REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
الجمهورية الجزائرية الديمقراطية الشعبية

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE SUPERIEUREEN EN SCIENCES APPLIQUEES
--T L E M C E N--

وزارة التعليم العالي والبحث العلمي

المدرسة العليا في العلوم التطبيقية
-تلمسان-

Département de la formation du Second Cycle

Polycopié des Travaux Pratiques

Réseaux et protocoles

Elaboré par

Dr BRAHAMI Mustapha Anwar

Dr MEGNAFI Hicham

Table des matières

Table des Figures

Préface

Ce polycopié de travaux pratiques (TP) regroupe un certain nombre d'énoncés autour des réseaux informatiques. Il est destiné à consolider et mettre en pratique les connaissances et les notions apprises dans le cours « Réseaux et protocoles » pour les élèves ingénieurs du second cycle. Ces TPs sont effectués à l'Ecole Supérieure en Sciences Appliquées de Tlemcen (ESSAT) depuis 2016 jusqu'à ce jour.

L'objectif principal de ce polycopié consiste à mettre à la disposition des étudiants une brochure de manipulation avec des explications détaillées pour servir et faciliter la mise en pratique des différentes activités abordées durant les séances de TP. Chaque étudiant doit remettre un compte-rendu après avoir réalisé toutes les activités demandées. Le rapport doit comprendre les réponses aux questions, les captures d'écran de la simulation ainsi que les explications et les commentaires sur chaque résultat trouvé.

Les travaux pratiques proposés nécessitent des connaissances de base en ce qui concerne l'outil informatique, l'architecture des systèmes informatiques et les systèmes de communication (Cours Informatique 1 et 2 des classes préparatoires). Par ailleurs, les TPs sont à effectuer dans les conditions des laboratoires d'informatique de l'ESSAT (équipés de 20 PC connectés en réseau), où chaque étudiant dispose d'un PC sous Windows 7 en dual boot avec Linux CentOS 7.3, doté d'une interface Ethernet, et équipé des différents logiciels nécessaires (Wireshark et Packet Tracer).

Le présent polycopié comprend cinq TP au total. Le premier TP est consacré à l'installation et la configuration d'un réseau local sous les deux systèmes d'exploitation Windows et Linux. Le deuxième TP consiste à utiliser l'analyseur de paquets Wireshark, d'une part, pour examiner les champs d'une trame Ethernet II et, d'autre part, pour capturer et analyser les échanges ARP entre les périphériques réseau. Le troisième TP est dédié à la configuration des routeurs Cisco afin de mettre en œuvre le routage statique permettant de faire communiquer différentes stations de travail sur des réseaux distants. Le quatrième TP s'intéresse au routage dynamique à travers l'utilisation du protocole de routage dynamique RIPv2. Enfin, le

cinquième et dernier TP décrit en détail 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.

TP N° 1

Installation et configuration d'un réseau local sous Windows/Linux

1.1 Objectifs

- Réaliser et tester des câbles réseau à paires torsadées que ce soit de type droit ou de type croisé.

- Configurer les interfaces réseau de façon à établir une communication entre deux ou plusieurs ordinateurs.

- Utiliser des commandes MS-DOS et Linux pour tester le fonctionnement du réseau.

1.2 Introduction

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 une 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) [1].

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

1.3 Travail à réaliser

Dans ce TP, nous allons d'abord vérifier le réseau informatique du laboratoire dans lequel nous travaillons, nous installons ensuite un réseau local entre deux ou plusieurs ordinateurs en suivant le protocole TCP/IP.

1.3.1 Le matériel utilisé

- Câble à paires torsadées de type UTP.

- Connecteurs RJ-45.
- Une pince à sertir RJ-45.
- Un testeur de câble Ethernet.
- Ordinateur avec deux systèmes d'exploitation installés (Windows et Linux).
- Carte réseau Ethernet 10/100 Mbit/s bien installée.

1.3.2 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- Suivez les câbles de liaison du réseau informatique puis représentez (sous forme dessinée) les différents équipements utilisés sur ce réseau (les câbles, le switch, …).

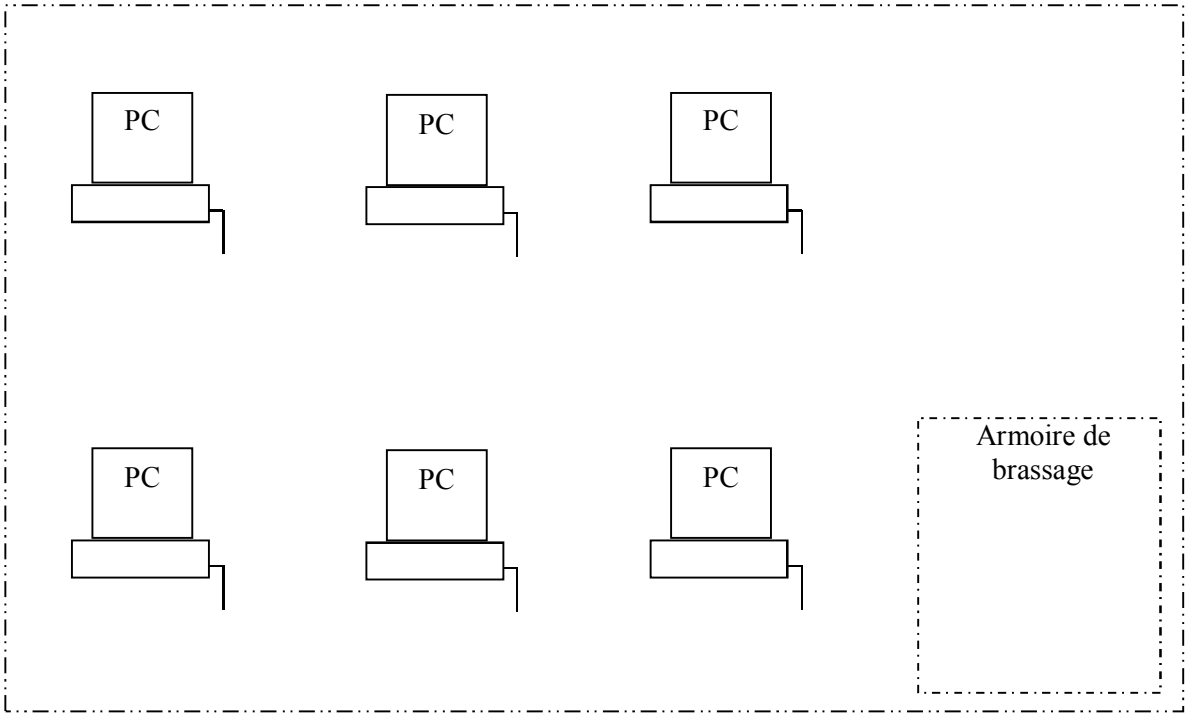


Figure 1.1 Norme de câblage T568A

1.3.3 Câblage physique d'un ordinateur au réseau

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

. . . . . .

. . . . . .

. . . . . .

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

NB: Chaque binôme travaille sur un tronçon de câble à paire torsadées (droit ou croisé), et chaque étudiant réalise une des 2 extrémités.

Tableau 1.1 Norme de câblage T568A

Côté 1 : Câble droit ou croisé			Côté 2 : Câble droit			Côté 2 : Câble croisé		
R/T	*Fils*	*Couleurs*	*R/T*	*Fils*	*Couleurs*	*R/T*	*Fils*	*Couleurs*
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

Pour fabriquer un câble RJ45, vous devez suivre, scrupuleusement, les étapes suivantes [2]:

- Coupez une section de câble à la longueur désirée. Les longueurs de câble à paires torsadées standard sont généralement de 0,6 m, 1,83 m ou 3,05 m. Dans ce TP, nous allons réaliser des câbles de 2 m.
- À l'aide d'une pince à dénuder, enlevez environ 3 cm de gaine à chaque extrémité du câble.

- Détorsadez une petite longueur des paires et placez-les dans l'ordre exact requis par la norme de câblage T568A (Tableau 1.1). Il est très important de détorsader le moins possible, car les torsades jouent un rôle d'étouffement du bruit.
- Redressez et aplatissez les fils entre le pouce et l'index. Assurez-vous que les fils sont toujours dans le bon ordre par rapport à la norme.
- Puis coupez-les droit à 1,25 cm minimum et 1,9 cm maximum du bord de la gaine. Si vous coupez le câble plus long, vous risquez de créer des interférences.
- Insérez les fils à fond dans le connecteur RJ-45. **Le fût (le petit levier en plastique du connecteur RJ-45) doit être dirigé vers le bas lors de l'insertion des fils.**
- Examinez l'extrémité du connecteur. Les huit fils doivent être bien serrés dans le fond du connecteur RJ-45.
- Une fois que tout est correctement inséré et aligné, faites entrer la fiche RJ-45 dans la pince à sertir et sertissez solidement de manière à assurer une bonne connexion entre les fils et les broches du connecteur (Figure 1.2).

Figure 1.2 Sertissage d'un câble à paires torsadées

- À l'aide d'un testeur de câble, vérifiez si le câble fonctionne. S'il ne fonctionne pas, répéter les étapes précédentes.

NB: Le professeur vous montrera comment utiliser le testeur de câble.

1.3.4 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). Chaque binôme d'étudiant réalise un réseau à deux

machines. Pour cela, il suffit d'utiliser les câbles à pairs torsadées que vous venez de réaliser pour raccorder chaque paire d'ordinateurs directement de la carte réseau à la carte réseau.

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 » (voir la figure 1.3). Dans la catégorie « Cartes réseau », identifiez votre carte réseau et assurez-vous qu'elle fonctionne correctement et ne présente aucun problème d'installation.

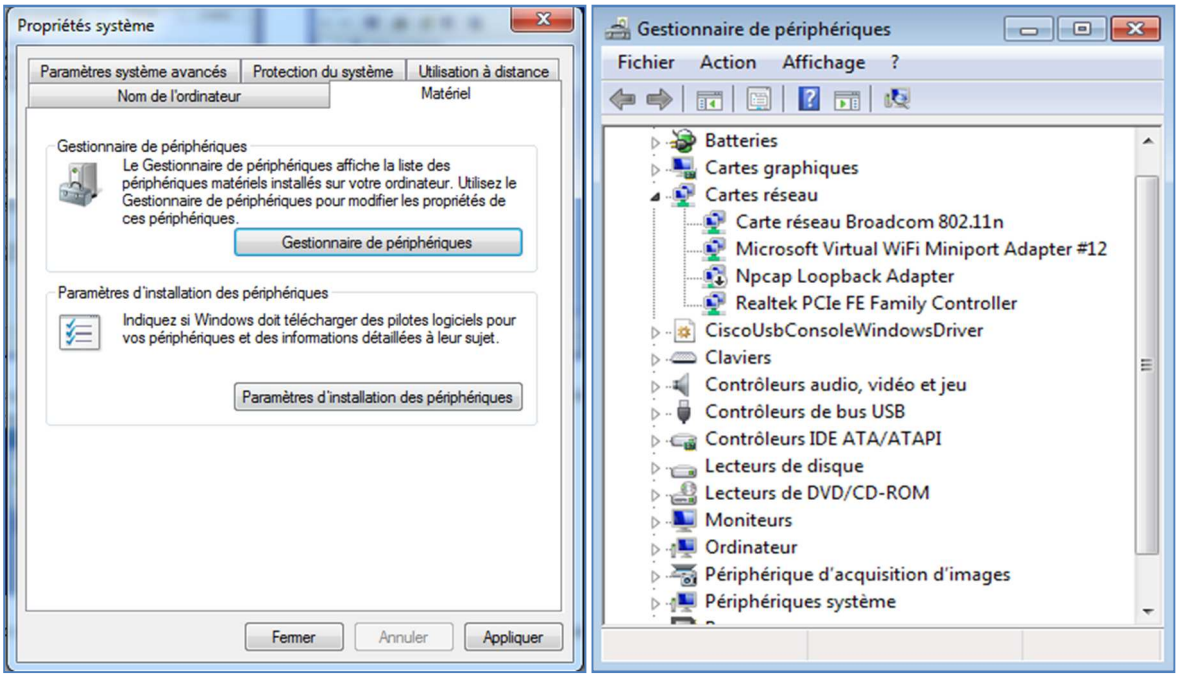


Figure 1.3 Vérification de la carte réseau

Maintenant, pour configurer votre carte réseau, vous devez aller 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 (Figure 1.4) :

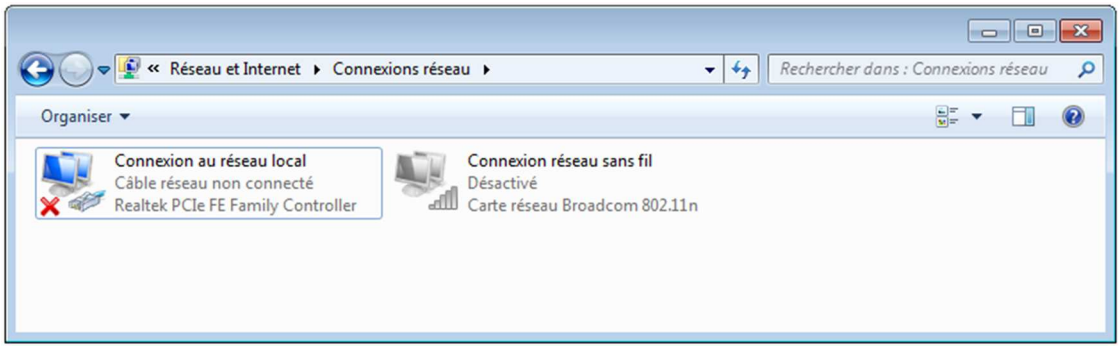


Figure 1.4 Connexions réseau

Faites un clic droit sur « Connexion au réseau local » et choisir propriétés. On arrivera à la page suivante (Figure 1.5) :

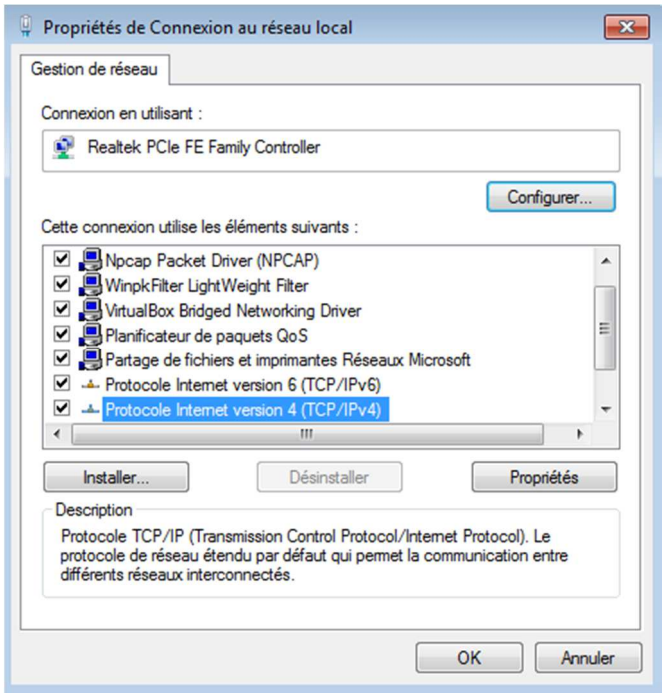


Figure 1.5 Propriétés de la connexion au réseau local

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, etc.) sur un réseau est identifié par cette adresse unique. 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. L'attribution de ces adresses doit être bien choisie pour les rendre compatibles.

Pour vos réseaux faites entrer des adresses de classe C pour chaque ordinateur, soit :

- Adresse IP pour la Machine-1: 192.168.0.1
- Adresse IP pour la Machine-2: 192.168.0.2

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 (Figure 1.6).

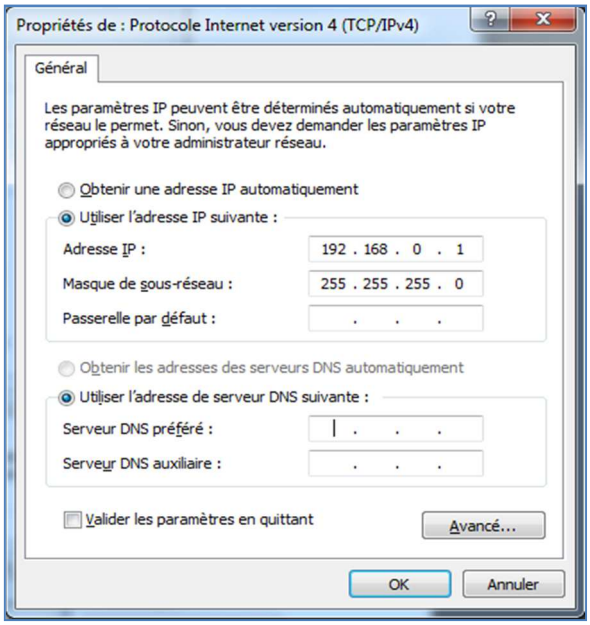


Figure 1.6 Attribution d'adresse IP (Machine-1)

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 (Figure 1.7).

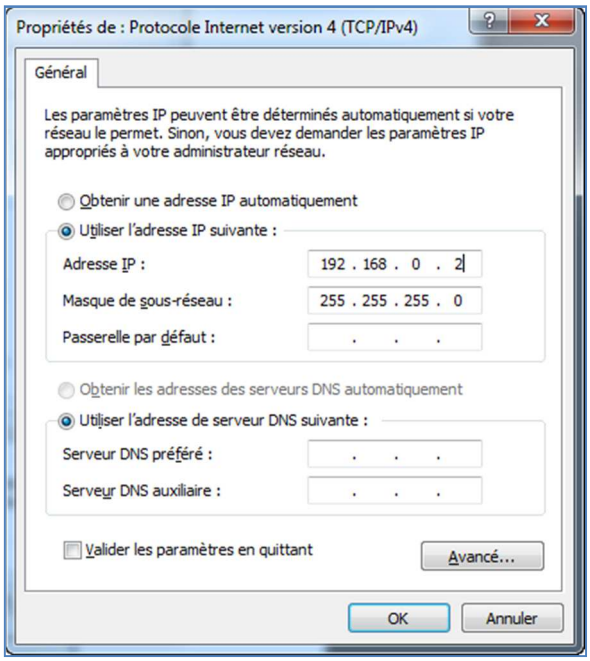


Figure 1.7 Attribution d'adresse IP (Machine-2)

Validez jusqu'à revenir sur le bureau. Voilà, les deux ordinateurs sont en réseau.

Test de la communication

La commande « ping »

Le test de la validité de l'adresse IP peut être réalisé à l'aide de la commande « ping ». Cette commande « ping » correspond à l'envoi d'une trame (paquet de données) à l'adresse IP choisie. Si l'ordinateur qui se trouve à cette adresse est connecté sur le réseau, il renvoi la même trame à son expéditeur. Cela permet de vérifier la connexion entre les deux.

Pour exécuter la commande « ping », il suffit d'ouvrir une fenêtre de ligne de commande :

Démarrer / Exécuter puis tapez : **cmd**

Exécutez la commande « ping » sur l'adresse IP de l'ordinateur voisin, par exemple :

ping 192.168.0.2

Si le réseau entre les deux machines est correctement configuré, 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

Figure 1.8 Résultat de la commande « ping »

La commande « ipconfig »

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

Relevez sur votre compte rendu les informations suivantes :

Nom de l'hôte de votre machine : ……..

Adresse physique MAC de votre carte réseau : ……..

Adresse IP de votre machine : ……

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 *numéro* de votre machine dans le laboratoire).

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

1.3.5 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, etc.

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 utilisation par des machines, un peu moins pour être utilisées par des 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. Comme précisé précédemment, la commande « 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.

TP N° 2
Liaison de données

2.1 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 la commande arp.
- Utiliser Wireshark pour examiner les échanges ARP.

2.2 Introduction

Un processus d'échange de données entre couches de même niveau mais sur deux systèmes ou deux ordinateurs différents s'effectue par le biais d'un mécanisme appelé « encapsulation » en passant d'une couche à une autre jusqu'à arriver à la machine destinatrice.

Dans le cas d'une émission, chaque couche (N) reçoit de la couche immédiatement supérieure (N+1) des données opaques qu'elle doit transférer à la couche immédiatement inférieure (N-1) [3]. L'encapsulation consiste alors à ajouter à ces données opaques des informations de contrôle (champs) propres au protocole de chaque couche. Par exemple, au niveau de la couche liaison de donnée, le protocole Ethernet (qui équipe actuellement la quasi-totalité des réseaux locaux LAN) permet d'encapsuler les paquets provenant de la couche réseau (souvent des paquets IP) en ajoutant un certain nombre de champs.

Par ailleurs, la communication entre machines ne peut s'effectuer qu'à travers l'interface physique en utilisant des adresses physiques (MAC). Cependant, les applications ne connaissent que les adresses IP. Ainsi, le protocole ARP (Address Resolution Protocol) est utilisé pour mapper une adresse IP de couche 3 à une adresse MAC de couche 2.

Dans ce TP, nous utilisons l'analyseur de paquets Wireshark, d'une part, pour examiner le processus d'encapsulation au niveau de la couche liaison de données à travers la capture et

l'analyse des champs des trames Ethernet II et, d'autre part, pour capturer et d'analyser les échanges ARP entre les périphériques réseau.

2.3 Travail à réaliser

2.3.1 Capture de trames

Après avoir ouvert une session sur votre poste, ouvrez une fenêtre de ligne de commande 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 IP 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 [4].

- Lancez le logiciel Wireshark.
- Sélectionnez l'interface connectée sur le réseau du laboratoire.
- Appropriez-vous l'application en consultant l'aide, le cas échéant.

L'interface de Wireshark est composée de trois zones (Figure 2.1) :

- en haut, la liste des trames reçues ou envoyées par l'interface réseau.
- en bas, le contenu du paquet sélectionné, au format hexadécimal.
- au milieu, Wireshark traduit les données brutes du paquet sélectionné dans un format compréhensible.

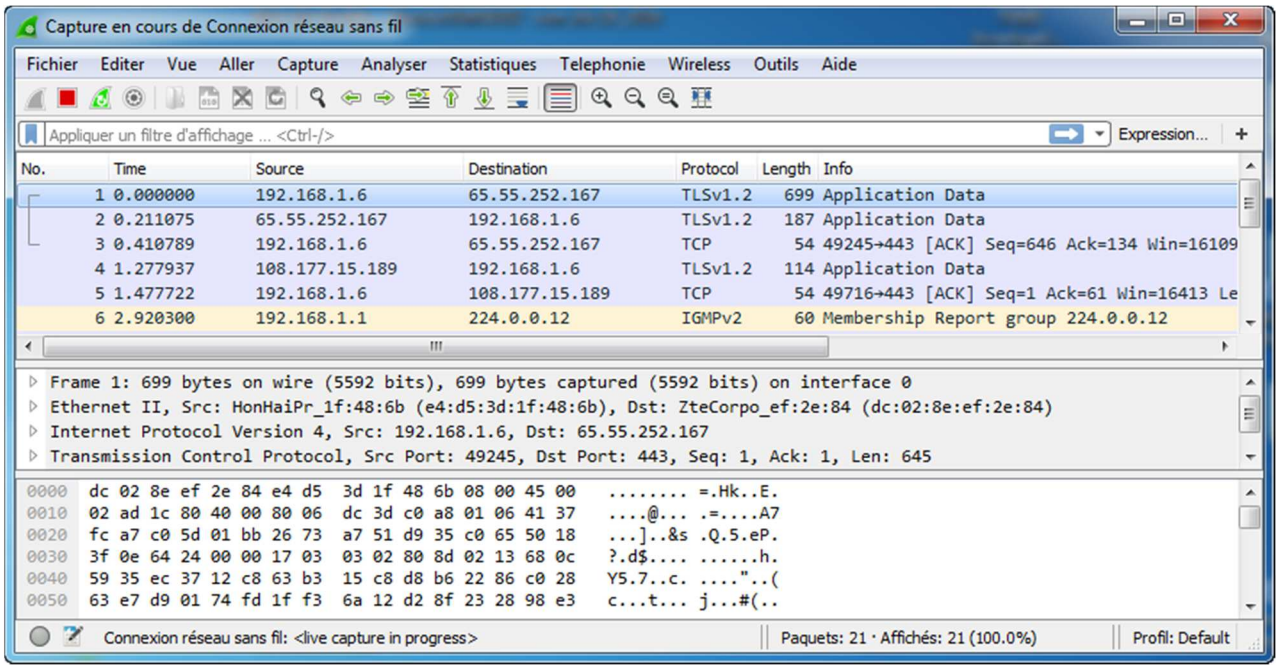


Figure 2.1 Interface de Wireshark

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 « Analyser > Filtres d'affichage », faites en sorte que s'affiche uniquement le dialogue entre votre machine et celle du voisin.

2.3.2 Ethernet

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

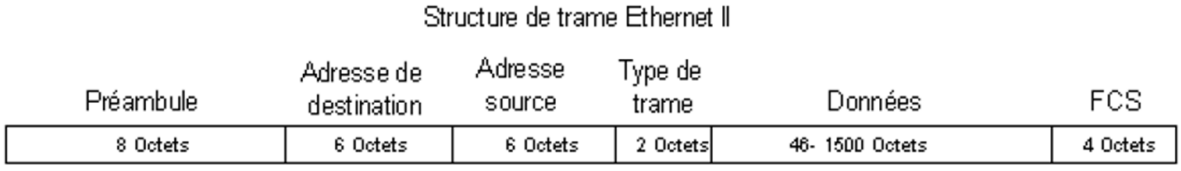


Figure 2.2 Format de trame Ethernet II

À l'aide du logiciel Wireshark, il est possible d'obtenir les informations suivantes sur la trame Ethernet II (Tableau 2.1):

Tableau 2.1 Description des champs d'une 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 ou adresses MAC. La longueur de chaque adresse MAC est de 48 bits, ou 6 octets, exprimée 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 https://miniwebtool.com/fr/mac-address-lookup/ pour obtenir une liste de codes fournisseurs. ✓ Les six derniers chiffres hexadécimaux, ac:a7:6a, indiquent 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. L'adresse source est toujours à monodiffusion.
Adresse source	e4:d5:3d:1f:48:6b	
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 ?

……

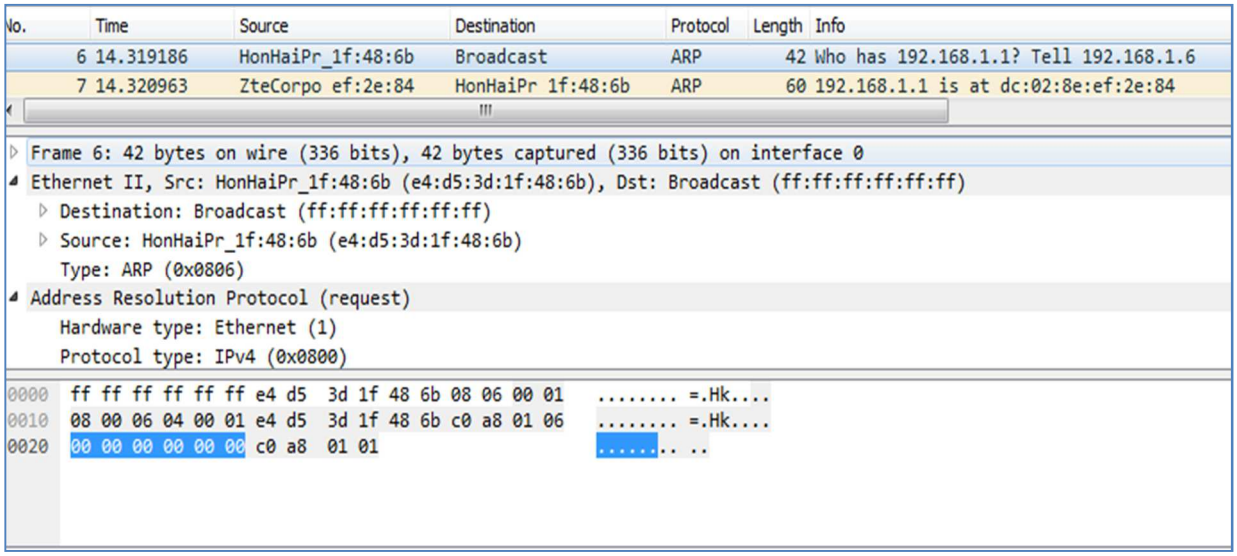


Figure 2.3 Exemple d'une trame capturée par Wireshark

La figure 2.3 contient une vue éclatée de la capture Wireshark de la première trame capturée. 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	

2.3.3 ARP

(a) 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 au Tableau 2.2.

Tableau 2.2 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.

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 ping pour ajouter de façon dynamique des entrées dans le cache ARP

Comme présenté dans le TP précédent, 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
192.168.0.2          B8-70-F4-5A-89-1E         dynamique
C:\>
```

Figure 2.4 Affichage du cache ARP

2. Comment l'entrée ARP a-t-elle été ajoutée au cache ARP ?

……..

3. Quelle est l'adresse physique et l'adresse IP de l'ordinateur « voisin » de destination ? Renseignez le tableau suivant :

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.

(b) 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

Remarque : l'option **–n 1** signifie l'envoie d'une seule requête ping.

4- Arrêtez la capture Wireshark et évaluez la communication. La zone supérieure de Wireshark affiche le nombre de paquets capturés et la zone du milieu 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.

TP N° 3
Routage statique

3.1 Objectifs

- Comprendre le fonctionnement d'un routeur Cisco.
- Connaitre les principales commandes des routeurs Cisco.
- Etudier et configurer le routage statique.

3.2 Prérequis

Pour réaliser ce TP, vous devez réviser le cours portant sur la couche réseau. Vous devez connaitre toutes les commandes de base pour la configuration des routeurs Cisco en consultant l'annexe A « Présentation générale des routeurs Cisco ».

Vous utiliserez le logiciel Packet Tracer de Cisco, qui permet de simuler et étudier les réseaux (voir l'annexe B « Prise en main Packet Tracer »).

3.3 Introduction

Le routage consiste à déterminer (choisir) la route par lesquels les paquets sont transmis de la source à la destination à l'aide d'équipements appelés **routeurs**. Ce dernier est un équipement matériel et logiciel (de couche 3) qui fait en sorte que les paquets émis par une machine d'un réseau puissent atteindre une machine destinataire située sur un réseau distant. Un routeur peut apprendre les routes vers les réseaux distants de deux manières différentes: (1) manuellement: les réseaux distants sont saisis manuellement dans la table de routage à l'aide de routes statiques ou (2) dynamiquement: les routes distantes sont automatiquement acquises via un protocole de routage dynamique [5].

Dans ce TP, vous allez apprendre à configurer des routeurs Cisco afin de mettre en œuvre le routage statique permettant de faire communiquer différentes stations de travail sur des réseaux distants.

3.4 Travail à réaliser

Les activités de ce TP s'effectuent à l'aide du logiciel Packet Tracer, fourni par Cisco. Cette application permet d'émuler des PCs et des équipements Cisco afin de schématiser des réseaux locaux ou étendus (Annexe B « Prise en main Packet Tracer »).

3.4.1 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 [6] :

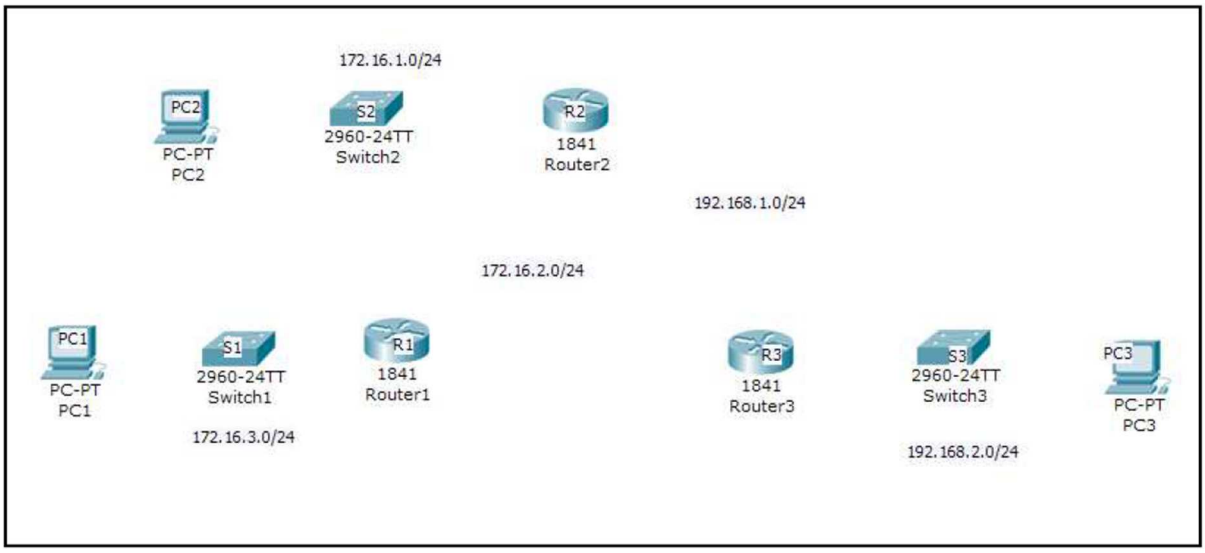


Figure 3.1 Périphériques du réseau simulé

3.4.2 Ajout des modules WIC-2T 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 (Figure 3.2). Pour réaliser ce TP, nous avons besoin de rajouter des interfaces séries (WIC-2T) aux différents routeurs utilisés.

Pour ajouter un module WIC-2T il faut le faire dans cet ordre :

- Mettre hors tension le routeur ;
- Glisser le module WIC-2T dans l'emplacement prévu à cet effet ;
- Remettre en tension le routeur.

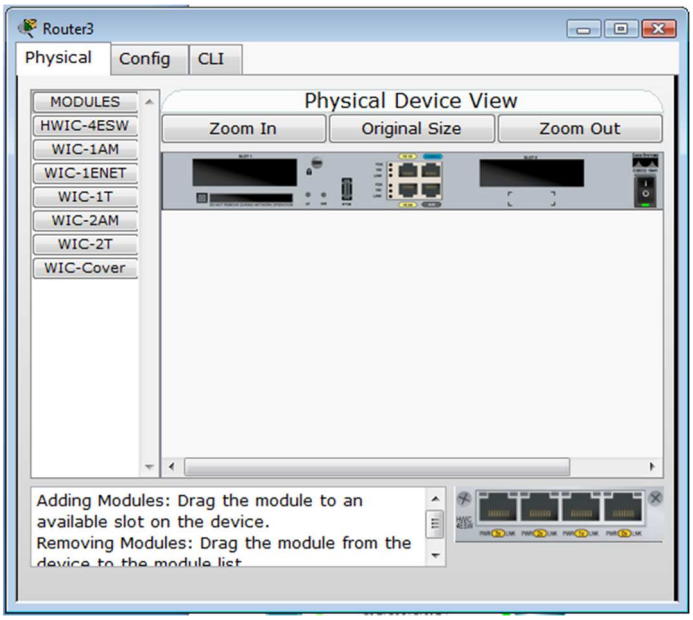


Figure 3.2 Ajout de port WIC-2T au routeur

3.4.3 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 3.3) :

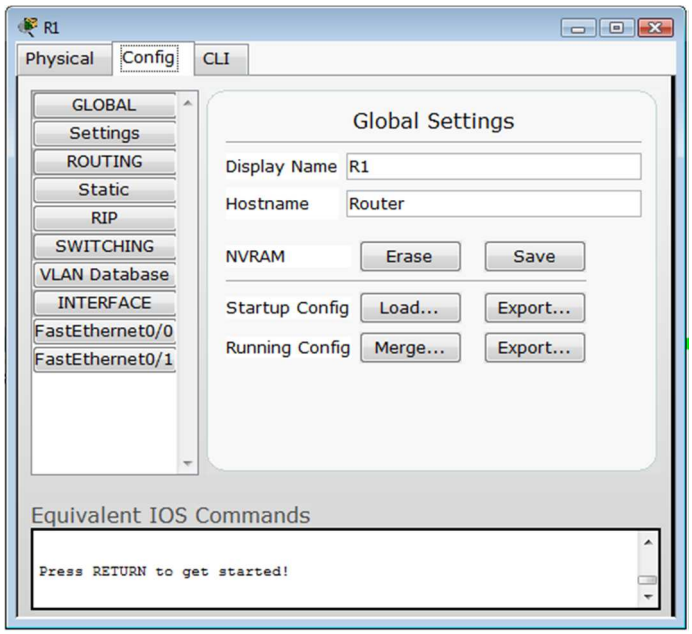


Figure 3.3 Changement de nom d'un routeur

De plus, nous changeons également le « hostname » des routeurs avec les commandes suivantes en mode CLI (exemple du premier routeur) :

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

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

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

Nous relions les autres équipements à l'aide de câbles Ethernet droits (Figure 3.4).

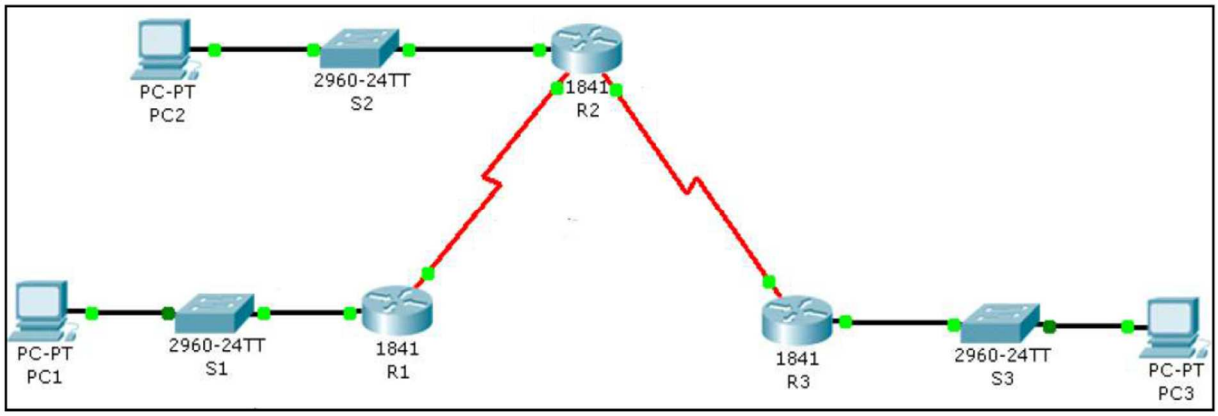


Figure 3.4 Connexion des équipements

3.4.5 Configuration des informations IP sur les interfaces

Le réseau que nous allons simuler comporte 5 sous-réseaux : 172.16.1.0/24, 172.16.3.0/24,172.16.2.0/24, 192.168.1.0/24 et 192.168.2.0/24 (Comme le montre la figure 3.5 ci-dessous).

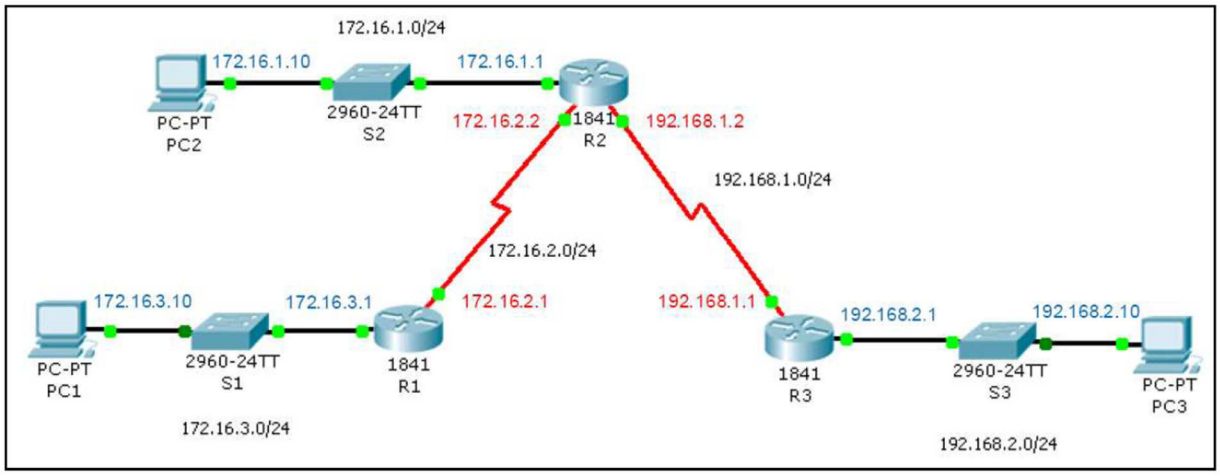


Figure 3.5 Adressage IP du réseau simulé [6]

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. Vous devez configurer 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 3.6).

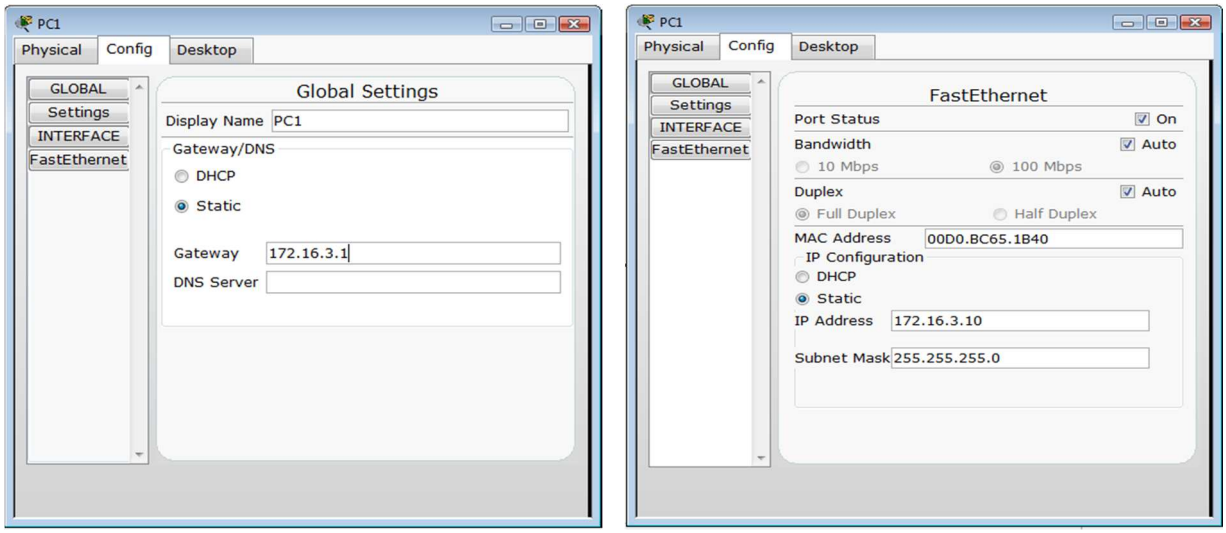


Figure 3.6 Configuration de l'interface réseau d'un PC

(b) Configuration des interfaces Ethernet des routeurs

Dans cette partie, vous allez 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
7  R1(config)#exit
8  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
7  R2(config)#exit
8  R2# copy running-config startup-config
```

Interface FastEthernet 0/0 (R3)

```
1  R3>enable
2  R3# conf t
3  R3(config)# interface fastEthernet0/0
4  R3(config-if)# ip address 192.168.2.1  255.255.255.0
5  R3(config-if)# no shutdown
6  R3(config-if)#exit
7  R3(config)#exit
8  R3# 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, dans la pratique, 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 devrons 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 devrons 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...
```

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

3.4.7 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 de la passerelle ou de l'interface de sortie) pour atteindre chacun de ces réseaux [7].

En général, la passerelle est l'adresse IP de l'interface du prochain routeur permettant d'atteindre le réseau distant.

Appliquons ce principe sur notre schéma ci-dessus:

(a) 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** via l'interface de sortie **Serial0/0/0**

(b) 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** via l'interface de sortie **Serial0/0/0**

La passerelle pour atteindre le réseau **192.168.2.0/24** est : **192.168.1.1** via l'interface de sortie **Serial0/0/1**

(c) 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** via l'interface de sortie **Serial0/0/1**

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

Il y a deux façons pour créer une route statique avec les routeurs Cisco, soit en utilisant l'adresse IP du prochain routeur (prochain saut ou passerelle), soit en en précisant l'interface de sortie permettant d'atteindre le réseau distant :

1 ou 2	*R#ip route [@IP du réseau dest] [masque du réseau dest] [@IP du prochain routeur]* *R#ip route [@IP du réseau dest] [masque du réseau dest] [interface de sortie]*

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 (passerelle) :

```
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
```

3.4.8 Vérification des informations sur la table de routage

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

- La lettre C devant chaque route (ou ligne) indique que les réseaux sont directement connectés au routeur.
- La lettre S devant chaque route (ou ligne) indique 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
```

Après consultation des trois tables de routage, nous constatons que le routage statique est correctement configuré et correspond bien à l'architecture du réseau étudié.

3.4.9 Vérification de la connectivité des périphériques

A l'aide de la commande « ping », effectuez les tests de connectivités nécessaires pour vérifier que chaque poste de chaque réseau puisse communiquer avec tous les postes de tous les autres réseaux.

Remarque: Pour la première tentative (du ping), c'est possible que ça ne marche pas car le réseau a besoin d'un peu de temps pour converger et acheminer les paquets d'un bout à l'autre. Retentez plusieurs fois pour que ça marche.

Enfin, pour connaitre le trajet emprunté par les paquets ainsi que le nombre de routeurs parcourus, utilisez la commande « traceroute » sur les routeurs Cisco et la commande « tracert » sur les PCs (sous Windows).

TP N° 4
Routage dynamique

4.1 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 nous intéressons au routage dynamique en utilisant le protocole RIP. Les objectifs de ce TP peuvent être résumés comme suit :

- Etude de réseau et découpage en sous-réseaux.
- Réaliser et tester le routage dynamique RIP entre les différents sous-réseaux.

4.2 Prérequis

Pour réaliser ce TP, vous devez réviser le chapitre portant sur la couche réseau. Vous devez aussi avoir fait le TP précédent « Routage statique » et connaitre toutes les commandes de base pour la configuration des routeurs Cisco (consulter l'annexe A « Présentation générale des routeurs Cisco »). Vous aurez besoin du logiciel Packet Tracer de Cisco (consulter l'annexe B « Prise en main Packet Tracer »).

4.3 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 [8].

4.3.1 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 [9].

Exemples de protocole de routage :

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

4.3.2 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 [10].

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 utilisons le protocole RIPv2 pour configurer le routage dynamique des différents routeurs.

4.4 Travail à réaliser

4.4.1 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 120 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^{ere} étage* : ce département rassemble l'unité de fabrication des panneaux photovoltaïque, le stockage … est composé de 80 PC.

2. **Département Transport :** *Bâtiment 1, 2ème étage* : 20 PC pour la gestion de transport.

3. **Département Commande :** *Bâtiment 2* : 50 ordinateurs de gestion des commandes.

4. **Département Administration** : *Bâtiment 3, 1ere étage* : 22 PC administratifs : direction, compatibilité, …

5. **Département Commercial :** *Bâtiment 3, 2eme 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 adresse 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. Calculez 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 calculez les adresses des premières et dernières machines configurées dans chacun des sous-réseaux. Remplissez le tableau suivant (Tableau 4.1) :

Tableau 4.1 Informations IP de chaque sous-réseau

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) ?

4.4.2 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.
- Etablissez les liaisons série et ethernet entre les différents équipements du réseau.
- **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.

4.4.3 Mise en place du routage RIP

La configuration du protocole RIP 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
```

- ✓ Précisez 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).

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

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

Exemple

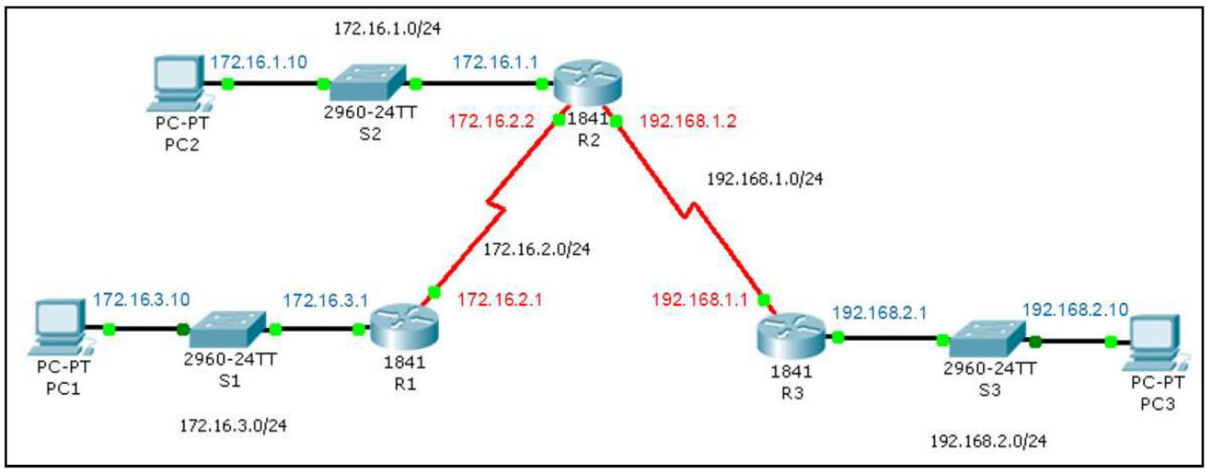


Figure 4.1 Exemple d'architecture réseau [6]

Dans cet exemple, nous reprenons l'architecture du réseau étudié dans le TP3 (Figure 4.1). 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.

4.4.4 Tests et vérification de la connectivité

A présent essayons de tester la communication entre différentes machines: lancez un **ping** entre les différentes machines des différents réseaux. 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 avions travaillé sur le routage statique (TP3), nous avions vu qu'il y'avait deux lettres utilisées pour décrire chaque route (ou chaque ligne). 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 les tables de routage sont en adéquation avec le schéma sur lequel vous avez travaillé.

Enfin et comme dans le TP précédent, vous pouvez utiliser la commande « **traceroute** » sur les routeurs Cisco et la commande « **tracert** » sur les PCs afin d'afficher les détails des chemins (routeurs et nombre de sauts) empruntés par les différents paquets pour aller d'une machine à une autre.

TP N° 5

Protocoles des couches transport et application

5.1 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.

5.2 Prérequis

Pour réaliser ce TP, vous devez réviser les chapitres portant sur les couches Transport et Application. Vous aurez aussi besoin de l'analyseur de réseau Wireshark.

5.3 Introduction

5.3.1 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) [11].

- 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.

La figure 5.1 ci-dessous illustre quelques applications employées sur Internet ainsi que les protocoles de la couche transport (TCP ou UDP) utilisés.

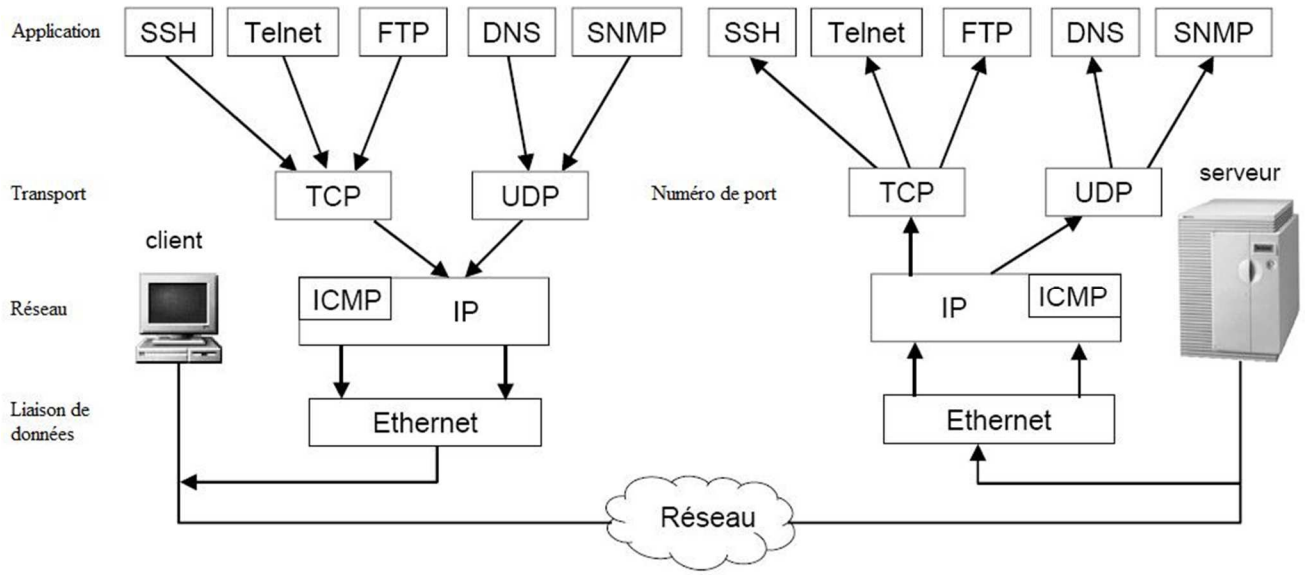


Figure 5.1 Différents protocoles des couches du modèle OSI

5.3.2 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) (Figure 5.2). Le système DNS s'appuie sur le protocole de transport UDP (port 53) [12].

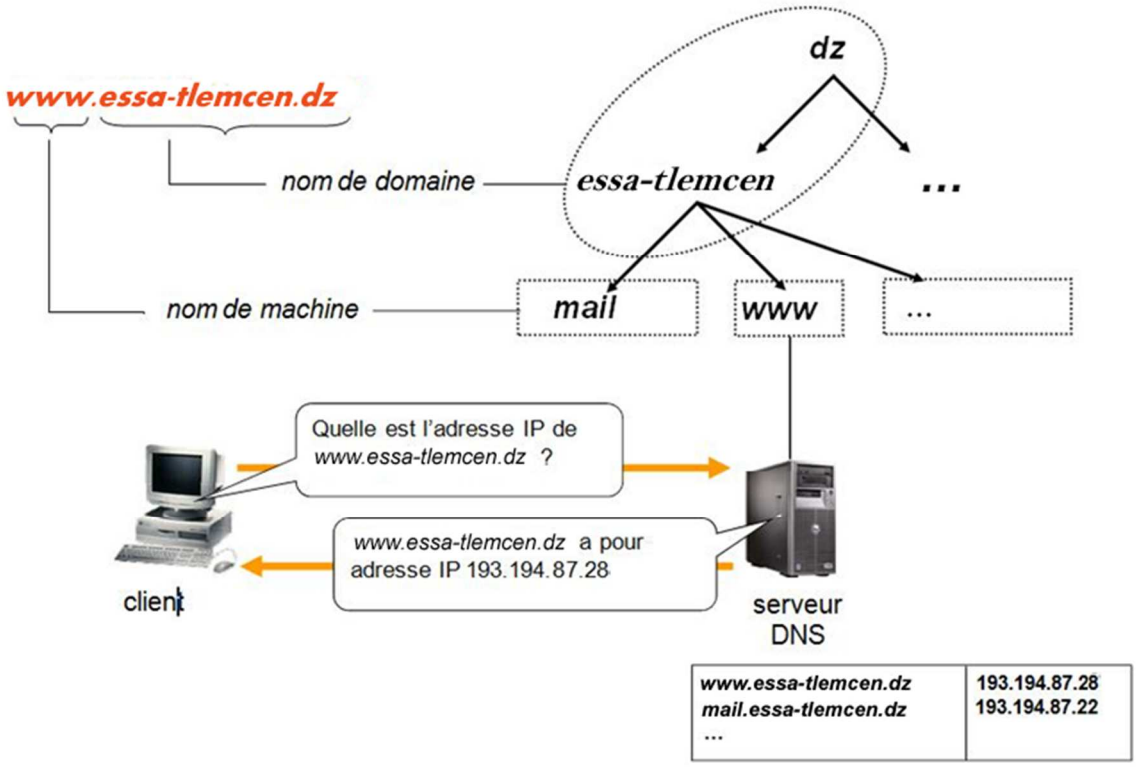


Figure 5.2 Serveur et requêtes DNS

5.3.3 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.

5.4 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).

5.4.1 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'ESSA 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 ?

5.4.2 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.

1. A l'aide de Wireshark, analysez les segments TCP échangés dans un dialogue Telnet lorsque vous vous connectez sur un serveur distant. 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 (qui vous seront donnés par votre enseignant de TP), 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 ?

Bibliographie

[1] DORDOIGNE, J. (2015). Réseaux informatiques - Notions fondamentales (6ième édition). ENI. ISBN : 9782746093928

[2] CCNA Discovery, Cisco. (2015). Travaux pratiques 4.5.3 Réalisation de câbles à paires torsadées non blindées (UTP) droits et croisés.

[3] IKNI Samir. 2019. TP Réseau Informatiques Locaux. Université de Guelma.

[4] Xavier Buche. 2018. TP n°2: Liaison de données. L3-S6 INFO/MIAGE, Réseaux. Université de Lille.

[5] Cisco Systems. *Notions de base sur les réseaux*. CCNA Exploration Fr V 6.0

[6] Vinel Emmanuel & Slimane Amine. (2009). TP5 ROUTAGE CISCO

[7] TP N° 03 : Routage Statique. (2015). Faculté de Technologie, Département de GEE, L3IBM. Université Abou-Bekr Belkaid de Tlemcen.

[8] Marc Silanus. (2008). TP réseau – Routage dynamique RIP. Sciences et technologies de l'industrie et du développement durable.

[9] ZHANG Tuo. (2013). Routage Dynamique RIP sur CISCO, M2103.IUT Dijon-Auxerre.

[10] TP N° 04 : Routage Dynamique. (2015). Faculté de Technologie, Département de GEE, L3IBM, Université Abou-Bekr Belkaid de Tlemcen.

[11] Christian Bulfone & Jean-Michel Adam. (2020). TP sur IP, Licence "Mathématiques et Informatique Appliquées aux Sciences Humaines et Sociales" (MIASHS). Université Grenoble Alpes.

[12] Christian Bulfone. (2020). Quelques protocoles applicatifs, Licence "Mathématiques et Informatique Appliquées aux Sciences Humaines et Sociales" (MIASHS). Université Grenoble Alpes.

[13] CCNA Exploration, Cisco. (2015).Présentation générale des routeurs Cisco.

[14] Marie-Agnès PERALDI-FRATI. (2013). Présentation et utilisation de Packet Tracer. TP Réseau LPSIL ADMIN. IUT de Nice Sophia-Antipolis.

Annexes

Annexe A Présentation générale des routeurs Cisco

A.1 Présentation du routeur

Le routeur est équipement matériel et logiciel (de couche 3) qui fait en sorte que les paquets émis par une machine d'un réseau puissent atteindre une machine destinataire situé sur un réseau différent. Les paquets ne peuvent circuler entre réseaux différents que si ces réseaux sont reliés par un ou plusieurs routeurs.

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 (Figure A.1). 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 [13].

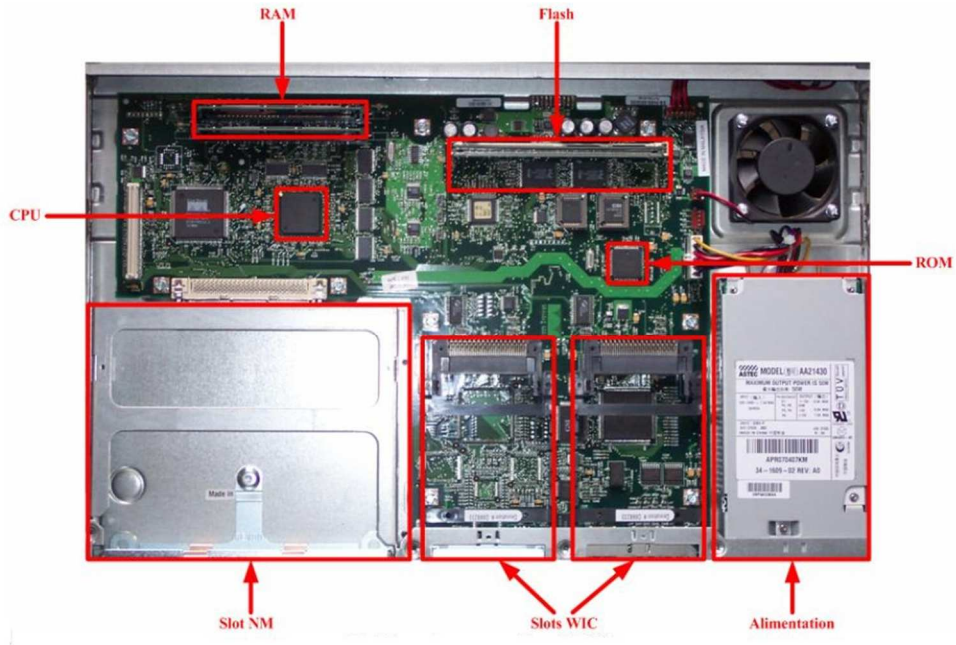


Figure A.1 Vue interne d'un routeur Cisco 2660XM

A.2 Processeur et mémoires d'un routeur Cisco

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

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

A.2.1 UC

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

A.2.2 Mémoire vive (RAM)

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.

A.2.3 Mémoire morte (ROM)

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.

A.2.4 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.

A.2.5 Mémoire vive non volatile (NVRAM)

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 (NVRAM), où elle est enregistrée en tant que fichier de configuration initiale. La mémoire vive non volatile (appelée aussi mémoire vive rémanente) conserve son contenu, même si le routeur se recharge ou s'il est mis hors tension.

A.3 Composants du routeur Cisco et leurs fonctions

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 (Figure A.2). L'architecture physique interne diffère d'un modèle à l'autre [13].

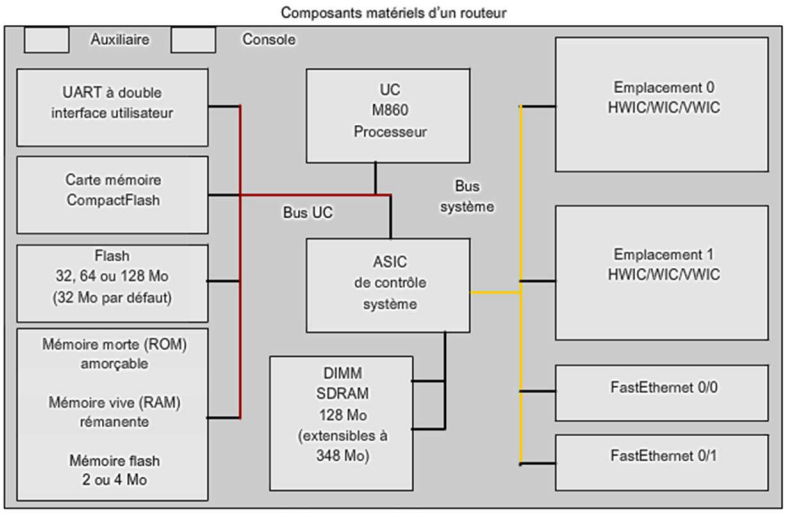


Figure A.2 Schéma logique des composants internes d'un routeur Cisco

A.3.1 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.

A.3.2 Port console

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

A.3.3 UART (émetteur-récepteur asynchrone universel) à double interface utilisateur

UART (universal asynchronous receiver/transmitter) à double interface, car il est accessible par deux moyens (le port auxiliaire et le port console).

A.3.4 Processeur

Le processeur est le cerveau du routeur. C'est le processeur qui gère la plupart des opérations réalisées, il interprète les instructions des programmes informatiques et traite les données.

A.3.5 ASIC de Contrôle système

Il contrôle les flux de données entre la mémoire. Les interfaces et le processeur.

A.3.6 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.

A.3.7 Mémoire ROM amroçable

Stocke le programme d'amorçage, le moniteur ROM et éventuellement une version simplifiée du logiciel IOS. Partage la mémoire vive RAM rémanente.

A.3.8 Mémoire vive rémanente (NVRAM)

Stocke la configuration initiale et partage la mémoire flash avec la mémoire ROM amorçable.

A.3.9 DIMM SDRAM

Stocke la configuration en cours, la table de routage et les autres structures dynamiques.

Les différentes interfaces et ports du routeur sont décrits dans la figure A.3 suivante :

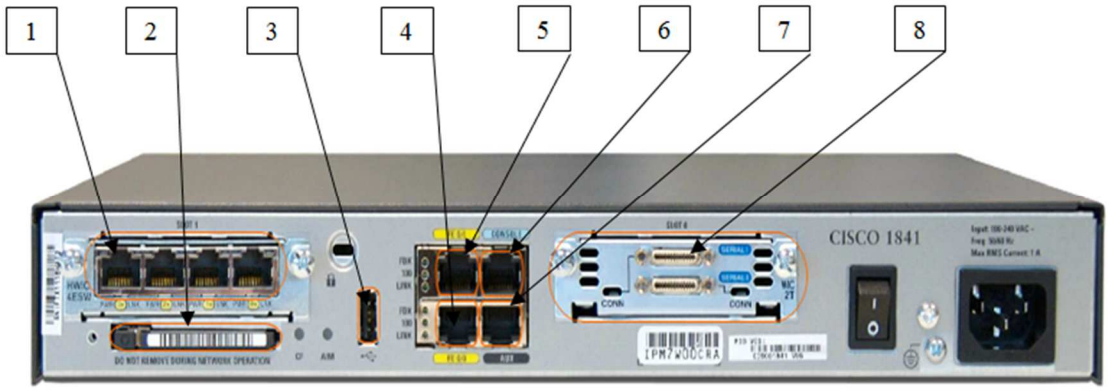


Figure A.3 Interfaces et ports d'un routeur Cisco 1841

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)

A.4 Internetwork Operating System (IOS)

Le système d'exploitation utilisé dans les routeurs Cisco est appelé Cisco Internetwork Operating System (IOS). Comme tout système d'exploitation d'ordinateur, Cisco IOS gère les ressources matérielles et logicielles du routeur, notamment l'allocation de mémoire, les processus, la sécurité et les systèmes de fichiers. Cisco IOS est un système d'exploitation multitâche qui exécute les fonctions de routage, de commutation, d'interconnexion et de télécommunications [13].

Bien que Cisco IOS semble être identique sur de nombreux routeurs, il existe de nombreuses images IOS différentes. Une image IOS est un fichier contenant l'IOS entier pour un routeur donné. Selon le modèle de routeur et les fonctions intégrées à l'IOS, Cisco a développé de nombreux types d'images IOS différentes. En général, plus l'IOS comprend de fonctions, plus l'image IOS est grande et plus la quantité de mémoire flash et de mémoire vive nécessaire au stockage et au chargement de l'IOS est importante. Par exemple, certaines fonctions comprennent la possibilité d'exécuter IPv6 ou la capacité pour le routeur de procéder à la traduction des adresses de réseau (NAT).

Comme les autres systèmes d'exploitation, Cisco IOS possède sa propre interface utilisateur. Bien que certains routeurs fournissent une interface graphique utilisateur, l'interface de ligne de commande (CLI) est la méthode la plus utilisée pour la configuration des routeurs Cisco.

À l'amorçage, le fichier de configuration initiale (startup-config) stocké dans la mémoire vive non volatile est copié dans la mémoire vive et enregistré en tant que fichier de configuration en cours (running-config). L'IOS exécute les commandes de configuration dans le fichier running-config. Toute modification apportée par l'administrateur réseau est enregistrée dans la configuration en cours et immédiatement implémentée par l'IOS. Dans la suite de cette annexe, nous allons passer en revue une partie des commandes IOS de base utilisées pour configurer un routeur Cisco.

A.5 Processus d'amorçage du routeur

Le processus d'amorçage comporte quatre phases principales (Figure A.4) :

- 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.

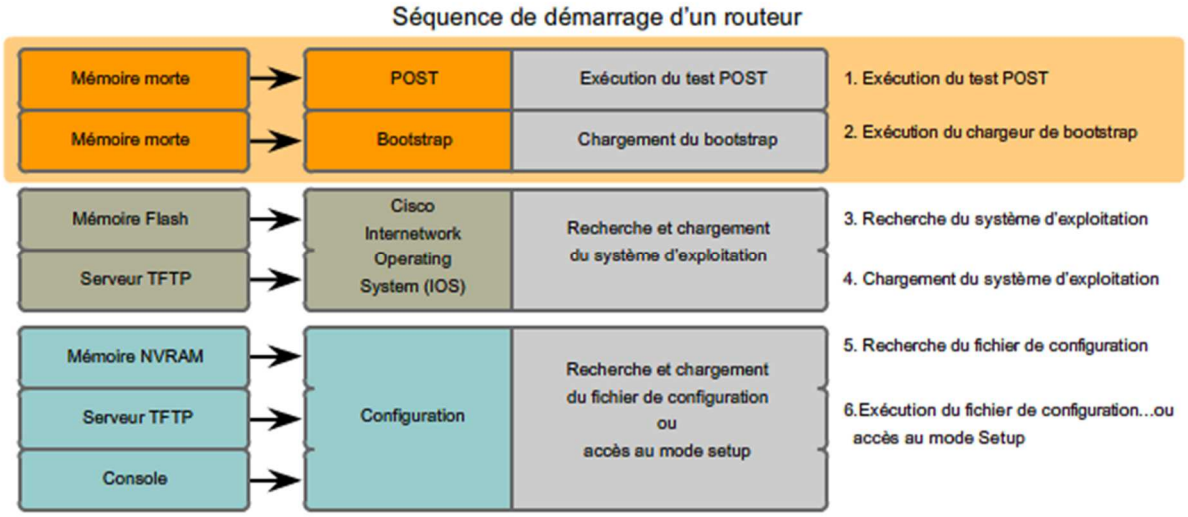


Figure 4.A Séquence de démarrage d'un routeur Cisco

A.5.1 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.

A.5.2 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.

A.5.3 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.

Remarques :

- 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.

A.5.4 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 démarrez 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

Dans nos TPs, 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.

Lorsque le mode Configuration n'est pas utilisé, l'IOS crée un fichier de configuration en cours par défaut. Le fichier de configuration en cours par défaut est un fichier de configuration de base contenant les interfaces du routeur, les interfaces de gestion et certaines informations par défaut. Il ne contient pas d'adresses d'interface, d'informations de routage, de mots de passe ou d'autres informations de configuration spécifiques.

A.6 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 (Figure A.5).

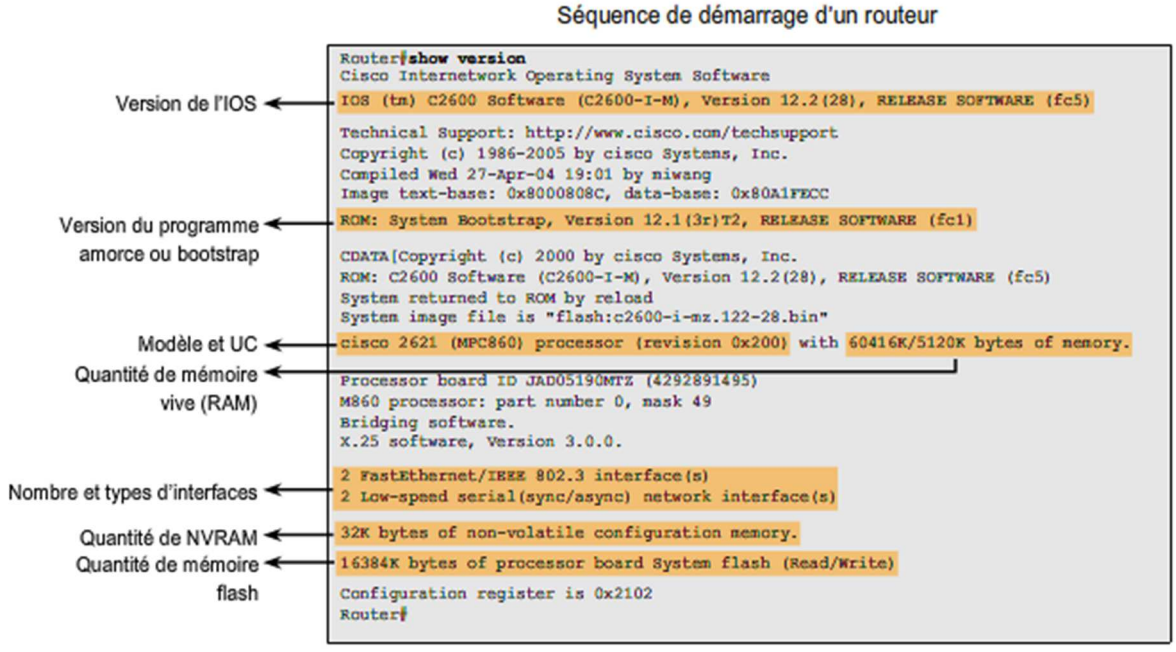


Figure A.5 Résultat de la commande « show version » [13]

Le résultat de la commande *show version* de la figure A.5 comprend les éléments suivants [13] :

A.6.1 Version IOS

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Il s'agit de la version du logiciel Cisco IOS qui se trouve en mémoire vive et qui est actuellement utilisé par le routeur.

A.6.2 Programme d'amorçage en mémoire morte

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Il s'agit de la version du logiciel d'amorçage système, stocké en mémoire morte, qui a été initialement utilisé pour démarrer le routeur.

A.6.3 Emplacement du logiciel IOS

System image file is "flash:c2600-i-mz.122-28.bin"

Indique où se trouve le programme d'amorçage et où il a chargé le logiciel Cisco IOS, ainsi que le nom de fichier complet de l'image IOS.

A.6.4 UC et quantité de mémoire vive

cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

La première partie de cette ligne indique le type d'UC sur ce routeur. La dernière partie de cette ligne affiche la quantité de mémoire vive dynamique. Certains modèles de routeurs, comme les routeurs 2600, utilisent une fraction de mémoire vive dynamique comme mémoire de paquets. Celle-ci est utilisée pour mettre les paquets en mémoire tampon.

Pour déterminer la quantité totale de mémoire vive dynamique présente sur le routeur, additionnez les deux nombres.

Dans cet exemple, le routeur Cisco 2621 a 60416 Ko (kilo-octets) de mémoire vive dynamique libre, utilisée pour le stockage temporaire de Cisco IOS et d'autres processus système. Les 5120Ko restants sont consacrés à la mémoire de paquets. Additionnés, ces deux nombres donnent 65536 Ko, ou 64 méga-octets (Mo), de mémoire vive dynamique totale.

Remarque: il peut être nécessaire de mettre à niveau la quantité de mémoire vive lors de la mise à niveau de l'IOS.

A.6.5 Interfaces

2 FastEthernet/IEEE 802.3 interface(s)

2 Low-speed serial(sync/async) network interface(s)

Cette partie du résultat indique les interfaces physiques sur le routeur. Dans cet exemple, le routeur Cisco 2621 a deux interfaces FastEthernet et deux interfaces séries à faible vitesse.

A.6.6 Quantité de mémoire vive non volatile

32K bytes of non-volatile configuration memory.

Il s'agit de la quantité de mémoire vive non volatile présente sur le routeur. La mémoire vive non volatile sert à stocker le fichier de configuration initiale.

A.6.7 Quantité de la mémoire flash

16384K bytes of processor board System flash (Read/Write)

Il s'agit de la quantité de mémoire flash présente sur le routeur. La mémoire flash sert à stocker le logiciel Cisco IOS de façon permanente.

Remarque: il peut être nécessaire de mettre à niveau la quantité de mémoire flash lors de la mise à niveau de l'IOS.

A.7 Configuration de base d'un routeur Cisco

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.7.1 Nom d'hôte et mots de passe

La figure A.6 indique la syntaxe de base des commandes de configuration du nom d'hôte, des mots de passe et de la bannière.

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.

R1(config)#enable secret mot_de_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 mot_de_passe
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password mot_de_passe
R1(config-line)#login
R1(config-line)#exit

A.7.2 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	`Router(config)#hostname name`
Définition des mots de passe	`Router(config)#enable secret password`
	`Router(config)#line console 0`
	`Router(config-line)#password password`
	`Router(config-line)#login`
	`Router(config)#line vty 0 4`
	`Router(config-line)#password password`
	`Router(config-line)#login`
Configuration d'une bannière de message du jour	`Router(config)#banner motd # message #`

Figure A.6 Commandes de configuration du nom d'hôte, des mots de passe et de la bannière [13]

A.7.3 Configuration des interfaces du routeur

Vous allez maintenant configurer les différentes interfaces du routeur à l'aide des adresses IP et d'autres informations (Figure A.7). 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 :

```
R1(config)#interface Serial0/0
R1(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 R1 ESSAT-AT (Aide: 043 - 41-55-43)

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 DTE 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

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`

Figure A.7 Commandes de configuration d'interfaces et de vérification [13]

A.7.4 Commandes d'enregistrement et de vérification de la configuration du routeur

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.

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 démarrer 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.

Affichez la configuration en cours à l'aide de la commande suivante :

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.

Pour afficher la configuration de démarrage (ou configuration initiale), vous devez utiliser la commande suivante :

R1#show startup-config

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 démarrage. 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 de l'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.

Annexe B Prise en main Packet Tracer

B.1 Présentation de Packet Tracer

Packet Tracer est un logiciel permettant de construire un réseau physique virtuel et de simuler le comportement de différents protocoles sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. [14]

B.2 Description générale

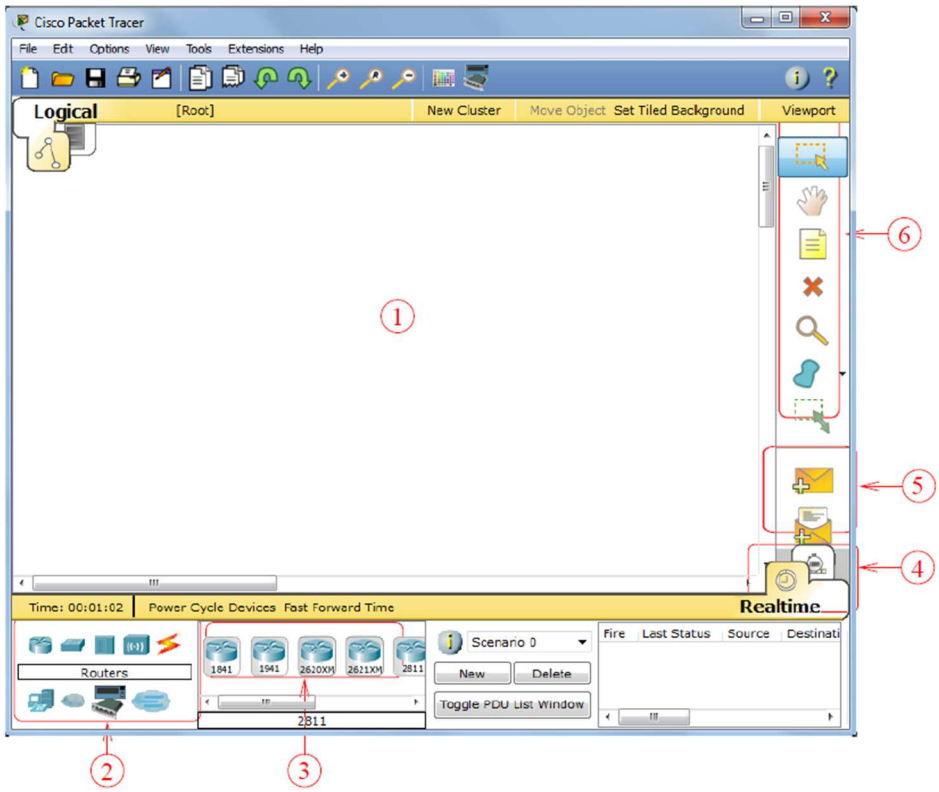


Figure B.1 Interface générale de Packet Tracer

La figure B.1 montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit, elle constitue l'espace de travail. Les équipements réseau pouvant être utilisés sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3). La zone (6) contient un ensemble d'outils :

– *Select* : pour déplacer ou éditer des équipements.

– *Move Layout* : permet de déplacer le plan de travail.

– *Place Note* : place des notes sur le réseau.

– *Delete* : supprime un équipement ou une note/

– *Inspect* : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage).

La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4) permet de passer du mode temps réel au mode simulation.

B.3 Construire un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi les 8 catégories proposées par Packet Tracer (Zone (2) - Figure B.1) : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multi-utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents (Zone (3) - Figure B.1). Pour ajouter un équipement, il suffit de le glisser sur l'espace de travail (Zone (1) - Figure B.1) à l'endroit choisi.

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée (Figure B.2). Dans nos différents travaux pratiques, nous n'utiliserons que 2 types de connexions : les câbles à paires torsadées droits (Copper Straight-Through), les câbles à paires torsadées croisés (Copper Cross-Over) et les câbles séries (Serial). Ils sont en position 3 et 4 sur la figure de droite ci-dessus.

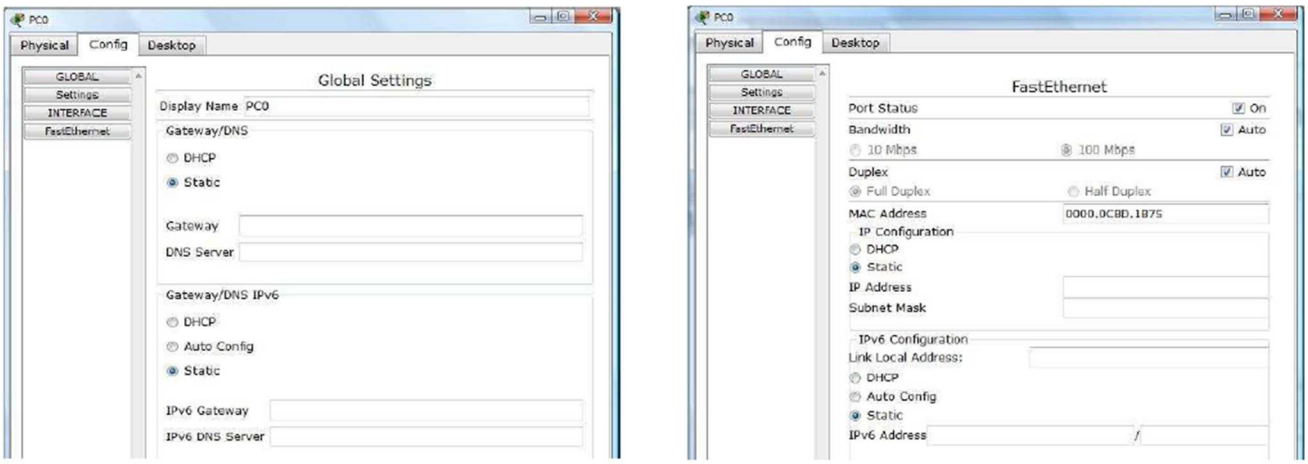
Figure B.2 Les différentes connexions proposées

B.4 Configuration d'un ordinateur

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config

(configuration passerelle, DNS et adresse IP) et Desktop (pour exécuter l'invite de commandes ou le navigateur Web).

Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global (Figure B.3(a)). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton FastEthernet en-dessous du bouton INTERFACE (Figure B.3(b)).



Configuration passerelle et DNS ***(a)*** *Configuration IP* ***(b)***

Figure B.3 Configuration d'un PC

B.4.1 Invite de commandes

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser).

L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau.

La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont accessibles. Si Packet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés.

B.5 Utilisation des routeurs sous Packet Tracer

Pour ajouter des routeurs dans un réseau, il faut sélectionner la catégorie *Routers* et glisser la version du routeur qu'on veut utiliser.

Les Routeurs Cisco offrent la possibilité d'ajouter différents modules. Packet Tracer permet de simuler une façade de routeur et ainsi monter différents modules (Figure B.4).

Pour ajouter un module à un routeur, il faut le faire dans cet ordre :

- Mettre hors tension le routeur ;
- Glisser le module dans l'emplacement prévu à cet effet (la figure B.4 illustre un exemple d'ajout du module WIC-2T) ;
- Remettre en tension le routeur.

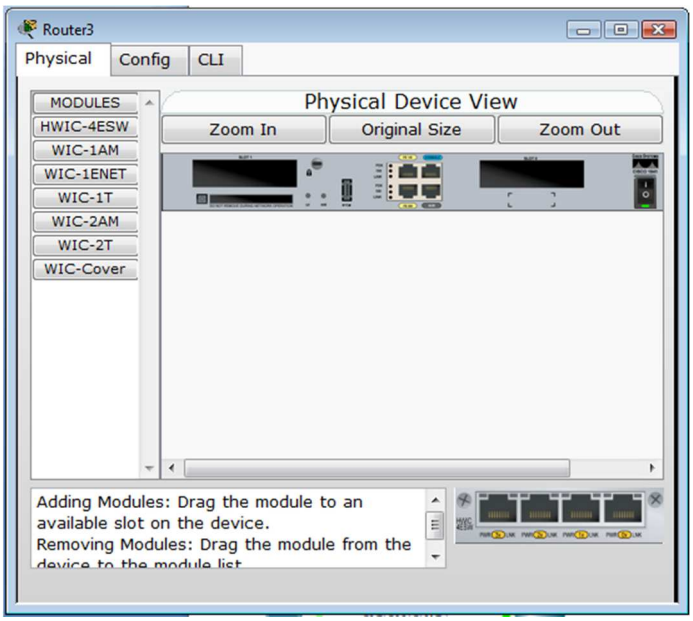
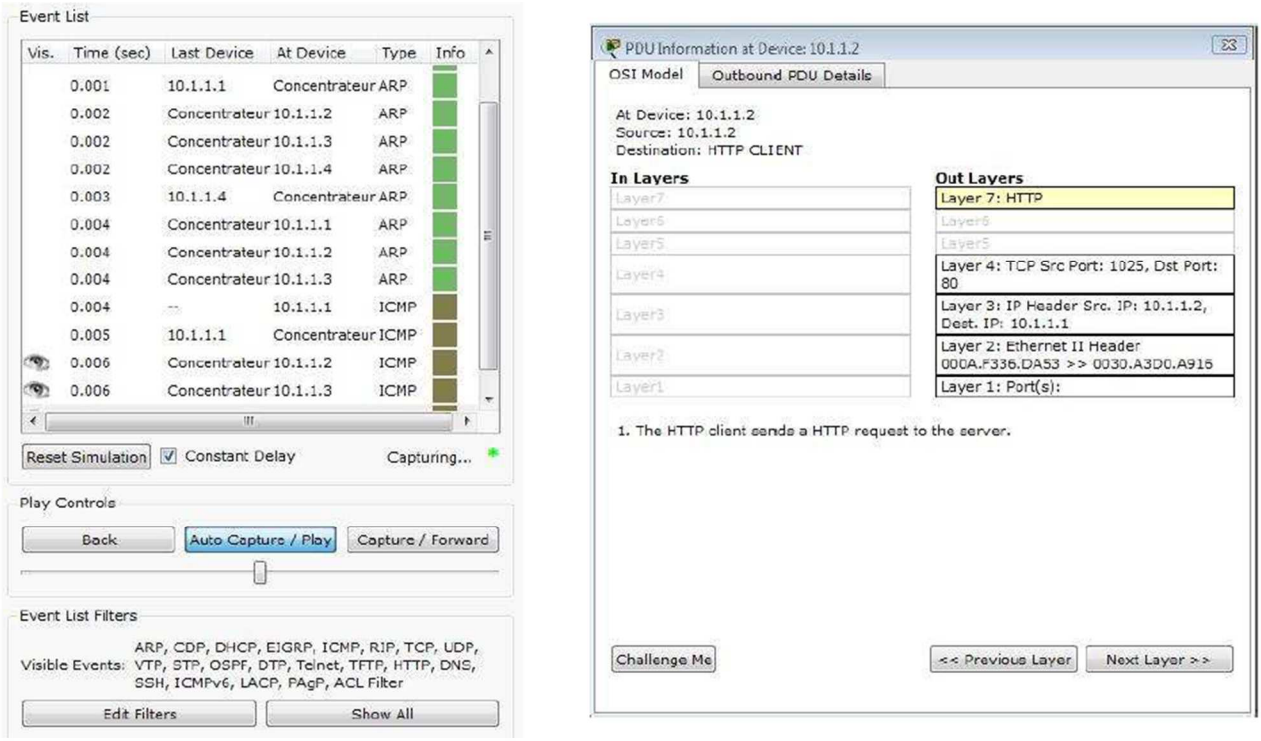


Figure B.4 Ajout du module WIC-2T au routeur

Une fois le routeur ajouté dans le réseau, il reste bien sûr à le configurer (configuration des mots de passe, interfaces, routage, etc.). Pour cela, cliquez sur le routeur et sélectionnez le troisième onglet CLI. C'est au niveau de cet onglet, que vous allez taper les différentes commandes permettant la bonne configuration du routeur.

B.6 Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles, etc. La figure B.5 ci-dessous, à gauche, montre la partie simulation, et à droite, montre les détails que l'on obtient en cliquant sur un message (ici HTTP).



Partie simulation ***(a)*** *Détails sur un paquet* ***(b)***

Figure B.5 Mode simulation