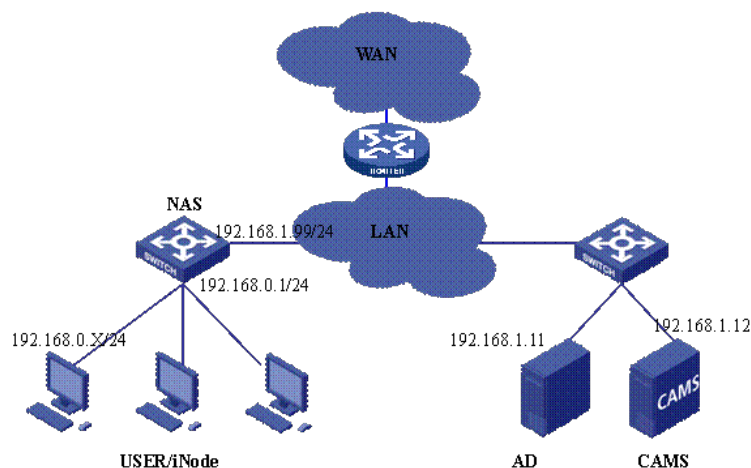


## CAMS与AD配合做域统一认证的典型配置

### 一、组网需求:

支持802.1X的交换机; CAMS服务器; Microsoft Active Directory; iNode客户端。

### 二、组网图:



设备说明:

NAS: S3952

CAMS V2.1 R0121SP1

Microsoft Active Directory 5.2

iNode V2.4-R0213

### 三、配置步骤:

前提条件是CAMS, AD, NAS, User均路由可达。

NAS可以采用802.1X认证或者Portal认证, 这里已 802.1X认证为例。

#### 1. 配置NAS

# 配置Radius服务器

```
[S3952]radius scheme h3c
[S3952-radius-h3c]server-type huawei
[S3952-radius-h3c]primary authentication 192.168.1.12 1812
[S3952-radius-h3c]primary accounting 192.168.1.12 1813
[S3952-radius-h3c]key authentication test
[S3952-radius-h3c]key accounting test
[S3952-radius-h3c]user-name-format without-domain
```

# 配置认证域

```
[S3952]domain h3c
[S3952-domain-h3c]radius-scheme h3c
[S3952]domain default enable h3c
```

# 配置VLAN

```
[S3952]Vlan 2
[S3952-vlan2]Port interface GigabitEthernet1/1/1 to GigabitEthernet1/1/4
[S3952]Interface vlan 2      \管理Vlan
[S3952-Interface-vlan-2]ip add 192.168.1.99 255.255.255.0
[S3952]Interface vlan 1      \用户Vlan
[S3952-Interface-vlan-1]ip add 192.168.0.1 255.255.255.0
```

# 启动802.1X认证

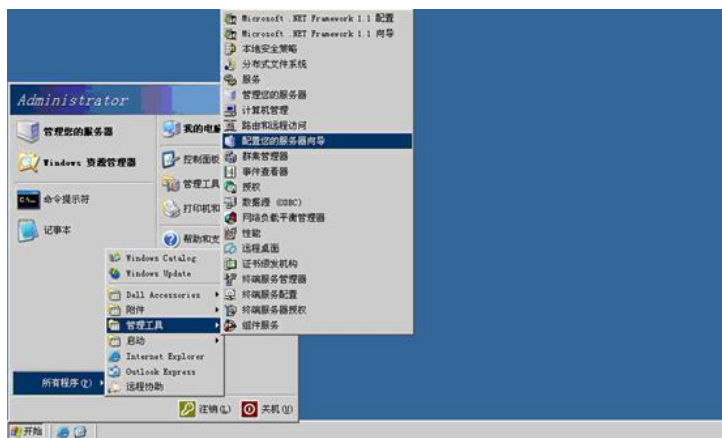
```
[S3952] dot1x
[S3952] dot1x authentication-method pap
[S3952] dot1x interface Ethernet 1/0/1 to Ethernet 1/0/48
```

注：这里只是列出了802.1X的所有必须的配置，还有一些高级选项可以自行配置，如version check, accounting on等。

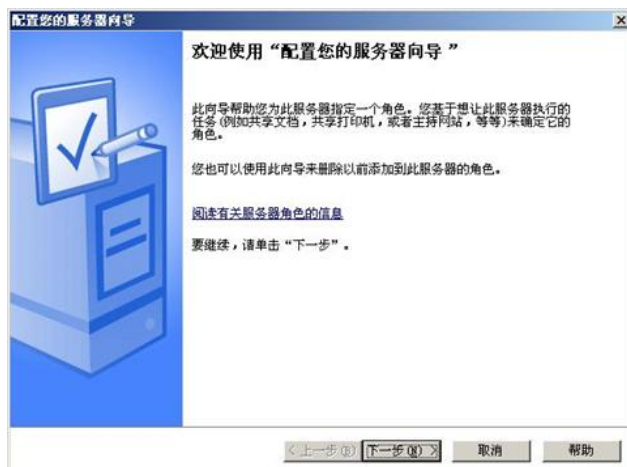
## 2. 安装AD

Windows 2000 server和windows server 2003都带有Active Directory，这里以windows server 2003为例说明AD的安装过程。

- 1). 首先为服务器配置正确的IP地址并连接网络。
- 2). 选择“开始->所有程序->管理工具->配置您的服务器向导”



- 3). 在欢迎界面点击“下一步”



- 4). 直接点击“下一步”



- 5). 会出现如下进度框



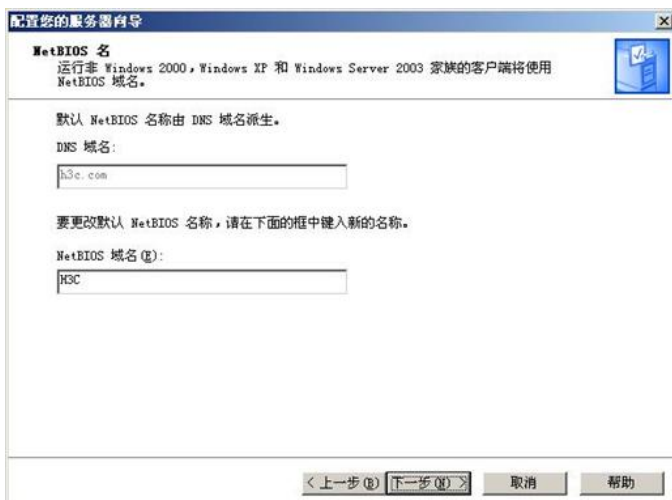
6). 选中“第一台服务器的典型配置”，点击下一步



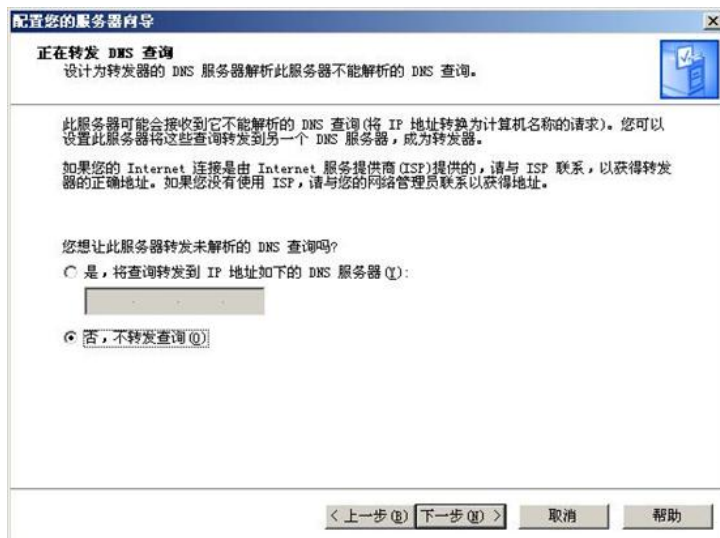
7). 在Active Directory域名一栏输入AD的域名，例如：“h3c.com”，然后点击“下一步”



8). 输入NetBIOS域名（推荐采用默认值），然后点击“下一步”



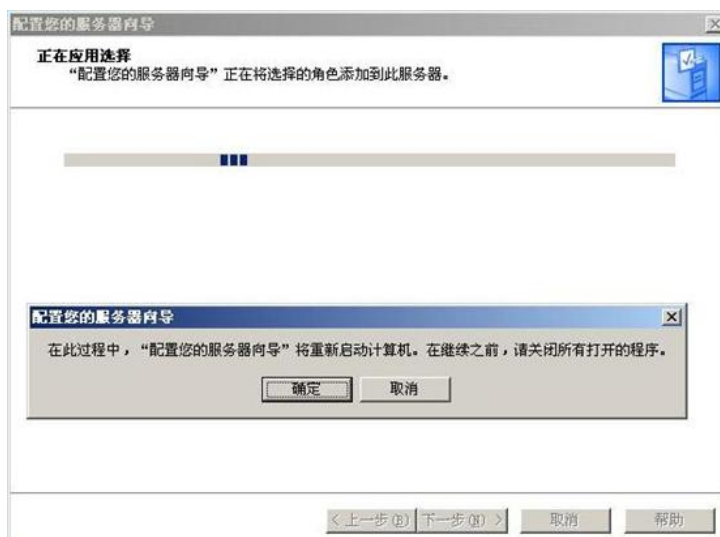
9). 选择“否，不转发查询”，点击“下一步”



10). 确认选项正确后点击“下一步”



11). 点击“确定”，开始服务器配置

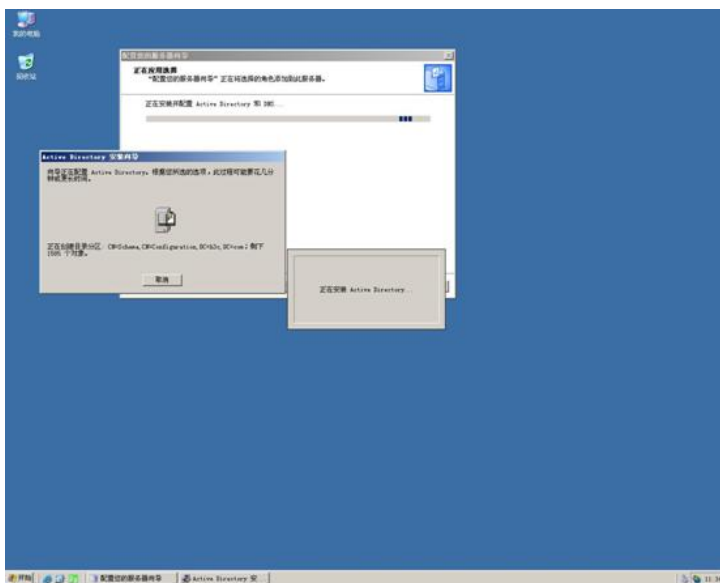


12). 放入操作系统光盘后，点击“确定”

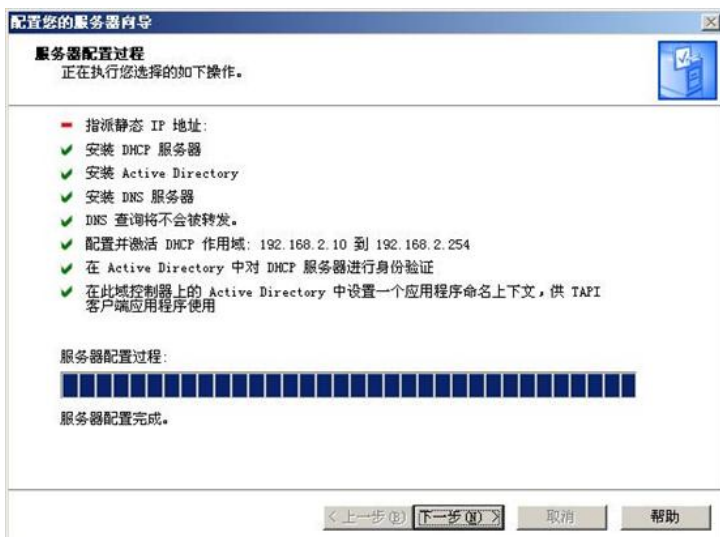




13). 配置过程当中会重新启动操作系统，无需人工干预，当下一次登陆系统后会继续完成域控制器的配置



14). 点击“下一步”

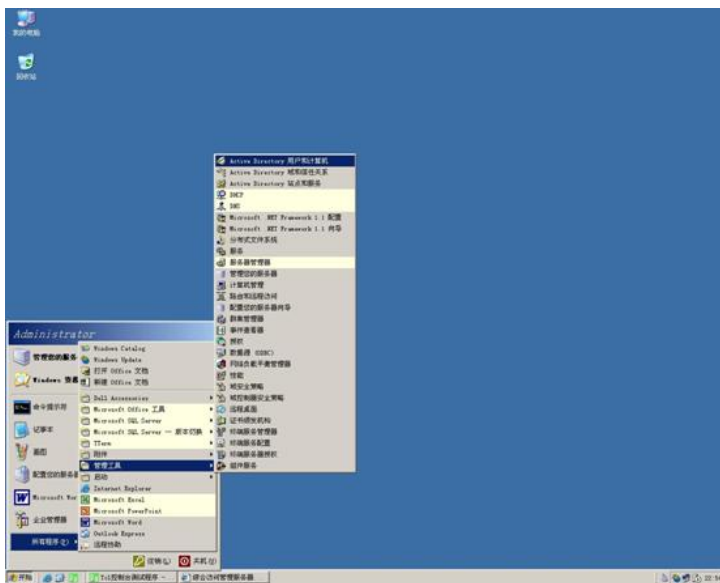


15). 点击“完成”，至此域控制器安装完毕

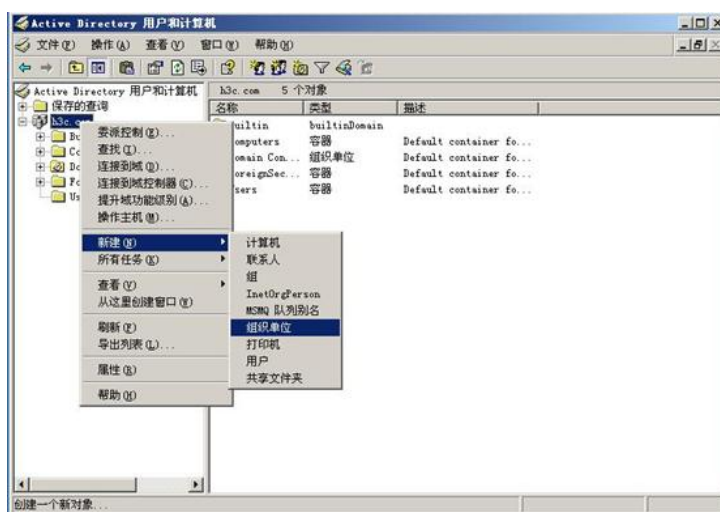


### 3. 配置AD

- 1). 配置域用户, 选择“开始->所有程序->管理工具->Active Directory用户和计算机”



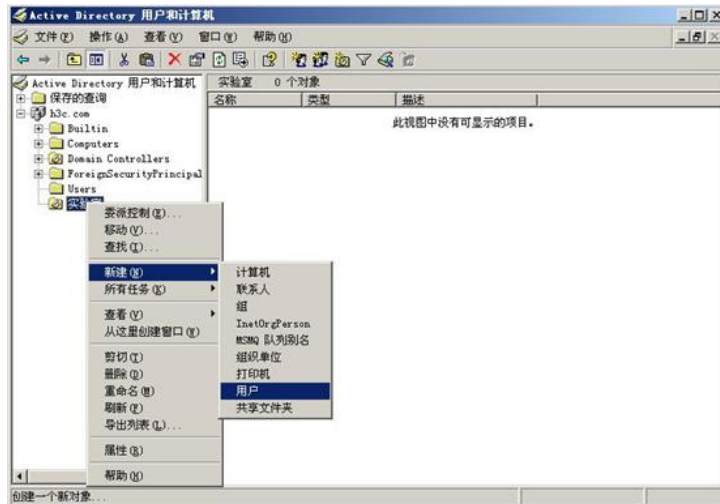
- 2). 右键菜单服务器图标“h3c.com”, 选择“新建->组织单位”



- 3). 填写组织单位名称, 中英文皆可



4). 右键菜单刚才新建的组织单位，选择“新建->用户”



5). 填写用户相关信息，用户姓名中英文皆可，登陆名务必填写英文

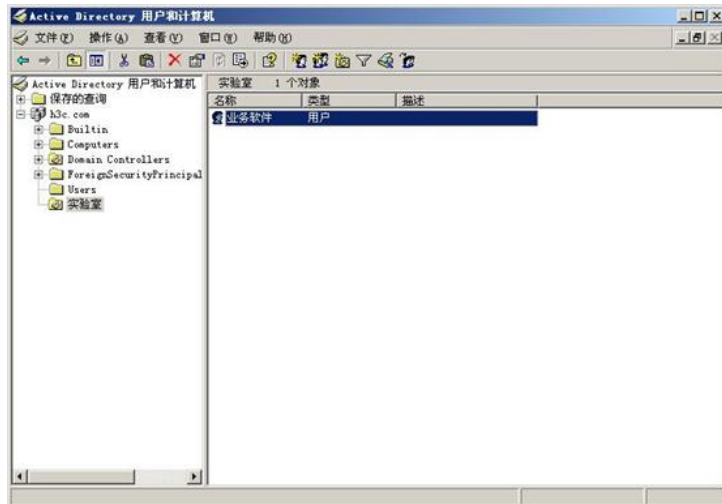


6). 创建密码，由于Windows 2003的域用户缺省密码策略，创建密码时需保证一定的复杂性。例子中创建为“h3c.com”，同时选中“用户不能更改密码”和“密码永不过期”





7). 单击“完成”，用户创建完毕，重复如上步骤，创建多个用户。



#### 4. 配置CAMS

1). 配置接入设备参数：系统管理>>系统配置>>接入设备配置

这里必须将NAS的上行端口（靠近CAMS的端口）地址添加到起始地址和结束地址之间。共享密钥和端口必须与设备的配置一致。



2). 配置LDAP服务器：组件管理>>LDAP组件>>LDAP服务器管理

这里的Base DN就是指所要同步AD中目录的范围，即CAMS只同步该Base DN路径下（包含所有子目录）的所有用户。若Base DN设置为根域h3c.com则会同步该AD中的所有用户。

管理员DN指具有查询权限的AD中的用户，可以与Base DN不在同一目录。

管理员DN和BaseDN的命名规则为：从左到右，依次从最小子目录到根目录，中间用逗号隔开。根目录前缀为dc=，原始目录（如users）和用户名（chenning）前缀为cn=，新建的目录前缀为ou=，用户名前缀。

对于AD服务器，用户名属性建议修改为saAccountName



LDAP组件 >> LDAP服务器管理 >> 修改LDAP服务器信息

### 修改LDAP服务器信息

\* 服务器名称: 192.168.1.11      \* 服务器版本: 3  
 \* 服务器IP地址: 192.168.1.11      \* 端口: 389  
 \* 服务器类型: 通用LDAP服务器  
 \* Base DN: ou=121, dc=h3c, dc=com  
 \* 自动连接间隔时长: 5 分钟      ☒ 是否连接服务器  
 \* 管理员DN: cn=chenming, ou=pyerj, ou=121, dc=h3c, dc=com  
 \* 管理员密码: \*\*\*\*\*      \* 是否需要实时认证: 否  
 \* 用户名属性名称: sAMAccountName      \* 用户密码属性名称: userPassword  
 \* 备用服务器IP地址:      ☒ 启用主服务器      ☐ 启用备用服务器  
☐ 从备用服务器自动切换回主服务器      切换间隔时间: 24 小时

确定 取消 帮助

3). 同步测试: 在LDAP服务器管理中选择建立的LADP服务器, 点击行末的<同步>, 若设置正确, 会出现同步成功的提示。

LDAP服务器管理

服务器名称: 服务器IP地址: 查询

增加 删除 全选 清除 重置 帮助

共有 2 条记录, 15 条记录/页 第1页/共1页 << 上一页 下一页 >>

| 服务器名称                                 | 服务器版本 | 服务器IP地址      | 查询 | 修改 | 绑定用户管理 | 同步 |
|---------------------------------------|-------|--------------|----|----|--------|----|
| <input type="checkbox"/> 192.168.1.11 | 3     | 192.168.1.11 | 查询 | 修改 | 绑定用户管理 | 同步 |
| <input type="checkbox"/> 1212         | 3     | 192.168.0.13 | 查询 | 修改 | 绑定用户管理 | 同步 |

<< 上一页 下一页 >>

4). 配置LDAP同步配置: 组件管理>>LDAP组件>>LDAP同步配置>>增加

出现如下的配置选项, 选择LDAP服务器, 配置过滤条件。对于AD, 建议过滤条件配置为: (&(distinguishedName=\*)(userPrincipalName=\*)。该过滤条件的意义是选出同时具有distinguishedName和userPrincipalName属性的用户。

LDAP组件 >> LDAP同步配置 >> 增加配置

### 增加配置

\* 配置名称: test      LDAP服务器: 192.168.1.11  
 \* 同步帐号类型: 帐号用户      过滤条件: (&(distinguishedName=\*)(userPrincipalName=\*))  
 \* 配置状态: 有效      ☒ 自动同步  
☒ 同步新增帐号

下一步 返回 帮助

点击下一步选择个列的属性, 建议如下图配置, 再选择相关的服务和计费方式。由于AD中的用户密码加密不可逆, 不能同步到CAMS中, 用户每次都会到AD中认证, 所以这里的CAMS本地密码可以任意设置。

LDAP组件 >> LDAP同步配置 >> 修改配置

### 修改配置

\* 帐号名: sAMAccountName      用户密码: 不从LDAP服务器同步  
 \* 用户姓名: displayName      密码确认: \*  
 \* 联系方式: name      证件号码: \*  
 \* 帐号类型: 预付费帐号      Email地址: userPrincipalName  
 \* 预付费金额: 不从LDAP服务器同步      0 元  
 \* 帐号失效时间: 不从LDAP服务器同步      不限

设备IP地址:      端口号:      用户IP地址:      修改密码/充值: 不限  
 VLAN ID:      最大闲置时长: 分钟  
 网卡MAC地址:      登录提示信息: 不从LDAP服务器同步

| 选择                                  | 服务名称 | 服务描述 | 计费策略 | 服务后缀 |
|-------------------------------------|------|------|------|------|
| <input checked="" type="checkbox"/> | xx   |      | 不计费  |      |

5). 同步用户: 在LDAP同步配置中选择同步配置, 点击行尾的<同步>, 则CAMS系统会自动同步AD中的所有Base DN中的用户到CAMS中。若同步成功会出现“同步LADP服务器用户成功”的提示。

LDAP同步配置

配置名称: \* LDAP服务器: 不限 配置状态: 不限 查询

增加 删除 定时设置 重置 帮助

共有2条记录, 8 条记录/页 第1页/共1页 << 上一页 下一页 >>

| 配置名称                          | LDAP服务器 | 配置状态 | 自动同步 | 查询 | 修改 | 同步用户管理 | 同步 |
|-------------------------------|---------|------|------|----|----|--------|----|
| <input type="checkbox"/> test | 1212    | 有效   | 是    | 查询 | 修改 | 同步用户管理 | 同步 |
| <input type="checkbox"/> 1213 | 1212    | 有效   | 是    | 查询 | 修改 | 同步用户管理 | 同步 |

<< 上一页 下一页 >>

同步成功后会在这里的<同步用户管理>和用户管理>>帐号用户中发现 LDAP用户。

LDAP同步配置 (1213) 所同步的用户管理

帐号名:  Email地址:

用户状态: 不限

共有 2 条记录, 15 条记录/页, 第1页/共1页 << 上一页 下一页 >>

| 帐号名                          | 帐号类型  | 用户姓名 | Email地址     | 同步时间                | 用户状态 |
|------------------------------|-------|------|-------------|---------------------|------|
| <input type="checkbox"/> fxy | 预付费帐号 | fen  | fxy@h3c.com | 2007-01-14 19:33:18 | 存在   |
| <input type="checkbox"/> bin | 预付费帐号 | chen | bin@h3c.com | 2007-01-14 19:33:18 | 存在   |

<< 上一页 下一页 >>

用户管理 >> 帐号用户 >> 帐号维护

修改 | 出帐 | 缴费 | 暂停 | 黑名单 | 更改付费类型 | 强制下线 | 在线删除 | 时间补追 | 帐户 | 帮助 | 返回

帐号信息 | 上网明细 | 用户帐单 | 缴费记录 | 认证失败日志 | 安全日志

帐号: fxy

### 帐号用户信息

|                           |            |               |                 |
|---------------------------|------------|---------------|-----------------|
| 帐号名                       | fxy        | 帐号类型          | 预付费帐号           |
| 帐号状态                      | 正常         | 帐号余额          | 0.00 元          |
| 用户姓名                      | fen        | 证件号码          |                 |
| 启用密码控制策略                  | 否          | 下次登录须修改密码     | 否               |
| 联系方式                      | fen        | Email地址       | fxy@aaa.bbb.ccc |
| 创建时间                      | 2007-01-14 | 帐号失效时间        | 不限              |
| 设备IP地址                    |            | 端口号           |                 |
| VLAN ID                   |            | 是否绑定多IP、MAC地址 | 否               |
| 用户IP地址                    |            | 网卡MAC地址       |                 |
| 在线数量限制                    | 1          | 最大闲置时长        | 不限              |
| 在线状态                      | 不在线        | 修改密码/充值       | 不限              |
| 登录提示信息                    |            |               |                 |
| LDAP服务器认证 (LDAP服务器中存在此帐号) |            | 服务器名称         | 1212            |

**已申请的服务信息:**

| 服务名 | 服务描述 | 计费策略 | 服务后缀 | 详细信息                              |
|-----|------|------|------|-----------------------------------|
| vv  |      | 不计费  |      | <input type="button" value="查询"/> |

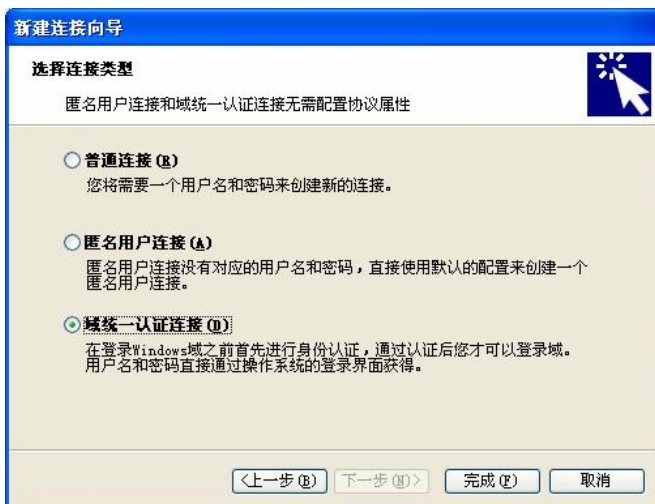
至此, CAMS与AD同步完成, 用户可以采用同步过来的用户进行LDAP认证。若需要进行域统一认证, 还需进行如下两步配置:

## 5. 配置客户端

1). 在iNode客户端中点击<新建>创建域统一认证了连接



2) 选择基本的认证方式, 本例中为802.1X认证, 再选择<域统一认证连接>

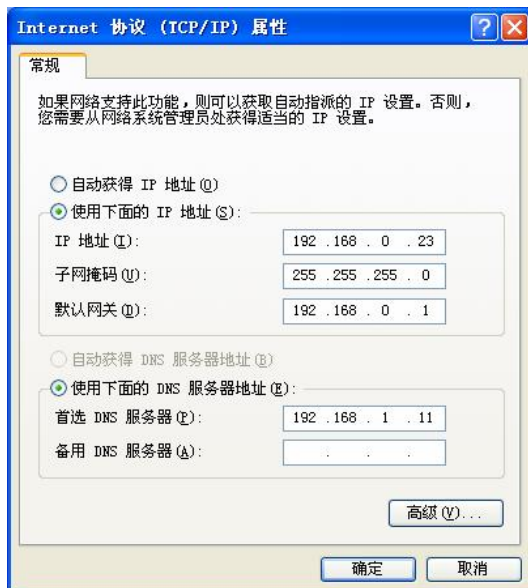


3) 然后会在iNode中发现新的域统一认证连接, 再在操作>>配置客户端运行方式 中选择启动域统一认证。



## 6. 配置用户电脑

1) 设置PC的网络连接，配置正确的DNS服务器。本例中DNS服务器和AD在同一台服务器上。



2) 将PC加入域：在我的电脑>>属性>>计算机名>>更改 中输入域名，再输入域管理员的用户名和密码，用户就可以加入到域中了。



重启PC，至此域统一认证配置完毕。

## 四、预期效果：

在PC登陆系统时，使用之前创建的域用户并选择登陆到域



点击确定后，会在登陆窗口的右侧出现“正在进行域统一认证，请等待”的提示，之后成功登陆。若在CAMS中配置了EAD检查，则登陆到系统后，iNode还会对系统进行安全检查，并采取相关策略。

##### 五、配置关键点：

1. NAS上802.1x的认证模式必须为pap。
2. CAMS的服务和NAS中配置的默认域都必须采用AD中域的NetBIOS名称，默认情况下是域的第一部分，例如h3c.com，则如上两处都应设置为h3c。