Information préalable valable pour <u>tous les groupes</u> et pour <u>tous les TP</u>.
les TP devront être rendus et seront notés. Nous utiliserons l'environnement Jalon pour le rendu des TPs (jalon.unice.fr) via l'ouverture de boîtes de dépôt. Le rendu de TP N se fait avec un deadline qui est la veille du TP N+1.
***Exemple** pour ce TP1 du mercredi , vous devrez rendre votre TP avant le TD du lundi suivant 10h . Les boîtes de dépôts seront configurées en conséquence.*
Aucun TP ne sera accepté par email (ils se perdraient dans nos boites surchargées!)
Les TPs vous seront fournis au format .doc, vous pourrez donc utilisez les versions électroniques des énoncés pour faciliter la rédaction de vos rendus de TP. Vous déposerez ces mêmes fichiers doc dans les boîtes de dépôt. PAS de .pdf car difficile à annotés par les correcteurs.
Merci de votre attention.

TD/TP Réseaux n°4 : Routage – Routage inter-VLANs- NAT

Notions abordées:

a. Table de routage
b. Configuration passerelle
c. Routage inter VLAN
d. NAT

Exercice n°1 : prochain saut

Un routeur possède les entrées (CIDR) suivantes dans sa table de routage :

Adresse/masque	Prochain saut
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Routeur 1
0.0.0.0	Routeur 2

Que fait le routeur s'il reçoit un paquet avec les adresses suivantes :

1. 135.46.63.10
2. 135.46.57.14
3. 135.46.52.2
4. 192.53.40.7
5. 192.53.56.7

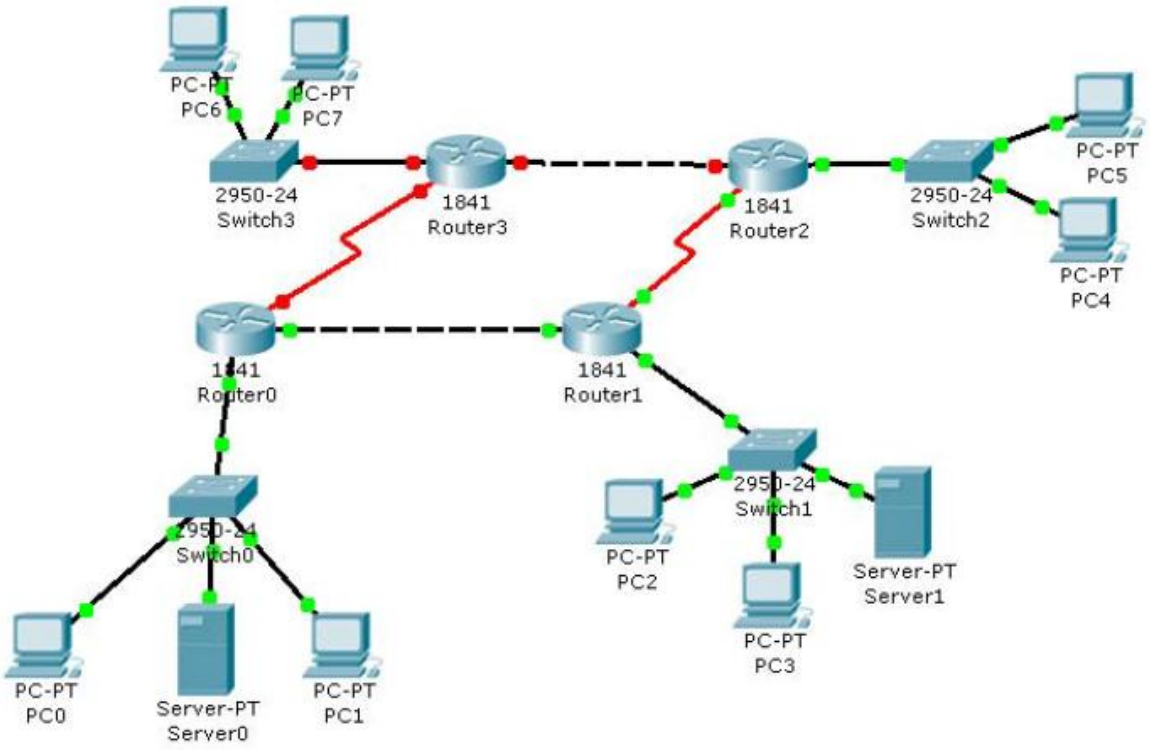
Exercice n°2 : commande route

Tapez la commande `route print`.

- Quelles sont les informations données ?
- Quelle est l'adresse de la passerelle ?
- A quoi sert la passerelle ?

Exercice n°3 : Routage sous packet Tracer

Dans ce TP, vous allez mettre en place un réseau relativement simple afin de vous familiariser avec les différentes fonctionnalités de Packet Tracer.
Le réseau à simuler est le suivant et comporte 4 sous réseaux reliés ensemble par des routeurs.



Les adresses ip des machines sont les suivantes :

Machines	@IP
PC0	200.6.0.10 / 24
PC1	200.6.0.11 / 24
PC2	200.6.1.10 / 24
PC3	200.6.1.11 / 24
PC4	200.6.2.10 / 24
PC5	200.6.2.11 / 24
PC6	200.6.3.10 / 24

Machines	@IP
PC7	200.6.3.11 / 24
Server0	200.6.0.250 / 24
Server1	200.6.1.250 / 24

1. Configuration des routeurs

Vous devez configurer les différents routeurs de manière à créer les routes entre les différentes machines. Vous testerez les configurations par des ping sur les différentes machines et interfaces.

2. Routage inter-Vlans

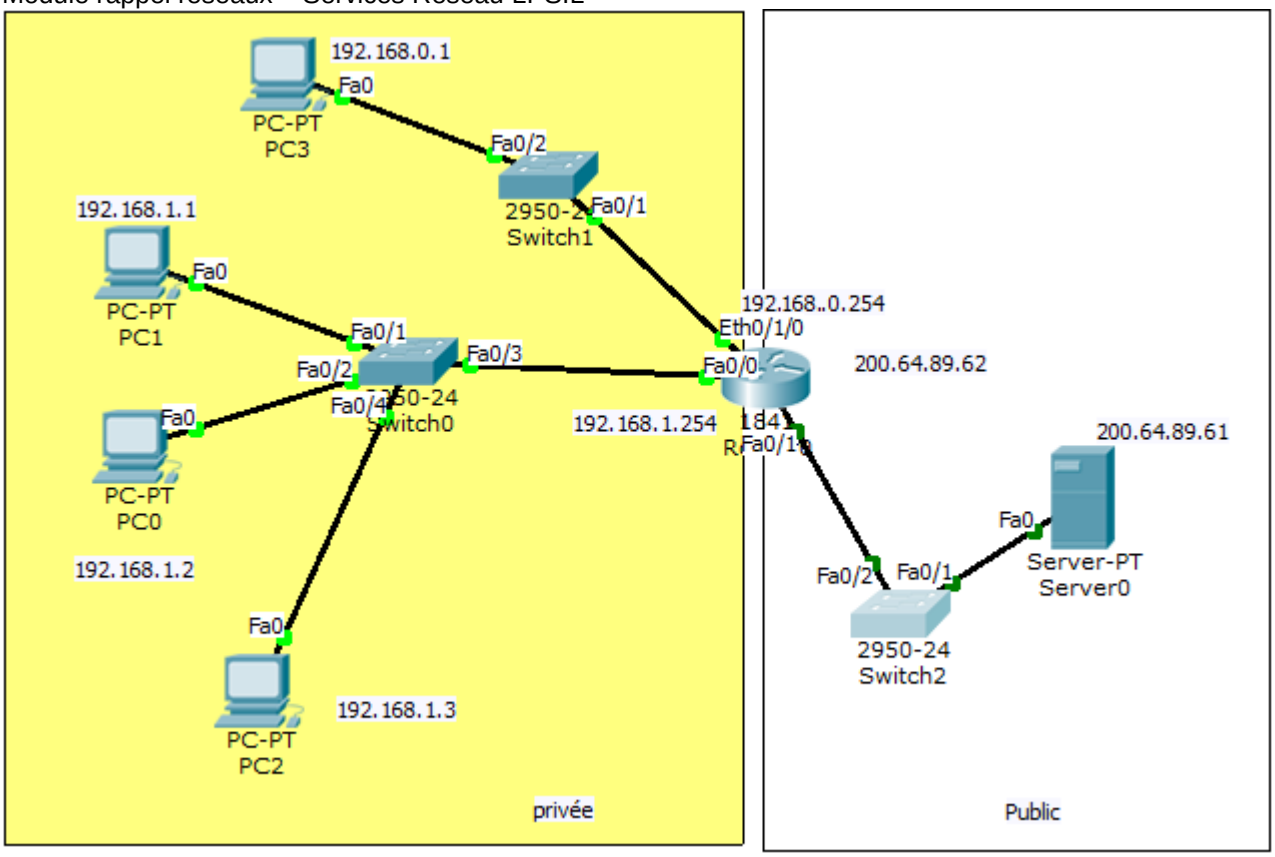
Vous allez ajouter deux machines (PC8 et PC9) sur le switch 0 dont les adresses IP sont 200.6.4.10 et 200.6.4.11. ces deux machines seront mises dans un vlan VLAN_4.
Vous réaliserez le routage de deux manières différentes.

a. La première façon consistera configurer une deuxième interface sur le routeur0 et à connecter cette deuxième interface comme passerelle pour le VLAN_4. Vous réaliserez les tests qui permettent de vérifier la bonne configuration de votre routeur.
b. La deuxième manière est d'utiliser le mode TRUNK entre le switch0 et le routeur0. Pour cela coté routeur vous allez associer à l'interface physique fa0/0 deux sous interfaces logiques fa0/0.1 et fa0/0.2.
    1. Vous supprimerez l'adresse IP de l'interface fa0/0,
        - *int fa0/0*
        - *no ip address*
    2. Vous configurerez l'interface en mode trunk et lui donnerez une adresse de passerelle.
        - *int fa0/0.1*
        - *encapsulation dot1q 4*
        - *ip address 200.6.4.254 255.255.255.0*

Configurer le switch0 et les routeurs des deux manières. Vous testerez les configurations par des ping sur les différentes machines et interfaces.

Exercice n°4 : Routage et NAT Statique

Nous allons mettre en place sur NAT sur un routeur. Soit la configuration réseau suivante :



Dès lors, nous allons configurer le NAT afin de permettre un accès à Internet

- La machine 192.168.1.1/24 sera accessible depuis le réseau publique grâce à une configuration de NAT statique.
- Le réseau 192.168.1.0/24 utilisera du NAT dynamique avec pool d'adresse.
- Le réseau 192.168.0.0/24 utilisera du NAT avec surcharge PAT.

1. Configuration commune à tout type de NAT

1. La première chose à faire lorsque l'on configure du NAT, quel qu'en soit le type, c'est d'indiquer au routeur où se situe le réseau privé et où se situe le réseau publique.

```
R1(config)#int fa0/0
R1(config-if)#ip nat inside
R1(config)#int s0/0
R1(config-if)#ip nat outside
```

2. Configuration de NAT statique

Vous allez explicitement indiquer au routeur que ce qui arrive sur son interface publique et dont l'adresse destination est 201.64.89.30 (une des adresses du pool publique) doit être redirigé vers PC1

192.168.1.1. Vice versa l'adresse source 192.168.1.1 sera remplacée par l'adresse indiquée dans la table de translation NAT.

1. Configurez le NAT dans ce sens.

```
R1(config)#ip nat inside source static 192.168.1.1 200.64.89.30
```

2. Visualiser et indiquez la table NAT que vous obtenez avec la commande *show ip nat translations*

3. Maintenant accédez à l'extérieur en lançant un browser internet et ensuite vérifier la table NAT avec la commande suivante

http://200.64.89.61

4. Affichez la liste des paquets qui ont été translatés.

3. Configuration du NAT avec pool d'adresses

Pour l'instant seul PC1 à accès au réseau publique, nous allons maintenant configurer un autre type de NAT pour le réseau 192.168.1.0/24 (à l'exception de PC1).

Ici, au lieu de configurer une translation statique, nous allons donner au routeur une plage d'adresses publiques (un pool d'adresse) dans laquelle il peut piocher pour créer dynamiquement les translations.

5. Tout d'abord créez le pool d'adresses nommé POOL-NAT allant de 200.64.89.17 à 200.64.89.20.

```
R1(config)#ip nat pool POOL-NAT 200.64.89.17 200.64.89.20 netmask 255.255.255.0
```

6. Il nous faut ensuite définir quelles adresses IP sources seront susceptibles d'être translatées … pour cela il faut créer une ACL.

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#access-list 1 deny 192.168.1.1
```

7. Il ne reste plus qu'à configurer le NAT en lui même

```
R1(config)#ip nat inside source list 1 pool POOL-NAT overload
```

NB Overload indique qu'il y a plus d'adresses privées que de publiques.

8. Vérifiez que les machines concernées accèdent au serveur web externe..

9. Affichez la liste des paquets translatés.

4. Configuration du NAT dynamique avec surcharge PAT (sans pool)

Il reste encore à configurer le routeur pour que le réseau 192.168.0.0/24 puisse accéder à l'extérieur. Pour cela nous allons configurer le troisième type de NAT, à savoir du NAT dynamique avec surcharge (overload) en utilisant l'adresse publique configurée sur l'interface externe du routeur.

10. Vous devez cette fois aussi identifier les adresses sources à faire passer par le NAT, Vous devez créez une nouvelle ACL.

```
R1(config)#access-list 2 permit 192.168.0.0 0.0.0.255
```

11. Configurez le NAT en disant au routeur de translater les paquets provenant des adresses décrites dans l'ACL 2 (192.168.0.0/24) et de remplacer l'adresse IP source par celle configurée sur l'interface publique en la surchargeant pour permettre à plus d'une machine de communiquer avec l'extérieur (PAT).

```
R1(config)#ip nat inside source list 2 interface Fa0/1 overload
```

12. Vérifier la table NAT du router après la requête http vers l'extérieur

```
Router#sh ip nat translations
```