

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique

– جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr BELKAÏD – Tlemcen

كلية التكنولوجيا

Faculté de Technologie



Polycopié de TP

Les réseaux locaux

Elaboré par :

Djilali MOUSSAOUI

Benamar KADRI

Formations :

Licence Informatique Biomédical

Licence en télécommunication

Année universitaire : 2019/2020

TP I

Installation et configuration d'un réseau local Ethernet

Ce premier TP a comme objectif d'établir une liaison physique entre un ensemble d'ordinateurs et réaliser la configuration logicielle permettant à ces ordinateurs de communiquer entre eux, partager des fichiers et imprimantes.

Ces objectifs passent par les étapes suivantes :

1. Etude des topologies réseaux existantes et se concentrer sur la topologie étoile.
2. Installation du matériel réseau nécessaire pour cette topologie en utilisant « Switch, câbles »
3. Faire la configuration du réseau « adressage, nom d'ordinateurs, nom de groupes »
4. Tester la configuration
5. Partager les fichiers et les imprimantes sous Windows
6. Utilisation du bureau à distance sous Windows.

1. Rappel sur les topologies réseaux

1.1 Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. Dans cette topologies un ensemble d'ordinateurs sont reliés à l'aide d'un câble généralement coaxial. Le mot « bus » désigne la ligne de câblage reliant les ordinateurs cette topologie est inespérée du réseau électrique qui existait déjà pour relier les équipements dans les maisons.

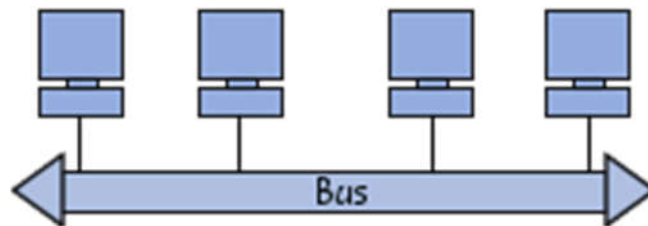


Figure I.1 topologie en bus

1.2 Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un concentrateur (en anglais hub ou Switch). Le hub joue le rôle d'une multiprise dans la façon ou il est utilisé pour distribuer de l'électricité « bits » vers tous les équipements du même réseau. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Si on compare toujours au réseau de l'électricité dans une maison, c'est une multiprise dont le but est de dispatcher de l'électricité vers des cartes réseaux.

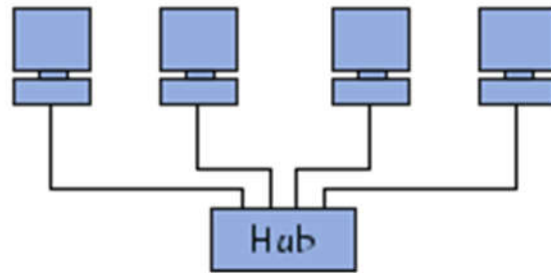


Figure I.2 topologie en étoile

1.3 Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. La communication est gérée à l'aide d'un jeton dont seul le propriétaire a le droit d'envoyer des données sur la boucle.

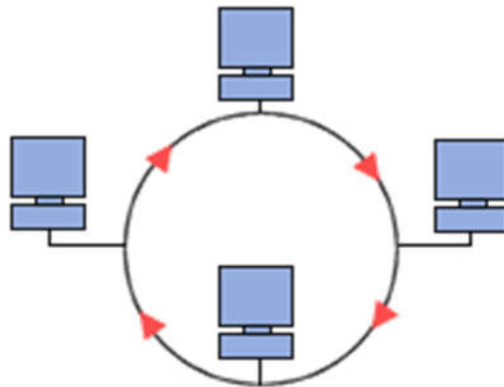


Figure I.3 topologie en anneau

2. Installation d'une topologie en étoile

Dans ce qui suit on va réaliser une topologie en étoile ou un ensemble d'ordinateurs sont reliés à un Switch qui joue le rôle du concentrateur dans ce réseau, ce réseau est généralement baptisé Ethernet.

La première étape consiste à étudier l'ensemble du matériel utilisé : Carte réseau, Switch, câble, connecteurs Ethernet, pinces Ethernet

2.1 Découverte du matériel utilisé

➤ Carte réseaux

La carte réseau est un périphérique permettant de connecter un ordinateur à un réseau. Elle sert d'interface entre la machine et le câble du réseau.

Il existe différentes normes des cartes réseaux mais les cartes Ethernet sont très répandues aussi bien en entreprise que chez les particuliers.

La carte Ethernet (correspondant à la norme IEEE 802.3). Ces cartes se présentent sous plusieurs formes suivant les besoins des utilisateurs « intégrée, non intégrée, USB »

Un autre standard très courant est le standard Wifi « IEEE 802.11 » pour les réseaux sans fil.

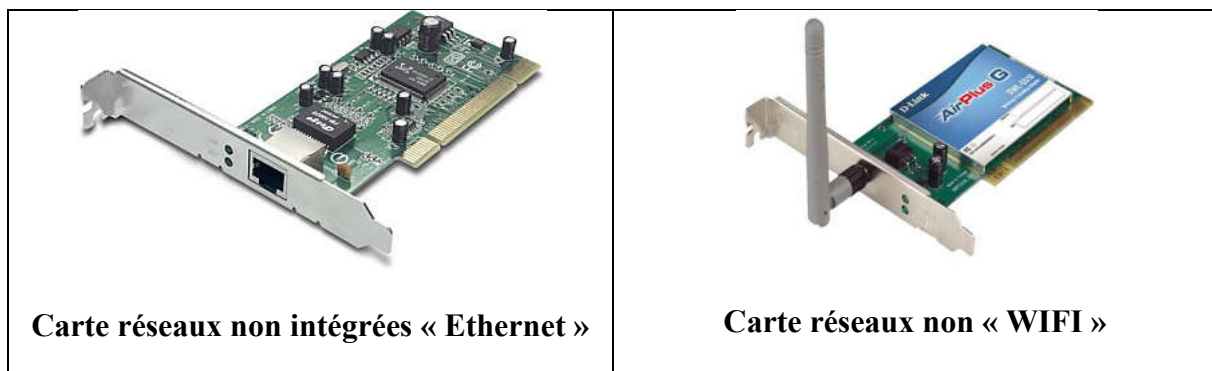


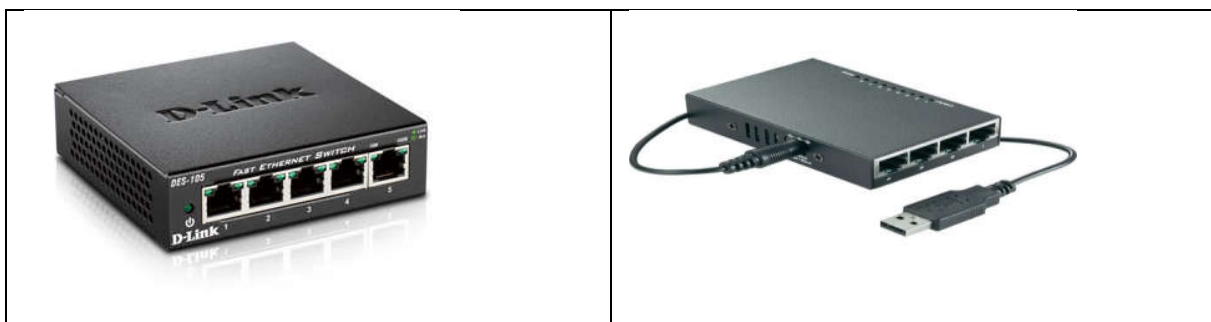


Figure I.4 types de cartes réseau

➤ **Switch « hub »**

Un Switch « concentrateur réseau », est un équipement qui relie plusieurs ordinateurs ou segments (câbles ou fibres) dans un réseau informatique.

Il s'agit d'un boîtier semblable à une multiprise ou commutateur disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines), les ordinateurs sont connectés au Switch via des câbles Ethernet pour réaliser une topologie en étoile « réseau Ethernet »



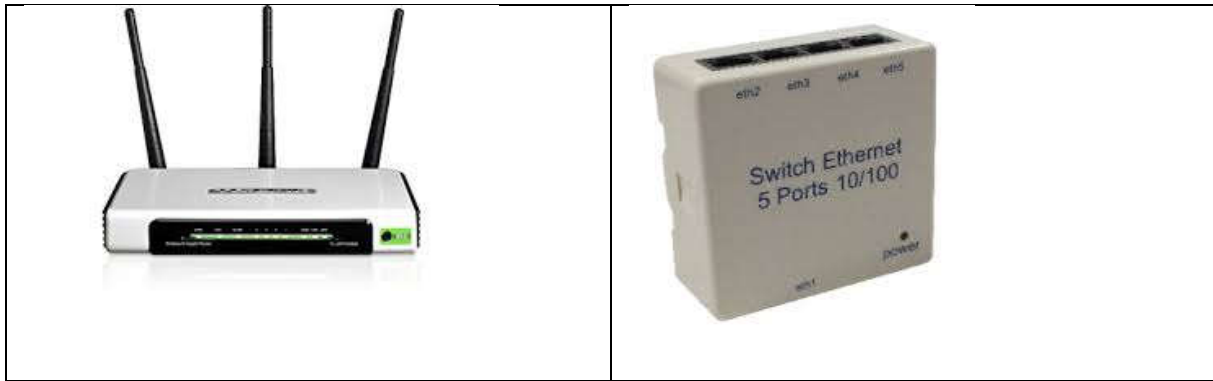


Figure I.5 hub et point d'Access

➤ Câblage Ethernet « RJ45 »

Un câble Ethernet ou câble RJ45 est un câble composé de quarts paires torsadées chacune a une couleur différentes « vert--blanc-vert, bleu.. blanc-bleu, orange-- blanc-orange et marron-- blanc-marron »

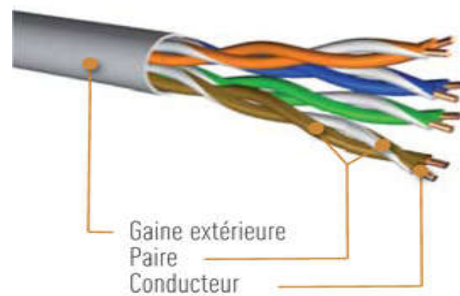


Figure I.6 câble Ethernet

Suivant le nature du matériel utilisé et le débit ciblé ou même l'installation à réaliser, différents types de câbles peuvent utilisés :

- Le **câble RJ45 UTP** (Unshielded Twisted Pair) est un câble RJ45 non blindé, non écrané.

- Le **câble RJ45 FTP** (Foiled Twisted Pair) est un câble RJ45 écranté avec une feuille d'aluminium.
- Le **câble RJ45 STP** (Shielded Twisted Pair) est un câble RJ45 écranté paire par paire.
- Le **câble RJ45 S/STP** (Shielded and Shielded Twisted Pair) est un câble RJ45 blindé paire par paire avec un blindage autour.

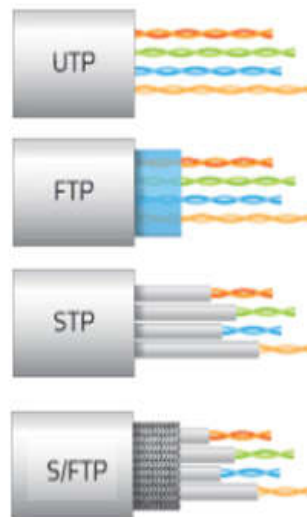










Figure I.7 blindage Ethernet

➤ Normes du câble RJ45

Deux normes de câblages sont principalement répandues pour les connexions de la prise : la norme T568A et la norme T568B. Ces normes sont très similaires puisque seuls les paires 2 (orange, blanc-orange) et 3 (vert, blanc-vert) sont interchangeables.

- **Norme EIA/TIA568A**

T568A			
Nom	N° Broche	N° Paire	Couleur
RD+	1	1	 Blanc-vert
RD-	2	1	 Vert
TD+	3	2	 Blanc-orange
Non utilisée	4	3	 Bleu
Non utilisée	5	3	 Blanc-bleu
TD-	6	2	 Orange
Non utilisée	7	4	 Blanc-brun
Non utilisée	8	4	 Brun

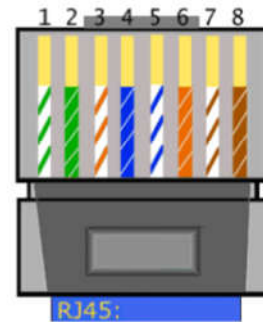










Figure I.8 Norme EIA/TIA568A

- Norme EIA/TIA568B

T568B			
Nom	N° Broche	N° Paire	Couleur
RD+	1	1	 Blanc-orange
RD-	2	1	 Orange
TD+	3	2	 Blanc-vert
Non utilisée	4	3	 Bleu
Non utilisée	5	3	 Blanc-bleu
TD-	6	2	 Vert
Non utilisée	7	4	 Blanc-brun
Non utilisée	8	4	 Brun

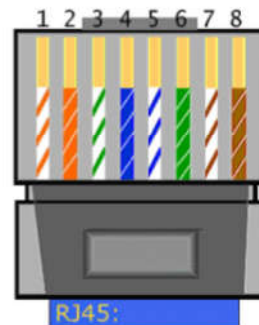


Figure I.9 Norme EIA/TIA568B

- **Câble droit** : est utilisé pour connecter un appareil hôte à un concentrateur réseau (hub) ou un commutateur réseau (switch).

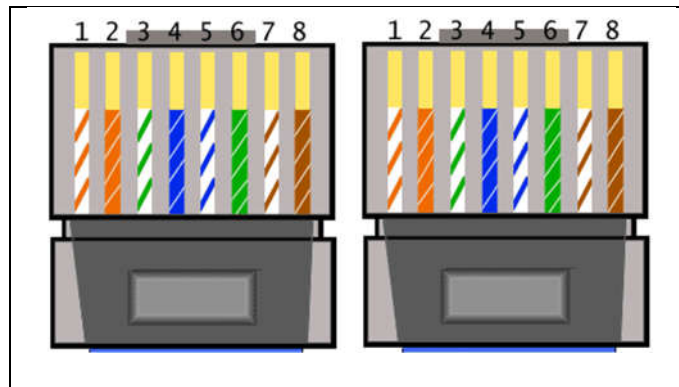


Figure I.10 câble droit

- **Câble croisé** : type de câble est utilisé pour connecter deux PCs sans l'utilisation de Switch ou HUB

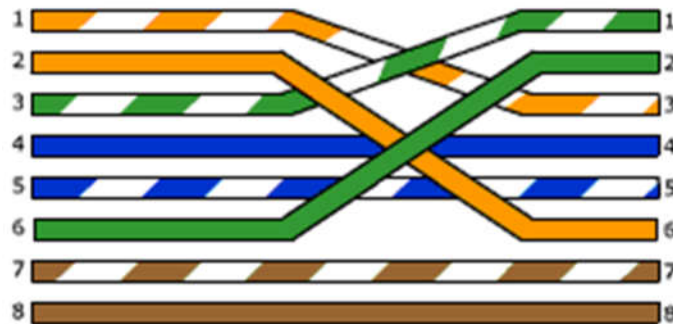


Figure I.11 câble croisé

➤ Connecteurs

Un connecteur RJ45 est une interface physique composé de huit broches de connexions électriques souvent utilisée pour connecter une carte réseau aux paires torsadés des câbles RJ45 et par la suite au Switch ou aux prises RJ45.

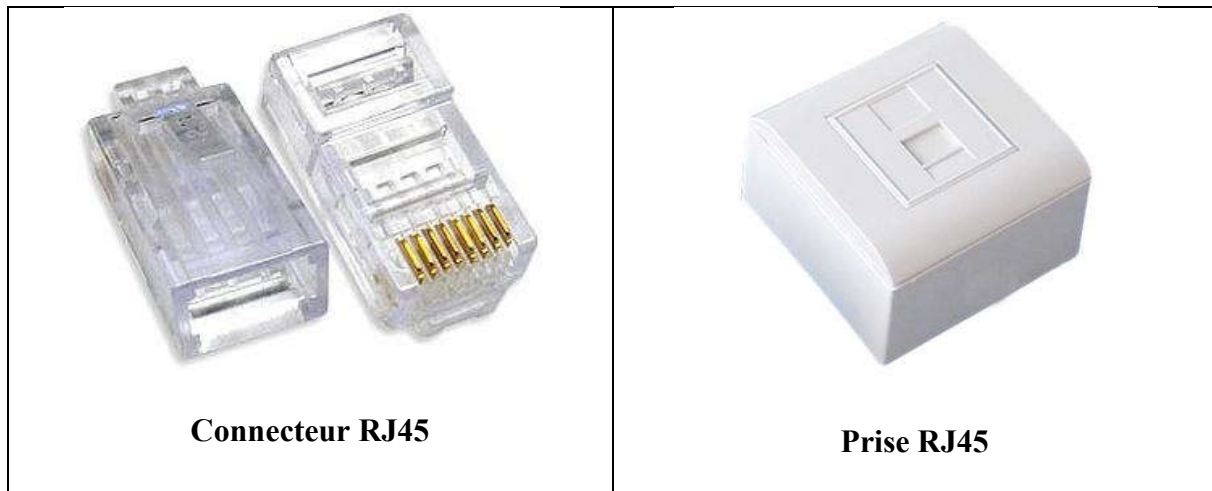


Figure I.12 connecteur RJ45

➤ **Pince RJ45**

Une pince RJ45 est une pince spéciale permet de serrer les paire torsadés d'un câble Ethernet a un connecteur RJ45



Figure I.13 pince RJ45

2.2 Installation du réseau

Dans cette section on va faire les raccordements nécessaires pour réaliser un réseau local Ethernet :

1. Réalisation d'un câble croisé et faire un réseau entre deux PCs.

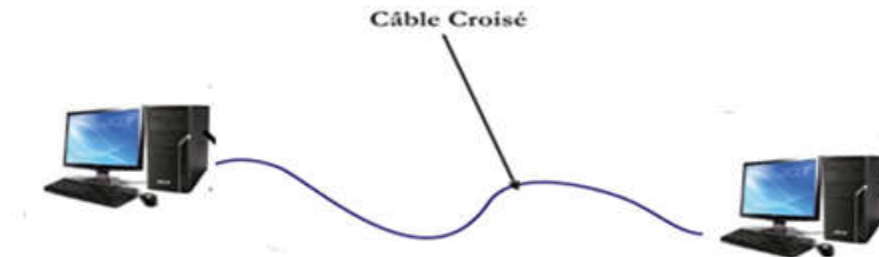


Figure I.14 réseau poste a poste

2. Réalisation des câblages réseau droite à l'aide des connecteurs, prises et des câbles RJ45.
3. Faire le raccordement final entre les PC et le Switch à l'aide des câbles réalisés dans la première étape.

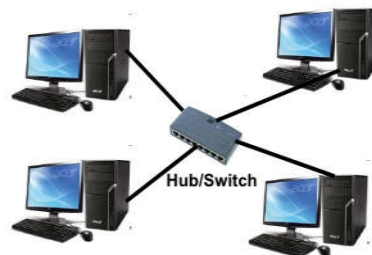


Figure I.14 réseau avec hub

3. Configuration d'un réseau local sous Microsoft Windows « XP »

3.1 Adressage des ordinateurs

La configuration d'un réseau Ethernet consiste à affecter à chaque ordinateurs une adresse IP unique et des noms aux PCs pour qu'ils puissent s'identifier sur le réseau afin d'exploiter l'infrastructure matériel pour pouvoir communiquer et partager des fichiers et des imprimantes.

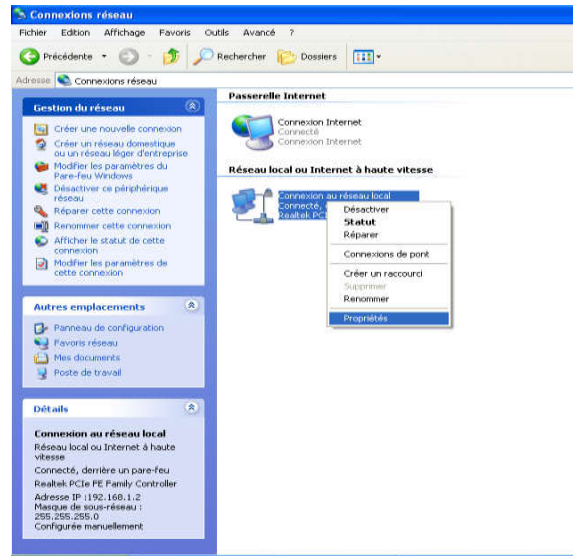
➤ Adresse IP

Chaque équipement (ordinateur, imprimante, routeur,...) sur un réseau est identifié par une adresse unique, adresse IP « internet Protocol ». Cette adresse IP est composée de 32 bits traités séparément par 8 bits donnant ainsi un octet comprenant des valeurs comprises entre 0 et 255.

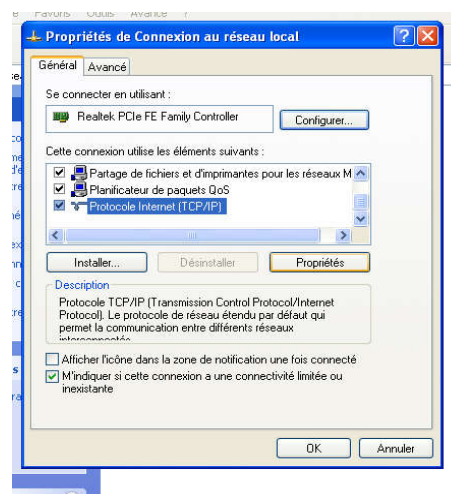
Exemple d'adresse IP : 192.168.0.1

➤ Configuration des adresses IP

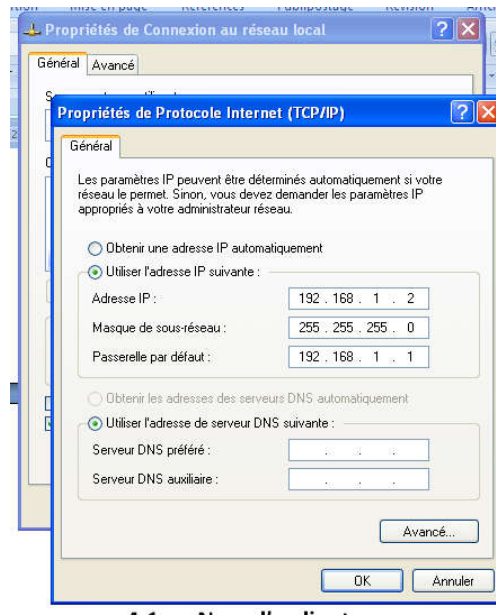
- Allez au panneau de configuration
- Chercher connexions réseau
- Chercher le nom de la connexion réseau à configurer « wifi ou Ethernet » avec le bouton droit de la souris sur la connexion réseau que vous souhaitez configurer.



- Dans le menu, sélectionnez **Propriétés**.
- Sélectionnez **Protocole Internet version 4 (TCP/IPv4)**.
- Cliquez sur le bouton **Propriétés**.



- Une nouvelle fenêtre s'ouvre :
 - Cochez la case Utiliser l'adresse IP suivante.
 - Dans le champ Adresse IP, saisissez une adresse située entre 192.168.1.1 et 192.168.1.254
 - Saisissez l'adresse 255.255.255.0 sur la ligne Masque de sous-réseau.



3.2 Nom d'ordinateurs

Chaque ordinateur ayant Windows comme système d'exploitation nécessite un nom unique lui permettant de s'identifier et de communiquer d'une manière unique dans même réseau local. Ce nom remplace l'adresse IP vue la complexité de retenir une telle adresse par des gens qui ne sont pas de spécialité.

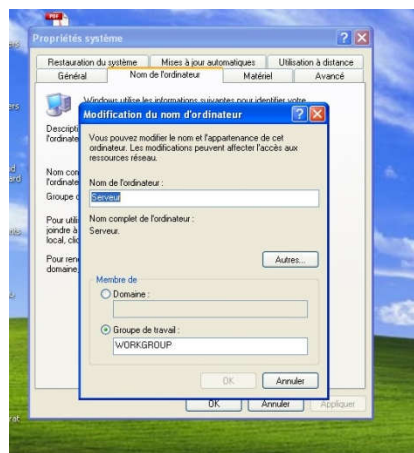
Il est recommandé d'utiliser uniquement les caractères standards sur Internet dans les noms d'ordinateur. Ces caractères correspondent aux nombres compris en 0 et 9, les majuscules et les minuscules de A à Z et le tiret (-).

Les noms d'ordinateur ne peuvent pas se composer uniquement de nombre ni contenir d'espace. Les noms ne peuvent pas non plus contenir des caractères spéciaux tels que : < > ; : " * + = \ | ? ,

➤ Modification des noms d'ordinateur

Pour modifier le nom d'un suivre les étapes ci-dessous

1. Faites un clic droit sur poste de travail, puis cliquez sur Propriétés.
2. Sous l'onglet Nom de l'ordinateur, cliquez sur Modifier, vous pouvez aussi donner une description à cet ordinateur « cette description sera afficher pour les utilisateurs réseau pour leur donner une vision de la tâche de ce dernier sur le réseau».
3. Sous Nom de l'ordinateur, supprimez l'ancien nom de l'ordinateur, tapez un nouveau nom, puis cliquez sur OK. Vous pouvez aussi entrer un nom du groupe de travail.



3.3 Groupes de travail

Les domaines, les groupes de travail et les groupes résidentiels représentent différentes méthodes d'organisation des ordinateurs dans les réseaux. Les ordinateurs exécutant Windows sur un réseau local appartiennent à un groupe de travail ou d'un domaine.

Les groupes de travail fournissent une base pour le partage de fichiers et d'imprimantes.

➤ Dans un groupe de travail ou groupe résidentiel :

- Tous les ordinateurs sont des homologues, aucun ordinateur n'en contrôle d'autres.

- Chaque ordinateur a un ensemble de comptes d'utilisateur. Pour ouvrir une session sur un ordinateur d'un groupe de travail, vous devez disposer d'un compte sur cet ordinateur.
- Il n'y a en général pas plus de vingt ordinateurs.
- Un groupe de travail n'est pas protégé par un mot de passe.
- Tous les ordinateurs doivent se trouver sur le même réseau local ou le même sous-réseau.

➤ **Modification d'un groupe de travail**

1. Faites un clic droit sur Ordinateur « POSTE DE TRAVAIL », puis cliquez sur Propriétés.
2. Sous l'onglet nom d'ordinateur, de domaine et de groupe de travail, cliquez sur Modifier les paramètres. .
3. Sous l'onglet Nom de l'ordinateur, cliquez sur Modifier.
4. Sous l'onglet groupe de résidentiel ou groupe de travail, supprimez l'ancien nom, tapez le nouveau nom du groupe, puis cliquez sur OK.

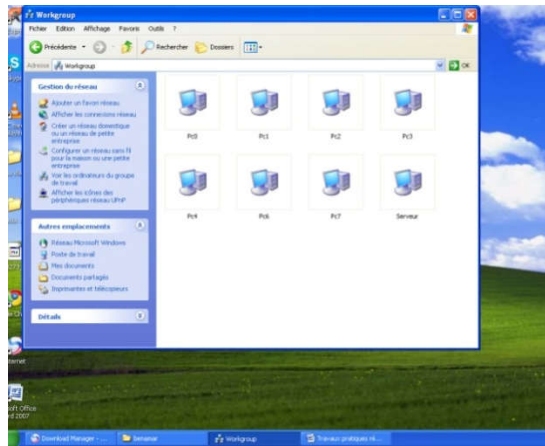
3.4 Teste de la configuration

➤ **Utilisation de l'utilitaire Windows**

Pour tester votre réseau, procédez comme suit sur chaque ordinateur en réseau :

Cliquez sur le bouton Démarrer, cliquez sur votre nom d'utilisateur puis, dans le volet gauche, cliquez sur Réseau.

Des icônes doivent s'afficher, représentant l'ordinateur sur lequel vous vous trouvez et tous les autres ordinateurs et imprimantes partagés du réseau.



➤ Utilisation de la commande PING

Pour tester les liaisons entre les différents postes, vous utiliserez la commande MS DOS « ping ».

La commande Ping c'est une ancienne commande sous DOS permettant de tester l'accessibilité d'une machine à travers un réseau IP, la commande PING mesure également le temps mis pour recevoir une réponse.

Pour utiliser la commande Ping, ouvrez une fenêtre DOS et tapez la commande Ping suivi du nom de l'ordinateur

Par exemple, pour tester la connexion à partir d'une machine dont l'adresse est 192.168.0.1, avec l'ordinateur d'adresse 192.168.0.2 vous taperez dans une fenêtre de commande (sous Xp menu démarrer → Tous les programmes → accessoire → invite de commande) , à partir de la première machine, la commande « PING 192.168.0.2 ».

Si l'ordinateur existe vous aurez une réponse positive avec la durée du va-et-vient du message entre les deux PCs

Envoi d'une requête 'ping' sur pc0 avec 32 octets de données :

Réponse de 192.168.1.10 : octets=32 temps=2 ms TTL=128

Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=128

Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

Si l'ordinateur n'existe pas sur le réseau un message sera affiché pour indiquer que l'ordinateur n'est pas accessible.

La requête Ping n'a pas pu trouver l'hôte pc10. Vérifiez le nom et essayez à nouveau.

➤ La commande ipconfig

C'est une commande propre à Windows elle permet de visualiser la configuration courante des interfaces réseau, adresse IP, adresse MAC, masque sous réseau et serveur DNS.

Dans une fenêtre DOS, taper « ipconfig /all » pour visualiser la configuration de votre interface réseau :

Carte Ethernet Connexion au réseau local:

Adresse physique : B8-97-5A-80-6C-03

DHCP activé. : Non

Adresse IP. : 192.168.1.2

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 192.168.1.1

Serveurs DNS :

4. Partage de fichiers et d'imprimantes

4.1 Partage de fichiers

Le partage de fichiers est une technique consistant à donner accès à d'autres utilisateurs sur le réseau à des fichiers sur votre disque dur. Il s'agit de fichiers de toutes sortes : logiciels, livres, vidéo, audio etc...

Pour partager un répertoire sous Windows suivez les étapes :

1. Faites un clic droit sur le répertoire, puis cliquez sur Propriétés.
2. Allez à l'onglet partage et cochez la case partager ce dossier.
3. Si cette case n'est pas active cliquez sur le lien activer le partage de fichier et d'imprimantes et suivez les étapes.
4. A la fin de ces étapes la case partager ce dossier sera activé.
5. Si vous voulez donner la possibilité aux utilisateurs de modifier le contenu de ce dossier cochez la case autoriser les utilisateurs réseau à modifier mes fichiers.

4.2 Partage d'imprimantes

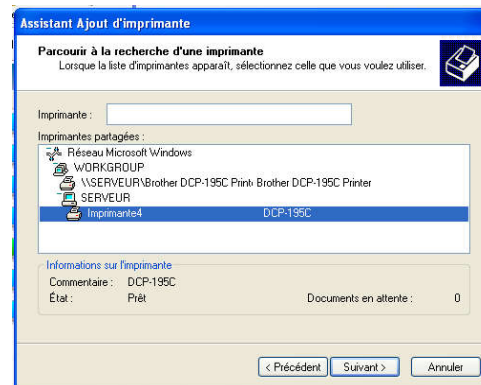
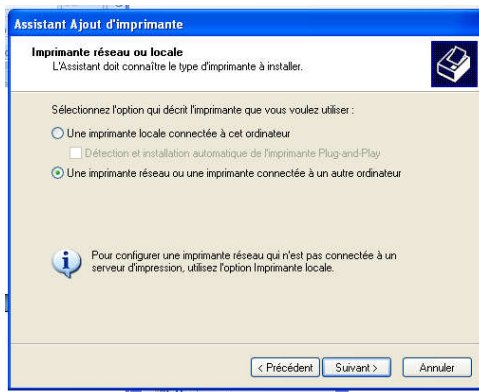
Le partage d'imprimante permet de donner au reste des utilisateurs réseau accès à votre imprimante et pouvoir imprimer sans faire des installations supplémentaires.

Pour partager une imprimante

1. Allez au panneau de configuration,
2. Allez à l'icône imprimante et télécopieur
3. Clic droite sur l'imprimante concernée ensuite cliquer sur propriétés.
4. Allez à l'onglet partage et cochez la case partager cette imprimante.

4.3 Ajouter une imprimante partagée

1. Allez au Imprimantes et télécopieurs dans le menu démarrer.
2. Cliquez sur ajouter une imprimante et suivez les étapes.
3. Cochez le choix : une imprimante connectée à un autre ordinateur
4. Cochez le choix : cherchez une imprimante
5. Cliquez sur le groupe de travail où se trouve l'ordinateur auquel est connectée l'imprimante
6. Cliquez sur l'ordinateur auquel est connectée l'imprimante dans la liste des ordinateurs du groupe de travail
7. Choisissez une imprimante parmi les imprimantes partagées par cet ordinateur.



4.4 Utilisation de l'application bureau distant

Cette application permet aux utilisateurs de Windows d'accéder à leurs ordinateurs depuis d'autres machines sur le réseau internet.

- **Activation** : l'activation de cette option donne la possibilité d'utiliser cet ordinateur à travers le réseau.

1. Faites un clic droit sur poste de travail, puis cliquez sur Propriétés.

2. Aller à l'onglet utilisation à distance
 3. Cochez l'option autoriser les utilisateurs à se connecter à cet ordinateur
 4. Cliquer sur ajouter des utilisateurs pour ajouter des utilisateurs pouvant accéder à cet ordinateur
- **Utilisation de bureau distant :** Pour pouvoir accéder à cet ordinateur à distance vous devez connaître son adresse IP et avoir un login et mot de passe d'une session sur cet ordinateur
 1. Aller au menu accessoire dans le menu démarrer
 2. Choisissez Connexion bureau distance
 3. Entrer le nom ou l'adresse IP de l'ordinateur
 4. Dans la fenêtre suivante entre le login et le mot de passe et commencer à utiliser votre PC à partir d'un autre PC sur le réseau

TP II

Installation et configuration d'un réseau local sans fil WIFI

Ce TP a comme objectif de réaliser un réseau local sans fil « WIFI » entre un ensemble d'ordinateurs et faire la configuration logicielle et matérielle afin que ces ordinateurs puissent communiquer entre eux, partager des fichiers et imprimantes.

Ces objectifs passent par les étapes suivantes :

1. Introduction au WIFI
2. Modes de fonctionnement
 - a. Mode infrastructure
 - b. Le mode ad hoc
3. Réalisation d'un réseau WIFI avec infrastructure
 - 3.1 Matériel utilisé
 - A. Les adaptateurs sans fil
 - B. Point d'accès
 - 3.2 Configuration des stations mobiles
 - i.* Installation des adaptateurs sans fil
 - ii.* Configuration de l'adresse IP
 - Configuration Manuelle
 - Configuration automatique
 - 3.3 Configuration du point d'accès
 - Serveur DHCP
 - Serveur DNS
 - SSID Service Set Identifier
 - 3.4 Accéder au point d'accès
 - Configuration du serveur DHCP
 - Configuration du SSID
 - 3.5 Configuration de la sécurité
 - a) Sécurité par le SSID
 - b) Filtrage des adresses MAC
 - c) WEP - Wired Equivalent Privacy
 - d) WPA WiFi protected Access
 - e) Activation de la sécurité sur le point d'accès

1. Introduction au WIFI

Grâce aux technologies de réseau sans fil, il est ainsi possible de créer un réseau local et pouvoir partager des ressources « répertoire, imprimante et internet » tout en garantissant la mobilité.

Un réseau sans fil permet de relier des ordinateurs portables, des ordinateurs de bureau, Smart phone ou tout type de périphérique à une liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert.



Figure II.1 réseau sans fil

La norme la plus répandue dans les réseaux sans fil est le Wi-Fi (Wireless Fidelity) ou la norme de réseau 802.11.

Un réseau WIFI opère dans la bande de fréquence de 2,4 GHz ou 5 GHz. Suivant la bande de fréquence et la technologie de modulation utilisées plusieurs variantes de WIFI existent :

Standard	Bande de fréquence	Débit	Portée
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2.4 GHz	11 Mbit/s	140 m
WiFi G (802.11g)	2.4 GHz	54 Mbit/s	140 m
WiFi N (802.11n)	2.4 GHz / 5 GHz	450 Mbit/s	250 m

2. Modes de fonctionnement

a. Mode infrastructure

Le mode « Infrastructure » est le mode de fonctionnement permettant de connecter des équipements mobiles équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès (PA) qui agissent comme des concentrateurs (HUB ou SWITCH en réseau Ethernet).

Les machines et le point d'accès doivent être configurées avec les mêmes paramètres pour être associés l'un à l'autre « mot de passe, nom du réseau (SSID) »

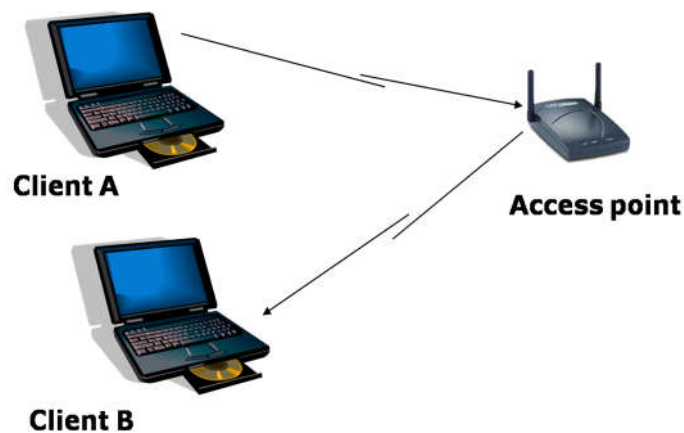


Figure II.2 réseau WIFI mode infrastructure

b. Le mode ad hoc

En mode ad hoc les équipements sans fil se connectent les uns aux autres sans point d'accès afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle d'une station ordinaire et le rôle de point d'accès pour faire le relais des données vers une autre machine dans le réseau.

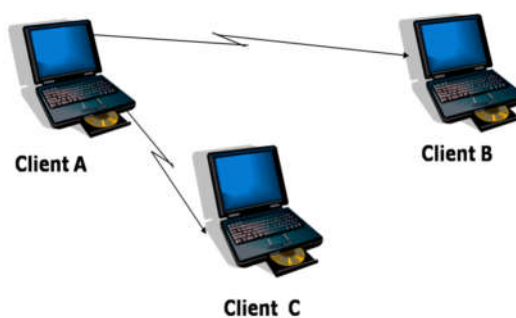


Figure II.3 réseau WIFI mode ad hoc

3. Réalisation d'un réseau WIFI avec infrastructure

3.1 Matériel utilisé

Il existe deux équipements pour la mise en place d'un réseau sans fil Wifi : Les adaptateurs sans fil et les points d'accès.

A. Les adaptateurs sans fil

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 WiFi sont disponibles dans de nombreux formats (carte PCI, adaptateur USB ...).



Figure II.4 : Types des cartes réseaux sans fil

B. Point d'accès

Un point d'accès (notés AP pour Access point) est un dispositif qui fonctionne au niveau de la couche MAC du modèle OSI. Un point d'accès fournit aux stations équipées d'une carte sans fil la possibilité de se connecter au réseau filaire existant « Ethernet, internet » en utilisant les ondes radio. Le point d'accès permet d'ajouter rapidement et facilement des postes de travail sans fil à un réseau câblé existant sans installation supplémentaire comme dans un réseau Ethernet.

Les points d'accès existent sous différentes formes suivant les besoins de l'utilisateur, et généralement on les trouve avec un système d'exploitation intégré qui contient plusieurs services tels que « le routage, serveur DHCP, connexion à l'internet, pare feux...etc ».

De nos jours même les smart phones peuvent être configurés comme des points d'accès afin de partager la connexion Internet.



Figure II.5 : Types des points d'accès

3.2 Configuration des stations mobiles

A. Installation des adaptateurs sans fil

Avant toute configuration, il est nécessaire d'équiper toutes les stations du futur réseau WIFI d'un adaptateur sans fil et d'installer les pilotes.

Après installation de la carte et ses pilotes une nouvelle icône apparaît dans la barre des tâches et dans le menu Connexions réseau dans le panneau de configuration, indiquant la présence d'un adaptateur sans fil actif dans l'ordinateur.

Similaire à l'icône d'une connexion filaire vu dans le TP précédent cette icône vous donne la possibilité de configurer l'adresse IP de la carte ainsi que les paramètres de sécurité qu'on va voir dans la section suivante.

B. Configuration de l'adresse IP

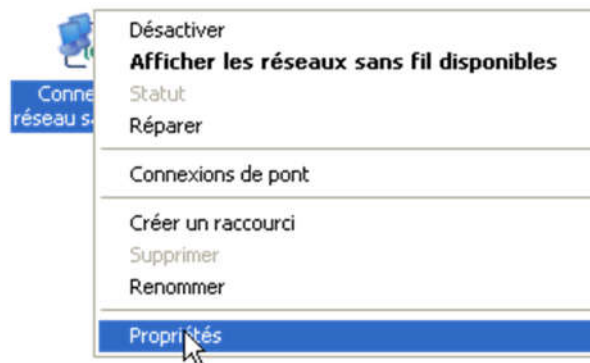
Deux modes de configurations existent :

- Configuration manuelle
- Configurations automatiques

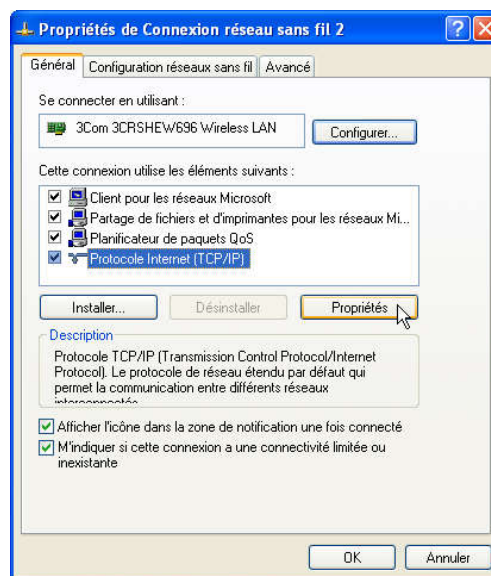
➤ Configuration Manuelle

Comme dans le premier TP « réseau Ethernet » dans notre réseau WIFI on va utiliser la plage d'adresse réservées au réseau locaux, comme 192.168.0.1 à 192.168.0.255 (ou 192.168.1.1 à 192.168.1.255).

Pour configurer la machine, il suffit de cliquer avec le bouton droit sur l'icône correspondante à la connexion réseau sans fil, puis de choisir « propriétés » :



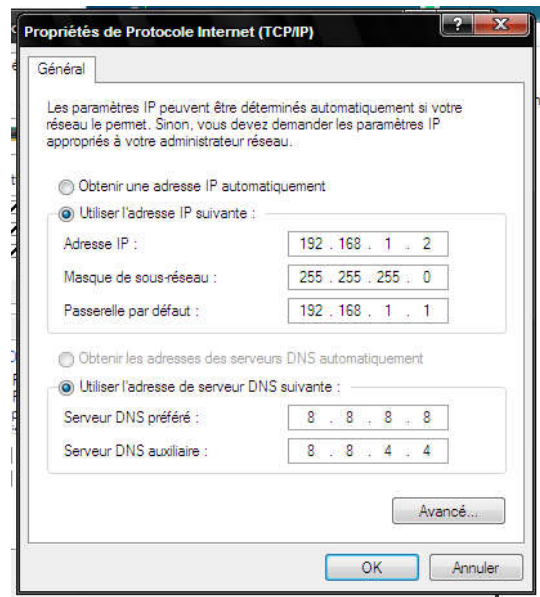
Puis, dans la liste des protocoles, sélectionnez « Protocole internet (TCP/IP) » et cliquez sur « Propriétés » :



Tapez l'adresse IP de chaque machine dans le champ correspondant, en veillant à ne pas utiliser deux fois la même adresse IP et tapez 255.255.255.0 comme masque de sous-réseau

En cas où il y a une connexion à l'internet Tapez l'adresse IP de la machine ou le modem assurant l'accès à internet (passerelle par défaut cette adresse est 192.168.0.1).

Dans les champs serveur DNS, saisissez les adresses IP des serveurs de noms exemples 8.8.8.8 et 8.8.4.4 :

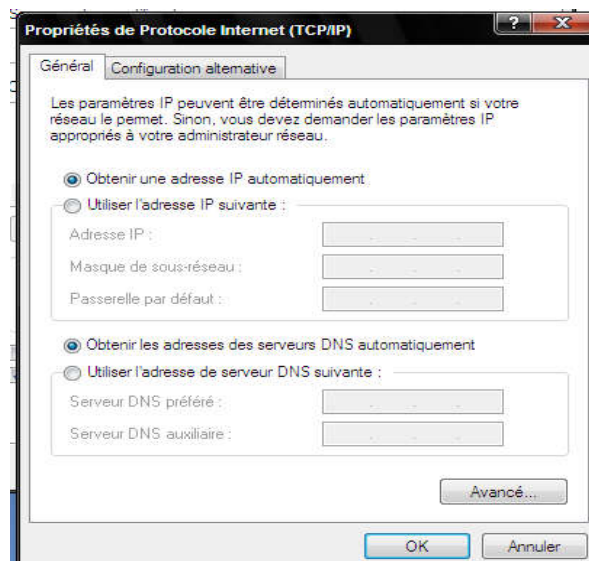


➤ Configuration automatique

Si vous choisissez de faire une configuration automatique, vous devez installer un serveur DHCP « Dynamic Host Configuration Protocol » qui permet de distribuer les adresses IP ainsi que les adresses des DNS aux stations mobiles automatiquement, dans ce TP le serveur DHCP sera installé avec le point d'accès WIFI.

Pour configurer les stations mobiles, il suffit de cliquer avec le bouton droit sur l'icône correspondant à la connexion réseau sans fil, puis de choisir « propriétés ». Puis, dans la liste des protocoles, sélectionnez « Protocole internet (TCP/IP) » et cliquez sur « Propriétés » et cliquez sur : « obtenir une adresse IP automatiquement »

Cochez aussi la case obtenir les adresses des serveurs DNS automatiquement pour que ces adresses soient fournies par le point d'accès.



3.3 Configuration du point d'accès

A. Introduction

Avant d'entamer la configuration du point d'accès, les notions qui doivent être connues préalablement sont:

- Serveur DHCP
- Serveur DNS
- SSID

➤ **Serveur DHCP**

DHCP est l'abréviation de Dynamic Host Configuration Protocol. Un serveur DHCP est un protocole TCP/IP qui permet de distribuer automatiquement une configuration IP aux équipements du réseau, il est généralement utilisé dans des réseaux où le nombre de PC est très grand ce qui rend leur configuration difficile. Une fois connecté sur un réseau local un ordinateur ou autre périphérique cherche l'existence de ce serveur pour obtenir les paramètres réseau, une fois trouvé l'ordinateur obtient une adresse IP, l'adresse du sous-réseau, passerelle par défaut, et les adresses des DNS.

➤ **Serveur DNS**

Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en en adresses IP de la machine portant ce nom.

Un nom de domaine substitue une adresse IP. Le but d'un nom de domaine est de retenir et communiquer facilement l'adresse d'un ordinateur sur internet (site web, courrier électronique, FTP). Par exemple, www.google.com est plus simple à mémoriser que 41.201.128.50.

➤ **SSID Service Set Identifier**

Le SSID, acronyme de Service Set Identifier, est le nom d'un réseau sans fil (Wi-Fi) selon la norme IEEE 802.11. Pour que des appareils sans fil puissent communiquer, ils doivent être configurés avec le même SSID. Ce nom comporte au plus 32 caractères identifiant de manière unique un réseau sans fil en mode infrastructure et en mode ad-hoc

L'objectif d'un SSID est d'empêcher que d'autres équipements sans fil n'accèdent à votre réseau local.

Un SSID est généralement diffusé par le point d'accès mais il y a la possibilité d'empêcher sa diffusion, dans ce cas le point d'accès ne sera pas détecté par les ordinateurs. Le SSID doit donc être saisi manuellement. Ce qui fait du SSID une mesure de sécurité préliminaire, il doit être renforcé par d'autres méthodes de sécurité comme le WEP et WPA.

B. Accéder au point d'accès

Pour permettre la manipulation des paramètres du point d'accès un système d'exploitation est intégré avec le point d'accès. Il faut faire une recherche dans menu de chaque paramètre « DHCP, Sécurité, SSID...etc » pour chaque modèle.

L'accès au point d'accès se fait généralement à l'aide d'un navigateur WEB « firefox, opéra, chrome...etc » en tapant l'adresse IP du point d'accès « généralement 192.168.1.1 ou 192.168.0.1 ». Pour cela il faut utiliser un câble Ethernet comme liaison avec le point d'accès et configurer l'ordinateur utilisé pour cette configuration par une adresse IP qui appartient au même espace d'adressage que le point d'accès « 192.168.1.2 ou 192.168.0.2 » et un masque de la forme 255.255.255.0 pour cette configuration (voire le TP 1).

Si la configuration est bonne et si l'adresse IP est juste (sinon vous pouvez trouver la bonne adresse IP du point d'accès dans le boîtier ou la documentation du point d'accès), chercher les menus de configuration pour :

- Configurer le serveur DHCP
- Configurer le nom du réseau SSID
- Configurer les paramètres de sécurité.

➤ Configuration du serveur DHCP

Généralement les points d'accès contiennent un serveur DHCP intégré pour distribuer les adresses IP aux stations mobiles, les paramètres réseau sont : adresse IP, masque réseau, passerelle par défaut, adresse DNS.

Dans le menu de configuration du point d'accès il y a une partie pour la configuration du « réseau local » ou vous pouvez trouver le menu correspondant au serveur DHCP et entrer les paramètres du DHCP « cet emplacement peut varier suivant le modèle du point d'accès »

- *Plage d'adresses* « 192.168.1.2 jusqu'à 192.168.1.254 »
- *Adresse sous réseau* : 255.255.255.0
- *Passerelle par défaut* : l'adresse de la passerelle internet
- *Serveurs DNS* : contient deux adresse IP « utilisé en cas de connexion à l'internet »
- *Durée de vie de chaque adresse* : c'est l'intervalle de temps dans lequel l'adresse est utilisable par une station après cette durée cette adresse peut être attribuée à une autre machine, cette technique permet de réutilise les adresses IP pour ne pas épuiser le stock des adresses IP.

The screenshot shows a router's web management interface. On the left is a navigation menu with options: Internet Setup, Wireless, Local Network, LAN IPv6, Time and Date, and Logout. The main content area is titled 'ROUTER SETTINGS' and contains the following fields and options:

- Router IP Address:** 192.168.1.1
- Subnet Mask:** 255.255.255.0
- Domain Name:** (empty field)
- Configure the second IP Address and Subnet Mask for LAN
- IP Address:** (empty field)
- Subnet Mask:** (empty field)

Below this is the 'DHCP SETTINGS (OPTIONAL)' section:

- Enable DHCP Relay
- Relay IP Address:** (empty field)
- Enable DHCP Server
- DHCP IP Address Range:** 192.168.1.33 to 192.168.1.199
- DHCP IP Mask:** 255.255.255.0
- DHCP Router IP:** 192.168.1.1
- DHCP Lease Time:** 43200 (seconds)

At the bottom, there is a section for configuring the DHCP Server on individual ports:

- LAN Port1
- LAN Port2
- LAN Port3

The URL at the bottom of the browser window is: `ge=html/index.html&var:menu=setup&var:page=lan`

➤ Configuration du SSID

Cette étape consiste à attribuer un nom au réseau sans fil, ce nom sera communiqué aux utilisateurs réseau pour leur donner accès au réseau.

Le SSID est configurable à partir du menu de *configuration du réseau local sans fil* (l'appellation peut varier selon le modèle du point d'accès)

Dans ce menu il y a au moins les paramètres suivants :

- **Le nom réseau ou SSID** : ce champ contient le nom pour le réseau local sans fil
- **Visible ou non visible** : ce bouton permet d'activer ou désactiver la visibilité du SSID par les visiteurs de votre réseau
- **La région** : pour définir la région où vous installer votre réseau, car et par suite du règlement de chaque pays les bandes de fréquence ne sont pas toutes autorisées donc il faut mentionner la région.
- **Mode 802.11** : dans ce champ il faut mentionner la version du 802.11 que les stations mobiles peuvent supporter « A, G ou N », vous devez faire un choix supporté par tous les clients de votre réseau, parce qu'ils existent des anciennes cartes WIFI qui ne supportent pas le 802.11n ou même le 802.11g.

8.1.1/cgi-bin/webproc

Product Page: DSL-2750U Firmware Version:ME_1.03

D-Link

DSL-2750U // SETUP ADVANCED MANAGEMENT STATUS HELP

Wizard
Internet Setup
Wireless
Local Network
LAN IPv6
Time and Date
Logout

WIRELESS BASIC

Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS NETWORK SETTINGS

Enable Wireless:

Enable MultiAP Isolation:

Wireless Network Name (SSID): licence3

Visibility Status: Visible Invisible

Country/Region: United Arab Emirates

Control Sideband: Upper

Wireless Channel: Auto Scan

802.11 Mode: 802.11b/g/n

Band Width: 20 M



Remember your SSID as you will need to configure the same settings on your wireless devices and PC.

Apply Cancel

BROADBAND

3.4 Configuration de la sécurité

Un réseau sans fil est beaucoup plus sensible qu'un réseau filaire aux attaques car les données circulent librement dans l'air, ce qui les rendent très vulnérables aux attaques réseau ce qui remet en cause l'utilité de notre réseau WIFI car n'importe quelle personne avec une antenne WIFI et un PC ou PDA peut capter, modifier ou supprimer les données transmises sur ce réseau.

Un réseau WIFI est cible d'une variété d'attaques :

- L'écoute clandestine et analyse de trafic « Le War Driving ».
- Création de système radio générant du bruit dans la bande des 2,4GHz ou 5 GHz.
- Génération de trafic inutile à travers le point d'accès
- Installation d'un Point d'accès « malicieux » pour détourner le trafic

Vu le nombre d'attaques et la facilité de les exécuter, il est indispensable de mettre en œuvre un mécanisme de sécurité robuste afin de protéger les données sur un réseau local WIFI.

De nos jours tous les points d'accès sont livrés avec plusieurs implémentations de protocoles de sécurité telle que WEP, WPA

Dans la section suivante en va citer en bref l'évolution des solutions de sécurité qu'a connue le monde du WIFI.

a) Sécurité par le SSID

C'est le mécanisme de sécurité de base et qui consiste à affecter à chaque point d'accès un identificateur unique «SSID (Service Set Identifier) » connu seulement par les utilisateurs du réseau, le client et le point d'accès doivent avoir le même SSID pour s'associer.

Le SSID n'offre aucun niveau de sécurité même s'il est caché et , ce qu'est le cas contraire dans la majorité des point d'accès car généralement les points d'accès émettent leur SSID.

b) Filtrage des adresses MAC

Dans un réseau local, chaque carte réseau (WIFI ou Ethernet) possède une adresse physique unique qui lui est propre (appelée adresse MAC). Cette adresse est représentée par 12 chiffres hexadécimaux .

Le filtrage MAC consiste à créer une liste des adresses MAC autorisés à se connecter au point d'accès, seuls les utilisateurs ayant enregistré leurs adresses MAC auprès du point d'accès peuvent s'associer à ce dernier, le reste des ordinateurs sera rejetés.

Cette solution n'est pas pratique dans des réseaux de grande taille car l'administrateur réseau doit connaître toutes les adresses MAC de tous les ordinateurs au préalable. D'autre part, le filtrage MAC est facilement contournable par le changement de l'adresse MAC d'un ordinateur non autorisé par une adresse MAC d'un ordinateur légitime ce qui lui donne la possibilité de s'associer au point d'accès.

c) WEP - Wired Equivalent Privacy

Dans les solutions précédentes les données sont émises en claire sur un réseau WIFI, donc il y a toujours la possibilité pour un attaquant de capter et lire ces données à l'aide d'une antenne WIFI et des logiciels d'espionnage dédiés.

Le protocole WEP propose donc de chiffrer les données échangées sur un réseau WIFI entre les stations mobiles et le point d'accès, de cette façon les données sont protégées contre l'écoute clandestine.

Le principe du WEP consiste à chiffrer les échanges sur le réseau en utilisant un algorithme symétrique « RC4 » avec des clés d'une longueur de 64 bits ou 128 bits. Cette clé est partagée par tous les utilisateurs du réseau, c'est-à-dire que seuls les utilisateurs ayant cette clé peuvent se connecter au réseau.

Wired Equivalent Privacy

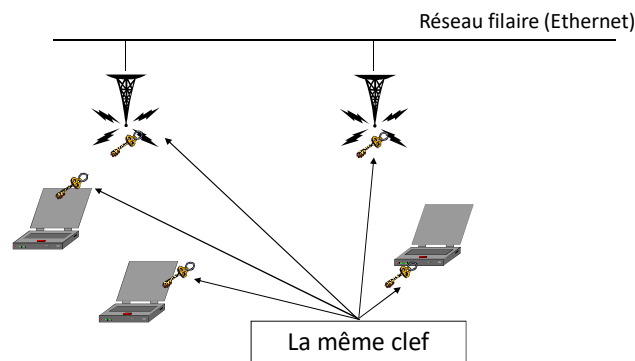


Figure II.6 sécurité WIFI

Bien que le WEP présente un bon seuil de sécurité par rapport aux autres solutions mais il présente certaines faiblesses :

- Les Clés sont statiques et rarement changées
- La clé peut être volée suite au vol d'une machine
- Les autres qui partagent la clé peuvent lire les données du reste des utilisateurs
- WEP peut être craqué en utilisant des logiciels comme : Aircrack-ng et Weptoolkit : <http://aircrack-ng.org/>

d) WPA WiFi protected Access

Vu les faiblesses qu'a présenté le WEP, la communauté de développement du WIFI « **WiFi Alliance** » a proposé en 2004 un nouveau protocole nommé WPA (**WiFi protected Access**), ce protocole dans sa version finale WPA2 sera basé sur un nouveau algorithme de cryptage AES « **Advanced Encryption Standard** » et un changement dynamique de clés ce qui permet un haut niveau de sécurité.

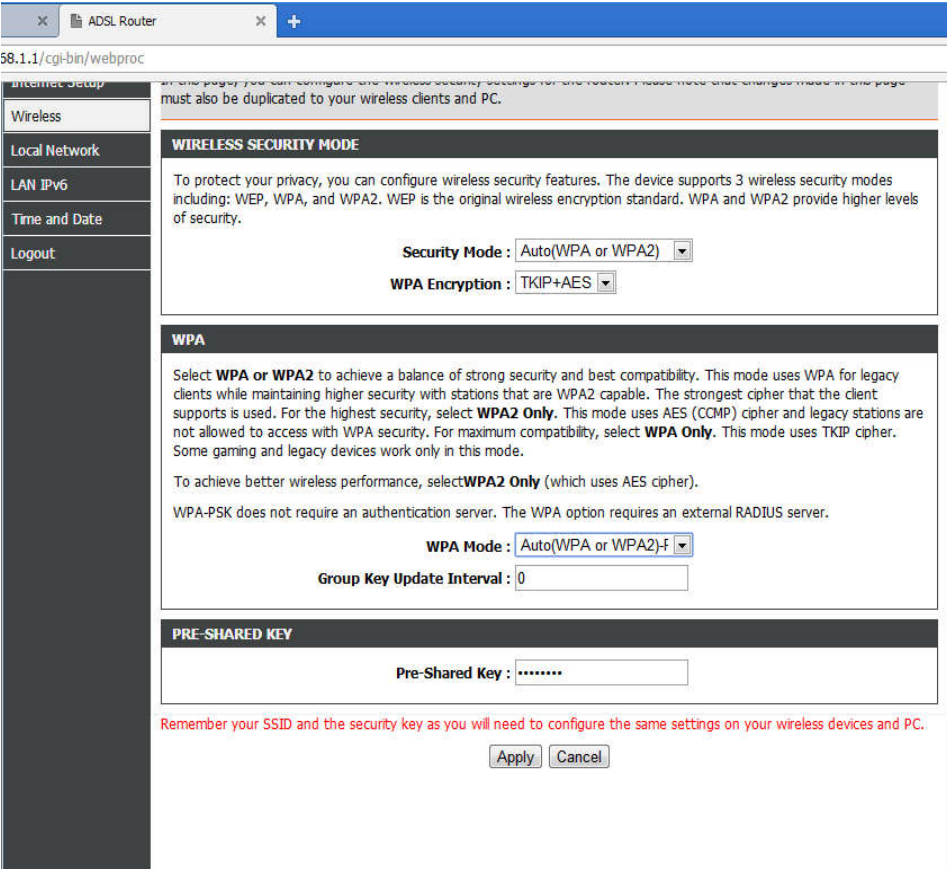
Cette solution se présente sous deux versions :

- **WPA-Personnel**: conçu pour des réseaux personnels ou de petite taille assurant la sécurité à l'aide un mot de passe de plus de 8 caractères
- **WPA Entreprise «WPA 802.1x** » basé sur l'utilisation des logins et des mots de passe mais nécessite l'installation d'un serveur RADIUS, cette solution est conçue pour les réseaux d'entreprise.

e) Activation de la sécurité sur le point d'accès

Dans le menu de configuration du point d'accès chercher l'onglet de configuration de la sécurité sans fil « cet emplacement peut varier suivant le modèle du point d'accès » dans cet onglet vous trouverez toutes les méthodes de sécurité présentées ci-dessus, choisissez l'une des méthodes présente dans cette page et remplissez les champs de ce choix.

Exemple si vous choisissez WPA2 personnel vous devez entrer une pre-shared key de 8 caractères cette chaine de caractère doit être introduisez par chaque nouvel utilisateur du réseau.



The screenshot shows the configuration page for wireless security on an ADSL Router. The browser address bar shows '58.1.1/cgi-bin/webproc'. The page has a sidebar menu on the left with options: Internet Setup, Wireless, Local Network, LAN IPv6, Time and Date, and Logout. The main content area is titled 'WIRELESS SECURITY MODE' and contains the following sections:

- WIRELESS SECURITY MODE**: A text block explaining security features and three modes: WEP, WPA, and WPA2. Below this are two dropdown menus: 'Security Mode' set to 'Auto(WPA or WPA2)' and 'WPA Encryption' set to 'TKIP+AES'.
- WPA**: A text block explaining WPA and WPA2 modes. Below this are two dropdown menus: 'WPA Mode' set to 'Auto(WPA or WPA2)-F' and a 'Group Key Update Interval' field set to '0'.
- PRE-SHARED KEY**: A text field for the 'Pre-Shared Key' with a masked input (dots).

At the bottom, there is a red warning message: 'Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.' and two buttons: 'Apply' and 'Cancel'.

TP III

Installation d'un réseau local avec plusieurs points d'accès

Le but de ce TP est d'installer un réseau local composé de plusieurs segments sans fil « chacun avec un point d'accès ». Chaque point d'accès est supposé être installé dans un étage d'un grand immeuble ou dans un département d'une faculté. Cette installation est généralement faite pour étendre le réseau local existant « système de distribution » car d'une part, les prises Ethernet sont insuffisantes vu le nombre croissant des utilisateurs et d'autre pour donner l'accès aux dispositifs mobile comme les Smartphones qui ont besoin des réseaux WIFI pour se connecter à l'internet.

Le réseau doit donner la possibilité aux utilisateurs ayant des Smartphones et des laptops de se connecter librement à l'internet tout en assurant la continuité de connexion même si l'utilisateur change de position « déplacement entre les départements ou les étages » en se connectant au point d'accès le plus proche.

La situation qu'on va étudier est similaire au réseau de la faculté de technologie, où les bureaux sont connectés à l'internet par le biais d'un réseau Ethernet. Cette installation est obsolète car le nombre d'utilisateurs est fixé par le nombre des prises Ethernet envisagées au début de la construction de la faculté ce qui n'est pas pratique aujourd'hui d'un point de vue extensibilité et flexibilité. La nouvelle installation va permettre aux utilisateurs « étudiants et enseignants de bénéficier de l'internet en utilisant le WIFI (smart phone, tablette et PC).

Dans ce TP on va réaliser une installation similaire à cette situation, en utilisant deux point d'accès (déjà utilisé dans le TP 2), ensuite on va relier ces points d'accès entre eux par un réseau Ethernet (câble RJ45), ensuite on va configurer chaque point d'accès (SSID, sécurité, DHCP, DNS, passerelle par défaut) pour permettre aux utilisateurs de se connecté à internet.

L'installation de ce réseau est réalisée dans quatre étapes :

1. Configuration de chaque point d'accès pour éviter le conflit d'adresses
2. Installation du réseau Ethernet reliant les points d'accès par des câbles RJ45
3. Configuration d'un seul serveur DHCP pour éviter le conflit d'adresses et pour distribuer les paramètres de connexion aux utilisateurs (adresse IP, passerelle par défaut, serveurs DNS)
4. Test de configuration : dans cette étape on va essayer d'installer des cartes WIFI sur des PC de bureau, leur donner des noms et partager des répertoires comme dans le TP 1

1. Configuration de chaque point d'accès pour éviter le conflit d'adresses

Pour relier les points d'accès entre eux il faut les reconfigurer pour qu'ils aient des adresses IP uniques différentes les uns des autres car dans un même réseau chaque équipement doit avoir une adresse unique ce qui n'est pas le cas si on raccorde les points d'accès directement car généralement les point d'accès ont la même adresse IP 192.168.1.1.

Pour changer l'adresse IP du point d'accès, relier le point d'accès à un PC à l'aide du câble RJ45 (voir TP 2) chercher dans le menu ou changer l'adresse IP, et donne lui une nouvelle adresse unique qui doit être différente du reste des point d'accès par exemple :

Point d'accès 1 : 192.168.1.2,

Point d'accès 2 :192.168.1.3,

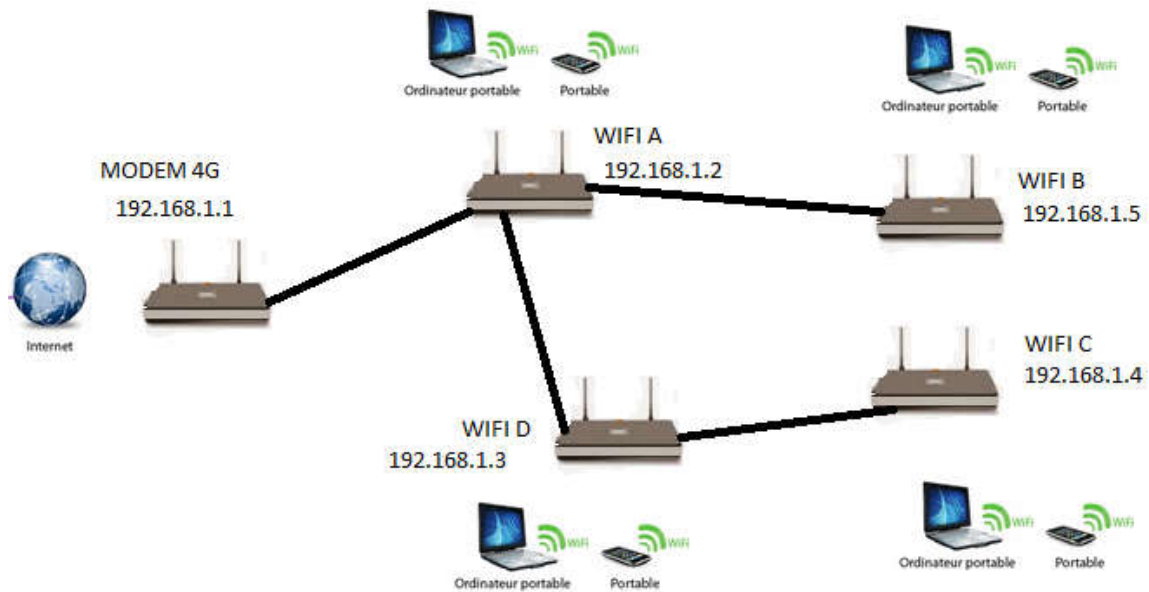
Point d'accès 3 :192.168.1.4,

Point d'accès 4 :192.168.1.5....etc

Point d'accès 0 : 192.168.1.1 ce point d'accès est un modem 4 G et il va jouer le rôle du serveur DHCP et passerelle par défaut pour connecter a l'internet.

2. Installation du réseau Ethernet

Après avoir affecté à chaque point d'accès une adresse IP unique et différente des autres points d'accès, ils sont maintenant prêts pour être relier entre eux par des câbles RJ 45, comme dans la figure ci-dessous.



3. Configuration des points d'accès

La configuration des points d'accès consiste à :

- 1- **Donner à chaque point d'accès un SSID**, dans le TP on va donner à chaque point d'accès le même SSID, dans la pratique les point d'accès sont installés dans des endroits éloignés mais dans notre cas on ne peut pas le faire à cause du manque de l'espace (superficie réduite du laboratoire).
- 2- **Configurer les paramètres de sécurité** : chercher dans le menu du point d'accès l'emplacement pour paramétrer la sécurité et choisir la méthode WPA2 et donner un mot de passe de huit caractères qu'est le même pour tous les point d'accès exemple « 12345678 »
- 3- **Configuration du DHCP** : comme vu dans le deuxième TP un serveur DHCP est responsable de la distribution des paramètres réseau « adresse IP, masque sous réseau, passerelle par défaut, adresse de DNS », dans un réseau il ne doit pas avoir plus d'un seul serveur DHCP pour qu'il n'y aura pas de conflit d'adresses IP en cas ou deux serveurs DHCP donnent la même adresse IP pour deux équipements dans le même réseau cela pourra bloquer la connexion. Donc on doit désactiver le serveur DHCP sur

tous les points d'accès et l'activer seulement au niveau du modem 4 G qui va jouer le rôle du serveur DHCP ainsi que la passerelle par défaut pour la connexion à l'internet.

Dans ce point d'accès « modem 4 g » configurer le serveur DHCP pour donner la configuration suivante :

- Des adresses IP allant de 192.168.1.6 jusqu'à 192.168.1.100 avec une durée de vie des adresses IP de 2 heures.
- Les adresses IP des serveurs DNS qui va les distribuer aux stations
 - ✓ DNS1 → 8.8.8.8
 - ✓ DNS → 8.8.4.4
- Masque de sous réseau : 255.255.255.0

4. Test de configuration

Installation et configuration des stations : Pour tester la configuration, installer les cartes WIFI sur chaque PC du laboratoire.

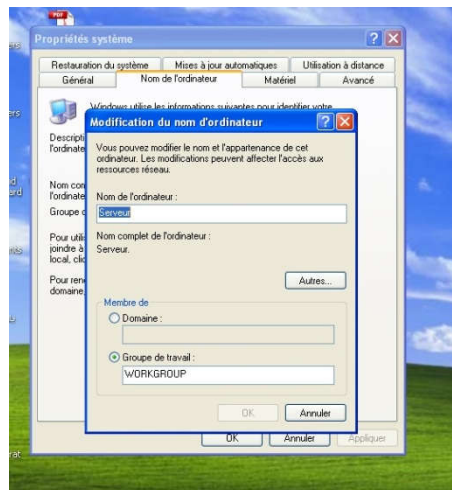
Sur chaque PC connecter à l'un des points d'accès qu'on a configuré précédemment, et vérifier si chaque station a bien obtenu sa configuration réseau en tapant la commande ipconfig /all.

Si la configuration est bien établie lancer la commande ping vers une autre station sur le réseau si le ping marche le réseau est bien configuré sinon il faut refaire la configuration.

5. Partage de fichiers

Maintenant si la configuration est bien faite, on doit refaire les étapes du TP 1 pour partager des dossiers et des imprimantes sur le réseau.

4. Faites un clic droit sur poste de travail, puis cliquez sur Propriétés.
5. Sous l'onglet Nom de l'ordinateur, cliquez sur Modifier, vous pouvez aussi donner une description à cet ordinateur (cette description sera affichée pour les utilisateurs réseau pour leur donner une vision de la tâche de ce dernier sur le réseau).
6. Sous Nom de l'ordinateur, supprimez l'ancien nom de l'ordinateur, tapez un nouveau nom, puis cliquez sur OK. Vous pouvez aussi entrer un nom du groupe de travail.
7. Sous l'onglet groupe de résidentiel ou groupe de travail, supprimez l'ancien nom, tapez le nouveau nom du groupe « TP3 », puis cliquez sur OK.



Pour partager un répertoire suivez les étapes :

6. Faites un clic droit sur le répertoire, puis cliquez sur Propriétés.
7. Allez à l'onglet partage et cocher la case partager ce dossier.
8. Si cette case n'est pas active cliquez sur le lien activer le partage de fichier et d'imprimantes et suivez les étapes.
9. A la fin de ces étapes la case partager ce dossier sera activé.
10. Si vous voulez donner la possibilité aux utilisateurs de modifier le contenu de ce dossier cochez la case autorisé les utilisateurs réseau à modifier mes fichiers.

6. Connexion à l'internet :

Si le modem 4G contient un abonnement internet, vérifiez si chaque PC ou Smartphone peut se connecter à l'internet.

Remarque

Si la zone géographique est assez grande on peut utiliser le même nom pour tous les points d'accès, et pour permettre le déplacement entre les points d'accès tout en assurant

TP IV

Analyse de trafic réseau

Ce TP a comme projet l'initialisation des étudiants dans le domaine d'analyse du trafic ainsi que la compréhension de la structure des paquets TCP/IP.

Ce TP donne une pratique indispensable pour les étudiants pour comprendre et appréhender les concepts des réseaux informatiques en leur donnant la possibilité de toucher et analyser des paquets et des échanges en temps réel.

Ce TP permet aux étudiants de compléter leurs acquis dans le domaine des réseaux à savoir les protocoles comme le DHCP, TCP, UDP...etc en analysant les échanges réseaux mettant en place ces protocoles.

1- Matériels et logiciels nécessaires

Avant de commencer l'analyse du trafic réseau une installation d'un réseaux local est nécessaire « voir TP 1,2,3 » ce réseau peut être WIFI ou Ethernet. Pour cela on besoin du matériel suivant :

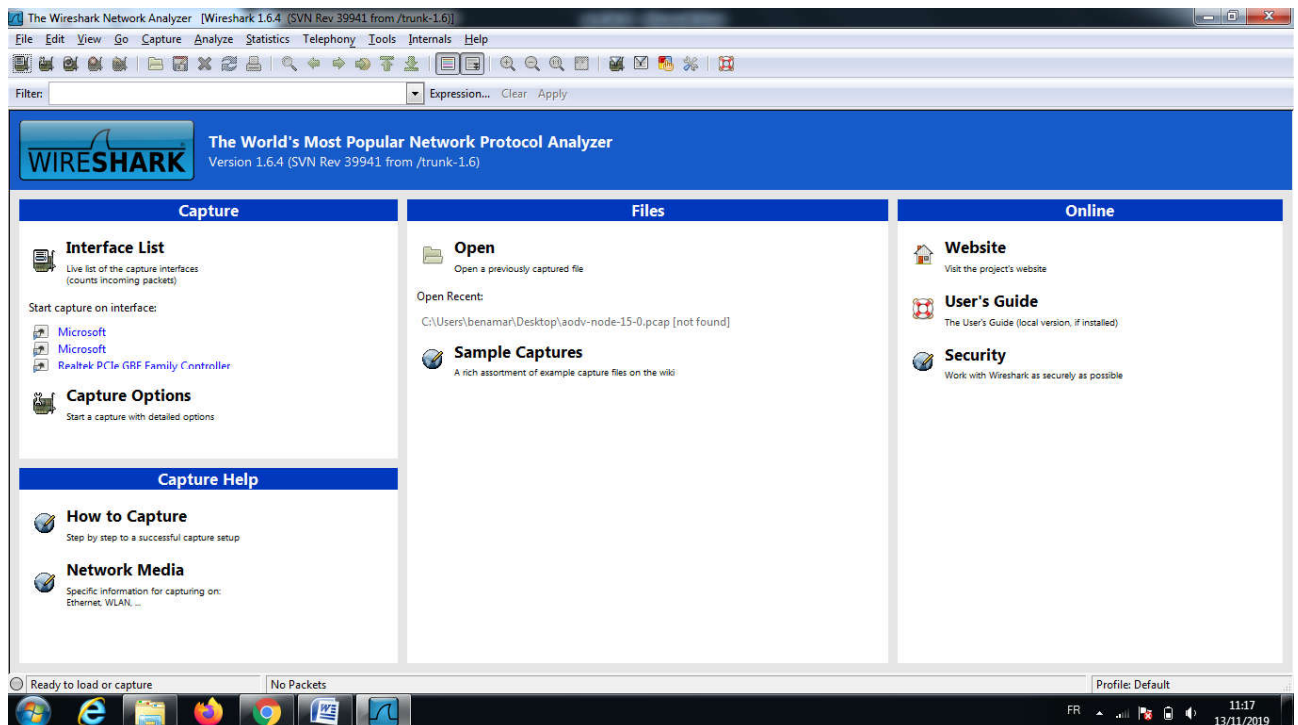
- **Les équipements**
 - Des PCs équipés chacun d'une carte réseau filaire (Ethernet) et/ou sans fil (Wifi)
 - Des câbles RJ45
 - Switch et/ou point d'accès
- **Les logiciels :**
 - Analyseur réseau (wireshark)

2- Présentation du Wireshark :

Wireshark est un logiciel, libre, de capture de trafic (un analyseur réseau : sniffer). Il utilise directement l'interface de communication (Ethernet, Wifi,...) d'une machine pour réaliser la capture des informations circulants sur le réseau (trames, paquets, protocoles...)

2.1 Capture de trafic :

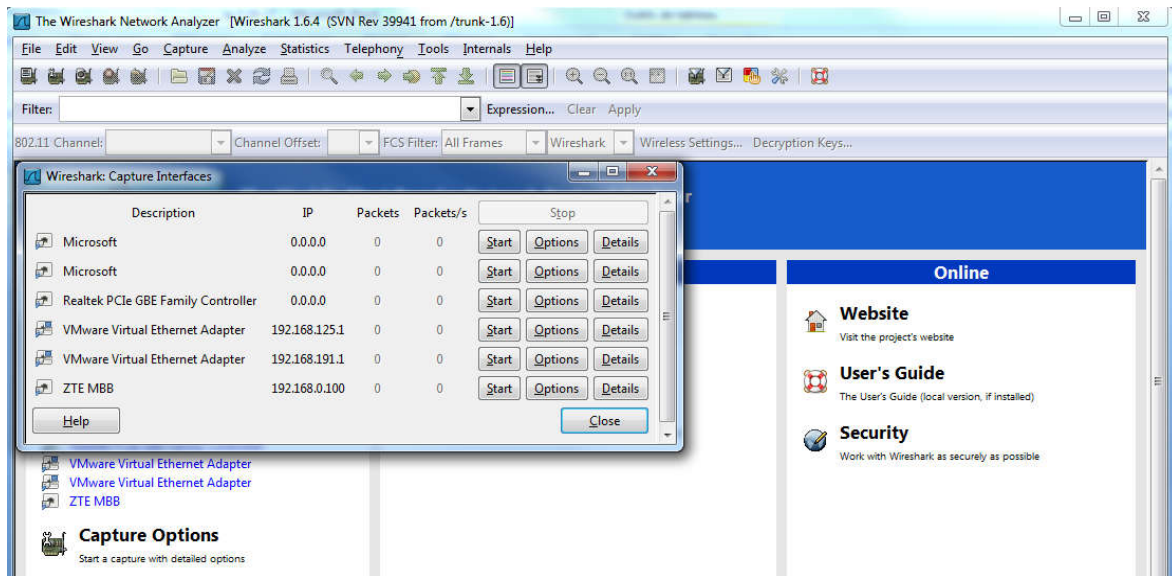
Lancez le Wireshark, vous devriez voir obtenir une fenêtre similaire à celle-ci :



Pour lancer une capture de trafic, vous devez sélectionner l'interface à partir de laquelle vous souhaitez analyser le trafic. Un ordinateur, peut disposer de plusieurs interfaces, correspondantes à des cartes réseaux réelles (Ethernet, Wifi) ou virtuelles.

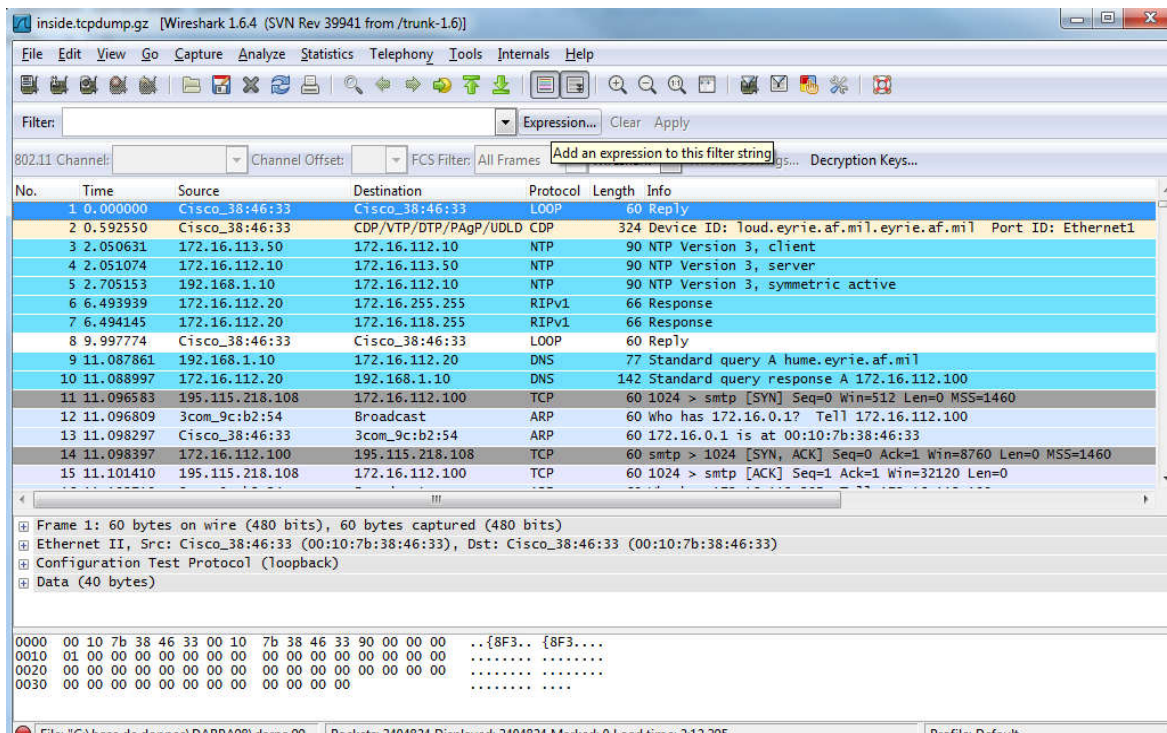
La sélection de l'interface de capture se fait à travers :

- « **Start capture on interface** » dans la colonne « **capture** »
- de menu **Capture/ interface**



Une fois la carte choisie, il suffit, pour capturer, de cliquer sur « **Start** »

La capture va alors démarrer et vous aurez une fenêtre qui ressemble à la figure suivante :



Pour arrêter la capture : **Menu \ Capture \ Stop**

Le résultat d'une capture se présente sous la forme d'un fichier « découpé » en trois parties :

- 1) Une partie supérieure contenant la liste les trames capturées (adresse source, destinataire, physique ou IP, protocole,...).
- 2) Une partie centrale permettant d'avoir le détail des différents champs de la trame, d'un paquet ou un segment.
- 3) Une partie inférieure donnant la trame en Hexa avec sa correspondance ASCII.

2.2 Analyse de la Capture (analyse de trafic) :

L'écran de capture présente toutes informations échangées dans le réseau.

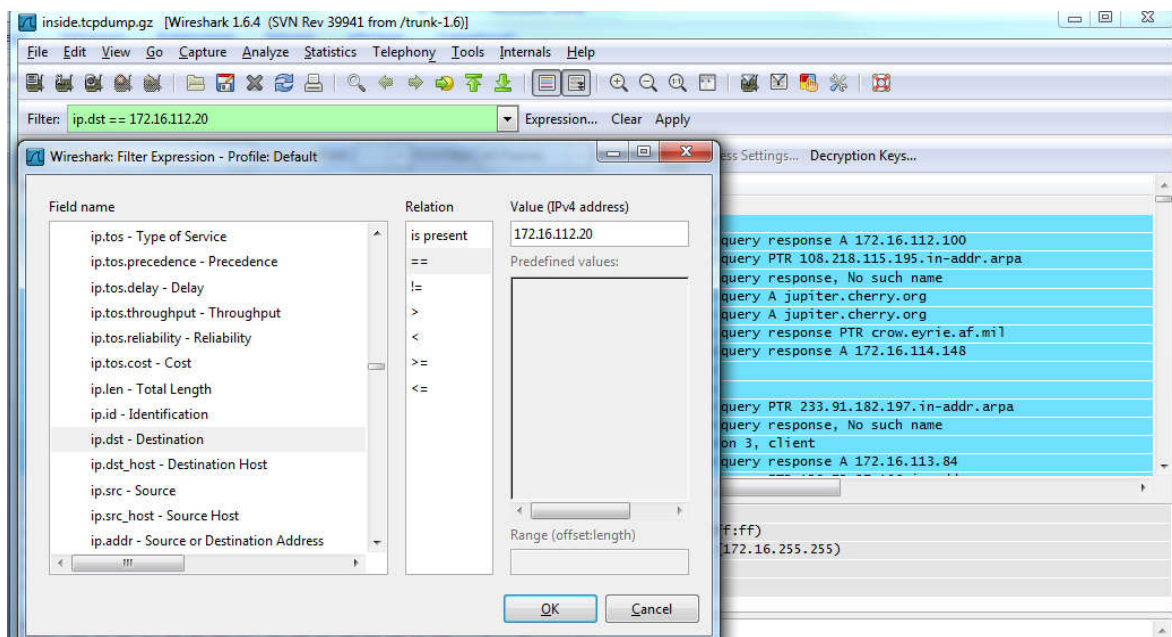
Il est possible de créer des filtres d'affichage qui permettent de masquer ou visualiser les trames suivant une ou plusieurs règles. Cela permettra d'isoler :

- Un échange en particulier ou l'analyse d'un protocole spécifique : IP, TCP, UDP, ICMP, ARP, DNS....
- Les conversations d'une Adresse IP (source ou destination),
- Paquets et champs spécifique dans une trame, un paquet...
- ...

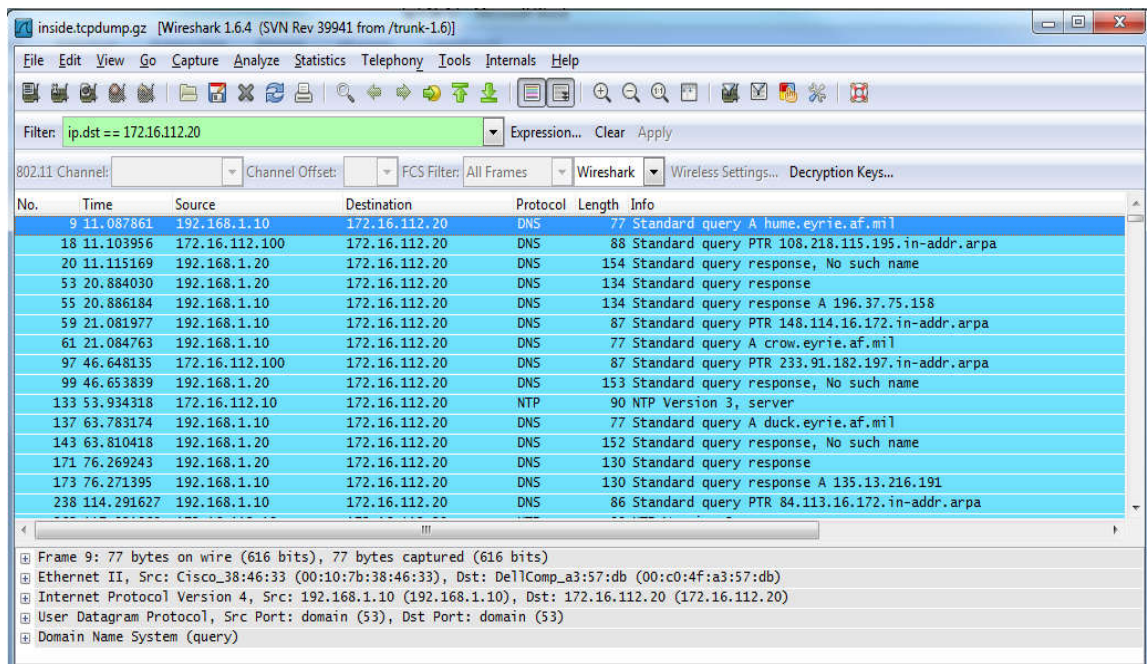
Le bouton « **Expression** » permet d'accéder à un assistant pour créer une règle de filtrage préconfiguré, comme il est possible de créer de nouvelles règles en les tapant directement dans **Filter**.

Une règle de filtrage s'appuie sur les champs des entêtes (header) des protocoles connus du logiciel Wireshark :

Par exemple, si vous s'intéressez au trafic reçu par la machine ayant l'adresse IP : 172.16.112.20 :



Après filtrage, vous obtenez :



2.3 Exemple de filtrage :

Connexion TCP :

- **Tous TCP** : tcp
- **Numéro de port** : source (tcp.srcport==), et/ou destination (tcp.dstport==)
- **Les drapeaux** : SYN : (tcp.flags.syn==1) et/ou ACK (tcp.flags.ack==1) ou (tcp.flags.syn== 1 && ACK tcp.flags.ack== 0)...

Protocole IP :

- **Tous IP** : ip
- **Adresses ip** : adresse (ip.addr==), adresse source(ip.src==) et/ou adresse destination (ip.dst==)
- **Bit DF** : (ip.flags.df == 1)...

3- Applications

3.1 Analyse de la capture du ping

- Créez un réseau local (entre deux ou plusieurs pc)
- Capturez et analysez les messages du ping.

3.2 Analyse le trafic de la capture d'un échange d'un serveur web :

- L'adresse IP du client
- Le serveur DNS
- Les sites visités

Références bibliographiques

1. José DORDOIGNE, Réseaux informatiques Notions fondamentales, 6eme édition, 2015
2. Philippe ATELIN. Réseaux informatiques, Notion fondamentales (Normes, Architectures, Modèle OSI, TCP/IP, Ethernet, WI-FI,...) Edition Eni, 3eme EDITION, 2009
3. Guy Pujolle, " les Réseaux", édition 2008.
4. <https://www.microsoft.com/>
5. Fabrice Lemainque, Tout sur les réseaux et Internet, 4e édition 2005
6. Romain LEGRAND et André VAUCAMPS, Les réseaux avec Cisco Connaissances approfondies sur les réseaux, 2ième édition, 2015
7. Aurélien Géron, WiFi Professionnel La norme 802.11, le déploiement, la sécurité, 3ème édition, 2009