同济大学
TONGJI UNIVERSITY

计算机网络 第1次作业

1951112 林日中

8. 记5个路由器为 A, B, C, D, E.

有10条潜在线路，即 AB, AC, AD, AE, BC, BD, BE, CD, CE, DE, 而每条线路有4种可能性（高、中、低速线路或不设置线路）.

故网络拓扑总数为 $4^{10} = 1048576$.

因为每个网络拓扑的生成、遍历时间为 100ms，故所需时间为 $1048576 \times 100ms = 104857.6s \doteq 29h$

即需要约29h才能遍历完所有的网络拓扑。

9. 记事件 A_i 为"第i台主机成功访问信道（即无冲突）"，有 $P(A_i) = p(1-p)^{n-1}$. $i = 1, 2, \dots, n$

记事件B为"信道空闲"，有 $P(B) = (1-p)^n$.

记事件C为"发生冲突".

由 $\sum_{i=1}^{n} P(A_i) + P(B) + P(C) = 1$，有 $P(C) = 1 - np(1-p)^{n-1} - (1-p)^n$.

即由于冲突而被浪费的时间槽比例是 $1 - np(1-p)^{n-1} - (1-p)^n$.

同济大学
TONGJI UNIVERSITY

装

订

线

11. 在OSI协议模型中，不同节点的同等层按照协议实现对等层之间的通信，而不是进行直接通讯，物理通讯只在最低的层中进行。本题中，总裁、法律部门、工程师都进行了直接物理通信。

16. 报文头的总大小为 hn 字节，报文的总大小为 $(M+hn)$ 字节，故报文头所占网络带宽比例是 $\frac{hn}{M+hn}$.

20. 第一种策略适用于网络较易丢失数据包的情况，这样丢失的数据包可被重新传输，确保了文件的完整性。

第二种策略适用于网络高度可靠的情况，这样仅在整个文件传送的结尾发送一次确认，减少了确认次数，可以节省带宽。但是，如果哪怕只有一个数据包丢失，也需要传输整个文件。

23. 图片的大小是 $1024\times768\times3$ 字节即2359296字节，也即18874368比特。通过56kbps的调制解调器、1Mbps的线缆调制解调器、10Mbps和100Mbps的以太网传输图像分别需要337.042s、18.874s、1.888s、0.189s.

同济大学
TONGJI UNIVERSITY

34.

互联网工程任务组（Internet Engineering Task Force, IETF）是一个开放的标准组织，负责开发和推广自愿互联网标准（Internet Standard, STD），特别是构成TCP/IP协议族的标准。目前，绝大多数国际互联网技术标准出自IETF，大量的技术性工作均由其内部的各种工作组承担和完成。

装

Secure Shell（SSH）是互联网安全通信的一个通用协议。在IETF RFC4253中，SSH最初定义了两个必须实现的密钥交

订

换（Key Exchange, KEX）方法名称。然而随着时间的推移，这种方式已不再安全。可以改进的地方是，废弃或不允许一些

线

已发布的KEX，并建议采用一些"应当"和"必须"的KEX.

例如，出于多种原因，SHA-1哈希正在被弃用。SHA-1哈希提供大约80位的安全强度，这意味着所使用的共享密钥最多具有80位的安全强度，这对于大多数用户来说可能还不够。而在SHA-2系列安全哈希函数中，SHA2-256, SHA2-384和SHA2-512分别具有128, 192, 256位的安全强度。综合性能和安全性考虑，SHA2-256可被广泛应用，但尚未有人在RFC中定义用于SSH的KEX。