

2018 年秋季学期计算机网络期末考试

Edited by Lyncien

2019.01.08

一、 选择题 10*4%

- 2018 年中国政府工作报告对过去 5 年工作回顾关于创新驱动发展成果，提到___**A**___广泛融入各行各业
A. 互联网 B. 移动支付 C. 电子商务 D. 共享经济
- 从网络分层体系结构来看，不属于网络层的功能是 **B**
A. 差错控制 B. 流量控制 C. 数据转发 D. 设备间通信
- 滑动窗口协议回退 N 步的接收方采用___**B**___方式确认收到的帧、
A. 逐个确认 B. 累计确认 C. 否定确认 D. 选择确认
- 差错检测加重传适用于 **A**
A. 出错概率高的情况
B. 出错概率低的情况
C. 无线信道
D. 单向信道
- 关于 Alhoa，错误的是 **C**
A. 可用于无线网络的信道分配
B. 可用于有线局域网
C. 适用于网络负载重的情况
D. 适用于网络负载轻的情况
- 以太网 MAC 协议的最小帧长的作用 **B**
A. 冲突检测 B. 冲突避让 C. 冲突增强 D. 安全传输
- IEEE802.11MAC 协议使用___**B**___控制帧通知隐藏终端互相避让
A. 信标(Beacon) B. RTS C. CTS D. ACK
- IPv4 首部分段偏移量的单位是___**D**___字节
A. 1 B. 2 C. 4 D. 8
- 关于 UDP 检验和，错误的是 **B**
A. 伪首部包含非零字段，故检验和不可能为 0
B. 无法提高 UDP 的可靠性
C. 接收方计算检验和有误时，丢弃报文，但报文中的部分参数出错可能引发 ICMP 向源节点报错
D. UDP 检验和的计算和 TCP 检验和的计算一样
- FTP 的控制连接使用的端口号是 **B (不考)** 21控制，20传数据
A. 20 B. 21 C. 25 D. 80

二、 简答题 5*4%

- 网络分层体系结构
- 分析面向连接服务的主要优点和缺点
- 分组交换原理
- 使用无分类地址的路由器为什么要用最长掩码匹配方式查找路由表
- 使用 NAT 技术的依据

1.应用层、传输层、网络层、链路层、物理层

2.面向连接的优点：可靠数据传输、流量控制、拥塞控制

缺点：建立连接和纠错纠错增加延时，无法按设定的速度发送数据因此不适用于流媒体等

3.分组交换原理：将要传送的数据分成一个个单位：分组将分组从一个路由器传到相邻路由器，一段段从源端传到目标端

4.最长前缀匹配方式的原因：在寻找子网时候是根据子网掩码来确定的，而子网掩码就是对应 IP 地址的前几位，这前面的几位为 IP 的网络部分

5. (不考)

□ **动机**：本地网络只有一个有效 IP 地址：

- 不需要从 ISP 分配一块地址，可用一个 IP 地址用于所有的（局域网）设备--省钱
- 可以在局域网改变设备的地址情况下而无须通知外界
- 可以改变 ISP（地址变化）而不需要改变内部的设备地址
- 局域网内部的设备没有明确的地址，对外是不可见的--安全

三、 综合题 40%

1. 使用最长匹配原则选择端口 6%

(1) 114.112.15.108

2

00001111 (第三个字节)

Prefix	Link interface
114.112.10.0/23	1
114.112.14.0/23	2
114.112.18.0/23	3
Otherwise	0

0000101

0000111

0001001

(2) 114.112.15.108

4

Prefix	Link interface
114.112.10.0/23	1
114.112.14.0/23	2
114.112.15.0/24	4
114.112.18.0/23	3
Otherwise	0

0000101

0000111

00001111

0001001

(3) 114.112.12.108

0

00001100

Prefix	Link interface
114.112.10.0/23	1
114.112.14.0/23	2
114.112.15.0/24	4
114.112.18.0/23	3
Otherwise	0

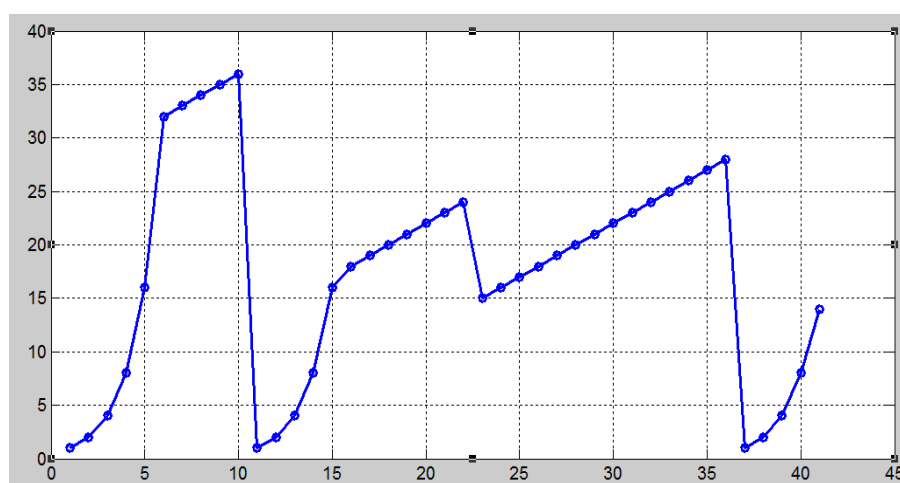
0000101

0000111

00001111

0001001

2. TCP 12%



(1) 是 TCP Reno 还是 TCP Tahoe, 为什么?

Reno, 因为Tahoe不管超时还是丢包都直接让cwnd回到1

(2) 初始的 ssthresh 是多少?

32

(3) Round10 发生了什么? Round11 的 cwnd 和 ssthresh 分别是多少?

超时, 1 16

(4) Round22 发生了什么? Round23 的 cwnd 和 ssthresh 分别是多少?

丢包, 15 12

(5) Round36 发生了什么? Round37 的 cwnd 和 ssthresh 分别是多少?

超时, 1 14

