

文档介绍:

- 作者 : gavin
- 电子邮箱 : gavin.zhou@gmail.com
- MSN : [gavin\\_zhm@msn.com](mailto:gavin_zhm@msn.com)
- 博客地址 : <http://blog.yepn.net>
- Wiki 地址 : <http://wiki.yepn.net>
- 建立日期 : 2008 年 07 月 15 日
- 版本 : 0.2
- 版权说明 : 本文基于创作共用约定, 内容归作者所有, 欢迎大家转载, 但要请保留作者的完整信息和出处, 谢谢!

本文参考:

Extreme Networks Technical Brief 文档号: TBLDAPEnviron\_1370

<http://www.nabble.com> 讨论列表也给了我很大的帮助, 很多关于 Freeradius 和 OpenLDAP 保存数据的概念都在此讨论区中弄明白的。对于文中所涉及的 radius 概念或是一些名词请借助 google 帮助学习, 文中没有更详细的解释。

关于:

公司原用认证服务器为 Soliton Net'Attest EPS, 知道为什么 EPS 证书一直不能正确导入到 VISTA 中, 这点是从厂商方面得到的证明, 不知道是什么特别的原因。再加上 EPS 更换产品的空白服务器, 让我感觉有些郁闷, 所以公司决定更换现在公司的认证系统, 包括 DHCP 服务器。

这是到公司后第二个自己独立完成的比较完整的公司网络改造过程, 记录一下方便自己以后查阅, 也希望能为准备用 Freeradius 认证和 OpenLDAP 的朋友提供一些有用的信息。

鉴于网络上流行的一些关于 Freeradius+OpenLDAP+PEAP 认证的一些资料都比较旧, 所以在测试的时候 Freeradius 采用最新的 Freeradius 2.0.5 版本。由于 2.0 以前的版本配置文件格式和文件出入比较大, 所以使用 Freeradius2.0 以前版本的朋友在配置的时候需要特别注意。CentOS 下用 yum 安装后为 1.1.7 版。

目的:

Freeradius 在公司使用不是做为 WLAN 接认证, 而是做为 LAN 接入认证用。先要通过认证后才能通论 DHCP 获得 IP, 而且会因为 Freeradius 返回的信息为 Client 划分 VLAN ID 以及访问控制。

感谢:

首先是老婆对我生活上的细心照顾，才能让我有更多的时间学习和测试来完成这份文档。  
Freeradius 的测试大部分在下班之后才能进行，所以每天晚上回家都很晚，老婆也一直等到我回家后才吃晚饭，另外要感谢远在国内的父母，生活在异乡的我们正因为有你们的牵挂，我们会更加努力。

服务器环境:

CentOS 5.1 Linux blackduck 2.6.18-53.el5

#安装时不含任何安装包

yum -y update

#全部更新升级

openssl.i686 0.9.8b-10.el5

openssl-devel.i386 0.9.8b-10.el5

openldap.i386 2.3.27-8.el5\_2.4

openldap-clients.i386 2.3.27-8.el5\_2.4

openldap-devel.i386 2.3.27-8.el5\_2.4

openldap-servers.i386 2.3.27-8.el5\_2.4

对于 OpenLDAP 的配置可以参看我以前的文档《Samba+LDAP+LAM 管理工具应用》一文件中 OpenLDAP 的配置

Freeradius 安装:

下载源码包

#wget <ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.0.5.tar.bz2>

#tar -jxvf freeradius-server-2.0.5.tar.bz2

#cd freeradius-server-2.0.5

#!/configure --with-openssl --with-openssl-includes=/usr/include/openssl/ \

--with-openssl-libraries=/usr/lib/openssl/

#configure 文件中说明配置支持 OpenSSL 但是装完后运行 EAP 支持的时候会报错。说手动没有支持 OpenSSL，所以此处给出 OpenSSL 的路径。

#make && make install

安装后可以直接执行进行测试

#radiusd -Xf (2.0 以前版本为-AXf X 为 Debug 模式 f 为不运行在 daemon 状态下)

安装后可以通过 radtest 测试

```
#radtest admin password localhost 0 testing123
```

返回信息如下说明测试成功，此步很重要，安装后第一步应该测试一下 Freeradius 是不是可以正常运行，再进行下面的配置。

```
Sending Access-Request of id 85 to 127.0.0.1 port 1812
```

```
    User-Name = "admin"
```

```
    User-Password = "password"
```

```
    NAS-IP-Address = 127.0.0.1
```

```
    NAS-Port = 0
```

```
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=85, length=20
```

测试通过后配置 Freeradius，配置文件在/usr/local/etc/raddb 下，2.0 之后的配置对于对认证的支持方式采用模块化，所以修改起来也很方便。配置文件忽略注释项

主配置文件 radiusd.conf:

```
#vi radiusd.conf
```

此文件只是把 log 选项中的认证 log 信息打开了其他部分没有做任何修改

```
log {  
    destination = files  
    file = ${logdir}/radius.log  
    syslog_facility = daemon  
    stripped_names = no  
    auth = yes  
    auth_badpass = no  
    auth_goodpass = no  
}
```

2.0 以后的版本，所以有的认证模块都保存在/usr/local/etc/raddb/modules 目录下  
用户认证配置文件

ldap 认证模块修改:

```
#vi ldap
```

比较重要的为前四行, 设置你 LDAP 服务器的配置, 如何过滤 User-Name 的字段, 以前你 LDAP 的搜索域, 如果你的 LDAP 需要权限控制才能访问, 请修改配置文件中被注释的两行。

```
ldap {  
    server = "localhost"  
    #identity = "cn=admin,o=My Org,c=UA"  
    #password = mypass  
    basedn = "dc=yepn,dc=net"  
    filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"  
    base_filter = "(objectclass=radiusprofile)"  
    ldap_connections_number = 15  
    timeout = 4  
    timelimit = 3  
    net_timeout = 1  
    tls {  
        start_tls = no  
    }  
    dictionary_mapping = ${confdir}/ldap.attrmap  
}
```

红色文件比较重要, 这个表示在检索 LDAP 时查找的字段和返回的信息值, 对于 Client 的网络配置部分都在这文件中表明, 后文会详细说明。

Freeradius 字典文件修改:

通过 LDAP 认证时的返回值全部都要在 Freeradius Dictionary 中说明, 否则不能被 Freeradius 识别。

Dictionary 配置文件保存在/usr/local/etc/raddb 目录下

```
#cat dictionary | grep -v "#"
```

```
$INCLUDE /usr/local/share/freeradius/dictionary
```

Dictionary 文件分部保存在/usr/local/share/freeradius/文件中

```
#cat dictionary | grep -v "#"
```

```
$INCLUDE dictionary.compat
```

```
$INCLUDE dictionary.rfc2865
```

```
$INCLUDE dictionary.rfc2866
```

```
$INCLUDE dictionary.rfc2867
```

```
$INCLUDE dictionary.rfc2868
```

```
$INCLUDE dictionary.rfc2869
```

```
$INCLUDE dictionary.rfc3162
```

```
$INCLUDE dictionary.rfc3576
```

```
$INCLUDE dictionary.rfc3580
```

以下略

我的 NAS 用的是 Extreme network summit X450 交换机, 需要修改的字典文件为 dictionary.extreme, 如果你使用的是其他 NAS 可以修改相应的字典文件, 或是自己创建一个字典文件也可以。

加入下面两行定义

```
ATTRIBUTE Extreme-Netlogin-Extended-Vlan 211 string
```

```
ATTRIBUTE Extreme-Security-Profile 212 string
```

字典修改后, 修改 ldap.attrmap 让 LDAP 可以返回 extreme 认证用的字段。配置文件保存在/usr/local/etc/raddb/下

添加以下属性

```
replyItem Tunnel-Type radiusTunnelType
```

```
replyItem Tunnel-Medium-Type radiusTunnelMediumType
```

```
replyItem Tunnel-Private-Group-Id radiusTunnelPrivateGroupId
```

```
replyItem Extreme-Security-Profile radiusExtremeSecurityProfile
replyItem Extreme-Netlogin-Vlan-Tag radiusExtremeNetloginVlanTag
replyItem Extreme-Netlogin-Extended-Vlan radiusExtremeNetloginExtendedVlan
```

另外需要把 NT-Password 字段修改如下，如果你希望 radius 用户使用 samba 的密码，可以不用修改这部分，因为我希望密码分开管理，而且网络认证的密码不会发给用户，所以我用了其他的字段做为 Freeradius 的认证密码。

```
checkItem User-Password userPassword
checkItem NT-Password radiusUserPassword
```

这部分再次说明一下：

如果是想通过 MAC 方式认证，比如客户端是 Linux 或是 MAC 累的机器，密码验证时需要使用 userPassword 字段。

如果是用 Winxp 客户端认证的话，无论你是否使用 CA 证书，一定要用 MD4(WinNT)方式加密后再放到 radiusUserPassword 中。

另外 Windows 通过 Freeradius 认证时，密码通过 MD4(WinNT)的方式加密，所以需要储存在 LDAP 中的 radiusUserPassword 也通过 MD4 的加密方式保存，这样才能通过认证。另外，通过 ntrading 验证工具是不能验证 MD4 是否成功的需要，通过 WinXP 客户端进行验证。

配置可使用的认证方式:

修改认证方式配置文件, 目录为/usr/local/etc/raddb/sites-available

两个比较重要的文件

**default** #默认配置文件

**inner-tunnel** #认证虚拟机配置文件, 这个文件我没做仔细研究, 如果有了解的朋友希望能交流一下

**#vi default**

用户认证部分只保留了 **ldap** 和 **eap** 部分, 其他的认证用不到我注释掉了, 如果你需要其他的认证去掉相应的注释部分。

```
authorize {  
    ldap  
    eap  
}
```

验证部分保留了下面的选项, 支持 **MS-CHAP** 验证方式, **LDAP** 验证和 **EAP** 验证

```
authenticate {  
    Auth-Type MS-CHAP {  
        mschap  
    }  
    ldap  
    eap  
}
```

**authorize** 配置用户信息通过那种方式获得, **LDAP** 服务器、**Mysql** 服务器、**Unix** 系统帐号还是 **files** 文件。

**authenticate** 配置验证方式, 密码的格式等等

除上述部分外未作任何修改。

配置 eap 认证方式:

修改内容如下

```
#cat eap.conf|grep -v "#"
```

```
eap {
    default_eap_type = peap
    timer_expire      = 60
    ignore_unknown_eap_types = no
    tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_password = cyberstep
        private_key_file = ${certdir}/server.pem
        certificate_file = ${certdir}/server.pem
        CA_file = ${cadir}/ca.pem
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random
        fragment_size = 1024
        include_length = yes
        make_cert_command = "${certdir}/bootstrap"
    }
    peap {
        default_eap_type = mschapv2
    }
    mschapv2 {
    }
}
```

主要修改部分为将 eap 的默认认证方式改为 peap，原为 MD5，另外添加对 tls 的支持，希望客户端和 Freeradius 通信时采用证书加密。另外将 peap 默认认证方式改为 mschapv2。

Freeradius 生成证书

Freeradius2.0.5 含有证书制作脚本，只要 OpenSSL 的路径正确，Freeradius 可以自己制作证书，不过需要修改一下相关的信息，文件在 /usr/local/etc/raddb/certs 目录下，需要修改的文件为 ca.cnf server.cnf client.cnf

```
#more ca.cnf
```

```
default_days          = 3650
```

```
default_crl_days     = 3650
```

```
[certificate_authority]
countryName          = JP
stateOrProvinceName = Tokyo
localityName         = Shibuya
organizationName     = Yepn Inc.
emailAddress         = zhou@yepn.net
commonName           = "yepn Certificate Authority"
```

其中比较重要的是这几部分，`days` 问题你也希望你的证书只能用一个月，或是一年的时间，相信网管都不喜欢这样，所以我把时间设的长一点改成了 10 年。下面的 `certificate_authority` 是你证书的相关信息这个是方便查询证书的出处，不清楚的地方请找 `OpenSSL` 的资料看一下，另外在 `cert` 文件夹中有 `Makefile` 文件，我也小修改了一下，不知道为什么前面对于 `ca.cnf` 日期的修改在 `cn.cnf` 中不生效，所以我只好把命令行那边加上一个 `-days 3650` 修改后如下

```
#more Makefile
```

```
openssl req -new -x509 -days 3650 -keyout ca.key -out ca.pem -config ./ca.cnf
```

因为 `OpenSSL` 自己也不是特别明白，所以没办法讲的更细了，希望明白的朋友指点一下。

这样生成后的 `ca.der` 证书可以导入到 `Winxp` 中。

到此为止 `Freeradius` 的配置就完成了，可以通过 `radiusd -Xf` 测试一下 `radius` 的配置是否正确。可以通过 `radtest` 命令来验证一下 `Freeradius` 能验证。

OpenLDAP 配置:

因为 LDAP 中加入了对于 radius 属性的支持, 所以需要修改 OpenLDAP 配置文件。

复制 radius.schema 文件到 openLDAP 的 schema 目录下

```
#cp /usr/local/share/doc/freeradius/examples/openldap.schema
/etc/openldap/schema/radius.schema
```

因为上面刚刚新加的几个 attribute 的值在这个标准的 radius.schema 文件中没有, 所以需要自己定义几个新的 attribute 的值

添加内容如下:

```
attributetype
```

```
( 1.3.6.1.4.1.3317.4.3.1.61
```

```
NAME 'radiusExtremeSecurityProfile'
```

```
DESC "
```

```
EQUALITY caseIgnoreIA5Match
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
```

```
)
```

```
attributetype
```

```
( 1.3.6.1.4.1.3317.4.3.1.62
```

```
NAME 'radiusExtremeNetloginVlanTag'
```

```
DESC "
```

```
EQUALITY caseIgnoreIA5Match
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
```

```
)
```

```
attributetype
```

```
( 1.3.6.1.4.1.3317.4.3.1.63
```

```
NAME 'radiusExtremeNetloginExtendedVlan'
```

```
DESC "
```

```
EQUALITY caseIgnoreIA5Match
```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
```

```
)
```

```
attributetype
```

```
( 1.3.6.1.4.1.3317.4.3.1.66
```

```
NAME 'radiusUserPassword'
```

```
DESC 'radiusUserPassword'
```

```
SUP userPassword
```

```
)
```

OpenLDAP schema 修改:

对于 OpenLDAP schema 的格式问题不在这里作更多说明, 有很多文章解决如果编写自己的 schema 文件请参阅。只在这里说明一点对于 radiusUserPassword 部分的定义, 我让 radiusUserPassword 继承 userPassword 的特性, 如果需要修改的朋友可以自己改成其他属性。

最后, 别忘记在你的 objectclass 里添加刚刚加的属性

objectclass

( 1.3.6.1.4.1.3317.4.3.2.1

NAME 'radiusprofile'

SUP top AUXILIARY

DESC "

MUST cn

MAY ( radiusArapFeatures \$ radiusArapSecurity \$ radiusArapZoneAccess \$  
radiusAuthType \$ radiusCallbackId \$ radiusCallbackNumber \$  
radiusCalledStationId \$ radiusCallingStationId \$ radiusClass \$  
radiusClientIPAddress \$ radiusFilterId \$ radiusFramedAppleTalkLink \$  
radiusFramedAppleTalkNetwork \$ radiusFramedAppleTalkZone \$  
radiusFramedCompression \$ radiusFramedIPAddress \$  
radiusFramedIPNetmask \$ radiusFramedIPXNetwork \$  
radiusFramedMTU \$ radiusFramedProtocol \$  
radiusCheckItem \$ radiusReplyItem \$  
radiusFramedRoute \$ radiusFramedRouting \$ radiusIdleTimeout \$  
radiusGroupName \$ radiusHint \$ radiusHuntgroupName \$  
radiusLoginIPHost \$ radiusLoginLATGroup \$ radiusLoginLATNode \$  
radiusLoginLATPort \$ radiusLoginLATService \$ radiusLoginService \$  
radiusLoginTCPPort \$ radiusLoginTime \$ radiusPasswordRetry \$  
radiusPortLimit \$ radiusPrompt \$ radiusProxyToRealm \$  
radiusRealm \$ radiusReplicateToRealm \$ radiusServiceType \$  
radiusSessionTimeout \$ radiusStripUserName \$  
radiusTerminationAction \$ radiusTunnelClientEndpoint \$  
radiusProfileDn \$  
radiusSimultaneousUse \$ radiusTunnelAssignmentId \$  
radiusTunnelMediumType \$ radiusTunnelPassword \$  
radiusTunnelPreference \$  
radiusTunnelPrivateGroupId \$ radiusTunnelServerEndpoint \$

```
radiusTunnelType $ radiusUserCategory $ radiusVSA $  
radiusExpiration $ dialupAccess $ radiusNASIpAddress $  
radiusReplyMessage $ radiusExtremeSecurityProfile $  
radiusExtremeNetloginVlanTag $ radiusExtremeNetloginExtendedVlan $  
radiusUserPassword)  
)
```

看似很复杂，其实 schema 的说明很简单，多找些资料看看会明白很多，我这里给出了全部的 objectclass 的值。

radius.schema 文件修改后，别忘了修改 slapd.conf 配置文件加载 radius.schema 文件，让 OpenLDAP 能识别这些新属性。

加入以下内容

```
include /etc/openldap/schema/radius.schema
```

重启 OpenLDAP

```
#service ldap restart
```

到这里 OpenLDAP 的配置就结束了，可以说 Freeradius+OpenLDAP+PEAP 认证的配置已经完成了一大部分了，最后就是 OpenLDAP 数据的添加。

对于批量的 OpenLDAP 数据库修改不放在这里，需要的朋友请到我的 Wiki 上查找，可以实现大批量的 LDAP 数据修改。

一个 radius 用户的例子:

```
#cat zhou.ldif
```

```
dn: uid=zhou,ou=Users,dc=yepn,dc=net
```

```
add: objectClass
```

```
objectClass: radiusprofile
```

```
-
```

```
add: radiusSessionTimeout
```

```
radiusSessionTimeout: 43200
```

```
-
```

```
add: radiusTunnelType
```

```
radiusTunnelType: VLAN
```

```
-
```

```
add: radiusTunnelMediumType
```

```
radiusTunnelMediumType: IEEE-802
```

```
-
```

```
add: radiusTunnelPrivateGroupId
```

```
radiusTunnelPrivateGroupId: 160
```

```
-
```

```
add: radiusTerminationAction
```

```
radiusTerminationAction: RADIUS-Request
```

```
-
```

```
add: radiusExtremeSecurityProfile
```

```
-
```

```
add: radiusUserPassword
```

```
radiusUserPassword: 178DEACBFD994B3A6A67F49F420DB96A
```

格式要与我上面的相同, 如果不一样的话不能通过 ldapmodify 方式导入

```
#ldapmodify -x -D "cn=root,dc=yepn,dc=net" -w password -f zhou.ldif
```

把修改后的数据导入到 LDAP 中

```
#ldapsearch -x uid=zhou
```

我的 LDAP 支持匿名查询

以下为完整的 zhou 用户信息

```
# extended LDIF
#
# LDAPv3
# base <> with scope subtree
# filter: uid=zhou
# requesting: ALL
#

# zhou, Users, cyberstep.com
dn: uid=zhou,ou=Users,dc=yepn,dc=com
sn: zhou
givenName: zhou
gecos: System User
sambaLogonTime: 0
sambaLogoffTime: 2147483647
displayName: zhou
sambaSID: S-1-5-21-1153389650-4125104348-4025214935-3060
sambaPrimaryGroupSID: S-1-5-21-1153389650-4125104348-4025214935-2001
sambaLogonScript: logon.bat
sambaProfilePath: \\PDC-SRV\profiles\zhou
sambaHomePath: \\PDC-SRV\zhou
sambaHomeDrive: H:
sambaPasswordHistory:
0000000000000000000000000000000000000000000000000000000000000000
00000000
mail: zhou@yepn.com
shadowMax: 45
uid: zhou
cn: zhou
homeDirectory: /home/zhou
uidNumber: 1030
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

```
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
objectClass: radiusprofile
gidNumber: 500
shadowLastChange: 14027
loginShell: /bin/bash
radiusSessionTimeout: 43200
radiusTunnelType: VLAN
radiusTunnelMediumType: IEEE-802
radiusTerminationAction: RADIUS-Request
sambaDomainName: YEPN
radiusTunnelPrivateGroupId: 310
sambaAcctFlags: [XU          ]
sambaLMPassword: 44EFCE164AB921CAAAD3B435B51404EE
sambaNTPassword: 32ED87BDB5FDC5E9CBA88547376818D4
sambaPwdLastSet: 1216031836
radiusUserPassword: 3FA45A060BD2693AE4C05B601D05CA0C
userPassword::
e0NSWVBUfSQxJGNFb0N5Z2JqJHpnSXdkUmpaUzl1MkdVR0hsZ2s3YTE=
```

```
# search result
search: 2
result: 0 Success
```

```
# numResponses: 2
# numEntries: 1
```

需要说明的一点，关于 radiusUserPassword 密码为 000000，通过 mkntpwd 加密成 MD4(WinNT)格式的密码放到 LDAP 中，修改密码时也不能直接修改，需要通过 mkntpwd 生成新密码后再添加到 LDAP 中。

mkntpwd 可以在 SF.net 的网站上下载

```
#wget http://nchc.dl.sourceforge.net/sourceforge/ldaputils/mkntpwd.tar.gz
```

```
#mkdir mkntpwd
```

```
#tar -zxvf mkntpwd.tar.gz -C mkntpwd
```

```
#cd mkntpwd
```

```
#make
```

```
#!/mkntpwd -N password
```

```
8846F7EAAE8FB117AD06BDD830B7586C
```

生成密码 MD4 格式密码

Summit X450 的配置

```
#configure radius netlogin primary server 172.31.7.7 1812 client-ip 172.16.0.1 vr
```

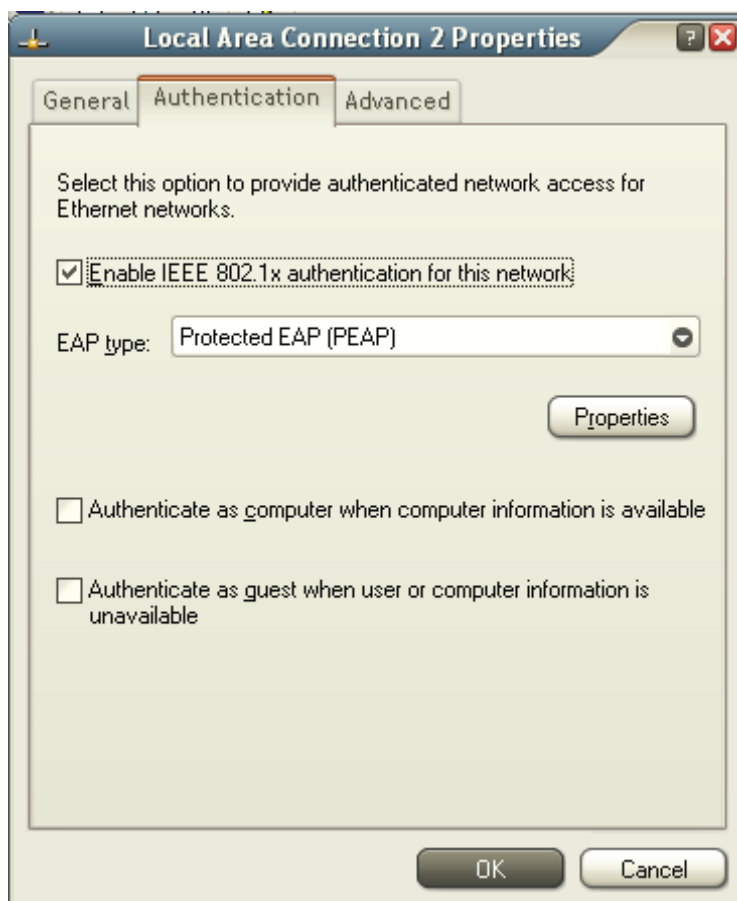
```
VR-Default
```

```
#configure radius netlogin primary shared-secret testing123
```

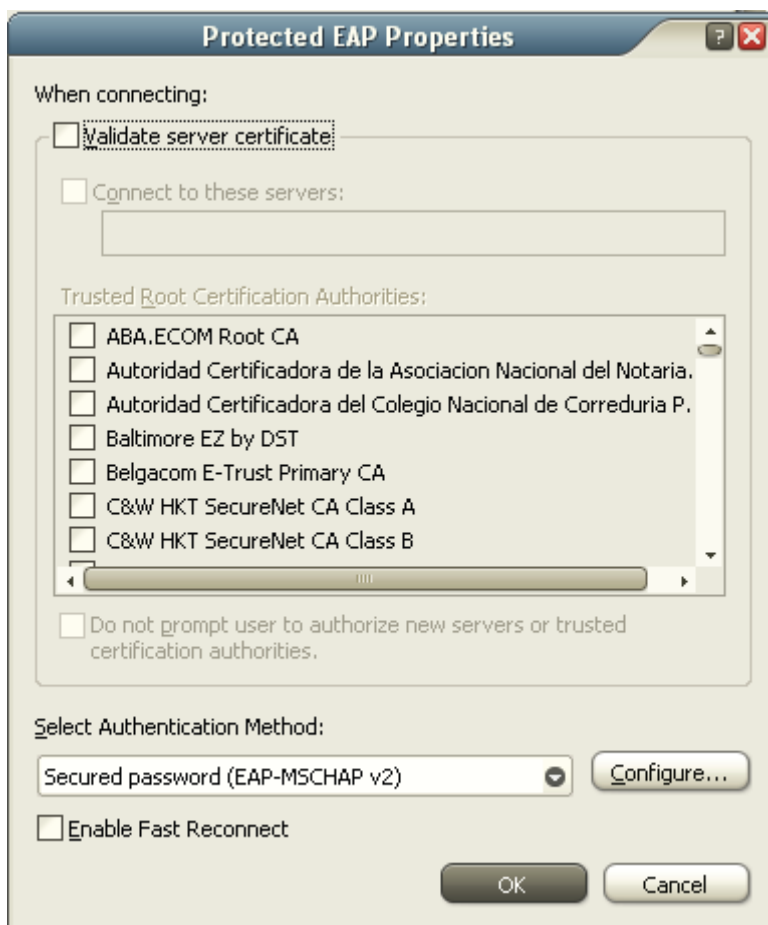
Summit 交换机因为我也了解不多，所以没办法做更多的说明。

客户端配置:

修改 WinXP 客户端配置, 网络属性中如下图修改。我的系统是日文的所以找来了一份英文的图片, 按下图修改就 OK 了。



这里没有使用 CA 证书，先测试一下能不能通过认证。



需要修改 Select Authentication Method 的 Configure 选项，把 Automatically use my Windows logon name and password 这里去掉。



祝你好运，希望能一次通过认证。