**第1章 概述**

**1-02 试简述分组交换的要点。**

答:在分组交换网络中，采用存储转发方式工作，数据以短的分组形式传送。如果一个源站有一个长的报文要发送，该报文就会被分割成一系列的分组。每个分组包含用户数据的一部分加上一些控制信息。控制信息至少要包括网络为了把分组送到目的地做路由选择所需要的信息。在路径上的每个结点，分组被接收，短时间存储，然后传递给下一结点。  
分组交换网的主要优点:①高效。②灵活。③迅速。④可靠。  
缺点:分组在节点转发时因排队而造成一定的延时;分组必须携带一些控制信息而产生额外开销;

**1-03 试从多个方面比较电路交换、报文交换和分组交换的主要优缺点。**

（1）电路交换：端对端通信质量因约定了通信资源获得可靠保障，对连续传送大量数据效率高。  
（2）报文交换：无须预约传输带宽，动态逐段利用传输带宽对突发式数据通信效率高，通信迅速。  
（3）分组交换：具有报文交换之高效、迅速的要点，且各分组小，路由灵活，网络生存性能好。

答: (1) 电路交换电路交换就是计算机终端之间通信时，一方发起呼叫，独占一条物理线路。当交换机完成接续，对方收到发起端的信号，双方即可进行通信。在整个通信过程中双方一直占用该电路。它的特点是实时性强，时延小，交换设备成本较低。但同时也带来线路利用率低，电路接续时间长，通信效率低，不同类型终端用户之间不能通信等缺点。电路交换比较适用于信息量大、长报文，经常使用的固定用户之间的通信。  
(2)报文交换将用户的报文存储在交换机的存储器中。当所需要的输出电路空闲时，再将该报文发向接收交换机或终端，它以“存储转发”方式在网内传输数据。报文交换的优点是中继电路利用率高，可以多个用户同时在一条线路上传送，可实现不同速率、不同规程的终端间互通。但它的缺点也是显而易见的。以报文为单位进行存储转发，网络传输时延大，且占用大量的交换机内存和外存，不能满足对实时性要求高的用户。报文交换适用于传输的报文较短、实时性要求较低的网络用户之间的通信，如公用电报网。  
(3)分组交换实质上是在“存储转发”基础上发展起来的。它兼有电路交换和报文交换的优点。分组交换在线路上采用动态复用技术传送按一定长度分割为许多小段的数据一分组。 每个分组标识后，在一条物理线路上采用动态复用的技术，同时传送多个数据分组。把 来自用户发端的数据智存在交换机的存储器内，接 着在网内转发。到达接收端，再去掉分组头将各数据字段按顺序重新装配成完整的报文。分组交换比电路交换的电路利用率高，比报文交换的传输时延小，交互性好。

**1-08 计算机网络都有哪些类别？各种类别的网络都有哪些特点？**

答:按网络的作用范围划分:  
(1)广域网WAN,作用范围通常为几十到几千公里，也称为远程网，是Internet的核心部分。  
(2)城域网MAN,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公里。  
(3)局域网LAN,作用范围局限在较小的范围(如1公里左右)。  
(4)个人区域网PAN,也称无线个人区域网，作用范围大约在10m左右。  
按网络的使用者划分:  
(1)公用网:面向公共营运、按规定缴纳费用的人都可使用的网络。  
(2)专用网:面向特定机构、不向本单位以外的人提供服务的网络。

**1-13 客户·服务器方式与P2P 对等通信方式的主要区别是什么？有没有相同的地方？**

客户-服务器方式是最常用的传统方式，客户是服务请求方，服务器是服务提供方，可同时处理多个远地或本地客户的请求。  
对等通信是两台主机在通信时并不区分哪个是服务器请求方还是服务提供方，只要两台主机都运行了对等连接软件，就可以平等的，对等连接通信。

相同的地方就是都能得到想要的服务，只不过前者可能速度较慢。

**1-14 计算机网络有哪些常用的性能指标？**

速率、带宽、吞吐量、时延、时延带宽积、往返时间RTT、利用率

1、速率  
　　计算机发送出的信号都是数字形式的。比特(bit)是计算机中的数据量的单位，也是信息论中使用的信息量单位。英文字bit来源binary digit(一个二进制数字)，因此一个比特就是二进制数字中的一个1或0。网络技术中的速率指的是链接在计算机网络上的主机在数字信道上传送数据的速率，也称为数据率(data rate)或者比特率(bit rate)。速率的单位是b/s(比特每秒)或者bit/s，也可以写为bps，即bit per second。当数据率较高时，可以使用kb/s(k=103=千)、Mb/s(M=106=兆)、Gb/s(G=109=吉)或者Tb/s(T=1012=太)。现在一般常用更简单并不是很严格的记法来描述网络的速率，如100M以太网，而省略了b/s，意思为数据率为100Mb/s的以太网。这里的数据率通常指额定速率。  
2、带宽  
　　带宽本上包含两种含义：  
　　(1)带宽本来指某个信号具有的频带宽度。信号的带宽是指该信号所包含的各种不同频率成分所占据的频率范围。例如，在传统的通信线路上传送的电话信号的标准带宽是3.1kHz(从300Hz到3.1kHz，即声音的主要成分的频率范围)。这种意义的带宽的单位是赫兹。在以前的通信的主干线路传送的是模拟信号(即连续变化的信号)。因此，表示通信线路允许通过的信号频带范围即为线路的带宽。  
　　(2)在计算机网络中，贷款用来表示网络的通信线路所能传送数据的能力，因此网络带宽表示在单位时间内从网络的某一点到另一点所能通过的“最高数据量“。这种意义的带宽的单位是”比特每秒“，即为b/s。子这种单位的前面也通常加上千(k)、兆(M)、吉(G)、太(T)这样的倍数。  
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。吞吐量进场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。显然，吞吐量受到网络的带宽或网络的额定速率的限制。例如，对于一个100Mb/s的以太网，其额定速率为100Mb/s，那么这个数值也是该以太网的吞吐量的绝对上限值。因此，对100Mb/s的以太网，其典型的吞吐量可能只有70Mb/s。  
4、时延  
　　时延指数据(一个报文或者分组)从网络(或链路)的一端传送到另一端所需的时间。时延是一个非常重要的性能指标，也可以称为延迟或者迟延。  
　　网络中的时延由以下几部分组成：  
　　(1)发送时延 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时间。发送时延也可以称为传输时延。发送的时延=数据帧长度(b)/发送速率(b/s)。  
　　对于一定的网络，发送时延并非固定不变，而是与发送的帧长成正比，与发送数率成反比。  
　　(2)传播时延 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数率(m/s)  
　　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。  
　　(3)处理时延 主机或路由器在收到分组时需要花费一定的时间处理，分析分组首部、从分组中提取数据部分、进行差错检验、查到适当路由等，这就产生了处理时延。  
　　(4)排队时延 分组在经过网络传输时，要经过许多的路由器。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。这就产生了排队延时。排队延时通常取决于网络当时的通信量。  
　　这样数据在网络中尽力的总延时就是  
　　总延时 = 发送延时 + 传播延时 + 处理延时 + 排队延时  
　　对于高速网络链路，提高的仅仅是数据的发送数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与数据的发送速率并无关系。提高的数据的发送速率只是减小了数据的发送时延。  
5、时延带宽积  
　　把以上两个网络性能的两个度量，传播时延和带宽相乘，就等到另外一个度量：传播时延带宽积，即  
　　时延带宽积 = 传播时延 × 带宽  
　　例如，传播时延为20ms，带宽为10Mb/s，则时延带宽积 = 20 × 10 × 10^3 /1000 = 2 × 10^5 bit。这就表示，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bit都在链路上向前移动。  
6、往返时间RTT  
　　在计算机网络中，往返时间RTT也是一个重要的性能指标，表示从发送方发送数据开始，到发送方收到来自接收方的确认，总共经历的时间。对于上面提到的例子，往返时间RTT就是40ms，而往返时间和带宽的乘积是4×10^5(bit)。  
　　显然，往返时间与所发送的分组长度有关。发送很长的数据块的往返时间，应当比发送很短的数据块往返时间要多些。  
　　往返时间带宽积的意义就是当发送方连续发送数据时，即能够及时收到对方的确认，但已经将许多比特发送到链路上了。对于上述例子，假定数据的接收方及时发现了差错，并告知发送发，使发送方立即停止发送，但也已经发送了40万个比特了。  
7、利用率  
　　利用率有信道利用率和网络利用率。信道利用率指出某信道有百分之几的时间是被利用的。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。  
　　如果D0表示网络空闲时的时延，D表示当前网络时延，可以用简单公式(D=D0/(1-U)来表示D，D0和利用率U之间的关系。U数值在0和1之间。当网络的利用率接近最大值1时，网络的时延就趋近于无穷大。

**1-21 协议与服务有何区别？有何关系？**

协议是水平的，服务是垂直的。  
协议是“水平的”，即协议是控制对等实体之间的通信的规则。  
服务是“垂直的”，即服务是由下层向上层通过层间接口提供的。  
协议与服务的关系  
在协议的控制下，上层对下层进行调用，下层对上层进行服务，上下层间用交换原语交换信息。同层两个实体间有时有连接。

**1-22 网络协议的三个要素是什么？各有什么含义？**

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。由以下三个要素组成：  
（1）语法：即数据与控制信息的结构或格式。  
（2）语义：即需要发出何种控制信息，完成何种动作以及做出何种响应。  
（3）同步：即事件实现顺序的详细说明。

**1-23 为什么一个网络协议必须把各种不利的情况都考虑到？**

因为网络协议如果不全面考虑不利情况，当情况发生变化时，协议就会保持理想状况，一直等下去！就如同两个朋友在电话中约会好，下午3点在公园见面，并且约定不见不撒。这个协议就是很不科学的，因为任何一方如果有耽搁了而来不了，就无法通知对方，而另一方就必须一直等下去！所以看一个计算机网络是否正确，不能只看在正常情况下是否正确，而且还必须非常仔细的检查协议能否应付各种异常情况。

**1-24 试述具有五层协议的网络体系结构的要点，包括各层的主要功能。**

答:综合OSI和TCP/IP的优点。采用一种原理体系结构。各层的主要功能：  
物理层：物理层的任务就是透明地传送比特流。(注意:传递信息的物理媒体，如双绞线、同轴电缆、光缆等，是在物理层的下面，当做第0层。)物理层还要确定连接电缆插头的定义及连按法。  
数据链路层：数据链路层的任务是在两个相邻结点间的线路上无差错地传送以帧(frame)为单位的数据。每一帧包括数据和必要的控制信息。  
网络层：网络层的任务就是要这择合适的路由。使发送站的运输层所传下来的分组能够正确无误地按照地址找到目的站，并交付给目的站的运输层。  
运输层：运输层的任务是向上一层的进行通信的两个进程之间提供-个可靠的端到端服务，使它们看不见运输层以下的数据通信的细节。  
应用层：应用层直接为用户的应用进程提供服务。

**第2章 物理层**

**2-01 物理层要解决哪些问题？物理层的主要特点是什么？**

(1) 物理层要解决的主要问题:  
①物理层要尽可能屏蔽掉物理设备、传输媒体和通信手段的不同，使上面的数据链路层感觉不到这些差异的存在，而专注于完成本曾的协议与服务。  
②给其服务用户(数据链路层)在一条物理的传输媒体上传送和接收比特流(一般为串行按顺序传输的比特流)的能力。为此，物理层应解决物理连接的建立、维持和释放问题。  
③.在两个相邻系统之间唯一地标识数据电路。  
(2) 物理层的主要特点:  
①.由于在OSI之前，许多物理规程或协议已经制定出来了，而且在数据通信领域中，这些物理规程已被许多商品化的设备锁采用。加之，物理层协议涉及的范围广泛，所以至今没有按OSI的抽象模型制定一套心的物理层 协议，而是沿用已存在的物理规程，将物理层确定为描述与传输媒体接口的机械、电气、功能和规程特性。  
②由于物理连接的方式很多，传输媒体的种类也很多，因此，具体的物理协议相当复杂。

**2-05 物理层的接口有哪几个方面的特性？各包含些什么内容？**

1、机械特性， 指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等。  
2、电气特性， 指明在接口电缆的各条线上出现的电压的范围。  
物理层的电气特性规定了在物理连接上传输二进制位流时线路上信号电压高低、阻抗匹配情况、传输速率和距离的限制等。  
3、功能特性，规定了接口信号的来源、作用以及其他信号之间的关系。即物理接口上各条信号线的功能分配和确切定义。物理接口信号般分为数据线、控制线、定时线和地线。  
4、规程特性， 定义了再信号线上进行二进制比特流传输的一组操作过程，包括各信号线的工作顺序和时序，使得比特流传输得以完成。

**2-10 常用的传输媒体有哪几种？各有何特点？**

1.双绞线  
双绞线分屏蔽双绞线和无屏蔽双绞线。由两根相互绝缘的导线组成。可以传输模拟信号，也可以传输数字信号，有效带宽达250kHz，通常距离一般为几道十几公里。导线越粗其通信距离越远。在数字传输时，若传输速率为每秒几兆比特，则传输距离可达几公里。一般用作电话线传输声音信号。虽然双绞线容易受到外部高频电磁波的干扰，误码率高，但因为其价格便宜，且安装方便，既适于点到点连接，又可用于多点连接，故仍被广泛应用。  
2.同轴电缆  
同轴电缆分基带同轴电缆和宽带同轴电缆，其结构是在一个包有绝缘的实心导线外，再套上一层外面也有一层绝缘的空心圆形导线。由于其高带宽（高达300~400Hz）、低误码率、性能价格比高，所以用作LAN中。同轴电缆的最大传输距离随电缆型号和传输信号的不同而不同，由于易受低频干扰，在使用时多将信号调制在高频载波上。  
3.光导纤维  
光导纤维以光纤维载体，利用光的全反向原理传播光信号。其优点是直径小、质量轻：传播频带款、通信容量大：抗雷电和电磁干扰性能好，五串音干扰、保密性好、误码率低。但光电接口的价格较昂贵。光纤被广泛用于电信系统铺设主干线。  
4.无线电微波通信  
无线电微波通信分为地面微波接力通信和卫星通信。其主要优点是频率高、频带范围宽、通信信道的容量大；信号所受工业干扰较小、传播质量高、通信比较稳定；不受地理环境的影响，建设投资少、见效快。缺点是地面微波接力通信在空间是直线传播，传输距离受到限制，一般只有50km，隐蔽性和保密性较差；卫星通信虽然通信距离远且通信费用与通信距离无关，但传播时延较大，技术较复杂，价格较贵。

**2-13 为什么要使用信道复用技术？常用的信道复用技术有哪些？**

为了通过共享信道、最大限度提高信道利用率。  
常用的信道复用技术：频分、时分、码分、波分。

**第3章 数据链路层**

**3-02 数据链路层中的链路控制包括哪些功能？试讨论数据链路层做成可靠的链路层有哪些优点和缺点。**

链路管理帧定界流量控制差错控制将数据和控制信息区分开透明传输寻址可靠的链路层的优点和缺点取决于所应用的环境：对于干扰严重的信道，可靠的链路层可以将重传范围约束在局部链路，防止全网络的传输效率受损；对于优质信道，采用可靠的链路层会增大资源开销，影响传输效率。

**3-03 网络适配器的作用是什么？网络适配器工作在哪一层？**

适配器（即网卡）来实现数据链路层和物理层这两层的协议的硬件和软件  
网络适配器工作在TCP/IP协议中的网络接口层（OSI中的数据链路层和物理层）

**3-04 数据链路层的三个基本问题（封装成帧、透明传输和差错检测）为什么都必须加以解决？**

答：封装成帧是分组交换的必然要求；透明传输是避免二进制比特流中出现与帧定界符号相同的模式，使节点错误识别帧；差错检测是为了避免接收到错误信息和防止信道中出现的无效数据帧浪费后续路由上的传输和处理资源。

**3-05 如果在数据链路层不进行封装成帧，会发生什么问题？**

答：在数据传输过程中的传输网中的结点及接收方将无法区分分组，也将无法确定分组的控制域和数据域，也不能实现差错控制。

**3-13 局域网的主要特点是什么？为什么局域网采用广播通信方式而广域网不采用呢？**

答：局域网LAN是指在较小的地理范围内，将有限的通信设备互联起来的计算机通信网络，从功能的角度来看，局域网具有以下几个特点：  
（1）共享传输信道，在局域网中，多个系统连接到一个共享的通信媒体上。（2）地理范围有限，用户个数有限。通常局域网仅为一个单位服务，只在一个相对独立的局部范围内连网，如一座楼或集中的建筑群内，一般来说，局域网的覆盖范围越位10m~10km内或更大一些。  
（3）一般为某个单位私有。  
从网络的体系结构和传输检测来看，局域网也有自己的特点：  
（1）低层协议简单  
（2）不单独设立网络层，局域网的体系结构仅相当于相当与OSI/RM的最低两层  
（3）采用两种媒体访问控制技术，由于采用共享广播信道，而信道又可用不同的传输媒体，所以局域网面对的问题是多源，多目的的连连管理，由此引发出多种媒体访问控制技术。  
在局域网中各站通常进行一对多访问，随机使用信道，共享通信媒体，采用广播通信方式是最合适的，且LAN中站点较少，带宽相对较大，也适宜于使用广播方式通信。在广域网中用户数较多，若采取广播通信，会造成广播风暴，使得整个网络无法使用。

**3-14 常用的局域网的网络拓扑有哪些种类？现在最流行的是哪种结构？为什么早期的以太网选择总线拓扑结构而不使用星形拓扑结构，但现在却改为使用星形拓扑结构？**

答：星形网，总线网，环形网，树形网 当时很可靠的星形拓扑结构较贵，人们都认为无源的总线结构更加可靠，但实践证明，连接有大量站点的总线式以太网很容易出现故障，而现在专用的ASIC芯片的使用可以讲星形结构的集线器做的非常可靠，因此现在的以太网一般都使用星形结构的拓扑。

**第4章 网络层**

**4-01 网络层向上提供的服务有哪两种？试比较其优缺点。**

答:网络层向上提供了数据报和虚电路两种服务，其优缺点的比较如下:  
(1)虚电路是面向连接的，提供的服务可以保证数据传输的可靠性和投递顺序的正确性;数据报是无连接的，只提供尽最大努力的交付，不能保证传输的可靠性和投递顺序的正确性。  
(2)网络采用数据报传输方式可大大简化网络层的结构:虚电路让电信网络负责保证可靠通信所采取的措施，使得电信网的结点交换机复杂而昂贵。但是相对而言，采用数据报时，由主机负责端到端的可靠性，包括差错处理和流量控制，因此主机的处理负担较大。  
(3)虚电路有连接建立和释放阶段，数据传输启动慢;数据报不用建立连接，数  
据传输启动快。  
(4)为了在交换结点进行存储转发，在使用数据报时，每个分组必须携带完整的  
地址信息。而在使用虚电路的情况下，每个分组不需要携带完整的目的地址，只需要有一个简单的虚电路号码标识，这就使得虚电路分组中的控制信息部分的比特数减少，从而减少了系统开销。  
(5)虚电路在连接建立的阶段确定数据传输的路由，属于同条虚电路的分组均  
按照同- 条路由进行转发:数据报对每个分组都独立的做路由选择。显然，在数据传输阶段，数据报的路由处理负担较大。但是在网络出现故障的情况下，所有通过故障结点的虚电路都不能工作，而数据报可以灵活的选择替代路由。

**4-02 网络互连有何实际意义？进行网络互连时，有哪些共同的问题需要解决？**

答: (1)单一的网络无法满足各种用户的多种需求，因此，把许多种不同类  
型的物理网络互相连接在一起， 可以实现更大范围内的通信。实际中使用的TCP/IP协议，定义了一种抽象的网络，隐藏了互连的各种不同物理网络的细节，使得互连后的网络像一个单一的大网络。  
(2)进行网络互连时，需要解决的共同的问题:不同的寻址方案、不同的最大分组的长度、不同的网络接入机制、不同的超时控制、不同的差错恢复方法、不同的状态报告方法、不同的路由选择技术、不同的用户接入控制、不同的服务(而向连接的服务和无连接的服务)不同的网络管理和控制方式等。

**4-03 作为中间设备，转发器、网桥、路由器和网关有何区别？**

答:它们工作在的层次不同，并且功能不同:  
转发器:物理层中继系统，在转发数据时不对传输媒体进行检测，只是对数据分组进行简单的转发(逐比特转发)因此只能连接 相同速率的网络.  
网桥:工作在数据链路层，网桥在转发数据前先对传输媒体进行检测，并且是把整个数据帧都收下之后再进行存储转发，具有过滤帧的功能，故能够连接不同、速率的网络。当中继系统是转发器或网桥时，股并不称之为网络互连， 因为这仅仅是把一个网络扩大了，而从网络层看仍然是一个网络。  
路由器:工作在网络层，具有存储转发功能，作用是在互连网中完成路由选择的功能。(由于历史的原因，有时把路由器称为网关)  
网关:网络层以上的中继系统，用网关连接两个互不兼容的系统需要在高层进行协议转换。(由于网关较复杂，用的较少)

**4-04 试简单说明下列协议的作用： IP, ARP, RARP 丰日ICMP 。**

答:IP:网际协议(互连网协议),用来使互连起来的网络能够相互通信。  
ARP:地址解析协议，用来把IP地址映射成物理地址。  
RARP:逆地址解析协议，使只知道自己硬件地址的主机能够知道其IP地址。  
ICMP:互连网控制报文协议，允许主机或路由器报告差错情况和提供有关是否有异常情况的报告。

**4-05 IP 地址分为几类？各如何表示？ IP 地址的主要特点是什么？**

答: IP地址共分为5类: A,B,C,D,E. A,B,C三类的网络号字段分别为1个，2个，3个字节;而网络号字段的最前面有1-3位的类别比特，其二进制数值分别为0.01, 110. A类，B类，C类地址的主机号字段分别为3, 2, 1个字节。D类地址用于多播;前4位包含二进制数值1110. E类地址保留为未来使用，前5位包含二进制数值11110.  
IP地址的特点:  
(1)是一种分等级的地址结构，每一个IP地址由网络号和主机号两部分组成。  
(2) IP地址实际上是标识个主机 (或路由器) 和一条链路的接口。当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的IP地址，而且其网络号必须是不相同的。  
(3)用转发器或网桥连接起来的若千个局域网仍为一个网络，这些局域网都具有相同的网络号。  
(4)在IP地址中，所有分配到网络号的网络，不论大小，都是平等的。

**4-07 试说明IP 地址与硬件地址的区别。为什么要使用这两种不同的地址？**

答:IP地址是主机在抽象的网络层中的地址，硬件地址是物理网络在数据链路层地址。IP地址是不能直接用来进行通信的，例如:在局域网中，若要将网络层中传输的数据报交给目的主机，还要传到链路层转变成MAC帧后发送到物理往里中。因此不管网络层使用的是什么协议，在实际网络的链路传输数据帧时，最终还是必须使用硬件地址。这就是说，我们需要使用两种不同的地址。

**4-11 IP 数据报中的首部检验和并不检验数据报中的数据。这样做的最大好处是什么？坏处是什么？**

答：好处：不检验数据部分会节省时间，从而转发分组更快；  
坏处：数据部分若有差错时不能及时发现。

**4-38 IGP 和EGP 这两类协议的主要区别是什么？**

IGP: 内部网关协议（Interior Gateway Protocol）  
内部网关协议（IGP）是一种专用于一个自治网络系统（比如：某个当地社区范围内的一个自治网络系统）中网关间交换数据流转通道信息的协议。网络IP协议或者其他的网络协议常常通过这些通道信息来决断怎样传送数据流。目前最常用的内部网关协议分别是：路由信息协议（RIP）和最短路径优先路由协议（OSPF）分级的链接状态路由协议（ISIS）。

EGP：外部网关协议（Exterior Gateway Protocol）  
外部网关协议（EGP）是一种在自治系统的相邻两个网关主机间交换路由信息的协议。 EGP 通常用于在因特网主机间交换路由表信息。它是一个轮询协议，利用 Hello 和 I-Heard-You 消息的转换，能让每个网关控制和接收网络可达性信息的速率，允许每个系统控制它自己的开销，同时发出命令请求更新响应。路由表包含一组已知路由器及这些路由器的可达地址以及路径开销，从而可以选择最佳路由。每个路由器每间隔 120 秒或 480 秒会访问其邻居一次，邻居通过发送完整的路由表以示响应，代表协议是边界网关协议（BGP）。

内部网关协议  
1GP是在一个自治 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。  
外部网关协议  
EGP是自治系统之间的路由选择协议，而这与自治系统内部选用什么路由选择协议无关。

**4-39 试简述RIP, OSPF 和BGP 路由选择协议的主要特点。**

| **主要特点** | **RIP** | **OSPF** | **BGP** |
| --- | --- | --- | --- |
| 网关协议 | 内部 | 内部 | 外部 |
| 路由表内容 | 目的网，下一站， 距离 | 目的网，下一站， 距离 | 目的网，下一站， 距离 |
| 最优通路依据 | 跳数 | 代价 | 多种策略 |
| 算法 | 距离向量 | 链路状态 | 路径向量 |
| 传送方式 | 运输层UDP | IP数据报 | 建立TCP连接 |
| 其他 | 简单、但效率低跳数16为不可达好消息传的快，坏消息传的慢 | 效率高、路由器频繁交换信息，难维持一致性 | 规模大、统一度量为可达性 |

**4-40 RIP使用UDP, OSPF 使用IP，而BGP 使用TCP 。这样做有何优点？为什么RIP 周期性地和邻站交换路由信息而BGP 却不这样做？**

RIP只和邻站交换信息，使用UDP无可靠保障，但开销小，可以满足RIP要求；  
OSPF使用可靠的洪泛法，直接使用IP，灵活、开销小；  
BGP需要交换整个路由表和更新信息，TCP提供可靠交付以减少带宽消耗；RIP使用不保证可靠交付的UDP，因此必须不断地（周期性地）和邻站交换信息才能使路由信息及时得到更新。但BGP使用保证可靠交付的TCP因此不需要这样做。

**4-44 什么是VPN? VPN 有什么特点和优缺点？ VPN 有几种类别？**

VPN的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络可以把它理解成是虚拟出来的企业内部专线。

VPN特点:  
(1)使用VPN可降低成本——通过公用网来建立VPN，就可以节省大量的通信费用，而不必投入大量的人力和物力去安装和维护WAN(广域网)设备和远程访问设备。  
(2)传输数据安全可靠——虚拟专用网产品均采用加密及身份验证等安全技术，保证连接用户的可靠性及传输数据的安全和保密性。  
(3)连接方便灵活——用户如果想与合作伙伴联网，如果没有虚拟专用网，双方的信息技术部门就必须协商如何在双方之间建立租用线路或帧中继线路，有了虚拟专用网之后，只需双方配置安全连接信息即可。  
(4)完全控制——虚拟专用网使用户可以利用ISP的设施和服务，同时又完全掌握着自己网络的控制权。用户只利用ISP提供的网络资源，对于其它的安全设置、网络管理变化可由自己管理。在企业内部也可以自己建立虚拟专用网。

优点:  
1)VPN能够让移动员工、远程员工、商务合作伙伴和其他人利用本地可用的高速宽带网连接（如DSL、有线电视或者WiFi网络）连接到企业网络。此外，高速宽带网连接提供一种成本效率高的连接远程办公室的方法。  
2)设计良好的宽带VPN是模块化的和可升级的。VPN能够让应用者使用一种很容易设置的互联网基础设施，让新的用户迅速和轻松地添加到这个网络。这种能力意味着企业不用增加额外的基础设施就可以提供大量的容量和应用。  
3)VPN能提供高水平的安全，使用高级的加密和身份识别协议保护数据避免受到窥探，阻止数据窃贼和其他非授权用户接触这种数据。  
4)完全控制，虚拟专用网使用户可以利用ISP的设施和服务，同时又完全掌握着自己网络的控制权。用户只利用ISP提供的网络资源，对于其它的安全设置、网络管理变化可由自己管理。在企业内部也可以自己建立虚拟专用网。  
缺点:  
1)企业不能直接控制基于互联网的VPN的可靠性和性能。机构必须依靠提供VPN的互联网服务提供商保证服务的运行。这个因素使企业与互联网服务提供商签署一个服务级协议非常重要，要签署一个保证各种性能指标的协议。  
2)企业创建和部署VPN线路并不容易。这种技术需要高水平地理解网络和安全问题，需要认真的规划和配置。因此，选择互联网服务提供商负责运行VPN的大多数事情是一个好主意。  
3)不同厂商的VPN产品和解决方案总是不兼容的，因为许多厂商不愿意或者不能遵守VPN技术标准。因此，混合使用不同厂商的产品可能会出现技术问题。另一方面，使用一家供应商的设备可能会提高成本。  
4)当使用无线设备时，VPN有安全风险。在接入点之间漫游特别容易出问题。当用户在接入点之间漫游的时候，任何使用高级加密技术的解决方案都可能被攻破。

答：按实用技术不同又分为以下类别  
　　pptp vpn ,l2tp vpn ,ipsec vpn, ssl vpn ,mpls vpn 等等

**4-45 什么是NAT? NAPT 有哪些特点？ NAT 的优点和缺点有哪些？**

NAT全称Network Address Translation即网络地址转换。  
NAPT全称Network Address and Port Translation即网络地址与端口号转换其特点是：  
(1)在路由器转发IP数据报时NAPT对IP地址和端口号都进行转换转换过程如下对于出专用网的数据把专用网内不同的源IP地址转换为同样的全球IP地址把源主机端口号转换为不同的新的端口号；对于入专用网的应答NAPT根据不同的目的端口号从NAPT转换表中找到正确的目的主机。  
(2)NAPT工作在网络层和传输层。  
NAT优点：(1)通过NAT专用网内部主机可使用专用地址与因特网上的主机通信。  
(2)通过NAT一个全球合法IP地址可被多台专用网内部主机分享使用节省全球IP地址资源。 NAT缺点：通信必须由专用网内的主机发起专用网内部的主机不能充当服务器。

**4-59 建议的1Pv6 协议没有首部检验和。这样做的优缺点是什么？**

优点：对首部的处理更简单。数据链路层已经将有差错的帧丢弃了，因此网络层可省去这一步骤；缺点：可能遇到数据链路层检测不出来的差错。

**4-60 在1Pv4 首部中有一个“协议”宇段，但在1Pv6 的固定首部中却没有。这是为什么？**

在IP数据报传送的路径上的所有路由器都不需要这一字段的信息。只有目的主机才需要协议字段。在IPv6使用“下一个首部”字段完成IPv4中的“协议”字段的功能。

**第5章 运输层**

**5-01 试说明运输层在协议栈中的地位和作用。运输层的通信和网络层的通信有什么重要的区别？为什么运输层是必不可少的？**

答:运输层在协议栈中的地位和作用:从通信和信息处理的角度看，运输层向它上面的应用层提供通信服务，它属于面向通信部分的最高层，同时也是用户功能中的最低层。当网络边缘的两个主机进行端到端的通信时，只有位于网络边缘的主机有运输层，而网络核心部分中的路由器在转发分组时都只用到下三层的功能。

运输层的通信和网络层的通信区别:  
运输层为应用进程之间提供端到端的逻辑通信，但网络层是为主机之间提供逻辑通信。  
从网络层来说，通信的两端是两个主机，P数据报的首部明确地标志了这两个主机的IP地址，但两个主机进行通信实际上就是两个主机中的应用进程互相通信。IP协议虽然能把分组送到目的主机，但这个分组还停留在主机的网络层而没有交付主机中的应用进程。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应用进程，也就是说，端到端的通信是应用进程之间的通信。因此，运输层是必不可少的。

**5-08 为什么说UDP 是面向报文的，而TCP 是面向字节流的？**

答:发送方UDP对应用程序交下来的报文，在添加首部后就向下交付IP层。UDP对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界。接收方UDP对IP层交上来的UDP用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。因此，UDP是面向报文的。  
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的无结构的字节流。TCP根据对方给出的窗口值和当前网络拥塞的程度来决定发送的一个报文段应包含多少个字节。如果应用进程传送的数据块太长，TCP就可以把它划分短一些再传送，如果应用进程一次只发来一个字节，TCP也可以等待积累足够多的字节再构成报文段传送出去。因此，TCP是面向字节流的。

**5-09 端口的作用是什么？为什么端口号要划分为三种？**

答:端口的作用是对TCP/IP体系的应用进程进行统一 的标志，使运行不同操作系统的计算机的应用进程能够互相通信。  
熟知端口，数值一般为0^ 1023.标记常规的服务进程;  
登记端口号，数值为1024 49151，标记没有熟知端口号的非常规的服务进程;  
短暂端口号， 数值为49152~65535， 标记客户进程，运行时才动态分配。

**5-10 试说明运输层中伪首部的作用。**

用于计算运输层数据报校验和。

**5-15 使用TCP 对实时话音数据的传输会有什么问题？使用UDP 在传送数据文件时会有什么问题？**

答: UDP不保证可靠交付，但UCP比TCP的开销要小很多。因此只要应用程序接受这样的服务质量就可以使用UDP。如果语音数据不是实时播放(边接收边播放)就可以使用TCP，因为TCP传输可靠。接收端用TCP讲话音数据接受完毕后，可以在以后的任何时间进行播放。但假定是实时传输，则必须使用UDP。

答: TCP是可靠传输协议，当实时语音数据传输出现差错时，TCP协议要对差错部分进行重传，而在实时话音通信中，我们宁可丢掉几个分组，也不愿意收到太迟到的分组，因此TCP不能实现实时语音数据的传输。若要对实时语音数据进行实时传输，则必须使用UDP协议。  
使用UDP传送数据文件时，如果出现了差错，UDP仅仅是少收了这个出错的报文段，并不通知发送方重传，这样就不能保证正确地传送数据。因此在传送数据文件时采用TCP来传送。

**5-23 主机A 向主机B 连续发送了两个TCP 报文段，其序号分别是70 和100 。试问：**

(1 ）第一个报文段携带了多少字节的数据？  
第一个报文段的数据序号是70到99，共30字节的数据。  
(2）主机B 收到第一个报文段后发回的确认中的确认号应当是多少？  
确认号应为100.  
(3）如果B 收到第二个报文段后发回的确认中的确认号是180，试问A 发送的第二个报文段中的数据有多少字节？  
80字节  
(4）如果A 发送的第一个报文段丢失了，但第二个报文段到达了B 。B 在第二个报文段到达后向A 发送确认。试问这个确认号应为多少？  
70

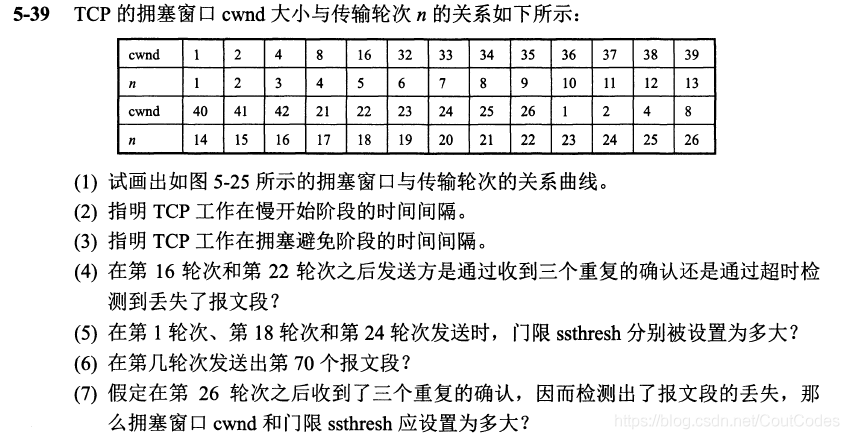
**5-29 在使用TCP 传送数据时，如果有一个确认报文段丢失了，也不一定会引起与该确认报文段对应的数据的重传。试说明理由。**

还未重传就收到了对更高序号的确认

**5-38 设TCP 的ssthresh 的初始值为8 （单位为报文段）。当拥塞窗口上升到12 时网络发生了超时， TCP 使用慢开始和拥塞避免。试分别求出第l 轮次到第15 轮次传输的各拥塞窗口大小。你能说明拥塞窗口每一次变化的原因吗？**

答:拥塞窗口大小及变化的原因:  
第1传输轮次，TCP执行慢开始算法，拥塞窗口cwnd是1;  
第2传输轮次，ssthresh 初始值为8，当前cwnd<8, TCP执行慢开始算法，拥塞窗口倍增是2:  
第3传输轮次，当前cwnd<8, TCP执行慢开始算法，拥塞窗口倍增是4;  
第4传输轮次，当前cwnd<8, TCP执行慢开始算法，拥塞窗口倍增是8:  
第5传输轮次，当前cwnd=8, TCP执行拥塞避免算法，拥塞窗口加1是9;  
第6传输轮次，8<当前cwnd<12, TCP执行拥塞避免算法，拥塞窗口加1是10;  
第7传输轮次，8<当前cwnd<12, TCP执行拥塞避免算法，拥塞窗口加1是1l;  
第8传输轮次，8<当前cwnd<12, TCP执行拥塞避免算法，拥塞窗口加1是12;  
第9传输轮次，当前cwnd=12,网络发生超时，执行乘法减小算法，新的ssthresh值为当前cwnd值的一半，即新的ssthresh值为6，TCP执行慢开始算法，拥塞窗口是1;  
第10传输轮次，当前cwnd<6, TCP执行慢开始算法，拥塞窗口倍增是2;  
第11传输轮次，当前cwnd<6, TCP执行慢开始算法，拥塞窗口倍增是4;  
第12传输轮次，当前cwnd<6, TCP 执行慢开始算法，拥塞窗口增加到当前的ssthresh值是6;  
剪13传输轮次，当前cwnd-6. TCP执行拥紧避免算法，拥来1口加1是2万  
第14传输轮次，6< 当前cwnd<12, TCP 执行拥来避免算法:拥来窗口1是8  
第15传输轮次，6<当前 cwnd<12, TCP 执行拥塞避免算法，拥塞窗口加1是9。

**5-39 TCP的拥塞窗口cwnd大小与传输轮次n的关系如下所示：**



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)拥寨窗口cwnd和门]限ssthresh应设置为8的一半，即4.

**5-45 解释为什么突然释放运输连接就可能会丢失用户数据，而使用TCP 的连接释放方法就可保证不丢失数据。**

答:当主机1和主机2之间连接建立后，主机1发送了一个TCP数据段并正确抵达主机2，接着主机1发送另一个TCP数据段，这次很不幸，主机2在收到第二个TCP数据段之前发出了释放连接请求，如果就这样突然释放连接，显然主机1发送的第二个TCP报文段会丢失。而使用TCP的连接释放方法，主机2发出了释放连接的请求，那么即使收到主机1的确认后，只会释放主机2到主机1方向的连接，即主机2不再向主机1发送数据，而仍然可接受主机1发来的数据，所以可保证不丢失数据。

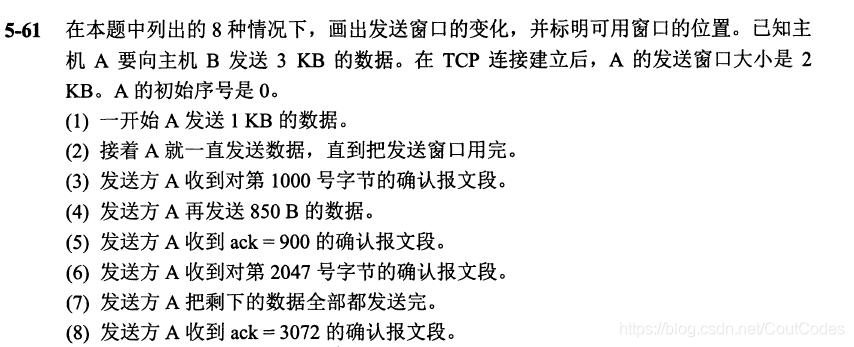
**5-46 试用具体例子说明为什么在运输连接建立时要使用三报文握手。说明如不这样做可能会出现什么情况。**

答:3次握手完成两个重要的功能，既要双方做好发送数据的准备工作(双方都知道彼此已准备好)，也要允许双方就初始序列号进行协商，这个序列号在握手过程中被发送和确认。假定B给A发送一个连接请求分组，A收到了这个分组，并  
发送了确认应答分组。按照两次握手的协定，A认为连接已经成功地建立了，可以开始发送数据分组。可是，B在A的应答分组在传输中被丢失的情况下，将不知道A是否已准备好↓不知道A建议什么样的序列号，B甚至怀疑A是否收到自己的连接请求分组，在这种情况下，B认为连接还未建立成功，将忽略A发来的任何数据分组，只等待连接确认应答分组。而A发出的分组超时后，重复发送同样的分组。这样就形成了死锁。

**5-52 UDP 和IP 的不可靠程度是否相同？请加以解释。**

UDP和IP的不可靠程度是不相同的，因为IP仅检验首部，而UDP检验整个数据报

**5-61 在本题中列出的8种情况下，画出发送窗口的变化，并标明可用窗口的位置。已知主在本要向主机B发送3KB的数据.在TCP连接建立后，A的发送窗口大小是2KB。A的初始序号是0.**



1.由tcp连接建立后，A的发送窗口大小是2KB，2KB=2\*1024=2048字节，故发送窗口：从0到第2047字节为止。后面的即为可用窗口。  
2.发送方A一直发送数据，直到把发送窗口用完。此时，整个窗口被用完，可用窗口大小为0。  
3.由发送方A收到对第1000号字节的确认报文段，表明A收到的确认报文段确认号ack=1001。发送窗口从第1001字节到第3048字节为止。可用窗口从第2048字节到第3048为止。可用窗口起始位置同上（2）  
4.由发送方A再发送850B的数据。2048+850=2898。故可用窗口从第2898字节到第3048字节为止。  
5.发送方收到ack=900的确认报文段。由900<1001，这是一个迟到的确认，不会对窗口产生影响，故窗口同上（4）  
6.发送方A收到对第2047号字节的确认报文段，同（3）故发送窗口从第2048字节到第4095字节为止。可用窗口从第2898字节到第3048字节为止。可用窗口起始位置同上（5）  
7.发送方A把剩下的数据全部都发送完，共3KB=3072字节，从0到3071字节。故可用窗口从第3072字节到第4095字节为止。  
8.由发送方A收到的ack=3072的确认报文段，即0到3071字节的数据均已收到，发送窗口从3072字节到5119字节。可用窗口从3072字节到5119字节，可用窗口起始位置同上（7）。整个发送窗口均为可用窗口。

**5-74 流量控制和拥塞控制的最主要的区别是什么？发送窗口的大小取决于流量控制还是拥塞控制？**

拥塞控制：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：网络能够承受现有的网络负荷。拥塞控制是一个全局性的过程，涉及到所有的主机、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：指点对点通信量的控制，是端到端中的问题。流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收

发送窗口的大小等于Min[拥塞窗口，接收窗口]，因此是两种控制共同作用。

**第6章 应用层**

**6-03 举例说明域名转换的过程。域名服务器中的高速缓存的作用是什么？**

（1）把不方便记忆的IP地址转换为方便记忆的域名地址。  
（2）作用：可大大减轻根域名服务器的负荷，使因特网上的DNS查询请求和回答报文的数量大为减少。

**6-08 解释以下名词。各英文缩写词的原文是什么？WWW, URL, HTTP, HTML, CGI，浏览器，超文本，超媒体，超链，页面，活动文档，搜索引擎。**

答：www:万维网WWW（World Wide Web）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.万维网用链接的方法能非常方便地从因特网上的一个站点访问另一个站点(也就是所谓的“链接到另一个站点”)，从而主动地按需获取丰富的信息。  
URL:为了使用户清楚地知道能够很方便地找到所需的信息，万维网使用统一资源定位符URL (Uniform Resource Locator 来标志万维网上的各种文档，并使每一个文档在整个因特网的范围内具有唯-的标识符URL.  
HTTP:为了实现万维网上各种链接，就要使万维网客户程序与万维网服务器程序之间的交互遵守严格的协议，这就是超文本传送协议HTTPHTTP是一个应用层协议，它使用TCP连接进行可靠的传送。  
CGI:通用网关接口CGI是一种标准，它定义了动态文档应该如何创建，输入数据应如何提供给应用程序，以及输出结果意如何使用。CGI程序的正式名字是CGI脚本。按照计算机科学的一般概念。  
浏览器:一个浏览器包括一-组客户程序、一组解释程序，以及一个控制程序。  
超文本:超文本的基本特征就是可以超链接文档:你可以指向其他位置，该位置可以在当前的文档中、局域网中的其他文档，也可以在因特网上的任何位置的文档中。这些文档组成了一个杂乱的信息网。目标文档通常与其来源有某些关联，并且丰富了来源:来源中的链接元素则将这种关系传递给浏览者。  
超媒体:超级媒体的简称，是超文本(hypertext)和多媒体在信息浏览环境下的结  
超链:超链接可以用于各种效果。超链接可以用在目录和主题列表中。浏览者可以在浏览器屏幕上单击鼠标或在键盘上按下按键，从而选择并自动跳转到文档中自己感兴趣的那个主题，或跳转到世界上某处完全不同的集合中的某个文档。超链接(hyper text)，或者按照标准叫法称为锚(anchor) ，是使用< a >标签标记的，可以用两种方式表示。锚的一种类型是在文档中创建一个热点，当用户激活或选中(通常是使用鼠标)这个热点时，会导致浏览器进行链接。  
页面:页面，类似于单篇文章页面，但是和单篇文章不同的是: 1. 每个页面都可以自定义样式，而单篇文章则共用一个样式。2.页面默认情况-般不允许评论，而单篇文章默认情况允许评论。3.页面会出现在水平导航栏上，不会出现在分类和存档里，而单篇文章会出现在分类和存档里，不会出现在水平导航栏上。  
活动文档:即正在处理的文档。在Microsoft Word中键入的文本或插入的图形将出现在活动文档中。活动文档的标题栏是突出显示的。一个基于Windows的、嵌入到浏览器中的非HTML应用程序，提供了从浏览器界面访问这些应用程序的功能的方法。  
搜索引擎:搜索引擎指能够自动从互联网上搜集信息，经过整理以后，提供给用户进行查阅的系统。

**6-31 基于万维网的电子邮件系统有什么特点？在传送邮件时使用什么协议？**

特点：不管在什么地方，只要能上网，在打开万维网浏览器后，就可以收发电子邮件。这时，邮件系统中的用户代理就是普通的万维网。  
电子邮件从A发送到网易邮件服务器是使用HTTP协议。  
两个邮件服务器之间的传送使用SMTP。  
邮件从新浪邮件服务器传送到是使用HTTP协议。

**6-33 什么是网络管理？为什么说网络管理是当今网络领域中的热门课题？**

答：网络管理即网络的运行、处理、维护（Maintenance）、服务提供等所需要的各种活动。网络管理是控制一个复杂的计算机网络使得它具有最高的效率和生产力的过程。

**第7章 网络安全**

**7-01 计算机网络都面临哪几种威胁？主动攻击和被动攻击的区别是什么？对于计算机网络，其安全措施都有哪些？**

答:计算机网络面临以下的四种威胁:截获( interception)，中断(nteruption)，篡改(modification),伪造( fabrication)。  
网络安全的威胁可以分为两大类:即被动攻击和主动攻击。  
主动攻击是指攻击者对某个连接中通过的PDU进行各种处理。如有选择地更改、删除、延迟这些PDU。甚至还可将合成的或伪造的PDU送入到一个连接中去。主动攻击又可进一步划分为三种，即更改报文流;拒绝报文服务;伪造连接初始化。  
被动攻击是指观察和分析某一个协议数据单元PDU而不干扰信息流。即使这些数据对攻击者来说是不易理解的，它也可通过观察PDU的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究PDU的长度和传输的频度，以便了解所交换的数据的性质。这种被动攻击又称为通信量分析。  
还有一种特殊的主动攻击就是恶意程序的攻击。恶意程序种类繁多，对网络安全威胁较大的主要有以下几种:计算机病毒;计算机蠕虫:特洛伊木马;逻辑炸弹。  
对付被动攻击可采用各种数据加密动技术，而对付主动攻击，则需加密技术与适当的鉴别技术结合。

**7-02 试解释以下名词： (1 ）重放攻击：（2）拒绝服务：（3 ）访问控制；（4）流量分析：（5）恶意程序。**

(1)重放攻击:所谓重放攻击(replay attack) 就是攻击者发送一 个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程。  
(2)拒绝服务: DoS(Denial of Service指攻击者向因特网上的服务器不停地发送大量分组，使因特网或服务器无法提供正常服务。  
(3)访问控制: ( access control 也叫做存取控制或接入控制。必须对接入网络的权限加以控制，并规定每个用户的接入权限。  
(4)流量分析:通过观察PDU的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究PDU的长度和传输的频度，以便了解所交换的数据的某种性质。这种被动攻击又称为流量分析(traffic analysis) 。  
(5)恶意程序:恶意程序(rogue program) 通常是指带有攻击意图所编写的一段程序。

**7-03 为什么说计算机网络的安全不仅仅局限于保密性？试举例说明，仅具有保密性的计算机网络不一定是安全的。**

计算机网络安全不仅仅局限于保密性，但不能提供保密性的网络肯定是不安全的。网络的安全性机制除为用户提供保密通信以外，也是许多其他安全机制的基础。例如，存取控制中登陆口令的设计。安全通信协议的设计以及数字签名的设计等，都离不开密码机制。

**7-07 对称密钥体制与公钥密码体制的特点各是什么？各有何优缺点？**

答:在对称密钥体制中，它的加密密钥与解密密钥的密码体制是相同的，且收发双方必须共享密钥，对称密码的密钥是保密的，没有密钥，解密就不可行，知道算法和若干密文不足以确定密钥。公钥密码体制中，它使用不同的加密密钥和解密密钥，且加密密钥是向公众公开的，而解密密钥是需要保密的，发送方拥有加密或者解密密钥，而接收方拥有另一个密  
两个密钥之一也是保密的， 无解密密钥，解密不可行，知道算法和其中一个密钥以及若干密文不能确定另一个密钥。  
优点:对称密码技术的优点在于效率高，算法简单，系统开销小，适合加密大量数据。对称密钥算法具有加密处理简单，加解密速度快，密钥较短，发展历史悠久等优点。  
缺点:对称密码技术进行安全通信前需要以安全方式进行密钥交换，且它的规模复杂。公钥密钥算法具有加解密速度慢的特点，密钥尺寸大，发展历史较短等特点。

**7-08 为什么密钥分配是一个非常重要但又十分复杂的问题？试举出一种密钥分配的方法。**

答：密钥必须通过最安全的通路进行分配。可以使用非常可靠的信使携带密钥非配给互相通信的各用户，多少用户越来越多且网络流量越来越大，密钥跟换过于频繁，派信使的方法已不再适用。  
举例：公钥的分配，首先建立一个值得信赖的机构（认证中心CA），将公钥与其对应的实体进行绑定，每个实体都有CA发来的证书，里面有公钥及其拥有者的标识信息，此证书被CA进行了数字签名，任何用户都可从可信的地方获得CA的公钥，此公钥可用来验证某个公钥是否为某个实体所拥有。

**7-10 试述数字签名的原理。**

答:数字签名采用了双重加密的方法来实现防伪、防赖。其原理为:被发送文件用SHA编码加密产生128bit 的数字摘要。然后发送方用自己的私用密钥对摘要再加密，这就形成了数字签名。将原文和加密的摘要同时传给对方。对方用发送方的公共密钥对摘要解密，同时对收到的文件用SHA编码加密产生又一摘要。将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比。如两者一致,则说明传送过程中信息没有被破坏或篡改过。否则不然。