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%
1.	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 $_{-}$ 广泛融入各行行业
	A. 互联网 B. 移动支付 C. 电子商务 D. 共享经济
2.	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
3.	滑动窗口协议回退 N 步的接收方采用 $_{\mathbf{B}}$ 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
4.	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
5.	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
6.	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
7.	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
8.	IPv4 首部分段偏移量的单位是D字节
	A. 1 B. 2 C. 4 D. 8
9.	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
10.	FTP 的控制连接使用的端口号是 B (不考) 21控制,20传数据
tota tota pro-	A. 20 B. 21 C. 25 D. 80
简答题 5*4%	5. (不考)
网络分层体系统	○不需要从TSP分配一块地址,可用一个TP地址用
	长务的主要优点和缺点 于所有的(局域网)设备省钱
分组交换原理	○可以在局域网改变设备的地址情况下而无须通知 外界

- 1.
 - 2.

 - 4. 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
 - 5. 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:建立连接和纠错校错增加延时,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

○可以改变**ISP**(地址变化)而不需要改变内部的

○局域网内部的设备没有明确的地址, 对外是不可

设备地址

见的--安全

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

三、 综合题 40%

1. 使用最长匹配原则选择端口 6%

(1) 114. 112. 15. 108

00001111 (第三个字节)

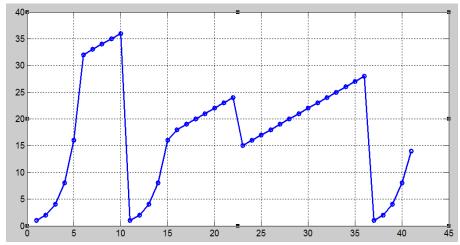
(1) 1111 1121 101 100				
Prefix	Link interface			
114. 112. 10. 0/23	1	0000101		
114. 112. 14. 0/23	2	0000111		
114. 112. 18. 0/23	3	0001001		
Otherwise	0			
(2) 114. 112. 15. 108	4			
Prefix	Link interface			
114. 112. 10. 0/23	1	0000101		
114. 112. 14. 0/23	2	0000111		
114. 112. 15. 0/24	4	00001111		
114. 112. 18. 0/23	3	0001001		
Otherwise	0			
(3) 114. 112. 12. 108	0 00001100			
Prefix	Link interface			
114. 112. 10. 0/23	1	0000101		
114. 112. 14. 0/23	2	0000111		

4

3

0

2. TCP 12%



- 是 TCP Reno 还是 TCP Tahoe,为什么? (1)
- Reno, 因为Tahoe不管超时还是丢包都直 接让cwnd回到1

00001111 0001001

初始的 ssthresh 是多少? 32 (2)

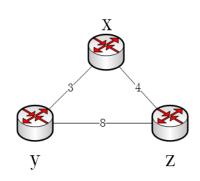
114. 112. 14. 0/23 114. 112. 15. 0/24

114. 112. 18. 0/23

Otherwise

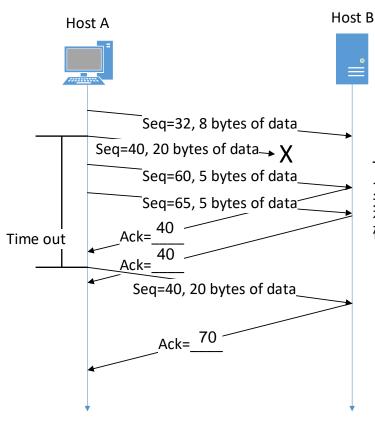
- Round10 发生了什么? Round11 的 cwnd 和 ssthresh 分别是多少? 超时,1 16 (3)
- Round22 发生了什么? Round23 的 cwnd 和 ssthresh 分别是多少? 丢包,15 12 (4)
- Round36 发生了什么? Round37 的 cwnd 和 ssthresh 分别是多少? 超时,1 14 (5)

3. 使用距离向量算法迭代计算每个路由器的向量表



	X	y	Z		X	y	Z		X	y	Z
X	0	3	4	X	0	3	4	X	0	3	4
у	∞	∞	ω	У	3	0	8	У	3	0	7
Z	ω	ω	ω	z	4	8	0	Z	4	7	0
	X	у	Z		X	у	Z		Х	у	Z
X	∞	ω	∞	×	0	3	4	X	0	3	4
у	3	0	8	У	3	0	7	У	3	0	7
z (∞	ω	ω	Z	4	8	0	Z	4	7	C
	x	у	Z		X	у	Z		Х	у	Z
X	∞	ω	∞	X	0	3	4	×	0	3	4
у	ω	ω	ω	У	3	0	8	У	3	0	7
z	4	8	0	Z	4	7	0	Z	4	7	(

4. A 与 B 进行 TCP 传输,填空 7%



8%

TCP传输的重传机制既不是SR 也不是GBN而是二者的混合体, 通常TCP会将乱序到达的分组缓 存下来(此处不考虑溢出), 确认方式为累计确认。

- 5. RSA 算法, p=3, q=11 7%
 - (1) 求 n, z
 - (2) 选择 e=3, d=7 可以吗? 原因。
 - (3) 用(e, n)加密 M=9,得到 C;用(d, n)解密 C,给出过程。
 - (1) n=3*11=33; z=(p-1)(q-1)=20
- (2)e和z无公因子,可以;ed-1=20,可以 原因见右图
 - (3) c=m^e mod n=9^3 mod 33=729 mod 33=3 m=c^d mod n=3^7 mod 33=2187 mod 33=9

RSA: 选择密钥

- 1. 选择2个很大的质数 *p, q.* (e.g., 1024 bits each)
- 2. 计算 n = pq, z = (p-1)(q-1)
- 3. 选择一个e (要求 e<n) 和z 没有一个公共因子,互素 ("relatively prime").
- 4. 选择 d 使得ed-1 正好能够被z整除. (也就是: ed mod z = 1).
- 5. 公钥(n,e). 私钥 (n,d)