计网复习题和知识点+最终版

分析题:

1.以太网交换机进行转发决策时使用的 **PDU** 地址是 _____。 （**A** ）

A. 目的物理地址 **B.**目的 **IP** 地址 **C.**源物理地址 **D.**源 **IP** 地址

分析：以太网交换机属于数据链路的设备，用的是MAC地址/物理地址/硬件地址。交换机实质上是一个多端口网桥，工作在数据链路层，数据链路层使用物理地址进行转发，而转发通常都是根据目的地址来决定出端口。
在转发过程中，使用的是目的地址来进行转发决策的，因此，PDU地址就是目的物理地址。
路由器在网络层用的是目的IP地址。

2.下列协议中，属于**TCP/IP**参考模型应用层的是（**DNS**）。

A.DNS B.ARP C.TCP D .UDP

解析： DNS：域名服务解析。域名系统，用于为ip地址进行名字解析。dns使用端口53。在访问一个web站点前、其web站址必须解折为ip地址，dns就是提供这种解析。是典型的应用层的协议，该协议提供的服务就是DNS解析服务。
APR：地址解析协议，是网络层的,用于IP地址到MAC的解析，是根据IP地址获取物理地址的一个TCP/IP协议。在TCP/IP模型中，ARP协议属于IP层（或称网络/络层，IP层）；在OSI模型中，ARP协议属于链路层。 TCP和UDP：属于传输层协议。

> 具有五层协议的体系结构（重点看）
> OSI：七层。从上到下：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，只有最上面的三层（最下面的网络接口层没有什么具体内容）。应用层（各种应用层协议：TELNET、FTP、SMTP）、运输层（TCP或UDP）、网际层IP、网络接口层。
> 五层协议：应用层、运输层、网络层、数据链路层、网络层。
> 协议数据单元PDU是指对等层次之间传递的数据单位。 （传输的基本单位）
> 应用层：域名系统DNS、主持万维网应用的HTTP协议、支出电子邮件的SMTP协议、FTP。应用层及其他更高层次的PDU是报文。
> 设备:应用网关。
> 运输层：传输控制协议TCP、用户数据报协议UDP。设备：传输网关。
> 网络层：ARP、IP协议，ICMP协议，ARP协议、EIGRP、IGRP。网络层的PDU是IP数据报/分组。网络层=网际层=IP层。设备：路由器（可以隔离冲突域和隔离广播域）。
> 数据链路层的：PDU是数据帧。设备：网桥、交换机（可以隔离冲突域，但不能隔离广播域）。
> 物理层：PDU是比特。设备：中继器、集线器（不可以隔离冲突域和隔离广播域，是在一个区域中的）。

3.有一个网络**23.16.0.0/15,** 需要划分成很小的网络，一个是**23.16.0.0/16,**另一个是（**23.17.0.0/16**）。

解析：IP地址是32位。前15位是网络位，另外一个肯定也是/16的地址块。 23.16.0.0的IP地址是0000010111.00010000.00000000.00000000（23.16.0.0/16）， 第十六位为0和1， 所以另外一个是0000010111.00010001.00000000.00000000（23.17.0.0/16）。

4.Internet采用的拓扑结构是网状结构。

分析・：拓扑图给出网络服务器、工作站的网络配置和相互间的连接，它的结构主要有星型结构、总线结构、树型结构、网状结构、蜂窝状结构、分布式结构等。

5.在无噪声情况下，若某通信链路的带宽为**3kHz,**采用**4**个相位， 每个相位具有**4**种振幅的**QAM**调制技术，则该通信链路的最大数据传输速率是（）。

解析： 奈奎斯特定理： 奈奎斯特定理适用的情况是无噪声信道，用来计算理论值。
无噪信道传输能力公式：Cmax=2×B×log2(L) （kbps=2×3×log2(4*4) = 24kbps
（Cmax：信道的最大容量，B：信道带宽3kH，L信号电平个数16(4个相位，每个相位4中振幅)）
补充： 香农定理： 香农公式是在带噪信道容量计算时使用的公式。 Cmax=B×log2（1+（S/N）） S/N指的是信道的信噪比，但是我们一般测量出来的以db为单位的是经过10×log10（S/N）换算的，所以这里还要换算回来才行，S为信号功率，N为噪声功率。

6.tracert实用程序使用的是（**ICMP**）协议。

A 、ICMP B、TCP/IP C、PPP D、SLIP

解析：ICMP的两种应用：ping命令（测试主机的连通性）、tracert。

7.关于**ARP**协议正确的有（**BCD**）。

A、应用层协议 **B**、**ARP**协议是解决同一个局域网上的地址映射问题 **C**、将**IP**地址转换为硬件地址 **D**、网络层协议

解析：B选项补充：通过arp广播形式；同一个区域网上将IP地址转化为硬件地址；当不在一个区域时，需要多次使用ARP协议。 补充：请求采用广播方式，应答采用单播方式。
应用层：域名系统DNS、主持万维网应用的HTTP协议、支出电子邮件的SMTP协议、FTP。应用层及其他更高层次的PDU是报文。设备:应用网关。

8.判断下列哪些属于推荐使用的子网掩码（**AD**）。

A、**255.128.0.0 B**、**255.196.0.0 C**、**255…0.0.250 D**、**192.0.0.0**

解析： 子网掩码是由连续的1加连续的0组成。 255.128.0.0表示成二进制为 11111111.10000000.00000000.00000000 而其他答案不能表示成连续的1加连续的0，非掩码。

9.TCP协议提供的服务特征包括（**ACD**）。

A、全双工传输方式 **B**、支持广播方式通信 **C**、面向连接的传输 **D**、用字节流方式传输

解析：广播是一对多，本身就是不可靠传输；UDP不保证完全可靠传输，是无连接的，对于单播、广播都支持。 特点补充：端到端的通信、高可靠性、紧急数据传送功能。 （TCP和UDP重点复习一下。）运输层：传输控制协议TCP、用户数据报协议UDP

10.常用的导引型传输媒体有（**ACD**）。

A、双绞线 **B**、无线传输 **C**、光纤 **D**、同轴电缆

解析：传输媒体可分为导引型传输媒体和非导引型传输媒体。 导引型传输媒体：铜线、光纤、双绞线、同轴电缆、光缆。 非导引型传输媒体：无线传输。

11.以十六进制格式存储的一个**UDP**首部：**AC82000D001C001C,**试问源端口号是（**AC82**）。

解析：前四位——AC82。格式在书P209页。

> 补充题型： 下面是以十六进制格式存储的一个 UDP 首部： CB84000D001C001C
> 1.源端口号是什么？ 最前面的四位十六进制（CB84），代表着源端口号为52100。
> 2.目的端口号是什么？ 第二个四位十六进制（000D），代表目的端口号为13。
> 3.这个用户数据报的总长度是什么？ 第三个四位十六进制（001C）定义了整个UDP分组的长度为28字节。
> 4.数据长度是多少？ 数据长度=整个分组的长度-首部的长度=28-8=20字节
> 5.这个分组是从客户到服务器方向的，还是从服务器到客户方向的？
> 目的端口号是13（熟知端口），所以是从客户到服务器的.

12.统一资源定位符**URL**由模式（或称协议、服务）、主机、端口、路径组成。

13.网络层提供的两种虚电路服务和（数据报服务）。
分析：网络层向运输层(网络层向上)提供了 ‘’ 面向连接”虚电路（Virtual Circuit）服务或“无连接”数据报服务

知识点:

98道题目，题型：单选+多选+填空

1.三网合一：电信网络、有线电视网络、计算机网络。

2.P10-11

互联网的组成：边缘部分、核心部分。
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(CIS方式)和对等方式(P2P方式) 。
客户-服务器方式(CIS方式)特点：客户是请求方，服务器是服务提供方；客户程序必须要知道服务器程序的地址；可以同时处理多个远地或本地客户的请求；程序不需要知道客户程序的地址；通信可以是双向的。
对等方式(P2P方式) 特点：本质上仍然是客户-服务器方式，知识对等连接中的每一台主机既是客户有同时是服务器。

3.三种交换方式：电路交换、报文交换、分组交换。

4.P20 计算机网络的类别

1.5.2 几种不同类别的计算机网络

计算机网络有多种类别，下面进行简单的介绍。

1. 按照网络的作用范围进行分类

(1) **广域网 WAN** (Wide Area Network)　广域网的作用范围通常为几十到几千公里，因而有时也称为**远程网**(long haul network)。广域网是互联网的核心部分，其任务是通过长距离（例如，跨越不同的国家）运送主机所发送的数据。连接广域网各结点交换机的链路一般都是高速链路，具有较大的通信容量。本书不专门讨论广域网。

(2) **城域网 MAN** (Metropolitan Area Network)　城域网的作用范围一般是一个城市，可跨越几个街区甚至整个城市，其作用距离约为 5 ~ 50 km。城域网可以为一个或几个单位所拥有，但也可以是一种公用设施，用来将多个局域网进行互连。目前很多城域网采用的是以太网技术，因此有时也常并入局域网的范围进行讨论。

(3) **局域网 LAN** (Local Area Network)　局域网一般用微型计算机或工作站通过高速通信线路相连（速率通常在 10 Mbit/s 以上），但地理上则局限在较小的范围（如 1 km 左右）。在局域网发展的初期，一个学校或工厂往往只拥有一个局域网，但现在局域网已非常广泛地使用，学校或企业大都拥有许多个互连的局域网（这样的网络常称为**校园网**或**企业网**）。我们将在第 3 章 3.3 至 3.5 节详细讨论局域网。

(4) **个人区域网** PAN (Personal Area Network)　个人区域网就是在个人工作的地方把属于个人使用的电子设备（如便携式电脑等）用无线技术连接起来的网络，因此也常称为**无线个人区域网** WPAN (Wireless PAN)，其范围很小，大约在 10 m 左右。我们将在第 9 章 9.2 节对这种网络进行简单的介绍。

般就称之为**多处理机系统**而不称它为计算机网络。

2. 按照网络的使用者进行分类

(1) **公用网**(public network)　这是指电信公司（国有或私有）出资建造的大型网络。“公用”的意思就是所有愿意按电信公司的规定交纳费用的人都可以使用这种网络。因此公用网也可称为**公众网**。

(2) **专用网**(private network)　这是某个部门为满足本单位的特殊业务工作的需要而建造的网络。这种网络不向本单位以外的人提供服务。例如，军队、铁路、银行、电力等系统均有本系统的专用网。

公用网和专用网都可以提供多种服务。如传送的是计算机数据，则分别是公用计算机网络和专用计算机网络。

3. 用来把用户接入到互联网的网络

这种网络就是**接入网** AN (Access Network)，它又称为**本地接入网**或**居民接入网**。这是一类比较特殊的计算机网络。我们在前面的 1.2.2 节已经介绍了用户必须通过 ISP 才能接入到互联网。由于从用户家中接入到互联网可以使用的技术有许多种，因此就出现了可以使用

按照网络的作用范围进行分类：广域网**WAN**（远程网）、城域网**MAN**、局域网**LAN**、个人局域网**PAN**。

按照网络的使用者进行分类：公用网/公众网、专用网。

5.计算机网络的性能指标：速率、带宽、吞吐量、时延、时延带宽积、往返时间**RTT**、利用率，单位换算注意。（**P21~25**）

4. 时延

时延(delay 或 latency)是指数据（一个报文或分组，甚至比特）从网络（或链路）的一端传送到另一端所需的时间。时延是个很重要的性能指标，它有时也称为**延迟**或**迟延**。

需要注意的是，网络中的时延是由以下几个不同的部分组成的：

(1) **发送时延**　**发送时延**(transmission delay)**是主机或路由器发送数据帧所需要的时间**，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。因此发送时延也叫做**传输时延**（我们尽量不采用传输时延这个名词，因为它很容易和下面要讲到的传播时延弄混）。发送时延的计算公式是：

$$\text{发送时延} = \frac{\text{数据帧长度 (bit)}}{\text{发送速率 (bit/s)}} \tag{1-1}$$

由此可见，对于一定的网络，发送时延并非固定不变，而是与发送的帧长（单位是比特）成正比，与发送速率成反比。

(2) 传播时延　**传播时延**(propagation delay)**是电磁波在信道中传播一定的距离需要花费的时间。**传播时延的计算公式是：

$$\text{传播时延} = \frac{\text{信道长度(m)}}{\text{电磁波在信道上的传播速率(m/s)}} \tag{1-2}$$

电磁波在自由空间的传播速率是光速，即 3.0×10^5 km/s。电磁波在网络传输媒体中的传播速率比在自由空间要略低一些：在铜线电缆中的传播速率约为 2.3×10^5 km/s，在光纤中的传播速率约为 2.0×10^5 km/s。例如，1000 km 长的光纤线路产生的传播时延大约为 5 ms。

以上两种时延有本质上的不同。但只要理解这两种时延发生的地方就不会把它们弄

节），**与传输信道的长度（或信号传送的距离）没有任何关系。**但传播时延则发生在机器外部的传输信道媒体上，而**与信号的发送速率无关。信号传送的距离越远，传播时延就越大。**可以用一个简单的比喻来说明。假定有 10 辆车按顺序从公路收费站入口出发到相距 50 公里的目的地。再假定每一辆车过收费站要花费 6 秒钟，而车速是每小时 100 公里。现在可以算出这 10 辆车从收费站到目的地总共要花费的时间：发车时间共需 60 秒（相当于网络中的发送时延），在公路上的行车时间需要 30 分钟（相当于网络中的传播时延）。因此从第一辆车到收费站开始计算，到最后一辆车到达目的地为止，总共花费的时间是二者之和，即 31 分钟。

下面还有两种时延也需要考虑，但比较容易理解。

(3) 处理时延　主机或路由器在收到分组时要花费一定的时间进行处理，例如分析分组的首部、从分组中提取数据部分、进行差错检验或查找适当的路由等，这就产生了处理时延。

(4) 排队时延　分组在经过网络传输时，要经过许多路由器。但分组在进入路由器后要先在输入队列中排队等待处理。在路由器确定了转发接口后，还要在输出队列中排队等待转发。这就产生了排队时延。排队时延的长短往往取决于网络当时的通信量。当网络的通信量很大时会发生队列溢出，使分组丢失，这相当于排队时延为无穷大。

这样，数据在网络中经历的总时延就是以上四种时延之和：

$$\text{总时延} = \text{发送时延} + \text{传播时延} + \text{处理时延} + \text{排队时延} \tag{1-3}$$

一般说来，小时延的网络要优于大时延的网络。在某些情况下，一个低速率、小时延的网络很可能要优于一个高速率但大时延的网络。

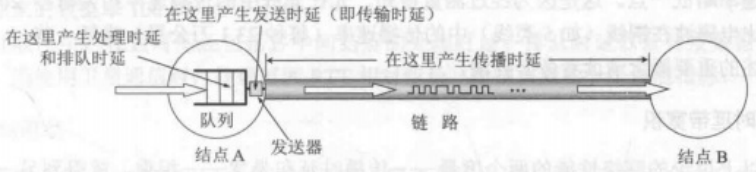


图 1-14　几种时延产生的地方不一样

必须指出，在总时延中，究竟是哪一种时延占主导地位，必须具体分析。下面举个例子。

现在我们暂时忽略处理时延和排队时延[①]。假定有一个长度为 100 MB 的数据块（这里的 M 显然不是指 10^6 而是指 2^{20}。B 是字节，1 字节 = 8 比特）。在带宽为 1 Mbit/s 的信道上（这里的 M 显然是 10^6）连续发送（即发送速率为 1 Mbit/s），其发送时延是

$$100 \times 2^{20} \times 8 \div 10^6 = 838.9 \text{ s}$$

现在把这个数据块用光纤传送到 1000 km 远的计算机。由于在 1000 km 的光纤上的传

① 注：当计算机网络中的通信量过大时，网络中的许多路由器的处理时延和排队时延将会大大增加，因而处理时延和排队时延有可能在总时延中占据主要成分。这时整个网络的性能就变差了。

播时延约为 5 ms，因此在这种情况下，发送 100 MB 的数据块的总时延 = 838.9 + 0.005 ≈

如果我们把发送速率提高到 100 倍，即提高到 100 Mbit/s，那么总时延就变为 8.389 + 0.005 = 8.394 s，缩小到原有数值的 1/100。

但是，并非在任何情况下，提高发送速率就能减小总时延。例如，要传送的数据仅有 1 个字节（如键盘上键入的一个字符，共 8 bit）。当发送速率为 1 Mbit/s 时，发送时延是

$$8 \div 10^6 = 8 \times 10^{-6}\ \text{s} = 8\ \mu\text{s}$$

若传播时延仍为 5 ms，则总时延为 5.008 ms。在这种情况下，传播时延决定了总时延。如果我们把数据率提高到 1000 倍（即将数据的发送速率提高到 1 Gbit/s），不难算出，总时延基本上仍是 5 ms，并没有明显减小。这个例子告诉我们，不能笼统地认为："数据的发送速率越高，其传送的总时延就越小"。这是因为数据传送的总时延是由公式(1-3)右端的四项时延组成的，不能仅考虑发送时延一项。

如果上述概念没有弄清楚，就很容易产生这样错误的概念："在高速链路（或高带宽链路）上，比特会传送得更快些"。但这是不对的。我们知道，汽车在路面质量很好的高速公路上可明显地提高行驶速率。然而**对于高速网络链路，我们提高的仅仅是数据的发送速率而不是比特在链路上的传播速率**。荷载信息的电磁波在通信线路上的传播速率（这是光速的数量级）取决于通信线路的介质材料，而与数据的发送速率并无关系。**提高数据的发送速率只是减小了数据的发送时延**。还有一点也应当注意，就是数据的发送速率的单位是每秒发送多少个比特，这是指在**某个点**或**某个接口上**的发送速率。而传播速率的单位是每秒传播多少公里，是指在**某一段传输线路上**比特的传播速率。因此，通常所说的"光纤信道的传输速率高"是指可以用很高的速率向光纤信道发送数据，而光纤信道的传播速率实际上还要比铜线的传播速率略低一点。这是因为经过测量得知，光在光纤中的传播速率约为每秒 20.5 万公里，它比电磁波在铜线（如 5 类线）中的传播速率（每秒 23.1 万公里）略低一些。

上述的重要概念请读者务必弄清。

5. 时延带宽积

用的度量：传播**时延带宽积**，即

$$\text{时延带宽积} = \text{传播时延} \times \text{带宽} \tag{1-4}$$

我们可以用图 1-15 的示意图来表示时延带宽积。这是一个代表链路的圆柱形管道，管道的长度是链路的传播时延（请注意，现在以**时间**作为单位来表示链路长度），而管道的截面积是链路的带宽。因此时延带宽积就表示这个管道的体积，表示这样的链路可容纳多少个比特。例如，设某段链路的传播时延为 20 ms，带宽为 10 Mbit/s。算出

$$\text{时延带宽积} = 20 \times 10^{-3} \times 10 \times 10^6 = 2 \times 10^5\ \text{bit}$$

这就表明，若发送端连续发送数据，则在发送的第一个比特即将达到终点时，发送端就已经发送了 20 万个比特，而这 20 万个比特都正在链路上向前移动。因此，链路的时延带宽积又称为**以比特为单位的链路长度**。

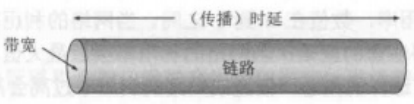


图 1-15　链路像一条空心管道

不难看出，管道中的比特数表示从发送端发出的但尚未到达接收端的比特。对于一条

6. 往返时间 RTT

在计算机网络中，**往返时间** RTT (Round-Trip Time)也是一个重要的性能指标。这是因为在许多情况下，互联网上的信息不仅仅单方向传输而是双向交互的。因此，我们有时很需要知道双向交互一次所需的时间。例如，A 向 B 发送数据。如果数据长度是 100 MB，发送速率是 100 Mbit/s，那么

$$\text{发送时间} = \frac{\text{数据长度}}{\text{发送速率}} = \frac{100 \times 2^{20} \times 8}{100 \times 10^6} \approx 8.39\text{s}$$

如果 B 正确收完 100 MB 的数据后，就立即向 A 发送确认，再假定 A 只有在收到 B 的

如果 B 正确收完 100 MB 的数据后，就立即向 A 发送确认。再假定 A 只有在收到 B 的确认信息后，才能继续向 B 发送数据。显然，这需要等待一个往返时间 RTT（这里假定确认信息很短，可忽略 B 发送确认的时间）。如果 RTT = 2 s，那么可以算出 A 向 B 发送数据的有效数据率。

$$有效数据率=\frac{数据长度}{发送时间+RTT}=\frac{100\times2^{20}\times8}{8.39+2}\approx80.7\times10^{6}\,bit/s\approx80.7Mbit/s$$

比原来的数据率 100 Mbit/s 小不少。

在互联网中，往返时间还包括各中间结点的处理时延、排队时延以及转发数据时的发送时延。当使用卫星通信时，往返时间 RTT 相对较长，是很重要的一个性能指标。

7. 利用率

利用率有信道利用率和网络利用率两种。信道利用率指出某信道有百分之几的时间是被利用的（有数据通过）。完全空闲的信道的利用率是零。网络利用率则是全网络的信道利用率的加权平均值。信道利用率并非越高越好。这是因为，根据排队论的理论，当某信道的利用率增大时，该信道引起的时延也就迅速增加。这和高速公路的情况有些相似。当高速公路上的车流量很大时，由于在公路上的某些地方会出现堵塞，因此行车所需的时间就会变

时延：发送时延、传播时延、处理时延、排队时延。（前两者要会计算，在哪里产生。）

发送时延：是主机或路由器发送数据帧所需要的时间，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。发送时延的 = 数据帧长度(bit) /发送速率(bit/s)。
传播时延：是电磁波在信道中传播一定的距离需要花费的时间。传播时延 = 信道长度(m) /电磁波在信道上的传播速率(m/s)。

6.体系结构 **1.7**节

（1）.协议概念：为进行网络中的数据交换而建立的规则、标准或约定称为网络协议。简称协议。
（2）.网络协议三要素：语法、语义、同步(时序)。
（3）.服务概念：服务是由下层向上层通过层间接口提供的。

（**4**）**.**具有五层协议的体系结构（重点看）

OSI：七层。从上到下：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，只有最上面的三层（最下面的网络接口层没有什么具体内容）。应用层（各种应用层协议：TELNET、FTP、SMTP）、运输层（TCP或UDP）、网际层IP、网络接口层。
五层协议：应用层、运输层、网络层、数据链路层、网络层。

（5）协议数据单元PDU是指对等层次之间传递的数据单位。（传输的基本单位）
（6）应用层：域名系统DNS、主持万维网应用的HTTP协议、支出电子邮件的SMTP协议、FTP。应用层及其他更高层次的PDU是报文。设备:应用网关。
（7）运输层：传输控制协议TCP、用户数据报协议UDP。设备：传输网关。
（8）网络层：ARP、IP协议，ICMP协议，ARP协议、EIGRP、IGRP。网络层的PDU是IP数据报/分组。网络层=网际层=IP层。设备：路由器（可以隔离冲突域和隔离广播域）。
（9）数据链路层的：PDU是数据帧。设备：网桥、交换机（可以隔离冲突域，但不能隔离广播域）。
（10）物理层：PDU是比特。设备：中继器、集线器（不可以隔离冲突域和隔离广播域，是在一个区域中的）。

7.实体概念：任何可以发送或接受信息的软件或硬件进程。

8.协议概念：控制两个对等/多个实体进行通信的规则的集合。是“水平的”。

9.服务概念：是“垂直的”。

10.物理层的四个特性：

机械特性：指明接口所用接线器的形状和尺寸、引脚数目和排列、固定和锁定装置，等。平时常见的各种规格的接插件都有严格的标准化的规定。
电气特性：指明在接口电缆的各条线上出现的电压的范围。
功能特性：指明某条线上出现的某一电平的电压的意义。
过程特性：指明对于不同功能的各种可能事件的出现顺序。

11.P44 常用编码方式

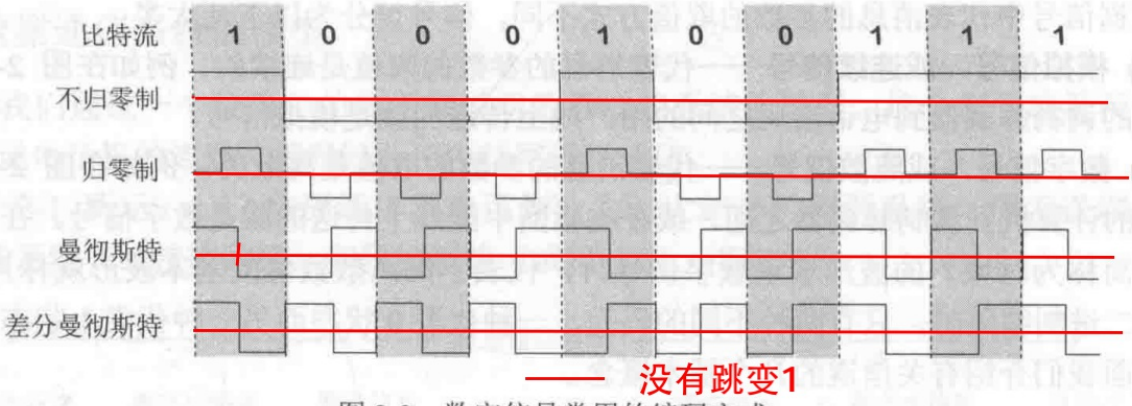


图 2-2　数字信号常用的编码方式

虚线部分：位开始边界

- **不归零制**　正电平代表 1，负电平代表 0。
- **归零制**　正脉冲代表 1，负脉冲代表 0。
- **曼彻斯特编码**　位周期中心的向上跳变代表 0，位周期中心的向下跳变代表 1。但也可反过来定义。
- **差分曼彻斯特编码**　在每一位的中心处始终都有跳变。位开始边界有跳变代表 0，而位开始边界没有跳变代表 1。

从信号波形中可以看出，曼彻斯特(Manchester)编码产生的信号频率比不归零制高。从自同步能力来看，不归零制不能从信号波形本身中提取信号时钟频率（这叫做没有自同步能力），而曼彻斯特编码具有自同步能力。

12.信道的极限容量：书**P45**

从概念上讲，限制码元在信道上的传输速率的因素有以下两个。
信道能够通过的频率范围、信噪比。
数据传输速率：R=1/T log2N (bps)，T－数字脉冲信号的宽度，N－－个码元所取的有效离散个数。
信号传输速率：B＝1/T (Baud)，也称码元速率、调制速率、波特率。表示单位时间内通过信道传输的码元个数。
R=B・log2N
B=R/ log2N

奈氏准则

奈奎斯特定理又称奈氏准则。
奈奎斯特定理适用的情况是无噪声信道，用来计算理论值。
无噪信道传输能力公式：Cmax=2×B×log2L（kbps）
（Cmax：信道的最大容量，单位为bit/s;B：信道带宽3kH，单位为Hz;L信号电平个数)）

香农公式

香农公式是在带噪信道容量计算时使用的公式。
C=B×log2(1+S÷N)(bit/s)
S/N指的是信道的信噪比，但是我们一般测量出来的以db为单位的是经过10×log10（S/N）换算的，所以这里还要换算回来才行，S为信号功率，N为噪声功率。

13.物理层下面的传输媒体

传输媒体可分为两大类，导引型传输媒体和非导引型传输媒体
导引型传输媒体中：铜线、光纤/光缆（用的多）、双绞线（用的多）、同轴电缆。
非导引型传输媒体就是指自由空间：无线传输。
注意：光纤分为多模光纤和单模光纤。
多模光纤：可以存在多条不同角度入射的光线在一条光纤中传输。特点：只适合于近距离传输。
单模光纤：它可使光线一直向前传播，而不会产生多次反射。特点：纤芯很细、制造起来成本较高、衰耗较小、适合远距离传输。
光纤的通信容量非常大。

14.信道复用技术

最基本的复用就是频分复用和时分复用。
统计时分复用STDM、码分复用、波分复用。
在CDMA中，每一个比特时间再划分为m个短的间隔，称为码片。通常m的值是64或128。通常是设m为8。

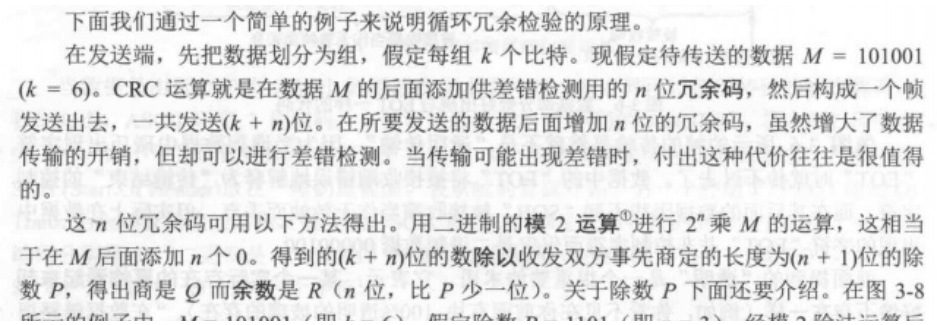
（书P57）
使用CDMA的每一个站被指派一个唯一的m bit 码片序外列。 一个站如果要发送比特1，则发送它自己的mbit码片序列。如果要发送比特0，则发送该码片序列的二进制反码。例如，指派给S站的8 bit 码片序列是00011011。当S发送比特1时，它就发送序列00011011，而当S发送比特0时，就发送11100100。为了方便，我们按惯例将码片中的0写为-1，将1写为+1。因此S站的码片序列是(-1-1-1+1+1-1+1 +1)。
码分复用需要知道：两个不同站的码片序列正交，就是向量s和T的规格化内积都是0；任何一个码片向量和该码片向量自己的规格化内积都是1；而一个码片向量和该码片反码的向量的规格化内积值是-1。

> *例题（重要）：共有四个站进行码分多址CDMA通信。四个站的码片序列为:*
> *A:(-1-1-1+1+1-1 +1 +1) B:(-1-1+1-1+1+1 +1-1) C:(-1+1-1+1 +1+1-1-1) D:(-1+1-1-1-1-1 +1-1)*
> *现收到这样的码片序列: (-1 +1-3+1-1-3+1 +1)。问哪个站发送数据了?发送数据的站发送的是1还是0?*
> *解析：假设收到的码片序列为X向量。*
> *判断A站是否发送了数据：A（Sx+Tx）。即计算一下A和X的规格化内积（=1），每一位分别相乘加起来求和ans，ans/m（位数8)=1，即A站发送了数据，发送的数据为1。B的规格化内积-1，发送了数据，发送的数据为0。C的规格化内积0，没有发送出去。D的规格化内积+1，发送了数据，发送的数据为1。*

15.数据链路层使用的信道主要是：点对点信道（一对一）、广播信道（一对多）。

16.数据链路层协议有许多种，但有三个基本问题则是共同的。这三个基本问题是：封装成帧、透明传输和差错检测。

具体含义：
封装成帧：就是在一段数据的前后分别添加首部和尾部，这样就构成了一个帧。
透明传输：（书P73）用字节填充解决透明传输的问题。需要知道如何实现的。
差错检测：比特差错：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。比特差错是传输差错中的一种。在一段时间内，传输错误的比特占所传输比特总数的比率称为误码率BER。误码率与信噪比有很大的关系。如果设法提高信噪比，就可以使误码率减小。实际的通信链路并非是理想的，它不可能使误码率下降到零。因此，为了保证数据传输的可靠性，在计算机网络传输数据时，必须采用各种差错检测措施。
目前在数据链路层广泛使用了循环冗余检验CRC的检错技术。（这个技术需要会，书P74。）



下面我们通过一个简单的例子来说明循环冗余检验的原理。

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 的后面添加供差错检测用的 n 位**冗余码**，然后构成一个帧发送出去，一共发送($k + n$)位。在所要发送的数据后面增加 n 位的冗余码，虽然增大了数据传输的开销，但却可以进行差错检测。当传输可能出现差错时，付出这种代价往往是很值得的。

这 n 位冗余码可用以下方法得出。用二进制的**模 2 运算**[1]进行 2^n 乘 M 的运算，这相当于在 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）。关于除数 P 下面还要介绍。在图 3-8

所示的例子中，$M = 101001$（即 $k = 6$）。假定除数 $P = 1101$（即 $n = 3$）。经模 2 除法运算后的结果是：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**帧检验序列** FCS (Frame Check Sequence)。因此加上 FCS 后发送的帧是 101001001（即 $2^nM + \text{FCS}$），共有$(k + n)$位。

顺便说一下，循环冗余检验 CRC 和帧检验序列 FCS 并不是同一个概念。CRC 是一种**检错方法**，而 FCS 是添加在数据后面的**冗余码**，在检错方法上可以选用 CRC，但也可不选用 CRC。

---

① 注：用模 2 运算进行加法时不进位。例如，1111 + 1010 = 0101，减法和加法一样。按加法规则计算。

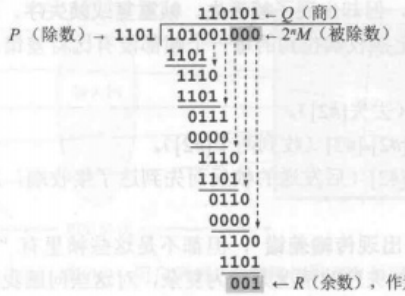


图 3-8　说明循环冗余检验原理的例子

在接收端把接收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（读者可以自己验算一下。被除数现在是 101001001，而除数是 $P = 1101$，看余数 R 是否为 0）。

但如果出现误码，那么余数 R 仍等于零的概率是非常非常小的（这可以通过不太复杂的概率计算得出，例如，可参考[TANE11]）。

总之，在接收端对收到的每一帧经过 CRC 检验后，有以下两种情况：

(1) 若得出的余数 $R = 0$，则判定这个帧没有差错，就接受(accept)。

(2) 若余数 $R \neq 0$，则判定这个帧有差错（但无法确定究竟是哪一位或哪几位出现了差错），就丢弃。

一种较方便的方法是用多项式来表示循环冗余检验过程。在上面的例子中，用多项式 $P(X) = X^3 + X^2 + 1$ 表示上面的除数 $P = 1101$（最高位对应于 X^3，最低位对应于 X^0）。多项式 $P(X)$称为**生成多项式**。现在广泛使用的生成多项式 $P(X)$有以下几种：

$$\text{CRC-CCITT} = X^{16} + X^{12} + X^5 + 1$$

$$\text{CRC-32} = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

在数据链路层，发送端帧检验序列 FCS 的生成和接收端的 CRC 检验都是用硬件完成的，处理很迅速，因此并不会延误数据的传输。

从以上的讨论不难看出，如果我们在传送数据时不以帧为单位来传送，那么就无法加入冗余码以进行差错检验。因此，如果要在数据链路层进行差错检验，就必须把数据划分为帧，每一帧都加上冗余码，一帧接一帧地传送，然后在接收方逐帧进行差错检验。

最后再强调一下，在数据链路层若**仅仅**使用循环冗余检验 CRC 差错检测技术，则只能做到对帧的**无差错接受**，即：**“凡是接收端数据链路层接受的帧，我们都能以非常接近于 1 的概率认为这些帧在传输过程中没有产生差错”**。接收端丢弃的帧虽然曾**收到**了，但最终还是因为有差错被丢弃，即没有被**接受**。以上所述的可以**近似地**表述为（通常都是这样认为）：

CRC计算（重要）
要发送的数据为1101011011。采用CRC的生成多项式是P(X)=X^4++X+ 1。试求应添加在数据后面的余数。数据在传输过程中最后一个1变成了0， 问接收端能否发现?
解析:
由多项式则可知位10011除数5位，n=5,则在数据后面加n-1位0(5-1=4位0)
1101011010000除以10011（多项式所在1的位置），余数1111（除数的位数-1）
接收端：1101011001111（FCS）%10011=1，（=0说明传输过程中没有差错。该题检测错误）

17.点对点协议**PPP**是目前使用得最广泛的数据链路层协议。

书P83

18.媒体共享技术的两种方法：静态划分信道、动态媒体接入控制（随机接入、受控接入）。

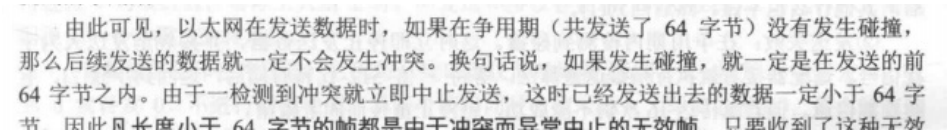
19.CSMA/CD协议的三个要点

多点接入：就是说明这是总线型网络，许多计算机以多点接入的方式连接在一根总线上。协议的实质是“载波监听”和“碰撞检测”。
载波监听：用电子技术检测总线上有没有其他计算机也在发送。其实总线上并没有什么“载波”，这里只不过借用一下“载波”这个名词而已。因此载波监听就是检测信道，这是个很重要的措施。不管在发送前，还是在发送中，每个站都必须不停地检测信道。在发送前检测信道，是为了获得发送权。如果检测出已经有其他站在发送，则自己就暂时不许发送数据，必须要等到信道变为空闲时才能发送。在发送中检测信道，是为了及时发现有没有其他站的发送和本站发送的碰撞。
碰撞检测：就是“边发送边监听”，又称冲突检测。即适配器边发送数据边检测信道上的信号电压的变化情况，以便判断自己在发送数据时其他站是否也在发送数据。
产生碰撞：当几个站同时在总线上发送数据时，总线上的信号电压变化幅度将会增大(互相叠加)。当适配器检测到的信号电压变化幅度超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了碰撞。
解决：适配器就立即停止发送，然后等待一段时间后再次发送。

20.最短帧长

以太网最小帧长是64字节，如果小于64字节，就认为是冲突、异常而产生的无效帧。
计算要会：因为：信号传播时延(μs)= 两站点间的距离(m)÷信号传播速度(200m/μs)，并且：数据传输时延 (s)=数据帧长度(bit)÷数据传输速率(bps)。
所以：CSMA/CD总线网中最短帧长的计算公式为：
最短数据帧长(bit)/数据传输速率(Mbps)=2*(两站点间的最大距离(m)/200m/μs)

为什么是64？看书，争用期等。书P88。


由此可见，以太网在发送数据时，如果在争用期（共发送了 64 字节）没有发生碰撞，那么后续发送的数据就一定不会发生冲突。换句话说，如果发生碰撞，就一定是在发送的前 64 字节之内。由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节。因此凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧。只要收到了这种无效

21.对于**10 Mbit/s** 以太网，发送**512bit**的时间需要**51.2**微秒。帧间最小间隔是**9.6**微秒，**96**比特时间。

22.以太网包括三种帧：单播帧、广播帧、多播帧。

23.在物理层扩展以太网，用的是集线器，共享带宽。在数据链路层扩展以太网，用的是交换机，独享带宽，独占传输媒体，无碰撞地传输数据。

24.通过划分虚拟局域网**VLAN**（逻辑的分组），可以隔离广播，同一个**VLAN**之间的主机可以通信，可以跨越多个交换机；不在一个**VLAN**之间的主机不可以通信。虚拟局域网限制了接收广播信息的计算机数，使得网络不会因传播过多的广播信息(即所谓的“广播风暴”)而引起性能恶化。

25.网络层提供的两种服务：数据报服务和虚电路服务。

虚电路服务与数据报服务的区别： 书上详细的P115。

表 4-1 归纳了虚电路服务与数据报服务的主要区别。

表 4-1 虚电路服务与数据报服务的对比

对比的方面	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
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	到达终点的时间不一定按发送顺序
端到端的差错处理和流量控制	可以由网络负责，也可以由用户主机负责	由用户主机负责

鉴于 TCP/IP 体系的网络层提供的是数据报服务，因此下面我们的讨论都是围绕网络层

	虚电路	数据报
端一端连接	要	不要
目的站地址	仅连接是需要	每个分组都需要
分组顺序	按序	按序
目的站地址	仅连接是需要	每个分组都需要
目的站地址	均由通信子网负责	均由主机负责
终点地址	连接建立用，短	每个分组都有终点的完整地址

26.网络层三个典型协议：地址解析协议**ARP**、网际控制报文协议**ICMP**、网际组组管理协议**IGMP**。

27.两级**IP**地址：**IP**地址 **::={**<网络号>,<主机号>**}**。**IP**地址为**32**位。

书P121

28.**常见的三种类别的**IP**地址（基础）

A类：1~126
B类：128.1~191.255
C类：192.0.1~223.255.255**
特殊不使用的IP地址（不能分配给某一台主机）：127、128.0.0、192.0.0。
全0和全1的也不分配：主机号为全1含义：这个网络上面的广播地址；全0：本主机。

29.从层次的角度看，物理地址是数据链路层和物理层使用的地址，而**IP**地址是网络层和以上各层使用的地址，是一种逻辑地址(称**IP**地址为逻辑地址是因为**IP**地址是用软件实现的)。

IP地址与硬件地址的区别

IP地址：是一种逻辑地址；IP地址称为逻辑地址，是因为IP地址是用软件实现的；是网络层及其以上各层(包括运输层、应用层等)使用的地址；放在IP数据报的首部。
硬件地址：是一种物理地址；硬件地址是用硬件实现的；是数据链里层和物理层使用的地址；放在MAC帧的首部。

IP地址与硬件地址的转换

由于是IP协议使用了ARP协议，因此通常就把ARP协议划归网络层。但ARP协议的用途是为了从网络层使用的IP地址，解析出在数据链路层使用的硬件地址。因此，有的教科书就按照协议的所用，把ARP协议划归在数据链路层。这样做当然也是可以的。

30.IP数据报的格式

32位

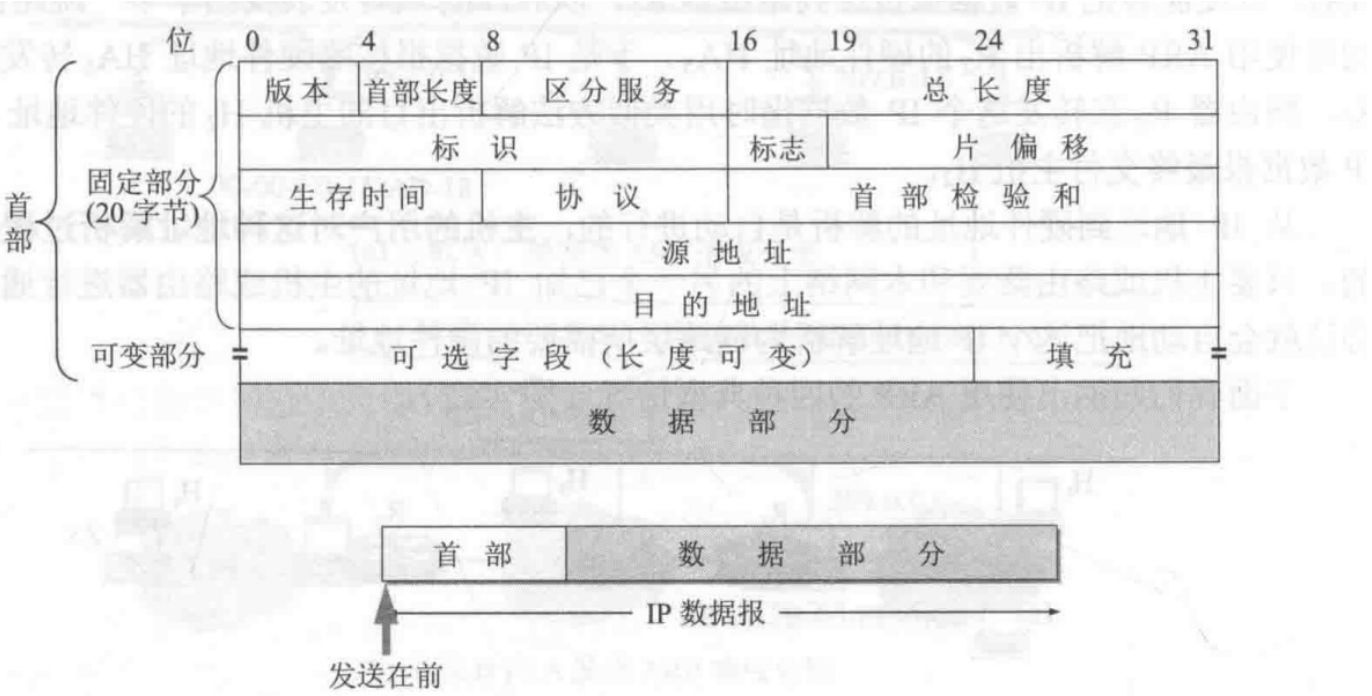


图 4-13 IP 数据报的格式

一个IP数据报由首部和数据两部分组成。首部的前一部分是固定长度，共20字节，是所有IP数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。

31.划分子网 书**P136**

需要会计算:
借了多少位划分子网合适?
之后主机位还有多少?
划分的子网可容纳的主机数是多少?
给IP地址和子网掩码计算网络地址？IP和子网掩码进行与运算

是相与的意思。算术"与"操作。“&&”这是逻辑“与”操作。基本操作有
0&1=0;
1&1=1;
0&0=0;

【例 4-2】已知 IP 地址是 141.14.72.24，子网掩码是 255.255.192.0。试求网络地址。

【解】 子网掩码是 11111111 11111111 11000000 00000000。请注意，掩码的前两个字节都是全 1，因此网络地址的前两个字节可写为 141.14。子网掩码的第四字节是全 0，因此网络地址的第四字节是 0。可见本题仅需对地址中的第三字节进行计算。我们只要把 IP 地址和子网掩码的第三字节用二进制表示，就可以很容易地得出网络地址（图 4-22）。

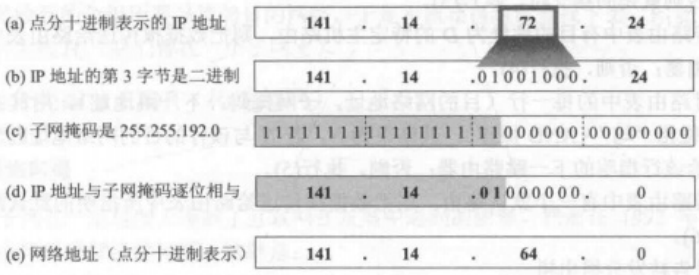


图 4-22 网络地址的计算

请注意，在一个 IP 地址中不允许把十进制和二进制混合使用。图 4-22 中(b)和(d)的写

默认子网掩码
A类地址的~：255.0.0.0
B类地址的~：255.255.0.0
C类地址的~：255.255.255.0

32.无分类编址CIDR（构造超网）

CIDR的斜线记法/CIDR记法：IP地址后面加上斜线 / ，然后写上网络前缀所占的位数。
给出一个地址块，要写的出范围，
进行聚合的时候：前多少位是一样，聚合为一个网络
具体例子看书P142。

(2) CIDR 把**网络前缀都相同**的连续的 IP 地址组成一个“**CIDR 地址块**”。我们只要知道 CIDR 地址块中的任何一个地址，就可以知道这个地址块的起始地址（即最小地址）和最大地址，以及地址块中的地址数。例如，已知 IP 地址 128.14.35.7/20 是某 CIDR 地址块中的一个地址，现在把它写成二进制表示，其中的前 20 位是网络前缀（用粗体和下划线表示出），而前缀后面的 12 位是主机号：

128.14.35.7/20 = **10000000 00001110 0010**0011 00000111

这个地址所在的地址块中的最小地址和最大地址可以很方便地得出：

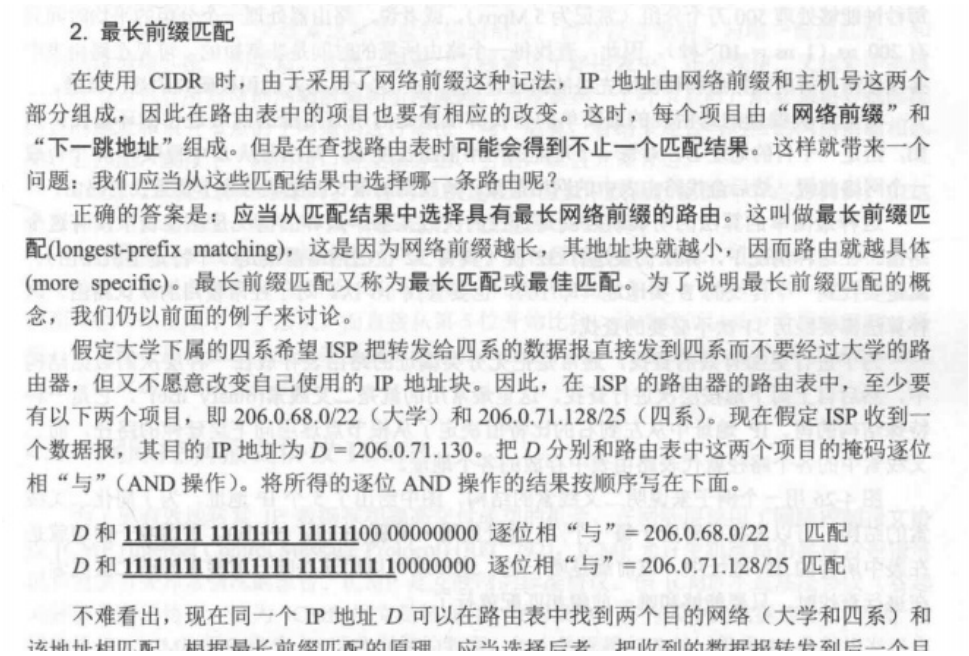
最小地址	128.14.32.0	**10000000 00001110 0010**0000 00000000
最大地址	128.14.47.255	**10000000 00001110 0010**1111 11111111

当然，以上这两个特殊地址的主机号是全 0 和全 1 的地址。一般并不使用。通常只使用在这两个特殊地址之间的地址。不难看出，这个地址块共有 2^{12} 个地址。我们可以用地址块中的最小地址和网络前缀的位数指明这个地址块。例如，上面的地址块可记为 128.14.32.0/20。在不需要指出地址块的起始地址时，也可把这样的地址块简称为“/20 地址

例如，地址 192.199.170.82/27 不仅表示 IP 地址是 192.199.170.82，而且还表示这个地址块的网络的前缀有 27 位（剩下的 5 位是主机号），因此这个地址块包含 32 个 IP 地址（2^5 = 32）。通过简单的计算还可得出，这个地址块的最小地址是 192.199.170.64，最大地址是 192.199.170.95。具体的计算方法是这样的。找出地址掩码中 1 和 0 的**交界处**发生在地址中的哪一个字节。现在是在第四个字节。因此只要把**这一个字节**的十进制 82 用二进制表示即可。十进制 82 的二进制是 01010010，取其前 3 位（这 3 位加上前 3 个字节的 24 位等于前缀的 27 位），再把后面 5 位都写成 0，即 010**00000**，等于十进制的 64。这就找出了地址块的最小地址 192.199.170.64。再把地址的第四字节的最后 5 位都置 1，即 010**11111**，等于十

33.最长前缀匹配

看书P145



2. 最长前缀匹配

在使用 CIDR 时，由于采用了网络前缀这种记法，IP 地址由网络前缀和主机号这两个部分组成，因此在路由表中的项目也要有相应的改变。这时，每个项目由“**网络前缀**”和“**下一跳地址**”组成。但是在查找路由表时**可能会得到不止一个匹配结果**。这样就带来一个问题：我们应当从这些匹配结果中选择哪一条路由呢？

正确的答案是：**应当从匹配结果中选择具有最长网络前缀的路由**。这叫做**最长前缀匹配**(longest-prefix matching)，这是因为网络前缀越长，其地址块就越小，因而路由就越具体(more specific)。最长前缀匹配又称为**最长匹配**或**最佳匹配**。为了说明最长前缀匹配的概念，我们仍以前面的例子来讨论。

假定大学下属的四系希望 ISP 把转发给四系的数据报直接发到四系而不要经过大学的路由器，但又不愿意改变自己使用的 IP 地址块。因此，在 ISP 的路由器的路由表中，至少要有以下两个项目，即 206.0.68.0/22（大学）和 206.0.71.128/25（四系）。现在假定 ISP 收到一个数据报，其目的 IP 地址为 $D = 206.0.71.130$。把 D 分别和路由表中这两个项目的掩码逐位相“与”（AND 操作）。将所得的逐位 AND 操作的结果按顺序写在下面。

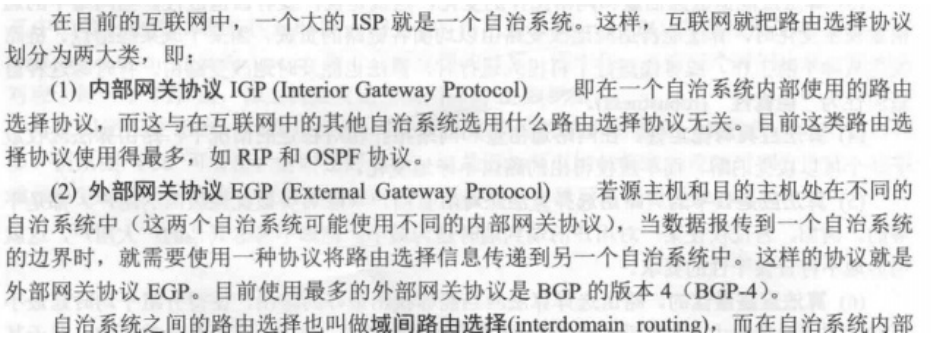
D 和 11111111 11111111 11111100 00000000 逐位相“与”= 206.0.68.0/22　匹配
D 和 11111111 11111111 11111111 10000000 逐位相“与”= 206.0.71.128/25 匹配

不难看出，现在同一个 IP 地址 D 可以在路由表中找到两个目的网络（大学和四系）和

34.ICMP报文的种类有两种：**ICMP**差错报告报文和**ICMP**询问报文。

ICMP的重要应用：PING、traceroute 。
分组网间探测PING：作用：用来测试两台主机之间的连通性。PING使用了ICMP 回送请求与回送回答报文。应用：PING是应用层直接使用网络层ICMP的一个例子。它没有通过运输层的TCP或UDP。
traceroute (这是UNIX操作系统中名字)：作用：用来跟踪一个分组从源点到终点的路径。在Windows操作系统中这个命令是tracert。

35、路由选择协议



在目前的互联网中，一个大的 ISP 就是一个自治系统。这样，互联网就把路由选择协议划分为两大类，即：

(1) **内部网关协议** IGP (Interior Gateway Protocol)　即在一个自治系统内部使用的路由选择协议，而这与在互联网中的其他自治系统选用什么路由选择协议无关。目前这类路由选择协议使用得最多，如 RIP 和 OSPF 协议。

(2) **外部网关协议** EGP (External Gateway Protocol)　若源主机和目的主机处在不同的自治系统中（这两个自治系统可能使用不同的内部网关协议），当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。这样的协议就是外部网关协议 EGP。目前使用最多的外部网关协议是 BGP 的版本 4（BGP-4）。

自治系统之间的路由选择也叫做**域间路由选择**(interdomain routing)，而在自治系统内部

互联网把路由选择协议分为：内部网关协议IGP、外部网关协议EGP
内部网关协议IGP：如RIP和OSPF协议。RIP基于距离向量的协议，特点：使用于小型的网络。只能包含15个路由器，当距离为16的时候不可达。不能在两个网络之间有多条路径，它没有负载均衡；好消息传播的快，坏消息传播的慢。实现简单、开销较小。OSPF对比来记。
OSPF：书P159。最主要的特征就是使用分布式链路状态协议。(向本自治系统中所有路由器发送信息。这里使用的方法是洪泛法(flooding)，这就是
路由器通过所有输出端口向所有相邻的路由器发送信息；发送的信息就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；只有当链路状态发生变化时，路由器才向所有路由器用洪泛法发送此信息。
外部网关协议EGP：用的最多的是BGP的版本4。

36.距离向量算法。书**P155**，要会计算。

2. 距离向量算法

对**每一个相邻路由器**发送过来的 RIP 报文，进行以下步骤：

(1) 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，并把所有的“距离”字段的值加 1（见后面的解释 1）。每一个项目都有三个关键数据，即：到目的网络 N，距离是 d，下一跳路由器是 X。

(2) 对修改后的 RIP 报文中的每一个项目，进行以下步骤：

若原来的路由表中没有目的网络 N，则把该项目添加到路由表中（见解释 2）。

否则（即在路由表中有目的网络 N，这时就再查看下一跳路由器地址）

若下一跳路由器地址是 X，则把收到的项目替换原路由表中的项目（见解释 3）。

否则（即这个项目是：到目的网络 N，但下一跳路由器不是 X）

若收到的项目中的距离 d 小于路由表中的距离，则进行更新（见解释 4），

否则什么也不做。（见解释 5）

(3) 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的路由器，即把距离置为 16（距离为 16 表示不可达）。

(4) 返回。

上面给出的距离向量算法的基础就是 Bellman-Ford 算法（或 Ford-Fulkerson 算法）。这种算法的要点是这样的：

设 X 是结点 A 到 B 的最短路径上的一个结点。若把路径 A→B 拆成两段路径 A→X 和 X→B，则每一段路径 A→X 和 X→B 也都分别是结点 A 到 X 和结点 X 到 B 的最短路径。

下面是对上述距离向量算法的五点解释。

解释 1：这样做是为了便于进行本路由表的更新。假设从位于地址 X 的**相邻**路由器发来的 RIP 报文的某一个项目是：“Net2, 3, Y”，意思是“我经过路由器 Y 到网络 Net2 的距离是 3”，那么本路由器就可推断出：“我经过 X 到网络 Net2 的距离应为 3 + 1 = 4”。于是，本路由进行比较时使用（只有比较后才能知道是否需要更新）。读者可注意到，收到的项目中的 Y 对本路由器是没有用的，因为 Y 不是本路由器的下一跳路由器地址。

解释 2：表明这是新的目的网络，应当加入到路由表中。例如，本路由表中没有到目的网络 Net2 的路由，那么在路由表中就要加入新的项目“Net2, 4, X”。

解释 3：为什么要替换呢？因为这是最新的消息，要以最新的消息为准。到目的网络的距离有可能增大或减小，但也可能没有改变。例如，不管原来路由表中的项目是“Net2, 3, X”还是“Net2, 5, X”，都要更新为现在的“Net2, 4, X”。

解释 4：例如，若路由表中已有项目“Net2, 5, P”，就要更新为“Net2, 4, X”。因为到网络 Net2 的距离原来是 5，现在减到 4，更短了。

解释 5：若距离更大了，显然不应更新。若距离不变，更新后得不到好处，因此也不更新。

【例 4-5】已知路由器 R_6 有表 4-9(a)所示的路由表。现在收到相邻路由器 R_4 发来的路

表 4-9(a)　路由器 R_6 的路由表

目的网络	距离	下一跳路由器
Net2	3	R_4
Net3	4	R_5
...	...	...

表 4-9(b)　R_4 发来的路由更新信息

目的网络	距离	下一跳路由器
Net1	3	R_1
Net2	4	R_2
Net3	1	直接交付

【解】 如同路由器一样，我们不需要知道该网络的拓扑。

先把表 4-9(b)中的距离都加 1，并把下一跳路由器都改为 R_4。得出表 4-9(c)。

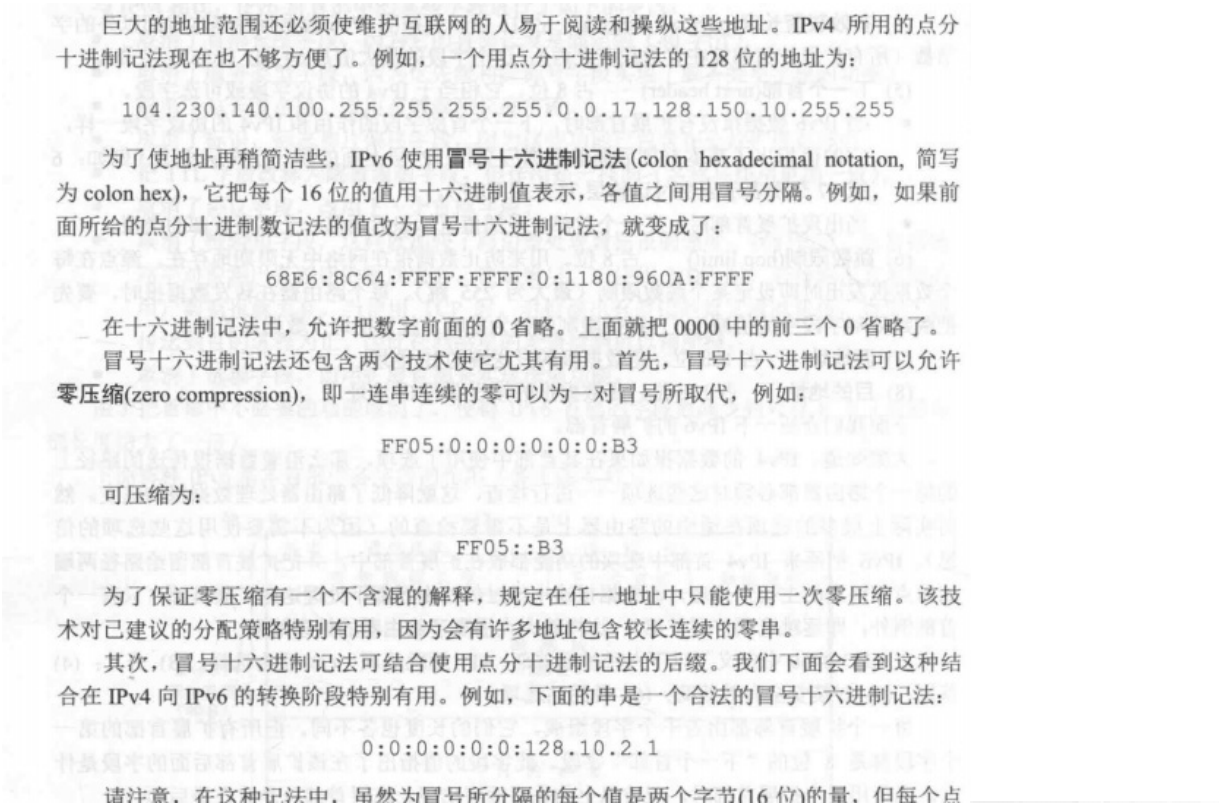
表 4-9(c)　修改后的表 4-9(b)

目的网络	距离	下一跳路由器
Net1	4	R_4
Net2	5	R_4
Net3	2	R_4

把这个表的每一行和表 4-9(a)进行比较

37.IPV6 书**P171**、写法**P174**

IPV6：格式：冒号16进制记法。PV6地址由128位组成，使用8个16位段来表示，每个16位段使用十六进制数字表示即每4个十六进制为一组，之间使用英文冒号:分开
格式为：x☒x☒x☒x:x x代表4个十六进制位，举例：2035:0001:2BC5:0000:0000:087C:0000:000A。
目的地址可以是：单播、多播放、任播。
要会：进行缩写。反过来能进行还原。



巨大的地址范围还必须使维护互联网的人易于阅读和操纵这些地址。IPv4 所用的点分十进制记法现在也不够方便了。例如，一个用点分十进制记法的 128 位的地址为：

104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255

为了使地址再稍简洁些，IPv6 使用**冒号十六进制记法**(colon hexadecimal notation，简写为 colon hex)，它把每个 16 位的值用十六进制值表示，各值之间用冒号分隔。例如，如果前面所给的点分十进制数记法的值改为冒号十六进制记法，就变成了：

68E6:8C64:FFFF:FFFF:0:1180:960A:FFFF

在十六进制记法中，允许把数字前面的 0 省略。上面就把 0000 中的前三个 0 省略了。

冒号十六进制记法还包含两个技术使它尤其有用。首先，冒号十六进制记法可以允许**零压缩**(zero compression)，即一连串连续的零可以为一对冒号所取代，例如：

FF05:0:0:0:0:0:0:B3

可压缩为：

FF05::B3

为了保证零压缩有一个不含混的解释，规定在任一地址中只能使用一次零压缩。该技术对已建议的分配策略特别有用，因为会有许多地址包含较长连续的零串。

其次，冒号十六进制记法可结合使用点分十进制记法的后缀。我们下面会看到这种结合在 IPv4 向 IPv6 的转换阶段特别有用。例如，下面的串是一个合法的冒号十六进制记法：

0:0:0:0:0:0:128.10.2.1

请注意，在这种记法中，虽然为冒号所分隔的每个值是两个字节(16 位)的量，但每个点

IPV4
点分十进制记法。IPv4使用32位（4字节）地址，因此地址空间中只有4,294,967,296（2^32） 个地址。
IPv4地址可被写作任何表示一个32位整数值的形式，但为了方便人类阅读和分析，它通常被写作点分十进制的形式，即四个字节被分开用十进制写出，中间用点分隔。
所以，通常IPv4地址的地址格式为nnn.nnn.nnn.nnn，其中 0<=nnn<=255，而每个 n 都是十进制数。可省略前导零。
要会：能够判断出是不是正确的（多少位、最大值、最大值、是否可划分）

38、从**IPv4**向**IPv6**过渡策略：双协议栈、隧道技术。

39、虚拟专用网**VPN**

三个专用地址块：（需要记下来）
10.0.0.0到10.255.255.255 (或记为 10.0.0.0/8， 它又称为24位块)
172.16.0.0到172.31.255.255 (或记为172.16.0.0/12，它又称为20位块)
192.168.0.0到192.168.255.255(或记为192.168.0.0/16， 它又称为16位块)
给出一个地址，要判断是否是专用地址。
网络地址转换NAT
要理解转换的过程。
要通过NAT路由器把专有IP转换为全球唯一IP才能够进行上网。
原IP地址需要进行转换。
基于端口号的NAPT=IP地址+运输层的端口号。
使用端口号的NAT也叫做网络地址与端口号转换NAPT，而不使用端口号的NAT就叫做传统的NAT。

要会做 4-10、4-20、4-21、4-25、4-26、4-32、4-33、4-37、4-65

4-10试辨认以下IP地址的网络类别:
(1) 128.36.199.3
(2) 21.12.240.17
(3) 183.194.76.253
(4) 192.12.69.248
(5) 89.3.0.1
(6) 200.3.6.2
4-20
4-21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，试给每一个地点分配
一个子网号码，并算出每个地点主机号码的最小值和最大值。
4-25以下有4个子网掩码，哪些是不推荐使用的?为什么?
(1) 176.0.0.0 不可 (2) 96.0.0.0 (3) 127.192.0.0 (4) 255.128.0.0 可 前七位网络位，后面主机位
解析：子网掩码特点：连续的1或连续的0（二进制）
4-26有如下的4个/24地址块，试进行最大可能的聚合。
212.56.132.0/24
212.56.133.0/24
212.56.134.0/24
212.56.135.0/24
4-32以 下的地址前缀中的哪一个地址 与2.52.90.140匹配?请说明理由。
(1)0/4; (2)32/4; (3) 4/6; (4) 80/4。
4-33下面的前缀中的哪一个和地址152.7.77.159及152.31.47.252都匹配?请说明理由。
(1) 152.40/13; (2) 153.40/9; (3)152.64/12; (4) 152.0/11。
4-37某单位分配到一个地址块136.23.12.64/26. 现在需要进一步划分为4个一样大的子网。试问:
(1)每个子网的网络前缀有多长?
(2)每一个子网中有多少个地址? 出崇向海味5实群市西基业胜》1民不 TH0
(3)每一个子网的地址块是什么?
(4)每一个子网可分配给主机使用的最小地址和最大地址是什么?
4-65 试把以下的零压缩的IPv6地址写成原来的形式:
(1) 0::0
(2) 0:AA::0
(3) 0⌧:3
(4) 123:1:2

39、两台主机进行通信就是两台主机中的应用进程互相通信。

40、从运输层的角度看，通信的真正端点并不是主机而是主机中的进程也就是说，端到端的通信是应用进程之间的通信。

41、运输层有一个很重要的功能一复用和分用。

复用：是指在发送方不同的应用进程都可以使用同一个运输层协议传送数据(当然需要加上适当的首部)。
分用：是指接收方的运输层在剥去报文的首部后能够把这些数据正确交付目的应用进程。

42、根据应用程序的不同需求，运输层需要有两种不同的运输协议，即面向连接的**TCP**和无连接的**UDP**。

他们之间的特点和不同要知道。TCP和UDP的格式等。TCP和UDP需要重点复习。书P208往后
UDP特点：无连接；不保证可靠交付；面向报文的；没有拥塞控制；支持一对一、-对多、多对一和多对多的交互通信；首部开销小。
TCP特点：面向连接的传输层协议；提供可靠交付服务；提供全双工通信；面向字节流；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。

43、**TCP/IP**的运输层用一个**16**位端口号来标志一个端口。

44、端口号分类

服务器端使用的端口号：又分为两类，最重要的一类叫做熟知端口号或系统端口号，数值为0~1023。另一类叫做登记端口号，数值为1024- 49151。这类端口号是为没有熟知端口号的应用程序使用的。使用这类端口号必须在IANA按照规定的手续登记，以防止重复。
客户端使用的端口号：49152- -65535。由于这类端口号仅在客户进程运行时才动态选择，因此又叫做短暂端口号。
问俩：服务器、客户端
三类：熟知端口号、登记、短暂。

45、流量控制和拥塞控制（重点）

为什么产生流量控制：
一般说来，我们总是希望数据传输得更快一些。但如果发送方把数据发送得过快，接收方就可能来不及接收，这就会造成数据的丢失。
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。
为什么产生拥塞？
在计算机网络中的链路容量(即带宽)、交换结点中的缓存和处理机等，都是网络的资源。在某段时间，若对网络中某一资源的需求超过了该资源所能提供的可用部分，网络的性能就要变坏。这种情况就叫做拥塞。
拥塞控制：
所谓拥塞控制就是防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。拥塞控制所要做的都有一个前提，就是网络能够承受现有的网络负荷。
TCP拥塞控制的算法：
慢开始、拥塞避免、快重传、快恢复。
什么时候执行这些算法：书P232。
什么时候 收到三个重复的确认？怎么办？

46、TCP是面向连接的协议。运输连接是用来传送**TCP**报文的。运输连接就有三个阶段，即**:**连接建立、数据传送和连接释放。运输连接的管理就是使运输连接的建立和释放都能正常地进行。

书P238 TCP的连接建立：三报文握手，TCP的连接释放：四报文握手（四次挥手），FIN等。（要知道使用了哪些字段，字段含义，值怎么设置，序号等含义）

47、应用层：域名系统**DNS**（作用主机名转换为**IP**地址）、域名系统采用层次的树状结构。

原先的顶级域名共分为三大类
国家顶级域名nTLD:如: cn表示中国，us 表示美国，uk表示英国，等等P。国家顶级域名又常记为ccTLD 。
通用顶级域名gTLD。最先确定的通用顶级域名有7个，即:com (公司企业)，net (网络服务机构)，org (非营利性组织)，int (国际组织)，edu(美国专用的教育机构)，gov (美国的政府部门)，mil 表示(美国的军事部门)。
基础结构域名:这种顶级域名只有一个，即arpa,用于反向域名解析，因此又称为反向域名。

48、FTP协议（文件传送协议）

工作原理：书P261。
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。
使用的端口号：21。

49、万维网**wWW**并非某种特殊的计算机网络。万维网是一个大规模的、联机式的信息储藏所，英文简称为**Web**。

50、HTTP超文本传输协议，端口号**80**。

51、URL

统一资源定位符URL是用来表示从互联网上得到的资源位置和访问这些资源的方法。
URL给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。
互联网上的所有资源，都有一个唯一确定的URL。
URL的一般形式由以下四个部分组成:<协议>://<主机>:<端口>/<路径> （端口、路径可以省略）

52、超文本标记语言**HTML**、简单邮件传送协议**SMTP**也属于应用层。

53、动态主机配置协议**DHCP**

作用：用来获取IP地址。（自动）

54、简单网络管理协议**SNMP**

要知道是干什么的。

55、SNMP的协议数据单元和报文

实际上，SNMP的操作只有两种基本的管理功能，即:
(1)“读”操作，用Get报文来检测各被管对象的状况;
(2)“写”操作，用Set报文来改变各被管对象的状况。
.第七章、第八章作为了解（就是不考？）