，其协议运行在 UDP 之上，使用 53 号端口 。



文件传输协议 FTP

文件传输协议 (File Transfer Protocol，FTP)

FTP 是因特网上使用得最广泛的文件传输协议。FTP 提供交互式的访问，允许客户指明文件的类型与格式，并允许文件具有存取权限。它屏蔽了各计算机系统的细节，因而适合于在异构网络中的任意计算机之间传送文件。

FTP 提供以下功能：

a)提供不同种类主机系统（硬、软件体系等都可以不同）之间的文件传输能力。

b)以用户权限管理的方式提供用户对远程 FTP 服务器上的文件管理能力。

c)以匿名 FTP 的方式提供公用文件共享的能力。

FTP 协议工作原理

FTP 采用客户/服务器的工作方式，它使用 TCP 可靠的传输服务。一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：一个主进程，负责接收新的请求；另外有若干从属进程，负责处理单个请求。其工作步骤如下：

1.打开熟知端口 21 （控制端口），使客户进程能够连接上

2.等待客户进程发连接请求

3.启动从属进程来处理客户进程发来的请求。主进程与从属进程并发执行，从属进程对客 户进程的请求处理完毕后即终止

4.回到等待状态，继续接收其他客户进程的请求。

FTP 服务器必须在整个会话期间保留用户的状态信息。特别是服务器必须把指定的用户账户与控制连

接联系起来，服务器必须追踪用户在远程目录树上的当前位置。

超文本传输协议（HTTP）

HTTP 定义了浏览器（万维网客户进程）怎样向万维网服务器请求万维网文档，以及服务器怎样把文档传送给浏览器。从层次的角度看，HTTP 是面向事务的（Transaction—oriented）应用层协议，它规定了在浏览器和服务器之间的请求和响应的格式与规则，是万维网上能够可靠地交换文件（包括文本、声音、图像等各种多媒体文件）的重要基础。

HTTP 的特点：

HTTP 是无状态的。也就是说，同一个客户第二次访问同一个服务器上的页面时，服务器的响应与第一次被访问时的相同。因为服务器并不记得曾经访问过的这个客户，也不记得为该客户曾经服务过多少次。

HTTP 的无状态特性简化了服务器的设计，使服务器更容易支持大量并发的 HTTP 请求。在实际应用中，通常使用 Cookie 加数据库的方式来跟踪用户的活动（如记录用户最近浏览的商品等）。Cookie 是一个存储在用户主机中的文本文件，里面含有一串“识别码”，如“123456”，用于 Web 服务识别用户。Web 服务器根据 Cookie 就能从数据库中查询到该用户的活动记录，进而执行一些个性化的工作，如根据用户之前浏览过的商品向其推荐新产品等。

HTTP 采用 TCP 作为运输层协议，保证了数据的可靠传输。HTTP 不必考虑数据在传输过程中被丢弃后又怎样被重传。但是，HTTP 本身是无连接的（请读者务必注意）。也就是说，虽然 HTTP 使用了 TCP 连接，但通信的双方在交换 HTTP 报文之前不需要先建立 HTTP 连接。

HTTP 既可以使用非持久连接，也可以使用持久连接（HTTP/1.1 支持）。

开课吧

使 命

让每个人都能公平和便利地获取优质教育服务，并实现可持续职业成长

愿 景

打造全球顶尖的人才科技公司，创办一所国际知名大学，成为令人尊敬的企业

价值观

关心并热爱、只为赋能人才、极致敢为、坦诚开放、拥抱变化、始终创业