الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 1945 Guelma

Faculté des Sciences et de la Technologie
Département d'électronique et Télécommunications

Brochure de Travaux Pratiques pour la Matière

TP Réseau Informatiques Locaux

Pour 3ème année Télécommunications
(Semestre 06 Unité d'enseignement UEM 3.2)

Préparé par

Dr. IKNI Samir

Année universitaire 2019/2020

Avant-propos

Ce polycopié de travaux pratiques est destiné aux étudiants de troisième année Licence Télécommunications (Intitulé de la matière dans le canevas : TP Réseaux informatiques locaux), ainsi qu'aux étudiants de troisième année Licence Electronique (Intitulé de la matière dans le canevas : TP Signal et Réseaux locaux).

Les travaux pratiques proposés dans ce polycopié sont basés principalement sur ce qui il y a comme matériels, équipements et manuels dans le laboratoire de Télécommunications au sien du département d'électronique et Télécommunications-Université 8 Mai 1945 Guelma.

L'objectif principal de ce polycopié est de mettre à la disposition des étudiants une brochure de manipulation avec des rappels de cours pour servir et faciliter la mise en pratique des expériences abordées durant les séances de TP. Chaque binôme doit remettre un compte-rendu après avoir fait toutes les manipulations. Le rapport doit comprendre des réponses aux questions et des commentaires sur chaque résultat trouvé. L'évaluation du travail sera sur le rapport comme 40 %, plus un examen à la fin du semestre sur 60 %. Les travaux pratiques proposés nécessitent des connaissances de base en ce qui concerne l'outil informatique et les systèmes de communication.

Sommaire

TP N°01 : Réalisation et tests de Câbles RJ45 ou à paire torsadée

I.1. Objectif de TP ……..01

I.2. Rappels théoriques……...……01

***I.2.1. Introduction*……01**

***I.2.2. Câbles à paires torsadées* ……01**

***I.2.3. Le connecteur RJ45*…….……03**

I.3. Partie pratique …….……07

I.3.1. Matériel utilisé dans ce TP*……..……*07

I.3.2. Réalisation d'un câble droit*…….……*07

I.4. Quelques questions pour conclure……12

TP N°02 : Mise en œuvre d'un réseau poste à poste entre deux PC

II.1. Objectif du TP……13

II.2. Partie théorique …….13

II.2.1. Introduction*……..……...*13

II.2.2. Architecture « client-serveur »…….13

II.2.3. Présentation de l'architecture d'égal à égal……..……...14

II.3. Partie pratique…….……15

II.3.1. Matériel utilisé……..….……15

II.3.2. Réseau poste à poste câblé……..……...15

II.3.3. Réseau poste à poste sans fil…….…....18

II.4. Quelques questions pour conclure …….…..20

TP N°03 : Configuration et mise en œuvre d'un réseau à plusieurs postes

III.1. Objectif du TP……..……*21*

III.2. Partie théorique……..…….21

III.2.1. Introduction ……...21

III.2.2. Carte réseau ou Interface réseau……...21

III.2.3. Protocoles de communication……..…….23

III.2.4. Adressage IPv4 …….……24

III.3. Partie pratique ……25

III.3.1. Matériel utilisé dans ce TP……25

III.3.2. Etablissement des liaisons physiques du réseau…….……..26

III.3.3. Configuration de la carte réseau ……..……...28

III.3.4. Test de connectivité entre les postes……..29

III.4. Quelques questions pour conclure ……31

TP N°04: Réalisation d'un réseau Wi-Fi et configuration d'un point d'accès

IV.1. Objectif du TP……..…….32

IV.2. Partie théorique……..……..32

IV.2.1. Introduction ……..32

IV.2.2. Mise en place d'un réseau WiFi …….……..33

IV.2.3. Topologie d'un réseau sans fil……...34

IV.2.4. Sécurité d'un réseau WiFi…….…….35

IV.3. Partie pratique……...……..36

IV.3.1. Matériel utilisé dans ce TP…….36

IV.3.2. Configuration du point d'accès…….……...36

IV.3.3. Test de connectivité ……..……39

IV.4. Quelques questions pour conclure ……..……40

TP N°05 : Fonctionnement des protocoles TCP/IP (utilisation de WireShark)

V.1. Objectif du TP……..…..…..……41

V.2. Partie théorique……..……..41

V.2.1. Introduction ……..……...41

V.2.2. Processus d'encapsulation ……..……..42

V.2.3. Format d'un paquet et d'une trame……..……43

V.2.4. Le logiciel analyseur de trames (Wireshark)…….…..….…….45

V.3. Partie pratique……..……...…….47

V.3.1. Analyse des trames ARP et ICMP…….……..47

V.3.2. Analyse d'une trame de données, TCP et http……..50

V.4. Quelques questions pour conclure…….52

TP N°01

Réalisation et test de Câbles RJ-45 ou à paires torsadées

(Croisé, Droit)

I.1. Objectif du TP

Découvrir les caractéristiques physiques d'un câble à paires torsadées. Apprendre à l'étudiant de réaliser des câbles réseau que ce soit de type droit ou de type croisé. Déterminer les différentes applications de chaque type de câble. Tester le câble à paire torsadées et identifier les genres de défaillances possibles.

I.2. Rappels théoriques

I.2.1. Introduction :

Un réseau informatique est constitué par un certain nombre d'ordinateurs et d'équipements informatiques qui sont interconnectés par des supports de transmission. Ces derniers peuvent être des câbles métalliques, des câbles en fibre optique, ou des ondes électromagnétiques (sans fil). Dans le cas des réseaux câblés on utilise des câbles dits à paires torsadées fabriqués à base de cuivre car ils sont moins couteux, faciles à installer et ils présentent une faible résistance au courant électrique.

I.2.2. Câbles à paires torsadées

Les câbles utilisés dans les réseaux informatiques sont de type : paires torsadées. Chaque deux fils conducteurs à l'intérieur du câble sont enroulés en hélice l'un autour de l'autre (voir la figure I.1). Cette configuration a pour but principal de limiter la sensibilité à la diaphonie (les effets des fils entre eux). En effet, lorsque la ligne est courte, la diaphonie est de toute façon faible. Lorsque la ligne est longue, les paires se trouvent tantôt en phase, tantôt en opposition de phase, annulant donc leurs effets. Le nombre moyen de torsades par mètre fait partie de la spécification du câble. Chaque paire d'un câble est torsadée de manière légèrement différente pour éviter la diaphonie **[1]**.

Figure I.1 : câble à paires torsadées

Pour limiter encore les interférences, les paires torsadées sont souvent blindées. Le blindage peut être appliqué individuellement aux paires, ou à l'ensemble formé par celles-ci. Lorsque le blindage est appliqué à l'ensemble des paires, on parle d'écrantage. Selon ce dernier point, on peut distinguer plusieurs types de paires torsadées **[2]** :

- Paire torsadée non blindée : Unshielded twisted pair (UTP). La paire torsadée non blindée n'est entourée d'aucun blindage protecteur.

- Paire torsadée écrantée : Foiled twisted pair (FTP). L'ensemble des paires torsadées a un blindage global assuré par une feuille d'aluminium. L'écran est disposé entre la gaine extérieure et les 4 paires torsadées. Les paires torsadées ne sont pas individuellement blindées.

- Paire torsadée blindée : Shielded twisted pair (STP). Chaque paire torsadée blindée est entourée d'un feuillard en aluminium, de façon similaire à un câble coaxial.

- Paire torsadée doublement écrantée : Foiled foiled twisted pair (FFTP). Chaque paire torsadée est entourée d'une feuille de blindage en aluminium. L'ensemble des paires torsadées a une feuille de blindage collectif en aluminium.

- Paire torsadée écrantée et blindée : Shielded foiled twisted pair (SFTP). Câble doté d'un double écran (feuille métallisée et tresse) commun à l'ensemble des paires. Les paires torsadées ne sont pas individuellement blindées (contrairement à ce que le terme Shielded foiled twisted pair pourrait faire croire).

- Paire torsadée super blindée : Super Shielded Twisted Pair (SSTP). Chacune des paires est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé.

D'autre part, cette configuration torsadée a pour but de maintenir précisément la distance entre fils de la même paire ce qui permet de définir une impédance caractéristique de la paire, afin de supprimer les réflexions de signaux en bout de ligne. Ainsi, pour des caractéristiques géométriques (épaisseur de l'isolant/diamètre du fil) bien spécifiées, cette impédance est maintenue autour de 100 ohms **[1]**.

Caractéristiques physiques de la paire torsadée :

Le tableau ci-dessous résume les différentes caractéristiques physiques des câbles à paires torsadées qui sont actuellement utilisés et qui ont comme connecteurs RJ-45 **[1]**.

Tableau I.1 : Caractéristiques physiques des câbles RJ-45

Catégorie	*Débit (Mbps)*	*Fréq max MHz*	*Application*
5	100-155	100	100Base-TX, ATM
5e	1000	100	Gigabit Ethernet
6	1000	250	1000Base-TX
6a	10000	500	10GBase-T

I.2.3. Le connecteur RJ45

Les câbles à paires torsadées sont utilisés pour interconnecter des nœuds d'un réseau local (LAN) et des périphériques d'infrastructure tels que des commutateurs (Switchs), des routeurs et des points d'accès sans fil. Le type de connexion et les périphériques associés possèdent des exigences de câblage précisées par les normes de la couche physique. Diverses normes de

couche physique spécifient l'utilisation de différents connecteurs. Ces normes définissent les dimensions mécaniques des connecteurs et les propriétés électriques acceptables de chaque type. Le connecteur RJ45 est largement employé dans les réseaux locaux avec un support de type « à paires torsadées ». Dans ce TP, un câble de réseau local de type UTP sera réalisé en suivant la norme précisée par l'organisation américaine de normalisation : TIA/EIA (Electronic Industry Association/Telecommunications Industry Association). Cette norme, appelée TIA/EIA-568A ou TIA/EIA-568B, donne l'ordre de structuration des fils au niveau du connecteur RJ45. Même si ces deux normes sont similaires, la norme T568A est principalement utilisée dans le domaine du résidentiel (souvent avec du câblage simple non blindé de type UTP) alors que la norme T568B est plutôt employée dans le domaine professionnel (avec du câblage blindé de type STP) **[2]**.

Chaque extrémité de ce câble à paires torsadées est un connecteur de type RJ45. Un tel connecteur est un dispositif de branchement à 8 contacts électriques (broches) qui est utilisé pour les connexions Ethernet sur des cartes d'interfaçage réseau. Ces 8 broches en cuivre sont numérotées de 1 à 8 comme le montre la figure I.2. Lors d'un câblage informatique en 10/100 Mbit/s, seules les quatre broches 1-2 et 3-6 sont utilisées pour transmettre les informations. L'utilisation des 8 broches ensemble est dans le cas d'un câblage en 1 Gbit/s.

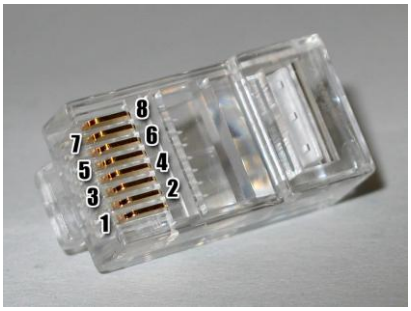

Figure I.2 : Connecteur RJ-45

Deux types de câble seront réalisés dans ce TP : le câble droit (ou direct) et le câble croisé. Le câble direct sert à raccorder des ordinateurs à un commutateur (switch) dans un réseau de topologie en étoile, tandis que le câble croisé sert à raccorder deux ordinateurs directement sans passer par le commutateur pour réaliser un réseau de topologie point à point **[3]**. Dans le

cas du câble droit, les deux extrémités sont identiques et conformes soit à T568A soit à T568B. Dans le cas du câble croisé, l'une des extrémités est conforme à T568A et l'autre T568B. Les deux câbles sont illustrés dans les Tableaux 1 et 2, respectivement.

Tableau .1 : Câble droit (direct) : **[14]**

Connecteur RJ45 câblé suivant T568A		**Connecteur RJ45 câblé suivant T568A**	
Broche	**Couleur**	**Couleur**	**Broche**
1	 Blanc-vert	 Blanc-vert	1
2	 Vert	 Vert	2
3	 Blanc-orange	 Blanc-orange	3
4	 Bleu	 Bleu	4
5	 Blanc-bleu	 Blanc-bleu	5
6	 Orange	 Orange	6
7	 Blanc-marron	 Blanc-marron	7
8	 Marron	 Marron	8

Tableau .2 : Câble croisé : **[14]**

Connecteur RJ45 câblé suivant T568A		**Connecteur RJ45 câblé suivant T568B**	
Broche	**Couleur**	**Couleur**	**Broche**
1	 Blanc-vert	 Blanc-orange	1
2	 Vert	 Orange	2
3	 Blanc-orange	 Blanc-vert	3
4	 Bleu	 Bleu	4
5	 Blanc-bleu	 Blanc-bleu	5
6	 Orange	 Vert	6
7	 Blanc-marron	 Blanc-marron	7
8	 Marron	 Marron	8

I.3. Partie pratique :

I.3.1. Matériel utilisé dans ce TP

- Câble à paires torsadées de type UTP cat 5e.
- Pince à sertir.
- Pince coupante.
- Pince à dénuder
- Connecteurs RJ45
- Testeur de câbles RJ-45

I.3.2. Réalisation d'un câble droit

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

On vous demande de réaliser un câble réseau de type droit. Pour cela, faites suivre, scrupuleusement, les étapes suivantes :

Étape 1

Déterminez la distance entre les équipements ou entre l'équipement et la prise, puis ajoutez au moins 30,48 cm. La longueur de ce câble ne doit pas dépasser 5 m selon les normes de câblage TIA/EIA, mais elle peut être variable. Les longueurs standard sont 1,83 m et 3,05 m. Il suffit d'utiliser un tronçon de 50 - 60 cm juste pour faire le TP.

Étape 2

Dégainez délicatement 3,3 cm d'une extrémité du câble (voir la figure I.3). Faites attention à ne pas couper un fil d'une paire, ceci va conditionner la performance de la connexion.

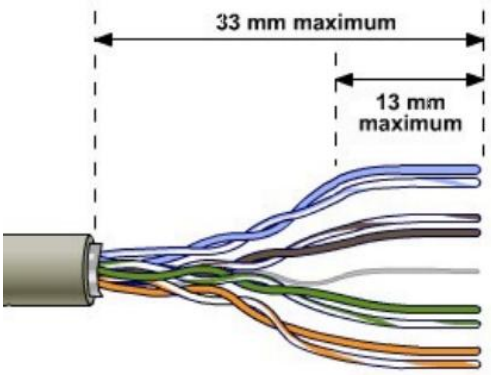

Figure I.3 : Dégainage du câble à paires torsadées

Étape 3

Tenez fermement les quatre paires torsadées à l'endroit où vous les avez dégainées et organisez-les selon la norme de câblage T568A (dans le tableau 1 précédent). Veillez à ce que les torsades restent bien en place, car elles protègent contre le bruit.

Étape 4

Aplatissez, redressez et alignez les fils, puis coupez-les de façon droite à 1,25 cm minimum et à 1,9 cm maximum du bord de la gaine. Veillez à ne pas relâcher la gaine et les fils afin de ne pas désorganiser les paires. Réduisez autant que possible la longueur des fils non torsadés, car des sections trop longues à proximité des connecteurs constituent une source de bruit électrique.

Q1 : Peut-on faire cette dernière opération avec la norme T568B ? Expliquez ?

Réponse :

……

……

……..

Q2 : Quel est le risque qu'on peut voir si la coupe des fils n'est pas droite ?

Réponse :

……

……

Q3 : D'où vient le risque de parasite électrique ? Expliquez ?

Réponse :

……

……

……...

Étape 5

Insérez délicatement les fils dans la fiche RJ-45 jusqu'à ce que vous aperceviez les extrémités de cuivre des fils de l'autre côté de la fiche, veillez à ce que l'ordre des fils reste inchangé et que les bouts des fils atteignent la butée du connecteur RJ-45. La face des broches en cuivre du connecteur doit être devant vous et la broche en dessus soit la paire verte. Si la gaine n'est pas fermement insérée dans la fiche, elle risque de provoquer des problèmes de connexion.

Étape 6

Si tout est correct, faites entrer la fiche RJ-45 dans la pince à sertir et sertissez solidement de manière à faire pénétrer des contacts dans l'isolation des fils et d'assurer ainsi une bonne connexion entre les fils et les broches du connecteur (voir la figure I.4).

Figure I.4: Sertissage d'un câble RJ-45

NB : Demandez à votre professeur de vérifier avant de sertir, sinon vous risquez de gâcher la fiche RJ-45 en cas d'erreur.

Étape 7

Pour tester le câble, on utilise un testeur de câble qui est un dispositif électronique ayant deux ports RJ-45, où l'une des extrémités est branchée sur le premier et l'autre sur le deuxième. En enfonçant le bouton TEST, l'appareil commence à tester les fils un par un et indique par des voyants (des LEDs) numérotés de 1 à 8, si la connexion est bonne pour tous les fils ou s'il y a une certaine défaillance (voir la figure I.5 ci dessous).

Figure I.5 : Testeur de câble RJ-45

Q4 : Expliquez, à travers le tableau ci-dessous, les résultats de test dans les différentes situations suivantes :

Etats des voyants (LEDs)	*Défaillant/Saint*	*Donnez une explication*
La paire de voyants (LEDs) N° 4 ne s'allume pas		
Sur la paire N° 5, la LED gauche est allumée et la LED droite ne s'allume pas		
La LED gauche sur la paire N°7 s'allume en même temps que la LED droite sur la paire N°8, et La LED gauche sur la paire N°8 s'allume en même temps que la LED droite sur la paire N°7		
Toutes les LED s'allument deux par deux (paire) cycliquement		
Aucune paire ne s'allume		

Q5 : D'après le tableau ci-avant, combien de défaillances peuvent être indiquées par un tel testeur de câbles ?

Réponse : …….

Q6 : Donnez le résultat de test qui correspond à la situation d'un câble croisé saint.

Réponse :

……

……

……

I.4. Quelques questions pour conclure :

1. Que doit-on faire si on veut réaliser un câble réseau croisé ? citez les étapes.
2. Dans quelle situation est utilisé chaque type de câble ?
3. Existe-t-il une autre norme d'arranger les fils du câble à paires torsadées ?
4. Faites une conclusion générale sur ce que vous avez manipulé dans ce TP.

TP N°02

Mise en œuvre d'un réseau poste à poste entre deux PC

(Adressage IP, Partage de dossiers)

II.1. Objectif du TP

Apprendre à établir une liaison physique entre deux postes reliés en réseau ad-hoc suivant le mode de fonctionnement « égal-à-égal ». Configurer les interfaces réseau de façon à établir une communication entre les deux postes. Utiliser des commandes MS-DOS pour tester le fonctionnement du réseau et apprendre à partager des fichiers et des périphériques.

II.2. Rappels théoriques

II.2.1. Introduction

Les réseaux ad-hoc ont une architecture qui s'appelle égal-à-égal. Cette architecture stipule que chacun des deux postes peut être un client et un serveur en même temps. Dans un tel réseau on a la possibilité de relier deux machines sans avoir besoin d'une infrastructure préexistante, comme des routeurs dans les réseaux filaires ou des points d'accès dans les réseaux sans fil. Dans le système d'exploitation Windows, il est très facile d'installer un réseau poste-à-poste qui permet aux 2 ordinateurs de communiquer directement entre eux sans avoir besoin de passer par un commutateur. Il est alors possible de partager une liaison internet ou des périphériques et des données **[4]**.

II.2.2. Architecture « client-serveur »

L'environnement client-serveur désigne un mode de communication à travers un réseau entre plusieurs programmes : l'un, qualifié de ***client***, envoie des requêtes pour demander des services, donc c'est un consommateur de service. Tandis que l'autre ou les autres, qualifiés de ***serveurs***, attendent les requêtes des clients et y répondent, ce sont donc des fournisseurs de services (voir la figure II.1).

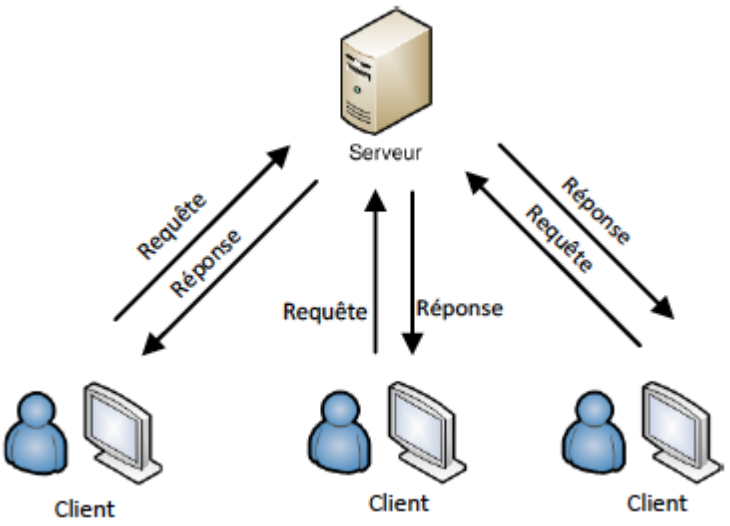

Figure V.1 : Architecture Client-serveur

II.2.3. Architecture « égal à égal »

Dans une architecture d'égal-à-égal (en anglais *peer to peer*), contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau joue le rôle d'un serveur et d'un client en même temps. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante ou une liaison internet pourra donc éventuellement la partager afin que les autres ordinateurs puissent y accéder via le réseau **[3]**.

Dans le cas d'un réseau filaire, l'architecture et limitée à 2 postes par réseau, car une carte réseau filaire n'a qu'un seul port RJ-45.

Dans le cas d'un réseau sans fil, on peut raccorder plusieurs postes par une topologie qui est physiquement en étoile et logiquement en égal-à-égal (ad-hoc sans fil). Ceci est possible si tous les postes sont reliés deux à deux en point-à-point. Dans ce cas, chaque nœud participe au routage en retransmettant les données aux autres nœuds, de façon à ce que le choix du nœud qui va transmettre les données est opéré dynamiquement sur la base de la connectivité du réseau et d'un certain algorithme de routage.

Les réseaux sans fil ad hoc sont des réseaux auto-configurant et dynamiques dans lesquelles les nœuds sont libres de se déplacer. Les réseaux sans fil ne souffrent pas des complexités liées à la configuration et à l'administration d'infrastructures, permettant ainsi aux appareils de créer et joindre des réseaux d'une manière souple et facile **[4]**.

II.3. Partie pratique

II.3.1. Matériel utilisé

On se propose de réaliser 03 réseaux Poste-à-Poste, dans les deux cas : réseau câblé et réseau sans fil, pour cela on doit disposer des équipements suivants :

- 06 Ordinateurs avec Système d'exploitation (de préférence Windows 7), avec protocoles TCP/IP qui soient bien installés (dans le cas de Windows 7 ils sont présents par défaut).
- Des cartes réseau Ethernet 10/100 Mbit/s (interface réseau) bien installée.
- Des cartes réseau sans fil (WiFi) avec pilotes bien installés.
- Des câbles réseaux de type croisé UTP cat 5e (crossover cable).

II.3.2. Réseau poste à poste câblé

Chaque binôme d'étudiant réalise un réseau à deux postes. Pour cela, il suffit d'utiliser les câbles RJ-45 croisés pour raccorder chaque paire d'ordinateurs directement de la carte réseau à la carte réseau comme illustré dans la figure II.2. Pour vos réseaux faites entrer des adresses de classe C pour chaque ordinateur (la même configuration pour les trois réseaux est possible puisque ils sont séparés l'un de l'autre), soit :

- ✓ Adresse IP ordinateur PC1: ***192.168.10.5***
- ✓ Adresse IP ordinateur PC2: ***192.168.10.10***

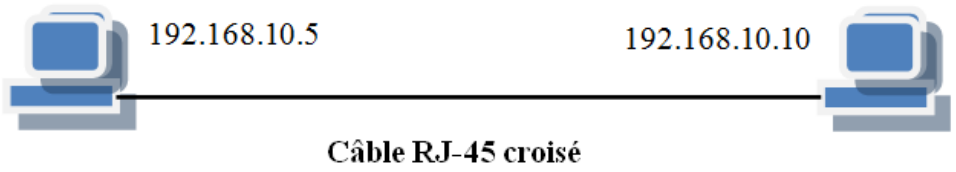

Figure II.2 : Réseau câblé poste à poste

En utilisant l'adresse ***127.0.0.1*** vérifiez que les protocoles TCP/IP sont bien installés et la carte réseau est bien reconnue.

- Recopiez la réponse obtenue sur votre compte rendu

……
……
……

- Refaites le test avec câble débranché, qu'est ce que vous constatez ?

……
……

Remarque : Dans les paramètres du système d'exploitation il faut vérifier le « Groupe de travail », il doit être identique sur les 2 postes. En effet, pour faire partie du même réseau, les ordinateurs doivent faire parti du même groupe de travail.

Test du réseau poste à poste câblé

- *La commande ping*

Pour tester les liaisons entre les différents postes, vous utiliserez la commande DOS « **ping** ». Cette commande Ping correspond à l'envoi d'une trame (paquet de données) à l'adresse IP choisie. Si le système qui se trouve à cette adresse est présent sur le réseau, il renvoi la même trame à son expéditeur. Cela permet de vérifier la connexion entre les deux.

Syntaxe : **ping @_IP_destinataire**

- Recopiez la réponse obtenue sur votre compte rendu

……
……
……

- Refaites le test avec câble débranché, d'où vient cette réponse alors que le câble est débranché ? faites vos commentaires.

……
……
…….

- *La commande ipconfig /all*

Dans une fenêtre de commande, taper « ipconfig /all ». Cette commande permet de renvoyer à l'écran l'ensemble des paramètres de configuration réseau présent sur votre PC.

Relevez sur votre feuille les informations suivantes :

- Nom d'hôte de votre machine : ……..

- Adresse physique MAC de votre carte réseau : ……

- Adresse IP de votre machine : ……..

- Masque de sous réseau : ……

- *Visualisation des postes*

Pour vérifier que les 2 postes sont visibles et donc accessibles sur les deux côtés, allez-vous sur le chemin :

Centre Réseau et partage/Afficher les ordinateurs et périphériques réseau

Les deux postes sont-ils visibles sur les deux PC ? …… (oui/non)

Si non, tapez dans la barre d'adresse :

\\nom_autre_ordinateur ou \\@IP_autre_ordinateur

Partage d'un fichier ou d'un périphérique :

Créez un dossier nommé **Docs_Partagé1** sur **PC1** et **Docs_Partagé2** sur **PC2** dans le dossier :

C:\Utilisateurs\Public\Documents publics

Créez un fichier texte dans le dossier ainsi créé. Dans le menu contextuel de ce dossier, procédez à le partager (partage simple ou avancé).

Via le bouton ***Autorisations*** vous accédez aux droits à attribuer aux utilisateurs qui accèdent à ce partage via le réseau (laisser les autorisations par défaut).

Une fois partagé, essayez de récupérer le fichier Sur l'autre poste et de le modifier.

Q1 : Quel est le message que vous signale le système ? Pouvez-vous l'ouvrir ? Le supprimer ? Le modifier ? Faites vos commentaires.

Réponse :

……

……

……

II.3.3. Réseau poste à poste sans fil

Débranchez les câbles des cartes réseau et activez la liaison sans fil de votre ordinateur.

Utilisez la même configuration précédente (il est préférable de donner des adresses IP différentes sur chacun des 6 ordinateurs pour éviter la confusion).

Sur chaque paire d'ordinateur, suivre les étapes suivantes :

- Sur le premier ordinateur, créez une liaison sans fil en allant sur le chemin :

Centre Réseau et partage/Gérer les réseaux sans fil/Ajouter/Créer un réseau ad hoc

Recopiez, ci-dessous, les informations indiquées sur la fenêtre qui s'affiche :

……

……

……..

Cliquez sur 'Suivant' puis saisissez les paramètres demandés :

Nom de réseau : *Labo1P2Pwifi*

Type de sécurité : *WPA2*

Clé de sécurité : *12345678 (plus simple et mémorisable)*

- Sur le deuxième ordinateur, vous détectez le SSID ainsi créé, essayez de vous y connecter.

Q1 : Y a-t-il un signe de connexion ? …… (oui/non)

Si non, revérifiez votre configuration (avec l'enseignant).

Si oui, refaire les étapes de test précédentes dans ce qui suit :

Test du réseau poste à poste sans fil

- *La commande ping*

Syntaxe : **ping @_IP_destinataire**

- Recopiez la réponse obtenue sur votre compte rendu

……

……

……

- *La commande ipconfig /all*

Relevez sur votre feuille les informations suivantes :

- Nom d'hôte de votre machine : ……..

- Adresse physique MAC de votre carte réseau : ……

- Adresse IP de votre machine : ……..

- Masque de sous réseau : ……

- *Visualisation des postes*

Q2 : Les deux postes sont-ils visibles et accessibles sur les deux PC ?

…… (oui/non)

Si oui, le réseau est bien configuré et fonctionne bien.

Si non, donnez votre diagnostic et suggérez une solution :

……
……
……

II.4. Quelques questions pour conclure :

1- Peut-on remplacer le câble croisé par un câble droit ? Pourquoi ?
2- A quoi sert le croisement dans le câble croisé ?
3- Quelle est l'utilité d'un réseau poste à poste et sa limitation ?
4- Si on veut autoriser quelqu'un à se connecter à notre réseau WiFi, que doit-on faire ?
5- Faites une conclusion générale du TP.

TP N°03

Configuration et mise en œuvre d'un réseau à plusieurs postes avec commutateurs

(Adressage IP, tests avec ipconfig, ping, arp, tracert, … etc.)

III.1. Objectif du TP

Apprendre à établir les liaisons physiques entre les différents postes du réseau et les périphériques. Configurer les ordinateurs de façon à établir une communication entre eux. Utiliser les commandes de base pour tester le réseau établi.

III.2. Rappels théoriques

III.2.1. 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 « 1 » imprimante par ordinateur (coût), soit déplacer l'imprimante sur le poste à imprimer, ou copier / coller les fichiers sur un support amovible et faire le transfert sur le poste où se trouve l'imprimante (perte de temps).

Avec le réseau, tout devient plus simple, mais encore faut-il savoir comment établir une liaison physique entre des ordinateurs et réaliser la configuration logicielle afin que ces ordinateurs puissent communiquer entre eux **[3]**.

III.2.2. Carte réseau ou Interface réseau

La carte réseau (NIC : Network Interface Card) constitue l'interface entre l'ordinateur et le réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau **[2]**.

La carte réseau possède généralement deux témoins lumineux (LEDs) :

- La LED verte indique l'alimentation de la carte ;
- La LED orange (10 Mb/s) ou rouge (100 Mb/s) indique une activité du réseau (émission/réception).

On distingue deux types de carte réseau : sans fil ou Wi-Fi (à gauche de la figure III.1) et filaire ou RJ-45 (à droite de la figure).

Figure III.1 : Cartes réseau

Pour préparer les données à envoyer, la carte réseau utilise un 'transceiver' qui transforme les données parallèles en données séries. Chaque carte dispose d'une adresse unique, appelée adresse MAC (Media Access Control), affectée par le constructeur de la carte, ce qui lui permet d'être identifiée de façon unique dans le monde.

Le rôle principal de la carte réseau est de préparer pour le câble réseau les données émises par l'ordinateur, de les transférer vers un autre ordinateur puis de contrôler le flux de données entre l'ordinateur et le câble. Elle traduit aussi les données venant du câble et les traduit en octets afin que l'Unité Centrale de l'ordinateur les comprenne.

La carte réseau sert aussi à restructurer les données arrivant en parallèle en données circulant en série (bit par bit). Pour cela, les signaux numériques sont convertis en un signal électrique ou optique (adapté à la nature du support) qui peut être transporté par le câble réseau. Le dispositif chargé de cette conversion est le *Transceiver* **[2]**.

Avant tout échange de données entre les ordinateurs, leurs cartes réseau effectuent un dialogue électronique pour s'accorder sur plusieurs règles de communication qu'on appelle : protocoles de communication, comme par exemple **[7]**:

- ✓ Taille maximale des blocs de données à envoyer
- ✓ Volume de données à envoyer avant confirmation de réception
- ✓ Intervalles de temps entre les transmissions partielles de données
- ✓ Délai d'attente avant envoi de la confirmation de réception
- ✓ Vitesse de transmission des données

III.2.3. Protocoles de communication

Pour que deux machines puissent échanger de l'information, il faut qu'elles établissent une liaison entre elles et utilisent le même protocole de communication. Un protocole est un langage qui permet aux périphériques d'un réseau de communiquer en utilisant les mêmes règles de communication, il constitue un langage entre machines **[5]**.

Le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) est le protocole utilisé sur les réseaux locaux (LAN). Il représente aussi l'ensemble des règles de communication utilisées sur Internet et se base sur la notion d'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Les protocoles TCP/IP ont été conçus pour répondre à un certain nombre de critères parmi lesquels :

- ✓ Le découpage des messages en paquets de petite taille
- ✓ L'utilisation d'un système d'adressage
- ✓ L'acheminement des données sur le réseau (routage)
- ✓ La détection/correction des erreurs de transmission de données

Le modèle TCP/IP, comparé au modèle OSI (en 7 couches), reprend l'approche modulaire (structure en couches) mais en contient uniquement quatre **[5][6]** :

- Couche Accès réseau : elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé en suivant un protocole spécifié (Ethernet, PPP, FDDI, …).
- Couche Internet : elle est chargée de construire le paquet de données (datagramme) et de routage à travers les nœuds du réseau suivant un système d'adressage IP.
- Couche Transport : elle assure le transport de données de bout en bout de façon fiable (protocole TCP) ou non fiable (protocole UDP).
- Couche Application : elle regroupe les applications standards du réseau (http, Telnet, SMTP, FTP, ...) Voici les principaux protocoles faisant partie de la suite TCP/IP :

III.2.4. Adressage IPv4

Sur un réseau (Internet par éxemple), les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 séparés par des points. On appelle cette forme la notation décimale pointée. Par exemple 194.153.205.26 est une adresse IP valide. Chaque ordinateur sur le réseau possède une adresse IP unique. C'est l'ICANN (Internet Corporation for Assigned Names and Numbers) qui est chargée d'attribuer des adresses IP des ordinateurs directement connectés sur le réseau public internet. On distingue en fait deux parties dans l'adresse IP **[8]**:

- ✓ Une partie des nombres à gauche désigne le réseau et est appelée net-ID.
- ✓ Les nombres de droite désignent les ordinateurs de ce réseau et est appelée host-ID.

Ainsi, le net-ID est utilisé pour localiser un sous réseau sur un grand réseau (Internet par exemple), puis le host-ID sera utilisé pour désigner une machine dans ce sous réseau.

Les Classes réseau :

Afin que la répartition des octets entre partie réseau et partie hôte corresponde aussi bien aux besoins de vastes réseaux qu'à ceux de petits, trois classes d'adresse ont été créées, comme l'illustre le tableau III.1.

Tableau III.1 : Les Classes d'adressage réseau

Classe	Plage de valeurs	Masque de sous-réseau	Nombre de réseaux	Nom d'hôtes
A	1 – 126	255.0.0.0	126	16 777 214
B	128 – 191	255.255.0.0	16 384	65 534
C	192 – 223	255.255.255.0	2 097 151	254

Affectation des adresses IP :

On distingue deux situations pour assigner une adresse IP à un équipement **[8]**:

- de manière statique : l'adresse est fixe et configurée manuellement.
- de manière dynamique : l'adresse est automatiquement assignée grâce au protocole DHCP (*Dynamic Host ConfigurationProtocol*).

Les ordinateurs au sein d'un réseau se reconnaissent tout d'abord par leurs adresses physiques (MAC : Media Access Control) en diffusant une requête de type ARP (Address Resolution Protocol) vers toutes les machines qui se trouvent sur le réseau **[9]**.

III.3. Partie pratique :

III.3.1. Matériel utilisé dans ce TP

On se propose de réaliser un réseau de 6 postes avec une topologie en étoile. Pour cela on dispose des éléments suivants :

1. Ordinateurs avec Système d'exploitation (de préférence Windows 7), avec protocoles TCP/IP qui soient bien installés (dans le cas de Windows 7 ils sont présents par défaut).
2. Un commutateur (switch) à 8 ports ou plus.
3. Câbles réseau de type direct UTP cat 5e (patch cable).

III.3.2. Etablissement des liaisons physiques du réseau

Sur votre poste, allez-vous sur :

'Panneau de configuration\Réseau et Internet\Connexions réseau'

Puis, ouvrirez les propriétés de votre « connexion au réseau local».

Q1 : Les cases sont-elles cochées ? Réponse : ……. (oui/non)

Q2 : Quelle est la signification de ces cases cochées ?

Réponse :

……

……

Q2 : Que doit-on faire si elles ne sont pas cochées ?

Réponse :

……

……..

Repérer la présence physique de la carte réseau sur l'unité centrale.

Q3 : La carte réseau est-elle présente ? Réponse : ……. (oui/non)

Vérifier maintenant qu'elle est installée sur votre système en allant sur **« Gestionnaire des périphériques ».**

Q4 : Que doit-on faire si elle n'est pas installée ?

Réponse :

……

……

En utilisant la commande ***ping*** et l'adresse de la machine locale : 127.0.0.1 vérifiez la liaison interne entre la machine et la carte réseau.

Q5 : Que pouvez-vous constater ? Refaire l'expérience à liaison WiFi désactivée, même question ?

Réponse :

……

……

En utilisant les câbles réseau et le commutateur (switch) réalisez la configuration physique du réseau à 6 poste de la figure III.2 suivante :

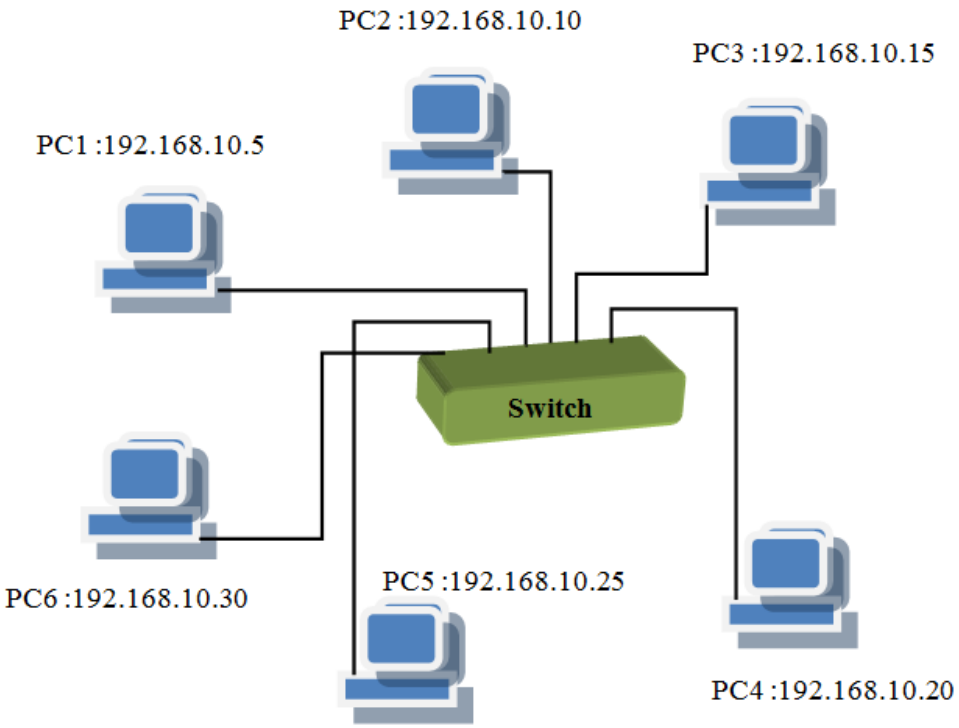

Figure III.2 : Câblage d'un réseau à 6 postes

III.3.3. Configuration de la carte réseau

Le réseau ainsi établi ne permet pas un échange de données pour le moment. Pour que la communication soit possible, on doit configurer tous les postes en leur affectant des adresses IP comme suit :

N° de Poste	Adresse IP affectée
PC1	192.168.10.5
PC2	192.168.10.10
PC3	192.168.10.15
PC4	192.168.10.20
PC5	192.168.10.25
Pc6	192.168.10.30

Le masque réseau est mis automatiquement à : **255.255.255.0**

Q6 : Que signifie ce masque réseau et pourquoi il est mis à cette valeur automatiquement ?

Réponse :

……

……

……

……

Q7 : Quelle est l'adresse réseau de notre réseau et comment peut-on la calculer ?

Réponse :

……

……

……

Q8 : Peut-on raccorder d'autres postes à ce réseau ? si oui, quel est le nombre maximum de postes qu'on peut raccorder ?

Réponse :

……

……

……

Q9 : Essayez de donner une même adresse IP à deux postes différents en même temps. Quel est le résultat ? Tirez une petite conclusion de cette remarque,

Réponse :

……

……

……

NB : Dans les paramètres du système d'exploitation vérifiez le « Groupe de travail », il faut que ce soit identique sur les postes.

III.3.4. Test de connectivité entre les postes

a) La commande ping

Pour tester les liaisons entre les différents postes, vous utilisez l'espace de commande DOS pour lancer la commande « ping » (Packet INternet Groper) ayant la syntaxe suivante :

***ping adresse_IP*.**

Chaque étudiant doit lancer un « ping » aux autres postes à partir de son poste et remplir le tableau ci-dessous en décrivant l'état de connectivité entre les deux postes :

bonne, mauvaise, pas de connexion) :

Poste source de « ping » ***(Le votre)***	***Poste destinataire de « ping »***				
	PC N° :……	PC N° :……	PC N° :……	PC N° :……	PC N° :……
PC N° :……	.....	.....	.....	.....	.....

Recopiez la réponse qu'a renvoyée la commande « ping » sur votre compte-rendu.

……
……
……..

Q10 : Combien d'échanges y a-t-il eu entre les postes ? Quel est le temps moyen d'échanges de données entre les postes ? En résumé, que permet de voir un « ping » ?

Réponse :

……
……
……
……

Refaire le test à câble débranché (au niveau du switch). Recopier la réponse correspondante et faites vos commentaires.

……
……
……..

b) La commande ipconfig

Lancez maintenant la commande « ipconfig /all » sur la fenêtre DOS. Relevez sur votre compte-rendu les informations suivantes :

Nom d'hôte :…… ……

Adresse physique :…….. ……

Adresse IP :……. ……

Masque de sous réseau :…….. ……

Passerelle par défaut :……. ……

Serveur DNS :……. ……

III.4. Quelques questions pour conclure :

1- Quelle est la vitesse de transmission utilisée dans ce réseau ?
2- Si on veut créer deux sous-réseaux dont l'un contient 2 ordinateurs et l'autre regroupe le reste (4 postes), quelle est la bonne reconfiguration pour le faire ?
3- Dans le cas où le protocole DHCP est activé, comment fait-on pour savoir notre adresse IP ?
4- Quel est le rôle d'un serveur DNS ?
5- Faites une conclusion générale du TP.

TP N°04

Réalisation d’un réseau Wi-Fi et configuration d’un point d’accès

(Adressage IP statiques et dynamiques par DHCP, sécurisation du point d’accès, … etc.)

IV.1. Objectif du TP

Apprendre à établir un réseau sans fil de type WiFi reliant plusieurs ordinateurs et périphériques munies de cartes réseau sans fil. Configurer un point d'accès (Access Point) de façon à établir un réseau WiFi offrant la connexion sans fil de plusieurs stations pour effectuer une communication entre elles. Sécuriser un réseau Wi-Fi par différentes méthodes de sécurisation. Utiliser les commandes de base pour tester le réseau WiFi établi.

IV.2. Rappels théoriques

IV.2.1. Introduction :

On distingue habituellement plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité (appelé communément zone de couverture) (voir la figure IV.1) suivante :

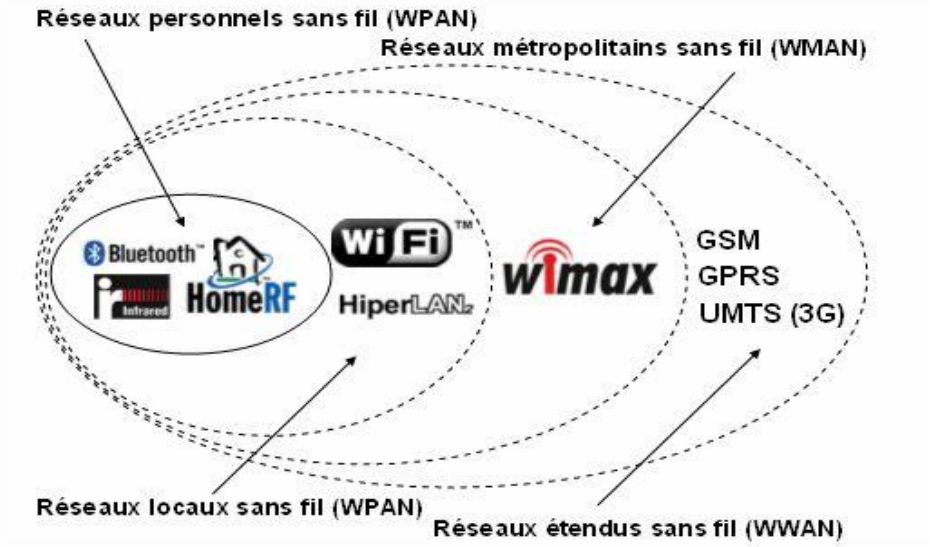

Figure IV.1 : Les Réseaux sans fil

Le WI-FI (Wireless-Fidelity) est une forme de réseau sans fil standardisée par la norme IEEE 802.11 (ISO/IEC 8802-11). La norme 802.11 regroupe quatre catégories **[14]**:

- ✓ Le IEEE 802.11b : Cette norme fonctionne sur la bande de fréquence 2.4 Ghz avec un débit nominal de 11Mbit/s.
- ✓ Le IEEE 802.11a : fonctionne sur 5Ghz et assure un débit nominal de 54 Mbit/s.
- ✓ Le IEEE 802.11g : est une évolution de la 802.11b pour offrir un débit de 54 Mbit/s, sur 2.4Ghz.
- ✓ La norme 802.11f : appelé itinérance (roaming). Elle propose le protocole *Inter-access point roaming protocol* permet à un utilisateur itinérant de changer de point d'accès afin d'obtenir un meilleur débit.

Un réseau Wi-Fi est souvent généré par un point d'accès (assurant le lien avec les stations) et de stations (ordinateur, routeur, Smartphone, modem Internet, etc.) munies de cartes réseau sans fil (Wi-Fi).

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit pour que les stations à proximité du point d'accès puissent se connecter sans avoir besoin de câbles physiques. Dans la pratique le Wi-Fi permet de relier des stations se trouvant sur un rayon de couverture allant jusqu'à plusieurs dizaines de mètres.

IV.2.2. Mise en place d'un réseau WiFi :

Il existe différents équipements pour la mise en place d'un réseau sans fil Wi-Fi, parmi lesquels **[10]**:

- ✓ Les adaptateurs sans fil ou cartes d'accès *(wireless adapters ou network interface controler, noté NIC)* : il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wi-Fi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateurs USB, etc…).

- ✓ Les points d'accès (Access Point en anglais) : dans les réseaux informatiques, un point d'accès est un dispositif électronique qui permet aux périphériques informatiques sans fil de se connecter à un réseau câblé ou au réseau Internet à l'aide d'une connexion radio. Le point d'accès en tant que dispositif autonome est habituellement relié à un routeur (par l'intermédiaire d'un réseau câblé), mais il peut aussi faire partie intégrante du routeur lui-même.

IV.2.3. Topologie d'un réseau sans fil

Une topologie de réseau informatique correspond à l'architecture (physique ou logique) de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux.

Elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau (topologie physique). Elle peut aussi définir la façon dont les données transitent dans les lignes de communication (topologies logiques) **[14]**.

Il existe deux topologies principales dans les réseaux sans fil (Wi-Fi) **[13]**:

- ✓ Le mode ad-hoc : dans ce mode toutes les stations se connectent les unes aux autres, elles sont toutes des points d'accès. Contrairement au mode infrastructure, l'SSID sert à identifier la connexion.

- ✓ Le mode infrastructure : dans ce mode chaque station se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa portée est appelé ensemble de services (SS Service Set). Chaque SS est identifié par un SSID qui sert à identifier le point d'accès (voir figure IV.2).

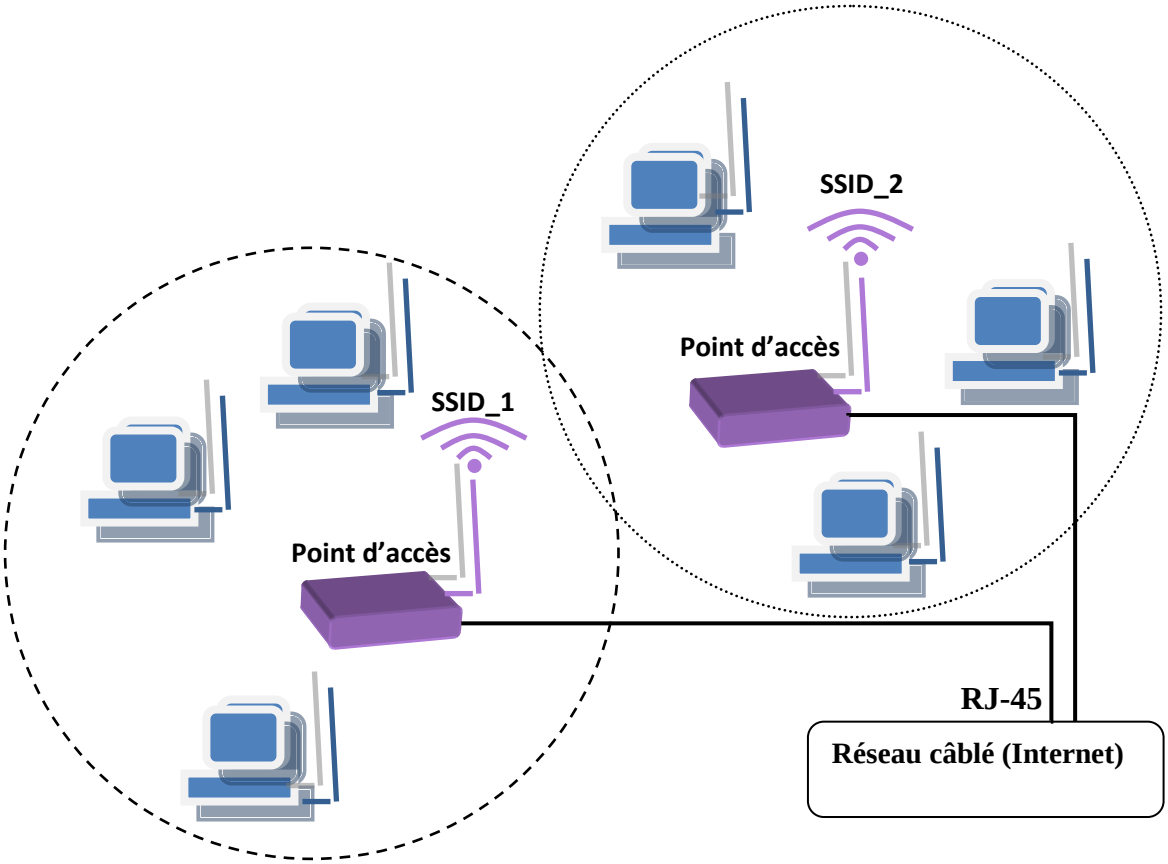

Figure IV.2 : Réseau sans fil (WiFi) à l'aide d'un point d'accès (Infrastructure)

IV.2.4. Sécurité d'un réseau Wi-Fi

Afin d'éviter les intrusions pirates sur le réseau, il est nécessaire de prendre des mesures de sécurité. Deux approches peuvent être mise en œuvre **[8]**.

- *Cryptage WEP*

On a la possibilité de sécuriser le réseau sans fil par un cryptage WEP qui est en fait une clé (suite de 10 ou 26 chiffres en hexadécimal selon le nombre de bits) sur le réseau sans fil. Cette clé peut être crypté sur 64 ou 128 bits, que l'on peut entrer directement en hexadécimal, ou qui

peut être générée automatiquement lorsque l'on entre des caractères. Si l'on défini une clé WEP sur le point d'accès, il faut absolument que ce soit la même clé sur la carte WiFi. Les clés WEP doivent être exactement identiques sur tous les appareils sans fil pour que ceux-ci puissent communiquer entre eux.

- *Filtrage des adresses MAC*

Afin d'accentuer la sécurité du réseau WiFi on peut permettre ou restreindre l'accès de certaines stations par leur adresse MAC. On pourra lors de la configuration, activer un filtrage d'adresses MAC, qui permettra l'accès au réseau sans fil, ou ne le permettra pas. Par l'intermédiaire des adresses MAC des cartes d'accès **[10]**.

IV.3. Partie pratique

IV.3.1. Matériel utilisé dans ce TP

On se propose de réaliser un réseau WiFi de 6 postes avec une topologie infrastructure. Pour cela on dispose du matériel suivant :

- Ordinateurs avec Système d'exploitation (de préférence Windows 7), avec protocoles TCP/IP qui soient bien installés (pour Windows 7, ils sont présents par défaut)
- Cartes réseau sans fil (avec antennes WiFi).
- Point d'accès (en occurrence le Dlink DAP-1360) avec son CD d'installation et son câble de configuration.

IV.3.2. Configuration du point d'accès

Le point d'accès doit être configuré par un seul ordinateur (tâche faite en groupe avec l'enseignant chargé de TP). Voici les étapes de configuration à suivre :

1. Dans un premier temps, il faut configurer le point d'accès. On doit d'abord l'alimenter via son adaptateur sur le réseau électrique puis le relier à un ordinateur par son câble de configuration.

2. Configurez les adresses IP de votre carte réseau de façon statique :

   Adresse IP : *192.168.0.10*

   Masque sous réseau : *255.255.255.0*

   Passerelle par défaut : *192.168.0.50*

3. Lancez votre navigateur web (Mozilla Firefox ou Google Chrome par exemple) et dans la ligne adresse 'URL', taper le nom du point d'accès ou son adresse IP.

   donc taper : **Dlink ou 192.168.0.50**

   NB : Vous pouvez changer l'adresse IP assignée au point d'accès, mais il faut donc charger la page de configuration par la nouvelle adresse.

4. Si le programme demande un nom d'utilisateur et mot de passe saisissez « **admin** » et laissez le mot de passe vide, cliquer sur « **Next** »,

5. Sélectionnez le mode « **Access Point** » puis cliquez sur « **Next** »,

6. Donnez un nom et un mot de passe pour votre réseau WiFi comme suit :

   SSID : *Wifi_Labi1*

   Mot de passe : *123456789*

   puis cliquez sur « **Next** »,

7. Entrer le canal du réseau. Les canaux vont de 1 à 14 selon les points d'accès. Le canal nous donne une plage de fréquence sur lequel émettra le point d'accès.

8. Pour sécuriser votre réseau, choisissez un mode de sécurisation, soit « **WPA2** », un type de chiffrement, soit « AES », et une clé de sécurité partagée « WEP » (soit entre 8 et 63 caractères), utilisez une toute simple clé soit : **12345678**.

9. Enregistrer les modifications par « **Save** ». le point d'accès est donc configuré.

Q1 : Dans l'étape 1, Quel type de câble doit-on utiliser pour la configuration ? pourquoi ?

Réponse :

……

……..

Q2 : Dans l'étape 2, peut-on donner l'adresse 192.168.1.10 à la carte réseau ? pourquoi ?

Réponse :

……

……

Q3 : L'étape 3 exige-t-elle une liaison internet ? pourquoi ?

Réponse :

……

……..

Q4 : Dans l'étape 6, peut-on considérer le SSID comme un premier niveau de sécurité ?

Réponse :

……

……

Q5 : Dans le cas de plusieurs points d'accès, peut-on mettre le même canal pour chacun ? Pourquoi ?

Réponse :

……

……

…….

Q6 : Que doit-on faire pour sécuriser davantage notre point d'accès ?

Réponse :

……

……

……

IV.3.3. Test de connectivité

Sur l'icône en bas de la liaison réseau sans fil, essayez de vous connecter au réseau ainsi établi.

Q7 : La connexion est-t-elle possible ?

Réponse :

……

……..

Vérifiez par la commande « **ping** » la connexion au point d'accès.

Q8 : Quelle est la réponse renvoyée par la commande ping ? Discutez ?

Réponse :

……

……

……

Faites un test à liaison désactivée. Puis réactivée la liaison de nouveau.

Q9 : Que constatez-vous ?

Réponse :

……

……

…….

IV.4. Quelques questions pour conclure :

1- Quelle est l'utilité d'un point d'accès ?
2- Relevez le débit binaire utilisé dans ce réseau ?
3- Peut-on remplacer le point d'accès par un modem ? pourquoi ?
4- Quelle est l'utilité des deux antennes présentes sur le point d'accès ?
5- Si on veut interdire quelqu'un de se connecter à notre réseau, que doit-on faire ?
6- Pourquoi existent-ils plusieurs modes de fonctionnement de cet équipement « point d'accès » ?
7- Faites une conclusion générale du TP.

TP N°05

Fonctionnement des protocoles TCP/IP

(Processus d'Encapsulation)

par analyse des trames de données

(Utilisation de Wireshark)

V.1. Objectif du TP

Apprendre à l'étudiant de capturer un trafic de données par un Sniffer (analyseur de trafic réseau). Analyser l'empilement protocolaire en utilisant le cas d'une application Web (http). Examiner la structure d'une trame Ethernet ainsi que l'entête d'un datagramme IP notamment les entêtes spécifiques des couches transport (TCP) et réseau (IP). Comprendre le rôle de chaque couche dans le modèle TCP/IP.

V.2. Rappels théoriques

V.2.1. Introduction :

Dans un réseau, les périphériques se communiquent grâce aux protocoles de communication. Un protocole de communication est un ensemble de règles de communication servant comme langage machine-machine. Un modèle de référence mondiale appelé OSI (Open Systems Interconnection) est défini par les organisations internationales (ISO : International Organization for Standardization **[11]**, ITU : International Telecommunication Union **[12]**) pour normaliser tout ce qui concerne les réseaux informatiques, y compris les protocoles de communication. Un deuxième modèle plus réaliste et plus simple appelé TCP/IP (Transmission Control Protocol / Internet Protocol) est mis en place pour gérer efficacement les communications au sien d'un réseau local (LAN). Ce modèle qui est structuré en quatre couches à savoir : Application, Transport, Internet, et Accès-réseau, est globalement conforme au modèle OSI, bien qu'il le précède historiquement. Ainsi, les informations échangées entre les différentes machines sont sous forme de trames de données dont le format est précisé dans les protocoles TCP/IP. Des logiciels spécialisés appelés « Sniffers » permettent d'analyser ces trames et voir le contenu de chaque couche, parmi lesquels le logiciel : ***WireShark***.

V.2.2. Processus d'encapsulation

Un processus d'échange de données entre couches de même niveau mais sur deux systèmes différents s'effectue par le biais d'un mécanisme appelé ***« encapsulation »*** en passant d'une couche à une autre jusqu'à arrivée à la machine destinatrice (voir la figure V.1).

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) (dans le cas d'une émission). Chaque couche ajoute à la donnée opaque qui est le SDU (Service Data Unit) des informations de contrôle de protocole dit PCI pour obtenir un PDU (Protocol Data Unit). Cela peut être résumé par **[14]**:

$$PDU_{(N)}=SDU_{(N)}+PCI_{(N)}$$

avec : $$PDU_{(N)}=PCI_{(N)}+PDU_{(N+1)}$$

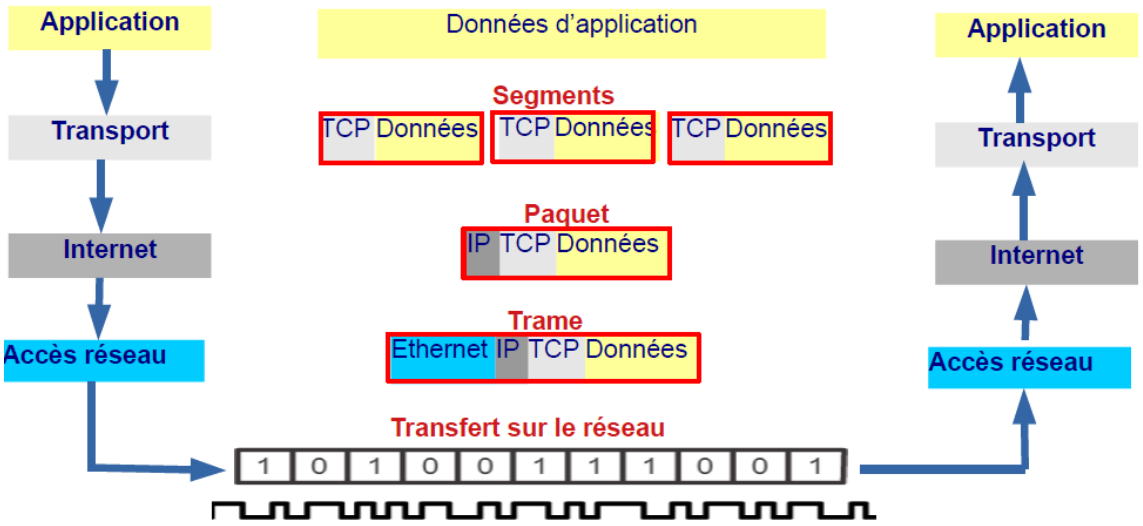

Figure V.1 : Principe d'encapsulation

Ainsi, les données au niveau de la couche haute (application) sont des massages de taille importante (image, vidéo, texte...). En descendant à la couche transport, le message sera

découpé en différents segments de données et un entête de transport sera rajouté à chacun d'eux, ainsi qu'un port de connexion sera affecté pour spécifier l'application qui a généré la donnée. A son tour, la couche Internet rajoute un entête à chaque segment fourni par la couche transport, l'ensemble est appelé datagramme ou paquet de données. Enfin, la couche Accès réseau construit des trames à partir des datagrammes fournis par la couche Internet, en rajoutant un entête spécifique à la couche 2. La couche Accès réseau produit aussi un signal adapté au support de transmission à partir du train binaire (bits) constitué par une succession de trames **[10]**.

A la réception, chaque couche reçoit le message transmis par la couche du même niveau sur l'autre système et enlève donc l'entête qui a été rajouté, puis elle passe le bloc restant à la couche supérieure. On appelle ce processus inverse la ***« décapsulation ».***

V.2.3. Format d'un paquet et d'une trame

Les données au niveau de la couche Internet se trouvent sous forme de paquets IP. Un paquet de données est un ensemble de champs ayant un certain format bien déterminé dans le protocole de communication **[11][12]**. Il consiste en un bloc de données restitué de la couche transport et d'un entête rajouté par la couche Internet. Le format général d'un paquet IP est montré dans la figure V.2.

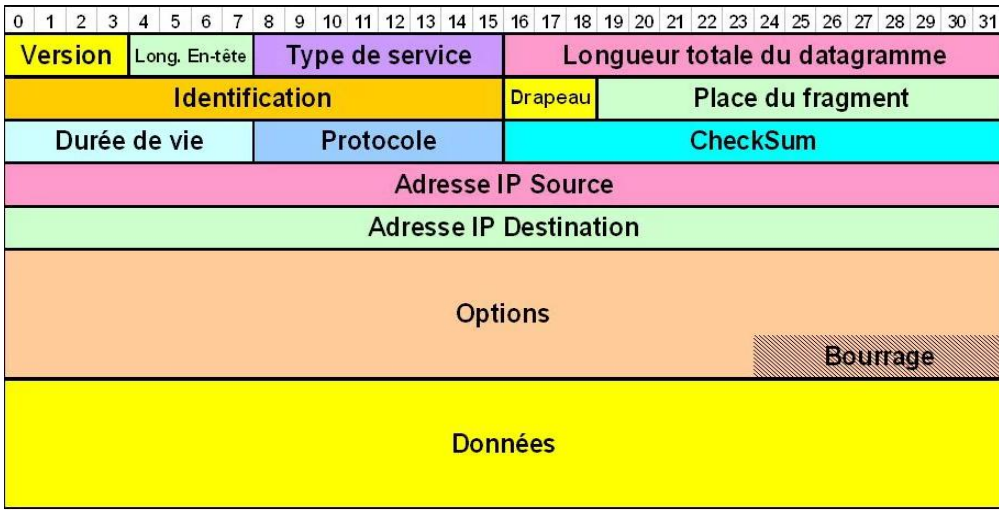

Figure V.2 : Format général d'un Datagramme IP

Ainsi, pour contrôler une certaine fonctionnalité telle que l'intégrité d'un message ou la connectivité entre deux postes, le système utilise le protocole ICMP en envoyant des paquets de contrôle qui vont interroger des machines sur le réseau. Les machines qui reçoivent ces messages doivent transmettre des réponses, c'est le cas de la commande **ping** par exemple (voir la figure V.3).

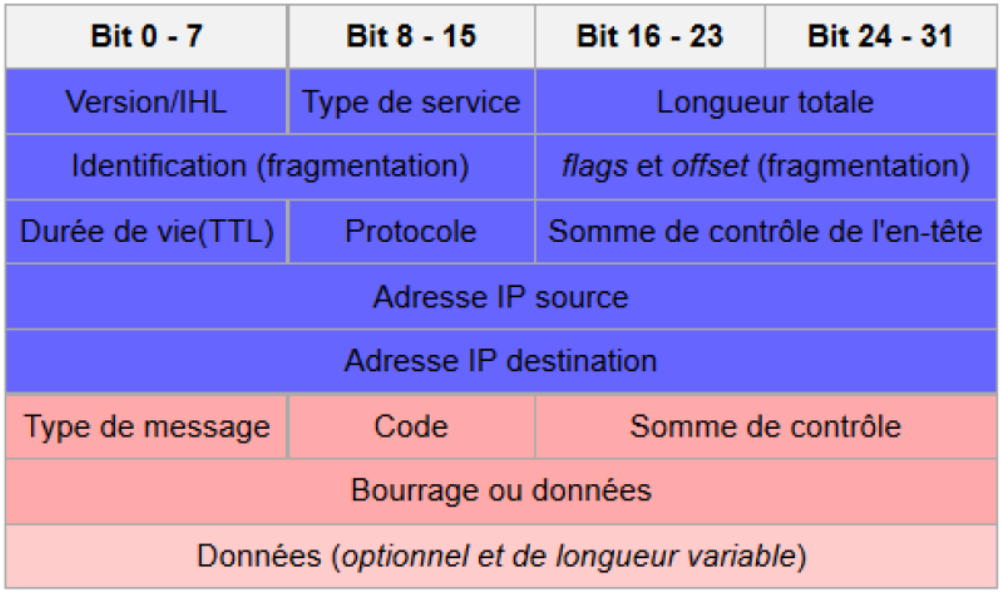

Figure V.3 : Format général d'un paquet ICMP

Les données au niveau de la couche Accès réseau se trouvent sous forme de trames de données de type Ethernet. Une trame est une succession de bits regroupés en des champs ayant chacun une signification bien définie dans le protocole de communication **[10]**. Chaque trame est donc constituée par le paquet restitué de la couche Internet et d'un entête rajouté par la couche Accès réseau. Le format général d'une trame est illustré dans la figure V.4.

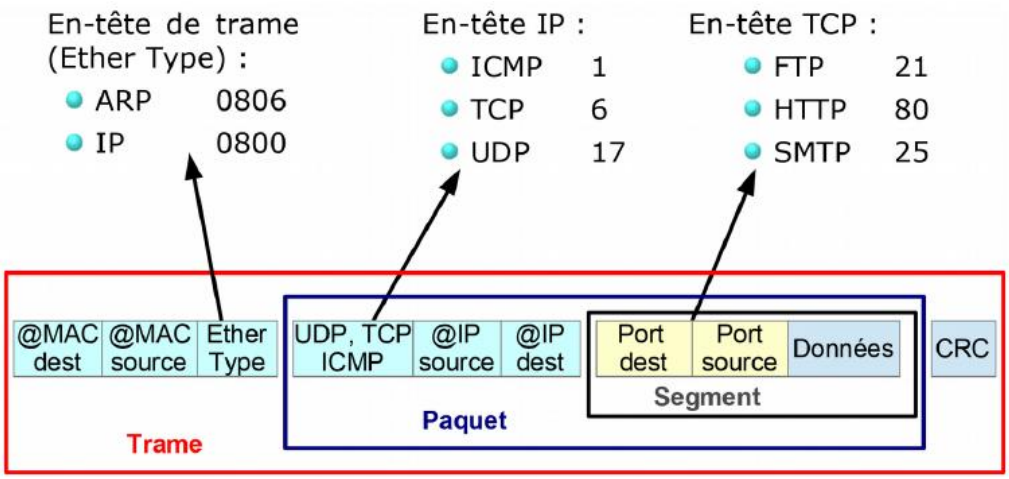

Figure V.4 : Format général d'une trame Ethernet

V.2.4. Le logiciel analyseur de trames (Wireshark)

Un analyseur de trames (ou en anglais sniffer), est une application permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent. Il sert généralement aux administrateurs pour diagnostiquer les problèmes sur leur réseau ainsi que pour connaître le trafic qui y circule. Ainsi les détecteurs d'intrusion (*IDS*, pour *intrusion detection system*) sont basés sur un sniffeur pour la capture des trames, et utilisent une base de données de règles pour détecter des trames suspectes.

Parmi ces logiciels sniffers, on a « Wireshark » qui a été spécifiquement conçu pour capturer et récupérer les trames de données qui circulent dans un réseau. WireShark est un logiciel conçu principalement pour des raisons d'administration des réseaux mais peut aussi être destiné aux étudiants qui l'utilisent pour apprendre le fonctionnement interne du protocole TCP/IP (voir la figure V.5). Le processus de capture est effectué de manière totalement transparente et il peut s'exécuter hors ligne.

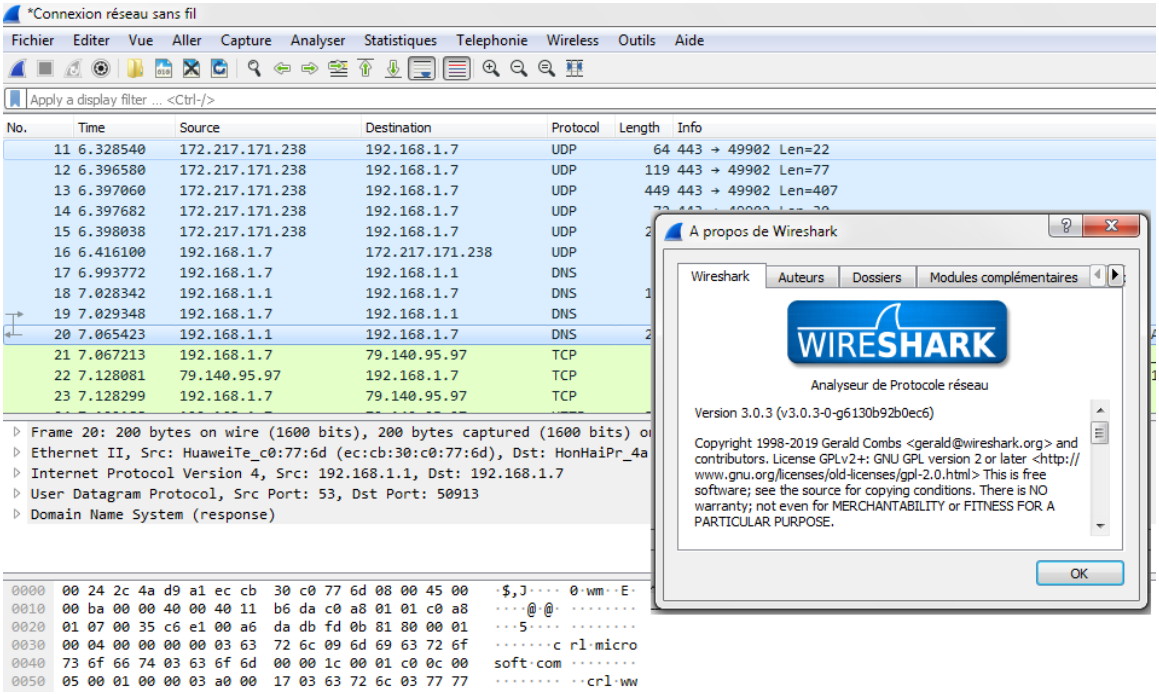

Figure V.5 : Exemple d'un trafic capturé par Wireshark

Le logiciel Wireshark fait partie des meilleurs analyseurs de paquets open source et gratuit disponibles sur internet.

L'interface de Wireshark est composée de trois zones :

- ✓ Zone supérieure : liste des trames capturées.
- ✓ Zone centrale : elle affiche le détail d'une trame sélectionnée par le curseur de la souris dans la liste de la zone supérieure.
- ✓ Zone inférieure : elle présente l'ensemble des octets sous forme ASCII. Ces octets contiennent les en-têtes des différentes couches de l'architecture TCP/IP ainsi que les données transmises par le processus à l'origine du message.

V.3. Partie pratique

Dans ce TP on va utiliser le logiciel sniffer WireShark, pour voir comment les couches ajoutent les entêtes (PCI) au bloc de données (PDU) de la couche immédiatement supérieure ($PDU_{(N)}=PDU_{(N+1)}+PCI_{(N)}$), ainsi pour voir le principe de fonctionnement du protocole TCP qui travaille en mode connecté : demande de communication, acceptation, transfert de données, etc. On va essayer de voir toutes ces opérations sur un réseau réel de quelques ordinateurs ayant accès à Internet. Pour cela, il faut travailler sur un réseau déjà établi et fonctionnel.

Tout d'abord, procédez à télécharger et installer WireShark. Puis, en ouvrant une session de ce logiciel, il nous donne accès à certains paramètres de réglages. Choisissez l'interface sur laquelle vous voulez capturer les données.

V.3.1. Analyse des trames ARP et ICMP

- Pour que les machines se reconnaissent, elles s'échangent des trames de ''reconnaissance'' appelées trames ARP (Address Resolution Protocol).

Avant de commencer la capture, il est nécessaire de vider le cache ARP à l'aide de cette ligne de commande :

Netsh interface ip delete arpcache

Q1 : Pourquoi doit-on effectuer cette commande ?

Réponse :

……

……

……

Juste après cette commande, mettre un filtre d'affichage pour qu'il n'affiche que les données qui nous intéressent, utilisez le filtre : ***host @destination***, et lancez la capture pour quelques secondes (10-15 sec) puis arrêtez-la. Pour @destination, il faut d'abord connaitre les adresses

IP de toutes les machines soit par configuration statique soit par la commande **ipconfig /all** dans le cas d'une configuration dynamique (DHCP activé).

Lacez maintenant l'analyse « bouton Start » et revenez sur la fenêtre de commande et lancez ***ping @destination*** et faites arrêter la capture (bouton Stop).

Vous avez maintenant un trafic à analyser.

En cliquant sur la première trame de type ARP, la zone centrale permet de visualiser clairement les différentes couches d'encapsulation de cette trame.

Q2 : Citer les différentes couches dans cette trame ?

……

……..

Q3 : Pourquoi on ne visualise pas les autres couches ?

Réponse :

……

……..

Q4 : Extraire les informations suivantes :

Longueur de trame : ……..

Contenu du champ type de la trame : ……

Adresse IP de destination : ……..

Adresse IP de votre ordinateur : …….

Quelle est la classe des adresses IP, source et destination ?

…….

Adresse physique de destination : ……

Adresse physique de votre ordinateur : ……

Quel est l'identifiant du constructeur de la carte réseau de votre ordinateur ?

Réponse : …….

Faites une comparaison avec le résultat donné par la commande : ***arp –a***

Q5 : Y a-t-il une différence ? …… (oui/non).

En cliquant sur la première trame de type ICMP (Internet Control Message Protocol), la zone centrale permet de visualiser clairement les différentes couches d'encapsulation de cette trame.

Q6 : Citer les différentes couches dans cette trame ?

Réponse :

……

Q7 : Pourquoi on ne visualise pas les autres couches ?

Réponse :

……

……..

Q8 : Extraire les informations suivantes :

Longueur de trame : ……..

Adresse IP de destination : ……..

Adresse IP de votre ordinateur : …….

Adresse physique de destination : ……

Adresse physique de votre ordinateur : ……

V.3.2. Analyse d'une trame de données, TCP et Http

Pour voir les différents entêtes ajoutés par les couches du modèle TCP/IP, faites un filtre sur les trames TCP reçues sur le port http, soit le filtre : ***tcp port http***, puis relancez une nouvelle capture de Wireshark. Sur une page web effectuer un certain trafic sur internet (exemple : chargement de la page : www.google.com et recherche du mot 'réseau'), puis arrêtez le processus de capture.

Cliquer sur une trame TCP, et localiser les couches d'encapsulation sur la zone centrale.

Q9 : Citer les différentes couches dans cette trame ?

……

Q10 : Pourquoi on ne visualise pas la couche « Application » ?

……

……..

Q11 : Extraire les informations suivantes :

Longueur de trame : ……..

Adresse physique de destination : ……..

Adresse physique de votre ordinateur : …….

Adresse IP de destination : ……

Adresse IP de votre ordinateur : ……

Longueur de l'entête IP : ……..

Valeur du champ TTL est : ……..

Port de destination : ……

Port de source : ……

En cliquant sur une trame HTTP, la zone centrale permet de visualiser clairement les différentes couches d'encapsulation de cette trame.

Q12 : Citer les différentes couches dans cette trame ?

……

Q13 : Pourquoi la couche « Application » est présente cette fois-ci ?

Réponse :

……

……..

Q14 : Extraire les informations suivantes :

Longueur de trame : ……..

Adresse physique de destination : ……..

Adresse physique de votre ordinateur : …….

Adresse IP de destination : ……

Adresse IP de votre ordinateur : ……

Longueur de l'entête IP : ……..

Valeur du champ TTL (Time To Live) est : ……

Port de destination : ……

Port de source : ……

V.4. Quelques questions pour conclure :

1- Quelle est l'utilité d'un logiciel 'Sniffer' ?
2- Quelle est la signification du champ : Time-To-Live (TTL) ?
3- Quelle est l'utilité d'un port de connexion ?
4- Quel est le protocole de transport utilisé dans cette transmission ? Existe-t-il un autre protocole de transport ?
5- Faites une conclusion générale sur ce que vous avez manipulé dans ce TP.

Bibliographie

[1] : Jacques Nozick, 'Guide du câblage universel', Eyrolles 3e édition 2009, ISBN-13 : 978-2212125238.

[2] : Vincent Breton, Philippe Boniface et Didier Mabriez, 'Memotech - Télécommunications et réseaux', édition Eyrolles, 2014. ISBN: 2206100010.

[3] : Guy Pujolle, ''Cours réseaux et télécoms'' : Avec exercices corrigés, 3e édition ; Eyrolles, 2008.

[4] : Guy Pujolle, Olivier Salvatori, ''Les réseaux'' avec des Annexes, Édition 2018-2020 de. © Eyrolles, 2018.

[5] : Andrew Tanenbaum, David Wetherall Tanenbaum ; ''Réseaux'' ; 5ème édition, © 2011 Pearson Education France.

[6] : Laurent Toutain, ''Réseaux locaux et Internet, des protocoles à l'interconnexion'', Hermes Science Publications, 3ème édition 2003, ISBN-13 : 978-2746206700.

[7] : Claude Servin ; ''Réseaux et télécoms'', édition Dunod, Paris, 2006.

[8] : Douglas Comer ; TCP/IP, 'Architectures, protocoles et applications', 5e édition, Pearson 2006. ISBN-13 : 978-2744071867.

[9] : René Parfait, 'Les réseaux de télécommunications' ; Hermes – Lavoisier, 5ème édition, 2003. ISBN13 : 978-2-7462-0470-6

[10] : José DORDOIGNE, 'Réseaux Informatiques - Maîtrisez les fondamentaux', Edition ENI livre canadien 6e, 2018, ISBN : 9782409014512.

[11] : https://www.iso.org

[12] : https://www.itu.int

[13] : https://www.wi-fi.org

[14] : https://fr.wikipedia.org

Annexe

Commande MS-DOS utiles pour les réseaux informatiques (exécutées sur une fenêtre CMD)

Ping Effectue un test de connectivité sur une machine distante à utiliser avec une adresse IP.
Syntaxe : *ping wikipédia.org ou bien ping 192.168.1.2*

Tracert : Affiche toutes les adresses IP intermédiaires par lesquelles passe un paquet entre la machine locale et l'adresse IP spécifiée.
Syntaxe : *tracert [@IP ou nom du host]*

IpConfig : Affiche toute la configuration réseau, y compris les serveurs DNS, WINS, bail DHCP, etc ...
Syntaxe : *ipconfig /all*

Netstat : Affiche l'état de la pile TCP/IP sur la machine locale, des statistiques, les ports de connexion, la table de routage…
Syntaxe : *netstat –a ou bien : –e –n –s –p –r*

Route : Efface et modifie la table de routage
Syntaxe : *route –f ou –p …*

Arp : Affiche et modifie les tables de traduction des adresses IP en adresses MAC utilisées par le protocole de résolution d'adresses ARP.
Syntaxe : *ARP –a ou bien –s –d.*

Nslookup: Envoie des requêtes DNS sur un serveur DNS au choix
Syntaxe : *nslookup domaine @IP_dns*

Telnet : Permet d'accéder en mode Terminal à une machine distante. Elle permet également de vérifier si un service quelconque TCP tourne sur un serveur distant en spécifiant après l'adresse IP le numéro de port TCP.
Syntaxe : *telnet 192.168.0.1*

Netsh : Permet de configurer des interfaces réseaux.
Syntaxe : *netsh interface ip reset C:\resetlog.txt*

Hostname : Affiche le nom de l'ordinateur (*ex : hostname*)
Syntaxe : *hostname*

NbtStat : Mise à jour du cache du fichier Lmhosts. Affiche les statistiques du protocole et les connexions TCP/IP actuelles utilisant NBT (NetBIOS sur TCP/IP).
Syntaxe : *Nbtstat -a @IP*