# 2020-2021 学年第 1 学期期末考试试卷

一、单选题（20 分，每题 2 分）

1.（）是关于循环冗余码（CRC）正确的描述

A.CRC 可以用于向前纠错

B.CRC 的检错能力取决于生成多项式

C.依靠 CRC 就可以实现从发送方到接收方的正确传送

D.CRC 不能检测突发型错误

2.以太网中二进制指数后退（BEB）算法的主要功能是（）

A.竞争检测

B.竞争避让

C.阻塞信道

D.流量控制

3.（）是关于 IEEE 802.11 MAC 协议的错误描述

A.可以采用非竞争的方法分配信道

B.解决了隐藏站（终端）问题

C.解决了暴露站（终端）问题

D.不检测冲突

4.IPv4 首部中标识字段的作用是（）

A.序列号

B.区分服务

C.分片

D.网络标识

5.在 IPv4 和 IPv6 中，IP 地址的长度分别是（）

A.16 比特，48 比特

B.32 比特，48 比特

C.32 比特，64 比特

D.32 比特，128 比特

6.采用 NAT 技术解决 IPv4 地址不足的最主要依据是（）

A.网络通信是通过物理地址完成的，IP 地址对网络互连作用不大

B.NAT 路由器有全球 IP 地址

C.数据包转发时主要考虑将数据包转发到目的网络

D.本地网将主机的物理地址与内网 IP 地址作为全球 IP 地址

7.（）是关于无分类编址路由表最长前缀匹配的错误描述

A.可降低路由查找算法的时间复杂度

B.可能需要遍历整个路由表

C.前缀长的网络地址虽然在前缀短的网络地址空间中，但可能并不在前缀短的网络中

D.同一个 IP 地址中的网络地址可能不相同

8.ICMP 协议中（）在报告差错时不将数据包丢弃
A.重定向
B.源抑制
C.超时
D.目的地不可达

9.（）是网络安全的目标
A.可用性
B.完整性
C.机密性
D.以上均是

10.MD5 算法摘要长度是（）
A.64
B.128
C.256
D.512

二、简答题（40 分，每题 8 分）
1. 分析 RIP 协议存在的不足

2. 分析 OSPF 协议存在的不足

3. IEEE 802.3 与 802.11 MAC 协议解决冲突的区别?

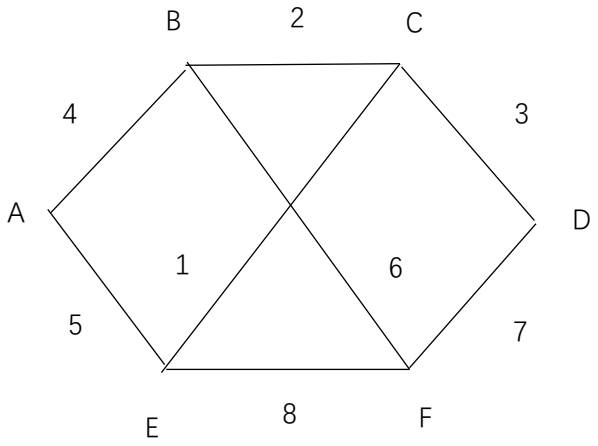
4. BGP 协议 AS 边界路由器交换信息主要内容

5. 数据报（例如 RIP）网络与虚电路（例如 MPLS）网络转发路由表的区别?

三、计算题（40 分，共 4 题）
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?

2. 生成多项式$G(x) = x^5 + x^4 + x^2 + 1$ (110101)，试计算帧 100110101101 的循环冗余码（CRC）。

3. 假定图中的节点为网络路由器，直线为相邻节点间的通信链路，直线上的数字为相邻节点间的通信距离，并且每个路由器至其它路由器的初始值均为∞，请使用若干表（每次的一个表对应路由器间交换的路由表）来说明每个路由器（基于距离向量算法）是如何获知至其它路由器的路由表。当距离相同时选用 IP 地址小的节点（假定 IP 地址顺序 A<B<C<D<E<F），例如当 A-B-C 与 A-E-C 距离相同时，选用 A-B-C。




4. 如果传送的明文信息为 m，散列函数为 H(·)，发送方鉴别用 RSA 私钥为（e,n)、公钥为（d,n)，对称加密算法、解密算法、密钥分别为 E(·)、D(·)、K。请给出发送方、接收方保证报文信息机密性和完整性的机制（或过程)。(机密性 4 分、完整性 6 分）

# 2020-2021 学年第 1 学期期末考试答案

一、单选题（20 分，每题 2 分）

1-5 BBCCD　　6-10 CAADB

二、简答题（40 分，每题 8 分）

1.（1）定期更新周期过于频繁（或过小或 30s）；（2）缺少分层，对大规模网络无法适用；（3）RIP1 存在收敛性问题（或坏消息传的慢）；（4）用跳数表示距离（或未使用实际代价表示距离）。4 个要点各 2 分。

2.（1）采用可靠（或带确认）洪泛（或广播）开销过大；（2）协议复杂（或多种链路状态、多种链路）。2 个要点各 4 分。

3.（1）802.3：冲突检测；（2）802.11：冲突避免。2 个要点各 4 分。

4.（1）可达性；（2）撤销路由（或不可达性）；（3）路径属性。第一个要点 4 分，其他两个要点各 2 分。

5.（1）顺序表，查找时间复杂度为 O(N)；（2）索引表或 Hash 表，查找时间复杂度为 O(1)。2 个要点各 4 分。

三、计算题（40 分，每题 10 分）

1.　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

各 2.5 分

2.11100

3.

第一次交换：3 分

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| A | - | (B,4) | ∞ | ∞ | (E,5) | ∞ |
| B | (A,4) | - | (C,2) | ∞ | ∞ | (F,6) |
| C | ∞ | (B,2) | - | (D,3) | (E,1) | ∞ |
| D | ∞ | ∞ | (C,3) | - | ∞ | (F,7) |
| E | (A,5) | ∞ | (C,1) | ∞ | - | (F,8) |
| F | ∞ | (B,6) | ∞ | (D,7) | (E,8) | - |

第二次交换：3 分

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| A | - | (B,4) | (B,6) | ∞ | (E,5) | (B,10) |
| B | (A,4) | - | (C,2) | (C,5) | (C,3) | (F,6) |

| | | | | | | |
|---|---|---|---|---|---|---|
| C | (B,6) | (B,2) | - | (D,3) | (E,1) | (B,8) |
| D | ∞ | (C,5) | (C,3) | - | (C,4) | (F,7) |
| E | (A,5) | (C,3) | (C,1) | (C,4) | - | (F,8) |
| F | (B,10) | (B,6) | (B,8) | (D,7) | (E,8) | - |

第三次交换：4 分

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| A | - | (B,4) | (B,6) | (B,9) | (E,5) | (B,10) |
| B | (A,4) | - | (C,2) | (C,5) | (C,3) | (F,6) |
| C | (B,6) | (B,2) | - | (D,3) | (E,1) | (B,8) |
| D | (C,9) | (C,5) | (C,3) | - | (C,4) | (F,7) |
| E | (A,5) | (C,3) | (C,1) | (C,4) | - | (F,8) |
| F | (B,10) | (B,6) | (B,8) | (D,7) | (E,8) | - |

4.（1）机密性：

发送方：

（2 分）加密：$p = E_K(m)$

接收方：

（2 分）解密：$m' = D_K(p)$

（2）完整性：

（2 分）发送方：$[H(m)]^e mod\ n$

（2 分）接收方：$[H(m')]^d mod\ n$ （m'为解密后的明文报文）

（2 分）比较上述两个结果是否一致。

说明：公式中的 H(m)代表 H(m)的数值。