



Matière : Réseaux informatiques

TP N° 1 : Installation et configuration d'un réseau local sous Windows/Linux

I. Mise en situation

Dans de nombreuses entreprises, il est nécessaire de pouvoir faire communiquer les ordinateurs afin de partager des ressources et améliorer le rendement tout en diminuant les coûts : impression d'un document, récupération d'une image scannée sur un ordinateur du réseau, accès internet partagé ... etc.

Pour imprimer un document sans réseau, il faudrait soit 1 imprimante par ordinateur (coûteux !), soit déplacer l'imprimante sur le poste à imprimer (galère !) ou copier/coller les fichiers sur un support amovible et faire le transfert sur le poste où se trouve l'imprimante (perte de temps).

Avec le réseau, tout devient plus simple mais encore faut-il savoir le mettre en œuvre ...

II. Problématique

Comment établir une liaison physique entre des ordinateurs et réaliser la configuration logicielle afin que ces ordinateurs puissent communiquer entre eux ?

III. Etude

On se propose de vérifier le réseau du laboratoire dans lequel nous travaillons, nous créerons ensuite un réseau local entre deux ou plusieurs ordinateurs en suivant le protocole TCP/IP.

IV. Activité

1- Etude de la structure du réseau du laboratoire

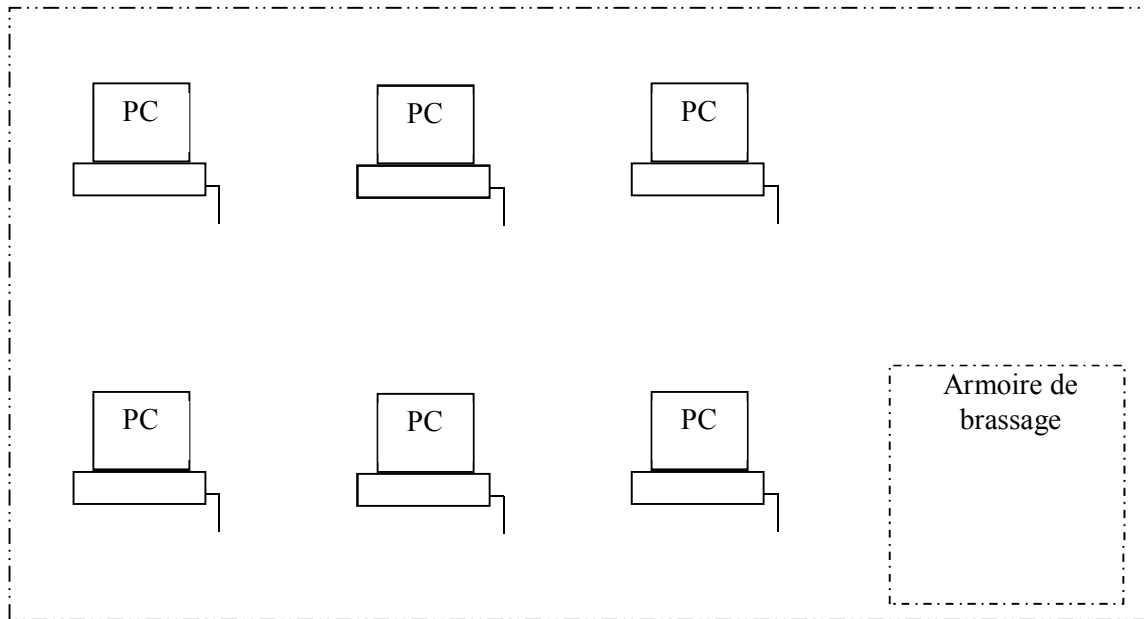
A partir des éléments du cours répondez aux questions suivantes :

a- Quelle est la topologie du réseau du laboratoire dans lequel vous travaillez ?

.....

b- Quel est le type de ce réseau (LAN, MAN ou WAN) ?

-
- c- Suivre les câbles de liaison du réseau informatique puis représenter (sous forme dessinée) les différents matériels utilisés sur ce réseau (représenter les câbles, le switch, ...).



2- Câblage physique d'un ordinateur au réseau

- a- A l'aide d'un testeur de câble réseau, vérifier la connexion entre une prise RJ45 du panneau de brassage et une prise RJ45 murale. Est-ce un câble croisé ou un câble droit (expliquer) ?

.....

.....

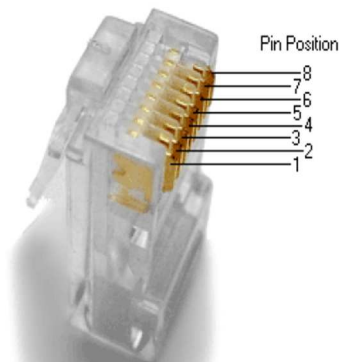
.....

.....

- b- A présent, vous devez réaliser un câble RJ45 **droit** et un autre câble RJ45 **croisé**.

Pour fabriquer un câble RJ45, connectez les fils suivant la procédure ci-dessous :

Saisissez la première fiche RJ45 entre vos doigts devant vous. Le petit levier en plastique doit être positionné derrière comme ci-dessous.



Côté 1 : Câble droit ou croisé			Côté 2 : Câble droit			Côté 2 : Câble croisé		
<i>R/T</i>	<i>Fils</i>	<i>Couleurs</i>	<i>R/T</i>	<i>Fils</i>	<i>Couleurs</i>	<i>R/T</i>	<i>Fils</i>	<i>Couleurs</i>
TD+	1	Blanc/Vert	TD+	1	Blanc/Vert	RD+	1	Blanc/Orange
TD-	2	Vert	TD-	2	Vert	RD-	2	Orange
RD+	3	Blanc/Orange	RD+	3	Blanc/Orange	TD+	3	Blanc/Vert
Non utilisée	4	Bleu	Non utilisée	4	Bleu	Non utilisée	4	Bleu
Non utilisée	5	Blanc/Bleu	Non utilisée	5	Blanc/Bleu	Non utilisée	5	Blanc/Bleu
RD-	6	Orange	RD-	6	Orange	TD-	6	Vert
Non utilisée	7	Blanc/Marron	Non utilisée	7	Blanc/Marron	Non utilisée	7	Blanc/Marron
Non utilisée	8	Marron	Non utilisée	8	Marron	Non utilisée	8	Marron

La tresse de masse n'est pas croisée, vous n'êtes donc pas obligé de la sectionner !

3- Configuration d'un réseau sous Windows

Dans cette partie, nous nous intéressons à la configuration d'un réseau local sous le système d'exploitation Windows.

a- Configuration d'un réseau entre deux machines

Dans un premier temps, vous devez installer et configurer un réseau entre deux machines (Machine-1 et Machine-2).

Question : Quel type de câble faut-il utiliser pour raccorder deux ordinateurs ?

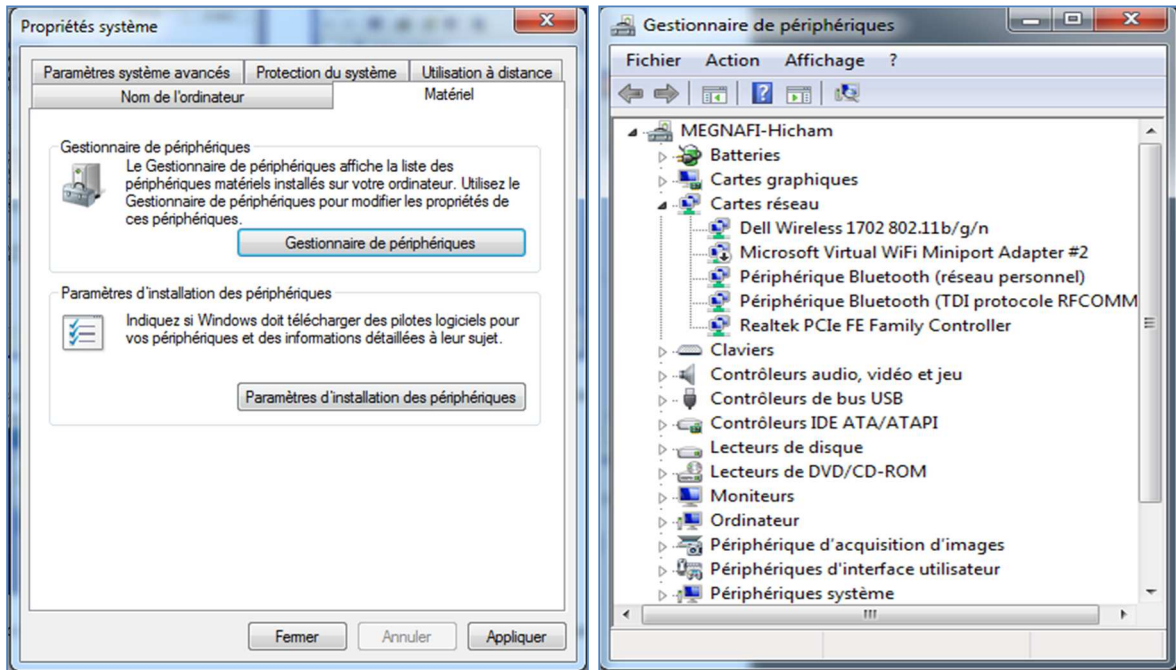
.....

Pour pouvoir communiquer entre eux les ordinateurs doivent être munis d'une carte réseau. Suivre la procédure suivante pour installer et configurer le réseau :

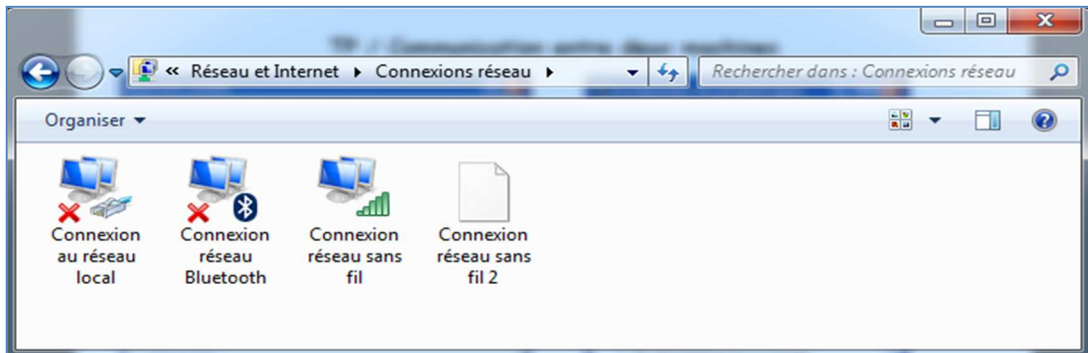
Configuration de la carte réseau sous Windows

Il faut d'abord vérifier si la carte réseau a bien été reconnue par Windows.

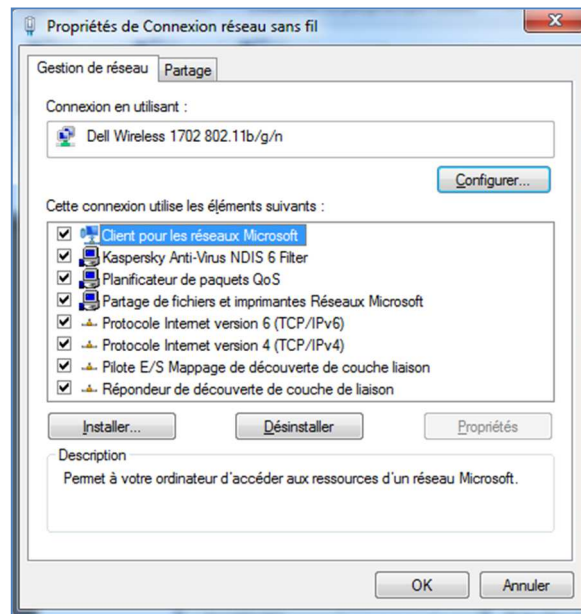
Pour vérifier si la carte réseau est bien installée, faites un clic droit sur le poste de travail, puis propriétés et choisir l'onglet « matériel » et cliquez sur « gestionnaire de périphériques ».



Allez dans la section « Centre Réseau et partage » (démarrer, panneau de configuration, Centre Réseau et partage) puis sur « Modifier les paramètres de la carte ». Vous arrivez à une page ressemblant à ceci :



Faites un clic droit sur « Connexion au réseau local » et choisir propriétés. On arrivera à la page suivante :



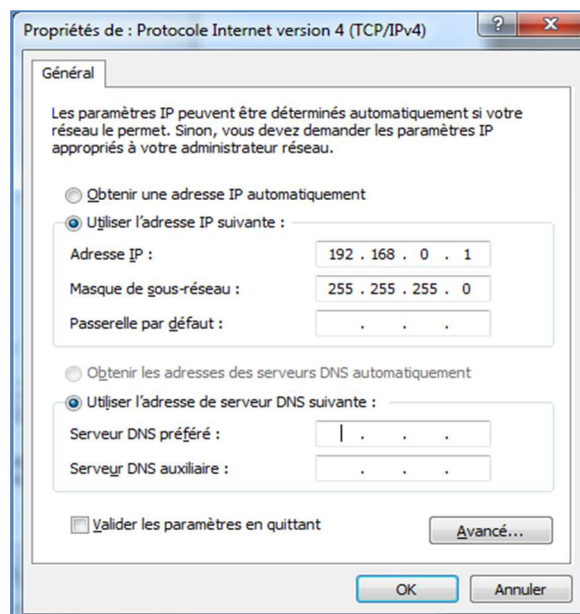
Pour créer un réseau avec le protocole TCP/IP, on doit attribuer à chaque machine du réseau une adresse appelée adresse IP. Chaque équipement (ordinateur, imprimante, routeur,...) sur un réseau est identifié par cette adresse unique, on parle encore de numéro IP. L'adresse IP est composée de 4 nombres séparés d'un point, chacun de ces nombres est codé sur un octet et peut donc prendre une valeur comprise entre 0 et 255.

Exemple d'adresse IP : 152.125.136.5

L'attribution de ces adresses doit être choisie pour les rendre compatibles.

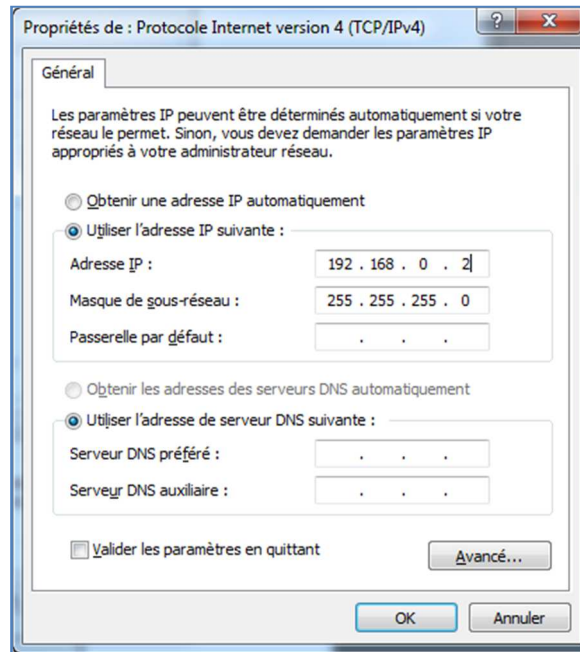
Attribution d'une adresse IP pour la Machine-1

Faire un double-clic sur « Protocole Internet TCP/IP », régler l'adresse IP à 192.168.0.1 et le masque de sous-réseau à 255.255.255.0 cela doit donner l'écran ci-dessous.



Attribution d'une adresse IP pour la Machine-2

Connectez-vous sur l'autre ordinateur (Machine-2). Aller ensuite dans les propriétés TCP/IP. Régler l'adresse IP à 192.168.0.2 et le masque de sous-réseau à 255.255.255.0



Valider jusqu'à revenir sur le bureau. Voilà, les PC sont en réseau.

Test de la communication

Le test de la validité de l'adresse IP peut être réalisé à l'aide de la commande « ping »
Pour tester le réseau en profondeur, il suffit d'ouvrir une fenêtre de ligne de commande :

Démarrer / Exécuter puis taper : **cmd**

puis d'effectuer successivement les étapes suivantes :

ping sur l'adresse locale (127.0.0.1), représentant votre ordinateur :

ping 127.0.0.1

ping sur les adresses IP des ordinateurs du réseau, par exemple :

ping 192.168.0.2

Si l'interface réseau est correctement configurée, le résultat suivant doit apparaître sur l'écran (*commande ping exécutée à partir de la Machine-1*) :

ping 192.168.0.2

Envoi d'une requête 'ping' sur 192.168.0.2 avec 32 octets de données :

Réponse de 192.168.0.2 : octets=32 temps=34 ms TTL=54

Réponse de 192.168.0.2 : octets=32 temps=37 ms TTL=54

Réponse de 192.168.0.2 : octets=32 temps=32 ms TTL=54

Réponse de 192.168.0.2 : octets=32 temps=33 ms TTL=54

Statistiques Ping pour 192.168.0.2 :

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

Durée approximative des boucles en millisecondes :

Minimum = 32ms, Maximum = 37ms, Moyenne = 34ms

La commande ipconfig

Dans une fenêtre DOS, taper « ipconfig /all ». Cette commande vous affiche tous les paramètres réseau de votre ordinateur, très pratique pour vérifier votre configuration

Relevez sur votre feuille les informations suivantes :

Nom de l'hôte :

Adresse physique :

Adresse IP :

Masque de sous réseau :

b- Configuration d'un réseau entre plusieurs machines

A présent, vous devez installer et configurer un réseau entre plusieurs machines à l'aide du commutateur (Switch) qui se trouve dans l'armoire réseau du laboratoire.

Question : Quel type de câble faut-il utiliser pour raccorder les ordinateurs au Switch ?

.....

A l'aide de la même procédure de configuration utilisée précédemment, attribuez à chaque machine l'adresse IP suivante 192.168.0.Y (ou Y correspond au n° de votre machine dans le laboratoire).

Utilisez les mêmes procédures de test vues précédemment pour tester la communication entre les différentes machines.

4- Configuration d'un réseau sous Linux

Dans cette partie, nous nous intéressons à la configuration d'un réseau local sous le système d'exploitation Linux.

Nous allons utiliser différentes commandes Linux qui permettant de configurer les différentes machines.

a- Attribution de l'adresse IP

Utilisez la commande ifconfig pour configurer les interfaces Ethernet.

A chaque carte Ethernet est associée au moins une interface dont le nom est sous la forme <eth><numéro>. Vous utiliserez ici l'interface eth0 qui correspond à l'unique carte Ethernet de votre machine. Pour configurer une interface, il faut lui fournir un certain nombre de renseignements : nom de l'interface, adresse IP, masque du réseau ...

Par exemple la commande suivante :

ifconfig eth0 192.168.0.3 netmask 255.255.255.0 up

attribue l'adresse 192.168.0.3 à la carte eth0 de la machine. Le mot clé up à la fin indique une commande d'activation de l'interface.

Utilisez la commande ifconfig pour configurer votre interface avec l'adresse suivante 192.168.0.Y (Y correspond au de n° de votre machine dans le laboratoire).

Vérifiez la configuration de l'interface à l'aide de la commande ifconfig avec pour seul argument le nom de l'interface. Quelles sont les informations affichées ?

.....
.....
.....
.....

b- Identification des machines par un nom symbolique

Les adresses IP sont bien adaptées pour l'utilisation par les machines, un peu moins pour être utilisées par les humains. Pour faciliter le nommage des machines un système d'adresses symboliques est mis en place.

En utilisant la commande hostname, attribuez un nom symbolique à chacune des machines de votre réseau. Utilisez, par exemple, vos noms.

hostname <nom_symbolique>

c- Contrôle du réseau

Il faut maintenant vérifier que les machines sont bien interconnectées et bien configurées. L'outil standard ping permet de vérifier qu'une machine distante répond bien quand on l'appelle.

Par exemple la commande suivante :

ping 192.168.0.2

permet de tester la connexion avec la machine qui a pour adresse IP 192.168.0.2

On peut utiliser la commande ping en lui fournissant le nom d'une machine distante à contacter :

ping <nom_symbolique_machine_distante>

Utilisez la commande ping pour vérifier la connexion avec vos voisins.



Matière : Réseaux informatiques TP N° 2 : Liaison de données

I. Objectifs

- ✓ Comprendre le principe d'encapsulation.
- ✓ Etudier l'adressage (MAC / IP) et la résolution d'adresses en utilisant le protocole ARP.
- ✓ Utiliser Wireshark pour capturer et analyser les trames Ethernet II.
- ✓ Expliquer les différents champs d'une trame Ethernet II.
- ✓ Utiliser Wireshark pour examiner les échanges ARP.
- ✓ Utiliser la commande arp.

II. Capture de trames

Après avoir ouvert une session sur votre poste, ouvrez un terminal et lancez la commande **ipconfig /all**

1. Que fait cette commande ?

.....
.....

2. Quelles interfaces réseaux sont actuellement actives ?

.....
.....

3. Parmi ces interfaces, quelle est celle qui vous permet de communiquer avec d'autres machines ?

.....
.....

4. Quelles sont les adresses MAC et IPv4 de cette interface ?

MAC	Adresse IP

5. Selon vous, de manière générale, pourquoi utilise-t-on l'adresse IP et non directement l'adresse MAC pour les communications réseaux ?

.....

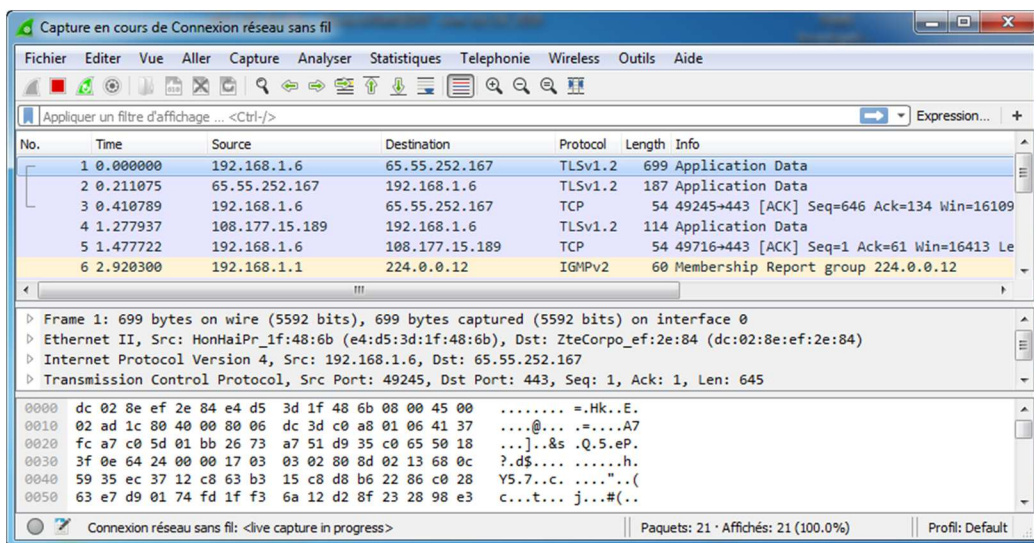
Pour mieux comprendre comment les données sont échangées sur le réseau, vous allez utiliser un « analyseur de paquets » appelé Wireshark.

Wireshark est un logiciel d'analyse réseau (sniffer) permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés.

- Lancez le logiciel Wireshark.
- Sélectionnez l'interface connectée sur le réseau du laboratoire.
- Appropriiez-vous l'application en consultant les info-bulles et l'aide, le cas échéant.

La fenêtre est divisée en 3 parties :

- ✓ en haut, la liste des paquets reçus ou envoyés par l'interface.
- ✓ en bas, le contenu du paquet sélectionné, au format hexadécimal.
- ✓ au milieu, Wireshark traduit les données brutes du paquet dans un format compréhensible.



6. Lancez la commande **ping** vers votre voisin. D'après les informations capturées et décodées par Wireshark, quels sont les paquets envoyés et reçus suite à l'exécution du **ping** ? Quels protocoles sont utilisés ?

Le panneau du milieu de Wireshark est basé sur le modèle OSI inversé : en haut, les couches basses (physique, liaison de données, etc.), en bas, les couches hautes (transport, application).

7. A quelles couches appartiennent les protocoles cités précédemment ?

Vous pouvez constater que vous capturez des paquets émis par d'autres machines du réseau. Pour éviter que vos captures ne soient polluées, vous pouvez utiliser des filtres. Wireshark propose deux types de filtres :

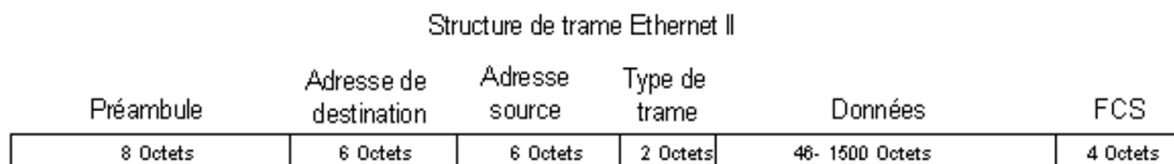
- Le filtre de capture : dans le menu « capture > options », faites en sorte que soit capturé uniquement le dialogue entre votre machine et celle du voisin. Vous pouvez utiliser le filtre de capture suivant :

host adresse_ip_voisin and (arp or icmp)

- Le filtre à l'affichage : après avoir effectué la capture précédente, dans le menu « analyse > display filters », faites en sorte que s'affiche uniquement le dialogue entre votre machine et celle du voisin.

III. Ethernet :

Le format d'une trame Ethernet II est illustré à la figure suivante :

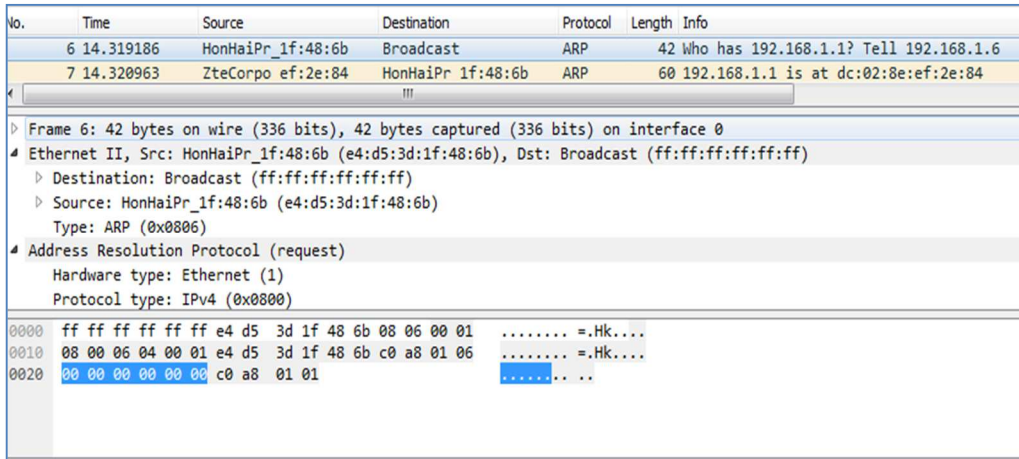


À l'aide de la fenêtre Packet Details obtenu par le logiciel Wireshark, il est possible d'obtenir les informations suivantes sur la trame Ethernet II :

Champ	Valeur	Description
Préambule	Non affichée dans la capture.	Ce champ contient des bits de synchronisation traités par la carte réseau.
Adresse de destination	ff:ff:ff:ff:ff:ff	Les adresses de couche 2 pour la trame. La longueur de chaque adresse est de 48 bits, ou 6 octets, exprimés en 12 chiffres hexadécimaux, 0-9,A-F. Le format courant est le suivant : 12:34:56:78:9A:BC. ✓ Les six premiers numéros hexadécimaux indiquent le fabricant de la carte réseau (NIC). Reportez-vous à http://www.neotechcc.org/forum/macid.htm pour obtenir une liste de codes fournisseurs. ✓ Les six derniers chiffres hexadécimaux, ac:a7:6a, ont le numéro de série de la carte réseau. ✓ L'adresse de destination peut être une adresse de diffusion qui ne contient que des 1 ou à monodiffusion.
Adresse source	00:16:76:ac:a7:6a	

		L'adresse source est toujours à monodiffusion.
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet II. Deux types de trame standard sont : Valeur Description 0x0800 Protocole IPv4 0x0806 Résolution de l'adresse ARP
Données	ARP	Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1500 octets.
FCS	Non affichée dans la capture.	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par l'ordinateur émetteur, et englobe les adresses de trames, le type et le champ de données. Elle est vérifiée par le récepteur.

1. Quelle est la signification de tous les 1 dans le champ adresse de destination ?



La figure contient une vue éclatée de la capture Wireshark de trame 1. Utilisez ces informations pour remplir le tableau suivant :

Champ	Valeur
Adresse de destination	Adresse MAC :
	Fabricant de la carte réseau :
	Numéro de série de la carte réseau :
Adresse source	Adresse MAC :
	Fabricant de la carte réseau :
	Numéro de série de la carte réseau :
Type de trame	

IV. ARP :

Tâche 1 : Utilisation de la commande arp de Windows :

Étape 1 : accès au terminal de Windows.

Sans options, la commande **arp** affiche des informations d'aide utiles. Reportez-vous à la figure «Syntaxe de la commande arp »

```
C:\> arp
Affiche et modifie les tables de conversion d'adresses IP en adresses physiques utilisées par le
protocole ARP.
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a                               Affiche les entrées ARP actuelles en interrogeant les données de
                                protocole actuelles. Si inet_addr est spécifié, seules les adresses IP et
                                physique de l'ordinateur spécifié s'affichent. Si plusieurs interfaces réseau
                                utilisent ARP, les entrées de chaque table ARP s'affichent.

-g                               Identique à -a.
inet_addr                       Spécifie une adresse Internet.
-N if_addr                      Affiche les entrées ARP de l'interface réseau spécifiée par if_addr.

-d                               Supprime l'hôte spécifié par inet_addr. inet_addr peut s'utiliser avec le
                                caractère générique * pour supprimer tous les hôtes.

-s                               Ajoute l'hôte et associe l'adresse Internet inet_addr à l'adresse physique
                                eth_addr. L'adresse physique est fournie sous forme de 6 octets
                                hexadécimaux séparés par des traits d'union. L'entrée est permanente.

eth_addr                        Spécifie une adresse physique.
if_addr                         Si présent, spécifie l'adresse Internet de l'interface dont la table de
                                conversion des adresses doit être modifiée. Si absent, la première
                                interface applicable est utilisée.

Exemple :
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Ajoute une entrée statique.
> arp -a .... Affiche la table arp.
```

Syntaxe de la commande arp

1. Exécutez la commande **arp** sur votre ordinateur, et examinez les résultats.
2. Quelle commande est utilisée pour afficher toutes les entrées dans le cache ARP ?

.....

3. Quelle commande est utilisée pour supprimer toutes les entrées du cache ARP (vider le cache ARP) ?

.....

4. Quelle commande est utilisée pour supprimer l'entrée du cache ARP pour 192.168.0.2 ?

.....

Étape 2 : utilisation de la commande arp pour examiner le cache ARP local.

```
C:\> arp -a
Aucune entrée ARP trouvée
C:\>
```

Cache ARP vide

Sans communication réseau, le cache ARP doit être vide. Ceci est illustré dans la figure « Cache ARP vide »

1. Exécutez la commande qui affiche les entrées ARP. Quels sont les résultats ?

.....

Étape 3 : utilisation de la commande ping pour ajouter de façon dynamique des entrées dans le cache ARP.

La commande **ping** sert à tester la connectivité réseau. En accédant à d'autres périphériques, les associations ARP sont ajoutées de façon dynamique au cache ARP.

1. Exécutez la commande **ping** vers un ordinateur « voisin ». La figure suivante illustre la nouvelle entrée du cache ARP.

```
C:\> arp -a
Interface : 192.168.0.1 --- 0x16
Adresse Internet  Adresse physique      Type
172.16.0.2        00-10-a4-7b-01-5f    dynamique
C:\>
```

Affichage du cache ARP

2. Comment l'entrée ARP a-t-elle été ajoutée au cache ARP ? Conseil : consultez la colonne Type.

3. Quelle est l'adresse physique de l'ordinateur « voisin » de destination ?

Adresse IP	Adresse physique	Mode de détection ?

Pour la tâche suivante, Wireshark est utilisé pour capturer et examiner un échange ARP. Ne fermez pas le terminal Windows. Il sera utilisé pour afficher le cache ARP.

Tâche 2 : utilisation de Wireshark pour examiner les échanges de ARP

- 1- Préparez Wireshark pour les captures (Utiliser le filtre vu précédemment).
- 2- Videz le cache ARP.
- 3- Envoyez une requête **ping** à votre voisin, à l'aide de la commande

ping -n 1 192.168.0.2

4- Arrêtez la capture Wireshark et évaluez la communication. La fenêtre Packet list de Wireshark affiche le nombre de paquets capturés. La fenêtre Packet Details affiche le contenu du protocole ARP.

5- Analysez la trame Ethernet II pour identifier le code associé au protocole ARP.

.....

6- À l'aide de votre capture Wireshark, répondez aux questions suivantes :

- Quel était le premier paquet ARP ?

.....

- Quel était le deuxième paquet ARP ?

.....

- Renseignez le tableau suivant avec les informations sur le premier paquet ARP :

Champ	Valeur
Adresse MAC de l'expéditeur	
Adresse IP de l'expéditeur	
Adresse MAC cible	
Adresse IP cible	

- Renseignez le tableau suivant avec les informations sur le deuxième paquet ARP :

Champ	Valeur
Adresse MAC de l'expéditeur	
Adresse IP de l'expéditeur	
Adresse MAC cible	
Adresse IP cible	

- Si la trame Ethernet II pour une requête ARP est une diffusion, pourquoi l'adresse MAC cible ne contient que des 0 dans le premier paquet ARP ?

.....

7- Faites un schéma représentant les différents champs de la requête et de la réponse ARP, ainsi que leur longueur.

Matière : Réseaux informatiques TP N° 3 : Routage statique

I. Objectifs

Le but de ce TP est de configurer des stations de travail et des routeurs afin de communiquer ensemble sur des réseaux différents.

II. Activités

Dans ce TP, nous utiliserons le logiciel **Packet Tracer**, fourni par Cisco.

1- Mise en place des périphériques dans la topologie

Dans cette partie nous faisons glisser les différents équipements du réseau (Routeurs, Commutateurs et PC) sur l'espace de travail afin d'arriver à la figure suivante :

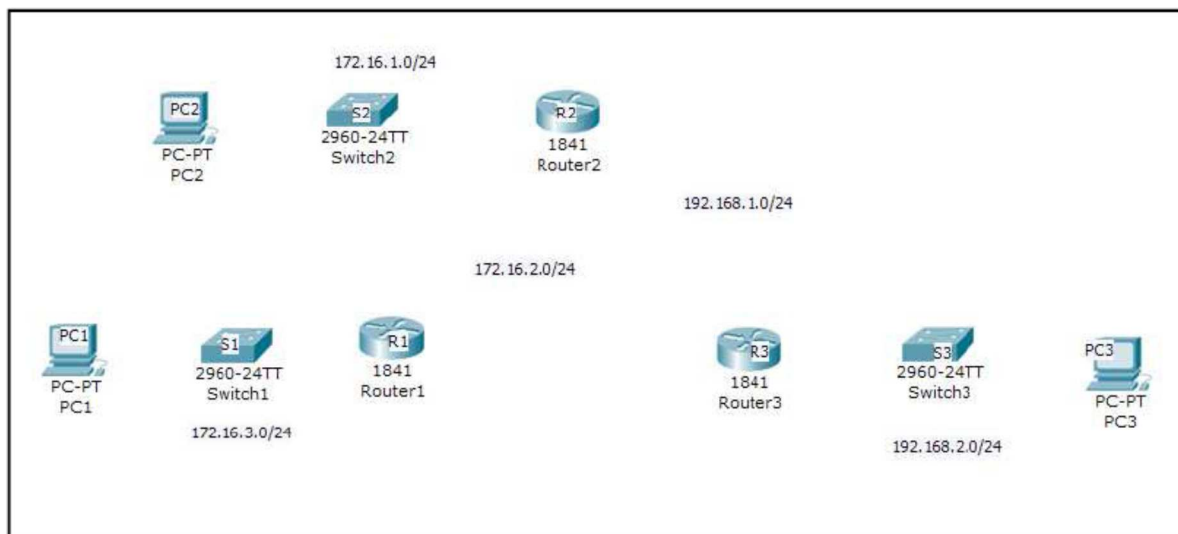


Figure 1 – Périphériques de la topologie simulée

2- Ajout des modules aux routeurs

Les Routeurs Cisco offrent la possibilité d'ajouter différents modules. L'outil de simulation Packet Tracer permet de simuler une façade de routeur et ainsi monter différents modules. Pour ajouter un module il faut le faire dans cet ordre :

- Mettre hors tension le routeur ;
- Glisser le module dans l'emplacement prévu à cet effet ;
- Remettre en tension le routeur.

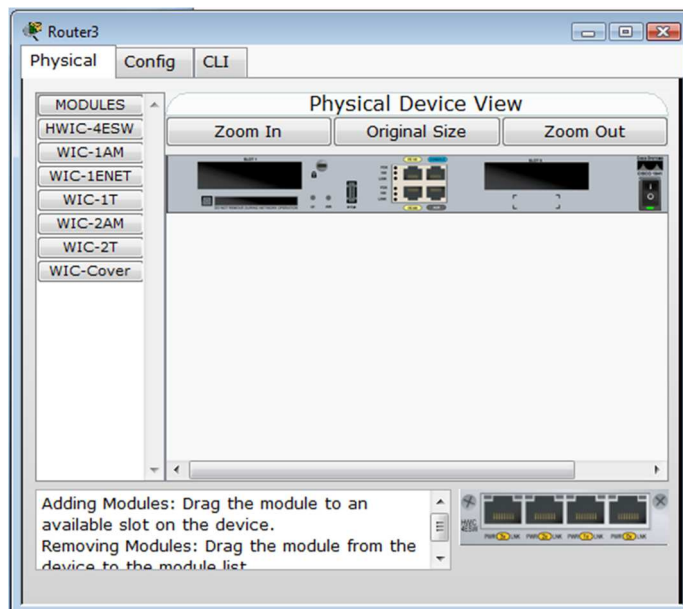


Figure 2 – Ajout de port WIC-2T au routeur

3- Attribution d'un nom aux périphériques

Nous attribuons un nouveau nom d'affichage sur l'espace de travail aux différents équipements du réseau ainsi qu'aux routeurs :

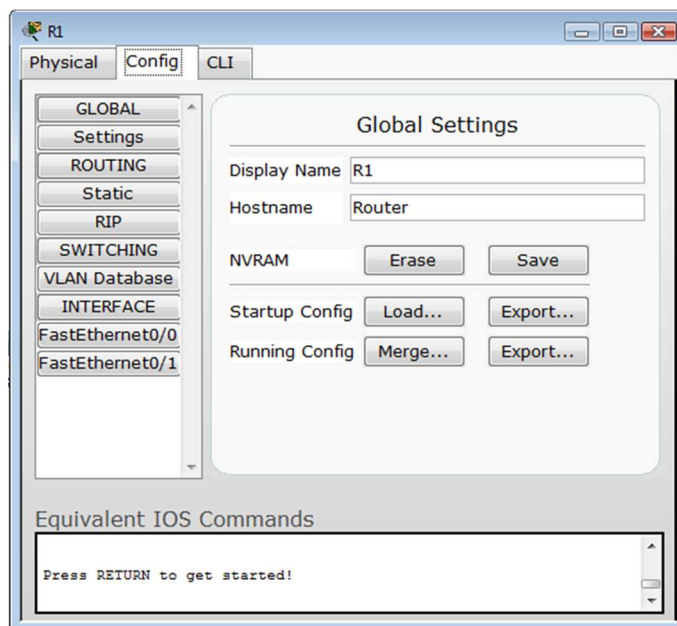


Figure 3 – Changement de nom d'un routeur

De plus nous changeons également le « hostname » des routeurs avec les commandes suivante en mode CLI :

```

1 Router1> enable
2 Router1 # conf t
3 Router1(config)#
4 Router1(config)#hostname R1
5 R1(config)#exit
6 R1#

```

3- Connexion des périphériques

Il est utile d'utiliser un commutateur afin de relier plusieurs PC entre eux dans le sous-réseau, car les routeurs ont un nombre limité de ports Ethernet.

Les routeurs permettent de relier des réseaux séparés par de grandes distances. Or, d'après la norme, un câble Ethernet ne doit pas dépasser 100m (en CAT 5 et 5e). Nous utilisons donc des câbles séries qui sont prévus à cet effet. De plus les câbles séries permettent d'atteindre de plus grandes vitesses que les câbles Ethernet.

Nous utilisons des câbles droits car le routeur et/ou le commutateur permettent le croisement.

Nous relierons à l'aide de câble série l'interface Serial0/0/0 du routeur R1 à l'interface Serial0/0/0 du routeur R2.

Nous relierons à l'aide de câble série l'interface Serial0/0/1 du routeur R2 à l'interface Serial0/0/1 du routeur R3.

Nous relierons les autres équipements à l'aide de câbles Ethernet droit.

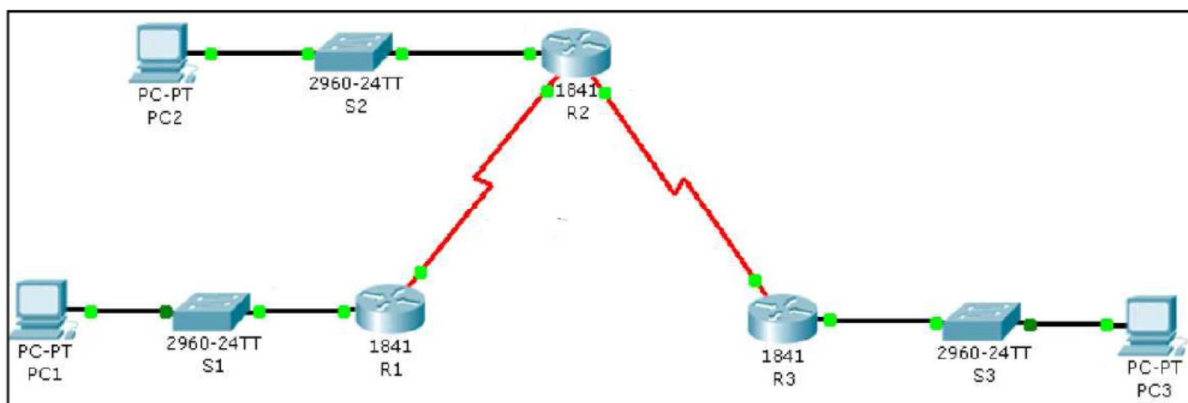


Figure 4 – Connexion des équipements

4- Configuration des informations IP sur les interfaces

Le réseau que nous allons simuler comporte 5 sous-réseaux : 172.16.1.0/24, 172.6.3.0/24, 172.16.2.0/24, 192.168.1.0/24 et 192.168.2.0/24 (Comme le montre la figure ci-dessous).

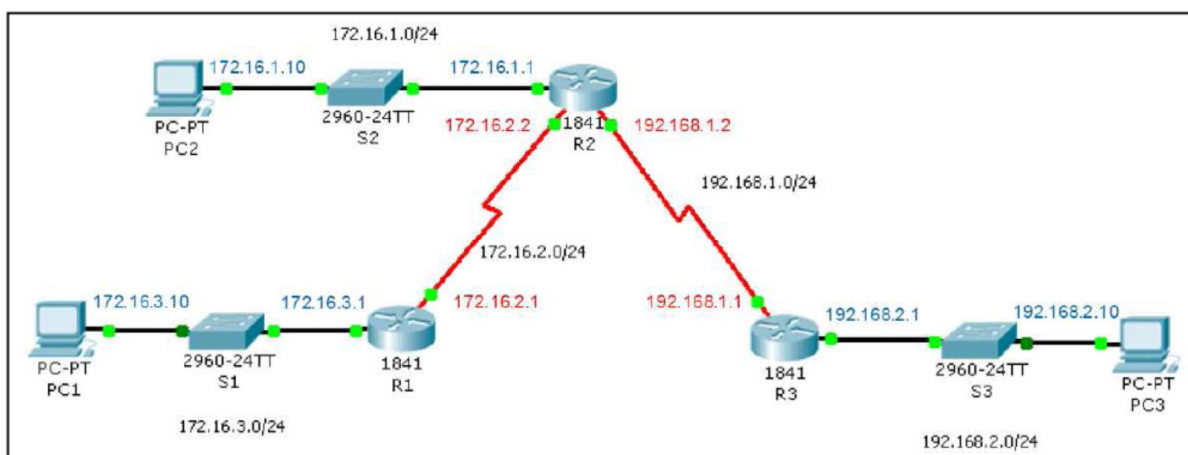


Figure 5 – Topologie du réseau simulé

Dans ce qui suit, nous allons attribuer les adresses IP aux interfaces des routeurs et des PCs.

a- Configuration des PCs

Avec Packet Tracer nous pouvons simuler des PCs, nous configurons les trois PCs en suivant la topologie du TP. N'oubliez pas de fixer l'adresse de la passerelle (Gateway) qui représente l'adresse du routeur connecté au réseau auquel appartient le PC (Figure 5).

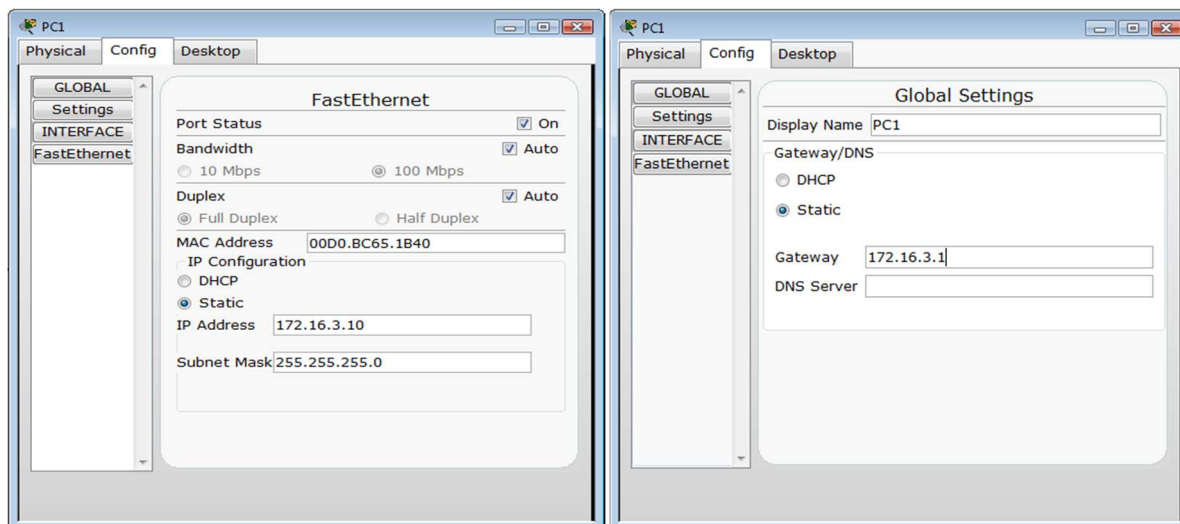


Figure 6 – Configuration de l'interface réseau d'un PC

b- Configuration des interfaces Ethernet des routeurs

Dans cette partie nous allons configurer les interfaces **FastEthernet** des routeurs R1, R2 et R3 en suivant le plan d'adressage donné ci-dessus.

Interface FastEthernet 0/0 (R1)

```
1 R1>enable
2 R1# conf t
3 R1(config)# interface fastEthernet0/0
4 R1(config-if)# ip address 172.16.3.1 255.255.255.0
5 R1(config-if)# no shutdown
6 R1(config-if)#exit
R1(config)#exit
R1# copy running-config startup-config
```

Interface FastEthernet 0/0 (R2)

```
1 R2>enable
2 R2# conf t
3 R2(config)# interface fastEthernet0/0
4 R2(config-if)# ip address 172.16.1.1 255.255.255.0
5 R2(config-if)# no shutdown
6 R2(config-if)#exit
R2(config)#exit
R2# copy running-config startup-config
```

Interface FastEthernet 0/0 (R3)

```
1 R2>enable
2 R2# conf t
3 R2(config)# interface fastEthernet0/0
4 R2(config-if)# ip address 192.168.2.1 255.255.255.0
5 R2(config-if)# no shutdown
6 R2(config-if)#exit
R2(config)#exit
R2# copy running-config startup-config
```

c- Configuration des interfaces série des routeurs

La procédure est identique aux interfaces Ethernet sauf qu'il faudra indiquer une fréquence d'horloge (clock rate) sur l'une des interfaces série. En fait, généralement, c'est le matériel du fournisseur d'accès (modem) qui fournit cette fréquence. En laboratoire, ce sera l'un des routeurs qui la fournira, au choix. Celui qui donnera la fréquence de l'horloge sera appelé DCE (Data Communication Equipment) et l'autre DTE (Data Terminating Equipment). On utilisera un câblage ayant une connexion DCE et DTE de part et d'autre. Le routeur DCE donnera la fréquence. On lui donnera donc un paramètre supplémentaire avec une fréquence au choix exprimée en bit/s.

Configuration de R1

Vérifions si Serial0/0/0 de R1 est DTE ou DCE :

```
1 R1#show controllers serial0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35
```

Serial0/0/0 de R1 est DCE donc nous devons configurer la clock rate :

```
1 R1(config)#interface serial0/0/0
2 R1(config-if)#ip address 172.16.2.1 255.255.255.0
3 R1(config-if)# clock rate 64000
4 R1(config-if)#no shutdown
5 R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Configuration de R2

Vérifions si Serial0/0/0 de R2 est DTE ou DCE :

```
1 R2#show controllers serial0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DTE V.35
```

Serial0/0/0 de R2 est DTE donc pas besoin de configurer la clock rate :

```
1 R2(config)#interface serial0/0/0
```

```
2 R2(config-if)#ip address 172.16.2.2 255.255.255.0
3 R2(config-if)# no clock rate
4 R2(config-if)#no shutdown
5 R2# copy running-config startup-config
  Destination filename [startup-config]?
  Building configuration...
```

Vérifions si Serial0/0/1 de R2 est DTE ou DCE :

```
1 R2#show controllers serial0/0/1
  Interface Serial0/0/1
  Hardware is PowerQUICC MPC860
  DCE V.35
```

Serial 0/0/0 de R2 est DTE donc pas besoin de configurer la clock rate :

```
1 R2(config)#interface serial0/0/1
2 R2(config-if)#ip address 192.168.1.2 255.255.255.0
3 R2(config-if)# no clock rate
4 R2(config-if)#no shutdown
5 R2# copy running-config startup-config
  Destination filename [startup-config]?
  Building configuration...
```

Configuration de R3

Vérifions si Serial0/0/1 de R3 est DTE ou DCE :

```
1 R3#show controllers serial0/0/1
  Interface Serial0/0/1
  Hardware is PowerQUICC MPC860
  DCE V.35
```

Serial0/0/1 de R3 est DCE donc nous devons configurer la clock rate :

```
1 R3(config)#interface serial0/0/1
2 R3(config-if)#ip address 192.168.1.1 255.255.255.0
3 R3(config-if)# clock rate 64000
4 R3(config-if)#no shutdown
5 R3# copy running-config startup-config
  Destination filename [startup-config]?
  Building configuration...
```

5- Vérification des différentes interfaces des routeurs

La commande « #show ip interface brief » permet d'afficher un résumé sous forme de tableau afin de voir si la configuration est conforme à nos attentes. Exemple de la commande « #show ip interface brief » pour le routeur R1.

1	<i>R1#show ip interface brief</i>					
	<i>Interface</i>	<i>IP-Address</i>	<i>OK?</i>	<i>Method</i>	<i>Status</i>	<i>Protocol</i>
	<i>FastEthernet0/0</i>	<i>172.16.3.1</i>	<i>YES</i>	<i>manual</i>	<i>up</i>	<i>up</i>
	<i>FastEthernet0/1</i>	<i>unassigned</i>	<i>YES</i>	<i>manual</i>	<i>administratively down</i>	<i>down</i>
	<i>Serial0/0/0</i>	<i>172.16.2.1</i>	<i>YES</i>	<i>manual</i>	<i>up</i>	<i>up</i>
	<i>Serial0/0/1</i>	<i>unassigned</i>	<i>YES</i>	<i>manual</i>	<i>down</i>	<i>down</i>
	<i>Vlan1</i>	<i>unassigned</i>	<i>YES</i>	<i>manual</i>	<i>administratively down</i>	<i>down</i>

6- Configuration du routage statique

Le principe du routage statique est le suivant: Pour chaque routeur, identifier tous les réseaux qui ne sont pas voisins (En d'autres termes, qui ne sont pas directement raccordés) à celui-ci. Ensuite il faut définir une route (à l'aide d'une passerelle) pour atteindre chacun de ces réseaux.

Appliquons ce principe sur notre schéma ci-dessus:

➤ **Pour le routeur R1**

Les réseaux qui ne sont pas directement raccordés au routeur R1 sont : **172.16.1.0/24**, **192.168.1.0/24** et **192.168.2.0/24**

La passerelle pour les atteindre est: **172.16.2.2**

➤ **Pour le routeur R2**

Les réseaux qui ne sont pas directement raccordés au routeur R2 sont : **172.16.3.0/24** et **192.168.2.0/24**.

La passerelle pour atteindre le réseau **172.16.3.0/24** est : **172.16.2.1**

La passerelle pour atteindre le réseau **192.168.2.0/24** est : **192.168.1.1**

➤ **Pour le routeur R3**

Les réseaux qui ne sont pas directement raccordés au Routeur R3 sont: **172.16.1.0/24**, **172.16.2.0/24** et **172.16.3.0/24**

La passerelle pour les atteindre est : **192.168.1.2**

Traduisons ensuite ce qu'on vient de faire en commande Cisco.

Il y a deux façons de créer une route statique avec les routeurs Cisco :

1	<i>R#ip route [@IP du réseaux dest] [masque du réseaux dest] [@IP du prochain équipement]</i>
2	<i>R#ip route [@IP du réseaux dest] [masque du réseaux dest] [interface de sortie]</i>

Tapez donc les commandes suivantes dans chaque routeur pour configurer le routage statique.

Routeur R1

Ajout des routes en fonction de l'interface de sortie :

```

1 R1(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
2 R1(config)#ip route 192.168.1.0 255.255.255.0 s0/0/0
3 R1(config)#ip route 192.168.2.0 255.255.255.0 s0/0/0

```

Routeur R2

Ajout des routes en fonction de l'interface de sortie :

```

1 R2(config)#ip route 172.16.3.0 255.255.255.0 s0/0/0
2 R2(config)#ip route 192.168.2.0 255.255.255.0 s0/0/1

```

Routeur R3

Ajout des routes en fonction de l'adresse IP du prochain routeur :

```

1 R3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.2
2 R3(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.2
3 R3(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.2

```

7- Configuration du routage statique

La commande « #show IP route » permet de visualiser la table de routage.

- Les C indiquent que les réseaux sont directement connectés au routeur.
- Les S indiquent que ce sont des routes statiques, effectivement nous les avons entrées en dur avec les commandes ci-dessus.

Table de routage pour le routeur R1 :

```

1 R1#show ip route
172.16.0.0/24 is subnetted, 3 subnets
S    172.16.1.0 is directly connected, Serial0/0/0
C    172.16.2.0 is directly connected, Serial0/0/0
C    172.16.3.0 is directly connected, FastEthernet0/0
S   192.168.1.0/24 is directly connected, Serial0/0/0
S   192.168.2.0/24 is directly connected, Serial0/0/0

```

Table de routage pour le routeur R2 :

```

1 R2#show ip route
172.16.0.0/24 is subnetted, 3 subnets
C    172.16.1.0 is directly connected, FastEthernet0/0/0
C    172.16.2.0 is directly connected, Serial0/0/0
S    172.16.3.0 is directly connected, Serial0/0/0
C   192.168.1.0/24 is directly connected, Serial0/0/1
S   192.168.2.0/24 is directly connected, Serial0/0/1

```

Table de routage pour le routeur R3 :

```

1 R3#show ip route

```

```

172.16.0.0/24 is subnetted, 3 subnets
S   172.16.1.0 is directly connected, Serial0/0/1
S   172.16.2.0 is directly connected, Serial0/0/1
S   172.16.3.0 is directly connected, Serial0/0/1
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0

```

8- Vérification de la connectivité des périphériques

Dans cette partie nous allons vérifier la connectivité entre les équipements.

Nous effectuons des ping sur tout le réseau et nous constatons qu'ils sont tous ok.

Le tableau ci-dessous est un récapitulatif.

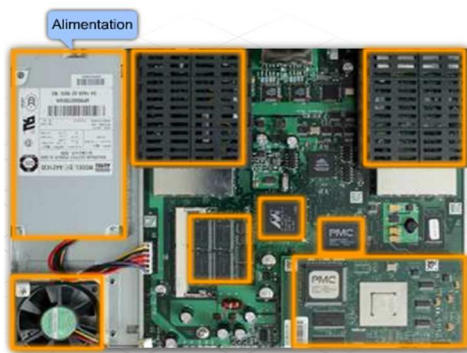
	FA 0/0 de R1	FA 0/0 de R2	FA 0/0 de R3	S 0/0/0 de R2	S 0/0/1 de R2	S 0/0/0 de R1	S0/0/1 de R3	PC1	PC2	PC3
R1	Black	Green	Green	Green	Green	Black	Green	Green	Green	Green
R2	Green	Black	Green	Black	Black	Green	Green	Green	Green	Green
R3	Green	Green	Black	Green	Green	Green	Green	Green	Green	Green
PC1	Green	Green	Green	Green	Green	Green	Green	Black	Green	Green
PC2	Green	Green	Green	Green	Green	Green	Green	Green	Black	Green
PC3	Green	Green	Green	Green	Green	Green	Green	Green	Green	Black

Matière : Réseaux informatiques

Annexe TP N° 3 : Routeur

I. Présentation du routeur :

Il existe plusieurs types et modèles de routeurs, chacun comporte, à la base, les mêmes composants matériels. Selon le modèle, ces composants se trouvent à différents emplacements dans le routeur. Pour voir les composants internes du routeur, vous devez dévisser et retirer son couvercle métallique. En général, il n'est pas nécessaire d'ouvrir le routeur, sauf pour mettre à niveau la mémoire.



Vue de l'intérieur du routeur



Vue de l'arrière du routeur

II. Processeur et mémoire du routeur :

Comme un PC, un routeur comprend également les éléments suivants :

- Unité centrale (UC)
- Mémoire vive (RAM)
- Mémoire morte (ROM)

a. UC :

L'UC exécute les instructions du système d'exploitation, telles que l'initialisation du système, des fonctions de routage et de commutation.

b. Mémoire vive :

La mémoire vive stocke les instructions et données requises pour exécution par l'UC. La mémoire vive est utilisée pour enregistrer ces composants :

- **Système d'exploitation** : le système IOS (Internetwork Operating System) de Cisco est copié dans la mémoire vive pendant l'amorçage.

- **Fichier de configuration en cours** : il s'agit du fichier de configuration qui enregistre les commandes de configuration actuellement utilisées par l'IOS du routeur. À de rares exceptions près, toutes les commandes configurées sur le routeur sont enregistrées dans le fichier de configuration en cours, appelé *running-config*.

- **Table de routage IP** : ce fichier stocke des informations sur les réseaux directement connectés et les réseaux distants. Il permet de déterminer le meilleur chemin pour le transfert du paquet.

- **Cache ARP** : ce cache contient les mappages d'adresses IPv4 et MAC, de manière similaire au cache ARP d'un PC. Le cache ARP est utilisé sur les routeurs dotés d'interfaces de réseau local, telles que les interfaces Ethernet.

- **Mémoire tampon de paquets** : les paquets sont stockés temporairement dans une mémoire tampon lors de leur réception sur une interface ou avant de quitter une interface.

La mémoire vive est une mémoire volatile : elle perd donc son contenu lorsque le routeur est mis hors tension ou redémarré. Cependant, le routeur contient également des zones de stockage permanent, comme la mémoire morte, flash et NVRAM.

c. Mémoire morte

La mémoire morte est une forme de stockage permanent. Les périphériques Cisco utilisent la mémoire morte pour enregistrer les éléments suivants :

- Instructions d'amorçage
- Logiciel de diagnostic de base
- Version réduite d'IOS

La mémoire morte utilise un *progiciel*, qui est un logiciel incorporé dans le circuit intégré. Le *progiciel* inclut les logiciels qui n'ont habituellement pas besoin d'être modifiés ou mis à niveau, les instructions d'amorçage par exemple. La mémoire morte ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

d. Mémoire flash

La mémoire flash est une mémoire non volatile pouvant être stockée et effacée électriquement. Elle sert de stockage permanent pour le système d'exploitation, Cisco IOS. Sur la plupart des modèles de routeurs Cisco, l'IOS est stocké de manière permanente dans la mémoire flash et copié dans la mémoire vive lors du processus d'amorçage, où il est ensuite exécuté par le processeur. Certains modèles plus anciens de routeurs Cisco exécutent l'IOS directement à partir de la mémoire flash. La mémoire flash se compose de barrettes SIMM ou de cartes PCMCIA, qui peuvent être mises à niveau pour en augmenter la capacité.

La mémoire flash ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

e. Mémoire vive non volatile

La mémoire vive non volatile ne perd pas les informations qu'elle contient lorsque le système est mis hors tension. Elle s'oppose aux formes les plus courantes de mémoire vive, telles que la mémoire vive dynamique (DRAM), qui nécessite une alimentation continue pour conserver les informations. La mémoire vive non volatile est utilisée par Cisco IOS comme stockage permanent pour le fichier de configuration initiale (startup-config). Toutes les modifications de configuration sont enregistrées dans le fichier de configuration en cours (running-config) dans la mémoire vive, et sont, à de rares exceptions près, immédiatement implémentées par l'IOS. Pour enregistrer ces modifications, au cas où le routeur serait redémarré ou mis hors tension, la configuration en cours doit être copiée dans la mémoire vive non volatile, où elle est enregistrée en tant que fichier de configuration initiale. La mémoire vive non volatile conserve son contenu, même si le routeur se recharge ou s'il est mis hors tension.

Il est plus important pour un professionnel des réseaux de comprendre la fonction des principaux composants internes d'un routeur que de connaître l'emplacement exact de ces composants dans un routeur donné. L'architecture physique interne diffère d'un modèle à l'autre.

III. Composants du routeur et leurs fonctions :

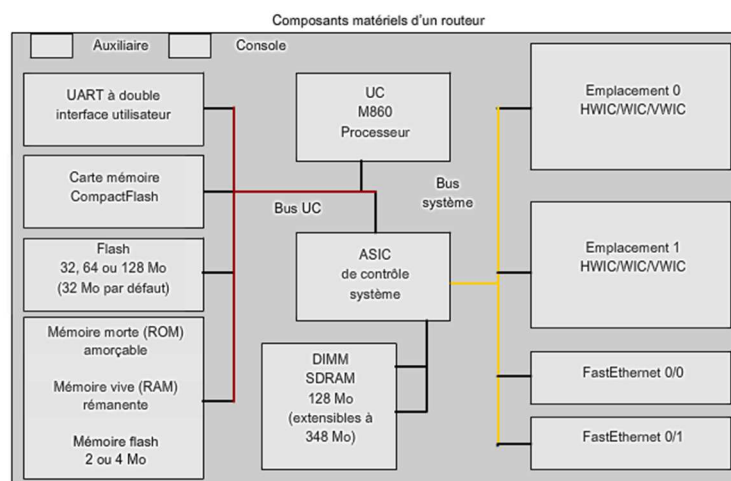


Schéma logique des composants internes d'un routeur Cisco 1841.
Surlignez chaque composant à l'aide du pointeur de la souris pour afficher la description correspondante.

Port auxiliaire : le port auxiliaire est un port de gestion qui permet de configurer le périphérique à distance. Il permet notamment de connecter un modem pour assurer la gestion des périphériques en cas de dysfonctionnement du chemin réseau. Les routeurs ne sont pas tous équipés d'un port auxiliaire.

Port console : le port de console permet de configurer localement le périphérique. Il s'agit d'un port de gestion, non conçu comme une mise en réseau.

UART (émetteur-récepteur asynchrone universel) à double interface utilisateur : UART (universal asynchronous receiver/transmitter) double interface, car il est accessible par deux moyens (le port auxiliaire et le port console).

Processeur : le processeur est le cerveau de l'ordinateur. C'est le processeur qui gère la plupart des opérations réalisées : il interprète les instructions des programmes informatiques et traite les données.

ASIC de Contrôle système : il contrôle les flux de données entre la mémoire. Les interfaces et le processeur.

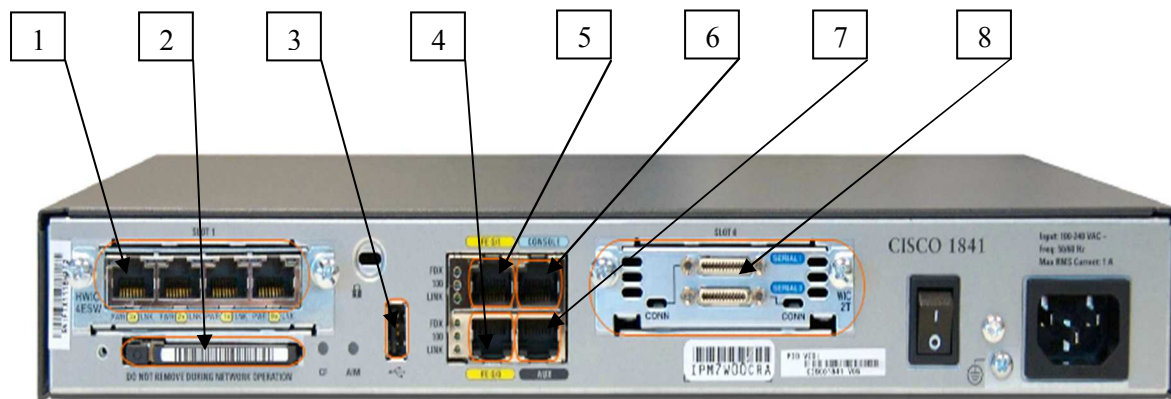
Mémoire Compact Flash et Flash : stocke l'image du logiciel Cisco IOS dans le module SIMM (Single In-line Memory Module, module de mémoire à connexion simple) flash ou dans la carte PCMCIA.

Mémoire ROM amorçable : stocke l'amorçable, le moniteur ROM et éventuellement une version simplifiée du logiciel IOS. Partage la mémoire vive RAM rémanente.

Mémoire vive rémanente (NVRAM) : stocke la configuration initiale et partage la mémoire flash avec la mémoire ROM amorçable.

DIMM SDRAM : il stocke la configuration en cours, la table de routage et les autres structures dynamiques.

Les différentes interfaces et ports du routeur est décrits dans la figure suivante :



1- Carte d'interface WAN haut débit (HWIC) à détection automatique Cisco EtherSwitch 10BASE-T/100BASE-TX 4 ports

2- Module Compact Flash

3- Port USB à logement unique

4- Port Fast Ethernet 0/1

5- Port Fast Ethernet 0/0

6- Port de console

7- Port auxiliaire

8- Logements de carte d'interface WAN haut débit (HWIC)

IV. Processus d'amorçage du routeur :

Le processus d'amorçage comporte quatre phases principales :

- Test automatique de mise sous tension (POST)
- Chargement du programme d'amorçage
- Localisation et chargement du logiciel Cisco IOS
- Localisation et chargement du fichier de configuration initiale ou passage en mode Configuration

a. Test automatique de mise sous tension (POST)

Le Power-On Self Test (POST) est un processus commun se produisant sur pratiquement tout ordinateur à l'amorçage. Le processus POST est utilisé pour tester le matériel du routeur. Lorsque le routeur est mis sous tension, le logiciel présent sur la puce de mémoire morte effectue le POST. Au cours de ce test automatique, le routeur exécute des diagnostics à partir de la mémoire morte sur plusieurs composants matériels, notamment le processeur, la mémoire vive et la mémoire vive non volatile.

b. Chargement du programme d'amorçage

Après le POST, le programme d'amorçage est copié de la mémoire morte à la mémoire vive. Ensuite, le processeur exécute les instructions du programme d'amorçage. Le rôle principal du programme d'amorçage est de localiser Cisco IOS et de le charger dans la mémoire vive.

Remarque : à ce stade, si vous disposez d'une connexion console au routeur, vous commencez à voir la sortie sur l'écran.

c. Localisation et chargement du logiciel Cisco IOS

L'IOS est généralement stocké dans la mémoire flash, mais il peut également l'être à d'autres endroits, sur le serveur TFTP (Trivial File Transfer Protocol) par exemple.

S'il est impossible de localiser une image IOS entière, une version réduite de l'IOS est copiée de la mémoire morte à la mémoire vive. Cette version de l'IOS permet de diagnostiquer tout problème et peut être utilisée pour charger une version complète de l'IOS sur la mémoire vive.

Remarque :

- le serveur TFTP sert généralement de serveur de sauvegarde de l'IOS, mais il peut également servir de point central pour le stockage et le chargement de l'IOS.
- une fois le chargement de l'IOS lancé, une suite de signes dièse (#) peut s'afficher, lors de la décompression de l'image.

d. Localisation et chargement du fichier de configuration

Une fois l'IOS chargé, le programme d'amorçage recherche dans la mémoire vive non volatile le fichier de configuration initiale, appelé startup-config. Ce fichier contient les commandes et paramètres de configuration précédemment enregistrés, notamment : les adresses d'interface ; les informations de routage ; les mots de passe ; toute autre configuration enregistrée par l'administrateur réseau.

Si le fichier de configuration initiale, startup-config, se trouve dans la mémoire vive non volatile, il est copié dans la mémoire vive en tant que fichier de configuration en cours (running-config).

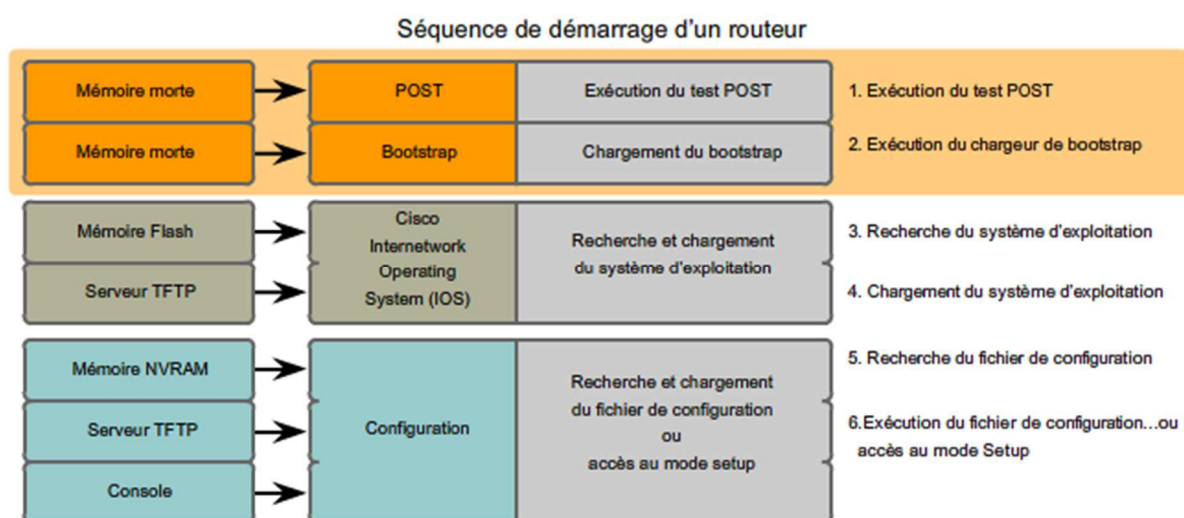
Exécution du fichier de configuration. Si un fichier de configuration initiale est trouvé dans la mémoire vive non volatile, l'IOS le charge dans la mémoire vive en tant que fichier *running-config* et exécute les commandes dans le fichier, ligne par ligne. Le fichier de configuration en cours contient des adresses d'interface, lance les processus de routage, configure les mots de passe du routeur et définit d'autres caractéristiques du routeur.

Passage en mode Configuration (facultatif). S'il est impossible de localiser le fichier de configuration initiale, le routeur invite l'utilisateur à passer en mode Assistant de configuration. Le mode Assistant de configuration est une série de questions invitant l'utilisateur à entrer des informations de configuration élémentaires. Ce mode n'est pas destiné à être utilisé pour effectuer des configurations de routeur complexes et n'est généralement pas utilisé par les administrateurs réseaux.

Lorsque vous amorcez un routeur ne contenant pas de fichier de configuration initiale, la question suivante apparaît après le chargement de l'IOS :

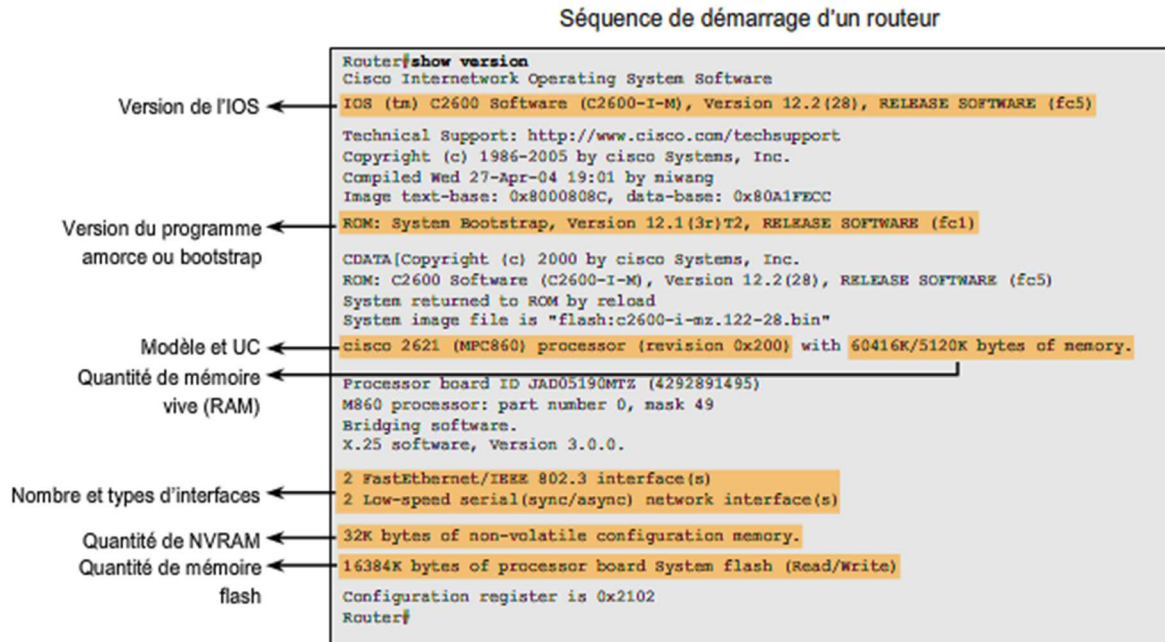
Would you like to enter the initial configuration dialog? [yes/no]: no

Le mode Assistant de configuration n'est pas utilisé pour configurer le routeur. Lorsque vous êtes invité à passer en mode Assistant de configuration, répondez toujours no. Si vous répondez yes et passez au mode Assistant de configuration, vous pouvez appuyer à tout moment sur la combinaison de touches Ctrl+C pour mettre fin au processus de configuration.



V. Vérification du processus d'amorçage du routeur

La commande show version affiche des informations sur la version du logiciel Cisco IOS active sur le routeur, la version du programme d'amorçage, ainsi que des informations sur la configuration matérielle, comme la quantité de mémoire système comme montre la figure suivante.



VI. Configuration de routeur de base

Lors de la configuration d'un routeur, certaines tâches de base sont effectuées :

- Attribution d'un nom au routeur
- Définition de mots de passe
- Configuration d'interfaces
- Configuration d'une bannière
- Enregistrement des modifications apportées à un routeur
- Vérification de la configuration de base et des opérations de routage

La première invite apparaît en mode Utilisateur. Le mode Utilisateur vous permet de voir l'état du routeur, mais pas de modifier sa configuration. Ne confondez pas le terme « utilisateur » faisant référence au mode Utilisateur et les utilisateurs du réseau. Le mode Utilisateur est destiné aux techniciens, opérateurs et ingénieurs réseau chargés de configurer les périphériques.

Router>

La commande enable permet de passer en mode d'exécution privilégié. Ce mode permet à l'utilisateur de modifier la configuration du routeur. L'invite affichée par le routeur (>) devient # dans ce mode.

Router>enable

Router#

a. Noms d'hôte et mots de passe

La figure indique la syntaxe de base de la commande de configuration de routeur utilisée pour configurer R1.

Passez tout d'abord en mode de configuration globale.

```
Router#config t
```

Appliquez ensuite un nom d'hôte unique au routeur.

```
Router(config)#hostname R1
```

```
R1(config)#
```

Configurez alors un mot de passe à utiliser pour passer en mode d'exécution privilégié.

```
Router(config)#enable secret motde passe
```

Configurez ensuite les lignes de console et Telnet avec le mot de passe. La commande login permet de vérifier le mot de passe sur la ligne. Si vous n'entrez pas la commande login sur la ligne de console, l'utilisateur pourra accéder à cette ligne sans entrer de mot de passe.

```
R1(config)#line console 0
```

```
R1(config-line)#password motde passe
```

```
R1(config-line)#login
```

```
R1(config-line)#exit
```

```
R1(config)#line vty 0 4
```

```
R1(config-line)#password motde passe
```

```
R1(config-line)#login
```

```
R1(config-line)#exit
```

b. Configuration d'une bannière

En mode de configuration globale, configurez la bannière du message du jour (motd). Un séparateur, un « # » par exemple, est utilisé au début et à la fin du message. Le séparateur vous permet de configurer une bannière sur plusieurs lignes, comme illustré ici.

```
R1(config)#banner motd #
```

```
Enter TEXT message. End with the character '#'.  
*****
```

```
WARNING!! Unauthorized Access Prohibited!!  
*****
```

```
#
```

La configuration d'une bannière appropriée assure l'efficacité d'un plan de sécurité. Une bannière doit au moins mettre en garde contre les accès non autorisés. Ne configurez jamais une bannière qui « accueille » un utilisateur non autorisé.

Configuration des paramètres de base d'un routeur

Syntaxe des commandes de configuration des paramètres de base d'un routeur	
Attribution d'un nom au routeur	<code>Router(config)#hostname name</code>
Définition des mots de passe	<code>Router(config)#enable secret password</code>
	<code>Router(config)#line console 0</code>
	<code>Router(config-line)#password password</code>
	<code>Router(config-line)#login</code>
	<code>Router(config)#line vty 0 4</code>
	<code>Router(config-line)#password password</code>
	<code>Router(config-line)#login</code>
Configuration d'une bannière de message du jour	<code>Router(config)#banner motd # message #</code>

VII. Configuration des interfaces du routeur

Vous allez maintenant configurer les différentes interfaces du routeur à l'aide des adresses IP et d'autres informations. D'abord, passez au mode de configuration d'interface en indiquant le type et le numéro d'interface. Configurez ensuite l'adresse IP et le masque de sous-réseau :

```
RI(config)#interface Serial0/0
```

```
RI(config-if)#ip address 192.168.2.1 255.255.255.0
```

Il est conseillé de configurer une description sur chaque interface pour mieux documenter les informations du réseau. Le texte de description est limité à 240 caractères. Sur les réseaux de production, une description peut être utile en matière de dépannage, puisqu'elle fournit des informations sur le type de réseau auquel l'interface se connecte et indique la présence éventuelle d'autres routeurs sur ce réseau.

```
Router(config-if)#description Circuit#VBN32696-123 (help desk:1-800-555-1234)
```

Une fois l'adresse IP et la description configurées, l'interface doit être activée à l'aide de la commande `no shutdown`. Cela revient à mettre l'interface sous tension. L'interface doit également être connectée à un autre périphérique (concentrateur, commutateur, autre routeur, etc.) pour que la couche physique soit active.

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

Remarque : lorsque vous câblez une liaison série point à point, une extrémité du câble est marquée ETTD et l'autre DCE. Le routeur dont l'interface série est connectée à l'extrémité DCE du câble nécessite également que la commande clock rate (fréquence d'horloge) soit configurée sur cette interface série.

R1(config-if)#clock rate 64000

Appliquez les commandes de configuration d'interface à toutes les autres interfaces à configurer. Dans notre exemple de topologie, l'interface FastEthernet doit être configurée.

R1(config)#interface FastEthernet0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#description R1 LAN

R1(config-if)#no shutdown

Syntaxe des commandes de configuration des paramètres de base d'un routeur	
Configuration d'une interface	Router (config) # interface type number
	Router (config-if) # ip address address mask
	Router (config-if) # description description
	Router (config-if) # no shutdown
Enregistrement des modifications apportées à un routeur	Router # copy running-config startup-config
Vérification des informations renvoyées par les commandes show	Router # show running-config
	Router # show ip route
	Router # show ip interface brief
	Router # show interfaces

VIII. Vérification de la configuration de routeur de base

À ce stade, toutes les précédentes commandes de configuration de routeur de base ont été entrées et immédiatement stockées dans le fichier de configuration en cours de R1. Le fichier de configuration en cours est stocké dans la mémoire vive. Ce fichier de configuration est utilisé par l'IOS. L'étape suivante consiste à vérifier les commandes entrées, en affichant la configuration en cours à l'aide de la commande suivante :

R1#show running-config

Maintenant que les commandes de configuration de base ont été entrées, il est important d'enregistrer la configuration en cours dans la mémoire vive non volatile, la mémoire NVRAM du routeur. Ainsi, en cas de panne de courant ou de rechargement accidentel, le routeur peut s'amorcer

avec la configuration en cours. Une fois la configuration du routeur effectuée et testée, il est important d'enregistrer la configuration en cours comme configuration initiale, pour qu'elle serve de configuration permanente.

R1#copy running-config startup-config

Une fois la configuration de base appliquée et enregistrée, vous pouvez utiliser plusieurs commandes pour vérifier que vous avez correctement configuré le routeur.

R1#show running-config

Cette commande affiche la configuration en cours stockée dans la mémoire vive. À de rares exceptions près, toutes les commandes de configuration qui ont été utilisées sont entrées dans le fichier de configuration en cours et immédiatement implémentées par l'IOS.

Cette commande affiche le fichier de configuration initiale stocké dans la mémoire vive non volatile. C'est la configuration que le routeur utilise au prochain amorçage. Cette configuration ne change pas, sauf si la configuration en cours est enregistrée dans la mémoire vive non volatile à l'aide de la commande *copy running-config startup-config*.

R1#show ip route

Cette commande affiche la table de routage actuellement utilisée par l'IOS pour choisir le meilleur chemin à emprunter afin d'atteindre les réseaux de destination. À ce stade, R1 n'a de routes que pour ses réseaux directement connectés via ses propres interfaces.

R1#show interfaces

Cette commande affiche tous les paramètres et toutes les statistiques de configuration d'interface.

R1#show ip interface brief

Cette commande affiche des informations sommaires sur la configuration d'interface, notamment l'adresse IP et l'état de l'interface. Il s'agit d'un outil utile de dépannage et d'un moyen rapide de déterminer l'état de toutes les interfaces du routeur.

Matière : Réseaux informatiques TP N° 4 : Routage dynamique

I. Objectifs

Dans le TP précédant, nous avons vu le principe du routage statique et comment le mettre en place dans un réseau afin de faire communiquer tous les équipements de celui-ci.

Dans ce TP, nous allons nous intéresser au routage dynamique en utilisant le protocole RIP.

Déroulement du TP

Vous devrez rédiger un compte-rendu, qui contiendra les réponses aux différentes questions, les commandes tapées, les captures d'écran de Packet Tracer ainsi que vos explications et commentaires.

Prérequis

Pour réaliser ce TP, vous devez réviser le chapitre 5 portant sur la couche réseau. Vous devez aussi avoir fait le TP « Routage statique » et connaître toutes les commandes de base pour la configuration des routeurs Cisco (consulter l'annexe du TP3 « Présentation générale des routeurs Cisco »).

II. Principe du routage dynamique

Lorsqu'un réseau atteint une taille assez importante, il devient contraignant de devoir ajouter les routes « à la main » dans les tables de routage. Il faut alors utiliser le routage dynamique qui permet de mettre à jour automatiquement les entrées dans les différentes tables de routage, donc de façon dynamique.

1- Protocole de routage

Un protocole de routage est un système de communication utilisé entre les routeurs. Le protocole de routage permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur leur proximité avec d'autres routeurs. Les informations qu'un routeur reçoit d'un autre routeur, à l'aide d'un protocole de routage, servent à construire et à mettre à jour une table de routage.

Exemples de protocole de routage :

- Protocole à vecteur de distance : RIP.
- Protocole à état de liens : OSPF (Open Shortest Path First).

2- Le protocole de routage RIP

Le protocole de RIP (Routing Information Protocol) est certainement le protocole de routage dynamique le plus répandu de nos jours. Ce protocole de type Vecteur de

Distances, est basé sur un jeu d'algorithmes qui consiste à comparer mathématiquement des itinéraires permettant ainsi d'identifier la meilleure route d'un point de départ A à une destination précise B.

Ses principales caractéristiques sont les suivantes:

- Il s'agit d'un protocole de routage à vecteur de distance.
- Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

Il existe deux versions du protocole RIP (RIPv1 et RIPv2). La deuxième version, développée en 1993, a été conçue pour permettre au protocole de répondre aux contraintes des réseaux actuels notamment en ce qui concerne le découpage des réseaux IP en sous-réseaux (chose qui était impossible avec la version 1).

Dans ce TP, nous utiliserons le protocole RIPv2 pour configurer le routage dynamique des différents routeurs.

III. Travail à réaliser

1- Etude du réseau et découpage en sous-réseaux

Afin de comprendre en détail le protocole RIP, on se propose d'étudier le problème suivant :

Vous êtes recrutés en tant qu'administrateur réseau dans une entreprise exerçant dans le secteur des énergies renouvelables. L'entreprise en question est structurée en 05 départements réparties sur 03 bâtiments distants de 80 mètres, deux bâtiments disposent de deux étages avec deux départements chacun, et un autre bâtiment dispose d'un département seulement.

Les départements sont :

1. **Département Fabrication** : *Bâtiment 1, 1^{ère} étage* : ce département rassemble l'unité de fabrication des panneaux photovoltaïque, le stockage ... est composé de 80 PC.
2. **Département Transport** : *Bâtiment 1, 2^{ème} étage* : 20 PC pour la gestion de transport.
3. **Département Commande** : *Bâtiment 2* : 50 ordinateurs de gestion des commandes.
4. **Département Administration** : *Bâtiment 3, 1^{ère} étage* : 22 PC administratifs : direction, compatibilité, ...
5. **Département Commercial** : *Bâtiment 3, 2^{ème} étage* : 10 commerciaux et les services.

La première tâche par laquelle vous voulez commencer est la réorganisation de l'adressage IP du réseau de l'entreprise. En tant qu'administrateur réseau, vous avez choisi de découper le réseau pour refléter la structure de la société, c'est-à-dire de créer autant de sous-réseaux que de départements. Vous avez donc prévu 05 sous-réseaux, numérotés de 1 à 5. Les adresses IP que vous allez attribuer sont des adresses privées. **L'adresse du réseau globale de l'entreprise est : 172.19.0.0 /16**

1. Combien de bits supplémentaires sont nécessaires pour définir cinq sous-réseaux ?
2. Calculer le nombre de sous-réseaux potentiels et le nombre maximum de machines par sous-réseau.

nombre de sous-réseaux potentiels	
nombre maximum de machines par réseau	

3. Quel est le masque sous-réseau qui permet la création de ces cinq sous-réseaux ?
4. Définir les adresses de chaque sous-réseau, et calculer les adresses des premières et dernières machines configurées dans chacun des sous-réseaux. Remplissez le tableau suivant :

Département	Adresse de sous-réseau	Masque de sous-réseau	Adresse de la première machine	Adresse de la dernière machine
Fabrication (sous-réseau numéro 1)				
Transport (sous-réseau numéro 2)				
Commande (sous-réseau numéro 3)				
Administration (sous-réseau numéro 4)				
Commercial (sous-réseau numéro 5)				

5. Quelle est l'adresse de diffusion (broadcast) du sous-réseau numéro 4 (Administration) ?

2- Simulation du réseau obtenu avec Packet Tracer

Dans cette étape, vous allez simuler à l'aide de Packet Tracer le réseau obtenu après le découpage en sous-réseaux en supposant que vous disposez de trois routeurs pour configurer votre réseau :

- Le premier routeur (R1) installé au niveau du bâtiment 1 permet de connecter les sous-réseaux numéro 1 et 2 (départements Fabrication et Transport).
- Le deuxième routeur (R2) installé au niveau du bâtiment 2 permet de connecter le sous-réseau numéro 3 (département Commande).
- Le troisième routeur (R3) installé au niveau du bâtiment 3 permet de connecter les sous-réseaux numéro 4 et 5 (départements Administration et Commercial).
- Vous reliez à l'aide d'un câble série l'interface Serial0/0/0 du routeur R1 à l'interface Serial0/0/0 du routeur R2 à travers le réseau 192.168.12.0 /24

- Vous reliez à l'aide d'un câble série l'interface Serial0/0/1 du routeur R2 à l'interface Serial0/0/1 du routeur R3 à travers le réseau 192.168.23.0 /24

Avec Packet Tracer, schématiser l'installation réseau en se référant au TP précédent (TP3) :

- Ajouter les équipements réseau utilisés (switchs, routeurs, PCs),
- Ajoutez aux routeurs les modules nécessaires.
- Liaisons série et ethernet, câbles droits ou croisés,...
- **Ajoutez qu'une seule machine par sous-réseau.**
- Attribuez ensuite les adresses IP aux différentes interfaces selon le schéma obtenu.
- Activer toutes les interfaces utilisées.

3- Mise en place du routage RIP

La configuration du protocole est très facile car il n'y a que trois commandes à taper.

- ✓ Activation du protocole RIP dans le routeur avec la commande suivante en mode configuration :

```
R(config)#router rip
```

- ✓ Préciser la version du protocole RIP à utiliser (version 2 dans notre cas) :

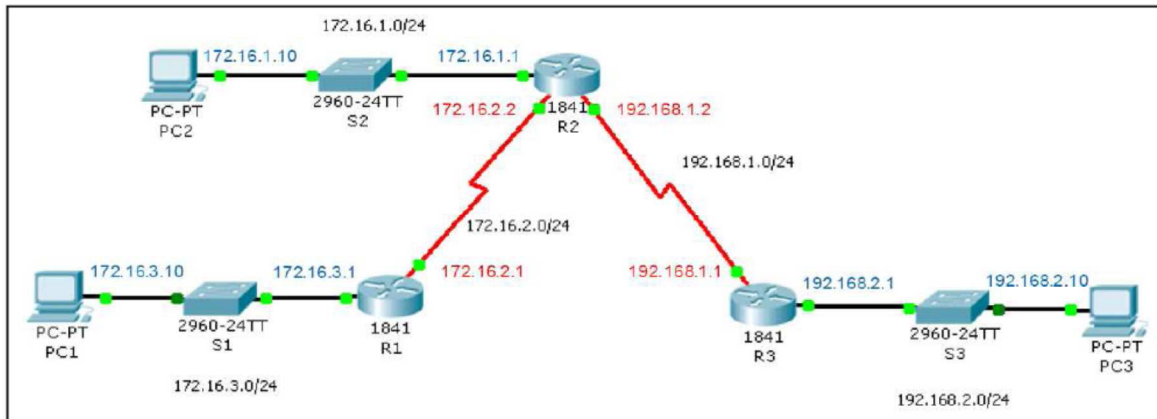
```
R(config-router)#version 2
```

- ✓ Définition des réseaux directement connectés à ce routeur (réseaux que vous voulez router). Le masque de sous-réseau a été défini lors de la configuration des interfaces, donc inutile de le définir une seconde fois.

```
R(config-router)#network [@réseau]
```

Vous remarquez que nous n'avons pas défini le masque sous-réseau dans la dernière commande. Le masque de sous-réseau a été défini lors de la configuration des interfaces, donc inutile de le définir une seconde fois.

Exemple



Supposant que nous voulons configurer RIP sur le routeur R2. Les réseaux qui sont directement connectés au routeur R2 sont : 172.16.1.0 /24, 172.16.2.0 /24 et 192.168.1.0 /24. Par conséquent, nous tapons les commandes suivantes:

```
1 R2(config)#router rip
2 R2(config-router)#version 2
3 R2(config-router)#network 172.16.1.0
4 R2(config-router)#network 172.16.2.0
5 R2(config-router)#network 192.168.1.0
6 R2(config-router)#exit
```

C'est tout en ce qui concerne la configuration du protocole RIP. Nous ferons le test pour s'assurer que le routage est opérationnel.

4- Tests et vérification de la connectivité

A présent essayons de tester la communication entre différentes machines: lancez un **ping** entre les différentes machines. Le résultat doit être positif si vous n'êtes pas trompés dans la configuration.

Affichez ensuite la table de routage de chaque routeur grâce à la commande "**show ip route**" et analysez les différentes informations s'y trouvant.

Souvenez-vous lorsque nous avons travaillé sur le routage statique (TP3), nous avons vu qu'il y'avait deux lettres utilisées pour décrire chaque route. Il s'agit de la lettre C (placée devant chaque réseau directement connecté au routeur concerné) et la lettre S (placée sur une route statique).

Dans le cas présent, nous aurons presque la même chose, à la différence qu'au lieu d'une route statique, on aura une route configurée selon le protocole RIP et par conséquent la lettre R sera placée devant la ligne. Pour les autres réseaux directement connectés au Routeur, on utilise toujours la lettre C.

Tapez la commande suivante en mode privilégié dans chaque routeur :

```
R#show ip route
```

Comme vous le constatez, les informations contenues dans la table sont en adéquation avec le schéma sur lequel vous avez travaillé.

Matière : Réseaux informatiques

TP N° 5 : Protocoles des couches transport et application

I. Objectifs

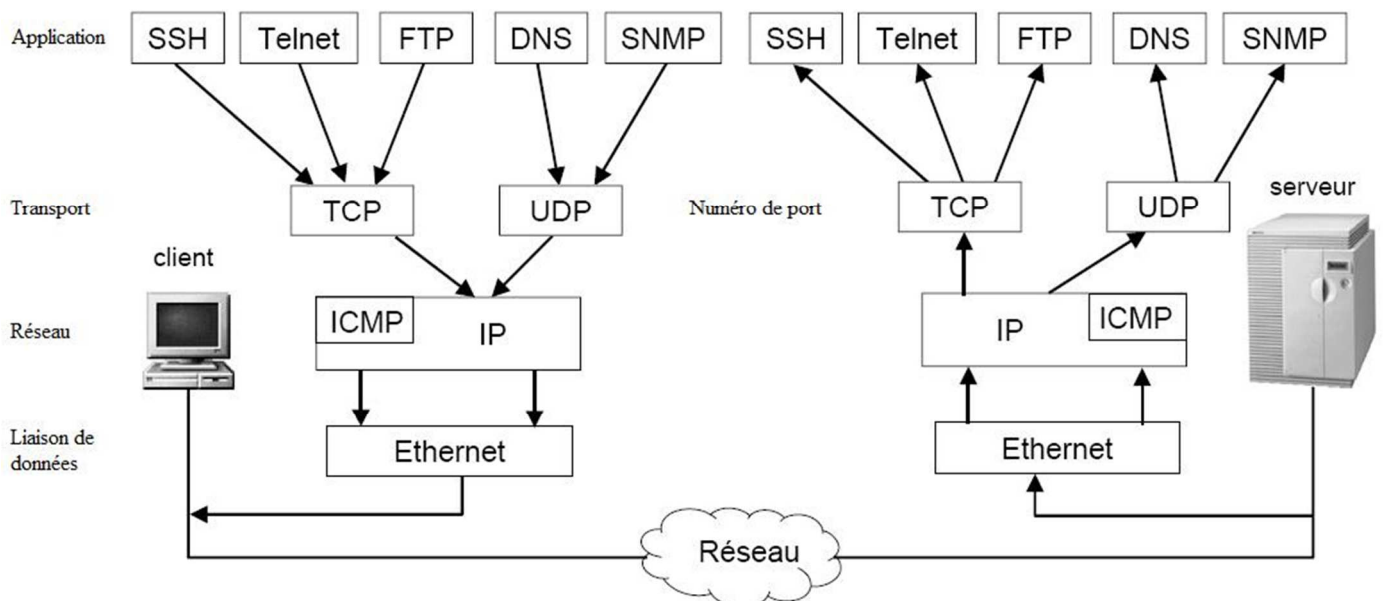
L'objectif de ce TP est de comprendre le fonctionnement des deux principaux protocoles de la couche transport, à savoir UDP et TCP à travers l'étude de deux protocoles applicatifs qui sont : DNS et Telnet.

II. Définitions

1- Notion de port

Plusieurs applications peuvent s'exécuter sur une machine cliente ou une machine serveur. Chacune d'entre elles utilise les services de la couche transport UDP ou TCP et est identifiée par un **numéro de port**. Un port est représenté par un entier (sur 16 bits).

- les ports de 0 à 1023 sont les ports **reconnus** ou **réservés**. Ils sont assignés par l'IANA (*Internet Assigned Numbers Authority*) et donnent accès aux services standards : serveur web (HTTP port 80), transfert de fichier (FTP port 21) courrier ou mail (SMTP port 25 et POP3 port 110), système de noms de domaine (DNS port 53), TELNET port 23, SSH port 22 ...
- les ports > 1024 sont les ports « **utilisateurs** » disponibles pour placer un service applicatif quelconque.

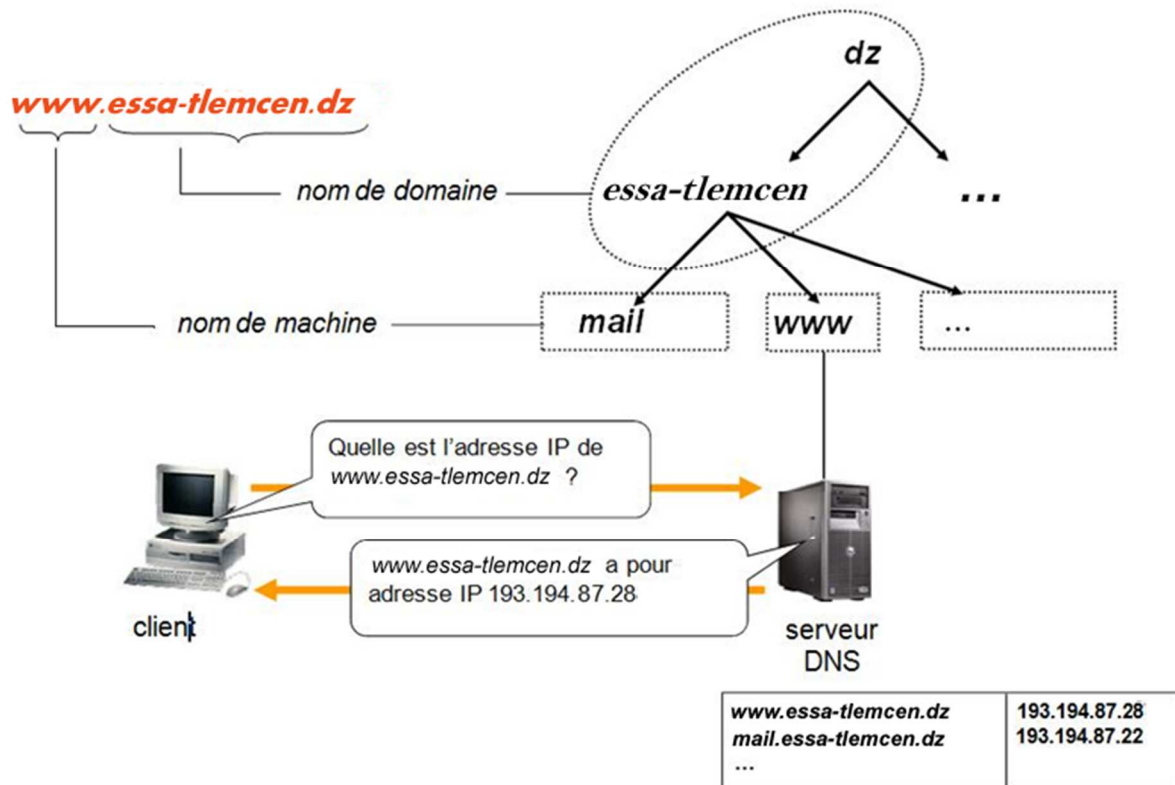


2- Le système DNS

Le système DNS (Domain Name System) permet d'associer des noms symboliques à des adresses numériques, en général des adresses IP. Les noms symboliques sont structurés et hiérarchiques :

- une partie désigne le **nom de la machine** (hostname)
- l'autre partie désigne le **nom de domaine** (domain name) auquel la machine appartient.

Dans chaque domaine, un serveur de noms ou serveur DNS est chargé de répondre aux requêtes des clients (les clients internes comme les clients externes au domaine).



3- Le protocole Telnet

Telnet est un protocole permettant à un ordinateur de se connecter à distance à un autre ordinateur, via l'Internet, en mode caractère uniquement. Dès que la connexion est établie, tout se passe comme si l'utilisateur Telnet se trouvait aux commandes de l'ordinateur distant; il peut alors utiliser le langage de commande disponible sur l'hôte distant et lancer l'exécution de programmes qui s'exécuteront sur cet hôte.

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet. Il fournit ainsi un système orienté connexion, bi-directionnel, codé sur 8 bits facile à mettre en œuvre. La connexion des clients aura lieu généralement sur le port TCP numéro 23 du serveur Telnet.

III. Travail à réaliser

Pour mieux comprendre le fonctionnement des protocoles TCP et UDP à travers l'étude des protocoles applicatifs, le trafic réseau de chacune de ces applications sera capturé et analysé avec l'outil Wireshark (que nous avons déjà utilisé dans le TP2).

1- Analyse d'UDP à travers le protocole DNS (*Domain Name System*)

- Le service DNS permet d'utiliser des noms symboliques pour accéder aux hôtes au lieu de leurs adresses IP.
- Il s'agit d'une sorte d'annuaire fonctionnant sur le principe requête/réponse et s'appuyant sur le protocole de transport UDP.
- Le serveur écoute les requêtes des clients sur le port 53.

1. Sur votre machine, capturez à l'aide de Wireshark les paquets UDP correspondant à une requête/réponse DNS, en utilisant le filtre de capture:

ip proto \udp and port domain

2. Une fois la capture démarrée, utilisez un navigateur web pour consulter le site web de l'epst tlemcen : <http://www.essa-tlemcen.dz>
3. Etudiez les différents champs de l'entête UDP.
4. Etudiez les requêtes et réponses DNS encapsulées :
Quelle est l'adresse IP de www.essa-tlemcen.dz ?
Quelle est la machine qui a répondu ? Quelle est son adresse IP ?

2- Analyse de TCP à travers le protocole Telnet (*TERminal NETwork emulation*)

- Telnet est utilisé pour émuler une connexion de terminal à un hôte distant.
- Il utilise TCP comme protocole de transport afin de transmettre les données entre l'utilisateur et l'hôte distant.
- Le serveur écoute sur le port 23.
- Analysez les segments TCP échangés dans un dialogue Telnet lorsque vous vous connectez sur un serveur distant.

1. Utilisez comme filtre de capture : ***ip proto \tcp and port telnet***
2. Depuis votre machine, lancez la capture et tapez la commande : ***telnet 192.168.1.1***
Avec *192.168.1.1*, l'adresse IP du serveur Telnet installé au niveau du laboratoire.
3. Entrez le nom de login et le mot de passe appropriés, puis une fois connecté, arrêtez la capture.
4. Etudiez les ports source et destination des différents segments TCP échangés.
5. Décodez l'ensemble du dialogue Telnet entre votre poste et le serveur, en cliquant sur la première trame capturée, puis en sélectionnant le menu « Analyser » puis l'item « Suivre Flux TCP ». Que constatez-vous ?