

TP-4 Couche Réseau - Routage et NAT

Objectifs pédagogiques

- (1) Mettre en place un réseau comprenant deux routeurs et des PC reliés aux routeurs sous Cisco Packet Tracer.
- (2) Configurer les interfaces réseau de chaque routeur. Assurer le routage statique puis dynamique selon le protocole RIP des routeurs.
- (3) Mettre en place la fonction NAT (*Network Address Translation*) afin d'émuler le cas de figure d'Internet : des petits réseaux locaux qui utilisent un plan d'adressage IP *privée* et qui se connectent entre eux via des grands réseaux étendus qui utilisent à son tour un plan d'adressage IP *public*.
- (4) Introduire la notion de filtrage de trafic dans les routeurs IP. En effet, les fonctions de routage ne se limitent pas à lire les en-têtes IP et acheminer les paquets et ils peuvent aussi implémenter des politiques réseaux comme le filtrage du trafic.

1 Consignes

Binômes : Vous pouvez travailler en binôme ou seul.

Ressources : Vous pouvez utiliser les matériels du cours (slides de CM, TPs passés, ...) ainsi que toute ressource disponible sur Internet.

2 Démarrer Cisco Packet Tracer

Cisco Packet Tracer est déjà installé sur les machines de la salle. Notez que le chemin par défaut de l'installation est `/opt/pt`, ce qui implique que pour le lancer il faut taper dans la ligne de commande `/opt/pt/packettracer` car on n'a pas fait de liens symboliques dans `/usr/local/bin`. Si vous avez installé Cisco Packet Tracer dans votre ordinateur, taper directement `/packettracer` dans la ligne de commande, cela suffira normalement.

La première fois que vous démarrez le logiciel, il faut se loguer avec l'identifiant (ou adresse email) que vous utilisez pour vous inscrire. Si vous ne sortez pas du *login*, il ne faudra pas le retaper dans les prochaines séances.

En plus du matériel officiel que vous pouvez trouver sur la *Cisco Networking Academy*, un manuel en français très simple de prise en main est disponible sur http://www.siloged.fr/cours/docs/manuels/doc_packettracer.pdf. De toute façon, vous pouvez le trouver aussi dans le site du TP.

3 Réalisation du réseau pour le routage

Réalisez le réseau décrit figure 1 pour mettre en place des fonctionnalités basiques de routage IP. Les routeurs sont des routeurs Cisco 1941. Si vous ne voulez pas perdre du temps à la dessiner, vous pouvez la trouver sur le site du cours dans le fichier `routing.pkt`.

Configurez les cartes réseaux des PC avec les valeurs des adresses IP indiqués dans le dessin comme dans le TP précédent. Mais, maintenant il faut aussi définir la passerelle (*gateway*) par défaut, c.-à.-d., l'adresse IP vers laquelle il faut envoyer par défaut les paquets dont le destinataire n'appartient pas aux sous-réseau IP du PC. Pour faire cela, rendez vous dans `Config` → `Global` → `Settings` → `Gateway/DNS IPv4` et dans la champ `Gateway` saisissez l'adresse IP de la passerelle du PC.

Pensez également à sauver périodiquement votre travail en cas de crash de l'application.

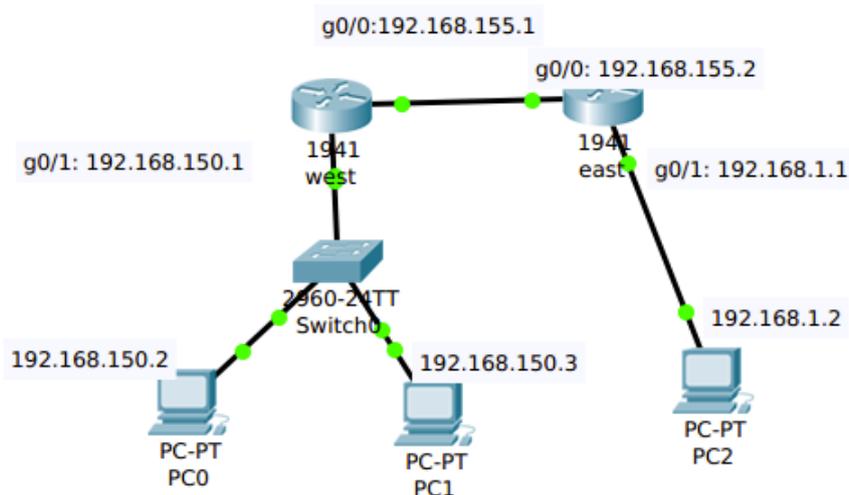


FIGURE 1 – Réseau pour le routage.

3.1 Configuration des routeurs Cisco 1941

Configurez les deux routeurs 1941 comme s'ils étaient des vraies routeurs physiques Cisco avec l'aide des rappels de configuration de routeurs d'IOS dans l'annexe à la fin de l'énoncé du TP.

Allez dans l'onglet *CLI* (c'est simplement la ligne de commandes du router) et à la question *Would you like to enter the initial configuration dialog? [yes/no] :*, tapez *no*. Laissez aux routeurs un temps pour démarrer. Après vous pouvez commencer à saisir des commandes pour configurer les machines.

Question 1 : *Depuis le PC0, essayer de pinger tous les interfaces réseaux des autres PCs et des deux routeurs. Quelles interfaces sont capables de répondre ? Quelles interfaces ne sont pas capables de répondre ? Listez les interfaces qui sont capables de répondre et les interfaces qui ne sont pas capables. Pourquoi il y a des interfaces qui ne peuvent pas répondre ?*

Depuis PC0, on peut obtenir des réponses uniquement de : PC1 (192.168.150.3), l'interface g0/1 du router0 (192.168.150.1) et l'interface g0/0 du router 0 (192.168.155.1). Les autres interfaces ne peuvent pas répondre parce que les tables de routage des routeurs contiennent uniquement les entrées correspondant aux sous-réseaux directement connectés sur eux. Donc, un ping qui doit traverser (dans l'aller et le retour) deux routeurs ne réussira pas.

Maintenant, vous devez configurer le tables de routage des deux routeurs.

D'avant, commencez avec le routeur *west*. Utilisez les commandes pour le routage statique pour configurer le table de routage de ce routeur *west* qui sont dans l'annexe à la fin de l'énoncé du TP.

Question 2 : *Depuis le PC0, essayer encore une fois de pinger tous les interfaces réseaux des autres PCs et des deux routeurs. Quelles interfaces sont capables de répondre ? Quelles interfaces ne sont pas capables de répondre ? Listez maintenant les interfaces qui sont capables de répondre et les interfaces qui ne sont pas capables. Si la table de routage du routeur west est correctement configurée, pourquoi il y a encore des interfaces qui ne peuvent pas répondre ?*

Depuis PC0, on obtiens le meme résultat qu'avant : des réponses uniquement de : PC1 (192.168.150.3),

l'interface g0/1 du router 0 (192.168.150.1) et l'interface g0/0 du router 0 (192.168.155.1). Maintenant, p.ex. un ping depuis PC0 vers l'interface g0/1 du router 1 (192.168.1.1) va réussir à arriver, mais pas à retourner puisque la table de routage de 1 n'est pas configurée. On ne l'a pas fait, mais si on avait essayer de pinger depuis PC2 vers vers l'interface g0/1 du router 0 (192.168.150.1), le ping aurait réussi.

On pourrait faire la même chose dans l'autre routeur *east*, c.-à.-d., mettre la route statique manquante à main. Mais, à la place de cela, vous allez à activer le routage dynamique par protocole RIP, ce qui permettra aux deux routeurs d'apprendre les routes manquantes.

Maintenant, on procède à activer le protocole RIP dans les deux routeurs en signalent les sous-réseaux IP qui participent dans le protocole RIP. Dans notre cas, tous les sous-réseaux IP directement connectés à chaque router. Vous trouverez encore un exemple de cette manipulation dans l'annexe.

Question 3 : *Depuis le PC0, essayer encore une fois de pinger tous les interfaces réseaux des autres PCs et des deux routeurs. Quelles interfaces sont capables de répondre ? Quelles interfaces ne sont pas capables de répondre ? Listez maintenant les interfaces qui sont capables de répondre et les interfaces qui ne sont pas capables. Est-ce que maintenant tous les interfaces peuvent répondre ? Vérifiez la configuration de tables de routage des deux routeurs. Sont-elles bien configurées ? Qu'est ce que ça veut dire les lettres S et R en devant des entrées des tables ?*

Depuis PC0, maintenant, tous les interfaces sont capables de répondre puisque les tables de routage des deux routeurs son bien configurées : dans les deux tables il y a des entrées correspondantes aux trois sous-réseaux IP : 192.168.150.0/24, 192.168.155.0/24 et 192.168.1.0/24. Les lettres S et R veulent dire que les entrées des tables ont été rajoutées statiquement (à la main par un opérateur) et dynamiquement (par le protocole RIP), respectivement.

Finalement, observez le contenu des tables `arp` des tous les dispositifs.

Question 4 : *Est-ce que, dans chaque table `arp`, on peut trouver toutes les correspondances entre les adresses MAC et les adresses IP de tous les interfaces du réseaux ? Pourquoi ? Dans les tables `arp` il y a des valeurs qui indique le temps d'existence de l'entrée. Est-ce que vous pouvez faire la liaison entre les mises à jour des tables et vos manipulations du réseau ?*

Dans les table `arp` on ne trouve que les *resolutions* (traductions adresse MAC - adresse IP) qui correspondent aux interfaces des sous-réseaux directement connectés à nos dispositifs. Les adresse MAC sont utilisées par le protocole Ethernet (couche 2 de liaison) pour délivrer des paquets des données dans l'enceinte d'un sous-réseaux IP. Le passage entre deux sous-réseaux est pris en main par le protocole IP (couche 3 de réseaux). Les entrées dans les tables `arp` avec un tiret comme temps d'existence de l'entrée correspondent aux interfaces locaux des machines. Les entrées dans les tables `arp` avec un certain temps d'existence correspondent aux interfaces des autres machines et le temps d'existence correspondent typiquement soit à la première fois qu'on a réussi a pinger l'interface (première fois qu'on a eu besoin de son adresse MAC) soit à la première fois que la machine a diffusé en broadcast sa traduction adresse MAC - adresse IP sans requête explicite après de se connecter au réseau.

4 Réalisation du réseau pour le NAT

D'abord, il faut réaliser une topologie de réseau similaire à la précédente mais avec un plan d'adressage IP différent qui est décrit dans la figure 2. Encore une fois, si vous ne voulez pas perdre du temps à la dessiner, vous pouvez la trouver sur le site du cours dans le fichier `nat.pkt`.

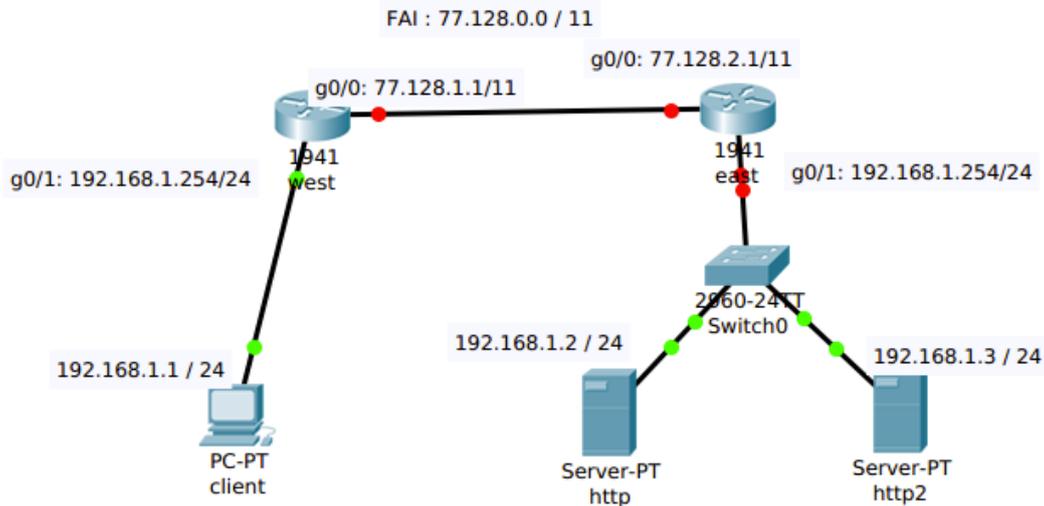


FIGURE 2 – Réseau pour le NAT.

Pensez également à sauvegarder périodiquement votre travail en cas de crash de l'application.

4.1 Configuration des serveurs

Une différence majeure par rapport au réseau précédent est la utilisation de deux serveurs *web* (*http* et *http2*) à la place de PC0 et PC1. (Si vous les dessinez, vous pouvez les trouver dans le panel inférieur en cliquant End Devices → End Devices → Generic-Sever PT)).

Comme dans le cas de PC classiques, il faudra aussi configurer son interface par défaut (FastEthernet0) avec les adresses IPs signalées dans la figure 2. On doit aussi attribuer une passerelle par défaut à chaque hôte (PC client et deux deux serveurs *web*) comme on ferait avec des vraies PCs. Pour ça on utilise l'adresse IP 192.168.1.254.

Finalement, on va rendre les machines *http* et *http2* des serveurs webs. Pour faire cela, on doit aller dans Services → HTTP et vérifier que les deux cases à cocher HTTP et HTTPS sont activées. Si c'est le cas, essayez d'accéder au site web hébergé en ouvrant le navigateur web local (Desktop → Web Browser) et en tapant dans la barre d'adresse `http://127.0.0.1` (l'adresse locale de *loopback*) comme URL. Le fichier `index.html` du site web s'ouvrira.

4.2 Configuration des routeurs Cisco 1941

Configurez les deux routeurs 1941 comme s'ils étaient des vraies routeurs physiques Cisco avec l'aide des rappels de configuration de routeurs d'IOS dans l'annexe à la fin de l'énoncé du TP. D'abord, vous devez reconfigurer tous les interfaces réseaux. Ensuite, vous allez mettre en place la translation d'adresses et de ports.

ATTENTION : La longueur du masque du réseau entre les deux routeurs west et east n'est pas multiple de 8.

Question 5 : Depuis le hôte client, essayez de pinguer l'interface `g0/0` du router west (77.128.1.1). Normalement, il devrait marcher, puisque tout est correctement configuré. Maintenant, ressayer avec l'interface

g0/0 du router east (77.128.2.1). Au router east, exécutez les commandes `debug ip icmp` ou `debug ip packet` pour voir ce qui se passe en détail. Est-il capable de répondre ? Pourquoi ?

No. Même si l'interface `g0/0` du router *east* (77.128.2.1) fait partie aussi du réseau (77.128.0.0/11), le router *east* n'est pas capable de acheminer correctement la réponse au ping car selon sa table local de routage le sous-réseau local du *client* (192.168.1.0/24) est directement connecté à son interface `g0/1` lorsque en réalité la PC *client* est au derrière de router *west*.

Question 6 : *Maintenant, depuis le hôte client, essayez de pinger l'un de deux servers web (http ou http2). Sont-ils capables de répondre ? Pourquoi ?*

No. Les adresses IP des servers web (`http` ou `http2`) font partie de sous-réseau local de *client* (192.168.1.0 / 24). Donc, le paquet est acheminé en local sans traverser le router *west* et comme il n'y pas d'interface réseaux avec l'IP 192.168.1.2 ou 192.168.1.3 directement connectés au réseau de *client*, le ping échoue.

4.3 Translation d'adresse statique

Afin de résoudre le problème relevé dans la question 1, on va mettre en place une translation d'adresse statique dans les deux routeurs. Dans la terminologie Cisco lorsqu'on configure une translation d'adresse, il y a 2 mondes : *inside* représentant l'intérieur, c.-à.-d. le réseau local et *outside* représentant l'extérieur, c.-à.-d. l'Internet au sens large). Il existe aussi une dénomination pour les adresses : *global* pour les adresses publiques et *local* pour les adresses privées.

Les deux réseaux auxquels les PCs sont connectés utilisent le même plage privé d'adresses IP (192.168.1.0 / 24) et représentant l'intérieur. Par contre, le réseau entre les deux routeurs utilise une plage publique d'adresses IP (77.128.0.0 / 11) et représente l'extérieur. Vous allez configurer dans les deux routeurs une translation d'adresse statique permettant aux paquets IP des réseaux intérieurs traverser les routeurs.

Pour indiquer au routeur qu'une interface est à l'intérieur on utilise la commande depuis l'interface :

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

Pour indiquer au routeur qu'une interface est à l'extérieur on utilise la commande depuis l'interface :

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

Pour indiquer au routeur qu'il doit faire une translation d'adresse statique pour une machine particulière, on utilise la commande :

```
Router(config)#ip nat inside source static @IP-privée-machine @IP-publique
```

Configurez un NAT statique pour l'interface par défaut (FastEthernet0) du *client* en utilisant l'adresse publique du routeur *west* (77.128.1.1). Afin de vérifier que la nouvelle configuration a été prise en compte, vous pouvez utiliser les suivantes commandes :

```
show running-config
show ip nat translations
show ip nat statistics
```

Question 7 : *Depuis client, essayez encore une fois de pinger l'interface `g0/0` du router *east* (77.128.2.1). Normalement, il devrait maintenant marcher. Pour voir ce qui se passe en détail, vous pouvez exécuter les commandes `debug ip nat` ou `show ip nat statistics` au router *west* ; et, les commandes `debug ip icmp` ou `debug ip packet` au router *east*. Ces commandes activent le mode debugging dans les dispositifs. Retapez la commande ping et regardez dans le CLIs des dispositifs. Expliquez pourquoi le ping a réussi maintenant.*

Maintenant, pour le router *east*, l'émetteur du ping est le router *west* car il y a une translation d'adresse. Le ping revient au router *west*, où la translation d'adresse permet de restituer l'adresse IP original du *client* et délivrer en local la réponse.

Question 8 : *Encore une fois, depuis le hôte client, essayez de pinger l'un de deux servers web (http ou http2). Sont-ils capables de répondre ? Pourquoi ?*

No. La translation d'adresse ne change rien. Toujours, les adresses IP des servers web (http ou http2) font partie de sous-réseau local de client (192.168.1.0 / 24). Donc, le paquet est acheminé en local sans traverser le router west et subir la translation d'adresse. Comme il n'y pas d'interface réseaux avec l'IP 192.168.1.2 ou 192.168.1.3 directement connectés au réseau de client, le ping échoue.

Maintenant, configurez un NAT statique pour l'interface par défaut (FastEthernet0) de *http* en utilisant l'adresse publique du routeur *east* (77.128.2.1).

Question 9 : *Depuis http, essayez de pinger l'interface g0/0 du router west (77.128.1.1). Normalement, il devrait marcher comme dans le précédent puisque on a une translation d'adresse active au routeur east pour http. On va mettre en place une deuxième translation au routeur east pour http2. Est-ce que vous réussissez à la mettre en place ? Pourquoi ?*

La seconde va bloquer car il n'y a qu'une adresse publique à disposition sur le routeur east.

4.4 Translation d'adresse et de port

Pour résoudre le problème précédent, nous allons mettre en place une translation d'adresse et de port. Pour cela, il faut indiquer au routeur quelles adresses de machines internes ont le droit de se faire traduire. Ceci se fait grâce à la commande :

```
Router(config)#access-list <numéro> permit <réseau-à-nater> <anti-masque>
```

où

- numéro : numéro de la liste d'accès dans le router
- réseau-à-nater : adresse de réseau privé à être naté
- anti-masque : complémentaire du masque de réseau privé à être naté

Supprimez votre NAT précédent dans le router *east* :

```
east(config)# no ip nat inside source static @IP-privée-machine @IP-publique
```

Puis il suffit d'indiquer au routeur de faire une translation d'adresse et de port au même temps pour toutes les adresses dans la liste d'accès grâce au mot clé *overload* :

```
east(config)# ip nat inside source list <numéro> interface <nom-if> overload
```

où

- numéro : numéro de la liste d'accès dans le router
- nom-if : nom de l'interface du routeur dont l'adresse IP sera utilisé comme adresse publique

Question 10 : *Répétez l'expérience de la question précédente. Depuis http et http2, essayez de pinger l'interface g0/0 du router west (77.128.1.1). Est-ce que cela fonctionne maintenant ? Utilisez les commandes debug ip nat ou show ip nat statistics afin de vérifier les translations. Pourquoi ?*

Oui, grâce à la manipulation précédente, on utilise la même adresse IP publique (east) pour le deux serveurs mais des ports différents.

4.5 NAT statique et accès à un serveur

Les configurations de NAT précédentes permettaient à des machines du réseau interne privé de sortir sur Internet. Nous allons maintenant configurer un NAT permettant à n'importe quelle machine sur Internet (y compris *http*) d'interroger l'un des serveurs web du réseau interne privé. Cela représente un cas de figure : typiquement les serveurs web sont hébergés dans l'enceinte des réseaux privés institutionnels en derrière d'un routeur dit d'accès à l'Internet.

Question 11 : *Encore une fois, depuis le hôte client, essayez de pinguer l'un des deux serveurs web (*http* ou *http2*). Sont-ils capables de répondre ? Pourquoi ?*

No. La translation d'adresse ne change rien. Toujours, les adresses IP des serveurs web (*http* ou *http2*) font partie du sous-réseau local du client (192.168.1.0 / 24). Donc, le paquet est acheminé en local sans traverser le routeur *west* et subir la translation d'adresse. Comme il n'y a pas d'interface réseau avec l'IP 192.168.1.2 ou 192.168.1.3 directement connectés au réseau du client, le ping échoue.

Toutes les configurations précédentes permettent à l'intérieur de passer à l'extérieur mais pas l'inverse : pinguer depuis *client*, *http* ou *http2* mais pas vers *client*, *http* ou *http2* (sauf si on est directement connecté au hôte.)

Nous allons résoudre ça. Pour rendre les serveurs web accessibles de l'extérieur, on va indiquer au routeur *east* que les demandes web qu'il reçoit sur son adresse publique doivent être re-routées vers les ports 80 (employé par *http*) des serveurs web :

```
east(config)# ip nat inside source static tcp <@IP-privée port> <@IP-pub port>
```

où

- @IP-privée port : adresse IP privée de machine à nater et port employé dans la machine à nater
- @IP-pub port : adresse IP publique du routeur qui fait le NAT et port employé dans le routeur

*ATTENTION : Les serveurs web de TP ne peuvent qu'employer le port 80 et 443 pour les protocoles *http* et *https*, respectivement. Par contre, comme port "publique" vous pouvez utiliser des valeurs autres que 80 comme 8080 qui est un autre port alternatif employé par *http*.*

Afin d'accéder aux ports 80 de deux serveurs web (*http* ou *http2*), vous ne pouvez plus utiliser la commande *ping*, soit vous ouvrez des connexions TCP en utilisant la commande *telnet* <@IP-pub port>, soit vous essayez d'accéder au site web hébergés dans les serveurs depuis le PC client en ouvrant le navigateur web (Desktop → Web Browser) et en tapant dans la barre d'adresse `http://<adresse>:<port>` comme URL. Dans les routeurs debug `ip packets` afin de vérifier s'il y a des échanges *http* dans les serveurs web lorsque vous naviguez.

Question 12 : *Depuis le hôte client, essayez d'ouvrir des connexions TCP vers les ports 80 de deux serveurs web (*http* ou *http2*) en utilisant la translation d'adresse et de ports mise en place. Quels sont l'adresse et les ports que vous devez utiliser dans la commande *telnet* ou dans la barre d'adresse du navigateur. Pourquoi ?*

Pour le *http*, 77.128.2.1 :80 et pour le *http2*, 77.128.2.1 :8080, p. ex.

5 Annexe : Commandes CISCO IOS

5.1 Modes d'utilisation

Si le routeur demande si on veut initier une configuration initiale, répondre NON. Organisé autour du principe de modes d'utilisation : **non privilégié** vs **privilégié**.

Mode non privilégié, aussi appelé EXEC mode :

- Permet d'exécuter ensemble commandes par terminal : ping, telnet et rlogin
- Accès limité aux commandes show opt
 - ?
 - version

Mode privilégié :

- Permet de configurer le routeur
- Passage au mode privilégié par enable, ce qui change du prompt :
 - Router>
 - Router#
- sous-modes du mode privilégié accessibles, changent le prompt en Router (argument) #, p.ex. :
 - Router(config) # : Mode configuration du router
 - Router(config-if) # : Mode configuration d'un interface du router
- affichage des informations essentielles de la configuration du routeur :
 - Router#show interfaces
 - Router#show ip protocols
 - Router#show ip route
 - Router#show ip arp

5.2 Configuration globale

Passage au mode de configuration depuis le mode privilégié par commande config ou conf t et retour au mode normal par ctrl-z où exit :

```
Router# conf t
Router(config)# exit
Router#
```

Changement du nom du routeur

```
Router(config)#hostname MonRouteur
MonRouteur(config)
```

Désignation du serveur dns à utiliser

```
Router(config)#ip name-server aa.bb.cc.dd
```

Ajout mot de passe pour mode privilégié

```
Router(config)#enable secret mot2pass
```

Commande effective après validation par ctrl-z

5.3 Configuration de l'interface

Interfaces référencées par la convention :

```
media type slot#/port#
```

où

- `media type` : p.e. ethernet, fast ethernet, fddi, serial,...
- `slot#` : slot disponible, seulement sur routeurs avec slots qui permettent insertion modules ; pour accéder à interface `slot6 port2` : ethernet 6/2

```
MonRouteur# show interface ethernet 6/2
MonRouteur# show interface serial 0
```

Exemple de configuration d'interface :

```
MonRouteur# show interface serial 1/1
MonRouteur#conf t
MonRouteur(config)#interface serial 1/1
MonRouteur(config-if)#ip address 192.168.155.2 255.255.255.0
MonRouteur(config-if)#no shutdown
MonRouteur(config-if)#exit
MonRouteur#show interface serial 1/1
```

Retirer une commande : il suffit de la faire précéder d'un `no`

```
MonRouteur(config)#interface serial 1/1
MonRouteur(config-if)#no ip address 192.168.155.2 255.255.255.0
MonRouteur(config-if)exit
MonRouteur#show interface serial 1/1
```

Forcer l'interface à être allumée :

```
MonRouteur(config-if)#no shutdown
```

5.4 Configuration du routage

Le routage est activé par défaut. Si désactivé, le réactiver par :

```
MonRouteur(config)#ip routing
MonRouteur(config)#ctrl-z
```

Routage statique

```
MonRouteur#config
MonRouteur(config)#ip route 172.16.0.0 255.255.255.0 192.168.150.1
MonRouteur(config)#ctrl-z
MonRouteur#show ip route
```

Dans l'exemple :

- 172.16.0.0 : c'est l'adresse de sous-réseau
- 255.255.255.0 : c'est le masque de sous-réseau
- 192.168.150.1 : c'est l'adresse de la passerelle (*gateway*), c.-à.-d., du routeur suivant

Routage dynamique (par `rip` ou `ospf`)

```
router rip
version 2
network xxx.yyy.zzz.0
no auto-summary
end
```

Dans l'exemple :

- `network xxx.yyy.zzz.0` : c'est l'adresse de sous-réseau directement connecté à l'interface du routeur. Avec cette commande, on indique que ce sous-réseau participe au process RIP.

5.5 Sauvegarde

Une fois la configuration terminée (interfaces et routage), le routeur peut fonctionner et remplir ses tables de routage et ses tables arp.

```
show ip route  
show ip arp
```

Si on éteint le routeur, la `running-config` est perdue.

- pour la voir : `show running-config`
- pour la sauver : `copy running-config startup-config`