目录

【注】确认收货后评价+带 3 图以上联系客服加 VIP 群

期末试题部分

西北工业大学 2007 年考试

一.不定项选择(共 24 题，每题 1 分，共 24 分；错选不给分，漏选 0.5 分)

1.ABCD	2.ABCD	3.C	4.ACD	5.ABC	6.CD	7.BC	8.AB	9.C
10.AD	11.CD	12.ABCD	13.BCD	14.A	15.ABCD	16. ABC	17. B	18. BCD
19. D	20. AC	21. ABD	22. AD	23. ABCD	24. ABC			

二.名词解释(共 12 题，每题 0.5 分，共 6 分) -见附录一

三.简答题(共 8 题，每题 5 分，共 40 分)

1.OSI 有 7 层：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层

①物理层：完成 0/1 在物理介质上的传输；

②数据链路层：将不可靠的物理链路变成可靠的数据链路；

③网络层：提供路由选择、拥塞控制及网络互连功能，为端到端(【注】这里有很多同学不理解，我解释一下，传输层是端到端的，所以网络层是为传输层提供服务的，可以写“为端到端”或“为传输层”)提供面向连接或无连接的数据传输服务；

④传输层：提供面向进程，面向连接或无连接的数据传输服务

(【注】上述传输层的概念是蔡皖东书上的，其他教材一般是：提供面向进程，面向连接的数据传输服务，从会话层接收数据而且把其分成较小的单元传递给网络层。因为 OSI 参考模型和 TCP/IP 模型的比较。在 OSI 参考模型中，传输层仅有面向连接的方式。而 TCP/IP 模型认为可靠性是端到端的问题，因此它在网络层仅支持无连接的方式，但在传输层支持无连接和面向连接的两种方式)；

⑤会话层：为进程之间的会话提供建立/维护/终止连接的功能；

⑥表示层：协商应用程序间交互的数据格式；

⑦应用层：为网络应用提供协议支持和服务。

【解析】很多同学可能看到《王道》中有一个大选择题考查的是辨析各个层之间的概念的，其中有一问是提供建立、维护和拆除端到端的连接的层是(　　)，这个与⑤会话层的概念相似度极高，容易错选，这道题说的是为端到端的传输提供连接，对进程而言是属于会话层的概念，从书中关于会话层的概念可以看到，它允许不同主机上各进程之间的会话，它是利用传输层提供的端到端的服务向表示层提供服务。请各位考生挖掘对概念的理解。

还有同学问到怎么理解这个建立、维护和拆除？答：我觉得可以联想物理层的电路交换。当两端点之间有需要无差错传输的信息时候，建立链路，类似电路交换的专用物理通信路径，只有你和我可以通信。当通信完毕这个链路继续存在会浪费带宽，肯定要释放掉，一般通过四次挥手来释放；维护可以理解为传输过程的一些非正常情况的发生，解决的方法，例如流量控制和拥塞控制，拥塞避免，网络负载处理慢开始，快恢复等等吧。

2.(1)星型网络通过中间节点将一个节点发来的数据同时转发给其他所有节点，达到“广播式”传输。

(2)环形网络通过发送方发送数据帧，数据帧遍历各个节点，最后由发送方将数据帧从环上取下，从而达到“广播式”传输。

(3)总线型依赖于数据信号沿着总线向两端传播的基本特性实现“广播式”传输。

3.【解析】(1)面向连接的通信，在建立连接阶段通过使用路由表建立一个路径转发表，连接建立好之后，不再使用路由表，而直接使用路径转发表。

(2)无连接的通信，在每个数据包到达路由器时，都需要进行路由选择，然后进行转发。

4.【解析】①HDLC 实现了完整的数据链路层功能，而在局域网体系中，数据链路层功能由 LLC 与 MAC 子层实现，LLC 封装在 MAC 帧中，因此没有校验或同步标志；②LLC 帧地址是服务访问点地址，不是物理地址，物理地址在 MAC 中；③LLC 只定义了一种数据传输模式，简化了 HDLC。

5.【解析】(1)255.255.255.224；(2)子网掩码可屏蔽 IP 地址中的主机号，而保留网络号与子网号。用于说明 IP 地址中子网的位置。

6.【解析】(1)主机相互通信时，首先要知道对方 IP 地址所对应的物理地址才能在物理网络上劲行传输；(2)地址解析通过 ARP 协议完成。

7.【解析】三次握手过程：①第一次握手：建立连接。客户端发送连接请求报文段，将 SYN 位置为 1，Sequence Number 为 x；然后，客户端进入 SYN_SEND 状态，等待服务器的确认；

②第二次握手：服务器收到 SYN 报文段。服务器收到客户端的 SYN 报文段，需要对这个 SYN 报文段进行确认，设置 Acknowledgment Number 为 x+1(Sequence Number+1)；同时，自己自己还要发送 SYN 请求信息，将 SYN 位置为 1，Sequence Number 为 y；服务器端将上述所有信息放到一个报文段（即 SYN+ACK 报文段）中，一并发送给客户端，此时服务器进入 SYN_RECV 状态；

③第三次握手：客户端收到服务器的 SYN+ACK 报文段。然后将 Acknowledgment Number 设置为 y+1，向服务器发送 ACK 报文段，这个报文段发送完毕以后，客户端和服务器端都进入 ESTABLISHED 状态，完成 TCP 三次握手。

握手的作用：防止报文段在传输连接建立过程中出现差错。通过三次握手，通信双方的进程之间就建立了一条传输连接，然后就可以使用全双工的方式在该传输链接上正常的传输数据报文段了；可以解决被延迟的分组问题，从而可以保证数据交换的安全和可靠

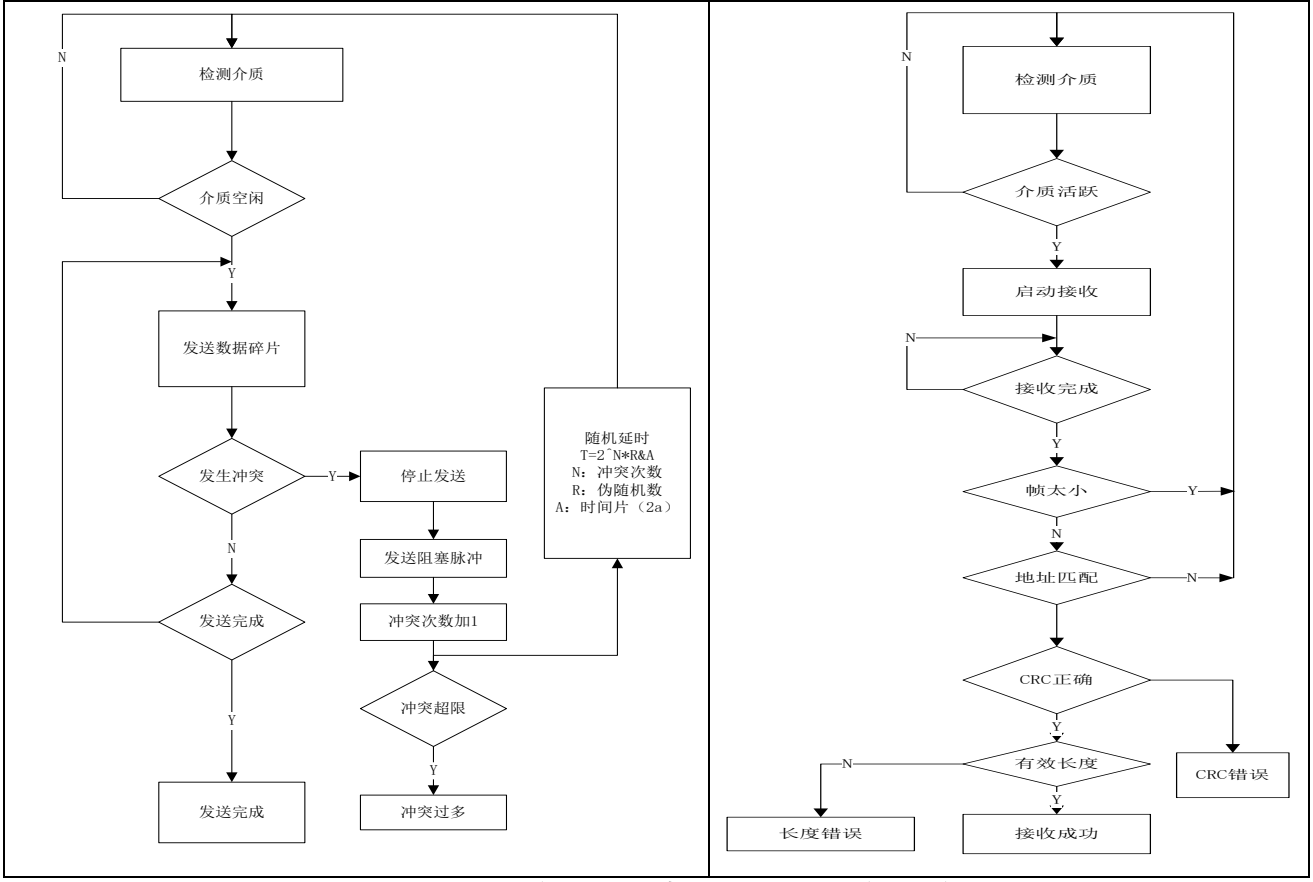
三次握手完成两个重要的功能，既要双方做好发送数据的准备工作，也要允许双方就初始序列号进行协商。

【补充①】为什么一定进行三次握手？当客户端向服务器端发送一个连接请求时，由于某种原因长时间驻留在网络节点中，无法达到服务器端，由于 TCP 的超时重传机制，当客户端在特定的时间内没有收到服务器端的确认应答信息，则会重新向服务器端发送连接请求，且该连接请求得到服务器端的响应并正常建立连接，进而传输数据，当数据传输完毕，并释放了此次 TCP 连接。若此时第一次发送的连接请求报文段延迟了一段时间后，到达了服务器端，本来这是一个早已失效的报文段，但是服务器端收到该连接请求后误以为客户端又发出了一次新的连接请求，于是服务器端向客户端发出确认应答报文段，并同意建立连接。如果没有采用三次握手建立连接，由于服务器端发送了确认应答信息，则表示新的连接已成功建立，但是客户端此时并没有向服务器端发出任何连接请求，因此客户端忽略服务器端的确认应答报文，更不会向服务器端传输数据。而服务器端却认为新的连接已经建立了，并在一直等待客户端发送数据，这样服务器端一直处于等待接收数据，直到超出计数器的设定值，则认为服务器端出现异常，并且关闭这个连接。在这个等待的过程中，浪费服务器的资源。如果采用三次握手，客户端就不会向服务器发出确认应答消息，服务器端由于没有收到客户端的确认应答信息，从而判定客户端并没有请求建立连接，从而不建立该连接。

8.【解析】(1)多路复用通过端口机制提供；(2)端口机制用于标志主机上的不同进程。一个主机上的多个应用程序可以通过不同的端口同时使用 TCP 进行通信。

四.应用题(共 2 题，每题 15 分，共 30 分)

1. (1)帧发送过程和接受过程见下图



(2)由于多个发送方同时检测到介质空闲，并且发送数据，因而产生冲突；冲突发生后，发送方各自延迟随机时间，再争用介质，随机时间采用二进制指数退避算法进行决定。

(3)当冲突产生后，会产生帧碎片当接受到的数据帧长度小于最小帧长限制时，则认为是帧碎片，进行丢弃。

2.【解析】(1) 协议及其功能如下：

应用层：HTTP：WWW 访问协议。

DNS：域名解析。

传输层：TCP：在客户和服务器之间建立连接，提供可靠的数据传输。

网络层：IP：进行路由选择。

ICMP：提供网络传输中的差错检测。

ARP：将目的 IP 地址映射成物理 MAC 地址。

网络接口层：LLC 和 MAC：提供数据链路层的功能，实现可靠的数据链路。

(2) 过程描述如下：

- 利用 DNS，查询到 WWW.GOOGLE.COM 对应的 IP 地址。
- 浏览器与 GOOGLE 的服务器利用 TCP 协议建立连接。
- 浏览器利用 HTTP 的 GET 方法向 GOOGLE 服务器发送资源请求。
- GOOGLE 发送回应信息。
- TCP 释放连接。
- 浏览器解释回应信息，并以图形化的方式显示。

西北工业大学期末考试(软微学院)

一、选择题

答案速查：CBCBB　BCABB　BDDBC　BABBC

7.C【解析】速率为 100Mbps≈10^8bps 的局域网发送 1bit 数据需要的时间越是 1×10^{-8}s

二、填空题

1.CMSA/CD　　2.数据传输速率为 10Mbps　传输模式为基带传输
3.逻辑电路子层　MAC 子层　　4.资源　通信　　5.同轴电缆　双绞线　光缆
6.信息流量　　7.顺序　　8.频分复用　时分复用　波分复用　码分复用
9.无差错按序　　10.暂无答案!　　11.透明　可靠　　12.透明网桥　源路由选择网桥
13.交换机端口节点之间的多对接点比并发连接　　14.性能管理　故障管理　计费管理
15.网间协议　　16.10　　17.硬件资源　软件资源
18.静态路由选择　动态路由选择　　19.传输　表示

三、简答题

1.与中继器相比，网桥不仅能使数据传送到更多的设备中，当冲突发生时，网桥可以将网络分割成两个相互独立的区域
2.发前先侦听，空闲时发送，边发边检测，冲突时退避。
3.在 CSMA/CD 协议中，一旦检测到冲突，为降低再冲突的概率，需要等待一个随机时间，然后再使用 CSMA 方法试图传输。为了保证这种退避维持稳定，采用了二进制指数退避算法的技术，其算法过程如下：
①将冲突发生后的时间划分为长度为 2t 的时隙
②发生第一次冲突后，各个站点等待 0 或 1 个时隙在开始重传
③发生第二次冲突后，各个站点随机地选择等待 0,1，2 或 3 个时隙在开始重传
④第 i 次冲突后，在 0 至 2 的 i 次方减一间随机地选择一个等待的时隙数，在开始重传
⑤10 次冲突后，选择等待的时隙数固定在 0 至 1023（2 的 10 次方减一）间
⑥16 次冲突后，发送失败，报告上层。
4.①各层之间是独立的②灵活性好③结构上可以分隔开④易于实现和维护⑤能促进标准化工作
5.IP 协议:在网络中主机使用 IP 地址进行百标识，主机之间使用分配的 IP 地址来发度送和接收 IP 分组。
ARP 协议: 通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通答信的顺利进行。
RARP:使只知道自己硬件地址的主机能够知道其 IP 地址。
ICMP:允许主机或者路由器报告差错情况专和有关异常情况，配合 IP 使用，提高分组交付成属功的机会。
DHCP:使用 DHCP 可以使客户端自动的获得 IP 地址。使用 DHCP 可以消除手工配置 TCP/IP 出现的一些配置故障。

四、计算题

1、解：C=Blog2L

C=1200bps,B=600 波特，得 L=4

信息取 4 位状态

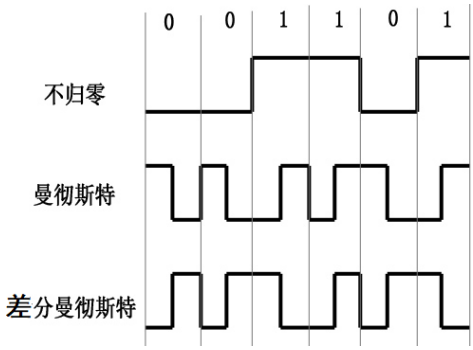
当 L=2 时，码元速率与数据速率相等

2、解：接收正确

接受信息/G（x），余数为 0，则正确，否则出错。推演过程如下:

```
          1101010
11001 | 10110011010
         11001
          11110
          11001
           11111
           11001
            11001
            11001
                0
```

3、



余数为 0，接收正确。

4、UGR--紧急数据指针字段中的数据有意义。

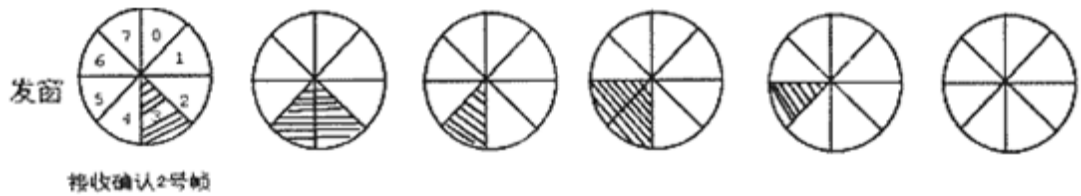
ACK--确认数据段中的数据有意义。

PSH--指出接收方不必等待一定量的数据再向应用提供数据，即立即提供该数据段。

SYN--在建立初始连接时，允许双方共同确认序列号。

FLN--标志是最后的 TCP 数据段。

5、



发送 4 号帧　接收确认 3 号帧　发送 5 号帧　接收确认 4 号帧　停止发送

西北工业大学 2011-2012 学年网络与分布式计算期末考试

一、单项选择题（每小题 2 分，共 30 分）

答案速查：AACCB　DACAA　CBDAA

二、判断题（每小题 1 分，共 10 分）

1 √　2 ×　3 √　4 √　5×　6 √　7 √　8×　9 √　10 √

三、名词解释（每小题 1 分，共 10 分）-见附录一

四、简答题（每小题 6 分，共 30 分）

1.(1)路由选择与网络控制；(2)提供面向连接(如虚电路网络)或无连接服务(如 IP 网络)；(3)提供异构网络互连。
2.子网数：1024（或 2^{10}）。每个子网最多容纳 62 台主机。
3.原因:(1)无线通信环境下很难实现边发送，边进行冲突检测。 (2)环境对无线通信有影响，即使距离相同的接收方，自于所处的环境不同，接收到的相同发送源的无线信号强度不同。(3)无线通信环境下存在“暴露终端”和“隐藏终端”问题。
运作机制: (1)发送方发送数据前首先侦听无线信道是否空闲，如果空闲，等待一个 FIS 时间，如果无线信道空闲，发送一个 RTS 控制帧。(2)否则，一直帧听直到信道为空闲。(3)接收方接收到 RTS 帧后，如果允许发送方发送数据帧，等待一个 FIS 时间，给发送方发送一个 CTS 帧。(4)发送方接收到 CTS 帧后，等待一个 FIS 时间，如果信道空闲，开始发送数据帧。
4.CSMA/CA：(1)CSMA/CA 是无线局域网络在 DCP 模式下所采用的一种介质访问控制协议。(2)含义：载波帧听、多路访问/冲突避免。
差异：(1)载波检测方式：因传输介质不同，CSMA/CD 与 CSMA/CA 的检测方式也不同。CSMA/CD 通过电缆中电压的变化来检测，当数据发生碰撞时，电缆中的电压就会随着发生变化；而 CSMA/CA 采用能量检测（ED）、载波检测（CS）和能量载波混合检测三种检测信道空闲的方式。
(2)信道利用率比较 CSMA/CA 协议信道利用率低于 CSMA/CD 协议信道利用率。但是由于无线传输的特性，在无线局域网不能采用有线局域网的 CSMA/CD 协议。信道利用率受传输距离和空旷程度的影响，当距离远或者有障碍物影响时会存在隐藏终端问题，降低信道利用率。
5.原因:(1)发送方只有在数据链路层将 MAC 地址封装在帧结构中才可以以帧的形式发送数据到物理线路上。
(2)接收方在数据链路层按照“地址匹配”的原则接收数据帧。所用到的相关协议为 ARP 协议，地址解折协议，主要实现 IP 地址到 MAC 地址的映射关系。

五、综合题（每小题 20 分，共 20 分）

【答】所用到的协议及作用如下：
应用层：1.HTTP 协议：实现应用层浏览器客户端与 WEB 服务器之间会话和数据传输。2.DNS 协议：实现域名到 IP 地址之间解析。
传输层：TCP 协议：实现端到端不同进程之间面向连接通信。
网络层：IP 协议：封装、解封分组，对分组的校验处理等；ICMP：网络控制、路由重定向等；ARP:实现 IP 地址到 MAC 地址映射。
网络接口层：LLC 子层：逻辑链路控制子层，实现点到点之间可靠数据传输；MAC 子层：介质访问控制协议，实现介质的有序访问控制。
描述浏览网页的整个逻辑过程：
①用户首先通过浏览器发送一个 HTTP 请求报文：Get http://ww.nwpu.edu.cn/index.html
②客户浏览器利用 DNS 协议，获得域名 ww.nwpu.edu.cn 对应的 IP 地址。
③TCP 协议利用目的 IP 地址，在客户与服务器之间通过三次握手建立一个 TCP 连接。
④ARP 协议获得下一跳（或目的 IP 地址）对应的 MAC 地址。
⑤接收方接受到 http 请求后，将西工大首页通过 http 协议发送给浏览器。
⑥浏览器接受到首页信息后，通过解析器在浏览器中显示。

历年真题部分

西北工业大学 2007 年研究生入学考试(401)

一.名词解释(给出简写的汉语意思，每题一分，满分 10 分)-见附录一

二.简答题(每题 6 分，满分 30 分)

(1)【解析】见《西北工业大学 2007 年考试》三.简答题 1 小题

(2)【解析】见《西北工业大学 2007 年考试》三.简答题 4 小题

(3)路由表是根据路由选择算法得出的，主要用途是路由选择。转发表是由路由表得到的，但转发表的格式和路由表的格式不同，其结构应使查找过程最优化，而路由表则需对网络拓扑变化的计算最优化。路由表总是用软件来实现，转发表可以用软件实现，甚至也可以用特殊的硬件来实现。路由表不等于转发表。分组的实际转发是靠直接查找转发表，而不是直接查找路由表。

(4)①CSMA/CD 协议要求每一个站点在发送本站数据的同时，还必须不间断地检测信道，但在无线局域网的设备中实现这种功能就会花费过大；②即使能够实现碰撞检测的功能，并且在发送数据时检测到信道是空闲的，接收端仍有可能发生碰撞，即“隐蔽站问题”；③“暴露站问题”。

运作机制：①首先检测信道是否有使用，如果检测出信道繁忙，则等待一段随机时间并进入争用窗口，使用二进制指数退避算法计算随机退避时间，以便再次重新接入信道，直到送出数据。

②预约信道：发送数据的同时向其它站点通知自己传输数据所需时间长度。以便其他站点在这段时间内不发送数据，避免碰撞。

③ACK 帧：接收端如果正确收到此帧，则向发送端发送确认帧 ACK。发送端收到 ACK 帧，确定数据正确传输。

④RTS/CTS 帧。可选的碰撞避免机制，解决“隐蔽站”问题。

【注】有同学问 CSMA/CA 不是不检测信道吗？答：冲突避免并不是说不检测信道，如果不知道信道情况如何进行避免？可见对概念的理解很不扎实。

【解析】有同学看到《王道》上写到：当且仅当检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧时，才不使用退避算法。产生了“发送第一个数据帧时到底使不使用二进制指数退避算法”的疑问，答案最后一条写的也很清楚，退避算法是使用在 1.发送第一个帧前检测到信道处于忙态，2.在每一次的重传后或者成功发送后。但发送前检测到信道是空闲的，并且数据帧是第一个就不用，所以答案说如果检测到空闲，就只等一个帧间隔就行。任何一个站发送数据帧时，都必须等待一个时间间隔。

(5)三次握手的过程及作用见《西北工业大学 2007 年考试试题-蔡皖东》三简答题 7 小题

【补充】释放连接有两种方式，非对称释放和对称释放。非对称释放是指通信双方任意一方释放连接，该连接便宣告终止，如在电话交换系统中，任意一方挂机终止了连接。如果一个双向连接是由两个独立的单项连接组合而成的，则通信双方必须分别释放单项连接，这个连接才能完全终止，这就是对称性释放。由于传输层协议所建立的连接是两个独立的单向连接，因此必须采用对称性释放方式来终止连接。

三次挥手的过程：对称性释放连接方式实际上是采用三次握手来释放连接的，它与三次握手建立连接的过程相类似。

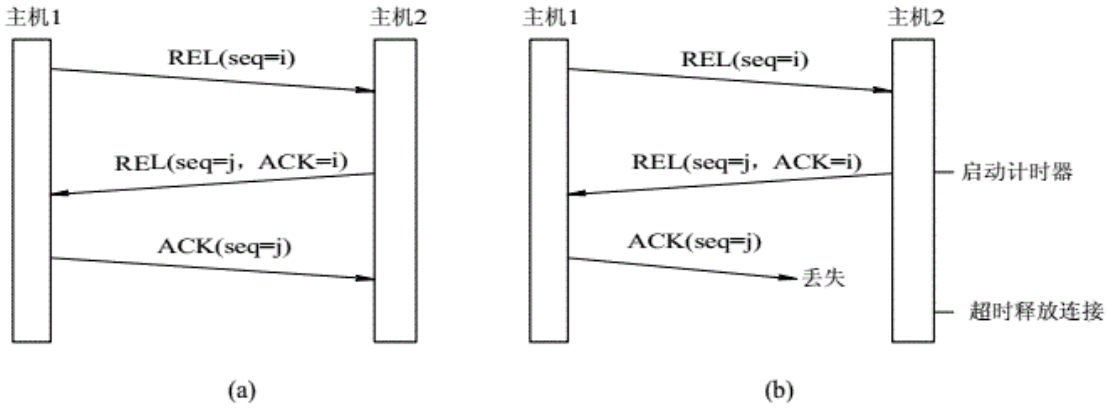


图 2.18　采用三次握手法释放连接的过程

(a) 正常情况；(b) 出现丢失应答分组情况

(a)为正常情况的释放连接的过程。如果主机 1 的应答分组丢失，并且主机 2 一直等待主机 1 的应答，则会形成非对称性释放而产生半连接问题，结果造成数据丢失或主机 2 死机的问题。解决的办法是主机 2 设有一个计时器，当主机 2 发出释放连接的请求后，计时器开始计时。如果超时仍未收到对方的应答分组，则认为应答分组已丢失，并立即释放连接，参见图(b)。

挥手的作用：三次握手法能够有效地保证建立和释放连接的安全性和可靠性，因而被很多传输层协议所采用。TCP 协议就是采用三次握手法来建立和释放连接的。

【补充①】四次挥手的过程：①第一次分手：主机 1(可以使客户端，也可以是服务器端)，设置 Sequence Number 和 Acknowledgment Number，向主机 2 发送一个 FIN 报文段；此时，主机 1 进入 FIN_WAIT_1 状态；这表示主机 1 没有数据要发送给主机 2 了；

②第二次分手：主机 2 收到了主机 1 发送的 FIN 报文段，向主机 1 回一个 ACK 报文段，Acknowledgment Number 为 Sequence Number 加 1；主机 1 进入 FIN_WAIT_2 状态；主机 2 告诉主机 1，我“同意”你的关闭请求；

③第三次分手：主机 2 向主机 1 发送 FIN 报文段，请求关闭连接，同时主机 2 进入 LAST_ACK 状态；

④第四次分手：主机 1 收到主机 2 发送的 FIN 报文段，向主机 2 发送 ACK 报文段，然后主机 1 进入 TIME_WAIT 状态；主机 2 收到主机 1 的 ACK 报文段以后，就关闭连接；此时，主机 1 等待 2MSL 后依然没有收到回复，则证明 Server 端已正常关闭，那好，主机 1 也可以关闭连接了。

【补充②】为什么 TCP 挥手要比握手多一次？因为当处于 LISTEN 状态的服务器端收到来自客户端的 SYN 报文(客户端希望新建一个 TCP 连接)时，它可以把 ACK(确认应答)和 SYN(同步序号)放在同一个报文里来发送给客户端。但在关闭 TCP 连接时，当收到对方的 FIN 报文时，对方仅仅表示对方已经没有数据发送给你了，但是你自己可能还有数据需要发送给对方，则等你发送完剩余的数据给对方之后，再发送 FIN 报文给对方来表示你数据已经发送完毕，并请求关闭连接，所以通常情况下，这里的 ACK 报文和 FIN 报文都是分开发送的。

【注】西工大使用的网络教材是蔡皖东版本的，是三次握手和三次挥手，实际上使用较为广泛的是三次握手、四次挥手的过程。

三.应用题(10 分)

参考见《西北工业大学 2007 年考试》四应用题 2 小题

西北工业大学 2007 年研究生入学考试(814/840)

【编者注】这应该是考博题，不知怎么流传下来了，大家做做填空题即可，大题看看就可以!

一.填空题(每小题 3 分，本题满分 45 分)

1.IP ICMP ARP　2. 192.168.5.120 【解析】IP 地址与子网掩码逐位与运算
3. 2.048Mbps　4.全双工 半双工　5.TCP UDP　6.比特　7.广域网 城域网 局域网
8.ICMP　9.调幅 调频 调相　10.数据报　11.B 128.11 3.31
12.报文交换网 分组交换网　13.域名解析　14.3 次　15.丢弃 源主机

二.简答题(每小题 8 分，本题满分 80 分)

1.同步通信是一种连续串行传送数据的通信方式，一次通信只传送一帧信息。这里的信息帧与异步通信中的字符帧不同，通常含有若干个数据字符。

它们均由同步字符、数据字符和校验字符（CRC）组成。其中同步字符位于帧开头，用于确认数据字符的开始。数据字符在同步字符之后，个数没有限制，由所需传输的数据块长度来决定；校验字符有 1 到 2 个，用于接收端对接收到的字符序列进行正确性的校验。同步通信的缺点是要求发送时钟和接收时钟保持严格的同步。

异步通信中，数据通常以字符或者字节为单位组成字符帧传送。字符帧由发送端逐帧发送，通过传输线被接收设备逐帧接收。发送端和接收端可以由各自的时钟来控制数据的发送和接收，这两个时钟源彼此独立，互不同步。

接收端检测到传输线上发送过来的低电平逻辑"0"（即字符帧起始位）时，确定发送端已开始发送数据，每当接收端收到字符帧中的停止位时，就知道一帧字符已经发送完毕。 在异步通行中有两个比较重要的指标：字符帧格式和波特率。

2.唯一的 IP 地址、子网掩码以及默认网关的 IP 地址

3.子网掩码：255. 255.224.0,二进制码:11111111.11111111.11100000.00000000,所以：子网号取 3 位，主机号取 13 位,每个子网可以连接 2^{13}-2=8192-2=8190 台主机,可以分成 2^{3}-2=6 个子网

4.①CSMA/CD 协议要求每一个站点在发送本站数据的同时，还必须不间断地检测信道，但在无线局域网的设备中实现这种功能就会花费过大；②即使能够实现碰撞检测的功能，并且在发送数据时检测到信道是空闲的，接收端仍有可能发生碰撞，即“隐蔽站问题”，③“暴露站问题”。

运作机制：

(1)首先检测信道是否有使用，如果检测出信道繁忙，则等待一段随机时间并进入争用窗口，使用二进制指数退避算法计算随机退避时间，以便再次重新接入信道，直到送出数据。

(2)预约信道：发送数据的同时向其它站点通知自己传输数据所需时间长度。以便其他站点在这段时间内不发送数据，避免碰撞。

(3)ACK 帧：接收端如果正确收到此帧，则向发送端发送确认帧 ACK。发送端收到 ACK 帧，确定数据正确传输。

(4)RTS/CTS 帧。可选的碰撞避免机制，解决“隐蔽站”问题。

【注】有同学问 CSMA/CA 不是不检测信道吗？答：冲突避免并不是说不检测信道，如果不知道信道情况如何进行避免？可见对概念的理解很不扎实。

【解析】有同学看到《王道》上写到：当且仅当检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧时，才不使用退避算法。产生了“发送第一个数据帧时到底使不使用二进制指数退避算法”的疑问，答案最

后一条写的也很清楚，退避算法是使用在 1.发送第一个帧前检测到信道处于忙态，2.在每一次的重传后或者成功发送后。但发送前检测到信道是空闲的，并且数据帧是第一个就不用，所以答案说如果检测到空闲，就只等一个帧间隔就行。任何一个站发送数据帧时，都必须等待一个时间间隔。

5.主机:A,B 间进行通讯的一般过程(A,B 的 IP 是 ISP 提供的静态 IP)(1)A 用 TCP 与 B 建立连接.(2)A 搜索自已的 ARP 缓存,得出默认网关 R1 的 MAC,并以 MAC 头的形式写入 IP 数据报,成为以太网帧.(3)A 的默认网关 R1 接到 A 送来的以太网帧,并搜索自已的 ARP 缓存,若发现有 B 的 MAC(说明 B 与 A 同网关),则直接把包发送给 B.若没有,则网关解掉 MAC 头,并转发该数据报,送入它的默认路由器，经过 N 个因特网路由器后,找到了与目标机 B 同网络号的网关 R2 了，R2 接到这个数据报后,把目标机 B 的 MAC 以 MAC 头的形式写入 IP 数据报,再次成为以太网帧.直接把包发送给 B

6.①开放式协议标准。可免费使用，且与具体的计算机硬件或操作系统无关。由于它受到如此广泛的支持，因而即使不通过 Internet 通信，利用 TCP/IP 来统一不同的硬件和软件也是很理想的； ②与物理网络硬件无关。这就允许 TCP/IP 可以将很多不同类型的网络集成在一起，它可以适用于以太网、令牌环网、拨号线、X.25 网络以及任何其它类型的物理传输介质；③通用的寻址方案。该方案允许任何 TCP/IP 设备唯一的寻址整个网络中的任何其他设备，该网络甚至可以象全球 Internet 那样大;④各种标准化的高级协议。可广泛而持续地提供多种用户服务。

7.网桥类似于中继器，连接两个局域网络段，但它是在数据链路层连接两个网。网间通信从网桥传送，而网络内部的通信被网桥隔离。网桥检查帧的源地址和目的地址，如果目的地址和源地址不在同一个网络段上，就把帧转发到另一个网络段上；若两个地址在同一个网络段上，则不转发，所以网桥能起到过滤帧的作用。网桥的帧过滤性很有用，当一个网络由于负载很重而性能下降时可以用网桥把它分成两个网络段并使得段间的通信量保持最小。例如，把分布在两层楼上的网络分成每层一个网络段，段间用网桥连接，这样的配置可最大限度地缓解网络通信繁忙的程度，提高通信效率。同时，由于网桥的隔离作用，一个网络段上的故障不会影响另一个网络段，从而提高了网络的可靠性。

8.TCP 使用一种窗口机制来控制数据流。当一个连接建立时，连接的每一端分配一个缓冲区来保存输入的数据，并将缓冲区的尺寸发送给另一端。当数据到达时，接收方发送确认，其中包含了自己剩余的缓冲区尺寸。剩余的缓冲区空间的大小被称为窗口，指出窗口大小的通知称为窗口通告（window advertisement）。接收方在发送的每一确认中都含有一个窗口通告。

如果接收方应用程序读数据的速度能够与数据到达的速度一样快，接收方将在每一确认中发送一个正的窗口通告。然而，如果发送方操作的速度快于接收方（由于 C P U 更快），接收到的数据最终将充满接收方的缓冲区，导致接收方通告一个零窗口（ zero window）。发送方收到一个零窗口通告时，必须停止发送，直到接收方重新通告一个正的窗口。

【或】答：在任意时刻，发送方维持一组连续的允许发送帧的序号，称为发送窗口；同时接收方也维持一组连续的允许接收帧的序号，称为接收窗口。即接收站的接收缓冲区容量可以存放 n 个帧，发送帧可以连续发送 n 个帧后再停下来等待接收站的应答帧，当接收到后再发送 n 个帧；接收站在处理完接收缓冲区的 n 个数据帧后发送应答帧，指示发送站发送下面的 n 个帧。这是一种多帧应答机制的通信协议。

9.①线路问题。线路接头是否接好，线路是否经过了什么干扰源，确保线路连接正确；

②网络硬件质量有问题。如，双胶线、水晶头、分离器、猫、路由器、网卡。猫、路由器、和网卡质量尤为重要，集成网卡如果工作出现不稳定，可换一块独立网卡；

③注意分离器、猫、路由器的散热；

④网卡驱动。驱动程序不对，造成不能上网或掉线，更换网卡，更新网卡驱动；

⑤宽带上网拨号软件；

⑥操作系统，。操作系统可能对 ADSL 的相关组件存在兼容性问题，这样可以到微软对系统进行升级，或者修复系统。有条件可以进行重装；

⑦软件冲突问题。如果软件有冲突就尽量找出冲突软件，对其卸载或者其他方法解决。比如有的朋友 BT 下载会导致网络掉线。可能下载的时候占用过多的线程导致断线；

⑧病毒问题。ADSL 虽然受到黑客和病毒的攻击可能性较小，但也不排除可能性，特别是网页病毒和蠕虫病毒。病毒如果破坏了 ADSL 相关组件也会有发生断流现象；

⑨防火墙。如果上网不稳定，可以尝试先关闭防火墙，测试稳定与否，在进行相应的设置。 另外防火墙引起或 IE 浏览器出现故障，也可导致可以正常连接，但不能打开网页。

10.(1)划分子网技术：将 IP 主机地址部分进一步划分为子网号和主机号两部分，既可节约网络地址，又可充分利用主机号部分的巨大编制能力

(2)NAT（network address translation）技术：NAT 技术能帮助解决令人头痛的 IP 地址紧缺的问题，而且能使得内外网络隔离，提供一定的网络安全保障，其解决问题的方法是在内部网络中使用内部私有地址，当要访问外部网络时，通过 NAT 把内部私有地址转换成公有地址在 Internet 上使用，具体的做法是把 IP 包内的地址域用公有 IP 地址来替换。NAT 功能通常被集成到路由器、防火墙、ISDN 路由器或者是单独的 NAT 设备中，NAT 设备维护一个状态表，用来把私有地址映射到公有地址上去，每个包在 NAT 设备中被转换成公有地址，发往下一级。

(3)无类域间选路 CIDR(classless interdomain routing)：无类域间选路技术也被称为超网，它把划分子网的概念向相反的方向做了扩展：通过借用前三个字节的几位可以把多个连续的 c 类地址聚集在一起，使得路由器可以忽略网络类别（c 类）地址，并可以在决定如何转发数据报时向前再多看几位。

(4)代理 ARP（address resolution protocol）：代理 ARP 也是一种 IP 网络地址复用技术，它要求网络采用 ARP 协议进行 IP 地址—物理地址映射。当主网络上各主机调用 ARP 解析隐藏网络上主机的物理地址时，网关 G（gateway）代替主机响应，但给出的物理地址是 G 本身在主网络上的物理地址，这样所有进入隐藏网络的数据都首先到达网关 G，网关对隐藏网络上的各主机了如指掌，收到进入数据报后，它进一步确定将数据报传给哪台隐藏主机，同样它也掌握主网络上各主机或网关位置，以便对外出数据报进行合适的操作。

(5)最终的解决方案---Ipv6：以上几种方案都没有从根本上解决 Ipv4 空间危机问题，很明显 IP 必须进一步发展且更具灵活性。Ipv6 保持了 IP 的优良特性，抛弃或减弱了其缺点，并且在有必要的地方加入了新特性。首先，Ipv6 有比 Ipv4 更长的地址，共有 128 位地址结构，它提供了一个有效的无线因特网地址空间，其地址长度 4 倍于 Ipv4；其次，Ipv6 对头部进行了简化，仅包含 7 个字段，而 Ipv4 有 13 个字段；

三．此题略，不必做!

西北工业大学软微学院未知年份真题一

一.单项选择题(每小题 2 分，共 30 分)

答案速查：DABAC　DADBA　BBCBD

2.A【解析】选项中前 24 位与题干中一致，因此直接看最后 8 位，题干 19=0001/0011，选项 A：17=0001 0001，选项 B：14=0000 1110，选项 C：16=0001 0000，选项 D：13=0000 1101。因此只有 A 选项前 24 位与题干完全一致。

4.A【解析】TCP/IP 参考模型从底向上依次为：网际层、网际接口层、传输层和应用层。

9.B【解析】以太网交换机是第二层交换机，第二层交换机工作在 OSI 参考模型的数据链路层，它依据数据帧中目的 MAC 地址进行数据帧的线速交换。因此答案选 B。

15.D【解析】 路由器是在网络层上实现多个网络互联的设备。由路由器互联的局域网中，每个局域网只要求网络层及以上高层协议相同，数据链路层与物理层协议可以是不同的。

二.判断正误题(每小题 1 分，共 10 分)

答案速查：×√×√×　　×√×√×

1.×【解析】采用曼彻斯特编码，波特率是数据速率的两倍，此题应为二分之一。
3.×【解析】POP3、IMAP4 协议接收电子邮件，SMTP 协议发送电子邮件。
5.×【解析】是用来实现网络中差错控制。
6.×【解析】BGP(外部网关协议)将网络划分成不同区域，适用于大规模网络
8.×【解析】以太网采用的是基于 CSMA/CD；令牌环网用令牌协议
10.×【解析】DNS 实现的为域与映射；ARP 协议实现 IP 地址到 MAC 地址的映射

三.名词解释(每题 1 分，共 10 分，仅写出中文名称即可)-见附录一

四.简答题(每题 5 分，共 25 分)

1.每个子网最多有 30 台主机，2^5=32，因为要产生最大数目的子网，故主机位为 5 位，子网 2 位，网络位为前 27 位，子网掩码为 255.255.255.224

子网掩码的作用：可屏蔽 IP 地址中的主机号，从而分离 IP 地址中的网络部分与主机部分，用于说明 IP 地址中子网的位置，管理员可将网络进一步划分为若干子网。

2.(1)TCP 与 UDP 相同点：都是基于 IP 协议的传输协议；

(2)TCP 与 UDP 区别总结：①TCP 面向连接;UDP 是无连接的，即发送数据之前不需要建立连接；

②TCP 提供可靠的服务。也就是说，通过 TCP 连接传送的数据，无差错，不丢失，不重复，且按序到达;UDP 尽最大努力交付，即不保证可靠交付

③TCP 面向字节流，实际上是 TCP 把数据看成一连串无结构的字节流;UDP 是面向报文的 UDP 没有拥塞控制，因此网络出现拥塞不会使源主机的发送速率降低(对实时应用很有用，如 IP 电话，实时视频会议等)

④每一条 TCP 连接只能是点到点的；UDP 支持一对一，一对多，多对一和多对多的交互通信；

⑤TCP 首部开销 20 字节；UDP 的首部开销小，只有 8 个字节；

⑥TCP 的逻辑通信信道是全双工的可靠信道，UDP 则是不可靠信道

常见使用 TCP 协议的应用如下：当对网络通讯质量有要求的时候，比如：整个数据要准确无误的传递给对方，这往往用于一些要求可靠的应用，比如 HTTP、HTTPS、FTP 等传输文件的协议，POP、SMTP 等邮件传输的协议。

浏览器用的 HTTP；FlashFXP 用的 FTP；Outlook 用的 POP、SMTP；Putty 用的 Telnet、SSH；

常见使用 UDP 协议的应用如下：当对网络通讯质量要求不高的时候，要求网络通讯速度能尽量的快，这时就可以使用 UDP，QQ 语音，在线视频，TFTP

3.Tracert 先发送 TTL 为 1 的回应数据包，当数据包上的 TTL 在路由器收到后 TTL 自动减 1，一旦某个服务器将 TTL 减 1 后等于 0 时，路由器应该将“ICMP Time Exceeded”的消息发回源计算机，源计算机就根据收到的信息判断达到的路由器和所用时间。下次再次发送数据包时，将 TTL 递增 1，继续上述测试，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 Tracert 实用程序中看不到，会显示请求超时的请求信息。

4.①为端到端数据传输提供面向连接和无连接的服务；②提供控制通信子网传输的有无操作，如路由选择、流量控制、网络互连等；③按照传输层的要求选择服务质量和安全级；④差错检测、复位。

5.CSMA/CA 是带有冲突避免的载波监听多路访问协议，流程如下。

（1）当主机需要发送一个数据帧时，首先检测信道，在持续检测到信道空闲达一个 DIFS 之后，主机发送数据帧。接收主机正确接收到该数据帧，等待一个 SIFS 后马上发出对该数据帧的确认。若源站在规定时间内没有

收到确认帧 ACK，就必须重传此帧，直到收到确认为止，或者经过若干次重传失败后放弃发送。

（2）当一个站检测到正在信道中传送的 MAC 帧首部的“持续时间”字段时，就调整自己的网络分配向量 NAV。NAV 指出了必须经过多少时间才能完成这次传输，才能使信道转入空闲状态。因此，信道处于忙态，或者是由于物理层的载波监听检测到信道忙，或者是由于 MAC 层的虚拟载波监听机制指出了信道忙

主要用在无线局域网中，在 CSMA 的基础上增加了冲突避免的功能，要检查接收方是否发回帧的确认，若收到确认，则表明无冲突发生，若在规定时间内没有收到确认，则重发该帧。

CSMA/CA 协议的工作原理。当某个站点发送数据帧时：

（1）先检测信道（进行载波侦听）。

（2）目的站若正确收到此帧，则经过时间间隔 SIFS 后，向源站发送确认帧 ACK。

（3）所有其他站都设置网络分配向量 NAV，表明在这段时间内信道忙，不能发送数据。

（4）当确认帧 ACK 结束时，NAV（信道忙）也就结束了。在经历了帧间间隔之后，接着会出现一段空闲时间，叫做争用窗口，表示在这段时间内有可能出现各站点争用信道的情况。

（5）争用信道比较复杂，因为有关站点要执行退避算法。

CSMA/CA（即带有冲突避免的载波侦听多路访问）是一种数据传输是避免各站点之间数据传输冲突的算法，其特点是发送包的同时不能检测到信道上有无冲突，只能尽量“避免”。

西北工业大学软微学院未知年份试题二

一.单选题(共 15 题，每题 2 分，满分 30 分)

答案速查：ACBDB　CDDAC　BACDB

1.A【解析】C 中查分不归零为 1.5 倍。

2.C【解析】异步 TDM 又称为统计时分多路复用技术。

3.B【解析】A 异步传输以字符为单位进行数据传输；C 应当采用相同的传输速率；D 同步传输的数据格式中，一般都需要加一个特殊的字符或者比特序列。

4.D【解析】A、B 均属于物理层，C 属于数据链路层。

9.A【解析】A 类地址：1~126；B 类地址：128~191；C 类地址：192~223。

12.A【解析】数据链路层为网络层提供传送数据的功能和过程；B.端口号是应用层；C.IP 地址是网络层；D.逻辑地址是传输层。

15.B【解析】IPV6 规定：为了简化表示方法，可以将连续的 0 省略为“::”且只能出现一次，因此 A、C、D 正确；IPv6 采用的是 128 位的冒分八段十六进制法，B 项错误。

二.填空(共 10 空，每空 1 分，满分 10 分)

1.幅移键控方式(ASK)　频移键控方式(FSK)　相移键控方式(PSK)

2.控制　帧校验序列(FCS)

3.逻辑链路控制　介质访问控制

4.3600【解析】$\log_2 8=3$，一个码元携带 3b 信息，因此传输率为 3600bps。

5.ARP

三.简答题(共 4 题，每题 5 分，满分 20 分)

1.【解析】见《西北工业大学 2007 年考试》三.简答题 1 小题

2.集线器实际是一个多端口的中继器，采用广播方式，不能隔离冲突域；交换机实际是一个多端口的网桥，采用存储转发方式，能隔离冲突域。区别如下：

①工作层次：集线器工作在物理层，属于 1 层设备，每发送一个数据，所有的端口均可以收到，采用了广播的方式，因此网络性能受到很大的限制；交换机工作在数据链路层，属于 2 层设备，通过学习之后，每个端口形成一张 MAC 地址转发表，根据数据包的 MAC 地址转发数据，而不是广播形式。

②转发方式：集线器的工作原理是广播形式，无论哪个端口收到数据之后，都要广播到所有的端口，当接入设备比较多时，网络性能会受到很大的影响；交换机根据 MAC 地址转发数据，收到数据包之后，检查报文的目的 MAC 地址，找到对应的端口进行转发，而不是广播到所有的端口。

③传输模式：集线器内部采用了总线型拓扑，各个节点共用一条总线进行通信，数据包的发送和接收采用了 CSMA/CD 协议，在同一时间内必须是单向的，只能维持在半双工模式下。两个端口不能同时收发数据，并且当两个端口通信时，其他端口不同工作；当交换机上的两个端口通信时，它们之间的通道是相互独立的，可以实现全双工通信。两个端口同时收发数据。

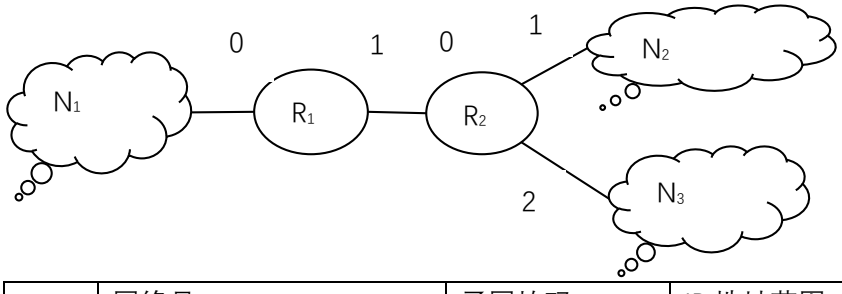
④带宽影响：集线器无论有多少个端口，所有的端口共享一条宽带，同一时刻只能有两个端口传输数据，并且只能工作在半双工模式下；交换机的每个端口独占带宽，两个端口交互数据并不影响其他端口交换数据。

3.相同点：都属于分组交换

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

4.【解析】见《西北工业大学 2007 年考试》三.简答题 8 小题

四.应用题(本题满分 15 分)



	网络号	子网掩码	IP 地址范围	直接广播地址

N1	195.100.86.0	255.255.255.192	195.100.86.1~62	195.100.86.63
N2	195.100.86.128	255.255.255.192	195.100.86.129~190	195.100.86.191
N3	195.100.86.192	255.255.255.192	195.100.86.193~254	195.100.86.255

【解析】因为 N_1、N_2、N_3三个网络主机数分别为 60、30、40，$2^5<60<2^6$，因此主机数选择 6 位，剩下的两位作为子网号，而图中需要的接口刚好需要四个子网。因此我们将 R1 端口 0、1 和 R2 端口 0、1、2 分别分配 00、01、10 和 11。此时 R1 路由表：

目的网络	子网掩码	下一跳
195.100.86.0	255.255.255.192	接口 0，直连 195.100.86.1
195.100.86.128	255.255.255.192	R2
195.100.86.192	255.255.255.192	R2

R2 路由表

目的网络	子网掩码	下一跳
195.100.86.128	255.255.255.192	接口 1，直连 195.100.86.129
195.100.86.192	255.255.255.192	接口 2，直连 195.100.86.193
195.100.86.0	255.255.255.192	R1

【解法 2】上述解答是从主机数不超过 60 台为出发点，有同学提出关于划分出四个子网，只使用了 3 个，浪费了一个子网的问题，也可以按照下述方法进行划分，即先将第 25 位划分成 0 和 1 两个网络，分别给 R1 的 0、1 接口，再将 1 继续划分成 10、11(可参考 17 最后一题非等长子网的划分)，而且在我看来这样的好处是与 R1 相连的只有 LAN1 和 R2，还更方便对于 LAN1 进行主机的扩展，因为他最多可以满足 126 台主机使用，这两种方法都符合题目要求。

	子网地址	直接广播地址	主机 IP 地址范围	子网掩码
LAN1	195.100.86.0	195.100.86.127	195.100.86.1~126	255.255.255.128
LAN2	195.100.86.128	195.100.86.191	195.100.86.129~190	255.255.255.192
LAN3	195.100.86.192	195.100.86.255	195.100.86.193~254	255.255.255.192

R1 路由表

目的网络	子网掩码	下一跳
195.100.86.0	255.255.255.128	接口 0，直连 195.100.86.1
195.100.86.128	255.255.255.192	R2
195.100.86.192	255.255.255.192	R2

R2 路由表

目的网络	子网掩码	下一跳
195.100.86.128	255.255.255.192	接口 1，直连 195.100.86.129
195.100.86.192	255.255.255.192	接口 2，直连 195.100.86.193
195.100.86.0	255.255.255.128	R1

2009 年研究生入学考试计算机统考 408

一.单项选择题：每小题 2 分

答案速查：BBCAD　DCA

33．**B**【解析】考查 OSI 模型中传输层的功能。

传输层提供应用进程间的逻辑通信，即端到端的通信。而网络层提供点到点的逻辑通信。因此选 B。

34．**B**【解析】考查奈氏准则和香农定理。

采用 4 个相位，每个相位有 4 种幅度的 QAM 调制方法，每个信号可以有 16 种变化， 传输 4bit 的数据。根据奈奎斯特定理，信息的最大传输速率为 2×3kHz×4bit=24kbit/s。

35．**C**【解析】考查后退 N 帧协议的工作原理。

在后退 N 帧协议中，发送方可以连续发送若干个数据帧，如果收到接收方的确认帧则 可以继续发送。若某个帧出错，接收方只是简单的丢弃该帧及其后所有的后续帧，发送方超 时后需重传该数据帧及其后续的所有数据帧。这里要注意，连续 ARQ 协议中，接收方一般 采用累积确认的方式，即接收方对按序到达的最后一个分组发送确认，因此题目中收到 3 的确认帧就代表编号为 0、1、2、3 的帧已接收，而此时发送方未收到 1 号帧的确认只能代表确认帧在返回的过程中丢失了，而不代表 1 号帧未到达接收方。因此需要重传的帧为编号是 4、5、6、7 的帧。

36．**A**【解析】考查交换机的工作原理。

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。

37．**D**【解析】考查 CSMA/CD 协议的工作原理。

若最短帧长减少，而数据传输速率不变，则需要使冲突域的最大距离变短来实现争用期的减少。争用期是指网络中收发节点间的**往返时延**，因此假设需要减少的最小距离为 s，单 位为 m，则可以得到下式（注意单位的转换）: 2×[s/(2×108)]=800/(1×109), 因此可得 s=80，即最远的两个站点之间的距离最少需要减少 80m。

38．**D**【解析】考查 TCP 的数据编号与确认。

TCP 是面向字节流的，其选择确认（Selective ACK）机制是接收端对字节序号进行确认，其返回的序号是接收端下一次期望接收的序号，因此主机乙接收两个段后返回给主机甲的确认序列号是 1000。

39．**C**【解析】考查 TCP 的拥塞控制方法。

无论在慢开始阶段还是在拥塞避免阶段，只要发送方判断网络出现拥塞（其根据就是没有按时收到确认），就要把慢开始门限 ssthresh 设置为出现拥塞时的发送方窗口值的一半（但 不能小于 2）。然后把拥塞窗口 cwnd 重新设置为 1，执行慢开始算法。这样做的目的就是要 迅速减少主机发送到网络中的分组数，使得发生拥塞的路由器有足够时间把队列中积压的分 组处理完毕。

因此，在发送拥塞后，慢开始门限 ssthresh 变为 16KB/2=8KB，发送窗口变为 1KB。在 接下来的 3 个 RTT 内，拥塞窗口执行慢开始算法，呈指数形式增加到 8KB，此时由于慢开 始门限 ssthresh 为 8KB，因此转而执行拥塞避免算法，即拥塞窗口开始“加法增大”。因此 第 4 个 RTT 结束后，拥塞窗口的大小为 9KB。

40．**A**【解析】考查 FTP 协议的特点。

FTP 协议是基于传输层 TCP 协议的。FTP 的控制连接使用端口 21，用来传输控制信息（如连接请求，传送请求等）；数据连接使用端口 20，用来传输数据。

二.综合应用题

47.【解】**（1）**CIDR 中的子网号可以全 0 或全 1，但主机号不能全 0 或全 1。

因此若将 IP 地址空间 202.118.1.0/24 划分为 2 个子网，且每个局域网需分配的 IP 地址 个数不少于 120 个，子网号至少要占用一位。

由 26-2<120<27-2 可知，主机号至少要占用 7 位。

由于源 IP 地址空间的网络前缀为 24 位，因此主机号位数+子网号位数=8。综上可得主机号位数为 7，子网号位数为 1。

因此子网的划分结果为子网 1：202.118.1.0/25，子网 2：202.118.1.128/25。地址分配方案：子网 1 分配给局域网 1，子网 2 分配给局域网 2；或子网 1 分配给局域网 2，子网 2 分配给局域网 1。

【评分说明】①每个子网地址解答正确给 1 分，共 2 分；每个子网掩码解答正确给 1 分，共 2 分；②采用 CIDR

方式正确给出 2 个子网，亦给满分 4 分。

（2）由于局域网 1 和局域网 2 分别与路由器 R1 的 E1、E2 接口直接相连，因此在 R1 的路由表中，目的网络为局域网 1 的转发路径是直接通过接口 E1 转发的，目的网络为局域网 2 的转发路径是直接通过接口 E1 转发的。由于局域网 1、2 的网络前缀均为 25 位，因此它们的子网掩码均为 255.255.255.128。

根据题意，R1 专门为域名服务器设定了一个特定的路由表项，因此该路由表项中的子 网掩码应为 255.255.255.255。对应的下一跳转发地址是 202.118.2.2，转发接口是 L0。

根据题意，到互联网的路由实质上相当于一个默认路由，默认路由一般写作 0/0，即目 的地址为 0.0.0.0，子网掩码为 0.0.0.0。对应的下一跳转发地址是 202.118.2.2，转发接口是 L0。综上可得到路由器 R1 的路由表如下：

若子网 1 分配给局域网 1，子网 2 分配给局域网 2，见下表。

目的网络 IP 地址	子网掩码	下一跳 IP 地址	接口
202.118.1.0	255.255.255.128		E1
202.118.1.128	255.255.255.128		E2
202.118.3.2	255.255.255.255	202.118.2.2	L0
0.0.0.0	0.0.0.0	202.118.2.2	L0

若子网 1 分配给局域网 2，子网 2 分配给局域网 1，见下表。

目的网络 IP 地址	子网掩码	下一跳 IP 地址	接口
202.118.1.128	255.255.255.128		E1
202.118.1.0	255.255.255.128		E2
202.118.3.2	255.255.255.255	202.118.2.2	L0
0.0.0.0	0.0.0.0	202.118.2.2	L0

【评分说明】①上述 4 个路由项每正确解答一项给 1 分，共 4 分；②若路由表中的“接口”未使用接口名，而正确使用相应的 IP 地址，亦给分；到局域网 1、局域网 2 的两个路由项对应的“下一跳 IP 地址”为空白或填写“直接到达”等同义词，亦给分；③若每个路由表项部分解答正确，可酌情给分。

（3）局域网 1 和局域网 2 的地址可以聚合为 202.118.1.0/24，而对于路由器 R2 来说，通 往局域网 1 和局域网 2 的转发路径都是从 L0 接口转发，因此采用路由聚合技术后，路由器 R2 到局域网 1 和局域网 2 的路由，见下表。

目的网络 IP 地址	子网掩码	下一跳 IP 地址	接口
202.118.1.0	255.255.255.0	202.118.2.1	L0

【评分说明】①若路由表中的“接口”未使用接口名，而正确使用相应的 IP 地址，亦给分；②若该路由表项部分解答正确，可酌情给分。

2010 年研究生入学考试计算机统考 408

一.单项选择题

答案速查：CCDCB　DAA

33．**C**【解析】考查计算机网络体系结构的基本概念。

我们把计算机网络的各层及其协议的集合称为体系结构。因此 A、B、D 正确，而体系结构是抽象的，它不包括各层协议及功能的具体实现细节。

34．**C**【解析】考查存储转发机制。

由题设可知，分组携带的数据长度为 980B，文件长度为 980000B，需拆分为 1000 个分 组，加上头部后，

每个分组大小为 1000B，总共需要传送的数据量大小为 1MB。由于所有 链路的数据传输速度相同，因此文件传输经过最短路径时所需时间最少，最短路径经过 2 个分组交换机。当 t=1M×8/(100Mbit/s)=80ms 时，H1 发送完最后一个 bit。

由于传输延时，当 H1 发完所有数据后，还有两个分组未到达目的地，其中最后一个分 组，需经过 2 个分组交换机的转发，在两次转发完成后，所有分组均到达目的主机。每次转 发的时间为 t0=1K×8/(100Mbit/s)=0.08ms。

所以，在不考虑分组拆装时间和等待延时的情况下，当 t=80ms+2t0=80.16ms 时，H2 接收完文件，即所需的时间至少为 80.16ms。

35．**D**【解析】考查 RIP 路由协议。

R1 在收到信息并更新路由表后，若需要经过 R2 到达 net1，则其跳数为 17，由于距离 为 16 表示不可达，因此 R1 不能经过 R2 到达 net1，R2 也不可能到达 net1。B、C 错误，D 正确。而题目中并未给出 R1 向 R2 发送的信息，因此 A 也不正确。

36．**C**【解析】考查 ICMP 协议。

ICMP 差错报告报文有 5 种：终点不可达、源点抑制、时间超过、参数问题、改变路由（重定向），其中源点抑制是当路由器或主机由于拥塞而丢弃数据报时，就向源点发送源点 抑制报文，使源点知道应当把数据报的发送速率放慢。

37．**B**【解析】考查子网划分与子网掩码、CIDR。

由于该网络的 IP 地址为 192.168.5.0/24，因此其网络号为前 24 位。第 25～32 位为子网 位+主机位。而子网掩码为 255.255.255.248，其第 25～32 位的 248 用二进制表示为 11111000，因此后 8 位中，前 5 位用于子网号，后 3 位用于主机号。

RFC 950 文档规定，对分类的 IPv4 地址进行子网划分时，子网号不能为全 1 或全 0。但 随着无分类域间路由选择 CIDR 的广泛使用，现在全 1 和全 0 的子网号也可以使用了，但一 定要谨慎使用，要弄清你的路由器所有的路由选择软件是否支持全 0 或全 1 的子网号这种用法。但不论是分类的 IPv4 地址还是无分类域间路由选择 CIDR，其子网中的主机号均不能为全 1 或全 0。因此该网络空间的最大子网个数为 2^5=32 个，每个子网内的最大可分配地址个数为 2^3-2=6 个。

38．**D**【解析】考查网络设备与网络风暴。

物理层设备中继器和集线器既不隔离冲突域也不隔离广播域；网桥可隔离冲突域，但不隔离广播域；网络层的路由器既隔离冲突域，也隔离广播域；VLAN 即虚拟局域网也可隔离 广播域。对于不隔离广播域的设备，它们互连的不同网络都属于同一个广播域，因此扩大了 广播域的范围，更容易产生网络风暴。

39．**A**【解析】考查 TCP 流量控制与拥塞控制。

发送方的发送窗口的上限值应该取接收方窗口和拥塞窗口这两个值中较小的一个，于是此时发送方的发送窗口为 min{4000B, 2000B}=2000B，由于发送方还没有收到第二个最大段 的确认，所以此时主机甲还可以向主机乙发送的最大字节数为 2000B-1000B=1000B。

40．**A**【解析】考查 DNS 系统域名解析过程。

当采用递归查询的方法解析域名时，如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查 询请求报文，这种方法用户主机和本地域名服务器发送的域名请求条数均为 1 条。

二.综合应用题

47.【解】（1）当主机甲和主机乙同时向对方发送数据时，信号在信道中发生冲突后，冲突信号继续向两个方向传播。这种情况下两台主机均检测到冲突需要经过的时间最短，等于单程的传播时延 t0=2km/200000km/s=0.01ms。

主机甲（或主机乙）先发送一个数据帧，当该数据帧即将到达主机乙（或主机甲）时，主机乙（或主机甲）也

开始发送一个数据帧，这时，主机乙（或主机甲）将立刻检测到冲突，而主机甲（或主机乙）要检测到冲突，冲突信号还需要从主机乙（或主机甲）传播到主机甲（或主机乙），因此甲、乙两台主机均检测到冲突所需的最长时间等于双程的传播时延 2t0=0.02ms。

（2）主机甲发送一个数据帧的时间，即发送时延 t1=1518×8bit/(10Mbit/s)=1.2144ms；主机乙每成功收到一个数据帧后，向主机甲发送确认帧，确认帧的发送时延 t2=64×8bit/10Mbit/s=0.0512ms；主机甲收到确认帧后，即发送下一数据帧，故主机甲的发送周期 T=数据帧发送时延 t1+确认帧发送时延 t2+双程传播时延=t1+t2+2t0=1.2856ms；于是主机甲的有效数据传输率为 1500×8/T=12000bit/1.2856ms≈9.33Mbit/s（以太网有效数据为 1500B，即以太网帧的数据部分）。

2011 年研究生入学考试计算机统考 408

一.单项选择题

答案速查：ABBDD　CCB

33．**A**【解析】考查 TCP/IP 参考模型。

TCP/IP 的网络层向上只提供简单灵活的、无连接的、尽最大努力交付的数据报服务。 考查 IP 首部，如果是面向连接的，则应有用于建立连接的字段，但是没有；如果提供可靠 的服务，则至少应有序号和校验和两个字段，但是 IP 分组头中也没有（IP 首部中只是首部 校验和）。因此网络层提供的是无连接不可靠的数据服务。通常有连接、可靠的应用是由运 输层的 TCP 实现的。

34．**B**【解析】考查调制解调。

有 4 种相位，那么一个码元携带 $\log_2 4=2$（bit）信息，则波特率=比特率/2=1200 波特。

35．**B**【解析】考查选择重传协议。

选择重传协议中，接收方逐个地确认正确接收的分组，不管接收到的分组是否有序，只要正确接收就发送选择 ACK 分组进行确认。因此选择重传协议中的 ACK 分组不再具有累积确认的作用，要特别注意其与 GBN 协议的区别。此题中只收到 1 号帧的确认，0、2 号帧超时，由于对于 1 号帧的确认不具累积确认的作用，因此发送方认为接收方没有收到 0、2 号帧，于是重传这两帧。

36．**D**【解析】考查各种复用协议。

可采用排除法。首先 CDMA 即码分多址，是物理层的内容；CSMA/CD 即带冲突检测的载波监听多路访问，接收方并不需要确认；CSMA，既然 CSMA/CD 是其超集，是 CSMA/CD 没有的内容，CSMA 自然也没有。于是排除法选 D。CSMA/CA 是无线局域网标准 802.11 中的协议。CSMA/CA 利用 ACK 信号来避免冲突的发生，也就是说，只有当客户端收到网络上返回的 ACK 信号后才确认送出的数据已经正确到达目的地址。

37．**D**【解析】考查路由表。

要使 R1 能够正确将分组路由到所有子网，则 R1 中需要有到 192.168.2.0/25 和 192.168.2.128/25 的路由。网络 192.168.2.0/25 和 192.168.2.128/25 的网络号的前 24 位都相同，于是可以聚合成超网 192.168.2.0/24，故下一跳地址应该是 192.168.1.2。

38．**C**【解析】考查子网的性质。

首先分析 192.168.4.0/30 这个网络，主机号占两位，地址范围 192.168.4.0/30～ 192.168.4.3/30，即可以容纳（4-2=2）个主机。主机位为全 1 时，即 192.168.4.3，是广播地址，因此网内所有主机都能收到。

39．**C**【解析】考查 TCP 建立的三次握手。

主机乙收到连接请求报文后，如同意连接，则向甲发送确认。在确认报文段中应把 SYN 位和 ACK 位都置 1，确认号是甲发送的 TCP 段的初始序号 seq=11220 加 1，即为 ack=11221， 同时也要选择并消耗一个初始序号 seq，seq 值由主机乙的 TCP 进程确定，本题取 seq=11221， 它与确认号、甲请求报文段的序号没有任

何关系。

40．**B**【解析】考查 TCP 的确认机制。

TCP 首部的序号字段是指本报文段所发送的数据的第一个字节的序号。第三个段的序 号为 900，则第二个段的序号为 900-400=500，而确认号是期待收到对方下一个报文段的第一个字节的序号。现在主机乙期待收到第二个段，故甲的确认号是 500。

二.综合应用题

47.【解】（1）以太网帧的数据部分是 IP 数据报，只要数出相应字段所在的字节即可。由图 47-c 可知以太网帧头部有 6+6+2=14 字节，由图 47-d 可知 IP 数据报首部的目的 IP 地址字段前有 4×4=16 字节，从图 5-2 的帧第 1 字节开始数 14+16=30 字节，得目的 IP 地址 40.aa.62.20（十六进制），转换成十进制为 64.170.98.32。由图 5-3 可知以太网帧的前 6 字节 00-21-27-21-51-ee 是目的 MAC 地址，即为主机的默认网关 10.2.128.1 端口的 MAC 地址。

（2）ARP 协议用于解决 IP 地址到 MAC 地址的映射问题。主机的 AR 进程在本以太网以广播的形式发送 ARP 请求分组，在以太网上广播时，以太网帧的目的地址为全 1，即 FF-FF-FF-FF-FF-FF。

（3）HTTP/1.1 协议以持续的非流水线方式工作时，服务器在发送响应后仍然在一段时间内保持这段连接，客户机在收到前一个请求的响应后才能发出下一个请求。第一个 RTT 用于请求 Web 页面，客户机收到第一个请求的响应后（还有五个请求未发送），每访问一次对象就用去一个 RTT。故共需 1+5=6 个 RTT 后浏览器收到全部内容。

（4）私有地址和 Internet 上的主机通信时，须由 NAT 路由器进行网络地址转换，把 IP 数据报的源 IP 地址（本题为私有地址 10.2.128.100）转换为 NAT 路由器的一个全球 IP 地址（本题为 101.12.123.15）。因此，源 IP 地址字段 0a 02 80 64 变为 65 0c 7b 0f。IP 数据报每经过一个路由器，生存时间 TTL 值就减 1，并重新计算首部校验和。若 IP 分组的长度超过输出链路的 MTU，则总长度字段、标志字段、片偏移字段也要发生变化。

西北工业大学 2014 年研究生入学考试(879)

一、单选题（共 15 题，每题 2 分，满分 30 分）

答案速查：DCABB　　BABDD　　ACDBD

二、填空题(共 10 空,每空分,满分 10 分)

1.双绞线、同轴电缆和光导纤维(简称光纤)　　2.异步传输 同步传输　　3.ICMP SMTP　4.控制　　5.32　128

三、简答题(共 4 题,每题 5 分,满分 20 分)

1.面向连接服务和电话系统的工作模式相似,面向连接服务的主要特点:

1)数据传输过程必须经过连接建立、连接维护与释放连接三个阶段

2)在数据传输过程中,各个分组不需要携带目的节点的地址

3)传输连接类似一个通信管道,发送者在一端放入数据,接收者在另一端取出数据,传输的分组顺序不变,因此传输的可靠性好,但是协议复杂,通信效率不高

无连接服务与邮政系统服务的信件投递过程相似,无连接服务的主要特点是:

1)每个分组都携带源节点与目的节点地址,各个分组的转发过程是独立的

2)传输过程不需要经过连接建立、连接维护与释放连接三个阶段

3)目的主机接收的分组可能出现乱序、重复与丢失现象

无连接服务的可靠性不是很好,但是由于省去了很多协议处理过程,因此它的通信协议相对简单,通信效率比较高。

2.【解析】保护带宽=15MHZ*10%=1.5MHZ，n*(1.5+15)≤100，n≤6.06,n=6，可复用 6 路信号。

3.握手的作用：防止报文段在传输连接建立过程中出现差错。通过三次握手，通信双方的进程之间就建立了一条传输连接，然后就可以使用全双工的方式在该传输链接上正常的传输数据报文段了；可以解决被延迟的分组问题，从而可以保证数据交换的安全和可靠

三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,也要允许双方就初始序列号进行协商。

【补充①】为什么一定进行三次握手？当客户端向服务器端发送一个连接请求时，由于某种原因长时间驻留在网络节点中，无法达到服务器端，由于 TCP 的超时重传机制，当客户端在特定的时间内没有收到服务器端的确认应答信息，则会重新向服务器端发送连接请求，且该连接请求得到服务器端的响应并正常建立连接，进而传输数据，当数据传输完毕，并释放了此次 TCP 连接。若此时第一次发送的连接请求报文段延迟了一段时间后，到达了服务器端，本来这是一个早已失效的报文段，但是服务器端收到该连接请求后误以为客户端又发出了一次新的连接请求，于是服务器端向客户端发出确认应答报文段，并同意建立连接。如果没有采用三次握手建立连接，由于服务器端发送了确认应答信息，则表示新的连接已成功建立，但是客户端此时并没有向服务器端发出任何连接请求，因此客户端忽略服务器端的确认应答报文，更不会向服务器端传输数据。而服务器端却认为新的连接已经建立了，并在一直等待客户端发送数据，这样服务器端一直处于等待接收数据，直到超出计数器的设定值，则认为服务器端出现异常，并且关闭这个连接。在这个等待的过程中，浪费服务器的资源。如果采用三次握手，客户端就不会向服务器发出确认应答消息，服务器端由于没有收到客户端的确认应答信息，从而判定客户端并没有请求建立连接，从而不建立该连接。

挥手的作用：拆除时防止一方再发送信息（可将补充中的相关内容做适当的补充）。

三次握手法能够有效地保证建立和释放连接的安全性和可靠性，因而被很多传输层协议所采用。

【补充②】为什么 TCP 挥手要比握手多一次？因为当处于 LISTEN 状态的服务器端收到来自客户端的 SYN 报文(客户端希望新建一个 TCP 连接)时，它可以把 ACK(确认应答)和 SYN(同步序号)放在同一个报文里来发送给客户端。但在关闭 TCP 连接时，当收到对方的 FIN 报文时，对方仅仅表示对方已经没有数据发送给你了，但是你自己可能还有数据需要发送给对方，则等你发送完剩余的数据给对方之后，再发送 FIN 报文给对方来表示你数据已经发送完毕，并请求关闭连接，所以通常情况下，这里的 ACK 报文和 FIN 报文都是分开发送的。

【注】西工大使用的网络教材是蔡皖东版本的，是三次握手和三次挥手，而目前使用较为广泛的是三次握手、四次挥手的过程。

4. (1) 主机相互通信时，首先要知道对方 IP 地址所对应的硬件地址才能在物理网络上进行传输。 (2) 地址解析通过 ARP 协议完成。

四、答案仅供参考，也可以有其它的划分方式。

	网络号	子网掩码	可用 ip 地址段	直接广播地址
A	202.116.75.192	255.255.255.224	202.116.75.193-202.116.75.222	255.255.255.223
B	202.116.75.224	255.255.255.224	202.116.75.225-202.116.75.244	255.255.255.255
C	202.116.75.128	255.255.255.192	255.255.255.129-255.255.255.178	255.255.255.191

西北工业大学 2015 年研究生入学考试(879)

一、选择题

答案速查：CBCBD　BBBAA　DBABA

5.D【解析】IEEE802.1 标准，定义了局域网体系结构、网络互联，以及网络管理与性能测试；IEEE802.2 标准，定义了逻辑链路控制（LLC）子层的功能与服务；IEEE802.3 标准，定义了 CSMA/CD 总线介质访问控制子层和物理层规范；IEEE802.4 标准，定义了令牌总线（Token Bus）介质访问控制子层与物理层规范。

二、判断题（每题 1 分，共 10 分）

1.×【解析】差错控制　　2.×【解析】1/2　　3.√　　4.√
5.×【解析】模拟转数字　　6.√【解析】修改为-每个数据字节　　7.×
8.√　　9.×【解析】21　　10.×【解析】HTTP

三、简答题

1.Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

Tracert 命令功能同 Ping 类似，但它所获得的信息要比 Ping 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。该命令比较适用于大型网络。

Tracert 先发送 TTL 为 1 的回应数据包，当数据包上的 TTL 在路由器收到后 TTL 自动减 1 ，一旦某个服务器将 TTL 减 1 后，等于了 0，路由器应该将“ICMP Time Exceeded”的消息发回源计算机，源计算机就根据收到的信息判断达到的路由器和所用时间。下次再次发送数据包时，将 TTL 递增 1，继续上述测试，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 Tracert 实用程序中看不到，我们会显示请求超时的请求信息。

2.静态路由选择算法也叫做非自适应路由选择算法，其特点是简单和开销较小，但不能及时适应网络状态的变化；动态路由选择算法也叫做自适应路由选择算法，其特点是能够较好的适应网络状态的变化，但实现起来较为复杂，开销也比较大。

3.见《西北工业大学软微学院未知年份试题一》四简答题 5 小题

4.每个子网最多有 30 台主机，2^5=32，故主机位为 5 位，网络位为 27 位，子网掩码为 255.255.255.224
子网掩码可屏蔽 IP 地址中的主机号，而保留网络号与子网号，用于说明 IP 地址中子网的位置。

5.虚电路交换技术的主要特点：在数据传输之前必须通过虚呼叫设置一条虚电路。它适用于两端之间长时间的数据交换。
优点：可靠、保持顺序； 缺点：如有故障，则经过故障点的数据全部丢失.

四、计算题

1.在一个 C 类网络中，主机号共有 8 位，可实际分配的 IP 地址共有 254 个。因此对于 2000 台主机，2000/254≈7.874，取整数为 8，必须为该公司分配 8 个 C 类网络。

由于需要 8 个 C 类网络，2^3=8，因此需要向网络号借用 3 个比特位用作主机号，其对应的子网掩码二进制表示为 1111 1111.1111 1111.1111 1000.0000 0000，即 255.255.255.248。

2.见《西北工业大学 2007 年考试》四应用题 2 小题

西北工业大学 2016 年研究生入学考试(879)

一.单项选择题(每小题 2 分，共 20 分)

答案速查：ABCDA　CBDBB　BCCAD

1.A【解析】曼彻斯特编码的好处有两个：**自同步**和**差错控制**。

5.A【解析】虚电路表示这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方式传送，而并不是真正建立了一条物理连接 。包括建立连接，传输数据，拆除连接三个阶段。建立连接之后就类似于专线，所以不存在路由选择。

8.D【解析】集线器是物理层，中继器是物理层，交换机工作在数据链路层，路由器工作在网络层。

9.B【解析】如果是一台主机，则使用 IP 地址 来表示，如 202.118.0.200；如果是主机上的应用，则使用主机的 IP 地址 加上应用使用的端口号 来表示，如 202.118.0.200::23。

12.C【解析】在 TCP/IP 协议簇中，地址转换协议(ARP)及反向地址转换协议(RARP)的协议数据单元(PDU)均封装在以太网的数据帧中传送，实现 IP 地址与 MAC 地址之间的相互转换。

13.C【解析】若路由器或目的主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发送一个 ICMP 源抑制报文，此时，源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到将发生拥塞，则发送源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目的主机。

当一台主机向自己的默认网关发送一个需要转发的数据包时，如果该网关路由器查找路由表发现有更好的路由，就会向源主机发出“重定向”的 ICMP 报文。

如果在 IP 数据报的传送过程中，路由器发现网络出现拥塞，则路由器将向源主机发出“目标不可到达”的 ICMP 报文。

一个 IP 包从源节点出发时，其 TTL 值被设定一个初始值(比如 255)，经过一跳一跳的传输，如果这个 IP 包的 TTL 降低到零，路由器就会丢弃此包。此时，该路由器上的 ICMP 便会发出一个“超时(time exceeded)”的 ICMP 报文。

二.填空题

1.电路交换 报文交换 分组交换　2.20Mbps　3.IP　4.异步传输 同步传输　5.发送 接收　6.ICMP

三.简答题

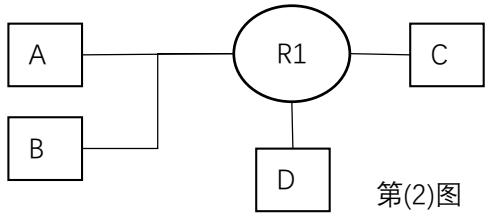
1.静态路由算法简单、可靠，在负荷稳定、拓扑变化不大的网络中效果很好，广泛用于均是系统和较小的商业网络；动态路由算法能改善网络的性能并有助于流量控制，但算法复杂，会增加网络的负担，有时会因变化过快而引起震荡。动态路由算法使用路由选择协议发现和维护路由信息，而静态路由算法只需要手动配置路由信息。

常用的动态路由算法有：距离-向量路由算法和链路状态路由算法；静态路由算法有：泛射路由选择、固定路由选择、随机路由选择。

2.见《西北工业大学软微未知年份真题二》三简答题 3 小题
3.见《西北工业大学 2015 年研究生入学考试》三简答题 3 小题
4. IPv4 地址如果只使用有类（A、B、C 类）来划分，会造成大量的浪费或者不够用，为了解决这个问题，可以在有类网络的基础上，通过对 IP 地址的主机号进行再划分，把一部分划入网络号，就能划分各种类型大小的网络了；

子网掩码的作用：可屏蔽 IP 地址中的主机号，从而分离 IP 地址中的网络部分与主机部分，用于说明 IP 地址中子网的位置，管理员可将网络进一步划分为若干子网。

四.应用题



第(2)图

(1)205.118.20.96　205.118.20.160　205.118.20.127　205.118.20.223
(2)A 和 B 可以直接通信，AB、C 和 D 之间需要通过路由器转发才能通信。
(3)205.118.20.161~205.118.20.189
(4)将 A、B、C、D 的 IP 地址范围设在 205.118.20.97~205.118.20.126

西北工业大学 2017 年研究生入学考试(879)

一.单项选择题(每小题 2 分，共 20 分)

答案速查：BCCCA　BBB

1.B【解析】 IPv6 的 128 位地址采用冒号十六进制表示法表达，即按每 16 位划分为 1 个位段，每个位段被转换为 1 个 4 位的十六进制数，并用冒号":"隔开。IPv6 的 128 位地址最多可被划分为 8 个位段，而选项 B 的"21DA:0:0:0:0:2A:F:F=E08:3"共有 9 个位段，因此选项 B 是地址表示是错误的。
IPv6 不支持子网掩码，它只支持前缀长度表示法。前缀是 IPv6 地址的一部分，用做 1Pv6 路由或子网标识。前缀的表示方法与 IPv4 中的无类域间路由 CIDR 表示方法基本类似。IPv6 前缀可以用"地址/前缀长度"来表示。例如，选项 C 的"21BC::0:0:1/48"。
2.C【解析】在发送方和接收方之间建立一条逻辑连接的虚电路，这点上虚电路方式和电路交换方式是相同的。
4.C【解析】各层协议总结如下：

物理层	RJ45 、 CLOCK 、 IEEE802.3 （中继器，集线器）
数据链路	PPP 、 FR 、 HDLC 、 VLAN 、 MAC （网桥，交换机）
网络层	IP 、 ICMP 、 ARP 、 RARP 、 OSPF 、 IPX 、 RIP 、 IGRP 、（路由器）
传输层	TCP 、 UDP 、 SPX（网关）
会话层	NFS 、 SQL 、 NETBIOS 、 RPC
表示层	JPEG 、 MPEG 、 ASII
应用层	FTP , DNS，Telnet , SMTP，HTTP , WWW , NFS，SNMP

6.B【解析】从子网掩码可以看到，前 27 位为网络号，因此我们重点关注后 5 位。A 项 63=0011 1111，后 5 位全 1，不能作为主机地址；B 项 93=0101 1101，后 5 位不全 0 全 1，可以作为主机地址；同理，C 项 159=1001 1111，D 项 192=1100 0000，后 5 位是全 0 或 1，因此也不能作为主机地址。
7.B【解析】 IP 地址由 4 个字节组成(32 bit)，采用点分十进制标记法，即 X.X.X.X 的形式，用 4 个十进制数来对应表示 4 个字节的二进制数值，数值中间用"."隔开。每个十进制数的取值在 0 ~ 255 之间。由于 A 类地址中

首位为 0，所以其第 1 个十进制数的取值范围被限定于 1 ~ 126 之间(0 和 127 另有指定)。同理，B 类地址中第 1、2 位为 10，第 1 个十进制数的取值范围被限定于 128 ~ 191 之间。 C 类地址中第 1、2、3 位为 110，第 1 个十进制数的取值范围被限定于 192 ~ 223 之间。据此，可以判断 B 正确。

8.B【解析】因为要解决“理论上相距的最远距离”，那么最远肯定要保证能检测到碰撞，而以太网规定最短帧长为 64B，其中 Hub 为 100Base-T 集线器，可知线路的传输速率为 100Mb/s，则单程传输时延为 64B÷100Mb/s÷2=2.56us, 又 Hub 在产生比特流的过程中会导致延时 1.535us, 则单程的传播时延为 2.56us-1.535us=1.025us, 从而 H3 与 H4 之间理论上可以相距的 最远距离为 200m/us*1.025us=205m。

二.简答题(每小题 6 分，共 30 分)

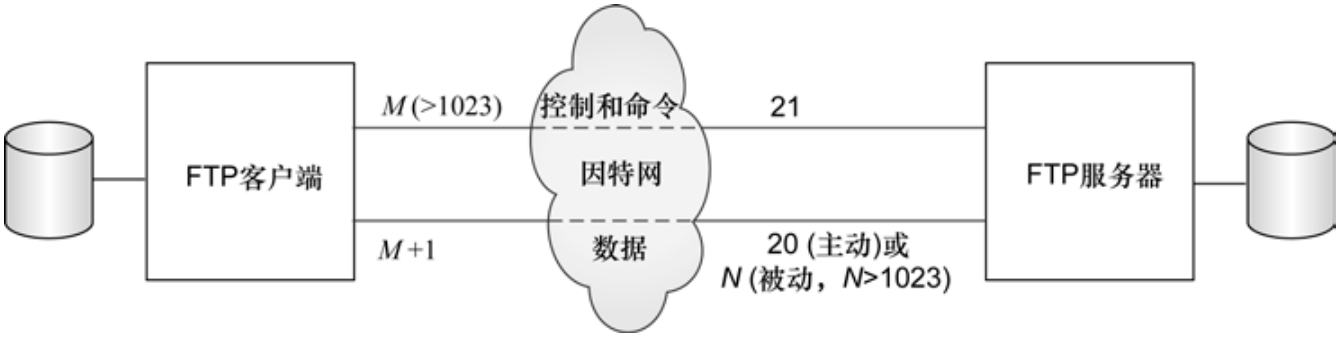
1.见《西北工业大学软微学院未知年份试题二》三简答题 2 小题

2.见《西北工业大学期末考试(软微学院)》三简答题 5 小题

3.见《西北工业大学 2007 年考试》三简答题 7 小题

4.FTP 是 File Transfer Protocol（文件传输协议）的英文简称，它基于传输层协议 TCP 建立，用于 Internet 上文件的双向传输（上传和下载）。与大多数 Internet 服务一样，FTP 也是一个客户端/服务器系统，要想完成文件传输需要 FTP 服务端和 FTP 客户端的配合。

FTP 协议使用了两条 TCP 连接，一条是命令链路，用于在 FTP 客户端与服务器之间传递命令；另一条是数据链路，用来上传或下载数据。FTP 服务器/客户端架构如图所示：



FTP 协议有两种工作方式：PORT 主动方式和 PASV 被动方式。无论哪种工作方式，首先都需要客户端主动与远程主机上的 FTP 服务器建立命令链路。

PORT 方式的连接过程：客户端从一个任意的非特权端口 M（M>1023，0 到 1023 用于绑定特定的服务）向 FTP 服务器的命令端口（默认是 21）发送连接请求，服务器接受连接，建立一条命令链路。当需要传送数据时，客户端在命令链上发送 FTP 命令“port M+1”到 FTP 服务器。接着客户端开始监听端口 M+1，服务器会从它自己的数据端口（默认是 20）连接到客户端指定的数据端口（M+1），建立一条数据链路来传送数据。

在 PASV 方式中，命令连接和数据连接都由客户端发起，当开启一个 FTP 连接时，客户端打开两个任意的非特权本地端口（ M > 1023 和 M +1）。第一个端口连接服务器的 21 端口建立一条命令链路，与 PORT 方式相同，但第二个端口建立数据链路的方式与 PORT 方式有所不同。当需要传送数据时，客户端提交 PASV 命令至服务器，这样做的结果是服务器会开启一个任意的非特权端口（N > 1023），并发送 PASV N 命令给客户端。于是客户端发起从本地端口 M+1 到服务器的端口 N 的连接，建立一条数据链路用来传送数据。

由于使用 FTP 传送文件时必须先登录，在远程主机上获得相应的权限以后，才可上传和下载文件。除非有用户 ID 和口令，否则便无法传送文件。Internet 上的 FTP 主机成千上万，不可能要求每个用户在每一台主机上都拥有帐号，这违背了 Internet 的开放性。于是产生了匿名 FTP 来解决这个问题。

通过匿名 FTP 机制，用户无需注册帐号就可以连接到远程主机上进行文件的上传和下载。系统管理员建立了一个特殊的用户 ID，名为 anonymous, Internet 上的任何人在任何地方都可使用该用户 ID。

5.$2^4<30<2^5$；$2^3<14<2^4$;因此第一个子网的主机位为 5 位，第二、三个子网的主机位为 4 位，C 类地址的网络号为 24 位，因此第一个子网的子网掩码为 255.255.255.224，第二、三个子网的子网掩码为 255.255.255.240

三.应用题(15 分)

1.能 ping 通 ip 则代表链路是通的，但是 ping 不通域名只能说明是域名解析出现了问题。
解决方案：①使用 nslookup 命令查看 dns 是否配置，未配置设置下 dns，使用 8.8.8.8 或 114.114.114.114 或其他；②使用 ipconfig /flushdns 刷新下 dns 缓存。
2.略

西北工业大学 2018 年研究生入学考试(879)

一.单选题（2*10 分）

答案速查：DABCD　　CDABC

5.D【解析】IPv4 地址采用 32 位的点分四段十进制表示，而 IPv6 采用的是 128 位的冒分八段十六进制法。例如：2031:0000:1F1F:0000:0000:0100:11A0:ADDF。为了简化其表示法，RFC2373 提出每段中前面的 0 可以省略，连续的 0 可省略为"::"，但只能出现一次，例如：1080:0:0:0:8:800:200C:417A 可以简写为 1080::8:800:200C:417A。类似于 IPv4 中的 CDIR 表示法，IPv6 用前缀来表示网络地址空间，比如：2001:250:6000::/48 表示前缀为 48 位的地址空间。而 D)选项中的 FF34：42：BC：：0：50F:21:0:03D 已经超过 8 段，所以表示错误，答案选择 D。
10.C【解析】在后退 N 帧的协议中，序列号个数 > =MAX_SEQ+1，在题目中发送窗口的大小是 32，那么序列号个数最少应该是 33 个。所以最少需要 6 位的序列号才能达到要求。

二.简答题（5*6 分）

1.

	虚电路服务	数据报服务
思路	可靠通信应该由网络保障	可靠通信应该由用户主机来保障
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	属于同一虚电路的分组均按同一路由转发	每个分组独立选择路由进行转发
节点出现故障	所有通过出故障的节点的虚电路均不能工作	出故障的节点可能会丢失分组，一些路由可能出现变化
分组顺序	总是按发送顺序到达终点	到达终点的时间，不一定按照发送顺序
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

2.(1)报文复杂性：LS 算法：O（nE），n 为网络中节点数，E 是链路数，而且当每一条链路的费用发生变化时，必须将该新的链路费用发向所有节点；
DV 算法：当链路费用发生变化时，DV 算法仅当在新的链路费用导致与该链路相联的节点的最低费用路径发生变化时，才传播已改变的链路费用。
(2)收敛速度：LS 算法：O（n^2）；
DV 算法：收敛较慢（取决于相关的路径费用），且在收敛时会遇到选路回环。DV 算法还会遇到计数到无穷的问题。

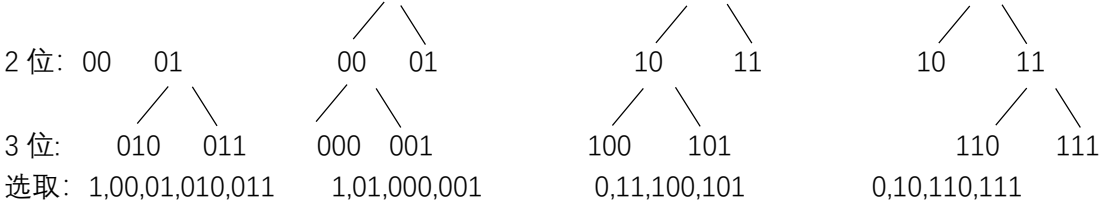
(3)健壮性：LS 算法：路由计算有相对的独立性，提供了一定的健壮性；
DV 算法：一个节点可向任意或所有目的节点发布其不正确的最低费用路径，这会引起其他路由器将大量通信流向故障路由器，并导致大部分网络连接中断。更一般地，DV 算法中一个节点的计算值会在每次迭代时传递给它的邻居，然后在下次迭代时再传给邻居的邻居。在此情况下，DV 算法中一个不正确的节点计算值会扩散到整个网络。
总之，没有一个算法对另一个算法而言是"胜利者"。两个算法都在网络上得到了应用。
3.见《西北工业大学 2015 年研究生入学考试(879)》四计算题 2 小题
4.见《西北工业大学 2014 年研究生入学考试(879)》三简答题 3 小题
5.子网就是将主机地址的几位用来做网络地址来将网络划分为若干个子网，便于管理还能减少 IP 的浪费。
子网的出现是基于以下原因：
节约 IP 资源：随着互联的发展 IPV4 地址资源可能会耗尽，如果不划分子网直接将一个 C 类地址分给一个企业，C 类地址可容纳 256 台主机，但是可能该企业只有 20 台计算机，这就造成极大浪费
减少网络流量，优化网络性能：隔离数据在整个网络内广播，提高信息传输速率。
子网掩码：又叫网络掩码，它是一种用来指明一个 IP 地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的位掩码。子网掩码不能单独存在，必须配合 IP 使用。
用途：通过子网掩码计算出一台主机所在的子网和其他网络的关系，进行正确的通信。

三.综合题（25 分）

1.由题设可知，分组携带的数据长度为 980B，文件长度为 980000B，需要拆分为 1000 个分组，加上头部之后，每个分组大小为 1000B，总共需要传送的数据量大小为 1MB。由于所有的数据传输速率相同，因此文件传输经过最短路径时所需时间最少，最短路径经过分组交换机。
当 t=1M*8/100Mbps = 80ms 时，H1 发送完最后一个比特；
到达目的地，最后一个分组，需经过 2 个分组交换机的转发，每次转发的时间为 t0 = 1K×8/100Mbps = 0.08ms，所以，在不考虑分组拆装时间和传播延时的情况下，当 t = 80ms + 2t0= 80.16ms 时，H2 接受完文件，即所需的时间至少为 80.16ms。
2.【解析】由题可知，如果采用等分子网的话，四个部门子网号要占 2 位，则主机号为 6 位，2^6最多可划分 62 个主机，无法满足工程技术部 100 台主机的要求，故应考虑子网号不等长，又因为最后 8 比特要满足 工程技术部<市场部<财务部<行政部，且最少的部门主机也有 25 台，需占用 5 位，则工程技术部、市场部、财务部和行政部的子网号应取 0、10、110、111，刚好可以满足各部门的主机数量，这都是出题人给你精心凑好的。

部门	可分配的IP地址范围	子网掩码(网络号和子网号 1)	网络地址(主机号全 0)	直接广播地址(主机号全 1)
工程技术部(0)	200.200.200.1-200.200.200.126	(2)255.255.255.128	(3)200.200.200.0	(4)200.200.200.127
市场部(10)	(5)200.200.200.129-200.200.200.190	(6)255.255.255.192	(7)200.200.200.128	(8)200.200.200.191
财务部(110)	(9)200.200.200.193-200.200.200.222	(10)255.255.255.224	(11)200.200.200.192	(12)200.200.200.223
行政部(111)	(13)200.200.200.225-200.200.200.254	(14)255.255.255.224	(15)200.200.200.224	(16)200.200.200.255

【注】很多同学也提到了子网划分应该按照什么原则，在此一并作答。在等长子网中如果是 1 位，则为 0,1；如果是 2 位，则为 00,01,10,11 这样的顺序。当然 0、1 你怎么使用都不会算作错，但是在非等长子网中按照上题这样划分可以最大程度避免重复问题，即"不重复原则"，一般按照：
1 位：　0　　1　　0　1　　0　1　　0　1



来选取，如第四组，取 0,10,110,111，若你取 01 的话，很可能读到第一位时为 0，以为还是 0 这一个子网，会产生重复的错误，所以要尽量避免与前面子网的重复

西北工业大学 2019 年研究生入学考试(879)

一、选择题（每题 2 分，共 10 题）

答案速查：CBCBA CCBDB

9.D【解析】TFTP（Trivial File Transfer Protocol,简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。端口号为 69。

二、简答题（共 40 分）

1.①在浏览器中输入 www.vedio.com 域名，操作系统会先检查自己本地的 hosts 文件是否有这个网址映射关系，如果有，就先调用这个 IP 地址映射，完成域名解析；

②如果 hosts 里没有这个域名的映射，则查找本地 DNS 解析器缓存，是否有这个网址映射关系，如果有，直接返回，完成域名解析；

③如果 hosts 与本地 DNS 解析器缓存都没有相应的网址映射关系，首先会找 TCP/ip 参数中设置的首选 DNS 服务器，在此我们叫它本地 DNS 服务器，此服务器收到查询时，如果要查询的域名，包含在本地配置区域资源中，则返回解析结果给客户机，完成域名解析，此解析具有权威性；

④如果要查询的域名，不由本地 DNS 服务器区域解析，但该服务器已缓存了此网址映射关系，则调用这个 IP 地址映射，完成域名解析，此解析不具有权威性；

⑤如果本地 DNS 服务器本地区域文件与缓存解析都失效，则根据本地 DNS 服务器的设置（是否设置转发器）进行查询，如果未用转发模式，本地 DNS 就把请求发至 13 台根 DNS，根 DNS 服务器收到请求后会判断这个域名(.com)是谁来授权管理，并会返回一个负责该顶级域名服务器的一个 IP。本地 DNS 服务器收到 IP 信息后，将会联系负责.com 域的这台服务器。这台负责.com 域的服务器收到请求后，如果自己无法解析，它就会找一个管理.com 域的下一级 DNS 服务器地址(vedio.com)给本地 DNS 服务器。当本地 DNS 服务器收到这个地址后，就会找 vedio.com 域服务器，重复上面的动作，进行查询，直至找到 www.vedio.com 主机；

⑥如果用的是转发模式，此 DNS 服务器就会把请求转发至上一级 DNS 服务器，由上一级服务器进行解析，上一级服务器如果不能解析，或找根 DNS 或把转请求转至上上级，以此循环。不管是本地 DNS 服务器用是是转发，还是根提示，最后都是把结果返回给本地 DNS 服务器，由此 DNS 服务器再返回给客户机。

2.①工作层次

集线器工作在物理层，属于 1 层设备，每发送一个数据，所有的端口均可以收到，采用了广播的方式，因此网络性能受到很大的限制。

交换机工作在数据链路层，属于 2 层设备，通过学习之后，每个端口形成一张 MAC 地址转发表，根据数据包的 MAC 地址转发数据，而不是广播形式。

②转发方式

集线器的工作原理是广播形式，无论哪个端口收到数据之后，都要广播到所有的端口，当接入设备比较多时，网络性能会受到很大的影响。

交换机根据 MAC 地址转发数据，收到数据包之后，检查报文的目的 MAC 地址，找到对应的端口进行转发，而不是广播到所有的端口。

③传输模式

集线器内部采用了总线型拓扑，各个节点共用一条总线进行通信，数据包的发送和接收采用了 CSMA/CD 协议，在同一时间内必须是单向的，只能维持在半双工模式下。两个端口不能同时收发数据，并且当两个端口通信时，其他端口不同工作。

当交换机上的两个端口通信时，它们之间的通道是相互独立的，可以实现全双工通信。两个端口同时收发数据。

④带宽影响

集线器无论有多少个端口，所有的端口共享一条宽带，同一时刻只能有两个端口传输数据，并且只能工作在半双工模式下。

交换机的每个端口独占带宽，两个端口交互数据并不影响其他端口交换数据。总结如下：

	交换机	集线器
工作层次	数据链路层	物理层
带宽影响	独享	共享
数据传输	有目的发送	广播发送
传输模式	全双工或半双工	半双工

3.(1)TCP 是面向连接的，UDP 是面向无连接的

TCP 在通信之前必须通过三次握手机制与对方建立连接，而 UDP 通信不必与对方建立连接，不管对方的状态就直接把数据发送给对方

(2)TCP 连接过程耗时，UDP 不耗时

(3)TCP 连接过程中出现的延时增加了被攻击的可能，安全性不高，而 UDP 不需要连接，安全性较高

(4)TCP 是可靠的，保证数据传输的正确性，不易丢包，UDP 是不可靠的，易丢包

(5)TCP 传输速率较慢，实时性差，UDP 传输速率较快

TCP 建立连接需要耗时，并且 TCP 首部信息太多，每次传输的有用信息较少，实时性差

(6)TCP 是流模式，UDP 是数据包模式

TCP 只要不超过缓冲区的大小就可以连续发送数据到缓冲区上，接收端只要缓冲区上有数据就可以读取，可以一次读取多个数据包，而 UDP 一次只能读取一个数据包，数据包之间独立

TCP/UDP 的使用场合

(1)对数据可靠性的要求。TCP 适用于可靠性高的场合，UDP 适用于可靠性低的场合。

(2)应用的实时性。TCP 有延时较大，UDP 延时较小。

(3)网络的可靠性。网络不好的情况下使用 TCP，网络条件好的情况下，使用 UDP。

4.子网就是将主机地址的几位用来做网络地址来将网络划分为若干个子网，便于管理还能减少 IP 的浪费。

子网的出现是基于以下原因：

(1)节约 IP 资源：随着互联的发展 IPV4 地址资源可能会耗尽，如果不划分子网直接将一个 C 类地址分给一个企业，C 类地址可容纳 256 台主机，但是可能该企业只有 20 台计算机，这就造成极大浪费

(2)减少网络流量，优化网络性能：隔离数据在整个网络内广播，提高信息传输速率。

子网掩码：又叫网络掩码，它是一种用来指明一个 IP 地址的哪些位标识的是主机所在的子网，以及哪些位标识的是主机的位掩码。子网掩码不能单独存在，必须配合 IP 使用。

用途：通过子网掩码计算出一台主机所在的子网和其他网络的关系，进行正确的通信。

5.(1)假定从下往上把 3 层楼编号为 1-3 层。在星形网中，集线器放在 2 层中间位置（第 4 间房）。电缆总程度等于：

$$5\sum_{i=1}^{3}\sum_{j=1}^{7}\sqrt{(i-2)2+(j-4)2}$$

(2)对于总线式以太网（如 10BASE2），每层需 5×6=30（m）水平电缆，垂直电缆需 5×2=10（m），所以总长度等于 3×30+10=100（m）

三、（1）1. 201.18.10.96　2. 201.18.10.127　3. 201.18.10.160　4. 201.18.10.223

（2）A 和 B 可以直接通信，C 与 D 之间通信需要路由器，C 或 D 与 A 或 B 通信也需要路由器

（3）要求加入计算机 E，与 D 通信。D 其 IP 地址的第四个字节的范围：11000001~11011110，而 D 的 IP 地址的第四个字节为 11011110，再考虑留一个 IP 地址给路由器 (201.18.10.221)，第四个字节为(11011101)，所以，E 的 IP 地址的第四个字节的范围：11000001~11011100

E 的 IP 地址范围是 201.18.10.193~201.18.10.220

西北工业大学 2020 年研究生入学考试(879)

一.选择题(每小题 2 分，共 20 分)

答案速查：BBDBA

二.简答题(每小题 10 分，共 40 分)

1.答:局域网的特点是: 1)较小的地域范围; 2)传输速率高,误码率低; 3)通常为一个单位所建,并自行管理和使用; 4)可使用的传输介质较丰富； 5)较简单的网络拓扑结构； 6)有限的站点数量。

CSMA/CA 协议与 CSMA/CD 协议都规定，节点在发送数据前，需要先进行载波侦听，查看媒体是否空闲。它们的主要区别在于 CSMA/CA 在媒体空闲后，还要等待一个随机的时间（随机退避）才发送，使信号碰撞发生的概率减到最小。而 CSMA/CD 协议中，是在发生冲突后才进行退避。另外，为了保证 CSMA/CA 协议的健壮性，使偶尔还可能发生的碰撞不会破坏协议的工作，CSMA/CA 设置了专门的 ACK 应答帧，用来指示碰撞的发生。接收节点需要发送 ACK 帧来告诉发送者数据帧是否原封不动到达了目的地，一旦发生碰撞，接收节点接收不到正确的数据帧，发生者就不会收到 ACK。

无线局域网中不采用了 CSMA/CD 协议的主要原因是无线局域网的网卡实现对信道是否存在碰撞进行检测十分困难，要检测到一个碰撞，无线网卡必须能够在发射时同时进行监测，但在高频无线电子电路中实现这样一种硬件十分昂贵，很不实际。

2.【解】整个传输过程的总时延=连接建立时延+源点发送时延+中间节点的发送时延+中间节点的处理时延+传播时延。

虚电路的建立时延已给出，为 s 秒。

源点要将 L 比特的报文分割成分组，分组数=L / p，每个分组的长度为(h+p)比特，源点要发送的数据量=(h+p)L / p 比特，所以源点的发送时延=(h+p)L / (pb)秒。

每个中间节点的发送时延=(h+p) / b 秒，源点和终点之间的线路数为 k，所以有 k-1 个中间节点，因此中间节点的发送时延=(h+p)(k-1) / b 秒。

中间节点的处理时延 m(k-1)秒。传播时延=kd 秒。

所以，源节点开始发送数据直到终点收到全部数据所需要的时间=s+(h+p)L / (pb)+(h+p)(k-1) / b+m(k-1)+kd 秒。

【举一反三】1.假定 x 比特的用户数据需要以一系列分组的形式，沿一条 k 跳的路径在分组交换网中传输。每个分组包含 p 比特数据和 h 比特报头，x>>(p+h)。线路的数据传输速率为每秒 b 比特，传输延迟时间忽略不

计。问 p 取什么值时，用户数据总的传输延迟时间最小。

【解】已知用户数据的长度为 x 比特，每个分组的数据部分长度为 p 比特，所以需要的分组总数是 x/p。每个分组的报头长度为 h 比特，因此需要传送的分组总长度为(p+h)x/p 比特。

源端发送(p+h)x/p 比特的数据需要的时间为((p+h)x/p)/b=(p+h)x/(pb)秒

最后一个到达目的地的分组必须经过中间路由器的(k-1)次转发，每次转发需要的时间为(p+h)/b

因此，用户数据总的传输时延为(p+h)x/(pb)+(k-1)(p+h)/b

对该函数求 p 的导数，得到(p-(p+h)x)/(p2b)+(k-1)/b

令(p-(p+h)x)/ (p2b)+(k-1)/b=0 得到 hx/p2=k-1。t=(k-1+x/p)*(p+h)/b，t'=(-x(p+h)+(k-1)p^2+px)/((p^2)*b)

因为 p>0，所以 p=(hx/(k-1))^(1/2)。因此，当 p=(hx/(k-1))^(1/2)时用户数据总的传输时延最小。

3.在 UDP 首部中：源端口占 2 个字节，即 06 32 ，化为十进制是 1586。（下面括号外数字代表进制）

(06 32)16=(00000110 00110010)$_2$=2+16+32+512+1024=(1586)10

或者直接用 16 进制转为十进制：(06 32)16=0x16^3+6x16^2+3x16^1+2x16^0=1536+48+2=1586

目的端口占 2 个字节，即 00 45，化为十进制是 69。

(00 45)16=(00000000 0100 0101)$_2$=1+4+64=(69)10

或者直接用 16 进制转为十进制：(00 45)16=4x16^1+5x16^0=64+5=69

用户数据报总长度也占 2 个字节，即 00 1C ,十进制为 28。

(00 1C)16=(00000000 00011100)$_2$=4+8+16=(28)10

或者直接用 16 进制转为十进制：(00 1C)16=1x16^1+12x16^0=16+12=28

数据部分长度为数据报总长度减去首部长度 8 字节，即 28-8=20 字节。

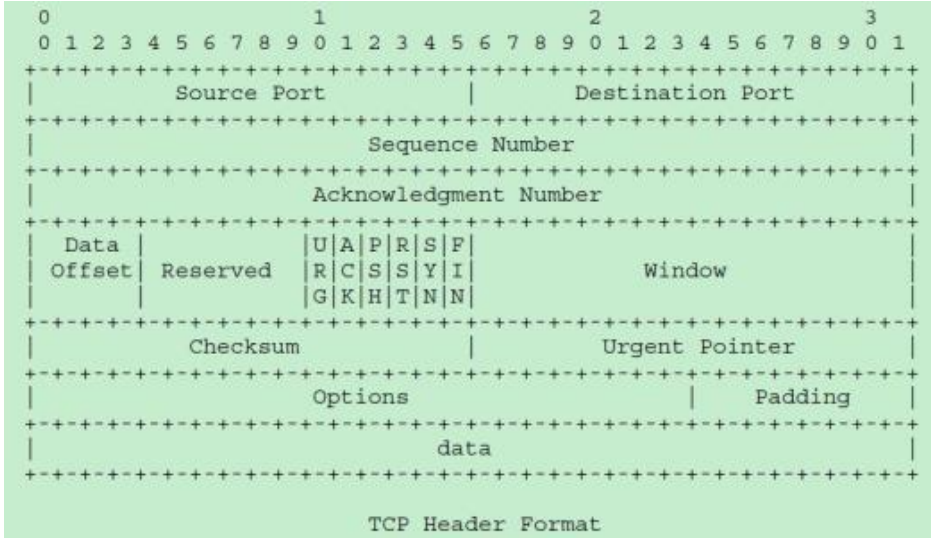
因为目的端口=69<1023（是熟知端口,熟知端口为 0~1023），所以数据报是从客户发送给服务器的。

服务器程序是 TFTP。

【举一反三】一个 TCP 的首部字节数据（以十六进制表示）为，0x0D 28 00 15 50 5F A9 06 00 00 00 00 70 02 40 00 C0 29 00 00.TCP 首部的格式如下图所示(注：试卷上所给的就是英文的 TCP 首部)。请解答下列问题。

本地的端口号是多少？目的端口号是多少？发送的序列号是多少？确认号是多少？

TCP 的首部长度是多少？这是一个使用什么协议的 TCP 连接？该 TCP 连接的状态是什么？（10 分）



【解】本地端口号字段为 2 字节 0D28（0000 1101 0010 1000），十进制即 3368；目的端口号字段为 2 字节 0015（0000 0000 0001 0101），十进制即 21；序列号字段为 4 字节 505F A906，可以不用化为十进制。十进制即 1348446470（仅作参考）；确认号字段为 4 字节 0000 0000，十进制即 0；数据偏移（即首部长度）字段占 4 位，即 7（以 4 字节为单位）所以首部长度为 28 字节。

因为此 TCP 报文的目的端口是 21，所以此连接使用 FTP 协议， SYN=1 表示这是一个连接请求或连接接受报文，连接建立后所有的 ACK 都置 1，此时 ACK=0 表示未确认，因此处于 FTP 客户端向服务器传输控制信息的

状态。

4.在万维网客户程序与万维网服务器程序之间进行交互所使用的协议，是超文本传送协议 HTTP (HyperText Transfer Protocol)。HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。特点：

简单快速：客户向服务器请求服务时，只需传送请求方法和路径。请求方法常用的有 GET、HEAD、POST。每种方法规定了客户与服务器联系的类型不同。由于 HTTP 协议简单，使得 HTTP 服务器的程序规模小，因而通信速度很快；

灵活：HTTP 允许传输任意类型的数据对象。正在传输的类型由 Content-Type 加以标记。

无连接：无连接的含义是限制每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接。采用这种方式可以节省传输时间。

无状态：HTTP 协议是无状态协议。无状态是指协议对于事务处理没有记忆能力。缺少状态意味着如果后续处理需要前面的信息，则它必须重传，这样可能导致每次连接传送的数据量增大。另一方面，在服务器不需要先前信息时它的应答就较快；

支持 B/S 及 C/S 模式；

HTTP1.1 版本后支持可持续连接。

三.计算题(15 分)（原题为子网划分类大题，数据已经缺失，下题为类似题目）

（1）可以将计算机中心的网络划分为 15 个 VLAN，其中 10 个计算机机房分别属于一个不同的 VLAN，部门 1、部门 2、部门 3 各属一个 VLAN，所有的服务器属于一个 VLAN，另外一个 VLAN 用于与学校网络中心连接。这样划分 VLAN，除了可以减少网络广播风暴、提高网络的性能和安全性外，还便于管理和维护，并且使得任课教师比较容易对机房中的计算机是否能访问 Internet 进行控制。

（2）由于计算机中心主机的数量远远超过了网络中心提供的 IP 地址的数量，因此，计算机机房中所有计算机均采用内部 IP 地址，而通过路由器或三层交换机进行地址转换。具体的 IP 地址划分方案如下：

子网	部门	主机数	IP 地址范围	子网掩码
VLAN2-11	10 个计算机机房	50	192.168.0.0 ~ 192.168.0.255 192.168.1.0 ~ 192.168.1.255 …… 192.168.9.0 ~ 192.168.9.255	255.255.255.0
VLAN12	部门 1	20	211.100.58.32 ~ 211.100.58.63	255.255.255.224
VLAN13	部门 2	40	211.100.58.64 ~ 211.100.58.127	255.255.255.192
VLAN14	部门 3	8	211.100.58.16 ~ 211.100.58.31	255.255.255.240
VLAN15	服务器	3	211.100.58.8 ~ 211.100.58.15	255.255.255.248
VLAN16	与网络中心互联	2	211.100.58.0 ~ 211.100.58.3	255.255.255.252

（3）可以在路由器或三层交换机中通过扩展的访问控制列表来实现题目中要求的安全控制，对 FTP 服务器可以设置根据原 IP 地址和目的 IP 地址匹配的访问控制列表；而对计算机机房的所有计算机，可以设置根据时间段和源 IP 地址匹配的访问控制列表，使得不同机房可以在不同的时间段访问 Internet。

（4）建议在网络中增设一台 DHCP 服务器，并在三层交换机或路由器中启用 DHCP 中继功能，使得所有 VLAN 能够共用一台 DHCP 服务器，可以减轻 IP 地址的分配和管理的负担。另外，可以考虑在与网络中心连接部位安装防火墙，以加强对内部网络的安全保护。

附录一

ARP	地址解析协议
ARQ	自动重传请求
AS	自治系统
BGP	边界网关协议
CRC	循环冗余检验
CSMA/CA	载波侦(监)听多路复用(多点接入/多路访问)/冲突避免
CSMA/CD	载波侦(监)听多路复用(多点接入/多路访问)/冲突检测
DNS	域名系统
FDDI	光纤分布式数据接口
FDM	频分多路复用
FTP	文件传输协议
HDLC	高级数据链路控制
HTTP	超文本传输协议
HTML	超文本标记语言
ICMP	网际控制报文协议
IGP	内部网关协议
IMAP	交互式邮件存取协议
MAC	媒体(介质)访问控制
MIME	通用因特网邮件扩充
MPLS	多协议标记交换
OSI	开放系统互连
OSPF	链路状态路由协议(开放最短路径优先路由选择算法)
PVC	永久虚电路
QoS	服务质量
RARP	逆地址解析协议
STP	屏蔽双绞线
SMTP	简单邮件传送协议
SVC	交换虚电路
TDM	时分多路复用
UDP	用户数据报协议
UNI	用户网络接口
URL	统一资源定位符
VLAN	虚拟局域网
WAN	广域网
WLAN	无线局域网

【提示】这是西工大常考的名词解释，每年什么情况不敢妄下结论，还是建议大家认真准备，多记忆背诵。没事的时候就拿出来背一背，把他当做单词来记忆，以我的为标准，很多资料上的是错的，以上这些我挨个都订正过，可以放心背诵