1. 一个子网IP地址为10.115.0.0，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？(15分)

答：网络地址：10.96.0.0

广播地址：10.127.255.255

最小用户地址：10.96.0.1

最大用户地址：10.127.255.254

2.假定路由器R的路由表如下。当目的地址为201.4.20.126的分组到达R时，R将使用哪个接口转发该分组？(10分)

|  |  |  |  |
| --- | --- | --- | --- |
| 掩码 | 网络地址 | 下一跳 | 接口 |
| /26 | 180.70.65.192 | - | s2 |
| /22 | 201.4.20.0 | - | s0 |
| /24 | 201.4.22.0 | - | s3 |
| /25 | 201.4.20.0 | - | s1 |

答：s1

3. 已知路由器R1有表3-1所示的路由表，现收到相邻路由器R2发来的路由更新信息，如表3-2所示。试根据RIP协议更新路由器R1的路由表。(15分)

表3-1 路由器R1的路由表

|  |  |  |
| --- | --- | --- |
| 目的网络 | 距离 | 下一跳 |
| Net2 | 3 | R2 |
| Net3 | 4 | R3 |
| Net5 | 5 | R4 |

表3-2 R2发给R1的更新

|  |  |  |
| --- | --- | --- |
| 目的网络 | 距离 | 下一跳 |
| Net1 | 1 | - |
| Net2 | 10 | R5 |
| Net3 | 2 | R6 |

答：路由器R1的路由表

|  |  |  |
| --- | --- | --- |
| 目的网络 | 距离 | 下一跳 |
| Net1 | 2 | R2 |
| Net2 | 11 | R2 |
| Net3 | 3 | R2 |
| Net5 | 5 | R4 |

4. 一个IPv4分组的分片中，MF(或M)位是0，HLEN是10，总长度是200，分片偏移值是300。试求该分片第一个字节和最后一个字节在原分组中的位置。(10分)

答：第一字节的位置是2400(800\*3)，最后一个字节的位置为2559(2400+200-**10\*4-**1)。

5. 基于目的地址转发“下一跳方法”的优缺点。(15分)

答：

优点：每个路由表项只需保留“下一跳”的地址，无需给出完整的路由(路径)。

缺点：要求“下一跳”路由器知道剩余的路径信息或网络中的所有路由器信息保持一致。

6. RIP、OSPF协议的缺点。(15分)

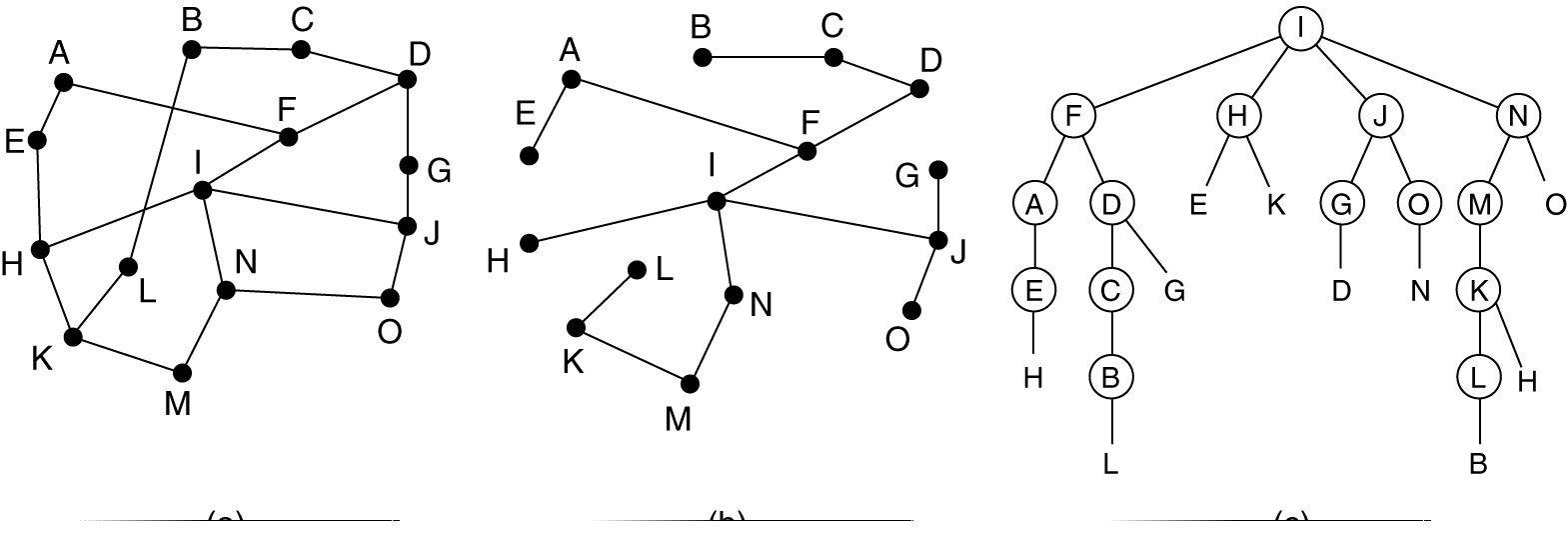
答：RIP缺点:(1)更新周期(30s)过短;(2)未进行区域划分

OSPF缺点：用可靠广播方式在整个区域广播所有节点的链路状态，开销过大

7. 对于下图中的子网，若采用下列方法，从K开始广播需要产生多少个分组？

1. 反向路径转发(Reverse path forwarding)?
2. 汇集树(sink tree)?

(注意：必须画出相应的两棵树.)



答：(1)24;(2)14(重点是画对图)

1. 对于**无控制洪泛、受控洪泛和生成树广播**三种广播选路方式，下列说法是否正确：a) 一个节点可能**收到同一个广播**分组的多个拷贝；b) 一个节点可能在相同的出链路上**多次转发同一个广播分组**

答：无控制洪泛：a)对，b)对。 受控洪泛：a)对，b)错。 生成树广播：a)错，b)错。

2. 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 。

3. 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

4. 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

5. 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。

1. 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。

1. 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。

1. 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”：
2. A向B发送一个一次性会话密钥，A用 加密该会话密钥。
3. Certifier.com用 为foo.com签发公钥证书。
4. A向B发送一个签名的报文，A用 生成这个数字签名。
5. A向B发送一个可供鉴别的报文，A用 生成报文鉴别码（写出一种方法即可）。
6. 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 完整性

防抵赖 防假冒

1. 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散列函数，④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 数据加密

生成报文鉴别码 加密会话密钥

1. 是非判断题：
2. 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。
3. 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。

1. 若一无限用户slotted ALOHA信道处于负载不足与过载的临界点，则

(1)信道中空闲时槽的比例是多少？

(2)成功发送一个帧发送次数是多少?(选做，对了加20分)

答：(1)p0=e-G，G=1≡p0(空闲比例)=36.8%

(2)G/S=1/0.368≈2.72(注：S=Ge-G)

2. IEEE 802.3 MAC协议的全称？它是如何解决冲突的？(15分，第1问5分，第2问10分)

答：(1)1-坚持CSMA/CD；

(2)发前侦听，边发边听，冲突避让

3. 若某站点经历了10次连续冲突，则该次冲突导致站点在IEEE 802.3、802.3u网络中站点的平均等待时间分别为多少？（15分，第1问7.5分，第2问7.5分）

答：(1)1024/2=512;802.3:512\*51.2μs;

(2)802.3u:512\*5.12μs

4. IEEE 802.11协议哪个(或几个)控制帧发现隐藏终端与暴露终端的？(15分, 第1问7.5分，第2问7.5分)

答：(1) 隐藏终端：CTS；

(2)暴露终端：RTS

5. IEEE 802.3 MAC协议中最小帧长的功能与计算依据？(20分)

答：

最小帧长的功能：检测冲突。

计算依据：传输速率\*相距最远的两个站点间传播时延

6.假定生成多项式，试计算帧100110101100 的循环冗余码(CRC)。(15分)

答：001101

7.数字签名是一种可提供发送方身份鉴别、报文完整性和防发送方抵赖的安全机制。(20分)

（1）请给出数字签名最常见的构造方法。

（2）根据数字签名的构造方法，说明数字签名为什么可以提供以上安全服务。

答：

(1) 当实体A需要为报文M生成数字签名时，A首先用一个散列函数计算M的报文摘要，然后用A的私钥加密该报文摘要，生成数字签名。

(2) A的私钥是只有A知道的秘密，任何其它实体无法得到，因而一个有效的数字签名可提供发送方身份鉴别。报文摘要可用于检测报文的完整性，对报文内容的任何修改将产生不同的报文摘要。用A的私钥加密后的报文摘要是不可伪造的，从而数字签名就将A与报文M紧密关联在一起，既能提供报文完整性服务，也能防止发送方抵赖。