


# UE31 - M3102 : Services Réseaux

## Enoncé du TP 8

### Administration d'un LAN et d'un routeur CISCO - Acte 2

 **Manipulez le matériel avec la plus grande précaution ! Ne tirez pas sur les prises ni sur les câbles !**

Au moins 15 minutes avant la fin de la séance, procédez à la remise en état du matériel :

-  copier votre running-config (affichée en tapant **show run** en mode privilégié) et **l'ajouter en fin de rapport** dans une partie intitulée «*Dernière Running Config*»
- rassembler les fichiers de ce que vous devez remettre à votre enseignant et les envoyer par mail (tout en PJ, pas d'archive svp !)
- garder une sauvergarde de votre travail sur clé USB (en cas de problème)
- restaurer sur le routeur la configuration startup-config.default en tapant, en mode privilégié :

```
# copy nvram:startup-config.default start
```

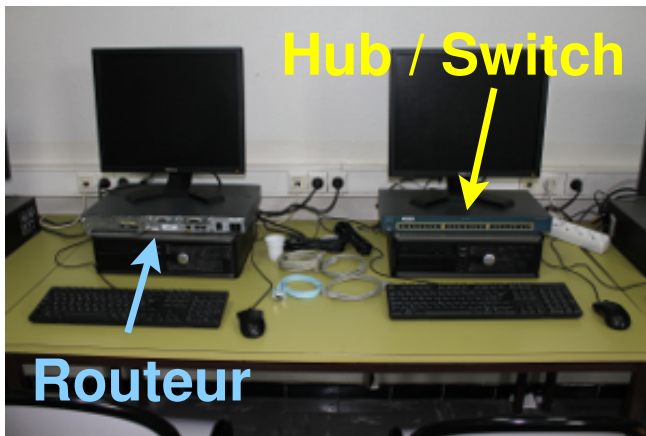
puis tapez  pour confirmer la restauration de la startup-config.

- débrancher le matériel et le remettre en ordre à sa place initiale. Les câbles et cordons doivent être correctement enroulés et attachés
- éteindre le PC-LAN et le rebrancher sur le réseau du département
- éteindre le PC-IUT.

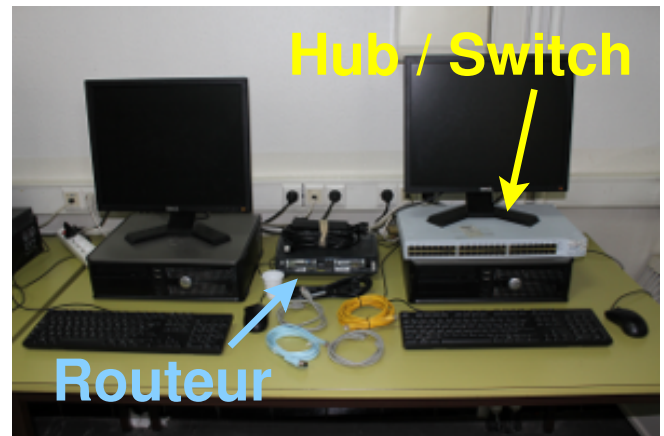
## Table des matières

<b>I</b>	<b>Installation</b>	<b>3</b>
	Exercice 1	3
	I.1 Rôle des PC et contexte du TP	4
	I.2 Création du rapport sur le PC-IUT	7
	Exercice 2	7
	I.3 Création (d'une partie) du rapport sur le PC-LAN	7
	Exercice 3	7
	I.4 Lancement des machines virtuelles sur le PC-LAN	7
	Exercice 4	8
<b>II</b>	<b>Minicom pour accéder à la console du routeur</b>	<b>10</b>
	Exercice 5	10
<b>III</b>	<b>Conception Réseau</b>	<b>14</b>
	Exercice 6	14

<b>IV Configurations Réseau</b>	<b>15</b>
IV.1 Raccordement et configuration côté WAN	15
Exercice 7	15
IV.2 Mise en place du LAN	16
IV.2.A Configuration de l'interface LAN du routeur	16
Exercice 8	16
IV.2.B Configuration de l'interface LAN de VMDEB	17
Exercice 9	17
IV.3 Configuration du routage sur le routeur	17
Exercice 10	18
IV.4 Accès à la CLI par TELNET	18
Exercice 11	19
<b>V Serveur DHCP sur le routeur</b>	<b>20</b>
V.1 Configuration de l'allocation dynamique	20
Exercice 12	21
V.2 Configuration de l'allocation statique	22
Exercice 13	23
<b>VI Configuration du NAT/PAT</b>	<b>25</b>
VI.1 Le PAT sur le routeur d'accès vers Internet (RPAT)	25
VI.2 Principes et terminologie du NAT	28
VI.2.A Traductions inside et outside	30
VI.2.B Variantes du NAT	31
VI.3 Configuration du PAT dynamique	32
Exercice 14	34
VI.4 Fonctionnement de la traduction dynamique PAT	34
VI.4.A Initiation d'une traduction dynamique PAT	34
VI.4.B Traduction dynamique PAT des messages sortants	36
VI.4.C Traduction dynamique PAT des messages entrants	37
Exercice 15	38
VI.5 PAT statique pour la redirection de port des connexions entrantes	38
Exercice 16	39
VI.6 ACL étendues et sécurisation des accès réseau	39
Exercice 17	40
VI.7 Interactions entre le NAT et les autres protocoles	41
Exercice 18	41
<b>VII Annexe</b>	<b>42</b>
VII.1 Message ICMP de test d'accessibilité et d'état (PING)	42



(a) Avec séries 2500, 2600 et modèle 1760



(b) Avec routeur 1720 ou 1721

**FIGURE 1** – Présentations probables de l'espace de travail

## I Installation

L'environnement de travail d'un binôme devrait ressembler à l'une des prises de vues de la figure 1.

### Exercice 1 (Démarrage des PC)

1. Le PC côté switch sera le PC-LAN ; l'autre sera le PC-IUT
2. **Après s'être assuré** que les deux PC sont branchés sur le réseau du département, les démarrer sur Linux ;
3. Sur PC-LAN :

- (a) se logger en tant que l'utilisateur **test**, mot de passe **test** ;

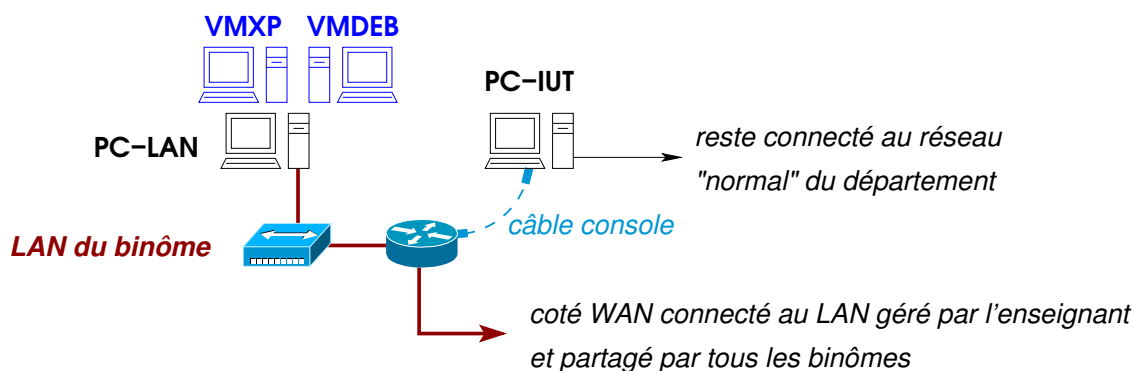
**i** Cet utilisateur est dédié à ce TP. Il ne dispose pas de compte AMU et n'a pas de amuhome, ce qui nous permettra de débrancher librement le PC-LAN du réseau.

- (b) ouvrir un terminal, puis exécuter la commande :

```
$ clean_test
```

qui va procéder au nettoyage des fichiers laissés par vos éventuels prédécesseurs sur ce PC.

4. Sur PC-IUT, se logger normalement avec vos identifiants habituels ;
5. **Sur les deux PC**, aller sur la page du module sur Ametice, et afficher l'énoncé du TP ainsi que **tous les documents de support** du TP, disponibles dans la section *Documents Utiles* → *Notes techniques*. Par la suite, on fera référence à ces documents par :
  - **DocCisco** pour le document [Administration des routeurs CISCO](#) ;
  - **DocWshark** pour le document [Initiation à l'analyse de trafic réseau avec Wireshark](#) ;
  - **DocRes** pour le document [Configuration et commandes réseau](#) ;
  - **DocVBox** pour le document [VirtualBox pour les TP de réseaux](#).



**FIGURE 2** – Environnement de travail d'un binôme : le PC-IUT reste connecté au réseau du département et servira à administrer le routeur. Le PC-LAN (et ses VM) sera relié au LAN du binôme qui comprend un switch et un routeur. Le binôme devra effectuer les câblages (en rouge). Le routeur devra être connecté au réseau géré par l'enseignant (côté WAN).

## I.1 Rôle des PC et contexte du TP

Comme l'an dernier (rappelez-vous !), vous disposez de câbles Ethernet, d'un routeur, d'un *switch* et des 2 PC :

- **PC-IUT** (le PC où se trouve votre routeur le cas échéant) va servir pour administrer le routeur (au moins au début) mais restera branché sur le réseau classique du département. L'administration se fera via un **câble console** qui raccordera le port série du PC-IUT et le port console du routeur ;
- **PC-LAN** (le PC où se trouve votre switch) sera débranché du réseau du département. Il sera connecté à votre switch, de même que votre routeur, pour former le LAN du binôme. Le PC-LAN n'est pas directement configurable par les utilisateurs, mais il servira à exécuter deux machines virtuelles **VMDEB** et **VMXP** sur lesquelles vous serez administrateurs. Les interfaces réseau de ces VM partageant la même carte réseau que PC-LAN, ce sont ces VM qui en réalité seront raccordées au LAN que vous allez administrer.

La figure 2 schématise les divers raccordements que vous effectuerez ultérieurement :

- en bleu, le câble console raccordera la prise série du PC-IUT au port console du routeur afin d'administrer le routeur. Cette liaison série n'est pas une liaison réseau ;
- en rouge, les raccordements *Ethernet* que vous réaliserez :
  - ◇ du PC-LAN et du routeur à votre *switch* pour constituer votre **LAN**
  - ◇ de votre routeur à l'un des switchs du LAN géré par l'enseignant, raccordé à Internet par le routeur **RPAT** (voir ci-après). Cette liaison (la flèche en rouge en bas à droite) constituera le côté **WAN** de votre routeur, car elle le raccordera à Internet.




Ainsi, dans ce qui suit :


- ◇ le **côté WAN de votre routeur** est la liaison (interface du routeur) menant vers le réseau de l'enseignant (et Internet) ;
- ◇ le **côté LAN de votre routeur** est la liaison (interface du routeur) au *switch* (LAN) du binôme.


La figure 3 schématise le réseau qui sera formé au cours du TP, avec les LAN des binômes, mais sans les PC-IUT (l'organisation exacte peut être sensiblement différente). Le réseau géré par l'enseignant se trouve dans la partie basse de la figure. Il comprend :

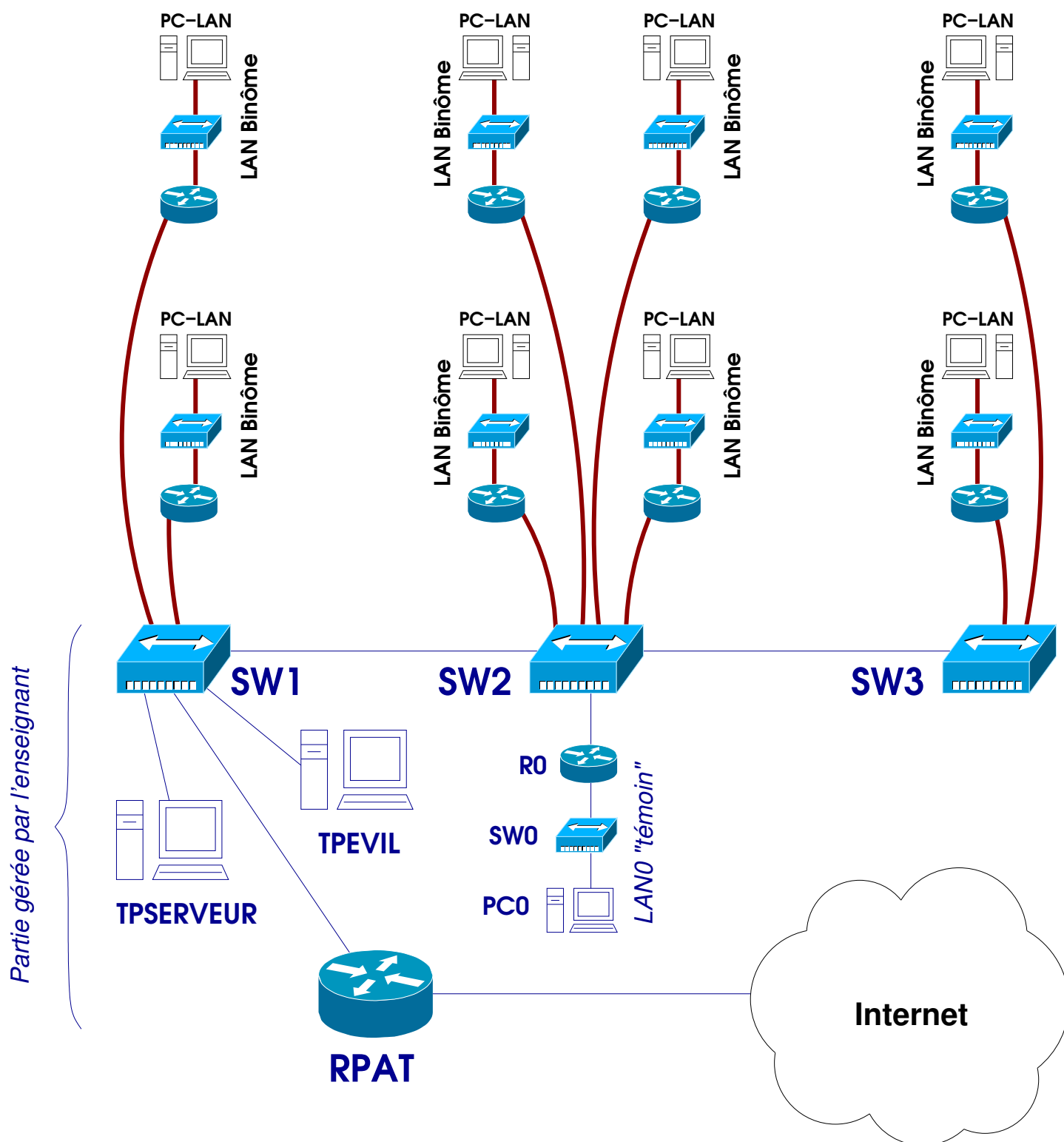
- 3 switchs (**SW1**, **SW2** et **SW3**) pour le raccordement WAN des binômes
- le routeur **RPAT** qui mène vers Internet
- deux PC/serveurs nommés **TPSERVEUR** et **TPEVIL**
- un LAN "témoin" **LAN0** constitué de **R0**, **SW0** et de **PC0**.

 Notons que les adresses IP de tous les équipements (votre LAN ainsi que RPAT, TPSERVEUR, TPEVIL etc.) font partie des paramètres qui vous ont été remis et diffèrent d'un groupe à l'autre.

 **L'emplacement des binômes n'a pas d'importance.** Nous y reviendrons quand sera présentée la **topologie logique** du réseau de l'enseignant.

 **L'environnement de travail doit être restitué dans le même état en fin de séance, propre, les câbles correctement enroulés et attachés.**  
**Les binômes ne respectant pas ces consignes seront pénalisés !**

 Ainsi qu'il est dit en début de TP, il faut prévoir au minimum 15 minutes en fin de séance pour fournir vos réalisations, restaurer le routeur et ranger l'environnement de travail. . .



**FIGURE 3** – Topologie physique globale du réseau du TP, où figurent en haut tous les LAN des binômes sans les PC-IUT. La partie du bas (switches SW1 à SW3, RPAT, les 2 PCS/serveurs et le LAN "témoin" LAN0) est gérée par l'enseignant. Les binômes devront câbler et configurer les liaisons en traits épais rouges.

## I.2 Création du rapport sur le PC-IUT



Un rapport et un certain nombre de fichiers seront à remettre à l'enseignant, de préférence par courrier électronique, à une adresse qu'il précisera. Le PC-IUT pourra servir à cet envoi car il reste connecté au réseau du département. La rédaction du rapport doit se faire de préférence sur le PC-IUT. Les fichiers à remettre créés sur le PC-LAN devront être déposés sur le PC-IUT, soit par clé USB, soit via le réseau si l'avancement du binôme le permet.



**On devrait se passer d'utiliser les clés USB directement dans les VM! Notamment, la VM XP peut ne pas supporter les clés de grande capacité. Ne les monter que sur le PC (système hôte) et utiliser le partage de fichiers entre les VM et le PC pour copier les fichiers.**

### Exercice 2 (rapport du PC-IUT)

Sur le PC-IUT, ouvrir **LibreOffice Writer** (menu *Applications* → *Bureautique*) et commencer la rédaction de votre rapport en faisant figurer vos noms, prénoms, numéro de groupe et de binôme. L'enregistrer sous le nom *groupe-binôme-Nom1\_Nom2-pciut.odt* où *Nom1* et *Nom2* sont vos noms.

 Dans l'énoncé, l'icône  précise les informations à rendre, soit dans le rapport, soit dans un fichier séparé.



**Un rapport non soigné ou difficilement lisible entraînera des pénalités! Utiliser une police à chasse fixe (type Courrier) et moduler sa taille pour les commandes tapées et leur résultat, qui doivent apparaître clairement afin de faciliter le contrôle par l'enseignant. Penser à indiquer le numéro de l'exercice correspondant à vos réponses!**

## I.3 Création (d'une partie) du rapport sur le PC-LAN

### Exercice 3 (rapport du PC-LAN)




**Sur le PC-LAN, vous devez être logé uniquement en tant que l'utilisateur test. Si ce n'est pas le cas, fermer votre session et revoir la procédure de démarrage du TP...**

Vous aurez un certain nombre de choses à reporter sur le PC-LAN aussi. Pour cela, créer un deuxième rapport avec **LibreOffice Writer** sous le nom *groupe-binôme-Nom1\_Nom2-pclan.odt*. De même que pour PC-IUT, commencer la rédaction de votre rapport en faisant figurer vos noms, prénoms, numéro de groupe et de binôme.

## I.4 Lancement des machines virtuelles sur le PC-LAN


Comme vous, l'utilisateur test n'a pas les droits d'administration. Vous ne pouvez (et ne devez) donc pas administrer directement ce PC, notamment sa configuration réseau. Cela dit, grâce à **VirtualBox**, nous allons y exécuter deux machines virtuelles : sous GNU/Linux (Debian Buster) et sous Windows XP. Vous en serez les administrateurs. Notons que dans ce TP, on utilisera principalement la VM Debian. Dans ces VM, vous pourrez


utiliser toutes les commandes d'administration nécessaires pour l'intégrer dans le LAN que vous allez constituer. Nous administrerons ces VM plus tard, mais nous les créons maintenant car cela prend du temps...


-  Pour être raccordées à votre LAN, les VM sont chacune créées avec une **carte réseau virtuelle** reliée par un bridge (pont virtuel) à la carte réseau du PC-LAN. Cela leur donne la possibilité d'émettre des trames avec leur propre adresse MAC en utilisant la carte réseau de l'hôte, mais aussi d'en recevoir, sans gêner le système hôte qui peut continuer à émettre et recevoir ses propres trames.


#### Exercice 4 (Lancement des machines virtuelles sur le PC-LAN)


1. Sur le PC-LAN, ouvrir **VirtualBox** (menu *Outils système* → *Oracle VM VirtualBox*). S'il y a des VM dans le panneau de gauche (probablement), faire un clic droit sur chacune et demander leur suppression, ainsi que tous leurs fichiers !
2. Sur un terminal du PC-LAN, taper la commande (exécution du script) **mkbusterbrg.bash** qui automatise la création et le lancement d'une machine virtuelle Debian GNU/Linux 10 « Buster » qu'on appellera par la suite **VMDEB**. Répondre aux questions concernant votre groupe d'étudiant et votre numéro de binôme ;


 Observer les informations affichées en début d'exécution. Sur cette VM, vous vous logerez en tant que **totoadm** mais vous pourrez réaliser des tâches d'administration en préfixant les commandes d'administration (nécessitant donc les droits de root) par **sudo**.

3.  Noter l'adresse MAC qui a été donnée à la carte réseau de cette VMDEB ;
4. Sur VMDEB :
  - (a) Se logger graphiquement en tant que **totoadm** ; mot de passe **<re>z0++**.

 Rappelons que cet utilisateur dispose de tous les droits d'administration, via **sudo**. En tant que membre du groupe **wireshark**, il pourra aussi capturer des trames avec **Wireshark**.

- (b)  Ouvrir un terminal. Taper la commande adéquate pour vérifier l'adresse MAC de la carte réseau. L'indiquer dans le rapport.


 Rappelons que de nombreuses commandes d'administration se trouvent dans des répertoires tels que **/sbin** ou **/usr/sbin** qui ne figurent pas dans le **PATH** d'un utilisateur normal. Pour les utiliser, soit spécifier leur chemin complet, ou les préfixer par **sudo** (car le **PATH** de root contient ces chemins).


 **Dans le rapport, reporter systématiquement la (les) commande tapée(s) en gras, ainsi que sa (leur) sortie dans une police à chasse fixe de type courrier. Puis interpréter le résultat pour répondre à la question posée.**

- (c) Cliquer dans le coin haut droit (icônes d'état) et, dans le menu du réseau filaire, sélectionner « Éteindre ». Nous activerons manuellement en ligne de commandes la connexion réseau plus tard.



5. Le partage de fichiers entre le système hôte et VMDEB est déjà opérationnel. Ainsi, le répertoire `hostshared` dans le répertoire d'accueil de `totoadm` est partagé avec le répertoire `vmshared` du bureau de l'utilisateur `test` sur le système hôte. Vérifier que ce partage est bien opérationnel en créant un fichier quelconque.

 Sur la VMDEB, enregistrer les fichiers demandés directement sur le partage. Vérifier chaque fois que les fichiers ainsi enregistrés sont bien présents sur le système hôte (PC-LAN).

6. Le partage du presse-papier (pour faire des copier-coller entre la VMDEB et le PC-LAN), devrait être lui aussi déjà activé, en mode bidirectionnel. Vérifier qu'il fonctionne correctement.
7. La VMDEB étant maintenant opérationnelle, revenir sur le système hôte. Sur un autre terminal de PC-LAN, taper la commande **`mkwinxpbrg.bash`** pour exécuter le script qui automatise la création et le lancement d'une nouvelle VM mais sous Windows XP, qu'on appellera ensuite **VMXP**. Répondre aux différentes questions et la démarrer. Noter son adresse MAC.
8. Sur VMXP :
- (a) Le partage de fichiers entre le système hôte et VMXP est lui aussi déjà opérationnel. Ainsi, le disque `Y:` est partagé avec le répertoire `vmshared` du bureau de l'utilisateur `test` sur le système hôte. Vérifier que ce partage est bien opérationnel en créant un fichier quelconque.
  - (b) De même, le presse-papier bidirectionnel est déjà activé pour cette VM. Vérifier qu'il fonctionne correctement.
  - (c)  Ouvrir un invite de commandes (menu *Démarrer, Exécuter*, puis **`cmd`**), taper la commande adéquate pour vérifier l'adresse MAC de la carte réseau. L'indiquer dans le rapport.

## II Minicom pour accéder à la console du routeur

Nous allons procéder à la mise en place de la console, à partir de laquelle nous prendrons le contrôle du routeur. Pour plus d'informations, consulter [DocCisco](#), section 4.

### Exercice 5 (Minicom pour émuler la console)

Dans un premier temps, le routeur sera administré via son port console, relié au PC-IUT sur lequel nous utiliserons **minicom** (cf. [DocCisco](#), section 4.2). Réaliser les étapes suivantes pour accéder à la console du routeur :

1. Utiliser le câble console (bleu clair) pour relier le port série du PC-IUT et le port console du routeur
2. Dans une fenêtre terminal sur le PC-IUT, lancer **minicom** dans son mode de configuration :

```
$ minicom -s
```

3. Un menu s'affiche. Utiliser les flèches pour choisir *Configurer le port série* :

```
+-----[configuration]-----+
| Noms de fichiers et chemins   |
| Protocoles de transfert      |
| Configuration du port série  |
| Modem et appel               |
| Ecran et clavier             |
| Enregistrer config. sous dfl |
| Enregistrer la configuration sous... |
| Sortir                       |
| Sortir de Minicom            |
+-----+
```

4. Le sous-menu affiché résume les paramètres actuels dont certains doivent être modifiés :

```
+-----+
| A -                               Port série : /dev/ttyS1 |
| B - Emplacement du fichier de verrouillage : /var/lock   |
| C -           Programme d'appel intérieur :              |
| D -           Programme d'appel extérieur :              |
| E -                               Débit/Parité/Bits : 115200 8N1 |
| F -                               Contrôle de flux matériel : Oui |
| G -                               Contrôle de flux logiciel : Non |
|                               |
|   Changer quel réglage ? [ ] |
+-----+
```

5. Taper **A** et spécifier le port série **/dev/ttyS0** puis valider le changement par **Entrée**

6. Taper **E** pour modifier les paramètres de communication. Le sous-menu correspondant devrait être :

```
+---[Paramètres de communication]---+
|
|   Actuellement : 115200 8N1
|   Speed          Parity      Data
|   A: <next>      L: None     S: 5
|   B: <prev>      M: Even     T: 6
|   C: 9600        N: Odd      U: 7
|   D: 38400       O: Mark     V: 8
|   E: 115200      P: Space
|
|   Stopbits
|   W: 1           Q: 8-N-1
|   X: 2           R: 7-E-1
|
|   Choix, ou <Entrée> pour sortir ?
+-----+
```

Modifier les paramètres pour obtenir **9600 8N1** (9600 baud ; 8 bits de données ; pas de bit de parité ; 1 bit stop). Valider les changements en tapant **Entrée**

7. Taper à nouveau **Entrée** pour revenir au menu principal
8. Puis, choisir "*Sortir*" afin de commencer la simulation du terminal. L'affichage devrait ressembler à :

```
Bienvenue avec minicom 2.3

OPTIONS: I18n
Compilé le Feb 24 2008, 16:35:15.
Port /dev/ttyS0


Tapez CTRL-A Z pour voir l'aide concernant les touches spéciales
```


9. Démarrer le routeur. Les premiers messages du routeur devraient apparaître sur la fenêtre **minicom** :

```
System Bootstrap, Version 12.2(7r)XM2, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2003 by cisco Systems, Inc.
```

Si, après quelques secondes, toujours rien n'est affiché, éteindre le routeur et revoir le câblage et les paramètres de **minicom**

10. Le routeur est plus ou moins long avant d'être opérationnel. Attendre qu'il affiche le prompt (tel que **Router>** ou **2600-2>**) ou un message vous invitant à taper sur **Entrée** (auquel cas, taper **Entrée** pour afficher le prompt). Le prompt est affiché par la CLI (*Command Line Interface*), qui est une sorte de shell fourni par le système du routeur CISCO : l'IOS (*Internetwork Operating System*).


 Il peut arriver que l'affichage du prompt passe inaperçu suite à l'affichage de messages d'information (lignes commençant par %). Si le prompt n'est toujours pas apparent après un temps significatif d'inactivité du routeur, taper **Entrée**, ce qui devrait le faire afficher.

 **Si le routeur vous demande (en anglais) si vous voulez entrer dans le menu de configuration, répondre no !**

11. Passer en mode privilégié en tapant :

```
Router>enable
Password: mypassword2
Router#
```


↔ Le prompt doit changer et se terminer par #

12.  Il se peut que le routeur affiche des messages d'information alors qu'on tape une commande, ce qui est très gênant. Pour réafficher la commande en cours de frappe, taper **CTRL-L**. Mais pour l'éviter, ainsi que d'autres ennuis, il vaut mieux effectuer les configurations suivantes (mettre dans le rapport l'ensemble des commandes et du prompt) :

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no cdp run
Router(config)#no ip domain-lookup
Router(config)#hostname G-B (remplacer par votre groupe et votre binôme)
G-B(config)#line con 0
G-B(config-line)#logging synchronous
G-B(config-line)#end
G-B#
%SYS-5-CONFIG_I: Configured from console by console
```

13. Enfin, sauver la configuration en cours en tapant :

```
G-B#copy run start
Destination filename [startup-config]? ↵
Building configuration...
[OK]
G-B#
```

 **Après avoir tapé la commande de la première ligne, l'IOS vous demande de confirmer le fichier de destination (entre crochets avant le ?). Taper juste **Entrée** et surtout pas autre chose sous peine d'écraser le système du routeur et être pénalisé !**

## Rappel sur les modes de la CLI

On rappelle que la CLI admet 4 modes principaux, chacun destiné à un type de configuration :

- **mode utilisateur** (*user mode*) : accès à un nombre limité de commandes, *a priori* inoffensives, permettant simplement d'observer l'état du routeur ;
- **mode privilégié** (*enable mode*) : manipulation des fichiers de configuration et tâches diverses ;
- **mode de configuration globale** : modification des paramètres globaux réseaux du routeur comme l'activation de certains protocoles ou fonctionnalités ;
- **mode de configuration d'interface** : configuration d'interface, notamment de ses paramètres IP

Comme le montre la figure 4, les modes ont chacun un prompt propre, et des commandes (en gras) permettent de passer d'un mode à l'autre. Le prompt actuellement affiché est celui du mode utilisateur.

❶ La plupart des commandes peuvent être abrégées, la tabulation permet de compléter des mots et la touche ? apporte une aide contextuelle. Par exemple, la dernière commande de l'exercice précédent est une abréviation de **copy running-config nvram:startup-config**, qui limite les risques d'erreurs de frappe et d'écrasement du système. Plus d'information sur l'IOS et la CLI sont disponibles dans [DocCisco](#), section 2.

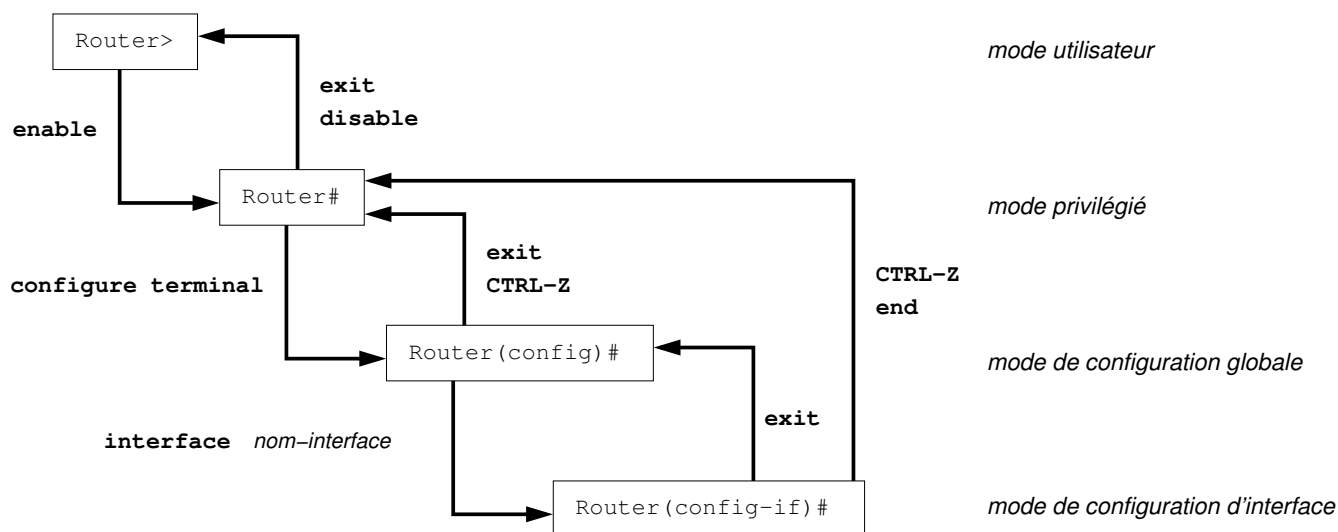


FIGURE 4 – Les principaux modes de la CLI

### III Conception Réseau

Nous allons nous pencher maintenant sur la partie "réseau". Mais avant de procéder à la configuration effective du matériel, nous allons travailler sur papier et nous pencher d'un peu plus près sur l'organisation du réseau mis en place et son plan d'adressage.

#### Exercice 6 (conception réseau)



**Aucune configuration ne seront demandés dans cet exercice, où l'on travaille exclusivement sur papier !**

1. Situer votre routeur et votre réseau local (LAN) sur le schéma global du réseau de la figure 3 de la page 6 (où seul figure votre PC-LAN et non le PC-IUT), qui devra être mis en place pour le TP.
2. Repérage des interfaces : repérer le nom des interfaces sur le chassis de votre routeur que vous relierez côté WAN et côté LAN. Choisir comme interface LAN de votre routeur, l'interface Ethernet qui admet le plus grand débit. En effet, l'essentiel du trafic réseau est supposé être local dans un LAN. L'interface WAN de votre routeur devra être choisie comme une interface Ethernet admettant éventuellement un débit moindre.
3. **(Adresses dans le LAN)** Le bloc d'adresses attribué à votre LAN, et que vous devez gérer, est indiqué dans vos paramètres. Dans votre LAN, l'adresse à attribuer à votre routeur doit être la plus grande adresse de station de votre bloc LAN, alors que celle de VMDEB du PC-LAN devra être la plus petite<sup>1</sup>. Celle de VMXP sera obtenue par DHCP mais devrait se terminer par 100. Les adresses des VM évolueront quant on configurera le service DHCP sur le routeur.
4. **(Adresses côté WAN)** Côté WAN (partie du réseau du TP gérée par l'enseignant), le réseau formé par les switchs (SW1, SW2 ou SW3), le routeur RPAT, les PC TPSEUR et TPEVIL, le LAN0 ainsi que les routeurs des binôme a une adresse indiquée dans vos paramètres, de même que l'adresse de votre routeur dans ce réseau.
5. Noter les adresses à attribuer au routeur (côtés LAN et WAN) et aux VM du PC-LAN, ainsi que les masques associés. Indiquer pour le routeur le nom IOS des interfaces correspondantes.



Utiliser un schéma du réseau est une bonne idée...

6. Écrire la table de routage (contenant les colonnes *destination*, *masque* et *routeur*) que devra avoir votre routeur en incluant :
  - les routes directes (de votre LAN et du réseau de l'enseignant) ;
  - la route vers le LAN0 (qui doit passer par R0) ;
  - les routes vers les LAN de 2 autres binômes (à préciser) ;
  - la route par défaut (pour Internet).

1. Il s'agit d'une restriction de l'énoncé car on peut attribuer n'importe quelle adresse valide à n'importe quel équipement du réseau, si elle n'est pas déjà utilisée.

## IV Configurations Réseau

### IV.1 Raccordement et configuration côté WAN






Vous allez relier votre routeur au reste du réseau du TP, géré par l'enseignant, tel que schématisé sur la figure 3 de la page 6. Pour cela, il nous faut câbler puis configurer l'interface WAN du routeur du binôme.

Rappelons que le réseau de l'enseignant comprend les switchs SW1, SW2 et SW3, placés en tête des rangées de tables, des PC, le routeur RPAT qui permet l'accès à Internet, et un LAN témoin.

On rappelle (!) que dans la CLI, la configuration et l'activation d'une interface se fait dans le **mode de configuration de l'interface** (voir [DocCisco](#), section 2.1.4). Pour entrer dans ce mode, il faut spécifier le nom IOS de l'interface à configurer :

```
Router>enable
Router#configure terminal
Router(config)#interface nom-interface
Router(config-if)#
```

#### Exercice 7 (configuration de l'interface WAN du routeur)

1.  En utilisant l'adresse de votre routeur, indiquée sur vos paramètres, réaliser la configuration (niveaux 1-2 et 3) de l'interface WAN de votre routeur et l'activer. Se reporter à [DocCisco](#), section 3 pour les commandes IOS de configuration. Ne pas laisser de configuration automatique de la vitesse et du mode duplex, et essayer de la configurer manuellement au mieux, de préférence en 100 Mbit et en full-duplex, si l'interface du routeur le permet. Vérifier à chaque tentative si l'interface est **up** (*line protocol*) et revoir à la baisse la configuration si ce n'est pas le cas. Fournir la trace des commandes de configuration que vous avez effectivement retenues, en justifiant vos choix.
2.  Depuis votre routeur, envoyer un **ping** à RPAT. En cas d'échec répété, reprendre la configuration de l'interface (et fournir les bonnes commandes !)
3.  Depuis votre routeur, envoyer un **ping** à R0. Cela doit fonctionner.
4.  Depuis votre routeur, envoyer un **ping** à TPSEUR. Cela doit aussi fonctionner.
5.  Explorer et vérifier la configuration de l'interface WAN avec les commandes suivantes (fournir les traces de leur sortie en les séparant clairement) :

```
Router#show interfaces nom-interface
Router#show interfaces nom-interface description
Router#show ip interface brief
```

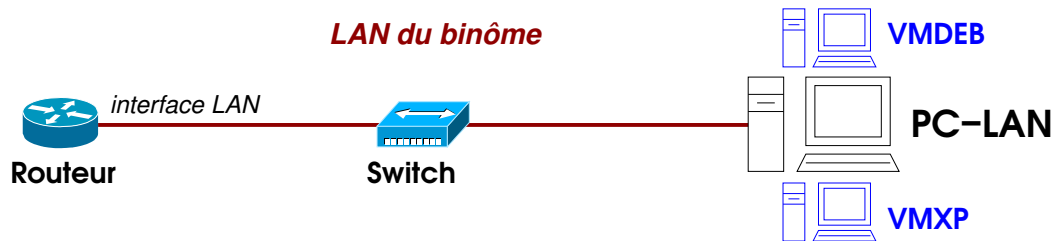
6. Pour terminer la configuration IP, enregistrer la configuration actuelle avec **copy run start**



À nouveau, taper juste **Entrée** pour confirmer le fichier de destination !!

## IV.2 Mise en place du LAN

Dans cette partie, votre binôme va configurer le LAN formé de votre routeur, d'un switch et (de VMDEB et VMXP) du PC-LAN, tel que schématisé dans la figure 5. Dans notre contexte, il faut ignorer PC-LAN et voir ces VM comme étant chacune reliées au switch par leur propre câble et leur propre interface. Dans un premier temps, on va configurer le routeur et VMDEB.




**FIGURE 5** – Topologie physique du LAN du binôme, correspondant aux traits rouges épais. Les VM de PC-LAN sont reliées au switch par l'interface Ethernet de PC-LAN.


### IV.2.A Configuration de l'interface LAN du routeur

Dans cette section, nous allons configurer l'interface LAN du routeur.

#### Exercice 8 (configuration de l'interface LAN du routeur)

1.  En vous basant sur les adresses reportées sur le schéma à l'exercice 6 (page 14), réaliser la configuration de l'interface LAN du routeur (niveaux 1-2 et 3) et l'activer. Fournir les commandes nécessaires en justifiant vos choix.

**i** Pour le moment, nous ne pouvons pas encore tester cette configuration car aucune des VM du LAN n'est encore configurée.

2.  Afficher et vérifier la configuration de l'interface avec les commandes suivantes tapées en mode privilégié :

```
Router#show interfaces nom-interface
Router#show interfaces nom-interface description
Router#show ip interface brief
```

**💣** Si la liaison reste down en ayant testé toutes les possibilités et changé de port du switch, le signaler à l'enseignant.

3. Pour terminer la configuration IP, enregistrer la configuration actuelle (...):




```
Router#copy run start
```



## IV.2.B Configuration de l'interface LAN de VMDEB

Il faut maintenant configurer l'interface réseau de VMDEB pour l'intégrer effectivement dans le LAN du binôme.

### Exercice 9 (configuration de l'interface de VMDEB)

1.  Procéder à la configuration de l'interface de VMDEB (se reporter à [DocRes](#), section 1.2 pour la configuration d'une interface réseau sous Linux) en vous basant sur les adresses reportées sur le schéma à l'exercice 6 (page 14)
2.  Sur un terminal de VMDEB, utiliser **ping** pour tester la connectivité avec votre routeur. Le ping devrait fonctionner. Revoir le câblage et les configurations (routeur et VMDEB) si cela ne va pas
3.  Sur le routeur (mode utilisateur ou privilégié), utiliser la commande **ping** pour tester la connectivité avec VMDEB


## IV.3 Configuration du routage sur le routeur

Pour le moment, le routeur ne sert pas à grand chose. Il ne peut pas encore envoyer un ping vers Internet le pauvre ! Avant de configurer son routage dans l'exercice 10, présentons comment procéder.

Tout d'abord, il faudra s'assurer d'activer le routage sur le routeur avec la commande suivante tapée en mode de configuration globale :

```
Router(config)#ip routing
```

La configuration de la table de routage est simple : on ajoute ligne par ligne les destinations qui nous intéressent.

 Il est inutile de configurer les routes directes car elles sont (ont été) générées automatiquement par l'IOS lors de la configuration des l'interfaces du routeur.

### Exemple 1

Si l'on doit ajouter la route suivante, où la colonne *Interface* indique l'interface à utiliser pour joindre le routeur correspondant :

Destination	Masque	Interface	Routeur
150.151.152.0	255.255.255.0	Serial0	195.196.20.254

alors on utilisera, en mode de configuration globale, la commande :

```
Router(config)#ip route 150.151.152.0 255.255.255.0 Serial0 195.196.20.254
```

et on utilise :

```
Router(config)#no ip route 150.151.152.0 255.255.255.0 Serial0 195.196.20.254
```







... pour l'enlever.




On peut ensuite vérifier table de routage en l'affichant avec :

```
Router#show ip route
```

## Exercice 10 (configuration de la table de routage du routeur)


1.  En vous basant sur la conception réseau de l'exercice 6, configurer les routes indirectes de votre routeur, sans oublier la route vers Internet. . .
2.  Essayer d'envoyer un ping à PC0. Il doit fonctionner. En cas d'échec répété, revoir la table de routage
3.  Essayer d'envoyer un ping à l'adresse 10.203.9.1. En cas d'échec répété, revoir la table de routage.
4.  Essayer d'envoyer un ping à l'adresse 139.124.187.1 (l'adresse d'un autre routeur de l'IUT). En cas d'échec répété, revoir la table de routage.
5.  Essayer d'envoyer un ping à la station 4.31.198.49 (station hébergeant le serveur web de [www.rfc-editor.org](http://www.rfc-editor.org)). En cas d'échec répété, revoir la table de routage
6.  Vérifier la table de routage en mode privilégié avec la commande **show ip route**. Fournir la sortie écran.

 En cas de problème, ou à des fins de vérification, vous pouvez afficher la coonfiguration courante du routeur en tapant **sh run** en mode privilégié.

## IV.4 Accès à la CLI par TELNET

Puisque notre routeur et notre VMDEB possèdent maintenant une adresse IP dans le même LAN, nous pouvons légitimement penser à exploiter le réseau pour se connecter au routeur par TELNET.


Rappelons qu'un accès à distance est vu comme un terminal réseau par le routeur. Ces terminaux sont dénommés des VTY (*Virtual Terminal*). Pour configurer le mot de passe du **terminal telnet**, il faut entrer dans le mode de configuration de cette interface en tapant **line vty 0 4** depuis le mode de configuration globale. Le prompt devrait alors changer pour devenir **(config-line)#** :

 On attendra l'exercice suivant pour configurer cet accès. . .


```
Router#conf ter
Router(config)#line vty 0 4
Router(config-line)#password mon-vty-password
Router(config-line)#login
Router(config-line)#end
Router#
```


- ➡ une fois dans la configuration du VTY, on peut entrer un le mot de passe *mon-vty-password* (avec la commande **password**) et activer la possibilité de se connecter (avec la commande **login** sans paramètre)




Une fois connecté par TELNET, on peut afficher sur le routeur les sessions TELNET en cours avec la commande **show user**.

 Lorsqu'on est connecté à la console, on ne figure pas dans la liste affichée par **show user**.


## Exercice 11 (accès par TELNET)

1.  Configurer l'accès par TELNET sur le routeur avec pour mot de passe **mypassword3**.

 Certaines configurations qui suivront pourront être faites si besoin via TELNET, notamment lorsqu'on voudra réserver la console à du "*debugging*".

2. Sur VMDEB, lancer **Wireshark** et commencer la capture de trames sur son interface LAN
3.  Se connecter au routeur par TELNET à partir de VMDEB. Cela doit fonctionner !
4.  Sur VMDEB, arrêter la capture et la sauver dans **11-telnet-all.pcap**
5.  Filtrer l'affichage des trames capturées pour ne retenir que le trafic TELNET. Faire une capture d'écran, et la sauver dans **11-telnet-filtre.png**. Sauver ces trames (uniquement) dans **11-telnet-filtre.pcap**

 On rappelle qu'un serveur TELNET utilise le port 23 de TCP

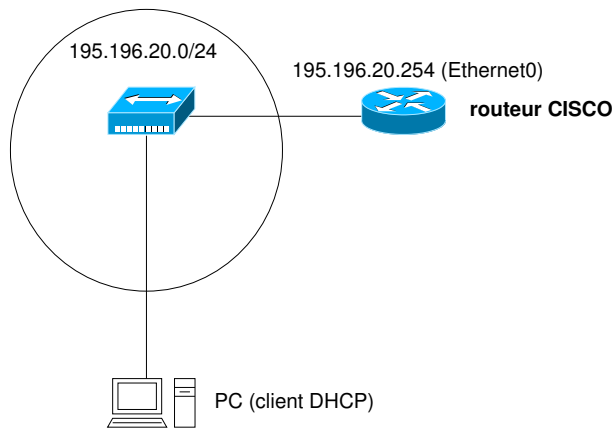
6.  Faire afficher les données TCP échangées, où l'on doit voir apparaître le mot de passe transmis par TELNET
7. Sur le routeur, sauvegarder la configuration actuelle

## V Serveur DHCP sur le routeur

Plutôt que de continuer à configurer manuellement les VM du PC-LAN, vous allez configurer un serveur DHCP sur votre routeur, puis demander aux VMs de se configurer par DHCP.

### V.1 Configuration de l'allocation dynamique

L'allocation (ou attribution) dynamique consiste à attribuer une adresse IP non utilisée à un client qui en fait la demande.



**FIGURE 6** – Réseau de l'exemple 2, où le routeur peut offrir le service DHCP pour les PC du LAN qui ont un client DHCP

#### Exemple 2

Soit le réseau d'adresse 195.196.20.0/24 présenté à la figure 6 sur lequel le routeur 195.196.20.254/24 doit faire office de serveur DHCP. Supposons que les adresses IP 195.196.20.250 à 195.196.20.254 ne doivent pas être allouées dynamiquement : elles sont déjà utilisées par des stations, ou sont à attribuer statiquement (voir section suivante). Une configuration possible du routeur serait :

```
Router#show running-config
...
ip dhcp excluded-address 195.196.20.250 195.196.20.254
!
ip dhcp pool my-pool
 network 195.196.20.0 255.255.255.0
 dns-server 195.196.20.1 195.196.110.10 150.151.152.3
 domain-name un.domaine.fr
 default-router 195.196.20.254
 lease 0 2
!
interface Ethernet0
 ip address 195.196.20.254 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
service dhcp
...
```

où les quatre parties de cette configuration comprennent :

- l'exclusion des adresses 195.196.20.250 à 195.196.20.254 du panel d'adresses attribuables dynamiquement
- la définition d'un *pool* d'attribution dynamique nommé *my-pool* comprenant les adresses attribuables ainsi que les informations à communiquer aux clients :
  - ◇ le réseau a pour adresse 195.196.20.0 de masque 255.255.255.0. Ces informations, comme celles qui suivent, sont communiquées au client. Aussi cette information indique au routeur les adresses qu'il doit allouer dynamiquement (moins celles exclues). On en déduit que le routeur allouera dynamiquement les adresses 195.196.20.1 à 195.196.20.249
  - ◇ les serveurs DNS à utiliser, par ordre de préférence, sont 195.196.20.1, 195.196.110.10 et 150.151.152.3
  - ◇ le domaine DNS par défaut est un.domaine.fr. Pour un client DHCP, cela correspondant au champ **search** de */etc/resolv.conf*
  - ◇ le routeur par défaut est 195.196.20.254
  - ◇ la durée du bail est fixée à 0 jour et 2 heures
- la configuration de l'interface du routeur sur le réseau 195.196.20.0/24
- l'activation du service DHCP



## Exercice 12 (configuration du service DHCP sur le routeur)

Il est temps de configurer le service DHCP du routeur, puis de le tester :

1.  Sur le routeur, passer d'abord en **mode configuration globale**. Puis, utiliser la commande

```
Router(config)#ip dhcp excluded-address début-adr-exclue [ fin-adr-exclue]
```


pour exclure du "pool" d'adresses allouées dynamiquement, celles qui ne doivent pas l'être (et uniquement celles-ci).

Ne permettre l'attribution que des adresses se terminant entre 100 et 150 dans votre LAN. Le paramètre *fin-adr-exclue* est optionnel. S'il est manquant, seule *début-adr-exclue* est exclue. Vous pouvez utiliser plusieurs fois cette commande, s'il y a plusieurs plages ou adresses à exclure. Fournir les commandes tapées.

2. Passer ensuite en *mode dhcp pool configuration* avec la commande :

```
Router(config)#ip dhcp pool nom-pool
```

où *nom-pool* est un nom pour cette configuration

3. En mode *dhcp pool configuration*, taper ? pour obtenir la liste des commandes disponibles.
4.  Configurer ce *pool* en adaptant les paramètres de l'exemple précédent à votre environnement (plage d'adresses IP, serveur DNS, nom de domaine, routeur par défaut et durée de bail), sachant que :
  - le nom de domaine est univ-amu.fr;
  - les serveurs DNS sont (dans l'ordre) : 10.193.51.5, 139.124.1.2 et 9.9.9.9;
  - le bail doit durer 2,5 jours.

Fournir les commandes (et le pool).





5. Retourner au mode de configuration globale, et activer le service DHCP avec la commande :


```
Router(config)#service dhcp
```



6. En mode privilégié, sauvegarder votre configuration avec **copy run start**
7. En mode privilégié **sur la console du routeur**, taper :

```
Router#debug ip dhcp server events
```

pour activer le *debugage* des événements liées à l'activité du serveur DHCP.

8. Sur VMXP, utiliser le service DHCP pour configurer l'interface (carte) réseau. Pour cela vous pouvez simplement désactiver puis réactiver la carte réseau Ethernet, dont la configuration est accessible via le *Panneau de configuration*, puis *Connexions réseau*. Un clic droit sur la carte propose un menu avec différents réglages (mais vous le savez déjà, n'est-ce pas ?).
9.  Faire une capture d'écran des messages affichés sur la console du routeur et la nommer **12-dhcp.png**
10.  Sur VMXP, ouvrir un invite de commandes et envoyer un ping vers votre routeur. Cela doit fonctionner !
11.  Sur VMXP, effectuer un ping vers VMDEB. Cela doit fonctionner.
12.  Sur VMXP, effectuer un ping vers R0. Cela doit fonctionner.

 Il n'est pas possible pour le moment, d'effectuer avec succès un ping de RPAT, ni du reste d'Internet !

13.  Sur VMXP, effectuer un ping vers PC0. Cela doit fonctionner.
14.  Sur la connexion TELNET au routeur depuis VMDEB, vérifier le serveur DHCP comme suit :

```
Routeur#show ip dhcp server statistics
```

```
Memory usage      13906
```

```
Address pools     1
```

```
...
```

```
Routeur#show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
195.196.20.2	0021.9bdf.dbf9	Mar 01 2010 02:28 AM	Automatic

```
...
```

## V.2 Configuration de l'allocation statique

L'inconvénient avec l'allocation dynamique d'adresse est qu'on ne sait jamais trop quelle adresse on va obtenir, puisque le serveur DHCP nous donnera la première disponible (ou éventuellement la dernière adresse qu'on avait obtenu). C'est parfois gênant et on peut souhaiter que le serveur nous attribue toujours une adresse précise : c'est l'allocation statique.

Cette allocation particulière —de type BOOTP— demande à ce que le serveur soit configuré pour reconnaître des clients en particulier, en se basant sur leur adresse MAC, et leur allouer toujours la même adresse. Sur un routeur CISCO, il faut définir une *pool* par client "statique".

### Exemple 3

Supposons que le routeur/serveur DHCP précédent doit attribuer statiquement l'adresse 195.196.20.250 à la station possédant l'adresse MAC 00:21:9b:df:db:a1, alors en plus du *pool* précédent, on peut ajouter un autre *pool* pour cette allocation :

```
ip dhcp pool pool-toto
host 195.196.20.250 255.255.255.0
hardware-address 0021.9bdf.dba1
client-name ordidetoto
```

- ⇒ où l'on voit que l'adresse MAC du client est au "format CISCO", et le paramètre **client-name** communique au client son nom court (information ignorée par défaut par le client). Les mêmes paramètres que précédemment peuvent être définis dans ce *pool*, mais puisque le paramètre **host** indique une adresse IP appartenant au réseau indiqué en paramètre **network** du *pool* précédent (my-pool), l'ensemble des paramètres de my-pool sont hérités par ce *pool* (mais peuvent être redéfinis).

✍ On peut remarquer que l'adresse allouée statiquement est une des adresses qui avaient été exclues de l'ensemble des adresses allouables dynamiquement.



### Exercice 13 (configuration de l'allocation statique)

1. Sur la connexion TELNET au routeur, définir un *pool* statique pour la VMDEB en lui associant la plus grande adresse **disponible** de son réseau avec une allocation pour une durée de 5 jours
2. Sur VMDEB, arrêter la session TELNET au routeur
3. Sur VMDEB, lancer une capture de toutes les trames avec **Wireshark**
4. Sur la console du routeur, s'assurer que le mode *debug* pour DHCP est toujours actif, sinon le réactiver
5. ✍ Sur VMDEB, configurer l'interface par DHCP avec **dhclient** :

```
vmdeb# sudo dhclient -v interface
```

où *interface* est l'interface de VMDEB à configurer par DHCP.

6. ✍ Observer les messages sur la console du routeur.
7. ✍ Sur VMDEB, s'assurer que l'adresse obtenue est celle attendue. Fournir :
  1. le résultat de **ifconfig**




On devrait constater avec stupéfaction que pour une raison obscure **ifconfig** affiche l'ancienne adresse et non celle obtenue par DHCP. Pour corriger ce défaut, activer le réseau filaire via les icônes du coin haut droit du bureau, et recommencer **ifconfig** qui devrait maintenant afficher la bonne adresse.

Une alternative est de taper la commande suivante :







```
vmdeb# sudo nmcli connection up ifname interface
```

2. le résultat de **route -n**
3. le contenu de `/etc/resolv.conf`
4. la partie de `/var/lib/dhcp/dhclient.leases` concernant l'interface ainsi configurée

 Selon l'OS du routeur, il est possible que VMDEB garde l'IP précédemment obtenue par l'allocation dynamique, malgré la nouvelle configuration statique. Dans ce cas, il faut demander au routeur de supprimer l'allocation dynamique de VMDEB en tapant, en mode privilégié :

```
# clear ip dhcp binding ip-dynamique-de-vmdeb
```

et reprendre à partir de la question 3 de cet exercice.

8.  Sur VMDEB, envoyer un ping vers votre routeur. Cela doit fonctionner !
9.  Sur VMDEB, effectuer un ping vers R0. Cela doit fonctionner !
10.  Sur VMDEB, effectuer un ping vers PC0. Cela doit fonctionner !
11.  Sur VMDEB, se connecter à nouveau au routeur par TELNET.
12.  Sur la session TELNET, exécuter **show ip dhcp binding** et commenter son résultat
13.  Sur VMDEB, Arrêter la capture des trames. Sauver les trames dans le fichier **13-dhcp-all.pcap**. Filtrer l'affichage pour ne retenir que les trames concernant DHCP. Faire une capture d'écran nommée **13-dhcp.png**. Sauver ces trames DHCP dans le fichier **13-dhcp-filtre.pcap**.
14. Sur la console du routeur, désactiver le *debugage* des événements DHCP en annulant la commande qui l'a activé :

```
Router#no debug ip dhcp server events
```


15. Sur la console du routeur, sauvegarder votre configuration
16. Sur VMDEB, tenter un ping de RPATet de 4.31.198.49. Cela devrait échouer.
17. Sur VMXP, tenter un ping des adresses RPAT. Cela devrait aussi échouer ! On règlera ça dans la partie suivante.



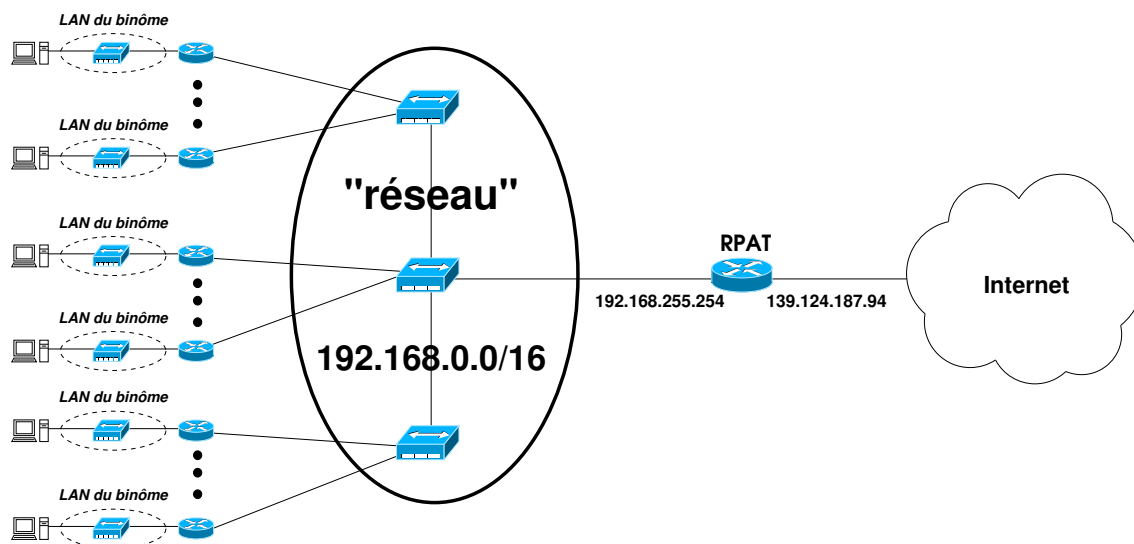
## VI Configuration du NAT/PAT

Vous avez pu constater que la discussion entre VMDEB et Internet n'est pas possible, de même que pour VMXP. Elle ne l'est même pas avec RPAT ! En fait, les VM peuvent tout à fait envoyer un datagramme à un hôte d'Internet. C'est la réponse qui ne peut leur revenir ! En effet, la réponse a pour adresse de destination celle de VMDEB(ou de VMXP). C'est une adresse dans votre LAN faisant partie des plages d'adresses privées non routables sur Internet (RFC 1918 et RFC 3927) : 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 et 169.254.0.0/16. En clair, les routeurs d'Internet ne sont censés connaître l'emplacement de votre LAN privé et les réponses éventuelles sont perdues.

Mais vous avez pu aussi constater que votre routeur a accès à Internet, alors qu'il utilise lui aussi une adresse privée pour son interface WAN (dans le réseau de l'enseignant) ! Ceci parce que le PAT est activé sur RPAT pour permettre aux équipements faisant partie du réseau de l'enseignant, et notamment vos routeurs, de communiquer avec Internet. Mais RPAT n'est pas configuré pour permettre cet accès à vos LAN, dont il ignore même l'existence. Afin de permettre l'accès à Internet aux stations de votre LAN, vous devrez configurer le PAT sur votre propre routeur.

 Dans ce qui suit, nous supposons (probablement à tort) dans les exemples que le réseau "enseignant" du TP a pour adresse **192.168.0.0/16** et que RPAT y possède l'adresse **192.168.255.254**. Adapter ces données aux paramètres de votre groupe/binôme.

### VI.1 Le PAT sur le routeur d'accès vers Internet (RPAT)

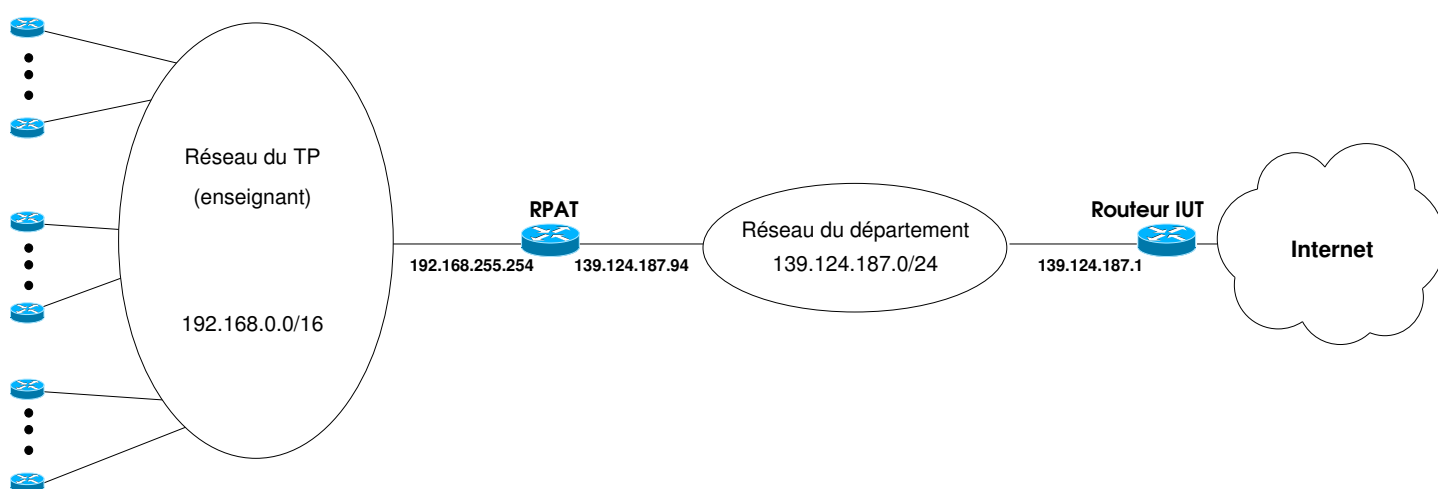


**FIGURE 7** – Schéma simplifié du réseau du TP ne présentant que les routeurs et LAN des binôme, ainsi que l'emplacement de RPAT sur le chemin d'Internet.

Avant d'entrer dans les détails, présentons dès maintenant ce que fait RPAT vers Internet. Sa situation est illustrée par la figure 7. Il met en œuvre le PAT (*Port Address Translation*) —contraction de NAPT (*Network Address and Port Translation*), soit en français « traduction d'adresse réseau et de port ». Le PAT est aussi appelé « *single address NAT* » ou encore « *port-level multiplexed NAT* », une variante du NAT (*Network Address Translation*), en français « traduction d'adresse réseau ». Aujourd'hui, le terme NAT (ou *aliasing*) est souvent utilisé pour désigner l'ensemble des techniques NAT y compris le PAT.

Vu d'Internet, le réseau 192.168.0.0/16 n'existe pas, et donc ni aucun de vos routeurs, et encore moins vos LANS. Seule est connue et **routable** l'adresse IP publique de RPAT (voir paramètres), qui est relié au réseau du département. Considérons que c'est **139.124.187.94**. Pour permettre aux équipements du réseau 192.168.0.0/16 de communiquer avec l'extérieur, ce dernier doit modifier les messages envoyés afin que les réponses puissent revenir.

✍ Avant d'aller plus loin, il faut savoir que RPAT joue pour vos LAN le rôle d'un hôte d'Internet : il ignore leur existence et ne connaît que les hôtes du réseau 192.168.0.0/16, ce qui inclut vos routeurs. La "vision" de RPAT peut alors se résumer au schéma de la figure 8. Ainsi, pour RPAT, vos routeurs ne sont que des hôtes (et seront traités comme tels dans les exemples qui suivent).

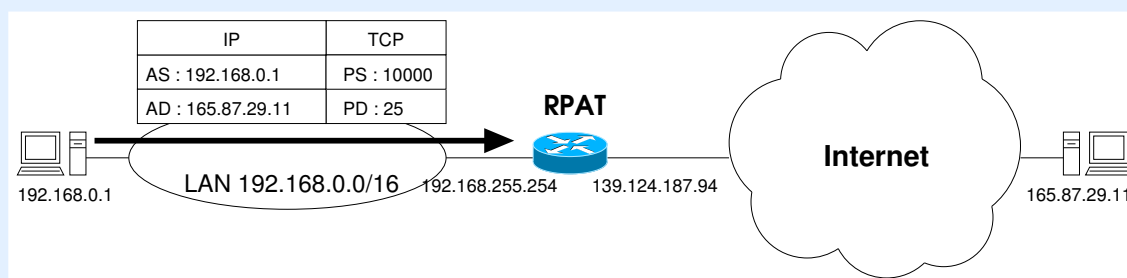


**FIGURE 8** – Réseaux "connus" de RPAT. On remarque que les routeurs des binômes sont présents sur la gauche mais pas les LANs des binômes qui sont inconnus de RPAT. Pour RPAT, les routeurs des binômes ne sont que des hôtes.

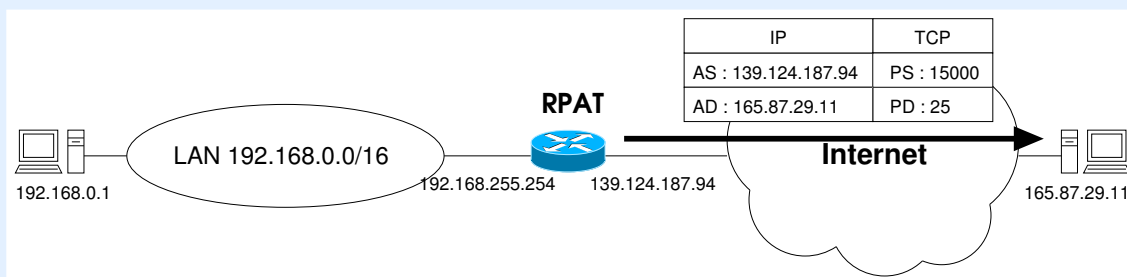
### Exemple 4

Suivons un exemple pour en comprendre le principe, où hôte (ce pourrait être un de vos routeurs) du réseau 192.168.0.0/16 entame un dialogue avec un hôte d'Internet. Dans les schémas, on utilisera les abréviations suivantes : AS : adresse source ; AD : adresse destination ; PS : port source et PD : port destination.

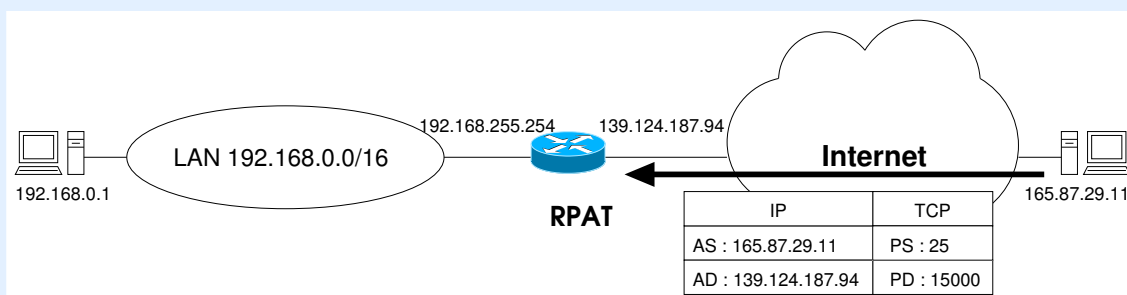
1. l'hôte 192.168.0.1 du réseau privé envoie un message TCP de port source 10000 à direction du port 25 (serveur SMTP) de l'hôte 165.87.29.11 d'Internet :



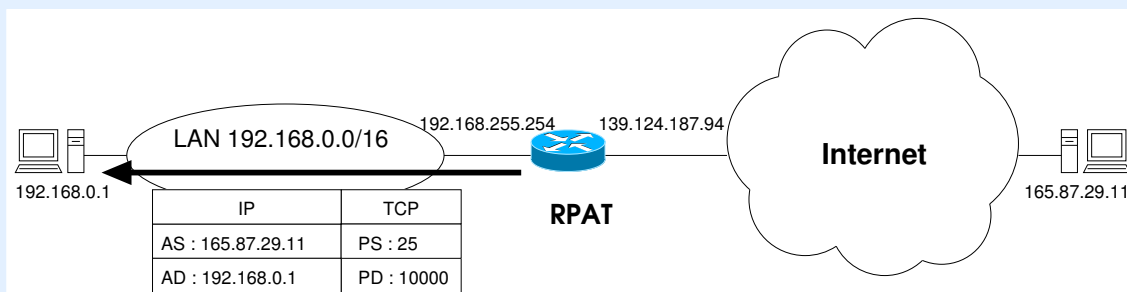
2. arrivé au routeur d'accès vers Internet, celui-ci remplace l'adresse source du datagramme par la sienne 139.124.187.94 et le port source par le port 15000, met à jour sa table de traductions PAT, puis route le datagramme vers Internet :



3. le serveur SMTP de 165.87.29.11 envoie en réponse un message à destination du port 15000 de 139.124.187.94 :



4. arrivée au routeur d'accès vers Internet, celui-ci consulte sa table PAT, qui lui dit de remplacer l'adresse 139.124.187.94 et le port 15000 par 192.168.0.1 et 10000. Puis il route le datagramme sur le réseau 192.168.0.0/16 :



5. la réponse parvient alors à 192.168.0.1 et est remise à l'application utilisant le port TCP 10000.



L'exemple précédent montre une partie d'une communication TCP. Ce peut être aussi une communication UDP ou ICMP. Le routeur PAT **traduit** (*translate*) les adresses IP et les ports afin que ne sortent vers Internet que des datagrammes ayant pour adresse source son adresse publique, et que les réponses revenant soient correctement acheminées vers leurs destinataires réels du LAN. C'est exactement les opérations des \*Box que les FAI mettent à disposition des particuliers.

## VI.2 Principes et terminologie du NAT

❗ Cette section reprend les notions présentées en cours. Vous pouvez la sauter et passer à la section **VI.3** si vous maîtrisez la terminologie et les concepts du PAT.

Le NAT (*Network Address Translation*) —ou *traduction d'adresse réseau*— a été proposé en 1994 dans la RFC 1631<sup>2</sup> comme solution à court terme face au manque d'adresses IPv4, le temps de mettre au point IPv6 et de le déployer. Le NAT a des inconvénients parce qu'il contredit le principe selon lequel les adresses IP des datagrammes doivent être celles des extrémités du dialogue. Il complique alors considérablement les communications pour certains protocoles (DNS, FTP, peer-to-peer, authentification/chiffrement, ...). Mais ses avantages sont tels qu'il sera probablement encore utilisé après le déploiement d'IPv6, qui se fait du coup sans précipitation.

L'objectif principal du NAT était de permettre aux adresses IP publiques d'être partagées par un grand nombre de périphériques réseau qui utiliseraient des adresses IP n'ayant pas de signification dans Internet (en particulier, les adresses privées définies dans la RFC 1918).

Le cas le plus courant aujourd'hui est celui de notre routeur NAT : avec une seule adresse IP publique permettre à une multitude d'hôtes (LAN) avec des adresses privées de communiquer avec Internet. C'est le type de NAT utilisé sur pratiquement tous les routeurs<sup>3</sup> DSL de type SOHO/PME, tels que les \*Box.

❗ Si plusieurs PC de votre LAN (société ou domicile) doivent accéder simultanément à Internet, alors que votre FAI (*Fournisseur d'Accès à Internet*) ne vous fournit qu'une seule adresse IP publique, vous êtes obligés de mettre en place un NAT/PAT.

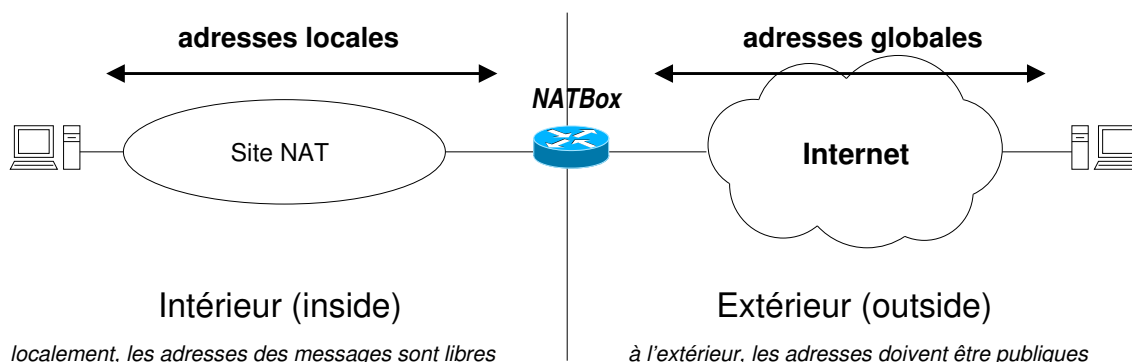
Dans la terminologie du NAT (issue de CISCO mais adoptée par la communauté réseau), on fait la distinction entre :

- **les adresses globales** (ou publiques) sont les adresses routables (sur Internet) car elles ont une signification à portée globale (pour l'ensemble d'Internet). Elles sont attribuées (indirectement) par l'IANA.
- **les adresses locales** qui n'ont un sens que localement, pour les hôtes du LAN

La différence se situe sur l'endroit où ces adresses sont utilisées dans les messages :

- à l'**intérieur** (*inside*), appelé Site NAT, on utilise des adresses locales
- à l'**extérieur** (*outside*), c'est à dire le WAN, on utilise des adresses globales.

La **NATBox** (ou routeur NAT) est la frontière entre ces mondes (et ces adresses), le seul point de passage :



2. Des versions plus actuelles sont les RFC 1663 et RFC 3022.

3. La quasi-totalité des routeurs du marché incluent les fonctionnalités NAT/PAT (et firewall).

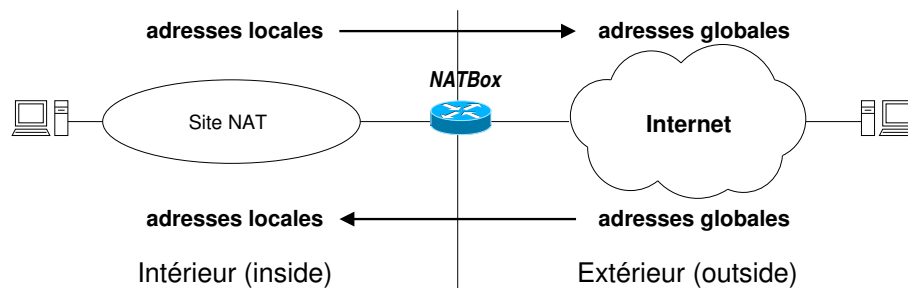
### Exemple 5

Dans l'exemple précédent, 192.168.0.1 est une adresse locale alors que 139.124.187.94 est une adresse globale. En revanche, l'adresse 165.87.29.11 est à la fois locale et globale, car elle apparaît dans les messages à l'intérieur et à l'extérieur du Site NAT. Cela sera clarifié par la suite.

□

Tous les messages franchissant la frontière *inside/outside* passent forcément par la NATBox qui en traduit les adresses :

- pour les **messages sortants** (*inside* → *outside*) :  
les adresses locales sont traduites en adresses globales
- pour les **messages entrants** (*inside* ← *outside*) :  
les adresses globales sont traduites en adresses locales



🔑 Le NAT/PAT n'est concerné que par les messages passant cette frontière. Les messages restant du côté *inside* ne sont pas soumis au NAT. De même que ceux qui restent du côté *outside*.

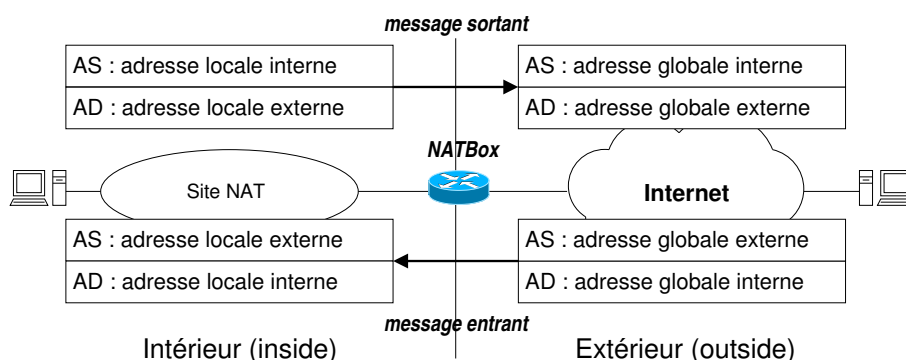
À cela s'ajoutent les qualificatifs d'**interne** et d'**externe** :

- les adresses internes (*inside*) sont celles maîtrisées par l'administrateur du site NAT ;
- les adresses externes (*outside*) font référence à des hôtes situés sur le WAN et qui possèdent (en principe) des adresses publiques.

On distingue donc en réalité les 4 types d'adresses suivantes :

- **adresses locales internes ou ALI** (*inside local address*) : les adresses (en principe privées) des hôtes du Site NAT ;
- **adresses globales internes ou AGI** (*inside global address*) : la (ou les) adresse(s) publique(s) de la NATBox et qui sont utilisées à la place des adresses locales internes quand un message sort du LAN vers Internet ;
- **adresses locales externes ou ALE** (*outside local address*) : les adresses des hôtes du WAN vues par les hôtes du LAN ;
- **adresses globales externes ou AGE** (*outside global address*) : les adresses des hôtes du WAN.

La NATBox traduit les adresses source (AS) et destination (AD) des messages qui franchissent la frontière *in-sideloutside*. Le schéma complet des traductions NAT opérables est :



✍ Dans le cadre du NAT, les AS et les AD sont des adresses IP.  
Dans sa variante PAT, il s'agit d'adresses d'applications.

✍ Dans le cas normal (hors *overlapping*), les adresses externes ne sont pas traduites (*adresse locale externe*  $\equiv$  *adresse globale externe*).

## Exemple 6

Reprenons encore l'exemple du début de cette section :

- 192.168.0.1 est une adresse locale interne ;
- 139.124.187.94 est une adresse globale interne ;
- 165.87.29.11 est à la fois locale externe et globale externe.

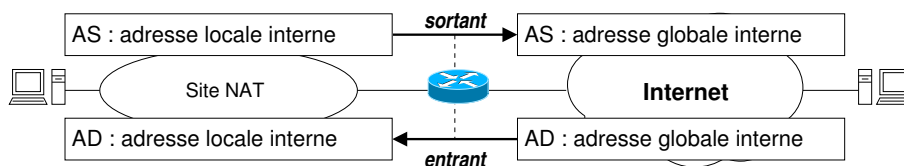
Mais puisqu'il met en œuvre le PAT (dynamique), il traduit des adresses d'application qui incluent aussi le protocole concerné (TCP, UDP ou ICMP), ainsi que les ports utilisés. Ce sera détaillé en section VI.4.

□

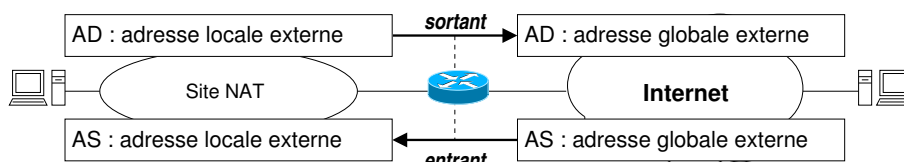
## VI.2.A Traductions inside et outside

Les traductions à opérer dépendent des situations, et les routeurs NAT professionnels peuvent être configurés pour opérer des traductions précises :

- **traduction inside** : traduire les adresses internes (*inside*)



- **traduction outside** : traduire les adresses externes (*outside*)



En temps normal, cette traduction n'est pas opérée. Et si elle l'est, c'est qu'on doit aussi opérer une traduction *inside* pour traiter l'*overlapping*.

- les deux traductions à la fois afin de traiter l'*overlapping* (voir plus loin).

 Les \*Box des FAI ne pratiquent que la traduction *inside*.

## L'overlapping

L'*overlapping* (ou chevauchement d'adresses) se caractérise par une intersection non vide des adresses locales internes et des adresses globales externes. En clair, des stations du Site NAT ont des adresses qui appartiennent aussi à des stations du WAN.

### Exemple 7

Si au lieu de l'adresse 192.168.0.0/16 en interne, on avait utilisé 165.87.0.0/16 et attribué l'adresse 165.87.29.11 à une station du LAN, alors on ne saurait plus à l'intérieur du Site NAT ce que représente cette adresse. La NATBox devrait alors pratiquer les traductions *inside* et *outside*, pour notamment modifier les adresses globales externes (légitimes) qui sont déjà utilisées (sans légitimité) en interne. Par exemple, la station externe 165.87.29.11 serait "vue" dans le Site NAT comme ayant l'adresse 10.0.0.1. C'est tout le sens des adresses locales externes.




Cette situation est plutôt exceptionnelle (voir des exemples dans le cours), et pose de nombreux problèmes. Elle ne s'applique pas à ce TP. Vous n'aurez besoin que de la traduction *inside*.

## VI.2.B Variantes du NAT

Avec un *pool* de  $n$  adresses publiques (AGI), plusieurs variantes sont possibles/combinables :

- **NAT statique** : on choisit par avance  $n$  stations et on associe leur adresse locale interne à une adresse globale interne. La traduction est un à un. Seules ces  $n$  stations pourront accéder à Internet. L'avantage est que ces  $n$  stations peuvent être contactées par des hôtes externes, et peuvent donc être des serveurs ;
- **NAT dynamique** : on choisit  $m$  stations autorisées (en général  $m$  est bien supérieur à  $n$ ) à accéder à internet. Les adresses globales internes leur sont associées dynamiquement et temporairement, lorsqu'une station entreprend un dialogue avec une station externe.
- **PAT dynamique** : une même adresse globale interne est associée dynamiquement à plusieurs adresses locales internes. La NATBox utilise aussi les informations des protocoles TCP, UDP ou ICMP et traduit les ports. La table d'association comprend aussi les ports, ce qui permet de distinguer le trafic. **Avec le PAT, on n'a besoin en général que d'une seule adresse globale interne qui peut être partagée par des milliers de stations !** C'est la traduction opérée par notre routeur PAT.
- **PAT statique** : utilisée pour permettre à des serveurs internes d'être joints depuis l'extérieur, alors qu'on n'a pas assez d'AGI pour du NAT statique. À nouveau, les ports TCP et UDP sont utilisés pour distinguer les ALI.

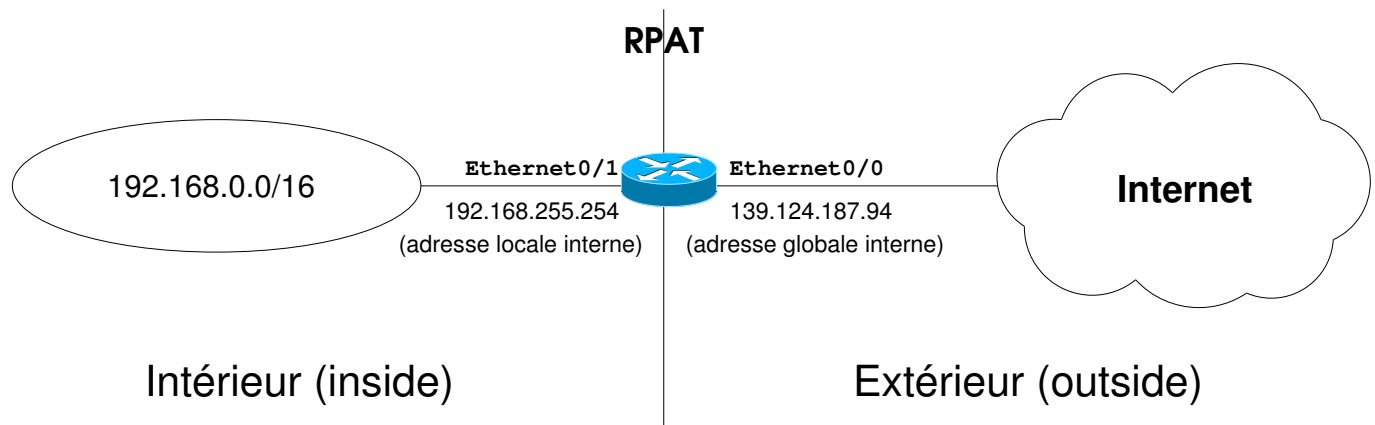
 Les \*Box des FAI réalisent des traduction PAT dynamiques si plusieurs ordinateurs du foyer doivent avoir accès à Internet. Elles permettent aussi le PAT statique.

✍ Nous allons nous concentrer sur le PAT (appelé *overloading* par CISCO), d'abord dynamique puis statique.

## VI.3 Configuration du PAT dynamique

Le routeur RPAT d'accès à Internet **doit opérer une traduction *inside*** : quand un message le traverse dans le sens *inside* → *outside*, il doit traduire (remplacer) les adresses<sup>4</sup> locales internes en adresses globales internes. Il doit faire la traduction inverse quand un message le traverse dans le sens *outside* → *inside*.

Il ne dispose que d'une seule adresse globale interne, 139.124.187.94. C'est l'adresse de son interface Ethernet0/0, côté externe (WAN). Son interface interne est Ethernet0/1 d'adresse 192.168.255.254. Il doit traduire les adresses du réseau 192.168.0.0/16 :



La configuration du PAT dynamique se fait dans les quelques lignes extraites de sa running-config, figurant ci-dessous :

```
interface Ethernet0/1
  ip address 192.168.255.254 ...
  ip nat inside
  ...

interface Ethernet0/0
  ip address 139.124.187.94 ...
  ip nat outside
  ...

access-list 1 permit 192.168.0.0 0.0.255.255

ip nat inside source list 1 interface Ethernet0/0 overload
```

Les différentes étapes qu'on suivra **dans le prochain exercice** pour la configuration PAT dynamique sont les suivantes :

1. Définition des interfaces **inside** et **outside** en mode de configuration d'interface :

4. On verra par la suite que « *adresse* » est à prendre dans un sens plus large car cela comprend le port.



(a) pour l'interface *inside* :

```
Router(config)#interface nom-interface-inside  
Router(config-if)#ip nat inside
```

(b) pour l'interface *outside* :


```
Router(config)#interface nom-interface-outside  
Router(config-if)#ip nat outside
```

2. En mode de configuration globale, définition d'un filtre d'adresses IP —par une **access-list** (ACL)— qui caractérise les adresses locales internes soumises au NAT/PAT :

```
access-list numéro-ACL permit IP-source wildcard-mask
```

où :

- *numéro-ACL* est le numéro d'une ACL, compris entre 1 et 99

 Une ACL est un filtre. Quand une commande précise une ACL, elle ne sera appliquée que pour les datagrammes passant ce filtre. Les ACL comprises entre 1 et 99 sont les **IP standard access-list** (les plus basiques) : elles n'examinent que les adresses IP sources des datagrammes. Par défaut, les ACL sont vierges (vides), et aucun datagramme ne peut passer le filtre correspondant. La commande ci-dessus permet (**permit**) aux datagrammes, dont l'adresse source correspond à ce qui suit, de passer le filtre de l'ACL *numéro-ACL*.


- *IP-source* et *wildcard-mask*, conjointement, représentent les adresses sources des datagrammes à retenir. Mais attention ! *wildcard-mask* **n'est pas un masque de sous-réseau, c'est même son inverse** : les bits à 0 indiquent la partie de l'adresse IP source du datagramme à comparer avec la valeur *IP-source*, alors que ceux à 1 indiquent les bits à ignorer


3. En mode de configuration globale, activation de la traduction **PAT inside**.

```
ip nat inside source list ACL-number interface nom-interface-outside overload
```

qui se traduit par : faire du PAT *inside* sur les messages entrant par une interface déclarée comme *inside* et sortant par une interface déclarée comme *outside*, et dont l'adresse source concorde avec le filtre de l'ACL *ACL-number*. Traduire (*to translate*) le message en utilisant l'adresse globale interne de l'interface *nom-interface-outside* (WAN). Plus précisément :









- **ip nat inside** active la traduction NAT *inside*, et, **overload**, sa variante PAT
- **source list** *ACL-number* filtre les messages à traduire par l'ACL *ACL-number*
- **interface** *nom-interface-outside* indique l'interface *outside* dont il faut utiliser l'adresse globale interne pour la traduction

 Si l'on dispose d'un ensemble d'adresses globales internes, on peut remplacer cette partie de la commande par **pool** *nom-pool*, où *nom-pool* est le nom du *pool* d'adresses, défini avec **ip nat pool**.

 En dépit des apparences, les messages seront traduits dans les deux sens. Les adresses internes sont traduites de *local* en *global* pour les messages sortants (*inside* → *outside*). Elles sont traduites de *global* en *local* pour les messages entrants (*outside* → *inside*)


## Exercice 14 (activation du PAT dynamique sur le routeur du binôme)

Il vous faut maintenant activer le PAT sur votre routeur en vous inspirant de la configuration du routeur d'accès vers Internet. Pour cela :

1.  Identifier les interfaces interne et externe de votre routeur, ainsi que les adresses IP associées
2.  Préciser, dans la configuration des interfaces, laquelle est *inside* et laquelle est *outside*
3.  Définir l'ACL caractérisant les adresses locales internes à traduire (celles de votre LAN)
4.  Activer la traduction **inside** de type PAT des messages correspondant à ce filtre
5.  Sur VMDEB, faire un ping de RPAT et de 10.203.9.1. Cela doit fonctionner.
6.  Sur VMDEB, faire un ping de [www.wireshark.org](http://www.wireshark.org). Ce doit aussi fonctionner !
7.  Sur VMDEB, ouvrir un navigateur et afficher la page <http://www.wireshark.org/>. Faire une capture d'écran nommée 14-pat.png.
8.  Sur VMDEB, utiliser **traceroute** pour tenter de voir quels sont les routeurs traversés pour arriver jusqu'à [www.wireshark.org](http://www.wireshark.org).
9. Sur VMXP, ouvrir un navigateur et afficher la page <http://www.wireshark.org/>. Cela doit fonctionner aussi.
10. Sauver la configuration du routeur.

## VI.4 Fonctionnement de la traduction dynamique PAT

Nous prendrons le cas de notre routeur RPAT simplifié (qu'on appellera aussi NATBox) : une seule adresse globale interne doit être partagée par un ensemble de stations du site NAT. Pour cela, la NATBox doit réaliser une traduction interne dynamique PAT. Avec le PAT, la NATBox ne traduit pas seulement les adresses IP mais doit traduire des adresses d'application.

 Le PAT traduit des adresses d'application locales en adresses d'application globales (internes et externes), et inversement.

La NATBox tient compte et traduit les informations des protocoles utilisant IP : TCP, UDP et ICMP. Pour TCP et UDP, elle doit traduire les ports utilisés. Pour ICMP, cela dépend du message.

En étendant ainsi les informations utilisées, elle ne garde pas seulement trace de la station interne qui dialogue avec Internet mais plutôt du dialogue lui-même, à travers les adresses des applications impliquées dans ce dialogue.

### VI.4.A Initiation d'une traduction dynamique PAT

**Pour une traduction interne dynamique PAT, la création d'une traduction dynamique n'a lieu qu'à l'initiative d'une station interne, lorsqu'elle entame un dialogue avec une station externe.** Quand une application (interne) initie un dialogue avec une application (station) externe, le message parvient à la NATBox qui identifie l'application (interne) par son adresse locale interne, le protocole (TCP, UDP, ICMP) et le port local<sup>5</sup> interne source du message. La NATBox traduit l'adresse locale interne en adresse globale interne. Le port local interne est aussi traduit en port global interne. La traduction modifie sa valeur si une autre application interne utilisant le même protocole et le même port source est déjà en train de dialoguer. Dans ce cas, le port global

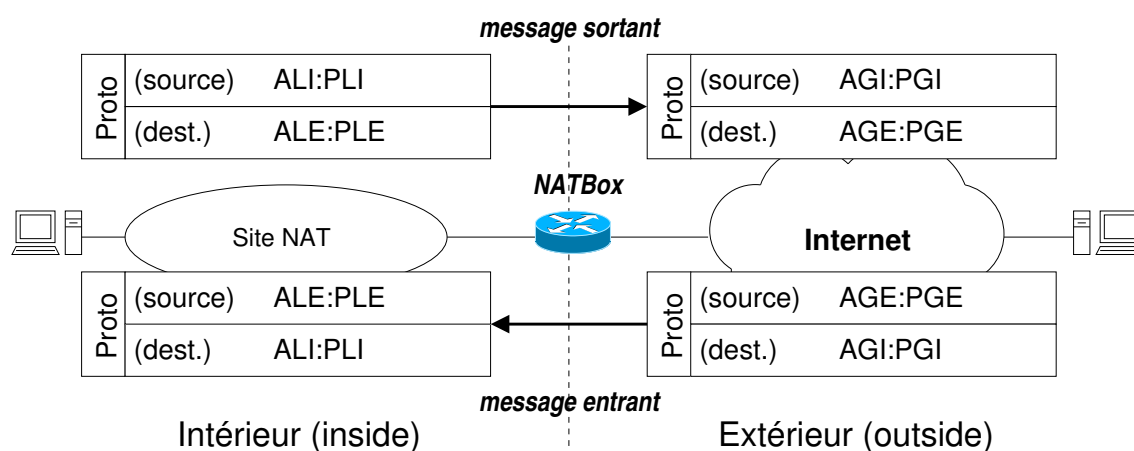
5. Par abus de langage, nous utiliserons « port » même pour un message ICMP. On verra le traitement particulier de ICMP plus loin.

interne est choisi parmi les ports du protocole considéré qui sont libres sur la NATBox.

La NATBox doit alors gérer une **table de traduction dynamique PAT** dans laquelle figurent les protocoles (TCP, UDP, ICMP) et les ports. Sur un routeur CISCO, cette table possède 5 colonnes : *Protocol*, *Inside global*, *Inside local*, *Outside global* et *Outside local*, où :

- *Protocol* est l'un des protocoles TCP, UDP ou ICMP
- *Inside global* a la forme *adresse-globale-interne:port-global-interne*
- *Inside local* a la forme *adresse-locale-interne:port-local-interne*
- *Outside global* a la forme *adresse-globale-externe:port-global-externe*
- *Outside local* a la forme *adresse-locale-externe:port-local-externe*

Le schéma complet des traductions PAT opérables est :



Notre routeur PAT est configuré pour opérer une traduction **inside** : les adresses internes (*Inside*) sont remplacées de *local* en *global* quand le message le traverse pour aller vers l'extérieur, et inversement pour un message entrant. Parce que c'est inutile dans notre cas (pas d'*overlapping*), il n'est pas configuré pour opérer une traduction **outside**, où les adresses externes (*Outside*) sont (aussi) traduites.

La table de traduction d'un routeur CISCO est visible en mode privilégié avec la commande :

```
Router#show ip nat translations
```

### Exemple 8

En reprenant l'exemple du routeur PAT (cf. section VI.1), la traduction opérée apparaîtrait ainsi :

```
Router#show ip nat translations
Pro    Inside global    Inside local    Outside local    Outside global
tcp    139.124.187.94:15000  192.168.0.1:10000  165.87.29.11:25  165.87.29.11:25
...    ...                ...                ...                ...
```

Nous voyons les traductions effectuées (seulement) sur les adresses internes. On remarque que le port 10000 a été traduit en port 15000, probablement parce qu'une station interne utilise déjà le port TCP 10000 dans un dialogue en cours avec une station externe. Si cette station est 192.168.0.21 et qu'elle dialogue avec le serveur POP3 (port 110) de la machine 124.2.96.28, alors la ligne suivante apparaît aussi dans cette table :

```
tcp    139.124.187.94:10000  192.168.0.21:10000  124.2.96.28:110  124.2.96.28:110
```



## VI.4.B Traduction dynamique PAT des messages sortants

On vient de le voir, pour une traduction interne, ce sont les messages sortants (*inside*  $\rightarrow$  *outside*) qui sont à l'origine de la création d'une traduction dynamique. Mais pour un dialogue donné entre une application interne et une application externe, seul le premier message sortant crée une traduction dynamique, et donc une entrée dans la table des traductions. Les autres messages sortants de ce dialogue sont traduits conformément à cette entrée.

Plus précisément, lorsqu'un message sortant se présente à la NATBox, celle-ci cherche dans sa table de traductions le dialogue correspondant, c'est à dire une entrée où *Protocole* correspond à celui du message, où *Inside local* correspond à sa source (adresse et port) et où *Outside local* correspond à sa destination (adresse et port).

S'il en existe une, le message est traduit en remplaçant les champs correspondant à *Inside local* par ceux figurant en *Inside global*. Les informations *Outside* seraient traduites aussi de local en global si la NATBox opérait aussi un NAT outside.

Sinon, il s'agit d'un nouveau dialogue et une nouvelle traduction (nouvelle entrée) est créée.

### Exemple 9

On continue l'exemple précédent, où le dialogue a été initié par l'application interne utilisant le port TCP 10000 de la station 192.168.0.1, et où l'application externe utilise le port 25 de la station 165.87.29.11. Quand l'application externe envoie d'autres messages de ce dialogue, ceux-ci ont 192.168.0.1 comme adresse locale interne, TCP comme protocole et 10000 comme port source. Quand ces messages passent par la NATBox pour sortir, elle se rend compte que la table contient une entrée (TCP) avec pour *Inside local* 192.168.0.1:10000, et traduit ces messages avec l'*Inside global* correspondant (139.124.187.94:15000).



D'autre part, si une application interne (identifiée par une adresse locale interne, un protocole, et un port) a initié des dialogues simultanément avec plusieurs applications externes, alors la table de traduction contient autant d'entrées qu'il y a de dialogues en cours. Chez CISCO, si le protocole utilisé est UDP ou ICMP, le routeur garde le même *Inside global* pour chacune de ces entrées. Mais si le protocole est TCP, le routeur crée une nouvelle traduction dynamique pour chacune de ces entrées en associant, à chaque *Inside local*, un nouvel *Inside global* (la même adresse globale interne mais un port global différent).

**i** Ce comportement des routeurs CISCO est un peu surprenant. En théorie, la NATBox pourrait utiliser le même *Inside global* pour les mêmes *Inside local*. S'ils ne le font pas, ce doit être par ce que cela leur facilite la tâche...

### Exemple 10

Si l'application interne précédente initie, à partir du même port, un nouveau dialogue avec l'application externe (serveur FTP) utilisant le port 21 de la station 85.110.28.91, alors que le dialogue précédent est toujours en cours, alors on aura une table qui ressemble à (si le port global 15001 était libre) :

```
Router#show ip nat translations
Pro    Inside global    Inside local    Outside local    Outside global
tcp    139.124.187.94:15000  192.168.0.1:10000  165.87.29.11:25  165.87.29.11:25
tcp    139.124.187.94:15001  192.168.0.1:10000  85.110.28.91:21  85.110.28.91:21
```

où l'on voit qu'une nouvelle entrée a bien été créée, avec un *Inside global* qui diffère du précédent par le port global utilisé. Mais si le protocole est UDP, on peut très bien avoir plusieurs entrées ayant le même couple *Inside global* et *Inside local* :

```
Router#show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
udp	139.124.187.94:22000	192.168.0.1:22000	138.142.18.5:13	138.142.18.5:13
udp	139.124.187.94:22000	192.168.0.1:22000	76.34.151.39:7	76.34.151.39:7



### VI.4.C Traduction dynamique PAT des messages entrants

Dans le cadre d'une traduction interne, les messages entrants (*outside* → *inside*) ne peuvent pas créer de nouvelle traduction dynamique. Lorsqu'ils arrivent à la NATBox, celle-ci recherche dans sa table le dialogue correspondant, c'est à dire une entrée où *Protocole* correspond à celui du message, où *Outside global* correspond à sa source (adresse et port) et où *Inside global* correspond à sa destination (adresse et port).

S'il elle en trouve une, le message est traduit en remplaçant les informations *Inside* de global en local (les adresses *Outside* seraient traduites aussi si la NATBox opérait aussi un NAT outside).

Si elle n'en trouve pas, le message est purement et simplement **rejeté** (un message d'erreur ICMP est éventuellement renvoyé). De cette façon, le NAT introduit un certain niveau de sécurité : les stations du LAN ne sont pas directement accessibles de l'extérieur sauf pour les dialogues en cours, qui —rappelons-le— sont établis à l'initiative des stations internes<sup>6</sup>. Ainsi, une NATBox est un peu un pare-feu. En revanche, en matière de sécurité, il ne s'agit toutefois que d'une option qui ne peut remplacer un véritable pare-feu avec un filtrage pertinent des communications TCP/IP (par exemple pour fournir une protection contre les communications abusives d'un *Cheval de Troie*).

#### Exemple 11





En tenant compte de la table de l'exemple précédent, un message entrant ne sera accepté que s'il correspond à l'une des quatre entrées (en comptant UDP). Le triplet *Protocole*, *Inside global* et *Outside global* doit coïncider avec les champs du message. Seuls seront donc acceptés :

- les messages TCP d'adresse source 165.87.29.11 et port source 25, et d'adresse destination 139.124.187.94 et port destination 15000
- les messages TCP d'adresse source 85.110.28.91 et port source 21, et d'adresse destination 139.124.187.94 et port destination 15001
- les messages UDP d'adresse source 138.142.18.5 et port source 13, et d'adresse destination 139.124.187.94 et port destination 22000
- les messages UDP d'adresse source 76.34.151.39 et port source 7, et d'adresse destination 139.124.187.94 et port destination 22000



6. Nous verrons plus loin qu'on peut établir des correspondances de ports TCP/UDP pour réaliser ce qu'on appelle communément la redirection de ports (*port redirection* ou *port forwarding*) pour les connexions entrantes (traduction PAT statique).

## Exercice 15 (gestion des traductions)

1. Sur VMDEB, lancer une capture de toutes les trames avec **Wireshark**
2. À partir d'un terminal de VMDEB, faire **ping** de TPSEUR et de `iut.univ-amu.fr`. Avec un navigateur, afficher dans deux onglets les URL <http://www.wireshark.org/> et <http://ent.univ-amu.fr>.
3. À partir d'un terminal de VMDEB, faire un **traceroute** de `10.203.9.1`.
4.  Sur VMDEB, dans un navigateur l'URL <http://TPSEUR/index.php>, où TPSEUR est à remplacer par son adresse. Observer les informations indiquées sur la page affichée par le serveur.
5.  Arrêter la capture de **Wireshark** et l'enregistrer sous le nom `15-debug-pat.pcap`
6.  Sur le routeur, afficher la table des traductions.
7.  Déterminer quelle est la traduction créée par votre routeur pour contacter ce serveur. Argumenter.

## VI.5 PAT statique pour la redirection de port des connexions entrantes

Nous avons vu précédemment que les connexions et sessions TCP/IP entrantes sont rejetées par la NATBox. Alors, que faire si une société souhaite mettre en place un serveur de messagerie (SMTP) ou un serveur Web (HTTP) derrière le NAT ? *A priori*, en utilisant le NAT/PAT dynamique sur votre routeur Internet, cette station ne sera jamais accessible à partir de l'extérieur.

La solution pour permettre une connexion entrante au travers d'un NAT est la mise en place d'une redirection de port (*port redirection*, ou *port forwarding*). Il s'agit d'une traduction PAT statique basée sur l'adresse d'un port TCP ou UDP. Souvent, la redirection de port est aussi appelé *virtual serveur* ou *virtual application*.

### Exemple 12

Dans l'exemple suivant (Live Box d'Orange), une redirection de port est définie pour rendre un serveur Web (derrière le NAT) accessible à partir de l'extérieur :

port externe	protocole	adresse locale
80	tcp	192.168.11.1

Certains routeurs PAT plus sophistiqués —dont le nôtre—permettent une redirection à la fois plus détaillée et plus restrictive, comme le montre l'exemple suivant :

adresse IP source externe	port externe (ou plage de ports)	protocole(s)	adresse IP interne	port interne (ou plage de ports)
80.139.53.71	8631–8632	tcp,udp	192.168.11.1	5631–5632

Dans cet exemple, uniquement les datagrammes provenant de l'adresse IP `80.139.53.71` véhiculant des paquets TCP ou UDP, dont le port de destination est 8631 ou 8632, sont traduits vers l'adresse `192.168.11.1`. Le port de destination 8631 est traduit vers 5631 et le port de destination 8632 est traduit vers 5632. La traduction inverse est opérée pour les datagrammes à destination de `80.139.53.71`, provenant de `192.168.11.1` et dont le port source est 5631 ou 5632.

□

Sur un routeur CISCO, sur lequel le PAT est activé en utilisant la seule adresse publique de l'interface Ethernet0, la redirection de port pour un serveur HTTP, FTP et un serveur SMTP hébergés par l'hôte `192.168.11.5` du LAN, peut être configurée comme suit :







```
ip nat inside source static tcp 192.168.11.5 21 interface Ethernet0 21
ip nat inside source static tcp 192.168.11.5 25 interface Ethernet0 25
ip nat inside source static tcp 192.168.11.5 80 interface Ethernet0 80
```



Pour un serveur FTP interne, il est parfois nécessaire d'informer la NATBox qu'elle doit suivre la communication TCP au niveau de la couche application (couches 5-7 du modèle TCP/IP simplifié) en ajoutant le paramètre **extendable** à la fin de la commande (ceci concerne en vérité que quelques anciens modèles des routeurs CISCO). La NAT box des CISCO 1720/1721 (IOS version 12.3) suit la couche application du protocole FTP par défaut et le paramètre **extendable** n'est pas nécessaire.

## Exercice 16 (redirection de ports)

Dans vos paramètres sont indiquées les redirections vous concernant configurées sur le routeur d'accès vers Internet. Ainsi, les connexions TCP entrantes (à destination de l'adresse publique de RPAT) sur les ports mentionnés en colonne *Port WAN* et vous concernant sont traduites et redirigées vers les ports mentionnés en colonne *Port LAN* vers l'adresse WAN de votre routeur :

-  Les paramètres qui vous ont été communiqués indiquent les redirections qui ont été préalablement configurées sur RPAT pour votre binôme, de manière à pouvoir contacter votre routeur depuis l'extérieur. Depuis le PC-IUT, se connecter par TELNET sur votre routeur en exploitant ces informations.
-  Configurer votre routeur pour qu'il opère une redirection de port pour les connexions entrantes (donc à destination de l'adresse WAN de votre routeur) sur ces ports (redirigés par RPAT) vers les ports TCP 22, 23 et 80 de VMDEB. Fournir les commandes correspondantes.
-  Depuis un navigateur sur le PC-IUT, afficher la page d'accueil du serveur Web qui est déjà actif sur VMDEB. Faire une capture d'écran et la nommer **16-staticpat-http.png**
-  Depuis un terminal sur le PC-IUT, se connecter au serveur SSH de VMDEB (se connecter en tant que root). Faire une capture d'écran et la nommer **16-staticpat-ssh.png**
- Depuis un terminal de VMDEB, installer un serveur TELNET en tapant (simplement) les commandes suivantes :

```
# sudo apt-get update
# sudo apt-get install telnetd
```

-  Depuis un terminal de VMDEB, taper la commande adéquate montrant que le service TELNET est bien actif et en écoute sur le port 23 de TCP
-  Depuis un terminal sur le PC-IUT, se connecter en tant que totoadm (mot de passe <re>zo++) au serveur TELNET de VMDEB. Faire une capture d'écran et la nommer **16-staticpat-telnet.png**
- Sauver la configuration du routeur


## VI.6 ACL étendues et sécurisation des accès réseau

Nous souhaitons maintenant sécuriser un peu les VM de la manière suivante :

- VMXP ne doit accéder qu'aux serveurs Web d'internet mais il doit pouvoir effectuer un ping quelconque et utiliser le DNS ;
- tout Internet doit pouvoir accéder au serveur Web de VMDEB ;
- seules les stations des réseaux 10.203.9.0/24 et des réseaux du TP doivent pouvoir accéder aux serveur SSH de VMDEB ;
- seul PC-IUT doit avoir accès au serveur TELNET de VMDEB
- aucun (autre) serveur de VMXP ni de VMDEB n'est autorisé à dialoguer. On supposera que les serveurs utilisent des ports inférieurs (ou égaux) à 1023 ;

- les clients de VMDEB sont libres d'utiliser des serveurs extérieurs. On supposera que les clients de VM-DEB utilisent des ports supérieurs à 1023 ;
- VMXP et VMDEB doivent pouvoir continuer à se configurer par DHCP auprès du routeur.

Pour cela, votre routeur doit faire office de **pare-feu** (*firewall*). Il dispose plutôt des fonctionnalités d'un pare-feu sans état (*stateless firewall*) mais cela sera suffisant. Il doit filtrer les datagrammes qui proviennent d'Internet et à destination des ports des serveurs de PC-LAN. Pour cela, il faut établir une ou plusieurs **ACL étendues**, puis configurer le routeur pour **filtrer en entrée** ou **en sortie** de ses interfaces afin de n'autoriser que les dialogues attendus.

 Les ACL que nous avons utilisées précédemment pour configurer le PAT sont les plus basiques : les **IP standard access-list**. Leur numéro est compris entre 1 et 99. Ces ACL n'examinent que les adresses IP sources des datagrammes et ne permettent pas d'opérer le filtrage demandé.

## Syntaxe des ACL étendues

La syntaxe que nous retiendrons pour les ACL étendues est la suivante :

```
Router(config)#access-list numéro action protocole source destination [qualificatif]
```

où :

- *numéro* est le numéro d'une ACL étendue, qui doit être compris entre 100 et 199
- *action* est soit **permit**, soit **deny**
- *protocole* peut être **ip**, **tcp**, **udp** ou **icmp** (d'autres sont possibles), ou le numéro du protocole (du champ *Protocole* du datagramme IP)
- *source* et *destination* identifient la source et la destination. Leur forme générale peut être :
  - ◇ *adresse wildcard-mask* : même signification pour les ACL basiques (voir section VI.3, page 32)
  - ◇ **host** *adresse* : qui est un raccourci pour *adresse 0.0.0.0*
  - ◇ **any** : qui est un raccourci pour *0.0.0.0 255.255.255.255*

Aussi, si *protocole* est **tcp** ou **udp**, alors on peut compléter la description de *source* et de *destination* avec des ports ou des intervalles de port en utilisant :


- ◇ **eq** *port* : uniquement le port *port*
- ◇ **gt** *port* : port supérieur strictement à *port*
- ◇ **le** *port* : port inférieur strictement à *port*
- ◇ **range** *port<sub>1</sub> port<sub>2</sub>* : port dans l'intervalle *port<sub>1</sub>* à *port<sub>2</sub>* inclus
- le *qualificatif*, optionnel, dépend du protocole :
  - ◇ pour **tcp**, on peut utiliser **established** pour faire référence à une connexion établie
  - ◇ pour **icmp**, on peut préciser le type de paquet : **echo**, **echo-reply**, **ttl-exceeded**...

Une ACL peut alors être exploitée pour filtrer les datagrammes en entrée et/ou en sortie du routeur. Pour cela, dans le mode configuration d'une interface donnée, on utilise l'expression :

```
Router(config-if)#access-group numéro-acl in|out
```

indiquant que l'ACL doit être appliquée en entrée (**in**) ou en sortie (**out**).

## Exercice 17 (sécurisation des accès aux serveurs)

 Effectuer les configurations nécessaires pour assurer le niveau de protection demandé. Demander à l'enseignant de valider l'exercice.



## VI.7 Interactions entre le NAT et les autres protocoles

La traduction opérée par le NAT/PAT doit être transparente, autant pour les ordinateurs que les protocoles de TCP/IP. Or, la modification des adresses/ports source et destination n'est pas anodine pour de nombreux protocoles comme IP, ICMP, TCP, UDP, FTP, etc. :

- IP inclut les adresses IP dans le calcul du *checksum*
- TCP et UDP les incluent aussi dans le calcul de leur *checksum* (pseudo en-tête)
- TCP et UDP y incluent aussi les ports et les données
- ICMP ne fournit pas de ports (problème pour le PAT). Les messages d'erreur ICMP (types 3 à 5 et 11) contiennent toutefois les en-têtes IP et TCP/UDP des datagrammes en cause et peuvent donc être traduits.
- Les messages ICMP de demande (ECHO<sup>7</sup>, Horodatage, etc.) contiennent un identificateur. L'identificateur (ainsi que l'adresse locale interne) est traduit par un identificateur global comme s'il s'agissait d'un port.
- FTP envoie, dans la commande PORT et en réponse de la commande PASV, une adresse IP et un port TCP à utiliser pour établir une connexion de données. Ils doivent être traduits, ce qui modifie le segment TCP qui transporte ce message.



**La NAT box doit en tenir compte et modifier tous les messages des protocoles qui utilisent les adresses qu'elle traduit !**

Il en découle que le NAT/PAT complique l'utilisation des protocoles utilisant les adresses et les ports dans leurs messages. Les NATBox savent en général traduire les messages des protocoles classiques. Mais elles peuvent être incompatibles avec des protocoles moins "standard", comme le protocole GRE (couche 4), utilisé par le protocole PTPP (*Point To Point Protocol*) qui permet de créer des tunnels VPN (accès à distance sécurisé).

### Exercice 18 (Dialogue ICMP au travers d'un routeur NAT/PAT)

1. Vider la table de traduction de votre routeur NAT avec :

```
Router#clear ip nat translation *
```

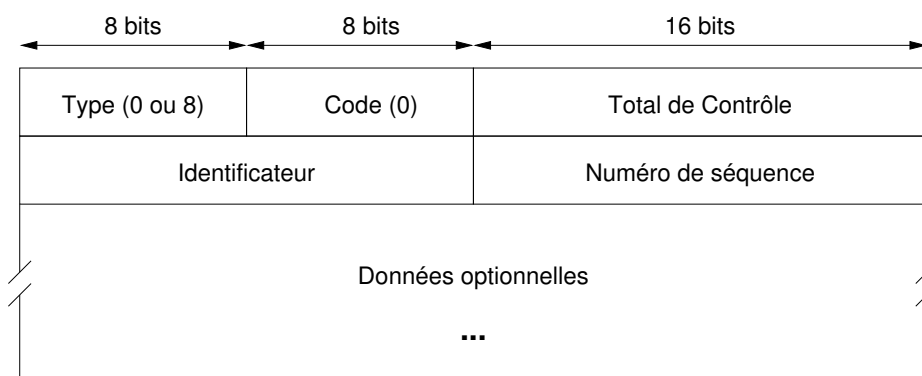
2. Lancer une capture par **Wireshark** sur VMDEB
3. À partir de VMXP, envoyer des pings (message ICMP de type ECHO) en continu (avec l'option adéquate) vers 10.203.9.1
4. À partir de VMDEB, envoyer un ping (message ICMP de type ECHO) vers 10.203.9.1 en utilisant deux paquets ICMP (**ping -c 2 ...**)
5. Arrêter la capture. Sauver les 4 trames (2 fois un message écho et la réponse à écho) concernant les messages ICMP dans le fichier 18-pat-icmp.pcap
6. Fournir la valeur du champ *Identificateur* de chaque message ICMP (voir annexe).
7. Afficher la table de traduction
8. En déduire si le routeur a dû ou pas modifier ce champ.

7. Voir aussi <http://www.reseaucerta.org/exonets/exonet83.htm>

## VII Annexe

### VII.1 Message ICMP de test d'accessibilité et d'état (PING)

Ces messages ICMP, utilisés notamment par la commande **ping**, ont le format suivant :



**Format du message ICMP d'ECHO**


où les champs ont la signification suivante :

**Type** : (8 bits) Sa valeur indique s'il s'agit d'une demande ou d'une réponse d'ECHO :

- 0 : réponse à une demande d'ECHO
- 8 : demande d'ECHO

**Identificateur** : (16 bits)

Permet l'identification (unique) de la demande. Puisque plusieurs demandes d'ECHO peuvent être transmises à un même ordinateur, ce champ permettra de distinguer les réponses. Par exemple, on peut utiliser deux fois **ping** en même temps sur deux terminaux à destination d'un seul ordinateur. Les deux processus **ping** recevront toutes les réponses et utiliseront ce champ pour distinguer les réponses qui les concernent.

 En cas de PAT, ce champ est utilisé et traduit comme un port TCP ou UDP.

**Numéro de séquence** : (16 bits)

Une demande d'ECHO n'est généralement pas unique : certaines versions de **ping** s'arrêtent après un nombre prédéfini de demandes/réponses et, pour d'autres, il faut stopper manuellement le processus. Bien souvent, le nombre de demandes/réponses est paramétrable (option **-c** sur Linux, option **-n** sur Windows). Dans ce cas, toutes les demandes ont le même Identificateur et c'est le Numéro de séquence qui change entre 2 demandes. Celui-ci commence à 1 et est incrémenté de 1 à chaque demande.

**Données** : (taille variable)

Zone optionnelle et ces données ne sont pas utilisées (mais reproduites dans la réponse). **ping** sur Linux place dans cette zone 56 octets, alors qu'il n'y en a que 32 sur Windows. Cette taille est paramétrable (option **-s** sur Linux et **-l** sur Windows). Un intérêt majeur de cette zone est de tester si le datagramme IP généré peut arriver sans fragmentation, quand on met à 1 son bit *Don't Fragment* (par défaut sur Linux, option **-f** sur Windows).