期中复习习题课

计算机网络 011144.01 2022FA

助教-梁峻滔

中国科学技术大学
计算机科学与技术学院

Oct. 26, 2022

期中考试相关信息

- 时间: 11 月 2 日 (周三) 14:00 ~16:00
- 地点: 具体试室请查看教务系统
- 形式: 半开卷-能且仅能携带一张 A4 纸的开卷资料, 正反两面可用, 可打印.
- 范围: 前三章
- 题型: 单项选择题、简答题、计算题

Outline

1. Chapter 1
   - 知识回顾
   - Supplementary Questions
   - 作业 1 & 测验题
2. Chapter 2
   - 知识回顾
   - Supplementary Questions
   - 作业 2 & 测验题
3. Chapter 3
   - 知识回顾
   - Supplementary Questions
   - 作业 3 & 测验题
4. 复习建议

Outline

1. Chapter 1
   - 知识回顾
   - Supplementary Questions
   - 作业 1 & 测验题
2. Chapter 2
   - 知识回顾
   - Supplementary Questions
   - 作业 2 & 测验题
3. Chapter 3
   - 知识回顾
   - Supplementary Questions
   - 作业 3 & 测验题
4. 复习建议

知识回顾-1.3 网络核心

1. 任务: 将数据包从发送侧的边缘路由器，传送到接收侧的边缘路由器
2. 通信网络中移动数据的两种基本方法:
   1. 电路交换 (独占信道): 电话网使用
   2. 分组交换 (复用信道): 计算机网络使用 (为什么?)
3. 分组交换 (需重点理解)
   1. 过程:
      1. 主机将要传输的数据分段，并组装成一系列分组
      2. **交换**: 在传输路径上，交换设备从一条链路上接收分组，将其发送到另一条链路上
      3. **存储转发**: 交换设备在接收到完整的分组后，才可以开始转发该分组 (为什么采用存储转发?)
   2. 存储转发引入**排队延迟和丢包**
      - ★ 排队延迟: 分组在输出链路的缓存中排队，引入延迟
      - ★ 丢包: 若输出链路的缓存满，溢出的分组被丢弃
      - ★ 当大量分组集中到达时，排队延迟和丢包较严重
4. 电路交换: 通话前完成两部电话机之间的电路接续，通话结束后释放整条电路。本质是**预留资源和独占资源**.
5. 分组交换与电路交换的对比

知识回顾-1.4 衡量网络性能的主要指标

1. 延迟: 分组从源终端到达目的终端的时间
   1. 分组延迟的来源
      - ★ 节点处理延迟 d_{proc}: 几个微秒或更低
      - ★ 排队延迟 d_{queue}: 变化范围很大, 取决于链路负载
      - ★ 传输延迟 $d_{trans} = \frac{L}{R}$, 注意区分 L 的单位是字节还是比特: 微秒 ~ 毫秒, 主要取决于链路传输速率 R
      - ★ 传播延迟 $d_{prop} = \frac{d}{s}$: 几微秒 ~ 几百毫秒, 主要取决于链路长度

      注意区分传输延迟和传播延迟
   2. 节点的总延迟 $d_{node} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$
   3. 端到端延迟: 分组传输路径上所有节点的节点延迟之和
2. 丢包率: 未成功交付到目的终端的分组比例
3. 吞吐量: 单位时间内向接收端成功交付的数据量. 端到端的吞吐量与瓶颈链路的带宽, 以及链路上的负载有关.

知识回顾-1.5 协议层次及其服务类型

1. 网络协议: 定义了通信实体之间交换的报文的格式和次序, 以及在发送/接收报文或其他事件 (例如检测到丢包) 后采取的动作.
2. 分层
3. 因特网协议栈
   - 应用层: 在应用程序之间传输应用特定的报文 (message)
   - 传输层: 在应用程序与网络的接口间 (进程-进程) 传输报文段 (segment)
   - 网络层: 在源主机和目的主机 (终端-终端) 之间传输分组 (packet)
   - 链路层: 在相邻设备之间传输帧 (frame)
   - 物理层: 在物理媒体上传输比特 (bit)
4. ISO/OSI 参考模型: 多两个层次
   - 表示层
   - 会话层

Supplementary Questions

1. 分组在交换网络中需要经历各种延迟，以下哪种延迟对分组的端到端延迟贡献最大?
   A. 传输延迟　B. 排队延迟　C. 传播延迟　D. 钝角

Supplementary Questions

1. 分组在交换网络中需要经历各种延迟，以下哪种延迟对分组的端到端延迟贡献最大?
   A. 传输延迟　B. 排队延迟　C. 传播延迟　D. 钝角
2. 以下那种设备运行了完整的协议栈?
   A. 交换机　B. 终端　C. 路由器　D. 钝角

Supplementary Questions

1. 分组在交换网络中需要经历各种延迟，以下哪种延迟对分组的端到端延迟贡献最大?
   A. 传输延迟　B. 排队延迟　C. 传播延迟　D. 钝角
2. 以下那种设备运行了完整的协议栈?
   A. 交换机　B. 终端　C. 路由器　D. 钝角
3. 下列选项中，不属于网络体系结构所描述的内容是 ()
   A. 网络的层次　B. 每层使用的协议　C. 协议的内部实现细节
   D. 每层必须完成的功能

Supplementary Questions

1. 分组在交换网络中需要经历各种延迟，以下哪种延迟对分组的端到端延迟贡献最大?
   A. 传输延迟　B. 排队延迟　C. 传播延迟　D. 钝角
2. 以下那种设备运行了完整的协议栈?
   A. 交换机　B. 终端　C. 路由器　D. 钝角
3. 下列选项中，不属于网络体系结构所描述的内容是 ()
   A. 网络的层次　B. 每层使用的协议　C. 协议的内部实现细节
   D. 每层必须完成的功能
4. 协议是以下哪两个实体之间通信时需要遵循的规则？
   A. 不同系统的相同层实体之间　B. 不同系统的不同层实体之间
   C. 同一个系统的相邻层实体之间　D. 以上都是

Supplementary Questions

1. 分组在交换网络中需要经历各种延迟，以下哪种延迟对分组的端到端延迟贡献最大?
   A. 传输延迟　B. 排队延迟　C. 传播延迟　D. 钝角
2. 以下那种设备运行了完整的协议栈?
   A. 交换机　B. 终端　C. 路由器　D. 钝角
3. 下列选项中，不属于网络体系结构所描述的内容是 ()
   A. 网络的层次　B. 每层使用的协议　C. 协议的内部实现细节
   D. 每层必须完成的功能
4. 协议是以下哪两个实体之间通信时需要遵循的规则？
   A. 不同系统的相同层实体之间　B. 不同系统的不同层实体之间
   C. 同一个系统的相邻层实体之间　D. 以上都是
5. D　B　C　A

作业 1 & 测验题

见答案文件和板书...

Outline

1. Chapter 1
   - 知识回顾
   - Supplementary Questions
   - 作业 1 & 测验题
2. Chapter 2
   - 知识回顾
   - Supplementary Questions
   - 作业 2 & 测验题
3. Chapter 3
   - 知识回顾
   - Supplementary Questions
   - 作业 3 & 测验题
4. 复习建议

知识回顾-2.1 网络应用架构

1. 客户-服务器架构 (Client/Server, C/S): 有一台总是在线的主机运行着服务器程序 (server)
   - 服务器处于接收请求的状态
   - 客户机发出服务请求后，等待接收响应
   - 服务器收到请求后，分析请求并处理，将结果发送给客户机

   Question: 判断对错: C/S 中一定有一台总是打开的服务器主机.
2. P2P 架构
   - 没有总是在线的服务器主机
   - 每个对等方 (Peer) 既可以请求服务，也可以提供服务
3. 两种架构的比较
4. 进程和 socket

知识回顾-2.2 超文本传输协议 (HTTP)

1. 网页、对象 (object)、URL 等概念
2. HTTP 概述
   - 定义了浏览器 (客户) 和 web 服务器之间的通信规则
   - HTTP 使用 TCP 服务
     1. 服务器进程不断监听 80 端口 (默认), 当监听到连接请求后就与浏览器建立连接
     2. TCP 连接建立后, 浏览器就向服务器发送 HTTP 请求
     3. 服务收到 HTTP 请求后, 将构建所请求的 Web 网页的必需信息, 通过 HTTP 响应返回给客户
     4. 浏览器将响应信息进行解析, 然后将网页呈现给用户
     5. 关闭 TCP 连接
3. 非持续连接和持续连接
   - 非持续连接: 在一个 TCP 连接上最多发送一个对象
   - 持续连接: 在一个 TCP 连接上可以发送多个对象
     - ★ 无流水线方式
     - ★ 流水线方式
4. Web 缓存和代理服务器: 更快地响应部分已缓存的请求
   - 延迟计算
   - 条件 GET: If-modified-since

知识回顾-2.3 FTP, 电子邮件协议, and other staff

1. FTP(使用 TCP)
   - 控制连接和数据连接分离 (为什么?)
   - 用关闭连接表示一个文件传输结束
2. 电子邮件协议
   - 用户代理
   - 邮件服务器
   - 邮件传输协议 (SMTP, POP3, IMAP)

这两个知识点可能会考选择题, 同学们需要注意自主复习.

知识回顾-2.4 域名系统 (DNS)

域名系统 (Domain Name System): 把便于人们记忆的具有特定含义的主机名转换为便与机器处理的 IP 地址. DNS 采用 C/S 模型, 其协议运行在 UDP 之上, 使用 53 端口.

- 层次域名: 国家顶级域名 (.cn, .us), 通用顶级域名 (.com, .org) 等
- 域名服务器: 每个域名服务器不但能进行一些域名到 IP 地址地解析, 而且还必须具有连向其他域名服务器的信息.
  1. 根域名服务器: 最高层次的域名服务器，所有的根域名服务器都知道所有的顶级域名服务器的 IP 地址. 若要对因特网上任何一个域名进行解析，只要自己无法解析，就首先要求助于根域名服务器 (?). 根域名服务器用来管辖顶级域 (如.com)
  2. 顶级域名服务器: 收到 DNS 查询请求时，就给出相应的回答 (可能是最后的结果，也可能是下一步应当查找的域名服务器的 IP 地址).
  3. 授权 (Authorized) 域名服务器 (权限域名服务器): 每台主机都必须在授权域名服务器处登记。许多域名服务器都同时充当本地域名服务器和授权域名服务器。授权域名服务器能将其管辖的主机名转换为该主机的 IP 地址.
  4. 本地域名服务器: 对于域名系统很重要，当一台主机发出 DNS 查询请求时，这个查询请求报文就发送给该主机的本地域名服务器.

知识回顾-2.4 域名系统 (DNS)

- 解析过程
  - 递归查询: 如果本地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，向根域名服务器继续发出查询请求报文，在这种情况下，本地域名服务器只需向根域名服务器查询一次，后面的几次查询都是递归地在其他几个域名服务器之间进行.
  - 迭代查询: 当根域名服务器收到本地域名服务器发出的迭代查询请求报文时, 要么给出所要查询的 IP 地址, 要么告诉本地域名服务器下一步应当向哪个顶级域名服务器进行查询. 然后让本地域名服务器向这个顶级域名服务器进行后续的查询, 如此迭代.
  - DNS 缓存: 为了提高 DNS 的查询效率, 并减少因特网上的 DNS 查询报文数量. 当一个 DNS 服务器接收到 DNS 查询结果时, 它可以将该 DNS 信息缓存在高速缓存中. 这样后面再遇到相同的域名查询时, 该 DNS 服务器就能够直接提供所要求的 IP 地址.

Supplementary Questions

1. 以下哪个协议不能用于访问用户信箱 (属于邮件服务器的一部分)?
   A. SMTP B. POP3 C. HTTP D. IMAP

Supplementary Questions

1. 以下哪个协议不能用于访问用户信箱 (属于邮件服务器的一部分)?
   A. SMTP B. POP3 C. HTTP D. IMAP
2. 以下有关 DNS 的说法, 哪一个是正确的?
   A. 一个域名唯一映射到一个 IP 地址
   B. 因特网上的每台主机都需要一个域名
   C. 域名解析每次都要从查询根域名服务器开始
   D. 本地域名服务器不属于域名服务器层次

Supplementary Questions

1. 以下哪个协议不能用于访问用户信箱 (属于邮件服务器的一部分)?
   A. SMTP B. POP3 C. HTTP D. IMAP
2. 以下有关 DNS 的说法, 哪一个是正确的?
   A. 一个域名唯一映射到一个 IP 地址
   B. 因特网上的每台主机都需要一个域名
   C. 域名解析每次都要从查询根域名服务器开始
   D. 本地域名服务器不属于域名服务器层次
3. 计算题: HW2 P8

Supplementary Questions

1. 以下哪个协议不能用于访问用户信箱 (属于邮件服务器的一部分)?
   A. SMTP B. POP3 C. HTTP D. IMAP
2. 以下有关 DNS 的说法, 哪一个是正确的?
   A. 一个域名唯一映射到一个 IP 地址
   B. 因特网上的每台主机都需要一个域名
   C. 域名解析每次都要从查询根域名服务器开始
   D. 本地域名服务器不属于域名服务器层次
3. 计算题: HW2 P8
4. A: SMTP 是一个" 推" 协议
   D: 严格来说, 本地 DNS 服务器不属于DNS 服务器的层次结构. 本地 DNS 服务器起着代理的作用, 负责将 DNS 查询报文发送到 DNS 层次结构中, 并将查询结果返回给解析器. 对于 C, 考虑 DNS 缓存

作业 2 & 测验题

见答案文件和板书...

Outline

1. Chapter 1
   - 知识回顾
   - Supplementary Questions
   - 作业 1 & 测验题
2. Chapter 2
   - 知识回顾
   - Supplementary Questions
   - 作业 2 & 测验题
3. Chapter 3
   - 知识回顾
   - Supplementary Questions
   - 作业 3 & 测验题
4. 复习建议

知识回顾-Chapter3 Outline

- 3.1 概述和传输层服务
- 3.2 多路复用与多路分解
- 3.3 无连接传输: UDP
- 3.4 可靠数据传输原理
- 3.5 面向连接的传输: TCP
- 3.6 拥塞控制原理
- 3.7 TCP 拥塞控制

知识回顾-3.1 概述和传输层服务

- 传输层把应用层报文 (message) 转换成传输层分组, 即报文段 (segment). 主要协议有 **UDP** 和 **TCP** 协议.
- 网络层提供主机之间的逻辑通信; 传输层提供进程之间的逻辑通信. 传输层依赖并增强网络层的服务.
- 因特网网络层协议 (IP) 的服务模型为" **尽力而为的交付**", 不确保交付, 因此被称为不可靠服务. 但是却可以通过其上层的传输层协议为应用程序提供可靠的数据传输服务 (为什么?).
- 传输层不能提供的服务?...

知识回顾-3.2 多路复用与解复用

- 传输层基本服务: 将主机间交付扩展到进程间交付.
- 多路复用 (发送端): 传输层从多个 socket 收集数据, 交给网络层发送.
- 解复用 (接收端): 传输层将收到的数据交付到正确的 socket(How?)–通过 socket 标识.
- socket 标识与端口号: 端口号是 socket 标识的一部分.
  - UDP 的 socket 标识是一个二元组: <IP 地址, 端口号 >
  - TCP 的 socket 标识是一个四元组: < 源 IP, 目的 IP, 源端口, 目的端口 >
  - 为什么会有这个差异?

知识回顾-3.3 无连接传输：UDP

- UDP 报文结构
- UDP checksum
- UDP 提供的服务，为什么需要 UDP 以及 UDP 适用的应用

知识回顾-Next..

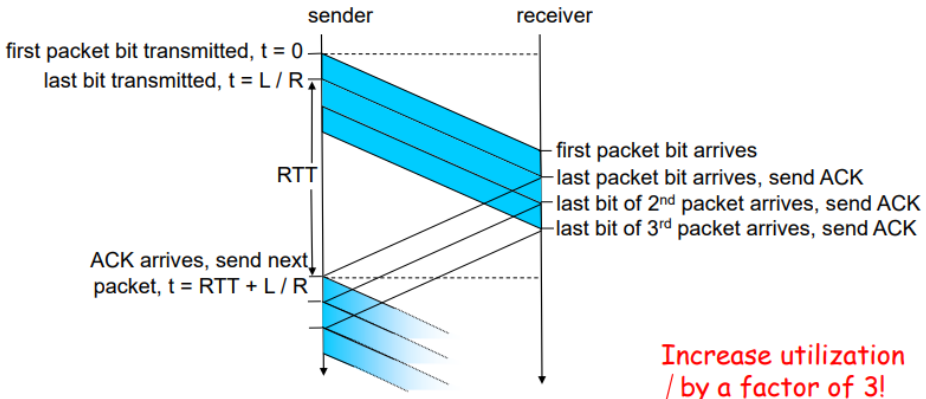
接下来就是最重要的 TCP, 先粗糙地回想一下, TCP 最重要的有哪些内容?

- 面向连接
- 可靠数据传输
- 拥塞控制

知识回顾-3.4 可靠数据传输原理

- 什么是可靠传输: 数据不会有比特损坏或丢失, 并按照发送的顺序被接收. 如何在不可靠的网络层上实现可靠的传输协议?
- 可靠数据传输协议:
  - 从 rdt1.0 到 rdt3.0 是如何演化的.
  - rdt3.0 是一种停-等 (stop and wait) 协议, 性能不佳. 引入流水线以提高链路利用率 (HW3: P15, P46)

流水线：提高链路利用率



Increase utilization by a factor of 3!

$$U_{sender} = \frac{3 * L / R}{RTT + L / R} = \frac{.024}{30.008} = 0.0008$$

Transport Layer 3-59

知识回顾-3.4 可靠数据传输原理: GBN

- 发送端

Sender:

- 假设最多允许N个已发送、未确认的分组
- 发送端看到的序号空间（由序号长度决定）划分为以下4个区域：

  - 仅当发送窗口不满时，才发送新的分组
  - 收到确认 (ACK) 后更新发送窗口
  - 发送窗口发生变化时需要重新设置定时器
  - 超时后，重发发送窗口中的全部分组
- 接收端
  - 按顺序接收分组，不缓存失序分组
  - 累积确认发送 ACK
- 特点：接收端简单，发送端复杂，出错后需要较多重传.

知识回顾-3.4 可靠数据传输原理: SR

一般情况下, 发送窗口大小 = 接收窗口大小

- 发送端
  - 每个已发送的分组都需要一个单独的定时器
  - 若定时器 n 超时, 仅重发序号为 n 的分组
- 接收端
  - 落在接收窗口中的分组都要接收, 每个分组单独发送 ACK 确认
  - 允许乱序接收, 但要求按序 (向应用层) 交付
- 特点: 出错后重传代价小, 发送端使用较多定时器, 接收端需要较大缓存空间, 实现复杂.
- 窗口大小和序号空间的关系

知识回顾-3.5 面向连接的传输: TCP

- Overview
  - 服务模型: 连接一对通信进程的字节流管道
  - 建立连接
  - 流水式发送报文段
  - 流量控制
- 序号和确认号
  - 序号: 报文段 (分组) 中第一个数据字节的序号
  - 确认号: 使用累积确认, 表示期望从对方那接收到下一个字节的序号
  - 确认号对于 TCP 超时设置的作用? -估计 RTT: 测量从发出某个报文段到收到其确认之间经过的时间, 作为 SampleRTT.
- TCP 采用的数据传输机制:
  - 发送端采用流水式发送分组
  - 接收到采用累积确认进行响应
  - 发送端采用重传来恢复丢失的报文段

Question: 以上三个方面, 哪些是属于可靠数据传输的要求?

知识回顾-3.5 面向连接的传输: TCP

- 发送方:
  - 流水式发送报文段
  - 仅对最早未确认的报文段使用一个重传定时器 (与 GBN 类似)
  - 超时后仅重发最早未确认的报文段 (与 SR 类似, 接收端缓存了失序的报文段)
- 接收方:
  - 仅在正确、按序收到报文段后更新确认号
  - 其余情况, 重复发送前一次的确认号 (与 GBN 类似, 使用累积确认)
  - 缓存失序的分组 (与 SR 类似)
- 快速重传 (Fast Retransmit): 利用重复的 ACK(3 个) 检测丢包, 在定时器到期前重发丢失的分组

知识回顾-3.5 面向连接的传输: TCP

- 流量控制: 发送端 TCP 调节发送速率, 避免接收端缓存溢出 (考虑的是接收端应用的数据取走速率).
  Question: 流量控制和后面介绍的拥塞控制的区别?
- 连接管理 (需要知道过程细节):
  - 建立连接: 三次握手
  - 关闭连接: 四次挥手

知识回顾-3.6 拥塞控制原理

- 端到端拥塞控制: 端系统通过观察丢包和延迟来推断拥塞的发生 (TCP 采用)
- 网络辅助的拥塞控制: ...

知识回顾-3.7 TCP 拥塞控制

三个问题

1. 发送方如何感知网络拥塞? -利用丢包事件
   - 超时
   - 3 次重复 ACK
2. 发送方采用什么机制来限制发送速率?
   - 使用拥塞窗口 (cwnd) 限制已发送未确认的数据量 (拥塞窗口跟前面的发送方窗口是什么关系?)
   - $$\text{LastByteSent} - \text{LastByteAcked} \leq min\{\text{cwnd}, \text{rwnd}\}$$

     这里的 rwnd 指接收方窗口剩余空间大小. rwnd 用于流量控制.
3. 发送方调节拥塞窗口的策略:
   - 加性增, 乘性减 (AIMD)
   - 慢启动: 迅速增大 cwnd 至可用的发送速率
     - ★ 每收到一个 ACK, cwnd 就增加一个 MSS ⇔ 每经过一个 RTT, cwnd 加倍

注: TCP 拥塞控制考虑的是外面网络整体的拥塞状况.

知识回顾-3.7 TCP 拥塞控制

TCP Reno

- cwnd $<$ ssthresh 时, 慢启动
- cwnd $>=$ ssthresh 时, 拥塞避免 (执行 AIMD)
- 收到 3 个冗余 ACK

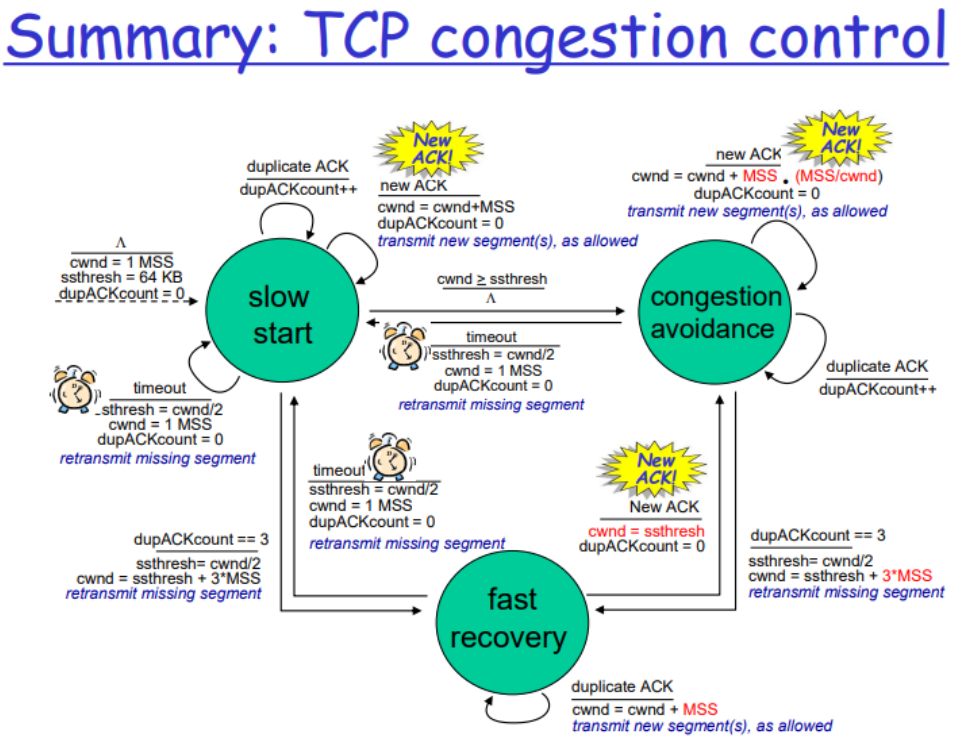
$$ssthresh = cwnd/2$$
$$cwnd = ssthresh + 3\,MSS$$

- 超时

$$ssthresh = cwnd/2$$
$$cwnd = 1\,MSS$$

知识回顾-3.7 TCP 拥塞控制

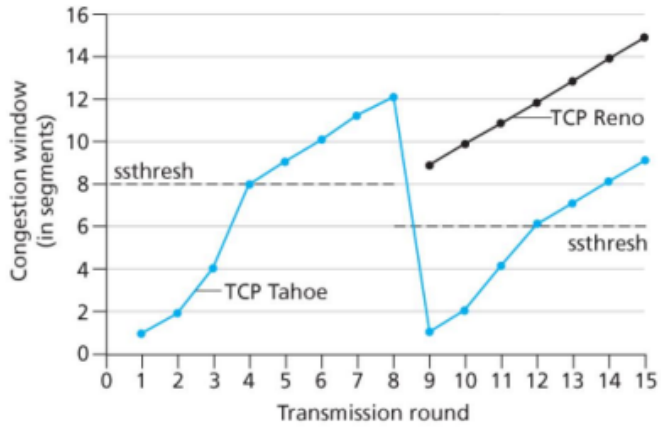
- TCP Summary



Question: 前面提到的快速重传 (Fast Retransmit) 和这里的快速恢复 (Fast Recovery) 有什么区别?

知识回顾-3.7 TCP 拥塞控制

- TCP Reno v.s.TCP Tahoe:



- TCP 吞吐量

Supplementary Questions

1. 传输层最基本的功能是?
   A. 流量控制　B. 拥塞控制　C. 实现不同主机的进程间通信　D. 可靠传输

Supplementary Questions

1. 传输层最基本的功能是?
   A. 流量控制　B. 拥塞控制　C. 实现不同主机的进程间通信　D. 可靠传输
2. 画图题: HW3 P27

Supplementary Questions

1. 传输层最基本的功能是?
   A. 流量控制　B. 拥塞控制　C. 实现不同主机的进程间通信　D. 可靠传输
2. 画图题: HW3 P27
3. TCP 确认报文段被用于确认已收到的报文段、检测丢失的报文段、调整超时定时器的设置, 简要说明 TCP 报文段是如何发挥以上作用的.

Supplementary Questions

1. 传输层最基本的功能是?
   A. 流量控制　B. 拥塞控制　C. 实现不同主机的进程间通信　D. 可靠传输
2. 画图题: HW3 P27
3. TCP 确认报文段被用于确认已收到的报文段、检测丢失的报文段、调整超时定时器的设置, 简要说明 TCP 报文段是如何发挥以上作用的.
4. TCP 流量控制 v.s. TCP 拥塞控制
5. 计算题: HW3 P40

Supplementary Questions

1. 传输层最基本的功能是?
   A. 流量控制　B. 拥塞控制　C. 实现不同主机的进程间通信　D. 可靠传输
2. 画图题: HW3 P27
3. TCP 确认报文段被用于确认已收到的报文段、检测丢失的报文段、调整超时定时器的设置, 简要说明 TCP 报文段是如何发挥以上作用的.
4. TCP 流量控制 v.s. TCP 拥塞控制
5. 计算题: HW3 P40
6. 1. C

作业 3 & 测验题

见答案文件和板书...

Outline

1. Chapter 1
   - 知识回顾
   - Supplementary Questions
   - 作业 1 & 测验题
2. Chapter 2
   - 知识回顾
   - Supplementary Questions
   - 作业 2 & 测验题
3. Chapter 3
   - 知识回顾
   - Supplementary Questions
   - 作业 3 & 测验题
4. **复习建议**

复习建议

- 时间紧时，首先复习重要的知识点和题目 (老师上课花更多事件讲的就是相对更重要的)，不要把过多时间和精力花在扣一些无关紧要的细节上，注重理解.

复习建议

- 时间紧时, 首先复习重要的知识点和题目 (老师上课花更多事件讲的就是相对更重要的), 不要把过多时间和精力花在扣一些无关紧要的细节上, 注重理解.
- 比如说, 助教准备习题课 slides 时都会下意识地跳过/省略一些内容, 就是因为觉得有些内容不是那么重要 (时间有限).

复习建议

- 时间紧时，首先复习重要的知识点和题目 (老师上课花更多事件讲的就是相对更重要的)，不要把过多时间和精力花在扣一些无关紧要的细节上，注重理解.
- 比如说，助教准备习题课 slides 时都会下意识地跳过/省略一些内容，就是因为觉得有些内容不是那么重要 (时间有限).
- 建议以老师的 PPT、作业、小测题为主要复习材料，教材和其他习题为辅，复习 PPT 时注意里面红色标注需要思考的地方，多结合例子来帮助理解.

复习建议

- 时间紧时，首先复习重要的知识点和题目 (老师上课花更多事件讲的就是相对更重要的)，不要把过多时间和精力花在扣一些无关紧要的细节上，注重理解.
- 比如说，助教准备习题课 slides 时都会下意识地跳过/省略一些内容，就是因为觉得有些内容不是那么重要 (时间有限).
- 建议以老师的 PPT、作业、小测题为主要复习材料，教材和其他习题为辅，复习 PPT 时注意里面红色标注需要思考的地方，多结合例子来帮助理解.
- 复习这些资料时多想想哪些知识哪些作业题会考选择题，简答题或是计算题，以此来判断复习的侧重点和投入时间.

复习建议

- 时间紧时，首先复习重要的知识点和题目 (老师上课花更多事件讲的就是相对更重要的)，不要把过多时间和精力花在扣一些无关紧要的细节上，注重理解.
- 比如说，助教准备习题课 slides 时都会下意识地跳过/省略一些内容，就是因为觉得有些内容不是那么重要 (时间有限).
- 建议以老师的 PPT、作业、小测题为主要复习材料，教材和其他习题为辅，复习 PPT 时注意里面红色标注需要思考的地方，多结合例子来帮助理解.
- 复习这些资料时多想想哪些知识哪些作业题会考选择题，简答题或是计算题，以此来判断复习的侧重点和投入时间.
- 比如说，老师 PPT 中所有标注的思考题都可以作为一道简答题的一小问.

复习建议

- 时间紧时，首先复习重要的知识点和题目 (老师上课花更多事件讲的就是相对更重要的)，不要把过多时间和精力花在扣一些无关紧要的细节上，注重理解.
- 比如说，助教准备习题课 slides 时都会下意识地跳过/省略一些内容，就是因为觉得有些内容不是那么重要 (时间有限).
- 建议以老师的 PPT、作业、小测题为主要复习材料，教材和其他习题为辅，复习 PPT 时注意里面红色标注需要思考的地方，多结合例子来帮助理解.
- 复习这些资料时多想想哪些知识哪些作业题会考选择题，简答题或是计算题，以此来判断复习的侧重点和投入时间.
- 比如说，老师 PPT 中所有标注的思考题都可以作为一道简答题的一小问.
- 简答题不要写小作文，但也不要写得像是跟助教说“你懂的”(助教不懂)：写得过长和过于简陋都不利于你自己得分!

最后

预祝同学们期中考试顺利 ~

谢谢!

计算机网络习题课#2

贺若舟 <fward@mail.ustc.edu.cn>

期末考试

- 考试范围：第4、5、6、7、8章
- ~~考试分A/B卷。时间分别为12月18日和开学后。参加一次即可，均为线下考试~~
  - ~~考两次仅取A卷成绩~~
- ~~A卷的考试地点为：~~
  - ~~3C101(88)~~
  - ~~3C102(88)~~

  ~~我们会在考试前公布详细座位名单~~
- ~~A卷的考试时间为12月18日的14:30~16:30~~
- 全体同学应该参加下学期的考试（否则应该申请缓考），考试地点和时间待定
- 我们会在下学期上一次习题课，但不是这个slide的内容
- 半开卷考试，允许带一张A4大小的cheat sheet

011144.01
计算机网络
3.5 理论实验课 笔试（半开卷） 176
期末考试

011
计算机科学与技术系

华蓓 宋骐



Contents

- 第四章 网络层：数据平面
- 第五章 网络层：控制平面
- 第六章 链路层和局域网
- 第七章 无线网络和移动网络
- 第八章 计算机网络安全

第4章 网络层：数据平面

要点

- 知道网络层提供了什么服务（选择题/问答题）
- 了解IP协议、编址方法
- 了解路由器工作原理
- 了解数据面和控制面的差异，理解数据面的功能（选择题/问答题）

P5

P5. 考虑使用32比特主机地址的某数据报网络。假定一台路由器具有4条链路，编号为0～3，分组能被转发到如下的各链路接口：

目的地址范围	链路接口
11100000 00000000 00000000 00000000 到 11100000 00111111 11111111 11111111	0
11100000 01000000 00000000 00000000 到 11100000 01000000 11111111 11111111	1
11100000 01000001 00000000 00000000 到 11100001 01111111 11111111 11111111	2
其他	3

a. 提供一个具有5个表项的转发表，使用最长前缀匹配，转发分组到正确的链路接口。

b. 描述你的转发表是如何为具有下列目的地址的数据报决定适当的链路接口的。

11001000 10010001 01010001 01010101

11100001 01000000 11000011 00111100

11100001 10000000 00010001 01110111

P5

a. 提供一个具有 5 个表项的转发表，使用最长前缀匹配，转发分组到正确的链路接口。
b. 描述你的转发表是如何为具有下列目的地址的数据报决定适当的链路接口的。
11001000 10010001 01010001 01010101
11100001 01000000 11000011 00111100
11100001 10000000 00010001 01110111

a. 考察最长前缀匹配和转发表构建
答案为

224.0.0.0/10	11100000 00	0
224.64.0.0/16	11100000 01000000	1
224.0.0.0/7	1110000	2
225.128.0.0/9	11100001 1	3
0.0.0.0	otherwise	3

b. 考察最长前缀匹配
简单来说就是谁是从前看最长的匹配项，就到那个匹配项对应的端口。
答案为3、2、3

P7

P7. 考虑使用 8 比特主机地址的数据报网络。假定一台路由器使用最长前缀匹配并具有下列转发表：

前缀匹配	接口
1	0
10	1
111	2
其他	3

对这 4 个接口中的每个，给出相应的目的主机地址的范围和在该范围中的地址数量。

- 先算最长的，也就是接口2：$2^{8-3} = 32$个地址
- 接口1：$2^{6} = 64$个地址
- 接口0：$2^{7} - N(\text{interface 1}) - N(\text{interface 2}) = 32$个地址
- 其他：$2^{8} - N(\text{interface 0}) - N(\text{interface 1}) - N(\text{interface 2}) = 128$个地址

P8

P8. 考虑互联 3 个子网（子网 1、子网 2 和子网 3）的一台路由器。假定这 3 个子网的所有接口要求具有前缀 223. 1. 17/24。还假定子网 1 要求支持多达 60 个接口，子网 2 要求支持多达 90 个接口，子网 3 要求支持多达 12 个接口。提供 3 个满足这些限制的网络地址（形式为 *a. b. c. d/x*）。

还是一样的考察点，下面为示例答案

- 223.1.17.0/26
- 223.1.17.128/25
- 223.1.17.192/28

P10

P10. 在习题 P5 中要求你给出转发表（使用最长前缀匹配）。使用 *a. b. c. d/x* 记法代替二进制字符串记法，重写该转发表。

前面给过了:)

P12

P12. 考虑图 4-20 中显示的拓扑。（在 12:00 以顺时针开始）标记具有主机的 3 个子网为网络 A、B 和 C，标记没有主机的子网为网络 D、E 和 F。

a. 为这 6 个子网分配网络地址，要满足下列限制：所有地址必须从 214.97.254/23 起分配；子网 A 应当具有足够地址以支持 250 个接口；子网 B 应当具有足够地址以支持 120 个接口；子网 C 应当具有足够地址以支持 120 个接口。当然，子网 D、E 和 F 应当支持两个接口。对于每个子网，分配采用的形式是 *a. b. c. d/x* 或 *a. b. c. d/x ~ e. f. g. h/y*。

b. 使用你对（a）部分的答案，为这 3 台路由器提供转发表（使用最长前缀匹配）。

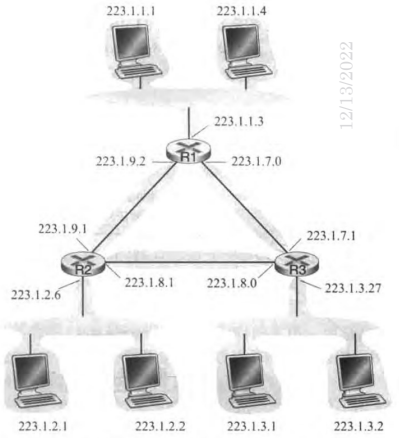


图 4-20　3 台路由器互联 6 个子网

a. Subnet A: 214.97.255.0/24 (256 addresses)
Subnet B: 214.97.254.0/25 - 214.97.254.0/29 (128-8 = 120 addresses)
Subnet C: 214.97.254.128/25 (128 addresses)
Subnet D: 214.97.254.0/31 (2 addresses)
Subnet E: 214.97.254.2/31 (2 addresses)
Subnet F: 214.97.254.4/30 (4 addresses)

b. 后页

Router 1

Longest Prefix Match	Outgoing Interface
11010110 01100001 11111111	Subnet A
11010110 01100001 11111110 0000000	Subnet D
11010110 01100001 11111110 000001	Subnet F

Router 2

Longest Prefix Match	Outgoing Interface
11010110 01100001 11111111 0000000	Subnet D
11010110 01100001 11111110 0	Subnet B
11010110 01100001 11111110 0000001	Subnet E

Router 3

Longest Prefix Match	Outgoing Interface
11010110 01100001 11111111 000001	Subnet F
11010110 01100001 11111110 0000001	Subnet E
11010110 01100001 11111110 1	Subnet C

P14

P14. 考虑向具有 700 字节 MTU 的一条链路发送一个 2400 字节的数据报。假定初始数据报标有标识号 422。将会生成多少个分片？在生成相关分片的数据报中各个字段的值是多少？

- 每个报文含长度为20的IP头，实际可用负载为700-20=680.
- 需要$\left\lceil \frac{2400-20}{680} \right\rceil = 4$个分片
- 需要调整的字段不包括标识符（始终为422）
- total length字段分别为700、700、360
- Flags中的MF字段需要调整
- Fragment offset字段分别为0, 85, 170, 255

第5章 网络层：控制平面

要点

本章可以出计算题和大题，也可以出选择题、主观题

- 理解网络层控制面的作用

网络层功能

回顾：网络层的两个功能

- 转发: 路由器将分组从输入端口转移到输出端口　　数据面
- 选路: 确定分组如何去往目的地址　　控制面

两种建立控制面的方法:

- per-router control (traditional)　我们的考试内容
- logically centralized control (software defined networking)

研究生课程 田野《高级计算机网络》

要点

- 理解网络层控制面的作用
- 传统选路算法
  - Link State: OSPF
  - Dijkstra: 如同OS的银行家算法，实际上不可用，但是考!
  - Distance Vector: RIP
  - BGP不属于以上的类别，它是path-vector routing
- 选路算法分类
  - 全局算法 or 分布式算法
  - 静态算法 or 动态算法
  - intra-AS (IGP) or inter-AS (EGP)
- AS

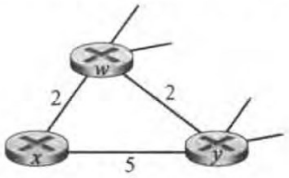
P3

考虑下面的网络。对于标明的链路开销，用Dijkstra的最短路算法计算出从x到所有网络节点的最短路径。通过计算一个类似于表5-1的表，说明该算法是如何工作的。

- 此题只有同学抄了书本上的下一题答案被判错，故不讲

P7

P7. 考虑下图所示的网络段。x 只有两个相连邻居 w 与 y。w 有一条通向目的地 u（没有显示）的最低开销路径，其值为5，y 有一条通向目的地 u 的最低开销路径，其值为6。从 w 与 y 到 u（以及 w 与 y 之间）的完整路径未显示出来。网络中所有链路开销皆为正整数值。



a. 给出 x 对目的地 w、y 和 u 的距离向量。

b. 给出对于 $c(x, w)$ 或 $c(x, y)$ 的链路开销的变化，使得执行了距离向量算法后，x 将通知其邻居有一条通向 u 的新最低开销路径。

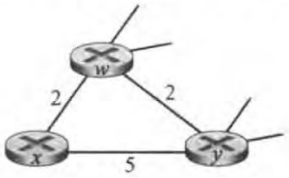
c. 给出对 $c(x, w)$ 或 $c(x, y)$ 的链路开销的变化，使得执行了距离向量算法后，x 将不通知其邻居有一条通向 x 的新最低开销路径。

a. x的距离向量为$\left(2, 4, \min\left(c(x,y) + d_y(u), c(x,w) + d_w(u)\right)\right) = (2,4,7)$

b/c. 需要分情况讨论。

P7

P7. 考虑下图所示的网络段。x 只有两个相连邻居 w 与 y。w 有一条通向目的地 u（没有显示）的最低开销路径，其值为5，y 有一条通向目的地 u 的最低开销路径，其值为6。从 w 与 y 到 u（以及 w 与 y 之间）的完整路径未显示出来。网络中所有链路开销皆为正整数值。



a. 给出 x 对目的地 w、y 和 u 的距离向量。

b. 给出对于 $c(x, w)$ 或 $c(x, y)$ 的链路开销的变化，使得执行了距离向量算法后，x 将通知其邻居有一条通向 u 的新最低开销路径。

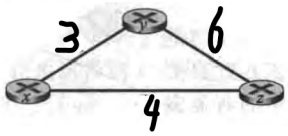
c. 给出对 $c(x, w)$ 或 $c(x, y)$ 的链路开销的变化，使得执行了距离向量算法后，x 将不通知其邻居有一条通向 x 的新最低开销路径。

b/c. $d_x(u) = \min\left(c(x,y) + d_y(u), c(x,w) + d_w(u)\right) = \min(c(x,y) + 6, c(x,w) + 5)$

- 若$c(x,y)$变化，那么，需要比目前的7更小才会通知。但是$c(x,y)$的取值范围无法做到，所以$c(x,y)$怎么变化都不会通知。
- 若$c(x,w)$变化，取1时，会通知邻居有更小的最低开销路径（但是此时路径不变）；大于等于6时也会通知邻居。

P8

P8. 考虑如图 5-6 中所示 3 个节点的拓扑。不使用显示在图 5-6 中的开销值，链路开销值现在是 $c(x, y)=3$，$c(y, z)=6$，$c(z, x)=4$。在距离向量表初始化后和在同步版本的距离向量算法每次迭代后，计算它的距离向量表（如我们以前对图 5-6 讨论时所做的那样）。



考察距离向量法

Cost to

From	x	y	z
x	0	3	4
y	∞	∞	∞
z	∞	∞	∞

Cost to

From	x	y	z
x	∞	∞	∞
y	3	0	6
z	∞	∞	∞

Cost to

From	x	y	z
x	∞	∞	∞
y	∞	∞	∞
z	4	6	0

Cost to

From	x	y	z
x	0	3	4
y	3	0	6
z	4	6	0

Cost to

From	x	y	z
x	0	3	4
y	3	0	6
z	4	6	0

Cost to

From	x	y	z
x	0	3	4
y	3	0	6
z	4	6	0

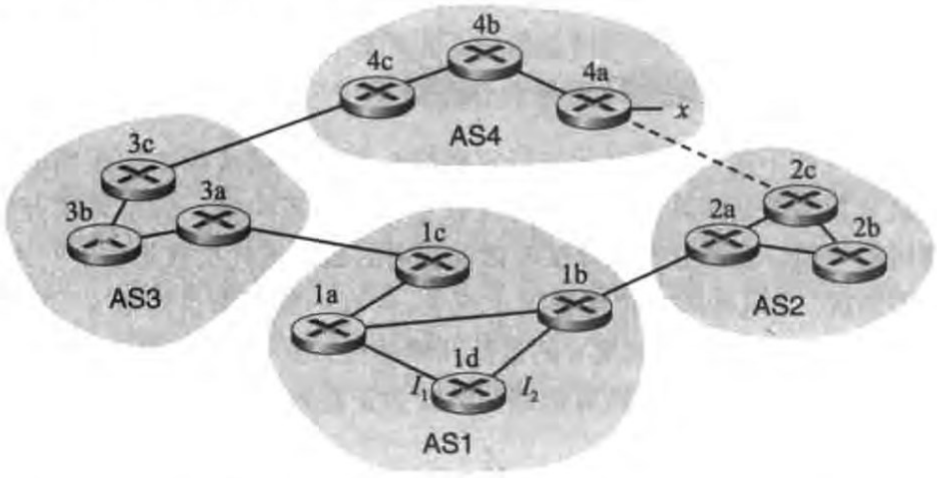
P14. 考虑下图所示的网络。假定 AS3 和 AS2 正在运行 OSPF 作为其 AS 内部路由选择协议。假定 AS1 和 AS4 正在运行 RIP 作为其 AS 内部路由选择协议。假定 AS 间路由选择协议使用的是 eBGP 和 iBGP。假定最初在 AS2 和 AS4 之间不存在物理链路。

a. 路由器 3c 从下列哪个路由选择协议学习到了前缀 x：OSPF、RIP、eBGP 或 iBGP?

b. 路由器 3a 从哪个路由选择协议学习到了前缀 x?

c. 路由器 1c 从哪个路由选择协议学习到了前缀 x?

d. 路由器 1d 从哪个路由选择协议学习到了前缀 x?



P14

考察对OSPF、RIP、eBGP、iBGP的理解

都是跨AS的，所以都是BGP；所以应该看是否是外部的BGP路由器告知的路径

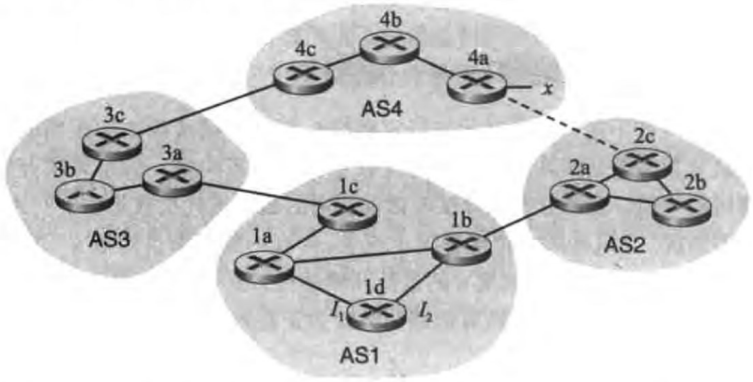
a. eBGP

b. iBGP

c. eBGP

d. iBGP

a. 路由器 3c 从下列哪个路由选择协议学习到了前缀 x：OSPF、RIP、eBGP 或 iBGP?
b. 路由器 3a 从哪个路由选择协议学习到了前缀 x?
c. 路由器 1c 从哪个路由选择协议学习到了前缀 x?
d. 路由器 1d 从哪个路由选择协议学习到了前缀 x?



P15

P15. 参考前面习题 P14，一旦路由器 1d 知道了 x 的情况，它将一个表项（x，I）放入它的转发表中。

a. 对这个表项而言，I 将等于 I_1 还是 I_2？用一句话解释其原因。

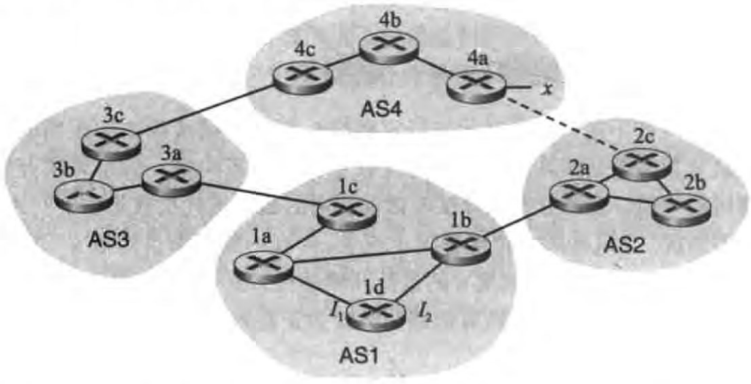
b. 现在假定在 AS2 和 AS4 之间有一条物理链路，显示为图中的虚线。假定路由器 1d 知道经 AS2 以及经 AS3 能够访问到 x。I 将设置为 I_1 还是 I_2？用一句话解释其原因。

c. 现在假定有另一个 AS，它称为 AS5，其位于路径 AS2 和 AS4 之间（没有显示在图中）。假定路由器 1d 知道经 AS2 AS5 AS4 以及经过 AS3 AS4 能够访问到 x。I 将设置为 I_1 还是 I_2？用一句话解释其原因。

a. I_1，此刻的最小代价路径要经过1a

b. I_2，此时AS-PATH相等，但是I_2拥有最小的NEXT-HOP

c. I_1，此时I_1拥有最小的AS-PATH



第6章 链路层和局域网

要点

- 了解数据链路层所提供的服务
  - 组装帧
  - 差错检测、纠正
    - CRC/二维奇偶校验
  - 多址接入技术（在共享广播信道如何处理冲突）
    - 多信道：常见于蜂巢移动网络，也可能多种方法同时复用（TD-SCDMA）
      - FDMA
      - TDMA
      - CDMA
    - 随机接入
      - Aloha系列
      - CSMA/CD
      - CSMA/CA
    - 轮流访问
      - 蓝牙
      - 令牌网

要点

- 了解数据链路层所提供的服务
  - 组装帧
  - 差错检测、纠正
  - 多址接入技术
  - 可靠交付
    - 部分链路层协议提供，比如WiFi等高误码率线路
  - 流量控制
    - 部分链路层协议提供，主要在不提供可靠交付的链路层协议（如以太网，IEEE 802.3 pause）
    - 提供可靠交付的链路层协议不需要专门的流量控制
  - 半双工和全双工
    - 半双工通信的时候会提供收发转换

要点

- 以太网：无连接、不可靠的数据传输
  - 类型
    - DIX Ethernet
    - IEEE 802.3
  - MAC地址及编址方法
    - ARP
  - CSMA/CD
  - 集线器（共享式）和交换机（交换式）

P5

P5. 考虑 5 比特生成多项式，$G = 10011$，并且假设 D 的值为 1010101010。R 的值是什么？

- 考察校验码计算

```
1010101010 0000
10011
0011001010 0000
  10011
0001010010 0000
   10011
0000011110 0000
     10011
0000001101 0000
      1001 1
0000000100 1000
       100 11
0000000000 0100
```

R=0100

P8

P8. 在 6.3 节中，我们提供了时隙 ALOHA 效率推导的概要。在本习题中，我们将完成这个推导。

a. 前面讲过，当有 N 个活跃节点时，时隙 ALOHA 的效率是 $Np(1-p)^{N-1}$。求出使这个表达式最大化的 p 值。

b. 使用在（a）中求出的 p 值，令 N 接近于无穷，求出时隙 ALOHA 的效率。（提示：当 N 接近于无穷时，$(1-1/N)^N$ 接近于 $1/e$。）

考察ALOHA网络

a. $E(p) = Np(1-p)^{N-1}$

$$E'(p) = N(1-p)^{N-1} - Np(N-1)(1-p)^{N-2} = N(1-p)^{N-2}((1-p) - p(N-1))$$

$$E'(p) = 0 \Rightarrow p^* = \frac{1}{N}$$

b. $E(p^*) = N\frac{1}{N}(1-\frac{1}{N})^{N-1} = (1-\frac{1}{N})^{N-1} = \frac{(1-\frac{1}{N})^N}{1-\frac{1}{N}}$

$$\lim_{N\to\infty} E(p^*) = \frac{1}{e}$$

P11

P11. 假定 4 个活跃节点 A、B、C 和 D 都使用时隙 ALOHA 来竞争访问某信道。假设每个节点有无限个分组要发送。每个节点在每个时隙中以概率 p 尝试传输。第一个时隙编号为时隙 1，第二个时隙编号为时隙 2，等等。

a. 节点 A 在时隙 5 中首先成功的概率是多少？

b. 某个节点（A、B、C 或 D）在时隙 4 中成功的概率是多少？

c. 在时隙 3 中出现首个成功的概率是多少？

d. 这个 4 节点系统的效率是多少？

a. $\left(1 - p(1-p)^3\right)^4 p(1-p)^3$

b. $4\,p(1-p)^3$

c. $\left(1 - 4\,p(1-p)^3\right)^2 4\,p(1-p)^3$

d. $4\,p(1-p)^3$

注：有同学说如果严格按照课本上关于时隙ALOHA的设定，答案不是这样的。因为第一次竞争应该是失败的。没错，但是题目里面有额外的假设。我们改作业的时候有注意这个问题，并且没有在这方面扣分。

P23. 考虑图 6-15。假定所有链路都是 100Mbps。在该网络中的 9 台主机和两台服务器之间，能够取得的最大总聚合吞吐量是多少？你能够假设任何主机或服务器能够向任何其他主机或服务器发送分组。为什么？

P24. 假定在图 6-15 中的 3 台连接各系的交换机用集线器来代替。所有链路是 100Mbps。现在回答习题 P23 中提出的问题。

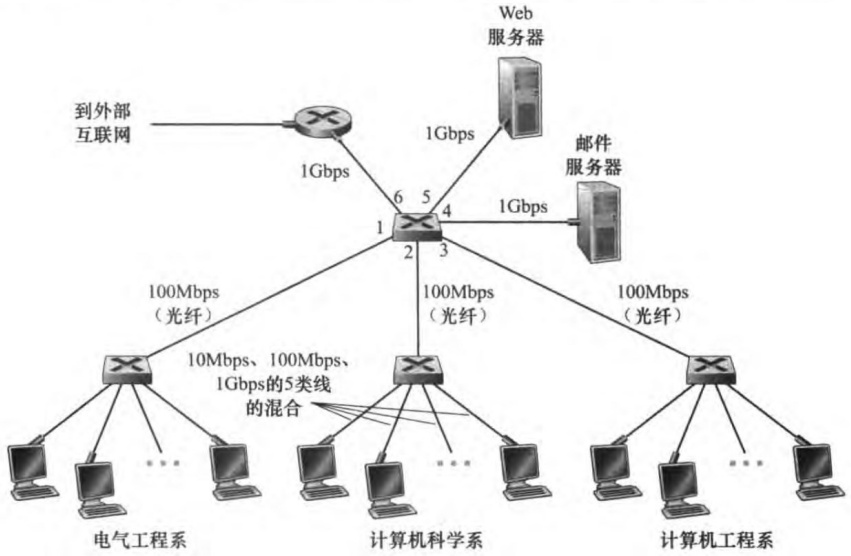
P25. 假定在图 6-15 中的所有交换机用集线器来代替。所有链路是 100Mbps。现在回答在习题 P23 中提出的问题。

只需要看冲突域的大小，冲突域大小乘以100Mbps就是答案!

P23. 1100Mbps

P24. 500Mbps

P25. 100Mbps



P26

P26. 在某网络中标识为 A 到 F 的 6 个节点以星形与一台交换机连接，考虑在该网络环境中某个正在学习的交换机的运行情况。假定：（i）B 向 E 发送一个帧；（ii）E 向 B 回答一个帧；（iii）A 向 B 发送一个帧；（iv）B 向 A 回答一个帧。该交换机表初始为空。显示在这些事件的前后该交换机表的状态。对于每个事件，指出在其上面转发传输的帧的链路，并简要地评价你的答案。

动作	交换机状态	交换机转发报文到	解释
B -> E	交换机学到了B的MAC地址	A, C, D, E, and F	**交换机不知道E的地址，所以向B之外的端口广播**
E -> B	交换机学到了E的MAC地址	B	**交换机知道B的地址，直接转发到对应端口**
A -> B	交换机学到了A的MAC地址	B	**交换机知道B的地址，直接转发到对应端口**
B -> A	交换机的状态不变	A	**交换机知道A的地址，直接转发到对应端口**

第七章
无线网络和移动网络

要点

- 无线网络
  - 分类
  - 特性
    - 隐藏节点、暴露节点
- IEEE 802.11 a/b/n/ac/ax
  - CSMA/CA
    - 信道预约机制/不使用信道预约机制的通信
  - AP和SSID
  - 802.11 Frame
  - AP间切换
- ITU 2G/3G/4G/5G
- 移动IP
- 承接上层协议时，与有线网络有何不同

R7 为什么 802. 11 中使用了确认，而有线以太网中却未使用？

- 因为无线信道具有高误码率，所以使用需要进行确认，以减少数据链路层的数据损坏
- 有线以太网误码率很低，故不使用确认机制。

R11

7.3.4节讨论了802. 11移动性，其中无线站点从一个BSS到同一子网中的另一BSS。当AP是通过交换机互连时，为了让交换机能适当地转发帧， 一个AP可能需要发送一个带有哄骗的MAC地址的帧，为什么?

- 因为交换机是根据MAC地址来确定将帧转发到哪个端口。
- 当一个无线节点转移之后，为正确转发通向那个无线节点的帧，新的AP会广播一个含有该无线站点MAC地址的帧，迫使交换机重新学习该无线站点的条目。
- 之后发向给无线站点的帧会被交换机正确转发

P5. 假设有两个 ISP 在一个特定的咖啡馆内提供 WiFi 接入，并且每个 ISP 有其自己的 AP 和 IP 地址块。

a. 进一步假设，两个 ISP 都意外地将其 AP 配置运行在信道 11。在这种情况下，802.11 协议是否将完全崩溃？讨论一下当两个各自与不同 ISP 相关联的站点试图同时传输时，将会发生什么情况。

b. 现在假设一个 AP 运行在信道 1，而另一个运行在信道 11。你的答案将会有什么变化？

a. 首先，我们需要假定这两个AP有不同的SSID和MAC地址。当一个无线站点给其关联的AP发送一个帧时，另一个AP虽然会收到，但是会忽视它（除非你开了monitor mode），因为帧中的MAC地址显示这并不是发送给它的。所以802.11允许这种现象出现。如果发生同时传输，那么两个站点发送的数据大概率会发生碰撞，各自进行回退，这两个AP的接入带宽会受到影响。

b. 这个时候不会发生碰撞，互不影响。

P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（如果侦听到该信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢?

- 此题描述的是不使用信道预约机制的CSMA/CA，先复习一下:

当节点有帧要发送时，侦听信道:

1）若一开始就侦听到信道空闲，等待DIFS时间后发送帧
2）否则，选取一个随机回退值，在侦听到信道空闲时递减该值；在此过程中若侦听到信道忙，冻结计数值
3）当计数值减为0时，发送整个帧并等待确认
4）若收到确认帧，表明帧发送成功，若还有新的帧要发送，从第2步开始CSMA/CA；若未收到确认，重新进入第2步中的回退阶段，并从一个更大的范围内选取随机回退值

P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（如果侦听到该信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢?

也就是发完帧之后不可以直接连续发送帧，还需要侦听信道是否空闲。不论空闲与否，都要等待一段时间。

这样的设计是为了保证节点之间能够尽量以**公平**的机会发送数据。

注：在TCP的拥塞控制算法设计中也有考虑和一个连接与其他TCP连接之间的公平。

第8章 网络安全

要点

- 有习题就有考点，但是这章好像内容有点多而且乱……
- 网络中的通信安全
  - 机密性、端点鉴别、报文完整性、运行安全性
  - 常见的安全机制
- 密码学基础
  - RSA、DES、AES、CBC
- 报文完整性与数字签名
- 网络安全应用
  - 加密邮件PGP、加密通信层TLS、网络层安全协议IPSec与VPN、ESP；
  - 早期的WiFi安全协议 WEP；
  - 防火墙与IDS

P8. 考虑具有 $p=5$ 和 $q=11$ 的 RSA。

a. n 和 z 是什么?

b. 令 e 为 3。为什么这是一个对 e 的可接受的选择?

c. 求 d 使得 $de=1 \pmod{z}$ 和 $d<160$。

d. 使用密钥 (n, e) 加密报文 $m=8$。令 c 表示对应的密文。显示所有工作。提示:为了简化计算,使用如下事实。

$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

RSA算法:生成密钥

- 选择两个大素数p和q(典型值为大于10^{100})
- 计算 n=p×q 和 z=(p-1) × (q-1)
- 选择一个与 z 互质的数,令其为 d
- 找到一个 e 使满足 e×d=1 (mod z)
- 公开密钥为 (e, n),私有密钥为 (d, n)

- 加密方法:
  - 将明文看成是一个比特串,将其划分成一个个数据块M,且有0≤M<n
  - 对每个数据块M,计算$C=M^e \pmod n$,C即为M的密文

a. $n = pq = 55, z = (p-1)(q-1) = 40$

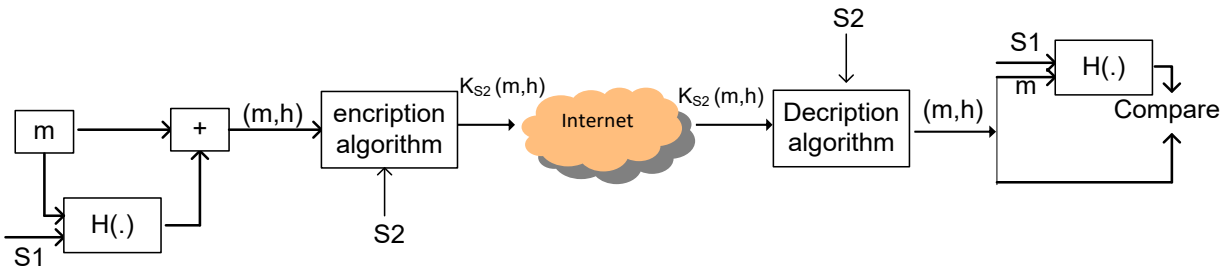
b. 因为e小于z,且与z没有公因数(也就是互质数)

c. $3d = 1 \pmod{40}$,得到$d = 27, 67, 107, 147$ $(d < 160)$

d. $m = 8, m^e = 8^3 = 512, c = m^e \bmod n = 512 \bmod 55 = 17$

P12

P12. 假定 Alice 和 Bob 共享两个秘密密钥：一个鉴别密钥 S_1 和一个对称加密密钥 S_2。扩充图 8-9，使之提供完整性和机密性。



- 其中$H(\cdot)$是哈希函数，h是哈希函数对报文m的输出

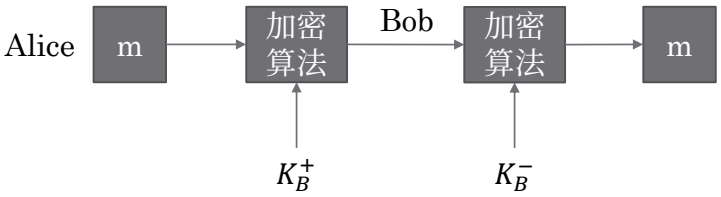
P18

P18. 假定 Alice 要向 Bob 发送电子邮件。Bob 具有一个公共－私有密钥对（K_B^+，K_B^-），并且 Alice 具有 Bob 的证书。但 Alice 不具有公钥私钥对。Alice 和 Bob（以及全世界）共享相同的散列函数$H(\cdot)$。

a. 在这种情况下，能设计一种方案使得 Bob 能够验证 Alice 创建的报文吗？如果能，用方框图显示 Alice 和 Bob 是如何做的。

b. 能设计一个对从 Alice 向 Bob 发送的报文提供机密性的方案吗？如果能，用方块图显示 Alice 和 Bob 是如何做的。

- 不能，原因是Bob没有Alice的公钥私钥对或者Alice的预先共享密钥。Bob无法验证Alice创建的报文。
- 可以。Alice可以直接用Bob的公钥加密。



从改卷者的角度对大家的建议

- 重视选择题
  - 期中考试，十成甚至**九成**的同学选择题就没了10分
  - 说到底还是因为需要集中精力抠字眼，很蓝的啦
- 问答题 or 主观题
  - 理解力很重要——例如期中考试第三道主观题，老师暗示了该如何去回答，但是似乎没有起作用
  - 同样表达能力也很重要，用尽可能简练（不是少！）的文字把**要点**答对
  - 改卷时改这部分相当痛苦！如有同学接下来要做这门课的助教，建议别改这个部分
- 计算题 or 大题
  - 复习各章作业吧
- 用考研题练手?
  - 之前有几届助教试过搞一些考研题，包括在习题课上使用，我个人觉得可以，但是显然你科的课程和外面差别还是很大的

从改卷者的角度对大家的建议（续）

- 小抄
  - 一定要保证上面的话是**正确的，直接的，中肯的，雅致的，客观的，完整的**。否则万一抄到试卷上的话是错的或者选择题纠结的时候看到了上面的鬼话，那就很寄
  - 根据老师期中考试扣字眼的习惯，个人觉得ppt上有很多东西大家没有注意到
    - 比如申必的TCP起始序号选择
    - 还有分组交换引入了什么延迟
  - 所以自己做一份或者自己审核一遍才是坠吼的！~~（当然还是看你时间多不多）~~

完

祝大家~~考试~~顺利返乡，~~喜气洋洋~~过大年，我们下学期见！

HW1 Solutions

计算机网络 011144.01

Fall 2022

Lecturer: 华蓓

TA: 贺若舟, 应宇峰, 孙若培, 梁奕涵, 梁峻滔

Posted: Sep. 19, 2022

Editor: 梁峻滔

Answer 1: P9

1. 使用电路交换, 需要为每个用户预留 100kbps 的资源, 则可支持的最大用户数量为

$$\frac{1Gbps}{100kbps} = 10,000$$

2. 记有 n($n \leq M$) 个用户发送数据的概率为 Pr[n], 相当于从 M 个用户中挑出 n 个, 挑中某个用户的概率为 p, 则

$$Pr[n] = \binom{M}{n} p^n (1-p)^{M-n}$$

那么多于 N 个用户发送数据的概率就是求和即可, 即

$$\sum_{n=N+1}^{M} Pr[n] = \sum_{n=N+1}^{M} \binom{M}{n} p^n (1-p)^{M-n}$$

Answer 2: P10

1. 链路时延包括传输时延 $\frac{L}{R_i}$ 和传播时延 $\frac{d_i}{s_i}$, 有三条链路; 交换机时延包括排队时延 (本题没有) 和处理时延 d_{proc}, 有两个交换机. 求和即得总的端到端时延 d_{all}

$$d_{all} = \sum_{i=1}^{3} \frac{d_i}{s_i} + L \sum_{i=1}^{3} \frac{1}{R_i} + 2d_{proc}$$

2. 代入数据计算

$$\begin{aligned} d_{all} &= \frac{5000km + 4000km + 1000km}{2.5\times10^8 m/s} + 3\frac{1500bytes}{2\times10^6 bps} + 2\times3ms \\ &= 40ms + 3\frac{1500\times8bits}{2\times10^6 bps} + 6ms \\ &= 40ms + 18ms + 6ms = 64ms \end{aligned} \tag{1}$$

P.S. 有不少同学算错结果了, 需要注意 $L = 1500$ 字节, 一个字节 (byte) 是 8bit, 而"bps" 中的"b" 指的是 bit.

Answer 3: P13

1. 有 N 个分组同时到达一条链路, 则第 i 个传输的分组需要等待前面 i-1 个分组传输完, 即第 i 的传输的分组的等待时间为 $(i-1)\frac{L}{R}$, 那么平均等待时间为

$$\frac{\sum_{i=1}^{N}\frac{(i-1)L}{R}}{N}=\frac{(N-1)L}{2R}$$

2. 想象分组是一批一批地到达, 每一批有 N 个分组, 现在是每隔 LN/R 才有新的一批分组到达, 此时前面一批刚好全部传输完了, 完全不影响新一批分组的传输, 因此平均排队时延与前一问相同.

Answer 4: P21

1. 首先一条链路的吞吐量就是其传输速率 (回顾定义), 一条路径的吞吐量等于其瓶颈链路的吞吐量, 当我们仅能使用一条路径时, 我们首先应该求出每条路径的吞吐量 (等于其瓶颈链路传输速率), 然后取最大的那条路径. 第 k 条路径的吞吐量为

$$R^k=\min_{1\le i\le N}R_i^k$$

那么取最大的一条路径, 可以取得的最大吞吐量为

$$maxR=\max_{1\le k\le M}R^k$$

2. 能使用全部路径, 则最大吞吐量就是全部 M 条路径的吞吐量之和

$$maxR=\sum_{k=1}^{M}R^k$$

Answer 5: P22

1. 要分组被成功接收, 就需要每一条链路都不丢包, 记分组被成功接收的概率为 P_s, 则

$$P_s = (1-p)^N$$

2. 记重传次数为 X, 重传 i 次才成功的概率为 Pr[X=i], 则

$$Pr[X=i] = (1-P_s)^i P_s$$

要求平均重传次数, 就是求期望

$$\begin{aligned} E[X] &= \sum_{i=1}^{\infty} i \cdot Pr[X=i] \\ &= \sum_{i=1}^{\infty} i \cdot (1-P_s)^i P_s \\ &= P_s \cdot \sum_{i=1}^{\infty} i \cdot (1-P_s)^i \\ &= P_s \cdot \frac{1-P_s}{P_s^2} \\ &= \frac{1}{P_s} - 1 \end{aligned} \tag{2}$$

fact: $for \quad |x|<1, \sum_{k=0}^{\infty} kx^k = \frac{x}{(1-x)^2}$
P.S. 有很多同学是直接给出结果, 但是像这种求平均重传次数, 结果并不是显然的, 好歹要给出一些求解过程, 比如有些同学写到利用几何分布的均值, 这也是可以的.

Answer 6: P25

1. $R \cdot t_{prop} = 2Mbps \times \frac{20000km}{2.5\times10^8 m/s} = 160,000bits$

2. $800000 > 160000$, 在任何给定的时间, 在链路上具有的比特数量最大值就是 160,000bits.

3. 就是在链路上具有的比特数量最大值.

4. $\frac{20000km}{160000bit} = 125m/bit$, 比一个足球场更长.

5. 一个比特的宽度 = 链路长度 / 链路上的比特数量, 即

$$\frac{m}{R \cdot t_{prop}} = \frac{m}{R \cdot \frac{m}{s}} = \frac{s}{R}$$

Answer 7: P31

1. 从源主机到第一台分组交换机移动报文需要

$$\frac{L}{R} = \frac{8\times10^6 bit}{2Mbps} = 4s$$

因为是分组交换, 有 3 段链路, 所以移动到目的主机总共需要

$$4s\times3 = 12s$$

2. 分段后一个分组长度为 $L = 10000$bits, 则从源主机移动第一个分组到第一台交换机需要

$$\frac{L}{R} = \frac{10000bit}{2Mbps} = 5ms$$

从第一台交换机发送第一个分组到第二台交换机和从源主机发送第二个分组到第一台交换机各需要 5ms, 从源主机发送第一个分组开始后 10ms, 第二个分组能被第一台交换机全部收到.

3. 分组数量 N=800, 最后一个分组开始发送需要等待

$$\frac{(N-1)L}{R} = 799\times5ms$$

最后一个分组从发送到它到达目的主机需要 $3\frac{L}{R}$, 故总时间为

$$\frac{(N+2)L}{R} = 4.01s$$

相当于 (a) 的 1/3, 是因为分段后传输过程可以流水化, 提高了链路的利用率.

4. 每一个分组更小, 每个交换机处理和传输一个分组的时间减少, 有利于减小排队时延; (后面会学到) 当分组出错或丢失时需要重传, 分段后分组更小, 重传代价小.

5. 各个分组需要在接收方重新进行组装; 报文分段后, 需要在每个小分组加上一些 headers, 降低了有效载荷的比例/增加开销.
P.S. 有不少同学答了" 各个分组需要按序发送/接收", 这是不对的, 这不属于分段的缺点, 到后面 TCP/IP 会学到, 只需要在目的地正确重组即可, 不需要按序发送/接收.

Answer 8: P33

$$
\begin{aligned}
N &= \frac{F}{S} \\
d_{all} &= \frac{(N-1)L}{R} + 3\frac{L}{R} \\
&= (N+2)\frac{L}{R} \\
&= (\frac{F}{S}+2)\frac{80+S}{R} \\
&= (F+160+\frac{80F}{S}+2S)/R \\
&\geq (F+160+2\sqrt{160F})/R
\end{aligned}
\tag{3}
$$

当且仅当 $\frac{80F}{S} = 2S$, 即 $S = 2\sqrt{10F}$ 时等号成立.

其他反馈:

- 给 10 分不代表全对, 建议同学们检查一下自己的作业有没有批注.
- 对于一些不那么直观的结论, 例如 P22 求平均重传次数, 需要写出求解过程, 用到的相关结论也要说明, 否则有理由怀疑是抄袭.
- 简答题需要回答清楚，不能过于简陋以至于可以有多种解读，否则期中期末的简答题可能会被薄纱... 例如 P31 的 (d)，需要答清楚为什么便于差错检测，为什么可以减少重传的开销，(e) 要答清楚在哪里、对什么排序，而不是简单的”需进行排序 “，真的让人很想扣分!

HW2 Solutions

计算机网络 011144.01

Fall 2022

Lecturer: 华蓓

TA: 贺若舟, 应宇峰, 孙若培, 梁奕涵, 梁峻滔

Posted: Oct. 17, 2022

Editor: 梁峻滔

Solution 1: P1

1. False. 获取每个对象都需要发送一个请求，客户将发送 4 个请求报文.
2. True. 位于同一个服务器上就可以通过同一个持续连接发送.
3. False. HTTP 比 TCP 更高层的协议, 有可能一个 HTTP 报文由多个 TCP 段组成, 但是一个 TCP 段是不可能携带两个不同的 HTTP 请求报文的.
   (有很多同学答的是, 在非持续连接的情况下, 每发一个请求都需要建立一个新的连接, 不过题目讨论的是一个 TCP 段 (segment), 不是一个 TCP 连接, 当然也可能是作者笔误)
4. False. Date 是服务器响应时间 (产生和发送响应报文的时间).
5. False. 比如 304 Not modified 就是空的报文体.

Solution 2: P3

运输层: TCP、UDP
应用层: DNS
注: HTTP 使用 TCP, DNS 使用 UDP.

Solution 3: P7

使用 DNS 查询到服务器 IP 地址需要 $\sum_{i=1}^{n} RTT_i$.
使用 HTTP 请求对象时, 因为传输层协议是 TCP, 需要一个 RTT_0 来建立连接, 然后请求对象和接收响应也需要一个 RTT_0, 而使用 DNS 查询时传输层协议是 UDP, 不需要建立连接.
所以总时间是 $\sum_{i=1}^{n} RTT_i + 2RTT_0$.

Solution 4: P8

1. 在同一服务器上, 所以 DNS 查询只需要执行一次.
   非持续 HTTP, 所以每请求一个对象就需要建立一个 TCP 连接.
   没有并行 TCP 连接, 所以是请求并接收到一个对象后才开始下一个请求.
   同 P7, 用 HTTP 请求一个对象包括建立连接, 所以一个对象就需要 $2RTT_0$. 所以总时间为
   $$\sum_{i=1}^{n} RTT_i + 2RTT_0 \cdot 9 = \sum_{i=1}^{n} RTT_i + 18RTT_0$$

2. 非持续 HTTP, 每请求一个对象就需要建立一个 TCP 连接.
   配置有 5 个并行 TCP 连接, 所以可以同时请求 5 个对象. 那么 8 个引用对象就需要分两批请求.
   但需要注意的是, 引用对象是在接收到 HTML 文件后才请求的.
   所以总时间为
   $$\sum_{i=1}^{n} RTT_i + 2RTT_0 + 2RTT_0 \cdot 2 = \sum_{i=1}^{n} RTT_i + 6RTT_0$$

3. 持续 HTTP, 可以在同一个连接请求所有对象, 同样需要注意引用对象是在接收到 HTML 文件后才请求.
   流水线方式 (HTTP1.1 默认): $\sum_{i=1}^{n} RTT_i + 2RTT_0 + RTT_0 = \sum_{i=1}^{n} RTT_i + 3RTT_0$
   其中 $2RTT_0$ 是建立连接和请求 HTML 文件, 后面一个 RTT_0 是流水线请求 8 个引用对象.
   非流水线方式: $\sum_{i=1}^{n} RTT_i + 2RTT_0 + 8RTT_0 = \sum_{i=1}^{n} RTT_i + 10RTT_0$

Solution 5: P9

1. $\beta = 16s^{-1}$, $\Delta = \frac{850000bit}{15Mbps} = \frac{17}{3} \times 10^{-2}s$
   平均接入时延为 $\frac{\Delta}{1-\Delta\beta}$
   平均因特网时延 3s
   则平均响应时间为
   $$\frac{\Delta}{1-\Delta\beta} + 3s = 3.607s$$
   PS, 这里算不算局域网的时延都可以 (题目不要求).

2. 注意此题题目中英文版本有差异, 英文版原文是"miss rate is 0.4", 而中文版是" 命中率为 0.4", 两种情况都给对.
   (1) 命中率为 0.4:
   $\beta = 16 \times 0.6$, 代入计算得访问因特网的平均响应时间为 3.124s, 但是注意需要用到因特网的情况只有 60%, 所以平均响应时间为
   $$3.124 \cdot 0.6 + 0 \cdot 0.4 = 1.874s$$
   (2)miss rate = 0.4:
   $\beta = 16 \times 0.4$, 访问因特网的平均响应时间为 3.089s, 总的平均响应时间为
   $$3.089 \cdot 0.4 + 0 \cdot 0.6 = 1.236s$$

其他反馈:

- 给 10 分不代表全对, 一些小错误不扣分, 但考试的时候肯定是会扣的, 建议同学们检查一下自己的作业有没有批注.
- P8.Q3 只答流水线方式/非流水线方式一种的不扣分，但也需要注意考虑问题要全面.
- 是非判断题不写原因不扣分，但同学们需要注意理解为什么.

HW3 Solutions

计算机网络 011144.01

Fall 2022

Lecturer: 华蓓 Posted: Oct. 24, 2022

TA: 贺若舟, 应宇峰, 孙若培, 梁奕涵, 梁峻滔 Editor: 梁峻滔

Solution 1: P15

分组长度 $L = 1500$ bytes, 传输速率 $R = 1Gbps = 1 \times 10^9 bps$, $RTT = 30ms$. 设窗口长度为 N. 参考如下流水线方式:

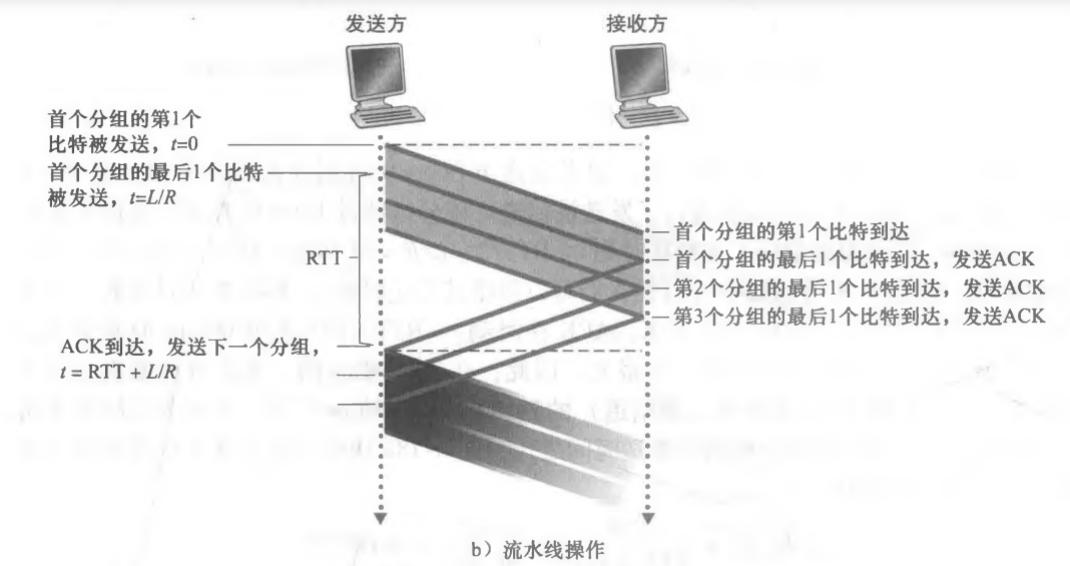


图 3-18 停等和流水线发送

只需要满足 $(N-1)\frac{L}{R} \leq RTT$, 即 $N \leq 2501$ 即可 (为什么会有这个限制?). 信道利用率为

$$U_{sender} = \frac{N\frac{L}{R}}{RTT + \frac{L}{R}}$$

英文版要求信道利用率大于 98%, 而中文版要求的是 90%, 两种都给对 (但是居然有同学用 90% 算出 2451, 这是怎么回事呢?).

英文版:

$$\begin{aligned} U_{sender} &= \frac{N\frac{L}{R}}{RTT + \frac{L}{R}} > 0.98 \\ \Rightarrow N &> \frac{0.98RTT}{\frac{L}{R}} + 0.98 = 2450.98 \\ \Rightarrow N &\geq 2451 \end{aligned}$$

中文版:

$$U_{sender} = \frac{N\frac{L}{R}}{RTT + \frac{L}{R}} > 0.90$$
$$\Rightarrow N > \frac{0.90RTT}{\frac{L}{R}} + 0.90 = 2250.90$$
$$\Rightarrow N \geq 2251$$

Question: 如果不考虑拥塞控制, 则发送窗口是不是可以无限增大? 发送窗口的大小与传输速率 R 有关系吗?

Solution 2: P22

GBN 协议, 发送方窗口大小 $N = 4$, 序号范围是 1024($0 \sim 1023$ **or** $1 \sim 1024$), 接收方期待的下一个有序分组的序号为 k, 即已经收到 $k-1$.

(a) 接收方已经收到 $k-1$, 则发送方已经发送 $k-1$, 但可能还没收到确认, 则这时 $k-1$ 号包仍留在发送窗口里, 往前推有可能 $k-1, ..., k-N$ 都没收到确认, 这样的话它们都会留在发送窗口里; 如果已收到 $k-1$ 的确认, 则发送方窗口是 $\{k, k+1, ..., k+N-1\}$.

所以在 t 时刻, 发送方窗口内的序号可能是 $\{k-N, ..., k+N-1\}$ 中连续的 N 个 (注意所有加减操作均为模 1024). 把 $N = 4$ 代入就是 $\{k-4, ..., k+3\}$ 中连续的 4 个.

(b) $\{k-1, ..., k-N\}$ 的 ACK 都可能在途中. 但 $k-N-1$ 不可能在途中, 因为那样的话发送方窗口就应包含 $k-N-1$, 从而不可能包含 $k-1$(发送窗口大小为 N). 因此在 t 时刻, 在途中的 ACK 序号可能的集合是 $\{k-4, ..., k-1\}$.

注意:

- 序号空间为 k 不是指最多只能发 k 个包, 而是序号就在 $0 \sim k-1$ 之间循环使用 (模 k 加)

Solution 3: P23

图 3-27:

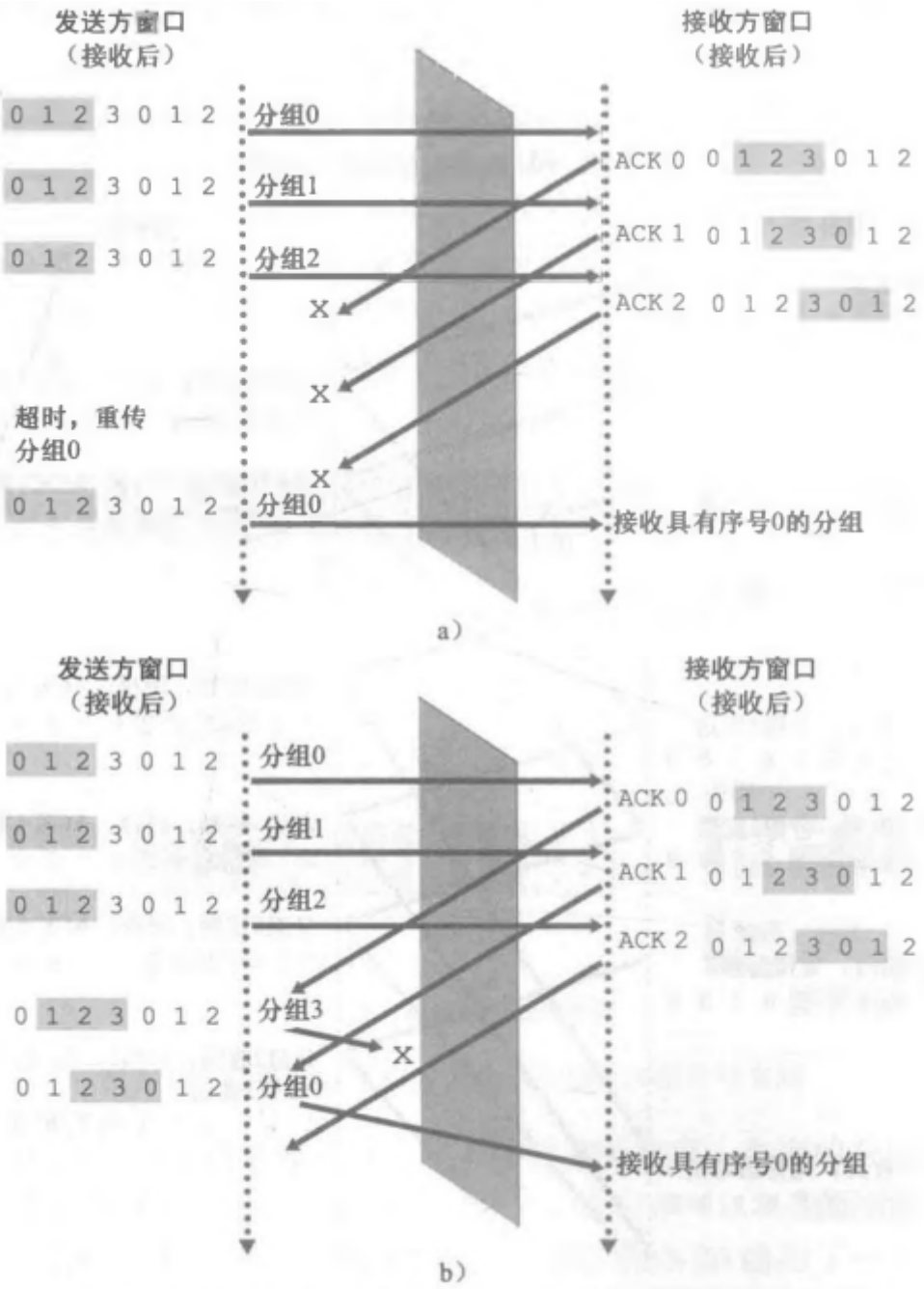
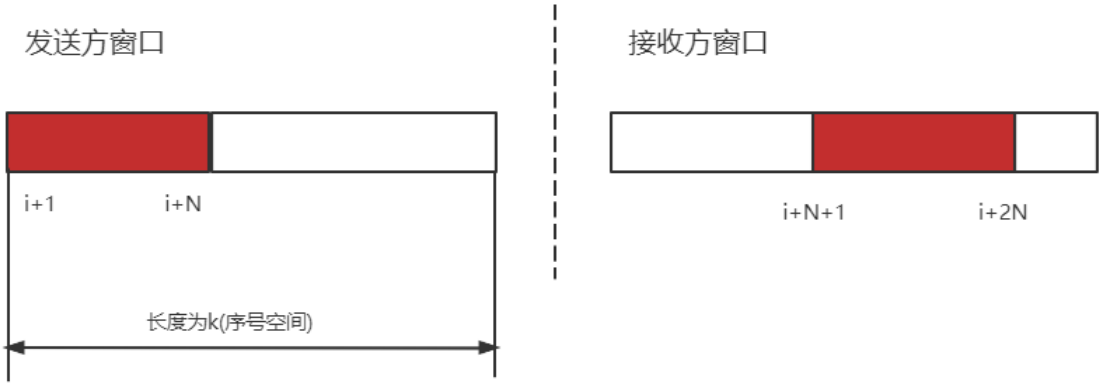


图 3-27 SR 接收方窗口太大的困境：是一个新分组还是一次重传

- SR 协议: 发送方窗口大小 = 接收方窗口大小, 记为 N.
  最坏情况下就是发送窗口的所有段都发过去了, 接收方也都收到了, 但是所有的 ACK 都丢失了, 就会有如下情况: 接收方窗口向前推进了 N.



  如果要避免图 3-27 的情况, 就要求这两个部分的序号没有重叠, 即 $\{i+1, ..., i+N\}$ 与 $\{i+N+1, i+2N\}$ 没有重叠 (注意加法操作是在模 k 意义下), 所以就是两个加起来的长度 $2N$ 要不大于序号空间 k, 即 $N \leq \frac{k}{2}$.

- GBN 协议: 相当于接收方窗口大小为 1. 即 $\{i+1, ..., i+N\}$ 与 $\{i+N+1\}$ 没有重叠 (加法操作是在模 k 意义下), 所以 $N \leq k-1$.

注意:

- 有同学直接给出结果的, 问题是, 老师的 slides 已经给出结果了, 做这道题肯定是要讨论证明一下的呀, 不给证明的会扣分.

Solution 4: P25

(a) TCP 协议将发送的数据放入发送缓冲区 (send buffer), 然后将发送缓冲区内的数据按 byte 封装成 TCP 段 (segment), 接收方可能一次收到多于一个或少于一个应用层报文 (message), 即数据可能被组装, 也可能被拆分 (分段), 发送方不能指定一个 TCP 段具体发送哪些数据; 而 UDP 协议则是直接将来自应用层的报文打包作为有效载荷 (payload) 交付给网络层, 接收方每次获得一个完整的应用层报文.

(b) TCP 协议会进行拥塞控制和流量控制, 而且要建立连接, 这些会带来延迟和重传, 数据的发送时机无法由发送方单独决定; 而 UDP 协议不需要进行上述操作, 不会有相应延迟, 更有即时性.

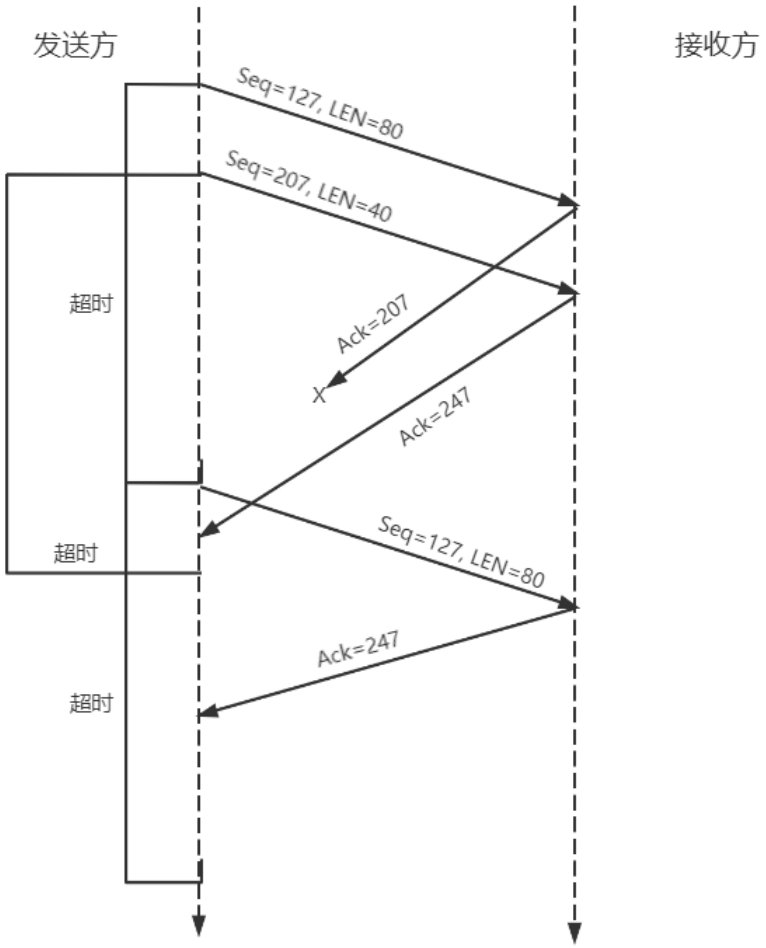
Solution 5: P27

(a) 序号: $127 + 80 = 207$, 源端口号:302, 目的端口号:80.

(b) 确认号就是接收方期待的下一个字节序号:207, 源端口号:80, 目的端口号:302.

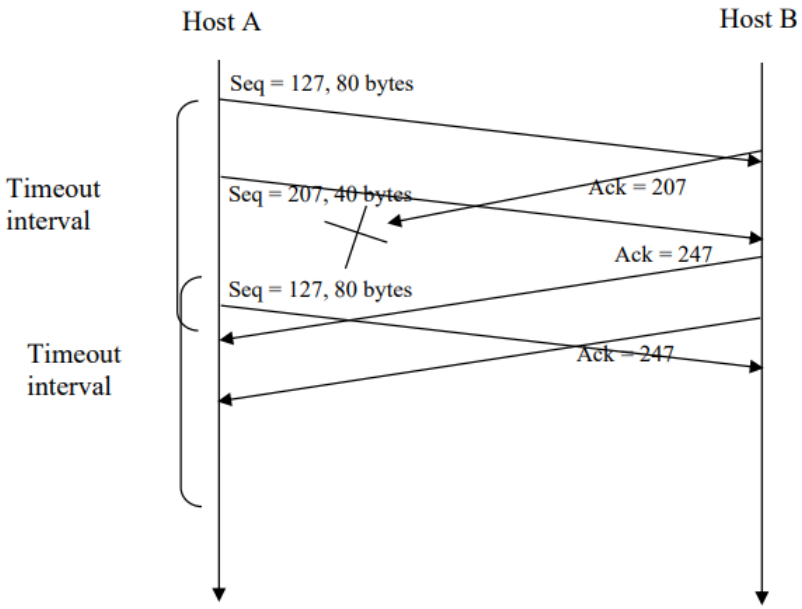
(c) 第二个报文段在第一个报文段之前到达, 接收方期待的下一个字节序号仍是第一个报文段的, 所以确认号仍为 127.

(d) 时序图:



注意:

- 画图应体现 Ack=247 是超时后到达的.
- 很多同学直接抄答案都不带检查的, 重传的 Seq=127 的箭头跟第二次 Ack=247 的起点不重合, 那肯定是有问题的. 以下是那张有问题的图:



是不是很熟悉？凡是见到这个痕迹的会加大扣分力度.

Solution 6: P37

(a) 加下划线表示丢失

- GBN(注意 GBN 不缓存失序分组)

  主机 A: 1, 2, 3, 4, 5, 2, 3, 4, 5　主机 B(**ACK**): 1, _, 1, 1, 1, 2, 3, 4, 5

  主机 A 共发送 9 个报文段, 主机 B 共发送 8 个 ACK.

- SR

  主机 A: 1, 2, 3, 4, 5, 2　主机 B(**ACK**): 1, _, 3, 4, 5, 2

  主机 A 共发送 6 个报文段, 主机 B 共发送 5 个 ACK.

- TCP

  主机 A: 1, 2, 3, 4, 5, 2　主机 B(**ACK**): 2, _, 2, 2, 2, 6

  主机 A 共发送 6 个报文段, 主机 B 共发送 5 个 ACK.

(b) 超时值比 5RTT 长得多, GBN 发的分组最多而且要等超时才会重传; SR 也需要等超时才会重传第二个报文段; TCP 在收到三个冗余 ACK 后 (3RTT) 就会重传, 所以是 TCP 会在最短的时间间隔中成功交付所有报文段.

Solution 7: P40

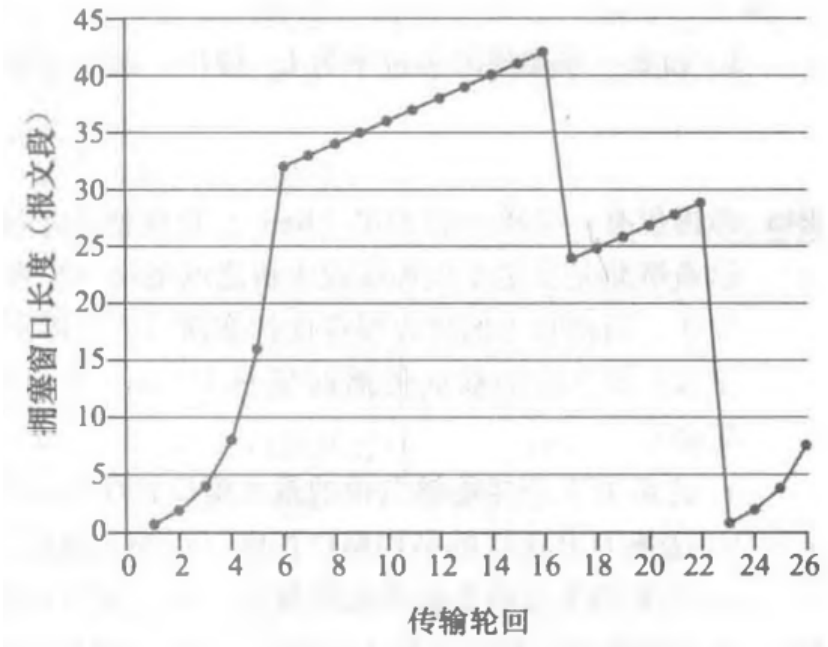


图 3-58　TCP 窗口长度作为时间的函数

cwnd: 拥塞窗口长度
ssthresh: 从慢启动转成拥塞避免的 cwnd 阈值

(a) 属于慢启动阶段 (cwnd 按 2-指数增长) 的区间: [1, 6], [23, 26]

(b) 属于拥塞避免阶段 (cwnd 按线性增长) 的区间: [6, 16]

(c) 根据 3 个冗余 ACK. 因为第 16 个 RTT 时 $cwnd = 42$, 第 16 个 RTT 过后 $cwnd = 24 = \frac{42}{2} + 3$.

(d) 根据超时. 因为第 22 个 RTT 时 $cwnd = 29$, 第 22 个 RTT 后 $cwnd = 1 \neq \frac{29}{2} + 3$, 而且可以看出后面紧跟的是慢启动.

(e) 在第 1 个 RTT 时, $ssthresh = 32$(从第一次慢启动阶段与拥塞避免阶段的转折点可以看出).

(f) 在第 18 个 RTT 时, $ssthresh = 21$. 因为在前面第 16 个 RTT 时经历了 3 个冗余 ACK, 导致 $ssthresh = \frac{cwnd}{2} = \frac{42}{2} = 21$.

(g) 在第 24 个 RTT 时, $ssthresh = 14$. 因为在前面第 22 个 RTT 时经历了超时, 导致 $ssthresh = \frac{cwnd}{2} = \frac{29}{2} = 14$.

(h) 前面 6 个 RTT 的报文段数求和为 $1 + 2 + 4 + 8 + 16 + 32 = 63$, 第 7 个 RTT 传输 33 个报文段, 因此可知第 70 个报文段是在第 7 个 RTT 里发送的.

(i) 在第 26 个 RTT 时, $cwnd = 8$, 此时收到 3 个冗余 ACK, 有

$$ssthresh = \frac{cwnd}{2} = 4$$
$$cwnd = ssthresh + 3 = 7$$

(j) 使用 TCP Tahoe(对 3 个冗余 ACK 的处理同超时的处理), 在第 16 个 RTT 时, $cwnd = 42$, 收到 3 个冗余 ACK, 则

$$ssthresh = \frac{cwnd}{2} = 21$$
$$cwnd = 1$$

然后开始慢启动, 在第 19 个 RTT 时, $ssthresh = 21$, $cwnd = 4$.

(k) 使用 TCP Tahoe, 延续 (j) 的结果, 在第 17 个 RTT 到第 22 个 RTT 期间, $ssthresh = 21$, 一共发送

$$1 + 2 + 4 + 8 + 16 + 21 = 52$$

个分组.

注意: 区分 ssthresh 和 cwnd 和它们的行为.

Question: 图 3-58 有快速恢复 (Fast Recovery) 阶段吗? 快速恢复和快速重传 (Fast Retransmit) 是同一个东西吗?

注: [17, 22] 区间按老师 PPT 上的状态图解释, 应该是属于快速恢复阶段而不是拥塞避免.

Solution 8: P44

(a) 不具有慢启动, 就是每收到一个 ACK 就增加一个 MSS, 如果没有丢包, 就是每经过一个 RTT 就增加一个 MSS. 所以 cwnd 从 6MSS 增加到 12 个 MSS, 需要花费 6RTT.

(b) cwnd 初始为 6MSS, 则 6RTT 内的平均吞吐量为

$$\frac{6+7+8+9+10+11}{6} = 8.5MSS/RTT$$

Solution 9: P45

(a) 题目的意思是, cwnd 从 $\frac{W}{2}$ 变到 W 的过程中, 在 $cwnd = W$ 发送完后丢失了一个分组. 假设是拥塞避免阶段, 发送的分组数量为

$$\frac{W}{2} + (\frac{W}{2}+1) + ... + W = \frac{3}{8}W^2 + \frac{3}{4}W$$

故丢包率为 $L = \frac{1}{\frac{3}{8}W^2+\frac{3}{4}W}$.

Question: 如果 cwnd 从 $\frac{W}{2}$ 变到 W 是慢启动阶段呢?

(b) 回顾第三章的一张 slide:

TCP吞吐量

一个长期存活的TCP连接的平均吞吐量是多少？（忽略慢启动阶段）

- 令W=发生丢包时的CongWin，此时
  throughput = W/RTT
- 发生丢包后调整 CongWin=W/2，此时
  throughput=W/2RTT
- 假设在TCP连接的生命期内，RTT 和 W几乎不变，则：Average throughout=0.75 W/RTT

Transport Layer 3-150

注意 slide 中的 W 是窗口大小, 单位是分组. 使用上一问的结果, 我们有

$$L = \frac{1}{\frac{3}{8}W^2 + \frac{3}{4}W}$$

当 W 足够大时, $\frac{3}{8}W^2 \gg \frac{3}{4}W$, 则

$$L \approx \frac{1}{\frac{3}{8}W^2}$$

$$\Rightarrow W \approx \sqrt{\frac{8}{3L}}\ \text{MSS}$$

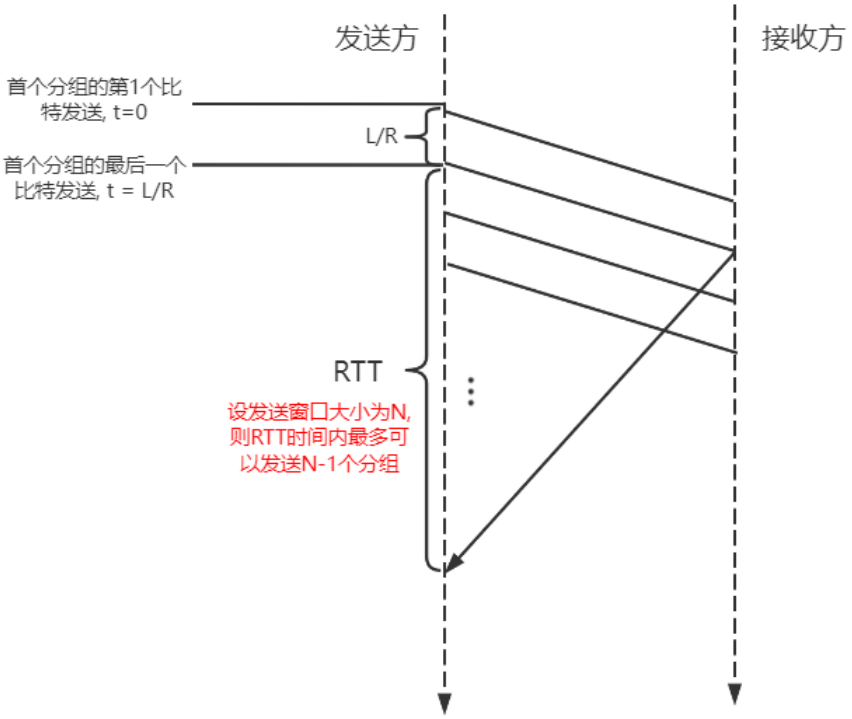
MSS 是一个分组的数据量单位. 代入经验公式,

$$\text{Average throughput} = 0.75W/\text{RTT} = 0.75 \times \sqrt{\frac{8}{3L}}\ \text{MSS/RTT} = \frac{1.22\ \text{MSS}}{\text{RTT}\sqrt{L}}$$

Solution 10: P46

每个 TCP 报文段长度 $L = 1500$ bytes, 链路传输速率 $R = 10$ Mbps, RTT $= 0.15$ s. 设发送窗口大小为 W.

(a) 考虑下图



则有

$$(W-1)\frac{L}{R} \leq \text{RTT}$$
$$\Rightarrow W \leq \frac{\text{RTT}}{L/R} + 1 = \frac{0.15}{1500 \times 8/10 \times 10^6} + 1 = 126$$

因此最大窗口长度为 126.

PS: 几乎所有同学都是用的 $W\frac{L}{R} \leq$ RTT 算出是 125, 也给对, 不过还是要有分析过程, 就是这个式子是怎么来的.

(b) 平均窗口长度为 $0.75W = 94.5$(W=125 时为 93.75)
平均吞吐量为 $\frac{0.75W}{\text{RTT}} = \frac{94.5 \times 1500 \times 8}{0.15} = 7.56$ Mbps(或 7.5).

(c) 关于对题目中 “从丢包中恢复”, 有两种理解:

(a) ” 丢包” 指 3 个冗余 ACK, 从丢包中恢复指从快速恢复状态 (Fast Recovery) 转移到拥塞避免状态 (Congenstion Avoidance), 会有 $cwnd = ssthresh$ 的赋值, 而 ssthresh 值是发生 3 个冗余 ACK 时 cwnd 的一半. 所以在 $cwnd = 126$ 时发生丢包 (3 个冗余 ACK), 经过快速恢复后, $cwnd = \frac{126}{2} = 63$.
参考教材中一段关于快速恢复的描述:

3. 快速恢复

在快速恢复中，对于引起 TCP 进入快速恢复状态的缺失报文段，对收到的每个冗余的 ACK，cwnd 的值增加一个 MSS。最终，当对丢失报文段的一个 ACK 到达时，TCP 在降低 cwnd 后进入拥塞避免状态。如果出现超时事件，快速恢复在执行如同在慢启动和拥塞避免中相同的动作后，迁移到慢启动状态：当丢包事件出现时，cwnd 的值被设置为 1 个 MSS，并且 ssthresh 的值设置为 cwnd 值的一半。

(b) ”丢包”指超时, 这是一种更合理的理解, 因为 3 个冗余 ACK 实际上是收到了 3 个失序分组, 相对超时而言, 真正是丢包的可能性更小. 不过超时的话也会有 $ssthresh = 126/2 = 63$. 题目说了忽略慢启动, 所以恢复后也是从 $cwnd = 63$ 开始算起. 计算过程是一样的.

再次达到最大窗口需要收到 63 个新的 ACK, 即需要经过 $63*\text{RTT} = 63\times 0.15 = 9.45\text{s}$.

注意:

- 求拥塞窗口长度一般都是要向下取整的 (除非问的是期望或平均)

其他反馈:

- 给 10 分不代表全对, 一些小错误不扣分, 但考试的时候肯定是会扣的, 建议同学们检查一下自己的作业有没有批注.

学号：　　姓名：

1. 写出至少三种接入网技术。对于每一种接入网技术，指出使用的传输媒体是什么。

接入网技术：DSL，HFC，以太网，WiFi，3G，…… （写出三种即可）
DSL 使用双绞线，HFC 使用光纤和同轴电缆，以太网使用双绞线或光纤，WiFi 和 3G 使用电磁波

2. 分组在交换网络中要经历哪四种延迟？哪种延迟的变化范围最大？什么情况下会出现丢包？

四种延迟：处理延迟，排队延迟，传输延迟，传播延迟
排队延迟的变化范围最大。
当分组到达交换设备时，若输出链路的缓冲队列满，发生丢包。

3. 从高到低列出因特网协议栈的五个层次。主机上运行哪些层次？TCP 协议运行在哪个层次？IP 协议运行在哪个层次？HTTP 协议运行在哪个层次？

因特网协议栈的五个层次：应用层，传输层，网络层，数据链路层，物理层
主机上运行全部五个层次
TCP 运行在传输层
IP 运行在网络层
HTTP 运行在应用层

4. 分组交换和电路交换中的同步时分复用（TDM），都是让用户轮流使用链路，它们之间的区别是什么？

分组交换：用户使用链路的模式不固定
TDM：用户使用链路的模式固定

5. A 和 B 两个终端通过一台分组交换机连接到一起。两段链路的数据速率分别为 R1 和 R2，忽略信号传播时间。A 向 B 连续发送 2 个长度为 L 的分组。假设路径上没有其它分组传输，请问从 A 开始发送到 B 完整收到 2 个分组，其间经过了多长时间？（提示：分 R1≤R2 和 R1>R2 两种情况考虑）

若 R1≤R2，T = 2L/R1 + L/R2
若 R1>R2，T = L/R1 + 2L/R2

学号：　　姓名：

1. Alice 从她的终端登陆到公司的文件服务器上下载了 4 个文件。请问 Alice 的终端和公司的文件服务器之间总共建立了几条 TCP 连接？这些 TCP 连接分别用来传输什么？

   5 条连接。一条控制连接，用于传输命令和响应。四条数据连接，每条连接用于传输一个文件。

2. 在某个时刻，Alice 的邮件服务器和 Bob 的邮件服务器之间需要交换一批邮件，这两个邮件服务器之间需建立几条 TCP 连接？

   一条 TCP 连接。

3. 以下哪些应用层协议可能会被用来传输一个邮件报文：HTTP，FTP，SMTP，POP，DNS？

   HTTP，SMTP，POP

4. Alice 向 Bob 发送了一封邮件，Bob 阅读了这封邮件。这封邮件在 Alice 的用户代理、Bob 的用户代理、Alice 的邮件服务器、Bob 的邮件服务器中停留过。请按顺序列出这封邮件经过的地方，经过邮件服务器时需指出是进入发送队列还是进入信箱。

   邮件从 Alice 的用户代理到达 Alice 的邮件服务器，进入发送队列；然后到达 Bob 的邮件服务器，进入 Bob 的邮箱；最后到达 Bob 的用户代理。

5. 如果 TCP 服务器支持 n 个并发连接，每个连接来自不同的客户机主机，TCP 服务器将需要多少个套接字？这些套接字是怎么分配的？

   服务器需要（n+1）个套接字。一个套接字用于监听来自客户的连接请求；其余 n 个套接字，每个用于和一个客户进程进行通信。

6. 以下是 DNS 数据库的一些片段，请回答以下问题：

（1）abc.com 的邮件服务器的别名是：mail.abc.com
（2）abc.com 的权威域名服务器的 IP 地址是：202.68.69.1
（3）abc.com 的 web 服务器的规范名是：venus.abc.com
（4）abc.com 的 FTP 服务器的 IP 地址是：202.68.69.3
（5）邮箱 bob@mail.abc.com 所在主机的 IP 地址是：202.68.69.7

Name	type	value
abc.com.	NS	dns.abc.com
dns.abc.com.	A	202.68.69.1
abc.com.	MX	mail.abc.com
jupiter.abc.com.	A	202.68.69.3

mars.abc.com.	A	202.68.69.7
venus.abc.com.	A	202.68.69.11
mail.abc.com.	CNAME	mars.abc.com
www.abc.com.	CNAME	venus.abc.com
ftp.abc.com.	CNAME	jupiter.abc.com

学号：　　姓名：

1. 是非判断题：

1）假设主机 A 通过一条 TCP 连接向主机 B 发送一个大文件，如果某个报文段的序号为 m，则其后续报文段的序号必定是 m+1。（ × ）

2）假设主机 A 通过一条 TCP 连接向主机 B 发送一个序号为 38、包含 4 个数据字节的报文段，则主机 B 对该报文段的确认号必定是 42。（ × ）

3）假设主机 A 通过一条 TCP 连接向主机 B 发送一个大文件，主机 A 已发送但未被确认的字节数不会超过接收缓存的大小。（ √ ）

4）在 TCP 连接的持续过程中，TCP 头中的 rwnd 不会变化。（ × ）

2. 假设主机 A 通过一条 TCP 连接向主机 B 发送两个紧接着的 TCP 报文段。第一个报文段的序号为 80，第二个报文段的序号为 120。请问：

1）第一个报文段中有多少数据？　120 - 80 = 40 bytes

2）假设第一个报文段丢失，而第二个报文段到达主机 B。那么在主机 B 发往主机 A 的确认报文中，确认号应该是多少？　80

3. 发送方 TCP 的基序号 SendBase 和接收方缓存中的 LastByteRcvd 之间的关系为（ A ）

(A) LastByteRcvd ≧ SendBase-1　(B) LastByteRcvd ≧ SendBase　(C) 不能确定

4. 假设发送方 TCP 收到了确认序号 y（表示 y 之前的字节均已正确收到），则 y 与接收方缓存中的 LastByteRcvd 之间的关系为　（B）

(A) LastByteRcvd = y-1　(B) LastByteRcvd ≧ y-1　(C) 不能确定

5. 主机 A 向主机 B 发起一个 TCP 连接，假设主机 A 和主机 B 选择的起始序号分别为 70 和 90，将下表中三次握手交换的报文段的相关信息填充完整。

报文段	SYN flag	ACK flag	Seq number	Ack number
1	1	0	70	--
2	1	1	90	71
3	0	1	71	91

6. TCP 用于流量控制的窗口是 __接收窗口__，用于拥塞控制的窗口是__拥塞窗口__。

7. 假设主机 A 在一条 TCP 连接上发送了一大批数据，然后在 t_1 时刻变得空闲（因为没有更多的数据需要发送）。在相对较长的一段时间空闲后，在 t_2 时刻又有一大批数据需要发送。你认为此时主机 A 应当使用 t_1 时刻的 CongWin 和 Threshold，还是应当使用慢启动发送数据？为什么？

答：应使用慢启动发送数据。从题意来看，t_1 时刻的 CongWin 和 Threshold 可能较大。经过了相对较长的一段时间后，网络状态可能发生了变化，此时应使用慢启动逐渐提高发送速度，以免一下子发送大量数据引起网络拥塞。

1. 一个 B 类网络 128.16.0.0/16 被网络管理员划分为 16 个大小相同的子网，则子网掩码为 255.255.240.0 。如果按照 IP 地址从小到大对子网进行编号，写出第 2 个子网的地址范围，用 a.b.c.d/x 的形式表示 128.16.16.0/20 。

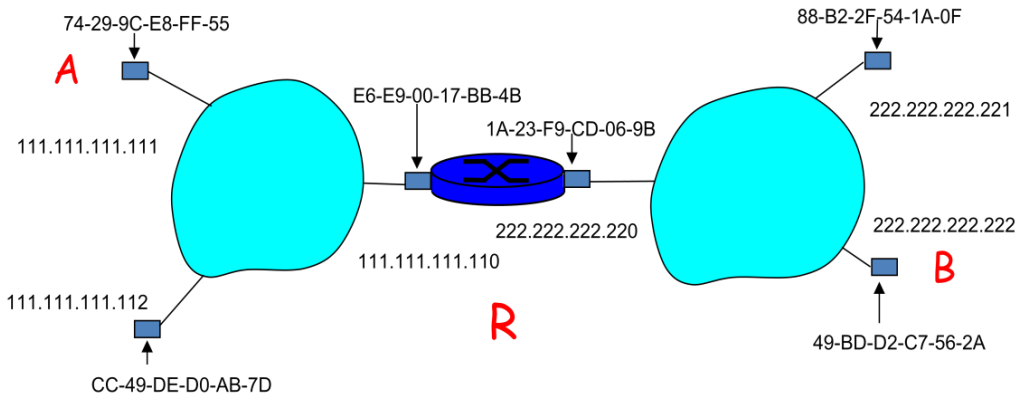
2. 一个路由器收到以下四条新的前缀：157.6.96.0/21、157.6.104.0/21、157.6.112.0/21 和 157.6.120.0/21，如果这些地址使用同一条输出线路，它们能被聚合吗？如果能，请给出聚合后的前缀；如果不能，请说明原因。

答：能，聚合后的前缀是 157.6.96.0/19

3. 若路由器中有以下三条前缀表项：200.24.0.0/21，200.24.8.0/22，200.24.16.0/20。路由器收到目的地址为 200.24.11.4 的数据包，请问应使用哪个表项转发数据包？

答：使用 200.24.8.0/22 表项转发包

4. 按以下格式给出主机 A 和路由器 R 中的转发表，假设图中两个网络的子网掩码均为 255.255.255.0，主机 A 的端口编号为 1，路由器 R 的端口从左至右编号为 1、2。



A 的转发表

目的前缀	下一跳	输出端口
111.111.111.0/24	—（写直接交付也可以）	1
default 或者 222.222.222.0/24	111.111.111.110	1

R 的转发表

目的前缀	下一跳	输出端口
111.111.111.0/24	—（写直接交付也可以）	1
222.222.222.0/24	—（写直接交付也可以）	2

1. 多址接入协议（multiple access protocol）划分为哪三种类型？其中，哪一种（或几种）是无冲突的协议？哪一种（或几种）是有冲突的协议？

答：

多址接入协议划分为信道划分、随机接入、轮流协议三种类型。

信道划分和轮流协议是无冲突的，随机接入是有冲突的。

2. 为什么 ARP 请求封装在一个广播帧中发送，而 ARP 响应封装在一个单播帧中发送？

答：

发送节点利用 ARP 请求查询目标主机的 MAC 地址，由于尚不知道目标主机的 MAC 地址，所以 ARP 请求封装在广播帧中发送。

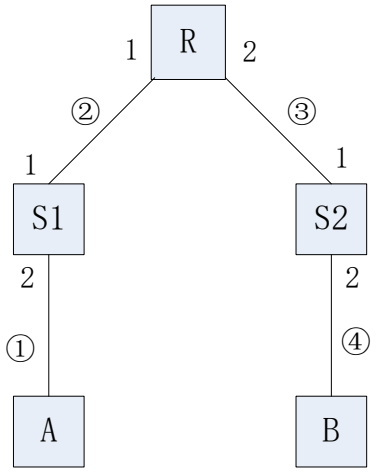
发送 ARP 响应的节点已经从 ARP 请求中获得了请求节点的 MAC 地址，所以 ARP 响应可以用单播帧发送。

3. 假设节点 A、B、C 连接到同一个广播局域网上，A 向 B 发送的单播帧（dest MAC = B），C 的适配器能收到吗？如果能收到，C 的适配器会处理这个帧吗？如果会处理，C 的适配器会把帧中的 IP 数据报交给自己的网络层吗？

答：

能收到；会处理；但不会将 IP 包交给自己的网络层。

4. 在如图所示的网络中，路由器 R 连接了两个链路层交换机 S1 和 S2。假设主机 A 向主机 B 发送了一个数据报（src IP = A，dest IP = B），请给出编号①～④的线路上传输的以太帧的源地址和目的地址，填入下表。MAC 地址用符号表示，比如 A 的 MAC 地址表示为 A，R 的端口 1 的 MAC 地址表示为 R-1，等等。



线路编号	Src MAC	Dest MAC
1	A	R-1
2	A	R-1
3	R-2	B
4	R-2	B

1. 在下面的空格中填入“谁的什么密钥”：

（1） A 向 B 发送一个一次性会话密钥，A 用 B 的公钥 加密该会话密钥。

（2） Certifier.com 用 自己的私钥 为 foo.com 签发公钥证书。

（3） A 向 B 发送一个签名的报文，A 用 自己的私钥 生成这个数字签名。

（4） A 向 B 发送一个可供鉴别的报文，A 用 与 B 共享的密钥 生成报文鉴别码。

2. 在下面的空格中填入可实现相应安全服务的安全机制：

机密性 数据加密　　完整性 报文鉴别

防抵赖 数字签名　　防假冒 端点鉴别

3. 在下面的空格中填入需要用到的算法或函数的序号：①对称密钥算法，②公开密钥算法，③密码散列函数。（报文鉴别码写出一种方法即可）

生成数字签名 ②③　　数据加密 ①

生成报文鉴别码 ③① 或 ③　　加密会话密钥 ②

4. 是非判断题：

1） 一对主机通过 IPSec 运行 TCP，封装重发的 TCP 包时，ESP 头中的序号不同。

对

2） 一对主机通过 IPSec 传输分组流，对每个发送的分组都要创建一个新的 SA。

错