某公司网络中有一个无线 AP，供公司内部笔记本电脑用户在会议室中上网使用，因为原来没有配置 WEP，使得未授权人员得以通过该 AP 连接 Internet。为了提高其安全性，公司网管就准备在该 AP 上配置 WEP。其配置界面如图 1 所示：

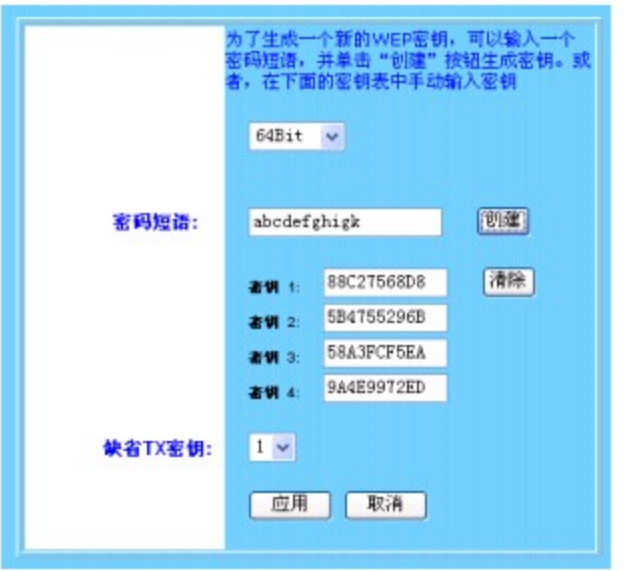

图 1 WEP 配置界面示意图

【问题 1】(8 分)

根据图 1 的配置，当点击“应用”按钮，使其生效之后，那么在授权用户的电脑上，应该如何设置无线网卡？其密码应该设置为什么？

【问题 2】(8 分)

根据 IEEE 802.11 标准，WEP 是属于认证机制还是数据加密机制？WEP 所采用的是什么加密算法？它包括哪两种类型？

【问题 3】(9 分)

设置了 WEP 之后，有些公司中未授权用户通过非正规渠道了解了 WEP 密码后仍然跳过了这层安全机制。如果希望在不改动用户端配置，透明地实现更进一步的安全限制，使得这些非授权用户无法访问，那么可以采用什么机制？

试题一参考答案

【问题 1】（8 分）

将无线网卡的“数据加密”选项设置为“WEP”，并输入相应的网络密钥。（4 分）

根据该配置，网络密钥应该是“88C27568D8”。（4 分）

【问题 2】（8 分）

WEP 是数据加密机制（2 分），它所使用的是 RC4 对称加密算法（2 分），包括 64 位密钥和 128 位密钥两种类型。（各 2 分）

【问题 3】（9 分）

可以采用 MAC 地址过滤机制。

查看分析

试题一分析

【问题 1】-【问题 2】

根据 IEEE 802.11 标准，其安全机制包括认证机制和数据加密机制。而数据加密机制就是有线等效加密 WEP。

WEP 是一个简单的加密算法，包括 64 位密钥和 128 位密钥两种类型。WEP 使用的是 RSA 数据安全公司的使用伪随机数生成器 RC4 对称加密算法。这种加密机制通过将一个短密钥（种子密钥，密钥短语）扩展为任意长度的伪随机密钥流，发送端再用这个生成的伪随机密钥流与报文进行异后运算来产生密文。接收端用相同的密钥产生相同的密钥流，并且用这个密钥流来对密文进行异或运算而得到原始的报文。

而在图 2 中，其创建过程就是在“密钥短语”中输入一个种子密钥，点下“创建”按钮之后，就会利用 RC4 算法，生成四组伪随机的密钥，而由于我们在“缺省 TX 密钥”中选择的是“1”，因此使用的是第 1 组密钥，即“88C27568D8”。

当在 AP 上设置了 WEP 密钥后，就需要将一个静态的密钥（在本例中，就是生成的“88C27568D8”）手动地分配到和它连接的有线客户端，具体的操作就是，在每个授权客户端的无线网卡属性中，将“数据加密”一项设置为“WEP”，并在“网络密钥”中设置为这个生成密钥，如图 2 所示：

图 2 客户端配置示意图

【问题 3】

正如前所述，由于 WEP 采用的是静态的密钥分发机制，因此其安全性还是比较有限的，只是最基本的安全机制。在无线局域网中还能够通过 802.1x、WPA+TRIP、WAPI 等技术来实现更高级别的安全机制，这些机制都能够避免非授权用户钻空子。或者采用 RADIUS 等技术来实现基于用户的认证，但这些都需要在客户端做相应的配置，或者是在登录时输入相应的用户帐号和密码，无法达到题目中“不修改客户端、透明应用”这两个需求，因此都不适用。

因此，我们可以使用的只有基于 MAC 地址过滤的方式，它可以将无线局域网设备为给特定的无线客户使用，只需将授权用户的笔记本电脑的 MAC 地址输入到允许访问的列表中，就可以解决这个问题。当然它会造成一定的不便性，需要手工来实现动态更新。

在某网络中拥有10余台的路由器，为了方便对这些路由器进行管理，该网络的管理员决定采用终端服务器来实现。终端服务器将通过 Async 端口与被管理的路由器的 Console 端口连接，如图1所示：

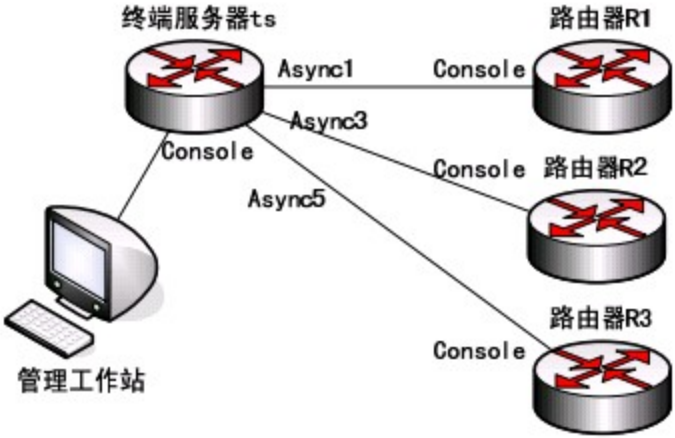

图1 终端服务器示意图

【问题1】（6分）

以下是终端服务器上的一个配置片段，请解释（1）-（3）处的命令，将答案填写在答题纸上。

```
……
inteface Loopback0
    ip address 1.1.1.1 255.255.255.255                    （1）
interface Ethernet0
    ip address 192.168.1.0 255.255.255.0
……
line con 0
line 1 16
    no exec                                                （2）
    transport input all                                    （3）
```

【问题 2】（3 分）

根据问题 1 中的终端服务器上的配置，如果在终端服务器上要连接路由器 R1，应该使用什么命令？该终端服务器最多可以连接多个台路由器？

【问题 3】（6 分）

如果希望能够在终端服务器上输入 R1 则连接到路由器 R1，输入 R2 就连接到路由器 R2，输入 R3 就连接到路由器 R3，则应该如何配置？请写出配置命令。

查看答案

试题二参考答案

【问题 1】（9 分）

（1）将回送地址设置为 1.1.1.1，子网掩码为 255.255.255.255。（3 分）

（2）关闭线路的 EXEC 处理，只允许从终端服务器连接到路由器。（3 分）

（3）设置为允许所有的协议通过连接到指定路由器的线路上。（3 分）

【问题 2】（7 分）

telnet 1.1.1.1 2001（3 分）

最多 16 个（4 分）

【问题 3】（9 分）

ip host R1 2001 1.1.1.1（3 分）

ip host R2 2003 1.1.1.1（3 分）

ip host R3 2005 1.1.1.1（3 分）

试题二分析

【问题 1】

终端路由器是路由器所提供的一种功能，现在大多数路由器都可以用作终端服务器。在终端服务器的配置中，需要增加一个 loopback 接口，即回送接口，用于逆向 Telnet。通常我们会将 loopback 接口的 IP 地址的子网掩码设置为 255.255.255.255，以节省 IP 地址。

而与路由器连接的是异步端口（Async，即在配置中的 line 1-16），根据终端服务器的不同其端口数也不同。但为了防止终端服务器在端口接收数据时产生一个 EXEC 进程，从而避免可能出现的线路无效，我们通常会用 no exec 来禁止这些异步线路上产后 EXEC 进程，而只允许线路出境（从终端服务器向其他路由器）连接。

而且为了更方便使用，通常会在 line 线路上配置 transport input all 来指明所有的协议可被用于连接到指定的路由器线路。

【问题 2】

当终端服务器与路由器之间通过异步端口连接之后，要从终端服务器连接到这些路由器就可以通过如下格式的命令来实现：

Telnet *loopback 接口的 IP 地址* **20*xx***　（其中 xx 表示异步端口号）

因此，连接到 R1，就应该是：Telnet 1.1.1.1 2001（连接的端口是 Async1）；同理连接到 R2，就应该是 Telnet 1.1.1.1 2003，连接到 R3 就应该是 Telnet 1.1.1.1 2005。

而本题中的配置文件中有 line 1-16，说明有 16 个 Async 端口，即可连接 16 台路由器。

【问题 3】

Cisco IOS 软件维护一个主机名表和它们相对应的地址，可以像域名服务器一样通过它们映射主机名到 IP 地址。因此，在本题中的需求就应该借助它来实现。它的命令格式是：

ip host *主机名 端口号 IP 地址*

因此显然就是：ip host R1 2001 1.1.1.1、ip host R2 2003 1.1.1.1、ip host R3 2005 1.1.1.1

试题三（25 分）

图 1 展示了某网络的结构情况，有两台交换机 SW1、SW2 通过一条 Trunk 线路连接在一起，共享着 VLAN 配置。该网络中共有 101-106 六个 VLAN，图中的小标签分别表示着这些 PC 所处的 VLAN。根据习惯 Trunk 线路总是从最后一个端口开始使用，而 SW1 和 SW2 都是一个 24 口交换机，该线路使用的是 24 号端口（f0/24）。

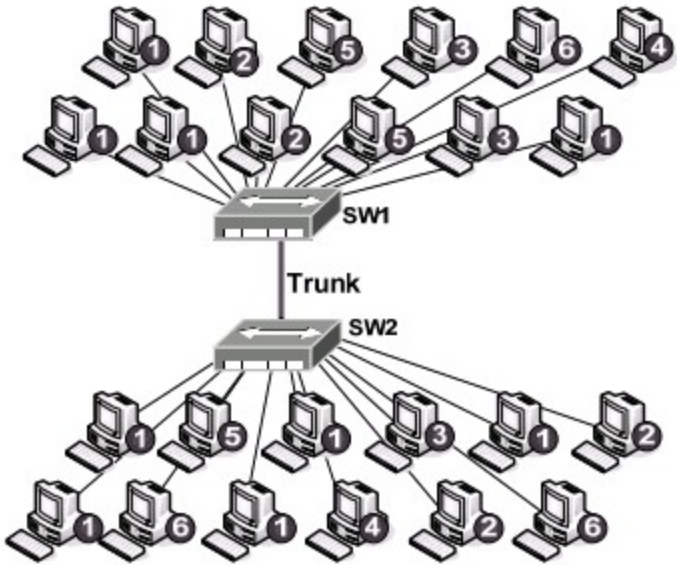

图 1 网络结构示意图

【问题 1】（5 分）

由于两个交换机中有多个 VLAN，因此使得 Trunk 线路的负载变得过重，这时小张提出一了可以增加一条 Trunk 线路。但有人认为这个解决方案会造成网络环路，小张马上说没关系可以使用 STP 来解决网络环路问题。请问 STP 指的是什么，它是怎么解决这个问题的？

【问题 2】（8 分）

在所有参与 STP 的交换机都将通过数据消息的交换来获取网络中其它交换机的信息，这些信息称为什么？在该信息中的计时器包括哪四种？

【问题 2】（8 分）

在所有参与 STP 的交换机都将通过数据消息的交换来获取网络中其它交换机的信息，这些信息称为什么？在该信息中的计时器包括哪四种？

【问题 3】（12 分）

在通过两个交换机的 f0/23 端口处增加了一个 Trunk 线之后，现在希望使得 VLAN 101-103 通过原来的 Trunk 线路，VLAN 104-106 则通过新的 Trunk 线路。

```
SW1# config terminal
SW1config)# interface __（1）__
SW1(config-if)# spanning-tree vlan 103 port-priority 20
SW1(config-if)# spanning-tree vlan 102 port-priority 20
SW1(config-if)# spanning-tree vlan 101 port-priority 20
SW1(config-if)# exit
SW1(config)# interface __（2）__
SW1(config-if)# spanning-tree __（3）__ port-priority 20
SW1(config-if)# spanning-tree __（4）__ port-priority 20
SW1(config-if)# spanning-tree __（5）__ port-priority 20
```

对于 SW2 的配置，可以与这里的配置一样吗？

查看答案

试题三参考答案

【问题 1】（5 分）

STP 是生成树协议。（2 分）

它是通过判断网络中存在环路的地方并阻断冗余链路，从而解决网络环路问题。（3 分）

【问题 2】（8 分）

BPDU，桥接协议数据单元。（4 分）

包括消息寿命（message age）、最大寿命（max age）、Hello 和转发延时四个。（4 分）

【问题 3】（12 分）

（1）f0/24（2 分）

（2）f0/23（2 分）

（3）vlan 104（2 分）

（4）vlan 105（2 分）

（5）vlan 106（2 分）

SW2 的这部分配置是可以与 SW1 一样的。（2 分）

查看分析

试题三分析

【问题 1】-【问题 2】

生成树协议（STP）是为克服冗余网络中透明桥接的问题而创建的。STP 的目的是通过协商一条到根网桥的无环路路径来避免和消除网络中的环路。它通过判断网络中存在环路的地方并阻断冗余链路来实现这个目的。如果某条链路失效了，因为根网桥知道还在冗余链路，就会启用先前关掉的这条冗余链路。也就是说某些端口需要被关闭或置为非转发模式。这些端口仍然知道网络的拓扑结构，并且，如果正在转发数据的链路失效了，它们就可以被启用。

生成树协议执行一种称为生成树算法（STA）的算法。为了找到冗余链路，STA 在网络中选择一个被称为根网桥的参考点，然后确定到该参考点的可用路径。如果它现存在冗余路径，它将选择最佳的路径来负责数据包转发，同时阻断所有其它冗余路径。这样就可以有效地切断网络中的冗余网络。

在一个扩展的局域网中参与 STP 的所有交换机都将通过数据消息的交换来获取网络中其他交换机的消息。这些消息称为桥接协议数据单元（BPDU）。BPDU 在每个端口上每两秒钟发送一次以确保一个稳定的、无环路的拓扑结构。

BPDU 中包括根信息、路径开销、网桥信息、端口信息以及计时器。计时器用于说明生成树用多长时间完成它的每项功能。这些功能包括消息寿命、最大寿命、hello 和转发延迟。

【问题 3】

要正确的解答这个问题的关键在于必须了解每个交换机端口的“端口权值”的默认值是 128，权值小的将优先通过。因此，在配置的第一部分，显然是使得 VLAN 101-103 能够通过，因此第（1）空就应该填入“f0/24”（原来的 Trunk 线路）。

这个问题得到解答后，就可以很快地得知。我们要在另一个 Trunk 端口中，使得 VLAN 104-106 的权值更小。

由于两台交换机都要配置这些信息，而且规则是一样的，因此显然配置是可以一样的。