Ministère de l'enseignement supérieur et de la recherche scientifique

Université Abderrahmane Mira, Béjaia

Faculté de Technologie

Département Automatique, Télécommunications et Électronique

Cours

Administration des Services Réseaux

Destiné aux Étudiants de Master 1

Filière

Télécommunications

Spécialité

Réseaux et Télécommunications

Dr. BELLAHSENE Hocine

Année Universitaire 2026

Avant-propos

Public visé

Ce polycopié de cours est destiné aux étudiants de Master 1 spécialité Réseaux et Télécommunications. Les étudiants en cycle ingénieurs en télécommunications et en informatique peuvent aussi en bénéficier.

L'administration des services réseaux est un pilier fondamental dans l'architecture et la gestion des infrastructures modernes de communication. Dans un monde où la connectivité est devenue essentielle, maitriser les services réseaux est indispensable pour tout professionnel des télécommunications.

Objectifs du cours

- ▷ Comprendre l'architecture et le fonctionnement des services réseaux.
- ▷ Maitriser la configuration des services essentiels (DNS, DHCP, HTTP, FTP, SMTP)
- ▷ Apprendre à sécuriser et monitorer les infrastructures réseaux (entre autre le protocole SNMP)
- ▷ Développer une approche méthodologique d'administration

Plan du cours

1. Présentation de l'administration réseaux
2. Le service SNMP
3. Les services annuaires
4. Gestion des utilisateurs et services NFS
5. Services de messagerie et services d'application
6. Contrôleurs de domaines
7. Virtualisation des services

Contenu synthétique

Compétences visées

À l'issue de ce cours, les Travaux dirigés ainsi que les Travaux pratiques, l'étudiant sera capable de déployer, configurer, sécuriser et maintenir des services réseaux en environnement professionnel.

Pour aller plus loin

La pratique en environnement virtualisé (VMware, VirtualBox, Docker, GNS3) est étudiée au travers d'exposés présentés par les étudiants et débattus avec leurs collègues ainsi que leur enseignant. Certains aspects sont supervisés, tels que :

- ▷ Pare-feu
- ▷ Certificats SSL/TLS et chiffrement
- ▷ Outils de monitoring (Nagios, Zabbix, Proxmox)
- ▷ Journaux et audits (syslog)

Table des matières

Chapitre 1

Présentation de l'administration réseau

1.1 Introduction

Dans ce chapitre, nous aborderons les objectifs et le rôle de l'administration des services réseaux. De plus, nous examinerons le modèle de gestion du réseau, les différents types de réseaux clients-serveurs, les protocoles de gestion, les services de la couche d'application et les concepts de ports de service.

1.2 Objectifs et rôle de l'administration des réseaux

1.2.1 Définition d'un réseau et son intérêt

Un réseau est un système complexe de deux ou plus d'objets (machines) reliés les uns aux autres. Des applications (programmes) qui fonctionnent sur des hôtes peuvent dialoguer et s'échanger des données. Cet échange peut être aussi bien matériel que logiciel. Parmi l'intérêt de la mise en place d'un réseau on trouve :

- ▷ Partage des ressources matérielles, logicielles et de données.
- ▷ La communication entre les utilisateurs et/ou les applications distantes (partage de données).
- ▷ La coopération en temps réel : collaborer sur des projets en temps réel.
- ▷ Accès à l'information : les réseaux permettent aux utilisateurs d'accéder à des informations en temps réel pour prendre des décisions et résoudre des problèmes.
- ▷ Sécurité : Utilisation de pare-feu et de cryptage pour protéger les données.

Les taches du superviseur

1. S'assurer que les utilisateurs de l'entreprise sont satisfaits du bon fonctionnement des systèmes informatiques et du réseau.
2. Garantir la disponibilité, la sécurité et l'intégrité des informations et des données sensibles.
3. Mettre en place des politiques et des procédures pour s'assurer que les normes et les règlementations sont respectées.
4. Suivre et optimiser les performances des systèmes informatiques.
5. Garantir que les activités continuent en cas de panne ou de sinistre
6. Organiser et superviser les mises à jour et les mises à niveau logiciels et matérielles.

L'administration est chargée de garantir l'atteinte des objectifs susmentionnés en mettant en œuvre les politiques, les procédures et les technologies appropriées. La gestion de l'infrastructure informatique, la gestion des utilisateurs, la sécurité et la sauvegarde des données, ainsi que la mise en œuvre de politiques de conformité. La figure 1.1 représente le système d'information qui décrit le réseaux d'une entreprise et recense toutes les données et évènements relatifs à chaque élément du réseau administré. Parfois pour répondre aux difficultés de gestion, l'administrateur fait appel à son intuition et à son expérience. En raison du développement de l'intelligence

artificielle, de nombreux moteurs d'inférence effectuent actuellement le diagnostic du réseau, sa simulation et la planification des opérateurs pour apporter des corrections ou des changements futurs.

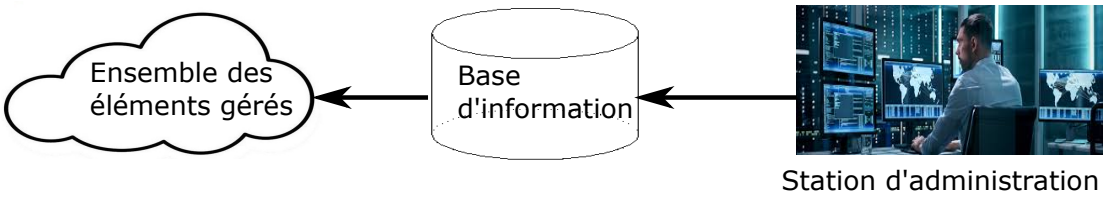


FIGURE 1.1 – Principe d'un système d'administration réseau

1.2.2 La structure fonctionnelle d'un système d'administration

Un grand nombre de composants (objets) du réseau sont surveillés par le système d'administration. Un programme en tâche de fond (Deamon : Disk And Execution MONitor) transmet régulièrement ou par sollicitation des informations pour surveiller l'état de chaque objet(voir figure 1.2).

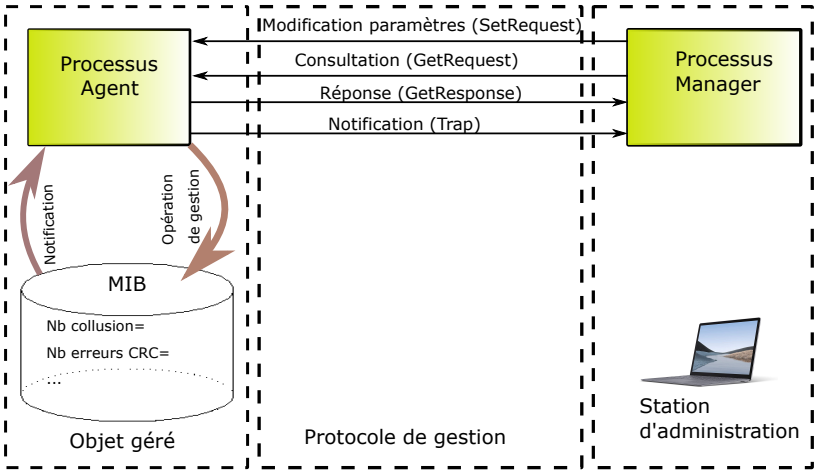


FIGURE 1.2 – Structure fonctionnelle d'un système d'administration

Les échanges ont lieu sur deux niveaux : entre le composant administré (processus agent) et sa base d'information MIB (Management Information Base), d'un côté, et entre le composant et le programme d'administration (processus manager), de l'autre.

1.3 Le modèle d'administration réseaux

Les différentes tâches et responsabilités qui doivent être accomplies pour gérer efficacement un réseau sont définies dans le modèle d'administration du réseau. Il est souvent présenté sous forme de couches, chacune dédiée à une tâche particulière, comme la gestion des adresses IP, la gestion des protocoles, la gestion des services et la gestion des utilisateurs.

Un cadre de référence pour la planification, la conception, l'implémentation, la gestion et l'optimisation des réseaux informatiques est le modèle d'administration des réseaux. Il fournit une structure claire pour les diverses fonctions et responsabilités nécessaires à l'administration d'un réseau, telles que la surveillance et la résolution des problèmes. Le modèle OSI (Open Systems Interconnection) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) font partie des différents modèles d'administration du réseau. Le modèle Open Systems Interconnection (OSI) divise la communication réseau en sept couches distinctes, chacune avec ses propres fonctionnalités. Le modèle TCP/IP définit les protocoles utilisés pour la transmission de données sur un réseau. Les administrateurs peuvent mieux comprendre les différentes couches d'un réseau et comment elles

interagissent en utilisant un modèle d'administration du réseau. De plus, cela leur permet de résoudre les problèmes plus rapidement et efficacement en localisant la source du problème à une couche spécifique.

1.3.1 L'administration réseau et ISO (International Standardization Organization)

Introduction

L'ISO définit un cadre architectural général (ISO 7498-4, OSI Management Framework) et donne un aperçu général des opération de gestion des systèmes (ISO 10040, OSI système Management) sans qu'elle ne spécifie aucun système d'administration réseau des deux documents précités décrivent trois modèles :

Modèle organisationnel ou architectural, MSA (Managed System and Agent)
Il définit la notion de systèmes gérés et organise la gestion OSI DMAP qui est un processus de gestion des applications dispersées((Distributed Management Application Processus). Un cadre de référence pour la conception et la mise en œuvre de systèmes d'information distribués est un modèle organisationnel ou architectural. Il décrit la structure fonctionnelle et les interactions entre les composants d'un système distribué, comme les protocoles de communication, les services de gestion, les interfaces utilisateur, les applications et les systèmes d'exploitation. Le modèle client-serveur, le modèle peer-to-peer et le modèle orienté services (SOA), qui sont utilisés dans les environnements d'entreprise et les architectures orientées web, font partie des modèles architecturaux courants.

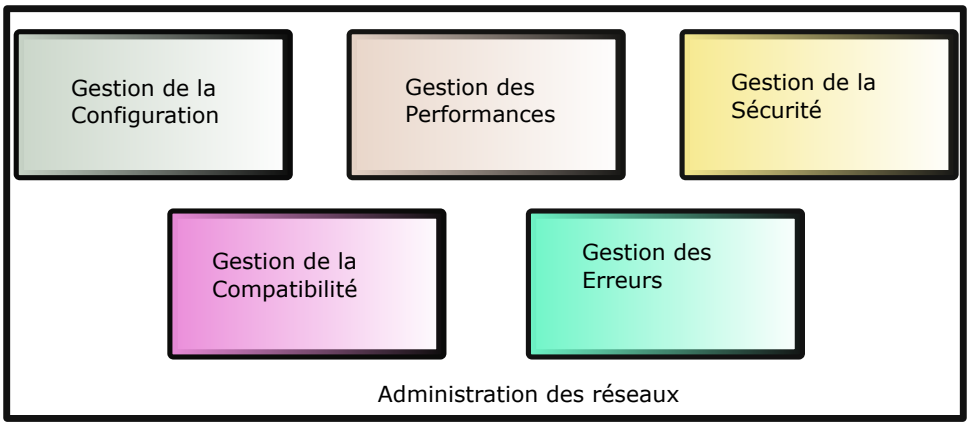


FIGURE 1.3 – Les aires fonctionnels de la gestion ISO

Le modèle de base d'information de gestion, ou MIB
La MIB est une base de données pour les informations de gestion qui regroupe les objets gérés ainsi que les informations qui s'y rapportent (attributs). C'est un ensemble de descriptions de données qui décrit les objets gérés dans un système de gestion de réseau. Les MIB sont utilisés pour surveiller les performances et diagnostiquer les problèmes ainsi que pour collecter des informations sur les périphériques réseau tels que les routeurs et les commutateurs. Les données de la MIB sont stockées dans une structure hiérarchique d'objets, chacun étant identifié par un identificateur d'objet unique OID (Object IDentitier) et défini par une syntaxe de données particulière. Les MIB peuvent fonctionner avec un certain nombre de protocoles de gestion de réseau, notamment le protocole SNMP (Simple Network Management Protocol).
Modèle fonctionnel, SMFA (Specific Management Function Area)
Les cinq domaines (aires) fonctionnels de l'administration sont définis sur la figure 1.3.

1.3.2 Étude des différents modèles

1.3.3 Modèle architectural

Il participe aux trois activités suivantes.

1. La gestion du système (System Management).
2. La gestion couche (Layer Management).
3. Les opérations de couche (Layer Operation).

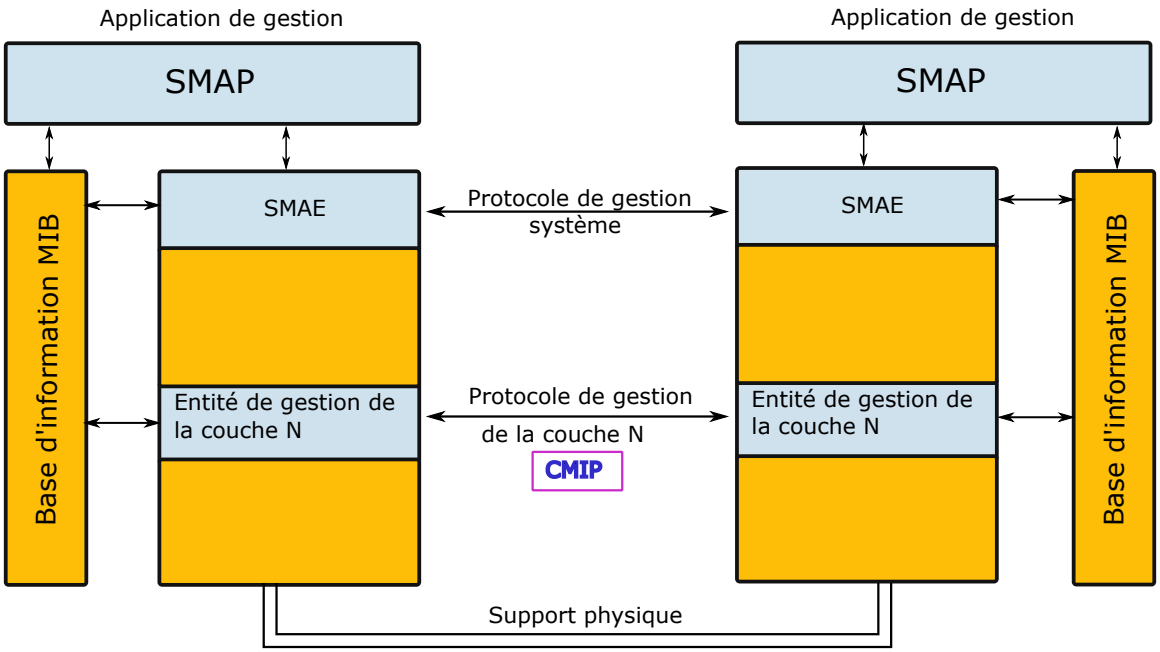


FIGURE 1.4 – Modèle architectural de l'ISO

La gestion du système SMAE (System Management Application Entity)

Elle connecte les processus gérant et agent. L'agent (équipement, protocole) gère les ressources locales tout en étant sous le contrôle de l'agent/gérant comme indiqué par la figure 1.4. La gestion système repose sur des échanges verticaux entre les couches du service d'information de gestion commune, également connu sous le nom de CMIS (Common Management Information Service). Le CMIS (ISO 9595) définit les primitives d'accès aux informations. Elles sont chargées de transférer les informations aux applications de gestion SMAP (System Management Application Process), Processus d'application de gestion du système, non spécifié par ISO.

La gestion de couches

La gestion ou le protocole de gestion de couches permet le transfert d'informations de gestion entre les sites administrés. Il s'agit d'un dialogue horizontal CMIP appelé protocole d'information de gestion commun ;(Common Management Information Protocol ; ISO 9595).

Les opérations de couches

Les protocoles de couche N gèrent une connexion de niveau N. Pour le transfert d'informations, ils utilisent les protocoles OSI conventionnels. Les primitives de service CMISE (Common Management Information Service Element) suivantes sont utilisées par CMIP :

- ▷ Get : pour lire la valeur d'un attribut le gérant utilise cet élément de service.
- ▷ Set : permet de fixer la valeur d'un attribut.
- ▷ Event : cet élément de service est utilisé par l'agent pour signaler un évènement.
- ▷ Create : génère un nouvel objet.
- ▷ Delate : permet à l'agent de supprimer un objet.

1.3.4 Modèle informationnel

Le modèle OSI décrit et modélise la représentation des données d'administration et fournit un ensemble de directives pour s'assurer que la base SMI (Structure of Management Information) qui est une structure des données d'administration est cohérente. La représentation des objets gérés est orientée objet dont les classes et les occurrences sont représentée selon un arbre - un objet est décrit par sa classe d'appartenance, son nom, ses attributs et les types d'opérations qu'il supporte.

- ▷ Les classes sont rattachées à un arbre dit d'héritage (Inheritance tree).
- ▷ Les occurrences sont rattachées à un arbre dit de contenance (Contenance tree).

La MIB (ISO 10165) est constituée par l'ensemble des objets gérés. Elle englobe toutes les informations administratives sur les objets gérés (pont, routeurs, cartes). La norme ne spécifie aucune organisation particulière des données. Le processus agent est le seul à accéder à la MIB même le processus manager n'accède à celle-ci qu'à travers lui.

1.3.5 Modèle fonctionnel SMFA (Specific Management Function Area)

Ce modèle définit les cinq domaines (aires fonctionnelles, figure 1.3) d'administration et leurs relations.

Gestion des anomalies (Fault Management)

L'objectif de l'administration du réseau est d'optimiser les ressources et les moyens, c'est pourquoi il est crucial de trouver rapidement un diagnostic en cas de défaillance du système. Il peut s'agir d'une source externe (un public coupé) ou interne au système (un routeur en panne). Elle inclut :

- ▷ La surveillance des alarmes (filtre, report..).
- ▷ Le traitement de celle-ci.
- ▷ La localisation et le diagnostique des incidents.
- ▷ La mémorisation des anomalies (journalisation).
- ▷ La définition des opérations curatives.

Gestion de la comptabilité (Accounting Management)

Les utilisateurs doivent payer les coûts après les avoir évalués par la gestion des éléments comptables, selon l'utilisation réelle des moyens. Les coûts sont répartis en fonction des centres de frais de l'entreprise (comptabilité analytique). Les tâches de comptabilité comprennent :

- ▷ Définition des centres de coût.
- ▷ Mesure des dépenses de structure (coûts fixes) et répartition.
- ▷ Mesure des communications par service.
- ▷ Imputation des coûts

Gestion de la configuration et des noms (Configuration Management)

Il s'agit d'enregistrer de manière précise les ressources matérielles (type, équipement...) et logicielles (version, fonctions...) ainsi que leur localisation géographique.Chaque objet lui est associé un nom qui l'identifie de façon unique.

Gestion des performances (Performance Management)

Elle implique l'évaluation du comportement des objets gérés. Une collecte d'informations statistiques pour déterminer en permanence si le réseau est capable de satisfaire la demande des utilisateurs. Il est possible d'évaluer les performances afin d'anticiper une défaillance avant qu'elle ne se produise. Il est également possible de programmer les évolutions du système. En résumé, il comprend :

- ▷ La collecte d'information(mesure du trafic, temps de réponse, taux d'erreurs).
- ▷ Le stockage (archivage...).
- ▷ L'interprétation des mesures (calcul de la charge du système).

Pour accomplir cette tâche, il est nécessaire d'utiliser un outil de modélisation et de simulation pour évaluer l'impact de la modification de l'un des paramètres sur l'ensemble du système.

Gestion de la sécurité (Secutity Management)

L'ISO sécurise les informations et les objets administrés grâce à des mécanismes d'encryptage et d'identification des extrémités (sources et destination) ainsi qu'au contrôle des accès aux données. Par conséquent, cinq services de sécurité garantissent l'intégrité des informations et des objets :

- ▷ Les contrôles d'accès réseau.
- ▷ La confidentialité qui consiste à s'assurer que les données ne sont communiquées qu'aux personnes ou processus autorisés.
- ▷ L'intégrité qui assure que les données n'ont pas été accidentellement ou volontairement modifiées ou détruites.
- ▷ L'authentification garantissant que l'entité participant la communication et bien celle déclarée.
- ▷ Le non désaveu mécanisme qui interdit, à une entité participant à une communication, de nier avoir participé à celle-ci.

1.4 Réseau clients serveurs

Un réseau client-serveur permet aux clients d'envoyer des demandes de services aux serveurs qui les fournissent. Les différents composants d'un réseau échangent des données via des protocoles administratifs. Les applications qui utilisent des protocoles pour fournir des services spécifiques, tels que la messagerie électronique, le transfert de fichiers et le partage de fichiers, sont appelées services de couche d'application.

1.4.1 Principe de fonctionnement

Un réseau client-serveur repose principalement sur la centralisation des ressources informatiques sur des ordinateurs appelés serveurs. En envoyant des requêtes au serveur, les clients peuvent accéder à ces ressources. Le serveur traite ces requêtes et fournit les ressources que les clients ont demandées. Cela améliore l'utilisation et la gestion des ressources car elles ne sont plus dispersées sur plusieurs ordinateurs. Voici les étapes de ce processus :

1. Le client demande au serveur d'accéder à une ressource ou à un service.
2. La requête est reçue par le serveur et traitée.
3. Le serveur examine si le client possède les autorisations nécessaires pour accéder à la ressource souhaitée.
4. Si le client possède les autorisations nécessaires, le serveur fournit au client la ressource qu'il a demandée.
5. Si le client n'a pas les autorisations nécessaires, le serveur peut refuser la requête ou la rediriger vers un autre serveur qui peut la traiter.

Les clients sont généralement des ordinateurs de bureau, des ordinateurs portables ou des appareils mobiles connectés au réseau local ou à distance. Les serveurs sont des ordinateurs dédiés ou multitâches qui fournissent des ressources à plusieurs clients en même temps. Ce modèle permet aux entreprises de centraliser les ressources et les services informatiques afin de les utiliser plus efficacement et de les gérer plus facilement. Les réseaux client-serveur sont largement utilisés pour fournir des services tels que des bases de données, des applications web, des messageries électroniques, des fichiers, des services d'impression, etc. Deux types d'architectures client/Serveur existe.

1.4.2 Architecture Centralisée

Une seule entité serveur fournit les réponses aux requêtes dans le cadre d'une architecture centralisée voir figure 1.5. C'est simple de maintenir, de sauvegarder, de mettre à jour et de garantir que les données fournies sont cohérentes car il n'y a qu'une seule source de données. Ses inconvénients comprennent une surcharge potentielle, une architecture unique fragile, un manque de flexibilité et des performances fluctuantes en fonction de l'emplacement géographique des clients comme du serveur.Architecture partagée.

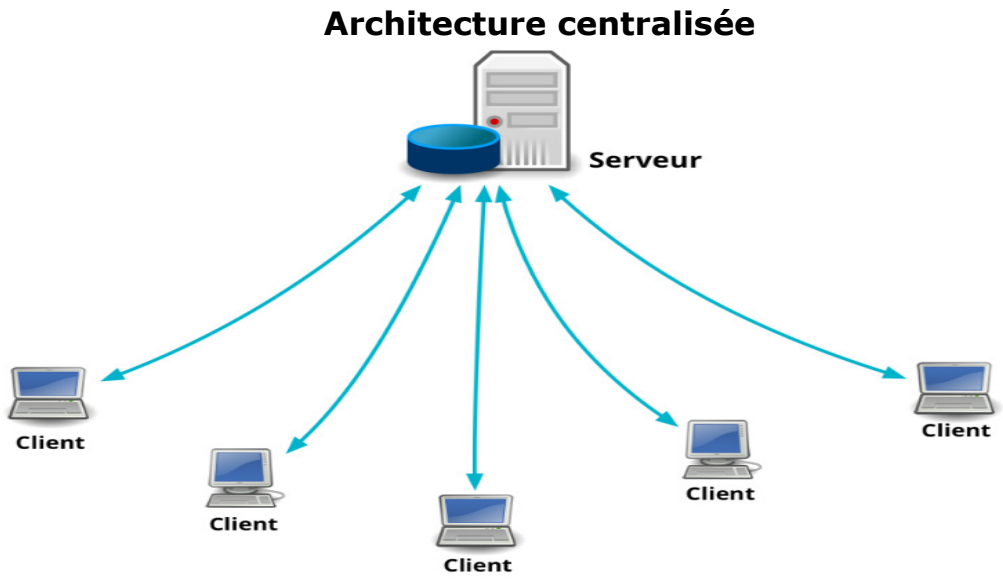


FIGURE 1.5 – Architecture Client Serveur Centralisée

1.4.3 Architecture Distribuée

Les données à servir peuvent être réparties entre plusieurs serveurs dans une architecture distribuée tel que montré par la figure . Les données peuvent être classées en différentes catégories (par exemple, un serveur gère uniquement les données des clients américains, un autre des clients asiatiques, etc.). Il est également possible de dupliquer les données entre plusieurs serveurs, ce qui permet aux serveurs de supporter un grand nombre de clients. C'est une architecture complexe qui peut être difficile à maintenir. En revanche, l'architecture est robuste en cas de panne et flexible en cas de montée en charge.

1.4.4 Exemples

1) Une banque en ligne est un exemple typique d'un système client-serveur. En utilisant leur ordinateur ou appareil mobile qui agit en tant que client, les clients peuvent accéder à leur compte bancaire en ligne. Le client demande l'accès à son compte en ligne pour voir ses informations financières, effectuer des transactions, etc. Le serveur bancaire reçoit cette requête. Le serveur traite la demande du client et renvoie les données au client. Les informations financières des clients sont stockées sur le serveur et traitées en temps réel. Dans ce scénario, le serveur est la source d'informations, et le client est l'appareil qui accède à ces informations pour les afficher et les utiliser.

2) Pour consulter des pages web via le protocole HTTP :

Quelques serveurs : Apache, Nginx, IIS, Lighthttpd...

Quelques clients : Firefox, Chrome, Safari, Opéra, Edge...

3) pour accéder aux données stockées dans des bases de données :

Quelques serveurs : MySQL, PostgreSQL, Oracle, Access, dBase, SQL Server...

Quelques clients : Mysql, Postgre...

4) l'envoi et la réception d'emails via le protocole SMTP :

Quelques serveurs : Qmail, postfix, Sendmail...

Quelques clients : Thunderbird, Outlook, Gmail, Apple Mail...

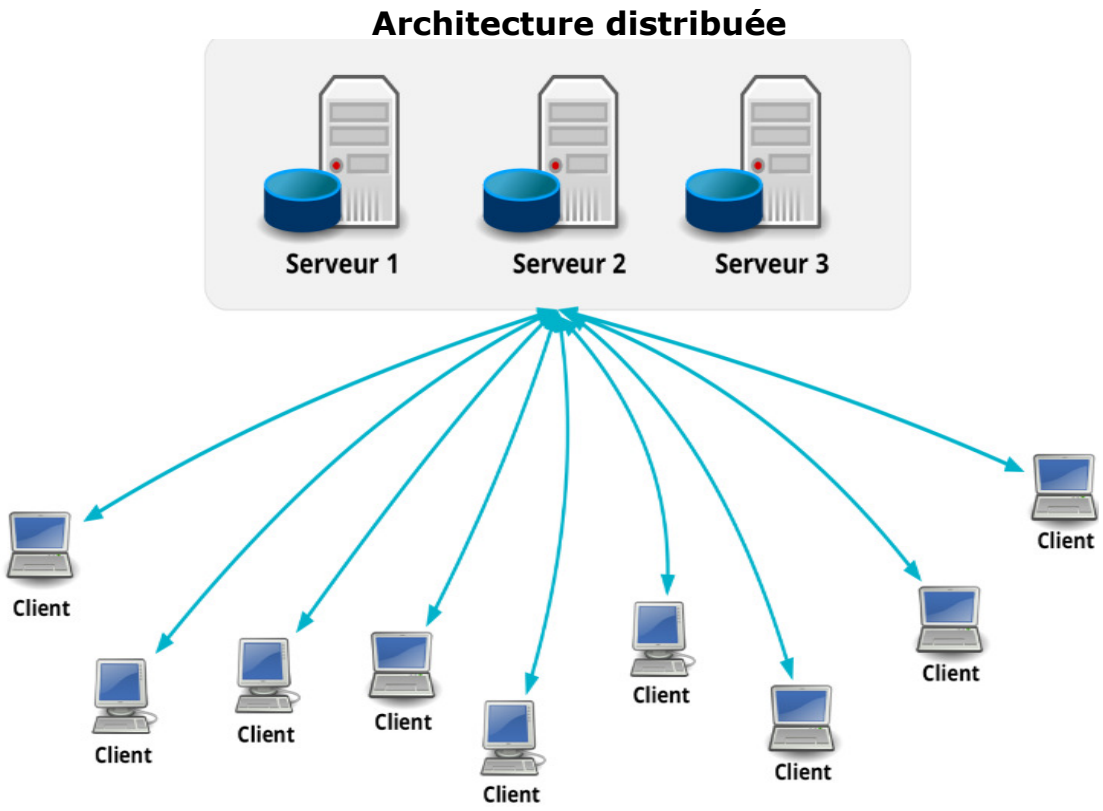


FIGURE 1.6 – Architecture Client Serveur Distribuée

1.5 Les Protocoles d'administration

1.5.1 Définition

Les protocoles d'administration sont des règles et des normes qui permettent aux équipements réseau de communiquer et de gérer les informations. Ils sont utilisés pour effectuer des tâches telles que la surveillance, la configuration, la gestion de la sécurité et le diagnostic des erreurs liées à l'administration du réseau. Les administrateurs de réseau utilisent fréquemment des protocoles d'administration pour gérer les réseaux à distance, vérifier leurs performances et effectuer des diagnostics en cas de problème. Les protocoles d'administration courants sont SNMP (Simple Network Management Protocol), Telnet et SSH.

1.5.2 Exemples

Sous Linux

Il y a plusieurs protocoles d'administration disponibles sous Linux, notamment SSH (Secure Shell), Telnet, RSH (Remote Shell) et FTP (File Transfer Protocol). Le protocole SSH protège les connexions à distance. Le cryptage protège les données transmises entre le client et le serveur. Telnet, un protocole de terminal à distance, permet à un utilisateur de se connecter et de gérer un ordinateur à distance. Cependant, Telnet n'utilise pas de cryptage pour protéger les données transmises, ce qui le rend moins sûr que SSH. RSH (Remote Shell) est un protocole comparable à Telnet, mais il est moins utilisé. Le protocole FTP permet aux utilisateurs de télécharger et de transférer des fichiers à partir d'un ordinateur où serveur distant.

Sous Windows

Les protocoles d'administration à distance les plus fréquemment utilisés sous Windows sont Remote Procedure Call (RPC), Remote Administration Daemon (RADMIN), Telnet et Remote Desktop Protocol (RDP). Un ordinateur distant peut exécuter des tâches sur un autre ordinateur grâce à RPC. RADMIN est un programme d'administration à distance capable de gérer centralement des ordinateurs distants. Un utilisateur peut utiliser Telnet pour se connecter à un ordinateur distant et le contrôler à partir d'un terminal. Un utilisateur peut se connecter à un ordinateur distant et le contrôler à l'aide d'une interface graphique grâce à RDP.

1.6 Les services de la couche d'application

Les protocoles qui permettent aux différentes applications sur un réseau de se connecter et de communiquer sont appelés services de la couche d'application. Ils offrent les fonctionnalités nécessaires pour effectuer des tâches particulières telles que l'envoi de messages électroniques, le transfert de fichiers, la consultation de pages Web, etc. Les protocoles tels que SMTP (Simple Mail Transfer Protocol) pour les e-mails, FTP (File Transfer Protocol) pour le transfert de fichiers, HTTP (Hypertext Transfer Protocol) pour le web et d'autres sont utilisés pour fournir des services de couche d'application. Ils sont souvent le point de contact direct entre les applications utilisateurs et le réseau, permettant aux utilisateurs de profiter des différentes fonctionnalités du réseau.

1.6.1 Quelques services de la couche d'application sous Linux

Dans Unix, les services de la couche d'application sont des applications qui facilitent le transfert de données entre les applications clientes et les applications serveurs grâce à l'utilisation de protocoles de communication standardisés. Il s'agit de services comme le service HTTP pour le Web, le service FTP pour le transfert de fichiers, le service SMTP pour l'envoi de courrier électronique, etc. Les couches inférieures du modèle Open Systems Interconnection (OSI) collaborent avec les services de la couche d'application pour gérer les protocoles de communication et les connexions réseau. Ils sont cruciaux pour la sécurité et la fiabilité des échanges de données sur un réseau.

Les programmes ou les applications qui permettent aux utilisateurs de communiquer avec le réseau sont appelés services de couche d'application. Sous Linux, les services de la couche d'application comprennent :

1. HTTP (Hypertext Transfer Protocol) est utilisé pour afficher et télécharger des pages web sur Internet.
2. Le protocole de transfert de fichiers ou FTP est utilisé pour transférer des fichiers entre différents ordinateurs.
3. Le logiciel SSH (Secure SHell) est destiné à créer une connexion sécurisée entre deux ordinateurs
4. Le protocole de transfert de courrier SMTP (Simple Mail Transfer Protocol) , est utilisé pour le transfert de courriers entre les serveurs de messagerie.
5. Le système de noms de domaine DNS (Domain Name System) sert à convertir les noms de domaine en adresses IP.

Ces protocoles sont des normes qui permettent aux divers équipements et applications de communiquer sur un réseau.

Exemple : La commande systemctl est utilisée sous Linux pour gérer les services système, y compris ceux de la couche d'application. La syntaxe de base est :

sudo systemctl [action] [nom-du-service]
Pour démarrer un service, on utilise :
sudo systemctl start nom-du-service
Pour mettre fin à un service :
sudo systemctl stop nom-du-service
Afin de relancer un service :
sudo systemctl restart nom-du-service
Pour vérifier l'état d'un service :
sudo systemctl status nom-du-service
Le terme "**nom-du-service**" doit être remplacé par le nom exact du service que nous souhaitons gérer dans les commandes précédentes.

1.6.2 Quelques services de la couche d'application sous Windows

Les services de la couche d'application sont des programmes logiciels qui fonctionnent sur une couche élevée de protocoles de communication et offrent des fonctionnalités spécifiques aux utilisateurs finaux et aux applications. Les exemples de services de la couche d'application sous Windows comprennent :

1. Services Web : Les services Internet Information Services (IIS) permettent la création de sites Web, de pages Web et d'applications Web.
2. Services de messagerie : Il est possible de gérer les boites aux lettres des utilisateurs, les agendas, les contacts et les tâches grâce à Microsoft Exchange Server.
3. Services de fichiers : Il est possible de partager des fichiers et des imprimantes avec des ordinateurs du réseau grâce au protocole de messagerie serveur SMB (Server Message Block).
4. Les services de terminal Remote Desktop Services (RDS) offrent la possibilité d'accéder à des ordinateurs distants afin d'exécuter des applications et de contrôler des ordinateurs.
5. Services VPN : Les utilisateurs distants peuvent obtenir des connexions VPN grâce aux services de routage et d'accès à distance RRAS (Routing and Remote Access Services).
6. Services de stockage : Le gestionnaire de stockage pour SANs, SMfS (Storage Manager for SANs) est en mesure de gérer les réseaux de zone de stockage SAN (Storage Area Networks) pour le stockage de données.

Exemple :

1) La ligne de commande suivante est utilisée sous Windows pour accéder aux services de la couche d'application :
service.msc
Cette commande ouvre la console des services, qui permet de gérer et de configurer les services système, y compris ceux liés à la couche d'application.
2) Sous l'invite de commande (CMD) de Windows, la première permet d'arreter un services et la seconde permet de le redémarer :
net stop NomDuService
net start NomDuService.

1.7 Notions de ports de service

Les numéros associés à des services particuliers sont appelés ports de service. Lorsqu'un client envoie une demande à un serveur, un port particulier est utilisé pour identifier le service requis. Par exemple, le port 25

est généralement lié au service de messagerie SMTP, tandis que le port 80 est lié au service Web HTTP. Les numéros attribués aux protocoles de communication particuliers qui permettent à un système de transmettre et de recevoir des données sur un réseau sont appelés ports de service. Ces numéros de port sont utilisés par les protocoles de communication tels que TCP et UDP pour désigner les applications ou les services qui gèrent les données.

Quelques exemples de protocoles courants liés à certains numéros de port :

- ▷ Le protocole de transfert d'hypertexte HTTP (Hypertext Transfer Protocol) utilise le port 80.
- ▷ HTTPS (Secure Hypertext Transfer Protocol) utilise le port 443.
- ▷ Le protocole de transfert de fichiers FTP utilise les ports 20 et 21.
- ▷ Le protocole de transfert de courrier simple SMTP utilise le port 25.
- ▷ Le système de nom de domaine (DNS) utilise le port 53.
- ▷ Le port 23 est utilisé par Telnet.

Il est a souligner que ces numéros de port sont standardisés et identifiés pour être liés à des protocoles particuliers. Cela permet aux systèmes de transmettre et de recevoir efficacement et sécurisément des données en utilisant des protocoles spécifiques pour des applications particulières.

1.7.1 Principe de gestion et de fonctionnement des ports

Une application client utilise un protocole de communication spécifique pour transmettre les données lorsqu'elle souhaite se connecter à un serveur pour accéder à un service ou envoyer une requête. Ce protocole établit des normes pour la transmission de données, y compris le format et la transmission des paquets de données. Les numéros associés à chaque protocole de communication sont appelés ports de service et sont utilisés pour identifier les services disponibles sur le serveur. Par exemple, le port 80 est lié au protocole HTTP et est utilisé pour identifier les services web qui sont disponibles sur le serveur.

Une application cliente envoie une requête à l'adresse IP du serveur en utilisant le port associé au protocole approprié lorsqu'elle souhaite se connecter à un service particulier sur le serveur. Le serveur reçoit la requête, l'examine et exécute le service demandé à l'aide du protocole correspondant. Le protocole et les règles utilisés pour transférer les données entre le client et le serveur. Les applications clientes peuvent se connecter aux services sur les serveurs de manière efficace et fiable grâce aux ports de service et aux protocoles associés.

1.7.2 Exemples

Sous Linux/Unix

Plusieurs outils tels que netstat, telnet et nc (netcat) peuvent être utilisés pour gérer les ports de service sous Unix/Linux. Les ports de service en écoute et les connexions actives du réseau peuvent être visualisés à l'aide de l'outil netstat. Par exemple, la commande "netstat -tulpn" montrera les ports de service en écoute et les connexions actives ainsi que les informations de processus associées. Un service est dit en écoute sur son port associé lorsqu'il est actif et prêt à accepter des connexions.
Le protocole de communication Telnet permet de créer une session à distance avec un serveur sur un port particulier. Par exemple, la commande "**telnet localhost 80**" tentera d'établir une session à distance avec le serveur local sur le port HTTP. Il est possible d'utiliser nc (netcat), un outil de test et de débogage de réseau, pour tester la connectivité sur un port de service spécifique. Par exemple, la commande "**nc -vz localhost 443**" vérifie si le port 443 (HTTPS) est actif sur le serveur local, avec :
nc : l'utilitaire Netcat.
-v : active le mode verbeux, ce qui signifie qu'il affichera des informations détaillées sur ce qu'il fait.
-z : demande à Netcat de scanner le port sans envoyer de données. localhost : l'hôte que vous souhaitez tester, dans ce cas, c'est votre propre machine (127.0.0.1).
443 : le numéro de port que vous souhaitez tester.

Sous Windows

Sous Windows, la commande netsh, un utilitaire en ligne de commande pour configurer et surveiller les paramètres d'ordinateur et de réseau, peut être utilisée pour gérer les ports de service. Cet utilitaire peut être utilisé pour ouvrir ou fermer un port de service particulier ou pour afficher une liste des ports ouverts sur votre ordinateur.
Pour ajouter une règle de pare-feu pour un port TCP spécifique, on utilise la commande suivante :
netsh advfirewall firewall add rule name="Nom de la règle" dir=in action=allow protocol=TCP localport=<numéro du port>
si le port est 80 en TCP et la règle est "HTTP" alors la commande présendante devient :
netsh advfirewall firewall add rule name="HTTP" dir=in action=allow protocol=TCP localport=80
supprimer une règle d'ouverture de port avec la syntaxe :
netsh advfirewall firewall delete rule name="HTTPS" protocol=TCP localport=443
Cette commande affiche toutes les règles du pare-feu, y compris le nom, l'action, le protocole et les ports locaux et distants.
netsh advfirewall firewall show rule name=all

1.7.3 Exemples sous Windows

Sous Windows, la commande netsh, un utilitaire en ligne de commande pour configurer et surveiller les paramètres d'ordinateur et de réseau, peut être utilisée pour gérer les ports de service. Cet utilitaire peut être utilisé pour ouvrir ou fermer un port de service particulier ou pour afficher une liste des ports ouverts sur votre ordinateur.

Pour ajouter une règle de pare-feu pour un port TCP spécifique, on utilise la commande suivante :

netsh advfirewall firewall add rule name="Nom de la règle" dir=in action=allow protocol=TCP localport=<numéro du port>

si le port est 80 en TCP et la règle est "HTTP" alors la commande présendante devient :

netsh advfirewall firewall add rule name="HTTP" dir=in action=allow protocol=TCP localport=80

supprimer une règle d'ouverture de port avec la syntaxe :

netsh advfirewall firewall delete rule name="HTTPS" protocol=TCP localport=443

Cette commande affiche toutes les règles du pare-feu, y compris le nom, l'action, le protocole et les ports locaux et distants.

netsh advfirewall firewall show rule name=all

1.8 Conclusion

En conclusion, le chapitre 1 introduit les concepts clés de l'administration des services réseaux, y compris les objectifs et le rôle de l'administration, les modèles d'administration réseau, les réseaux clients-serveurs, les protocoles d'administration, les services de la couche d'application et les ports de service.

Chapitre 2

Le Service SNMP (Simple Network Management Protocol)

2.1 Généralités

2.1.1 Approche pédagogique introductive

Si les composants d'un réseau (routeurs, switchs, serveurs...) sont répartis sur plusieurs sites, il est impératif de les inspecter régulièrement pour garantir leur bon fonctionnement. on parle de supervision où surveillance du réseau. la surveillance.
Pour se concentrer correctement, il est essentiel de surveiller les services (logiciels) et le matériel qui composent le réseau. La gestion des pannes est le résultat de la supervision, qui consiste à analyser et vérifier le fonctionnement des équipements et des services. Voici quelques commandes système pour accéder localement aux informations d'une machine :

netstat/ping/traceroute/nmap/iperf permettent de tester et de récolter des statistiques sur le réseau.
telnet/ssh valident l'accès à distance à une machine
uptime donne la charge du système sous Linux et **systeminfo** sous windows
free -h, df -h donne les statistiques sur la mémoire et le disque sous linux.
wmic logicaldisk get deviceid, freespace, size donne les statistiques sur le disque sous windows.

Problématique

Si l'on veut accéder à ces informations, il est nécessaire d'exécuter ces commandes individuellement sur une machine locale. Mais si le réseau est dispersé sur différents sites et avec un nombre important de machines dont chacune a son propre système d'exploitation (hétérogènes), il devient difficile d'obtenir ces informations.
La complexité et l'hétérogénéité plus la dispersion ⇒ Recherche de standards pour la supervision ⇒il faut trouver un protocole pour l'administration des réseaux
La solution trouvée est d'utiliser le protocole SNMP Simple Network Management Protocol

introduction du SNMP en administration réseau

Le protocole d'administration réseau SNMP (Simple Network Management Protocol) permet la supervision et la gestion des équipements réseau tels que les routeurs, les commutateurs, les imprimantes et les serveurs. Il permet aux administrateurs de surveiller en temps réel le fonctionnement et l'état de leur réseau. Il vise également à diagnostiquer le réseau et à résoudre rapidement les problèmes. Il est basé sur un serveur de supervision et un agent qui correspond aux équipements que les administrateurs souhaitent superviser. La base d'informations de gestion (MIB) est une structure de données utilisée par le SNMP pour stocker des informations sur les équipements réseau. Un outil de gestion SNMP permet aux administrateurs d'accéder à ces informations pour surveiller les performances, détecter les problèmes et effectuer des tâches administratives telles que la mise à jour des configurations et la configuration d'alertes. Les réseaux d'entreprise utilisent fréquemment le protocole SNMP pour surveiller les performances du réseau et détecter les problèmes de façon proactive. De plus, il peut être utilisé pour surveiller les équipements distants, ce qui en fait un outil utile pour les administrateurs de réseau. Grâce à ce protocole toutes les informations logicielles ou matérielles peuvent être lues, modifiées et reconfigurées. voir figure 2.1.
Une console de supervision (la station d'administration où la console de supervision) interroge les agents en envoyant une requête, qui est ensuite exécutée par un agent SNMP.

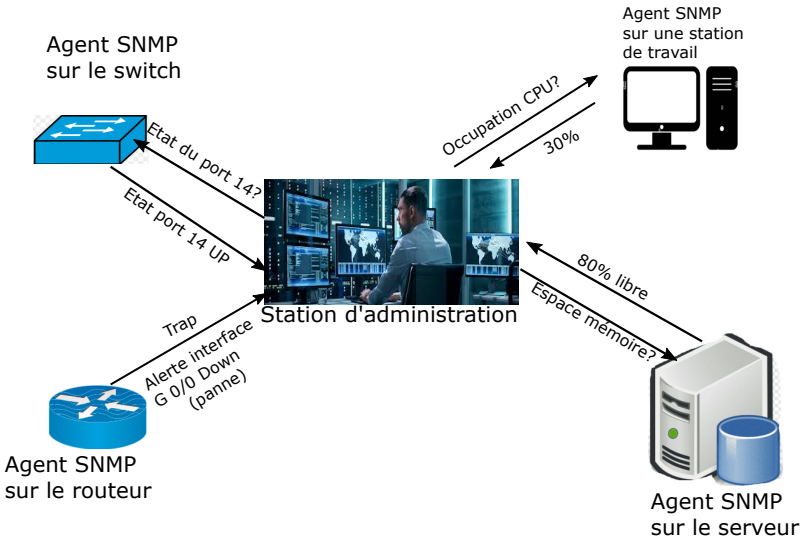


FIGURE 2.1 – Schéma de supervision utilisant le protocole SNMP

Un agent SNMP est programme (logiciel) qui s'exécute en arrière plan sur l'équipement. La supervision se fait sur tous les équipements à administrer.

2.1.2 Historique

La communauté informatique a créé SNMP (Simple Network Management Protocol) dans les années 1980 pour fournir une méthode standardisée de gestion des réseaux informatiques. Il a été initialement conçu pour les réseaux locaux (LAN), mais il a également été utilisé par les fabricants de matériel et de logiciels pour gérer les réseaux étendus (WAN) et les réseaux sans fil (WLAN). Depuis lors, SNMP est devenu l'un des protocoles de gestion de réseau les plus populaires, permettant aux administrateurs de réseau de surveiller et de gérer les équipements réseau tels que les routeurs, les commutateurs et les périphériques sans fil.
Même si la version SNMPv2c (RFC 1901 à 1908 ; http ://www.faqs.org/rfcs/) a été créée en 1990 et est actuellement la plus utilisée, il existe deux autres versions : SNMPv1 (RFC 1155 à 1157) en 1996 et SNMPv3 (RFC 2571 à 2575 et 3411 à 3413) en 1999. Il convient de noter que la version 3 est considérée comme la plus sure des trois.

2.2 Le protocole SNMP

2.2.1 Protocole SNMP rôle et fonctionnalités

Il permet aux administrateurs, depuis un poste de contrôle central, de gérer les équipements réseau et de diagnostiquer les problèmes très rapidement. Il fonctionne avec un serveur de supervision et des agents que les administrateurs supervisent (Switch, Router, Firewall, PC etc). Il est possible de modifier divers éléments de configuration d'équipements actifs et de logiciels et même des services de l'équipement. Les appareils compatibles SNMP utilisent les informations stockées dans la MIB, peuvent être supervisées.

2.2.2 Format de message des protocoles SNMPv1 SNMPv2

Il est donné par la figure (2.2).

- ▷ Le champ **version number** indique la version (0 pour SNMPv1 et 1 pour SNMPv2).
- ▷ Le champ **Community string** est le mots de passe qui est transmis en clair sur le réseau, il défini le droit d'un utilisateur sur une branche de la MIB (MIB views) ce qui rend ces deux versions non sécurisées.
- ▷ Le champ variable bindings : name1 et value1 constitue l'OID1 : value1, de même pour le reste de la trame.

Les primitives **GetRequest**, **GetResponse** et **SetRequest** utilisent la même structure de données. Les primitives **Get**, **GetNextRequest**, **GetRequest** et **GetBull** (SNMPv2) permettent sous l'initiative de la station d'administration NMS (Network Station Management) de lire les valeurs des objets de la MIB. **GetNextRequest** : récupère les valeurs des objets qui suivent dans l'ordre lexicographique de l'arbre de nommage. C'est une primitive qui permet de faire des appels récursifs.
La version 2 introduit la primitive **GetBulk** qui limite le nombre de variables retournées (maximum de répétition. Ainsi **GetBulkRequest** réalise la recherche d'un groupe de variables. **Set** fixe une valeur un objet.

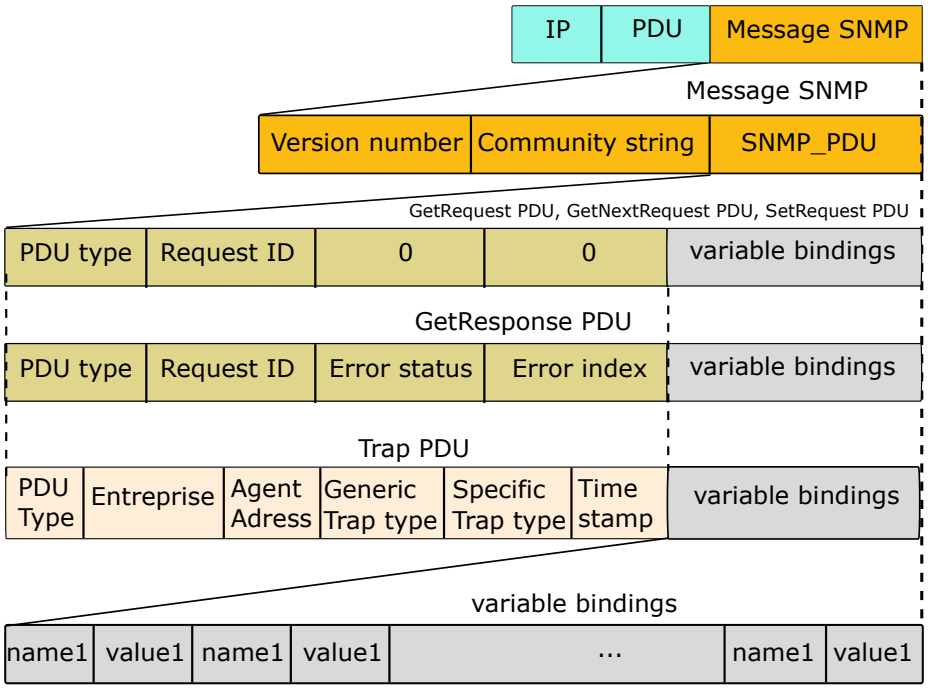


FIGURE 2.2 – Format d'un message (paquet) SNMP

Ces primitives sont acquittées par la primitive **GetResponse**. Les primitives de type ***Event*** (**Trap** et **Trap-SNMPv2**) sont émises par l'agent à destination de la station administrative sur condition d'alerte, et elles ne sont pas acquittées voir figure (2.5).
Le format de message des protocoles SNMP v1 et v2 détaillé
Header : Le header d'un message SNMP commence toujours par la même séquence d'octets, appelée "SNMP Version Identifier". Cette séquence indique la version du protocole SNMP utilisée (par exemple, 0x00 pour SNMPv1 et 0x01 pour SNMPv2c). Le header comprend également les champs suivants :

1. Community String : Cette chaine de caractères est utilisée pour authentifier l'utilisateur ou l'application émettant la requête SNMP. Elle est généralement définie par l'administrateur réseau ou l'utilisateur, et peut être utilisée pour restreindre l'accès aux informations dans la MIB.
2. Request ID : Il s'agit d'un numéro unique qui identifie la requête SNMP. Ce numéro est généré par l'application émettant la requête et est utilisé pour faire correspondre les réponses aux requêtes correspondantes.
3. Error Status : Ce champ indique si une erreur s'est produite lors du traitement de la requête. Si la requête a été traitée avec succès, ce champ est généralement défini à zéro. Si une erreur s'est produite, ce champ contient un code d'erreur spécifique (par exemple, 1 pour "tooBig" ou 2 pour "noSuchName").
4. Error Index : Ce champ est utilisé pour indiquer l'objet dans la requête qui a causé l'erreur. Si aucun objet n'a causé l'erreur, ce champ est défini à zéro.

PDU : Le PDU (Protocol Data Unit) est la partie du message SNMP qui contient les données spécifiques de la requête ou de la réponse. Il existe plusieurs types de PDU, notamment :

1. GetRequest : Ce type de PDU est utilisé pour récupérer des informations sur un ou plusieurs objets de la MIB. Le PDU GetRequest contient une liste d'OIDs correspondant aux objets que l'on souhaite interroger.
2. GetNextRequest : Ce type de PDU est utilisé pour récupérer des informations sur le prochain objet dans la MIB après celui spécifié. Le PDU GetNextRequest contient une liste d'OIDs correspondant aux objets à interroger.
3. SetRequest : Ce type de PDU est utilisé pour modifier la valeur d'un ou plusieurs objets de la MIB. Le PDU SetRequest contient une liste de paires OID/valeur correspondant aux objets que l'on souhaite modifier.
4. Response : Ce type de PDU est utilisé pour renvoyer des informations demandées dans une requête SNMP. Le PDU Response contient une liste d'OIDs correspondant aux objets renvoyés, ainsi que leurs valeurs associées.

Objets : Les objets SNMP sont identifiés par un Object Identifier (OID) unique, qui est une chaine d'entiers codés en binaire. Les valeurs associées à ces OID peuvent être des données de type simple, telles que des entiers

ou des chaines de caractères, ou des données de type composé, telles que des tables de données. Les objets sont stockés dans la MIB (Management Information Base), qui est une base de données hiérarchique des informations de gestion du réseau.

2.2.3 Les nouveautés de la SNMPv2

- ▷ L'entité SNMPv2 peut être à la fois manager et agent, ce qui est une nouveauté en soit.
- ▷ Introduction de la primitive **inform** qui permet le dialogue manager à manager.
- ▷ Modélisation des objets améliorée, cependant elle reste proche de la v1.
- ▷ Rajout de la primitive **GetBulk.**
- ▷ Les messages de types Trap améliorés à snmpv2_Trap).
- ▷ Authentification par message digest (MD5) introduisant une sécurité relative et cryptographie par DES des messages SNMP en plus de la synchronisation des horloges.

2.2.4 Les nouveautés de la SNMPv3

La version 3.0 améliore la sécurité et les fonctions administratives (authentification, intégrité et confidentialité des données). Les modèles serveur/client de la v1 et v2 sont transposés en modèles ***Peer to Peer*** (égal à égal). Elle remplace la différentiation agent/manager par l'entité SNMP plus générale (***snmpentity***).
SNMPv3 (Simple Network Management Protocol version 3) est la version la plus récente du protocole SNMP. Elle introduit plusieurs fonctionnalités de sécurité qui n'existent pas dans les versions précédentes de SNMP. Voici quelques-unes des nouveautés avec SNMPv3 :

1. Authentification et confidentialité : SNMPv3 prend en charge l'authentification et la confidentialité des messages SNMP en utilisant des algorithmes de chiffrement tels que MD5, SHA-1 et AES.
2. Sécurité basée sur les rôles : SNMPv3 permet aux administrateurs de définir des rôles et des niveaux d'accès pour les utilisateurs afin de restreindre l'accès aux informations sensibles de la MIB.
3. Support de l'IPv6 : SNMPv3 prend en charge IPv6, le nouveau protocole de couche réseau, qui permet une plus grande sécurité et une gestion plus efficace des adresses IP.
4. Authentification de l'utilisateur : SNMPv3 permet l'authentification de l'utilisateur à l'aide de différents mécanismes tels que les mots de passe et les certificats numériques.
5. Notifications trap sécurisées : SNMPv3 prend en charge les notifications trap sécurisées pour garantir que les messages de notification ne sont pas modifiés ou falsifiés.

Les fonctionnalités d'authentification pour la gestion de réseau, ce qui est important pour les entreprises et les organisations qui gèrent des réseaux complexes et sensibles.
Voici un exemple de commande SNMPv3 utilisant l'outil de ligne de commande snmpwalk pour récupérer les informations système d'un appareil distant :

```
snmpwalk -v3 -u myuser -l authPriv -a MD5 -A myauthpass -x DES -X myprivpass 192.168.1.1 system
```

Dans cet exemple, nous utilisons l'option "-v3" pour indiquer que nous utilisons SNMPv3. L'option "-u" spécifie le nom d'utilisateur, "-l" spécifie le niveau de sécurité (authPriv signifie que nous utilisons à la fois l'authentification et la confidentialité), "-a" spécifie l'algorithme d'authentification (MD5 dans cet exemple), "-A" spécifie le mot de passe d'authentification, "-x" spécifie l'algorithme de chiffrement (DES dans cet exemple) et "-X" spécifie le mot de passe de chiffrement.
Enfin, nous spécifions l'adresse IP de l'appareil distant et l'OID (dans ce cas, "system") pour récupérer les informations système. Ce type de commande peut être utilisé pour récupérer différentes informations SNMPv3 d'un appareil, selon les autorisations de l'utilisateur.

2.3 Comparaison SNMP et ISO

La méthode collecte des informations est la principale différence entre **SNMP** et **ISO**. Le polling (sollicitation) est la technique d'interrogation d'un objet à la fois dans le **SNMPv1** ce qui ne permettait pas de gérer les réseaux vastes. Ceci a été corrigé dans la **v2** de **SNMP** avec la fonction **BDT** (Bulk Data Transfert) qui autorise l'interrogation de plusieurs objets. Afin de limiter le dialogue **WAN** un proxy agent à été rajouté. Ainsi le dialogue SNMP se fait entre le **proxy agent** et l'organe administré, de plus, le proxy agent ne transmet que les alertes au manager. Par ailleurs, les tables de routage sur la **MIB I** circule en clair rendant la sécurité inexistante. Les correctifs apportés en **MIB II** ont permis de palier au problème.
Les grands réseaux utilisent le protocole CMIS/CMIP d'ISO malgré qu'il prend beaucoup de ressources. Aussi, les systèmes administrés n'implémentent que des agents SNMP. Par conséquent, le protocole CMIP à été simplifié par celui dit **CMOT** (CMIP over TCP/IP) afin d'utiliser les agents SNMP des réseaux **TCP/IP** dans le environnements de gestion ISO. L'interfaçage entre modèle **TCP/IP** et le modèle **ISO** à été réalisé à travers une couche de présentation nommée **LPP** (Lightweight Presentation Protocol) définie juste au dessus d'UDP.

2.4 L'administration dans l'environnement TCP/IP et protocole SNMP

2.4.1 Principes généraux et état de l'art (Normes et RFC)

Le protocole SNMP (Simple Network Management Protocol) est l'un des standards de gestion des réseaux TCP/IP, présenté dans la figure 2.3, qui n'est pas orienté objet (il n'y an aucune distinction entre attributs et objets) mais est proche de l'ISO. Il a été créé à partir du protocole de surveillance des passerelles IP SGMP (Simple Gateway Monitoring Protocol, RFC 1028), qui est détaillé dans la RFC (1157) et complété par :

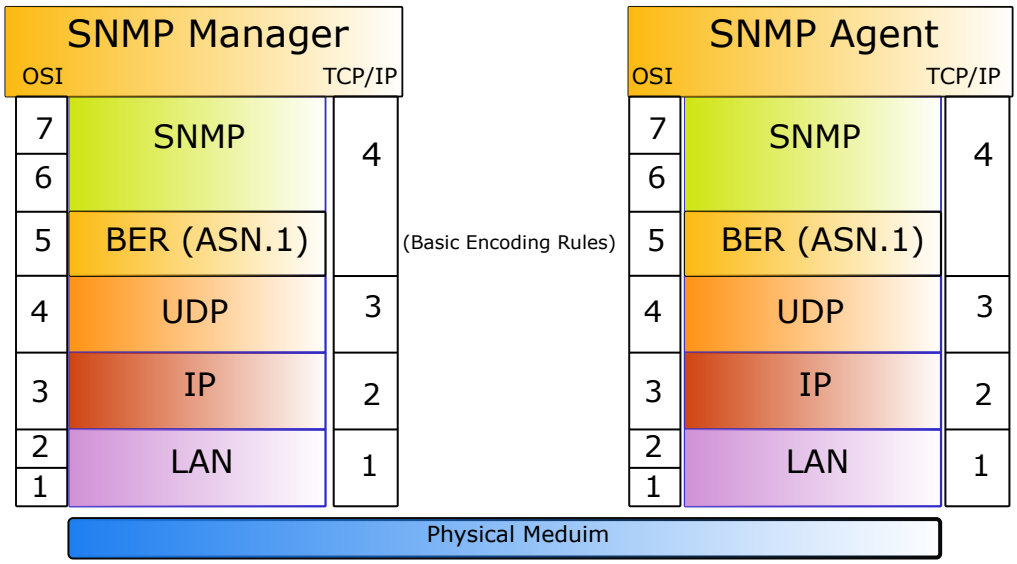


FIGURE 2.3 – Architecture Protocolaire SNMP

- La RFC 1155 : spécifie la représentation des objets dans la base d'informations SMI (Structure Management Information) qui utilise la notation ASN1 (Abstract Syntax Notation 1). ASN.1 est un standard international spécifiant une notation destinée à décrire des structures de données [http ://www.faqs.org/rfcs/].
- Les RFC1152 et 1213 (MIB I et MIB II) fournissent des descriptions des objets gérés (attributs ISO). La RMON MIB (Remote Monitor Network MIB) est spécifiée pour les réseaux Ethernet et Token Ring locaux et est mise en œuvre dans des sondes d'analyse et de surveillance. Les RMON n'ont accès qu'aux segments de leur environnement commuté. Pour permettre l'accès aux différents éléments des réseaux commutés, une sonde spécifique SMON (Switched RMON, RFC 2613) a été définie.

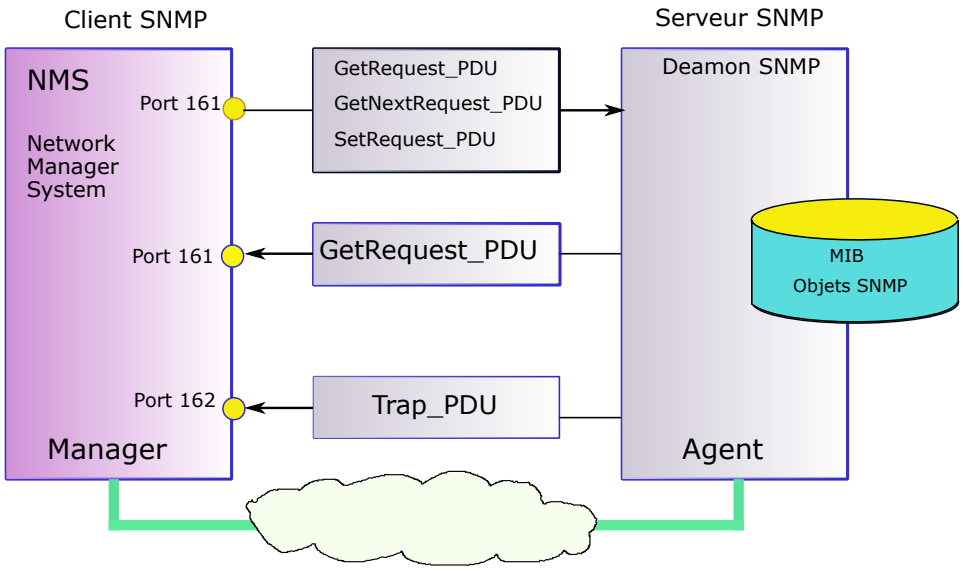


FIGURE 2.4 – Les échanges SNMP

2.4.2 Protocole d'échange SNMP

Il s'agit d'un mode non connecté qui utilise UDP (User Datagram Protocol) pour définir les interactions entre la station d'administration et l'agent, comme illustré dans la figure 2.4. Les avantages du choix UDP sont les suivants :

- ▷ Résistance aux défaillances des réseaux.
- ▷ Meilleures performances.
- ▷ Implémentation simple puisqu'il n'y a pas de connexion à gérer.

Remarque

Les alarmes (Trap) ne sont pas confirmées car le mode non connecté permet une meilleure résistance aux défaillances et une grande rapidité lors des échanges par rapport au mode connecté.

Exemple

Pour lire la valeur d'un objet administré (variable) SNMP utilise les attributs ISO : **GetRequest** et **GetNextRequest** pour faire respectivement de la cherche de la variable et de la suivante.
La commande "**GetRequest**" est utilisée pour récupérer une valeur unique d'un objet de gestion SNMP. Par exemple, si vous voulez récupérer la valeur de l'objet de gestion sysDescr qui contient une description textuelle de la plate-forme matérielle et du système d'exploitation, vous pouvez utiliser la commande suivante :

snmpget -v2c -c community_string agent_IP_address sysDescr.0

Cette commande récupère la valeur de l'objet **sysDescr** avec l'OID 1.3.6.1.2.1.1.1.0 qui se trouve à l'index 0. "community_string" sera remplacé par la communauté SNMP que vous avez configurée sur votre agent SNMP et "agent_IP_address" par l'adresse IP de l'agent SNMP.
un autre exemple de commande "**snmpwalk**" (qui utilise GetNextRequest) pour récupérer les valeurs de tous les objets de gestion dans la MIB à partir de la racine :

snmpwalk -v2c -c community_string agent_IP_address

Cette commande utilise la version 2c du protocole SNMP avec la communauté "community_string" et l'adresse IP de l'agent SNMP "agent_IP_address". Le point "." spécifie la racine de la MIB, ce qui signifie que toutes les valeurs de tous les objets de gestion dans la MIB seront récupérées. Les résultats de la commande "snmpwalk" sont affichés dans la console, généralement sous la forme d'une liste hiérarchique d'OID et de leurs valeurs associées.
Pour modifier la valeur d'un objet (d'une variable) **SetRequest** est utilisée.

snmpset -v2c -c community_string agent_IP_address sysContact.0 s "nouvelle_valeur"

ou bien

snmpset -v2c -c community_string agent_IP_address 1.3.6.1.2.1.1.4.0 s "nouvelle_valeur"

Cette commande modifie la valeur de l'objet **sysContact** avec l'**OID 1.3.6.1.2.1.1.4.0** qui se trouve à l'**index 0**. La lettre "s" après l'OID indique que la valeur est une chaine de caractères. "**community_string**" sera remplacé par la communauté SNMP que vous avez configurée sur votre agent SNMP et "**agent_IP_address**" par l'adresse IP de l'agent SNMP. la "**nouvelle_valeur**" sera remplacée par la nouvelle valeur configurée pour l'objet sysContact.
La réponse de l'agent administré est **GetResponse**.
Le message Trap est émis sur l'initiative de l'agent, informant l'administrateur qu'une condition d'alarme a été détectée. La figure (2.5) représente le dialogue entre le manager et l'agent.

2.4.3 Les MIB (Manager Information Base)

Description des objets

Les objets gérés sont décrit par les MIB qui définit :

1. Le nommage.
2. Le type.
3. Le format.
4. Les actions.

A la demande du manager, l'agent vient consulter les différentes valeurs des objets, qui ne sont pas contenues dans la MIB mais plutôt dans des registres externes. La structure de définition des objets est formalisée par la RFC 1213 (MIB II).

Exemple
description formelle d'un objet selon la MIB II
OBJET_TYPE.MACRO : :=

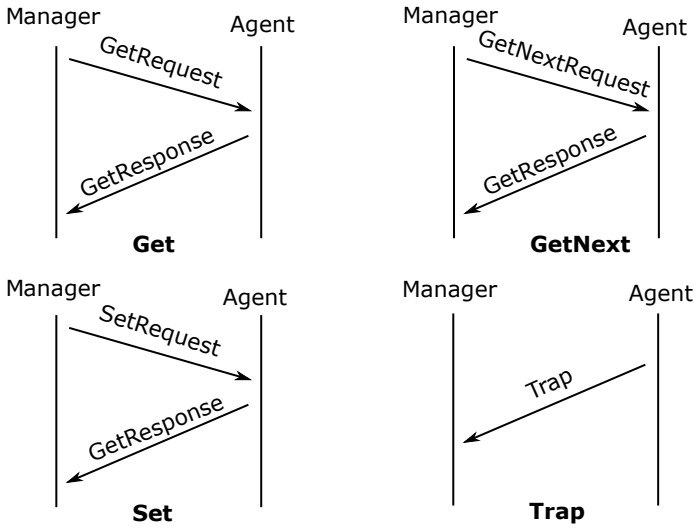


FIGURE 2.5 – Les attributs ISO SNMP

BEGIN
TYPE NOTATION : :=
"SYNTAX" type (TYPE ObjetSyntax)
"ACCESS" Access
"STATUS" Status
VALUE NOTATION : :=value (VALUE ObjectName)
DESCRIPTION value (description DisplayString) | empty
Access : :="read_only" | "write_only" | "not_accessible"
Status : :="madatory" | "optional" | "obsolete" | "deprecated"
DisplayString : := OCTET STRING SIZE (0..255)
END

Explication du code précédant. Il s'agit d'un formalisme qui décrit les propriétés d'un objet SNMP, telles que sa syntaxe, son accès, son statut et sa description.
Voici ce que signifie chaque élément de cette définition :
OBJET_TYPE.MACRO : := : Cette ligne indique que nous allons définir un nouvel objet SNMP.
TYPE NOTATION : := : Cette ligne indique que nous allons définir un type de notation.
"SYNTAX" type (TYPE ObjetSyntax) : Cette ligne définit la syntaxe de l'objet SNMP. Elle spécifie le type de données qui peut être utilisé pour stocker la valeur de l'objet.
"ACCESS" Access : Cette ligne spécifie l'accès à l'objet SNMP. L'attribut Access peut être "read_only" pour un objet en lecture seule, "write_only" pour un objet en écriture seule ou "not_accessible" pour un objet qui ne peut pas être accédé.
"STATUS" Status : Cette ligne spécifie le statut de l'objet SNMP. L'attribut Status peut être "mandatory" pour un objet obligatoire, "optional" pour un objet optionnel, "obsolete" pour un objet qui n'est plus pris en charge ou "deprecated" pour un objet qui est déconseillé.
VALUE NOTATION : :=value (VALUE ObjectName) : Cette ligne définit une valeur pour l'objet SNMP. Elle spécifie le nom de l'objet et sa valeur par défaut.
DESCRIPTION value (description DisplayString) | empty : Cette ligne décrit l'objet SNMP. Elle fournit une description textuelle de l'objet SNMP qui peut aider à comprendre son but et son fonctionnement. L'attribut DisplayString est une chaine de caractères de taille maximale 255 octets.
En résumé, cette définition d'objet SNMP décrit les caractéristiques de l'objet, telles que sa syntaxe, son accès, son statut et sa description, et fournit une valeur par défaut pour l'objet. Cette définition est utilisée pour aider à gérer et surveiller les appareils et les systèmes sur un réseau en utilisant le protocole SNMP.

Détails de l'objet SysUpTime

SysUpTime est un objet de type TimeTicks qui mesure le temps (centième de seconde) depuis que l'agent à été réinitialisé. C'est un type de variable définit dans la SMI et il est accessible uniquement en lecture (read only). C'est un objet obligatoire (Mandatory) qui est classé troisième objet décrit dans la MIB système. Sa description (objet MIB II) est donnée comme suit :

SysUpTime OBJET_TYPE
Syntax TimeTicks
Access read_only
Status mandatory
Description "The Time (in handreths of second) since the network management portion of system was last reinitialized"

: :={system 3}
Voici ce que signifie chaque élément de cette définition :
SysUpTime OBJET_TYPE : Cette ligne définit le nom de l'objet SNMP que nous allons décrire.
Syntax TimeTicks : Cette ligne spécifie la syntaxe de l'objet SNMP. Dans ce cas, il s'agit d'un type de données appelé "TimeTicks", qui stocke le temps en centièmes de seconde.
Access read_only : Cette ligne spécifie que l'objet SNMP est en lecture seule. Cela signifie que sa valeur ne peut pas être modifiée via le protocole SNMP.
Status mandatory : Cette ligne spécifie que l'objet SNMP est obligatoire. Cela signifie qu'il doit être présent dans tout système conforme à cette définition.
Description "The Time (in handreths of second) since the network management portion of system was last reinitialized" : Cette ligne fournit une description textuelle de l'objet SNMP. Dans ce cas, il décrit le temps écoulé depuis la dernière réinitialisation de la partie de gestion du système.
: :={system 3} : Cette ligne définit l'emplacement de l'objet SNMP dans l'arborescence du MIB (Management Information Base). Dans ce cas, l'objet est situé sous l'objet "system" et a l'identificateur 3. Cela signifie que l'objet peut être référencé par l'OID (Object Identifier) 1.3.6.1.2.1.1.3 dans le protocole SNMP.
En résumé, cette définition d'objet SNMP décrit le temps écoulé depuis la dernière réinitialisation de la partie de gestion du système. Elle fournit également une description textuelle de l'objet et le place dans l'arborescence du MIB pour qu'il puisse être référencé par les applications SNMP.

Nommage des objets

Les objets gérés par la MIB sont désignés par l'ISO selon une hiérarchie en arbre dit ***arbre de nommage.*** Sur la figure 2.6 , chaque organisation de normalisation possède une entité au premier niveau. Les différentes branches permettent de nommer un objet de manière unique. L'IETF (Internet Engeneering Task Force), établit les MIB standards pour qu'elle appartiennent à la branche "internet" et sont classés dans la branche mgmt(2). Ainsi l'objet SysUpTime de la figure 2.6, est désigné en format texte par iso.org.dod.internet.mgmt-2.system.sysuptime. En format numérique le même objet peut être lu de la racine "Root" l'objet : le nombre 1.3.6.1.2.1.1.3. Cette suite d'entiers séparée par un ".", désigne de manière unique (non ambigüe) un objet SNMP et l'OID de l'objet.

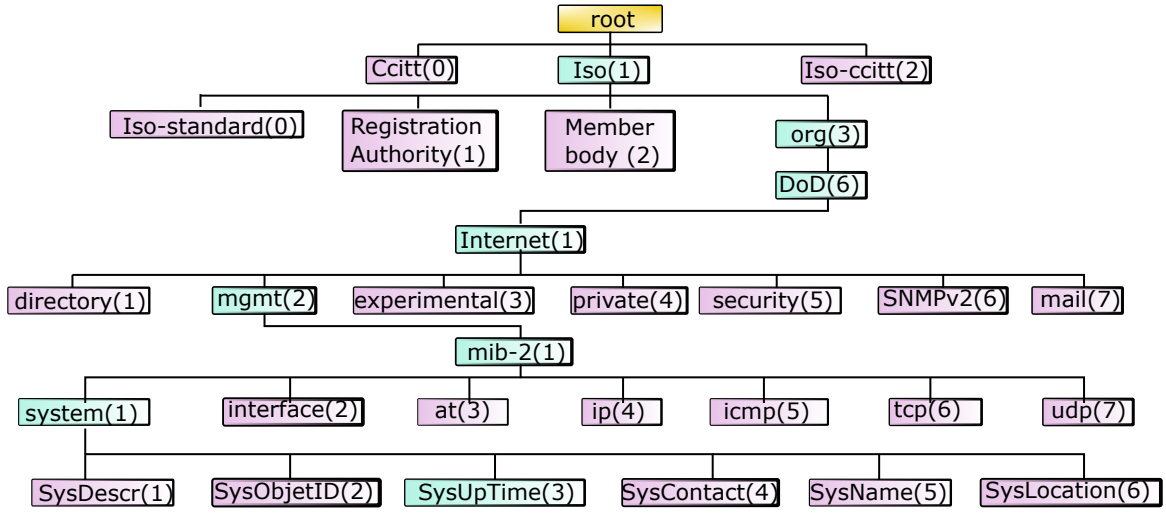


FIGURE 2.6 – Arbre de nommage des objets SNMP

Le fichier MIB

L'arbre de la MIB hiérarchisé contient des informations et chaque portion de l'arbre est décrite par un fichier MIB particulier. Le fichier MIB est de format texte qui contient la spécification de différents OID. Il est écrit en utilisant la syntaxe SMI (Structure of Management Information). Elle est basée sur ASN1. Pour chaque OID, cette spécification comprend (voir exemple 2.4.3) :

- ▷ Un OID unique, dans l'arbre des OID. Par exemple 1.3.6.1.2.1.1.3 ;
- ▷ Un nom générique. Par exemple sysUpTime.
- ▷ Une description de cet OID. Par exemple, "The time (in hundredths of a second) since the network management portion of the system was last re-initialized".
- ▷ Son type. Par exemple TimeTicks. Il existe différents types possibles de données qui permettent de couvrir tous les besoins.
- ▷ Son statut. Par exemple mandatory. Les différents statuts possibles sont "mandatory", "optional", "obsolete".

▷ Son mode d'accès. Par exemple read-only. Les différents accès sont "read-only", "read-write", "write-only", "not-accessible".

Les MIB privées

Malgré l'extension de la RMON MIB et que la MIB I et la MIB II contiennent respectivement 114 et 170 objets, les constructeurs ont constitué des MIB privées qui découlent de la branche private (4).

Exemple

La MIB IBM contient 600 objets figure (2.7) et l'accès aux variables de celles-ci est assuré par un agent spécifique qui effectue le connexions nécessaire dit **Proxy-agent**.

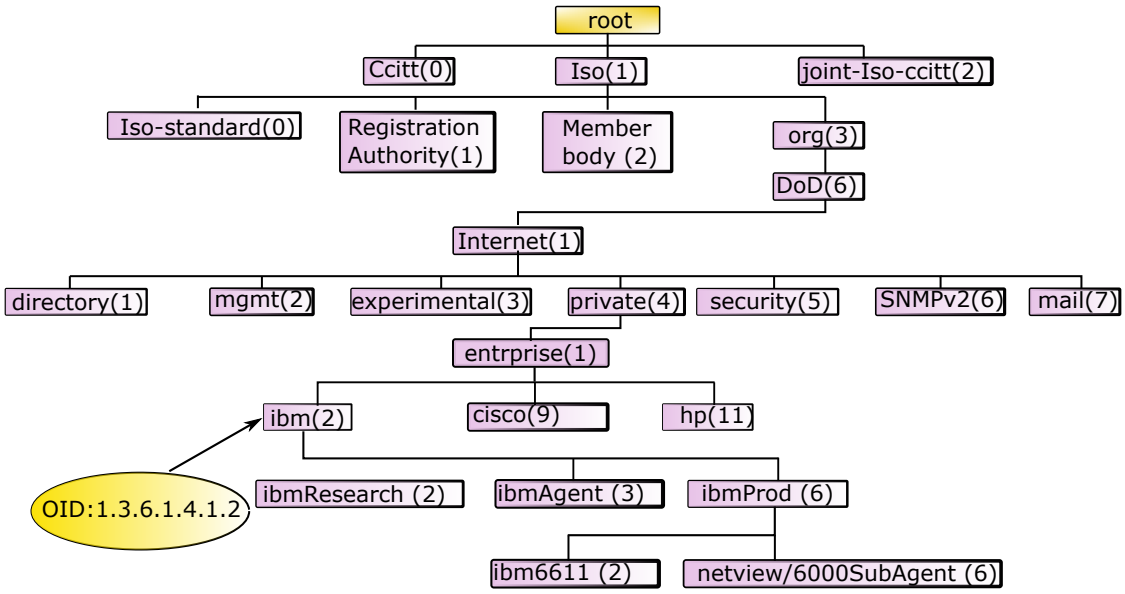


FIGURE 2.7 – Extrait de la branche private de la MIB IBM

Le Proxy-Agent

Le principe du proxy-agent est donné en figure 2.8, il permet le dialogue de deux systèmes d'administration différents. Il peut être localisé dans le serveur pour l'utilisation d'une MIB privée ou dans le nommage si l'agent serveur n'est pas conforme au standard (conversion de protocole). Le proxy agent reçoit les demandes des clients et les transmet aux serveurs appropriés, puis renvoie les réponses des serveurs aux clients. Il peut également être utilisé pour filtrer les demandes ou pour fournir une couche de sécurité supplémentaire en limitant les types de demandes qui peuvent être traitées ou en fournissant une authentification supplémentaire pour les demandes de service.

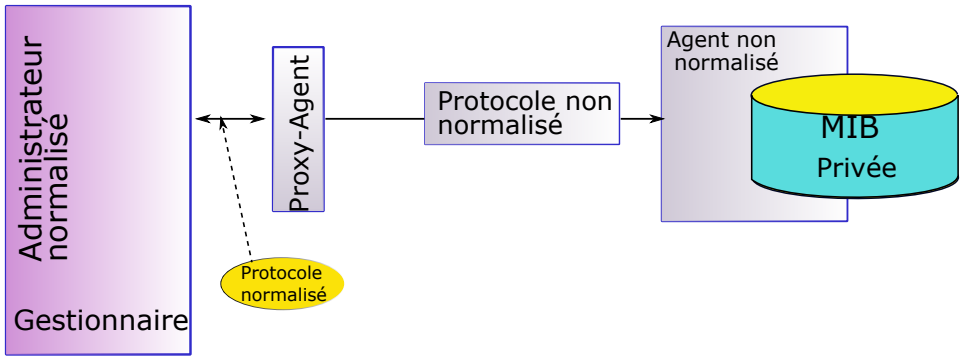


FIGURE 2.8 – Utilité d'un proxy-agent

L'utilisation d'un proxy agent est par exemple lorsque vous utilisez un serveur mandataire pour accéder à Internet à partir d'un réseau d'entreprise. Dans ce cas, le serveur de proxy sert d'intermédiaire entre votre ordinateur et les serveurs web externes auxquels vous souhaitez accéder. En ajoutant des fonctionnalités telles que la gestion du cache, la limitation de bande passante et la sécurité du réseau, le serveur de proxy peut filtrer et contrôler les demandes de l'utilisateur.

Définitions : ASN1 :BER et règle de codage

ASN.1 (Abstract Syntax Notation One) est un langage de description de données formellement défini par l'UIT-T (Union internationale des télécommunications - secteur des normes de télécommunication). Il est utilisé pour décrire la structure des données dans les communications entre systèmes.
BER (Basic Encoding Rules) est l'un des schémas de codage ASN.1. Il est utilisé pour encoder les données en un format binaire compact. BER définit les règles de base pour l'encodage des types de données ASN.1 en une séquence d'octets.
La méthode de codage BER utilise une structure hiérarchique de type arborescent appelée PDU (Protocol Data Unit), qui est une représentation binaire de la structure de données ASN.1. Les données sont codées dans l'ordre hiérarchique, du plus général au plus spécifique.
L'avantage de la codification BER est qu'elle permet la représentation de données complexes dans un format binaire compact, tout en garantissant une interopérabilité entre différents systèmes, car les règles de codage sont normalisées et bien définies.

Les règles de codage de la ASN1 :BER

Chaque élément est représenté par un triplet (type, longueur, valeur) Le type indique la signification sémantique de l'élément et est codé sur un octet La longueur indique la taille de la valeur de l'élément et est codée sur un ou plusieurs octets La valeur est le contenu de l'élément et est codée selon le type de l'élément et sa longueur Les éléments sont encodés en ordre séquentiel, en commençant par le premier élément et en continuant jusqu'au dernier Les éléments sont encodés dans un format binaire, où chaque bit représente un 0 ou un 1 Les éléments sont encodés de manière à être indépendants du système d'exploitation et du matériel Le codage ASN1 :BER est utilisé dans de nombreux protocoles de communication, notamment **SNMP** (Simple Network Management Protocol), **LDAP** (Lightweight Directory Access Protocol) et **X.509** (standard de cryptographie pour les certificats numériques).

La représentation codée des objets

L'objet sollicité est identifié par des requêtes SNMP. C'est la ASN1 :BER (Basic Encoding Rules) qui code le **type**, la **longueur du champ** et **la valeur** de l'OID (Object IDentifier) selon des règles stricts de codage.

- ▷ La nature de l'étiquette de l'objet est identifiée par les deux premiers bits : 00 **universal**, 01 **application**, 10 **context** et 11 **private**.
- ▷ Le type est désigné par le $3^{ème}$ bit il distingue un type **primitif** d'un type **construit** à savoir : 0 pour primitif et 1 pour construit.
- ▷ La variable est désignée par les cinq bits suivants.
- ▷ Les sous-ensembles de désignation des types de SNMP est donné par le tableau 2.1.

ID	Types primitifs	Signification
2	INTEGER	entier de taille arbitraire, utilisable pour définir des types énumérés
4	OCTET SPRING	Liste d'octets (valeur 0 à 255)
5	NULL (NIL)	Objet sans type, peut être utilisé pour finir une liste
6	OBJECT IDENTIFIER	Identifie l'objet dans l'arbre de nommage
16	SEQUENCE	Autorise la contruction de types complexes

Table 2.1 – Types UNIVERSAL d'ASN1 utilisé par SNMP

Il y a des règles particulières auxquelles est soumis le codage des deux premiers octets de l'OID. En effet, le 1^{er} octet ne prend que les valeurs de 1 à 3 (UIT à jonction UIT-ISO) et le second est toujours inférieur à 40. Par conséquent, les deux premiers entiers sont codés sur un seul octet : $(A \cdot 40 + B)$ avec A est le 1^{er} octet et B est le second. L'objet sysUpTime de l'exemple 2.4.3 est codé suivant le tableau 2.2 il est de type TimeTicks qui est un type de données dans SNMP qui représente le temps écoulé depuis un événement de référence spécifique, tel que le démarrage d'un périphérique. Cela permet aux gestionnaires de réseau de surveiller l'état des périphériques et de diagnostiquer les problèmes en surveillant les changements dans les valeurs de TimeTicks.

Type	Longueur	Valeur	
OBJECT IDENTIFIER	6	$(1 \cdot 40 + 3)$,6,1,2,1,1,3	Décimal
0×06	0×7	$0 \times 2B$ 0×06 0×01 0×02 0×01 0×01 0×03	Hexadécimal

Table 2.2 – Codage de l'objet sysUpTime

2.5 Les hyperviseurs

Un hyperviseur est un logiciel qui permet la virtualisation des ressources d'un ordinateur, telles que la mémoire, les processeurs et les entrées/sorties. Il agit comme une couche intermédiaire entre le matériel d'un ordinateur et les systèmes d'exploitation invités. Cela permet à plusieurs systèmes d'exploitation d'être exécutés en parallèle sur le même matériel, offrant ainsi une meilleure utilisation des ressources et une plus grande flexibilité.

2.5.1 Principe

Le principe de fonctionnement d'un hyperviseur est de fournir une abstraction du matériel informatique pour les systèmes d'exploitation invités. Il s'agit d'une couche intermédiaire qui gère les ressources du système physique et les affecte aux différents systèmes d'exploitation virtuels qui tournent sur le même matériel. Chaque système d'exploitation invité pense avoir accès à l'intégralité des ressources du système physique, mais en réalité, c'est l'hyperviseur qui contrôle et attribue ces ressources en temps réel en fonction des besoins de chaque système d'exploitation. Le but est d'optimiser l'utilisation des ressources et de permettre à plusieurs systèmes d'exploitation de coexister sur le même matériel en toute sécurité.
Voici les hyperviseurs les plus connus :

- ▷ 1. VMware vSphere
- ▷ 2. Microsoft Hyper-V
- ▷ 3. Citrix XenServer
- ▷ 4. Red Hat Enterprise Virtualization (RHEV)
- ▷ 5. Oracle VM VirtualBox
- ▷ 6. KVM (Kernel-based Virtual Machine)
- ▷ 7. Proxmox VE
- ▷ 8. Nutanix Acropolis Hypervisor (AHV)

Ces hyperviseurs sont utilisés dans différents environnements, des centres de données aux petits environnements de test et développement, en passant par les environnements cloud publics et privés. Chacun a ses propres fonctionnalités, avantages et coûts pour s'adapter aux différents besoins des utilisateurs.

2.5.2 Microsoft Hyper-V

C'est un hyperviseur de type 1 développé par Microsoft. Il permet de créer et de gérer des machines virtuelles sur des ordinateurs exécutant le système d'exploitation Windows. Les fonctionnalités de Hyper-V incluent :

- ▷ 1. Création et gestion de machines virtuelles : Hyper-V permet de créer et de gérer des machines virtuelles, avec des options de configuration de la mémoire, du stockage et des réseaux pour chaque machine virtuelle.
- ▷ 2. Virtualisation de la mémoire et des processeurs : Hyper-V offre une virtualisation complète de la mémoire et des processeurs, ce qui permet aux machines virtuelles d'être isolées les unes des autres et de fonctionner en toute sécurité sur le même matériel.
- ▷ 3. Stockage en réseau : Hyper-V prend en charge la virtualisation du stockage en réseau, ce qui permet aux machines virtuelles d'accéder à des disques partagés sur un réseau.
- ▷ 4. Live Migration : Hyper-V permet de déplacer des machines virtuelles d'un ordinateur à un autre sans interrompre leur fonctionnement.
- ▷ 5. Protection de la vie privée : Hyper-V inclut des fonctionnalités de protection de la vie privée pour les machines virtuelles, telles que la création de machines virtuelles protégées pour les applications sensibles.

Microsoft Hyper-V est un outil puissant pour la virtualisation des ordinateurs et des systèmes d'exploitation. Il offre une virtualisation complète des ressources et une gestion simplifiée des machines virtuelles pour les environnements d'entreprise et de développement.

Le mécanisme de fonctionnement de Microsoft Hyper-V

Il repose sur la virtualisation des ressources matérielles de l'ordinateur, telles que la mémoire, les processeurs et les entrées/sorties. Il utilise une couche intermédiaire appelée "hyperviseur" qui gère les ressources du système physique et les affecte aux différentes machines virtuelles en cours d'exécution. Voici les étapes principales du mécanisme de fonctionnement de Hyper-V :

- ▷ 1. Installation de Hyper-V : L'installation de Hyper-V se fait sur un ordinateur exécutant Windows. Une fois installé, il peut être utilisé pour créer et gérer des machines virtuelles.
- ▷ 2. Création de machines virtuelles : Hyper-V permet de créer des machines virtuelles en spécifiant la configuration de la mémoire, du stockage et des réseaux pour chaque machine virtuelle.
- ▷ 3. Affectation des ressources matérielles : L'hyperviseur affecte les ressources matérielles, telles que la mémoire et les processeurs, aux différentes machines virtuelles en fonction de leurs besoins en temps réel.

- ▷ 4. Exécution des systèmes d'exploitation invités : Les systèmes d'exploitation invités sont installés sur les machines virtuelles et exécutés par Hyper-V. Chaque système d'exploitation invité pense avoir accès à l'intégralité des ressources du système physique, mais en réalité, c'est l'hyperviseur qui contrôle et attribue ces ressources.
- ▷ 5. Gestion des machines virtuelles : Hyper-V permet de gérer les machines virtuelles, telles que la définition de la configuration, la migration en direct et la sauvegarde des machines virtuelles.

Exemple

Voici un exemple concret d'utilisation de Microsoft Hyper-V :

- ▷ 1. Un administrateur informatique installe Hyper-V sur un ordinateur doté de Windows Server.
- ▷ 2. L'administrateur crée une machine virtuelle en spécifiant 2 Go de mémoire, 50 Go d'espace disque et une connexion réseau. Il installe un système d'exploitation invité, tel que Windows Server, sur la machine virtuelle.
- ▷ 3. L'administrateur installe une application de gestion de base de données sur la machine virtuelle et la configure pour utiliser une base de données en ligne de commande.
- ▷ 4. Des utilisateurs se connectent à l'application de gestion de base de données en utilisant un navigateur web sur leur ordinateur. Ils interagissent avec l'application via le système d'exploitation invité sur la machine virtuelle.
- ▷ 5. Si l'ordinateur sur lequel est installé Hyper-V devient inaccessible, l'administrateur peut déplacer la machine virtuelle vers un autre ordinateur exécutant Hyper-V en utilisant la fonctionnalité de migration en direct de Hyper-V. Les utilisateurs continuent à interagir avec l'application de gestion de base de données sans interruption.

En résumé, dans cet exemple, Microsoft Hyper-V a permis de virtualiser une application de gestion de base de données sur un ordinateur exécutant Windows Server, permettant ainsi aux utilisateurs d'interagir avec l'application via un navigateur web sur leur ordinateur. L'utilisation d'Hyper-V a également permis une migration en direct de la machine virtuelle vers un autre ordinateur en cas de besoin.

Quelques commandes

Voici quelques commandes couramment utilisées pour gérer Microsoft Hyper-V via la ligne de commande :

- ▷ 1. Get-VM : Cette commande permet d'afficher la liste des machines virtuelles existantes sur le serveur Hyper-V.
- ▷ 2. Start-VM : Cette commande permet de démarrer une machine virtuelle spécifiée.
- ▷ 3. Stop-VM : Cette commande permet d'arrêter une machine virtuelle spécifiée.
- ▷ 4. New-VM : Cette commande permet de créer une nouvelle machine virtuelle.
- ▷ 5. Remove-VM : Cette commande permet de supprimer une machine virtuelle existante.
- ▷ 6. Get-VMProcessor : Cette commande permet d'afficher les informations sur les processeurs affectés à une machine virtuelle spécifiée.
- ▷ 7. Set-VMProcessor : Cette commande permet de définir les paramètres des processeurs pour une machine virtuelle spécifiée.
- ▷ 8. Get-VMMemory : Cette commande permet d'afficher les informations sur la mémoire affectée à une machine virtuelle spécifiée.
- ▷ 9. Set-VMMemory : Cette commande permet de définir les paramètres de la mémoire pour une machine virtuelle spécifiée.

Ces commandes sont exécutées à partir de l'interface de ligne de commande Windows PowerShell. Il existe également d'autres commandes pour gérer d'autres aspects de Microsoft Hyper-V, telles que les disques virtuels, les réseaux et les snapshots. Voici quelques commandes supplémentaires pour gérer les disques virtuels, les réseaux et les snapshots sur Microsoft Hyper-V :

- ▷ 1. Get-VHD : Cette commande permet d'afficher la liste des disques virtuels associés à une machine virtuelle.
- ▷ 2. New-VHD : Cette commande permet de créer un nouveau disque virtuel pour une machine virtuelle.
- ▷ 3. Get-VMNetworkAdapter : Cette commande permet d'afficher les informations sur les adaptateurs réseau associés à une machine virtuelle.
- ▷ 4. New-VMNetworkAdapter : Cette commande permet de créer un nouvel adaptateur réseau pour une machine virtuelle.
- ▷ 5. Get-VMSnapshot : Cette commande permet d'afficher la liste des snapshots associés à une machine virtuelle.
- ▷ 6. Checkpoint-VM : Cette commande permet de prendre un snapshot de la machine virtuelle spécifiée.
- ▷ 7. Restore-VMSnapshot : Cette commande permet de restaurer une machine virtuelle à un état précédent défini par un snapshot.

Ces commandes permettent de gérer les différents composants de Microsoft Hyper-V, tels que les disques virtuels, les réseaux et les snapshots, à partir de la ligne de commande Windows PowerShell.

Les snapshots sont des instantanés d'un système de virtualisation, qui permettent de capturer l'état d'une machine virtuelle à un moment donné. Cela peut être utile pour des tâches telles que la sauvegarde d'un système, la résolution de problèmes ou la mise en place d'un système test.
Avec Microsoft Hyper-V, les snapshots peuvent être pris à partir de l'interface de ligne de commande Windows PowerShell en utilisant la commande Checkpoint-VM. Les snapshots peuvent être consultés et gérés à l'aide de la commande Get-VMSnapshot. Il est également possible de restaurer une machine virtuelle à un état précédent en utilisant la commande Restore-VMSnapshot.
Il est important de noter que les snapshots peuvent consommer de l'espace disque sur le serveur Hyper-V, il est donc conseillé de les utiliser avec parcimonie et de les supprimer régulièrement. De plus, les snapshots peuvent affecter les performances de la machine virtuelle et il est recommandé de les utiliser uniquement pour des tâches temporaires.

Les réseaux virtuels

Les réseaux sont un composant clé de la virtualisation. Avec Microsoft Hyper-V, les réseaux virtuels permettent de connecter les machines virtuelles entre elles, ainsi qu'avec le réseau physique. Cela permet aux machines virtuelles de communiquer entre elles, d'accéder à Internet et d'être gérées à distance.
Microsoft Hyper-V prend en charge plusieurs types de réseaux virtuels, tels que les réseaux internes, les réseaux externes et les réseaux privés. Les réseaux internes permettent aux machines virtuelles de se connecter entre elles, mais pas à Internet. Les réseaux externes permettent aux machines virtuelles d'accéder à Internet et d'être gérées à distance. Les réseaux privés permettent aux machines virtuelles de communiquer entre elles, sans accès à Internet.
Pour gérer les réseaux virtuels sur Microsoft Hyper-V, vous pouvez utiliser l'interface de ligne de commande Windows PowerShell. Vous pouvez afficher les informations sur les adaptateurs réseau en utilisant la commande Get-VMNetworkAdapter. Vous pouvez également créer de nouveaux adaptateurs réseau en utilisant la commande New-VMNetworkAdapter.

Chapitre 3

Les Services Annuaires et le Réseau Internet

3.1 Introduction

Les réseaux interconnectés utilisent les mêmes protocoles de routage et de transport à savoir TCP/IP connus sous l'appellation Internet. Ce dernier permet d'offrir des services tels que la messagerie (émail) le transfert de fichier (FTP et Peer to Peer), les serveurs Web en ligne, le streaming ou la VoD (Vedeo on Demand). Internet repose sur quatre éléments principaux (figure 3.1) :

1. Les opérateurs (câblage et transport).
2. Les fournisseurs d'accès Internet (FAI).
3. Les services et protocoles associés.
4. Les outils.

Le principe de chacun des acteurs sera détaillé dans ce chapitre.

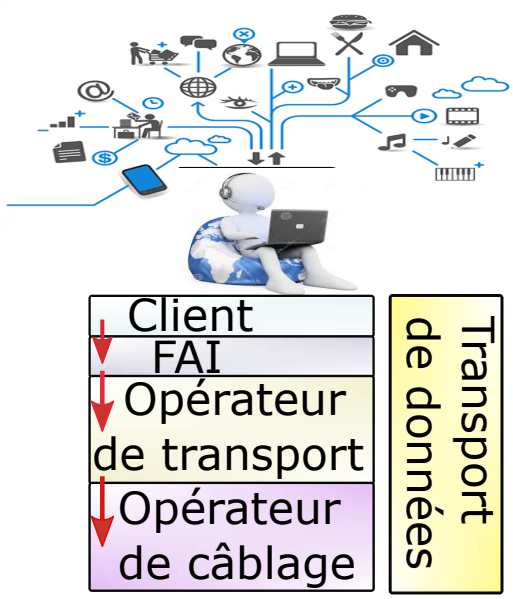


FIGURE 3.1 – Les intervenants dans l'internet

3.2 Les opérateurs

L'appellation générique ISP (Internet Service Provider) est donnée aux opérateurs de transport qui fournissent à différents niveaux des services pour l'internet. Leur hiérarchie est donnée par figure 3.2, elle décrit leurs propres réseaux et leurs organisation.

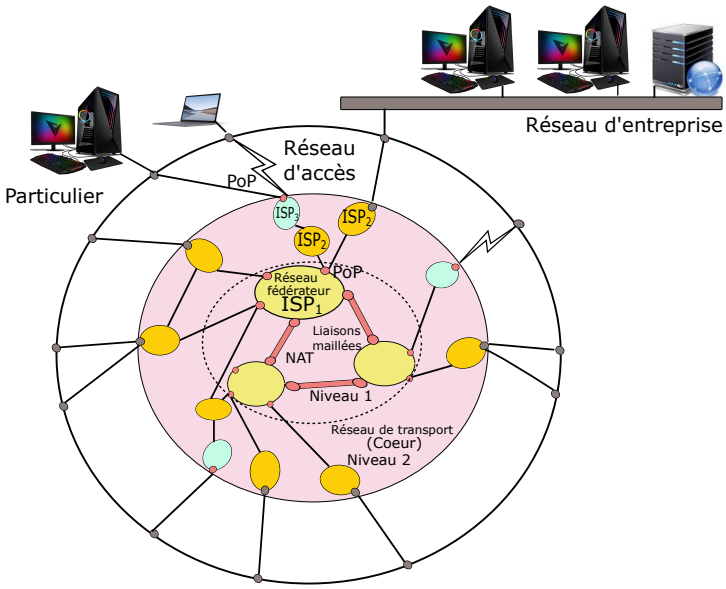


FIGURE 3.2 – Hiérarchie des opérateurs Internet

3.2.1 Réseaux fédérateurs

Nommés aussi *backbone*, **ISP** ou **ISP niveau 1** les réseaux fédérateurs se trouvent dans le réseau cœur de l'internet. Ils ont une couverture internationale et sont reliés entre eux directement par des NAP (Network access Point) leurs débits atteignent 10Gbit/s. Aux états unis on trouve les **UUNet** (Unix to Unix Network), **AT&T** (American Telephone & Telegraph), **QWEST** et **GEAN**T.

3.2.2 ISP de niveau 2 ou 3

Ils se situent à la frontière du réseau d'accès et leur couverture peut être nationale ou régionale. Ce sont des clients des ISP1 auxquels ils sont connectés au niveau des **PoP** (Point of Presence). Ils sont considérés comme des fournisseur d'accès Internet (**FAI**) aux entreprises et aux particuliers (voir figure 3.2) avec des débits de l'ordre du Gbit/s. En France Free, Orange, Bouygues et SFR sont les opérateurs pour les entreprises et les particuliers, Renater est le FAI de l'éducation et la recherche (50 Mb/s à 10Gb/s pour l'excellence recherche).
Les **GIX** (Groupment Internet eXchange) permettent l'échange de trafic Internet au niveau régional entre les ISP1, les ISP2 ou ISP3 sans passer systématiquement par le réseau cœur. Un **GIX** est une infrastructure physique qui relie les réseaux précédents est aussi appelé AS (Autonemous System) grâce à des accord mutuels dit de peering.

3.3 Les FAI

Les Fournisseurs d'accès Internet ou ISP de niveau 3 sont connectés à Internet par des opérateurs de transport et ont pour rôle de fournir :

- ▷ les adresses IP pour les entreprises et les particuliers (les adresses étant attribuées par bloc d'adresses),
- ▷ des services d'hébergement de pages web, stockage de fichiers ou messagerie,
- ▷ des services de connexions qui utilisent les réseaux d'opérateurs de télécommunications.

Il est à signaler que certains FAI, qui peuvent être aussi des opérateurs Internet, s'intéressent plus aux particuliers et d'autres au marché des entreprises. De ce fait, les FAI maîtrisent mieux le rapport client/capacité du réseau.

3.3.1 Autorité de gestion des adresses IP

Les adresses IP sont fournies par des organismes agrées ICANN (Internet Corporation for Assigned Names and Numbers) sous forme de classes pour les FAI. Ces derniers les répartissent à leurs clients sur la base de deux principes :

Mode connecté en permanence (Full internet)

Le client obtient une adresse IP fixe et peut héberger un serveur web par exemple.

Mode connexion temporaire (dial up)

Le prestataire loue une des adresse au client le temps de la consultation. Le serveur qui est utilisé dans ce cas est dynamique appelé DHCP (Dynamic Host Configuration Protocol).
Le FAI doit donc répartir les N adresses dont il dispose en N_1 adresses pour les client de premier mode et $N - N_1$ adresses pour les second mode. Par conséquent, il y aura $N - N_1$ clients connectés simultanément au maximum.

3.3.2 Les équipements du FAI

Les équipements du FAI sont représentés sur la figure 3.3. On y trouve :

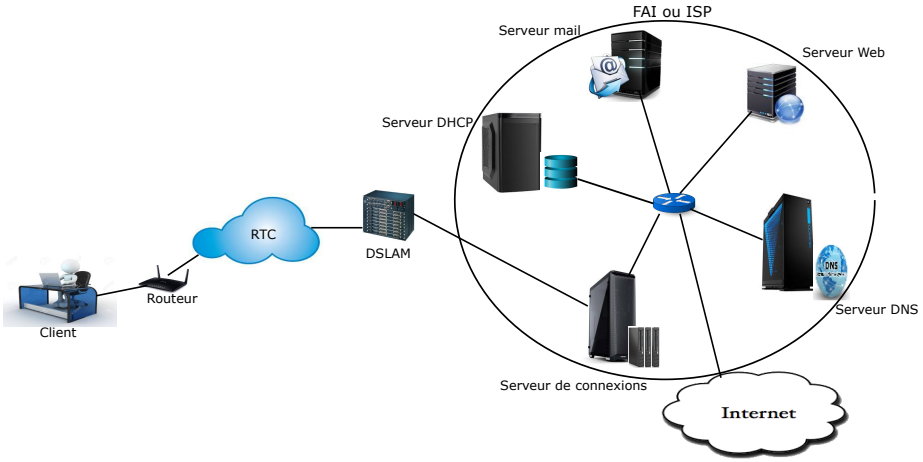


FIGURE 3.3 – Les équipement d'un FAI

- ▷ Des modems ADSL ou câble, un serveur de connexions pour générer les accès des clients et des équipements pour assurer la sécurité (Firewall, serveur d'authentification...).
- ▷ Du coté opérateurs, des routeurs et des équipements de raccordement de type LS (Ligne Spécialisée) pour débit élevés.
- ▷ Les Différents types de serveurs de services (DNS, DHCP, Messagerie...).

3.4 Les connexions

La boucle locale ou réseau d'accès permet aux équipements terminaux qui sont situés à la périphérie d'Internet (PC, Serveurs, Smartphone...) d'être reliés à Internet. Cette boucle (quelques mètres ou Km) est réalisée par des supports de type :

- ▷ La paire torsadés, modem **xDSL** et accès par **RTC**.
- ▷ Le réseau câblé (**CATV** : Cable TV et **HFC** : Hybrid Fiber/Coaxial).
- ▷ La fibre optique (**FITL** : Fiber In The Loop).
- ▷ L'accès hertzien (**WLL** Wireless Local Loop).
- ▷ L'accès par les réseaux cellulaires (**3G**, **3G+**, **4G** et **5G**).

3.4.1 Accès par le câble

En région dense la technologie, réseau de télévision câblé est utilisée. Elle permet le transfert de données numériques sur un ou plusieurs canaux de câble de 6 MHz. Pour ce qui est de la vidéo et l'audio (TV sur câble et Son FM), la transmission est réalisée sur d'autres canaux du même câble. La coexistence de tous ces services est possible grâce à la technologie du réseau local large bande.

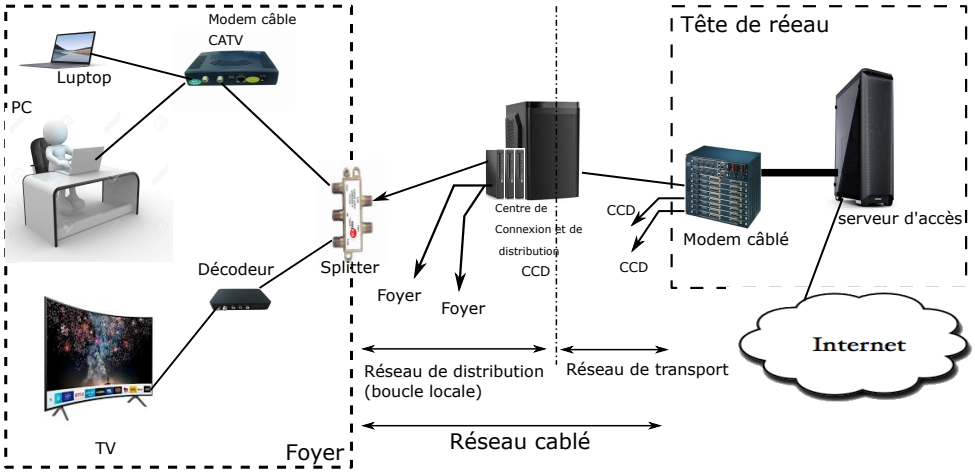


FIGURE 3.4 – Représentation d'une connexion câblée

A partir d'une entête de réseau (voir figure 3.4), un réseau de transport en fibre optique distribue les données ainsi que les signaux TV en numérique jusqu'à un centre local de distribution qui regroupe plusieurs habitations ou immeubles. Les signaux sont acheminés sur un câble TV (CATV) de type coaxial vers chacun des foyer et la connexion est réalisée par un boitier de raccordement (modem-câble). Il est dédié au réseau HFC (Hybrid Fiber Coaxial) représentant la norme pour les réseaux câblés bidirectionnels avec des débits de 100MHz selon la qualité des équipements et des liaisons.

3.4.2 L'accès ADSL

Les modems xDSL utilisent les paires torsadées du réseau téléphonique pour réaliser une boucle locale haut débit selon la distance par rapport au répartiteur. Les débits descendant en ADSL2+ peuvent atteindre 20 Mb/s.

3.4.3 La fibre optique

Deux stratégies de déploiement sont actuellement utilisées pour câbler entièrement le réseau de distribution en fibre optique et qui sont le PON (Passive Optical Network) et FTTH (Fiber To The Home).

La technologie PON

Une topologie en arbre passif est utilisée dans ce cas pour réaliser la boucle locale fournissant pour chaque terminaison une longueur d'onde spécifique. Ainsi, l'infrastructure de câblage se résume en une ligne partiellement partagée pour desservir plusieurs abonnés (figure 3.5).

La technologie FTTH

Dans cette technologie l'abonné est câblé par fibre optique permettant un débit théorique important au prix plus élevé en terme de câblage. Les deux technologies peuvent atteindre des débits supérieur à 100 Mb/s.

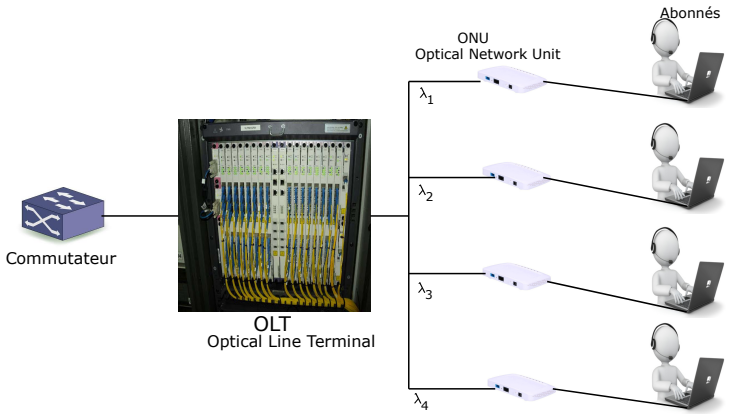


FIGURE 3.5 – Technologie PON

L'accès sans fil

L'accès sans fil est une technologie proposant une solution pour la boucle locale, avec deux orientations suivant la mobilité de l'abonné.
Le handover (Mobilité importante) L'abonné se déplace d'une cellule à l'autre sans interruption de la communication. Le terminal qui utilise la technologie de téléphonie cellulaire (UMTS, HSDPA, LTE, LTE Advanced) se voit régulé en débit afin de bénéficier des connexions Internet. Pour une tablette ou un smartphone une puce SIM (USIM) permet la connexion au haut débits. Dans le cas d'un PC, et pour des raisons commerciales, il est nécessaire d'ajouter une clé USB avec carte SIM pour se connecter à Internet.
Réseaux locaux sans fil (Mobilité réduite) : Dans se cas les réseaux locaux sans fil et leurs extensions : IEEE 802.11 (WiFi) et IEEE 802.16 (WiMax, Word wide interoperability for Microwave Access, 50 Km et 70 Mb/s théoriquement) qui sont utilisés. cette technologie est considérée comme une connexion ADSL sans fil et à été très utilisée dans les zones rurales.

3.5 Les Protocoles ARP, PARP, ICMP et DHCP

3.5.1 Rappels sur le fonctionnement des équipements d'interconnexion

Le fonctionnement de deux équipements (switch et routeur) nécessaires pour la compréhension de la suite du chapitre vont être rappelé dans cette sous section.

Le Switch (Commutateur)

Un switch, commutateur ou commutateur réseau, est un équipement de niveau 2 qui fonctionne comme un pont multiports et qui permet de relier plusieurs segments d'un réseau informatique entre eux. Le switch est chargé d'analyser les trames qui arrivent sur les ports d'entrée. Il opère une filtration des données afin de les orienter vers le bon port. Le switch a donc une double fonction de filtrage et de connectivité. Il sert de véhicule au transport de trame, comme peut également le faire le routage. Il crée également des circuits virtuels. Il existe une multitude de types de switchs comme le switch Ethernet, le switch HDMI, etc. Tous sont proposés par des entreprises spécialisées comme Cisco, Netgear ou D-Link. Chacun peut employer un mode de transmission particulier selon la méthode du mode direct (sans détection d'erreur), du mode différé (avec opération de contrôle sur chaque trame), du fragment free (mélange entre les deux modes précédents) ou de la commutation automatique (choix automatique entre les trois modes précédents). Un exemple explicatif de la table de switching est donnée en figure 3.6

Le Routeur

L'acheminement des paquets entre différents réseaux est la tâche principale d'un routeur. Après analyse de l'en-tête du paquets, il lui choisit le chemin à base de l'adresse de destination qu'il

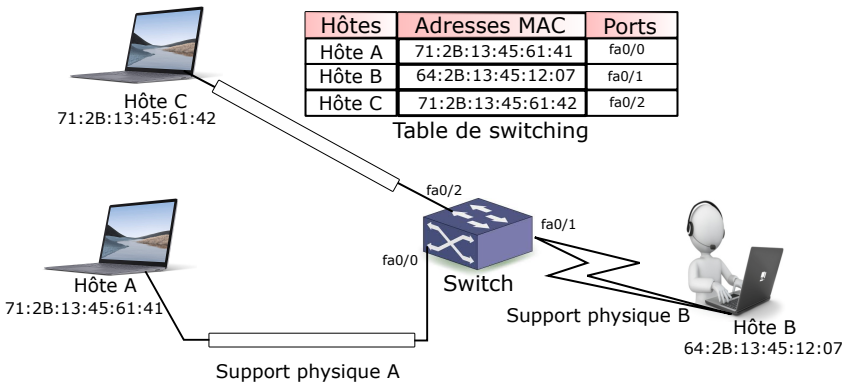
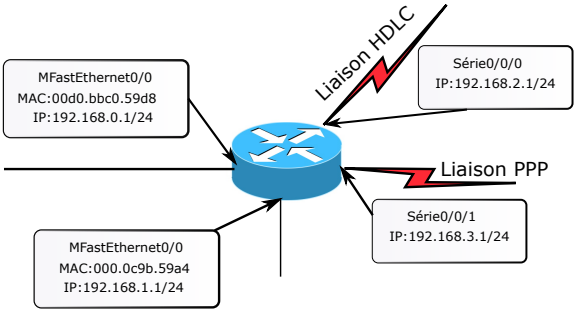
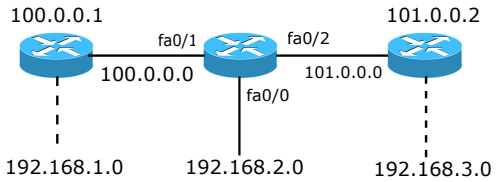


FIGURE 3.6 – Table du switch

porte. Parfois les en-têtes des paquets sont adaptés aux normes et aux contraintes du réseau sur lequel la trame sera envoyée.
La table de routage : Un routeur utilise une table (figure3.7.b) de routage pour déterminer le lieu d'acheminement des paquets, elle contient un ensemble de routes. Chaque route décrit la passerelle ou l'interface utilisée par le routeur pour atteindre un réseau donné.



(a) Représentation logique des interfaces d'un routeur



Réseau	Masque	Support	Métrique
192.168.2.0	255.255.255.0	fa0/0	0
101.0.0.0	255.0.0.0	fa0/1	0
101.0.0.0	255.0.0.0	fa0/2	0
192.168.1.0	255.255.255.0	100.0.0.1	1
192.168.3.0	255.255.255.0	101.0.0.2	1

(b) Table de routage

FIGURE 3.7 – Interfaces d'un routeur et sa table de routage

Les types de routes : chaque table de routage contient plusieurs types de routes :
• Route directement connectée (C), reliée directement au routeur.
• Route statique (S) : programmée manuellement, en indiquant l'adresse et le masque de destination, ainsi que la passerelle correspondant.
• Route dynamique (R) ou (O) ou (D) : a été envoyée au routeur par le routeur voisin. Il existe différents protocoles dynamiques, parmi lesquels on peut citer RIP, OSPF, BGP, EIGRP, IGRP, IS-IS.
• Route par défaut (S*) : est un type de route statique qui spécifie une passerelle à utiliser lorsque la table de routage ne contient pas de chemin vers le réseau de destination. Si le routeur ne trouve pas de route correspondant à l'adresse de destination et qu'il ne possède pas de route par défaut, le message est tout simplement détruit. L'expéditeur est alors informé par un message ICMP.
•Interfaces d'un routeur : Comme il relie plusieurs réseaux, le routeur dispose de plusieurs interfaces, chacune appartenant à un réseau IP différent (voir figure 3.7a). Ces interfaces peuvent être connectées à des réseaux locaux (LAN) ou à des réseaux étendus (WAN). Du côté LAN le routeur possède généralement une interface Ethernet de type RJ45. Comme une carte réseau Ethernet de PC, une interface Ethernet de routeur possède également une adresse MAC de couche 2 et participe au réseau local Ethernet de la même manière que tous les autres hôtes de ce réseau. du côté WAN : les interfaces servent à connecter les routeurs à des réseaux externes,

généralement sur une distance géographique importante. L'encapsulation de couche 2 peut être de différents types, notamment PPP, Frame Relay et HDLC (High-Level Data Link Control) voir figure 3.7a.

3.5.2 Le Protocole ARP (Address Resolution Protocol)

La fonction principale du protocole ARP est d'établir une correspondance entre les adresses logiques IP et les adresses physiques MAC (Media Acces Control). Le principe de ce protocole est d'interroger les machines du réseau pour connaitre leur adresse physique auxquelles il fait correspondre leur adresses MAC en créant une table dite table de correspondance dans une mémoire cache. Quant une machine veut communiquer avec une autre elle consulte tout d'abord sa table. Si l'adresse n'y figure pas, elle fait une recherche illustrée sur la figure 3.8. Il est plus facile d'utiliser des adresses IP car elle ont une portée dans le réseau tout entier à l'inverse des adresses MAC qui sont par construction uniques (numéro de fabrication, numéro de fabrication etc) car leur portée est dans le réseau local. Cependant, elles restent uniques mais trop aléatoires pour les utiliser, c'est pour cela qu'on fait correspondre une adresse MAC à une adresse IP à travers une table de routage. C'est ainsi que le protocole ARP permet de chercher de l'adresse MAC correspondante.

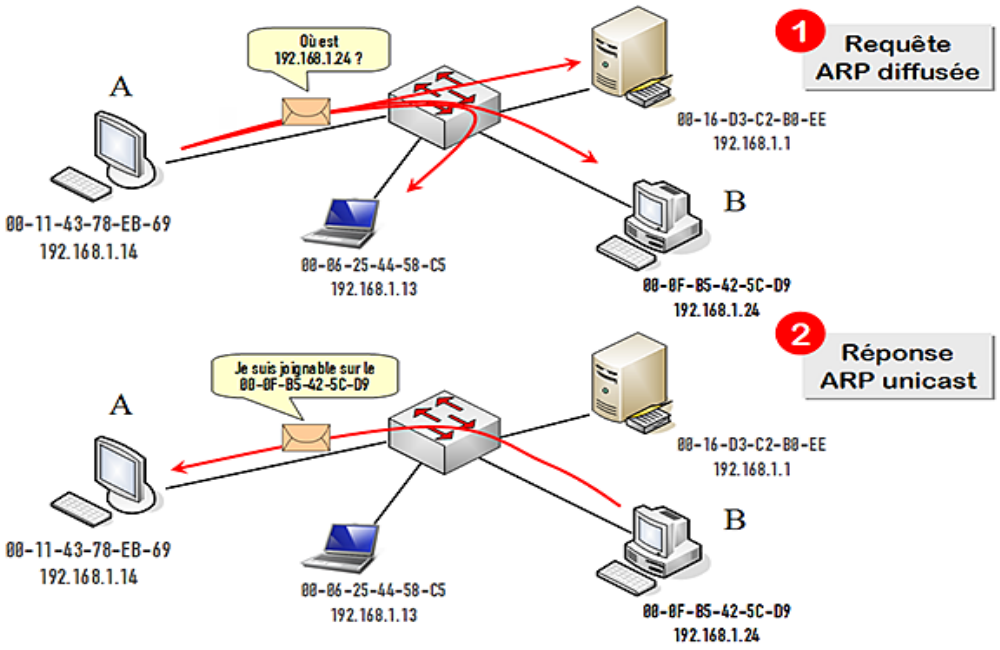


FIGURE 3.8 – Requête ARP (cisco)

Exemple :

En exécutant sous CMD administrateur la commande

C :\>arp -a on obtient la table de routage avec toutes les adresses IP et MAC de notre machine

3.5.3 Le Protocole RARP (Reverse Adress Resolution Protocol)

Comme indiqué par son nom, le protocole permet d'établir la correspondance inverse c'est à dire les adresses physiques MAC, sont reliées aux adresses logiques (Internet).

3.5.4 Le Protocole ICMPv4 (Internet Contrôle Message Protocol, RFC 792)

Il est classé de niveau 3 (voir chapitre Rappels) car il sert à la gestion du protocole IP, même si en réalité il utilise l'encapsulation IP. Entre autre il a pour rôle la collecte d'erreurs qui peuvent survenir lors de l'émission de messages (coupure sur le réseau, expiration de délais

etc). Il permet de tester l'accessibilité d'une machine sur le réseau. Les messages ICMPv4 sont encapsulés dans un datagramme IP ou (protocole est mis à 1). Ils sont de deux natures :

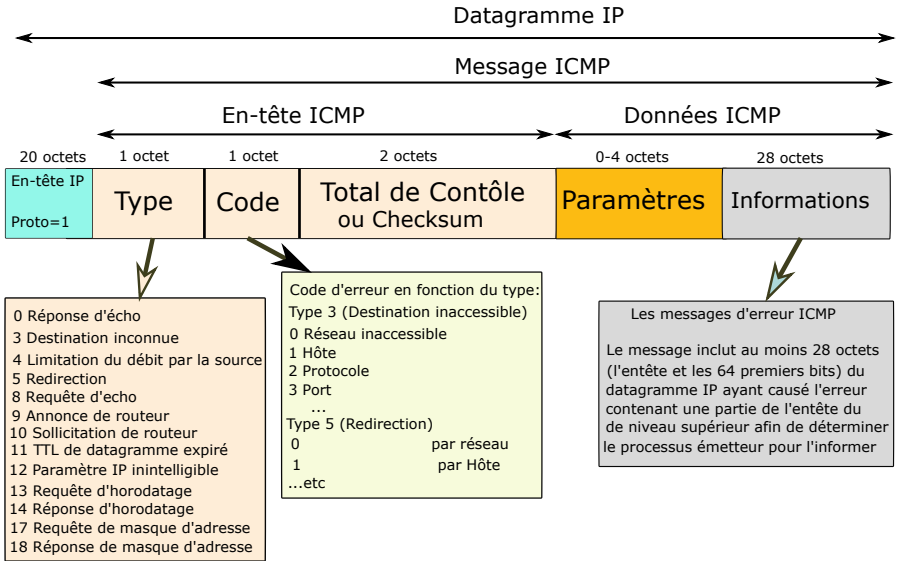


FIGURE 3.9 – Structure du message d'erreur ICMPv4 dans un datagramme IP

Les messages d'erreur : lorsqu'une erreur est constatée sur un datagramme celui ci est souvent détruit.
Les messages d'interrogation ou information : ce sont des message divers qui soit ils contribuent au bon fonctionnement des équipement, soit ils informent sur leurs état. Ils sont encapsulés dans un datagramme IP ou (protocole est mis à 1). La figure 3.9 détaille les message d'erreurs ICMP ainsi que quelques exemples de codage des différents champs.

3.5.5 Le Protocole ICMPv6

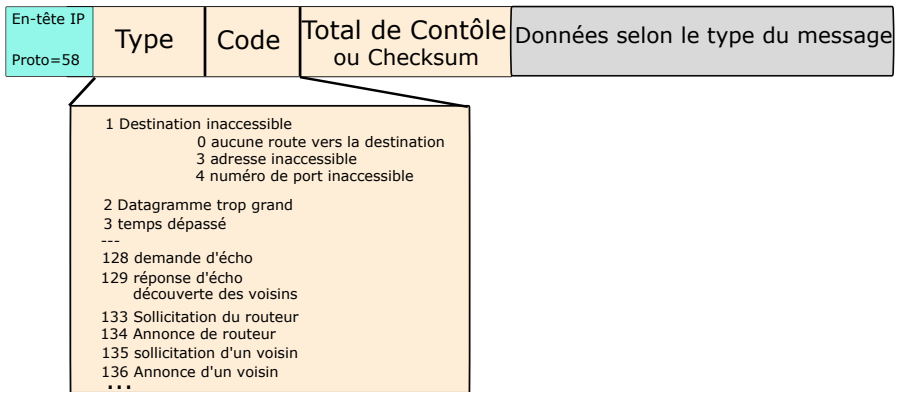


FIGURE 3.10 – Le message ICMPv6

L'ICMP pour IPv6 (Internet Control Message Protocol Version 6) noté ICMPv6 fait partie à part entière de l'architecture IPv6, il est supportée par toutes les implémentations d'IPv6. ICMPv6 combine des fonctions antérieurement subdivisées à travers différents protocoles, tels que ICMPv4, IGMP (Internet Group Membership Protocol) et ARP (Address Resolution Protocol). Il a permis d'éliminer des types de messages obsolètes. De nouvelles fonctionnalités ont été introduites pour l'auto-configuration (découverte de voisins ...). Le message ICMPv6 est donné en figure (3.10)

Obtention de masque sous-réseau par message ICMPv4

Dans le but de se configurer, une station a besoin de connaitre le masque de sous-réseau utilisé (Netmask) dans son réseau, elle émet une requête (Type=17) voir figure (3.9). Qui elle même

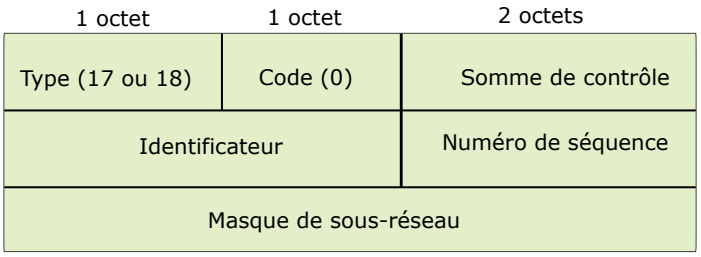


FIGURE 3.11 – Requête ICMP de masque sous-réseau

est émise destination de la passerelle par défaut, si celle ci est connue, sinon elle est diffusée à toutes les stations du réseau (broadcast). La réponse à la requête d'origine est donnée dans les champs Identificateur et Numéro de séquence voir le figure (3.11).

Deux Utilitaires importants qui utilisent les messages ICMPv4

L'utilitaire Ping (Packet INternet Groper)
Il permet de tester l'accessibilité d'un système et d'évaluer le temps d'un aller retour entre la source et la destination.
Par exemple en mode CMD admin tapez ping 127.0.0.1 permet de tester l'installation de la pile TCP/IP sur la machine source.
L'utilitaire Traceroute (Tracert)
Il permet de découvrir la route empruntée par un datagramme entre la source et la machine destination.
Par exemple en mode CMD admin tapez tracert google.com vous donnera tous les routeurs qui se trouvent entre la machine source (la votre) et le serveur google.com.

3.5.6 Le Protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol, RFC 2131 et 2132) offre de véritables fonctions de configuration automatique des stations. Le serveur DHCP détient un jeu d'adresses valides et les paramètres associés de configuration IP à allouer dynamiquement aux clients DHCP. Les stations configurées par DHCP libèrent les adresses lorsqu'elles n'en ont plus besoin. DHCP propose trois mécanismes d'adressage :

- ▷ L'allocation manuelle : DHCP alloue une adresse spécifique à un client. L'administrateur gère donc les adresses IP (DHCP statique).
- ▷ L'allocation automatique : elle permet, lors d'une configuration initiale, d'attribuer automatiquement à une station une adresse IP choisie par le système parmi un pool d'adresses. La station conserve cette adresse tant qu'elle n'a pas été libérée explicitement par l'administrateur.
- ▷ L'allocation dynamique : dans ce mode de fonctionnement, DHCP alloue temporairement (bail) une adresse IP. En fin de bail, la machine cliente peut en demander le renouvellement.

3.6 Les Services Annuaires

3.6.1 Généralités

Les services d'annuaires permettent de rechercher un nom d'entité, un restaurant par exemple, dans un contexte connu, comme la ville où l'on réside. La recherche d'un restaurant particulier peut aussi se faire par son nom. Grâce aux services d'annuaires, **un programme recherche** des **attributs** de différents types concernant le contrôle d'accès, **l'authentification**, **les domaines**, **les groupes**, **les adresses réseau**, **les adresses de port** etc.

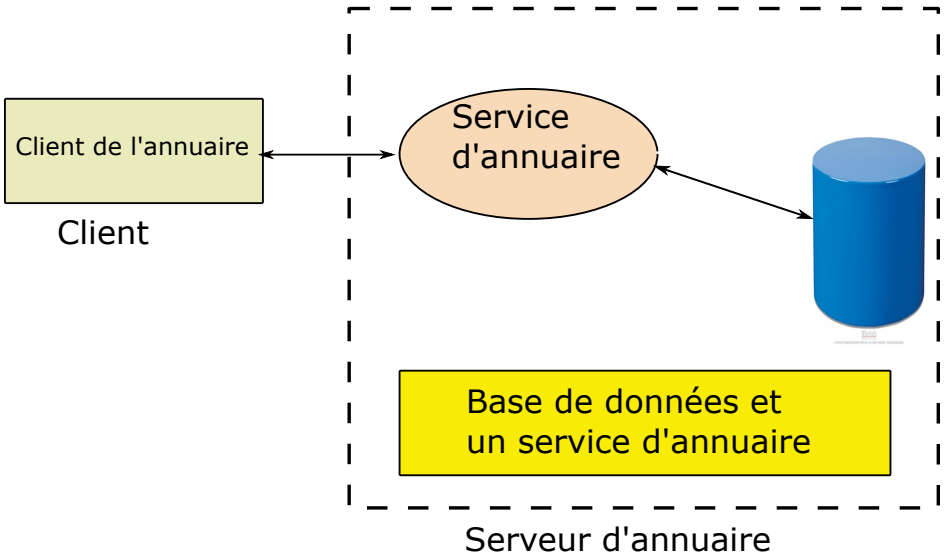


FIGURE 3.12 – Schématisation d'un service annuaire

Les services d'annuaires fournissent fréquemment une correspondance entre une dénomination explicite, facile à mémoriser, et une adresse qui le serait difficilement. On appelle cette correspondance un service de noms. C'est l'un des nombreux services que peut offrir un service d'annuaires. Le système de noms de domaines **DNS** (Domain Name System) représente ce type de services, il est considéré "comme l'annuaire des ordinateurs".

3.6.2 Le service de nommage DNS

Le nommage est un service de résolution qui permet l'identification des terminaux (machines) localement ou à l'échelle mondiale, à travers des noms au lieu des adresses IP. DNS permet en quelque sorte de traduire les adresses IP en noms de domaines. A l'aide d'un service permettant une organisation hiérarchisée (le DNS), tous les noms des machines spécifiques (les serveurs de noms) sont gérés de façon centralisé. Le réseau globale est divisé en un ensemble de domaines primaires, secondaires... suivant une organisation arborescente. L'ICANN (Internet Corporation for Assignment Names and Numbers) est l'autorité de nommage de l'Internet. voir le lien : https ://www.iana.org/.
Exemple

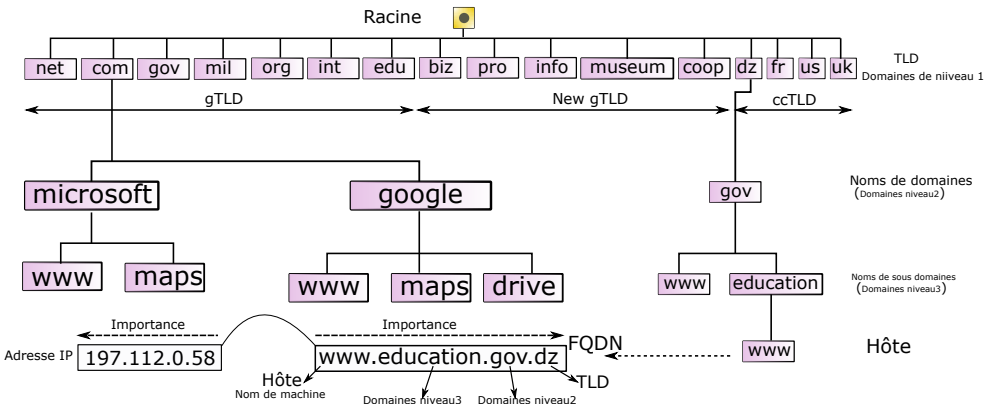


FIGURE 3.13 – Structure arborescente du nommage DNS

En Algérie c'est NIC (Network Internet Center) qui gère la zone (toute la base de données). C'est un organisme agrée par l'ICANN pour la gestion du CCTLD (Country Code Top Level Domain) .dz à l'Algérie (CERIST). En France c'est l'AFNIC (Association Française pour le Nommage Internet en Coopération). La figure 3.13 montre la structure arborescente où sont définit les domaines de premier niveau (TLD, Top Level Domains) rattachés au nœud racine

représenté par un petit carré ensuite viennent les domaines du $2^{ème}$ niveau SLD (Second Level Domain) et juste après le $3^{ème}$niveau ...
Les TLG génériques gTLD sont définies au même niveau de l'arborescence que les TLD correspondant un pays ccTLD (country code TLD).
QFDN (Fully Qualified Domain Name) est le nom complet d'un hôte, il est constitué des domaines successifs séparés d'un point. A l'inverse des adresse IP ou le hôte est situé à droite, les noms DNS pressente le nom à gauche suivi des noms de domaine d'importance croissante, voir figure 3.13.

3.6.3 Requête DNS

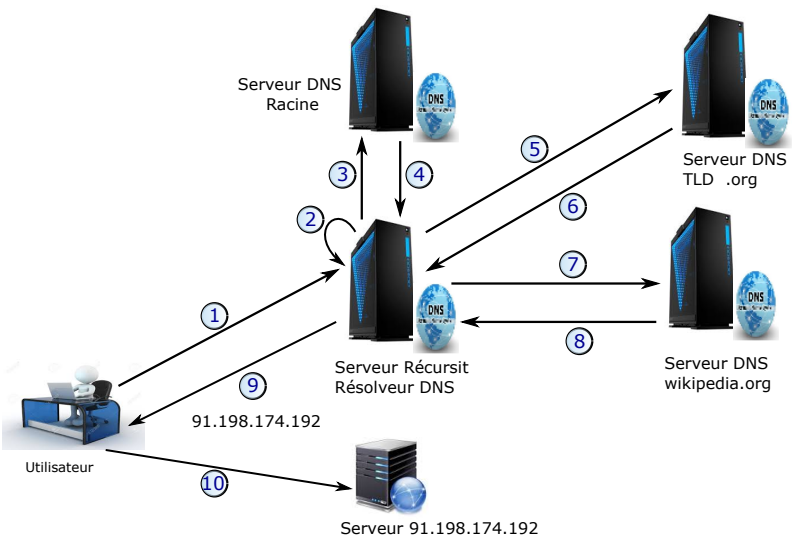


FIGURE 3.14 – Requête DNS

La requête DNS représentée sur la figure 3.14 peut être expliquée suivant les étapes allant de 1 à 9 comme suit :

1. Le client souhaite accéder au site wikipedia.org mais ne connaît pas l'adresse IP associée. Il envoie donc une requête à son résolveur DNS.
2. Le serveur DNS vérifie dans sa base de connaissance interne (appelée cache) s'il a l'adresse IP associée au nom de domaine wikipedia.org. Si c'est le cas, il renvoie directement l'information au client (Étape 9).
3. Si le serveur DNS n'a pas l'adresse, il va interroger l'un des 13 serveurs DNS racines. Ces serveurs possèdent des informations sur tous les serveurs TLD.
4. Le serveur DNS racine va renvoyer l'adresse d'un serveur TLD ".org".
5. Le serveur DNS va interroger le serveur TLD ".org". Si ce dernier possède l'adresse IP, il la renverra (et on continuera sur l'étape 9). Il peut également avoir l'adresse du serveur DNS faisant autorité sur le domaine. Cette dernière peut également être renvoyée. on dira dans ce cas que c'est un serveur autoritaire.
6. Dans notre cas le serveur DNS va soit renvoyer l'adresse de wikipedia.org s'il la possède. Sinon il peut rediriger vers les serveurs de nom "wikipedia" (wikipedia.org).
7. Le serveur DNS va faire une requête au serveur DNS "wikipedia.org" pour savoir où est l'adresse IP de wikipedia.
8. Le serveur DNS "wikipedia.org" va renvoyer l'adresse IP de "wikipedia.org" (91.198.174.192).
9. Le serveur DNS renvoie au client l'adresse IP de wikipedia.org.
10. Le client accède à wikipedia.org par son adresse IP.

Ce fonctionnement un peu long est réalisé lorsque l'on tente d'accéder pour la première fois à une ressource. Dans le cas où le client a déjà accédé à la ressource, il est possible que le cache le redirige directement vers cette ressource.

Chapitre 4

Gestion des utilisateurs et service NFS Network File System

Introduction Imaginez une petite entreprise avec dix employés. Chaque employé travaille sur son propre ordinateur. Comment partager des documents entre collègues ? Plusieurs solutions existent, mais elles ont toutes des inconvénients.
La première idée serait d'utiliser des clés USB. Chaque fois qu'un employé veut partager un fichier, il le copie sur une clé et la donne à son collègue. Cette méthode est rapide pour de petits volumes, mais elle devient vite ingérable. Les fichiers se dupliquent, on ne sait plus quelle version est la plus récente, et il est impossible de travailler à plusieurs sur le même document.
Une autre approche consiste à envoyer les fichiers par courrier électronique. C'est pratique pour des documents occasionnels, mais les pièces jointes alourdissent les boites mails, et là encore, les versions se multiplient sans contrôle.

Définition

Un système de fichiers réseau est une technologie qui permet à un ordinateur d'accéder à des fichiers stockés sur une autre machine comme s'ils étaient sur son propre disque dur. L'utilisateur n'a pas besoin de copier les fichiers : il les ouvre directement depuis le serveur.

Le principe est simple : on désigne un ordinateur comme serveur de fichiers. Ce serveur contient tous les documents partagés. Les autres ordinateurs, appelés clients, se connectent au serveur pour accéder aux fichiers, figure 4.1. Quand un employé modifie un document, c'est la version sur le serveur qui est mise à jour, accessible immédiatement à tous.

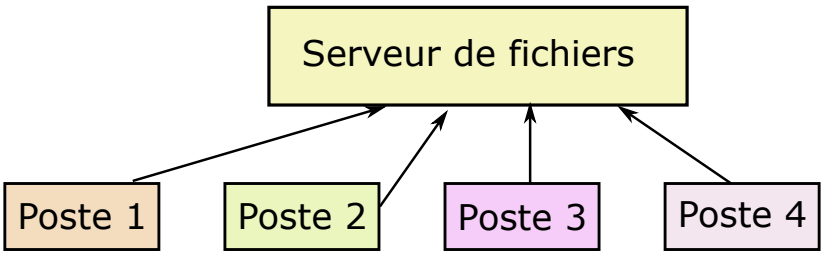


FIGURE 4.1 – Architecture simplifiée d'un serveur de fichiers réseau

Le deuxième problème : la gestion des utilisateurs Dans une entreprise qui grandit, un nouveau problème apparaît. Comment gérer les comptes utilisateurs ? Sur chaque ordinateur, il faut créer un compte pour chaque employé, avec son mot de passe. Si un employé change de poste, il faut recréer son compte. Si un employé quitte l'entreprise, il faut supprimer son compte partout. Pour une centaine d'employés, cette tâche devient vite compliquée.

Définition

Un service d'annuaire est une base de données centralisée qui contient toutes les informations sur les utilisateurs : leurs noms, leurs mots de passe, leurs droits d'accès, et parfois d'autres informations comme leur numéro de téléphone ou leur service.

Avec un service d'annuaire, les comptes sont créés une seule fois sur le serveur. Quand un employé se connecte à n'importe quel ordinateur du réseau, celui-ci interroge l'annuaire pour vérifier le mot de passe. Plus besoin de créer des comptes partout.

Les trois technologies Il existe plusieurs technologies pour résoudre ces problèmes.

- ▷ NFS (Network File System) (1980) chez Sun Microsystems. C'est la solution historique pour les systèmes Unix et Linux. Son avantage est sa simplicité et sa transparence.
- ▷ NIS (Network Information System) est également issu de Sun Microsystems. Il fournit un annuaire simple pour les comptes utilisateurs. Bien qu'ancien et peu sécurisé, il reste intéressant à comprendre car ses concepts ont été repris dans des technologies plus modernes comme LDAP.
- ▷ SMB (Server Message Block) est le protocole de Microsoft. C'est la solution standard pour les réseaux Windows, mais il fonctionne aussi très bien avec Linux grâce à un logiciel appelé Samba. C'est aujourd'hui la solution la plus complète et la plus sécurisée.

4.1 NFS - Le partage de fichiers pour Unix et Linux

4.1.1 Le principe de fonctionnement de NFS

NFS rend les fichiers distants invisibles

L'idée maîtresse de NFS est la transparence. Pour un utilisateur qui utilise un logiciel, ouvrir un fichier sur le serveur doit être exactement la même chose qu'ouvrir un fichier sur son propre disque dur. Le système d'exploitation se charge de toute la complexité.
Pour comprendre comment cela fonctionne, il faut savoir que les systèmes Unix et Linux ont une couche logicielle appelée **VFS** (Virtual File System). Cette couche fait l'abstraction des différents types de systèmes de fichiers. Qu'il s'agisse d'un disque dur local en ext4, d'une clé USB en FAT32 ou d'un répertoire distant en NFS, le VFS présente la même interface aux logiciels.
Quand une application demande d'ouvrir un fichier, le VFS détermine de quel type de système de fichiers il s'agit. Si c'est un fichier local, il transmet la demande au pilote du disque dur. Si c'est un fichier NFS, il transmet la demande au client NFS. Celui-ci envoie une requête sur le réseau au serveur NFS, qui lit le fichier et renvoie son contenu.

Définition

Le client NFS est le logiciel installé sur la machine qui veut accéder à des fichiers distants. **Le serveur NFS** est le logiciel installé sur la machine qui expose ses fichiers aux autres.

4.1.2 Les différentes versions de NFS

NFS a beaucoup évolué depuis sa création. Il existe plusieurs versions, et il est important de comprendre leurs différences.
La version 2, apparue en 1989, utilisait uniquement le protocole UDP et ne pouvait pas manipuler des fichiers de plus de 2 gigaoctets, ce qui était acceptable à l'époque mais plus du tout aujourd'hui.
La version 3, sortie en 1995, a apporté des améliorations majeures. Elle supporte le protocole TCP, ce qui est plus fiable pour les transferts importants. Elle gère les fichiers de grande taille (jusqu'à 64 bits). Elle permet aussi les écritures asynchrones, ce qui améliore les performances.
La version 4, normalisée en 2000, est la plus intéressante aujourd'hui en simplifiant la configuration car elle utilise un seul port réseau (le 2049) au lieu de ports dynamiques difficiles à gérer avec les pare-feu. Elle intègre la sécurité avec Kerberos et supporte les ACL (listes de contrôle d'accès plus fines que les simples droits Unix) [1]

1. Il est recommandé d'utiliser NFS version 4 quand c'est possible. La version 3 reste acceptable pour des environnements simples et sécurisés en interne. La version 2 ne devrait plus être utilisée.

4.1.3 Configurer un partage NFS

Sur le serveur : exporter un répertoire

Pour qu'un répertoire devienne accessible par NFS, il faut le déclarer dans un fichier de configuration appelé /etc/exports. La syntaxe est simple : on indique le chemin du répertoire à partager, puis la liste des clients autorisés avec leurs droits.

Exemple

Supposons qu'on veuille partager le répertoire /partage avec tous les ordinateurs du réseau local. On ajoute cette ligne dans /etc/exports :
/partage *(rw,sync)
Le symbole * signifie tous les clients. rw autorise la lecture et l'écriture. sync garantit que les données sont bien écrites sur le disque avant de confirmer l'opération.
Après avoir modifié ce fichier, on doit exécuter cette commande pour que les changements soient pris en compte :
sudo exportfs -a

Il est possible d'être plus précis sur les clients autorisés. Voici différentes façons de les désigner :
- serveur1 : une machine nommée serveur1 (si la résolution DNS fonctionne)
- 192.168.1.10 : une machine par son adresse IP
- 192.168.1.0/24 : tout un réseau (toutes les adresses de 192.168.1.1 à 192.168.1.254)
- *.monentreprise.local : toutes les machines d'un domaine

Sur le client : monter le partage

Une fois le serveur configuré, le client doit monter le partage. Monter signifie attacher le répertoire distant à un endroit dans l'arborescence locale. C'est comme si on greffait une branche distante sur notre propre arbre de fichiers.

Exemple

Dans l'exemple précédent, sur le client, on veut que le répertoire /partage du serveur (dont l'adresse IP est 192.168.1.100) soit accessible dans le dossier /mnt/nfs. On commence par créer ce dossier :
sudo mkdir -p /mnt/nfs
Puis on monte le partage :
sudo mount -t nfs4 192.168.1.100 :/partage /mnt/nfs
Maintenant, tout fichier placé dans /mnt/nfs sur le client est en réalité stocké sur le serveur. Si on modifie un fichier, tous les clients qui ont monté ce partage verront la modification immédiatement.

Pour que le montage soit automatique à chaque démarrage du client, on peut ajouter une ligne dans le fichier /etc/fstab :
192.168.1.100 :/partage /mnt/nfs nfs4 defaults 0 0

4.1.4 Les inconvénients de NFS

NFS est un protocole pratique, mais il présente quelques faiblesses qu'il faut connaître.
- ▷ Le premier problème est la sécurité. Dans ses versions anciennes, NFS ne chiffre pas les données qui circulent sur le réseau. Une personne malveillante qui capturerait le trafic pourrait lire les fichiers transférés. NFSv4 permet le chiffrement, mais il faut le configurer explicitement.
- ▷ Le deuxième problème est la gestion des identifiants. NFS fonctionne avec des numéros d'utilisateur (UID) et de groupe (GID). Si l'utilisateur untel a l'UID 1001 sur le serveur mais l'UID 1002 sur le client, NFS ne comprendra pas qu'il s'agit de la même personne. Pour que NFS fonctionne bien, il faut synchroniser les comptes utilisateurs entre toutes les machines. Ce problème est surmonté grâce au protocole NIS.

4.2 NIS - Centraliser les comptes utilisateurs

4.2.1 Network Information System NIS

Reprenons notre exemple d'entreprise avec de nombreux postes de travail. Sur chaque poste, les utilisateurs doivent pouvoir se connecter avec leur mot de passe. Si on crée les comptes un par un sur chaque machine et

dans le cas d'un nombre important de machines, le travail est fastidieux. De plus, si on utilise NFS sans NIS, les numéros d'utilisateurs risquent d'être incohérents d'une machine à l'autre. Par conséquent, un protocole dit NIS apporte une solution simple : tous les comptes sont stockés une seule fois sur un serveur. Les clients interrogent ce serveur pour authentifier les utilisateurs.

Définition

NIS (Network Information System) est un service d'annuaire qui centralise les fichiers système comme /etc/passwd (les comptes), /etc/shadow (les mots de passe), /etc/group (les groupes) et /etc/hosts (les noms de machines).

4.2.2 Organisation des données à travers le protocole NIS

Sur le serveur NIS [2], on trouve un ensemble de fichiers appelés maps. Chaque map est une version indexée d'un fichier système. Par exemple, la map passwd.byname permet de retrouver rapidement un utilisateur par son nom, tandis que passwd.byuid permet de le retrouver par son numéro.

Les maps sont générées automatiquement à partir des fichiers classiques. Quand on ajoute un utilisateur avec la commande useradd sur le serveur, on doit ensuite régénérer les maps pour que cet utilisateur soit connu des clients.

4.2.3 La Configuration d'un serveur NIS

Installation et définition du domaine

NIS fonctionne avec des domaines. Un domaine NIS est simplement un nom qui regroupe un ensemble de machines. Par exemple, on pourrait avoir un domaine école pour les ordinateurs d'une école, et un domaine recherche pour les laboratoires.

Exemple

Mise en place d'un serveur NIS pour un petit laboratoire
Sur le serveur, on installe les paquets nécessaires. Sous Debian ou Ubuntu :
sudo apt install nis
Pendant l'installation, on nous demande le nom du domaine NIS. Nous allons utiliser laboratoire.
Ensuite, on indique que cette machine sera serveur. Pour cela, on édite /etc/default/nis et on modifie la ligne :
NISSERVER=master\par Enfin, on génère les maps pour la première fois :
cd /var/yp

La Configuration d'un client NIS

Sur un client qui veut utiliser le serveur NIS, la configuration est encore plus simple. On installe le paquet nis, on indique le même nom de domaine (laboratoire), et on spécifie l'adresse du serveur.

Le client doit ensuite savoir qu'il doit interroger NIS pour les comptes utilisateurs. Cela se configure dans le fichier /etc/nsswitch.conf. Ce fichier détermine l'ordre dans lequel les différentes sources d'information sont consultées.

Exemple

Configuration du fichier nsswitch.conf
Pour que les comptes soient d'abord cherchés localement puis sur NIS, on configure :
passwd : compat nis
group : compat nis
shadow : compat nis
Avec cette configuration, quand un utilisateur tente de se connecter, le système vérifie d'abord dans /etc/passwd local. Si l'utilisateur n'est pas trouvé, il interroge le serveur NIS.

2. La particularité de NIS est d'être stateless : le serveur ne garde aucune information sur l'état des connexions. Chaque requête est indépendante. Cela simplifie la conception mais limite certaines fonctionnalités.

Les limites de NIS

NIS est une technologie ancienne où la sécurité est totalement absente. Les mots de passe circulent en clair sur le réseau. Toute personne capable de capturer le trafic peut intercepter les mots de passe. La map passwd.byuid qui contient les mots de passe cryptés est accessible à n'importe quel client. Un attaquant peut récupérer cette map et tenter de casser les mots de passe hors ligne. Il n'y a pas non plus d'authentification du serveur. Un attaquant peut installer un faux serveur NIS et usurper l'identité du vrai serveur. Les clients ne peuvent pas faire la différence.

Important

NIS est à éviter sur des réseaux non sécurisés.

4.3 Le Server Message Block SMB

4.3.1 La solution universelle

SMB (Server Message Block) est un protocole développé par IBM dans les années 1980, puis largement étendu par Microsoft. C'est aujourd'hui le protocole de partage standard dans Windows, mais grâce à un logiciel appelé Samba, il fonctionne aussi parfaitement sur Linux.

Contrairement à NFS qui s'est développé dans le monde Unix, SMB a été conçu dès l'origine pour être riche en fonctionnalités. Il gère non seulement les fichiers, mais aussi les imprimantes, les communications entre processus, et même des fonctionnalités avancées comme les notifications de changement de répertoire.

4.3.2 L'évolution de SMB

SMB a connu plusieurs versions, et il est important de connaître les différences car certaines versions anciennes sont dangereuses.

SMB 1.0 est la version historique, aussi appelée CIFS (Common Internet File System). Elle est extrêmement vulnérable. Le ver WannaCry de 2017 a utilisé une faille de SMB 1.0 pour se propager dans le monde entier.

SMB 2.0 est apparue avec Windows Vista en 2006. Elle a réduit le nombre de commandes (de plus d'une centaine à une vingtaine), ce qui a simplifié le protocole et amélioré les performances.

SMB 3.0 est la version moderne, introduite avec Windows 8 et Windows Server 2012. Elle apporte le chiffrement AES, la prise en charge de multiples canaux réseau, et la tolérance aux pannes [3].

4.3.3 Le Partage d'un dossier avec SMB sous Windows

Sur Windows, partager un dossier est une opération graphique simple, mais il est utile de connaître les commandes PowerShell pour automatiser.

Exemple

Création d'un partage SMB sur Windows Server
Pour créer un partage appelé Donnees qui donne accès au dossier D :\backslash Partages\backslash Donnees :
New-SmbShare -Name "Donnees" -Path "D :\Partages\
Donnees" -FullAccess "DOMAINE\Administrateur" -
ChangeAccess "DOMAINE\Utilisateurs"
Cette commande donne un accès total à l'administrateur, et un accès en modification (lecture, écriture, suppression) aux utilisateurs du groupe Utilisateurs.
Pour désactiver l'ancien protocole SMB 1.0, ce qui est fortement recommandé :
Set-SmbServerConfiguration -EnableSMB1Protocol $false

4.4 SMB sur Linux via Samba :

Samba est un logiciel libre qui implémente le protocole SMB sur les systèmes Unix et Linux. Il permet à une machine Linux de servir des fichiers à des clients Windows, mais aussi à des clients Linux.

3. Sur les systèmes modernes, SMB 3.1.1 (introduit avec Windows 10) est la version recommandée. Elle améliore encore la sécurité avec une authentification renforcée et un chiffrement par défaut.

4.4.1 Le fichier de configuration smb.conf

Toute la configuration de Samba se trouve dans un fichier appelé /etc/samba/smb.conf. Ce fichier est divisé en sections. Une section [global] pour les paramètres généraux, puis une section par partage.

Exemple

Partage Samba
Voici un fichier smb.conf pour partager le répertoire /var/partage :
[global]
workgroup = BUREAU
server string = Serveur de fichiers
security = user
[documents]
path = /var/partage
browsable = yes
read only = no
guest ok = no
valid users = mohamed, said

Ce partage s'appelle documents. Il est accessible depuis le réseau. Seuls les utilisateurs mohamed et said peuvent s'y connecter. Ils ont le droit de lire et d'écrire.

Pour que cela fonctionne, il faut aussi créer des comptes Samba pour ces utilisateurs :

Exemple

sudo smbpasswd -a mohamed
sudo smbpasswd -a said

4.4.2 Accéder à un partage SMB depuis Linux

Pour accéder à un partage SMB depuis Linux, on utilise la commande `smbclient` ou on monte le partage avec `mount`.

Exemple

Montage d'un partage SMB
Supposons qu'un serveur Windows à l'adresse 192.168.1.50 partage un dossier appelé `PartagePublic`.
Pour le monter sur Linux :

```
sudo mount -t cifs //192.168.1.50/PartagePublic /mnt/smb -o username=mohamed,
    password=secret
```

Pour un montage automatique au démarrage, on ajoute une ligne dans `/etc/fstab` :

```
//192.168.1.50/PartagePublic  /mnt/smb  cifs  username=mohamed,password=secret,
    uid=1000,gid=1000  0  0
```

4.4.3 Comparatif entre SMB vs NFS

Le choix entre SMB et NFS dépend de votre environnement.
Dans un environnement **purement Linux**, NFS est souvent plus simple à mettre en œuvre et offre de meilleures performances. Il s'intègre naturellement avec les droits Unix.
Dans un environnement **mixte** avec des clients Windows et Linux, SMB est la solution évidente. Tous les clients Windows le comprennent nativement, et Samba fonctionne parfaitement sur Linux.
Dans un environnement **purement Windows**, le partage SMB natif est bien sûr la solution à utiliser.
Pour la **sécurité**, SMB 3.0 est supérieur à NFS version 3. NFS version 4 rattrape son retard avec le support de Kerberos et du chiffrement, mais sa configuration est plus complexe.

4.5 Conclusion

▷ Si tous les clients sont sous Linux et que le réseau est sécurisé : utiliser NFSv4

▷ Si les clients sont sous Windows ou si on a besoin de sécurité : utiliser SMB 3.0
▷ Si on a besoin d'un annuaire utilisateur : ne pas utiliser NIS, il faut utiliser LDAP ou un annuaire récent.

Chapitre 5

Services de messagerie et services d'application

5.1 Introduction aux services de messagerie

Les services de messagerie électronique constituent l'un des piliers fondamentaux des communications modernes sur Internet. Ils permettent l'échange asynchrone de messages entre utilisateurs, quels que soient leur localisation géographique ou leur fuseau horaire. Ce chapitre explore en détail les protocoles fondamentaux qui régissent le transport et la gestion des courriels, ainsi que les agents logiciels qui en assurent le bon fonctionnement.

5.2 Protocoles de messagerie

5.2.1 SMTP (Simple Mail Transfer Protocol)

Définition

SMTP est le protocole standard pour l'envoi de courriels sur Internet, défini à l'origine par la RFC 821 en 1982, puis mise à jour par la RFC 5321. Il fonctionne selon un modèle client-serveur et utilise une approche de type "push" pour transférer les messages d'un client vers un serveur ou entre serveurs de messagerie.

Architecture

L'architecture SMTP repose sur une communication en mode texte utilisant des commandes ASCII. Le client émet des commandes auxquelles le serveur répond par des codes numériques à trois chiffres.

Le processus typique d'envoi suit cette séquence :

Les commandes SMTP essentielles

EHLO/HELO : Identification du client auprès du serveur
MAIL FROM : Spécifie l'expéditeur
RCPT TO : Spécifie le(s) destinataire(s)
DATA : Indique le début du contenu du message
QUIT : Termine la session

Avantages

- ▷ Simplicité d'implémentation et de débogage
- ▷ Large compatibilité avec tous les serveurs de messagerie
- ▷ Support du relais entre serveurs (store-and-forward)
- ▷ Extensible via les commandes ESMTP

Inconvénients

- ▷ Absence native de chiffrement (vulnérabilité aux interceptions)
- ▷ Vulnérabilité au relais ouvert (open relay) et au spam
- ▷ Authentification faible dans sa version originale
- ▷ Limitation à 7 bits pour les caractères non-ASCII

5.2.2 Versions sécurisées de SMTP

SMTPS (SMTP over SSL/TLS) Utilise une couche SSL/TLS avant l'établissement de la session SMTP. Le port dédié est le **port 465** (parfois considéré obsolète au profit de STARTTLS). La sécurité est établie dès la connexion TCP.

SMTP avec STARTTLS Extension permettant de négocier une connexion chiffrée sur le port standard **587** (soumission) ou **25**. La commande STARTTLS initie le handshake TLS après l'établissement de la connexion initiale en clair.

Les ports SMTP

Protocole	Port	Utilisation
SMTP (standard)	**25**	**Transfert entre serveurs**
SMTP (soumission)	**587**	**Soumission par clients authentifiés**
SMTPS	**465**	**SMTP sur TLS (déprécié, mais utilisé)**

5.2.3 POP3 (Post Office Protocol version 3)

Définition

POP3, défini par la RFC 1939, est un protocole de "pull" permettant aux clients de messagerie de récupérer les messages stockés sur un serveur. Contrairement à SMTP qui pousse les messages, POP3 les tire vers le client.

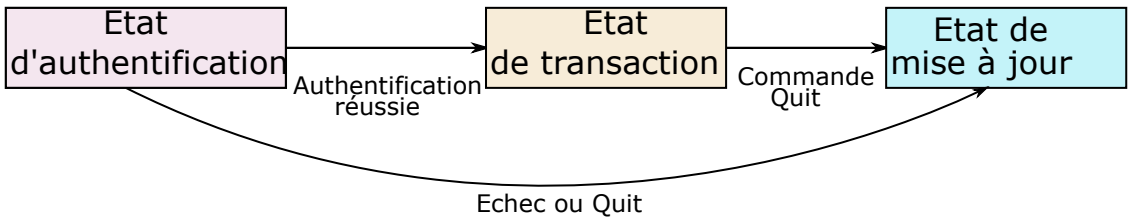


FIGURE 5.1 – Architecture POP3

Architecture

Le fonctionnement de POP3 suit un modèle simple, figure 5.1 : le client se connecte au serveur, s'authentifie, récupère les messages, puis les supprime généralement du serveur. Trois états principaux sont définis :

Avantages

- ▷ Très simple à implémenter et à configurer
- ▷ Réduction de l'utilisation d'espace disque sur le serveur
- ▷ Idéal pour les connexions intermittentes
- ▷ Faible consommation de bande passante

Inconvénients

- ▷ Gestion limitée des dossiers (un seul dossier par boite aux lettres)
- ▷ Synchronisation difficile entre plusieurs clients
- ▷ Téléchargement systématique même pour les messages déjà lus
- ▷ Perte possible des messages si sauvegarde locale insuffisante

5.2.4 Versions sécurisées de POP3

POP3S (POP3 over SSL/TLS) Utilise le port **995** pour établir une connexion chiffrée dès le départ. Toute la session, y compris l'authentification, est protégée.

POP3 avec STLS Extension similaire à STARTTLS pour SMTP, permettant d'élever la sécurité sur le port standard 110 après la connexion initiale.

5.2.5 IMAP (Internet Message Access Protocol)

Présentation théorique IMAP, actuellement en version 4 (IMAP4, RFC 3501), est un protocole de messagerie avancé qui permet une gestion distante des messages. Contrairement à POP3, les messages restent sur le serveur et peuvent être organisés dans différents dossiers.

Architecture IMAP maintient une connexion persistante entre le client et le serveur, permettant une manipulation sophistiquée des messages sans les télécharger complètement. Les fonctionnalités incluent :

Définition

IMAP, actuellement en version 4 (IMAP4, RFC 3501), est un protocole de messagerie avancé qui permet une gestion distante des messages. Contrairement à POP3, les messages restent sur le serveur et peuvent être organisés dans différents dossiers.

Architecture

IMAP maintient une connexion persistante entre le client et le serveur, permettant une manipulation sophistiquée des messages sans les télécharger complètement.

Les fonctionnalités incluent :

Fonctionnalités spécifiques à IMAP

Dossiers distants : Création, suppression et renommage de dossiers
Drapeaux d'état : Messages lus, répondus, marqués, supprimés
Téléchargement partiel : Récupération uniquement des en-têtes
Recherche côté serveur : Filtrage sans transfert de données
Accès simultané : Plusieurs clients synchronisés

Avantages

- ▷ Conservation centralisée des messages avec sauvegarde automatique
- ▷ Synchronisation parfaite entre plusieurs clients
- ▷ Gestion avancée des dossiers et du stockage
- ▷ Téléchargement efficace grâce aux fonctionnalités partielles

Inconvénients

- ▷ Nécessite une connexion plus stable et plus rapide
- ▷ Consommation d'espace serveur potentiellement importante
- ▷ Complexité d'implémentation plus élevée
- ▷ Coût de stockage pour les fournisseurs de services

5.2.6 Versions sécurisées d'IMAP

IMAPS (IMAP over SSL/TLS) Utilise le port **993** pour une connexion chiffrée immédiate.

IMAP avec STARTTLS Permet le chiffrement sur le port standard 143 après la commande STARTTLS.

5.2.7 MAPI (Messaging Application Programming Interface)

Présentation théorique MAPI est une architecture propriétaire développée par Microsoft, spécifiquement conçue pour les environnements Windows et Exchange Server. Contrairement aux protocoles standards, MAPI est une interface de programmation permettant aux applications d'interagir avec les services de messagerie.

Architecture L'architecture MAPI suit plusieurs couches telle que donnée par la figure 5.2 :

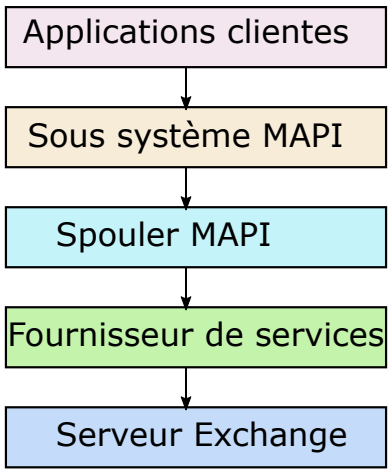


FIGURE 5.2 – Architecture MAPI

Avantages

- ▷ Intégration profonde avec Outlook et l'écosystème Microsoft
- ▷ Fonctionnalités avancées : calendriers, tâches, contacts, règles
- ▷ Performance optimisée pour Exchange
- ▷ Support du mode cache et du travail hors ligne

Inconvénients

- ▷ Propriétaire et dépendant de Microsoft
- ▷ Complexe à implémenter pour des applications tierces
- ▷ Nécessite généralement Exchange Server
- ▷ Migration difficile vers d'autres solutions

5.3 Agents de messagerie

5.3.1 MUA (Mail User Agent)

Définition et rôle

Le MUA est l'interface utilisateur finale permettant la consultation, la rédaction et l'envoi des courriels. Il interagit avec les serveurs de messagerie via SMTP (pour l'envoi) et POP3/IMAP (pour la réception).

Exemples courants

- ▷ **Graphiques** : Microsoft Outlook, Mozilla Thunderbird, Apple Mail
- ▷ **Webmails** : Gmail, Outlook.com, Roundcube
- ▷ **Console** : Mutt, Alpine, mail

Fonctionnalités typiques

Rédaction avec mise en forme (HTML/texte)
Gestion des contacts et carnets d'adresses
Filtrage et règles de tri
Recherche et indexation
Signature et chiffrement (PGP, S/MIME)

Fonctionnalités typiques

- ▷ Rédaction avec mise en forme (HTML/texte)
- ▷ Gestion des contacts et carnets d'adresses
- ▷ Filtrage et règles de tri
- ▷ Recherche et indexation
- ▷ Signature et chiffrement (PGP, S/MIME)

5.3.2 MTA (Mail Transfer Agent)

Définition et rôle

Le MTA est responsable du routage et du transfert des courriels entre serveurs. Il implémente principalement le protocole SMTP et assure la livraison des messages selon les enregistrements DNS MX (Mail Exchange).

Exemples courants

- ▷ Postfix (populaire, sécurisé)
- ▷ Sendmail (historique, complexe)
- ▷ Exim (configurable)
- ▷ Microsoft Exchange (intégré)

Fonctionnalités essentielles

Réception des messages depuis les MUA ou autres MTA
Résolution DNS des domaines destinataires
Résolution DNS des domaines destinataires
Routage vers le MTA approprié
File d'attente (queue) en cas d'indisponibilité
Tentatives de livraison multiples avec backoff exponentiel
NDR (Non-Delivery Reports) en cas d'échec définitif

5.3.3 MDA (Mail Delivery Agent)

Définition et rôle

Le MDA reçoit les messages du MTA et les dépose dans la boite aux lettres appropriée de l'utilisateur. Il peut également appliquer des filtres et effectuer des transformations.

Exemples courants

- ▷ Dovecot (avec IMAP/POP3)
- ▷ Procmail (filtrage avancé)
- ▷ Maildrop
- ▷ Cyrus

Fonctionnalités

Dépôt dans différents formats (mbox, Maildir)
Filtrage et tri automatique (procmail)
Vérification anti-spam et anti-virus
Gestion des quotas f

5.4 Schéma de transmission d'un courriel

Détail des étapes est représenté par la figure 5.3.

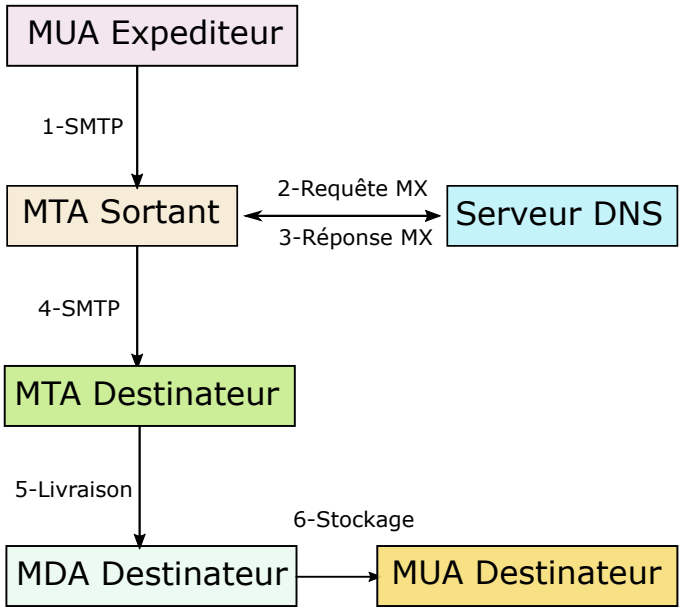


FIGURE 5.3 – Schéma de transmission d'un courriel

1. **Rédaction et envoi** : L'utilisateur rédige son message dans le MUA qui le transmet au MTA sortant via SMTP (port 587 généralement).
2. **Résolution MX** : Le MTA sortant interroge le DNS pour obtenir l'enregistrement MX du domaine destinataire.
3. **Routage** : Le MTA sortant établit une connexion SMTP avec le MTA destinataire.
4. **Transfert** : Le message est transféré au MTA destinataire qui vérifie sa validité.
5. **Livraison locale** : Le MTA destinataire remet le message au MDA.
6. **Dépôt** : Le MDA dépose le message dans la boite aux lettres de l'utilisateur.
7. **Consultation** : L'utilisateur récupère le message via POP3 (port 110/995) ou IMAP (port 143/993).

5.5 Introduction aux protocoles de transfert de fichiers

Les protocoles de transfert de fichiers sont des éléments fondamentaux de l'architecture des réseaux IP. Ils permettent l'échange structuré de données entre systèmes distants, que ce soit sur un réseau local ou à travers Internet. Les domaines d'applications peuvent être très variés tels que l'administration système, le développement logiciel, la sauvegarde de données, ou encore la distribution de contenu.
Les quatre protocoles majeurs qui ont marqué l'évolution des transferts de fichiers seront étudiés dans ce chapitre. Le FTP (File Transfer Protocol), créé en 1985, est l'ancêtre de tous les protocoles de transfert. Le TFTP (Trivial File Transfert Protocol) est une version allégée conçue pour les systèmes embarqués. Enfin, nous aborderons les versions sécurisées : le FTPS (FTP over SSL/TLS) et le SFTP (SSH File Transfer Protocol), ce dernier étant aujourd'hui la référence pour les transferts sécurisés sur Internet.

5.5.1 Le protocole FTP (File Transfer Protocol)

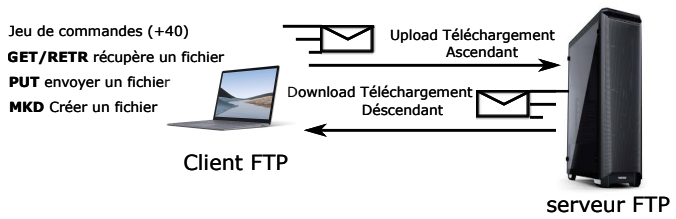


FIGURE 5.4 – Architecture client/Serveur FTP

Le FTP, défini dans la RFC 959, est historiquement le premier protocole standardisé pour le transfert de fichiers sur un réseau TCP/IP. Il fonctionne selon un modèle client-serveur et présente une particularité architecturale importante : l'utilisation de deux canaux de communication distincts. Le canal de commande,

établi sur le port 21, transporte les instructions et les réponses du serveur. Le canal de données, généralement sur le port 20, assure le transfert effectif des fichiers. Cette séparation permet une gestion plus efficace des transferts, mais complexifie la configuration des pare-feu. Dans ce cas on parle de mode actif tel que donné sur la figure 5.5. Afin d'éviter le problème de blocage par le firewall, le **mode passif** est utilisé. Dans ce cas le download est initié par le client FTP en attribuant un port aléatoire au serveur FTP qui ouvre de son coté un port aléatoire au lieu du port 20.

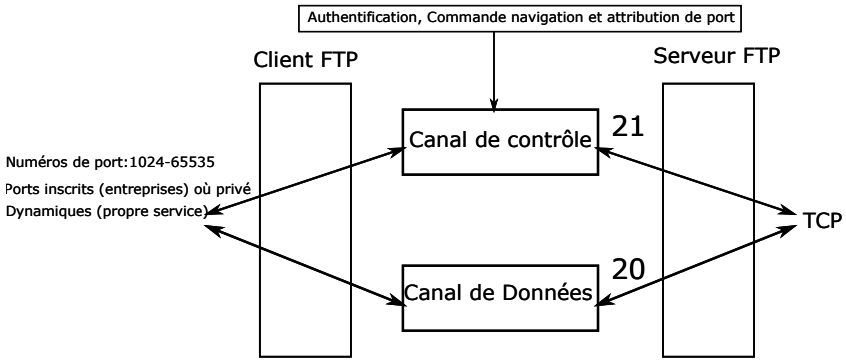


FIGURE 5.5 – FTP, mode actif

Étape 1 : le déclenchement du processus PI

Le déclenchement du processus client PI qui dialogue avec le serveur PI figure 5.6. Dans ce cas de figure, le canal de contrôle gère les commandes (cmd). Cette étape débute par une séquence d'initialisation, qui se déroule immédiatement après l'établissement de la connexion TCP sur le port 21, comprend plusieurs étapes obligatoires. Le serveur commence par envoyer un message de bienvenue (code 220) pour signaler sa disponibilité. Le client doit alors fournir un nom d'utilisateur via la commande USER, puis un mot de passe avec la commande PASS. Le serveur valide ces informations d'authentification et retourne un code 230 en cas de succès, ou un code d'erreur dans le cas contraire. Finalement le client PI doit :

- ▷ Initier la connexion n avec le serveur PI (créer le canal de contrôle)
- ▷ Envoyer les commandes FTP.
- ▷ Recevoir les réponses du serveur PI (qui peuvent être positives ou négatives).

Quelques commandes : Get/RETR (Retrieve) demande d'une copie d'un fichier au serveur FTP.
STOR demander, accepter les données envoyées sur le canal de données et les stocker dans un fichier.
REST (restart) reprendre le transfert là où il s'était arrêté.
TYPE précise le format de données.
PUT envoyer un fichier
MKD créer un répertoire
Close terminer la session FTP
Quit Quitter

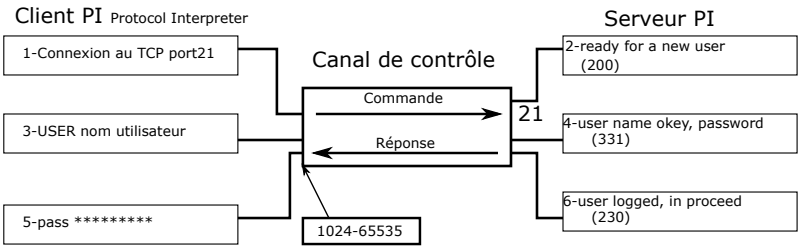


FIGURE 5.6 – Étape PI

Analyse de la séquence d'authentification FTP

La séquence d'authentification FTP illustrée par la figure 5.6 suit un schéma précis de requête-réponse qui garantit une communication fiable entre le client et le serveur. Chaque commande envoyée par le client doit

être acquittée par le serveur avant de passer à l'étape suivante. Le code 220 initial confirme que le serveur est opérationnel et prêt à accepter des commandes. La réponse 331 indique que le nom d'utilisateur est valide et que le mot de passe est attendu. Enfin, le code 230 valide le succès de l'authentification. Cette séquence gère également des cas particuliers comme les comptes sans mot de passe ou les tentatives d'authentification échouées.

Etape2 : Le processus Data Server Protocol (DTP)

Le Data Server Protocol représenté par la figure 5.7 est, responsable du transfert effectif des données. Il est déclenché par le client DTP afin d'échanger avec le serveur DTP. Un canal de données est créé (communication) celui-ci ne permet que le transfert de données. A chaque transfert de données , il faut créer un canal de données permettent le transfert dans les deux sens. Une fois le fichier transféré, le canal est détruit et les deux processus responsables de la création du canal arrivent à fin discussion.

Si le client veut télécharger/déposer un fichier il doit passer par une autre session (étape 2).

Si le client veut terminer, il utilise QUIT et le canal de commande est lui aussi supprimé.

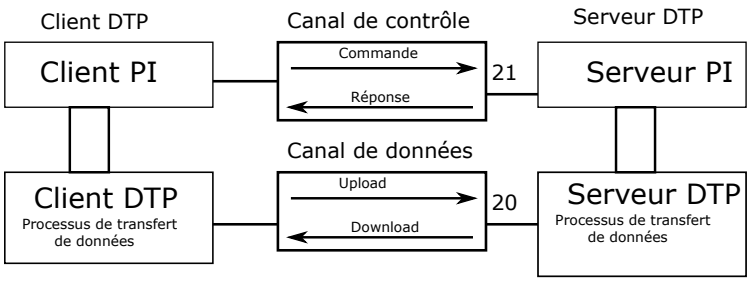


FIGURE 5.7 – Processus DTP en mode actif. Dans le mode passif le port DTP est remplacé par un port aléatoire.

5.5.2 Les modes de transfert FTP

Le choix entre mode actif et mode passif a des implications importantes sur la configuration réseau. Le mode actif, le plus ancien historiquement, pose problème lorsque le client est protégé par un pare-feu, car celui-ci doit accepter une connexion entrante du serveur. Le mode passif inverse les rôles : c'est le client qui initie toutes les connexions, ce qui est beaucoup plus compatible avec les politiques de sécurité modernes. La plupart des clients FTP modernes essayent d'abord le mode passif et basculent en mode actif si nécessaire. En mode actif, après avoir reçu la commande de transfert, le client ouvre un port d'écoute et communique son numéro au serveur via la commande PORT. Le serveur initie alors une connexion depuis son port 20 vers ce port client. En mode passif, développé pour pallier les problèmes de pare-feu, le client envoie la commande PASV. Le serveur ouvre alors un port aléatoire, communique ses coordonnées au client, et c'est ce dernier qui initie la connexion de données.

5.5.3 Le protocole TFTP (Trivial File Transfer Protocol)

Présentation et caractéristiques techniques

Le TFTP, normalisé dans la RFC 1350, conçu pour être extrêmement simple à implémenter, il sacrifie de nombreuses fonctionnalités au profit de la légèreté. Contrairement au FTP, il utilise le protocole UDP (port 69) plutôt que TCP, ce qui le rend non fiable. Chaque paquet de données doit être acquitté individuellement, et des mécanismes de timeout gèrent les pertes éventuelles.

Caractéristique	**FTP**	**TFTP**
Port	21-20	69
Transport	TCP (fiable)	UDP (non fiable)
Authentification	Oui	Non
Listing répertoire	Oui (LIST)	Non
Taille fichier max	Illimitée	32 Mo
Commandes	40+	5 seulement

TABLE 5.1 – Analyse comparative des protocoles FTP et TFTP.

Mécanisme du transfert TFTP

Le mécanisme de transfert du TFTP est une illustration du protocole "stop-and-wait". Pour chaque paquet de données envoyé, l'émetteur attend un acquittement avant de transmettre le suivant. Cette approche garantit l'intégrité des données dans un environnement non fiable. Le transfert débute toujours par une requête de lecture RRQ (Read Request) ou d'écriture WRQ (Write Request). Les données sont segmentées en blocs de 512 octets, sauf le dernier qui est plus petit et signale la fin du transfert. Un exemple de transfert avec numérotation d'un fichier de 1500 octets est donné ci après :

Client (demande) → RRQ (fichier.txt)
Serveur→ DATA #1 (512 octets, positions 0-511)
Client → ACK #1
Serveur → DATA #2 (512 octets, positions 512-1023)
Client → ACK #2
Serveur → DATA #3 (476 octets, positions 1024-1499) ← DERNIER PAQUET
Client → ACK #3 Fin du transfert

On remarque facilement la simplicité du mécanisme du TFTP illustré ci-dessus. Chaque paquet de données est numéroté séquentiellement, et l'acquittement correspondant permet à l'émetteur de savoir quel bloc a été correctement reçu. En cas de perte, un timeout déclenche la retransmission. La terminaison du transfert est détectée lorsque la taille d'un paquet DATA est inférieure à 512 octets. Il est à signaler que le téléchargement n'est pas sécurisé d'où la nécessité de l'utiliser strictement en réseaux LAN. Aussi, il est préférable de l'utiliser pour le transfert de fichiers peu volumineux.

5.5.4 Les protocoles sécurisés : FTPS et SFTP

FTPS (FTP over SSL/TLS) - Architecture et fonctionnement

Le FTPS représente une évolution naturelle du FTP pour répondre aux exigences de sécurité modernes. Il ajoute une couche de chiffrement SSL/TLS soit immédiatement (mode implicite), soit après négociation (mode explicite). En mode implicite, la connexion est chiffrée dès l'établissement sur le port 990. En mode explicite, le client se connecte d'abord sur le port 21 en clair, puis demande le basculement vers TLS via la commande AUTH TLS ou bien AUTH SSL et PROT P (PROT P (Private) le canal de données est entièrement chiffré (figure5.8). Le FTPS apporte une sécurité renforcée grâce au chiffrement TLS/SSL, mais conserve la complexité architecturale du FTP. Dans ce cas, le serveur présente systématiquement un certificat pour prouver son identité, et le client peut optionnellement présenter le sien pour une authentification mutuelle. Le chiffrement protège à la fois les identifiants de connexion et les données transférées contre l'espionnage.

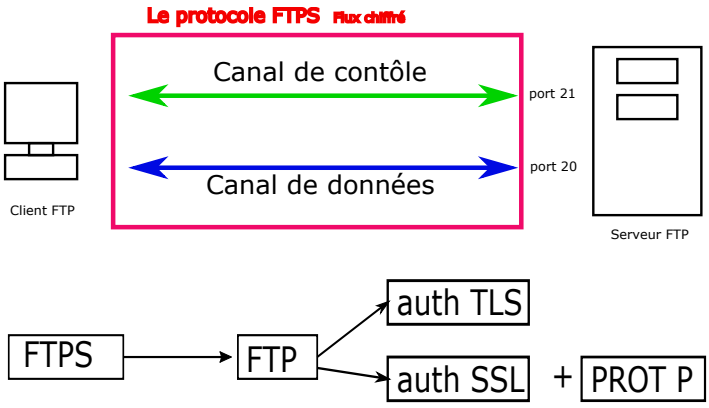


FIGURE 5.8 – Protocole FTPS

SFTP (SSH File Transfer Protocol) - Encapsulation dans un tunel SSH

Le SFTP est différent du FTPS : il ne s'agit pas d'une extension du FTP, mais d'un protocole complètement nouveau, conçu comme une extension du protocole SSH (Secure Shell). Il utilise un canal unique sur le port 22, déjà sécurisé par SSH, pour toutes les opérations : commandes, transferts de données, gestion de fichiers. Cette simplicité architecturale élimine les problèmes de pare-feu et simplifie grandement le déploiement. L'intégration avec SSH, telle que illustrée par la figure 5.9 apporte plusieurs avantages décisifs : canal unique simplifiant la configuration réseau, sécurité native robuste, authentification forte par clés publiques, et support des fonctionnalités avancées comme la reprise de transfert. C'est pourquoi SFTP est devenu un standard pour l'administration système et les échanges de fichiers sensibles.

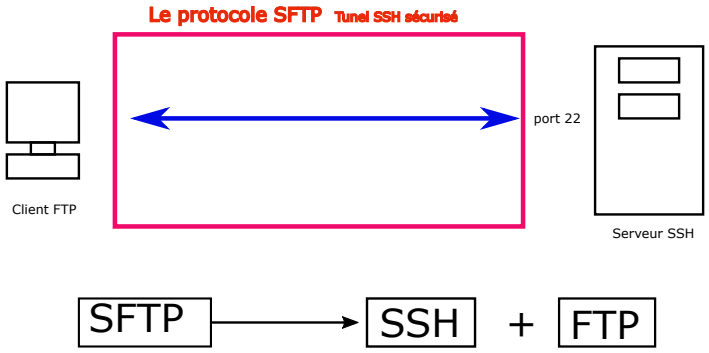


FIGURE 5.9 – Le protocole SFTP

5.5.5 Tableau comparatif exhaustif

Critère	**FTP**	**TFTP**	**FTPS**	**SFTP**
Ports	21,20	69	21/990,20/989	22
Transport	TCP	UDP	TCP+TLS	TCP+SSH
Canaux	2 séparés	1 unique	2 séparés sécurisés	1 unique sécurisé
Auth	Login/Pwd	Aucune	Login/Pwd/Certs	Clés SSH
Chiffrement	Non	Non	TLS/SSL	SSH
Listing répertoire	Oui (LIST)	Non	Oui (LIST)	Oui (ls)
Reprise transfert	Oui (REST)	Non	Oui	Oui
Compatibilité firewall	Difficile	Facile	Complexe	Très facile
Performance	Bonne	Médiocre	Moyenne	Bonne

TABLE 5.2 – Comparaison technique complète des quatre protocoles de transfert de fichiers.

5.6 Conclusion

L'évolution des protocoles de transfert de fichiers illustre parfaitement la maturation d'Internet. Du FTP non sécurisé au SFTP intégrant la sécurité comme fondation, en passant par le TFTP pour l'embarqué et le FTPS comme solution de transition, chaque protocole a sa place. actuellement, SFTP est le protocole à adopter, offrant le meilleur compromis entre sécurité, fonctionnalités et facilité de déploiement.

Chapitre 6

Les Contrôleurs de Domaine

6.1 Introduction

Dans une infrastructure réseau d'entreprise, la gestion centralisée des utilisateurs, des ordinateurs et des ressources est un défi majeur. Les contrôleurs de domaine (Domain Controllers - DC) constituent la pierre angulaire de cette gestion centralisée. Ils permettent d'authentifier les utilisateurs, d'appliquer des politiques de sécurité et de gérer les ressources partagées.

6.2 Présentation des contrôleurs de domaine

Définition

Un contrôleur de domaine est un serveur qui héberge une base de données d'annuaire contenant tous les objets du domaine : utilisateurs, groupes, ordinateurs, imprimantes, et autre équipements. Il assure trois fonctions principales :

- ▷ **Authentification** : Vérification des identifiants des utilisateurs
- ▷ **Autorisation** : Attribution des droits d'accès
- ▷ **Réplication** : Synchronisation avec les autres contrôleurs

6.2.1 Avantages

- ▷ Centralisation de la gestion
- ▷ Sécurité renforcée
- ▷ Redondance et tolérance aux pannes
- ▷ Évolutivité

6.2.2 Historique et évolution

Le tableau 6.1 résume l'évolution des contrôleurs de domaine.

Version	**Caractéristiques**
Windows NT 4.0	Premier domaine, PDC/BDC
Windows 2000	Active Directory, DNS intégré
Windows Server 2003	Forêts à plusieurs domaines
Windows Server 2008	Read-Only DC (RODC)
Windows Server 2016+	Privilège Access Management, PAM

Table 6.1 – Évolution des contrôleurs de domaine

6.3 Architecture des contrôleurs de domaine

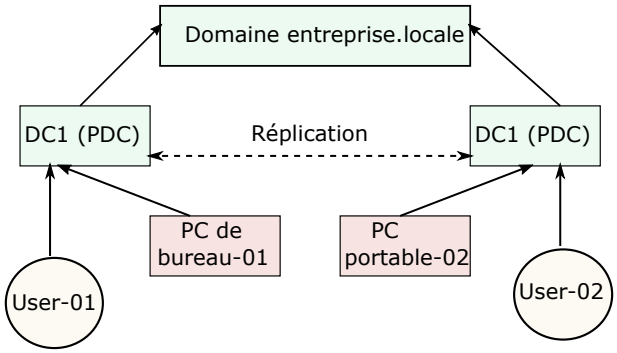


FIGURE 6.1 – Architecture typique d'un domaine avec deux contrôleurs

La figure 6.1 présente l'architecture classique d'un domaine Active Directory nommé `entreprise.local`. Cette structure repose sur plusieurs composants interconnectés :

- ▷ **Le domaine** : représenté par le bloc `entreprise.local`, il constitue l'unité administrative et sécuritaire principale. Il contient l'ensemble des objets (utilisateurs, ordinateurs, ressources) et définit une frontière de sécurité commune.
- ▷ **Les contrôleurs de domaine** : deux serveurs (DC1 et DC2) assurent la redondance et la haute disponibilité.
  - — **DC1 (PDC)** : contrôleur primaire (Primary Domain Controller) qui joue un rôle spécial dans la synchronisation horaire, le verrouillage des comptes et la résolution des conflits de réplication.
  - — **DC2 (Backup)** : contrôleur secondaire qui prend le relais en cas de panne du primaire et participe à la distribution de la charge d'authentification.
- ▷ **La réplication** : est le mécanisme qui garantit que toute modification effectuée sur un contrôleur (création d'utilisateur, modification de mot de passe, etc.) est automatiquement synchronisée vers l'autre. La fonction de réplication doit être :
  1. *multidirectionnelle* : chaque contrôleur peut initier une synchronisation
  2. *rapide* : les modifications critiques sont propagées en quelques secondes
  3. *cohérente* : utilise des numéros de version pour résoudre les conflits
- ▷ **Les utilisateurs** : User-01 et User-02 sont des comptes d'utilisateurs authentifiés. Leur flèche vers les contrôleurs symbolise la demande d'authentification. Ils peuvent se connecter indifféremment à l'un ou l'autre contrôleur grâce à la réplication.
- ▷ **Les postes de travail** : PC-Bureau-01 et PC-Portable-01 sont des ordinateurs membres du domaine. Ils rejoignent également le domaine et bénéficient des politiques de sécurité appliquées par les contrôleurs.

Fonctionnement typique :

- ▷ Un utilisateur (ex : User-01) saisit ses identifiants sur son poste (PC-Bureau-01)
- ▷ Le poste interroge le contrôleur DC1 pour valider l'authentification
- ▷ DC1 vérifie dans sa base Active Directory les informations d'Alice
- ▷ En cas de succès, DC1 délivre un ticket Kerberos permettant à Alice d'accéder aux ressources autorisées
- ▷ Si DC1 est indisponible, le poste bascule automatiquement vers DC2

Avantages de cette architecture :

- ▷ **Tolérance aux pannes** : la panne d'un contrôleur n'interrompt pas le service
- ▷ **Équilibrage de charge** : les authentifications sont réparties entre les deux serveurs
- ▷ **Maintenance sans interruption** : on peut mettre à jour un contrôleur pendant que l'autre reste actif
- ▷ **Répartition géographique** : chaque site distant peut avoir son propre contrôleur

Cette architecture constitue la base de toute infrastructure Active Directory professionnelle. Quelque soit la taille d'un domaine, il est recommandé d'avoir au moins deux contrôleurs.

6.3.1 Arborescence et hiérarchie

L'arborescence des domaines représente une structure hiérarchique utilisant le système de noms de domaine (DNS) vu au chapitre 2. La figure 6.2 illustre la structure hiérarchique d'une arborescence de domaines au sein

d'une forêt Active Directory. Cette arborescence s'appuie sur le système de noms de domaine (DNS) pour établir une organisation logique et hiérarchique des entités.

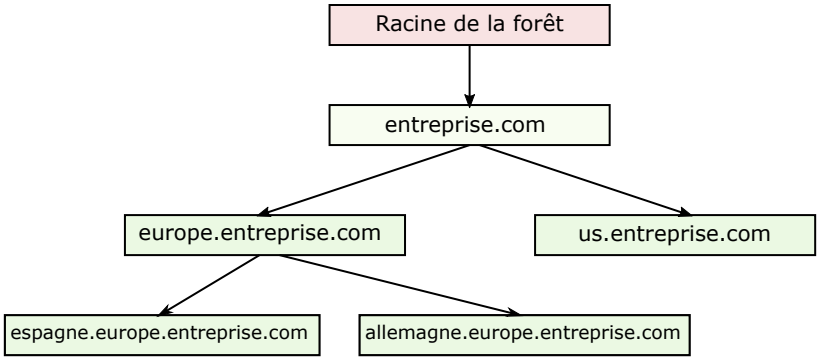


FIGURE 6.2 – Arborescence de domaines

Structure hiérarchique :

- ▷ À la racine de l'arborescence se trouve la `Racine de la forêt`. Cette racine est le point de départ de l'arborescence et représente le niveau le plus élevé de la hiérarchie. Tous les autres domaines sont des descendants de cette racine.
- ▷ Le domaine parent `entreprise.com` constitue le premier niveau de l'arborescence. Il s'agit du domaine racine de l'organisation, souvent appelé *domaine racine de la forêt* (forest root domain). Tous les autres domaines lui sont rattachés directement ou indirectement.
- ▷ Les domaines enfants `europe.entreprise.com` et `usa.entreprise.com` représentent le deuxième niveau hiérarchique. Ils héritent de la configuration et des approbations de leur domaine parent.
- ▷ Les domaines `espagne.europe.entreprise.com` et `allemagne.europe.entreprise.com` constituent le troisième niveau de l'arborescence. Ils sont rattachés au domaine `europe.entreprise.com` et illustrent la possibilité d'étendre l'arborescence sur plusieurs niveaux.

Particularités de cette structure :

1. Relations parent-enfant : Chaque flèche dans la figure représente une relation d'approbation transitive bidirectionnelle entre un domaine parent et son domaine enfant. Cette relation permet aux utilisateurs d'un domaine enfant d'accéder aux ressources du domaine parent, et vice-versa.
2. Héritage du nom DNS : Le nom de chaque domaine reflète sa position dans l'arborescence. Par exemple, `allemagne.europe.entreprise.com` indique que ce domaine se trouve dans la branche `europe` de l'organisation `entreprise.com`.
3. Contiguïté des noms : Une arborescence de domaines est dite *contigüe* car les noms des domaines enfants contiennent le nom complet de leur domaine parent. Cette propriété est essentielle pour le fonctionnement du DNS et des approbations automatiques.

Implications pratiques : Cette organisation hiérarchique permet de :

- ▷ Décentraliser l'administration : chaque domaine peut avoir ses propres administrateurs
- ▷ Appliquer des politiques de groupe différenciées selon les branches géographiques ou fonctionnelles
- ▷ Isoler des problèmes de réplication au sein d'une branche spécifique
- ▷ Refléter la structure organisationnelle ou géographique de l'entreprise

Exemple concret : Une entreprise espagnole implantée en Europe et aux États-Unis pourrait structurer son Active Directory comme suit :

entreprise.com (siège social)
⌈ ⟶europe.entreprise.com (direction Europe)
| ⌈ ⟶espagne.europe.entreprise.com (agence Espagne)
| ⌊ ⟶allemagne.europe.entreprise.com (agence Allemagne)
⌊ ⟶usa.entreprise.com (direction Amerique du Nord)

Cette structure facilite la gestion des ressources locales tout en maintenant une cohérence globale au niveau de l'entreprise.

6.3.2 Forêt

Une forêt est un ensemble de domaines qui partagent :

- ▷ Un schéma d'annuaire commun
- ▷ Une configuration commune
- ▷ Une confiance transitive automatique

▷ Un catalogue global (Global Catalog)

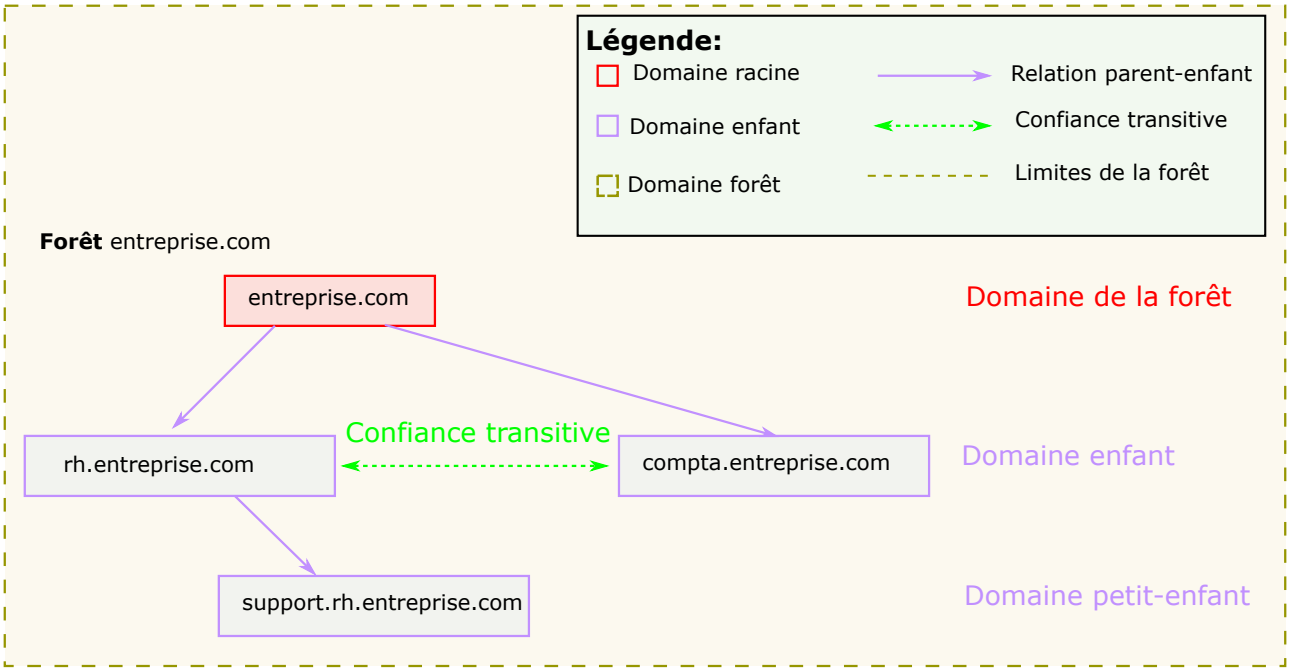


FIGURE 6.3 – Structure d'une forêt Active Directory

La figure 6.3 présente une forêt Active Directory nommée `entreprise.com`, qui constitue le conteneur logique de plus haut niveau. À l'intérieur de cette forêt, on distingue plusieurs domaines organisés hiérarchiquement :

- ▷ **Domaine racine** : `entreprise.com` — C'est le domaine parent de la forêt, créé en premier. Il contient les rôles FSMO [1] (Flexible Single Master Operations) au niveau forêt (Schema Master et Domain Naming Master).
- ▷ **Domaines enfants directs** :
  - — `rh.entreprise.com` (Ressources Humaines)
  - — `compta.entreprise.com` (Comptabilité)

  Ces domaines héritent automatiquement d'une relation d'approbation transitive bidirectionnelle avec le domaine parent.
- ▷ **Domaine petit-enfant** : `support.rh.entreprise.com` — Sous-domaine du domaine RH, illustrant la profondeur possible de l'arborescence (jusqu'à plusieurs niveaux).

En synthèse :

1. **Approbation transitive** : La flèche en pointillés entre `rh.entreprise.com` et `compta.entreprise.com` symbolise une confiance transitive automatique. Cela signifie que les utilisateurs du domaine RH peuvent accéder aux ressources du domaine Comptabilité, et vice-versa, sans configuration manuelle.
2. **Catalogue global (Global Catalog)** : Tous les domaines d'une même forêt partagent un catalogue global qui contient une copie partielle de tous les objets de la forêt, facilitant les recherches inter-domaines.
3. **Schéma unique** : Toute modification du schéma (ajout d'attributs, classes) s'applique à l'ensemble de la forêt via le Schema Master.
4. **Sécurité isolée** : Malgré les approbations automatiques, chaque domaine conserve ses propres administrateurs et politiques de sécurité.

Exemple

Un utilisateur du domaine `support.rh.entreprise.com` peut accéder à une imprimante située dans le domaine `compta.entreprise.com` sans qu'aucune approbation supplémentaire ne soit configurée, grâce à la transitivité des approbations (`support` → `rh` → `entreprise.com` → `compta`).

1. Dans un environnement multi-maîtres standard, tous les contrôleurs peuvent théoriquement modifier la base AD. Cependant, certaines opérations pourraient causer des conflits si plusieurs contrôleurs les effectuaient simultanément. Les rôles FSMO évitent ces conflits en centralisant ces opérations critiques sur un seul contrôleur.

Limites et considérations

- ▷ Profondeur maximale : Une arborescence peut contenir jusqu'à plusieurs niveaux, mais la performance peut diminuer au-delà de 5-6 niveaux
- ▷ Nombre de domaines : Une forêt peut contenir jusqu'à 1 200 domaines (limite théorique)
- ▷ Séparation administrative : Pour une séparation stricte (ex : filiales indépendantes), on doit privilégier des forêts distinctes avec des approbations explicites.

6.4 Gestion des utilisateurs, des groupes et permissions

6.4.1 Unités d'organisation (OU)

Les Unités d'Organisation permettent de structurer logiquement les objets d'un domaine.

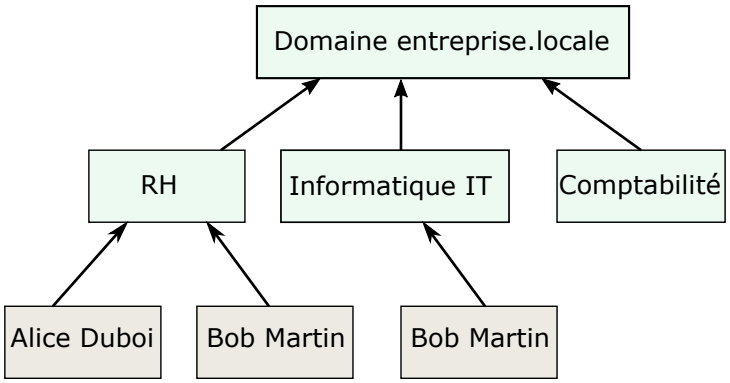


FIGURE 6.4 – Structure de l'OU (Organization Unit)

La hiérarchie fondamentale d'Active Directory illustrée par la figure 6.4 Résume comment un Domaine contient des OU, et les OU contiennent des Utilisateurs. Ce Concept est basé sur :
a) **Hiérarchisation :** La structure montre un arbre à 3 niveaux :

- ▷ Niveau 1 : Domaine
- ▷ Niveau 2 : Unités d'Organisation
- ▷ Niveau 3 : Utilisateurs (objets)

b) **Délégation administrative implicite :** Cette organisation permet de :

- ▷ Déléguer la gestion des mots de passe des utilisateurs RH au responsable RH
- ▷ Appliquer des stratégies de groupe différentes selon l'OU
- ▷ Isoler les politiques de sécurité par département

c) **Regroupement logique vs physique :** Les utilisateurs sont regroupés par fonction (leur service), pas par leur localisation physique. C'est un regroupement logique.

6.4.2 Types de groupes

Type	**Portée**	**Utilisation**
Local au domaine	Domaine uniquement	Attribution des permissions sur les ressources locales
Global	Domaine uniquement	Regroupement d'utilisateurs du même domaine
Universel	Toute la forêt	Regroupement d'utilisateurs de domaines différents

TABLE 6.2 – Types de groupes sous Active Directory

Le tableau6.2 les différents types de groupes.

6.4.3 Le modèle AGDLP pour la gestion des permissions

Le modèle **AGDLP** est une pratique d'administration d'Active Directory pour la gestion des permissions. Il a été créé par Microsoft pour simplifier l'administration des accès dans les environnements en domaine. Son

acronyme est décrit par le tableau 6.3. Il repose sur une chaîne d'imbrication à sens unique tel que montré par la figure 6.5 :

Lettre	Signification	Anglais	Rôle
A	Comptes	Accounts	Les utilisateurs
G	Global	Global	Groupes globaux
D	Local au domaine	Domain Local	Groupes locaux au domaine
L	Local	Local	Groupes locaux (sur la ressource)
P	Permissions	Permissions	Attribution des droits

TABLE 6.3 – Signification de l'acronyme AGDLP et son rôle

Remarque : Une variante courante est **AGDLP** (sans le L final explicite) où le "Domain Local" joue directement le rôle d'attribution des permissions.

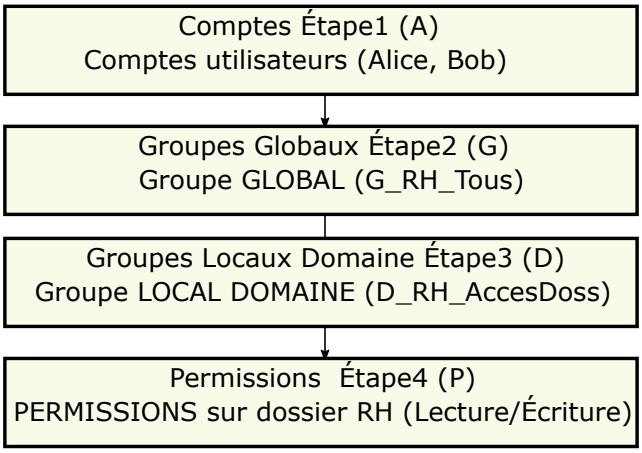


FIGURE 6.5 – Les quatre étapes du modèle AGDLP

Règle d'or *: Les permissions sont toujours attribuées aux groupes locaux du domaine, jamais directement aux utilisateurs.*

Explication détaillée de chaque étape

Étape A - Comptes (Accounts) Ce sont les **utilisateurs** individuels du domaine.

Exemples de Comptes

- Alice.Dubois@entreprise.local
- Bob.Martin@entreprise.local
- Charlie.Admin@entreprise.local

Principe : On n'attribue JAMAIS directement une permission à un compte utilisateur. On utilise toujours des groupes.

Étape G - Groupes Globaux Les groupes globaux **regroupent des utilisateurs** qui partagent une même **fonction** ou un même **rôle**.

Caractéristique	Description
Portée	Valable uniquement dans le domaine où ils sont créés
Contenu	Peut contenir des utilisateurs et d'autres groupes globaux du MÊME domaine
Utilité	Regrouper des comptes par métier/service

Exemples de groupes GLOBAUX

- GRHEmployes (tous les employés RH)
- GRHManagers (les managers RH)
- GITAdmins (les administrateurs IT)
- GComptaControleurs (les contrôleurs de gestion)

Étape D - Groupes Locaux Domaine (Domain Local) Ces groupes sont utilisés pour **regrouper des groupes globaux** et **attribuer des permissions**.

Caractéristique	**Description**
Portée	Valable uniquement dans le domaine
Contenu	Peut contenir des utilisateurs, groupes globaux, groupes universels de N'IMPORTE quel domaine
Utilité	Représenter un DROIT d'accès à une ressource

Exemples de groupes LOCAUX DOMAINE

- D_DossierRH_Lecture (donne droit de lecture sur dossier RH)
- D_DossierRH_Ecriture (donne droit d'écriture sur dossier RH)
- D_ImprimanteRH_Impression (donne droit d'impression)

Étape P - Permissions C'est l'**attribution effective** des droits sur une ressource (dossier, imprimante, application et autres ressources).

Exemples d'attribution

- Attribuer "Lecture" sur D :\Dossiers\RH au groupe D_DossierRH_Lecture
- Attribuer "Modification" sur D :\Dossiers\RH au groupe D_Dossier RH_Ecriture

Exemple concret complet

Cas pratique : Gestion des accès au dossier RH

1. Situation initiale

▷ Dossier partagé : `\\serveur\RH`
▷ 3 utilisateurs RH : Alice, Bob, Claire
▷ 1 manager RH : David

2. Application du modèle AGDLP

Étape	**Action**	**Résultat**
A	Création des comptes	Alice, Bob, Claire, David
G	Création groupes GLOBAUX	`G_RH_Employes` (Alice,Bob,Claire) `G_RH_Managers` (David)
D	Création groupes LOCAUX DOMAINE	`D_RH_LectureSeule` `D_RH_LectureEcriture`
P	Attribution permissions	Lecture seule → `D_RH_LectureSeule` Modification → `D_RH_LectureEcriture`

3.Imbrication des groupes

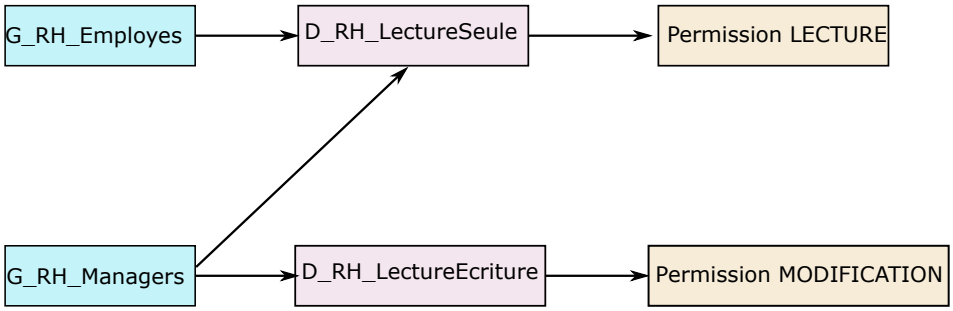


FIGURE 6.6 – Imbrication des groupes selon le modèle AGDLP

4.Résultat final

Utilisateur	Groupe global	Groupe local domaine	Permission réelle
Alice	G_RH_Employes	D_RH_LectureSeule	**Lecture seule**
Bob	G_RH_Employes	D_RH_LectureSeule	**Lecture seule**
Claire	G_RH_Employes	D_RH_LectureSeule	**Lecture seule**
David	G_RH_Managers	D_RH_LectureSeule + D_RH_LectureEcriture	**Modification**

Avantages du modèle AGDLP

Avantage	Explication
Centralisation	Les permissions sont gérées au niveau du groupe local domaine
Flexibilité	Pour modifier les droits d'un utilisateur, on change son groupe global
Lisibilité	La nomenclature (G_ / D_) indique immédiatement le type de groupe
Évolutivité	Ajout/suppression d'utilisateurs = simple modification des groupes globaux
Sécurité	Pas de permission directe sur les comptes utilisateurs
Délégation	On peut déléguer la gestion des groupes globaux sans donner les droits sur les ressources

TABLE 6.4 – Les avantages du modèle AGDLP

Exemple d'implémentation PowerShell

Exemple d'implémentation PowerShell

```
# Étape A : Création des comptes utilisateurs
-New-ADUser -Name "Alice Dubois" -SamAccountName "alice.dubois" -Enabled $true
-New-ADUser -Name "Bob Martin" -SamAccountName "bob.martin" -Enabled $true
# Étape G : Création du groupe GLOBAL
New-ADGroup -Name "GRHEmployes"
-GroupScope Global
-GroupCategory Security
-Description "Employés du service RH"
# Ajout des utilisateurs au groupe GLOBAL
Add-ADGroupMember -Identity "GRHEmployes" -Members "alice.dubois", "bob.martin"
# Étape D : Création du groupe LOCAL DOMAINE
New-ADGroup -Name "D_DossierRHLecture"
-GroupScope DomainLocal
-GroupCategory Security
-Description "Accès lecture au dossier RH"
# Ajout du groupe GLOBAL dans le groupe LOCAL DOMAINE
Add-ADGroupMember -Identity "DDossierRHLecture" -Members "GRHEmployes"
# Étape P : Attribution de la permission (à faire via ACL sur le dossier)
# icacls D :\Dossiers\RH /grant "ENTREPRISE \D_DossierRH_Lecture :(RX)"
```

Les principes incontournables

1. *Les Utilisateurs vont dans les Groupes Globaux,*
2. *Les Groupes Globaux vont dans les Groupes Locaux Domaine,*
3. *Les Groupes Locaux Domaine reçoivent les Permissions*
4. *Jamais de permission directe sur un compte utilisateur*
5. *Un utilisateur peut être dans plusieurs groupes globaux*
6. *Un groupe global peut être dans plusieurs groupes locaux domaine*
7. *Les groupes locaux domaine sont liés à des ressources spécifiques*
8. *La modification des droits se fait au niveau* **D** *ou* **P**, *jamais au niveau* **A**

6.5 Conclusion

Les contrôleurs de domaine constituent l'épine dorsale de l'administration des réseaux Windows. Leur compréhension est essentielle pour tout administrateur système. Active Directory offre une solution robuste et éprouvée, mais nécessite une planification soigneuse et une maintenance régulière.

Chapitre 7

Les outils et les compétances pour administrer un réseau IP

7.1 Objectifs et rôle de l'administration

7.1.1 Introduction

Que faut-il pour devenir un administrateur de service réseau ?

Pour devenir un bon administrateur de services réseaux, il est important d'avoir certaines compétences et certains matériels, notamment :

1. Connaissances en réseau : Il est crucial d'avoir une compréhension solide des principes de base de la communication réseau, tels que les protocoles réseau (TCP/IP, UDP), les adresses IP, les sous-réseaux, les routes, les passerelles, les VLAN.

2. Compétences en système : Les administrateurs de services réseaux doivent être familiarisés avec les systèmes d'exploitation, notamment Windows et Linux, ainsi que les services associés tels que DHCP, DNS, FTP, HTTP et autres.

3. Connaissances en sécurité : Les administrateurs de services réseaux doivent être conscients des menaces potentielles aux réseaux et disposer de compétences en matière de sécurité informatique, telles que la configuration de pare-feu, la gestion des identifiants et des mots de passe, la détection et la résolution des incidents de sécurité.

4. Matériel de réseau : Il est important d'avoir accès à un équipement réseau, comme des routeurs, des commutateurs, des modems, des pare-feu, pour pouvoir mettre en pratique les compétences et les connaissances acquises.

5. Logiciels de simulation : Les logiciels de simulation peuvent être utiles pour simuler des scénarios réseau et tester des configurations avant de les implémenter dans un environnement de production.

7.2 L'environnement dans lequel un administrateur de service réseau doit évoluer

Un administrateur de services réseaux doit combiner ses connaissances théoriques et ses compétences pratiques pour être en mesure de comprendre les principes de base des réseaux, d'avoir des compétences en système et en sécurité, d'avoir accès à du matériel réseau et d'utiliser des outils de simulation pour tester et valider les configurations avant de les implémenter dans un environnement de production. Pour un administrateur de services réseaux, il est important de maîtriser les logiciels suivants :

7.2.1 Systèmes d'exploitation :

Connaissance approfondie de systèmes d'exploitation tels que Windows, Linux, Unix et macOS.

FIGURE 7.1 – Les systèmes d'exploitations les plus connus

Pour comprendre la connaissance approfondie de systèmes d'exploitation, il est important de comprendre les concepts de base suivants :

- ▷ Système d'exploitation (OS) : il s'agit d'un logiciel qui gère les ressources informatiques telles que la mémoire, le processeur et les périphériques d'entrée/sortie.
- ▷ Types de systèmes d'exploitation : il existe deux grands types de systèmes d'exploitation, soit les systèmes d'exploitation propriétaires (tels que Windows et MacOS) et les systèmes d'exploitation open source (tels que Linux et Unix).
- ▷ Tâches du système d'exploitation : les tâches du système d'exploitation incluent la gestion de la mémoire, la planification des tâches, la gestion des fichiers et des périphériques, ainsi que la sécurité.
- ▷ Architecture du système d'exploitation : les systèmes d'exploitation sont généralement conçus selon une architecture en couches, avec une couche pour le noyau, une couche pour les programmes système, une couche pour les applications et une couche pour l'interface utilisateur.
- ▷ Commandes de base : pour travailler avec un système d'exploitation, il est important de comprendre les commandes de base telles que les commandes de ligne de commande, les commandes de copie de fichiers, les commandes de gestion des processus et les commandes de gestion des fichiers.

En résumé, la connaissance approfondie de systèmes d'exploitation implique la compréhension de ce qu'est un système d'exploitation, de ses différents types, de ses tâches et de son architecture, ainsi que la maîtrise des commandes de base pour travailler avec celui-ci. Les commandes de base les plus couramment utilisées dans les systèmes d'exploitation courants (tels que Windows, Linux et macOS) incluent :

- ▷ Commandes de gestion des fichiers et des répertoires : cd, ls, mkdir, rm, cp, mv, touch, etc.
- ▷ Commandes de gestion des processus : ps, kill, top, etc.
- ▷ Commandes de gestion des utilisateurs et des groupes : adduser, useradd, groupadd, usermod, userdel, etc.
- ▷ Commandes de gestion des permissions : chmod, chown, etc.
- ▷ Commandes de gestion de la mémoire : free, top, etc.
- ▷ Commandes de gestion des réseaux : ping, traceroute, ifconfig, ip, netstat, etc.
- ▷ Commandes de gestion des paquets : apt-get, yum, dnf, brew, pacman, etc.

Il est important de noter que ces commandes peuvent varier en fonction du système d'exploitation utilisé et de la distribution Linux choisie.

7.2.2 Les serveurs d'application

Connaissance des serveurs d'application tels que Apache, Nginx, IIS. Les différents types de serveurs d'application et leur fonctionnement. Cela peut inclure :

Les Serveurs Web

Les serveurs Web tels que Apache et Nginx permettent de héberger et de fournir du contenu Web aux utilisateurs sur Internet. Il est important de comprendre comment configurer et gérer ces serveurs, ainsi que les protocoles associés tels que HTTP et HTTPS.

FIGURE 7.2 – Les Serveurs Web

Les Serveurs de messagerie

Les serveurs de messagerie tels que Microsoft Exchange et Postfix permettent de gérer les e-mails entrants et sortants dans une organisation. Il est important de comprendre comment configurer la sécurité, la fiabilité et la gestion des courriels pour les utilisateurs.

FIGURE 7.3 – Les Serveurs de messagerie

Les Serveurs DNS

Les serveurs DNS tels que BIND et Microsoft DNS sont responsables de la résolution des noms de domaines en adresses IP. Il est important de comprendre comment configurer et gérer ces serveurs pour assurer un fonctionnement optimal de la communication sur le réseau.

FIGURE 7.4 – Les Serveurs DNS

Les Serveurs de bases de données

Les serveurs de bases de données tels que Microsoft SQL Server et MySQL permettent de stocker, gérer et interroger des données pour les applications. Il est important de comprendre les différentes architectures de bases de données et comment les administrer pour assurer la disponibilité et la sécurité des données.

FIGURE 7.5 – Les Serveurs de bases de données

En plus de comprendre le fonctionnement de ces différents types de serveurs, il est également important de maîtriser les logiciels et outils associés tels que les outils de gestion de bases de données, les outils de monitoring de performance et les outils de sauvegarde et de récupération de données.

7.2.3 Les Bases de données

Il est important de comprendre comment fonctionnent ces différents types de serveurs et de comprendre les logiciels et outils associés, tels que les outils de gestion de bases de données, les outils de surveillance de la performance et les outils de sauvegarde et de récupération de données.

FIGURE 7.6 – Les Bases de données

Les bases de données sont souvent utilisées pour stocker les informations des utilisateurs, des applications et des services, telles que les informations de connexion, les préférences utilisateur et les données d'application. Il est donc important de comprendre comment les bases de données sont conçues, comment elles peuvent être administrées et comment elles peuvent être sécurisées. Il est également important de maîtriser les différents systèmes de gestion de bases de données (DBMS), tels que MySQL, Oracle, Microsoft SQL Server et PostgreSQL. L'administrateur de saura comment administrer, configurer et dépanner les bases de données pour les applications et les services de son réseau.

7.2.4 Le Routage et la commutation

Le routage est un processus dans lequel un routeur prend une décision sur la façon d'envoyer des paquets de données entre différents réseaux. Le but du routage est de trouver le chemin le plus efficace pour acheminer les paquets de données d'un expéditeur à un destinataire. Pour prendre cette décision, le routeur utilise des informations telles que les adresses IP et les tables de routage. Le routage peut se faire de différentes manières, telles que le routage statique et le routage dynamique. Dans le routage statique, les chemins sont configurés manuellement sur chaque routeur du réseau. Dans le routage dynamique, les routeurs communiquent entre eux pour partager des informations sur les différents chemins disponibles. Le routage peut également être classé en fonction de la couche OSI à laquelle il opère. Le routage de couche 3 se concentre sur les adresses IP, tandis que le routage de couche 2 se concentre sur les adresses MAC. Le routage peut également être interne, s'appliquant à un seul réseau, ou externe, impliquant des réseaux multiples et des passerelles entre eux.

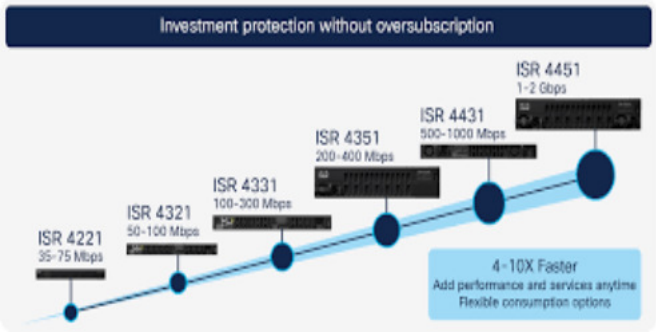


FIGURE 7.7 – Cisco ISR 4000 Series

Les protocoles de routage permettent de déterminer comment les paquets de données sont acheminés à travers le réseau. Les protocoles de routage les plus couramment utilisés sont :

- ▷ Routing Information Protocol (RIP)
- ▷ Open Shortest Path First (OSPF)
- ▷ Border Gateway Protocol (BGP)
- ▷ Intermediate System to Intermediate System (IS-IS)

Il est important de comprendre le fonctionnement de ces protocoles et de savoir comment les configurer pour garantir un fonctionnement optimal de votre réseau.

Il y a plusieurs options de routeurs pour les entreprises, chacune avec des fonctionnalités et des spécifications différentes en fonction des besoins spécifiques de l'entreprise. Voici quelques exemples de routeurs populaires pour les entreprises :

- ▷ Cisco ISR 4000 Series : un routeur modulaire avec des options de connectivité WAN flexibles, une sécurité avancée, une haute disponibilité et une évolutivité pour répondre aux besoins changeants des entreprises.
- ▷ Juniper Networks SRX Series : une solution de sécurité intégrée qui fournit des services de sécurité avancés, une haute disponibilité, une fiabilité et une gestion simplifiée pour protéger les réseaux d'entreprise contre les menaces de sécurité.

FIGURE 7.8 – Juniper Networks SRX Series

- ▷ Huawei AR2200 Series : un routeur de nouvelle génération avec une capacité de traitement de haut niveau pour prendre en charge les besoins de réseaux d'entreprise évolutifs, des performances stables et une gestion facile.

FIGURE 7.9 – Huawei AR2200 Series

Fortinet FortiGate : une plate-forme de sécurité unifiée avec des fonctionnalités avancées de pare-feu, de VPN, d'analyse de trafic et de contrôle d'accès pour protéger les réseaux d'entreprise contre les menaces.

FIGURE 7.10 – Fortinet FortiGate

Il convient de noter que ces routeurs sont destinés aux grandes entreprises et peuvent avoir un coût élevé. Il existe également des options moins coûteuses pour les petites et moyennes entreprises, comme les routeurs de la série Cisco Small Business ou les routeurs de la série TP-Link SafeStream.

7.2.5 La Virtualisation

Les administrateurs de services réseaux peuvent utiliser ces logiciels pour créer et gérer des machines virtuelles, ce qui leur permet de tester et de déployer des configurations réseau dans un environnement sécurisé et contrôlé.

L'optimisation des ressources informatiques en créant des environnements virtuels qui peuvent être utilisés pour héberger plusieurs systèmes d'exploitation et applications sur une seule machine physique est un domaine

FIGURE 7.11 – Les routeurs pour petite et moyennes entreprises

important pour les administrateurs réseau. Les administrateurs réseau doivent être familiers avec les différentes techniques de virtualisation, telles que la virtualisation de serveur, de stockage, de réseau et de bureau, ainsi que les différents produits de virtualisation, tels que VMware et Hyper-V. Ils doivent également comprendre les avantages et les inconvénients de la virtualisation pour les réseaux, tels que la consolidation des serveurs, l'optimisation des ressources, la facilité de déplacement et la réduction des coûts d'exploitation.

FIGURE 7.12 – VMware et Hyper-V outils de virtualisation

Il existe plusieurs logiciels de virtualisation disponibles sur le marché, tels que :
VMware vSphere : une plateforme de virtualisation de serveurs pour les entreprises de toutes tailles.

FIGURE 7.13 – Autres types d'outils de virtualisation

- ▷ Microsoft Hyper-V : une plateforme de virtualisation de serveurs intégrée dans le système d'exploitation Windows Server.
- ▷ Oracle VirtualBox : un logiciel de virtualisation open source pour les ordinateurs de bureau.
- ▷ Citrix XenServer : une plateforme de virtualisation de serveurs pour les entreprises de toutes tailles.
- ▷ Red Hat Enterprise Virtualization (RHEV) : une plateforme de virtualisation de serveurs pour les entreprises utilisant la distribution Linux Red Hat.

7.2.6 Le Stockage en réseau

Les administrateurs doivent comprendre les différents types de systèmes de stockage en réseau, tels que les baies de stockage, les systèmes de fichiers distribués, les systèmes de stockage en nuage et les systèmes de stockage basés sur le protocole iSCSI. Ils doivent également comprendre les concepts clés tels que la mise en miroir, la redondance, la tolérance aux pannes et les politiques de stockage. En outre, ils doivent être en mesure de planifier, de déployer et de gérer efficacement les systèmes de stockage en réseau pour répondre aux exigences en matière de capacité, de performance et de disponibilité des données. Exemple de logiciels de gestion de stockage en réseau : NetApp OnCommand, EMC Storage, Dell EMC PowerVault.

Les baies de stockage sont des systèmes de stockage en réseau qui permettent de centraliser les données pour un accès facile et sécurisé. Elles peuvent être formées de plusieurs disques durs ou de disques SSD qui peuvent être connectés en interne ou en externe à un ou plusieurs serveurs. Les baies de stockage peuvent prendre en charge divers protocoles de stockage tels que Fibre Channel, iSCSI et NFS. Elles peuvent également offrir des fonctionnalités telles que la réplication de données, la sauvegarde et la restauration, la réduction de la taille des données, la tolérance aux pannes et la gestion de la capacité de stockage. Les baies de stockage sont souvent utilisées par les entreprises pour gérer les grandes quantités de données stockées dans le cadre de leurs

FIGURE 7.14 – Le Stockage en réseau

opérations commerciales. Les systèmes de fichiers distribués (ou systèmes de fichiers en réseau) sont des logiciels qui permettent de stocker les fichiers sur plusieurs ordinateurs reliés en réseau, de manière à pouvoir y accéder depuis n'importe quel ordinateur de ce réseau. Cela peut être très utile pour les entreprises qui souhaitent centraliser leur stockage de données pour une meilleure gestion, une plus grande sécurité et une accessibilité accrue à partir de plusieurs emplacements. Les exemples courants de systèmes de fichiers distribués incluent les systèmes de stockage en nuage tels que Google Drive ou Dropbox, ainsi que les systèmes de fichiers distribués tels que CIFS (Common Internet File System) ou NFS (Network File System). Les systèmes de stockage en nuage sont des systèmes qui permettent de stocker des données sur un serveur distant, accessible via internet. Les utilisateurs peuvent accéder à leurs données stockées en nuage à partir de n'importe où et à tout moment en utilisant une connexion internet. Les systèmes de stockage en nuage sont souvent fournis en tant que service par des entreprises spécialisées telles que Amazon Web Services, Microsoft Azure et Google Cloud. Les avantages de l'utilisation de ces systèmes incluent la disponibilité des données à distance, la flexibilité pour accéder et partager des données avec d'autres utilisateurs et la possibilité de sauvegarder des données en toute sécurité.

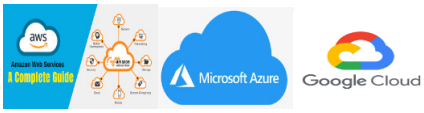


FIGURE 7.15 – Stockage en Cloud

Les systèmes de stockage basés sur le protocole iSCSI sont des systèmes de stockage qui utilisent le protocole iSCSI pour transmettre les données entre le serveur et les périphériques de stockage. Les systèmes de stockage iSCSI permettent aux utilisateurs de connecter des serveurs à des périphériques de stockage distants via une connexion IP. Les données sont transmises sous forme de blocs de données, similaires à ceux utilisés dans les baies de stockage traditionnelles. Les systèmes de stockage iSCSI peuvent être utilisés pour des applications telles que la sauvegarde de données, la gestion de la capacité de stockage et la création de clusters de stockage haute disponibilité.

7.2.7 Les outils de surveillance réseau

Connaissance des outils de surveillance réseau tels que, entre autres Wireshark, Nagios et nmap.

FIGURE 7.16 – Quelques outils d'administration réseau

Les outils de surveillance réseau permettent de surveiller et de gérer les performances et les problèmes du réseau. Il est important de les connaître car ils permettent de détecter et de résoudre les problèmes rapidement avant qu'ils n'affectent les utilisateurs. Comme exemples d'outils de surveillance réseau on trouve : Nagio, SolarWinds, Zabbix, Cacti, Wireshark et NetFlow Analyzer. Pour un administrateur réseau, la familiarisation

avec ce type d'outlis est obligatoire. Chaque outil à déployer, dépend de la taille et de la complexité du réseau que vous gérez.

7.2.8 Les protocoles de sécurité

Connaissance des protocoles de sécurité tels que SSL/TLS, VPN. Il est important de maîtriser les protocoles de sécurité pour assurer la protection des données et des réseaux. Les exemples courants de protocoles de sécurité comprennent SSL/TLS pour le cryptage des données sur le Web, IPSec pour la sécurité de la couche réseau, SSH pour la sécurité de la connexion à distance, et Firewall pour la protection du réseau contre les attaques externes. Les administrateurs de services réseau doivent comprendre comment implémenter et configurer ces protocoles, ainsi que comment les utiliser pour maintenir la sécurité du réseau.

Le protocole SSL (Secure Socket Layer) et le protocole TLS (Transport Layer Security) sont des protocoles de sécurité couramment utilisés pour crypter les communications sur le réseau. Ils permettent de garantir la confidentialité et l'intégrité des données transmises sur un réseau en utilisant des algorithmes de chiffrement. Les certificats SSL/TLS sont également utilisés pour authentifier les sites web, ce qui est important pour les transactions en ligne telles que les achats en ligne et la saisie de données confidentielles.

Un administrateur de services réseaux doit comprendre les principes de fonctionnement de SSL/TLS, savoir comment les installer et les configurer correctement, et être capable de dépanner les problèmes de sécurité associés à ces protocoles.

L'installation de protocoles de sécurité tels que SSL/TLS dépend de plusieurs facteurs, tels que le système d'exploitation utilisé, le type de serveur sur lequel vous souhaitez installer SSL/TLS, etc.

Les étapes générales pour installer SSL/TLS sur un serveur web sont :

1. Acheter un certificat SSL/TLS auprès d'un fournisseur de certificats.
2. Configurer le serveur web pour utiliser SSL/TLS. Pour cela, vous pouvez utiliser des outils tels Apache, Nginx ou Microsoft IIS. La configuration dépend du type de serveur web utilisé.
3. Configurer le serveur pour écouter sur le port 443 (le port par défaut pour SSL/TLS).
4. Importer le certificat SSL/TLS acheté sur le serveur.
5. redémarrer le serveur web pour que les modifications prennent effet.
6. Vérifier que SSL/TLS est en cours d'exécution en accédant au site web via un navigateur web et en vérifiant que le protocole est en HTTPS.
7. Notez que ces étapes peuvent varier en fonction du système d'exploitation et du type de serveur utilisé.

FIGURE 7.17 – Protocoles de sécurité

Il est donc recommandé de consulter la documentation de votre serveur web pour obtenir des instructions plus détaillées.

IPSec (Internet Protocol Security) est un protocole de sécurité pour les communications sur les réseaux informatiques. Il permet de protéger les données transmises sur un réseau en utilisant des algorithmes de chiffrement pour sécuriser les paquets de données. IPSec peut être utilisé pour sécuriser diverses applications, notamment les communications VPN (Virtual Private Network), les communications à distance, les e-mails, les transferts de fichiers, etc.

L'installation d'IPSec dépend du système d'exploitation utilisé. Pour un système d'exploitation Windows, vous pouvez l'installer en utilisant le Gestionnaire de serveur ou en utilisant la ligne de commande. Pour un système d'exploitation Linux, vous pouvez utiliser des outils tels que Openswan ou StrongSwan pour configurer IPSec. Il est important de noter que l'installation d'IPSec peut être complexe et nécessite une connaissance approfondie des protocoles de sécurité et de la configuration du réseau. Il est donc recommandé de consulter la documentation du système d'exploitation ou d'un expert en sécurité pour installer correctement IPSec. L'installation d'IPSec dépend de l'environnement réseau et du système d'exploitation utilisé. Les étapes générales pour installer IPSec peuvent inclure les étapes suivantes :

1. Configuration du protocole IPSec sur chaque dispositif réseau : Cela peut être fait à l'aide de la console de gestion de l'équipement réseau ou de l'interface de ligne de commande.
2. Définition des règles de sécurité IPSec : Les règles définissent les protocoles et les ports autorisés à traverser le tunnel IPSec, ainsi que les clés utilisées pour chiffrer les données.
3. Configuration des politiques de sécurité IPSec : Les politiques définissent les algorithmes de chiffrement et d'authentification à utiliser pour sécuriser les données.
4. Vérification de la fonctionnalité : Après l'installation, vous devrez vérifier que IPSec est correctement configuré et fonctionne en testant les connexions à travers le tunnel IPSec. L'installation d'IPSec via la ligne de commande dépend du système d'exploitation que vous utilisez.

Sur un système d'exploitation Windows, vous pouvez utiliser la commande "netsh" pour configurer IPSec. Par exemple, pour activer IPSec sur une connexion réseau nommée "Local Area Connection", vous pouvez utiliser la commande suivante :

netsh ipsec static add policy name="IPSec Policy" assign=yes

netsh ipsec static add filter filterlist="IPSec Filter" srcaddr=any dstaddr=any protocol=all srcport=0 dstport=0

netsh ipsec static add filteraction name="IPSec Action" action=block

netsh ipsec static add rule name="IPSec Rule" policy="IPSec Policy" filterlist="IPSec Filter" filteraction="IPSec Action"

Sur un système d'exploitation Unix/Linux, vous pouvez utiliser la commande "ipsec" pour configurer IPSec. Par exemple, pour activer IPSec sur une connexion réseau, vous pouvez utiliser les commandes suivantes :

ipsec auto –add myconn

ipsec auto –status

ipsec auto –up myconn

7.2.9 Les outils de gestion de projet

Les outils de gestion de projet permettent de planifier, suivre et contrôler les activités liées à un projet. Il existe plusieurs outils de gestion de projet populaires tels que Microsoft Project, Trello, Asana, et Jira. Ils offrent des fonctionnalités telles que la planification de la timeline, la gestion des tâches et des ressources, la collaboration en temps réel et la génération de rapports. Les administrateurs de services réseau doivent être en mesure de choisir et d'utiliser les outils les plus appropriés pour leurs projets, en fonction de la complexité et de la taille de chaque projet. Microsoft Project est un outil de gestion de projet qui permet aux utilisateurs de planifier, suivre et gérer des projets en utilisant des graphiques de Gantt, des tableaux de bord et des indicateurs clés de performance. Il fournit des fonctionnalités pour la planification des ressources, la gestion des coûts et la collaboration en temps réel avec les équipes. Microsoft Project est utilisé par les administrateurs de services réseaux pour gérer les projets de mise en œuvre de nouveaux réseaux, de mise à niveau d'infrastructures existantes, de déploiement de nouveaux services réseaux.

Figure 7.18 – Microsoft Project

Microsoft Project est un logiciel de gestion de projet qui permet aux utilisateurs de planifier, suivre et gérer des projets. Il permet aux utilisateurs de créer des diagrammes de Gantt, de définir les tâches, les dépendances, les dates de début et de fin, les ressources et les coûts. Les utilisateurs peuvent également suivre l'avancement du projet en temps réel et effectuer des ajustements en fonction des délais, des coûts et des ressources.

Exemple

Simple utilisation de Microsoft Project :

1. Créer un nouveau projet : Ouvrir Microsoft Project et cliquer sur "Nouveau projet" pour démarrer un nouveau projet.
2. Définir les tâches : Ajouter les tâches nécessaires au projet, telles que la planification, la conception, la construction, le test et la mise en service.
3. Assigner les ressources : Assigner des personnes ou des ressources aux tâches pour les effectuer.
4. Planifier les dates : Définir les dates de début et de fin pour chaque tâche en fonction de la durée estimée et des dépendances.
5. Créer un diagramme de Gantt : Générer un diagramme de Gantt pour visualiser la chronologie du projet et les dépendances entre les tâches.
6. Suivre l'avancement : Ajouter des mises à jour sur l'avancement du projet pour vérifier si les délais sont respectés et effectuer des ajustements en conséquence.
7. Imprimer le rapport final : Imprimer un rapport final qui inclut le diagramme de Gantt, les tâches, les ressources et les coûts pour partager avec les parties prenantes.

7.2.10 Les logiciels de simulation

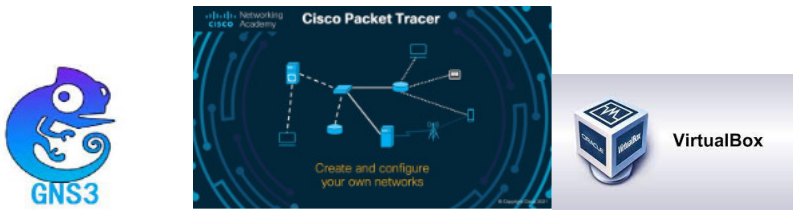


FIGURE 7.19 – Les logiciels de simulation

Ils permettent aux administrateurs réseau de tester différentes configurations réseau sans affecter les systèmes en production et dans un environnement virtuel. Les outils de simulation de réseau les plus populaires incluent :

GNS3 (Graphical Network Simulator 3) : un logiciel open source qui permet de simuler un réseau complexe en utilisant des équipements réels.

Packet Tracer : un logiciel développé par Cisco pour former les administrateurs réseau sur les technologies Cisco.

VirtualBox : une plateforme de virtualisation qui permet de simuler plusieurs systèmes d'exploitation dans un seul environnement.

Ces outils de simulation permettent aux administrateurs réseau de tester différentes configurations réseau et de développer leurs compétences en matière d'administration réseau.

7.3 Conclusion

Pour devenir un bon administrateur de service réseau, il est important d'avoir une solide compréhension des concepts de base des réseaux, des protocoles de communication et des systèmes d'exploitation. Il est également essentiel de connaître les outils de gestion de réseau, les protocoles de sécurité, les systèmes de stockage et les technologies émergentes. Une excellente capacité d'analyse, une grande attention aux détails, une excellente résolution de problèmes et de bonnes compétences en communication sont également nécessaires. Enfin, l'apprentissage continu, la formation et la pratique sont essentiels pour rester à jour avec les dernières tendances et technologies en matière de réseau.

Exercices d'application

Exercice pratique sur la MIB

Il s'agit de configurer sur Cisco packet tracer la topologie donnée par la figure 7.20.

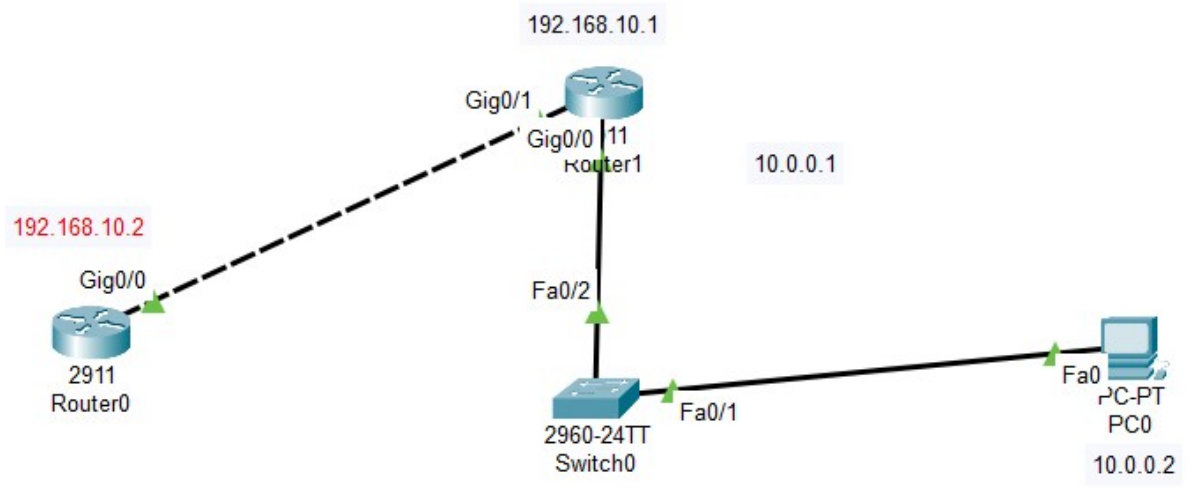


FIGURE 7.20 – Visualisation des élément de la MIB

Configuration Le PC sera le SNMP manager, le router 1 sera le SNMP agent qu'on veut superviser.

1. Les interfaces seront correctement configurés
2. L'écriture et la lecture avec les communautés seront mis en place sur l'agent.
3. La NMS sera configurée en mode statique.
4. A partir de la NMS, dans MIB Browser, la MIB sera visualisée et supervisée en parcourant l'arborescence.
5. On effectuera des read pour vérifier entre autres les interfaces, le nom générique, l'OID et ainsi de suite (GETrequest).
6. Par la suite, il s'agira de renomer l'agent en utilisant la commande SETrequest.

Problème de synthèse sur les protocoles : DHCP, FTP, DNS, HTTP et RIP

Il s'agit de configurer sur Cisco packet tracer la topologie donnée par la figure 7.21.

Dans cette topologie :

1. Le serveur sera configuré en mode statique, sont emplacement est facultatif.
2. Les routeurs doivent être connectés par des liaisons séries (pour les longues distances).
3. Le protocole RIP sera configuré sur les trois routeurs afin de connaître les différents réseaux auxquels ils sont raccordés.
4. Le protocole DHCP sera configuré avec les pool1 20.0.0.5 à 20.0.0.254, pool2 30.0.0.5 à 30.0.0.254 et la pool3 50.0.0.5 à 50.0.0.254 sur les réseaux respectifs.
5. Vérifier que les adresses ont bien été attribuées par le serveur.

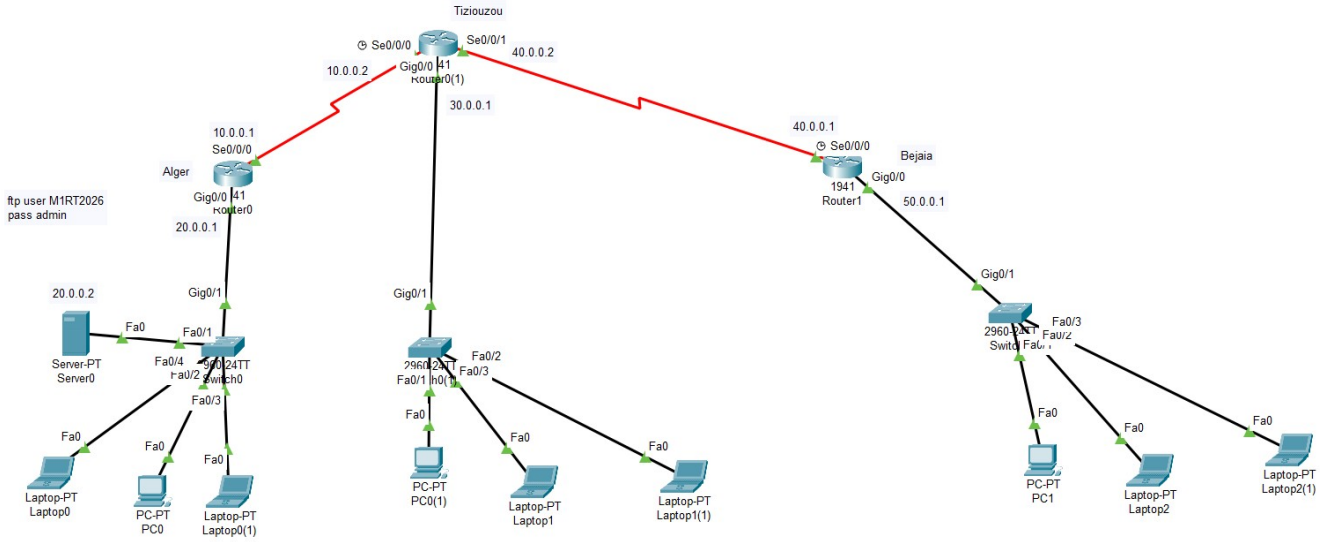


FIGURE 7.21 – Topologie englobant l'ensemble des protocoles vus dans le programme pédagogique

6. Les gateway seront configurées aussi selon la topologie.
7. Afin de localiser le serveur, sur chaque routeur il faudra configurer les helper (commande helper-adress)
8. Le protocole DNS sera aussi configurer et on choisira le nom google.com pour la connexion de tous les utilisateurs des différents réseaux.
9. Configurer le protocole FTP et choisir un username : M1RT un password :telecoms.
10. Mettre un fichier texte dans le serveur ftp, lire ce fichier sur un équipement de chaque réseau.
11. Changer le nom de ce fichier à partir d'un équipement du réseau 20.0.0.0.
12. Enfin, le protocole HTTP sera aussi configuré et testé après avoir modifié certains paramètres d'affichage sur la page web du browser.

Bibliographie

[1] François Pignet, "Réseaux informatiques : Supervision et administration", Édition ENI -274 pages,10 décembre 2007.

[2] Pierre-Yves et Rafael Corvalan,"Les Annuaires LDAP, méta-annuaires et e-provinionning", Édition Dunos -334 pages, 2ème édition, 1et juin 2004.

[3] Damien Soulages,"Administrateur réseau : Vous allez adorer ce métier rempli d'opportunité", Éditeur : Independently published -550, 16 janvier 2023.

[4] Stéphane Lohier et Dominique Présent, "Réseaux et transmission -Protocoles, Infrastructures et Services", Édition Dunos -352 pages, 7ème édition, 26 aout 2020.

[5] Apple Inc. (2024). *macOS - Système d'exploitation*. Disponible : https ://www.apple.com/macos

[6] Linux Foundation. (2024). *Linux Operating System*. Disponible : https ://www.linux.org

[7] Microsoft Corporation. (2024). *Windows Operating System*. Disponible : https ://www.microsoft.com/windows

[8] Apache Software Foundation. (2024). *Apache HTTP Server Project*. Disponible : https ://httpd.apache.org

[9] F5 Networks. (2024). *NGINX High Performance Load Balancer*. Disponible : https ://www.nginx.com

[10] Microsoft Corporation. (2024). *Microsoft Exchange Server*. Disponible : https ://www.microsoft.com/exchange

[11] Postfix Project. (2024). *Postfix Mail Server*. Disponible : https ://www.postfix.org

[12] Internet Systems Consortium. (2024). *BIND - Berkeley Internet Name Domain*. Disponible : https ://www.isc.org/bind

[13] Microsoft Corporation. (2024). *Windows Server DNS*. Disponible : https ://www.microsoft.com/windows-server

[14] Microsoft Corporation. (2024). *Microsoft SQL Server*. Disponible : https ://www.microsoft.com/sql-server

[15] Oracle Corporation. (2024). *MySQL Database*. Disponible : https ://www.mysql.com

[16] Oracle Corporation. (2024). *Oracle Database*. Disponible : https ://www.oracle.com/database

[17] PostgreSQL Global Development Group. (2024). *PostgreSQL Database*. Disponible : https ://www.postgresql.org

[18] Cisco Systems. (2024). *Cisco ISR 4000 Series Routers*. Disponible : https ://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers/index.html

[19] Juniper Networks. (2024). *SRX Series Services Gateways*. Disponible : https ://www.juniper.net/us/en/products/security/srx-series.html

[20] Huawei Technologies. (2024). *AR2200 Series Enterprise Routers*. Disponible : https ://e.huawei.com/en/products/enterprise-routers/ar2200

[21] Fortinet Inc. (2024). *FortiGate Next-Generation Firewall*. Disponible : https ://www.fortinet.com/products/next-generation-firewall

[22] Cisco Systems. (2024). *Cisco Small Business Routers*. Disponible : https ://www.cisco.com/c/en/us/products/routers/small-business-routers/index.html

[23] TP-Link Technologies. (2024). *SafeStream Series Routers*. Disponible : https ://www.tp-link.com/us/business-networking/safestream-router

[24] VMware Inc. (2024). *VMware vSphere Virtualization Platform*. Disponible : https ://www.vmware.com/products/vsphere.html

[25] Microsoft Corporation. (2024). *Hyper-V Server Virtualization*. Disponible : https ://www.microsoft.com/en-us/cloud-platform/server-virtualization

[26] VMware Inc. (2024). *VMware vSphere - Serveur de virtualisation*. Disponible : https ://www.vmware.com/fr/products/vsphere.html

[27] Oracle Corporation. (2024). *VirtualBox Open Source Virtualization*. Disponible : https ://www.virtualbox.org

[28] Citrix Systems. (2024). *Citrix Hypervisor (XenServer)*. Disponible : https ://www.citrix.com/products/citrix-hypervisor

[29] Red Hat Inc. (2024). *Red Hat Enterprise Virtualization (RHEV)*. Disponible : https ://www.redhat.com/en/technologies/virtualization/enterprise-virtualization

[30] Dell Technologies. (2024). *Dell EMC PowerVault Storage*. Disponible : https ://www.dell.com/en-us/work/shop/powervault-storage

[31] NetApp Inc. (2024). *NetApp OnCommand Storage Management*. Disponible : https ://www.netapp.com/data-management/oncommand-insight

[32] Amazon Web Services. (2024). *Amazon Web Services Cloud Storage*. Disponible : https ://aws.amazon.com

[33] Microsoft Corporation. (2024). *Microsoft Azure Cloud Platform*. Disponible : https ://azure.microsoft.com

[34] Google LLC. (2024). *Google Cloud Platform*. Disponible : https ://cloud.google.com

[35] Wireshark Foundation. (2024). *Wireshark Network Protocol Analyzer*. Disponible : https ://www.wireshark.org

[36] Nagios Enterprises. (2024). *Nagios Network Monitoring*. Disponible : https ://www.nagios.org

[37] SolarWinds Inc. (2024). *SolarWinds Network Performance Monitor*. Disponible : https ://www.solarwinds.com/network-performance-monitor

[38] Zabbix LLC. (2024). *Zabbix Enterprise Monitoring Solution*. Disponible : https ://www.zabbix.com

[39] The Cacti Group. (2024). *Cacti Network Graphing Tool*. Disponible : https ://www.cacti.net

[40] Cisco Systems. (2024). *NetFlow Network Traffic Analyzer*. Disponible : https ://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

[41] F5 Networks. (2024). *NGINX Web Server Documentation*. Disponible : https ://nginx.org/en/docs

[42] Microsoft Corporation. (2024). *Internet Information Services (IIS)*. Disponible : https ://www.iis.net

[43] Microsoft Corporation. (2024). *Microsoft Project - Gestion de projet*. Disponible : https ://www.microsoft.com/microsoft-365/project/project-management-software

[44] GNS3 Technologies. (2024). *GNS3 Network Simulator*. Disponible : https ://www.gns3.com

[45] Cisco Systems. (2024). *Cisco Packet Tracer*. Disponible : https ://www.netacad.com/courses/packet-tracer