

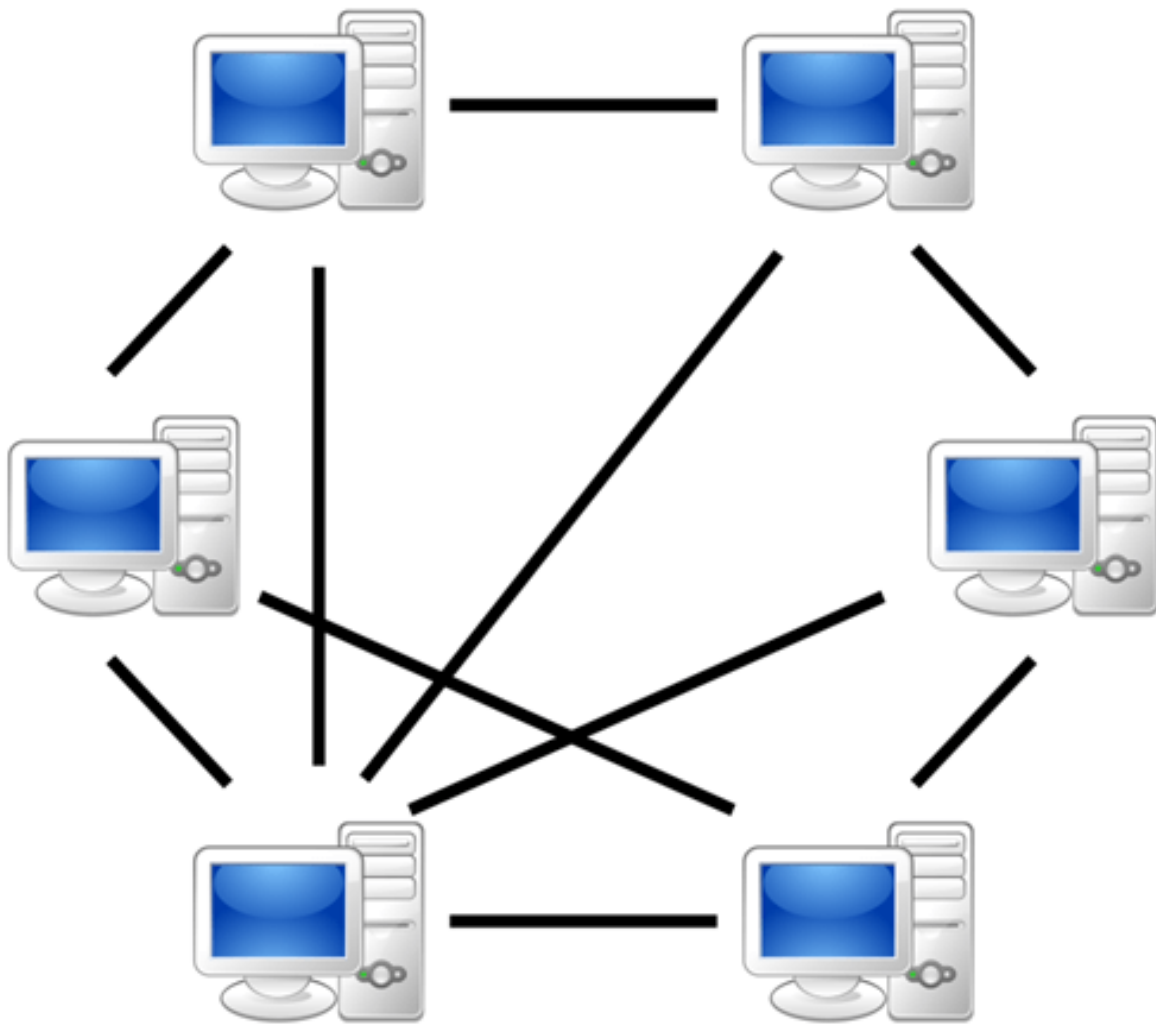
Notions de réseaux informatiques

Xavier Gendre 

Réseau informatique

Un ensemble d'appareils reliés entre eux pour échanger de l'information est appelé un **réseau**.

Des ordinateurs peuvent faire partie d'un réseau mais aussi de nombreux autres équipements (routeur, imprimante, ...).



Le principe concerne autant les réseaux étendus sur de vastes zones géographiques (WAN) que les réseaux locaux (LAN).

Modèle OSI

Norme de communication entre des ordinateurs en réseau.

Sept couches organisées par niveau d'abstraction croissant :

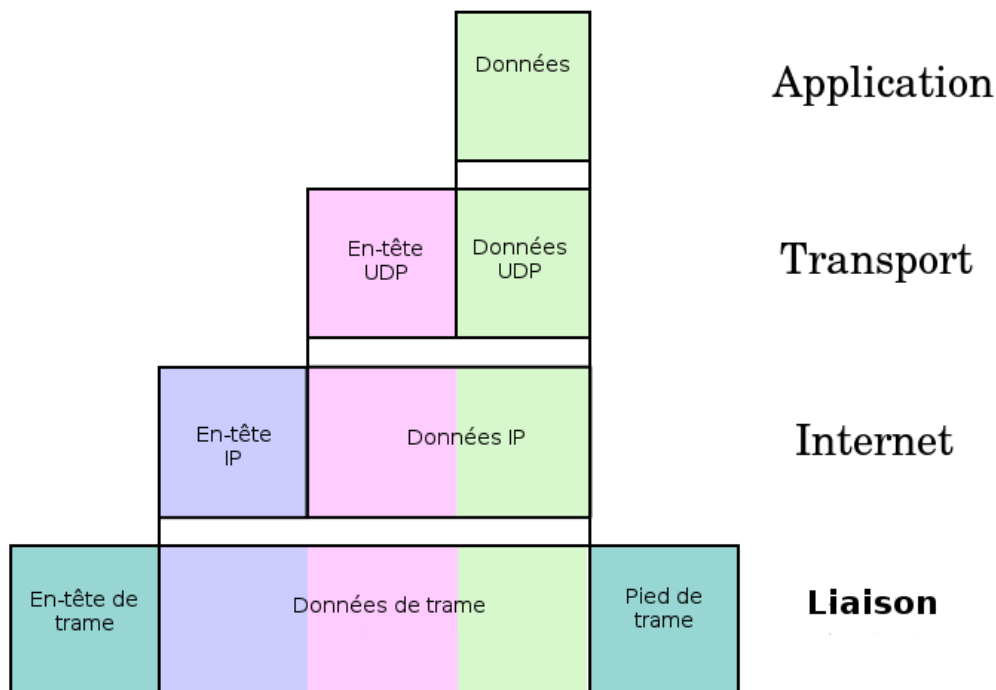
1. Physique (émission et réception de bits)
2. Liaison (connexion directe, adresse MAC)

3. Réseau (communication de proche en proche, **adresse IP**)
4. Transport (connexion de bout en bout, **TCP** et **UDP**)
5. Session (synchronisation et transactions : cookies, ...)
6. Présentation (codage, chiffrement et déchiffrement)
7. Application (point d'accès aux services : **HTTP** / **HTTPS**, ...)

Notion de protocole

Un **protocole réseau** est un ensemble de règles qui précisent comment mettre en forme, transmettre et recevoir des données pour assurer la communication dans un réseau.

Encapsulation : un protocole à un niveau donné s'appuie généralement sur d'autres protocoles dans les niveaux inférieurs.



Un exemple connu : HTTP

Il s'agit du protocole de communication **client-serveur** développé pour le Web dans les années 1990 et toujours d'actualité. Il est au niveau *Application*.

Le protocole définit des méthodes (HEAD, GET, POST, PUT, ...) pour échanger avec le serveur des données textuelles.

HTTPS est la variante sécurisée du HTTP par **chiffrement** et **authentification**.



Port logiciel

Un protocole utilise des **ports** (entiers 16 bits) pour recevoir et émettre des information et se distinguer des autres protocoles. Il s'agit essentiellement d'un *identifiant de processus*.

Grâce à ce mécanisme, une même machine peut exécuter **plusieurs logiciels serveurs**.

Par exemple, un serveur HTTP utilise le port 80 et un serveur HTTPS utilise le port 443.

Protocole IP

Au niveau 3 (*Réseau*), un protocole important est **IP** (*Internet Protocol*).

Ce protocole permet la **communication entre réseaux** et non uniquement entre machines directement connectées comme dans la couche de Liaison.

Ce protocole est technique (routage, *best effort delivery*, ...) et nous n'entrerons pas dans les détails.

Il permet en particulier un **service d'adressage unique** pour les équipements connectés.

IPv4 : version largement utilisée, les adresses sont codées sur 32 bits généralement présentés comme 4 entiers de 8 bits.

Par exemple, 185.15.58.224 est l'adresse IPv4 d'un serveur web de Wikipedia.

IPv6 : pour pallier l'épuisement des adresses IPv4, la version 6 du protocole a été introduite et code les adresses sur 128 bits sous la forme de 8 groupes en hexadécimal de 16 bits.

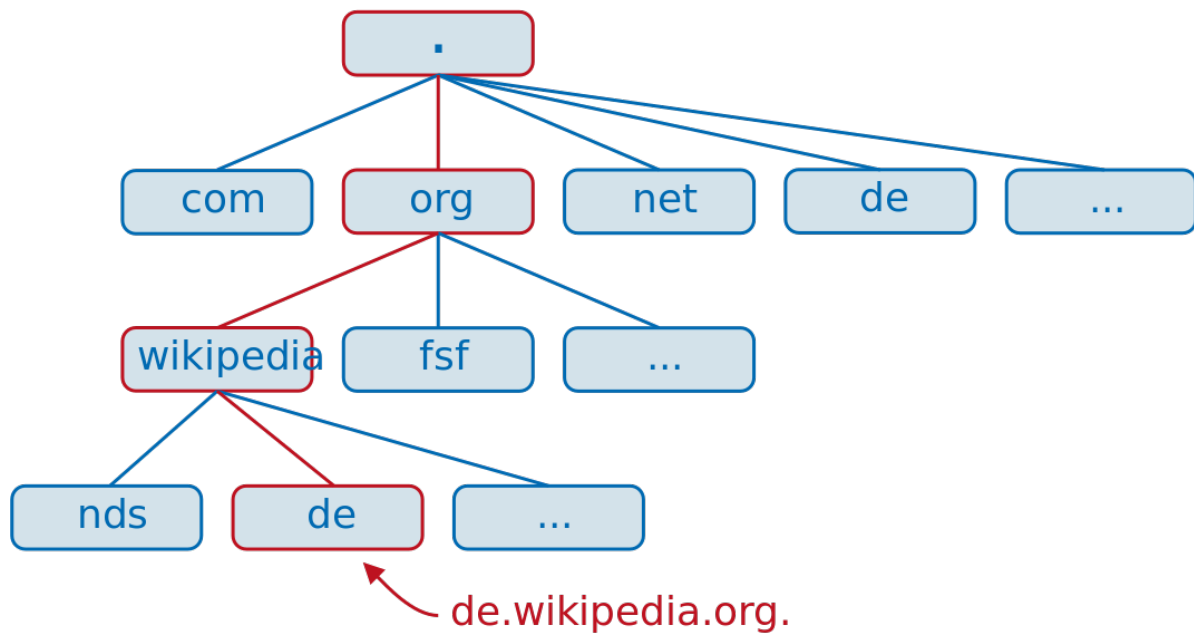
Par exemple, 2a02:ec80:600:ed1a::1 est l'adresse IPv6 d'un serveur web de Wikipedia.

(Les caractères :: sont un raccourci, l'adresse complète est 2a02:ec80:0600:ed1a:0000:0000:0000:0001)

Retrouver ses petits avec le DNS

Le **DNS** (*Domain Name System*) est un service essentiel qui associe les noms de domaines avec leurs adresses IP (ou d'autres types d'enregistrements).

La réponse DNS pour **wikipedia.org** donne les adresses 185.15.58.224 et 2a02:ec80:600:ed1a::1 (et d'autres enregistrements pour le mail, ...).



Protocole SSH

Le protocole SSH permet d'établir une **connexion chiffrée** à travers des réseaux non sécurisés.

Cette connexion peut être utilisée pour de nombreuses applications (ligne de commande, transfert de fichiers, ...).

Par défaut, un serveur SSH utilise le port 22.



Clé SSH

Une alternative au mot de passe pour se connecter à distance via SSH consiste à utiliser une **clé SSH**.

Cette clé est composée de deux fichiers appelés **clé publique** et **clé privée**.

La clé publique peut être **diffusée largement** et copiée sur le serveur SSH. La clé privée doit rester **secrète** et peut être protégée par un mot de passe (fortement conseillé).

L'utilisation d'une clé SSH avec un (bon) mot de passe **élève nettement le niveau de sécurité** de l'authentification. Certains serveurs imposent l'utilisation d'une telle clé.

Fully connected!