

2020 年 11 月网络工程师上午真题试卷及答案

1.关系型数据库采用（1）解决数据并发引起的冲突[1 分]

- A.锁机制
- B.索引
- C.分区表
- D.读写分离

参考答案：A

解析：

数据库锁机制一般可以分为两类，一个是悲观锁，一个是乐观锁。用以解决数据并发冲突，简单的来悲观锁：顾名思义，就是很悲观，每次去拿数据的时候都认为别人会修改，所以每次在拿数据的时候都会上锁，这样别人想拿这个数据就会 block 直到它拿到锁。传统的关系型数据库里边就用到了很多这种锁机制，比如行锁，表锁等，读锁，写锁等，都是在做操作之前先上锁乐观锁：顾名思义，就是很乐观，每次去拿数据的时候都认为别人不会修改，所以不会上锁，但是在更新的时候会判断一下在此期间别人有没有去更新这个数据，可以使用版本号等机制。乐观锁适用于多读的应用类型，这样可以提高吞吐量。

2.把模块按照系统设计说明书的要求组合起来进行测试，属于（2）[1 分]

- A.单元测试
- B.集成测试
- C.确认测试
- D.系统测试

参考答案：B

解析：

集成测试，也叫组装测试或联合测试。在单元测试的基础上，将所有模块按照设计要求（如根据结构图）组装成为子系统或系统，进行集成测试。检验各部分工作是否达到或实现相应技术指标及要求的活动

3.虚拟存储体系由（3）两级存储器构成。[1 分]

- A.主存-辅存
- B.寄存器-Cache
- C.寄存器-主存
- D.Cache-主存

参考答案：A

解析：

虚拟存储器是一个容量非常大的存储器的逻辑模型，不是任何实际的物理存储器。它借助于磁盘等辅助存储器来扩大主存容量，使之能为更大或更多的程序所使用。

虚拟存储器是为了给用户提供更人的随机存储空间而采用的一种存储技术。它将内存和外存结合使用，速度接近于主存，成本与辅存相近。所以虚拟存储器由主存和辅存组成

4.下列操作系统中，不是基于 linux 内核的是（4） [1 分]

A.AIX

B.Centos

C.红旗

D.中标麒麟

参考答案：A

解析：

Centos（Community Enterprise Operating System，社区企业操作系统）是 Linux 发行版之一，它是来自于 Red Hat Enterprise Linux 依照开放源代码规定释出的源代码所编译而成。两者的不同，在于 Centos 完全开源红旗和中标麒麟是国产操作系统，均是基于 Linux 内核开发的适合国内用户使用的操作系统，有桌面版、服务器版等版本而 AIX，是 IBM 专有 UNIX 操作系统的商标名。名称来自先进交互运行系统（英语：Advance Interactive eXecutive，缩写为）。是 IBM 基于 AT&T Unix System V 开发的一套类 UNIX 操作系统，运行在 IBM 专有的 Power 系列芯片设计的小型机硬件系统之上

5.8086 微处理器中执行单元负责指令的执行，它主要包括（5）。 [1 分]

A.AL 运算器、输入输出控制电路、状态寄存器

B.AU 运算器、通用寄存器、状态寄存器

C.通用寄存器、输入输出控制电路、状态寄存器

D.ALU 运算器、输入输出控制电路、通用寄存器的

参考答案：B

解析：

8086 微处理器由两个部分即指令执行部件（E）和总线接口部件（BIU）组成。指令执行部件由算术逻辑运算单元（ALU）、标志寄存器（FLAGS）、通用寄存器组和 EU 控制器 4 个部件组成，其主要功能是执行指令

6.使用白盒测试时，确定测试数据应根据（6）指定覆盖准则。 [1 分]

A.程序的内部逻辑

B.程序的复杂程度

C.使用说明书

D.程序的功能

参考答案：A

解析：

白盒测试又称结构测试、透明盒测试、逻辑驱动测试或基于代码的测试。白盒指的是盒子是可视的，像白天看盒子内部一样，即清楚盒子内部的东西以及里面是如何运作的。“白盒”法全面了解程序内部逻辑结构、对所有逻辑路径进行测试

7.以下关于 RISC 指令系统基本概念的描述中，错误的是（7） [1 分]

- A.选取使用频率低的一些复杂指令，指令条数多
- B.指令长度固定
- C.指令功能简单
- D.指令运行速度快

参考答案：A

解析：

精简指令集 RISC：指令格式固定统一、种类比较少、寻址方式简单，处理速度大大提高。目前在中高档服务器中普遍采用这一指令系统的 CPU，特别是高档服务器全都采用 RISC 指令系统的 CPU

8.计算机上采用的 SSD（固态硬盘）实质上是（8）存储器。 [1 分]

- A.Flash
- B.磁盘
- C.磁带
- D.光盘

参考答案：A

解析：

固态驱动器简称 SSD，俗称固态硬盘，是用固态电子存储芯片阵列制成的硬盘。SSD 由控制单元和存储单元（FLASH 芯片、DRAM 芯片）组成。

固态硬盘在接口的规范和定义、功能及使用方法上与普通硬盘的完全相同，在产品外形和尺寸上基本与普通硬盘一致（但新兴的 S 采用 U.2，M .2 等形式的固态硬盘尺寸和外形与 SATA 机械硬盘完全不

9.信息安全强调信息数据本身的安全属性，下面（9）不属于信息安全的属性 [1 分]

- A.信息的秘密性
- B.信息的完整性
- C.信息的可用性
- D.信息的实时性

参考答案：D

解析：

信息安全的基本属性主要有三个方面，也称为三要素 1、保密性，也称秘密性、机密性，保证信息为授权者享用回而不泄漏给未经授答权者。

2、完整性，保证信息从真实的发信者传送到真实的收信者手中，传送过程中没有被非法用户添加、删除、替换等。

3、可用性，保证信息和信息系统随时为授权者提供服务，保证合法用户对信息和资源的使用不会被不合理的拒绝

10.我国由（10）主管全国软件著作权登记管理工作。[1 分]

A.国家版权局

B.国家新闻出版署

C.国家知识产权局

D.地方知识产权局

参考答案：A

解析：

国家版权局主管全国软件著作权登记管理工作，国家版权局认定中国版权保护中心为软件登记机构，经国家版权局批准，中国版权保护中心可以在地方设立软件登记办事机构

11.8 条模拟信道采用 TM 复用成 1 条数字信道，T 额的结构为 8 字节加 1 比特同步开销（每条模拟信道占 1 个字节），若模拟信号频率范围为 1016kHz，样本串至少为（11）样本/秒，此时数字信道的数据速率为（12）M bps[1 分]

A.8k

B.10k

C.20K

D.32K

参考答案：D

解析：

采样频率大于等于最大频率的 2 倍。即采样率为 16kHz 的 2 倍是 32k。

12.8 条模拟信道采用 TM 复用成 1 条数字信道，T 额的结构为 8 字节加 1 比特同步开销（每条模拟信道占 1 个字节），若模拟信号频率范围为 1016kHz，样本串至少为（11）样本/秒，此时数字信道的数据速率为（12）M bps[1 分]

A.0.52

B.0.65

C.1.30

D.2.08

参考答案: D

解析:

数字信道包含 8 个模拟信道（每条模拟信道占 1 个字节），8 字节（1 字节=8 比特）正好为 8 个模拟信道则共有比特（位）为：（8*8+1）位/帧最大传输速率即数据速率=位数/帧×采样频率=（1+8×8）×32k=2080Kbps=2.08M bps。

13.在异步传输中，1 位起始位，7 位数据位，2 位停止位，1 位校验位，每秒传输 200 字符，采用曼彻斯特编码，有效数据速率是（13）kb/s，最大波特率为（14）Baud [1 分]

A.1.2

B.1.4

C.2.2

D.2.4

参考答案: B

解析:

每秒传 200 字符，每个字符中只有 7 位数据位为有效位，那么每秒传送 200*7=1400bit，即有效数据速率为 1.4kb/s

14.在异步传输中，1 位起始位，7 位数据位，2 位停止位，1 位校验位，每秒传输 200 字符，采用曼彻斯特编码，有效数据速率是（13）kb/s，最大波特率为（14）Baud [1 分]

A.700

B.2200

C.1400

D.4400

参考答案: D

解析:

每秒传 200 字符，每个字符有 1+7+2+1=11 位，那么每秒传 200*11=2200bit，数据速率为 2200b/s 在采用曼切斯特编码方式的数字通信中，传输 1 个比特需要发送 2 个码元，波特率是数据速率的 2 倍。

以其码元速率为 2200*2=4400Baud

15.在卫星通信中，通常采用的差错控制机制为（15） [1 分]

A.停等 ARQ

B.后退 N 帧 ARQ

C.选择重发 ARQ

D.最大限额 ARQ

参考答案: C

解析：

在卫星 ATM 宽带网络中，差错控制主要有三种方法，分别是选择性重发协议（SRQ）、前向差错控制

（FEC）、多站分集的自动反馈重发其中，选择性重发协议：在长时延的卫星链路上进行差错控制，为了提高吞吐量，必然要使用滑动窗口协议。在滑动窗口协议中，处理出错帧有 2 种方法：后退协议和 SRQ 协议 SRQ 协议主要优点是只重传出错的帧，这可节省卫星链路的带宽，效率较高；缺点是实现较复杂并且对内存敏感。在差错率较高的情况下，这需要占用较大的内存来存储后续正确的帧。

16.以下千兆以太网标准中，支持 1000m 以上传输距离的是（16）[1 分]

- A.1000BASE-T
- B.1000BASE-CX
- C.1000BASE-SX
- D.1000BASE-LX

参考答案：D

解析：

1000BASE-T，使用双绞线，最大传输距离 100m

1000BASE-CX，使用屏蔽铜线，最大传输距离 25m
1000BASE-Sx，使用多模光纤，最大传输距离 550m

1000BASE-LX，使用单模光纤，最大传输距离 5000m

17.综合布线系统中，用于连接各层配线室，并连接主配线室的子系统为（17）[1 分]

- A.工作区子系统
- B.水平子系统
- C.垂直子系统
- D.管理子系统

参考答案：C

解析：

垂直干线子系统：作用是通过骨干线缆将主设备间与各楼层配线间体系联接起来，由设备间的配线设备和跳线以及设备间至各楼层配线间的联接电缆构成，由于其通常是顺着大楼的弱电井垂直而下，因此也称为垂直子系统

18.光纤传输测试指标中，回波损耗是指（18）[1 分]

- A.信号反射引起的衰减
- B.传输距离引起的发射端的能量与接收端的能量差
- C.光信号通过活动连接器之后功率的减少

D.传输数据时线对间信号的相互泄漏

参考答案：A

解析：

回波损耗：也叫反射损耗，一般指接头连接的反射损耗，一般要求大于 40dB 串扰：是指线缆传输数据时线对间信号的相互泄漏。串扰一般只有铜缆存在，如双绞线。

插入损耗：是指光纤中的光信号通过活动连接器之后，其输出光功率相对输入光功率的分贝数衰减损耗：指的是整条光纤链路能够正常工作的情况下，光信号发射端的能量与接收端的能量差

19.以 10/s 以太网连接的站点 A 和 B 相隔 2000，通过停等机制进行数据传输，传播速率为 200m /us，有效的传输速率为（19）M bs[1 分]

A.50.8

B.82.9

C.90.1

D.92.3

参考答案：D

解析：

以太网帧大小为 1518 字节，有效数据为 1500 字节，一个帧的发送时延为 $(1500 \times 8) / 100 = 120$ （单位 us），传播时延为 $2000 / 200 = 10$ us，其有效的传输速率为：有效总比特 / 总时间 = $(1500 \times 8) / (120 + 10) \approx 92.3$ （单位 M bps）。

20.采用 ADSL 接入互联网，计算机需要通过（20）和分离器连接到电话入户接线盒。在 HFC 网络中，用户通过（21）接入 CATV 网络[1 分]

A.ADSL 交换机

B.Cable M odem

C.ADSL M odem

D.无线路由器

参考答案：C

解析：

非对称数字用户线路 ADSL，允许用户在传统的电话线上提供高速的数据传输，用户计算机借助于 ADSL 调制解调器连接到电话线上，通过 ADSL 连接访问因特网络或者企业网络。

它提供高达 8M ps 的下行速度和 1M bps 的上行速度。ADSL2 可以达到 12M bps，上行速度仍然是 1

M bDs.ADSL2+，它使用双绞线上的双倍带宽（2.2M Hz）把下行速度翻了一倍，达到 24M bps

21.采用 ADSL 接入互联网，计算机需要通过（20）和分离器连接到电话入户接线盒。在 HFC 网络中，用户通过（21）接入 CATV 网络[1 分]

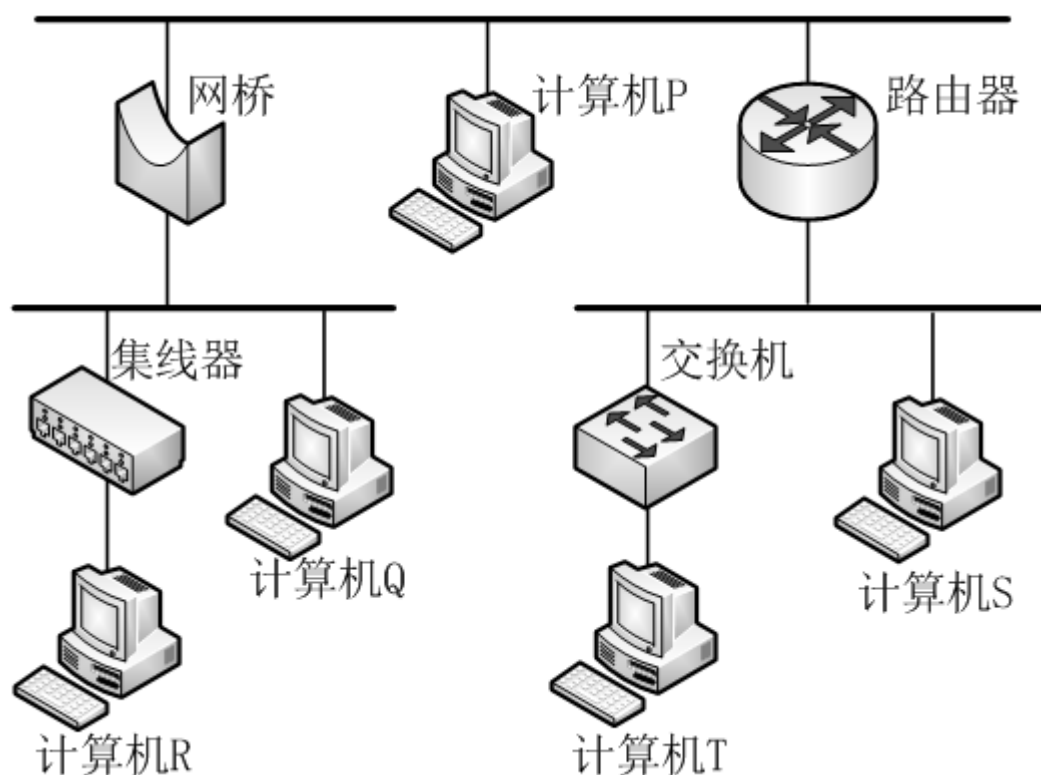
- A.ADSL 交换机
- B.Cable modem
- C.ADSL Modem
- D.无线路由器

参考答案：B

解析：

HFC 是光纤同轴电缆混合网，营运商通过光纤把网络信号送到小区，在小区内通过有线电视（CATV）使用的同轴电缆入户。用户端按装 Cable modem 线缆调制解调器，把网络信号解调出来供上网用典型的 CATV 网络系统提供 25~50Mbps 的下行带宽和 2~3Mbps 的上行带宽

22.某 IP 网络连接如下图所示，下列说法中正确的是（22）



[1 分]

- A.共有 2 个冲突域
- B.共有 2 个广播域
- C.计算机 5 和计算机 T 构成冲突域
- D.计算机 Q 查找计算机 R 的 MAC 地址时，ARP 报文会传播到计算机 5

参考答案：B

解析：

路由器一个端口一个广播域，一个端口一个冲突域交换机所有端口一个广播域，一个端口一个冲突域集线器所有端口一个广播域，所有端口一个冲突域从图中看出路由器上下两个端口构成了2个广播域是对的。并且会分割广播域

23.采用 HLC 协议进行数据传输时，F5 表明（23）[1 分]

- A.拒绝编号为 5 的帧
- B.下一个接收的帧编号应为 5，但接收器未准备好，暂停接收
- C.后退锁重传编号为 5 的帧
- D.选择性拒绝编号为 5 的帧

参考答案：B

解析：

00——接收就绪（RR），由主站或从站发送。主站可以使用 R 型 S 帧来轮询从站，即希望从站传输编号为 N（R）的帧，若存在这样的帧，便进行传输；从站也可用 R 型 S 帧来作响应，表示从站希望从主站那里接收的下一个帧的编号是 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，并暗示它编号的帧已全部确

24.若主机采用以太网接入 Internet,TCP 段格式中，数据字段最大长度为（24）字节[1 分]

- A.20
- B.1460
- C.1500
- D.65535

参考答案：B

解析：

以太网最大帧长为 1518 字节，有效数据部分（MTU）最大长度为 1500 字节（18 字节的控制信息）。去除 20 字节 IP 包头，20 字节 TCP 包头，剩余 TCP 中数据部分 1460 字节。

25.TCP 采用拥塞窗口（cwnd）进行拥塞控制。以下关于 cwnd 的说法中正确的是（25）[1 分]

- A.首部中的窗口段存放 cwnd 的值
- B.每个段包含的数据只要不超过 cwnd 值就可以发送了

C.cwnd 值由对方指定

D.cwnd 值存放在本地

参考答案: D

解析:

拥塞窗口 (cwnd): TCP 拥塞控制措施, 发送方维持一个 (congestion window) 的状态变量。拥塞窗口大小取决于网络的拥塞程度, 并且动态地在变化, 发送方让自己的发送窗口等于拥塞, 所以拥塞窗口 cwnd 存在于发送方本地

26.UDP 头部的大小为 (26) 字节。[1 分]

A.8

B.16

C.20

D.32

参考答案: A

解析:

UDP 协议分为首部字段和数据字段, 其中首部字段只占用 8 个字节, 分别是源端口、目的端口、长度和检验和, 共 8 个字节

27.为了控制 IP 数据报在网络中无限转发, 在 IPv4 数据报首部中设置了 (2) 字段[1 分]

A.标识符

B.首部长度

C.生存期

D.总长度

参考答案: C

解析:

生存期: TTL, 占 8 位, 表示数据报在网络中的寿命。由发送数据报的源点设置这个字段, 其目的是为了防止那些无法交付的数据报无限制的在互联网中兜圈子。数据报每经过一个路由器, 这个值就会减 1, 当减至 0 时, 就丢弃该数据报, 防止产生环路。

28.Telnet 是用于远程访问服务器的常用协议, 下列关于 Telnet 的描述中, 不正确的 (28) [1 分]

A.可传输数据和口令

B.默认端口号是 23

C.一种安全的通信协议

D.用 TP 作为传输层协议

参考答案: C

解析：

Telnet 远程登录协议：TCP/IP 终端仿真协议，登录到远程主机上操作，采用 TCP 的 23 端口，C/S 工作。

传输过程是明文的、不安全的，因此选项 C 是不正确的

29.Cookie 为客户端持久保持数据提供了方便，但也存在一定的弊端，下列选项中，不属于 Cookie 弊端的是（29） [1 分]

- A.增加流量消耗
- B.明文传输，存在安全性隐患
- C.存在敏感信息泄露风险
- D.保存访问站点的缓存数据

参考答案：D

解析：

Cookie 实际上是一小段的文本信息，浏览器用来保存用户身份的缓存数据，以方便下次直接访问网站，据此得出选项 D 是优势 cookie 弊端有 1、增加流量消耗，浏览器每次请求服务器都需要带上 cookie 信息+网址提交给服务器安全隐患， cookie 使用明文传输。如果 cookie 被人拦截了，那人就可以取得所有的 session 信息，存在泄漏等安全隐患 3、Cookie 数量和长度的限制。每个 domain 最多只能有 20 条 cookie，每个 cookie 长度不能超过 4KB，否则会被截掉

30.使用电子邮件客户端从服务器下载邮件，使实现邮件的移动、删除等操作在客户端和邮箱上更新同步，所使用的电子邮件接收协议是（30）。 [1 分]

- A.SMTP
- B.POP3
- C.IMAP4
- D.MIME

参考答案：C

解析：

IMAP4 和 POP3 的区别是：POP3 协议允许电子邮件客户端下载服务器上的邮件，但是在客户端的操作（如移动邮件、标记已读等），不会反馈到服务器上，比如通过客户端收取了邮箱中的 3 封邮件并移动到其他文件夹，邮箱服务器上的这些邮件是没有同时被移动的而 IMAP4 客户端的操作都会反馈到服务器上，对邮件进行的操作，服务器上的邮件也会做相应的动作

31.在 Linux 系统中，DNS 配置文件的（31）参数，用于确定 DNS 服务器地址。 [1 分]

- A.nameserver

B.domain

C.search

D.sortist

参考答案：A

解析：

DNS 配置文件/etc/resolv.conf中的参数有 domain（可选）：声明服务器的域名，search（可选）：多个参数指明域名查询次序 nameserver（必须）：表明 DNS 服务器的 IP 地址 shortlist：允许将得到的域名结果进行特定的排序

32.在 Linux 系统中，要将文件复制到另一个目录中，为防止意外覆盖相同文件名的文件，可使用（32）

命令实现[1 分]

A.cp -a

B.cp -i

C.cp -R

D.cp-f

参考答案：B

解析：

cp-a：保留源文件或目录属性的前提下复制文件 cp-i：交互式覆盖既有文件之前先询问用户是否覆盖源文件。

Cp-R：递归处理，将指定目录下的所有文件与子目录一并处理 cp-f：强行复制文件或目录，不论目标文件或目录是否已存在

33.在 Linux 系统中，可在（33）文件中修改系统主机名[1 分]

A./etc/hostname

B./etc/sysconfig

C./dev/hostname

D./dev/sysconfig

参考答案：A

解析：

etc/hostname 文件，该文件包含了 Linux 系统的主机名。例如主机名【root@redhat~】#，使用 v 编辑器直接修改/etc/hostname 配置文件中的 redhat 为 redhat-64，保存文件，然后重新登录，此时，静态主机名已经更改为【root@redhat-64~】#

34.在 windows 命令提示符运行 nslookup 命令，结果如下所示，为 www.softw aretest.com 提供解析的 DNS 服务器 IP 地址是（34）

C: \Documents and Settings \user> nslookup www.softw aretest.com

Server: ns1softw aretest.com

Address: 192.168.1.254

Non-authoritative answer:

Name www.softw aretest.com

Address: 10.10.1.3 [1 分]

A.192.168.1.254

B.10.10.1.3

C.192.168.1.1

D.10.10.1.1

参考答案: A

解析:

Serverns1.softw aretest.com , 返回的 DNS 服务器名字。

Address: 192.168.1.254 返回的 DNS 服务器的 IP 地址 Non-authoritative answer, 非权威应答。除非实际存储 DNS Server 中获得域名解析回答的, 都称为非权威应答。也就是从缓存中获取域名解析结果。

Name www.softw aretest.com , 访问的目标 DNS 域名 Address: 10.10.1.3, 解析出来的访问的目标 IP 地址。

35.W indows Server2008R2 上 IIS7.5 能提供的服务有 (35)。 [1 分]

A.DHCP 服务

B.FTP 服务

C.DNS 服务

D.远程桌面服务

参考答案: B

解析:

IIS7.5 是基于 W indows 操作系统的 W eb 服务器, 计算机开启 IIS 服务后, 存储在上面的 ASP 等网站程序就能在互联网上正常发布和显示。IS (Internet Information Server, 互联网信息服务) 是一种 W eb (网页) 服务组件, 其中包括 W eb 服务器、FTP 服务。

36.某网络上 MAC 地址为 00-FF-78ED-20DE 的主机, 可首次向网络上的 DHCP 服务器发送 (36) 报文以请求 IP 地址配置信息, 报文的源 MAC 地址和源 IP 地址分别是 () [1 分]

A.Dhcp discover

B.Dhcp request

C.Dhcp offer

D.Dhcp ack

参考答案：A

解析：

当DHCP客户端第一次登录网络的时候，它会向网络发出一个Dhcpdiscover包。因为客户端还不知道自己属于哪一个网络，所以包的来源地址会为0.0.0.0，源MAC地址是自己的MAC地址，而目的地址则为255.255.255.255，然后再附上Dhcpdiscover的信息，向网络进行广播

37.某网络上MAC地址为00-FF-78-ED-20-DE的主机，可首次向网络上的DHCP服务器发送（36）报文以请求IP地址配置信息，报文的源MAC地址和源IP地址分别是（27）[1分]

A.0000000000 0.0.0.0

B.0000000000 255.255.255.255

C.00FF-78-ED-20DE 0.0.0.0

D.00-FF-78-ED 20-DE 255.255.255.255

参考答案：C

解析：

当DHCP客户端第一次登录网络的时候，它会向网络发出一个Dhcpdiscover包。因为客户端还不知道自己属于哪一个网络，所以包的来源地址会为0.0.0.0，源MAC地址是自己的MAC地址，而目的地址则为255.255.255.255，然后再附上Dhcpdiscover的信息，向网络进行广

38.用户在登录FTP服务器的过程中，建立TCP连接时使用的默认端口号是（38）[1分]

A.20

B.21

C.22

D.23

参考答案：B

解析：

文件传输协议：FTP，负责文件通过服务器上下传送。采用TCP的两条连接：数据连接20端口，控制连接21端口，C/S工作。用户登录时，建立TCP连接是控制连接，所以是21端口。

39.用户使用域名访问某网站时，是通过（39）得到目的主机的IP地址[1分]

A.Http

B.ARP

C.DNS

D.ICMP

参考答案：C

解析：

DNS 协议：域名解析协议，用于把主机域名解析为对应的 IP 地址。是一个分布式数据库，C/S 工作方式。主要基于 UDP 协议，少数情况下使用 TCP，端口号都是 53

40.在 DNS 的资源记录中，类型 A（40）[1 分]

- A.表示 IP 地址到主机名的映射
- B.表示主机名到 IP 地址的映射
- C.指定授权服务器
- D.指定区域邮件服务器

参考答案：B

解析：

每年必考内容，强调过多次。

41.下列关于防火墙技术的描述中，正确的是（41）[1 分]

- A.防火墙不能支持网络地址转换
- B.防火墙通常部署在企业内部网和 Internet 之间
- C.防火墙可以查、杀各种病毒
- D.防火墙可以过滤垃圾邮件

参考答案：B

解析：

防火墙技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全的一种技术。

防火墙的主要功能：①访问控制功能。②内容控制功能。③全面的日志功能。④集中管理功能。⑤自身的安全功能
防火墙的附加功能：①流量控制。②网络地址转换 NAT。③虚拟专用网 VPN

42.SHA-256 是（42）算法[1 分]

- A.加密
- B.数字签名
- C.认证
- D.报文摘要

参考答案：D

解析：

常见的信息摘要算可以用来保护数据的完整性。包括 MD5：信息摘要算法第五版，输入以 512 位为分组，进行处理，产生一个 128 位的输出 SHA：安全散列算法，也是按 512 位的分组进行处理，产生一个 160 位的输出

43.根据国际标准 TU-TX509 规定，数字证书的一般格式中会包含认证机构的签名，该数据域的作用是（43）。[1 分]

- A.用于标识颁发证书的权威机构 CA
- B.用于指示建立和签署证书的 CA 的 X509 名字
- C.用于防止证书的伪造
- D.用于传递 CA 的公钥

参考答案：C

解析：

证书包含 CA 的签名和用户的公钥信息，签名是为了防止伪造，类似身份证上面公安部门的防伪标记。

44.以下关于三重 DES 加密算法的描述中，正确的是（44）。[1 分]

- A.三重 DES 加密使用两个不同密钥进行三次加密
- B.三重 DES 加密使用三个不同密创进行三次加索
- C.三重 DES 加密的密钥长度是 DES 密钥长度的三倍
- D.三重 DS 加密使用一个密创进行三次加制

参考答案：A

解析：

三重 DES，即 3DES（Triple DES），是 DES 的改进算法，他使用两把密钥对报文做三次 DES 加密，第一层和第三层中使用相同的密钥，产生一个有效长度为 112 位的密钥

45.以下关于 HTP 和 HTTPS 的描述中，不正确的是（45）。[1 分]

- A.部署 HPS 需要到 CA 申请证书
- B.HTP 信息采用明文传输，H PS 则采用 SSL 加密传输
- C.HTP 和 HTTPS 使用的默认端口都是 80
- D.HTPS 由 SSL-HTTP 构建，可进行加密传输、身份认证，比 HTP 安全

参考答案：C

解析：

H ttps 和 HTTP 的区别 1、H ttps 协议需要到 CA 申请证书。

2、HTTP 是超文本传输协议，信息是明文传输，H ttps 则是具有安全性的 SS 加密传输协议

3、HTTP 和 H ttps 使用的是完全不同的连接方式，用的端口也不一样，前者是 80，后者是 443。

4、HTTP 的连接很简单，是无状态的；HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议，比 HTTP 协议安全

46.假设有一个 LAN，每 10 分钟轮询所有被管理设备一次，管理报文的处理时间是 50ms，网络延迟为 1ms，没有明显的网络拥塞，单个轮询需要时间大约为 0.2s，则该管理站最多可支持（46）个设备[1 分]

A.4500

B.4000

C.3500

D.3000

参考答案：D

解析：

网络管理中轮询设备和时间计算公式： $N \leq T/\Delta$ ，其中 N 为代理管理站数，T 轮询总时间， Δ 为单轮询需要的时间。依题意 $T=10$ 分钟=600s， $\Delta=0.2$ s。故 $N \leq T/\Delta=600/0.2=3000$ 个设备。（大涛提醒：题目中 50ms、1ms 为干扰项用不到）

47.某主机能够 ping 通网关，但是 ping 外网主机 IP 地址时显示“目标主机不可达”，出现该故障的原因可能是（47）[1 分]

A.本机 TCP/IP 协议安装错误

B.域名服务工作不正常

C.网关路由错误

D.本机路由错误

参考答案：C

解析：

网络管理命令：ping。利用 ICMP 报文来测试网络的连通性、是否丢包、名称解析等。例如 ping 127.0.0.1 检查 TCP/IP 协议、ping 本机 IP 检查网卡工作、ping 网关检查外网的连通性等。“目标主机不可达”般是由于网关路由错误或 ACL 过滤。

48.Windows 系统中的 Snmp 服务程序包括 SnmpService 和 SnmpTrap 两个。其中 SnmpService 接收 SNMP 请求报文，根据要求发送响应报文；而 SnmpTrap 的作用是（48）[1 分]

A.处理本地计算机上的陷入信息

B.被管对象检测到差错，发送给管理站

C.接收本地或远程 SNMP 代理发送的陷入信息

D.处理远程计算机发来的陷入信息

参考答案：B

解析：

Trap 机制是一种事件报告机制，用于意外或突发故障情况下，被管代理主动向管理站发送报警信息，而不是等待 SNMP 管理器的再次轮询。常见的报警类型有冷启动、热启动、线路故障线路故障恢复、认证失败等

49.某主机 IP 地址为 192.168.88.156，其网络故障表现为时断时续。通过软件进行抓包分析，结果如下图所示，造成该主机网络故障的原因可能是（49）

No.	Time	Source	Desnation	Protocol	Length	Info
1	0.000000	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.156
2	0.000001	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.190
3	0.000013	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.190
4	0.000015	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.156
5	0.000097	CompalIn_14:f_	CompalIn_14:f_	ARP	42	Who has 192.168.88.190? Tell 192.168.88.48
6	0.000102	CompalIn_14:f_	CompalIn_14:f_	ARP	42	Who has 192.168.88.190? Tell 192.168.88.48
7	0.000109	CompalIn_14:f_	Routerbo_36:2_	ARP	42	192.168.88.190 is at f0:76:1c:14:f9:43
8	0.000114	CompalIn_14:f_	Routerbo_36:2_	ARP	42	192.168.88.190 is at f0:76:1c:14:f9:43
9	0.000279	Routerbo_36:2_	CompalIn_14:f_	ARP	60	192.168.88.48 is at e4:8d:8c:36:23:3a
10	0.000279	Routerbo_36:2_	68:6f:3d:04:5_	ARP	60	192.168.88.48 is at e4:8d:8c:36:23:3a
11	0.010002	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.190
12	0.010004	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.156
13	0.010014	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.156
14	0.010016	CompalIn_14:f_	Routerbo_36:2_	ARP	42	Who has 192.168.88.48? Tell 192.168.88.190
15	0.010269	Routerbo_36:2_	68:6f:3d:04:5_	ARP	60	192.168.88.48 is at e4:8d:8c:36:23:3a

[1 分]

- A.网关地址配置不正确
- B.DNS 配置不正确或者工作不正常
- C.该网络遭到 ARP 病毒的攻击
- D.该主机网卡硬件故障

参考答案：C

解析：

ARP 病毒是利用 ARP 协议的漏洞进行传播的一类病毒的总称。ARP 协议是 TCP/IP 协议组的一个协议，能够把网络地址翻译成物理地址（又称 MAC 地址）。通常此类攻击的手段有两种：路由欺骗和网关欺骗。是一种入侵电脑的木马病毒。对电脑用户私密信息的威胁很大。从图中信息关键词“ARP 可只是 ARP 病毒，从 Who has 192.168.88.48? ”中看出不停的向网关发送数据报可知这是网关欺骗。

50.Windows 中标准的 SNMP Service 和 SNMP Trap 分别使用的默认 UDP 口是（50） [1 分]

- A.25 和 26

B.160 和 161

C.161 和 162

D.161 和 160

参考答案: C

解析:

SNMP 使用 UDP 作为传输协议, 是一种异步的请求/响应协议, 默认端口有两个: 用于数据传送与接收的 161 端口。用于报警 (Trap) 信息接收的 162 端口 SNMP Service 服务用于接收管理站的 request、next-request、response 报文, 报文的目标端口是 161。

SNMP Trap 服务用于被管象检测到差错, 发送给管理站, 报文目标端口是 162

51. 公司为服务器分配了 IP 地址段 121.21.35.192/28, 下面的 IP 地址中, 不能作为 web 服务器地址 [1 分]

A.121.21.35.204

B.121.21.35.205

C.121.21.35.206

D.121.21.35.207

参考答案: D

解析:

三步划分子网法, 子网掩码是 /28, 可知变化在第四段, 那么块大小为: $32-28=4$ 的 4 次方=16, 范围是 192~207.完整的范围是: 121.21.35.192~121.21.35.207 可知该网络广播地址是: 121.21.35.207, 不能作为 Web 服务器地址

52. 使用 CIDR 技术将下列 4 个 C 类地址: 202.145.27.0/24, 202.145.29.0/24, 202.145.31.0/24 和 202.145.33.0/24 汇总为一个超网地址, 其地址为 (52), 下面 (53) 不属于该地址段, 汇聚之后的地址空间是原来地址空间的 (54) 倍

(52) [1 分]

A.202.145.27.0/20

B.202.145.0.0/20

C.202.145.0.0/18

D.202.145.32.0/19

参考答案: C

解析:

根据大涛三步划分子网法: 观察题目, 可知变化在第三段, 那么块大小为: $33-27+1=7$, 取块大小 8 即 2 的 3 次方, 左借 3 位, 块大小 8, 范围是 24~31, 此时不能包括 4 个 C 类。

同样取块大小 16, 范围是 16~31, 不能包括 4 个 C 类; 取块大小 32, 范围是 0~31, 也不

能包括 4 个 C 类；只有取块大小 64，范围是 0~63，可以包括 4 个 C 类。此时 $64=2$ 的 6 次方，左借 6 位，可知网络地址是：202.145.0.0/18 ($24-6=18$)。

（大涛注：此题较为特殊，计算块大小以后，要验算一下块大小能否包含题目中的 4 个 C 类，不能包含就要扩大块大小，直到包含。）

53.使用 CDR 技术将下列 4 个 C 类地址：202.145.27.0/24,202.145.29.0/24,202.145.31.0/24 和 202.145.33.0/24 汇总为一个超网地址，其地址为 (52)，下面 (53) 不属于该地址段，汇聚之后的地址空间是原来地址空间的 (54) 倍 [1 分]

- A.202.145.20.255
- B.202.145.35.177
- C.202.145.60.210
- D.202.145.64.1

参考答案：D

解析：

根据上题取块大小 64，范围是 0~63，完整的范围是 202.145.0.0~202.145.63.255.可知 202.145.64.1 不在范围内，不属于该网段地址

54.使用 CDR 技术将下列 4 个 C 类地址：202.145.27.0/24,202.145.29.0/24,202.145.31.0/24 和 202.145.33.0/24 汇总为一个超网地址，其地址为 (52)，下面 (53) 不属于该地址段，汇聚之后的地址空间是原来地址空间的 (54) 倍 [1 分]

- A.2
- B.4
- C.8
- D.16

参考答案：D

解析：

原有掩码为/24，标准 C 类地址，按照现有掩码为/18 划分后有： $24-18=6$ 位， $2^6=64$ 个 C 类地址；而原来有 4 个 C 类地址，汇聚之后的地址空间是原来地址空间的 $64/4=16$ 倍

掩码/28 将 27、29、31、33 写成 01 模式分别是：

$27=16+8+2+1=00011011$
 $29=16+8+4+1=00011101$
 $31=16+8+4+2+1=00011111$
 $33=32+1=00100001$

地址 202.145.0.0/18，地址块为 $2^{24-18}=64$ ，那么下一个子网是 202.145.64.0/18，所以可用

地址区间为 202.145.0.1-202.145.63.254，只有 D 不在此范围原有掩码为/24，标准 C 类地址，现有掩码为/18，那么一个/18 可用划分 6 位做子网位，可用划出 $2^6=64$ 个 C 类地址，而原来有 4 个 C 类地址，即 16 倍。

55.下面的 IP 地址中，可以用作主机 IP 地址的是 (55) [1 分]

A.192.168.15.255/20

B.172.16.23.255/20

C.172.20.83.255/22

D.202.100.10.15/28

参考答案: B

解析:

按照大涛三步划分子网法，计算如下选项 A:/20，第三段变化，块大小 $2^{24-20}=4, 2^4=16$ ，范围是 0~15，完整的范围是 192.168.0.0~192.168.15.255，可知选项 A 是一个广播地址。

选项 B:/20，第三段变化，块大小 $2^{24-20}=4, 2^4=16$ ，范围是 16~31，完整的范围是 172.16.16.0~172.16.31.255，可知选项 B 是一个主机地址。

继续按此方法计算出来，选项 C 是广播地址、选项 D 也是广播地址。可自行计算验证一下。

A 的地址块为 $2^4=16$ ，那么 192.168.16.0 是网络号，则 192.168.15.255 是广播地址，不能做主机 IP

B 与 A 类似，子网地址可推算出为 172.16.0.0/20、172.16.16.0/20、172.16.32.0/20，故 B 给出的地址正好落到 16.0 到 32.0 两个子网间，可用作为主机 IP。

CD 自行计算即可

56.交换设备上配置 STP 的基本功能包括 (56)

①将设备的生成树工作模式配置成 STP

②配置根桥和备份根桥设备

③配置端口的路径开销值，实现将该端口阻塞

④使能 STP，实现环路消除 [1 分]

A.①③④

B.①②③

C.①②③④

D.①②

参考答案: C

解析:

教程 P468、469、470 页，配置 STP 基本功能，有以下步骤：

- 1、配置环网中的设备生成树协议工作在 STP 模式
- 2、配置根桥和备份根桥设备。
- 3、配置设备端口路径开销计算方法为华为计算方法。
- 4、配置启用 STP 实现破除环路。

57.OSPF 协议相对于 RIP 的优势在于（57）

- ①没有跳数的限制
 - ②支持可变长子网掩码（VLSM）
 - ③支持网络规模大
 - ④收敛速度快[1 分]
- A.①③④
B.①②③
C.①②③④
D.①②

参考答案：C

解析：

教程 P224 页、228 页，有 OSPF 是一种链路状态协议，因而不具有跳数限制。OSPF 具有支持大型网络、占用网络资源少、路由收敛快等优点，在目前的网络配置中占有很重要的地位。

链路状态协议支持无类别的路由和路由汇总功能，可以使用 VLSM 和 CIDR 技术。

58.OSPF 协议中 DR 的作用范围是（58）[1 分]

- A.一个 area
B.一个网段
C.一台路由器
D.运行 OSPF 协议的网络

参考答案：B

解析：

教程 P225 页，在一个广播网络（指的就是一个网段的广播网络）或 NBMA 网络中要选个指定路由器（Designated Router,DR），其他的路由器都与 DR 建立毗邻关系，把自己掌握的链路状态信息提交给 DR，由 DR 代表这个网络向外界发布。

其他点到点网络、点到多点网络，不属于广播网络，也不需要选取 DR。可以看出，DR 的存在减少了毗邻关系的数量，从而也减少了向外发布的路由信息量

59.GVRP 定义的四种定时器中缺省值最小的是（59）[1 分]

- A.Hold 定时器
- B.Join 定时器
- C.Leave 定时器
- D.LeaveAll定时

参考答案: A

解析:

GVRP 是一种 GARP (通用属性注册协议) 的具体应用, GARP 消息发送的时间间隔是通过定时器来实现的 GARP 定义了四种定时器, 用于控制 GARP 消息的发送周期 LeaveL1定时器: 缺省情况下, LeaveL1定时器的值为 1000 厘秒。

配置 Hold 定时器: 缺省情况下, Hold 定时器的值为 10 厘秒。(1 秒=100 厘秒)

配置 Join 定时器: 缺省情况下, Join 定时器的值为 20 厘秒。

配置 Leave 定时器: 缺省情况下, Leave 定时器的值为 60 厘秒

60.下列命令片段的含义是 (60)

```
< huawei> system -view
[Huawei]vlan 10
[Huawei-vlan10]name huawei
[Huawei-vlan10]quit [1 分]
```

- A.创建了两个 VLAN
- B.恢复接口上VLAN 缺省配置
- C.配置 W lan 的名称
- D.恢复当前VLAN 名称的缺省值

参考答案: C

解析:

```
< Huawei> system -vieW /进入系统视图
【 Huawei】 van10//创建并进入 van10
【 Huawei-vlan10】 name huawei//配置该 van 的名称为" huawei"
【 Huawei-vlan10】 quit//退出当前配置模式
```

61. (61) 的含义是一台交换机上的VIM 配置信息可以传播、复制到网络中相连的其他交换机上。 [1 分]

- A.中继端口
- B.VLAN 中继
- C.w lan 穿透
- D.SuperVLAN

参考答案: B

解析：

VLAN 中继，是保证VILAN 信息全网一致性的协议，只要在一台主交换机上创建、删除、重命名 van，主交换机可以传播、复制到其他交换机，其他交换机就也会同步学习到这些 van 信息的变化，大大减少了管理员的工作量

62.以下关于 BGP 的说法中，正确的是（62） [1 分]

- A.BGP 是一种链路状态协议
- B.BGP 通过 UDP 发布路由信息
- C.BGP 依据延迟来计算网络代价
- D.BGP 能够检测路由循环

参考答案：D

解析：

边界网关协议 BGP：是外部网关协议，用于不同自治系统 AS 之间。依据路径属性计算网络代价。通过 TCP 的 179 端口建立连接。支持子网VILSM 和 CDR，是一种路径矢量协议。

BGP 的防环（即路由循环）机制主要有 2 条第一是 AS 内部防环：通过 BGP 水平分割来实现的，BGP 水平分割的基本思想是属不把从 BGP 邻居学到的路由传递给其他 BGP 邻居。第二是 AS 间的防环：通过属性 AS_PATH 来实现，基本思想是：如果某台 BGP 路由器从其外部对等体收到某条路由的 AS_PATH 中包含有自己的 AS 号那么该路由器就知道出现了环路，因而丢弃该路由。

63.快速以太网 100BASE-T4 采用的传输介质为（63） [1 分]

- A.3 类 UTP
- B.5 类 UTP
- C.光纤
- D.同轴电缆

参考答案：A

解析：

表 4-9 快速以太网物理层规范

标 准	传 输 介 质	特性阻抗	最大段长
100Base-TX	两对 5 类 UTP	100Ω	100m
	两对 STP	150Ω	
100Base-FX	一对多模光纤 MMF	62.5/125μm	2km
	一对单模光纤 SMF	8/125μm	40km
100Base-T4	四对 3 类 UTP	100Ω	100m
100Base-T2	两对 3 类 UTP	100Ω	100m

如图所示。

64.CSM A/CD 采用的介质访问技术属于资源的（64） [1 分]

- A.轮流使用
- B.周定分配
- C.竞争使用
- D.按需分配

参考答案：C

解析：

W LAN 的安全措施有 ssID 访问控制物理地址过滤有线等效保密（W EP）：使用 RC4 协议加密 W PA/W PA2：包含认证、加密和数据完整性校验 3 部分。

IEEE802.11：IEEE802.11 标准是结合 IEEE802.1X 进行用户端口身份验证和设备验证

65.W LAN 接入安全控制中，采用的安全措施不包括（65）。 [1 分]

- A.SSID 访问控制
- B.CA 认证
- C.物理地址过滤
- D.W PA2 安全认证

参考答案：B

66.下列 IEEE802.11 系列标准中，阻 A 的传输速率达到 300Mbps 的是（66） [1 分]

- A.802.11a
- B.802.11b
- C.802.11g
- D.802.11n

参考答案：D

解析：

名称	发布时间	工作频段	调制技术	数据速率
802.11	1997 年	2.4GHz ISM 频段	DB/SK DQPSK	1Mbps 2Mbps
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mbps, 11Mbps
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mbps
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mbps
802.11n	2009 年	2.4/5GHz 频段	OFDM MIMO	300Mbps 600Mbps
802.11ac	2012 年	5GHz U-NII 频段	OFDM MIMO	433Mbps 6.9Gbps
802.11ax	2019 年	2.4/5GHz 频段	OFDM MIMO	600Mbps 9.6Gbps

67.某单位计划购置容量需求为 60TB 的存储设备，配置一个 RAID 组，采用 RAID5 冗余，并配置一块全局热备盘，至少需要（67）块单块容量为 4TB 的磁盘。[1 分]

- A.15
- B.16
- C.17
- D.18

参考答案：C

解析：

RAID5 校验盘占 1 个，热备盘占 1 个，那么需要 $60T/4T+2=17$ 块。

RAID5 的存储利用率为 $(n-1)/n$ ，要存储 60TB，需要 $60/4=15$ ，RAID5 需要 1 个冗余盘，另外再配置 1 块全局热备盘，则需要 $15+1+1=17$ 块 4T 的磁盘

68.对某银行业务系统的网络方案设计时，应该优先考虑（68）原则[1 分]

- A.开放性
- B.先进性
- C.经济性
- D.高可用性

参考答案：D

解析：

高可用性（High Availability）通常来描述一个系统经过专门的设计，从而减少停工时间，而保持其服务的高度可用性。银行、电力、金融业务的网络对可用性要求高，要求几乎不能停工，在网络方案设计中，要优先考虑高可用性。

69.在项目管理过程中，变更总是不可避免，作为项目经理应该让项目干系人认识到（69）[1 分]

- A.在项目设计阶段，变更成本较低
- B.在项目实施阶段，变更成本较低
- C.项目变更应该由项目经理批准
- D.应尽量满足建设方要求，不需要进行变更控制

参考答案：A

解析：

项目变更管理是指项目组织为适应项目运行过程中与项目相关的各种因素的变化，保证项目目标的实现而对项目计划进行相应的部分变更或全部变更，并按变更后的要求组织项目实施的过初期变更成本较低，后期变更成本较大，随着项目的进展变更不可避免，变更有变更控制委员会 CCB 批准

70.进行项目风险评估最关键的时间点是（70） [1 分]

- A.计划阶段
- B.计划发布后
- C.设计阶段
- D.项目出现问题时

参考答案：A

解析：

风险评估越早做越好，如果风险特别大，可能都不会做这个项目。项目生命周期和阶段划分的特点之一是，随着项目推进，项目面临的风险和不确定性逐渐降低，外界因素对项目的影 响程度也逐渐减弱。即在项目开始阶段，面临的风险最大。

般越早识别风险，就越容易制定相对的应对措施，减少风险可能造成的损失。所以在规划阶段进行项目风险评估是很关键的

71.The Address Resolution Protocol (ARP) was developed to enable communications on of the OSI model, and allows computers to introduce each other across a network prior to communication. ARP finds the (72) address of a host from its known (73) address. Before a device sends a datagram to another device, it looks in its ARP cache to see if there is a MAC address and corresponding IP address for the destination device. If there is no entry, the source device sends a (74) message to every device on the network. Each device compares the IP address to its own. Only the device with the matching IP address replies with a packet containing the MAC address for the device (except in the case of "proxy ARP"). The source device adds the (75) device mac address to its arp table for future reference [1 分]

- A.1 and 2
- B.2 and 3
- C.3 and 4
- D.4 and 5

参考答案：B

72. [1 分]

- A.IP
- B.logical
- C.hardware
- D.network

参考答案：C

73. [1 分]

A.IP

B.physical

C.MAC

D.virtual

参考答案: A

74. [1 分]

A.unicast

B.m ulticast

C.broadcast

D.p oint-to-p oint

参考答案: C

75. [1 分]

A.source

B.destination

C.gatew ay

D.proxy

参考答案: B

≡ 本试卷共计 75 题，此处为结束标志。

≡ exam coo™