

Cours de réseaux

M1 Informatique
Faculté Jean Perrin



Plan du cours

Partie 1 : Introduction

Partie 2 : Couche physique

Partie 3 : Couche liaison des données

Partie 4 : Couche Réseau / IPv4

Partie 5 : Couche Réseau / Routage

Partie 6 : Couche Réseau / IPv4, IPv6

Partie 7 : Couche transport : TCP et UDP

Partie 8 : Couche application : généralités

Partie 9 : Couche application / Etude de protocoles

Partie 10 : Notions d'attaques et de sécurité

Partie 8

Couche application

Vous êtes ici

Modèle OSI

7	Application ●
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Physique

TCP/IP

<i>Applications</i> <i>Services Internet</i> ●
<i>Transport (TCP)</i>
<i>Internet (IP)</i>
<i>Accès au Réseau</i>

Rôles de la couche application

La couche application est la couche supérieure du modèle OSI. Elle sert d'**interface** entre les applications offertes à l'utilisateur et le réseau.

Les protocoles de la couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes source et destination.

Rôles de la couche application

Les fonctionnalités des protocoles de couche application de TCP/IP intègrent les trois couches supérieures du modèle OSI

- Application
- Présentation
- Session

Fonctionnalités

Couche présentation

- Codage et conversion des données issues de l'application source vers l'application destination
- Compression et décompression
- Chiffrement et déchiffrement

Couche session

- Initie et maintient les sessions permettant l'établissement d'un dialogue entre les hôtes

Protocoles connus

DNS (**D**omain **N**ame **S**ervice)

conversion d'adresses « internet » en adresses IP

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol)

assignation automatique d'adresse IP, de masque de sous-réseau, de passerelle...

HTTP (**H**ypertext **T**ransfer **P**rotocol)

transfert de fichiers définissant des pages Web

SMTP (**S**ingle **M**ail **T**ransfert **P**rotocol)

transfert de mail et pièces jointes

Telnet

émulation de terminal, accès distant

FTP (**F**ile **T**ransfert **P**rotocol)

transfert de fichiers entre systèmes

Applications, services et protocoles

La couche application comprend deux types de processus permettant d'accéder au réseau :

Applications réseau : applications destinées à l'utilisateur final et capables de communiquer directement avec les couches inférieures.

Exemples : clients de messagerie, navigateurs Web

Services de couche application : processus établissant l'interface avec le réseau et préparant les données à transférer. Ces services sont utilisés par d'autres programmes.

Exemples : mise en file de tâches d'impression réseau, transfert de fichiers

Applications, services et protocoles

Applications et services réseau utilisent un ou des protocoles définissant normes et formats de données.

Ces protocoles permettent de définir les méthodes communes pour formater les données et les transmettre sur le réseau.

Dans certains cas, applications, services et protocoles sont intégrés au sein du même programme exécutable... et peuvent même porter le même nom.

Exemple : telnet

Utilisation des applications et services

Deux modèles distincts peuvent s'appliquer pour la mise en œuvre de la couche applicative :

- Modèle client serveur
- Modèle Peer-to-Peer (pair à pair)

Modèle client/serveur

Architecture réseau dans lequel un périphérique (appelé **serveur**) offre des « services » à d'autres périphériques (appelé **clients**).

- Le début des échanges se fait à l'initiative du client.
- Les protocoles décrivent le format des requêtes et des réponses entre les deux parties.
- Les échanges peuvent également intégrer des informations de contrôle (ex. authentification de l'utilisateur, identification des fichiers, etc)

Modèle client/serveur

Exemple : serveur de messagerie d'entreprise.

Attention : en général, le flux de données va du serveur vers le client mais il se peut qu'il soit dans les deux sens, voire même être plus important dans le sens client vers serveur.

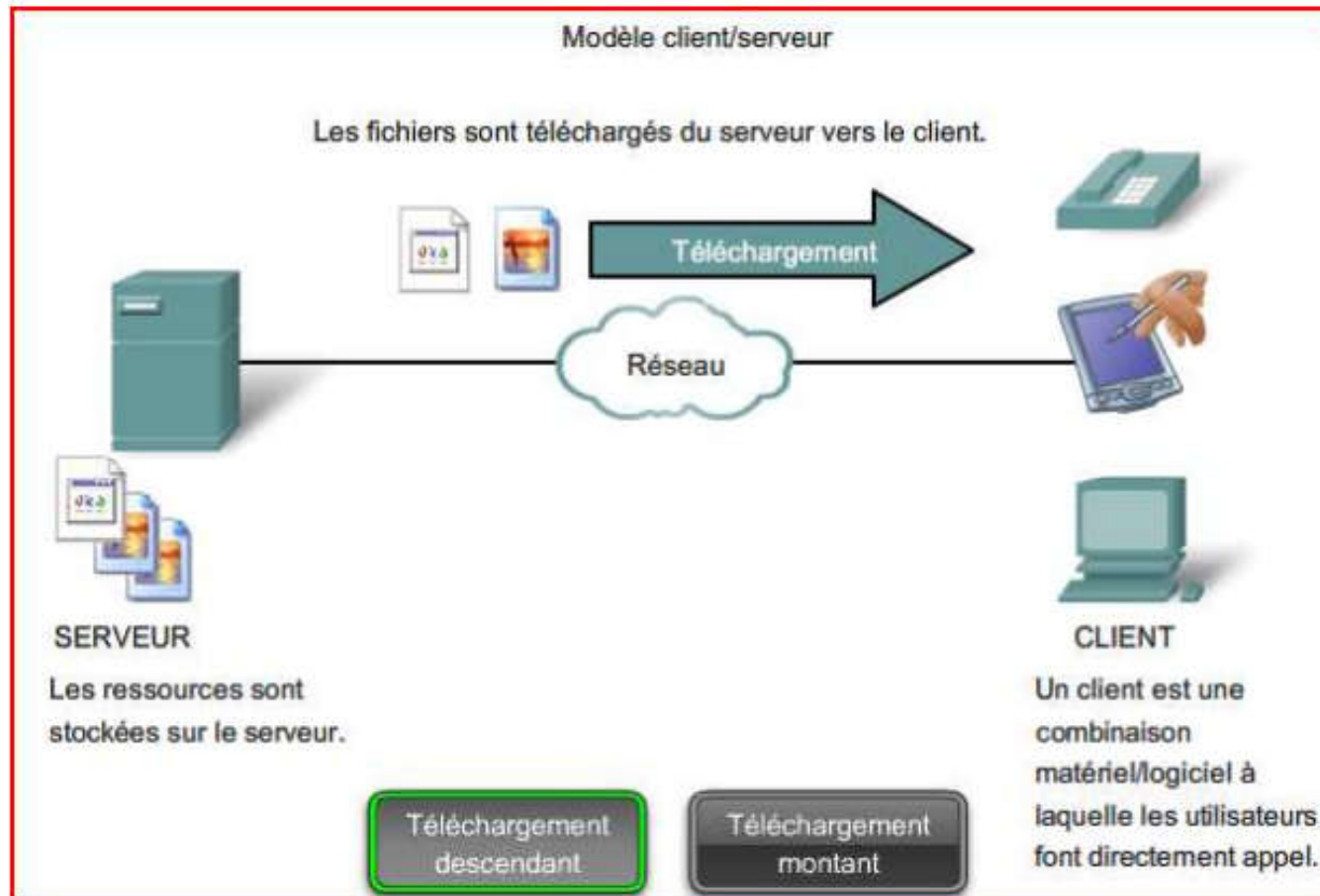
Exemple : serveur de stockage de fichiers...

Modèle client/serveur

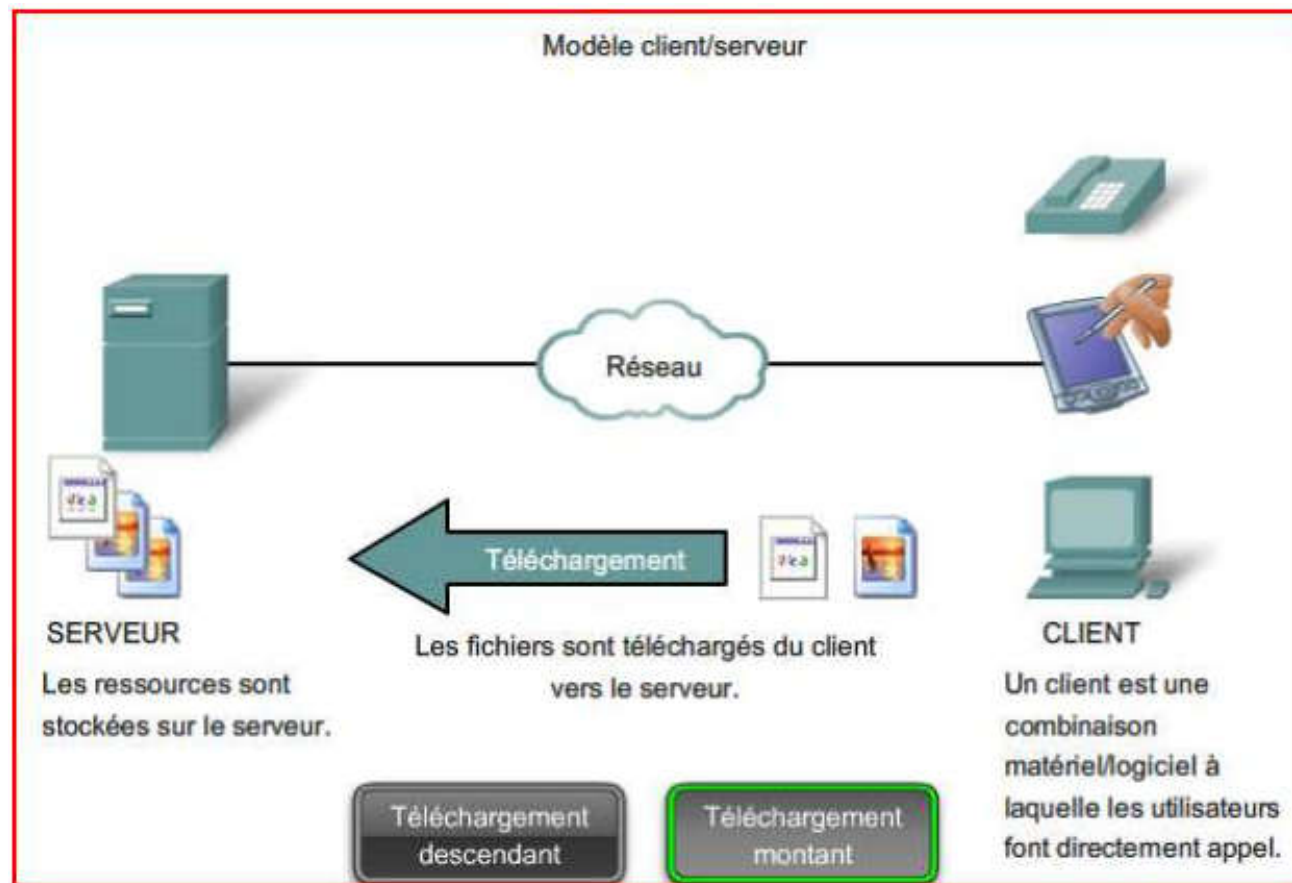
Téléchargement montant (upload) : transfert de données d'un client vers un serveur.

Téléchargement descendant (download) : transfert de données d'un serveur vers un client.

Modèle client/serveur



Modèle client/serveur



Notion de serveur

Dans un contexte réseau, on appelle serveur un périphérique répondant à des requêtes d'applications clientes.

Il peut s'agir :

- d'un ordinateur contenant de l'information à partager avec des systèmes clients

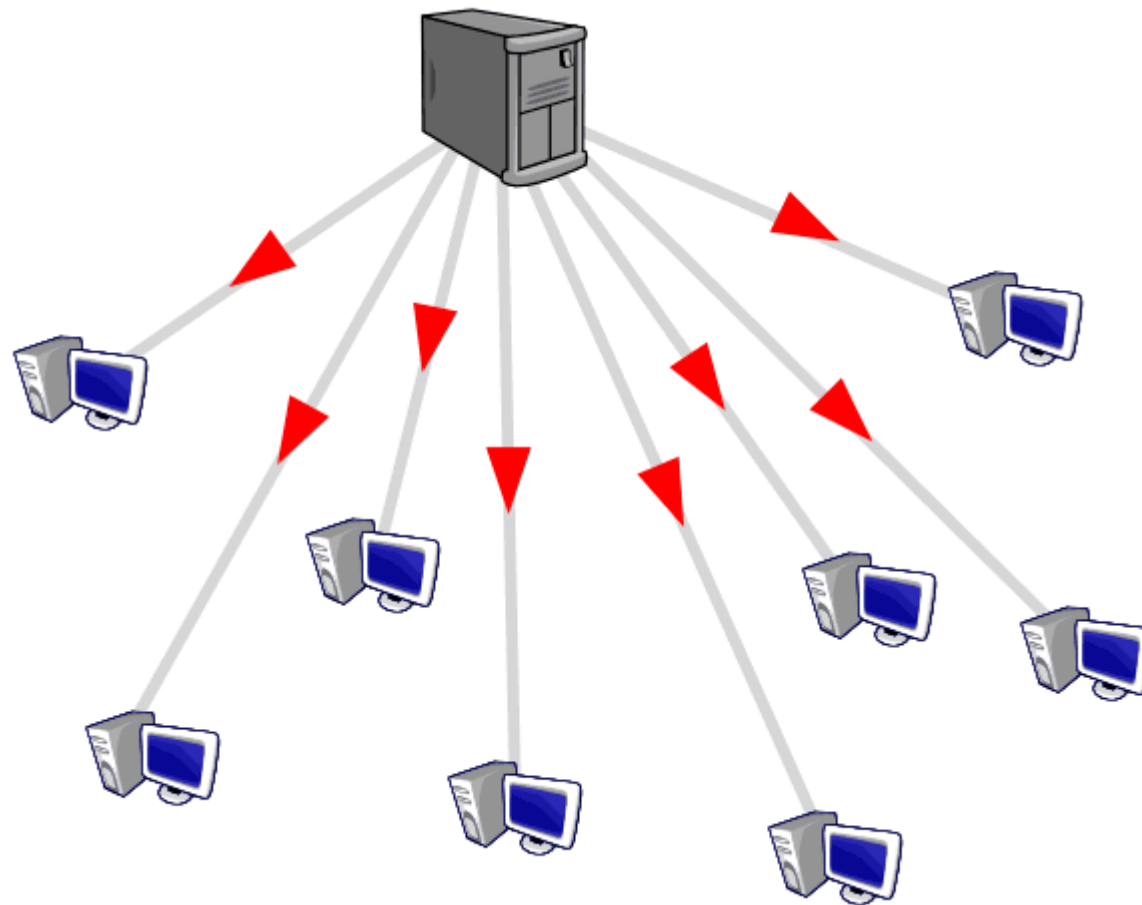
Exemples : serveur Web, bases de données, serveurs vidéo.

- d'un ordinateur proposant une tâche spécifique à ses clients

Exemples : serveur d'imprimante, serveur de calcul.

Le serveur exécute un service ou processus parfois appelé **démon**.

Notion de serveur



Démon de serveur

Comme la plupart des services, les démons :

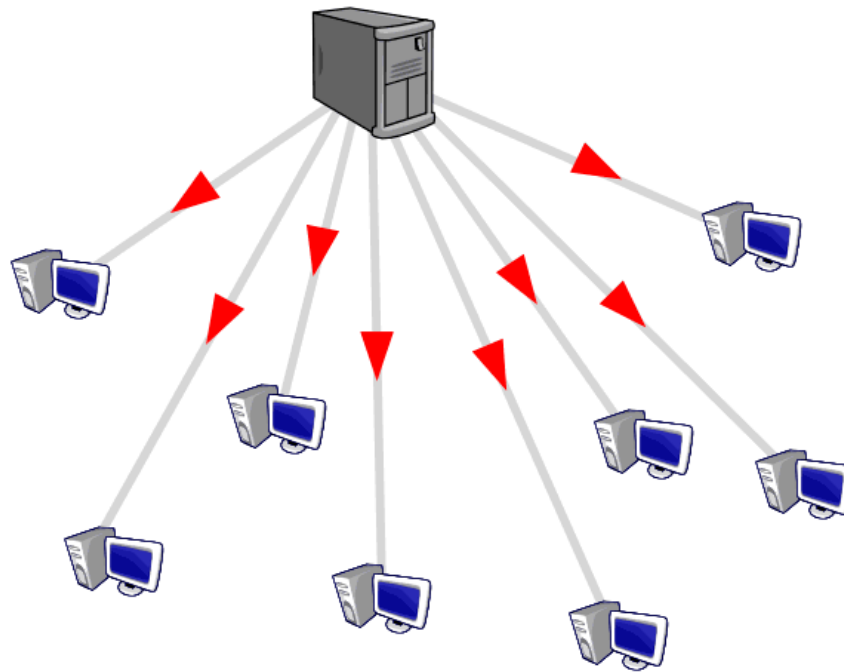
- s'exécutent en tâche de fond,
- ne sont pas sous le contrôle direct de l'utilisateur final.

Les démons sont « **à l'écoute** » des requêtes de la part des clients.

Lorsqu'un démon « **entend** » une requête, il échange avec le client et lui répond en suivant son protocole.

Inconvénients du modèle

Quel problème le modèle client/serveur peut-il engendrer ?



Inconvénients du modèle

Les ressources n'étant disponibles que sur un seul périphérique une forte demande d'accès à celles-ci entraîne une saturation du service.

Comment faire autrement ?

Modèle Peer to Peer

Un modèle Peer to Peer (d'égal à égal) peut être mis en place sous deux formes différentes :

- Réseau peer to peer
- Applications Peer to Peer (P2P)

Ces deux formes ont des caractéristiques similaires mais fonctionnent très différemment.

Réseaux Peer to Peer

Chaque ordinateur du réseau peut partager des ressources (imprimantes, fichiers,...) sans disposer de serveur dédié.

Chaque périphérique final peut **simultanément** agir en tant que serveur ou en tant que client.

Chaque rôle est défini en fonction de la requête.

Réseaux Peer to Peer

Contrairement au modèle client/serveur qui utilise des serveurs dédiés, les réseaux Peer to Peer décentralisent les ressources sur le réseau.

Les données peuvent se trouver n'importe où sur un périphérique du réseau.

Exemple : réseau domestique avec 2 ordinateurs qui partagent une imprimante.

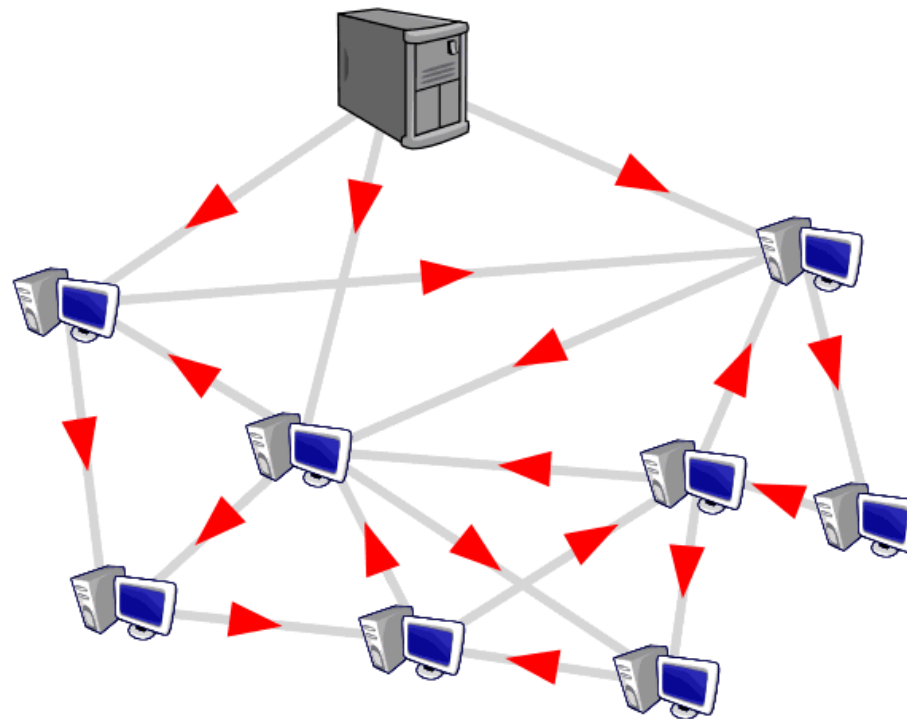
Applications Peer to Peer

Une application Peer to Peer (P2P) permet à un périphérique d'opérer à la fois comme un client et comme un serveur au sein d'une même communication.

Chaque client est un serveur et chaque serveur est un client.

Applications Peer to Peer

Le serveur d'origine n'est plus la seule source pour accéder à la ressource



Applications Peer to Peer

Une application P2P nécessite que chaque périphérique final fournisse une interface utilisateur et exécute un service en tâche de fond.

Certaines applications P2P utilisent un système hybride :

- Partage de ressources décentralisées
- Système de références et d'index vers l'emplacement des ressources centralisé.

Client/serveur vs Peer to Peer

Client/Serveur

- Sécurité : possibilité de contrôler les droits d'accès aux ressources
- Gestion maîtrisée des ressources
- Engorgement possible
- Peu robuste à la panne

Peer to peer

- Partage rapide et efficace
- Peu sécurisé, maîtrise des ressources difficile
- Robuste à la panne

L'homme du jour

Shawn Fanning, né le 22 novembre 1980 à Brockton aux Etats-Unis.



Fin 1998, alors étudiant en informatique à l'Université, il quitte ses études pour se lancer dans l'écriture d'un logiciel permettant d'échanger des fichiers de musique. L'échange des MP3 via les moteurs de recherche étant catastrophique.

Il crée la première application P2P après plusieurs mois de travail et la première version de son logiciel est lancée en juin 1999 qu'il appelle avec son pseudo sur internet.

Il s'agit de **Napster**.

Ce logiciel est un véritable succès très rapidement et il décide de créer une start-up. En septembre 2000, Napster atteint un nombre de téléchargements record. 1,39 Milliards de chansons sont échangées par ses utilisateurs.

En 2001, la 9eme cour d'appel de San Francisco interdit l'échange gratuit de fichiers musicaux MP3 dans l'intérêt des maisons de disques et des artistes (ex Metallica)

Aujourd'hui, Shawn est à la tête d'une société d'édition de musique en ligne.

Il n'a pas reçu le prix Turing.

La couche application : du réseau vers l'utilisateur

La couche application est la couche se trouvant à l'interface entre le réseau et l'utilisateur.

Elle a donc pour vocation d'offrir des services permettant d'abstraire les composantes purement réseaux et difficiles à manipuler pour l'humain.

C'est ce que font, par exemple, les deux services suivants :

DNS : Domain Name Service

DHCP : Dynamic Host Configuration Protocol

Est-ce vraiment utile ?

Retrouvons notre analogie de courrier postal.
Supposons que nous voulions envoyer une lettre
comme suit :

Monsieur 1 73 01 59 xxx xxx

Latitude : 50.435362 N

Longitude : 2.823822 E

Est-ce vraiment utile ?

N'est-ce pas plus pratique comme cela ?

Monsieur B Hovel

UFR des Sciences Jean Perrin

Rue Jean Souvraz SP 18

62307 Lens Cedex

France

Services et protocoles DNS

Notion de noms de domaine

Sur internet, les périphériques sont étiquetés par des adresses IP (numériques) difficiles à mémoriser par les utilisateurs humains.

Mise en place de noms de domaine plus faciles à mémoriser et plus explicites

www.lewebdetataMicheline.com

Il existe une correspondance entre chaque adresse IP et chaque nom de domaine.

Services et protocoles DNS

L'utilisation des noms de domaine permet :

- De mémoriser facilement et de manière claire ce qui se cache derrière une adresse IP
- De pouvoir modifier une adresse IP de manière transparente à l'utilisateur.

Format d'un nom de domaine

Formé de plusieurs parties séparées par un point.

www.google.fr

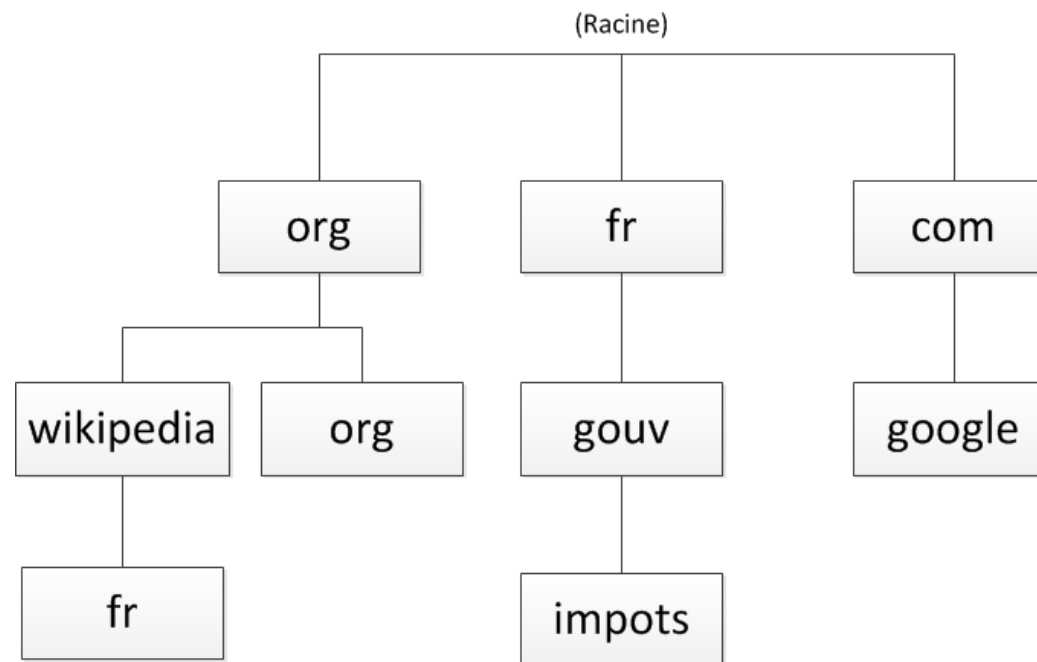
La partie la plus à droite (extension) est appelée Top Level Domain (TLD) et correspond à des identifiants

- nationaux : fr, de, it
- type d'organisation : com, org, net,...

Les autres parties constituent les identifiants des sites découpés éventuellement en sous-domaines.

Format d'un nom de domaine

L'ensemble de ces noms de domaine découpés en sous-parties forme une arborescence.



Format d'un nom de domaine

Chaque partie est appelée **label**.

Un chemin dans cet arbre partant d'une feuille jusqu'à la racine est appelé **FQDN** (Fully Qualified Domain Name).

Par convention un FQDN se termine **TOUJOURS** par un point afin d'assurer qu'il ne s'agit pas d'un sous-domaine d'un autre domaine.

Services et protocoles DNS

Comment passer d'un nom de domaine à une adresse IP facilement ?

Table de mappage : ok mais ça c'était avant...

Services et protocoles DNS

DNS : Domain Name System

Port TCP/UDP : 53

Protocole définissant un service automatique qui associe les noms de ressources aux adresses IP correspondantes.

Il utilise un ensemble distribué de serveurs pour convertir les noms associés aux adresses.

Services et protocoles DNS

Le protocole DNS définit

- le format des demandes
- le format des réponses
- les messages d'erreurs liés au service
- le format de données permettant l'enregistrement de ressources entre les différents serveurs (RFC 1035).

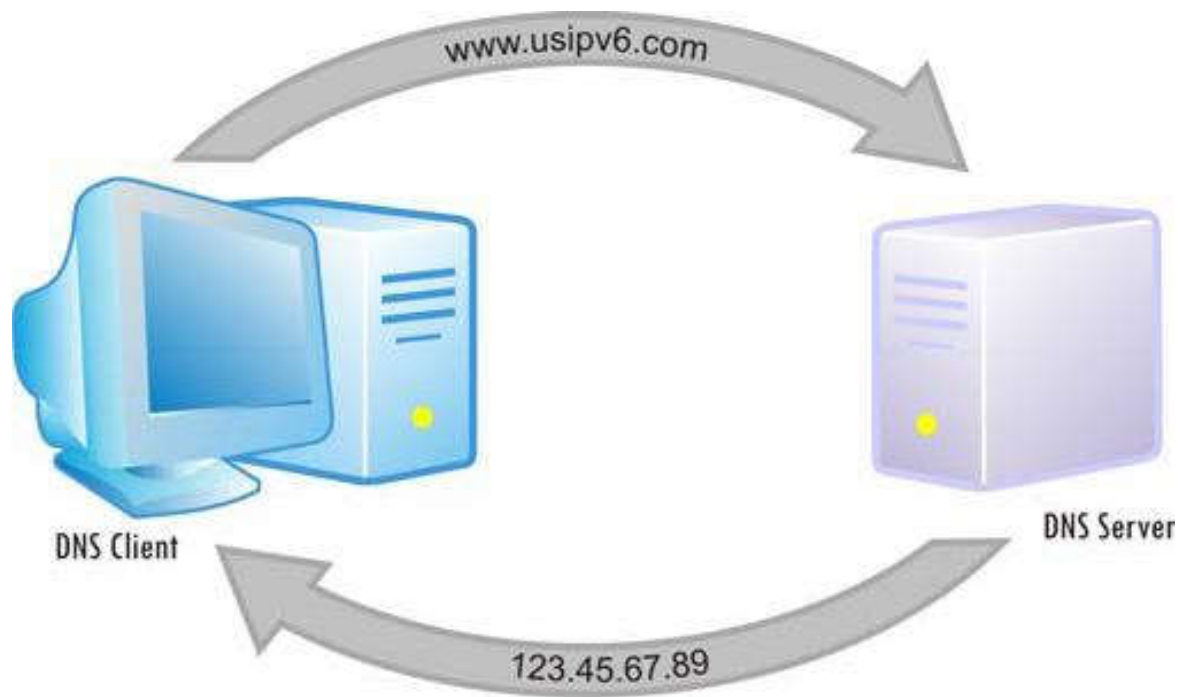
Services et protocoles DNS

Le service DNS est un service basé sur le modèle client/serveur.

Le client DNS, nommé **résolveur DNS**, s'exécute lui-même en tant que service.

Ce client prend charge la **résolution** de noms pour les autres applications et services qui en ont besoin.

Services et protocoles DNS



Utilisation de DNS

Lors de la configuration d'un périphérique réseau, on fournit l'adresse d'au moins un serveur DNS (donné généralement par le FAI).

Le client DNS interroge ce serveur DNS pour répondre aux demandes des applications devant se connecter à un périphérique distant à l'aide d'un nom.

L'outil **nslookup** permet à l'utilisateur d'envoyer une requête « manuellement » vers le serveur DNS.

Fonctionnement d'un serveur DNS

Un serveur DNS stocke différents types d'enregistrements contenant :

- Nom
- Adresse
- TTL
- Nombreux types d'enregistrements. Exemple :
 - A : adresse de périphérique final
 - NS : serveur de noms autorisé (i.e fiable)
 - CNAME : nom canonique (ou nom de domaine complet)
 - MX : enregistrement d'échange de mails

Fonctionnement d'un serveur DNS

Lorsqu'un client effectue une demande, le processus démon du serveur regarde dans sa propre table d'enregistrements.

S'il ne peut résoudre le nom, il contacte d'autres serveurs de noms. Il complétera sa propre table avec les réponses reçues des autres serveurs (mise en cache).

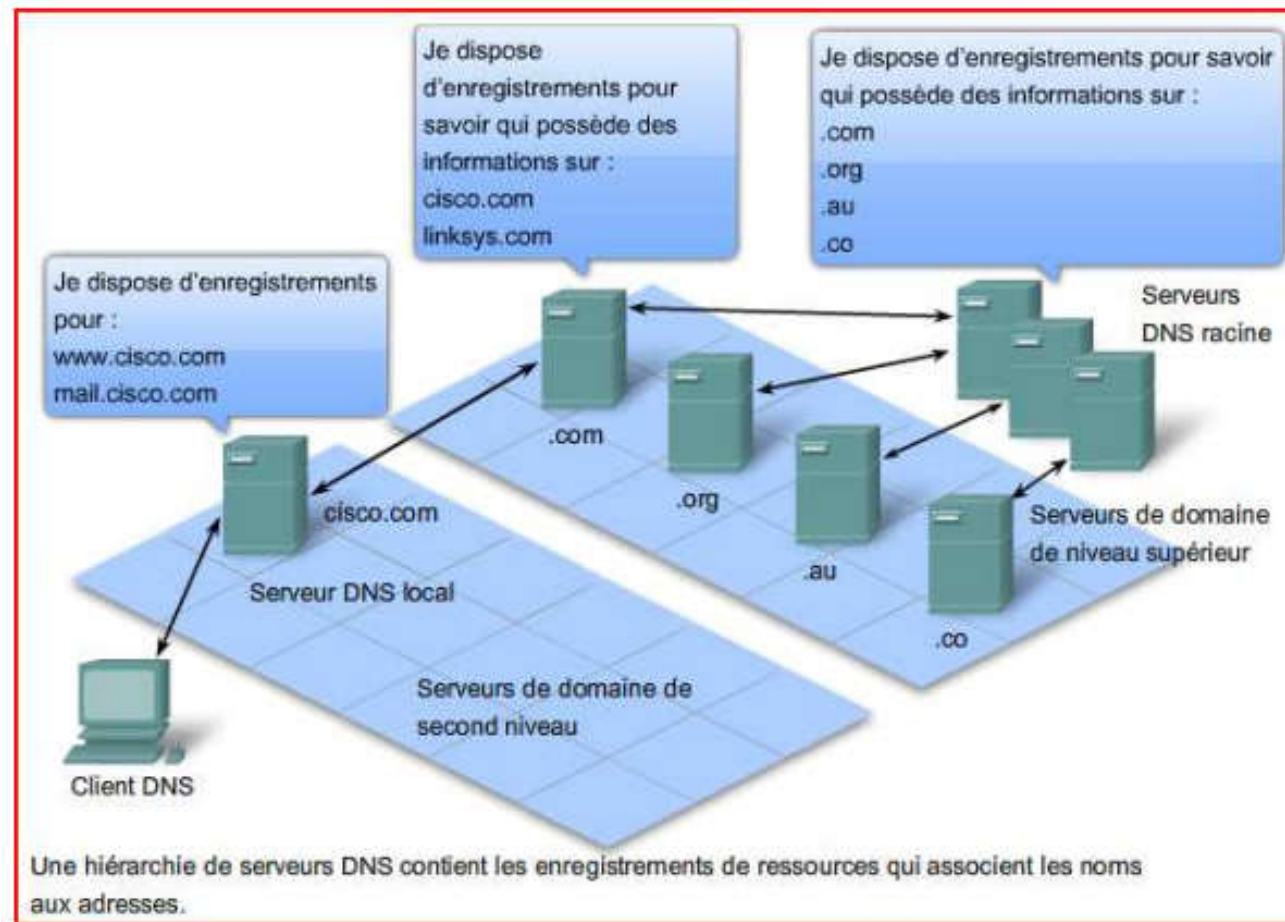
Remarque : le service client DNS de nos PC stockent également en mémoire les noms déjà résolus.

Hiérarchie de serveurs

Le protocole DNS se base sur la hiérarchie arborescente définissant les domaines.

Il existe ainsi un serveur DNS en charge de chaque sous-domaine identifié par un label qui dispose des enregistrements concernant ce niveau : on dit qu'il est **autorisé** pour ces enregistrements.

Hiérarchie de serveurs



Reverse DNS

Connu sous le nom : enregistrement PTR

Permet de retrouver un nom de domaine à partir d'une adresse IP.

Permet d'effectuer des contrôles

Exemple : pour l'envoi de mails (contre le spam). On vérifie que l'adresse IP de l'émetteur correspond bien au nom de domaine associé.

Commandes :

nslookup ADD_IP (windows, Unix)

dig -x ADD_IP (MacOS)

Reverse DNS

Aujourd'hui, l'utilisation de rDNS comme solution antiSpam se contente de vérifier l'existence du PTR sans comparer les domaines.

Autres techniques pour contrôler le spam :

SPF : Sender Policy Framework

DKIM : DomainKey Identified Mail

Service DHCP

Dynamic Host Configuration Protocol

Service automatisant l'affectation des adresses IP, des masques de sous-réseau, des paramètres de passerelle....

Permet une grande flexibilité dans l'organisation d'un réseau.

Permet d'accéder à internet via des points d'accès sans fil.

Service DHCP

Exemple

Lorsqu'un hôte se connecte au réseau, il demande au serveur DHCP une adresse **IP dynamique**.

Le serveur DHCP choisit une adresse dans une plage d'adresses prédéfinie (nommée pool d'adresses) et affecte celle-ci pour une **durée définie**.

Une fois l'hôte déconnecté, l'adresse retourne dans le pool pour être attribuée à un autre hôte.

Service DHCP

Les périphériques exécutent des logiciels clients.

Le serveur DHCP échange avec ses clients afin d'attribuer les adresses IP.

Dans les réseaux de taille moyenne ou grande, le serveur DHCP tourne généralement sur un ordinateur dédié.

Dans un réseau domestique, il est situé au niveau du FAI (pour la box).

Service DHCP

Le service DHCP peut représenter un risque pour la sécurité du réseau.

Beaucoup de réseaux utilisent à la fois l'adressage statique et l'adressage dynamique (DHCP) :

- l'adressage statique est utilisé pour les périphériques réseaux (passerelles, commutateurs, serveurs,...)
- DHCP est utilisé pour les hôtes à utilisation générale.

Service DHCP

Fonctionnement

Lorsqu'un périphérique configuré pour DHCP se connecte au réseau, son client diffuse un paquet **DHCP DISCOVER** afin d'identifier le(s) serveur(s) DHCP.

Le serveur répond avec un paquet **DHCP OFFER** : message d'offre de **bail** indiquant :

- l'adresse IP,
- le masque de sous-réseau,
- le serveur DNS,
- la passerelle par défaut,
- la durée du bail.

Service DHCP

Fonctionnement

Dans le cas où le réseau dispose de plusieurs serveurs DHCP, le client peut recevoir plusieurs paquets DHCP OFFER. Il doit alors choisir parmi ceux-ci et diffuser un paquet **DHCP REQUEST** qui identifie son choix.

Le bail doit être renouvelé avant expiration en utilisant un nouveau message DHCP REQUEST.

Service DHCP

Remarque

Il est possible pour un client de demander une adresse déjà attribuée précédemment.

Dans ce cas, le serveur retourne le message DHCP ACK.

S'il est impossible de réutiliser la même IP, le serveur répondra DHCP NAK.

Dans ce dernier cas, le client doit recommencer le processus avec un nouveau message DHCP DISCOVER.

Conclusion

La couche application repose soit sur le modèle client/serveur, soit peer-to-peer.

C'est la seule couche qui interagit directement avec l'utilisateur.

Par conséquent, elle offre un certain nombre de services permettant d'aborder les concepts purement réseau de manière plus « humaine ».

Il existe un très grand nombre de services et protocoles propres à la couche application. Nous en étudierons dans la prochaine partie.