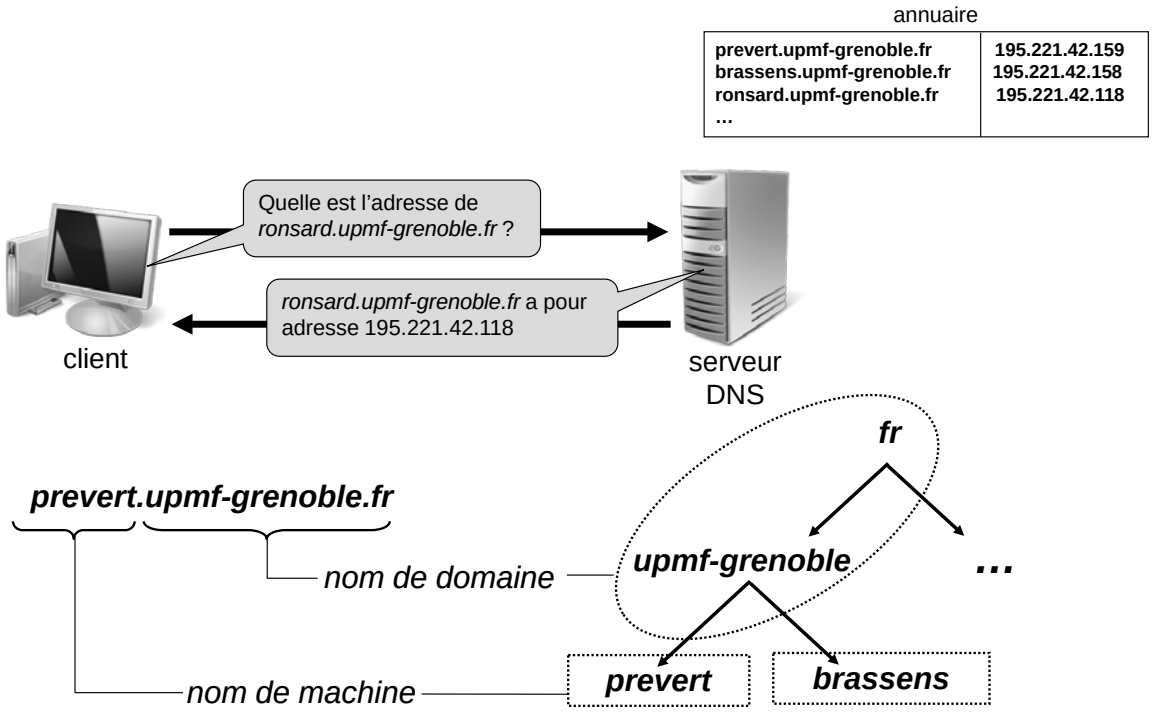
5 Quelques protocoles applicatifs

1. DNS

Le système DNS (*Domain Name System*) permet d'associer des noms symboliques à des adresses numériques. Comme les adresses IP, les noms symboliques sont **structurés** et **hiérarchiques**

- une partie désigne le **nom de la machine** (*hostname*)
- l'autre partie désigne le **nom de domaine** (*domain name*) auquel la machine appartient.

Dans chaque domaine, un serveur de noms ou serveur DNS est chargé de répondre aux requêtes des clients (les clients internes comme les clients externes au domaine). Le système DNS s'appuie sur le protocole de transport UDP (port 53).



2. FTP

Le protocole FTP (*File Transfer Protocol*) est un protocole de transfert de fichiers décrit par le RFC 959 (*File Transfer Protocol (FTP) - Specifications*). Ce dernier définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP.

Le protocole FTP a pour objectifs de :

- permettre un partage de fichiers entre machines distantes
- permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
- permettre de transférer des données de manière efficace

Le protocole FTP s'inscrit dans un modèle client/serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur). Lors d'une connexion FTP, deux canaux de transmission sont ouverts (port 21 et port 20 en TCP) :

- Un canal pour les commandes (canal de contrôle)
- Un canal pour les données

3. Telnet / SSH

Le protocole Telnet (*TErminaL NETwork protocol*) est utilisé pour **émuler une connexion de terminal** à un hôte distant. Telnet utilise TCP comme protocole de transport afin de transmettre les informations entre le clavier de l'utilisateur et l'hôte distant, ainsi que pour afficher des informations en provenance de l'hôte distant sur l'écran de l'utilisateur.
Telnet fonctionne en client/serveur : le client se trouve sur la station de travail de l'utilisateur ; le serveur sur l'hôte distant. Le serveur écoute sur le port TCP 23. Le client initie la connexion.

Attention : lors d'une session Telnet, le nom de l'utilisateur (login) et le mot de passe sont transmis en clair (c'est-à-dire sans chiffrement) à travers le réseau.

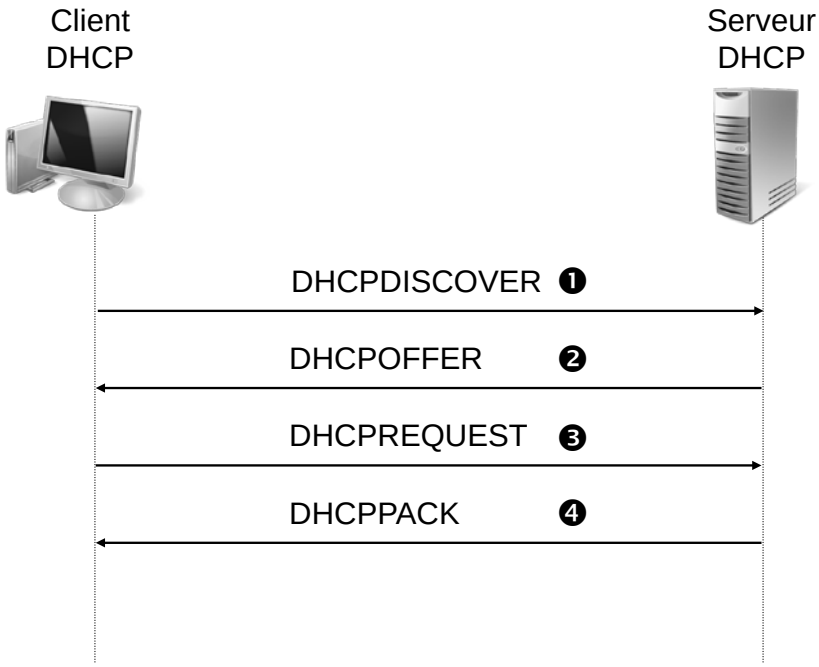
SSH (*Secure Shell*) est à la fois la définition d'un protocole et un ensemble de programmes permettant :
- des sessions interactives depuis une machine cliente à distance sur des serveurs
- de transférer des fichiers entre deux machines de manière sécurisée

Ces programmes ont pour but de remplacer les utilitaires de connexions classiques n'utilisant pas de chiffrement (**rlogin**, **rcp**, **rsh** et **telnet** notamment). SSH utilise la cryptographie pour protéger les communications entre le client et le serveur. SSH permet également d'identifier les utilisateurs et machines en présence à l'aide de clés.
Le serveur SSH écoute sur le port TCP 22. Le client initie la connexion.

4. DHCP

DHCP (*Dynamic Host Configuration Protocol*) est un protocole d'attribution d'adresses défini par la RFC 2131. Il permet la **configuration automatique** des paramètres TCP/IP (adresse IP, masque, gateway …) des différents hôtes du réseau.

Il s'agit d'un protocole conçu comme une extension du protocole BOOTP (*Bootstrap Protocol*) et fonctionnant en client/serveur. Il s'appuie sur UDP (ports 67 et 68).
DHCP utilise 3 méthodes d'allocation des adresses IP
- allocation manuelle : attribution par le serveur DHCP d'une adresse IP définie par l'administrateur
- allocation automatique : attribution automatique par le serveur DHCP d'une adresse IP
- allocation dynamique : attribution par le serveur DHCP d'une adresse IP pour une certaine durée (bail)



❶·Le client (d'adresse IP inconnue 0.0.0.0) envoie une requête DHCPDISCOVER en broadcast (255.255.255.255) dans laquelle il insère son adresse MAC.
Avant d'envoyer le paquet de diffusion DHCPDISCOVER, le client marque une pause aléatoire pouvant aller de 1 à 10 secondes. Cela permet d'éviter que tous les clients DHCP n'envoient leurs requêtes en même temps au moment où l'alimentation électrique est rétablie.
Il peut exister au sein d'un même réseau plusieurs serveurs DHCP (c'est même conseillé). Le client sélectionne alors une réponse DHCPOFFER parmi plusieurs, et envoie un message DHCPREQUEST au serveur correspondant.
❷·Le serveur lui répond avec un DHCPOFFER émis aussi en broadcast, qui contient l'adresse MAC du client, la durée du bail et l'adresse IP du serveur.
❸·Si le client accepte, il envoie un DHCPREQUEST pour recevoir les paramètres.
❹·Le serveur envoie un DHCPACK confirmant que le client accepte.

A l'issue du DHCPPACK, le client peut éventuellement vérifier que l'adresse IP que lui envoie le serveur n'est pas en cours d'utilisation en envoyant simplement une requête ARP en diffusion à l'adresse indiquée. Si l'adresse est déjà utilisée, le client l'ignorera et enverra au serveur un message DHCPDECLINE.

5. Utilisation de TCP/IP

5.1. Avantages

- gratuit
- ouvert
- indépendant des constructeurs
- disponibles sur tous les types de matériel : micro-ordinateur, station de travail, super calculateur et équipements réseaux.
- facile à installer

- produits éprouvés depuis longtemps dans un monde hétérogène
- inclut de très nombreuses applications
- bien standardisé et documenté
- les protocoles sont simples mais efficaces

5.2. Handicaps

- les standards sont édités aux USA ; il n'y a pas de norme internationale
- la plage d'adresses IPv4 est désormais épuisée[2]
- le protocole est très ouvert : on peut créer facilement un réseau que rapidement on ne peut plus gérer
- il n'y a pas de routage basé sur l'adresse d'origine
- la sécurité n'est pas prise en compte dans la conception. De plus le mode non-connecté est un problème difficile pour la sécurité

[2] L'IANA, filiale de l'ICANN, société californienne à but non lucratif, a attribué en février 2011 le dernier «gros bloc» de 16 millions d'adresses IPv4 (/8) à ses partenaires.