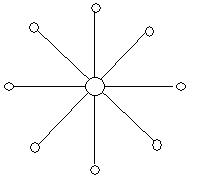
# Une histoire de mailles

## Création d’Internet

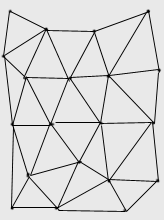
Internet a été créé au départ pour une raison bien particulière.

À l'époque, dans les années 1950, les communications étaient de point à point, c'est-à-dire qu'on ne pouvait communiquer qu'avec une seule machine à la fois. Les chercheurs qui devaient communiquer avec plusieurs autres chercheurs lors de réunions, se sont rendu compte qu'il serait intéressant de pouvoir le faire en temps réel plutôt que de passer d'un interlocuteur à l'autre successivement.

Ils ont donc cherché à créer un nouveau moyen de communication qui ne serait alors plus centralisé, mais maillé.



Cela veut dire que toute information pourrait passer par différents points, et que si certains points disparaissaient, cela n'empêcherait pas l'information de circuler. La figure suivante permet de constater qu'avec un réseau de communication maillé, si un point de communication n'est plus en état de fonctionner, l'information peut passer par un chemin différent.



Les chercheurs vont donc travailler et notamment mettre en place un réseau pour l'armée. C'est seulement au début des années 1960 que l'on voit apparaître des textes décrivant les prémices de ce que sera Internet.

À la fin des années 1960, l'Arpanet, l'ancêtre d'Internet, ne comportait que quatre machines ! Les protocoles utilisés alors ne permettaient pas d'atteindre les buts fixés, à savoir de faire dialoguer des machines provenant de différents réseaux en utilisant différentes technologies de communication.

C'est alors que les chercheurs se sont orientés vers la création d'autres protocoles de communication, et notamment TCP/IP. Internet a continué de croître au fil des années, mais c'est en 1990 qu'une révolution va permettre sa croissance réelle : le langage HTML et le protocole d'échange HTTP qui permettent la création de pages web.

Tout va s'accélérer alors avec la création des premiers navigateurs capables d'afficher des images, et la libération de l'utilisation des noms de domaine. Nous pouvons voir sur la figure suivante la progression phénoménale d'Internet dans les années 1990-2000.

# Vocabulaire, concepts de base et architecture

Le terme de réseau désigne l’organisation des connexions, appelées voies de communication, entre les différents nœuds d’un système téléinformatique. On distingue deux grandes catégories de nœuds …

* **Ordinateurs au sens large**;
* **Équipements remplissant des fonctions spécifiques** dans le réseau.

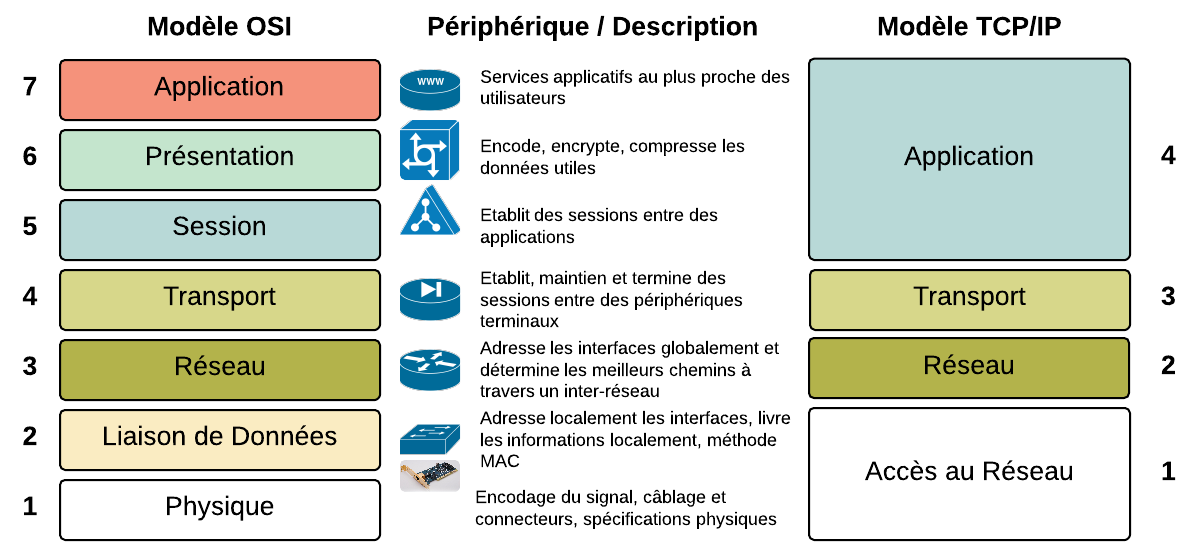
Le but d’un réseau est d’échanger des informations d’une entité à une autre via un canal de transmission. La transmission entre deux entités communicantes est caractérisée par …

* le **sens des échanges**unidirectionnel  
  bidirectionnel à l’alternat   
  ou   
  simultané
* le **mode de transmission**en série  
  en parallèle
* la **synchronisation**mode synchrone  
  mode asynchrone

Pour que l’échange des données fonctionne …

* un **codage des signaux de transmission** doit être choisi;
* des **règles communes régissant la communication** doivent être adoptées (notion de protocole)

## Modèle TCP/IP

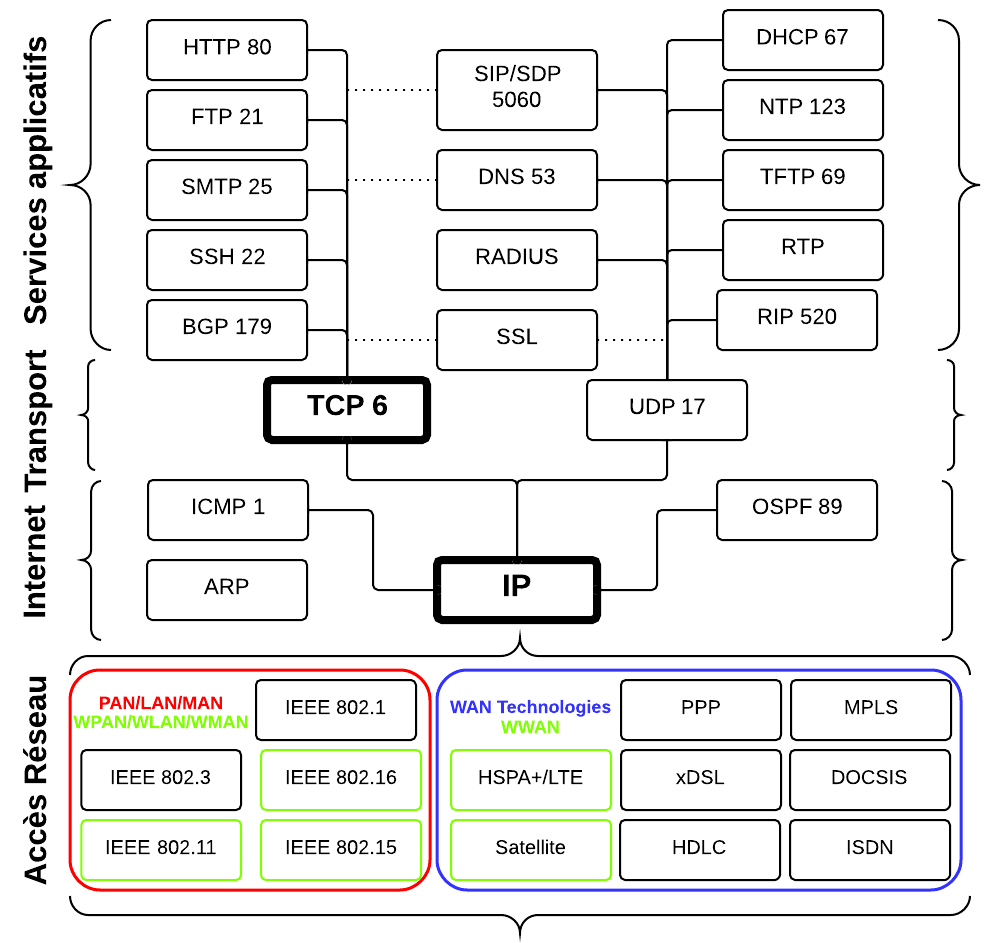


La partie de gauche représente le modèle OSI et la partie de droite représente le modèle TCP/IP et ses principaux protocoles.

Les différences pourraient se résumer comme suit …

* **Les couches 1 et 2 du modèle OSI correspondent à une seule couche du modèle TCP/IP**.   
  Malgré qu’il soit multi-platteforme, le protocole réseau IP a été conçu pour utiliser de préférence les réseaux de type Ethernet.   
  C’est pourquoi la couche accès réseau est au contraire du modèle OSI peu détaillé.
* **Les couches 5, 6 et 7 du modèle OSI sont fusionnées dans le modèle TCP/IP**.   
  Les protocoles de la couche Applications du modèle TCP/IP prennent en charge les fonctions comme l’ouverture de session, l’encodage, …, fonctions explicitement séparées dans le modèle OSI.

Il serait important de préciser à nouveau que le modèle OSI a été proposé dans le but de standardiser les étapes de communication entre deux hôtes.   
Le modèle TCP/IP quant à lui impose une série de protocoles qui par définition sont les mêmes pour tous les hôtes du réseau Internet. Ceci explique pourquoi le modèle est plus simple.



# Couche physique

Dans le domaine des réseaux informatiques, la couche physique est la première couche du modèle OSI (de l'anglais *Open Systems Interconnecti*on ou Interconnexion de systèmes ouverts).

## Principes

La couche physique est chargée de la transmission effective des signaux électriques, radiofréquences ou optiques entre les interlocuteurs.

Cette couche physique s'occupe de la transmission physique des données entre deux équipements réseaux. Elle s'occupe de tout ce qui a trait au bas-niveau, au matériel …

* la **transmission des bits** ;
* leur **encodage** ;
* la **synchronisation entre deux interfaces réseau** ;
* ...

Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.

Il existe trois catégories principales de lien de couche physique, selon le type de distance physique qu'ils permettent de faire circuler ...

* les **supports filaires** permettent de faire circuler une grandeur électrique sur un câble généralement métallique ;
* les **supports aériens** désignent l'air ou le vide, ils permettent la circulation d'ondes électromagnétiques ou radioélectriques diverses ;
* les **supports optiques** permettent d'acheminer des informations sous forme lumineuse.

Son travail est généralement limité à l'émission et la réception d'un bit ou d'un train de bits continu   
(notamment pour les supports synchrones comme la fibre optique).

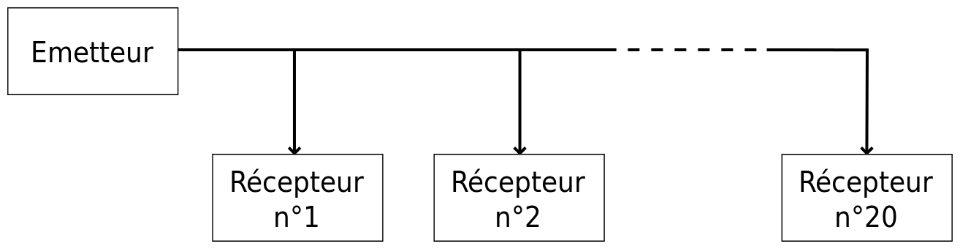
La couche physique est chargée de la conversion entre bits et signaux électriques ou optiques.  
Elle est en pratique toujours réalisée par un circuit électronique spécifique.

**Remarque** …  
Tous les supports de transmission réseau ne transfèrent qu'un bit à la fois.   
En termes techniques, on dit que ce sont des liaisons séries.   
Il existe des liaisons qui échangent plusieurs bits en même temps, les liaisons parallèles, mais ils ne sont pas beaucoup utilisés dans le domaine du réseau. Ils sont plus utilisés à l'intérieur des circuits électroniques, dans les ordinateurs ou pour relier un PC à un périphérique.   
Pour résumer, les transmissions réseaux sont des flux de bits, transmis un par un, à la file indienne.

### Bus de communication

Sur un bus, on peut connecter un nombre assez important de composants, qui dépasse largement les deux nœuds d'une liaison point à point. Avec un bus, un émetteur va envoyer ses données à tous les autres récepteurs.

Sur tous ces récepteurs, il se peut que seul l'un d'entre eux soit le destinataire du paquet : les autres vont alors ignorer le paquet, seul le destinataire traitant le paquet.   
Toutefois, il se peut qu'il y ait plusieurs récepteurs comme destinataires : dans ce cas, les destinataires vont tous recevoir la donnée et la traiter.   
Ces bus permettent donc de faire des envois de données à plusieurs composants en une seule fois.



### Affectation d’un bit lors de sa transmission

Il existe plusieurs phénomènes qui influence la qualité des transmissions.   
Ces éléments perturbateurs peuvent, soit diminuer l’efficacité du support de transport, soit le rendre totalement inopérationnel.

Parmi les plus importants, on note …

* **Propagation**  
  Temps mis par un bit pour se déplacer dans le média ;
* **Atténuation**  
  Perte de la force (amplitude) du signal ;
* **Bruit**  
  Ajout indésirable d’énergie à un signal causé par des sources d’énergie se trouvant à proximité ;
* **Dispersion**  
  Étalement des impulsions dans le temps ;
* **Gigue**  
  Variation du délai de transfert de l’information ;
* **Latence**  
  Retard de transmission causé par le temps de déplacement d’un bit dans le média et la présence de circuits électroniques dans le cheminement ;
* **Collisions**  
  Phénomène qui existe lorsque deux ordinateurs utilisant le même segment de réseau émettent en même temps.

## Réseau Local (Local Area Network)

Un LAN, pour *Local Area Network* est, comme son nom anglais l'indique, un réseau d'aire locale, ou encore un Réseau Local d'Entreprise (RLE). En fait un LAN est un réseau qui possède une couverture géographique très limitée, généralement celle d’un site ou d’un bâtiment.

**Caractéristiques**  
Voici en quelques lignes les caractéristiques essentielles d’un LAN ...

* **Couverture géographique limités**;
* **Hauts débits de transmission** (plusieurs mégabits par seconde -- Mbps).   
  Leur faible couverture géographique permet d'installer des supports physiques d'excellente qualité (affaiblissement faible, peu de diaphonie et paradiaphonie, bande passante élevée) pour la transmission de données.   
  Ces supports sont de la paire torsadée (L120, catégorie 5, etc.), de la fibre optique ou du câble coaxial (de plus en plus rare) ;
* **Réseau de diffusion** (avant l'arrivée des commutateurs (*switchs*).  
  Toute donnée émise sur le réseau est vue par tous les connectés.   
  Lorsqu'une station envoie une trame de niveau 2, cette trame est diffusée à toutes les stations présentes sur le réseau local. Cette opération est facilitée par la topologie logique (et éventuellement physique) du réseau.  
  Les stations sont connectées à un bus ou à un anneau (pour 99% des cas !). On dit que les réseaux locaux fonctionnent sur des supports partagés. Cette caractéristique est extrêmement importante car c'est elle qui oblige à la mise en place d'un adressage au niveau 2.
* **Méthode d'accès au support**  
  Chaque type de LAN met en œuvre une procédure particulière, et normalisée, d'accès au support afin d'émettre les trames. Cette procédure est communément appelée le MAC: Medium Access Control.   
  D'une manière générale étant donné que le support est partagé entre toutes les stations d'un réseau local, seule une trame à la fois est véhiculée par le support. Le MAC veille donc à donner équitablement la parole à chaque station, et bien sûr détecte les éventuelles cacophonies si certaines stations ne respectent pas le jeu.

Pour la suite de ce document, il est important de retenir que ...

* un **LAN est un réseau de diffusion qui partage son suppor**t entre toutes les stations présentes   
  (technologie logique du bus) ;
* un L**AN implémente une procédure de niveau 2 nommée MAC** qui définit un format de trame et gère la méthode d'accès au support ;
* en raison de la caractéristique de diffusion, le **MAC défini un adressage de niveau 2 pour les trames**   
  (adresse de destination et adresse source).

### Mode de transmission

* **Diffusion dirigée (*Unicast*)**   
  Adresse MAC -- 0A:00:81:2F:42:51  
  Adresse désignant une seule interface ;
* **Multi diffusion (Multicast)**   
  Adresse MAC -- 01:XX:XX:XX:XX:XX (premier octet impair)  
  Adresse désignant plusieurs stations (groupe de diffusion) ;
* **Adresse de diffusion globale (Broadcast address)**  
  Adresse MAC -- FF:FF:FF:FF:FF:FF  
  Adresse de diffusion qui désigne l’ensemble des stations du domaine de collision.concerné

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Monodiffusion (**unicast**) | Multidiffusion (*multicast*) | Diffusion générale (*broadcast*) |

# Couche réseau

## Définition

La couche réseau construit une voie de communication de bout à bout à partir de voies de communication avec ses voisins directs. Ses apports fonctionnels principaux sont donc …

* le **routage**  
  Détermination d'un chemin permettant de relier les 2 hôtes distants ;
* le **relayage**  
  Retransmission d'un PDU (*Protocol Data Unit* ou Unité de données de protocole) dont la destination n'est pas locale pour le rapprocher de sa destination finale.

Cette couche est donc la seule à être directement concernée par la topologie du réseau.   
C'est aussi la dernière couche supportée par tous les hôtes du réseau pour le transport des données utilisateur : les couches supérieures sont réalisées uniquement dans les machines d'extrémité.

Le PDU de cette couche est souvent appelé paquet. La fonction de relayage (terme OSI) est parfois appelée acheminement.

**Remarques** …  
Cette couche est la plus caractéristique d'une architecture réseau.   
C'est pourquoi l'architecture prend souvent le nom du protocole principal de niveau réseau.

Déterminer un chemin est une tâche complexe normalement réalisée dans les grands réseaux par des protocoles dédiés dont le rôle est de découvrir la topologie du réseau et d'en tirer la meilleure route. Les protocoles de routage se différencient par les critères de choix des routes et la précision de la topologie découverte. En dehors du cas des petits réseaux, le routage est hiérarchique : la précision de la connaissance de l'environnement d'un routeur décroît avec la distance.

Si les routeurs n'ont pas de couche supérieure à la couche réseau du point de vue des hôtes utilisateurs du réseau, ils peuvent supporter des protocoles de niveau transport et au-dessus pour la gestion du réseau (supervision et exécution des protocoles de routage par exemple).   
Bien que les données calculées par les protocoles de routage soient utilisées par la couche réseau, ce ne sont pas des protocoles de niveau réseau car ils ne servent pas à transporter les données des hôtes utilisateurs du réseau. D'ailleurs, dans le monde IP, les protocoles de routage non local (i.e. hors RIP) sont transportés par TCP.

Voici les principaux protocoles de la couche Réseau …

* **Protocoles IP** (v4 et v6) ;
* **Protocole ARP** ;
* **Protocole ICMP** ;
* **Protocole IGMP**.

## Le protocole IP (v4 et v6)

Les protocoles TCP/IP se situent dans un modèle souvent nommé famille de protocoles TCP/IP.  
Les protocoles TCP et IP ne sont que deux des membres de la suite de protocoles IP.

Le protovole IP (*Internet Protocol*) est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisé sans connexion. Le terme optimisé souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. La fonctionnalité de somme de contrôle du protocole ne confirme que l'intégrité de l'entête IP. Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP (et de leur ordre de réception).

Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis par le niveau 3 sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

### Principes guidant IP

Dès l’origine deux principes de base ont guidés les concepteurs d’Internet pour la création du protocole de transport (en occurrence IP). Ces deux principes sont les suivants …

* La **communication de bout en bout**  
  Une communication se fait entre deux partenaires et ce sont ces derniers qui en gèrent les modalités. On sait que la commutation des paquets implique la présence de plusieurs intervenants intermédiaires (souvent désignés comme aiguilleurs dans le langage Internet) et que ces intermédiaires sont transparents et ne participent pas dans la communication (en fait ils ne sont que des relais).  
  Les nœuds d’extrémités sont considérés comme intelligents, permettant ainsi le déploiement d’applications client/serveur à l'aide du réseau.
* La **livraison au meilleur effort**Ce principe implique que tous les éléments intermédiaires (aiguilleurs) de la connexion n’offre aucune garantie quant au transport des paquets entre les nœuds d’extrémités. Ils « font de leur mieux » pour rendre les paquets à destination. IP n’est donc pas selon ce principe un protocole fiable. Toutefois, on le considère comme étant robuste. Agissant ainsi le protocole n’utilise pas de ressources supplémentaires aux intermédiaires pour fournir une qualité de service à priori.   
  Seulement les nœuds d’extrémités vont utiliser un protocole de la couche Transport du modèle OSI pour garantir cette livraison (ce qui n’est pas le cas des nœuds intermédiaires).  
  C’est pourquoi le protocole TCP est implicitement lié au protocole IP.

### **Configuration IP**

Toute configuration IP doit comporter les données suivantes …

* l’**adresse IP**   
  (unique à l’hôte) ;
* le **masque de sous-réseau** ;
* l’**adresse** **de la passerelle par défaut**   
  (un aiguilleur est traditionnellement appelé ainsi pour le réseau Internet).  
  La passerelle est la porte d’entrée sur le réseau Internet ;
* l’**adresse** **d’un serveur DNS**  
  Le serveur DNS est l’intermédiaire qui résout un nom convivial comme www.profsavard.info en une adresse valide de destination comme 206.167.36.22.

Toute configuration IP valide doit obligatoirement comporter les deux premiers éléments.   
Sans ces informations il sera impossible pour un hôte de communiquer avec un hôte distant (qu’il soit dans son propre réseau ou sur le réseau Internet).   
Quant au troisième il est essentiel si un hôte veut communiquer avec un hôte distant hors de son propre réseau local.   
Enfin, sans le quatrième élément, l’utilisateur devra toujours connaître l’adresse exacte pour rejoindre un hôte en dehors de son réseau local.

### Adresses IPv4

Pour pouvoir établir une communication avec un autre hôte branché au réseau Internet une machine (ou nœud) doit obligatoirement posséder une adresse IP unique.

Cette adresse peut être caractérisée comme étant statique ou dynamique.

* Une **adresse statique est généralement attribuée manuellement** par un administrateur réseau.   
  Certains nœuds du réseau Internet nécessitent une adresse qui ne sera pas modifiée (ce qui est le cas de la plupart des serveurs).
* Une **adresse dynamique est une adresse qui sera attribuée de manière automatique** lors de l’ouverture d’un hôte.   
  Cette adresse est généralement attribuée par un serveur DHCP[[1]](#footnote-2).

Plusieurs avantages liés à la présence d’un serveur DHCP …

* **Attribution automatique de la configuration IP** à un hôte;
* **Résolution du problème d’un réseau** qui possède plus d’hôtes que d’adresses disponibles.

## Internet Protocol version 6 (IPv6)

Au début des années 90, l’évolution du réseau Internet semblait compromise à court terme car le protocole IP (Internet Protocol) limitait le nombre d’équipements qui pouvaient s’y connecter.

À sa création, ce réseau ne devait servir qu’à relier une centaine de machines mais de nombreuses catégories d’utilisateur sont très vite venues s’y joindre. On y trouvait les scientifiques, les universitaires, puis en 1992, le réseau fut ouvert aux activités commerciales ainsi qu’aux particuliers. Depuis, le nombre d’équipements connectés ne cesse d’augmenter et on approche de la saturation du réseau.

Les chercheurs ont repoussé cette saturation afin de développer une nouvelle version du protocole IP qui sera nommé IPv6. IPv6 prend en compte les avancées issues des recherches sur les réseaux menées depuis 25 ans.

Elle porte notamment sur …

* l’**auto configuration** ;
* la **mobilité** ;
* la **diffusion multipoints**  
  et
* la **sécurité**.

IPv6 est le protocole de la prochaine génération d'Internet et c'est pour cela qu'on l'appelle aussi IPng, initiales de ***Internet Protocol Next Generation***.  
On s'attend à ce que IPv6 remplace graduellement IPv4, avec une période de transition de plusieurs années de coexistence.

## Protocole ICMP

ICMP (*Internet Control Messaging Protocol*) est le protocole de gestion de la suite TCP/IP, qui est requis dans chaque mise en œuvre TCP/IP et autorise deux nœuds d'un réseau IP à partager des informations d'erreur ainsi que l'état IP.   
ICMP est utilisé par l'utilitaire *ping* pour déterminer l'accessibilité d'un système distant

Avec ICMP, les hôtes et les aiguilleurs (*routers*) qui utilisent la communication IP peuvent faire état des erreurs et échanger des informations sur le contrôle limité et sur l'état.

Les messages ICMP sont généralement envoyés automatiquement dans l'un des cas suivants ...

* Un p**aquet (datagramme) IP ne peut pas atteindre sa destination** ;
* Un **aiguilleur IP (passerelle) ne peut pas transmettre les paquet**s et donne des informations sur l'état de la transmission ;
* Un **aiguilleur IP redirige l'hôte d'envoi pour utiliser un meilleur itinéraire** vers la destination.

## Protocole IGMP (Multidiffusion)

En informatique, le terme multi-diffusion (*multicast*) définit une connexion réseau multipoint.

### Définition

On entend par multi-diffusion le fait de communiquer simultanément avec un groupe d'ordinateurs identifiés par une adresse spécifique (adresse de groupe).

### Avantages

L'avantage de ce système par rapport à la classique monodiffusion (*unicast*) devient évident quand on veut diffuser de la vidéo. En streaming on envoie une image autant de fois que l'on a de connexions simultanées. Comme résultat ... moins de perte de temps, de ressources du serveur et surtout de bande passante.

En multidiffusion le paquet n'est émis qu'une seule fois et sera aiguillé (routé) vers tous les hôtes du groupe de diffusion.

### Protocoles

En multidiffusion, le protocole IP utilise les adresses de la classe d'adresses D (224.0.0.1 à 239.255.255.254).   
Les adresses IP de multidiffusion 224.0.0.1 à 224.0.0.255 ont un rôle spécifique à utilisation locale.

Les paquets de données sont aiguillés sur le réseau selon l'adresse des destinataires encapsulée dans la trame transmise. Normalement, seuls les destinataires interceptent et décodent les paquets qui leurs sont adressés.

Exemple d'une adresse IP locale pouvant servir à une communication de multidiffusion …  
224.0.0.1 ;   
Exemple d'une adresse IP Internet pouvant servir à une communication de multidiffusion …  
239.254.254.254.

Un groupe de multidiffusion se compose d'un ensemble d’hôtes. Il est entièrement dynamique (un hôte peut rejoindre ou quitter le groupe à tout moment) et ouvert (une station peut émettre un paquet dans un groupe sans en faire partie).

Un groupe de multidiffusion est désigné par une adresse IP (de 224.0.0.1 à 239.255.255.255).   
Lorsqu'un hôte veut envoyer un paquet à un groupe multidiffusion, il envoie ce paquet à l'adresse IP identifiant ce groupe (par ex : 224.1.2.3). La réception est réalisée par un aiguilleur abonné au groupe et le paquet est alors dupliqué et renvoyé grâce à une trame de niveau 2 Multicast.

Le protocole IGMP est utilisé par le protocole IP pour l'adhésion aux groupes de multidiffusion.

### Utilisation

L'usage de la multidiffusion sur Internet est encore limité aux universités ou utilisé en interne par les fournisseurs d'accès Internet (diffusion des chaînes de télévision pour certains).  
Certaines radio web expérimentent un flux de multidiffusion pour la diffusion de leurs programmes.

# Couche Transport

La couche transport remplit également d’autres fonctions …

* Elle permet à de **nombreuses applications de communiquer sur le réseau au même moment**, sur un même périphérique ;
* elle **vérifie**, si cela est nécessaire, **que toutes les données sont reçues de façon fiable et dans l’ordre** par l’application voulue ;
* elle **utilise des mécanismes de gestion des erreurs**.

## Rôle et fonction de la couche transport

### Rôles de la couche transport

La couche transport segmente les données et se charge du contrôle nécessaire au réassemblage de ces blocs de données ans les divers flux de comunication. Pour ce faire, il doit …

* effect**uer un suivi des communications individuelles entre les applications** résidant sur les hôtes source et de destination ;
* **segmenter les données et gérer chaque bloc individuel** ;
* **réassembler les segments en flux de données d’application** ;
* **identifier les différentes applications**.

**Suivi des conversations individuelles**   
Tout hôte peut héberger plusieurs applications qui communiquent sur le réseau. Chacune de ces applications communique avec une ou plusieurs applications hébergées sur des hôtes distants.   
Il incombe à la couche Transport de gérer les nombreux flux de communication entre ces applications.

**Segmentation des données**   
Chaque application crée un flux de données à envoyer vers une application distante. Ces données doivent donc être préparées pour être expédiées sur le support sous forme de blocs faciles à gérer.   
Les protocoles de la couche transport décrivent les services qui segmentent les données provenant de la couche application. Il s’agit notamment de l’encapsulation devant s’appliquer à chaque bloc de données.   
Des en-têtes doivent être ajoutés à chaque bloc de données d’application au niveau de la couche Transport pour indiquer à quelle communication il est associé.

**Reconstitution des segments**   
L’hôte recevant les blocs de données peut les diriger vers l’application appropriée.   
Il faut en outre que ces blocs de données individuels puissent être réassemblés dans un flux de données complet utile à la couche Application.   
Les protocoles intervenant au niveau de la couche Transport gèrent la façon dont les informations d’entête de la couche Transport servent à réassembler les blocs de données en flux qui seront transmis à la couche Application.

**Identification des applications**   
Pour que les flux de données atteignent les applications auxquelles ils sont destinés, la couche Transport doit identifier l’application cible. Pour cela, la couche Transport affecte un identificateur à chaque application.   
Les protocoles TCP/IP appellent cet identificateur un numéro de port. Chaque processus logiciel ayant besoin d’accéder au réseau se voit affecter un numéro de port unique sur son hôte. Ce numéro de port est inclus dans l’entête de la couche Transport afin de préciser à quelle application ce bloc de données est associé.

La couche Transport fait le lien entre la couche Application et la couche inférieure responsable de la transmission réseau. Cette couche accepte les données provenant de plusieurs conversations et les fait descendre vers les couches inférieures sous forme de blocs faciles à gérer pouvant au final faire l’objet d’un multiplexage sur le support.   
Les applications n’ont pas besoin de connaître les détails du fonctionnement du réseau utilisé. Les applications génèrent des données qui sont envoyées d’une application à une autre sans se soucier du type de l’hôte de destination, du type de support que les données doivent emprunter, du chemin suivi par ces données, de l'encombrement d’une liaison ni de la taille du réseau.

En outre, les couches inférieures ignorent ce que les applications envoient comme données sur le réseau. Leur responsabilité se limite à livrer les données au périphérique approprié.   
La couche transport trie ensuite ces blocs avant de les acheminer vers l’application voulue.

**Variabilité des besoins en données**  
Parce que des applications différentes ont des besoins différents, il existe plusieurs protocoles pour la couche Transport. Dans le cas de certaines applications, les segments doivent arriver dans un ordre bien précis pour être traités correctement. Pour d’autres applications, il faut que toutes les données soient arrivées pour qu’il soit possible de traiter n’importe laquelle d’entre elles. D’autres applications, enfin, tolèrent la perte d’une certaine quantité de données lors de la transmission sur le réseau.

**Séparation de communications multiples**  
Un hôte connecté à un réseau peut envoyer et recevoir simultanément des courriels et messages instantanés, afficher des sites Web et passer un appel téléphonique par voix sur IP. Chacune de ces applications envoie des données sur le réseau et en reçoit simultanément.   
Pourtant, les données de l’appel téléphonique ne sont pas orientées vers le fureteur Web et le texte des messages instantanés ne finit pas dans un courriel.  
De plus, les informations contenues dans un courriel ou une page Web doivent avoir été intégralement reçues et affichées pour présenter un intérêt pour l’utilisateur.   
On considère certains retards comme acceptables pour veiller à ce que l’ensemble des informations soit reçu et présenté.

### Fonctions de la couche Transport

Tous les protocoles de la couche Transport ont des fonctions essentielles communes …

**Segmentation et reconstitution**  
La plupart des réseaux limitent la quantité de données pouvant être incluses dans une même unité de données de protocole. La couche Transport divise les données d’application en blocs de données d’une taille adéquate.   
Une fois ces blocs parvenus à destination, la couche Transport réassemble les données avant de les envoyer vers l’application ou le service de destination.

**Multiplexage de conversations**De nombreux services ou applications peuvent s’exécuter sur chaque hôte sur le réseau. Une adresse, appelée port, est affectée à chacun de ces services ou applications afin que la couche transport puisse déterminer à quel service ou application les données se rapportent.

**Établissement d’une session**   
La couche Transport est en mesure d’orienter la connexion en créant des sessions entre les applications. Ces connexions préparent les applications à communiquer entre elles avant le transfert des données. Dans ces sessions, il est possible de gérer avec précision les données d’une communication entre deux applications.

**Acheminement fiable**Bien des circonstances peuvent entraîner la corruption ou la perte d’un bloc de données lors de son transfert sur le réseau. La couche transport veille à ce que tous les blocs atteignent leur destination en demandant au périphérique source de retransmettre les données qui ont pu se perdre.

**Livraison dans un ordre défini**  
Étant donné que les réseaux fournissent une multitude de routes dont les délais de transmission varient, il se peut que les données arrivent dans le désordre.   
En numérotant et en ordonnant les segments, la couche transport s’assure que ces segments sont réassemblés dans le bon ordre.

**Contrôle du flux**  
Les hôtes du réseau disposent de ressources limitées, par exemple en ce qui concerne la mémoire ou la bande passante. Quand la couche Transport détermine que ces ressources sont surexploitées, certains protocoles peuvent demander à l’application qui envoie les données d’en réduire le flux.   
Ceci s’effectue au niveau de la couche Transport en régulant la quantité de données que la source transmet sous forme de groupe. Le contrôle du flux contribue à prévenir la perte de segments sur le réseau et à rendre inutiles les retransmissions.

## Protocole TCP

TCP (qui signifie *Transmission Control Protocol*, soit en français: Protocole de Contrôle de Transmission) est un des principaux protocoles de la couche Transport du modèle TCP-IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP).

Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP, en fixant le champ protocole à 6 (pour savoir que le protocole en amont est TCP).

TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux hôtes qui communiquent de contrôler l'état de la transmission.

Les caractéristiques principales du protocole TCP sont les suivantes :

* TCP permet de **remettre en ordre les datagrammes en provenance du protocole IP**;
* TCP permet de **vérifier le flot de données afin d'éviter une saturation du réseau** ;
* TCP permet de **formater les données en segments de longueur variable** afin de les remettre au protocole IP;
* TCP permet de **multiplexer les données**, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne;
* TCP permet enfin l'**initialisation et la fin d'une communication de manière courtoise**.

### Objectif de TCP

Grâce au protocole TCP, les applications peuvent communiquer de façon sûre (grâce au système d'accusés de réception du protocole TCP), indépendamment des couches inférieures. Cela signifie que les aiguilleurs (qui travaillent sur la couche Réseau) ont pour seul rôle l'acheminement des données sous forme de datagrammes, sans se préoccuper du contrôle des données, car celui-ci est réalisé par la couche Transport (plus particulièrement par le protocole TCP).

Lors d'une communication à travers le protocole TCP, les deux hôtes doivent établir une connexion.   
L’hôte émetteur (celui qui demande la connexion) est appelé client, tandis que l’hôte récepteur est appelé serveur.   
On dit qu'on est alors dans un environnement client-serveur.

Les hôtes dans un tel environnement communiquent en mode connecté, c'est-à-dire que la communication se fait dans les deux sens.   
Pour permettre le bon déroulement de la communication et de tous les contrôles qui l'accompagnent, les données sont encapsulées, c'est-à-dire qu'on ajoute aux paquets de données un en-tête qui va permettre de synchroniser les transmissions et d'assurer leur réception.

Une autre particularité de TCP est de pouvoir réguler le débit des données grâce à sa capacité à émettre des messages de taille variable, ces messages sont appelés segments.

### Protocole UDP

Le protocole UDP ou *User Datagram Protocol* est un des principaux protocoles de télécommunication utilisé par Internet. Il fait partie de la couche Transport de la pile de protocole TCP/IP: dans l'adaptation approximative de cette dernière au modèle OSI, il appartiendrait à la couche 4, comme TCP.   
Il est détaillé dans la RFC 768.

Le rôle de ce protocole est de permettre la transmission de paquets de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port (pour différencier différents utilisateurs sur le même hôte). Contrairement au protocole TCP, il travaille en mode non connecté: il n'y a pas de moyen de vérifier si tous les paquets envoyés sont bien arrivés à destination et dans quel ordre (le séquencement peut cependant être assuré par un protocole réseau de couche inférieure).   
Il n'est prévu aucun contrôle de flux ni contrôle de congestion. C'est pour cela qu'il est souvent décrit comme étant un protocole non fiable.   
En revanche, pour un paquet UDP donné, l'exactitude du contenu des données est assurée grâce à une somme de contrôle (*checksum*).

### Utilisation

Le protocole UDP est utilisé ...

* soit de t**ransmettre des données très rapidement** et où la **perte d'une partie de ces données n'a pas grande** **importance**,
* soit de **transmettre des petites quantités de données**, là où la connexion en trois phase de TCP serait trop lourde.

Par exemple, dans le cas de la transmission de la voix sur IP, ce n'est pas grave si l'un ou l'autre paquet se perd (il existe des mécanismes de substitution des données manquantes), par contre la rapidité de transmission est un critère primordial pour la qualité d'écoute.

Exemples d'utilisation …

* le programme *traceroute* ;
* les protocoles DNS, TFTP, … ;
* les jeux en réseau ;
* La diffusion (*streaming*) :  
  Il est indispensable pour les applications multimédias de par sa faible latence.

# Protocoles de la couche Applications

## Fonctionnement général

Pour désigner les informations transmises et leur enveloppe, selon le niveau concerné, on parle de message (ou de flux) entre applications, de datagramme (ou segment) au niveau TCP, de paquet au niveau IP, et enfin, de trames au niveau de l'interface réseau (Ethernet ou Token Ring).

Les protocoles du niveau Application les plus connus sont ...

* **HTTP** (*HyperText Transfer Protocol*) permet l'accès aux documents HTML et le transfert de fichiers depuis un site WWW ;
* **FTP** (*File Transfer Protocol*) pour le transfert de fichiers s'appuie sur TCP et établit une connexion sur un serveur FTP ;
* **DNS** (*Domain Naming Service*) et **DHCP** (*Dynamic Hosts Configuration Protocol*) pour la configuration IP des hôtes ;
* **SSH**(*Secure shell*)pour les connexions à distance en émulation terminal à un hôte Linux ;
* **SMTP** (*Simple Mail Transfer Protocol*) pour la messagerie électronique (UDP et TCP).  
  Il travaille conjointement avec **POP** et **IMAP** ;
* **SNMP** (*Simple Network Management Protocol*) et NTP (*Network Time Protocol*) pour l'administration du réseau ;
* **NFS** (*Network File System*) pour le partage des fichiers Linux.

## Fonctions

La couche Application du modèle TCP/IP …

* i**dentifie et détermine la disponibilité des partenaires de communication** voulus ;
* **synchronise les applications coopératives** ;
* **établit une entente sur les procédures de reprise sur incident et de contrôle de l'intégrité** des données.

La couche Application propose un ensemble complet de programmes d'interface à Internet.   
À chaque type d'application correspond un protocole d'application qui lui est propre.

Exemple de service de la couche Application **…**

* Les programmes de **messagerie électronique** supportent les protocoles de couche application SMTP, POP3 et IMAP4 pour le courrier électronique ;
* Les programmes d'**accès distant** utilisent le protocole SSH afin de se connecter directement aux ressources distantes ;
* Les utilitaires de **transfert de fichiers** utilisent le protocole FTP pour copier et déplacer les fichiers entre emplacements distants.  
  Le protocole TFTP (*Trivial File Transfert Protocol*) est également un protocole de transferts de fichiers ;
* Les outils de **saisie et de contrôle des données réseau** utilisent le protocole SNMP et NTP ;
* Le protocole d’**accès Internet** comme HTTP ;
* Les protocoles de **gestion des hôtes** comme DHCP et DNS.

## Accès Internet

**HTTP (*Hypertext Transfect Protocol*)**  
HTTP est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (avec S pour *secured*) est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS.

HTTP peut fonctionner sur n'importe quelle connexion fiable. Toutefois, dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).

Les clients HTTP les plus connus sont les fureteurs Web permettant à un utilisateur d'accéder à un serveur contenant les données. Il existe aussi des systèmes pour récupérer automatiquement le contenu d'un site tel que les aspirateurs de site Web ou les robots d'indexation.

HTTP utilise le langage HTML  
HTML (Hypertext Markup Language) est le langage standard pour les documents Internet.

**Méthodes**

Pour le protocole HTTP, une méthode est une commande spécifiant un type de requête, c'est-à-dire qu'elle demande au serveur d'effectuer une action. En général l'action concerne une ressource identifiée par l'URL qui suit le nom de la méthode.

**Exemple d’une méthode** …  
**GET / HTTP/1.1**  
**Host: www.profsavard.info**

Il existe de nombreuses méthodes, les plus courantes étant GET, HEAD et POST ...

* **GET**  
  C'est la méthode la plus courante pour demander une ressource.   
  Une requête GET est sans effet sur la ressource, il doit être possible de répéter la requête sans effet ;
* **HEAD**  
  Cette méthode ne demande que des informations sur la ressource, sans demander la ressource elle-même ;
* **POST**  
  Cette méthode est utilisée pour transmettre des données en vue d'un traitement à une ressource (le plus souvent depuis un formulaire HTML).   
  L'URI fourni est l'URI d'une ressource à laquelle s'appliqueront les données envoyées.   
  Le résultat peut être la création de nouvelles ressources ou la modification de ressources existantes.   
  À cause de la mauvaise implémentation des méthodes HTTP par certains fureteurs (et la norme HTML qui ne supporte que les méthodes GET et POST pour les formulaires), cette méthode est souvent utilisée en remplacement de la requête PUT, qui devrait être utilisée pour la mise à jour de ressources.

**Autres méthodes**Il existe aussi d’autres méthodes qui dsont néanmoins moins utilisées ...

* **OPTIONS**  
  Cette méthode permet d'obtenir les options de communication d'une ressource ou du serveur en général ;
* **CONNECT**  
  Cette méthode permet d'utiliser un proxy comme un tunnel de communication ;
* **TRACE**  
  Cette méthode demande au serveur de retourner ce qu'il a reçu, dans le but de tester et effectuer un diagnostic sur la connexion ;
* **PUT**  
  Cette méthode permet de remplacer ou d'ajouter une ressource sur le serveur.   
  L'URI fourni est celui de la ressource en question ;
* **PATCH**  
  Cette méthode permet, contrairement à PUT, de faire une modification partielle d'une ressource ;
* **DELETE**  
  Cette méthode permet de supprimer une ressource du serveur.

Ces 3 dernières méthodes nécessitent généralement un accès privilégié.

Certains serveurs autorisent d'autres méthodes de gestion de leurs ressources (par exemple WebDAV).

**Du client au serveur**

La liaison entre le client et le serveur n'est pas toujours directe car il peut exister des hôtes intermédiaires servant de relais ...

* Un **proxy** (ou serveur mandataire) peut modifier les réponses et requêtes qu'il reçoit et peut gérer un cache des ressources demandées ;
* Une **passerelle** (ou gateway) est un intermédiaire modifiant le protocole utilisé ;
* Un **tunnel** transmet les requêtes et les réponses sans aucune modification, ni mise en cache.

**Identification**

HTTP permet l'identification du visiteur par transmission d'un nom et d'un mot de passe.

Il existe 2 modes d'identification ... Basic et Digest (RFC 26176) …

* Le premier mode transmet le mot de passe en clair, et ne doit donc être utilisé qu'avec le protocole HTTPS ;
* Le deuxième mode permet une identification sans transmettre le mot de passe en clair.   
  L'identification est cependant souvent effectuée par une couche applicative supérieure à HTTP.



## Messagerie électronique

**SMTP, POP3 et IMAP4**  
Le courrier électronique permet l'envoi de messages entre des ordinateurs sur un réseau

**Présentation**  
Le courrier électronique, aussi simple soit-il à utiliser, repose sur un fonctionnement plus compliqué que celui du web.   
Il est un des plus important service réseau. Pour la plupart des utilisateurs son fonctionnement est transparent, ce qui signifie qu'il n'est pas nécessaire de comprendre comment le courrier électronique fonctionne pour pouvoir l'utiliser.  
Néanmoins, il est important de comprendre le principe.

Linux propose un gestionnaire de courriels même dans un environnement totalement dépourvu de réseau: certains sous-systèmes Linux, tels que *cron*, peuvent utiliser le courrier électronique pour informer de ses activités.   
Pour cette raison, la plupart des distributions Linux sont livrées avec le logiciel de serveur de messagerie installé et configuré pour les activités de base.

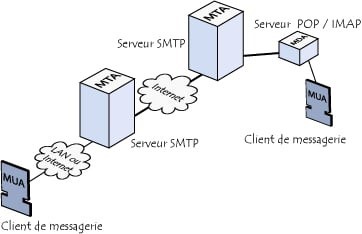
**Fonctionnement du courrier électronique**  
Le fonctionnement du courrier électronique est basé sur l'utilisation d'une boîte à lettres électronique.   
Lors de l'envoi d'un email, le message est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire.   
Plus exactement, le message est envoyé au serveur de courrier électronique chargé du transport (nommé MTA pour *Mail Transport Agent*), jusqu'au MTA du destinataire. Sur internet, les MTA communiquent entre-eux grâce au protocole SMTP et sont logiquement appelés serveurs SMTP (parfois serveur de courrier sortant).

Le serveur MTA du destinataire délivre alors le courrier au serveur de courrier électronique entrant (nommé MDA pour *Mail Delivery Agent*), qui stocke alors le courrier en attendant que l'utilisateur vienne le relever.

Il existe deux principaux protocoles permettant de relever le courrier sur un MDA :

* le protocole POP3 (*Post Office Protocol*), le plus ancien, permettant de relever son courrier et éventuellement d'en laisser une copie sur le serveur ;
* le protocole IMAP (*Internet Message Access Protocol*), permettant une synchronisation de l'état des courriers (lu, supprimé, déplacé) entre plusieurs clients de messagerie.   
  Avec le protocole IMAP une copie de tous les messages est conservée sur le serveur afin de pouvoir assurer la synchronisation.

Ainsi, les serveurs de courrier entrant sont appelés serveurs POP ou serveurs IMAP, selon le protocole utilisé.



## Protocoles de gestion des courriels

### SMTP (Simple Mail Transfer Protocol)

SMTP permet d’envoyer des messages texte vers des hôtes disposant de services de courriel.  
L’usager communique avec le serveur à partir d’un agent utilisateur (User agent).  
Le serveur dispose d’un d’agent d’envoi et de réception (MTA ou Message Transfert Agent).  
SMTP est un protocole de transfert simple basé sur le protocole TCP.   
Il n’offre aucune interface utilisateur.



### POP3 (Post Office Protocol version 3)

SMTP s’attend à ce que l’hôte destinataire qui reçoit le courriel soit disponible et connecté sur le réseau Internet (sinon il est impossible d’ouvrir une session TCP). Les hôtes d’extrémités doivent être ouverts en permanence.  
Pour la majorité des environnements réseau, les courriels sont reçus par des serveurs SMTP.   
Les clients communiquent avec ces serveurs de courriels avec le protocole POP3 afin de récupérer leurs messsages.



**IMAP4 (*Internet Message Access Protocol* rev. 4)**  
Protocole qui succède à POP3 qui possède la limite que le courriel doit être téléchargé sur la station de travail.   
En effet, POP3 ne permet pas de manipuler les courriels directement sur les serveurs.  
IMAP4 permet en plus de …

* **accéder et de manipuler des portions de courriels sans avoir à les télécharger** ;
* **voir des messages et des pièces jointes sans les télécharger** ;
* t**élécharger les messages pour les consulter hors connexion** ;
* **manipuler (créer, supprimer et renommer) des répertoires appelés boîte aux lettres** ;
* **synchroniser le client sur le serveur**.

Tout comme POP3, IMAP4 ne spécifie pas de méthode d’envoi de courrier.   
Cette fonctionnalité est offerte pour SMTP.



## Accès distant

Secure SHell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé.

Le protocole de connexion impose un échange de clés de chiffrement en début de connexion.   
Par la suite, tous les segments TCP sont authentifiés et chiffrés.   
Il devient alors impossible (ou presque) d'utiliser un renifleur (*sniffer*) pour voir ce que fait un utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

Le protocole SSH existe en deux versions majeures : la version 1.0 et la version 2.0.

* La **première version** permet de se connecter à distance à un ordinateur afin d'obtenir un shell ou ligne de commande.   
  Cette version souffrait néanmoins de problèmes de sécurité dans la vérification de l'intégrité des données envoyées ou reçues, la rendant vulnérable à des attaques actives.   
  En outre, cette version implémentait un système sommaire de transmission de fichiers, et du port tunneling.
* La **version 2** est beaucoup plus sûre au niveau cryptographique, et possède en plus un protocole de transfert de fichiers complet, le **SSH File Transfer Protocol** (SFTP).

Habituellement le protocole SSH utilise le port TCP 22.   
Il est particulièrement utilisé pour ouvrir un shell sur un hôte distant.

SSH peut également être utilisé pour transférer des ports TCP d'un hôte vers un autre, créant ainsi un tunnel.   
Cette méthode est couramment utilisée afin de sécuriser une connexion qui ne l'est pas (par exemple le protocole de récupérations de courrier électronique POP3) en la faisant transférer par le biais du tunnel chiffré SSH.

Il est également possible de faire plusieurs sauts entre consoles SSH, c'est-à-dire ouvrir une console sur un serveur, puis, de là, en ouvrir une autre sur un autre serveur.

Les usages de base de SSH sont ...

* L'**accès à distance à la console en ligne commande** (shell), ce qui permet, entre autres, d'effectuer la totalité des opérations courantes et/ou d'administration sur un hôte distant ;
* Le **déport de l'affichage graphique** de l’hôte distant ;
* Le **transfert des fichiers en ligne de commande** ;
* Le **montage ponctuel et/ou automatique d’un répertoire distant**, soit en ligne de commande, soit à l’aide d’une interface graphique.

### Tunnel SSH

Un tunnel, dans le contexte de réseaux informatiques, est une encapsulation de données d'un protocole réseau dans un autre, situé dans la même couche du modèle en couches, ou dans une couche de niveau supérieur.

Par exemple, pour faire passer le protocole IPv6 par le réseau Internet actuel (qui est en grande partie en IPv4) on va créer un tunnel entre deux machines IPv4 ; ce tunnel, pour le protocole IPv6, semblera un simple lien point-à-point   
(un logiciel comme traceroute ne verra donc pas le tunnel).

En sécurité, on crée souvent des tunnels chiffrés, par exemple comme le fait SSH. Les données peuvent alors y circuler sans craindre d'être écoutées. Les tunnels peuvent être utilisés pour créer des réseaux privés virtuels (VPN).

Le tunnel HTTP est un cas particulier qui consiste à faire passer une connexion explicitement interdite par un pare-feu (le protocole SSH par exemple) encapsulé dans un protocole HTTP presque toujours autorisé. C'est particulièrement utile quand le pare-feu ne bloque pas simplement les ports associés (22 pour SSH par exemple), mais analyse aussi les protocoles utilisés.

## Transfert de fichiers

### FTP

En règle générale, FTP est utilisé lorsque le montage d’un partage permanent ou temporaire n’est pas souhaité ou réalisable et la vitesse de transfert est un problème. Idéal pour les situations où les fichiers sont partagés pour téléchargement uniquement, par exemple lorsqu'un instructeur sur un réseau local de laboratoire local partage des fichiers binaires avec les débutants étudiants Linux.

Le protocole de transfert de fichier (FTP) existe depuis longtemps. C'est un protocole réseau simple pour le partage de fichiers entre systèmes. Il est principalement utilisé pour partager des documents publics sur un réseau.

Lors d’une connexion à un service FTP, son processus d'authentification peut obliger à lui attribuer un nom d'utilisateur et un mot de passe valides. Une fois authentifié, en fonction de la configuration du service FTP, on pourra essentiellement rechercher et télécharger (ou téléverser) des fichiers.

**Attention** …  
En utilisant des informations de compte et des mots de passe pour se connecter à un service FTP, il est important de savoir qu’elles ne sont généralement pas chiffrées. Cela signifie que toute personne utilisant une application de détection de réseau, telle que Wireshark, verra le nom d'utilisateur et le mot de passe vers serveur FTP en clair. Il est préférable d’utiliser Secure FTP (SFTP), qui chiffre FTP via openSSH.

Il est plus courant de configurer un service FTP pour un accès anonyme et d’autoriser uniquement les téléchargements de fichiers. Avec un accès FTP anonyme, au lieu d’un nom d’utilisateur attribué individuellement, un nom d’utilisateur général, tel que **anonymous** ou **ftp**, est utilisé. Il se peut qu'aucun mot de passe ne soit requis ou qu'une demande d'adresse de courriel ne soit demandée (bien que l'adresse de courriel ne soit pas vérifiée).

**Attention** …  
Avec FTP, toutes les données (dont les mots de passe) sont transmises en clair.



# Protocoles de configuration des hôtes

## Protocole DHCP

Dynamic Host Configuration Protocol (DHCP) désigne le protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres TCP-IP d'un hôte, notamment en lui assignant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et de nombreux autres paramètres.



## Protocole DNS

## Concepts de base

DNS (Domain Name Service) est un protocole conçu pour fournir une résolution de nom en adresse IP.   
Il fait partie de la suite de protocoles TCP/IP standard et de l'un des protocoles pouvant fournir cette fonctionnalité ; les autres étant NIS et LDAP.

Ce qui distingue le DNS des autres protocoles similaires est que son unique objectif est la résolution de noms; NIS et LDAP fournissent d'autres opérations de résolution.   
DNS est également la solution de résolution de noms standard de facto pour la majorité des systèmes connectés à Internet.

**Fichier hosts.txt**

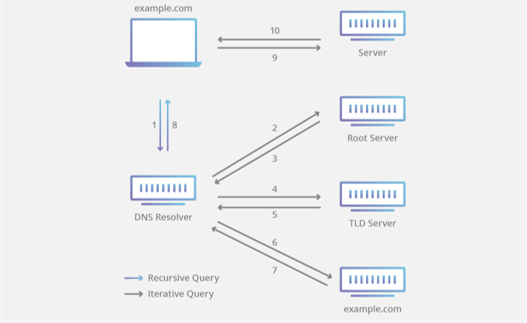
Avant le DNS, la résolution d'un nom sur Internet devait se faire grâce à un fichier texte appelé HOSTS.TXT (RFC 60813) et copié sur chaque ordinateur du réseau par transfert de fichier.

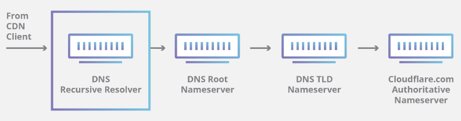
En 1982, ce système centralisé montre ses limites et plusieurs propositions de remplacement voient le jour, parmi lesquelles le Domain Name System afin de gérer la croissance de l'internet en déléguant la gestion des noms de domaine à des serveurs de noms distribués.

En 1987, le fichier hosts.txt contenait 5 500 entrées, tandis que 20 000 hôtes étaient définis dans le DNS.

### Processus simplifié de résolution de noms

Voici un processus de résolution de noms générique …



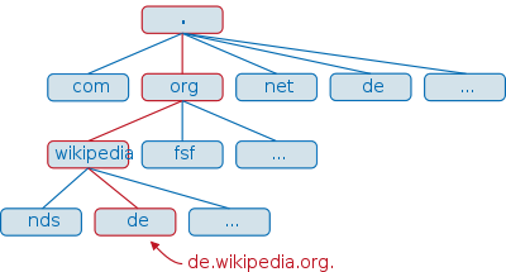


### Nom de domaine

On représente un nom de domaine en indiquant les domaines successifs séparés par un point, les noms de domaines supérieurs se trouvant à droite.

Par exemple, profsavard.info. …

* Le domaine info. est un TLD, sous-domaine de la racine ;
* Le domaine profsavard.info. est un sous-domaine de .info.



Cette délégation est accomplie en indiquant la liste des serveurs DNS associée au sous-domaine dans le domaine de niveau supérieur.

Les noms de domaines sont donc résolus en parcourant la hiérarchie depuis le sommet et en suivant les délégations successives, c'est-à-dire en parcourant le nom de domaine de droite à gauche.



# Références

* http://cvardon.fr/plaquetteOSI.html
* http://www.linux-france.org/prj/edu/archinet/systeme/ch01s03.html
* https://fr.wikipedia.org/wiki/IPv4
* http://www.laissus.fr/cours/node9.html#SECTION04414000000000000000
* http://www.supinfo-projects.com/fr/2006/
* http://cisco.goffinet.org/s1/modele-tcp-ip-et-protocoles#.Vssi60aj92A
* http://www.diml.org/goodies/standards/rfc768/768.dim?session
* http://www.laissus.fr/cours/node9.html#SECTION04470000000000000000
* https://fr.wikipedia.org/wiki/Domain\_Name\_System
* http://www.kloth.net/services/dig.php
* http://fr.wikipedia.org/wiki/Nmap
* <http://blog.nicolargo.com/2007/08/nmap-le-scanneur-de-reseau.html>
* Openclassroom  
  https://openclassrooms.com/fr/courses/857447-apprenez-le-fonctionnement-des-reseaux-tcp-ip

|  |  |
| --- | --- |
| **Document distribué sous licence** |  |

1. DHCP (*Dynamic Hosts Configuration Protocol*) est un protocole de la couche Applications. [↑](#footnote-ref-2)