

机器字长为 n 位的二进制数可以用补码来表示 (1) 个不同的有符号定点小数。

- (1) A. $2n$ B. $2n-1$ C. $2n-1$ D. $2n-1+1$

【答案】A

【解析】 本题考查计算机系统基础知识。

进制数据在计算机系统表示方法是最基本的专业知识。补码本身是带符号位的，补码表示的数字中 0 是唯一的，不像原码有 +0 和 -0 之分，也就意味着 n 位二进制编码可以表示 $2n$ 个不同的数。

计算机中 CPU 对其访问速度最快的是 (2)。

- (2) A. 内存 B. Cache C. 通用寄存器 D. 硬盘

【答案】C

【解析】 本题考查计算机系统基础知识。

计算机系统 CPU 内部对通用寄存器的存取操作是速度最快的，其次是 Cache，内存的存取速度再次，选项中访问速度最慢的就是作为外存的硬盘。它们同组成分级存储体系来解决存储容量、成本和速度之间的矛盾。

计算机中 CPU 的中断响应时间指的是 (3) 的时间。

- (3) A. 从发出中断请求到中断处理结束
B. 从中断处理开始到中断处理结束
C. CPU 分析判断中断请求
D. 从发出中断请求到开始进入中断处理程序

【答案】D

【解析】 本题考查计算机组成基础知识。

中断系统是计算机实现中断功能的软硬件总称。一般在 CPU 中设置中断机构在外设接口中设置中断控制器，在软件上设置相应的中断服务程序。中断源在需要得到 CPU 服务时，请求 CPU 暂停现行工作转向为中断源服务，服务完成后，再让 CPU 回到原工作状态继续完成被打断的工作。中断的发生起始于中断源发出中断请求，中断处理过程中，中断系统需要解决一系列问题，包括中断响应的条件和时机，断点信息的保护与恢复，中断服务程序入口、中断处理等。中断响应时间，是指从发出中断请求到开始进入中断服务程序所需的时间。

总线宽度为 32bit,时钟频率为 200MHz,若总线上每 5 个时钟周期传送一个 32bit 的字,则该总线的带宽为(4)MB/S。

(4) A. 40

B. 80

C. 160

D. 200

【答案】C

【解析】本题考查计算机系统基础知识。

总线宽度是指总线的线数,即数据信号的并行传输能力,也体现总线占用的物理空间和成本;总线的带宽是指总线的最大数据传输率,即每秒传输的数据总量。总线宽度与时钟频率共同决定了总线的带宽。

$32\text{bit}/8=4\text{Byte}$, $200\text{MHz}/5\times 4\text{Byte}=160\text{MB/s}$

以下关于指令流水线性能度量的叙述中,错误的是(5)。

(5) A. 最大吞吐率取决于流水线中最慢一段所需的时间

B. 如果流水线出现断流,加速比会明显下降

C. 要使加速比和效率最大化应该对流水线各级采用相同的运行时间

D. 流水线采用异步控制会明显提高其性能

【答案】D

【解析】本题考查计算机系统结构的基础知识。

对指令流水线性能的度量主要有吞吐率,加速比和效率等指标。吞吐率是指单位时间内流水线所完成的任务数或输出结果的数量,最大吞吐率则是流水线在达到稳定状态后所得到的吞吐率,它取决于流水线中最慢一段所需的时间,所以该段成为流水线的瓶颈。流水线的加速比定义为等功能的非流水线执行时间与流水线执行时间之比,加速比与吞吐率成正比,如果流水线断流,实际吞吐率将会明显下降,则加速比也会明显下降。流水线的效率是指流水线的设备利用率,从时空图上看效率就是 n 个任务所占的时空区与 m 个段总的时空区之比。因此要使加速比和效率最大化应该对流水线各级采用相同的运行时间。另外,流水线采用异步控制并不会给流水线性能带来改善,反而会增加控制电路的复杂性。

对高级语言源程序进行编译或解释的过程可以分为多个阶段,解释方式不包含(6)。

(6) A. 词法分析

B. 语法分析

C. 语义分析

D. 目标代码生成

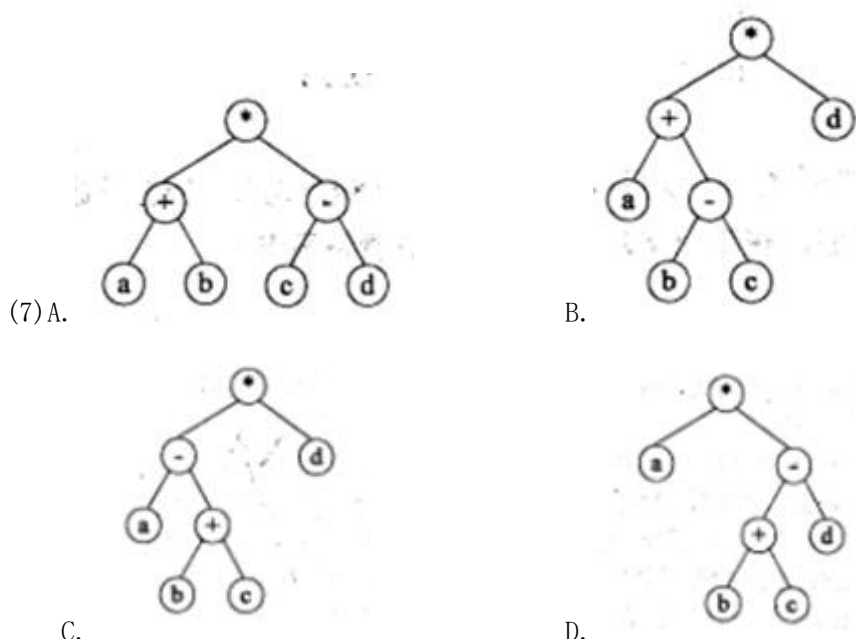
【答案】D

【解析】本题考查程序语言基础知识。

用某种高级语言或汇编语言编写的程序称为源程序不能直接在计算机上执行。汇编语言源程序需要用一个汇编程序将其翻译成目标程序后才能执行。高级语言源程序则需要对应的解释程序或编译程序对其进行翻译，然后在机器上运行。

解释程序也称为解释器，它或者直接解释执行源程序，或者将源程序翻译成某种中间代码后再加以执行；而编译程序（编译器）则是将源程序翻译成目标语言程序，然后在计算机上运行目标程序。这两种语言处理程序的根本区别是：在编译方式下，机器上运行的是与源程序等价的目标程序，源程序和编译程序都不再参与目标程序的执行过程；而在解释方式下，解释程序和源程序（或其某种等价表示）要参与到程序的运行过程中，运行程序的控制权在解释程序。简单来说，在解释方式下，翻译源程序时不生成独立的目标程序，而编译器则将源程序翻译成独立保存的目标程序。

与算术表达式 “ $(a+(b-c))*d$ ” 对应的树是 (7)。



【答案】B

【解析】本题考查程序语言与数据结构基础知识。

对算术表达式 “ $(a+(b-c))*d$ ” 求值的运算处理顺序是：先进行 $b-c$ ，然后与 a 相加，最后再与 d 相乘。只有选项 B 所示的二叉树与其相符。

C 程序中全局变量的存储空间在 (8) 分配。

(8) A. 代码区 B. 静态数据区 C. 栈区 D. 堆区

【答案】B

【解析】本题考查程序语言基础知识。

程序运行时的用户内存空间一半划分为代码区、静态数据区、栈区和堆区，其中栈区和堆区也称为动态数据区。全局变量的存储空间在静态数据区。

某进程有4个页面，页号为0~3，页面变换表及状态位、访问位和修改位的含义如下图所示。系统给该进程分配了3个存储块，当采用第二次机会页面替换算法时，若访问的页面1不在内存，这时应该淘汰的页号为(9)。

页号	页帧号	状态位	访问位	修改位
0	6	1	1	1
1	—	0	0	0
2	3	1	1	1
3	2	1	1	0

状态位含义 {
=0 不在内存
=1 在内存

访问位含义 {
=0 未访问过
=1 访问过

修改位含义 {
=0 未修改过
=1 修改过

(9)A. 0

B. 1

C. 2

D. 3

【答案】D

【解析】

试题(9)的正确选项为D。根据题意页面变换表中状态位等于0和1分别表示页面不在内存或在内存，所以0、2和3号页面在内存。当访问的页面1不在内存时，系统应该首先淘汰未被访问的页面，因为根据程序的局部性原理最近未被访问的页面下次被访问的概率更小；如果页面最近都被访问过，应该先淘汰未修改过的页面。因为未修改过的页面内存与辅存一致，故淘汰时无须写回辅存，使系统页面置换代价小。经上述分析，0、2和3号页面都是最近被访问过的，但0和2号页面都被修改过而3号页面未修改过，故应该淘汰3号页面。

王某是某公司的软件设计师，每当软件开发完成后均按公司规定编写软件文档，并提交公司存档，那么该软件文档的著作权(10)享有。

(10)A. 应由公司

B. 应由公司和王某共同

C. 应由王某

D. 除署名权以外，著作权的其他权利由王某

【答案】A

【解析】 本题考查知识产权的基本知识。

依据著作权法第十一条、第十六条规定，职工为完成所在单位的工作任务而创作的作品属于职务作品。职务作品的著作权归属分为两种情况。

①虽是为完成工作任务而为，但非经法人或其他组织主持，不代表其意志创作，也不由其承担责任的职务作品，如教师编写的教材，著作权应由作者享有，但法人或者其他组织有权在其业务范围内优先使用的权利，期限为2年。

②由法人或者其他组织主持，代表法人或者其他组织意志创作，并由法人或者其他组织承担责任的职务作品，如工程设计、产品设计图纸及其说明、计算机软件、地图等职务作品，以及法律规定或合同约定著作权由法人或非法人单位单独享有的职务作品，作者享有署名权，其他权利由法人或者其他组织享有。

当登录交换机时，符号(11)是特权模式提示符。

(11)A. @

B. #

C. >

D. &

【答案】B

【解析】

登录交换机时首先遇到的符号是>，这表示交换机处于用户执行模式。

switch>

这时输入 enable 命令，则交换机进入特权模式

switch>enable

switch#

进入全局配置模式模式的命令是 config terminal

Switch#config terminal

Switch (config) # (配置模式提示符)

下面的选项中显示系统硬件和软件版本信息的命令是(12)。

(12)A. show configuration

B. show environment

C. show version

D. show platform

【答案】C

【解析】

路由器显示命令如下所示：.

查看版本及引导信息	show version
查看运行设置	show running-config
查看开机设置	show startup-config
显示端口信息	show interface <i>type slot/number</i>
显示路由信息	show ip route

Cisco 路由器高速同步串口默认的封装协议是_(13)。

- (13) A. PPP B. LAPB C. HDLC D. AIM-DXI

【答案】C

【解析】

路由器不仅能实现局域网之间的连接，还能实现局域网与广域网、广域网与广域网之间的连接。路由器与广域网连接的端口称为WAN 端口，路由器与局域网连接的端口称为LAN 口。常见的网络端口有以下几种：

- ①RJ-45 端口：这种端口通过双绞线连接以太网。可实现 10M/100M/1000M 高速数据传输。
- ②高速同步串口：路由器通过高速同步串口（Synchronous Serial Port）连接 DDN、帧中继、X.25 等网络。高速同步串口默认的封装协议是 HDLC。
- ③异步串口：异步串口（ASYNC）主要用于与 Modem 的连接，以实现远程计算机通过 PSTN 拨号接入。
- ④Console 端口：Console 端口通过专用电缆连接至计算机串行口，利用终端仿真程序对路由器进行本地配置。路由器的 Console 端口为 RJ-45 口。
- ⑤AUX 端口：这是用于远程配置的异步端口（Auxiliary Port），主要用于拨号连接，还可以通过收发器连接 MODEM，支持硬件流控。
- ⑥SC 端口：这是光纤端口，用于连接到具有光纤端口的交换机，一般以“100bFX”标注，传输距离可以达到几百米甚至几千米，传输速率能够达到 1Gb/s 或 10Gb/s。另外还有 GBIC 插槽和 SFP 插槽，SFP 比 GBIC 占用的位置少，可以适应各种复杂的网络环境。

以下关于网桥和交换机的区别的叙述中，正确的是_(14)。

- (14) A. 交换机主要是基于软件实现，而网桥是基于硬件实现的
B. 交换机定义了广播域，而网桥定义了冲突域

- C. 交换机根据 IP 地址转发，而网桥根据 MAC 地址转发
- D. 交换机比网桥的端口多，转发速度更快

【答案】D

【解析】

传统的网桥是在计算机上安装两个网卡，通过网桥软件实现局域网之间的帧转发，而交换机则是基于硬件实现的高速转发设备，标准的商用交换机都具有 24 个端口。

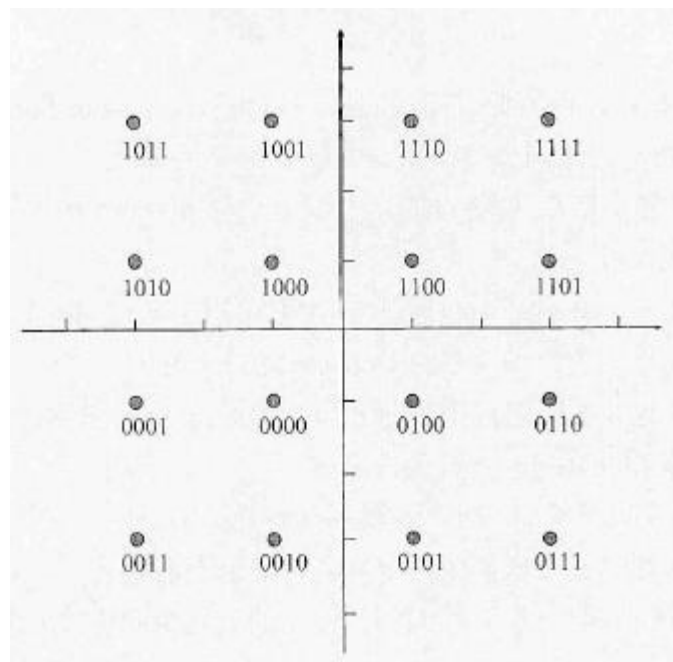
正交幅度调制 16-QAM 的数据速率是码元速率的 (15) 倍。

- (15) A. 2 B. 4 C. 8 D. 16

【答案】B

【解析】

正交幅度调制 (Quadrature Amplitude Modulation, QAM) 是把两个幅度相同但相位相差 90° 的模拟信号合成为一个载波信号，经过信道编码后把数据组合映射到星座图上，如下图所示。



QAM 调制实际上是幅度调制和相位调制的组合，同时利用了载波的幅度和相位来传递数据信息。与单纯的 PSK 调制相比，在最小距离相同的条件下，QAM 星座图中可以容纳更多的载波码点，可以实现更高的频带利用率。16-QAM 是用一个码元表示 4 比特二进制数据，它的数据速率是码元速率的 4 倍。目前最高可以达到 1024-QAM，即用一个码元表示 10 比特数据。

电话线路使用的带通滤波器的宽带为 3KHz (300~3300Hz)，根据奈奎斯特采样定理，最小采样频率应为(16)。

- (16) A. 300Hz B. 3300Hz C. 6000Hz D. 6600Hz

【答案】D

【解析】

PCM 主要经过 3 个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续幅度连续的模拟信号变换为时间离散、幅度连续的采样信号，量化过程将采样信号变为时间离散、幅度离散的数字信号，编码过程将量化后的离散信号编码为二进制码组。

采样的频率决定了可恢复的模拟信号的质量。根据奈奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即 $f=1/T=2f_{\max}$ ，其中 f 为采样频率， T 为采样周期， f_{\max} 为信号的最高频率。

人耳对 25~22000 Hz 的声音有反应。在谈话时，大部分有用的信息的能量分布在 200Hz~3500Hz 之间。因此电话线路使用的带通滤波器的带宽为 3kHz (即 300~3300Hz)。根据 Nyquist 采样定理，最小采样频率应为 6600Hz, 实际上，CCITT 规定对话音信号的采样频率为 8kHz。

当一个帧离开路由器接口时，其第二层封装信息中(17)。

- (17) A. 数据速率由 10 BASE-TX 变为 100 BASE-TX
B. 源和目标 IP 地址改变
C. 源和目标 MAC 地址改变
D. 模拟线路变为数字线路

【答案】C

【解析】

帧头中的主要信息是源和目标的 MAC 地址，另外还有一些用于帧控制的信息。数据速率和调制方式（模拟/数字）属于物理层机制，而 IP 地址则属于网络层信息，都与第二层封装信息无关。

(18)时使用默认路由。

(18)A. 访问本地 Web 服务器

B. 在路由表中找不到目标网络

C. 没有动态路由

D. 访问 ISP 网关

【答案】B

【解析】

在路由表中找不到目标网络时使用默认路由。默认路由通常指本地网关的地址。

以下关于 OSPF 的区域 (Area) 的叙述中, 正确的是 (19)。

(19)A. 各个 OSPF 区域都要连接到主干区域

B. 分层的 OSPF 网络不需要多个区域

C. 单个 OSPF 网络只有区域 1

D. 区域 ID 的取值范围是 1~32768

【答案】A

【解析】

为了适应大型网络配置的需要, OSPF 协议引入了“分层路由”的概念。如果网络规模很大, 则路由器要学习的路由信息很多, 对网络资源的消耗很大, 所以典型的链路状态协议都把网络划分成较小的区域 (Area), 从而限制了路由信息传播的范围。每个区域就如同一个独立的网络, 区域内的路由器只保存该区域的链路状态信息, 使得路由器的链路状态数据库可以保持合理的大小, 路由计算的时间和报文数量都不会太大。OSPF 主干网负责在各个区域之间传播路由信息。

每个 OSPF 区域被指定了个 32 位的区域标识符, 可以用点分十进制表示, 例如主干区域的标识符可表示为 0.0.0.0 (Area0), 各个 OSPF 区域都要连接到主干区域。OSPF 的区域分为以下 5 种, 不同类型的区域对由自治系统外部传入的路由信息的处理方式 不同:

标准区域: 标准区域可以接收任何链路更新信息和路由汇总信息。

主干区域: 主干区域是连接各个区域的传输网络, 其他区域都通过主干区域交换路由信息, 主干区域拥有标准区域的所有性质,

存根区域: 不接受本地自治系统以外的路由信息, 对自治系统以外的目标采用默认路由 0.0.0.0。

完全存根区域: 不接受自治系统以外的路由信息, 也不接受自治系统内其他区域的路由汇总信息, 发送到本地区域外的报文使用默认路由 0.0.0.0。完全存根区域是 Cisco 定义的, 是非标准的。

不完全存根区域 (NSAA): 类似子存根区域, 但是允许接收以类型 7 的链路状态公告发送的外部路由信息。

运行 OSPF 协议的路由器用 (20) 报文来建立和更新它的拓扑数据库。

- (20) A. 由其他路由器发送的链路状态公告 (LSA) B. 从点对点链路收到的信标
C. 由指定路由器收到的 TTL 分组 D. 从邻居路由器收到的路由表

【答案】A

【解析】

OSPF 路由器之间通过链路状态公告 (Link State Advertisement, LSA) 交换网络拓扑信息, 建立和更新自己的拓扑数据库。LSA 中包含连接的接口、链路的度量值 (Metric) 等信息。

链路状态路由协议的主要特点是 (21)。

- (21) A. 邻居之间交换路由表 B. 通过事件触发及时更新路由
C. 周期性更新全部路由表 D. 无法显示整个网络拓扑结构

【答案】B

【解析】

运行链路状态路由协议 (例如 OSPF) 的路由器通过各自的接口连接到一个共同的网络上, 它们之间是邻居关系。在一个广播网络或 NBMA 网络中要选举一个指定路由器 (DR), 其他路由器都与 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, 所以链路状态协议是通过组播机制来共享路由信息的。链路状态协议只是在网络拓扑结构出现变化时才通过事件触发机制增量式地发送路由更新消息。与之相反, 距离矢量协议是在邻居之间周期性地交换路由表。

从下面一条 RIP 路由信息中可以得到的结论是 (22)。

R 10.10.10.7 [120/2] via 10.10.10.8, 00:00:24, Serial 0/1

- (22) A. 下一个路由更新将在 36 秒之后到达 B. 到达目标 10.10.10.7 的距离是两跳
C. 串口 S0/1 的 IP 地址是 10.10.10.8 D. 串口 S0/1 的 IP 地址是 10.10.10.7

【答案】B

【解析】

这一条 RIP 路由信息说明到达目标 10.10.10.7 的距离是两跳, 下一跳的地址是

10.10.10.8, 通过本地串口 S0/I 转发。

运行距离矢量路由协议的路由器 (23)。

- (23) A. 把路由表发送到整个路由域中的所有路由器
- B. 使用最短道路算法确定最佳路由
- C. 根据邻居发来的信息更新自己的路由表
- D. 维护整个网络的拓扑数据库

【答案】C

【解析】

运行距离矢量路由协议的路由器把自己的路由表发送给邻居路由器, 邻居路由器根据收到的路由信息更新自己的路由表, 再向其他邻居发送自己的路由表。这样使得路由变化信息在整个网络中逐步扩散开来。每个路由器只知道它连接的邻居, 而不能了解整个网络的拓扑连接情况。

以下关于 VLAN 的叙述中, 正确的是 (24)。

- (24) A. VLAN 对分组进行过滤, 增强了网络的安全性
- B. VLAN 提供了在大型网络中保护 IP 地址的方法
- C. VLAN 在可路由的网络中提供了低延迟的互联手段
- D. VLAN 简化了在网络中增加、移除和移动主机的操作

【答案】D

【解析】

把局域网划分成多个不同的 VLAN, 使得网络接入不再局限于物理位置的约束, 这样就简化了在网络中增加、移除和移动主机的操作, 特别是动态配置的 VLAN, 无论主机插在哪里, 它都处于自己的 VLAN 中。VLAN 内部可以相互通信, VLAN 之间不能直接通信, 必须经过特殊设置的路由器才可以连通。这样做的结果是, 通过在较大的局域网中创建不同的 VLAN, 可以抵御广播风暴的影响, 也可以通过设置防火墙来提高网络的安全性。VLAN 并不能直接增强网络的安全性。

当局域网中更换交换机时, 怎样保证新交换机成为网络中的根交换机? (25)。

- (25) A. 降低网桥优先级
- B. 改变交换机的 MAC 地址

- C. 降低交换机端口的根通路费用 D. 为交换机指定特定的 IP 地址

【答案】A

【解析】

在交换式局域网中由环路引起的循环转发破坏了网桥的数据库，使得网桥无法获得正确的转发信息。为了消除环路，从而发明了生成树协议。该协议规定，生成树的根是通过分布式选举算法产生的。每一个网桥有唯一的优先级和唯一的 MAC 地址，优先级+MAC 地址构成网桥的标识符，标识符最小的网桥自动成为生成树的根桥。所以为了保证新交换机成为网络中的根交换机，则必须降低网桥优先级。

双绞线电缆配置如下图所示，这种配置支持(26)之间的连接。

Pin Number	Color	Function	Pin	Color	Function
1	white/Green	TX+	3	Orange	RX-
2	Green	TX-	6	white/Orange	RX-
3	white/Orange	RX+	1	Green	TX+
6	Orange	RX-	2	white/Green	TX-

- (26) A. PC 到路由器 B. PC 到交换机 C. 服务器到交换机 D. 交换机到路由器

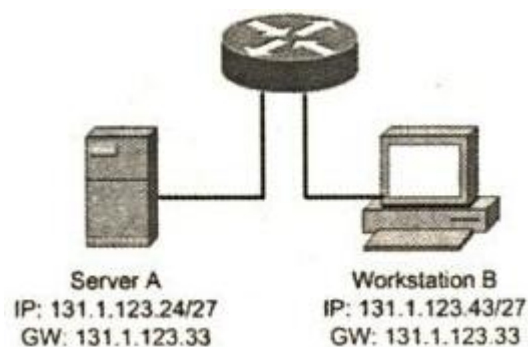
【答案】A

【解析】

图中的双绞线是交叉双绞线，用来连接同类设备，4 个选项中只有 PC 和路由器是同类设备。

参加下图的网络配置，发现工作站 B 无法与服务器 A 通信，什么故障影响了两者互通？

(27)。



- (27) A. 服务器 A 的 IP 地址是广播地址 B. 服务器 B 的 IP 地址是网络地址
C. 工作站 B 与网关不属于同一子网 D. 服务器 A 与网关不属于同一子网

【答案】D

【解析】

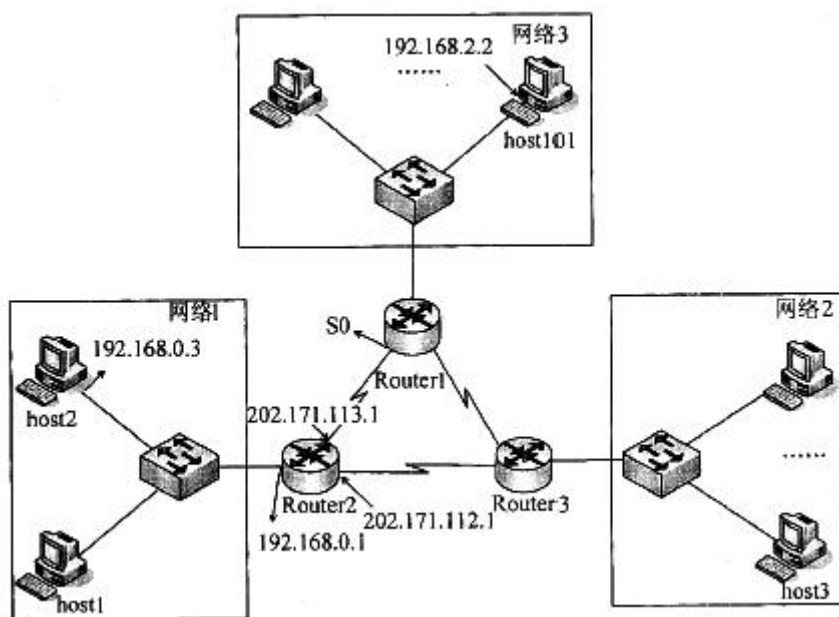
服务器 A 的 IP 地址 131.1.123.24/27: 10000011.00000001. 01111011.00011000 服务器 A 的地址不是广播地址。

服务器 A 的网关地址 131.1.123.33: 10000011.00000001. 01111011.00100001 这个地址与服务器 A 的地址不属于同一个子网。

工作站 B 的 IP 地址 131.1.123.43/27: 10000011.00000001. 01111011.00101011 这个地址不是网络地址。

工作站 B 的网关地址 131.1.123.33: 10000011.00000001. 01111011.00100001 工作站 B 与网关属于同一个子网。

某网络拓扑图如下所示，若采用 RIP 协议，在路由器 Router2 上需要进行 RIP 声明的网络是 (28)。



(28) A. 仅网络 1

B. 网络 1、202.117.112.0/30 和 202.117.113.0/30

C. 网络 1、网络 2 和网络 3

D. 仅 202.117.112.0/30 和 202.117.113.0/30

【答案】B

【解析】 本题考查路由器上 RIP 路由协议的配置。

在路由器中采用 RIP 协议时,每个路由器需要声明直接连接的各个网络,路由器 Router2 直接连接了网络 1、202.117.112.0/30 和 202.117.113.0/30 三个网络,均需进行声明。

IIS 服务身份验证方式中,安全级别最低的是_(29)。

- (29)A. .NET PASSPORT 身份验证 B. 集成 Windows 身份验证
C. 基本身份验证 D. 摘要式身份验证

【答案】C

【解析】本题考查 IIS 服务器配置及安全性等知识。

IIS 服务身份验证方式有摘要式身份验证、基本身份验证、.NET Passport 身份验证和集成 Windows 身份验证,其中安全级别最低的是基本身份验证。

有较高实时性要求的应用_(30)。

- (30)A. 电子邮件 B. 网页浏览 C. VoIP D. 网络管理

【答案】C

【解析】本题考查 Internet 应用及相关知识。

不同的应用有不同的实时性要求,电话、音频和视频有较高的实时性要求。故有较高实时性要求的应用是 VoIP。

在 Linux 中,文件_(31)_用于解析主机域名。

- (31)A. etc/hosts B. etc/host.conf C. etc/hostname D. etc/bind

【答案】B

【解析】本题考查 Linux 系统文件的基本知识。

etc/hosts 中包含了 IP 地址和主机名之间的映射,还包括主机名的别名;etc/host.conf 文件指定如何解析主机域名,Linux 通过解析器库来获得主机名对应的 IP 地址;etc/hostname 文件中包含了 Linux 系统的主机名称,包括完全的域名;D 选项中的 etc/bind 是一个干扰项。

在 Linux 中,要删除用户组 group1 应使用_(32)_命令。

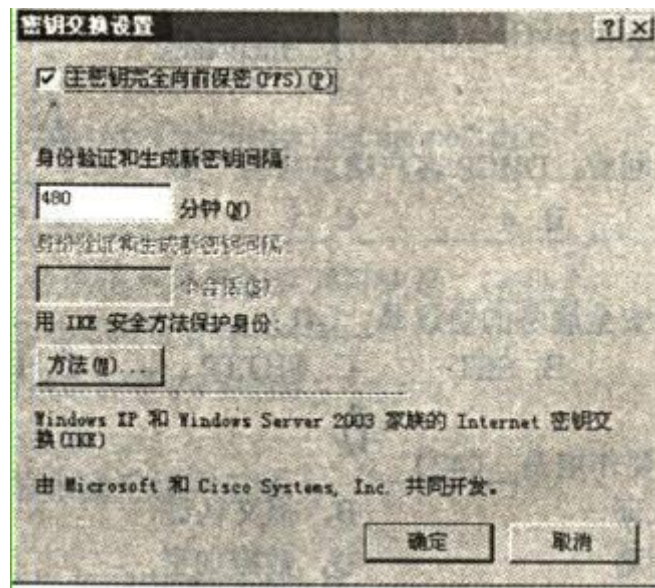
- (32)A. [root@localhost]#delete group1 B. [root@localhost]#gdelete group1
C. [root@localhost]#groupdel group1 D. [root@localhost]#gd group1

【答案】C

【解析】本题考查 Linux 系统命令的使用方法。

要删除用户组需使用的命令是 `groupdel group1`, 其他各个选项均为错误的对命令的缩写和简写。

Windows server2003 采用 IPSec 进行保密通信, 如果密钥交换采用“主密钥完全向前保密 (PFS)”, 则“身份验证和生成密钥间隔”默认值为 480 分钟和 (33) 个会话。



(33)A. 1

B. 2

C. 161

D. 530

【答案】A

【解析】本题考查 IPSec 基础知识。

IPSec 使用称为动态重新加密的方法来控制通信过程中生成新密钥的频率。通信以块的形式发送, 对每个数据块都使用不同的密钥进行保护, 这样可防止已经获取部分通信和相应的会话密钥的攻击者获取其余部分的通信。如果“启用主密钥完全向前保密 (PFS)”, 则不使用快速模式会话密钥刷新限制。

将会话密钥刷新限制设置为 1, 与启用主密钥 PFS 的效果相同。

在 Windows 用户管理中, 使用组策略 A-G-DL-P, 其中 P 表示 (34)。

(34)A. 用户账号

B. 资源访问权限

C. 域本地组

D. 通用组

【答案】B

【解析】本题考查 Windows 用户管理的组策略基础知识。

组策略 A-G-DL-P 中 A 表示用户账号，G 表示全局组，DL 表示域本地组，P 表示资源访问权限（Permission）。A-G-DL-P 策略是将用户账号添加到全局组中，将全局组添加到另一个域的域本地组中，然后为域本地组分配本地资源的访问权限，这样来自其他域的用户就可以访问本地域中的资源了。

以下叙述中，不属于无源光网络优势的是 (35)。

- (35) A. 设备简单，安装维护费用低，投资相对较小
B. 组网灵活，支持多种拓扑结构
C. 安装方便，不要另外租用或建造机房
D. 无源光网络适用于点对点通信

【答案】 D

【解析】 本题考查无源光网络 (PON) 方面的基础知识。

无源光网络 (PON) 是一种纯介质网络, 避免了外部设备的电磁干扰和雷电影响, 减少了线路和外部设备的故障率, 提高了系统可靠性, 同时节省了维护成本。

分光器就是连接 OLT 和 ONU 的无源设备，它的功能是分发下行数据，并集中上行数据。分光器带有一个上行光接口，若干下行光接口，实现点对多点的通讯。

查看 DNS 缓存记录的命令是 (36)。

- (36) A. ipconfig/flushdns
B. nslookup
C. ipconfig/release
D. ipconfig/displaydns

【答案】D

【解析】本题考查 ipconfig 及 nslookup 网络管理命令。

ipconfig /flushdns 是清除 DNS 缓存记录;ipconfig /displaydns 为显示 DNS 缓存记录;
nslookup 为显示域名解析服务器;ipconfig /release 是释放 DHCP 自动分配的 IP 地址。

在 Windows 操作系统中，(37) 文件可以帮助域名解析。

- (37) A. cookie B. index C. hosts D. default

【答案】C

【解析】 本题考查 hosts 域名解析文件。

在 Windows 操作系统中，可以帮助域名解析的文件是 hosts。

DHCP (38) 报文的目 IP 地址为 255.255.255.255。

(38) A. DhcpDiscover B. DhcpOffer C. DhcpNack D. DhcpAck

【答案】A

【解析】 本题考查 DHCP 的报文格式。

四种报文格式中，采用广播的只有 DhcpDiscover。当主机启动时需要自动分配 IP 地址，又不知道 DHCP 服务器地址，故请求报文 DhcpDiscover 中目的 IP 地址为 255.255.255.255。

客户端采用 (39) 报文来拒绝 DHCP 服务器提供的 IP 地址。

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

【答案】B

【解析】 本题考查 DHCP 的报文格式及各自应用场合。

DhcpOffer 为 DHCP 服务器给客户机提供 IP 地址的相应报文；如果客户端拒绝服务器提供的 IP 地址，采用 DhcpDecline；当 DHCP 服务器接收到客户端的 Dhcprequest 之后，会向客户端发出一个 DHCPACK 回应提供地址给客户，或者发出一个 DHCPNACK 回应不提供地址给客户。

若一直得不到回应，DHCP 客户端总共会广播 (40) 次请求。

(40) A. 3 B. 4 C. 5 D. 6

【答案】B

【解析】 本题考查 DHCP 协议的工作模式。

在 Windows 的预设情形下，Dhcpdiscover 的等待时间预设为 1 秒，也就是当客户端将第一个 Dhcpdiscover 包送出去之后，在 1 秒之内没有得到回应的话，就会进行第二次 Dhcpdiscover 广播。若一直得不到回应的情况下，客户端一共会有 4 次 Dhcpdiscover 广播，除了第一次会等待 1 秒之外，其余三次的等待时间分别是 9, 13, 16 秒。如果都没有得到 DHCP 服务器的回应，客户端则会显示错误信息，宣告 Dhcpdiscover 的失败。之后，基于使用者的选择，系统会继续在 5 分钟之后再重复一次 Dhcpdiscover 的过程。

提供电子邮件安全服务的协议是 (41)。

(41) A. PGP B. SET C. SHTTP D. Kerberos

【答案】A

【解析】 本题考查安全电子邮件协议的基础知识。

PGP (Pretty Good Privacy)是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。它能够在各种平台上免费试用,并得到了众多的制造商支持。PGP 提供数据加密和数字签名服务,可用于电子邮件的加密和签名。

SET (Secure Electronic Transaction)是安全电子交易的英文简写,它是一种安全协议和报文格式的集合,融合了 Netscape 的 SSL、Microsoft 的 STT、Terisa 的 S-HITP 以及 PKI 技术,通过数字证书和数字签名机制,使得客户可以与供应商进行安全的电子交易。目前,SET 已经获得了 Mastercard、Visa 等众多厂商的支持,成为电子商务安全中的安全基础设施。

SHTTP 也可以写作 S-HPPT,是一种商向报文的安全通信协议,其目的是保证商业贸易信息的传输安全,促进电子商务的发展。但是在 SSL 出现后,S-HTTP 并未获得广泛的应用,目前,SSL 基本已经取代了 S-HTTP。

Kerberos 是一项认证服务,它要解决的问题是在公开的分布式环境中,工作站上的 用户希望通过安全的方式访问分布在网络的服务器。

IDS 设备的主要作用是 (42)。

(42)A. 用户认证 B. 报文认证 C. 入侵检测 D. 数据加密

【答案】C

【解析】 本题考查的是网络安全设备的功能。

IDS (Intrusion Detection System)入侵检测系统,是作为防火墙之后的第二道安全屏障,通过网络中关键地点收集信息并对其进行分析,从中发现违反安全策略的行为和遭到入侵攻击的迹象,并自动做出响应。

它的主要功能包括对用户和系统行为的监测与分析、系统安全漏洞的检查和扫描、重要文件的完整性评估、已知攻击行为的识别、异常行为模式的统计分析、操作系统的审计跟踪,以及违反安全策略的用户行为的检测等。入侵检测通过实时地监控入侵事件,在造成系统损坏或数据丢失之前阻止入侵者进一步的行动,使系统能尽快恢复正常工作。同时还要收集有关入侵的技术资料,用于改进和增强系统抵抗入侵的能力。

宏病毒可以感染后缀为 (43) 的文件。

(43) A. exe

B. txt

C. pdf

D. xls

【答案】D

【解析】本题考查病毒的基本知识。

宏病毒是一种脚本病毒，宏病毒的前缀是 Macro，第二前缀是 Word、Word 97、Excel、Excel 97 等。宏病毒可以寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

因此，只有微软的 Word 文档或者 Excel 文档才会感染宏病毒。

Kerberos 是一种 (44)。

(44) A. 加密算法

B. 签名算法

C. 认证服务

D. 病毒

【答案】C

【解析】本题考查的是认证的基本知识。

Kerberos 是一项认证服务，它要解决的问题是：在公开的分布式环境中，工作站上的用户希望通过安全的方式访问分布在网络的服务器。

Kerberos 的设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无须基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下，Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。

以下关于三重 DES 加密的叙述中，正确的是 (45)。

(45) A. 三重 DES 加密使用一个密钥进行三次加密

B. 三重 DES 加密使用两个密钥进行三次加密

C. 三重 DES 加密使用三个密钥进行三次加密

D. 三重 DES 加密的密钥长度是 DES 密钥长度的 3 倍

【答案】B

【解析】本题考查的是三重 DES 加密的基本知识。

三重 DES 加密谁的 DES 加密算法的改进算法，它使用两把密钥对待加密报文作三次 DES

加密，其效果相当将 DES 密钥的长度加倍，从而克服了 DES 密钥长度较短的缺点。其加密的过程如下：

假设两个密钥分别为 K1 和 K2, 其加密过程是：

- ①用密钥 K1 进行 DES 加密。
- ②用 K2 对步骤（1）的结果进行 DES 解密。
- ③对步骤（2）的结果使用密钥 K1 进行 DES 加密。

SNMP 协议属于 (46) 层协议。

- (46) A. 物理 B. 网络 C. 传输 D. 应用

【答案】D

【解析】 本题考查 SNMP 方面的基础知识。

SNMP 为应用层协议，是 TCP/IP 协议族的一部分。它通过用户数据报协议（UDP）来操作。在分立的管理站中，管理者进程对位于管理站中心的 MIB 的访问进行控制，并提供网络管理员接口。管理者进程通过 SNMP 完成网络管理。

SNMPv3 新增了 (47) 功能。

- (47) A. 管理站之间通信 B. 代理 C. 认证和加密 D. 数据块检索

【答案】C

【解析】 本题考查 SNMPv3 方面的基础知识。

SNMPv3 通过对数据进行认证和加密，确保数据在传输过程中不被篡改。确保数据从合法的数据源发出、加密报文，确保数据的机密性等安全特性。

网络管理系统中故障管理的目标是 (48)。

- (48) A. 自动排除故障 B. 优化网络性能 C. 提升网络安全 D. 自动监测故障

【答案】D

【解析】 本题考查网络管理系统方面的基础知识。

ISO/IEC74984 文档定义了网络管理的相关知识，其中故障管理的目标应包括：故障监测、故障报警、故障信息管理、排错支持工具、检索/分析故障信息等内容。

一台主机的浏览器无法访问域名为 www.sohu.com 的网站，并且在这台计算机执行

tracert 命令时有如下信息:

```
Tracing route to www.sohu.com [202.113.96.10]Over maximum of 30 hops:
 1 <1ms <1ms <1ms 59.67.148.1
 2 59.67.148.1 reports:Destination net unreachable
Trace complete
```

根据以上信息,造成这种现场的原因可能是 (49)。

- (49)A. 该计算机 IP 地址设置有误 B. 相关路由器上进行了访问控制
C. 本地网关不可达 D. 本地 DNS 服务器工作不正常

【答案】B

【解析】本题考查网络管理命令 tracert 的使用及相关结果分析方面的基础知识。

59.67.148.1 是第 1 跳即网关,从返回的延迟信息可以看到到网关的连接很顺畅,排除了 A 和 C;再由输入的是域名 www.sohu.com 能正常地解析到地址 202.113.96.10,说明本地 DNS 服务器工作正常;到达网关之后到不了下 1 跳,极大可能是出口路由器上进行了访问控制。

使用 netstat-o 命令可显示网络 (50)。

- (50)A. IP、ICMP、TCP、UDP 协议的统计信息 B. 以太网统计信息
C. 以数字格式显示所有连接、地址及端口 D. 每个连接的进程 ID

【答案】D

【解析】本题考查网络管理命令 netstat 的使用及相关参数的作用。

netstat 命令用于显示 TCP 连接。Netstat 命令的语法如下:

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

对以上参数解释如下:

-a

显示所有活动的 TCP 连接,以及正在监听的 TCP 和 UDP 端口。

e

显示以太网统计信息,例如发送和接收的字节数,以及出错的次数等。这个参数可以与-s 参数联合使用。

-n

显示活动的 TCP 连接,地址和端口号以数字形式表示。

-o

显示活动的 TCP 连接以及每个连接对应的进程 ID。在 Windows 任务管理器中可以找到与进程 ID 对应的应用。这个参数可以与 -a、-n 和 -p 联合使用。

-p Protocol

用标识符 Protocol 指定要显示的协议，可以是 TCP、UDP、TCPv6 或者 UDPv6。如果与参数 -s 联合使用，则可以显示协议 TCP、UDP，ICMP、IP、TCPv6、UDPv6，ICMPv6 或 IPv6 的统计数据。

-s

显示每个协议的统计数据。默认情况下，统计 TCP、UDP、ICMP 和 IP 协议发送和接收的数据包、出错的数据包、连接成功或失败的次数等。如果与 -p 参数联合使用，可以指定要显示统计数据的协议，

-r

显示 IP 路由表的内容，其作用等价于路由打印命令 `route print`

Interval

说明重新显示信息的时间间隔，键入 Ctrl+C 则停止显示。如果不使用这个参数，则只显示一次。

IEEE 802.1x 是一种基于_(51)_认证协议。

(51)A. 用户 ID B. 报文 C. MAC 地址 D. SSID

【答案】C

【解析】

IEEE 802.1x 协议实现基于端口（MAC 地址）的访问控制。认证系统对连接到链路对端的请求者进行认证。一般在用户接入设备上实现 802.1x 认证。在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的可以顺利地通过以太网端口。

为了弥补 WEP 协议的安全缺陷，WPA 安全认证方案增加的机制是_(52)。

(52)A. 共享密钥认证 B. 临时密钥完整性协议
C. 较短的初始化向量 D. 采用更强的加密算法

【答案】B

【解析】

有线等效保密 WEP 的设计目的是提供与有线局域网等价的机密性。WEP 使用 RC4 协议进行加密, 并使用 CRC-32 校验保证数据的完整性。

最初的 WEP 标准使用 24bit 的初始向量, 加上 40bit 的字符串, 构成 64bit 的 WEP 密钥。后来美国政府也允许使用 104bit 的字符串, 加上 24bit 的初始向量, 构成 128bit 的 WEP 密钥。然而 24bit 的 IV 并没有长到足以保证不会出现重复, 只要网络足够忙碌, 在很短的时间内就会耗尽可用的 IV 而使其出现重复, 这样 WEP 密钥也就重复了。

Wi-Fi 联盟厂商以 802.11i 草案的子集为蓝图制定了称为 WPA (Wi-Fi Protected Access) 安全认证方案。在 WPA 的设计中包含了认证、加密和数据完整性校验三个组成部分。首先是 WPA 使用了 802.1x 协议对用户的 MAC 地址进行认证; 其次是 WEP 增大了密钥和初始向量的长度, 以 128bit 的密钥和 48 位的初始向量 (IV) 用于 RC4 加密。WPA 还采用了可以动态改变密钥的临时密钥完整性协议 TKIP, 以更频繁地变换密钥来减少安全风险。最后, WPA 强化了数据完整性保护, 使用报文完整性编码来检测伪造的数据包, 并且在报文认证码中包含有帧计数器, 还可以防止重放攻击。

由 DHCP 服务器分配的默认网关地址是 192.168.5.33/28, (53) 是本地主机的有效地址。

(53) A. 192.168.5.32 B. 192.168.5.55 C. 192.168.5.47 D. 192.168.5.40

【答案】D

【解析】

默认网关地址 192.168.5.33/28 的二进制: 11000000.10101000.00000101.00100001
192.168.5.32 的二进制: 11000000.10101000.00000101.00100000 这是一个子网地址。
192.168.5.55 的二进制: 11000000.10101000.00000101.00110111 这个地址与网关地址不在同一子网中。
192.168.5.47 的二进制: 11000000.10101000.00000101.00101111 这是一个广播地址。
192.168.5.40 的二进制: 11000000.10101000.00000101.00101000 这是本地主机的有效地址。

如果指定的地址掩码是 255.255.254.0, 则有效的主机地址是 (54)。

(54) A. 126.17.3.0 B. 174.15.3.255 C. 20.15.36.0 D. 115.12.4.0

【答案】A

【解析】

地址掩码是 255.255.254.0, 所以主机地址占最后的 9 位。

126.17.3.0 地址的二进制为: 01111110.00010001.00000011.00000000 这是一个有效的主机地址。

174.15.3.255 的二进制: 10101110.00001111.00000011.11111111 这是一个广播地址。

20.15.36.0 的二进制: 00010100.00001111.00100100.00000000 这是一个子网地址。

115.12.4.0 的二进制: 01110011.00001100.00000100.00000000 这也是一个子网地址。

如果要检查本机的 IP 协议是否工作正常, 则应该 ping 的地址是 (55)。

(55)A. 192.168.0.1 B. 10.1.1.1 C. 127.0.0.1 D. 128.0.1.1

【答案】C

【解析】

要检查本机的 IP 协议是否工作正常, 则应该 ping 的地址是 127.0.0.1, 该地址在 Windows 中被称为本地回环地址 (LoopbackAddress)。

工作站 A 的 IP 地址是 202.117.17.24/28, 而工作站 B 的 IP 地址是 202.117.17.100/28, 当两个工作站直接相连时不能通信, 怎样修改地址才能使得这两个工作站可以互相通信? (56)。

- (56)A. 把工作站 A 的地址改为 202.117.17.15
B. 把工作站 B 的地址改为 202.117.17.112
C. 把子网掩码改为 25
D. 把子网掩码改为 26

【答案】C

【解析】

工作站 A 的 IP 地址是 202.117.17.24/28: 11001010.01110101.00010001.00011000
工作站 B 的 IP 地址是 202.117.17.100/28: 11001010.01110101.00010001.01101000
当前的这两个地址不属于同一个子网, 把地址掩码改为 25 就属于同一个子网了。

运营商指定本地路由器接口的地址是 200.15.10.6/29, 路由器连接的默认网关的地址是 200.15.10.7, 这样配置后发现路由器无法 ping 通任何远程设备, 原因是 (57)。

- (57) A. 默认网关的地址不属于这个子网 B. 默认网关的地址是子网中的广播地址
C. 路由器接口地址是子网中的广播地址 D. 路由器接口地址是组播地址

【答案】B

【解析】

本地路由器接口的地址 200.15.10.6/29: 11001000.00001111. 00001010.00000110

默认网关的地址 200.15.10.7: 11001000.00001111. 00001010.00000111

默认网关的地址是广播地址。

访问控制列表(ACL)配置如下,如果来自因特网的HTTP报文的目标地址是162.15.10.10,经过这个ACL过滤后会出现什么情况? (58)。

```
Router#show access-lists
Extended IP access list 110
 10 deny tcp 162.15.0.0 0.0.255.255 any eq telnet
 20 deny tcp 162.15.0.0 0.0.255.255 any eq smtp
 30 deny tcp 162.15.0.0 0.0.255.255 any eq http
 40 permit tcp 162.15.0.0 0.0.255.255 any
```

- (58) A. 由于行 30 拒绝, 报文被丢弃
B. 由于行 40 允许, 报文被接受
C. 由于 ACL 末尾隐含的拒绝, 报文被丢弃
D. 由于报文源地址未包含在列表中, 报文被接受

【答案】C

【解析】

语句 10 deny tcp 162.15.0.0 0.0.255.255 any eq telnet 的作用是拒绝来自162.15.0.0 网络的 telnet 访问。

语句 20 deny tcp 162.15.0.0 0.0.255.255 any eq smtp 的作用是拒绝来自162.15.0.0 网络的 smtp 访问。

语句 30 deny tcp 162.15.0.0 0.0.255.255 any eq http 的作用是拒绝来自162.15.0.0 网络的 http 访问。来自因特网的目标地址是162.15.10.10 的 http 报文不能被这个语句过滤。语句 40 permit tcp 162.15.0.0 0.0.255.255 any 的作用是允许来自162.15.0.0 网络的任何访问。这个语句也不会过滤来自因特网的目标地址是162.15.10.10 的 http 报文。

所以来自因特网的目标地址是162.15.10.10 的 http 报文被 ACL 末尾隐含的拒绝语句阻

止，报文被丢弃。

下面的 4 个 IPv6 地址中，无效地址是 (59)。

(59) A. ::192:168:0:1

B. :2001:3452:4955:2367::

C. 2002:c0a8:101::43

D. 2003:dead:beef:4dad:23:34:bb:101

【答案】B

【解析】

4 个 IPv6 地址中，无效的地址是 B. :2001:3452:4955:2367:: 最后一对冒号的写法是错误的，其他 3 种写法都正确。::192:168:0:1 是一个 IPv4 地址，2002:c0a8:101::43 中的双冒号表示 4 个双字节，2003:dead:beef:4dad:23:34:bb:101 是完整的 IPv6 地址。

IPv6 站点通过 IPv4 网络通信需要使用隧道技术，常用的 3 种自动隧道技术是 (60)。

(60) A. VPN 隧道、PPTP 隧道和 IPsec 隧道

B. 6to4 隧道、6over4 隧道和 ISATAP 隧道

C. VPN 隧道、PPP 隧道和 ISATAP 隧道

D. IPsec 隧道、6over4 隧道和 PPTP 隧道

【答案】B

【解析】

IPv6 站点通过 IPv4 网络通信，最常用的 3 种自动隧道技术是 6to4 隧道、6over4 隧道和 ISATAP 隧道。

如果在网络的入口处通过设置 ACL 封锁了 TCP 和 UDP 端口 21、23 和 25，则能够访问该网络的应用是 (61)。

(61) A. FTP

B. DNS

C. SMTP

D. Telnet

【答案】B

【解析】

由于 TCP 和 UDP 端口 21、23 和 25 被封锁，它们分别是 FTP、Telnet 和 SMTP 的端口号，所以只有 DNS 应用可以访问该网络。

以太网采用物理地址的目的是 (62)。

(62) A. 唯一地标识第二层设备

B. 使用不同网络中的设备可以互相通信

C. 用于区分第二层的帧和第三层的分组

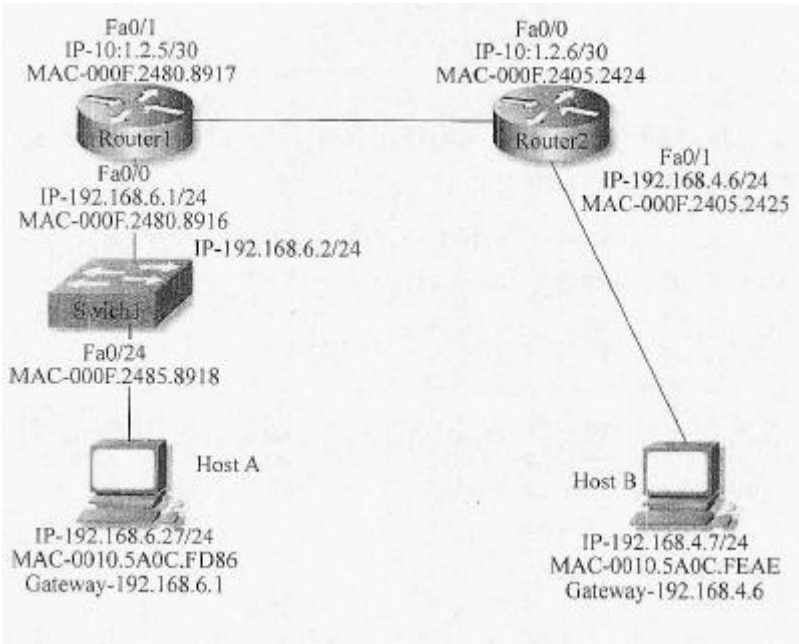
D. 物理地址比网络地址的优先级高

【答案】A

【解析】

以太网物理地址（即 MAC 地址）是第二层设备的唯一标识。

参加下面的网络连接图，4 个选项是 Host A 的 ARP 表，如果 HostA ping HostB，则 ARP 表中的哪一选项用来封装传输的帧？ (63)。



	Interface Address	Physical Address	Type
(63)A.	192.168.4.7	000f 2480 8916	dynamic
B.	192.168.4.7	0010 5a0c feae	dynamic
C.	192.168.6.2	0010 5a0c feae	dynamic
D.	192.168.6.1	000f 2480 8916	dynamic

【答案】D

【解析】

在 HostA 处组成的分组应该以 HostB 的 IP 地址 192. 168. 4. 7 为目标地址，查找本地 ARP 表，得到的不是 HostB 的 MAC 地址，而是边界路由器的 MAC 地址 000f2480 8916，所以 HostA 装配成帧时只能以边界路由器的 MAC 地址为目标地址，这就是说，路由器以自己的 MAC 地址代理了目标主机 HostB 的 MAC 地址，这就是代理 ARP 的概念，当两个主机不属于同一子网时，必须借助于这种机制才能互相通信。

4G 移动通信标准 TD-LTE 与 FDD-LTE 的区别是_(64)。

- (64)A. 频率的利用方式不同
B. 划分上下行信道的方式不同
C. 采用的调制方式有区别
D. 拥有专利技术的厂家不同

【答案】B

【解析】

LTE 标准由 TDD 和 FDD 两种不同的全双工模式组成，前者代表时分双工，上、下行在同一频段按照时间分配交叉进行，后者是上下行分处不同的频段。

关于移动 Ad Hoc 网络 MANET，_(65)_不是 MANET 的特点。

- (65)A. 网络拓扑结构是动态变化的
B. 电源能量限制了无线终端必须以最节能的方式工作
C. 可以直接应用传统的路由协议支持最佳路由选择
D. 每个结点既是主机又是路由器

【答案】C

【解析】

在移动 Ad Hoc 网络 MANET 中，每一个结点既是主机又是路由器，而且无线终端所带的电源能量有限，所以必须以最节能的方式工作。由于无线终端的移动，使得网络拓扑结构随时变化，传统的路由协议是不适用的，必须采用特别研制路由协议来支持最佳路由的选择。

_(66)_针对 TCP 连接进行攻击。

- (66)A. 拒绝服务
B. 暴力攻击
C. 网络侦察
D. 特洛伊木马

【答案】A

【解析】

拒绝服务主要是针对 TCP 连接进行攻击的，通过发送大量的建立连接请求，使得服务端穷于应付，无法提供正常的网络服务。暴力攻击是穷举式猜测用户密码。网络侦察是探测远端系统的漏洞，以便利用漏洞进行入侵。特洛伊木马是通过远端控制，对目标系统实施内部破坏或盗窃用户机密数据。

安全需求可划分为物理安全、网络安全、系统安全和应用安全，下面的安全需求中属于

系统安全的是 (67), 属于应用安全的是 (68)。

(67) A. 机房安全 B. 入侵检测 C. 漏洞补丁管理 D. 数据库安全

(68) A. 机房安全 B. 入侵检测 C. 漏洞补丁管理 D. 数据库安全

【答案】C D

【解析】

机房安全属于物理安全, 入侵检测属于网络安全, 漏洞补丁管理属于系统安全, 而数据库安全则是应用安全。

一个中等规模的公司, 3 个不同品牌的路由器都配置了 RIPv1 协议。ISP 为公司分配的地址块为 201. 113. 210. 0/24。公司希望通过 VLSM 技术把网络划分为 3 个子网, 每个子网中有 40 台主机, 下面的配置方案中最优的是 (69)。

(69) A. 转换路由协议为 EIGRP, 3 个子网地址分别设置 201. 113. 210. 32/27、201. 113. 210. 64/27 和 201. 113. 210. 92/27

B. 转换路由协议为 RIPv2, 3 个子网地址分别设置为 201. 113. 210. 64/26、201. 113. 210. 128/26 和 201. 113. 210. 192/26

C. 转换路由协议为 OSPF, 3 个子网地址分别设置为 201. 113. 210. 16/28、201. 113. 210. 16/28 和 201. 113. 210. 48/28

D. 保持路由协议为 RIPv1, 3 个子网地址分别设置为 201. 113. 210. 32/26、201. 113. 210. 64/26 和 201. 113. 210. 192/26

【答案】B

【解析】

每个子网中有 40 台主机, 所以主机地址要占用 6 位, 因而子网掩码必须是 26 位, 同时把路由协议由 RIPv1 转换为 RIPv2, 它是无类别的协议 (Classless Protocol), 可以使用可变长子网掩码 (VLSM), 也支持无类别域间路由 (CIDR)。

如果发现网络的数据传输很慢, 服务质量也达不到要求, 应该首先检查哪一个协议层工作情况? (70)。

(70) A. 物理层 B. 会话层 C. 网络层 D. 传输层

【答案】C

【解析】

如果网络的数据传输很慢,服务质量也达不到要求,通常先要检查网络层工作是否正常。网络故障诊断是从故障现象出发,以网络诊断工具为手段获取诊断信息,确定网络故障点,查找问题的根源,排除故障,恢复网络的正常运行。

网络故障通常有以下几种可能:

- 物理层中物理设备相互连接失败或者硬件和线路本身的问题;
- 数据链路层的网络设备的接口配置问题;
- 网络层网络协议配置或操作错误;
- 传输层的设备性能或通信拥塞问题;
- 网络应用程序错误。

诊断网络故障的过程应该沿着 OSI 7 层模型从物理层开始向上进行。首先检查物理层,然后检查数据链路层,以此类推,确定故障点。

Traditional network layer packet forwarding relies on the information provided by network layer (71) protocols, or static routing, to make an independent forwarding decision at each (72) within the network. The forwarding decision is based solely on the destination (73) IP address. All packets for the same destination follow the same path across the network if no other equal-cost (74) exist. Whenever a router has two equal-cost paths toward a destination, the packets toward the destination might take one or both of them, resulting in some degree of load sharing. Enhanced Interior Gateway Routing Protocol (EIGRP) also supports non-equal-cost (75) sharing although the default behavior of this protocol is equal-cost. You must configure EIGRP variance for non-equal-cost load balancing.

- | | | | |
|-------------------|-----------------|--------------|-------------|
| (71)A. switching | B. signaling | C. routing | D. session |
| (72)A. switch | B. hop | C. host | D. customer |
| (73)A. connection | B. transmission | C. broadcast | D. customer |
| (74)A. paths | B. distance | C. broadcast | D. session |
| (75)A. loan | B. load | C. content | D. constant |

【答案】 C B D A B

【解析】

传统的网络层分组转发是根据网络层路由协议或者静态路由提供的信息,在网络中的每

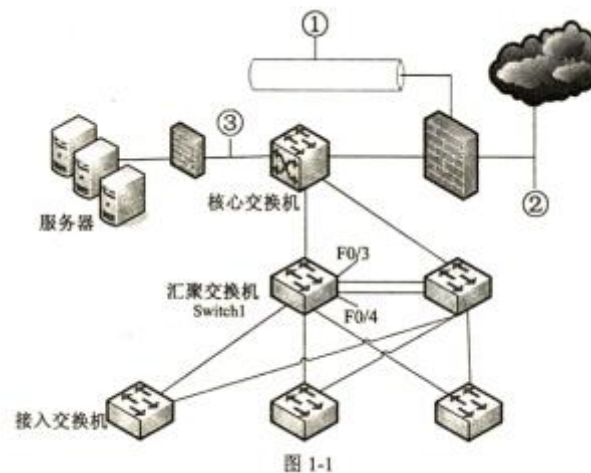
一跳都做出一个独立的转发决策。转发决策只是基于目标单播地址而做出的。如果没有相等费用的其他通路存在，朝着同一目标的所有分组都遵循网络中的同样路径。当路由器具有通向同一目标的相等费用的两条通路时，流向目标的分组就可能走两条通路中的任何一条，这就产生了同样程度的负载共享。增强的内部网关路由协议（EIGRP）也支持不等费用的负载共享，虽然这个协议默认的行为是相等费用的负载共享。通过配置，你可以把 EIGRP 变成不等费用的负载共享方式。

试题一

阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

【说明】

某企业网络拓扑图如图 1-1 所示。



工程师给出了该网络的需求：

1. 用防火墙实现内外网地址转换和访问控制策略；
2. 核心交换机承担数据转发，并且与汇聚层两台交换机实现 OSPF 功能；
3. 接入层到汇聚层采用双链路方式组网；
4. 接入层交换机对地址进行 VLAN 划分；
5. 对企业的核心资源加强安全防护。

【问题 1】（4 分）

该企业计划在①、②或③的位置部署基于网络的入侵检测系统(NIDS)，将 NIDS 部署在①的优势是（1）；将 NIDS 部署在②的优势是（2）、（3）；将 NIDS 部署在③的优势是（4）。

（1）～（4）备选答案：

- A. 检测外部网络攻击的数量和类型
- B. 监视针对 DMZ 中系统的攻击
- C. 监视针对关键系统、服务和资源的攻击
- D. 能减轻拒绝服务攻击的影响

（1） C

（2） A

(3) D

(4) B

本题考查网络规划以及组网的相关基础知识。包括入侵检测系统部署的技术规范，企业组网中路由协议的选用、线路聚合、生成树协议等相关知识。

入侵检测系统 (IDS) 可以基于主机部署也可以基于网络进行部署，将 IDS 部署在网络中不同的位置区域可以达到对网络中异常行为和攻击的识别，对特定网络区域的资源进行保护。例如，将 IDS 部署在网络出口常用于监测外部网络攻击的数量和类型。

【问题 2】(4 分)

OSPF 主要用于大型、异构的 IP 网络中，是对 (5) 路由的一种实现。若网络规模较小，可以考虑配置静态路由或 (6) 协议实现路由选择。

(5) 备选答案：A. 链路状态 B. 距离矢量 C. 路径矢量

(6) 备选答案：A. EGP B. RIP C. BGP

(5) A

(6) B

路由器提供了异构网互联的机制，实现将一个网络的数据包发送到另一个网络。而路由就是指导 IP 数据包发送的路径信息。路由协议就是在路由指导 IP 数据包发送过程中事先约定好的规定和标准。常见的路由协议分为动态路由和静态路由，而动态路由协议又距离矢量路由协议和链路状态路由协议。

OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。

【问题 3】(4 分)

对汇聚层两台交换机的 F0/3、F0/4 端口进行端口聚合，F0/3、F0/4 端口默认模式是 (7)，进行端口聚合时应配置为 (8) 模式。

(7)、(8) 备选答案：

A. multi B. trunk C. access

(7) C

(8) B

端口聚合也叫做以太通道 (Ethernet Channel), 主要用于交换机之间连接。由于两个交换机之间有多条冗余链路的时候, STP 会将其中的几条链路关闭, 只保留一条, 这样可以避免二层的环路产生。

同一个汇聚组中端口的配置应该保持一致, 即如果某端口为 trunk 端口, 则其他端口也配置为 trunk 端口; 如该端口的链路类型改为 access 端口, 则其他端口的链路类型也改为 access 端口。

【问题 4】(6 分)

为了在汇聚层交换机上实现虚拟路由冗余功能, 需配置 (9) 协议, 可以采用竞争的方式选择主路由设备, 比较设备优先级大小, 优先级大的为主路由设备。若备份路由设备长时间没有收到主路由设备发送的组播报文, 则将自己的状态转为 (10)。

为了避免二层广播风暴, 需要在接入与汇聚设备上配置 (11)。

(10)、(11) 备选答案:

A. Master B. Backup C. VTP Server D. MSTP

(9) VRRP 或者 HSRP

(10) A

(11) D

汇聚交换机采用虚拟路由冗余, 目的是当一台汇聚交换机出现故障时, 启用备份线路的措施。

根据设备情况可以采用虚拟路由器冗余协议 (VRRP) 或热备份路由器协议 (HSRP)。

生成树协议是一种二层管理协议, 它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的, 同时具备链路的备份功能。

【问题 5】(2 分)

阅读汇聚交换机 Switch 1 的部分配置命令, 回答下面的问题。

```
Switch 1(config)#interface vlan 20
```

```
Switch 1 (config-if)#ip address 192.168.20.253 255.255.255.0
```

```
Switch 1 (config-if)#standby 2 ip 192.168.20.250
```

```
Switch 1 (config-if)#standby 2 preempt
```

Switch 1 (config-id#exit

VLAN20standby 默认优先级的值是 (12) 。

VLAN20 设置 preempt 的含义是 (13)。

(12) 100

(13) 设置为抢占模式，或交换机故障恢复后抢占 vlan20 的控制权。

HSRP 协议利用优先级决定哪个路由器成为活动路由器。如果一个路由器的优先级比其他路由器的优先级高，则该路由器成为活动路由器，路由器的默认优先级是 100。

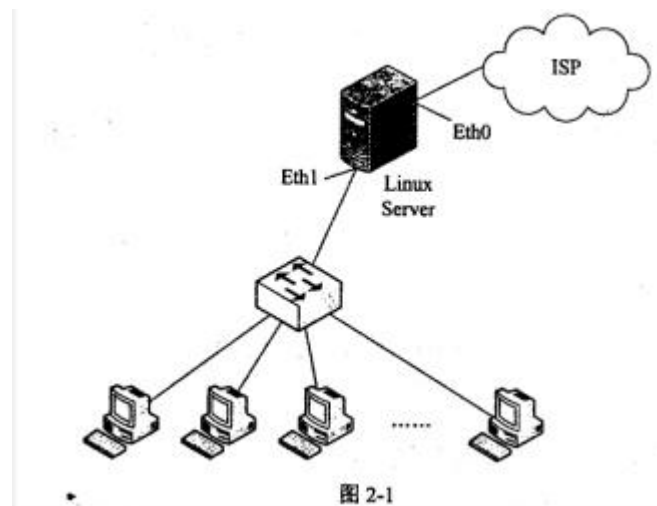
当在交换机上配置链路冗余或负载均衡后，保证故障设备恢复后正常工作，需要设置 preempt 模式。

试题二

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】

某公司内部搭建了一个小型的局域网，拓扑图如图 2-1 所示。公司内部拥有主机约 120 台，用 C 类地址段 192.168.100.0/24。采用一台 Linux 服务器作为接入服务器，服务器内部局域网接口地址为 192.168.100.254，ISP 提供的地址为 202.202.212.62。



【问题 1】(2 分)

在 Linux 中，DHCP 的配置文件是 (1)。

(1) `dhcpd.conf`

本题考查 Linux 服务器下 DHCP 服务器的配置。

DHCP 服务是一种动态的为客户端主机分配 IP 地址的服务，在 Linux 服务器中，该服务的配置文件是 `dhcpd.conf`。

【问题 2】(8 分)

内部邮件服务器 IP 地址为 192.168.100.253，MAC 地址为 01:A8:71:8C:9A:BB；内部文件服务器 IP 地址为 192.168.100.252，MAC 地址为 01:15:71:8C:77:BC。公司内部网络分为 4 个网段。

为方便管理，公司使用 DHCP 服务器为客户机动态配置 IP 地址，下面是 Linux 服务器为 192.168.100.192/26 子网配置 DHCP 的代码，将其补充完整。

Subnet (2) netmask (3)

```
{  
option routers 192.168.100.254;  
option subnet-mask (4) ;  
option broadcast-address (5);  
option time-offset -18000;  
  
range (6) (7) ;  
default-lease-time 21600;  
max-lease-time 43200;  
host servers  
{  
Hardware ethemet (8) ;  
fixed-address 192.168.100.253;  
hardware ethemet 01:15:71:8C:77:BC;  
fixed-address (9) ;  
}  
}
```

(2) 192.168.100.192

(3) 255.255.255.192

(4) 255.255.255.192

(5) 192.168.100.255

(6) 192.168.100.193

(7) 192.168.100.251

(8) 01:A8:71:8C:9A:BB

(9) 192.168.100.252

问题中给出了该公司所使用的 IP 地址所在子网为 192.168.100.192/26，网络号为 192.168.100.192，子网掩码为 255.255.255.192。本网的广播地址是将本网段中所有主机部分的二进制位数全部变为 1 得到，为 192.168.100.255。

空(6)和空(7)是要求计算该子网的 IP 地址范围，其有效的 IP 地址为 192.168.100.193-192.168.100.254。

空(8)和空(9)按照问题的描述，要求填写对应的硬件地址和 IP 地址。

【问题3】(2分)

配置代码中“option time-offset -18000”的含义是(10)。“default-lease-time 21600”表明，租约期为(11)小时。

(10) 备选答案：

A. 将本地时间调整为格林威治时间 B. 将格林威治时间调整为本地时间 C. 设置最长租约期

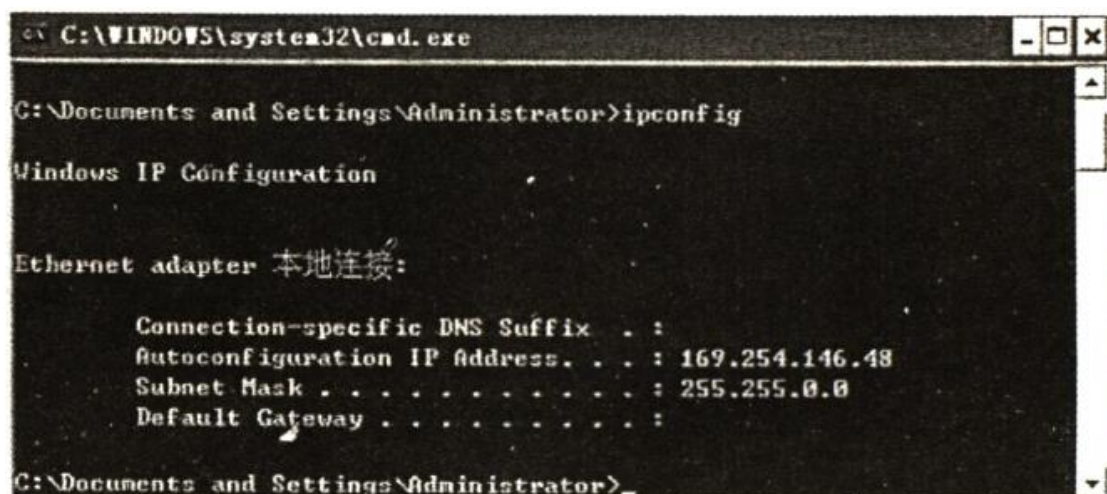
(10) B

(11) 6

option time-offset -18000 的配置项，是为了使得本地的 DHCP 服务器时间采用本地的时间进行计时，将从时间服务器中获取的格林威治时间调整到与本地时间同步的目的。default-lease-time 21600 的配置项是设置 IP 地址分配给客户端后的失效时间，改时间以秒为单位，即时间为 12600 秒，将其换算为小时的方法是 216000 秒/3600 秒=6 小时。

【问题4】(3分)

在一台客户机上使用 ipconfig 命令输出如图 2-2 所示，正确的说法是 (12)。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . :
    Autoconfiguration IP Address. . . : 169.254.146.48
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

C:\Documents and Settings\Administrator>
```

图 2-2

此时可使用(13)命令释放当前 IP 地址，然后使用(14)命令向 DHCP 服务器重新申请

IP 地址。

(12) 备选答案:

- A. 本地网卡驱动未成功安装
- B. 未收到 DHCP 服务器分配的地址
- C. DHCP 服务器分配给本机的 IP 地址为 169.254.146.48
- D. DHCP 服务器的 IP 地址为 169.254.146.48

(12) B

(13) `ipconfig/release`

(14) `ipconfig/renew`

图中所示的故障,是由于该客户端并未接收到系统的DHCP服务器所发来的IP地址配置信息,而有TCP/IP协议集为该客户端分配的169.254.x.x段的地址。169.254.x.x地址是IANA组织规定的保留地址,为了未采用DHCP服务器动态分配IP地址的用户,当未获取DHCP分配的IP地址时,自动使用该段地址,该段地址一般不能使网络正常运行。

试题三

阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。

【说明】

某企业在采用 Windows Server 2003 配置了共享打印、FTP 和 DHCP 服务。

【问题 1】（8 分）

1. Internet 共享打印使用的协议是（1）。（1 分）

（1）备选答案：

- A. PPI B. IPP C. TCP D. IP

2. Intemet 共享打印配置完成后，需在如图 3-1 所示的 Web 服务扩展选项卡中将“Active Server Pages”设置为“允许”，其目的是（2）。（2 分）



图 3-1

3. 检验 Internet 打印服务是否安装正确的方法是在 Web 浏览器的地址栏输入 URL 是（3）。（2 分）

（3）备选答案：

- A. HTTP: //127.0.0.1/PRINTERS
B. FTP: //127.0.0.1/PRINTERS
C. HTTP: //PRINTERS

D. FTP: //PRINTERS

4. 使用 Internet 共享打印流程为 6 个步骤:

- ①在终端上输入打印设备的 URL
- ②服务器向用户显示打印机状态信息
- ③客户端向打印服务器发送身份验证信息
- ④用户把要打印的文件发送到打印服务器
- ⑤打印服务器生成一个 cabinet 文件，下载到客户端
- ⑥通过 Internet 把 HTTP 请求发送到打印服务器

对以上步骤进行正确的排序（4）。（3 分）

(1) B

(2) 可采用页面显示打印机状态信息

(3) A

(4) ①⑥③②⑤④

本题考查 Windows Server 2003 配置共享打印、FTP 和 DHCP 服务等相关知识。

IPP 协议是一个基于 Internet 应用层的协议，它面向终端用户和终端打印设备。IPP 基于常用的 Web 浏览器向终端设备传送打印机的属性和状态信息需要将 Web 服务扩展选项卡中将“Active Server Pages”设置为“允许”。

Internet 打印流程如下：

- ①用户输入打印设备的 URL（统一资源定位符），通过 Internet 连接到打印服务器。
- ②HTTP 请求通过 Internet 发送到打印服务器。
- ③打印服务器要求客户端提供身份验证信息。这样能够确保只有经过授权的用户才能在打印服务器上打印文件。
- ④当用户获得授权可以访问打印服务器后，服务器使用活动服务器页(Active Server Pages, ASP)向用户显示状态信息，其中包括有关当前空闲打印机的信息。
- ⑤当用户连接 Internet 打印网页上的任何打印机时，客户端计算机首先尝试在本地寻找该打印机的驱动程序。如果没有找到适合的驱动程序，打印服务器将会生成一个 Cabinet 文件（.cab 文件，又称为 Setup 文件），其中包含正确的打印机驱动程序文件。打印服务器把.cab 文件下载到客户端计算机上。客户端计算机提示用户允许下载该.cab 文件。

⑥当用户连接到 Internet 打印机后，他们可以使用 Internet 打印协议 (Internet Printing Protocol, IPP) 把文件发送到打印服务器。

【问题 2】(8 分)

FTP 的配置如图 3-2、图 3-3 所示。

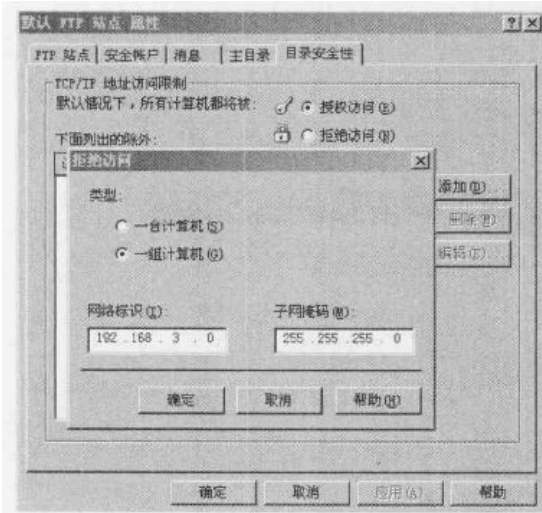


图 3-2

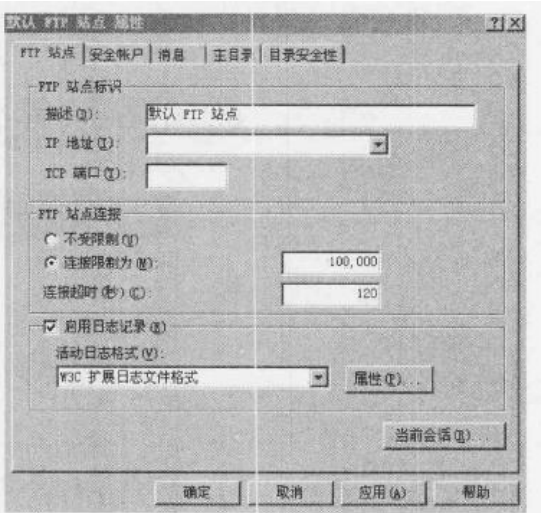


图 3-3

1. 默认情况下，用户登录 FTP 服务器时，服务器端建立的 TCP 端口号为 (5)。
2. 如果只允许一台主机访问 FTP 服务器，参考图 3-2 给出具体的操作步骤 (6) 。
3. 参考图 3-3，在一台服务器上搭建多个 FTP 站点的方法是 (7)。
4. 如点击图 3-3 中“当前会话”按钮，显示的信息是 (8) 。

(5) 21

(6) 在“目录安全性”页面选中“拒绝访问”，单击“添加”，在弹出的“授权访问”页面，选中“一台计算机”，填入允许访问的主机 IP

(7) 增加 IP 地埤或修改 TCP 端口

(8) 连接 FTP 的用户或主机的信息

在 Windows Server 2003 环境下安装 FTP 服务需要在“Internet 信息服务”组件中添加“文件传输协议 (FTP)”功能模块。该功能模块的配置可以实现特定用户对 FTP 的访问、建立多个 FTP 站点、显示用户连接 FTP 状态等功能。

FTP 服务器端建立的 TCP 端口号是 21。

【问题 3】（4 分）

DHCP 的配置如图 3-4 和 3-5 所示。

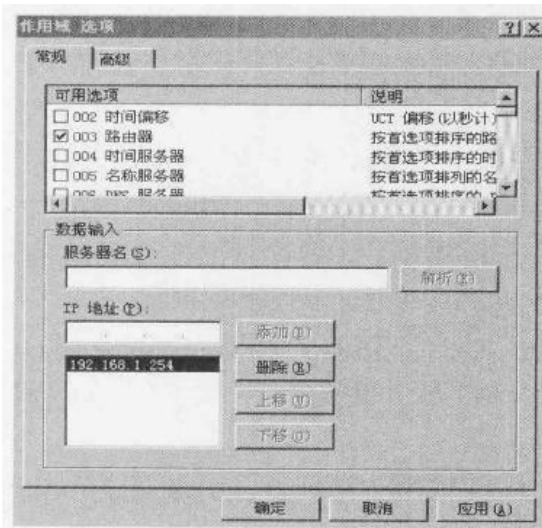


图 3-4

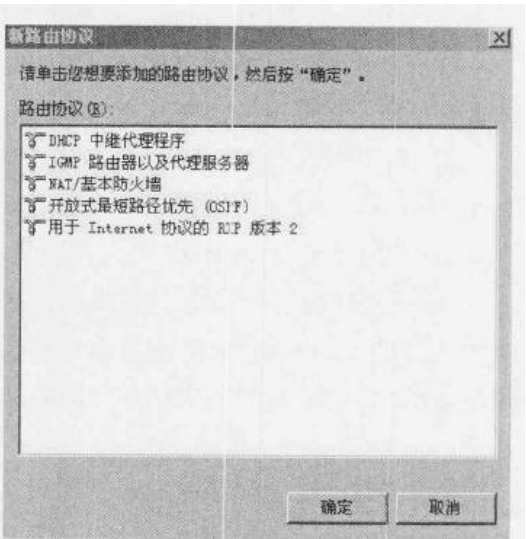


图 3-5

1. 图 3-4 中填入的 IP 地址是 （9） 。
2. 图 3-5 中配置 DHCP 中继代理程序，可以实现（10）。

（9） 备选答案：

- A. 分配给客户端的 IP 地址
- B. 默认网关的 IP 地址
- C. DHCP 服务器的 IP 地址

（10） 备选答案：

- A. 使普通客户机获取 IP 等信息
- B. 跨网段的地址分配
- C. 特定用户组访问特定网络

（9） B

（10） B

动态主机分配协议（DHCP）是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 Wmdows Server 2003 提供的组件进行 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作。在进行 DHCP 服务器配置时需要填入待分配的 IP 段以及默认网关等信息。

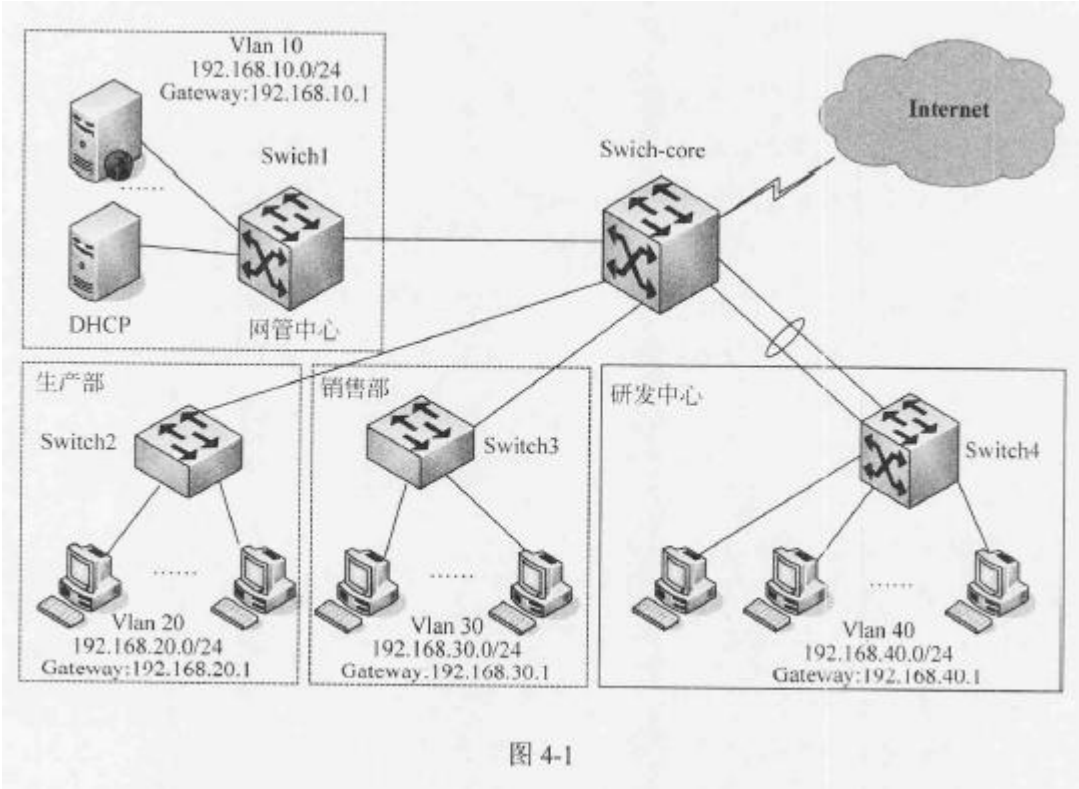
在大型的网络中，可能会存在多个子网。DHCP 客户机通过网络广播消息获得 DHCP 服务器的响应后得到 IP 地址。但广播消息是不能跨越子网的。如果 DHCP 客户机和服务器在不同的子网内，就要用到 DHCP 中继代理。

试题四

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】

某企业的网络拓扑结构如图 4-1 所示。



由于该企业路由设备数量较少，为提高路由效率，要求为企业构建基于静态路由的多层安全交换网络。根据要求创建 4 个 VLAN 分别属于网管中心、生产部、销售部以及研发中心，各部门的 VLAN 号及 IP 地址规划如图 4-1 所示。该企业网采用三层交换机 Switch-core 为核心交换机，Switch-core 与网管中心交换机 Switch1 和研发中心交换机 Switch4 采用三层连接，Switch-core 与生产部交换机 Switch2 及销售部交换机 Switch3 采用二层互联。各交换机之间的连接以及接口 IP 地址如表 4-1 所示。

表 4-1 各交换机之间的连接以及接口 IP 地址表							
上联端口				下联端口			
交换机	端口	描述	IP 地址	交换机	端口	描述	IP 地址
Switch-core	G0/1	scsw-g1/1		Switch2	G1/1	core-g0/1	
	G0/2	wgsw-g0/1	192.168.101.1/24	Switch1	G0/1	core-g0/2	192.168.101.2/24
	F0/1	yfsw-f0/1	192.168.102.1/24	Switch4	F0/1	core-f0/1	192.168.102.2/24
	F0/2	yfsw-f0/2			F0/2	core-f0/2	
	F0/3	yfsw-f0/3			F0/3	core-f0/3	
	F0/4	yfsw-f0/4			F0/4	core-f0/4	
	F0/5	xssw-f0/1		Switch3	F0/1	core-f0/5	

【问题 1】（4 分）

随着企业网络的不断发展，研发中心的上网计算机数急剧增加，在高峰时段研发中心和核心交换机之间的网络流量非常大，在不对网络进行大的升级改造的前提下，网管人员采用了以太信道（或端口聚合）技术来增加带宽，同时也起到了（1）和（2）的作用，保证了研发中心网络的稳定性和安全性。

在两台交换机之间是否形成以太信道，可以用协议自动协商。目前有两种协商协议：一种是（3），是 Cisco 私有的协议；另一种是（4），是基于 IEEE 802.3ad 标准的协议。

（3）、（4）备选答案：

- A. 端口聚合协议 (PAgP)
- B. 多生成树协议 (MSTP)
- C. 链路聚合控制协议 (LACP)

（1）负载均衡

（2）链路冗余

（3）A

（4）C

本题考查使用三层交换机实现 VLAN 间路由的相关知识点和配置命令。

本问题主要考查以太信道（或端口聚合）技术。

EtherChannel 是由 Cisco 研发的，应用于交换机之间的多链路捆绑技术。它的基本原理是：将两个设备间多条相同特性的快速以太或千兆位以太物理链路捆绑在一起组成一条逻辑链路，从而达到带宽倍增的目的。除了增加带宽外，EtherChannel 还可以在多条链路上均衡分配流量，起到负载均衡的作用；当一条或多条链路故障时，只要还有链路正常，流量将转移到其他的链路上，整个过程在几毫秒内完成，从而起到链路冗余的作用，增强了网络的稳定性和安全性。在 EtherChannel 中，负载在各个链路上的分布可以根据源 IP 地址、目的 IP 地址、源 MAC 地址、目的 MAC 地址、源 IP 地址和目的 IP 地址组合，以及源 MAC 地址和目的 MAC 地址组合等来进行分布。

两台交换机之间是否形成 EtherChannel 也可以用协议自动协商。目前有两个协商协议：PAgP 和 LACP，PAgP（端口汇聚协议 Port Aggregation Protocol）是 Cisco 私有的协议，而 LACP（链路汇聚控制协议 Link Aggregation Control Protocol）是基于 IEEE 802.3ad 的国际标

准。语法为：channel-group [num] mode [auto | on | desirable]

其中，auto:被动协商；on:不协商；desirable: 主动协商。

on 只能和 on 起 channel, 两个 auto 不能起 channel。

【问题2】(7分)

核心交换机Switch-core与网管中心交换机Switch1通过静态路由进行连接。根据需求，完成或解释 Switch-core 与 Switch1 的部分配置命令。

1. 配置核心交换机 Switch-core

```
Switch-core#config terminal
Switch-core(config)#interface gigabitEthernet 0/2
Switch-core(config-if)#description wgs-g0/1 // (5)
Switch-core(config-if)#no switchport // (6)
Switch-core(config-if)#ip address (7)
Switch-core(config-if)#no shutdown
Switch-core(config)#ip route 192.168.10.0 255.255.255.0 192.168.101.2
Switch-core(config)#exit
...
```

2. 配置网管中心交换机 Switch1

```
Switch1#config terminal
Switch1(config)#no ip domain lookup // (8)
Switch1(config)#interface gigabitEthernet 0/1
Switch1(config-if)#description core-g0/2
Switch1(config-if)#no switchport
Switch1(config-if)#ip address (9)
Switch1(config-if)#exit
Switch1(config)#vlan 10
Switch1(config-vlan)#name wgl0
Switch1(config-vlan)#exit
Switch1(config)#interface vlan 10 //创建 VLAN10
Switch1(config-if)#ip address (10)
Switch1(config-if)#exit
```

```

Switch1(config)#interface range f0/2-20
Switch1(config-if-range)#switchport mode access //设置端口模为 access 模式
Switch1(config-if-range)#switchport access (11) //设置端口所属的 VLAN
Switch1(config-if-range)#no shutdown
Switch1(config-if-range)#exit
Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1
Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1
...

```

- (5) 描述该端口或者给该端口做备注
- (6) 关闭二层交换功能，启用三层路由模式
- (7) 192.168.101.1 255.255.255.0
- (8) 关闭域名解析功能
- (9) 192.168.101.2 255.255.255.0
- (10) 192.168.10.1 255.255.255.0
- (11) VLAN 10

本问题主要考查三层交换机使用静态路由进行路由选择的配置方法。

```

(1)配置核心交换机 Switch-core
Switch-core#config terminal
Switch-core(config)#interface gigabitEthernet 0/2
//进入核心交换机三层网络接口
Switch-core(config-if)#description wgs-wg0/1
//描述该端口或者给该端口做备注
Switch-core(config-if)#no switchport //
关闭二层交换功能，启用三层路由模式
Switch-core(config-if)#ip address 192.168.101.1 255.255.255.0
//配置三层网络接口的IP地址
Switch-core(config-if)#no shutdown
//激活接口

```



```
Switch-core(config)#ip route 192.168.10.0 255.255.255.0 192.168.101.2
```

//配置核心交换机到 192.168.10.0 网段的静态路由

```
Switch-core(config)#exit
```

...

(2)配置网管中心交换机 Switch1

```
Switch1#config terminal
```

```
Switch1(config)#no ip domain lookup
```

//关闭域名解析功能

```
Switch1(config)#interface gigabitEthernet 0/1
```

//进入 gigabitEthernet 0/1 接口

```
Switch1(config-if)#description core-g0/2
```

//描述该接口

```
Switch1(config-if)#no switchport
```

//关闭二层交换功能，启用三层路由模式

```
Switch1(config-if)#ip address 192.168.101.2 255.255.255.0
```

//配置三层网络接口的 IP 地址和子网掩码

```
Switch1(config-if)#exit
```

```
Switch1(config)#vlan 10
```

```
Switch1(config-vlan)#name wg10
```

```
Switch1(config-vlan)#exit
```

```
Switch1(config)#interface vlan 10
```

//进入 VLAN10 接口

```
Switch1(config-if)#ip address 192.168.10.1 255.255.255.0
```

//配置该接口的 IP 地址和子网掩码

```
Switch1(config-if)#exit
```

```
Switch1(config)#interface range f0/2-20
```

//选择接口范围为 f0/2-20

```
Switch1(config-if-range)#switchport mode access
```

//设置端口模式为 access 模式

```
Switch1(config-if-range)#switchport access vlan 10
```

```
//设置端口所属的 VLAN

Switch1(config-if-range)#no shutdown

Switch1(config-if-range)#exit

Switch1(config)#ip route 192.168.20.0 255.255.255.0 192.168.101.1

Switch1(config)#ip route 192.168.30.0 255.255.255.0 192.168.101.1

//配置 switch1 到 192.168.20.0 及 192.168.30.0 网段的静态路由

...
```

【问题 3】（7 分）

为确保研发中心网络的稳定性，在现有条件下尽量保证带宽，要求实现核心交换机 Switch-core 与研发中心交换机 Switch4 的三层端口聚合，然后通过静态路由进行连接。根据需求，完成或解释以下配置命令。

1. 继续配置核心交换机 Switch-core

```
Switch-core#config terminal

Switch-core(config)#interface port-channel 10 // (12)

Switch-core(config-if)#no switchport

Switch-core(config-if)#ip address (13)

Switch-core(config-if)#no shutdown

Switch-core(config-if)#exit

Switch-core(config)#interface range fastEthernet0/1-4 //选择配置的物理接口

Switch-core(config-if-range)#no switchport

Switch-core(config-if-range)#no ip address //确保该物理接口没有指定的 IP 地址

Switch-core(config-if-range)#switchport //改变该端口为 2 层接口

Switch-core(config-if-range)#channel-group 10 mode on // (14)

Switch-core(config-if-range)#no shutdown

Switch-core(config-if-range)#exit

Switch-core(config)#ip route 192.168.40.0 255.255.255.0 192.168.102.2

...
```

2. 配置研发中心交换机 Switch4

```
Switch4#config terminal
```

```

Switch4(config)#interface port-channel 10

Switch4(config-if)#no switchport

Switch4(config-if)#ip address (15)

Switch4(config-if)#no shutdown

Switch4(config-if)#exit

Switch4(config)#interface range fastEthernet0/1-4 //选择配置的物理接口

Switch4(config-if-range)#no switchport

Switch4(config-if-range)#no ip address

...

Switch4(config-if-range)#no shutdown

Switch4(config-if-range)#exit

Switch4(config)# (16) //配置默认路由

Switch4(config)#vlan 40

Switch4(config-vlan)#name yf10

Switch4(config-vlan)#exit

Switch4(config)# (17) //开启该交换机的三层路由功能

Switch4(config)#interface vlan 40

Switch4(config-if)#ip address 192.168.40.1 255.255.255.0

Switch4(config-if)#exit

Switch4(config)#interface range fastEthernet0/5-20

Switch4(config-if-range)#switchport mode access

...

Switch4(config-if-range)# (18) //退回到特权模式

Switch4#

...

```

(12) 创建编号为 10 的 port-channel 接口

(13) 192.168.102.1 255.255.255.0

(14) 分配接口并指定 PAgP 模式

```
(15) 192.168.102.2    255.255.255.0  
(16) ip route 0.0.0.0.0.0.0 192.168.102.1  
(17) ip routing  
(18) end 或者 Ctrl+Z
```

本问题主要考查冗余链路汇聚的相关配置知识。

(1)继续配置核心交换机 Switch-core

```
Switch-core#config terminal  
  
Switch-core(config)#interface port-channel 10  
  
//创建编号为 10 的 port-channel 接口  
  
Switch-core(config-if)#no switchport  
  
//关闭二层交换功能，启用三层路由模式  
  
Switch-core(config-if)#ip address 192.168.102.1 255.255.255.0  
  
//为该接口分配 IP 地址和子网掩码  
  
Switch-core(config-if)#no shutdown  
  
Switch-core(config-if)#exit  
  
Switch-core(config)#interface range fastEthernet0/1-4  
  
//选择配置的物理接口  
  
Switch-core(config-if-range)#no switchport  
  
//关闭二层交换功能，启用三层路由模式  
  
Switch-core(config-if-range)#no ip address  
  
//确保该物理接口没有指定的 IP 地址  
  
Switch-core(config-if-range)#switchport  
  
//改变该端口为 2 层接口  
  
Switch-core(config-if-range)#channel-group 10 mode on  
  
//分配接口并指定为 PAgP 模式  
  
Switch-core(config-if-range)#no shutdown  
  
Switch-core(config-if-range)#exit  
  
Switch-core(config)#ip route 192.168.40.0 255.255.255.0 192.168.102.2  
  
//配置核心交换机到 192.168.40.0 网段的静态路由
```

...

(2) 配置研发中心交换机 Switch4

```
Switch4#config terminal
Switch4(config)#interface port-channel 10
//创建编号为 10 的 port-channel 接口
Switch4(config-if)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch4(config-if)#ip address 192.168.102.2 255.255.255.0
//为该接口分配 IP 地址和子网掩码
Switch4(config-if)#no shutdown
Switch4(config-if)#exit
Switch4(config)#interface range fastEthernet0/1-4
//选择配置的物理接口范围为 f0/1-4
Switch4(config-if-range)#no switchport
//关闭二层交换功能，启用三层路由模式
Switch4(config-if-range)#no ip address
//确保该物理接口没有指定的 ip 地址
...
Switch4(config-if-range)#no shutdown
Switch4(config-if-range)#exit
Switch4(config)# ip route 0.0.0.0 0.0 . 0 . 0 192.168.102.1
//配置默认路由
Switch4(config)#vlan 40
Switch4(config-vlan)#name yf10
Switch4(config-vlan)#exit
Switch4(config)# ip routing
//开启该交换机的三层路由功能
Switch4(config)#interface vlan 40
//进入 VLAN40 接口
Switch4(config-if)#ip address 192.168.40.1 255.255.255.0
```

```
//配置该接口的 IP 地址和子网掩码

Switch4(config-if)#exit

Switch4(config)#interface range fastEthernet0/5-20

//选择接口范围为 f0/5-20

Switch4(config-if-rang)#switchport mode access

//设置端口模式为 access 模式

...

Switch4 (config-if-range) #end 或 Ctrl+Z

//在该接口模式下使用 end 或 Ctrl+Z 可直接退回到特权模式

Switch4#

...
```

【问题 4】（2 分）

为了保障局域网用户的网络安全，防范欺骗攻击，以生产部交换机 Switch2 为例，配置 DHCP 侦听。根据需求完成或解释 Switch2 的部分配置命令。

```
Switch2#config terminal

Switch2(config)#ip dhcp snooping //（19）

Switch2(config)#ip dhcp snooping vlan 20

Switch2(config)#interface gigabitEthernet1/1

Switch2(config-if)#ip dhcp snooping trust //（20）

Switch2(config-if)#exit

...
```

（19）启用 DHCP 探测

（20）g1/1 端口为信任端口

问题主要考查交换机利用 DHCP 探测防范欺骗攻击的相关配置知识。

```
Switch2#config terminal

Switch2(config)#ip dhcp snooping

//启用 DHCP 探测
```

```
Switch2(config)#ip dhcp snooping vlan 20
//指定要实现 DHCP 探测的 VLAN

Switch2(config)#interface gigabitEthernet1/1
Switch2(config-if)#ip dhcp snooping trust
//配置端口信任， g1/1 端口为信任端口

Switch2(config-if)#exit
...
```