TP de création d'un tunnel PPP à travers `ssh` avec `pppd` sous Solaris 7

Ronan.Keryell@enst-bretagne.fr

—

Département Informatique
École Nationale Supérieure des Télécommunications de Bretagne

—

Mastère IAR2M

28 janvier 2000

Résumé

Ce TP présente l'installation sur Solaris 7 du logiciel libre `pppd` permettant de disposer du protocole PPP pour créer des accès IP via modem ou plus généralement de l'encapsulation multi-protocole dans un flux d'octets (Intranet).

Bien que Solaris 7 dispose déjà d'un démon PPP livré en standard, c'est une version libre qui est ici utilisée car elle est disponible sur de nombreux Unix.

Comme il n'est pas possible d'avoir suffisamment de modems et de lignes téléphoniques, on se restreint à tester un système chiffré de type Intranet au dessus d'Internet avec PPP et `ssh`.

1 Installation de pppd

Dans ce TP certaines choses sont faites avec *vos* droits, d'autres avec le droit de `root`. Afin de faciliter les manipulations, il est conseillé d'avoir plusieurs fenêtres dont une a les droits de `root` via un `su miam`.

Vérifier avec `ifconfig -a` que l'interface `ppp0` n'existe pas (encore).

Créer un répertoire pour faire le TP, par exemple

```
mkdir -p ~/TP/PPP
cd ~/TP/PPP
```

Récupérer sur la page `ftp://cs.anu.edu.au/pub/software/ppp/` la version courante de la distribution de `pppd` sous forme d'archive `tar` comprimée.

Afin d'éviter de surcharger le réseau, il peut est plus simple d'utiliser la version déjà récupérées dans `/usr/local/src/Reseau` que est `ppp-2.3.11.tar.gz`.

Extraire les fichiers des archives dans son répertoire `~/TP/PPP`:

```
xter
gtar zxvf /usr/local/src/Reseau/ppp-2.3.11.tar.gz
cd ppp-2.3.11
```

`gtar` permet de gérer les fichiers d'archivage et en l'occurrence « `x` » spécifie l'extraction de contenu, « `v` » indique que l'on veut de l'information verbeuse sur ce qui est fait et « `f` » précise le nom du fichier d'archive. Comme le fichier d'archive est comprimé (extension du fichier typiquement « `.gz` » ou « `.Z` » l'option « `z` » demande la décompression au vol, « `gtar zxvf` *`fichier`* » est un raccourci pour « `gunzip -c` *`fichier`* `| gtar xvf -` où on passe par `stdout` de `gunzip` et `stdin` de `gtar` respectivement.

Les curieux prendront avantage de la lecture des fichiers `README`, `FAQ` (les *Frequently Asked Questions*), `SETUP` au sujet de PPP et `pppd` en pariculier.

Le répertoire `etc.ppp` contient des fichiers types qui iront dans `/etc/ppp`. Le répertoire `scripts` donne d'autres fichiers types et un fichier `README` avec d'autres exemples tels que le rappel automatique ou l'utilisation du langage `expect` gérant des connexions sécurisées par carte d'identification.

Afin d'utilise le compilateur `gcc`, décommenter les 2 dernières lignes du fichier `svr4/Makedefs` en :

```
CC = gcc
COPTS = -O2
```

Comme chaque élève installe PPP sur sa machine, l'installation a lieu dans `/usr` au lieu du classique `/usr/local` partagé par tout le monde. Pour ce faire, modifier dans le même fichier `svr4/Makedefs` les valeurs de `BINDIR` et `MANDIR` en :

```
BINDIR = /usr/bin
MANDIR = /usr/man
```

Modifier aussi `pppd/Makefile.sol2` et `pppd/Makefile.sol2` en commentant la ligne avec

```
COPS=
```

Lancer la compilation avec

```
./configure
make
```

Installer (sous les droits de `root`) avec :

```
make install
```

Si on veut accéder aux manuels des différentes commandes installées qui sont mises en section 8, il faut utiliser l'option `-s 8` de `man` comme par exemple :

```
man -s 8 pppd
```

On peut récupérer le fichier `http://www.cri.ensmp.fr/~keryell/systeme/PPP/etc.ppp.tar.gz` et en faire un `gtar zxvf` chez vous comme exemple de fichiers de configurations même si ces fichiers sont plutôt spécifiés pour l'utilisation avec modem.

Comme l'interface est créée dynamiquement on ne peut pas encore la voir avec un `ifconfig -a`.

Penser à avoir une fenêtre séparée pour voir d'éventuels messages d'erreur en lançant :

```
tail -f /var/adm/messages
```

qui aura pour effet d'afficher en permanence les messages du système rajoutés à ce fichier par le démon `pppd` et autre `chat`. Cela nécessite d'avoir configuré `syslogd` en mode verbeux comme indiqué en cours mais cela devrait déjà être le cas avec l'installation du système faite au mastère.

2 Création d'un Intranet au dessus d'Internet

On va essayer de créer un tunnel au dessus d'Internet en faisant passer le traffic IP Intranet entre 2 machines d'Internet reliées par la commande `ssh` qui permet de lancer des commandes à distance sous Unix tout en détournant ses `stdin`, `stdout` et `stderr` de manière chiffrée. On réalisera ainsi un tunnel sécurisé au dessus d'Internet.

Pour des raisons de simplicité du TP, nos 2 machines distantes sur Internet seront en fait 2 machines locales. Choisir un(e) collègue dont la machine sera l'autre bout de votre Intranet par rapport à votre propre machine.

Si on considère que l'autorisation de la connexion est faite au niveau de `ssh` on peut omettre l'utilisation de l'authentification style PAP ou CHAP au niveau de `pppd`. Pour ce faire on rajoutera dans le fichier `/etc/ppp/options` la ligne

```
noauth
```

On peut dans un premier temps tester le système avec `rsh`, c'est à dire non chiffré, puis lorsque cela fonctionne avec `ssh` que l'on installera en s'aidant par exemple du TP de sécurité.

Vérifier que `rsh` fonctionne bien, par exemple avec :

```
keryell@voltaire PPP/ppp-2.3.5: rsh oberkampf uname -a
SunOS oberkampf.ensmp.fr 5.7 Generic i86pc i386
keryell@voltaire PPP/ppp-2.3.5: rsh oberkampf ls
Mail
TP
bin
db.cache
hosts
mbox
nsmail
```

Dans ces exemples, les commandes `uname` et `ls` sont lancées à distance et leur `stdin`, `stdout` et `stderr` détournés afin d'interagir et d'afficher le résultats localement. Les entrées-sorties sont transférées par la commande `rsh` sur les entrées-sorties locales. Il se peut qu'il y ait un problème de droit. Si tel est le cas, enrichir votre `~/.rhosts` sur la machine destination.

Nous allons donc lancer un `pppd` à distance sur B et connecter aux entrées-sorties standard de `rsh` un `pppd` local sur la machine A. Ainsi, le `pppd` local communiquera au `pppd` distant via `rsh` et assurera le transport de trafic IP entre A et B via le canal `rsh`. Ceci est effectué par le lancement sur A de la commande :

```
pppd pty 'rsh B pppd notty'
```

Au préalable il va falloir attribuer des adresses à chaque bout du tunnel. On va les allouer dans une plage d'adresses privées RFC 1597. Le bout sur A s'appellera Apriv et sur B Bpriv numérotés par exemple respectivement `10.0.0.1` et `10.0.0.2`. Cela peut être fait en rajoutant par exemple dans le fichier `/etc/ppp/options` de A la ligne

```
10.0.0.1:10.0.0.2
```

Regarder les tables de routages établies par les `pppd` de part et d'autre du tunnel. Faire des mesures de performances avec des commandes du type

```
ping -sv B 60000
ping -sv Bpriv 60000
```

Vous pouvez regarder ce qui passe dans le tunnel avec des commandes du genre `snoop -d ppp0` ou `tcpdump -i ppp0`.

Une fois que cela fonctionne bien, basculer dans une solution `ssh` avec distribution de clés préalables.

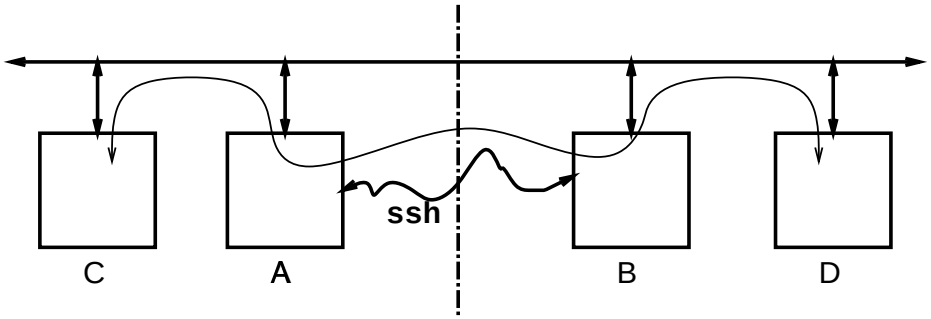

FIG. 1 – *Petit intranet.*

Créer une topologie de votre Intranet que vous mettrez en œuvre en rajoutant d'autres machines en utilisant des liens Intranet de collègues en s'inspirant par exemple de la figure 1. Le routage sera statique et réalisé en utilisant la commande `route add` avec vos collègues administrant d'autres nœuds de votre Intranet. L'établissement automatique des routes lors de la connexion pourra être gérée dans les scripts `ip-up` et `ip-down`. On peut vérifier les chemins parcourus avec la commande `traceroute`.

Pour simplifier on va construire et tester l'Intranet progressivement en ayant déjà mis en place le tunnel entre Apriv et Bpriv :

```
C> traceroute B
C> traceroute D
C> route add B A 1
C> route add D A 1
C> traceroute D
D> traceroute C
A> route add D Bpriv 1
C> traceroute D
D> traceroute C
D> route add A B 1
D> route add C B 1
C> traceroute D
D> traceroute C
A> route add C Apriv 1
C> traceroute D
D> traceroute C
```

Dans un vrai Intranet au dessus d'Internet, toutes les machines auraient des adresses privées sauf A et B qui auraient des adresses publiques pour faire leur lien `ssh` au dessus du réseau Internet.