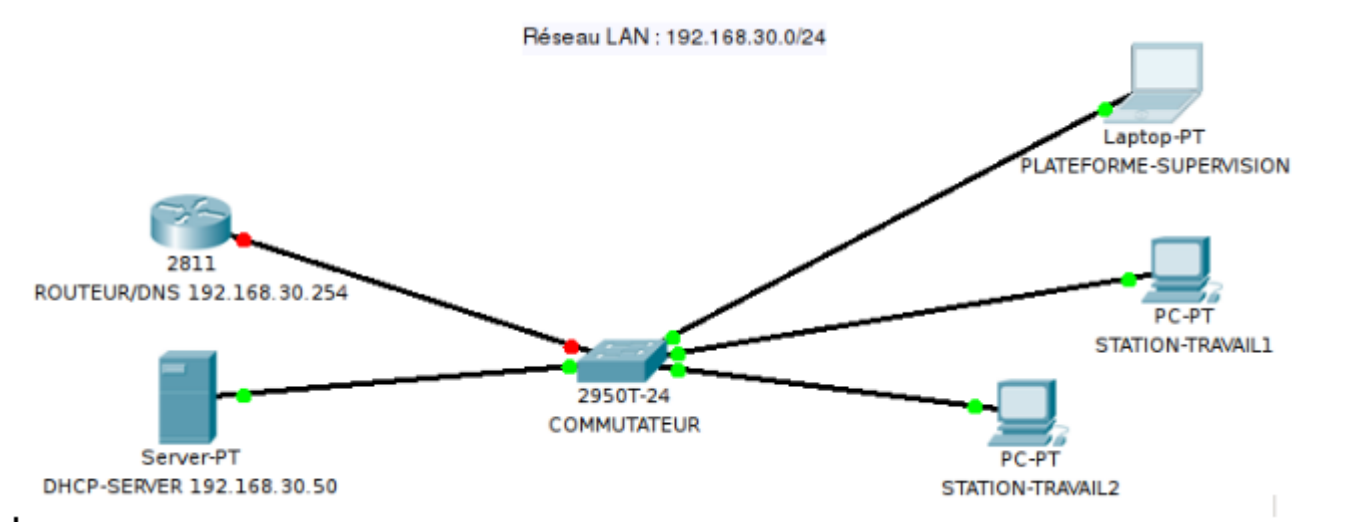


SERVEUR DHCP SIMPLE

MONTER UN SERVEUR DHCP SIMPLE

Avec **NetKit**, Vous allez réaliser l'architecture suivante :



Remarque : Le ROUTEUR/DNS n'a pas besoin d'être démarré pour faire ce TP.

Le serveur DHCP, ayant pour hostname « PROTEINE», sera configuré de la façon suivante :

HOSTNAME	PROTEINE
ADRESSE IP	192.168.30.50/24 configurée « en dur » dans le fichier /etc/network/interfaces
PLAGE ADRESSES	192.168.30.100/24 → 192.168.30.150/24
IP ROUTEUR	192.168.30.254
DNS	192.168.30.254 ; 208.67.222.222

DUREE BAIL PAR DEFAULT|30 secondes|

REMARQUE : la **PLATEFORME-SUPERVISION** sera configurée en mode « client DHCP » mais l'adresse IP délivrée par **PROTEINE** à cette machine sera toujours : **192.168.30.200/24** (adresse réservée).

LA CONFIGURATION BASIQUE

Remarque : on ne configure pas pour l'instant la durée de bail et l'adresse IP réservée à la machine **PLATEFORME-SUPERVISION**.

- configurer les stations STATION-TRAVAIL1, STATION-TRAVAIL2 et PLATEFORME-SUPERVISION en mode « client dhcp ». Vérifier leur bonne configuration en relançant le service réseau (/etc/init.d/networking restart)
- configurer le serveur DHCP en adaptant le fichier « /etc/dhcp3/dhcpd.conf » : il est prudent de faire une copie de ce fichier avant toute modification ! :)
- Relancer le service DHCP sur le serveur PROTEINE.

VERIFICATION DU BON FONCTIONNEMENT DU SERVICE DHCP

- Pour chaque station cliente, vérifier que celle-ci récupère bien une adresse IP et un masque de sous-réseau valides, une adresse passerelle et une adresse DNS : les commandes « dhclient », « route » vous seront utiles ! Pour vérifier les DNS, pensez à visualiser le fichier « /etc/resolv.conf ».
- Relâchez la configuration IP d'une station cliente (dhclient -r eth0) et vérifier la configuration IP (ifconfig eth0). Qu'en concluez-vous ? Visualisez également la table de routage et le fichier « /etc/resolv.conf »
- Lancez depuis la même station cliente une requête DHCP et refaites les vérifications précédentes.
 - Pour conclure, assurez vous que TOUTES les machines (serveur DHCP compris) peuvent bien communiquer entre elles (« ping »).

AFFINER LA CONFIGURATION DU SERVEUR DHCP

RESERVER UNE ADRESSE IP POUR PLATEFORME-SUPERVISION

- réservez l'adresse 192.168.30.200/24 à la PLATEFORME-SUPERVISION.
- Vérifiez !!
- Quel peut être l'intérêt d'une telle configuration ?

MODIFIER LA DUREE DE BAIL

- Modifiez « dhcpd.conf » avec les paramètres :
 - temps de renouvellement des adresses par défaut : 30 secondes.
 - temps de renouvellement des adresses maxi. : 1 minute.
- Quel est l'intérêt de ce paramétrage ?

VISUALISER LES BAUX DHCP

L'information cherchée se trouve dans le fichier **/var/lib/dhcp3/dhcpd.leases**

- Visualisez son contenu et notez les horaires de renouvellement et d'expiration des baux.

ALLER PLUS LOIN ENCORE !! ANALYSER LES TRAMES ETHERNET

Lancer une capture de trames sur l'interface eth0 de PROTEINE (voir annexe)

- Connecter une nouvelle machine sur le réseau configurée en « client DHCP ». Une fois le client DHCP configuré, Relancer le service réseau.
- Arrêter la capture sur PROTEINE.
- Lancer l'analyseur de trames WIRESHARK sur la machine hôte Ubuntu-Server et ouvrir le fichier de capture.
- Appliquer un filtre sur le protocole BOOTP.
- Repérer les 4 trames correspondant aux 4 échanges qui ont eu lieu entre la nouvelle machine attachée au réseau et PROTEINE. Ces 4 trames correspondent réciproquement à :
 - la découverte d'un serveur DHCP (trame broadcast DHCPDISCOVER émise par la nouvelle machine)
 - la première réponse du serveur PROTEINE (trame unicast DHCP OFFER)
 - l'acceptation de l'offre de PROTEINE par la nouvelle machine (trame broadcast DHCP REQUEST).
 - L'accusé de réception de PROTEINE (trame unicast DHCP ACK).
- Analyser les différents champs de ces 4 trames en distinguant bien les champs des couches 2, 3 et 4 du modèle OSI.
- Le service DHCP travaille-t-il en UDP ou en TCP ? Quelle différence faites-vous entre UDP et TCP ?
- Quel est le numéro de port du serveur DHCP ?
- Pourquoi la 3ème trame (acceptation de l'offre PROTEINE par le client) est-elle une trame de diffusion ?

ANNEXE : EXTRAIT DOCUMENTATION NETKIT : CAPTURE DE TRAMES

Sur NETKIT, le répertoire /hosthome de chaque machine virtuelle est mappée sur le répertoire /home/user de la machine hôte (machine physique sauf installation virtuelle de NETKIT)

Les machines virtuelles lancées par NETKIT ne supportent pas une interface graphique. La capture de trames ne peut se faire par WIRESHARK. Nous utiliserons donc tcpdump.

La commande suivante permet de lancer une capture de trame :

```
# tcpdump -i eth0 -U -w /hosthome/monfichier.cap
```

Sur la machine hôte et après la fin de la capture, vous pouvez lancer WIRESHARK pour lire le fichier **/home/user/monfichier.cap**

[INTRODUCTION A NETKIT](#)

From:

/ - **Les cours du BTS SIO**

Permanent link:

[/doku.php/si5/simplifiedhcp](#)

Last update: **2014/01/07 11:51**

