

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

DATE DE DERNIERE MISE A JOUR : 09 SEPTEMBRE 2009

INDUSTRIALISATION « 802.1X » CONFIG : 802.1X – PEAP – MSCHAPV2

PRONETIS

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

SOMMAIRE

1. ITINERANCE INTERNE	3
1.1. COMPOSANTS TECHNOLOGIQUES	3
1.2. ARCHITECTURE DE TEST	3
1.3. CONFIGURATION DU SWITCH.....	4
1.4. CONFIGURATION DU SERVEUR LINUX.....	7
1.5. INSTALLATION DE OPENSSE 0.9 .8J.....	15
1.6. SERVICE D’AUTHENTIFICATION RADIUS	15
1.7. INTEGRATION DU SERVEUR LINUX FREERADIUS DANS LE DOMAINE	18
1.8. AUTHENTIFICATION NTLM - EAP PEAP	21
1.9. SERVEUR DHCP	23
1.10. CONFIGURATION DU SUPPLICANT – POSTE DE TRAVAIL – PEAP	24
2. ANNEXES.....	26
2.1. COMMANDES DE CONFIGURATION RESEAU	26
2.2. COMMANDES DE DEBUGGING FREERADIUS	26
2.3. POUR L’INSTALLATION DE OPEN LDAP :	27

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

1. ITINERANCE INTERNE

1.1. COMPOSANTS TECHNOLOGIQUES

La solution a été choisie de manière collégiale avec l'équipe informatique.

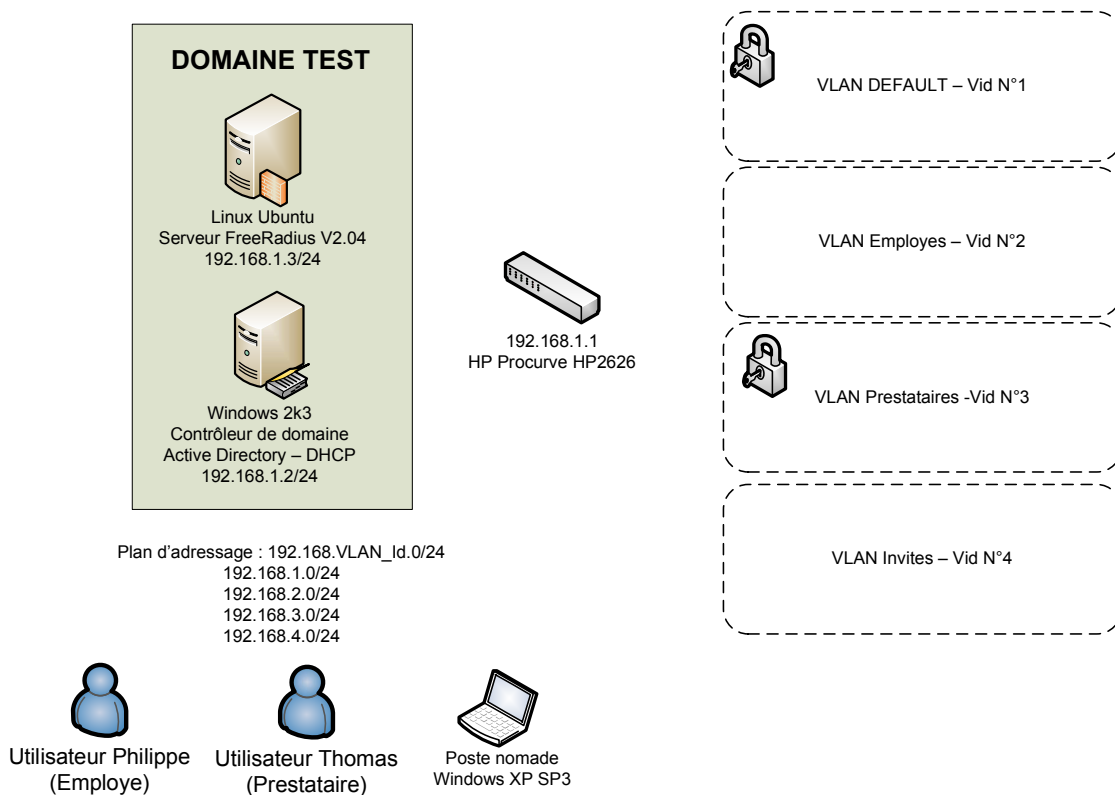
Les différentes technologies et composants retenus :

- Authentification réseau 802.1X – EAP¹ PEAP
- Serveur d'authentification réseau RADIUS
- Annuaire Active Directory Microsoft sur un contrôleur de domaine Windows
- Switch HP 2626 Procurve – switchs en place sur le réseau XXX (Version H.10.67)

Récapitulatif des composants utilisés et les versions associées

COMPOSANT	VERSION
Switch HP2626	HP2626 Version H.10.67
Serveur Windows	Serveur 2003
Serveur Linux	Ubuntu 8.10 server
VMware Serveur	V2.0.0 Build 122956
FreeRadius	V2.1.3
Samba	V3.2.3
OpenSSL	V0.9.8j

1.2. ARCHITECTURE DE TEST



¹ Extensible Authentication Protocol): EAP enables network access that supports multiple authentication methods.

Rapport Technique - Société		Restreint
Date	Auteurs	Classification
23/09/09	P.P.	D3
		Référence
		CAE-AUDIT

1.3. CONFIGURATION DU SWITCH

1.3.1. Configuration du switch HP 2626

```

; J4900B Configuration Editor; Created on release #H.10.67
hostname "SWITCH"
no web-management
web-management ssl
no telnet-server
Commande de debugging du Switch
ip ssh
interface 1
  no lacp2
exit
.....
interface 26
  no lacp
exit
vlan 1
  name "Default"
  untagged 1-26
  exit
vlan 2
  name "Employes"
  ip address 192.168.2.1 255.255.255.0
  ip helper-address 192.168.0.2
  exit
vlan 3
  name "Prestataires"
  ip address 192.168.3.1 255.255.255.0
  ip helper-address 192.168.0.2
  exit
vlan 4
  name "Invites"
  ip address 192.168.4.1 255.255.255.0
  ip helper-address 192.168.0.2
  exit

aaa authentication port-access eap-radius
radius-server key testing123
radius-server timeout 1
radius-server dead-time 1
radius-server host 172.28.32.16

```

Durcissement de l'administration des Switchs – Accès autorisés en SSL et SSH uniquement

LACP ne peut pas être active en même temps que le 802.1X

VLAN N°1 par défaut tous les équipements sont dans ce VLAN (Untagged 1 à 26)– Conseil ne pas utiliser ce VLAN pour de la production

*VLAN N°2 VLAN pour les employés de la société
Proxy ARP activé
Help-address – définit l'adresse IP du serveur DHCP de référence dans chaque VLAN
Help-address activé*

*VLAN N°3 VLAN pour les prestataires, sous-traitants de la société
Help-address activé*

VLAN N°4 Par défaut, si le supplicatant n'est pas authentifié, il est redirigé automatiquement vers ce VLAN aux accès limités

*Activation de l'authentification EAP avec un serveur RADIUS
Définition du serveur Radius et de la clé de chiffrement des échanges entre le Switch et le serveur Radius
Activation de l'authentification sur les ports 17 à 24
Dead-time permet basculer plus rapidement sur le Radius backup et donc d'attribuer le VLAN correspondant*

² Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.

Rapport Technique - Société			Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

```

aaa port-access authenticator 17-24
aaa port-access authenticator 17 auth-vid 2
aaa port-access authenticator 17 unauth-vid 3
aaa port-access authenticator 18 auth-vid 2
aaa port-access authenticator 18 unauth-vid 3
aaa port-access authenticator 19 auth-vid 2
aaa port-access authenticator 19 unauth-vid 3
aaa port-access authenticator 20 auth-vid 2
aaa port-access authenticator 20 unauth-vid 3
aaa port-access authenticator 21 auth-vid 2
aaa port-access authenticator 21 unauth-vid 3
aaa port-access authenticator 22 auth-vid 2
aaa port-access authenticator 22 unauth-vid 3
aaa port-access authenticator 23 auth-vid 2
aaa port-access authenticator 23 unauth-vid 3
aaa port-access authenticator 24 auth-vid 2
aaa port-access authenticator 24 unauth-vid 3
aaa port-access authenticator active
aaa port-access 17-24

ip routing
gvrp
dhcp-relay

```

*Lorsque l'équipement est authentifié correctement, le VLAN par défaut affecté est le N°1, sinon le N°28
Inutile avec le serveur RADIUS – utile si le serveur Radius n'est pas joignable*

Activation de l'authentification 802.1X sur le Switch

Routing : Activer le routage entre les VLAN

GVRP : création dynamique des routes

Relayage des échanges DHCP entre les clients et le serveur à partir d'autres sous-réseaux – comme cela, le serveur n'est pas (IP routing doit être activé) obligatoirement présent dans chaque VLAN

1.3.2. Commande de debugging des switchs HP

show authentication

```

172.28.32.218 - PuTTY
Test-itinerance# MAC-Auth | ChapRadius None
Invalid input: MAC-Auth
Test-itinerance# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

Access Task | Login      Login      Enable     Enable
             | Primary   Secondary  Primary    Secondary
-----+-----+-----+-----+-----+
Console     | Local     None       Local      None
Telnet      | Local     None       Local      None
Port-Access | EapRadius None       Local      None
Webui       | Local     None       Local      None
SSH         | Local     None       Local      None
Web-Auth    | ChapRadius None
MAC-Auth    | ChapRadius None

Test-itinerance#

```

show radius

```

172.28.32.218 - PuTTY
Web-Auth | ChapRadius None
MAC-Auth | ChapRadius None

Test-itinerance# show r
radius
rmon
running-config
Test-itinerance# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key : testing123

Server IP Addr  Auth Port  Acct Port  Encryption Key
-----+-----+-----+-----+-----+
172.28.32.16   1812 1813

Test-itinerance#

```

show port-access authenticator

```

172.28.32.218 - PuTTY
port-security
power-management
Test-itinerance# show port-access
Incomplete input: port-access
Test-itinerance# show port-access authenticator

Port Access Authenticator Status

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

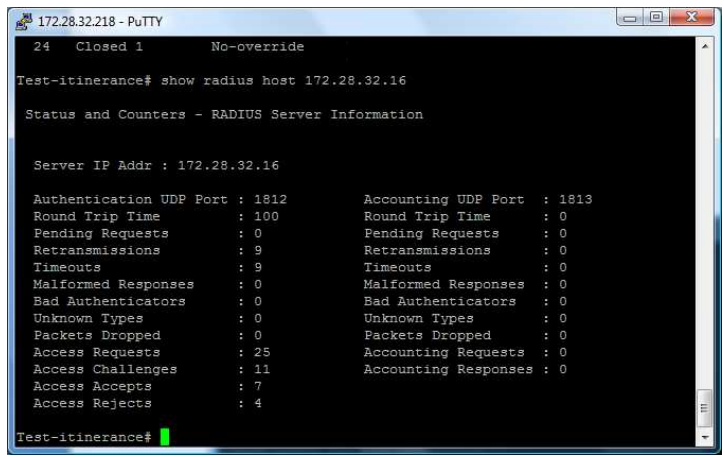
Current Current
Port Status VLAN ID Port COS
-----+-----+-----+-----+
17  Closed 1      No-override
18  Closed 1      No-override
19  Closed 1      No-override
20  Closed 1      No-override
21  Closed 1      No-override
22  Closed 1      No-override
23  Closed 1      No-override
24  Closed 1      No-override

Test-itinerance#

```

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

show radius host 172.28.32.16



1.4. CONFIGURATION DU SERVEUR LINUX

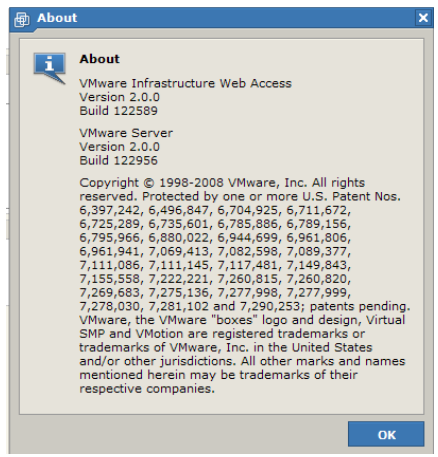
1.4.1. Téléchargement de l'ISO Ubuntu

Ubuntu 8.10 « Intrepid Ibex » : Il s'agit de la dernière version qui inclus les dernières améliorations.

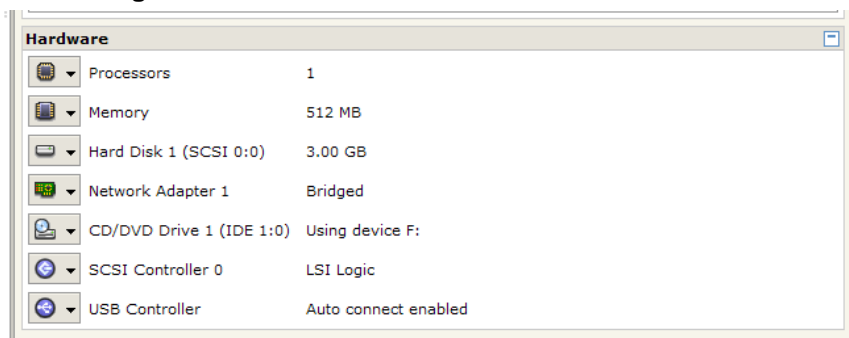
Lien pour le téléchargement : <http://www.ubuntu.com/getubuntu/download>
(Sélectionner l'onglet serveur)

1.4.2. Installation de la version VmWare Serveur

Logiciel « VMware-server-2.0.0-122956.exe »



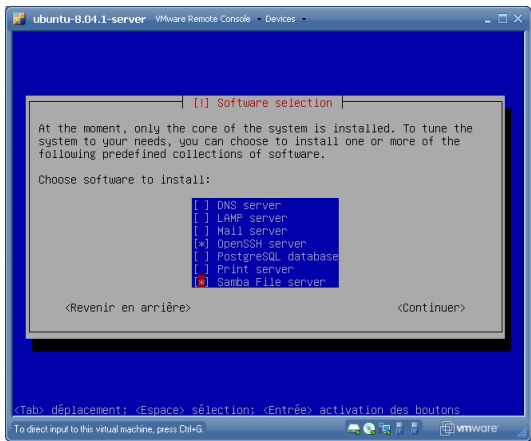
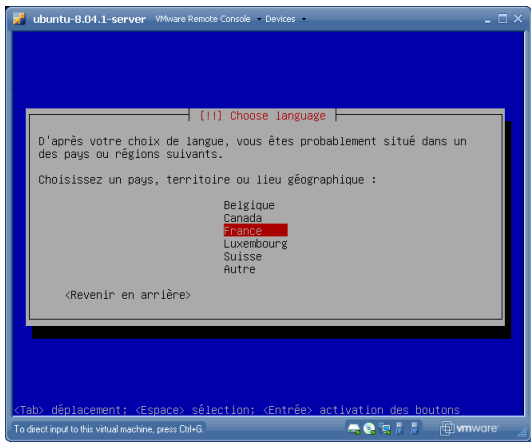
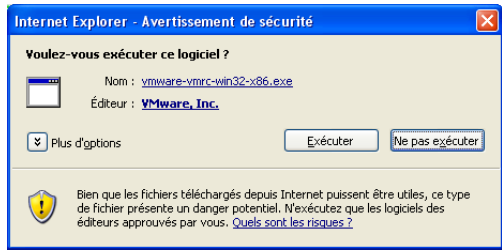
1.4.3. Paramétrage de la VMWARE Linux



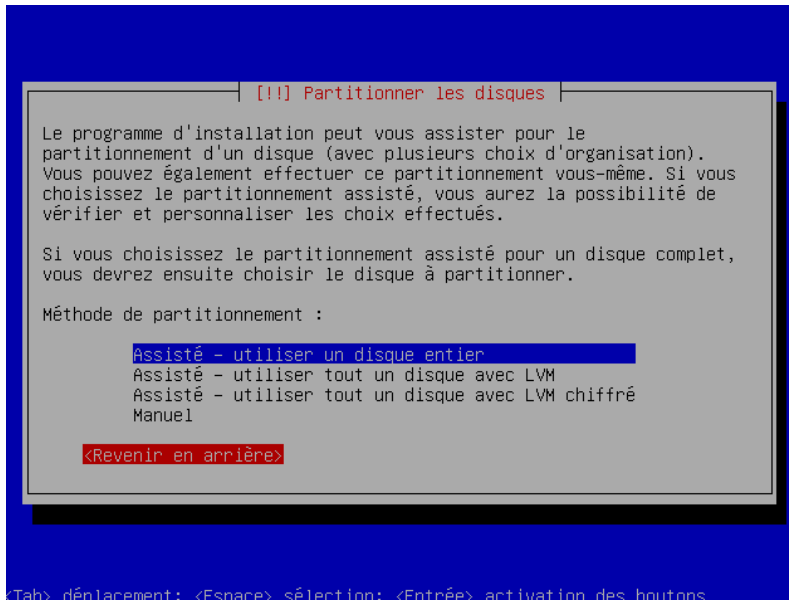
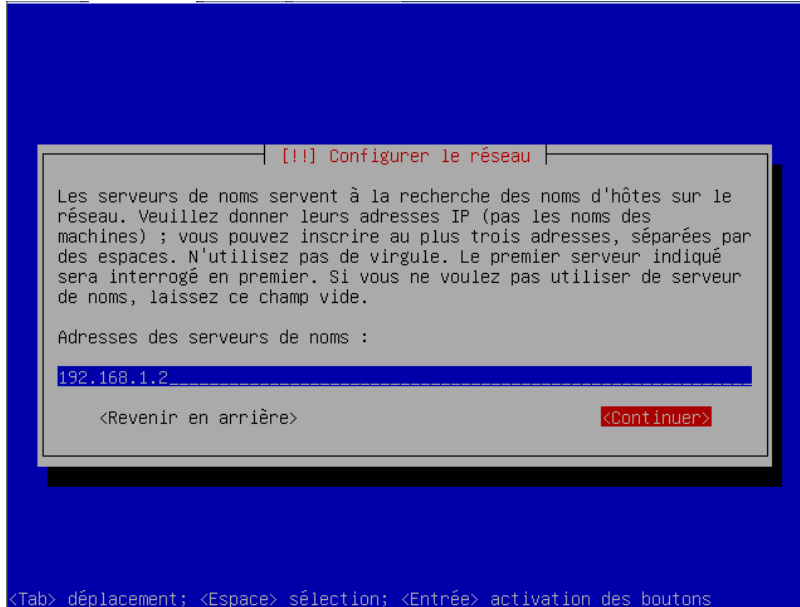
Remarque : Mettre au minimum 3 GB

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

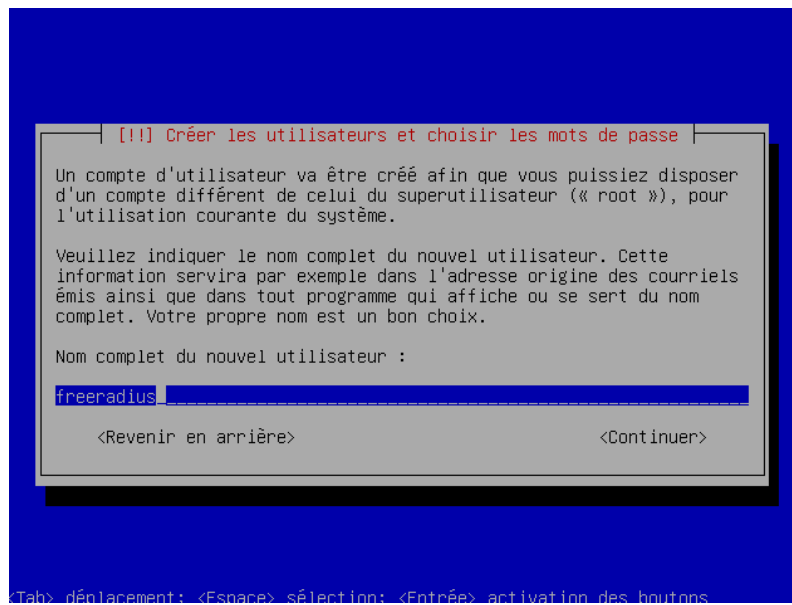
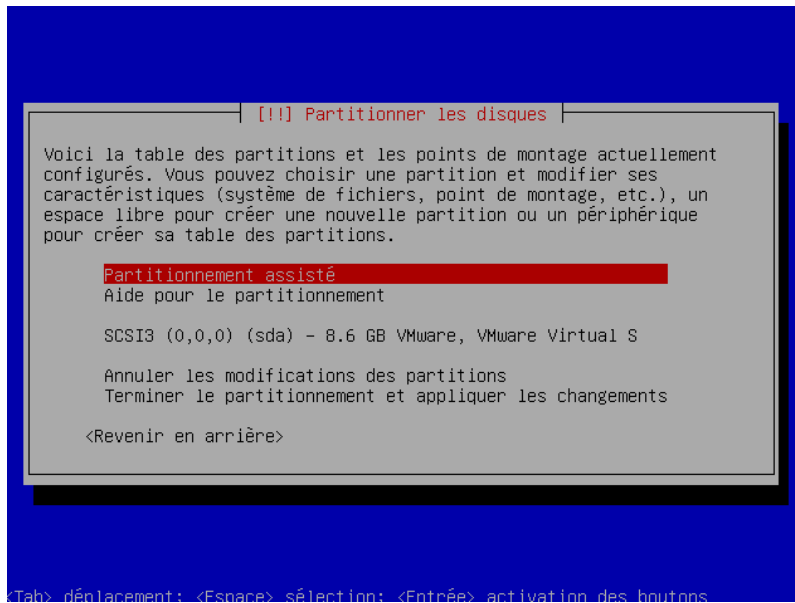
1.4.4. Installation de la version Ubuntu 8.04.1 « Hardy Heron »
 Installer le plug-in avant l'installation de l'iso Linux.



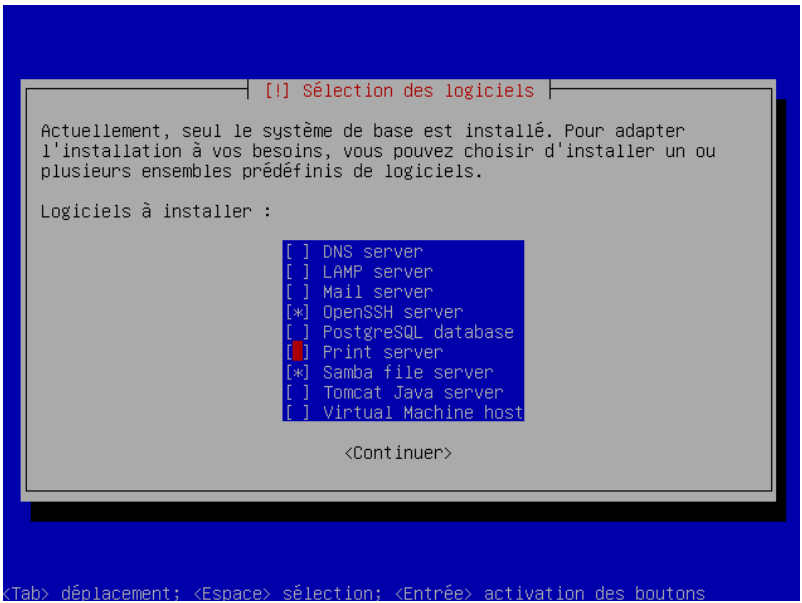
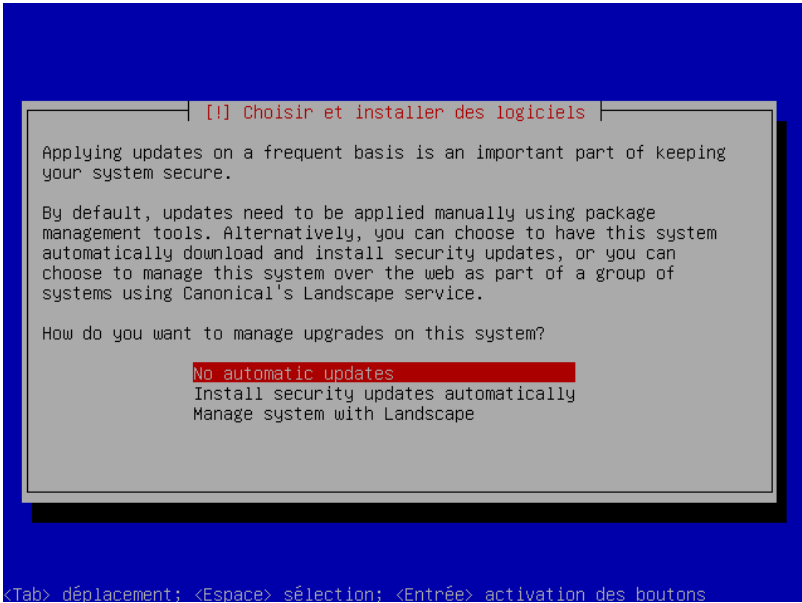
	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT



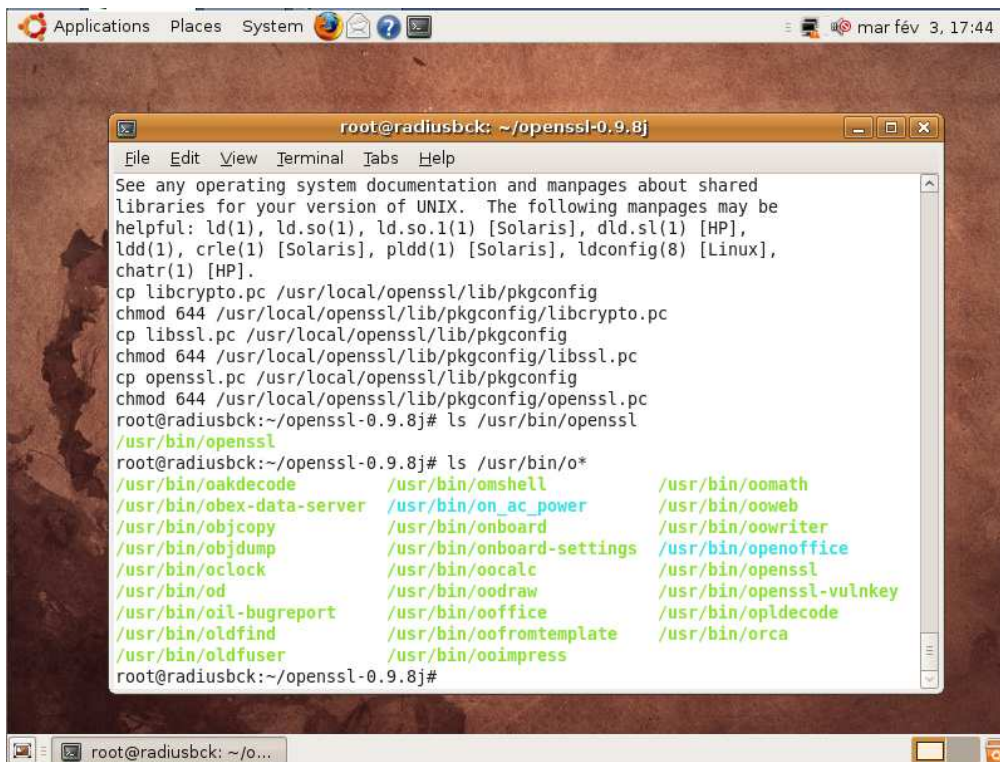
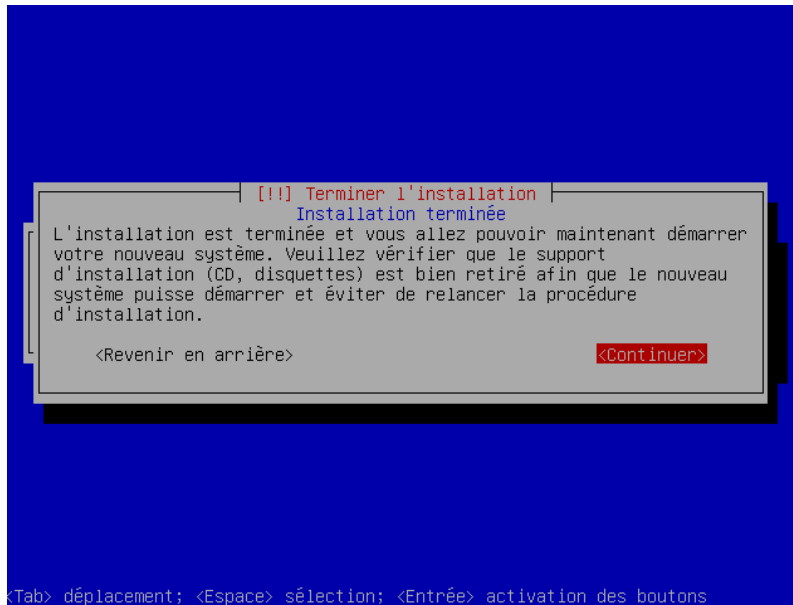
	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT



	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT



	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT



Rapport Technique - Société		Restreint
Date	Auteurs	Classification
23/09/09	P.P.	D3
		Référence
		CAE-AUDIT

Une fois que l'installation est terminée, on se logg avec le login « freeradius » et le mot de passe « freeradius » .

```
// modification du password root
$ sudo passwd radius

// on ferme la session
$ logout
```

On se logue en root puis :

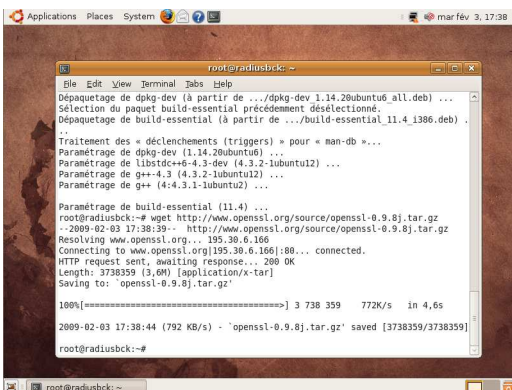
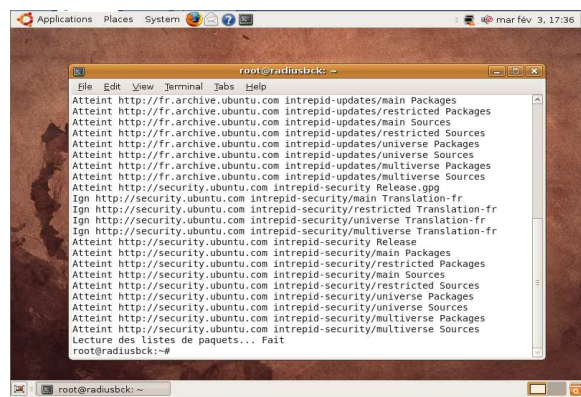
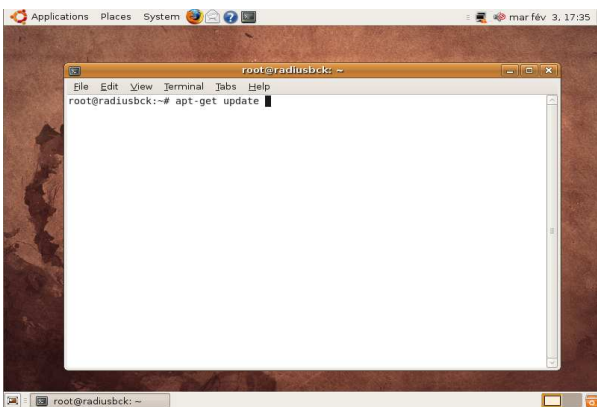
```
// obtenir une adresse IP
# dhclient

// mise à jour des packages
# apt-get update

// window manager
# apt-get install gnome-bin
# apt-get install ubuntu-desktop

// lancer l'interface graphique
# startx (cliquer sur Don't reload)

// Télécharger les compilateurs -> ATTENTION : nécessite le reboot
# apt-get install build-essential
```



	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

1.5. INSTALLATION DE OPENSSL 0.9.8J

openssl.sh (ne pas oublier de le chmod +x) :

```
#/bin/sh
#openssl
wget http://www.openssl.org/source/openssl-0.9.8j.tar.gz
tar xzf openssl-0.9.8j.tar.gz
cd openssl-0.9.8j
./config --prefix=/usr/local/openssl shared
make && make install
cd ..
```

Faire un lien symbolique de openssl pour pouvoir l'utiliser (s'il n'existe pas dans /usr/bin) :

```
# ln -s /usr/local/openssl/bin/openssl /usr/bin/openssl
```

1.6. SERVICE D'AUTHENTIFICATION RADIUS

1.6.1. Installation du logiciel FreeRadius 2.04

(Installation des outils pour la compilation et l'installation de Freeradius V2.1.3)

freeradius.sh (ne pas oublier de le chmod +x) :

```
#/bin/sh
# freeradius
wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.1.3.tar.gz
tar xzf freeradius-server-2.1.3.tar.gz
cd freeradius-server-2.1.3
./configure --with-openssl --with-openssl-includes=/usr/local/openssl/include/ --with-openssl-  
libraries=/usr/local/openssl/lib/
make
make install

#Mettre à jour le cache des librairies
ldconfig
```

En cas d'erreur, il est utile de consulter le fichier « **config.log** »

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

```

root@radiusbck: /usr/local/etc/raddb
File Edit View Terminal Tabs Help
PATH="$PATH:/sbin" ldconfig -n /usr/local/lib
-----
Libraries have been installed in:
  /usr/local/lib

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the '-LLIBDIR'
flag during linking and do at least one of the following:
- add LIBDIR to the 'LD_LIBRARY_PATH' environment variable
  during execution
- add LIBDIR to the 'LD_RUN_PATH' environment variable
  during linking
- use the '-Wl,-rpath -Wl,LIBDIR' linker flag
- have your system administrator add LIBDIR to '/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
-----
root@radiusbck:~/openssl-0.9.8j/freeradius-server-2.1.3# ldconfig
root@radiusbck:~/openssl-0.9.8j/freeradius-server-2.1.3# cd /usr/local/etc/raddb/
root@radiusbck: /usr/local/etc/raddb# ls
acct_users      clients.conf    huntgroups      preproxy_users  sql.conf
attrs            dictionary      ldap.attrmap    proxy.conf       sqlippool.conf
attrs.access_reject  eap.conf        modules          radiusd.conf     templates.conf
attrs.accounting_response  example.pl      otp.conf        sites-available  users
attrs.pre-proxy      experimental.conf  policy.conf     sites-enabled
certs                hints            policy.txt      sql
root@radiusbck: /usr/local/etc/raddb#

```

Rapport Technique - Société			Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

1.6.2. Les fichiers de configuration

Les principaux fichiers de configurations sont les suivants :

- **clients.conf** (déclaration des switches – et – secret partagé)
- **radiusd.conf** (ports d'écoute)
- **users** (création des utilisateurs en base locale)
- **eap.conf** (non modifié – EAP-MD5)

D'autres logiciels sont nécessaires pour implémenter la méthode PEAP :

- **OpenSSL** pour la génération de certificat
- **KERBEROS** : pour authentifier le serveur radius auprès du contrôleur de domaine Windows
- **SAMBA** : pour inclure le serveur radius dans l'annuaire Active Directory

Les autres fichiers de configuration

- **/etc/resolv.conf**
- **/etc/hosts**
- **/etc/krb5.conf**
- **/etc/samba/smb.conf**

Le fichier : /usr/local/etc/raddb/clients.conf (Configuration des clients)

Rajout du switch 192.168.1.1 et de localhost (pour les tests) :

```
# gedit /usr/local/etc/raddb/clients.conf
```

```
client 192.168.1.1 {
    secret = testing123
}
client 192.168.0.0/16 {
    secret = testing123
}
```

} Pour les tests

Pour des raisons de test avec l'outil NTRadiusPing

Le fichier : /usr/local/etc/raddb/users

```
# gedit /usr/local/etc/raddb/users
```

Testing purpose : mettre tous les utilisateurs par défaut en authentification ntlm

En bas du fichier :

```
DEFAULT Auth-Type = MS-CHAP
```

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

Le fichier : /usr/local/etc/raddb/eap.conf

```
# gedit /usr/local/etc/raddb/eap.conf
```

Par défaut, la méthode d'authentification sélectionnée est EAP-MD5. Pour la première phase de test de la maquette, cette méthode a été utilisée temporairement avant la mise en œuvre de la méthode PEAP.

```
eap {
    default_eap_type = peap
    ...
}

peap {
    default_eap_type = mschapv2
    ...
}
```

1.7. INTEGRATION DU SERVEUR LINUX FREERADIUS DANS LE DOMAINE

/etc/samba/smb.conf :

```
[global]
    # nom du domaine
    workgroup = TEST

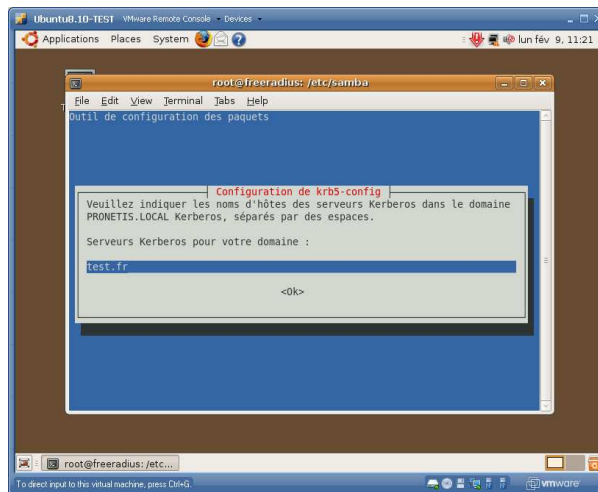
    # nom de domaine AD (a rajouter car n'existe pas dans le fichier de config)
    realm = TEST.FR

    # nom de machine
    server string = Freeradius

    # mode de sécurité
    security = ADS
```

Installation de Kerberos 5 :

```
# apt-get install krb5-clients krb5-user
```



Rapport Technique - Société			Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

/etc/krb5.conf :

```
[libdefaults]
    default_realm = TEST.FR

[realms]
    TEST.FR = {
        kdc = activedirectory.test.fr
        admin_server = 192.168.1.2
        default_domain = TEST.FR
    }

[domain_realm]
    test.fr = TEST.FR
    .test.fr = TEST.FR
```

/etc/resolv.conf :

```
# On rajoute les enregistrements DNS :
nameserver 192.168.1.2
domain TEST.FR
search TEST.FR
```

L'ordre des items dans ce fichier a une importance – pour le temps de résolution des noms typiquement

/etc/hosts :

```
127.0.0.1    localhost
127.0.0.1    freeradius.test.fr    freeradius
# On rajoute ces lignes au cas où le serveur DNS aurait un souci
192.168.1.2 activedirectory.test.fr
192.168.1.2 test.fr
```

/etc/nsswitch.conf

```
passwd: files winbind
group: files winbind
```

Tous les autres également

Vérification pour rejoindre le domaine :

```
# net ads join -U administrateur
```

```
Enter administrateur's password :
Using short domain name -- TEST
Joined 'FREERADIUS' to realm 'test.fr'
```

!! Attention!! Si synchronisation de temps nécessaire!!

```
# sudo ntpdate 192.168.1.2
```

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

Afficher les informations du serveur Active Directory :

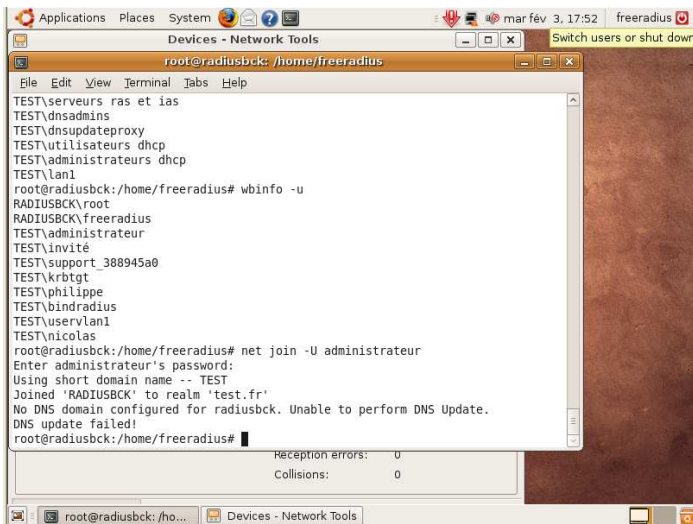
```
# net ads info
```

```
LDAP server : 192.168.1.2
LDAP server name: ActiveDirectory.test.fr
Realm: TEST.FR
Bind Path: dc=TEST,dc=FR
LDAP port 389
Server time: lun, 12 jan 2009 15:39:04 CET
KDC server: 192.168.1.2
Server time offset: 10
```

Commande wbinfo

```
// pour afficher les utilisateur
# wbinfo -u
```

```
// pour afficher les groupes
# wbinfo -g
```



Test d'authentification d'un utilisateur.

```
# kinit philippe
```

```
Password for Philippe : XXXXX
```

Si l'utilisateur n'existe pas ou bien le MdP est faux – alors message d'erreur

Liste des tickets Kerberos obtenus.

```
# klist
```

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Philippe@TEST.FR
Valid starting Expires Service principal
05/13/05 11:11:53 05/13/05 21:11:57 krbtgt/TEST.FR@TEST.FR
renew until XXXXXXXXXXXXXXXX
Kerberos 4 ticket cache: /tmp/tkt0
```

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

klist: You have no tickets cached

1.8. AUTHENTIFICATION NTLM - EAP PEAP

Test de l'authentification d'un utilisateur

```
# ntlm_auth --request-nt-key--domain=TEST.FR --username= philippe
```

password : philippe

The command line returns
NT_STATUS_OK : Success (0x0)

Fichier mschap : /usr/local/etc/raddb/modules/mschap

Tout en bas décommenter la ligne, et la modifier :

```
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{mschap:User-Name:-None} --  
domain=%{mschap:NT-Domain:-TEST} --challenge=%{mschap:Challenge:-00} --nt-  
response=%{mschap:NT-Response:-00}"
```

Remarque pour la gestion des groupes avec NTLM : (uniquement dans ce fichier exemple LAN1)

```
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{mschap:User-Name:-None} --  
domain=%{mschap:NT-Domain:-TEST} --require-membership-of=TEST\LAN1 --  
challenge=%{mschap:Challenge:-00} --nt-response=%{mschap:NT-Response:-00}"
```

Tester si l'utilisateur est "ok" :

```
# radtest philippe philippe localhost 0 testing123
```

rad_recv : Access-Accept

```
# radtest philippe philippe localhost 0 testing123
```

rad_recv : Access-Reject (car mauvais password)

Generation du certificat SSL du serveur radius pour PEAP et TTLS

```
# cd /usr/local/etc/raddb/certs/
```

Champs a changer dans le **ca.cnf** et **server.cnf** :

```
[certificate_authority]  
countryName = FR  
stateOfProvinceName = Radius  
localityName = Somewhere  
organizationName = PRONETIS  
emailAddress = admin@pronetis.fr  
commonName = "freeradius"
```

```
# make
```

```
// pour supprimer les anciens certificats  
# rm -f *csr *key
```

Rapport Technique - Société			Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

Vérification des utilisateurs

```
# radtest test test localhost 0 testing123
```

Traces enregistrée ci-dessous :

```
Sending Access-Request of id 37 to 127.0.0.1 port 1812
User-Name = "test"
User-Password = "test"
NAS-IP-Address = 127.0.0.1
NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=37, length=20
```

1.8.1. Installation du FreeRadius en tant que Service

Soit mettre dans un fichier annexe

```
# nano /etc/init.d/autolauch.sh
# chmod +x /etc/init.d/autolauch.sh
# update-rc.d autolauch.sh defaults
```

Soit mettre dans le fichier rc.local

```
# vi /etc/rc.local
```

```
ifconfig eth0 192.168.1.3 netmask 255.255.255.0
route add default gw 192.168.1.1
ntpdate 192.168.1.2
/usr/local/sbin/rc.radiusd start
```

Ce test permet de voir que le serveur freeRADIUS est correctement installé et fonctionne en répondant à une requête pour un utilisateur local. Il se chargera automatiquement à chaque démarrage du serveur grâce au fichier « /etc/rc.local ».

Modification du hostname dans le fichier /etc/hostname

```
hostname freeradius
```

1.8.2. Configuration réseau et synchronisation de temps

Contenu du script de démarrage : /etc/init.d.setip.sh

```
# /etc/init.d/setip.sh
```

```
ifconfig eth0 192.168.1.3 netmask 255.255.255.0
route add default gw 192.168.1.1
ntpdate 192.168.1.2
```

⚠ PENSER A REINITIALISER LA CARTE RESEAU APRES MODIF DE L'IP !!

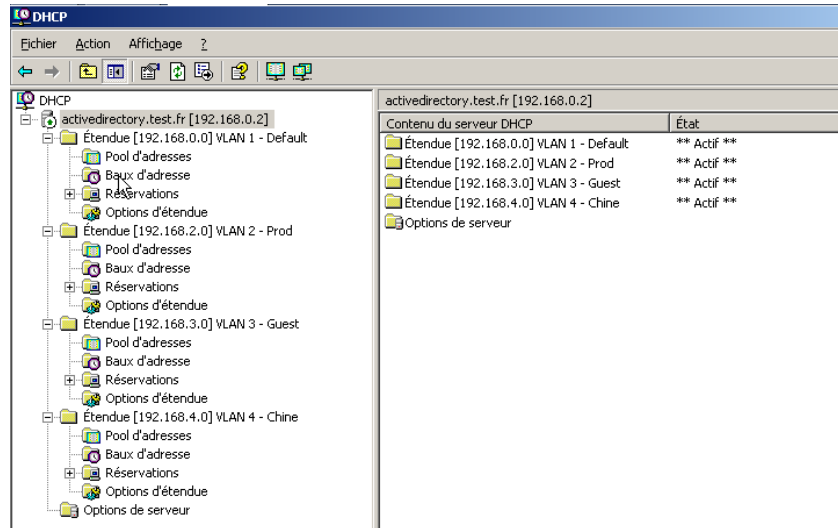
```
# ifconfig eth0 down
# ifconfig eth0 up
```

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

1.9. SERVEUR DHCP

Le service DHCP est activé sur cette maquette sur le contrôleur de domaine.

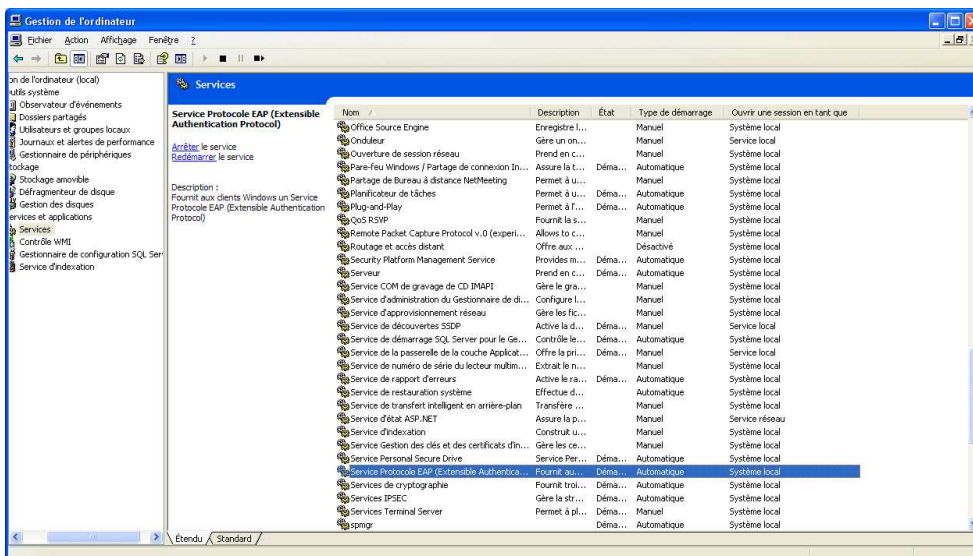
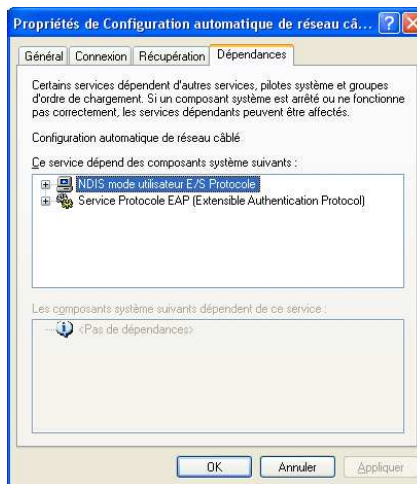
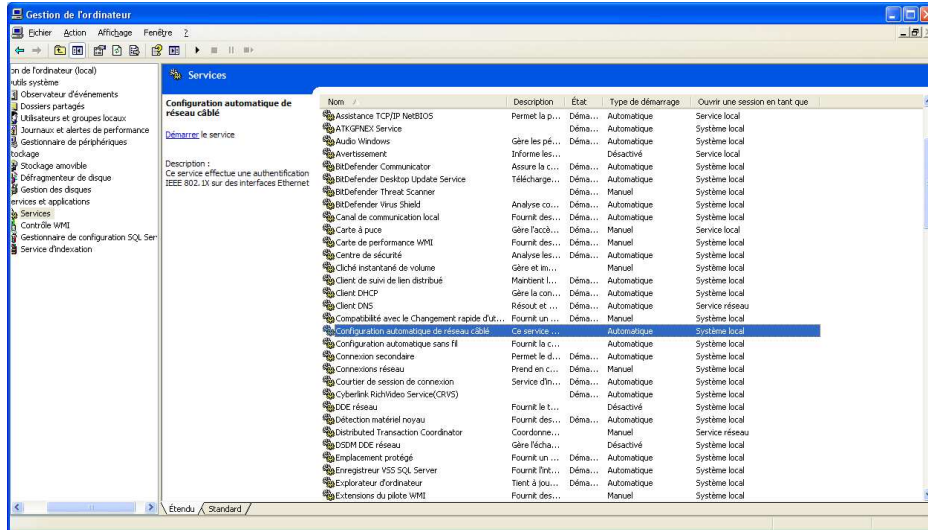
Configuration du service DHCP



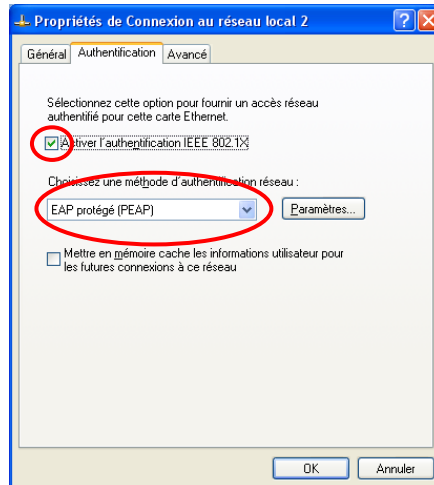
	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

1.10. CONFIGURATION DU SUPPLICANT – POSTE DE TRAVAIL – PEAP

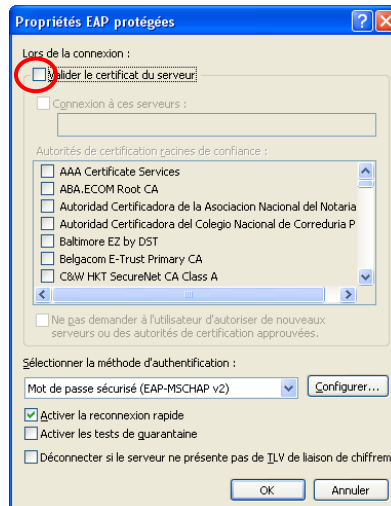
Activation des services suivants sur le poste de travail XP SP3 :



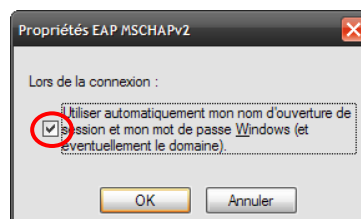
	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT



Remarque : Ne pas activer la mise en mémoire des informations de connexion



Ne pas sélection « valider le certificat du serveur



	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

2. ANNEXES

2.1. COMMANDES DE CONFIGURATION RESEAU

```
ifconfig eth0 192.168.1.4 netmask 255.255.255.0  
route add default gw 192.168.1.1  
ntpdate 192.168.1.2
```

ATTENTION : Ne pas installer le freeradius avec ces commandes (la Version 1.17 n'est plus activement maintenu), sinon :

```
sudo apt-get remove freeradius  
sudo apt-get autoclean
```

2.2. COMMANDES DE DEBUGGING FREERADIUS

Demarrage en mode debugging

Lancement de FreeRadius dans un screen a part (pour vérifier les échanges) :

```
screen -S radiusd
```

```
sudo radiusd -X -xx (sudo si on est pas en Root)
```

```
radiusd -X -xx ou bien /usr/local/sbin/radius start
```

on détache par les touches suivantes

```
Ctrl+A+D
```

on rattache le screen dans la session terminal par la commande

```
screen -r
```

Demarrage

```
Sudo radiusd -X (en mode debug light)
```

Arrêt

```
CTRL + C  
ou  
Sudo radius stop (que si le service radius est installé en tant que service)
```

Affichage des processus

```
#ps -ax
```

Remarque : les processus systèmes sont entre parenthèses

Suppression d'un processus

```
#kill -9 N°PID
```

	Rapport Technique - Société		Restreint
Date	Auteurs	Classification	Référence
23/09/09	P.P.	D3	CAE-AUDIT

2.3. POUR L'INSTALLATION DE OPEN LDAP :

openldap.patch :

```

--- openldap-2.4.13.orig/libraries/liblutil/getpeereid.c
+++ openldap-2.4.13/libraries/liblutil/getpeereid.c
@@ -14,6 +14,8 @@
 * <http://www.OpenLDAP.org/license.html>.
 */

+#define _GNU_SOURCE
+
#include "portable.h"

#ifdef HAVE_GETPEEREID

```

berkeleydb

apt-get install libdb4.7 libdb4.7++ libdb4.7-dev libdb4.7++-dev

openldap

wget <ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/openldap-2.4.13.tgz>

tar xzf openldap-2.4.13.tgz

mv openldap.patch openldap-2.4.13/

cd openldap-2.4.13

./configure --prefix=/usr/local/openldap

make depend

patch -Np1 -i openldap.patch

make && make install

cd ..