

1.常用的通信传输介质有哪些？它们之间的主要区别？

(1)有线：双绞线、同轴电缆、光纤；无线

(2)区别：带宽、误码率、传输距离、价格、频谱及复用方式、是否支持移动通信等。

2.无连接分组交换与面向连接(虚电路)分组交换的区别？

(1)分组格式:前者完全源、目的地址；后者虚电路号

(2)路由表：前者面向整个网络拓扑，转发时顺序查找路由表；后者面向特定路径或源路由，转发基于索引查找路由表。

(3)可靠性、顺序性：前者无；后者有

(4)建立、维护连接：前者无；后者有

3.ADSL 通道数(子频带)？其中数据通道数？若每个通道均使用 QAM-128 调制，数据通道总容量？

256,248,248*7*4k

4.假定要传送的报文共有 x (单位 bit)，从源节点到目的节点共有 k 跳链路，每条链路的传播时延为 d (单位 s)，链路带宽为 b (单位 bit/s)；电路交换(包括连接建立与拆除)使用的控制帧(或信令)长度、在各节点的排队时延忽略不计；分组交换使用的分组头、分组长度分别为 h 、 p (单位 bit)，分组在各节点的排队时延 q (单位 s)。试分析在何种条件下电路交换的总时延要小于分组交换的总时延？

电路交换总时延 $D(c)$:

(1)连接建立时间: kd

(2)连接拆除时间: kd

(3)数据传输时间: x/b

(4)数据传播时间: kd

$D(c)=3kd+x/b$

分组交换总时延 $D(p)$:

(1)单个分组传输时间: $(p+h)/b$

(2)第 1 跳传输时间: $(x/p) \cdot ((p+h)/b)$ (x/p 为分组个数)

(3)传输时间每 1 跳增加 1 个分组的传输时间

→总的传输时间为 $x/p \cdot (p+h)/b + (k-1) \cdot (p+h)/b$

(4)排队时间: kq

(5)传播时间: kd

$D(p)=x/p \cdot (p+h)/b + (k-1) \cdot (p+h)/b + kd + kq$

若 $D(c) < D(p)$ ，则

1. 首先计算 frame 100110101111 及 $G(x) = (x^4 + x^3 + 1)(x + 1)$ 的 CRC, 然后描述 $G(x)$ 的检错能力.

(1) $G(x) = x^5 + x^3 + x + 1 (101011)$, CRC=00000

(2) 检错能力:

- ① 可检测所有单个错误 ($G(x)$ 多于一项)
- ② 奇数个错误 (含 $1+x$ 项)
- ③ 2 个错误 (说明: 该项回答不扣分)
- ④ 长度不大于 5 的突发错误
- ⑤ $(1-2^{-4})$ 长为 6 的突发错误
- ⑥ $(1-2^{-5})$ 更长和突发错误

2. 若使用一个 256-kbps 的无差错卫星信道(往返传播时延为 512-msec)一个方向上发送 512-byte 数据帧, 而在另一个方向上返回很短的确认帧。则对于窗口大小为 1, 15, 127 的最大吞吐量是多少?

$512 * 8 / 256k = 16ms$

- (1) $k=1, 16 / (16 + 512) * 256 = 7.75$
- (2) $k=15, 7.75 * 15 = 116.36$
- (3) $k=127, 256$

3. 链路层 ACK 的作用?

- (1) 差错控制, 确认, 实现可靠传送
- (2) 流量控制, 滑动窗口

4. 滑动窗口协议中, 退后 N 帧与选择性重传利用链路缓冲能力连续发送多个帧, 令帧的传输时间 (transmission time)=1 (归一化)、传播时间 (propagation time)=a, 则链路的缓冲能力为?

a(单向)或 2a(双向)

5. HDLC 与 PPP 协议的主要区别?

- (1) HDLC 使用序列号(滑动窗口协议), PPP 在控制域为缺省值时不使用序列号(停等协议)且为不可靠传输
- (2) HDLC 面向 bit 填充(同步传输), PPP 除支持面向比特填充(同步传输, 直接使用 HDLC 协议), 还可使用面向 byte 填充(异步传输, 使用类 HDLC 协议 RFC1662)
- (3) PPP 基于 HDLC, 主要用于在点到点链路上传输 IP 流量, 并可支持多种网络协议

6. 假设数据帧为 D bits, 链路带宽为 b bps, 链路出错概率为 p, 采用前向纠错策略需要 x bits 的冗余码, 采用检错加重传策略需要 y bits 的冗余码。试比较分析两种策略的带宽利用率与时延性能。

- (1) 前向纠错策略: 传输数据量 $D+x$, 传输次数 1, 故带宽需求量为 $(D+x)$ 、传输时延为 $(D+x)/b$
- (2) 检错加重传策略: 一次传输数据量 $D+y$, 传输次数 $1/(1-p)$, 故带宽需求量为 $(D+y)/(1-p)$ 、传输时延为 $(D+y)/(b*(1-p))$

1. 若一有限用户 slotted ALOHA 信道处于负载不足与过载的临界点，则

(1)信道中空闲时槽的比例是多少？

(2)成功发送一个帧发送次数是多少？

答：(1) $p_0 = e^{-G}$ ， $G=1 \Rightarrow p_0$ (空闲比例)=36.8%

(2) $G/S-1=1/0.368 \approx 2.72$

2. IEEE 802.3 MAC 协议的全称？它是如何解决冲突的？

答：1-坚持 CSMA/CD；发前侦听，边发边听，冲突避让

3. 若某站点经历了 10 次连续冲突，则在 IEEE 802.3、802.3u 网络中站点的平均等待时间分别为多少？

答：1024/2=512; 802.3: 512*51.2 μ s; 802.3u: 512*5.12 μ s

4. IEEE 802.11 协议哪个(或几个)控制帧发现隐藏终端与暴露终端的？

答：隐藏终端：CTS；暴露终端：RTS

5. IEEE 802.3 MAC 协议中最小帧长的功能与计算依据？

答：最小帧长的功能：检测冲突。

计算依据：传输速率*相距最远的两个站点间传播时延

6. 交换机是如何提升网络性能的？

答：划分冲突域

7. 16 个(编号 1~16)站点正在竞争一条采用自适应遍历树(adaptive tree walk)协议的共享信道。若地址编号大于或等于 13 的站点全部处于发送就绪状态，则需要多少时槽才能解决竞争？

答：11 个

1. 一个子网 IP 地址为 10.80.0.0, 子网掩码为 255.224.0.0 的网络, 它的网络地址、广播地址、最小用户地址、最大用户地址分别是?

答: 网络地址: 10.64.0.0

广播地址: 10.95.255.255

最小用户地址: 10.64.0.1

最大用户地址: 10.95.255.254

2. 假定路由器 R 的路由表如下。当目的地址为 201.4.20.125 的分组到达 R 时, R 将使用哪个接口转发该分组?

掩码	网络地址	下一跳	接口
/26	180.70.65.192	-	s2
/22	201.4.20.0	-	s0
/24	201.4.22.0	-	s3
/25	201.4.20.0	-	s1

答: s1

3. 已知路由器 R1 有表 3-1 所示的路由表, 现收到相邻路由器 R2 发来的路由更新信息, 如表 3-2 所示。试根据 RIP 协议更新路由器 R1 的路由表。

表 3-1 路由器 R1 的路由表

目的网络	距离	下一跳
Net2	3	R2
Net3	4	R3
Net5	5	R4

表 3-2 R2 发给 R1 的更新

目的网络	距离	下一跳
Net1	1	R5
Net2	5	-
Net3	2	R6

答: 路由器 R1 的路由表

目的网络	距离	下一跳
Net1	2	R2
Net2	6	R2
Net3	3	R2
Net5	5	R4

4. 一个 IPv4 分组的分片中, MF(或 M)位是 0, HLEN 是 10, 总长度是 100, 分片偏移值是 200。试求该分片第一个字节和最后一个字节在原分组中的位置。

答: 第一个字节的位置是 1600(200×8), 最后一个字节的位置为 1659($1600 + 100 - 10 \times 4 - 1$)。

5. 基于目的地址转发“下一跳方法”的优缺点。

答:

优点: 每个路由表项只需保留“下一跳”的地址, 无需给出完整的路由(路径)。

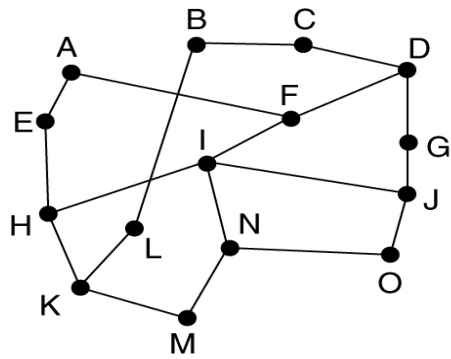
缺点: 要求“下一跳”路由器知道剩余的路径信息或网络中的所有路由器信息保持一致。

6. 对于下图中的子网，若采用下列方法，从 K 开始广播需要产生多少个分组？

(1) 反向路径转发(Reverse path forwarding)?

(2) 汇集树(sink tree)?

(注意：必须画出相应的两棵树.)



答：(1)24;(2)14(重点是画对图)

1. TCP 协议中 ACK 的作用。(20 分)

答：(1)建立连接、拆除连接
 (2)差错控制(或可靠传送)
 (3)流量控制
 (4)拥塞控制

2. TCP 连接的目标。(20 分)

答：(1)实现进程间通信
 (2)实现可靠传送
 (3)实现按序传送
 (4)进行流量控制
 (5)进行拥塞控制

3. 在 TCP 连接中，客户端的初始号 215。客户打开连接，只发送一个携带有 100 字节数据的报文段，然后关闭连接。试问下面从客户端发送的各个报文段的序号分别是多少？(10 分)

(1)SYN 报文段；(2)数据报文段；(3)FIN 报文段。

答：(1)215；(2)216；(3)316

4. 在一条新建的 TCP 连接上发送一个长度为 32KB 的文件。发送端每次都发送一个最大长度的段 (MSS)，MSS 的长度为 1KB，接收端正确收到一个 TCP 段后立即给予确认。发送端的初始拥塞窗口门限设为 16KB。假设发送端尽可能快地传输数据，即只要发送窗口允许，发送端就发送一个 MSS。(20 分)

(1) 已知发生第一次超时后，发送端将拥塞窗口门限调整为 4KB。请问发生超时的时侯，发送端的拥塞窗口是多大？此时发送端共发送了多少数据？其中有多少数据被成功确认了？

(2) 发送端从未被确认的数据开始使用慢启动进行重传。假设此后未再发生超时，当文件全部发送完毕时，发送端的拥塞窗口是多大？

答：(1) 第一次超时发生时，发送端拥塞窗口大小 $= 4KB * 2 = 8KB$

在新建立的 TCP 连接上，发送端采用慢启动开始发送，因此当第一次超时发生时，发送端已发送的数据量 $= 1KB + 2KB + 4KB + 8KB = 15KB$ 。

此时，除最后一批 8 个 TCP 段未获确认外，之前发送的 TCP 段都被确认，因此成功确认的数据量为 7KB。

(2) 发送端采用慢启动重新开始发送，在拥塞窗口达到 4KB 时发送数据量 $= 1KB + 2KB + 4KB = 7KB$ 。

然后进入拥塞避免阶段：在收到全部 4 个 MSS 的确认后，拥塞窗口增至 5KB，相应地发送端发送了 5KB 数据；收到全部 5 个 MSS 的确认后，拥塞窗口增至 6KB；收到全部 6 个 MSS 的确认后，拥塞窗口增至 7KB；此时刚好发完。因此，文件发送结束时，发送端的拥塞窗口大小为 7KB。

5. 数字签名是一种可提供发送方身份鉴别、报文完整性和防发送方抵赖的安全机制。(20 分)

(1) 请给出数字签名最常见的构造方法。

(2) 根据数字签名的构造方法，说明数字签名为什么可以提供以上安全服务。

答：(1) 当实体 A 需要为报文 M 生成数字签名时，A 首先用一个散列函数计算 M 的报文摘要，然后用 A 的私钥加密该报文摘要，生成数字签名。

(2) A 的私钥是只有 A 知道的秘密，任何其它实体无法得到，因而一个有效的数字签名可提供发送方身份鉴别。报文摘要可用于检测报文的完整性，对报文内容的任何修改将产生不同的报文摘要。用 A 的私钥加密后的报文摘要是不可伪造的，从而数字签名就将 A 与报文 M 紧密关联在一起，既能提供报文完整性服务，也能防止发送方抵赖。

6.当两个主机采用传输(transport)方式使用 IPSec，试问此两台主机是如何建立一条虚拟面向连接的服务？(10 分)

答：SA

文件名:	answer
目录:	C:\Users\mbinary\Desktop\计算机网络\homework-quiz
模板:	C:\Users\mbinary\AppData\Roaming\Microsoft\Templates\Normal.dotm
标题:	1
主题:	
作者:	微软用户
关键词:	
备注:	
创建日期:	2017/11/19 22:43:00
修订号:	2
上次保存日期:	2017/11/19 22:43:00
上次保存者:	King Zevin
编辑时间总计:	0 分钟
上次打印时间:	2018/10/27 19:19:00
打印最终结果	
页数:	7
字数:	690 (约)
字符数:	3,938 (约)