***第一次课***

* 计算机网络的主要功能

连通性: 上网用户之间可以交换信息

资源共享：信息、软件，硬件

* Internet 与internet区别

internet: 互连网, 是一个通用名词

Internet: 因特网或互联网, 一个专用名词。指当前全球最大的、开放的、由众多网络相互连接而成的特定计算机网络，它采用 TCP/IP 协议族作为通信的规则，且其前身是美国的 ARPANET。

* 什么是Internet?

网络和网络可以通过路由器互联起来，组成一个覆盖范围更大的网络

* ISP分类

根据服务范围和所拥有的IP 地址数目，ISP分为：

主干ISP: 服务面积最大(国家)，拥有高速主干网(≥10Gb/s)

地区ISP：较小的ISP，通过一个或多个主干ISP连接起来，数据率也低一些

本地ISP：给端用户提供直接的服务。可以直接连接到地区ISP,或主干ISP。可以是：仅提过因特网服务的公司 、拥有网络并向自己的雇员提过服务的企业 、运行自己的网络的非盈利机构（大学等）

* 从工作方式看，互联网的组成，各部分的构成成分及作用？

依据工作方式，因特网分为两大块：

边缘部分

* + - 由所有连接在因特网上的主机组成
    - 是用户直接使用的，用来进行通信，资源共享

核心部分

* + - 由大量网络和连接这些网络的路由器组成
    - 是为边缘部分提供服务的（提供连通性和交换）

***第二次课***

* 边缘部分主机的信息交换方式？

客户−服务器方式（ Client/Server-- C/S 方式）

对等方式（ Peer-to-Peer -- P2P 方式）

* 什么是电路交换？

经过以下三个步骤的交换方式称为电路交换

建立连接（占用通信资源）

通信（一直占用通信资源）

释放连接（归还通信资源）

* 报文交换的数据传送单位，转发原理

以“报文”作为数据传输单元；存储转发原理

* 什么是分组交换？

发送端欲发送的报文较长不便于传输，先把它划分成较短的、固定长度的数据段，每一个数据段前面添加上首部构成分组

* 主机与路由器的区别？

1.主机为用户进行信息处理的，并且可以和其他主机通过网络交换信息

2.主机在因特网的边缘部分

3.路由器是用来转发分组，进行分组交换的

* 什么是计算机网络？分类？

计算机网络最简单的定义：计算机网络是一些互相连接的、自治的计算机的集合.

从网络的使用者进行分类:公用网 ，专用网

从网络的作用范围进行分类：广域网 WAN，局域网 LAN，城域网 MAN，个人区域网 PAN

* 速率，带宽，时延

速率：是指连接在计算机网络上的主机向数字信道上传送数据的速率，一个比特就是二进制数字中的一个 1 或 0

带宽：通信线路传送数据的能力,单位时间内从网络的一点到另一点所能通过的“最高数据率”

时延：指数据从网络的一端传送到另一端所需的时间

时延=发送时延+传播时延+处理时延+排队时延

***第三次课***

* 时延带宽积，RTT

若发送端连续发送数据，在发送的第一个比特即将到达终点时，表示发送端已经发出的比特数

时延带宽积 = 传播时延 × 带宽

RTT:表示从发送方发送数据开始，到发送方收到来自接收方的确认，总共经历的时间

RTT与所发送的分组长度有关:长数据块的RTT>短数据块的RTT

* OSI 七层体系结构, TCP/IP 四层体系结构

OSI，七层体系结构：应用层，表示层，会话层，运输层，网络层，数据链路层，物理层

TCP/IP 四层体系结构：应用层、运输层、网际层和网络接口层

* 计算机网络的五层体系结构：分层，每层的功能，数据单元

应用层

任务：通过应用进程间的交互来完成特定网络应用

应用层协议定义了应用进程间通信和交互的规则，http, ftp, smtp

报文(message)：应用层传递的数据单元

运输层

负责两个主机中进程之间的通信

为端到端提供：可靠的传输服务，流量控制、差错控制、复用和分解功能

TCP协议：面向连接的可靠的数据传输服务, 报文段(segment)

UDP协议: 无连接的、尽最大努力的数据传输服务，用户数据报

网络层

负责为网络上的不同主机提供通信服务

选择合适的路由，使分组能够通过网络中的路由器到达目的主机

分组或包(packet)，数据报(datagram)

网际协议IP(Internet Protocol)

网际层，IP层

数据链路层

负责为网络上相邻的结点提供通信服务

成帧(framing)：IP数据报🡪帧(数据和控制信息)

物理层

所传数据的单位：比特

确定与传输媒体接口有关的一些特性

多大电压代表0和1

连接电缆的插头的引脚数以及如何连接

注意：物理媒体，如双绞线等，并不在物理层协议之内，而是在物理层协议的下面，物理层媒体当做第0层

***第四次课***

* 物理层的主要任务

物理层的主要任务：确定与传输媒体的接口有关的一些特性：

机械特性、电气特性、功能特性、过程特性

* 信号，码元

信号(signal)——数据的电气的或电磁的表现

码元(code)——一个数字脉冲就是一个码元

* 三种通信方式

单向通信（单工通信） ：只能有一个方向的通信而没有反方向的交互。如，无线电广播，电视广播

双向交替通信（半双工通信）：通信的双方都可以发送信息，但不能同时发送(或同时接收)。

双向同时通信（全双工通信）：通信的双方可以同时发送和接收信息

* 常用的编码方式

不归零制：正电平—1，负电平—0

归零制：正脉冲—1，负脉冲—0

曼彻斯特编码：位周期中心：向上跳变—0，向下跳变—1

差分曼彻斯特编码：在每一位的中心处始终都有跳变

位开始边界：有跳变—0，没有跳变—1

曼彻斯特编码产生的信号频率>不归零制；曼彻斯特编码具有自同步能力

* 香农定理

香农定理：带宽受限且有噪声干扰的信道

根据香农定理定理，可推出：信道的W或S/N越大，信息的极限数据传输速率越高；W和S/N确定，信息的极限数据传输速率也确定

* 两大类传输媒体

导引型传输媒体:电磁波被导引着沿固体媒体传播，如，铜线，光纤等

非导引型传输媒体:自由空间，其中电磁波的传输常称为无线传输

* 信道复用技术

***第五次课***

* CDM

码分复用 CDM

* SONET,SDH

同步光纤网SONET；同步数字系列 SDH

* ADSL, HFC, FTTx, PON

ADSL: 非对称数字用户线；HFC：光纤同轴混合网；

FTTx(Fiber To The …, 光纤到…)

X -- 不同的光纤接入地点(光电转换地点)：

例子：FTTH (H, Home)，光纤到户 ：光纤一直铺设到用户家庭，才把光信号转化为电信号

***第六次课***

* 数据链路层使用的信道类型

点对点信道: 使用一对一的点对点通信方式

广播信道: 使用一对多的广播通信方式

* 数据链路, 帧长，MTU

数据链路(data link)：实现这些协议的硬件和软件加到链路

帧长：数据链路的协议数据单元

MTU:数据部分长度上限

* CRC: 发送端工作，接收端工作，冗余码

在发送端，假设待传送的数据为 *M，*共 *k* 个比特，在 *M* 的后面再添加*n* 位冗余码一起发送

接收端把收到的数据以帧为单位进行CRC检验。把收到的每个帧都除以同样的除数*P*，然后检查余数，若余数 *R* = 0，则判定这个帧没有差错，就接受，若余数 *R* ≠ 0，差错，就丢弃

FCS（冗余码）的生成和CRC检验都由硬件来完成，处理速度很迅速，不会延误数据的传输

* 生成多项式🡪除数？

对于上面除数*P*=1101,可以用多项式*P(X)*=*X3*+*X2*+1

***第七次课***

* PPP 协议不需要的功能

纠错 ，流量控制 ，序号 ，多点线路 ，半双工或单工链路

* PPP协议帧的格式，MTU



* 比特填充

在 SONET/SDH 链路使用同步传输

PPP 协议采用零比特填充方法

* + 发送端只要发现有 5 个连续 1，则立即填入1个 0
  + 接收端对帧中的比特流进行扫描。每当发现 5 个连续1时，就把这 5 个连续 1 后的一个 0 删除
* Ppp链路涉及的三种连接

物理连接、LCP连接、网络层连接

* 局域网的拓扑

星形网、环形网、总线网

* 数据链路层包括的两个分层

逻辑链路控制 LLC子层

媒体接入控制 MAC子层

* 适配器包含的主要部分

处理器和存储器(ROM+RAM)

***第八次课***

* 以太网的两种通信措施

曼彻斯特(Manchester) 编码

无连接的

* CSMA/CD全称

载波监听多点接入/碰撞检测

* CSMA/CD协议的要点/工作过程

1. 准备发送：适配器将来自网络层的分组封装成帧，存入它的缓存。

2. 发送前，先侦听信道

* + 若信道忙，则不停地检测，直到信道转为空闲
  + 若空闲，并在96比特时间内保持空闲就发送这个帧

3. 在发送过程中仍然侦听信道，即，边发边侦听

* + 在争用期内未检测到碰撞，则继续发送直至完成。回到(1)
  + 如果检测到碰撞，则立即停止数据发送，并发送干扰信号。适配器执行指数退避算法，等待一段时间后，返回到步骤(2). 如果重传达16次，仍未成功，则停止重传，向上报错
* 以太网的通信方式，PPP链路通信方式

半双工通信；全双工通信

* 争用期或碰撞窗口

以太网的端到端往返时延 2*τ* 称为争用期，或碰撞窗口。

* 截断二进制指数退避算法

发生碰撞的站在停止发送数据后，要推迟（退避）一个随机时间才能再发送数据

基本退避时间为争用期 2*τ*

从离散整数集合[0,1,…, (2*k* −1)]中随机地取出一个数，记为 *r*。重传所需的时延= *r* 2*τ*

参数 *k*的计算： *k* = min[重传次数, 10]

当 *k* ≤ 10 时，参数 *k* 等于重传次数

当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告

* 以太网争用期的长度，最短有效帧长，覆盖范围

以太网取 51.2 μs 为争用期的长度。

对于 10 Mb/s 以太网，在争用期内可发送512 bit，即 64 字节。

以太网在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。

最短有效帧长？64字节

无效帧

以太网的最大端到端长度(覆盖范围)<5km

* 10BASE-T，集线器的工作原理

10BASE-T：10Mb/s，基带信号，双绞线

集线器:1.使用电子器件来模拟实际电缆线的工作🡪整个系统仍然像一个传统的以太网那样运行

2.星形以太网在逻辑上仍是一个总线网，各工作站使用CSMA/CD 协议，共享逻辑上的总线

3.工作在物理层，很像一个多接口的转发器

* 硬件地址

硬件地址又称为物理地址，MAC 地址

***第九次课***

* 硬件地址的位数，字节数，表示方法

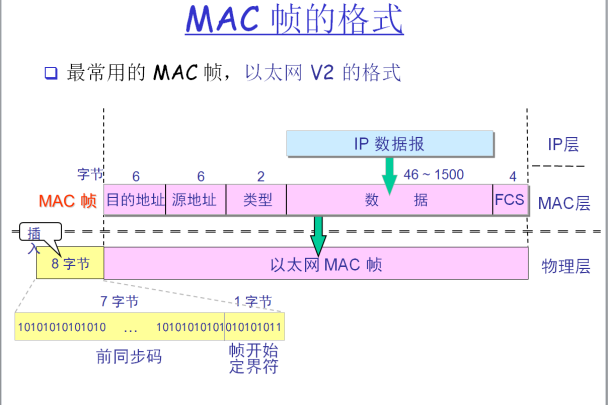
48个比特位，6字节，表示方法：

* 硬件地址的广播地址表示，广播帧

FF-FF-FF-FF-FF-FF

广播帧：发送给本地局域网的所有站点的帧(全1)

* MAC 帧的格式



* 帧间最小间隔

帧间最小间隔为 9.6 μs

* 无效的 MAC 帧

帧的长度不是整数个字节；用收到的帧检验序列FCS查出有差错；帧的MAC客户数据字段的长度不在46—1500字节之间。

***第十次课***

* 扩展以太网的方法

在数据链路层进行

* 以太网交换机的特点

多接口的网桥

工作在全双工方式

具有并行性

独占传输媒体

接口有存储器

即插即用设备

专用的交换结构芯片

* 以太网交换机的交换方式

存储转发方式

* + 把整个数据帧先缓存后再进行处理。

直通 (cut-through) 方式

* + 接收数据帧的同时就立即按数据帧的目的 MAC 地址决定该帧的转发接口，因而提高了帧的转发速度。
  + 缺点是它不检查差错就直接将帧转发出去，因此有可能也将一些无效帧转发给其他的站。
* 交换机自学习和转发帧的步骤

以太网交换机运行自学习算法自动维护交换表。

开始时，以太网交换机里面的交换表是空的。

* A 先向 B 发送一帧，从接口 1 进入到交换机。
* 交换机收到帧后，先查找交换表，没有查到应从哪个接口转发这个帧。
* 交换机把这个帧的源地址 A 和接口 1 写入交换表中，并向除接口1以外的所有的接口广播这个帧。
* C 和 D 将丢弃这个帧，因为目的地址不对。只 B 才收下这个目的地址正确的帧。这也称为过滤。
* 从新写入交换表的项目 (A, 1) 可以看出，以后不管从哪一个接口收到帧，只要其目的地址是A，就应当把收到的帧从接口1转发出去。
* B 通过接口 3 向 A 发送一帧。
* 交换机查找交换表，发现交换表中的 MAC 地址有 A。表明要发送给A的帧（即目的地址为 A 的帧）应从接口1转发。于是就把这个帧传送到接口 1 转发给 A。显然，现在已经没有必要再广播收到的帧。
* 交换表这时新增加的项目 (B, 3)，表明今后如有发送给 B 的帧，就应当从接口 3 转发出去。
* 经过一段时间后，只要主机 C 和 D 也向其他主机发送帧，以太网交换机中的交换表就会把转发到 C 或 D 应当经过的接口号（2 或 4）写入到交换表中。

归纳

* 交换机收到一帧后先进行自学习。查找交换表中与收到帧的源地址有无相匹配的项目。
  + 如没有，就在交换表中增加一个项目（源地址、进入的接口和有效时间）。
  + 如有，则把原有的项目进行更新（进入的接口或有效时间）。
* 转发帧。查找交换表中与收到帧的目的地址有无相匹配的项目。
  + 如没有，则向所有其他接口（进入的接口除外）转发。
  + 如有，则按交换表中给出的接口进行转发。
  + 若交换表中给出的接口就是该帧进入交换机的接口，则应丢弃这个帧（因为这时不需要经过交换机进行转发）。

***第十一次课***

* 高速以太网

速率≥ 100 Mb/s 的以太网称为高速以太网

* PPPoE

在以太网上运行 PPP

FTTx 都要使用 PPPoE 的方式进行接入。

* 互联网的网络层提供的服务

简单灵活的，无连接的，尽最大努力交付的数据报服务

* 辅助IP协议的三个协议：ARP,ICMP,IGMP

地址解析协议 ARP、网际控制报文协议 ICMP、网际组管理协议 IGMP

* 默认网关

上互联网途径的第一个路由

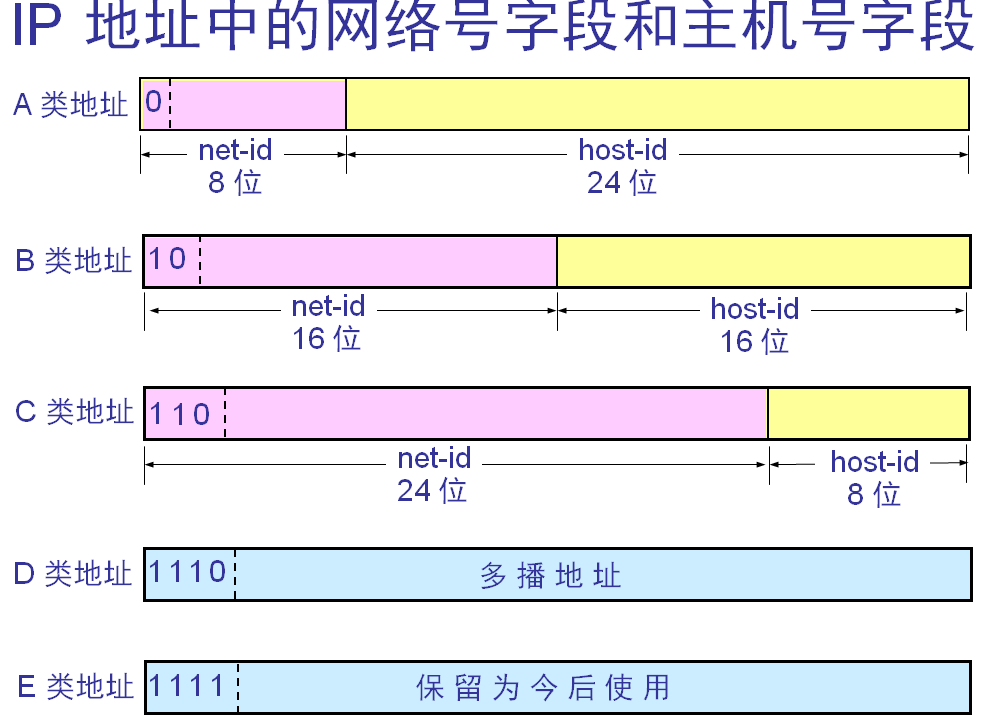
* 直接交付，间接交付

直接交付：不需要经过任何路由器

* 分类 IP 地址的结构

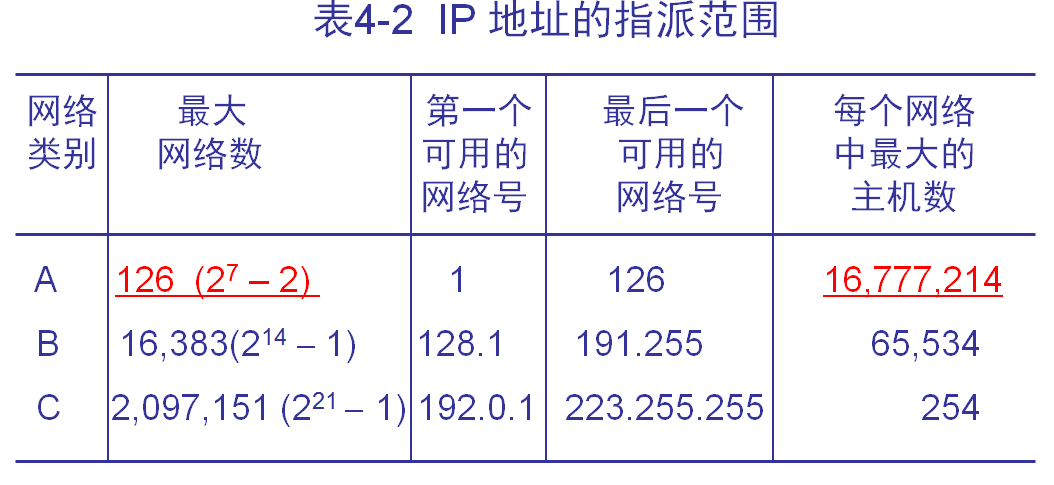
IP 地址 ::= { <网络号>, <主机号>}

* 对A.B.C三类地址，第一个字节的取值范围



***第十二次课***

* 每类IP地址最大的网络数，主机数，网络地址，广播地址



* IP 地址的一些重要特点

用转发器或网桥连接起来的若干个局域网仍为一个网络🡪都具有同样的网络号 net-id

所有分配到网络号 net-id 的网络都是平等的

网络：范围很小的局域网，或可能覆盖很大地理范围的广域网

平等的：互联网同等对待每个IP地址

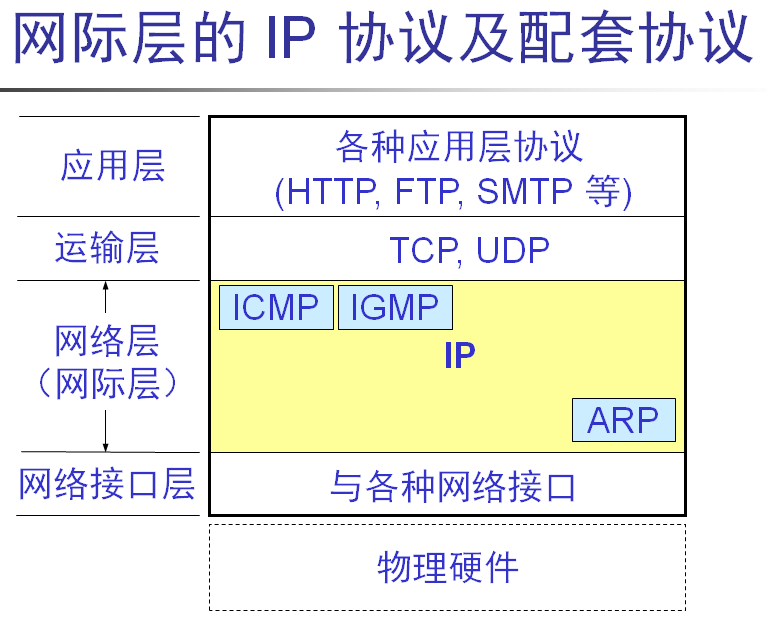
* ARP要点

每一个主机都有 ARP 高速缓存，里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表

当主机 A 欲向本局域网上的主机 B 发送 IP 数据报

先查看ARP高速缓存中有无主机B的IP地址:YES，就可查出其硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址；NO，怎么办？

***第十三次课***



* IP数据报格式：（P127）
  + 长度：首部长度（单位），
  + 总长度占 16 位，指首部和数据之和的长度，单位为字节，数据报的最大长度为 65535 字节
  + 片偏移
  + 分片相关字段
  + TTL
* 路由表构成：列

目的主机IP号，下一跳地址

* 分组转发算法

(1) 依据数据报首部的目的主机 IP 地址 *D* 🡪目的网络地址为 *N*。

(2) 若网络 *N* 与此路由器直接相连，则把数据报直接交付目的主机；否则是间接交付，执行(3)。

(3) 若路由表中有目的地址为 *D* 的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由器；否则，执行(4)。

(4) 若路由表中有到达网络N的路由，则把数据报传送给路由表指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

***第十四次课***

* 三级IP地址结构

IP地址：：={<网络号>，<子网号>，<主机号>}

* 子网地址

主机号全为0

* 子网掩码的定义

网络号、子网号全1，主机号全0

* 默认子网掩码

网络号为1，子网号、主机号全0

* 子网划分方法

所有的子网掩码都相同，子码号长度相同

* 采用子网划分，路由表的构成（行）

目的网络、子网掩码、下一跳

* 子网划分的分组转发方法

(1) 从收到分组的首部提取目的 IP 地址 *D*。

(2) 先判断是否为直接交付。逐个检查路由器直接相连网络：用各网络的子网掩码和 *D* 逐位相“与”，看是否和相应的网络地址匹配。若匹配，则将分组直接交付。否则就是间接交付，执行(3)。

(3) 若路由表中有目的地址为 *D* 的特定主机路由，则将

分组传送给指明的下一跳路由器；否则，执行(4)。

(4) 对路由表中的每一行，用子网掩码和 *D* 逐位相“与”，

若其结果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(5)。

(5) 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(6)。

(6) 报告转发分组出错。

***第十五次课***

* 无分类的两级编址的记法

IP地址：：={<网络前缀>，<主机号>}

* 220.78.168.0/26 的含义

网络前缀占26位，主机号为6位，子网掩码为11111111.11111111.11111111.11000000

* CIDR 地址块

CIDR把网络前缀相同的连续的IP地址组成一个“CIDR 地址块” 。

* IP地址128.14.35.7/24，地址块的起始(最小)地址和最大地址，以及地址块中的地址数？

Min:128.14.35.00000000

Max:128.14.35.00000000

2的8次方

* + 构成超网/路由聚合的方法

一个 CIDR 地址块中有很多地址,这种地址的聚合常称为路由聚合, 或构成超网

* + 10/10 的含义

10.0.0.0/10

* + 已知CIDR地址块 /18，则 地址数, 包含的C类网络数？

地址数：2的14次方=16K

C类网络数：2的8次方=64

* 最长前缀匹配

从匹配结果中选择具有最长网络前缀的路由

网络前缀越长，其地址块就越小 🡺 路由就越具体

* 4 种ICMP 差错报告报文，不发送差错报告报文的情况

网际控制报文协议 ICMP差错报告报文：

终点不可达，类型值:3

* + 当路由器或主机不能交付数据报时，向源点发送

时间超过，类型值:11

* + 当路由器遇到数据报TTL=0，丢弃，向源点发送

参数问题，类型值:12

* + 当路由器或主机收到的数据报的首部字段有错

改变路由（重定向），类型值:3

* + 路由器发送给主机，使主机知道下次应该将数据报发送给另外的路由器

不发送差错报告报文的情况：

对 ICMP 差错报告报文不再发送 ICMP 差错报告报文。

对第一个分片的数据报片的所有后续数据报片都不发送 ICMP 差错报告报文。

对具有多播地址的数据报都不发送 ICMP 差错报告报文。

对具有特殊地址（如127.0.0.0 或 0.0.0.0）的数据报不发送 ICMP 差错报告报文。

* Ping命令使用ICMP的哪种报文实现的？

ICMP 回送请求与回送回答报文

***第十六次课***

* tracert分别使用ICMP的哪个报文实现的？

利用 IP 数据报中的 TTL 字段和 ICMP 时间超过差错报告报文实现对从源点到终点的路径的跟踪

* 路由算法的分类--自适应性

静态路由选择策略--非自适应路由选择

动态路由选择策略--自适应路由选择

* 自治系统 AS

一个AS对其他AS表现出的是一个单一的和意志的路由选择

* 互联网有两大类路由选择协议

内部网关协议 IGP

外部网关协议EGP

* RIP距离的定义， 距离为16 表示什么？

从一路由器到它直接相连的网络距离为1，16表示不可达

* RIP 协议的三个要点

① 仅和相邻路由器交换信息

②路由器交换的信息，即自己的路由表

③按固定时间间隔交换信息

* 距离向量算法

收到相邻路由器（地址为 X）的一个 RIP 报文：

㈠ 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，并把所有的“距离”字段的值加 1。

㈡ 对修改后的 RIP 报文中的每一个项目，重复以下步骤：

① 若项目中的目的网络不在路由表中，则把该项目加到  
 路由表中。否则，

② 若下一跳字段给出的路由器地址是同样的，则把收到  
 的项目替换原路由表中的项目。否则，

③ 若收到项目中的距离小于路由表中的距离,则进行更新

④ 否则，什么也不做。

㈢ 若 3 分钟还没有收到相邻路由器的更新路由表，则把此  
 相邻路由器记为不可达路由器，即将距离置为16

㈣ 返回。

***第十七次课***

* OSPF 协议的三个要点

①向本自治系统中所有路由器发送信息

②发送的信息: 与本路由器相邻的所有路由器的链路状态

③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

* 区域 P158

OSPF 将一个自治系统再划分为若干个更小的范围

* OSPF分组类型及作用

类型1，问候(Hello)分组

用来发现和维持邻站的可达性

类型2，数据库描述(Database Description)分组

向邻站给出自己的LS数据库中的所有LS项目的摘要信息

类型3，链路状态请求(Link State Request)分组

向对方请求发送某些LS项目的详细信息

类型4，链路状态更新(Link State Update)分组

用洪泛法对全网更新链路状态。

类型5，链路状态确认(LS Acknowledgment)分组

对链路更新分组的确认

* 一个 BGP 发言人与其他的 BGP 发言人交换路由信息的过程

①先建立TCP连接

②在此连接上交换BGP报文以建立BGP会话

③利用BGP会话交换路由信息

* BGP 所交换的网络可达性的信息？P163

路由向量

***第十八次课***

(BGP属于应用层)

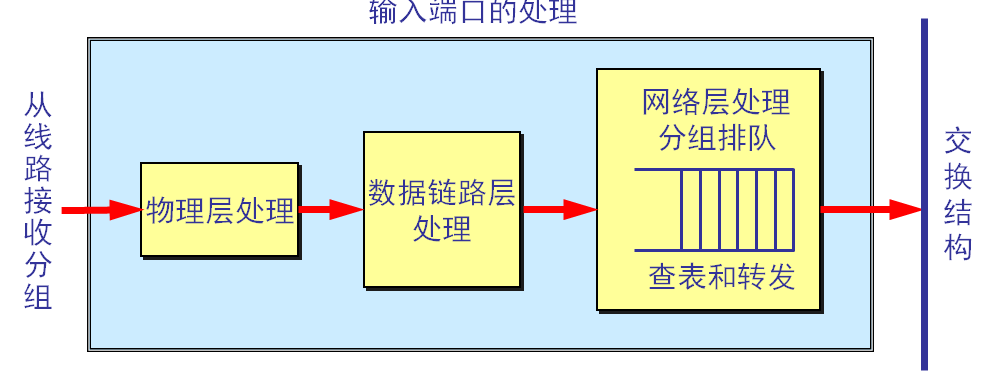
* 路由器

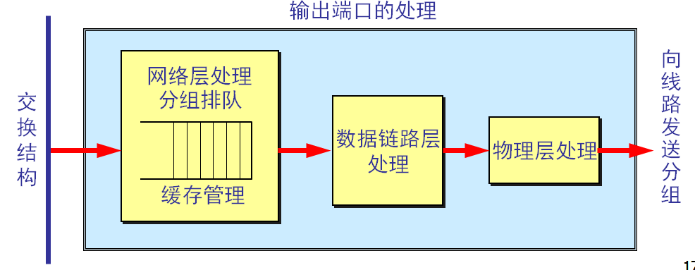
具有多个输入端口和多个输出端口的专用计算机。其任务是转发分组

* “转发”和“路由选择”的区别

“转发”(forwarding)就是路由器根据转发表将用户的 IP 数据报从合适的端口转发出去。转发仅涉及到一个路由器。“路由选择”(routing)涉及到很多路由器 ，路由表则是许多路由器协同工作的结果。按照复杂的路由选择，构造出整个路由表。

* 路由器的构成：两大部分，每部分的组成





* 什么时候出现分组丢弃？

①设备出现故障

②发生在路由器中的输入或输出队列产生溢出时

* 专用地址块有哪些？

(1) 10.0.0.0 到 10.255.255.255

A类，或记为10.0.0.0/8

(2) 172.16.0.0 到 172.31.255.255

B类，或记为172.16.0.0/12

(3) 192.168.0.0 到 192.168.255.255

C类，或记为192.168.0.0/16

* IPv6地址的位数，三种基本类型地址

位数：128

(1) 单播 (unicast)：传统的点对点通信。

(2) 多播 (multicast)：一点对多点的通信。

(3) 任播 (anycast)：目的站是一组计算机，但数据报在交付时只交付其中的一个，通常是距离最近的一个。

* 什么是“流”？

“流”是互联网络上从特定源点到特定终点的一系列数据报，所经过的路径上的路由器都保证指明的服务质量。所有属于同一个流的数据报都具有同样的流标号。

* 冒号十六进制记法

每个 16 位的值用十六进制值表示，各值之间用冒号分隔。

在十六进制记法中，允许把数字前面的0省略。例如把0000中的前三个0省略，写成1个0。

***第十九次课***

* 运输层的主要功能

①为应用进程之间提供端到端的逻辑通信。

②对收到的报文进行差错检测。

③复用和分用

* 运输层的两个主要协议 ,传送的数据单位

①用户数据报协议 UDP ，UDP 传送的数据单位是UDP 用户数据报

②传输控制协议 TCP ，TCP 传送的数据单位是 TCP 报文段

* 运输层的UDP 用户数据报与IP数据报区别

IP 数据报要经过互连网中许多路由器的存储转发

UDP 用户数据报是在运输层抽象的端到端的逻辑信道中传送的

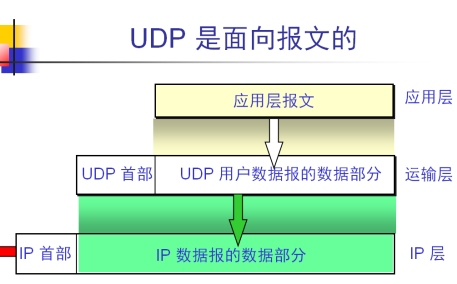
* 端口,端口号分类,熟知端口P192
* UDP 是面向报文的

发送方 UDP 对应用程序交下来的报文，在添加首部后就向下交付 IP 层。

UDP 对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界。

应用层交给 UDP 多长的报文，UDP 就照样发送，即一次发送一个报文。

接收方 UDP 对 IP 层交上来的 UDP 用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。



* UDP校验和检查的内容

UDP校验和，既检查了UDP用户数据报的首部和数据部分，又检查了IP数据报的源IP地址和目的IP地址

***第二十次课***

* TCP 最主要的特点

面向连接的

点对点

提供可靠交付的服务

全双工通信

面向字节流

* TCP 的连接的标识

套接字 socket = (IP地址: 端口号)

TCP 连接 ::= {socket1, socket2} = {(IP1: port1), (IP2: port2)}

* 实现可靠的通信的方法

使用上述的确认和重传机制（P199），就可以在不可靠的传输网络上实现可靠的通信。

这种可靠传输协议常称为自动重传请求ARQ (Automatic Repeat reQuest)。

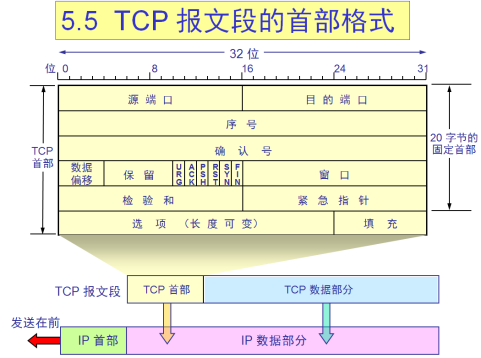
* ARQ, 连续ARQ,累积确认

ARQ：停止等待协议

连续ARQ：在确认前发多个分组

累积确认：对按序到达的最后一个分组发送确认（Ｐ２０１）

* TCP 报文段的首部格式：序 号，确认号，ACK,SYN,FIN,PSH,URG,窗口



①序 号:占 4 字节。该字段值则指的是本报文段所发送的数据的第一个字节的序号

②确认号：占 4 字节，是期望收到对方下一个报文段的数据的第一个字节的序号。

③紧急 URG：当 URG = 1 时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据(相当于高优先级的数据) ，应尽快传送。

④确认 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

⑤推送PSH：接收 TCP 收到 PSH = 1 的报文段，就尽快地交付接收应用进程，而不再等到整个缓存都填满了后再向上交付

⑥同步 SYN：在连接建立时用来同步序号

当SYN=1，ACK=0：连接请求报文段

对方同意建立连接，则在响应报文段中使SYN=1，ACK=1

同步 SYN = 1 表示这是一个连接请求或连接接受报文

⑦终止 FIN (FINis)：用来释放一个连接。FIN = 1 表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。

⑧窗口：占 2 字节，单位为字节，指发送该报文段一方的接收窗口大小。窗口值告诉对方：从本报文段首　部中的确认号算起，目前允许对方发送的数据量。是对方设置其发送窗口的依据。

***第二十一次课***

* TCP 报文段的首部格式：序 号，确认号，ACK,SYN,FIN,窗口
* 以字节为单位的滑动窗口的实现（Ｐ２０６）,流量控制（Ｐ２１２）

7. 在采用TCP连接的数据传输阶段，如果发送端的发送窗口值由1000变为2000，那么发送端在收到一个确认之前可以发送（）。

A. 2000个TCP报文段 B. 2000字节 C. 1000字节

8. A和B建立了TCP连接，当A收到确认号为100确认报文段时，表示（）

A. 报文段99已收到 B. 报文段100已收到

C. 末字节号为99的报文段已收到 D.末字节号为100的报文段已收到

9.为保证数据传输的可靠性，TCP采用了对（）确认的机制

A. 报文段 B. 分组 C. 字节 D. 比特

11. 滑动窗口的作用是（）

A. 流量控制 B. 拥塞控制 C. 路由控制 D. 差错控制

18. A和B之间建立了TCP连接，A向B发送了一个报文段，其中序号字段seq=200，确认号字段ACK=201，数据部分有2个字节，那么在B对该报文的确认报文段中（ ）

A. seq=202,ack=200 B. seq=201,ack=201

C. seq=201,ack=202 D. seq=202,ack=201

***第二十二次课***

* 拥塞控制的算法：慢开始，拥塞避免，快重传，快恢复，加法增大，乘法减小

慢开始：在主机刚刚开始发送报文段时设置拥塞窗口 cwnd = 1，即设置为一个最大报文段 MSS 的数值。 在每收到一个对新的报文段的确认后，将cwnd加1，即增加一个 MSS 的数值。用这样的方法逐步增大发送端的cwnd 🡺 分组注入到网络的速率更加合理。传输轮次: 把cwnd所允许发送的报文段都连续发送出去，并收到了对已发送的最后一个字节的确认。慢开始算法: 每经过一个传输轮次，cwnd 就加倍。慢开始中的“慢”：不是指增长速度慢，而是指开始发送时cwnd=1

拥塞避免算法：让拥塞窗口 cwnd 缓慢地增大，即每经过一个传输轮次，发送方把cwnd加1，而不是加倍，这样，cwnd按线性规律缓慢增长。

快重传：接收方每收到一个失序的报文段后，立即发出重复确认，以便让发送方及早知道有报文段没有到达接收方。

发送方只要一连收到三个重复确认，就立即重传对方尚未收到的报文段，不必继续等待重传计时器超时。

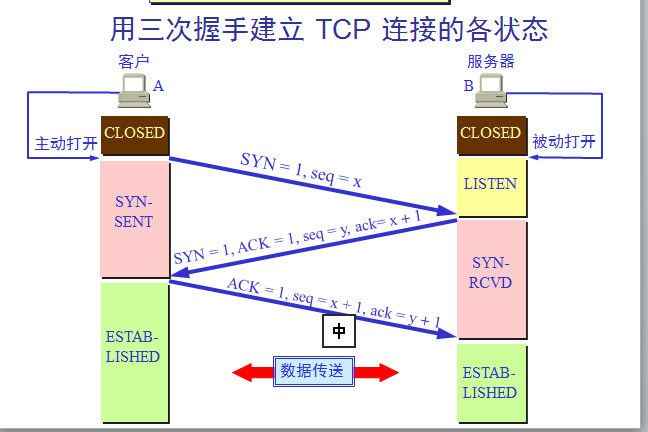
由于发送方能尽早地重传未被确认的报文段，因此采用快重传后可以使整个网络的吞吐量提高约20%。

乘法减小“(multiplicative decrease)：不论在慢开始阶段还是拥塞避免阶段，只要出现一次超时（即出现一次网络拥塞），ssthresh ← ½ ×当前的cwnd。

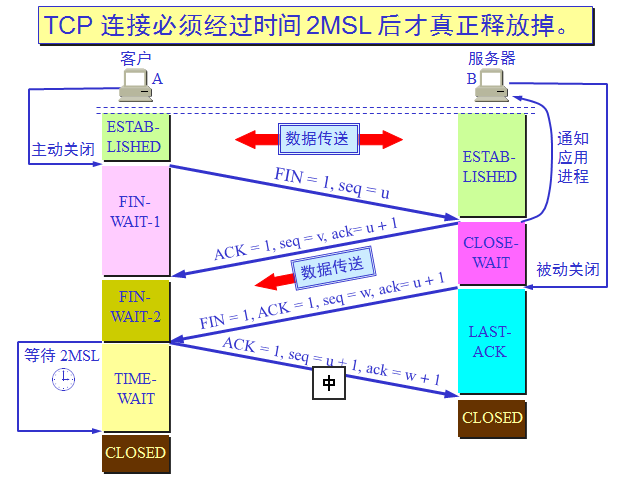
当网络频繁出现拥塞时，ssthresh 值就下降得很快，以大大减少注入到网络中的分组数。

“加法增大” (additive increase)： 执行拥塞避免算法后，每经过一次传输轮次，cwnd++，使拥塞窗口缓慢增大，以防止网络过早出现拥塞。

* TCP连接建立过程



* TCP连接释放过程



***第二十三次课***

* 应用层的功能

规定应用进程在通信时所遵循的协议

* 什么DNS，DNS服务器的分类及存储内容

域名系统 DNS: 互联网使用的命名系统，用来把人们使用的机器名字转换为IP地址

* 域名解析过程

主机向本地域名服务器的查询一般都是采用递归查询:如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。递归查询返回的结果或是所需的IP地址，或报错

本地域名服务器向根域名服务器的查询采用迭代查询：根域名服务器收到本地域名服务器的查询请求报文，或给出所要查询的 IP 地址，或告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。通常，根域名服务器把自己知道的顶级域名服务器的IP地址告诉本地域名服务器。顶级域名服务器收到本地域名服务器的查询请求，要么给出IP地址，要么告之权威域名服务器IP地址。最后，本地域名服务器获得解析的IP地址，返回给发起查询的主机

***第二十四次课***

* 什么是FTP，FTP协议使用的TCP连接个数及作用

文件传送协议 FTP是互联网上使用得最广泛的文件传送协议。、

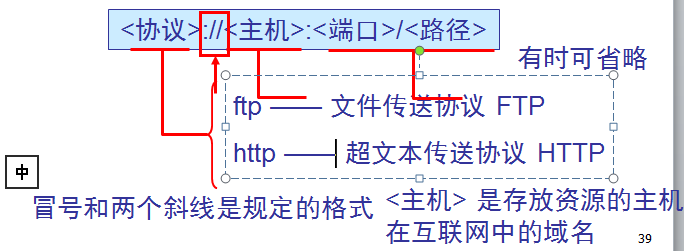
两个TCP连接，控制连接在整个会话期间一直保持打开

FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。数据连接实际用于传输文件。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建“数据传送进程”和“数据连接”。数据连接用来连接客户端和服务器端的数据传送进程。数据传送进程实际完成文件的传送，在传送完毕后关闭“数据传送连接”并结束运行。

* 万维网的概念

万维网, WWW (World Wide Web)/Web 并非某种特殊的计算机网络，是一个大规模的、联机式的信息储藏所

* URL 的一般形式



* 点击链接后使用的运输层以上的协议有哪些？

***第二十五次课***

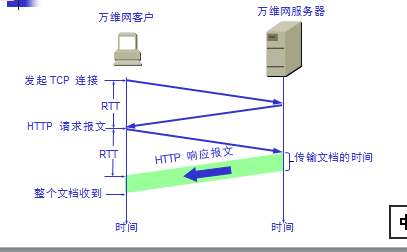
* http主要特点

使用面向连接的 TCP，保证了数据的可靠传输

HTTP 本身无连接的：通信的双方在交换HTTP报文之前不需要先建立HTTP连接

HTTP 1.0 协议是无状态的(stateless)：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相同；服务器并不记得这个客户，也不记得为该客户服务了几次；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

* http使用TCP连接的方式



* 非流水线方式，流水线方式

非流水线方式:客户在收到前一个响应后才能发出下一个请求 ，TCP连接建立后，客户每访问一次对象都要用去一个RTT。这比非持续连接的开销节省了一个 RTT 时间

缺点：服务器在发送完一个对象后，其 TCP 连接就处于空闲状态，浪费了服务器资源。

流水线方式：客户在收到响应报文之前能够接着发送新的请求报文，连续多个请求报文到达服务器后，服务器就可连续发回响应报文，客户访问所有的对象只需花费一个 RTT时间，使 TCP 连接中的空闲时间减少，提高了下载文档效率

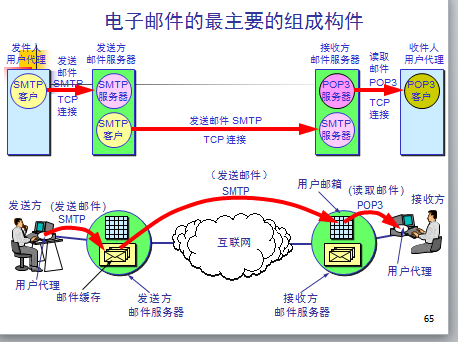
* 代理服务器

代理服务器(proxy server) ，又称为万维网高速缓存(Web cache) ，是一种网络实体

* HTTP报文开始行格式：请求报文，响应报文

***第二十六次课***

* 电子邮件的最主要的组成构件



* 各构件的作用
* 发送和接收邮件的步骤及使用的协议

➊ 发件人调用PC中的UA撰写和编辑要发送的邮件

➋ 发件人的UA把邮件用 SMTP 协议发给发送方邮件服务器

➌ 此服务器把邮件临时存放在邮件缓存队列中，等待发送

➍ 发送方邮件服务器的 SMTP 客户与接收方邮件服务器的 SMTP 服务器建立 TCP 连接，然后就把邮件缓存队列中的邮件依次发送出去。

注意：邮件不会在互联网中的某个中间邮件服务器中转。

➎ 接收方邮件服务器中的SMTP服务器进程收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取

➏ 收件人在打算收信时，就运行 PC 机中的用户代理，使用 POP3（或 IMAP）协议读取发送给自己的邮件。

两种通信方式：推(push)—SMTP 拉(pull)– POP3

* 电子邮件的组成部分

电子邮件由信封(envelope)和内容(content)两部分组成

* SMTP 通信的三个阶段

1.连接建立：在发送主机的 SMTP 客户和接收主机的 SMTP 服务器之间建立TCP连接。端口号为25。

2.邮件传送

3.连接释放：发送完毕后，SMTP 释放 TCP 连接。

* POP3协议的特点

只要用户从POP服务器读取了邮件，POP服务器就把该邮件删除。

* 网际报文存取协议IMAP

网际报文存取协议IMAP (Internet Message Access Protocol)，读取邮件的协议，IMAP4

按客户服务器方式工作。运行IMAP时，用户主机上的IMAP客户进程🡨🡪邮件服务器上的IMAP服务器进程：TCP连接。用户在自己的 PC 机上就可以操纵邮件服务器的邮箱，就像在本地操纵一样。

当用户 PC 机上的 IMAP 客户程序打开 IMAP 服务器的邮箱时，就可看到邮件的首部。用户打开某个邮件，该邮件才传到用户的计算机上。创建文件夹，在文件夹之间移动邮件。查找邮件，删除邮件

* 基于万维网的电子邮件收发邮件使用的协议

万维网邮件服务器都使用IMAP，用户可以在这种邮件服务器存放很多的邮件。电子邮件从 A 发送到网易邮件服务器是使用 HTTP 协议。两个邮件服务器之间的传送使用 SMTP。例如，邮件从新浪邮件服务器传送到 B 是使用 HTTP 协议。

***第二十七次课***

* 连接到互联网的计算机的协议软件需要配置的项目

IP 地址, 子网掩码

默认路由器的 IP 地址, DNS服务器的 IP 地址

* DHCP, DHCP 协议的工作过程

***第二十八次课***

* + WiFi无线局域网使用的协议
  + 移动IP的基本概念