中国海洋大学 2021 年硕士研究生招生考试试题

科目代码：940　　科目名称：计算机网络与安全

一、选择题（共 20 题，每题 2 分，共 40 分）

1. 在局域网中，MAC 指的是（　　）。

A. 逻辑链路控制子层　　B. 介质访问控制子层

C. 物理层　　D. 数据链路层

2. 在下列网络中，有哪些分组交换网络是通过建立虚电路进行通信？（　　）（多选题）

A. 帧中继　　B. X.25　　C. FDDI　　D. ATM

3. 在以太网中，如果网卡发现某个帧的目的地址不是自己的（　　）。

A. 它将该帧递交给网络层，由网络层决定如何处理

B. 它将丢弃该帧，并向网络层发送错误消息

C. 它将丢弃该帧，不向网络层提供错误消息

D. 它将向发送主机发送一个 NACK 帧

4. 下列关于 RIP 协议和 OSPF 协议的叙述中，错误的是（　　）。

A. RIP 协议和 OSPF 协议不都是网络层协议

B. 在进行路由信息交换时，RIP 协议中的路由器仅向自己相邻的路由器发送信息，OSPF 协议中的路由器向本自治系统中的所有路由器发送信息

C. 在进行路由信息交换时，OSPF 协议中的路由器发送的信息是整个路由表，RIP 协议中的路由器发送的信息只是路由表的一部分

D. RIP 协议中的路由器不知道全网的拓扑结构，OSPF 协议的任何一个路由器都知道自己所在区域的拓扑结构

5. 下列关于 Cookie 的说法中，错误的是（　　）。

A. Cookie 存储在服务器端　　B. Cookie 是服务器产生的

C. Cookie 会威胁客户的隐私　　D. Cookie 用于跟踪用户的访问和状态

6. 下列关于 PPP 和 HDLC 协议的叙述中，正确的是（　　）。

A. PPP 是网络层协议，而 HDLC 是数据链路层协议

B. PPP 支持半双工或全双工通信

C. PPP 两端的网络层必须运行相同的网络层协议

D. PPP 是面向字节的协议，而 HDLC 是面向比特的协议

7. 在 IP 首部的字段中，与分片和重组有关的字段是（　　）。（多选题）

A. 总长度　　B. 标识　　C. 标志　　D. 片偏移

8. 若某通信链路的数据传输速率为 2400b/s，采用 4 相位调制，则该链路的波特率是（　　）。

A. 600 波特　　B. 1200 波特　　C. 4800 波特　　D. 9600 波特

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

9. 关于链路状态协议的描述，正确的是（　　）。（多选题）

A.仅相邻路由器需要交换各自的路由表

B.全网路由器的拓扑数据库是一致的

C.采用洪泛技术更新链路变化信息

D.具有收敛速度慢的缺点

10. 下列说法错误的是（　　）。

A. Internet 上提供客户访问的主机一定要有域名

B.同一域名在不同时间可能解析出不同的 IP 地址

C.多个域名可以指向同一个主机 IP 地址

D. IP 子网中主机可以由不同的域名服务器来维护其映射

11. 下列关于中继器和集线器的说法中，正确的是（　　）。（多选题）

A.中继器在 OSI 参考模型的物理层，而集线器工作在数据链路层

B.二者都可以对信号进行放大和整形

C.通过中继器或集线器互连的网段数量不受限制

D.中继器通常只有 2 个端口，而集线器通常有 4 个或更多端口

12. 下列设备中，哪些不可以隔离 ARP 广播帧？（　　）。（多选题）

A. 路由器　　B. 网桥　　C. 以太网交换机　　D. 集线器

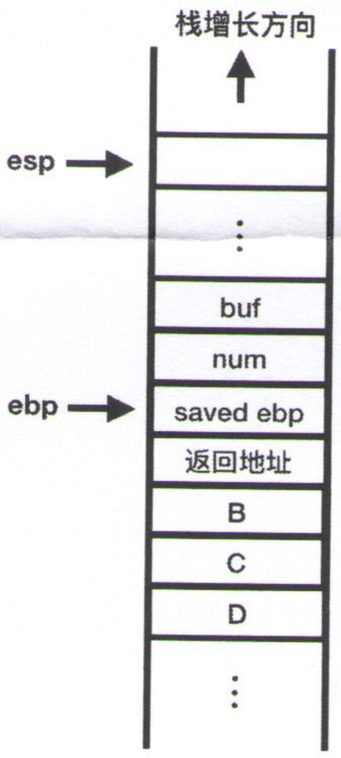
13. 下列协议组中需要使用传输层的 TCP 协议建立连接的是（　　）。

A. DNS、DHCP、FTP　　B. TELNET、SMTP、HTTP

C. RIP、FTP、TELNET　　D. SMTP、FTP、TFTP

14. 32 位 Linux 上某进程的当前调用栈如下图所示。由于程序对 buf 数组未设置边界检查，攻击者可以通过给 buf 数组输入超长字符串进行栈溢出攻击。如果攻击者通过溢出将“返回地址”修改为 int system(char *command)函数的地址，那么当 system 函数被调用时，参数 *command 所在的地址为栈中的（　　）。

A. saved ebp　　B. B　　C. C　　D. D



特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

15. 在 UNIX 中，如果某个文件的权限位设置为 rwxr-xr--，表示①可读、写、执行，②可读和执行，其他用户仅可以读。（　　）

A. ①root 用户，②文件属主　　B. ①特权用户，②普通用户

C. ①属主用户，②同组用户　　D. ①root 用户，②普通用户

16. 使用 IP 数据包进行的拒绝服务攻击可以进行源地址伪造，是因为 IP 协议是一种（　　）的协议。

A. 无连接、不可靠　　B. 面向连接、可靠

C. 无连接、可靠　　D. 面向连接、不可靠

17. BLP（Bell-Lapudula）模型的简单安全性（ss 特性）是指（　　）。

A. 不下写　　B. 不上读　　C. 不上写　　D. 不下读

18. PKI 中 CA（认证中心）的重要作用是解决了（　　）。

A. 用户不掌握产生公私钥的计算能力　　B. 用户缺乏验证签名的能力

C. 快速加密问题　　D. 信任问题

19. 进程被攻击者劫持，被损害的主要是（　　）。

A. 机密性　　B. 完整性　　C. 可用性　　D. 非否认性

20. 以下哪些特性是属于 MD5、SHA-1 等单向散列函数的特性（　　）。（多选题）

A. 输入不定长　　B. 算法保密　　C. 输出定长　　D. 可快速计算

二、填空题（共 30 空，每空 1 分，共 30 分）

1. 脉冲编码调制的过程简单的说可分为三个过程，分别是（　　）、量化和编码。
2. 实现 IP 地址到硬件地址转换的是（　　）协议，在 IP 层实现差错控制的是（　　）协议。
3. 以太网交换机进行转发决策时使用的 PDU 地址是（　　）。
4. 对二进制数据 11001100 10000001 00111000 进行 base64 编码后进行传送，则所传送的 ASCII 码是（　　）。
5. 某端口的 IP 地址为 172.16.7.131/26，则该 IP 地址所在网络的广播地址是（　　）。
6. RIP 协议使用（　　）协议进行传输；OSPF 协议使用（　　）协议进行传输；BGP 协议使用（　　）协议进行传输。
7. Windows 操作系统中 PING 或 tracert 命令所使用的网络层协议为（　　）。
8. 当用 n 个比特进行编号时，若接受窗口大小为 1，则发送窗口应满足（　　）时，连续 ARQ 协议才能正确运行。
9. 在子网 192.168.4.0/30 中，能接收目的地址为 192.168.4.3 的 IP 分组的最大主机数是（　　）。
10. FDDI 使用的是（　　）局域网技术。
11. 早期的 Napster 以及现在的迅雷、BT 等软件能够实现高速下载主要采用的是（　　）技

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

术。

12. 从 IPv4 向 IPv6 过渡的策略可以采用双协议栈和（　　）。
13. 当使用鼠标点击一个万维网文档时，若该文档除了有文本外，还包含 3 个 jpg 图像，在 HTTP/1.0 中需要（　　）次 UDP 请求和（　　）次 TCP 连接。
14. C 语言代码“int sockfd = socket(AF_INET,SOCK_STREAM, 0);”的含义是（　　）。
15. 如果带宽为 4kHz，信噪比为 30dB，则该信道的极限信息传输速率为（　　）。
16. 若码元为 1，则其前半个码元的电平与上一个码元的后半个码元的电平一致；若码元为 0，则其前半个码元的电平与上一个码元的后半个码元的电平相反，这称之为（　　）编码。
17. 入侵检测系统的基率谬误是指：很难同时满足具有高检测率和低（　　）的标准。
18. Linux 中如果具有 root 权限的程序读写的某个临时文件的名字是固定的，那么攻击者可能会使用（　　）连接来利用该程序覆盖重要的系统文件。
19. TLS 协议中的两个重要概念是 TLS 会话和 TLS（　　）。
20. 区块链技术是我国重点推动的分布式账本技术，它由一组技术组成，其中以工作量证明（PoW）为代表的（　　）算法用来达成分布式账本的一致性。
21. 基本安全原则中的（　　）原则是指访问控制应当基于许可而不是排除；（　　）原则是指每个进程和系统用户都应当使用完成某项任务必需而非额外的特权集进行操作。
22. 分组密码一次处理一个元素分组，而（　　）密码则持续地处理输入元素。
23. 访问控制的基本元素是主体、客体和访问权。但主体一般不能直接访问客体，而是通过（　　）进行代理。客体可能是设备、文件等，是一个可以包含或者接收（　　）的实体。
24. 在数据库安全中，攻击者通过大量可访问的数据项的组合来分析出某个保密的数据项，叫做（　　）攻击。

三、问答与计算题（共 12 题，共 80 分）

1. （6分）说明为什么在无线局域网中不能使用CSMA/CD 协议而必须使用CSMA/CA 协议？结合暴露站和隐蔽站问题，说明 RTS 帧和 CTS 帧的作用。
2. （6 分）试分别解释 NAT、IP 组播、SDN。
3. （6 分）A、B 两站位于长 2km 的基带总线局域网的两端，C 站位于 A、B 站之间，数据传输速率为 10Mbps，信号传播速度为 200m/μs，B 站接收完毕 A 站发来的一帧数据所需的时间是 80 μs。

   （1）求数据帧的长度；

   （2）若 A、C 两站同时向对方发送一帧数据，4 μs 后两站发现冲突，求 A、C 两站的距离。
4. （6 分）HTTP 协议的特点是什么？HTTP1.1 协议比 HTTP1.0 协议有哪些主要变化？说明 HTTP 请求首部 User-Agent 和响应首部字段 Location 分别代表什么含义。

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

5. （6 分）试说明从客户机到服务器的 TCP 连接释放的过程。

6. （8 分）某路由器具有下表所示的路由表项：

网络前缀	下一跳
131.128.56.0/24	A
131.128.55.32/28	B
131.128.55.32/30	C
131.128.0.0/16	D

（1）假设路由器收到两个分组：分组 A 的目的地址是 131.128.55.33，分组 B 的目的地址是 131.128.55.38。请确定路由器为这两个分组选择的下一跳，并解释说明。

（2）在以上路由表中增加一条表项，该路由表项使以 131.128.55.33 为目的地址的 IP 分组选择 A 作为下一跳，而不影响其他目的地址的 IP 分组转发。

（3）在以上路由表中增加一条表项，使所有目的地址与该路由表中任何路由表项都不匹配的 IP 分组被转发到下一跳 E。

（4）将 131.128.56.0/24 划分为 4 个规模尽可能大的等长子网，给出子网掩码及每个子网的可分配地址范围。

7. （8 分）使用连续 ARQ 协议，发送窗口的大小为 3，帧序号的范围是[0, 15]，传输媒体保证在接收方能够按序收到分组。在某个时刻，接收方下一个期望收到的序号是 5。试问：

（1）在发送方的发送窗口中可能出现的序号组合有哪几种？

（2）接收方已经发送出去的，但在网络中（即还未到达发送方）的确认分组可能有哪些？说明这些确认分组是用来确认哪些序号的分组。

8. （6 分）以下是一段病毒指令和该病毒指令变形后的版本，该变形要达到什么目的？变形指令中哪些行指令是无用指令？如果在 C 代码中进行类似的变形效果反而不好，为什么？

病毒指令：

```
1  MOV AX, 3
2  MOV BX, 6
3  ADD AX, BX
```

病毒指令变形版本：

```
1  PUSH AX
2  POP AX
3  MOV AX, 3
4  MOV BX, 6
5  SWAP AX, BX
6  SWAP AX, BX
7  ADD AX, BX
8  NOP
```


特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。

9. （6 分）什么是主动攻击？什么是被动攻击？举出每种攻击各两个具体的攻击方式。为什么说理想的量子密码通信不存在被动攻击？

10. （6 分）防火墙设计的三个目标是什么？

11. （8 分）以下代码段存在什么安全漏洞？这一漏洞是由哪一行代码直接导致的？是如何导致的？如何避免？

```
typedef struct chunk {
    char inp[64];
    void (*process)(char *);
} chunk_t;
void showlen(char *buf) {
    int len;
    len = strlen(buf);
    printf("buffer5 read %d chars\n", len);
}
int main(int argc, char *argv[]) {
    chunk_t *next;
    setbuf(stdin, NULL);
    next = malloc(sizeof(chunk_t));
    next->process = showlen;
    printf("Enter value: ");
    gets(next->inp);
    next->process(next->inp);
    printf("buffer5 done\n");
}
```

12. （8 分）简述什么是 DAC（自主访问控制）、MAC（强制访问控制），请说明二者最主要的区别。RBAC（基于角色的访问控制）如何与 DAC 和 MAC 联系起来？

特别提醒：答案必须写在答题纸上，若写在试卷或草稿纸上无效。