

TP Réseau n°3b - LAN

© 2011 tv <tvaira@free.fr> - v.1.0 - produit le 13 novembre 2011

Table des matières

Manipulations	2
Objectifs	2
Mise en situation	2
Installation du TP	2
Démarrage des machines virtuelles	3
Travail demandé	4
DHCP	4
DNS (1° partie)	4
NAT	5
DNS (2° partie)	6
HTTP	6
FAQ	7

*Un compte-rendu au format texte (**UTF-8**) devra être rédigé et envoyé à l'adresse
tvaira@free.fr*

*La convention de nommage pour les compte-rendus est la suivante : **tp-3b-nom.txt***

Manipulations

Objectifs

- configuration d'un client par DHCP
- fonctionnement basique du DNS
- mise en place d'un NAT
- échanges lors d'une connexion HTTP

Ce TP est un TP d'observation. Il est important de bien identifier les caractéristiques de chaque communication et chaque service utilisé.

Mise en situation

1. **Solution n°1** : Vous devez disposer d'un PC possédant une distribution Linux (sur une partition spécifique, sur une clé USB bootable, sur un Live CD ou encore à l'aide d'un logiciel de virtualisation du type *VMware* ou *VirtualBox*). Le logiciel de virtualisation **Netkit** doit être installé sur la machine Linux ainsi que le programme `uml_dump`. Évidemment, le logiciel `wireshark` doit être installé sur votre système.
 - **Site de NetKit** : www.netkit.org
 - **Site pour uml_dump** : kartoch.msi.unilim.fr
2. **Solution n°2** : utilisez un **Live CD/DVD/USB Netkit**. Vous pouvez aussi utiliser l'image ISO à l'aide d'un logiciel de virtualisation du type *VMware* ou *VirtualBox*.
 - **Site du Netkit live DVD/USB** : tocai.dia.uniroma3.it
 - **Site du Netkit4TIC live DVD** : tocai.dia.uniroma3.it
 - **Site du Live CD Raizo** : www.utec-tic.org

Installation du TP

Le TP3 est disponible dans l'archive `tp3.tgz`. Par exemple :

```
host> cd /home/user
host> mkdir tp
host> cd tp
host> tar zxvf ../Memos/tp/tp3.tgz
host> cd tp3
```

Rappels

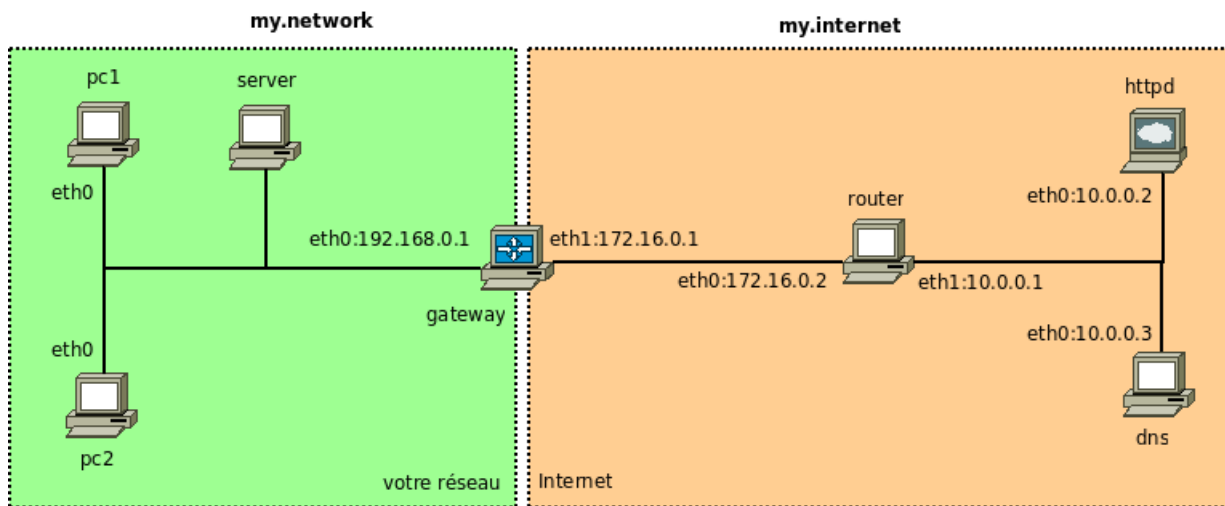
- le prompt `host>` indique que la commande doit être tapée dans le terminal de votre machine réelle (par opposition aux terminaux ouverts par les machines virtuelles).
- le prompt `name :~#` représente le terminal de la machine virtuelle `name`.

Démarrage des machines virtuelles

Démarrer le tp en lançant la commande `lstart` dans le répertoire du lab :

```
host> cd /home/user/tp/tp3
host> lstart -s
```

La configuration suivante est lancée :



Cette configuration possède deux ensembles :

- votre réseau (*my.network*) : les machines **server**, **pc1** et **pc2** représentent un réseau domestique derrière une passerelle (**gateway**). Chacune des machine est sous votre contrôle.
- Internet (*my.internet*) : **router**, **httpd** et **dns** sont des machines extérieures à votre réseau (vous ne devez pas modifier leur configuration).

Les machines sont les suivantes :

- **pc1** et **pc2** représentent des postes clients dans votre réseau
- **server** est une machine fournissant le service DNS et DHCP dans votre réseau.
- **gateway** représente votre passerelle pour l'accès à Internet
- **dns** (*my.internet*) est un serveur DNS
- **httpd** est un serveur HTTP
- **router** représente un routeur sur Internet

La configuration de votre réseau local est sensiblement identique à celle d'un réseau domestique connecté par une free/orange/neuf/sfr box à Internet.

Travail demandé

DHCP

La machine **server** fournit le service DHCP, permettant de configurer les paramètres réseaux de chaque poste client. Lancer `vdump` sur le domaine de collision **A** (*my.network*) et démarrer sur **pc1** et **pc2** l'utilitaire permettant de faire une requête DHCP sur le réseau local :

```
pc1 :~# dhclient eth0
pc2 :~# dhclient eth0
```

Question 1. En observant les échanges DHCP, trouver les informations suivantes :

- Quel est l'adresse IP de **server** ?
- Quel est l'adresse IP affectée à chaque PC ?
- Quels sont les ports sources et destinations utilisés en DHCP ?
- Quelle est la pile de protocoles utilisée dans un échange DHCP ?
- Quelles sont les informations de configuration envoyées par la passerelle aux PC : adresse IP, broadcast, masque, adresse du routeur, adresse du serveur DNS ?
- Retrouver ces informations sur chaque machine avec les commandes suivantes : `ifconfig`, `route` et dans le contenu du fichier `/etc/resolv.conf`.

Remarque : les paquets ICMPv6 correspondent à l'équivalent d'une demande DHCP pour le protocole IPv6. Nous ne nous y intéresserons pas dans ce TP.

Question 2. Quels sont les messages échangés par DHCP au cours de ces différentes étapes ? On attend une réponse détaillée.

Remarque : vous pouvez arrêter et relancer le client DHCP pour configurer l'interface :

```
pc1 :~# killall dhclient
pc1 :~# dhclient eth0
```

DNS (1° partie)

gateway, **pc1** et **pc2** ont chacune une adresse DNS dans le domaine **my.network**, c'est-à-dire une association entre une adresse IP et un nom. Lorsque l'on veut communiquer avec une machine on utilise son adresse IP. Par exemple si l'on effectue un ping sur le nom DNS d'une machine on peut voir apparaître l'adresse IP :

```
pc1 :~# ping pc2.my.network
```

Pour savoir l'adresse IP associée à une entrée DNS, chaque machine fait une résolution DNS. Vous pouvez demander une résolution de noms avec les commandes `nslookup`, `host` ou `dig` :

```
pc1 :~# nslookup pc2.my.network
pc1 :~# host -v pc2.my.network
pc1 :~# dig pc2.my.network
```

Question 3. En observant les échanges DNS, trouver les informations suivantes :

- Quel est l'adresse IP du serveur DNS ?
- A partir de quel fichier les postes **pc1** et **pc2** ont-ils obtenu cette information ?
- Quel est le port d'écoute d'un serveur DNS ?
- Quelle est la pile de protocoles utilisée dans un échange DNS ?
- Quel est le type de la requête DNS ?

Question 4. Quel est le type de la requête émise par **pc1** lorsqu'on tape la commande : `dig -x adresse_ip_de_poste2` ?

Question 5. Quelle est alors la différence entre les requêtes DNS de type A et les requêtes DNS de type PTR ?

Activer des captures wireshark sur les domaines A, B et C.

Question 6. A partir du poste **pc1** ou **pc2**, on n'obtiendra pas de réponse lorsqu'on demande une résolution de nom pour la machine **httpd** du réseau *my.internet* : `host -v httpd.my.internet`. Suivez et analysez les échanges pour répondre aux questions suivantes :

- A quelle adresse IP est envoyée la requête DNS émise par **pc1** (ou **pc2**) ?
- A votre avis, le serveur cache DNS **server** de votre réseau local connaît-il l'adresse IP de la machine **httpd** ?
- Pourquoi ?
- Que fait alors le serveur cache DNS de votre réseau local ?
- A quelle adresse IP envoie-t-il la requête DNS ?
- La requête arrive-t-elle au serveur DNS du réseau *my.internet* ?
- Le serveur DNS du réseau *my.internet* répond-il à la requête ?
- Si votre machine n'obtient pas cette réponse, expliquez alors le problème ?

NAT

Comme vous ne pouvez pas modifier la configurations des machines se trouvant en dehors de votre réseau privée (cela représente une configuration présente dans la réalité où chaque boîtier ADSL ne possède qu'une seule adresse IP publique), il faut trouver une solution pour permettre à plusieurs machines d'être derrière une passerelle.

Il faut donc que **gateway** s'occupe de modifier l'adresse source du paquet et les ports afin que la réponse revienne vers **gateway** et puisse être redirigée vers le bon poste (**pc1** ou **pc2**) dans le réseau local.

Pour cela, il faut activer sur **gateway** le mécanisme de translation d'adresse **NAT** (*Network Address Translation*) :

```
gateway :~# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Question 7. Donner une commande qui permet de vérifier que la translation d'adresse fonctionne ?

Question 8. Dans une communication, la machine **httpd** pourra-t-elle connaître l'adresse IP du poste **pc1** ou du poste **pc2** ?

DNS (2° partie)

Maintenant que le NAT est mis en oeuvre, chaque machine du réseau local peut résoudre des noms du réseau *my.internet*. Vous pouvez demander une résolution pour les noms suivants :

```
pc1 :~# nslookup httpd.my.internet
pc1 :~# host -v router.my.internet
pc1 :~# dig dns.my.internet
```

Question 9. Donner les trois adresses IP obtenues par la résolution DNS pour les machines **httpd**, **router** et **dns**.

Question 10. A partir de la machine **httpd**, est-il possible de résoudre l'adresse IP correspondant au nom **pc1** avec la commande : `host pc1.my.network` ? Justifier votre réponse.

HTTP

Il y a un serveur HTTP (**apache**) en fonctionnement sur **httpd**. Pour voir le contenu de la page d'accueil (`index.html`), il suffit de lancer **lynx**, un navigateur en mode texte à partir de **pc1** :

```
pc1 :~# lynx http ://httpd.my.internet/
```

Question 11. Donner le diagramme des échanges complet jusqu'à ce que la page HTML soit retournée (ARP, DNS, ...).

Question 12. Donner la pile de protocoles utilisée par HTTP.

Question 13. Quel est le numéro de port du serveur HTTP (**apache**) ?

Question 14. Comment le client (**lynx**) connaît-il le numéro de port utilisé par le serveur (**apache**) ?

Question 15. Quel est le numéro de port du client HTTP (**lynx**) ?

Question 16. Qui a choisi ce numéro de port ?

Question 17. Comment le serveur (**apache**) connaît-il le numéro de port utilisé par le client (**lynx**) ?

Question 18. Quelle est la requête HTTP envoyée par le client (**lynx**) pour obtenir la page HTML ?

Question 19. Quelle est la version du protocole HTTP utilisée dans cet échange par le client (**lynx**) ?
Quelle est celle utilisée par le serveur (**apache**) ?

Question 20. A quelle(s) RFC correspondent-elles ?

FAQ

Remarque : il est possible que les machines virtuelles n'aient pas eu accès à leurs fichiers de configuration à partir d'un lancement avec `lstart -s`. Dans ce cas, il vous faudra faire ces opérations manuellement.

Comment copier les fichiers de configuration destinés à une machine virtuelle à partir de la machine réelle ?

```
httpd :~# cp -r /hostlab/httpd/etc /
httpd :~# cp -r /hostlab/httpd/var /
router :~# cp -r /hostlab/router/etc /
server :~# cp -r /hostlab/server/etc /
dns :~# cp -r /hostlab/dns/etc /
```

Faut-il redémarrer un service sur une machine virtuelle si on a modifié ses fichiers de configuration ?

Oui

Quels sont les services utilisés dans ce TP ?

Les services utilisés sont :

- apache sur machine **httpd** : serveur HTTP
- dnsmasq sur machine **router** : serveur DHCP et serveur cache DNS
- dnsmasq sur machine **server** : serveur DHCP et serveur cache DNS
- bind sur machine **dns** : serveur DNS

Comment connaître l'état d'un service sur une machine virtuelle ?

```
httpd :~# /etc/init.d/apache2 status
router :~# /etc/init.d/dnsmasq status
server :~# /etc/init.d/dnsmasq status
dns :~# /etc/init.d/bind status
```

Comment arrêter un service sur une machine virtuelle ?

```
httpd :~# /etc/init.d/apache2 stop
router :~# /etc/init.d/dnsmasq stop
server :~# /etc/init.d/dnsmasq stop
dns :~# /etc/init.d/bind stop
```

Comment démarrer un service sur une machine virtuelle ?

```
httpd :~# /etc/init.d/apache2 start
router :~# /etc/init.d/dnsmasq start
server :~# /etc/init.d/dnsmasq start
dns :~# /etc/init.d/bind start
```

Comment redémarrer un service sur une machine virtuelle ?

```
httpd :~# /etc/init.d/apache2 restart
router :~# /etc/init.d/dnsmasq restart
server :~# /etc/init.d/dnsmasq restart
dns :~# /etc/init.d/bind restart
```

Comment observer les communication sur le réseau virtuel reliant les machines UML ?

Pour connecter `wireshark` (qui permet de sniffer un réseau local sur un *hub*) avec le domaine de collision **A** d'un *lab*, il faut taper :

```
host> vdump A | wireshark -i - -k
```

Pour ne perdre l'accès à cette console, il est préférable de lancer le processus en arrière plan :

```
host> vdump A | wireshark -i - -k &
```

Pour se déconnecter, il suffit de fermer l'application `wireshark`.

Attention : si vous avez plusieurs domaines de collision (A, B, C, ...), il vous faudra exécuter plusieurs `wireshark` pour *sniffer* les différents trafics.

Comment sauver l'ensemble des commandes ou leurs résultats ?

Vous pouvez sauvegarder l'ensemble de vos commandes tapées :

```
pc :~# history >> /hostlab/save.txt
```

Cette commande va sauvegarder vos commandes en les ajoutant à la fin du fichier `save.txt` situé à la racine de votre lab.

On peut aussi utiliser ce principe pour sauvegarder le résultat des commandes exécutées sur une machine virtuelle :

```
pc :~# ifconfig eth0 >> /hostlab/compte-rendu.txt
```