Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S5

Couche Application

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes

2009/2010

Introduction

Introduction
Couche Application

Elle se situe au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures.

Les applications de cette couche communiquent donc grâce à un des deux protocoles de la couche transport, TCP ou UDP, elles sont de différents types, mais la plupart sont des services réseau, c'est-à-dire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation.

Introduction
Couche Application

On peut les classer selon les services qu'ils rendent :

- Les services de gestion (transfert) de fichier et d'impression,
- Les services de connexion à distance,
- Les utilitaires Internet divers.
- …etc

Les différents protocole existants dans cette couches : TELNET, SSH, FTP, DNS, SNMP, HTTP, SMTP, POP…..

Le protocole HTTP (Port 80)

Le protocole HTTP

HTTP (Hyper Text Transfer Protocol) est le protocole de communication du web permettant d'échanger des documents hypertextes contenant des données sous la forme de texte, d'images fixes ou animées et du son.

Tout client web communique avec le port 80 d'un serveur HTTP par l'intermédiaire d'une, ou plusieurs, connexions TCP simultanées, chacune des connexions TCP ouvertes servant à récupérer l'un des composants de la page web.

Le protocole HTTP (Requête)

GET /~ferment/http/prog/page_test1.html HTTP/1.1

Connection: Keep-Alive
User-Agent: Mozilla/5.0 (compatible; Konqueror/3.1; Linux; Fr)
Referer: http://www.u-picardie.fr/~ferment/http/prog/
Pragma: no-cache
Cache-control: no-cache
Accept: text/html, image/jpeg, image/png, text/*, image/*, */*
Accept-Encoding: x-gzip, x-deflate, gzip, deflate, identity
Accept-Charset: iso-8859-1, utf-8; q=0.5, *; q=0.5
Accept-Language: fr, en
Host: www.u-picardie.fr

Eventuel corps **……..**

Le protocole HTTP (Réponse)

HTTP/1.1 200 OK

Date: Tue, 22 Jun 2004 13:18:15 GMT
Server: Apache/1.3.26 (Unix) Debian GNU/Linux PHP/4.1.2 mod_ssl/2.8.9 OpenSSL/0.9.6g DAV/1.0.3
Last-Modified: Tue, 22 Jun 2004 13:15:43 GMT
ETag: "63f3d-8e-40d830ff
Accept-Ranges: bytes
Content-Length: 142
Keep-Alive: timeout=15, max=2000
Connection: Keep-Alive
Content-Type: text/html

<Html> <Body><h1>page html **</h1> ** contenant une image **
et une seule<img src="balle.gif“> </Body><Html>**

Le protocole HTTP (code de réponse)

Code	Classe	Usage
1xx	Information	Informationnel : demande reçu, processus continue…
2xx	Succès	L'action a été correctement reçue, interprétée, et exécutée…
3xx	Redirection	Une décision supplémentaire doit être prise pour terminer la requête...
4xx	Erreur Client	La requête présente une erreur de forme et ne peut être satisfaite…
5xx	Erreur Serveur	La requête est valide, mais le serveur ne peut la satisfaire….

Le protocole HTTP et TCP

No.	Time	Source	Destination	Proto Info
1	0.000000	192.168.0.10	192.168.0.253	TCP 1282 > 80 [SYN]
2	0.000163	192.168.0.253	192.168.0.10	TCP 80 > 1282 [SYN, ACK]
3	0.000565	192.168.0.10	192.168.0.253	TCP 1282 > 80 [ACK]
4	0.001410	192.168.0.10	192.168.0.253	HTTP GET / HTTP/1.1
5	0.001487	192.168.0.253	192.168.0.10	TCP 80 > 1282 [ACK]
6	0.068550	192.168.0.253	192.168.0.10	HTTP HTTP/1.1 200 OK
7	0.098435	192.168.0.10	192.168.0.253	HTTP GET /images/tux.gif HTTP/1.1
8	0.098593	192.168.0.253	192.168.0.10	TCP 80 > 1282 [ACK]
9	0.099450	192.168.0.253	192.168.0.10	HTTP HTTP/1.1 200 OK
10	0.099724	192.168.0.253	192.168.0.10	HTTP Continuation
11	0.102794	192.168.0.10	192.168.0.253	TCP 1282 > 80 [ACK]
12	0.102915	192.168.0.253	192.168.0.10	HTTP Continuation
13	0.280331	192.168.0.10	192.168.0.253	TCP 1282 > 80 [ACK]

Le protocole HTTP

A Etudier

- Les méthodes(**GET,** POST, OPTIONS, PUT, DELETE, TRACE, CONNECT)
- Les connexions persistantes
- Gestion d'une connexion HTTP avec pipelining
- Négociation de contenu
- Le caching en HTTP
- L'authentification HTTP

DNS (Domaine Name Systèm)
port 53

DNS

Chaque station possède une adresse IP propre. Cependant, il n'est pas commode de travailler avec des adresses numériques du genre 194.153.205.26, la solution est d'utiliser des noms de stations ou des adresses plus explicites du style http://www.yahoo.fr/.

Ainsi, TCP/IP permet d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name Service).

On appelle résolution de noms de domaines la corrélation entre les adresses IP et le nom de domaine associé.

DNS

Avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallut mettre en place un système plus centralisé de gestion des noms. Ce système est nommé Domain Name System, ou Système de nom de domaine.

Ce système est mis en œuvre par une base de données distribuée au niveau mondial et Les noms sont gérés par un organisme mondial : l'interNIC et les organismes délégués : NIC France, NIC Angleterre, etc.

Le système est basé sur le modèle client / serveur tel que le logiciel client interroge un serveur de nom.

DNS

L'utilisateur associe un nom de domaine à une application,

Exemple : **Telnet www.yahoo.fr ou http//: www.yahoo.fr**

- L'application cliente requiert la traduction du nom de domaine auprès d'un serveur de nom (DNS) : cette opération s'appelle la **résolution de nom**.
- Le serveur de noms interroge d'autres serveurs de noms jusqu'à ce que l'association nom de domaine / adresse IP soit trouvée.

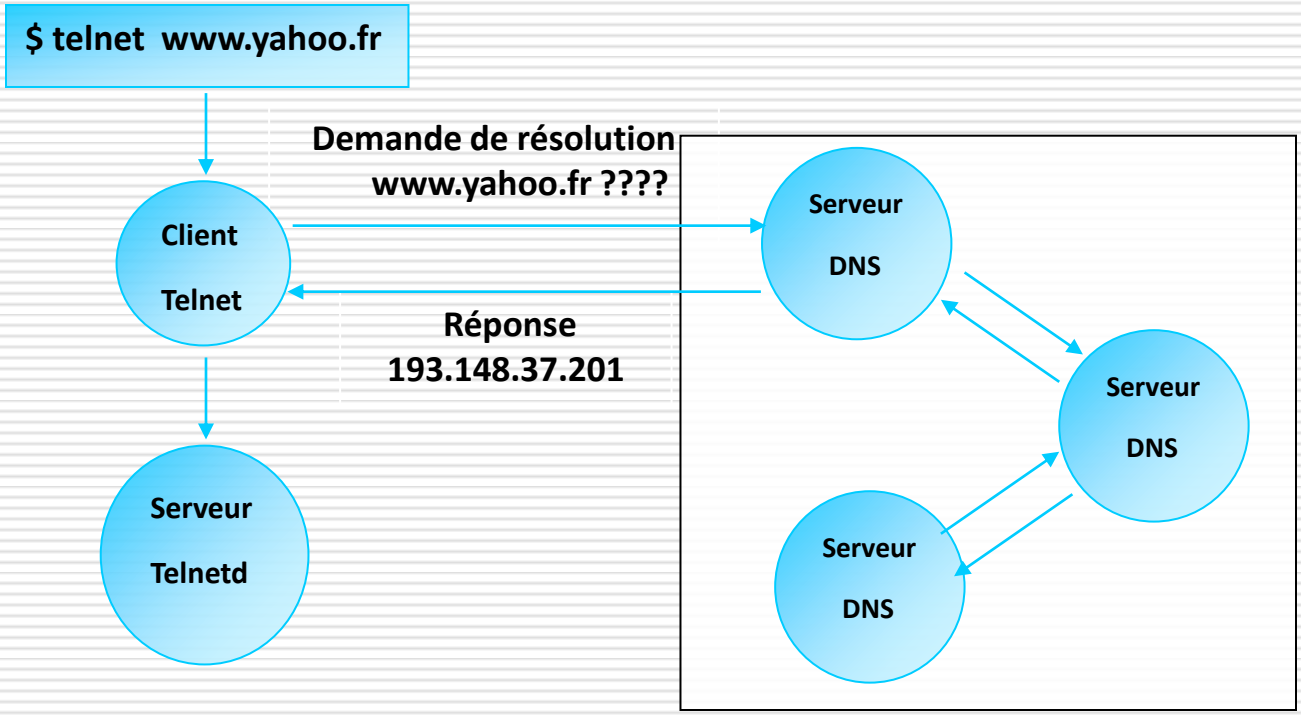
DNS

- Le serveur de noms retourne l'adresse IP au logiciel client par exemple : 193.148.37.201.

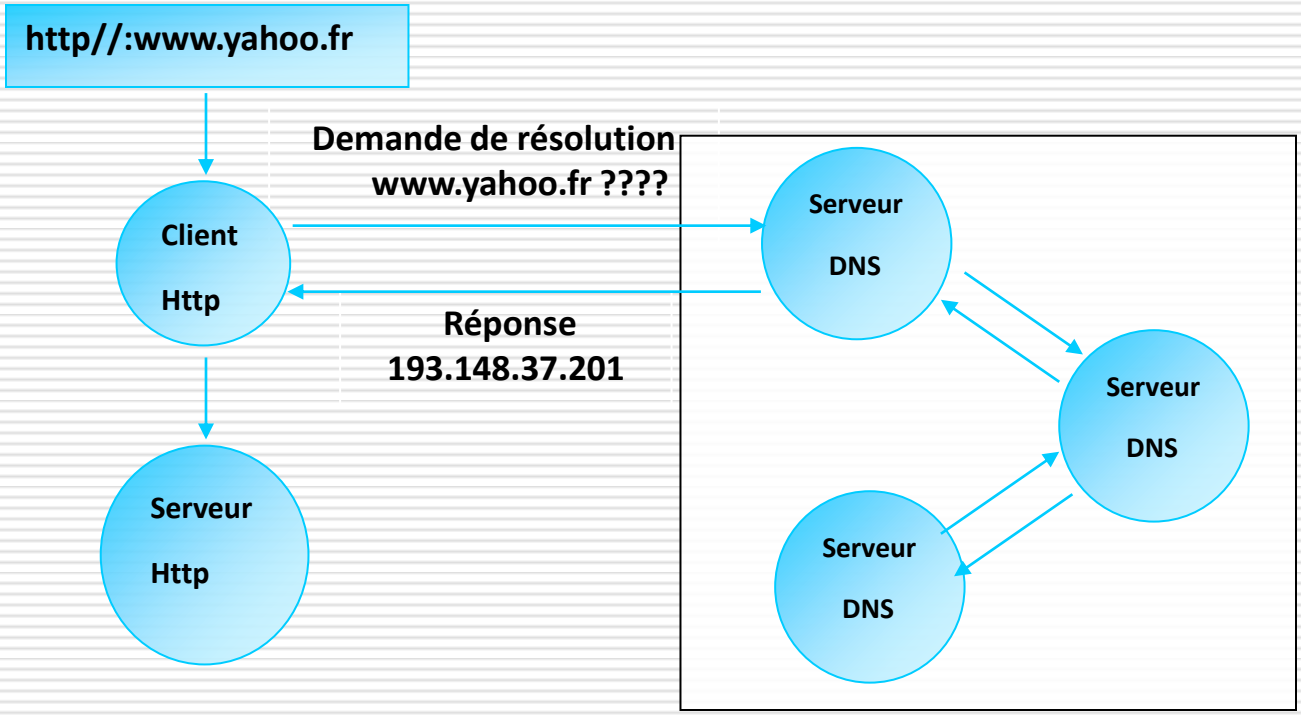
- Le logiciel client contacte le serveur (telnetd) comme si l'utilisateur avait spécifié une adresse IP :

  Telnet 193.148.37.201 ou http//:193.148.37.201

DNS (Telnet)


$ telnet www.yahoo.fr
Demande de résolution
www.yahoo.fr ????
Client
Telnet
Réponse
193.148.37.201
Serveur
Telnetd
Serveur
DNS
Serveur
DNS
Serveur
DNS

DNS(Http)


http//:www.yahoo.fr
Demande de résolution
www.yahoo.fr ????
Client
Http
Réponse
193.148.37.201
Serveur
Http
Serveur
DNS
Serveur
DNS
Serveur
DNS

L'espace Nom de domaine

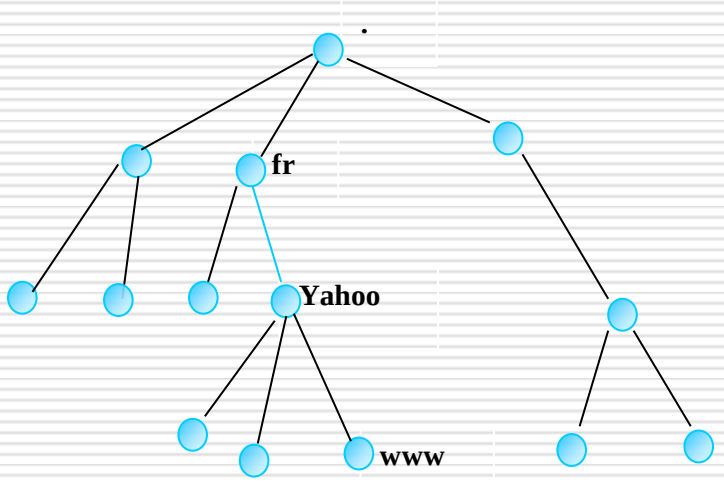
L'espace Nom de domaine

Les noms constituent un chemin dans un arbre inversé appelé *l'espace Nom de domaine* dont l'organisation est similaire à un système de gestion de fichiers.

Chaque nœud de l'arbre est identifié par un nom et la racine est appelée root, identifiée par «.».

Prenons l'exemple : **www.yahoo.fr**

Un nom de domaine est la séquence de labels depuis le nœud de l'arbre correspondant jusqu'à la racine. Deux nœuds fils ne peuvent avoir le même nom donc unicité d'un nom de domaine au niveau mondial.



Notion de Domaine

Notion de Domaine

Un domaine est un sous-arbre de l'espace nom de domaine.

Les machines sont reliées entre elles dans un même domaine logiquement et non par adressage.
Exemple : 10 machines d'un même domaine appartiennent à 10 réseaux différents et recouvrent 6 pays différents.

Domaines racine Il existe 7 domaines racines prédéfinis :

Notion de Domaine

com : organisations commerciales ; ibm.com

edu : organisations concernant l'éducation ; mit.edu

gov : organisations gouvernementales ; nsf.gov

mil : organisations militaires ; army.mil

net : organisations réseau Internet ; worldnet.net

org : organisations non commerciales ; eff.org

int : organisations internationales ; nato.int

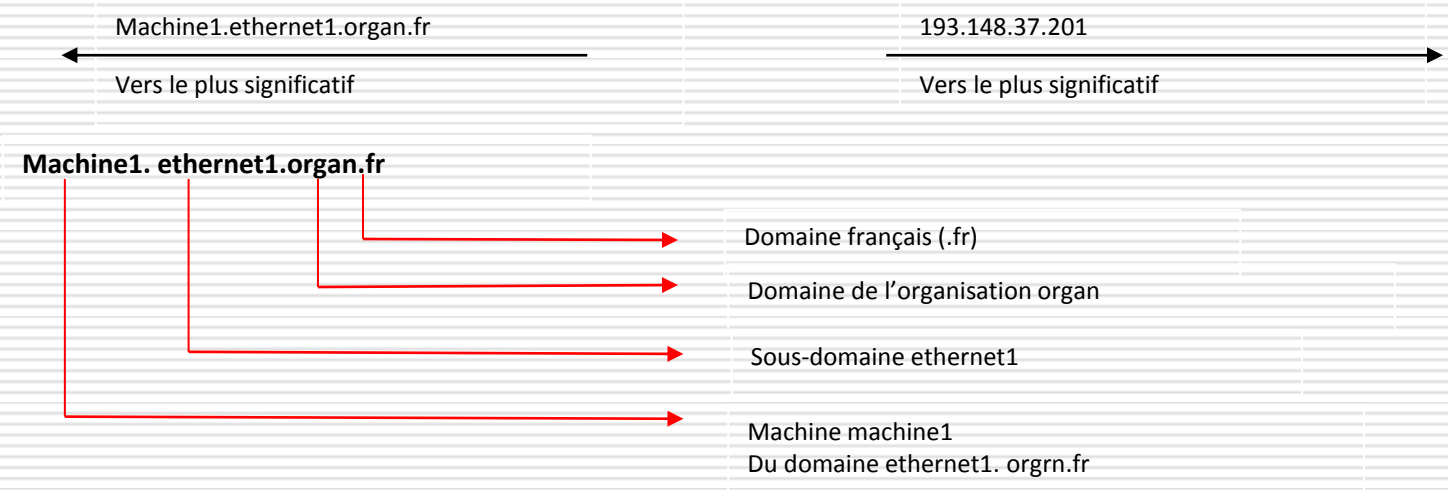
arpa : domaine réservé à la résolution de nom inversée

organisations nationales *: fr, uk, de, it, us, au, ca, se,dz …etc.*

Lecture des noms de domaine

Lecture des noms de domaine

À l'inverse de l'adressage IP la partie la plus significative se situe à gauche de la syntaxe :



Autres protocoles
(Résumés)

Le protocole DHCP

DHCP

Dynamic Host Configuration Protocol (DHCP) est un terme anglais désignant un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, 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 des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).

DHCP

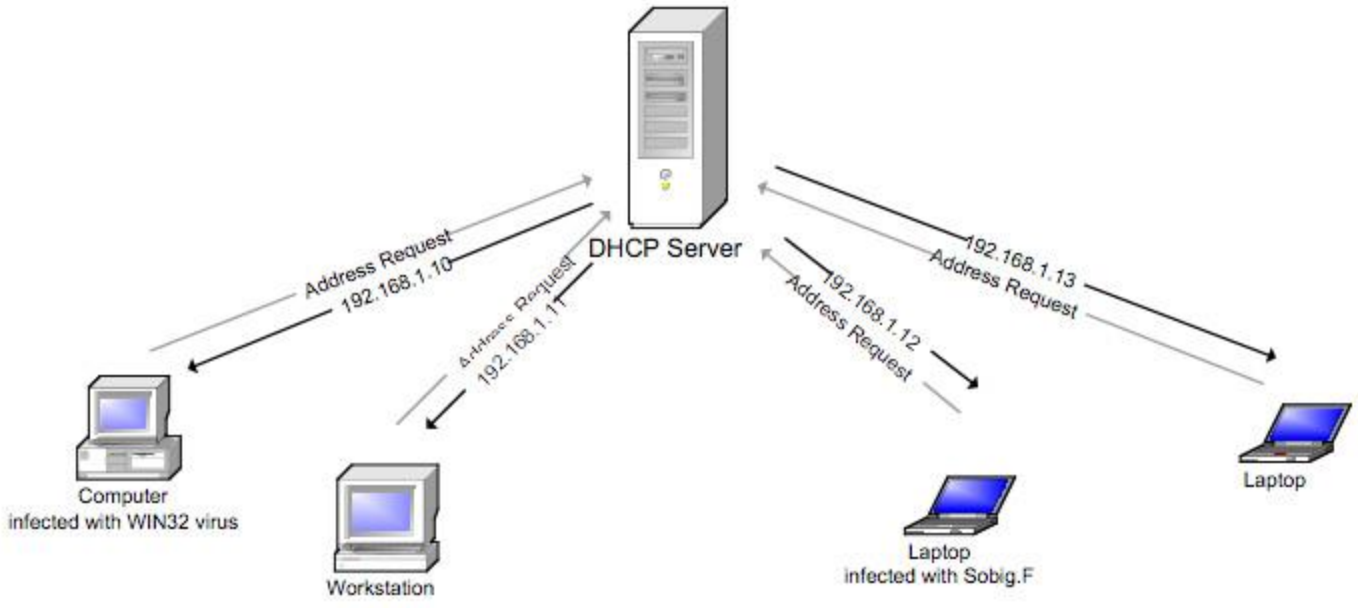


Figure 1: Standard DHCP provides IP addresses to all machines

Le protocole TELNET **(Port 23)**

TELNET

Telnet (***TE****rmina****l*** ***NET****work* ou ***TEL****ecommunication* ***NET****work*, ou encore ***TEL****etype* ***NET****work*) est un protocole réseau utilisé sur tout réseau supportant le protocole TCP/IP. Il appartient à la couche session du modèle OSI et à la couche application du modèle ARPA.

Selon, l'IETF, le but du protocole Telnet est de fournir un moyen de communication très généraliste, bi-directionnel et orienté octet.

Telnet est aussi une commande permettant de créer une session Telnet sur une machine distante. Cette commande a d'abord été disponible sur les systèmes Unix, puis elle est apparue sur la plupart des systèmes d'exploitation.

TELNET (**Défaut de sécurité**)

Le côté sommaire de Telnet fait que toute communication est transmise en clair sur le réseau, mots de passe compris.

Des *sniffeurs* comme tcpdump ou Wireshark permettent d'intercepter les communications de la commande telnet.

Des protocoles chiffrés comme SSH ont été développés pour fournir un accès distant remplaçant Telnet et dont l'interception ne fournit aucune donnée utilisable à un éventuel espion.

Le protocole SSH **(Port 22)**

Le protocole SSH (Secure Shell**)**

Les protocoles d'accès distant à une machine tels que Telnet, rlogin, etc.. Sont limités:

- Circulation des mots de passe en clair
- Authentification faible basée sur le numéro IP

(Cas du protocole rlogin)

- Commandes à distance non sécurisées.
- Transferts de fichiers non sécurisés.

Solution: l'utilisation du protocole SSH

SSH utilise la cryptographie asymétrique (RSA) et Symétrique (à étudier dans le module sécurité informatique)

Faille du protocole SSH

.

- Attaque à base de la méthode Man In The Middle
- L'attaquant se place entre le client et le serveur afin d'intercepter les clés de l'encryptage.

Le protocole FTP **(Port 21)**

Le protocole FTP

Le ***File Transfer Protocol*** (protocole de transfert de fichiers), ou **FTP**, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.

Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

Le protocole, qui appartient à la couche session du modèle OSI et à la couche application du modèle ARPA, utilise une connexion TCP. Il peut s'utiliser de deux façons différentes :

Le protocole FTP

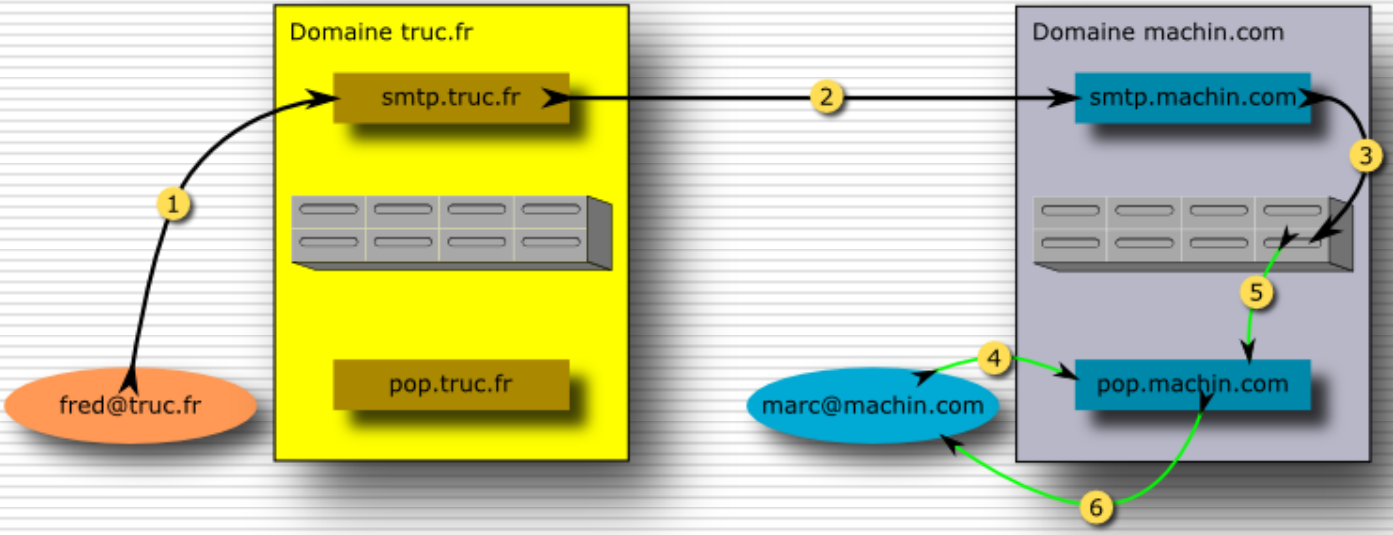
Mode actif : c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données.

Mode passif : le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client.

Messagerie électronique

Les protocoles SMTP **(Port 25)**,
POP **(Port 109/110)** et autres

Messagerie électronique



Et beaucoup d'autres protocoles:

- SNMP (Port 161)
- https (Port 443)
- Imap (Port 143)
- TFTP (Port 69)
- …etc.

Conclusion

Conclusion

Une bonne compréhension de TCP/IP est nécessaire si l'on souhaite savoir comment les données transitent sur les réseaux et bien comprendre les différents mécanismes d'interconnexion que ce soit matériel ou logiciel.