

# 哈工大2023秋计网开箱手册

---

## 哈工大2023秋计网开箱手册

### 课程学习思路

1. 知识点学习
2. 平时上课
3. 实验
4. 考试

### 附：计网复习笔记

1. 计算机网络概述
  - 1.1 计算机网络相关概念
  - 1.2 计算机网络结构
  - 1.3 数据交换技术
    - 1.3.1 电路交换技术
    - 1.3.2 报文交换技术
    - 1.3.3 分组交换技术
  - 1.4 多路复用技术
  - 1.5 计算机网络性能
  - 1.6 计算机网络体系结构
2. 应用层
  - 2.1 网络应用体系结构
  - 2.2 HTTP协议
  - 2.2 FTP协议
  - 2.3 电子邮件
  - 2.4 DNS协议
3. 传输层
  - 3.1 传输层服务概述
  - 3.2 UDP协议
  - 3.3 可靠数据传输原理
  - 3.4 TCP协议
4. 网络层
  - 4.1 网络层概述
  - 4.2 IP协议
    - 4.2.1 IPV4分组的格式
    - 4.2.2 IP地址与子网划分
  - 4.3 DHCP协议与NAT
  - 4.4 ICMP协议
  - 4.5 路由协议
  - 4.6 IPv6简介
  - 4.7 移动IP
5. 数据链路层
  - 5.1 数据链路层服务
  - 5.2 差错检测
  - 5.3 多路访问控制（MAC）协议
  - 5.4 随机访问MAC协议
  - 5.5 ARP协议
  - 5.6 以太网
  - 5.7 交换机
  - 5.8 VLAN
  - 5.9 PPP协议
6. 物理层
  - 6.1 基本概念
  - 6.2 信道容量
  - 6.3 编码与调制

# 课程学习思路

哈工大的计网课程属实一言难尽（懂的都懂），同学们一定要提前做好心理准备。手册后会附上计网课程复习笔记，希望对大家能够有所帮助。下面将从知识点学习、平时上课、实验、考试四个方面谈一谈个人经验：

## 1. 知识点学习

整体来讲，**计网知识点十分繁杂，细节很多而且全都要记住**，还要在此基础上融会贯通（迫于逆天考题），个人认为记忆量是计组的两倍。刚开始学的时候可能会有一种与初学计组计统类似的感觉，表现为不知道他在说什么，说到哪了，各种东西为什么这么设计之类的感受。这种感觉应该会随着课程学习的逐渐深入而渐渐淡化，学完整个课程可能会有一种豁然开朗的感觉。另外，如果觉得从顶向下学起来有些吃力，可以尝试反过来从物理层开始向上学（不过这么学会导致平时上课很难受）。

知识点学习策略：多背，多练，多思考，注意细节。计网知识点和细节非常多，一定要在理解的基础上进行记忆，很多设计的背后都有着客观实际的考量和原因。从实际问题出发，去思考这些协议是如何进行工作的，以及为什么要这样设计，对知识点的记忆会有很大的帮助。此外，也推荐大家做一些思维导图，构建宏观的知识体系，这对于学习计网这类偏记忆的课程会很有帮助。

在网课方面：哈工大的计网mooc讲的还是可以的，如果觉得听不下去，这里推荐两个公认的神级网课：一是**中科大郑烱老师的计网**，二是**湖科大教书匠的计网**，二者都可以在b站搜到。

在教材方面：虽然基本上所讲述的内容都可以在计网大黑书中找到，但个人认为计网大黑书可看可不看，考试会以**ppt上的内容为准进行出题**，大黑书中有些内容考试不会涉及。因此如果嫌麻烦的话可以直接把ppt下载下来当教材用。其实如果不看大黑书，只跟着ppt走，学到最后再回来翻大黑书，也会发现大黑书的大部分内容基本都很熟悉了。

## 2. 平时上课

平时上课基本处于**翻转课堂**的状态，同学会分成各个小组，每个小组在学期内完成一次翻转课堂，大约40分钟。之后老师会就mooc上没有的东西（但是可能大黑书有，可能其他网课中会讲到）进行一些知识拓展（比如CDN，比如移动IP），或者就一些问题展开发散性思考，或对某些协议的相关做法进行较深入的分析（比如为什么TCP必须要做成三次握手而不是两次握手）。这部分会有课堂互动，老师会在雨课堂里布置一系列的题，有的需要个人作答，有的需要整个小组作答，每道题的分数都会**作为平时成绩的一部分计入最终成绩里**（不过每道题的分数占比最后折起来其实挺少），不建议翘课。老师在讲这部分内容时，如果平时自己没有提前学到这一章，大概率会听不懂。老师讲的这部分内容**在期末题中也会考，但考的不多，也不是重点**，基本就是简单考些概念和相关原理。建议最后复习时间不充裕的同学挑这里面一些比较重要的知识点进行选择性的复习即可（如之前考了移动IP的相关概念）。

## 3. 实验

3学分的计网**共4个实验**，时间紧迫，难度较高。每个实验会分必做和选做，这里**选做的意思是：可以选择不做，但是会拿不到相应的分数**（老师和助教的解释：必做分数占比大，必做不做的话这一次的实验成绩就直接没了，选做分数占比小，不做的话只是选做部分会没分）。

实验不限编程语言，但实验手册里会直接把基本的c++代码框架给出来，同学需要在这个代码框架的基础上添加新功能（基本就是选做的那一部分）。关于编程语言（这里只谈c++和python）的选择，个人认为各有各的好处，使用c++的好处在于实验指导书中给了基本的框架，坏处在于读懂代码并添加新的功能会比较费劲；使用python的好处在于有现成的很方便的库，写代码和添加新功能会很方便，代码也很容易能读懂，但坏处在于可能需要从头开始实现基本的框架。

实验验收的时候助教会让同学解释代码里是如何实现的各个功能（所以重点在于能否看懂代码）。实验所做内容基本都是考试重点考察的内容，因此如果有时间的话比较推荐自己认真做一做，收获还是不小的。如果实在没时间，可以参考github和csdn上一些现成的火炬。

## 4. 考试

考试**难度大（比考研题难）**，**时间紧，可能会翻车**，建议大家提前做好心理准备，**提前准备复习，速成很容易寄掉**。考试会有选择题，填空题，判断题，简答题。小题大多不会出的很难，主要考察一些细节，涉及的知识点也较广，出题组为了压高分，会专门出几道很偏的题。大题会逐渐上难度，最后一道题更是会综合应用层，传输层，网络层，数据链路层四层的知识进行综合考察（王道中没有那么难的题），且题目中的细节很多，很容易出错。MOOC上的测验题在难度上与考试题相仿（或比考试题稍简单些），值得大家认真推敲。在历年考题的获取上，出题组为了进一步压高分，他们规定历年考题均属于保密范畴，禁止外传（跟计统真是两个极端），在网上只能找到一两年的计网题。如果同学拿着以前考试考过的题问老师，老师只会简单说说思路，不会说具体的答案。

计算机网络毕竟是计算机专业非常重要的一门核心课程，通过本课程的锤炼后，同学们会获得扎实的计网基础知识功底，并能够轻松拿捏考研408计网题。希望同学们重视起来，认真对待这门课程。

哈工大计算学部金牌讲师团 周宇航

2023年8月

## 附：计网复习笔记

### 1. 计算机网络概述

本章不是课程核心，但考试可能会考一些细节性的问题。各种数据交换技术的优缺点、计算机网络各层次的功能等内容需要着重掌握，计算题可能会考分组交换时间的计算，以及码分多路复用的编码和解码。

#### 1.1 计算机网络相关概念

- 计算机网络的定义：互连的、自治的计算机集合。连接到计算机网络的设备称为**主机（端系统）**，端系统分为客户端与服务器。端系统通过由通信链路以及分组交换机构成的网络核心相连接，通过接入ISP连接到Internet。
- 网络协议：为进行网络中的数据交换而建立的规则、标准或约定（比如两个外国人来到中国留学，他们约定使用中文交流，这样双方都能够听得懂）
- 协议三要素：**语法**（定义传输格式）、**语义**（定义所要完成的动作、信息的含义等）、**时序**（定义各种操作的顺序）。
- 计算机网络的拓扑结构：**总线形、星形、环形、网状网络**等。（以太网的逻辑拓扑是总线形结构，物理拓扑是星形或拓展星形结构）

#### 1.2 计算机网络结构

- 网络边缘：主机（端系统）。
- 接入网络概念：将网络边缘（即各个主机）接入核心网（边缘路由器），例如住宅（家庭）接入网络、机构接入网络（学校、企业等），移动接入网络。
- 接入网络举例：
  - 数字用户线路网络DSL（利用已有的电话线连接中心局的DSLAM，每个用户**直接连接到中心局**）
  - 电缆网络（多个用户**共享**一根电缆，例如混合光纤同轴电缆）
  - **以太网（占统治地位的有线局域网，802.3标准）**
  - **WLAN（无线局域网，802.11标准）**。

- 网络核心：互连的路由器网络，关键功能是**路由和转发**。

## 1.3 数据交换技术

### 1.3.1 电路交换技术

- 最典型的电路交换网络：**电话网络**
- 电路交换的三个阶段：**建立连接，通信，释放连接**。
- 特点：是真正的物理线路交换，**预先建立电路连接，独占资源，在通信结束后才会释放资源**（由于需要共享中继线，所以需要使用信道的多路复用技术），效率较低，**不适合突发数据传输，但适合强实时性应用，传输时延小**。

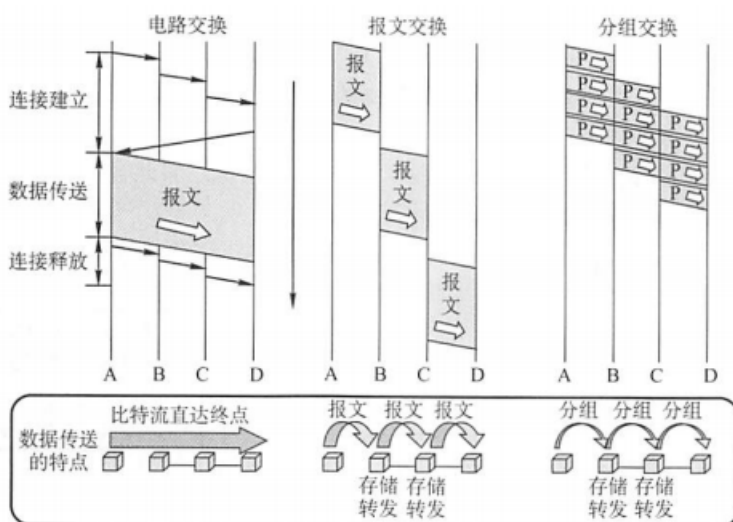
### 1.3.2 报文交换技术

报文交换技术相比于电路交换技术：采用了**存储转发**的传输方式，无须建立连接，动态分配链路，提高了线路的利用率。但由于数据进入交换结点后要经历存储-转发过程，因此会引起**转发时延**。

报文交换技术主要是用于早期的电报通信网络中，现在**多被较先进的分组交换技术方式所取代**。

### 1.3.3 分组交换技术

分组交换技术可看成是报文交换技术的改进，将大的数据块划分为许多的小的数据块，加上一些必要的信息之后构成分组，在网络中进行传输。相比于报文交换，它的线路利用率更高，加速了数据的传输，但同时需要传输额外的信息量（即每个划分的数据块都需要加上一些必要的控制信息才能够传输，否则会出现很多问题）



分组交换技术可分为**面向连接的虚电路方式**和**无连接的数据报方式**。二者的比较如下表所示：

表 2.1 数据报服务和虚电路服务的比较

	数据报服务	虚电路服务
连接的建立	不需要	必须有
目的地址	每个分组都有完整的目的地址	仅在建立连接阶段使用,之后每个分组使用长度较短的虚电路号
路由选择	每个分组独立地进行路由选择和转发	属于同一条虚电路的分组按照同一路由转发
分组顺序	不保证分组的有序到达	保证分组的有序到达
可靠性	不保证可靠通信,可靠性由用户主机来保证	可靠性由网络保证
对网络故障的适应性	出故障的结点丢失分组,其他分组路径选择发生变化时可以正常传输	所有经过故障结点的虚电路均不能正常工作
差错处理和流量控制	由用户主机进行流量控制,不保证数据报的可靠性	可由分组交换网负责,也可由用户主机负责

分组交换的报文交付时间的计算：

设报文为  $M \text{ bit}$ ，链路带宽（数据传输速率）为  $R \text{ bps}$ ，每个分组的长度为  $L \text{ bit}$ ，跳步数为  $h$ ，不考虑其他时延，则总的传输时间  $T$  为：

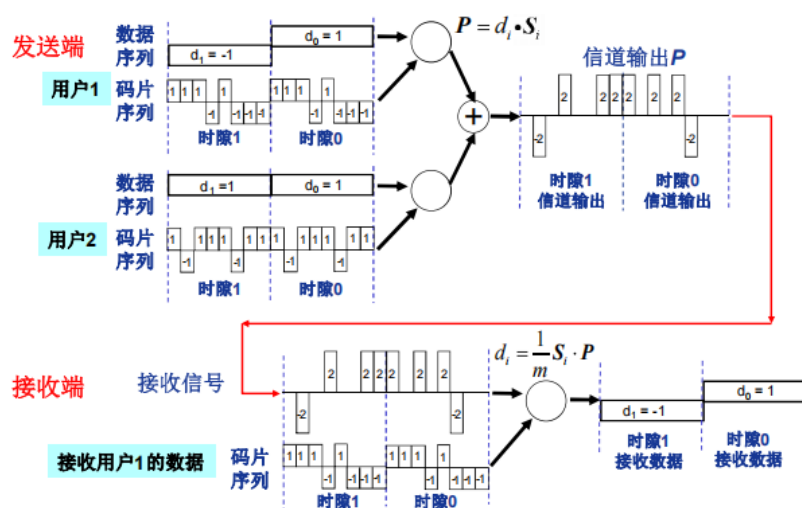
$$T = \frac{M - L}{R} + h \times \frac{L}{R} = \frac{M + (h - 1)L}{R}$$

（对于该式子，可以这么理解：第一个式子为除最后一个分组外，其余分组在源主机上传输需要的时间，第二个式子为最后一个分组在网络中传输需要的时间）

## 1.4 多路复用技术

典型的多路复用方法：

- 频分多路复用：各用户占用不同的频率带宽
- 时分多路复用：将时间分为一段段等长的时分复用帧（TDM），各用户占用一个时分复用帧的不同时隙。各用户占用相同的频带宽度
- 波分多路复用：即光的频分复用
- 码分多路复用：每个用户分配一个唯一的码片序列，依据线性代数中的相关原理来进行编码和解码。



## 1.5 计算机网络性能

一些可以反映计算机网络性能的量：速率、带宽、延迟/时延（分为结点处理延迟、排队延迟、传输延迟、传播延迟）、丢包率、时延带宽积、吞吐量/率等

传输延迟与传播延迟的区分：类比车队，车队通过收费站的时间为传输延迟，每台车从第一个收费站到第二个收费站的用时为传播延迟。

流量强度：设链路带宽为  $R$ ，分组长度为  $S$ ，平均分组到达速率为  $a$ ，则流量强度为  $\frac{La}{R}$ 。当流量强度大于1时，平均排队延迟无限大。

## 1.6 计算机网络体系结构

计算机网络体系结构是计算机网络的各层协议的集合。

采用分层结构的好处：结构清晰，便于系统更新和维护，利于标准化。

实体：表示任何可发送或接收信息的硬件或软件进程。

OSI参考模型中的三个主要概念：服务、协议、接口。

- OSI参考模型：**应用层、表示层、会话层、传输层、网络层、数据链路层、物理层**。端到端层有应用层、表示层、会话层、传输层。
  - 应用层：运行网络应用程序，互相传输报文。
  - 表示层：进行数据表示转换、压缩/解压缩、加密/解密等。

- 会话层：建立和维护对话，在数据流中插入同步点。
- 传输层：负责端到端（进程之间）的完整报文数据的传输，传输的分组称为报文段，具有分段重组，连接控制，**流量控制**，**拥塞控制**，**差错控制**，等功能，使用**端口号**对进程进行寻址。
- 网络层：负责源主机到目标主机的分组交付，传输的分组称为数据报，具有路由和转发的功能。
- 数据链路层：在相邻结点间进行分组传输，传输的分组称为**帧**，具有流量控制、差错控制、访问接入控制的功能。
- 物理层：在相邻结点之间，通过物理介质进行比特传输。

易混淆的地方：

- **数据链路层具有流量控制的功能，但不具有拥塞控制功能。**传输层和网络层具有拥塞控制的功能。
- TCP/IP参考模型：应用层、运输层、网际层、网络接口层。

易混淆的地方：**OSI模型在网络层支持无连接和面向连接的通信，但在传输层仅有面向连接的通信。而TCP/IP模型中的网际层仅有一种无连接的通信模式，但在传输层支持无连接和面向连接两种模式。**

- 5层参考模型：应用层、传输层、网络层、数据链路层、物理层。（会话层和表示层的功能直接由应用程序实现）

## 2. 应用层

本章的核心内容是HTTP协议，但同时也需要掌握其他应用层协议的工作原理，以及一些容易出判断题的细节内容。DNS可能会结合具体的场景进行考查。HTTP1.0/HTTP1.1的文件传输时间计算必考，且有可能结合TCP流量控制/拥塞控制机制出综合题，特征是题目中出现了“MSS”（最大报文段长度）。另外可能会考的计算题是P2P模式文件分发的时间计算。

### 2.1 网络应用体系结构

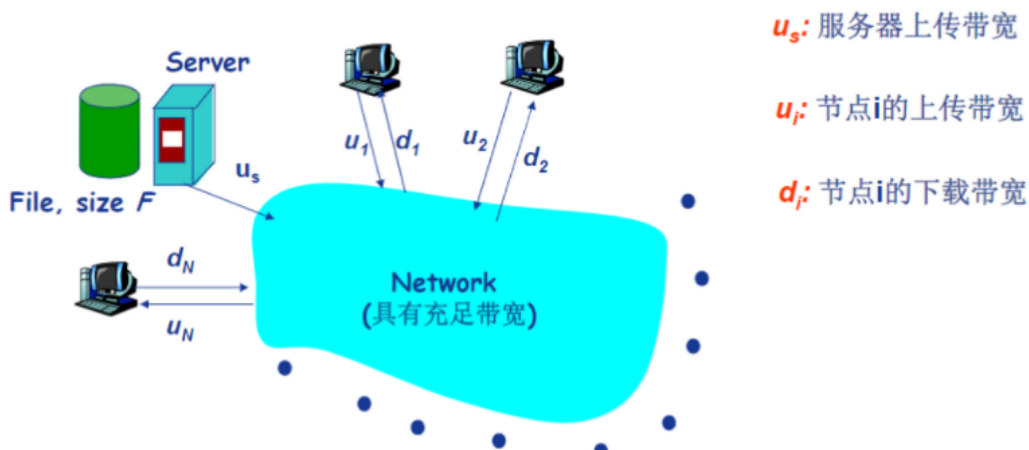
在应用层通信场景中，发起通信的进程被标识为**客户（C）**，在会话开始时等待联系的进程被标识为**服务器（S）**。

- C/S结构：客户发送请求，接收服务器响应，服务器具永久性的地址/域名，利用大量服务器来实现可扩展性。典型应用：Web、FTP应用等。
- P2P结构：通信在对等实体之间进行，结点间歇性接入网络，具有高度可伸缩性。典型应用：BT、Skype、QQ等。

应用进程使用**套接字**调用传输层协议来收发报文，一个进程的标识符为**IP地址+端口号**。

C/S结构与P2P结构文件分发的时间计算：

考虑从一个服务器向  $N$  个节点分发大小为  $F$  的文件所需的时间：



- 普通C/S模式下：

$$d_{cs} = \max\left\{\frac{NF}{u_s}, \frac{F}{\min\{d_i\}}\right\}$$

- P2P模式下：

$$d_{p2p} = \max\left\{\frac{F}{u_s}, \frac{F}{\min\{d_i\}}, \frac{NF}{u_s + \sum u_i}\right\}$$

## 2.2 HTTP协议

一个Web页面由基本的HTML文件和若干引用对象组成，HTML文件包含对其他对象引用的链接。对象通过URL来寻址，结构为服务器主机名+路径名。HTTP协议使用TCP传输服务，工作在80端口。

HTTP分为两种连接模式：**非持久性连接**，**持久性连接**。HTTP1.0版本**只能**使用非持久性连接，HTTP1.1版本默认使用持久性连接。

- 非持久性连接：每次请求/响应都单独建立一个TCP连接，响应结束之后关闭该连接。
- 持久性连接：多次的请求/响应使用最初建立的相同的TCP连接，响应完成之后不会立即关闭连接。
- 带流水线的持久性连接：连续的多个对象的请求可以逐个连续发送而不必等待回答。

建立TCP连接需要三次握手，但是第三次握手时客户端可以附带发送数据，因此建立TCP连接消耗1个RTT。严格来讲，在非持久性连接中还需要考虑关闭TCP连接时的四次挥手需要的时间，但是**我们做题时一般不考虑这部分时间**。

HTTP报文首部格式的组成：

- 请求行，包含请求方法、URL以及协议版本，请求方法包括 GET、POST、HEAD（请Server不要将所请求的对象放入响应消息中）等。
- 首部行，包含一些带有名称的字段，如 Host、Connection（表示建立的TCP连接是否可持续）等。
- 实体主体（一般用不到）。

HTTP响应消息：包含响应状态码，首部行，响应数据等。

HTTP协议本身是**无状态的**，但很多应用需要服务器掌握用户的状态，如网上购物等，实现的方法是**使用Cookie技术**。cookie保存在**客户端的主机上**，由浏览器管理。

cookie的作用：**身份认证、购物车、推荐（大数据的精准广告投放：“你可能喜欢”）、Web e-mail等**。

客户第一次请求服务器时，服务器会生成一个Cookie值，并在响应报文中以 Set-Cookie 字段告知服务器。

Web缓存/代理服务器技术（计网实验1）：

- 功能：**在不访问服务器的前提下满足客户端的HTTP请求**。
- 作用：缩短客户请求的响应时间、减少机构/组织的流量、在大范围内实现有效的内容分发。
- 特点：缓存既充当客户端，也充当服务器。

证实缓存中的对象是最新的机制：

- 代理服务器向网站主机发送HTTP请求消息，在首部添加 If-modified-since: <date> 字段，表示询问该对象从上次缓存时间以来是否被修改过。
- 网站主机收到代理服务器发送的请求消息后，根据 If-modified-since 字段进行检查：
  - 若未被修改过：发送 304 Not Modified 响应报文，响应报文中**不包含对象**。这样代理服务器可以直接使用缓存对象。
  - 若被修改过：返回新对象（即正常响应报文）



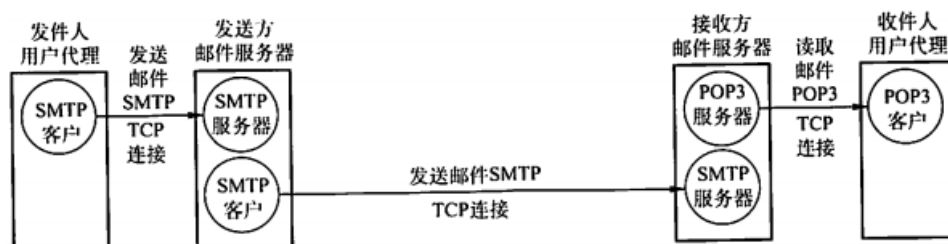
## 2.2 FTP协议

采用C/S工作方式，使用TCP传输服务。FTP维护两个并行的TCP连接：

- 控制连接：端口号为21，用来传输控制信息（如连接请求、传送请求等），控制信息均以7位ASCII格式传送。在整个会话期间一直保持打开的状态。
- 数据连接：端口号为20，用来传送文件数据，分为主动模式和被动模式，是非持续连接（每次进行文件传输都要建立新的数据连接）

## 2.3 电子邮件

电子邮件系统由三部分构成：用户代理、邮件服务器、电子邮件使用的协议。



- SMTP协议：使用TCP进行可靠数据传输，是推式协议，Email消息只能包含7位ASCII码。对于更一般的数据（如图像、其他语言的文本）可以使用MIME（多媒体邮件扩展）将数据编码为7位ASCII码来传输。
- POP3协议：是无状态的协议，是拉式协议，用于简单的邮件访问。
- IMAP协议：相比于POP3，功能更多，更复杂，所有消息统一保存在服务器中，允许用户利用文件夹组织消息，支持跨会话的用户状态。

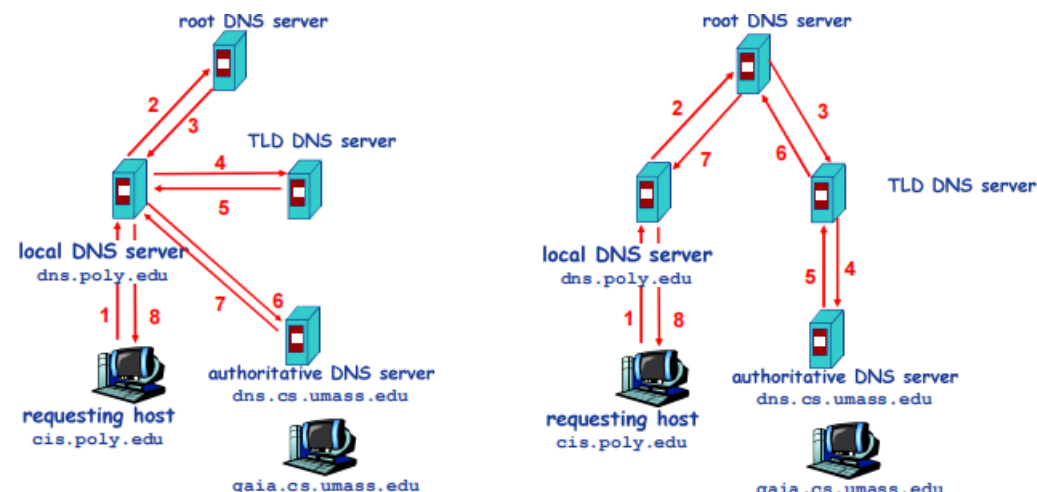
邮件访问协议：用户可以从服务器获取邮件，有POP协议、IMAP协议、HTTP协议（典型应用：163、QQ mail、Gmail）等。

一些基于万维网的电子邮件（如Hotmail、Gmail）**仅在不同邮件服务器之间传送邮件时才使用SMTP，而用户浏览器与邮件服务器之间的邮件发送或接收使用的是HTTP。**

## 2.4 DNS协议

DNS使用分布式的DNS服务器，提供**域名向IP地址的翻译、主机别名、邮件服务器别名、负载均衡**等功能，**使用UDP协议进行传输**。层次结构从上至下依次为：**根DNS服务器、顶级域DNS服务器（即.com、.net等）、权威DNS服务器（即xxx.com等）**。此外，ISP或者局域网中还可以部署**本地DNS服务器**（不严格属于层级体系），客户端的DNS查询请求会直接发给本地DNS服务器（具有缓存的作用）。

DNS查询可分为迭代查询和递归查询（本地DNS未缓存），：





DNS服务器中维护的DNS资源记录表示为四元组 (Name, Value, Type, TTL)，其中 TTL 为记录有效时间，Type 为记录类型。Type 有四种类型：

- Type=A：描述主机名与IP地址间的映射关系。
- Type=NS：描述域名与权威DNS服务器主机名之间的映射。
- Type=CNAME：表示某一真实域名的别名。
- Type=MX：描述邮件服务器与规范主机名之间的映射。

注册一个名为 networkutopia.com 的域名时：

- 向域名管理机构提供**权威域名解析服务器的名字和IP地址**
- 域名管理机构向com顶级域名解析服务器中插入两条记录 (networkutopia.com, dns1.networkutopia.com, NS)，(dns1.networkutopia.com, 212.212.212.1, A) (第一条用来记录为了解析该域名需要寻找什么名字的DNS服务器，第二条用来记录该DNS服务器的IP地址是多少，从而能够在网络中找到)

## 3. 传输层

本章重难点内容是滑动窗口协议和TCP，TCP协议的数据传输机制、建立连接的三次握手和拆除连接四次挥手的各种细节一定要记住。要重点掌握TCP的流量控制机制以及拥塞控制机制以及相关计算。

### 3.1 传输层服务概述

传输层为运行在不同主机上的**进程**提供了逻辑通信（网络层提供的是**主机**之间的逻辑通信），具有**复用**和**分用**功能（注意，网络层也具有复用和分用功能）。

传输层的多路复用/分用：

- 发送端的多路复用：传输层从不同的套接字中接收数据，为每块数据封装上头部信息，生成 Segment，交给网络层
- 接收端的多路分用：传输层依据头部信息将接收到的Segment交给正确的Socket，即不同的进程

端口号：长度为16bit，能够表示65536个不同的端口号。端口号分为两类，一类是熟知端口号，数值为0~1023，把这些端口号指派给了TCP/IP最重要的一些应用程序，另一类称为登记端口号，共没有熟知端口号的应用程序使用。

套接字：套接字 (Socket) 可以理解为一个通信端点，可以唯一地标识网络中的一台主机和其上的一个应用 (进程)。

- UDP是**无连接协议**，套接字使用二元组 (目的IP地址，目的端口号) 标识。由于无连接，接收方原本不知道源，但收到数据后可以通过报文段首部记录的源IP+源端口号。
- TCP是**面向连接的协议**，套接字使用四元组 (源IP，源端口号，目的IP，目的端口号) 标识。来自不同的源的数据只能通过各自的TCP连接被送到不同的目的套接字，但这些套接字可以使用相同的端口号 (如Web服务器并行维护多个TCP连接，端口都使用80)。

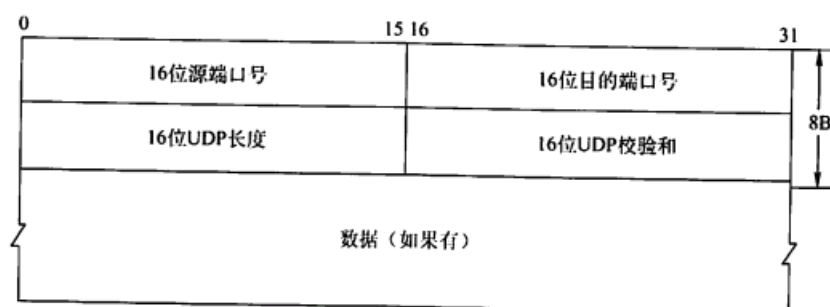
### 3.2 UDP协议

UDP协议是无连接的协议，仅在IP的数据报服务之上增加了两个最基本的服务：复用和分用以及差错检测。它具有以下特点：

- 无须建立连接，不会引入建立连接的时延。
- 实现简单，无须维护连接状态。
- 分组首部开销小，**只有8B**。
- 没有拥塞控制机制，应用可更好地控制发送时间和速率。

基于以上特点，UDP适合于一些**对实时性要求高且能够容忍少量的数据丢失**的应用（如实时视频会议、IP电话、流媒体等应用）。

UDP数据报格式：



UDP校验和的计算：**先在UDP数据报之前添加12B的仅用于计算校验和的伪首部，并把全零放入校验和字段**，之后在末尾补0使得报文长度为偶数字节，将数据报视为许多16bit（2B）的字串的拼接。之后将这些字串进行累加，进位加在和的后面，将最终的结果按位取反，即得到校验和。接收方收到UDP数据报后，加上伪首部，以同样的方式对报文段进行求和，若结果为全1，则**视为正确（但不一定真的没有差错）**，否则**将其丢弃，或交付给上层并附上错误报告，无法对其进行恢复**。

注意：**UDP的校验和检查首部和数据部分，但IP数据报的校验和只检验IP数据报的首部**。

### 3.3 可靠数据传输原理

- 停等协议（rdt3.0）：发送方每发送一帧，都要等待接收方的应答信号。之后才能发送下一帧；接收方每接收一帧，都要反馈一个应答信号，表示可接收下一帧，如果接收方不反馈应答信号，则发送方必须一直等待，每次只允许发送一帧，然后就陷入等待接收方确认信息的过程中，因而传输效率很低。
- Go-Back-N协议（GBN）：采用滑动窗口，发送方窗口大小 $>1$ ，接收方窗口大小 $=1$ 。发送方不断从上层接收分组并将其发送并缓存在窗口中，直至窗口满，窗口内缓存的内容为**已发送但未确认**的分组。发送方为最早发送的未确认分组设置**1个定时器**，若最早的未确认分组的定时器超时，则该帧被判为出错或丢失，发送方会**重传此后所有的已发送未确认的分组**。接收方由于窗口大小 $=1$ ，如果收到的分组不是期望收到的（即出现了失序或出错），则直接扔掉，并向发送方发送 **ACK=i**，其中 **i** 为上一个正确接收的编号，**具有累积确认的含义（i 及 i 之前的分组均被正确接收）**。
- Selective Repeat协议（SR）：发送方窗口大小 $>1$ ，接收方窗口大小 $>1$ 。相比于GBN协议，SR协议中接收方若收到了乱序的分组，若该分组未被缓存，则缓存下来，并发送**该分组对应序号的ACK**（没有累积确认的含义），否则只发送该分组对应序号的ACK。发送方对每一个未确认的分组都会设置一个定时器，当某个分组超时，重发该分组即可。

滑动窗口协议中发送/接收窗口大小的设置：设序号位数为  $n$ ，发送窗口大小为  $N_s$ ，接收窗口大小为  $N_r$ ，则需要满足  $N_s + N_r \leq 2^n$ 。此外，SR协议中一般  $N_s = N_r$ ，原因是发送窗口大于接收窗口会导致溢出，发送窗口小于接收窗口没有意义。

信道利用率的计算（此处只给出公式，但可以自己推出来，具体推导过程此处不详细介绍）：设发送窗口大小为  $W$ ，时延带宽积为  $BDP$ （链路带宽 $\times$ 单程传播时延），发送帧的长度为  $L_s$ ，确认帧的长度为  $L_R$ ，则：

$$\text{信道利用率} = \frac{W \times L_s}{L_s + L_R + 2 \times BDP}$$

### 3.4 TCP协议

TCP协议里遍地都是重点内容，细节很多，最好都要理解并记住。

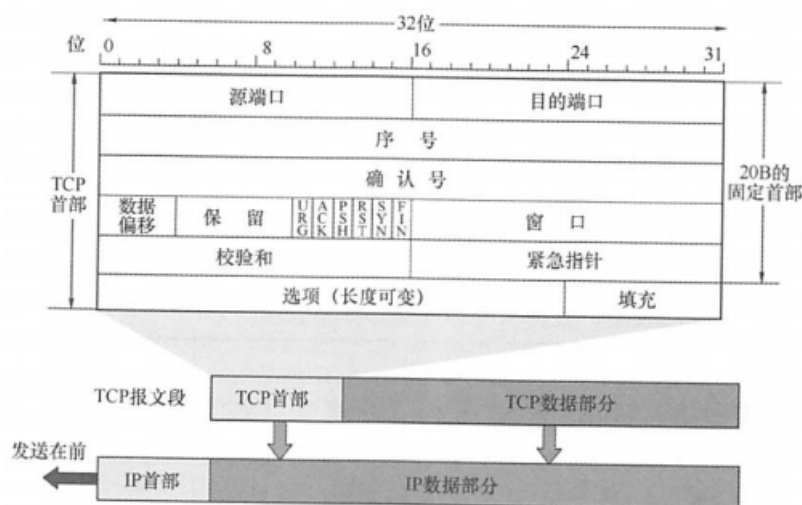
TCP是在不可靠的IP层上实现的可靠的数据传输，主要解决的是数据传输的可靠、有序、无丢失和不重复问题。相比于UDP，它的机制非常复杂。

TCP协议的主要特点如下：

- 点对点，全双工。TCP连接是一条逻辑连接，在同一连接中能够传输双向数据流。
- 提供可靠交付的服务，保证传送的数据无差错、不丢失、不重复且有序。
- 可靠数据传输原理方面类似GBN和SR的综合体，有以下特点：
  - 发送方和接收方都设有缓存，用来临时存放双向通信的数据。
  - TCP是面向字节流的，序列号 seq 指的是**报文段中第一个字节的编号，而不是报文段本身的编号**，但ACK机制本身采用的是**对报文段的确认机制**，发送的 ack 的内容代表对报文段中字节编号的确认。三次握手建立TCP连接时，发送的 seq 序列号是双方随机选择的。
  - ACK**具有累积确认的含义**，ack=k 的含义为**序号为k之前的字节均已被正确接收到，现在希望收到的下一个字节的序列号是k（序号为k的字节还没有被接收）**
  - 对于乱序到达的报文段，TCP规范中**没有规定**，由**TCP的实现者**做出决策。
  - 仅设置单一的计时器，超时后仅重传该分组。具有快速重传机制，如果连续收到**3个冗余ACK**（注意冗余的含义）后不等超时就直接重传第一个分组。
  - 超时时间 $TimeoutInterval$ 基于**指数加权移动平均算法**。根据分组的实际往返时间，对RTT进行记录采样，根据算法得出RTT的估计值  $EstimatedRTT$  以及RTT的波动程度  $DevRTT$ ，有：

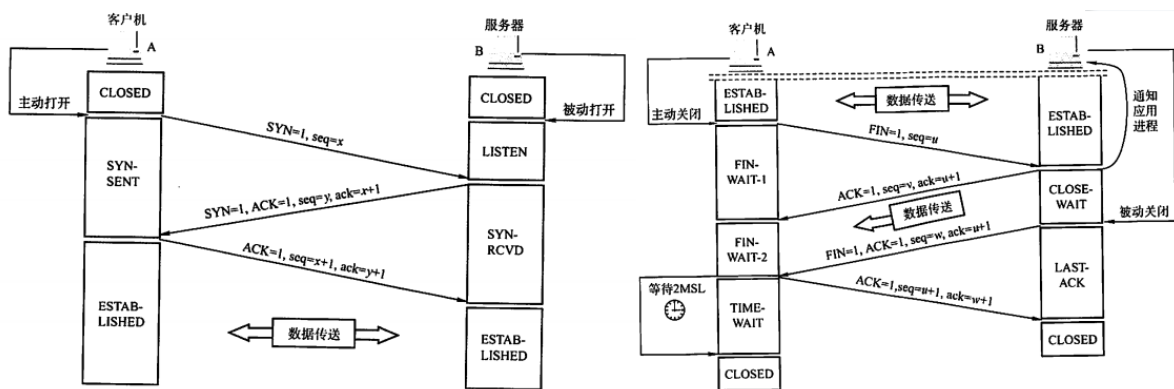
$$EstimatedRTT_{\text{新}} = (1 - \alpha) \times EstimatedRTT_{\text{旧}} + \alpha \times SampleRTT$$
$$DevRTT_{\text{新}} = (1 - \beta) \times DevRTT + \beta \times |SampleRTT - EstimatedRTT|$$
$$TimeoutInterval = EstimatedRTT + 4 \times DevRTT$$

TCP报文段格式如下：



此处需要注意，TCP首部字段最短为**20B**，最长为60B，首部字段中的“数据偏移”代表了**首部长度**，单位为4B（注意与IP数据报首部中的“数据偏移”字段进行区分）。

TCP的连接过程分为三个阶段：连接建立、数据传送和连接释放。连接建立需要三次握手，连接释放需要四次挥手。详细步骤如下（细节很多，最好全都记住）：



三次握手和四次挥手过程中一些需要注意的地方：

- $SYN=1$  代表该报文段是一个连接建立请求， $FIN=1$  代表该报文段是一个连接释放请求。 $SYN$  报文段不能携带数据，会消耗掉一个序号； $FIN$  报文段即使不携带数据也会消耗掉一个序号。
- TCP是全双工的，可以想象为有两条数据通路，一方发送  $FIN=1$  报文段只会拆除一条数据通路，另一方还可以继续发送数据。
- 客户机收到服务器发来的连接释放报文段后，TCP连接还未完全释放，必须经过2MSL（最长报文段寿命）后，客户机才会进入连接关闭的状态。

TCP发送窗口大小同时受到流量控制和拥塞控制的限制。

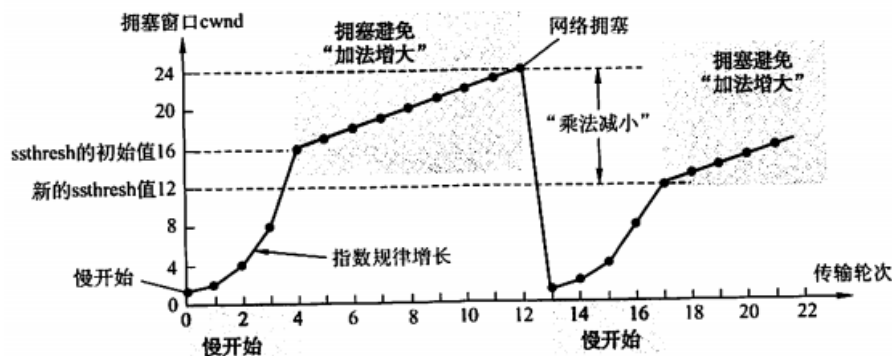
- 流量控制：

设接收方的缓存剩余空间为  $rwnd$ ， $rwnd$  会通过TCP报文段中的首部字段传递给发送方，让发送方的窗口大小（已发送未确认的字节数）不得超过  $rwnd$ ，这样发送方就不至于发送数据过快，使得接收方的缓存溢出。

- 拥塞控制：

发送方会维护一个“拥塞窗口”  $cwnd$ ，从而避免网络造成拥塞。具体的机制如下：

- “慢启动”：先令拥塞窗口  $cwnd = 1$ ，即一个最大报文段长度MSS，每收到一个对新报文段的确认后，将  $cwnd + 1$ ，即增大一个MSS。不考虑接收窗口的情况下，每经过1个RTT， $cwnd$  会呈指数型变化。“慢启动”一直把  $cwnd$  增大到一个规定的门限值  $ssthresh$ ，然后改用拥塞避免算法。
- “拥塞避免”：每经过1个RTT， $cwnd$  的值加1。此时  $cwnd$  按线性规律缓慢增长。
- 网络拥塞处理：若发生超时事件，则把  $ssthresh$  的值设为出现拥塞时的发送方的  $cwnd$  值的一半，然后把  $cwnd$  重新设置为1，执行慢启动算法。
- 快重传和快恢复：若发送方连续收到3个冗余ACK，则直接重传对方尚未收到的报文段，把  $ssthresh$  的值设为出现拥塞时的发送方的  $cwnd$  值的一半，并将  $cwnd$  的值设置为  $ssthresh$  改变后的数值，然后开始执行拥塞避免算法。



- 发送窗口的设置：

设发送窗口大小为  $swnd$ ，则发送窗口取接收窗口和拥塞窗口的较小值，即  $swnd = \min\{rwnd, cwnd\}$ 。

## 4. 网络层

本章遍地都是重点内容，内容又多又杂，必出一道综合性的大题，而且可能会结合数据链路层、传输层等的相关内容进行综合考查。希望大家认真学习这部分知识。

### 4.1 网络层概述

网络层提供主机到主机的服务，主要使用IP协议，主要任务是把网络层的协议数据单元从源端传到目的端，为分组交换网上的不同主机提供通信服务，传输单位是数据报，核心功能为**路由与转发**。网络层可分为两种服务类型：无连接服务（数据报网络，如Internet）、连接服务（虚电路网络，如ATM）。

（注意，数据报网络和虚电路网络都是分组交换网络）

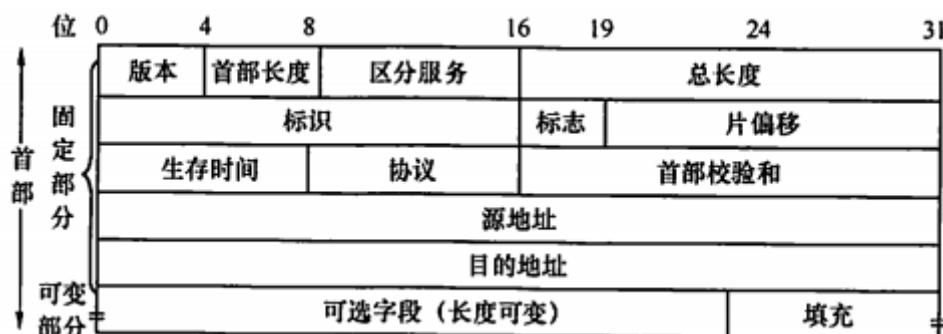
源主机向不在同一子网的目的主机发送数据的简要过程：源主机将数据报发送给默认网关（一般设为路由器在该子网内的接口地址），路由器根据路由表对该数据报进行转发，路由表在自治域内使用RIP或OSPF等协议计算得出，在域间使用BGP等协议计算得出。经历一次次转发后，数据报会被转发给目的子网下的路由器，之后由目的子网的路由器负责发送给目的主机。

近年来流行的一种创新网络架构是SDN（软件定义网络），采用**集中式的控制平面和分布式的数据平面**，路由器的工作很单纯：收到分组，查找转发表，转发分组。SDN提供的编程接口称为北向接口，SDN控制器和转发设备建立双向会话的接口称为南向接口。

### 4.2 IP协议

#### 4.2.1 IPv4分组的格式

IP数据报的格式如下：



IP首部的各个字段都很重要，都要理解其含义以及用途，有些细节需要作为“常识”来进行记忆。

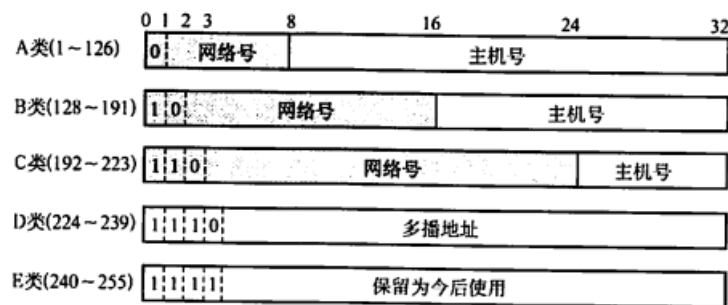
一些需要注意的地方：

- 总长度的单位为**1B**，指首部和数据之和的长度；首部长度字段的单位为**4B**。IP首部字段长度范围为**20B~60B**；片偏移的单位为**8B**，主要用于数据分片后目的主机对分组的组装（防止分片组装时乱序）。**除最后一个分片外，每个分片的长度一定是8B的整数倍**（此处小心计算题）
- 注意区分“标志”和“标识”。“标志”占3位，最低位为MF，MF=1表示后面还有分片，MF=0表示后面没有分片；中间的一位是DF，DF=0表示允许分片。标识是一个计数器，每产生一个数据报就加1，主要用于数据分片后目的主机对分组的组装（表明是同一个IP数据报的分片）。
- 首部校验和字段**只校验分组的首部，而不校验数据部分**。（注意与UDP校验和进行区分）
- 分组每经过一个路由器，必须要改变的字段有TTL、首部校验和；可能发生变化的有标志、片偏移、数据报总长度。

#### 4.2.2 IP地址与子网划分

IP地址由网络号和主机号组成，一共32位。传统IP地址分类如下：





注意有些IP地址具有特殊的用途，不用做主机的IP地址：

- 主机号全0：表示本网络本身，如 202.98.174.0。
- 主机号全1：表示**广播地址**，如 202.98.174.255。
- 形为 127.x.x.x 的地址：环回自检地址，表示主机本身，**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**。（如 127.0.0.1，代表本机）
- 32位全0，即 0.0.0.0：表示**本网络上的本主机**（DHCP协议中会用到，因为主机还没有被分配IP地址，只能使用 0.0.0.0）
- 32位全1，即 255.255.255.255：表示全网的广播地址，**但由于路由器能够隔离广播域，所以实际上等效为本网络的广播地址**。

对于一个给定的传统IP地址，考虑到实际连接的主机可能不会太多，或想要实现广播域隔离等功能，可以进行子网划分，并使用子网掩码进行标记。目前在变长子网掩码的基础上，又使用了无分类编址CIDR技术，可以实现超网构造，进行路由聚合。

- CIDR的记法为：<IP地址/网络前缀所占比特数>，如 201.2.3.64/26，含义是前26位代表网络号，后6位代表主机号，子网掩码中前26位为全1，后6位为全0，即 255.255.255.192。对于一个主机号有  $x$  位的子网，**可供分配的IP地址数为  $2^x - 2$  个**。（除了主机号全0和全1的IP地址）
- 判断两台主机是否在同一个子网的方法：计算两台主机IP地址的网络号，若二者相同则说明在同一子网。
- 路由聚合技术：可以减少路由表项，根据网络前缀，将一些具有相同网络前缀的网络聚合成一个更大的地址块，并使用一条路由表项进行代替。
- 采用CIDR编址时，如果一个分组在转发表中可以找到多个匹配的前缀，则应当选择前缀最长的一个作为匹配的前缀，称为最长前缀匹配。

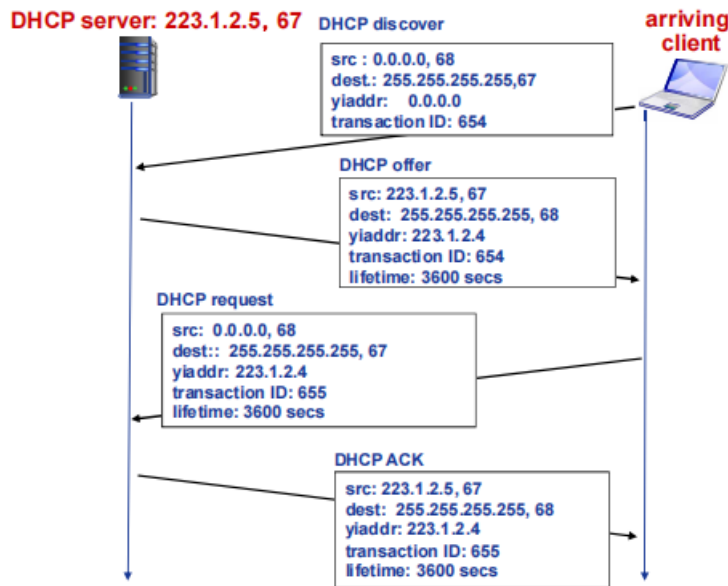
路由表中要注意两种特殊的路由：

- 主机路由：对特定主机的IP地址专门指明一个路由（如子网内配备了一个域名服务器，与路由器相连接），此处转发表中的子网掩码应为全1。
- 默认路由：使用 0.0.0.0/0 表示默认路由，只要目的网络是其他网络（不在转发表中），则一律选择默认路由。

### 4.3 DHCP协议与NAT

DHCP协议为应用层协议，是典型的C/S架构，基于UDP协议。DHCP服务器可以为子网内的主机配置动态的IP地址。工作过程分为**DHCP发现**、**DHCP提供**、**DHCP请求**、**DHCP确认**四步，具体如下所示：





注意，DHCP服务器构造的ACK报文中，包括分配给客户的IP地址、子网掩码、默认网关、DNS服务器地址。

NAT技术：网络地址转换（NAT）可以将本地专用网络地址转换为公用的IP地址，这样本地网络地址可以对外隐藏，不同本地网络内可以使用相同地址。实现过程如下：

- 替换：利用（NAT IP地址，新端口号）来替换每个外出IP数据报的（源IP地址，源端口号）。
- 记录：将每对（NAT IP地址，新端口号）与（源IP地址，源端口号）的替换信息存储到NAT转换表中。
- 替换：根据NAT转换表，利用（源IP地址，源端口号）替换每个进入内网IP数据报的（目的IP地址，目的端口号）。

一般情况下，NAT后面的主机一般只能作为客户端，难以作为服务器。该问题即NAT穿透问题。解决办法有：

- 静态配置NAT，将特定的端口的连接请求转发给服务器。
- 利用UPnP协议自动配置。
- NAT内部客户与内网外的一个中继服务器建立连接，外部客户也与中继服务器建立连接，由中继服务器负责转发内容。

## 4.4 ICMP协议

ICMP为**网络层协议**，报文内容直接作为IP数据报中的数据，具有让主机或路由器报告差错和异常情况的作用。（最常见的应用：`ping x.x.x.x`）

ICMP有两类报文：ICMP差错报告报文、ICMP询问报文。

差错报告报文可分为5种：

- 目的不可达，路由器或主机不能交付数据报。
- 源点抑制，路由器或主机由于网络拥塞而丢弃了数据报。
- 时间超过，TTL字段减为零（注意，TTL为跳数而不是以秒为单位的时间）或者目的主机在规定的时间内没有收到一个完整数据报的全部分片。（典型应用：`Traceroute`）
- 参数问题，路由器或目的主机收到的数据报的首部中有的字段写值不正确。
- 改变路由：让主机知道下次应将数据报发给另外的路由器。

不应发送ICMP差错报告报文的几种情况：ICMP差错报告报文本身、非第一个分片、具有组播地址的数据报、具有特殊地址（如 `127.0.0.0`）的数据报。

ICMP询问报文：有4种，最常用的两种为回送请求和回答报文（典型应用：`ping`）、时间戳请求和回答报文。

## 4.5 路由协议

自治系统：单一技术管理下的一组路由器，一个自治系统内的所有网络都由一个行政单位（如一家公司、一所大学等）管辖。自治系统内部的路由选择称为**域内路由选择**，常用的有**RIP协议或OSPF协议**等；自治系统之间的路由选择称为**域间路由选择**，主要使用**BGP协议**等。

两种基础算法：

- 距离向量算法：是分布式算法，基于**动态规划**的思想，每个结点维护一个到其他结点的最短距离  $D_{ij}$ ，相邻结点之间不断交换距离向量，最终达到收敛。
- 链路状态算法：每个结点都知道整个网络的结构，基于**Dijkstra算法**求出到每个结点的单源最短路径。

内部网关协议：

- RIP协议：是**应用层协议**，基于**UDP**，使用的是**距离向量算法**，通过**跳数**来寻找最佳的下一跳路由器，**距离（跳数）等于16表示网络不可达**。RIP协议只适用于**小型互联网**，每隔一段时间，**仅和相邻路由器交换信息**。最大的优点是**实现简单，开销小**，但会出现**慢收敛现象**（即"坏消息传得慢"），缓解该问题的方法是使用**水平分割、毒性逆转**等。
- OSPF协议：是**网络层协议**，内容直接封装到IP数据报中，使用的是**链路状态算法**，可灵活设置链路的权值，当链路状态发生变化时，使用**洪泛法**来向自治系统内所有路由器发送信息，可以用于**规模较大的互联网**。

外部网关协议：

- BGP协议：是**应用层协议**，基于半永久的**TCP**，使用的是**路径向量算法**，求出的是具体路径，且路径**不一定最优**。BGP的路由表包括目的网络前缀、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。根据BGP协议，可以求出到达一个子网需要经过哪些AS。

## 4.6 IPv6简介

IPv6主要解决的是IPv4地址不够用的问题。IPv6中使用了128位的地址，表示为8个16位数（16进制表示，用：连接，中间连续的多个0字段可以使用::压缩表示，但只能压缩一次）。

IPv6首部取消了校验和字段，取消了选项字段，首部长度**固定**为40字节，并**禁止在中间路由器分片**。

IPv6地址支持**单播、多播和任意播**的通信方式。

IPv4向IPv6的过渡：使用隧道技术，IPv6数据报作为IPv4数据报的载荷进行封装，穿越IPv4网络。

## 4.7 移动IP

移动网络中，移动主机可以在物理上随意地从一个网络移动到另一个网络。移动IP定义了三种功能实体：移动节点、本地代理（通常为原始连接到的网络上的路由器）和外地代理（通常为连接在被访问网络上的路由器）。

每个移动站都有一个原始地址，即永久地址（或归属地址），所在的网络为归属网络。移动主机会**被归属网络中的归属代理进行永久管理**。当移动主机移动到外地网络中时，移动站会向外地代理进行登记，外地代理会再向移动站的归属代理登记移动站的转交地址。其他外网主机通过移动主机的主IP地址向移动主机发送IP数据报时，会先被**归属代理**收到，归属代理再负责将该数据报发送给外地代理，外地代理再将该数据报发送给移动主机。

移动主机在外地网络对外发送数据报时，将仍然使用自己的永久地址作为数据报的源地址。

## 5. 数据链路层

本章重点掌握以太网、MAC协议，其中CSMA/CD是MAC协议中的重难点（日常生活中局域网无处不在，而以太网是局域网中垄断式的存在，以太网采用的就是CSMA/CD）。要理解以太网以及交换机设备的运行原理。另外，802.11无线局域网、CRC校验等小知识点也可能会出小题。

## 5.1 数据链路层服务

数据链路层功能：在物理层提供服务的基础上向网络层提供服务，主要作用是加强物理层传输原始比特流的功能，将物理层可能出错的物理连接改造为逻辑上无差错的数据链路。数据链路层负责通过一条链路从一个节点向另一个物理链路直接相连的相邻结点传送数据报。

链路层可提供**组帧、链路接入、相邻结点间的可靠交付、流量控制、差错检测与纠正**等服务。

链路层在硬件层面的网卡实现，每个网卡具有**唯一的48位MAC地址（物理地址）**，一般固定不变。广播MAC地址为全1，即 `FF-FF-FF-FF-FF-FF`。

## 5.2 差错检测

数据链路层使用差错编码，可以实现差错检测。差错编码可以分为检错码与纠错码。

- 对于检错码，设编码集的汉明距离为  $d_s$ ，想要检测  $r$  位的差错，则需要满足的关系式为：  
$$d_s \geq r + 1。$$
- 对于纠错码，设编码集的汉明距离为  $d_s$ ，想要纠正  $r$  位的差错，则需要满足的关系式为：  
$$d_s \geq 2r + 1。$$

**循环冗余校验码（CRC）：**

选取一个  $r + 1$  位的比特模式  $G$ ，对于一个  $n$  位的有效数据  $D$ ，希望在其后面添加  $r$  位的帧检验序列（FCS），使得这个  $m + r$  位的比特序列能够被预先确定的  $G$  模2整除。计算FCS的方法是，先在  $D$  后面添加  $r$  位的0，然后计算该序列被  $G$  模2除得到的余数  $R$ （这个  $R$  为  $r$  位，因为除数是  $r + 1$  位），这个  $R$  即作为FCS。例如，设  $G = 1101$ ，待传送的数据为  $M = 101001$ ，经模2除得到的余数  $R = 001$ ，则最后发送的数据为  $101001001$ 。

## 5.3 多路访问控制（MAC）协议

多路访问控制协议所要完成的任务：由于多个结点共用一条广播信道，同时发送帧会造成信号冲突，MAC协议希望为使用介质的每个结点隔离来自同一信道上其他结点所传送的信号。

常见的介质访问控制方法有：

- 信道划分MAC协议：使用多路复用共享链路，如TDMA、FDMA、WDMA、CDMA，不会引起冲突。
- 随机访问MAC协议：信道不划分，以最大速率发送帧，允许冲突，但通过采取一些措施来缓解该问题。典型的协议有ALOHA协议、CSMA协议、CSMA/CD协议、CSMA/CA协议等。
- 轮转访问MAC协议：结点轮流使用信道，设置一个主结点，轮询每个结点是否需要发送，交付链路占用权。典型的有FDDI、令牌环网等。

## 5.4 随机访问MAC协议

随机访问MAC协议不进行信道划分，但需要研究的问题是**如何检测冲突、如何在冲突中恢复**。

- 纯ALOHA协议：网络中的任何一个站点**不进行任何检测就发送数据**（想发就发，无拘无束），如果在一段时间内未收到确认，则站点认为传输过程中发生了冲突，发送站点需要**等待一段随机时间**后再发送数据。信道利用率很低，为  $\frac{1}{2e} \approx 0.184$ 。
- 时隙ALOHA协议：是ALOHA协议的改进版本，按照发送一帧的时间划分一个个等长的时隙，各结点只能在时隙开始时刻发送帧（稍微限制一下发送时刻，但还是想发就发）。若发生冲突，该该结点在下一个时隙以概率  $p$  尝试重传该帧，直至成功。信道利用率有所提高，为  $\frac{1}{e} \approx 0.37$ 。

- CSMA协议：分为1-坚持CSMA、非坚持CSMA、p-坚持CSMA。大致思路为，发送帧之前监听信道，若空闲则尝试发送帧，否则推迟发送。三种协议在信道空闲和信道忙时具体的处理方式如下：

信道状态	1-坚持	非坚持	p-坚持
空闲	立即发送数据	立即发送数据	以概率 $p$ 发送数据，以概率 $1 - p$ 推迟到下一个时隙
忙	继续坚持监听	放弃监听，等待一个随机的时间后再侦听	继续坚持监听，直至信道空闲

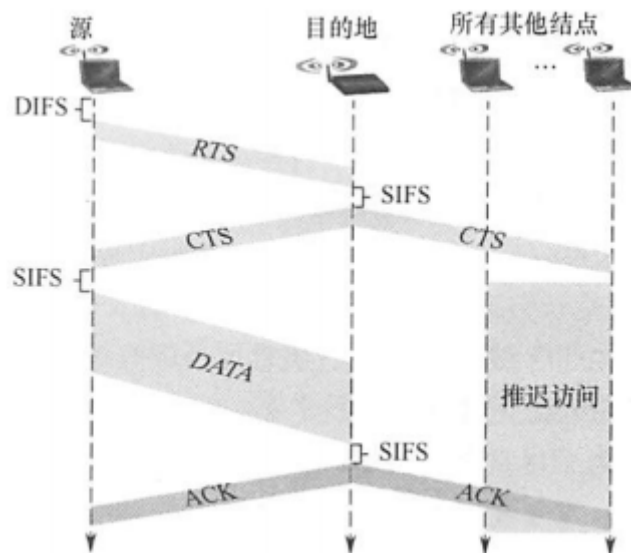
- CSMA/CD协议：是CSMA协议的改进版本，工作流程可概括为“先听后发，边听边发，冲突停发，随机重发”。采用CSMA/CD协议的以太网只能进行半双工通信。（全双工网络不会产生冲突，因此不需要该协议）
  - 冲突后等待时间的计算方法：**使用二进制指数退避算法**，取基本退避时间，一般为两倍的总线端到端传播时延（即争用期） $2\tau$ ，第  $m$  次发生冲突时，从  $0 \sim 2^{\min(m,10)} - 1$  中随机选择  $k$ ，等待的时间为  $k \times 2\tau$ 。
  - 最短帧长/最远距离的相关计算：由于必须保证在帧还没传完的情况下，也能够监听到在距离自己最远的地方发生冲突后传回来的信号，最极端的情况是**两倍的端到端信号传播时间**。这导致帧不能特别短，结点距离不能特别远。这类题目可以根据这个极端时间来列出一个方程，对方程进行求解即可。设最远距离为  $s$ ，最短帧长为  $L$ ，信号传播速率为  $v_p$ ，数据传输速率为  $v_t$ ，则方程为（不考虑其他时间，如要考虑其他时间根据该方程的原理稍作修改即可）：

$$\frac{2s}{v_p} = \frac{L}{v_t}$$

根据该方程，对于  $10Mb/s$  的以太网，规定取  $51.2\mu s$  为争用期长度，在争用期内可发送 512bit，因此**以太网的最短帧长为64B（含46B数据）**。

- CSMA/CA协议：该协议应用于802.11标准的**无线局域网**。由于无线局域网中有“隐蔽站”等问题，802.11标准将CSMA/CD协议进行了修改，把**碰撞检测改为了碰撞避免**，基本思想是在发送数据时先广播告知其他结点，让其他结点在某段时间内不要发送数据，以免出现碰撞。为了尽量避免碰撞，802.11还规定所有的站完成发送后，必须等待一段很短的时间才能发送下一帧，即帧间间隔IFS。802.11使用了下列三种IFS：
  - SIFS（短IFS）：最短的IFS，用于分隔属于一次对话的各帧，使用SIFS的帧类型有ACK帧、CTS帧、分片后的数据帧，以及所有回答AP探寻的帧等。
  - PIFS（点协调IFS）：中等长度的IFS，在PCF操作中使用。
  - DIFS（分布式协调IFS）：最长的IFS，用于异步帧竞争访问的时延。

为了处理隐蔽站问题，802.11允许发送站对信道进行预约，源站预约信道使用请求发送RTS（Request To Send）控制帧进行广播；AP通过广播允许发送CTS（Clear To Send）控制帧进行响应，表示同意信道预约请求，同时其他所有收到广播的站点会在预约期内抑制发送。下图为CSMA/CA的工作过程：



## 5.5 ARP协议

无论网络层使用什么协议，在实际网络的链路上传输数据帧时，最终必须使用硬件地址。所以需要一种方法来完成**IP地址到MAC地址的映射**，这就是ARP协议（地址解析协议）。ARP协议**工作在网络层**。工作原理如下：

主机A欲向本局域网上的某台主机B发送IP数据报时，先在其ARP高速缓存中查看有无主机B的IP地址。

- 如果有：即可查出对应的MAC地址，将其作为链路层帧的目的MAC地址并发送。
- 如果没有：在子网内**广播**ARP请求分组，广播帧的目的MAC地址为 `FF-FF-FF-FF-FF-FF`。局域网中目的主机B收到请求后，就会向主机A发送ARP响应分组（**单播发送**），分组中包含B的IP地址与MAC地址的映射关系。这样A收到后就可以更新自己的ARP表，之后按照对应的MAC地址发送帧。

不考虑NAT，一般情况下主机向远端主机通信时，数据报的源IP地址/目标IP地址不会改变，但封装的链路层帧中源MAC地址/目标MAC地址会一直改变。

## 5.6 以太网

以太网中有一些知识点应作为“常识”进行记忆，实际的题目里如果想要增加难度，可能不会给这部分数据。

以太网是应用最广泛的有线局域网。以太网有下列特点：

- 逻辑拓扑是总线形结构，物理拓扑是星形或拓展星形结构。
- 提供无连接不可靠的服务，没有握手过程，接收网卡也不向发送网卡进行确认。
- 采用的MAC协议是CSMA/CD协议。
- 以太网规定的争用期长度为  $51.2\mu s$ ，在数据传输速率为  $10Mb/s$  的以太网中，能够传输512bit数据，这也即以太网的最短帧长64B。
- 以太网帧前需要有8B的前导码，用于发送端与接收端的时钟同步。除去前导码，网络层的数据报封装成以太网帧需要附加18B的数据。以太网数据帧长度范围为64~1518B，有效数据长度为46~1500B，以太网的MTU为1500B。
- 以太网中发送的数据的编码方式使用曼彻斯特编码。

## 5.7 交换机

链路层交换机支持即插即用，对于子网中的主机和路由器都是透明的，实质上是一个多端口的网桥，能够根据MAC地址存储-转发数据帧。



交换机中存有交换表，一个表项包含了MAC地址以及连通该MAC地址的交换机端口。交换机可以通过**自主学习**来维护该交换表：当交换机从接口  $x$  收到数据帧时，会将其源MAC地址  $D$  与  $x$  更新到交换表中，生成一个表项： $\langle D, x \rangle$ ，表示通过端口  $x$  可以到达MAC地址  $D$ 。当交换机从端口  $x_0$  收到一个目的MAC地址为  $D_0$  的数据帧，且交换表中没有关于地址  $D_0$  的信息时，交换机会向除端口  $x_0$  外的所有端口**广播这个帧**。其他主机收到这个帧后会检查该帧的目的MAC地址，若不对则直接丢弃。只有目的MAC地址为  $D_0$  的主机会收下该帧。

注意，链路层交换机是第二层的设备（不考虑第三层交换机），不会涉及有关IP地址的操作，寻址都使用MAC地址。

交换机（Switch）可以隔离冲突域，但不能隔离广播域。只有网络层设备（路由器）才可以隔离广播域。而物理层设备集线器（Hub）既不能隔离冲突域，也不能隔离广播域，因为集线器仅将链路简单连接，从一个接口收到数据后会在其他所有接口进行转发。

网桥也工作在数据链路层，相当于只有两个接口的交换机，能够隔离冲突域，但不能隔离广播域。

## 5.8 VLAN

虚拟局域网（VLAN）技术支持多个局域网共享一台交换机。在交换机中可以以软件方式配置接口与VLAN的映射表，将不同的接口划分到不同的VLAN中，不同的VLAN之间不能够直接进行相互通信，这样实现了流量隔离的作用。

如果需要实现在不同的VLAN间进行信息交换，则需要路由器连接不同VLAN的端口，由路由器进行路由。

若要跨越多个交换机实现同一个VLAN，则需要使用端口类型为trunk的中继端口，该类端口可以承载不同VLAN下的数据帧。在trunk类型的端口下，为了表明传送的数据帧原属于哪一个VLAN，需要使用802.1Q协议，该协议可以为经过中继端口转发的帧增加/去除额外的首部域。

## 5.9 PPP协议

PPP协议即点对点（Point-to-Point）协议，是使用串行线路通信的面向字节的协议，仅一个发送端和一个接收端，不存在冲突，不需要复杂的介质访问控制。它具有以下特点：

- 提供差错检测但不提供纠错功能，是不可靠的传输协议，不需要流量控制，也不需要支持多点链路。
- 只支持全双工链路，两端可以运行不同的网络层协议。
- PPP帧以标志字节 01111110 表示帧的开始和帧的结束。若传输的有效数据中出现了定界符的标志模式 01111110，则在该字节前填充转义字节 01111101；若传输的有效数据中出现了转义字节的标志模式 01111101，则在该字节前再添加一个转义字节 01111101。

## 6. 物理层

相较于网络层和数据链路层，物理层不太重要，但考试也会涉及物理层的相关内容。较重点的内容为信道最大传输速率的计算、比特率/波特率的转换，以及差分曼彻斯特编码。

### 6.1 基本概念

以下为几个个人认为比较重要的概念：

- 信道：按传输信号形式的不同，可分为模拟信道和数字信道；按传输介质的不同，可分为无线信道和有线信道。信道上传送的信号可分为基带信号和宽带信号，基带传输对应的是数字信道，宽带传输对应的是模拟信道。
- 码元传输速率：又称波特率，表示单位时间内数字通信系统所传输的码元个数（也可称为脉冲个数或信号变化的次数）。若一个码元携带  $n$  比特的信息量，则  $M$  波特率的码元传输速率所对应的信息传输速率为  $Mn$  比特/秒。



- 物理介质：物理层的有线传输介质主要有双绞线、同轴电缆、光纤等；无线传输介质主要有无线电波、微波、红外线和激光等。
- 物理层的接口特性：机械特性、电气特性、功能特性、过程特性。

## 6.2 信道容量

- 理想无噪声信道下的信道容量： $C = 2W \log_2 V$ ，其中  $W$  为理想无噪声信道的带宽， $V$  为每个码元离散电平的数目（即有多少种不同的码元，如有16种不同的码元，此时1波特可以代表4比特的数据）。
- 有噪声信道下的信道容量： $C = W \log_2(1 + \frac{S}{N})$ ，其中  $W$  为信道带宽， $\frac{S}{N}$  为信噪比（题目中信噪比可能以分贝值的格式给出，单位为dB，设分贝值为  $B$ ，则由分贝值计算出  $\frac{S}{N}$  的关系式为  $B = 10 \log_{10} \frac{S}{N}$ ）。

## 6.3 编码与调制

把数据变换为数字信号的过程称为编码，把数据变换为模拟信号的过程称为调制。

编码方法有：归零编码、4B/5B编码、**曼彻斯特编码**（可以实现自同步，以太网使用该编码方式）、**差分曼彻斯特编码**（"0跳变，1保持"）等。

调制方法有：幅移键控（ASK）、频移键控（FSK）、相移键控（PSK）、差分相移键控（DPSK）、正交振幅调制（QAM，也称为幅值相位联合键控APK）。二进制下分别为2ASK、2FSK、2PSK、2DPSK。各调制方法有以下特性：

- 频带利用率：2ASK、2PSK以及2DPSK的频带利用率相同，2FSK的频带利用率最低。
- 误码率：相同信噪比下，2PSK误码率最低，2ASK的误码率最高。
- 对信道特性的敏感性：2ASK对信道特性变化比较敏感，性能最差。2FSK和2PSK对信道特性变化不敏感。
- QAM：具有频带利用率高，抗噪声能力强、调制解调系统简单等优点。