République Algérienne Démocratique & Populaire

Ministère de l'Enseignement Supérieur & de la Recherche Scientifique

Université Dr Moulay Tahar de Saida

Faculté de technologie

Département d'informatique

Polycopié pédagogique

Réseaux

Niveau : deuxième année licence Informatique

Dr Kadda BENYAHIA

Maitre de conférences -A- en informatique

Kadda.benyahia@univ-saida.dz

Octobre 2022

Tables des matières

Liste des figures	5
Liste des tableaux	8
Avant-propos	9
Introduction aux réseaux	
Définition	10
Avantages des réseaux	10
Architectures des réseaux	11
les topologies	12
Topologie en bus	12
Topologie en Etoile	13
Topologie en Anneau	14
Topologie maillée	14
Les équipements réseaux	15
le répéteur (repeater)	15
Le concentrateur (HUB)	15
les types des réseaux	16
LAN : Réseau Local	16
MAN : Réseau métropolitaine	17
WAN : Réseau Étendu	17
Protocole	18
Les modèles de références	20
Le modèle OSI	20
Les couches du modèle OSI	21
Le modèle Tcp/ip	22
La couche hôte réseau	22
La couche internet	23
La couche transport	24
La couche application	24
Fonctions de la couche physique	26
Les éléments d'une transmission	26
Le Débit	27
Modes de transmission	27
Simplex (simplex):	27
Semi-duplex:(half-duplex)	27
Semi-duplex(full-duplex):	27
les transmissions parallèle /série	28

la transmission parallèle 28
la transmission série 28
Transmission synchrone /asynchrone 29
Transmission synchrone 29
transmission Asynchrone 29
Les supports de transmission 29
médias en cuivre 29
paires torsadées 29
média optique 30
Média sans fils (wireless network) 32
Bluetooth 32
Wifi (Wireless Fidelity) 32
Les équipement de la couche physique 33
Répéteur (repeater) 33
Concentrateur (hub) 33
le modem 33
Fiche TD1 35
Couche liaison de données
Détection des erreurs 37
La parité 37
Les codes à redondance cyclique (CRC) 38
La carte réseau 39
La technologie Ethernet 41
Trame ethernet 41
Contrôle d'Accès multiple 42
CSMA/CD (Carrier sense multiple access with collision detection) 42
TOKEN RING (passage de jeton) 43
Fiche TD2 44
Couche réseaux
Notions fondamentales 48
L'Adressage 48
Encapsulation 49
Routage 49

Désencapsulation 49
L’adressage IP 49
Définition 49
Format Des Adresses 50
Classe D’adresses 51
Adresse De Bouclage 51
Adresse De Bouclage 52
L'adresse réseau 53
L’adresse de diffusion (broadcast) 53
Adresse privée 53
Adresse IP Publique 54
le masque de réseau 54
Calcul sous réseaux 56
Démarche 56
Exemple de subnetting 57
Le routage 59
Routage statique 60
Routage dynamique 61
Les différents protocoles de routage 62
Le protocole de routage RIP 63
Le protocole OSPF (OPEN SHORTEST PATH FIRST) 64
Fiche TD3 65
Couche transport
Introduction 68
La procédure de communication entre applications 69
La relation entre la couche transport et la couche réseau 71
Les services de la couche transport 71

Les protocoles de la couche transport **75**

Le protocole UDP (**U**ser **D**atagram **P**rotocol) **75**

Le protocole TCP **77**

Fiche TD4 **81**

Couches applicatives

La couche session **83**

La couche Présentation **83**

La couche Application **84**

les protocoles de la couche application **85**

SMTP : le protocole de transmission de mail **86**

HTTP (Le service web) **88**

FTP (Le service de transfert de fichier) **90**

DHCP : Dynamic Host Configuration Protocol **91**

Séries de travaux pratiques

TP1 **93**

TP2 **97**

TP3 **102**

TP4 **105**

TP5 **109**

Références bibliographiques **111**

Liste des figures

Fig I.1 Architecture client/serveur 11
Fig I.2 Architecture Peer to Peer 12
Fig I.3 Topologie en bus 12
Fig I.4 Topologie en étoile 13
Fig I.5 Topologie en Anneau 14
Fig I.6 Topologie maillée 14
Fig I.9 Le répéteur 15
Fig I.10 Le concentrateur 15
Fig I.11 Routeur 16
Fig I.12 Réseau Local (LAN) 17
Fig I.13 Réseau MAN 17
Fig I.14 Réseau WAN 18
Fig I.15 Relations entre couches 20
Fig I.16 Le modèle OSI 21
Fig I.17 Modèle OSI vs modèle TCP/IP 23
FigII.1 Les éléments d’une transmission 26
Fig II.2 Modes de transmission 27
Fig II.3 transmission parallèle 28
Fig II.4 transmission Série 28
Fig II.5 Câble UTP 29
Fig II.6 Connecteur Rj45 29
Fig II.7 Cable coaxial 30
Fig II.8 Connecteur BNC 30
Fig II.9 fibre optique 31
Fig II.10 Structure d'une fibre optique 32
Fig II.11 Connecteurs fibre optique 32
Fig II.12 Technologie bluetooth 33

Fig II.13 Répeteur 33
Fig II.14 concentrateur (hub) 34
Fig II.15 fonctionnement d'un modem 34
Fig III.1 Carte réseau 39
Fig III.2 Sous couche LLc 40
Fig III.3 Format de la trame Ethernet 41
Fig III.4 CSMA/CD 43
Fig IV.1 Besoin d’adressage 50
Fig IV.2 Format d’adresse IP 50
Fig IV.3 Adresse IP Classe A 51
Fig IV.4 Adresse IP Classe B 52
Fig IV.5 Adresse IP Classe C 52
Fig IV.6 Masque sous réseau 55
Fig IV.7 Opération Et logique 54
Fig V.1 Les couches applicatifs 69
Fig V.2 Procédure de communications entre applications 70
Fig V.3 Etapes de Connexion 80
Fig VI.1 Fonctionnement du protocole SMTP 87
Fig VI.2 protocole http : fonctionnement 89
Fig VI.3 processus FTP 90
Fig VI.4 DHCP 91

Liste des tableaux

Tableau IV.1 plages d'adresses **59**

Tableau V.2 les deux types de communication **68**

Tableau V.1 les catégories des numéros de ports **73**

Tableau V.2 Numéros de ports répandus **74-76**

Avant-propos

Le contenu de ce cours est issu d'un cours qui s'adresse aux étudiants de deuxième année informatique et s'adresse aussi à tout lecteur désireux de s'initier aux réseaux informatiques.

A travers ce cours, le lecteur peut Acquérir une connaissance pratique et théorique des réseaux informatique et comprendre le principe de son fonctionnement à travers le modèle de référence OSI et ses couches.

Introduction aux réseaux

1

I. Définition :

Un réseau est un ensemble d'équipements connectés afin de réaliser des tâches bien précises :

- Le partage des ressources matériels et logiciels

-L'échange des fichiers

-La communications

II- Avantages des réseaux

Les réseaux informatiques offrent actuellement plusieurs services aux utilisateurs :

1- L'enseignement : les réseaux permettent

- La création de classes virtuelles ;
- La diffusion vidéo à la demande ;
- Les espaces d'apprentissage collaboratifs ;
- L’apprentissage sur appareils mobiles.

2-La **communication** : les réseaux permettent aux utilisateurs de se communiquer de différentes façon (**- Messagerie instantanée/messages texte** ;-**Réseaux sociaux ;blogs , p2p ,..)**

3-Le travail : Travailler à distance (télétravail), les réseaux permettent la transmission de nombreux types de service d'informations, parmi lesquels les e-mails, la vidéo, les messageries et la téléphonie.

4- Consommer différents produits avec les paiements sécurisés en ligne

III- Architectures des réseaux

1.client/serveur

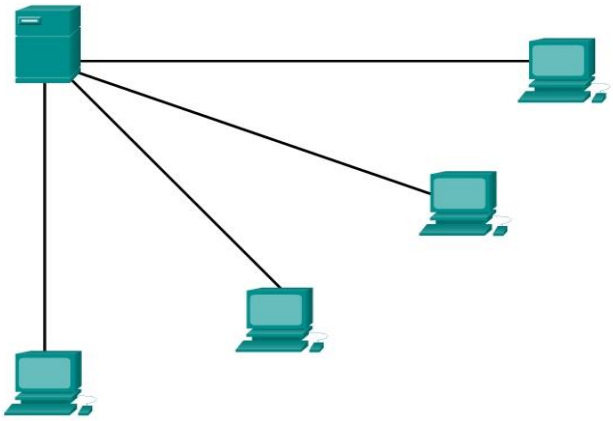


Fig I.1 Architecture client/serveur

- Le client émet une requête vers le serveur grâce à son adresse et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port

2/point à point (Peer to Peer)

Dans un réseau point à point chaque poste est **à la fois client et serveur**. Toutes les stations ont le même rôle

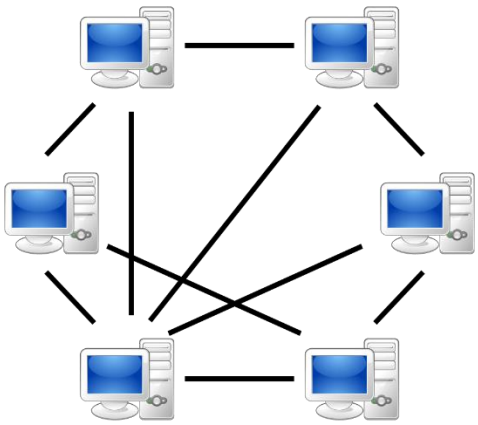


Fig I.2 Architecture Peer to Peer

IV. les topologies

La topologie d'un réseau représente la façon avec laquelle les équipements sont interconnectés et donc la configuration réelle du câblage. Nous citons :

IV.1Topologie en bus

Dans cette topologie, tous les ordinateurs sont connectés entre eux par le biais d'un seul câble réseau débuté et terminé par des **terminateurs**. Les terminateurs ont pour but de maintenir les (signaux électriques dans le câble et d'empêcher les "rebonds" des données le long du fil.

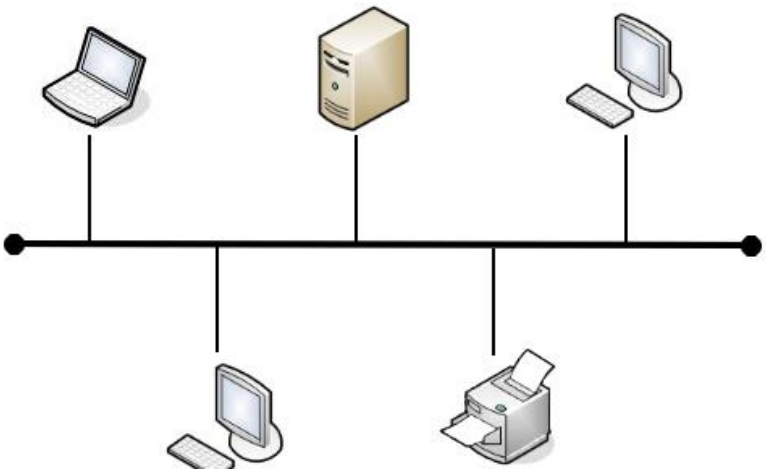


Fig I.3 Topologie en bus

Il est caractérisé par

-Toutes les machines utilisent le même câble.

-Vitesse de transmission faible

IV.2. Topologie en Etoile

La forme physique du réseau ressemble à une étoile, toutes les machines se connectent à un équipement central (qui est généralement un commutateur) et chaque communication entre ces machines doit passer par cet équipement.

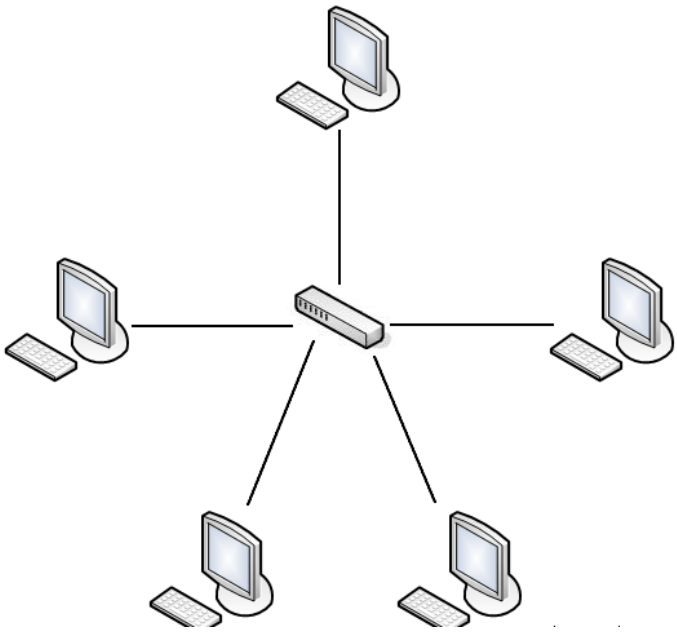


Fig I.4 Topologie en étoile

Le principal défaut de cette topologie, c'est que si l'élément central ne fonctionne plus, plus rien ne fonctionne : toute communication est impossible. Cependant, il n'y a pas de risque de collision de données.

IV.3- Topologie en Anneau

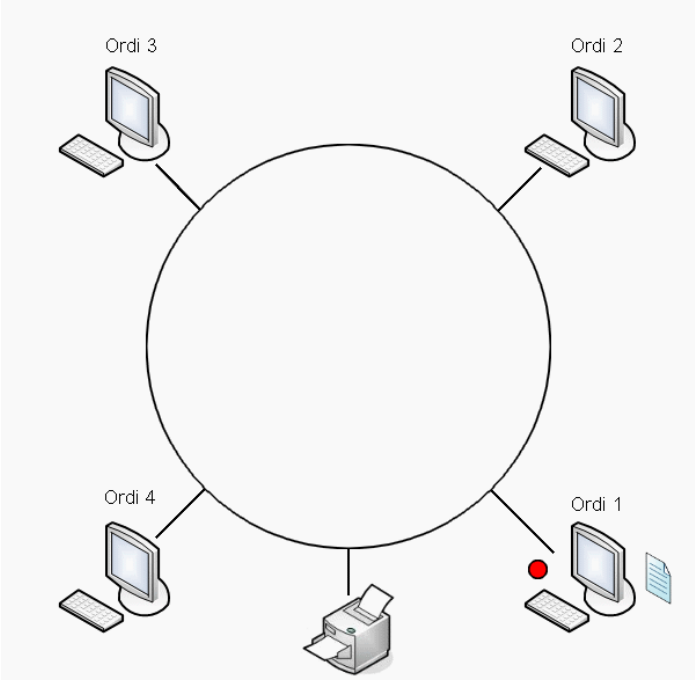


Fig I.5 Topologie en Anneau

IV.4.Topologie maillée

Le principe de la topologie maillée est de relier tous les ordinateurs entre eux (ou du moins, un maximum).

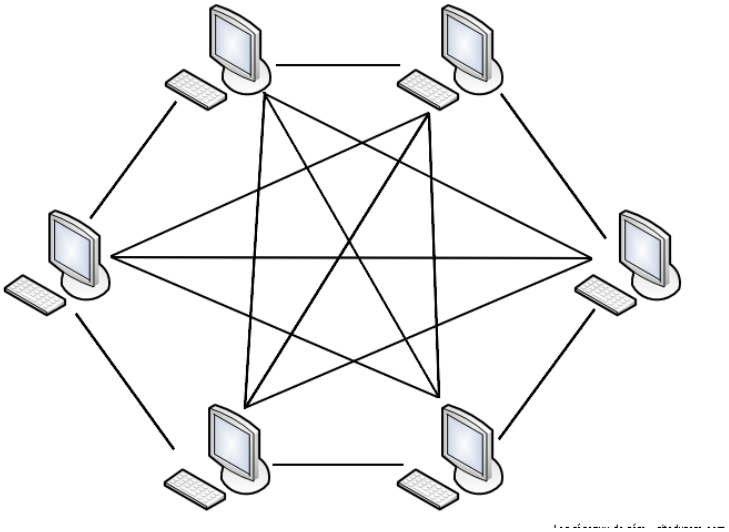


Fig I.6 Topologie maillée

V- Les équipements réseaux

C'est l'ensemble des équipements qui participent à la communication dans un réseau informatique.

V.1.le répéteur (repeater)

Un répéteur est un équipement réseau qui possède généralement deux ports, il reçoit un signal sur le port d'entrée, le régénère et le transmet vers le port de sortie. Cela permet aux signaux de voyager sur de plus longues distances à travers le média.

Fig I.9 Le répéteur

I.2-Le concentrateur (HUB)

Un concentrateur ou Hub est considéré comme un répéteur multiport.

Les données qui arrivent sur un port sont répétées sur tous les autres ports (tous les équipements raccordés au concentrateurs reçoivent toutes les données qui y transitent).

Fig I.10 Le concentrateur

3-Le Commutateur (switch)

Il réalise principalement deux fonctions : commutation des trames et la gestion des fonctions de commutation. La première fonction correspond à l'acheminement des trames qui arrivent sur un média d'entrée vers un autre média de sortie. La seconde fonction représente la constitution des tables de commutation qui aident à la commutation. En utilisant les informations contenues dans les trames qu'il reçoit, un commutateur constitue une table de commutation qui va lui servir à sélectionner le port auquel est connecté l'équipement de destination

4-Le Routeur (router)

Est un dispositif qui véhiculent les données sur le réseau vers leur destinataire en fonction des adresses logiques.

Il relie entre plusieurs réseaux.

Fig I.11 Routeur

VI. les types des réseaux

Selon la taille géographique , les réseaux sont divisés en :

VI.1 LAN : Réseau Local

LAN (**L**ocal **A**rea **N**etwork) (en français réseau local) est un réseau limité à un espace géographique comme un bâtiment. Par exemple, l'ensemble des ordinateurs dans une école forme un LAN.

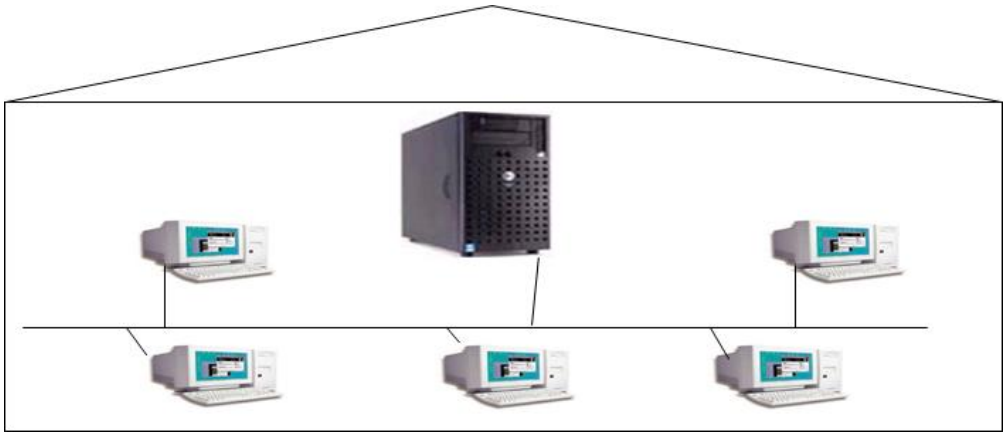


Fig I.12 Réseau Local (LAN)

-Constitué d'ordinateurs et de périphériques reliés entre eux et implantés dans une même entreprise, et à caractère privé.

- Il ne dépasse pas généralement la centaine de machines et ne dessert jamais au-delà du kilomètre.

VI.2 MAN : Réseau métropolitaine

(MEROPOLITAIN AREA NETWORK)

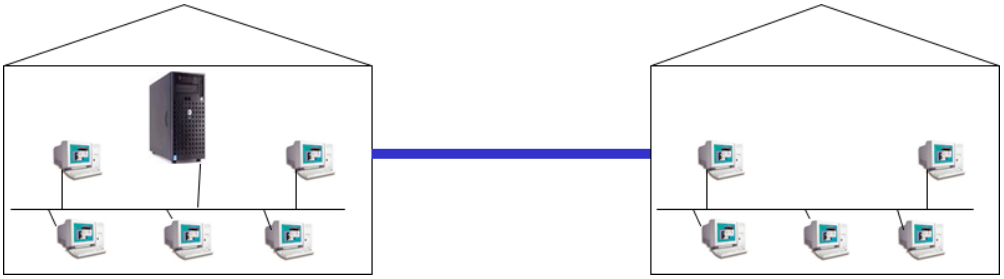


Fig I.13 Réseau MAN

Correspond à la réunion de plusieurs réseaux locaux (LAN) à l'intérieur d'un même périmètre d'une très grande Entreprise ou d'une ville par ex. pouvant relier des points distants de 10 à 25 Km.

VI.3 WAN : Réseau Étendu

Signifie WIDE AREA NETWORK , on peut le traduire par "réseau étendu". Un WAN est en fait une association de plusieurs LAN.

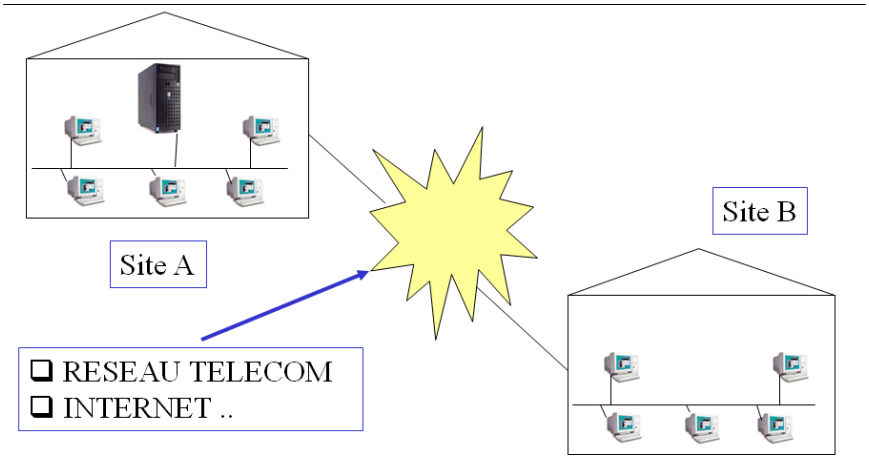


Fig I.14 Réseau WAN

Il s'agit cette fois d'un réseau multi-services couvrant un pays ou un groupe de pays, qui est en fait constitué d'un ensemble de réseaux locaux interconnectés.

exemple : Internet

VII Protocole

Un protocole est un ensemble de règles qui définissent comment se produit une communication dans un réseau

Un protocole de communication doit remplir quelques exigences rigoureuses. Un protocole est un ensemble de règles dictant comment doit s'effectuer la communication entre deux entités. Ceci dit, il faudrait que ledit protocole soit en mesure d'assurer des fonctions vitales au bon déroulement d'une communication. Il existe plusieurs « fonctions vitales » (comprendre exigences) qu'un protocole de communication doit être capable de remplir. Parmi ces fonctions :

- Un protocole définit comment s'effectue la communication. Or, qui dit communication dit échanges de données. Le protocole doit donc avoir des « fonctions » permettant de gérer le format de ces données.
- Durant la procédure de transmission des données, il faudrait bien gérer les adresses : qui est l'émetteur, qui est le destinataire ? dans l'entête des données « encapsulées », il

faudrait qu'un protocole soit en mesure de spécifier l'adresse de l'émetteur et du destinataire.

- Un protocole doit assurer des fonctions de correspondance entre les adresses logiques (IP) et les adresses physiques (MAC). Cette correspondance s'appelle **« address mapping »** en anglais.
- Un protocole assure le routage qui consiste à « diriger » les données entre deux réseaux d'un plan d'adressage différent.
- Un protocole devrait donc être en mesure de détecter et corriger les erreurs qui peuvent se produire dans la procédure de transmission des informations.

VIII Les modèles de références

VIII.1.Le modèle OSI

Le modèle OSI (*Open Systems Interconnection* : « interconnexion de systèmes ouverts ») est une façon standardisée de segmenter en plusieurs blocs le processus de communication entre deux entités. Chaque bloc résultant de cette segmentation est appelé couche. Une couche est un ensemble de services accomplissant un but précis.

L'avantage de cette segmentation en couches est que chaque couche communique avec la couche au-dessus et au-dessous d'elle (on parle également de couches adjacentes). La couche au-dessous pourvoit des services que la couche en cours utilise, et la couche en cours pourvoit des services dont la couche au-dessus d'elle aura besoin pour assurer son rôle.

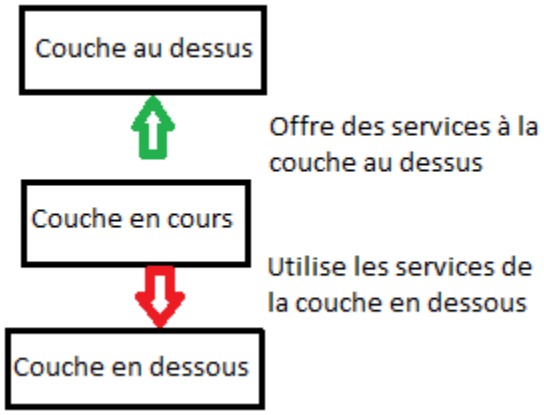


Fig I.15 Relations entre couches

Ainsi le modèle OSI permet de comprendre de façon détaillée comment s'effectue la communication entre un ordinateur A et un ordinateur B.

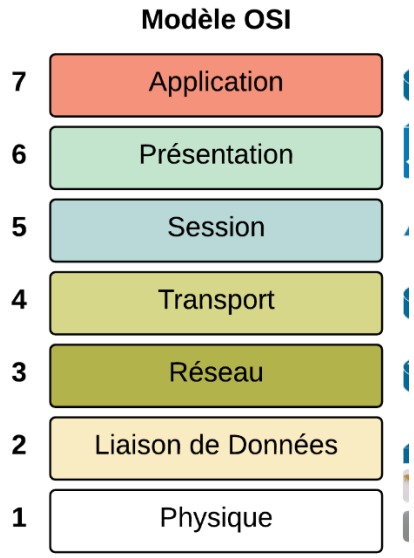


Fig I.16 Le modèle OSI

VIII.1.1 Les couches du modèle OSI

1. la couche physique

Permet de convertir les bits en signaux pour les envoyer sur un média physique. Elle détermine le voltage, la périodicité, le débit...etc des données physiques grâce aux différentes opérations telles que : codage, modulation...etc.

2. la couche Liaison des données

Prépare les paquets de couche réseau pour être transmis et contrôle l'accès aux supports physiques. Elle fragmente les données en plusieurs trames, qui sont envoyées une par une dans un réseau local. Elle assure la livraison des trames dans un réseau local.

3.la couche réseau

Organise les données de communication de sorte qu'elles puissent voyager à travers les inter-réseaux de l'hôte source vers un hôte de destination. Elle se charge du routage des données du point A au point B et de l'adressage

4.la couche transport

A pour fonction de diviser et de gérer les communications entre les processus s'exécutant sur les deux systèmes d'extrémité. Elle divise les données en plusieurs segments (ou séquences) et les réunit dans la couche transport de l'hôte récepteur. Cette couche permet de choisir, en fonction des contraintes de communication, la meilleure façon d'envoyer une information. Elle est caractérisée par les deux protocoles Tcp et Udp.

5.la couche session

La couche session du modèle OSI vous permet principalement d'ouvrir une session, de la gérer et de la clore. La demande d'ouverture d'une session peut échouer. Si la session est terminée, la « reconnexion » s'effectuera dans cette couche.

6.la couche présentation

Garantit que les communications en transit présentent une forme adaptée au destinataire. Elle s'occupe de la sémantique, de la syntaxe, du cryptage/décryptage, de tout aspect « visuel » de l'information

7.la couche application

Fournit une interface à l'utilisateur, pour lui donner accès aux différents services, qui lui permettent notamment de transférer des fichiers, de rédiger un mail, d'établir une session à distance, de visualiser une page web.

VIII.2.Le modèle Tcp/ip

Le modèle TCP/IP fut créé dans les années 1970 par le département de la Défense des États-Unis d'Amérique, plus précisément par l'agence DARPA (*Defense Advanced Research Projects Agency*).

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

2.1 – La couche hôte réseau

Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

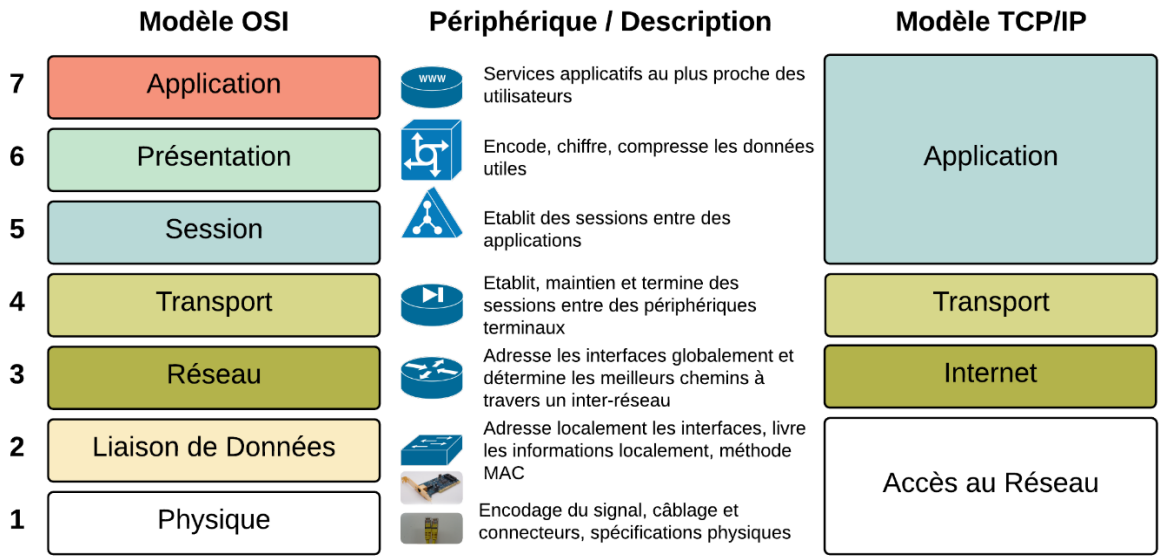


Fig I.17 Modèle OSI vs modèle TCP/IP

2.2 – La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

Remarquons que le nom de la couche (« internet ») est écrit avec un i minuscule, pour la simple et bonne raison que le mot internet est pris ici au sens large (littéralement, « interconnexion de réseaux »), même si l'Internet (avec un grand I) utilise cette couche.

2.3 – La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là une avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne

gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

2.4 – La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

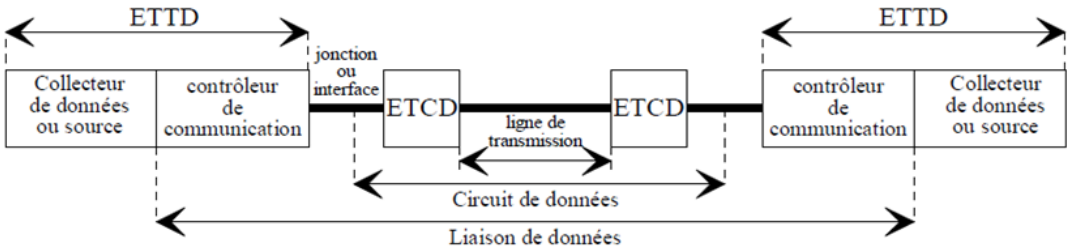
Couche 2 Physique

I. Fonctions de la couche physique

Elle assure la transmission physique de trains de bits sur les moyens physiques d'interconnexion entre deux entités de liaison adjacentes (support de transmission).

Elle détermine la façon selon laquelle les bits sont transportés sur le support physique. Elle permet d'introduire les bits 0 et 1 sur le support sous une forme spécifique, reconnaissable par le récepteur

II.Les éléments d'une transmission



FigII.1 Les éléments d'une transmission

ETTD : Equipement Terminal de Traitement de Données

représente les calculateurs d'extrémité, Il réalise la fonction de contrôle du dialogue . (un pc)

ETCD : Equipement Terminal de Circuit de Données

sont les équipements qui réalisent l'adaptation entre les calculateurs d'extrémité et le support de transmission.(ex: un modem)

III. Le Débit

une liaison de données est caractérisée par son Débit (D) qui représente le nombre de bits transmis par unité de temps (bits/s) et par l'organisation des échanges.

$$D=Q/t$$

D: (débits bit/s)

Q: quantité de données à transmettre (Bits)

t: Durée de transmission

IV.Modes de transmission

La liaison peut être exploitée en :

IV.1.Simplex (simplex): l'échange de données se fait dans un seul sens

IV.2.Semi-duplex:(half-duplex) : L'échange se fait alternativement dans les deux sens, c'est-à-dire que les deux stations ne doivent pas transmettre simultanément.

IV.3.Semi-duplex(full-duplex): L'échange se fait alternativement dans les deux sens, c'est-à-dire que les deux stations ne doivent pas transmettre simultanément

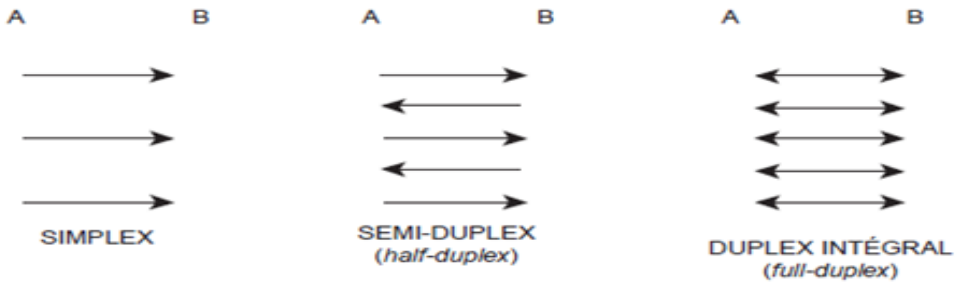


Fig II.2 Modes de transmission

V. les transmissions parallèle /série

V.1 la transmission parallèle

Caractérisée par un transfert simultané de tous les bits d'un mot , elle nécessite donc autant de fils qu'il y a de bits à transmettre

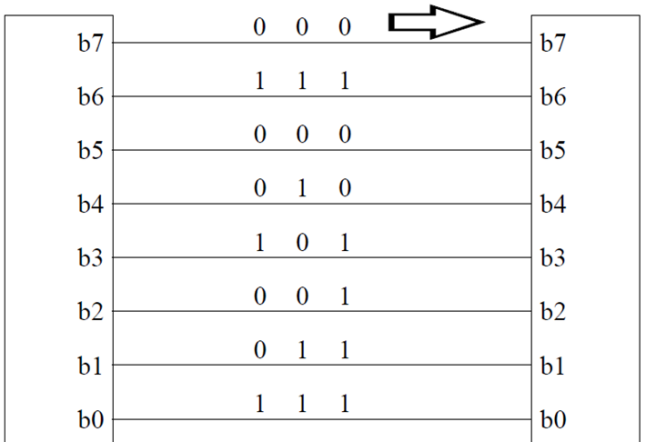


Fig II.3 transmission parallèle

V.2 la transmission série

Dans la transmission série , tout les bits d'un mot sont transmis bit par bits (successivement) sur la même ligne.

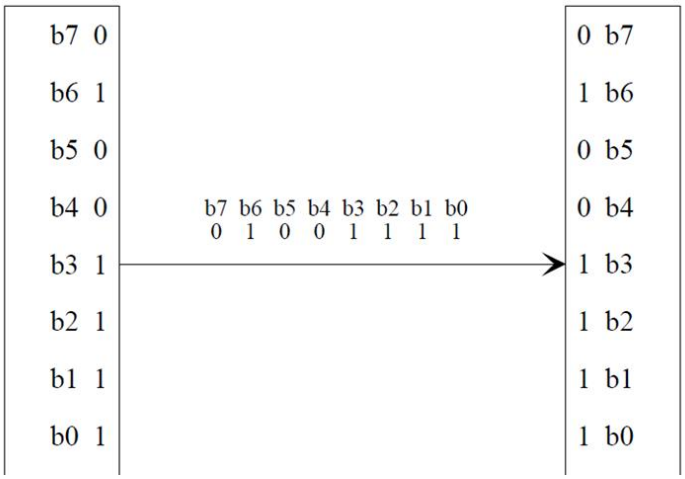


Fig II.4 transmission Série

VI. Transmission synchrone /asynchrone

VI.1 Transmission synchrone

Les bits d'un même message sont régulièrement espacés , les horloges émetteur et récepteur sont en phase.

VI.2 transmission Asynchrone

L'intervalle qui sépare la transmission de deux caractères peut être variable. Les caractères sont délimités par un bit start et bits stops .

VII. Les supports de transmission

Les supports de transmission (médias) sont nombreux, Parmi ceux-ci, trois familles sont à distinguer : médias en cuivre , média optique et media sans fils.

VII.1 médias en cuivre

VII.1.1 paires torsadées

Une paire torsadée non blindée (UTP, Unshielded Twisted Pair) se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal. son connecteur est de type : RJ45

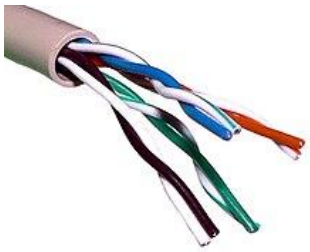


Fig II.5 Câble UTP

Fig II.6 Connecteur Rj45

VII.1.2 Cable coaxial

Le câble coaxial est composé d'un fil de cuivre entouré d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure. il utilise comme connecteur le BNC

Fig II.7 Cable coaxial

Fig II.8 Connecteur BNC

Il est utilisé généralement dans :

- Les réseaux téléphoniques
- Dans les réseaux téléphoniques numériques : Un coaxial a un débit de données de 600 Mbps.
- Dans les RÉSEAUX locaux Ethernet traditionnels
- Dans la transmission des signaux de télévision par câble et Internet.

VII.2 média optique

La fibre optique est un support de transmission optique , il transmet des données dans un sens seulement. Aussi pour que deux entités communiquent en full duplex, un câble optique doit contenir deux fibres optiques : l'une pour transmission et l'autre pour réception. Un câble peut contenir plusieurs fibres.

il utilise la lumière pour la transmission des données , La lumière est guidée dans le centre de la fibre(coeur) qui est constitué en majorité de silicium dioxyde (silice), enrichi avec d'autres éléments. Il est entouré par la gaine optique.

Les matières de compositions des couches de la fibre permettent à la lumière de se réfléchir.

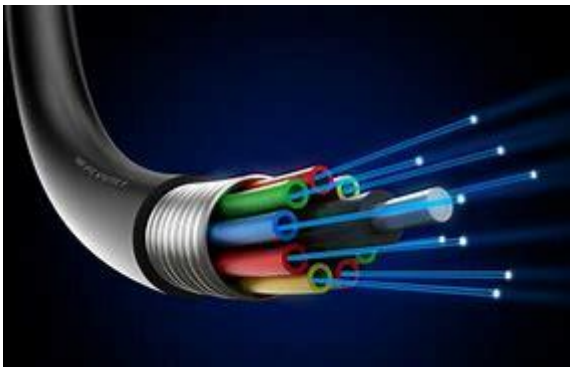


Fig II.9 fibre optique

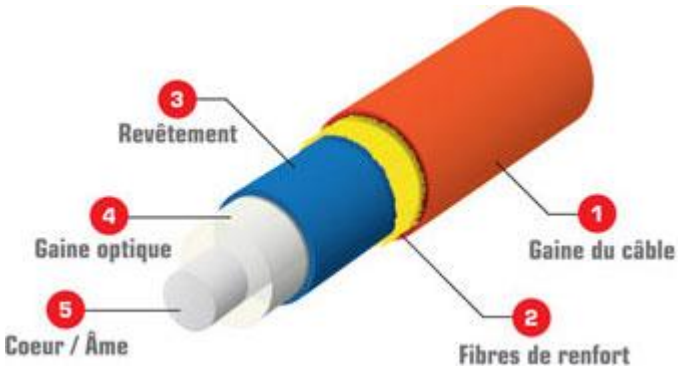


Fig II.10 Structure d'une fibre optique

Le rayon lumineux entre dans la fibre et il subit de multiples réflexions totales internes, il se propage alors jusqu'à l'autre extrémité de la fibre optique sans perte. Il utulise des connectes SC et ST (selon le type du connecteur)

Fig II.11 Connecteurs fibre optique

VII.3 Média sans fils (wireless network)

Un réseau sans fils estun réseau dans lequel au moins deux hôtes peuvent communiquer sans liaison filaire. Il existe plusieurs types des réseaux sans fils :

VII.3.1 Bluetooth

c'est un réseau d'une portée de dizaines de mètres et un débit théorique de 1 Mbps .il utilise une liaison hertzienne . Au sein d'un réseau bluetooth, un appareil sert de maître et jusque 7 périphériques esclaves qui se partagent la bande passante.

Fig II.12 Technologie bluetooth

VII.3.2-Wifi (Wireless Fidelity)

Le **wifi** est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau local . Il couvre des surfaces locales(locaux, aéroports , cyber café...)et offres des services de partage des différentes ressources comme l'internet grâce aux ondes radio.

Un réseau Wi-Fi utilise des ondes radio pour transmettre des données à travers un réseau.

Pour que votre connexion Wi-Fi fonctionne, votre ordinateur doit être équipé **d'un adaptateur réseau sans fil** qui convertit les informations envoyées en un signal radio. Ce dernier est ensuite communiqué, via une antenne, à un point d'accès.

VIII. Les équipement de la couche physique

VIII.1 Répéteur (repeater)

Le répéteur est un composant actif. Son rôle est de régénérer et de resynchroniser le signal afin de pouvoir étendre la portée des câbles.

Fig II.13 Répeteur

VIII.2 Concentrateur (hub)

Le concentrateur, ou répéteur multi ports, reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité. En effet, il dispose de plusieurs ports ce qui permet d'interconnecter plusieurs équipements réseau. Chaque signal arrivant sur un port est régénéré, resynchronisé et ré émis au travers de tous les autres ports.

Fig II.14 concentrateur (hub)

VIII.3 le modem

Abréviation de **modulateur / démodulateur**, un **modem** est un périphériquequi permet à un ordinateur d'envoyer et de recevoir des informations sur des lignes téléphoniques Lors de l'envoi d'un signal, l'appareil convertit (« module ») les données numériques en un signal audio analogique et les transmet sur une ligne téléphonique. De même, lorsqu'un signal analogique est reçu, le modem le reconvertit (« le démodule ») en signal numérique.

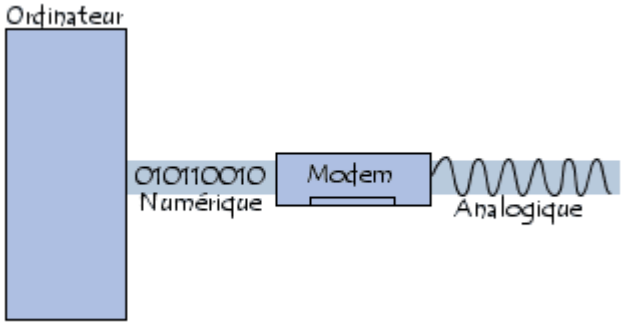


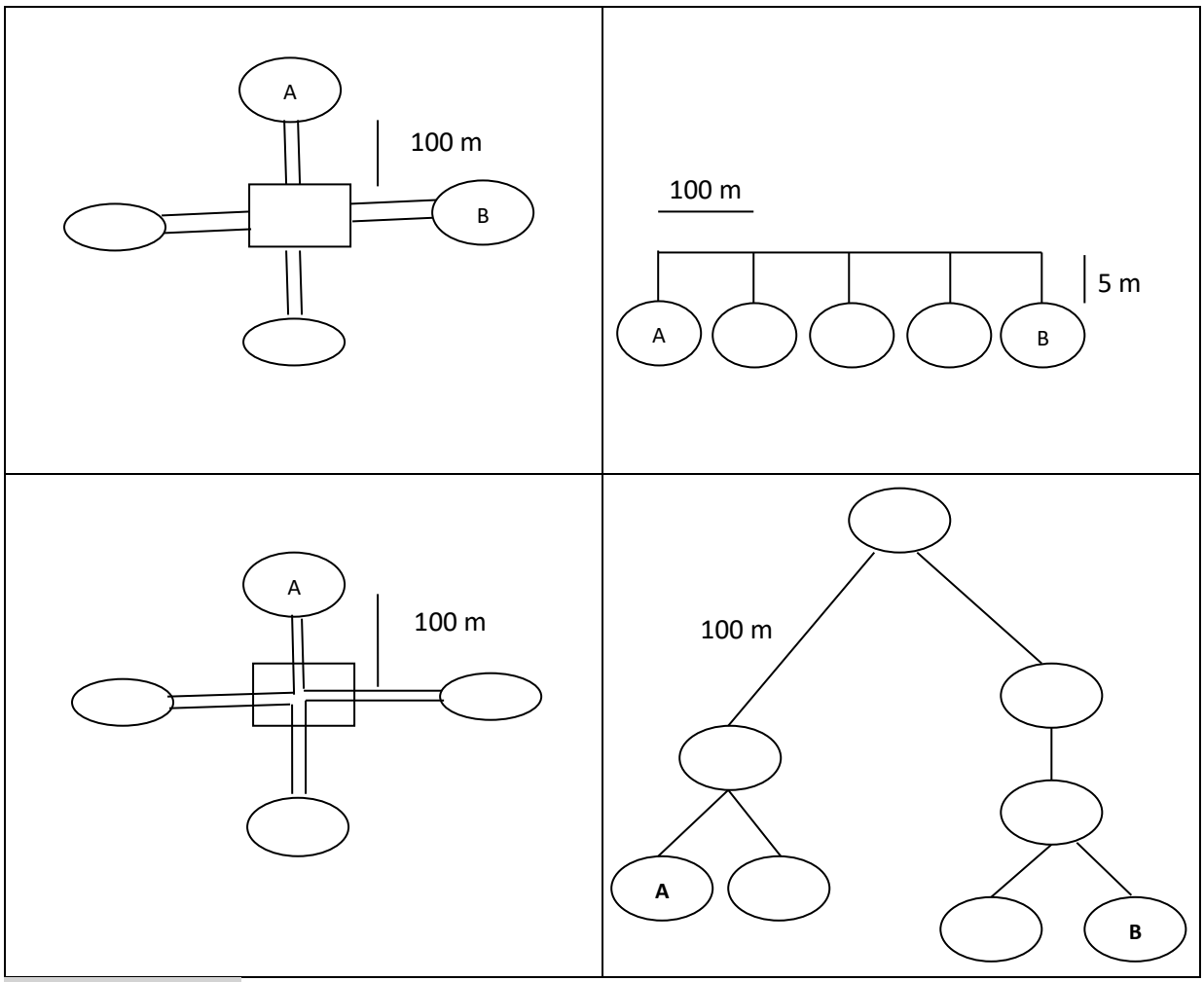
Fig II.15 fonctionnement d'un modem

Fiche Td n° :01

Exercice n° :01

1- Préciser la topologie physique pour chacun des réseaux représentés sur la figure1

2. calculer La distance entre la station A et la station B.



Exercice n° :02 :

1-Citer quelques types d'informations transmises par les réseaux informatiques.

2-Quelles sont les différentes formes employées pour la transmission de l'information?

3-Quelle est la différence entre le la bande passante et le débit.

4-Sur un réseau dont le débit théorique est de 9600 bits/s, combien de temps prend le transfert de 2 pages de texte. (une page contient une moyenne de 1000 caractères)

Exercice n° :03 :

Un coursier doit transporter un paquet de dix disquettes d'une société A à une société B distante de 20 kms. Chaque disquette contient 1,4 Mo. L'homme se déplace en scooter à travers la ville avec une vitesse moyenne estimée à 30 km/h.

1. Sur cette distance, utiliser un coursier n'est-il pas une solution obsolète par rapport à l'utilisation d'une ligne téléphonique dont la vitesse de transmission est de 56Kbit/s ?
2. Même question en remplaçant les dix disquettes par un CD-ROM dont la capacité est de 700Mo

Exercice n° :04

Quelle est le délai de retour d'un message de Q Kbits envoyé sur un anneau comprenant N stations?

Chaque station introduit un délai de traversée de t seconds. Les stations sont reliées, deux à deux, par un câble de L mètres. La vitesse de propagation de signaux est V km/s. Le débit du réseau est de d Mb/s.

Remarque : Délai = Temps de transmission + temps de propagation + retards.

Exercice n° :05

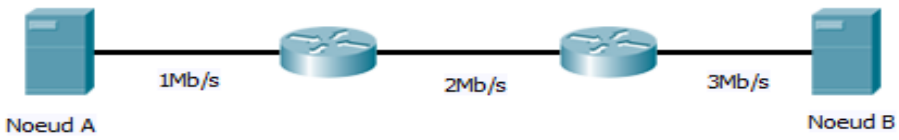
On considère un réseau dont le débit est de 10 Mbits/s. Les messages envoyés sur ce réseau ont une taille maximale de 1000 bits dont un champ de contrôle de 16 bits.

1. Quel est le nombre de messages nécessaires pour envoyer un fichier F de 4 Mbits d'une station à une autre ?

Exercice n° :06

Soit le réseau décrit par la figure suivante. On considère que le réseau ne présente pas d'encombrement et que le nœud A veut envoyer à B un message de longueur de 10 Mbits.

Combien de temps faut-il au message pour rejoindre B si A ne segmente pas le message ?



3 Couche liaison De données

La couche liaison des données fournit les moyens nécessaires à l'établissement, le maintien et la libération d'une liaison de données entre émetteurs et récepteurs. Elle fournit un mécanisme de détection des erreurs de transmission. Elle assure ces deux services de base :

-Elle accepte les paquets de couche 3 et les encapsule dans des unités de données appelées des trames.

-Elle contrôle l'accès au support et détecte les erreurs.

I. Détection des erreurs

La couche liaison détecte les erreurs de transmission dans un boc de bits envoyé sur un support physique, les techniques utilisé a ce niveau est l'ajout des informations aux blocs de bits à envoyés pour que le récepteur se sert à cette information pour détecter si une erreur s'est produite.

I.1 La parité

le principe est d'ajouter à chaque bloc de k bits (k=7) émis un bit de parité en assurant que parmi les les k+1 bits envoyé le nombre de bit (=1) soit toujours pair (pour la parité paire) ou impair (pour la parité impaire).

Exemple :

Soit le bloc à envoyer : 1011011

pour la parité paire: on ajoute donc **1** pour assurer que le nombre des 1 est pair le bloc envoyé devient :10110111

pour la parité impaire: on ajoute donc **0** pour assurer que le nombre des 1 est impair le bloc envoyé devient :1011011**0**

A la réception , le récepteur calcule le nombre de bit à 1 et assure le critère (selon le type de parité paire ou impaire).

Cette technique sert à détecter la présence d'une erreur et non à la localisation.

I.2. Les codes à redondance cyclique (CRC)

Cette technique consiste à ajouter un ensemble de bits qui sont en relation avec ls bits composants le bloc à envoyer.

Le principe :

1. le polynôme CRC

C'est un polynôme défini par :

$\mathbf{P(x) = a_{(r-1)}x^{(r-1)} + a_{(r-2)}x^{(r-2)} +...+ a_1x^1 + a_0x^0}$

Ce polynôme est appelé c(X) est représenté par une série de bits : a(r-1),a(r-2),.....a0

Exemple : :

le polynôme :

$\mathbf{C(X) = X^4 + X^2 + 1.}$

est représenté par : 10101

$\mathbf{1.X^4 +0.X^3 +1.X^2 +0.X^1 +1.}$

2. Fonctionnement

Si le polynôme est d'ordre n , on ajoute n (0) à la série de bits à transmettre.

$C(X) = X^4 + X^2 + 1.$

c(x) est d'ordre 4 donc on ajoute 4 bit au bloc à transmettre

Exemple:

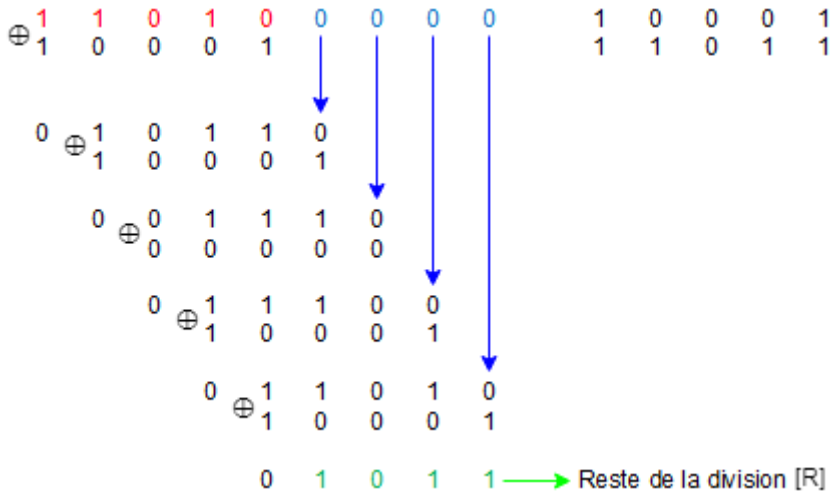
Soit le message à transmettre : M=11010 et le polynôme c(x)=$\mathbf{X^4 + 1}$

c(x) est représenté par : 10001

c(x) est d'ordre 4 alors on ajoute 4 bits au message M

M devient : 11010**0000**

Maintenant on réalise le xor binaire successif qui est équivalent ici à la division euclidienne de M sur C



Le reste est **1011** c'est le crc qui sera ajouter à m

Le message à transmettre est donc : 11010**1011**

A la réception, une division du message reçu sur le même polynôme, si le reste est nul alors le mesasge est bien reçu sinon, on déclare qu'il y a une erreur pendant la transmission.

II. La carte réseau

Les cartes réseau connectent un périphérique au réseau. Les cartes réseau Ethernet sont utilisées dans les connexions filaires, tandis que les cartes réseau WLAN (réseau local sans fil) sont utilisées dans les connexions sans fil. Un périphérique utilisateur peut comporter l'un de ces deux types de carte réseau ou les deux. Une imprimante réseau, par exemple, peut ne comporter qu'une carte réseau Ethernet et doit, dans ce cas, être connectée au réseau à l'aide d'un câble Ethernet. D'autres périphériques, tels que les tablettes et les smartphones peuvent n'être équipés que d'une carte réseau WLAN et doivent donc utiliser une connexion sans fil.

Fig III.1 Carte réseau

Les sous couches :

la couche liaison des données est divisée en 2 sous couches : LLC et Mac

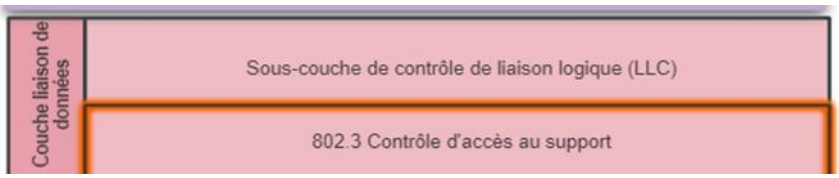


Fig III.2 Sous couche LLc

La sous-couche LLC (*Logical Link Control*) permet le contrôle de la liaison logique : elle fiabilise le protocole MAC par un contrôle d'erreur et un contrôle de flux (asservissement du débit de l'émetteur vers le récepteur).

la sous couche Mac

Elle assure trois fonctions de base :

· **Délimitation des trames** : le processus de tramage fournit des délimiteurs importants utilisés pour identifier un groupe de bits qui composent une trame. Ce processus permet la synchronisation entre les noeuds de transmission et ceux de réception.

· **Adressage** : l'encapsulation fournit également un adressage pour la couche liaison de données. Chaque en-tête Ethernet ajouté à la trame contient l'adresse physique (MAC) qui permet de remettre celle-ci au nœud de destination.

· **Détection d'erreur** : chaque trame Ethernet contient une fin avec un contrôle de redondance cyclique (CRC, Cyclic Redundancy Check) du contenu des trames. Après

réception d'une trame, le noeud récepteur crée un CRC pour le comparer à celui de la trame. Si ces deux calculs de CRC correspondent, cela signifie probablement que la trame a été reçue sans erreur.

Adresse MAC

Il permet d'identifier les nœuds source et de destination sur un réseau Ethernet. Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux (4 bits par chiffre hexadécimal).

L'adresse MAC est souvent dite rémanente, car elle était au départ stockée dans la mémoire morte (ROM) de la carte réseau.

III.La technologie Ethernet

Ethernet est considéré comme la technologie de réseau local prédominante dans le monde. Elle fonctionne au niveau de la couche liaison de données et de la couche physique.

Lorsque des messages sont transmis entre hôtes sur un réseau Ethernet, ces derniers formatent les messages dans la structure de la trame spécifiée par les normes.

Son principe est basé sur la diffusion des messages sur un bus logique qui peut être un bus ou une étoile physique. C'est à dire une station qui parle, envoie une trame contenant le message, sa propre adresse et l'adresse du destinataire sur le bus. Toutes les stations voient passer cette trame mais seule celle qui se reconnaît comme étant le destinataire la lit.

III.1 Trame ethernet

Les normes Ethernet IEEE 802.3 définisse une taille de trame minimale de 64 octets et maximale de 1 518 octets. Toute trame inférieure à cette valeur est est automatiquement rejetée par les périphériques récepteurs.

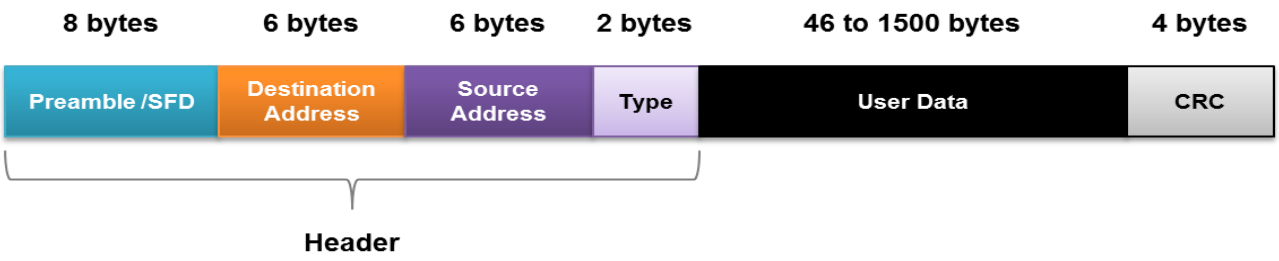


Fig III.3 Format de la trame Ethernet

Description de la trame :

Préambule et Indicateurs de début et de fin de trame :

Préambule (7 octets) et Délimiteur de début de trame (1 octet) sont utilisés par la sous-couche MAC pour identifier les limites de début et de fin de la trame. Ils servent à synchroniser les périphériques émetteurs et destinataires. Les huit premiers octets de la trame préparent les noeuds de réception à recevoir. Les quelques premiers octets indiquent essentiellement aux récepteurs de se préparer à recevoir une nouvelle trame

Adresse mac de destination :

De taille 6 octets, sert à identifier les nœuds de destination. Cette adresse est utilisée par la couche 2 pour aider les périphériques à déterminer si une trame leur est adressée. L'adresse de la trame est comparée à l'adresse MAC du périphérique. Si les deux correspondent, le périphérique accepte la trame.

Adresse mac source : De taille 6 octets, elle identifie les nœuds de destination, la carte réseau ou l'interface d'origine de la trame.

Type/longueur : Définit la longueur exacte du champ de données de la trame. Cette longueur est ensuite utilisée dans la séquence de contrôle de trame, pour garantir la réception du message. Sinon, le rôle de ce champ est d'indiquer le protocole de couche supérieure présent.

Données : De 46 à 1 500 octets contient les données encapsulées d'une couche supérieure. La longueur minimale de la trame est fixée à 64 octets. Si un paquet de petite taille est encapsulé, d'autres bits sont utilisés pour augmenter la trame et la ramener à sa taille minimale. Ces bits sont appelés champs de remplissage.

FCS : Ou (Séquence de contrôle de trame) de taille (4 octets) permet de détecter les erreurs d'une trame. Il fait appel à un contrôle par redondance cyclique (CRC). Le périphérique d'envoi inclut les résultats d'un CRC dans le champ FCS de la trame.

IV. Contrôle d'Accès multiple

Une topologie d'accès multiple permet à des nœuds de communiquer en utilisant le même support partagé. Les données uniquement issues d'un seul noeud peuvent être placées sur le support à tout moment. Chaque nœud voit toutes les trames qui se trouvent sur le support, mais seul le nœud auquel la trame est destinée en traite le contenu.

Les méthodes d'accès fournissent les procédures permettant de gérer l'accès au réseau de sorte que toutes les stations de travail puissent accéder au réseau.

note : On désigne par le mot **collision** , la superposition de deux trames sur le média lorsque deux stations émettent simultanément.

IV.1 CSMA/CD (Carrier sense multiple access with collision detection)

Le périphérique final établit si le support comporte un signal de données. Si aucun signal de données n'est détecté et donc que le support est libre, le périphérique transmet ses données. Si des signaux sont alors détectés indiquant qu'un autre périphérique était au même moment en train de transmettre des données, tous les périphériques arrêtent de transmettre leurs données et réessayent ultérieurement.

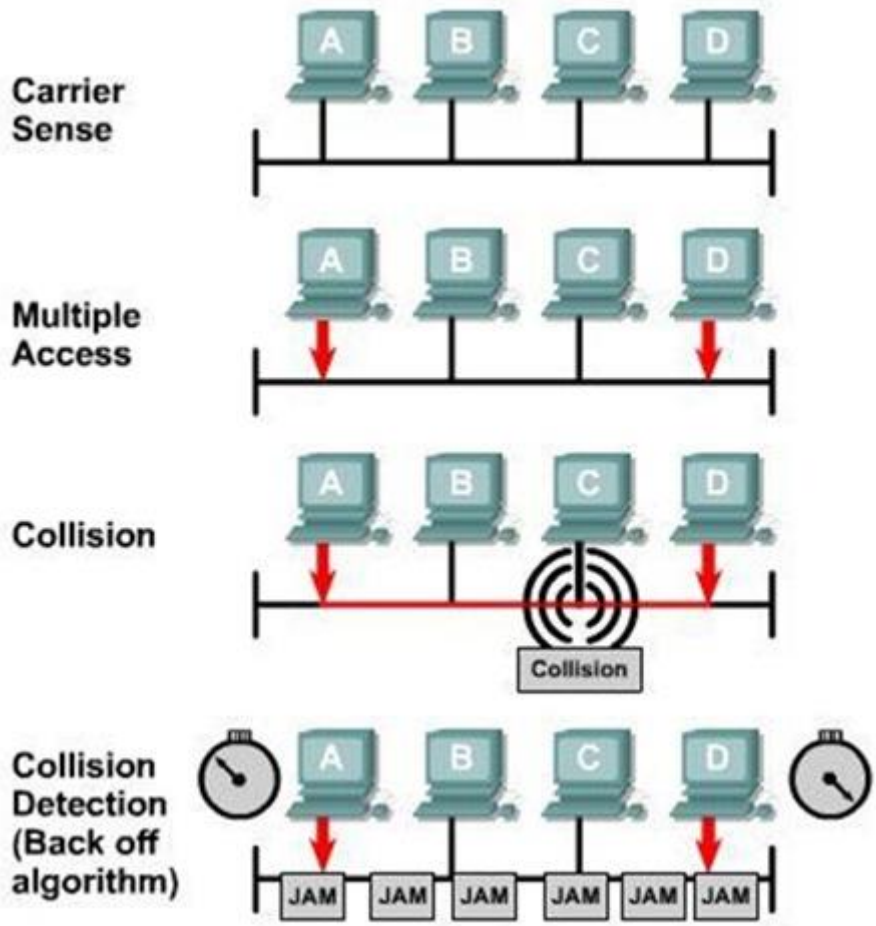


Fig III.4 CSMA/CD[1]

IV.2 TOKEN RING (passage de jeton)

Promu par IBM pour se démarquer d'Ethernet,

Un jeton tourne, va de station en station. Lorsque l'on veut parler on attend que le jeton passe. Si il est libre on le marque occupé et on parle. Lorsque l'on reçoit un message on marque la trame pour signaler qu'on l'a lue et on la laisse continuer. L'émetteur reçoit donc la trame qu'il a émise en sachant si le destinataire l'a lue. Il libère le jeton et le passe à son voisin. Comme il n'y a qu'un jeton en circulation sur l'anneau une seule station peut transmettre à un instant donné. Ceci évite l'émission simultanée de plusieurs

[1] CSMA/CD - DatakomWiki - NTNU Wiki

Fiche Td n° :02

Exercice n° :01

On utilisera le polynôme générateur $\mathbf{x^4 + x^2 + x.}$

1. On souhaite transmettre le message suivant :1111011101, quel sera le CRC à ajouter ?

2. Même question avec le mot 1100010101.

3. Je viens de recevoir les messages suivants : 1111000101010, 11000101010110, sont-ils corrects ?

Exercice n° :02

Le format de l'information qui caractérise une trame Ethernet (annexe1)

1) Quelle est la longueur d'une trame minimum?

2) Quelle est la longueur minimum des données transportables?

3) Pourquoi la couche physique ajoute un préambule?

Exercice n° 03 (Analyse des trames)

Les suites hexadécimales ci-dessus correspondent à 5 trames ETHERNET capturées par un logiciel d'analyse de trames ; basant sur les formats des trames en annexe (*Annexe 1*), Analyser manuellement ces trames en commençant par identifier/extraire ses différents champs (Adresses, EtherType, Données) et les présenter sous une forme adaptée, dépendant de la nature du champ. Le champ EtherType doit permettre d'identifier le protocole destinataire des données de la trame.

Trame 1

```
00 0a b7 a3 4a 00 00 01 02 6f 5e 9b 08 00 45 00

00 28 00 00 40 00 40 01 82 ae 84 e3 3d 17 c2 c7

49 0a 08 00 75 da 9c 7a 00 00 d4 45 a6 3a 62 2a

09 00 ff ff ff ff 00 00 00 00 00 00
```

Trame 2

```
00 01 02 6f 5e 9b 00 0a b7 a3 4a 00 08 00 45 00
00 28 d0 92 00 00 3a 01 5a db c2 c7 49 0a 84 e3
3d 17 00 00 7d da 9c 7a 00 00 d4 45 a6 3a 62 2a
09 00 ff ff ff ff 00 00 00 00 00 00
```

Trame 3

```
ffff ffff ffff 09ab 14d8 0548 0806 0001

0800 0604 0001 09ab 14d8 0548 7d05 300a

0000 0000 0000 7d12 6e03
```

Trame 4

```
00 01 02 af f5 e2 00 60 08 61 04 7b 08 00

45 00 00 3d dc 56 00 00 80 11 aa 42 0a 0a

9f 02 0a 0a 01 01 0a 79 00 35 00 29 a1 e4

00 02 01 00 00 01 00 00 00 00 00 00 02 77

70 08 6e 65 74 73 63 61 70 65 03 63 6f 6d

00 00 01 00 01
```

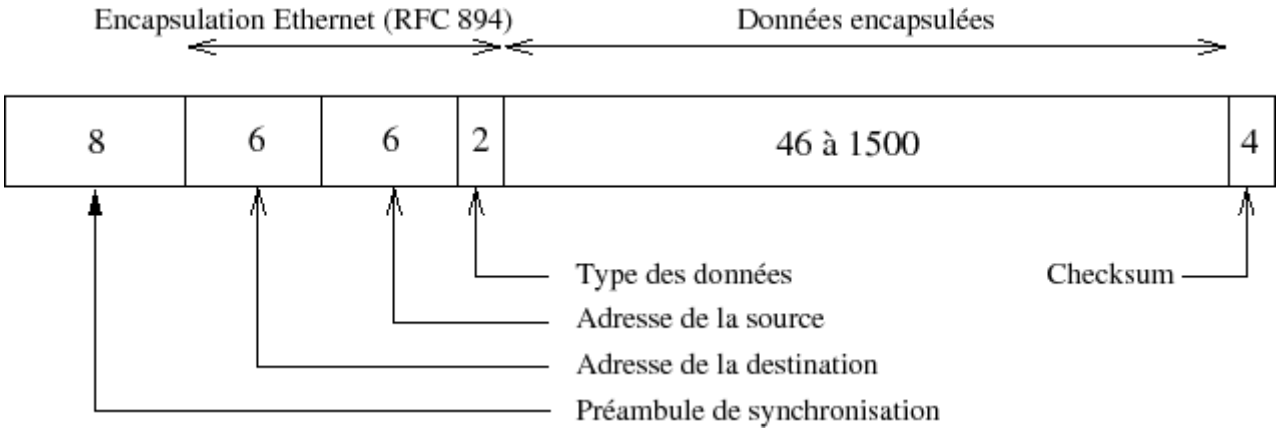
Trame 5

```
00 60 08 61 04 7b 00 01 02 af f5 e2 08 06

00 01 08 00 06 04 00 02 00 01 02 af f5 e2

0a 0a 01 01 00 60 08 61 04 7b 0a 0a 9f 02

00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00
```

Note : les trames sont données sans préambule, ni CRC

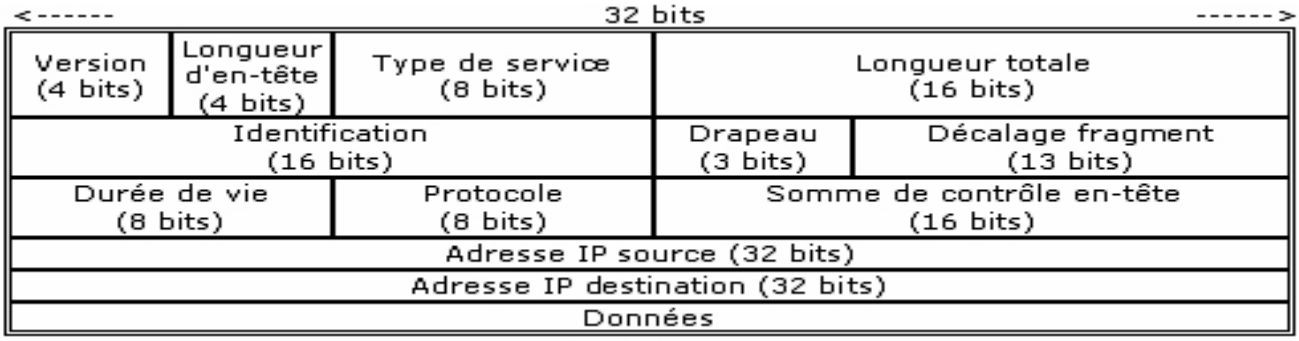
Annexe 1

Trame Ethernet :



Type : (0800 Ip, 0806 ARP , 00c0 PPP)

Le paquet IP



Version : numéro de version de protocole IP, actuellement version 4,
Lg entete : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
Drapeaux : composé de trois bits
–Le bit **D** « *do not fragment* »(010) signifie que le réseau doit traiter le paquet dans son intégrité ou pas du tout.
–Le bit **M** « *more fragments* » (001) signifie d'autres fragments à suivre et permet au destinataire final de reconstituer le datagramme initial en identifiant les différents fragments (milieu ou fin du datagramme initial). Si **M**=0, alors c'est le dernier fragment.
Protocole : 6 : TCP --- 17 : UDP --- 1 : ICMP

Couche 4 Réseaux

La couche réseau ou couche 3 du modèle OSI, qui correspond à la couche internet du modèle TCP-IP, est responsable du routage. Oui, en fait c'est la fonction principale de cette couche. Une fois que la couche transport a assuré son rôle, les données sont envoyées à la couche réseau. Cette dernière se chargera d'ajouter toutes informations en rapport avec le routage, soit l'adresse IP du destinataire. C'est la seule couche du modèle OSI qui utilise la connexion logique. En fait, bien que cette couche ait pour rôle de déterminer le chemin physique à emprunter en se basant sur l'adresse IP du destinataire, les conditions du réseau et plusieurs autres facteurs, elle ne peut pas établir une connexion physique. D'où son rôle se limite à la connexion logique.

I. Notions fondamentales

Afin que La couche réseau assure ces tâches, elle utilise un ensemble de processus:

I.1 L'Adressage

Chaque périphérique doit être configuré avec une adresse IP unique pour être identifié sur le réseau.

I.2 Encapsulation

La couche réseau reçoit une unité de données de protocole (PDU) de la couche transport. Dans le cadre d'un processus appelé l'encapsulation, La couche réseau ajoute ses informations (adresse IP source et de destination) à l'unité de données reçu de la couche transport (segment). L'unité de donnée de la couche réseau est appelée paquet.

I.3 Routage

Le processus de sélection du meilleur chemin pour diriger les paquets vers la destination est la tâche principale du routeur et est appelée routage.

I.4 Désencapsulation

Est le processus de suppression des en-têtes des couches inférieures (adresse Ip source et destination) qui s'effectue lorsque le paquet arrive au niveau de la couche réseau de la destination.

II L'adressage IP

II.1 Définition

Le contrôler de la route empruntée par un paquet nécessite une identification de tous les hôtes connectés sur le réseau.

De la même façon que l'on repère l'adresse postale d'un bâtiment à partir de la ville, la rue et un numéro dans cette rue, on identifie un hôte réseau par une adresse qui englobe les mêmes informations.

Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle : l'adressage IP .

Chaque hôte TCP/IP est identifié par une adresse IP logique.

Comme l'adresse d'une rue doit identifier une résidence unique, une adresse IP doit être unique.

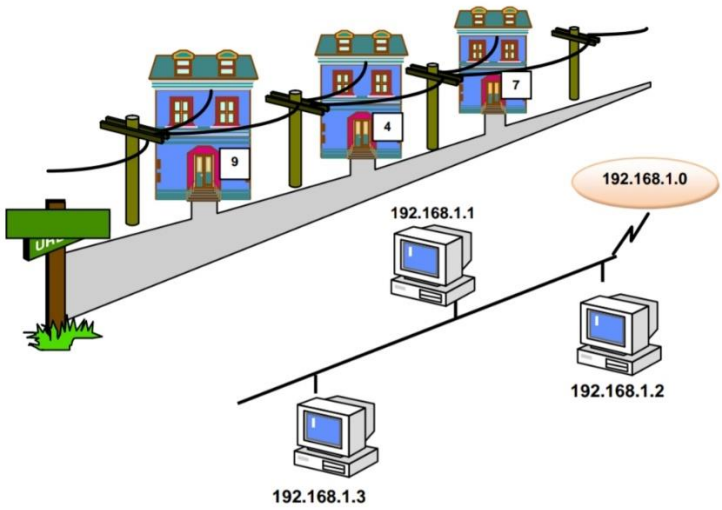


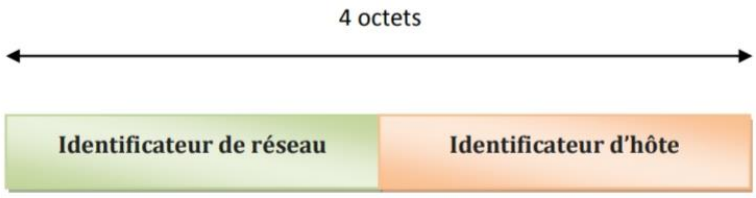
Fig IV.1 Besoin d'adressage

II.2. Format Des Adresses

Les adresses IP sont composées de 4 octets soit 32 bits

Par convention, on note ces adresses sous forme de 4 nombres décimaux (0-255) séparés par des points.

Les 4 octets de la définition des adresses IP rassemblent une partie réseau et une partie hôte.



- La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte est unique et désigne une seule interface physique .

Fig IV.2 Format d'adresse IP

II.3. Classe D’adresses

Plusieurs groupes d’adresses ou Classes ont été définis dans le but d’optimiser le routage des paquets.

Ces classes correspondent à des regroupements en réseaux de même taille.

Les réseaux de la même classe ont le même nombre d’hôtes maximum.

Classe A:

Le premier octet a une valeur strictement inférieure à 128 (de 0 à 126

Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l’adresse de l’hôte.

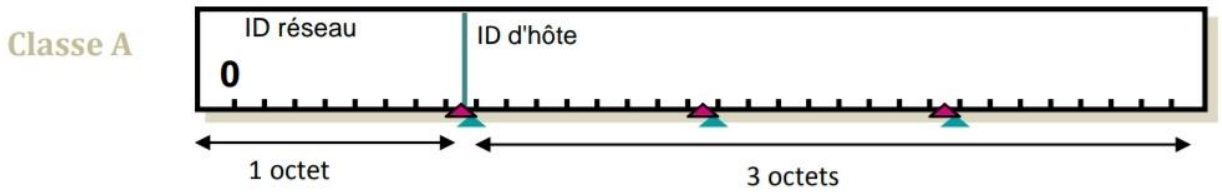


Fig IV.3 Adresse IP Classe A

Classe B

Le premier octet a une valeur comprise entre 128 et 192

Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l’adresse de l’hôte.

(2 bits de poids fort à 10).

65536 réseaux, et pour chacun 65 534 hôtes

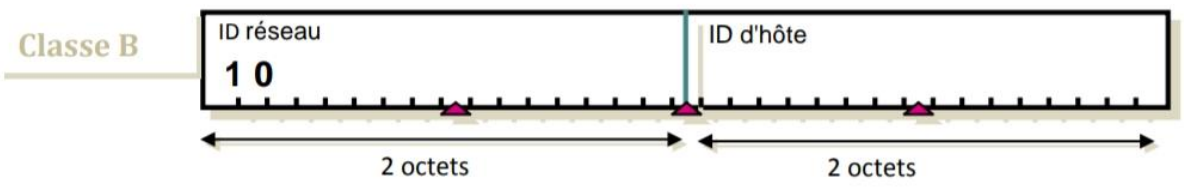


Fig IV.4 Adresse IP Classe B

Classe C

Le premier octet a une valeur comprise entre 192 et 223 (3 bits de poids fort à 110).

Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

16777216 réseaux, et pour chacun 28

254 hôtes

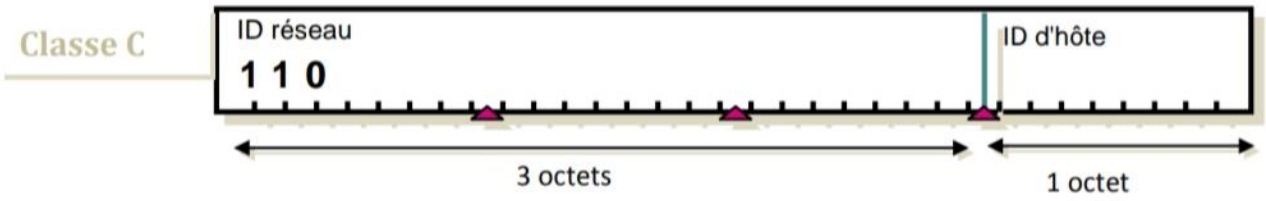


Fig IV.5 Adresse IP Classe C

II.4.Adresse De Bouclage

Les adresses **127.0.0.0 jusqu'à 127.255.255.255** sont des adresses de bouclage (loopback) destinées à vérifier le bon fonctionnement des couches TCP/IP. L'adresse de bouclage **127.0.0.1** est souvent utilisée

II.5.L’adresse réseau et l’adresse de diffusion

II.5.1 L'adresse réseau

Est généralement utilisée pour faire référence à un réseau , dans la plage d'adresses IPv4 d'un réseau, la première adresse est réservée à l'adresse réseau. **La partie hôte de cette adresse comprend uniquement des 0**. Tous les hôtes du réseau partagent la même adresse réseau.

Exemple :

L'adresse 192.168.1.2 appartient au réseau qui a comme :

R h

192.168.1.**00000000** = 192.168.1.0 : adresse réseau

192.168.1.**11111111**=192.168.1.255 : adresse de diffusion (braodcast)

II.5.2 L’adresse de diffusion (broadcast)

Permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour envoyer les données à tous les hôtes d'un réseau en une seule fois, un hôte peut envoyer un paquet adressé à l'adresse de diffusion du réseau. **La partie hôte de cette adresse comprend uniquement des 1**. Tous les hôtes du réseau partagent la même adresse de diffusion

II.6.Adresse privée

L’adresse IP Privée est une adresse qui ne fonctionne pas sur Internet et fonctionne uniquement sur les réseaux privés (réseau local par exemple). Un réseau privé est un réseau qui utilise les plages d'adresses IP non accessibles depuis Internet. Les adresses privées sont utilisées au sein d’un réseau local (entreprise, site, …) et permettent de communiquer localement. Il est unique seulement au niveau sur le réseau local, mais pas sur l’échelle

mondial (ce qui explique par exemple de trouver l'adresse ip : 192.168.1.1 chez vous , et chez le cyber)

L'adresse privée se retrouve dans chacune des classes A, B et C

• La classe A : comprend 16 millions d'adresses. **de 10.0.0.1 à 10.255.255.254**

• La classe B : comprend 65535 adresses **de 172.16.0.1 à 172.31.255.254**

• La classe c : comprend 256 adresses d**e 192.168.0.1 à 192.168.255.254**

Note :

Pour permettre un appareil ayant une adresse privée d'accéder à l'internet, elle doit être d'abord traduite en adresse publique. C'est le protocole NAT(Network Adresse Translation) qui s'occupe de cette tâche.

II.7. Adresse IP Publique

Les adresses IP Publique sont des adresses attribuées au machines pour permettre aux ordinateurs du réseau de communiquer entre eux sur internet. L'adresse IP publique est délivrée par le FAI (fournisseur d'accès à Internet) . L'adresse IP publique est une adresse qui est unique au niveau mondial et non comprise dans la partie privée.

II.8. le masque de réseau

Lorsqu'un hôte IP est configuré, un masque de sous-réseau est attribué avec une adresse IP. Comme l'adresse IP, le masque de sous-réseau est constitué de 32 bits. Le masque de sous-réseau indique quelle partie de l'adresse IP correspond au réseau et quelle partie correspond à l'hôte Le masque de sous-réseau est créé en plaçant le nombre binaire 1 dans chaque position de bit qui représente la partie réseau et en plaçant le nombre binaire 0 dans chaque position de bit qui représente la partie hôte

Partie réseau			Partie hôte
192	168	10	1
On remplace la partie réseau par des 1 et la partie hôte par des 0			
11111111	11111111	11111111	00000000
Le masque sous-réseau est :			
255	255	255	0

Fig IV.6 Masque sous réseau

Le masque par défaut des adresses de :

classe A est : 255.0.0.0

classe B est : 255.255.0.0

classe C est : 255.255.255.0

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse.

A quoi sert le masque sous réseau ?

On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau. Pour une adresse IP spécifique, l'opération ET logique bit à bit entre cette adresse et le masque de réseau permet de déterminer à quel sous-réseau l'adresse appartient

Adresse Ip	192	168	1	2
	11000000	10101000	0000001	00000010
ET logique:				
Masque	255	255	255	0
	11111111	11111111	11111111	00000000
Résultat	192	168	1	0
C'est l'adresse réseau				

Fig IV.7 Opération Et logique

II.9. Calcul sous réseaux

Le calcul sous/réseau Dans un réseau où le nombre de machine est élevé, si un périphérique doit traiter une quantité importante de diffusions, il peut même ralentir ses opérations. De ce fait, les grands réseaux doivent être segmentés en sous-réseaux plus petits qui permettent la localisation des hôtes. Les petits réseaux obtenus lors de la segmentation sont appelés sous-réseaux (subnets) en anglais.la segmentation consiste à regrouper les périphériques et les services dans des sous-réseaux. La segmentation en sous-réseaux peut réduire le trafic global et améliorer les performances réseau. Par exemple dans une entreprise, la segmentation permet de créer un sous réseau pour l'administration, un sous réseau pour le service production et un sous réseau pour le service commercial.

II.9.1 Démarche

Avant de prendre un exemple concret, vous devez connaitre quelques généralités. Tout d'abord, quelle que soit la classe d'adresses dans laquelle vous allez travailler, la formule est la même :

S = 2^n

Dans cette formule, S est le nombre de sous-réseaux désirés. À partir de S, vous devez déterminer n, qui est un nombre entier positif, et qui correspond au nombre de bits devant être **masqués**.

Masquer signifie, en gros, le mettre à 1 pour les besoins du subnetting. Comme vous le savez normalement, le subnetting consiste en l'emprunt des bits de la partie hôte pour créer des sous-réseaux. Ce processus d'emprunt de bits est appelé **masquage**. Masquer un bit, c'est donc l'emprunter, l'allumer.

En fait, S ne pourra pas toujours être égal au nombre de sous-réseaux désirés, nous verrons dans les exemples comment nous allons faire dans ce cas très courant.

II.9.2 Exemple de subnetting

Considérons le réseau **40.0.0.0**. Nous voulons le diviser en 20 sous-réseaux. Déterminons le nombre de bits à masquer pour obtenir un masque de sous-réseau personnalisé, qui devra être appliqué à tous les hôtes.

On ne peut pas obtenir exactement 20 avec la formule **2^n** ! Dans ce cas, nous allons prendre une valeur un peu supérieure pour avoir au moins 20 sous-réseaux. Allons-y doucement :

- 2^4 = 16
- 2^5 = 32

  On a suffisamment de réseaux en masquant 5 bits, on arrête là.

Quand vous avez trop d'adresses IP par sous-réseau, vous devriez empêcher l'assignation des adresses inutilisées. C'est une question de sécurité, pour empêcher qu'un intrus puisse s'octroyer une adresse IP libre.

On ne peut pas mélanger les 1 et les 0, **tous** les 1 doivent être à gauche, et les 0 à droite. Cela veut dire le masquage se fait de la gauche vers la droite.

Nous allons donc masquer 5 bits de cette manière. Nous avons les puissances suivantes (les 8 premières puissances de 2) :
2^7 = 128
2^6 = 64
2^5 = 32
2^4 = 16
2^3 = 8
2^2 = 4
2^1 = 2
2^0 = 1

Voilà donc les 8 premières puissances de deux, par ordre décroissant. Nous allons masquer les 5 bits qu'il nous faut pour obtenir 20. Donc, nous allons **additionner** les valeurs des 5

premières puissances ci-dessus. Cela nous donne donc :
2^7 + 2^6 + 2 ^5 + 2^4 + 2^3 = **248**.
Nous avons masqué 5 bits du 2è octet de notre masque de sous-réseau. Schématiquement, ça nous donne ceci :

255 248 0 0

ssssssss sssssshh hhhhhhhh hhhhhhhh

s = subnet ; h = host

La valeur de notre **nouveau masque de sous-réseau** est à présent **255.248.0.0**

Maintenant il faudrait définir les limites de chaque sous-réseau, sinon ça ne va pas être très utile. Dans le cas présent, nous en avons 31, on va vous donner les 5 premières plages et la dernière, vous allez faire le reste vous-mêmes, il faut bien que vous fassiez quelque chose !

Comment calculer les plages ?

C'est relativement simple. Pour calculer les plages, il faut retrancher le nombre calculé du nouveau masque de sous-réseau à 256. Ce nombre est 248, 256 - 248 = 8. Donc nos sous-réseaux seront séparés par un intervalle de 8.
Concrètement, reprenons le réseau que nous avions choisi à la base : 40.0.0.0.
Le premier sous-réseau est 40.0.0.0, le deuxième est 40.8.0.0, le troisième 40.16.0.0, le quatrième 40.24.0.0.

Pour calculer les plages, il faut savoir que la dernière adresse d'un sous-réseau donné est toujours égale à l'adresse de l'identité du prochain sous-réseau moins 1. Dans notre cas, notre premier sous-réseau est 40.0.0.0. La première adresse IP **adressable** (pouvant être donnée à un hôte) est donc 40.0.0.1 et la dernière... 40.7.255.254.

Techniquement, la dernière adresse dans un réseau est réservée pour la diffusion dite de **broadcast**. Cela sert à envoyer la même chose à tous les hôtes du réseau. Ici, l'adresse 40.7.255.255 est réservée pour le broadcast et n'est pas donc pas assignable à un hôte.

Nous avons donc :

Ordinal	Adresse du sous-réseau	Première adresse IP d'hôte	Dernière adresse IP d'hôte
1er	40.0.0.0	40.0.0.1	40.7.255.254
2ème	40.8.0.0	40.8.0.1	40.15.255.254
3ème	40.16.0.0	40.16.0.1	40.23.255.254
4ème	40.24.0.0	40.24.0.1	40.31.255.254
5ème	40.32.0.0	40.32.0.1	40.39.255.254
...	...	...	...
Dernier	40.240.0.0	40.240.0.1	40.247.255.254

Tableau IV.1 plages d'adresses

Remarquez que le 2ème octet de la dernière adresse IP du dernier sous-réseau est inférieure à la valeur du 2ème octet du masque personnalisé (248).

III.Le routage

Le routage consiste à faire passer des données à travers des routeurs, ou plus précisément, à tracer la route que doivent emprunter des données pour arriver à un point B depuis un point A.

Le routage est l'action de router des packets d'un sous-réseau a un autre. Nous avons vu que lors de la transmission des packets, les hôtes utilisaient un processus internet appelle ANDing ou ET logique. Maintenant que nous sommes dans l'étude des couches du modèle OSI, il est temps d'être plus précis dans les termes. ANDing, n'est pas en fait applique par les hôtes, mais c'est le protocole IP (Internet Protocol) que nous allons étudier, qui effectue cette vérification. Souvenez-vous que chaque couche ajoute des informations dans l'entête des packets, comme nous l'avons vu, de la couche applicative à la couche réseau. Au niveau de la couche réseau, IP doit vérifier s'il s'agit d'une communication intra-réseau ou d'une communication inter-réseau. En fait, c'est comme lorsque vous passez un appel. Il y'a des procédures techniques au niveau de votre opérateur qui vérifient s'il s'agit d'un appel local ou international . Par analogie, c'est ce que fait le protocole IP au niveau de la couche 3.

Quand il s'agit d'une transmission en dehors du réseau, les packets sont transmis au routeur qui se chargera du reste. Cette transmission de packets d'un sous-réseau à un autre est définie par **« routage »**.

Il faut également noter qu'il y'a deux types de routage : le routage statique et le routage dynamique.

III.1 Routage statique

Les routeurs dans un réseau doivent communiquer normalement et s'échanger des informations telles que le contenu de la table de routage, que nous allons étudier plus bas. Le processus d'échange d'informations entre routeurs dépend du type de routage utilisé. Dans un routage statique, c'est vous l'administrateur réseau qui devez construire et mettre à jour manuellement vos tables de routages. Donc dans un routage statique, le contenu des tables de routage est également statique. Ce type de routage n'est pas vraiment pratique pour les raisons évidentes ci-dessous :

- Les routeurs ne découvriront pas automatiquement les Network ID des autres réseaux, ce sera à vous de les leur apprendre par une configuration manuelle
- Les routeurs ne pourront pas communiquer entre eux pour s'échanger des informations, ce sera à vous de modifier les changements des données de votre réseau dans chaque routeur, manuellement
- Les routeurs ne seront pas intelligents et pourront garder des données erronées dans leur table. Etant donné qu'ils ne communiquent pas entre eux dans un routage statique, cela veut dire que si un chemin vers un réseau n'est plus praticable, un routeur continuera à considérer ce chemin comme étant valable, du moins, tant que vous ne l'aurez pas changé

Par routage statique, tout ce que vous devez comprendre est que le routage se fait manuellement par l'administrateur.

III.2 Routage dynamique

Le routage dynamique est exactement le contraire du routage statique . Ceci dit, tout se fait automatiquement grâce à un protocole de routage.

1.La table de routage

Le routage est la fonction principale d'un routeur. Imaginez un réseau de milliers d'hôtes segmentes en une dizaine de sous-réseaux. Il faudrait beaucoup de routeurs pour assurer la communication entre ces 10 sous-réseaux. Les routeurs doivent s'assurer que chaque hôte de n'importe quel sous-réseau communique avec les hôtes de tous les sous-réseaux. Pour implémenter un routage effectif, il faut que les routeurs sachent prendre des décisions, pour savoir par quel routeur passer pour arriver à tel sous-réseau. Les routeurs, pour ce faire, utilisent ce qu'on appelle **« une table de routage »**. Quand un hôte x du réseau A veut communiquer avec un hôte Y du réseau B, les packets seront envoyé au routeur AB qui relie le réseau A et B. Dans l'entête du packet (comme nous allons le voir bientôt) se trouve l'adresse IP de l'émetteur et celle du destinataire. Le routeur devra donc vérifier dans **sa table de routage** comment faire pour arriver au sous-réseau dans lequel se trouve l'adresse IP du destinataire. Cette table de routage contient les Network ID de tous les routeurs qui sont directement connectes au routeur AB. La table de routage contiendra également tous les chemins possibles pour atteindre un sous-réseau donne, ainsi que le cout que cela implique.

2.Métrique

La métrique est simplement la distance entre un réseau et un routeur. Nous avons vu qu'un saut était le nombre de fois qu'un packet « traversait » un routeur avant d'arriver à sa destination. Ce saut est une forme de métrique, tout comme la bande passante d'un chemin. Nous allons voir cela dans les détails, après avoir étudié les protocoles de routage, car la métrique est une notion liée aux protocoles de routage . C'est le protocole de routage en fait qui détermine ce qu'est une métrique. Par exemple avec OSPF, la métrique peut correspondre à un vecteur qui tient compte de plusieurs paramètres tel que le délai et la charge.

3.Interface

Une interface est le point de contact de deux systèmes. Par exemple, une interface graphique est le point de contact entre un programme et un utilisateur.

En réseau, une interface est en fait un port. Il s'agit d'un port physique (comprendre « point de connexion ») qui relie des sous-réseaux. Ainsi un routeur doit avoir plusieurs interfaces pour pouvoir relier plusieurs sous-réseaux entre eux

III.3 1.Les différents protocoles de routage

Il existe plusieurs protocoles de routage. Normalement un routeur peut supporter plusieurs protocoles. Pourquoi en avoir plusieurs, s'ils servent tous à faire la même chose ? La réponse se trouve dans la méthodologie. Ces protocoles font la même chose, mais certains sont plus pratiques que d'autres, d'autres ont des contraintes plus couteuses par exemple. Les protocoles les plus célèbres sont :

- RIPv1 et RIPv2
- OSPF
- EIGRP
- IGRP
- BGP
- MPLS
- IS-IS

Ces protocoles peuvent se classer dans des « familles » . Il existe deux « classes » de protocole de routage :

- **IGP (Interior Gateway Protocol, Protocole de routage internet)** : C'est la famille des protocoles qui peuvent échanger des informations de routage avec des AS (Autonomous Systems). En d'autres termes c'est simplement un ensemble de réseaux IP contrôlés par une organisation ou une entreprise
- **EGP (Exterior Gateway Protocol, Protocole de routage externe)** : C'est la famille des protocoles qui déterminent la disponibilité d'un réseau ente deux systèmes autonomes. Les protocoles de cette famille, utilisent les protocoles IGP pour résoudre

les routes dans un système autonome. Il s'agit des protocoles permettant le routage entre deux systèmes autonomes différents. Les FAIs (Fournisseurs d'accès Internet) par exemple utiliseront un protocole de cette famille pour effectuer un routage externe. C'est donc la famille du protocole de routage utilisé par internet.

III.3.1 Le protocole de routage RIP

RIP (ROUTING INFORMATION PROTOCOL) , est conçu RIP (Routing Information Protocol) pour fonctionner en tant que protocole interne dans des systèmes autonomes de taille modérée

Principe de fonctionnement

Le protocole est limité aux réseaux dont le plus long chemin (qu'on appelle couramment le diamètre du réseau) implique quinze routeurs au maximum. Il est mal adapté au traitement des boucles dans les chemins et utilise des mesures du coût des chemins (ou métriques) fixes pour comparer les routes alternatives. Les situations où les routes doivent être choisies en fonction de paramètres mesurés en temps réel comme un délai, une fiabilité ou une charge, se prêtent mal à ce type de traitement. Un routeur RIP calcule des chemins pour différentes destinations, lesquelles sont spécifiées par leurs adresses IP, c'est-à-dire qu'une entrée dans la table peut représenter soit un réseau, soit un sous-réseau ou encore un nœud isolé. RIP ne spécifie pas le type de l'adresse : les routeurs découvrent la nature du destinataire en analysant les adresses transmises. Les routeurs RIP sont actifs ou passifs. Actifs, ils transmettent et reçoivent les routes : ils diffusent leurs informations aux autres routeurs. Passifs, ils ne font qu'attendre la réception des informations. En fonction de celles-ci, ils calculent leurs tables de routage mais ne partagent pas les résultats de leurs calculs avec d'autres routeurs. Le routeur RIP actif permet aux autres routeurs de mettre à jour leurs tables de routage toutes les 30 secondes. Si un routeur ne reçoit aucune mise à jour d'un autre routeur dans un délai de 180 secondes, il marque les routes desservies par ce dernier comme inutilisables. S'il n'y a aucune mise à jour après 240 secondes, le protocole RIP supprime toutes les entrées correspondant au routeur qui ne répond pas. Chaque diffusion RIP contient des paires adresses IP/nombre de routeurs à traverser (ou nombre de sauts). Comme le nombre de sauts est la seule mesure utilisée par le protocole, RIP ne garantit pas que le chemin sélectionné soit le

plus rapide : un chemin court mais embouteillé peut être un mauvais choix par rapport à un chemin plus long mais totalement dégagé. Lorsqu'un événement dans le réseau provoque un changement dans la table de routage d'un routeur actif, celui-ci envoie un message de mise à jour à ses voisins. Si cet événement a un impact sur les voisins, ceux-ci propagent l'information. On utilise une temporisation afin de stabiliser l'état du réseau et garantir que tous les messages de mise à jour ont été pris en compte avant de renvoyer une nouvelle mise à jour.

III.3.2 Le protocole OSPF (OPEN SHORTEST PATH FIRST)

L'algorithme SPF (Shortest Path First) calcule le plus court chemin vers toutes les destinations de la zone ou du système autonome, en partant du routeur où s'effectue le calcul (à partir de sa base de données topologiques). Il utilise un algorithme conçu par Dijkstra et calcule le plus court chemin, selon un critère de coût où interviennent de multiples paramètres : l'état des liens, l'encombrement du réseau et des mémoires des routeurs intermédiaires.

Principe de fonctionnement

Le calcul du plus court chemin est effectué de manière indépendante par tous les routeurs internes d'un système autonome SA. Grâce à cet algorithme, un routeur peut connaître le prochain routeur qui transmettra le message : il trouve les plus courts chemins (en termes de coût) d'un point à un autre, pour que le message arrive de manière optimale à son destinataire, puis il effectue la mise à jour de sa table de routage. Chaque mise à jour de la base de données entraîne celle de la table de routage. Il y a, comme précédemment, communication entre les routeurs. Celle-ci est régie par le protocole OSPF. Ce protocole définit les règles et les formats de messages entre routeurs OSPF internes à un système autonome. Il a la particularité de s'appuyer directement sur IP (et non sur UDP comme le protocole RIP). C'est une nette amélioration, car le routage devient un traitement interne à la couche réseau et n'est plus considéré comme une application. De plus, le fonctionnement d'OSPF est optimisé si le SA est découpé en zones ; OSPF prévoit un découpage avec une hiérarchie à deux niveaux de zones. La zone de niveau le plus élevé est l'épine dorsale (ou backbone zone). Elle interconnecte les « routeurs de bordure » . À l'intérieur de chaque zone du second niveau, les routeurs ne connaissent – et ne diffusent – que des informations internes à leur zone

Fiche Td n° :03

Exercice n°1: Questions de cours

1. De combien d'octets est constituée une adresse IP ?
2. Combien de classe d'adresses IP existe-t-il ?
3. Pour chaque classe, combien d'octets sont réservés pour :
   - La partie réseau
   - La partie machine
4. Quelle est la limitation des adresses IP V4 ?
5. Qu'est ce qu'une adresse IP Privée.
6. Donner les plages d'adresse IP privée réservé pour chaque classe.
7. Expliquer la technique utilisée pour créer des sous réseaux.

Exercice n°2: Classes d'adresses IP

1. Indiquer pour chacune des adresses IP ci-dessous :

204.160.241.93
138.96.32.3
172.31.255.254
18.181.0.31
226.192.60.40
10.10.10.4

- Sa classe
- L'adresse de réseau
- L'adresse de broadcast
- Le masque de sous-réseau
- Le nombre de machine possible

2. Quelle est la particularité des 3eme et dernière adresses ?

Exercice n°3: Sous Réseaux

Un réseau de classe B dispose du masque de sous-réseau 255.255.240.0.

1. Combien de bits ont-ils été empruntés à la partie host-id pour créer des sous-réseaux ?
2. En déduire le nombre de sous-réseaux possibles.
3. Combien de bits restent-ils à host-id ?
4. En déduire le nombre de machines possibles pour chacun des sous-réseaux.
5. Reprendre les questions précédentes avec un réseau de classe A disposant du masque 255.248.0.0

Exercice n°4 : Masque de sous-réseau

Une entreprise à succursales multiples s'est vue affecter l'adresse IP 196.179.110.0. Pour une gestion plus fine de ses sous-réseaux, le responsable informatique désire pouvoir affecter une adresse IP propre à chaque sous-réseau des 10 succursales.

1. De quelle classe d'adressage s'agit-il ?
2. Donner et expliquez la valeur du masque de sous-réseau correspondant à ce besoin.
3. Combien de machines chaque sous-réseau pourra-t-il comporter et pourquoi ?
4. Définissez les adresses de réseau et de broadcast de chacune des succursales.
5. Donner la première et la dernière adresse de machine possible pour chaque succursale.

Exercice n°5: Masque de sous-réseau et dysfonctionnement

Certains utilisateurs du réseau local d'une entreprise, utilisant une application au-dessus de UDP (couche 4 OSI), se plaignent de ne pas pouvoir communiquer avec tous les autres utilisateurs alors que ceux-ci le peuvent avec eux. Le responsable bureautique local vous demande d'expertiser son réseau. Pour lui le fait qu'une station puisse émettre des messages vers une autre et que cette dernière ne puisse répondre le laisse perplexe. Votre rapport d'expertise, à compléter, comporte les éléments suivants :

Vous constatez que toutes les stations sont sur le même segment Ethernet et que celui-ci ne comporte aucun routeur et qu'aucune station n'est configurée pour remplir ce rôle;

Vous relevez les configurations suivantes :

Station A @ 150.150.1.28/24
Station B @ 150.150.1.57 /16
Station C @ 150.150.2.2 8/24
Station D @ 150.150.2.57/16

1. Vous écrirez dans le tableau sous l'adresse de chaque station son masque de sous-réseau
2. Vous établirez la matrice de communication (complétez par oui, dans le tableau ci-dessous lorsque la communication est possible et par non dans le cas contraire)

Source Destination	150.150.1.28 . . . •. . . •. . . •. . .	150.150.1.57 . . . •. . . •. . . •. . .	150.150.2.28 . . . •. . . •. . . •. . .	150.150.2.57 . . . •. . . •. . . •. . .
150.150.1.28	oui			
150.150.1.57				
150.150.2.28				
150.150.2.57				

3. Vous expliquerez votre démarche en justifiant votre réponse pour un exemple de communication:
   - possible
   - impossible

Rappel : Pour déterminer si la machine cible est localisée sur le même sous-réseau, la machine source réalise un « ET » logique entre les bits de l'adresse source et ceux du masque de sous-réseau, elle procède de même avec l'adresse destination. Si le résultat donne une valeur identique les deux machines sont sur le même sous-réseau, sinon le datagramme est adressé au routeur (passerelle par défaut).

Exercice n° 6 : Adressage CIDR

1. Indiquez à quelle zone géographique appartiennent les adresses suivantes :

202.12.0.15

199.3.2.1

201.254.11.33

197.5.0.4

2. Une entreprise basée en chine possède un réseau informatique de 920 machines. Indiquez en justifiant votre réponse quelles pourraient être la plage d'adresse de classe C qui lui serait attribuée ? Indiquez le masque de sous réseau correspondant.

(Contrainte le deuxième octet de chaque adresse sera fixée à 33 : -------- . 33 . -------- . --------)

3. Même question pour une société située à Montréal et possédant un parc de 3125 machines ?

Exercice n° 7 : Adressage CIDR

Quelles sont les adresses IP couvertes par l'adresse CIDR 192.168.10.0/20 ?

xxxx/20 signifie masque avec les 20 bits de gauche à 1

Exercice n° 8 : Adressage CIDR

Indiquez en regard de chaque plage d'adresses le réseau en notation standard et CIDR

Cette plage d'adresses	**provient du réseau noté en CIDR**
Ex : 10.0.0.1. -- 10.255.255.254	10.0.0.0 / 8
192.168.15.117 -- 192.168.15.118	
172.16.0.1 -- 172.31.255.254	
10.1.64.1 – 10.1.127.254	
210.44.8.81 -- 210.44.8.94	

Couche Transport

5

I.Introduction

Le rôle de la couche transport est de **rendre possible la communication logique entre applications**. En anglais, on parle de *logical end-to-end communication*.

Nous avons vu ce qu'est une connexion logique en expliquant la couche 3 (réseau). C'est une communication "distante", dans le sens où les hôtes communiquant ne sont pas forcément reliés physiquement. En effet, il peut y avoir plusieurs matériels intermédiaires allant d'un simple concentrateur (hub) à une passerelle applicative (gateway). **Note :**

Il y a une **grande différence** entre la communication logique établie par la couche transport et celle établie par la couche réseau. La couche transport établit une communication logique entre les **processus d'applications** alors que la couche réseau établit une communication logique entre **les hôtes**.

Voici un tableau qui résume ces deux types de communication :

Couche	Type de communication	Entre
Transport	Logique	Processus
Réseau	Logique	Hôtes

Tableau V.2 les deux types de communication

La communication logique qu'établit la couche transport se fait entre les applications impliquées dans la communication. En effet, lorsque deux hôtes A et B communiquent, c'est par le biais d'une application. Par « bout-à-bout », la pensée exprimée est que la communication entre les couches se fait de façon parallèle.

Voici un schéma illustrant ce principe de communication parallèle :

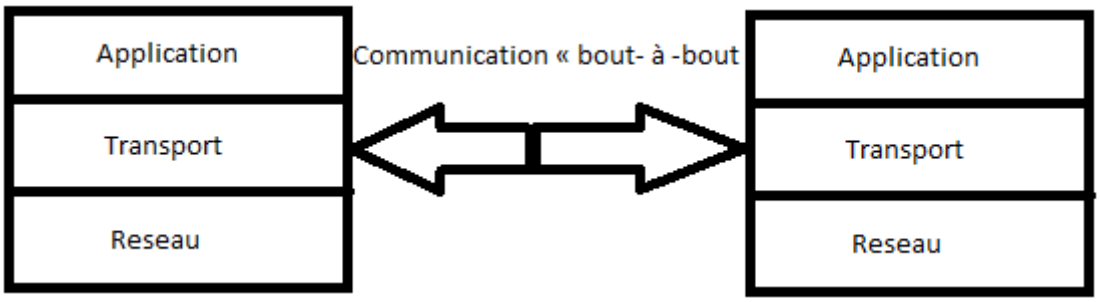


Fig V.1 les couches applicatifs

Ce principe reste valable pour les autres couches du modèle OSI ou TCP-IP. Chaque couche communique parallèlement avec sa couche « homologue ». La couche application de l'hôte émetteur communique directement avec la couche application de l'hôte récepteur, de même que la couche transport de l'émetteur communique directement avec la couche transport de l'hôte récepteur.

II. La procédure de communication entre applications

Quand l'hôte A envoie un message, il utilise une application comme un client de messagerie. Cette application lui donne accès aux services réseaux pour envoyer un mail, donc le protocole SMTP sera utilisé, par exemple. Une fois ce SDU reçu par la couche transport, il sera converti en un PDU, comme nous l'avons vu. La couche transport, qui est aussi responsable de la fragmentation des unités de données, va « couper » ce SDU en plusieurs chaînes (ou morceaux) qu'on appelle « chunks » en anglais. À chaque « morceau » sera ajouté un en-tête. Le SDU reçu par la couche transport sera donc « brisé » en 4 PDU distincts, par exemple.

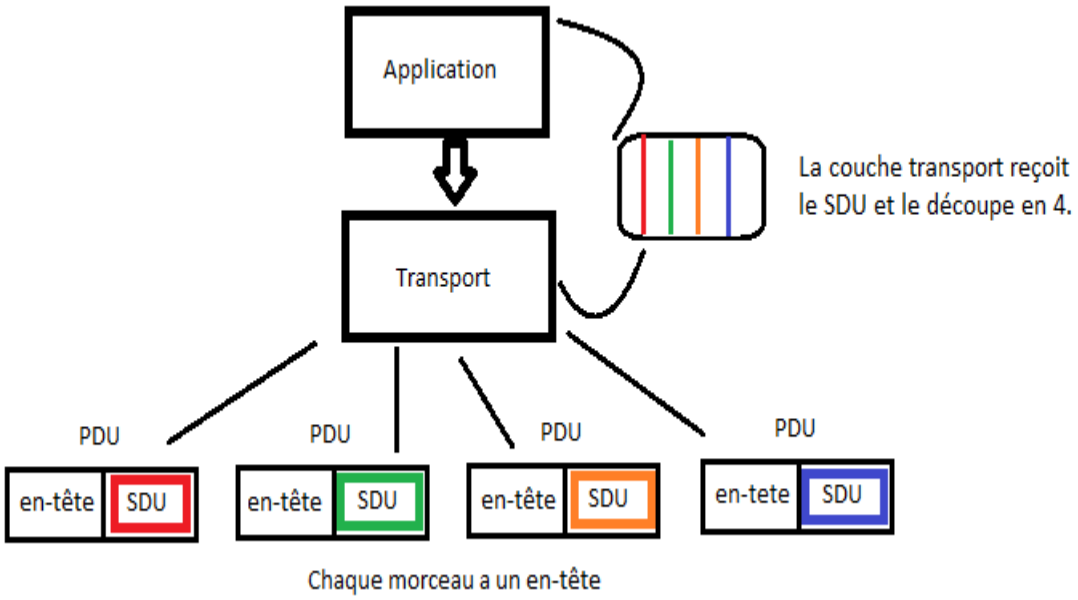


Fig V.2 Procédure de communications entre applications

Ces 4 PDU seront envoyés à la couche la couche réseau.

Voilà, c'est tout ce qui se passe dans la procédure de transmission.

Du côté de l'hôte récepteur B, La couche transport de cet hôte recevra les 4 PDU originaux, lira leurs en-têtes et les rassemblera en une seule unité de donnée, après avoir supprimé les en-têtes bien sûr (n'oubliez pas les règles du principe de l'encapsulation). Finalement, le « message » sera transmis au processus de l'application réceptrice.

Notion de Processus :

Un processus est une instance d'une application en cours d'exécution (l'application qui est **actuellement** exécutée). Parfois, un processus peut être constitué de plusieurs threads (des « sous-processus », en quelque sorte) qui exécutent des instructions au même moment. C'est tout ce que vous avez besoin de savoir pour l'instant.

III. La relation entre la couche transport et la couche réseau

Chaque couche communique avec une couche adjacente (soit supérieure, soit inférieure).

Il se trouve que la couche transport est juste avant la couche réseau dans l'ordre décroissant des couches. Il va donc sans dire que la couche transport communique avec la couche réseau.

La couche transport n'échappe pas à la règle. Cette couche est un ensemble de services. Ces services sont généralement fournis par un protocole ou une bibliothèque externe.

IV. Les services de la couche transport

- **Communication orientée connexion** : de l'anglais ***Connection-oriented communication***, ce service est bénéfique pour plusieurs applications, notamment parce qu'il interprète la connexion établie entre processus comme étant un flux de données. Ce flux de données n'est en fait qu'une séquence d'octets (8 bits). Ainsi, il faudrait donc gérer l'orientation des octets, qui est également un service de cette couche. Il est plus facile de gérer ce genre de communication que d'avoir affaire au mode orienté non connexion.
- **L'ordre de livraison** : nous savons que la couche transport fragmente les données en plusieurs séquences. La couche réseau ne peut pas garantir que les données envoyées arriveront exactement dans l'ordre même de leur envoi. (le contrôle de séquences). C'est la couche transport qui se charge de gérer les séquences, de s'assurer que l'ordre de livraison est le même que l'ordre d'envoi. Cette gestion de séquences se fait en utilisant un numéro de séquence.
- **Fiabilité** : Le but de ce service est de vérifier l'intégralité des paquets car ces derniers peuvent se perdre en cours de transmission à cause de la congestion du réseau. Cette vérification d'intégralité se fait souvent en utilisant un code de détection d'erreurs tel que la **somme de contrôle (*checksum*)**. La fiabilité consiste aussi à s'assurer que le récepteur reçoit chaque segment qui lui est envoyé. Cela est accompli par l'envoi des **ACK et NACK** (accusés de réception) à l'émetteur. Il faudrait donc également être en mesure de renvoyer les séquences qui se sont perdues : cela se fait par une **requête automatique de renvoi**.

- **Gestion de flux** : Quand deux personnes parlent, il est nécessaire de donner à celui qui "écoute" le temps de comprendre ce qui est dit, puisqu'il se peut que l'émetteur parle plus vite que le récepteur. Il faut donc gérer cette volubilité, ce flux. Dans les réseaux, il y a des cas où un hôte-émetteur peut transmettre plus vite que ne peut recevoir un hôte-récepteur. C'est là qu'intervient l'utilité de la gestion des flux.
- **Contrôle de congestion** : Le contrôle de congestion sert à contrôler le trafic dans un réseau (informatique ou de télécom) afin de réduire la congestion (saturation) d'un réseau en évitant que les autres clients utilisent les liens de connexion qui sont déjà extrêmement utilisés.
- ***Multiplexing* / *demultiplexing*** : La couche transport implémente le multiplexage afin de permettre à plusieurs processus de communiquer sur le même réseau. Les informations sont divisées en segments (PDU) associés à une application spécifique. Concrètement cela consiste en l'utilisation d'un port associé à un socket pour chaque processus d'une machine. Ces informations sont contenues dans l'en-tête du segment de la couche transport.

Les numéros de port :

Un numéro de port sert également à identifier *quelque chose*. Mais ce *quelque chose* est une application. Le numéro de port est donc le numéro qui nous permet de faire la distinction entre les applications. Nous savons déjà que la couche transport établit une communication bout-à-bout entre les processus d'applications. Alors comment faire pour distinguer les nombreux processus d'une application qui sont en fait des services exécutés sur une machine ? C'est le numéro de port qui permettra de les différencier.

L'organisme IANA (Internet Assigned Numbers Authority) (en) classe les numéros de port en trois catégories principales, comme l'illustre le tableau ci-dessous.

Portée	Catégorie	Description
0 - 1023	Ports bien connus	Ports réservés pour des services bien connus (web, envoi de mail, etc.).

Portée	Catégorie	Description
1024 – 49 151	Ports réservés	Ports réservés pour être utilisés par des applications propriétaires.
49 152 – 65 635	Ports dynamiques	Ports « libres » que vous pouvez utiliser pour vos applications. Ils ne sont ni pour des services bien connus, ni réservés par une entreprise quelconque.

Tableau V.1 les catégories des numéros de ports

Voici quelques ports bien connus :

Protocole	Description	Protocole de transmission	Numéro de port	Statut d'assignation
File Transfert Protocole (FTP)	Protocole de transfert de fichier	TCP	21	Officiel
Secured SHell (SSH)	Protocole permettant l'échange de données par le biais d'un canal sécurisé	TCP & UDP	22	Officiel
Telnet	Utilisé pour l'établissement des sessions à distance	TCP	23	Officiel
Simple Mail Transfer Protocol (SMTP)	Protocole d'envoi de courrier électronique	TCP	25	Officiel
WHOIS protocol	Protocole ou service utilisé pour l'identification d'une machine par son nom de domaine ou son adresse IP. La procédure d'identification se fait par une requête envoyée à un des registres	TCP	43	Officiel

Protocole	Description	Protocole de transmission	Numéro de port	Statut d'assignation
	Internet pour obtenir des informations.			
Domain Name System (DNS)	Protocole de résolution des noms de domaine	TCP & UDP	53	Officiel
HyperText Transfer Protocol (HTTP)	Protocole de téléchargement (principalement de pages web)	TCP & UDP	80	Officiel
Post Office Protocol Version 2 (POP2)	Protocole de retrait de mails d'un serveur de messagerie	TCP	109	Officiel
Post Office Protocol Version 3 (POP3)	Protocole de retrait de mails d'un serveur de messagerie	TCP	110	Officiel
Internet Message Access Protocol (IMAP)	Protocole de retrait et consultation de mails d'un serveur de messagerie	TCP & UDP	143	Officiel
...	...	...	...	...

Tableau V.2 Numéros de ports répandus

V. Les protocoles de la couche transport

Nous allons nous focaliser sur les deux protocoles principaux de cette couche, a savoir TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). Nous commencerons par étudier UDP, ensuite nous attirerons votre attention sur TCP.

V.1 le protocole UDP (User Datagram Protocol)

UDP est l'un des protocoles les plus utilisés au niveau de la couche transport, juste après TCP. Les deux sont des protocoles dont la vocation est de transporter les données d'une application à une autre comme nous l'avons vu.

UDP signifie **User Datagram Protocol** (protocole d'utilisateur de datagramme). C'est un protocole de transport qui ne peut pas garantir que les données arriveront toutes à destination. C'est d'ailleurs l'un des principaux défauts de ce protocole. On ne peut pas être sûr que les données arriveront au destinataire car UDP n'a pas de mécanisme de retransmission quand un paquet se perd et il est un protocole **non orienté connexion**.

Pourquoi « non orienté connexion » ?

Par exemple dans une conversion au téléphone, comment opéraient les protocoles. La première étape d'une communication était l'établissement de la connexion,
En effet, lorsque vous téléphonez à un ami, il décroche en disant « Allô » et vous répondez « Allô ». C'est le même principe que la poignée de main, vous vous êtes mis d'accord sur le fait que vous allez engager une conversation.

En réseau, le principe reste fondamentalement le même. Quand vous voulez communiquer avec un autre hôte dans un réseau, il faut que les deux hôtes se mettent d'accord. Cette entente se fait par la poignée de main. En fait, l'hôte émetteur envoie un paquet qui dit « Est-ce qu'on peut parler ? » et l'hôte récepteur répond « Vas-y, j'écoute ». Et là les deux peuvent s'échanger des données !

Le rapport avec UDP ?

Justement, UDP n'est pas orienté connexion du fait qu'il n'implémente pas ce principe de la poignée de main. En d'autres termes, lorsqu'une application utilise UDP comme protocole, les données sont envoyées sans au préalable établir une session ou une connexion avec l'hôte récepteur. C'est pour cela que UDP ne garantit pas que les données vont arriver.

Quand vous utilisez UDP, c'est comme si vous parliez à quelqu'un qu'il soit éveillé ou endormi. S'il est éveillé tant mieux, il vous écoute, il **reçoit votre message**. Par contre si il dort, il ne recevra rien. Voilà pourquoi UDP est un protocole dit **orienté transaction**, en d'autres termes, il se contente d'envoyer le message et d'espérer que tout se passe bien.

Caractéristiques du UDP

- **Mode non connecté** : nous avons dit que UDP n'utilisait pas un mode orienté connexion, donc il n'implémente pas le principe de connexion par poignée de main
- **État de connexion** : l'état de connexion est un sujet un peu complexe pour l'instant, et il est propre à TCP. UDP ne maintient pas des informations sur l'état de la connexion.
- **La longueur de l'en-tête** : l'en-tête d'un segment UDP est relativement simple. Il ne vaut que 8 octets. L'en-tête de TCP est plus complexe que celui d'UDP.
- **Taux de transmission** : avec UDP, la vitesse (ou le taux) de transmission est intimement liée aux caractéristiques de l'environnement du système d'exploitation. C'est-à-dire que cette vitesse dépend des ressources système (fréquence du processeur, etc.) d'une part, et de la bande passante d'autre part. Puisque UDP n'a pas de mécanisme de contrôle de congestion, le taux de transmission dépend de la vitesse à laquelle l'application utilisée génère ces datagrammes.

Utilisez UDP lorsque vous n'avez pas besoin de garantir que les données envoyées arriveront à leurs destinataires. Par exemple, dans le cadre de la VoIP (la téléphonie via Internet), plusieurs applications utilisent UDP, comme Skype. S'il faut renvoyer les messages vocaux à chaque fois jusqu'à ce qu'ils arrivent, cela va significativement alourdir le réseau, voilà pourquoi les conversations téléphoniques sur Internet se font via UDP. Le service DNS (qui permet de traduire les adresses IP en noms de domaine) utilise également UDP.

UDP n'étant pas vraiment un protocole très fondamental de la suite TCP-IP,.

V.2 Le protocole TCP

TCP, qui signifie Transmission Control Protocol, Protocole de contrôle de transmission en anglais, est un protocole de la couche transport défini par les RFC 793, 1122, 1323 et aussi 2581.
Tout comme UDP, le but de TCP est d'assurer la transmission des SDU. Tout comme UDP, TCP nous offre des services de multiplexage et démultiplexage. La différence se situe fondamentalement dans ce que nous avons appelé « principe de transmission fiable »

UDP, comme nous l'avons vu, est un protocole orienté transaction, par conséquent, il ne peut garantir que les données transmises arriveront à destination. TCP, en revanche, étant un protocole orienté-connexion par le principe de la poignée de main (handshake) établit une connexion au préalable, entre les processus avant de débuter la transmission.

TCP offre des services de détection d'erreurs dans les transmissions, mais n'a malheureusement aucune propriété de « réparation » de ces données dont l'intégrité est affectée

L'état de connexion avec TCP

Nous avons dit que TCP était un protocole orienté-connexion, mais qu'est ce que ca veut dire concrètement ? Pour qu'il y'ait échange ou transmission entre deux applications utilisant TCP comme protocole de transport, il faut établir une connexion TCP. La poignée de main (handshake), ou le genre de connexion que TCP établit est aussi appelé « three-way handshake ». Cela veut dire que la connexion se fait en trois étapes. En effet, TCP est un protocole full-duplex, ce qui implique qu'une communication bidirectionnelle et simultanée est possible dans une connexion TCP.

Etapes de connexion

Supposons que 2 processus de deux hôtes différents veulent s'échanger des informations. Il faut, bien entendu, qu'un hôte initialise la connexion (demande à l'autre hôte la permission de communiquer). Comme vous le savez, l'hôte qui initialise la connexion est le client, et celui qui accepte est le serveur.

Dans le cas où une connexion TCP est initialisée au même moment, les deux applications (ou processus) sont à la fois client et serveur.

Le client et le serveur s'échangent donc des unités de données appelées des segments TCP (TCP segments en anglais) qui sont composés bien entendu d'un entête et d'un espace de données (data area en anglais).

Nous considérons 6 paramètres extrêmement importants pour saisir la procédure d'établissement d'une connexion TCP entre un client et un serveur. Ces paramètres sont :

1.Etat du serveur : Définit dans quel état se trouve le serveur dans l'établissement de la connexion

2.Etat du Client : Définit dans quel état se trouve le client dans l'établissement de la connexion

3.Segment transmis par le client : la constitution du segment TCP constitué d'un entête et d'une donnée que les deux s'échangent le long de la procédure

4.Segment transmis par le serveur : la constitution du segment TCP constitué d'un entête et d'une donnée que les deux s'échangent le long de la procédure

5.Etat de transition du client : définit simplement un état entre deux états. :-' C'est maladroit de le dire ainsi, grossièrement, lorsque le serveur par exemple, passe de l'état fermé (closed) à l'état ouvert, l'état de transition ici est l'état d'écoute (Listen). En effet pour pouvoir ouvrir ou initialiser une connexion, il faut bien que le serveur écoute le port auquel il est attaché. On dit que cet état d'écoute est un **état de transition.**

6.Etat de transition du serveur : définit simplement un état entre deux états. :-' C'est maladroit de le dire ainsi, grossièrement, lorsque le serveur par exemple, passe de l'état fermé (closed) à l'état ouvert, l'état de transition ici est l'état d'écoute (Listen). En effet pour pouvoir ouvrir ou initialiser une connexion, il faut bien que le serveur écoute le port auquel il est attaché. On dit que cet état d'écoute est un **état de transition.**

-Le terme client se réfère à l'application ayant initialisée la demande de connexion,

-Le terme serveur se réfère à l'application réceptrice de cette demande.

Etape 1 : Pour faire une demande d'initialisation de connexion, le client envoi un segment TCP qui ne contient **QUE** l'entête. Il est important de noter que le premier segment TCP envoyé dans le three-way handshake n'a **aucun** payload, mais **seulement un entête**

L'entête contient un flag (drapeau) de synchronisation : Flag SYN (avec SYN diminutif de SYNchroniser). L'entête contient aussi le numéro de port TCP du serveur, ce qui est logique, car le numéro de port, est pour une application, ce que l'adresse IP est pour un hôte.

Après l'envoi de ce premier segment TCP, le client se met dans un état **SYN_SENT**. (SYN_SENT signifie que le segment TCP ayant le flag SYN a été envoyé).

Le serveur de son côté, est en état **Listen**. Il écoute sur le numéro de port, attendant une demande de connexion. Dès qu'Il reçoit le segment TCP envoyé par le client (celui qui n'a qu'un entête et un flag SYN), il envoie un segment TCP vers le client pour confirmer la réception du flag SYN. Ce segment également n'est constitué que d'un entête portant deux flags : **SYN** (chronize) et **ACK**(nowledge). Finalement, le serveur change d'état et passe de Listen à **SYN_RCVD**. RCVD est le diminutif de **received** (reçu en anglais). Cet état confirme que le segment TCP portant le flag SYN a été reçu.

SYN ou ACK sont deux flags importants dans l'entête d'un segment TCP. Quand le client ou le serveur envoi un SYN ou ACK, ça veut dire que le bit de ce flag est allumé (mis a 1) dans l'entête.

Etape 2 et 3 : Le client reçoit le segment TCP et analyse l'entête. Il remarque qu'il contient les flags SYN et ACK, qui sont pour lui des indicateurs que le serveur a accepté d'initialiser une connexion avec lui. La connexion passe donc de **Closed** (fermée) à **established** (établie).

Il conclut la procédure en envoyant un segment TCP avec le flag ACK au serveur. Ce dernier ACK envoyé est la conclusion de la procédure et va également mettre le serveur en état de connexion établie (established state).

Maintenant que les deux (client et serveur) ont établi une connexion, cette dernière peut être utilisée pour transmettre des informations

Etant donné que dans notre scénario c'est le client qui est responsable d'avoir fait une demande de connexion, on dit que le client effectue une **connexion active (active open)** alors que le serveur n'a fait qu'accepter l'invitation, ce dernier effectue une **connexion passive (passive open). Les deux figures suivantes montrent la procédure**

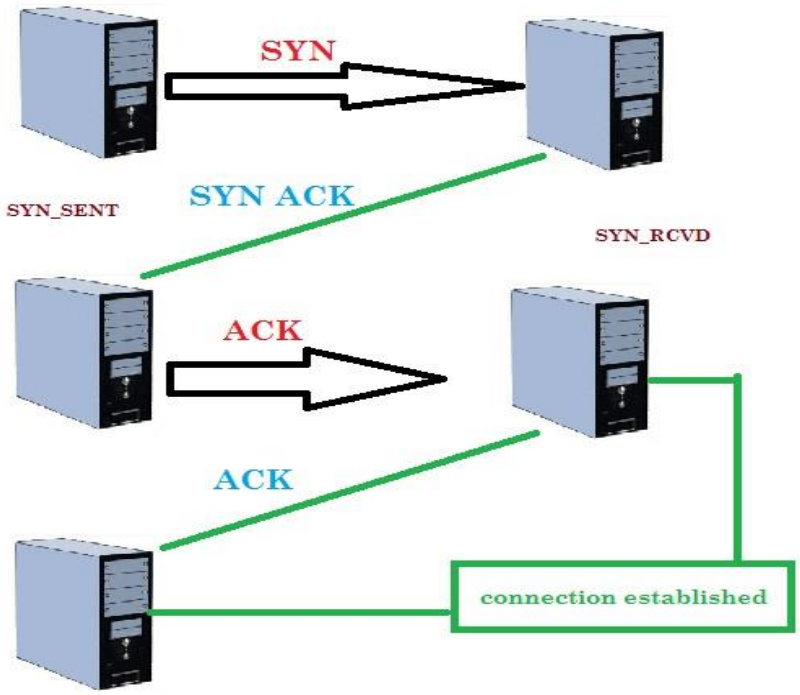


Fig V.3 Etapes de Connexion

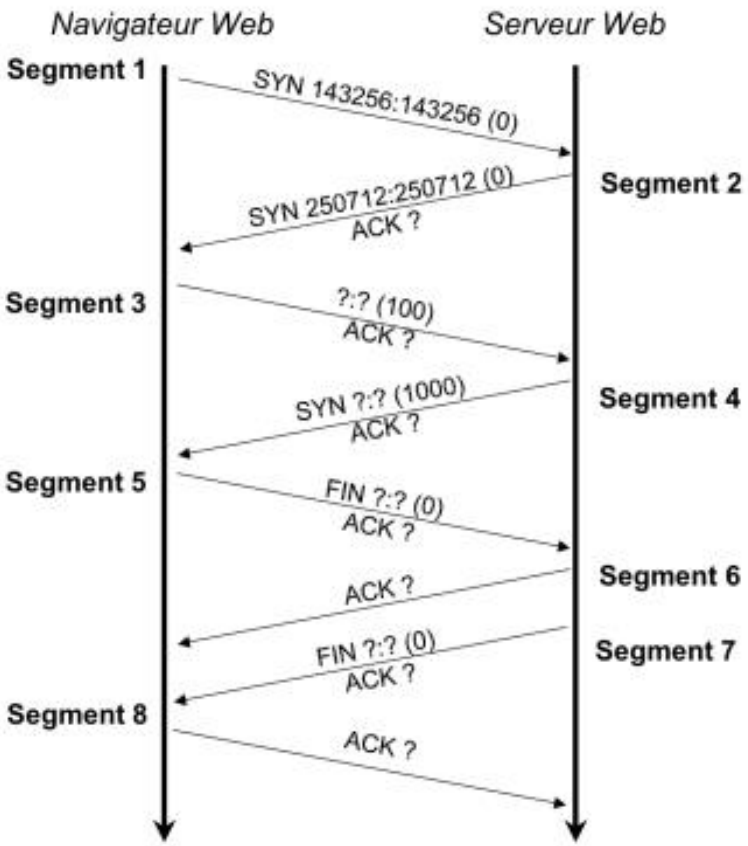
Séquence émotion et acquittement

Comment TCP s'assure que les données sont bien arrivées ? Grâce à des **numéros de séquence** ! Lorsqu'une connexion TCP est initialisée, un nombre est généré : l'ISN (cela peut être un zéro ou un nombre aléatoire suivant les systèmes). Quand des données sont envoyées, ce numéro de séquence est augmenté d'autant d'octets de données qui sont envoyés.

Fiche Td n° :04

Exercice 1 :

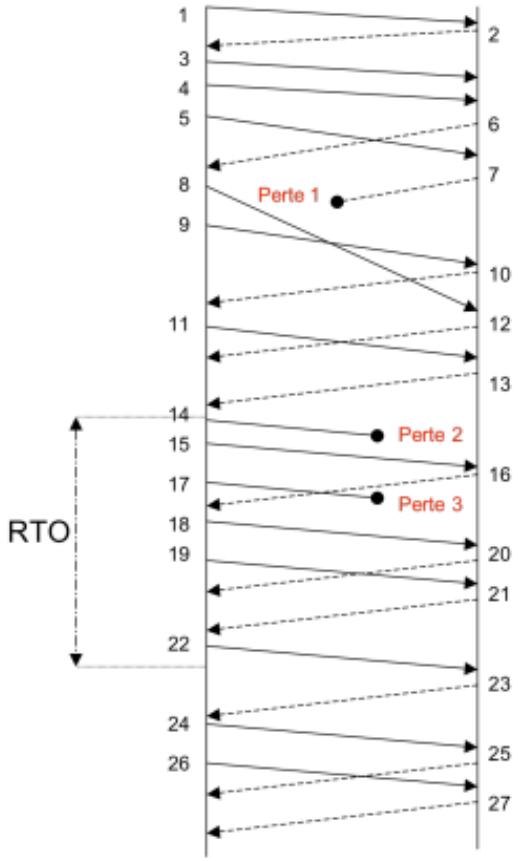
L'échange TCP de la figure ci-dessus correspond au transfert d'une page WEB entre un navigateur WEB et un serveur WEB. On fait l'hypothèse que la requête à la page WEB fait 100 octets et que la page WEB retournée fait 1000 octets. Il n'y a pas d'erreurs de transmission. Pour chaque segment de données, différentes informations apparaissent. D'une part la présence d'un ou plusieurs des différents indicateurs comme SYN, FIN, ACK. Par ailleurs sur la première ligne deux chiffres sont portés. Le premier chiffre correspond au numéro de séquence du premier octet du segment, le deuxième chiffre correspond au numéro du premier octet du prochain segment à envoyer. Le chiffre entre parenthèses correspond au nombre total d'octets transmis dans le segment. Si le segment est porteur d'un acquittement positif, l'indicateur ACK est mentionné et a coté de lui doit figurer la valeur du champ acquittement du segment TCP.



Complétez les numéros de séquence et les numéros d'acquittement qui manquent sur la figure (qui apparaissent sous forme de point d'interrogation). Indiquez à quoi correspondent les différents segments numérotés de 1 à 8.

Exercice 2 :

Considérons le transfert d'un fichier de taille illimité sur une connexion TCP classique. La taille maximale des données d'un segment (MMS) est 200 octets. La transmission démarre, nous représentons dans la figure 1 le chronogramme obtenu :



#	Num Seq	Num Ack	URG	ACK	PSH	RST	SYN	FIN	Taille Données
1	3999	-					X		0
2	122	4000		X			X		0
3	4000	123		X					0
4	4000	123							200

1-Complétez dans le tableau ci-dessus les paramètres associés à chaque segment (Numéros de séquence et d'acquittement, flags et Taille des données)

2- Qu'implique la première perte au niveau des acquittements suivants ?

3- Comment est détectée la première perte d'un segment de données et comment est elle réparée ?

Couches Applicatives

6

Les couches 7, 6 et 5 du modèle OSI correspondent à une seule couche applicative dans le modèle TCP/IP, voilà pourquoi nous allons les étudier dans ce chapitre.

Nous allons présenter les trois dernières couches du modèle OSI, à savoir, de bas en haut : la couche de session (5), la couche de présentation (6) et la couche applicative (7).

I.La couche session

La couche 5 du modèle OSI a la responsabilité de l'ouverture, de la fermeture et de la gestion des sessions entre les applications. Les deux services principaux offerts par cette couche sont la gestion des sessions (ouverture, fermeture, restauration) et la gestion des permissions (quelle application peut faire quoi).

Les protocoles de la couche 5, tels que X.225, peuvent déterminer la direction de la communication. Il existe deux types de communication :

- *Half Duplex* (HDX) : système de communication permettant l'échange par tour. Si deux entités A et B sont membres d'un réseau fondé sur ce système de communication, elles ne peuvent pas échanger de données au même moment. Chacune doit attendre son tour !
- *Full Duplex* (FDX) : l'exact contraire du HDX. A et B peuvent communiquer simultanément sans que cela ne pose problème.

II.La couche Présentation

la couche 6 s'occupe de tout ce qui a trait à la présentation. En d'autres termes, elle offre des services permettant de convertir des données d'un système d'encodage à un autre (de l'EBCDIC vers l'ASCII, par exemple), de compresser des fichiers, de les crypter, etc. Lorsque vous utilisez Winzip, un logiciel de compression, vous utilisez un service de la couche 6 du modèle OSI. Par conséquent, c'est dans cette couche que nous trouvons des protocoles tels que LPP (*Lightweight Presentation Protocol*), NDR (*Network Data Representation*) ou encore NCP (*NetWare Core Protocol*).

III.La couche Application

Cette couche n'a pas de rôle défini. En fait, il s'agit seulement d'une couche-interface qui sert de point de contact ou d'interaction entre l'utilisateur que vous êtes et les services en réseaux. Par exemple, le navigateur web est une application qui nous permet d'être en contact avec un service offert par le protocole HTTP (*HyperText Transfer Protocol*). Quand nous utilisons notre messagerie, nous sommes en interaction avec la couche applicative.

La couche applicative héberge principalement :

- Des API (*Application Programming Interface* : « interface de programmation d'application ») : une API est grosso-modo un ensemble de fonctions permettant à un programme externe d'interagir avec un programme interne pour ne pas exposer le code source.
- Des services : plusieurs services en réseaux tels que la navigation Internet, la messagerie, la résolution de noms de domaine sont concentrés dans cette couche.

Cette couche regorge de protocoles tels que :

- SMTP
- HTTP ;
- FTP
- DHCP ;
- DNS ;

IV. les protocoles de la couche application

IV.1 .SMTP : le protocole de transmission de mail

Le service de messagerie (instantanée ou non) est sans doute le plus utilisé de nos jours quotidiennement. Enfin, en dehors de Facebook. Chacun de nous est amené à consulter ses mails régulièrement, voire à en rédiger. La messagerie électronique nous a facilité la tâche en réduisant le temps de rédaction et d'acheminement d'un courrier. Ça vous dirait de voir comment ça se passe dans les coulisses ? Nous allons donc étudier le fonctionnement d'un protocole nous permettant d'envoyer un message électronique.

Présentation rapide de SMTP

SMTP (*Simple Mail Transfer Protocol* : « protocole simple de transfert de courrier ») a été créé dans les années 1970, aux débuts d'Internet. Comme tout bon protocole qui se veut être un standard, il a fallu qu'il soit spécifié par une requête de commentaires (RFC). C'est donc en 1982 qu'il est spécifié par la RFC 821.

SMTP a commencé à être massivement utilisé au début des années 1980. Il sert principalement à envoyer des mails. Comme son nom l'indique, il s'agit d'un protocole de transmission et non de réception. Cependant, les serveurs de messagerie utilisent SMTP pour faire les deux, c'est-à-dire la transmission **et** la réception, cette dernière n'étant en fait qu'une transmission. Elle est similaire à un envoi d'une lettre :

- Vous écrivez une lettre (physique) à un ami à Oran
- La lettre arrive à la poste centrale de Oran.
- La poste centrale va à son tour transmettre la lettre au domicile de votre Ami.

Vous avez confié la lettre à la poste, qui l'a envoyée au destinataire. Pour vous et pour la poste, il s'agit d'une transmission ; pour votre ami, d'une réception. La réception n'est donc qu'une autre transmission.

Ainsi, les serveurs de messagerie utilisent SMTP pour la transmission et la réception, tandis que les clients de messagerie utilisent SMTP pour l'envoi et un autre protocole (POP ou IMAP) pour la réception. Nous allons étudier ces protocoles de retrait dans la sous-partie suivante.

SMTP est un protocole de transfert. Or pour transférer, il faut un autre protocole de transmission.

Les protocoles qui assurent la transmission se trouvent dans la couche de transport. Par conséquent, un protocole de transfert de la couche application (comme SMTP) ne peut se passer d'un protocole de transmission de la couche transport (UDP ou TCP).

Nous allons voir les étapes par lesquelles passe un courriel avant d'atteindre son destinataire. Comme il est de coutume dans ce tutoriel, nous allons commencer par une analogie qui ne doit pas vous être inconnue. Mohamed (encore lui) habite à Saida. Il veut écrire une lettre à Kamel, qui habite Oran. Dans notre scénario, la procédure de transmission/réception de la lettre se fera ainsi :

- Mohamed écrit la lettre.
- Le facteur vient la chercher.

- La lettre arrive à la poste locale.
- La poste envoie la lettre à Oran.
- Elle arrive à la poste locale de Oran.
- Un facteur est chargé de la porter au domicile d'Kamel.
- Kamel reçoit la lettre.

Hormis l'étape 1 (écriture de la lettre) et l'étape 7 (réception), la lettre est passée entre les mains du facteur, de la poste locale, de la poste distante (celle de Oran) et d'un autre facteur. Soit quatre étapes.

Vous pouvez constater qu'il y a deux facteurs dans notre exemple : le premier peut être qualifié de « facteur de transmission », car il est impliqué dans l'étape de transmission de notre lettre ; le second, de « facteur de réception », car il est impliqué dans la transmission/réception de notre lettre.

Voici un schéma illustrant ces étapes :

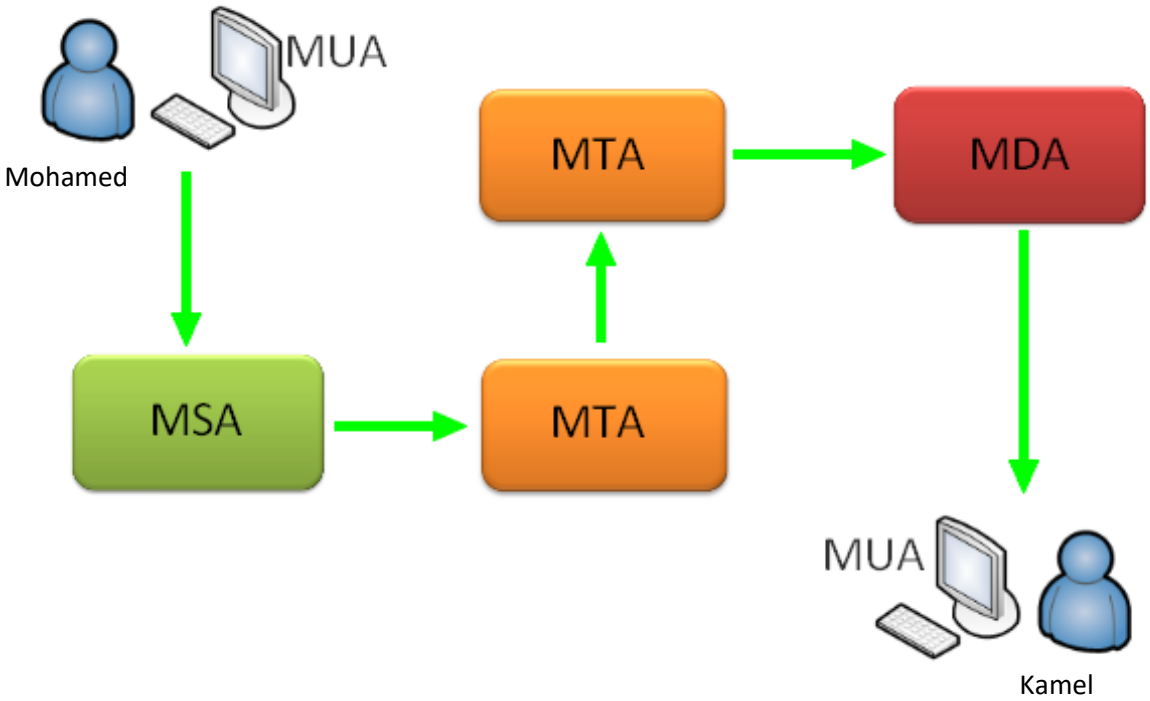


Fig VI.1 Fonctionnement du protocole SMTP

IV.2 HTTP (Le service web)

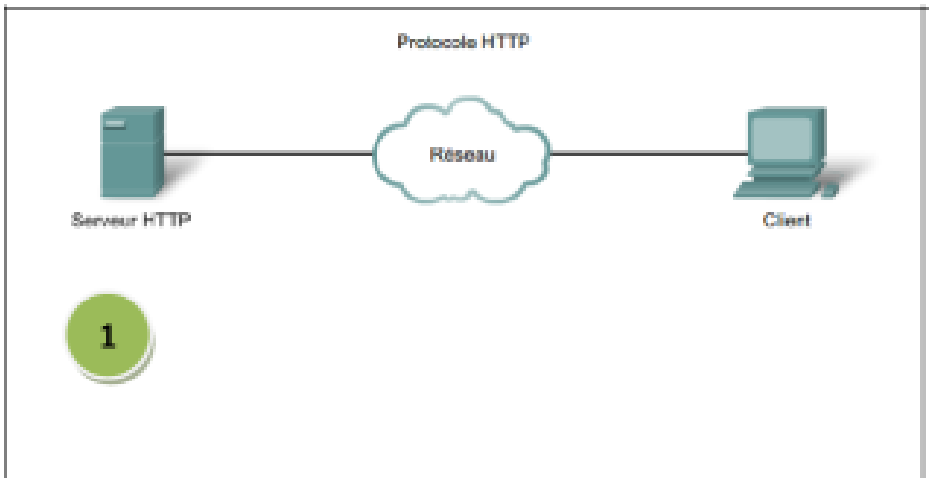
Le protocole HTTP est utilisé à travers le Web pour le transfert des données et constitue l'un des protocoles d'application les plus utilisés.

C'est un protocole de requête/réponse. Lorsqu'un client (généralement un navigateur Web) envoie une requête à un serveur, le protocole HTTP définit les types de messages que le client utilise pour demander la page Web, ainsi que les types de messages que le serveur utilise pour répondre. Les trois types de messages courants sont GET, POST et PUT.

- GET est une requête cliente pour obtenir des données. Un navigateur Web envoie le message GET pour demander des pages à un serveur Web.
- POST sert à envoyer des messages qui téléchargent des données vers le serveur Web. Par exemple, lorsque l'utilisateur entre des données dans un formulaire incorporé à une page Web, la requête POST comprend les données dans le message envoyé au serveur.
- PUT télécharge des ressources ou du contenu vers le serveur Web.

Bien qu'il soit remarquablement flexible, le protocole HTTP n'est pas un protocole sécurisé. Les messages POST téléchargent des informations vers le serveur dans un format de texte clair pouvant être intercepté et lu. De même, les réponses du serveur (généralement, des pages HTML) ne sont pas chiffrées.

Pour une communication sécurisée via Internet, le protocole HTTPS (HTTP Secure) est utilisé lors de l'accès aux informations du serveur Web ou de leur publication. Le protocole HTTPS peut procéder à l'authentification et au chiffrement pour sécuriser les données pendant qu'elles circulent entre le client et le serveur. Le protocole HTTPS spécifie des règles supplémentaires de transmission de données entre la couche application et la couche transport



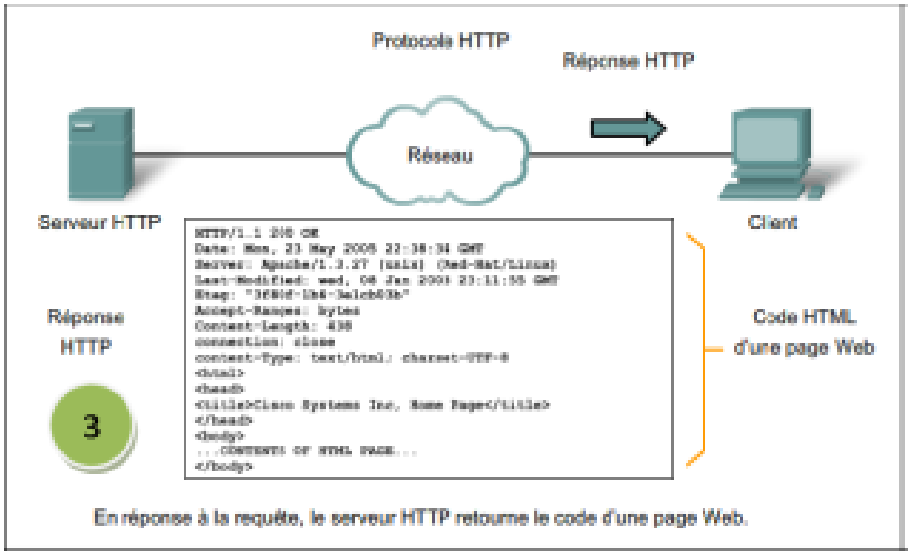


Fig VI.2 protocole http : fonctionnement[2]

[2] STI2D - Découverte des réseaux informatiques - Service web : protocole http (silanus.fr)

IV.3.FTP (Le service de transfert de fichier)

Le protocole FTP (File Transfer Protocol) a été développé pour permettre le transfert de fichiers entre un client et un serveur. Un client FTP est une application s'exécutant sur un ordinateur et utilisée pour extraire des fichiers d'un serveur exécutant le démon FTP.

Pour transférer les fichiers correctement, le protocole FTP nécessite que deux connexions soient établies entre le client et le serveur : une connexion pour les commandes et les réponses et une autre pour le transfert même des fichiers.

Le client établit la première connexion au serveur sur le port TCP 21. Cette connexion est utilisée pour le trafic de contrôle et se compose de commandes clientes et de réponses serveur.

Le client établit la seconde connexion au serveur via le port TCP 20. Cette connexion est destinée au transfert même des fichiers et est établie à chaque transfert de fichiers.

Le transfert de fichiers peut s'effectuer dans l'une des deux directions. Le client peut télécharger un fichier à partir du serveur ou en direction du serveur

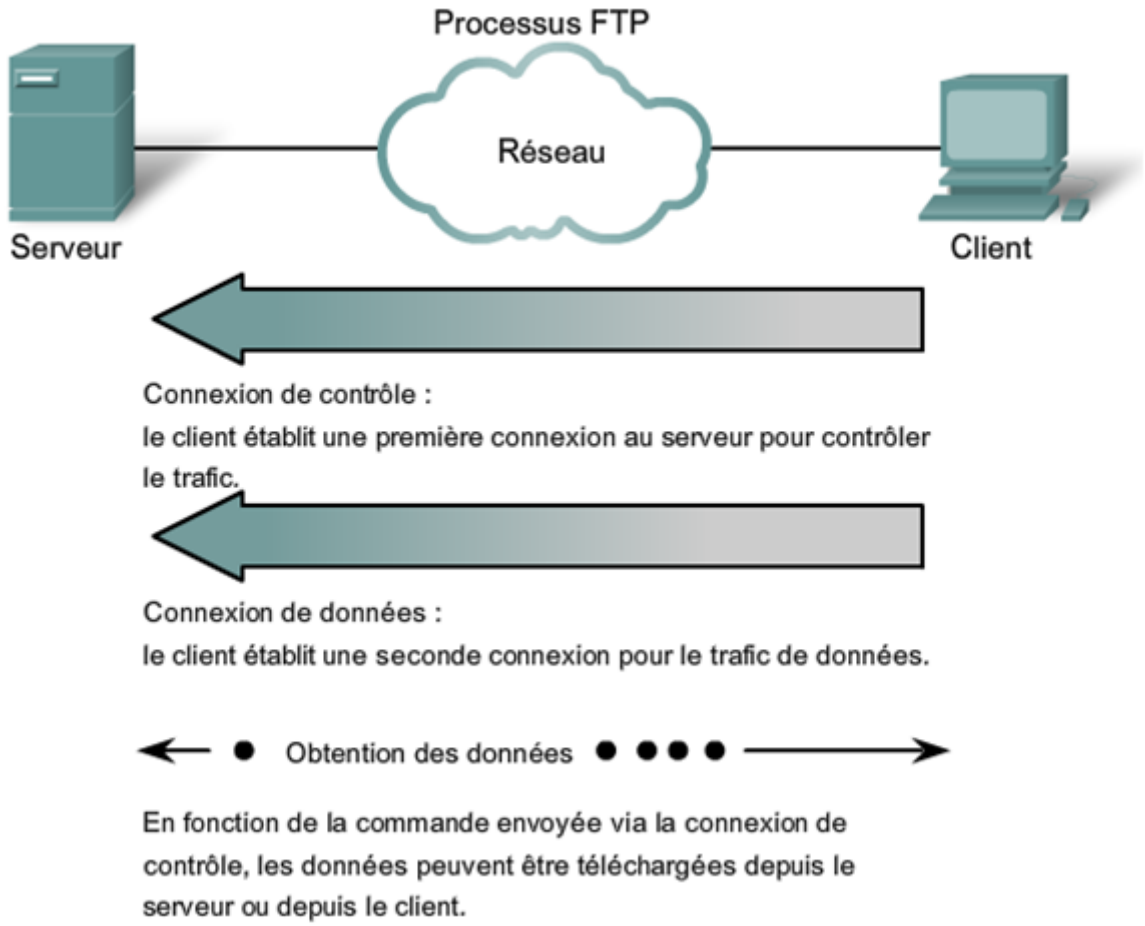


Fig VI.3 processus FTP

IV.4. DHCP : Dynamic Host Configuration Protocol

Le protocole de configuration dynamique DHCP fournit un cadre pour transmettre des informations de configuration à des machines d'un réseau TCP/IP : il leur communique leurs paramètres de configuration, en particulier leurs adresses IP.

Principe de fonctionnement

Le service DHCP garantit l'unicité d'une adresse IP dans le réseau. C'est une aide précieuse pour l'administrateur du réseau puisqu'il permet de supprimer la configuration manuelle des machines du réseau (celle-ci reste toujours possible et doit être compatible avec l'allocation dynamique). En outre, il évite les erreurs liées à cette configuration manuelle. Il sera très utile pour le déploiement d'un grand parc de machines qui possèdent les mêmes caractéristiques et dont la seule différence est la configuration réseau.

Le serveur DHCP dispose d'une plage d'adresses IP à attribuer. Quand un client en demande une pour la première fois, le serveur lui en fournit une qu'il n'a pas encore utilisée. S'il a déjà distribué toutes ses adresses IP, il réutilise celle d'un client qui n'est plus connecté au réseau. Quand un client a déjà obtenu dynamiquement une adresse IP lors d'une connexion antérieure, le serveur lui fournit a priori la même adresse, si c'est possible. La réattribution d'une adresse ne s'avère nécessaire qu'en cas de pénurie. En effet, DHCP peut s'utiliser avec un nombre de clients supérieur au nombre d'adresses IP disponibles. Cette méthode ne convient pas pour définir l'adressage des machines ayant un rôle de serveurs, qui doivent avoir une adresse fixe. On utilise donc également l'attribution fixe d'une adresse IP pour les machines qui en ont besoin. Dans ce cas, l'adresse MAC qui identifie la machine est mise en correspondance avec une adresse IP fixe. Par ailleurs, l'attribution fixe est une façon de lutter contre les intrusions dans le réseau

Fig VI.4 DHCP

7 Travaux pratiques

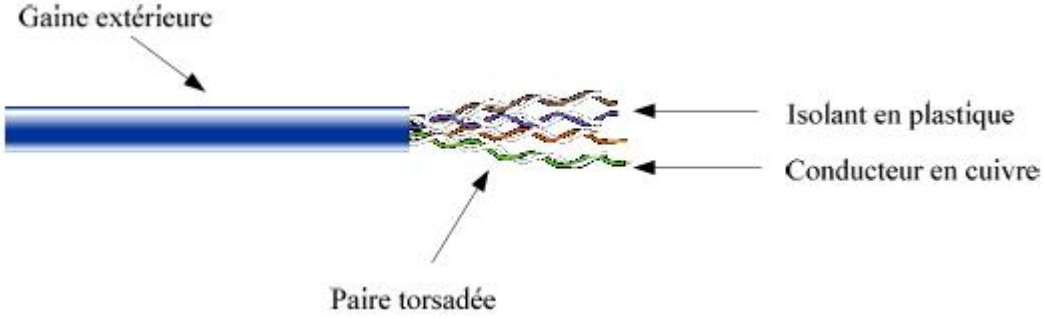
TP-01
Réalisation et tests de câbles RJ45 ou paire torsadée (Croisé, Droit)

Rappels :

1. Médias de cuivres

1.1. Le câble à paires torsadées non blindées

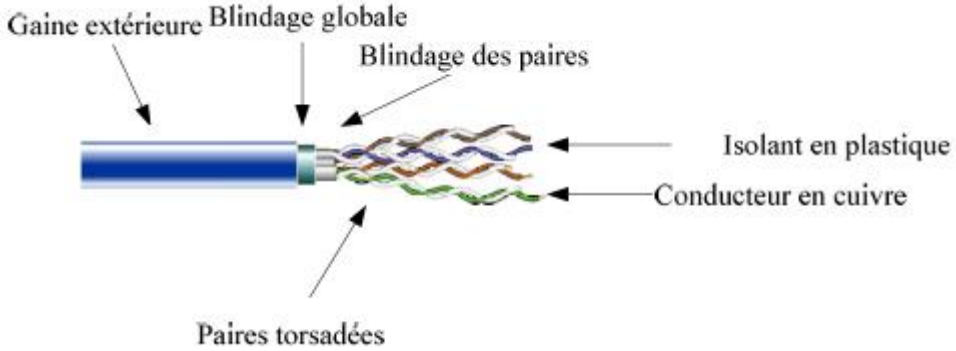
Le câble UTP (Unshielded Twisted Pair) est composé de 4 paires de fils torsadées 2 à 2, chacune de ses paires étant isolées des autres. Les paires torsadées limitent la dégradation du signal causée par les perturbations électromagnétique. Lorsque le câble à paires torsadées non blindées est utilisé comme média de réseau, il comporte quatre paires de fils de cuivre.



Câble UTP

1.2. Le câble à paires torsadées blindées

Le câble à paires torsadées et blindées, ou STP(ShieldedTwisted Pair), ajoute aux spécifications de l'UTP une méthode de blindage, des câbles à paires torsadées blindées offrent une meilleur résistance à l'interférence électromagnétique, ainsi qu'à l'interférence de radiofréquences.



Câble STP

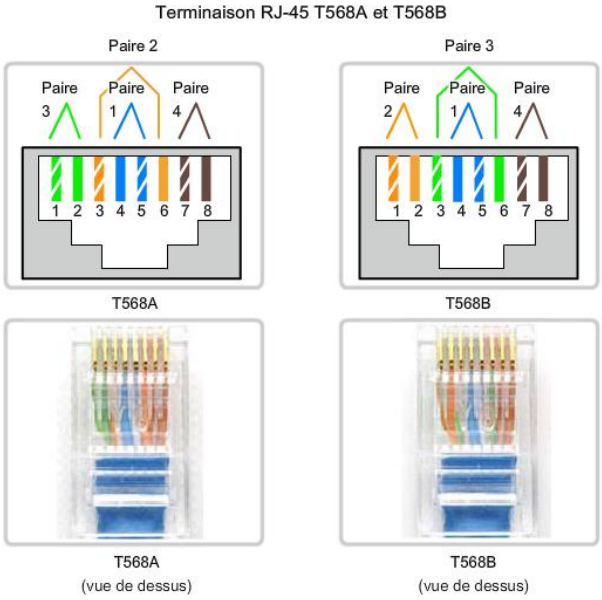
1.3. Le Les connecteurs RJ-45

Il s'agit d'un composant réseau passif, car il sert uniquement au passage du courant entre les quatre paires torsadées de câbles torsadés de catégorie 5 et les broches du connecteur RJ-45.
Les connecteurs RJ-45 s'insèrent dans les réceptacles ou les prises RJ-45. Les prises mâles RJ-45 ont huit connecteurs qui s'enclenchent avec la prise RJ-45. De l'autre côté de la prise RJ-45, il y a un bloc où les fils sont séparés et fixés dans des fentes avec l'aide d'un outil semblable à une fourche. Ceci offre un passage de courant en cuivre aux bits.

Prise RJ-45 et connecteur RJ-45

2. Etablissement des connexions de réseau local

Les connexions de câblage UTP sont spécifiées par l'eIA/TIA (Electronics Industry Alliance/Telecommunications Industry Association). Le connecteur RJ-45 est le composant mâle serti à l'extrémité du câble. Vues de face, les broches sont numérotées de 8 à 1. Vues du dessus avec la porte d'ouverture face à vous, les broches sont numérotées de 1 à 8, de gauche à droite. Il est important de se souvenir de cette orientation lorsque vous identifiez un câble.



2.1. Types d'interfaces

Dans un réseau local Ethernet, les périphériques utilisent un des deux types d'interfaces UTP - MDI ou MDIX.
L'interface MDI (Media-Dependent Interface) utilise le brochage Ethernet normal. Les broches 1 et 2 sont utilisées pour la transmission, les broches 3 et 6 pour la réception. Les périphériques comme les ordinateurs, les serveurs ou les routeurs ont des connexions MDI.
Les périphériques qui fournissent la connectivité du réseau local (généralement des concentrateurs ou des commutateurs) utilisent habituellement des connexions à interface croisée dépendante du support (MDIX, Media-Dependent Interface, Crossover). Les câbles MDIX permutent les paires de transmission en interne. Cette permutation permet de connecter les périphériques finaux au concentrateur ou au commutateur à l'aide d'un câble droit.

Lorsque vous connectez différents types de périphériques, utilisez généralement un câble droit. Et lorsque vous connectez le même type de périphérique, utilisez un câble croisé.

2.2. Câbles UTP droits

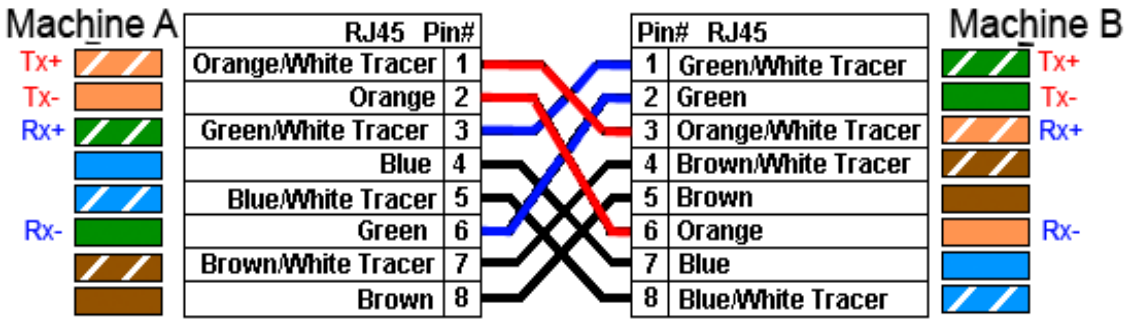
Un câble droit possède des connecteurs à chaque extrémité, qui sont terminés à l'identique conformément à la norme T568A ou à la norme T568B.

Câble droit

L'identification de la norme de câble utilisée vous permet de déterminer si vous utilisez le câble adapté à la tâche. Plus important, il est de bon ton d'utiliser les mêmes codes de couleur sur l'ensemble du réseau local pour assurer une cohérence tout au long de la documentation.
Utilisez des câbles droits pour les connexions suivantes :
Commutateur à port Ethernet d'un routeur
Ordinateur à commutateur
Routeur à commutateur

2.3. Câbles UTP croisé

Pour deux périphériques qui communiquent directement par le biais d'un câble, le terminal de transmission d'un des périphériques doit être connecté au terminal de réception de l'autre périphérique.



Câble Croisé

Le câble doit être terminé afin que la broche de transmission (Tx), qui utilise le signal provenant du périphérique A à une extrémité, soit câblée à la broche de réception (Rx) sur le périphérique B. De même, la broche de transmission (Tx) du périphérique B doit être connectée à la broche de réception (Rx) du périphérique A. Si la broche de transmission d'un périphérique porte le numéro 1 et que la broche de réception porte le numéro 2, le câble connecte la broche 1 à une extrémité avec la broche 2 à l'autre extrémité. Ces connexions de broche « croisées » donnent son nom à ce type de câble, appelé câble croisé.

Pour obtenir ce type de connexion avec un câble UTP, une extrémité doit être terminée selon le brochage de la norme EIA/TIA T568A et l'autre extrémité terminée avec le brochage de la norme T568B.

Pour résumer, les câbles de croisement connectent directement les périphériques suivants sur un réseau local :

Commutateur à commutateur

Routeur à connexion du port Ethernet d'un routeur

Ordinateur à ordinateur

Ordinateur à port Ethernet d'un routeur

TP-02

Création et configuration un réseau local

Objectif : Découvrir la configuration nécessaire pour partager un dossier entre des stations dans un réseau local.

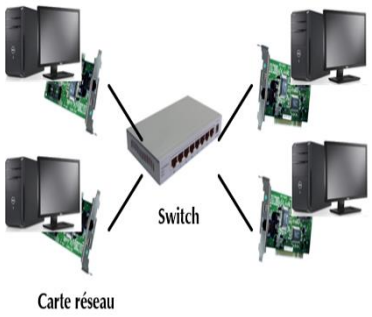
1. Introduction :

Un réseau LAN (Local Area Network) est un réseau permettant l'interconnexion d'ordinateurs dans un périmètre géographique restreins (cybercafé). Le présent TP décrit les étapes à suivre pour partager un ou plusieurs dossiers entre des ordinateurs interconnecté avec un switch (formant un réseau LAN).

2. Câblage et configuration des ordinateurs :

2.1 Réalisation d'une topologie en étoile :

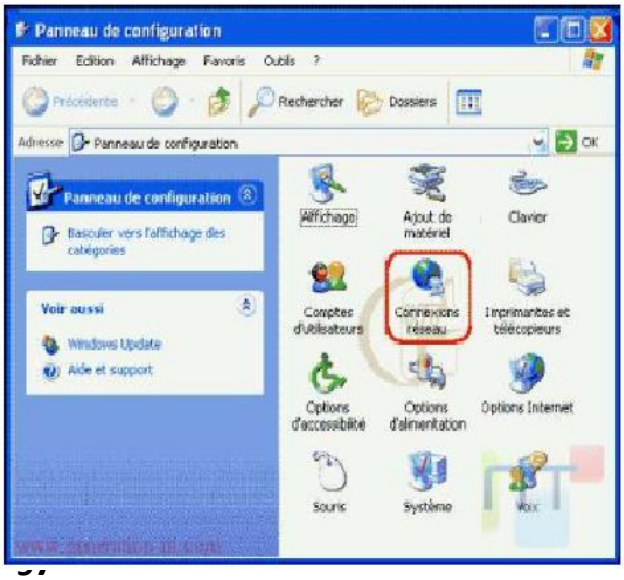
Matériel nécessaire : Pour créer un réseau local, il faut des ordinateurs équipés chacun d'une carte réseau Ethernet. Afin d'interconnecté les ordinateurs entre eux suivant une topologie en étoile, nous aurons besoin d'un équipement d'interconnexion (Switch ou hub).



Réalisation : Muni des câbles Ethernets, relier les cartes réseaux aux ports du switch. Une fois que tout le matériel est branché, il ne reste plus qu'à configurer la carte.

2.2 Configuration des adresses IP :

Cliquez sur "**Démarrer**", puis "**Panneau de Configuration**".

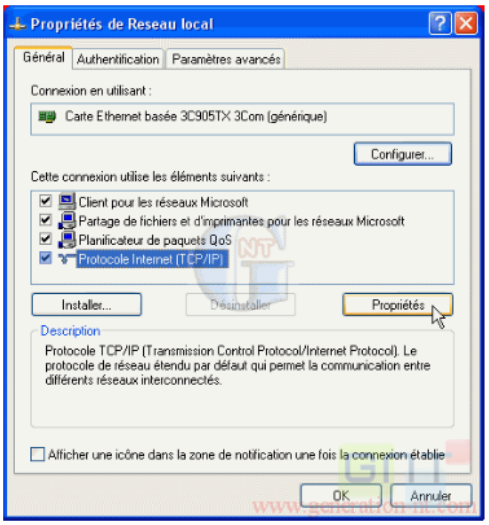


Si vous étiez en "**Affichage classique**", vous devez avoir la figure ci-dessus, cliquez alors sur "**Connexions réseau**"

Maintenant, quel que soit la voie choisie, vous devez obtenir ceci :

Vous devez obtenir une fenêtre qui ressemble à celle présentée ci-dessus. Nous pouvons y voir une connexion à Internet et une connexion au réseau local "Réseau Local". Cette connexion doit être activée, elle l'est par défaut. Si ce n'est pas le cas, réinstallez les drivers de votre carte réseau.

Cliquez ensuite avec le bouton droit de la souris sur l'icône "**Réseau local**", qui correspond à votre carte Ethernet, et choisissez "**Propriétés**".



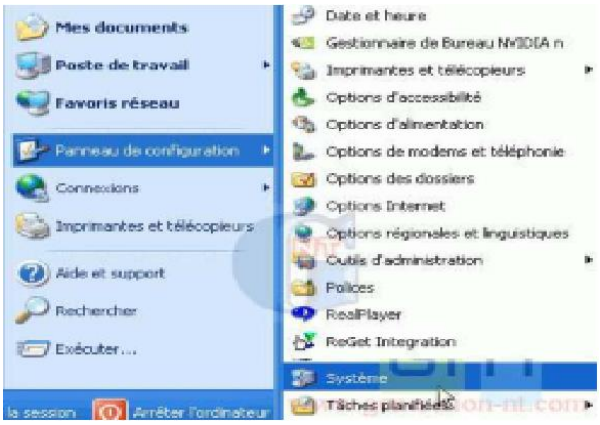
Sélectionnez "Utiliser l'adresse IP suivante :"
et tapez : Adresse IP : 192.168.0.1
Masque de sous-réseau : 255.255.255.0 puis validez en cliquant sur OK.

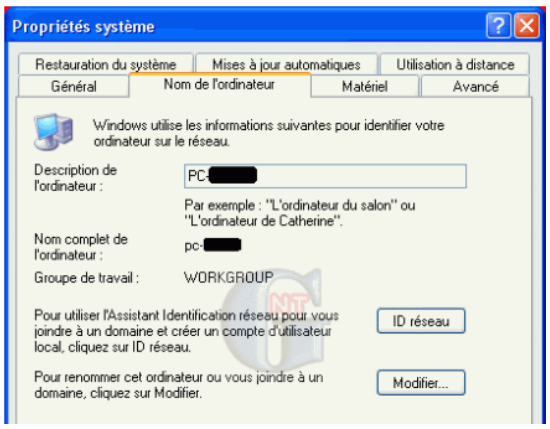
Répétez la même opération sur tous les autres ordinateurs du réseau en changeant l'adresse IP, par exemple 192.168.0.2, puis 192.168.0.3 puis...mais en conservant le même masque de sous-réseau.
Ensuite cliquez sur la case Avancé… puis rendez-vous sur l'onglet WINS, cochez la case « Activer
NetBIOS avec TCP/IP ». Ne négligez pas cette option, c'est elle qui va vous permettre de voir vos
différentes machines dans le Voisinage Réseau.

Vous devez assigner aux ordinateurs du réseau une adresse IP différente pour chaque machine. Sur le premier ordinateur, par exemple, sélectionnez "Protocole Internet (TCP/IP)" et cliquez sur le bouton "Propriétés".

2.3 Configuration du WORKGROUP

Avant de commencer la configuration, il faut vérifier que tous les groupes de travail sont identiques sur tous les ordinateurs du réseau. Pour cela, faîtes "**Démarrer**", "**Panneau de configuration**" puis "**Système**".





Pour modifier ce dernier cliquez sur "Modifier...". Sélectionnez ensuite "Groupe de Travail". Vous pouvez choisir ce que vous voulez à condition qu'il soit identique sur tous les PC.

2.4 Vérification de la configuration :

Pour vérifier si les ordinateurs du réseau communiquent entre eux. Ouvrez le Menu "**Démarrer**", puis cliquez sur "**Exécuter**"

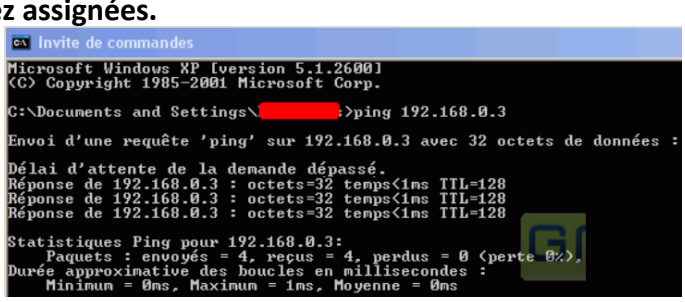
Tapez "**cmd**" puis validez avec **OK**

Chaque ordinateur connecté au réseau est caractérisé particulièrement par une adresse IP (Adresse logique) et une adresse MAC (Adresse physique). A l'aide de la commande **ipconfig /all,** veuillez compléter le tableau ci-dessous.

Adresse IP (Adresse logique) ……
Adresse MAC (Adresse physique) ……

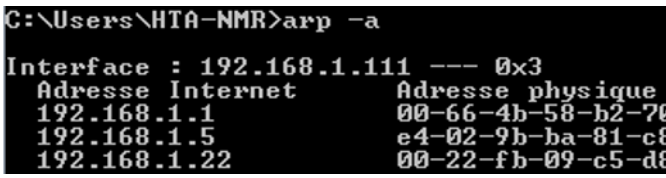
Maintenant, si l'ordinateur sur lequel vous êtes possède l'adresse IP 192.168.0.1, tapez ping 192.168.0.2 si cette adresse correspond à un autre ordinateur de votre réseau (ou 192.168.0.3 ...).
Faîtes de même pour toutes les IP que vous avez assignées.

Si vous obtenez ceci pour chaque adresse, c'est que les ordinateurs "communiquent" entre eux, donc que le réseau fonctionne bien.



Puisque les ordinateurs du réseau communiquent entre eux, il est possible de connaitre leurs adresses Mac avec le Protocol ARP.

ARP -a affiche la correspondance IP / adresse mac des ordinateurs et périphériques connectés. Les correspondances dynamiques utilisent le DHCP pour configurer l'adresse IP.



2.5 Exercices Pratiques :

Veuillez compléter le tableau ci-dessous avec les adresses IP et Mac du réseau que vous avez configuré dans le présent TP.

Nom du PC	Adresse IP	Adresse MAC

TP-03

Création et configuration d'un réseau local

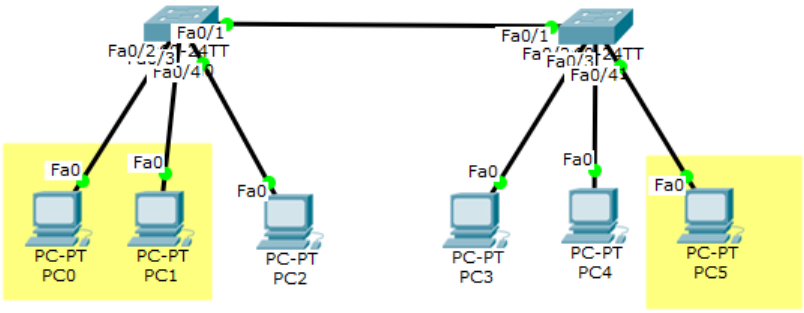
Objectif : Découvrir le principe de commutation de trame et l'utilité d'un routeur entre deux réseaux différents.

3. Introduction :

Le présent TP sera divisé en deux parties. La première partie est axée sur la commutation de trame par un switch avec une topologie contenant deux switches et quatre ordinateurs afin de réalisé deux réseaux, la deuxième partie consistera à relié les deux réseaux avec un routeur.

4. Manipulation :

2.1 Partie 1 :

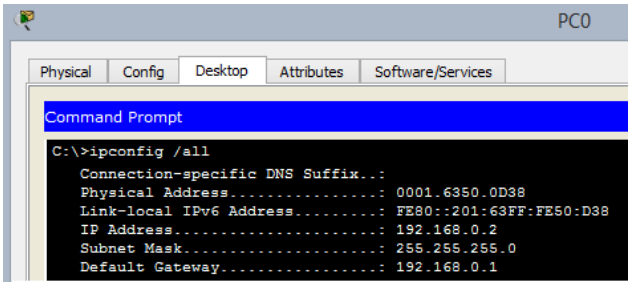


-Suivant le tableau ci-dessous réalisé la topologie et la configuration des PCs

Périphériques	Adresse IP	Masque	Gateway	Port switch
PC0	192.168.0.2	255.255.255.0	192.168.0.1	Swi 1 --- F0/2
PC1	192.168.0.3	255.255.255.0	192.168.0.1	Swi 1 --- F0/3
PC2	192.168.1.2	255.255.255.0	192.168.1.1	Swi 1 --- F0/4
PC3	192.168.1.3	255.255.255.0	192.168.1.1	Swi 2 --- F0/2
PC4	192.168.1.4	255.255.255.0	192.168.1.1	Swi 2 --- F0/3
PC5	192.168.0.4	255.255.255.0	192.168.0.1	Swi 2 --- F0/4

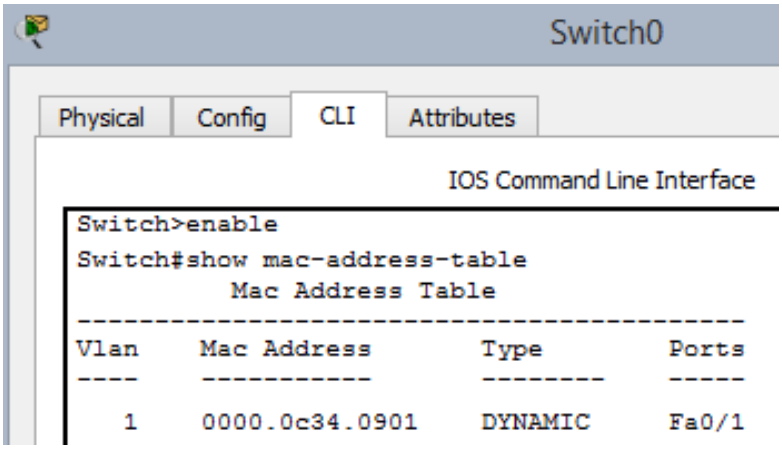
Remarque : Les deux switch sont relié par les ports F0/1 de chaque switch.

- A l'aide de la figure qui présente le résultat de la commande **ipconfig /all**, veuillez compléter le tableau ci-dessous



Périphérique	Adresse MAC	Port du switch
PC0		
PC1		
PC2		
PC3		
PC4		
PC5		

- Exécuté la commande **show mac-address-table** dans les deux switchs



Remarque : le résultat de cette commande n'affiche qu'une seul ligne.

- A partir du PC 0 et du PC 2 vérifier les liaisons entre les PCs avec la commande ping et cocher la bonne réponse.

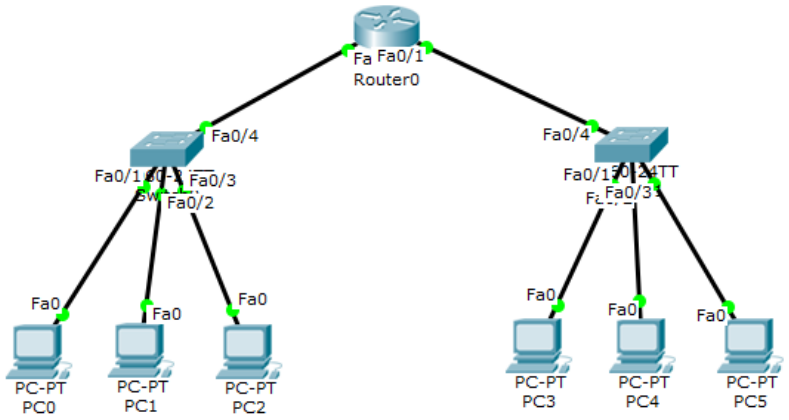
Le ping à partir du PC0 vers PC1 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC2 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC3 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC4 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC5 a-t-il aboutie oui non
Le ping à partir du PC2 vers PC0 a-t-il aboutie oui non
Le ping à partir du PC2 vers PC1 a-t-il aboutie oui non
Le ping à partir du PC2 vers PC3 a-t-il aboutie oui non
Le ping à partir du PC2 vers PC4 a-t-il aboutie oui non
Le ping à partir du PC2 vers PC5 a-t-il aboutie oui non

- Donner une explication brève aux ping qui n'ont pas pu aboutir :
- Retaper la commande **show mac-address-table** dans les deux switchs et complété le tableau ci-dessous.

Switch 1		Switch 2	
Ports	Adresse mac	Ports	Adresse mac

2.2 Partie 2 :

Complété la topologie précédente avec le raccordement du routeur aux deux switch et configurer les interfaces du routeur avec les adresses IP adéquates.



- A partir du PC 0 et du PC 2 vérifier les liaisons entre les PCs avec la commande ping et cocher la bonne réponse.

  Le ping à partir du PC0 vers PC1 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC2 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC3 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC4 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC5 a-t-il aboutie oui non
  Le ping à partir du PC2 vers PC0 a-t-il aboutie oui non
  Le ping à partir du PC2 vers PC1 a-t-il aboutie oui non
  Le ping à partir du PC2 vers PC3 a-t-il aboutie oui non
  Le ping à partir du PC2 vers PC4 a-t-il aboutie oui non
  Le ping à partir du PC2 vers PC5 a-t-il aboutie oui non

- Que constater vous ?

  .....

- La commande **tracert** permet d'afficher le chemin qu'un paquet va prendre pour aller de la machine source a la machine de destination. Veuillez exécuter cette commande à partir du PC0 vers le PC1 et noté le chemin pris par le paquet.

TP-04 :

Segmentation d'un réseau en Vlan

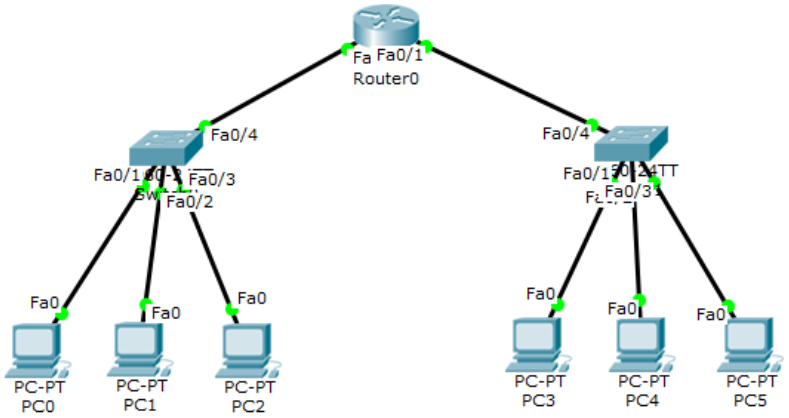
Objectif : Découvrir la configuration de base d'un commutateur et créer des réseaux locaux virtuel (Vlan-Virtual LAN).

5. Introduction :

Le présent TP sera divisé en trois parties. La première partie est une réalisation d'une topologie incluant deux commutateurs et un routeur, la deuxième partie consistera à remplacer les deux commutateurs avec un seul en configurant dans ce dernier deux vlan et la dernière partie traitera la configuration de deux interfaces virtuelle dans le routeur.

6. Manipulation :

2.1 Partie 1 :



- Suivant le tableau ci-dessous réalisé la topologie et la configuration des PCs et routeur

Périphériques	Adresse IP	Masque	Gateway	Port switch
PC0	192.168.0.2	255.255.255.0	192.168.0.1	Swi 1 --- F0/2
PC1	192.168.0.3	255.255.255.0	192.168.0.1	Swi 1 --- F0/3
PC2	192.168.0.4	255.255.255.0	192.168.0.1	Swi 1 --- F0/4
PC3	192.168.1.2	255.255.255.0	192.168.1.1	Swi 2 --- F0/2
PC4	192.168.1.3	255.255.255.0	192.168.1.1	Swi 2 --- F0/3
PC5	192.168.1.4	255.255.255.0	192.168.1.1	Swi 2 --- F0/4
Routeur F0/0	192.168.0.1	255.255.255.0	///	Swi 1 --- F0/1
Routeur F0/1	192.168.1.1	255.255.255.0	///	Swi 2 --- F0/1

Remarque : Les deux switch sont relié au routeur par les ports F0/1 de chaque switch.

Vérification de la configuration

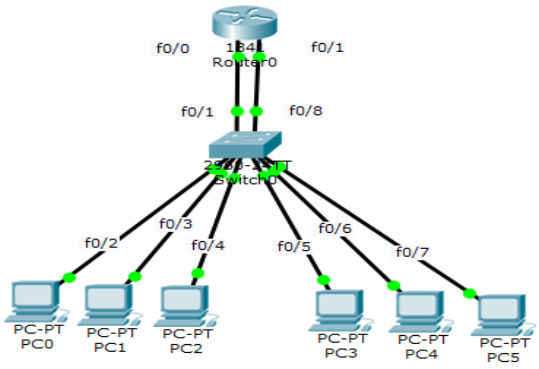
- A partir du PC 0 et du vérifier les liaisons entre les PCs avec la commande ping et cocher la bonne réponse.

Le ping à partir du PC0 vers PC1 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC2 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC3 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC4 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC5 a-t-il aboutie oui non

2.2 Partie 2 :

Dans cette partie nous allons supprimer un commutateur et configurer le deuxième avec deux VLAN. Veuillez à bien suivre la connectique des ports suivant le tableau d'affectation des ports ci-dessous :

Périphériques	Interfaces	Port switch
PC0	F0/0	Swi 1 --- F0/2
PC1	F0/0	Swi 1 --- F0/3
PC2	F0/0	Swi 1 --- F0/4
PC3	F0/0	Swi 1 --- F0/5
PC4	F0/0	Swi 1 --- F0/6
PC5	F0/0	Swi 1 --- F0/7
Routeur	F0/0	Swi 1 --- F0/1
Routeur	F0/1	Swi 1 --- F0/8



Configuration du Commutateur

Étape 1 : Création des réseaux locaux virtuels sur le commutateur

En mode de configuration globale créer deux réseaux locaux virtuels au commutateur. Le vlan 11 sera le premier avec le nom de AAA et le deuxième vlan sera 22 avec le nom BBB.

Switch>enable
Switch#configure terminal
Switch (config)#vlan 11
Switch (config-vlan)#name AAA
Switch (config-vlan)#exit
Switch (config)#vlan 22
Switch (config-vlan)#name BBB
Switch (config-vlan)#exit

Étape 2 : Affectation des ports du commutateur aux réseaux locaux virtuels

Reportez-vous à la table d'affectation des ports. Les ports sont affectés aux réseaux locaux virtuels à l'aide de la commande switchport access vlan id-vlan (11 ou 22).

Switch (config)#interface **fastEthernet0/1**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 11**
Switch (config-if)#interface **fastEthernet0/2**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 11**
Switch (config-if)#interface **fastEthernet0/3**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 11**

Switch (config)#interface **fastEthernet0/8**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 22**
Switch (config-if)#interface **fastEthernet0/5**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 22**
Switch (config-if)#interface **fastEthernet0/6**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 22**

Switch (config-if)#interface **fastEthernet0/4**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 11**
Switch (config-if)#end

Switch (config-if)#interface **fastEthernet0/7**
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access **vlan 22**
Switch (config-if)#end

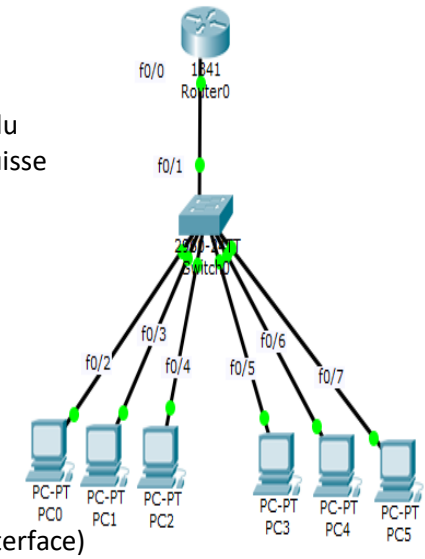
Vérification de la configuration

- A partir du PC 0 et du vérifier les liaisons entre les PCs.

Le ping à partir du PC0 vers PC1 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC2 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC3 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC4 a-t-il aboutie oui non
Le ping à partir du PC0 vers PC5 a-t-il aboutie oui non

2.3 Partie 3 :

Dans cette dernière partie on va **supprimer** un câble (**routeur F0/1** et **f0/8 commutateur**) entre le commutateur et le routeur. Nous allons créer deux interfaces virtuelle sur une seule interface physique du coté du routeur et du coté du commutateur nous allons configurer l'interface F0/1 pour quelle puisse acheminer le flux des deux vlans précédemment configurer.



Configuration du routeur

En mode de configuration globale créer deux interfaces réseaux dans le routeur. L'interface f0/0.11 acheminera les données du vlan 11 et l'interface f0/0.22 acheminera les données du vlan 22.

Router>enable
Router#conf t
Router(config)#int f0/0
Router(config-if)#no ip add (supprimer la configuration d'adresse IP de l'interface)
Router(config-if)#no shu
Router(config-if)#int f0/0.11 (création de la première interface virtuelle)
Router(config-subif)#encapsulation dot1Q 11 (choisir le protocole Dot1Q pour l'encapsulation)
Router(config-subif)#ip add 192.168.0.1 255.255.255.0
Router(config-if)#int f0/0.22
Router(config-subif)#encapsulation dot1Q 22
Router(config-subif)#ip add 192.168.1.1 255.255.255.0
Router(config-subif)#end

Configuration du commutateur

En mode de configuration globale supprimer la configuration précédente de l'interface f0/1 sur laquelle l'interface ne pouvais acheminer que les données du vlan 11 et configurer l'interface pour quelle puisse acheminer les données des deux VLANs (11 et 22).

Switch>enable
Switch#configure terminal
Switch(config)#int f0/1
Switch(config-if)#no switchport access vlan 11
Switch(config-if)#no switchport mode

Switch(config-if)#switchport mode trunk (configuration de l'interface avec le protocole Dot1Q)
Switch(config-if)#switchport trunk allowed vlan all (permettre l'acheminement de tous les vlans)
Switch(config-if)#end

Vérification de la configuration

- A partir du PC 0 et du vérifier les liaisons entre les PCs.
  Le ping à partir du PC0 vers PC1 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC2 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC3 a-t-il aboutie oui non
  Le ping à partir du PC0 vers PC4 a-t-il aboutie oui non

Le ping à partir du PC0 vers PC5 a-t-il aboutie oui non

TP-05 :

Segmentation d'un réseau en Vlan

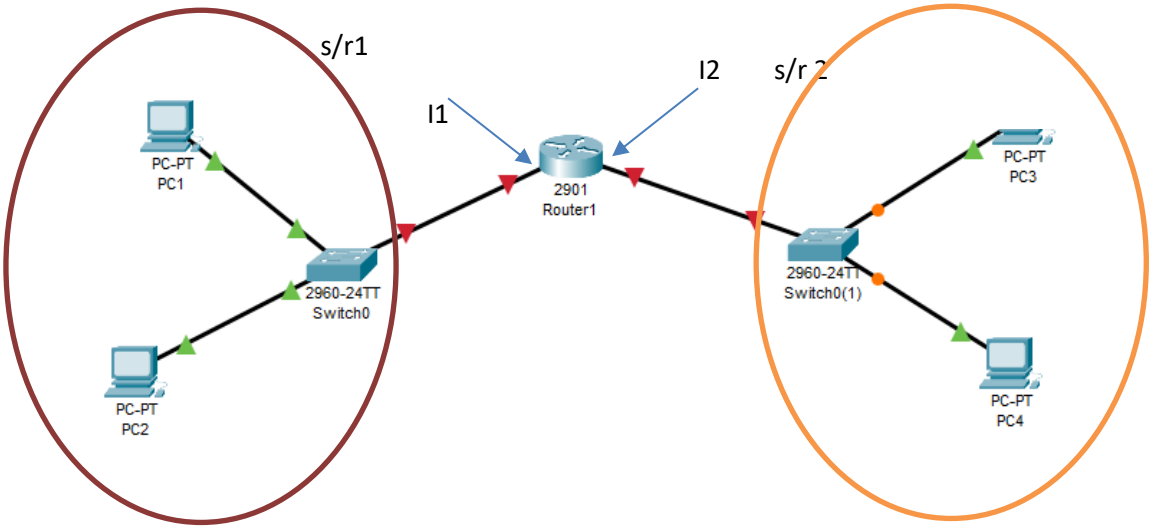
Objectif : Découvrir la configuration de base d'un routeur et configuration du routage statique et du routage dynamique.

7. Introduction :

Le présent TP consiste à configurer les différents équipements que l'on retrouve dans un réseau. Vous aurez à configurer des stations, des commutateurs, ainsi que des routeurs. L'accent sera mis sur la configuration du routage statique et du routage dynamique.

I/ interconnexion de deux sous réseaux

Réaliser la topologie suivante.



a) Adresser les pc suivant le tableau suivant :

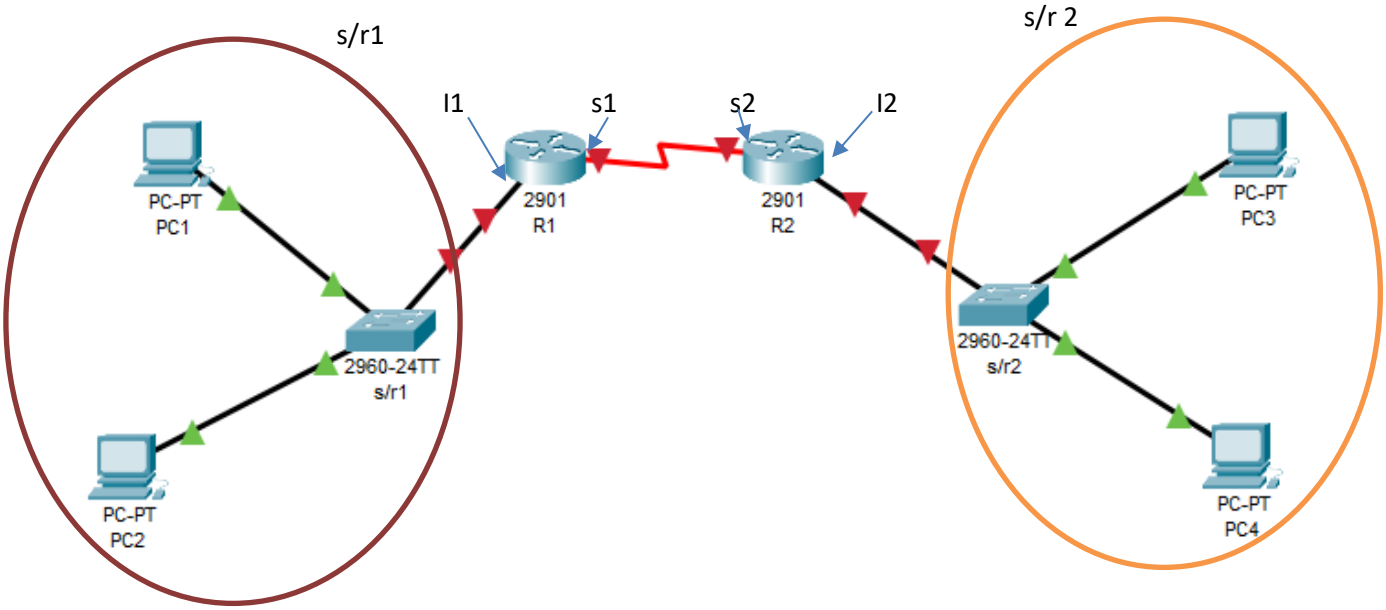
hôte	Adresse
Pc1	192.168.1.33/26
Pc2	192.688.1.34/26
Pc3	192.168.1.65/26
Pc4	192.688.1.66/26
I1	192.688.1.35/26
I2	192.688.1.67/26

b)- Détailler le contenu de la table de routage (du routeur) obtenue avec la commande : show ip route.

c)- Une station du réseau s/r1 peut-elle pinger une station du réseau s/r 2? Pourquoi ?

II/ Le routage statique

Réaliser la topologie suivante.



a) Adresser les pc suivant le tableau suivant :

hôte	Adresse
Pc1	192.168.1.33/26
Pc2	192.688.1.34/26
Pc3	192.168.1.65/26
Pc4	192.688.1.66/26
I1	192.688.1.35/26
I2	192.688.1.67/26
S1 (interface série)	10.1.1.1/8
S2 (interface série)	10.1.1.2/8

- Compléter la configuration des deux routeurs.
- Une station du réseau s/r1 peut-elle pinger une station du réseau s/r 2 ? Pourquoi ?
- Utiliser la commande **Ip route** pour configurer les routes statiques.
- Détailler le contenu de la table de routage (du routeur) obtenue avec la commande : show ip route

III/ Le routage dynamique

a)- Réaliser la même topologie précédente avec les mêmes adresses.

b)- Utiliser la commande **route rip** pour indiquer a Rip sur quels réseaux on souhaite voir la diffusion des routes

c)- Détailler le contenue de la table de routage d'un des routeurs.

d)-vérifier la connectivité entre une station de s/r1 et une station de s/r2

Références Bibliographiques

- Forouzan, Behrouz A., and S. C. Fegan. "Data communication and computer networks." (2007).
- Tanenbaum, Andrew S. "Computer networks, 4-th edition." ed: Prentice Hall (2003).
- Architecture des réseaux, Danièle DROMARD, Dominique SERET, Pearson édition ,2009.
- José DORDOIGNE , Réseaux informatiques : Notions fondamentales ; edition ENI , 2017
- Cours CCNA1, CCNA2 n cisco Networking, version 3.1
- https://www.commentcamarche.net/ consulté du 16/2/2021 au 18/04/2022