الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 1945 Guelma

Faculté des Sciences et de la Technologie
Département d'électronique et Télécommunications

Support de cours : Pour Master 1 Réseaux et Télécommunications
(Semestre 06 Unité d'enseignement UEF 1.2.1)

Matière :
Administration des services réseaux

Chargé de la Matière :
Dr. IKNI Samir

Version récente (2019/2020)

Matière : Administration des services réseaux

Chapitre I : Présentation de l'administration réseau

I.1. Introduction : Objectifs et rôle de l'administration :

L'objectif de l'administration réseau et d'assurer l'évolutivité, la maintenance et le bon fonctionnement d'une infrastructure réseau au sein d'une société ou entreprise. Il s'agit de faire en sorte que le réseau puisse fonctionner de manière autonome de façon à minimiser les interventions manuelles. Par exemple, l'utilisation de protocoles de routage dynamique, tels que RIP, OSPF ou EIGRP, permet de pallier aux défaillances d'équipements actifs pour que des chemins alternatifs existent toujours. Un deuxième exemple serait le protocole DHCP permettant de simplifier la configuration des ordinateurs et offre plus de souplesse pour modifier le plan d'adressage IP. En outre, pour s'assurer que les services rendus par le réseau soient convenables et sécurisés, il est nécessaire de surveiller et d'agir quand un incident (erreur ou intrusion) se produit, nous parlons alors de l'***administration réseaux***.

L'administration peut concerner des concentrateurs, commutateurs, routeurs, modems, pare-feu, proxy, connectivité Internet et des réseaux privés virtuels (VPN). Donc un administrateur réseau sera chargé des tâches suivantes :

a. gestion de connexion physique entre plusieurs machines ;
b. gestion du routage (connexion logique entre l'intérieur et l'extérieur du réseau ou entre plusieurs sous-réseaux) ;
c. gestion de la sécurité (protection antivirale, pare-feu, prévention des intrusions etc.) ;
d. gestion des droits d'accès des utilisateurs (accès au réseau, etc.).

L'administrateur réseau veille à ce que tous les utilisateurs aient un accès rapide au système d'information de l'entreprise. Pour exercer ce métier, il faut avoir un sens de la logique, être minutieux et trouver une solution à des problèmes rapidement et le plus souvent à distance. Un administrateur n'a généralement pas d'horaire fixe. Il travaille le plus souvent dans son bureau, c'est de là qu'il gère les problèmes qui surviennent dans l'entreprise. Il doit réagir de toute urgence pour identifier la cause de l'incident, puis effectuer les réparations nécessaires dans les plus brefs délais. L'administrateur réseau doit assurer une constante veille technologique, et tester des nouveaux matériels pour les insérer, si besoin, dans son système.

I.2. Réseau clients serveurs

Dans un réseau client-serveur des machines clientes (faisant partie du réseau) contactent un serveur - une machine généralement très puissante en termes de capacités d'entrées-sorties - qui leur fournit des services ce qui permet d'exploiter au mieux les réseaux, et permet un haut niveau de coopération entre différentes machines sans que l'utilisateur se préoccupe des détails de compatibilité.

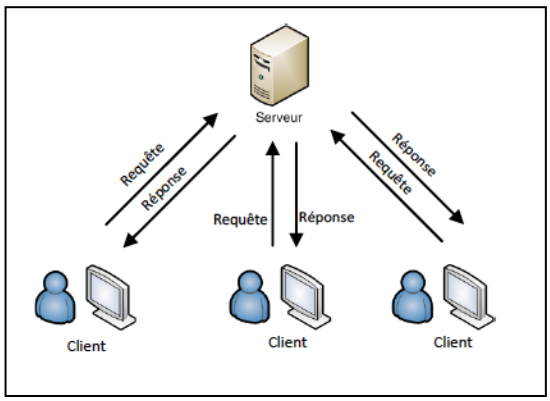
L'architecture client-serveur met en œuvre une conversation entre 2 programmes pour répondre aux objectifs précédemment cités.

I.2.1. Le serveur :

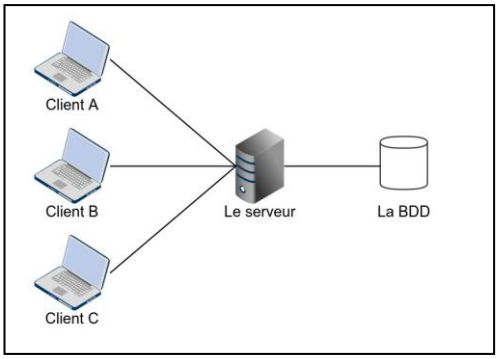
Un serveur est un programme qui tourne sur un ordinateur dans le seul but de répondre à des requêtes de logiciels tournant sur d'autres ordinateurs, donc le serveur est un ***fournisseur de services***.

I.2.2. Le client :

Un client est un programme tournant sur une machine cliente et qui permet, de soumettre des requêtes à un ou à plusieurs serveurs donc le client est un ***consommateur de services***.

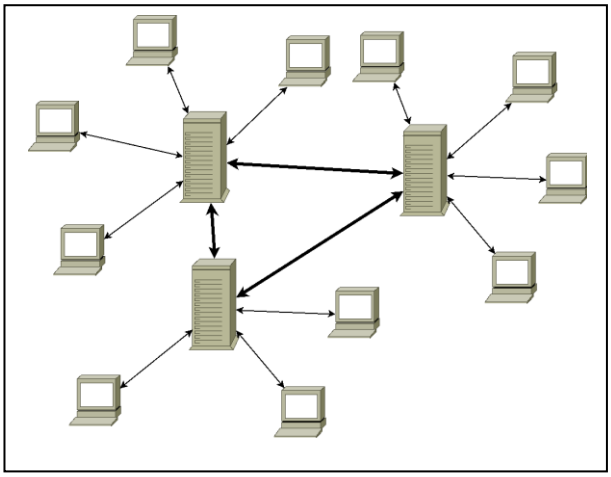


a. ***Architecture centralisée*** La première génération de client-serveur intègre des outils clients autour d'une base de données relationnelle centrale. L'application est développée sur le client qui dispose d'une interface graphique permettant de lancer des requêtes au serveur.



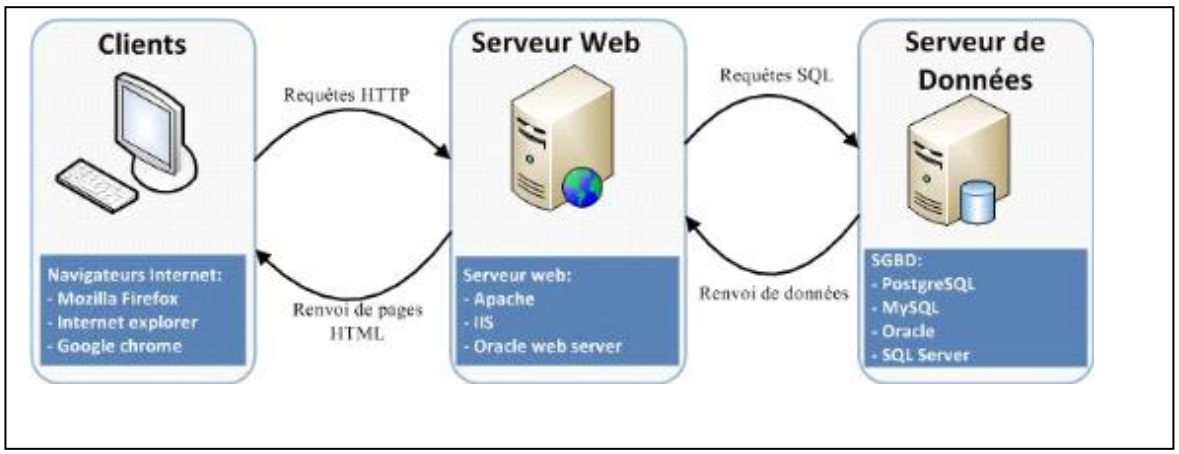
b- Architecture décentralisée Le client-serveur de deuxième génération est caractérisé par l'évolution des outils dans trois directions :

- Possibilité de développer des traitements sous forme de procédures stockées sur le serveur. Ces procédures sont soit appelées explicitement par les applications clientes, soit déclenchées par des événements survenant sur les données (triggers) ;
- Utilisation intensive de l'approche orientée objet aussi bien pour construire les interfaces que pour modéliser le système d'information ;
- Répartition des fonctions en trois niveaux : la présentation incombe au client, la gestion des données à un serveur de données, les traitements à un serveur d'applications.



c- Architecture universelle

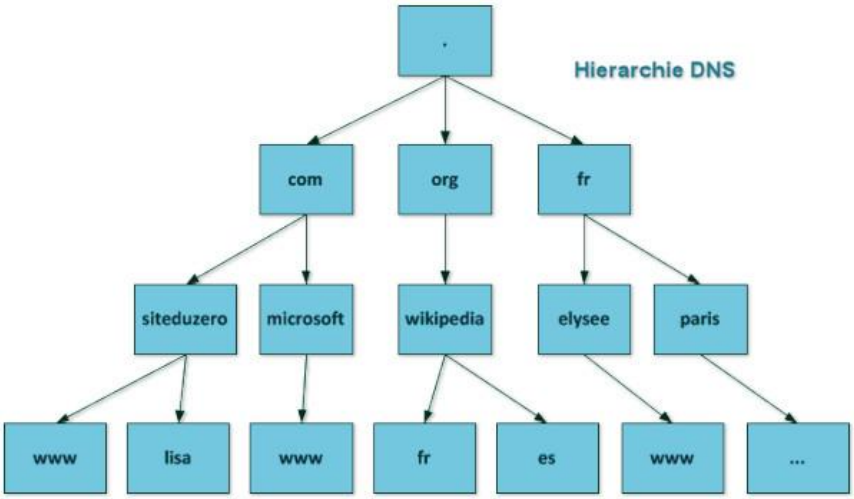
Cette génération de client-serveur s'appuie sur le compte de client léger représenté par un navigateur web. Celui-ci est chargé de la présentation et possède des possibilités d'exécution locale de traitements. Les serveurs sont spécialisés (données ou applications) et dispersés à travers un réseau étendu (Internet) ou local (Intranet).



I.3. Les services de la couche application

- **Le service DNS**

Le Domain Name System (ou DNS, système de noms de domaine) est un service de la couche application permettant de traduire un nom de domaine en adresse IP de la machine portant ce nom. Les équipements (hôtes) connectés à un réseau IP (Internet), possèdent une adresse IP qui les identifie sur le réseau. Ces adresses sont numériques afin de faciliter leur traitement par les machines. Pour faciliter l'accès aux hôtes sur un réseau IP, un mécanisme a été mis en place permettant d'associer un nom à une adresse IP, plus simple à retenir, appelé « nom de domaine ». Résoudre un nom de domaine consiste à trouver l'adresse IP qui lui est associée.



Le système des noms de domaines consiste en une hiérarchie dont le sommet est appelé la racine. On représente cette dernière par un point. Dans un domaine, on peut créer un ou plusieurs sous-domaines ainsi qu'une délégation pour ceux-ci, c'est-à-dire une indication que les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur. Ces sous-domaines peuvent à leur tour déléguer des sous-sous-domaines vers d'autres serveurs.

Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau (TLD : Top Level Domain). Les noms de domaines ne correspondant pas à une extension de pays sont appelés des domaines génériques (gTLD), par exemple .org ou .com. S'ils correspondent à des codes de pays (fr, be, ch…), on les appelle ccTLD (country code TLD).

Exemples de ccTLD : Au, de, es, fr, uk, us, …

Les entités au niveau 3 ce sont appelés « serveurs DNS d'autorité », et ceux de niveau 4 sont des Hôtes (machines).

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, le domaine org. est un TLD, sous-domaine de la racine. Le domaine wikipedia.org. est un sous-domaine de .org.
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.
Quelques exemples de domaines : com, edu, gov, int, mil, net, org.
Les serveurs racine sont actuellement au nombre de 13 et sont connus. Nous pouvons trouver leur liste, par exemple, ici : ftp://ftp.rs.internic.net/domain/named.root ce fichier est maintenu par l'InterNIC (Internet's Network Information Center) qui est devenu en 1998 Internet Corporation for Assigned Names and Numbers (ICANN).
FQDN : Le nom qualifié d'une machine (en anglais, fully qualified domain name ou FQDN), c'est-à-dire son nom complet comprenant le domaine, par exemple **guinness.b1-4.ensta.fr**, ne peux excéder 255 caractères. Chacun des composants (les parties entre deux points successifs) ne peut excéder 63 caractères et s'appelle également une « zone ».
Un nom de machine ou un nom de domaine ne peut contenir que :

e. des lettres (majuscules ou minuscules, aucune différence n'est faite à ce niveau).
f. des chiffres.
g. des tirets

Tout autre caractère est interdit.
Chaque zone dispose d'un ou plusieurs serveurs DNS. S'il y en a plusieurs, l'un d'eux est dit maître et les autres sont ses esclaves (on parlait de primaire et de secondaires dans l'ancienne terminologie du DNS). Le serveur maître est le vrai détenteur des informations de la zone, les esclaves se contentent de les recopier, c'est un serveur autoritaire ou d'autorité.
À chaque modification des informations d'une zone, le serveur maître avertit ses esclaves pour qu'ils puissent se mettre à jour. Toute modification sur le maître se répercute donc très rapidement sur ses esclaves. L'opération de mise à jour s'appelle un « transfert de zone ».
Le processus d'interroger les serveurs à partir de la racine jusqu'à l'hôte s'appelle la « résolution de nom ».

I.4. Notion de port

Quand un paquet contenant une requête arrive sur un serveur, comment l'OS sait à quel service il doit donner la requête ?
En fait, chaque paquet réseau contient :
- L'adresse IP de la machine d'origine (le client dans le cas d'une requête),

- L’adresse IP de la machine de destination (le serveur dans notre cas),

et une information qui permet de savoir à quel « service » est destinée le paquet. On parle alors de « numéro de port ».

L’expéditeur possède aussi un numéro de port, alloué dynamiquement et aléatoirement par le système, utilisé pour la réponse.

Le numéro de port occupe 16 Bits (une valeur entière comprise entre 0 et 65 535).

Les numéros de ports entrent dans différentes catégories définies par l'IANA (Internet Assigned Numbers Authority). Le document RFC1700 (Request For Comments) traite de la désignation des numéros de port.

I.3.1. Les ports bien connus (well known ports) : ce sont les ports entre 0 et 1023. Ils correspondent à des applications serveur très courantes.

Exemple : les services standards (dans **/etc/services** sous Unix, dans **%SystemRoot%\System32\drivers\etc\services** pour Windows).

Exemples :

telnet	**23/tcp**	**HTTP**	**80/tcp**
Smtp	**25/tcp**	**Pop3**	**110/tcp**
tftp	**69/udp**	**imap**	**143/tcp**

I.3.2. Les ports enregistrés (registered ports) : entre 1024 et 49151, utilisés par des applications clientes identifiées, ou des serveurs qui n'entrent pas dans la catégorie précédente.

I.3.3. Les ports dynamiques ou éphémères : au-delà de 49152, ce sont des ports qui ne peuvent pas être enregistrés, réservés aux connexions temporaires.

Un site peut offrir plusieurs services. Chacun de ces services est fourni sur **un port de communication** identifié par un **numéro**. Ce numéro identifie le service quel que soit le site (ex. le service HTTP est offert sur le port numéro 80, FTP le numéro 21...).

Pour accéder donc à un service, il faut préciser l'adresse du site et le numéro du port, on appelle le couple [adresse IP, num port] socket.

I.4. Notion de protocole

Un protocole est un ensemble de règles et procédures standards à respecter pour émettre et recevoir des données sur un réseau. Cette standardisation a pour but principal de permettre à deux programmes s'exécutant généralement sur différentes machines de communiquer et de se comprendre mutuellement et de manière harmonieuse.

Internet est un ensemble de protocoles regroupés sous le terme "TCP-IP" (Transmission Control Protocol/Internet Protocol).

I.4.1. Quelques protocoles qui peuvent être utilisés :

HTTP : (Hyper Texte Transfert Protocol) : c'est celui que l'on utilise pour consulter les pages web.

FTP : (File Transfert Protocol) : C'est un protocole utilisé pour transférer des fichiers.

SMTP : (Simple Mail Transfert Protocol) : c'est le protocole utilisé pour envoyer des mails.

POP : (Post Office Protocol) C'est le protocole utilisé pour recevoir des mails.

Telnet : (**tel**ecommunication **net**work) utilisé surtout pour commander des applications côté serveur en ligne.

IP (internet Protocol) (l'adresse IP) : il vous attribue une adresse lors de votre connexion à un serveur.

On classe généralement les protocoles en deux catégories selon le niveau de contrôle des données que l'on désire :

I.4.2. Les protocoles orientés connexion: Il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines.

Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice peut garantir la validité des données qu'elle envoie. TCP est un protocole orienté connexion.

I.4.3. Les protocoles non orientés connexion: Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'accusés de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes). UDP est un protocole non orienté connexion.

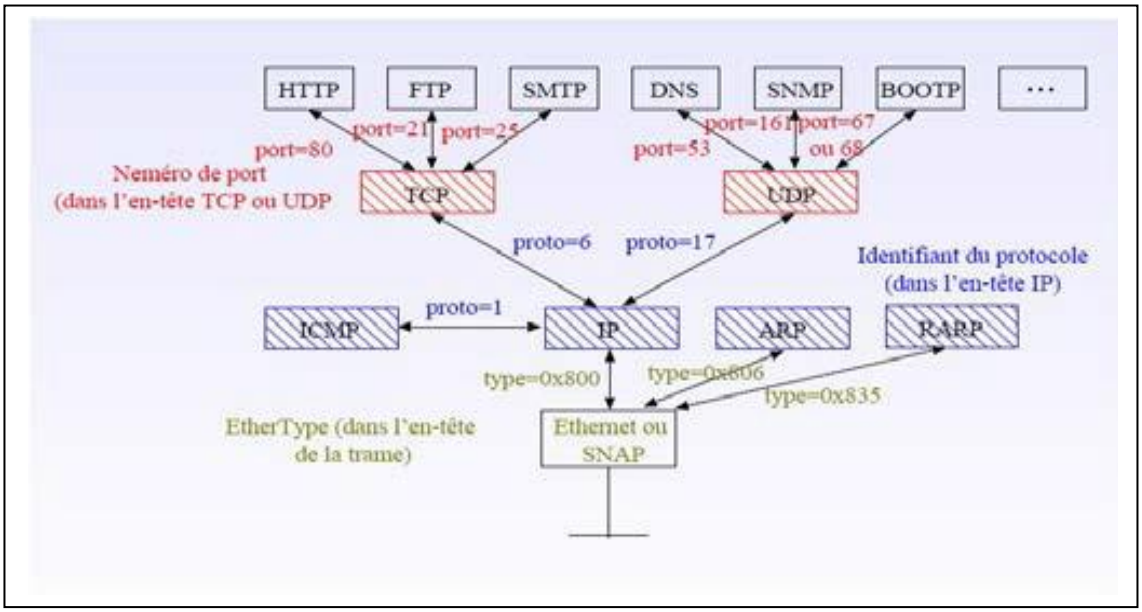
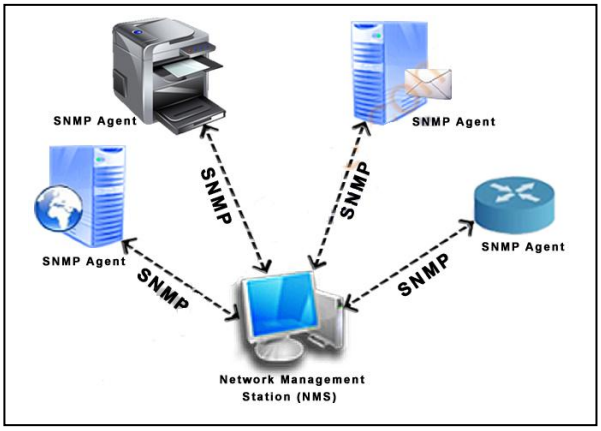


Figure : Les protocoles TCP/IP

Chapitre II : Les Services SNMP (Simple Network Management Protocol)

II.1. Introduction : Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication de la couche application, qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels ***<u>à distance</u>***. Il s'agit d'un protocole permettant de **collecter** et **d'organiser**, dans une base d'informations de gestion (**MIB**), des informations sur les périphériques gérés sur les réseaux IP *(Bp, température cpu, marche, arrêt …etc)* et de manipuler ces informations à distance pour gérer les applications et le comportement des périphériques. Les périphériques qui prennent généralement en charge SNMP incluent les modems, les routeurs, les commutateurs, les serveurs (physiques ou virtuels), les stations de travail, les imprimantes, etc.



II.2. Les versions du protocole SNMP

Trois versions significatives de SNMP ont été développées et déployées : SNMPv1, SNMPv2 et SNMPv3.

SNMPv1 (jusqu'à 100 Mbps): Cette version a été critiquée pour sa faible sécurité, en effet, l'authentification des clients est effectuée uniquement par une "chaîne de communauté" (un type de mot de passe) qui est transmis en clair.

SNMPv2 : Cette version a été jugée non praticable à cause de son système de sécurité trop complexe.

SNMPv2c : (jusqu'à 10 Gbps rapide) Cette version est acceptable puisque elle utilise un système de sécurisation relativement simple mais toujours en « clear text ».

SNMPv3 (10 Gbps toujours rapide) définit une version plus sécurisée, elle offre une authentification forte (hashing) et un chiffrement des données (data encryption) pour la confidentialité, et facilite également la configuration à distance des entités SNMP. Cette version se base sur le chiffrement AES (Advanced Encryption Standard) avec deux mots de passes ou clés sur 64 bits chacun partagés

entre l'agent et le manager : un pour l'authentification et un pour le chiffrement. Actuellement, SNMP en sa 3ème version est principalement utilisé pour la surveillance et la gestion de la performance.

II.3. Principe du SNMP

Le système SNMP est basé sur trois éléments principaux : superviseur « manager », des agents et une base de données MIB. Dans la terminologie SNMP, le terme « manager » est plus souvent employé que superviseur. Le Manager est le serveur qui permet à l'administrateur réseau d'exécuter des requêtes de gestion (get request). Les agents sont des entités qui se trouvent au niveau de chaque interface, connectant au réseau l'équipement géré et permettant de récupérer des informations sur différents objets. SNMP permet le dialogue entre le manager et les agents afin de recueillir les informations souhaitées et les stocker dans une base de données MIB bien organisée.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc fondée sur quatre principaux éléments :

- les équipements gérés (managed devices) sont des éléments du réseau (commutateurs, routeurs ou serveurs), contenant des « objets de gestion » (managed objects) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;
- les agents, c'est-à-dire les applications SNMP de gestion de réseau installées sur un périphérique, sont chargés de transmettre les données locales de gestion du périphérique au format SNMP vers le Manager ;
- les systèmes de gestion de réseau (network management systems notés NMS), c'est-à-dire les consoles à travers lesquelles les administrateurs peuvent réaliser des tâches d'administration à partir du Manager. Dans la pratique, pour qu'un serveur devienne « Manager », il doit disposer d'un programme (exemple MRTG (Multi Router Traffic Grapher), PRTG (Paessler Router Traffic Grapher)).
- La base d'informations MIB dans laquelle les données sont structurées et organisées par un identificateur OID (Object ID). Les messages envoyés par un manager SNMP sont de type : Get, Get next, Set, Response, Inform, sur des paquet UDP avec numéro de port 161 ; et Trap (Interruption ou Alertes): avec numéro de port 162.

Donc, SNMP utilise les ports UDP utilisateur suivants :

- 161 pour l'agent
- 162 pour le manager

Le protocole de base pour les communications entre le manager et l'agent est le suivant :

- Le manager peut envoyer des demandes depuis un port disponible à l'agent sur le port 161. L'agent répond ensuite à ce port source à la demande du manager.
- L'agent génère des notifications et les envoie à partir d'un port disponible au manager sur le port 162.

Le processus de configuration de SNMP est le suivant :

Après avoir activé les services SNMP sur l'ordinateur Manager, on doit suivre le processus suivant pour une bonne configuration et donc un bon fonctionnement du SNMP :

1. Récupérer les informations MIB à partir de la bibliothèque de chaque agent.
2. Gérez les utilisateurs SNMP qui peuvent accéder et donc superviser le réseau.
3. Configurez les destinataires des messages SNMP (ports de destination).
4. Activez l'agent dans la carte de contrôleur de la bibliothèque.

   L'agent doit maintenant répondre aux commandes « **get »** du manager.

5. Configurez les informations de service SNMP sur le manager.

Avantages du SNMP :

- L'avantage majeur dans le fait d'utiliser SNMP est qu'il est de conception **simple** ; il est donc aisé à implémenter sur un réseau, puisqu'il ne prend pas longtemps à configurer et qu'il est de petite taille. Le résultat flagrant de cette simplicité est une administration de réseau simple à implémenter et rapide.
- Un autre avantage de SNMP est qu'il est vraiment beaucoup **répandu** aujourd'hui. Presque tous les grands constructeurs de matériel hardware inter-réseaux, tels que les ponts ou les routeurs, conçoivent leurs produits de manière à ce qu'il supportent SNMP, rendant ce dernier très facile à implémenter.
- **L'expansion** est un autre avantage de SNMP. De par sa simplicité de conception, il est facile de mettre à jour le protocole pour qu'il réponde aux besoins des utilisateurs futurs.
- Enfin, SNMP est basé sur le protocole de transport UDP ce qui nécessite **moins de ressources et de connexions simultanées** qu'avec TCP.

Inconvénients du SNMP :

- Le premier défaut de SNMP est qu'il contient quelques gros trous de sécurité à travers lesquels des intrus peuvent accéder aux informations transitant sur le réseau. La solution à ce problème est apportée dans SNMPv3 qui implémente des mécanismes de sécurité en ce qui concerne le caractère privé des données, l'authentification et le contrôle d'accès.
- Puisque SNMP utilise le protocole UDP, il n'y a pas de reprise sur erreur, ni de contrôle de flux. La requête ou la réponse peut être égarée. Le Manager surveille donc son environnement en procédant à des interrogations régulières de ses agents, c'est ce que l'on appelle le Polling. SNMP est donc un protocole bavard. Cette surcharge de trafic n'est pas trop gênante sur un réseau local mais devient embarrassante via le réseau public.

II.4. La base d'information de gestion MIB

Une MIB (management information base, base d'information pour la gestion du réseau) est un ensemble d'informations structuré sur une entité réseau, par exemple un routeur, un commutateur ou un serveur. Ces informations peuvent être récupérées, ou parfois modifiées, par un protocole comme SNMP.

La structure de la MIB est hiérarchique : les informations sont regroupées en arbre. Chaque information a un Object IDentifier, une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, indiqué dans le document qui décrit la MIB.

Par exemple, 1.3.6.1.2.1.2.2.1.2 est l'object identifier ***ifDescr*** qui est la chaîne de caractères décrivant une interface réseau (Ethernet0 sur un routeur Cisco).

Une des MIB les plus connues est MIB-II, décrite dans le RFC 1213, et qui est mise en œuvre dans quasiment tous les équipements TCP/IP. Elle compte dix groupes, "system", "interfaces" (dont fait partie ifDescr, citée plus haut), "Address Translation", "IP", "ICMP", "TCP", "UDP", "EGP", "transmission" et "SNMP". Chaque nœud est associé d'un numéro d'identification appelé OID (voir la figure ci-dessous).

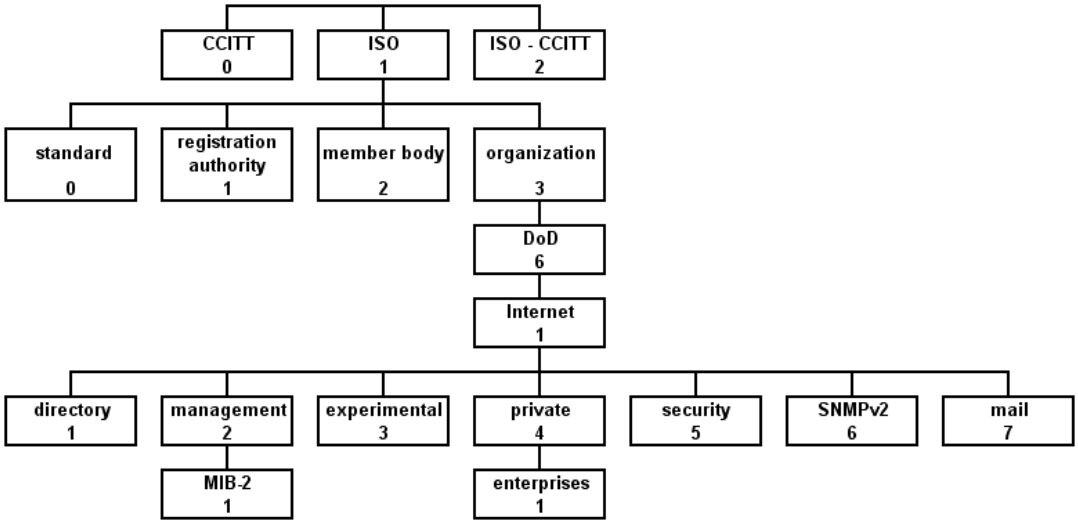


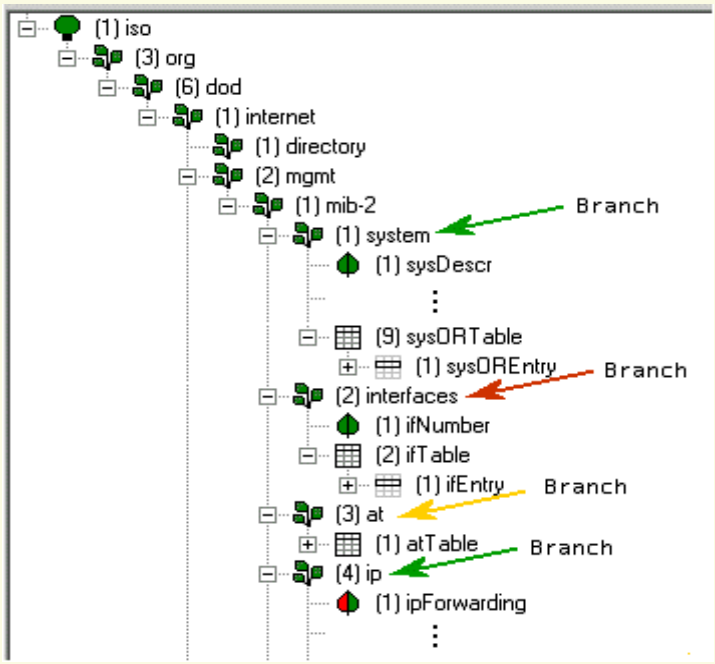
Figure : Architecture hiérarchisée d'une MIB

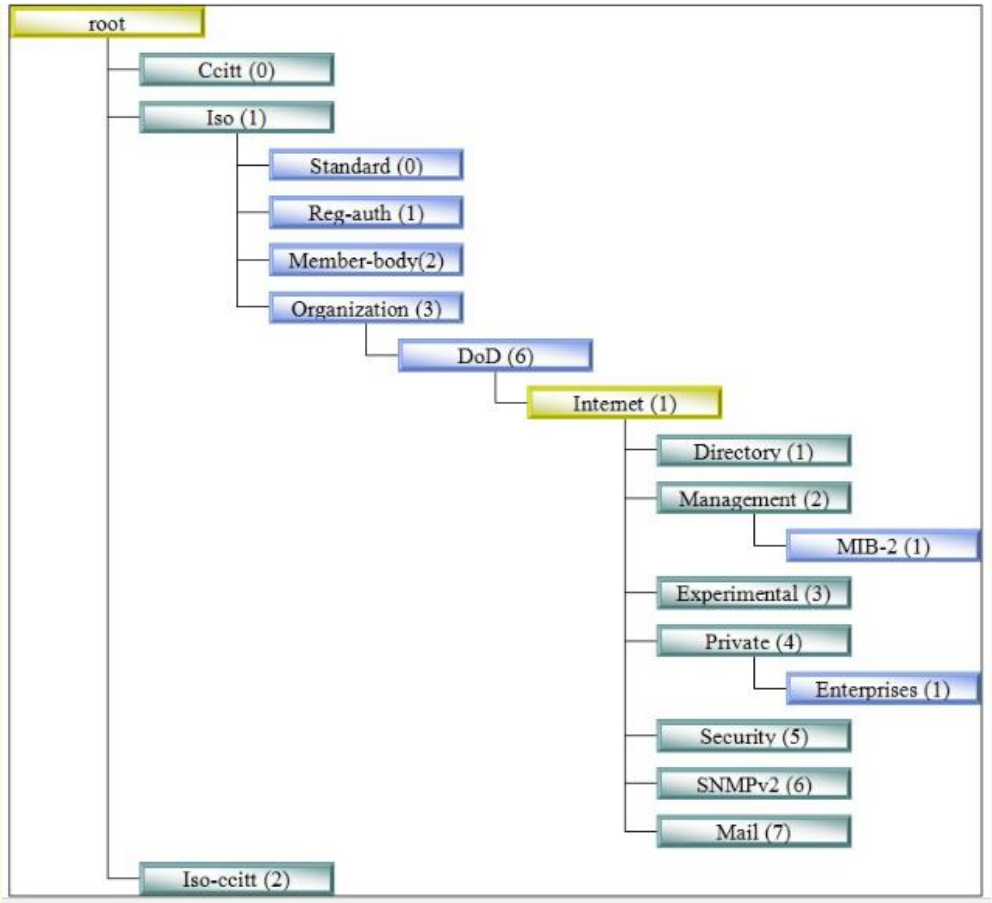
ASN.1 (Abstract Syntax Notation One) est un standard international spécifiant une notation destinée à décrire des structures de données dans le secteur des télécommunications et des réseaux informatiques. Les MIB sont décrites en utilisant ASN.1.

Une MIB se présente comme une base de données normalisée, qui permettra de lire et d'écrire sur les équipements distants, de façon également normalisée. Ce sera à l'agent lui-même de faire l'interface entre les informations récupérables sur la plateforme où il est installé et le Manager SNMP.

II.4.1. Structure d'une MIB

Elle est organisée hiérarchiquement, de la même façon que l'arborescence des domaines Internet DNS.





Non seulement la structure est normalisée, mais également les appellations des diverses rubriques. En réalité, chaque niveau de la hiérarchie est repéré par un index numérique.

Tout constructeur d'un matériel spécifique peut développer une MIB pour ce matériel, cette MIB devra prendre sa place dans l'arbre, sans piétiner celle des voisins, et c'est le rôle de l'IETF ou de l'IANA d'attribuer un point de branchement pour le matériel de ce constructeur.

Exemple : HP peut développer une MIB générique à tous ses matériels qui viendrait se greffer sur la branche ***private.enterprise***, puis des MIBs spécifiques à chaque matériel qui viendraient elles-mêmes se développer dans la MIB.

Sur l'arborescence en illustration, nous constatons que le sommet est représenté par un point originel, puisque chaque embranchement dispose d'un nom (iso, org, internet…) et aussi d'un numéro (1, 3, 6, 1…).

Voici un exemple du chemin qui mène à sysDescr soit :

- .iso.org.dod.internet.mgmt.mib-2.system.sysDescr (en mode texte) ;
- .1.3.6.1.2.1.1.1 (en mode numérique).

D’autres exemples :

Exemple : :

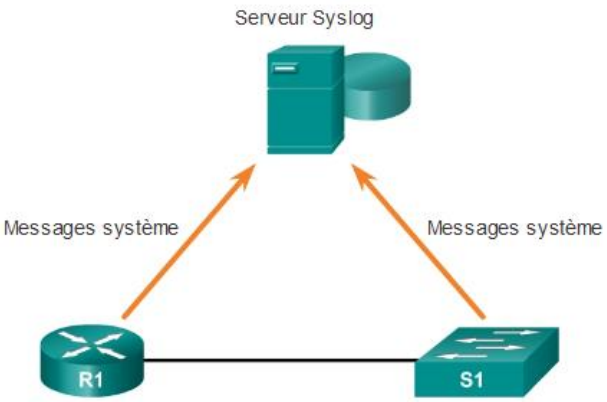
1.3.6.1.2.1.1.1.0 te retourne les caractéristiques d'une machine (materiellement parlant)

1.3.6.1.2.1.1.5.0 te retourne le nom de la machine

1.3.6.1.2.1.1.3.0 te retourne le temps

II.5. Le service Syslog :

Le protocole Syslog a été développé pour les systèmes UNIX dans les années 1980, mais a été documenté pour la première fois dans la RFC 3164 par l'IETF en 2001. Le protocole Syslog utilise le port UDP 514 pour envoyer des messages de notification d'événement sur des réseaux IP à des collecteurs de messages d'événement, comme le montre la figure ci-dessous.



L'intérêt de Syslog est donc de centraliser les journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau. Il existe aussi un logiciel appelé Syslog, qui est responsable de la prise en charge des fichiers de journalisation du système. Voir la figure ci-dessous qui montre un extrait d'un fichier de journalisation Syslog.

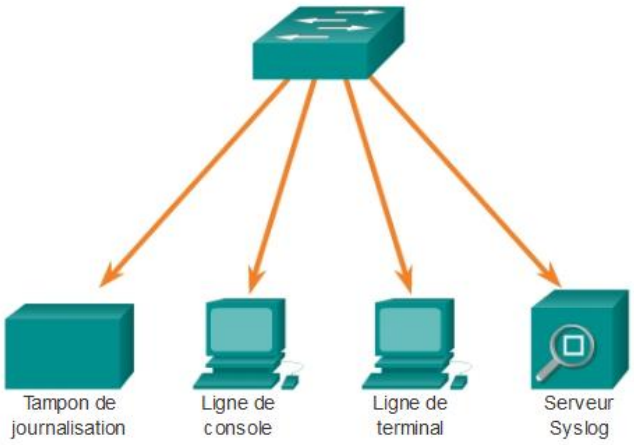
```
  GNU nano 2.0.2                                Fichier : syslog

Oct 30 18:02:41 debian5 syslogd 1.4.1#18: restart.
Oct 30 18:02:41 debian5 anacron[3116]: Job `cron.daily' terminated
Oct 30 18:02:41 debian5 anacron[3116]: Normal exit (1 job run)
Oct 30 18:06:16 debian5 dhclient: DHCPREQUEST on eth0 to 192.168.30.1 port 67
Oct 30 18:06:16 debian5 dhclient: DHCPACK from 192.168.30.1
Oct 30 18:06:16 debian5 NetworkManager: <information>^IDHCP daemon state is now 3 (renew) for interface eth0
Oct 30 18:06:16 debian5 dhclient: bound to 192.168.30.185 -- renewal in 279 seconds.
Oct 30 18:10:55 debian5 dhclient: DHCPREQUEST on eth0 to 192.168.30.1 port 67
Oct 30 18:10:55 debian5 dhclient: DHCPACK from 192.168.30.1
Oct 30 18:10:55 debian5 dhclient: bound to 192.168.30.185 -- renewal in 244 seconds.
Oct 30 18:10:55 debian5 NetworkManager: <information>^IDHCP daemon state is now 3 (renew) for interface eth0
Oct 30 18:14:59 debian5 dhclient: DHCPREQUEST on eth0 to 192.168.30.1 port 67
Oct 30 18:14:59 debian5 dhclient: DHCPACK from 192.168.30.1
Oct 30 18:14:59 debian5 dhclient: bound to 192.168.30.185 -- renewal in 295 seconds.
Oct 30 18:14:59 debian5 NetworkManager: <information>^IDHCP daemon state is now 3 (renew) for interface eth0
Oct 30 18:17:01 debian5 /USR/SBIN/CRON[3480]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct 30 18:19:54 debian5 dhclient: DHCPREQUEST on eth0 to 192.168.30.1 port 67
Oct 30 18:19:54 debian5 dhclient: DHCPACK from 192.168.30.1
Oct 30 18:19:54 debian5 dhclient: bound to 192.168.30.185 -- renewal in 248 seconds.
Oct 30 18:19:54 debian5 NetworkManager: <information>^IDHCP daemon state is now 3 (renew) for interface eth0
Oct 30 18:24:02 debian5 dhclient: DHCPREQUEST on eth0 to 192.168.30.1 port 67
Oct 30 18:24:02 debian5 dhclient: DHCPACK from 192.168.30.1
Oct 30 18:24:02 debian5 dhclient: bound to 192.168.30.185 -- renewal in 249 seconds.
Oct 30 18:24:02 debian5 NetworkManager: <information>^IDHCP daemon state is now 3 (renew) for interface eth0
Oct 30 18:28:11 debian5 dhclient: DHCPREQUEST on eth0 to 192.168.30.1 port 67
Oct 30 18:28:11 debian5 dhclient: DHCPACK from 192.168.30.1
```

De nombreux périphériques réseau prennent en charge le protocole Syslog, comme les routeurs, les commutateurs, les serveurs d'applications, les pare-feu et d'autres dispositifs réseau. Le protocole Syslog permet aux périphériques réseau d'envoyer leurs messages système sur le réseau aux serveurs Syslog.

Il existe divers packages logiciels de serveur Syslog pour Windows et UNIX. A travers c'est outils l'administrateur réseau peut spécifier que seuls certains types de messages sont envoyés à différentes destinations. Il est par exemple possible de configurer le périphérique de telle sorte qu'il transfère les messages système de débogage vers un serveur Syslog externe.

La figure ci-dessous illustre les destinations classiques des messages Syslog.



Il est possible de surveiller à distance les messages système en affichant les journaux sur un serveur Syslog ou en accédant au périphérique par le biais de Telnet, de SSH (Secure Shell) ou du port de console.

Les périphériques Cisco génèrent des messages Syslog à la suite des événements réseau. Chaque message Syslog contient un niveau de gravité et une capacité. Plus les numéros des niveaux sont petits, plus les alarmes Syslog sont critiques. La liste complète des niveaux Syslog est illustrée à la Figure suivante :

Gravité	Niveau de gravité	Explication
Urgence	Niveau 0	Système inutilisable
Alerte	Niveau 1	Action immédiate requise
Critique	Niveau 2	Condition critique
Erreur	Niveau 3	Condition d'erreur
Avertissement	Niveau 4	Condition d'avertissement
Notification	Niveau 5	Événement normal mais important
Informatif	Niveau 6	Message informatif
Débogage	Niveau 7	Message de débogage

Chaque niveau Syslog a sa propre signification :

- **Niveau d'avertissement - Niveau d'urgence** : ces messages sont des messages d'erreur relatifs aux dysfonctionnements logiciels ou matériels ; ces types de messages signifient que la fonctionnalité du périphérique est affectée.
- **Niveau de débogage** : ce niveau indique que c'est message de correction d'une certaine erreur.

- **Niveau de notification** : le niveau de notification existe à titre purement informatif, la fonctionnalité des périphériques n'étant pas affectée.

En plus de spécifier la gravité du problème, les messages Syslog contiennent également des informations de capacité.

Les capacités classiques des messages Syslog signalées sur les routeurs Cisco IOS sont les suivantes :

- IP
- Protocole OSPF
- Système d'exploitation SYS
- IPsec (IP Security)
- Adresse IP d'interface (IF)

Le paquet Syslog :

Les champs contenus dans un paquet Syslog du logiciel Cisco IOS sont expliqués sur la Figure suivante.

Champ	Explication
numéro d'ordre	Horodatage des messages de journal avec un numéro d'ordre uniquement si la commande de configuration globale `service sequence-numbers` est configurée.
horodatage	Date et heure du message ou de l'événement, visibles uniquement si la commande de configuration globale `service timestamps` est configurée.
établissement	Établissement auquel le message se réfère
gravité	Code à un seul chiffre de 0 à 7, représentant la gravité du message.
MOYEN MNÉMOTECHNIQUE	Chaîne de texte décrivant le message de façon unique.
description	Chaîne de texte contenant des informations détaillées sur l'événement signalé.

Les messages les plus courants sont les messages indiquant si la liaison est active ou non, ainsi que ceux qu'un périphérique produit lorsqu'il quitte le mode de configuration.

Il existe d'autres protocoles de surveillance tels que **NetFlow** dont le fonctionnement et légèrement différent du Syslog.

Chapitre III : Les services annuaires (DNS, ARP, DHCP) :

III.1. Domain Name System (DNS)

Le protocole et le système DNS permet de résoudre des noms en adresses IP. DNS est une sorte de service mondial de correspondance entre des noms et des adresses IP.

DNS utilise les **ports UDP/TCP 53** pour ses transactions. Les transferts de zones utilisent TCP alors que les requêtes habituelles utilisent UDP.

Le fichier « hosts » est un fichier utilisé par le système d'exploitation d'un ordinateur lors de l'accès à Internet. Son rôle est d'associer des noms d'hôtes à des adresses IP. Lors de l'accès à une ressource réseau par nom de domaine, ce fichier est consulté avant l'accès au serveur DNS et permet au système de connaître l'adresse IP associée au nom de domaine sans avoir recours à une requête DNS. Les modifications sont prises en compte directement. Il est présent dans la plupart des systèmes d'exploitation.

- Unix, Unix-like,POSIX dans /etc/hosts
- Microsoft Windows %SystemRoot%\system32\drivers\etc\hosts

III.1.1. Enregistrements DNS

La base de données d'une zone (un domaine) peut comporter certains types d'enregistrements DNS comme par exemple :

- **A** : qui fait correspondre un nom d'hôte à une adresse IPv4 ;
- **AAAA** : qui fait correspondre un nom d'hôte à une adresse IPv6 ;
- **CNAME** : qui permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original ;
- **MX** : qui définit les serveurs de courriel pour ce domaine ;
- …et bien plus

III.1.2. Les différents types de serveur DNS

On distingue quatre types de serveurs DNS à savoir : les serveurs locaux, les serveurs autoritaires, les serveurs racine et les serveurs résolveurs.

a. ***Les serveurs de noms locaux :*** ceux qui répondent aux clients, chaque zone a un serveur de noms local par défaut. Toutes les requêtes DNS en provenance de cette zone vont vers ce serveur de nom local.
b. ***Les serveurs faisant autorité :*** serveurs DNS qui connaissent le contenu des domaines TLD. Exemple : DZ.NIC est le serveur agréé par l'ICANN pour la gestion du ccTLD « .dz » relatif à l'Algérie. chaque hôte est enregistré auprès d'au moins deux serveurs d'autorité (le primaire et le secondaire), qui stockent son adresse IP et son nom. Un serveur de noms est dit d'autorité pour un hôte s'il est responsable de la correspondance nom/@IP pour cet hôte.
c. ***Les serveurs DNS de racine :*** ceux qui définissent les rôles. Il existe 13 serveurs de racine dans l'Internet. Chaque serveur DNS local connaît un serveur de noms racine qu'il peut interroger s'il ne connaît pas une correspondance de premier niveau (.dz, .com, ...). Un serveur de noms racine connaît au moins les serveurs de source autoritaires du premier niveau.
d. ***Les Résolveurs (ou serveurs récursifs) :*** ces serveurs DNS ne connaissent rien mais posent des questions (requêtes) aux serveurs faisant autorité et mémorise les réponses. Ces requêtes peuvent être soit :

- Requête récursive : la machine qui demande la résolution de nom contacte un serveur DNS et attend que ce dernier lui retourne la réponse, et si il en a besoin, le serveur demande à un autre serveur et ainsi de suite.
- Requête itérative : le serveur de noms contacté fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution (je ne connais pas ce nom mais demande à ce serveur).

Les fournisseurs d'accès à Internet mettent à disposition de leurs clients ces serveurs récursifs. Il existe des serveurs récursifs publics comme celui de Google Public DNS qui est un service de Google qui consiste à offrir des serveurs DNS récursifs aux utilisateurs d'Internet. Il a été annoncé le 9 décembre 2009. Ses adresses IPv4 et IPv6 sont : 8.8.8.8 et 8.8.4.4 et 2001:4860:4860::8888 et 2001:4860:4860::8844.

Références utiles pour DNS:

http://msaidallah.free.fr/cours/dns.pdf

https://nsrc.org/workshops/2004/ccTLD-Cameroun/jour1/Introduction-au-dns.pdf

https://cisco.goffinet.org/ccna/services-infrastructure/protocole-resolution-noms-dns/

III.2. Protocole ARP (Address Resolution Protocol)

L'Address Resolution Protocol (ARP, protocole de résolution d'adresse) est un protocole utilisé pour traduire une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse de protocole de couche de liaison (typiquement une adresse MAC). Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

Un ordinateur connecté à un réseau informatique souhaite émettre une trame ethernet à destination d'un autre ordinateur dont il connaît l'adresse IP et placé dans le même sous-réseau. Dans ce cas, cet ordinateur va placer son émission en attente et effectuer une requête ARP en broadcast de niveau 2. Cette requête est de type « quelle est l'adresse MAC correspondant à l'adresse IP @IP ? Répondez à monAdresseIP » comme l'illustre la figure ci-dessous :

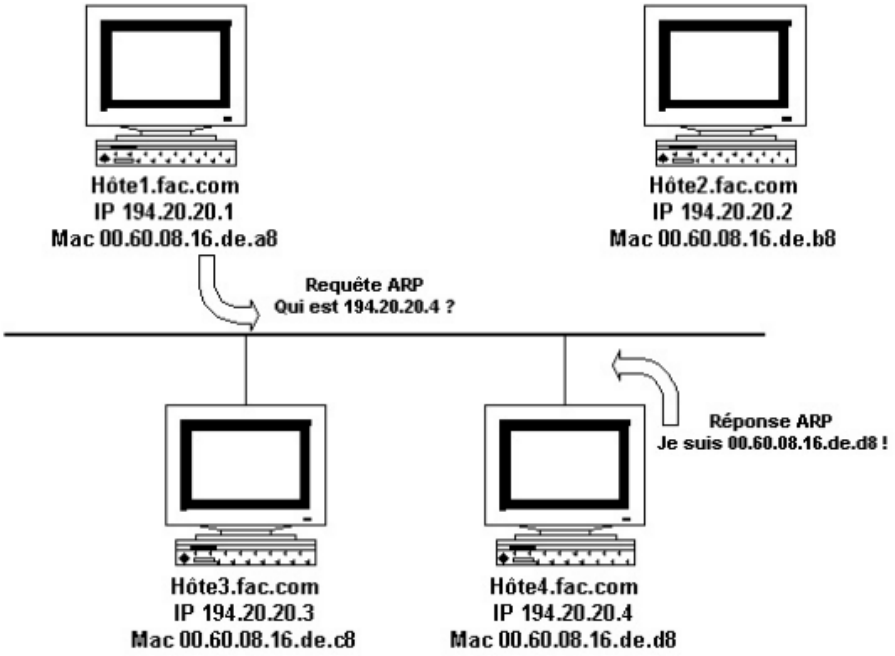


Figure : Requête ARP sur un réseau Ethernet

Puisqu'il s'agit d'un broadcast, tous les ordinateurs du segment vont recevoir la requête. En observant son contenu, ils pourront déterminer quelle est l'adresse IP sur laquelle porte la recherche. La machine qui possède cette adresse IP sera la seule à répondre en envoyant à la machine émettrice une réponse ARP du type « je suis adresseIP, mon adresse MAC est adresseMAC ». La machine réceptrice crée une entrée dans son cache ARP à partir des données contenues dans la requête ARP qu'il vient de recevoir.

La machine à l'origine de la requête ARP reçoit la réponse, met à jour son cache ARP et peut donc envoyer à l'ordinateur concerné le message qu'elle avait mis en attente.

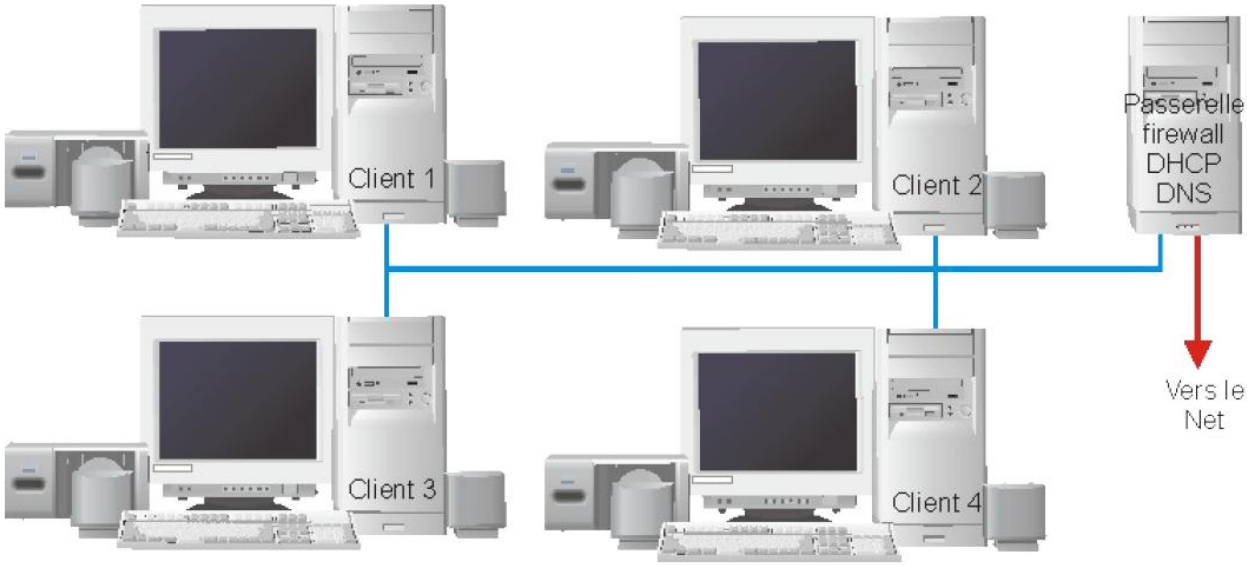
Il suffit donc d'un broadcast et d'un unicast pour créer une entrée dans le cache ARP de deux ordinateurs.

III.3. Dynamic Host Configuration Protocol (DHCP)

III.3.1. Introduction :

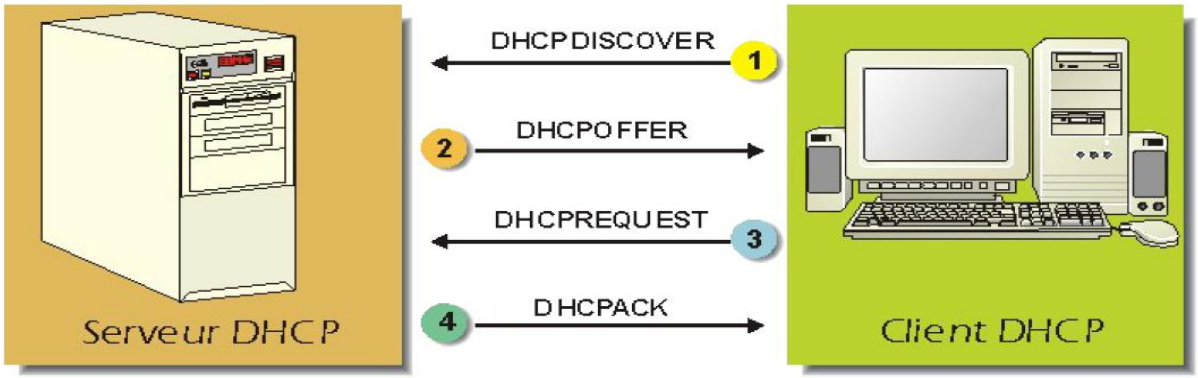
Le protocole DHCP (Dynamic Host Configuration Protocol) est un standard TCP/IP conçu pour simplifier la gestion de la configuration d'IP hôte. Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les

paramètres tels que (serveur de noms, l'adresse de passerelle par défaut, @ip du réseau), un serveur DHCP alloue à un client, un « bail » d'accès au réseau, pour une durée déterminée (durée du bail).



DHCP permet d'utiliser des serveurs pour affecter dynamiquement des adresses IP et d'autres paramètres de configuration correspondants pour les clients DHCP de votre réseau. Dans un réseau TCP/IP chaque ordinateur doit disposer d'un nom d'ordinateur et d'une adresse IP unique. L'adresse IP (avec son masque de sous-réseau associé) identifie l'ordinateur hôte et le sous-réseau auquel il est associé. Quand on déplace un ordinateur vers un autre sous-réseau, l'adresse IP doit alors être modifiée. DHCP permet d'affecter de manière dynamique une adresse IP à un client, à partir de la base de données des adresses IP, gérée par le serveur DHCP du réseau local. Le serveur DHCP doit disposer quant à lui d'une adresse IP fixe (non dynamique). Pour les réseaux TCP/IP, DHCP réduit la complexité et la quantité de travail de l'administrateur impliqué dans la reconfiguration des ordinateurs.

III.3.2. Principe de fonctionnement du DHCP : Le principe est celui illustré dans cette figure :



1. Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau. Il envoie donc une trame "DHCPDISCOVER", destinée à trouver un serveur DHCP. Cette trame est en "Broadcast", donc envoyée à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi sa "MAC Address".

IP du client src : 0.0.0.0
adresse MAC src : 00 80 C8 FC FE A7 (par exemple)
datagramme UDP envoyé : recherche DHCP
IP dest : 255.255.255.255 (diffusion)
MAC dest : FF FF FF FF FF FF (diffusion)
ID de transaction (par exemple 14321).

2. Le, ou les serveurs DHCP du réseau qui vont recevoir cette trame vont se sentir concernés et répondre par une trame Broadcast "DHCPOFFER" (de point de vue MAC c'est unicast). Cette trame contient une proposition de bail et la "MAC Address" du client, avec également l'adresse IP du serveur. Tous les DHCP répondent et le client normalement accepte la première réponse venue.

Datagramme UDP envoyé : proposition d'@IP et de bail et d'autres paramètres
IP : 255.255.255.255 (diffusion)
MAC : 00 80 C8 FC FE A7 (dirigée unicast)

3. Le client répond alors par un DHCPREQUEST à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.
Datagramme UDP envoyé : offre accepté
IP : 255.255.255.255 (diffusion)
MAC : FF FF FF FF FF FF (diffusé)
ID de transaction, par exemple 18336.

4. Le serveur DHCP concerné répond définitivement par un DHCPACK qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

Datagramme UDP envoyé : confirmation

IP : 255.255.255.255 (diffusée)

MAC : 00 80 C8 FC FE A7 (dirigée)

ID transaction : 18336

III.3.3. Avantages de DHCP dans l'administration d'un réseau

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.
- Facilite la configuration des machines portables sur des réseaux différents.
- Economie d'adresse : ce protocole est presque toujours utilisé par les fournisseurs d'accès Internet qui disposent d'un nombre d'adresses limité. Ainsi grâce à DHCP, seules les machines connectées en ligne ont une adresse IP. En effet, imaginons un fournisseur d'accès qui a plus de 1000 clients. Il lui faudrait 5 réseaux de classe C, s'il voulait donner à chaque client une adresse IP particulière. S'il se dit que chaque client utilise en moyenne un temps de connexion de 10 mn par jour, il peut s'en sortir avec une seule classe C, en attribuant, ce que l'on pourrait appeler des "jetons d'accès" en fonction des besoins des clients.

III.3.4. Renouvellement de bail IP

a) Lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST. Si la tentative se solde par un échec, le client continue à utiliser la même adresse IP s'il lui reste du temps sur son bail. Les clients DHCP d'un serveur DHCP tentent de renouveler leur bail lorsqu'ils ont atteint 50% de sa durée par un DHCPREQUEST. Si le serveur DHCP est disponible il envoie un DHCPACK avec la nouvelle durée et éventuellement les mises à jour des paramètres de configuration.

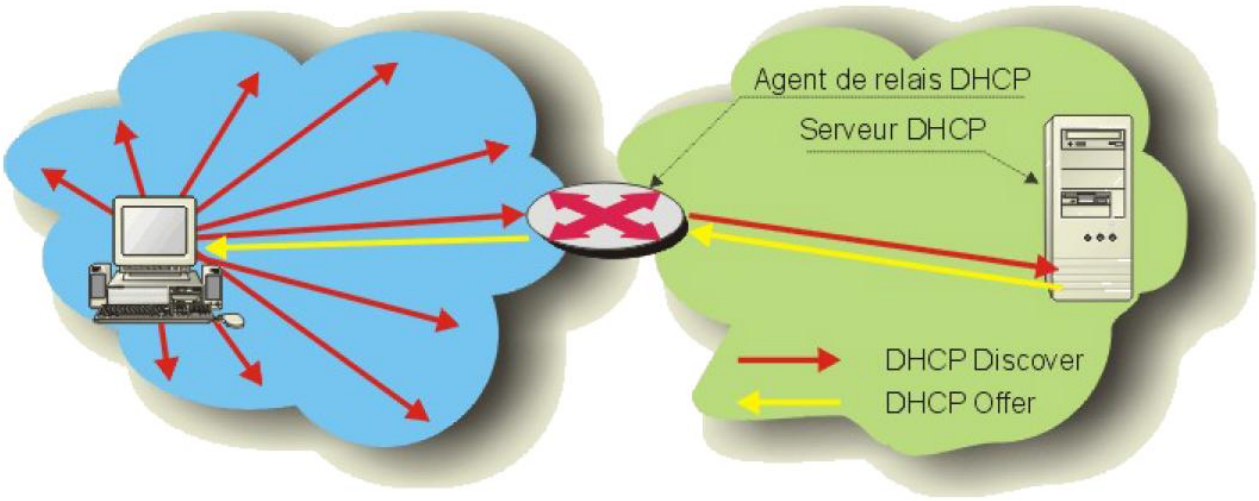
b) Si à 50% de la durée le bail n'a pu être renouvelé, le client tente de contacter l'ensemble des serveurs DHCP (diffusion) lorsqu'il atteint 87,5% de son bail, avec un DHCPREQUEST, les serveurs répondent soit par DHCPACK soit par DHCPNACK (adresse inutilisable).

c) Lorsque le bail expire ou qu'un message DHCPNACK est reçu le client doit cesser d'utiliser l'adresse IP et demande un nouveau bail (retour à l'étape 1 du processus de souscription).

Lorsque le bail expire et que le client n'obtient pas d'autre adresse la communication TCP/IP (Internet) s'interrompt.

III.3.5. Relais DHCP

Lorsque le serveur DHCP et son client sont sur des réseaux disjoints distants de plusieurs routeurs. La diffusion de la recherche DHCP aux autres réseaux s'effectue par les routeurs.



Ces routeurs joueront le rôle de relais DHCP. Le relais(le routeur) écoute les diffusions envoyées par les clients, lorsqu'un datagramme est reçu il est retransmis vers le serveur DHCP du réseau voisin et lorsqu'il reçoit des datagrammes à partir d'un serveur il diffuse sur le réseau du client DHCP.

III.4 Le protocol LDAP (Lightweight Directory Access Protocol)

III.4.1. Les services d'annuaires

Un service d'annuaire peut être associé à un système de stockage de données permettant de rendre accessible un ensemble d'informations à tous les utilisateurs de ce système.

Exemple d'annuaire: serveur DNS, annuaire téléphonique, ...

Avec l'informatique, il est devenu intéressant de numériser ces annuaires et de mettre en place des systèmes centralisés qui permettent à plusieurs utilisateurs d'obtenir des informations d'une même source. Ainsi, au sein d'une entreprise, il est possible de partager des informations et de les rendre accessibles à tous les collaborateurs.

Sur un système informatique, les données ne sont pas organisées de manière relationnelle comme sur les SGBD (Système de Gestion de Base de Données) classiques (MySQL, PgSQL, SQLServer, ...) mais de manière hiérarchique. La différence réside dans quelques points :

- La consultation des données est plus rapide pour l'annuaire par rapport aux SGBD classiques
- La duplication des données est facilitée

- Le stockage des données peut être réalisé dans un plus faible espace.

Les avantages des services d'annuaire sont leur rapidité pour accéder aux informations, les mécanismes de sécurité pouvant être mis en œuvre, la centralisation des informations et les possibilités de redondance de l'information.

III.4.1. Le service LDAP

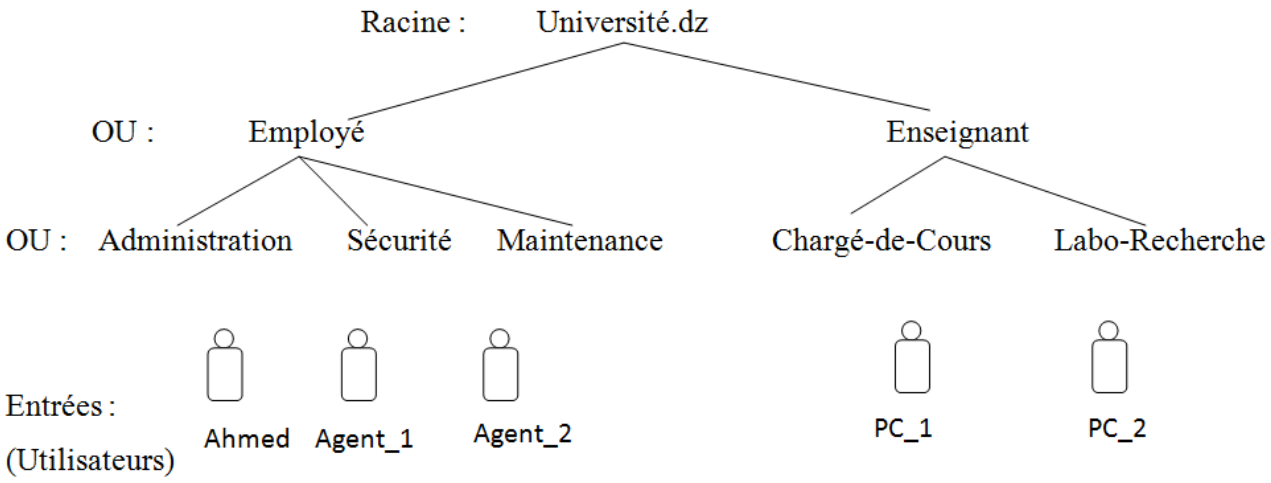
Un annuaire est un ensemble d'informations sur différents objets structuré sous forme arborescente. Un service d'annuaire est un protocole qui assure l'exploitation (modifier, gérer, interroger, …) cet annuaire.

Le service LDAP est à l'origine un protocole permettant l'accès aux annuaires informatiques. Il repose sur les protocoles TCP/IP (contrairement à la version classique X.500 qui repose sur le modèle OSI). Il a cependant évolué pour devenir une norme pour les systèmes d'annuaires. C'est un protocole de la couche application qui utilise le port 389.

LDAP est structuré sous une forme hiérarchique ***(arborescente)*** dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.

Le nommage des objets constituant l'arbre (racine, branches, feuilles) ressemble à celui du DNS pour les éléments de base de l'annuaire (racine et premières branches, domain components ou dc=…). Les branches plus profondes de l'annuaire peuvent représenter des unités d'organisation ou des groupes (organizational units ou ou=…), des personnes (common name ou cn=… voire user identifier uid=…). L'assemblage de tous les composants (du plus précis au plus général) d'un nom forme son distinguished name 'dn', l'exemple suivant en présente un :

cn=Agent_1, ou=Sécurité, ou=Employé, dc=Université, dc=dz



Chaque entrée a aussi un identificateur ID qui est unique sur toute la structure. Contrairement au dn qui peut changer.
La dernière version en date du protocole est LDAPv3. Cette version est définie par l'IETF.
Le LDAP permet principalement de gérer les annuaires en réseau et de normaliser les opérations d'accès et de recherche dans les données. Pour cela, LDAP définit :

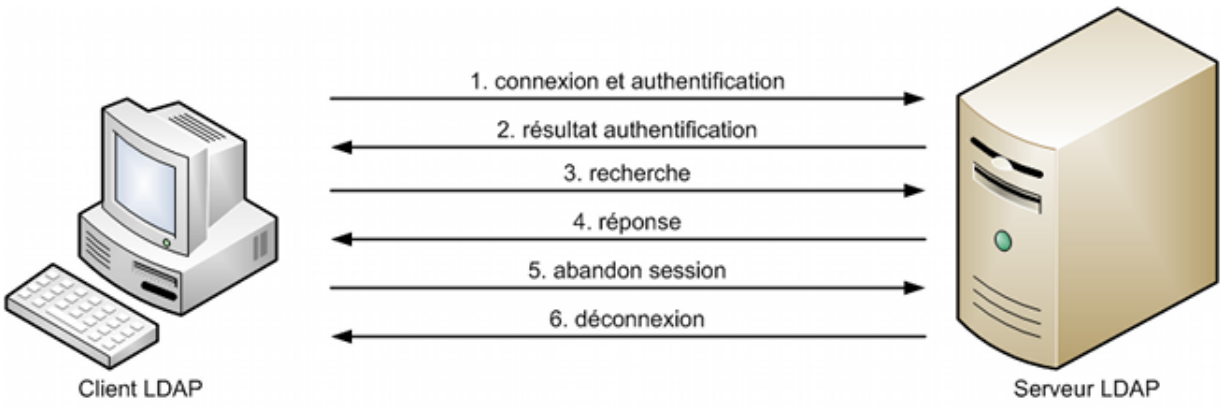
- un modèle d'information: pour définir le type de données de l'annuaire
- un modèle de nommage: pour indiquer comment les données sont organisées
- un modèle fonctionnel: pour indiquer comment accéder aux données
- un modèle de sécurité: pour indiquer comment protéger l'accès aux données
- un modèle de réplication : pour indiquer comment répartir les données entre serveurs

En plus de ces modèles, LDAP met en jeu un protocole d'accès pour permettre la communication entre clients recherchant l'information et serveurs contenant l'information.

III.4.2. Le modèle client-serveur

Pour son fonctionnement, LDAP met en place 2 méthodes de communication pour 2 fonctionnalités différentes :

- Une communication de type client/serveur pour permettre au client d'accéder aux informations contenues sur le serveur.
- Une communication de type serveur/serveur pour permettre au serveur de dupliquer ou synchroniser ses informations sur d'autres serveurs.



Exemple de communication client/serveur

Les échanges avec le protocole LDAP se font au format ASCII comme pour HTTP ou SMTP.

III.4.3. Le modèle LDAP

LDAP permet de gérer des données. Ces données utilisent un modèle particulier pour être stockées. Dans ce modèle, l'élément de base est appelé "Entry" (entrée).

Une entrée (entry) est un élément de base de l'annuaire. Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, ...). Une entrée est constituée de plusieurs objets. Un objet est constitué d'un ensemble de paires clés/valeurs appelées attributs permettant de définir de façon unique les caractéristiques de l'objet à stocker. Par analogie avec la terminologie objet on parle ainsi de classe d'objet pour désigner la structure d'un objet, c'est-à-dire l'ensemble des attributs qu'il doit comporter. De cette façon un objet est une "instanciation" de la classe d'objet, c'est-à-dire un ensemble d'attributs avec des valeurs particulières. Voici un exemple d'entrée de l'annuaire :

Client	
Type d'attribut	Valeur d'attribut
cn:	Ziggy NIGHT
uid	Znight
telnumber	0388123456
mail	Ziggy.night@gmail.co
solde	1000000

Exemple d'entrée

Sur l'exemple ci-dessus, on a une entrée de type "Client" qui contient plusieurs arguments avec les différentes informations sur le client.

Un attribut est caractérisé par:

- un nom unique
- un format et une limite de taille
- une syntaxe (la façon selon laquelle l'attribut doit être renseigné)
- un « Object Identifier » (IOD) qui permet de l'identifier de façon unique

Il s'agit d'utiliser une série de paires clé/valeur permettant de repérer une entrée de manière unique. Voici une série de clés généralement utilisées :

- uid (userid), il s'agit d'un identifiant unique obligatoire
- cn (common name), il s'agit du nom de la personne
- o (organization), il s'agit de l'entreprise de la personne
- mail, il s'agit de l'adresse de courrier électronique de la personne
- ...

Chapitre IV : Gestion des utilisateurs et service NFS

IV.1. introduction :

Network File System (ou NFS), pour système de fichiers en réseau, est à l'origine un protocole développé par Sun Microsystems en 1985 qui permet aux hôtes distants de monter des systèmes de fichiers sur un réseau et d'interagir avec ces systèmes de fichiers comme si ceux-ci sont montés localement. Autrement dit, un serveur NFS permet l'utilisation d'un répertoire ou de tout le système de fichiers d'un ordinateur distant de manière totalement transparente, comme s'il s'agissait d'un disque dur connecté directement à votre ordinateur. Ceci permet aux administrateurs système de consolider leurs ressources sur des serveurs centralisés sur le réseau. NFS fait partie de la couche application du modèle OSI et utilise le protocole RPC (Remote Procedure Call).

Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Mais il y a des versions pour Windows, par exemple : SMB Server Message Block. NFS peut fonctionner avec IPv4 et IPv6 sur la plupart des systèmes.

IV.2. Principes de NFS :

- Le serveur NFS exporte tout ou une partie de l'arborescence des fichiers.
- Il ne s'agit pas de transfert de fichier comme FTP mais un accès à distance avec une gestion totalement transparente des fichiers (modifier, supprimer, copier…).
- Il y'a des droits d'accès, des restrictions et des options sur les répertoires exportés.
- Le client s'il est autorisé peut monter tout ou une partie de l'arborescence exportée par le serveur.
- Un serveur NFS ne garde aucun historique des requêtes concernant les fichiers.

IV.3. Le programme portmap (RPC program number mapper) :

NFS offre des services basés sur RPC. Il a donc besoin de portmap pour lui dire sur quel port il écoute. Contrairement aux well-known services, les numéros de port RPC peuvent changer à chaque

redémarrage. Donc quand un client veut utiliser un service RPC, il demande d'abord au portmapper sur quel port va écouter. Portmap est un serveur qui fait la conversion entre les numéros de programmes RPC et les numéros de port des protocoles Internet. Il faut donc installer et démarrer portmap avant de lancer le serveur NFS.

Une fois le serveur NFS est installé, il faut le configurer. Egalement sur la machine distante il faut créer et configurer le client NFS pour qu'il puisse monter les fichiers à partir du serveur.

IV.4. les versions de NFS

Les versions 1 et 2 sont non sécurisées, prévues pour fonctionner sur UDP. La version 3 est étendue pour prendre en charge TCP.

Dans ces versions, la gestion de la sécurité reste élémentaire et souffre d'importantes lacunes.

La version 4 du protocole marque une rupture totale avec les versions précédentes. NFSv4 intègre :

- Une gestion totale de la sécurité : Chiffrement des communications possible (kerberos 5p par exemple).
- La gestion de la reprise sur incident est intégrée du côté client et du côté serveur.
- Compatibilité : NFSv4 peut être utilisé sous Unix et sous MS-Windows.
- Utilise TCP comme un protocole de transport fiable.

IV.5. Les applications du NFS :

Les applications du NFS sont multiples :

- travail collaboratif sur des mêmes documents
- centralisation de documents sur un serveur de fichiers
- stockages des sauvegardes d'un ordinateur sur un autre ordinateur du réseau
- installation des nouveaux ordinateurs à partir d'un serveur local
- etc..

Références :

Chapitre V : Service de messagerie SMTP

V.1. Introduction :

Simple Mail Transfer Protocol (SMTP, littéralement « protocole simple de transfert de courrier ») est un protocole de communication utilisé pour transférer le courrier électronique (appelé aussi courriel) vers les serveurs de messagerie électronique.

SMTP est un protocole assez simple (comme son nom l'indique). On commence par spécifier l'expéditeur du message, puis le ou les destinataires d'un message, puis, en général après avoir vérifié leur existence, le corps du message est transféré.

SMTP ne permet pas de récupérer à distance des courriels arrivés dans une boîte aux lettres sur un serveur. Les standards Post Office Protocol (POP) et IMAP ont été créés dans ce but.

V.2. Principes de base de la messagerie électronique :

Le service SMTP est constitué par plusieurs agents, chacun assurant une fonction spécifique.

- MUA : Mail User Agent, c'est le client de messagerie utilisé pour écrire le mail et le recevoir (Outlook, Thunderbird, Hotmail, Gmail, ...) autrement dit c'est l'application de rédaction d'un courriel (couche application) par laquelle on accède à la messagerie électronique par l'intermédiaire d'un navigateur web.
- MSA : Mail Submission Agent, a pour rôle de transmettre le mail après authentification de l'utilisateur et vérification de l'acheminabilité du courrier. Est un logiciel intermédiaire entre le client de messagerie et le serveur de messagerie MTA (comme le bureau de poste, exemple : serveur Gmail ou autre).
- MTA : Mail Transfert Agent, c'est l'agent qui va transférer votre mail vers le MTA de votre destinataire, après exécution d'un certain nombre de logiciels, par exemple un antivirus pour éviter de propager des mails contenant des virus ou des filtres à spam pour essayer d'éliminer des courriers indésirables.
- MDA : Mail Delivery Agent, c'est l'agent chargé de délivrer le mail à votre destinataire. C'est la boîte aux lettres, qui va stocker le mail jusqu'à ce que l'utilisateur utilise un logiciel de MUA pour pouvoir le lire.

Quand vous écrivez un mail à une personne dont l'adresse appartient à un autre domaine que le votre, il passe par un second MTA, comme l'illustre la figure ci-dessous :

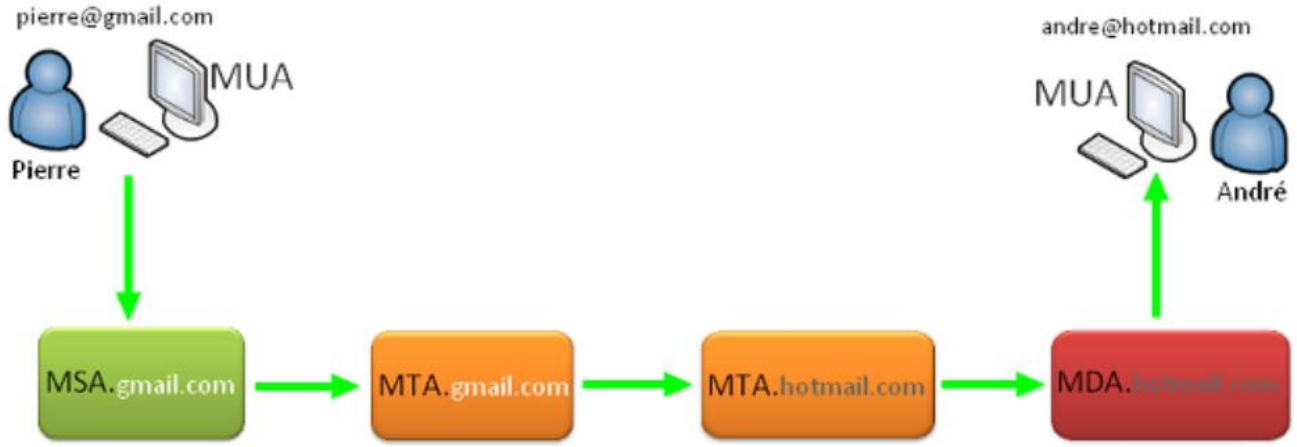


Figure : Modèle du protocole SMTP

Lorsqu'il s'agit d'un mail interne à un même domaine, il est directement pris en charge par le MDA sans passer par le second MTA.

Du MUA au dernier MTA impliqué dans le processus de transmission (émission et réception), c'est le protocole SMTP qui est utilisé. Entre le MDA et le MUA de réception, c'est un autre protocole de réception qui sera utilisé : POP3 ou IMAP4.

Les serveurs MDA sont bien entendus protégés par des Login, mots de passes, pour garder de la confidentialité entre utilisateurs.

V.3. Protocole SMTP :

SMTP utilise TCP comme protocole de transport de données. Il définit la manière de communiquer entre deux MTA en utilisant une connexion TCP (fiable) avec un numéro de port 25. Il utilise un alphabet ASCII 7 bits (en TCP : transmission de 8 bits avec le bit de poids fort fixé à 0).

Exemple :

Il est possible de tester un serveur SMTP en utilisant la commande **telnet** sur le **port 25/TCP** d'un serveur distant par l'instruction : ***telnet smtp.wanadoo.fr 25***

Le MTA émetteur lance un certain nombre de commandes, et reçoit des codes de retour comme par exemples : 250 : Action de messagerie effectuée, succès ; 251 : Utilisateur non local ; 450 : Action

non effectuée : boîte aux lettres non disponible, 220 : Service disponible, 221 : Canal de transmission en cours de fermeture…etc.

Une fois la connexion au serveur effectuée, une vérification s'impose pour savoir si le client demandeur parle bien au serveur demandé (une confirmation). Les 2 commandes utilisées à l'établissement et à la fermeture de la connexion sont : EHLO et QUIT.

La commande EHLO permet à la machine source de s'identifier auprès du serveur SMTP, exemple : EHLO gmail.com.

Il existe trois étapes pour les transactions de messagerie SMTP. La transaction est lancée avec une commande MAIL qui donne l'identification de l'expéditeur. Une série d'une ou plusieurs commandes RCPT successives, donnant les informations du récepteur. Ensuite, une commande DATA donne les données du courrier. Et enfin, l'indicateur de fin de données de courrier confirme la transaction.

La première étape de la procédure est la commande MAIL. Le « chemin inverse » contient la boîte aux lettres source:

MAIL <SP> FROM: <chemin inverse> <CRLF>

La commande MAIL indique au récepteur SMTP qu'une nouvelle transaction de messagerie est en cours de démarrage et de réinitialiser toutes ses tables d'état et tampons, y compris les destinataires ou les données de messagerie. Il donne le chemin inverse qui peut être utilisé pour signaler des erreurs. S'il est accepté, le récepteur SMTP renvoie une réponse « 250 OK ». La commande MAIL est suivie de la chaîne "FROM:" et d'une adresse de retour (la chaîne < > représente une adresse vide), exemple :

MAIL FROM : Omar@gmail.com

250 OK

La deuxième étape de la procédure est la commande RCPT:

RCPT <SP> TO: <forward-path> <CRLF>

Cette commande donne le chemin identifiant un destinataire. S'il est accepté, le récepteur-SMTP renvoie une réponse « 250 OK » et stocke le chemin identifié. Si le destinataire est inconnu, le

récepteur SMTP renvoie une réponse « 550 Failure ». Cette deuxième étape de la procédure peut être répétée un nombre illimité de fois.

La troisième étape de la procédure est la commande DATA:

DATA <CRLF>

S'il est accepté, le récepteur SMTP renvoie une réponse « 354» et considère toutes les lignes suivantes comme étant le texte du message. Lorsque la fin du texte est reçue et stockée, le récepteur SMTP envoie une réponse « 250 OK ».

Donc une transaction SMTP se déroule en 3 étapes.

- La première donne l'identificateur de la transaction.
- La deuxième donne les destinataires.
- La troisième donne le contenu message.

V.4. Format des messages SMTP :

Le format des messages/courriers est constitué de deux parties principales :

En-tête	Corps de message

- ***En-tête :*** utilisé par le MTA pour l'acheminement du courrier. Il est de la forme « Nom: valeur » et il s'agit essentiellement de :

• Date : date du message.

• From : indique l'expéditeur.

• To : indique le/les destinataire(s).

• Cc : indique le/les destinataire(s) en copie.

• Bcc : indique les destinataires en copie cachée.

• Subject : sujet du message ou (Objet)

Exemple de transaction SMTP avec un serveur de messagerie:

z03:~# telnet a.mx.mail.yahoo.com 25
220 mta604.mail.mud.yahoo.com ESMTP YSmtp service ready
helo toto.com
250 mta604.mail.mud.yahoo.com
mail from: <toto@toto.com>
250 sender <totot@toto.com> ok
rcpt to: <xxxxxx@yahoo.com>
250 recipient <xxxxxx@yahoo.com> ok
data
354 go ahead
Subject: Test
Test
250 ok dirdel
quit
221 mta604.mail.mud.yahoo.com

- ***Corps de message :***

Le corps c'est le contenu du message envoyé au destinataire. Il est défini par le type de codage : MIME (Multipurpose Internet Mail Extensions) qui permet de coder des documents multimédia : textes, images, sons, tableurs. Ainsi de transmettre des corps de message comportant plusieurs parties (message avec plusieurs attachements).

V.5. Le protocole POP3 :

POP3 signifie Post Office Protocol version 3. Le service POP3 utilise TCP sur le **port 110** d'un serveur.

Le protocole POP3 a un objectif précis : permettre à l'utilisateur de relever son courriel depuis un hôte qui ne contient pas sa boîte aux lettres. En d'autres termes, POP3 établie un dialogue entre le logiciel de messagerie (MUA) et la boîte aux lettres de l'utilisateur sur le serveur MTA.

POP a l'avantage d'être simple et efficace et surtout, il est supporté par tous les clients de messagerie, de ce fait il ne propose que des fonctionnalités basiques:

- Délimiter chaque message de la boite aux lettres,
- Compter les messages disponibles,
- Calculer la taille des messages,
- Supprimer un message,

- Extraire chaque message de la boite aux lettres.

Ces fonctionnalités sont amplement suffisantes pour répondre aux besoins de la plupart des utilisateurs.

Tout comme HTTP et SMTP, POP est un protocole de type client/serveur.

Avantages : Le service POP3 est très simple mais propose toutes les fonctionnalités nécessaires pour la gestion d'un compte mail. Ainsi, de part son efficacité, POP3 reste l'un des protocoles les plus utilisés actuellement pour récupérer ses mails.

Inconvénient : POP3 présente quelques points faibles notamment le fait que le mot de passe circule en clair sur le réseau lors de l'établissement de la connexion avec le serveur. Ainsi, une personne malhonnête équipée d'un sniffer peut le récupérer et l'utiliser à mauvais escient.

V.6. Le protocole IMAP4 :

Le protocole IMAP (Internet Message Access Protocol) : la version actuellement utilisée est la 4. Le service IMAP utilise le protocole TCP et écoute sur le port 143 d'un serveur SMTP (ou TCP/993 pour IMAP sur SSL (Secure Socket Layer) (imaps) la version sécurisée). Tout comme POP3, IMAP est un protocole de récupération de mails. IMAP4 se pose donc comme une alternative à POP3. Non seulement IMAP propose plus de services que POP3, mais il est aussi plus évolués. Une des principales nouveautés est la possibilité de pouvoir lire uniquement les objets des messages (sans le corps). Ainsi on peut par exemple effacer des messages sans les avoir lus.

Contrairement au protocole POP3 où tous les mails sont rapatriés du serveur vers le logiciel de messagerie du client (MUA), avec IMAP4, les mails restent stockés dans des dossiers sur le serveur. Ceci permet de proposer de nombreuses fonctionnalités très pratiques, telles que :

- créer des dossiers sur le serveur,
- effacer, déplacer des messages sans les lire, éventuellement avec des règles de tri automatique,
- Transférer en local certains messages et pas d'autres, en faisant une copie ou un déplacement,
- lire des messages en les laissant sur le serveur,
- marquer des messages sur le serveur,
- recopier sur le serveur des messages qui sont en local.

Avantages de IMAP par rapport au POP :

Etant donné les fonctionnalités implémentées dans IMAP, celui-ci est donc plus puissant que POP. Voici les points forts par rapport à POP :

- permet de gérer plusieurs accès simultanés
- permet de gérer plusieurs boîtes aux lettres en même temps
- permet de trier le courrier selon plus de critères
- protection contre les virus

Néanmoins, IMAP n'est pas aussi répandu que POP, peut-être parce que certains logiciels de messagerie (MUA) ne l'exploitent pas à 100 %. Outllook fait parti des ces MUA qui n'utilisent pas 100% des fonctionnalités implémentées dans IMAP. Ainsi, si on limite l'utilisation d'IMAP aux fonctionnalités de POP, autant utiliser ce dernier. De plus, les serveurs IMAP sont plus complexes à installer et à maintenir que les serveurs POP. Les Fournisseurs d'Accès à Internet ne proposent donc le plus souvent que le protocole POP à leurs abonnés.

Quelques exemples de serveurs IMAP : UW Imap, Courier IMAP, Cyrus IMAP Server, Microsoft Exchange Server, Dovecot,…etc.

V.7. Adresses de courriel :

L'adresse globale d'un courriel est définie par les standards RFC 5321 et RFC5322.

Une adresse se compose en deux parties :

- le nom de boîte à lettre
- le nom de domaine DNS

exemple: Ahmed.tlc@gmail.com

La taille du nom de boîte à lettre ne doit pas dépasser ***64 octets*** ;

Le système de nom de domaines (DNS) permet de déterminer le serveur de courrier avec un enregistrement de type : MX (*Mail eXchanger).*

Un enregistrement MX est un type d'enregistrements du DNS qui associe un nom de domaine à un serveur de messagerie électronique MTA associé à son numéro de préférence (priorité).

Ces enregistrements permettent de déterminer vers quel serveur un courrier électronique doit être acheminé lorsque le protocole SMTP est utilisé. Autrement dit, les enregistrements MX permettent

d'associer la partie à droite de l'arobase (@) aux adresses IP des serveurs qui servent de boîtes aux lettres.

Le serveur d'envoi MTA fait une requête au serveur DNS pour obtenir la liste des enregistrements MX associés au domaine de destination demandé, puis il tente de contacter le serveur dont la priorité est la plus forte (ce qui correspond au numéro de préférence le plus petit), et s'il n'y arrive pas, il contacte le second, et ainsi de suite.

Remarque : Le serveur d'envoi détermine de manière autonome la durée d'attente maximum à partir de laquelle le serveur MX de priorité forte sera considéré comme indisponible provoquant ainsi la sollicitation du prochain MX de priorité suivante.

Exemple d'un enregistrement MX pour un domaine fictif ***example.org*** :

```
example.org.    MX    50 secondaire.example.org.
                MX    10 principal.example.org.
```

Pour envoyer un courriel à un destinataire du domaine example.org, le serveur d'envoi devra d'abord essayer de le livrer au serveur SMTP (MTA) de la machine ***principal.example.org***, puis s'il n'arrive pas à la contacter, à celui de la machine ***secondaire.example.org***.

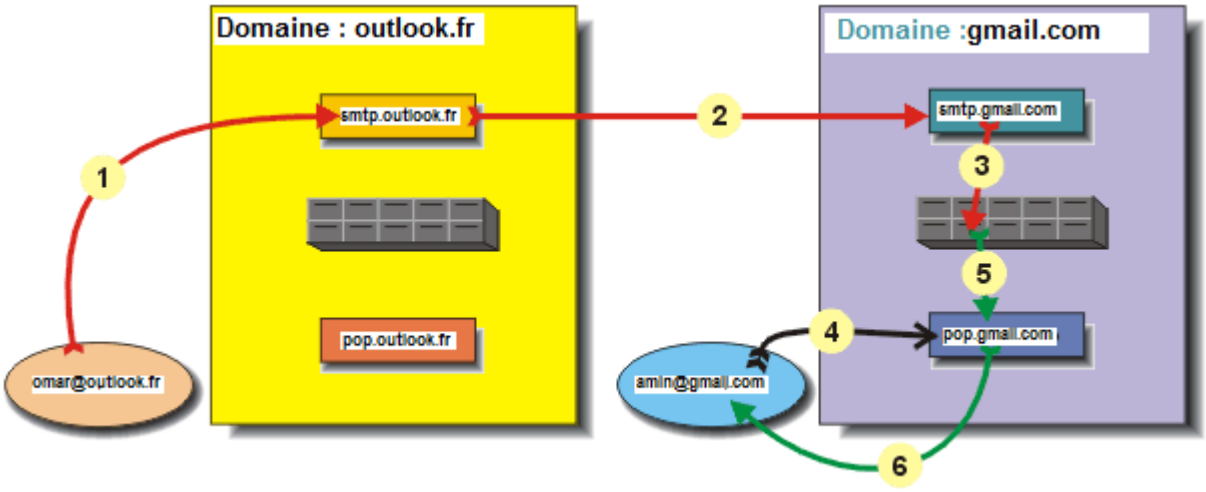
Les enregistrements MX peuvent aussi être utilisés pour réaliser un partage de charge approximatif entre plusieurs serveurs de messagerie. Pour cela on utilise plusieurs enregistrements MX ayant une même priorité. Exemple :

```
example.org.    MX    10 serveur1.example.org.
                MX    10 serveur2.example.org.
                MX    10 serveur3.example.org.
```

On peut se servir aussi de la multitude des serveurs de destination pour la tolérance de panne.

V.8. Phases d'envoi d'un email :

L'opération d'envoie d'un MAIL consiste en plusieurs phases qui s'échangent entre l'expéditeur et le destinataire. Le schéma suivant présente la succession des différentes phases :



Explication : Soit un utilisateur '**omar'** abonné chez "**outlook.fr**" ayant l'adresse électronique: omar@outlook.fr

Soit un autre utilisateur '**amine'** abonné chez "**gmail.com**" ayant l'adresse : amine@gmail.com

Le domaine **outlook.fr** dispose des serveurs : « **smtp.outlook.fr** » et « **pop.outlook.fr** »

Le domaine **gmail.com** dispose des serveurs : « **smtp.gmail.com** » et « **pop.gmail.com** »

omar doit envoyer un message à **amine**, le processus se déroule comme suit :

1. **omar** compose le message avec son outil de messagerie préféré, disons c'est 'outlook express' par exemple. Une fois le message composé, **omar** clique sur le bouton "envoyer". Comme il a correctement configuré son outil, le message est envoyé sur le serveur **smtp.outlook.fr**
2. Le serveur **smtp.outlook.fr** reçoit le message, constate que le destinataire n'est pas dans son domaine. Il cherche alors un serveur de messagerie pour le domaine **gmail.com** et le trouve. Il envoie alors le message à **smtp.gmail.com**.
3. Le serveur **smtp.gmail.com** reçoit le message, constate que le destinataire est bien dans son domaine. Il range alors le message dans la boîte aux lettres d'amine.
4. amine décide de regarder s'il a de nouveaux messages. Il envoie donc une requête à son serveur **pop.gmail.com**, au moyen de son outil de messagerie préféré (sa boite email).
5. Le serveur **pop.gmail.com** consulte alors la boîte aux lettres d'amine, constate qu'il y a un nouveau message dedans.

6. Il l'envoie alors à l'outil de messagerie de **amine** qui, par défaut, demandera à **pop.gmail.com** de le considérer comme lu et donc il devient un ancien message.

V.9. Le service FTP ou File Transfer Protocol :

C'est un service qui appartient à la couche application du modèle OSI. Il utilise une connexion TCP (mode connecté), et peut fonctionner avec IPv4 et IPv6. C'est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS.

FTP obéit à un modèle client-serveur où le serveur est un ordinateur sur lequel fonctionne un logiciel appelé serveur FTP. Pour accéder sur un serveur FTP, on utilise un logiciel client FTP et on doit disposer de droits d'accès à ce serveur FTP.

Le protocole FTP n'est pas sécurisé : les mots de passe sont envoyés sans cryptage entre le client FTP et le serveur FTP. *(Le protocole FTPS avec S pour « secure » permet de crypter les données).*

Lors d'une connexion FTP, deux canaux de transmission sont ouverts :

- Un canal pour les commandes (canal de contrôle) utilisant le port 21 par convention
- Un canal pour les données utilisant le port 20 par convention.

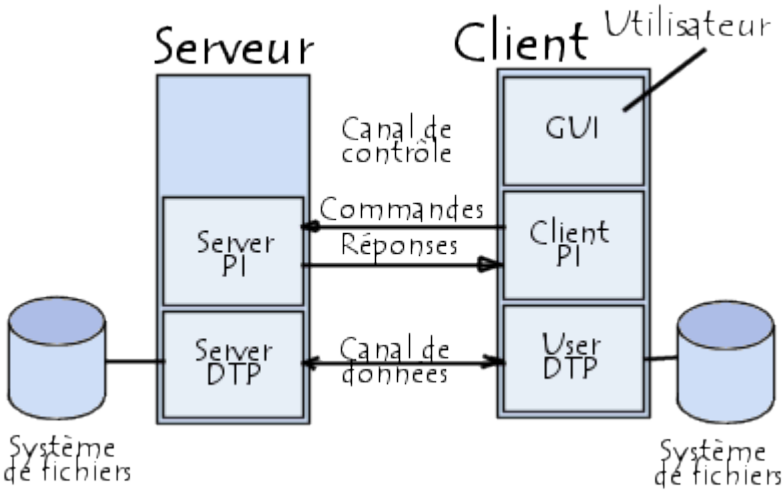
Remarque : Dans quelques cas particuliers, le port 20 ne peut pas être utilisé, il faut donc utiliser des ports hauts (de 1024 à 65635).

Ainsi, le client comme le serveur possèdent deux processus permettant de gérer ces deux types d'information :

- ✓ le DTP (Data Transfer Process) est le processus chargé d'établir la connexion et de gérer le canal de données. Le DTP côté serveur est appelé SERVER-DTP, le DTP côté client est appelé USER-DTP.
- ✓ le PI (Protocol Interpreter) est l'interpréteur de protocole permettant de commander le DTP à l'aide des commandes reçues sur le canal de contrôle. Il est différent sur le client et sur le serveur :
  - Le SERVER-PI est chargé d'écouter les commandes provenant d'un USER-PI sur le canal de contrôle, d'établir la connexion pour le canal de contrôle, de recevoir sur celui-ci les commandes FTP de l'USER-PI et d'y répondre.

- Le USER-PI est chargé d'établir la connexion avec le serveur FTP, d'envoyer les commandes FTP et de recevoir les réponses du SERVER-PI.

Lors de la connexion d'un client FTP à un serveur FTP, le USER-PI initie la connexion au serveur selon le protocole Telnet. Le client envoie des commandes FTP au serveur, ce dernier les interprète, pilote son DTP, puis renvoie une réponse standard. Lorsque la connexion est établie, le serveur-PI donne le port sur lequel les données seront envoyées au Client DTP. Le client DTP écoute alors sur le port spécifié pour les données en provenance du serveur.



Quelques logiciels serveur FTP :

- VsFTPd (Linux)
- FileZilla Server (Windows)
- WS_FTP server (Windows)
- ProFTPd (Linux)

Quelques logiciels client FTP :

- FileZilla client (Windows, Linux, IOs)
- Cute FTP Home (payant) (Windows, IOs)
- SmartFTP (payant)

Chapitre VI : Contrôleur de domaine

VI.1. Définition et objectif :

Active Directory (AD) est un annuaire qui répertorie est organise les informations concernant le monde Microsoft (pour les systèmes d'exploitation Windows) que ceux soient des utilisateurs, des machines ou des applications.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système d'exploitation : Windows, MacOs et encore Linux. Il permet également l'installation de mises à jour critiques par l'administrateur. Active Directory permet de répertorier les éléments d'un réseau tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées.

Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012 et Windows Server 2016. Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ».

Tout comme le serveur SNMP, AD stocke des informations sur les objets réseau et implémente également les services qui rendent ces informations disponibles et utilisables par les utilisateurs, les ordinateurs et les applications. Les informations sont stockées dans une base de données distribuée sur un ou plusieurs contrôleurs de domaine. La taille d'une base Active Directory peut varier de quelques centaines d'objets, pour de petites installations, à plusieurs millions d'objets, pour des configurations étendues.

VI.2. Les objets d'un AD :

Une structure Active Directory (AD) est une organisation hiérarchisée d'objets. Les objets sont classés en trois grandes catégories : les ressources (par exemple les imprimantes), les services (par exemple le courrier électronique) et les utilisateurs (comptes utilisateurs et groupes). L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité.

Chaque objet représente une entité unique (utilisateur, ordinateur, imprimante ou groupe) ainsi que ses attributs. Un objet est identifié de manière unique dans l'AD par son nom et possède son propre jeu d'attributs (les caractéristiques et les informations que l'objet peut contenir) défini par un schéma, qui détermine également le type d'objets qui peuvent être stockés dans l'AD.

Chaque objet attribut peut être utilisé dans plusieurs classes d'objets de schéma différents. Ces objets de schéma existent pour permettre au schéma d'être étendu ou modifié si nécessaire. Cependant, comme chaque objet de schéma est intégral à la définition des objets de l'AD, la désactivation ou la

modification de ces objets peut avoir de graves conséquences car elle entraîne des modifications fondamentales dans la structure de l'AD. Un objet de schéma, lorsqu'il est modifié, est automatiquement propagé dans Active Directory et une fois créé, il ne peut plus être supprimé (il peut seulement être désactivé). Pour cette raison, une modification du schéma doit être mûrement réfléchie et planifiée.

Active Directory étant un annuaire objet, la notion de schéma définit les contraintes concernant la dérivation et l'héritage des objets, sensiblement de la même manière qu'en programmation objet. Cela introduit également la notion d'extension, permettant d'ouvrir l'annuaire à toutes sortes d'applications souhaitant stocker des objets personnalisés au niveau du ou des domaines constituant la forêt Active Directory.

VI.3. La structure arborescente d'un AD :

Une arborescence Active Directory est composée de :

- La forêt : structure hiérarchique d'un ou plusieurs domaines indépendants (ensemble de tous les sous domaines Active Directory).
- L'arbre ou l'arborescence : domaine de toutes les ramifications. Par exemple, dans l'arbre ***domaine.tld***, *sousdomaine1.domaine.tld* et *sousdomaine2.domaine.tld* sont des sous-domaines de ***domaine.tld***.
- Le domaine : constitue les feuilles de l'arborescence. ***photo.sousdomaine1.domaine.tld*** peut-être un domaine au même titre que domaine.tld.

Le protocole principal d'accès aux annuaires est LDAP qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans Active Directory, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger Active Directory ou pour y ajouter, y modifier ou y supprimer des données.

VI.4. Relation entre AD et DNS :

DNS est le système de dénomination de facto pour les réseaux IP et le service de dénomination utilisé pour localiser les ordinateurs sur Internet. Le système d'exploitation utilise donc le DNS pour localiser les ordinateurs et les contrôleurs de domaine (AD). Un poste de travail ou un serveur membre trouve un contrôleur de domaine en interrogeant le DNS.

Les ensembles d'espaces de nom correspondant aux arborescences d'Active Directory formant la forêt Active Directory sont superposables à l'espace de nom formé par les zones DNS. DNS est un service

indispensable pour le bon fonctionnement de toute l'architecture Active Directory, localisation des contrôleurs de domaine, réplication, etc.