【1】A

【解析】

控制部件

英文 Control unit；控制部件，主要是负责对指令译码，并且发出为完成每条指令所要执行的各个操作的控制信号。

其结构有两种：一种是以微存储为核心的微程序控制方式；一种是以逻辑硬布线结构为主的控制方式。

微存储中保持微码，每一个微码对应于一个最基本的微操作，又称微指令；各条指令是由不同序列的微码组成，这种微码序列构成微程序。中央处理器在对指令译码以后，即发出一定时序的控制信号，按给定序列的顺序以微周期为节拍执行由这些微码确定的若干个微操作，即可完成某条指令的执行。

简单指令是由（3～5）个微操作组成，复杂指令则要由几十个微操作甚至几百个微操作组成。

【2】C

【解析】

DMA 方式主要适用于一些高速的 I/O 设备。这些设备传输字节或字的速度非常快。对于这类高速 I/O 设备，如果用输入输出指令或采用中断的方法来传输字节信息，会大量占用 CPU 的时间，同时也容易造成数据的丢失。而 DMA 方式能使 I/O 设备直接和存储器进行成批数据的快速传送。

【3】D

【解析】

CRC 校验码

编码思想：任何一个由二进制数位串组成的代码，都可以唯一地与一个只含有 0 和 1 两个系数的多项式建立一一对应的关系。例如，1011011 可以看成是一元多项式 X6+X4+X3+X+1 的系数。

在使用 CRC 编码时，发送方和接收方事先约定一个生成多项式 G（X），这个多项式最高位和最低位必须是 1。

假设一个帧有 m 位，它对应的多项式是 M（X），为了计算检验和，该帧长度必须大于生成多

项式的长度。循环冗余码的编码思想就是：在帧的尾部追加一个检验和，使得追加之后的帧对应的多项式能够被 G（X）除尽（即余数为 0）。当接收方收到带有检验和的帧之后，试着用 G（X）去除它，如果余数不为 0，则表明在传输过程中有错误

【4】B

【解析】

为了提高操作系统的效率，人们最初选择了向指令系统中添加更多、更复杂的指令这种方式来实现，而且随着不断地升级和向后兼容的需要，指令集也越来越大。这种类型的计算机，我们成为复杂指令计算机（CISC）。后来研究发现，计算机指令系统如果使用少量结构简单的指令，就会提高计算机性能，这就是精简指令集（RISC）。

指令系统类型	指令	寻址方式	实现方式
CISC	数量多，使用频率差别大，可变长格式	支持多种寻址方式	
RISC	数量少，使用频率接近，定长格式	支持方式少	硬件布线逻辑控制为主

【5-6】A B

【解析】

计算机软件著作权的归属

（1）软件著作权归属的基本原则

我国《著作权法》规定著作权属于作者。《计算机软件保护条例》规定软件著作权属于软件开发者。

（2）职务开发软件著作权的归属

当公民作为某单位的雇员时，如其开发的软件属于执行本职工作的结果，则软件著作权应归单位享有。若开发的软件不是执行本职工作的结果，其著作权不属于单位享有；如果该雇员主要使用了单位的设备，按照《计算机软件保护条例》第十三条第三款规定，不能属于该雇员所有

（3）合作开发软件著作权的归属

由两个或两个以上的公民、法人或其他组织订立协议，共同开发完成的软件属于合作开发的软件。其著作权的归属一般是共同享有，合作开发者不能单独行使转让权。如果有软件著作权的协议，则按照协议确定软件著作权的归属。

【7】D

【解析】

沟通渠道数为 n*（n-1）/2=10*9/2=45

【8】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。有的系统把"0"作为盘块已分配的标记，把“1”作为空闲标志。(它们的本质上是相同的，都是用一位的两种状态标志空闲和已分配两种情况。)磁盘上的所有盘块都有一个二进制位与之对应，这样，由所有盘块所对应的位构成一个集合，称为位示图。

1024*1024/4/64=4096

【9】C

【解析】

相对路径：即相对于当前文件的路径，前端开发中比较常用的路径表示方法

绝对路径：即主页文件或者目录在硬盘上真正的路径。

【10】C

【解析】

NFA-->DFA.整体的步骤是三步： 一，先把正规式转换为 NFA（非确定有穷自动机）， 二，在把 NFA 通过“子集构造法”转化为 DFA， 三，在把 DFA 通过“分割法”进行最小化。

NFA 可以有 000 状态，因此排除 A；NFA 可以有 010 状态，可以排除 BD。

【11】B

【解析】

信号的波特率为 1000Baud，信道支持的最大数据速率为 2000b/s

R=Blog2(N),2000=1000*log2(N),N=4,显然码元种类数为 4 个，QPSK 是四进制相移键控。

【12】D

【解析】

奈奎斯特采样定律，采样频率必须是信号最大频率的 2 倍。

【13】B

【解析】

IEEE802.3Z 工作组已确定了以下一组规范，统称为 1000Base－X。

• 1000Base－LX：多模光纤传输距离为 550 米，单模光纤传输距离为 3000 米。

• 1000Base－SX：62.5 微米多模光纤传输距离为 300 米，50 微米多模光纤传输距离为 550 米。

• 1000Base－CX：用于短距离设备的连接，使用高速率双绞铜缆，最大传输距离为 25 米。

• 1000Base－T：5 类铜缆传输最大距离为 100 米。

【14】B

【解析】

直通式交换，也就是交换机在收到帧后，只要查看到此帧的目的 MAC 地址，马上凭借 MAC 地址表向相应的端口转发；这种方式的好处是速度快，转发所需时间短，但问题是可能同时把一些错误的、无用的帧也同时转发向目地端。

存储转发机制就是交换机的每个端口被分配到一定的缓冲区（内存空间，一般为 64 k），数据在进入交换机后读取完目标 MAC 地址，凭借 MAC 地址表了解到转发关系后，数据会一直在此端口的缓冲区内存储，直到数据填满缓冲区然后一次把所有数据转发到目的地。在数据存储在缓冲区期间，交换机会对数据作出简单效验，如果此时发现错误的数据，就不会转发到目地端，而是在这里直接丢弃掉了。当然这种方式可以提供更好的数据转发质量，但是相对的转发所需时间就会比直通交换要长一点。碎片隔离式也叫改进型直通式交换，利用到直通式的优势就是转发迟延小，同时会检查每个数据帧的长度。因为原理上，每个以太网帧不可能小于 64 字节，大于 1518 字节。如果交换机检查到有小过 64 字节或大于 1518 字节的帧，它都会认为这些帧是“残缺帧”或“超长帧”，那么也会在转发前丢弃掉。这种方式综合了直通交换和存储转发的优势，很多高速交换机会采用，但是并没有存储转发方式来的普及。无论是直通转发还是存储转发都是一种二层的转发方式，而且它们的转发策略都是基于 目

的 MAC（DMAC）的，在这一点上这两种转发方式没有区别。第三种方法主要是第一种“直通转发”的变形。它们之间的最大区别在于，它们何时去处理转发，也就是交换机怎样去处理数据包的接收进程和转发进程的关系。

【15】D

【解析】

串扰指的是网线在传输网络信号中，产生了彼此的互相干扰，严重的时候会影响到网络传输得质量。网线的双绞程度越紧密，绞距越均匀时，其抗干扰的能力也会越强，且内部的串扰也会越小，在长距离网络传输中，效果也就越好。

近端串扰，缩写为 NEXT，是衡量单链路/通道的一个性能参数，测量从一对线耦合到另一对线的信号。引起干扰的线对被称为“干扰线对”，而受串扰影响的线对被称为“被干扰线对”。

远端串扰缩写为 FEXT，也在一个通道内测量。远端串扰与 NEXT 有很多相似之处，但在通道的远端测量。

【16-17】B C

【解析】

HDLC 用 01111110 作为帧的边界标志

地址字段用于标识从站的地址，用在点对点链路中 HDLC 定义了三种帧：信息帧（I 帧）、管理帧（S 帧）和无编号帧（U 帧）

信息字段：只有 I 帧和某些无编号帧还有信息字段

帧中继工作在 OSI 低两层，即物理层与数据链路层。

FR 帧比较简单，只做检错，不再重传，没有滑动窗口的流控，只用拥塞控制

帧中继速率可达 64Kbit/s - 2Mbit/s

帧中继具有动态分配带宽的功能，允许用户数据速率在一定范围内变化，可以有效处理突发性数据。

帧中继无法保证可靠提交，不适用于对延迟敏感的应用，如音频、视频。

【18-19】B C

【解析】

常见数字传输系统

T1 载波：在北美和日本广泛使用。它把 24 路按时分多路的原理复合在一条 1.54Mbps 的高速信道上。每路话音信道有 7 位数据位和一个信令位，周期为 125us，因此 24 路话音信道可容纳 8×24=192 位长的数字串。这 192 位数字组成一帧，最后再加入一个帧同步位，故帧长为 193 位。每 123us 传送一帧，这样，对每一路话音信道来说，传输数据的速率为 7b/125us=56Kbps，传输控制信息的速率为 1b/125us=8Kbps，总的速率为 193b/125us=1.544Mbps。

E2 载波由 4 个 E1 载波组成数据速率为 8.448Mbps；E3 载波由 4 个 E2 载波组成，数据速率为 34.368Mbps；E4 载波由 4 个 E3 载波组成，数据速率为 139.24Mbps；E5 载波由 4 个 E4 载波组成，数据速率为 565.148Mbps。

【20】D

【解析】

TCP 和 UDP 有各自的端口号相互独立，均使用 16 位端口号

【21】A

【解析】

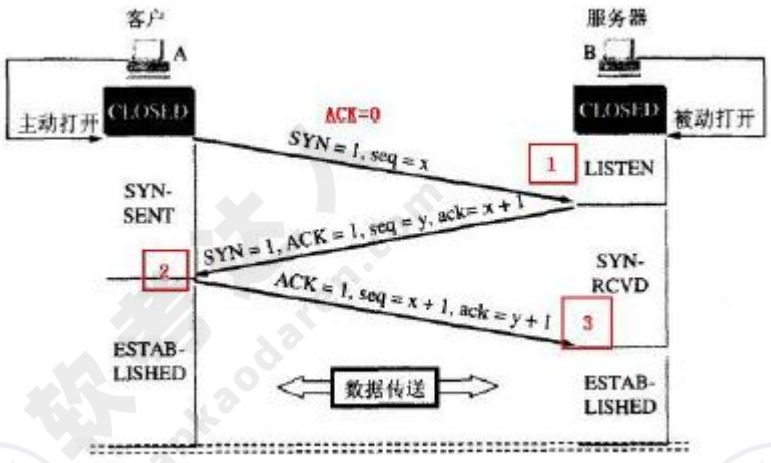
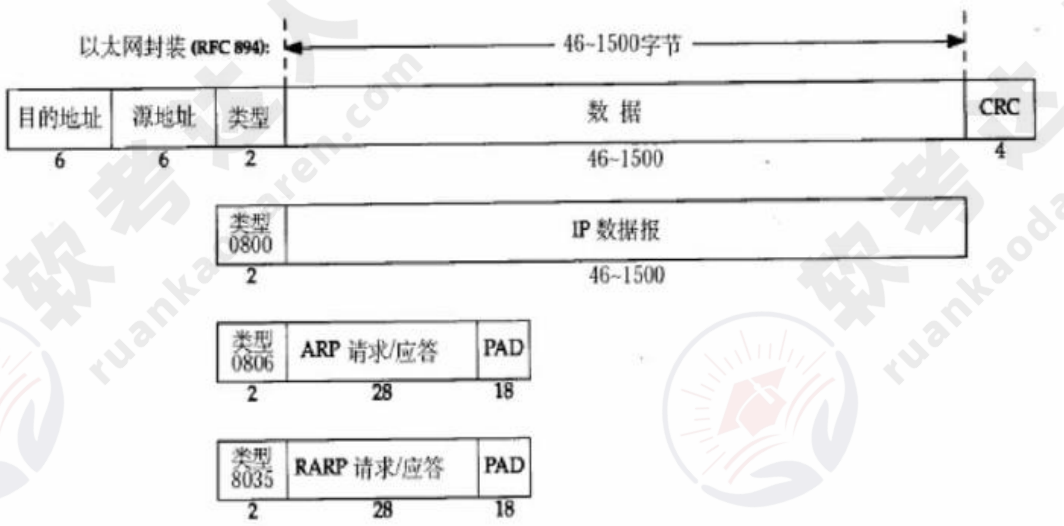


图 5-31 用三次握手建立 TCP 连接

【22-24】A B D

【解析】



【25】A

【解析】

OSPF 定义的 5 种网络类型：

1.点到点网络(point-to-point)，由 cisco 提出的网络类型，自动发现邻居，不选举 DR/BDR，hello 时间 10s。

2.广播型网络(broadcast)，由 cisco 提出的网络类型，自动发现邻居，选举 DR/BDR，hello 时间 10s。

3.非广播型（NBMA）网络 (non-broadcast)，由 RFC 提出的网络类型，手工配置邻居，选举 DR/BDR，hello 时间 30s。

4.点到多点网络 (point-to-multipoint)，由 RFC 提出，自动发现邻居，不选举 DR/BDR，hello 时间 30s。

5.点到多点非广播，由 cisco 提出的网络类型，手动配置邻居，不选举 DR/BDR，hello 时间 30s

【26】D

【解析】

边界网关协议（BGP）是运行于 TCP 上的一种自治系统的路由协议。BGP 是唯一一个用来处理像因特网大小的网络的协议，也是唯一能够妥善处理好不相关路由域间的多路连接的协议。

BGP 构建在 EGP 的经验之上。 BGP 系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括列出的自治系统（AS）的信息。这些信息有效地构造了 AS 互联的拓朴图并由此清除了路由环路，同时在 AS 级别上可实施策略决策。

【27-29】A C A

【解析】

从 interface 192.168.1.1 和 neighbor 192.168.1.2 以及拓扑图可以看出是 R1.有明显的 area 0.0.0.0 和 DR 之类的信息，肯定是 ospf 协议。从 state full 可以看出。

【30】D

【解析】

SMTP 协议与人们用于面对面交互的礼仪之间有许多相似之处。首先，运行在发送端邮件服务器主机上的 SMTP 客户，发起建立一个到运行在接收端邮件服务 器主机上的 SMTP 服务器端口号 25 之间的 TCP 连接。如果接收邮件服务器当前不在工作，SMTP 客户就等待一段时间后再尝试建立该连接。SMTP 客户和服务器先执行一些应用层握手操作。就像人们在转手东西之前往往先自我介绍那样，SMTP 客户和服务器也在传送信息之前先自我介绍一下。在这个 SMTP 握手阶段，SMTP 客户向服务器分别指出发信人和收信人的电子邮件地址。
彼此自我介绍完毕之后，客户发出邮件消息。

POP 的全称是 Post Office Protocol，即邮局协议，用于电子邮件的接收，它使用 TCP 的 110 端口。现在常用的是

第三版 ，所以简称为 POP3。POP3 仍采用 Client/Server 工作模式，Client 被称为客户端，一般我们日常使用电脑都是作为客户端，而 Server（服务器）则是网管人员进行管理的。举个形象的例子，Server（服务器）是许多小信箱的集合，就像我们所居住楼房的信箱结构，而客户端就好比是一个人拿着钥匙去信箱开锁取信一样的道理。

【31】B

【解析】

Mode：权限设定字串，格式为[ugoa...][[+-=][rwxX]...][,...]，其中 u 表示该文档的拥有者，g 表示与该文档的拥有者同一个组（group）者，o 表示其他的人，a 表示所有的用户。如图 17-1-1 所示，“+”表示增加权限、“-”表示取消权限、“=”表示直接设定权限。“r”

表示可读取，“w”表示可写入，“x”表示可执行，“x”表示只有当该文档是个子目录或者已经被设定为可执行。此外，chmod 也可以用数字来表示权限。

【32】D

【解析】

httpd 为 web 服务器进程，配置文件为 httpd.conf

【33】B

【解析】

ls 命令

就是 list 的缩写，通过 ls 命令不仅可以查看 linux 文件夹包含的文件，而且可以查看文件权限(包括目录、文件夹、文件权限)查看目录信息等等

常用参数搭配：

ls -a 列出目录所有文件，包含以.开始的隐藏文件

ls -A 列出除.及..的其它文件

ls -r 反序排列

ls -t 以文件修改时间排序

ls -S 以文件大小排序

ls -h 以易读大小显示

ls -l 除了文件名之外，还将文件的权限、所有者、文件大小等信息详细列出来

【34】B

【解析】

ipconfig

主要是了解当前 TCP/IP 协议所设置的值，如 IP 地址、子网掩码、缺省网关、Mac 地址等.

基本使用方法：ipconfig [/all/release/renew]

ipconfig：当不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值.

/all：当使用 all 选项时，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，它会显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期.

/release & /renew ： 这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用.如果我输入 ipconfig/release,那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）.如果输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址.请注意，大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址.

【35】C

【解析】

Workstation 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。

【36】D

【解析】

邮件服务器是一种用来负责电子邮件收发管理的设备。它比网络上的免费邮箱更安全和高效，因此一直是企业公司的必备设备。邮件服务器与其它程序协同工作用以组成有时被称作消息系统的内容。消息系统包括了所有必要的应用程序来保证电子邮件按照应有的路径传送。当你发送电子邮件消息时，你的电子邮件程序，如 Outlook 或 Eudora，发送消息到你的邮件服务器，它再依次发送到其它邮件服务器或同一服务器的保存区，过后再发送出去。作为一个规则，该系统使用 SMTP（简单邮件传送协议）或 ESMTP（扩展 SMTP）来发送电子邮件，使用 POP3（电子邮局协议 3）或 IMAP（因特网消息访问协议）来接收电子邮件。

【37】C

【解析】

MIME(Multipurpose Internet Mail Extensions)多用途互联网邮件扩展类型。是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开. 其作用就是能够支持：非 ASCII 字符文本；非文本格式附件（二进制、声音、图像等）；由多部分（multiple parts）组成的消息体；包含非 ASCII 字符的头信息（Header information）。

【38】C

【解析】

APIPA 是一个 DHCP 故障转移机制。当 DHCP 服务器出故障时， APIPA 在 169.254.0.1 到 169.254.255.254 的私有空间内分配地址，所有设备使用默认的网络掩码 255.255.0.0。客户机调整它们的地址使用它们在使用 ARP 的局域网中是唯一的。APIPA 可以为没有 DHCP 服务器的单网段网络提供自动配置 TCP/IP 协议的功能。

【39】B

【解析】

IIS 支持 web、FTP 和虚拟的 SMTP 服务器，dns 有专门的服务器。

【40】C

【解析】

HTTP 505 错误是 HTTP 状态码的一种,表示“HTTP 版本不受支持”,当服务器不支持请求中所使用的 HTTP 协议版本时就返回此错误。

【41-42】B D

【解析】

在非对称加密算法中，私钥用于解密和签名，公钥用于加密和认证。

【43-44】A D

【解析】

数字签名

数字签名是用于确认发送者身份和消息完整性的一个加密的消息摘要。数字签名应满足以下 3 点：

接收者能够核实发送者;发送者事后不能抵赖对报文的签名;接收者不能伪造对报文的签名。

数字签名可以利用对称密码体系（如 DES）、公钥密码体系或公正体系来实现。

最常用的实现方法是建立在公钥密码体系和单向散列函数算法（如 MD5、SHA）的组合基础上。

【45-46】A A

【解析】

SNMP 协议实体发送请求和应答报文的默认端口号是 161，SNMP 代理发送陷阱报文（Trap）的默认端口号是 162。

【47】B

【解析】

C:\>snmputil get 192.168.1.31 public .1.3.6.1.2.1.1.3.0

public .1.3.6.1.2.1.1.3.0 是指的系统开机时间多长。

OID(对象标识符)，是 SNMP 代理提供的具有唯一标识的键值。MIB（管理信息基）提供数字化 OID 到可读文本的映射。

所有完全验证 OID 都有 .iso.org.dod.internet.private 开始，数字表达为:.1.3.6.4. 。几乎所有的 OID 都会跟上企业(.1)和由 IANA（互联网编号分配中心分配的）唯一的厂商标号。 OID 的相对格式，从企业值开始，略过所有的隐含地址。因此，可以用相对地址 enterprises.netapp.netappl.raid.diskSUmmary.diskSpaceCount.0 来表示上述的 OID，或者用数字格式 .1.789.6.4.8.0 .

某些唯一键值，可用多个实例表示，这样所有的 OID 都以实例值结尾。因此可以看到大多数 OID 都是以一个 .0 结尾的。

【48】B

【解析】

查看日志信息，可以用 display logbuffer 或者 display trapbuffer。这两个命令为会经常用到。

【49】B

【解析】

问题现象：

设备不断重启，每次在配置恢复阶段（未输出“Recover configuration...”）之前就发生复位。

解决方法：

1. 在交换机启动时按照提示信息，输入Ctrl-B进入bootrom菜单。

2. 在bootrom菜单中，将系统大包文件传入设备，并设置为启动文件，重启设备。
3. 若仍然无法解决，则需要继续更新bootrom。
4. 仍然不能解决请联系华为技术支持处理。

【50】A

【解析】

设备上无法学习正确的 MAC 表项的原因包括：

没有收到报文（链路 Down、接口未加入 VLAN、接口参与环路协议计算并且被阻塞、配置了 MAC 地址漂移检测功能并且接口或 MAC 被阻断等导致）。

网络中存在环路导致 MAC 表项震荡。

去使能了 MAC 地址学习功能或者已经存在对应的 Sticky MAC 地址。

MAC 表项已达设备支持的最大规格。

配置了对应的静态路由或黑洞路由。

【51-52】D A

【解析】

8000/254=31.49 ，因此必须 32 个。2^5=32,因此需要借用 5bit。24-5=19.再用快速计算算出 192.168.210.181 所在的网络范围即可。[210/32]*32=192.

【53】C

【解析】

C 的范围是 20.96.0.0---20.127.255.255

【54-55】B C

【解析】

IPv6 报头结构

版本号表示协议版本．值为 6

流量等级主要用于 QoS

流标签用来标识同一个流里面的报文

载荷长度表明该 IPv6 包头部后包含的字节数，包含扩展头部

下一报头该字段用来指明报头后接的报文头部的类型，若存在扩展头，表示第一个扩展头的类型，否则表示其上层协议的类型，它是 IPv6 各种功能的核心实现方法

跳数限制该字段类似于 IPv4 中的 TTL，每次转发跳数减一，该字段达到 0 时包将会被丢弃

源地址标识该报文的来源地址

目的地址标识该报文的目的地址

【56】D

【解析】

19+5=24

【57-58】A B

【解析】

从 192.168.2.0 direct 这个信息可以看出只能是 R1 或者 R4.而从 192.168.3.0 通过 rip

学习到的情况，说明是 R1 的路由表。从 netxhop 都是 192.168.2.1 这个信息，说明是从 R4 通过的，也就是 R1 g0/0/1 这个链路故障了，对端是 R2 g0/0/2.

【59】C

【解析】

1518 个字节中，实际用于封装数据的部分只有 1500 字节，也就是 1500*8=12000bit。现在要传输 240000 个 bit，需要传输 240000/12000=20 次。 每一次传输需要的时间 =9.6us+(1518+8)*8/100*10^6(s)=9.6us+122.8us=131.68us.因此总的时间 =20*131.68=2633.6us=2.63ms

【60】A

【解析】

4B:5B 编码方案是把数据转换成 5 位符号,供传输。这些符号保持线路的交流(AC)平衡;

在传输中,其波形的频谱为最小。信号的直流(DC)分量变化小于额定中心点的 10%。

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。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。三种应用实例是 FDDI、100BASE－TX 和 100BASE－FX

【61】C

【解析】

二进制指数后退算法最大重试次数为 16.

【62】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，比如核电站，水坝，国家电网。

【63】B

【解析】

默认 vlan 指的是交换机初始就有的，通常 id 为 1，所有接口都处于这个 vlan 下，这就是为什么交换机上来就能用，还能互相通信。

【64】A

【解析】

跳频（Frequency-Hopping Spread Spectrum，FHSS）。

扩频技术的基本特征是使用比发送的信息数据速率高很多倍的伪随机码，将载有信息数据的基带信号的频谱进行扩展，形成宽带的低功率频谱密度的信号来发射。 它的特点是对无线噪声不敏感、产生的干扰小、安全性较高，但是占用带宽较高。增加带宽可以在低信噪比、等速率的情况下，提高数据传输的可靠性。

基本运作过程：发送端首先把信息数据调制成基带信号，然后进入载波频率调制阶段。此时载波频率受伪随机码发生器控制，在给定的某带宽远大于基带信号的频带内随机跳变，使基带信号带宽扩展到发射信号使用的带宽，然后跳频信号便由天线发送出去。 因此安全性较高、带宽消耗较大，占用了比传输信息带宽高许多倍的频率带宽。

【65】A

【解析】

zigbee 近距离。传输范围一般介于 10～100m 之间，在增加发射功率后，亦可增加到 1～3km。两个敏感度和发射功率都较高的 1 类设备相连接，射程可远高于一般水平的 100m，取决于应用所需要的吞吐量。有些设备在开放的环境中的射程能够高达 1km 甚至更高。

【66】D

【解析】

PCF 是选项，是用接入点 AP 集中控制整个 BsS 内的活动，因此自组网络就没有 PCF 子层。PCF 使用集中控制的接入算法，类似于探询的方法把发送数据权轮流交给各个站，从 111J 避免了碰撞的产生。对于时间敏感的业务，如分组话音，就应使用提供无争用服务的点协调功能 PCF。为了尽量避免碰撞，802.11 规定，所有的站在完成发送后，必须再等待一段很短的时间（继续监听）才能发送下一帧。这段时间通称为帧间间隔 IFs CntCrFramc space）。帧间间隔的长短取决于该站要发送的帧的类型。高优先级帧需要等待的时间较短，因此可优先获得发送权，但低优先级帧就必须等待较长的时间。若低优先级帧还没来得及发送而其他站的高优先级帧

已发送到媒体,则媒体变为忙态,那么低优先级帧就只能再推迟发送了,这样就减少了发生碰撞的机会。至于各种帧间间隔的具体长度,则取决于所使用的物理层特性。

【67】B

【解析】

raid1 利用 50%。

【68】D

【解析】

核心层：将分组从一个区域高速地转发到另一个区域。

汇聚层：策略控制。

接入层：用户接入。

【69】D

【解析】

需求分析的几点注意事项：任何网络都不可能是一张能够满足各项功能需求的万能网；采用合适的而不是最先进的网络设备，获得合适的而不是最高的网络性能；网络需求分析不能脱离用户、应用系统等现实因素；考虑网络的扩展性，极大地保护投资。

【70】C

【解析】

基本工期 7 天，因此保持 C 不变。AB 只能串行工作，由于 A 需要 4 人，因此考虑 B 能否增加人数,降低工作时间,B 的工作量是 5*3=15 人天。因此考虑 4 人的情形下,可以实现 4*4=16 人天。因此在 B 工作增加 1 人即可实现，两个任务流 ab 与 C 并行，因此总投入 7 人。

【71-75】ADAAC

试题一

【问题 1】

（1）A

（2）C

【问题 2】

（3）DHCP 采用全局地址池方式

（4）pool

（5）192.168.100.1

【问题 3】

（6）创建虚拟接口

（7）3002

（8）配置 3G 接口为备份接口，优先级默认为 0

（9）wcdma-only

（10）3gprofile

（11）100

【问题 4】

（12） A

（13）数据加密传输及身份认证

解析：从 OSI 七层网络结构的角度来看：

- 在物理层采用防窃听技术来加强通信线路的安全；
- 在数据链路层使用通信保密技术进行链路加密，使用 L2TP、PPTP 来实现二层隧道通信；
- 在网络层采用防火墙来处理信息内外网络边界的流动，利用 IPSec 建立透明的安全加密信道；
- 在传输层使用 SSL 对底层安全服务进行抽象和屏蔽；

试题二

【问题 1】

（1）RAID10

（2）RAID1

（3）2 或者 3

（4）0

（5）RAID5

（6）1

【问题 2】

（7）50

（8）75

（9）图 2-2

（10）图 2-3

解析：

小 io 的数据库类型操作，建议采用 RAID10,而大型文件存储，数据仓库，则从空间利用的角度，可以采用 RAID5

【问题 3】

（11）B

（12）C

（13）A

（14）B 13-14 可交换位置

试题三

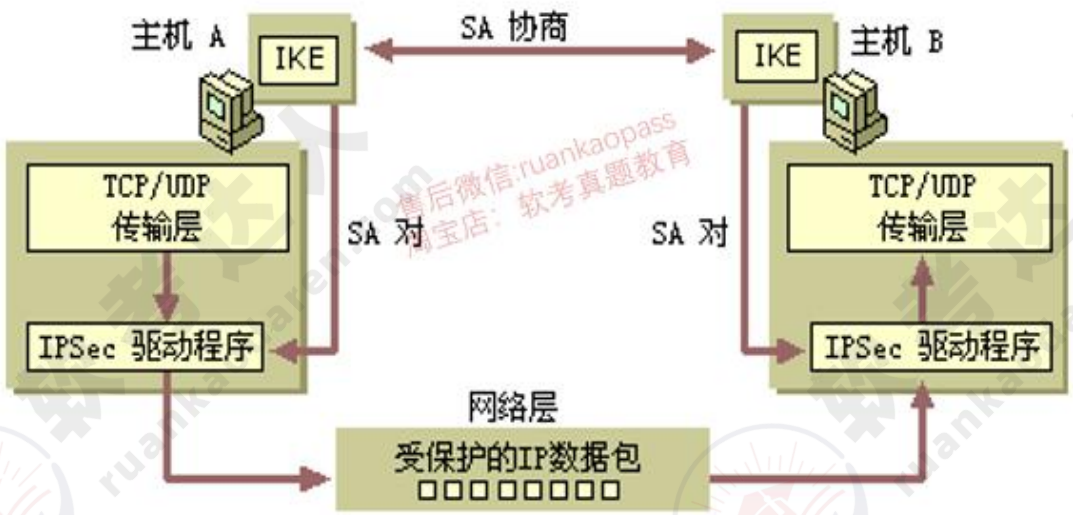
【问题 1】

（1）A

（2）B

（3）C

解析：



SAKMP/IKE 第一阶段称为 ISAKMP/IKE 的管理连接阶段. 使用双向的 UDP 端口为 500 的数据连接, 来共享 IPSEC 消息.

第一阶段

有主模式和积极模式 2 种。

主模式执行 3 步, 6 个数据包的双向交换. 过程如下:

1. 对等体间协商如何来保护管理连接. (使用加密变换集来保护)

2. 对等体间使用 DH 算法来共享密钥以及保护连接.

3. 对等体间进行彼此的验证.

积极模式执行的过程:

1. 交换保护管理连接的策略, DH 算法建立公钥/密钥对并在对等体间进行认证.

2. 对收到的数据包做验证, DH 算法来共享加密的密钥, 并查看连接是否成功建立.

PS:除了预共享密钥认证外. 其他的认证方式默认为主模式.

第二阶段

快速模式

协商 IPSEC SA 使用的安全参数, 创建 IPSEC SA, 使用 AH 或 ESP 来加密 IP 数据流

【问题 2】

（4）C

（5）E

解析：

IPSec 策略配置：

- 创建 IPSec 策略
- 创建筛选器列表
- 配置隧道规则
- 进行策略指派

【问题 3】

（6）192.168.5.2 255.255.255.255

（7）192.168.6.3 255.255.255.255

（8）任何

【问题 4】

（9）202.1.1.2

（10）将图 3-5 中的“接送受不安全的通信，但始终用 Ipsec 响应”前的选中“”去掉。

试题四

【问题 1】

（1）system-view

（2）RouterA

（3）IPv6

（4）24 或者 255.255.255.0

（5）IPv6

【问题 2】

(6)创建隧道接口 tunnel 0/0/1

(7) tunnel-protocol

(8) auto-tunnel

(9) enable

(10)为接口设置 IPv6 地址

(11)指定隧道的源接口为 S0

【问题 3】

（12）A

（13）存在，因为使用的隧道是 IPv6 兼容 IPv4 地址方案，因此对于 IPv4 地址会通过 ipv6 地址前 96 位填充 0，后 32 位为对应的 IPv4 地址即可。