

●在磁盘调度管理中，应先进行移臂调度，再进行旋转调度。假设磁盘移动臂位于 21 号柱面上，进程的请求序列如下表所示。如果采用最短移臂调度算法，那么系统的响应序列应为( )。

| 请求序列 | 柱面号 | 磁头号 | 扇区号 |
|------|-----|-----|-----|
| ①    | 17  | 8   | 9   |
| ②    | 23  | 6   | 3   |
| ③    | 23  | 9   | 6   |
| ④    | 32  | 10  | 5   |
| ⑤    | 17  | 8   | 4   |
| ⑥    | 32  | 3   | 10  |
| ⑦    | 17  | 7   | 9   |
| ⑧    | 23  | 10  | 4   |
| ⑨    | 38  | 10  | 8   |

- (1) A. ②⑧③④⑤①⑦⑥⑨                      B. ②③⑧④⑥⑨①⑤⑦  
 C. ①②③④⑤⑥⑦⑧⑨                      D. ②⑧③⑤⑦①④⑥⑨

解析：D

当进程请求读磁盘时，操作系统先进行移臂调度，再进行旋转调度。最短移臂调度算法指距离现在移动臂位置最近的柱面号请求将优先得到响应(移动臂移动距离最短)，所以响应顺序应该为 21→23→17→32→38，而对于同样柱面号不同扇区号的请求，将按磁头旋转时的划过头顺序，可以简单理解为扇区号小的优先响应。

●某文件系统采用多级索引结构,若磁盘块的大小为 4K 字节,每个块号需占 4 字节,那么采用二级索引结构时的文件最大长度可占用( )个物理块。

- (2) A. 1024                      B. 1024 x 1024                      C. 2048 x 2048                      D. 4096 x 4096

解析：B

一级文件索引(直接索引)结构中：在文件目录表项中有一组表项用于索引，每一个表项登记的是逻辑记录所在的磁盘块号。逻辑记录与磁盘块号的大小相等，都为 512B。

二级文件索引(一级间接索引)结构中：文件目录中有一组表项，其内容登记的是第一级索引表块的块号。第一级索引表块中的索引表登记的是文件逻辑记录所在的磁盘块号。

三级文件索引（二级间接索引）结构中：文件目录项中有一组表项，其内容登记的是第二级索引表块的块号。第二级索引表块中的索引表项登记的是第一级索引表块的块号，第一级索引表项中登记的是文件逻辑记录所在的磁盘块号。

磁盘块为 4 KB，一个地址项(块号)为 4 字节，所以一个磁盘块可以存储  $4 \times 1024 / 4 = 1024$  个地址项(块号)，二级间接地址索引可以表示  $1024 \times 1024 = 1048576$  个磁盘块。

●CPU 的频率有主频、倍频和外频。某处理器外频是 200MHz，倍频是 13，该款处理器的主频是( )。

- (3) A. 2.6GHz                      B. 1300MHz                      C. 15.38Mhz                      D. 200MHz

解析：A

CPU 的主频，即 CPU 内核工作的时钟频率 (CPU Clock Speed)。通常所说的某某 CPU 是多少兆赫的，而这个多少兆赫就是“CPU 的主频”。主频越高，CPU 的运算速度就越快。但主频不等于处理器一秒钟执行的指令条数，因为一条指令的执行可能需要多个时钟周期。对于 CPU，在有兼容性的前提下，主要看其速度，而主频越高，字节越长，CPU 速度就越快。CPU 的主频=外频\*倍频=200MHz\*13=2.6GHz

●为了优化系统的性能，有时需要对系统进行调整。对于不同的系统，其调整参数也不尽相同。例如，对于数据库系统，主要包括 CPU/内存使用状况、(4)、进程/线程使用状态、日志文件大小等。对于应用系统，主要包括应用系统的可用性、响应时间、(5)、特定应用资源占用等。

- (4) A. 数据丢包率                      B. 端口吞吐量  
C. 数据处理速率                      D. 查询语句性能  
(5) A. 并发用户数                      B. 支持协议和标准  
C. 最大连接数                      D. 时延抖动

解析：D A

此题为历年真题原题。

●软件重用是使用已有的软件设计来开发新的软件系统的过程，软件重用可以分为垂直式重用和水平式重用。( )是一种典型的水平式重用。

- (6) A. 医学词汇表                      B. 标准函数库

C. 电子商务标准

D. 网银支付接口

解析：B

- 1) 可重用性（可复用性）是指系统和（或）其组成部分能在其他系统中重复使用的程度。
- 2) 软件重用（软件复用）是使用已有的软件产品（如设计、代码和文档等）来开发新的软件系统的过程。
- 3) 软件重用的形式大体可分为垂直式重用和水平式重用。
- 4) 水平式重用是重用不同应用领域中的软件元素，如标准函数库。
- 5) 垂直式重用是在一类具有较多公共性的应用领域之间重用软件构件。
- 6) Caper Jones 定义了 10 种可能重用的软件要素，分别是项目计划、成本估计、架构、需求模型和规格说明、设计、源程序代码、用户文档和技术文档、用户界面、数据结构和测试用例。
- 7) 系统的软件重用包括可重用的资产（构件）的开发、管理、支持和重用 4 个过程。

●软件测试一般分为两个大类:动态测试和静态测试。前者通过运行程序发现错误,包括(7)等方法;后者采用人工和计算机辅助静态分析的手段对程序进行检测,包括(8)等方法。

- |                        |                   |
|------------------------|-------------------|
| (7) A. 边界值分析、逻辑覆盖、基本路径 | B. 桌面检查、逻辑覆盖、错误推测 |
| C. 桌面检查、代码审查、代码走查      | D. 错误推测、代码审查、基本路径 |
| (8) A. 边界值分析、逻辑覆盖、基本路径 | B. 桌面检查、逻辑覆盖、错误推测 |
| C. 桌面检查、代码审查、代码走查      | D. 错误推测、代码审查、基本路径 |

解析：A C

●某软件程序员接受 X 公司(软件著作权人)委托开发一个软件,三个月后又接受 Y 公司委托开发功能类似的软件,该程序员仅将受 X 公司委托开发的软件略作修改即完成提交给 Y 公司,此种行为( )

- |                 |              |
|-----------------|--------------|
| (9) A. 属于开发者的特权 | B. 属于正常使用著作权 |
| C. 不构成侵权        | D. 构成侵权      |

解析：D

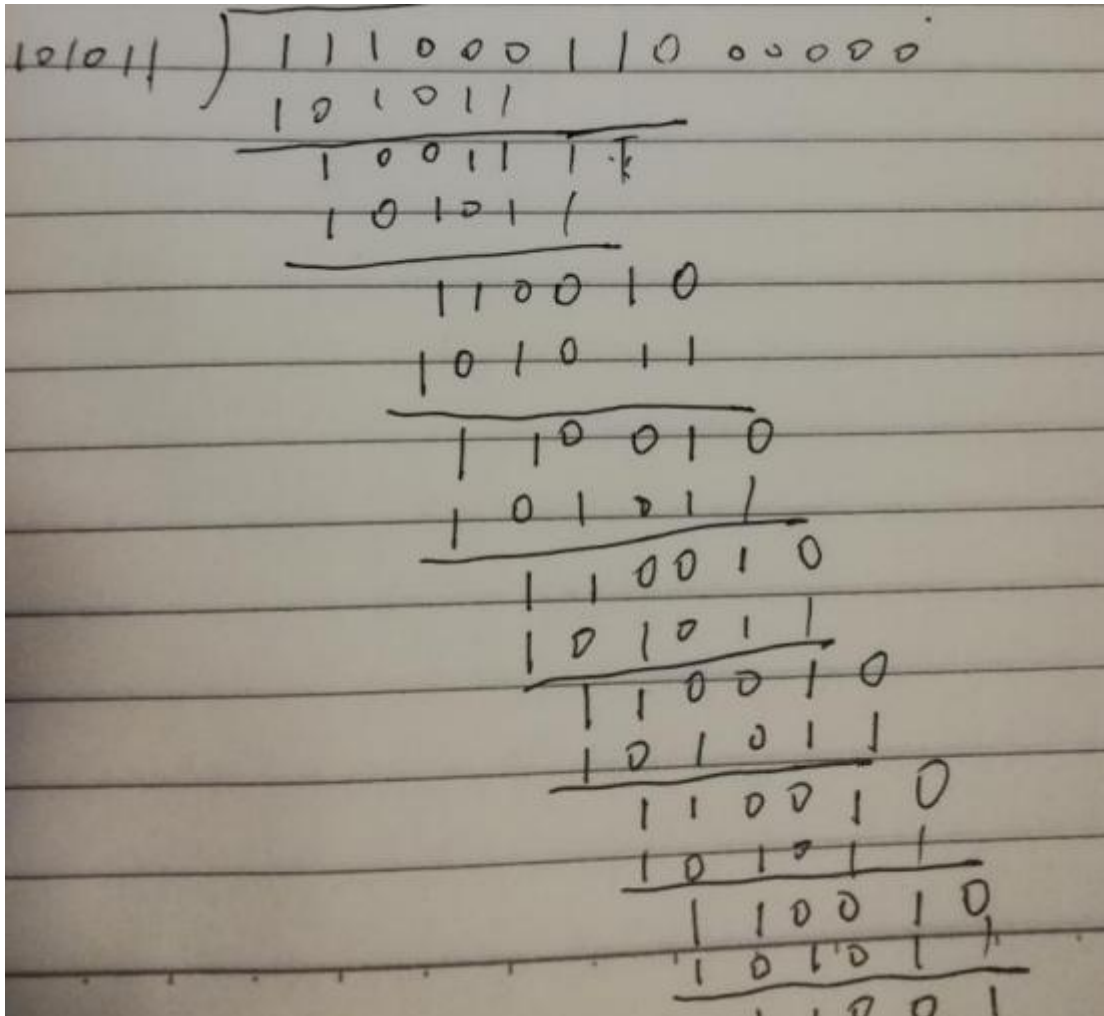
职务作品著作权归公司享有。未经软件著作权人或者其合法受让者的同意,修改、翻译、

注释其软件作品。此种行为是侵犯了著作权人或其合法受让者的使用权中的修改权、翻译权与注释权。

●若信息码字为 111000110,生成多项式  $G(X)=x^5+x^3+x+1$ ,则计算出的 CRC 校验码为( )。

- (10) A. 01101                      B. 11001                      C. 001101                      D. 011001

解析: B



●关于 HDLC 协议的帧顺序控制, 下列说法中正确的是( )。

- (11) A. 只有信息帧(I)可以发送数据
- B. 信息帧(I)和管理帧(S)的控制字段都包含发送顺序号和接收序列号
- C. 如果信息帧(I)的控制字段是8位,则发送顺序号的取值范围是  $0 \sim 7$
- D. 发送器每收到一个确认帧,就把窗口向前滑动一格

B. 信息帧(I)和管理帧(S)的控制字段都包含发送顺序号和接收序列号

C. 如果信息帧(I) 的控制字段是 8 位, 则发送顺序号的取值范围是  $0 \sim 7$

D. 发送器每收到一个确认帧，就把窗口向前滑动一格

解析: C

## HDLC 的帧类型

### (1) 信息帧 (I 帧)

本文档由微信号:ruankaopass, 一手整理, 通过他人购买的, 拒绝售后。本人专业提供软考历年真题

信息帧用于传送有效信息或数据, 通常简称 I 帧。I 帧以控制字段第一位为“0”来标志。信息帧的控制字段中的 N(S) 用于存放发送帧序号, 以使发送方不必等待确认而连续发送多帧。N(R) 用于存放接收方下一个预期要接收的帧的序号, N(R)=5, 即表示接收方下一帧要接收 5 号帧, 换言之, 5 号帧前的各帧接收到。N(S) 和 N(R) 均为 3 位二进制编码, 可取值 0~7。

### (2) 监控帧 (S 帧)

监控帧用于差错控制和流量控制, 通常简称 S 帧。S 帧以控制字段第一、二位为“10”来标志。S 帧带信息字段, 只有 6 个字节即 48 个比特。S 帧的控制字段的第三、四位为 S 帧类型编码, 共有四种不同编码, 分别表示:

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, 但目前正处于忙状态, 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。

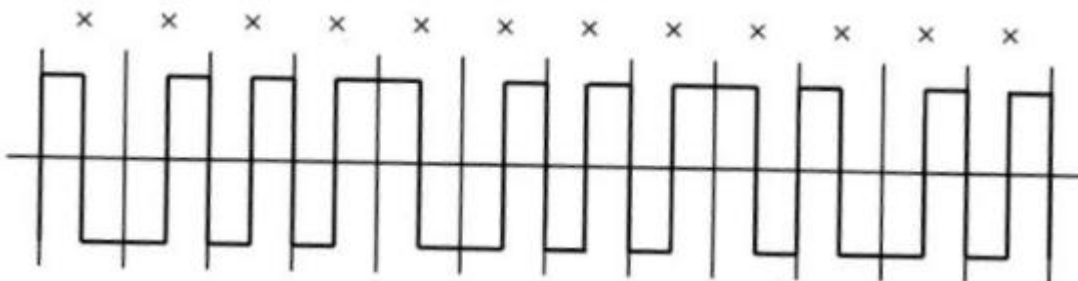
11——选择拒绝 (SREJ), 它要求发送方发送编号为 N(R) 单个 I 帧, 并暗示它编号的 I 帧已全部确认。可以看出, 接收就绪 RR 型 S 帧和接收未就绪 RNR 型 S 帧有两个主要功能: 首先, 这两种类型的 S 帧用来表示从站已准备好或未准备好接收信息; 其次, 确认编号小于 N(R) 的所有接收到的 I 帧。拒绝 REJ 和选择拒绝 SREJ 型 S 帧, 用于向对方站指出发生了差错。REJ 帧用于 GO-back-N 策略, 用以请求重发 N(R) 以前的帧已被确认, 当收到一个 N(S) 等于 REJ 型 S 帧的 N(R) 的 I 帧后, REJ 状态即可清除。SREJ 帧用于选择重发策略, 当收到一个 N(S) 等 SREJ 帧的 N(R) 的 I 帧时, SREJ 状态即应消除。

### (3) 无编号帧 (U 帧)

无编号帧因其控制字段中不包含编号 N(S) 和 N(R) 而得名, 简称 U 帧。U 帧用于提供对链路的建立、拆除以及多种控制功能, 但是当要求提供不可靠的无连接服务时, 它有时也可

以承载数据。这些控制功能 5 个 M 位（M1、M2、M3、M4、M5，也称修正位）来定义。5 个 M 位可以定义 32 种附加的命令功能或 32 种应答功能，但目前许多是空缺的。

●下图中 12 位差分曼彻斯特编码的信号波形表示的数据是（ ）。



- (12) A. 001100110101                      B. 010011001010  
C. 100010001100                      D. 011101110011

解析：B

在曼彻斯特编码中，每一位的中间有一跳变，位中间的跳变既作时钟信号，又作数据信号；从低到高跳变表示“1”，从高到低跳变表示“0”。还有一种是差分曼彻斯特编码，每位中间的跳变仅提供时钟定时，而用每位开始时有无跳变表示“0”或“1”，有跳变为“0”，无跳变为“1”。

●100BASE-X 采用的编码技术为 4B/5B 编码，这是一种两级编码方案，首先要把 4 位分为一组的代码变换成 5 单位的代码，再把数据变成（ ）编码。

- (13) A. NRZ-I                                  B. AMI  
C. QAM    D. PCM

解析：A

4B:5B 编码方案是把数据转换成 5 位符号，供传输，因其效率高和容易实现而被采用。这种编码的特点是将欲发送的数据流每 4bit 作为一个组，然后按照 4B/5B 编码规则将其转换成相应 5bit 码，并且由 NRZI 方式传输。5bit 码共有 32 种组合，但只采用其中的 16 种对应 4bit 码的 16 种，其他的 16 种或者未用或者用作控制码，以表示帧的开始和结束、光纤线路的状态（静止、空闲、暂停）等。

●在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位，每秒钟传送 200 个字符，采用 QPSK 调制，则码元速率为（ ）波特。

- (14) A. 500  
B. 550  
C. 1100  
D. 2200

解析：C

每个字符包括 11 位，每秒传送 200 个字符，所以数据速率 R 为  $200 \times 11 = 2200\text{bps}$ 。采用 QPSK 调制，码元种类为 4 种， $R = B \log_2 N$ ，所以  $B = 1100$

●通过 HFC 接入 Internet，用户端通过( )连接因特网。

- (15) A. ADSL Modem  
B. Cable Modem  
C. IP Router  
D. HUB

解析：B

电缆调制解调器 (Cable Modem, CM)，Cable 是指有线电视网络，Modem 是调制解调器。平常用 Modem 通过电话线上互联网，而电缆调制解调器是在有线电视网络上用来上互联网的设备，它是串接在用户家的有线电视电缆插座和上网设备之间的，而通过有线电视网络与之相连的另一端是在有线电视台(称为头端：Head-End)。它把用户要上传的上行数据以 5-65M 的频率以 QPSK 或 16QAM 的调制方式调制之后向上传送，带宽 2-3M 左右，速率从 300 到 10Mbps。它把头端发来的下行数据，解调的方式是 64QAM 或 256QAM，带宽 6-8M，速率可达 40Mbps。电缆调制解调器 (Cable Modem) 技术就是基于 CATV (HFC) 网的网络接入技术。

●若采用后退 N 帧 ARQ 协议进行流量控制，帧编号字段为 7 位，则发送窗口最大长度为( )。

- (16) A. 7  
B. 8  
C. 127  
D. 128

解析：C

●在局域网中仅某台主机上无法访问域名为 www.ccc.com 的网站(其他主机访问正常)，在该主机上执行 ping 命令时有显示信息如下：

```
C:\>ping www.ccc.com
Pinging www.ccc.com [202.117.112.36] with 32 bytes of data:
Reply from 202.117.112.36: Destination net unreachable.
Reply from 202.117.112.36: Destination net unreachable.
Reply from 202.117.112.36: Destination net unreachable.
Reply from 202.117.112.36: Destination net unreachable.

Ping statistics for 202.117.112.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- (17) A. 该主机的 TCP/IP 协议配置错误  
B. 该主机设置的 DNS 服务器工作不正常  
C. 该主机遭受 ARP 攻击导致网关地址错误  
D. 该主机所在网络或网站所在网络中配置了 ACL 拦截规则

解析：D

通过观察回包发现目的端已经 ping 通，但是正常数据过不去，说明有可能是 ACL 限制。

● 以下关于网络冗余设计的叙述中，错误的是( )。

- (18) A. 网络冗余设计避免网络组件单点失效造成应用失效  
B. 备用路径提高了网络的可用性，分担了主路径部分流量  
C. 负载分担是通过并行链路提供流量分担  
D. 网络中存在备用路径、备用链路时，通常加入负载分担设计

解析：B

备用路径做备份使用，在主路径故障后可以顶上。

● 在客户机上运行 nslookup 查询某服务器名称时能解析出 IP 地址，查询 IP 地址时却不能解析出服务器名称，解决这一问题的方法是( )

- (19) A. 清除 DNS 缓存  
B. 刷新 DNS 缓存  
C. 为该服务器创建 PTR 记录  
D. 重启 DNS 服务

解析：C



PTR (Pointer Record)，指针记录，是电子邮件系统中的一种数据类型，被互联网标准文件 RFC1035 所定义。与其相对应的是 A 记录、地址记录。二者组成邮件交换记录。

A 记录解析名字到地址，而 PTR 记录解析地址到名字。

地址是指一个客户端的 IP 地址，名字是指一个客户的完全合格域名。

●在 DHCP 服务器设计过程中，不同的主机划分为不同的类别进行管理，下面划分中合理的是( )

- (20) A. 移动用户采用保留地址  
B. 服务器可以采用保留地址  
C. 服务器划分到租约期最短的类别  
D. 固定用户划分到租约期较短的类别

解析：B

服务器需要使用固定地址对外提供服务。

●IP 数据报首部中 IHL (Internet 首部长度) 字段的最小值为( )。

- (21) A. 5  
B. 2  
C. 32  
D. 128

解析：A

- Version - 4 位字段，指出当前使用的 IP 版本。
- IP Header Length (IHL) - 指数据报协议头长度，具有 32 位字长。指向数据起点。正确协议头最小值为 5。
- Type-of-Service - 指出上层协议对处理当前数据报所期望的服务质量，并对数据报按照重要性级别进行分配。这些 8 位字段用于分配优先级、延迟、吞吐量以及可靠性。
- Total Length - 指定整个 IP 数据包的字节长度，包括数据和协议头。其最大值为 65,535 字节。典型的主机可以接收 576 字节的数据报。
- Identification - 包含一个整数，用于识别当前数据报。该字段由发送端分配帮助接收端集中数据报分片。

●若有带外数据需要传送，TCP 报文中( )标志字段置“1”。

- (22) A. PSH    B. FIN  
C. URG    D. ACK

解析: C

紧急字段 URG:告诉系统此报文段中有紧急数据,应尽快传送。当 URG=1 时。紧急指针:指出在本报文段中的紧急数据的最后一个字节的序号,即指出带外数据字节在正常字节流中的位置。当 TCP 发送带外数据时,他的 TCP 首部一定是设置了 URG 标志和紧急指针的。而紧急指针就是用来指出带外数据字节在正常字节流中的位置的。

- 如果发送给 DHCP 客户端的地址已经被其他 DHCP 客户端使用，客户端会向服务器发送 ( ) 信息包拒绝接受已经分配的地址信息。

- (23) A. DhcpAck  
B. DhcpOffer  
C. DhcpDecline  
D. DhcpNack

解析: C

1) DHCPDISCOVER (0x01), 此为 Client 开始 DHCP 过程的第一个报文

2) DHCP OFFER (0x02), 此为 Server 对 DHCP DISCOVER 报文的响应

3) DHCPREQUEST (0x03), 此报文是 Client 开始 DHCP 过程中对 server 的 DHCP OFFER 报

文的回应, 或者是 Client 续延 IP 地址租期时发出的报文

4) DHCPDECLINE (0x04), 当 Client 发现 Server 分配给它的 IP 地址无法使用, 如 IP 地址冲突时, 将发出此报文, 通知 Server 禁止使用 IP 地址。

5) DHCPACK (0x05), Server 对 Client 的 DHCPREQUEST 报文的确认响应报文, Client 收到此报文后, 才真正获得了 IP 地址和相关的配置信息。

6) DHCPNAK (0x06), Server 对 Client 的 DHCPREQUEST 报文的拒绝响应报文, Client 收到此报文后, 一般会重新开始新的 DHCP 过程。

7)DHCPRELEASE(0x07),Client 主动释放 server 分配给它的 IP 地址的报文,当 Server 收到此报文后,就可以回收这个 IP 地址,能够分配给其他的 Client。

8)DHCPINFORM(0x08),Client 已经获得了 IP 地址,发送此报文,只是为了从 DHCP SERVER 处获取其他的一些网络配置信息,如 route ip, DNS Ip 等,这种报文的应用非常少见。

●地址 202.118.37.192/26 是(24)，地址 192.117.17.255/22 是(25)。

- (24) A. 网络地址  
B. 组播地址  
C. 主机地址  
D. 定向广播地址
- (25) A. 网络地址  
B. 组播地址  
C. 主机地址  
D. 定向广播地址

解析：A C

192/26 1100 0000。主机地址全 0，表示网络地址。

17.255/22 00010001 11111111 表示主机地址。

●将地址块 192.168.0.0/24 按照可变长子网掩码的思想进行子网划分，若各部门可用主机地址需求如下表所示，则共有(26)种划分方案，部门 3 的掩码长度为(27)。

| 部门   | 所需地址总数 |
|------|--------|
| 部门 1 | 100    |
| 部门 2 | 50     |
| 部门 3 | 16     |
| 部门 4 | 10     |
| 部门 5 | 8      |

- (26) A. 4  
B. 8  
C. 16  
D. 32
- (27) A. 25  
B. 26  
C. 27  
D. 28

解析：C C

部门一需要 100 台机子，所以需要  $2^7=128>100$  需要 7 位主机位，这种组合方式有两种。同理部门 50 台机子，所以需要  $2^6=64>50$  需要六位主机位，这种组合方式有两种。..... 最后部门 4、部门 5 在一个组合之内。故共有  $2^4=16$  种组合方式。

●若一个组播组包含 6 个成员，组播服务器所在网络有 2 个路由器，当组播服务器发送信息时需要发出( )个分组。

- (28) A. 1  
B. 2

C. 3

D. 6

答案：A

组播(Multicast)传输是在发送者和每一接收者之间实现点对多点网络连接。它解决了单播和广播方式效率低的问题。当网络中的某些用户需求特定信息时，组播源(即组播信息发送者)仅发送一次信息，组播路由器借助组播路由协议为组播数据包建立树型路由，被传递的信息在尽可能远的分叉路口才开始复制和分发。

●在 BGP4 协议中，当出现故障时采用( )报文发送给邻居。

(29) A. trap

B. update

C. keepalive

D. notification

答案：D

BGP 使用四种消息、类型：

Open 消息：Open 消息是 TCP 连接建立后发送的第一个消息用于建立 BGP 对等体之间的连接关系。

Keepalive 消息：BGP 会周期性地向对等体发出 Keepalive 消息，用来保持连接的有效性。

Update 消息：Update 消息用于在对等体之间交换路由信息。它既可以发布可达路由信息、也可以撤销不可达路由信息。

Notification 消息：当 BGP 检测到错误状态时，就向对等体发出 Notification 消息，之后 BGP 连接会立即中断。

●下列 DNS 查询过程中，合理的是( )

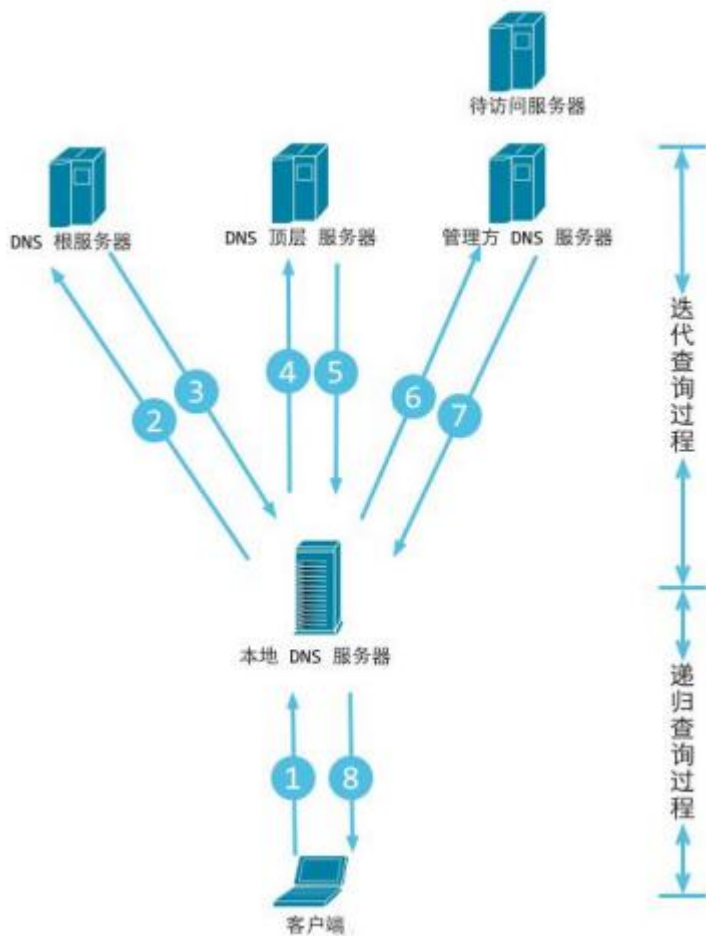
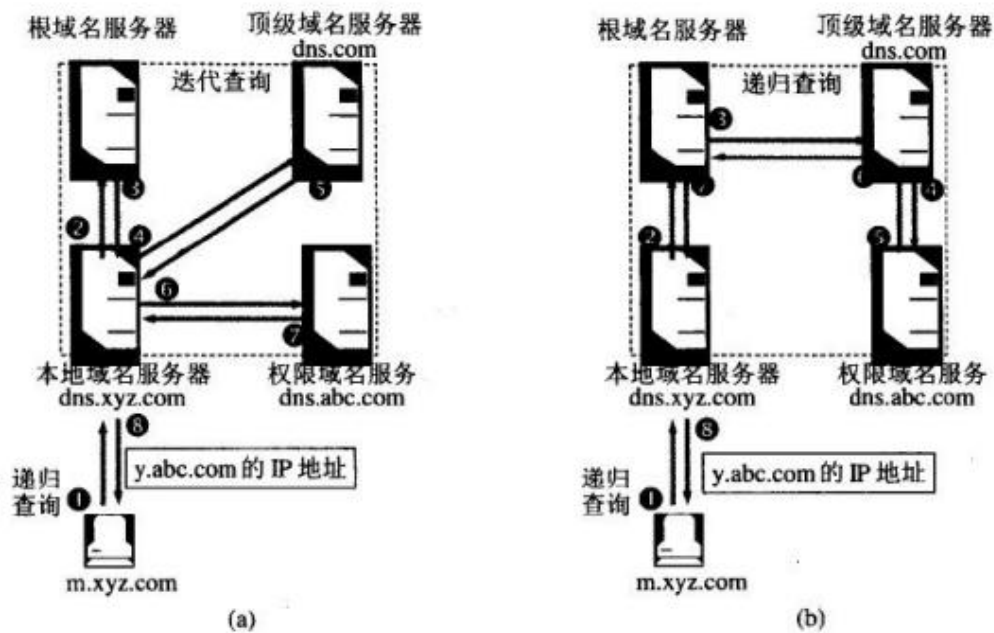
(30) A. 本地域名服务器把转发域名服务器地址发送给客户机

B. 本地域名服务器把查询请求发送给转发域名服务器

C. 根域名服务器把查询结果直接发送给客户机

D. 客户端把查询请求发送给中介域名服务器

解析：B





区域内路由器 IR (Internal Routers)：该类路由器的所有接口都属于同一个 OSPF 区域。区域边界路由器 ABR (Area Border Routers)：该类路由器可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。骨干路由器 BR (Backbone Routers)：该类路由器至少有一个接口属于骨干区域。因此，所有的 ABR 和位于 Area0 的内部路由器都是骨干路由器。自治系统边界路由器 ASBR (AS Boundary Routers)：与其他 AS 交换路由信息的路由器称为 ASBR。ASBR 并不一定位于 AS 的边界，它可能是区域内路由器，也可能是 ABR。

本文档由微信号:ruankaopass，一手整理，通过他人购买的，拒绝售后。本人专业提供软考历年真题

●DNS 服务器中提供了多种资源记录，其中定义区域授权域名服务器的是( )。

- (34) A. SOA B. NS  
C. PTR D. MX

解析：A

A 记录:也称为主机记录，作用是将域名解析成对应的 IP

NS 记录:也称为名称服务器记录，用于说明这个区域有哪些。NS 服务器负责解析

SOA 记录:起始授权机构记录，SOA 记录说明在众多 NS 记录里那台是主服务器

MX 记录:邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮件服务器。

CNAME 记录:别名记录

SRV 记录:服务器资源记录，作用是说明一个服务器能够提供什么样的服务

PTR 记录:也被称为指针记录，作用是把 IP 地址解析为域名。

●网络开发过程包括需求分析、通信规范分析、逻辑网络设计、物理网络设计、安装和维护等五个阶段。以下关于网络开发过程的叙述中，正确的是( )

- (35) A. 需求分析阶段应尽量明确定义用户需求，输出需求规范、通信规范  
B. 逻辑网络设计阶段设计人员一般更加关注于网络层的连接图  
C. 物理网络设计阶段要输出网络物理结构图、布线方案、IP 地址方案等  
D. 安装和维护阶段要确定设备和部件清单、安装测试计划，进行安装调试

解析：B

●某高校欲重新构建高校选课系统，配备多台服务器部署选课系统，以应对选课高峰期的大规模并发访问。根据需求，公司给出如下 2 套方案：

方案一：

- (1)配置负载均衡设备，根据访问量实现多台服务器间的负载均衡；
- (2)数据库服务器采用高可用性集群系统，使用 SQL Server 数据库，采用单活工作模式。

方案二：

- (1)通过软件方式实现支持负载均衡的网络地址转换，根据对各个内部服务器的 CPU、磁盘 I/O 或网络 I/O 等多种资源的实时监控，将外部 IP 地址映射为多个内部 IP 地址；
- (2)数据库服务器采用高可用性集群系统，使用 Oracle 数据库，采用双活工作模式。对比方案一和方案二中的服务器负载均衡策略，下列描述中错误的是（ ）。

两个方案都采用了高可用性集群系统，对比单活和双活两种工作模式，下列描述中错误的是（ ）

- (36) A. 方案一中对外公开的 IP 地址是负载均衡设备的 IP 地址
- B. 方案二中对每次 TCP 连接请求动态使用一个内部 IP 地址进行响应
- C. 方案一可以保证各个内部服务器间的 CPU、IO 的负载均衡
- D. 方案二的负载均衡策略使得服务器的资源分配更加合理
- (37) A. 单活工作模式中一台服务器处于活跃状态，另外一台处于热备状态
- B. 单活工作模式下热备服务器不需要监控活跃服务器并实现数据同步
- C. 双活工作模式中两台服务器都处于活跃状态
- D. 数据库应用一级的高可用性集群可以实现单活或双活工作模式

解析：C B

配置负载均衡设备可以实现流量均衡分发。

●某高校实验室拥有一间 100 平方米的办公室，里面设置了 36 个工位，用于安置本实验室的 36 名研究生。根据该实验室当前项目情况，划分成了 3 个项目组，36 个工位也按照区域聚集原则划分出 3 个区域。该实验室采购了一台具有 VLAN 功能的两层交换机，用于搭建实验室有线局域网，实现三个项目组的网络隔离。初期考虑到项目组位置固定



且有一定的人员流动，搭建实验室局域网时宜采用的 VLAN 划分方法是( )

随着项目进展及人员流动加剧，项目组区域已经不再适合基于区域聚集原则进行划分，而且项目组长或负责人也需要能够同时加入到不同的 VLAN 中。此时宜采用的 VLAN 划分方法是( )。

在项目后期阶段，三个项目组需要进行联合调试，因此要实现三个 VLAN 间的互联互通。目前有两种方案：

方案一：采用独立路由器方式，保留两层交换机，增加一个路由器。

方案二：采用三层交换机方式，用带 VLAN 功能的三层交换机替换原来的两层交换机。

与方案一相比，下列叙述中不属于方案二优点的是( )

- (38) A. 基于端口 B. 基于 MAC 地址  
C. 基于网络地址 D. 基于 IP 组播
- (39) A. 基于端口 B. 基于 MAC 地址  
C. 基于网络地址 D. 基于 IP 组播
- (40) A. VLAN 间数据帧要被解封成 IP 包再进行传递  
B. 三层交换机具有路由功能，可以直接实现多个 VLAN 之间的通信  
C. 不需要对所有的 VLAN 数据包进行解封、重新封装操作  
D. 三层交换机实现 VLAN 间通信是局域网设计的常用方法

解析：A B C

注意看清题目先期时候使用的是二层交换机，后期换成了三层交换。

●用户 A 在 CA 申请了自己的数字证书 I，下面的描述中正确的( )。

- (41) A. 证书 I 中包含了 A 的私钥，CA 使用公钥对证书 I 进行了签名  
B. 证书 I 中包含了 A 的公钥，CA 使用私钥对证书 I 进行了签名  
C. 证书 I 中包含了 A 的私钥，CA 使用私钥对证书 I 进行了签名  
D. 证书 I 中包含了 A 的公钥，CA 使用公钥对证书 I 进行了签名

解析：B

在 x. 509 格式中，数字证书包括版本号、序列号(CA 下发的每个证书的序列号都是唯一的)、签名算法标识符、发行者名称、有效性、主体名称、主体的公开密钥信息、发行者唯一识别符、主体唯一识别符、扩充域、签名(即 CA 用自己的私钥对上述域进行数字签名的结果，即 CA 中心对用户证书的签名)在数字签名体系中，签发着使用私

钥签名，公钥验证签名。

●数字签名首先需要生成消息摘要，然后发送方用自己的私钥对报文摘要进行加密，接收方用发送方的公钥验证真伪。生成消息摘要的目的是( )，对摘要进行加密的目的是( )。

- (42) A. 防止窃听 B. 防止抵赖  
C. 防止篡改 D. 防止重放  
(43) A. 防止窃听 B. 防止抵赖  
C. 防止篡改 D. 防止重放

解析：C B

消息摘要能够验证消息的完整性

数值签名可以抗抵赖

●下面关于第三方认证服务说法中，正确的是( )。

- (44) A. Kerberos 采用单钥体制  
B. Kerberos 的中文全称是“公钥基础设施”  
C. Kerberos 认证服务中保存数字证书的服务器叫 CA  
D. Kerberos 认证服务中用户首先向 CA 申请初始票据

解析：A

●SSL 的子协议主要有记录协议、( )，其中( )用于产生会话状态的密码参数，协商加密算法及密钥等。

- (45) A. AH 协议和 ESP 协议 B. AH 协议和握手协议  
C. 警告协议和握手协议 D. 警告协议和 ESP 协议  
(46) A. AH 协议 B. 握手协议  
C. 警告协议 D. ESP 协议

解析：C B

SSL 的工作原理

握手协议 (Handshake protocol)

记录协议 (Record protocol)

警报协议 (Alert protocol)

●在进行 POE 链路预算时，已知光纤线路长 5km，下行衰减 0.3dB/km；热熔连接点 3 个，衰减 0.1dB/个；分光比 1:8；衰减 10.3dB；光纤长度冗余衰减 1dB。下行链路衰减的值是（ ）

- (47) A. 11.7 dB  
B. 13.1 dB  
C. 12.1  
D. 10.7

解析: B

下行链路衰减值=5 \*0.3+3\*0.1+10.3+1=13.1dB

●路由器收到包含如下属性的两条 BGP 路由，根据 BGP 选路规则，（ ）。

| Network       | NextHop  | MED | LocPrf | PrefVal | Path/Ogn |
|---------------|----------|-----|--------|---------|----------|
| M 192.168.1.0 | 10.1.1.1 | 30  | 0      |         | 100i     |
| N 192.168.1.0 | 10.1.1.2 | 20  | 0      |         | 100 200i |

- (48) A. 最优路由 M, 其 AS-Path 比 N 短  
B. 最优路由 N, 其 MED 比 M 小  
C. 最优路由随机确定  
D. local-preference 值为空, 无法比较

解析: A

按照顺序每一步都依次进行评估直到找到一条最佳路径为止。

1 WEIGHT 值最高的路径优先。WEIGHT 是 CISCO 专有的参数，且只对配置该参数的本地路由器有效，不能传递。缺省条件下，本地始发的路径具有相同的 WEIGHT 值（32768），所有其它的路径的 WEIGHT 值为 0。想让某条路由在自己的路由表中优先，妄图直接修改 weight 的话 就在 neighbour 加入一条 neighbour xxxx weight 100 那么这个邻居传过来的路由直接改了，这样就可以直接保证它的优先级。

2 LOCAL-PREF 值（本地优先级）。CISCO IOS 中，LOCAL-PREF 缺省值为 100。该属性只能在本 AS 内传递。事实上如果你要影响一条路由由本地路由器的选路，那么用 route-map 做 in 的策略，如果用 out 方向的策略，那么会影响本 AS 内部这个路由的 localpreference，导致做策略的那个路由器会成为优化的路径。

3 基于始发地 (origination) 评估路由, 路由器本地始发的路径优先。依次降低的优

优先级顺序是：default-originate(针对每个邻居配置)，default-information originate (针对每种地址簇配置)，network, redistribute, aggregate-address。

4 评估 AS-PATH 的长度，AS-PATH 列表最短的路径优先。但可以通过配置 bgp bestpath as-path ignore (隐藏命令) 来忽略这一步。

5 评估路由的 origin 属性，origin 属性值最低的路由优先。IGP: origin 值=0; EGP: origin 值=1; INCOMPLETE: origin 值=3

6 评估 MED。MED 值最小的路径胜出。该属性可以传递出 AS。缺省条件下，只有在两条路径的第一个 AS 相同的情况下才会进行比较。如果配置了：bgp always-compare-med，那么对于所有路径都将比较 MED，而不考虑它们是否来自于同一个 AS。

●在 Windows Server 2008 系统中，某共享文件夹的 NTFS 权限和共享文件权限设置的  
不一致，则对于访问该文件夹的用户而言，下列( )有效。

- (49) A. 共享文件夹权限  
B. 共享文件夹的 NTFS 权限  
C. 共享文件夹权限和共享文件夹的 NTFS 权限累加  
D. 共享文件夹权限和共享文件夹的 NTFS 权限中更小的权限

解析：D

选择最小权限

●光网络设备调测时，一旦发生光功率过高就容易导致烧毁光模块事故，符合规范要求的是( )

- ①调测时要严格按照调测指导书说明的受光功率要求进行调测  
②进行过载点测试时，达到国标即可，禁止超过国标 2 个 dB 以上，否则可能烧毁光模块  
③使用 OTDR 等能输出大功率光信号的仪器对光路进行测量时，要将通信设备与光路断开  
④不能采用将光纤连接器插松的方法来代替光衰减器

- (50) A. ①②③④ B. ②③④  
C. ①② D. ①②③



C. display ospf neighbor

D. display ip ospf neighbor

解析：B A

display ospf cumulative OSPF 的统计信息

display ospf spf-statistics 查看 OSPF 进程下路由计算的统计信息。

display ospf interface 显示 OSPF 的接口信息

display ospf peer 显示 OSPF 的邻居信息

display ospf lsdb 显示 OSPF 的 lsdb

display ospf routing 显示 OSPF 的路由信息

display ospf error 显示 OSPF 的错误信息

reset ospf process 重启 OSPF 进程

●一个完整的无线网络规划通常包括( )。

①规划目标定义及需求分析

②传播模型校正及无线网络的预规划

③站址初选与勘察

④无线网络的详细规划

(56) A. ①②③④

B. ④

C. ②③

D. ①③④

解析：A

●下面 RAID 级别中，数据冗余能力最弱的是( )

(57) A. RAID5

B. RAID1

C. RAID6

D. RAID0

解析：D

RAID 0 又称为 Stripe 或 Striping，它代表了所有 RAID 级别中最高存储性能。RAID 0 提高存储性能的原理是把连续的数据分散到多个磁盘上存取，这样，系统有数据请求就可以被多个磁盘并行的执行，每个磁盘执行属于它自己的那部分数据请求。这种数据上的并行操作可以充分利用总线的带宽，显著提高磁盘整体存取性能。RAID 0 并不是真正的 RAID 结构，没有数据冗余，没有数据校验的磁盘陈列。实现 RAID 0 至少需要两块

以上的硬盘，它将两块以上的硬盘合并成一块，数据连续地分割在每块盘上。

●在五阶段网络开发过程中，网络物理结构图和布线方案的确定是在( )阶段确定的。

- (58) A. 需求分析 B. 逻辑网络设计  
C. 物理网络设计 D. 通信规范设计

解析：C

●按照 IEEE 802.3 标准，不考虑帧同步的开销，以太帧的最大传输效率为( )。

- (59) A. 50% B. 87.5%  
C. 90.5% D. 98.8%

解析：D

以太网数据部分封装大小为 46-1500，而以太网最大帧长范围为 64-1518

所以最大传输效率为  $1500/1518=98.8$

●进行链路传输速率测试时，测试工具应在交换机发送端口产生( )线速流量。

- (60) A. 100% B. 80%  
C. 60% D. 50%

答案：A

进行链路传输速率测试时，测试工具应在交换机发送端口产生 100%线速流量

●下面描述中，属于工作区子系统区域范围的是( )。

- (61) A. 实现楼层设备之间的连接  
B. 接线间配线架到工作区信息插座  
C. 终端设备到信息插座的整个区域  
D. 接线间内各种交连设备之间的连接

解析：C

●下列测试指标中，属于光纤指标的是( )，仪器( )可在光纤的一端测得光纤的损耗。

- (62) A. 波长窗口参数 B. 线对间传播时延差  
C. 回波损耗 D. 近端串扰

- (63) A. 光功率计  
B. 稳定光源  
C. 电磁辐射测试笔  
D. 光时域反射仪

解析：A D

光时域反射仪（英文名称：optical time-domain reflectometer，OTDR）是通过对测量曲线的分析，了解光纤的均匀性、缺陷、断裂、接头耦合等若干性能的仪器。它根据光的后向散射与菲涅耳反向原理制作，利用光在光纤中传播时产生的后向散射光来获取衰减的信息，可用于测量光纤衰减、接头损耗、光纤故障点定位以及了解光纤沿长度的损耗分布情况等，是光缆施工、维护及监测中必不可少的工具。

● 以下关于光缆的弯曲半径的说法中不正确的是（ ）。

- (64) A. 光缆弯曲半径太小易折断光纤  
B. 光缆弯曲半径太小易发生光信号的泄露影响光信号的传输质量  
C. 施工完毕光缆余长的盘线半径应大于光缆半径的 15 倍以上  
D. 施工中光缆的弯折角度可以小于 90 度

解析：D

弯曲半径是曲率半径。通俗地说，是把曲线上一个极小的段用一段圆弧代替。这个圆的半径即为弯曲半径。动态弯曲半径是指光纤在运动中的弯曲半径一般是不得小于光缆外径的 20 倍。静态弯曲半径是光纤在静止时的弯曲半径一般是光缆外径的 15 倍。不能直接弯，可以打个圆圈再进行转弯。否则，第一信号衰减严重，第二光纤容易老化断裂。在出现折角时一定要小心，一般折角可以控制在 90-120 度。

● 网络管理员在日常巡检中，发现某交换机有个接口(电口)丢包频繁，下列处理方法中正确的是（ ）。

- ①检查连接线缆是否存在接触不良或外部损坏的情况  
②检查网线接口是否存在内部金属弹片凹陷或偏位  
③检查设备两端接口双工模式、速率、协商模式是否一致  
④检查交换机是否中病毒

- (65) A. ①②  
B. ③④  
C. ①②③  
D. ①②③④

解析：D



●网络管理员在对公司门户网站([www.onlineMall.com](http://www.onlineMall.com)) 巡检时,在访问日志中发现如下入侵记录:

2018-07-10 21:07:44 219.232.47.183 访问 www.onlineMall.com/manager/html/start?path=&lt;script&gt;alert(/scanner/)&lt;/script&gt;

该入侵为( )攻击,应配备( )设备进行防护。

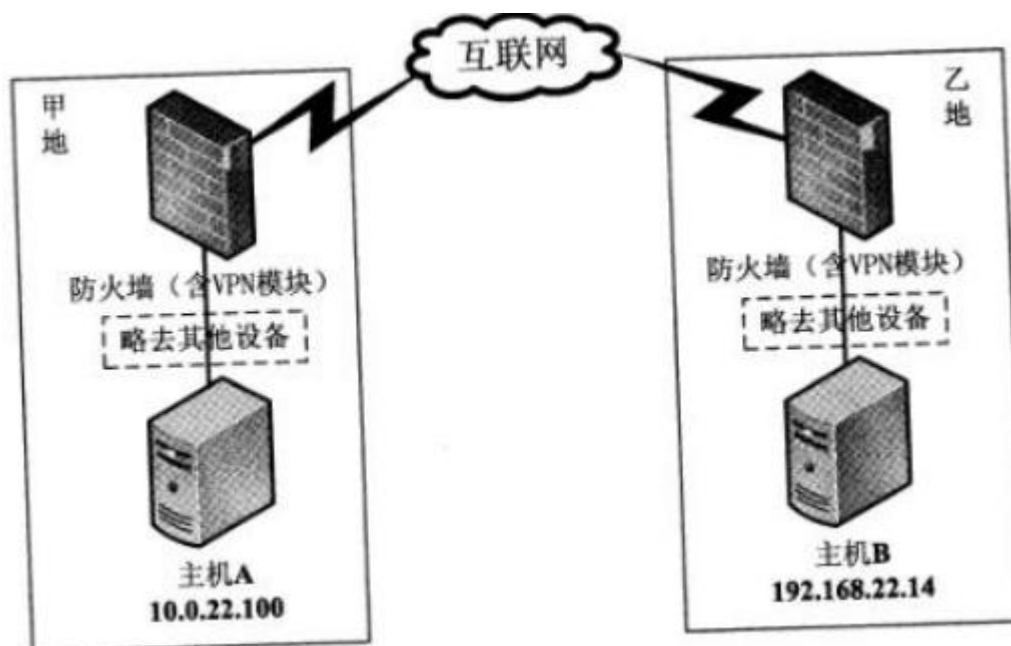
- (66) A. 远程命令执行 B. 跨站脚本 (XSS)  
C. SQL 注入 D. Http Heads
- (67) A. 数据库审计系统 B. 堡垒机  
C. 漏洞扫描系统 D. Web 应用防火墙

解析: B D

XSS 攻击全称跨站脚本攻击，是为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆，故将跨站脚本攻击缩写为 XSS，XSS 是一种在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中。

本文档由微信号:ruankaopass, 一手整理, 通过他人购买的, 拒绝售后。本人专业提供软考历年真题

●如下图所示，某公司甲、乙两地通过建立 IPsec VPN 隧道，实现主机 A 和主机 B 的互相访问，VPN 隧道协商成功后，甲乙两地访问互联网均正常，但从主机 A 到主机 B ping 不通，原因可能是（）、（）。



- (68) A. 甲乙两地存在网络链路故障  
 B. 甲乙两地防火墙未配置虚拟路由或者虚拟路由配置错误  
 C. 甲乙两地防火墙策略路由配置错误  
 D. 甲乙两地防火墙互联网接口配置错误
- (69) A. 甲乙两地防火墙未配置 NAT 转换  
 B. 甲乙两地防火墙未配置合理的访问控制策略  
 C. 甲乙两地防火墙的 VPN 配置中未使用野蛮模式  
 D. 甲乙两地防火墙 NAT 转换中未排除主机 A/B 的 IP 地址

解析：C B

●构件组装成软件系统的过程可以分为三个不同的层次( )

- (70) A. 初始化、互连和集成                      B. 连接、集成和演化  
 C. 定制、集成和扩展                              D. 集成、扩展和演化

解析：C

●Anytime a host or a router has an IP datagram to send to another host or router, it has the (71) address of the receiver. This address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router. But the IP datagram must

be (72) in a frame to be able to pass through the physical network. This means that the sender needs the (73) address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is (74) over the network. Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and physical addresses. The packet is (75) directly to the inquirer by using the physical address received in the query packet.

(71) A. port      B. hardware      C. physical      D. logical

(72) A. extracted B. encapsulated C. decapsulated D. decomposed

(73) A. local      B. network      C. physical      D. logical

(74) A. multicast B. unicast      C. broadcast      D. multiple unicast

(75) A. multicast B. unicast      C. broadcast      D. multiple unicast

解析：D B C C B

### 试题一

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

#### 【说明】

某园区组网方案如图 1-1 所示，数据规划如表 1-1 内容所示。

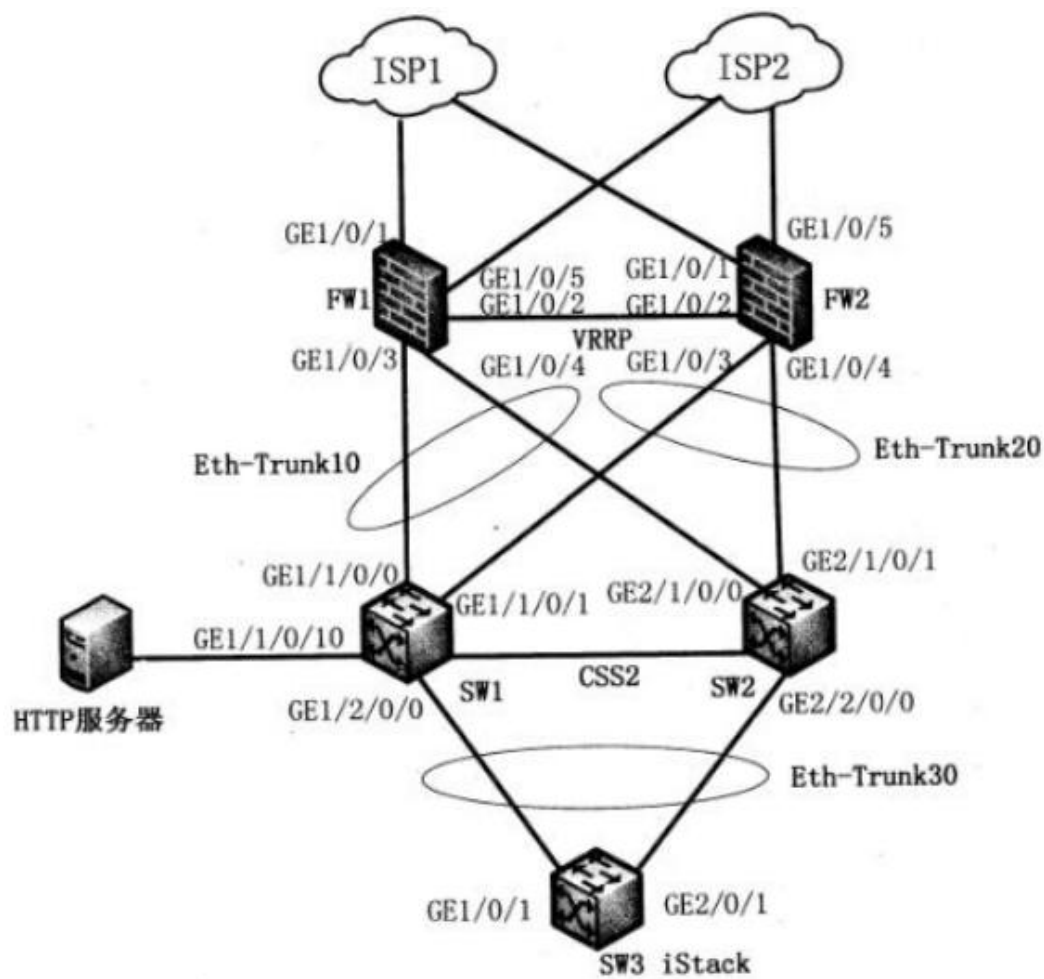


图 1-1

表 1-1

| 设备  | 接口          | 成员接口               | VLANIF | IP 地址           | 对端设备         | 对端接口        |
|-----|-------------|--------------------|--------|-----------------|--------------|-------------|
| FW1 | GE1/0/1     | -                  | -      | 202.1.1.1/24    | ISP1 外网出口 IP |             |
|     | GE1/0/5     | -                  | -      | 202.2.1.2/24    | ISP2 外网出口 IP |             |
|     | GE1/0/2     | -                  | -      | 172.16.111.1/24 | FW2          | GE1/0/2     |
|     | Eth-Trunk10 | GE1/0/3<br>GE1/0/4 | -      | 172.16.10.1/24  | SW CSS       | Eth-Trunk10 |
| FW2 | GE1/0/1     | -                  | -      | 202.1.1.2/24    | ISP1 外网出口 IP |             |
|     | GE1/0/5     | -                  | -      | 202.2.1.1/24    | ISP2 外网出口 IP |             |
|     | GE1/0/2     | -                  | -      | 172.16.111.2/24 | FW1          | GE1/0/2     |
|     | Eth-Trunk20 | GE1/0/3<br>GE1/0/4 | -      | 172.16.10.2/24  | SW CSS       | Eth-Trunk20 |

|        |             |           |          |                 |        |             |
|--------|-------------|-----------|----------|-----------------|--------|-------------|
| SW CSS | GE1/1/0/10  | -         | VLANIF50 | 172.16.50.1/24  | HTTP   | 以太网接口       |
|        | Eth-Trunk10 | GE1/1/0/0 | VLANIF10 | 172.16.10.3/24  | FW1    | Eth-Trunk10 |
|        |             | GE2/1/0/0 |          |                 |        |             |
|        | Eth-Trunk20 | GE1/1/0/1 | VLANIF10 | 172.16.10.3/24  | FW2    | Eth-Trunk20 |
|        |             | GE2/1/0/1 |          |                 |        |             |
|        | Eth-Trunk30 | GE1/2/0/0 | VLANIF30 | 172.16.30.1/24  | SW3    | Eth-Trunk30 |
|        |             | GE2/2/0/0 | VLANIF40 | 172.16.40.1/24  |        |             |
| SW3    | Eth-Trunk30 | GE1/0/1   | VLANIF30 | 172.16.30.2/24  | SW CSS | Eth-Trunk30 |
|        |             | GE2/0/1   |          |                 |        |             |
| HTTP   | 以太网接口       | -         | -        | 172.16.50.10/24 | SW CSS | GE1/1/0/10  |

### 【问题1】(8分)

该网络对汇聚层交换机进行了堆叠，在此基础上进行链路聚合并配置接口，补充下列命令片段。

```
[SW3] interface (1)
[SW3-Eth-Trunk30] quit
[SW3] interface gigabitethernet 1/0/1
[SW3-GigabitEthernet1/0/1] eth-trunk 30
[SW3-GigabitEthernet1/0/1] quit
[SW3] interface gigabitethernet 2/0/1
[SW3-GigabitEthernet2/0/1] eth-trunk 30
[SW3-GigabitEthernet2/0/1] quit
[SW3] vlan batch (2)
[SW3] interface eth-trunk 30
[SW3-Eth-Trunk30] port link-type (3)
[SW3-Eth-Trunk30] port trunk allow-pass vlan 30 40
[SW3-Eth-Trunk30] quit
[SW3] interface vlanif 30
[SW3-Vlanif30] ip address (4)
[SW3-Vlanif30] quit
```

解析：

(1) eth-trunk 30

(2) 30 40

(30) Trunk

(4) 172.16.30.2 24

**【问题2】(8分)**

该网络对核心层交换机进行了集群，在此基础上进行链路聚合并配置接口，补充下列命令片段。

```
[CSS] interface loopback 0
```

```
[CSS-LoopBack0] ip address 3.3.3.3 32
```

```
[CSS-LoopBack0] quit
```

```
[CSSs] vlan batch 10 30 40 50
```

```
[CSS] interface eth-trunk 10
```

```
[CSS-Eth-Trunk10] port link-type access
```

```
[CSS- Eth-Trunk10] port default vlan 10
```

```
[CSS- Eth-Trunk10] quit
```

```
[CSS] interface eth-trunk 20
```

```
[CSS-Eth-Trunk20] port link-type (5)
```

```
[CSS- Eth-Trunk20] port default vlan 20
```

```
[CSS-Eth-Trunk20] quit
```

```
[CSS] interface eth-trunk 30
```

```
[CSS- Eth-Trunk30] port link-type (6)
```

```
[CSS-Eth-Trunk30] port trunk allow-pass vlan 30 40
```

```
[CSS-Eth-Trunk30] quit
```

```
[CSS] interface vlanif 10
```

```
[CSS-Vlanif10] ip address 172.16.10.3 24
```

```
[CSS-Vlanif10] quit
```

```
[CSS] interface vlanif 30
```

```
[CSS-Vlanif30] ip address 172.16.30.1 24
```

```
[CSS-Vlanif30] quit
```

```
[CSS] interface vlanif 40
```

```
[CSS-Vlanif40] ip address (7)
[CSS-Vlanif40] quit
[CSS] interface gigabitethernet 1/1/0/10
[CSS-GigabitEthernet1/1/0/10] port link-type access
[CSS-GigabitEthernet1/1/0/10] port default vlan 50
[CSS-GigabitEthernet1/1/0/10] quit
[CSS] interface vlanif 50
[CSS-Vlanif50] ip address (8)
[CSS-Vlanif50] quit
```

解析：

- (5) access
- (6) trunk
- (7) 172.16.40.1 24
- (8) 172.16.50.1 24

### 【问题 3】(3 分)

配置 FW1 时，下列命令片段的作用是 (9) 。

```
[FW1] interface eth-trunk 10
[FW1-Eth-Trunk10] quit
[FW1] interface gigabitethernet 1/0/3
[FW1-GigabitEthernet1/0/3] eth-trunk 10
[FW1-GigabitEthernet1/0/3] quit
[FW1] interface gigabitethernet 1/0/4
[FW1-GigabitEthernet1/0/4] eth-trunk 10
[FW1-GigabitEthernet1/0/4] quit
```

解析：把 gigabitethernet 1/0/3 和 gigabitethernet 1/0/4 加入 eth-trunk 10 逻辑端口中。

### 【问题 4】(6 分)

在该网络以防火墙作为出口网关的部署方式，相比用路由器作为出口网关，防火墙旁挂的部署方式，最主要的区别在于 (10) 。



为了使内网用户访问外网，在出口防火墙上配置（11），实现私网地址和公网地址之间的转换；在出口防火墙上配置（12），实现外网用户访问 HTTP 服务器。

解析：（10）可以在防火墙上配置相关安全策略，对进出的网络流量进行检测，根据策略要求放行、阻断相关流量。（11）NAT （12）NAT Server

## 试题二

阅读下列说明，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

### 【说明】

图 2-1 为某台服务器的 RAID (Redundant Array of Independent Disk, 独立冗余磁盘阵列) 示意图，一般进行 RAID 配置时会根据业务需求设置相应的 RAID 条带深度和大小，本服务器由 4 块磁盘组成，其中 P 表示校验段、D 表示数据段，每个数据块为 4KB，每个条带在一个磁盘上的数据段包括 4 个数据块。

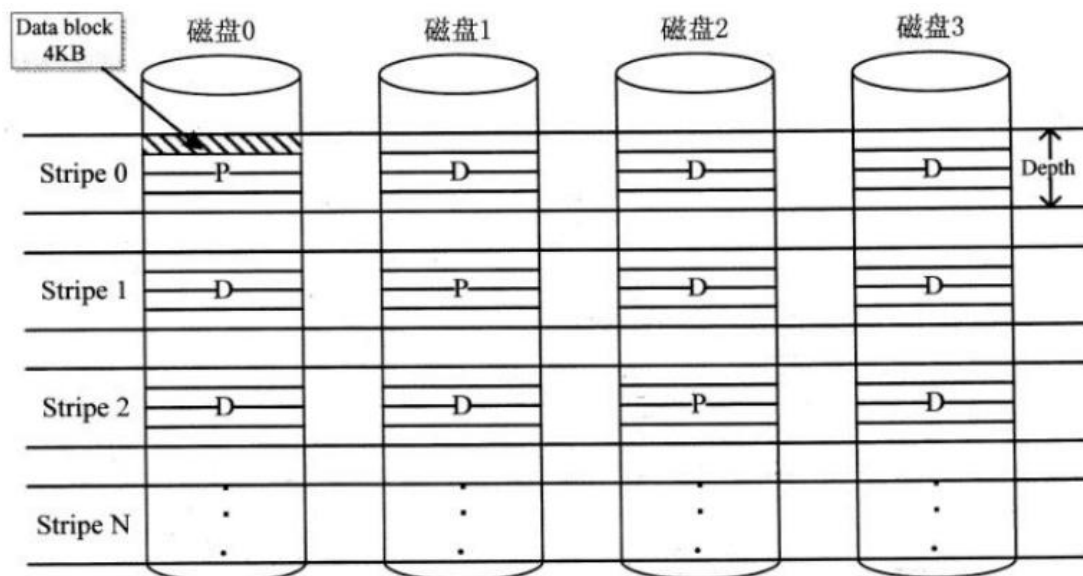


图 2-1

### 【问题 1】(6 分)

图 2-1 所示的 RAID 方式是(1) ， 该 RAID 最多允许坏(2) 块磁盘而数据不丢失，通过增加(3) 盘可以减小磁盘故障对数据安全的影响。

解析：

(1) RAID5

(2) 1

(3) 热备盘

raid5+1 个磁盘做热备盘，Raid5 如果坏了 1 个盘，马上就能有个热备盘自动同步数据热备盘就会顶替 Raid 里的那个坏盘，同时利用异或校验算法，把坏盘上面的数据原样做出来并存储在热备盘中。

这样一来就等于 Raid 没受到损坏，然后再找个一个同样的盘把坏盘替换掉，Raid 和热备盘的状态又正常了！

**【问题 2】（5 分）**

1. 图 2-1 所示，RAID 的条带深度是(4) KB，大小是 (5) KB。
2. 简述该 RAID 方式的条带深度大小对性能的影响。

解析：

1、(4) 16 (5) 4

条带深度：指的是条带的大小，也叫条带大小。有时也被叫做 block size, chunk size, stripe length 或者 granularity。这个参数指的是写在每块磁盘上的条带数据块的大小。

2、减小条带大小：由于条带大小减小了，则文件被分成了更多个，更小的数据块。这些数据块会被分散到更多的硬盘上存储，因此提高了传输的性能，但是由于要多次寻找不同的数据块，磁盘定位的性能就下降了。增加条带大小：与减小条带大小相反，会降低传输性能，提高定位性能。

**【问题 3】（7 分）**

图 2-1 所示的 RAID 方式最多可以并发 (6) 个 IO 写操作，通过 (7) 措施可以提高最大并发数，其原因是 (8) 。

解析： (6) 2 (7) 增加条带宽度 (8) 条带宽度：是指同时可以并发读或写的条带数量。这个数量等于 RAID 中的物理硬盘数量。例如一个经过条带化的，具有 4 块物理硬盘的阵列的条带宽度就是 4。增加条带宽度，可以增加阵列的读写性能。道理很明显，增加更多的硬盘，也就增加了可以同时并发读或写的条带数量。在其他条件一样的前提下，一个由 8 块 18G 硬盘组成的阵列相比一个由 4 块 36G 硬盘组成的阵列具有更高的传输性能。

**【问题 4】（7 分）**

某天，管理员发现该服务器的磁盘 0 故障报警，管理员立即采取相应措施进行处理。

1. 管理员应采取什么措施？
2. 假设磁盘 0 被分配了 80%的空间，则在 RAID 重构时，未被分配的 20%空间是否参与重构？请说明原因。

解析：

- 1、立即更换同型号，同容量的硬盘。
- 2、未分配的 20%空间不参与重构

### 试题三

阅读下列说明，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

#### 【说明】

图 3-1 为某公司拟建数据中心的简要拓扑图，该数据中心安全规划设计要求符合信息安全等级保护(三级)相关要求。

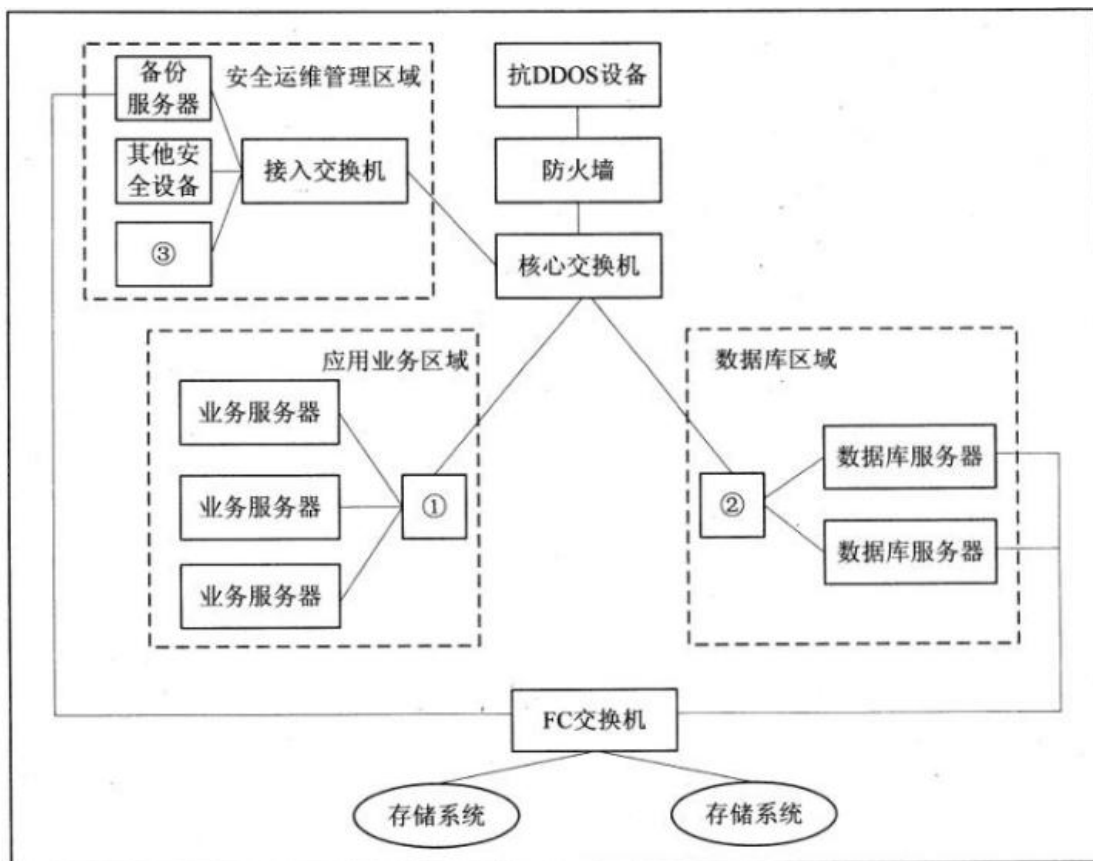


图 3-1

#### 【问题 1】(9 分)

1. 在信息安全规划和设计时，一般通过划分安全域实现业务的正常运行和安全的有  
效保障，结合该公司实际情况，数据中心应该合理地划分为 (1)、(2)、(3) 三个安全域。

2. 为了实现不同区域的边界防范和隔离，在图 3-1 的设备①处应部署 (4) 设备，  
通过基于 HTTP/HTTPS 的安全策略进行网站等 Web 应用防护，对攻击进行检测和阻  
断；在设备②处应部署 (5) 设备，通过有效的访问控制策略，对数据库区域进行安全  
防护；在设备③处应部署 (6) 设备，定期对数据中心内服务器等关键设备 进行扫  
描，及时发现安全漏洞和威胁，可供修复和完善。

解析：

- (1) 运维管理安全域
- (2) 应用业务安全域
- (3) 数据、存储安全域
- (4) WAF
- (5) 数据库防火墙
- (6) 漏洞扫描设备

**【问题 2】(6 分)**

信息安全管理一般从安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面进行安全管理规划和建设。其中应急预案制定和演练、安全事件处理属于 (7) 方面；人员录用、安全教育和培训属于 (8) 方面；制定信息安全方针与策略和日常操作规程属于 (9) 方面；设立信息安全工作领导小组，明确安全管理职能部门的职责和分工属于 (10) 方面。

解析：

- (7) 系统运维管理
- (8) 人员安全管理
- (9) 安全管理制度
- (10) 安全管理机构

**【问题 3】(4 分)**

随着 DDoS (Distributed Denial of Service, 分布式拒绝服务) 攻击的技术门槛越来越低，使其成为网络安全中最常见、最难防御的攻击之一，其主要目的是让攻击目标无法提供正常服务。请列举常用的 DDoS 攻击防范方法。

解析：

DDoS 攻击防御方法

1. 过滤不必要的服务和端口：可以使用 Inexpress、Express、Forwarding 等工具来过滤不必要的服务和端口，即在路由器上过滤假 IP。比如 Cisco 公司的 CEF (Cisco Express Forwarding) 可以针对封包 Source IP 和 Routing Table 做比较，并加以过滤。只开放服务

端口成为目前很多服务器的流行做法，例如 WWW 服务器那么只开放 80 而将其其他所有端口关闭或在防火墙上做阻止策略。

2. 异常流量的清洗过滤：通过 DDOS 硬件防火墙对异常流量的清洗过滤，通过数据包的规则过滤、数据流指纹检测过滤、及数据包内容定制过滤等顶尖技术能准确判断外来访问流量是否正常，进一步将异常流量禁止过滤。单台负载每秒可防御 800-927 万个 syn 攻击包。

本文档由微信号:ruankaopass，一手整理，通过他人购买的，拒绝售后。本人专业提供软考历年真题

3. 分布式集群防御：这是目前网络安全界防御大规模 DDOS 攻击的最有效办法。分布式集群防御的特点是在每个节点服务器配置多个 IP 地址（负载均衡），并且每个节点能承受不低于 10G 的 DDOS 攻击，如一个节点受攻击无法提供服务，系统将会根据优先级设置自动切换另一个节点，并将攻击者的数据包全部返回发送点，使攻击源成为瘫痪状态，从更为深度的安全防护角度去影响企业的安全执行决策。

4. 高防智能 DNS 解析：高智能 DNS 解析系统与 DDOS 防御系统的完美结合，为企业提供对抗新兴安全威胁的超级检测功能。它颠覆了传统一个域名对应一个镜像的做法，智能根据用户的上网路线将 DNS 解析请求解析到用户所属网络的服务器。同时智能 DNS 解析系统还有宕机检测功能，随时可将瘫痪的服务器 IP 智能更换成正常服务器 IP，为企业的网络保持一个永不宕机的服务状态。

#### DDoS 攻击的网络流量清洗

当发生 DDOS 攻击时，网络监控系统会侦测到网络流量的异常变化并发出报警。在系统自动检测或人工判断之后，可以识别出被攻击的虚拟机公网 IP 地址。这时，可调用系统的防 DDOS 攻击功能接口，启动对相关被攻击 IP 的流量清洗。流量清洗设备会立即接管对该 IP 地址的所有数据包，并将攻击数据包清洗掉，仅将正常的数据包转发给随后的网络设备。这样，就能保证整个网络正常的流量通行，而将 DDOS 流量拒之门外。采用云 DDoS 清洗方式，可以为企业用户带来诸多好处。其表现在不仅可以提升综合防护能力，用户能够按需付费，可弹性扩展，而且还能够基于大数据来分析预测攻击，同时能够免费升级。对于企业用户来说，则可实现零运维、零改造。

**【问题 4】（6 分）**

随着计算机相关技术的快速发展，简要说明未来十年网络安全的主要应用方向。

解析：（1）云安全、大数据安全 （2）物联网安全 （3）区块链安全 （4）人工智能安全  
（5）国家关键基础设施安全 （6）生物识别技术及应用安全 （7）关键技术本土化、安全自主可控（芯片、操作系统、国产设备、 国产密码等等）

【软考达人】

# 软考资料免费获取

- 1、最新软考题库
- 2、软考备考资料
- 3、考前压轴题
- 4、免费督考群



**微信扫一扫，立马获取**



**最新免费题库**



**备考资料+督考群**

PC版题库：[ruankaodaren.com](http://ruankaodaren.com)