2019 年上半年网络工程师上午真题+答案

详细解析完整版

第 1 题：计算机执行指令的过程中，需要由（ ）产生每条指令的操作信号并将信号送往相应的部件进行处理，以完成指定的操作。

A.CPU 的控制器

B.CPU 的运算器

C.DMA 控制器

D.Cache 控制器

参考答案：A

解析：

控制器（Control Unit）：是中央处理器的核心，主要功能就是统一指挥并控制计算机各部件协调工作，所依据的是机器指令。其实就是向计算机其他部件发送控制指令。控制器的组成包含程序计数器（PC）、指令寄存器（IR）、指令译码器、时序部件、微操作控制信号形成部件（PSW）和中断机构。

第 2 题：DMA 控制方式是在（ ）之间直接建立数据通路进行数据的交换处理。

A.CPU 与主存

B.CPU 与外设

C.主存与外设

D.外设与外设

参考答案：C

解析：

DMA 存取方式，是一种完全由硬件执行 I/O 数据交换的工作方式。它既考虑到

中断的响应，同时又要节约中断开销。此时，DMA 控制器代替 CPU 完全接管对总线的控制，数据交换不经过 CPU，直接在内存和外围设备之间成批进行。

第 3 题：在（　）校验方法中，采用模 2 运算来构造校验位。

A.水平奇偶

B.垂直奇偶

C.海明码

D.循环冗余

参考答案：D

解析：

模 2 运算是一种二进制算法，属于 CRC 校验技术中的核心部分，具体用的模二除算法。垂直奇偶校验又称为纵向奇偶校验，它是将要发送的整个信息块分为定长 p 位的若干段(比如说 q 段)，每段后面按"1"的个数为奇数或偶数的规律加上一位奇偶位。

水平奇偶校验又称为横向奇偶校验，它是对各个信息段的相应位横向进行编码，产生一个奇偶校验冗余位。奇偶校验用的是模二加运算法则。

第 4 题：以下关于 RISC（精简指令系统计算机）技术的叙述中，错误的是（　）。

A.指令长度固定、指令种类尽量少

B.指令功能强大、寻址方式复杂多样

C.增加寄存器数目以减少访存次数

D.用硬布线电路实现指令解码，快速完成指令译码

参考答案：B

解析：

RISC 鼓励尽可能使用较少的寻址方式，这样可以简化实现逻辑、提高效率。相反地，CISC 则提倡通过丰富的寻址方式来为用户编程提供更大的灵活性。

第 5 题：甲公司购买了一个工具软件，并使用该工具软件开发了新的名为“恒友”的软件，甲公司在销售新软件的同时，向客户提供工具软件的复制品，则该行为（　）。甲公司未对“恒友”软件注册商标就开始推向市场，并获得用户的好评。三个月后，乙公司也推出名为“恒友”的类似软件，并对之进行了商标注册，则其行为（　）。

A.侵犯了著作权

B.不构成侵权行为

C.侵犯了专利权

D.属于不正当竞争

参考答案：A

解析：

提供工具软件的复制品，属于侵犯著作权。类似软件产品和注册商标，不构成侵权。

第 6 题：甲公司购买了一个工具软件，并使用该工具软件开发了新的名为“恒友”的软件，甲公司在销售新软件的同时，向客户提供工具软件的复制品，则该行为（　）。甲公司未对“恒友”软件注册商标就开始推向市场，并获得用户的好评。三个月后，乙公司也推出名为“恒友”的类似软件，并对之进行了商标注册，则其行为（　）。

A.侵犯了著作权

B.不构成侵权行为

C.侵犯了商标权

D.属于不正当竞争

参考答案：B

解析：

提供工具软件的复制品，属于侵犯著作权。类似软件产品和注册商标，不构成侵权。

第 7 题：10 个成员组成的开发小组，若任意两人之间都有沟通路径，则一共有（ ）条沟通路径。

A.100

B.90

C.50

D.45

参考答案：D

解析：

N(N−1)/2 个路径。类似于广播型的 OSPF 邻居关系。

第 8 题：某文件系统采用位示图（bitmap）记录磁盘的使用情况。若计算机系统的字长为 64 位，磁盘的容量为 1024GB，物理块的大小为 4MB，那么位示图的大小需要（ ）个字。

A.1200

B.2400

C.4096

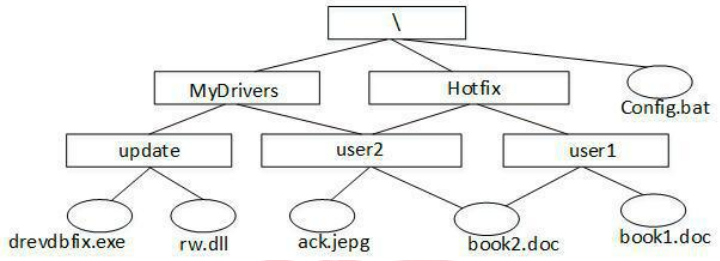
D.9600

参考答案：C

解析：

位示图是利用二进制的一位来表示磁盘中的一个盘块的使用情况。当其值为“0”时，表示对应的盘块空闲；为“1”时，表示已经分配。系统中字长为 64 位，可记录 64 个物理块的使用情况，根据题意，若磁盘的容量为 1024GB，物理块的大小为 4MB，那么该磁盘就有 256×1024 个物理块，位示图的大小为 256×1024/64=4096 个字节。

第 9 题：若某文件系统的目录结构如下图所示，假设用户要访问文件 book2.doc 且当前工作目录为 MyDrivers，则该文件的绝对路径和相对路径分别为（　）。



A.MyDriversuser2 和 user2\

B.MyDriversuser2 和 user2\

C.MyDriversuser2 和 user2\

D.MyDriversuser2 和 user2\

参考答案：C

解析：

路径又分相对路径和绝对路径。绝对路径是指从根目录开始的路径，也称为完全路径；相对路径是指从用户工作目录开始的路径。应该注意到，在树型目录结构中到某一确定文件的绝对路径和相对路径均只有一条。绝对路径是确定不变的，

而相对路径则随着用户工作目录的变化而不断变化。

第 10 题：设信号的波特率为 1000Baud，信道支持的最大数据速率为 2000b/s，则信道采用的调制技术为（　）。

A.BPSK

B.QPSK

C.BFSK

D.4B5B

参考答案：B

解析：

比特率和波特率的具体的换算公式为：R=Blog2N。

根据题目，现在 R=2B，说明 N=4，QPSK（正交相移键控或四相相移键控）：四相相移调制是利用载波的四种不同相位差来表示输入的数字信息，规定了四种载波相位，分别为 45°，135°，225°，315°。QPSK 中每次调制可传输 2 个信息比特。在选项中只有 QPSK 的码元种类数是 4。

第 11 题：假设模拟信号的频率为 10～16MHz，采样频率必须大于（　）时，才能使得到的样本信号不失真。

A.8MHz

B.10MHz

C.20MHz

D.32MHz

参考答案：D

解析：

奈奎斯特取样定理：如果取样速率大于模拟信号最高频率的 2 倍，则可以用得到的样本中恢复原来的模拟信号。

第 12 题：下列千兆以太网标准中，传输距离最短的是（　）。

A.1000BASE-FX

B.1000BASE-CX

C.1000BASE-SX

D.1000BASE-LX

参考答案：B

解析：

（1）1000 Base-T 标准使用的是 5 类非屏蔽双绞线，双绞线长度可以达到 100m。（2）1000Base-X 是基于光纤通道的物理层，使用的媒体有三种：

1000 Base-CX 标准使用的是屏蔽双绞线，双绞线长度可以达到 25m； 1000 Base-LX 标准使用的是波长为 1300nm 的单模光纤，光纤长度可以达到 3000m；

1000 Base-SX 标准使用的是波长为 850nm 的多模光纤，光纤长度可以达到 300～550m。

其中前三项标准是 IEEE 802.3z，而 1000 Base-T 的标准是 IEEE 802.3ab。

100BASE-FX：运行在光纤上的快速以太网，光纤类型可以是单模或多模。

第 13 题：以下关于直通式交换机和存储转发式交换机的叙述中，正确的是（　）。

A.存储转发式交换机采用软件实现交换

B.直通式交换机存在坏帧传播的风险

C.存储转发式交换机无需进行 CRC 校验

D.直通式交换机比存储转发式交换机交换速度慢

参考答案：B

解析：

根据交换机的帧转发方式，交换机可以分为 3 类：

（1）直接交换方式（cut-through switching）；交换机只接收帧并检测目的地址，就立即将该帧转发出去，而不用判断这帧数据是否出错。帧出错检测任务由节点完成。这种交换方式的优点就是交换延迟低；缺点就是缺乏差错检测能力，不支持不同速率端口之间的帧转发。

（2）存储转发交换方式（Store-and-Forward switching）；交换机需要完成接收帧并进行差错检测。如果接收帧正确，则根据目的地址确定输出端口，然后再转发出去。这种交换方式的优点是具有差错检测能力，并支持不同速率端口间的帧转发；缺点就是交换延迟会增长。

（3）改进直接交换方式（segment-free switching，无碎片转发方式）。改进的直接交换方式就是上述两种方式的结合。在接收到帧的前 64B 后，判断帧头字段是否正确，如果正确则转发出去。长度小于 64 字节。冲突碎片并不是有效的数据帧，应该被丢弃。这种方式对于短的帧来说，交换延迟与直接交换方式比较接近；对于长的帧来说，由于它只对帧的地址字段与控制字段进行差错检测，因此交换延迟将会减少。

第 14 题：下列指标中，仅用于双绞线测试的是（　）。

A.最大衰减限值

B.波长窗口参数

C.回波损耗限值

D.近端串扰

参考答案：D

解析：

近端串音是指在双绞线内部中一对线中的一条线与另一条线之间的因信号耦合效应而产生的串音。

第 15 题：采用 HDLC%2C >HDLC 协议进行数据传输，帧 0−7 循环编号，当发送站发送了编号为 0、1、2、3、4 的 5 帧时，收到了对方应答帧 REJ3，此时发送站应发送的后续 3 帧为（　），

若收到的对方应答帧为 SREJ3，则发送站应发送的后续 3 帧为（　）。

A.2、3、4

B.3、4、5

C.3、5、6

D.5、6、7

参考答案：B

解析：

HDLC 的监控帧用于差错控制和流量控制，通常简称 S 帧。00——接收就绪（RR），由主站或从站发送。主站可以使用 RR 型 S 帧来轮询从站，即希望从站传输编号为 N（R）的 I 帧，若存在这样的帧，便进行传输；从站也可用 RR 型 S 帧来作响应，表示从站希望从主站那里接收的下一个 I 帧的编号是 N（R）。01——拒绝（REJ），由主站或从站发送，用以要求发送方对从编号为 N（R）开始的帧及其以后所有的帧进行重发，这也暗示 N（R）以前的 I 帧已被正确接

收。10——接收未就绪（RNR），表示编号小于 N（R）的 I 帧已被收到，但当前正处于忙状态，尚未准备好接收编号为 N（R）的 I 帧，这可用来对链路流量进行控制。11——选择拒绝（SREJ），它要求发送方发送编号为 N（R）单个 I 帧，并暗示其它编号的 I 帧已全部确认。

第 16 题：采用 HDLC 协议进行数据传输，帧 0-7 循环编号，当发送站发送了编号为 0、1、2、3、4 的 5 帧时，收到了对方应答帧 REJ3，此时发送站应发送的后续 3 帧为（　），若收到的对方应答帧为 SREJ3，则发送站应发送的后续 3 帧为（　）。

A.2、3、4

B.3、4、5

C.3、5、6

D.5、6、7

参考答案：C

解析：

HDLC 的监控帧用于差错控制和流量控制，通常简称 S 帧。00——接收就绪（RR），由主站或从站发送。主站可以使用 RR 型 S 帧来轮询从站，即希望从站传输编号为 N（R）的 I 帧，若存在这样的帧，便进行传输；从站也可用 RR 型 S 帧来作响应，表示从站希望从主站那里接收的下一个 I 帧的编号是 N（R）。01——拒绝（REJ），由主站或从站发送，用以要求发送方对从编号为 N（R）开始的帧及其以后所有的帧进行重发，这也暗示 N（R）以前的 I 帧已被正确接收。10——接收未就绪（RNR），表示编号小于 N（R）的 I 帧已被收到，但当前正处于忙状态，尚未准备好接收编号为 N（R）的 I 帧，这可用来对链路流量

进行控制。

11——选择拒绝（SREJ），它要求发送方发送编号为 N（R）单个 I 帧，并暗示其它编号的 I 帧已全部确认。

第 17 题：E1 载波的控制开销占（　），E1 基本帧的传送时间为（　）。

A.0.518%

B.6.25%

C.1.25%

D.25%

参考答案：B

解析：

E1 载波的控制开销占 2/32*100%=6.25%。

第 18 题：E1 载波的控制开销占（　），E1 基本帧的传送时间为（　）。

A.100ms

B.200μs

C.125μs

D.150μs

参考答案：C

解析：

E1 载波的基本帧传送时间是 125us。

第 19 题：TCP 和 UDP 协议均提供了（　）能力。

A.连接管理

B.差错校验和重传

C.流量控制

D.端口寻址

参考答案：D

解析：

UDP 是一种简单的面向数据报的传输协议，实现的是不可靠、无连接的数据报服务，通常用于不要求可靠传输的场合，可以提高传输效率，减少额外开销。使用 UDP 传输时，应用进程的每次输出均生成一个 UDP 数据报，并将其封装在一个 IP 数据报中发送。

UDP 没有拥塞控制，所以网络出现的拥塞不会让源主机的发送速率降低。这对于某些实时应用是很重要的。很多实时的应用，例如 IP 电话、实时视频会议）要求源主机以恒定的速率发送数据，并且允许在网络拥塞情况下丢失一些数据，但却不允许数据有太大的时延，UDP 正好适合这种要求。

TCP 的特点：

（1）面向连接的传输层协议。

（2）每一条 TCP 连接只能有两个端点：只能是点对点。

（3）TCP 提供可靠交付的服务：通过 TCP 连接传送的数据无差错、不丢失、不重复、并且按顺序到达。

（4）TCP 提供全双工通信：TCP 允许通信双方的应用进程在任何时刻都能发送数据。在 TCP 连接的两端都有发送缓存和接收缓存，用来临时存放通信的数据。

（5）面向字节流：TCP 把应用进程交下来的数据看成是一连串无结构的字节流。TCP 并不关心应用进程一次把多长的报文发送到 TCP 的缓存中，而是根

据对端给出的窗口值和当前网络拥塞的程度来决定一个报文段应包含多少个字节。

第 20 题：建立 TCP 连接时，一端主动打开后所处的状态为（　）。

A.SYN SENT

B.ESTABLISHED

C.CLOSE-WAIT

D.LAST-ACK

参考答案：A

解析：

LISTEN：服务器等待连接过来的状态。SYN_SENT：客户端发起连接（主动打开），变成此状态，如果 SYN 超时，或者服务器不存在直接 CLOSED。SYN_RCVD：服务器收到 SYN 包的时候，就变成此状态。ESTABLISHED：完成三次握手，进入连接建立状态，说明此时可以进行数据传输了。

第 21 题：ARP 的协议数据单元封装在（　）中传送；ICMP 的协议数据单元封装在（　）中传送，RIP 路由协议数据单元封装在（　）中传送。

A.以太帧

B.IP 数据报

C.TCP 段

D.UDP 段

参考答案：A

解析：

ARP 协议数据单元被封装在以太帧中传输，ICMP 协议作为 IP 数据报中的数

据，封装在 IP 数据包中发送。RIP 协议属于应用层协议，被封装在 UDP 报文中传输。

第 22 题：ARP 的协议数据单元封装在（ ）中传送；ICMP 的协议数据单元封装在（ ）中传送，RIP 路由协议数据单元封装在（ ）中传送。

A.以太帧

B.IP 数据报

C.TCP 段

D.UDP 段

参考答案：B

解析：

ARP 协议数据单元被封装在以太帧中传输，ICMP 协议作为 IP 数据报中的数据，封装在 IP 数据包中发送。RIP 协议属于应用层协议，被封装在 UDP 报文中传输。

第 23 题：ARP 的协议数据单元封装在（ ）中传送；ICMP 的协议数据单元封装在（ ）中传送，RIP 路由协议数据单元封装在（ ）中传送。

A.以太帧

B.IP 数据报

C.TCP 段

D.UDP 段

参考答案：D

解析：

ARP 协议数据单元被封装在以太帧中传输，ICMP 协议作为 IP 数据报中的数

据，封装在 IP 数据包中发送。RIP 协议属于应用层协议，被封装在 UDP 报文中传输。

第 24 题：在点对点网络上，运行 OSPF 协议的路由器每（ ）秒钟向它的各个接口发送 Hello 分组，告知邻居它的存在。

A.10

B.20

C.30

D.40

参考答案：A

解析：

OSPF 路由器周期性（默认 10 秒）的从其启动 OSPF 协议的每一个接口以组播地址 224.0.0.5 发送 HELLO 包，以寻找邻居。

第 25 题：下列路由协议中，用于 AS 之间路由选择的是（ ）。

A.RIP

B.OSPF

C.IS-IS

D.BGP

参考答案：D

解析：

在一个 AS 内部传递更新的 IGP 路由协议有 RIP，EIGRP，OSPF，IS-IS，可以在 AS 之间传递更新的路由协议目前只有 BGP。

第 26 题：下图 1 所示内容是在图 2 中的（ ）设备上执行（ ）命令查看到的信

息片段。该信息片段中参数（ ）的值反映邻居状态是否正常。

A.R1

B.R2

C.R3

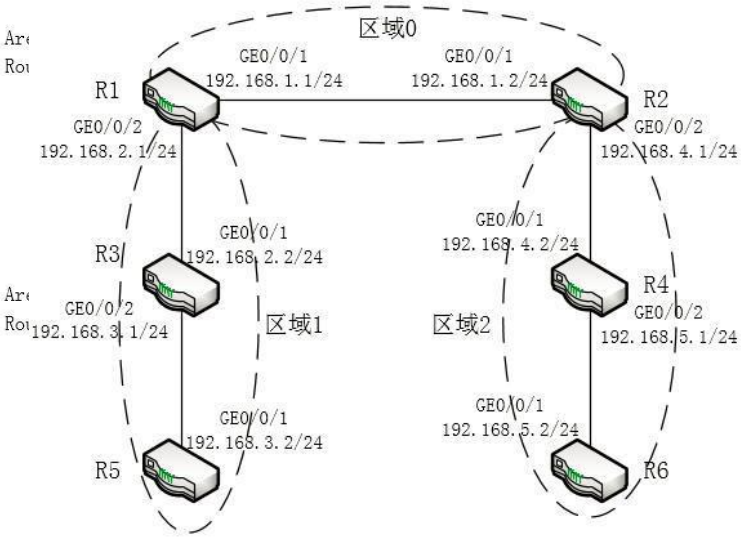


图2

D.R4

参考答案：A

解析：

display ospf [1] peer //查看 OSPF 邻居表的详细信息。

Area：邻居所属的区域。

Interface：与邻居相连的接口。

Router ID：邻居 Router ID。

Address：邻居接口地址。State：邻居状态。

Down：该状态为邻居的初始状态。

Attempt：该状态只存在于 NBMA 网络上，表明正在尝试建立邻居关系。Init：

该状态表明已经接收到了从邻居发送来的 Hello 报文。2-Way：该状态表明已经接收到了从邻居发送过来的 Hello 报文，并且该 Hello 报文的 Neighbor List 中包含本地 Router ID，即双方可以互通。

ExStart：该状态为建立 Adjacency 的第一步，进行主从关系、DD Sequence Number 的协商。

Exchange：从该状态开始，进行 LSDB 同步操作，交互的报文有 DD 报文、LSR 报文、LSU 报文。

Loading：LSDB 正在进行同步操作，交互的报文有 LSR 报文和 LSU 报文。

Full：该状态说明，邻居的 LSDB 已经同步完成，双方建立了 Full 邻接关系。

第 27 题：下图 1 所示内容是在图 2 中的（ ）设备上执行（ ）命令查看到的信息片段。该信息片段中参数（ ）的值反映邻居状态是否正常。

第 27 题：下图 1 所示内容是在图 2 中的（ ）设备上执行（ ）命令查看到的信息片段。该信息片段中参数（ ）的值反映邻居状态是否正常。

```
Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet0/0/1)'s neighbors
Router ID: 2.2.2.2              Address: 192.168.1.2
    State: Full   Mode: Nbr is Master  Priority: 1
    DR: 192.168.1.1   BDR: 192.168.1.2  MTU: 0
    Dead timer due in 32 sec
    Retrans timer interval: 5
    Neighbor is up for 01:06:23
    Authentication Sequence: [0]
        Neighbors
Area 0.0.0.1 interface 192.168.2.1(GigabitEthernet0/0/2)'s neighbors
Router ID: 3.3.3.3              Address 192.168.2.2
    State: Full   Mode: Nbr is Master  Priority: 1
    DR: 192.168.2.1   BDR: 192.168.2.2  MTU: 0
    Dead timer due in 28 sec
    Retrans timer interval: 5
```

图1

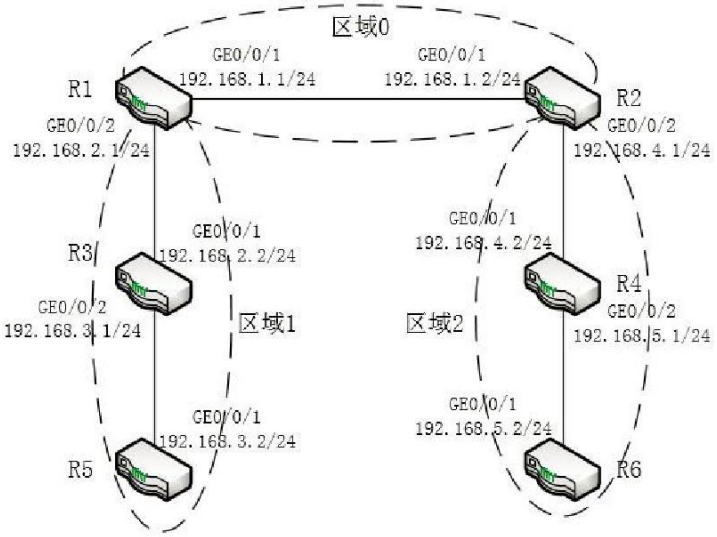


图2

A.display bgp routing-table

B.display isis lsdb

C.display ospf peer

D.dis ip rout

参考答案：C

解析：

display ospf [1] peer //查看 OSPF 邻居表的详细信息。

Area：邻居所属的区域。

Interface：与邻居相连的接口。

Router ID：邻居 Router ID。

Address：邻居接口地址。

State：邻居状态。

Down：该状态为邻居的初始状态。Attempt：该状态只存在于 NBMA 网络上，表明正在尝试建立邻居关系。Init：该状态表明已经接收到了从邻居发送来的 Hello 报文。2-Way：该状态表明已经接收到了从邻居发送过来的 Hello 报文，并且该 Hello 报文的

Neighbor List 中包含本地 Router ID，即双方可以互通。

ExStart：该状态为建立 Adjacency 的第一步，进行主从关系、DD Sequence Number 的协商。

Exchange：从该状态开始，进行 LSDB 同步操作，交互的报文有 DD 报文、LSR 报文、LSU 报文。

Loading：LSDB 正在进行同步操作，交互的报文有 LSR 报文和 LSU 报文。

Full：该状态说明，邻居的 LSDB 已经同步完成，双方建立了 Full 邻接关系。

第 28 题：下图 1 所示内容是在图 2 中的（ ）设备上执行（ ）命令查看到的信息片段。该信息片段中参数（ ）的值反映邻居状态是否正常。

```
Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet0/0/1)'s neighbors
Router ID: 2.2.2.2              Address: 192.168.1.2
    State: Full   Mode: Nbr is Master  Priority: 1
    DR: 192.168.1.1   BDR: 192.168.1.2  MTU: 0
    Dead timer due in 32 sec
    Retrans timer interval: 5
    Neighbor is up for 01:06:23
    Authentication Sequence: [0]
          Neighbors
Area 0.0.0.1 interface 192.168.2.1(GigabitEthernet0/0/2)'s neighbors
Router ID: 3.3.3.3              Address 192.168.2.2
    State: Full   Mode: Nbr is Master  Priority: 1
    DR: 192.168.2.1   BDR: 192.168.2.2  MTU: 0
    Dead timer due in 28 sec
    Retrans timer interval: 5
```

A.State

B.Mode

C.Priority

D.MTU

参考答案：A

解析：

display ospf [1] peer //查看 OSPF 邻居表的详细信息。

Area：邻居所属的区域。

Interface：与邻居相连的接口。

Router ID：邻居 Router ID。

Address：邻居接口地址。State：邻居状态。

Down：该状态为邻居的初始状态。

Attempt：该状态只存在于 NBMA 网络上，表明正在尝试建立邻居关系。Init：该状态表明已经接收到了从邻居发送来的 Hello 报文。2-Way：该状态表明已经接收到了从邻居发送过来的 Hello 报文，并且该 Hello 报文的

Neighbor List 中包含本地 Router ID，即双方可以互通。

ExStart：该状态为建立 Adjacency 的第一步，进行主从关系、DD Sequence Number

的协商。

Exchange：从该状态开始，进行 LSDB 同步操作，交互的报文有 DD 报文、LSR 报文、

LSU 报文。

Loading：LSDB 正在进行同步操作，交互的报文有 LSR 报文和 LSU 报文。

Full：该状态说明，邻居的 LSDB 已经同步完成，双方建立了 Full 邻接关系。

第 29 题：配置 POP3 服务器时，邮件服务器中默认开放 TCP 的（ ）端口。

A.21

B.25

C.53

D.110

参考答案：D

解析：

POP3 是邮局协议，用的是 TCP 的 110 端口。

第 30 题：在 Linux 中，可以使用命令（ ）针对文件 newfiles.txt 为所有用户添加执行权限。

chmod-xnewfiles.txt

B.chmod+xnewfiles.txt C.chmod-w newfiles.txt

D.chmod+w newfiles.txt

参考答案：B

解析：

chmod 更改文件的属性的语法格式为： chmod [who] [opt] [mode] 文件/目录名

其中 who 表示对象，是以下字母中的一个或组合：u（文件所有者）、g（同组用户）、o（其他用户）、a（所有用户）；opt 则代表操作，可以为：+（添加权限）、-（取消权限）、=（赋予给定的权限，并取消原有的权限）；而 mode 则代表权限。

第 31 题：在 Linux 中，可在（ ）文件中修改 Web 服务器配置。

A./etc/host.conf

B./etc/resolv.conf

C./etc/inetd.conf

D./etc/httpd.conf

参考答案：D

解析：

Linux 上 apache 服务的主配置文件是：/etc/httpd.conf。

第 32 题：在 Linux 中，要查看文件的详细信息，可使用（ ）命令。

A.ls-a

B.ls-l

C.ls-i

D.ls-s

参考答案：B

解析：

ls-a：显示当前目录下的所有文件及文件夹包括隐藏的文件；ls-l：显示不隐藏的文件与文件夹的详细信息； ls-i ：查看任意一个文件的 i 节点（类似于身份证唯一信息）；ls-s：在每个文件的后面打印出文件的大小。

第 33 题：在 Windows 命令行窗口中使用（ ）命令可以查看本机各个接口的 DHCP 服务是否已启用。

A.ipconfig

B.ipconfig/all

C.ipconfig/renew

D.ipconfig/release

参考答案：B

解析：

ipconfig/all——当使用 all 选项时，IPConfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，IPConfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

第 34 题：在 Windows 系统的服务项中，（　）服务使用 SMB 协议创建并维护客户端网络与远程服务器之间的连接。

A.SNMP Trap

B.Windows Search

C.Workstation

D.Superfetch

参考答案：C

解析：

SuperFetch 是 Windows Vista 中引入的一项功能。它静静地置于后台，不断分析 RAM

使用模式，并了解您最常运行的应用程序类型。随着时间的推移，SuperFetch 将这些应用程序标记为“经常使用”，并提前将它们预加载到 RAM 中。

关闭 Windows Search 的结果：Windows 中的所有搜索框都将消失，其中包括 Windows 资源管理器、“开始”菜单、“控制面板”、文档库以及其他库中的搜索框，依赖于 Windows Search 的程序可能无法正常运行。

Workstation 服务：创建和维护到远程服务的客户端网络连接。如果服务停止，

这些连接将不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动。

第 35 题：下列不属于电子邮件协议的是（　）。

A.POP3

B.IMAP

C.SMTP

D.MPLS

参考答案：D

解析：

传统的 IP 网络中，分组每到达一个路由器，都必须查找路由表，并按照“最长网络前缀”原则找到下一跳的 IP 地址。当网络很大的时候，查找含有大量项目的路由表要花费很多的时间。MPLS 的一个重要特点就是不用长度可变的 IP 地址网络位来查找路由表中的匹配项目，而是利用标记（label）进行数据转发的。当分组进入网络时，要为其分配固定长度的短的标记，并将标记与分组封装在一起，在整个转发过程中，交换节点仅根据标记进行转发。转发的过程就省去了每到达一个路由器都要上升到第三层用软件去查找路由表的过程，而是根据标记在第二层用硬件转发，所以转发速率大大提高。MPLS 可以使用多种链路层协议，比如 PPP、以太网、ATM 和帧中继等。

第 36 题：下述协议中与安全电子邮箱服务无关的是（　）。

A.SSL

B.HTTPS

C.MIME

D.PGP

参考答案：C

解析：

MIME 即多用途互联网邮件扩展，是目前互联网电子邮件普遍遵循的邮件技术规范。在 MIME 出现之前，互联网电子邮件主要遵循由 RFC 822 所制定的标准，电子邮件一般只用来传递基本的 ASCII 码文本信息，MIME 在 RFC 822 的基础上对电子邮件规范做了大量的扩展，引入了新的格式规范和编码方式，在 MIME 的支持下，图像、声音、动画等二进制文件都可方便的通过电子邮件来进行传递，极大地丰富了电子邮件的功能。目前互联网上使用的基本都是遵循 MIME 规范的电子邮件。

第 37 题：DHCP 服务器设置了 C 类私有地址作为地址池，某 Windows 客户端获得的地址是

169.254.107.100，出现该现象可能的原因是（　）。

A.该网段存在多台 DHCP 服务器

B.DHCP 服务器为客户端分配了该地址

C.DHCP 服务器停止工作

D.客户端 TCP/IP 协议配置错误

参考答案：C

解析：

如果都没有得到 DHCP Server 的回应，客户机会从 169.254.0.0/16 这个自动保留的私有 IP 地址中选用一个 IP 地址。并且每隔 5 分钟重新广播一次，如果收到某个服务器的响应，则继续 IP 租用过程。

第 38 题：在 Windows Server2008 系统中，不能使用 IIS 搭建的是（　）服

务器。

A.WEB

B.DNS

C.SMTP

D.FTP

参考答案：B

解析：

IIS 组件无法搭建 DNS 服务。

第 39 题：用户发出 HTTP 请求后，收到状态码为 505 的响应，出现该现象的原因是（　）。

A.页面请求正常，数据传输成功

B.服务器根据客户端请求切换协议

C.服务器端 HTTP 版本不支持

D.请求资源不存在

参考答案：C

解析：

4 开头的 http 状态码表示请求出错。

服务器不理解请求的语法。

请求要求身份验证。 对于需要登录的网页，服务器可能返回此响应。

服务器拒绝请求。

服务器找不到请求的网页。

禁用请求中指定的方法。

无法使用请求的内容特性响应请求的网页。

此状态代码与 401 类似，但指定请求者应当授权使用代理。

服务器等候请求时发生超时。

服务器在完成请求时发生冲突。 服务器必须在响应中包含有关冲突的信息。

如果请求的资源已永久删除，服务器就会返回此响应。

服务器不接受不含有效内容长度标头字段的请求。

服务器未满足请求者在请求中设置的其中一个前提条件。

服务器无法处理请求，因为请求实体过大，超出服务器的处理能力。

请求的 URI（通常为网址）过长，服务器无法处理。

请求的格式不受请求页面的支持。

如果页面无法提供请求的范围，则服务器会返回此状态代码。

服务器未满足”期望”请求标头字段的要求。

5 开头状态码：

500 （服务器内部错误） 服务器遇到错误，无法完成请求。

501 （尚未实施） 服务器不具备完成请求的功能。 例如，服务器无法识别请求方法时可能会返回此代码。

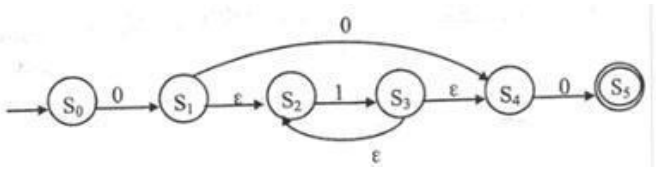
502 （错误网关） 服务器作为网关或代理，从上游服务器收到无效响应。

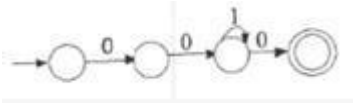
503 （服务不可用） 服务器目前无法使用（由于超载或停机维护）。 通常，这只是暂时状态。

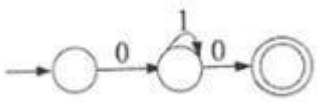
504 （网关超时） 服务器作为网关或代理，但是没有及时从上游服务器收到请求。

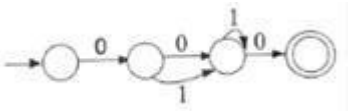
505 （HTTP 版本不受支持） 服务器不支持请求中所用的 HTTP 协议版本

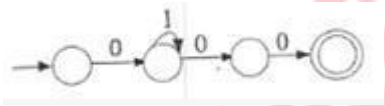
第 40 题：下图所示为一个不确定有限自动机（NFA）的状态转换图，与该 NFA 等价的 DFA 是（　）。



A. 

B. 

C. 

D. 

参考答案：C

解析：

本题可以直接以实例方式排除错误选项。本题给出的 NFA，能够识别字符串 000，010 等，以这两个字符串为例进行分析。

与之等价的 DFA，也必须能够识别这样的串。A 选项不能识别 000，B 选项不能识别 010，D 选项不能识别 010。只有 C 选项能够同时识别这 2 个串，因此本题选择 C 选项。

第 41 题：非对称加密算法中，加密和解密使用不同的密钥，下面的加密算法中（　）属于非对称加密算法。若甲、乙采用非对称密钥体系进行保密通信，甲用

乙的公钥加密数据文件，乙使用（　）来对数据文件进行解密。

A.AES

B.RSA

C.IDEA

D.DES

参考答案：B

解析：

公钥密钥体制的加密和解密过程如下：

（1）密钥对产生器产生出接收者 B 的一对密钥：加密密钥 PKB 和解密密钥 SKB。发送者 A 所用的加密密钥 PKB 就是接收者 B 的公钥，向公众公开。而 B 所用的解密密钥 SKB 就是接收者 B 的私钥，对其他人都保密。

（2）发送者 A 就用 B 的公钥对明文 X 加密，得到密文 Y，发送给 B。（3）B 用自己的私钥进行解密，恢复出明文。

典型的公钥加密算法有：RSA、ECC、背包加密、Rabin 算法等。

第 42 题：非对称加密算法中，加密和解密使用不同的密钥，下面的加密算法中（　）属于非对称加密算法。若甲、乙采用非对称密钥体系进行保密通信，甲用乙的公钥加密数据文件，乙使用（　）来对数据文件进行解密。

A.甲的公钥

B.甲的私钥

C.乙的公钥

D.乙的私钥

参考答案：D

解析：

公钥密钥体制的加密和解密过程如下：

（1）密钥对产生器产生出接收者B的一对密钥：加密密钥PKB和解密密钥SKB。发送者A所用的加密密钥PKB就是接收者B的公钥，向公众公开。而B所用的解密密钥SKB就是接收者B的私钥，对其他人都保密。

（2）发送者A就用B的公钥对明文X加密，得到密文Y，发送给B。

（3）B用自己的私钥进行解密，恢复出明文。

典型的公钥加密算法有：RSA、ECC、背包加密、Rabin算法等。

第43题：用户A和B要进行安全通信，通信过程需确认双方身份和消息不可否认，A、B通信时可使用（　）来对用户的身份进行认证，使用（　）确保消息不可否认。

A.数字证书

B.消息加密

C.用户私钥

D.数字签名

参考答案：A

解析：

数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，提供了一种在Internet上验证您身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构-CA机构，又称为证书授权（CA）中心发行的，人们可以在网上用它来识别对方的身份。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。可以更加方便灵活地运用在电子商务和电子政务

中。

第 44 题：用户 A 和 B 要进行安全通信，通信过程需确认双方身份和消息不可否认，A、B 通信时可使用（ ）来对用户的身份进行认证，使用（ ）确保消息不可否认。

A.数字证书

B.消息加密

C.用户私钥

D.数字签名

参考答案：D

解析：

数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，提供了一种在 Internet 上验证您身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构-CA 机构，又称为证书授权（CA）中心发行的，人们可以在网上用它来识别对方的身份。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。可以更加方便灵活地运用在电子商务和电子政务中。

第 45 题：Windows7 环境下，在命令行状态下执行（ ）命令，可得到下图所示的输出结果，输出结果中的（ ）项，说明 SNMP 服务已经启动，对应端口已经开启。

C :\Users\Administrator>
活动连接

协议	本地地址	外部地址	状态
TCP	0.0.0.0:135	DHKWDF5E3QDGPBE:0	LISTENING
TCP	0.0.0.0:445	DHKWDF5E3QDGPBE:0	LISTENING
TCP	192.168.1.31:139	DHKWDF5E3QDGPBE:0	LISTENING
TCP	[::]:135	DHKWDF5E3QDGPBE:0	LISTENING
TCP	[::]:445	DHKWDF5E3QDGPBE:0	LISTENING
UDP	0.0.0.0:161	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	[::]:161	*:*	
UDP	[::]:500	*:*	
UDP	[::]:4500	*:*	

A.netstat-a

B.ipconfig/all

C.tasklist

D.net start

参考答案：A

解析：

netstat/a：显示本机所有连接和监听端口。

第 46 题：Windows7 环境下，在命令行状态下执行（ ）命令，可得到下图所示的输出结果，输出结果中的（ ）项，说明 SNMP 服务已经启动，对应端口已经开启。

```
C :\Users\Administrator>
活动连接

协议    本地地址          外部地址              状态
TCP     0.0.0.0:135       DHKWDF5E3QDGPBE:0     LISTENING
TCP     0.0.0.0:445       DHKWDF5E3QDGPBE:0     LISTENING
TCP     192.168.1.31:139  DHKWDF5E3QDGPBE:0     LISTENING
TCP     [::]:135          DHKWDF5E3QDGPBE:0     LISTENING
TCP     [::]:445          DHKWDF5E3QDGPBE:0     LISTENING
UDP     0.0.0.0:161       *:*
UDP     0.0.0.0:500       *:*
UDP     0.0.0.0:4500      *:*
UDP     [::]:161          *:*
UDP     [::]:500          *:*
UDP     [::]:4500         *:*
```

A.UDP 0.0.0.0:161

B.UDP 0.0.0.0:500

C.TCP 0.0.0.0:135

D.TCP 0.0.0.0:445

参考答案：A

解析：

161 是 SNMP 协议的轮询端口。

第 47 题：使用 snmptuil.exe 可以查看代理的 MIB 对象，下列文本框内 oid 部分是（ ）。

```
C:\221>snmputil get 192.168.1.31 public .1.3.6.1.2.1.1.3.0
Variable = system.sysUpTime.0
Value    =TimeTicks 1268803
```

A.192.168.1.31

B.1.3.6.1.2.1.1.3.0

C.system.sysUpTime.0

D.TimeTicks 1268803

参考答案：B

解析：

Snmputil 是一个命令行下的软件，查看代理 MIB 信息库的内容，使用语法如下： usage: snmputil get|getnext|walk] agent community oid [oid ...] snmputil trap 其中 agent 表示代理进程的 IP 地址，community 表示团体名，oid 表示 MIB 对象 ID。查询计算机连续开机多长时间

C:>snmputil get 192.168.0.3 public .1.3.6.1.2.1.1.3.0 Variable = system.sysUpTime.0

第 48 题：在华为交换机的故障诊断命令中，查看告警信息的命令是（ ）。

A.dis patch

B.dis trap

C.dis int br

D.dis cu

参考答案：B

解析：

dis patch：查看补丁信息 display patch-information ；

dis trap：查看告警信息 display trapbuffer ；

dis int br：查看接口开启情况 display interface brief ； dis cu：查看当前配置 display current-configuration 。

第 49 题：华为交换机不断重启，每次在配置恢复阶段（未输出“Recover configuration...”之前）就发生复位，下面哪个故障处理措施可以不考虑？（ ）。

A.重传系统大包文件，并设置为启动文件，重启设备

B.新建空的配置文件上传，并设置为启动文件，重启设备

C.重传系统大包文件问题还未解决，再次更新 BOOTROM

D.多次重启后问题无法解决，将问题反馈给华为技术支持

参考答案：B

解析：

是在配置恢复阶段，也就是已经输出 recover configuration 之后。

第 50 题：设备上无法创建正确的 MAC 转发表项，造成二层数据转发失败，故障的原因包括（ ）。

①MAC、接口、VLAN 绑定错误

②配置了 MAC 地址学习去使能

③存在环路 MAC 地址学习错误④MAC 表项限制或超规格

A.①②③④

B.①②④

C.②③

D.②④

参考答案：A

解析：

四个原因都会造成二层数据转发失败。

第 51 题：假设某公司有 8000 台主机，采用 CIDR 方法进行划分，则至少给它分配（ ）个 C 类网络。如果 192.168.210.181 是其中一台主机地址，则其网络地址为（ ）。

A.8

B.10

C.16

D.32

参考答案：D

解析：

8000 台主机，需要 8000/254=32 个 C 类网络。如果 192.168.210.181 是其中 CIDR 地址块的某一个地址，地址块的掩码长度就应该是 8+8+3=19 位。

第 52 题：假设某公司有 8000 台主机，采用 CIDR 方法进行划分，则至少给它分配（　）个 C 类网络。如果 192.168.210.181 是其中一台主机地址，则其网络地址为（　）。

A.192.168.192.0/19

B.192.168.192.0/20

C.192.168.208.0/19

D.192.168.208.0/20

参考答案：A

解析：

其网络地址是 192.168.110 00000 00000000/19。

第 53 题：路由器收到一个数据报文，其目标地址为 20.112.17.12，该地址属于（　）子网。

A.20.112.17.8/30

B.20.112.16.0/24

C.20.96.0.0/11

D.20.112.18.0/23

参考答案：C

解析：

路由器收到一个目的地址为 20.112.17.12 的 IP 数据包，属于 C 选项：20.01100000.0.0——20.01111111.255.255 的范围内。20.96.0.0——20.127.255.255。

第 54 题：IPv6 基本首部的长度为（ ）个字节，其中与 IPv4 中 TTL 字段对应的是（ ）字段。

A.20

B.40

C.64

D.128

参考答案：B

解析：

IPv6 定义了很多可选的扩展首部。可提供比 IPv4 更多的功能。基本首部长度是 40 字节。

第 55 题：IPv6 基本首部的长度为（ ）个字节，其中与 IPv4 中 TTL 字段对应的是（ ）字段。

负载长度

B.通信类型

C.跳数限制

D.下一首部

参考答案：C

解析：

IPv6 协议对其报头定义了 8 个字段。

（1）版本：长度为 6 位，对于 IPv6，本字段的值必须为 6。

（2）通信量类：长度为 8 位，区分不同的 IPv6 数据报的类别或优先级。

流标号：长度为 20 位，用于标识属于同一业务流的包（和资源预分配挂钩）。

（4）有效净荷长度：长度为 16 位，除基本首部以外的字节数。

（5）下一个首部：长度为 8 位，指出了 IPv6 头后所跟的头字段中的协议类型（指出高层是 TCP 还是 UDP）。

（6）跳数限制：长度为 8 位，每转发一次该值减 1，到 0 则丢弃，用于高层设置其超时值。

源地址：长度为 128 位，指出发送方的地址。

（8）目标地址：长度为 128 位，指出接收方的地址。

第 56 题：某校园网的地址是 202.115.192.0/19，要把该网络分成 30 个子网，则子网掩码应该是（　）。

A.255.255.200.0

B.255.255.224.0

C.255.255.254.0

D.255.255.255.0

参考答案：D

解析：

划分成 30 个子网，需要从主机位中拿出 5 位进行子网划分，所以划分后的掩码长度是 19+5=24。

第 57 题：下图 1 所示是图 2 所示网络发生链路故障时的部分路由信息，该信息

来自设备（ ），发生故障的接口是（ ）。

Route Flags: R - relay, D - download to fib

Routing Tables: Public
Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
172.16.1.0/24	RIP	100	2	D	192.168.2.1	GigabitEthernet0/0/2
192.168.2.0/24	Direct	0	0	D	192.168.2.2	GigabitEthernet0/0/2
192.168.2.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
192.168.2.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
192.168.3.0/24	RIP	100	1	D	192.168.2.1	GigabitEthernet0/0/2
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

图1

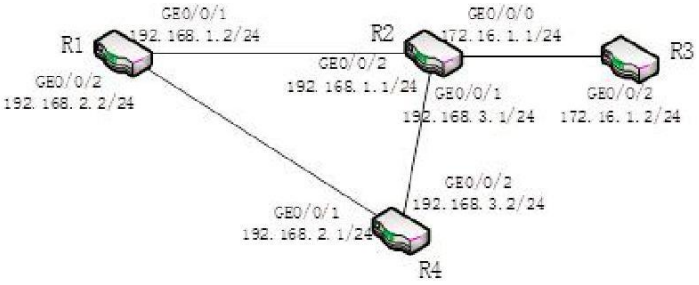


图2

Route Flags: R - relay, D - download to fib

Routing Tables: Public
Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
172.16.1.0/24	RIP	100	2	D	192.168.2.1	GigabitEthernet0/0/2
192.168.2.0/24	Direct	0	0	D	192.168.2.2	GigabitEthernet0/0/2
192.168.2.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
192.168.2.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/2
192.168.3.0/24	RIP	100	1	D	192.168.2.1	GigabitEthernet0/0/2
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

图1

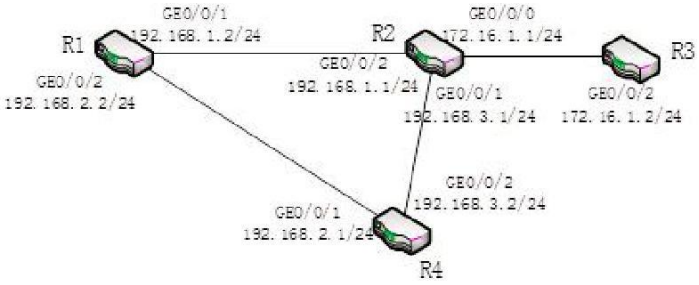


图2

A.R1

B.R2

C.R3

D.R4

参考答案：A

解析：

从路由表的直连网段以及 RIP 学习到的网段来看，属于 R1 的路由表。

第 58 题：下图 1 所示是图 2 所示网络发生链路故障时的部分路由信息，该信息来自设备（　），发生故障的接口是（　）。

A.R2 GE0/0/1

B.R2 GE0/0/2

C.R4 GE0/0/1

D.R4 GE0/0/2

参考答案：B

解析：

RIP 路由协议是基于跳数定义最佳路由，认为经过的路由器数目少为最佳路由。但 R1 路由表显示到达 172.16.1.0/24 网络经过路由器 R4 而不是 R2，所以判断发生故障的接口是 R2 的 GE0/0/2。

第 59 题：以太网的最大帧长为 1518 字节，每个数据帧前面有 8 个字节的前导字段，帧间隔为 9.6μs。传输 240000bit 的 IP 数据报，采用 100BASE-TX 网络，需要的最短时间为（　）。

A.1.23ms

B.12.3ms

C.2.63ms

D.26.3ms

参考答案：C

解析：

IP 数据包的长度是 240000 比特，一共 30000 字节，封装在以太帧里面，需要分片，一共分 20 片（实际应该是 21 片，此题以 20 片计算）。

每个以太帧的传输时间是（1518+8）*8/100Mbps=0.00012208s。20 个以太帧的传输时间是 20*0.00012208=0.0024416s。20 个帧中间会存在 20 个帧间间隔时间 192us。

所以总时间=2441.6+192=2633.6us=2.63ms。

第 60 题：下面列出的 4 种快速以太网物理层标准中，采用 4B5B 编码技术的是（　）。

A.100BASE-FX

B.100BASE-T4

C.100BASE-TX

D.100BASE-T2

参考答案：A

解析：

100BASE-FX 使用与 100BASE-TX 相同的 4B5B 编码和 NRZI 线路代码。

第 61 题：以太网协议中使用了二进制指数后退算法，其冲突后最大的尝试次数为（　）次。

A.8

B.10

C.16

D.20

参考答案：C

解析：

以太网采用截断二进制指数退避算法来解决碰撞问题。截断二进制算法并不复杂，这种算法让发生碰撞的站在停止发送数据后，不是等待信道变为空闲后就立即再发送数据，而是推迟一个随机的时间。这样做是为了使的重传时再次发生冲突的概率减少。当重传次数达 16 次仍不能成功时，则表明同时打算发送数据的站太多，以至连续发生冲突，则丢弃该帧，并向高层报告。

第 62 题：震网（Stuxnet）病毒是一种破坏工业基础设施的恶意代码，利用系统漏洞攻击工业控制系统，是一种危害性极大的（　）。

A.引导区病毒

B.宏病毒

C.木马病毒

D.蠕虫病毒

参考答案：D

解析：

震网（Stuxnet）病毒于 2010 年 6 月首次被检测出来，是第一个专门定向攻击真实世界中基础（能源）设施的“蠕虫”病毒这种病毒可以破坏世界各国的化工、发电和电力传输企业所使用的核心生产控制电脑软件。

第 63 题：默认管理 VLAN 是（　）。

A.VLAN 0

B.VLAN 1

C.VLAN 10

D.VLAN 100

参考答案：B

解析：

默认 VLAN 是 1，也是管理 VLAN。

第 64 题：以下关于跳频扩频技术的描述中，正确的是（　）。

A.扩频通信减少了干扰并有利于通信保密

B.用不同的频率传播信号扩大了通信的范围

C.每一个信号比特编码成 N 个码片比特来传输

D.信号散步到更宽的频带上增加了信道阻塞的概率

参考答案：A

解析：

跳频扩频通信特点：

（1）抗干扰性能好，它具有极强的抗人为宽带干扰、窄带瞄准式干扰、中继转发式干扰的能力，有利于电子反对抗。如果再采用自适应对消、自适应天线、自适应滤波，可以使多径干扰消除，这对军用和民用移动通信是很有利的。

（2）隐蔽性强、干扰小，因信号在很宽的频带上被扩展，单位带宽上的功率很小，即信号功率谱密度很低。信号淹没在白噪声之中，难以发现信号的存在，再加上扩频编码，就更难拾取有用信号。扩频通信技术把被传送的信号带宽展宽，从而降低了系统在单位频宽内的电波“通量密度”，这对空间通信大有好处。

（3）易于实现码分多址，扩频通信占用宽带频谱资源，改善了抗干扰能力，提高了频带的利用率。在跳频扩频中，调制数据信号的载波频率不是固定的，而是扩频码变化。在时间周期 T 中，载波频率不变；但在每个时间周期后，载波频率跳到另一个频率上。跳频扩频是在时间周期后跳到另一个载频上，减少了干扰，并不能扩大通信的范围。每一个信号比特编码成 N 个码片比特来传输是直接序列扩频的原理。扩频技术是将要发送的信息扩展到一个很宽的频带上，以很宽的信道传送信息，抗干扰和抗衰落能力强，抗阻塞能力也强。

第 65 题：下列无线网络技术中，覆盖范围最小的是（　）。

A.802.15.1 蓝牙

B.802.11n 无线局域网

C.802.15.4 ZigBee

D.802.16m 无线城域网

参考答案：A

解析：

1、WIFI，WIFI 是目前应用最广泛的无线通信技术，传输距离在 100-300M，速率可达 300Mbps，功耗 10-50mA。

2、Zigbee，传输距离 50-300M，速率 250kbps，功耗 5mA，最大特点是可自组网，网络节点数最大可达 65000 个。

3、蓝牙，传输距离 2-30M，速率 1Mbps，功耗介于 zigbee 和 WIFI 之间。ZigBee 应用于智能家居的比较多，而蓝牙应用于特别短距离的文件传输。

第 66 题：无线局域网中 AP 的轮询会锁定异步帧，在 IEEE 802.11 网络中定义了（　）机制来解决这一问题。

A.RTS/CTS 机制

B.二进制指数退避

C.超级帧

D.无争用服务

参考答案：D

解析：

通信协议中的 RTS/CTS 协议：即请求发送/允许发送协议，相当于一种握手协议，主要用来解决"隐藏终端"问题。

为了有效地解决无线信道传输中的碰撞问题，IEEE802.11 协议引入了两种媒体访问控制方法：分布式协调功能 DCF 与点协调功能 PCF，这两种方法都属于 MAC 层的虚载波检测机制。在 802.11 的 MAC 层中分为了两个字层：PCF 和 DCF DCF 子层在每一个结点使用 CSMA 机制的分布式接入算法，让各个站通过争用信道来获取发送权。PCF 子层使用集中控制的接入算法将发送数据权轮流交给各个站从而避免了碰撞的产生。PCF 是可选项。对于时间敏感的业务，如分组语音，就应使用提供无争用服务的点协调功能 PCF，可以锁定异步通信量。IEEE802.11 协议允许 PCF 与 DCF 共存于一个无线局域网中，而实现这种共存的具体方法是引入“超级帧”（Super Frame）的概念。超级帧只是一个逻辑上的概念，而并非实际存在的一种帧格式。或者更确切地说是因为它在时间上表现为非严格周期性地以类似帧的形式出现，代表了一段时间内媒体上的业务量。在超级帧中包含两部分：无竞争时期（Contention Free Period，简称为 CFP）和竞争时期（Contention Period，简称为 CP）。在 CFP 期间，由 PCF 控制对媒体的访问，而在 CP 期间，由 DCF 来控制。CFP 与 CP 的

交替出现，使得 PCF 与 DCF 轮流行使对无线媒体的访问控制权，从而实现 PCF 与 DCF 在一个基本服务组 BSS 内的共存。

第 67 题：RAID 技术中，磁盘容量利用率最低的是（　）。

A.RAID0

B.RAID1

C.RAID5

D.RAID6

参考答案：B

解析：

RAID 0 磁盘利用率 100%，RAID 1 利用率 50%，RAID 5 磁盘利用率（N-1）/N，N 最

小取 3。RAID 6 磁盘利用率（N-2）/N，N 最小为 4。

第 68 题：三层网络设计方案中，（　）是汇聚层的功能。

A.不同区域的高速数据转发

B.用户认证、计费管理

C.终端用户接入网络

D.实现网络的访问策略控制

参考答案：D

解析：

核心层是互连网络的高速主干网，在设计中应增加冗余组件，使其具备高可靠性，能快速适应通信流量的变化。设计核心层设备的功能时应避免使用数据包过滤、策略路由等降低转发速率的功能特性，使得核心层具有高速率、低延迟和良好的

可管理性。 核心层设备覆盖的地理范围不宜过大，连接的设备不宜过多，否则会使得网络的复杂度增大，导致网络性能降低。 核心层应包括一条或多条连接外部网络的专用链路，使得可以高效地访问互联网。汇聚层是核心层与接入层之间的分界点，应实现资源访问控制和流量控制等功能。汇聚层应该对核心层隐藏接入层的详细信息，不管划分了多少个子网，汇聚层向核心路由器发布路由通告时，只通告各个子网汇聚后的超网地址。 如果局域网中运行了以太网和弹性分组环等不同类型的子网，或者运行了不同路由算法的区域网络，可以通过汇聚层设备完成路由汇总和协议转换功能。

接入层提供网络接入服务，并解决本地网段内用户之间互相访问的需求，要提供足够的带宽，使得本地用户之间可以高速访问； 接入层还应提供一部分管理功能，例如 MAC 地址认证、用户认证、计费管理等； 接入层要负责收集用户信息(例如用户 U 地址、MAC 地址、访问日志等)，作为计费和排错的依据。选项“不同区域的高速数据转发”为核心层、选项“用户认证、计费管理”为接入层、选项“终端用户接入网络”为接入层，选项“实现网络的访问策略控制”为汇聚层。

第 69 题：以下关于网络工程需求分析的叙述中，错误的是（ ）。

A.任何网络都不可能是一个能够满足各项功能需求的万能网

B.需求分析要充分考虑用户的业务需求

C.需求的定义越明确和详细，网络建成后用户的满意度越高

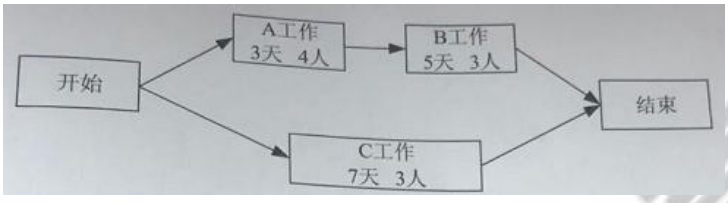
D.网络需求分析时可以先不考虑成本因素

参考答案：D

解析：

在建设或扩建一个网络系统前，用户方的 IT 主管或中标的网络系统设计者都必须关注网络系统中的需求问题。也就是说要确定网络系统支持的业务、完成的功能、要达到的性能。

第 70 题：下图为某网络工程项目的施工计划图，要求该项目 7 天内完工，至少需要投入（　）人才能完成该项目（假设每个技术人员均能胜任每项工作）。



A.4

B.6

C.7

D.14

参考答案：C

解析：

当投入 7 人时候，分给 C 工作 3 人，分给 A 工作 4 人，A 工作 3 天完成，完成后这 4 人投入到 B 工作，B 工作可以把时长缩短到 7.5/2 天，能满足 7 天完工的需求。

第 71 题：Network security consists of policies and practices to prevent and monitor（ ）access,misuse, modification, or denial of a computer network and network-accessible resources.Network security involves the authorization of access to data in a network, which is

controlled by the network( ).Users choose or are assigned an ID and password or other authenticating information that allows them to access to information and programs within their authority.Network security secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a （ ） name and a corresponding password. Network security starts with authentication. Once authenticated,a（ ）enforces access policies such as what services are allowed to be accessed by the network users.Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer（ ）or Trojans being transmitted over the network.

A.unauthorized

B.harmful

C.dangerous

D.frequent

参考答案：A

第 72 题： Network security consists of policies and practices to prevent and monitor（ ）access,misuse, modification, or denial of a computer network and network-accessible resources.Network security involves the authorization of access to data in a network, which is controlled by the network（ ）.Users choose or are assigned

an ID and password or other authenticating information that allows them to access to information and programs within their authority.Network security secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a （ ） name and a corresponding password. Network security starts with authentication.

Once authenticated,a（ ）enforces access policies such as what services are allowed to be accessed by the network users.Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer（ ）or Trojans being transmitted over the network.

A.user

B.agent

C.server

D.administrator

参考答案：D

第 73 题： Network security consists of policies and practices to prevent and monitor（ ）access,misuse, modification, or denial of a computer network and network-accessible resources.Network security involves the authorization of access to data in a network, which is controlled by the network（ ）.Users choose or are assigned

an ID and password or other authenticating information that allows them to access to information and programs within their authority.Network security secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a （ ） name and a corresponding password. Network security starts with authentication. Once authenticated,a（ ）enforces access policies such as what services are allowed to be accessed by the network users.Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer（ ）or Trojans being transmitted over the network.

A.complex

B.unique

C.catchy

D.long

参考答案：B

第 74 题： Network security consists of policies and practices to prevent and monitor（ ）access,misuse, modification, or denial of a computer network and network-accessible resources.Network security involves the authorization of access to data in a network, which is controlled by the network（ ）.Users choose or are assigned an ID and password or other authenticating information that allows

them to access to information and programs within their authority.Network security secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a （ ） name and a corresponding password. Network security starts with authentication.

Once authenticated,a（ ）enforces access policies such as what services are allowed to be accessed by the network users.Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer（ ）or Trojans being transmitted over the network.

A.firewall

B.proxy

C.gateway

D.host

参考答案：A

第 75 题： Network security consists of policies and practices to prevent and monitor（ ）access,misuse, modification, or denial of a computer network and network-accessible resources.Network security involves the authorization of access to data in a network, which is controlled by the network（ ）.Users choose or are assigned an ID and password or other authenticating information that allows

them to access to information and programs within their authority.Network security secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a （ ） name and a corresponding password. Network security starts with authentication. Once authenticated,a（ ）enforces access policies such as what services are allowed to be accessed by the network users.Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer（ ）or Trojans being transmitted over the network.

A.spams

B.malwares

C.worms

D.programs

参考答案：C