



iNFO

IUT
GRAND OUEST
NORMANDIE

R 3.06

2023 - 2024

Architecture des réseaux

TP n° 4
NAT



ANNE Jean-François
D'après le cours de M. JEANPIERRE

Proxy, traduction d'adresses et routage

Le but de ce TP est de se familiariser avec les notions de routeur NAT. On reviendra aussi sur les concepts du DHCP. En définitive, nous allons configurer l'équivalent d'une « box » internet.

Le logiciel à utiliser pour se connecter en liaison série au routeur :

- ^ GTKTerm à installer !

Le matériel mis en jeu (par binôme) :

- ^ 2 machines Linux, 1 routeur Cisco, 1 commutateur (Switch)(celui de la salle)

Vous avez également (pour toute la salle) :

- ^ 1 serveur DHCP : *galvani*,
- ^ Une 'machine cible' (le pc-prof) que vous ne pourrez PAS configurer,
- ^ Un serveur Web, tournant sur la machine cible.

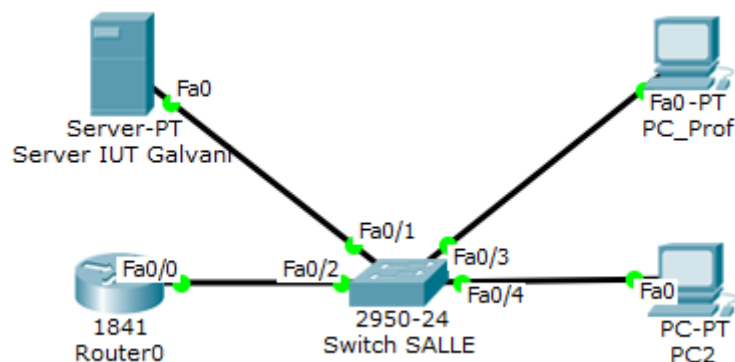
Ne pas prendre de matériels génériques !

Dessiner au fur et à mesure les réseaux logiques et physiques que vous allez construire....

1°) Configuration du routeur en client DHCP

Débrancher le câble réseau de PC1 et mettez-le sur le port Fa0/0 du routeur. Nous allons configurer le port Fa0/0 du routeur en IP dynamique pour qu'il puisse communiquer avec le réseau de l'IUT.

Schéma de montage :



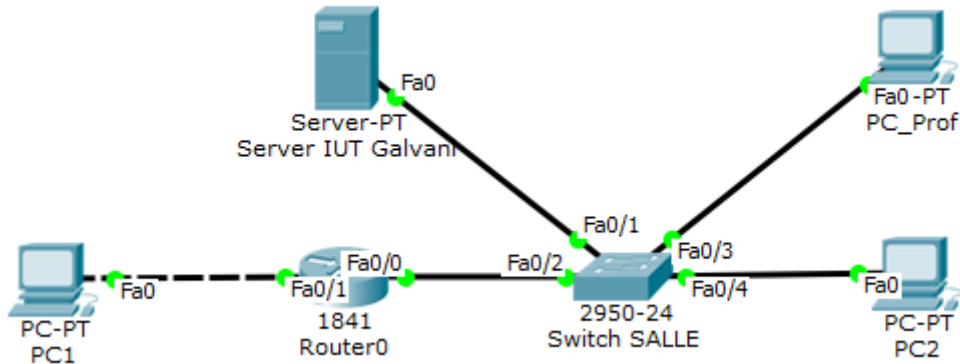
Les routeurs Cisco peuvent auto-configurer leurs adresses IP via un serveur DHCP. Configurez l'interface Fa0/0 du routeur en adresse IP dynamique. Pour cela on utilise la commande suivante (à la place de la configuration d'IP statique) :

```
Router(config-if)# ip address dhcp
```

- ^ A partir du routeur, essayez de pinger la machine-cible (le pc-prof) ou le PC2.

2°) Configuration du routeur en serveur DHCP

Notre « Box » étant en place coté fournisseur d'accès, on va s'occuper de notre réseau interne. Pour que notre réseau puisse fonctionner il faut que notre box puisse distribuer des adresses IP sur les machines de notre réseau. On va donc configurer un service DHCP sur notre routeur pour notre réseau.



Attention aux types de câbles à utiliser !

Les routeurs Cisco peuvent aussi servir de serveur DHCP. Vous allez donc configurer l'interface FastEthernet0/1 afin qu'elle attribue une IP à vos PC.

- Déterminez l'adresse IP que vous allez attribuer à votre réseau privé : 192.168.X.Y 255.xxx.xxx.xxx
- Déterminez l'adresse IP que vous allez attribuer à votre routeur (Box) : A.B.C.D /m
- Déterminez la plage d'adresses que vous voulez garder pour faire de l'adressage statique : low [high]

Configurez le port F0/1 du routeur avec l'adresse IP que vous avez choisie.

Nous allons maintenant activer le service DHCP de notre routeur :

Router(config)# no ip dhcp conflict logging	<i>Pas de log des conflits</i>
Router(config)# ip dhcp excluded-address <u>low [high]</u>	<i>Plage d'adresses à ne PAS attribuer (reservées)</i>
Router(config)# ip dhcp pool <u>1</u>	<i>Mode configuration des adresses allouables</i>
Router(config-dhcp)# network <u>192.168.X.Y 255.xxx.xxx.xxx</u>	<i>Définition du réseau où choisir les adresses IP</i>
Router(config-dhcp)# default-router <u>A.B.C.D</u>	<i>Passerelle par défaut des futurs clients</i>
Router(config-dhcp)# lease <u>j h m</u>	<i>Durée de bail offerte (jours heures minutes)</i>

Une fois le routeur configuré, configurez vos PC en clients DHCP.

Sur le PC1, redemandez une nouvelle adresse IP au serveur DHCP avec la commande suivante :

```
sudo dhclient -r
sudo dhclient
```

Vérifiez alors l'adresse IP qui vous a été attribuée sur le PC1, et qu'elle correspond bien à la plage que vous avez spécifiée.

Sur le routeur, vous pouvez vérifier les adresses IP distribuées avec :

```
show ip dhcp binding.
```

- ▲ Vérifier que la passerelle par défaut a bien été insérée dans votre configuration réseau.
- ▲ Observez via *Wireshark* les échanges de trames DHCP.
- ▲ Essayez de pinguer PC2 depuis votre PC1. Si cela ne fonctionne pas expliquez pourquoi et comment on pourrait corriger le problème.

```
sudo route add -net 192.168.x.0 netmask 255.255.255.0 gw 192.168.1.Y
```

3°) Configuration du routeur en mode NAT

Le mode *Network Address Translation*, ou traduction d'adresses réseau, permet par exemple le partage d'une connexion internet unique (une seule IP) par plusieurs machines. Cette partie vise à mettre en évidence les bases du fonctionnement de ce protocole. Pour plus de détails, voir la RFC 1631 ou votre enseignant.

Vous allez configurer votre routeur en tant que routeur NAT, la machine cible étant sur le réseau « publique » et vos PC étant sur le réseau « privé ». Pour cela, vous devez configurer l'une de des interfaces du routeur comme « privée » et l'autre comme « publique » :

Router(config-if)# ip nat inside	<i>Cette interface est connectée au réseau privé</i>
Router(config-if)# ip nat outside	<i>Cette interface est connectée au réseau public</i>

Il faut ensuite définir la liste des machines autorisées à utiliser cette fonctionnalité. Par défaut, toutes sont

refusées :

```
Router(config)# access-list 1 permit 192.168.X.0 0.0.0.255  
Router(config)# ip nat inside source list 1 interface FastEthernet0/0 overload
```

Attention, le masque est écrit à l'inverse d'un masque de réseau !!! (bits à 1 pour le n° de machine)

Ces deux commandes autorisent les machines d'adresse IP comprise entre 192.168.X.0 et 192.168.X.255 à utiliser ce service : L'adresse d'une machine *privée* sera remplacée par celle de l'interface FastEthernet 0/0 du routeur.

Vous pouvez vérifier les adresses qui ont été traduitées avec la commande :

```
show ip nat translations
```

⤴ Pingez la machine-cible depuis votre PC.

4°) A Faire à la fin du TP :

Remettre FireFox en mode « proxy 192.168.0.2 : 3128 » ou en détection automatique.
Eteindre le routeur.

N'oubliez pas le NETTOYAGE en fin de séance