

**UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI
(UNITECH)
DESS EN TECHNOLOGIE DE L'INFORMATION
ANNÉE ACADÉMIQUE 2024-2025
SESSION 1**

Architecture des Réseaux

Enseignante: Judith Soulamite Nouho Noutat, Msc en Informatique

Chapitre 1: Introduction aux réseaux et modèles

Concepts de base

Généralités

- Le terme informatique provient d'information et d'automatique, l'informatique étant le traitement automatique de l'information.
- Un réseau est une organisation de voies de communication entre différentes entités.
 - Cette définition est générale et peut s'appliquer par exemple aux réseaux routiers, ferroviaires, de télécommunications, etc.
- Un réseau d'ordinateurs est un ensemble d'ordinateurs autonomes interconnectés au moyen d'une seule technologie.
 - Deux ordinateurs sont dits interconnectés s'ils peuvent échanger des informations.

Généralités

- De manière plus générale, les entités qui communiquent au sein d'un réseau informatique sont des ressources informatiques dont on distingue deux types :
 - les ressources matérielles :
 - composants de traitement : ordinateurs, tablettes tactiles, imprimantes, scanners, . . .
 - composants de transmission : modems, cartes réseaux, commutateurs, routeurs, câbles, . . .
 - les ressources logicielles : applications informatiques, jeux, bases de données, . . .
- Un réseau informatique est constitué des moyens à la fois matériels et logiciels mis en œuvre pour assurer les communications entre des ressources informatiques.
- Un réseau informatique permet aux entités reliées de partager des informations, les résultats de traitements, les ressources, par exemple pour que plusieurs utilisateurs travaillant sur des ordinateurs différents puissent utiliser la même imprimante

Généralités

Réseaux Informatiques



Représentation de l'information

- Les données informatiques sont représentées par des suites de nombres.
 - Ces nombres sont écrits en binaire (c'est-à-dire en base 2).
 - En base 2, on n'utilise que les chiffres 0 et 1.
- Un symbole binaire (donc en base 2) est appelé un bit (binary digit).
 - 1 bit permet de coder 2 états : 0 et 1 ;
 - 2 bits permettent de coder 4 états : 00, 01, 10 et 11 ;
 - 3 bits permettent de coder 8 états : 000, 001, 010, 011, 100, 101, 110 et 111 ;
 - ...
 - n bits permettent de coder 2^n états.
- Une suite de 8 bits est appelée un octet.
 - Attention, en anglais le bit est appelé bit, alors que l'octet est appelé byte

Représentation de l'information

- Les unités multiples des bits et des octets sont décrites dans les tableaux ci-dessous:

Unité	Symbole	Valeur (bits)
kilo-bit	Kb	$10^3 = 1\,000$
méga-bit	Mb	$10^6 = 1\,000\,000$
giga-bit	Gb	$10^9 = 1\,000\,000\,000$
téra-bit	Tb	$10^{12} = 1\,000\,000\,000\,000$

Unité	Symbole	Valeur (octets)
kibi-octet	Kio	$2^{10} = 1\,024$
mébi-octet	Mio	2^{20}
gibi-octet	Gio	2^{30}
tébi-octet	Tio	2^{40}

Mesures de performance - Débit

- Le débit d'un réseau mesure la quantité d'information que le réseau peut transmettre par unité de temps :

$$\text{débit} = \frac{\text{quantité d'information}}{\text{temps}}$$

- L'unité est par conséquent le bit par seconde, noté b/s. Les réseaux actuels ayant un débit assez élevé, on utilise plus souvent des mégabits par secondes, notés Mb/s

Débits nominal et utile

- Le **débit nominal** d'un réseau est la quantité théorique maximale d'information pouvant être transmise par unité de temps.
- Le débit **utile** est la quantité d'information effectivement transmise par unité de temps.

Taux d'utilisation

- Le taux d'utilisation du réseau est donc le rapport du débit utile au débit nominal:

$$\text{taux d'utilisation} = \frac{\text{débit utile}}{\text{débit nominal}}$$

- Le taux d'utilisation est inférieur à 100%.
 - Ceci est dû entre autres aux pertes sur la voie de communication et à l'intervalle de temps laissé entre l'envoi de deux messages.

Temps d'acheminement des messages

- Le temps total d'acheminement d'un message se compose de deux parties :
 - le temps de transmission est le temps mis pour transmettre la quantité d'information du message:

$$temps_{transmission} = \frac{\text{quantité d'information}}{\text{débit}}$$

- le temps de propagation est le temps mis pour que le signal se propage sur le matériel. Les équipements traversés peuvent introduire des retards.

$$temps_{propagation} = \frac{\text{distance parcourue}}{\text{vitesse}} + \text{retards}$$

- On a donc : $temps_{total} = temps_{transmission} + temps_{propagation}$

Classification des réseaux

- Les réseaux sont caractérisés non seulement par leur débit, mais également par le rayon de couverture géographique qu'ils permettent d'atteindre.
- Les différentes caractéristiques sont présentées dans le tableau suivants:

Sigle	Nom	Distance	Débit
PAN	Personal Area Network	quelques mètres	1Mb/s
LAN	Local Area Network	jusqu'à 2km	de 10Mb/s à 1Gb/s
MAN	Metropolitan Area Network	jusqu'à 100km	environ 100Mb/s
WAN	Wide Area Network	milliers de km	quelques Mb/s

- Le PAN est utilisé chez un particulier, le LAN dans un bâtiment (ou plusieurs bâtiments proches) d'une entreprise, le MAN interconnecte différents sites à l'échelle d'une agglomération, et le WAN s'étend sur un pays.

Topologies de réseaux - Composants

- Les composants des réseaux se répartissent selon trois types :
 - Les composants de traitement ou périphériques finaux sont les entités produisant et/ou consommant les informations qui circulent sur le réseau (par exemple les ordinateurs, tablettes, scanners, ...) ;
 - Les composants de routage ou périphériques intermédiaires assurent la transition et la circulation des informations échangées entre les composants de traitement (par exemple, commutateurs, routeurs, point d'accès sans fil, ...).
 - Les supports de communication ou média interconnectent les équipements
 - Support filaire: fil de cuivre, fibre optique
 - Support sans fil

Topologies de réseaux - Connexions

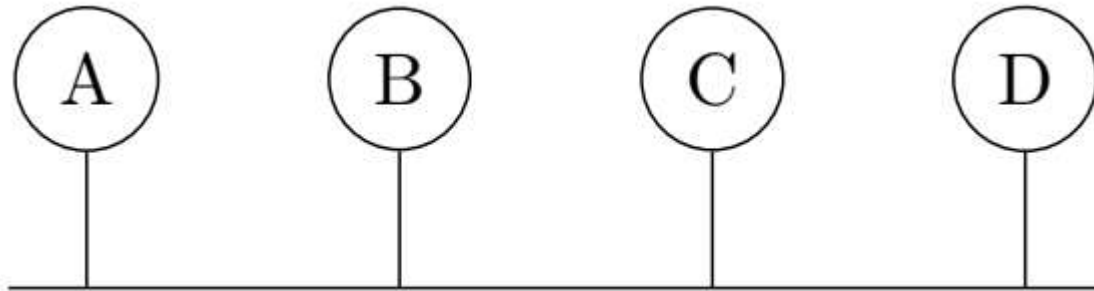
- La connexion entre entités peut être point-à-point, c'est-à-dire qu'elle peut associer exactement deux entités, ou peut être une connexion multipoints qui en associe plus.
- Les modes de communication sont simplex, c'est-à-dire dans un seul sens, ou duplex, dans les deux sens.

Architectures des réseaux

- L'architecture d'un réseau comprend 3 parties :
 - L'architecture **physique** définit la topologie physique d'interconnexion des composants du réseau.
 - L'architecture **logique** définit la topologie de circulation de l'information. Elle peut être différente de l'architecture physique.
 - L'architecture **logicielle** définit les logiciels assurant l'acheminement des données.
- Les architectures physiques et logiques les plus classiques sont le bus, l'étoile, l'anneau, l'arbre, le graphe et la topologie complète.

Le bus

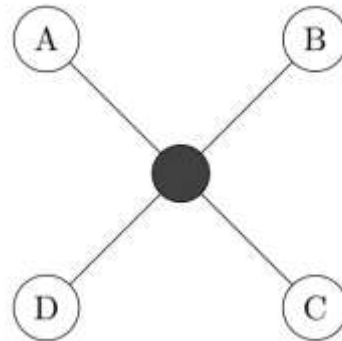
- La topologie en bus consiste en un câblage unique auquel les différents nœuds sont connectés.



- Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent des signaux.
 - Lorsqu'une station est en panne et ne transmet plus sur le réseau, elle ne perturbe pas le réseau.
 - Par contre une seule coupure du câble empêche toute station d'échanger des messages sur le réseau.

L'étoile

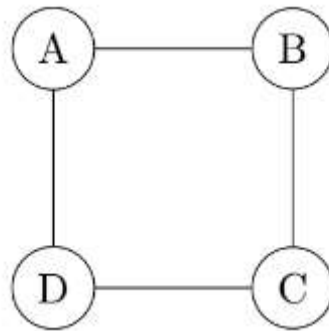
- Dans la topologie en étoile tout nœud est connecté à un point central.
 - Le point central doit être un matériel actif, comme un concentrateur ou un commutateur, c'est-à-dire un matériel qui remet en forme les signaux et les régénère avant de les retransmettre.



- La panne d'un nœud ne perturbe pas le fonctionnement global du réseau.
- En revanche, une panne de l'équipement central qui relie toutes les stations rend le réseau totalement inutilisable.

L'anneau

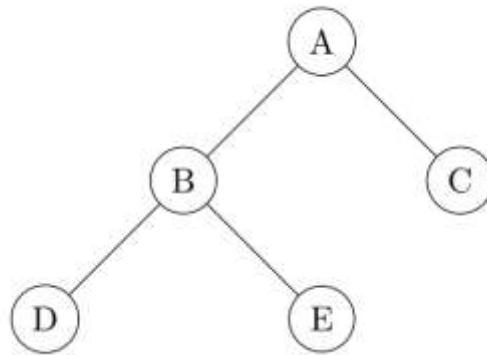
- La topologie en anneau repose sur une boucle fermée, en anneau, où toutes les stations sont connectées en chaîne les unes aux autres par une liaison point-à-point.



- Chaque station joue le rôle de nœud intermédiaire.
 - Les informations transitent par chaque nœud, qui se comporte comme un répéteur et retransmet les informations au nœud suivant.
 - La défaillance d'une station rend le réseau inutilisable.

L'arbre

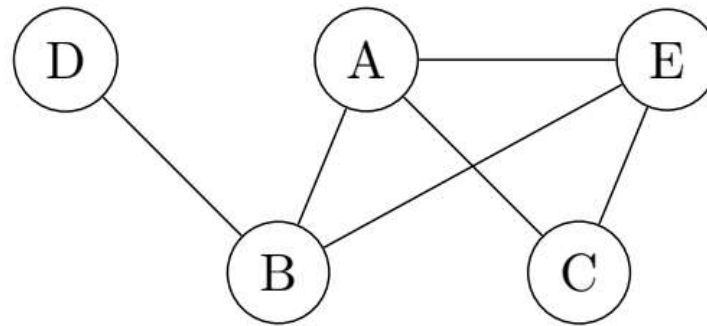
- Dans l'architecture en arbre, les nœuds sont reliés entre eux de manière hiérarchique, donc par niveaux.
 - Le sommet de haut niveau est appelé racine.
 - Chaque nœud peut être connecté à plusieurs nœuds de niveau inférieur : dans ce cas on appelle ce nœud parent et les nœuds de niveau inférieur fils.



- Le point faible de cette topologie est le fait que si le nœud parent tombe en panne, il paralyse tout le sous-arbre dont il est racine.

Le graphe

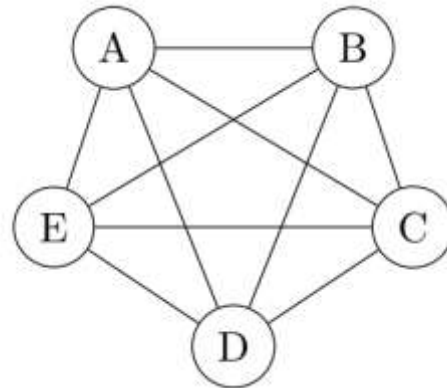
- Dans la topologie en graphe les nœuds sont connectés entre eux par des liaisons point-à-point, de manière à constituer un graphe connexe.



- L'information peut parcourir le réseau suivant des itinéraires différents.

La topologie complète

- Dans la topologie complète il y a une liaison point-à-point entre chaque paire de nœuds, donc toute station est reliée à toutes les autres.



- L'inconvénient de cette topologie est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de stations augmente.

Modèle de référence OSI

Normalisation

- L'établissement de normes permet d'avoir une structure homogène pour faire communiquer différents équipements.
 - La conformité à une norme garantit la satisfaction de règles précises.
- Ainsi, des matériels différents, fabriqués par diverses entreprises, peuvent communiquer car la norme offre un cadre compatible entre ces entités hétérogènes.
- La norme permet également d'assurer un niveau minimum de qualité.

Organismes de normalisation

- La normalisation est effectuée par des organismes compétents au sein desquels les différents acteurs du domaine sont représentés.
- Trois organismes internationaux sont concernés par la normalisation dans le domaine des réseaux :
 - UIT (Union Internationale des Télécommunications) est l'institution spécialisée de l'ONU (Organisation des Nations Unies) dans le domaine des télécommunications.
 - Elle comprend deux branches :
 - l'UIT-T chargée de la normalisation dans le domaine des télécommunications et
 - l'UIT-R qui s'occupe du domaine des radiocommunications.
 - IEC (International Electrotechnic Commission), fondée en 1906, est chargée de coordonner et d'unifier les normes dans le domaine de l'électricité.
 - ISO (International Standards Organisation) est une organisation privée chargée de la normalisation dans tous les domaines sauf l'électricité et l'électronique.
- Au Cameroun, les normes sont gérées par l' **Agence des Normes et de la Qualité (ANOR)**

Modèle de référence OSI

- Le modèle de référence défini par l'**ISO** est l'**OSI** (Open System Interconnection).
 - Il permet à des systèmes hétérogènes de s'interconnecter et d'échanger des informations.
 - Il est par conséquent indépendant de la structure et de la technologie des matériels employés.
- Ce modèle offre un cadre permettant d'assurer une compatibilité maximum entre les entités communicantes tout en minimisant les contraintes permettant de les réaliser.

Principes de la structuration en couches

- La complexité de conception, de réalisation et de maintenance des logiciels et de l'architecture des réseaux, est maîtrisée grâce à une organisation en couches ou niveaux, chaque couche étant bâtie au-dessus de la précédente.
 - Le rôle de la couche de niveau N est de fournir des services à la couche de niveau $N + 1$ tout en lui dissimulant les détails d'implémentation. La couche de niveau $N + 1$ communique à la couche N les caractéristiques du service attendu.
 - La couche N , pour offrir les services à la couche $N + 1$, utilise les services offerts par la couche $N - 1$.
 - Par conséquent, chaque couche peut interagir uniquement avec les deux couches adjacentes.

Principes de la structuration en couches

- Une couche N est constituée d'un ensemble d'entités formant un sous-système de niveau N.
 - Elle ne peut dialoguer qu'avec une couche de même niveau N sur une autre machine.
 - Les communications se font donc entre entités homologues.
 - La communication entre deux entités homologues de niveau N obéit à un ensemble de règles et formats, syntaxiques et sémantiques, prédéfinis pour les entités de niveau N.
- Ces règles et formats définissent le **protocole** de niveau N.

Couches du modèle OSI

- Le modèle OSI est composé de sept couches, qui sont organisées de la façon suivante :

Niveau	Couche
7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison de données
1	Physique

Couches du modèle OSI

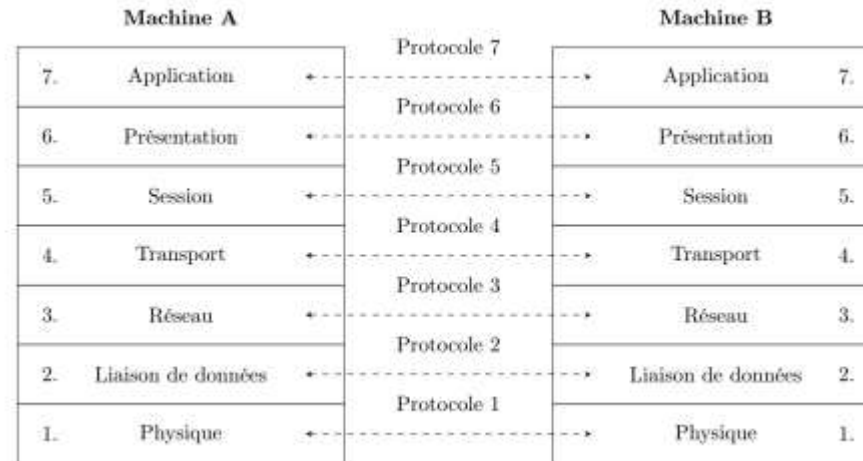
- Chaque couche a un rôle spécifique :
 - 7. La couche application offre aux utilisateurs des services normalisés pour la conception de leurs applications.
 - 6. La couche présentation réalise la compression et le chiffrement, et vérifie la syntaxe des données échangées.
 - 5. La couche session contrôle le dialogue entre les machines qui communiquent.
 - Elle gère en particulier la synchronisation du dialogue et la reprise après interruption.
 - 4. La couche transport assure le transport de bout en bout, c'est-à-dire entre les deux stations qui communiquent.
 - Elle garantit que le message est acheminé entre les deux stations avec la qualité de service demandée.
 - Le terme qualité de service désigne un ensemble de propriétés que le demandeur du service exige du prestataire, telles que la garantie d'un débit minimum, le respect d'une borne maximum de temps de livraison de messages, . . .

Couches du modèle OSI

- 3. La couche réseau assure l'acheminement des blocs d'information à travers le sous-réseau.
 - Elle choisit le meilleur chemin entre les deux commutateurs d'entrée-sortie du sous-réseau.
 - Les blocs d'information de niveau 3 sont appelés **paquets**.
- 2. La couche liaison de données est responsable de l'acheminement sans erreur des blocs d'information entre les deux machines qui se trouvent aux extrémités d'une liaison de données.
 - Les blocs d'information de niveau 2 sont appelés **trames**.
- 1. La couche physique définit les moyens mécaniques (connecteurs), électriques et fonctionnels nécessaires à l'activation, au maintien et à la désactivation des connexions physiques destinées à la transmission des données binaires au niveau de la couche liaison de données.
 - Elle fournit donc tous les éléments matériels et logiciels nécessaires au transport correct des données binaires, comme :
 - les interfaces de connexion des équipements informatiques au support de transmission, appelées jonctions ;
 - les supports de transmission ;
 - les cartes réseaux ;
 - les modems ;
 - les multiplexeurs, qui concentrent plusieurs communications sur une ligne de transmission unique.

Protocoles et services

- D'un point de vue logique la communication intervient entre deux entités homologues, qui discutent en suivant des protocoles.



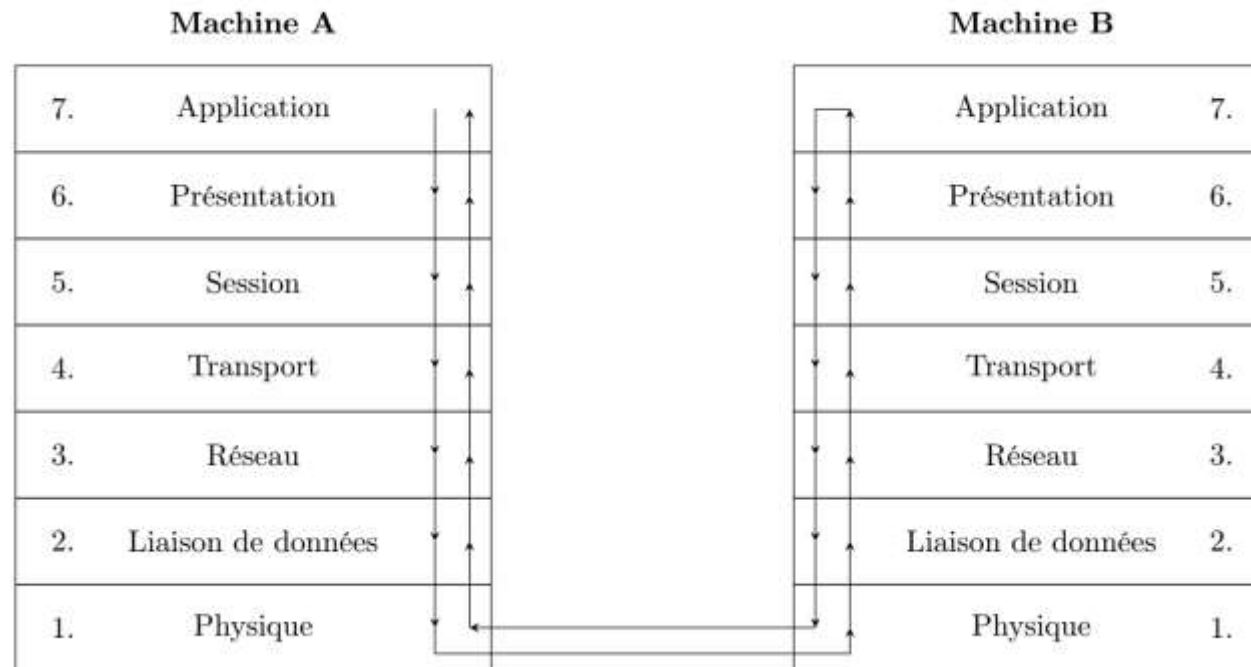
- En réalité aucune donnée ne passe directement de la couche N de la machine A à la couche N de la machine B.
 - Chaque couche utilise les services de la couche immédiatement au-dessous et offre des services à la couche au-dessus.
 - Les notions de protocole et de service sont donc fondamentales pour le fonctionnement de la pile des protocoles.

Protocoles et services

- Un **protocole** de niveau N est un ensemble de règles et formats, syntaxiques et sémantiques prédéfinis qui sont utilisés dans la communication entre entités d'un même niveau N de deux machines différentes.
- Un **service** est fourni par une couche de niveau N à la couche de niveau N + 1 d'une même machine.
- Les services fournis par une couche N sont identifiés par des **SAP (Service Access Point)**.
- L'**interface** définit les opérations fondamentales et les services que la couche inférieure offre à la couche supérieure.

Protocoles et services

- La figure suivante décrit la communication entre les 7 niveaux de couches de deux entités communicantes A et B.



Encapsulation, PDU et SDU

- Les messages échangés par un protocole de niveau N sont appelés des **PDU_N (Protocol Data Unit de niveau N)**.
- Les messages échangés entre la couche N et la couche inférieure N – 1 sont appelés des **SDU_{N-1} (Service Data Unit de niveau N – 1)**.
- De plus, un protocole de niveau N ajoute au SDU_N qu'il a reçu des informations de contrôle visant à contrôler la bonne exécution du protocole.
 - Ces informations de contrôle sont appelées **PCI_N (Protocol Control Information de niveau N)**.
- On a par conséquent :
$$\begin{aligned} PDU_N &= SDU_N + PCI_N \\ SDU_N &= PDU_{N+1} \end{aligned}$$
 - On dit alors que le PDU_N **encapsule** le SDU_N .
 - Au lieu d'indexer le PDU ou le SDU par le numéro de la couche, on le fait souvent précéder de la première lettre du nom de la couche (en anglais).
 - Par exemple, NPDU = PDU_3 , où le N indique la couche réseau (network).

Encapsulation, PDU et SDU

- Exemple:
 - Considérons deux machines, A et B, qui communiquent en utilisant un modèle à 5 couches.
 - Une application de niveau 5 de la machine A doit envoyer des données à sa couche homologue de la machine B.
 - Supposons que toutes les couches rajoutent une en-tête (dénnotée H comme header) et que les couches 1 et 2 rajoutent aussi une en-queue (dénnotée T comme tail).
 - La structure d'un message de niveau 5 sera donc la suivante :



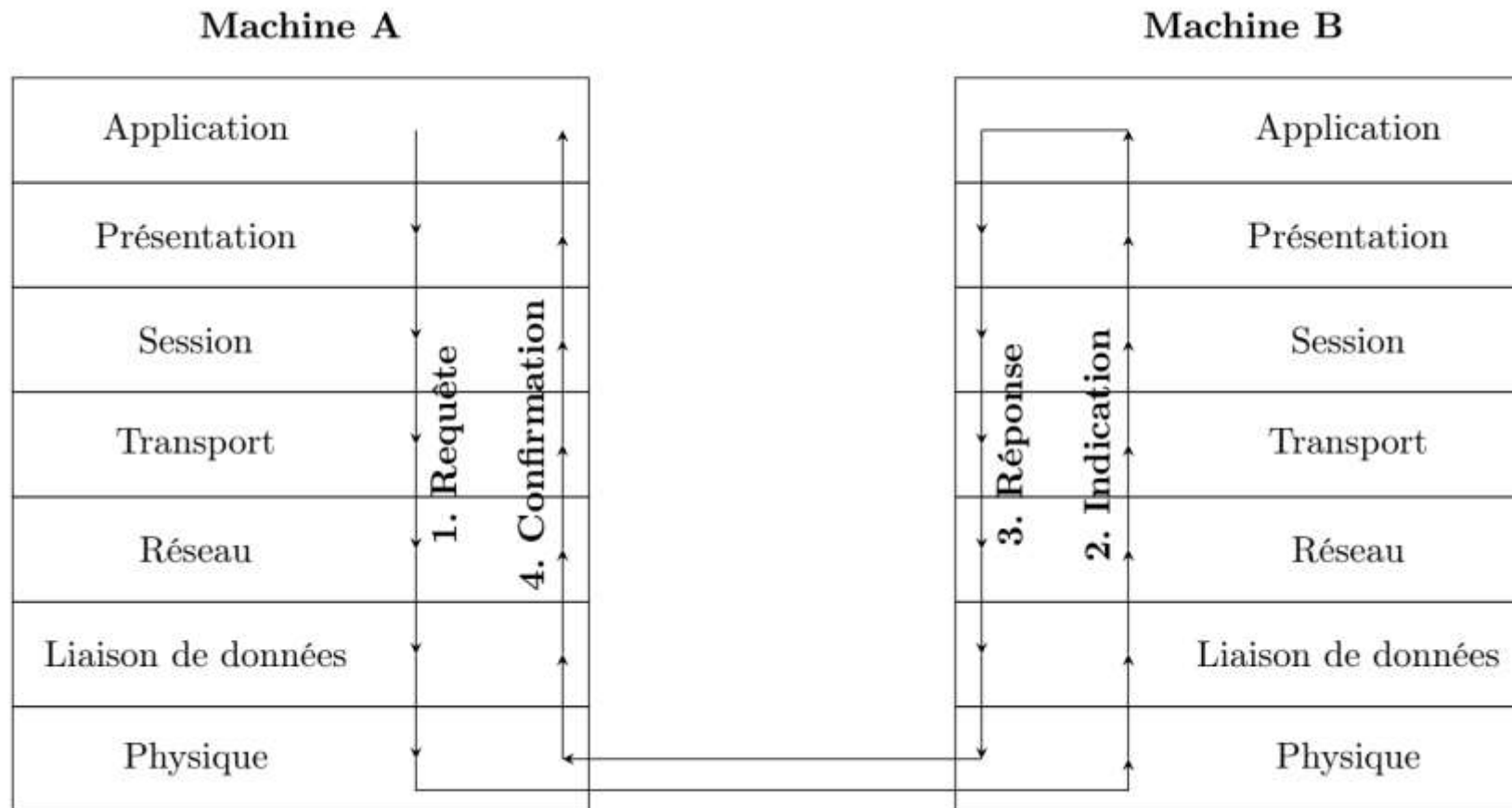
Primitives de service

- Les protocoles peuvent opérer en mode connecté ou en mode déconnecté.
- En mode **connecté**, la communication entre entités homologues de même niveau passe par l'établissement d'une connexion.
 - Le transfert des données comporte donc trois phases :
 - 1. l'établissement de la connexion,
 - 2. le transfert des données,
 - 3. la déconnexion.
 - Le contexte de la communication est préservé.
- En mode **déconnecté**, seule la phase de transfert a lieu, et la communication s'effectue sans mémoire.

Primitives de service

- Il existe 4 primitives de service : requête (en anglais : request), indication (indication), réponse (response) et confirmation (confirmation).
- Les protocoles qui fournissent des services avec confirmation utilisent les quatre primitives, en revanche les protocoles qui fournissent des services sans confirmation utilisent seulement les primitives « requête » et « indication ».
 - Une requête est initialement envoyée par la couche N à la couche N – 1 d'une même entité.
 - Ensuite, une indication est transmise de la couche N – 1 à la couche N de l'autre entité communicant.
 - Ensuite, si le service est avec confirmation, la réponse est envoyée par la couche N à la couche N – 1 de cette seconde entité.
 - Enfin, une confirmation est transmise de la couche N – 1 à la couche N de l'entité ayant émis la requête.

Primitives de service



Modèle TCP/IP

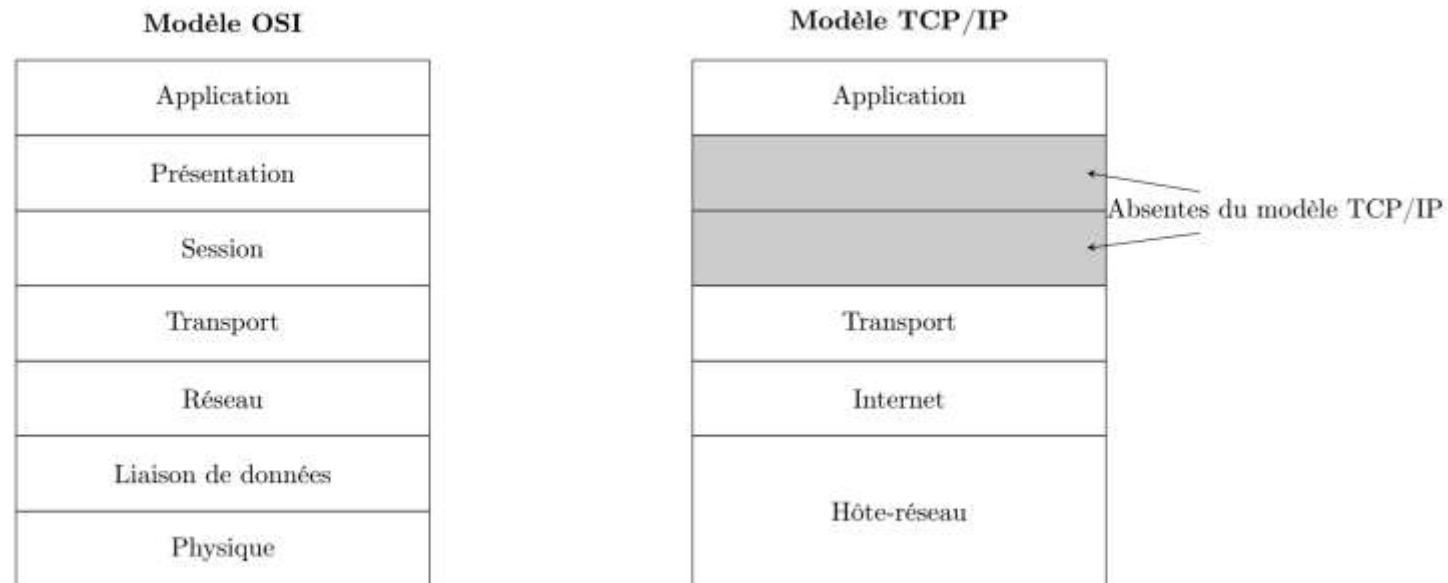
Modèle TCP/IP

- Le modèle TCP/IP est nommé d'après ses deux protocoles principaux TCP et IP, mais il comporte en réalité plusieurs dizaines de protocoles.
- Il définit un modèle de quatre couches.

Niveau	Couche
4	Application
3	Transport
2	Internet
1	Hôte-réseau

Modèle TCP/IP

- Ce modèle a été proposé dix ans avant le modèle OSI et c'est le modèle couramment utilisé.



Couche Hôte-réseau

- La couche Hôte-réseau utilise un système d'adressage basé sur les adresses MAC.
- Une adresse **MAC (Media Access Control)** est un identifiant physique codé sur 6 octets qui est enregistré dans la carte réseau.
- Les adresses MAC sont souvent écrites en hexadécimal par 6 mots de 2 lettres séparés par un ":".
 - Cette adresse identifie de façon unique l'interface réseau de la machine : les premiers trois octets constituent l'identifiant du constructeur de la carte, les derniers trois l'identifiant de la carte attribué par le constructeur.
 - Exemple: L'adresse MAC 00000000 00011000 11011110 00010000 11111010 10000111 sera écrite 00:18:DE:10:FA:87.
 - L'identifiant du constructeur est 00:18:DE (Intel), l'identifiant de la carte attribué par Intel est 10:FA:87.
- Une machine avec plusieurs cartes réseaux aura plusieurs adresses MAC.
 - Hors cas de falsification ou piratage, une adresse MAC est unique sur toute la planète.
- L'adresse MAC de diffusion est FF:FF:FF:FF:FF:FF.

Ethernet

- Le protocole Ethernet, normalisé comme IEEE 802.3, a fini par devenir omniprésent en entreprise.
- Il repose sur une topologie physique et logique en bus : il y a donc plusieurs machines connectées au même câble.
 - Lorsqu'une machine A envoie une trame à une machine B toutes les stations du réseau vont la recevoir, mais seulement la machine B la traite (les autres l'ignorent).

Ethernet

- Pour régler l'accès au canal physique, Ethernet utilise une technologie appelée **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**.
 - **Carrier Sense Multiple Access.** Quand une station doit envoyer des données, elle exécute l'algorithme CSMA :
 - 1. elle commence par écouter le support de transmission pour savoir si une autre station n'est pas déjà en train de transmettre.
 - 2. Si c'est le cas, elle attend que le support se libère.
 - 3. Quand le support est de nouveau disponible elle transmet sa trame.
 - **Collision Detection.** Néanmoins, si deux stations, après s'être assurées que le canal est libre, commencent une transmission au même moment elles provoqueront une collision qu'elles sauront toutefois détecter en écoutant le support.
 - Lorsqu'une collision se produit, la station émettrice d'une trame lance la procédure de gestion des collisions :
 - 1. elle continue la transmission à hauteur pour s'assurer que toutes les stations détectent la collision,
 - 2. elle observe un temps de pause aléatoire dépendant du nombre de tentatives de transmission,
 - 3. elle redémarre l'envoi de la trame

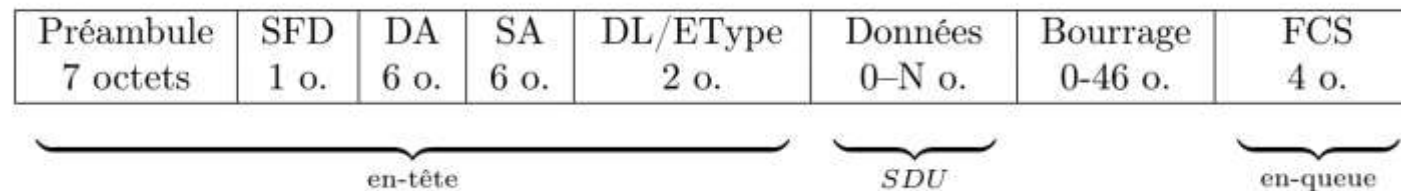
Ethernet

- **Trame**

- La couche ajoute à son SDU 22 octets d'en-tête et 4 octets d'en-queue, donc un total de 26 octets de PCI.
- Si le SDU encapsulé a une taille inférieure à 46 octets, alors des 0 sont rajoutés à la fin de telle manière à atteindre cette taille minimale.
- Ces octets à 0000 0000 sont appelés **octets de bourrage**.

Ethernet

- La trame Ethernet a donc la structure suivante :



- Préambule** : séquence de 7 octets à 1010 1010. Il permet la synchronisation des horloges de l'émetteur et du récepteur.
 - SFD (Start Frame Delimiter)** : un octet à 1010 1011 indiquant le début de la trame.
 - DA** : adresse MAC destination.
 - SA** : adresse MAC source.
 - DL/Etype** : si plus petit que 1 500 c'est la longueur des données (Ethernet I), sinon c'est le type de la trame (Ethernet II). Par exemple 0800 correspond à l'encapsulation d'un paquet IP.
 - FCS (Frame Check Sequence)** : utilisé par le code polynomial
- Le préambule et le SFD sont souvent considérés juste comme une phase de synchronisation et donc extérieurs à la structure de la trame.

Token Ring

- Le protocole Token Ring (anneau à jeton) a été normalisé comme IEEE 802.5.
 - Il existe différents standards autorisant des débits de 4 Mbit/s, 16 Mbit/s, puis 100 Mbit/s qui sont fonction du câblage utilisé.
 - Son concurrent Ethernet, moins onéreux et plus facile d'exploitation, quoique moins efficace, a fini par le supplanter, même si l'on retrouve encore Token Ring dans des infrastructures importantes.
- Token Ring repose sur une topologie logique en anneau, où chaque machine se comporte comme un répéteur.
 - Les trames parcourent l'anneau dans un sens qui est toujours le même.
 - Pour régler l'accès au support physique, ce protocole utilise une trame spéciale de trois octets, appelée **jeton**, qui est répétée de poste en poste et circule dans le sens l'anneau.

Token Ring

- Le fonctionnement du protocole est le suivant :
 - 1. À la réception du jeton, une machine qui désire envoyer une trame conserve le jeton et envoie ses données.
 - 2. Les données sont répétées de station en station jusqu'à atteindre son destinataire.
 - 3. La trame est alors marquée pour préciser à l'émetteur si les données ont été reçues correctement.
 - 4. La trame revient alors vers son émetteur qui constate que ses données sont effectivement arrivées à destination. L'émetteur peut éventuellement envoyer plusieurs trames, mais il ne peut garder le jeton que pendant une durée maximale.
 - 5. Le jeton est remis en circulation et le processus peut recommencer.
- La machine de l'anneau ayant l'adresse MAC la plus élevée joue le rôle de surveillant du jeton.
 - Elle est en charge de résoudre un certain nombre de problèmes comme :
 - la détection de la perte du jeton,
 - la suppression d'une trame qui a déjà effectué un tour complet (l'émetteur a disparu avant de supprimer sa trame de l'anneau).

Couche Internet

- Internet Protocol (IP) fournit un système de livraison de paquets, sans connexion et non fiable.
 - « **Sans connexion** » signifie qu'IP ne maintient aucune information d'état concernant les trames successives.
 - Quand une machine envoie plusieurs trames à une autre machine, chaque trame est gérée indépendamment des autres, donc les trames peuvent emprunter des chemins différents, et l'ordre de réception peut être différent de l'ordre d'envoi.
 - « **Non fiable** » signifie qu'il n'existe aucune garantie que la trame IP arrive à destination avec succès.
 - Toute fiabilité requise doit être assurée par les couches supérieures (par exemple en utilisant TCP)

Couche Internet

- Adressage
 - Le protocole IP gère des **adresses logiques** qui sont appelées **adresses IP**.
 - Une adresse IP est un numéro d'identification de quatre octets (IPv4) qui est attribué de façon permanente ou provisoire à chaque carte réseau utilisant le protocole IP.
 - L'adresse IP est assignée soit manuellement par l'administrateur du réseau local, soit automatiquement via le protocole DHCP.
 - Si un composant dispose de plusieurs interfaces, chacune dispose d'une adresse IP spécifique.

Couche Internet

- Les adresses IP sont généralement écrites sous forme décimale pointée : ce sont quatre entiers de 0 à 255 séparés par des points.
 - Exemple: L'adresse binaire 00001010 00000000 00000000 00000001 est notée 10.0.0.1
- La suite d'octets d'une adresse IP est divisée en deux parties :
 - **NET-ID** : une sous-séquence qui désigne l'adresse d'un réseau.
 - **HOST-ID** : une sous-séquence qui désigne l'adresse d'une machine sur le réseau désigné par le NET-ID

Couche Internet

- Les adresses IP sont réparties en cinq classes. Les champs NET-ID et HOST-ID ont des longueurs variables, qui dépendent de la classe de l'adresse IP.
 - **Classe A** (grands réseaux) : ce sont les adresses dont le bit de poids fort est à 0.
 - Le NET-ID est alors codé sur le premier octet et les trois derniers octets représentent le HOST-ID.
 - Plage : de 1.0.0.0 à 127.255.255.255.
 - **Classe B** (réseaux moyens) : ce sont les adresses dont les deux bits de poids fort sont 10.
 - Le NET-ID est alors codé sur 2 octets et le HOST-ID sur les deux autres octets.
 - Plage : de 128.0.0.0 à 191.255.255.255.
 - **Classe C** (Petits réseaux) : ce sont les adresses dont les trois bits de poids forts sont 110.
 - Le NET-ID est alors codé sur les 3 premiers octets et le HOST-ID sur le dernier octet.
 - Plage : de 192.0.0.0 à 223.255.255.255.

Couche Internet

- **Classe D (Multicast)** : Ce sont les adresses dont les quatre bits de poids forts sont 1110.
 - Les 28 bits qui restent désignent dans ce cas un groupe de multicast.
 - Plage : de 224.0.0.0 à 239.255.255.255.
- **Classe E (Classe réservée)** : ce sont les adresses dont les cinq bits de poids fort sont 1111.
 - C'est une classe réservée pour des usages futurs.
 - Plage : de 240.0.0.0 à 255.255.255.255.

Couche Internet

- Certaines adresses IP sont réservées pour des usages particuliers :
 - 255.255.255.255 : adresse de diffusion.
 - NET-ID 1 . . . 1 : adresse de diffusion sur le réseau identifié par le NET-ID.
 - NET-ID 0 . . . 0 : adresse d'un réseau.
 - 127.X.Y.Z : adresse de la boucle locale.
 - Il permet de tester la pile de protocoles TCP/IP locale d'une machine sans passer par un réseau.
 - 0.0.0.0 : valeur qui indique l'absence d'une adresse IP.

Couche Internet

- Le masque réseau est une suite de quatre octets dont les bits correspondant à la partie **NET-ID** sont à **1**, et ceux du **HOST-ID** sont à **0**.
- En faisant un « et logique » bit à bit entre une adresse IP et le masque associé on obtient l'adresse du réseau auquel il appartient.
- La paire (adresse IP, masque) peut être représentée en notation **CIDR (Classless Inter-Domain Routing)** par l'adresse IP suivie d'une barre oblique « / » et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau.
 - Exemple:
 - Le masque réseau associé à l'adresse 192.168.1.1 est 255.255.255.0 puisque c'est une adresse de la classe C.
 - En notation CIDR on indiquera les deux comme 192.168.1.1/24.
 - Un « et logique » entre 192.168.1.1 et 255.255.255.0 donne l'adresse réseau 192.168.1.0.

Couche Internet

- **Routage**

- Les réseaux locaux peuvent être reliés entre eux à travers des machines particulières que l'on appelle routeurs.
- Le protocole IP est capable de choisir la route suivant laquelle les paquets de données seront relayés de proche en proche jusqu'au destinataire.
- Donc le routage IP fonctionne de façon totalement décentralisée : aucun routeur n'a une vision globale de la route que prendront les paquets de données.
- Chaque réseau a un certain **Maximum Transmission Unit (MTU)**.
 - Le MTU est la taille maximale d'un paquet pouvant circuler sur le réseau.
 - Si la taille du paquet est plus grande que le MTU du réseau le protocole IP du routeur fragmente le paquet en plusieurs paquets avant de les injecter sur le réseau.
- Une fois que tous les fragments sont arrivés à destination, le paquet original est reconstruit

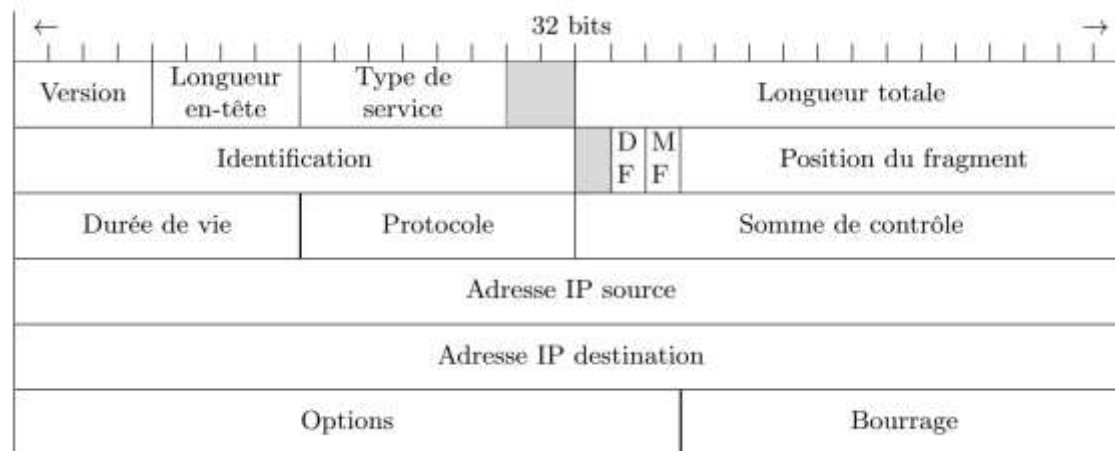
Couche Internet

- **Routage**

- Les adresses IP des machines source et destinataire sont spécifiées dans l'en-tête IP des paquets.
- Chaque routeur possède une table interne, appelée **table de routage**, qui lui indique la ligne sur laquelle les paquets doivent être expédiés pour une destination donnée.
 - La table contient des entrées qui associent l'adresse IP de destination et la ligne qu'il faut emprunter pour l'atteindre.
- Dans le cas du **routage statique**, l'administrateur réseau doit initialiser la table de routage de chaque routeur en saisissant les entrées correctement.
 - Ces routes ne changeront que si l'administrateur les modifie ensuite manuellement.
- Dans le cas du **routage dynamique**, les routes sont calculées automatiquement par un algorithme qui est exécuté sur chaque routeur.
 - Le protocole de routage permet aux routeurs d'échanger des informations concernant l'état du réseau et utiliser ces informations afin de calculer la meilleure route possible et mettre à jour leurs tables de routage.

Couche Internet

- Paquet IP
 - Les paquets IP sont encapsulés dans Ethernet ou Token Ring.
 - Le format d'un paquet IP est le suivant.



Couche Internet

- Paquet IP
 - **Version** : précise la version du protocole IP. La version couramment la plus utilisée est la 4.
 - **Longueur d'en-tête** : donne la longueur de l'en-tête du paquet IP en mot de 4 octets.
 - **Type de service** : informe les routeurs de la priorité du paquet et de la qualité de la route souhaitée.
 - **Longueur totale** : donne la longueur (en octets) du paquet, en-tête comprise.
 - **Numéro d'identification** : le couple (adresse IP source, identification) identifie un paquet de manière unique.
 - Ces informations sont nécessaires pour effectuer l'assemblage des fragments d'un paquet qui a subi une fragmentation.
 - **DF (Do not Fragment)** : si ce drapeau est positionné la fragmentation du paquet sera interdite.
 - **MF (More Fragments)** : si ce drapeau est positionné, le paquet fait partie d'une série de fragments, mais ce n'est pas le dernier d'entre eux. Sinon, c'est le dernier fragment.
 - **Position du fragment (Offset)** : indique la position du premier octet dans le paquet initial (non fragmenté), exprimée en multiple de 8 octets.
 - **TTL (Time To Live)** : si la valeur de la durée de vie d'un paquet est N alors ce paquet peut encore traverser $N - 1$ routeurs.

Couche Internet

- **Paquet IP**
 - **Protocole** : indique la nature du protocole encapsulé dans le paquet IP. La liste des protocoles est donnée dans le RFC 1700.
 - Quelques valeurs : ICMP (1), TCP (6) et UDP (17).
 - **Somme de contrôle** : code de protection de l'en-tête IP.
 - **Adresse IP Source/Destination**.
 - **Options** : ce champ peut être complété par des octets de bourrage afin de rendre la taille de l'en-tête IP un multiple de 4 octets puisque la longueur de l'en-tête est exprimée en mots de 4 octets

Couche Internet

- Address Resolution Protocol (ARP)
 - Le protocole de résolution d'adresse (ARP, Address Resolution Protocol) effectue la traduction d'une adresse de protocole de couche (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse Ethernet).
- ARP : Adresse Logique → Adresse Physique
- Ce protocole permet à une machine de trouver l'adresse physique d'une autre machine (connectée sur le même réseau) à partir de son adresse IP.
 - Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

Couche Internet

- ARP
 - Le fonctionnement du protocole est le suivant :
 - 1. La machine source demande l'adresse physique correspondant à une certaine adresse IP en envoyant en mode diffusion un paquet *ARP-Request*.
 - 2. Le paquet *ARP-Request* contient l'adresse IP de la machine recherchée ainsi que les adresses IP et physique de la machine source.
 - 3. Si la machine recherchée se trouve sur le réseau local alors elle répond directement à la machine source en envoyant un paquet *ARP-Reply* qui contient son adresse physique.
 - Un mécanisme de cache permet de réduire les délais d'attente dus à l'exécution du protocole.
 - La machine garde en mémoire pour un certain temps les correspondances obtenues entre les adresses logiques et les adresses physiques.

Couche Internet

- Message **ARP**

- Les messages ARP sont encapsulés directement dans Ethernet ou Token Ring.
- Le format du message ARP est le suivant:

Type Mat.	Type Prot.	Long. Adr. Phy.	Long. Adr. Prot.	OP	Adr. Phy. Source	Adr. Prot. Source	Adr. Phy. Dest.	Adr. Prot. Dest.
2 o.	2 o.	1 o.	1 o.	2 o.	6 o.	4 o.	6 o.	4 o.

- Type Mat. : type de matériel physique (par exemple : Ethernet, Token Ring, etc.),
 - Type Prot. : type de protocole (par exemple : IP),
 - Long. Adr. Phy. : longueur de l'adresse physique,
 - Long. Adr. Prot. : longueur de l'adresse du protocole,
 - OP : opération,
 - Adr. Phy. Source : adresse physique de l'émetteur,
 - Adr. Prot. Source : adresse du protocole de l'émetteur,
 - Adr. Phy. Dest. : adresse physique du destinataire,
 - Adr. Prot. Dest. : adresse du protocole du destinataire.
- Le **protocole RARP (Reverse Address Resolution Protocol)** effectue la traduction inverse, c'est-à-dire des adresses physiques en adresses logiques

Couche Internet

- Exemple:
 - Une trame ARP a la structure suivante :



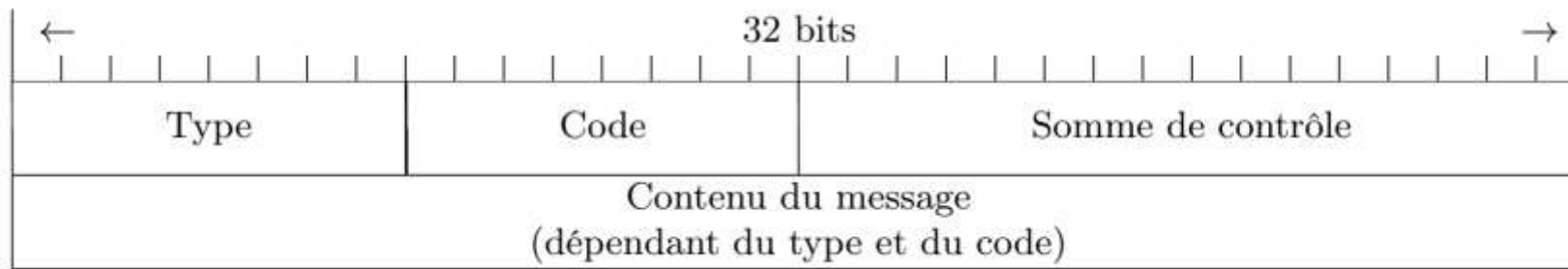
- Calculons sa taille, en considère aussi le préambule et le SFD.
- Le message ARP a une taille de $2 + 2 + 1 + 1 + 2 + 6 + 4 + 4 = 22$ octets. L'en-tête et l'en-queue
- Ethernet comportent $7 + 1 + 6 + 6 + 2 + 4 = 20$ octets. De plus, le message ARP ayant une taille inférieure à 46 octets, il faut ajouter $46 - 22 = 24$ octets de bourrage. Donc au total, la trame ARP a une longueur de $22 + 20 + 24 = 66$ octets.
- Remarque 4 Le protocole RARP (Reverse Address Resolution Protocol) effectue la traduction inverse, c'est-à-dire des adresses physiques en adresses logiques.

Couche Internet

- Internet Control Message Protocol (ICMP)
 - Lorsqu'un événement inattendu se produit pendant la communication entre les entités d'un réseau, il est signalé par le protocole de messages de contrôle de l'Internet, **ICMP (Internet Control Message Protocol)**.
 - Plus généralement, ce protocole permet d'envoyer des messages de collecte d'informations sur l'état du réseau

Couche Internet

- Message ICMP
 - Les messages ICMP sont encapsulés dans IP. Un message ICMP a le format suivant.



Couche Internet

- Message ICMP
 - Le champ type spécifie le type de message ICMP.
 - Certains types de messages ICMP se servent du champ code pour préciser la nature de l'erreur signalée. Le champ somme de contrôle est calculé sur l'intégralité du message ICMP et est utilisé pour vérifier s'il y a eu des erreurs de transmission du message.
 - Le contenu du message peut varier selon le type et le code de l'erreur rencontrée.
 - Le tableau suivant montre les principaux types de messages ICMP.

Type de Message	Description
Destination inaccessible	Le paquet n'as pas pu être livré
Délai expiré	Le paquet a expiré
Demande d'écho	Demande à une machine si elle est active
Envoi d'écho	La machine distante est active

Couche Transport

- Au niveau transport, il y a deux principaux protocoles : **TCP** (en mode connecté) et **UDP** (en mode non connecté).
- Les SAP de la couche transport sont des identifiants sur 16 bits appelés **ports**.
 - Un port désigne l'application sur la machine qui a fait appel au protocole de transport.
 - Les numéros de port de 0 à 1023 sont réservés pour les services systèmes (http sur le port 80, telnet sur le port 23, etc.)
- Une connexion entre deux applications est caractérisée de manière unique par :
 - les adresses IP source et destination,
 - les numéros de ports source et destination,
 - le protocole de transport utilisé : UDP ou TCP

Transmission Control Protocol (TCP)

- Transmission Control Protocol (TCP) est un protocole de transport qui assure un service orienté connexion avec confirmation.
- Il garantit la livraison sans erreur à n'importe quel hôte du réseau d'un flot d'octets émis par une machine.
 - Il fragmente le flot d'octets entrant en messages qu'il passe à la couche Internet.
 - À l'arrivée, le processus TCP destinataire réassemble les messages reçus en un flot de sortie.
- TCP assure aussi un contrôle de flux pour éviter qu'un émetteur rapide ne submerge un récepteur lent de plus de paquets que celui-ci ne peut en traiter.

Transmission Control Protocol (TCP)

- **Établissement de la connexion**

- Tout d'abord, une connexion est ouverte entre le client et le serveur.

- **Transfert des données**

- Une fois que la connexion est établie, le protocole procède à l'envoi des messages.
- Pour accélérer la transmission et faire en sorte que l'émetteur n'attende pas de recevoir l'accusé de réception pour envoyer le message suivant, une notion de fenêtre glissante est utilisée.
- Le protocole TCP permet donc des acquittements groupés.

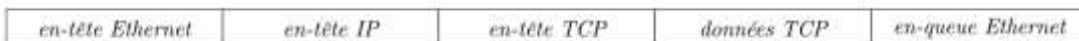
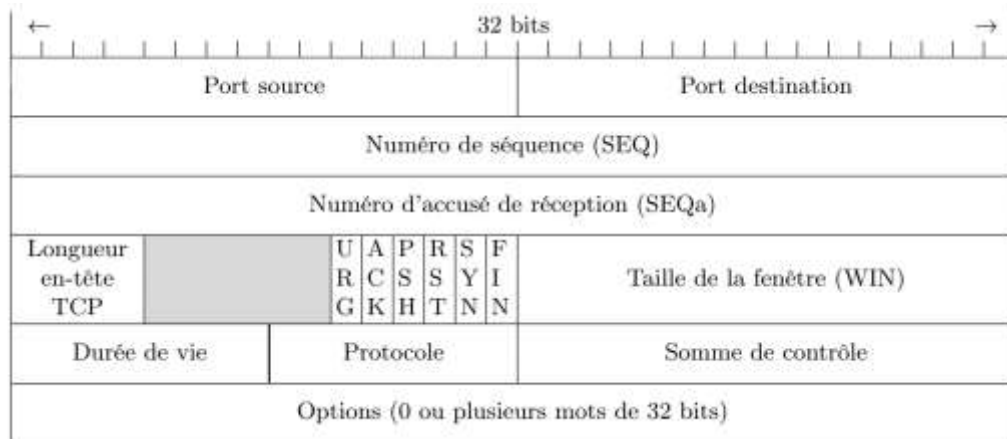
- **Déconnexion**

- Après communication, la connexion est terminée normalement par un dialogue entre le client et son serveur, avec une annonce de fin d'envoi, et l'accusé de réception correspondant

Transmission Control Protocol (TCP)

- En-tête TCP

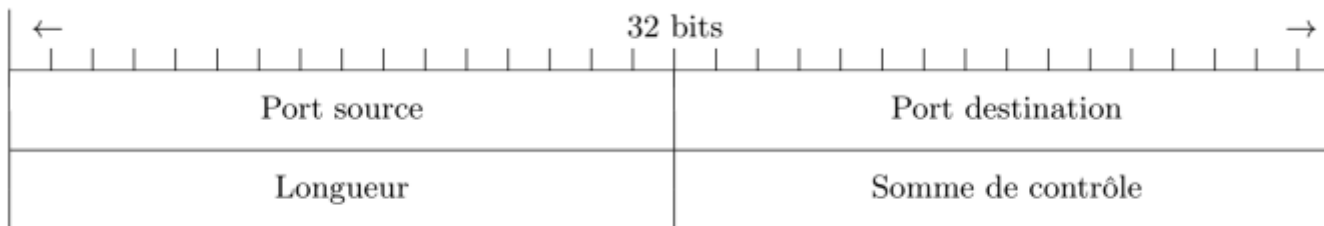
- Les messages TCP sont encapsulés dans IP.
- Le format TCP est le suivant



- **Port source** : numéro de port source.
- **Port destination** : numéro de port destination.
- **Numéro de séquence** : indique le numéro du premier octet transmis dans le message. À l'ouverture de connexion un numéro de séquence initial (ISN, Initial Sequence Number) est attribué d'une manière aléatoire.
- **Numéro d'accusé de réception** : contient le numéro de la séquence du prochain octet attendu.
- **Longueur de l'en-tête** : indique la longueur de l'en-tête TCP en mot de 4 octets.
- Six bits de drapeaux :
 - **URG** (Urgent) : si positionné, indique que la valeur du champ message urgent est significative,
 - **ACK** (Acknowledgement) : si positionné, indique que la valeur du champ acquittement est significative,
 - **PSH** (Push) : Les données reçues doivent être transmises immédiatement à la couche supérieure,
 - **RST** (Reset) : fermeture de la connexion suite à une erreur,
 - **SYN** (Synchronise) : ouverture de la connexion,
 - **FIN** (Finish) : fin de la connexion.
- **Fenêtre** : indique le nombre d'octets que le récepteur peut accepter. Ce champ permet de gérer le contrôle de flux. Ainsi la valeur de la fenêtre indique à l'émetteur le nombre d'octets qu'il peut envoyer sans que ceux-ci soient acquittés.
- **Pointeur message urgent** : indique des octets qui doivent être traités en priorité

User Datagram Protocol (UDP)

- Le protocole UDP (User Datagram Protocol) est un protocole de transport non orienté connexion ; il opère sans confirmation. Il y a donc seulement la phase d'envoi des données.
 - Cela permet de gagner en débit pour les transmissions gourmandes, telles que vidéos et sons
- En-tête UDP.
 - Les messages UDP sont encapsulés dans IP.
 - Le format UDP est le suivant.



- Port source,
- Port destination,
- Longueur : indique la longueur totale du message (données et en-tête compris).
- Somme de contrôle : FCS pour protéger le message UDP.

Couche Application

- Les protocoles de la couche Application seront traités dans d'autres cours.
- Une liste des principaux protocoles de cette couche est néanmoins donnée ci-dessous :
 - **SMTP** (Simple Mail Transfer Protocol) est un protocole de transfert simple, utilisé par la messagerie électronique (e-mail). Il repose sur TCP et IP.
 - **POP3** (Post Office Protocol 3) est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.
 - **IMAP** (Internet Message Access Protocol) permet aux messages électroniques d'être stockés et conservés sur le serveur de messagerie, plutôt que d'être transférés sur le poste client.
 - **HTTP** (HyperText Transfer Protocol) est un protocole de communication client-serveur développé pour le World Wide Web.
 - **HTTPS** (Secure HyperText Transfer Protocol) est la variante de HTTP sécurisée par l'utilisation des protocoles SSL ou TLS.
 - **FTP** (File Transfer Protocol) est un protocole de communication destiné à l'échange de fichiers sur le réseau.

Architecture réseau

Architecture réseau

- Définition

- Le terme architecture réseau est utilisé pour identifier l'ensemble des principes qui aident à la conception et à la mise en œuvre des réseaux.
- L'architecture d'un réseau décrit principalement les équipements de connexion, les ressources logicielles, les méthodes d'accès, les protocoles et les liaisons qu'il utilise pour la transmission des données.

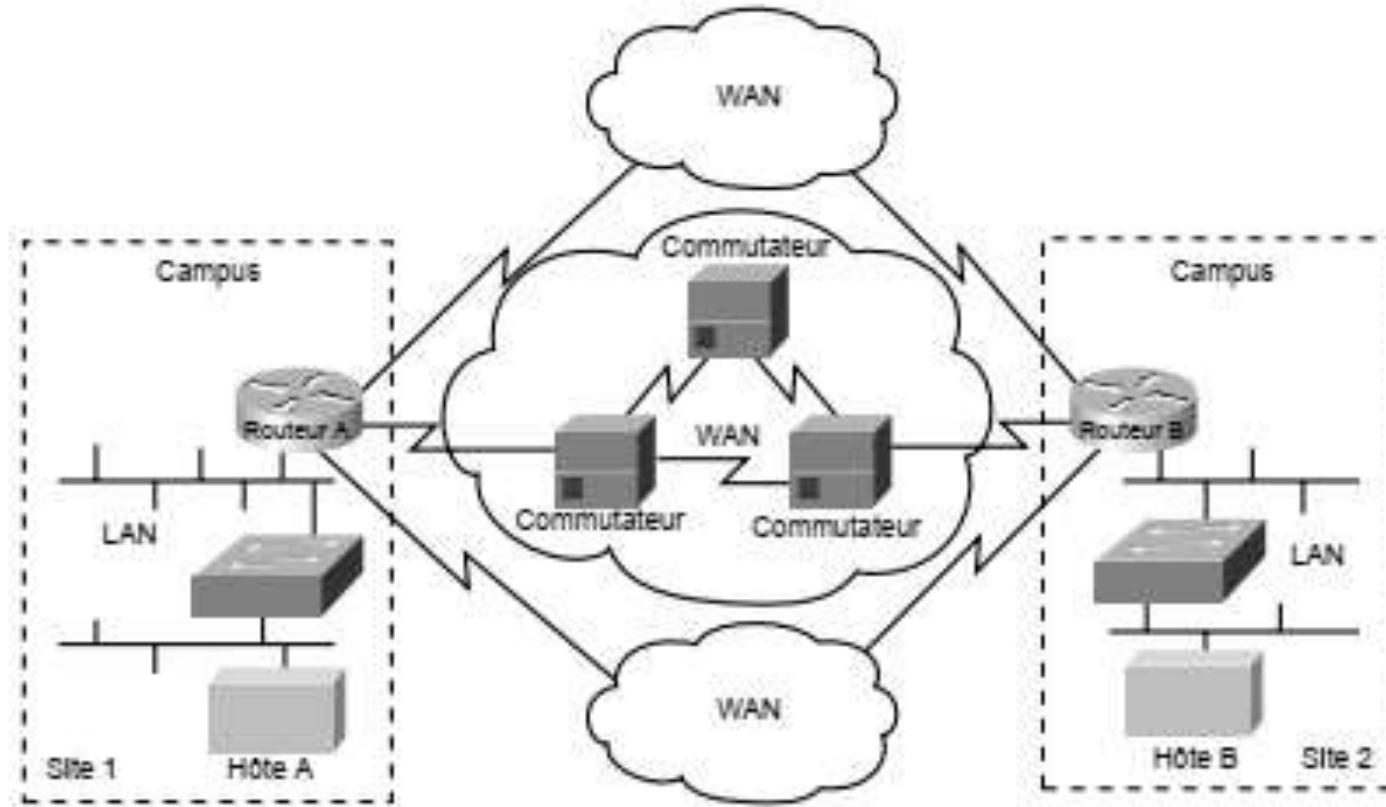
L'interconnexion de réseaux

- L'interconnexion de réseaux permet à deux réseaux ou plus de communiquer et englobe tous les aspects de la connexion des ordinateurs entre eux
- Les réseaux se sont développés pour pouvoir répondre à des exigences de communication entre systèmes terminaux très variés.
 - Ils nécessitent la mise en œuvre de nombreux protocoles et fonctionnalités pour pouvoir rester évolutifs et être administrés sans qu'il soit nécessaire de recourir en permanence à des interventions manuelles.
- Les réseaux de grande taille peuvent se composer des trois éléments suivants :
 - les réseaux de campus, qui comprennent les utilisateurs connectés localement, au sein d'un immeuble ou d'un groupe d'immeubles ;
 - les réseaux étendus (WAN, Wide Area Network) qui relient des campus ;
 - les technologies de connexion à distance, qui relient les bureaux de succursales et les utilisateurs isolés (itinérants et télétravailleurs) à un campus local ou à l'Internet.

Exemple de réseau d'entreprise

Figure 1.1

Un exemple de réseau d'entreprise type.

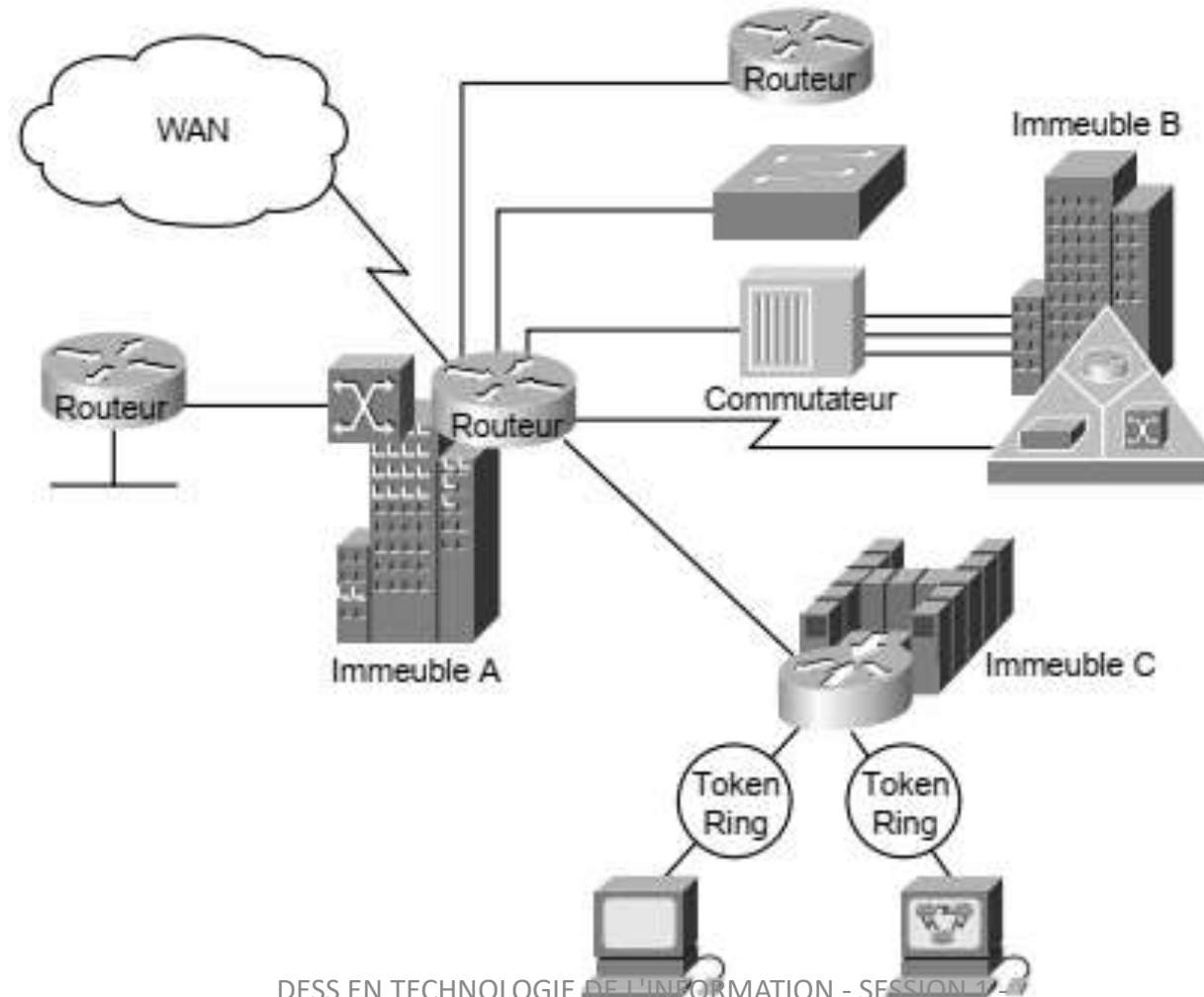


Conception d'un réseau de campus

- Un réseau de campus raccorde un immeuble ou un groupe d'immeubles à un réseau d'entreprise qui comprend plusieurs réseaux locaux (LAN, Local Area Network).
 - Il concerne généralement une portion d'une entreprise (mais pourrait tout aussi bien en couvrir la totalité) limitée à une zone géographique fixe.
- La caractéristique propre à un environnement de campus est que l'entreprise propriétaire du réseau possède en général également le câblage.
 - Sa topologie suit principalement une technologie de réseau local qui interconnecte tous les systèmes terminaux au sein d'un immeuble, comme Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface), Fast Ethernet, Gigabit Ethernet ou ATM (Asynchronous Transfer Mode).
- Un grand campus peut aussi exploiter une technologie de réseau étendu (WAN) pour raccorder des immeubles entre eux.
 - Bien qu'il utilise le câblage et les protocoles propres à cette technologie, il échappe aux contraintes de coût élevé de la bande passante.
 - Après l'installation du câblage, la bande passante se révèle peu coûteuse, car l'entreprise en est propriétaire et n'a donc pas à supporter les frais récurrents d'un fournisseur de services.
 - Faire évoluer le câblage reste toutefois une opération onéreuse.

Exemple de réseau de campus.

Figure 1.2
Exemple de réseau de campus.

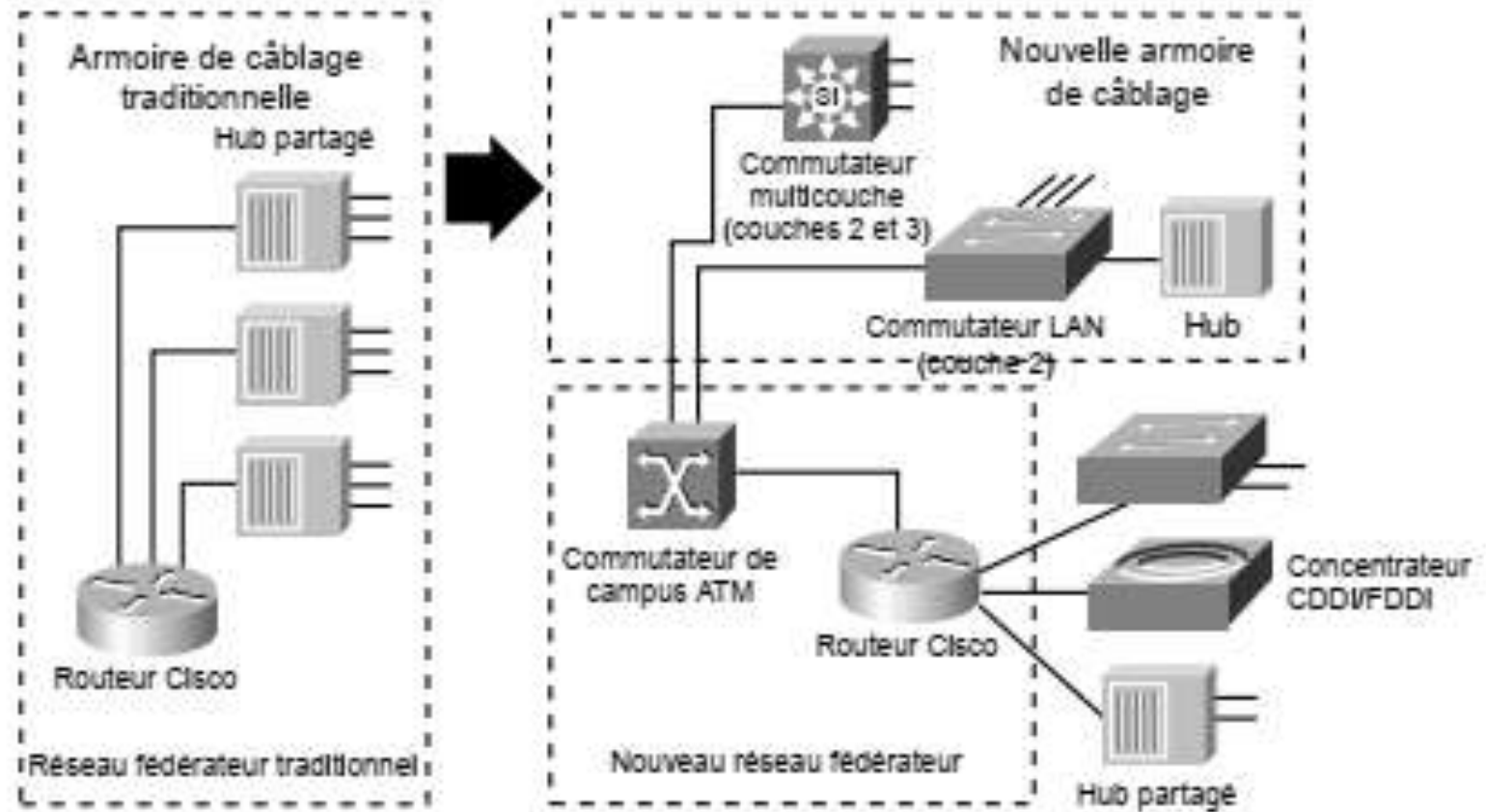


Tendances de conception

- Par le passé, les concepteurs ne disposaient que d'un nombre limité d'options matérielles, à savoir routeurs ou hubs, lorsqu'ils devaient faire l'acquisition d'une technologie pour leurs réseaux de campus. Une erreur dans la conception matérielle était donc chose rare.
- Les hubs (concentrateurs) étaient prévus pour les armoires de câblage et les routeurs pour le centre de traitement des données ou les opérations principales de télécommunication.
- Plus récemment, la technologie du réseau local a été révolutionnée par l'explosion de l'emploi de la commutation LAN au niveau de la couche 2 (liaison de données) afin d'augmenter les performances et fournir davantage de bande passante pour répondre à l'émergence de nouvelles applications de gestion de données en réseau.
 - Grâce à ces avantages, les commutateurs LAN offrent à des groupes de travail et à des serveurs locaux un débit plus élevé. Ils se trouvent aujourd'hui placés en bordure du réseau dans les armoires de câblage et sont généralement prévus pour remplacer les hubs partagés et fournir à l'utilisateur des connexions à plus large bande passante.

Tendances de conception d'un réseau de campus

Figure 1.3
Tendances de conception d'un réseau de campus.



Récapitulatif des technologies LAN

<i>Technologie LAN</i>	<i>Exploitation habituelle</i>
Technologies de routage	Le routage est une technologie essentielle pour connecter des LAN dans un réseau de campus. Il peut consister en une commutation de couche 3 ou en un routage plus traditionnel incluant la commutation de couche 3 et des fonctionnalités de routeur supplémentaires.
Gigabit Ethernet	Cette solution est implémentée au-dessus du protocole Ethernet, mais offre un débit dix fois supérieur à celui du Fast Ethernet atteignant 1 000 Mbit/s ou 1 Gbit/s. Elle fournit une grande capacité de bande passante pour concevoir des réseaux fédérateurs tout en assurant une compatibilité avec les médias installés.
Technologies de commutation LAN — Commutation Ethernet	La commutation Ethernet assure la commutation de niveau 2 et offre des segments Ethernet dédiés pour chaque connexion. Elle représente la structure de base du réseau.
Technologies de commutation LAN — Commutation Token Ring	La commutation Token Ring propose les mêmes fonctionnalités que la commutation Ethernet, mais utilise une technologie propre à l'architecture d'anneau à jeton. Vous pouvez utiliser un commutateur Token Ring comme pont transparent ou pont à routage par la source.
Commutation ATM	Elle assure la commutation à haut débit pour transporter la voix, la vidéo et les données. Son fonctionnement est semblable à la commutation LAN pour les opérations sur les données, mais elle fournit toutefois une bande passante de plus grande capacité.

Conception d'un réseau étendu (WAN)

- La communication WAN a lieu entre des zones géographiquement distantes.
- Sur un réseau d'entreprise, un réseau étendu relie des campus.
 - Lorsqu'une station souhaite communiquer avec une autre station distante (située sur un site différent), les informations doivent transiter par une ou plusieurs liaisons WAN.
 - Les routeurs situés sur les réseaux d'entreprise représentent les points de jonction LAN/WAN.
 - Ils déterminent le chemin le plus approprié pour le transport des données.
- La connexion de liaisons WAN est assurée par des commutateurs qui relaient les informations sur le réseau étendu et contrôlent le service que celui-ci fournit.
- La communication sur un réseau étendu est souvent appelée un service, car le fournisseur de réseau facture généralement aux utilisateurs les services qui sont assurés par les trois technologies de commutation principales suivantes :
 - la commutation de circuits ;
 - la commutation de paquets ;
 - la commutation de cellules.

Techniques de commutation

- Chaque technique de commutation a ses avantages et ses inconvénients.
 - La commutation de circuits offre à l'utilisateur une bande passante dédiée sur laquelle les connexions des autres utilisateurs ne peuvent empiéter.
 - La commutation de paquets est connue pour offrir une plus grande souplesse et exploiter la bande passante avec plus d'efficacité.
 - La commutation de cellules combine certains aspects des deux types de commutation précédents pour autoriser l'installation de réseaux offrant une faible latence et un débit élevé.
 - Elle a rapidement gagné en popularité, et ATM est actuellement la technologie de commutation de cellules la plus prisée.

Tendances de conception d'un WAN

- Les réseaux étendus sont connus pour leur faible débit, leurs longs délais de transmission et leur taux d'erreur élevé.
 - Ils se caractérisent également par un coût de location du média de transmission (le câblage) auprès d'un fournisseur de services.
- L'infrastructure d'un tel réseau est souvent louée, par conséquent, sa conception doit permettre d'optimiser le coût et l'efficacité de la bande passante utilisée.
- Par exemple, toutes les technologies et fonctionnalités mises en œuvre pour raccorder des campus par l'intermédiaire d'un réseau étendu sont développées pour répondre aux exigences de conception suivantes :
 - optimisation de la bande passante WAN ;
 - réduction maximale du coût des services ;
 - optimisation du service effectif pour les utilisateurs finaux.

Tendances de conception d'un WAN

- Aujourd'hui, les réseaux de médias partagés souffrent d'une surtaxe en raison des nouvelles exigences suivantes :
 - nécessité de se connecter à des sites distants ;
 - besoin croissant des utilisateurs de se connecter à distance à leur réseau d'entreprise ;
 - croissance rapide des intranets d'entreprise ;
 - utilisation accrue des serveurs d'entreprise.
- Les concepteurs de réseaux se tournent vers la technologie WAN pour répondre à ces nouveaux besoins.
 - Les connexions WAN transportent généralement des informations critiques et sont optimisées pour offrir un bon rapport performances/prix de la bande passante.
 - Les routeurs qui relient des campus, par exemple, mettent en œuvre l'optimisation du trafic, la redondance d'itinéraires, l'ouverture de lignes commutées de secours en cas de sinistre, et améliorent la qualité de service pour les applications critiques.

Récapitulatif des technologies WAN

<i>Technologie WAN</i>	<i>Exploitation</i>
ADSL (<i>Asymmetric Digital Subscriber Line</i>)	Variante du service DSL, ADSL permet d'utiliser les lignes téléphoniques existantes pour former des chemins d'accès plus rapides destinés au multimédia et aux communications de données à haute vitesse. L'utilisateur doit disposer d'un modem ADSL. Les vitesses supportées sont variables selon la distance ; elles peuvent être supérieures à 6 Mbit/s en réception et atteindre 640 Kbit/s en émission.
Modem analogique	Cet équipement peut être utilisé par les télétravailleurs et les utilisateurs itinérants qui accèdent au réseau moins de deux heures par jour, ou en tant que matériel de secours pour un autre type de liaison.
Lignes spécialisées louées	Elles peuvent être utilisées pour les réseaux PPP (<i>Point-to-Point Protocol</i>) et les topologies Hub-and-Spoke, ou comme ligne de secours pour un autre type de liaison.
RNIS	Cette technologie peut être utilisée pour fournir des accès distants rentables à des réseaux d'entreprise. Elle peut servir au transport de la voix et de la vidéo, et être utilisée comme moyen de communication de secours pour un autre type de liaison.
Frame Relay (relais de trames)	Le Frame Relay permet d'implémenter une topologie rentable à faible latence et à fort débit entre des sites distants. Il peut être utilisé à la fois pour des réseaux privés ou des réseaux d'opérateurs.
SMDS (<i>Switched Multimegabit Data Service</i>)	Ce service offre des connexions hautement performantes avec un débit élevé sur des réseaux de données publics. Il peut également être implémenté sur un réseau métropolitain (<i>MAN, Metropolitan Area Network</i>).
X.25	X.25 peut être utilisé pour fournir un circuit ou un réseau fédérateur WAN fiable. Il assure également le support des applications existantes.
ATM WAN	Cette technologie peut être utilisée pour devancer les exigences en bande passante. Elle assure également la gestion de plusieurs classes de qualité de service, afin de pouvoir distinguer les besoins des applications en cas de retards et de pertes.

Conception pour les connexions distantes

- Les connexions distantes relient des utilisateurs isolés (itinérants ou télétravailleurs) et des succursales à un campus ou à l'Internet.
- Un site distant est généralement de petite taille, possède peu d'utilisateurs, et ne requiert par conséquent qu'une liaison WAN de faible étendue.
 - Toutefois, les exigences d'un réseau en matière de communication distante impliquent habituellement un grand nombre d'utilisateurs isolés ou de sites distants, ce qui induit une augmentation de la charge WAN globale.
 - Le nombre d'utilisateurs isolés ou de sites distants est tel que le coût total de la bande passante WAN est proportionnellement plus élevé sur les connexions distantes que sur les connexions WAN.
- A la différence des connexions WAN, les petits sites ou les utilisateurs distants ont rarement besoin d'être connectés 24 h/24.
 - En conséquence, les concepteurs de réseaux choisissent habituellement entre la numérotation (dialup) et les liaisons WAN dédiées comme solution de connexion à distance.
- Un concepteur de réseau peut aussi employer des ponts sur un site distant pour leur facilité d'installation, leur topologie simple et leurs exigences de faible trafic.

Tendances de conception des connexions distantes

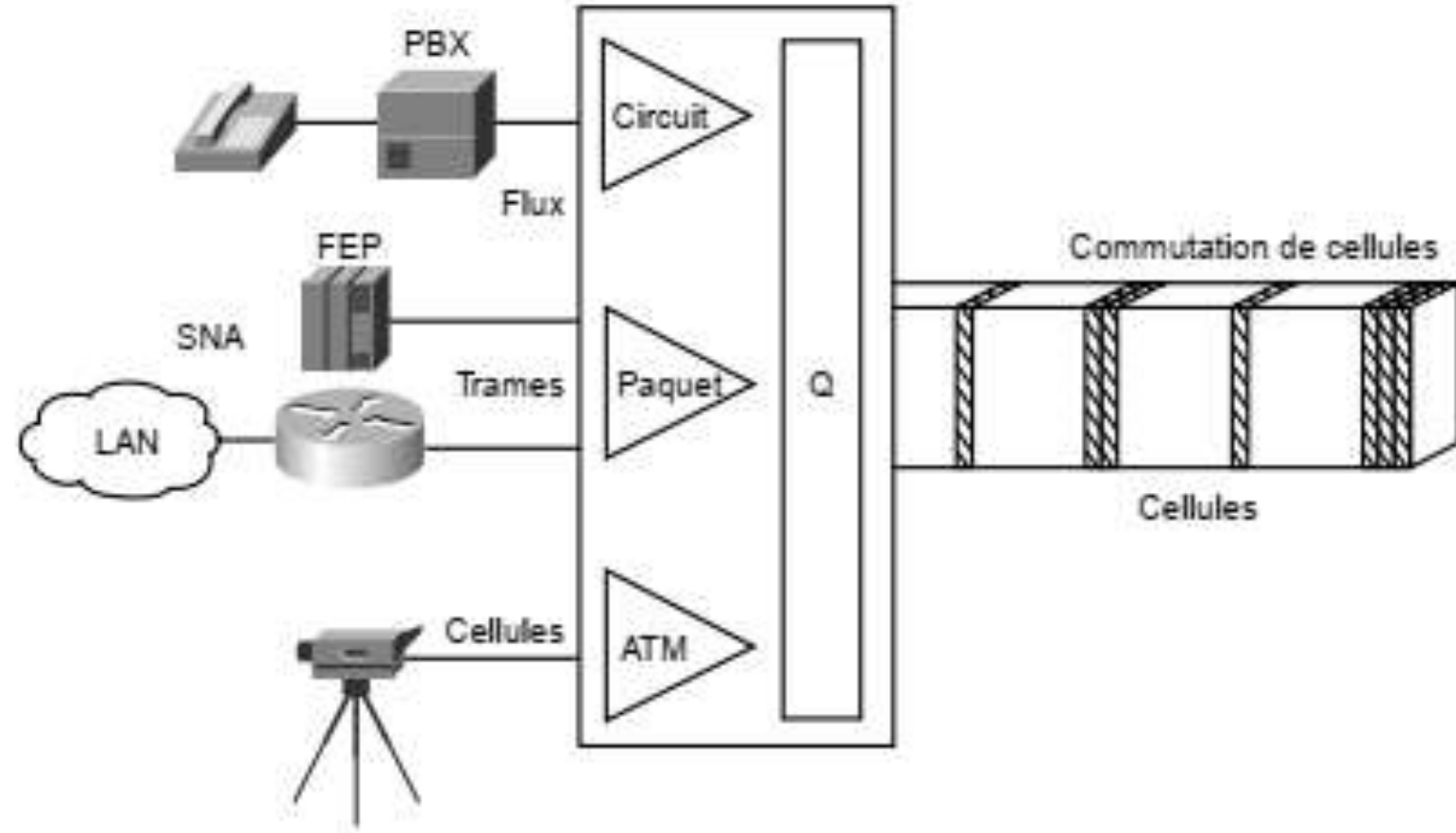
- Il existe aujourd'hui un large éventail de médias pour les réseaux WAN distants, parmi lesquels :
 - modem analogique ;
 - ADSL (Asymmetric Digital Subscriber Line) ;
 - ligne louée ;
 - Frame Relay (relais de trames) ;
 - X.25 ;
 - RNIS.
- Les connexions distantes permettent aussi un usage optimal de l'option WAN appropriée pour fournir une bande passante rentable, minimiser les coûts des services de numérotation et optimiser le service pour les utilisateurs finaux.

Tendances de l'intégration LAN/WAN

- L'Internet est la première source d'échange multimédia avec l'ordinateur personnel.
 - Il a radicalement modifié la donne en matière d'échanges.
 - Les applications concernées, transportant la voix ou la vidéo en temps réel, requièrent des performances accrues et plus prévisibles, que ce soit sur réseau local ou sur réseau étendu.
 - Ces applications multimédias commencent à compter parmi les ingrédients essentiels à une bonne productivité d'entreprise.
- A mesure que les sociétés entrevoient d'implémenter sur IP de nouvelles applications multimédias consommatrices en bande passante et basées sur des intranets — telles la formation par la vidéo, la vidéoconférence et la téléphonie —, l'impact de ces applications sur l'infrastructure de réseau existante constitue un vrai problème.
 - Par exemple, si une société s'appuie sur son réseau d'entreprise pour l'acheminement du trafic SNA de première importance et souhaite installer une application de formation en ligne par la vidéo, le réseau doit être en mesure de fournir une garantie de qualité de service pour acheminer le trafic multimédia sans l'autoriser à interférer avec le flux des informations capitales de l'entreprise.
 - ATM a été présenté comme l'une des technologies d'intégration de réseaux locaux et de réseaux étendus.
 - La qualité des fonctionnalités de service d'ATM autorise le support de n'importe quel type de trafic en flux séparés ou mixtes, qu'ils soient sensibles au retard de livraison ou non.
 - ATM peut également s'adapter pour fournir aussi bien des faibles débits que des débits élevés.
 - Il a été adopté par tous les fabricants d'équipements de l'industrie, des réseaux locaux au commutateur privé (PBX, Private Branch eXchange)

Support ATM de divers types de trafics.

Figure 1.4
Support ATM de
divers types de trafics.



Solutions intégrées

- Concernant la mise en œuvre de réseaux, la tendance actuelle est d'apporter aux concepteurs une plus grande souplesse dans la résolution de problèmes, sans qu'ils aient besoin de créer de multiples réseaux ou de faire une croix sur les investissements existants en matière de communication de données.
- Les routeurs peuvent permettre l'installation de réseaux fiables et sûrs, et servir de barrières contre les tempêtes de broadcast sur les réseaux locaux.
- Des commutateurs, que l'on peut diviser en deux catégories principales, LAN et WAN, peuvent être déployés aux niveaux groupe de travail, épine dorsale de campus ou WAN.
- Les sites distants peuvent employer des routeurs d'entrée de gamme pour se connecter au WAN.

Définition des exigences de réseau

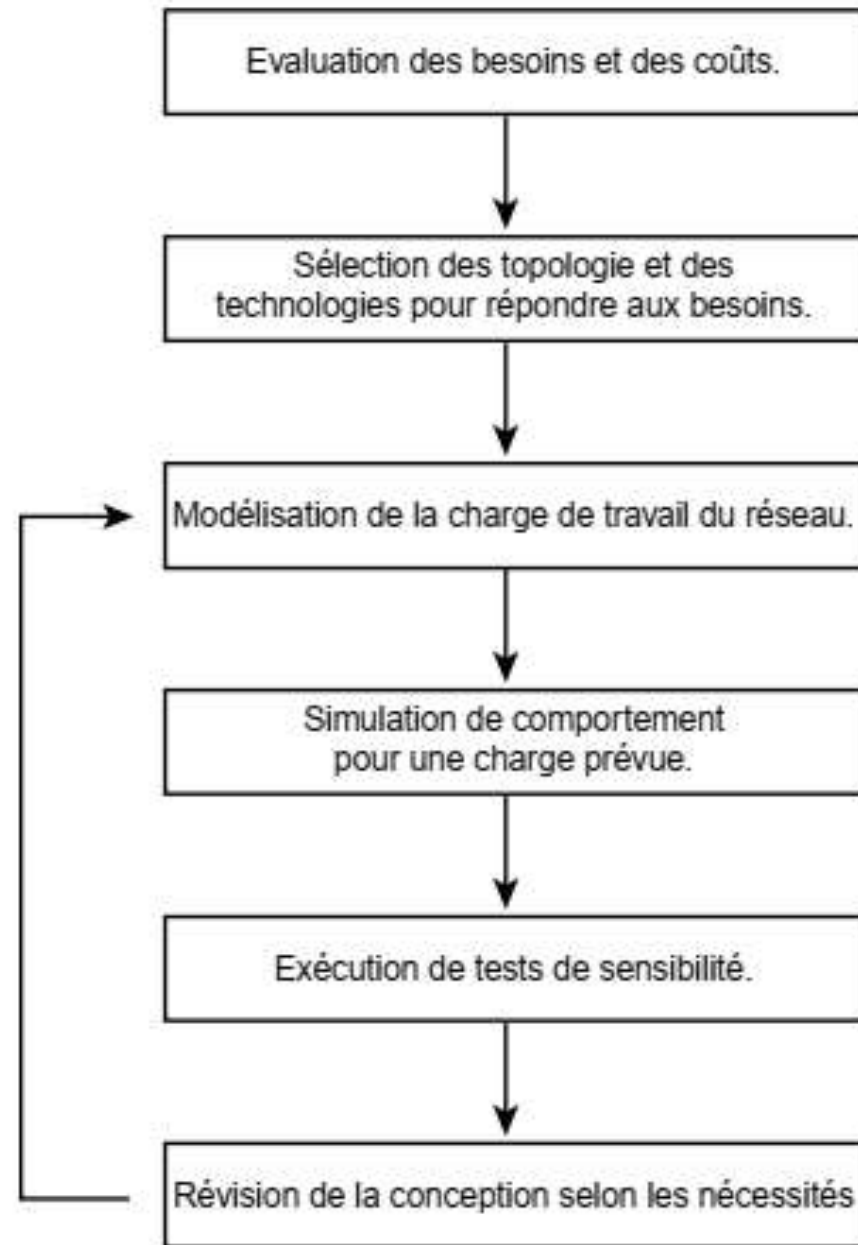
- Les équipements de réseau choisis doivent refléter les objectifs, les caractéristiques et les règles des organisations dans lesquelles ils opèrent.
- La conception d'un réseau et son implémentation doivent prendre en compte deux paramètres principaux :
 - **Disponibilité des applications.**
 - Les réseaux transportent les informations d'applications entre les ordinateurs.
 - Si les applications ne sont pas disponibles pour les utilisateurs du réseau, celui-ci ne remplit pas sa fonction.
 - **Coût de possession d'un réseau.**
 - Les budgets accordés aux systèmes d'informations se chiffrent aujourd'hui en millions de francs.
 - Etant donné que l'exploitation de grandes organisations repose de plus en plus sur des données électroniques, les coûts associés aux ressources informatiques continueront à augmenter.

Problèmes de conception : optimisation de la disponibilité et des coûts

- En général, les problèmes liés à la conception de réseaux impliquent les trois types d'éléments généraux suivants :
 - **Éléments de l'environnement.**
 - Ils comprennent l'emplacement des hôtes, des serveurs, des terminaux et autres nœuds d'extrémité ; les prévisions de trafic pour l'environnement ; les prévisions de coûts, afin de garantir différents niveaux de service.
 - **Contraintes de performances.**
 - Elles incluent la fiabilité du réseau, le débit des données transportées et les vitesses assurées par les ordinateurs hôtes/clients (par exemple, la vitesse des cartes réseau ou la vitesse d'accès aux disques durs).
 - **Éléments variables de réseau.**
 - Ils concernent la topologie du réseau, les capacités des lignes et les allocations de flux de paquets.

Figure 1.5

Processus général de conception d'un réseau.



Questions de révision

- 1- Définir: Réseaux informatique, Protocole, Bande passante, Délai, Architecture Réseau, PDU
- 2- Citer les 7 couches du modèle OSI
- 3- Citer les 4 couches de la pile de protocole TCP/IP
- 4- Citer les étapes de conception d'un réseau

Travaux pratiques

- 1- Exploration des couches OSI à l'aide de Wireshark.
- 2- Présentation du logiciel de simulation Packet Tracer