第一章 概述

1、计算机网络的基本概念

简单定义：为了实现资源共享而相互连接起来的一组自治计算机的集合。

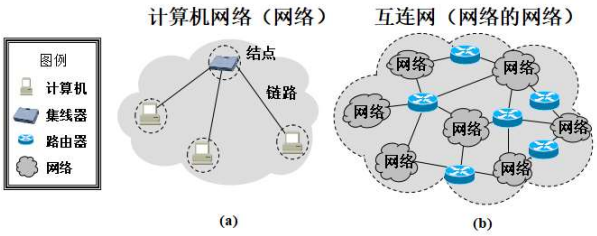
文献定义：利用通信设备和线路将分散在不同地点的、具有独立功能的多个计算机系统互相连接起来，并按照网络协议进行数据通信，实现资源共享的计算机集合

2、计算机网络的特征

资源共享、分布在不同地理位置的“自制系统”、遵循“网络协议”、连通性

3、网络的结构组成

网络（network）由若干结点（node）和连接这些结点的链路（link）组成。



(a) 简单的网络　　(b) 由网络构成的互连网

4、因特网（Internet）

网络和网络通过路由器互连起来形成互联网，它是“网络的网络”（network of networks）。习惯上，大家把连接在因特网上的计算机都称为主机（host）。

5、资源子网和通信子网

1）资源子网

包括主机、终端、软件等（网络边缘），主要功能是进行数据处理、运行网络应用程序。

传统设备：桌面 PC、工作站、服务器等

非传统设备：PDA、TV、移动计算机、汽车等

2）通信子网

简称子网，负责主机之间的数据通信（网络核心）。

传输线路：用于机器之间传送数据。

交换元素（交换机、路由器）：负责连接传输线路。

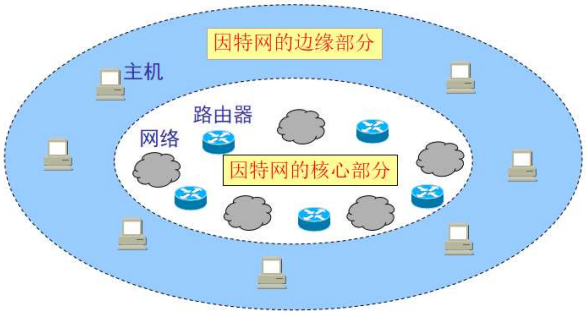
传输线路和一组路由器（不包含主机）的集合构成子网。

6、因特网的结构

边缘部分：由所有连接在因特网上的主机（也称作端系统）组成。这部分是用户直接使用的，用来进行通信（传送数据、音频或视频）和资源共享。

核心部分：由大量网络和连接这些网络的路由器组成。这部分是为边缘部分提供服务的（提供连通性和交换）。

接入网：将端系统连接到其边缘路由器的通信线路，通常称为“最后一公里”网络。



7、边缘部分

主机 A 的某个进程和主机 B 上的另一个进程进行通信。简称为“计算机之间通信”。

在网络边缘的端系统之间的通信方式通常可划分为两大类：客户-服务器方式（C/S 方式）和对等方式（P2P 方式）

1）客户-服务器方式：

存储数据的性能强大的计算机称为“服务器”，访问服务器的主机称为“客户机”，客户机和服务器通过网络连接。

客户机进程：通过网络将一个消息发送给服务器进程，然后客户进程等待应答消息。

服务器进程：获得了请求消息之后，执行所请求的工作，或者查询客户请求的数据，返回应答消息。

2）对等方式：

个人主机之间的通信、交互式娱乐，没有固定的客户端和服务器

8、核心部分

网络核心部分是因特网中最复杂的部分，因为网络中的核心部分要向哇网络边缘中的大量主机提供连通性，使边缘部分中的任何一台主机都能够向其他主机通信。

在网络核心部分起特殊作用的是路由器（router），它是一种专用计算机（但不是主机）。路由器是实现分组交换（packet switching）的关键构件，其任务是转发收到的分组。这是网络核心部分最重要的功能。

1）电路交换

电路交换是面向连接的，分为三个阶段：建立连接、通信、释放连接。

缺点是通信链路的利用率很低，资源浪费；维持连接的信令复杂，成本高。

2）分组交换

采用储存转发技术。把较长的报文划分成一个个更小的等长数据段，在每一个数据段前面加上一些必要的控制信息组成的首部（header）后，构成一个分组 （packet）。分组又称为“包”，而分组的首部也可称为“包头”。分组是在因特网中传送的数据单元。先完整的接受完一个分组，再向输出链路发送该分组。接收端收到分组后剥去首部还原成原来的报文。

9、接入网

接入网分为有线接入网（ADSL、以太网、FTTx、HFC）和无线网（WiFi、移动无线接入）

10、计算机网络的分类

按距离尺度：

个域网 PAN、局域网 LAN、城居网 MAN、广域网 WAN（资源子网、通信子网）、互联网 Internet（通常由路由器连接的 LAN 或 WAN 组成。网关：将两个或多个网络连接起来并提供必要转换的及其，其硬件和软件方便的总称为网关（gateway））

路由器+传输线路→子网　子网+主机→网络　网络×n→互联网

从网络的使用者进行分类：

公用网、专用网

用来把用户接入到互联网的网络：

接入网 AN

11、分组交换网的性能

1）速率

数据率（data rate）或比特率（bit rate），往往指额定速率或标称速率，单位是 b/s 或 kb/s、Mb/s、Gb/s 等。

2）带宽

带宽（bandwidth）是数字信道所能传送的“最高数据率”，单位是 b/s 或 kb/S、Mb/s、Gb/s、Tb/s 等。

3）吞吐量

吞吐量（throughput）表示在单位时间内通过某个网络（或信道、接口）的数据量。吞吐量更经常地用于对现实世界中的网络的一种测量，以便知道实际上到底有多少数据量能够通过网络。

4）时延

时延（delay 或 latency）是指数据（一个报文或分组）从网络（或链路）的一段传送到另一端所需的时间。总时延=发送时延+传播时延+排队时延+处理时延

①发送时延（传输时延）

发送数据时，数据块从结点进入到传输媒体所需要的时间。也就是从发送数据帧的第一个比特算起，到该帧的最后一个比特发送完毕所需的时间。

发送时延 = 数据块长度 L（bit）/信道带宽 R（bit/s）

②传播时延

电磁波在信道中需要传播一定的距离而花费的时间。

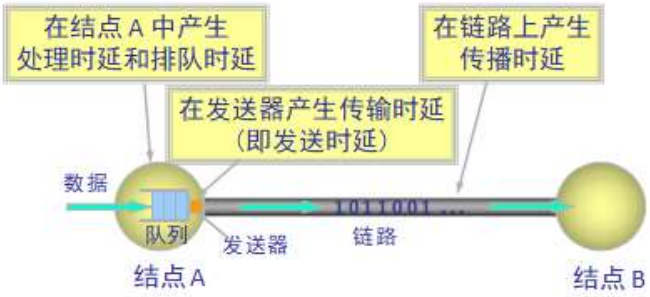
传播时延 = 信道长度 d（m）/信号在信道上的传播速率 s（m/s）

③排队时延

结点缓存队列中分组排队所经历的时延

④处理时延

交换结点为存储转发而进行一些必要的处理所花费的时间。



5）丢包

由于缓存队列（buffer）具有有限的存储能力，当年分组到达满的队列时，分组又被丢弃（lost），丢失的分组可能由前面的结点或源端系统重传，或根本不重传。

6）时延带宽积

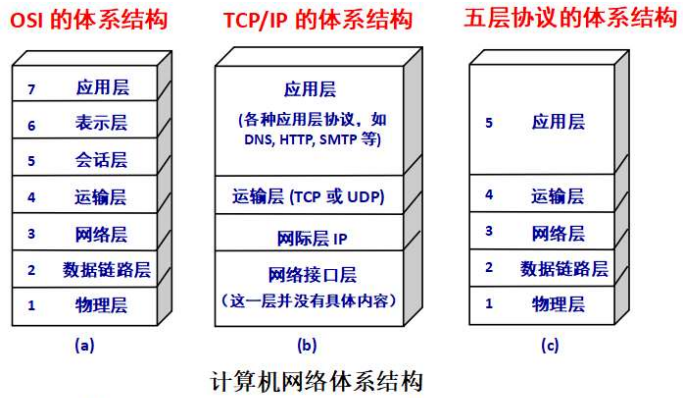
链路的时延带宽积又称为以比特为单位的链路长度。只有在代表链路的管道都充满比特时，链路才得到了充分利用。

时延带宽积 = 传播时延 × 带宽

7）往返时间

往返时间（RTT）指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。在互联网中，往返时间还包括各中间节点的处理时延、排队时延以及转发数据时的发送时延。

12、计算机网络体系结构



计算机网络体系结构

(a) OSI 的七层协议； (b) TCP/IP 的四层协议； (c) 五层协议

1）应用层

应用层是网络应用程序及它们的应用层协议存留的地方。因特网的应用层包括许多协议，例如 HTTP、SMTP、FTP

2）运输层

因特网的运输层在应用程序端点之间传送应用层报文。在因特网中，有两个运输协议，即 TCP 和 UD，利用其中的任一个都能运输应用层报文。运输层分组称为报文段（segment）。

3）网络层

因特网的网络层负责将称为数据报（datagram）的网络层分组从一台主机移动到另一台主机。因特网的网络层仅有一个 IP 协议。

4）链路层

因特网的网络层通过源和目的地之间的一系列路由器路由数据报。为了将分组从一个结点（主机或路由器）移动到路径上的下一个结点，网络层必须依靠链路层的服务。由链路层提供的服务取决于应用于该链路的特定链路层协议，包括以太网、WiFi 和电缆接入网的 DOCSIS 协议。链路层分组称为帧（frame）。

5）物理层

虽然链路层的任务是将整个帧从一个网络元素移动到临近的网络元素，而物理层的任务是将该帧中的一个一个比特从一个结点移动到下一个结点。在这层中的协议仍然是链路相关的，并且进一步与该链路的实际传输媒体相关。

第一章课后题

1、试在下列条件下比较电路交换和分组交换。要传送的报文共 x（bit）。从源点到终点共经过 k 段链路，每段链路的传播时延为 d（s），数据率为 b（b/s）。在电路交换时电路的建立时间为 s（s）。在分组交换时分组长度为 p（bit），且各结点的排队等待时间可忽略不计。问在怎样的条件下，分组交换的时延比电路交换的要小？（提示：画一下草图观察 k 段链路共有几个结点）

答：对电路交换，当 t=s 时，链路建立；
当 t=s+x/b，发送完最后一 bit；
当 t=s+x/b+kd，所有的信息到达目的地。
对分组交换，当 t=x/b， 发送完最后一 bit；
为到达目的地，最后一个分组需经过 k-1 个分组交换机的转发，
每次转发的时间为 p/b，
所以总的延迟= x/C+(k-1)p/b+kd
所以当分组交换的时延小于电路交换
x/b+(k-1)p/b+kd＜s+x/b+kd 时，
(k-1)p/C＜s
由上式可知，当 k 和 b 一定时，p 越小，分组交换的时延越小，即需要传送少量数据时（即 p<<x），分组交换的时延较小。

2、在上题的分组交换网中，设报文长度和分组长度分别为 x 和（p+h）（bit），其中 p 为分组的数据部分的长度，而 h 为每个分组所带的控制信息固定长度，与 p 的大小无关。通信的两端共经过 k 段链路。链路的数据率为 b（b/s），但传播时延和结点的排队时间均可忽略不计。若打算使总的时延为最小，问分组的数据部分长度 p 应取为多大？

答：分组个数 x/p，
传输的总比特数：(p+h)x/p
源发送时延：(p+h)x/pb
最后一个分组经过 k-1 个分组交换机的转发，中间发送时延：(k-1)(p+h)/b
总发送时延 D=源发送时延+中间发送时延
D=(p+h)x/pb+(k-1)(p+h)/b
令其对 p 的导数等于 0，求极值
p=√hx/(k-1)

3、长度为 100 字节的应用层数据交给传输层传送，需加上 20 字节的 TCP 首部。再交给网络层传送，需加上 20 字节 的 IP 首部。最后交给数据链路层的以太网传送，加上首部和尾部共 18 字节。试求数据的传输效率。数据的传输效率是指发送的应用层数据除以所发送的总数据（即应用数据加上各种首部和尾部的额外开销）。若应用层数据长度为 1000 字节，数据的传输效率是多少？

答：数据长度为 100 字节时
传输效率=100/（100+20+20+18）=63.3%
数据长度为 1000 字节时，
传输效率=1000/（1000+20+20+18）=94.5%

第二章 应用层

1、网络应用程序体系结构

1）客户-服务器体系结构

服务器：总是在线，具有固定的 IP 地址，可通过数据中心进行扩展。

客户端：与服务器进行通信，可以是间接性在线连接，可以具有动态 IP 地址，客户端彼此之间不直接通信。

2）对等（P2P）体系结构

没有总是在线的服务器角色，任意端系统之间直接通信，在对等方直接向其他对等方请求服务，对等方彼此之间互相提供服务，对等方彼此间间断性的连接，对等方的 IP 地址不固定，管理复杂。

2、进程通信

一个进程可以被认为时运行在端系统中的一个程序。在两个不同端系统上的进程，通过跨越计算机网络交换报文（message）而相互通信。发送进程生成并向网络中发送报文，接受进程接受这些报文并可能通过将报文发送回去进行响应。

在一个 P2P 文件共享系统中，文件从一个对等方中的进程传输到另一个对等方中的进程。对每对通信进程，我们通常将前者标识为客户（client），后者标识为服务器（server）。

3、套接字（Sockets）

运行在不同主机上的进程彼此通过套接字传递报文来进行通信。进程通过 Sockets 向网络发送/接受报文。

Sockets 类似于进程的通向网络的门，考虑报文发送过程：

发送进程将报文推出该门（socket）；

报文的发送还依赖该门到目的进程的门之间的运输基础设施。

4、进程寻址

为了接收分组，接收进程需要一个地址（标识）：主机地址（IP 地址）、接收进程的标识符（端口号）

常用的应用程序被指派固定的端口号（周知端口）。创建一个新的网络应用程序时必须分配一个唯一的端口号。

5、Web

Web（或 WWW）是互联网上分布式的超文本/超媒体系统，是由超链接连接而成的大规模信息和多媒体的集合（页面的形式）。

页面可以包含指向世界上任何一个连接到 Internet 上的其他页面的链接。超文本就是用超链接的方法，让一个页面链接指向另一个页面。超链接：链接到其他页面的文本字符串。

1）工作方式

以客户-服务器方式工作。

Web 客户程序：浏览器

Web 服务器：Web 文档所驻留的计算机，运行 Web 服务器程序。

客户程序向服务器程序发出请求，服务器程序向客户程序送回客户所需要的 Web 文档。

页面（page）：在一个客户程序主窗口上显示出的 Web 文档。

2）统一资源定位符 URL

使用统一资源定位符 URL 来标志万维网上的各种文档。每一个文档在整个互联网的范围内具有唯一的标识符 URL。URL 的一般格式：<协议> : // <主机> (:端口) / <路径>

6、超文本传输协议 HTTP

1）Web 应用程序使用 HTTP 协议进行通信，它使用 TCP 连接进行可靠的数据传送。

HTTP 客户端首先发起一个与 HTTP 服务器的 TCP 连接，端口号 80，服务器相应并建立 TCP 连接（三次握手），客户端和服务器进程通过套接字（sockets）访问 TCP，发送或接收 HTTP 报文，关闭 TCP 连接。

TCP 确保 HTTP 报文最终能完整顺序的到达对方。

2）HTTP 的报文有两种：请求报文和相应报文。报文采用普通的 ASCII 文本书写，HTTP 报文都是纯文本。因而每个字段的长度都是不确定的。

①请求报文由三部分组成：请求行、首部行、实体。

请求行有三个字段：方法字段、URL 字段和 HTTP 版本字段。

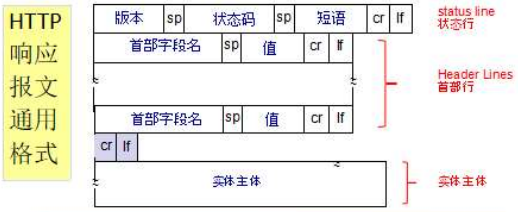
方法字段可以取几种不同的值，包括 GET、POST、HEAD、PUT 和 DELETE。绝大部分的 HTTP 请求报文使用 GET 方法。

②.响应报文由三个部分组成：初始状态行、首部行、实体

状态行有三个字段：协议版本字段、状态码和相应状态信息。

一些常见的状态码包括 200、301、400、404、505。

HTTP方法	描 述	是否包含实体
GET	从服务器上获取一份文档对象	NO
PUT	将来自客户端请求的实体部分存储到服务器上	YES
DELETE	从服务器中删除一份文档	NO
POST	向服务器发送需要处理的数据（添加注释）	YES
HEAD	仅从服务器获取文档的HTTP首部	NO



HTTP状态码	描 述
200	OK,文档正确返回
301	Redirect（重定向）,请求的已永久移动到新位置
400	Bad request,请求出错
404	Not Found,无法找到这个资源
505	HTTP Version Not Supported, HTTP版本不支持

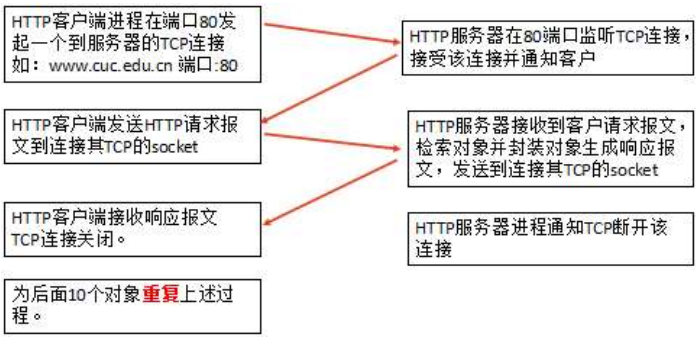
3）连接管理

HTTP 连接是 HTTP 报文传输的通道。HTTP 连接就是 TCP 连接和连接使用规则。连接一旦建立起来，服务器和客户端之间的报文交互就不会丢失、破坏和乱序。

①非持续连接

每个 TCP 连接只发送一个对象，发送完就关闭 TCP 连接。发送多个对象则需要建立多个 TCP 连接。每个对象至少需要 2RTT，草所系统要为每个连接分配缓冲区和保持 TCP 变量，客户浏览器可以配置成并行连接。

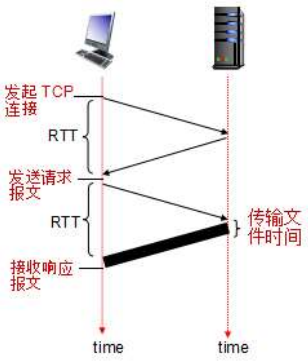
采用非持续连接的 HTTP 通信流程：



非持续连接的响应时间计算：

往返时间 RTT 定义为一个短分组从客户到服务器然后返回客户所用的时间。包括传播时延、排队时延和分组处理时延。

总相应时间 = 2RTT+文件传输时间



②持续连接

多个对象经过同一个 TCP 连接发送。HTTP1.1 协议允许使用持续连接。服务器在发送完响应报文后，仍保持 TCP 连接打开。相应客户/服务器的后续请求和相应报文可以通过相同的连接传输。客户端可以连续的发送请求报文，而不必等收到相应之后。

4）cookie

HTTP 是无状态协议。HTTP 服务器最初不保存关于客户的任何信息，简化了服务器的设计。

现在的 web 网站都使用 cookie 来跟踪用户信息。Cookie 技术的四个组件：①在 HTTP 相应报文中有一个 cookie 首部行 ②在 HTTP 请求报文中有一个 cookie 首部行 ③在客户端系统中保留有一个 cookie 文件，由用户浏览器管理 ④在 Web 站点有一个后端数据库

跟踪用户状态信息方法：

Web 站点给首次发送请求报文的用户分配一个唯一的识别码，以此唯一识别码在后端数据库产生对访问者的表项。Web 站点用一个包含 set-cookie 首部的 HTTP 相应报文将其识别码贴上。

怎样维持状态信息：

HTTP 服务器和 HTTP 客户端都管理关于回话的状态信息，HTTP 的 cookie 首部携带状态信息。

7、Web 缓存

Web 缓存（cache），也叫代理服务器（proxy server），是能够代表 Web 源氏服务器还满足 HTTP 请求的网络实体。用户的请求由缓存相应。可以配置用户浏览器将 HTTP 请求首先定到 Web 缓存器。

Web 缓存对客户端来说是服务器，对源氏服务器来说是客户端。Web 缓存一般可以是公司、学校的 LAN 上的服务器，也可以是 ISP 的服务器。Web 缓存可以降低响应时延

8、条件 GET 方法

确定缓存副本是不是最新：

通过 GET 方法来查询，缓存检查 Web 服务器中的该对象是否已被修改，发送一个条件 GET 请求报文：If-modified-since：<date>。目的是：缓存是最新的就仅发送一个相应报文头，而不是发送所请求的对象。

9、超文本标记语言 HTML

HTML 是制作和显示 Web 页面的标准语言，兴义了许多用于排版的命令（即标签），把各种标签嵌入到 Web 的页面中，这样就构成了所谓的 HTML 文档。

10、DNS 域名系统

1）标识主机的两种方式：

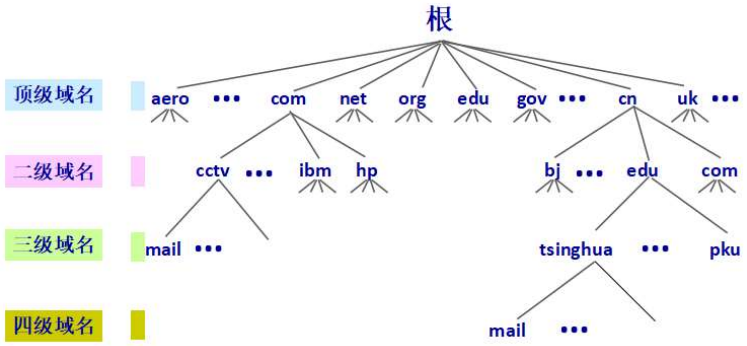
主机名：域名，由不定长的字母和数字组成，便于记忆。如 www.baidu.com

IP 地址：由四个字节组成，有着严格的层次结构。如（点分十进制）：121.7.106.83（第一字节网络号，后三字节主机号）

2）域名结构

互联网上的端系统都有一个唯一的层次结构的名字，即域名。域名采用了层次树状结构的命名方法。结构由标号序列组成，各标号之间用点隔开：… . 三级域名 . 二级域名 . 顶级域名，各标号分别代表不同级别的域名。

DNS 域名系统是由分层的 DNS 服务器实现的分布式数据库。DNS 协议允许主机查询分布式数据库的应用层协议。DNS 协议运行在 UDP 上，端口号：53。DNS 通常直接由其他的应用层协议（如 HTTP、SMTP、FTP）使用，用户只是间接使用。



4）域名服务器

①根域名服务器

共有 13 套装置。并不直接把域名直接转换成 IP 地址。

②顶级域名服务器

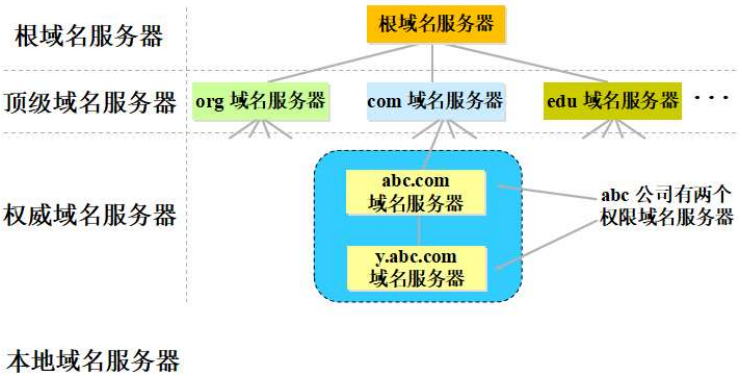
TLD 服务器，负责管理在该顶级域名服务器注册的所有二级域名。对 DNS 查询请求的相应，可能是最后的结果，也可能是下一步应当找的域名服务器的 IP 地址。

③权威域名服务器

负责一个区的域名服务器。当一个权威域名服务器还不能给最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权威域名服务器。

④本地域名服务器

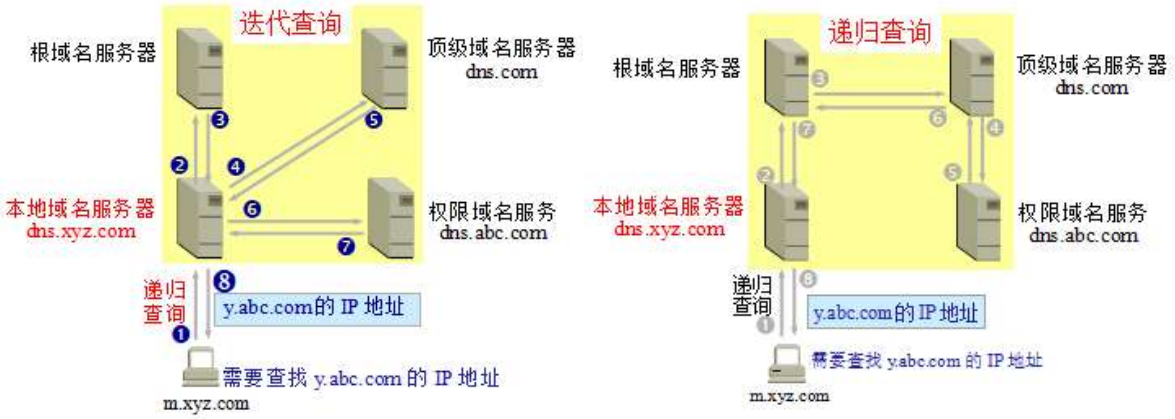
当本地域名服务器无法解析时，就向跟服务器查询。



5）提高域名服务器的可能性

DNS 域名服务器都把数据复制到几个域名服务器来保存，其中的一个是主域名服务器，其他的是辅助域名服务器。主域名服务器定期把数据复制到辅助域名服务器中。对数据的更改只能在主域名服务器中进行，这样就保证了数据的一致性。

6）域名解析



7）DNS 缓存

每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。主机→IP 地址的映射并不是永久的，域名服务器对缓存的每项内容设置计时器，确定该资源记录从缓存中删除的时间。

11、动态主机配置协议 DHCP

动态主机配置协议 DHCP 提供了即插即用联网的机制，这种机制允许一台计算机加入新的网络和获取 IP 地址而不用手工参与。

主机需要配置的项目：IP 地址、子网掩码、默认路由器的 IP 地址、域名服务器的 IP 地址

12、文件传输协议 FTP

1）FTP 提供互联网上从一台主机到另一台主机的文件传送服务。FTP 的主要功能是减少或消除在不同操作系统下处理文件的不兼容性。

FTP 使用 TCP 可靠的运输服务，使用客户服务器方式，端口号：20、21。

用户通过一个 FTP 用户代理与 FTP 服务器交互，向远程主机上传或下载文件

2）FTP 使用两个并行的 TCP 连接：控制链接、数据连接

①控制链接用于在两主机间传输控制信息。FTP 的客户机与服务器在 21 号端口上建立 TCP 连接，持续连接。FTP 的客户机通过该连接发送用户标识和口令、改变远程目录的命令。

②数据连接用于在两主机间传输文件。当服务器收到一个文件传输的命令后，在 20 端口发起一个到客户机的 TCP 连接，非持续连接。在该数据连接上传送一个文件并关闭连接。

3）FTP 与 HTTP 比较

FTP 和 HTTP 都是文件传输协议，都运行在 TCP 上。

①FTP 是带外传送：控制数据使用分离的独立连接。

HTTP 是带内传输：请求和相应的控制信息都是在传输文件的 TCP 连接中发送。

②FTP 是有状态的：FTP 服务器对每个活动用户会话的状态进行追踪，并保留；限制同时会话的总数。

HTTP 是无状态的：不对用户状态进行追踪。

13、Email 电子邮件系统

1）发送/接收步骤

发件人调用 PC 中的用户代理撰写和编辑要发送的邮件

发件人的用户代理把邮件用 SMTP 协议发给发送方邮件服务器

SMTP 服务器把邮件临时存放在邮件缓存队列中，等待发送

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，然后把邮件缓存队列中的邮件依次发送出去

运行在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

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

2）系统组成

用户代理 UA：是用户与电子邮件系统的接口，是电子邮件客户端软件。能够撰写、显示、处理和通信。

邮件服务器：按照客户-服务器方式工作。能够发送和接收邮件，同时还要向发信人报告邮件传送的情况（已交付、被拒绝、丢失等）。需要使用发送和读取两个不同的协议。

3）协议

发送邮件的协议：SMTP

读取邮件的协议：POP3 和 IMAP

RFC822 消息格式

MIME 在其邮件首部中说明了邮件的数据类型（如文本、声音、图像、视像等），使用 MIME 可在邮件中同时传送多种类型的数据。

4）报文格式

首部行（收发人、主题）：From、To、Cc、Subject

主体：报文（均为 ASCII 字符）

RFC822：首部、空行、主题

MIME：多用途互联网邮件扩展协议，用于非 ASCII 数据传输，将非 ASCII 数据编码后传输，接收方再解码还原。

第三章 运输层

1、运输层服务概述

网络边缘部分的主机的协议栈才有运输层。网络核心部分的路由器在转发分组时都只用到下三层的功能。

1）作用

运输层为相互通信的应用进程提供了逻辑通信

2）服务

面向连接的传输服务：建立连接，数据传输，释放链接

无连接的传输服务：不可靠传输

3）端口

网络的运输层使用协议端口号，简称为端口，来标识服务功能。漩口是应用层各种协议进程与运输实体进行层间交互的一种地址。

端口库由一个 16 位端口号来表示。端口号只具有本地意义，端口号只是为了标识本地主机应用层中的各进程。在互联网中，不同计算机的相同端口号是没有联系的。两个计算机中的进程要互相通信，不仅必须知道对方的 IP 地址（为了找到对方的主机），而且还要知道对方的端口号（为了找到对方主机中的应用进程）。

服务器端使用的端口号

熟知端口，数值一般为 0~1023

登记端口号，数值为 1024~49151，为没有熟知端口号的应用程序使用的

客户端使用的端口号

短暂端口号，数值为 49152~65535，留给客户进程选择暂时使用

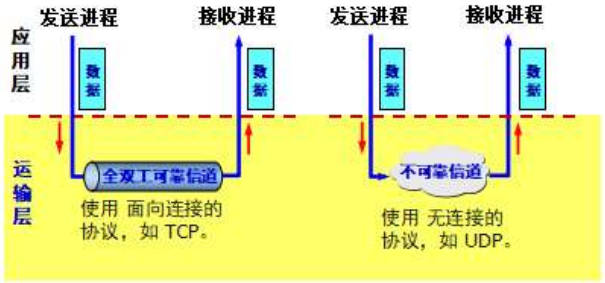
2、多路复用与多路分解

多路复用：将不同套接字中收集的数据块生成报文段（分组）并传递到网络的过程。

多路分解：将传输报文段定向到对应的套接字的过程。

在接受主机分解：将接受到的报文段交付给正确的套接字。

在发送主机复用：从多个套接字收集数据，为数据封装首部。



3、用户数据报协议 UDP

无连接传输 UDP 只在 IP 的数据服务上增加了很少一点的功能，这就是复用和分用的功能以及差错监测的功能。

主要特点：

无连接，尽力而为，面向报文，没有拥塞控制，支持一对一、一对多、多对一和多对多的交互通信，首部开销小。

4、可靠数据传输原理

Rdt1.0：经完全可靠信道的可靠数据传输

Rdt2.0：经具有比特差错信道的可靠数据传输

Rdt2.1：使用了从接收方到发送方的肯定确认和否定确认

Rdt2.2：在有比特差错信道上实现的一个无 NAK 的可靠数据传输协议

Rdt3.0：具有比特差错的丢包信道的可靠数据传输（停等协议）

流水线可靠数据传输协议

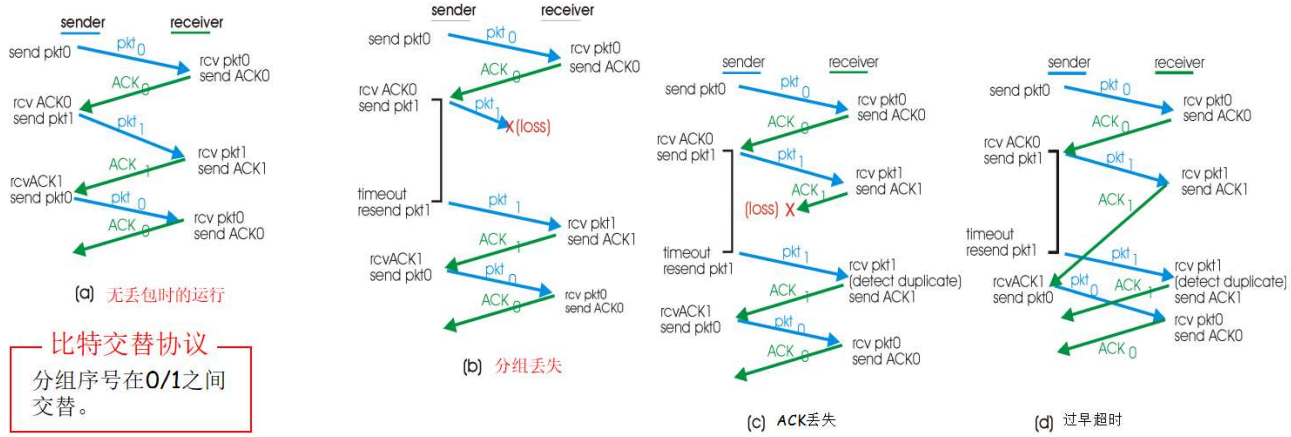
滑动窗口协议：采用连续 ARQ，是 TCP 协议的精髓。

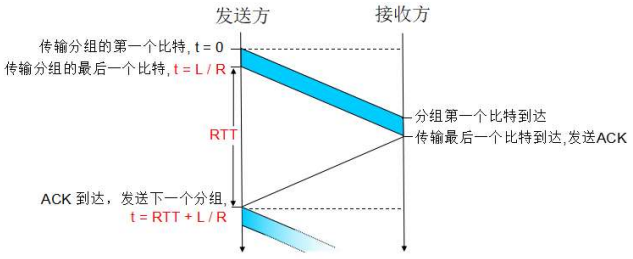
连续 ARQ 协议：发送方维持一个发送窗口，位于发送窗口内的分组都可连续发送出去，而不需要等待对方的确认，发送方每收到一个确认，就把发送窗口向前滑动一个分组的位置。

接收方一般采用累计确认的方式，不必对收到的分组逐个发送确认，而是对按序到达的最后一个分组发送确认。累计确认容易实现，但不能向发送方反映出接收方已经正确收到的所有分组的信息。

发送分组若有丢失则发送方需要把丢失的分组再重传一次，叫做 Go-Back-N（绘图 N），表示需要再退回来重传已发送过的 N 个分组。

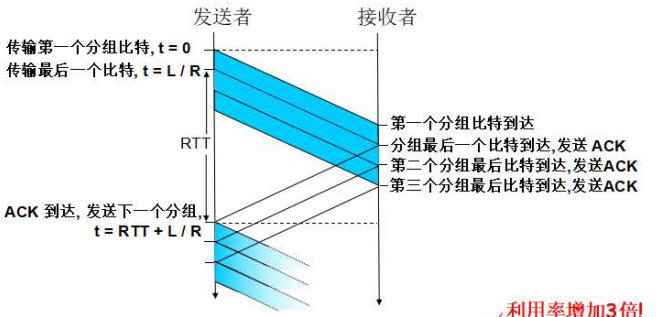
选择性重传（SR）





$$T_{transmit} = \frac{L\ (\text{packet length in bits})}{R\ (\text{transmission rate, bps})} = \frac{8\text{kb/pkt}}{10\text{^}9\ \text{b/sec}} = 8\ \text{us}$$

$$U_{sender} = \frac{L / R}{RTT + L / R} = \frac{.008}{30.008} = 0.00027$$



$$U_{sender} = \frac{3 * L / R}{RTT + L / R} = \frac{.024}{30.008} = 0.0008$$

利用率增加3倍!

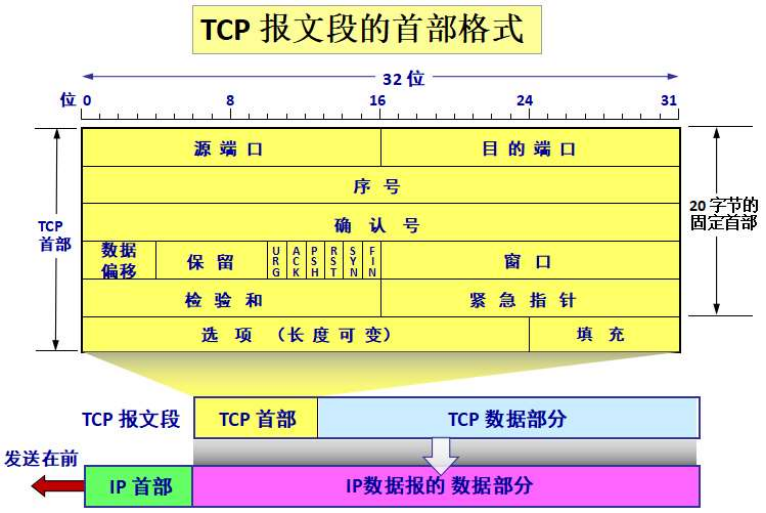
5、传输控制协议 TCP

1）主要特点：面向连接的运输层协议，每一条 TCP 连接只能有两个端点，每一条 TCP 连接只能是点对点的，提供可靠交付的服务，提供全双工通信，面向字节流（TCP 中的“流”指的是流入或流出进程的字节序列。“面向字节流”的含义是：虽然应用程序和 TCP 的交互是一次一个数据块，但 TCP 把应用程序交下来的数据看成仅仅是一连串无结构的字节流）。

2）报文段结构

一个 TCP 报文段分为首部和数据两部分，而 TCP 的全部功能都体现在它首部中各个字段的作用。

TCP 报文段首部的前 20 个字节试固定的，后面有 4n 字节试根据需要而增加的选项。因此 TCP 首部的最小长度是 20 字节。



源端口和目的端口：各占 2 字节，分别写入源端口号和目的端口号。

序号：占 4 字节。序号范围是[0,2^{32}-1]。

确认号：占 4 字节，是期望收到对方下一个报文段的第一个数据字节的序号。

数据偏移：占 4 字位支出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远，

保留：占 2 位，保留为今后使用，但目前应置为 0。

紧急 URG：当 URG=1 时，表明紧急指针字段有效。告诉系统此报文段中有紧急数据，应尽快传送。

确认 ACK：仅当 ACK=1 时确认号字段才有效，当 ACK=0 时，确认号无效。

推送 PSH：接受 TCP 收到 PSH=1 的报文段，就尽快交付接受应用进程，而不再等到整个缓存都填满了后再向上交付。

复位 RST ：当 RST=1 时，表明 TCP 连接中出现严重差错（如由于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。

同步 SYN：SYN=1 表示这是一个连接请求或连接接受报文。

终止 FIN：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。

窗口：占 2 字节，用来让对方设置发送窗口的依据，单位为字节。

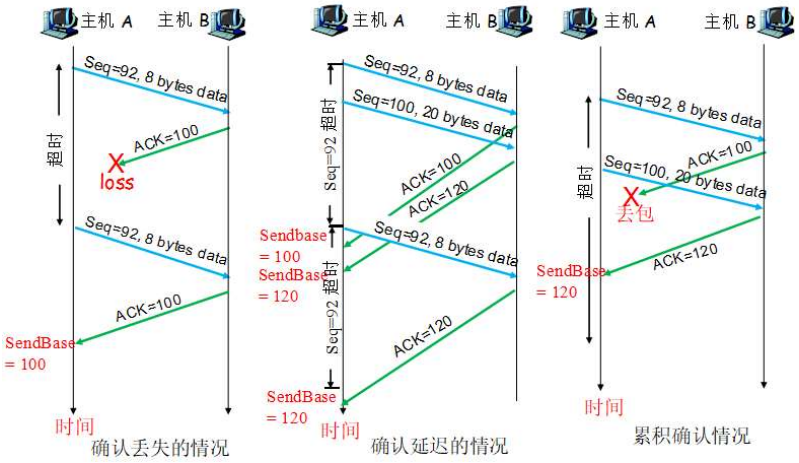
检验和：占 2 字节。检验和字段检验的范围包括首部和数据这两部分。在计算检验和时，要在 TCP 报文段的前面加上 12 字节的伪首部。

紧急指针：占 16 位，指出在本报文段中紧急数据共有多少个字节，紧急数据放在本报文段数据的最前面。

选项：长度可变，最多 40 字节。

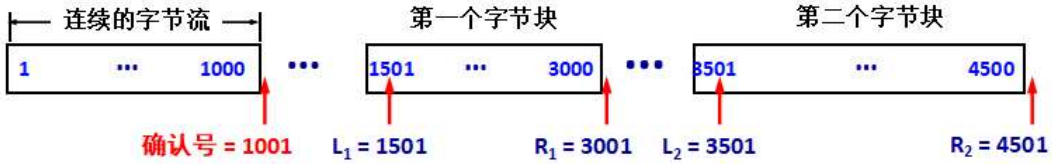
3）超时重传

超时重传一个分组：最早的未被确认的分组。超时前，未收到 ACK(n)而先收到 ACK(n+1)，TCP 不会重传分组 n。超时事件发生，重启计时器。对同一分组每重启一次计时器，计时器超时时间加倍。收到确认，计时器超时时间恢复为 RTT 推算值



4）选择确认 SACK

TCP 的接收方通过选择确认，告诉发送方缓存的不连续字节块的边界信息，每一个不连续字节块都有两个边界，左边界和右边界。



6、流量控制

流量控制就是让发送方的发送速率不要太快，要让接收方来得及接收。利用个滑动窗口机制可以很方便地在 TCP 连接上实现对发送方的流量控制。

发送方的发送窗口不能超过接收方给出的接收窗口的数值（TCP 的窗口单位是字节不是报文段）。

7、拥塞控制

网络中某段时间内，某资源的需求超过了该资源所能提供的可用部分，使得网络的性能变坏，这种现象称为拥塞。出现拥塞的原因为： ∑对资源需求>可用资源

拥塞表现为丢包（路由器缓冲区溢出）和长时延（路由器缓冲区中排队）。

1）与流量控制的区别：

拥塞控制就是防止过多的数据注入到网络中，使网络中的路由器或链路不致过载。是一个全局性的过程，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。

流量控制往往指点对点通信量的控制，是个端到端的问题（接收端控制发送段），所要做的是抑制发送端发送数据的速率，以便接收端来得及接受。

2）几种拥塞控制方法

慢开始、拥塞避免、快重传、快恢复

3）拥塞窗口

TCP 采用基于窗口的方法进行拥塞控制，开始时设定接收窗口 rwnd，发送方的窗口不能超过接收方给出的接收窗口的数值。TCP 发送方维持一个拥塞窗口 cwnd。拥塞窗口的大小取决于网络的拥塞程度，并且动态地变换。发送端利用拥塞窗口根据网络的拥塞情况调整发送的数据量。也就是发送窗口大小不仅取决于接收方公告的接收窗口，还取决于网络的拥塞状况。所以真正的发送窗口值=Min（rwnd，cwnd）

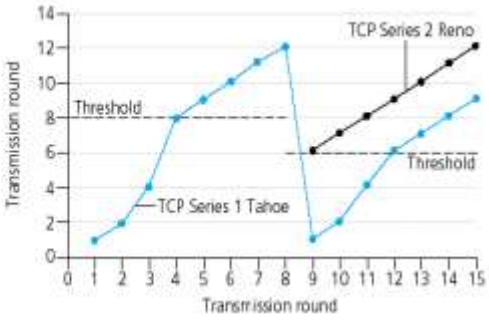
4）慢启动与拥塞避免

慢启动：由小到大逐渐增大拥塞窗口值，每收到一个数据报文段的确认后，cwnd 就增加 1 个 MSS（最大报文段）的数值；即每经过一个 RTT，cwnd 的值就加倍。

拥塞避免：每经过一个往返时间 RTT 就把发送方的拥塞窗口 cwnd 加 1，而不是加倍，使拥塞窗口 cwnd 按线性规律缓慢增长。

慢启动门限 ssthresh：防止拥塞窗口 cwnd 增长过大引起网络拥塞。当 cwnd<ssthresh 时，使用慢启动算法，cwnd 指数增长；当 cwnd≥ssthresh 时，停止使用慢启动算法而改用拥塞避免算法，cwnd 线性增长。当超时发生时，阈值 ssthresh 设置为 cwnd/2，并且 cwnd 设置为 1MSS；当出现三个冗余确认时，阈值 ssthresh 设置为 cwnd/2，且 cwnd 设置为 ssthresh。

初始门限ssthresh=8



第三章课后题

1、一个 UDP 用户数据报的数据字段为 8192 字节。在链路层要使用以太网来传送。试问应当划分为几个 IP 数据报片？说明给每一个 IP 数据报片的数据字段长度和片偏移字段的值。

答：6 个

数据字段的长度：前 5 个是 1480 字节，最后一个是 800 字节。

片偏移字段的值分别是：0，1480，2960，4440，5920 和 7400.

2、主机 A 向主机 B 房一个很长的文件，其长度为 L 字节。假定 TCP 使用的 MSS 为 1460 字节。

（1）在 TCP 的序号不重复使用的条件下，L 的最大值是多少？

（2）假定使用上面计算出的文件长度，而运输层、网络层和数据链路层所用的首部开销共 66 细节，链路的数据率为 10Mb/s，试求这个文件所需的最短发送时间。

解：（1）L_max 的最大值是 2^32=4GB,G=2^30.

(2) 满载分片数 Q={L_max/MSS}取整=2941758 发送的总报文数

N=Q*(MSS+66)+{（L_max-Q*MSS）+66}=4489122708+682=4489123390

总字节数是 N=4489123390 字节，发送 4489123390 字节需时间为：N*8/（10*10^6）=3591.3 秒，即 59.85 分，约 1 小时。

3、通信信道带宽为 1Gb/s，端到端传播时延为 10ms。TCP 的发送窗口为 65535 字节。试问：可能达到的最大吞吐量是多少？信道的利用率是多少？

答：

L=65536×8+40×8=524600

C=109b/s

L/C=0.0005246s

Td=10×10-3s

0.02104864

Throughput=L/(L/C+2×Td)=524600/0.0205246=25.5Mb/s

Efficiency=(L/C)//(L/C+2×D)=0.0255

最大吞吐量为 25.5Mb/s。信道利用率为 25.5/1000=2.55%

3、TCP 的拥塞窗口 cwnd 大小与传输轮次 n 的关系如下所示：

Cwnd	1	2	4	8	16	32	33	34	35	36	37	38	39
N	1	2	3	4	5	6	7	8	9	10	11	12	13
Cwnd	40	41	42	21	22	23	24	25	26	1	2	4	8
N	14	15	16	17	18	19	20	21	22	23	24	25	26

（1）试画出拥塞窗口与传输轮次的关系曲线。

（2）指明 TCP 工作在慢开始阶段的时间间隔。

（3）指明 TCP 工作在拥塞避免截断的时间间隔。

（4）在第 16 轮次和第 22 轮次之后发送方是通过收到三个重复的确认还是通过超时检测到丢失了报文段？

（5）在第 1 轮次、第 18 轮次和第 24 轮次发送时，门限 ssthresh 分别被设置为多大？

（6）在第几轮次发送出第 70 个报文段？

（7）假定在第 26 轮次之后收到了三个重复的确认，因而检测出了报文段的丢失，那么拥塞窗口 cwnd 和门限 ssthresh 应设置为多大？

答：（1）拥塞窗口与传输轮次的关系曲线如图所示（课本后答案）：

（2） 慢开始时间间隔：【1，6】和【23，26】

（3） 拥塞避免时间间隔：【6，16】和【17，22】

（4） 在第 16 轮次之后发送方通过收到三个重复的确认检测到丢失的报文段。在第 22 轮次之后发送方是通过超时检测到丢失的报文段。

（5） 在第 1 轮次发送时，门限 ssthresh 被设置为 32
在第 18 轮次发送时，门限 ssthresh 被设置为发生拥塞时的一半，即 21.
在第 24 轮次发送时，门限 ssthresh 是第 18 轮次发送时设置的 21

（6） 第 70 报文段在第 7 轮次发送出。

（7） 拥塞窗口 cwnd 和门限 ssthresh 应设置为 8 的一半，即 4.

第四章 网络层

1、网络层服务

网络层提供主机到主机的通信服务，因特网网络采用尽力而为的服务模型

关键功能：

转发：将分组从路由器的输入移动到适当的路由器输出

选路：决定分组从源到目的地所采用的路由（路径）

网络层的协议数据单元 PDU 是数据报（分组）

2、网络层为传输层提供的服务：

1）虚电路网络提供网络层连接服务

面向连接服务：借鉴电信网的经验，由网络层实现复杂功能，提供可靠的、面向连接的服务（通信子网）。

与电路交换的连接不同，虚电路（VC）只是一条逻辑上的连接，分组都沿着这条逻辑连接按照存储转发的方式传送，但并不是真正建立了一条物理连接。

虚电路数据传送的阶段：

①VC 建立，呼叫/指定接受地址/确定链路 VC 号/预留资源

②数据传送，沿着虚电路传送数据

③VC 拆除，结束呼叫并更新转发表

2）数据报网络提供网络层无连接服务

无连接服务：Internet 观点，网络层向上值提供简单灵活的、无连接的、尽最大努力交付的数据报服务，将复杂的功能放在传输层。

每一个分组（即 IP 数据报）独立发送，与其前后的分组无关。

网络层不提供服务质量的承诺。即所传送的分组可能出错、丢失、重复和失序，也不保证分组传送的时限。

对比的项	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由端系统来保证
连接的建立	必须有	不需要
终点地址	仅在连接建立阶段使用，每个分组使用短的虚电路号	每个分组都有终点的完整地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
当结点出故障时	所有通过出故障的结点的虚电路均不能工作	出故障的结点可能会丢失分组，一些路由可能会发生变化
分组的顺序	总是按发送顺序到达终点	到达终点时不一定按发送顺序
端到端的差错处理和流量控制	可以由网络负责，也可以由端系统负责	由端系统负责

3、路由器转发表

IP 地址：32bit，{<网络号>,<主机号>}

通常从一个网络转发到另一个网络

转发根据路由表进行 IP 最长地址前缀匹配

4、 路由器的构成

1）功能

维护路由表：运行选路算法/协议（RIP，OSPF，BGP）

转发数据报：从入链路到出链路的分组交换

2）构成

路由转发平面 ┌ 输入端口
              ├ 交换结构
              └ 输出端口

路由控制平面

①输入端口

查找：根据目的地址，在转发表中查找对应的输出短偶

转发：将分组发送进交换结构

排队：被阻塞的分组进入队列排队

②输出端口

队列缓存：交换结构传送速率比线路传输速率更快时，输入输出缓存都存在队列延时、溢出丢包

分组调度：选择排队的数据报进行发送

5、网际协议 IP

网际协议 IP 是 TCP/IP 体系中两个最主要的协议之一，也是最重要的因特网标准协议之一。与 IP 协议配套使用的还有三个协议：地址解析协议 ARP、网际控制报文协议 ICMP、网际组管理协议 IGMP

1）数据报格式

一个 IP 数据报由首部和数据两部分组成。

首部的前一部分是 20 字节的固定长度，是 IP 数据报必须具有的。首部的固定部分之后是可选字段，其长度是可变的，不超过 40 字节。

版本：占 4 位，指 IP 协议的版本。目前的 IP 协议版本号为 4 (即 IPv4)。

首部长度：占 4 位，可表示的最大数值是 15 个单位，单位为 4 字节，即 IP 的首部长度的最大值是 60 字节。

区分服务：占 8 位，一般的情况下都不使用，只有在使用区分服务（DiffServ）时，这个字段才起作用。

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 65535 字节。总长度必须不超过最大传送单元 MTU。

标识(identification) ：占 16 位，它是一个计数器，用来产生 IP 数据报的标识。

标志(flag)：占 3 位，目前只有前两位有意义。

标志字段最低位是 MF (More Fragment)。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 (Don't Fragment) 。只有当 DF=0 时才允许分片。

片偏移：占 13 位，表示较长的分组在分片后，该片在原分组中的相对位置。片偏移以 8 个字节为偏移单位。

生存时间：占 8 位，记为 TTL (Time To Live)，指示数据报在网络中可通过的最大跳数(最大路由器数)。

协议：占 8 位，表示此数据报携带的数据所使用的协议。

首部检验和：占 16 位，只检验数据报的首部，不检验数据部分。检验和采用简单 16 位二进制反码求和算法。

源地址和目的地址：各占 4 字节，IP 地址。

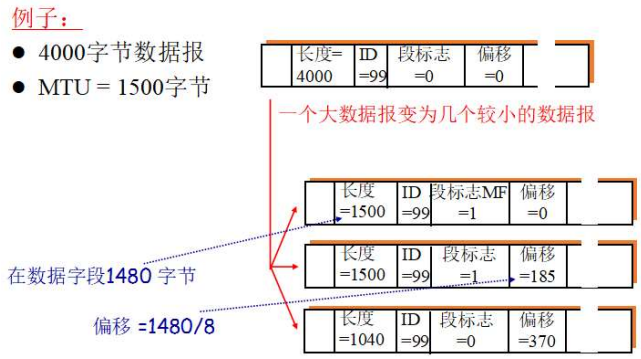
2）IP 分片

①原因：

网络链路能承载的最大传输单元 MTU 的限制

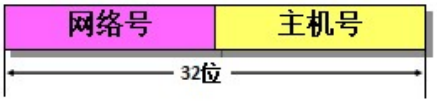
不同的链路类型，不同的 MTU

②划分和重新组装



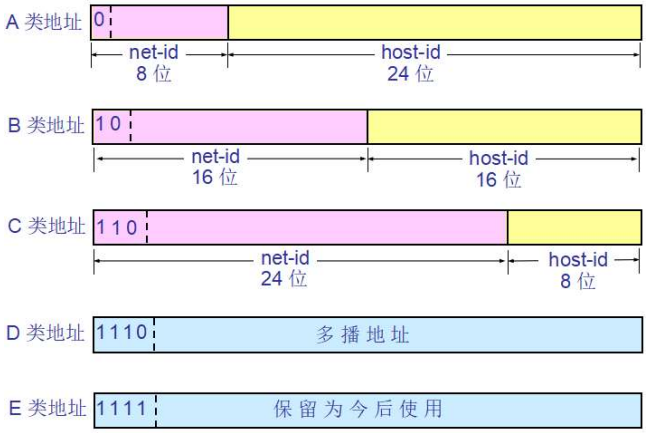
3）IPv4

每一类地址都由两个固定长度的字段组成，其中一个字段是网络号 net-id，它标志主机（或路由器）所连接到的网络，另一个字段是主机号 host-id，它标志该主机（或路由器）。



IP 地址 ::= { <网络号>, <主机号> }

①IP 地址的分类



常用的三种类别的 IP 地址

A类：1.0.0.1-126.255.255.255

00000001 00000000 00000000 00000001-
01111110 11111111 11111111 11111111

B类：128.1.0.1-191.255.255.255

10000000 00000001 00000000 00000001-
10111111 11111111 11111111 11111111

C类：192.0.1.1-223.255.255.255

11000000 00000000 00000001 00000001-
11011111 11111111 11111111 11111111

IP 地址的指派范围

网络类别	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中最大主机数
A	126 (2^7-2)	1	126	16,777,214
B	16383 ($2^{14}-1$)	128.1	191.255	65,534
C	2097151 ($2^{21}-1$)	192.0.1	223.255.255	254

一般不使用的特殊的 IP 地址

- 3组私有地址（仅用在局域网）
  - A类：10.0.0.0~10.255.255.255
  - B类：172.16.0.0~172.31.255.255
  - C类：192.168.0.0~192.168.255.255

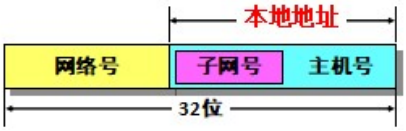
网络号	主机号	源地址使用	目的地址使用	代表的意思
0	0	Yes	No	在本网络上的本主机（DHCP协议）
0	host-id	Yes	No	在本网络上的某台主机 host-id
全1	全1	No	Yes	只在本网络上进行广播（受限广播，路由器不转发）
net-id	全1	No	Yes	对net-id上的所有主机进行广播
127	非全0或全1的任何数	Yes	Yes	用作本地软件环回测试之用

②划分子网

IP 地址中又增加了一个“子网号字段”，使两级的 IP 地址变成为三级的 IP 地址。

从主机号借用若干个位作为子网号 subnet-id，而主机号 host-id 也就相应减少了若干个位。

划分子网纯属一个单位内部的事情。单位对外仍表现为没有划分子网的网络。



IP 地址 ::= {<网络号>, <子网号>, <主机号>}

③子网掩码

从一个 IP 数据报的首部并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。使用子网掩码（subnet mask）可以找出 IP 地址中的子网部分

规则：子网掩码长度=32 位。某位=1：IP 地址中的对应位为网络号和子网号。某位=0：IP 地址中的对应位为主机号。

4）网络地址转换 NAT

NAT 的作用：解决 IP 地址匮乏问题

保守解决方案：为连在网上并使用网络的计算机动态分配一个 IP 地址，主机不活跃时回收该 IP 地址，再分配给其他活跃的计算机

长期解决方案：从 IPv4 迁移到 IPv6

快速方案：目前普遍使用网络地址转换

5）互联网控制报文协议 ICMP

ICMP 是 IP 层的一个组成部分，IP 数据报中携带 ICMP 报文

ICMP 的作用：它传递差错报文或其他需要注意的信息，由主机或路由器用于网络级信息的通信

应用举例：PING

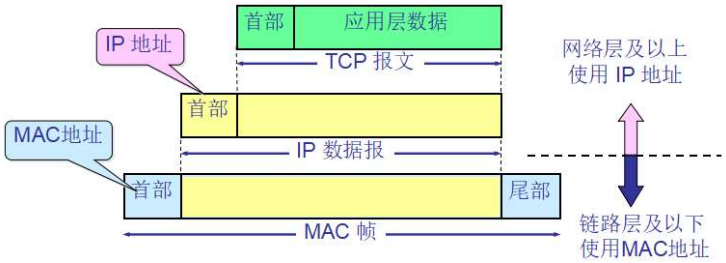
PING 用来测试两个主机之间的连通性。PING 使用了 ICMP 回送请求与回送回答报文。PING 是应用层直接使用 ICMP 的例子，它没有通过运输层的 TCP 或 UDP。

6）ARP 协议

因特网中的每个节点采用网络层地址（IP 地址）来唯一标识。用于把分组送到目的 IP 网络，长度为 32 比特（IPv4）。网络层及以上使用 IP 地址交互，而实际通信必须使用物理地址。

①MAC 地址（物理地址）：

是结点“网卡”本身所带的地址，MAC 地址长度通常为 6 字节，共 2^{48} 个，6 字节地址用 16 进制表示，每个字节以 1 对 16 进制数表示，“网卡”的 MAC 地址是永久的（生产时固化在其 ROM 里）。



②ARP 的作用：从网络层的 IP 地址解析出在数据链路层使用的硬件地址。

③工作过程：

每一个主机都有一个 ARP 高速缓存(ARP cache)，里面缓存所在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（ARP 表）。

ARP 表: 对所在 LAN 每个节点的 IP/MAC 地址映射表。< IP 地址; MAC 地址; TTL>

LAN 上节点(主机、路由器)都通过广播方式获得目的 MAC 地址。

从 IP 地址到硬件地址的解析是自动进行的。

ARP 请求和响应的报文格式：

目的 MAC	源 MAC	帧类型	硬件类型	协议类型	…	发端 MAC	发端 IP	目标 MAC	目标 IP

④使用 ARP 的四种典型情况

发送方是主机，要把 IP 数据报发送到本网络上的另一个主机。这时用 ARP 找到目的主机的硬件地址。

发送方是主机，要把 IP 数据报发送到另一个网络上的一个主机。这时用 ARP 找到本网络上的一个路由器的硬件地址。剩下的工作由这个路由器来完成。

发送方是路由器，要把 IP 数据报转发到本网络上的一个主机。这时用 ARP 找到目的主机的硬件地址。

发送方是路由器，要把 IP 数据报转发到另一个网络上的一个主机。这时用 ARP 找到本网络上另一个路由器的硬件地址。剩下的工作由这个路由器来完成。

7）IPv6

IPv6 仍支持无连接的分组传送。分组即协议数据单元 PDU。

IPv6 相对 IPv4 的主要变化如下：

更大的地址空间。IPv6 将地址从 IPv4 的 32 位增大到了 128 位。

简洁高效的首部。IPv6 定义了 40 字节的定长首部，舍弃了不必要的字段或作为选项。

流标签和优先级。IPv6 首部可标识流和区分流的优先级。

改进的选项。IPv6 允许数据报包含有选项的控制信息，其选项放在有效载荷中。

支持即插即用（即自动配置）。因此 IPv6 不需要使用 DHCP。

支持资源的预分配。IPv6 支持实时视像等要求，保证一定的带宽和时延的应用。

IPv6 首部改为 8 字节对齐。首部长度必须是 8 字节的整数倍。

使用冒号 16 进制记法。冒号十六进制记法中：

允许把数字前面的 0 省略。

0000 可写成一个 0，省略前三个 0。

允许零压缩，即连续的零可以用一对冒号表示，但只能用一次。例如 FF05:0:0:0:0:0:0:B3 可压缩为： FF05::B3

CIDR 的斜线表示法仍然可用。

例如 60 位的前缀 12AB00000000CD3

可记为 12AB:0000:0000:CD30:0000:0000:0000:0000/60

写作 12AB::CD30:0:0:0:0/60 或 12AB:0:0:CD30::/60 （零压缩）

地址类型	二进制前缀
未指明地址	00…0（128位），可记为 ::/128。
环回地址	00…1（128位），可记为 ::1/128。
多播地址	11111111（8位），可记为 FF00::/8。
本地链路单播地址	1111111010（10位），可记为 FE80::/10。
全球单播地址	（除上述四种外，所有其他的二进制前缀）

6、路由选择算法

1）距离向量（DV）路由选择算法

全局式路由选择算法，路由器向所有其他路由器交换信息（洪泛式），交换的是与相邻路由器的连通性和链路费用，所有路由器具有完全的拓扑、链路费用信息。

①Bellman-Ford 方程 （动态规划）定义:

d_x（y）:=从 x 到 y 最低费用路径的费用。d_x（y） = min { c（x,v）+ d_v（y）}

其中 c（x,v）为 x 到其邻居 v 的链路费用，min 是对 x 的所有邻居 v 取最小

x 结点：

x 知道自己与所有邻居结点 v 的链路费用 c（x,v）。

x 与邻居 v 交换各自到网络其他所有结点的链路费用信息：Dv = [D_v（y）： y∈N]

②基本思想

每个结点周期性的向其邻居结点发送它自己所维护的到网络其他结点的距离向量估计（DV）。

当结点 x 接收到来自邻居的新 DV 估计，它使用 B-F 方程更新其自己的 DV：

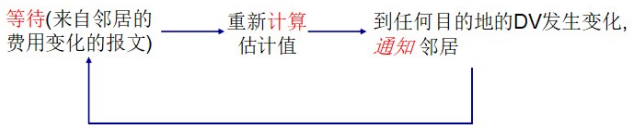
$D_x(y) \leftarrow \min_v\{c(x,v) + Dv(y)\}$ for each node y∈N

③算法

算法迭代：每次本地算法迭代由下列引起:

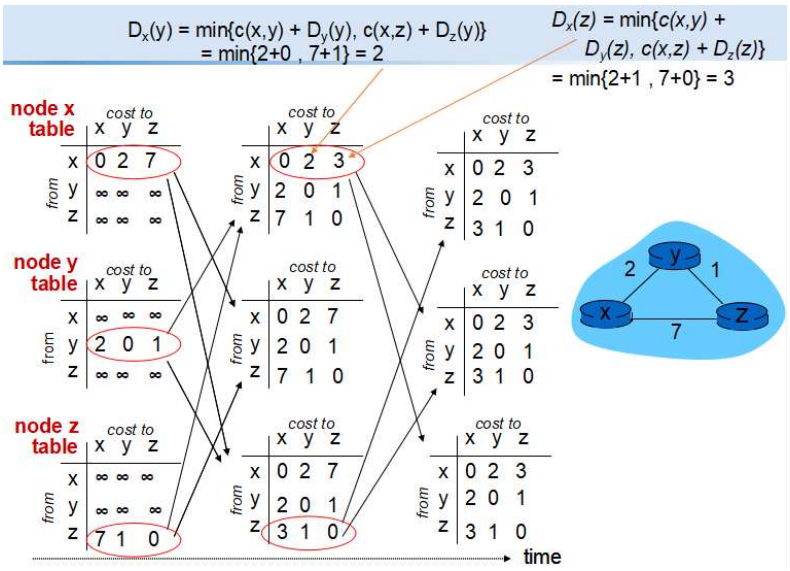
本地链路费用改变

从邻居接收到 DV 更新报文



算法分布式：

每个节点仅当其 DV 改变时通知邻居



2）链路状态（LS）路由算法

分散式路由选择算法，路由器只和相邻路由器交换信息，交换的是路由表（到其他所有目的网络的距离），分布式、迭代计算方式。

①Dijkstra 算法：

所有节点知道网络拓扑、链路费用。经“链路状态广播”完成信息传送，所有节点具有相同信息。

从一个结点（源）到所有其他结点计算最低费用路径。得出路由表，即沿最短路径的上一跳。

迭代：k 次迭代后，得知到 k 个目的地的最低费用路径

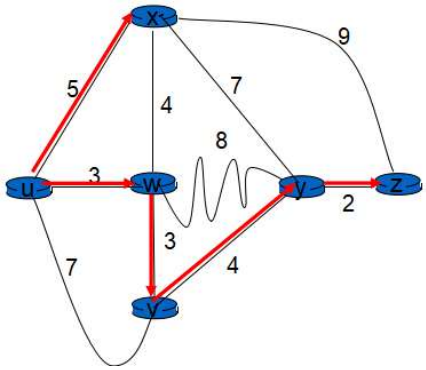
c(x,y): 从结点 x 到 y 的链路费用，如果不是直接邻居则=∞。

D(v):从源到目的地 v 路径费用的当前值。

p(v): 从源到 v 沿路径的前一结点。

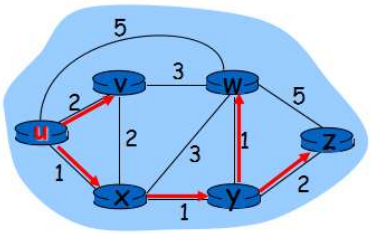
N’：已知在最小费用路径中的节点集合。

注意：最短路径树是基于前一结点来构建



Step	N'	D(v) p(v)	D(w) p(w)	D(x) p(x)	D(y) p(y)	D(z) p(z)
0	u	7,u	3,u	5,u	∞	∞
1	uw	6,w		5,u	11,w	∞
2	uwx	6,w			11,w	14,x
3	uwxv				10,v	14,x
4	uwxvy					12,y
5	uwxvyz					

步骤	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					



3）LS 和 DV 算法的比较

报文复杂性：对 N 个结点，E 条链路的网络

LS：向所有结点交换，发送 O（|N| |E|）报文

DV：仅在邻居之间交换，仅当最低费用路径改变时交换

收敛速度：

LS：算法计算复杂性 O（$|N|^2$），可能具有震荡

DV：收敛较慢，可能由选路环路，无穷计数问题

健壮性：如果路由器异常，将发生什么现象

LS：每个结点仅计算它自己的路由表，隔离

DV：每个结点的表能由其他结点使用，导致差错通过网络传播

7、域间路由算法 BGP

BGP（边界网关协议）——BGP4

BGP 所交换的网络可达性信息就是要到达某个网络所要经过的一系列自治系统 AS。

向 AS 内部的所有路由器传播可达性信息。

基于可达性信息和策略，决定到子网的“好”路由。

BGP 对等方交换选路信息通过半永久的 TCP 连接。

BGP 支持 CIDR。

8、广播路由算法

1）洪泛

复制分组向除接受该分组的邻居以外的所有其他邻居转发。

会形成广播风暴

2）受控洪泛

序号控制洪泛：分组添加源标识（地址）和广播序号。

反向路径转发（RPF）——（RPB，反向路径广播）。

思想：广播分组来自于路由器到分组源地址的最短单播路径上就复制转发，否则丢弃不转发。

3）生成树广播（spanning tree）

消除了冗余的广播分组

最小生成树——prim 算法，kruskal 算法

目的：构造和维护最小生成树

输入：图 G=（N,E）

输出：包含所有顶点 N 的无环的连通的子图构成一棵树，该图的所有链路费用之和最小，即为最小生成树。

①prim 算法：

首先任取一个顶点加入生成树 G’；

在那些一个端点在生成树里，另一个端点不在生成树里的边中，选取一条费用最小的边，将该边和另一个端点加入生成树 G’。

重复上一步，直到所有的顶点都进入了生成树为止，此时的生成树 G’就是最小生成树。

②kruskal 算法：

构造只包含图 G 所有顶点、边集合为空的子图 G’，G’构成一个森林，每个顶点为一棵独立的树。

G 的边集按费用从小到大排序。

从中选取一条费用最小的边，若该边的两个顶点分属不同的树，则将其加入子图 G’；反之，若该边的两个顶点已落在同一棵树上，则不可取。

按序取下一条费用最小的边，依次类推，直至所有顶点都构成连通的一棵树。

第四章课后题

1、设某路由器建立了如下路由表：

目的网络	子网掩码	下一跳
128.96.39.0	255.255.255.128	接口 m0
128.96.39.129	255.255.255.128	接口 m1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
*（模拟）	-	R4

现共收到 5 个分组，其目的地址分别为：

（1）128.96.39.10

（2）128.96.40.12

（3）128.。96.40.0

（4）192.4.153.17

（5）192.4.153.90

试分别计算其下一跳

解：（1）分组的目的站 IP 地址为：128.96.39.10。先与子网掩码 255.255.255.128 相与，得 128.96.39.0，可见该分组经接口 0 转发。

（2）分组的目的 IP 地址为：128.96.40.12。

① 与子网掩码 255.255.255.128 相与得 128.96.40.0，不等于 128.96.39.0。

② 与子网掩码 255.255.255.128 相与得 128.96.40.0，经查路由表可知，该项分组经 R2 转发。

（3）分组的目的 IP 地址为：128.96.40.151，与子网掩码 255.255.255.128 相与后得 128.96.40.128，与子网掩码 255.255.255.192 相与后得 128.96.40.128，经查路由表知，该分组转发选择默认路由，经 R4 转发。

（4）分组的目的 IP 地址为：192.4.153.17。与子网掩码 255.255.255.128 相与后得 192.4.153.0。与子网掩码 255.255.255.192 相与后得 192.4.153.0，经查路由表知，该分组经 R3 转发。

（5）分组的目的 IP 地址为：192.4.153.90，与子网掩码 255.255.255.128 相与后得 192.4.153.0。与子网掩码 255.255.255.192 相与后得 192.4.153.64，经查路由表知，该分组转发选择默认路由，经 R4 转发。

2、一个数据报长度为 4000 字节（固定首部长度）。现经过一个网络传送，但此网络能够传送的最大数据长度为 1500 字节。试问应当划分为几个短些的数据报片？各数据报片的数据字段长度、片偏移字段和 MF 标志应为何数值？

答：IP 数据报固定首部长度为 20 字节

	总长度(字节)	数据长度(字节)	MF	片偏移
原始数据报	4000	3980	0	0
数据报片 1	1500	1480	1	0
数据报片 2	1500	1480	1	185
数据报片 3	1040	1020	0	370

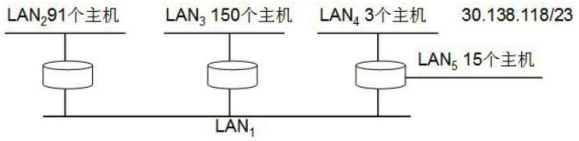
3、某单位分配到一个 B 类 IP 地址，其 net-id 为 129.250.0.0。该单位有 4000 台机器，平均分布在 16 个不同的地点。如选用子网掩码为 255.255.255.0，试给每一个地方分配一个子网号码，并计算出每个地点主级号码的最小值和最大值。

答：4000/16=250，平均每个地点 250 台机器。如选 255.255.255.0 为掩码，则每个网络所连主机数=28-2=254>250，共有子网数=28-2=254>16，能满足实际需求。

可给每个地点分配如下子网号码

地点：	子网号（subnet-id）	子网网络号	主机 IP 的最小值和最大值
1：	00000001	129.250.1.0	129.250.1.1---129.250.1.254
2：	00000010	129.250.2.0	129.250.2.1---129.250.2.254
3：	00000011	129.250.3.0	129.250.3.1---129.250.3.254
4：	00000100	129.250.4.0	129.250.4.1---129.250.4.254
5：	00000101	129.250.5.0	129.250.5.1---129.250.5.254
6：	00000110	129.250.6.0	129.250.6.1---129.250.6.254
7：	00000111	129.250.7.0	129.250.7.1---129.250.7.254
8：	00001000	129.250.8.0	129.250.8.1---129.250.8.254
9：	00001001	129.250.9.0	129.250.9.1---129.250.9.254
10：	00001010	129.250.10.0	129.250.10.1---129.250.10.254
11：	00001011	129.250.11.0	129.250.11.1---129.250.11.254
12：	00001100	129.250.12.0	129.250.12.1---129.250.12.254
13：	00001101	129.250.13.0	129.250.13.1---129.250.13.254
14：	00001110	129.250.14.0	129.250.14.1---129.250.14.254
15：	00001111	129.250.15.0	129.250.15.1---129.250.15.254
16：	00010000	129.250.16.0	129.250.16.1---129.250.16.254

4、一个自治系统有 5 个局域网，其连接图如图所示。LAN2 至 LAN5 上的主机数分别为：91,150,3 和 15。该自助系统分配到的 IP 地址块为 30.138.118/23。试给出每一个局域网的地址块（包括前缀）。



答案：对 LAN_3，主机数 150，$(2^7-2)<150+1<(2^8-2)$，所以主机位为 8bit，网络前缀为 24，分配地址块 30.138.118.0/24。（第 24 位为 0）

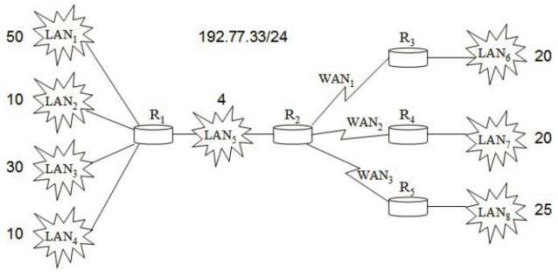
对 LAN_2，主机数 91，$(2^6-2)<91+1<(2^7-2)$，所以主机位为 7bit，网络前缀为 25，分配地址块 30.138.119.0/25。（第 24、25 位为 10）

对 LAN_5，主机数 15，$(2^4-2)<15+1<(2^5-2)$，所以主机位为 5bit，网络前缀为 27，分配地址块 30.138.119.192/27。（第 24、25、26、27 位为 1110）

对 LAN_1，主机数 3，$(2^2-2)<3+1<(2^3-2)$，所以主机位为 3bit，网络前缀为 29，分配地址块 30.138.119.232/29。（第 24、25、26、27、28、29 位为 111101）

对 LAN_4，主机数 3，$(2^2-2)<3+1<(2^3-2)$，所以主机位为 3bit，网络前缀为 29，分配地址块 30.138.119.240/29。（第 24、25、26、27、28、29 位为 111110）

5、一个大公司有一个总部和三个下属部门。公司分配到的网络前缀是 192.77.33/24.公司的网络布局如图所示。总部共有五个局域网，其中的 LAN_1~LAN_4 都连接到路由器 R_1 上，R_1 再通过 LAN_5 与路由器 R_2 相连。R2 和远地的三个部门的局域网 LAN_6~LAN_8 通过广域网相连。每一个局域网旁边表明的数字是局域网上主机数。试给每一个局域网分配一个合适的网络前缀。



答案：分配网络前缀时应先分配地址数较多的前缀，本题的答案很多种，下面是其中的一种答案.

LAN1：192.77.33.0/26

LAN3：192.77.33.64/27；

LAN6：192.77.33.192/27；

LAN7：192.77.33.160/27；

LAN8；192.77.33.128/27

LAN2：192.77.33.96/28；

LAN4：192.77.33.11228

LAN5：192.77.33.224/27（考虑到以太网可能还要连接及个主机，故留有余地）WAN1:192.77.33.232/30；WAN2：192.77.33.236/30；192.77.33.240/30

第五章 数据链路层

1、链路层服务和概述

结点：主机和路由器等设备

链路：沿着通信路径的连接相邻结点的通信信道，有有线链路、无线链路、局域网

帧：数据链路层的分组

数据链路层提供经一条链路从一个结点传输数据到相邻结点的功能

1）功能

网络层：

将运输层报文段从源主机传送到目的主机

能够在各段链路层提供异构服务的情况下，完成主机到主机的工作

链路层：

将网络层数据报从一个结点传送到下一个结点

不同的的链路采用不同的链路层协议，提供的服务不同

2）数据链路层提供的服务

成帧：

根据链路层协议把网络层数据报封装成链路层帧，不同的链路层协议，帧格式可能不同。

差错检测和纠错：

差错检测用来检测是否存在一个或多个比特差错。纠错则不仅能检测差错，还能纠正。

发送节点：在帧中设置差错检测比特；

接收节点：对收到的帧进行差错检测或纠正。

通过硬件实现。

媒介访问控制（MAC 协议）：

点对点链路：一个发送方和一个接收方，MAC 协议比较简单(或不存在)，即任何时候只要链路空闲，发送方都能够发送帧。

广播链路：多个结点共享一个链路（多路访问），使用 MAC 协议协调多个结点的帧传输。

可靠交付：

保证网络层的数据报无差错地通过链路层。与运输层的可靠传输类似，通过确认和重传实现，用于高差错率链路，例如无线链路，在比特差错低的链路不提供可靠交付服务(光纤，双绞线)。

流量控制：

链路结点的帧缓存容量有限。防止发送结点的发送速率过高，避免接收结点来不及处理。

3、多路访问协议

1）数据链路层使用的信道有点对点信道和广播信道

点对点信道：

链路两端各一个结点，一个发送和一个接受。这种信道使用一对一的点对点通信方式。例如点对点协议 PPP。

广播信道：

多个结点连接到一个共享的广播信道。常用于局域网 LAN 中，如以太网和无线局域网。

广播：任何一个结点传输一帧时，信号在信道上广播，其他结点都可以收到一个拷贝。

2）目的

协调多个结点在共享广播信道上的传输。避免多个结点同时使用信道，发生冲突（碰撞），产生互相干扰。

冲突：两个以上的结点同时传输帧，是接收方收不到正确的帧（所有冲突的帧都受损丢失）。造成广播信道带宽的浪费。多路访问协议可用于 许多不同的网络环境，如有线和无线局域网等。

3）载波侦听多路访问 CSMA

①载波侦听 CS：某个节点在发送之前，先监听信道。

信道忙：侦听到有其他结点正在使用信道，则该结点不发送帧，而等待一段时间再发送。

信道空：该结点开始传输帧

冲突检测 CD：边发送边接听，即结点在传输的同时帧听信道。

如果检测到有其他结点正在传输帧，发生冲突，立即停止传输，并用某种方法来决定何时再重新传输。

②相应的协议

载波侦听多路访问 CSMA

带冲突检测的载波侦听多路访问 CSMA/CD

带冲突避免载波侦听多路访问 CSMA/CA

③基本原理

传送前侦听，只增加“载波侦听”规则。也叫“先听后讲”LBT

信道闲，传送整个帧。信道忙，延迟传送。

④特点

发前监听，可减少冲突。由于传播时延的存在，仍有可能出现冲突，并造成信道浪费。

⑤CSMA/CD

基本原理：

传送前侦听，增加“载波侦听”和“冲突检测”两个规则。“边说边听”LWT。

信道忙，延迟传送。信道闲，传送整个帧。

发送同时进行冲突检测。一旦检测到冲突就立即停止传输，发送强化干扰信号，随机等待一段时间重发。

目的：

缩短无效传送时间，提高信道的利用率。

4、局域网 LAN

LAN 是一个地理范围较小的计算机网络。

特点：地理范围小，IEEE 定义了采用 1-坚持是 CSMA/CD 的 802.3 局域网标准，数据传输速率 R 一般为 10Mb/s、100Mb/s、1Gb/s、10Gb/s

1）硬件地址

广播信道 LAN 中，一个结点发送的帧，在信道上广播传输，其他结点都能收到该帧。一般情况下，一个结点只向某个特定的结点发送，由“网卡”负责 MAC 地址的封装和识别。

适配器从网络上每收到一个 MAC 帧就首先用硬件检查 MAC 帧中的 MAC 地址。如果是发往本站的帧则收下，进行下一步处理。否则就将此帧丢弃，不再进行其他的处理。

“发往本站的帧”包括以下三种帧：单播帧、广播帧、多播帧。所有适配器都至少能够识别单播地址和广播地址。有的适配器可用编程方法识别多播地址。

IEEE 规定地址字段的第一字节的最低位为 I/G 位。I/G 表示 Individual / Group。当 I/G 位=0 时，表示一个单播地址。当 I/G 位=1 时，表示组地址，用来进行多播。此时，IEEE 只分配地址字段前三个字节中的 23 位。

广播地址：

所有 48 位全为 1，即：FF-FF-FF-FF-FF-FF。

只能作为目的地址使用。

2）以太网

以太网是指符合 DIX Ethernet V2 或 IEEE 802.3 标准的局域网。DIX Ethernet V2 标准与 IEEE 的 802.3 标准只有很小的差别。严格来说，符合 DIX Ethernet V2 标准的局域网才是以太网。以太网采用 CSMA/CD 多路访问控制

①服务

以太网提供的是无连接的不可靠的交付服务，即尽最大努力的交付。以太网对发送的数据帧不进行编号，也不要求对方发回确认。当目的站收到有差错的数据帧时就丢弃此帧，其他什么也不做。差错的纠正由高层来决定。如果高层发现了数据丢失而进行重传，但以太网并不知道这是一个重传的帧，而是当作一个新的数据帧来发送。

②以太网 MAC 帧结构

常用的以太网 MAC 帧格式有两种标准：DIX Ethernet V2 标准和 IEEE 的 802.3 标准，最常用的 MAC 帧是以太网 V2 的格式。

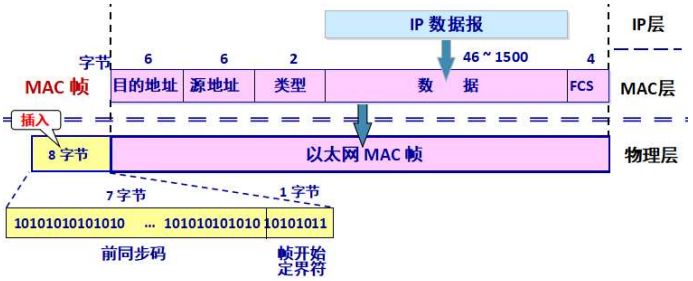
目的地址：6 字节，目的 MAC 地址。

源地址：6 字节，源 MAC 地址。

类型：2 字节，标志上一层使用的协议。

数据：46-1500 字节，IP 数据报。不足 46 字节的则加入整数字节的填充字段补足。

FCS：4 字节，CRC 校验字段。



物理层在帧的前面插入（硬件生成的）8 字节中，第一个字段共 7 个字节，是前同步码，用来迅速实现 MAC 帧的比特同步。第二个字段 1 个字节是帧开始定界符，表示后面开始的信息就是 MACC 帧。

无效的 MAC 帧：数据字段的长度与长度字段的值不一致；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；数据字段的长度不在 46 ~ 1500 字节之间。有效的 MAC 帧长度不为 64 ~ 1518 字节之间。

802.3 与以太网 V2 MAC 帧格式相似，区别在于：IEEE 802.3 规定的 MAC 帧的第三个字段是“长度/类型”。当这个字段值大于 0x0600 时（相当于十进制的 1536），表示“类型”，这时的帧和以太网 V2 MAC 帧完全一样。当这个字段值小于 0x0600 时才表示“长度”。现在市场上流行的都是以太网 V2 的 MAC 帧，但通常也称为 IEEE 802.3 标准的 MAC 帧。

帧最小间隔为 9.6μs，相当于 96bit 的发送时间。一个站在检测到总线开始空闲后，还要等待 9.6μs 才能再次发送数据。这样做是为了使刚刚收到数据帧的站的接收缓存来得及清理，做好接收下一帧的准备。

3）扩展以太网

扩展以太网更常用的方法是在数据链路层进行。早期使用网桥，现在使用以太网交换机。

①网桥

网桥工作在数据链路层。它根据 MAC 帧的目的 MAC 地址对收到的帧进行转发和过滤。当网桥收到一个帧时，并不是向所有的接口转发此帧，而是先检查此帧的目的 MAC 地址，然后再确定该帧转发到对应的端口，或把它丢弃。

网桥通过查询站表转发帧：

目的 MAC 地址对应的端口与入端口不同，则转发帧；目的 MAC 地址对应的端口与入端口相同，则丢弃帧；目的 MAC 地址对应的端口未知，则洪泛转发。

网桥的缺陷：

存储转发会增加时延。桥接不同 MAC 子层的网段时时延更大。MAC 子层不具备流量控制功能。适用于用户数不多和流量不大的局域网，否则可能会出现网络拥塞，例如由于广播数据造成广播风暴。

②交换机

交换式集线器可明显地提高以太网的性能。交换式集线器常称为以太网交换机或第二层交换机。

以太网交换机的交换方式：

存储转发方式：把整个数据帧接受缓存后再进行处理。

直通方式：不需要接受完整个数据帧，边接收的同时就立即按数据帧的目的 MAC 地址转发该帧，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。

以太网交换机的自学习：

以太网交换机运行自学习算法自动维护交换表。以太网交换机启动时，其交换表是空的。采用洪泛的方法转发帧。

③交换机自学习和转发帧的步骤

自学习：

交换机收到一帧后先查找交换表中与收到帧的源地址有无相匹配的表项。如没有，就在交换表中增加一个表项 <MAC 地址 接口 有效时间>。如有，则对原有的表项进行更新。

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，则向入接口除外的所有其他接口转发。如有，则向交换表中的对应接口转发。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。

④网桥与集线器比较

转发：

集线器：转发帧时，只是广播发送比特到链路上，并不侦听该链路是否忙；

网桥：将帧转发到共享链路上时（半双工），运行 CSMA/CD。如果侦听到要转发的 LAN 网段上忙，停止传输；如果出现冲突，采用指数后退算法。

互联：

网桥：可以互联不同技术的以太网段、无地理范围限制。

集线器：不具备该特性。

4）虚拟局域网 VLAN

虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。这些网段具有某些共同的需求。每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN。虚拟局域网限制广播域的大小。虚拟局域网只是局域网给用户提供的一种服务，而并不是一种新型局域网。 以太网交换机可以很方便地实现虚拟局域网。

①标准定义

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议(802.1Q)，它在以太网帧的基础上增加了 VLAN 头，允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域(或称 VLAN)。

②划分方法

基于端口划分的 VLAN：是根据交换机端口来划分。

基于 MAC 地址划分 VLAN：是根据每个主机的 MAC 地址来划分。

基于网络层划分 VLAN：根据每个主机的网络层地址(IP 地址)或协议类型(如果支持多协议)划分。

根据 IP 组播划分 VLAN：这种划分认为一个组播组就是一个 VLAN ，该方法将 VLAN 扩大到了广域网。

5、循环冗余检测 CRC

显示的通信链路都不会是理想的。这就是说，比特在传输过程中可能会产生差错：1 可能会变成 0，而 0 也可能变成 1，这就叫做比特差错。

在一段时间内，传输错误的比特站所传输比特总数的比率称为误码率 BER。

目前在数据链路层广泛使用了循环冗余检测 CRC 的检错技术。

举例说明（这是旧课本的 新课本见 P295）：

在发送端，先把数据划分为组，假定每组 k 个比特。现假定待传送的数据 M=101001（k=6）。CRC 运算就是在数据 M 的后面添加供差错监测用的 n 位冗余码，然后构成一个帧发送出去，一共发送（k+n）位。

这 n 位冗余码可用以下方法得出：

用二进制的模 2 运算进行 2^n 乘 M 的运算，相当于在 M 后面添加 n 个 0。得到的（k+n）位的数除以收发双方事先商定的长度为（n+1）位的除数 P，得出商是 Q 而余数是 R（n 位，比 P 少一位）。在下面的例子中，假定 P=1101（设 n=3）。经模 2 除运算后的结果是：商 Q=110101（这个商并没有什么用处），而余数 R=001.这个余数 R 就作为冗余码拼接在数据 M 的后面发送出去。这种为了进行检错而添加的冗余码常称为帧检测序列 FCS。因此加上 FCS 后发送的帧是 101001001。

```
                    1 1 0 1 0 1 ←Q（商）
P（除数）→    1 1 0 1 ┌ 1 0 1 0 0 1 0 0 0 ←2ⁿM（被除数）
                  1 1 0 1
                  ─────────
                    1 1 1 0
                    1 1 0 1
                    ─────────
                      0 1 1 1
                      0 0 0 0
                      ─────────
                        1 1 1 0
                        1 1 0 1
                        ─────────
                          0 1 1 0
                          0 0 0 0
                          ─────────
                            1 1 0 0
                            1 1 0 1
                            ─────────
                              0 0 1 ←R（余数），作为 FCS
```

在接收端把接受到的数据以帧为单位进行 CRC 检验：把收到的每一个帧都除以同样的除数 P（模 2 运算），然后检查得到的余数 R。如果在传输过程中无差错，那么经过 CRC 检验后得出的余数 R 肯定是 0。

循环冗余检验过程也可以用多项式表示，例如该例中的 P 可表示为 $P(X) = x^3+x^2+1$

6、PPP 协议

①PPP 协议由三个组成部分。一个将 IP 数据报封装到串行链路的方法，链路控制协议 ICP，网络控制协议 NCP。

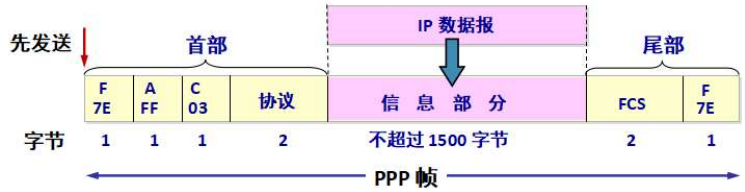
②PPP 协议的帧格式

PPP 帧的首部和尾部分别为 4 个字段和 2 个字段。

标志字段 F = 0x7E（符号“0x”表示后面的字符是用十六进制表示）。

地址字段 A 只置为 0xFF。地址字段实际上并不起作用。

控制字段 C 通常置为 0x03。



③透明传输

当 PPP 用在异步传输时，就使用一种特殊的字符填充法。

当 PPP 用在同步传输链路时，协议规定采用硬件来完成比特填充。

第五章课后题

1、数据链路层中的链路控制包括那些功能？试讨论数据链路层做成可靠的链路层有哪些优点和缺点。

答： 数据链路层中的链路控制包括以下功能：链路管理；帧同步；流量控制；差错控制；将数据和控制信息分开；透明传输；寻址。

数据链路层做成可靠的链路层的优点和缺点：所谓“可靠传输”就是：数据链路层的发送端发送什么，在接收端就收到什么。这就是收到的帧并没有出现比特差错，但却出现了帧丢失、帧重复或帧失序。以上三种情况都属于“出现传输差错”，但都不是这些帧里有“比特差错”。“无比特差错”

与“无传输差错”并不是同样的概念。在数据链路层使用 CRC 检验，能够实现无比特差错的传输，但这不是可靠的传输。

2、一个 PPP 帧的数据部分（用十六进制写出）是 7D 5E FE 27 7D 5D 7D 5D 65 7D 5E。试问真正的数据是什么（用十六进制写出）？

答：7E FE 27 7D 7D 65 7E。

3、假定站点 A 和 B 在同一个 10Mb/s 以太网网段上。这两个站点之间的传播时延为 225 比特时间。现假定 A 开始发送一帧，并且在 A 发送结束之前 B 也发送一帧。如果 A 发送的是以太网所容许的最短的帧，那么 A 在检测到和 B 发生碰撞之前能否把自己的数据发送完毕？换言之，如果 A 在发送完毕之前并没有检测到碰撞，那么能否肯定 A 所发送的帧不会和 B 发送的帧发生碰撞？（提示：在计算时应当考虑到每一个以太网帧在发送到信道上时，在 MAC 帧前面还要增加若干字节的前同步码和帧定界符）

答：设在 t=0 时 A 开始发送。在 t=576 比特时间，A 应当发送完毕。

t=225 比特时间，B 就检测出 A 的信号。只要 B 在 t=224 比特时间之前发送数据，A 在发送完毕之前就一定检测到碰撞。就能够肯定以后也不会再发送碰撞了。

如果 A 在发送完毕之前并没有检测到碰撞，那么就能够肯定 A 所发送到帧不会和 B 发送的帧发生碰撞（当然也不会和其他的站点发送碰撞）。

4、在上题中的站点 A 和 B 在 t=0 时同时发送了数据帧。当 t=225 比特时间，A 和 B 同时检测到发生了碰撞，并且在 t=225+48+273 比特时间完成了干扰信号的传输，A 和 B 在 CSMA/CD 算法中选择不同的 r 值退避。假定 A 和 B 选择的随机数分别是 rA=0 和 rB=1.试问 A 和 B 各在什么时间开始重传其数据帧？A 重传的数据帧在什么时间到达 B？A 重传的数据会不会和 B 重传的数据再次发送碰撞？B 会不会在预定的重传时间停止发送数据？

答：t=0 时，A 和 B 开始发送数据。

t=255 比特时间，A 和 B 都检测到碰撞。

t=273 比特时间，A 和 B 结束干扰信号的传输。

t=594 比特时间，A 开始发送

t=785 比特时间，B 再次检测信道。如空闲，则 B 在 881 比特时间发送数据。否则再退避。

A 重传的数据在 819 比特时间到达 B, B 先检测到信道忙，因此 B 在预定的 881 比特时间停止发送数据。