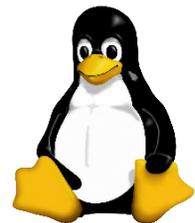
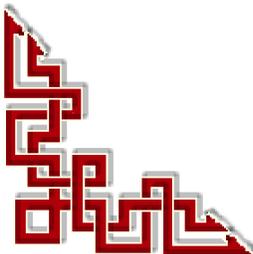


RF-232

Micronator

SME / sans fil
Gestion à distance



© RF-232, Montréal 2012,
6447, avenue Jalobert, Montréal. Québec H1M 1L1

Tous droits réservés RF-232

Décharge de responsabilité

Ce document est uniquement destiné à informer. Les informations, ainsi que les contenus et fonctionnalités de ce document sont fournis sans engagement et peuvent être modifiés à tout moment. *RF-232* n'offre aucune garantie quant à l'actualité, la conformité, l'exhaustivité, la qualité et la durabilité des informations, contenus et fonctionnalités de ce document. L'accès et l'utilisation de ce document se font sous la seule responsabilité du lecteur ou de l'utilisateur.

RF-232 ne peut être tenu pour responsable de dommages de quelque nature que ce soit, y compris des dommages directs ou indirects, ainsi que des dommages consécutifs résultant de l'accès ou de l'utilisation de ce document ou de son contenu.

Chaque internaute doit prendre toutes les mesures appropriées (mettre à jour régulièrement son logiciel antivirus, ne pas ouvrir des documents suspects de source douteuse ou non connues) de façon à protéger le contenu de son ordinateur de la contamination d'éventuels virus circulant sur la toile.

Avertissement

Bien que nous utilisions ici un vocabulaire issu des techniques informatiques, nous ne prétendons nullement à la précision technique de tous nos propos dans ce domaine.

Sommaire

I-	Introduction.....	5
1.	Description générale.....	5
1.1.	Note au lecteur.....	5
1.2.	Conventions.....	5
2.	À savoir.....	6
2.1.	SSH.....	6
2.2.	DNS dynamique.....	6
2.3.	DynDNS.....	6
II-	Pré requis.....	7
1.	Installation d'un serveur SME.....	7
2.	Installation de DD-WRT.....	7
3.	Configuration de E1000-1.....	7
4.	Configuration de E1000-2.....	7
5.	Vérification du réseau.....	7
6.	Adresse internet du serveur SME.....	7
7.	PuTTY.....	7
III-	Configuration du serveur SME.....	8
1.	Introduction.....	8
2.	Server-manager.....	8
2.1.	Paramètres SSH.....	8
2.2.	Sécurité pour la gestion du serveur.....	9
2.3.	FTP.....	10
3.	Service DNS dynamique.....	10
4.	Configuration pour no-ip.com.....	10
4.2.	Recréer la config de no-ip.com.....	15
IV-	Configuration du tunnel.....	16
1.	Introduction.....	16
2.	PuTTY.....	16
2.1.	Session.....	16
2.2.	Window Translation.....	17
2.3.	Connection SSH X11.....	17
2.4.	Connection SSH Tunnels.....	18
2.5.	Sauvegarde.....	18
V-	Configuration de FireFox.....	20
1.	Introduction.....	20
2.	Configuration.....	20
VI-	Vérification en simulant l'internet.....	21
1.	Introduction.....	21
2.	Configuration du serveur SME.....	21
3.	Configuration du routeur Linksys.....	23
4.	Configuration du gestionnaire distant.....	24

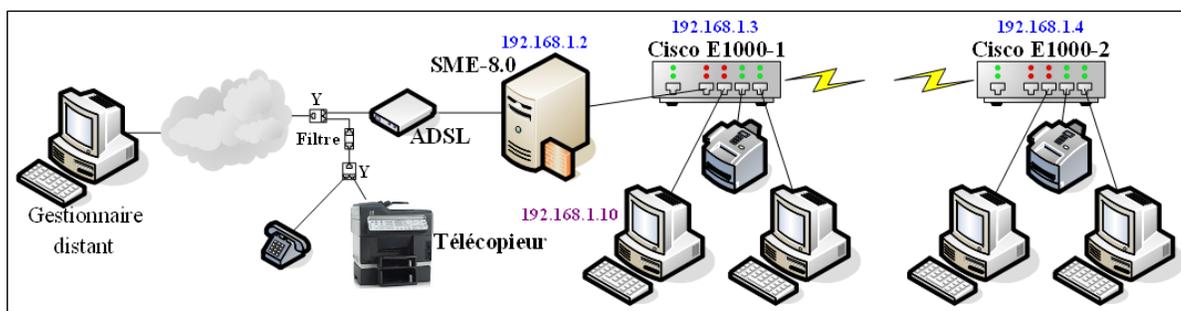
5.	Création du tunnel.....	24
6.	Déconnexion du sans fil.....	25
7.	Connexion distante au serveur SME.....	25
8.	Connexion distante à E1000-1.....	25
9.	Connexion distante à E1000-2.....	26
VII-	Vérification à distance.....	27
1.	Introduction.....	27
	Crédits.....	29

I- Introduction

1. Description générale

Ce sixième document de la série *SME sans fils* décrit l'installation d'un client d'un service **DNS** dynamique, la création d'un tunnel **SSH**, la configuration de **FireFox** pour utiliser le tunnel et la gestion à distance.

Référence: http://www.dd-wrt.com/wiki/index.php/Easy_SSH_tunnels
<http://www.tuteurs.ens.fr/internet/loin/tunnel.html>



1.1. Note au lecteur

* Les captures d'écrans ne sont que des références.

** Les informations écrites ont préséance sur celles retrouvées dans les captures d'écrans. Veiller à se référer aux différents tableaux lorsque ceux-ci sont présents.

1.2. Conventions

Toutes les commandes à entrer sur le serveur sont en **gras**. Les affichages à surveiller sont en **rouge** ou en **bleu**.

```
# ping 192.168.1.149
192.168.1.149 is alive
#
```

Les liens de référence internet sont en [bleu](#) et ceux intra-document en [bleu](#).



Manipulation, truc ou ruse pour se tirer d'embaras.



Une recommandation ou astuce.



Une note.



Une étape, note ou procédure à surveiller.



Un site de téléchargement **FTP**.

2. À savoir

2.1. SSH

Référence: <http://wiki.mandriva.com/fr/Ssh>

Les services réseau usuels comme **FTP**, **POP** ou **telnet** sont pratiques mais intrinsèquement non sûrs puisqu'ils font tous transiter les données et les mots de passe en clair sur un réseau incroyablement peu sûr. Il est très facile d'intercepter les informations de ces services et de copier les données transférées. De plus, l'authentification du serveur est faible : les services sont à la merci d'attaques du type *man-in-the-middle* (un homme au milieu), où un intrus peut se faire passer pour le serveur et ainsi recevoir toutes les données que le client envoie.

Et voici **SSH (Secure SHell)**. En utilisant **SSH**, le trafic est chiffré et vous rendez les attaques du type 'man-in-the-middle' presque impossibles. Cela vous protège aussi du **DNS** et de l'**IP spoofing**. En prime, il offre la possibilité de compresser le trafic et ainsi rendre les transferts plus rapides. **SSH** est un outil très souple : non seulement il remplace telnet, mais vous pouvez aussi créer un tunnel chiffré pour faire passer les services comme **FTP**, **POP** et même **PPP**.

Le **SSH** original a été développé par une société finlandaise. À cause de contraintes de copyright et des algorithmes brevetés, le monde du Logiciel Libre utilise maintenant **OpenSSH**, un système à la **SSH**.

Comme tout service, **SSH** s'appuie sur une architecture client-serveur. Tout administrateur système compétent utilise un serveur **SSH**. Si votre système hôte distant n'utilise pas **SSH**, vous devriez vraiment penser à changer pour un système qui l'utilise. Un site qui n'utilise pas un serveur **SSH** affiche un manque d'intérêt certain pour la sécurité.

2.2. DNS dynamique

Référence: http://fr.wikipedia.org/wiki/Domain_Name_System#Mise_.C3.A0_jour_dynamique

Une extension du **DNS** nommée **DNS dynamique** (en) (**DDNS**) permet à un client de mettre à jour une zone avec des informations qui le concernent (**RFC 2136**). Ceci est utile quand des clients obtiennent une adresse **IP** par **DHCP** et qu'ils souhaitent que le **DNS** reflète le nom réel de la machine.

2.3. DynDNS

Référence: <http://fr.wikipedia.org/wiki/DynDNS>.

DynDNS est un service américain permettant à des utilisateurs qui utilisent une [adresse IP](#) dynamique de disposer quand même d'un [nom de domaine](#).

Il est souvent utilisé par des particuliers qui hébergent leur [site web](#) sur leur propre machine mais qui, ne disposant pas d'adresse **IP** fixe, doivent actualiser régulièrement leur **DNS**. Un logiciel installé sur cette machine teste l'adresse **IP** à intervalles réguliers et informe le serveur de **DynDNS** en cas de changement. Celui-ci met alors à jour les serveurs de **DNS**.

2.3.1. Site offrant un service DNS dynamique

<http://www.no-ip.com/>

II- Pré requis

1. Installation d'un serveur SME

Pour le premier document de la série *SME sans fil* décrivant l'installation d'un serveur **SME-8.0**, on peut se référer au document suivant: http://www.micronator.org/PDF/RF-232_SME-8.0_Installation.pdf.

2. Installation de DD-WRT

Pour le deuxième document décrivant l'installation du micrologiciel **DD-WRT**, on peut se référer au document suivant: http://www.micronator.org/PDF/RF-232_SME_Sans-Fil_Inst_DD-WRT.pdf.

3. Configuration de E1000-1

Pour le troisième document décrivant la configuration du premier routeur, **E1000-1**, on peut se référer au document suivant: http://www.micronator.org/PDF/RF-232_SME_Sans-Fil_Config_DD-WRT_No-1.pdf.

4. Configuration de E1000-2

Pour le quatrième document décrivant la configuration du premier routeur, **E1000-1**, on peut se référer au document suivant: http://www.micronator.org/PDF/RF-232_SME_Sans-Fil_Config_DD-WRT_No-2.pdf.

5. Vérification du réseau

Pour le cinquième document décrivant la vérification du réseau, on peut se référer au document suivant: http://www.micronator.org/PDF/RF-232_SME_Sans-Fil_Config_DD-WRT_verification.pdf.

6. Adresse internet du serveur SME

Pour ce document, nous nous sommes inscrits chez le fournisseur de service **DNS** dynamique **no-ip.com** et avons créé le domaine **AinesSansFil.no-ip.org** afin de vérifier l'accès distant à notre réseau.

7. PuTTY

PuTTY est un utilitaire pour se brancher à distance.

Téléchargement: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

III- Configuration du serveur SME

1. Introduction

Nous allons ajuster les paramètres du serveur **SME** pour l'accès **SSH**, l'accès à distance et la désactivation du service **FTP**. Nous allons aussi installer et configurer le client **Linux** pour le service **DNS** dynamique de **no-ip.com**.

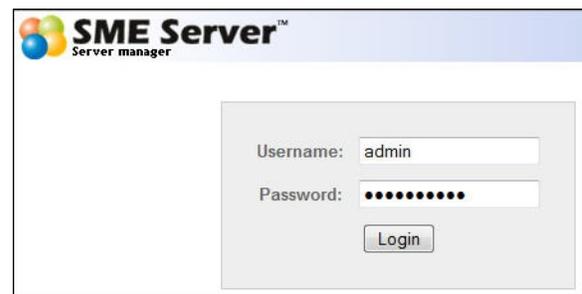
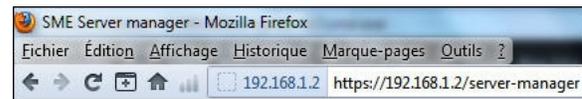
Si le serveur **SME** n'a pas d'adresse internet fixe, il est recommandé d'utiliser un service **DNS** dynamique.

2. Server-manager

On accède à **Server-Manager**.

<https://192.168.1.2/server-manager/>.

On se logue obligatoirement avec l'utilisateur **admin**. Le mot de passe est le même que celui de **root** car **admin** est un **alias** de **root**.



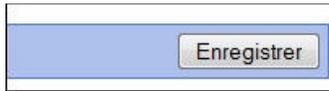
2.1. Paramètres SSH

Autorisation: l'accès depuis **tout l'internet**, l'**administrateur** peut se connecter, **SSH** à l'aide de **mot de passe standards** et on va utiliser le **port 2222**.

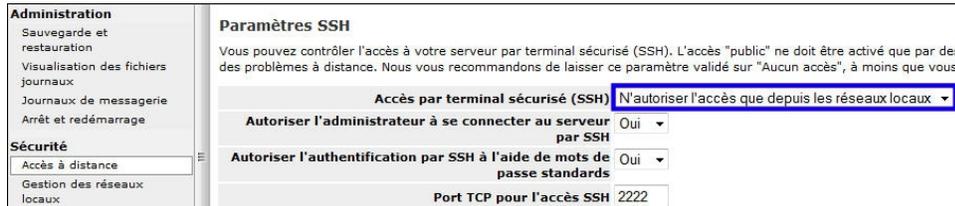
On peut aussi ne pas autoriser l'administrateur **root** et alors il faudra se loguer sous un autre nom et utiliser **su** pour acquérir les privilèges de **root**.



On enregistre les nouveaux paramètres.



Pour une plus grande sécurité, on peut n'autoriser SSH que depuis le réseau local. L'inconvénient est qu'on ne pourra plus administrer à distance les routeurs sans fils.



Administration
Sauvegarde et restauration
Visualisation des fichiers journaux
Journaux de messagerie
Arrêt et redémarrage

Sécurité
Accès à distance
Gestion des réseaux locaux

Paramètres SSH
Vous pouvez contrôler l'accès à votre serveur par terminal sécurisé (SSH). L'accès "public" ne doit être activé que par des problèmes à distance. Nous vous recommandons de laisser ce paramètre validé sur "Aucun accès", à moins que vous

Accès par terminal sécurisé (SSH) N'autoriser l'accès que depuis les réseaux locaux

Autoriser l'administrateur à se connecter au serveur par SSH Oui

Autoriser l'authentification par SSH à l'aide de mots de passe standards Oui

Port TCP pour l'accès SSH 2222

2.2. Sécurité pour la gestion du serveur

Pour une plus grande sécurité pour **Server-Manager**, on peut autoriser seulement une adresse internet unique ou une plage d'adresses pouvant y accéder.

Ici on autorise toutes les adresses IP du réseau **123.123.123.0**.



Sécurité
Accès à distance
Gestion des réseaux locaux
Renvoi de port
Services Proxy

Configuration
Mise à jour logicielle
Date et heure
Groupe de travail
Annuaire LDAP

Gestion à distance
Il est possible de permettre l'accès au gestionnaire du serveur à des hôtes situés sur des réseaux distants. Permettre l'accès qu'à une machine unique. Tout hôte contenu dans la plage d'adresses spécifiée pour

Réseau	Masque de sous-réseau	Nombre d'hôtes	Supprimer
192.168.1.0	255.255.255.0	256	<input type="checkbox"/>

Pour ajouter une nouvelle plage d'adresses de gestion à distance, entrez les informations ci-dessous :

Réseau 123.123.123.0

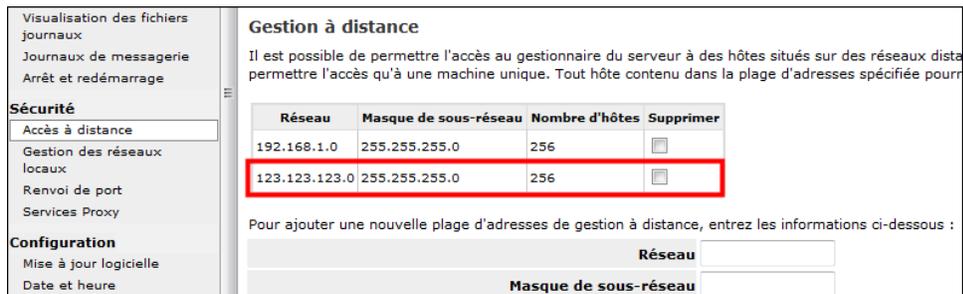
Masque de sous-réseau 255.255.255.0

On enregistre.



Voilà, seulement **123.123.123.1 à 123.123.123.255** peuvent accéder par internet à **Server-Manager**.

Dans ce cas-ci, il n'y aura que les ordinateurs des réseaux **192.168.1.0** et **123.123.123.0** qui pourront accéder à **Server-Manager**. Tous les autres seront exclus.



Sécurité
Accès à distance
Gestion des réseaux locaux
Renvoi de port
Services Proxy

Configuration
Mise à jour logicielle
Date et heure

Gestion à distance
Il est possible de permettre l'accès au gestionnaire du serveur à des hôtes situés sur des réseaux distants. Permettre l'accès qu'à une machine unique. Tout hôte contenu dans la plage d'adresses spécifiée pour

Réseau	Masque de sous-réseau	Nombre d'hôtes	Supprimer
192.168.1.0	255.255.255.0	256	<input type="checkbox"/>
123.123.123.0	255.255.255.0	256	<input type="checkbox"/>

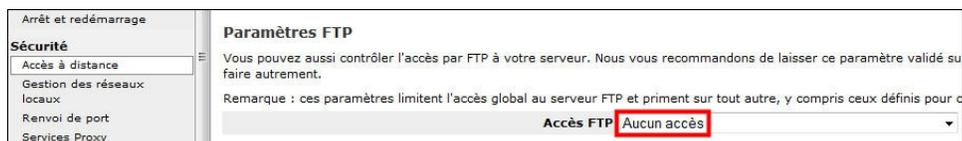
Pour ajouter une nouvelle plage d'adresses de gestion à distance, entrez les informations ci-dessous :

Réseau

Masque de sous-réseau

2.3. FTP

Il ne faut pas autoriser le service **FTP** car la transmission du **mot de passe** se fait en clair sur l'internet.



3. Service DNS dynamique

Si on utilise **Dyndns.org** pour la configuration du service **DNS** dynamique, se référer au premier document de la série **SME sans fil** décrivant l'installation d'un serveur **SME-8.0**:

http://www.micronator.org/PDF/RF-232_SME-8.0_Installation.pdf.

4. Configuration pour no-ip.com

Lors de l'installation du serveur **SME**, nous avons utilisé le service **DNS** dynamique de **Dyndns.org** car nous y avons un compte. Maintenant, il faut payer pour utiliser ce service, ce qui n'était pas le cas lorsque nous avons créé notre compte.

Pour ceux que ça peut intéresser, nous allons expliquer une méthode pour utiliser le service de **DNS** dynamique de **no-ip.com**. Ce service est gratuit. Lors de l'installation du serveur **SME**, choisir "*Ne pas utiliser de service DNS dynamique*".



Il faut savoir que pour compiler le logiciel client de **no-ip.com**, il faut installer le compilateur **gcc** sur le serveur **SME** ce qui n'est pas recommandé par la distribution car la présence de **gcc** sur le serveur induit une **faille de sécurité**. Nous croyons qu'il existe une faible possibilité d'avoir un problème de sécurité à cause de **gcc**. Néanmoins, nous pouvons toutefois remédier à la situation en désinstallant **gcc** après la compilation. Nous allons aussi enlever **cpp** que **gcc** va installer comme dépendance.

4.1.1. Installation de gcc

On se logue sur le serveur **SME**.

On crée un répertoire temporaire et on s'y rend.

```
[root@t110 ~]# mkdir /temp
[root@t110 ~]#

[root@t110 ~]# cd /temp
[root@t110 temp]#

[root@t110 temp]# pwd
/temp
[root@t110 temp]#
```

On installe **gcc**.

On répond "**y**" à la question **Is this ok [y/N]:**.

```
[root@t110 temp]# yum install gcc
Loaded plugins: fastestmirror, protect-packages, smeserver
Loading mirror speeds from cached hostfile
* base: mirror.trouble-free.net
* smeaddons: distro.ibiblio.org
...
...
Total download size: 34 M
Is this ok [y/N]: Y
```

Configuration du serveur SME

```
...
...
Complete!

=====
WARNING: You now need to run BOTH of the following commands
to ensure consistent system state:

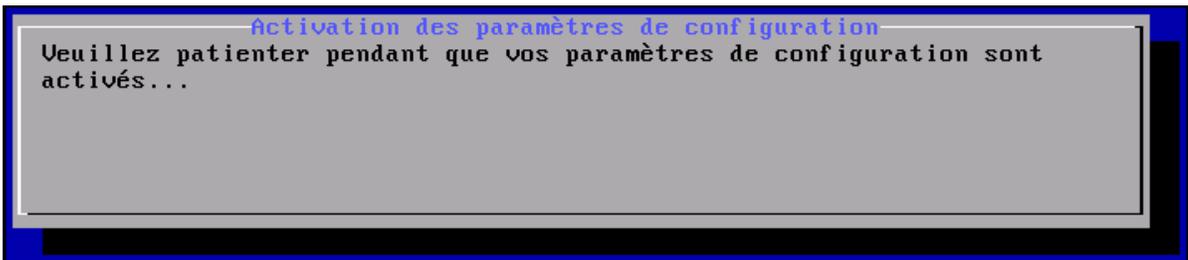
signal-event post-upgrade; signal-event reboot

You should run these commands unless you are certain that
yum made no changes to your system.
=====
[root@t110 temp]#
```

Tel que demandé, il faut maintenant donner les deux commande suivantes pour terminer l'installation.

```
[root@t110 temp]# signal-event post-upgrade; signal-event reboot
[root@t110 temp]#
```

On attend que le serveur ait fini de ré-amorcer.



```
Activation des paramètres de configuration
Veuillez patienter pendant que vos paramètres de configuration sont
activés...
```

4.1.2. Téléchargement du client no-ip

On se logue, on se rend dans le répertoire `/temp` et on télécharge le client **Linux** du service **DNS** dynamique de **no-ip.com**.

```
[root@t110 ~]# cd /temp
[root@t110 temp]#

[root@t110 temp]# pwd
/temp
[root@t110 temp]#

[root@t110 temp]# wget http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz
--2012-11-10 21:30:53-- http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz
Resolution de www.no-ip.com... 8.23.224.110
Connexion vers www.no-ip.com[8.23.224.110]:80...connect.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 134188 (131K) [application/x-gzip]
Saving to: `noip-duc-linux.tar.gz.1'

100%[=====>] 134 188
210K/s in 0,6s

2012-11-10 21:30:54 (210 KB/s) - noip-duc-linux.tar.gz.1 sauvegardé [134188/134188]
[root@t110 temp]#
```

On vérifie.

```
[root@t110 temp]# ls -als
total 144
 4 drwxr-xr-x  2 root root   4096 nov. 10 21:30 .
 4 drwxr-xr-x 25 root root   4096 nov. 10 21:15 ..
136 -rw-r--r--  1 root root 134188 juin  5 2011 noip-duc-linux.tar.gz
[root@t110 temp]#
```

On extrait le **tar.gz**.

```
[root@t110 temp]# tar -zxvf noip-duc-linux.tar.gz
./._noip-2.1.9-1
noip-2.1.9-1/
noip-2.1.9-1/._binaries
...
...
noip-2.1.9-1/._redhat.noip.sh
noip-2.1.9-1/redhat.noip.sh
[root@t110 temp]#
```

4.1.3. Compilation

On se rend dans le répertoire créé par la décompression.

```
[root@t110 temp]# ls -als
total 152
 4 drwxr-xr-x  3 root root   4096 nov. 10 21:35 .
 4 drwxr-xr-x 25 root root   4096 nov. 10 21:15 ..
 4 -rwxr-xr-x  1 501 games   205 nov. 25 2008 ._noip-2.1.9-1
 4 drwxr-xr-x  3 501 games   4096 nov. 25 2008 noip-2.1.9-1
136 -rw-r--r--  1 root root 134188 juin  5 2011 noip-duc-linux.tar.gz
[root@t110 temp]#

[root@t110 temp]# cd noip-2.1.9-1
[root@t110 noip-2.1.9-1]#
```

On lance le **make**.

```
[root@t110 noip-2.1.9-1]# make
gcc -Wall -g -Dlinux -DPREFIX=\"/usr/local\" noip2.c -o noip2
[root@t110 noip-2.1.9-1]#
```

On lance la **make install**.

On spécifie **eth1** pour la carte réseau-externe en indiquant **1**.

On entre le **nom de login** chez **no-ip.com**: **generaltoto@toto.com**.

On entre le **mot de passe** de l'utilisateur chez **no-ip.com**: *********.

On n'a qu'un nom d'hôte. Si on en a plusieurs on choisit celui du serveur désiré.

On choisit l'intervalle proposée en faisant un **<RETOUR>**.

On ne veut rien lancer après une mise à jour de l'adresse **IP** en répondant: **N**.

```
[root@t110 noip-2.1.9-1]# make install
if [ ! -d /usr/local/bin ]; then mkdir -p /usr/local/bin;fi
if [ ! -d /usr/local/etc ]; then mkdir -p /usr/local/etc;fi
cp noip2 /usr/local/bin/noip2
/usr/local/bin/noip2 -C -c /tmp/no-ip2.conf
Auto configuration for Linux client of no-ip.com.
```

```
Multiple network devices have been detected.

Please select the Internet interface from this list.

By typing the number associated with it.
0      eth0
1      eth1

Please enter the login/email string for no-ip.com          1
                                                         generaltoto@toto.com
Please enter the password for user 'michelandre@micronator.org' *****

Only one host [ainessansfil.no-ip.org] is registered to this account.
It will be used.
Please enter an update interval:[30]                      <RETOUR>
Do you wish to run something at successful update?[N] (y/N)  N

New configuration file '/tmp/no-ip2.conf' created.

mv /tmp/no-ip2.conf /usr/local/etc/no-ip2.conf
[root@t110 noip-2.1.9-1]#
```

Il faut maintenant donner les deux commande suivantes pour terminer l'installation.

```
[root@t110 noip-2.1.9-1]# signal-event post-upgrade; signal-event reboot
[root@t110 noip-2.1.9-1]#
```

On attend que le serveur ait fini de ré-amorcer.

4.1.4. Installation du client

On se relogue.

On vérifie que le fichier de configuration a bien été transféré.

```
[root@t110 ~]# ls -als /usr/local/etc/no-ip2.conf
4 -rw----- 1 root root 156 nov. 10 21:48 /usr/local/etc/no-ip2.conf
[root@t110 ~]#
```

On se rend dans le répertoire créé par le tar.

```
[root@t110 ~]# cd /temp/noip-2.1.9-1
[root@t110 noip-2.1.9-1]#
```

Le nom du script de mise à jour est: **noip2**. On cherche sa localisation.

```
[root@t110 noip-2.1.9-1]# which noip2
/usr/local/bin/noip2
[root@t110 noip-2.1.9-1]#
```

On ajoute la commande d'appel du script de mise à jour à la fin du fichier **/etc/rc.local**. Ainsi, *la commande va être exécuté à chaque amorçage*.

```
[root@t110 noip-2.1.9-1]# echo '/usr/local/bin/noip2' >> /etc/rc.local
[root@t110 noip-2.1.9-1]#
```

On vérifie.

```
[root@t110 noip-2.1.9-1]# tail /etc/rc.local
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
/usr/local/bin/noip2
[root@t110 noip-2.1.9-1]#
```

4.1.5. Vérification du client

On ré-amorce le serveur pour vérifier si la mise à jour va être exécutée.

```
[root@t110 noip-2.1.9-1]# reboot

Broadcast message from root (tty1) (Sat Nov 10 23:20:40 2012):

The system is going down for reboot NOW!
```

On attend que le serveur remonte et on se rend chez **no-ip.com** pour vérifier si la mise à jour a eu lieu.

Hostname Information	
Hostname:	ainessansfil.no-ip.org 
Host Type:	<input checked="" type="radio"/> DNS Host (A) <input type="radio"/> DNS Host (Round Robin) <input type="radio"/> DNS Alias (CNAME)  <input type="radio"/> Port 80 Redirect <input type="radio"/> Web Redirect
IP Address:	206.248.138.152 Last Update: 2012-11-10 20:21:58 PST 
Assign to Group:	- No Group -   Configure Groups 
Enable Wildcard:	Wildcards are a Plus / Enhanced feature. Upgrade Now! 
Advanced Records:	TXT, SPF, and SRV records and the use of some special clients are Plus / Enhanced features. Upgrade now to use them. 

On se logue et on vérifie si le script roule toujours.

```
[root@t110 ~]# ps aux | egrep noip
nobody  3678  0.0  0.0  1956  708 ?        Ss   23:22   0:00 /usr/local/bin/noip2
root    3745  0.0  0.0  4272  672 pts/0    R+   23:29   0:00 egrep noip
[root@t110 ~]#
```

On enlève gcc et cpp.

```
[root@t110 ~]# rpm -e gcc
[root@t110 ~]#
[root@t110 ~]# rpm -e cpp
[root@t110 ~]#
```

On vérifie.

```
[root@t110 ~]# rpm -qa | egrep gcc
libgcc-4.1.2-52.el5_8.1
[root@t110 ~]#
[root@t110 ~]# rpm -qa | egrep cpp
[root@t110 ~]#
```



libgcc fait partie de l'installation initiale du serveur **SME**, il faut le garder.

Voilà, maintenant il sera possible de se connecter au serveur depuis un ordinateur distant en utilisant le nom du domaine.

4.2. Recréer la config de no-ip.com

Si on veut recréer la configuration pour le **client no-ip.com** à cause d'un changement du nom du domaine ou pour quelque raison que ce soit, on n'a qu'à lancer la commande suivante à la console du serveur **SME**.

```
[root@t110 ~]# /usr/local/bin/noip2 -C
```

"-C" pour Configuration.



Hissons la bannière de la victoire.

IV- Configuration du tunnel

1. Introduction

On configure **PuTTY** pour qu'il puisse créer et ouvrir un **tunnel** lors d'une connexion au serveur **SME**.

2. PuTTY

On lance **PuTTY**.



2.1. Session

Host name (or IP address):

AinesSansFil-no-ip.org

Port:

2222



Port qu'on a choisi dans **Server-Manager** du serveur **SME**.

Connection Type:

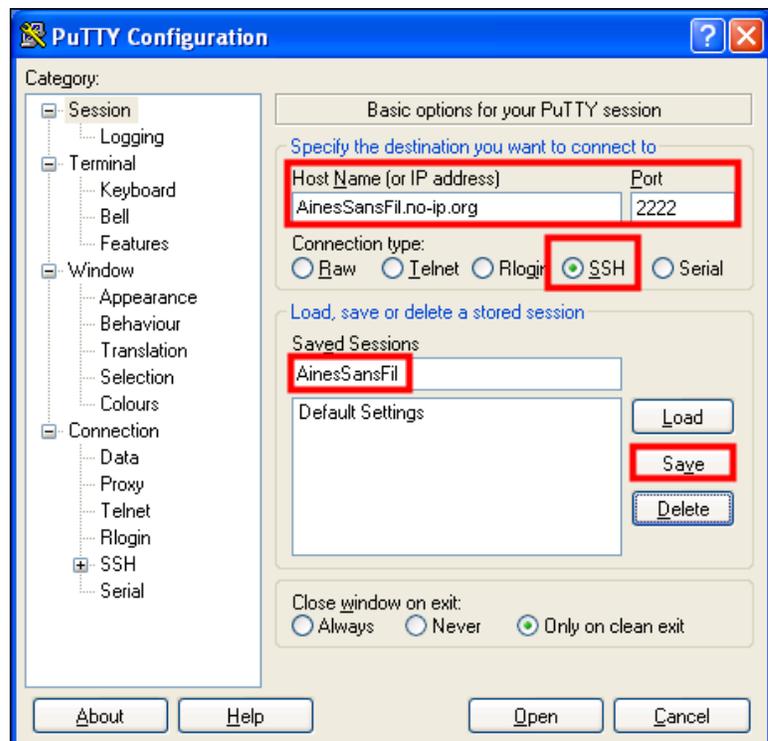
SSH

Saved Sessions:

AinesSansFil

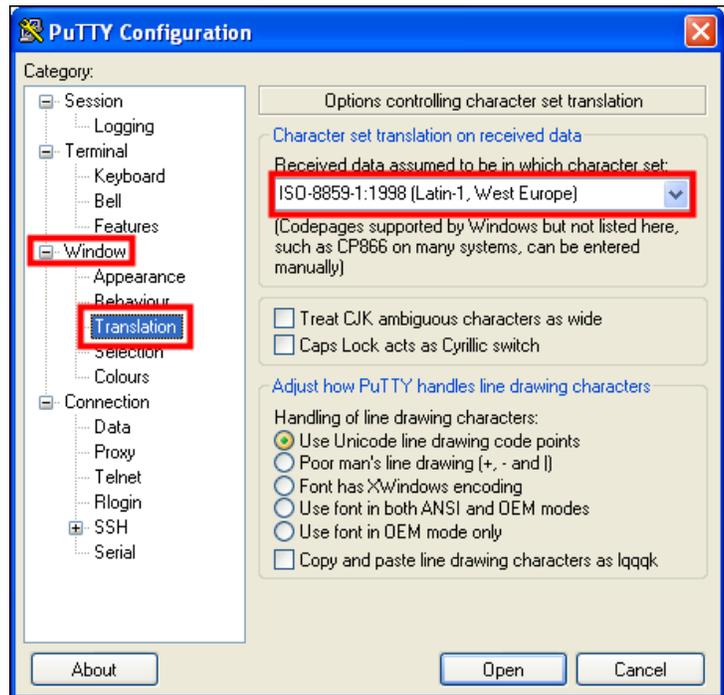
On sauvegarde les paramètres déjà entrés:

Save



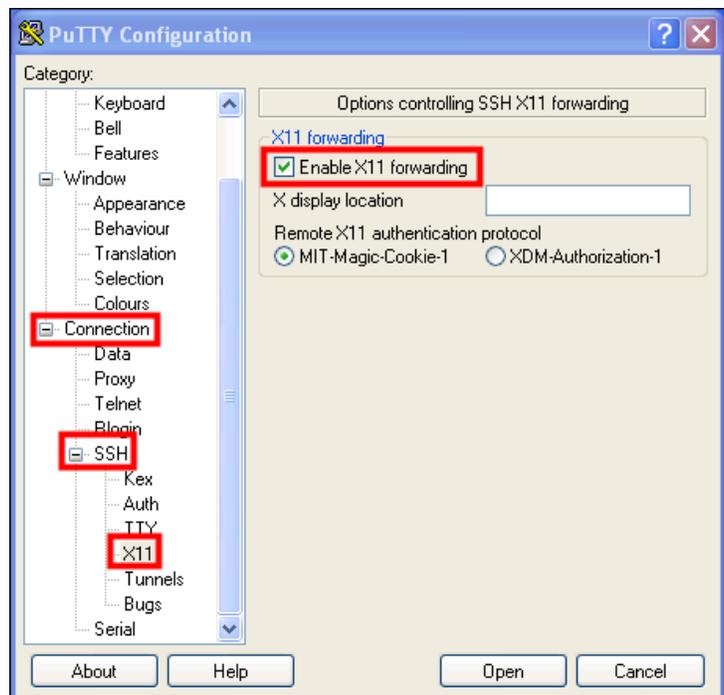
2.2. Window | Translation

S'assurer qu'on utilise le jeu de caractères **ISO-8859-1:1998 (Latin-1, West Europe)**. Autrement, PuTTY pourrait afficher de drôles de cadres autour de l'écran lorsqu'on se loguera avec **admin** pour faire l'administration des paramètres de base du serveur SME.



2.3. Connection | SSH | X11

Cocher **Enable X11 forwarding**.



2.4. Connection | SSH | Tunnels

Source port

On choisit un port entre 1024 et 64255.



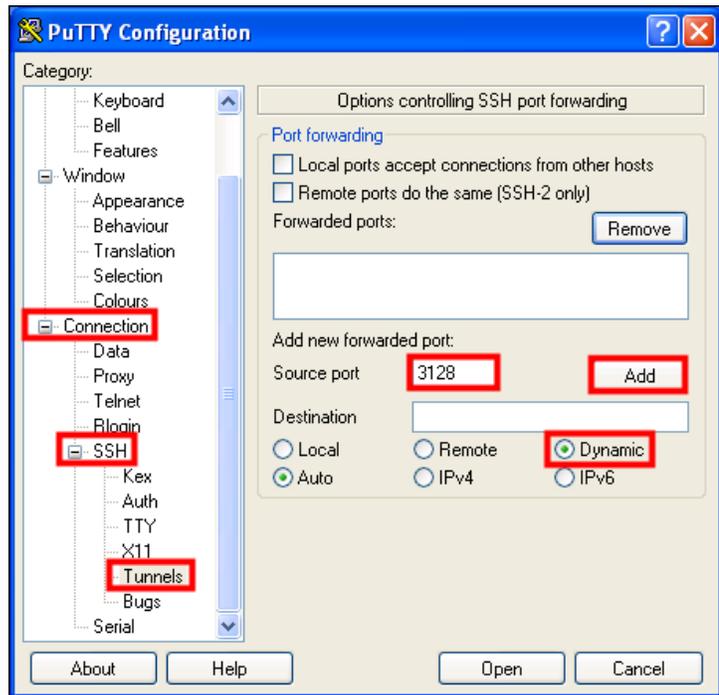
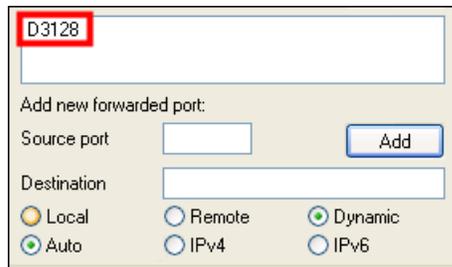
Dans notre cas, on choisit **3128**

Destination

Sélectionner **Dynamic**

Add

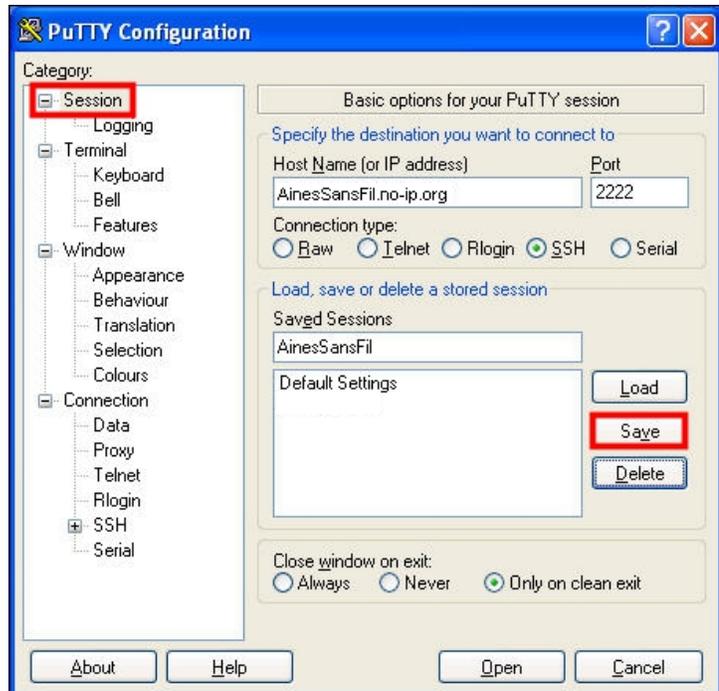
Après l'ajout.



2.5. Sauvegarde

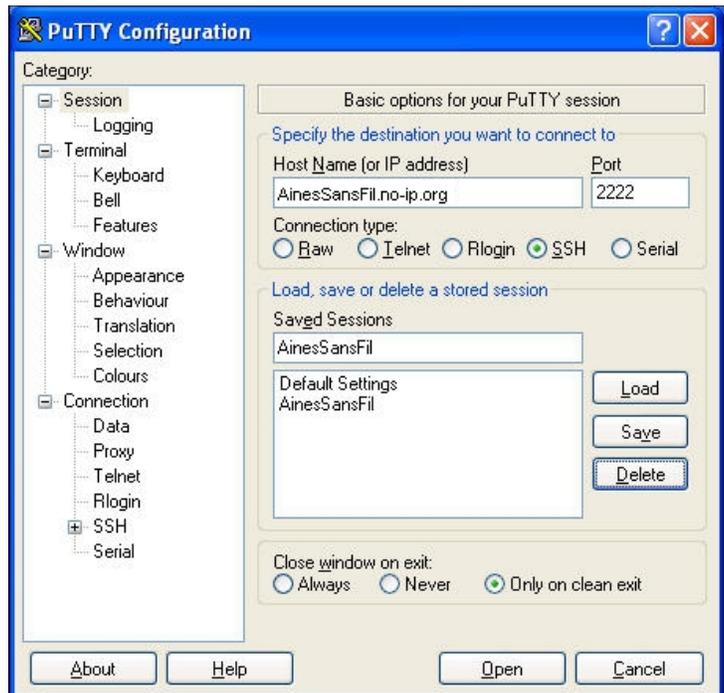
On sauvegarde toutes les options entrées.

Save



Configuration du tunnel

La partie de la configuration de PuTTY est terminée.



V- Configuration de FireFox

1. Introduction

Il reste à emprunter le tunnel.

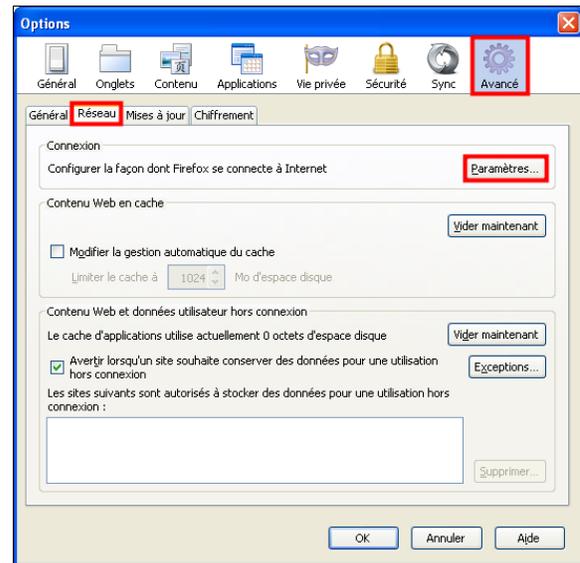
Pour ce faire, nous devons configurer le fureteur pour qu'il utilise le **proxy localhost** avec le port **3128**, que nous avons choisi pendant la configuration de **PuTTY**.

Nous utilisons **FireFox**.

La configuration pour les autres fureteurs est sensiblement la même.

2. Configuration

Outils | Options | Avancées | Réseau | Connexion | Paramètres.



Sélectionner **Configuration manuelle du proxy**:

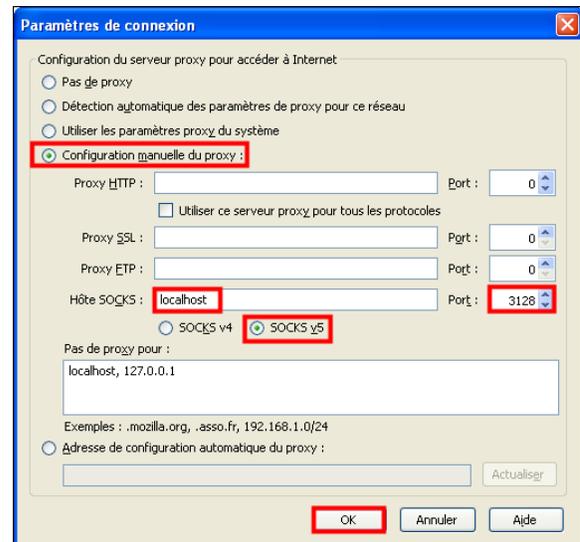
Hôte SOCKS: entrer **localhost**



Ports: **3128**

Sélectionner **SOCKS v5**

OK | OK.



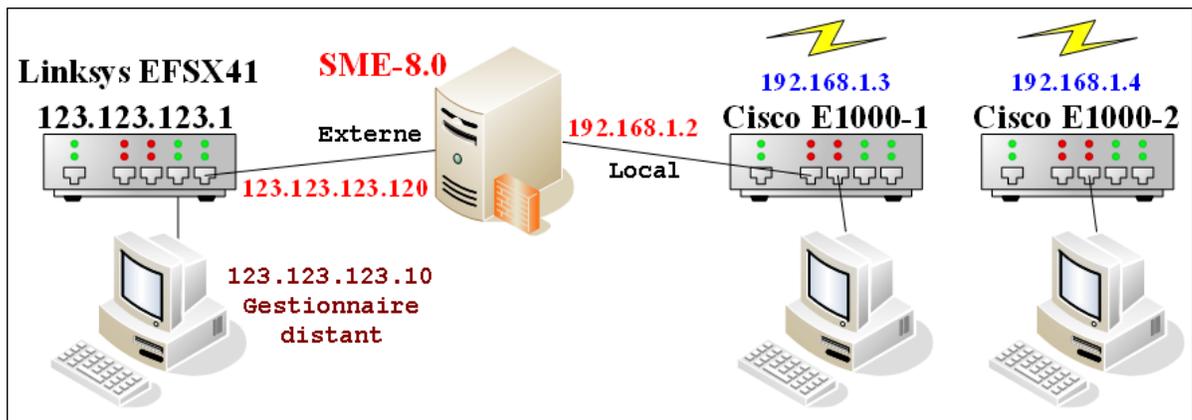
Voilà, le fureteur est prêt.

VI- Vérification en simulant l'internet

1. Introduction

Nous allons simuler l'internet pour pouvoir vérifier le fonctionnement de tout le réseau sans avoir recours à une deuxième connexion ou à une station sur un autre réseau IP non connecté au notre.

Habituellement, tout ce que fait notre FAI est de nous donner une adresse IP publique et nous fournir une adresse de passerelle de même qu'un service DNS. Pour remplacer le FAI, nous allons attribuer une adresse IP publique au serveur SME et lui dire d'utiliser l'adresse publique du Linksys comme passerelle.



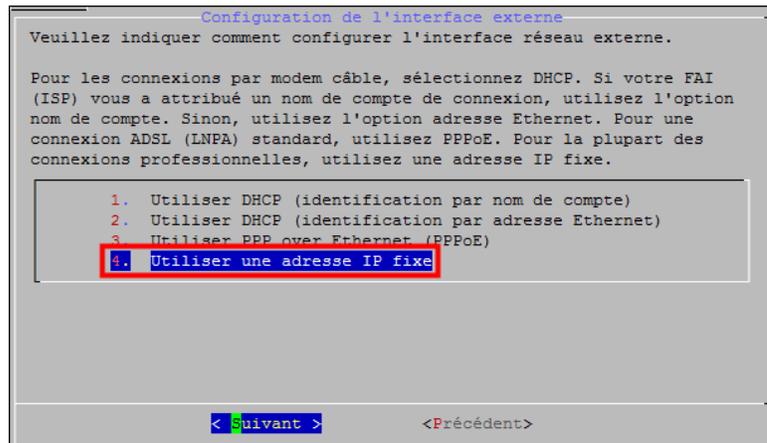
2. Configuration du serveur SME

Nous ouvrons une session PuTTY et nous nous connectons au serveur SME avec l'utilisateur **admin** pour modifier la configuration de base du serveur.

```
login as: admin
admin@192.168.1.2's password: █
```

Après nous être connectés, nous ne modifions aucun paramètre jusqu'à l'écran de **Configuration de l'interface externe**.

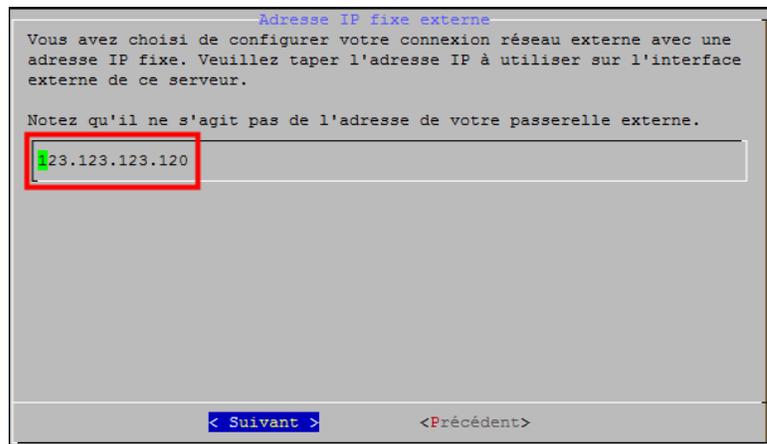
Utiliser une adresse IP fixe | <Suivant>.



Nous entrons l'adresse publique choisie pour notre simulation.

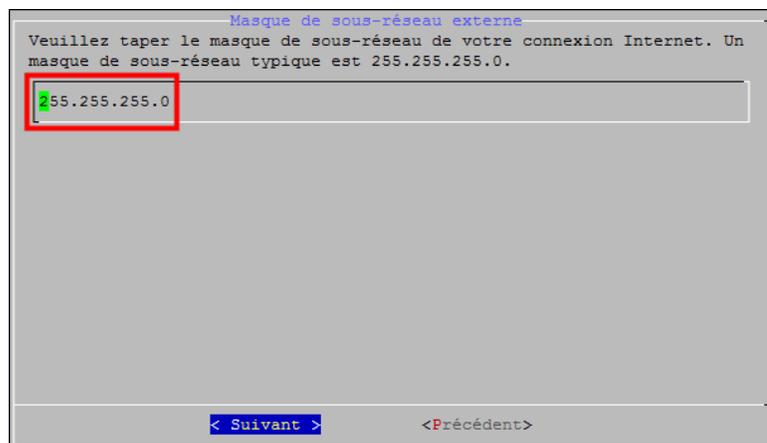


123.123.123.120 <Suivant>.



Nous entrons le masque réseau.

255.255.255.0 | <Suivant>.

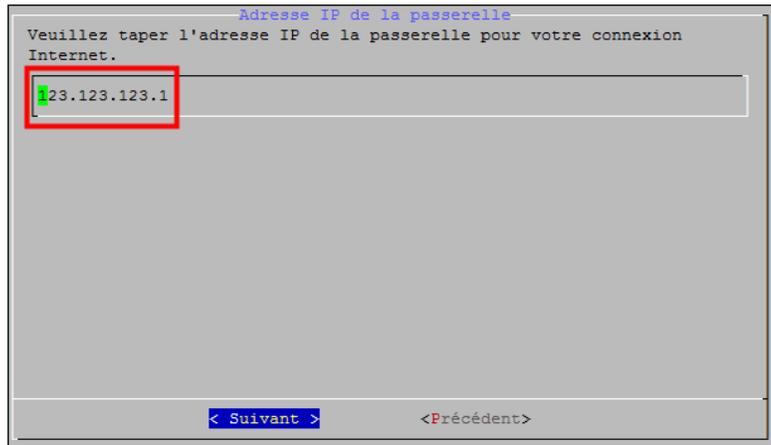


Nous indiquons l'adresse du routeur **Linksys** comme adresse **IP** pour la passerelle.



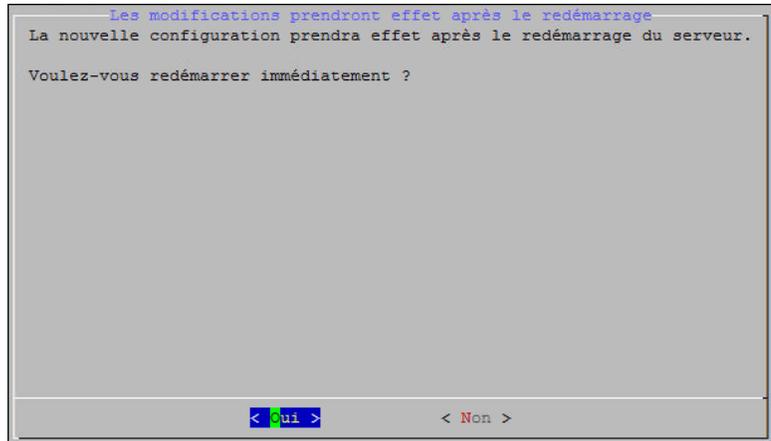
255.255.255.1 | <Suivant>.

En réalité, la passerelle ne sert pas car nous ne sortirons pas par la carte du réseau-externe, nous y entre-



Nous nous rendons jusqu'au dernier écran et acceptons les modifications apportées en cliquant < **Oui** >.

Nous quittons **PuTTY** et attendons que le serveur ait terminé son ré-amorçage.



3. Configuration du routeur Linksys

Après avoir fait in "**Reset**" du **Linksys** pour lui redonner les paramètres initiaux du fabricant, nous modifions seulement son adresse **IP** locale et lui assignons:

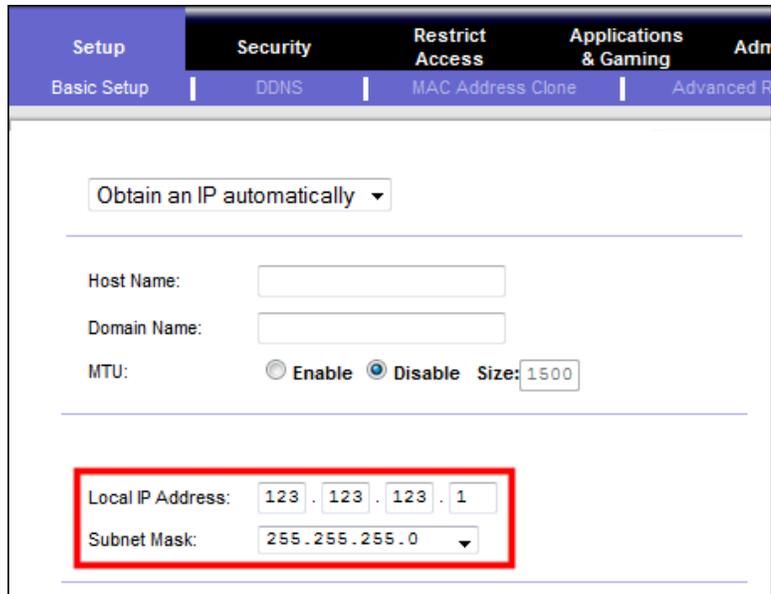


123.123.123.1 | **255.255.255.0**

Nous sauvegardons les changements.



Notre simulateur internet est en place.



4. Configuration du gestionnaire distant

Nous configurons la station pour une adresse **IP** qui sera sur le même segment que le routeur **Linksys** et lui indiquons l'adresse **IP** de la passerelle.

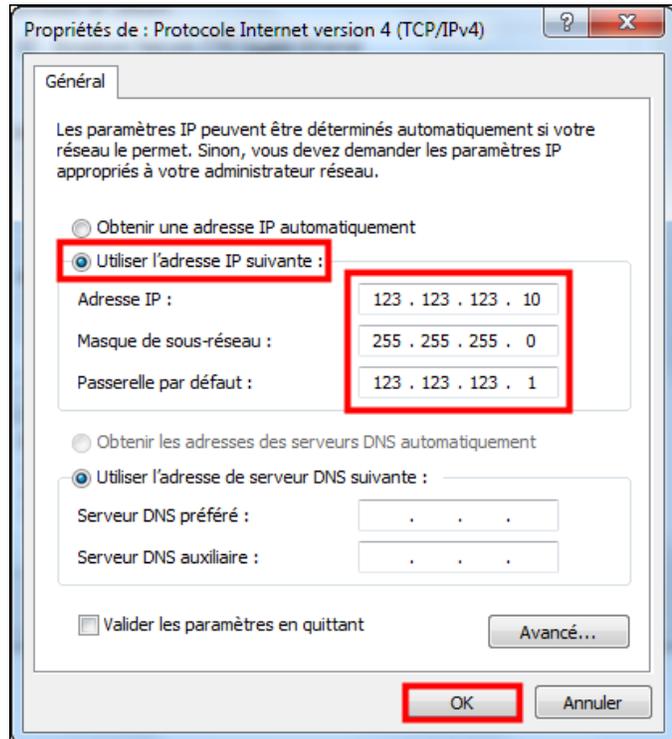
Utiliser l'adresse IP suivante: |

123.123.123.10 |

255.255.255.0 |

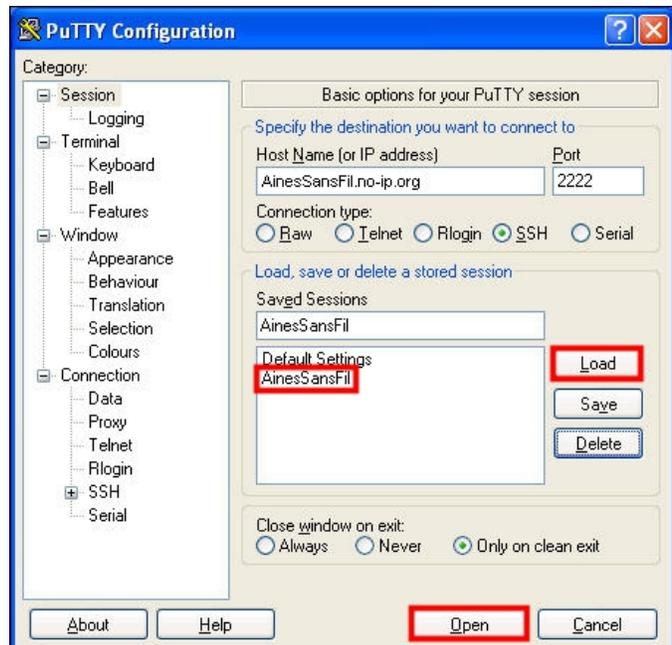


123.123.123.1 | OK.



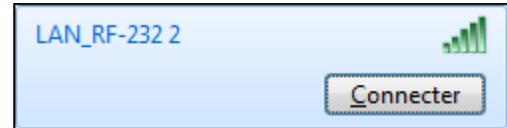
5. Création du tunnel

À l'aide de **PuTTY**, nous créons le tunnel en lançant la session **AinesSansFil** | **Load** | **Open**.



6. Déconnexion du sans fil

⚠ Nous faisons certains que nous ne sommes pas en connexion sans fils.



7. Connexion distante au serveur SME

Vu que nous sommes en simulation d'internet, nous ne possédons pas de service **DNS**. Il nous faut utiliser les adresses **IP** et non le nom du domaine **AinesSansFil.no-ip.org**.

Nous entrons donc l'adresse **IP** du serveur **SME**.

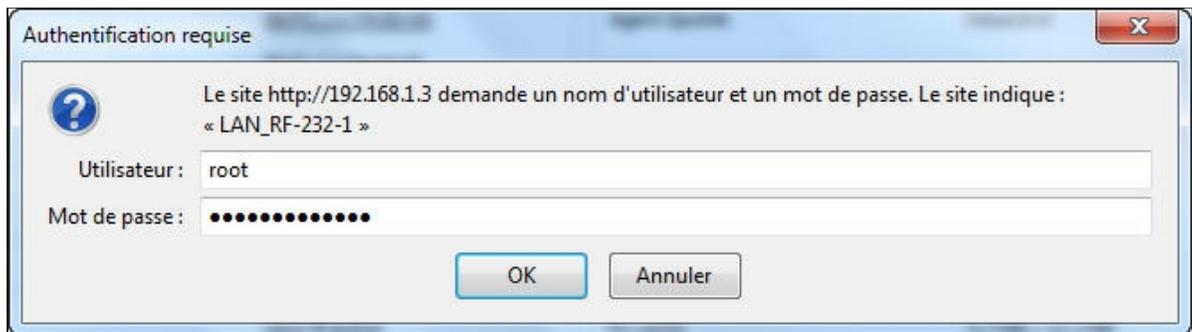
Nous sommes bien sur notre site.



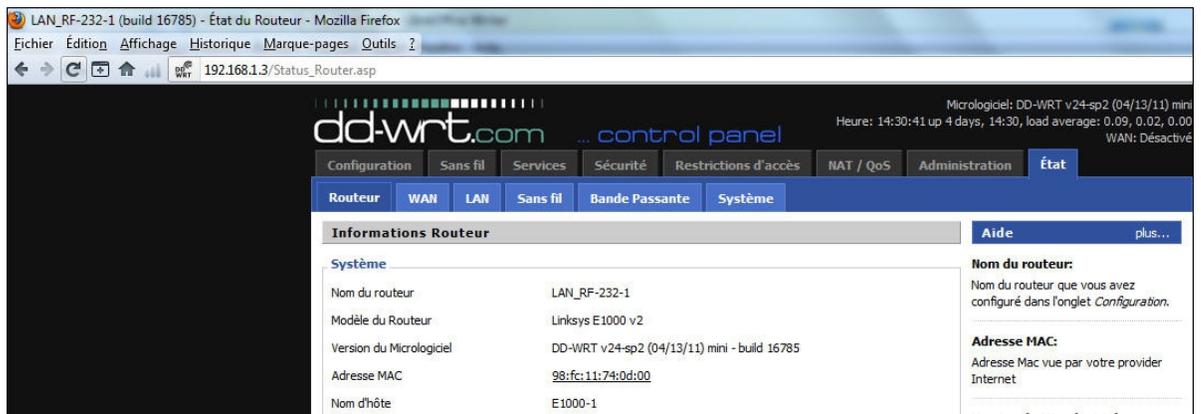
8. Connexion distante à E1000-1

On entre l'adresse du routeur **E1000-1**.

Un miracle se produit et **FireFox** affiche la demande de login de **E1000-1**.



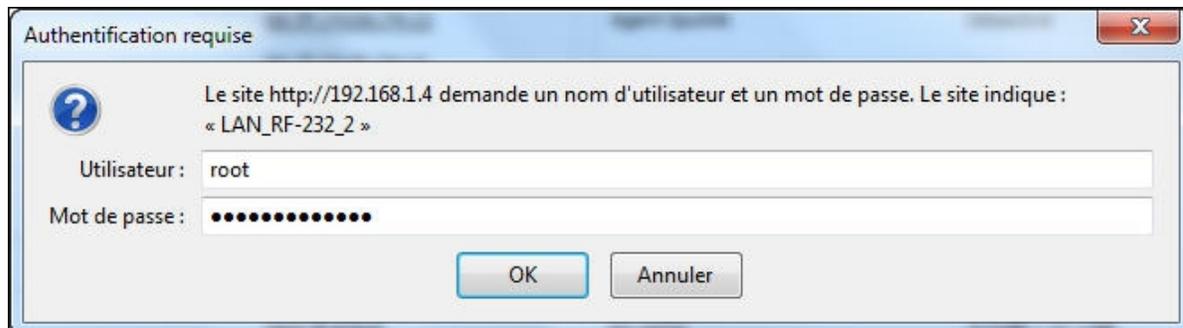
On se logue et le miracle continue, la page **DD-WRT** du routeur sans fil est affichée.



9. Connexion distante à E1000-2

On entre l'adresse du routeur **E1000-2**.

Merveilles des merveilles, **Firefox** affiche la demande de login de **E1000-2**.



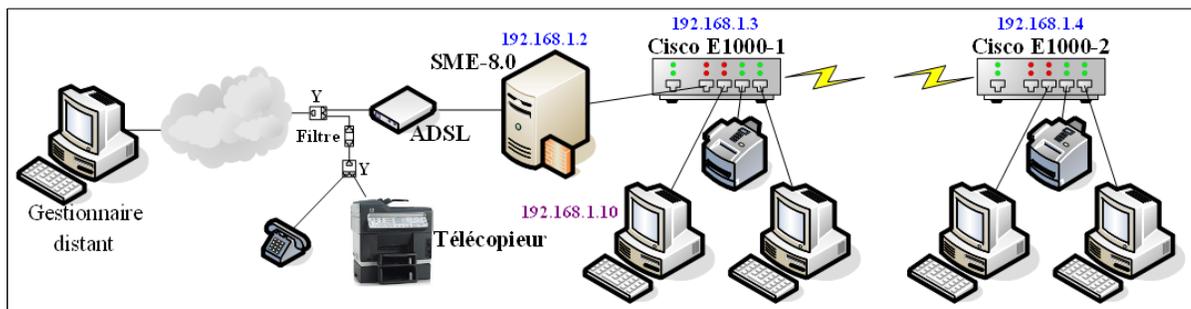
On se logue et la page **DD-WRT** du routeur sans fil est affichée.



Tout fonctionne. L'étape suivante est la vérification ailleurs qu'en laboratoire.

VII- Vérification à distance

1. Introduction



On branche le serveur **SME** à l'internet. D'une station sur le réseau, on vérifie qu'on peut naviguer sur internet au travers du serveur **SME** et que les routeurs fonctionnent comme ils doivent le faire.

Le seul problème qu'on peut avoir est de trouver une autre connexion internet qui ne soit pas sur le même réseau **IP** que le serveur **SME**. On peut se rendre chez un ami, une bibliothèque publique, un café internet etc...

Une fois cette nouvelle connexion trouvée et sans configurer **Firefox**, on se branche à l'internet et on vérifie qu'on peut accéder au domaine **AinesSansFil.no-ip.org** du serveur **SME**.

Tout est en place pour débiter la vérification:

- Le serveur **SME** est fonctionnel et accède à l'internet. Il est configuré pour accepter un connexion **SSH** de n'importe où de l'internet.
- Les deux routeurs sans fil **E1000-1** et **E1000-2** sont configurés pour accepter les connexions distantes à leur console.
- On est distant et on peut se brancher sur le site du Serveur **SME**.
- PuTTY** est configuré pour établir le tunnel.
- On lance **PuTTY** et on se logue en **SSH** sur le serveur **SME** qui est maintenant distant.
- On configure **Firefox** pour passer par le port **3128** du mandataire **localhost**.
- On entre sur **Firefox** le nom du domaine hébergé par le serveur **SME** distant. La page principale du site est affichée.
- On entre sur **Firefox** l'adresse **IP** du premier ou du deuxième routeur.

Le miracle se produit et **Firefox** affiche la demande de login du routeur sans fils. On se logue et le miracle continue, la page **DD-WRT** du routeur sans fil est affichée.



Encore une fois, hissons la bannière de la victoire.

Crédits

© 2012 **RF-232**.

Auteur: **Michel-André Robillard CLP**

Remerciement: **Tous les contributeurs GNU/GPL.**

Intégré par: **Michel-André Robillard CLP**

Contact: **michelandre at micronator.org**

Répertoire de ce document: E:\000_DocPourRF232_general\RF-232_SME-8.0_Sans-Fil\RF-232_SME_Sans-Fil_Config_Gestion-Distance_20121213_08h51.odt

Historique des modifications:

<i>Version</i>	<i>Date</i>	<i>Commentaire</i>	<i>Auteur</i>
0.0.1	2012-11-10	Début.	M.-A. Robillard
0.0.2	2012-11-16	Ajout de la note sur la passerelle du serveur SME et corrections mineures.	M.-A. Robillard
0.0.3	2012-12-13	Coquille dans l'entête de l'index.	M.-A. Robillard

Index

1		
1024.....	18	
123.123.123.0.....	9	
123.123.123.1.....	9, 23, 24	
123.123.123.10.....	24	
123.123.123.120.....	22	
123.123.123.255.....	9	
192.168.1.0.....	9	
2		
2222.....	16	
255.255.255.0.....	22-24	
255.255.255.1.....	23	
3		
3128.....	18, 20	
6		
64255.....	18	
A		
Add.....	18	
administrateur.....	8	
admin.....	8	
Adresse internet du serveur SME...7		
AinesSansFil.....	16, 24	
AinesSansFil-no-ip.org.....	16	
ainessansfil.no-ip.org.....	13	
AinesSansFil.no-ip.org.....	25	
alias.....	8	
astuce.....	5	
Avancées Réseau.....	20	
Avertissement.....	2	
C		
captures d'écrans.....	5	
client Linux.....	11	
client no-ip.com.....	15	
Commentaire.....	29	
Compilation.....	12	
Complete!.....	11	
Configuration de E1000-1.....	7	
Configuration de E1000-2.....	7	
Configuration de FireFox.....	20	
Configuration de l'interface externe		
.....	22	
Configuration du routeur Linksys.....	23	
Configuration du serveur SME.....	8, 21	
Configuration du tunnel.....	16	
Configuration manuelle du proxy.....	20	
Configuration pour no-ip.com.....	10	
Connection SSH Tunnels.....	18	
Connection SSH X11.....	17	
Connection Type.....	16	
Connexion Paramètres.....	20	
Connexion distante à E1000-1.....	25	
Connexion distante à E1000-2.....	26	
Connexion distante au serveur SME		
.....	25	
Contributeur.....	33	
Conventions.....	5	
cp noip2.....	12	
cpp.....	10, 15	
Création du tunnel.....	24	
Crédits.....	29	
D		
D3128.....	18	
DD-WRT.....	25-27	
DDNS.....	6	
Déconnexion du sans fil.....	25	
Description générale.....	5	
Destination.....	18	
DynDNS.....	6	
Dyndns.org.....	10	
E		
E1000-1.....	7	
echo.....	13	
egrep noip.....	14	
Enable X11 forwarding.....	17	
étape.....	5	
eth1.....	12	
F		
FAI.....	21	
faille de sécurité.....	10	
FireFox.....	20	
FTP.....	5, 8, 10	
fureteur.....	20	
G		
gcc.....	10, 15	
H		
Host name.....	16	
Hôte SOCKS:.....	20	
I		
Installation d'un serveur SME.....	7	
Installation de DD-WRT.....	7	
Installation de gcc.....	10	
Installation du client.....	13	
Introduction.....	5	
Is this ok [y/N]:.....	10	
ISO-8859-1:1998.....	17	
L		
la "Licence".....	33	
Latin-1, West Europe.....	17	
libgcc.....	15	
Linksys.....	21	
Linux client of no-ip.com.....	12	
localhost.....	27	
M		
make.....	12	
make install.....	12	
Manipulation.....	5	
micrologiciel DD-WRT.....	7	
mot de passe.....	12	
mot de passe standards.....	8	
mv /tmp/no-ip2.conf.....	13	
N		
Ne pas utiliser de service DNS		
dynamique.....	10	
no-ip.com.....	8, 10, 11	
no-ip2.conf.....	13	
noip-2.1.9-1.....	12	
noip-duc-linux.tar.gz.....	11	
noip2.....	12, 13	
nom de login.....	12	
note.....	5	
Note au lecteur.....	5	
Notice de Licence.....	33	

O	Sauvegarde.....18	V
Only one host.....13	Save.....16	Vérification à distance.....27
OpenSSH.....6	Saved Sessions.....16	Vérification du client.....14
Options Avancées.....20	script.....14	Vérification du réseau.....7
Outils Options.....20	Sécurité pour la gestion.....9	Vérification en simulant l'internet 21
	Sélectionner Dynamic.....18	
P	Server-Manager.....8, 9, 16	W
Paramètres SSH.....8	Service DNS dynamique.....10	wget.....11
POP.....6	Session.....16	which noip2.....13
port 2222.....8	signal-event post-upgrade..... 11, 13	Window Translation.....17
Ports:.....20	signal-event reboot..... 11, 13	
Pré requis.....7	SME sans fil.....10	Y
procédure.....5	SME-8.0.....7	yum install gcc.....10
proxy localhost.....20	SME-8.0:.....10	
ps.....14	SOCKS v5.....20	-
PuTTY.....7, 16	Source port.....18	-DPREFIX="/usr/local/".....12
pwd.....10, 11	SSH.....16	"
	su.....8	"-C".....15
R		©
ré-amorcer.....11	T	©.....2
reboot.....14	tail.....14	© 2012.....29
recommandation.....5	tar.....12, 13	/
Recréer la config de no-ip.com....15	tar.gz.....12	/etc/rc.local.....13
Réseau Connexion.....20	Téléchargement du client no-ip...11	/temp.....11
réseau local.....9	the "License".....33	/usr/local/bin/noip2.....12
RF-232.....2	Total download size.....10	/usr/local/etc/no-ip2.conf.....13
RFC 2136.....6	tout l'internet.....8	/var/lock/subsys/local.....14
root.....8	tunnel.....16	
rpm -e cpp.....14		
rpm -e gcc.....14	U	
rpm -qa.....15	update interval.....13	
	Utiliser l'adresse IP suivante:.....24	
S	Utiliser une adresse IP fixe.....22	

Licence PDL

Notice de Licence de Documentation Publique

Le contenu de cette documentation est soumis à la Licence de Documentation Publique dans sa version 1.0 (la "Licence"); vous ne pouvez utiliser cette documentation que si vous respectez les conditions de cette Licence. Une copie de la Licence, en anglais, est disponible à l'adresse suivante: <http://www.openoffice.org/licenses/PDL.html>,

La documentation d'origine s'intitule: **RF-232_SME_Sans-Fil_Config_Gestion-Distance**. L'auteur initial de la documentation d'origine est **Michel-André Robillard CLP** copyright © 2012. Tous droits réservés. (Coordonnées de l'auteur initial: michelandre at micronator dot org).

Contributeur(s): _____.

Certaines parties ont été créées par _____ et sont protégées par le droit d'auteur © _____ [Insérer l'année (les années) de création]. Tous droits réservés. (Coordonnées du (des contributeur(s)): _____ [Insérer un lien hypertexte ou adresse(s) courriel]).

NOTE: Le texte de cet annexe-ci peut différer légèrement du texte des notices dans les fichiers de la documentation d'origine. Vous devez utiliser le texte de cet annexe-ci plutôt que le texte de la documentation d'origine pour vos propres modifications.

Public Documentation License Notice

The contents of this Documentation are subject to the Public Documentation License Version 1.0 (the "License"); you may only use this Documentation if you comply with the terms of this License. A copy in English of the License is available at: <http://www.openoffice.org/licenses/PDL.html>,

The Original Documentation is: **RF-232_SME_Sans-Fil_Config_Gestion-Distance**. The Initial Writer of the Original Documentation is **Michel-André Robillard CLP** Copyright © 2012. All Rights Reserved. (Initial Writer contact(s): michelandre at micronator dot org).

Contributor(s): _____.

Portions created by _____ are Copyright © _____ [Insert year(s)]. All Rights Reserved. (Contributor contact(s): _____ [Insert hyperlink/alias]).

NOTE: The text of this Appendix may differ slightly from the text of the notices in the files of the Original Documentation. You should use the text of this Appendix rather than the text found in the Original Documentation for Your Modifications.

