Les réseaux locaux

Plan :

Chapitre Aperçu

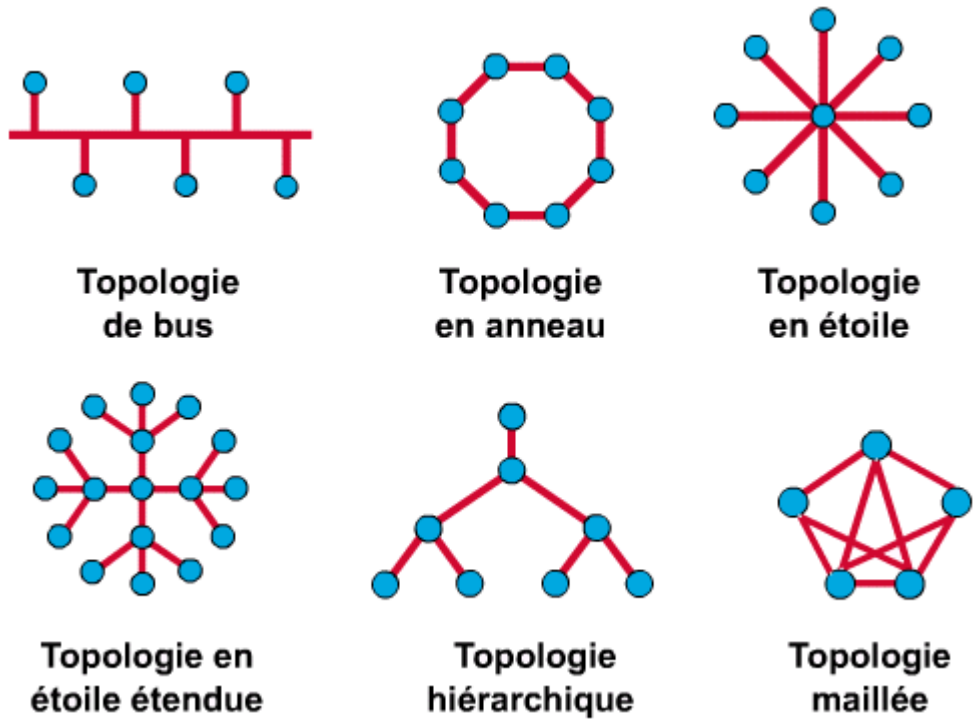
Maintenant que vous avez acquis une compréhension de base du modèle OSI et de ce qui arrive aux paquets de données lorsqu'ils traversent les couches, il est temps de commencer à examiner les unités de réseautage élémentaires. Couche par couche, vous étudierez les unités utilisées à chaque couche lorsque les paquets de données circulent de la source à la destination. Ce chapitre porte sur les unités de réseau local. Comme vous le savez, les réseaux locaux sont des réseaux à haute vitesse et à faible pourcentage d'erreur couvrant une région géographique relativement peu étendue (jusqu'à quelques milliers de mètres). Les réseaux locaux relient des postes de travail, des périphériques, des terminaux et d'autres unités à l'intérieur d'un immeuble ou d'une région géographique limitée.

Dans le présent chapitre, vous étudierez les unités de réseau local de base et l'évolution des unités de réseautage. Vous étudierez aussi les unités de réseautage qui fonctionnent à chaque couche du modèle OSI, ainsi que la façon dont les paquets sont acheminés par chaque unité lorsqu'ils traversent les couches du modèle OSI. Enfin, vous étudierez les étapes de base de la construction des réseaux locaux. Durant l'étude de ce chapitre, n'oubliez pas que grâce à l'interconnexion des unités de réseautage, les nombreux appareils de bureau (habituellement des ordinateurs personnels) connectés en réseaux locaux ont accès à un média à large bande.

1 Les unités de réseau local de base

1.1 Les topologies

La *topologie* définit la structure du réseau. La définition de la topologie comprend deux parties : la topologie physique, qui est la disposition réelle des fils (média), et la topologie logique, qui précise la façon dont les hôtes accèdent au média. Les topologies physiques couramment utilisées sont la topologie de bus, en anneau, en étoile, en étoile étendue, hiérarchique et maillée. Elles sont illustrées dans la figure. [1]



1.1.1 La topologie de bus linéaire

Dans la *topologie de bus*, tous les nœuds sont connectés directement à une liaison et il n'y a aucune connexion entre les nœuds.
Chaque unité hôte est connectée à un fil commun. Dans cette topologie, les unités clés sont celles qui permettent à l'unité hôte de joindre le média partagé unique ou de se connecter à lui. L'un des avantages de cette topologie est que toutes les unités hôtes sont connectées entre elles et qu'elles peuvent donc communiquer directement. En revanche, l'un des inconvénients est que les unités hôtes sont déconnectées les unes des autres s'il se produit un bris du câble.
Une topologie de bus permet à toutes les unités de réseautage de voir tous les signaux de toutes les autres unités, ce qui peut être un avantage si vous voulez que toute l'information se rende à toutes les unités. Cela peut toutefois être un désavantage car les collisions et les problèmes de trafic sont courants.

1.1.2 La topologie en anneau

Une *topologie en anneau* est un anneau fermé constitué de nœuds et de liaisons, chaque nœud étant connecté aux deux nœuds adjacents uniquement. Toutes les unités sont directement connectées les unes aux autres en série.
Pour que l'information circule, chaque station doit la passer à la station adjacente.

1.1.3 La topologie à deux anneaux

Une *topologie à deux anneaux* consiste en deux anneaux concentriques dans lesquels chaque station est liée uniquement à sa voisine d'anneau. Les deux anneaux ne sont pas interconnectés.
La topologie à deux anneaux est identique à la topologie en anneau, sauf qu'elle comporte un deuxième anneau redondant qui relie les mêmes unités. En d'autres termes, pour assurer la fiabilité et la souplesse du réseau, chaque unité de réseautage fait partie de deux topologies en anneau indépendantes.
La topologie à deux anneaux agit comme s'il y avait deux anneaux indépendants, mais un seul est utilisé à la fois.

1.1.4 La topologie en étoile

Une *topologie en étoile* comporte un nœud central, duquel partent toutes les liaisons aux autres nœuds, et ne permet aucune autre liaison.
Son principal avantage est que tous les autres nœuds peuvent communiquer entre eux de manière pratique grâce au nœud central. Par contre, son plus grand désavantage est que tout le réseau est déconnecté si le nœud central connaît une défaillance. Selon le type d'unité de réseautage utilisé au centre du réseau en étoile, les collisions peuvent s'avérer un problème.
Toute l'information en circulation passe par une unité. Cela peut être souhaitable pour des raisons de sécurité ou de restriction d'accès, mais cette méthode souffre de tout problème associé au nœud central de l'étoile.

1.1.5 La topologie en étoile étendue

La *topologie en étoile étendue* est identique à la topologie en étoile, sauf que chaque nœud connecté au nœud central est aussi le centre d'une autre étoile.
Une topologie en étoile étendue est constituée d'une topologie en étoile principale dont chacun des nœuds d'extrémité est aussi le centre de sa propre topologie en étoile. L'avantage de cette topologie est qu'elle réduit les longueurs de câble et qu'elle limite le nombre d'unités interconnectées à un nœud central.
La topologie en étoile étendue est très hiérarchique et contribue à maintenir l'information à un niveau local. C'est la façon dont le système téléphonique est présentement structuré.

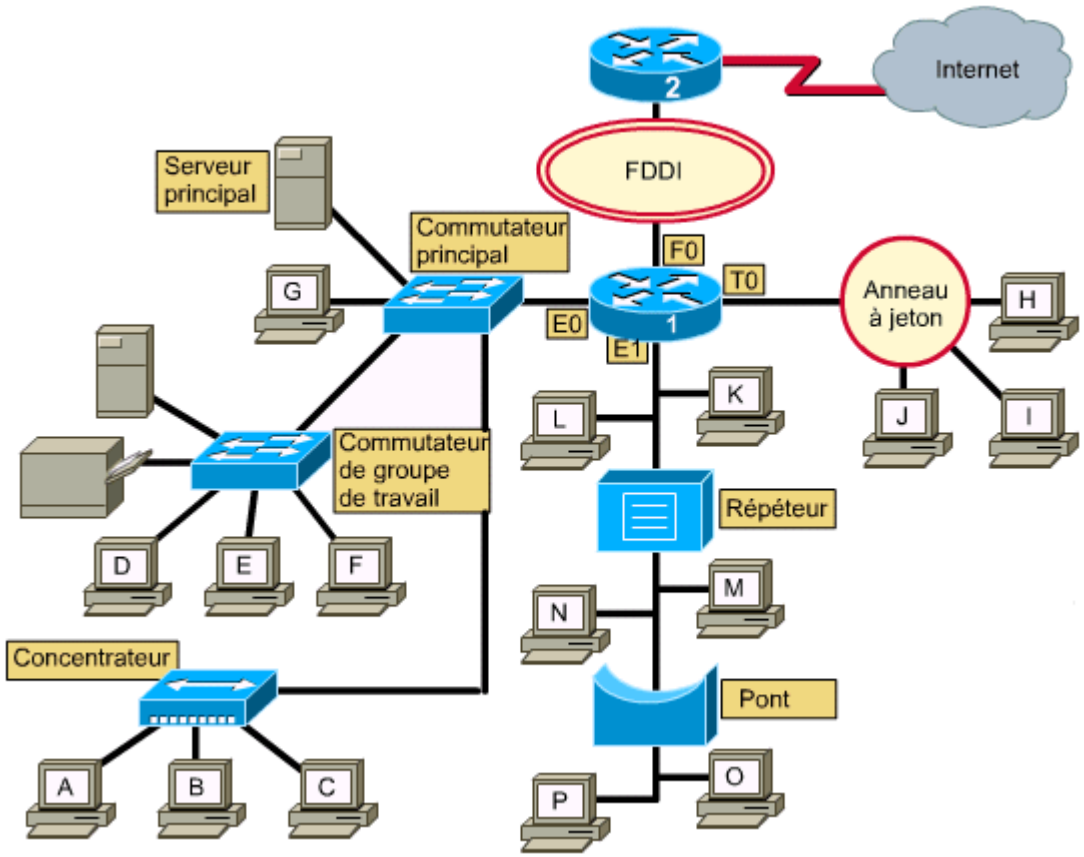
1.1.6 La topologie hiérarchique

La *topologie hiérarchique* ressemble à la topologie en étoile étendue, la principale différence étant qu'elle n'utilise pas un nœud central. Elle utilise plutôt un nœud de circuit duquel partent des branches vers d'autres nœuds. Il existe deux types de topologies arborescentes : l'arbre binaire (chaque nœud se divisant en deux liaisons) et l'arbre de base (un circuit de base comportant des branches de nœud avec des liaisons). Le flux d'information est hiérarchique.

1.1.7 La topologie maillée complète

Dans une topologie complète, ou *topologie maillée*, chaque nœud est relié directement à chacun des autres nœuds.
Ce type de câblage présente des avantages et des inconvénients très particuliers. Comme chaque nœud est physiquement relié à chacun des autres nœuds, créant ainsi une connexion redondante, l'information peut passer par d'autres connexions pour atteindre sa destination si l'une des liaisons est défaillante. En outre, cette topologie permet à l'information d'emprunter plusieurs trajets dans son voyage à travers le réseau. Le principal inconvénient physique est que si le nombre de nœuds n'est pas très réduit, la quantité de média pour les liaisons et le nombre de connexions à ces liaisons deviennent gigantesques.

La topologie logique d'un réseau est la méthode qu'utilisent les hôtes pour communiquer par le média. Les deux types de topologie logique les plus courants sont la diffusion et le passage de jeton.
La diffusion signifie simplement que chaque hôte envoie ses données à tous les autres hôtes sur le média du réseau. Les stations n'ont pas à respecter un certain ordre pour utiliser le réseau; il s'agit d'une méthode de type "premier arrivé, premier servi". L'Ethernet fonctionne de cette façon.
Le deuxième type de topologie est le passage de jeton. Selon cette méthode, l'accès au réseau est contrôlé en passant un jeton électronique de manière séquentielle à chaque hôte. Lorsqu'un hôte reçoit le jeton, cela signifie qu'il peut transmettre des données sur le réseau. Si l'hôte n'a pas de données à transmettre, il passe le jeton à l'hôte suivant et le processus est répété.



Le schéma de la figure précédente présente de nombreuses topologies, il représente un réseau local de complexité moyenne, comme celui qu'on retrouve habituellement dans une école ou une petite entreprise. Il fait appel à plusieurs symboles et illustre de nombreux concepts de réseautage dont l'apprentissage demande un certain temps.

1.2 Les unités de réseau local dans une topologie

Les unités directement connectées à un segment de réseau sont appelées hôtes. Ces hôtes peuvent être des ordinateurs, des clients, des serveurs, des imprimantes, des scanneurs et de nombreux autres dispositifs. Ces unités fournissent les connexions réseau aux utilisateurs grâce auxquelles ils peuvent partager, créer et obtenir de l'information. Les unités hôte peuvent exister sans réseau. Toutefois, les capacités d'un hôte qui n'est pas relié à un réseau sont très limitées.

Les unités hôte n'appartiennent à aucune couche. Elles sont connectées physiquement au média réseau grâce à leur carte réseau et les fonctions des autres couches OSI sont exécutées par des logiciels exploités par l'hôte. Cela signifie que les unités hôte fonctionnent au niveau des sept couches du modèle OSI. Elles se chargent du processus d'encapsulation et de désencapsulation afin de pouvoir envoyer du courrier électronique, imprimer des rapports ou accéder à des bases de données.

1.3 Les cartes réseau

La carte réseau, appartient à la couche 2, la couche liaison de données, du modèle OSI. Pour ce qui est de son aspect physique, une carte réseau est une plaquette de circuits imprimés qui loge dans l'emplacement d'extension d'un bus, sur la carte-mère d'un ordinateur ou sur un périphérique. On l'appellent aussi adaptateur réseau. Sa fonction consiste à adapter l'unité hôte au média de réseau.

Les cartes réseau sont considérées comme des dispositifs de couche 2 parce que chaque carte réseau dans le monde porte un nom de code unique appelé adresse MAC (Media Access Control). Cette adresse est utilisée pour contrôler la communication des données de l'hôte dans le réseau. La carte réseau contrôle l'accès de l'hôte au média.

1.4 Média

La fonction de base des médias consiste à acheminer un flux d'informations, sous forme de bits et d'octets, dans un réseau local. Si on exclut les réseaux locaux sans fil (qui utilisent l'atmosphère ou l'espace comme média), de façon générale, les médias de réseautage confinent les signaux réseau à des fils, des câbles ou à la fibre optique. Les médias de réseautage sont considérés comme des composants de couche 1 des réseaux locaux.
Vous pouvez construire des réseaux informatiques en utilisant plusieurs types de médias différents. Chaque média présente des avantages et des désavantages et ce qui constitue un avantage dans le cas d'un média (le coût, dans le cas du câble de catégorie 5) peut être un désavantage dans le cas d'un autre (le coût, dans le cas de la fibre optique). Certains des avantages et des désavantages sont énumérés ci-dessous.

- Longueur de câble
- Coût
- Facilité d'installation
- Nombre total d'ordinateurs connectés au média.

Le câble coaxial, la fibre optique et même l'atmosphère peuvent transporter des signaux de réseau. Toutefois, le principal média que nous étudierons se nomme câble à paires torsadées non blindées de catégorie 5.

1.5 Les répéteurs

Il existe un grand nombre de médias, qui présentent chacun leurs avantages et leurs inconvénients. Par exemple, pour le câble à paires torsadées non blindées de catégorie 5 la longueur maximale dans un réseau est de 100 mètres. Pour prolonger un réseau au-delà de cette limite, nous devons y ajouter une unité nommée *répéteur*.

Le but du répéteur est d'amplifier les signaux réseau et de les resynchroniser au niveau du bit pour leur permettre de voyager sur de plus longues distances dans le média. N'oubliez pas de prendre en compte la règle des 5 avec les répéteurs, aussi nommée règle 5-4-3, lorsque vous prolongez des segments de réseau local. Cette règle stipule que vous pouvez connecter cinq segments de réseau de bout en bout à l'aide de quatre répéteurs, mais seuls trois des segments peuvent comporter des hôtes (ordinateurs).

Les répéteurs sont des unités à un seul port "d'entrée" et à un seul port de "sortie". Ce sont des unités de couche 1 du modèle OSI, car ils agissent uniquement au niveau du bit et ne se soucient d'aucune autre information.

1.6 Les concentrateurs

Le but du concentrateur est d'amplifier et de resynchroniser les signaux réseau. Il fait cela au niveau du bit pour un grand nombre d'hôtes (p. ex. 4, 8 ou même 24) en utilisant un processus nommé concentration. Cette définition est très semblable à celle du répéteur, c'est pourquoi le concentrateur est aussi connu sous le nom de répéteur multiport. La différence entre les deux est le nombre de câbles connectés à l'unité. On utilise un concentrateur pour créer une topologie physique en étoileet ainsi accroître la fiabilité d'un réseau, car le concentrateur permet à un câble unique de défaillir sans perturber le fonctionnement d'un réseau entier. Cela diffère de la topologie de bus dans laquelle un câble défectueux perturbe le réseau entier. Les concentrateurs sont considérés comme des unités de couche 1 parce qu'ils ne font qu'amplifier le signal et le diffuser par tous leurs ports (connexions réseau).

Il existe différentes classifications des concentrateurs en réseautage. La première est celle des concentrateurs actifs ou passifs. La plupart des concentrateurs modernes sont actifs; ils tirent l'énergie d'un bloc d'alimentation pour rafraîchir les signaux réseau. Certains concentrateurs sont appelés passifs, car ils ne font que diviser le signal entre plusieurs utilisateurs, tout comme un cordon en "Y". Les concentrateurs passifs n'amplifient pas les bits, ainsi ils ne prolongent pas la longueur des câbles, ils ne font que permettre à deux hôtes ou plus de se connecter à un même segment de câble.
Une autre classification divise les concentrateurs en unités intelligentes et unités non intelligentes. Les concentrateurs intelligents sont dotés de ports de console, ce qui signifie qu'ils peuvent être programmés pour gérer le trafic réseau. Les concentrateurs non intelligents prennent simplement un signal de réseau entrant et le répètent à chaque port sans avoir la capacité d'effectuer des fonctions de gestion.
Dans un réseau en anneau à jeton, le rôle du concentrateur est assumé par l'unité d'accès au média MAU (Media Access Unit). Physiquement, cette unité ressemble à un concentrateur, mais la technologie en anneau à jeton est très différente. Dans le cas des interfaces FDDI, l'unité d'accès au média est appelée concentrateur. Les unités d'accès au média sont aussi des unités de couche 1.

1.7 Les ponts

Un pont est une unité de couche 2 conçue pour connecter deux segments de réseau local. Le rôle du pont est de filtrer le trafic sur un réseau local pour conserver le trafic local au niveau local, tout en établissant une connectivité avec d'autres parties (segments) du réseau local pour le trafic qui y est destiné. Comme chaque unité de réseautage possède une adresse MAC unique sur la carte réseau, le pont effectue le suivi des adresses MAC se trouvant de chacun de ses côtés et prend des décisions en fonction de cette liste d'adresses.

Il est important de noter que, tout comme un répéteur, un pont connecte deux segments à la fois. Comme nous l'avons vu dans le cas de la combinaison répéteur-concentrateur, une autre unité est utilisée dans le cas des connexions à plusieurs ponts.

1.8 Les commutateurs

Le commutateur est une unité de couche 2 tout comme le pont. En fait, un commutateur se nomme aussi un pont multiport, tout comme un concentrateur est aussi un répéteur multiport. La différence entre le concentrateur et le commutateur est que ce dernier prend des décisions en fonction des adresses MAC et que le concentrateur ne prend aucune décision. En raison des décisions qu'il prend, le commutateur rend le réseau local beaucoup plus efficace. Il effectue cela en "commutant" les données uniquement au port auquel le bon hôte est connecté. Par contraste, un concentrateur achemine les données à tous les ports, de sorte que tous les hôtes doivent examiner et traiter (accepter ou rejeter) toutes les données.

1.9 Les routeurs

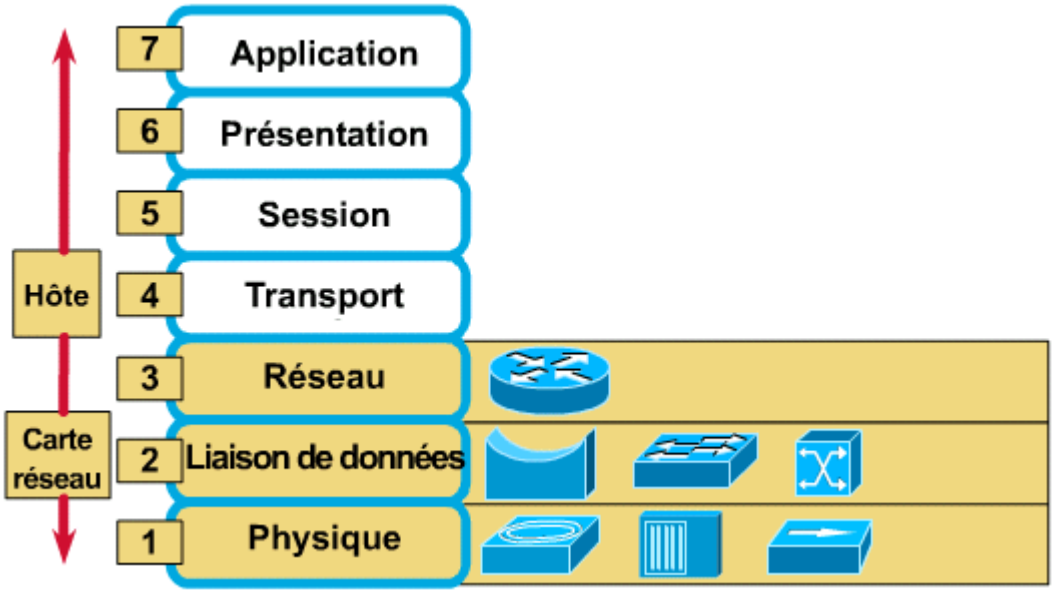
Le routeur fonctionne à la couche réseau du modèle OSI, aussi nommée couche 3. Travailler à la couche 3 permet au routeur de prendre des décisions en fonction de groupes d'adresses réseau (classes), par opposition aux adresses MAC individuelles utilisées à la couche 2. Les routeurs peuvent aussi connecter différentes technologies de couche 2, telles qu'Ethernet, l'anneau à jeton et l'interface FDDI. En raison de leur capacité d'acheminer les paquets en fonction de l'information de couche 3, les routeurs sont devenus le fédérateur d'Internet et exécutent le protocole IP.
Le rôle du routeur consiste à examiner les paquets entrants (données de couche 3), à choisir la meilleure voie pour les acheminer sur le réseau et à les commuter ensuite au port de sortie approprié. Sur les grands réseaux, les routeurs sont les dispositifs de régulation du trafic les plus importants. Ils permettent à presque tous les types d'ordinateur de communiquer avec tout ordinateur n'importe où dans le monde!

2. Unités et couches correspondantes

Les ordinateurs hôtes et les serveurs fonctionnent au niveau des couches 2 à 7 et sont responsables de l'encapsulation. Les émetteurs-récepteurs, les répéteurs et les concentrateurs sont tous considérés comme des dispositifs actifs de couche 1, car ils n'agissent que sur les bits et ont besoin d'énergie. Les câbles de raccordement, tableaux de connexions et autres éléments d'interconnexion sont considérés comme des composants passifs de couche 1, car ils fournissent simplement une voie de passage pour le courant (figure ci dessous)

À titre de dépositaires des adresses MAC, les cartes réseau sont des dispositifs de couche 2, mais elles sont aussi des dispositifs de couche 1, car elles s'occupent également de signalisation et d'encodage. Les ponts et les commutateurs sont considérés comme des dispositifs de couche 2 parce qu'ils utilisent l'information de couche 2 (adresses MAC) pour décider d'acheminer ou non les trames. Ils fonctionnent aussi à la couche 1 afin de permettre aux bits d'interagir avec le média.

Les routeurs sont considérés comme des unités de couche 3 parce qu'ils utilisent les adresses de couche 3 (adresses réseau) pour optimiser le routage et commuter les paquets sur la bonne route. Les interfaces des routeurs fonctionnent aux couches 1, 2 et 3. Les nuages, qui peuvent comprendre des routeurs, des commutateurs, des serveurs et de nombreux autres dispositifs dont nous n'avons pas encore parlé, touchent les couches 1 à 7.



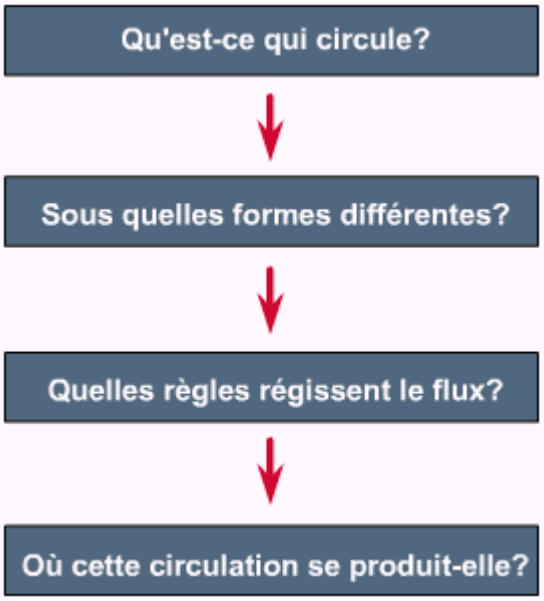
Unités et couches correspondantes

Chapitre 2 : Modèle OSI

2.1 Modèle général de communication

2.1.1 Utilisation des couches pour analyser des problèmes dans le flux de matériaux

Le concept de *couches* vous aidera à comprendre ce qui se produit pendant la communication entre deux ordinateurs. Les questions indiquées dans la figure 1portent sur le mouvement d'objets physiques comme le trafic routier ou les données électroniques. Ce déplacement d'objets, qu'il soit physique ou logique, s'appelle flux. De nombreuses couches aident à décrire en détail le cheminement du flux.



2.1.2 Protocole

Pour que des paquets de données puissent se rendre d'un ordinateur source à un ordinateur de destination sur un réseau, il est important que toutes les unités du réseau communiquent dans la même langue ou *protocole*. Un *protocole* consiste en un ensemble de règles qui rehaussent l'efficacité des communications au sein d'un réseau.

Voici une définition technique d'un protocole de communication de données : ensemble de règles ou convention qui détermine le format et la transmission des données. La couche n d'un ordinateur communique avec la couche n d'un autre ordinateur. Les règles et conventions utilisées lors de cette communication sont collectivement appelées *protocole de couche n*.

2.2.1 La raison d'être du modèle de référence OSI

Le modèle de référence OSI est le principal modèle des communications en réseau. Bien qu'il existe d'autres modèles, la majorité des fournisseurs de réseaux relient aujourd'hui leurs produits à ce modèle de référence, particulièrement lorsqu'ils désirent donner aux utilisateurs la formation sur l'utilisation de leurs produits. Ils le considèrent comme le meilleur outil offert pour décrire l'envoi et la réception de données dans un réseau.

Le modèle de référence OSI vous permet de voir les fonctions réseau exécutées à chaque couche. Plus important encore, ce modèle de référence constitue un cadre que vous pouvez utiliser pour comprendre comment l'information circule dans un réseau. En outre, vous pouvez vous servir du modèle de référence OSI pour visualiser comment l'information, ou les données, circule à partir des programmes d'application (ex. : tableurs, documents, etc.), en passant par un média réseau (ex. : fils, etc.), jusqu'à un autre programme d'application se trouvant dans un autre ordinateur en réseau, même si l'expéditeur et le destinataire utilisent des types de réseau différents.

Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau précise. Cette répartition des fonctions réseau est appelée *organisation en couches*. Le découpage du réseau en sept couches présente les avantages suivants :

- Il permet de diviser les communications sur le réseau en éléments plus petits et simples.
- Il uniformise les éléments du réseau de manière à permettre le développement et le soutien multifournisseur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Il empêche les changements apportés à une couche d'influer sur les autres couches, ce qui assure un développement plus rapide.
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.

Le problème consistant à déplacer de l'information entre des ordinateurs est divisé en sept problèmes plus petits et plus faciles à gérer dans le modèle de référence OSI. Chacun des sept petits problèmes est représenté par une couche particulière du modèle. Voici les sept couches du modèle de référence OSI :

Couche 7 : la couche application
Couche 6 : la couche de présentation
Couche 5 : la couche session
Couche 4 : la couche de transport
Couche 3 : la couche réseau
Couche 2 : la couche liaison de données
Couche 1 : la couche physique

2.2.2 Les fonctions de chaque couche

Chaque couche du modèle OSI doit exécuter une série de fonctions pour que les paquets de données puissent circuler d'un ordinateur source à un ordinateur de destination sur un réseau. Vous trouverez ci-dessous une brève description de chaque couche du modèle de référence OSI qui est illustré dans la figure.

Couche 7 : La couche application 7

La couche application est la couche OSI la plus près de l'utilisateur; elle fournit des services réseau aux applications de l'utilisateur. Elle se distingue des autres couches en ce qu'elle ne fournit pas de services aux autres couches OSI, mais seulement aux applications à l'extérieur du modèle OSI. Voici des exemples de ce type d'application : tableurs, traitement de texte et logiciels de terminaux bancaires. La couche application détermine la disponibilité des partenaires de communication voulus, assure la synchronisation et établit une entente sur les procédures de reprise sur incident et de contrôle de l'intégrité des données. Pour vous souvenir facilement des fonctions de la couche 7, pensez aux navigateurs.

Couche 6 : La couche de présentation 6

La couche de présentation s'assure que l'information envoyée par la couche application d'un système est lisible par la couche application d'un autre système. Au besoin, la couche de présentation traduit différents formats de représentation des données en utilisant un format commun. Pour vous souvenir facilement des fonctions de la couche 6, pensez à un format de données courant.

Couche 5 : La couche session 5

Comme son nom l'indique, la couche session ouvre, gère et ferme les sessions entre deux systèmes hôtes en communication. Cette couche fournit des services à la couche de présentation. Elle synchronise également le dialogue entre les couches de présentation des deux hôtes et gère l'échange des données. En plus de la régulation de la session, la couche session assure également le transfert efficace des données et la classe de service, ainsi que la signalisation des écarts de la couche session, de la couche de présentation et de la couche application. Pour vous souvenir facilement des fonctions de la couche 5, pensez aux dialogues et aux conversations.

Couche 4 : La couche de transport 4

La couche de transport segmente les données envoyées par l'hôte émetteur et les rassemble en flot de données à l'hôte récepteur. La frontière entre la couche session et la couche de transport peut être vue comme la frontière entre les protocoles de couche média et les protocoles de couche hôte. Alors que les couches application, de présentation et de transport se rapportent aux applications, les trois couches qui les suivent se rapportent au transport des données.

La couche de transport tente de fournir un service de transport des données qui protège les couches supérieures des détails d'implantation du transport. Plus particulièrement, les questions comme la façon d'assurer la fiabilité du transport entre deux systèmes hôtes relèvent de la couche de transport. En fournissant un service de communication, la couche de transport établit et raccorde les circuits virtuels, en plus d'en assurer la maintenance. En fournissant un service fiable, elle fait appel à des contrôles de détection des erreurs de transport, de reprise sur incident et de flux d'information. Pour vous souvenir facilement des fonctions de la couche 4, pensez à la qualité de service et à la fiabilité.

Couche 3 : La couche réseau 3

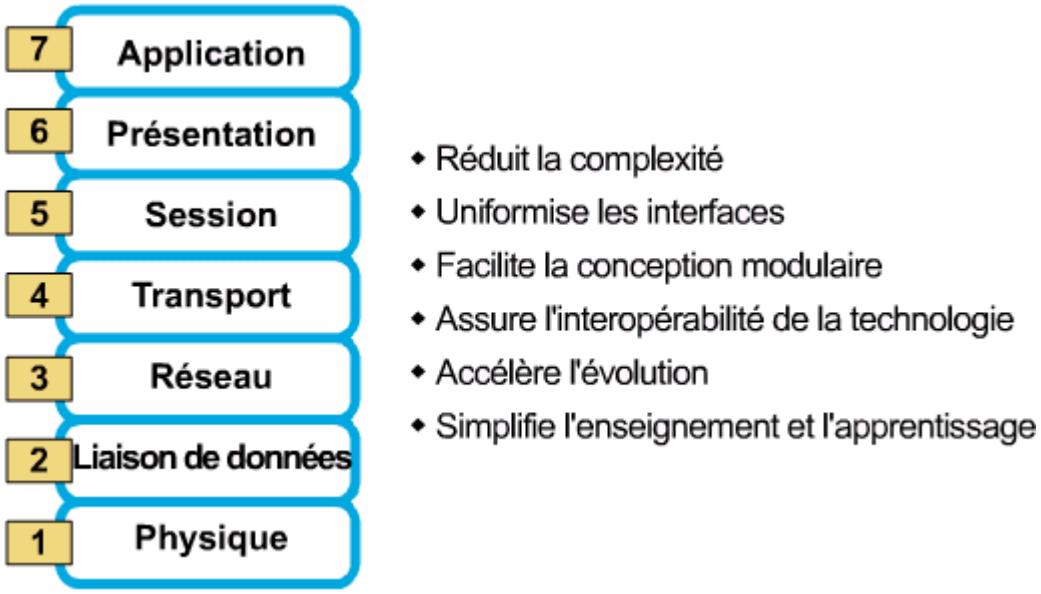
La couche réseau est une couche complexe qui assure la connectivité et la sélection du trajet entre deux systèmes hôte pouvant être situés sur des réseaux géographiquement éloignés. Pour vous souvenir facilement des fonctions de la couche 3, pensez à la sélection de trajet, au routage et à l'adressage.

Couche 2 : La couche liaison de données 2

La couche liaison de données assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (plutôt que logique), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux. Pour vous souvenir facilement des fonctions de la couche 2, pensez aux trames et aux adresses MAC.

Couche 1 : La couche physique : 1

La couche physique définit les spécifications électriques, mécaniques, procédurales et fonctionnelles pour activer, maintenir et désactiver la liaison physique entre les systèmes d'extrémité. Les caractéristiques comme les niveaux de tension, la synchronisation des changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et autres attributs semblables sont définies par la couche physique. Pour vous souvenir facilement des fonctions de la couche 1, pensez aux signaux et aux médias.



2.2.3 Encapsulation

Vous savez que toutes les communications dans un réseau partent d'une source, qu'elles sont acheminées à une destination et que l'information envoyée dans le réseau est appelée données ou paquets de données. Si un ordinateur (hôte A) veut envoyer des données à un autre ordinateur (hôte B), les données doivent d'abord être préparées grâce à un processus appelé encapsulation.

Ce processus conditionne les données en leur ajoutant l'information relative au protocole qui est nécessaire, avant que les données soient transmises sur le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes, des informations de fin et d'autres informations. (Remarque : Le terme "en-tête" fait référence à l'information d'adresse.)

Pour comprendre comment se produit l'encapsulation, examinons la manière dont les données traversent les couches, comme l'illustre la figure. Les données qui sont envoyées par l'ordinateur source (voir la figure) traverse la couche application et les autres couches. Comme vous pouvez le constater, la présentation et le flux des données échangées subissent des changements au fur et à mesure que les réseaux fournissent leurs services aux utilisateurs. Comme l'illustrent les figures, les réseaux doivent effectuer les cinq étapes de conversion ci-dessous afin d'encapsuler les données :

1. **Construction des données.**

   Lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques qu'il contient sont convertis en données pouvant circuler dans l'inter réseau.

2. **Préparation des données pour le transport de bout en bout.**

   Les données sont préparées pour le transport interréseau. En utilisant des segments, la fonction de transport s'assure que les systèmes hôtes à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.

3. **Ajout de l'adresse réseau à l'en-tête.**

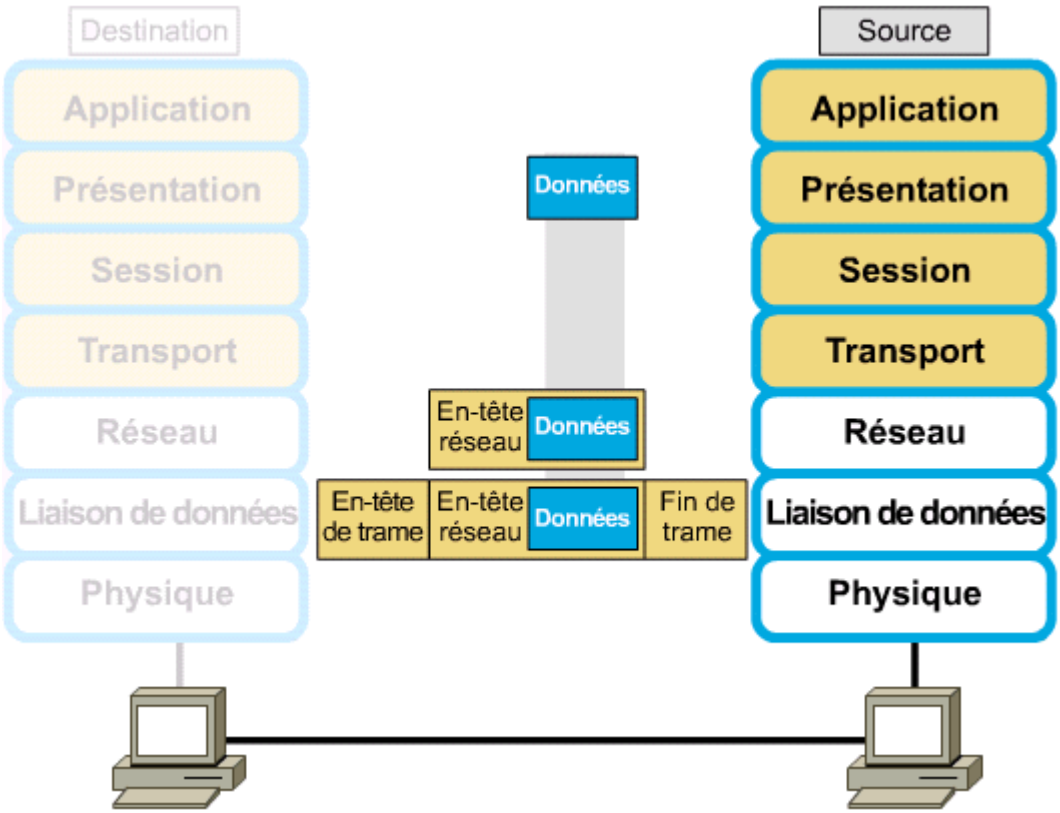
   Les données sont organisées en paquet, ou datagramme, contenant un en-tête réseau constitué des adresses logiques source et de destination. Ces adresses aident les unités réseau à acheminer les paquets dans le réseau suivant un chemin déterminé.

4. **Ajout de l'adresse locale à l'en-tête de liaison de données.**

   Chaque unité réseau doit placer le paquet dans une trame. La trame permet d'établir la connexion avec la prochaine unité réseau directement connectée de la liaison. Chaque unité se trouvant sur le chemin déterminé doit effectuer la mise en trame pour pouvoir se connecter à la prochaine unité.

5. **Conversion en bits pour la transmission.**

   La trame doit être convertie en une série de un et de zéro (bits) pour la transmission sur le média (habituellement un fil). Une fonction de synchronisation permet aux unités de distinguer ces bits lorsqu'ils circulent sur le média. Tout au long du trajet suivi dans l'interréseau physique, le média peut varier. Par exemple, le message électronique peut provenir d'un réseau local, traverser le réseau fédérateur d'un parc de bâtiments, sortir par une liaison réseau longue distance pour atteindre sa destination sur un autre réseau local éloigné. Les informations d'en-tête et de fin sont ajoutées au fur et à mesure que les données descendent dans les couches du modèle OSI.



2.2.4 Désignation des données à chaque couche du modèle OSI

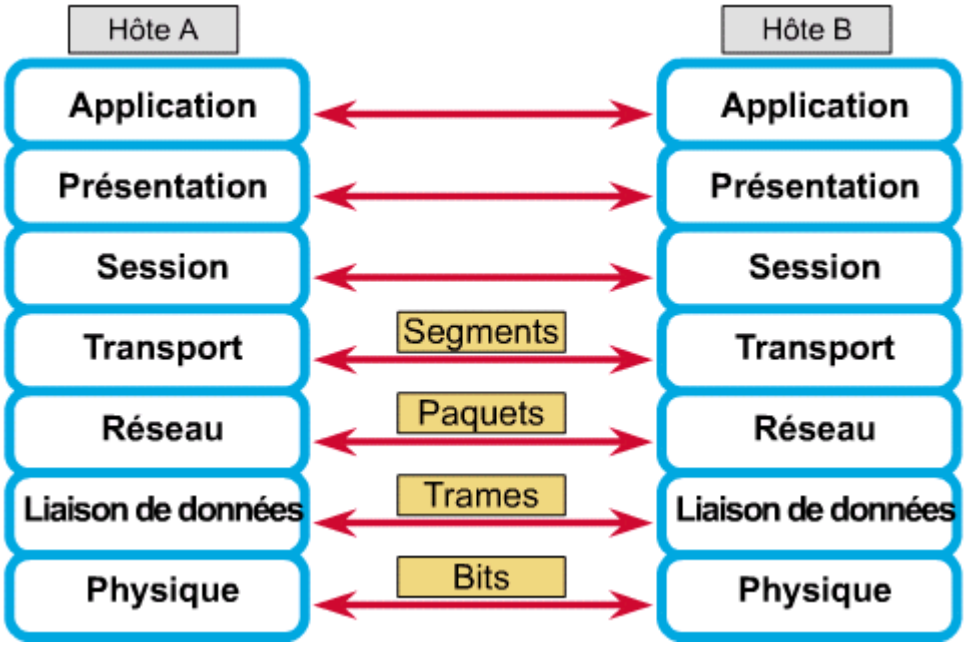
Afin de permettre l'acheminement des paquets de données entre l'ordinateur source et l'ordinateur de destination, chaque couche du modèle OSI sur l'ordinateur source doit communiquer avec sa couche homologue sur l'ordinateur de destination. Cette forme de communication est appelée *communication d'égal à égal*. Au cours de ce processus, le protocole de chaque couche assure l'échange de l'information, appelée *unité de données de protocole* (*ou PDU),* entre les couches homologues. Chaque couche de communication, sur l'ordinateur source, communique avec l'unité de données de protocole propre à une couche, ainsi qu'avec la couche correspondante sur l'ordinateur de destination, comme l'illustre la figure. [1]

Dans un réseau, les paquets de données proviennent d'une source et s'acheminent vers une destination. Chaque couche dépend de la fonction de service de la couche OSI sous elle. Pour fournir ce service, la couche inférieure a recours à l'encapsulation pour placer l'unité de données de protocole de la couche supérieure dans son champ de données, puis elle ajoute l'information d'en-tête et de fin dont elle a besoin pour remplir ses fonctions. Ensuite, au fur et à mesure que les données traversent les couches du modèle OSI, d'autres informations d'en-tête et de fin sont ajoutées. Une fois que les couches 7, 6 et 5 ont ajouté leurs informations, la couche 4 en ajoute d'autres. Ce regroupement des données, soit l'unité de données de protocole de couche 4, est appelé un *segment*. [2]

La couche réseau, par exemple, fournit un service à la couche de transport, qui présente les données au sous-système de l'interréseau. La couche réseau est chargée de déplacer les données dans l'interréseau. Pour ce faire, elle encapsule les données et leur joint un en-tête de manière à créer un paquet (soit la PDU de couche 3). L'en-tête contient l'information requise pour effectuer le transfert, notamment les adresses logiques de source et de destination.

La couche liaison de données fournit un service à la couche réseau. Elle encapsule l'information de couche réseau dans une *trame* (l'unité de données de protocole de couche 2); l'en-tête de trame contient l'information (les adresses physiques, par exemple) nécessaire à l'exécution des fonctions de liaison de données. La couche liaison de données fournit donc un service à la couche réseau en encapsulant l'information de couche réseau dans une trame.

La couche physique fournit un service à la couche liaison de données. Elle code la trame de liaison de données en une série de un et de zéro (bits) en vue de la transmission sur un média (habituellement un fil) à la couche 1.



Chapitre 3

Couche 2 - Notions

Plan :

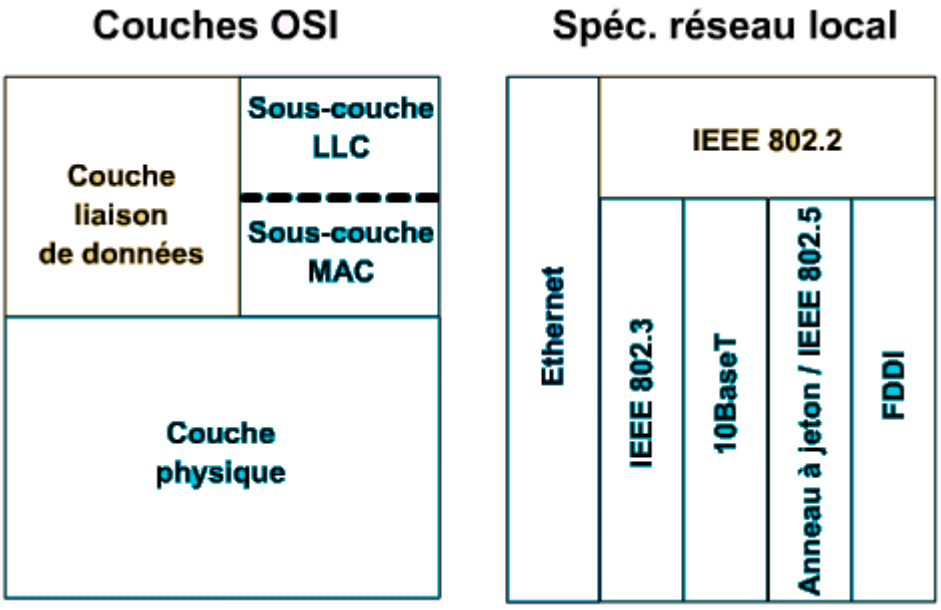
Chapitre Aperçu

Toutes les données transmises sur un réseau proviennent d'une source et se dirigent vers une destination. Une fois que les données ont été transmises, la couche liaison de données du modèle OSI fournit l'accès au média réseau et assure la transmission physique sur le média. Les données peuvent ainsi trouver leur destination sur le réseau. Cette couche se charge également de la notification des erreurs, de la topologie réseau et du contrôle de flux.

1.1 Couche 2

La couche 2 a une solution pour chaque limite de la couche 1. Par exemple, la couche 1 ne peut pas communiquer avec les couches supérieures; or la couche 2 le peut, grâce à la *méthode de contrôle de liaison logique* (*LLC - Logical Link Control*). La couche 1 ne peut pas nommer ni identifier les ordinateurs; la couche 2 y parvient en utilisant un processus *d'adressage* (ou d'attribution de noms). La couche 1 peut uniquement décrire les trains binaires; la couche 2 a recours à la *mise en trame* pour organiser ou regrouper les bits. Dans un groupe d'ordinateurs qui tentent d'envoyer des données en même temps, la couche 1 ne peut pas déterminer celui qui transmettra des données binaires. La couche 2 fait appel à un système appelé *Media Access Control* (ou *MAC*).

1.2 Comparaison des couches 1 et 2 du modèle OSI et de diverses normes de réseau local



L'Institute of Electrical and Electronic Engineers (IEEE) est une organisation professionnelle qui définit les normes touchant les réseaux. Les normes de l'IEEE (dont IEEE 802.3 et IEEE 802.5) sont actuellement les normes prédominantes et les plus connues dans le monde en matière de réseau local. La norme IEEE 802.3 définit la couche physique, ou couche 1, et la portion d'accès au canal de la couche liaison de données, ou couche 2.
Le modèle OSI comporte sept couches. Les normes de l'IEEE ne concernent que les deux couches inférieures. Par conséquent, la couche liaison de données se divise en deux parties :

- la norme LLC 802.2, non tributaire de la technologie
- et des éléments tributaires de la technologie, qui intègrent la connectivité de la couche 1.

L'*IEEE* divise la couche liaison OSI en deux sous-couches distinctes. Elle reconnaît les sous-couches suivantes :

- Media Access Control (MAC) (transitions vers le bas jusqu'au média)
- Logical Link Control (LLC) (transitions vers le haut jusqu'à la couche réseau)

1.3 La méthode de contrôle de liaison logique LLC

L'IEEE a créé la sous-couche LLC afin de permettre à une partie de la couche liaison de données de fonctionner indépendamment des technologies existantes. Cette couche assure la polyvalence des services fournis aux protocoles de couche réseau situés au-dessus d'elle tout en communiquant efficacement avec les technologies variées se trouvant sous elle. En tant que sous-couche, LLC participe au processus d'encapsulation.
La sous-couche LLC de la couche liaison de données gère les communications entre les dispositifs sur une liaison particulière d'un réseau. Cette sous-couche est définie dans la norme IEEE 802.2 et autorise tant les services sans connexion que les services orientés connexion qui sont utilisés par les protocoles de couche supérieure. La norme IEEE 802.2 définit un certain nombre de champs dans les trames de couche liaison de données, qui permettent à plusieurs protocoles de couche supérieure de partager une liaison de données physique.

La couche 2 comporte quatre notions essentielles :

1. La couche 2 communique avec les couches de niveau supérieur à l'aide de la sous-couche LLC.
2. Elle utilise une convention d'attribution de noms non hiérarchique (l'attribution de noms est en fait l'attribution d'identificateurs uniques, c.-à-d. les adresses).
3. Elle fait appel à la mise en trame pour organiser ou regrouper les données.
4. La couche 2 utilise Media Access Control (MAC) pour choisir l'ordinateur qui transmettra les données binaires, parmi un groupe d'ordinateurs qui cherchent tous à transmettre des données en même temps.

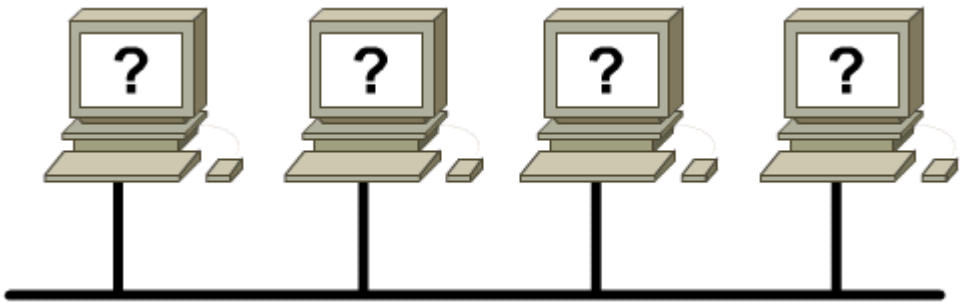
1.4 Sous-couches MAC

La sous-couche MAC concerne les protocoles que doit suivre un ordinateur hôte pour accéder au média physique.

2 L'adressage MAC

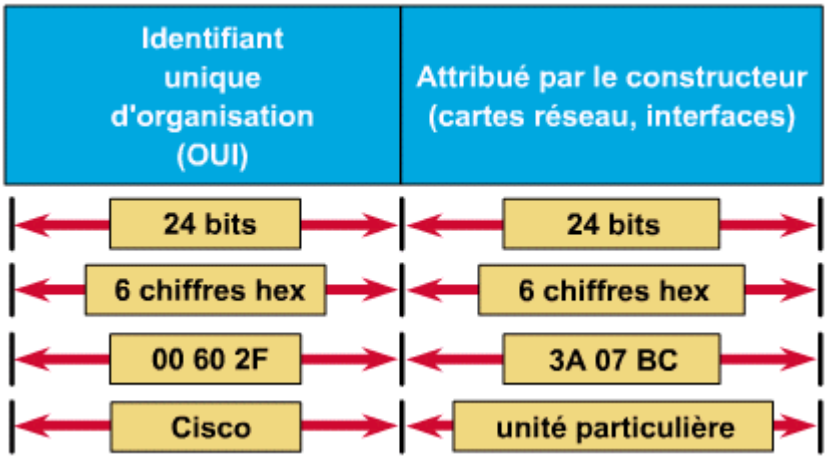
2.1 L'adresse MAC et les cartes réseau

Sans adresses MAC, votre réseau local comporterait un groupe d'ordinateurs sans nom.



Chaque ordinateur a une façon unique de s'identifier. Tout ordinateur, qu'il soit relié à un réseau ou non, comporte une adresse physique. Il n'y a jamais deux adresses physiques identiques. L'adresse physique, appelée adresse MAC, se trouve sur la carte réseau.

Les adresses MAC comportent 48 bits et sont exprimées à l'aide de douze chiffres hexadécimaux. Les six premiers chiffres hexadécimaux, qui sont administrés par l'IEEE, identifient le fabricant ou le fournisseur et constituent donc l'*identifiant unique d'organisation* (*OUI - Organizational Unique Identifier*). Les six autres chiffres hexadécimaux forment le *numéro de série d'interface* ou une autre valeur administrée par le fabricant. On dit parfois des adresses MAC qu'elles sont *rémanentes* (*BIA - burned-in adresses*) parce qu'elles demeurent en mémoire morte et sont copiées en mémoire vive au moment de l'initialisation de la carte réseau.



Avant que la carte réseau quitte l'usine, le fabricant lui attribue une adresse physique unique. Cette adresse est programmée sur une puce de la carte réseau. Comme l'adresse MAC se trouve sur la carte réseau, l'adresse physique de l'ordinateur changera si la carte réseau dont il est doté est remplacée. Il existe deux formats d'adresse MAC : 0000.0c12.3456 ou 00-00-0c-12-34-56.

2.2 Comment la carte réseau utilise les adresses MAC

Les réseaux locaux Ethernet et 802.3 sont des réseaux de diffusion. Toutes les stations voient toutes les trames. Chaque station doit examiner chacune des trames pour déterminer si elle en est la destinataire.
Dans un réseau Ethernet, lorsqu'une unité désire envoyer des données à une autre unité, elle peut ouvrir une voie de communication vers l'autre unité à l'aide de l'adresse MAC de cette dernière. Lorsqu'une unité source envoie des données dans un réseau, ces données transportent l'adresse MAC de leur destination. Pendant que les données se déplacent dans le média réseau, la carte réseau de chaque hôte vérifie si son adresse MAC correspond à l'adresse physique de destination transportée par la trame. En l'absence de correspondance, la carte réseau abandonne la trame. S'il n'y a pas de correspondance, la carte réseau ignore la trame, qui poursuit son chemin jusqu'à la prochaine station.

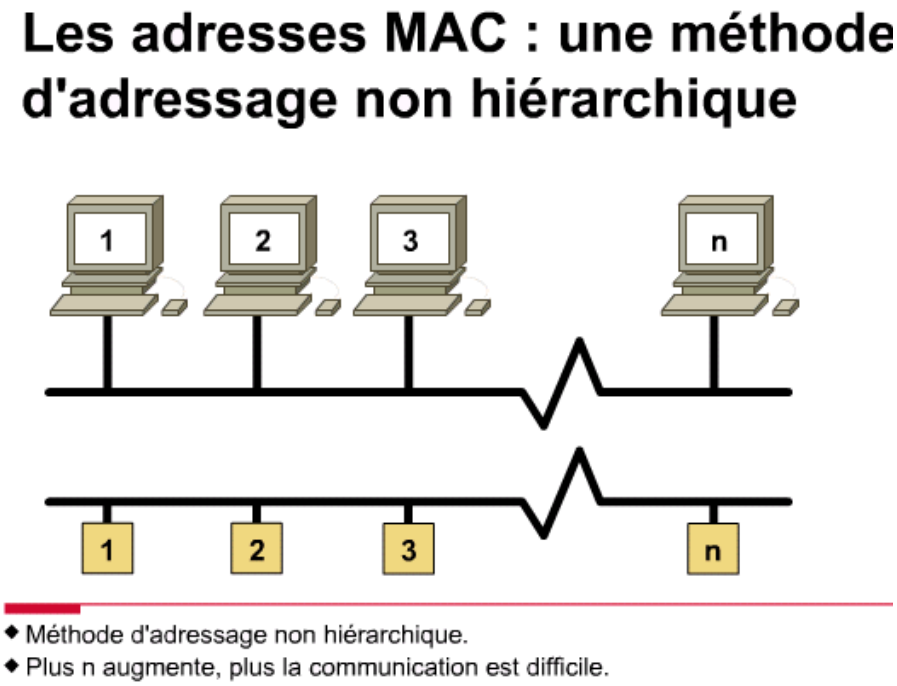
2.3 L'encapsulation et le désencapsulation des adresses de couche 2

Une partie importante des opérations d'encapsulation et de désencapsulation est l'ajout des adresses MAC source et de destination. Sans ces adresses, l'information ne peut pas être envoyée ou acheminée correctement dans un réseau.

2.4 Les limites de l'adressage MAC

Les adresses MAC sont essentielles au fonctionnement d'un réseau informatique. Ces adresses constituent un moyen pour les ordinateurs de s'identifier. Elles attribuent un nom permanent et unique à chaque système hôte. Il n'y a aucun risque d'épuisement des adresses MAC puisqu'il existe 16^12 (ou plus de 2 billions!) adresses MAC possibles.

Les adresses MAC présentent un désavantage important. Elles n'ont aucune structure et sont considérées comme des espaces adresse non hiérarchiques. Des fabricants différents ont des identifiants uniques d'organisation (OUI) différents, mais ceux-ci équivalent à des numéros d'identification personnels. Dès qu'un réseau comporte plusieurs ordinateurs, ce désavantage devient un véritable problème.



3 La mise en trame

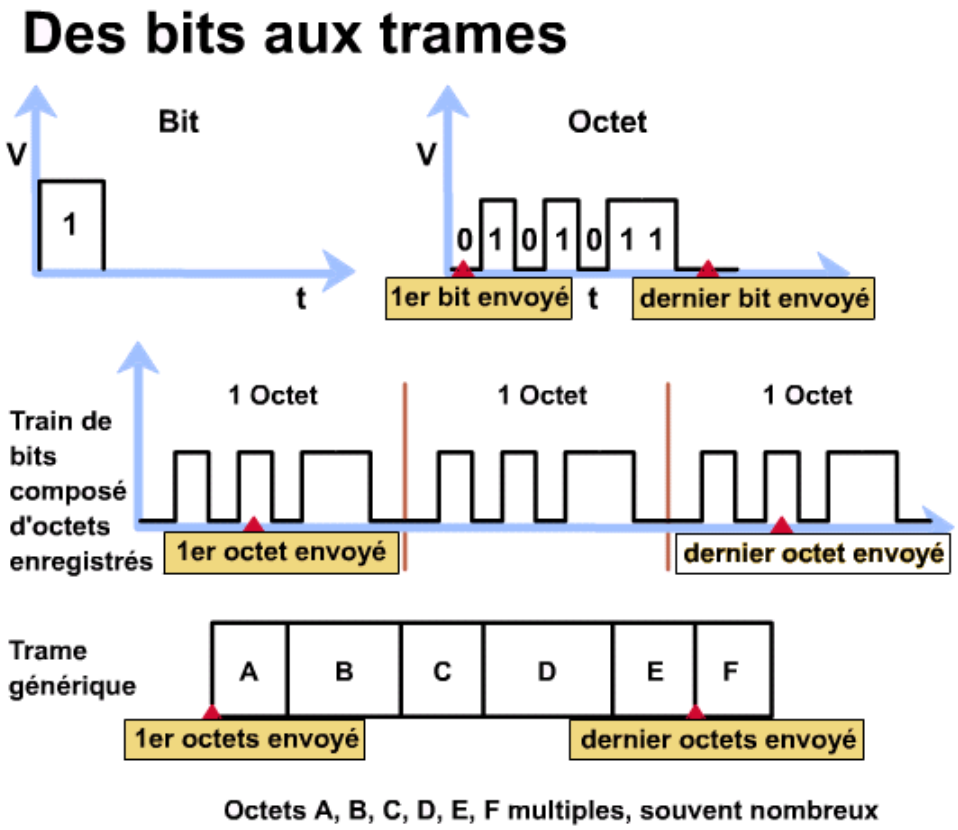
3.1 Pourquoi la mise en trame est-elle nécessaire?

Des trains binaires codés sur un média physique ne suffisent pas à assurer la communication. La mise en trame aide à récupérer de l'information essentielle qu'il n'était pas possible d'obtenir uniquement avec les trains binaires codés. Voici des exemples de ces éléments d'information :

- quel ordinateur communique avec quel autre;
- quand commence la communication entre certains ordinateurs et quand elle se termine;
- quelles erreurs se sont produites pendant la communication;
- à qui le tour de "parler" dans une "conversation" entre ordinateurs.

Après que vous avez décidé de la façon de nommer les ordinateurs, vous pouvez passer à l'étape suivante, soit la mise en trame. La mise en trame est le processus d'encapsulation de couche 2; une trame est l'unité de données de protocole de couche 2.

3.2 Schéma de structure de trame



Octets A, B, C, D, E, F multiples, souvent nombreux

3.3 Un format de trame générique

Il existe plusieurs différents types de trame, décrits par diverses normes. Une trame générique comporte des sections appelées champs et chaque champ est constitué d'octets. Les noms des *champs* sont les suivants :

- champ de début de trame
- champ d'adresse
- champ de longueur / type / contrôle
- champ de données
- champ de séquence de contrôle de trame
- champ de fin de trame

Nom des champs					
A	B	C	D	E	F
Champ début de trame	Champ d'adresse	Champ type / longueur	Champ données	Champ FCS	Champ fin de trame

Structure de trame générique

champ de début de trame
Il doit y avoir une façon pour les ordinateurs connectés à un média physique d'attirer l'attention des autres ordinateurs afin de diffuser le message "Voici une trame!". Même si la méthode utilisée diffère selon la technologie, toutes les trames contiennent une séquence d'octets de signalisation de début.

champ d'adresse
Toutes les trames contiennent de l'information d'identification, comme le nom de l'ordinateur source (adresse MAC) et celui de l'ordinateur de destination (adresse MAC).

champ de longueur / type / contrôle
La plupart des trames contiennent des champs spécialisés. Dans certaines technologies, un champ de longueur indique la longueur exacte de la trame. Certaines trames comportent un champ de type précisant le protocole de couche 3 qui émet la demande d'envoi. Par ailleurs, plusieurs technologies n'utilisent aucun de ces champs.

champ de données
L'envoi de trames a pour but de faire parvenir les données de couche supérieure et en bout de ligne, les données d'application utilisateur, de l'ordinateur source à l'ordinateur de destination. Le paquet de données que vous voulez livrer comporte deux parties. Premièrement, le message que vous voulez envoyer et deuxièmement, les octets encapsulés qui doivent se rendre à l'ordinateur de destination. Ces données doivent être accompagnées d'autres octets. Appelés *octets de remplissage*, il sont parfois ajoutés pour que les trames aient une longueur minimale à des fins de synchronisation. Des octets LLC sont également ajoutés au champ de données dans les trames standard IEEE. N'oubliez pas que la sous-couche LLC ajoute aux données du protocole réseau, soit le paquet IP, de l'information de contrôle qui facilitera la livraison du paquet IP à sa destination. La couche 2 communique avec les couches de niveau supérieur à l'aide de la sous-couche LLC.

champ de séquence de contrôle de trame
Toutes les trames ainsi que les bits, les octets et les champs qu'elles contiennent peuvent comporter des erreurs provenant d'une variété de sources. Vous devez savoir comment les détecter. Une méthode de détection efficace mais non efficiente consiste à envoyer chaque trame deux fois ou à faire retourner par l'ordinateur de destination une copie de la trame initiale à l'ordinateur source avant que celui-ci ne puisse envoyer une autre trame.

Il existe une meilleure façon, plus efficace, qui consiste à éliminer uniquement les trames erronées, puis à retransmettre les trames. Le champ de la séquence de contrôle de trame contient un nombre, calculé par l'ordinateur source, qui est fondé sur les données contenues dans la trame. Lorsque l'ordinateur de destination reçoit la trame, il calcule de nouveau la séquence de contrôle de trame et la compare à celle qui est incluse dans la trame. Si les deux nombres sont différents, il y a une erreur, la trame est abandonnée et l'ordinateur source est invité à transmettre de nouveau.
Il existe trois principales façons de calculer la séquence de contrôle de trame :

- *code de redondance cyclique (CRC)* - exécution de calculs polynomiaux sur les données
- *parité bidimensionnelle* - ajout d'un 8e bit grâce auquel une séquence de huit bits contient un nombre pair ou impair de 1 binaires
- *total de contrôle Internet* - somme résultant de l'addition des valeurs de tous les bits de données.

champ de fin de trame
L'ordinateur qui transmet les données doit attirer l'attention des autres unités afin de commencer une trame, puis doit le faire de nouveau afin de mettre fin à la trame. Le champ de longueur implique la fin de la trame; celle-ci est terminée après la séquence de contrôle de trame (FCS). Il existe parfois une séquence officielle d'octets appelée délimiteur de fin de trame.

5.5 Collisions et domaines de collision dans les environnements à couches partagées

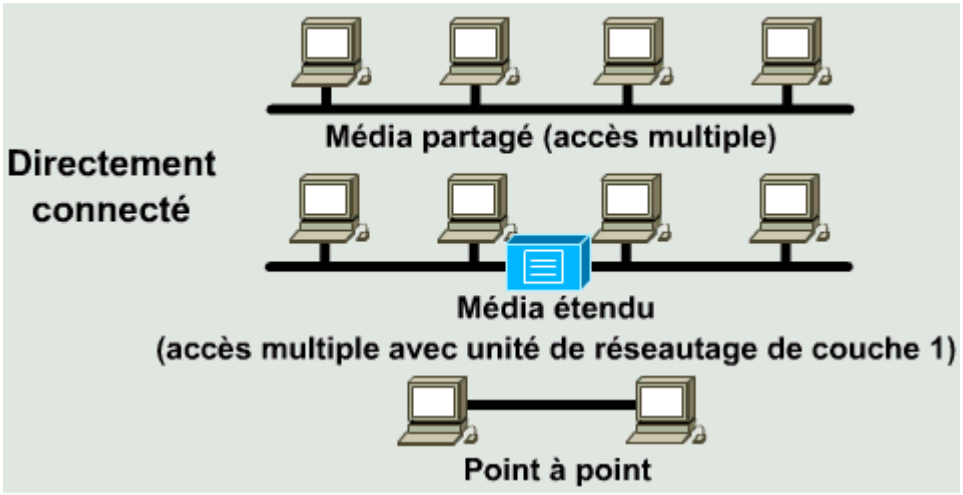
5.5.1 Environnement à média partagé

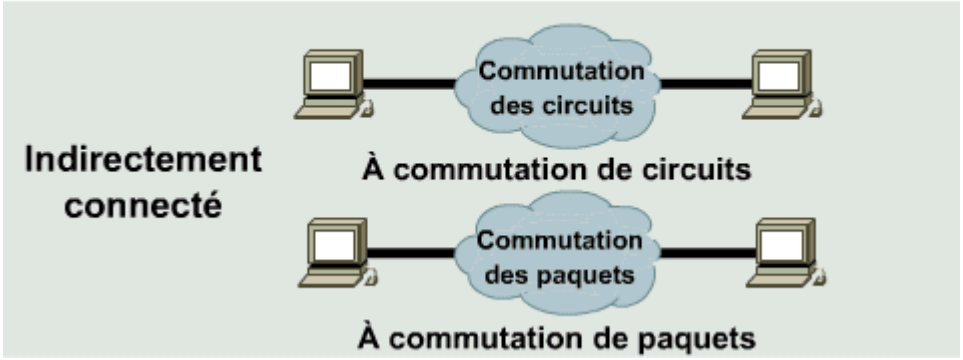
Certains réseaux sont directement connectés; tous les hôtes partagent la couche 1. Par exemple :

- *environnement à média partagé* - dans ce cas, de nombreux hôtes ont accès au même média. Par exemple, si plusieurs PC sont connectés au même fil physique ou au même câble à fibres optiques, ou s'ils partagent le même "espace aérien", ils sont dans un environnement à média partagé. Il se peut que vous entendiez l'expression "tous les ordinateurs sont sur le même fil". Cela signifie qu'ils partagent tous le même média, même si le "fil" peut être un câble à paires torsadées non blindées de catégorie 5 qui compte quatre paires de fils.
- *environnement à média partagé étendu* - type spécial d'environnement à média partagé dans lequel les unités réseau peuvent étendre l'environnement de manière à supporter les accès multiples ou un plus grand nombre d'utilisateurs. Cela présente toutefois quelques inconvénients, malgré les avantages.
- *environnement réseau point à point* - le plus utilisé pour les réseaux longue distance et celui que vous connaissez sans doute le mieux. Dans ce type d'environnement de réseau, une unité est connectée à une seule autre unité par l'intermédiaire d'une liaison.

Certains réseaux sont indirectement connectés, en ce sens que des unités réseau de couche supérieure se situent entre les hôtes en communication ou que ces hôtes sont éloignés. Il en existe deux types :

- *réseau à commutation de circuits* - réseau indirectement connecté au sein duquel de véritables circuits électriques sont établis pour la durée de la communication. Le système téléphonique actuel est encore partiellement commuté, bien que dans la plupart des pays les systèmes téléphoniques reposent de moins en moins sur les technologies de commutation de circuits.
- *réseau à commutation de paquets* - plutôt que d'attribuer une liaison pour la connexion exclusive de deux hôtes en communication, la source envoie des messages par paquets. Chaque paquet contient suffisamment d'information pour être routé à l'hôte de destination approprié. De nombreuses unités hôtes peuvent ainsi partager la même liaison, mais cela peut donner lieu à de la contention.



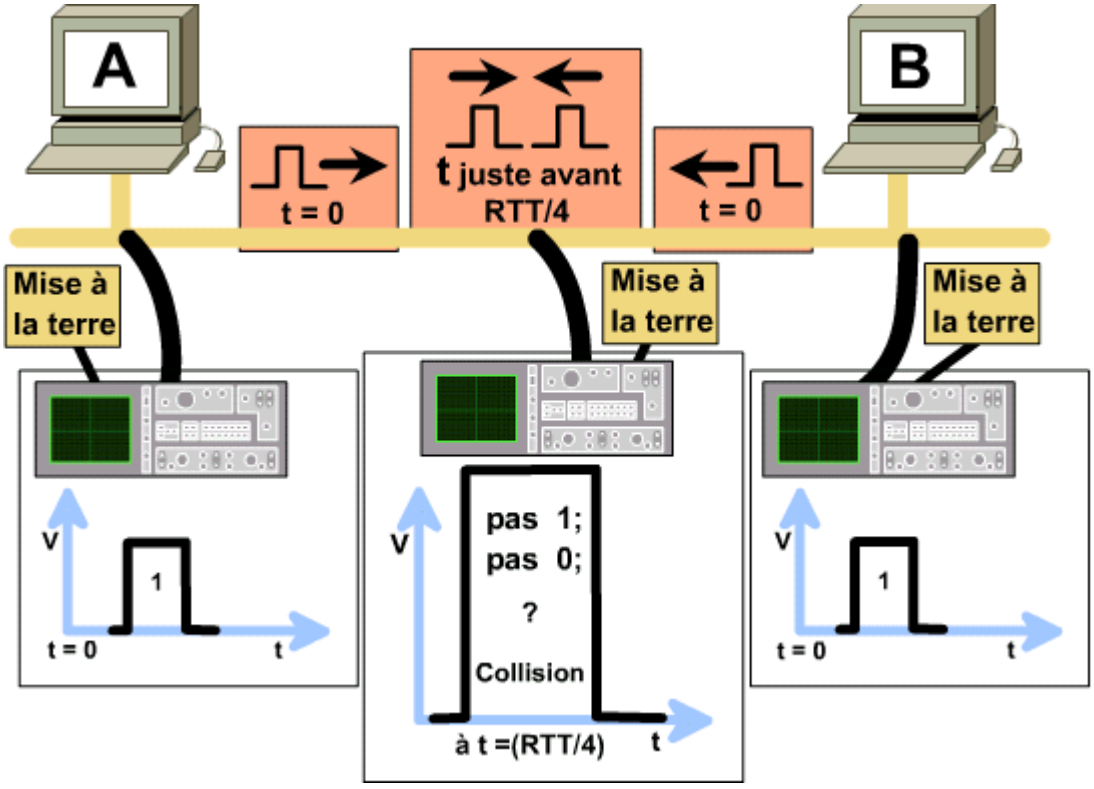


5.5.2 Collisions et domaines de collision

L'un des problèmes pouvant se produire lorsque deux bits voyagent en même temps dans le même réseau est une *collision*. Un réseau restreint et lent pourrait utiliser un système selon lequel deux ordinateurs seulement enverraient des messages, et ce, à tour de rôle. Ainsi, les deux hôtes pourraient envoyer des messages, mais un seul bit circulerait à la fois dans le système. Le problème est que de nombreux ordinateurs sont connectés à de vastes réseaux et que chacun d'eux cherche à communiquer des milliards de bits chaque seconde. Il importe de garder à l'esprit que les "bits" sont en fait des paquets contenant plusieurs bits.

De graves problèmes peuvent survenir lorsque le trafic devient trop élevé dans un réseau. Si un seul câble interconnecte toutes les unités d'un réseau ou si des segments d'un réseau sont connectés uniquement par des dispositifs sans filtrage, comme les répéteurs, la possibilité que plus d'un utilisateur essaie d'envoyer des données dans le réseau en même temps est très élevée. Ethernet ne permet qu'à un seul paquet de données d'accéder au câble à un moment donné. Si plusieurs nœuds tentent de transmettre en même temps, il se produit une collision et les données de chaque nœud sont endommagées.

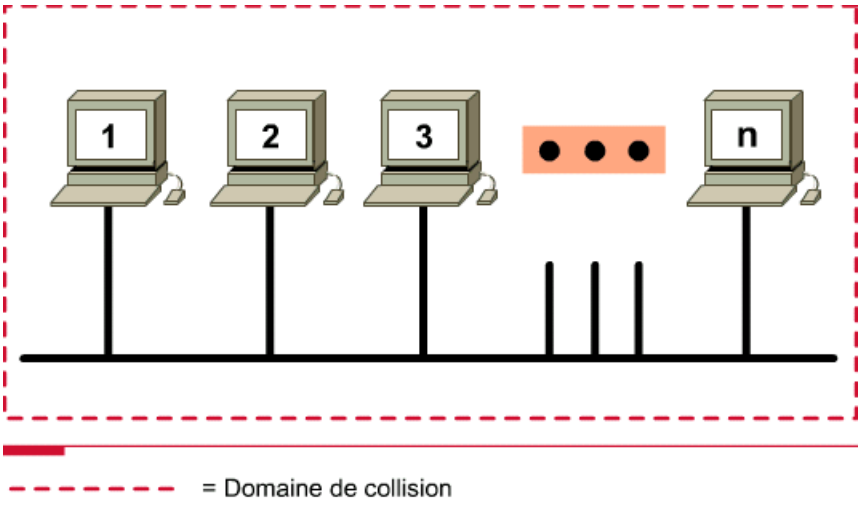
La portion du réseau d'où proviennent les paquets de données et où la collision s'est produite est appelée *domaine de collision* et comprend tous les environnements à média partagé. Un "fil" peut être relié à un autre par l'intermédiaire de câbles de raccordement, d'émetteurs-récepteurs, de tableaux de connexions, de répéteurs et même de concentrateurs. Toutes ces interconnexions de couche 1 font partie du domaine de collision.



Lors d'une collision, les paquets de données touchés sont détruits, bit par bit. Pour éviter ce problème, le réseau doit disposer d'un système pour gérer l'accès au média (*contention*). Par exemple, un système numérique ne peut reconnaître que deux états, représentés par des tensions, des signaux lumineux ou des ondes électromagnétiques. Par conséquent, lors d'une collision, les signaux s'entrechoquent et se brouillent. Tout comme deux voitures ne peuvent pas occuper le même espace sur la route en même temps, deux signaux ne peuvent pas circuler sur le même média en même temps.

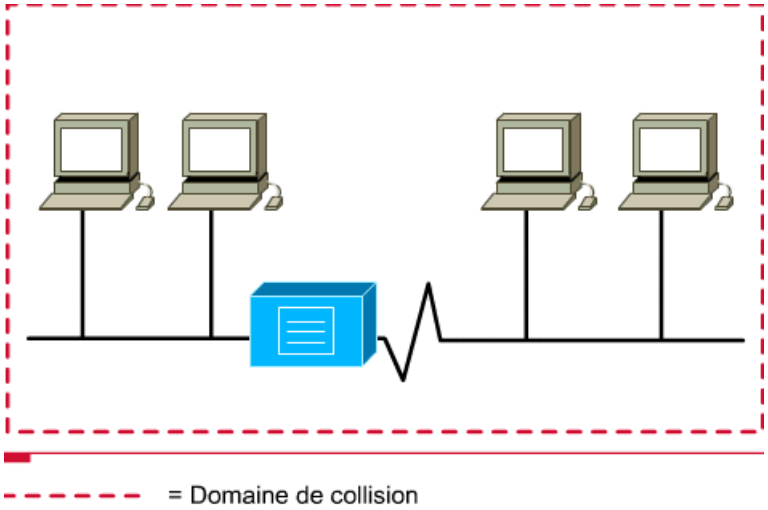
5.5.4 Accès partagé comme domaine de collision

Si vous connectez n ordinateurs à un seul média sans aucune autre unité de réseautage, vous créez une situation d'accès partagé de base et vous avez là un domaine de collision. Selon la technologie utilisée, cela limite le nombre d'ordinateurs pouvant utiliser cette portion du média, aussi appelée un segment.



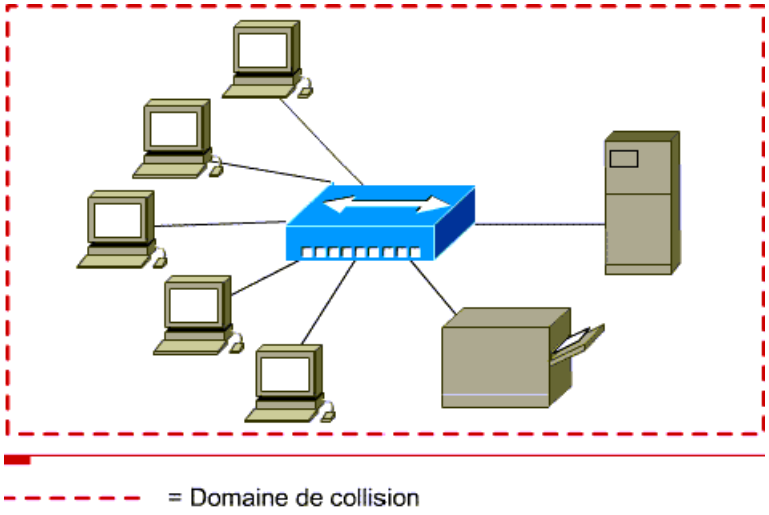
5.5.5 Répéteurs et domaines de collision

Les répéteurs régénèrent et resynchronisent les signaux, mais ils ne peuvent pas filtrer le flux de trafic qui passe par eux. Les données (bits) qui arrivent à un port d'un répéteur sont envoyées par tous les autres ports. L'utilisation d'un répéteur étend le domaine de collision, par conséquent, le réseau qui s'étend des deux côtés du répéteur est un domaine de collision encore plus grand.



5.5.6 Concentrateurs et domaines de collision

Vous savez déjà qu'un concentrateur est aussi appelé répéteur multiport. Tout signal entrant par un port du concentrateur est régénéré, resynchronisé, puis envoyé par tous les autres ports. Par conséquent, les concentrateurs, par ailleurs fort utiles pour connecter un grand nombre d'ordinateurs, contribuent aussi à étendre les domaines de collision. Il en résulte des performances réduites si tous les ordinateurs du réseau demandent simultanément une grande largeur de bande.



5.5.7 La règle des 4 répéteurs

La règle des 4 répéteurs dans Ethernet stipule que le nombre maximal de répéteurs ou de concentrateurs entre deux ordinateurs du réseau est quatre. Chaque répéteur ajoute du temps de latence ou ralentit les bits pendant la régénération du signal. L'utilisation de plus de quatre répéteurs peut faire dépasser le délai maximal. Lorsque le délai est dépassé, le nombre de *collisions tardives* augmente considérablement. Une *collision tardive* est une collision qui se produit après la transmission des 64 premiers octets de la trame. Les jeux de circuits des cartes réseau ne transmettent pas de nouveau automatiquement lorsqu'une collision tardive se produit. Les trames de collisions tardives ajoutent un délai appelé *délai de consommation*. À mesure que le délai de consommation et la latence augmentent, la performance réseau se détériore. Cette règle d'or Ethernet est aussi appelée règle 5-4-3-2-1. Cinq sections du réseau, quatre répéteurs ou concentrateurs, trois sections du réseau sont des segments de "mixage" (avec des hôtes), deux sections sont des segments de liaison (sans hôtes) et un grand domaine de collision.

Ethernet et IEEE 802.3

1. Comparaison entre Ethernet et IEEE 802.3

Ethernet est la technologie de réseau local la plus répandue. Le réseau Ethernet a été conçu pour palier au manque entre les réseaux longue distance lents et les réseaux informatiques spécialisés acheminant des données à haut débit sur des distances très limitées. La technologie Ethernet convient particulièrement aux applications dans lesquelles un média de transmission local doit acheminer de façon sporadique et occasionnelle un important trafic à des débits de crête élevés.

L'architecture de réseau Ethernet a été conçue dans les années 1960 à l'université d'Hawaii, où l'on a développé la méthode d'accès qu'utilise l'Ethernet aujourd'hui, soit la détection de porteuse avec accès multiple et détection de collisions (CSMA/CD). Le Palo Alto Research Center (PARC) de Xerox Corporation' a développé le réseau Ethernet dans les années 1970. Cela a été utilisé comme fondement pour l'élaboration de la norme 802.3 de l'Institute of Electrical and Electronic Engineers (IEEE), publiée en 1980.

Peu après, Digital Equipment Corporation, Intel Corporation et Xerox Corporation ont conjointement élaboré et publié une spécification Ethernet, la version 2.0, qui est en grande partie compatible avec la norme IEEE 802.3. Conjointement, les réseaux Ethernet et IEEE 802.3 possèdent actuellement une plus grande part du marché que tout autre protocole de réseau local. Aujourd'hui, le terme Ethernet est souvent utilisé pour faire référence à tous les réseaux locaux à détection de porteuse avec accès multiple et détection de collisions (CSMA/CD)' qui sont généralement conformes aux spécifications Ethernet, y compris la norme IEEE 802.3.

Les normes Ethernet et IEEE 802.3 précisent des technologies semblables; les deux décrivent des réseaux à accès CSMA/CD. Les stations d'un réseau local à accès CSMA/CD peuvent accéder au réseau en tout temps. Avant de transmettre des données, les stations d'un réseau à accès CSMA/CD écoutent le réseau afin de déterminer s'il est déjà en utilisation. Le cas échéant, elles attendent. Si le réseau n'est pas en utilisation, la station transmet les données. Une collision se produit lorsque deux stations écoutent le trafic du réseau, n'entendent rien et émettent toutes les deux simultanément. Dans un tel cas, les deux transmissions sont endommagées et les stations doivent retransmettre plus tard. Des algorithmes de réémission temporisée déterminent à quel moment les stations en collision peuvent retransmettre. Les stations à accès CSMA/CD peuvent détecter les collisions, ainsi elles savent à quel moment elles doivent retransmettre.

Les réseaux locaux Ethernet et IEEE 802.3 sont des réseaux de diffusion. Cela signifie que chaque station peut voir toutes les trames, peu importe qu'elle soit ou non la destination prévue de ces données. Chaque station doit examiner les trames reçues afin de déterminer si elles correspondent à la destination des données. Le cas échéant, la trame est passée à un protocole de couche supérieure à l'intérieur de la station afin de recevoir le bon traitement.

Les différences qui existent entre les réseaux Ethernet et IEEE 802.3 sont subtiles. L'Ethernet offre des services correspondant aux couches 1 et 2 du modèle de référence OSI et la norme IEEE 802.3 définit la couche physique, la couche 1, et la portion d'accès au réseau de la couche liaison de données, la couche 2, mais ne précise pas de protocole de contrôle de liaison logique. Les spécifications de réseau local Ethernet et IEEE 802.3 sont mises en œuvre par du matériel informatique. Habituellement, la partie physique de ces protocoles est une carte d'interface située dans un ordinateur hôte ou un circuit sur une carte de circuits primaire située à l'intérieur d'un ordinateur hôte.

2. La famille Ethernet

Il existe au moins 18 types d'Ethernet, qui ont été précisés ou qui sont à être précisés. Le tableau de l'illustration principale indique certaines des technologies Ethernet les plus courantes et les plus importantes.

paramètres	médium de transmission	technique de signalistation	vitesse de transmission	longueur max du segment	couverture maximale du réseau	nbr max de nœuds par segment	espacement min entre les nœuds	diamètre du câble
10 base 5	Coaxial (50 ohms)	Manchester	10 Mbit/s	500 m	2500 m	100	2,5 m	10 mm
10 base 2	Coaxial (50 ohms)	Manchester	10 Mbit/s	185 m	925 m	30	0,5 m	5 mm
1 base 5	Paire non blindée	Manchester	1 Mbit/s	500 m	2500 m	*	*	0.4-0.6 nnn
10 broad 18	Coaxial (75 ohms)	DPSK	10 Mbit/s	1800 m	3600 m	*	*	*
10 base T	Paire téléphonique	Manchester	10 Mbit/s	100 m (étoile)	500 m	dépend de l'équipement actif	*	*
10 base FL	Fibre optique multimode	*	10 Mbit/s	2000 m	*	*	*	*
100 base TX	UTP cat5	Manchester	100 Mbit/s	100	500 m	dépend de l'équipement actif	*	*
100 base FX	Fibre optique multimode	*	100 Mbit/s	2000 m	*	*	*	
1000 base CX	UTP cat5	Manchester	1000 Mbit/s	100 m	*	*	*	

3. Configuration de trame Ethernet

Les champs de trame des réseaux Ethernet et IEEE 802.3 sont décrits dans les courtes définitions suivantes :

- *préambule* - Configuration composée de 1 et de 0 en alternance qui indique aux stations réceptrices qu'il s'agit d'une trame Ethernet ou IEEE 802.3. La trame Ethernet comporte un octet supplémentaire qui équivaut au champ de début de trame précisé dans la trame IEEE 820.3.

- *début de trame* - Caractère séparateur du réseau IEEE 802.3 se terminant par deux bits 1 consécutifs, qui servent à synchroniser les portions réception des trames de toutes les stations du réseau local. Le début de trame est explicitement précisé dans la norme Ethernet.

- *adresses source et de destination* - Les trois premiers octets des adresses sont précisés par l'IEEE en fonction du fabricant. Les trois derniers octets sont précisés par le fabricant de la carte réseau Ethernet ou IEEE 802.3. L'adresse source est toujours une adresse monodestinataire (nœud simple). L'adresse de destination peut être une adresse monodestinataire, une adresse multipoint (groupe) ou une adresse de diffusion (tous les nœuds).

- *type (Ethernet)* - Précise le protocole de couche supérieure qui reçoit les données une fois que le traitement Ethernet est terminé.

- *longueur (IEEE 802.3)* - Indique le nombre d'octets de données qui suit ce champ.

- *données (Ethernet)* - Une fois le traitement de couche physique et de couche liaison terminé, les données contenues dans la trame sont transmises à un protocole de couche supérieure qui est précisé dans le champ type;. Bien que la version 2 d'Ethernet ne précise pas d'élément de remplissage, contrairement à l'IEEE 802.3, l'Ethernet doit recevoir au moins 46 octets de données.

- *données (IEEE 802.3)* - Une fois le traitement de couche physique et de couche liaison terminé, les données sont transmises à un protocole de couche supérieure, qui doit être précisé dans la portion données de la trame. Si les données contenues dans la trame sont insuffisantes pour occuper les 64 octets qui représentent la taille minimale de la trame, des octets de remplissage sont insérés afin que la trame contienne au moins 64 octets.

- *séquence de contrôle de trame* -Séquence contenant un code de redondance cyclique (CRC) de 4 octets, qui est créée par le dispositif émetteur et recalculée par le dispositif récepteur afin de s'assurer qu'aucune trame n'a été endommagée.

?	1	6	6	2	46-1500	4
Préambule	Délimiteur de début de trame	Adresse destination	Adresse source	Type	Données	Séquence de contrôle de trame

Trame Ethernet

?	1	6	6	2	46-1500	4
Préambule	Délimiteur de début de trame	Adresse destination	Adresse source	Longueur	en-tête 802.2 et données	Séquence de contrôle de trame

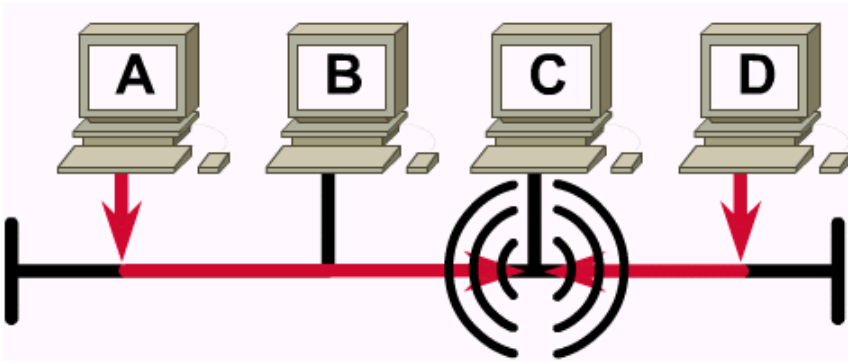
Trame IEEE 802.3

4. MAC Ethernet

Ethernet est une technologie de diffusion à média partagé. La méthode d'accès CSMA/CD utilisée par le réseau Ethernet assure les trois fonctions suivantes :

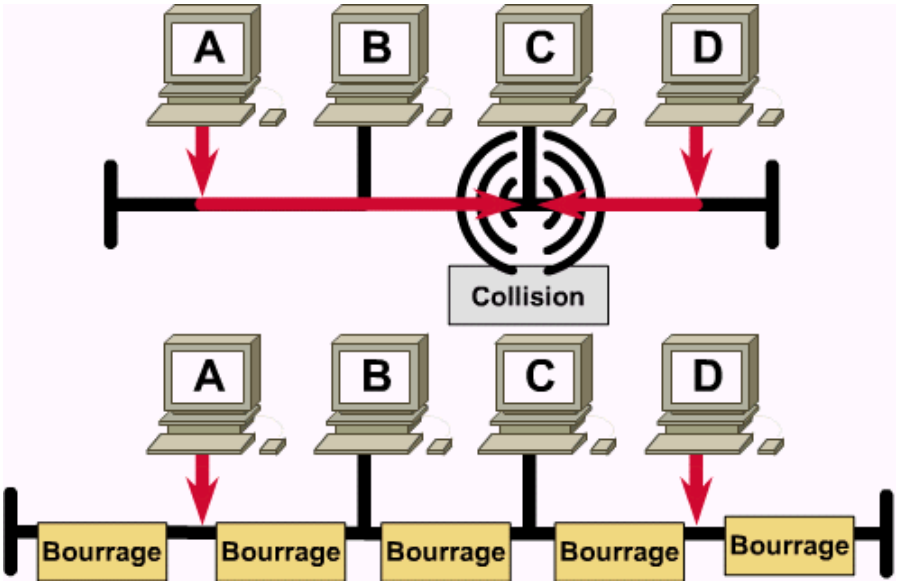
1. transmission et réception de paquets de données
2. décodage des paquets de données et vérification de ces paquets afin de s'assurer qu'ils ont une adresse valide avant de les passer aux couches supérieures du modèle OSI.
3. détection d'erreurs à l'intérieur des paquets de données ou sur le réseau.

Dans la méthode d'accès CSMA/CD, les dispositifs de réseautage qui ont des données à transmettre sur le média de réseautage, ne transmettent les données qu'après écoute de porteuse. Cela signifie que lorsqu'un dispositif désire transmettre des données, il doit d'abord s'assurer que le média de réseautage est libre. Le dispositif doit vérifier s'il y a présence de signaux sur le média de réseautage. Une fois que le dispositif a déterminé que le média est libre, il commence la transmission de ses données. Tout en transmettant ses données sous formes de signaux, le dispositif écoute. Il fait cela pour s'assurer qu'aucune autre station ne transmet de données au média de réseautage en même temps. Une fois la transmission de données terminée, le dispositif se remet en mode d'écoute.
Les dispositifs de réseautage ont la capacité de détecter une collision, car dans un tel cas, l'amplitude du signal augmente sur le média de réseautage.



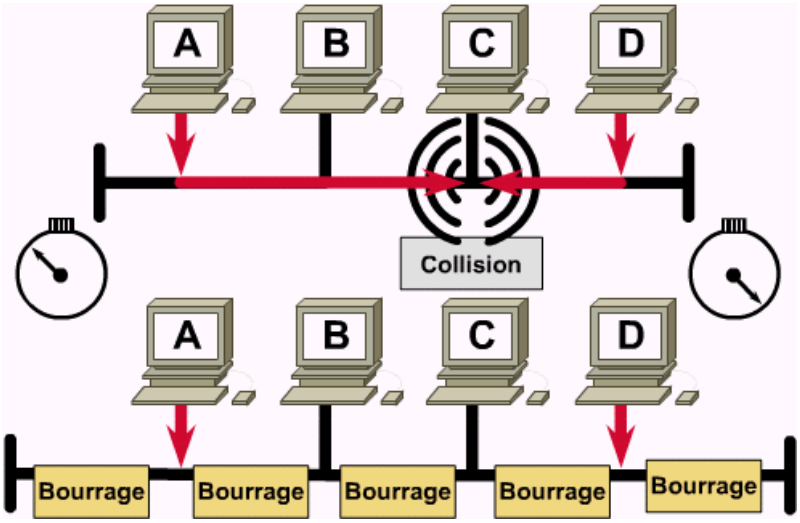
Collision

Lorsqu'une collision se produit, chaque dispositif transmetteur continue de transmettre des données pendant une courte période. Cela afin de veiller à ce que tous les dispositifs voient la collision. Une fois que tous les dispositif d'un réseau ont vu qu'une collision s'est produite, chaque dispositif fait appel à un algorithme.



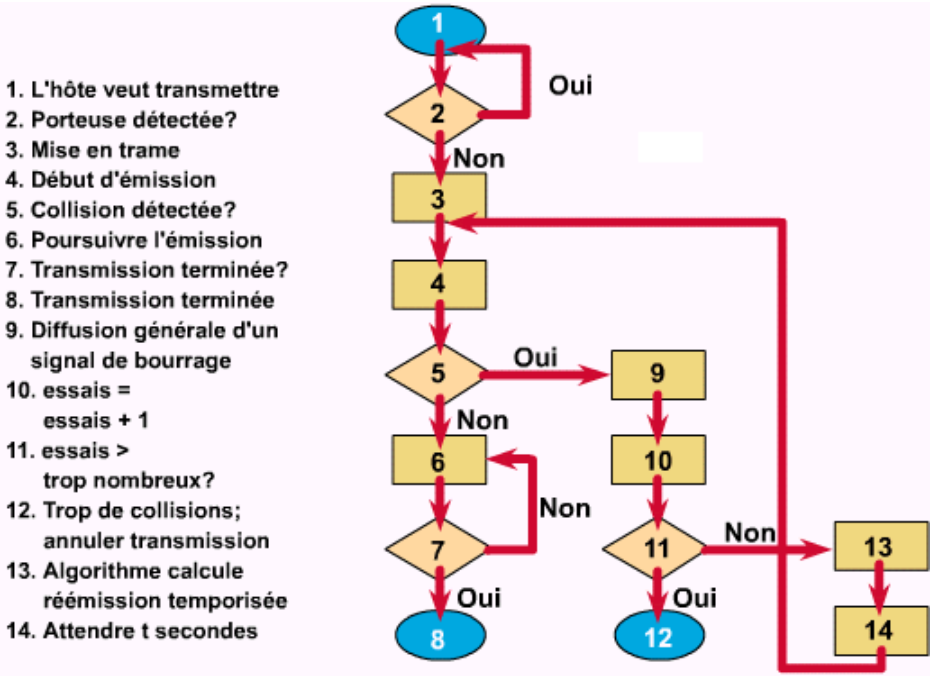
Données de brouillage

Une fois que tous les dispositifs du réseau ont cessé de transmettre pendant un certain laps de temps (différent pour chaque dispositif), n'importe quel d'entre eux peut essayer de nouveau d'avoir accès au média de réseautage. Lorsque la transmission de données reprend sur le réseau, les dispositifs en cause dans la collision n'ont pas la priorité de transmission des données.



Attente aléatoire

La figure suivante résume la méthode d'accès CSMA/CD.



Algorithme CSMA/CD

Ethernet est un média de transmission de diffusion. Cela signifie que tous les dispositifs d'un réseau peuvent voir toutes les données acheminées sur le média de réseautage. Toutefois, ce ne sont pas tous les dispositifs du réseau qui traiteront des données. Seuls les dispositifs dont l'adresse MAC correspond à l'adresse de destination MAC transportée par les données capteront les données.
Une fois qu'un dispositif a vérifié l'adresse de destination MAC transportée par les données, il s'assure que la trame ne contient aucune erreur. Si le dispositif détecte des erreurs, la trame est supprimée. Le dispositif de destination n'avisera pas le dispositif d'origine que la trame comporte ou non des erreurs. L'architecture de réseau sans connexion Ethernet est décrite comme un système de remise au mieux.

5. Paramètres du protocole

On appelle *Tranche Canal (TC) ou Time Slot (TS)* la durée nécessaire à une application pour que celle-ci soit certaine que son message soit transmis sans problème. Cette période est au minimum égale à deux fois la durée maximale de propagation d'un message sur le câble. Ceci justifie les contraintes de câblage vues précédemment.
Si l'on additionne tous les délais dans l'aller et le retour d'un signal introduit pour la transmission de celui-ci et si l'on considère les deux stations les plus éloignées, le calcul donne une durée maximale de propagation de 44,99 ps. Ainsi pour un réseau Ethemet classique la norme indique une valeur légèrement supérieure. La durée d'une tranche canal est équivalente à la durée d'émission de 512 bits soit 51,2 ps à
10 Mbit/s.
La durée d'émission des trames doit toujours être supérieure ou égale à la tranche canal. Pour un réseau à 10 Mbit/s, 51,2 µs correspondent à la durée d'émission d'une trame de 64 octets. Si le paquet est plus petit, des bits de *bourrage (ou padding)* sont introduits en fin de trame pour atteindre cette taille.
Cette durée minimale a été introduite pour que toutes les stations soient dans le même état à la fin d'une transmission.
La taille maximale d'une trame est de 1 518 octets (1500 octets de données, 14 octets d'en-tête et 4 octets de CRC), pour éviter qu'une station monopolise le canal. Cette taille est fixée arbitrairement.

Quand une collision est détectée par une station, celle-ci n'interrompt pas immédiatement la transmission mais continue à émettre des données de brouillage *(ou jamming)* pour permettre la détection de la collision par les autres stations. La taille du brouillage est de 32 bits. L'émission d'une trame en collision peut donc durer moins d'une tranche canal.

6. Algorithme du BEB

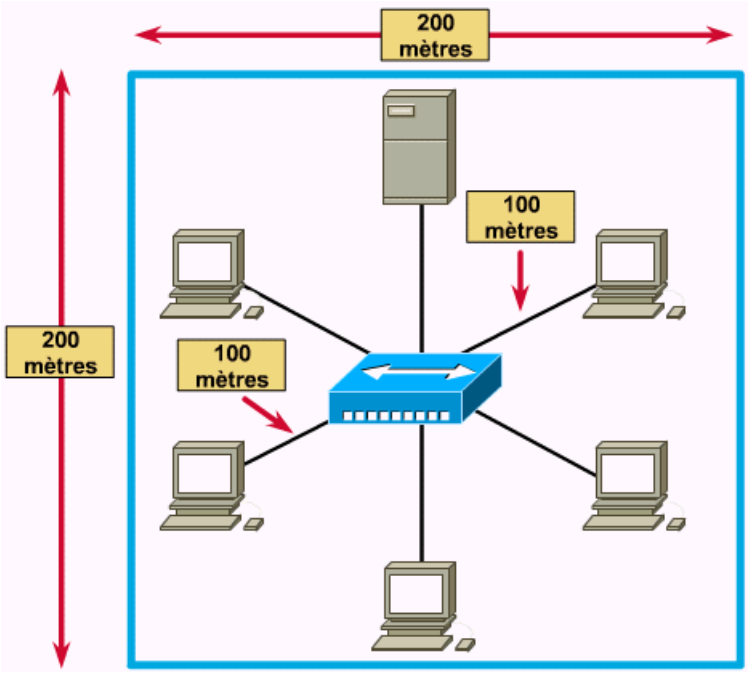
On appelle BEB *(Binary Exponential Backoff),* l'algorithme qui permet de limiter la charge du réseau quand une collision se produit. Lors d'une collision, les stations impliquées arrêtent leur émission après que celle-ci ait durée une tranche canal. Il reste à définir ce que font les stations après la collision. Si celles-ci recommencent à émettre aussitôt après, une autre collision se produira et ainsi de suite ; plus aucun message ne sera émis sur le support. Il faut trouver un mécanisme pour départager les stations (bien entendu sans échanger de message!) Il faut aussi s'arranger pour limiter l'accès au support physique en cas de congestion. Les résolutions des collisions, plus l'arrivée des nouveaux messages, risquent d'induire de nouvelles collisions qui vont encore plus limiter la bande passante utile, ce qui va entraîner de nouvelles collisions, et ainsi de suite en s'amplifiant.
L'algorithme du BEB permet aux stations de tirer au sort la durée d'attente avant la prochaine tentative de ré-émission. Notons 0 et 1 les deux choix possibles. En supposant que deux stations seulement participent à la résolution de la collision, on trouve les quatre possibilités suivantes :

- la première station et la seconde station tirent 0 : les deux stations recommencent à émettre juste après la collision et reproduisent une collision ;
- la première station tire 0 et la seconde station tire 1 : la première station commence à émettre, au bout d'une tranche canal la seconde veut émettre, ainsi détectant une activité sur le médium, elle va attendre la fin de la transmission du message de la première station pour émettre son message. La collision est résolue ;
- la première station tire 1 et la seconde station tire 0 : le cas est identique au cas précédent. La collision est résolue ;
- la première station et la deuxième station tirent 1 : les deux stations vont attendre une tranche canal, puis vont simultanément tenter d'émettre leur message en produisant une nouvelle collision.

Sur cet exemple on remarque qu'il existe une chance sur deux de résoudre la collision. Dans le cas où celle-ci n'est pas résolue (les deux stations ont tiré le même nombre ou plus de deux stations sont en cause dans la collision), on double l'espace de tirage. Les stations pourront attendre 0, 1, 2 ou 3 tranches canal. Ce qui réduit à 1/4 la probabilité que deux stations émettent simultanément. De plus les stations vont attendre plus longtemps en moyenne pour émettre leur message, ce qui va réduire la charge sur le réseau.
Par défaut, l'espace de tirage est doublé jusqu'à la $10^{ème}$ tentative. Si au bout de 16 tentatives la trame n'est toujours pas émise, le protocole abandonne et informe la couche supérieure de l'échec.

7. Topologies et média Ethernet 10Base-T

Dans le cas d'un réseau local qui utilise la topologie en étoile, le média de réseautage relie chaque équipement du réseau à un concentrateur. La configuration physique de la topologie en étoile ressemble aux rayons reliant la jante au moyeu d'une roue. Comme le démontre l'illustration ci-dessous, un point de contrôle central est utilisé dans la topologie en étoile. Dans une topologie en étoile, la communication entre les dispositifs reliés au réseau local se fait par le biais de câblage point à point au lien central ou concentrateur. Dans le cas d'un réseau à topologie en étoile, tout le trafic passe par le concentrateur.

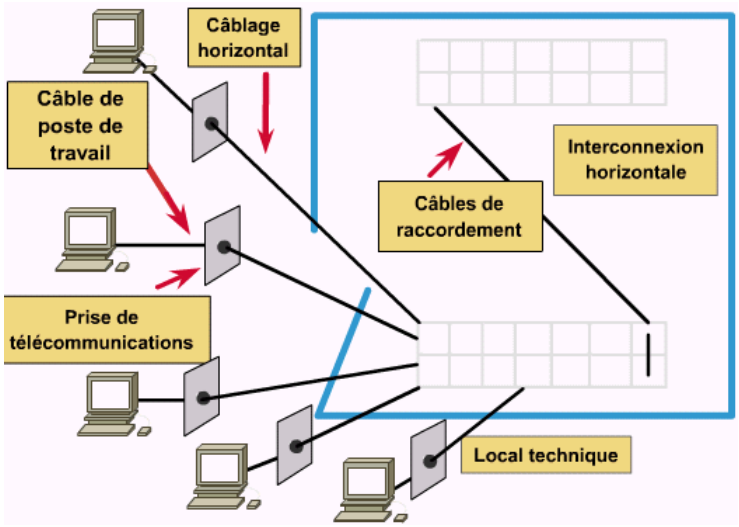


Le concentrateur reçoit une trame sur un port, puis copie et transmet (répète) la trame à tous les autres ports. Le concentrateur peut être actif ou passif. Un concentrateur actif connecte le média de réseautage et régénère le signal. Dans le cas d'un réseau Ethernet, les concentrateurs agissent à titre de répéteurs multiports. En régénérant le signal, les concentrateurs actifs permettent aux données de se déplacer sur de plus grandes distances. Un concentrateur passif est un dispositif utilisé pour connecter le média de réseautage, qui ne régénère pas les signaux.

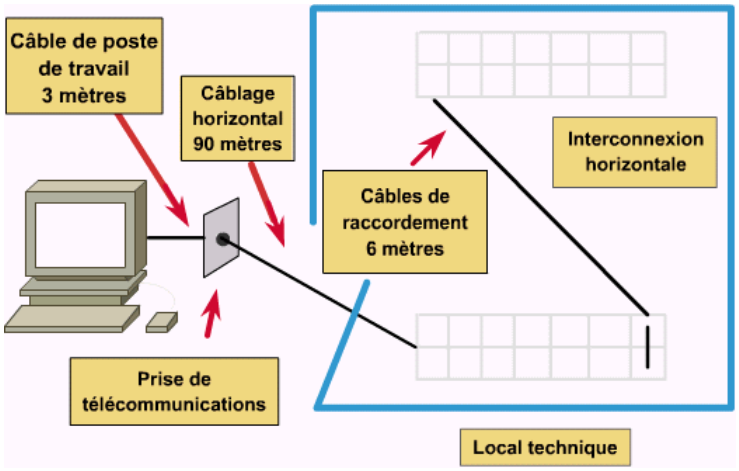
L'un des avantages de la topologie en étoile est qu'elle est considérée comme la plus facile à concevoir et à installer parce que le média de réseautage relie directement chaque poste de travail à un concentrateur. Un autre avantage est la facilité de maintenance, car la seule zone de concentration est située dans le concentrateur. Dans le cas d'une topologie en étoile, il est facile de modifier la configuration utilisée pour le média de réseautage et d'effectuer le dépannage. Des postes de travail peuvent facilement être ajoutés à un réseau utilisant la topologie en étoile. Si l'un des liens de média de réseautage est brisé ou court-circuité, seul le dispositif relié à ce point est hors service, le reste du réseau local demeure en fonction. En bref, une topologie en étoile signifie une plus grande fiabilité.

De certaines façons, les avantages de la topologie en étoile peuvent aussi être considérés comme des désavantages. Par exemple, bien que le fait de limiter le nombre de dispositifs à un par longueur de média de réseautage puisse faciliter l'établissement d'un diagnostic lorsqu'un problème survient, cela augmente aussi le nombre de médias de réseautage nécessaires, ce qui se traduit par une augmentation des coûts d'installation. De plus, bien que le concentrateur facilite la maintenance, il représente un point de défaillance unique (si le concentrateur fait défaut, toutes les connexions du réseau sont perdues).

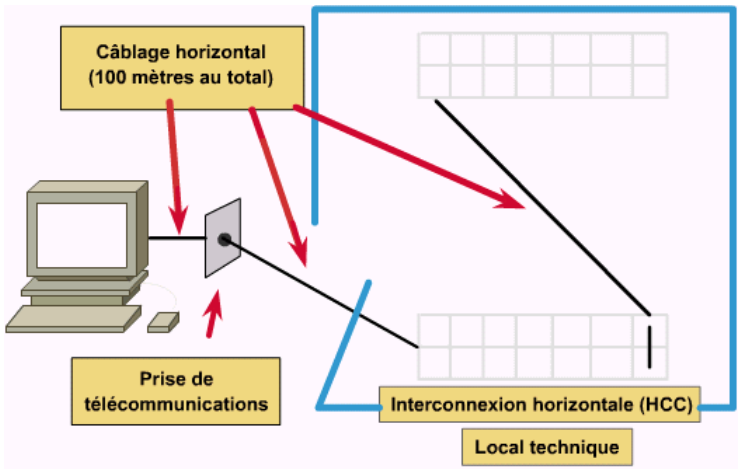
La norme TIA/EIA-568-A précise que la configuration physique, ou la topologie, utilisée dans le cas du câblage horizontal doit être une topologie en étoile. Cela signifie que le raccordement mécanique de chaque sortie ou connecteur de télécommunication est situé dans le tableau de connexions dans le local technique. Chaque sortie est câblée indépendamment et directement au tableau de connexions.

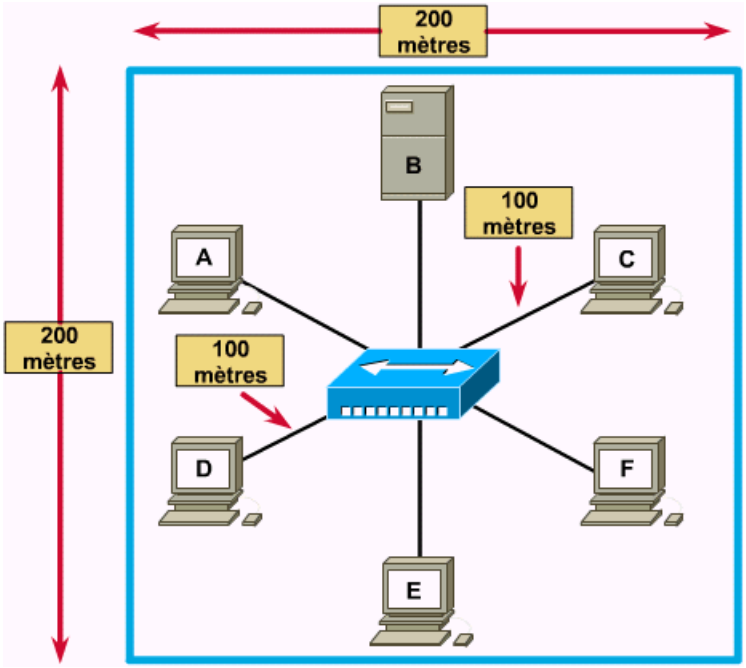


La norme TIA/EIA-568-A indique que la longueur maximale de câblage horizontal de paires torsadées non blindées est de 90 m. [4]La longueur maximale des câbles de raccordement à la sortie ou au connecteur de télécommunication est de 3 m, et la longueur maximale des câbles de raccordement à l'interconnexion horizontale est de 6 m.



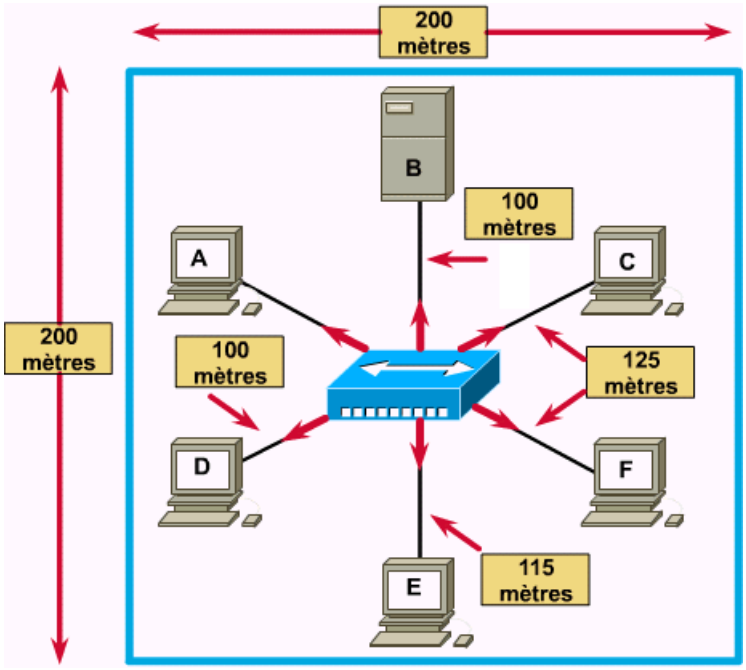
La longueur maximale d'un parcours de câble horizontal, qui s'étend du concentrateur à n'importe quel poste de travail, est de 100 m (en réalité, il s'agit de 99 m, mais la valeur est arrondie à 100 m). Cette longueur comprend les 90 mètres de câblage horizontal, les trois mètres de câbles de raccordement et les six mètres pour les interconnexions horizontales. Les parcours de câbles horizontaux dont la topologie est en étoile s'étendent à partir du concentrateur, comme les rayons d'une roue. Cela signifie que le réseau local qui utilise cette topologie peut couvrir une superficie équivalente à celle d'un cercle dont le rayon est de 100 m.



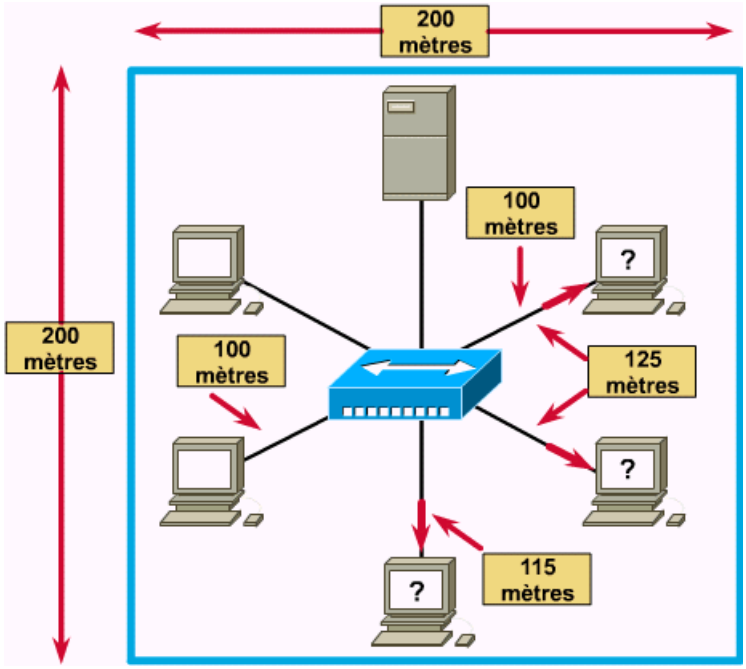


Il y aura des circonstances où la zone à desservir par un réseau sera supérieure aux longueurs maximales précisées par la norme TIA/EIA-568-A que peut utiliser une topologie en étoile simple. Par exemple, imaginez un édifice dont les dimensions sont de 250 m x 250 m. Une topologie en étoile simple qui adhérerait à la norme TIA/EIA-568-A de câblage horizontal ne pourrait pas desservir tout un immeuble de cette dimension.

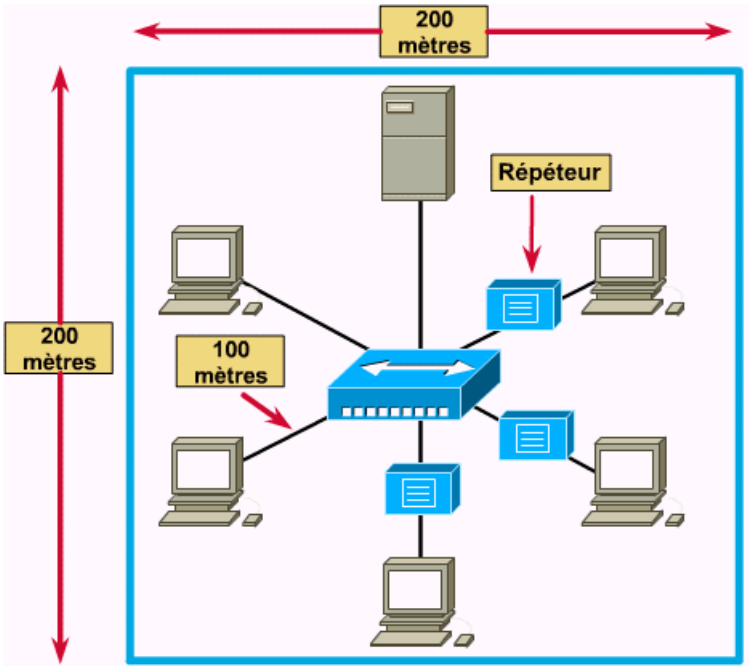
Tel qu'il est indiqué dans l'illustration ci-dessous, les postes de travail E, F et C sont situés à l'extérieur de la zone desservie par une topologie en étoile conforme à la norme TIA/EIA-568-A. Comme il est indiqué, ils ne font pas partie du réseau local. Ainsi, les utilisateurs de ces postes de travail qui veulent transmettre, partager et recevoir des fichiers sont dans l'obligation d'utiliser le réseau disquettes. Comme personne ne veut retourner au temps du réseau disquettes, certains installateurs de câbles sont tentés de résoudre ce problème en prolongeant la longueur du média de réseautage au-delà des longueurs maximales précisées par la norme EIA/TIA-568-A.



Lorsque les signaux quittent une station émettrice, ils sont purs et facilement reconnaissables. Toutefois, plus le câble est long, plus les signaux s'affaiblissent et se détériorent à mesure qu'ils circulent sur le média de réseautage. Si un signal se déplace au-delà de la distance prescrite, rien ne garantit que la carte réseau qu'il atteindra sera capable de le lire.



Si une topologie en étoile ne peut offrir une couverture équivalant à la zone à réseauter, l'utilisation de dispositifs d'interréseautage qui n'entraînent pas l'affaiblissement du signal peut permettre de l'étendre. La topologie qui en résulte se nomme une topologie en étoile étendue. L'utilisation de répéteurs permet d'étendre la distance d'exploitation d'un réseau. Les répéteurs reçoivent les signaux affaiblis, les regénèrent, les resynchronisent et les transmettent de nouveau sur le réseau.



8. Ethernet à 100 Mbit/s

La version à 100 Mbit/s doit être aussi simple, bon marché et compatible avec le réseau Ethernet à 10 Mbit/s. Le câblage actuel des réseaux 10 base T est conservé ainsi que le format des trames. L'Ethernet 100 Mbit/s ne fonctionnera que sur cette topologie, la topologie en bus est abandonnée.

S'il est relativement facile de construire des équipements électroniques capables d'émettre et de recevoir des données à 100 Mbit/s, le gros problème vient de la limitation des radiations électromagnétiques imposée par la législation.

Deux sous-comités IEEE travaillent sur cette normalisation et ont produit des normes incompatibles entre elles. Le comité IEEE 802.3u, soutenu par la presque totalité des constructeurs, reprend les caractéristiques du CSMA/CD, mais modifie les règles de câblage pour que le réseau puisse fonctionner à 100 Mbit/s. Le comité IEEE 802.12, aussi appelé *IOOVG-AnyLan,* est soutenu principalement par HP. Un nouveau protocole d'accès est défini. Ce protocole intègre aussi bien les formats de trames de l'anneau à jeton que ceux d'Ethernet d'où son nom d'AnyLan. Le terme VG par ailleurs signifie *Voice Grade,* ce qui indique que ce protocole peut fonctionner sur des câblages destinés à supporter la voix, c'est-à-dire un câblage de catégorie 3.

8.1. *Le sous-comité IEEE 802.3u : 100 base T* 3.10.1.1. *Les* règles *de câblage et les connecteurs*

Le comité IEEE 802.3 qui avait déjà travaillé sur l'Ethernet à 10 Mbit/s propose les standards :

- 100 base TX qui utilise deux paires torsadées en duplex comme pour le câblage Ethernet 10 Mbit/s. Le câblage doit être de catégorie 5 ;
- 100 base T4 qui utilise quatre paires torsadées de manière unidirectionnelle (alternat). Ce câblage est en principe incompatible avec le câblage Ethernet existant. Mais en pratique les deux paires non utilisées sont disponibles. Ce standard permet d'utiliser des câblages moins performants comme ceux de la catégorie 3 ;
- 100 base FX qui utilise des liens en fibre optique multimode.

La norme pour les réseaux à 10 Mbit/s précise que la durée d'émission minimale d'une trame est de 51,2 µs. A 100 Mbit/s cela correspondrait à une taille minimale de 640 octets. Les petites trames, qui constituent une part essentielle du trafic interactif, ne contiendraient pratiquement plus d'information utile mais presque uniquement des bits de bourrage. L'émission d'une petite trame à 100 Mbit/s mettra autant de temps qu'à 10 Mbit/s, soit 51,2 µs ! Autre inconvénient, lors de la recopie d'une trame d'un réseau à 100 Mbit/s sur un réseau à 10 Mbit/s, le bourrage ne peut pas être éliminé par Ethernet et la taille des trames serait comprise entre 640 et 1 518 octets.

La seule solution pour que les principes de fonctionnement du CSMA/CD restent valable consiste à réduire la durée de propagation maximale du signal dans le réseau. Il est physiquement impossible d'augmenter la célérité du signal sur le support. Le temps de traversée des couches électroniques est difficilement réductible pour un coût abordable. La seule manière de réduire la durée de parcours du signal est de limiter la taille du réseau.

Ceci est aujourd'hui possible. Ethernet 10 Mbit/s a été conçu à une époque où les équipements d'interconnexion étaient peu nombreux et très chers. L'Ethernet 10 Mbit/s devait pouvoir couvrir de grandes étendues : la distance entre deux stations étant au maximum de 2,5 km. A l'heure actuelle, les réseaux locaux sont surtout employés pour interconnecter des machines qui sont à un même étage d'un immeuble ou dans une même pièce. Les distances de câblage peuvent être réduites sans pour autant pénaliser les performances du réseau. De plus, la présence de ponts sur le réseau permet de limiter la superficie des domaines de collision.

Le paramétrage d'Ethernet 100 Mbit/s a été fait pour que la tranche canal soit de 5,12 µs. Ainsi la taille minimale de la trame est toujours de 64 octets. La taille maximale est toujours fixée à 1 518 octets. Les réseaux à 10 Mbit/s et 100 Mbit/s sont entièrement compatibles. Les contraintes de câblage, d'électronique pour les équipements découlent de ce choix.

L'espacement entre les trames (IFS : *Inter Frame Spacing)* vaut 0,96 µs. L'architecture en bus n'a pas été retenue. Les stations doivent se connecter à des hubs qui font office de répéteur comme pour la topologie 10 base T. Il ne faut pas confondre 100 Mbit/s et commutation. Bien qu'un commutateur améliore les performances en supprimant les collisions, le 100 base T a été conçu pour fonctionner avec des répéteurs qui émulent et propagent les collisions.

Les câbles entre la station et le répéteur font au maximum 100 mètres.

Principes fondamentaux de l'anneau à jeton

1. Aperçu de l'anneau à jeton et de ses variantes

IBM a mis au point le premier réseau en anneau à jeton au cours des années 1970. Il s'agit toujours de la principale technologie de réseau local d'IBM. Elle se situe juste derrière la norme Ethernet (IEEE 802.3) concernant la mise en œuvre de réseaux locaux. La norme IEEE 802.5 est presque identique au réseau en anneau à jeton d'IBM, et elle est entièrement compatible avec celui-ci. La norme IEEE 802.5 a été inspirée du réseau en anneau à jeton d'IBM; elle continue de calquer ses innovations. Le terme anneau à jeton se rapporte à l'anneau à jeton d'IBM et à la norme IEEE 802.5. Le tableau de l'illustration principale fait la comparaison et établit les différences entre les deux normes.

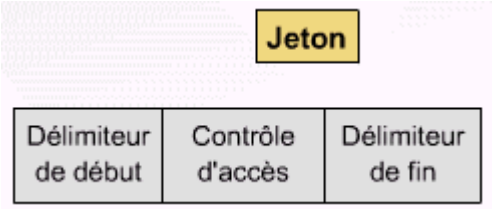
	Anneau à jeton IBM	IEEE 802.5
Débits	4 ou 16 Mbits/s	4 ou 16 Mbits/s
Postes/segment	260 (câble à paires torsadées blindées) 72 (câble à paires torsadées non blindées)	250
Topologie	En étoile	Non spécifié
Média	Câble à paires torsadées	Non spécifié
Signalisation	Bande de base	Bande de base
Méthode d'accès	Passage de jeton	Passage de jeton
Codage	Différentiel Manchester	Différentiel Manchester

Comparaison Anneau à jeton IBM et IEEE 802.5

2. Format de trame de réseaux en anneau à jeton

Jetons

Les jetons ont une longueur de trois octets et sont composés d'un *délimiteur de début de trame*, d'un *octet de contrôle d'accès* et d'un *délimiteur de fin de trame*. Le délimiteur de début de trame avertit chaque station de l'arrivée d'un jeton ou d'une trame de données ou de commande. Ce champ comporte aussi des signaux qui distinguent l'octet de l'ensemble de la trame en violant le codage utilisé ailleurs dans la trame.



Octet de contrôle d'accès

L'octet de contrôle d'accès comprend un champ *priorité* et un champ *réservation* ainsi qu'un bit représentant le *jeton* et un bit de *comptage moniteur*. Le bit représentant le jeton distingue le jeton de la trame de données ou de commande, et le bit de comptage moniteur détermine si la trame circule constamment autour de l'anneau. Le délimiteur de fin de trame indique la fin du jeton ou de la trame de données ou de commande. Il comprend des bits indiquant une trame endommagée et d'autres indiquant la dernière trame d'une séquence logique.

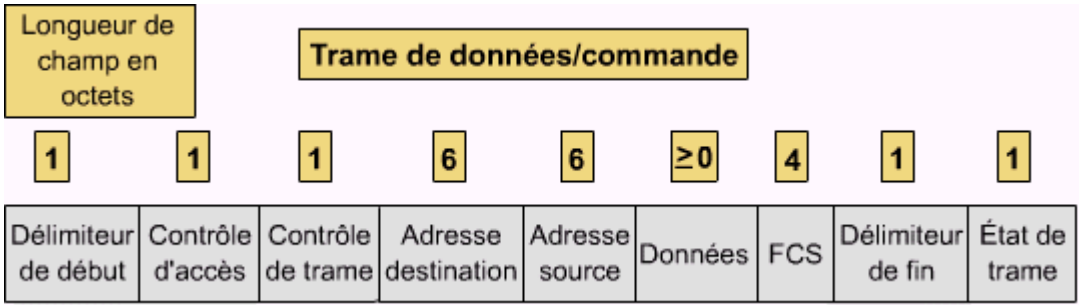
Trames de données / commande

La taille des trames de données / commande varie selon la taille du champ d'information. Les trames de données transportent de l'information à l'intention des protocoles de couche supérieure; les trames de commande comportent de l'information de contrôle, mais ne contiennent pas de données pour les protocoles de couche supérieure.

Dans le cas des trames de données / commande, un *octet de commande de trame* suit l'octet de contrôle d'accès. L'octet de contrôle de trame indique si la trame comporte des données ou de l'information de contrôle. Dans le cas des trames de commande, cet octet précise le type d'information de contrôle.

À la suite de l'octet de commande de trame se trouvent deux champs d'adresse qui précisent les stations de source et de destination. Comme dans le cas de la norme IEEE 802.5, ces adresses ont 6 octets. Le champ de données suit le champ d'adresse. La longueur de ce champ est limitée par le jeton de l'anneau qui comprend la période maximale durant laquelle une station peut conserver le jeton.

À la suite du champ de données se trouve le champ *séquence de contrôle de trame (FCS)*. Dans ce champ, la station source indique une valeur calculée en fonction du contenu de la trame. La station de destination recalcule la valeur afin de déterminer si la trame a été endommagée pendant le transport. Les trames endommagées sont supprimées. Comme dans le cas du jeton, la trame de données / commande se termine par un délimiteur de fin de trame.



3. MAC d'anneau à jeton

3.1 Passage de jeton

Le réseau en anneau à jeton et IEEE 802.5 sont les principaux exemples de réseaux de passage de jeton. Les réseaux de passage de jeton font circuler une petite trame, appelée jeton, autour du réseau. La possession du jeton confère le droit de transmettre des données. Si le nœud qui reçoit un jeton n'a pas d'information à transmettre, il passe le jeton à la prochaine station d'extrémité. Chaque station peut conserver le jeton pour un délai maximal qui varie en fonction de la technologie mise en place.

Lorsqu'une station qui a de l'information à transmettre passe un jeton, elle le saisit et en altère un bit. Le jeton se transforme en une séquence de début de trame. Ensuite, la station annexe au jeton l'information à transmettre et envoie ces données à la prochaine station sur l'anneau. Il n'y a pas de jeton sur le réseau pendant que la trame d'information circule sur l'anneau, à moins que l'anneau n'ait la capacité d'effectuer des libérations anticipées du jeton. Les autres stations de l'anneau ne peuvent pas transmettre pendant ce temps. Elles doivent attendre que le jeton soit disponible. Aucune collision ne survient dans les réseaux en anneau à jeton. Si le réseau possède des capacités de libération anticipée du jeton, un nouveau jeton peut être libéré une fois la transmission de la trame terminée.

La trame d'information circule sur l'anneau jusqu'à ce qu'elle atteigne la station de destination prévue. Cette station copie alors l'information dans le but de la traiter. La trame d'information circule autour de l'anneau jusqu'à ce qu'elle atteigne la station d'émission où elle est alors retirée. La station d'émission peut vérifier si la trame a été reçue et copiée par la station de destination.

À l'opposé des réseaux à accès CSMA/CD, comme les réseaux de type Ethernet, les réseaux de passage du jeton sont déterministes. Cela signifie que vous pouvez calculer la période maximale qui s'écoulera avant que toute station d'extrémité soit en mesure de transmettre. Cette caractéristique, ainsi que plusieurs caractéristiques de fiabilité, rendent les réseaux en anneau à jeton idéaux dans le cas d'applications où tout retard doit être prévisible et qui requièrent un réseau solide. Les environnements d'automatisation d'usine représentent des exemples de réseaux devant être prévisibles et solides.

3.2 Système de priorité

Les réseaux en anneau à jeton font appel à un système de priorité d'avant-garde qui permet à certaines stations prioritaires définies par l'utilisateur de se servir du réseau plus souvent. Les trames des réseaux en anneau à jeton ont deux champs qui contrôlent la priorité - le champ *priorité* et le champ *réservation*.

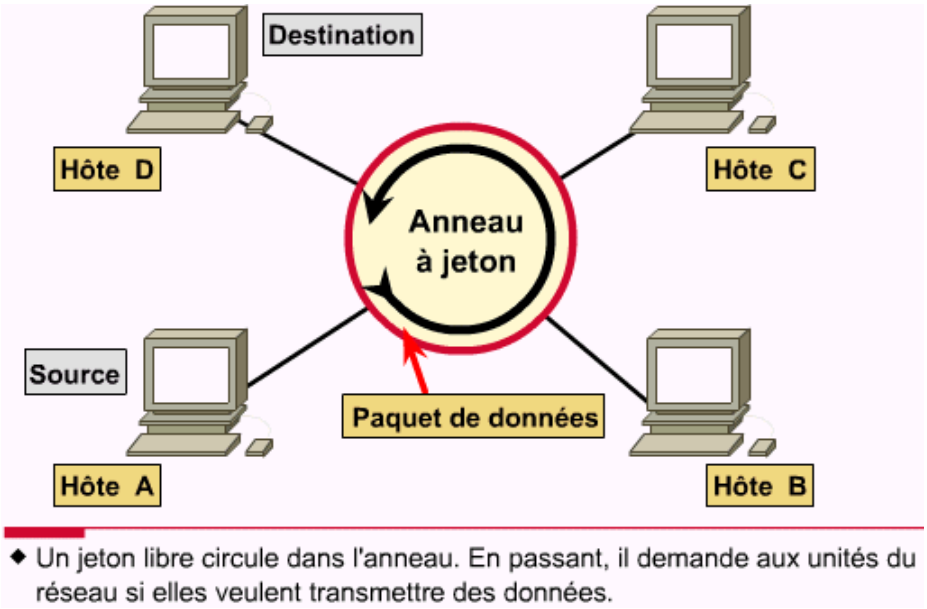
Seules les stations dont la priorité est égale ou supérieure à la valeur de priorité contenue dans un jeton peuvent saisir ce jeton. Une fois que le jeton a été saisi et transformé en trame d'information, seules les stations dont la valeur de priorité est supérieure à la valeur de la station émettrice peuvent réserver le jeton pour le prochain passage sur le réseau. Le prochain jeton généré comprend la priorité plus élevée de la station qui a effectué la réservation. Les stations qui élèvent le niveau de priorité d'un jeton doivent remettre le jeton au niveau de priorité où il se trouvait une fois leur transmission terminée.

3.3 Mécanismes de gestion

Les réseaux en anneau à jeton utilisent plusieurs mécanismes pour détecter les incidents réseau et compenser pour eux. Un des mécanismes consiste à sélectionner une station du réseau en anneau à jeton afin qu'elle soit le moniteur actif. Cette station agit à titre de source centralisée de renseignements de synchronisation pour les autres stations du réseau en anneau à jeton et exécute une gamme de fonctions de maintenance de l'anneau. N'importe quelle station peut potentiellement jouer le rôle de moniteur actif. Une des fonctions de cette station est de retirer de l'anneau les trames qui sont en circulation constante. Lorsqu'un dispositif émetteur fait défaut, sa trame peut continuer à circuler sur l'anneau et empêcher les autres stations de transmettre leurs propres trames; cela peut bloquer le réseau. Le moniteur actif peut détecter ces trames, les retirer de l'anneau et générer un nouveau jeton.

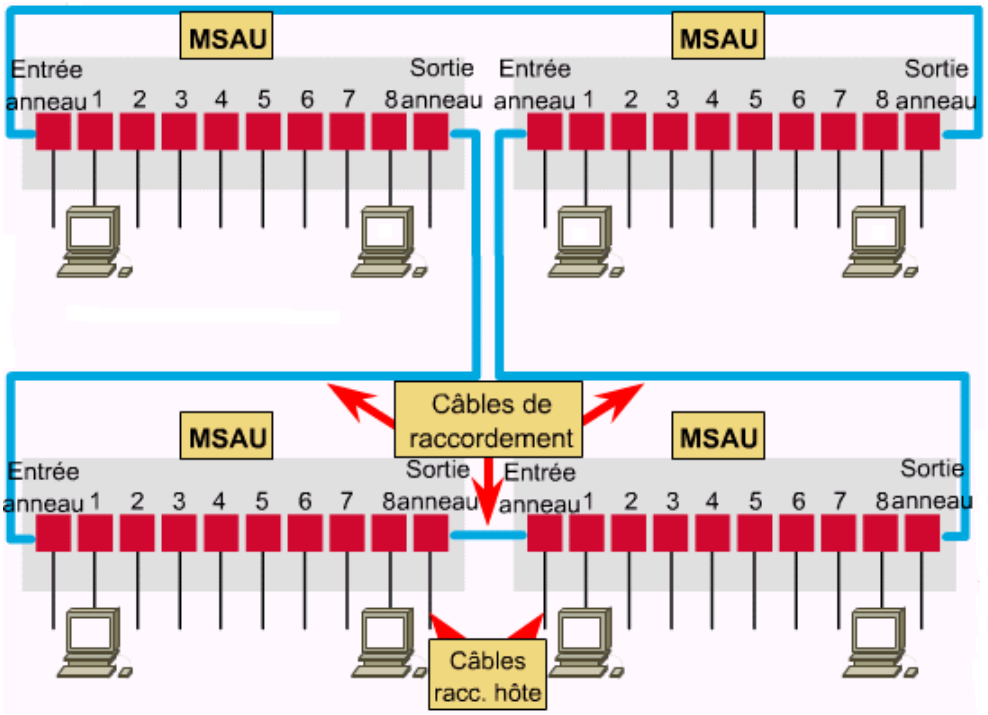
La topologie en étoile du réseau en anneau à jeton d'IBM contribue aussi à la fiabilité globale du réseau. Les *MSAU* (*unités d'accès multistation*) actives peuvent voir toute l'information contenue dans un réseau en anneau à jeton, ce qui leur permet de détecter les problèmes et de retirer, au besoin, des stations de l'anneau de façon sélective. La *trame Beacon*, une formule d'anneau à jeton, détecte et essaie de réparer les incidents de réseau. Lorsqu'une station détecte un problème grave sur le réseau, comme un bris de câble par exemple, elle envoie une *trame Beacon*. La trame Beacon précise un *domaine de faute*. Le domaine de faute comprend la station signalant la défaillance, son *prochain voisin actif en amont (NAUN)* et tout ce qui se trouve entre les deux. La trame Beacon lance un processus nommé *autoreconfiguration*, par lequel les nœuds qui se trouvent à l'intérieur du

domaine de faute effectuent automatiquement des diagnostics. Ce processus tente de reconfigurer le réseau en contournant la zone où la défaillance s'est produite. Physiquement, les MSAU peuvent accomplir cela par le biais de la reconfiguration électrique.



4. Topologies physiques et média de l'anneau à jeton

Les stations en anneau à jeton d'IBM (qui utilisent souvent les câbles à paires torsadées blindées et non blindées comme média) sont directement connectées aux unités MSAU (unités d'accès multistation) et peuvent être inter-reliées afin de former un grand anneau. Des câbles de raccordement connectent les unités MSAU aux unités MSAU voisines. Des câbles de lobe connectent les unités MSAU aux stations. Ces unités comportent des relais de contournement permettant de retirer des stations de l'anneau.



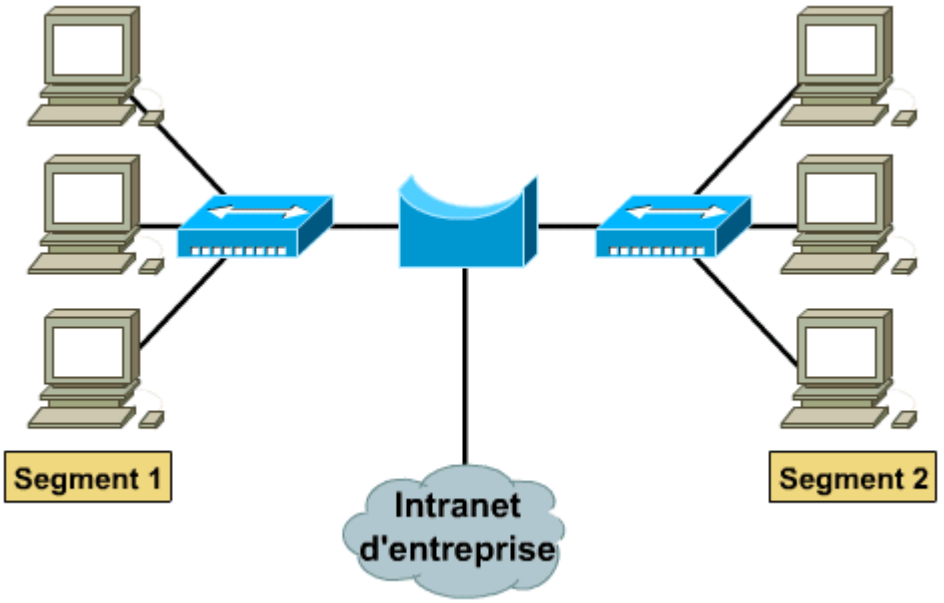
Chapitre 4

4 Les unités de couche 2

4.1 Ponts

Un pont relie des segments de réseau. Il doit prendre des décisions intelligentes quant au passage ou non des signaux au prochain segment. Un pont peut améliorer les performances d'un réseau en éliminant le trafic non nécessaire et en minimisant les risques de collision. Le pont divise le trafic en segments et le filtre en fonction de la station ou de l'adresse MAC.

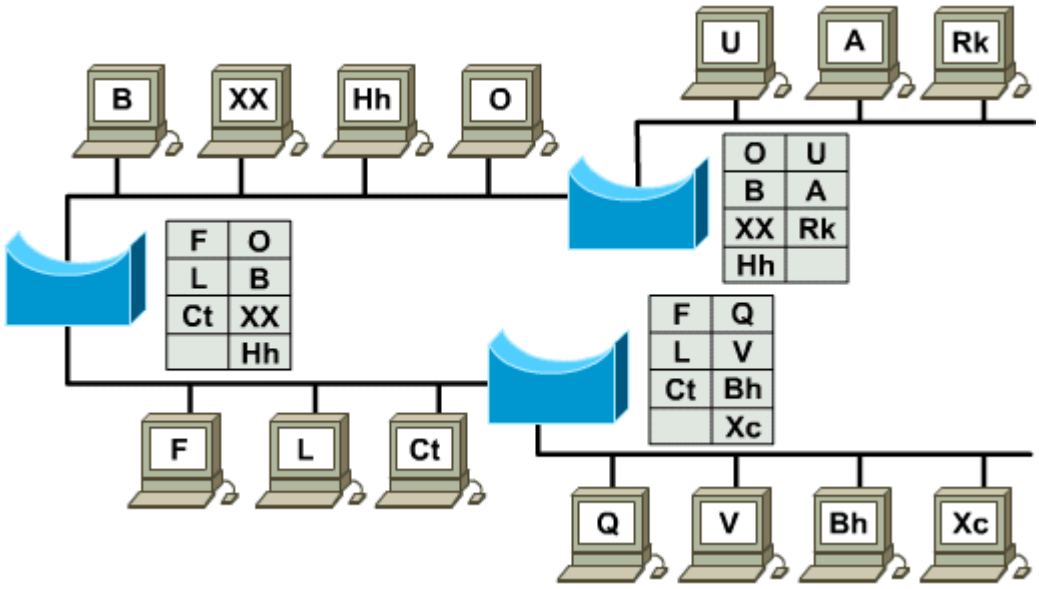
Les ponts ne sont pas des dispositifs complexes. Ils analysent les trames d'arrivée, prennent des décisions quant à la transmission de trames en fonction de l'information qu'elles contiennent et les acheminent vers leur destination. Les ponts se préoccupent uniquement de passer les paquets, ou de ne pas les passer, en fonction de leur adresse de destination. Les ponts passent souvent des paquets entre des réseaux utilisant deux protocoles de couche 2 différents.



Exemple de Pont

4.2 Fonctionnement d'un pont de couche 2

Le pontage se fait au niveau de la couche liaison des données, qui contrôle le flux des données, traite les erreurs de transmission, fournit un adressage physique et gère l'accès au média physique. Le pontage assure ces fonctions grâce à divers protocoles de couche liaison, qui précisent des algorithmes particuliers de contrôle du flux, de traitement des erreurs, d'adressage et d'accès aux médias. Comme exemples de protocoles de couche liaison des données, mentionnons Ethernet, l'anneau à jeton et FDDI.
La transparence des protocoles de couche supérieure est un des principaux avantages du pontage. Comme les ponts fonctionnent au niveau de la couche liaison des données, ils n'ont pas à examiner les informations de la couche supérieure. Ils peuvent ainsi acheminer rapidement du trafic représentant n'importe quel protocole de la couche réseau. Un pont achemine souvent des protocoles et d'autres types de trafic entre deux segments de réseau.
Les ponts n'ont pas à examiner les informations de la couche supérieure parce qu'ils fonctionnent au niveau de la couche liaison des données, soit la couche 2 du modèle OSI. Ils filtrent le trafic réseau en regardant seulement l'adresse MAC et non les protocoles. Un pont achemine souvent des protocoles et d'autres types de trafic entre deux segments de réseau ou plus. Comme les ponts ne regardent que l'adresse MAC, ils peuvent acheminer rapidement du trafic représentant n'importe quel protocole de la couche réseau. Pour filtrer ou livrer de façon sélective du trafic réseau, un pont crée des tables de toutes les adresses MAC situées sur les segments de réseau qui lui sont directement reliés. (figure **)



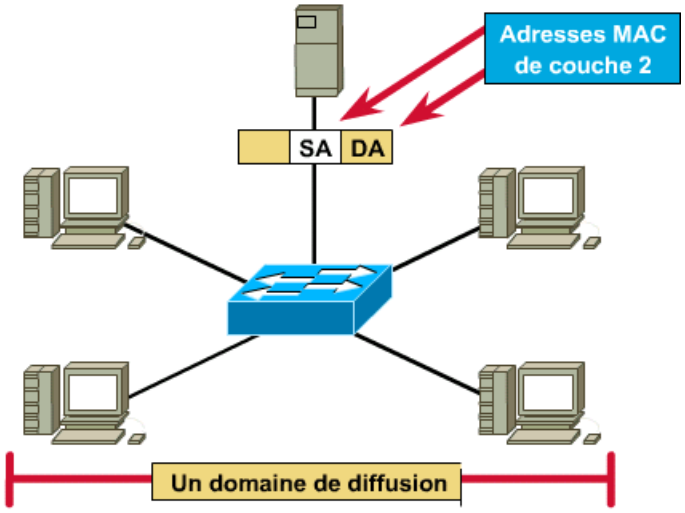
Lorsque des données arrivent sur le média de réseau, un pont compare l'adresse MAC de destination transportée par les données aux adresses MAC contenues dans ses tables. Si le pont détermine que l'adresse MAC de destination des données provient du même segment de réseau que la source, il n'achemine pas les données à d'autres segments du réseau. Si le pont détermine que l'adresse MAC de destination des données ne provient pas du même segment de réseau que la source, il achemine les données au segment approprié. Ainsi, les ponts peuvent réduire de manière importante la quantité de trafic entre les segments de réseau en éliminant le trafic inutile.

Les ponts sont des unités d'interconnexion de réseaux qui peuvent servir à réduire de grands domaines de collisions. Les domaines de collisions sont des zones où il peut vraisemblablement y avoir des interférences entre les paquets. Pour éviter cette situation, on divise le réseau en segments plus petits et on réduit le volume du trafic qui doit passer d'un segment à un autre. Les ponts fonctionnent au niveau de la couche 2 (liaison de données) du modèle OSI, car ils ne s'intéressent qu'aux adresses MAC. Au fur et à mesure que les données sont acheminées sur le réseau en route vers leur destination, elles sont captées et examinées par chacune des unités du réseau, y compris les ponts. Les ponts fonctionnent mieux là où le volume de trafic n'est pas trop dense entre les segments d'un même réseau. Lorsque le trafic entre des segments de réseau devient dense, les ponts peuvent devenir un goulot d'étranglement et ralentir les communications.

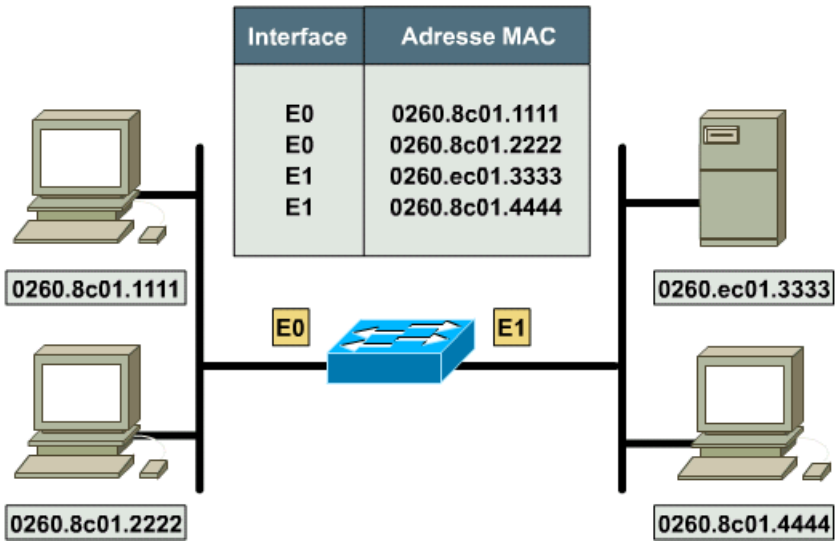
L'utilisation d'un pont peut entraîner un autre problème. En effet, les ponts répandent et multiplient un type spécial de paquets de données. Ces paquets de données surviennent lorsqu'une unité de réseau veut atteindre une autre unité du réseau, mais qu'elle ne connaît pas l'adresse de destination de cette dernière. Lorsque cela se produit, il arrive fréquemment que la source envoie une *diffusion* à toutes les unités d'un réseau. Puisque chacune des unités du réseau doit porter attention à ces messages de diffusion, les ponts les acheminent toujours. Une tempête de messages de diffusion peut se produire si un trop grand nombre de messages de diffusion est envoyé sur un réseau. Une telle tempête peut entraîner des temps d'indisponibilité et des ralentissements dans le trafic, ainsi que diminuer les performances du réseau à un niveau inférieur au niveau acceptable.

4.3 Commutateurs

La commutation est une technologie qui permet d'atténuer la congestion dans les réseaux locaux Ethernet en réduisant le trafic et en augmentant la largeur de bande. Les commutateurs, aussi connus comme commutateurs LAN, remplacent les concentrateurs et fonctionnent avec les infrastructures de câblage existantes.
Aujourd'hui, dans le domaine des communications de données, tout l'équipement de commutation et de routage effectue deux activités de base :
1- la commutation de trames de données : Il s'agit d'une activité de stockage et de retransmission selon laquelle une trame arrive à un média d'entrée pour être ensuite transmise à un média de sortie.
2- maintenance des activités de commutation : Les commutateurs créent et gardent à jour des tables de commutation et cherchent des boucles. Les routeurs créent et gardent à jour des tables de routage et des tables de service.

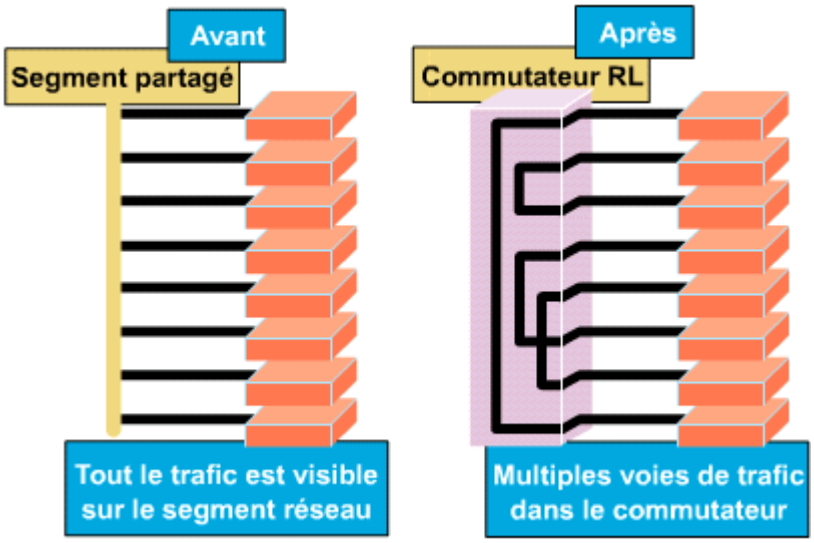


Tout comme les ponts, les commutateurs connectent des segments de réseau local, utilisent une table d'adresses MAC pour déterminer sur quel segment la trame doit être transmise et réduisent le volume de trafic. Les commutateurs fonctionnent à des vitesses plus élevées que celles des ponts.
Un commutateur Ethernet offre plusieurs avantages tels que permettre à de nombreux utilisateurs de communiquer en parallèle, grâce à l'utilisation de circuits virtuels et de segments de réseau spécialisés, dans un environnement libre de collisions. Cela maximise la largeur de bande disponible sur le média partagé. Un autre avantage : il est très rentable de passer à un environnement réseau local commuté, car il est possible de réutiliser le matériel et le câblage existants. Enfin, les administrateurs réseau ont une grande souplesse pour gérer le réseau grâce au commutateur et au logiciel utilisé pour configurer le réseau local.



4.4 Fonctionnement d'un commutateur de couche 2

Les commutateurs de réseau local sont considérés comme des ponts multiports sans domaine de collision, en raison de la microsegmentation (figure***). Les données sont échangées à haute vitesse en commutant le paquet vers sa destination. En lisant l'information de l'adresse MAC de destination de couche 2, les commutateurs peuvent atteindre de hauts débits de transferts de données, un peu à la manière des ponts. Le paquet est envoyé au port de la station réceptrice avant que tout le paquet entre dans le commutateur. Cela entraîne de bas niveaux de latence et une grande vitesse d'acheminement des paquets.
La commutation Ethernet augmente la largeur de bande disponible sur un réseau. Elle le fait en créant des segments de réseau spécialisés ou des connexions point à point et en connectant ces segments en un réseau virtuel à l'intérieur du commutateur. Ce circuit de réseau virtuel n'existe que lorsque deux nœuds ont besoin de communiquer. Cela s'appelle un *circuit virtuel*, car il n'existe qu'au besoin et qu'il est établi dans le commutateur même.
Bien que le commutateur de réseau local réduise la taille des domaines de collision, tous les hôtes connectés au commutateur continuent de faire partie du même domaine de diffusion; par conséquent, une diffusion provenant d'un nœud continuera d'être vue par tous les autres nœuds connectés au moyen du commutateur de réseau local.
Les commutateurs sont des unités de la couche liaison de données qui, comme les ponts, permettent à de multiples segments physiques d'un réseau local de s'interconnecter en un seul et unique réseau de plus grande envergure. Comme les ponts, les commutateurs acheminent et diffusent le trafic en fonction des adresses MAC. Puisque la commutation s'effectue au niveau matériel plutôt qu'au niveau logiciel, l'acheminement se fait beaucoup plus rapidement. Pensez à chaque port du commutateur en terme de micro-pont; ce processus s'appelle la *microsegmentation*. Ainsi, chaque port du commutateur agit comme un pont distinct et fournit la pleine largeur de bande du média à chaque hôte.



Microsegmentation

4.5 Segmentation de réseau local Ethernet

Deux raisons principales sont à la base de la segmentation d'un réseau local. Premièrement, pour isoler le trafic entre les segments et deuxièmement, pour obtenir une plus grande largeur de bande par utilisateur en créant de plus petits domaines de collision. Sans segmentation, les réseaux locaux plus étendus qu'un petit groupe de travail seraient vite submergés de trafic et de collisions et n'offriraient pratiquement aucune largeur de bande. L'ajout d'unités telles que des ponts, des commutateurs et des routeurs, segmente le réseau local.
En divisant les grands réseaux en unités autonomes, les ponts et commutateurs confèrent plusieurs avantages. 3Un pont ou un commutateur diminue le trafic reçu par les unités sur tous les segments connectés, parce que seulement un certain pourcentage du trafic est acheminé. Ces deux dispositifs agissent comme *pare-feu* dans le cas de certaines erreurs susceptibles d'endommager le réseau. Ils établissent aussi la communication entre un nombre d'unités supérieur à celui qui serait supporté sur n'importe quel réseau local connecté au pont. Les ponts et commutateurs étendent la longueur effective d'un réseau local, permettant la connexion de stations éloignées qui n'étaient pas acceptées auparavant.
Bien que les ponts et commutateurs partagent des attributs très pertinents, il y a encore plusieurs aspects qui les distinguent. En effet, les commutateurs sont beaucoup plus rapides parce qu'ils effectuent la commutation au niveau du matériel, tandis que les ponts effectuent la commutation au niveau du logiciel et peuvent interconnecter des réseaux locaux de largeurs de bande différentes. Il est possible de connecter un réseau local Ethernet 10 Mbits/s et un réseau local Ethernet 100 Mbits/s en utilisant un commutateur. Les commutateurs peuvent supporter de plus grandes densités de port que les ponts. Certains commutateurs supportent la commutation "cut-through", ce qui permet de réduire le temps de latence et les retards sur le réseau, tandis que les ponts ne prennent en charge qu'une commutation en différé (store-and-forward). Enfin, les commutateurs réduisent le nombre de collisions et augmentent la largeur de bande sur les segments de réseau parce qu'ils offrent une largeur de bande réservée à chacun des segments de réseau.

4.6 Segmentation d'un domaine de collision par des commutateurs

Un réseau local qui utilise une topologie Ethernet commutée crée un réseau qui fonctionne comme s'il n'avait que deux nœuds– le nœud émetteur et le nœud récepteur. Ces deux nœuds partagent une bande passante de 10 Mbits/s, ce qui veut dire que la presque totalité de la largeur de bande est disponible pour la transmission des données. Un réseau local Ethernet commuté permet à une topologie de réseau local de travailler plus rapidement et de façon plus efficace qu'un réseau local Ethernet standard, car il utilise efficacement la largeur de bande. Dans une mise en œuvre Ethernet commutée, la largeur de bande disponible peut atteindre près de 100 %.
Il est important de noter que même si l'ensemble de la largeur de bande est disponible, les réseaux Ethernet fonctionnent de manière optimale lorsqu'ils sont utilisés à 30 ou 40 % de leur capacité globale. Cette limite est attribuable à la méthode de détection de porteuse avec accès multiple (CSMA/CD) d'Ethernet. L'utilisation de la largeur de bande au-delà de la limite recommandée accroît le nombre de collisions. Le but de la commutation sur réseau local est d'alléger les contraintes de largeur de bande et de réduire les goulots d'étranglement sur le réseau, tels que ceux qui se produisent entre un groupe de PC et un serveur de fichiers éloigné. Un commutateur de réseau local est un pont multiport haute vitesse muni d'un port pour chaque nœud ou segment du réseau local. Un commutateur divise un réseau local en micro-segments, créant ainsi des domaines libres de collisions à partir d'un domaine de collision plus grand.
Un réseau Ethernet commuté a pour base un réseau Ethernet standard. Chaque nœud est directement connecté à l'un de ses ports ou à un segment qui est connecté à l'un des ports du commutateur. Cela crée une connexion à 10 Mbits/s entre chaque nœud et chaque segment du commutateur. Un ordinateur relié directement à un commutateur Ethernet constitue son propre domaine de collision et peut tirer parti de la totalité des 10 Mbits/s. Lorsqu'une trame entre dans un commutateur, celui-ci la lit pour connaître l'adresse source ou de destination. Le commutateur détermine ensuite l'action de commutation qui s'ensuivra, en fonction de l'information recueillie sur la trame. Si l'adresse de destination se trouve sur un autre segment, la trame est ensuite commutée à destination.

Chapitre 5
Couche 3 Routage et adressage

1 L'importance de la couche réseau

1.1 Identificateurs

La couche réseau assure le transport des données parmi un ensemble de réseaux (*interréseau*). Les unités utilisent le système d'adressage de la couche réseau pour déterminer la destination des données pendant leur acheminement.
Les protocoles sans couche réseau ne conviennent qu'aux petits réseaux internes. Ces protocoles n'utilisent généralement qu'un nom (l'adresse MAC) pour identifier les ordinateurs d'un réseau. Le défaut de cette méthode est qu'il devient de plus en plus difficile de gérer les noms à mesure que le réseau grandit, en particulier de s'assurer que tous les noms sont uniques.
Les protocoles qui supportent la couche réseau utilisent une technique d'identification des unités qui garantit l'unicité des désignations. Alors en quoi cet identificateur diffère-t-il d'une adresse MAC qui, elle aussi, est unique? Les adresses MAC utilisent un système d'adressage linéaire qui rend difficile la localisation des unités dans d'autres réseaux. Les adresses de couche réseau utilisent un système d'adressage hiérarchique qui garantit des adresses uniques au-delà des limites du réseau, ainsi qu'une méthode de sélection de la voie d'acheminement des données entre les réseaux.
L'adressage hiérarchique permet aux données de circuler dans des réseaux multiples et de trouver leur destination de manière efficace. Le système téléphonique est un exemple de système d'adressage hiérarchique. Le système téléphonique utilise un indicatif régional pour diriger un appel vers son premier relais (*saut*). Les trois chiffres suivants représentent le central téléphonique local (deuxième saut). Les quatre derniers chiffres sont le numéro de l'abonné demandé (dernier saut, jusqu'à la destination).
Les unités d'un réseau ont besoin d'un système d'adressage cohérent leur permettant d'acheminer des paquets d'un réseau à un autre dans le cadre de l'interréseau (ensemble de réseaux segmentés ou non, utilisant le même système d'adressage). Les unités utilisent le système d'adressage de la couche réseau pour déterminer la destination des données tout au long de leur cheminement dans l'interréseau.

1.2 Segmentation et systèmes autonomes

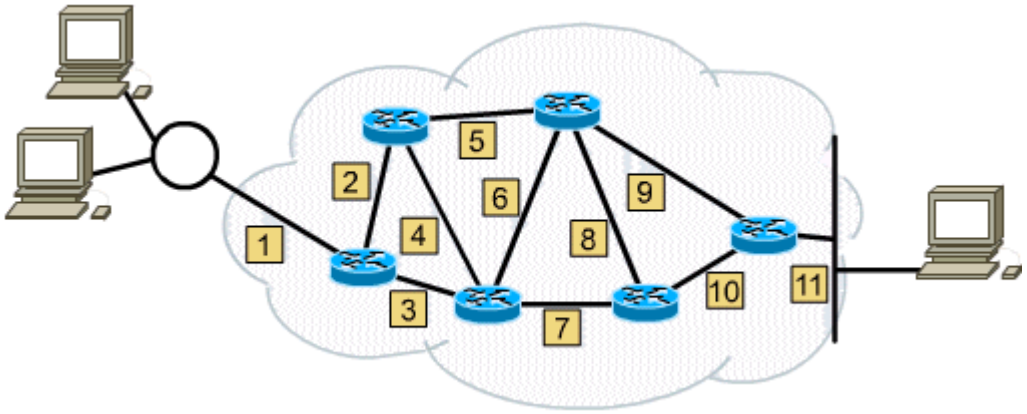
La multiplication des réseaux résulte de deux tendances fondamentales : l'augmentation de la taille de chaque réseau et la création constante de nouveaux réseaux.
Lorsqu'un réseau local, un réseau métropolitain ou un réseau longue distance prend de l'expansion, il devient nécessaire - pour des raisons pratiques de gestion du trafic - de le subdiviser en réseaux plus petits appelés *segments réseau* (ou simplement *segments*). Notre grand réseau devient donc une mosaïque de réseaux plus petits dont chacun a besoin d'une adresse distincte.
Il existe déjà un grand nombre de réseaux; des réseaux privés sont répandus dans les bureaux, les écoles, les entreprises et les organisations gouvernementales. Tous ces réseaux distincts (ou systèmes autonomes s'ils sont gérés par un seul administrateur réseau) souhaitent communiquer par l'entremise d'Internet, mais leur interconnexion exige des systèmes d'adressage efficaces et des interfaces appropriées. Si ce n'est pas le cas, il se produira des embouteillages affectant le fonctionnement des réseaux locaux et aussi celui d'Internet.
Pour comprendre la nécessité de la segmentation des réseaux, pensez à un réseau routier et aux véhicules qui y circulent. À mesure que la population des communautés desservies augmente, les routes deviennent de plus en plus encombrées par un nombre croissant de véhicules. Les réseaux fonctionnent de manière très semblable. À mesure que les réseaux s'étendent, le trafic augmente. Comme première solution, on peut augmenter la largeur de bande, ce qui équivaut à élever la limite de vitesse ou à ajouter des voies sur les autoroutes. Une autre solution consiste à utiliser des unités de régulation pour segmenter le réseau et gérer le trafic, de la même façon qu'on utilise les feux de circulation pour régulariser le trafic routier.

1.3 Les communications entre réseaux

Internet est un ensemble de segments de réseaux interconnectés pour faciliter les échanges d'information. Une fois de plus, l'analogie avec le réseau routier est valable avec ses autoroutes à voies multiples servant à relier rapidement les grandes régions géographiques.
Les réseaux fonctionnent de façon très semblable grâce à l'apparition de compagnies appelées *fournisseurs de services Internet* (*FSI*), qui offrent des services d'interconnexion aux propriétaires de réseaux autonomes.

1.4 Unités réseau de la couche 3

Les unités d'interconnexion de réseaux qui appartiennent à la couche 3 (couche réseau) du modèle OSI relient des segments de réseau ou des réseaux entiers. Ces unités s'appellent des routeurs. Leur rôle consiste à acheminer les paquets de données entre les réseaux en fonction de l'information du protocole réseau de la couche 3.



Les routeurs prennent des décisions logiques d'optimisation pour choisir la meilleure voie d'acheminement des données d'un réseau à un autre et dirigent ensuite les paquets vers le port de sortie qui correspond au segment de réseau suivant. Le routeur reçoit des paquets de données des unités (postes de travail, etc.) d'un réseau local et, en fonction de l'information de couche 3, les achemine dans l'interréseau. Le routage est parfois appelé commutation de couche 3.

2 La sélection de la voie

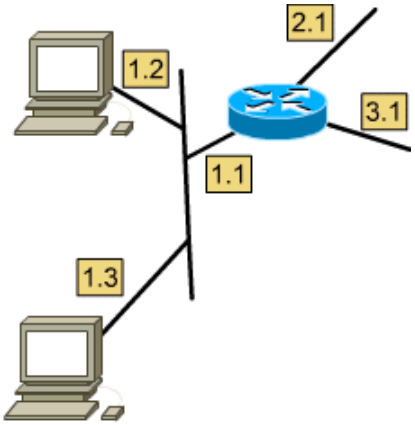
2.1 Sélection de la voie

La *sélection de la voie* se fait au niveau de la couche 3 (couche réseau); elle permet au routeur d'évaluer l'état des circuits menant à une certaine destination et d'établir la voie optimale pour un paquet particulier. Les services de routage utilisent l'information de topologie du réseau dans l'évaluation des voies. La sélection de la voie est le processus que le routeur utilise pour choisir le prochain saut du trajet que le paquet empruntera vers sa destination. Ce processus est également appelé le *routage du paquet*.
La sélection de la voie pour un paquet peut être comparée au cheminement d'un automobiliste qui traverse une ville. Il dispose d'un plan montrant tous les itinéraires qui lui permettent de se rendre à destination. Le trajet d'une intersection à la suivante est un "saut". De même, le routeur utilise un "plan" qui présente toutes les voies possibles vers une destination donnée.
Les routeurs prennent aussi des décisions en fonction de la densité du trafic et du débit des liaisons (bande passante), tout comme notre automobiliste peut choisir une voie rapide (une autoroute) ou des rues secondaires moins achalandées.

2.2 Adressage de couche réseau

L'adresse réseau permet au routeur de choisir une voie optimale au sein du réseau. Le routeur utilise les adresses réseau pour identifier le réseau de destination d'un paquet à l'intérieur d'un interréseau.
Dans certains protocoles de couche réseau, l'administrateur du réseau attribue les adresses réseau en fonction d'un plan d'adressage interréseau prédéterminé. Dans d'autres protocoles de couche réseau, l'attribution d'adresses est effectuée partiellement ou entièrement de façon dynamique ou automatique. En plus des adresses réseau, les protocoles réseau utilisent une forme quelconque d'adresse de l'hôte ou du nœud. Le schéma illustre trois unités du réseau 1 (deux postes de travail et un routeur), chacun ayant sa propre adresse d'hôte (on voit également que le routeur est relié à deux autres réseaux : les réseaux 2 et 3).

Réseau	Hôte
1	1
	2
	3
2	1
3	1



L'adressage est effectué par la couche réseau. Dans l'analogie du numéro de téléphone utilisée pour décrire une adresse réseau, les premières parties (indicatif régional et numéro de central) constituaient l'adresse du central de rattachement du destinataire. Les quatre derniers chiffres, indiquant au commutateur local à quelle ligne de téléphone il doit acheminer l'appel, correspondent à la partie hôte de l'adresse, qui précise l'identité du dispositif de destination.
Sans adressage de couche réseau, le routage devient impossible. Les routeurs ont besoin de l'adresse réseau pour assurer la livraison sans erreur des paquets. Sans une forme quelconque de structure d'adressage hiérarchique, il serait impossible d'acheminer les paquets au sein d'un interréseau. D'une manière analogue, sans structure hiérarchique pour les numéros de téléphone, les adresses postales ou les systèmes de transport, la livraison des biens et des services serait infiniment plus complexe.

2.3 Couche 3 et mobilité de l'ordinateur

L'adresse MAC est comme le nom d'une personne; son adresse réseau est comme son adresse postale. Lorsqu'une personne déménage dans une autre ville, elle conserve son nom, mais son adresse postale indique son nouvel emplacement. Les unités réseau (tant les routeurs que les ordinateurs individuels) sont dotées d'une adresse MAC et d'une adresse de protocole (couche réseau). Si un ordinateur est déplacé physiquement à un réseau différent, il conserve son adresse MAC, mais une nouvelle adresse réseau doit lui être attribuée.

2.4 Comparaison de l'adressage linéaire et de l'adressage hiérarchique

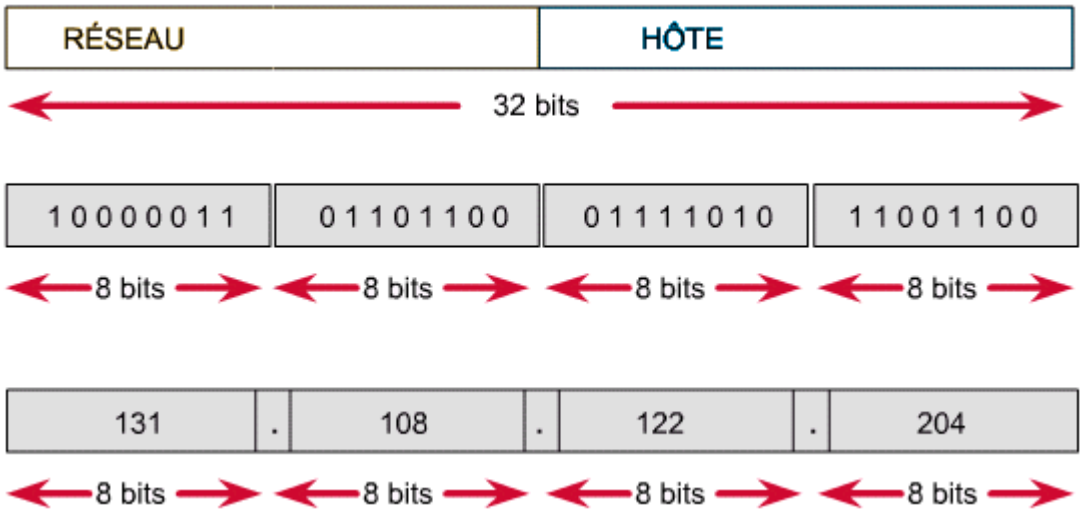
Le rôle de la couche réseau est de trouver la meilleure voie au sein d'un réseau. Pour ce faire, elle utilise deux méthodes d'adressage : l'adressage linéaire et l'adressage hiérarchique. Un système d'*adressage linéaire* attribue à une unité la prochaine adresse disponible. Aucune importance n'est accordée à la structure du système d'adressage. Les numéros d'assurance sociale ou de certificats de naissance sont des exemples de systèmes d'adressage linéaire. Les adresses MAC fonctionnent de cette manière. Un fournisseur reçoit un bloc d'adresses; la première portion de chaque adresse représente le code du fournisseur, le reste de l'adresse MAC est un numéro aléatoire attribué selon un système de numérotation séquentiel.

Dans un système d'*adressage hiérarchique*, comme celui que le système des postes utilise pour les codes postaux, l'adresse est déterminée par l'emplacement de la maison et non par un numéro attribué au hasard. Le système d'adressage que vous utiliserez tout au long de ce programme d'études est l'adressage du protocole Internet (IP). Les adresses IP ont une structure spécifique et elles ne sont pas attribuées de manière aléatoire.

3 Les adresses IP dans l'en-tête IP

3.1 Datagrammes de couche réseau

Le protocole Internet (IP) est la méthode d'adressage privilégiée des réseaux hiérarchiques. Le protocole IP est le protocole réseau d'Internet. À mesure que les données circulent vers le bas du modèle OSI, les données sont encapsulées à chaque couche. À la couche réseau, les données sont encapsulées dans des paquets (aussi appelés datagrammes). Le protocole IP détermine le format de l'en-tête IP (qui comprend l'information d'adressage et de contrôle), mais ne se préoccupe pas des données proprement dites; il accepte tout ce qui provient des couches supérieures.



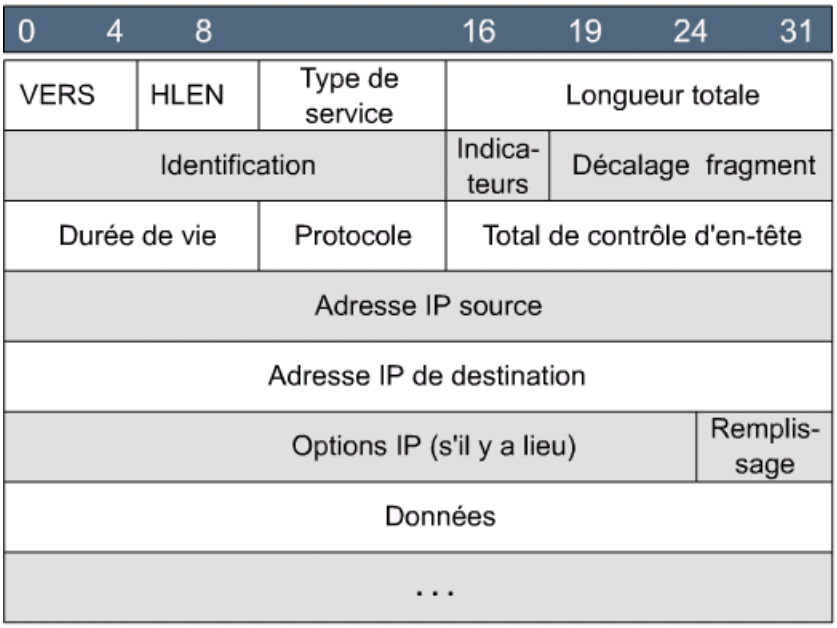
Structure d'une adresse IP

3.2 Champs de couche réseau

Le paquet ou datagramme de couche 3 devient les données de la couche 2, qui sont ensuite encapsulées en trames (comme nous l'avons déjà mentionné). De même, le paquet IP est composé des données des couches supérieures plus un en-tête IP constitué des éléments suivants :

- *version* - indique la version de protocole IP utilisée (4 bits)
- *HLEN (IP header length)* - indique la longueur de l'en-tête du datagramme en mots de 32 bits (4 bits)
- *type de service* - indique l'importance qui lui a été accordé par un protocole de couche supérieure donné (8 bits)
- *longueur totale* - précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits)
- *identification* - contient un nombre entier qui identifie le datagramme actuel (16 bits)
- *indicateurs* - un champ de 3 bits dont les 2 bits inférieurs contrôlent la fragmentation – un bit précise si le paquet peut être fragmenté et le second indique si le paquet est le dernier fragment d'une série de paquets fragmentés (3 bits)
- *décalage de fragment* - ce champ sert à rassembler les fragments du datagramme (16 bits)
- *durée de vie minimum* - un compteur qui décroît graduellement, par incréments, jusqu'à zéro. À ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle (8 bits)
- *protocole* - précise le protocole de couche supérieure qui recevra les paquets entrants après la fin du traitement IP (8 bits)
- *total de contrôle d'en-tête* - assure l'intégrité de l'en-tête IP (16 bits)

- *adresse source* - précise le nœud émetteur (32 bits)
- *adresse de destination* - précise le nœud récepteur (32 bits)
- *options* - permet au protocole IP de supporter différentes options, telle la sécurité (longueur variable)
- *données* - contient de l'information de couche supérieure (longueur variable, maximum 64 Ko)
- *remplissage* - des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits



3.3 Champs source et de destination de l'en-tête IP

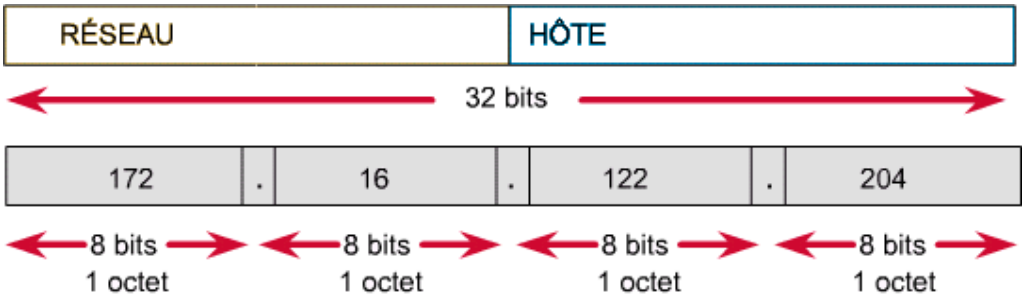
L'adresse IP contient l'information nécessaire pour le routage d'un paquet au sein du réseau. Chaque champ d'adresse source et de destination contient une adresse de 32 bits. Le champ d'adresse source contient l'adresse IP de l'unité qui envoie le paquet. Le champ de destination contient l'adresse IP de l'unité qui reçoit le paquet.

3.4 Adresse IP comme nombre binaire 32 bits

Une adresse IP est représentée par un nombre binaire de 32 bits. Rappelez-vous que les chiffres binaires ne sont composés que de deux valeurs, 0 et 1. Dans un nombre *binaire*, la valeur du bit à l'extrême droite (bit le moins significatif) est soit 0 ou 1. La valeur décimale correspondant à chaque bit d'un nombre binaire double chaque fois que vous vous déplacez d'une position vers la gauche. Ainsi, la valeur décimale du deuxième bit à partir de la droite est soit 0 ou 2. Le troisième bit est soit 0 ou 4; le quatrième, 0 ou 8, etc.
Les adresses IP sont présentées en format décimal 32 bits. Les 32 bits de l'adresse sont subdivisées en quatre *octets* (un octet est un groupe de 8 bits). La valeur décimale maximale d'un octet est de 255 (le plus grand nombre binaire de huit bits est 11111111 et ces bits, de droite à gauche, ont des valeurs décimales de 1, 2, 4, 8, 16, 32, 64 et 128 pour un total de 255).
Quelle est la valeur décimale de l'octet mis en évidence dans le schéma? Quelle la valeur du bit à l'extrême gauche? Celle du bit suivant? Puisque seuls ces deux bits sont activés (réglés à 1), la valeur décimale du nombre est 128+64=192!

3.5 Champs de l'adresse IP

Le numéro de réseau d'une adresse IP précise le réseau auquel une unité est connectée alors que la portion hôte d'une adresse IP pointe au dispositif spécifique au sein de ce réseau. Puisque les adresses IP sont composées de quatre octets séparés par des points, un, deux ou trois de ces octets peuvent servir à déterminer le numéro de réseau. De même, un, deux ou trois de ces octets peuvent servir à déterminer la partie hôte d'une adresse IP.



4 Les classes d'adresses IP

4.1 Classes d'adresses IP

Un organisme peut recevoir trois classes d'adresses IP de l'ARIN (ou de son fournisseur de services Internet). Il s'agit des classes A, B et C. L'ARIN réserve maintenant les adresses de classe A aux gouvernements de par le monde (bien que certaines grandes entreprises, telles que Hewlett Packard, en ont déjà reçues) et les adresses de classe B aux entreprises de taille moyenne. Tous les autres demandeurs reçoivent des adresses de classe C.

Classe A

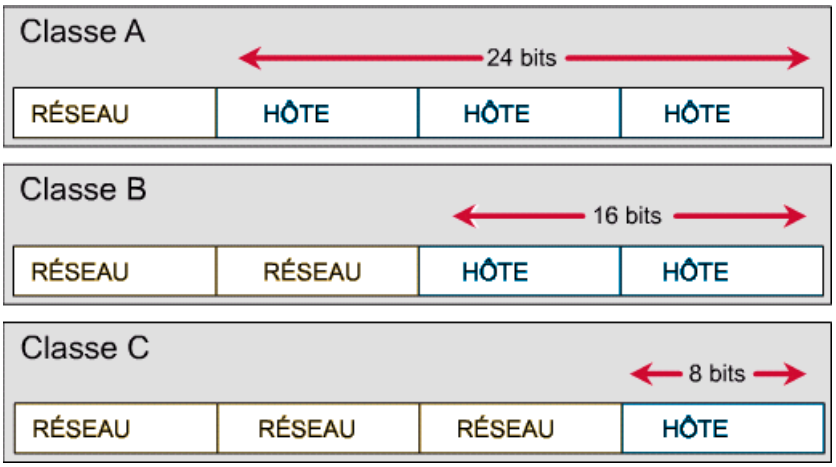
En format binaire, le premier bit (à l'extrême gauche) d'une adresse de classe A est toujours 0. Un exemple d'adresse IP de classe A serait 124.95.44.15. Le premier octet, 124, représente le numéro de réseau attribué par l'ARIN. Les administrateurs internes du réseau attribuent les valeurs des 24 bits qui restent. Pour déterminer si une unité fait partie d'un réseau de classe A, il suffit de regarder le premier octet de son adresse IP, qui variera entre 0 et 126. (127 *commence* avec un bit à 0, mais cette valeur est réservée à des fins particulières).

Toutes les adresses IP de classe A n'utilisent que les huit premiers bits pour indiquer la partie réseau de l'adresse. Les trois octets restants peuvent servir pour la portion hôte de l'adresse. Les réseaux qui utilisent un système d'adressage IP de classe A peuvent attribuer jusqu'à 2 à la 24 (2^{24}) (moins 2) ou 16 777 214 adresses IP aux unités qui en font partie.

Classe B

Les deux premiers bits d'une adresse de classe B sont toujours 10 (un et zéro). Un exemple d'adresse IP de classe B serait 151.10.13.28. Les deux premiers octets représentent le numéro de réseau attribué par l'ARIN. Les administrateurs internes du réseau attribuent les valeurs des 16 bits qui restent. Pour déterminer si une unité fait partie d'un réseau de classe B, il suffit de regarder le premier octet de son adresse IP. La valeur du premier octet des adresses IP de classe B varie entre 128 et 191.

Toutes les adresses IP de classe B utilisent les 16 premiers bits pour indiquer la partie réseau de l'adresse. Les deux octets restants de l'adresse IP sont réservés à la portion hôte de l'adresse. Les réseaux qui utilisent un système d'adressage IP de classe B peuvent attribuer jusqu'à 2 à la 16 (2^{16}) (moins 2 encore!) ou 65 534 adresses IP aux unités qui en font partie.



Classe C
Les trois premiers bits d'une adresse de classe C sont toujours 110 (un, un et zéro). Un exemple d'adresse IP de classe C serait 201.110.213.28. Les trois premiers octets représentent le numéro de réseau attribué par l'ARIN. Les administrateurs internes du réseau attribuent les valeurs des 8 bits qui restent. Pour déterminer si une unité fait partie d'un réseau de classe C, il suffit de regarder le premier octet de son adresse IP. La valeur du premier octet des adresses IP de classe C varie entre 192 et 223.
Toutes les adresses IP de classe C utilisent les 24 premiers bits pour indiquer la partie réseau de l'adresse. Seul le dernier octet d'une adresse IP de classe C est réservé à la portion hôte de l'adresse. Les réseaux qui utilisent un système d'adressage IP de classe C peuvent attribuer jusqu'à 2^8 (moins 2) ou 254 adresses IP aux unités qui en font partie.

4.2 Adresses IP exprimées en nombres décimaux

Les adresses IP identifient les unités d'un réseau, ainsi que le réseau auquel elles sont connectées. Pour faciliter leur mémorisation, les adresses IP sont généralement exprimées en *notation décimale* (quatre nombre décimaux séparés par des points, 166.122.23.130, par exemple - rappelez-vous qu'un nombre décimal est un nombre en base 10, le système de numération que nous utilisons quotidiennement).

5 L'espace adresse réservé

5.1 Buts des ID réseau et des adresses de diffusion

Si votre ordinateur voulait communiquer avec toutes les unités d'un réseau, il serait difficile de lister les adresses IP de chacune de ces unités. Vous pourriez préciser deux adresses séparées par un tiret pour représenter toutes les unités au sein de cette plage de nombres, mais cette solution n'est guère plus pratique. Il existe, toutefois, une méthode plus efficace.
Une adresse IP dont tous les bits hôte sont occupés par des zéros binaires est réservée à l'adresse réseau (parfois appelée *adresse de fil*). Ainsi, dans un réseau de classe A, 113.0.0.0 est l'adresse IP du réseau comprenant l'hôte 113.1.2.3. Un routeur utilise l'adresse IP d'un réseau pour acheminer des données sur Internet. Dans un réseau de classe B, l'adresse IP 176.10.0.0 est une adresse de réseau.
Les nombres décimaux qui composent les deux premiers octets d'une adresse de réseau de classe B sont attribués et représentent les numéros de réseau. Les deux derniers octets contiennent des 0, parce que ces 16 bits sont des numéros d'hôte et sont réservés aux unités qui sont connectées au réseau. L'adresse IP de notre exemple (176.10.0.0) est réservée à l'adresse de réseau. Elle ne sera jamais utilisée comme adresse pour une unité connectée au réseau.
Pour envoyer des données à toutes les unités d'un réseau, il vous faudrait utiliser une *adresse de diffusion*. Une diffusion se produit lorsqu'une source envoie des données à toutes les unités d'un réseau. Pour s'assurer que toutes les unités d'un réseau tiennent compte d'un tel message de diffusion, la source doit utiliser une adresse IP que toutes les unités peuvent reconnaître et recevoir. Les adresses de diffusion IP se terminent par des 1 binaires dans toute la portion hôte de l'adresse (le *champ hôte*).
Dans le cas du réseau cité en exemple (176.10.0.0), dans lequel les 16 derniers bits constituent le champ hôte (ou portion hôte de l'adresse), le message de diffusion envoyé à toutes les unités du réseau comprendrait l'adresse de destination 176.10.255.255 (puisque 255 est la valeur décimale de l'octet binaire 11111111).

5.2 ID réseau

Il est essentiel de comprendre l'importance de la portion réseau d'une adresse IP - l'*ID réseau*. Les hôtes d'un réseau ne peuvent communiquer directement qu'avec les unités qui partagent la même ID réseau. Ils peuvent partager le même segment physique, mais s'ils ont des numéros de réseau différents, la communication entre eux est habituellement impossible, à moins qu'une autre unité puisse établir la connexion entre les réseaux.

5.3 Analogie pour les ID réseau

Les codes postaux et les ID réseau fonctionnent de façon très semblable. Les codes postaux permettent au système des postes d'acheminer votre courrier à votre bureau de poste local, et ensuite, à votre quartier. De là, l'adresse postale permet au facteur de déposer votre courrier dans votre boîte aux lettres. Alors que l'ID réseau permet à un routeur de mettre un paquet dans le bon segment de réseau, l'ID hôte aide le routeur à acheminer la trame de couche 2 (en encapsulant le paquet) à l'hôte de destination précis au sein de ce réseau.

Le modèle de référence TCP/IP

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le *protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol).* Le *modèle de référence TCP/IP* et la *pile de protocoles TCP/IP* rendent possible l'échange de données entre deux ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière. Le modèle TCP/IP présente une importance historique tout comme les normes qui ont permis l'essor des industries du téléphone, de l'électricité, du chemin de fer, de la télévision et de la bande vidéo.

1. Les couches du modèle de référence TCP/IP

Le ministère américain de la Défense a créé le modèle de référence TCP/IP parce qu'il avait besoin d'un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire. Imaginez en effet un monde en guerre, quadrillé de connexions de toutes sortes - fils, micro-ondes, fibres optiques et liaisons satellites. Imaginez ensuite que vous ayez besoin de faire circuler l'information/les données (sous forme de paquets), peu importe la situation d'un nœud ou d'un réseau particulier de l'interréseau (qui pourrait avoir été détruit par la guerre). Le ministère de la Défense veut que ses paquets se rendent chaque fois d'un point quelconque à tout autre point, peu importe les conditions. C'est ce problème de conception très épineux qui a mené à la création du modèle TCP/IP, qui, depuis lors, est devenu la norme sur laquelle repose Internet.

Lors de vos lectures sur les couches du modèle TCP/IP, gardez à l'esprit le but initial d'Internet, cela vous aidera à comprendre pourquoi certaines choses sont ainsi. Le modèle TCP/IP comporte quatre couches : la couche application, la couche de transport, la couche *Internet* et la couche d'accès réseau. Remarquez que certaines couches du modèle TCP/IP portent le même nom que des couches du modèle OSI. Il ne faut pas confondre les couches des deux modèles, car la couche application comporte des fonctions différentes dans chaque modèle.

La couche application

Les concepteurs de TCP/IP estimaient que les protocoles de niveau supérieur devaient inclure les détails des couches session et présentation. Ils ont donc simplement créé une couche application qui gère les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

La couche de transport

La couche de transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (Transmission Control Protocol - protocole de contrôle de transmission), fournit d'excellentes façons de créer en souplesse des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé. Le protocole TCP est orienté connexion. Il établit un dialogue entre l'ordinateur source et l'ordinateur de destination pendant qu'il prépare l'information de couche application en unités appelées segments. Un

protocole orienté connexion ne signifie pas qu'il existe un circuit entre les ordinateurs en communication (ce qui correspondrait à la commutation de circuits). Ce type de fonctionnement indique qu'il y a un échange de segments de couche 4 entre les deux ordinateurs hôtes afin de confirmer l'existence logique de la connexion pendant un certain temps. C'est ce qu'on appelle la commutation de paquets.

La couche Internet

Le rôle de la *couche Internet* consiste à envoyer des paquets source à partir d'un réseau quelconque de l'interréseau et à les acheminer à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche s'appelle IP (Internet Protocol - protocole Internet). L'identification du meilleur trajet et la commutation de paquets ont lieu à cette couche. Pensez au système postal. Lorsque vous postez une lettre, vous ne savez pas comment elle arrive à destination (il existe plusieurs routes possibles), tout ce qui vous importe c'est qu'elle se rende.

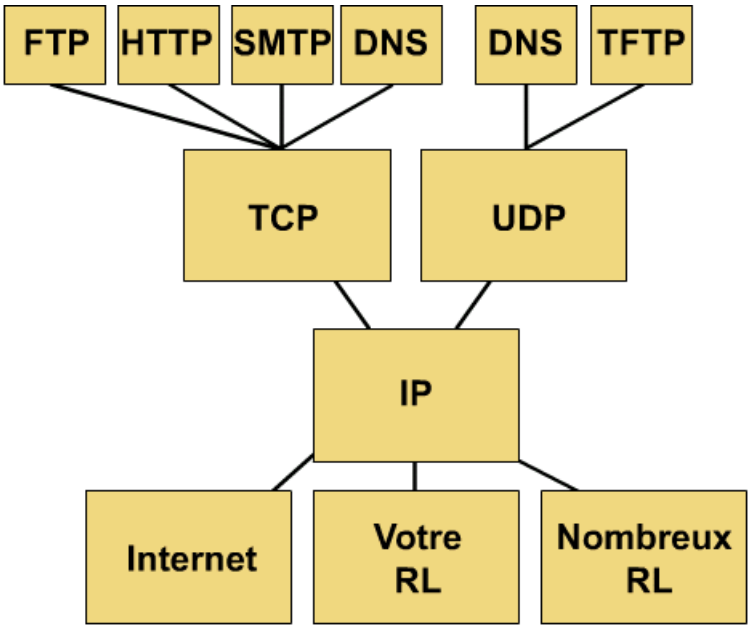
La couche d'accès réseau

Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On l'appelle également la couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies de réseau local et de réseau longue distance, ainsi que tous les détails dans les couches physique et liaison de données du modèle OSI.

2. Schéma de protocoles TCP/IP

Le diagramme illustré dans la figure s'appelle un *schéma de protocoles*. Il présente certains protocoles communs spécifiés par le modèle de référence TCP/IP. À la couche application, vous ne reconnaîtrez peut-être pas certaines tâches réseau, mais vous les utilisez probablement tous les jours en tant qu'internaute. Vous étudierez chacune de ces tâches dans le cadre du programme d'études. Ces applications sont les suivantes :

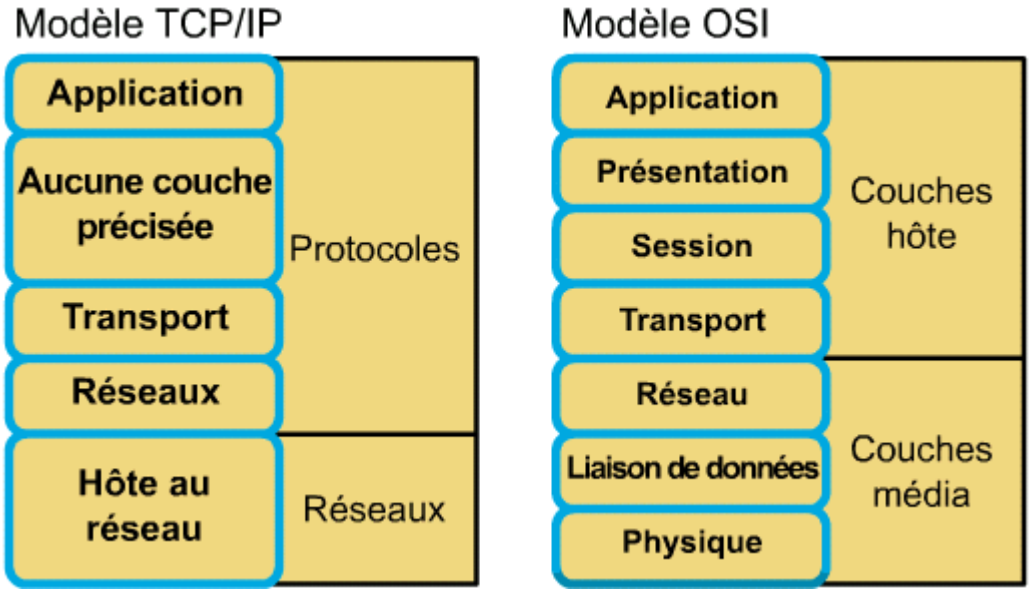
- *FTP* - Protocole de transfert de fichiers ou protocole FTP
- *HTTP* - Protocole HTTP (Hypertext Transfer Protocol)
- *SMTP* - Protocole SMTP (Simple Mail Transport protocol)
- *DNS* - Système DNS (Domain Name Service)
- *TFTP* - Protocole TFTP (Trivial File Transport Protocol)



Le modèle TCP/IP met l'accent sur une souplesse maximale, à la couche application, à l'intention des développeurs de logiciels. La couche de transport fait appel à deux protocoles - le protocole TCP (protocole de contrôle de transmission) et le *protocole UDP (protocole de datagramme utilisateur)*. Vous approfondirez ces protocoles plus tard au cours du programme. La couche inférieure, soit la couche réseau, se rapporte à la technologie de réseau local ou de réseau longue distance utilisée .
Dans le modèle TCP/IP, peu importe l'application qui demande des services réseau et le protocole de transport utilisé, il n'y a qu'un seul protocole réseau : IP (Internet Protocol). C'est une décision de conception délibérée. *IP* est le protocole universel qui permet à un ordinateur quelconque de communiquer en tout temps.

3. Comparaison du modèle OSI et du modèle TCP/IP

En comparant le modèle OSI au modèle TCP/IP, vous remarquerez des similitudes et des différences. Voici des exemples :



Similitudes

- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services très différents.
- Tous deux comportent des couches réseau et transport comparables.
- Tous deux supposent la technologie de commutation de paquets (et non de commutation de circuits).
- Les professionnels du réseautage doivent connaître les deux modèles.

Différences

- TCP/IP intègre la couche de présentation et la couche session dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données OSI en une seule couche.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Les protocoles TCP/IP constituent la norme sur laquelle s'articule Internet, aussi le modèle TCP/IP a-t-il acquis sa crédibilité en raison de ses protocoles. Par contraste, aucun réseau ne s'articule sur des protocoles particuliers au modèle OSI, même si tous se servent du modèle OSI comme guide.

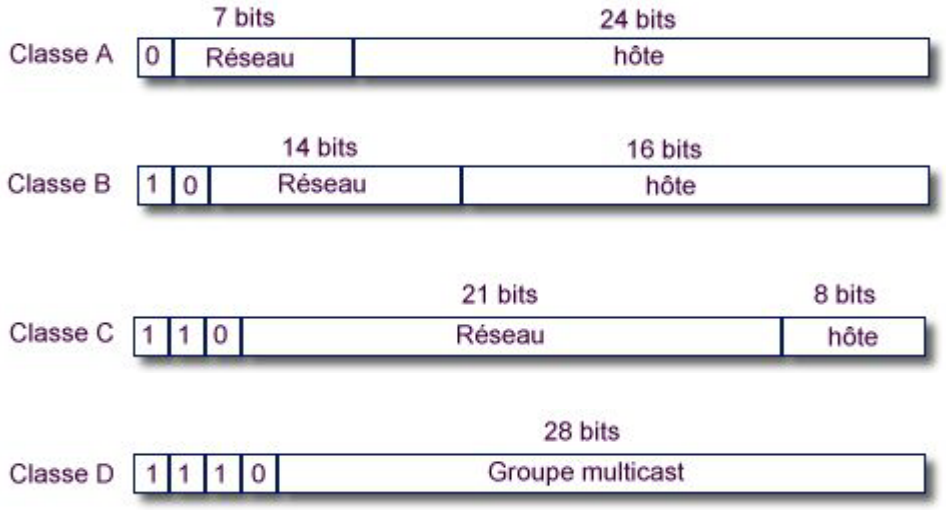
Subnetting TCP/IP

L'adressage IP :

Quand un ordinateur cherche a communiquer avec un autre ordinateur ou avec un périphérique réseau quelconque en utilisant le protocole TCP/IP, la procédure suivante se déroule :

1. Le nom de la machine est transformé en une adresse TCP/IP. Ceci est effectué par le resolver qui utilise un service de nommage (table hosts, DNS)..
2. Les routines des couches TCP/IP associent ce numéro et le masque de réseau pour déterminer si la machine à atteindre fait ou non partie de même réseau.
1. Si oui, l'adresse TCP/IP est résolue en une adresse Ethernet; une trame est alors formée avec cette dernière et est envoyée sur le réseau.
2. Sinon, et si il existe une table de routage, l'adresse ethernet du routeur est utilisée pour former une trame qui est envoyée sur le réseau (donc vers le routeur approprié).
3. Sinon, un message d'erreur est renvoyé vers le programme utilisateur (celui qui cherchait à envoyer des données). Ce message indique que l'adresse de la machine destinataire est impossible à joindre.

Pour réaliser le masquage, on utilise l'opération AND binaire. Tout d'abord, les différentes classes d'adresses utilisables peuvent être représentées comme suit; chaque adresse ayant une largeur totale de 4 octets, soit 32 bits (ici, seule les valeurs des bits de poids fort du premier octet sont détaillées) :



Si on somme bit à bit ces deux valeurs (opération 'OU binaire'), on obtient l'adresse du réseau qui est indispensable pour savoir comment expédier le paquet TCP/IP, c'est à dire : 12.0.0.0.

Autre exemple, si on a un réseau de classe B (sans sous-réseau), le masque est de 255.255.0.0. La machine dont l'adresse TCP/IP est 171.21.36.12 appartient au réseau 171.21.0.0 (AND binaire entre 171.21.36.12 et 255.255.0.0).

L'utilisation de TCP/IP oblige donc de choisir une classe d'adresse. Chaque classe proposée offre un compromis entre le nombre maximum de réseaux et le nombre de machines.

Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254
Classe D	224.x.x.x 239.x.x.x	N.A	N.A
Classe E	240.x.x.x 247.x.x.x	N.A	N.A

Les adresses de la classe D sont réservées au muticasting. Les adresses de la classe E sont réservées à un usage futur (...). Les seules classes vraiment utiles sont les classes A, B et C.

On le voit, plus le nombre de réseaux par classe est important, moins le nombre possible de machines est important.

Note : Dans la classe A, le réseau 127 tient une place à part. Conventionnellement, il désigne l'adresse de la machine (moi même) dans le contexte TCP/IP. La table « hosts » de toute machine comporte par exemple la mention "127.0.0.1 localhost". Tout autre numéro de ce réseau peut être utilisé pour cet usage.

On peut alors choisir, à partir du nombre de machines que l'on compte mettre en oeuvre, le type de classe le plus approprié.

Pour trouver à quelle classe appartient une machine donnée, il suffit de repérer la valeur du premier octet de l'adresse TCP/IP. L'adresse 174.23.2.45 est par exemple une adresse de classe B, car le premier octet, 174, est compris entre 128 et 191. L'adresse 5.6.7.8 est une adresse de classe A

Les adresses TCP/IP réservées ("privées").

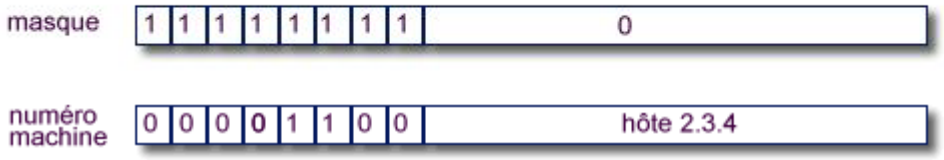
Il existe aussi, à l'intérieur de chaque classe, un sous-ensemble d'adresses qui sont destinées à un usage privé. Ce qui signifie que tout routeur du marché ne routera pas, par défaut, ces adresses sur Internet. Plusieurs réseaux locaux utilisent donc ces adresses pour leur usage interne. Il n'y a pas de conflit, puisque ce sont des réseaux privés dont les adresses ne sont pas accessibles depuis Internet. Ces adresses sont définies dans la RFC1918 :

1. pour la classe A les adresses 10.x.x.x
2. pour la classe B les adresses 172.16.x.x à 172.31.x.x
3. pour la classe B les adresses 192.168.x.x

Le masque de réseau.

Un masque réseau TCP/IP est un ensemble de 4 octets qui permet de distinguer, dans une adresse TCP/IP, la partie réseau de la partie machine.
Exemple : 184.23.3.67, masque 255.255.0.0; l'adresse de la machine est bien 184.23.3.67. Cette machine appartient au réseau 184.23.0.0.

Dans le cas d'une machine dont le numéro TCP/IP est 12.2.3.4 et le masque de 255.0.0.0, on a alors les valeurs de masque et d'adresse hôte ci-dessous :



Pourquoi un subnet sur un LAN ou WAN, MAN ?

Dans un réseau local Ethernet TCP/IP il peut y avoir des problèmes de charge de réseau qui apparaissent pour plusieurs raisons :

- diffusion trop importante (broadcast)
- trop grande quantité de machines sur un seul réseau logique d'ou un trafic trop important.

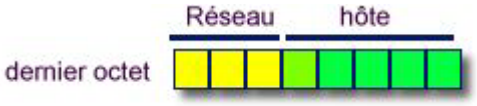
Dans un réseau local, par sécurité, on peut vouloir isoler certains utilisateurs de certaines ressources. Dans un réseau MAN ou WAN, les phénomènes de diffusion sont à éviter pour des problèmes de coût. Pour des questions de sécurité, il est préférable d'isoler certaines portions de réseau. Dans tout ces cas de figure, tout en gardant les mêmes adresses TCP/IP, le découpage en sous-réseaux (subnetting) associé à l'utilisation de routeurs peut être une solution.

La création d'un sous-réseau.

On comprend bien maintenant tout l'intérêt de diviser de grands réseaux en sous-réseaux plus faciles à gérer. Pour ce faire, l'espace d'adressage alloué va être re-découpé. Le (ou les) dernier(s) octet(s) va donc être utilisé pour "coder" un sous-réseau et une adresse de machine. Une contrainte va apparaître : chacun des sous-réseaux formé devra avoir une adresse de réseau et une adresse de diffusion (broadcast). Ces deux adresses ne pourront pas être allouées à des machines.

Raisonnons sur un exemple. L'espace d'adressage 204.34.57.0 de classe C nous a été allouée avec un masque de 255.255.255.0. Si on ne découpe pas en sous-réseaux, la totalité du dernier octet sert à numéroter les machines. Mais on désire créer des sous-réseaux. On va donc re-découper l'espace fourni par les 8 bits du dernier octet.

On peut par exemple allouer les bits de la façon suivante :



Les 3 bits de poids 32, 64 et 128 (jaunes) seront utilisés pour déterminer le sous-réseau et les 5 bits de poids 1, 2, 4, 8 et 16 (verts) pour définir les adresses des hôtes au sein des sous-réseaux. En groupant les bits de sous-réseau avec les bits de réseau, on va définir les sous réseaux suivants :

204.34.57.0 (bits de sous-réseau = 000)
204.34.57.32 (bits de sous réseau = 001)
204.34.57.64 (bits de sous-réseau = 010)
204.34.57.96 (bits de sous-réseau = 011)
204.34.57.128 (bits de sous-réseau = 100)
204.34.57.160 (bits de sous-réseau = 101)
204.34.57.192 (bits de sous-réseau = 110)
204.34.57.224 (bits de sous-réseau = 111)

Remarquez bien que l'on utilise les combinaisons 000 et 111 pour ces sous-réseaux. La RFC950 qui stipulait que la première et la dernière adresse d'un réseau ne devaient pas être utilisées, est maintenant obsolète. En effet, la plupart des routeurs modernes savent très bien gérer des adresses réseau dont tous les bits de sous-réseau sont à 1 ou à 0. Pour plus de précision, reportez-vous à la RFC1878 qui propose un découpage en sous-réseaux indépendant des classes (voir également CIDR ci-dessous). Cet aspect "sans classe" se retrouve sur certains routeurs ou l'on peut spéccifier 'ip classless'.(pour les routeurs, voir la RFC1812)
Pour notre exemple, on obtient donc 8 sous-réseaux possibles.
Les bits de poids faibles (les bits verts) vont indiquer, pour chacun de ces sous-réseaux, les adresses à allouer aux machines. Par exemple, dans le réseau 204.34.57.32, la premiere machine portera l'adresse 1. Le dernier octet aura alors la valeur suivante :

soit 33. L'adresse TCP/IP complète sera donc 204.34.57.33. Ainsi de suite jusqu'à 204.34.57.62. On ne peut utiliser l'adresse 204.34.57.63 pour une machine, car elle correspond a l'adresse de broadcast du sous-réseau 204.34.57.32.
Ensuite, dans le réseau 204.34.57.64, la première machine aura pour adresse 204.34.57.65 et ainsi de suite.
En procédant ainsi, on a découpé un espace ou l'on pouvait initialement allouer 254 machines en 8 sous-réseaux dans lesquels on ne peut allouer au total que 8 fois 30 machines. Le tableau ci-dessous montre, en fonction des bits alloués soit au réseau soit aux hôtes, les différentes possibilités envisageables en classe C.

bits réseau/ bits hôte	nb de sous-réseaux	nb d'hôtes	masque
1 / 7	2	126	255.255.255.128
2 / 6	4	62	255.255.255.192
3 / 5	8	30	255.255.255.224
4 / 4	16	14	255.255.255.240
5 / 3	32	6	255.255.255.248
6 / 2	64	2	255.255.255.252
7 / 1	128	0	255.255.255.254

La dernière ligne est à écarter, pour des raisons évidentes. Il reste donc 6 possibilités de découpage en classe C. En classe B, ces possibilités sont différentes, mais les contraintes sont les mêmes.

Les nouveaux masques réseau.

Avec ces nouveaux sous-réseaux, on doit également modifier le masque de réseau. Dans le cas ci-dessus, le masque initial fourni pour la classe C était de 255.255.255.0. Mais on a utilisé les trois bits de poids fort du dernier octet pour coder les sous-réseaux. Il faut donc rajouter au masque initial le masque de sous-réseau. Ce dernier vaut 32+64+128, soit 224. Le nouveau masque réseau est donc 255.255.255.0 + 224 = 255.255.255.224.

Ce nouveau masque s'applique à tous les 6 sous-réseaux de l'exemple ci-dessus, puisque les trois bits de poids 32, 64 et 128 sont affectés à la fonction "sous-réseau".

Pour résumer, le masque ne dépend que du nombre de bits affectés au réseau et au sous-réseau : il suffit de positionner ces bits à 1 et de faire une somme binaire (un 'OU binaire') pour obtenir le masque.

Ce masque de réseau est important, car il va déterminer l'adresse de diffusion (broadcast) et, partant, limiter les diffusions aux seules machines faisant partie d'un sous-réseau déterminé.

Les adresses de diffusion (broadcast).

Chaque sous-réseau ainsi constitué doit avoir une adresse réseau, un masque de réseau et une adresse de diffusion (broadcast). L'adresse de diffusion est simple à calculer : elle correspond à l'adressse du réseau ou du sous-réseau plus l'adresse de l'hôte dont tous les bits sont à 1.

Chaque sous-réseau possède une adresse de diffusion propre.

Dans le cas du sous-réseau 204.34.57.32, le numéro d'hôte dont tous les bits (les bits verts de la figure ci-dessus) sont à 1 est 31. Si on ajoute ce nombre à l'adresse du réseau, on obtient 204.34.57.32 + 31 = 204.34.57.63.

Le cas du réseau de classe B.

Dans le cas d'un réseau de classe B, si il n'y pas de sous-réseau, 2 octets sont utilisés pour numéroter les machines. C'est sur l'ensemble de ces deux octets que vont s'effectuer les re-découpages. Il y a bien sûr plus de possibilités de découpage qu'en classe C, mais la démarche reste identique.

bits réseau/ bits hôte	nb de sous-réseaux	nb d'hôtes	masque
1 / 15	2	32766	255.255.128.0
2 / 14	4	16382	255.255.192.0
3 / 13	8	8190	255.255.224.0
4 / 12	16	4094	255.255.240.0
5 / 11	32	2046	255.255.248.0
6 / 10	64	1022	255.255.252.0
7 / 9	128	510	255.255.254.0
8 / 8	255	254	255.255.255.0

On notera que le tableau s'arrête à 8 bits par réseau. Ee effet, on "tombe "ensuite dans le cas d'un réseau de classe C, tout du moins en ce qui concerne le découpage en sous-réseaux. Pour le représentation des sous-réseaux de classe C, la RFC1878 parle d'ailleurs "d'extended class B subnets".

Le cas du réseau de classe A.

Dans le cas d'un réseau de classe A, 3 octets sont utilisés pour numéroter les machines. C'est sur l'ensemble de ces deux octets que vont s'effectuer les re-découpages.

Plus de classe : le CIDR.

Maintenant que vous avez assimilé cette méthode quelque peu complexe, oubliez là. En voici une à la fois plus simple et plus générale.

Vous savez sans doute que l'on va bientôt arriver à une pénurie d'adresses TCP/IP sur Internet. Pourquoi ? Supposons par exemple que vous ayez 300 machines et/ou périphériques à installer sur un réseau connecté à l'Internet. Si vous vous faites allouer un réseau de clase B avec 65535 adresses, la plupart ne seront donc pas utilisées.

Partant de ce constat, les organismes chargé d'allouer les adresses ont décidé d'abandonner ce découpage en classes et de proposer le CIDR (Classless Inter Domain Routing) qui est détaillé dans la RFC1519. Ce procédé vise à :

1. alléger les tables de routage sur les routeurs Internet
2. optimiser l'allocation d'adresses en évitant le gaspillage actuel.

Ce procédé consiste à allouer un lot de plusieurs adresses, et un masque de réseau associé qui couvre ces adresses. Par exemple, si on désire 300 adresses, il faut fournir un lot d'adresses correspondant à plusieurs adresses de réseau en classe C :

204.34.50.0 soit 254 hôtes
204.34.51.0 soit 254 hôtes

avec le masque de réseau : 255.255.254.0

Dans ce cas, la notation adoptée est 204.34.50.0/23. Ce qui signifie : adresse de réseau 204.34.50.0 avec un masque de sous réseau de 32 bits dont les 23 bits les plus à gauche (les bits jaunes) sont à 1. Les 9 bits de poids faibles (les bits verts) sont utilisés pour numéroter les 510 hôtes. Les adresses 204.34.50.0 et 204.34.51.255 étant réservées respectivement pour l'adresse du réseau et l'adresse de diffusion.

En utilisant le CIDR, les fournisseurs d'accès se voient allouer de larges espaces d'adressage qu'il répartissent ensuite à leurs clients.