试题一（25 分）

图 1 所示的是某公司办公区的一个局部，其中 WNC 是无线网络控制器，用来自动探测、监控、管理无线 AP（图中两个 AP 均采用的是全向天线）。该网络采用 Web＋DHCP 方式解决用户接入问题，当用户连上无线接入点，由无线网络控制器为用户自动的分配 IP 地址，基于 Web 的认证成功后即可访问 Internet。认证过程采用 RADIUS 技术，以防止非法用户的盗用。

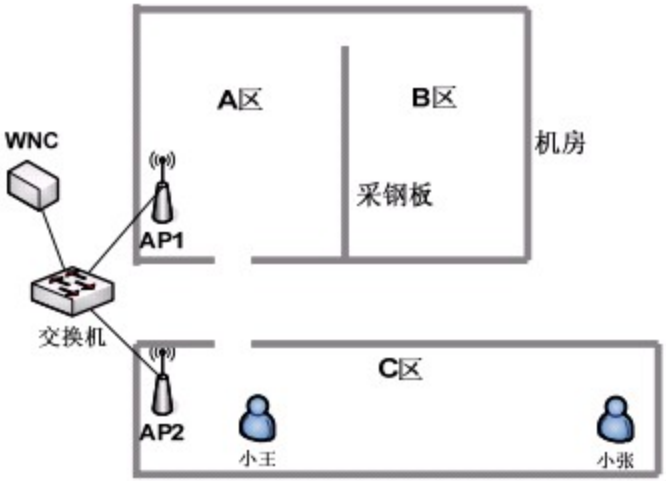

图 1 某公司办公区无线网络示意图

【问题 1】（7 分）

1. 该网络安装完成后，B 区的用户经常反馈说网络连接质量很差，信号很弱，试说明原因，并提出解决方案。（字数控制在 100 字以内）
2. 而在 C 区的用户小张也是经常反馈说网络连接质量比较差，而小王却说不会，试说明原因，并提出两种解决方案。（字数控制在 100 字以内）

【问题 2】（4 分）

由于 AP1 和 AP2 离得太近，因此经常会使得 A 区用户连接到 AP2 上，C 区的用户连接到 AP1 上，产生一定的不便。如何通过 AP 的配置来杜绝这一现象的发生？

【问题 3】(14 分)

RADIUS 的主要功能是用于对用户进行授权和认证，在客户端进行 RADIUS 验证时，其整个过程为：

① 客户端提交 Access-Request 数据包，该数据包中的“用户名/口令”是__（1）__格式的。

② 客户端发送一个__（2）__数据包给 RADIUS 服务器，其中包含了用户名、口令、ID 号和用户访问的端口号，其中“用户名/口令”的加密情况是__（3）__。

③ RADIUS 服务器返回一个 Access-Accept 数据包，其中包括__（4）__及相关信息。

④ RADIUS 在认证数据库中查找用户是否存在，并根据用户的权限信息进行验证，如果通过则向客户端发送__（5）__数据包。

另外，如果 RADIUS 服务器收到没有加“共享密钥”的请求，则会__（6）__。以上四条描述，正确的顺序应该是__（7）__。

查看答案

试题一参考答案

【问题 1】(7 分)

1. 因为受到 A 区和 B 区之间隔墙的影响，使得信号强度降低。(2 分) 应在 B 区增加一个 AP。(2 分)

2. 因为 C 区是一个较狭长的办公区，小张的位置离 AP 太远，因此信号强度降低。(1 分) 可以将 AP2 移到办公区中心位置 (1 分)，或者换成定向天线的 AP。(1 分)

【问题 2】(4 分)

将 AP1 和 AP2 的信道 (或称为频道) 设置为不同 (2 分)，最好是分别使信道 1 和信道 11 (2 分)。

【问题 3】（14 分）

（1）密文格式

（2）Access-Request

（3）用户名不加密，口令用 MD4 加密

（4）服务类型

（5）Access-Challenge

（6）直接抛弃

（7）②④①③

查看分析

试题一分析

【问题 1】

这是一道无线 AP 位置摆放的问题，与实际应用结合得比较紧密。在摆放无线 AP 时，有两个要点必需牢记于心：一是无线 AP 是基于微波进行通信的，因此在遇到障碍物时信号会衰减；二是传输距离会使得信号减弱。因此在实际的摆放时，要注意这两点。

显然根据这两个原则，可以发现 B 区和 AP1 之间有面墙，会减弱信号。而且这面墙还是使用了衰减影响最大的金属，因此网络质量必然是很差的。对于这种情况最简单的方案就是在 B 区再设置一个 AP。

而 C 区一个狭长的办公区，随着距离的加大，信号也会衰减，因此用户小张会觉得网络质量差。由于其使用的是全向天线，因此首先应该想到的是将其放置在办公区的中间位置，而另一种方案则是利用定向天线的特性，将信号集中在一个特定的方向，从而增加了信号的强度，从而解决这个问题。

【问题 2】

由于 AP1 和 AP2 两个访问点的信号范围是重叠的，因此它们会相互干扰，而一般同一品牌的 AP 的工作信道设置是相同的，因此会出协同信道干扰。对于协同信道干扰的解决方案通常有两个：

- 对于每一个无线局域网用不同的、非重叠的信道使用；
- 如果无线局域网的距离较大，则使访问接入点的小区没有信道重叠。

而一个最简单的选择是，在仅仅两个访问接入点的情况下使用信道 1 和信道 11.不管两个系统多么接近，仅仅应用这两个信道将确保我们在信道之间没有重叠。因此，对于每一个无线 AP 的吞吐量上没有危害的影响。

如果网络规模要求必须是 3 个以上的无线 AP 才可以，特别是在被要求无缝漫游时，为了减轻邻近和相同信道干扰，可以使用信道复用技术。信道复用就是并排放置的非重叠的小区构成一个覆盖网，如图 2 所示：

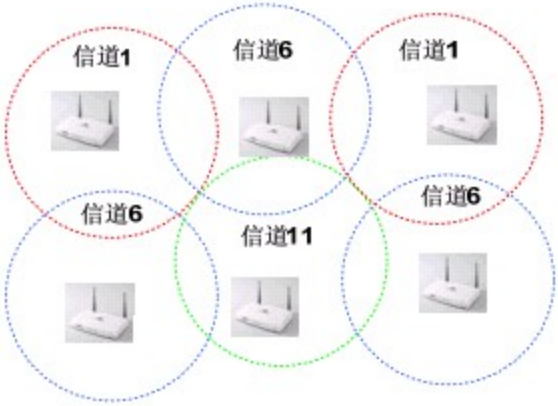

图 2 多信道复用示意图

【问题 3】

在使用 RADIUS 验证时，整个过程为：

- 客户端发送一个“Access-Request”数据包给 RADIUS 服务器，其中包含了用户名、口令（使用 MD5 加密）、ID 号和用户访问的端口号。
- RADIUS 服务器收到“Access-Request”包后，会在认证数据库中查找用户是否存在，如果存在，则提取此用户的信息列表，其中包括了用户的口令、访问端口和访问权限。并根据该信息进行验证。
  - 如果信息被否认，则返回“Access-Reject”数据包，指示此用户非法。
  - 如果确认，则发送“Access-Challenge”数据包，并加入状态属性等反馈信息。
  - 如果没有加“共享密钥”的请求，将直接抛弃。
- 客户端收到“Access-Challenge”包后，就会再次提交带新请求 ID 的“Access-Request”数据包，其内容与最初的不同的地方在于：“用户名/口令”信息替换为加密信息，加上了“Access-Challenge”的状态属性。
- 如果所要求的合法，RADIUS 服务器返回一个“Access-Accept”数据包，其中包括了服务类型（可以是 SLIP、PPP、Login User）及相关信息。例如 PPP 中就包括 IP 地址、子网掩码、MTU 和数据包过滤标示等。

试题二（25 分）

某公司原先公司共有 20 余台电脑，连接在一个 24 口的交换机上，大家都在同一个子网之内。后来为了实现逻辑的子网划分，根据公司的部分不同来分隔网络，就决定采用交换机支持的 VLAN 技术。

【问题 1】（10 分）

VLAN 的划分方法有哪四种？在默认配置下，交换机（支持 VLAN）有几个 VLAN，端口的分配情况是什么？

【问题 2】（8 分）

如果我们要将交换机上的端口直接分配给某个 VLAN，有两种配置的方法，请说明分别是什么？

【问题 3】（7 分）

如果需要动态地配置将交换机端口指定给 VLAN，则通常需要使用什么服务器？它采用的应用层协议是什么？

查看答案

试题二参考答案

【问题 1】（10 分）

按端口划分，按 MAC 地址划分，按协议地址划分，按策略划分。（每个 2 分）

默认情况下，有一个 VLAN1，所有端口都属于该 VLAN。（2 分）

【问题 2】（8 分）

一种是进入要配置的端口的子配置模式，用 switchport mode access 和 switchport access 命令来配置。（4 分）

另一种是采用 set vlan 来对多个端口同时配置其归属的 VLAN。（4 分）

【问题 3】（7 分）

需要 VMPS（VLAN 成员策略服务器），（3 分）它是基于 TFTP 协议的（4 分）。

【问题 1】

VLAN 的划分策略类型包括静态虚拟网、动态虚拟网、多虚拟网端口三种，而具体则包括四种划分的方法，如表 1 所示：

表 1　VLAN 划分方法

方法	说明	优点	具体方法
静态虚拟网	直接设置交换机端口，使其从属于某个 VLAN	安全、易于配置和维护	按端口划分
动态虚拟网	通过 MAC 地址、逻辑地址或协议类型来决定 VLAN 从属	灵活、高效，但不安全	按 MAC 地址划分 按协议地址（IP）划分 按策略划分
多虚拟网端口	支持一用户或端口同时访问多个 VLAN	可以实现 VLAN 之间的路由，但存在安全隐患	

对于新的交换机而言，只要是其支持 VLAN，则默认就会有一个 VLAN1，所有的端口都属于该 VLAN。

【问题 2】

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。我们可以使用 set vlan 命令来设置一个 VLAN，用 clear vlan 来清除一个 VLAN：

CTest# set vlan *vlan_num mod_num/port_list*　　（设置 VLAN）

CTest# clear vlan *vlan_num*　　（清除 VLAN）

其中：vlan_num 是指 VLAN 编号，mod_num 是模块号，port_list 是端口列表。我们可以使用独立的条目输入，也可以使用连字符格式，例如：

CTest# set vlan *101 2/1-10*　　（将模块 2 的 1-10 号端口分到 VLAN 101）

CTest# set vlan *102 2/11*　　（将模块 2 的 11 号端口分到 VLAN 102）

同样，我们还可以进入某个端口的子配置模式后，再通过以下两个命令来使其属于某个特定的 VLAN：

CTest（config-if）# switchport mode access

CTest（config-if）# switchport mode *vlan_num*

【问题 3】

设置为动态 VLAN 的端口将被动态指定给 VLAN，它是由 VLAN 成员策略服务器（VMPS）完成的。VMPS 通常是一个 TFTP 服务器，提供了 VMPS 数据库（文本文件）下载功能，该文本文件包含了 VLAN 到 MAC 地址的映射。当动态 VLAN 端口启动后，交换机将检查 VMPS 服务器，将源 MAC 地址与数据库比较，如果存在条目，端口就将指定给目标 VLAN。

某大学申请了一个名为“abc.edu”的域名，为了方便动态地根据院系的需要，分配、管理和解析二级域名，决定自行架设 DNS 服务器，他们采用了 Linux+Bind 的解决方案来构建。

【问题 1】（12 分）

Bind 安装完成后，它会运行一个 named 的服务进程，而该服务进程在启动时会读取一个初始化配置文件，该文件的名称是什么？该文件的配置内容如下所示：

```
1   diretory   /etc/named
2   primary    abc.edu                          db.abc
3   primary    55.101.202.IN-ADDR.ARPA   db.202.101.55
4   cache      .                                db.cache
```

请说明第 2、3、4 行配置命令的功能分别是什么。

【问题 2】（11 分）

在配置文件 db.abc 中，其中包括以下内容：

```
1   @        IN     SOA    dns.abc.edu      root.dns.abc.edu. (
                                200002011    ；文件版本号
                                28800        ；刷新时间（秒）
                                7200         ；重试时间（秒）
                                3600000      ；终止时间（秒）
                                86400）      ；TTL 生存时间（秒）
2               IN     NS     dns.company.com
3   www         IN     A      202.101.55.1
4   computer    IN     A      202.101.55.2
5   cs          IN     CNAME  computer
6   mail        IN     MX     202.101.55.10
```

1. 在配置的第 1 行，有一个严重的错误，请以“xxx”应为“xxx”的格式指出。

2. 计算机系的域名为 computer.abc.edu，其对应的 IP 地址是什么？除了该域名外，还可以用什么域名来访问该系的网站。

3. 该学校的邮件服务器的 IP 地址是什么？

【问题 3】（2 分）

当完成了 DNS 配置之后，可以使用什么命令来验证？

查看答案

试题三参考答案

【问题 1】（12 分）

初始化配置文件：named.boot（2 分）

第 2 行配置：说明该 DNS 服务器是 abc.edu 的主域名服务器（2 分），所有*.abc.edu 形式的域名解析数据都存在 db.abc 文件中。（2 分）

第 3 行配置：说明该 DNS 服务器作为 202.101.55 网段地址转换主服务器（2 分），所有以 202.101.55.*形式的地址到域名的转换数据均存在 db.202.101.55 文件中。（2 分）

第 4 行配置：指定 DNS 从 db.cache 文件中获得 Internet 的顶层“根”服务器地址。（2 分）

【问题 2】（11 分）

1. “dns.abc.edu”应为“dns.abc.edu.”（2 分）
2. 202.101.55.2（3 分），cs.abc.edu（3 分）
3. 202.101.55.10（3 分）

【问题 3】（2 分）

应使用 nslookup。（2 分）

试题三分析

【问题 1】

named 启动时需要读取一个初始化文件——/etc/named.boot，这个文件是 named 的基本配置文件。它并不包含任何 DNS 数据，主要是指定与其相关的配置环境与配置信息：

- 在第 1 行中我们指定 named 从/etc/named 目录下读取 DNS 数据文件。这个目录可以自行指定并创建，指定后将所有的 DNS 数据文件均存放在这个目录下；
- 第 2 行指定 named 作为 abc.edu 的主域名服务器，并将该域名下的所有二级、三级域名（也就是所有*.abc.edu 形式的子域名）以及其它相关的解析数据存入到 db.abc 文件中。该文件中就是实现 DNS 正向解析（根据域名，解析 IP 地址）的依据。
- 第 3 行指定 named 作为 202.101.55 网段地址转换主服务器，db.202.101.55 文件中包含了所有以 202.101.55.*形式的地址到域名的转换数据。字实际上就是实现 DNS 反向解析（根据 IP 地址，解析域名）的依据。
- 最后一行指定 named 从 db.cache 文件中获得 Internet 的顶层“根”服务器地址，也就是使其能够从其它的域名服务器获得信息来解析不属于其管理的域名信息。

【问题 2】

题目中给出的是一个典型的域名解析数据的配置，以下我们就逐一地解释一下它的作用与含义。

- SOA 是主服务器设定文件中一定要设定的命令，我们通常将它放在文件的第一行。
  - 最前面的符号“@”代表目前所管辖的域。
  - 接着的“IN”代表地址类别，这里就是固定使用“IN”的。
  - 接下来就是命令 SOA。
  - 接下来填入域名服务器，记住由于 DNS 数据文件的要求使用全称域名（也就是最后必须加上一个“.”），因此我们应该填入域名服务器：“**dns.abc.edu.**”，而在本例中，这里就一个严重的错误，会造成其无法解析。
  - 接下来是域名服务器管理员的 E-MAIL 地址，但要注意的是，E-Mail 地址中的分隔符“@”在这里用“.”来代替，在最后也要加上“.”，在这里，我们相应写入：“root.dns.abc.edu.”
  - 接下来在括号内填入的一些相关的配置选项：

表 17-5 SOA 记录配置选项

配置项	含义
文件版本号	修改文件时同步修改，以区分是否更新
更新时间	指定二级服务器向主服务器拷贝数据的更新时间周期
重试时间	指定二级服务器在更新出现通信故障时的重试时间
终止时间	指定二级服务器重新执行更新动作后仍然无法完成更新任务而终止更新的时间
生存时间	指定当域名服务器询问某个域名和其 IP 地址后，在域名服务器上放置的时间。

注：二级服务器所设定的域名服务器是主服务器的备份主机。

- 在第 2 行中，我们用 NS 命令指定这个域的域名服务器。在这里我们指出这个域的域名服务器是“dns.abc.edu”。
- 接下来的两行我们使用 A 命令来指定域名与 IP 地址的对应关系。我们将 Web 服务器的域名 www.abc.edu 与其 IP 地址 202.101.55.1 对应起来；将计算机系的域名 computer.abc.edu 与其 IP 地址 202.101.55.2 对应起来。
- 在第 5 行，我们使用了 CNAME 命令为 computer.abc.edu 指定了一个别名：cs.abc.edu。
- 在第 6 行，我们使用 MX 记录为 abc.edu 设置其 E-Mail 服务器。

【问题 3】

nslookup 命令的功能是查询域名服务器中的数据资料。下例就是使用它来测试域名服务器是否架设成功，其中粗体字代表要输入的内容。

```
# nslookup
Default server:dns.abc.edu
Address:202.101.55.55                ；能出现这些信息代表成功
> computer
server:dns.abc.edu
Address:202.101.55.2                  ；正确地解析出 computer.abc.edu 的 IP 地址
```