**1.基础准备**

**1.1 题库**

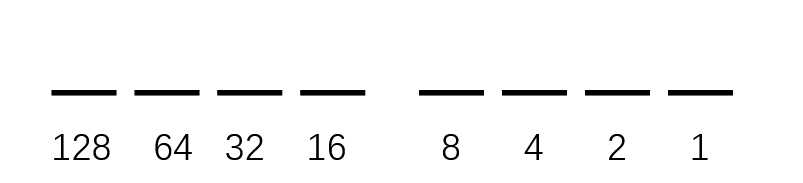
买一本三级网络技术题库或者是题库软件（20 元左右），不需要买更多，总之有成套的题可以做就行。真题目前大概有二十套左右。

**1.2 二进制转换**

应该学过

网络技术用到的一般是八位二进制数。也就是 0 ~ 255，即 0000 0000 ~ 1111 1111（每四位空一格便于观察）

我做题前在草稿纸上先这样画



这样，比如说我看见 1001 1000 这个数，就知道这是 128+16+8 对应的数。

反过来，十进制转换二进制也可以利用这个简图。还有一些规律，自己做题中摸索吧，你可能会找到更好的方法。

下面几组记忆一下，做题时会比较方便（不要畏难，做题见多了就记住了）

|  |  |
| --- | --- |
| 二进制 | 十进制 |
| 1000 0000 | 128 |
| 1100 0000 | 192 |
| 1110 0000 | 224 |
| 1111 0000 | 240 |
| 1111 1111 | 255 |

**1.3 基础概念**

如果是学过计算机网络相关知识的同学可以不看，下面是非专业的不标准的可能还有错的描述，仅仅是为了完全没有基础的同学有个粗略了解。

计算机网络是一些电脑相互链接组成的，这些电脑叫做**主机**，可能相距很远，也可能是一间屋子里的。

就像正常情况下两个人要用同一种语言交流一样。主机之间的联系也要按照相同的标准才行，这些标准叫做**协议**。因为主机之间的联系是一件复杂的事。所以有多种协议解决不同方面的问题，比如 TCP、BGP、DHCP 等等。

相距太远的主机之间不能直接联系，就需要一些设备，比如路由器、交换机等等，你只知道他们都是为了主机联系的中间转发设备就行。

还需要地址，因为没有地址就不知道主机在哪，这个标识主机的就是 IP 地址。

IP 地址是类似这样的：10000000.1110000.01000000.10110001，一共 **32** 位，为了人看起来方便就写成 128.224.64.177 这种点分十进制的形式。

还有一种叫做 MAC 地址，是标识硬件设备的地址。

主机还可以广播给整个网络，广播地址是 IP地址 32 位全置 1 的地址，即 255.255.255.255。

当你访问一个网站，你的电脑先将网址发送给 DNS 服务器（域名解析服务器），这个服务器能将你写的网址域名变成 IP 地址，这样你的电脑就知道想要访问的网页放在哪了。

上面这些并不能让你真正理解计算机网络（其实我也不是很清楚），主要是让你在见到陌生名词的时候别害怕，有些名词不理解也不会影响做题。

**1.4 备考建议**

这就是个人的方法了，也不一定适合你。

【1】首先对着一套三级题和答案看一遍，每道题都看答案解析是怎么说的。看答案不必弄懂（当然你要真的全弄懂也很厉害），知道怎么选出来就行，不明白跳过也行。同时也找找看看我笔记里写没写这道题的知识点。

这一遍是比较简略的，对题目有个简单的印象就够了。但这遍也是比较困难的，因为几乎都是陌生的东西。

【2】接下来，同时做两三套试题甚至更多套。按着笔记里的知识点做，看到哪个知识点就到这些套题里找，对照着做题来掌握这个知识点。如果笔记里没有提到或者没写详细的就看答案怎么说，实在不明白的还可以跳过。

这个阶段是需要比较认真的看了，我这个阶段是在写笔记中度过的。经过这个阶段你就能明白哪些知识点考察比较固定，一些题的固定做法是什么，对考试有比较完全的认识了。

【3】接下来，就把剩下的套题都做了，反正一共就二十套左右。怎么做都行，按套或者按题型什么的自己安排，反正做一遍。如果没时间了，至少把选择题做一遍。

这一遍就是完善熟练的阶段，还可能有一些我笔记里没写的知识点你也会了。

【补充】有的同学还是感觉难，那就先把第一道大题和最后一道大题的两个填表都仔细弄会了。这两个表就 20 分到手了。接下来学习可能会感觉踏实一点。

**2.选择题（40 道 40 分）**

根据做题方法不同划为三类

1. 第一类：几乎每套题都考，掌握简单做法即可选出正确答案
2. 第二类：每套题里有 5 道左右，看上去非常复杂的大段配置代码
3. 第三类：从四个选项里选出一项正确或错误的，其中部分知识点是常考的，比较零散

**2.1 第一类选择题**

**2.1.1 问传输速度**

OC-3 对应 155.52 Mbps

OC-12 对应 622.08 Mbps

（显然，这是一道送分题）

**2.1.2 求交换机带宽**

通常是求总带宽

例：某交换机有 12 个 10/100 Mbps 电端口和 2 个 1000 Mbps 光端口，所有端口都在全双工状态下，那么总带宽为（ ）

解：忽略 10/100 中的 10，当成 100 Mbps 就好。12 \* 100 + 2 \* 1000 = 3200，又因为**全双工**所以乘以 2 得 6400 Mbps ,即 6.4 Gbps

有时候求上联端口带宽

例：某交换机有 16个100/1000 Mbps 全双工下联端口，那么上联端口带宽至少为（ ）

解：16 \* 1000 \* 2 = 32000 Mbps = 32 Gbps，**上联一般是下联的 1/20**，所以至少为 32 除以 20 得 1.6 Gbps

**2.1.3 系统可用性与停机时间**

|  |  |
| --- | --- |
| 可用性 | 停机时间 |
| 99.9% | ≤8.8小时 |
| 99.99% | ≤53分钟 |
| 99.999% | ≤5分钟 |

也是送分题，但要记准确。比如 53 分钟，有时候会问 55 分钟的情况，要是记成 50 或者大约 1 小时就没法做了。

**2.1.4 写地址块的子网掩码**

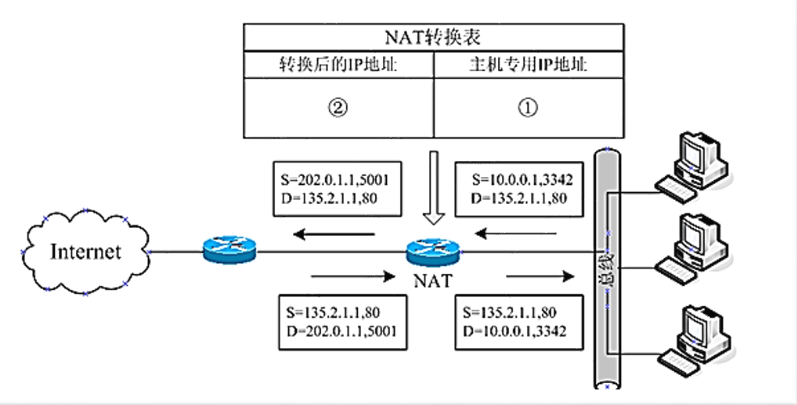
例：IP 地址块 59.67.159.125/11 的子网掩码可写为（ ）

解：不用看 IP 地址，只看 **/11** 就够了。

11 代表子网掩码的前 11 位都是 1 ，所以可以写出子网掩码 11111111.11100000.00000000.00000000 转换为十进制即是 255.224.0.0

做题熟练后其实不用写上面那堆 1 和 0 就能选出正确答案。

**2.1.5 网络地址转换 NAT**



会给你一个这样的图，问你 ① ② 是什么

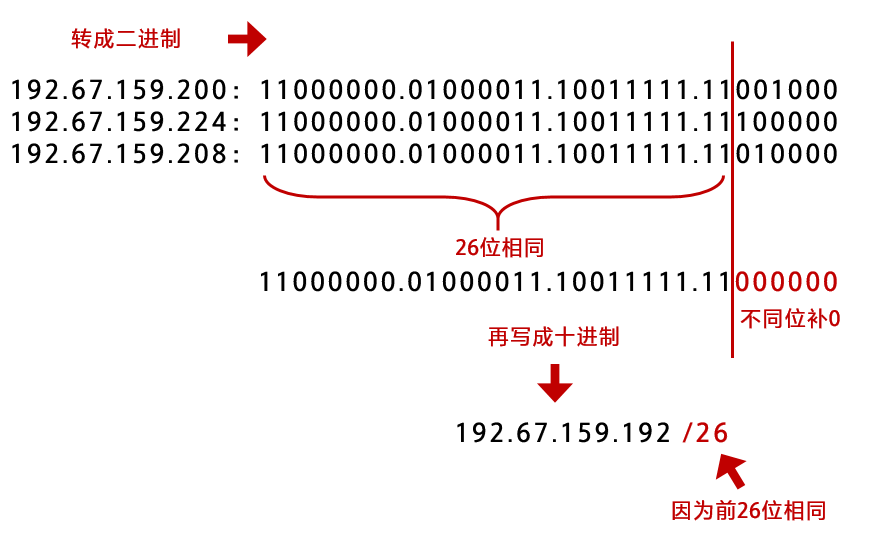
只需要知道②和紧挨着它的 S 数字相同，所以②应该是 202.0.1.1,5001 ;同理，①是 10.0.0.1,3342。

还有时候会问某个小方框里的 S,D 分别是什么，看上面的图你会发现，上面两个方框和下面两个方框里的数字是对称的，做题时对称一下就写出答案了。

**2.1.6 IP 地址块聚合**

**第一种：问聚合后的地址块**

下面演示三个地址的聚合



步骤为：转成二进制；对齐找前多少位是相同的；转回十进制写答案。

这样就得出聚合后的地址为：192.67.159.192/26

Tips：转换二进制时，因为前三段十进制本来就一样，所以可以只转换最后一段；

不要一个一个数有多少位相同的，因为前三段相同就知道有 3 \* 8 = 24 位，再加上 2 就是 26。

**第二种：问聚合后可用 IP 数**

**下面两种情况的做法由网友 Yes 补充，十分感谢**，之前我写的不当方法已删除。

【第一种情况】如未来教育上机考试第一套试题第10题：

“ IP 地址块 202.113.79.128/27、202.113.79.160/27 和 202.113.79.192/27 经过聚合后可用的地址数为\_\_\_”

因为格式都是 xxx.xxx.xxx.xxx/27，本题中“/”后边的数字都是相同的。

所以遇到这种题，先把前两个 IP 聚合求出可用地址数，然后单独算出第三个 IP 地址可用地址数，两个地址数相加即正确答案。

【第二种情况】如未来教育上机考试第三套试题第10题：

“ IP 地址块 202.113.79.0/27、202.113.79.32/27、202.113.79.64/26 经过聚合后可用的地址数为\_\_\_”

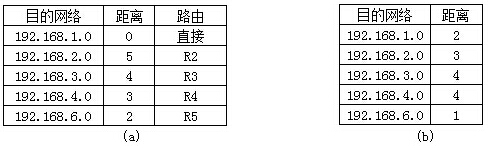
本题中“/”后边的数字前两个是相同的，第三个与前两个不同。

所以遇到这种题，直接将三个 IP 聚合得到地址块，然后求出三个 IP 的可用地址数。

**2.1.7 路由表距离更新**

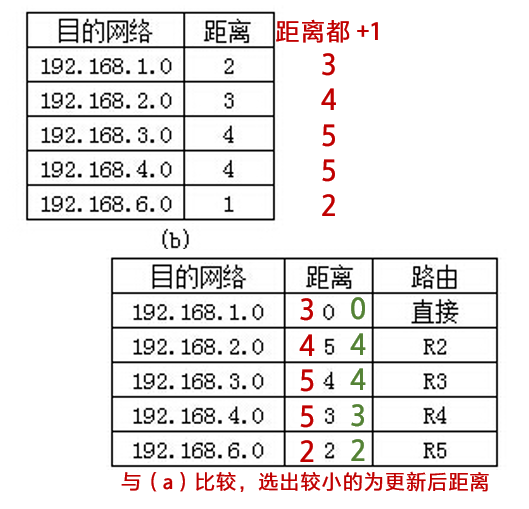
例：R1,R2 是一个系统中采用RIP路由协议的两个相邻路由器，R1 的路由表如（a）所示，

R1 收到 R2 发送的报文（b）后，R1 更新后的距离值从上到下依次是（ ）



解：做法如下

步骤为：b距离+1；



与a距离比较；更新为距离最小的。则更新后的距离值从上到下依次是 0、4、4、3、2

还经常这样考——给出更新后距离值和（a）中的距离，求（b）报文距离的可能值。

规则不变，上面的做法反过去求就行。

**2.1.8 IPv6 地址简化表示**

例：某地址 FF23:0:0:0:0510:0:0:9C5B，

可以简化为 FF23::0510:0:0:9C5B，双冒号替代连续出现的 0 位段，

不能简化为 FF23::0510::9C5B，因为双冒号只能使用一次，

可以简化为 FF23::510:0:0:9C5B，因为 0510 就是 510 ，

不能简化为 FF23::051:0:0:9C5B，因为 0510 不是 51。

例：下列 IPv6 地址表示中错误的是（ ）

A) ::10F:BC:0:0:03DA

B) FE::0:45:03/48

C) FE31:0:BC:3E:0:050D:BC::03DA

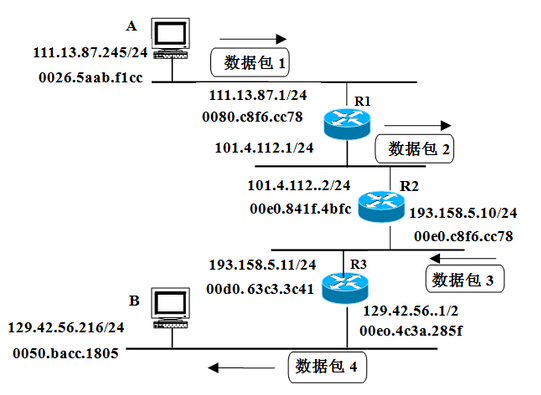
D) FF34:42:BC::3E:50F:21:03D

解：IPv6 地址是 128 位划分为 8 段的地址，而 C 项不算双冒号那段已经有了 8 段，双冒号又至少压缩一个 0 位段，所以超了 8 段，是错误的。

B 中的 /48 做题时可以忽略，写不写没关系。做这种题先看最长的那项有没有超过 8 段。

**2.1.9 数据包**

例：下图是 A 发送的数据包通过路由器转发到 B 的过程示意图，求数据包 3 中的**目的IP地址**和**目的MAC地址**



解：无论哪个数据包，目的 IP 地址就是 B 的 IP 地址，所以数据包 3 的目的 IP 为 129.42.56.216；

而目的 MAC 地址就是下一个路由器的 MAC 地址，数据包 3 的下一个路由器是 R3，所以数据包 3 的目的 MAC 地址是 00d0.63c3.3c41。

**2.1.10 三种备份**

备份速度从快到慢：增量备份、差异备份、完全备份（备份越详细越慢）

恢复速度从快到慢：完全备份、差异备份、增量备份（和上面顺序相反，也好理解，备份时详细的恢复快）

空间占用从多到少：完全备份、差异备份、增量备份（备份越详细占用空间越多）

题目通常问你其中某一种的顺序。

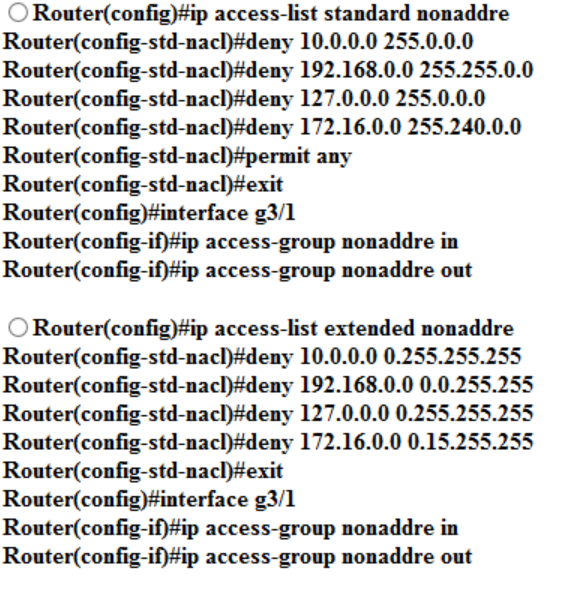
**2.2 第二类选择题**

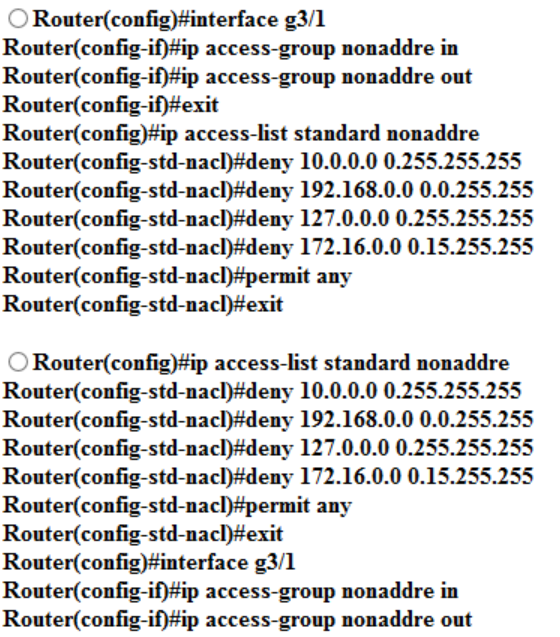
这部分将进一步体现本指南的优越性



我们先来看一道“第二类选择题”的四个选项，不需要看题。

-从这开始



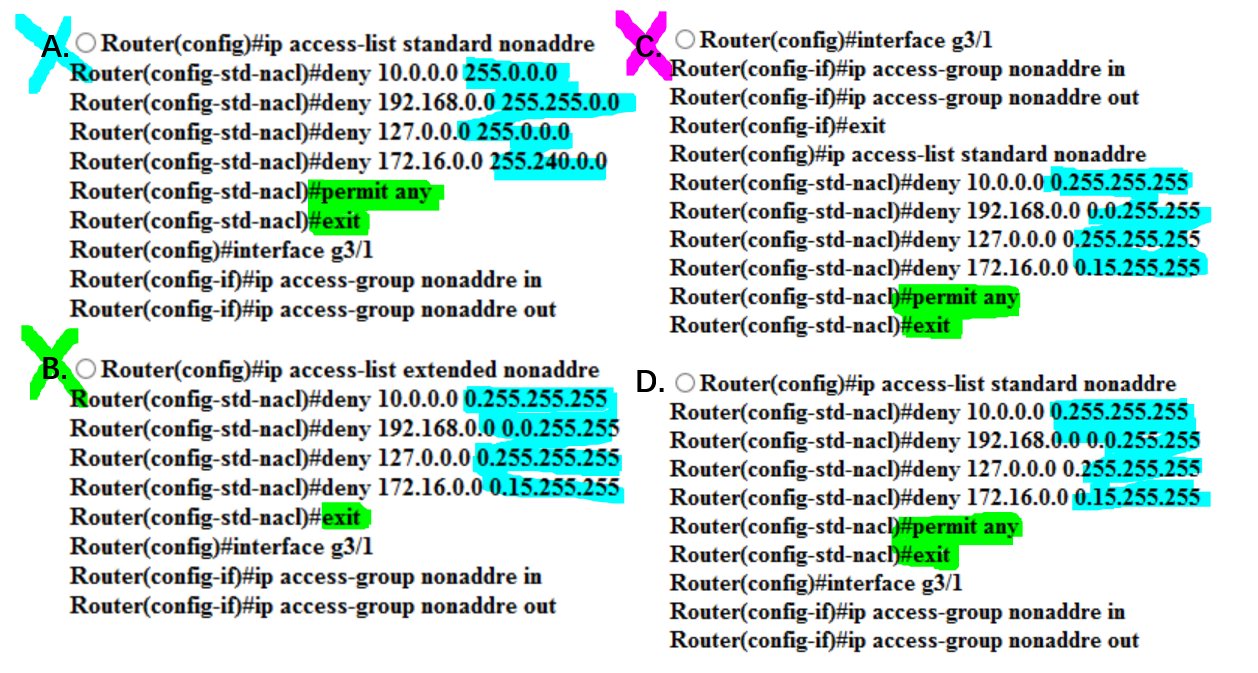


-到这结束

看起来异常复杂，但这是在我完全不懂知识点的情况下就能选对的题。

**下面要讲的是技巧方法，不是知识点，适用于这类题**

首先，你需要来回观察这四个选项，找出他们的不同点。可能是两句颠倒的代码，可能是一个单词一个数，也可能是其他的。



这是我把他们不同的地方做了荧光标记

首先一眼看上去，C 项的大段数字位置和其他三项不一样，所以排除 C；

然后，看蓝色的数字，只有 A 项和其他三项不一样，所以排除 A；

最后，看绿色的地方，只有 B 项少了一句，所以排除 B；

选 D。

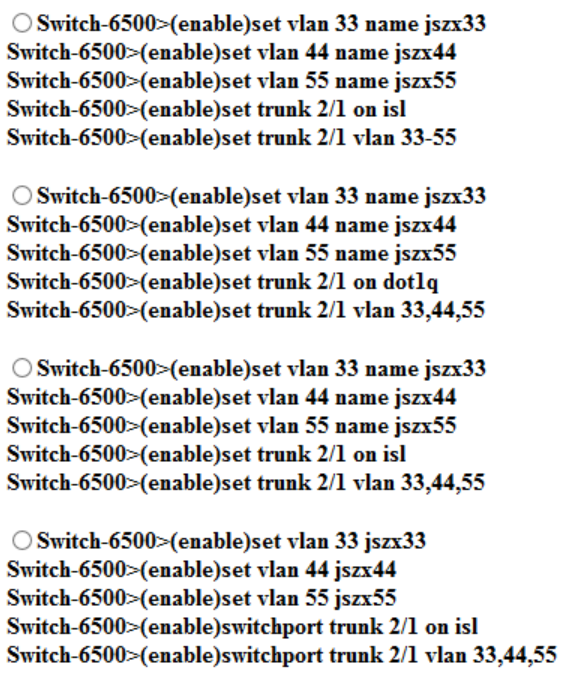
悟性比较高的同学肯定已经明白了，为了大家更好的体会，再换一道题演示：

不先写选项了，直接展示标记后的



方法一样，找出不同点，然后“少数服从多数”，最后选 C。

下面一道题自己练习一下



答案是C。

说出来你可能不信，这种方法可以解决80%以上的“第二类选择题”，

有的题可能没办法排除掉三个选项，这时候就要结合一下题目内容推断来做或者蒙。

**2.3 第三类选择题**

下面列举的是高频考点，需要记忆，但不要死记。一开始可能感觉很陌生很难，做题碰见得多了就熟悉了能迅速选出答案。

**2.3.1 弹性分组环 RPR**

1. 每一个节点都执行**SRP**公平算法
2. 与 FDDI 一样使用**双环结构**
3. 传统的 FDDI 环，当源结点向目的节点成功发送一个数据帧之后，这个数据帧由**源结点**从环中回收
4. 而 RPR 环，当源结点向目的节点成功发送一个数据帧之后，这个数据帧由**目的结点**从环中回收
5. RPR 采用自愈环设计思路，能在 **50ms** 时间内隔离故障结点和光纤段
6. 两个 RPR 结点间的裸光纤最大长度可达 **100公里**
7. RPR 的外环（顺时针）和内环（逆时针）**都可以**用于传输分组和控制分组

**2.3.2 无线接入技术**

1. 主要有 WLAN、WiMAX、WiFi、WMAN 和 Ad hoc ( WiFi 肯定知道，记住无线技术一般是W开头的，但有个特殊的A开头)
2. APON 不是无限传输技术，这个经常是迷惑项

**2.3.3 广域网 QoS**

考的时候通常只写英文缩写，下面写上中文名是为了方便你记忆（其他的地方也应该养成粗略推测英文缩写的习惯）

1. 主要的技术有 资源预留（**RSVP**）、区分服务（**DiffServ**）、多协议标记交换（**MPLS**）

**2.3.4 接入技术特征**

1. ASDL 使用一对铜双绞线，具有**非对称**技术特性，上行速率 64 kbps~640 kbps，下行速率 500 kbps~7 Mbps
2. 采用 ADSL 技术可以通过 PSTN 接入 Internet
3. Cable Modom（电缆调制解调器）利用**频分复用**的方法将信道分为上行信道和下行信道，把用户计算机与有线电视同轴电缆连接起来
4. 光纤传输距离可达 100km 以上（这个知道光纤很远就行了）

**2.3.5 服务器技术**

1. 热插拔功能允许用户在不切断电源的情况下更换硬盘、板卡等（不能更换主板卡）
2. 集群技术中，如果一台主机出现故障，不会影响正常服务，但会影响系统性能
3. 磁盘性能表现在储存容量和 I/O 速度（I/O=input/output 即输入/输出，学过计算机应该知道）
4. 服务器总体性能取决于 CPU 数量、CPU 主频、系统内存、网络速度

**2.3.6 综合布线**

1. 双绞线可以避免电磁干扰
2. **嵌入式插座**用来连接双绞线
3. **多介质插座**用来连接铜缆和光纤，满足用户“光纤到桌面”的需求
4. 建筑群子系统可以是多种布线方式的任意组合，**地下管道布线**是最理想的方式
5. STP 比 UTP 贵、复杂、抗干扰能力强、辐射小
6. 水平布线子系统电缆长度在 90 m 以内
7. 干线线缆铺设经常采用点对点结合和分支结合两种方式

**2.3.7 BGP 协议**

1. BGP 是**边界网关协议**，而不是内部网关协议（所以遇到问某两个自治系统之间使用什么协议，就选 BGP）
2. BGP 交换路由信息的节点数不小于自治系统数
3. 一个 BGP 发言人使用 **TCP**（不是UDP）与其他自治系统的 BGP 发言人交换信息
4. BGP 采用路由向量协议，而 RIP 采用距离向量协议
5. BGP 发言人通过 update 而不是 noticfication 分组通知相邻系统
6. open 分组用来与相邻的另一个 BGP 发言人建立关系，两个 BGP 发言人需要周期性地交换 keepalive 分组来确认双方的相邻关系

**2.3.8 RIP 协议**

1. RIP 是内部网关协议中使用最广泛的一种协议，它是一种分布式、基于距离向量的路由选择协议，要求路由器周期性地向外发送路由刷新报文
2. 路由刷新报文主要内容是由若干个（V，D）组成的表。V 标识该路由器可以到达的目标网络（或目的主机）；D 指出该路由器到达目标网络（或目标主机）的距离。距离D对应该路由器上的跳数。其他路由器在接收到某个路由器的（V，D）报文后，按照***最短路径原则***对各自的路由表进行刷新
3. 使用 RIP v1 路由协议在配置网络地址时***无须给定子网掩码***

**2.3.9 OSPF 协议**

1. OSPF 是内部网关协议的一种，每个区域有一个 32 位的标识符，区域内路由器不超过 200 个
2. 区域内每个路由器包含**本区域的完整网络拓扑**，而不是全网的情况（拓扑的意思是链接形式和位置关系之类的）
3. 链路状态“度量”主要指费用、距离、延时、带宽等
4. OSPF 采用**洪泛法**交换链路状态信息

**2.3.10 集线器**

1. 工作在物理层，连接到一个集线器的所有结点共享一个冲突域
2. 集线器不是基于 MAC 地址完成数据转发，而是用广播的方法
3. 在链路中串接一个集线器可以监听数据包
4. 每次只有一个结点能够发送数据，而其他的结点都处于接收数据的状态。这些结点执行CSMA/CD介质访问控制方法

**2.3.11 交换机**

1. 是一种工作在数据链路层的网络设备，基本功能是维护一个表示 MAC 地址和交换机端口对应关系的交换表
2. 在源端口与目的端口间建立虚链接
3. 具有三种交换模式：1.快速转发直通式，接收到前 14 个字节就转发数据；2.碎片丢弃式，缓存前 64 个字节；3.储存转发式，转发之前读取整个帧
4. 三层交换机是具有部分路由器功能的交换机，用于加快大型局域网内部的数据交换

**2.3.12 路由器**

1. 丢包率是衡量路由器超负荷工作时的性能指标之一
2. 背板能力决定路由器吞吐量
3. 传统路由器一般采用共享背板的结构，高性能路由器一般采用交换式的结构
4. 突发处理能力**不是**以最小帧间隔值来衡量的
5. 语音视频业务对延时抖动要求较高
6. 高端路由器应达到：无故障连续工作时间大于 10 万小时；故障恢复时间小于 30 分钟；切换时间小于 50 毫秒

**2.3.13 IEEE 802.11**

1. IEEE 802.11 最初定义的三个物理层包括了两个扩频技术和一个红外传播规范，无线频道定义在 2.4GHz ISM频段，传输速度 1~2 Mbps
2. **802.11b** 最大容量 33 Mbps，将传输速率提高到 **11 Mbps**，**802.11a**和**802.11g** 将传输速率提高到 **54 Mbps**
3. IEEE 802.11d 是当前最流行的 STP（生成树协议）标准
4. IEEE 802.11b 标准使用的是开放的 2.4GHZ 频段，无须申请就可以直接使用

**2.3.14 蓝牙**

1. 同步信道速率 64 kbps，跳频速率为 1600 次/s
2. 工作在 2.402 ~ 2.480 GHz 的 ISM 频段
3. 非对称的异步信道速率为 723.2 kbps / 57.6 kbps
4. 对称的异步信道速率为 433.9 kbps
5. 发射功率为100mw时，最大传输距离为100米

**2.3.15 Serv-U FTP 服务器**

1. 使用动态 IP 地址时，服务器 IP 地址应配置为空，而不是 0.0.0.0。（为空代表全部 IP 地址）
2. 每个 Serv-U FTP 服务器中的虚拟服务器由 **IP 地址和端口号**唯一识别，而不是依靠 IP 地址
3. 向服务器中添加“anonymous”，系统自动判定为匿名。而不是创建新域时自动添加一个“anonymous”匿名
4. 服务器最大用户数是指服务器允许同时在线的最大用户数量
5. 用户上传下载选项要求 FTP 客户端在下载信息的同时也要上传文件

**2.3.16 DNS 服务器**

1. 允许客户机在发生更改时动态更新其资源记录
2. DNS 服务器中的根服务器被自动加入到系统中，**不需**管理员手工配置
3. 转发器是网络上的 DNS 服务器（不是路由器），用于外域名的 DNS 查询
4. 使用 nslookup 命令可以测试正向和反向查找区域
5. 主机记录的生存时间指该记录被客户端查询到，放在缓存中的持续时间

**2.3.17 DHCP 服务器**

1. 负责多个网段 IP 地址分配时需配置**多个作用域**
2. 添加保留时需在 DHCP 客户机上获得其 MAC 地址信息（**添加排除时不需**从客户端获得 MAC 地址）
3. 不添加排除和保留时，服务器可将地址池内的 IP 地址动态指派给 DHCP 客户机
4. 地址池是作用域应用排除范围之后剩余的 IP 地址
5. 保留是指确保 DHCP 客户端永远可以得到同一 IP 地址，客户端**可以释放**该租约
6. 收到非中继转发的“DHCP发现”消息时,选择收到该消息的子网所处的网段分配 IP 地址

**2.3.18 WWW 服务器**

1. Web 站点可以配置**静态**和**动态** IP 地址
2. 访问 Web 站点时可以使用站点的域名或站点的 IP 地址
3. 建立 Web 站点时必须为该站点指定一个主目录好，也可以是虚拟的子目录
4. Web 站点的性能选项包括影响带宽使用的属性和客户端 Web 连接的数量
5. 在 Web 站点的主目录选项卡中，可配置主目录的读取和写入等权限

**2.3.19 Wmail 邮件服务器**

1. Winmail 用户**不可以**使用 Outlook 自行注册新邮箱
2. Winmail 快速设置向导中创建新用户时，输入新建用户的信息，包括用户名、域名及用户密码（不是系统邮箱的密码）
3. 建立路由时，需在 DNS 服务器中建立该邮件服务器主机记录和邮件交换器记录
4. 邮件系统工作过程：1.用户在客户端创建新邮件；2.客户端软件使用 SMTP 协议将邮件发到**发件方的邮件服务器**；3.发件方邮件服务器使用 SMTP 协议将邮件发到**收件方的邮件服务器**；4.接收方邮件服务器将收到邮件储存待处理；5.接收方客户端软件使用 POP3 或 IMAP4 协议从邮件服务器读取邮件
5. 邮件交换器记录的配置只能在服务器上，不能通过浏览器配置
6. Winmail 支持基于 Web 方式的访问和管理，管理工具包括系统设置、域名设置等
7. 发送邮件时通常采用 SMTP 协议，接收邮件时通常采用 POP3 或者 IMAP 协议。Winmail 用户使用浏览器查看邮件会使用到 HTTP 协议

**2.3.20 PIX 防火墙**

1. **监视模式**中，可以更新操作系统映像和口令恢复
2. 防火墙开机自检后处于非特权模式，输入“enable”进入特权模式

**2.3.21 可信计算机评估准则**

1. 没有保护就是 D类，不能用于多用户环境下重要信息处理
2. 提到用户**自主保护**就是 C类

**2.3.22 入侵防护系统**

1. HIPS 基于主机的入侵防护系统，安装在受保护的主机系统中
2. NIPS 基于网络的入侵防护系统，布置在网络出口
3. AIPS 基于应用的入侵防护系统，部署于应用服务器前端

（他们的首字母 H、N、A 即 Host、Net、Application）

**2.3.23 网络攻击**

1. DDos 攻击：利用已经攻占的多个系统向目标攻击，被害设备面对大量请求无法正常处理而拒绝服务
2. SYN Flooding 攻击：利用 TCP 三次握手过程，使受害主机处于会话请求之中，直至连接超时停止响应
3. SQL 注入攻击：属于利用系统漏洞，防火墙（基于网络的防护系统）无法阻断
4. Land攻击：向某个设备发送数据包，并将数据包的源 IP 地址和目的地址都设置成攻击目标的地址
5. 基于网络的防护系统也无法阻断 Cookie篡改 和 DNS欺骗
6. Tear doop 、Smurf 攻击可以被路由器阻止

**2.3.24 无线局域网设备**

1. 无线接入点（AP）：集合无线或者有线终端（类似于集线器和交换机），负责频段管理和漫游工作（SSID 是客户端设备用来访问接入点的唯一标识）
2. 无线路由器：具有无线路由功能和 NAT 功能的 AP ，可用来建立小的无线局域网。
3. 无线网桥：用于连接几个不同的网段，实现较远距离的无线通信（网桥最重要的维护工作是构建和维护 MAC 地址表）
4. 无线网卡：实现点对点通信，安装于各终端节点

**2.3.25 VLAN**

1. VLAN name 用 1~32 个字符表示，它可以是字母和数字。不给定名字的 VLAN 系统自动按缺省的 VLAN 名（VLAN00xxx）
2. VLAN ID的取值范围是 1~4094。其中无法执行“no vlan 1”命令

**2.3.26 Cisco 路由器上的存储器**

1. Flash 主要用于存储当前使用的操作系统映像文件和微代码
2. NVRAM 主要存储启动配置文件或备份配置文件
3. RAM 主要存储路由表、快速交换缓存、ARP 缓存、数据分组缓冲区和缓冲队列、运行配置文件等
4. ROM 主要用来永久保存路由器的开机诊断程序、引导程序和操作系统软件

**2.3.27 防火墙对应端口的连接方案**

pix525 在缺省情况下

1. ethernet0 被命名为外部接口 outside，安全级别是 0
2. ethernet1 被命名为内部接口 inside，安全级别是 100
3. ethernet2 被命名为中间接口 dmz，安装级别是 50

**2.3.28 STP 生成树结构**

1. 无论是根的确定，还是树状结构的生成，主要依靠 BPDU 提供的信息
2. Bridge ID 由两个字节的优先级值和 6 个字节的交换机 MAC 地址组成，优先级取值范围是0~61440，增值量是4096，优先值越小，优先级越高
3. MAC 地址最小的为根网桥
4. BPDU 数据包有两种类型，配置 BPDU 不超过 35 个字节，拓扑变化通知 BPDU 不超过 4 个字节

**2.3.29 Catelyst 配置命令**

1. Catelyst3548 设置时间的格式是：clock set 小时:分钟:秒 日 月 年
2. Catelyst6500 设置时间的格式是：set time 星期 月/日/年 小时 分钟 秒

**2.3.30 其他**

有一些知识点因为考频不是很高或者比较复杂，就不写了，自己做题时积累或者放弃。

在遇到陌生题目时，试着结合常识思考推断。

比如说，某网络计划有三台计算机，但只有一个 VLAN 端口，需要的设备是（）

这里需要的其实就是路由器，联想宿舍上网的情况

**3.大题（前四道每道10分，最后一道20分）**

**3.1 第一道 填地址表**

例：

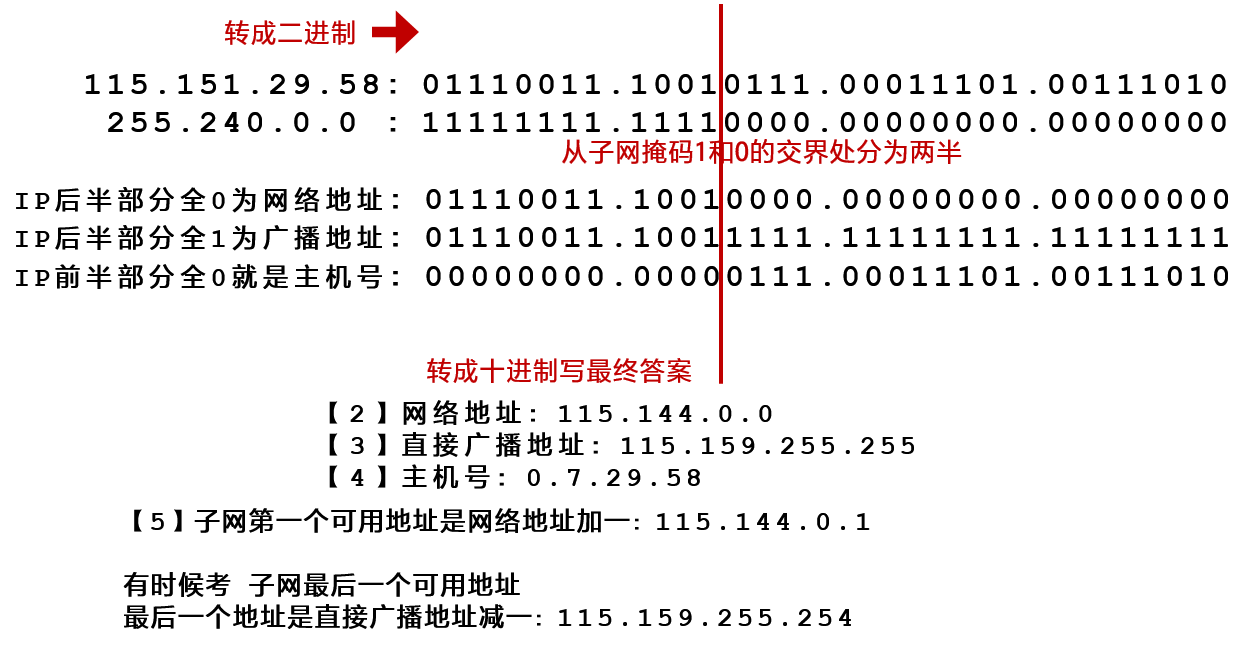
|  |  |
| --- | --- |
| IP 地址 | 115.151.29.58 |
| 子网掩码 | 255.240.0.0 |
| 地址类别 | 【1】 |
| 网络地址 | 【2】 |
| 直接广播地址 | 【3】 |
| 主机号 | 【4】 |
| 子网内第一个可用 IP 地址 | 【5】 |

解：

|  |  |
| --- | --- |
| IP 地址类别 | IP 首段范围 |
| A类 | 1~127 |
| B类 | 128~191 |
| C类 | 192~223 |

则【1】填：A类

对 IP地址和子网掩码做如下处理：

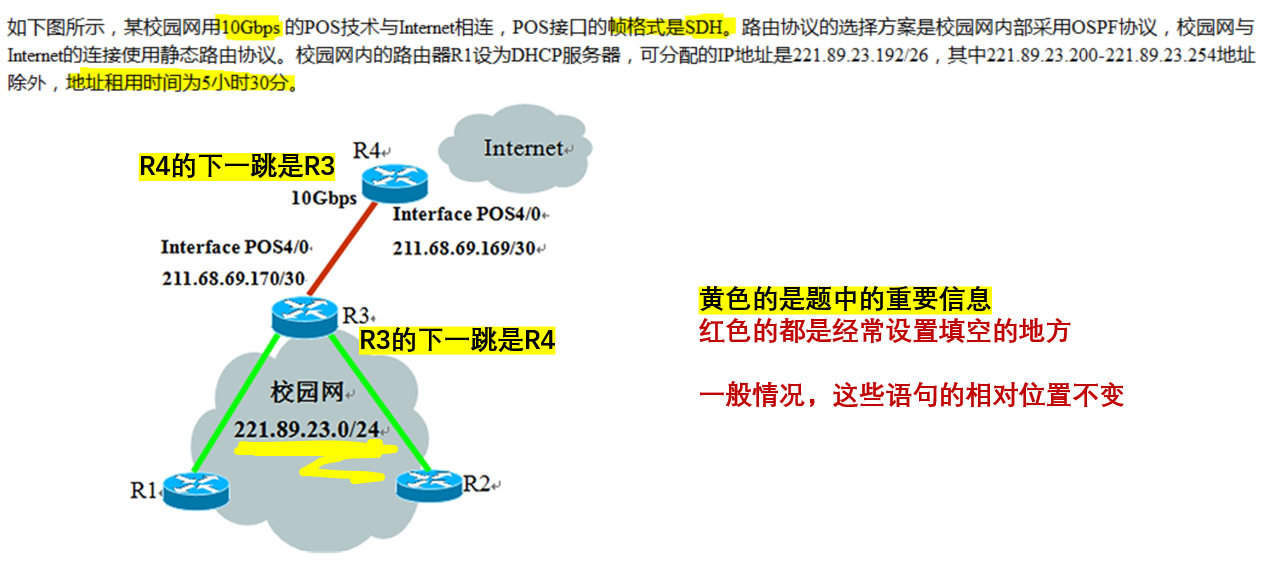


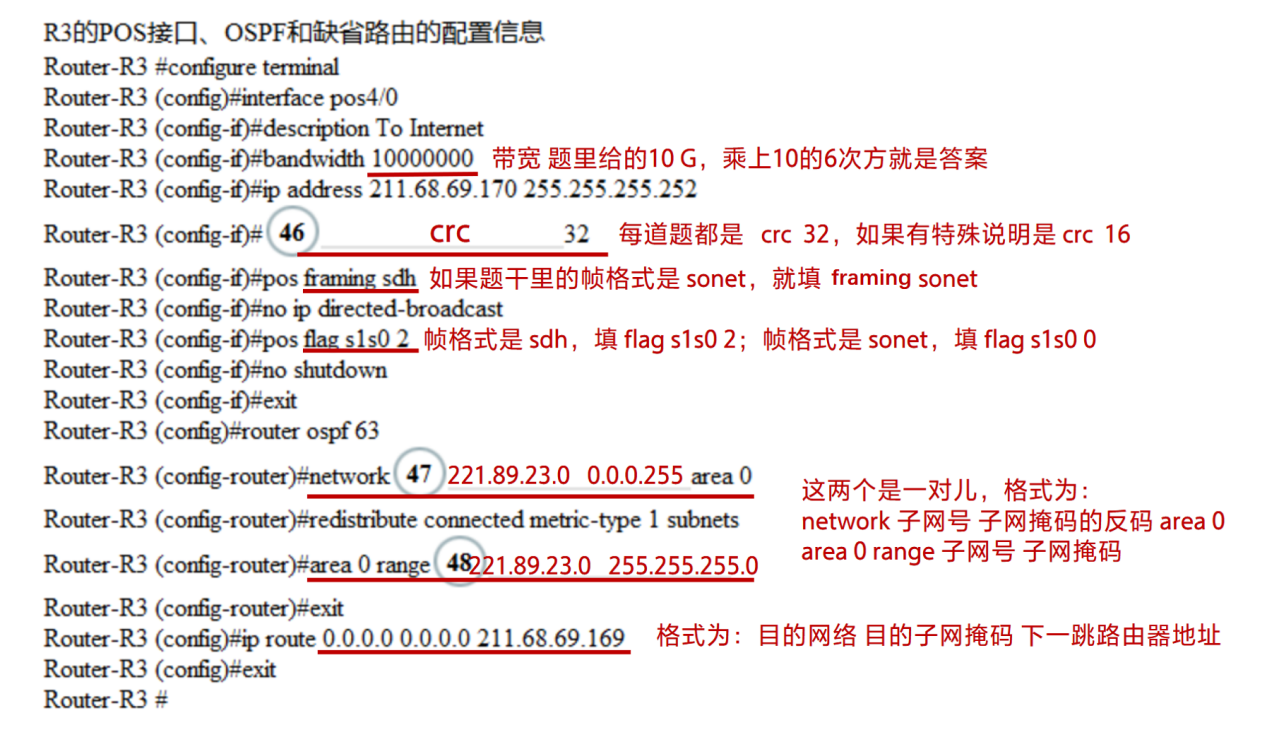
熟练以后其实没有看起来这么麻烦，做两道就会了。少数情况会给出表格的后两项，让你补充前五项，原理其实是一样的，倒推一下。

这道题是大题里面考点最稳定的一道，必须掌握。

**3.2 第二道 配置路由器**

例：



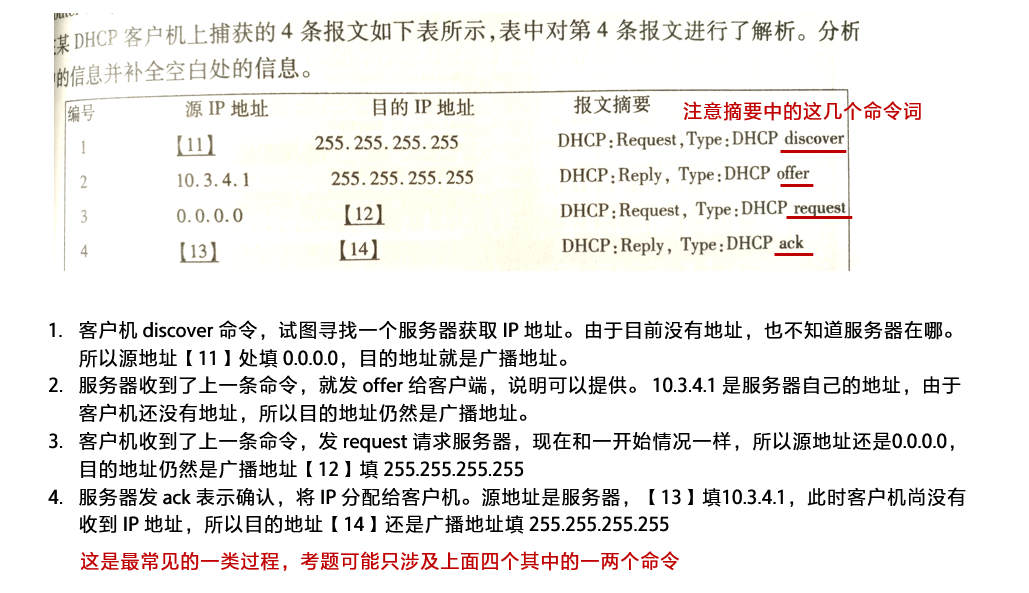


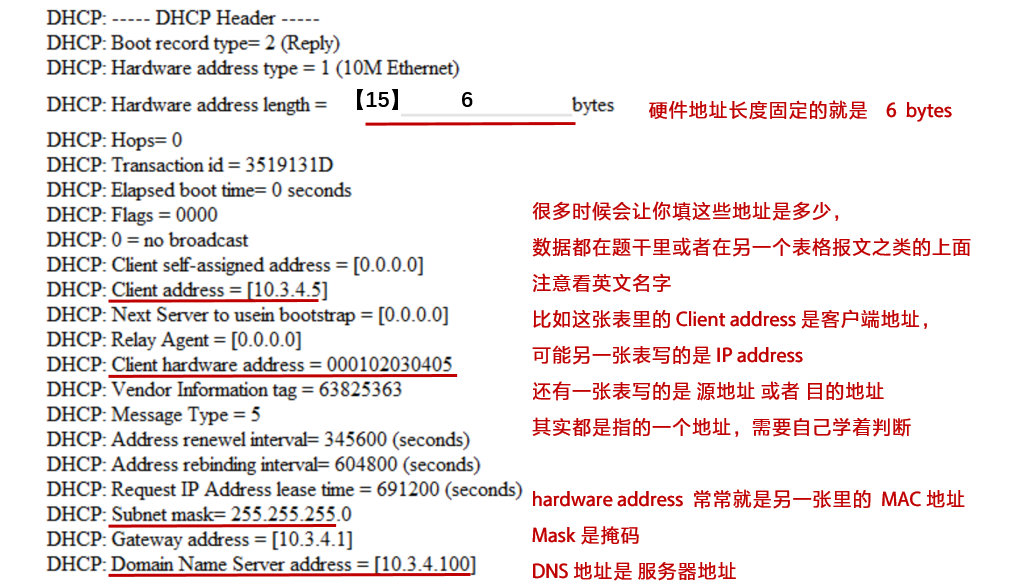


一般就考这些空，做几道之后就能填上大部分，小部分可以放弃。

**3.3 第三道 DHCP 报文**

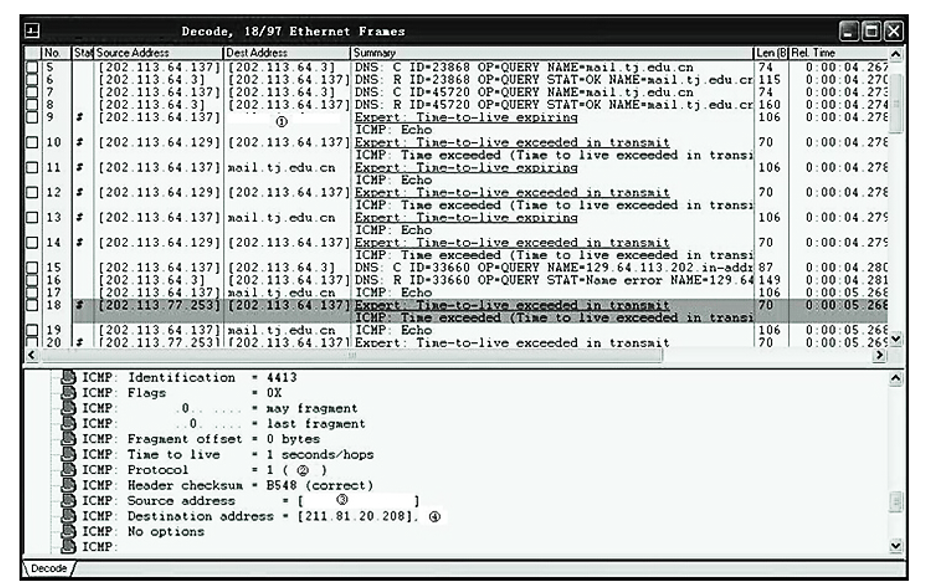
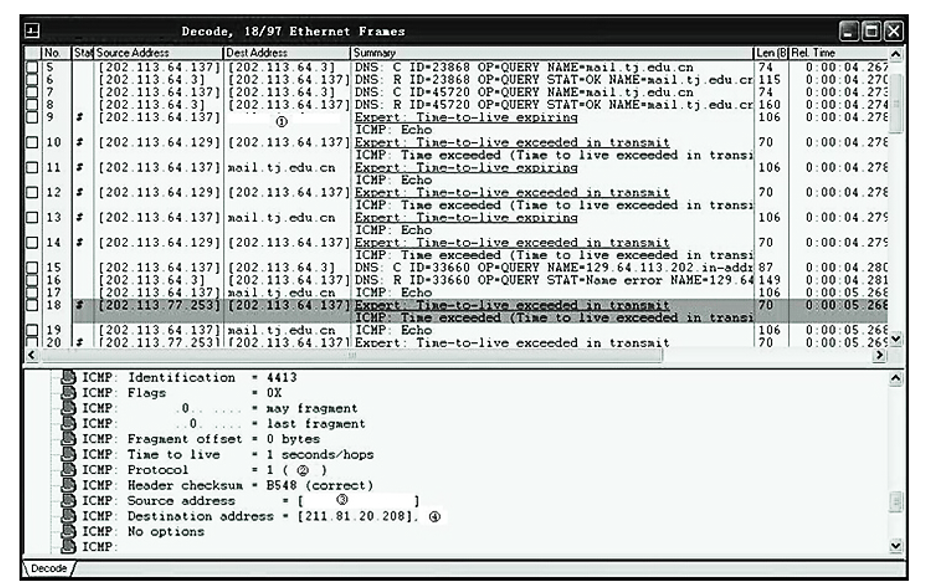
例：





**3.4 第四道 sniffer 数据包**

例1：



根据图中信息回答以下问题

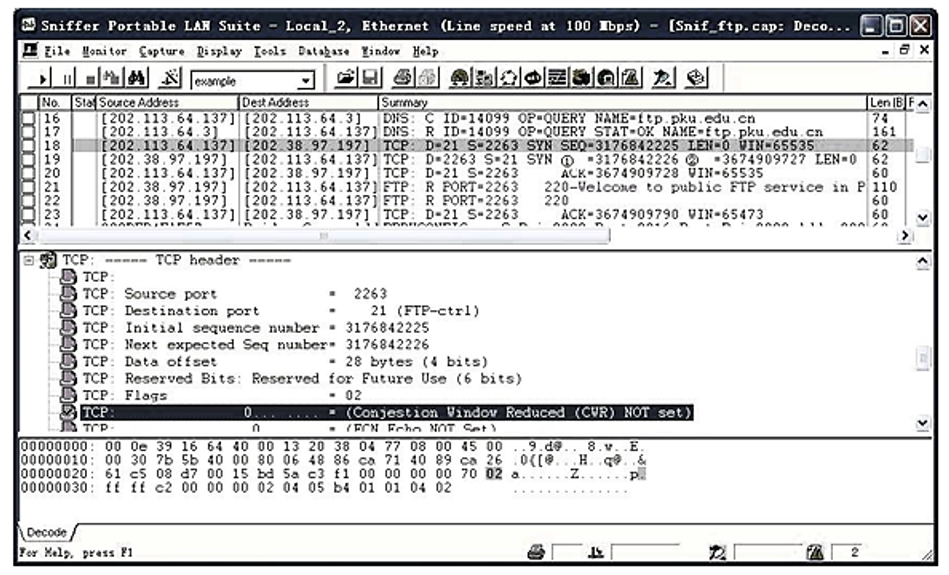
1. 该主机执行的命令是（ ），该主机配置的 DNS 服务器的 IP 地址是（ ）

解：看图中有 ICMP 几个字母，还有个邮箱地址，所以命令是 tracert mail.tj.edu.cn，DNS服务器的 IP 地址是第一行第二个地址 202.113.64.3（只要这么问，就基本是第一行第二个）

1. 图中 ② ③ ④ 处分别是（ ）

解：② 处前面 Protocol 意思是协议，协议就是 ICMP；③ 写源地址，就是第一行第一个地址 202.113.64.137；④ Destination address 意思是目的地址，这个位置应该写题中有的网址 mail.tj.edu.cn。

例2：



根据图中信息回答以下问题

1. 该主机配置的域名服务器的 IP 地址是（ ）

解：和上题一样，还是第一行第二个 202.113.64.3

1. ① 处的信息应该是（ ）

解：填 ACK。一般都是有一个 SEQ，后再有一个 ACK，接着再有 SEQ，再有 ACK。他们的数值每次 +1，有时候会根据上下行填数字。

1. 主机 202.38.97.197 是（ ）服务器，其提供服务的端口是（ ）

解：因为图中有 FTP 几个字母，所以这是 ftp服务器；提供服务的端口是 21（DNS服务器的端口是 53，邮件服务器的端口是 6）

1. 该主机执行的命令是（ ）

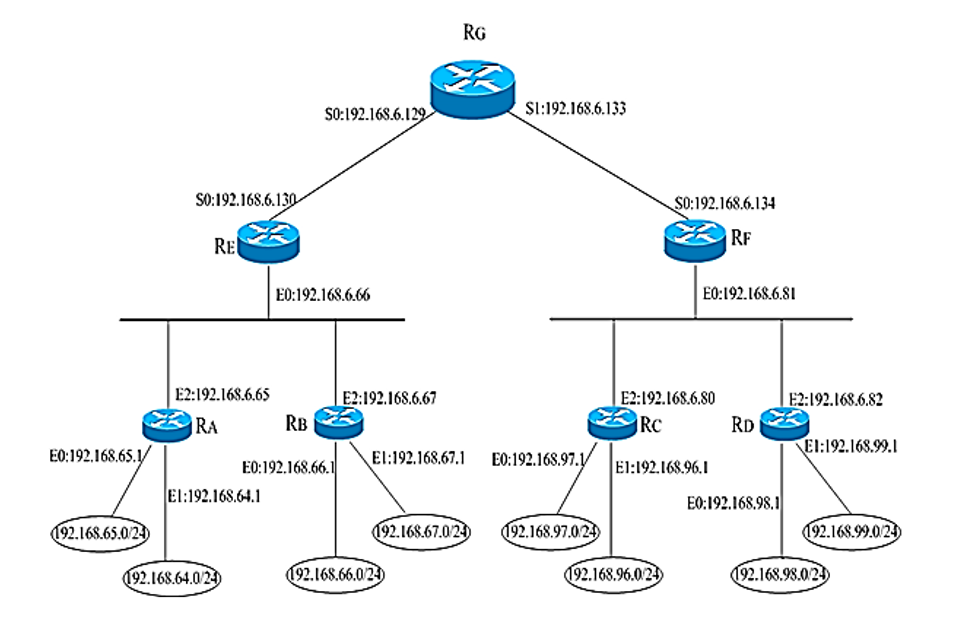
解：填 ftp ftp.pku.edu.cn（网站在图中，前面加 ftp）

这道题通常就考上面这两种模式，一种有 ICMP 对应 tracert mail.tj.edu.cn 的，一种有 FTP 对应 ftp ftp.pku.edu.cn 的。

如果让写 URL 就是 https :// mail.tj.edu.cn 或者 ftp :// ftp.pku.edu.cn（中间都没有空格，我为了格式不自动转换成链接才加的）

第四道大题也是考点很不稳定的一道。

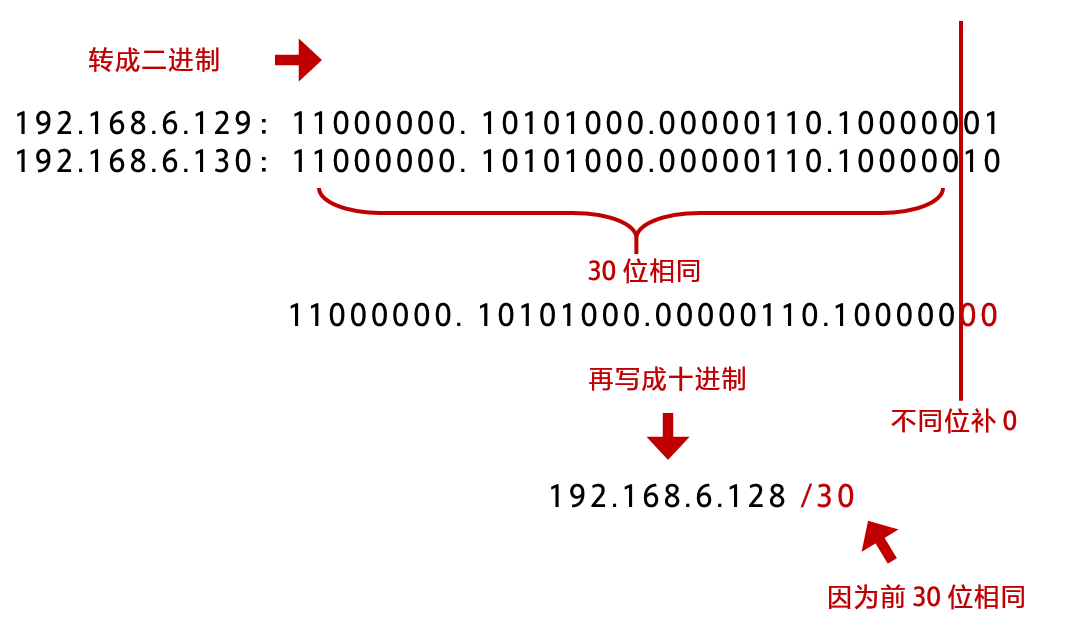
**3.5 最后一道**



**3.5.1 填表部分（12分）**

|  |  |
| --- | --- |
| 目的网络/掩码长度 | 输出端口 |
| 【1】 | S0（直接连接） |
| 【2】 | S1（直接连接） |
| 【3】 | S0 |
| 【4】 | S1 |
| 【5】 | S0 |
| 【6】 | S1 |

解：图中最上方的 RG 有两个分支，左侧分支是 S0 ，有末段为 129 和 130 的两个地址，进行聚合：



所以【1】处填 192.168.6.128/30 ；同理【2】处是 192.168.6.133 和 192.168.6.134 聚合，结果为 192.168.6.132/30。

做题实际上只要写出最后那段就行，前面选择题时已经说过了。

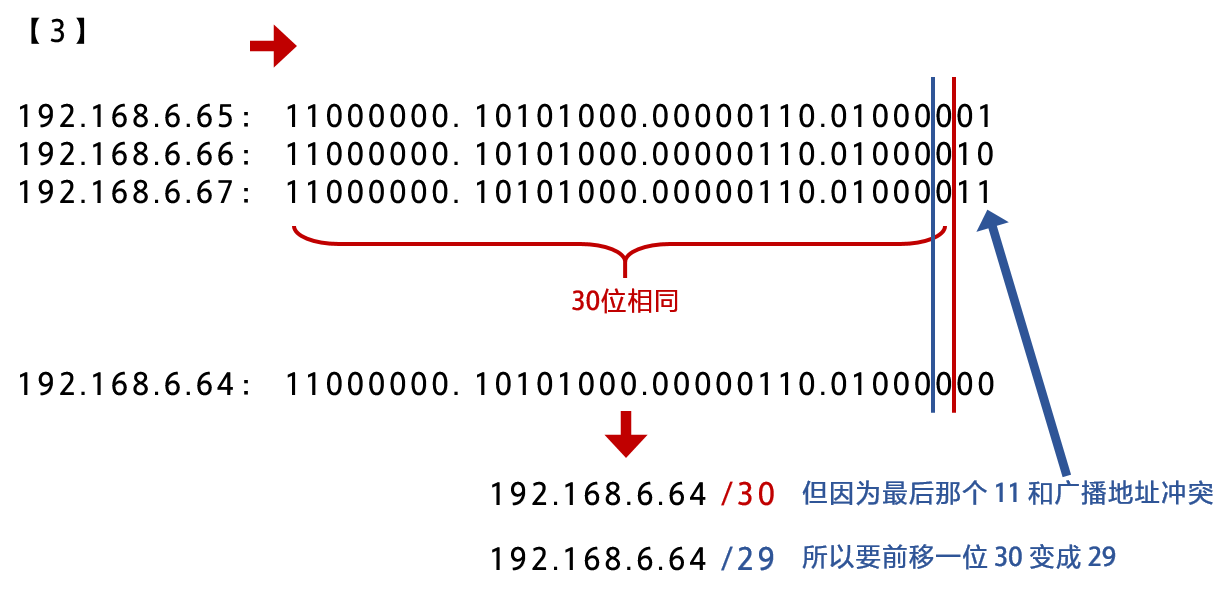
【3】是 RE 下方 192.168.6.**65**、192.168.6.**66**、192.168.6.**67** 三个子网的聚合；

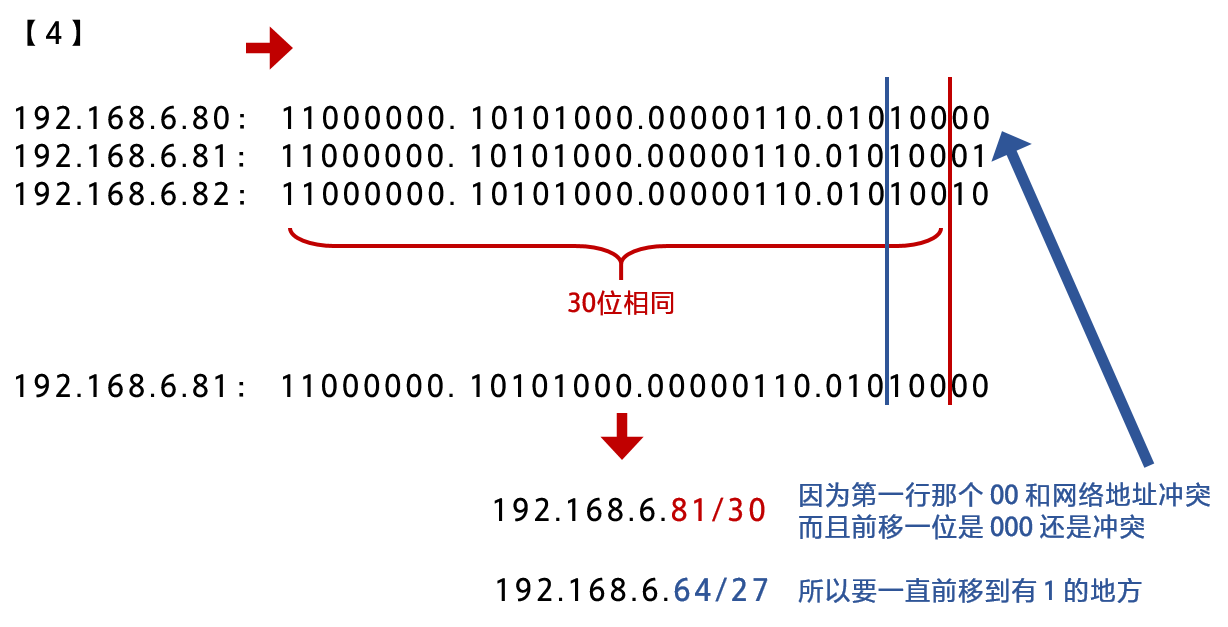
【4】是 RF 下方 192.168.6.**80**、192.168.6.**81**、192.168.6.**82** 三个子网的聚合；

【5】是 左下方 192.168.**64**.0/24、192.168.**65**.0/24、192.168.**66**.0/24、192.168.**67**.0/24 四个地址块的聚合；

【6】是 右下方 192.168.**96**.0/24、192.168.**97**.0/24、192.168.**98**.0/24、192.168.**99**.0/24 四个地址块的聚合；

在【3】【4】两空聚合时往往需要多注意





最终答案应为

【3】192.168.6.64/29

【4】192.168.6.64/27

【5】192.168.64.0/22

【6】192.168.96.0/22

这个填表是必拿分的题。

**3.5.2 中间部分（2~4分）**

这部分考点很不固定，下面是频率稍高的，考试这几分放弃也可以

1. 问在某路由器上，最多还可链接的路由器数量是多少。如果所在子网掩码是 /29 就填 3，是 /28 就填 11。
2. 问串接一种设备能监听路由器之间的流量，写 TAP
3. 问串接一种设备能提供安全保护，一般是 IPS
4. 问防火墙访问外网设置，分别填 nat 和 global

**3.5.3 计算子网掩码和 IP 段部分（4~6分）**

例：将 192.168.66.128/25 划分为三个子网，子网 1 能容纳 50 台主机，子网 2 和 3 能分别容纳 20 台主机……求他们的子网掩码和可用 IP 地址段

解：题中说多少台主机的具体数字不重要，刚好大于那个数字的 2 的 n 次方的数才重要。

比如 50 台，就是 64，是 2 的 6 次方。所以子网掩码后 6 位都是 0 （前面全是 1 ），11111111.11111111.11111111.11000000 ，最后填空写 255.255.255.192

同理 20 台，就是 32，是 2 的 5次方。所以子网掩码后 5位都是 0，最后填空 2 和 3 的子网掩码都是 255.255.255.224

可用 IP 地址从题目所给的那个数 +1 开始，本题是 192.168.66.129（因为太乱，下面只写末段数字，反正前面都一样）

从 129 开始，因为子网 1 的那个数字是 64 ，所以到 190 结束（129+64**-3**=190，不用管为什么，结束都是 -3）

下一段从 193 开始（190**+3**=193，不用管为什么，开始都是 +3），因为子网 2 的那个数字是 32 ，所以到 222 结束（193+32**-3**=222）

再下一段从 225 开始（222**+3**=225），因为子网 3 的那个数字也是 32 ，所以到 254 结束（225+32**-3**=254）

写成答案分别为：

子网 1 的可用 IP 地址段为 192.168.66.129~192.168.66.190

子网 2 的可用 IP 地址段为 192.168.66.193~192.168.66.222

子网 3 的可用 IP 地址段为 192.168.66.225~192.168.66.254

看起来上面写了一大堆，其实明白了就很简单，这个也是必拿分的题。

**总结：得分策略**

目标是通过考试，也就是 60 分

1. 选择题部分：前面一共写了 10 个做法固定的“第一类选择题”，还有 19 个“第三类选择题”的高频考点，加上“第二类选择题”。选择题得分在 20 分以上是很保守的估计，没有意外的话选择题应该在 25 分以上。
2. 大题部分：第一道的 10 分是必得的，最后一道除了中间部分后有 16 分是必得的。从前面写的也能看出第二、三、四道大题的考点不是特别固定，所以尽量写，填对一半就很好了（其实也没有那么难），所以这三道大题 30 分目标是得 15 分。

来算一下 20 + 10 + 16 + 15 = 61 分。实际情况当然可能会出现意外，比如三道大题没得到 15 分，但刚才也没算你蒙对的题得分。

多练习几套题，来回对照着知识点就熟悉了，这个考试题型固定，含金量不高，难度不大，不用害怕。题库软件有很多缺陷，比如大题评分不准、填空题缺少空格，甚至是答案错误。自己要注意核对。这份文档并未涵盖所有知识点，多做一套题就多了一分考过的把握。

（未来教育题库的第九套题有点特殊，看起来像 13 年考试改革之前的老题，和其他套的题有很大差别，留意一下。）

完。

2017/3/19 初版

2017/4/25 修改了前言与总结

2017/5/12 修改内容略

2017/5/16 刚查到成绩，84分，本来还以为能上90…

2017/8/23 补充了备考建议

2017/9/12 改正了 2.1.6 IP地址块聚合

2017/9/21 增加了 2.3 中近一半的内容，感谢佚名进行的补充

2017/12/18 考试获证条件改变，三级不再需要对应的二级科目通过

2018/3/24 增加了一些知识的补充。