Bases des services réseaux
Module M2106

Travaux pratiques

IUT de Villetaneuse — R&T — DUT R&T

Camille Coti
camille.coti@iutv.univ-paris13.fr

1 Configuration automatique des machines

Le but de ce TP est de mettre en place un réseau constitué de plusieurs machines configurées automatiquement.

Ce TP se déroule grâce au simulateur de réseaux marionnet disponible gratuitement sous licence GPL, voir `www.marionnet.org`. Rappel : le mot de passe de root d'une machine virtuelle est `root`.

Le réseau que vous devez utiliser est pré-configuré. Récupérez le fichier à l'adresse `http://www.lipn.fr/~coti/cours/M2106_TP_DHCP.mar` dans votre répertoire personnel. Démarrez Marionnet et ouvrez ce fichier. Vous devriez obtenir le réseau représenté à la figure 1 (les numéros des interfaces ne sont pas les memes).

Ce réseau est composé des éléments suivant :
— Réseau 1 : 192.168.1.0/24, quatre machines (dont une sera le serveur) reliées par un switch
— Réseau 2 : 192.168.2.0/24, trois machines reliées par un switch
— Réseau 3 : 192.168.3.0/24, trois machines reliées par un switch
— Un routeur reliant les trois réseaux 1, 2 et 3

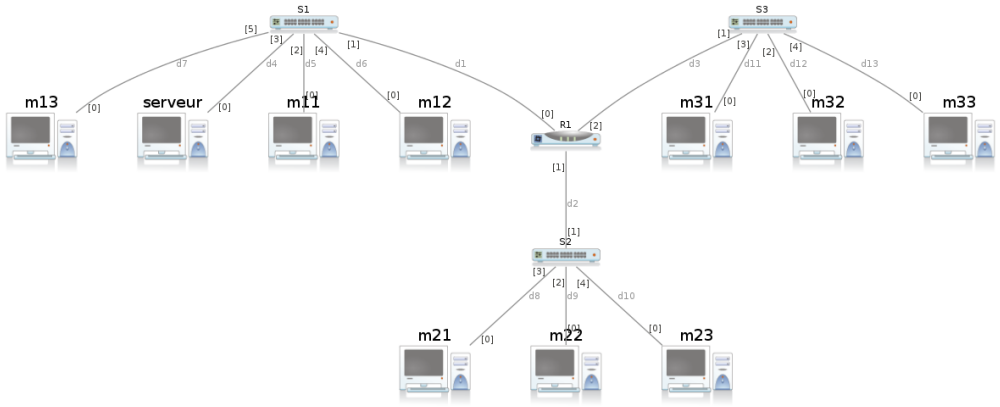

FIGURE 1 – Réseau à mettre en place pour le TP

1 Plan d'adressage et routage statique

1. Proposez des configurations IP pour toutes les machines et les interfaces du routeur. Donnez les tables de routage des machines et du routeur. Ne faites pas la configuration des machines.
2. Démarrez le switch 1, le routeur et le serveur.
3. Configurez les interfaces et la table de routage du routeur, ainsi que la machine serveur. Quelles sont les commandes utilisées ?
   Si une interface réseau apparait "DOWN", vous pouvez l'activer avec `ip link set ethX up`, si l'interface s'appelle ethX.

2 Serveur DHCP

2.1 Service DHCP dans le même sous-réseau

1. La configuration du serveur DHCP se trouve dans le répertoire `/etc/dhcp`. Éditez le fichier `/etc/dhcp/dhcpd.conf` et lisez les indications données en commentaires.
2. Le serveur DHCP peut fournir la configuration DNS (les adresses des serveurs de noms). Quelle ligne faut-il modifier pour fournir comme serveur DNS l'adresse 10.0.2.3 dans le domaine portant le nom "monreseau.org" ?
3. Quelle ligne faut-il décommenter pour définir le serveur DHCP comme étant le serveur officiel du réseau local ?
4. Les adresses IP sont attribuées pour un certain temps au-delà duquel les clients doivent émettre une nouvelle requête. On parle de *bail DHCP*, ou *lease* en anglais. Dans le fichier de configuration, à combien est ce bail ?
5. Les sous-réseaux (*subnets*) sont déclarés individuellement dans le fichier `/etc/dhcp3/dhcpd.conf`. Vous devrez donc déclarer ici trois sous-réseaux. Le réseau 3 concerne des machines qui font partie du même réseau que le serveur. Leurs requêtes vont donc lui arriver directement.

   Un *subnet* se déclare de la façon suivante :

   ```
   subnet <adresse du reseau> netmask <masque de sous-reseau> {
       range  <premiere adresse> <derniere adresse>;
       option routers <passerelle du reseau>;
       option domain-name <nom de domaine>;
       option domain-name-servers <liste de serveurs DNS>;
   }
   ```

   Dans ce fichier de configuration, définissez un sous-réseau simple pour le réseau 3, en permettant de fournir 100 adresses. Attention : votre serveur dispose d'une adresse IP configurée statiquement dans ce réseau, cette adresse ne doit pas faire partie de l'intervalle d'adresses IP attribuées dynamiquement. N'oubliez pas de définir la passerelle par défaut pour ce réseau.
6. Il est nécessaire de spécifier au serveur DHCP sur quelle interface il doit écouter les requêtes entrantes. Sur quelle interface va-t-il écouter ? Modifiez le fichier `/etc/default/dhcp3-server` pour le spécifier. Si le fichier n'existe pas, créez-le. Il doit contenir :

   ```
   INTERFACES="NOM DE L'INTERFACE"
   ```

   En remplaçant par le nom de l'interface concernée.
7. Le système de journalisation est très utile pour la configuration et l'exploitation de services. Sur votre serveur, c'est `rsyslog` qui est installé. Démarrez-le. Sur ces machines, le système n'utilise pas le système de gestion de services systemd mais le vieux SysV init. Les services se démarrent et s'arrêtent en lançant les scripts qui se trouvent dans `/etc/init.d/` et en leur passant la commande `start`, `stop` ou `restart`.

   ```
   serveur:~# /etc/init.d/rsyslog restart
   ```

8. Redémarrez le serveur DHCP. Si tout se passe bien, il ne doit pas y avoir de message d'erreur après le redémarrage (le message d'erreur au moment de l'arrêt n'est pas grave). Si il y a une erreur, corrigez-la.

   ```
   serveur:~# /etc/init.d/dhcpd restart
   Stopping DHCP server: dhcpd3 failed!
   Starting DHCP server: dhcpd3.
   ```

NB : à chaque fois que vous modifiez la configuration d'un serveur, vous devez le relancer pour que le fichier de configuration soit lu à nouveau et que les modifications soient prises en compte.

9. Sur le serveur, regardez la fin du fichier de journalisation (également appelée log) en mode défilant avec :

```
serveur:~# tail -f /var/log/messages
serveur:~# tail -f /var/log/syslog
```

10. Démarrez les trois autres machines du réseau 1.
11. Sur chacune des trois machines, obtenez une configuration IP dynamique avec `dhclient`, en lui passant en paramètre l'interface sur laquelle il doit envoyer ses requêtes DHCP.

```
m11:~# dhclient eth0
```

12. Que constatez-vous dans le log du serveur ? Détaillez l'affichage correspondant à la requête DHCP émise par une machine.

2.2 Service DHCP dans un autre sous-réseau

13. Sur le serveur, définissez la configuration du serveur DHCP pour le réseau 1. Les adresses attribuées devront être entre 192.168.1.1 et 192.168.1.100.
14. Redémarrez le serveur DHCP.
15. Vous pouvez constater que le serveur et les six machines des réseaux 1 et 2 ne sont pas sur les mêmes réseaux. Pour que les requêtes DHCP de ces six machines puissent arriver au serveur, il faut que le routeur les transfère. Pour celà, le routeur dispose de l'utilitaire `dhcprelay`. Il s'utilise de la manière suivante :

```
dhcprelay <liste des interfaces vers les clients> <interface vers le serveur>
```

Les interfaces réseaux allant vers les réseaux des clients sont listées en les séparant par des virgules (attention, pas d'espace). Lancez `dhcprelay` pour relayer les requêtes en provenance des réseaux 1 et 2 vers le serveur.

16. Nous allons maintenant nous intéresser aux machines du réseau 1. Démarrez les trois machines et leur switch.
17. Sur le serveur, regardez la fin du fichier de journalisation (également appelée log) de la même façon qu'à la question 9
18. Sur les trois machines du réseau 3, obtenez une configuration IP automatique avec `dhclient` de la même façon qu'à la question 11.
19. Depuis quelle machine le client voit-il venir l'acquittement ?
20. Que constatez-vous dans le log du serveur ? Détaillez l'affichage correspondant à la requête DHCP émise par une machine et ce qui est différent des requêtes émises depuis le réseau 1.
21. Sur une machine client, regardez la configuration DNS dans le fichier `/etc/resolv.conf`. Que constatez-vous ?
22. Laissez tourner votre système un certain temps et gardez un oeil sur le fichier de log du serveur DHCP. À l'expiration du bail des clients, vous devriez vour passer les requêtes correspondant au renouvellement de leur configuration. En quoi sont-elles différentes des demandes initiales ?

3 Restrictions et adresses attribuées statiquement

1. Dans le réseau 2, on souhaite être plus restrictifs et n'attribuer des adresses IP qu'aux machines que l'on connait. En outre, ces machines se verront attribuer toujours la même adresse IP. Le réseau 2 aura par ailleurs un bail d'une durée plus longue : on utilisera une durée par défaut de 3000 secondes, au maximum 6000 secondes. Dans la déclarations de votre subnet, ajoutez l'option `deny unknown-clients` pour ne pas accepter les clients inconnus dans ce réseau.

   En lisant les exemples donnés dans le fichier de configuration du serveur DHCP et notamment les sections `host`, définissez un sous-réseau spéficique pour le réseau 2 et deux hôtes `riri` et `fifi` correspondant à deux des machines de ce réseau. Spécifiez-leur l'adresse 192.168.2.11 pour la première, 192.168.2.12 pour la deuxième.

   N'oubliez pas de redémarrer votre serveur DHCP une fois les modifications effectuées afin de les prendre en compte.

2. Allumez toutes les machines du réseau 2 et leur switch. Sur les trois machines, effectuez une demande de configuration automatique. Que se passe-t-il ? Que se passe-t-il côté serveur (fichiers `/var/log/messages` et `/var/log/syslog` ?

3. Modifiez la configuration du serveur pour définir un troisième hôte `loulou` correspondant à la troisième machine. Attribuez-lui l'adresse IP 192.168.3.13.

4. Selon vous, que doit prendre en compte l'administrateur réseau lorsqu'il fixe la durée du bail DHCP ? Quels sont les avantages et les inconvénients d'un bail long ? D'un bail court ?

5. Selon vous, dans quelles situation sera-t-il plus intéressant d'attribuer des adresses IP à tout le monde (situation du réseau 1) ? Dans lesquelles sera-t-il plus intéressant d'être restrictif et de lister exhaustivement les hôtes (situation du réseau 2) ?

2 DNS

(Franck Butelle : `franck.butelle@iutv.univ-paris13.fr`)

Le but de ce TP est de créer une hiérarchie DNS de la forme `mach1.g2.p13.fr`.

Ce TP se déroule grâce au simulateur de réseaux marionnet disponible gratuitement sous licence GPL, voir `www.marionnet.org`. Rappel : le mot de passe de root d'une machine virtuelle est `root`.

Créez deux machines virtuelles (avec les valeurs par défaut) reliées par un switch.

1 Nommage statique

On utilisera les noms suivants (x est le numéro de la machine, y est le numéro du groupe) : mstat$x$.gy.p13.fr, alias mstat$x$. Avec marionnet, on commence par le groupe $y = 1$.

1. Attribuez des adresses IP aux machines. Les numéros attribués doivent être de la forme 10.10.y.x/16, avec y le numéro de groupe et x le numéro de la machine (1, 2,...) (commande `ifconfig eth0...`).
   Quel est le masque équivalent sous forme décimale pointée ?
2. Consultez le fichier `/etc/nsswitch.conf` et trouvez la ligne qui détermine l'ordre d'utilisation des méthodes de résolution (hosts). Assurez-vous qu'on utilise d'abord la résolution statique, puis la résolution par serveur DNS. Si le fichier /etc/resolv.conf existe, **supprimez-le** dans toutes les machines virtuelles (on le reconstruira plus tard).
3. Éditez le fichier `/etc/hosts` pour ajouter le nom `mstat1.gy.p13.fr` à la machine numéro 1 qui pointe sur l'adresse IP 10.10.y.1. Testez le bon fonctionnement par ping.
4. Faites la même opération sur les autres machines pour que chaque machine connaisse son nom. Testez. Que se passe-t-il quand la machine 2 fait `ping mstat1.gy.p13.fr` ? Comment corriger ce problème ?

2 Serveur DNS maître (ou primaire/autorité)

— Les noms donnés par le DNS seront de la forme : mach$x$.gy.p13.fr, alias mx.gy.p13.fr, alias un nom au choix des utilisateurs (par exemple tintin.gy.p13.fr) ;
— Les machines numéros 1 auront de plus l'alias ns.gy.p13.fr ;
— On pourra récupérer des squelettes de fichiers de configuration dans `/home/TP/TPINFO/butelle/Reseaux/TP_DNS`. Vous pourrez copier ces fichiers presque directement dans les machines virtuelles grâce à un montage spécial déjà en place. Copiez les fichiers que vous voulez envoyez dans vos machines virtuelles dans le répertoire `/tmp/marionnet.<numero>.dir/<nom projet>/hostfs/<numero machine>`. Attention le numero de machine selon marionnet est (normalement) dépendant de l'ordre de création de la machine virtuelle. Depuis la machine virtuelle, vous devriez voir apparaître les fichiers dans `/mnt/hostfs`. Cela fonctionne dans les deux sens et donc vous pourrez sauver vos fichiers dans la machine hôte puis sur votre compte.

1. Créer un répertoire qui contiendra les définitions des fichiers de zone sur la machine 1 : `/var/named/maitre`.
   Créer un fichier de configuration pour BIND (programme `named`) `/etc/bind/named.conf` :

Fichier /etc/bind/named.conf

```
// Définition de zone pour le groupe y
options {
    directory "/var/named";
};
zone 127.in-addr.arpa. {
    type master;
    file "maitre/127";
};
zone gy.p13.fr. {
    type master;
    file "maitre/gy.p13.fr"; // nom de fichier conseillé
};
zone y.10.10.in-addr.arpa. {
    type master;
    file "maitre/10.10.y"; // nom de fichier conseillé
};
```

Ensuite, il faut créer les fichiers suivants : `/var/named/maitre/127`, `/var/named/maitre/gy.p13.fr`, `/var/named/maitre/10.10.y`, en vous appuyant sur le cours et les contraintes suivantes :

— numéro de série au format usuel
— temps de rafraichissement (refresh) de 120 s
— délai entre essais infructueux (retry) de 60 s
— délai d'expiration définitif (Expire) de 200 s
— TTL de 180 s.
— adresse mail du responsable : root@mach1.g*y*.p13.fr
— serveur de mail (priorité 10) du domaine g*y*.p13.fr. : mach1.g*y*.p13.fr.
— enregistrement TXT : "domaine du groupe *y*"

2. (re)Démarrez ensuite le serveur de nom : `/etc/init.d/bind9 restart`. Attention le message OK est parfois faux, voir toute de suite la fin du fichier `/var/log/messages` (ou ici `/var/log/syslog`).
3. Testez votre serveur en cherchant l'enregistrement TXT rattaché à votre groupe : `host -t txt gy.p13.fr 10.10.y.1`. Essayez ensuite d'autres requêtes (enregistrement de type NS, SOA, adresse de mach1.g*y*.p13.fr).
4. Comment faire la résolution inverse d'adresses de deux façons différentes par la commande host (voir man host) ?
5. Configurez la deuxième machine pour qu'elle utilise le serveur DNS en mettant la ligne `nameserver` *`AdresseIPServeur`* dans le fichier `/etc/resolv.conf`. Vérifiez le bon fonctionnement de la résolution de nom.
6. Refaites les tests en faisant des captures de trames (avec wireshark). Le filtre de capture que vous pouvez utiliser est `port 53`. Réalisez ces captures à partir du serveur. Observez les **quatre** parties (S1,S2,S3,S4) des requêtes et réponses.
7. Que donne un `ping mach1` ? Pourquoi ?
8. Ajoutez `search gy.p13.fr` dans `/etc/resolv.conf`. Faites à nouveau un `ping mach1`. Que se passe-t-il si l'on fait `ping mach6` ?
9. Paramétrez aussi le maître pour qu'il utilise son propre serveur DNS. Vérifiez que cela fonctionne.
10. Concluez par un plan d'adressage et un plan de nommage.

3 Serveur DNS cache

1. Créez un serveur DNS cache (voir cours) sur la machine `mach2`. Créez une nouvelle machine mach3 qui interroge par défaut le serveur DNS cache de mach2. Avec des captures de trames, observez l'effet de cache.
2. Quel est le Userid du démon named/bind ? A quelle identité correspond ce UID ?
3. Vérifiez le contenu du cache par `rndc dumpdb` et en lisant le fichier texte généré `/var/named/named_dump.db`. Attention aux droits d'écriture dans ce répertoire !
4. A quoi correspond le champ numérique de chaque ligne (sauf commentaires) de ce fichier ? Vérifiez en consultant plusieurs fois ce cache !

4 Serveur DNS esclave (secondaire)

1. Transformez le serveur cache en serveur esclave (voir fichier suivant). Redémarrez le serveur de `mach2` par `/etc/init.d/bind9 restart` et observez ce qui se passe au démarrage de ce service (capture de trames active).

Fichier /etc/bind/named.conf

```
// Définition d'un serveur esclave pour la rangée y
options {
    directory "/var/named";
    forwarders {10.10.y.1;};
};
zone gy.p13.fr. {
    type slave;
    file "slave/gy.p13.fr";
    masters {10.10.y.1;};
};
zone y.10.10.in-addr.arpa. {
    type slave;
    file "slave/10.10.y";
    masters {10.10.y.1;};
};
```

2. Il est probable que, même si vous voyez les trames portant des transfert de zone passer, les fichiers `slave/gy.p13.fr` et `slave/10.10.y` ne soient pas créés. C'est normal ! Retournez à la question sur l'UID du démon named pour comprendre.
3. Vérifiez ce qui se passe dans le cas d'une requête sur une zone non-esclave (mais connue du serveur maître).
4. Vérifiez le contenu du cache par `rndc dumpdb` et en lisant le fichier généré `/var/named/named_dump.db`. Expliquez le résultat obtenu.
5. Vérifiez que l'arrêt du serveur primaire n'empêche pas le serveur secondaire de fonctionner... Combien de temps ?
6. Rajoutez une machine bidon au fichier de zone de votre DNS maître sans changer le numéro de version. Redémarrez le serveur. Pourquoi cette modification n'est pas prise en compte par le serveur esclave ? Comment corriger ce problème ?
7. Essayez d'observer les requêtes de mise à jour émises par le serveur esclave.

5 Domaine p13.fr

Ajoutez deux machines virtuelles reliées au switch. Configurez une des deux pour être serveur maître du domaine g2.p13.fr.

1. L'autre machine sera un serveur serveur.p13.fr, maître, d'adresse IP 10.10.0.1 pour TOUT le domaine p13.fr (qui inclut g1.p13.fr et g2.p13.fr). Modifiez votre installation pour que toutes vos machines puissent maintenant reconnaître toutes les machines : le serveur serveur.p13.fr doit faire délégation de domaine vers m1.g1.p13.fr pour le domaine g1.p13.fr etc.

Fichier /etc/bind/named.conf

```
// Définition de zone p13.fr
options {
    directory "/var/named";
};
zone 127.in-addr.arpa. {
    type master;
    file "maitre/127";
}
zone p13.fr. {
    type master;
    file "maitre/p13.fr";
}
zone 10.10.in-addr.arpa. {
    type master;
    file "maitre/10.10";
}
```

Fichier /var/named/maitre/10.10

```
$ORIGIN 10.10.in-addr.arpa.
$TTL 180
@  IN  SOA serveur.p13.fr. jo.serveur.p13.fr. aaaammjj01 120 60
300 180
       NS    serveur.p13.fr.
1.0    PTR   serveur.p13.fr.
1      NS    mach1.g1.p13.fr.
1.1    PTR   mach1.g1.p13.fr.
2      NS    mach1.g2.p13.fr.
1.2    PTR   mach1.g2.p13.fr.
```

Fichier /var/named/maitre/p13.fr

```
$ORIGIN p13.fr.
$TTL 180
@  IN  SOA serveur.p13.fr. jo.serveur.p13.fr. aaaammjj01 120 60
300 180
       NS    serveur.p13.fr.
       TXT   "Domaine general p13.fr"
serveur  A     10.10.0.1
ns       CNAME serveur
g1       NS    mach1.g1
mach1.g1 A     10.10.1.1
g2       NS    mach1.g2
mach1.g2 A     10.10.2.1
```

2. Grâce à l'analyse de trame déterminez si les requêtes sont faites en mode récursif ou en mode itératif.
3. Completez le plan d'adressage de votre réseau.

3 Annuaire et système de fichiers en réseau

Le but de ce TP, s'étalant sur deux séances de 3H chacune, est de mettre en place un système d'annuaire en réseau des utilisateurs et des machines (NIS) et un système de fichiers en réseau (NFS).

Ce TP se déroule grâce au simulateur de réseaux marionnet disponible gratuitement sous licence GPL, voir `www.marionnet.org`. Rappel : le mot de passe de root d'une machine virtuelle est `root`.

Le réseau que vous devez utiliser est pré-configuré. Copiez le fichier `/home/TP/TPRT/M2106/M2106_TPNISNFS.mar` dans votre répertoire personnel. Démarrez Marionnet et ouvrez ce fichier. Vous devriez obtenir le réseau représenté à la figure 2.

Ce réseau est composé des éléments suivant :
— Un commutateur 6 ports (switch)
— Quatre machines reliées au switch : l'une de ces machines sera le serveur (vous pourrez l'appeler, par exemple, `serveur`) et les trois autres machines sernt des postes clients du réseau (vous pourrez les appeler, par exemple, `athos`, `porthos` et `aramis`).
Le réseau que vous obtenez ressemble à la figure 2.

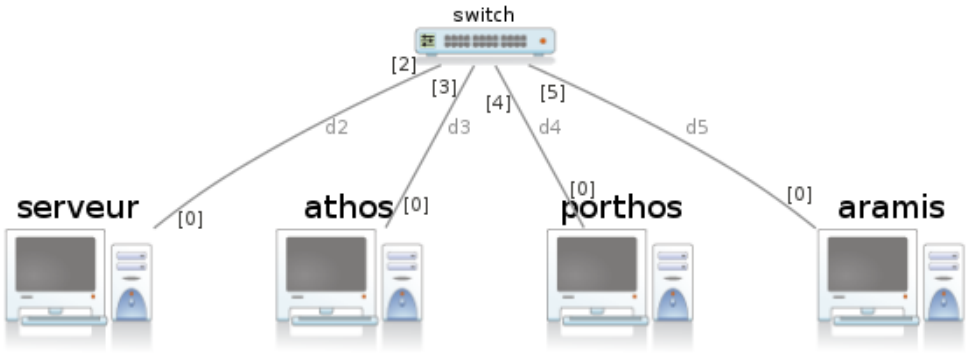

FIGURE 2 – Réseau à mettre en place pour le TP

1 Adressage et routage

Les quatre machines font partie du réseau 198.168.1.0/24.

1. Proposez des configurations IP pour toutes les machines. Donnez les tables de routage des machines.
2. Démarrez le commutateur et le serveur.
3. Configurez l'interface réseau de la machine serveur. Quelles sont les commandes utilisées ?
4. Démarrez `athos`, `porthos` et `aramis`. Configurez leur interface réseau et leur table de routage.
5. Vérifiez que les machines communiquent bien entre elles avec l'aide de la commande `ping`.

2 Annuaire des utilisateurs et résolution DNS avec NIS

Dans cet exercice, vous allez mettre en place, sur le serveur, un système d'annuaire spécifique à Unix : NIS. Cet annuaire vous servira pour gérer les utilisateurs de votre réseau et pour effectuer les résolutions DNS des noms des machines de votre réseau. Le serveur NIS sera la machine que vous avez appelée `serveur`. Les trois autres machines (`athos`, `porthos` et `aramis`) seront les clients.

2.1 Gestion des utilisateurs

1. NIS utilise les appels de procédure à distance (Sun RPC). Les RPC utilisent un démon spécifique appelé `portmapper`. Vérifiez que le `portmapper` tourne bien sur le serveur avec la commande `rpcinfo -p`. Quels services RPC sont actuellement en train de tourner sur votre serveur ?
2. Il existera dans votre réseau deux types d'utilisateurs :
   — Les utilisateurs *locaux*, dont l'existence est circonscrite à une machine ;
   — Les utilisateurs *réseaux*, qui existent sur tout le réseau et peuvent s'authentifier sur n'importe quelle machine avec leur login et leur mot de passe.
   Chaque utilisateur (local ou réseau) dispose d'un *user id* (ou iud) unique qui sert à l'identifier. Afin de ne pas risquer de collision entre les utilisateurs locaux et les utilisateurs réseau, il faut définir des intervalles de valeurs acceptables pour les user ids. La même chose s'applique pour les groupes : les groupes disposent d'un *group id* (ou gid), et il existe des groupes locaux et des groupes réseaux. Ces intervalles pour les utilisateurs et les groupes locaux sont définis dans le fichier `/etc/login.defs`. Modifiez ce fichier sur vos quatre machines pour que les iud locaux soient compris entre 100 et 1000 et que les gid locaux soient compris entre 100 et 1000.
3. Quel est l'uid de `root` ?
4. Les utilisateurs locaux sont créés avec la commande `useradd`. Sur Athos, créez un utilisateur local nommé par exemple `figatellix` et vérifiez son uid et son gid avec la commande `id`.
5. Avec `rpcinfo -p`, quels services RPC tournent désormais sur le serveur ?
6. Vous aurez besoin d'avoir un nom de domaine "fully qualified" (FQDN, ou Fully Qualified Domain Name) sur vos machines. Avec la commande `domainname` ou `hostname -d`, vérifiez quel est le nom de domaine de vos machines. Si vous n'en avez pas, mettez-le à `monreseau.org` en le mettant dans votre fichier `/etc/defaultdomain` et en éditant votre fichier `/etc/hosts` :

   ```
   127.0.0.1       localhost
   127.0.0.1       athos.monreseau.org     athos
   ```

7. Vérifiez qu'il a bien été pris en compte par NIS avec `ypdomainname`
8. Les données de votre serveur NIS sont stockées dans le répertoire `/var/yp`. Vous y trouverez notamment le fichier `Makefile`, qui est utilisé pour générer les maps, et les maps elles-mêmes. Vous avez précédemment configuré vos machines pour définir l'intervalle des uids et gids des utilisateurs locaux. Les uids et gids des utilisateurs NIS sont dans un intervalle défini dans ce `Makefile`. Éditez ce fichier afin de définir des intervalles tels qu'il n'y ait pas de collision possible entre les uids et gids locaux et réseaux.
9. Le serveur NIS doit être également client ; il est client de lui-même. Le serveur NIS à interroger est défini dans le fichier `/etc/yp.conf`. Modifiez ce fichier afin d'utiliser l'hôte local (`127.0.0.1` comme serveur.
10. Définissez-vous comme comme serveur maître NIS (par opposition à serveur esclave ou client) en éditant le fichier `/etc/default/nis`.

11. Pour des raisons évidentes de confidentialité, il faut définir des restrictions sur les clients auxquels le serveur va accepter de répondre. Dans le fichier `/etc/ypserv.securenets`, laissez la ligne concernant le réseau local et ajouter une ligne pour accepter les clients provenant du réseau local.
12. Les maps seront stockées dans le répertoire `/var/yp/<domaine>`. Si votre réseau a le nom de domaine `monreseau.org`, créez le répertoire `/var/yp/monreseau.org`.
13. Initialisez votre système avec la commande `/usr/lib/yp/ypinit -m`. Il vous sera demandé d'entrer la liste des serveurs NIS du réseau : quelle est-elle ?

    Vous aurez quelques messages d'erreurs, qui correspondent à des éléments qui ne sont pas configurés pour le moment :

```
failed to send 'clear' to local ypserv: RPC: Program not registeredUpdating
    passwd.byuid...
```

14. Lisez l'affichage produit par la commande précédente. Quels fichiers ont été générés ?
15. Redémarrez le serveur NIS :

```
serveur:~# /etc/init.d/nis restart
```

16. Quels services sont démarrés ? Regardez avec `rpcinfo -p` quels nouveaux services RPC sont en train de tourner.
17. Maintenant que les services tournent, relancez la commande `/usr/lib/yp/ypinit -m`. Il ne devrait plus y avoir d'erreurs.
18. Sur les machines clientes `athos`, `porthos` et `aramis`, éditez le fichier `/etc/nsswitch.conf`. Ce fichier définit comment les utilisateurs sont authentifiés, comment est effectuée la résolution des noms de domaines, etc. Modifiez ce fichier pour que les utilisateurs soient authentifiés d'abord en utilisant le mode "classique" (`compat`), puis NIS.
19. De même que sur le serveur, éditez le fichier `/etc/yp.conf` et définissez la machine `serveur` comme serveur. Attention, vous n'avez pas encore de résolution DNS disponible : vous devez donc utiliser son adresse IP. En cas de doute, vous pouvez vérifier si votre fichier `/etc/yp.conf` avec `ypbind -c` ('c' comme "check").
20. Sur les machines clientes, redémarrez le service NIS :

```
athos:~# /etc/init.d/nis restart
```

21. La commande `ypcat -x` permet de récupérer la liste des maps disponibles sur le NIS. Sur une machine cliente, essayez d'utiliser cette commande. Quelles maps peut-on obtenir ? À quoi correspondent-elles ?
22. Sur le serveur, créez un nouvel utilisateur, nommé par exemple `salamix`. Laissez les valeurs par défaut, en particulier concernant son répertoire personnel. Que constatez-vous vis-à-vis de NIS ?
23. Vérifiez que l'iud de Salamix est bien dans l'intervalle configuré pour les utilisateurs NIS
24. Il faut maintenant mettre à jour les maps sur le serveur, afin de prendre en compte le nouvel utilisateur. Placez-vous dans le répertoire `/var/yp` et tapez la commande `make`. Que se passe-t-il lors de la mise à jour des maps ?
25. La map `passwd` a la même structure que le fichier `/etc/passwd`. Obtenez-la avec `ypcat` sur le serveur pour voir ce qui a été généré par la mise à jour des maps.
26. Faites la même chose sur les autres machines.
27. Plus tôt dans ce TP, vous avez créé un utilisateur `figatellix`. Pourquoi n'apparaît-il pas dans la sortie de `ypcat`, alors que `salamix` apparaît ?

28. Sur le serveur, créez un groupe NIS `utilisateurs` dans lequel vous mettrez votre utilisateur `salamix`. N'oubliez pas de mettre à jour les maps de votre serveur. Attention au group id de votre nouveau groupe : vous aurez peut-être besoin de le forcer à une valeur particulière pour qu'il soit bien dans l'intervalle des groupes NIS.
29. La commande `ypwhich` permet de savoir à quel serveur un client est associé. Utilisez-là sur vos machines clientes pour vérifier qu'elles sont bien associées à votre serveur.

2.2 Résolution des adresses

Le NIS permet d'effectuer la correspondance entre des adresses IP et des noms symboliques. Pour cela, nous allons poursuivre ce qui a été fait précédemment en utilisant d'autres maps.

1. Les maps NIS sont générées sur le serveur à partir du fichier `/etc/hosts` du serveur. Modifiez ce fichier afin d'insérer la résolution des noms des machines et du routeur de votre réseau.
2. Placez-vous dans le répertoire `/var/yp` et générez la mise à jour des maps avec la commande `make`. Quels fichiers sont concernés ? Qu'en déduisez-vous sur les fichiers concernant les informations sur la résolution des noms de machines ?
3. Modifiez le fichier `/etc/nsswitch.conf` afin d'effectuer la résolution DNS des noms d'hôtes dans l'ordre suivant : fichiers locaux (`files`), NIS (`nis`) et enfin DNS (`dns`).
4. Essayez d'utiliser un nom de machine pour communiquer entre deux machines, par exemple avec `ping`. Que se passe-t-il ?

3 Système de fichiers en réseau

Dans cette partie du TP, vous allez mettre un place un système de fichiers en réseau. Ainsi, un utilisateur de votre système, qui pourra se connecter depuis n'importe quelle machine (grâce au NIS que vous venez de mettre en place), aura accès à son répertoire personnel sur n'importe quelle machine. Ainsi, il pourra notamment avoir accès à son espace de travail depuis toutes les machines du réseau.

1. La machine `serveur` va servir de serveur de fichiers. Elle va *exporter* un répertoire de son arborescence de fichiers sur le réseau : c'est-à-dire que ce répertoire sera accessible depuis n'importe quelle machine du réseau via le système de fichiers en réseau. Ce répertoire sera le répertoire qui contient les répertoires des utilisateurs : `/home`.
   Éditez le fichier `/etc/exports` du serveur. Ce répertoire devra être accessible en lecture/écriture (`rw`) synchrone (`sync`), c'est-à-dire que les modifications seront effectuées directement sur le serveur et non pas mises dans une mémoire cache locale un certain temps. On veut le partager sur notre réseau local. Désactivez la vérification des sous-répertoires du répertoire exporté avec l'option `no_subtree_check`. Ajoutez l'option `root_squash` pour empêcher le super-utilisateur des machines d'accéder au montage NFS.
2. Redémarrez le service NFS (`nfs-kernel-server`) sur le serveur.
3. Le montage du répertoire exporté par le serveur dans l'arborescence de fichiers locale d'une machine cliente se fait comme n'importe quel montage, avec la commande `mount`. Il faut ici spécifier le serveur, le chemin vers le répertoire dans l'arborescence locale de fichiers du serveur, et le point de montage dans l'arborescence locale :

   ```
   athos:~# mount serveur:/home /home
   ```

   On peut ajouter des options : lecture/écriture, synchrone :

```
athos:~# mount serveur:/home /home -o rw,sync
```

Attention, il ne faut pas exécuter les commandes de montage sur le serveur : en effet, cela monterait le répertoire exporté au même point de l'arborescence de fichiers que celui où il est déjà.

Avec la commande `mount` sans arguments, vous pouvez voir tous les montages actuellement effectifs sur votre machine. Comment se présente sur votre client le montage de ce répertoire du système de fichiers en réseau ?

4. Avec la commande `umount /home`, démontez le répertoire distant.
5. Les montages permanents sont définis dans le fichier `/etc/fstab`. Chaque montage correspond à une ligne. Sa structure est comme suit :
   — Première colonne : localisation du système de fichiers (ici : `serveur:/home`)
   — Deuxième colonne : point de montage dans l'arborescence local (ici : `/home`)
   — Troisième colonne : type de système de fichiers (ici : `nfs`
   — Quatrième colonne : options (ici : `rw`, pour lecture/écriture)
   — Les deux dernières colonnes correspondent à des options de vérifications, vous les laisserez à 0 toutes les deux.

   Éditez le fichier `/etc/fstab` de vos clients et ajoutez une ligne pour définir de façon permanente le montage NFS du répertoire exporté par le serveur.
6. Le montage du répertoire NFS se fait désormais avec simplement `mount /home`. Sur vos machines clientes, montez le répertoire NFS. Avec `mount`, vérifiez le montage.
7. Sur vos machines clientes, connectez-vous en tant que `salamix`. Pour cela, vous utiliserez la commande `su` :

```
athos:~# su - salamix
```

Après l'exécution de cette commande, vous devriez normalement être dans le répertoire personnel de `salamix`. Quel est ce répertoire ?

8. Sur une machine cliente (par exemple `athos`, créez un fichier dans le répertoire utilisateur. Quels sont les fichiers présents dans ce répertoire sur cette machine ?
9. Sur les deux autres machines clientes, listez le contenu du répertoire personnel. Que constatez-vous ?
10. Sur une machine (par exemple `porthos`, modifiez le fichier que vous venez de créer. Par exemple, renommez-le. Listez le contenu du répertoire personnel sur les autres machines. Que constatez-vous ?

4 Considérations de sécurité

NFS, tout du moins dans la version que vous utilisez ici, présente de grosses lacunes en matière de sécurité. Vous allez en examiner une dans cet exercice.

1. Sur le serveur, créez un nouvel utilisateur NIS, par exemple `carferrix`. N'oubliez pas de mettre à jour les maps.
2. Sur la machine `athos`, connectez-vous en tant que `carferrix`. Sur la machine `porthos`, connectez-vous en tant que `salamix`.
3. Sur `athos`, restreignez les droits sur le répertoire utilisateur de `carferrix` avec la commande `chmod`, de telle sorte que lui seul puisse accéder à son contenu.
4. Sur `athos`, créez un fichier dans le répertoire utilisateur de `carferrix` :

```
carferrix@athos:~$ echo "bonjour" > unfichier
carferrix@athos:~$ ls
unfichier
```

5. Avec `salamix` sur `porthos`, essayez le lire le contenu du répertoire utilisateur de `carferrix`. Que constatez-vous ?
6. Sur `porthos`, vous êtes connecté en tant que `salamix` mais vous connaissez le mot de passe du super-utilisateur. Avec la commande `su`, devenez le super-utilisateur. En étant super-utilisateur, listez le contenu du répertoire de `carferrix`. Que constatez-vous ?
7. Sur le serveur, modifiez le contenu du fichier `/etc/exports` en remplaçant l'option `root_squash` par `no_root_squash`. Relancez le service NFS sur le serveur, et, sur `porthos`, démontez et remontez le répertoire NFS (vous aurez besoin de vous déconnecter de l'identité de `figatellix` sous laquelle vous êtes devenu root avec deux Ctrl+D successifs). Toujours en tant que super-utilisateur sur `porthos`, listez le contenu du répertoire de `carferrix`. Que constatez-vous de différent par rapport à la question précédente ?
8. Rétablissez l'option `root_squash` dans le fichier `/etc/exports` de la machine `serveur`, redémarrez le service NFS et démontez/remontez le répertoire NFS sur `porthos`.
9. Le super-utilisateur peut devenir n'importe quel utilisateur sans avoir à taper de mot de passe, même un utilisateur NIS. Sur `porthos` où vous êtes sous l'identité du super-utilisateur, devenez `carferrix`. Essayez d'accéder au répertoire personnel de `carferrix`. Que constatez-vous ?
10. Qu'en déduisez-vous sur les failles que vous venez d'explorer et la sécurité et la confidentialité apportées par NIS ? Celles apportées par NFS ?