在程序运行过程中，CPU 需要将指令从内存中取出并加以分析和执行。CPU 依据（1）来区分在内存中以二进制编码形式存放的指令和数据。

(1)A.指令周期的不同阶段　　B.指令和数据的寻址方式

C.指令操作码的译码结果　　D.指令和数据所在的存储单元

【答案】B

【解析】

指令和数据均存放在内存中，通常由 PC（程序计数器）提供存储单元地址取出的是指令，由指令地址码部分提供存储单元地址取出的是数据。因此通过不同的寻址方式来区别指令和数据。

计算机在一个指令周期的过程中，为从内存读取指令操作码，首先要将（2）的内容送到地址总线上。

(2)A.指令寄存器（IR）　　B.通用寄存器（GR）

C.程序计数器（PC）　　D.状态寄存器（PSW）

【答案】C

【解析】

为了保证程序能够连续地执行下去，CPU 必须具有某些手段来确定下一条指令的地址。程序计数器存放的是下一条指令的地址。

设 16 位浮点数，其中阶符 1 位、阶码值 6 位、数符 1 位，尾数 8 位。若阶码用移码表示，尾数用补码表示，则该浮点数所能表示的数值范围是（3）。

(3)A.-264~（1-2-8）264　　B.-263~（1-2-8）263

C.-（1-2-8）264~（1-2-8）264　　D.-（1-2-8）263~（1-2-8）263

【答案】B

【解析】

如果浮点数的阶码(包括 1 位阶符)用 R 位的称码表示，尾数(包括 1 位数符)用 M 位的补码表示，则浮点数表示的数值范围如下。

最大正数：$+\left(1-2^{-M+1}\right)\times 2^{(2^{R-1}-1)}$，最小负数$-1\times 2^{(2^{R-1}-1)}$

已知数据信息为16位，最少应附加（4）位校验位，以实现海明码纠错。

(4)A.3　　B.4　　C.5　　D.6

【答案】C

【解析】

校验码个数为K，2的K次方个校验信息，1个校验信息用来指出没有错误，其余（2K)-1个指出错误发生在那一位，但也可能是校验位错误，所以满足m+k+1<=2k

将一条指令的执行过程分解为取指、分析和执行三步，按照流水方式执行，若取指时间t取指=4△t、分析时间t分析=2△t、执行时间t执行=3△t，则执行完100条指令，需要的时间为（5）△t。

(5)A.200　　B.300　　C.400　　D.405

【答案】D

【解析】

流水线执行时间的计算的算法：

T＝第一条指令执行所需时间+（指令条数－1（指令最长所需的T，此题是4s））×流水线周期

在敏捷过程的开发方法中，（6）使用了迭代的方法，其中，把每段时间（30天）一次的迭代称为一个“冲刺”，并按需求的优先级别来实现产品，多个自组织和自治的小组并行地递增实现产品。

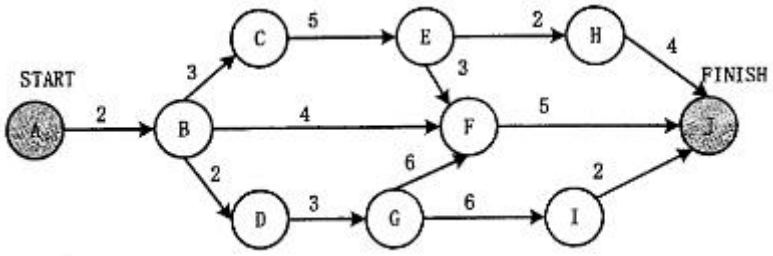
(6)A.极限编程XP　　B.水晶法　　C.并列争球法　　D.自适应软件开发

【答案】C

【解析】

并列争球法使用迭代的方法，把每30天一次的迭代称为一个冲刺，按需求的优先级别来实现产品。多个自组织的小组并行地递增实现产品。协调通过简短的日常会议来进行。

某软件项目的活动图如下图所示，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，边上的数字表示相应活动的持续时间（天），则完成该项目的最少时间为（7）天。活动BC和BF最多可以晚开始（8）天而不会影响整个项目的进度。



(7)A.11　　B.15　　C.16　　D.18

(8)A.0 和 7　　B.0 和 11　　C.2 和 7　　D.2 和 11

【答案】D　A

【解析】

在网络图中的某些活动可以并行地进行，所以完成工程的最少时间是从开始顶点到结束顶点的最长路径长度，从开始顶点到结束顶点的最长（工作时间之和最大）路径为关键路径，关键路径上的活动为关键活动。

假设系统有 n 个进程共享资源 R，且资源 R 的可用数为 3，其中 n≥3 。若采用 PV 操作，则信号量 S 的取值范围应为（9）。

(9)A.-1～n-1　　B.-3～3　　C.-（n-3）～3　　D.-（n-1）～1

【答案】C

【解析】

比如，有三个某类资源，假设四个进程 A、B、C、D 要用该类资源，最开始 S=3，当 A 进入，S=2，当 B 进入 S=1，当 C 进入时 S=0，表明该类资源刚好用完，D 进入 S=-1，表明有一个进程被阻塞了，当 A 用完该类资源时，进行 V 操作，S=0，释放该类资源，这时候，S=0，表明还有进程阻塞在该类资源上，然后再唤醒一个。

甲、乙两厂生产的产品类似，且产品都拟使用“B″商标。两厂于同一天向商标局申请商标注册，且申请注册前两厂均未使用“B″商标。此情形下，（10）能核准注册。

(10)A.甲厂　　B.由甲、乙厂抽签确定的厂　　C.乙厂　　D.甲、乙两厂

【答案】B

【解析】

商标权取得的原则有以下三种：

（1）使用原则

使用原则，即使用取得商标权原则，是指商标权因商标的使用而自然产生，商标权根据商标使用事实而得以成立。

（2）注册原则

注册原则，即注册取得商标权原则，是指商标权因注册事实而成立，只有注册商标才能取得商标权。

（3）混合原则

混合原则，即折衷原则，是指在确定商标权的成立时，兼顾使用与注册两种事实，商标权既可因注册而产生，也可因使用而成立。

能隔离局域网中广播风暴、提高带宽利用率的设备是（11）。

(11)A.网桥　　B.集线器　　C.路由器　　D.交换机

【答案】C

【解析】

广播域被认为是OSI中的第二层概念，所以像Hub，交换机等这些第一，第二层设备连接的节点被认为都是在同一个广播域。而路由器，第三层交换机则可以划分广播域，即可以连接不同的广播域。

点对点协议PPP中LCP的作用是（12）。

(12)A.包装各种上层协议　　B.封装承载的网络层协议

C.把分组转变成信元　　D.建立和配置数据链路

【答案】D

【解析】

PPP协议是一种点到点的链路层协议，它提供了点到点的一种封装、传递数据的一种方法。PPP协议一般包括三个协商阶段：LCP（链路控制协议）阶段，认证阶段，NCP（网络层控制协议）阶段。拨号后，用户计算机和接入服务器在LCP阶段协商底层链路参数，然后在认证阶段进行用户计算机将用户名和密码发送给接入服务器认证，接入服务器可以进行本地认证，可以通过RADIUS协议将用户名和密码发送给AAA服务器进行认证。认证通过后，在NCP（IPCP）协商阶段，接入服务器给用户计算机分配网络层参数如IP地址等。

TCP/IP网络中的（13）实现应答、排序和流控功能。

(13)A.数据链路层　　B.网络层　　C.传输层　　D.应用层

【答案】C

【解析】

传输层提供应用程序间的通信。（1）格式化信息流；（2）提供可靠传输。

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 1 位终止位，每秒钟传送 100 个字符，采用 DPSK 调制，则码元速率为（14），有效数据速率为（15）。

(14)A.200 波特　　B.500 波特　　C.1000 波特　　D.2000 波特

(15)A.200b/s　　B.500b/s　　C.700b/s　　D.1000b/s

【答案】C　C

【解析】

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 1 位终止位，每秒钟传送 100 个字符，采用 DPSK 调制，则码元速率为 1000 波特，有效数据速率为是 700bps。

E1 载波的数据速率是（16）Mb/s，E3 载波的数据速率是（17）Mb/s。

(16)A.1.544　　B.2.048　　C.8.448　　D.34.368

(17)A.1.544　　B.2.048　　C.8.448　　D.34.368

【答案】B　D

【解析】

E1 的一个时分复用帧（其长度 T=125us）共划分为 32 相等的时隙，时隙的编号为 CH0~CH31。其中时隙 CH0 用作帧同步，时隙 CH16 用来传送信令，剩下 CH1~CH15 和 CH17~CH31 共 30 个时隙用作 30 个话路。每个时隙传送 8bit，因此共用 256bit。每秒传送 8000 个帧，因此 PCM 一次群 E1 的数据率就是 2.048Mbit/s。

E3 就是 16 个 E1 复用。

IPv6 的链路本地地址是在地址前缀 1111 1110 10 之后附加（18）形成的。

(18)A.IPv4 地址　　B.MAC 地址　　C.主机名　　D.随机产生的字符串

【答案】B

【解析】

链路本地地址是使用链路本地前缀 FE80::/10 的 IPv6 单播地址(1111 1110 10)和在已

修改 EUI-64 格式的接口标识符在所有接口可以自动地配置。

连接终端和数字专线的设备 CSU/DSU 被集成在路由器的（19）端口中。

(19)A.RJ-45 端口　　B.同步串口　　C.AUI 端口　　D.异步串口

【答案】B

【解析】

CSU/DSU 是用于连接终端和数字专线的设备，而且 CSU/DSU 属于 DCE 数据通信设备，目前 CSU/DSU 通常都被集成在路由器的同步串口之上。

下面哪个协议可通过主机的逻辑地址查找对应的物理地址？（20）。

(20)A.DHCP　　B.SMTP　　C.SNMP　　D.ARP

【答案】D

【解析】

已经知道一个主机的 IP 地址，需要找出其对应的物理地址。或者反过来，已经知道了物理地址，需要找出相应的 IP 地址。地址解析协议 ARP 和逆地址解析协议 RARP 就是解决这样的问题的。

下面的应用层协议中通过 UDP 传送的是（21）。

(21)A.SMTP　　B.TFTP　　C.POP3　　D.HTTP

【答案】B

【解析】

TFTP 是简单文件传输协议，传输层的承载协议是 UDP。

代理 ARP 是指（22）。

(22)A.由邻居交换机把 ARP 请求传送给远端目标

B.由一个路由器代替远端目标回答 ARP 请求

C.由 DNS 服务器代替远端目标回答 ARP 请求

D.由 DHCP 服务器分配一个回答 ARP 请求的路由器

【答案】B

【解析】

路由器从开启 ARP 代理的接口收到一个 ARP 请求，并且该目标 IP 地址是自己可达的，并且这个对应路由条目的出接口不是收到该 ARP 请求的接口，那么路由器将执行代理 ARP 功能。

如果路由器收到了多个路由协议转发的、关于某个目标的多条路由，它如何决定采用哪个路由？（23）。

(23)A.选择与自己路由协议相同的　　B.选择路由费用最小的

C.比较各个路由的管理距离　　D.比较各个路由协议的版本

【答案】C

【解析】

一条路由比其他的路由拥有更高优先权的概念叫做管理距离 AD。主要是比较不同路由协议有多条路径到达目的网络的参数，AD 值越小，就表示这条路由可信度级别就越高。AD 为 0，优先级最高。数字是介于 0-255 之间，255 表示这路由最不被信任。

下面的选项中属于链路状态路由选择协议的是（24）。

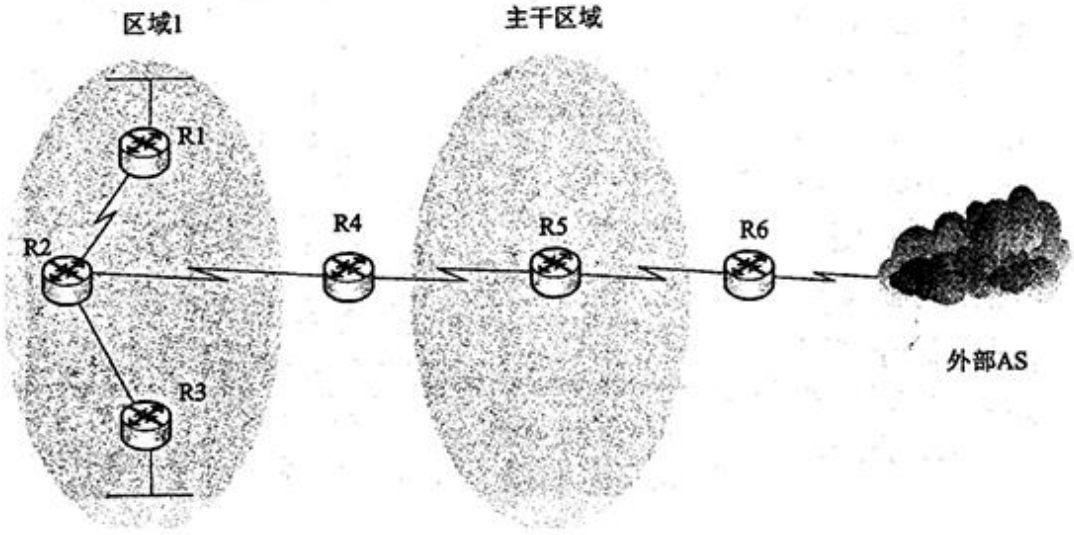
(24)A.OSPF　　B.IGRP　　C.BGP　　D.RIPv2

【答案】A

【解析】

运行链路状态路由协议的路由器，在相互学习路由之间，会首先向自己的邻居路由器学习整个网络的拓扑结构，在自己的内存中建立一个拓扑表，然后使用最短路径优先 SPF 算法，从自己的拓扑表里计算出路由来。OSPF 是典型的链路状态路由选择协议。

下面的 OSPF 网络由多个区域组成。在这些路由器中，属于主干路由器的是（25），属于自治系统边界路由器（ASBR）的是（26）。



(25)A.R1　　B.R2　　C.R3　　D.R4

(26)A.R3　　B.R4　　C.R5　　D.R6

【答案】D　D

【解析】

主干路由器是指至少有一个接口定义为属于主干区域的路由器。任何一个与主干区域互联的 ABR 或者 ASBR 也将成为主干路由器。

AS 边界路由器是与 AS 外部的路由器互相交换路由信息的 OSPF 路由器。该路由器在 AS 内部通告其所得到的 AS 外部路由信息，这样 AS 内部的所有路由器都知道 AS 边界路由器的路由信息。

RIPv2 与 RIPv1 相比，它改进了什么？（27）。

(27)A.RIPv2 的最大跳数扩大了，可以适应规模更大的网络

B.RIPv2 变成无类别的协议，必须配置子网掩码

C.RIPv2 用跳数和带宽作为度量值，可以有更多的选择

D.RIPv2 可以周期性地发送路由更新，收敛速度比原来的 RIP 快

【答案】B

【解析】

RIPv1 和 v2 版本的区别， RIPv1 是有类别路由协议，它只支持以广播方式发布协议报文。RIPv1 的协议报文无法携带掩码信息，它只能识别 A、B、C 类这样的标准分类网段的路由，RIPv2 是一种无类别路由协议。使用 224.0.0.9 的组播地址。支持 MD5 认证。

在采用CRC校验时，若生成多项式为G（X）=X5+X2+X+1，传输数据为1011110010101时，生成的帧检验序列为（28）。

(28)A.10101　　B.01101　　C.00000　　D.11100

【答案】C

【解析】

CRC码利用循环码的误码检测特性进行误码检测，它是从循环差错控制编码中分出的一类检错码。循环码的已编码码字可被生成多项式g(x)整除。接收端可以利用这一特点进行检错，若收码字不能被g(x)整除，则有错。

要计算CRC校验码，需根据CRC生成多项进行。例如：原始报文为11001010101，其生成多项式为：X5+X2+X+1。在计算时，是在原始报文的后面添加若干个0（个数为生成多项式的最高次幂数，它也是最终校验位的位数。上式中，校验位数应该为5）作为被除数，除以生成多项式所对应的二进制数（由生成多项式的幂次决定，此题中除数应该为100111），最后使用模除，得到的余数为校验码。

结构化布线系统分为六个子系统，其中干线子系统的作用是（29）。

(29)A.连接各个建筑物中的通信系统

B.连接干线子系统和用户工作区

C.实现中央主配线架与各种不同设备之间的连接

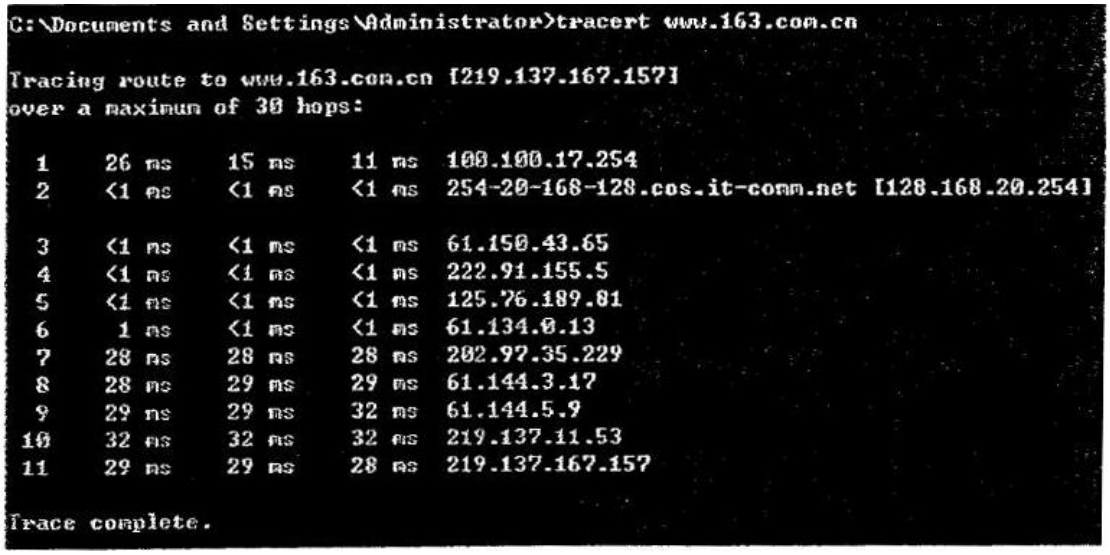
D.实现各楼层设备间子系统之间的互连

【答案】D

【解析】

干线子系统：就是将接入层交换机连接到分布层（或核心层）交换机的网络线路，由于其通常是顺着大楼的弱电井而下，是与大楼垂直的，因此也称为垂直子系统。

Windows命令tracert www.163.com.cn显示的内容如下，那么本地默认网关的IP地址是（30），网站www.163.com.cn的IP地址是（31）。



(30)A.128.168.20.254　　B.100.100.17.254

C.219.137.167.157　　D.61.144.3.17

(31)A.128.168.20.254　　B.100.100.17.254

C.219.137.167.157　　D.61.144.3.17

【答案】B　C

【解析】

tracert 也被称为 Window 路由跟踪实用程序,在命令提示符(cmd)中使用 tracert 命令可以用于确定 IP 数据包访问目标时所选择的路径。

在 Linux 系统中，要查看如下输出，可使用命令（32）。

```
eth0 Link encap:Ethernet HWaddr 00:20:5C:00:78:33
inet addr:192.168.0.5 Beast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9625272 errors:0 dropped:0 overruns:0 frame:0
TX packets:6997276 errors:0 dropped:0 overruns:0 frame:0
collisions:0 txqueuelen:100
interrupt:19 Base address:0xc800
```

(32)A.[root@localhost]#ifconfig　　B.[root@localhost]#ipconfig eth0

C.[root@localhost]#ipconfig　　D.[root@localhost]#ifconfig eth0

【答案】D

【解析】

ifconfig 是 linux 中用于显示或配置网络设备（网络接口卡）的命令。

当DHCP服务器拒绝客户端的IP地址请求时发送（33）报文。

(33)A.DhcpOffer　　B.DhcpDecline　　C.DhcpAck　　D.DhcpNack

【答案】D

【解析】

当DHCP服务器拒绝客户端的IP地址请求对发送DhcpNack报文。

在进行域名解析过程中，当主域名服务器查找不到IP地址时，由（34）负责域名解析。

(34)A.本地缓存　　B.辅域名服务器　　C.根域名服务器　D.转发域名服务器

【答案】C

【解析】

根域名服务器知道所有顶级域名服务器的域名和IP地址。只要本地域名服务器无法解析的话，都要先求助于根域名服务器。

在建立TCP连接过程中，出现错误连接时，（35）标志字段置“1”。

(35)A.SYN　　B.RST　　C.FIN　　D.ACK

【答案】B

【解析】

复位RST：RST=1，表明TCP连接出现严重错误，需要释放连接，重新建立。

POP3服务器默认使用（36）协议的（37）的端口。

(36)A.UDP　　B.TCP　　C.SMTP　　D.HTTP

(37) A.21　　B.25　　C.53　　D.110

【答案】B　D

【解析】

POP3服务器默认使用TCP协议的110的端口。

当客户端收到多个DHCP服务器的响应时，客户端会选择（38）地址作为自己的IP地址。

(38)A.最先到达的　　B.最大的　　C.最小的　　D.租期最长的

【答案】A

【解析】

当客户端收到多个 DHCP 服务器的响应时，客户端会选择最先到达的地址作为自己的 IP 地址。

在 Windows 的 DOS 窗口中键入命令

C：\> nslookup

> set type=a

> xyz.com.cn

这个命令序列的作用是（39）。

(39)A.查询 xyz.com.cn 的邮件服务器信息

B.查询 xyz.com.cn 到 IP 地址的映射

C.查询 xyz.com.cn 的资源记录类型

D.显示 xyz.com.cn 中各种可用的信息资源记录

【答案】B

【解析】

每一个 DNS 服务器包含了它所管理的 DNS 命名空间的所有资源记录。资源记录包含和特定主机有关的信息，如 IP 地址、提供服务的类型等等。常见的资源记录类型有：SOA（起始授权结构）、A（主机）、NS（名称服务器）、CNAME（别名）和 MX（邮件交换器）。

A 记录：也称为主机记录，是 DNS 名称到 IP 地址的映射，用于正向解析。

下面是 DHCP 协议工作的 4 种消息，正确的顺序应该是（40）。

①DHCP Discovery

②DHCP Offer

③DHCP Request

④DHCP Ack

(40)A.①③②④　　B.①②③④　　C.②①③④　　D.②③①④

【答案】B

【解析】

DHCP 协议采用 UDP 作为传输协议，主机发送请求消息到 DHCP 服务器的 67 号端口，DHCP 服务器回应应答消息给主机的 68 号端口。

DHCP Client 以广播的方式发出 DHCP Discover 报文。

所有的 DHCP Server 都能够接收到 DHCP Client 发送的 DHCP Discover 报文，所有的 DHCP Server 都会给出响应，向 DHCP Client 发送一个 DHCP Offer 报文。

DHCP Client 只能处理其中的一个 DHCP Offer 报文，一般的原则是 DHCP Client 处理最先收到的 DHCP Offer 报文。

DHCP Client 会发出一个广播的 DHCP Request 报文，在选项字段中会加入选中的 DHCP Server 的 IP 地址和需要的 IP 地址。

DHCP Server 收到 DHCP Request 报文后，判断选项字段中的 IP 地址是否与自己的地址相同。如果不相同，DHCP Server 不做任何处理只清除相应 IP 地址分配记录；如果相同，DHCP Server 就会向 DHCP Client 响应一个 DHCP ACK 报文，并在选项字段中增加 IP 地址的使用租期信息。

DHCP Client 接收到 DHCP ACK 报文后，检查 DHCP Server 分配的 IP 地址是否能够使用。如果可以使用,则 DHCP Client 成功获得 IP 地址并根据 IP 地址使用租期自动启动续延过程；如果 DHCP Client 发现分配的 IP 地址已经被使用,则 DHCP Client 向 DHCP Server 发出 DHCP Decline 报文，通知 DHCP Server 禁用这个 IP 地址，然后 DHCP Client 开始新的地址申请过程。

DHCP Client 在成功获取 IP 地址后，随时可以通过发送 DHCP Release 报文释放自己的 IP 地址，DHCP Server 收到 DHCP Release 报文后，会回收相应的 IP 地址并重新分配。

在 Linux 中，（41）命令可将文件以修改时间顺序显示。

(41)A. ls -a　　B. ls -b　　C. ls -c　　D. ls -d

【答案】C

【解析】

在 Linux 中，ls -c 命令可将文件以修改时间顺序显示。

要在一台主机上建立多个独立域名的站点，下面的方法中（42）是错误的。

(42)A.为计算机安装多块网卡　　B.使用不同的主机头名

C.使用虚拟目录　　D.使用不同的端口号

【答案】C

【解析】

IIS 通过分配 TCP 端口、IP 地址和主机头名来在一台服务器上运行多个网站。虚拟主机

之间相互独立，由用户自行管理。采用这种技术可以节约硬件投资、节省空间，降低成本。

（1）基于附加 TCP 端口架设多个 Web 网站。

使用格式为 http://域名:端口的网址来访问的网站实际上是利用 TCP 端口号，在同一服务器上架设不同的 Web 网站。例如 http://www.csai.cn:8080。

（2）基于不同的 IP 地址架设多个网站

将每个网站绑定到不同的 IP 地址，以确保每个网站域名对应于独立的 IP 地址。

（3）基于主机头名架设多个 Web 网站

由于传统的 IP 虚拟主机浪费 IP 地址，实际应用中更倾向于采用非 IP 虚拟主机技术，也就是把多个域名的主机头名绑定到同一 IP。前提条件就是在 DNS 服务器上将多个域名映射到同一 IP 地址。一旦来自客户端的 Web 访问请求到达服务器，服务器将使用 HTTP 头中传递的主机头名来确定客户请求的是哪个网站。

下面不属于数字签名作用的是（43）。

(43)A.接收者可验证消息来源的真实性　　B.发送者无法否认发送过该消息

C.接收者无法伪造或篡改消息　　D.可验证接收者的合法性

【答案】D

【解析】

数字签名能够实现三点功能：

（1）接收者能够核实发送者对报文的签名，也就是说，接收者能够确信该报文确实是发送者所发送的。其他人无法伪造对报文的签名，这就叫做报文鉴别。

（2）接收者确信所收到的数据和发送者发送的完全一样，没有被篡改过。这就叫做报文的完整性。

（3）发送者事后不能抵赖对报文的签名。这就做不可否认性。

下面可用于消息认证的算法是（44）。

(44)A.DES　　B.PGP　　C.MD5　　D.KMI

【答案】C

【解析】

报文摘要算法是精心选择的一种单向函数，我们很容易计算出一个长报文 X 的报文摘要 H，但是想从报文摘要 H 反过来找到原始报文 X，实际上是不可能的。另外，找到两个任意

的报文，使得他们具有相同的报文摘要，也是不可能的。

RFC 1321 提出的报文摘要算法 MD5 已经获得广泛的应用。它可对任意长度的报文进行运算，得出 128 位的 MD5 报文摘要代码。另一种标准是安全散列算法 SHA，和 MD5 相似，但码长为 160 位，SHA 比 MD5 更安全，但计算的效率不如 MD5。

DES 加密算法的密钥长度为 56 位，三重 DES 的密钥长度为（45）位。

(45)A.168　　B.128　　C.112　　D.56

【答案】C

【解析】

3DES 算法：密码学中，3DES 是三重数据加密算法通称。它相当于是对每个数据块应用三次 DES 加密算法。其中第一次和第三次密钥一样，所以是 112 位的密钥长度。由于计算机运算能力的增强，原版 DES 密码的密钥长度变得容易被暴力破解；3DES 即是设计用来提供一种相对简单的方法，即通过增加 DES 的密钥长度来避免类似的攻击，而不是设计一种全新的块密码算法。

在 Windows Server 2003 中，（46）组成员用户具有完全控制权限。

(46)A.Users　　B.Power Users　　C.Administrators　　D.Guests

【答案】C

【解析】

在 Windows Server 2003 中，Administrator 组成员用户具有完全控制权限。

SNMP 协议中网管代理使用（47）操作向管理站发送异步事件报告。

(47) A.trap　　B.set　　C.get　　D.get-next

【答案】A

【解析】

SNMP 使用的是无连接的 UDP 协议，因此在网络上传送 SNMP 报文的开销很小，但 UDP 是不保证可靠交付的。同时 SNMP 使用 UDP 的方法有些特殊，在运行代理程序的服务器端用 161 端口来接收 Get 或 Set 报文和发送响应报文（客户端使用临时端口），但运行管理程序的客户端则使用熟知端口 162 来接收来自各代理的 Trap 报文。

当发现主机受到 ARP 攻击时需清除 ARP 缓存，使用的命令是（48）。

(48)A.arp －a　　B.arp －s　　C.arp －d　　D.arp -g

【答案】C

【解析】

当发现主机受到 ARP 攻击时需清除 ARP 缓存，使用的命令是 arp-d。

从 FTP 服务器下载文件的命令是（49）。

(49)A.get　　B.dir　　C.put　　D.push

【答案】A

【解析】

从 FTP 服务器下载文件的命令是 get，上传是 put。

由于内网 P2P、视频 / 流媒体、网络游戏等流量占用过大，影响网络性能，可以采用（50）来保障正常的 Web 及邮件流量需求。

(50)A.使用网闸　　B.升级核心交换机

C.部署流量控制设备　　D.部署网络安全审计设备

【答案】C

【解析】

由于内网 P2P、视频 / 流媒体、网络游戏等流量占用过大，影响网络性能，可以采用部署流量控制设备来保障正常的 Web 及邮件流量需求。

ISP 分配给某公司的地址块为 199.34.76.64/28，则该公司得到的 IP 地址数是（51）。

(51)A.8　　B.16　　C.32　　D.64

【答案】B

【解析】

地址块为 199.34.76.64/28，说明网络位占 28 位，主机位占 4 位，那么 IP 地址数是 16。

下面是路由表的 4 个表项，与地址 220.112.179.92 匹配的表项是（52）。

(52)A.220.112.145.32/22　　B.220.112.145.64/22

C.220.112.147.64/22　　D.220.112.177.64/22

【答案】D

【解析】

下面是路由表的 4 个表项，与地址 220.112.179.92 匹配的表项是具有最大相同位数的选项。

下面 4 个主机地址中属于网络 110.17.200.0/21 的地址是（53）。

(53)A.110.17.198.0　　B.110.17.206.0

C.110.17.217.0　　D.110.17.224.0

【答案】B

【解析】

110.17.200.0/21 的范围是：

110.17.11001 000——110.17.11001 111，所以答案选择 B。

某用户得到的网络地址范围为 110.15.0.0～110.15.7.0，这个地址块可以用（54）表示，其中可以分配（55）个可用主机地址。

(54)A.110.15.0.0/20　　B.110.15.0.0/21

C.110.15.0.0/16　　D.110.15.0.0/24

(55)A.2048　　B.2046　　C.2000　　D.2056

【答案】B　B

【解析】

110.15.0.0～110.15.7.0，8 个子网做汇聚，汇聚后掩码长度是 21 位，那么主机位就是 11 位，可以容纳 211-2=2046 个地址。

下面的提示符（56）表示特权模式。

(56)A.>　　B.#　　C.（config）#　　D.!

【答案】B

【解析】

用户模式>：在 Cisco 设备启动工作完成之后，我们就会进入用户模式，只允许基本的监测命令，比如 PING 其他的网络设备等。在这种模式下不能改变路由器的配置。

特权模式#：用户模式下敲入 enable 命令，进入特权模式，在特权模式下，我们可以使

用比用户模式更多的命令，可以使用 SHOW 命令来观察设备的状况和我们所做的配置。在特权模式下不能对设备进行配置。

全局模式（config）#：在特权模式下，我们键入 config terminal 命令就进入全局模式，全局模式下可以网络设备进行配置，在全局模式下所做的配置，对整个设备都有效。

如果对某个接口进行单独的配置，就需要从全局模式进入这个接口子模式。

把路由器当前配置文件存储到 NVRAM 中的命令是（57）。

(57)A.Router（confg）#copy current to starting

B.Router#copy starting to running

C.Router（config）#copy running-config starting-config

D.Router#copy run startup

【答案】D

【解析】

把路由器当前配置文件存储到 NVRAM 中的命令是 Router#copy run startup。

如果路由器显示“Serial 1 is down，line protocol is down”故障信息，则问题出在 OSI 参考模型的（58）。

(58)A.物理层　　B.数据链路层　　C.网络层　　D.会话层

【答案】A

【解析】

如果路由器显示“Serial 1 is down，line protocol is down”故障信息，则问题出在 OSI 参考模型的物理层。

下面的交换机命令中（59）为端口指定 VLAN。

(59)A.S1（config-if）# vlan-menbership static

B.S1（config-if）# vlan database

C.S1（config-if）# switchport mode access

D.S1（config-if）#switchport access vlan 1

【答案】D

【解析】

在默认配置下，所有的接口都处于可用状态并且都属于 VLAN1。通常在配置 VLAN 时采用的是静态设置法，也就是手动在交换机上直接将某个端口分配给一个 VLAN：

S1（config-if）#switchport access vlan 1

STP 协议的作用是（60）。

(60)A.防止二层环路　B.以太网流量控制　　C.划分逻辑网络　D.基于端口的认证

【答案】A

【解析】

产生交换环路会造成什么样的危害呢？

（1）广播风暴：广播风暴就由于自然界的飓风一样，是网络设计者都要极力避免的灾难之一，它可以在短时间内无情地摧毁整个网络，使得交换机处于极度忙碌的状态，交换机所做的工作就是在转发广播，而正常的网络流量将会被阻塞。而在用户的主机上，由于网卡被迫不断的处理大量的广播帧，也呈现网络传输速率缓慢或根本无法连通的现象。

广播风暴的原因除了个别网卡出现故障以外，交换环路也是一个重要的原因。另外也不是所有的广播都是不正常的，有一些应用必须用到广播，比如 ARP 解析。

（2）MAC 地址表不稳定。两个方向上的广播造成。

我们要利用生成树协议 STP 来解决这个问题。

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于在网络中建立树形拓扑，消除网络中的环路，并且可以通过一定的方法实现路径冗余，但不是一定可以实现路径冗余。生成树协议适合所有厂商的网络设备，在配置上和体现功能强度上有所差别，但是在原理和应用效果是一致的。

VLAN 之间通信需要（61）的支持。

(61)A.网桥　　B.路由器　　C.VLAN 服务器　D.交换机

【答案】B

【解析】

想让两台属于不同 VLAN 主机之间能够通信，就必须使用三层设备为 VLAN 之间做路由。

以太网中出现冲突后，发送方什么时候可以再次尝试发送？（62）。

(62)A.再次收到目标站的发送请求后

B.在 JAM 信号停止并等待一段固定时间后

C.在 JAM 信号停止并等待一段随机时间后

D.当 JAM 信号指示冲突已经被清除后

【答案】C

【解析】

如果在发送数据的过程中检测出冲突，为了解决信道争用冲突，发送节点要进入停止发送数据、随机延迟后重发的流程。

网桥怎样知道网络端口连接了哪些网站？（63）。当网桥连接的局域网出现环路时怎么办？（64）。

(63)A.如果从端口收到一个数据帧，则将其目标地址记入该端口的数据库

B.如果从端口收到一个数据帧，则将其源地址记入该端口的数据库

C.向端口连接的各个站点发送请求以便获取其 MAC 地址

D.由网络管理员预先配置好各个端口的地址数据库

(64)A.运行生成树协议阻塞一部分端口

B.运行动态主机配置协议重新分配端口地址

C.通过站点之间的协商产生一部分备用端口

D.各个网桥通过选举产生多个没有环路的生成树

【答案】B　A

【解析】

网桥如果从端口收到一个数据帧，则将其源地址记入该端口的数据库。形成 MAC 和端口的对应表。当网桥连接的局域网出现环路时，运行生成树协议阻塞一部分端口。

IEEE802.11 标准采用的工作频段是（65）。

(65)A.900MHz 和 800MHz　B.900MHz 和 2.4GHz　C.5GHz 和 800MHz　D.2.4GHz 和 5GHz

【答案】D

【解析】

IEEE802.11 标准采用的工作频段是 2.4GHz 和 5GHz。

IEEE802.11MAC 子层定义的竞争性访问控制协议是（66）。

(66)A.CSMA/CA　　B.CSMA/CB　　C.CSMA/CD　　D.CSMA/CG

【答案】A

【解析】

CSMA/CD 协议已经成功应用于是用有线连接的局域网，但在无线局域网的环境下，不能简单的搬用 CSMA/CD 协议，特别是冲突检测部分。IEEE 802.11MAC 子层定义的竞争性访问控制协议是 CSMA/CA。

无线局域网的新标准 IEEE802.11n 提供的最高数据速率可达到（67）Mb/s。

(67)A.54　　B.100　　C.200　　D.300

【答案】D

【解析】

无线局域网的新标准 IEEE802.11n 提供的最高数据速率可达到 300Mb/S。

在网络设计和实施过程中要采取多种安全措施，下面的选项中属于系统安全需求措施的是（68）。

(68)A.设备防雷击　　B.入侵检测　　C.漏洞发现与补丁管理　　D.流量控制

【答案】C

【解析】

在网络设计和实施过程中要采取多种安全措施，下面的选项中属于系统安全需求措施的是漏洞发现与补丁管理。

在网络的分层设计模型中，对核心层工作规程的建议是（69）。

(69)A.要进行数据压缩以提高链路利用率

B.尽量避免使用访问控制列表以减少转发延迟

C.可以允许最终用户直接访问

D.尽量避免冗余连接

【答案】B

【解析】

核心层是因特网络的高速骨干，由于其重要性，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能快速适应变化。

在选择核心层设备时候，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

在网络规划和设计过程中，选择网络技术时要考虑多种因素。下面的各种考虑中不正确的是（70）。

(70)A.网络带宽要保证用户能够快速访问网络资源

B.要选择具有前瞻性的网络新技术

C.选择网络技术时要考虑未来网络扩充的需要

D.通过投入产出分析确定使用何种技术

【答案】B

【解析】

在网络规划和设计过程中，选择网络技术时要考虑多种因素。下面的各种考虑中不正确的是要选择具有前瞻性的网络新技术，应该是选择成熟可靠的技术。

All three types of cryptography schemes have unique function mapping to specific applications.For example, the symmetric key（71） approach is typically used for the encryption of data providing（72）, whereas asymmetric key cryptography is mainly used in key(73)and nonrepudiation, thereby providing confidentiality and authentication. The hash(74)（noncryptic）, on the other hand, does not provide confidentiality but provides message integrity, and cryptographic hash algorithms provide message（75）and identity of peers during transport over insecure channels.

(71)A.cryptography　B.decode　C.privacy　D.security

(72)A.conduction　B.confidence

C.confidentiality　D.connection

(73)A.authentication　B.structure　C.encryption　D.exchange

(74)A.algorithm　B.secure　C.structure　D.encryption

(75)A.confidentiality　B.integrity　C.service　D.robustness

【答案】A　C　C　A　A

【解析】

所有三种类型的加密方式都有映射到特定应用中的独特功能。例如，对称密钥加密方法典型地用于保障加密数据的保密性，非对称方式主要用于密钥交换和不可否认性场景，因而提供保密性和身份验证。相比之下，哈希算法（不带密钥）不提供保密性只保障消息的完整性，而带密钥的哈希算法保障数据的完整性并且能为点对点信息通过不安全信道传递时提供身份验证。

试题一（20 分）

阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。

【说明】

某企业的行政部、技术部和生产部分布在三个区域，随着企业对信息化需求的提高，现拟将网络出口链路由单链路升级为双链路，提升 ERP 系统服务能力以及加强员工上网行为管控。网络管理员依据企业现有网络和新的网络需求设计了该企业网络拓扑图 1-1，并对网络地址重新进行了规划，其中防火墙设备集成了传统防火墙与路由功能。

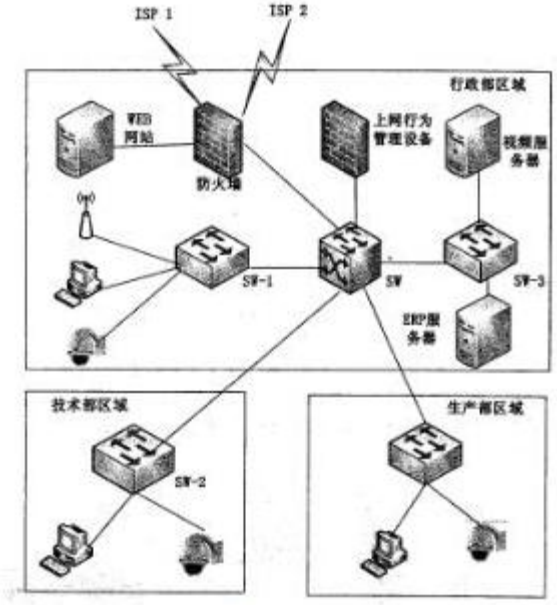


图1-1

【问题 1】（4 分）

在图 1-1 的防火墙设备中，配置双出口链路有提高总带宽、（1）、链路负载均衡作用。通过配置链路聚合来提高总带宽，通过配置（2）来实现链路负载均衡。

（每空 2 分，共 4 分）

（1）提高可靠性

（2）策略路由

在图 1-1 的防火墙设备中，配置双出口链路有提高总带宽、提高可靠性、链路负载均衡作用。通过配置链路聚合来提高总带宽，通过配置策略路由来实现链路负载均衡。

【问题 2】（4 分）

防火墙工作模式有路由模式、透明模式、混合模式，若该防火墙接口均配有 IP 地址，

则防火墙工作在（3）模式，该模式下，ERP 服务器部署在防火墙的（4）区域。

（每空 2 分，共 4 分）

（3）路由模式

（4）信任区域

防火墙能够工作在三种模式下：路由模式、透明模式、混合模式。如果防火墙以第三层对外连接（接口具有 IP 地址），则认为防火墙工作在路由模式下；若防火墙通过第二层对外连接（接口无 IP 地址），则防火墙工作在透明模式下；若防火墙同时具有工作在路由模式和透明模式的接口（某些接口具有 IP 地址，某些接口无 IP 地址），则防火墙工作在混合模式下。

该模式下，ERP 服务器部署在防火墙的内部区域。内部区域（内网）。内部区域通常就是指企业内部网络或者是企业内部网络的一部分。它是互连网络的信任区域，即受到了防火墙的保护。

外部区域（外网）。外部区域通常指 Internet 或者非企业内部网络。它是互连网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务，通过防火墙，就可以实现有限制的访问。

非军事区（DMZ，又称停火区）。是一个隔离的网络，或几个网络。位于区域内的主机或服务器被称为堡垒主机。一般在非军事区内可以放置 Web、Mail 服务器等。停火区对于外部用户通常是可以访问的，这种方式让外部用户可以访问企业的公开信息，但却不允许它们访问企业内部网络。

【问题 3】（4 分）

若地址规划如图 1-1 所示，从 IP 规划方案看该地址的配置可能有哪些方面的考虑？

（共 4 分）

可扩展性、连续性、唯一性、实意性。

【问题 4】（3 分）

该网络拓扑中，上网行为管理设备的位置是否合适？请说明理由。

（共 3 分）

不合适，应该接在防火墙和核心交换机之间，因为试题说了要对用户上网行为进行管控，不能以旁路模式接入。

【问题 5】（3 分）

该网络中有无线节点的接入，在安全管理方面应采取哪些措施？

（共 3 分）

注意 SSID 的管理、MAC 地址的过滤，加密方式的选择

无线加密：在设置无线路由器的时候，一个必要的环节就是设置无线加密（通俗点来说就是设置无线密码），在无线路由器的安全配置页面，大家会经常见到三种无线加密方式，分别是 WPA-PAK/WPA2-PSK、WPA/WPA2 以及 WEP。

WEP 加密技术使用静态共享密钥和未加密循环冗余码校验（CRC），无法保证加密数据的完整性，并存在弱密钥等。这使得 WEP 加密技术在安全保护方面存在明显的缺陷，对熟练的入侵者而言，往往只需很短时间甚至几分钟便可攻破。于是就出现了新的 WLAN 加密技术--WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）和 WPA2。显然，WPA2 技术是 WPA 技术的升级版。从技术角度看，WPA/WPA2 主要解决了 WEP 在共享密钥上的漏洞，添加了数据完整性检查和用户级认证措施。WPA2 是 WPA 的第二个版本，是对 WPA 在安全方面的改进版本。与第一版的 WPA 相比，主要改进的是所采用的加密标准。

【问题 6】（2 分）

该网络中视频监控系统与数据业务共用网络带宽，存在哪些弊端？

（共 2 分）

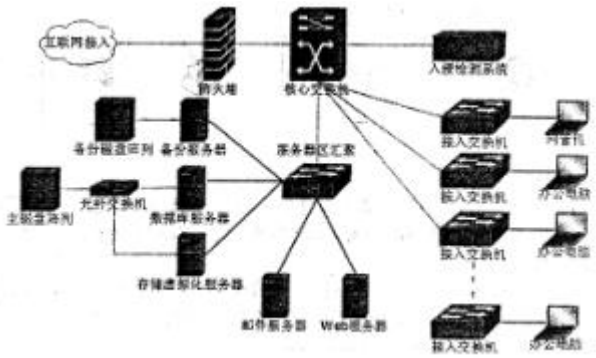
存在视频监控系统的带宽出现不能满足大量图像传输需求，容易出现数据传输排队和丢包的问题。

试题二（20 分）

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 是某互联网企业网络拓扑，该网络采用二层结构，网络安全设备有防火墙、入侵检测系统，楼层接入交换机 32 台，全网划分 17 个 VLAN，对外提供 Web 和邮件服务，数据库服务器和邮件服务器均安装 CentOS 操作系统(Linux 平台),Web 服务器安装 Windows 2008 操作系统。



【问题 1】(6 分)

SAN 常见方式有 FC-SAN 和 IP SAN，在图 2-1 中，数据库服务器和存储设备连接方式为（1），邮件服务器和存储设备连接方式为（2）。

虚拟化存储常用文件系统格式有 CIFS、NFS，为邮件服务器分配存储空间时应采用的文件系统格式是（3），为 Web 服务器分配存储空间应采用的文件系统格式是（4）。

（每空 1.5 分，共 6 分）

（1）FC SAN

（2）IP SAN

（3）NFS

（4）CIFS

从效率上看，FC SAN 明显高于 IP SAN，因此 FC SAN 更加适合于对效率敏感的应用，例如对性能要求很高的数据库应用，而 IP SAN 则主要应用到对性能和效率要求不高的环境中，例如 OA，文档处理，多媒体环境等。

虚拟化存储常用文件系统格式有 CIFS、NFS，由于邮件服务器是 Linux 系统分配存储空间时应采用的文件系统格式是 NFS，为 Web 服务器分配存储空间应采用的文件系统格式是

CIFS。

【问题 2】（3 分）

该企业采用 RAID5 方式进行数据冗余备份。请从存储效率和存储速率两个方面比较 RAID1 和 RAID5 两种存储方式，并简要说明采用 RAID5 存储方式的原因。

（共 3 分）

RAID1 只是做磁盘镜像，存储效率 RAID1 只有 50%，没有提高存储性能，RAID5 存储效率是（N-1）/N，其中 N 是磁盘数目，在 RAID5 上，读/写指针可同时对阵列设备进行操作，提供了更高的存储性能。

【问题 3】（8 分）

网络管理员接到用户反映，邮件登录非常缓慢，按以下步骤进行故障诊断：

1．通过网管机，利用（5）登录到邮件服务器，发现邮件服务正常，但是连接时断时续。

2．使用（6）命令诊断邮件服务器的网络连接情况，发现网络丢包严重，登录服务器区汇聚交换机 S1，发现连接邮件服务器的端口数据流量异常，收发包量很大。

3．根据以上情况，邮件服务器的可能故障为（7），应采用（8）的办法处理上述故障。

(5)～(8)备选答案：

(5)A．ping B．ssh C．tracert D．mstsc

(6)A．ping B．telnet C．tracet D．netstat

(7)A．磁盘故障 B．感染病毒 C．网卡故障 D．负荷过大

(8)A．更换磁盘 B．安装防病毒软件，并查杀病毒

C．更换网卡 D．提升服务器处理能力

（每空 2 分，共 8 分）

（5）B

（6）A

（7）B

（8）B

网络管理员接到用户反映，邮件登录非常缓慢，按以下步骤进行故障诊断：

1．通过网管机，利用 SSH 登录到邮件服务器，因为是 Linux 系统，发现邮件服务正常，但是连接时断时续。

2．使用 PING 命令诊断邮件服务器的网络连接情况，发现网络丢包严重，登录服务器区

汇聚交换机 S1，发现连接邮件服务器的端口数据流量异常，收发包量很大。

3．根据以上情况，邮件服务器的可能故障为感染病毒，应采用安装防病毒软件，并查杀病毒的办法处理上。

【问题 4】（3 分）

上述企业网络拓扑存在的网络安全隐患有：（9）、（10）、（11）。

(9)~(11)备选答案

A．缺少针对来自局域网内部的安全防护措施

B．缺少应用负载均衡

C．缺少流量控制措施

D．缺少防病毒措施

E．缺少 Web 安全防护措施

F．核心交换机到服务器区汇聚交换缺少链路冗余措施

G．VLAN 划分太多

（每空 1 分、共 3 分）

（9） B

（10）C

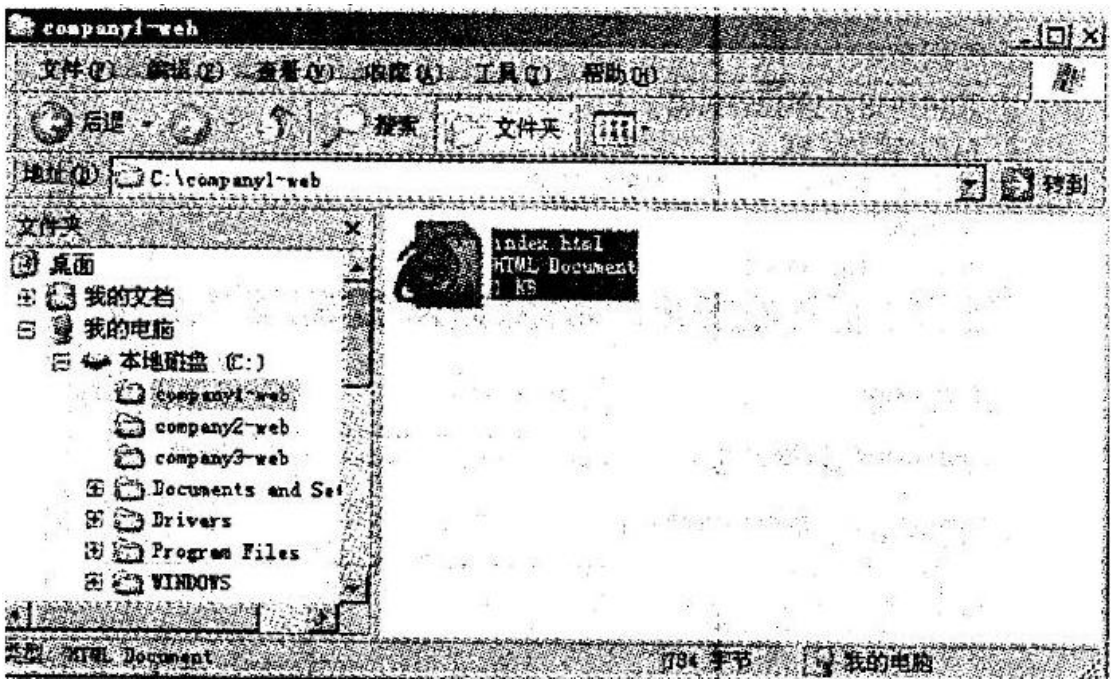
（11）F

试题三（20 分）

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】

某公司的 IDC（互联网数据中心）服务器 Server1 采用 Windows Server 2003 操作系统，IP 地址为 172.16.145.128/24，为客户提供 Web 服务和 DNS 服务；配置了三个网站，域名分别为 www.company1.com、www.company2.com 和 www.company3.com，其中 company1 使用默认端口。基于安全的考虑，不允许用户上传文件和浏览目录。company1.com、company2.com 和 company3.com 对应的网站目录分别为 company1-web、company2-web 和 company3-web，如图 3-1 所示。



【问题 1】（2 分，每空 1 分）

为安装 Web 服务和 DNS 服务，Server1 必须安装的组件有（1）和（2）。

(1)～(2)备选答案：

A. 网络服务 B. 应用程序服务器 C. 索引服务 D. 证书服务 E. 远程终端

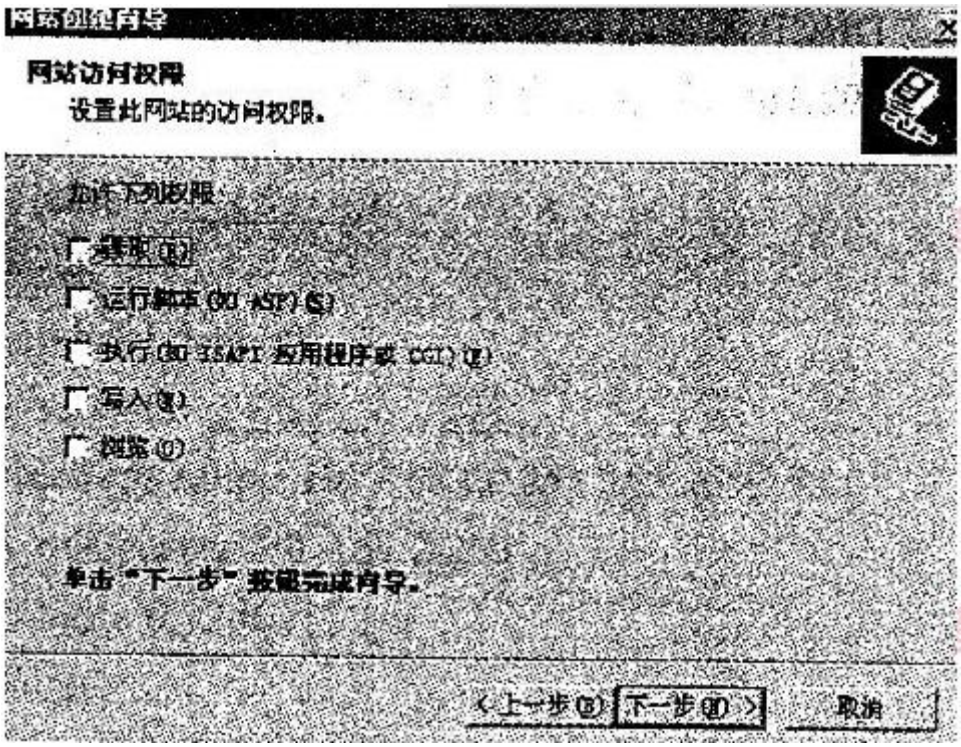
（每空 1 分，共 2 分）

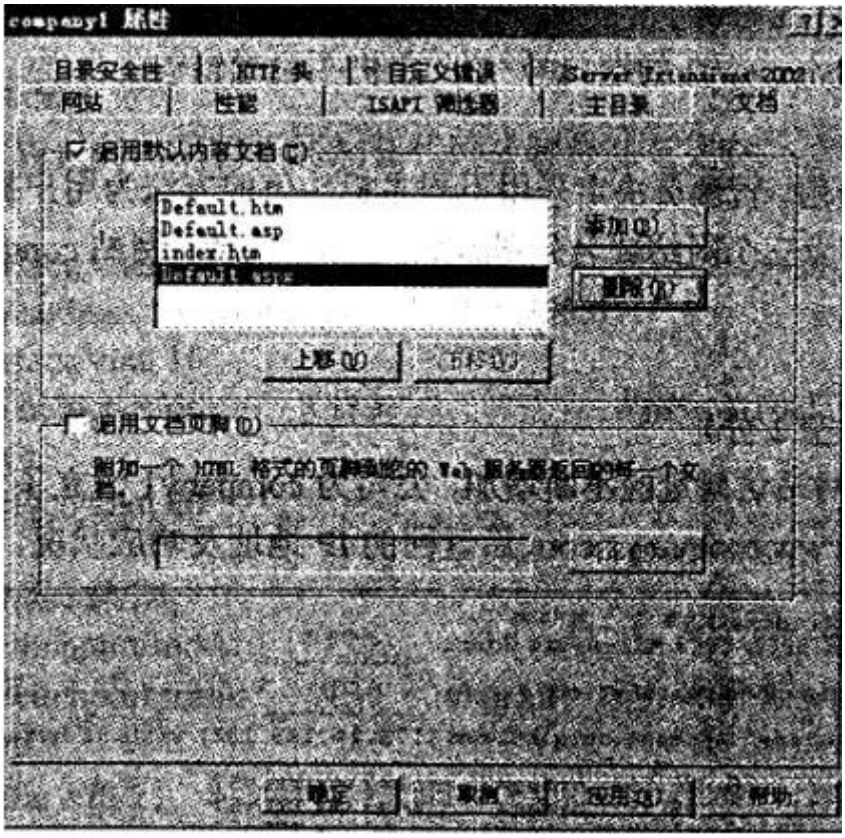
（1）B

（2）A

【问题 2】（4 分，每空 2 分）

在 IIS 中创建这三个网站时，在图 3-2 中勾选读取、（3）和执行，并在图 3-3 所示的文档选项卡中添加（4）为默认文档。





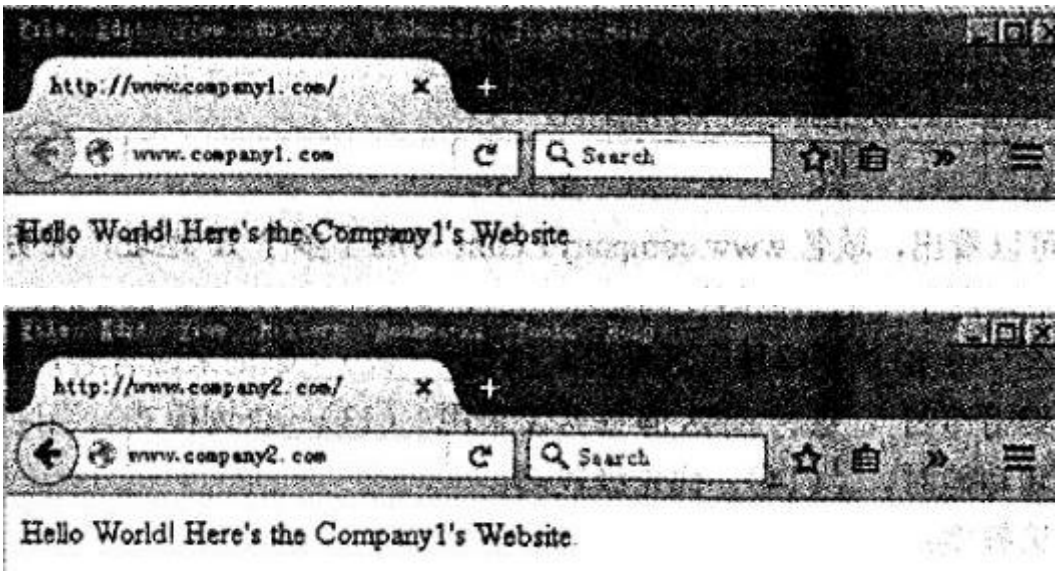
（每空 2 分，共 4 分）

（3）运行脚本

（4）index.html

【问题 3】（6 分，每空 1 分）

1、为了节省成本，公司决定在一台计算机上为多类用户提供服务。使用不同端口号来区分不同网站，company1 使用默认端口（5），company2 和 company3 的端口应在 1025 至（6）范围内任意选择，在访问 company2 或者 company3 时需在域名后添加对应端口号，使用（7）符号连接。设置完成后，管理员对网站进行了测试，测试结果如图 3-4 所示，原因是（8） 。



(8)备选答案：

A. IP 地址对应错误

B. 未指明 company1 的端口号

C. 未指明 company2 的端口号

D. 主机头设置错误

2、为便于用户访问，管理员决定采用不同主机头值的方法为用户提供服务，需在 DNS 服务中正向查找区域为三个网站域名分别添加（9） 记录。网站 company2 的主机头值应设置为（10） 。

（每空 1 分，共 6 分）

（5）80

（6）65535

（7）：

（8）C

（9）A

（10）www.commany2.com

【问题 4】（8 分，每空 2 分）

随着 company1 网站访问量的不断增加，公司为 company1 设立了多台服务器。下面是不同用户 ping 网站 www.company1.com 后返回的 IP 地址及响应状况，如图 3-5 所示。

```
Microsoft Windows [版本 5.2.3790]
(c) 版权所有 1985-2003 Microsoft Corp.

C:\Users>ping www.company1.com

Pinging company1.wscache.ourglb0.com [172.16.145.192] with 32 bytes of data:

Reply from 172.16.145.192: bytes=32 time=11ms TTL=57
Reply from 172.16.145.192: bytes=32 time=13ms TTL=57
Reply from 172.16.145.192: bytes=32 time=15ms TTL=57
Reply from 172.16.145.192: bytes=32 time=13ms TTL=57

Ping statistics for 172.16.145.192:
    Packets: Sent=4, Received=4, Lost=0 <0% loss>,
Approximate round trip times in milli-seconds:
    Minimum=11ms, Maximum=15ms, Average=13ms
```

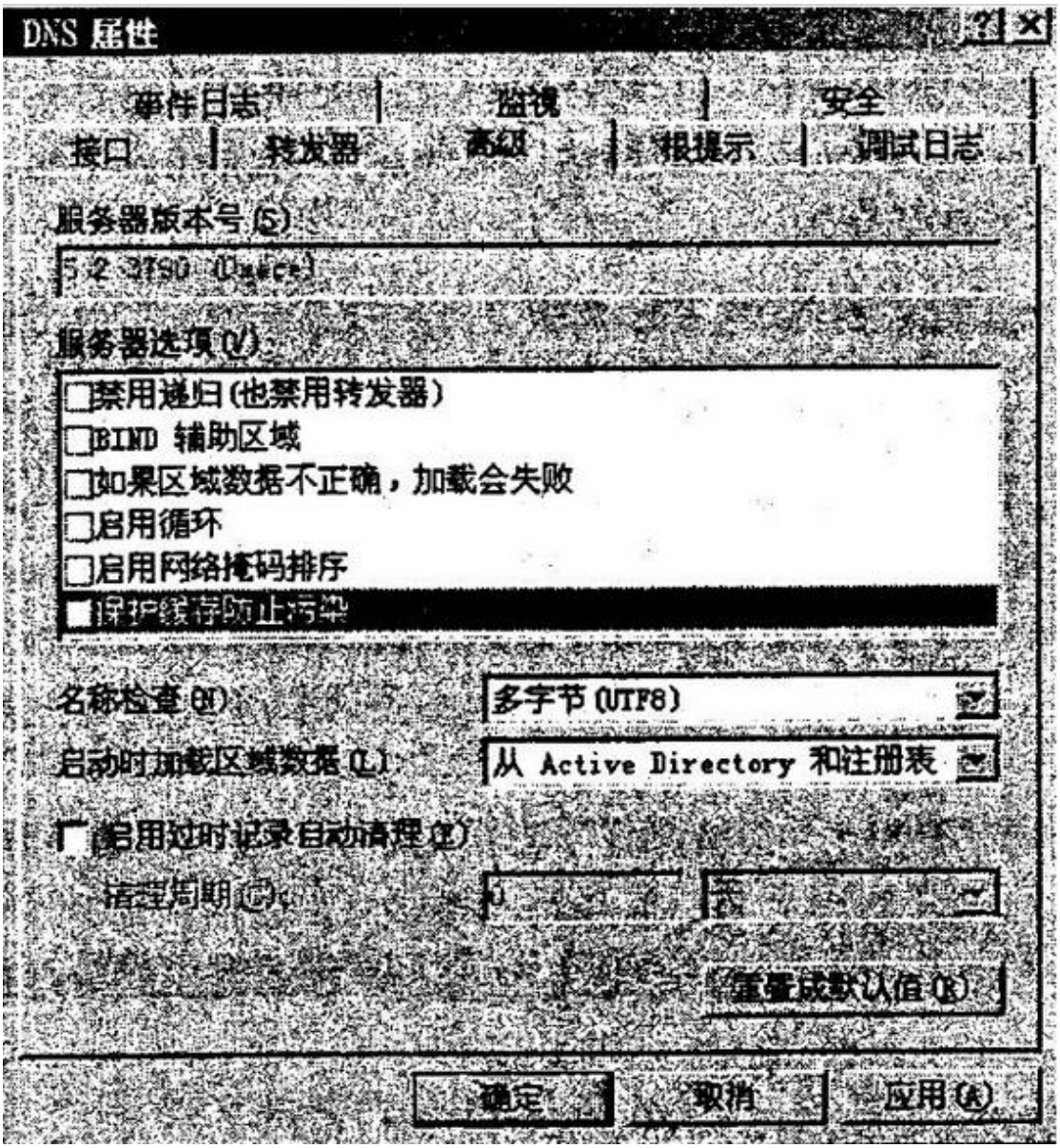
```
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation.

C:\Users>ping www.company1.com

Pinging company1.wscache.ourglb0.com [172.16.145.193] with 32 bytes of data:

Reply from 172.16.145.193: bytes=32 time=5ms TTL=57
Reply from 172.16.145.193: bytes=32 time=6ms TTL=57
Reply from 172.16.145.193: bytes=32 time=5ms TTL=57
Reply from 172.16.145.193: bytes=32 time=8ms TTL=57

Ping statistics for 172.16.145.193:
Packets: Sent=4, Received=4, Lost=0 <0% loss>,
Approximate round trip times in milli-seconds:
Minimum=5ms, Maximum=8ms, Average=6ms
```

从图 3-5 可以看出，域名 www.company1.com 对应了多个 IP 地址，说明在图 3-6 所示的 DNS 属性中启用了（11） 功能。

在图 3-6 中勾选了“启用网络掩码排序”后，当存在多个匹配记录时，系统会自动检查这些记录与客户端 IP 的网络掩码匹配度，按照（12） 原则来应答客户端的解析请求。如果勾选了“禁用递归”，这时 DNS 服务器仅采用（13） 查询模式。当同时启用了网络掩码排序和循环功能时，（14） 优先级较高。

(14)备选答案：

A. 循环 B. 网络掩码排序



（每空 2 分，共 8 分）

（11）启用循环

（12）掩码接近度匹配，对来访者实行的本地子网优先级匹配

（13）迭代

（14）B

试题四(15 分)

阅读以下说明，回答问题 1 至问题 2，将解答填入答题纸对应的解答栏内。

【说明】

某公司建立局域网拓扑图如图 4-1 所示。公司计划使用路由器作为 DHCP 服务器，根据需求，公司内部使用 C 类地址段，服务器地址段为 192.168.2.0/24，S2 和 S3 分别为公司两个部门的接入交换机，分别配置 VLAN 10 和 VLAN 20，地址段分别使用 192.168.10.0/24 和 192.168.20.0/24，通过 DHCP 服务器自动为两个部门分配 IP 地址，地址租约期为 12 小时。其中，192.168.10.1~192.168.10.10 作为保留地址。

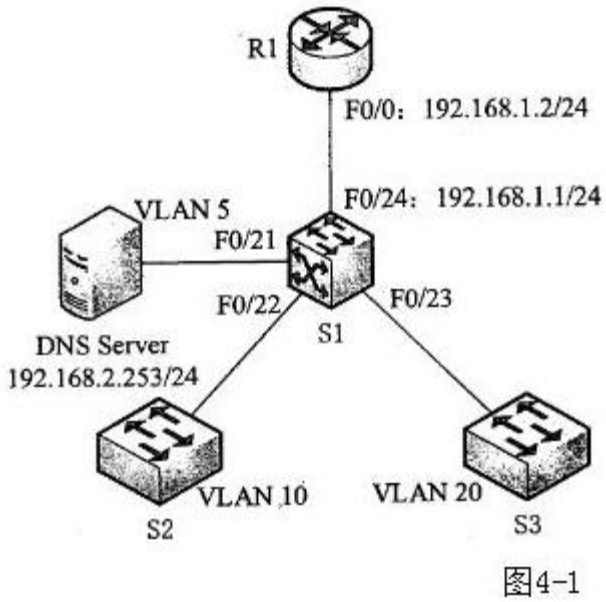


图4-1

【问题 1】(10 分，每空 1 分)

下面是 R1 的配置代码，请将下面配置代码补充完整。

```
R1#config t
R1 (config)# interface FastEthernet0/0
R1 (config-if)#ip address（1） （2）
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#ip dhcp（3） depart1
R1 (dhcp-config)#network 192.168.10.0 255.255.255.0
R1 (dhcp-config)#default-router 192.168.10.254 255.255.255.0
R1 (dhcp-config)#dns-server（4）
```

R1 (dhcp-config)#lease 0 （5） 0

R1 (dhcp-config)#exit

R1 (config)#ip dhcp pool depart2

R1 (dhcp-config)# network（6） （7）

R1 (dhcp-config)#default-router 192.168.20.254 255.255.255.0

R1 (dhcp-config)# dns-server 192.168.2.253

R1 (dhcp-config)# lease 0 12 0

R1 (dhcp-config)#exit

R1 (config)# ip dhcp excluded-address （8） （9）

R1 (config)# ip dhcp excluded-address（10） //排除掉不能分配的 IP 地址

R1 (config)# ip dhcp excluded-address 192.168.20.254

.....

(10 分，每空 1 分)

下面是 R1 的配置代码，请将下面配置代码补充完整。

R1#config t

R1 (config)# interface FastEthernet0/0

R1 (config-if)#ip address 192.168.1.2 255.255.255.0 //配置接口 IP 地址和掩码

R1 (config-if)#no shutdown //激活接口

R1(config-if)#exit

R1 (config)#ip dhcp pool depart1 //配置 DHCP 地址池名字

R1 (dhcp-config)#network 192.168.10.0 255.255.255.0

R1 (dhcp-config)#default-router 192.168.10.254 255.255.255.0

R1 (dhcp-config)#dns-server 192.168.2.253 //DNS 地址

R1 (dhcp-config)#lease 0 12 0 //租约时间 12 小时

R1 (dhcp-config)#exit

R1 (config)#ip dhcp pool depart2

R1(dhcp-config)# network 192.168.20.0 255.255.255.0 //作用域范围

R1 (dhcp-config)#default-router 192.168.20.254 255.255255.0

R1 (dhcp-config)# dns-server 192.168.2.253

R1 (dhcp-conlig)# lease 0 12 0

R1 (dhcp-coniig)#exit

R1 (config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10

R1 (config)# ip dhcp excluded-address 192.168.10.254 //排除掉不能分配的 IP 地址

【问题 2】(5 分，每空 1 分)

下面是 S1 的配置代码，请将下面配置代码或解释补充完整。

S1#config terminal

S1(config)#interface vlan 5

S1(config-if)#ip address 192.168.2.254 255.255.255.0

S1(config)#interface vlan 10

S1(config-if)#ip helper-address（11） //指定 DHCP 服务器的地址

S1(config-if)#exit

S1(config)#interface vlan 20

.....

S1(config)#interface f0/24

S1(config-if)#switchport mode （12）

S1(config-if)# switchport trunk （13）vlan all //允许所有 VLAN 数据通过

S1(config-if)#exit

S1(config)#interface f0/21

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 5

S1(config-if)#exit

S1(config)#interface f0/22

S1(config-if)#switchport mode access

S1(config-if)#switchport access（14）

S1(config)#interface f0/23

S1(config-if)#switchport mode access

S1(config-if)#switchport access（15）

（每空 1 分，共 5 分）

下面是 S1 的配置代码，请将下面配置代码或解释补充完整。

S1#config terminal

S1(config)#interface vlan 5

S1(config-if)#ip address 192.1682.254 255.255255.0

S1(config)#interface vlan 10

S1(config-if)#ip helper-address 192.168.1.2 // 指定 DHCP 服务器的地址

S1(config-if)#exit

S1(config)#interface vlan 20

…

S1(config)#interface f0/24

S1(config-if)#switchport mode trunk

Sl(config-if)# switchport trunk allowed vlan all //允许所有 VLAN 数据通过

S1(config-if)#exit

S1(config)#interface f0/21

Sl(config-if)#switchport mode access

S1(config-if)#switchport access vlan 5

S1(config-if)#exit

S1(config)#interface f0/22

Sl(config-if)#switchport mode access

S1(config-if)#switchport access vlan 10

S1(config)#interface f0/23

S1(config-if)#switchport mode access

Sl(config-if)#switchport access vlan 20