الجمهورية الجزائرية الديموقراطية الشعبية

وزارة التعليم العلمي و البحث العالي

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

جامعة وهران 2 محمد بن أحمد

معهد الصيانة و الأمن الصناعي

Université d'Oran 2 Mohamed Ben Ahmed

Institut de Maintenance et Sécurité Industrielle

Cours de

Réseaux Informatiques

1 ère année

Master Génie Industriel

Sarah Benziane

1 ère édition : Année universitaire 2019 – 2020

Avant-propos

A propos

Ce cours donne une très bonne compréhension de la communication de données et des réseaux informatiques. Après avoir terminé ce tutoriel, vous vous retrouverez à un niveau d'expertise modéré dans la connaissance des réseaux informatiques, d'où vous pourrez passer au niveau suivant qui est un module qui concerne les réseaux industriels du deuxième semestre.

Audience

Ce tutoriel est préparé pour les étudiants de première année du master Génie Industriel pour les aider à comprendre la communication de données et les réseaux informatiques du module réseaux informatiques.

Conditions préalables

Avant de continuer ce cours, vous avez besoin d'une compréhension de base de l'ordinateur. Vous devez connaître les bases des périphériques d'entrée et de sortie, de la mémoire principale et secondaire et du système d'exploitation.

Table des matières

Tables des figures

CHAPITRE 1 : INTRODUCTION AUX RESEAUX INFORMATIQUES

1.1. INTRODUCTION

Un système d'ordinateurs interconnectés et de périphériques informatisés tels que des imprimantes est appelé réseau informatique. Cette interconnexion entre ordinateurs facilite le partage d'informations entre eux. Les ordinateurs peuvent se connecter les uns aux autres par un média filaire ou sans fil.

1.1.1. CLASSIFICATION DES RESEAUX INFORMATIQUES

Les réseaux informatiques sont classés en fonction de divers facteurs. Ils comprennent:

- *Distance géographique,*
- *Inter-connectivité,*
- *Administration,*
- *Architecture.*

1.1.2. DISTANCE GEOGRAPHIQUE

Géographiquement, un réseau peut être vu dans l'une des catégories suivantes:

- *Il peut être réparti sur votre table, parmi les appareils compatibles Bluetooth, ne dépassant pas quelques mètres.*
- *Il peut être réparti sur un bâtiment entier, y compris des dispositifs intermédiaires pour connecter tous les étages.*
- *Il peut être étendu à travers une ville entière.*
- *Il peut être réparti entre plusieurs villes ou provinces.*
- *Il peut s'agir d'un réseau couvrant le monde entier.*

1.1.3. INTER CONNECTIVITE

Les composants d'un réseau peuvent être connectés les uns aux autres différemment d'une manière ou d'une autre. Par connectivité, nous entendons soit logiquement, physiquement ou les deux.

- *Chaque périphérique peut être connecté à tous les autres périphériques du réseau, ce qui rend le réseau maillé.*
- *Tous les appareils peuvent être connectés à un seul média mais géographiquement déconnectés, créant une structure semblable à un bus.*
- *Chaque périphérique est uniquement connecté à ses homologues gauche et droite, créant ainsi une structure linéaire.*
- *Tous les périphériques connectés ensemble avec un seul périphérique, créant une structure en étoile.*
- *Tous les périphériques connectés arbitrairement en utilisant toutes les façons précédentes de se connecter les uns aux autres, ce qui entraîne une structure hybride.*

1.1.4. ADMINISTRATION

Du point de vue de l'administrateur, un réseau peut être un réseau privé qui appartient à un seul système autonome et ne peut être accessible en dehors de son domaine physique ou logique. Un réseau peut être public, auquel tous accèdent.

1.1.5. ARCHITECTURE DE RESEAU

Les réseaux informatiques peuvent être distingués en différents types tels que Client-Serveur, pair-à-pair ou hybride, en fonction de leurs architectures.

- *Il peut y avoir un ou plusieurs systèmes agissant en tant que serveur. Autre étant Client, demande au serveur de répondre aux demandes. Le serveur prend et traite la demande au nom des clients.*
- *Deux systèmes peuvent être connectés point à point, ou de manière dos-à-dos. Ils résident tous les deux au même niveau et appellent leurs pairs.*
- *Il peut y avoir un réseau hybride qui implique une architecture de réseau des deux types ci-dessus.*

1.1.6. APPLICATIONS DES RESEAUX

Les systèmes informatiques et les périphériques sont connectés pour former un réseau. Ils offrent de nombreux avantages :

- *Partage de ressources telles que les imprimantes et les périphériques de stockage*
- *Échange d'informations par e-mails et FTP*
- *Partage d'informations en utilisant le Web ou Internet*
- *Interaction avec d'autres utilisateurs utilisant des pages Web dynamiques*
- *Téléphones IP*
- *Vidéoconférences*
- *Calcul parallèle*
- *Messagerie instantanée*

1.2. TYPE DE RESEAUX INFORMATIQUES

Généralement, les réseaux sont distingués en fonction de leur étendue géographique. Un réseau peut être aussi petit que la distance entre votre téléphone mobile et son casque Bluetooth et aussi grand que l'Internet lui-même, couvrant l'ensemble du monde géographique.

1.2.1. RESEAU PERSONNEL (PERSONAL AREA NETWORK)

Un réseau personnel (PAN) est le plus petit réseau qui soit très personnel pour un utilisateur. Cela peut inclure des périphériques compatibles Bluetooth ou des périphériques compatibles infrarouges. PAN a une portée de connectivité allant jusqu'à 10 mètres. PAN peut inclure un clavier et une souris d'ordinateur sans fil, un casque compatible Bluetooth, des imprimantes sans fil et des télécommandes TV.

Par exemple, Piconet est un réseau personnel à capacité Bluetooth qui peut contenir jusqu'à 8 appareils connectés ensemble de façon maître-esclave.

Figure 1 : Exemple de connexion bluetooth

1.2.2. RÉSEAU LOCAL (LOCAL AREA NETWORK)

Un réseau informatique s'étendant à l'intérieur d'un bâtiment et exploité sous un système administratif unique est généralement appelé réseau local (LAN). Habituellement, LAN couvre les bureaux d'une organisation, les écoles, les collèges ou les universités. Le nombre de systèmes connectés au réseau local peut varier de deux à 16 millions.

LAN fournit un moyen utile de partager les ressources entre les utilisateurs finaux. Les ressources telles que les imprimantes, les serveurs de fichiers, les scanners et Internet sont facilement partageables entre les ordinateurs.

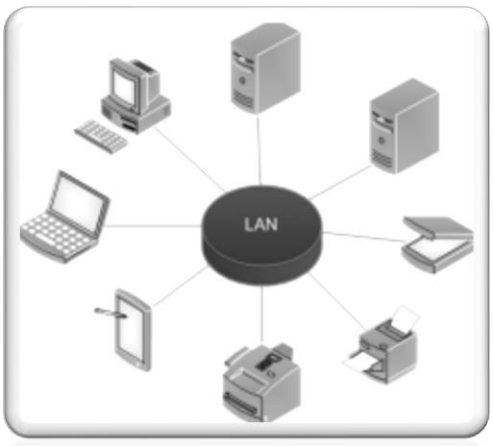


Figure 2 : Réseau LAN

Les réseaux locaux sont composés d'équipements de mise en réseau et de routage peu coûteux. Il peut contenir des serveurs locaux servant au stockage de fichiers et d'autres applications partagées localement. Il fonctionne principalement sur des adresses IP privées et n'implique pas de routage lourd.

LAN fonctionne sous son propre domaine local et est contrôlé centralement.

Le LAN utilise la technologie Ethernet ou Token-ring. Ethernet est le plus largement employé

La technologie LAN utilise la topologie Star, tandis que Token-ring est rarement visible.

LAN peut être câblé, sans fil, ou dans les deux formes à la fois.

1.2.3. RESEAU METROPOLITAIN (METROPOLITAN AREA NETWORK)

Le réseau métropolitain (MAN) s'étend généralement à travers une ville comme le réseau de télévision par câble. Il peut s'agir d'Ethernet, de Token-ring, d'ATM ou d'interface FDDI (Fiber Distributed Data Interface).

Metro Ethernet est un service fourni par les FAI. Ce service permet à ses utilisateurs d'étendre leurs réseaux locaux. Par exemple, MAN peut aider une organisation à connecter tous ses bureaux dans une ville.

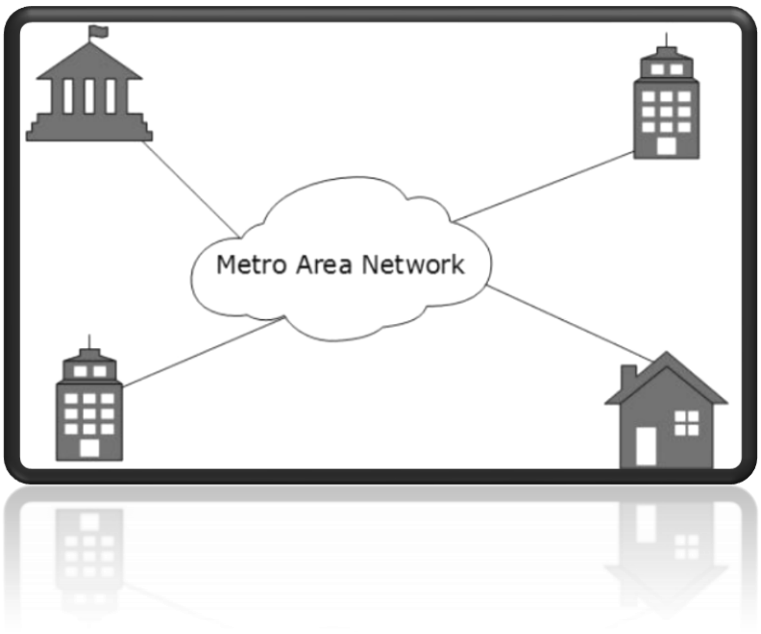


Figure 3 : Réseau MAN

Le Backbone du MAN est la fibre optique de haute capacité et haute vitesse. Le MAN travaille entre le réseau local et le réseau étendu. Il fournit une liaison montante pour les LAN vers les réseaux WAN ou Internet.

1.2.4. RESEAU ETENDU (WIDE AREA NETWORK)

Comme son nom l'indique, le réseau étendu (WAN) couvre une vaste zone qui peut couvrir plusieurs provinces et même un pays entier. Généralement, les réseaux de télécommunication sont des réseaux étendus. Ces réseaux fournissent une connectivité aux MAN et aux LAN. Comme ils sont équipés d'un réseau dorsal à très haut débit, les réseaux WAN utilisent un équipement de réseau très coûteux.

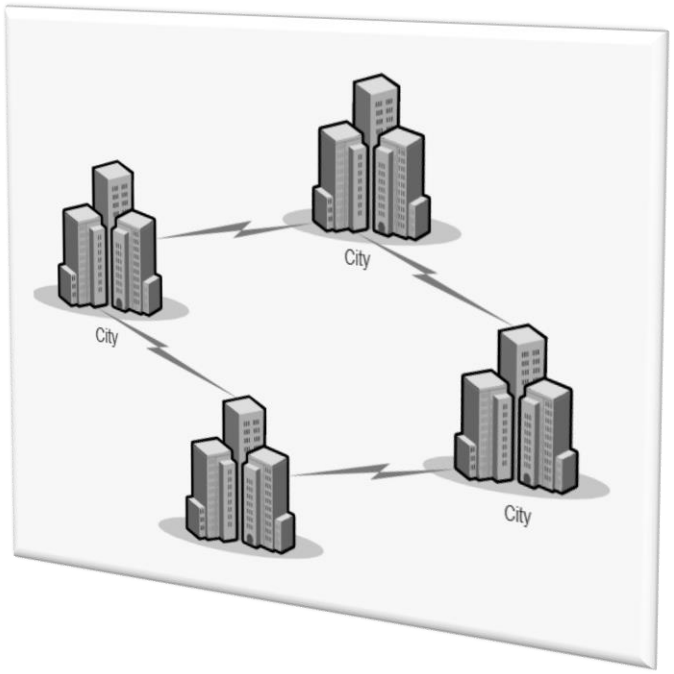


Figure 4 : Réseau WAN [1]

Le WAN peut utiliser des technologies avancées telles que le mode de transfert asynchrone (ATM), le relais de trame et le réseau optique synchrone (SONET). Le réseau étendu peut être géré par plusieurs administrations.

1.2.5. INTERNETWORK

Un réseau de réseaux s'appelle un inter-réseau, ou simplement Internet. C'est le plus grand réseau existant sur cette planète. L'Internet connecte tous les réseaux étendus et il peut avoir une connexion aux réseaux locaux et domestiques. Internet utilise la suite de protocoles TCP / IP et utilise l'IP comme protocole d'adressage. Aujourd'hui, Internet est largement implémenté en utilisant IPv4. En raison de la pénurie d'espaces d'adressage, il migre progressivement d'IPv4 vers IPv6.

Internet permet à ses utilisateurs de partager et d'accéder à une énorme quantité d'informations dans le monde entier. Il utilise WWW, FTP, les services de messagerie électronique, audio et vidéo en continu, etc. À un niveau énorme, Internet fonctionne sur le modèle Client-Serveur.

Internet utilise le backbone à très haut débit de la fibre optique. Pour interconnecter les différents continents, les fibres sont posées sous la mer et connues sous le nom de câble de communication sous-marin. Internet est largement déployé sur les services World Wide Web en utilisant des pages HTML et est accessible par un logiciel client connu sous le nom de navigateurs Web. Lorsqu'un utilisateur demande une page à l'aide d'un navigateur Web situé sur un serveur Web n'importe où dans le monde, le serveur Web répond avec la page HTML appropriée. Le délai de communication est très faible.

1.3. CONCLUSION

Internet est au service de nombreuses propositions et est impliqué dans de nombreux aspects de la vie. Certains d'entre eux sont:

- *Web sites*
- *E-mail*
- *Instant Messaging*
- *Blogging*
- *Social Media*
- *Marketing*
- *Networking*
- *Partage de ressource*
- *Audio et Video Streaming*

Chapitre 2 : Technologie, topologie et modèle

2.1. INTRODUCTION

On va passer par diverses technologies LAN en bref :

Ethernet est une technologie LAN largement déployée. Cette technologie a été inventée par Bob Metcalfe et D.R. Boggs dans l'année 1970. Il a été normalisé dans IEEE 802.3 en 1980.

2.2. TECHNOLOGIE DES RESEAUX LAN

2.2.1. ETHERNET

Ethernet partage les médias. Réseau qui utilise des médias partagés a une forte probabilité de collision de données. Ethernet utilise la technologie CSMA / CD (Carrier Sense Multi Access / Collision Detection) pour détecter les collisions. En cas de collision dans Ethernet, tous ses hôtes sont annulés, attendent un certain temps et transmettent de nouveau les données.

Le connecteur Ethernet est une carte d'interface réseau équipée d'une adresse MAC 48 bits. Cela permet à d'autres périphériques Ethernet d'identifier et de communiquer avec des périphériques distants dans Ethernet.

L'Ethernet traditionnel utilise les spécifications 10BASE-T. Le numéro 10 représente la vitesse 10MBPS, BASE signifie bande de base et T signifie Ethernet épais. L'Ethernet 10BASE-T fournit une vitesse de transmission allant jusqu'à 10 Mbps et utilise un câble coaxial ou un câble à paire torsadée Cat-5 avec connecteur RJ-5. Ethernet suit la topologie Star avec une longueur de segment allant jusqu'à 100 mètres. Tous les appareils sont connectés à un concentrateur / commutateur à la manière d'une étoile.

2.2.2. FAST ETHERNET

Pour répondre aux besoins des technologies logicielles et matérielles émergentes rapides, Ethernet s'étend lui-même en tant que Fast-Ethernet. Il peut fonctionner sur UTP, fibre optique et sans fil aussi. Il peut fournir une vitesse allant jusqu'à 100MBPS. Cette norme est nommée 100BASE-T dans IEEE 803.2 en utilisant un câble à paire torsadée Cat-5. Il utilise la technique CSMA / CD pour le partage de médias câblés entre les hôtes Ethernet et la technique CSMA / CA (CA signifie Collision Avoidance) pour un LAN Ethernet sans fil.

Fast Ethernet sur fibre est défini sous la norme 100BASE-FX qui fournit une vitesse jusqu'à 100MBPS sur fibre. Ethernet sur fibre peut être étendu jusqu'à 100 mètres en mode semi-duplex et peut atteindre un maximum de 2000 mètres en full-duplex par rapport aux fibres multimodes.

2.2.3. GIGA ETHERNET

Après avoir été introduit en 1995, Fast-Ethernet a conservé son statut de haute vitesse seulement trois ans avant l'introduction de Giga-Ethernet. Giga-Ethernet fournit une vitesse allant jusqu'à 1000mbits / secondes. La norme IEEE802.3ab standardise le Giga-Ethernet sur UTP à l'aide de câbles Cat-5, Cat5e et Cat-6. IEEE802.3ah définit Giga-Ethernet sur fibre.

2.2.4. LAN VIRTUEL

LAN utilise Ethernet qui à son tour fonctionne sur les médias partagés. Les médias partagés dans Ethernet créent un seul domaine de diffusion et un seul domaine de collision. L'introduction de commutateurs vers Ethernet a supprimé le problème du domaine de collision unique et chaque périphérique connecté au commutateur fonctionne dans son domaine de collision distinct. Mais même les commutateurs ne peuvent pas diviser un réseau en domaines de diffusion distincts.
Virtual LAN est une solution permettant de diviser un seul domaine de diffusion en plusieurs domaines de diffusion. L'hôte dans un VLAN ne peut pas parler à un hôte dans un autre. Par défaut, tous les hôtes sont placés dans le même VLAN.

Dans ce diagramme, différents VLAN sont représentés dans des codes de couleurs différents. Hôtes dans un VLAN, même si connecté sur le même commutateur ne peut pas voir ou parler à d'autres hôtes dans différents VLAN. VLAN est la technologie Layer-2 qui fonctionne étroitement sur Ethernet. Pour acheminer les paquets entre deux VLAN différents, un périphérique de couche 3 tel que le routeur est requis.

2.3. LES TOPOLOGIES DES RESEAUX INFORMATIQUES

Une topologie réseau est l'arrangement avec lequel les systèmes informatiques ou les périphériques réseau sont connectés les uns aux autres. Les topologies peuvent définir à la fois l'aspect physique et logique du réseau. Les topologies logiques et physiques peuvent être identiques ou différentes dans un même réseau.

2.3.1.POINT A POINT

Les réseaux point à point contiennent exactement deux hôtes tels qu'un ordinateur, des commutateurs, des routeurs ou des serveurs connectés dos à dos à l'aide d'un seul câble. Souvent, l'extrémité de réception d'un hôte est connectée à l'extrémité d'envoi de l'autre et vice versa.

Figure 5 : Réseau Bi-poste

Si les hôtes sont connectés point à point de manière logique, ils peuvent avoir plusieurs périphériques intermédiaires. Mais les hôtes finaux ne sont pas conscients du réseau sous-jacent et se voient comme s'ils étaient directement connectés.

2.3.2. LA TOPOLOGIE EN BUS

En cas de topologie Bus, tous les périphériques partagent une seule ligne de communication ou câble. La topologie de bus peut rencontrer des problèmes lorsque plusieurs hôtes envoient des données en même temps. Par conséquent, la topologie Bus utilise la technologie CSMA / CD ou reconnaît un hôte comme Bus Master pour résoudre le problème. C'est l'une des formes simples de mise en réseau où une panne d'un appareil n'affecte pas les autres appareils. Mais l'échec de la ligne de communication partagée peut empêcher tous les autres périphériques de fonctionner.

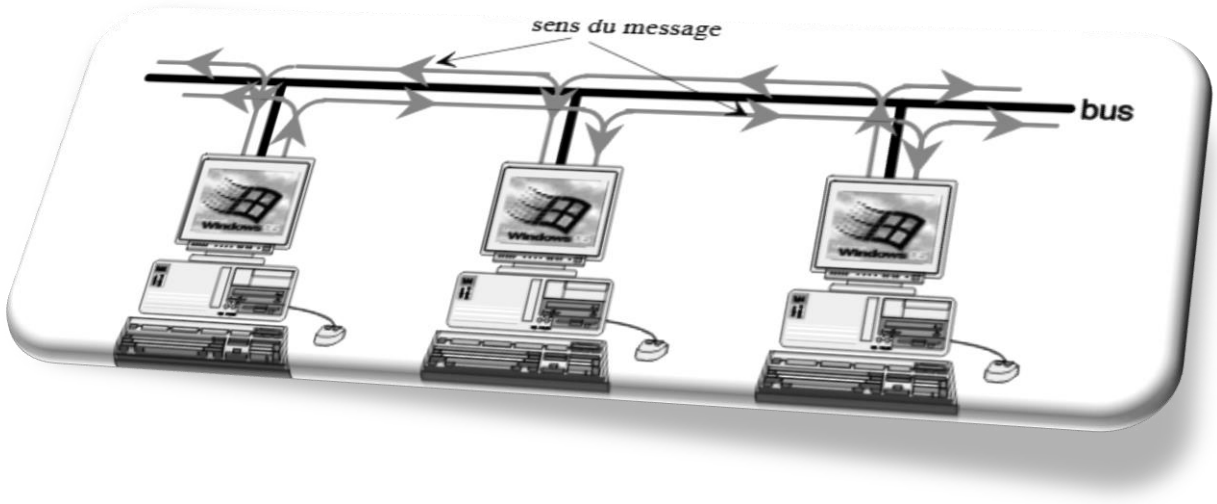


Figure 6 : Topologie en bus bidirectionnel

Les deux extrémités du canal partagé ont un terminateur de ligne. Les données sont envoyées dans un seul sens et dès qu'elles atteignent l'extrémité, le terminateur supprime les données de la ligne.

2.3.3. LA TOPOLOGIE EN ETOILE

Tous les hôtes de la topologie Star sont connectés à un périphérique central, appelé périphérique hub, à l'aide d'une connexion point à point. Autrement dit, il existe une connexion point à point entre les hôtes et le concentrateur. Le périphérique concentrateur peut être l'un des éléments suivants:

- *Appareil de couche 1 tel qu'un concentrateur ou un répéteur*
- *Appareil de couche 2 tel qu'un commutateur ou un pont*
- *Appareil de couche 3 tel qu'un routeur ou une passerelle*

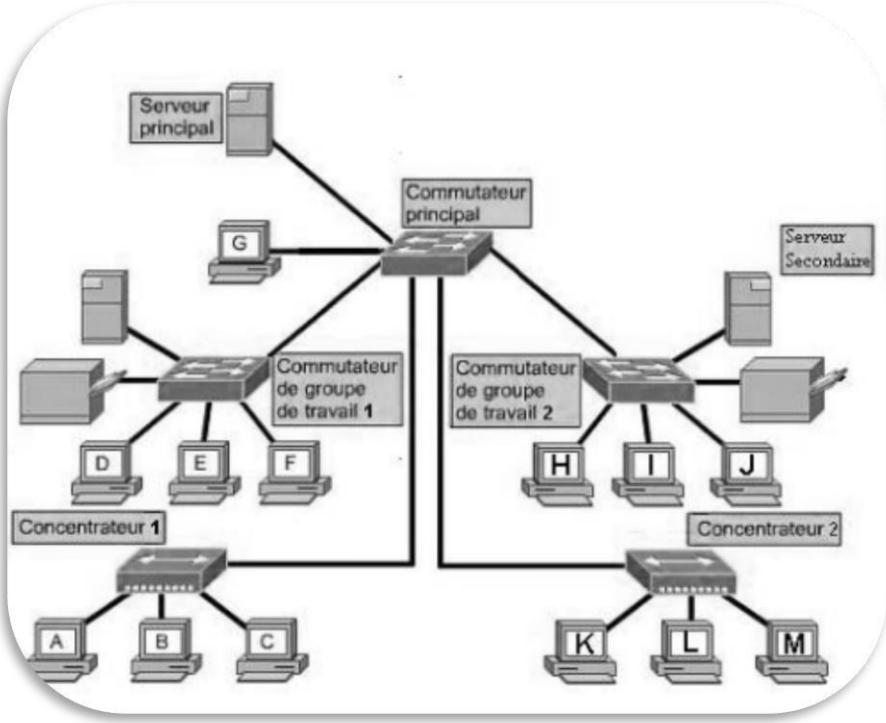


Figure 7 : Topologie en étoile étendue [2]

Comme dans la topologie Bus, le hub agit comme un point de défaillance unique. Si le concentrateur tombe en panne, la connexion de tous les hôtes à tous les autres hôtes échoue. Chaque communication entre les hôtes s'effectue uniquement via le hub. La topologie en étoile n'est pas coûteuse car elle permet de connecter un hôte supplémentaire, un seul câble est requis et la configuration est simple.

2.3.4. LA TOPOLOGIE EN ANNEAU

En topologie en anneau, chaque machine hôte se connecte exactement à deux autres machines, créant une structure de réseau circulaire. Lorsqu'un hôte tente de communiquer ou d'envoyer un message à un hôte qui n'est pas adjacent à celui-ci, les données transitent par tous les hôtes intermédiaires. Pour connecter un autre hôte dans la structure exstante, l'administrateur peut n'avoir besoin que d'un câble supplémentaire.

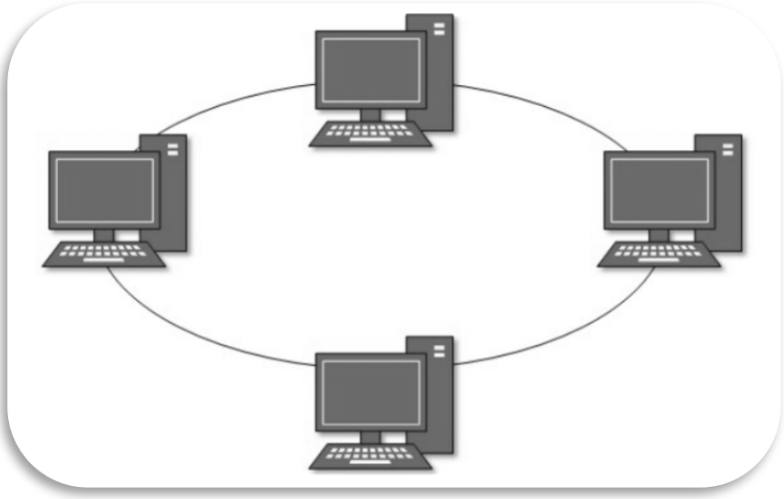


Figure 8 : Réseau en Anneau

La défaillance d'un hôte entraîne la défaillance de l'anneau entier. Ainsi, chaque connexion dans l'anneau est un point d'échec. Il existe des méthodes qui utilisent un anneau de sauvegarde supplémentaire.

2.3.5. TOPOLOGIE EN MAILLE

Dans ce type de topologie, un hôte est connecté à un ou plusieurs hôtes. Cette topologie a des hôtes en connexion point à point avec tous les autres hôtes ou peut également avoir des hôtes qui sont en connexion point à point avec seulement quelques hôtes.

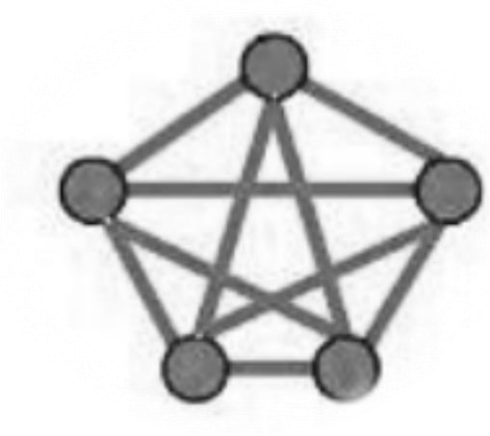


Figure 9 : Topologie du réseau en Maille

Les hôtes dans la topologie Mesh fonctionnent également comme relais pour d'autres hôtes qui ne disposent pas de liaisons directes point à point. La technologie de la maille est de deux types:

- *Full Mesh: tous les hôtes ont une connexion point à point avec tous les autres hôtes du réseau. Ainsi, pour chaque nouvel hôte, n (n-1) / 2 connexions sont requises. Il fournit la structure de réseau la plus fiable parmi toutes les topologies de réseau.*
- *Maillage partiel : tous les hôtes n'ont pas de connexion point à point avec tous les autres hôtes. Les hôtes se connectent les uns aux autres de façon arbitraire. Cette topologie existe où nous devons fournir la fiabilité à certains hôtes de tous.*

2.3.6. TOPOLOGIE EN ARBRE

Aussi connue sous le nom de topologie hiérarchique, c'est la forme de topologie réseau la plus couramment utilisée actuellement. Cette topologie imite la topologie Star étendue et hérite des propriétés de la topologie Bus.

Cette topologie divise le réseau en plusieurs niveaux / couches de réseau. Principalement dans les réseaux locaux, un réseau est divisé en trois types de périphériques réseau. Le plus bas est la couche d'accès où les ordinateurs sont attachés. La couche intermédiaire est appelée couche de distribution, qui agit comme médiateur entre la couche supérieure et la couche inférieure. La couche la plus haute est appelée couche centrale et est le point central du réseau, c'est-à-dire la racine de l'arbre à partir de laquelle tous les nœuds se chevauchent.

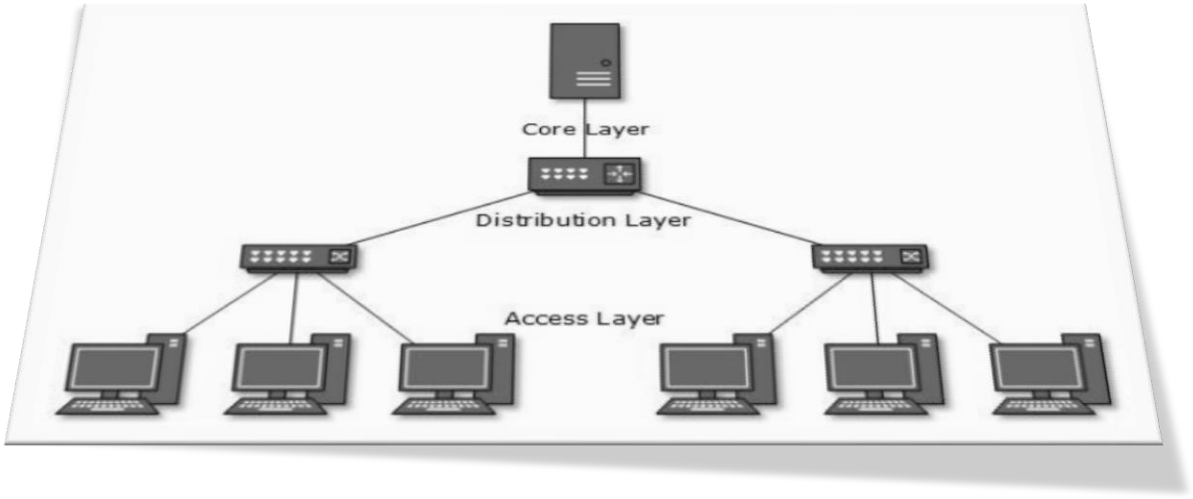


Figure 10 : Topologie réseau en Arbre

Tous les hôtes voisins ont une connexion point à point entre eux. Similaire à la topologie Bus, si la racine tombe en panne, alors tout le réseau souffre même si ce n'est pas le seul point de défaillance. Chaque connexion sert de point de défaillance, à défaut de quoi le réseau se divise en segment inaccessible.

2.3.7. CHAINE DAISY

Cette topologie connecte tous les hôtes de manière linéaire. Semblable à la topologie en anneau, tous les hôtes sont connectés à deux hôtes uniquement, à l'exception des hôtes finaux. Cela signifie que si les hôtes finaux dans la chaîne sont connectés, cela représente la topologie en anneau.

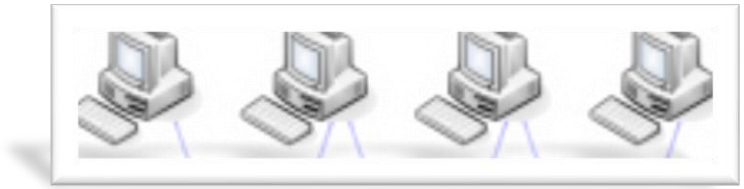


Figure 11 : Topologie en réseau chaine daisy

Chaque lien dans la topologie en guirlande représente un point de défaillance unique. Chaque défaillance de lien divise le réseau en deux segments. Chaque hôte intermédiaire fonctionne comme relais pour ses hôtes immédiats.

2.3.8. TOPOLOGIE HYBRIDE

Une structure de réseau dont la conception contient plus d'une topologie est dite topologie hybride. La topologie hybride hérite des mérites et des démérites de toutes les topologies incorporées.

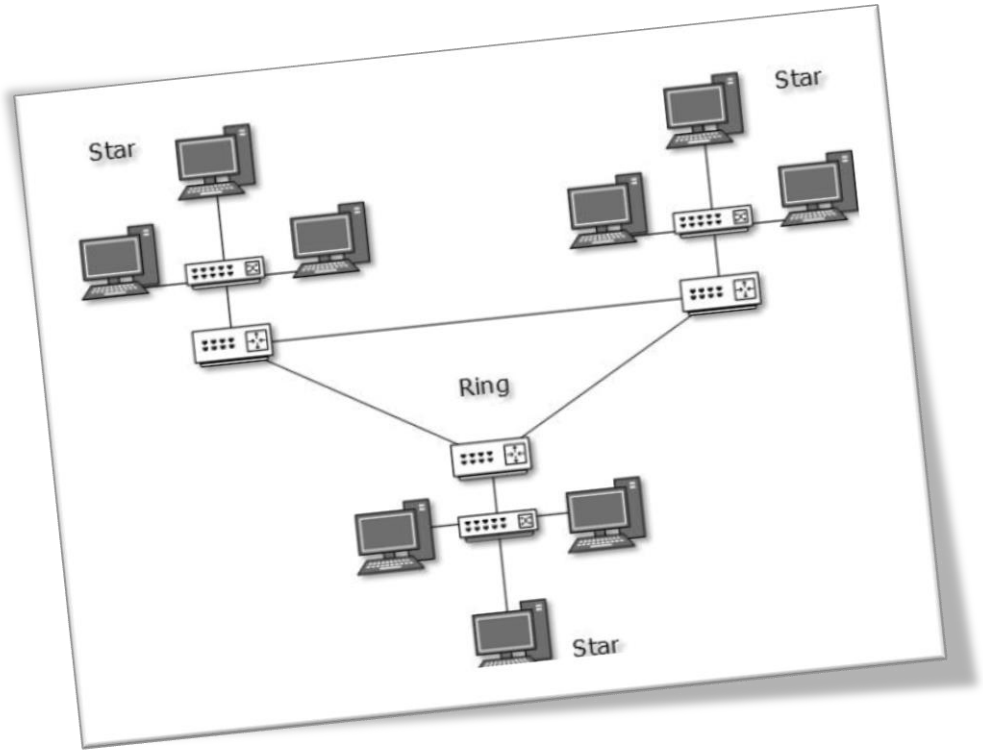


Figure 12 : Topologie en réseau hybride

L'image ci-dessus représente une topologie arbitrairement hybride. Les topologies combinées peuvent contenir des attributs des topologies Star, Ring, Bus et Daisy-chain. La plupart des réseaux étendus sont connectés au moyen d'une topologie à double anneau et de réseaux connectés à eux par des réseaux de topologie étoile. Internet est le meilleur exemple de la plus grande topologie Hybride.

2.4. MODELE DE RESEAU INFORMATIQUE

L'ingénierie de réseau est une tâche compliquée qui implique des logiciels, des microprogrammes, l'ingénierie au niveau de la puce, du matériel et des impulsions électriques. Pour faciliter l'ingénierie réseau, l'ensemble du concept de réseau est divisé en plusieurs couches. Chaque couche est impliquée dans une tâche particulière et est indépendante de toutes les autres couches. Mais dans l'ensemble, presque toutes les tâches de mise en réseau dépendent de toutes ces couches. Les calques partagent des données entre eux et ils ne dépendent l'un de l'autre que pour prendre l'entrée et envoyer la sortie.

2.4.1. TACHES EN COUCHES

Dans l'architecture en couches du modèle de réseau, un processus de réseau entier est divisé en petites tâches. Chaque petite tâche est ensuite assignée à une couche particulière qui travaille uniquement pour traiter la tâche. Chaque couche ne fait que du travail spécifique. Dans un système de communication en couches, une couche d'un hôte traite la tâche effectuée par ou doit être effectuée par sa couche homologue au même niveau sur l'hôte distant. La tâche est initiée par couche au niveau le plus bas ou au plus haut niveau. Si la tâche est initiée par la couche supérieure, elle est transmise à la couche située en dessous pour un traitement ultérieur. La couche inférieure fait la même chose, elle traite la tâche et passe à la couche inférieure. Si la tâche est initiée par la couche inférieure, le chemin inverse est pris.

Chaque couche regroupe toutes les procédures, les protocoles et les méthodes dont elle a besoin pour exécuter sa tâche. Toutes les couches identifient leurs contreparties au moyen de l'en-tête et de la queue d'encapsulation.

2.4.2. MODELE OSI

Open System Interconnect est une norme ouverte pour tous les systèmes de communication. Le modèle OSI est établi par l'Organisation internationale de normalisation (ISO). Ce modèle a sept couches :

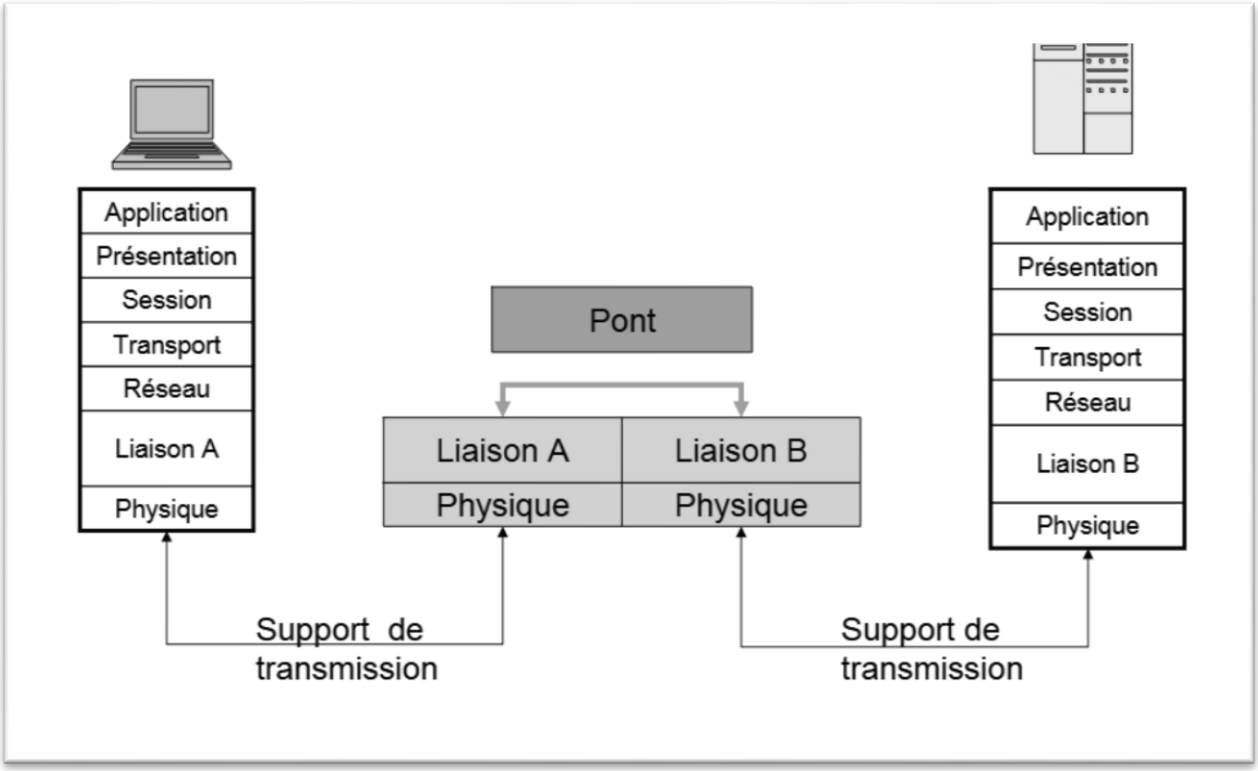


Figure 13 : Modèle OSI [3]

Couche d'application : *Cette couche est chargée de fournir une interface à l'utilisateur de l'application. Cette couche englobe les protocoles qui interagissent directement avec l'utilisateur.*

Couche de présentation : *Cette couche définit comment les données dans le format natif de l'hôte distant doivent être présentées dans le format natif de l'hôte.*

Couche Session : *Cette couche gère les sessions entre les hôtes distants. Par exemple, une fois l'authentification utilisateur / mot de passe terminée, l'hôte distant conserve cette session pendant un certain temps et ne demande plus d'authentification dans ce laps de temps.*

Couche de transport : *Cette couche est responsable de la livraison de bout en bout entre les hôtes.*

Couche réseau : *Cette couche est responsable de l'attribution des adresses et des adresses uniques des hôtes dans un réseau.*

Couche liaison de données : cette couche est responsable de la lecture et de l'écriture des données depuis et vers la ligne. Les erreurs de liaison sont détectées sur cette couche.

Couche physique : *Cette couche définit le matériel, le câblage, le câblage, la puissance de sortie, le pouls, etc.*

2.4.3. MODELE INTERNET

Internet utilise la suite de protocoles TCP / IP, également appelée suite Internet. Ceci définit le modèle Internet qui contient quatre architectures en couches. Le modèle OSI est un modèle de communication général, mais

Internet Model est ce que l'Internet utilise pour toutes ses communications. L'Internet est indépendant de son architecture de réseau sous-jacente, tout comme son modèle. Ce modèle a les couches suivantes :

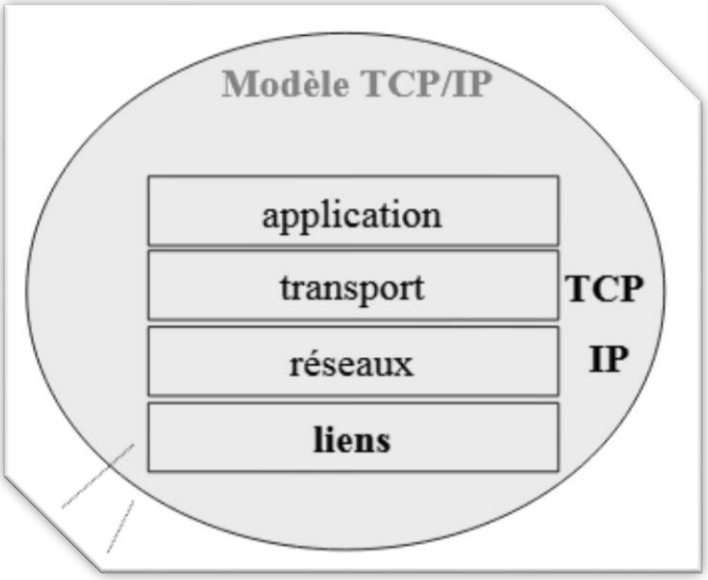


Figure 14 : Modèle Internet

Couche d'application : *Cette couche définit le protocole qui permet à l'utilisateur d'interagir avec le réseau. Par exemple, FTP, HTTP, etc.*

Couche de transport : *cette couche définit la manière dont les données doivent circuler entre les hôtes. Le protocole majeur de cette couche est le protocole TCP (Transmission Control Protocol). Cette couche garantit que les données fournies entre les hôtes sont en ordre et est responsable de la livraison de bout en bout.*

Couche Internet : *le protocole Internet (IP) fonctionne sur cette couche. Cette couche facilite l'adressage et la reconnaissance de l'hôte. Cette couche définit le routage.*

Couche de liaison : *Cette couche fournit un mécanisme d'envoi et de réception de données réelles. Contrairement à son homologue modèle OSI, cette couche est indépendante de l'architecture réseau et du matériel sous-jacents.*

Chapitre 3 : Sécurité des réseaux informatiques

3.1. INTRODUCTION

Au cours des premiers jours d'Internet, son utilisation était limitée aux militaires et aux universités à des fins de recherche et de développement. Plus tard, lorsque tous les réseaux ont fusionné et formé Internet, les données utilisées pour voyager à travers le réseau de transport en commun. Les gens ordinaires peuvent envoyer les données qui peuvent être très sensibles telles que leurs identifiants bancaires, nom d'utilisateur et mots de passe, documents personnels, détails d'achat en ligne ou documents confidentiels. Toutes les menaces de sécurité sont intentionnelles, c'est-à-dire qu'elles ne se produisent que si elles sont intentionnellement déclenchées. Les menaces de sécurité peuvent être réparties dans les catégories suivantes:

3.2. SECURITE

Interruption

L'interruption est une menace pour la sécurité dans laquelle la disponibilité des ressources est attaquée. Par exemple, un utilisateur est incapable d'accéder à son serveur Web ou le serveur Web est piraté.

Violation de la vie privée

Dans cette menace, la vie privée d'un utilisateur est compromise. Quelqu'un, qui n'est pas la personne autorisée, accède ou intercepte les données envoyées ou reçues par l'utilisateur authentifié original.

Intégrité

Ce type de menace inclut toute altération ou modification dans le contexte original de la communication. L'attaquant intercepte et reçoit les données envoyées par l'expéditeur et l'attaquant modifie ou génère de fausses données et les envoie au destinataire. Le récepteur reçoit les données en supposant qu'il est envoyé par l'expéditeur d'origine.

Authenticité

Cette menace se produit lorsqu'un attaquant ou un violateur de sécurité se présente comme une personne authentique et accède aux ressources ou communique avec d'autres utilisateurs authentiques.

Aucune technique dans le monde actuel ne peut fournir une sécurité à 100%. Mais des mesures peuvent être prises pour sécuriser les données alors qu'il se déplace dans un réseau non sécurisé ou sur Internet. La technique la plus largement utilisée est la cryptographie.

La cryptographie est une technique permettant de chiffrer les données en texte clair, ce qui les rend difficiles à comprendre et à interpréter. Il existe plusieurs algorithmes cryptographiques disponibles aujourd'hui décrits ci-dessous :

- ✓ *Clé secrète*
- ✓ *Clé publique*
- ✓ *Message Digest*

3.2.1. CHIFFREMENT DE CLE SECRETE

L'expéditeur et le destinataire ont une clé secrète. Cette clé secrète est utilisée pour crypter les données à la fin de l'expéditeur. Une fois les données chiffrées, elles sont envoyées sur le domaine public au destinataire. Parce que le récepteur connaît et a la clé secrète, les paquets de données cryptés peuvent facilement être déchiffrés.

Exemple de cryptage de clé secrète est Data Encryption Standard (DES). Dans le cryptage à clé secrète, il est nécessaire d'avoir une clé séparée pour chaque hôte sur le réseau, ce qui rend la gestion difficile.

3.2.2. CHIFFREMENT DE CLE PUBLIQUE

Dans ce système de chiffrement, chaque utilisateur a sa propre clé secrète et ce n'est pas dans le domaine partagé. La clé secrète n'est jamais révélée sur le domaine public. Avec la clé secrète, chaque utilisateur a sa propre clé publique. La clé publique est toujours rendue publique et est utilisée par les expéditeurs pour crypter les données. Lorsque l'utilisateur reçoit les données cryptées, il peut facilement les déchiffrer en utilisant sa propre clé secrète.
Exemple de cryptage de clé publique est Rivest-Shamir-Adleman (RSA).

3.2.3. MESSAGE DIGEST

Dans cette méthode, les données réelles ne sont pas envoyées; à la place, une valeur de hachage est calculée et envoyée. L'autre utilisateur final calcule sa propre valeur de hachage et la compare à celle qui vient d'être reçue. Si les deux valeurs de hachage correspondent, alors il est accepté; autrement rejeté. Exemple de message Digest est le hachage MD5. Il est principalement utilisé dans l'authentification où le mot de passe de l'utilisateur est croisé avec celui enregistré sur le serveur.

3.3. INTRODUCTION AUX COUCHES PHYSIQUE

La couche physique dans le modèle OSI joue le rôle d'interaction avec le matériel réel et le mécanisme de signalisation. La couche physique est la seule couche du modèle de réseau OSI qui gère réellement la connectivité physique de deux stations différentes. Cette couche définit l'équipement matériel, le câblage, le câblage, les fréquences, les impulsions utilisées pour représenter les signaux binaires, etc.

La couche physique fournit ses services à la couche de liaison de données. La couche de liaison de données transmet les trames à la couche physique. La couche physique les convertit en impulsions électriques, qui représentent des données binaires. Les données binaires sont ensuite envoyées sur le support filaire ou sans fil.

3.3.1. SIGNAUX

Lorsque les données sont envoyées sur un support physique, elles doivent d'abord être converties en signaux électromagnétiques. Les données elles-mêmes peuvent être analogiques, telles que la voix humaine, ou numériques, comme les fichiers sur le disque. Les données analogiques et numériques peuvent être représentées dans des signaux numériques ou analogiques.

Signaux numériques

Les signaux numériques sont de nature discrète et représentent une séquence d'impulsions de tension. Les signaux numériques sont utilisés dans les circuits d'un système informatique.

Signaux analogiques

Les signaux analogiques sont sous forme d'onde continue dans la nature et sont représentés par des ondes électromagnétiques continues.

3.3.1. DEFICIENCE DE TRANSMISSION

Lorsque les signaux traversent le médium, ils ont tendance à se détériorer. Cela peut avoir plusieurs raisons:
Atténuatsion
Pour que le récepteur interprète correctement les données, le signal doit être suffisamment fort. Lorsque le signal traverse le milieu, il a tendance à s'affaiblir. Comme il couvre la distance, il perd de la force.

Dispersion

Lorsque le signal traverse les médias, il a tendance à se propager et à se chevaucher. La quantité de dispersion dépend de la fréquence utilisée.

Retarder la distorsion

Les signaux sont envoyés sur des supports avec une vitesse et une fréquence prédéfinies. Si la vitesse et la fréquence du signal ne correspondent pas, il existe des possibilités que le signal atteigne la destination mode arbitraire. Dans les médias numériques, il est très important que certains bits atteignent plus tôt que les bits précédemment envoyés.

Bruit

Une perturbation aléatoire ou une fluctuation dans un signal analogique ou numérique est considérée comme un signal de bruit, ce qui peut fausser l'information réelle transportée. Le bruit peut être caractérisé dans l'une des classes suivantes:

Bruit thermique

La chaleur agite les conducteurs électroniques d'un milieu susceptible d'introduire du bruit dans les médias. Jusqu'à un certain niveau, le bruit thermique est inévitable.

Intermodulation

Lorsque plusieurs fréquences partagent un support, leur interférence peut provoquer du bruit dans le support. Le bruit d'intermodulation se produit si deux fréquences différentes partagent un support et que l'une d'elles a une force excessive ou si le composant lui-même ne fonctionne pas correctement, alors la fréquence résultante peut ne pas être délivrée comme prévu.

Crosstalk

Ce type de bruit se produit lorsqu'un signal étranger entre dans le média. C'est parce que le signal dans un milieu affecte le signal du deuxième milieu.

Impulsion

Ce bruit est introduit en raison de perturbations irrégulières telles que l'éclairage, l'électricité, les courts-circuits ou les composants défectueux. Les données numériques sont principalement affectées par ce type de bruit.

3.3.3. MEDIAS DE TRANSMISSION

Le média sur lequel est envoyée l'information entre deux systèmes informatiques, appelé support de transmission. Les médias de transmission se présentent sous deux formes.

Médias guidés

Tous les fils / câbles de communication sont des supports guidés, tels que les câbles UTP, coaxiaux et fibres optiques. Dans ce média, l'expéditeur et le destinataire sont directement connectés et l'information est envoyée (guidée) à travers elle.

Médias non guidés

L'espace sans fil ou en plein air est considéré comme un média non guidé, car il n'y a pas de connectivité entre l'expéditeur et le destinataire. L'information est diffusée dans les airs, et toute personne y compris le destinataire réel peut recueillir l'information.

3.3.4. CAPACITE DE CANAL

La vitesse de transmission de l'information est censée être la capacité du canal. Nous le considérons comme un débit de données dans le monde numérique. Cela dépend de nombreux facteurs tels que:

- *Bande passante: limite physique des médias sous-jacents.*
- *Taux d'erreur: Réception incorrecte des informations à cause du bruit.*
- *Encodage: Le nombre de niveaux utilisés pour la signalisation.*

3.3.5. MULTIPLEX

Le multiplexage est une technique permettant de mélanger et d'envoyer plusieurs flux de données sur un seul support. Cette technique nécessite un matériel système appelé multiplexeur (MUX) pour multiplexer les flux et les envoyer sur un support, et un démultiplexeur (DMUX) qui prend des informations du support et les distribue vers différentes destinations.

3.3.6. COMMUTATION

La commutation est un mécanisme par lequel les données / informations envoyées de la source vers la destination ne sont pas directement connectées. Les réseaux ont des dispositifs d'interconnexion, qui reçoivent des données provenant de sources directement connectées, stockent des données, les analysent et les transmettent ensuite au prochain dispositif d'interconnexion le plus proche de la destination. La commutation peut être catégorisée comme:

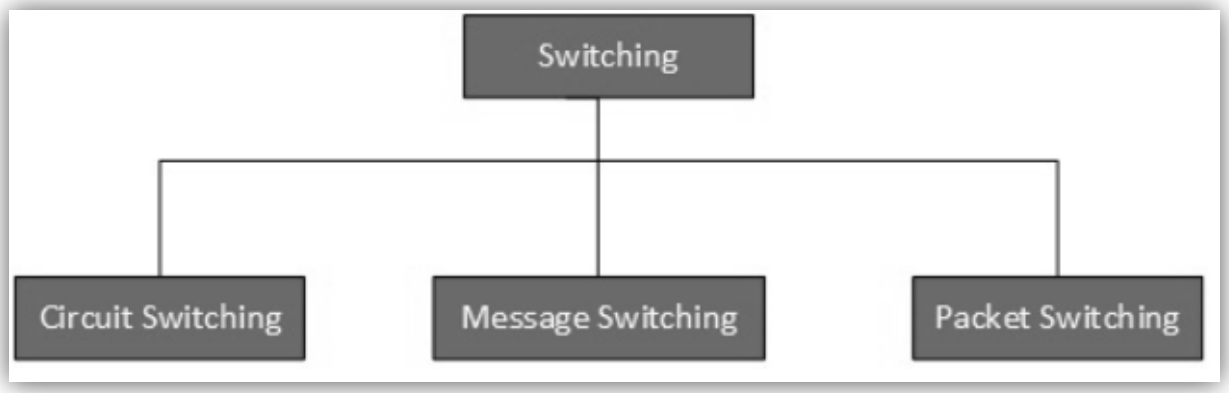


Figure 15 : Commutation

Chapitre 4 : Transmission des données

4.1. INTRODUCTION

Les données ou les informations peuvent être stockées de deux manières, analogiques et numériques. Pour qu'un ordinateur utilise les données, il doit être sous forme numérique discrète.

4.2. TRANSMISSION DIGITALE

Similaire aux données, les signaux peuvent également être sous forme analogique et numérique. Pour transmettre numériquement des données, il faut d'abord les convertir en format numérique.

4.2.1. CONVERSION NUMERIQUE-NUMERIQUE

Cette section explique comment convertir les données numériques en signaux numériques. Cela peut se faire de deux façons: le codage de ligne et le codage par blocs. Pour toutes les communications, le codage de ligne est nécessaire alors que le codage de bloc est facultatif.

4.2.2. CODAGE DE LIGNE

Le processus de conversion de données numériques en signal numérique est dit codage de ligne. Les données numériques se trouvent au format binaire. Il est représenté (stocké) en interne sous forme de séries de 1 et de 0.

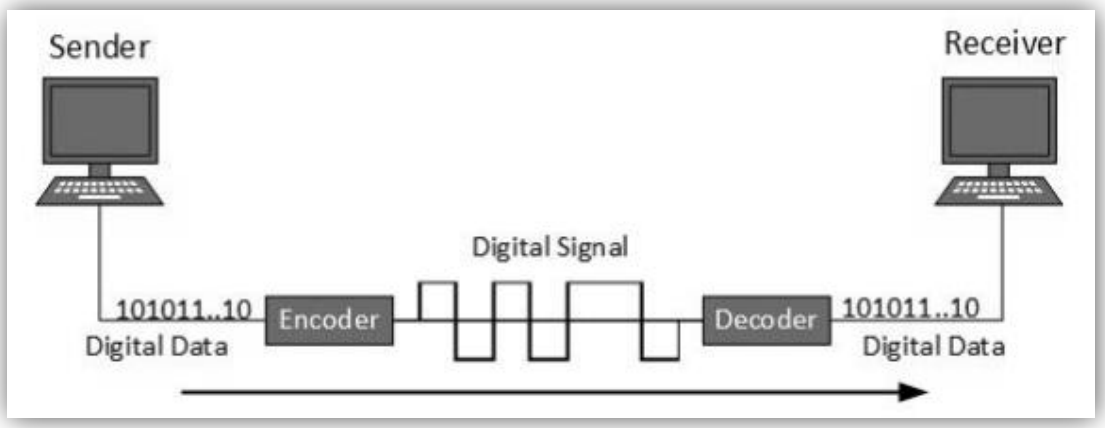


Figure 16 : Le codage des signaux

Le signal numérique est indiqué par un signal discret, qui représente des données numériques. Il existe trois types de systèmes de codage de ligne disponibles :

4.2.3. CODAGE UNIPOLAIRE

Les schémas de codage unipolaires utilisent un niveau de tension unique pour représenter les données. Dans ce cas, pour représenter le binaire 1, une haute tension est transmise et pour représenter 0, aucune tension n'est

transmise. Il est également appelé Unipolar-Non-return-to-zero, car il n'y a pas de condition de repos, c'est-à-dire qu'il représente 1 ou 0.

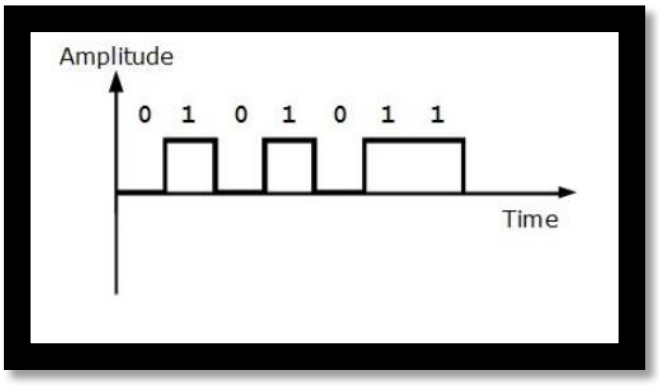


Figure 17 : Schéma de codage unipolaire

4.2.4. CODAGE POLAIRE

Le schéma de codage polaire utilise plusieurs niveaux de tension pour représenter les valeurs binaires. Les codages polaires sont disponibles en quatre types:

Polar non retour à zéro (Polar NRZ)

Il utilise deux niveaux de tension différents pour représenter les valeurs binaires. Généralement, la tension positive représente 1 et la valeur négative représente 0. C'est aussi NRZ car il n'y a pas de condition de repos.

Le schéma NRZ a deux variantes: NRZ-L et NRZ-I.

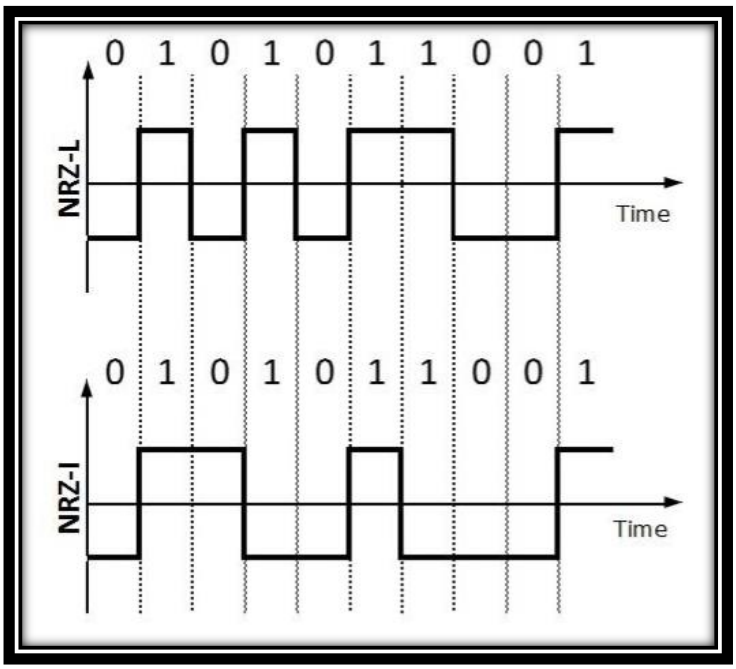


Figure 18 : Schéma de codage polaire

NRZ-L change le niveau de tension quand un bit différent est rencontré tandis que NRZ-I change de tension quand un 1 est rencontré.

Retour à zéro (RZ)

Le problème avec NRZ est que le récepteur ne peut pas conclure quand un bit est terminé et quand le bit suivant est démarré, dans le cas où l'émetteur et l'horloge du récepteur ne sont pas synchronisés.

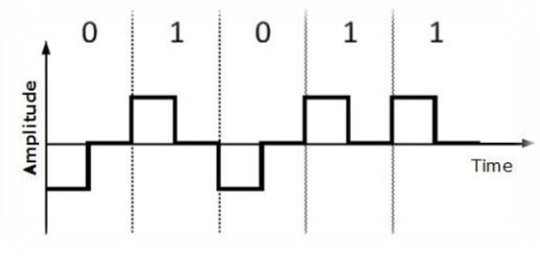


Figure 19 : Schéma de retour à zéro (RZ)

RZ utilise trois niveaux de tension, une tension positive pour représenter 1, une tension négative pour représenter 0 et une tension nulle pour aucun. Les signaux changent pendant les bits et non entre les bits.

Manchester

Ce schéma de codage est une combinaison de RZ et NRZ-L. Le temps de bits est divisé en deux moitiés. Il transite au milieu du bit et change de phase lorsqu'un bit différent est rencontré.

Différentiel Manchester

Ce schéma de codage est une combinaison de RZ et NRZ-I. Il transite également au milieu du bit mais ne change de phase que lorsque 1 est rencontré.

4.2.5. CODAGE BIPOLAIRE

L'encodage bipolaire utilise trois niveaux de tension, positif, négatif et zéro. Zéro tension représentent binaire 0 et le bit 1 est représenté en modifiant les tensions positives et négatives.

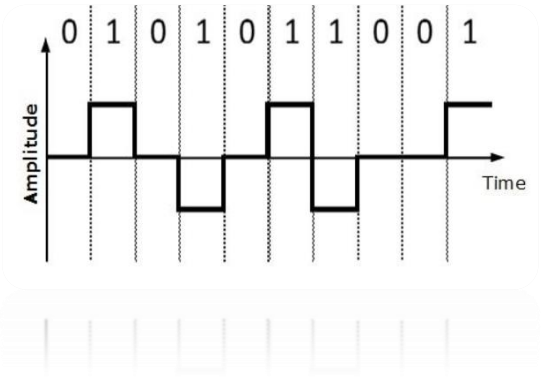


Figure 20 : Schéma de codage bipolaire

4.2.6. CODAGE EN BLOC

Pour garantir la précision de la trame de données reçue, des bits redondants sont utilisés. Par exemple, dans la parité paire, un bit de parité est ajouté pour que le nombre de 1 dans la trame soit pair.

De cette façon, le nombre de bits d'origine est augmenté. C'est ce qu'on appelle le codage par bloc. Le codage de bloc est représenté par une notation de barre oblique, mB / nB. Moyens, un bloc de m bits est substitué par un bloc de n bits où n> m. Le codage en bloc implique trois étapes :

1. Division

2. Substitution

3. Combinaison.

Une fois le codage par bloc effectué, il est codé en ligne pour la transmission.

4.2.7. CONVERSION ANALOGIQUE-NUMERIQUE

Les microphones créent une voix analogique et la caméra crée des vidéos analogiques, qui sont traitées en données analogiques. Pour transmettre ces données analogiques sur des signaux numériques, nous avons besoin d'une conversion analogique-numérique.

Les données analogiques sont un flux continu de données sous forme d'onde tandis que les données numériques sont discrètes. Pour convertir les ondes analogiques en données numériques, nous utilisons la modulation par impulsions codées (PCM).

PCM est l'une des méthodes les plus couramment utilisées pour convertir les données analogiques sous forme numérique. Cela implique trois étapes:

- *Échantillonnage*
- *Quantification*
- *Encodage.*

4.2.8. ÉCHANTILLONNAGE

Le signal analogique est échantillonné chaque intervalle T. Le facteur le plus important dans l'échantillonnage est la vitesse à laquelle le signal analogique est échantillonné. Selon le théorème de Nyquist, le taux d'échantillonnage doit être au moins deux fois supérieur à la fréquence la plus élevée du signal.

4.2.9. QUANTIFICATION

L'échantillonnage donne une forme discrète de signal analogique continu. Chaque motif discret montre l'amplitude du signal analogique à cette instance. La quantification est terminée entre la valeur d'amplitude maximale et la valeur d'amplitude minimale. La quantification est une approximation de la valeur analogique instantanée.

4.2.10. ENCODAGE

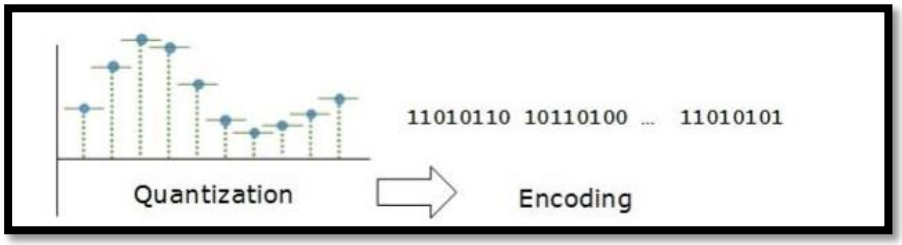


Figure 21 : Schéma d'encodage

En codage, chaque valeur approximée est ensuite convertie en format binaire.

4.2.11. MODES DE TRANSMISSION

Le mode de transmission décide comment les données sont transmises entre deux ordinateurs. Les données binaires sous forme de 1 et de 0 peuvent être envoyées dans deux modes différents: Parallèle et Série.

Transmission parallèle

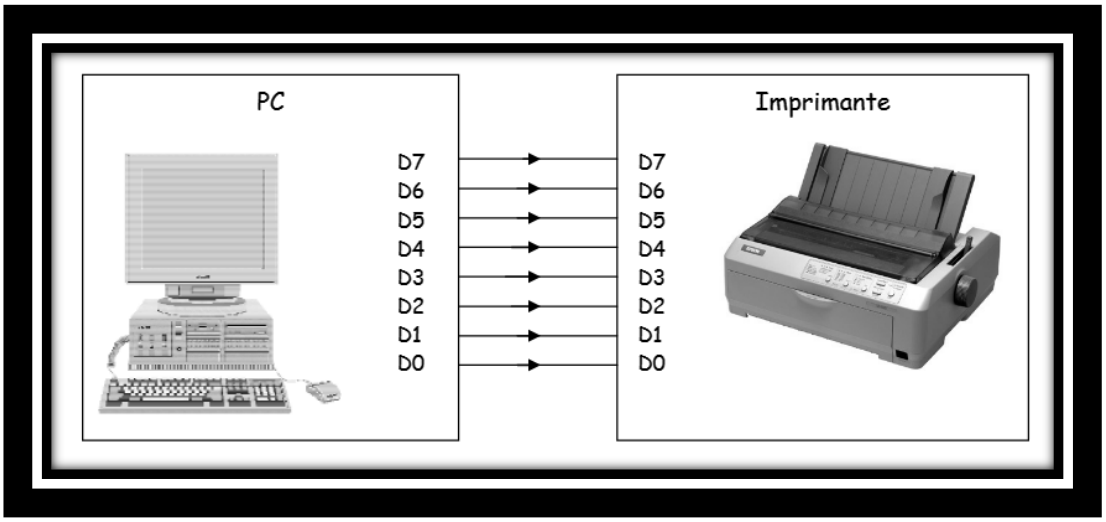


Figure 22 : Mode de transmission en parallèle

Les bits binaires sont organisés en groupes de longueur fixe. Expéditeur et destinataire sont connectés en parallèle avec le nombre égal de lignes de données. Les deux ordinateurs distinguent les lignes de données d'ordre élevé et d'ordre inférieur. L'expéditeur envoie tous les bits à la fois sur toutes les lignes. Parce que les lignes de données sont égales au nombre de bits dans un groupe ou trame de données, un groupe complet de bits (trame de données) est envoyé en une fois. L'avantage de la transmission parallèle est la vitesse élevée et le désavantage est le coût des fils, car il est égal au nombre de bits envoyés en parallèle.

Transmission en série

En transmission série, les bits sont envoyés les uns après les autres en file d'attente. La transmission en série ne nécessite qu'un seul canal de communication.

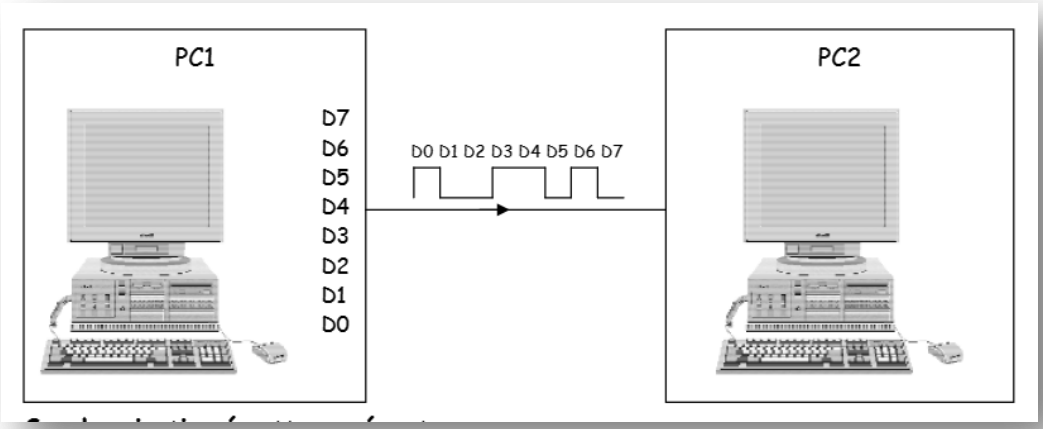


Figure 23 : Mode de transmission en série

La transmission en série peut être asynchrone ou synchrone.

Chapitre 4 : Transmission des données

Transmission série asynchrone

Il est nommé ainsi parce qu'il n'y a pas d'importance de timing. Les bits de données ont un motif spécifique et aident le récepteur à reconnaître les bits de données de début et de fin. Par exemple, un 0 est préfixé sur chaque octet de données et un ou plusieurs 1 sont ajoutés à la fin. Deux trames de données continues (octets) peuvent avoir un écart entre elles.

Transmission série synchrone

La synchronisation dans la transmission synchrone a de l'importance car il n'y a pas de mécanisme suivi pour reconnaître les bits de données de début et de fin. Il n'y a pas de modèle ou de méthode de préfixe / suffixe. Les bits de données sont envoyés en mode rafale sans maintenir l'écart entre les octets (8 bits). Une seule rafale de bits de données peut contenir un nombre d'octets. Par conséquent, le timing devient très important.

Il appartient au récepteur de reconnaître et de séparer les bits en octets. L'avantage de la transmission synchrone est une vitesse élevée, et il n'y a pas de surcharge des bits d'en-tête et de pied de page supplémentaires comme dans la transmission asynchrone.

4.3. TRANSMISSION ASYNCHRONE

Pour envoyer les données numériques sur un support analogique, il doit être converti en signal analogique. Il peut y avoir deux cas selon le formatage des données.

Bandpass: Les filtres sont utilisés pour filtrer et transmettre les fréquences d'intérêt. Une bande passante est une bande de fréquences qui peut passer le filtre.

Passe-bas: passe-bas est un filtre qui transmet les signaux de basse fréquence.

Lorsque les données numériques sont converties en un signal analogique passe-bande, on parle de conversion numérique-analogique. Lorsque le signal analogique passe-bas est converti en signal analogique passe-bande, il est appelé conversion analogique-analogique.

4.3.1. CONVERSION NUMERIQUE-ANALOGIQUE

Lorsque les données d'un ordinateur sont envoyées à un autre via une porteuse analogique, elles sont d'abord converties en signaux analogiques. Les signaux analogiques sont modifiés pour refléter les données numériques.

Un signal analogique est caractérisé par son amplitude, sa fréquence et sa phase. Il existe trois types de conversions numérique-analogique :

Modulation par déplacement d'amplitude

Dans cette technique de conversion, l'amplitude du signal porteur analogique est modifiée pour refléter les données binaires.

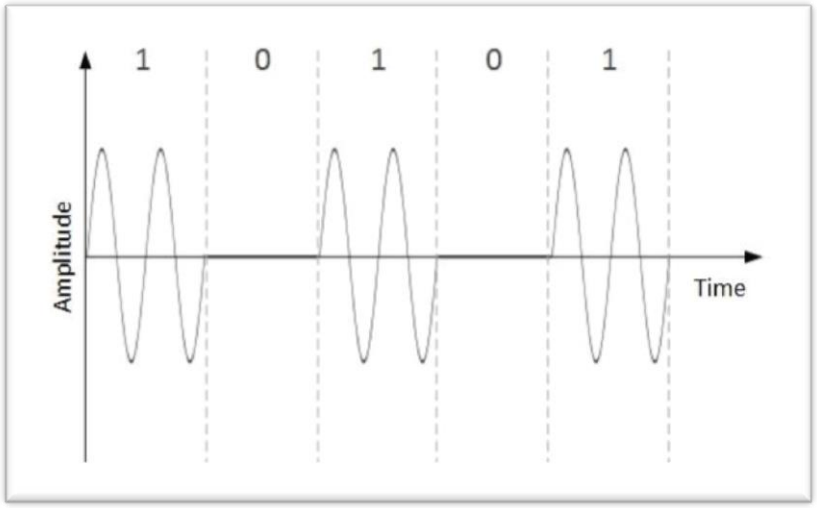


Figure 24 : Technique de modulation (déplacement d'amplitude)

Lorsque les données binaires représentent le chiffre 1, l'amplitude est maintenue; sinon, il est mis à 0. La fréquence et la phase restent les mêmes que dans le signal porteur d'origine.

Modulation par déplacement de fréquence

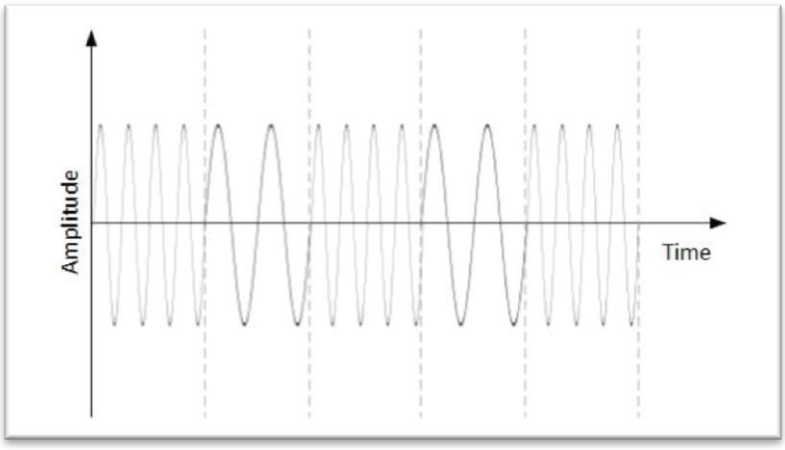


Figure 25 : Technique de modulation (déplacement de fréquence)

Cette technique utilise deux fréquences, f1 et f2. L'un d'eux, par exemple f1, est choisi pour représenter le chiffre binaire 1 et l'autre est utilisé pour représenter le chiffre binaire 0. L'amplitude et la phase de l'onde porteuse sont toutes deux maintenues intactes.

Modulation par déplacement de phase

Dans ce schéma de conversion, la phase du signal porteur d'origine est modifiée pour refléter les données binaires.

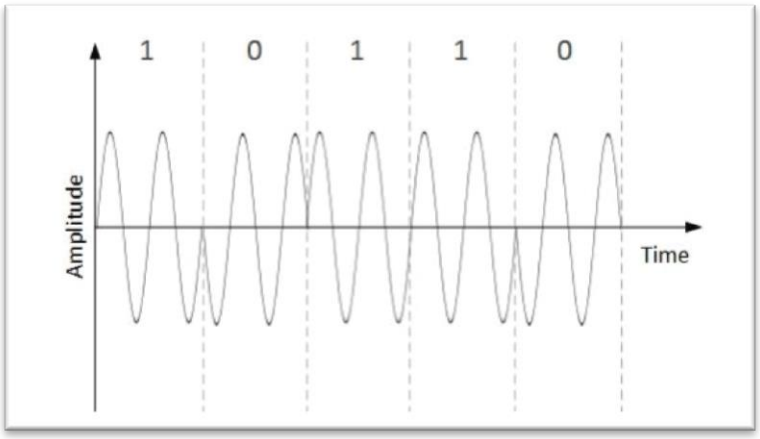


Figure 26 : Technique de modulation (déplacement de phase)

Lorsqu'un nouveau symbole binaire est rencontré, la phase du signal est modifiée. L'amplitude et la fréquence du signal porteur d'origine sont conservées intactes.

Modulation par déplacement de phase de quadrature

QPSK modifie la phase pour refléter deux chiffres binaires à la fois. Ceci est fait en deux phases différentes. Le flux principal de données binaires est divisé également en deux sous-flux. Les données série sont converties en

parallèle dans les deux sous-flux, puis chaque flux est converti en signal numérique en utilisant la technique NRZ. Plus tard, les deux signaux numériques sont fusionnés ensemble.

4.3.2. CONVERSION ANALOGIQUE-ANALOGIQUE

Les signaux analogiques sont modifiés pour représenter les données analogiques. Cette conversion est également connue sous le nom de modulation analogique. Une modulation analogique est requise lorsque la bande passante est utilisée. La conversion analogique-analogique peut être effectuée de trois façons:

La modulation d'amplitude

Dans cette modulation, l'amplitude du signal porteur est modifiée pour refléter les données analogiques.

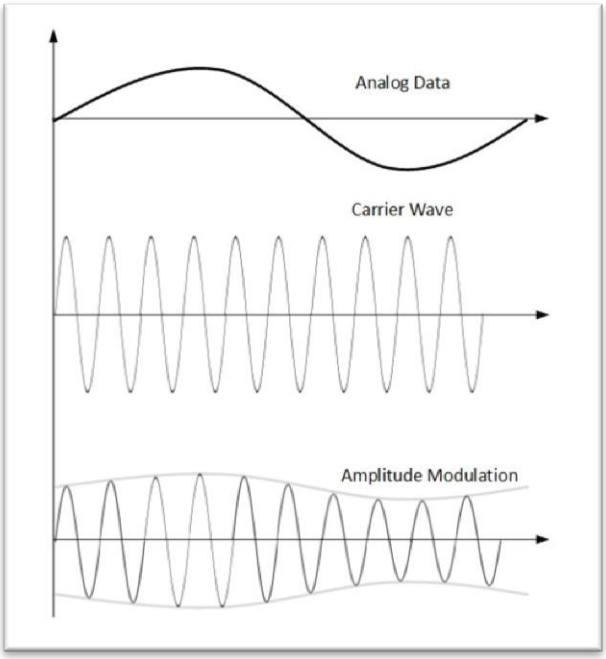


Figure 27 : Schéma de la modulation d'amplitude

La modulation d'amplitude est mise en oeuvre au moyen d'un multiplicateur. L'amplitude du signal de modulation (données analogiques) est multipliée par l'amplitude de la fréquence porteuse, qui reflète alors les données analogiques.

La fréquence et la phase du signal porteur restent inchangées.

Modulation de fréquence

Dans cette technique de modulation, la fréquence du signal de porteuse est modifiée pour refléter la variation des niveaux de tension du signal de modulation (données analogiques).

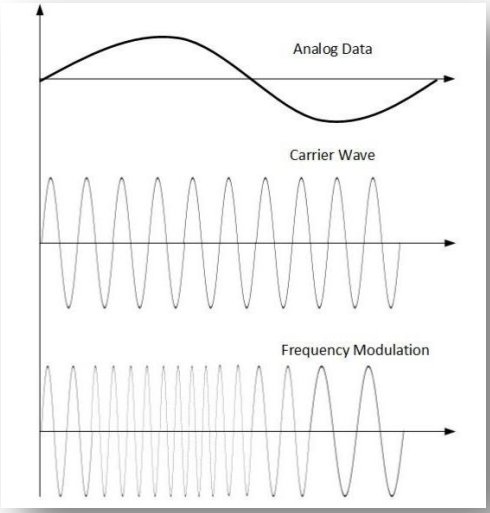


Figure 28 : Schéma de la modulation de fréquence

L'amplitude et la phase du signal porteur ne sont pas modifiées.

Phase de modulation

Dans la technique de modulation, la phase du signal porteur est modulée afin de refléter le changement de tension (amplitude) du signal de données analogique.

La modulation de phase est pratiquement similaire à la modulation de fréquence, mais en modulation de phase, la fréquence du signal porteur n'est pas augmentée. La fréquence de la porteuse est modifiée (rendue dense et éparse) pour refléter le changement de tension dans l'amplitude du signal de modulation.

4.4. MEDIA DE TRANSMISSION

Le média de transmission n'est rien d'autre que le support physique sur lequel la communication a lieu dans les réseaux informatiques.

4.4.1. MEDIAS MAGNETIQUES

L'un des moyens les plus pratiques de transférer des données d'un ordinateur à un autre, même avant la mise en réseau, consistait à les sauvegarder sur certains supports de stockage et à les transférer physiquement d'une station à une autre. Bien que cela puisse sembler à l'ancienne mode dans le monde d'Internet haute vitesse d'aujourd'hui, mais lorsque la taille des données est énorme, les médias magnétiques entrent en jeu.

Par exemple, une banque doit gérer et transférer d'énormes données de son client, qui en garde une copie de sauvegarde dans un endroit éloigné géographiquement pour des raisons de sécurité et pour éviter les calamités incertaines. Si la banque doit stocker ses énormes données de sauvegarde, son transfert via Internet n'est pas réalisable. Les liens WAN peuvent ne pas supporter une telle vitesse. Même s'ils le font le coût est trop élevé pour se permettre. Dans ces cas, la sauvegarde des données est stockée sur des bandes magnétiques ou des disques magnétiques, puis déplacée physiquement à des endroits éloignés.

4.4.2. PAIRE DE CABLES ENROULES

Un câble à paires torsadées est constitué de deux fils de cuivre isolés en plastique torsadés ensemble pour former un seul média. Sur ces deux fils, un seul porte le signal réel et un autre est utilisé pour la référence au sol. Les torsions entre les fils sont utiles pour réduire le bruit (interférence électromagnétique) et la diaphonie.

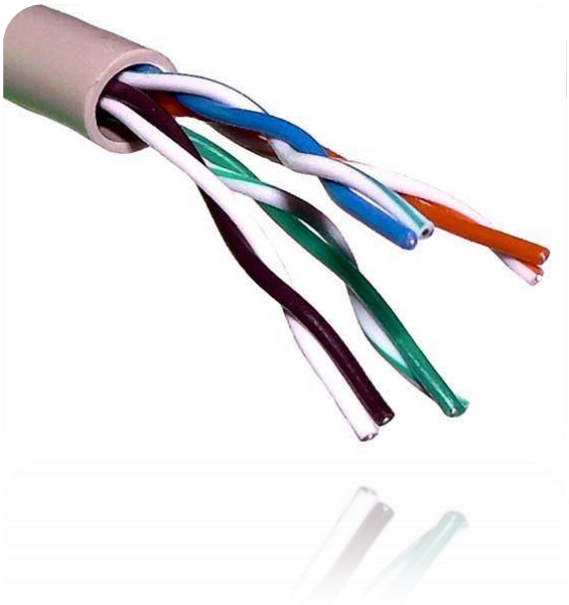


Figure 29 : La paire torsadée

Il existe deux types de câbles à paire torsadée:

- *Câble à paires torsadées blindées (STP)*
- *Câble à paires torsadées non blindées (UTP)*

Les câbles STP sont livrés avec une paire de fils torsadés recouverte d'une feuille de métal. Cela le rend plus indifférent au bruit et à la diaphonie.

UTP a sept catégories, chacune adaptée à un usage spécifique. Dans les réseaux informatiques, Cat5,

Les câbles Cat-5e et Cat-6 sont principalement utilisés. Les câbles UTP sont connectés par des connecteurs J45.

Câble coaxial

Le câble coaxial a deux fils de cuivre. Le fil d'âme se trouve au centre et il est fait de conducteur solide. Le noyau est enfermé dans une gaine isolante. Le second fil est enroulé autour de la gaine et celui-ci est à son tour enveloppé par une gaine isolante. Tout est recouvert de plastique.

Figure 30 : Câble Coaxial

En raison de sa structure, le câble coaxial est capable de transporter des signaux à haute fréquence que celui du câble à paire torsadée. La structure enveloppée fournit une bonne protection contre le bruit et les interférences. Les câbles coaxiaux offrent des débits de bande passante élevés allant jusqu'à 450 Mbps.

Il existe trois catégories de câbles coaxiaux, à savoir le RG-59 (câblodistribution), le RG-58 (Ethernet mince) et le RG-11 (Ethernet épais). RG est l'abréviation de Radio Government. Les câbles sont connectés en utilisant le connecteur BNC et le BNC-T. BNC terminator est utilisé pour terminer le fil aux extrémités.

4.4.3. LES LIGNES ELECTRIQUES

La communication par courant porteur (PLC) est une technologie de couche 1 (couche physique) qui utilise des câbles d'alimentation pour transmettre des signaux de données. Dans l'automate, les données modulées sont envoyées sur les câbles. Le récepteur à l'autre bout module et interprète les données.

Comme les lignes électriques sont largement déployées, l'API peut contrôler et surveiller tous les appareils alimentés. L'automate fonctionne en semi-duplex.

Il existe deux types d'automates :

- *PLC à bande étroite*
- *PLC à large bande*

L'automate à bande étroite offre des débits de données inférieurs à 100 kbps, car ils fonctionnent à des fréquences plus basses (3-5000 kHz). Ils peuvent être répartis sur plusieurs kilomètres.

L'API à large bande fournit des débits de données supérieurs jusqu'à 100 Mbits / s et fonctionne à des fréquences plus élevées (1,8 à 250 MHz). Ils ne peuvent pas être aussi étendus que Narrowband PLC.

4.4.4. LA FIBRE OPTIQUE

La fibre optique fonctionne sur les propriétés de la lumière. Lorsque le rayon lumineux atteint un angle critique, il a tendance à réfracter à 90 degrés. Cette propriété a été utilisée en fibre optique. Le noyau du câble de fibre optique est fait de verre ou de plastique de haute qualité. D'une extrémité de la lumière est émise, il voyage à travers elle et à l'autre extrémité détecteur de lumière détecte le flux de lumière et le convertit en données électriques.

La fibre optique fournit le mode de vitesse le plus élevé. Il existe deux modes, l'un est une fibre monomode et l'autre est une fibre multimode. Une fibre monomode peut porter un seul rayon de lumière alors que le multimode est capable de transporter de multiples faisceaux de lumière.

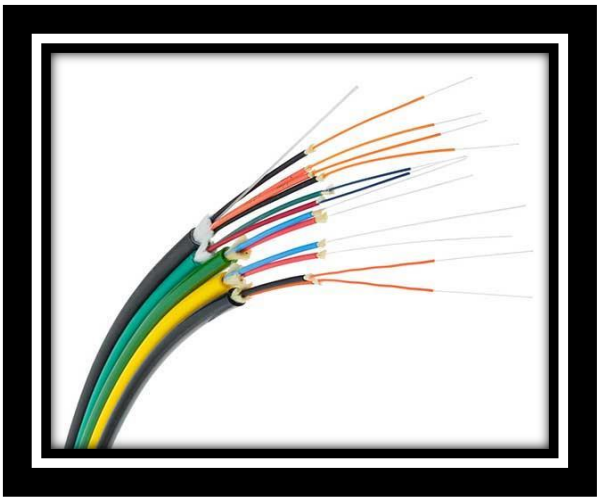


Figure 31 : Fibre Optique

La fibre optique vient également dans des capacités unidirectionnelles et bidirectionnelles. Pour connecter et accéder à la fibre optique, des connecteurs spéciaux sont utilisés. Ceux-ci peuvent être le canal d'abonné (SC), l'extrémité droite (ST) ou le MT-RJ.

4.5. TRANSMISSION SANS FIL

La transmission sans fil est une forme de média non-guidé. La communication sans fil n'implique aucun lien physique établi entre deux appareils ou plus, communiquant sans fil. Les signaux sans fil sont diffusés dans l'air et sont reçus et interprétés par des antennes appropriées.

Lorsqu'une antenne est connectée au circuit électrique d'un ordinateur ou d'un appareil sans fil, elle convertit les données numériques en signaux sans fil et se propage partout dans sa gamme de fréquences. Le récepteur à l'autre extrémité reçoit ces signaux et les convertit en données numériques.

Une petite partie du spectre électromagnétique peut être utilisée pour la transmission sans fil.

4.5.1. TRANSMISSION PAR RADIO

La fréquence radio est plus facile à générer et en raison de sa grande longueur d'onde, elle peut pénétrer à travers les murs et les structures. Les ondes radio peuvent avoir une longueur d'onde de 1 mm à 100 000 km et une fréquence allant de 3 Hz (extrêmement basse fréquence) à 300 GHz (extrêmement haute fréquence). Les fréquences radio sont subdivisées en six bandes.

Les ondes radioélectriques à des fréquences plus basses peuvent traverser les murs, tandis que les fréquences radioélectriques plus élevées peuvent se déplacer en ligne droite et rebondir. La puissance des ondes de basse fréquence diminue brusquement car elles couvrent de longues distances. Les ondes radio à haute fréquence ont plus de puissance. Les basses fréquences telles que les bandes VLF, LF, MF peuvent voyager sur le sol jusqu'à 1000 kilomètres, sur la surface de la Terre.

Les ondes radioélectriques des hautes fréquences sont susceptibles d'être absorbées par la pluie et d'autres obstacles. Ils utilisent l'ionosphère de l'atmosphère terrestre. Les ondes radio à haute fréquence telles que les bandes HF et VHF sont réparties vers le haut. Quand ils atteignent l'ionosphère, ils sont réfractés à la terre.

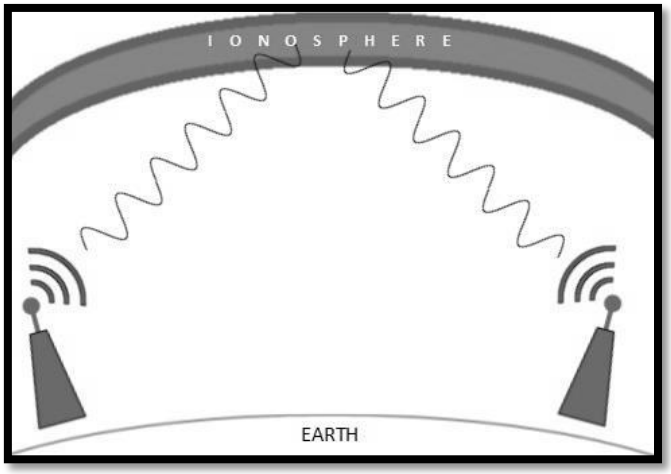


Figure 32: Schéma de transmission d'ondes radioélétriques

4.5.2. TRANSMISSION PAR MICRO-ONDES

Les ondes électromagnétiques au-dessus de 100 MHz ont tendance à se déplacer en ligne droite et les signaux qui les traversent peuvent être émis en envoyant ces ondes vers une station particulière. Parce que les micro-ondes voyagent dans des lignes droites, l'émetteur et le récepteur doivent être alignés pour être strictement en ligne de mire.

Les micro-ondes peuvent avoir une longueur d'onde allant de 1 mm à 1 mètre et une fréquence allant de 300 MHz à 300 GHz. Les antennes hyperfréquences concentrent les ondes en en faisant un faisceau. Comme le montre l'image ci-dessus, plusieurs antennes peuvent être alignées pour atteindre plus loin. Les micro-ondes ont des fréquences plus élevées et ne pénètrent pas dans la paroi comme des obstacles. La transmission par micro-ondes dépend fortement des conditions météorologiques et de la fréquence d'utilisation.

4.5.3. TRANSMISSION INFRAROUGE

L'onde infrarouge se situe entre le spectre de la lumière visible et les micro-ondes. Il a la longueur d'onde de 700nm à 1mm et la gamme de fréquence de 300GHz à 430THz. L'onde infrarouge est utilisée à des fins de communication à très courte distance telles que la télévision et sa télécommande. L'infrarouge se déplace en ligne droite, par conséquent il est directionnel par nature. En raison de la plage de fréquence élevée, l'infrarouge ne peut pas traverser des obstacles ressemblant à des murs.

4.5.4. TRANSMISSION DE LA LUMIERE (Li-FI)

Le spectre électromagnétique le plus élevé pouvant être utilisé pour la transmission de données est la signalisation lumineuse ou optique. Ceci est réalisé au moyen de LASER.

En raison de la fréquence des utilisations de la lumière, il a tendance à voyager strictement en ligne droite. Par conséquent, l'expéditeur et le destinataire doivent être dans la ligne de mire. Parce que la transmission laser est unidirectionnelle, aux deux extrémités de la communication, le laser et le photo-détecteur doit être installé. Le

faisceau laser est généralement de 1mm de large, c'est donc un travail de précision pour aligner deux récepteurs lointains pointant chacun vers une source de lasers.

Le laser fonctionne comme Tx (émetteur) et les photo-détecteurs fonctionnent comme Rx (récepteur).

Les lasers ne peuvent pas pénétrer les obstacles tels que les murs, la pluie et le brouillard épais. De plus, le faisceau laser est déformé par le vent, la température de l'atmosphère ou la variation de température sur le trajet.

Le laser est sûr pour la transmission de données, car il est très difficile d'exploiter un laser de 1 mm de large sans interrompre le canal de communication.

5.1. INTRODUCTION

Le multiplexage est une technique par laquelle différents flux de transmission analogiques et numériques peuvent être traités simultanément sur une liaison partagée. Le multiplexage divise le support haut capacité en un support logique de faible capacité qui est ensuite partagé par différents flux.

5.2. MULTIPLEXAGE

La communication est possible sur les ondes (radiofréquence), en utilisant un support physique (câble) et de la lumière (fibre optique). Tous les supports sont capables de multiplexer.

Lorsque plusieurs expéditeurs tentent d'envoyer sur un seul support, un périphérique appelé Multiplexeur divise le canal physique et en alloue un à chaque. À l'autre extrémité de la communication, un démultiplexeur reçoit des données d'un seul support, les identifie et les envoie à différents récepteurs.

5.2.1. MULTIPLEXAGE PAR REPARTITION EN FREQUENCE

Lorsque le transporteur est la fréquence, FDM est utilisé. FDM est une technologie analogique. FDM divise le spectre ou la bande passante de porteuse dans les canaux logiques et alloue un utilisateur à chaque canal. Chaque utilisateur peut utiliser la fréquence du canal indépendamment et en a un accès exclusif. Tous les canaux sont divisés de telle sorte qu'ils ne se chevauchent pas. Les canaux sont séparés par des bandes de garde. La bande de garde est une fréquence qui n'est utilisée par aucun canal.

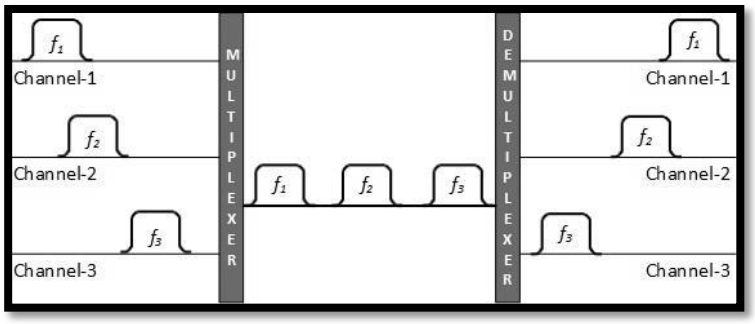


Figure 33: Schéma de multiplexage par répartition en fréquence

5.2.2. MULTIPLEXAGE PAR REPARTITION DANS LE TEMPS

Le TDM est principalement appliqué aux signaux numériques, mais peut également être appliqué aux signaux analogiques. Dans TDM, le canal partagé est divisé entre ses utilisateurs au moyen d'un intervalle de temps. Chaque utilisateur peut transmettre des données dans l'intervalle de temps fourni uniquement. Les signaux numériques sont divisés en trames, équivalant à un intervalle de temps, c'est-à-dire une trame d'une taille optimale qui peut être transmise dans un créneau temporel donné.

TDM fonctionne en mode synchronisé. Les deux extrémités, c'est-à-dire le multiplexeur et le dé-multiplexeur, sont synchronisées en temps opportun, et les deux commutent au canal suivant simultanément.

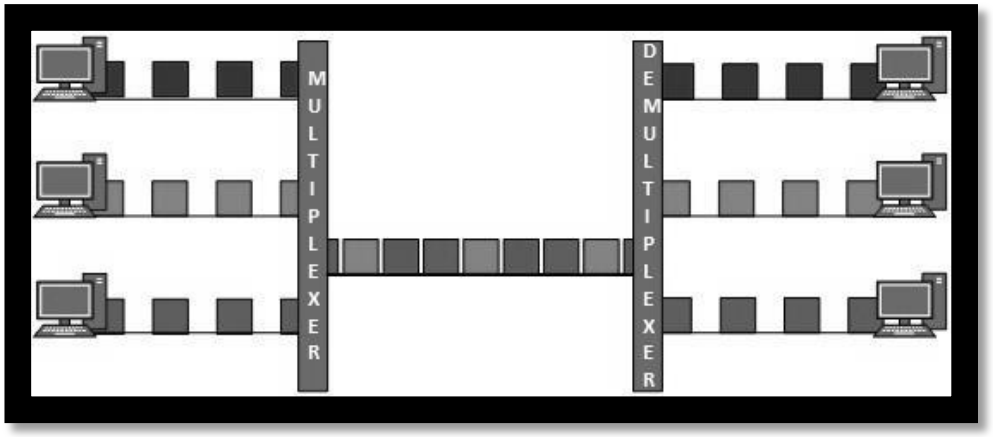


Figure 34 : Schéma de multiplexage par répartition dans le temps

Lorsque le canal A transmet sa trame à une extrémité, le démultiplexeur fournit le média au canal A à l'autre extrémité. Dès que le créneau temporel du canal A expire, ce côté passe au canal B. À l'autre extrémité, le dé-multiplexeur fonctionne de manière synchronisée et fournit le média au canal B. Les signaux provenant de canaux différents parcourent le chemin de manière entrelacée.

5.2.3. MULTIPLEXAGE PAR REPARTITION EN LONGUEUR D'ONDE

La lumière a différentes longueurs d'onde (couleurs). En mode fibre optique, plusieurs signaux de porteuse optique sont multiplexés dans une fibre optique en utilisant différentes longueurs d'onde. C'est une technique de multiplexage analogique et elle est faite conceptuellement de la même manière que FDM mais utilise la lumière comme signaux.

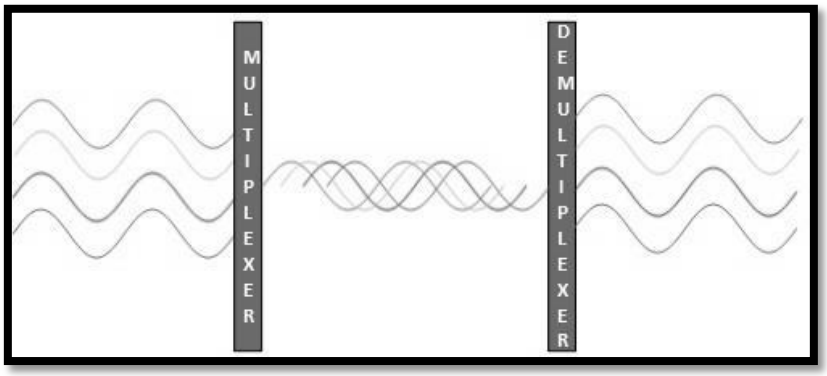


Figure 35 : Schéma de multiplexage par répartition en longueur d'onde

En outre, sur chaque longueur d'onde, le multiplexage par répartition dans le temps peut être incorporé pour recevoir plus de signaux de données.

5.2.4. MULTIPLEXAGE PAR REPARTITION DE CODE

Plusieurs signaux de données peuvent être transmis sur une seule fréquence en utilisant le multiplexage par répartition en code. FDM divise la fréquence en canaux plus petits mais CDM permet à ses utilisateurs de disposer d'une bande passante complète et de transmettre des signaux tout le temps en utilisant un code unique. CDM utilise des codes orthogonaux pour diffuser les signaux.

Chaque station est assignée avec un code unique, appelé puce. Les signaux voyagent avec ces codes indépendamment, à l'intérieur de toute la bande passante. Le récepteur connaît à l'avance le signal de code à puce qu'il doit recevoir.

5.3. SWITCHING

La commutation est un processus de transfert de paquets arrivant d'un port vers un port menant vers la destination. Lorsque les données arrivent sur un port, elles s'appellent ingress, et lorsque les données quittent un port ou disparaissent, elles s'appellent egress. Un système de communication peut inclure le nombre de commutateurs et de nœuds. Au niveau général, la commutation peut être divisée en deux catégories principales:

- ✓ *Sans connexion: les données sont transférées au nom des tables de transfert. Aucune prise de contact préalable n'est requise et les accusés de réception sont facultatifs.*
- ✓ *Connexion orientée: Avant de commuter les données à transférer vers la destination, il est nécessaire de préétablir un circuit le long du chemin entre les deux extrémités. Les données sont ensuite transmises sur ce circuit. Une fois le transfert terminé, les circuits peuvent être conservés pour une utilisation future ou peuvent être immédiatement désactivés.*

5.3.1. COMMUTATION DE CIRCUIT [4]

Lorsque deux nœuds communiquent entre eux sur un chemin de communication dédié, on parle de commutation de circuit. Il existe un besoin d'itinéraire prédéfini à partir duquel les données circulent et aucune autre donnée n'est autorisée. En commutation de circuit pour transférer les données, le circuit doit être établi de sorte que le transfert de données puisse avoir lieu.

Les circuits peuvent être permanents ou temporaires. Les applications qui utilisent la commutation de circuit peuvent devoir passer par trois phases:

- ✓ *Établir un circuit*
- ✓ *Transférer les données*
- ✓ *Déconnectez le circuit*

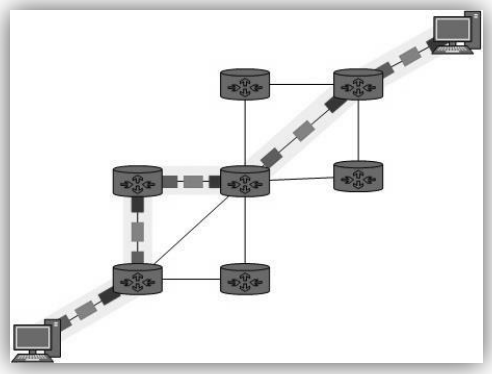


Figure 36 : Commutation de circuit

La commutation de circuits a été conçue pour des applications vocales. Le téléphone est le meilleur exemple de commutation de circuit. Avant qu'un utilisateur puisse passer un appel, un chemin virtuel entre l'appelant et l'appelé est établi sur le réseau.

5.3.2. COMMUTATION DE MESSAGE

Cette technique se situait quelque part au milieu de la commutation de circuits et de la commutation de paquets. Dans la commutation de messages, le message entier est traité comme une unité de données et est commuté / transféré dans son intégralité.

Un commutateur travaillant sur la commutation de messages reçoit d'abord le message entier et le met en mémoire tampon jusqu'à ce qu'il y ait des ressources disponibles pour le transférer au saut suivant. Si le saut suivant n'a pas assez de ressources pour prendre en charge les messages de grande taille, le message est stocké et le commutateur attend.

Cette technique a été considérée comme un substitut à la commutation de circuit. Comme dans la commutation de circuit, le chemin entier est bloqué pour deux entités seulement. La commutation de messages est remplacée par la commutation de paquets. La commutation de messages présente les inconvénients suivants:

- *Chaque commutateur en transit a besoin d'un espace de stockage suffisant pour recevoir le message entier.*
- *En raison de la technique de stockage et retransmission et des attentes incluses jusqu'à ce que des ressources soient disponibles, la commutation des messages est très lente.*
- *La commutation de messages n'était pas une solution pour le streaming des médias et des applications en temps réel.*

5.3.3. COMMUTATION DE PAQUETS

Les lacunes de la commutation de messages ont donné naissance à une idée de la commutation de paquets. Le message entier est décomposé en plus petits morceaux appelés paquets. L'information de commutation est ajoutée dans l'en-tête de chaque paquet et transmise indépendamment.

Il est plus facile pour les périphériques de mise en réseau intermédiaires de stocker des paquets de petite taille et ils ne prennent pas beaucoup de ressources sur le chemin de support ou dans la mémoire interne des commutateurs.

La commutation de paquets améliore l'efficacité de la ligne car les paquets provenant de plusieurs applications peuvent être multiplexés sur l'opérateur. L'Internet utilise la technique de commutation de paquets. La commutation de paquets permet à l'utilisateur de différencier les flux de données en fonction des priorités. Les paquets sont stockés et transmis selon leur priorité afin de fournir une qualité de service.

Chapitre 6 : Couche OSI I

6.1. INTRODUCTION

La couche de liaison de données est la deuxième couche du modèle en couches OSI. Cette couche est l'une des couches les plus complexes et a des fonctionnalités et des responsabilités complexes. La couche de liaison de données cache les détails du matériel sous-jacent et représente elle-même la couche supérieure comme moyen de communication.

6.2. INTRODUCTION DE COUCHE DE LIAISON DE DONNÉES

Couche de liaison de données fonctionne entre deux hôtes qui sont directement connectés dans un certain sens. Cette connexion directe pourrait être point à point ou diffusée. Les systèmes sur le réseau de diffusion sont censés être sur le même lien. Le travail de couche de liaison de données a tendance à devenir plus complexe lorsqu'il s'agit de plusieurs hôtes sur un seul domaine de collision.

La couche de liaison de données est chargée de convertir le flux de données en signaux bit par bit et de les envoyer sur le matériel sous-jacent. Au niveau de la réception, la couche de liaison de données récupère les données du matériel qui sont sous la forme de signaux électriques, les assemble dans un format de trame reconnaissable et transmet à la couche supérieure.

La couche de liaison de données comporte deux sous-couches:

- ✓ *Contrôle de liaison logique: il traite des protocoles, du contrôle de flux et du contrôle des erreurs.*
- ✓ *Contrôle d'accès au média: il traite du contrôle réel des médias.*

6.2.1. FONCTIONNALITE DE LA COUCHE DE LIAISON DE DONNEES

La couche de liaison de données effectue de nombreuses tâches pour le compte de la couche supérieure. Ceux-ci sont:

Encadrement

La couche de liaison de données prélève des paquets à partir de la couche réseau et les encapsule dans des trames. Ensuite, il envoie chaque trame bit par bit sur le matériel. À la fin du récepteur, la couche de liaison de données capte les signaux du matériel et les assemble en images.

Adressage

La couche de liaison de données fournit un mécanisme d'adressage matériel de couche 2. L'adresse matérielle est supposée être unique sur le lien. Il est codé dans le matériel au moment de la fabrication.

Synchronisation

Lorsque des trames de données sont envoyées sur le lien, les deux machines doivent être synchronisées pour que le transfert ait lieu.

Contrôle d'erreur

Parfois, les signaux peuvent avoir rencontré un problème en transition et les bits sont inversés. Ces erreurs sont détectées et ont tenté de récupérer les bits de données réels. Il fournit également un mécanisme de rapport d'erreurs à l'expéditeur.

Contrôle de flux

Les stations sur le même lien peuvent avoir une vitesse ou une capacité différente. La couche de liaison de données assure un contrôle de flux qui permet à la machine d'échanger des données à la même vitesse.

Multi-accès

Lorsque l'hôte sur le lien partagé essaie de transférer les données, il a une forte probabilité de collision. La couche de liaison de données fournit un mécanisme tel que CSMA / CD pour équiper la capacité d'accéder à un média partagé entre plusieurs systèmes.

6.3. DETECTION ET CORRECTION D'ERREUR

Il existe de nombreuses raisons telles que le bruit, les interférences, etc., qui peuvent aider à corrompre les données pendant la transmission. Les couches supérieures travaillent sur une vue générale de l'architecture du réseau et ne connaissent pas le traitement réel des données matérielles. Par conséquent, les couches supérieures s'attendent à une transmission sans erreur entre les systèmes. La plupart des applications ne fonctionneraient pas normalement si elles recevaient des données erronées. Les applications telles que la voix et la vidéo peuvent ne pas être affectées et avec certaines erreurs, elles peuvent encore fonctionner correctement.

La couche de liaison de données utilise un mécanisme de contrôle d'erreur pour s'assurer que les trames (flux de bits de données) sont transmises avec un certain niveau de précision. Mais pour comprendre comment les erreurs sont contrôlées, il est essentiel de savoir quels types d'erreurs peuvent se produire.

6.3.1. TYPES D'ERREURS

Il peut y avoir trois types d'erreurs:

Single bit error

***Figure 37:** Single bit Error*

Dans un cadre, il n'y a qu'un seul bit, n'importe où, qui est corrompu.

Multiple bits error

Figure 38 : Multiple bit Error

La trame est reçue avec plus d'un bit à l'état corrompu.

Burst error

Figure 39 : Burst Error

Le cadre contient plus de 1 bit consécutif corrompu.

Le mécanisme de contrôle d'erreur peut impliquer deux manières possibles:

- *Détection d'erreur*
- *Correction d'erreur*

6.3.2. DETECTION D'ERREUR

Les erreurs dans les trames reçues sont détectées au moyen de la vérification de parité et du contrôle de redondance cyclique (CRC). Dans les deux cas, peu de bits supplémentaires sont envoyés avec les données réelles pour confirmer que les bits reçus à l'autre extrémité sont identiques à ceux qui ont été envoyés. Si le contre-contrôle à la fin du récepteur échoue, les bits sont considérés comme corrompus.

Contrôle de parité

Un bit supplémentaire est envoyé avec les bits d'origine pour faire le nombre de 1 soit même en cas de parité paire, soit impair en cas de parité impaire.

L'expéditeur lors de la création d'un cadre compte le nombre de 1 dans celui-ci. Par exemple, si la parité paire est utilisée et que le nombre de 1 est pair, alors un bit avec la valeur 0 est ajouté. De cette façon, le nombre de 1 reste pair. Si le nombre de 1 est impair, pour le faire même un peu avec la valeur 1 est ajouté.

Figure 40 : Contrôle de parité

Le récepteur compte simplement le nombre de 1 dans un cadre. Si le nombre de 1 est pair et que la parité est utilisée, la trame est considérée comme non corrompue et est acceptée. Si le nombre de 1 est impair et la parité impaire est utilisée, la trame n'est toujours pas corrompue.

Si un seul bit retourne en transit, le récepteur peut le détecter en comptant le nombre de 1s. Mais lorsque plus d'un bit est erroné, il est très difficile pour le récepteur de détecter l'erreur.

Contrôle de redondance cyclique (CRC)

CRC est une approche différente pour détecter si la trame reçue contient des données valides. Cette technique implique une division binaire des bits de données envoyés. Le diviseur est généré en utilisant des polynômes. L'expéditeur effectue une opération de division sur les bits envoyés et calcule le reste. Avant d'envoyer les bits réels, l'expéditeur ajoute le reste à la fin des bits réels. Les bits de données réels plus le reste sont appelés un mot de code. L'expéditeur transmet des bits de données en tant que mots de code.

À l'autre extrémité, le récepteur effectue une opération de division sur les mots de code en utilisant le même diviseur CRC. Si le reste contient tous les zéros, les bits de données sont acceptés, sinon il est considéré comme il y a une corruption de données en transit.

6.3.3. CORRECTION DES ERREURS

Dans le monde numérique, la correction d'erreur peut être effectuée de deux manières:

Correction d'erreur vers l'arrière

Lorsque le récepteur détecte une erreur dans les données reçues, il demande à l'expéditeur de retransmettre l'unité de données.

Correction d'erreur directe

Lorsque le récepteur détecte une erreur dans les données reçues, il exécute un code de correction d'erreur, ce qui l'aide à récupérer automatiquement et à corriger certains types d'erreurs.

Le premier, Backward Error Correction, est simple et ne peut être utilisé efficacement que lorsque la retransmission n'est pas coûteuse. Par exemple, la fibre optique. Mais en cas de transmission sans fil, la retransmission peut coûter trop cher. Dans ce dernier cas, la correction d'erreur directe est utilisée.

Pour corriger l'erreur dans la trame de données, le récepteur doit savoir exactement quel bit de la trame est corrompu. Pour localiser le bit en erreur, des bits redondants sont utilisés comme bits de parité pour la détection d'erreur. Par exemple, nous prenons des mots ASCII (données 7 bits), alors il pourrait y avoir 8 sortes d'informations dont nous avons besoin: les sept premiers bits pour nous dire quel bit est erroné et un autre pour dire qu'il n'y a pas d'erreur.

Pour m bits de données, r bits redondants sont utilisés. r bits peuvent fournir 2r combinaisons d'informations. Dans m + r mot de code de bit, il est possible que les bits r eux-mêmes puissent être corrompus. Ainsi, le nombre de r bits utilisés doit renseigner sur les emplacements de bits m + r plus les informations sans erreur, c'est-à-dire m + r + 1.

$$2^r \geq m + r + 1$$

6.3.4. CONTRÔLE DE LIAISON DE DONNÉES ET PROTOCOLES

La couche de liaison de données est responsable de la mise en œuvre du mécanisme de contrôle de flux et d'erreurs point à point.

Contrôle de flux

Lorsqu'une trame de données (données de couche 2) est envoyée d'un hôte à un autre sur un seul support, il est nécessaire que l'émetteur et le récepteur fonctionnent à la même vitesse. C'est-à-dire que l'expéditeur envoie à

une vitesse à laquelle le destinataire peut traiter et accepter les données. Que faire si la vitesse (matériel / logiciel) de l'expéditeur ou du récepteur diffère? Si l'expéditeur envoie trop vite, le récepteur peut être surchargé (saturé) et les données peuvent être perdues.

Deux types de mécanismes peuvent être déployés pour contrôler le flux:

Stop and Wait

Ce mécanisme de contrôle de flux force l'expéditeur après l'émission d'une trame de données à s'arrêter et attend jusqu'à ce que l'accusé de réception de la trame de données envoyée soit reçu.

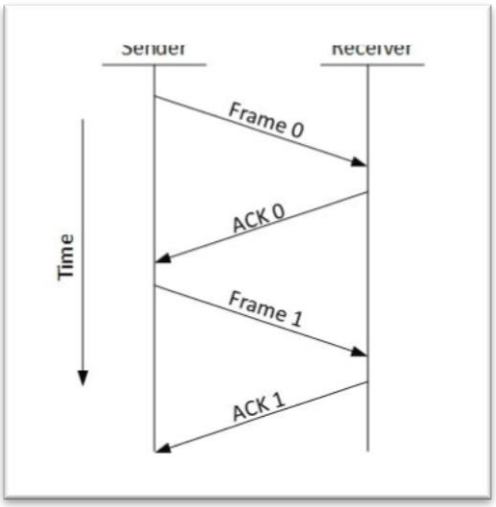


***Figure 41 :** Stop and wait*

Sliding Window

Dans ce mécanisme de contrôle de flux, l'émetteur et le récepteur s'accordent sur le nombre de trames de données après lesquelles l'accusé de réception doit être envoyé. Comme nous l'avons appris, arrêtez et attendez que le mécanisme de contrôle de flux gaspille des ressources, ce protocole essaye de faire usage des ressources sous-jacentes autant que possible.

6.3.5. CONTROLE D'ERREUR

Lorsque la trame de données est transmise, il y a une probabilité que la trame de données soit perdue dans le transit ou qu'elle soit reçue corrompue. Dans les deux cas, le récepteur ne reçoit pas la trame de données correcte et l'expéditeur ne sait rien de toute perte. Dans ce cas, l'expéditeur et le destinataire sont équipés de certains protocoles qui les aident à détecter les erreurs de transit, telles que la perte de trame de données. Par conséquent, soit l'expéditeur retransmet la trame de données, soit le destinataire peut demander à renvoyer la trame de données précédente.

Exigences pour le mécanisme de contrôle d'erreur:

- ***Détection d'erreur:** l'expéditeur et le destinataire, qu'ils soient tous les deux ou non, doivent s'assurer qu'il y a une erreur dans le transit.*
- ***ACK positif:** Lorsque le récepteur reçoit une trame correcte, il doit le reconnaître.*

- ***ACK négatif:*** *lorsque le récepteur reçoit un cadre endommagé ou une trame dupliquée, il renvoie un NACK à l'expéditeur et l'expéditeur doit retransmettre la trame correcte.*
- ***Retransmission:*** *l'expéditeur gère une horloge et définit une période d'expiration. Si un accusé de réception d'une trame de données précédemment transmise n'arrive pas avant le délai, l'expéditeur retransmet la trame, en pensant que la trame ou son accusé de réception est perdu en transit.*

Il existe trois types de techniques disponibles que la couche de liaison de données peut déployer pour contrôler les erreurs par des demandes de répétition automatique (ARQ):

Stop and wait ARQ

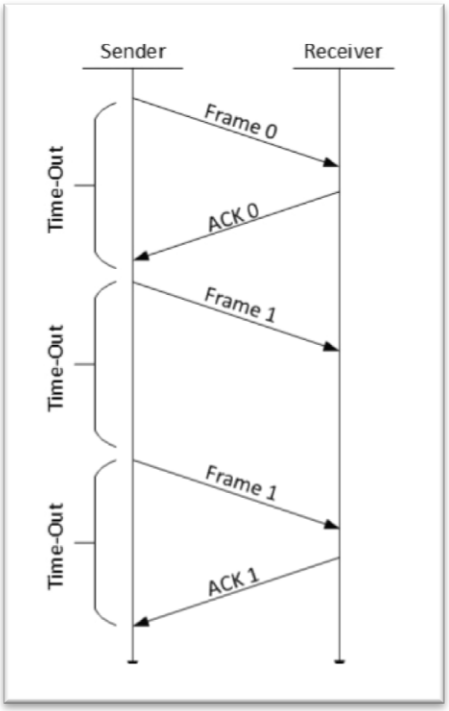


Figure 42 : Stop and Wait ARQ

La transition suivante peut se produire dans ARQ Stop-and-Wait:

- *L'expéditeur gère un compteur de dépassement de délai.*
- *Lorsqu'une trame est envoyée, l'expéditeur démarre le compteur de délai.*
- *Si l'accusé de réception de l'image arrive à temps, l'expéditeur transmet l'image suivante dans la file d'attente.*
- *Si l'accusé de réception ne vient pas à temps, l'expéditeur suppose que le cadre ou son accusé de réception est perdu pendant le transport. L'expéditeur retransmet le cadre et lance le compteur de délai.*
- *Si un accusé de réception négatif est reçu, l'expéditeur retransmet la trame. Go-Back-N ARQ*

Arrêtez et attendez que le mécanisme ARQ n'utilise pas les ressources à leur meilleur niveau. Lorsque l'accusé de réception est reçu, l'expéditeur reste inactif et ne fait rien. Dans la méthode ARQ Go-Back-N, l'expéditeur et le destinataire maintiennent une fenêtre.

La taille de la fenêtre d'envoi permet à l'expéditeur d'envoyer plusieurs trames sans recevoir l'accusé de réception des précédentes. La fenêtre de réception permet au récepteur de recevoir plusieurs trames et de les acquitter. Le récepteur conserve la trace du numéro de séquence de l'image entrante.

Lorsque l'expéditeur envoie toutes les images dans la fenêtre, il vérifie jusqu'à quel numéro de séquence il a reçu un accusé de réception positif. Si toutes les trames sont acquittées positivement, l'expéditeur envoie l'ensemble de trames suivant. Si l'expéditeur constate qu'il a reçu NACK ou n'a reçu aucun ACK pour une trame particulière, il retransmet toutes les trames après lesquelles il ne reçoit aucun accusé de réception positif.

Répétition ARQ sélective

Dans Go-back-N ARQ, il est supposé que le récepteur n'a pas d'espace tampon pour sa taille de fenêtre et doit traiter chaque image comme elle vient. Cela impose à l'expéditeur de retransmettre toutes les trames non reconnues.

En mode ARQ de répétition sélective, le récepteur, tout en gardant la trace des numéros de séquence, met les images en mémoire tampon et envoie NACK uniquement pour les images manquantes ou endommagées.

L'expéditeur dans ce cas envoie uniquement le paquet pour lequel NACK est reçu.

6.4. INTRODUCTION A LA COUCHE RESEAU

La couche 3 du modèle OSI est appelée couche réseau. La couche réseau gère les options relatives à l'adressage de l'hôte et du réseau, à la gestion des sous-réseaux et à l'inter réseautage.

La couche réseau prend la responsabilité du routage des paquets de la source à la destination à l'intérieur ou à l'extérieur d'un sous-réseau. Deux sous-réseaux différents peuvent avoir des schémas d'adressage différents ou des types d'adressage non compatibles. Même avec les protocoles, deux sous-réseaux différents peuvent fonctionner sur des protocoles différents qui ne sont pas compatibles entre eux. La couche réseau a la responsabilité de router les paquets de la source à la destination, en mappant différents schémas et protocoles d'adressage.

6.4.1. FONCTIONNALITES DE COUCHE RESEAU

Les périphériques qui fonctionnent sur Network Layer se concentrent principalement sur le routage. Le routage peut inclure diverses tâches visant à atteindre un seul objectif. Ceux-ci peuvent être:

- *Adressage des appareils et des réseaux.*
- *Remplissage des tables de routage ou des routes statiques.*
- *Mettre en file d'attente les données entrantes et sortantes, puis les transmettre en fonction des contraintes de qualité de service définies pour ces paquets.*
- *Interconnexion de réseaux entre deux sous-réseaux différents.*
- *Livrer les paquets à destination avec les meilleurs efforts.*
- *Fournit un mécanisme orienté connexion et connexion moins.*

Avec sa fonctionnalité standard, Couche 3

- *Gère de la qualité de service*
- *Assure l'Équilibrage de charge et de gestion des liens ainsi que la Sécurité*
- *Fait l'Interrelation de différents protocoles et sous-réseaux avec des schémas différents.*
- *Conçois un réseau logique différent par rapport à la conception physique du réseau.*
- *Les VPN et tunnels L3 peuvent être utilisés pour fournir une connectivité dédiée de bout en bout.*

6.5. RESEAU D'ADRESSAGE

L'adressage réseau de couche 3 est l'une des principales tâches de la couche réseau. Les adresses réseau sont toujours logiques, c'est-à-dire que ce sont des adresses logicielles qui peuvent être modifiées par des configurations appropriées.

Une adresse réseau pointe toujours vers hôte / noeud / serveur ou peut représenter un réseau entier. L'adresse réseau est toujours configurée sur la carte d'interface réseau et est généralement mappée par le système avec l'adresse MAC (adresse matérielle ou adresse de couche 2) de la machine pour la communication de couche 2.

Il existe différents types d'adresses réseau:

- *IP*
- *IPX*
- *AppleTalk*

Nous discutons de propriété intellectuelle ici car c'est la seule que nous utilisons en pratique ces jours-ci.

L'adressage IP fournit un mécanisme permettant de différencier les hôtes et le réseau. Les adresses IP étant attribuées de manière hiérarchique, un hôte réside toujours sous un réseau spécifique. L'hôte qui doit communiquer en dehors de son sous-réseau doit connaître l'adresse réseau de destination, où le paquet / les données doivent être envoyés. Les hôtes d'un sous-réseau différent ont besoin d'un mécanisme pour se localiser. Cette tâche peut être effectuée par DNS. DNS est un serveur qui fournit l'adresse Layer-3 de l'hôte distant mappé avec son nom de domaine ou FQDN. Lorsqu'un hôte acquiert l'adresse de couche 3 (adresse IP) de l'hôte distant, il transmet tout son paquet à sa passerelle. Une passerelle est un routeur équipé de toutes les informations qui permettent de router les paquets vers l'hôte de destination.

Les routeurs prennent l'aide des tables de routage, qui ont les informations suivantes:

- *Adresse du réseau de destination*
- *Méthode pour atteindre le réseau*

Routeurs à la réception d'une demande de transfert, transmet le paquet à son saut suivant (routeur adjacent) vers la destination.

Le routeur suivant sur le chemin suit la même chose et finalement le paquet de données atteint sa destination.

L'adresse réseau peut être l'une des suivantes:

- *Unicast (destiné à un hôte)*
- *Multicast (destiné au groupe)*
- *Diffusion (destinée à tous)*
- *Anycast (destiné au plus proche)*

Un routeur ne transmet jamais le trafic de diffusion par défaut. Le trafic multicast utilise un traitement spécial car il s'agit d'un flux vidéo ou audio avec la plus haute priorité. Anycast est similaire à la monodiffusion, sauf que les paquets sont livrés à la destination la plus proche lorsque plusieurs destinations sont disponibles.

6.5.1. ROUTAGE DES RESEAUX

Lorsqu'un périphérique a plusieurs chemins pour atteindre une destination, il sélectionne toujours un chemin en le préférant aux autres. Ce processus de sélection est appelé Routage. Le routage est effectué par des

périphériques réseau spéciaux appelés routeurs ou peut être fait au moyen de processus logiciels. Les routeurs logiciels ont des fonctionnalités limitées et une portée limitée.

Un routeur est toujours configuré avec un itinéraire par défaut. Une route par défaut indique au routeur où transférer un paquet s'il n'y a pas d'itinéraire trouvé pour une destination spécifique. Dans le cas où plusieurs chemins existent pour atteindre la même destination, le routeur peut prendre une décision en fonction des informations suivantes:

- *Nombre de sauts*
- *Bande passante*
- *Métrique*
- *Préfixe-longueur*
- *Retard*

Les routes peuvent être configurées de manière statique ou apprises dynamiquement. Une route peut être configurée pour être préférée à d'autres.

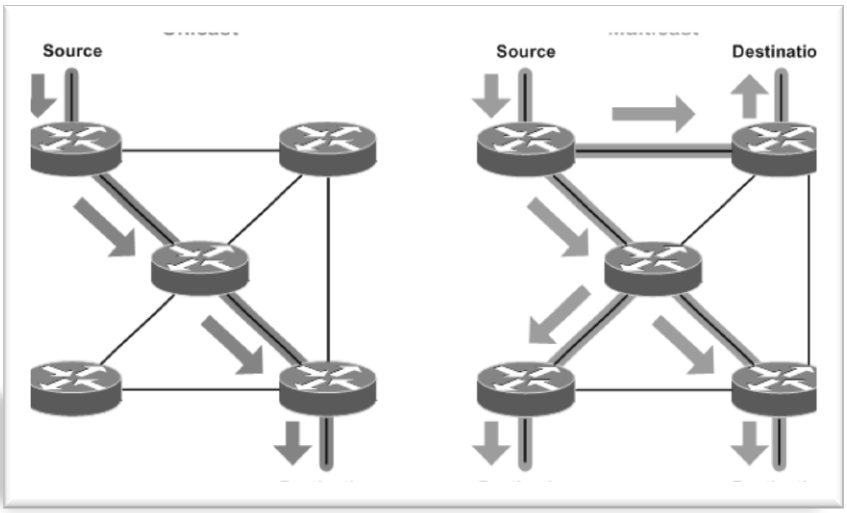


Figure 43 : Routage unicast and multicast

6.5.2. ROUTAGE UNICAST

La majeure partie du trafic sur Internet et les intranets connus sous le nom de données de monodiffusion ou de trafic monodiffusion sont envoyés avec une destination spécifiée. Le routage des données de monodiffusion sur Internet est appelé routage monodiffusion. C'est la forme la plus simple de routage car la destination est déjà connue. Par conséquent, le routeur doit simplement rechercher la table de routage et transmettre le paquet au saut suivant.

6.5.3. ROUTAGE DE DIFFUSION

Par défaut, les paquets de diffusion ne sont pas routés et transmis par les routeurs sur n'importe quel réseau. Les routeurs créent des domaines de diffusion. Mais il peut être configuré pour transmettre des émissions dans certains cas particuliers. Un message de diffusion est destiné à tous les périphériques réseau.

Le routage de diffusion peut être effectué de deux façons (algorithme):

- *Un routeur crée un paquet de données et l'envoie ensuite à chaque hôte un par un. Dans ce cas, le routeur crée plusieurs copies de paquet de données unique avec différentes adresses de destination. Tous les paquets sont envoyés en monodiffusion, mais comme ils sont envoyés à tous, ils simulent comme si le routeur diffusait.*
- *Cette méthode consomme beaucoup de bande passante et le routeur doit indiquer l'adresse de destination de chaque nœud.*
- *Deuxièmement, lorsque le routeur reçoit un paquet à diffuser, il ne fait qu'inonduire ces paquets hors de toutes les interfaces. Tous les routeurs sont configurés de la même manière.*
- *Cette méthode est facile sur le processeur du routeur mais peut causer le problème des paquets en double reçus des routeurs pairs.*
- *L'inversion du chemin d'accès est une technique dans laquelle le routeur connaît à l'avance son prédécesseur d'où il devrait recevoir la diffusion. Cette technique est utilisée pour détecter et éliminer les doublons.*

6.5.4. ROUTAGE MULTICAST

Le routage multidiffusion est un cas particulier de routage de diffusion avec différence de signification et défis. Dans le routage de diffusion, les paquets sont envoyés à tous les nœuds même s'ils ne le veulent pas. Mais dans le routage Multicast, les données sont envoyées uniquement aux nœuds qui souhaitent recevoir les paquets.

Le routeur doit savoir qu'il y a des nœuds, qui souhaitent recevoir des paquets de multidiffusion (ou flux) alors seulement il devrait avancer. Le routage multicast fonctionne de manière à éviter le bouclage.

Le routage multidiffusion utilise également la technique de transfert de chemin inverse, pour détecter et éliminer les doublons et les boucles.

6.5.5. ROUTAGE ANYCAST

Le transfert de paquets Anycast est un mécanisme dans lequel plusieurs hôtes peuvent avoir la même adresse logique. Lorsqu'un paquet destiné à cette adresse logique est reçu, il est envoyé à l'hôte le plus proche dans la topologie de routage.

Le routage Anycast est fait avec l'aide du serveur DNS. Chaque fois qu'un paquet Anycast est reçu, il est demandé à DNS où l'envoyer. DNS fournit l'adresse IP qui correspond à l'adresse IP la plus proche.

6.5.6. PROTOCOLES DE ROUTAGE MONODIFFUSION

Il existe deux types de protocoles de routage disponibles pour acheminer les paquets monodiffusion:

Protocole de routage de vecteur de distance

Distance Vector est un protocole de routage simple qui prend la décision de routage sur le nombre de sauts entre la source et la destination. Un itinéraire avec moins de sauts est considéré comme le meilleur itinéraire. Chaque routeur annonce ses meilleurs itinéraires aux autres routeurs. En fin de compte, tous les routeurs construisent leur topologie de réseau en fonction des publicités de leurs routeurs homologues, par exemple, le protocole RIP (Routing Information Protocol).

Protocole de routage d'état de lien

Le protocole d'état de liaison est un protocole légèrement compliqué par rapport au vecteur de distance. Il prend en compte les états de liens de tous les routeurs dans un réseau. Cette technique aide les routes à construire un graphique commun de l'ensemble du réseau. Tous les routeurs calculent ensuite leur meilleur

chemin à des fins de routage, par exemple, OSPF (Open Shortest Path First) et ISIS (Intermediate System to Intermediate System).

6.5.7. PROTOCOLES DE ROUTAGE DE MULTIDIFFUSION

Les protocoles de routage monodiffusion utilisent des graphiques tandis que les protocoles de routage multicast utilisent des arborescences, c'est-à-dire des arborescences étendues pour éviter les boucles. L'arbre optimal est appelé le spanning path spanning tree.

- *DVMRP : protocole de routage de multidiffusion de vecteur de distance*
- *MOSPF : Multicast ouvre le chemin le plus court en premier*
- *TCC : arbre de base*
- *PIM : Multicast indépendant du protocole*

Protocole Multicast indépendant est couramment utilisé maintenant. Il a deux saveurs:

- *Mode dense PIM*

Ce mode utilise des arbres basés sur des sources. Il est utilisé dans un environnement dense tel que LAN.

- *Mode fragmenté PIM*

Ce mode utilise des arbres partagés. Il est utilisé dans un environnement clairsemé tel que WAN.

ALGORITHMES DE ROUTAGE

Les algorithmes de routage sont les suivants :

Inondation

L'inondation est la méthode la plus simple de transmission de paquets. Lorsqu'un paquet est reçu, les routeurs l'envoient à toutes les interfaces sauf celle sur laquelle il a été reçu. Cela crée trop de fardeau sur le réseau et beaucoup de paquets en double errant dans le réseau.

Time to Live (TTL) peut être utilisé pour éviter une boucle infinie de paquets. Il existe une autre approche pour l'inondation, appelée inondation sélective, pour réduire les frais généraux sur le réseau. Dans cette méthode, le routeur n'influe pas sur toutes les interfaces, mais sur les interfaces sélectives.

Le plus court chemin

Les décisions de routage dans les réseaux sont généralement prises en fonction du coût entre la source et la destination. Le nombre de sauts joue un rôle majeur ici. Le chemin le plus court est une technique qui utilise divers algorithmes pour décider d'un chemin avec un nombre minimum de sauts.

Les algorithmes communs les plus courts sont :

- *L'algorithme de Dijkstra*
- *Algorithme Bellman Ford*
- *Algorithme Floyd Warshall*

Chapitre 7 : Couche OSI II

7.1. INTRODUCTION

Dans le scénario réel, les réseaux sous la même administration sont généralement dispersés géographiquement. Il peut exister une exigence de connexion de deux réseaux différents du même type ainsi que de différents types. Le routage entre deux réseaux est appelé interréseautage.

7.2. INTERNETWORKING

Les réseaux peuvent être considérés comme différents en fonction de divers paramètres tels que le protocole, la topologie, le réseau de couche 2 et le schéma d'adressage. Dans l'interréseautage, les routeurs ont connaissance de l'adresse et des adresses des uns et des autres. Ils peuvent être configurés statiquement sur un réseau différent ou ils peuvent apprendre en utilisant le protocole de routage inter-réseaux.

Les protocoles de routage utilisés dans une organisation ou une administration sont appelés Interior Gateway Protocols ou IGP. RIP, OSPF sont des exemples d'IGP. Le routage entre différentes organisations ou administrations peut avoir un protocole de passerelle extérieure, et il n'y a qu'un seul protocole EGP, c'est-à-dire un protocole de passerelle frontalière.

7.2.1. TUNNELING

S'il s'agit de deux réseaux séparés géographiquement, qui souhaitent communiquer entre eux, ils peuvent déployer une ligne dédiée ou transmettre leurs données via des réseaux intermédiaires.

Le tunneling est un mécanisme par lequel deux ou plusieurs mêmes réseaux communiquent entre eux, en passant des complexités de réseau intermédiaires. La tunnellisation est configurée aux deux extrémités.

Lorsque les données entrent d'une extrémité du tunnel, elles sont marquées. Ces données étiquetées sont ensuite routées à l'intérieur du réseau intermédiaire ou de transit pour atteindre l'autre extrémité du tunnel. Lorsque des données existent dans le tunnel, son tag est supprimé et transmis à l'autre partie du réseau.

Les deux extrémités semblent être directement connectées et l'étiquetage permet aux données de circuler dans le réseau de transport en commun sans aucune modification.

7.2.3. FRAGMENTATION DE PAQUETS

La plupart des segments Ethernet ont leur unité de transmission maximale (MTU) fixée à 1500 octets. Un paquet de données peut avoir plus ou moins de longueur de paquet en fonction de l'application. Les périphériques dans le chemin de transit ont également leurs capacités matérielles et logicielles qui indiquent quelle quantité de données ce périphérique peut gérer et quelle taille de paquet il peut traiter.

Si la taille du paquet de données est inférieure ou égale à la taille du paquet que le réseau de transit peut gérer, il est traité de manière neutre. Si le paquet est plus grand, il est cassé en morceaux plus petits et ensuite transmis. C'est ce qu'on appelle la fragmentation des paquets. Chaque fragment contient la même destination et la même adresse source et est acheminé facilement via le chemin de transit. À la réception, il est à nouveau assemblé.

Si un paquet avec un bit DF (ne pas fragmenter) mis à 1 arrive à un routeur qui ne peut pas gérer le paquet en raison de sa longueur, le paquet est abandonné.

Lorsqu'un paquet est reçu par un routeur, son bit MF (plus de fragments) est mis à 1, le routeur sait alors qu'il s'agit d'un paquet fragmenté et que des parties du paquet original sont en route. Si le paquet est fragmenté trop petit, le surcoût augmente. Si le paquet est fragmenté trop volumineux, le routeur intermédiaire peut ne pas être en mesure de les traiter et il peut être supprimé.

7.3. PROTOCOLES DE COUCHE RESEAU

Chaque ordinateur d'un réseau dispose d'une adresse IP permettant de l'identifier et de l'adresser de manière unique. Une adresse IP est une adresse logique de couche 3 (couche réseau). Cette adresse peut changer chaque fois qu'un ordinateur redémarre. Un ordinateur peut avoir une adresse IP à une instance de temps et une autre adresse IP à un moment différent.

7.3.1. PROTOCOLE DE RESOLUTION D'ADRESSE (ARP)

Lors de la communication, un hôte a besoin de l'adresse Layer-2 (MAC) de la machine de destination appartenant au même domaine de diffusion ou réseau. Une adresse MAC est physiquement gravée dans la carte d'interface réseau (NIC) d'une machine et elle ne change jamais. D'un autre côté, l'adresse IP sur le domaine public est rarement modifiée. Si la carte réseau est modifiée en cas de panne, l'adresse MAC change également. De cette façon, pour que la communication de couche 2 ait lieu, un mappage entre les deux est requis.

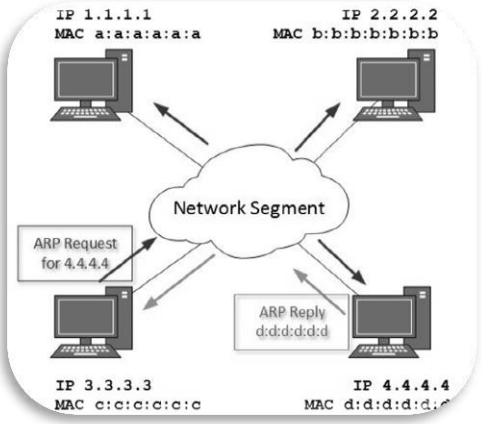


Figure 44 : Protocole ARP

Pour connaître l'adresse MAC de l'hôte distant sur un domaine de diffusion, un ordinateur souhaitant initier une communication envoie un message de diffusion ARP demandant "Qui a cette adresse IP?" Parce que c'est une diffusion, tous les hôtes du segment de réseau (domaine de diffusion) reçoivent ce paquet et le traiter. Le paquet ARP contient l'adresse IP de l'hôte de destination, auquel l'hôte expéditeur souhaite parler. Lorsqu'un hôte reçoit un paquet ARP qui lui est destiné, il répond avec sa propre adresse MAC.

Une fois que l'hôte a reçu l'adresse MAC de destination, il peut communiquer avec l'hôte distant en utilisant le protocole de liaison Layer-2. Ce mappage MAC vers IP est enregistré dans le cache ARP des hôtes d'envoi et de réception. La prochaine fois, s'ils ont besoin de communiquer, ils peuvent se référer directement à leur cache ARP respectif.

Reverse ARP est un mécanisme par lequel l'hôte connaît l'adresse MAC de l'hôte distant mais nécessite de connaître l'adresse IP pour communiquer.

7.3.2. PROTOCOLE ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

ICMP est un protocole de diagnostic réseau et de rapport d'erreurs. ICMP appartient à la suite de protocole IP et utilise IP comme protocole de porteuse. Après la construction du paquet ICMP, il est encapsulé dans un paquet IP. Parce que l'IP elle-même est un protocole non fiable de meilleur effort, ICMP l'est aussi.

Tout retour sur le réseau est renvoyé à l'hôte d'origine. Si une erreur survient dans le réseau, elle est signalée au moyen d'ICMP. ICMP contient des dizaines de messages de diagnostic et de rapport d'erreurs.

ICMP-echo et ICMP-echo-reply sont les messages ICMP les plus couramment utilisés pour vérifier l'accessibilité des hôtes de bout en bout. Lorsqu'un hôte reçoit une requête ICMP-echo, il est tenu de renvoyer une réponse ICMP-echo. S'il y a un problème dans le réseau de transit, l'ICMP signalera ce problème.

7.3.3. INTERNET PROTOCOL VERSION 4 (IPV4)

IPv4 est un schéma d'adressage 32 bits utilisé comme mécanisme d'adressage hôte TCP / IP. L'adressage IP permet à chaque hôte du réseau TCP / IP d'être identifiable de manière unique. IPv4 fournit un schéma d'adressage hiérarchique qui lui permet de diviser le réseau en sous-réseaux, chacun avec un nombre d'hôtes bien défini. Les adresses IP sont divisées en plusieurs catégories:

- *Classe A: utilise le premier octet pour les adresses réseau et les trois derniers octets pour l'adressage de l'hôte.*
- *Classe B: il utilise les deux premiers octets pour les adresses réseau et les deux derniers pour l'adressage de l'hôte.*
- *Classe C: elle utilise les trois premiers octets pour les adresses réseau et le dernier pour l'adressage de l'hôte.*
- *Classe D: Il fournit un schéma d'adressage IP plat contrairement à la structure hiérarchique pour les trois ci-dessus.*
- *Classe E: Il est utilisé comme expérimental.*

IPv4 dispose également d'espaces d'adressage bien définis à utiliser comme adresses privées (non routables sur Internet) et adresses publiques (fournies par les FAI et routables sur Internet).

Bien que la propriété intellectuelle ne soit pas fiable; il fournit un mécanisme de «meilleur effort-livraison».

7.3.4. INTERNET PROTOCOL VERSION 6 (IPV6)

L'épuisement des adresses IPv4 a donné naissance à une version 6 du protocole Internet de prochaine génération. IPv6 adresse ses nœuds avec une adresse large de 128 bits offrant beaucoup d'espace d'adressage pour une utilisation future sur toute la planète ou au-delà.

IPv6 a introduit l'adressage Anycast mais a supprimé le concept de diffusion. IPv6 permet aux périphériques d'auto-acquérir une adresse IPv6 et de communiquer

dans ce sous-réseau. Cette auto-configuration supprime la fiabilité des serveurs DHCP (Dynamic Host Configuration Protocol). De cette façon, même si le serveur DHCP sur ce sous-réseau est en panne, les hôtes peuvent communiquer entre eux.

IPv6 fournit une nouvelle fonctionnalité de mobilité IPv6. Les machines équipées d'un système IPv6 mobile peuvent circuler sans avoir à changer d'adresse IP.

IPv6 est encore en phase de transition et devrait remplacer complètement IPv4 dans les années à venir. Actuellement, il existe peu de réseaux fonctionnant sous IPv6. Certains mécanismes de transition sont

disponibles pour que les réseaux compatibles IPv6 puissent parler et circuler facilement sur différents réseaux sur IPv4. Ceux-ci sont:

- *Implémentation à double pile*
- *Tunneling*
- *NAT-PT*

7.4. INTRODUCTION DE LA COUCHE DE TRANSPORT

La couche suivante dans le modèle OSI est reconnu en tant que couche de transport (couche 4). Tous les modules et procédures relatifs au transport de données ou d'un flux de données sont classés dans cette couche. Comme toutes les autres couches, cette couche communique avec sa couche de transport homologue de l'hôte distant.

La couche de transport offre une connexion d'égal à égal et de bout en bout entre deux processus sur des hôtes distants. La couche de transport prend les données de la couche supérieure (c'est-à-dire la couche Application), puis les divise en segments de plus petite taille, numérote chaque octet et transmet la couche inférieure (couche réseau) pour la distribution.

7.4.1. LES FONCTIONS

- *Ce calque est le premier qui casse les données d'information fournies par la couche Application en unités plus petites appelées segments. Il numérote chaque octet dans le segment et maintient leur comptabilité.*
- *Cette couche garantit que les données doivent être reçues dans la même séquence que celle dans laquelle elles ont été envoyées.*
- *Cette couche fournit des données de bout en bout entre des hôtes appartenant ou non au même sous-réseau.*
- *Tous les processus serveurs qui ont l'intention de communiquer sur le réseau sont équipés de points d'accès aux services de transport (TSAP) bien connus, également appelés numéros de port.*

7.4.2. COMMUNICATION DE BOUT EN BOUT

Un processus sur un hôte identifie son hôte homologue sur un réseau distant au moyen de TSAP, également appelés numéros de port. Les PATS sont très bien définis et un processus qui essaie de communiquer avec ses pairs le sait à l'avance.

Par exemple, lorsqu'un client DHCP souhaite communiquer avec un serveur DHCP distant, il demande toujours le numéro de port 67. Lorsqu'un client DNS souhaite communiquer avec un serveur DNS distant, il demande toujours le numéro de port 53 (UDP).

Les deux principaux protocoles de couche Transport sont:

- ***Protocole de contrôle de la transmission***

Il fournit une communication fiable entre deux hôtes.

- ***Protocole de datagramme utilisateur***

Il fournit une communication non fiable entre deux hôtes.

7.5. PROTOCOLE DE COMMANDE DE TRANSMISSION

Le protocole TCP (Transmission Control Protocol) est l'un des protocoles les plus importants de la suite Internet Protocols. C'est le protocole le plus largement utilisé pour la transmission de données dans un réseau de communication tel qu'internet.

7.5.1. CARACTERISTIQUES

- *TCP est un protocole fiable. C'est-à-dire que le récepteur envoie toujours un accusé de réception positif ou négatif concernant le paquet de données à l'expéditeur, de sorte que l'expéditeur a toujours une idée claire du fait que le paquet de données est atteint ou qu'il doit le renvoyer.*
- *TCP garantit que les données atteignent la destination prévue dans le même ordre que celui où elles ont été envoyées.*
- *TCP est orienté connexion. TCP nécessite que la connexion entre deux points distants soit établie avant d'envoyer des données réelles.*
- *TCP fournit un mécanisme de vérification des erreurs et de récupération.*
- *TCP fournit une communication de bout en bout.*
- *TCP fournit le contrôle de flux et la qualité de service.*
- *TCP fonctionne en mode point à point Client / Serveur.*
- *TCP fournit un serveur full duplex, c'est-à-dire qu'il peut jouer les rôles de récepteur et d'expéditeur.*

7.5.2. ENTETE

La longueur de l'en-tête TCP est d'au moins 20 octets et d'au plus 60 octets.

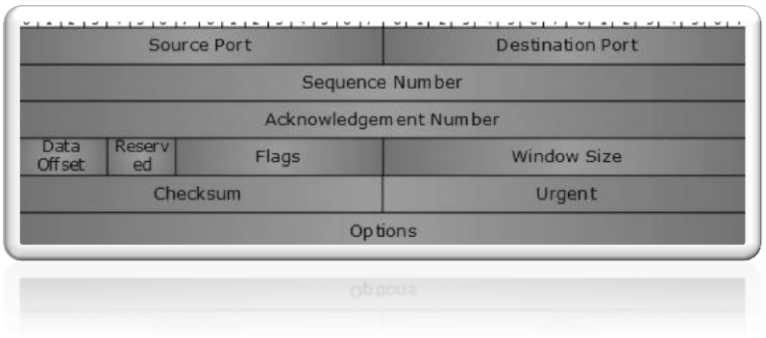


Figure 45 : Entête du Protocole

- *Port source (16 bits): identifie le port source du processus d'application sur l'appareil d'envoi.*
- *Port de destination (16 bits): identifie le port de destination de l'application processus sur le périphérique de réception.*
- *Numéro de séquence (32 bits): numéro de séquence des octets de données d'un segment dans une session.*
- *Numéro d'accusé de réception (32 bits): lorsque l'indicateur ACK est activé, ce numéro contient le numéro de séquence suivant de l'octet de données prévu et fonctionne comme accusé de réception des données précédentes reçues.*
- *Data Offset (4 bits): ce champ implique à la fois la taille de l'en-tête TCP (32 bits) mots) et le décalage des données dans le paquet courant dans tout le segment TCP.*
- *Réservé (3 bits): Réservé pour une utilisation future et tous sont définis par défaut sur zéro.*
- *Drapeaux (1 bit chacun): NS: le bit Nonce Sum est utilisé par la signalisation de notification d'encombrement explicite processus.*

- *CWR: lorsqu'un hôte reçoit un paquet avec l'ensemble de bits ECE, il définit la congestion Windows réduit à reconnaître que ECE a reçu.*
- *ECE: Il a deux significations:*
  - *Si le bit SYN est à 0, alors ECE signifie que le paquet IP a son CE (expérience de congestion) bit mis.*
  - *Si le bit SYN est défini sur 1, ECE signifie que le périphérique est compatible avec ECT.*
- *URG: Indique que le champ Urgent Pointer contient des données importantes et devrait être traité.*
- *ACK: Cela indique que le champ Accusé de réception a une signification. Si ACK est effacé à 0, cela indique que le paquet ne contient aucun acquittement.*
- *PSH: Lorsque cette option est activée, il s'agit d'une demande à la station réceptrice d'envoyer des données PUSH dès qu'elles parviennent à l'application réceptrice sans la mettre en mémoire tampon.*
- *RST: le drapeau de réinitialisation a les caractéristiques suivantes:*
  - *Il est utilisé pour refuser une connexion entrante.*
  - *Il est utilisé pour rejeter un segment.*
  - *Il est utilisé pour redémarrer une connexion.*
- *SYN: cet indicateur est utilisé pour établir une connexion entre les hôtes.*
- *FIN: cet indicateur est utilisé pour libérer une connexion et aucune autre donnée n'est échangée par la suite. Les paquets avec les indicateurs SYN et FIN ayant des numéros de séquence, ils sont traités dans le bon ordre.*

- *Windows Size: Ce champ est utilisé pour le contrôle de flux entre deux stations et indique la quantité de tampon (en octets) allouée par le récepteur à un segment, c'est-à-dire le nombre de données attendues par le récepteur.*
- *Checksum: ce champ contient la somme de contrôle de Header, Data et Pseudo Headers.*
- *Pointeur urgent: Il indique l'octet de données urgent si l'indicateur URG est défini sur 1.*
- *Options: Cela facilite les options supplémentaires qui ne sont pas couvertes par l'en-tête normal. Le champ Option est toujours décrit en mots de 32 bits. Si ce champ contient des données inférieures à 32 bits, le remplissage est utilisé pour couvrir les bits restants pour atteindre la limite de 32 bits.*

7.5.3. ADRESSAGE

La communication TCP entre deux hôtes distants se fait au moyen de numéros de port (TSAP). Les numéros de ports peuvent être compris entre 0 et 65535, répartis comme suit:

- *Ports système (0 - 1023)*
- *Ports utilisateur (1024 - 49151)*
- *Ports privés / dynamiques (49152 - 65535)*

7.5.4. GESTION DE CONNEXION

La communication TCP fonctionne dans le modèle Serveur / Client. Le client initie la connexion et le serveur l'accepte ou la rejette. L'établissement d'une liaison à trois est utilisé pour la gestion de la connexion.

Établissement

Le client initie la connexion et envoie le segment avec un numéro de séquence. Le serveur le reconnait avec son propre numéro de séquence et ACK du segment du client, qui est un de plus que le numéro de séquence du client. Client après réception ACK de son segment envoie un accusé de réception de la réponse du serveur.

Libération

L'un ou l'autre des serveurs et des clients peut envoyer un segment TCP avec l'indicateur FIN défini sur 1. Lorsque l'extrémité réceptrice répond par ACKnowledging FIN, la direction de la communication TCP est fermée et la connexion est libérée.

7.5.5. GESTION DE LA BANDE PASSANTE

TCP utilise le concept de taille de fenêtre pour répondre aux besoins de gestion de la bande passante. La taille de la fenêtre indique à l'expéditeur à l'extrémité distante le nombre de segments d'octets de données que le récepteur peut recevoir à cette fin. TCP utilise une phase de démarrage lent en utilisant la taille de fenêtre 1 et augmente exponentiellement la taille de la fenêtre après chaque communication réussie.

Par exemple, le client utilise Windows taille 2 et envoie 2 octets de données. Lorsque l'accusé de réception de ce segment a reçu la taille de Windows est doublé à 4 et à côté le segment envoyé aura 4 octets de données de long. Lorsque l'accusé de réception d'un segment de données de 4 octets est reçu, le client définit la taille de la fenêtre à 8 et ainsi de suite. Si un accusé de réception est manqué, c'est-à-dire des données perdues dans le réseau de transit ou qu'il a reçu NACK, alors la taille de la fenêtre est réduite à moitié et la phase de démarrage lent recommence.

7.5.6. CONTROLE D'ERREUR ET CONTROLE DE FLUX

TCP utilise les numéros de port pour connaître le processus d'application dont il a besoin pour transférer le segment de données. Parallèlement à cela, il utilise des numéros de séquence pour se synchroniser avec l'hôte distant. Tous les segments de données sont envoyés et reçus avec des numéros de séquence. L'expéditeur sait quel dernier segment de données a été reçu par le récepteur lorsqu'il reçoit ACK. Le récepteur connaît le dernier segment envoyé par l'expéditeur en se référant au numéro de séquence du paquet reçu récemment.

Si le numéro de séquence d'un segment récemment reçu ne correspond pas au numéro de séquence attendu par le récepteur, il est ignoré et NACK est renvoyé. Si deux segments arrivent avec le même numéro de séquence, la valeur d'horodatage TCP est comparée pour prendre une décision.

7.5.7. MULTIPLEX

La technique permettant de combiner deux flux de données ou plus en une session est appelée multiplexage. Lorsqu'un client TCP initialise une connexion avec Server, il se réfère toujours à un numéro de port bien défini qui indique le processus d'application. Le client utilise lui-même un numéro de port généré aléatoirement à partir de pools de numéros de port privés.

En utilisant TCP Multiplexing, un client peut communiquer avec un certain nombre de processus d'application différents en une seule session. Par exemple, un client demande une page Web qui contient à son tour différents types de données (HTTP, SMTP, FTP, etc.). Le délai d'attente de la session TCP est augmenté et la session reste ouverte plus longtemps afin d'éviter la surcharge de la prise de contact à trois voies. .

Cela permet au système client de recevoir plusieurs connexions via une connexion virtuelle unique. Ces connexions virtuelles ne sont pas bonnes pour les serveurs si le délai d'attente est trop long.

7.5.8. CONTROLE DE CONGESTION

Lorsqu'une grande quantité de données est envoyée au système qui n'est pas capable de la gérer, une congestion se produit. TCP contrôle la congestion au moyen du mécanisme de fenêtre. TCP définit une taille de fenêtre indiquant à l'autre extrémité combien de segments de données envoyer. TCP peut utiliser trois algorithmes pour le contrôle de congestion:

- *Augmentation additive, diminution multiplicative*
- *Démarrage lent*
- *Délai d'attente pour réagir*

7.5.9. GESTION DE MINUTERIE

TCP utilise différents types de minuteurs pour contrôler et gérer diverses tâches:

Minuterie Keep-alive:

- *Cette minuterie est utilisée pour vérifier l'intégrité et la validité d'une connexion.*
- *Lorsque le temps de maintien en vie expire, l'hôte envoie une sonde pour vérifier si la connexion existe toujours.*

Minuterie de retransmission:

- *Cette minuterie maintient une session avec état des données envoyées.*
- *Si l'accusé de réception des données envoyées n'est pas reçu pendant la période de retransmission, le segment de données est à nouveau envoyé.*

Minuteur de persistance:

- *La session TCP peut être mise en pause par l'un ou l'autre hôte en envoyant la taille de la fenêtre 0.*
- *Pour reprendre la session, un hôte doit envoyer une taille de fenêtre avec une valeur plus grande.*
- *Si ce segment n'atteint jamais l'autre extrémité, les deux extrémités peuvent attendre l'une l'autre pendant un temps infini.*
- *Lorsque la minuterie de persistance expire, l'hôte renvoie la taille de sa fenêtre pour informer l'autre extrémité.*
- *Persist Timer permet d'éviter les blocages dans la communication.*

Timed-Wait:

- *Après avoir libéré une connexion, l'un des hôtes attend un temps d'attente temporisé pour terminer la connexion complètement.*
- *Ceci afin de s'assurer que l'autre extrémité a reçu l'accusé de réception de sa demande de terminaison de connexion.*
- *Le délai d'attente peut être de 240 seconds maximums (4 minutes).*

7.5.10. RECUPERATION APRES UN CRASH

TCP est un protocole très fiable. Il fournit le numéro de séquence à chacun des octets envoyés dans le segment. Il fournit le mécanisme de rétroaction, c'est-à-dire lorsqu'un hôte reçoit un paquet, il est lié à ACK ce paquet ayant le prochain numéro de séquence attendu (si ce n'est pas le dernier segment).

Lorsqu'un serveur TCP bloque la communication à mi-chemin et redémarre son processus, il envoie une diffusion TPDU à tous ses hôtes. Les hôtes peuvent alors envoyer le dernier segment de données qui n'a jamais été ignoré et continuer.

Chapitre 8 : Couche OSI III

8.1. INTRODUCTION

Le protocole UDP (User Datagram Protocol) est le protocole de communication Transport Layer le plus simple de la suite de protocoles TCP / IP. Cela implique un minimum de mécanisme de communication. UDP est dit être un protocole de transport peu fiable, mais il utilise des services IP qui fournit le meilleur mécanisme de livraison effort.

8.2. PROTOCOLE DE DATAGRAMME UTILISATEUR

En UDP, le récepteur ne génère pas d'accusé de réception de paquet et à son tour, l'expéditeur n'attend pas d'accusé de réception du paquet envoyé. Cette lacune rend ce protocole peu fiable et facilite le traitement.

8.2.1. EXIGENCE DE UDP

Une question peut se poser, pourquoi avons-nous besoin d'un protocole non fiable pour transporter les données? Nous déployons UDP où les paquets d'accusé de réception partagent une quantité importante de bande passante avec les données réelles. Par exemple, en cas de streaming vidéo, des milliers de paquets sont transférés vers ses utilisateurs. La reconnaissance de tous les paquets est gênante et peut contenir énormément de gaspillage de bande passante. Le meilleur mécanisme de livraison du protocole IP sous-jacent assure les meilleurs efforts pour délivrer ses paquets, mais même si certains paquets dans le streaming vidéo se perdent, l'impact n'est pas catastrophique et peut être ignoré facilement. La perte de quelques paquets dans le trafic vidéo et vocal passe parfois inaperçue.

8.2.2. CARACTERISTIQUES

- *UDP est utilisé lorsque la reconnaissance des données n'a aucune signification.*
- *UDP est un bon protocole pour le flux de données dans une direction.*
- *UDP est simple et adapté aux communications basées sur des requêtes.*
- *UDP n'est pas orienté connexion.*
- *UDP ne fournit pas de mécanisme de contrôle de congestion.*
- *UDP ne garantit pas la livraison ordonnée des données.*
- *UDP est apatride.*
- *UDP est un protocole approprié pour les applications de streaming telles que la VoIP, le streaming multimédia.*

8.2.3. EN-TETE UDP

L'en-tête UDP est aussi simple que sa fonction.

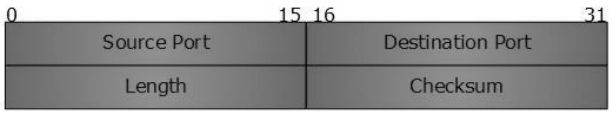


Figure 46: entête UDP

L'en-tête UDP contient quatre paramètres principaux :

***1. Port source :** cette information 16 bits est utilisée pour identifier le port source du paquet.*

2. Port de destination: *cette information de 16 bits est utilisée pour identifier le service au niveau de l'application sur la machine de destination.*

3. Longueur: *Le champ Longueur spécifie la longueur totale du paquet UDP (y compris l'en-tête). Il s'agit d'un champ de 16 bits et la valeur minimale est de 8 octets, c'est-à-dire la taille de l'en-tête UDP lui-même.*

4. Checksum: *Ce champ stocke la valeur de somme de contrôle générée par l'expéditeur avant l'envoi. IPv4 a ce champ comme facultatif ainsi quand le champ de somme de contrôle ne contient aucune valeur, il est fait 0 et tous ses bits sont mis à zéro.*

8.2.4. APPLICATION UDP

Voici quelques applications où UDP est utilisé pour transmettre des données :

- *Services de noms de domaine*
- *Protocole de gestion de réseau simple*
- *Protocole de transfert de fichiers trivial*
- *Protocole d'informations de routage*

8.3. INTRODUCTION DE LA COUCHE APPLICATION

La couche application est la couche la plus élevée dans le modèle en couches OSI et TCP / IP. Cette couche existe dans les deux modèles en couches en raison de son importance, de l'interaction avec les applications utilisateur et utilisateur. Cette couche est pour les applications qui sont impliquées dans le système de communication.

Un utilisateur peut ou non interagir directement avec les applications. La couche d'application est l'endroit où la communication réelle est initiée et reflète. Étant donné que cette couche est au sommet de la pile de calques, elle ne sert aucune autre couche. Couche d'application prend l'aide de Transport et toutes les couches ci-dessous pour communiquer ou transférer ses données à l'hôte distant.

Lorsqu'un protocole de couche d'application souhaite communiquer avec son protocole de couche d'application homologue sur un hôte distant, il transmet les données ou les informations à la couche de transport. La couche de transport fait le reste avec l'aide de toutes les couches en dessous.

Il y a une ambiguïté dans la compréhension de la couche application et de son protocole. Toutes les applications utilisateur ne peuvent pas être placées dans Application Layer à l'exception des applications qui interagissent avec le système de communication. Par exemple, la conception de logiciels ou de texteditor ne peut pas être considérée comme un programme de couche application.

D'un autre côté, lorsque nous utilisons un navigateur Web, qui utilise en fait le protocole HTTP (Hyper Text Transfer Protocol) pour interagir avec le réseau, HTTP est le protocole Application Layer.

Un autre exemple est le protocole de transfert de fichiers, qui aide un utilisateur à transférer des fichiers texte ou binaires sur le réseau. Un utilisateur peut utiliser ce protocole dans un logiciel basé sur une interface graphique comme FileZilla ou CuteFTP et le même utilisateur peut utiliser FTP en mode ligne de commande.

Par conséquent, quel que soit le logiciel que vous utilisez, c'est le protocole qui est pris en compte lors de la couche application utilisée par ce logiciel. DNS est un protocole qui aide les protocoles d'application utilisateur tels que HTTP à accomplir son travail.

8.3.1. ARCHITECTURE CLIENT SERVEUR

Deux processus d'application distants peuvent communiquer principalement de deux manières différentes:

- *Peer-to-peer: les deux processus distants s'exécutent au même niveau et ils échangent des données en utilisant une ressource partagée.*
- *Client-Serveur: un processus distant agit en tant que client et demande une ressource à un autre processus d'application agissant en tant que serveur.*

Dans le modèle client-serveur, tout processus peut agir en tant que serveur ou client. Ce n'est pas le type de machine, la taille de la machine, ou sa puissance de calcul qui en fait le serveur; c'est la possibilité de servir une requête qui fait d'une machine un serveur.

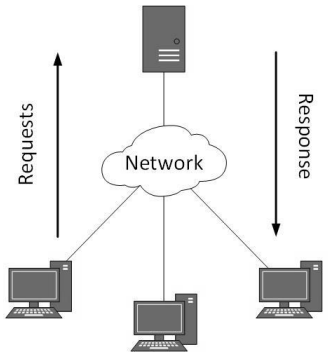


Figure 47: ACR Architecture client serveur

Un système peut agir en tant que serveur et client simultanément. Autrement dit, un processus agit en tant que serveur et un autre agit en tant que client. Cela peut également arriver que les processus client et serveur résident sur la même machine.

8.3.2. LA COMMUNICATION

Deux processus dans le modèle client-serveur peuvent interagir de différentes manières:

- *Douilles*
- *Appels de procédure distante (RPC)*

Sockets

Dans ce paradigme, le processus agissant en tant que serveur ouvre un socket en utilisant un port bien connu (ou connu par le client) et attend jusqu'à ce qu'une requête client arrive. Le deuxième processus agissant en tant que client ouvre également une socket; mais au lieu d'attendre une demande entrante, le client traite les 'demandes d'abord'.

Lorsque la requête est arrivée au serveur, elle est servie. Il peut s'agir d'un partage d'informations ou d'une demande de ressources.

Remote call for procedure

C'est un mécanisme où un processus interagit avec un autre au moyen d'appels de procédure. Un processus (client) appelle la procédure située sur l'hôte distant. Le processus sur l'hôte distant est dit serveur. Les deux processus sont des talons alloués. Cette communication se passe de la manière suivante:

- *Le processus client appelle le talon du client. Il passe tous les paramètres relatifs au programme local à lui.*
- *Tous les paramètres sont ensuite empaquetés (marshalled) et un appel système est fait pour les envoyer à l'autre côté du réseau.*
- *Le noyau envoie les données sur le réseau et l'autre le reçoit.*
- *L'hôte distant transmet les données au talon du serveur où il n'est pas masqué.*
- *Les paramètres sont passés à la procédure et la procédure est ensuite exécutée.*
- *Le résultat est renvoyé au client de la même manière.*

8.4. PROTOCOLE APPLICATION

Il existe plusieurs protocoles qui fonctionnent pour les utilisateurs dans Application Layer. Les protocoles de couche d'application peuvent être globalement divisés en deux catégories:

- *Les protocoles utilisés par les utilisateurs. Par exemple, eMail.*
- *Les protocoles qui aident et supportent les protocoles utilisés par les utilisateurs. Par exemple, DNS.*

Peu de protocoles de couche Application sont décrits ci-dessous:

8.4.1. SYSTEME DE NOMS DE DOMAINES

Le système DNS (Domain Name System) fonctionne sur le modèle Client Server. Il utilise le protocole UDP pour la communication de la couche de transport. DNS utilise un schéma de nommage basé sur un domaine hiérarchique. Le serveur DNS est configuré avec des noms de domaine complets (FQDN) et des adresses e-mail mappées avec leurs adresses de protocole Internet respectives. Un serveur DNS est demandé avec le nom de domaine complet et répond avec l'adresse IP associée à celui-ci. DNS utilise le port UDP 53.

8.4.2. PROTOCOLE DE TRANSFERT DE MAIL

Le protocole SMTP (Simple Mail Transfer Protocol) est utilisé pour transférer le courrier électronique d'un utilisateur à un autre. Cette tâche est effectuée au moyen d'un logiciel client de messagerie (User Agents) que l'utilisateur utilise. Les agents utilisateurs aident l'utilisateur à taper et formater l'e-mail et à le stocker jusqu'à ce que l'internet soit disponible. Lorsqu'un envoi de courrier électronique est envoyé, le processus d'envoi est géré par Message Transfer Agent, qui est normalement intégré dans le logiciel client de messagerie.

Message Transfer Agent utilise SMTP pour transférer l'e-mail à un autre agent de transfert de messages (côté serveur). Alors que SMTP est utilisé par l'utilisateur final pour envoyer uniquement les e-mails, les serveurs utilisent normalement SMTP pour envoyer et recevoir des e-mails. SMTP utilise les numéros de port TCP 25 et 587.

Le logiciel client utilise les protocoles IMAP (Internet Message Access Protocol) ou POP pour recevoir des courriels.

8.4.3. PROTOCOLE DE TRANSFER DE FICHIER

Le protocole FTP (File Transfer Protocol) est le protocole le plus utilisé pour le transfert de fichiers sur le réseau. FTP utilise TCP / IP pour la communication et fonctionne sur le port TCP 21. FTP fonctionne sur le modèle client / serveur où un client demande un fichier au serveur et le serveur renvoie la ressource demandée au client.

FTP utilise un contrôle hors bande, c'est-à-dire que FTP utilise le port TCP 20 pour échanger des informations de contrôle et que les données réelles sont envoyées sur le port TCP 21.

Le client demande au serveur un fichier. Lorsque le serveur reçoit une demande de fichier, il ouvre une connexion TCP pour le client et transfère le fichier. Une fois le transfert terminé, le serveur ferme la connexion. Pour un deuxième fichier, le client demande à nouveau et le serveur rouvre une nouvelle connexion TCP.

8.4.4. PROTOCOLE POST OFFICE (POP)

Le protocole POP3 (Post Office Protocol version 3) est un protocole de récupération de courrier simple utilisé par les agents utilisateurs (logiciel de messagerie client) pour récupérer les messages du serveur de messagerie.

Lorsqu'un client a besoin de récupérer des mails du serveur, il ouvre une connexion avec le serveur sur le port TCP 110. L'utilisateur peut alors accéder à ses mails et les télécharger sur l'ordinateur local. POP3 fonctionne en deux modes. Le mode le plus courant, le mode de suppression, consiste à supprimer les courriers électroniques du serveur distant après leur téléchargement sur des machines locales. Le deuxième mode, le mode keep, ne supprime pas l'e-mail du serveur de messagerie et donne à l'utilisateur une option pour accéder aux mails plus tard sur le serveur de messagerie.

8.4.5. HYPER TEXT TRANSFER PROTOCOL (HTTP)

Le protocole HTTP (Hyper Text Transfer Protocol) est la base de World Wide Web. L'hypertexte est un système de documentation bien organisé qui utilise des hyperliens pour lier les pages dans les documents texte. HTTP fonctionne sur le modèle de serveur client. Lorsqu'un utilisateur souhaite accéder à une page HTTP sur Internet, la machine client à la fin de l'utilisateur initie une connexion TCP au serveur sur le port 80. Lorsque le serveur accepte la requête du client, le client est autorisé à accéder aux pages Web.

Pour accéder aux pages Web, un client utilise normalement des navigateurs Web, chargés d'initier, de maintenir et de fermer les connexions TCP. HTTP est un protocole sans état, ce qui signifie que le serveur ne conserve aucune information sur les demandes antérieures des clients.

Versions http :

- *HTTP 1.0 utilise un HTTP non persistant. Au plus un objet peut être envoyé via une seule connexion TCP.*
- *HTTP 1.1 utilise le protocole HTTP permanent. Dans cette version, plusieurs objets peuvent être envoyés via une connexion TCP unique.*

Chapitre 9 : Les Services dans les réseaux

9.1. INTRODUCTION

Les systèmes informatiques et les systèmes informatisés aident les êtres humains à travailler efficacement et à explorer l'impensable. Lorsque ces périphériques sont connectés ensemble pour former un réseau, les capacités sont améliorées plusieurs fois. Certains services de base du réseau informatique peuvent offrir sont:

9.1.1. SERVICES D'ANNUAIRE

Ces services sont la correspondance entre le nom et sa valeur, qui peut être variable ou fixe. Ce système logiciel permet de stocker l'information, de l'organiser et de fournir divers moyens d'y accéder.

Comptabilité

Dans une organisation, un certain nombre d'utilisateurs ont leur nom d'utilisateur et leur mot de passe associés. Les services d'annuaire fournissent des moyens de stocker ces informations sous forme cryptée et de les rendre disponibles sur demande.

Authentification et autorisation

Les informations d'identification de l'utilisateur sont vérifiées pour authentifier un utilisateur au moment de la connexion et / ou périodiquement. Les comptes d'utilisateurs peuvent être définis dans une structure hiérarchique et leur accès aux ressources peut être contrôlé à l'aide de schémas d'autorisation.

Services de noms de domaine

Le DNS est largement utilisé et l'un des services essentiels sur lequel Internet fonctionne. Ce système mappe les adresses IP aux noms de domaine, qui sont plus faciles à retenir et à rappeler que les adresses IP. Parce que le réseau fonctionne avec l'aide d'adresses IP et que les humains ont tendance à se souvenir des noms de site, le DNS fournit l'adresse IP du site qui est mappée à son nom à la demande d'un nom de site Web de l'utilisateur.

9.1.2. SERVICES DE FICHIERS

Les services de fichiers incluent le partage et le transfert de fichiers sur le réseau.

Partage de fichiers

L'une des raisons qui a donné naissance au réseautage était le partage de fichiers. Le partage de fichiers permet à ses utilisateurs de partager leurs données avec d'autres utilisateurs. L'utilisateur peut télécharger le fichier sur un serveur spécifique, accessible à tous les utilisateurs prévus. Comme alternative, l'utilisateur peut partager son fichier sur son propre ordinateur et fournir un accès aux utilisateurs prévus.

Transfert de fichier

Il s'agit d'une activité permettant de copier ou de déplacer un fichier d'un ordinateur vers un autre ordinateur ou vers plusieurs ordinateurs, à l'aide du réseau sous-jacent. Le réseau permet à son utilisateur de localiser d'autres utilisateurs sur le réseau et de transférer des fichiers.

9.1.3. SERVICES DE COMMUNICATION

Email

Le courrier électronique est une méthode de communication et quelque chose qu'un utilisateur d'ordinateur ne peut pas travailler sans. C'est la base des fonctionnalités Internet d'aujourd'hui. Le système de messagerie a un ou plusieurs serveurs de messagerie. Tous ses utilisateurs sont fournis avec des identifiants uniques. Lorsqu'un utilisateur envoie un courrier électronique à un autre utilisateur, il est effectivement transféré entre les utilisateurs à l'aide du serveur de messagerie.

Réseaux sociaux

Les technologies récentes ont rendu la vie technique sociale. Les gens avertis en informatique, peuvent trouver d'autres personnes connues ou des amis, peuvent se connecter avec eux, et peuvent partager des pensées, des images et des vidéos.

Chat Internet

Le chat Internet fournit des services de transfert de texte instantané entre deux hôtes. Deux personnes ou plus peuvent communiquer entre elles à l'aide de services de messagerie instantanée Internet. Ces jours-ci, le chat vocal et le chat vidéo sont très courants.

Forums de discussion

Les forums de discussion fournissent un mécanisme pour connecter plusieurs peuples avec les mêmes intérêts. Il permet aux utilisateurs de poser des questions, des questions, des suggestions, etc. qui peuvent être vues par tous les autres utilisateurs. D'autres peuvent également répondre.

Accès à distance

Ce service permet à l'utilisateur d'accéder aux données résidant sur l'ordinateur distant. Cette fonctionnalité est appelée Bureau à distance. Cela peut être fait via un dispositif distant, par ex. téléphone portable ou ordinateur personnel.

9.1.4. SERVICES D'APPLICATION

Ce ne sont que des services basés sur le réseau pour les utilisateurs tels que les services Web, la gestion de bases de données et le partage de ressources.

Partage de ressources

Pour utiliser les ressources efficacement et économiquement, le réseau fournit un moyen de les partager. Cela peut inclure des serveurs, des imprimantes et des supports de stockage, etc.

Bases de données

Ce service d'application est l'un des services les plus importants. Il stocke les données et les informations, les traite et permet aux utilisateurs de les récupérer efficacement en utilisant des requêtes. Les bases de données aident les organisations à prendre des décisions basées sur des statistiques.

Services Web

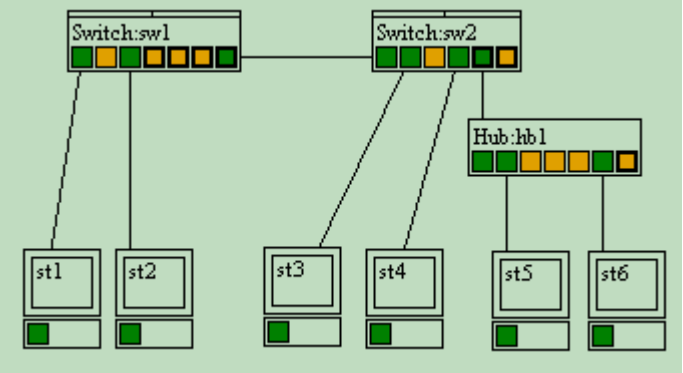
Le World Wide Web est devenu le synonyme d'Internet. Il est utilisé pour se connecter à Internet et accéder aux fichiers et aux services d'information fournis par les serveurs Internet.

ANNEXE

T.P. 1

1. Deux Switch (Labo01-2Switch-1Hub)

Passer en mode Ethernet



Le mode de transmission des trames

Méthode : mode trame réelle

***Test 1 :** émettre une trame à partir de st1 vers st4 (unicast vers st4).*

Question

- Dans cette configuration, la trame est-elle reçu complètement par le switch avant d'être transmise sur le port

- Menu contextuel sur le switch, configurer, comment se nomme ce type de switch (transmission) ?

Préparation : Menu contextuel sur les switchs, sélectionner configurer, choisir "On the fly".

Méthode : mode trame réelle

***Test 2 :** émettre une trame à partir de st4 vers st1 (unicast vers st1).*

Questions

- Dans cette configuration, quel est le comportement du switch pour transmettre la trame ?

- Quel est l'avantage de ce mode de transmission ?

Choisir d'émettre une trame à partir de st5 (broadcast) et à partir de st6 (broadcast) sans émettre les trames (cette situation sera l'étape de départ avant les tests 3 et 4)

***Test 3 :** émettre les trames à partir de st5 et de st6 de manière simultanée.*

Annexe

Remarque : les longueurs de câble pour st5 et st6 sont très différentes

Questions

- Une collision est-elle détectée sur le réseau ?

- Que fait le switch sw2 avec la trame avant la collision?:

- Comment est la trame que reçoivent les postes st1 à st4 à la première transmission ?

Préparation : Menu contextuel sur les switchs, sélectionner configurer, choisir "Store and forward".

***Test 4 :** émettre les trames à partir de st5 et de st6 de manière simultanée.*

Questions

- Une collision est-elle détectée sur le réseau ?

- Que fait le switch sw2 avec la trame avant la collision?:

- Les postes st1 à st4 sont-ils concernés par le trafic généré par la collision ? 5

- Quel est l'avantage du mode de transmission "Store and forward" ?

Préparation : Menu contextuel sur les switchs, sélectionner configurer, choisir "On the fly".

méthode : mode trame réelle, tracé le switch sw2, cocher Démo émission

Choisir d'émettre une trame à partir de st1 (unicast vers st4) et à partir de st4 (unicast vers st1) sans émettre les trames (cette situation sera l'étape de départ avant les tests 5 et 6)

***Test 5 :** émettre les trames à partir de st1 et de st4 (attendre que la trame de st1 arrive sur sw1 avant d'émettre de st4).*

Questions

- Une collision est-elle détectée sur le réseau ?

- Les trames peuvent-elles circuler vers leur destinataire, de manière simultanée ?

- Que fait le switch sw2 avec les deux trames avant de les transmettre ?:

Préparation : Cocher la case Full duplex.

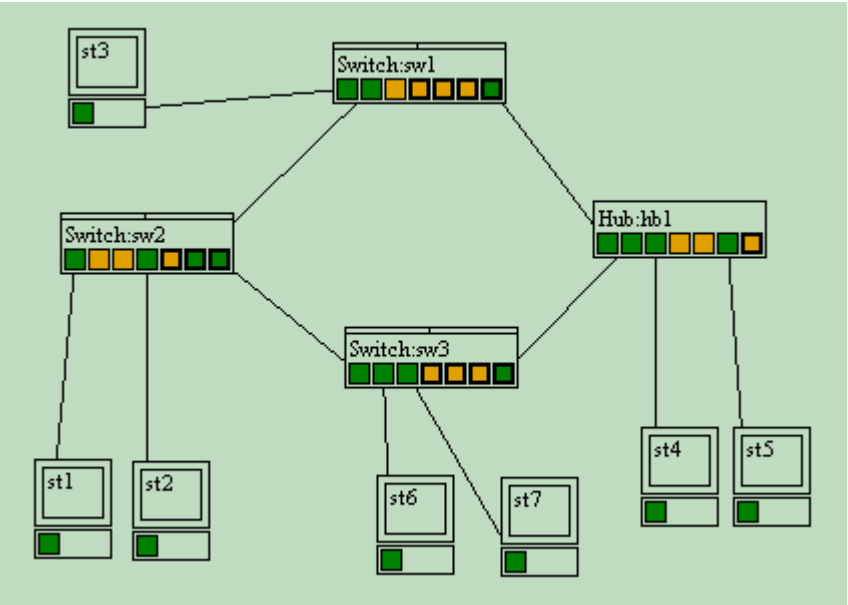
***Test 6 :** émettre les trames à partir de st1 et de st4 (attendre que la trame de st1 arrive sur sw1 avant d'émettre de st4).*

Question

- Le mode Full duplex est-il réalisé sur les deux types de liaison Station<->Switch et Switch<->Switch ?

T.P. 2

1. Spanning Tree (Labo02-Spanning)



Passer en mode Ethernet

La gestion des boucles avec les switchs

Méthode : mode automatique

Question : *Dans quel état sont les ports de cascade connectés des switchs et du hub ?*

Test 1 : A partir de la station st1, émettre une trame unicast vers st7.

Question

Expliquer le problème :

Préparation : Passer en mode Conception réseau, menu contextuel sur les switchs, sélectionner configurer, cocher gestion spanning tree pour chaque switch. Passer en mode Ethernet, méthode : mode automatique

Question :

Dans quel état sont les ports de cascade connectés des switchs ?

Test 2 : *A partir de la station st1, émettre une trame unicast vers st4, puis l'inverse, de st4 vers st1.*

Conclusion sur le spanning tree :

Préparation : Passer en mode Conception réseau, supprimer la connexion entre le switch sw2 et le switch sw3 pour simuler une rupture de liaison (clic droit sur un port de cascade, supprimer le câble).

Passer en mode Ethernet, méthode : mode automatique

Annexe

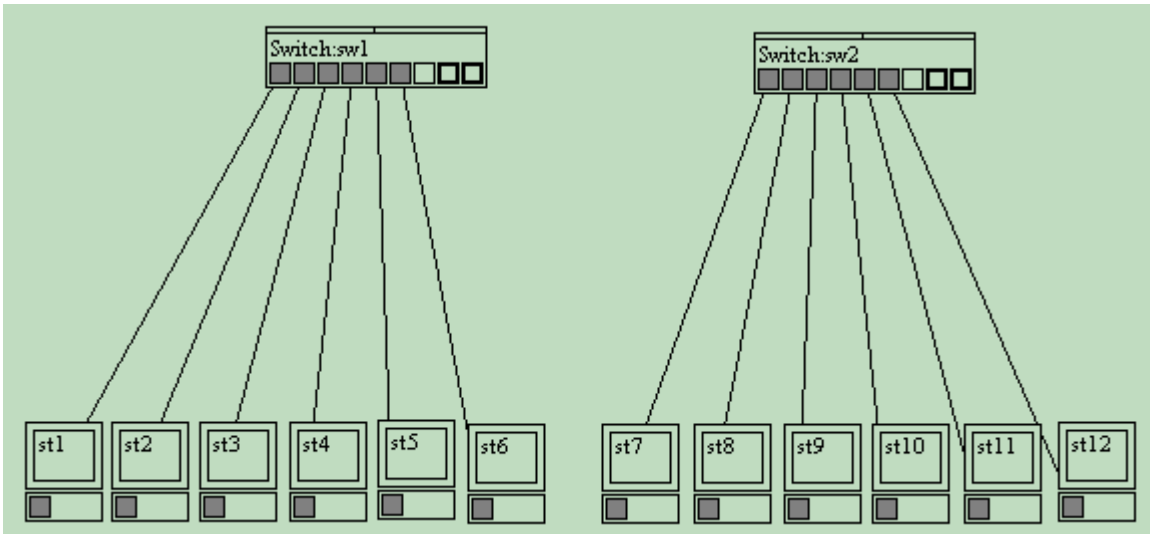
Question :

Dans quel état sont les ports de cascade connectés des switchs ?

Test 3 : *A partir de la station st1, émettre une trame unicast vers st4, puis l'inverse, de st4 vers st1.*

Conclusion sur l'intérêt d'avoir une boucle dans le réseau avec la gestion spanning tree :

T.P. 3



. Deux Switchs

Mode conception réseau

Relier les deux switchs pour obtenir une communication entre les 12 postes, vérifier en mode Ethernet.

Question :
- Comment obtenir une connexion correcte entre les deux switchs ?

Mode Ethernet, type de simulation automatique

Test 1 : *émettre une trame broadcast à partir de st3.*

Question :
- Quels postes reçoivent la trame ?

Test 2 : *émettre une trame unicast à partir de st3 vers st11.*

Question :
- La trame est-elle diffusée sur tous les ports ?

2. Vlan de niveau 1

Mode conception réseau

Préparation : Configurer les commutateurs pour définir des vlan de niveau 1 (bouton droit sur le switch, Configurer, Niveau vlan).

Annexe

Mode Ethernet, type de simulation automatique

*Préparation : Définir la configuration des vlan suivante pour **chaque** commutateur :*

(bouton droit sur le switch, Editer table port/vlan, sélectionner une ligne, bouton modifier (…)).

sw1 *:*	*Postes*	*vlan*	***sw2*** *:*	*Postes*	*vlan*
	st1	*1 (par défaut)*		*st7*	*3*
	st2	*1 (par défaut)*		*st8*	*3*
	st3	*2*		*st9*	*1 (par défaut)*
	st4	*2*		*st10*	*1 (par défaut)*
	st5	*3*		*st11*	*2*
	st6	*3*		*st12*	*2*

Laisser les valeurs par défaut pour les autres ports.

Test 1 : *émettre une trame broadcast à partir de st1.*

Question :

- Quels postes reçoivent la trame ?

Test 2 : *émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ?

Test 3 : *émettre une trame broadcast à partir de st5.*

Question :

- Quels postes reçoivent la trame ?

Méthode : type de simulation pas à pas, tracé : sw1 (bouton aucun nœud tracé)

Test 4 : *émettre une trame broadcast à partir de st3 (idem test 2).*

Questions :

- Expliquer pourquoi sw2 ne reçoit pas les broadcasts des tests 2 à 4 ?

- Expliquer pourquoi st1 et st5 ne reçoivent pas la trame broadcast ?

3. Port 802.1q

Mode conception réseau

Préparation : Configurer les deux commutateurs pour définir un port 802.1q (bouton droit sur le switch, Configurer, Nbre de ports 802.1q).

Refaire la liaison entre les deux commutateurs en utilisant le port 802.1q de chaque commutateur.

Mode Ethernet, type de simulation automatique ***sans tracé sw1*** *(bouton aucun nœud tracé)*

Test 1 : *émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ?

Mode Ethernet, type de simulation pas à pas, ***tracé sw2*** *(bouton aucun nœud tracé)*

Test 2 : *émettre une trame broadcast à partir de st5.*

Questions :

- Quels postes reçoivent la trame ?

- Pour les observateurs, la trame qui circule entre les deux ports 802.1q est légèrement différente, comment le simulateur représente cette différence ?

- Quelle action particulière a le port 802.1q de sw2 sur le contenu de la trame ?

- Quels vlan utilisent le port 802.1q ?

Mode Ethernet, type de simulation automatique, ***sans tracé sw2*** *(bouton aucun nœud tracé)*

Test 3 : *émettre une trame unicast à partir de st11 vers st3.*

Question :

- Quels postes reçoivent la trame ?

Test 4 : *émettre une trame unicast à partir de st11 vers st5.*

Question :

- Quels postes reçoivent la trame et expliquer ?

Conclusion :

- Les broadcasts d'un vlan générent-ils du trafic sur les autres vlan ?

- La communication entre les vlan est-elle possible dans notre configuration ?

- En appelant domaine de diffusion, un ensemble de postes recevant la même trame de broadcast, combien de domaines de diffusion différents présente ce réseau ?

4. Gestion des vlan de niveau 1

Mode conception réseau

Préparation : Connecter st11 sur le port 4 de sw2 et st10 sur le port 5 de sw2

Mode Ethernet, type de simulation automatique,

***Test 1 :** émettre une trame unicast à partir de st11 vers st3 (idem test 3 précédent).*

Question :

- Quels postes reçoivent la trame ?

*Mode Ethernet, type de simulation pas à pas, **tracé sw1** (bouton aucun nœud tracé)*

***Test 2 :** émettre une trame unicast à partir de st11 vers st3 (idem test 1).*

Questions :

- Le poste st11 a-t-il changé de vlan après son déplacement ?

- Expliquer le résultat pour la trame ?

- Avec des vlan de niveau 1, quelle est le problème lié au déplacement d'un poste pour l'administrateur réseau ?

Mode conception réseau

Préparation : Ajouter un hub, connecter st11 et st10 sur ce hub et connecter le hub au port 5 du switch sw2 (utiliser le port de cascade du hub)

*Mode Ethernet, type de simulation automatique, **sans tracé sw1** (bouton aucun nœud tracé)*

***Test 3 :** émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ?

- Pourquoi st10 st11 sont-ils maintenant dans le même vlan ?

Mode conception réseau

Préparation : Remettre st11 et st10 sur leur port d'origine, (st11 sur le port 5 de sw2 et st10 sur le port 4) et supprimer le hub.

5. Vlan de niveau 2

Mode conception réseau

Préparation : Configurer les commutateurs pour définir des vlan de niveau 2, (bouton droit sur le switch, Configurer, Niveau vlan).

Mode Ethernet, type de simulation automatique.

*Préparation : Redéfinir les vlan du **§2**, mais en utilisant les adresses mac (clic droit sur le switch, Editer table mac/vlan, bouton ajouter (+) ou modifier (…))*

sw1 :	*Postes*	*vlan*	***sw2*** :	*Postes*	*vlan*
	st3 (mac3)	*2*		*st7 (mac7)*	*3*
	st4 (mac4)	*2*		*st8 (mac8)*	*3*
	st5 (mac5)	*3*		*st11 (mac11)*	*2*
	st6 (mac6)	*3*		*st12 (mac12)*	*2*

st1, st2, st9 et st10 sont affectés au vlan 1 par défaut (vlan invité).

IMPORTANT : Bouton droit sur chaque commutateur, sélectionner découvrir le réseau (mise à jour des tables mac/port et port/vlan).

***Test 1 :** émettre une trame broadcast à partir de st1.*

Question :

- Quels postes reçoivent la trame ?

***Test 2 :** émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ?

Test 3 : *émettre une trame broadcast à partir de st5.*

Question :

- Quels postes reçoivent la trame ?

Conclusion :

- Après l'apprentissage automatique des tables mac/port et port/vlan, le comportement des vlan de niveau 2 est-il différent de celui des vlan de niveau 1 ?

6. Gestion des vlan de niveau 2

Mode conception réseau

Préparation : Connecter st11 sur le port 4 de sw2 et st10 sur le port 5 de sw2

Mode Ethernet, type de simulation automatique,

Test 1 : *émettre une trame unicast à partir de st11 vers st3*

Questions :

- Quels postes reçoivent la trame ?

- Quelle est la différence avec les tests 1 et 2 du §4 (vlan de niveau 1) ?

Mode Ethernet, type de simulation pas à pas, ***tracé sw2*** *(bouton aucun nœud tracé)*

Test 2 : *émettre une trame unicast à partir de st11 vers st3 (idem test 1).*

Questions :

- Expliquer comment le switch a trouvé le vlan du poste st11 ?

- Le poste st11 a-t-il changé de vlan après son déplacement ?

- Par rapport au vlan de niveau 1, quel est l'intérêt après un déplacement de poste ?

- Quel est l'inconvénient si on remplace un poste par un nouveau ?

Mode conception réseau

Préparation : Ajouter un hub, connecter st11 et st10 sur ce hub et connecter le hub au port 5 du switch sw2 (utiliser le port de cascade du hub)

Annexe

Mode Ethernet, type de simulation automatique, ***sans tracé sw1*** *(bouton aucun nœud tracé)*

Test 3 : *émettre une trame broadcast à partir de st10.*

Consulter la table port/vlan de sw2 (bouton droit sur le switch, consulter table port/vlan)

Question :

- A quel vlan est affecté le port 5 ?

Test 4 : *émettre une trame broadcast à partir de st11.*

Consulter la table port/vlan de sw2 (bouton droit sur le switch, consulter table port/vlan)

Questions :

- A quel vlan est affecté le port 5 ?

- L'accès aux postes du hub en fonction de leur vlan est-il fonctionnel ?

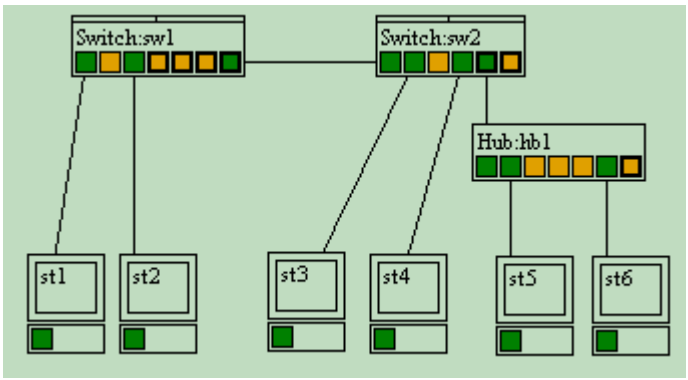
- Quelle précaution faut-il prendre avec cette architecture ?

SOLUTION

T.P. 1

1. Deux Switch (Labo01-2Switch-1Hub)

Passer en mode Ethernet



Le mode de transmission des trames *Objectif : découvrir les modes "On the fly" et "Store and foward"*

Méthode : mode trame réelle

Test 1 : *émettre une trame à partir de st1 vers st4 (unicast vers st4).*

Question

- Dans cette configuration, la trame est-elle reçu complètement par le switch avant d'être transmise sur le port Oui, le switch attend la réception complète de la trame pour la transmettre (Dans la réalité, il vérifie l'intégrité de la trame)

- Menu contextuel sur le switch, configurer, comment se nomme ce type de switch (transmission) ? Store and forward

Préparation : Menu contextuel sur les switchs, sélectionner configurer, choisir "On the fly".

Méthode : mode trame réelle

***Test 2 :** émettre une trame à partir de st4 vers st1 (unicast vers st1).*

Questions

- Dans cette configuration, quel est le comportement du switch pour transmettre la trame ? Il n'attend plus la réception complète de la trame, mais il la transmet dès qu'il a défini le port concerné (lecture de l'en-tête de la trame).

- Quel est l'avantage de ce mode de transmission ? La transmission est plus rapide (mais plus risquée si la trame est défectueuse)

Choisir d'émettre une trame à partir de st5 (broadcast) et à partir de st6 (broadcast) sans émettre les trames (cette situation sera l'étape de départ avant les tests 3 et 4)

***Test 3 :** émettre les trames à partir de st5 et de st6 de manière simultanée.*

Remarque : les longueurs de câble pour st5 et st6 sont très différentes

Questions

- Une collision est-elle détectée sur le réseau ? Oui, au niveau du hub

- Que fait le switch sw2 avec la trame avant la collision?: Il commence à la transmettre avant de détecter la collision

- Comment est la trame que reçoivent les postes st1 à st4 à la première transmission ? Incomplète

Préparation : Menu contextuel sur les switchs, sélectionner configurer, choisir "Store and forward".

***Test 4 :** émettre les trames à partir de st5 et de st6 de manière simultanée.*

Questions

- Une collision est-elle détectée sur le réseau ? Oui, au niveau du hub

- Que fait le switch sw2 avec la trame avant la collision?: Il stocke la trame.

- Les postes st1 à st4 sont-ils concernés par le trafic généré par la collision ? Non

- Quel est l'avantage du mode de transmission "Store and forward" ? Les trames défectueuses ne sont pas transmises sur le reste du réseau.

Préparation : Menu contextuel sur les switchs, sélectionner configurer, choisir "On the fly".

méthode : mode trame réelle, tracé le switch sw2, cocher Démo émission

Choisir d'émettre une trame à partir de st1 (unicast vers st4) et à partir de st4 (unicast vers st1) sans émettre les trames (cette situation sera l'étape de départ avant les tests 5 et 6)

***Test 5 :** émettre les trames à partir de st1 et de st4 (attendre que la trame de st1 arrive sur sw1 avant d'émettre de st4).*

Questions

- Une collision est-elle détectée sur le réseau ? Non

- Les trames peuvent-elles circuler vers leur destinataire, de manière simultanée ? Non

- Que fait le switch sw2 avec les deux trames avant de les transmettre ?: Il les stocke en attendant que les ports soient libres

Préparation : Cocher la case Full duplex.

***Test 6 :** émettre les trames à partir de st1 et de st4 (attendre que la trame de st1 arrive sur sw1 avant d'émettre de st4).*

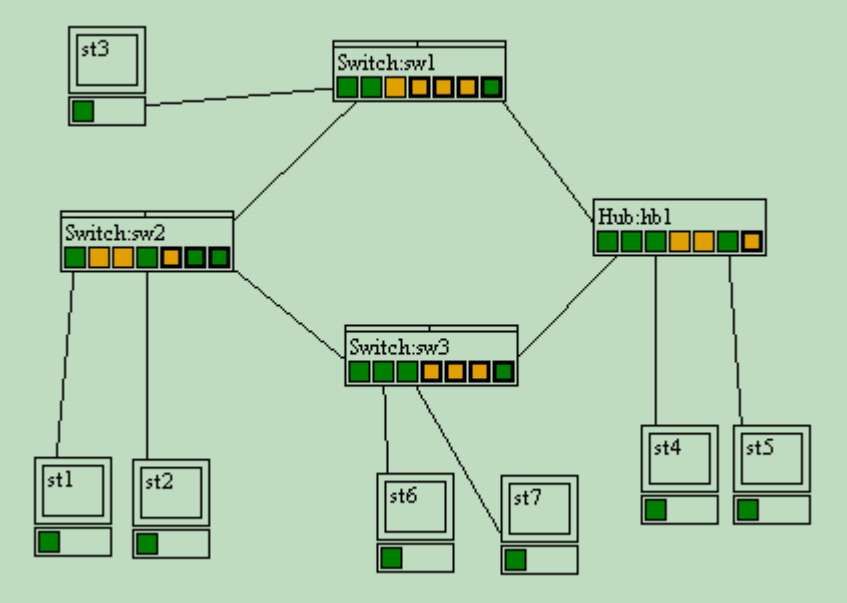
Question

- Le mode Full duplex est-il réalisé sur les deux types de liaison Station<->Switch et Switch<->Switch ? Oui

T.P. 2

1. Spanning Tree (Labo02-Spanning)

Passer en mode Ethernet



La gestion des boucles avec les switchs *Objectif : découvrir l'intérêt du spannig tree*

Méthode : mode automatique

Question : *Dans quel état sont les ports de cascade connectés des switchs et du hub ? connexion active.*

Test 1 : A partir de la station st1, émettre une trame unicast vers st7.

Question   *Expliquer le problème : On retrouve le problème vu avec les hubs, si le réseau comporte une boucle, certaines trames vont circuler en boucle de manière infinie (répéter sur les autres ports par chaque hub) , provocant de nombreuses collisions et perturbant le fonctionnement du réseau.*

Préparation : Passer en mode Conception réseau, menu contextuel sur les switchs, sélectionner configurer, cocher gestion spanning tree pour chaque switch. Passer en mode Ethernet, méthode : mode automatique

Question :   *Dans quel état sont les ports de cascade connectés des switchs ? Pour un switch (sw1), un port de cascade connecté est bloqué automatiquement (en rose par défaut)*

Test 2 : *A partir de la station st1, émettre une trame unicast vers st4, puis l'inverse, de st4 vers st1.*

Conclusion sur le spanning tree : La gestion spanning tree des switchs a supprimé la boucle en bloquant une liaison sur un des ports d'un switch.

Préparation : Passer en mode Conception réseau, supprimer la connexion entre le switch sw2 et le switch sw3 pour simuler une rupture de liaison (clic droit sur un port de cascade, supprimer le câble).

Passer en mode Ethernet, méthode : mode automatique

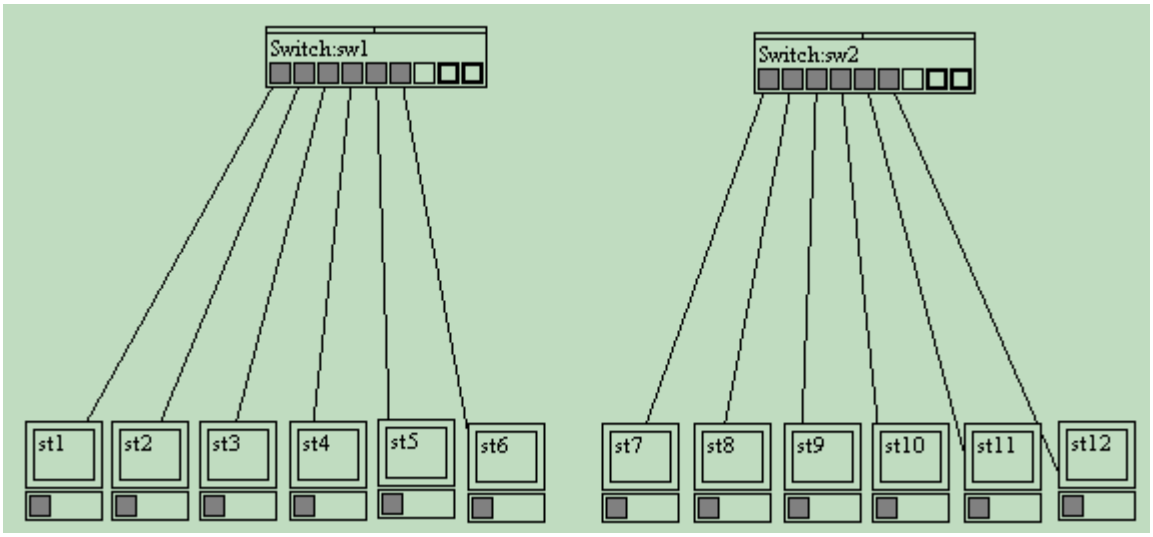
Question :

Dans quel état sont les ports de cascade connectés des switchs ? Les ports sont : connexion active, le port de cascade qui était bloqué est devenu actif automatiquement.

Test 3 : *A partir de la station st1, émettre une trame unicast vers st4, puis l'inverse, de st4 vers st1.*

Conclusion sur l'intérêt d'avoir une boucle dans le réseau avec la gestion spanning tree : L'intérêt de la boucle est d'avoir un chemin redondant non actif (désactivé par le spanning tree) qui automatiquement peut devenir actif si une des liaisons entre les switchs devient défectueuse. Dans ces conditions, on obtient une tolérance aux pannes pour les liaisons entre les switchs.

T.P. 3



1. Deux Switchs - (Labo3)

Mode conception réseau

Relier les deux switchs pour obtenir une communication entre les 12 postes, vérifier en mode Ethernet.

Question :
- Comment obtenir une connexion correcte entre les deux switchs ?

Mode Ethernet, type de simulation automatique

Test 1 : *émettre une trame broadcast à partir de st3.*

Question :
- Quels postes reçoivent la trame ? Tous

Test 2 : *émettre une trame unicast à partir de st3 vers st11.*

Question :
- La trame est-elle diffusée sur tous les ports ? Non, seulement le port 9 de sw1 et le 5 de sw2

2. Vlan de niveau 1

Mode conception réseau

Préparation : Configurer les commutateurs pour définir des vlan de niveau 1 (bouton droit sur le switch, Configurer, Niveau vlan).

Annexe

Mode Ethernet, type de simulation automatique

*Préparation : Définir la configuration des vlan suivante pour **chaque** commutateur :*

(bouton droit sur le switch, Editer table port/vlan, sélectionner une ligne, bouton modifier (…)).

sw1 *:*	*Postes*	*vlan*	***sw2*** *:*	*Postes*	*vlan*
	st1	*1 (par défaut)*		*st7*	*3*
	st2	*1 (par défaut)*		*st8*	*3*
	st3	*2*		*st9*	*1 (par défaut)*
	st4	*2*		*st10*	*1 (par défaut)*
	st5	*3*		*st11*	*2*
	st6	*3*		*st12*	*2*

Laisser les valeurs par défaut pour les autres ports.

***Test 1 :** émettre une trame broadcast à partir de st1.*

Question :

- Quels postes reçoivent la trame ? st2, st9 et st10

***Test 2 :** émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ? st4

***Test 3 :** émettre une trame broadcast à partir de st5.*

Question :

- Quels postes reçoivent la trame ? st6

Méthode : type de simulation pas à pas, tracé : sw1 (bouton aucun nœud tracé)

***Test 4 :** émettre une trame broadcast à partir de st3 (idem test 2).*

Questions :

- Expliquer pourquoi sw2 ne reçoit pas les broadcasts des tests 2 à 4 ? Ce broadcast est transmis sur les ports du Vlan 2 et les ports 802.1q, mais le port 9 (non 802.1q) qui est connecté au sw2 est sur le vlan 1

- Expliquer pourquoi st1 et st5 ne reçoivent pas la trame broadcast ? Ces postes sont sur les vlan 1 et 3

3. Port 802.1q

Mode conception réseau

Préparation : Configurer les deux commutateurs pour définir un port 802.1q (bouton droit sur le switch, Configurer, Nbre de ports 802.1q).

Refaire la liaison entre les deux commutateurs en utilisant le port 802.1q de chaque commutateur.

*Mode Ethernet, type de simulation automatique **sans tracé sw1** (bouton aucun nœud tracé)*

***Test 1 :** émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ? st4, st11 et st12

*Mode Ethernet, type de simulation pas à pas, **tracé sw2** (bouton aucun nœud tracé)*

***Test 2 :** émettre une trame broadcast à partir de st5.*

Questions :

- Quels postes reçoivent la trame ? st6, st7 et st8

- Pour les observateurs, la trame qui circule entre les deux ports 802.1q est légèrement différente, comment le simulateur représente cette différence ? La trame commence par une zone rouge pour simuler la marque "tag" qui permet de définir le vlan associé à la trame.

- Quelle action particulière a le port 802.1q de sw2 sur le contenu de la trame ? Il enlève la marque du vlan 2

- Quels vlan utilisent le port 802.1q ? tous

*Mode Ethernet, type de simulation automatique, **sans tracé sw2** (bouton aucun nœud tracé)*

***Test 3 :** émettre une trame unicast à partir de st11 vers st3.*

Question :

- Quels postes reçoivent la trame ? st3

***Test 4 :** émettre une trame unicast à partir de st11 vers st5.*

Question :

- Quels postes reçoivent la trame et expliquer ? aucun, st5 n'est pas dans le même vlan que st11

Conclusion :

- Les broadcasts d'un vlan générent-ils du trafic sur les autres vlan ? Non

- La communication entre les vlan est-elle possible dans notre configuration ? Non

- En appelant domaine de diffusion, un ensemble de postes recevant la même trame de broadcast, combien de domaines de diffusion différents présente ce réseau ? 3 (un par vlan)

4. Gestion des vlan de niveau 1

Mode conception réseau

Préparation : Connecter st11 sur le port 4 de sw2 et st10 sur le port 5 de sw2

Mode Ethernet, type de simulation automatique,

***Test 1 :** émettre une trame unicast à partir de st11 vers st3 (idem test 3 précédent).*

Question :

- Quels postes reçoivent la trame ? aucun

*Mode Ethernet, type de simulation pas à pas, **tracé sw1** (bouton aucun nœud tracé)*

***Test 2 :** émettre une trame unicast à partir de st11 vers st3 (idem test 1).*

Questions :

- Le poste st11 a-t-il changé de vlan après son déplacement ? Oui, il est passé sur le port 4, vlan 1

- Expliquer le résultat pour la trame ? la trame est perdue, st11 n'est plus dans le même vlan que st3

- Avec des vlan de niveau 1, quelle est le problème lié au déplacement d'un poste pour l'administrateur réseau ? Chaque déplacement de poste (changement de port) nécessite une configuration de la table port/vlan.

Mode conception réseau

Préparation : Ajouter un hub, connecter st11 et st10 sur ce hub et connecter le hub au port 5 du switch sw2 (utiliser le port de cascade du hub)

*Mode Ethernet, type de simulation automatique, **sans tracé sw1** (bouton aucun nœud tracé)*

***Test 3 :** émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ? st4, st10, st11 et st12

- Pourquoi st10 st11 sont-ils maintenant dans le même vlan ? Ils sont connectés au hub qui lui même est connecté à sw2 sur un port affecté au vlan 2, donc tous les postes du hub sont dans le vlan 2.

Mode conception réseau

Préparation : Remettre st11 et st10 sur leur port d'origine, (st11 sur le port 5 de sw2 et st10 sur le port 4) et supprimer le hub.

5. Vlan de niveau 2

Mode conception réseau

Préparation : Configurer les commutateurs pour définir des vlan de niveau 2, (bouton droit sur le switch, Configurer, Niveau vlan).

Mode Ethernet, type de simulation automatique.

*Préparation : Redéfinir les vlan du **§2**, mais en utilisant les adresses mac (clic droit sur le switch, Editer table mac/vlan, bouton ajouter (+) ou modifier (…))*

sw1 :	Postes	vlan	**sw2** :	Postes	vlan
	st3 (mac3)	2		st7 (mac7)	3
	st4 (mac4)	2		st8 (mac8)	3
	st5 (mac5)	3		st11 (mac11)	2
	st6 (mac6)	3		st12 (mac12)	2

st1, st2, st9 et st10 sont affectés au vlan 1 par défaut (vlan invité).

IMPORTANT : Bouton droit sur chaque commutateur, sélectionner découvrir le réseau (mise à jour des tables mac/port et port/vlan).

***Test 1 :** émettre une trame broadcast à partir de st1.*

Question :

- Quels postes reçoivent la trame ? st2, st9 et st10

***Test 2 :** émettre une trame broadcast à partir de st3.*

Question :

- Quels postes reçoivent la trame ? st4, st11 et st12

***Test 3 :** émettre une trame broadcast à partir de st5.*

Question :

- Quels postes reçoivent la trame ? st6, st7 et st8

Conclusion :

- Après l'apprentissage automatique des tables mac/port et port/vlan, le comportement des vlan de niveau 2 est-il différent de celui des vlan de niveau 1 ? Non

6. Gestion des vlan de niveau 2

Mode conception réseau

Préparation : Connecter st11 sur le port 4 de sw2 et st10 sur le port 5 de sw2

Mode Ethernet, type de simulation automatique,

***Test 1 :** émettre une trame unicast à partir de st11 vers st3*

Questions :

- Quels postes reçoivent la trame ? st3

- Quelle est la différence avec les tests 1 et 2 du §4 (vlan de niveau 1) ? Ici, la trame n'est pas perdue après le déplacement du poste.

*Mode Ethernet, type de simulation pas à pas, **tracé sw2** (bouton aucun nœud tracé)*

***Test 2 :** émettre une trame unicast à partir de st11 vers st3 (idem test 1).*

Questions :

- Expliquer comment le switch a trouvé le vlan du poste st11 ? grâce à la table mac/vlan et l'adresse mac11

- Le poste st11 a-t-il changé de vlan après son déplacement ? Non

- Par rapport au vlan de niveau 1, quel est l'intérêt après un déplacement de poste ? pas de configuration vlan

- Quel est l'inconvénient si on remplace un poste par un nouveau ? adresse mac dans vlan invité

Mode conception réseau

Annexe

Préparation : Ajouter un hub, connecter st11 et st10 sur ce hub et connecter le hub au port 5 du switch sw2 (utiliser le port de cascade du hub)

Mode Ethernet, type de simulation automatique, ***sans tracé sw1*** *(bouton aucun nœud tracé)*

Test 3 : *émettre une trame broadcast à partir de st10.*

Consulter la table port/vlan de sw2 (bouton droit sur le switch, consulter table port/vlan)

Question :

- A quel vlan est affecté le port 5 ? vlan 1 (mac10 appartient au vlan 1)

Test 4 : *émettre une trame broadcast à partir de st11.*

Consulter la table port/vlan de sw2 (bouton droit sur le switch, consulter table port/vlan)

Questions :

- A quel vlan est affecté le port 5 ? vlan 2 (mac11 appartient au vlan 2)

- L'accès aux postes du hub en fonction de leur vlan est-il fonctionnel ? Non, le port 5 est affecté à un seul vlan à la fois, qui de plus va changer en fonction du trafic.

- Quelle précaution faut-il prendre avec cette architecture ? Tous les postes du hub (adresses mac) doivent-être dans le même vlan.

Références

[1] www.westnetlearning.com

[2] « Les réseaux locaux LAN », Alain Bawin, Notes 2002-2003.

[3] « Les équipements d'interconnexion », B. Jaumard, IFT3320/IFT6320 – Hiver 2003.

[4] Delmas, O. (1997). Communications par commutation de circuits dans les réseaux d'interconnexion (Doctoral dissertation, Université Nice Sophia Antipolis).