2009

Proposition de la gestion du serveur D.H.C.P << cas de campus Kiriri >>

Niyonizigiye, Pierre Claver

UB, Institut Technique Supérieur

UNIVERSITE DU BURUNDI
INSTITUT TECHNIQUE SUPERIEUR
DEPARTEMENT DE GENIE ELECTROMECANIQUE

PROPOSITION DE LA GESTION DU SERVEUR D.H.C.P
« Cas du campus KIRIRI »

Par

NIYONIZIGIYE Pierre Claver
et
NDAYIHIMBAZE Moïse

Sous la direction de :

Ir. Constaque HAKIZIMANA
Ir. Yves NDUWAYO

Projet de fin d'Etudes présenté et soutenu
Publiquement en vue de l'obtention du grade
D'Ingénieur Industriel en Génie Electromécanique

Bujumbura, juillet 2009

DEDICACES

A Dieu Tout Puissant
A mon regretté père Jonas SIGUZA
A ma mère Noadie NTIKUYEKO
A mon épouse NKUNZIMANA Jeannine
A mon fils aîné Michaël Friend Orion NIYONIZIGIYE
A mon regretté Grand frère Gérard NIYONGOMA
A mon beau frère Ayubu BOBA
A ma belle famille
A mes frères et sœurs
A mes cousins et cousines
A mes amis

Je dédie ce mémoire
NIYONIZIGIYE Pierre Claver

A Dieu Tout Puissant
A mon père Barthélémy MAHINJA
A ma mère Esther NDIHOKUBWAYO
A mon regretté Donathe NIYONKURU
A madame Léocadie SABIMBONA
A mes frères et sœurs
A mes beaux frères
A mes cousins et cousines
A ma future épouse
A mes amis

Je dédie ce mémoire
NDAYIHIMBAZE Moïse

REMERCIEMENTS

Au terme de ce travail de fin d'études académiques, nous voudrions de tout notre cœur exprimer nos remerciements et notre gratitude à toutes les personnes qui ont contribué de près ou de loin à l'aboutissement de ce travail.

Nos vifs remerciements sont adressés aux Ingénieurs Constaque HAKIZIMANA et Yves NDUWAYO respectivement directeur et codirecteur de ce projet qui, malgré leurs multiples responsabilités ont pu nous suivre pendant ce travail avec enthousiasme. Leurs précieux conseils et leur disponibilité nous ont été d'une grande utilité, ce travail leur donne une entière satisfaction. Que tous les professeurs de l'université du Burundi, en particulier ceux de l'Institut Technique Supérieur, trouvent dans ce travail l'expression de notre reconnaissance pour la formation morale, technique, scientifique, intellectuelle et l'esprit de recherche dont ils nous ont dotés.

Nos sincères remerciements vont aussi au personnel de la société COMPUTEL et au personnel de l'Agence Universitaire de la Francophonie(AUF). Leur franche collaboration, leurs conseils nous ont suffisamment facilité la tâche.

En fin, aux parents, amis et connaissances qui ont contribué à notre épanouissement dès notre enfance, nous exprimons par la même occasion nos sentiments de reconnaissance.

A tous et à chacun nous disons

« Grand merci ».

ABREVIATIONS ET SIGLES

AH: Authentical header
ARP: Adress Resolution Protocol
ARPA: Advanced Research Project Agency Network
BOOTP: Boostrap Protocol
CAN: Campus Area Network
CIDR: Classless Inter Domain Routing
CUK: Campus Universitaire KIRIRI
C.I.D.R.: Classess Inter Domain Routing
dB: decibel
DHCP: Dynamic Host Configuration Protocol
DHCPNACK: Dynamic Host Configuration Protocol Negative acknowledgment
DNS: Domain Name System
EGP: Exterior Gateway Protocol
FAI: Fournisseur d'Accès Internet
FSA : Faculté des sciences Appliquées
FTP: File Transfer Protocol
HSRP: Host Standby Router Protocol
IANNA: Internet Assigned Numbers Agency
ICANN: Internet Cooperation for Assigned Names and Numbers
ICMP : Internet Control Message Protocol
IEPS : Institut d'Education Physique et de Sport
IETF: Internet Engineering Task Force
IGMP: Internet Group Management Protocol
IGRP: Interior Gateway Routing Protocol
IP: Internet Protocol
IPS: Internet Protocol Security
ITS: Institut Technique Supérieur
LAN: Local Area Network
MAC: Medium Access Control
MAN: Metropolitan Area Network
MAU: Multistation Access Unit
NAT: Network Adress Translation

NTP: Network Time Protocol
OSI: Open System Interconnection
OSPF: Open Shortest Path First
RARP: Reserve Address Resolution Protocol
RFC: Request for Comments
T: Time
TAN: Tinny Area Network
TCP/IP: Transmission Control Protocol/Internet Protocol
UDP: User Datagram Protocol
WAN: World Area Network
WINS: Windows Internet Naming Service
WWW: World Wide Web

TABLE DES MATIERES

I^{ère} PARTIE: THEORIE DES RESEAUX

CHAPITRE 0 : INTRODUCTION GENERALE

A l'heure actuelle, la communication est le centre de tout pour échanger des informations.
Dans les industries, le bon fonctionnement des différents secteurs repose sur la possibilité d'avoir accès à toutes les informations internes et externes nécessaires à un moment donné. Cette quantité d'informations est telle que l'on ne peut pas envisager de les stocker toutes dans chaque lieu géographique les nécessitant. Cette problématique se retrouve au niveau système ou différents sous systèmes échangent un grand nombre d'informations pour fonctionner. La possibilité de communiquer des informations actualisées entre des structures distantes est donc devenue un enjeu majeur. La solution choisie pour permettre cette communication est une connexion des différentes entités générant ou stockant des informations sous la forme d'un réseau informatique. Chaque entité peur partager une partie de ces ressources propres et recevoir des ressources des autres entités connectées.
En effet, dans les infrastructures réseaux, la gestion des adresses IP reste une tâche assez difficile. Cela est dû en général aux certaines adresses qui entrent en conflits, une longue durée de la configuration, aux adresses perdues et qui ne sont pas récupérées ainsi que l'administration de TCP/IP.
C'est dans cette perspective que ce travail a été mis en place pour étudier la gestion des adresses IP dans les réseaux TCP/IP à l'aide du serveur DHCP.
D'où notre sujet : PROPOSITION DE LA GESTION DU SERVEUR DHCP « cas du Campus Universitaire KIRIRI ».

0.1. Intérêt du sujet

L'évolution technologique s'accélère aujourd'hui, de nouvelles technologies sont inventées pour pallier aux lacunes des anciennes techniques.
En effet, à l'heure actuelle, dans la plupart des infrastructures réseaux, il y a un conflit d'adresses IP, des adresses perdues et qui ne sont pas récupérées. C'est pour cette raison que notre choix a été porté sur le serveur DHCP dans les réseaux TCP/IP.

0.2. Méthodologie de travail

Pour bien mener notre travail, nous avons consulté les documents des bibliothèques notamment la bibliothèque centrale de Mutanga et celle du campus Kiriri.
De plus, comme notre travail concerne la gestion du serveur DHCP dans les réseaux TCP/IP.
Les sites web internet dédiés aux réseaux TCP/IP nous ont été de grande utilité.

0.3. Articulation du sujet

Notre travail dont le sujet est : Proposition de la Gestion du Dynamic Host Configuration Protocol « cas du campus Kiriri » est subdivisé en sept chapitres regroupés en deux parties.
La première partie composée de chapitre I, chapitre II, chapitre III et le chapitre 0, elle sera consacrée à la théorie des réseaux tandis que la deuxième partie composée de chapitre IV, chapitre V, chapitre VI et chapitre VII essentiellement réservé à la gestion de DHCP, sera consacré aux fonctionnements du serveur DHCP, la description du campus universitaire Kiriri, installation de DHCP et découpage du réseau IP et enfin la configuration exploitation et maintenance du serveur DHCP.

CHAPITRE I : LE CONCEPT DE RESEAUX

I.1. Introduction

Le terme générique réseau définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.
Selon le type d'entité concernée, le terme utilisé sera ainsi différent :

- Réseau de transport : ensemble d'infrastructures et de dispositions permettant de transporter des personnes et des biens entre plusieurs zones géographiques ;
- Réseau téléphoniques : infrastructure permettant de faire circuler la voix entre plusieurs postes téléphoniques ;
- Réseau de neurones : ensemble de cellules interconnectées entre-elles ;
- Réseau de malfaiteurs : ensemble d'escrocs qui sont en contact les uns avec les autres ;
- Réseau informatique : ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangent des informations sous forme de données numériques (valeurs binaires).

Dans la suite nous nous intéresserons bien évidemment aux réseaux informatiques.

I.2. Intérêt d'un réseau informatique

Un réseau informatique peut servir plusieurs buts distincts :

- le partage de ressources ;
- la communication entre personnes ;
- la communication entre processus ;
- la garantie de l'unicité et de l'universalité de l'accès à l'information ;
- le jeu vidéo multi-joueurs.

Les réseaux permettent aussi de standardiser les applications, on parle généralement de « groupware » pour qualifier les outils permettant à plusieurs personnes de travailler en réseau.

Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement.
Voici un aperçu des avantages qu'offrent de tels systèmes :

- diminution des coûts grâce aux partages des données et des périphériques ;
- standardisation des applications ;
- accès aux données en temps utile ;
- communication et organisation plus efficace.

Aujourd'hui, avec Internet, on assiste à une unification des réseaux. Ainsi, les intérêts de la mise en place d'un réseau sont multiples, que ce soit pour une entreprise ou un particulier.

I.3. La similitude entre types de réseaux informatiques

Les différents types de réseaux informatiques ont généralement les points suivants en commun :

- serveurs : ordinateurs qui fournissent des ressources partagées aux utilisateurs par un serveur de réseau ;
- clients : ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau ;
- support de connexion : conditionne la façon dont les ordinateurs sont reliés entre eux ;
- données partagées : fichiers accessibles sur les serveurs du réseau ;
- imprimantes et autres périphériques partagés : fichiers, imprimantes ou autres éléments utilisés par usagers du réseau.
- ressources diverses : autres ressources fournies par le serveur.

I.4. Différents types de réseaux

On distingue généralement les deux types de réseaux suivants :

- les réseaux poste à poste (peer to peer/égal à égal) ;
- les réseaux organisés autour du serveur (Client/Serveur).

Ces deux types de réseau ont des capacités différentes.

Le type de réseau à installer dépend des critères suivants :

- taille de l'entreprise ;
- niveau de sécurité nécessaire ;
- type d'activités ;
- niveau de compétence d'administration disponible ;
- volume du trafic sur le réseau ;
- besoin d'utilisateur du réseau ;
- budget alloué au fonctionnement du réseau.

I.5. Représentation des données

Le but d'un réseau est de transmettre des informations d'un ordinateur à un autre. Pour cela, il faut dans un premier temps décider du type de codage des données à envoyer, c'est-à-dire sa représentation informatique. Celle-ci sera différente selon le type de données, car il peut s'agir de :

- données sonores ;
- données textuelles ;
- données graphiques ;
- données vidéo.

La représentation de ces données peut se diviser en deux catégories :

- une représentation numérique : c'est-à-dire le codage de l'information en un ensemble de valeurs binaires, soit une suite de 0 et de 1 ;
- une représentation anarchique : c'est-à-dire que la donnée sera représentée par la variation d'une grandeur physique continue.

I.6. Transmission des données

Pour que la transmission de données puisse s'établir, il doit exister une ligne de transmission, appelée aussi voie de transmission ou canal, entre les deux machines.
Ces voies de transmission sont constituées de plusieurs tronçons permettant de faire circuler les données sous forme d'ondes électromagnétiques, courant électrique, ondes lumineuses ou même acoustiques. On a donc un phénomène vibratoire qui se propage sur le support physique.

I.7. Codages des signaux de transmission

Pour qu'il puisse y avoir échange des données, un codage des signaux de transmission doit être choisi, celui-ci dépend essentiellement du support physique utilisé pour transférer les données ainsi que de la garantie de l'intégrité des données et de la vitesse de transmission.

I.8. Protocole de communication

Un protocole est un langage commun utilisé par l'ensemble des acteurs de la communication pour échanger des données. Toutefois, son rôle ne s'arrête pas là.
Un protocole permet aussi :

- l'initiation de la communication ;
- l'échange de données ;
- le contrôle d'erreur ;
- une fin de communication « courtoise ».

I.9. Les différents types de réseaux

On distingue différents types de réseaux selon leur taille, leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation.

On fait généralement trois catégories de réseaux : LAN, MAN, WAN
Il existe deux autres types de réseaux : les TAN identiques aux LAN mais moins étendus (2 à 3 machines) et les CAN identiques au MAN.

I.9.1. Les LAN

LAN signifie local area Network. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie, la plus répandue étant Ethernet.
Un réseau local est donc un réseau sous forme la plus simple.

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps et 1Gbps. La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.
En élargissant le contexte de la définition aux services qu'apporte le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'égal à égal dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire ;
- dans un environnement « client/serveur », dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

I.9.2. Les MAN

Les MAN interconnectent plusieurs LAN géographiquement proches au maximum de quelques dizaines de km à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits en général en fibre optique.

I.9.3. Les WAN

Un WAN interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons qui augmentent avec la distance et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau.

I.10. La topologie des réseaux locaux

I.10.1. Signification du terme topologie

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données).

Les dispositifs matériels mis en œuvre ne sont pas suffisants à l'utilisation du réseau local. En effet, il est nécessaire de définir une méthode d'accès standard entre les ordinateurs, afin que ceux-ci connaissent la manière de laquelle les ordinateurs échangent les informations, notamment dans le cas où plus de deux ordinateurs se partagent le support physique.

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes :

- topologies en bus ;
- topologie en étoile ;
- topologie en anneau ;
- topologie en arbre ;
- topologie maillée.

La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication.

I.10.2. La topologie en bus

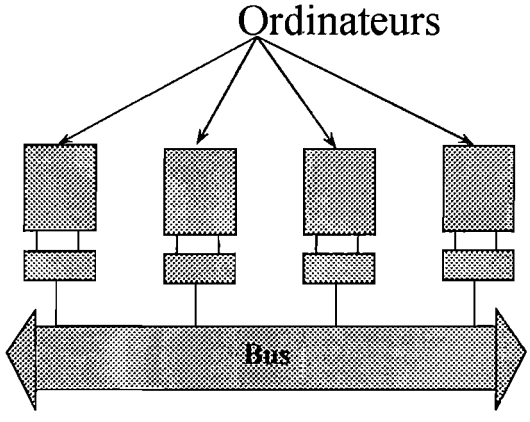

Figure I.1 : La topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot bus désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

I.10.3. La topologie en étoile

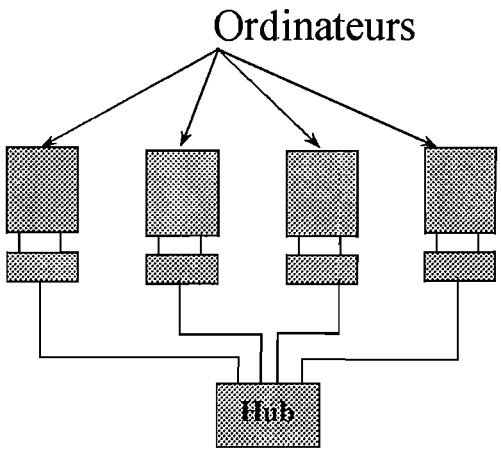

Figure I.2 : Topologie en Etoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub, littéralement moyeu de roue). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs.

Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Contrairement aux réseaux construits sur une topologie en bus, le réseau suivant une topologie en étoile est beaucoup moins vulnérable car une des connexions peut être débranchée sans paralyser le reste du réseau.
Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.
En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus, un matériel supplémentaire est nécessaire (le hub).

I.10.4. Topologie en anneau

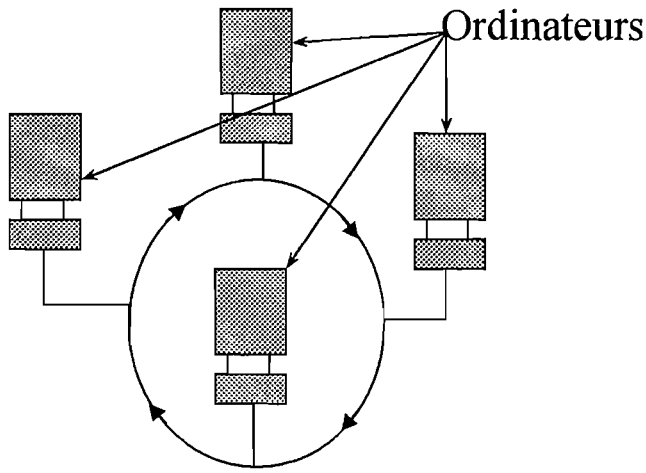

Figure I.3. Topologie en anneau

En réalité, dans une topologie en anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur appelé MAU qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.

I.11. Présentation de l'architecture d'un système client/serveur

De nombreuses applications fonctionnement selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc.

I.11.1. Avantages de l'architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction ;

- une meilleure sécurité : car le nombre de point d'entrée permettant l'accès aux données est moins important ;
- une administration au niveau du serveur : les clients ayant peu d'importance dans ce modèle sont moins administrés ;
- un réseau évolutif : grâce à cette architecture ; il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

I.11.2. Inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- un coût élevé dû à la technicité du serveur ;
- un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ; heureusement le serveur a une grande tolérance aux pannes notamment grâce au système RAID.

I.11.3. Fonctionnement d'un système client/serveur

Un système client/serveur fonctionne selon le schéma suivant :

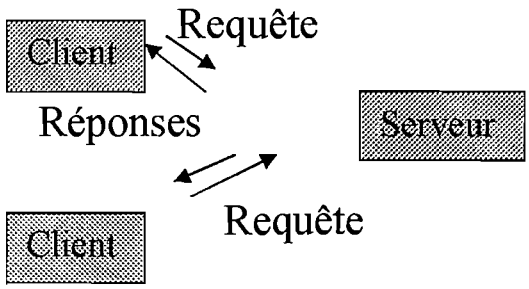

Figure I.4 : Fonctionnement du système client/serveur

- le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur ;
- le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

CHAPITRE II : LES MODELES DE REFERENCE OSI ET TCP/IP

II.1. Le modèle de référence OSI

II.1.1. Introduction

Tout comme le 19ème siècle fut le siècle de la machine à vapeur, le 20ème fut le siècle de la collecte, du traitement et de la distribution d'information. Ce dernier siècle vit donc l'apparition et le déploiement d'un réseau téléphonique à l'échelle planétaire, de l'invention de radio et de la télévision, des satellites de télécommunication et l'explosion de l'informatique.

L'une des caractéristiques de ces technologies est qu'elles ont eu tendance, petit à petit, à converger. On est progressivement passé des systèmes centralisés, avec généralement un unique ordinateur central que plusieurs informaticiens « alimentaient » de leur programmes, à une interconnexion globale des équipements, aux réseaux informatiques et systèmes repartis qui permettent de répartir les puissances de calcul et de stockage.

II.1.2. Les couches du modèle OSI

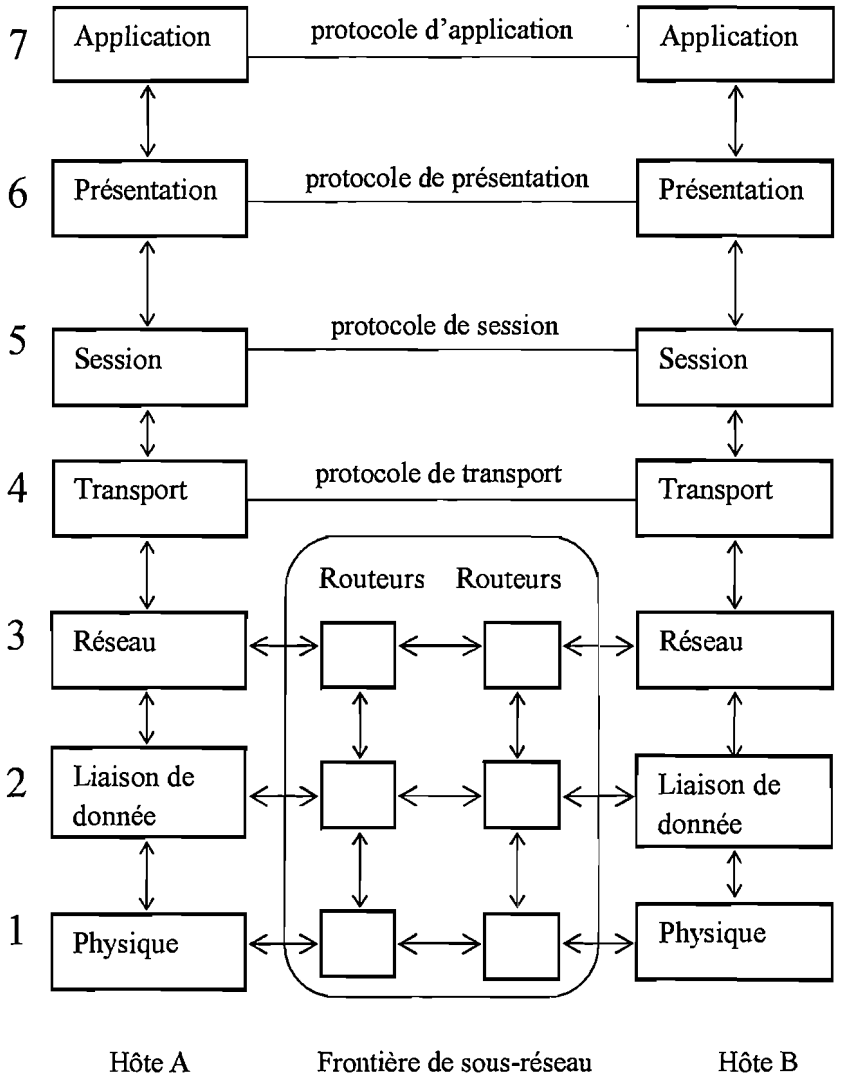

Figure II.1. Les couches du modèle OSI

Les principes qui ont conduit à ces 7 couches sont les suivantes :

- une couche doit être créée lorsqu'un niveau d'abstraction est nécessaire ;
- chaque couche a des fonctions bien définies ;
- les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles ;
- les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces ;

- le nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser.

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparés par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

II.1.2.1. La couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit être bien reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie, ...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de donnée.

II.1.2.2. La couche liaison de données

Elle à pour rôle de « liant » : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de Transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames d'acquittement renvoyées par le récepteur.

La couche liaison de données doit être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission.
De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique.
Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

II.1.2.3. La couche réseau

C'est la couche qui permet de gérer le sous-réseau, le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de la conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamique…).

La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer les fonctions de comptabilité pour facturation au volume.

II.1.2.4. Couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couches session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseaux par processus de la couche session pour répartir les données, par exemple pour améliorer le débit.

A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tous ceci doit être transparent pour la couche session.

Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garanti d'ordre de délivrance, diffusion du message à plusieurs destinateurs à la fois… ; cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau. Un des tous derniers rôles à évoquer est contrôle de flux. C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion avec toutes les contraintes qui y sont liées.

II.1.2.5. La couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établi également une liaison entre deux programmes d'application devant coopérer et commander leur dialogue (qui doit parler, qui parle,...) dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des ponts de reprise dans le front de données de manière à pouvoir reprendre les dialogues après une panne.

II.1.2.6. La couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

II.1.2.7. La couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie,…

II.1.3. Transmission de donnée au travers du modèle OSI

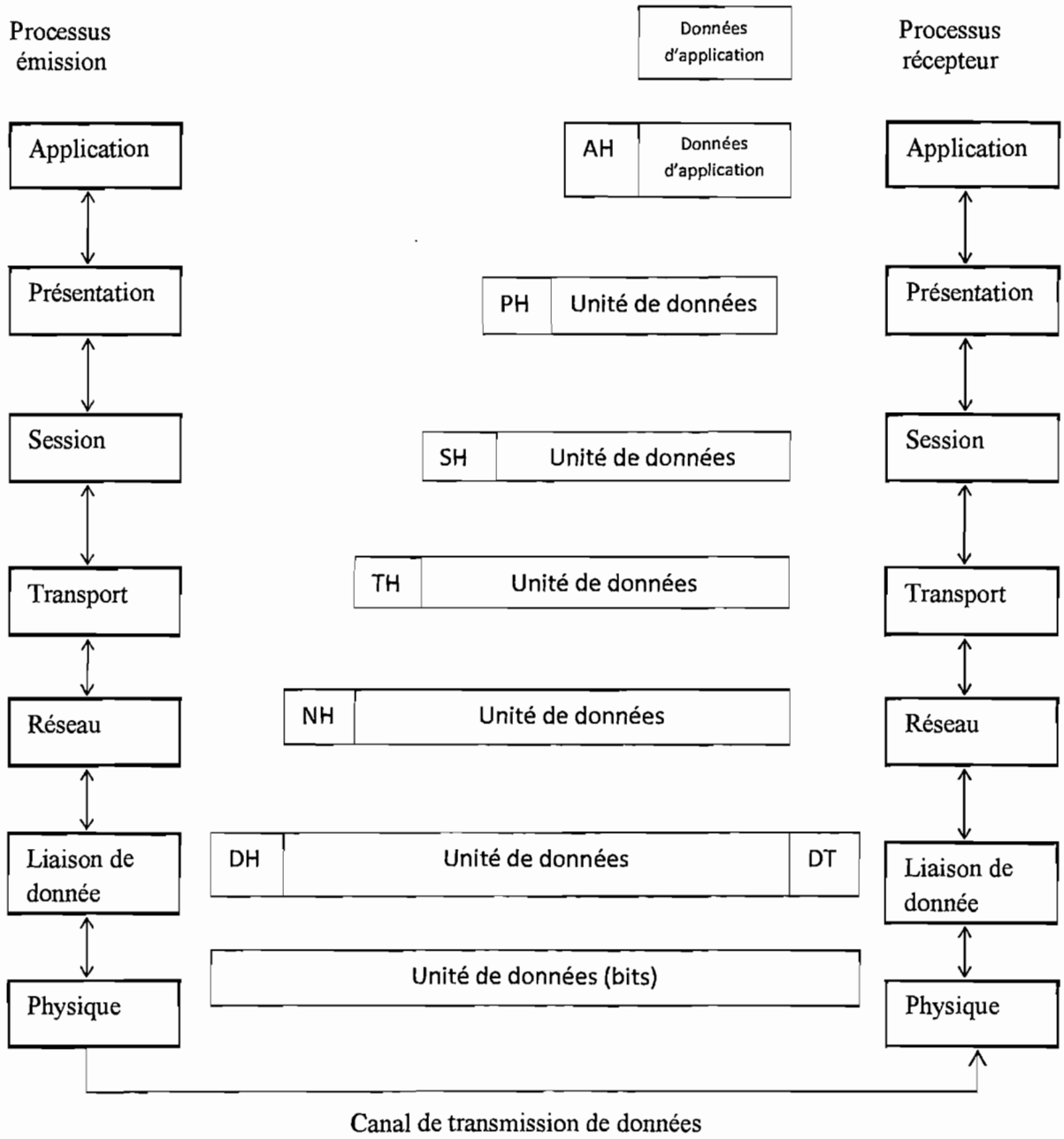

Figure II.2 : Transmission des données au travers du modèle OSI

Le processus émetteur remet les données à envoyer au processus récepteur à la couche application qui leur ajoute un en-tête application AH. Le résultat est alors transmis à la couche présentation.

La couche présentation transforme ce message et lui ajoute ou non un nouvel en-tête éventuellement nul. La couche présentation ne connaît et ne doit pas connaître l'existence éventuelle de AH ; pour la couche présentation, AH fait en fait partie des données utilisateurs. Une fois le traitement terminé, la couche présentation envoie le nouveau « message » à la couche session et le même processus recommence.

Les données atteignent alors la couche physique qui va effectivement transmettre les données au destinataire.
A la réception, le message va remonter les couches et les en-têtes sont progressivement retirés jusqu'à atteindre le processus récepteur :

Le concept important est le suivant : il faut considérer que chaque couche est programmée comme elle était vraiment horizontale, c'est-à-dire qu'elle dialoguait directement avec sa couche paire réceptrice. Au moment du dialogue avec sa couche paire, chaque couche rajoute un en-tête et l'envoie (virtuellement, grâce à la couche sous-jacente à sa couche paire).

II.1.4. Les principes de base du modèle

Les fonctions à exécuter doivent être divisées en niveaux séparables du point de vue physique et logique. Les fonctions associées dans un niveau doivent avoir une finalité cohérente :

- chaque couche doit contenir un volume suffisant afin de minimiser le nombre des couches ;
- les protocoles doivent agir uniquement à l'intérieur de la même couche ;
- les interfaces entre couches doivent être aussi simples que possible de manière à minimiser les échanges entre couches ;
- les couches doivent pouvoir être modifiées sans que soient affectés les services qu'elles offrent ;
- une fonction ne devrait apparaître qu'une seul fois ;
- l'ensemble doit être efficace en termes de performance.

Le premier objectif de la norme OSI a été de définir un modèle de toute architecture de réseau basé sur un découpage en 7 couches, chacune de ces couches correspondant à une fonctionnalité particulière d'un réseau. Les couches 1, 2, 3 et 4 sont dites basses et les couches 5, 6 et 7 sont dites hautes. Chaque couche est constituée d'éléments matériels et logiciels et offre un service à la couche située immédiatement au dessus d'elle en lui épargnant les détails d'implémentation nécessaires.
En fait, aucune donnée n'est transférée directement d'une couche n vers une autre couche n, mais elle l'est par étapes successives. Supposons un message à transmettre de l'émetteur A vers le récepteur B. Ce message, généré par une application de la machine A va franchir les couches successives de A via les interfaces qui existent entre chaque couche pour finalement atteindre le support physique.
Là, il va transiter via différents nœuds du réseau, chacun de ces nœuds couches du récepteur B via les différentes interfaces et atteint l'application chargée de traiter le message reçu.

II.2. Le modèle TCP/IP

II.2.1. Définition

TCP/IP est une suite de protocoles utilisé sur Internet. Il signifie Transmission Control Protocol/Internet Protocol, la notation TCP/IP se prononce « T-C-P-1-P », elle provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP. Pour cela, il se base sur l'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite de protocoles TCP/IP a été créée à l'origine dans un but militaire, elle doit répondre à un certain nombre de critères parmi lesquels on peut citer :

- le fractionnement des messages en paquet ;
- l'utilisation d'un système d'adresses ;
- le contrôle des erreurs de transmission de données pour un simple utilisateur, au même titre qu'un téléspectateur n'a pas besoin de savoir comment fonctionne son téléviseur. Toutefois, sa connaissance est nécessaire pour les personnes désirant administrer ou maintenir un réseau fonctionnant dans un système de protocole TCP/IP.

II.2.2. Les différentes couches

Afin de pouvoir appliquer le modèle TCP/IP à n'importe quelle machine indépendamment du système d'exploitation, le protocole TCP/IP a été décomposé en plusieurs modules effectuant chacun une tâche précise. De plus, ces modules effectuent ces tâches les uns après les autres dans un ordre précis, on a donné un système stratifié, c'est la raison pour laquelle on parle de modèle en couches.

Le terme de couche est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs niveaux de protocoles.

Ainsi, les données (paquets d'informations) qui circulent sur le réseau sont traitées successivement par chaque couche, qui vient rajouter un élément d'information appelé en-tête puis sont transmises à la couche suivante.

II.2.2.1. La couche liaison

Elle est la plus facile à comprendre, elle est composée de la quincaillerie réseau et des pilotes réseau, la couche réseau est le plus bas niveau de la pile de protocoles. Lorsqu'elle reçoit des données du réseau, elle prend les paquets du câble du réseau, en retire toutes les informations d'en-tête de la couche liaison, et les remet à la couche réseau lorsqu'elle transmet des données sur le réseau, elle reçoit les paquets de la couche réseau, y colle les informations en-tête de la couche liaison, et envoie les paquets sur le câble du réseau.
L'avantage de rendre indépendant la quincaillerie, c'est que les développeurs de protocoles n'ont à écrire la couche réseau qu'une seule fois. Ils fournissent une interface commune à la couche réseau en écrivant un pilote différent pour chaque type de carte réseau.

II.2.2.2. La couche réseau

C'est à cet endroit que le protocole IP et le protocole ICMP, entre autres, résident. ICMP est utilisé pour garantir la fiabilité du réseau et des informations par des utilitaires et trace route. IP est utilisée pour presque toutes les autres communications sur Internet. Lorsqu'elle envoie des paquets, elle doit trouver comment les faire parvenir à leur destination ; lorsqu'elle reçoit des paquets, elle doit trouver à qui ils appartiennent. Parce qu'elle n'a pas à se préoccuper si les paquets arrivent bel et bien à destination, ou que les paquets arrivent dans le même ordre qu'ils ont été envoyés, son travail est beaucoup simplifié.
Si un paquet pose des problèmes, par exemple, un paquet endommagé, IP s'en débarrasse tranquillement. Les couches supérieures ont la responsabilité d'assurer la fiabilité dans la réception des paquets.

Le comportement du protocole IP est dit « sans état » ou « débranché » car l'existence de paquets antérieurs ou futurs n'a pas d'importance dans le traitement du paquet courant. On pourrait débrancher le câble du réseau, attendre une minute, rebrancher le câble et IP n'en saurait rien. IP est capable d'envoyer les paquets à leur destination car chaque carte réseau sur Internet a sa propre adresse numérique unique. Ces adresses sont appelées adresses IP. Chaque interface a sa propre adresse. Si un ordinateur possède plusieurs interfaces, c'est le cas d'un routeur et chacune a sa propre adresse IP. L'Internet a la responsabilité d'assigner des ensembles d'adresses aux organisations, assurant ainsi l'unicité dans les adresses.

II.2.2.3. La couche transport

Il y a deux protocoles dans la couche transport : le TCP et UDP. Le TCP permet d'établir une communication point à point fiable alors que l'UDP ne le permet pas.
Le protocole UDP ressemble au protocole IP mais permet aux gens d'écrire des logiciels qui créent leur propre format de paquet ; ce qui est très utile si vous désirez écrire de nouveaux protocoles.

Le protocole TCP établit un « circuit virtuel » entre deux processus.

Il s'assure que les paquets sont reçus dans l'ordre transmis et que les paquets perdus sont retransmis. Des programmes interactifs tels que ftp et Telnet utilisent le protocole TCP.

II.2. 2.4. La couche application

C'est à cet endroit que l'utilisateur interagit avec le réseau ; tous les programmes réseaux tels que Telnet, ftp, mail, news, et les clients WWW sont situés dans la couche application. Ils utilisent le protocole TCP ou UDP pour communiquer avec d'autres ordinateurs.

II.2.3. Intérêt d'un système en couches

Le but d'un système en couches est de séparer le problème en différentes parties selon leur niveau d'abstraction. Chaque couche du modèle communique avec une couche adjacente.
Chaque couche utilise ainsi les services des couches inferieures et en fournit à celle de niveau supérieur.

II.2.4. Encapsulation des données

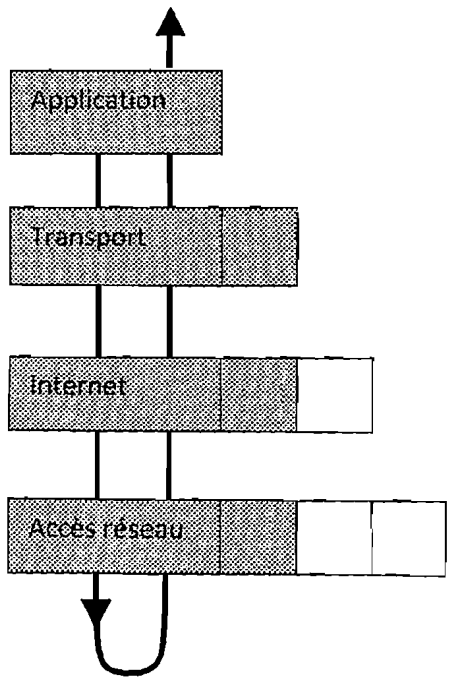

Figure II.3 : Les couches du modèle TCP/IP

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête ; ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.
A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête.
Ainsi les appellations changent suivant les couches :

- le paquet de données est appelé message au niveau de la couche application ;
- le message est ensuite encapsulé sous forme de segment dans la couche transport ;
- le segment une fois encapsulé dans la couche Internet prend le nom de datagramme.

Enfin, on parle de trame au niveau de la couche accès réseau.

La couche accès réseau est la première couche de la pile TCP/IP, il offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-a-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.
Ainsi, la couche accès réseau contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local, de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau.
Elle prend en charge les notions suivantes :

- acheminement des données sur la liaison ;
- coordination de la transmission de données (synchronisation) ;
- format des données ;
- conversion des signaux (analogique/numérique) ;
- contrôle des erreurs à l'arrivée.

Heureusement toutes ces spécifications sont transparentes aux yeux de l'utilisateur, car l'ensemble de ces tâches est en fait réalisé par système d'expiration, ainsi que les divers matériels permettant la connexion au réseau.
La couche Internet est la couche « la plus importante » car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP.

Elle permet l'acheminement des datagrammes vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à la réception.

La couche Internet contient 5 protocoles :

- protocole IP ;
- protocole ARP ;
- protocole ICMP ;
- protocole RARP ;
- protocole IGMP.

Les trois premiers protocoles sont les protocoles les plus importants de cette couche. Les protocoles des couches précédentes permettent d'envoyer des informations d'une machine à une autre. La couche transport permet à des applications tournant sur des machines distantes de communiquer. Le problème consiste à identifier ces applications. En effet, suivant la machine et son système d'exploitation, l'application pourra être un programme, une tache, un processus... de plus, la dénomination de l'application peut varier d'un système à une autre, c'est la raison pour laquelle un système de numéro a été mis en place afin de pouvoir associer un type d'application à un type de données ; ces identifiants sont appelés ports. La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type de réseau emprunté c'est-à-dire indépendamment des couches inférieures, il s'agit des protocoles suivants :

- TCP, un protocole orienté connexion qui assure le contrôle des erreurs ;
- UDP, un protocole non orienté connexion dont le contrôle d'erreur est archaïque.

La couche application est la couche située au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure, c'est-à-dire TCP ou UDP. Les applications de cette couche sont de différents types, mais la plupart sont des services réseau, c'est-à-dire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation.

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

- les services de gestion de fichier et d'impression ;
- les services de connexion au réseau ;
- les services de connexion à distance.

II.2.8. Comparaison du modèle OSI et TCP/IP

Les modèles OSI et TCP/IP sont tous fondés sur le concept de pile de protocoles indépendants. De plus, les fonctionnalités des couches sont globalement les mêmes.

Le modèle OSI est un modèle qui comporte 7 couches alors que le modèle TCP/IP n'en comporte que 4.

En réalité le modèle TCP/IP a été développé à peu près au même moment que le modèle OSI, c'est la raison pour laquelle il s'en inspire mais n'est pas totalement conforme aux spécifications du modèle OSI. Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire mais en contient uniquement quatre.

Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèles OSI étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

Le modèle OSI faisait clairement la différence entre 3 concepts principaux, alors que ce n'est plus tout à fait le cas pour le modèle TCP/IP. Ces 3 concepts sont les concepts de services, interfaces et protocoles. En effet, TCP/IP fait peu la distinction entre ces concepts, et ce malgré les efforts des concepteurs pour se rapprocher de l'OSI. Cela est du au fait que pour le modèle TCP/IP ; ce sont les protocoles qui sont d'abord apparus. Le modèle ne fait finalement que justification théorique aux protocoles, sans les rendre véritablement indépendants les uns des autres.

Enfin, la dernière grande différence est liée au mode connexion. Certes, le mode orienté connexion et sans connexion sont disponibles dans les deux modèles sur la même couche : pour le modèle OSI, ils ne sont disponibles qu'au niveau de la couche réseau, au niveau de la couche transport, seul le mode orienté connexion n'est disponible alors qu'ils ne sont disponibles qu'au niveau de la couche transport pour le modèle TCP/IP, la couche Internet n'offre que le mode sans connexion, le modèle TCP/IP a donc cet avantage par rapport au modèle OSI : les applications qui utilisent directement la couche transport ont véritablement choix entre les deux modes de connexion.

CHAPITRE III : ROUTAGE ET ADRESSAGE

III.1. Généralités

Le routage comporte deux aspects :
La transmission des datagrammes et la gestion des tables de routage. Chaque routeur dispose d'une table de routage qui établit une correspondance entre l'adresse réseau de destination et la sortie locale. Les protocoles de routage échangent des messages qui sont périodiques entre routeurs pour mettre à jour des tables.
Le routage mémorise les routes, affecte un ou plusieurs critères de coût à ces routes, prend en compte les pannes et les modifications.

La gestion des tables comporte différents aspects :
La diffusion de l'information et le calcul des chemins. Les routes sont apprises de différentes façons :

- route par défaut ou routes statiques ;
- routes apprises par un message de redirection ICMP ;
- routes apprises par le protocole de passerelle intérieure (RIP ou OSPF) ;
- routes apprises par un protocole de passerelle extérieure (EGP, BGP) ;
- routage par source.

Les routes statiques sont définies manuellement sur les routeurs, certains chemins privilégiés sont définis de cette façon, par exemple pour adresser directement le destinataire par un réseau longue distance.
Par contre, avec les protocoles de routage, les modifications de l'interconnexion sont prises en compte dynamiquement. La route par défaut est la route empruntée en l'absence d'une autre route.
La table de transmission IP détermine vers quelle sortie émettre un datagramme en circulation pour le rapprocher de son destinataire. L'adresse destination pointe dans la table de transmission pour déterminer la sortie vers laquelle envoyer le datagramme.

S'il n'ya ni route explicite, ni route par défaut, le datagramme est rejeté et un message ICMP « destination inaccessible » est envoyé à l'émetteur initial.
Le routage IP travaille au niveau de l'adresse réseau et non pas de l'adresse station, cela diminue notamment la taille des tables de routage. Avec l'agrégation d'adresses CIDR (Classess Inter Domain Routing), la taille des tables diminue également.
Des méthodes de rangement des adresses réseaux dans des arbres binaires sont employées pour retrouver un réseau IP dans une table. Chaque interface d'un routeur a une adresse IP utilisée par le routage. Une des difficultés du routage IP vient de l'absence de notion géographique dans l'adresse IP. Les tables de routage devront donc être exhaustives.

III.2. Algorithmes de routage

On distingue les algorithmes de routage à vecteur distance et à état de lien. Avec l'algorithme distribué dit « vecteur distance » l'émetteur transmet le tableau des distances avec les routeurs qu'il connaît. Avec l'algorithme « link state », c'est état des liaisons d'un routeur qui est transmis. Les algorithmes « link state » sont plus coûteux en mémoire et en temps de traitement. Par contre, comme chaque routeur à une connaissance globale du réseau, les routes sont calculées localement et non par convergence distribuée comme pour l'algorithme « vecteur distance ».

Les principaux mécanismes employés par le routage sont : l'inondation, le plus court chemin, l'arbre de recouvrement minimal. Les principes de la numérotation en séquence et de marquage temporel sont également mis en œuvre. L'un des problèmes du routage est la cohérence des informations.
Une analogie existe avec la communication humaine, une personne B apprend une information I de la personne A, puis A reçoit de nouvelles informations qui changent I, mais B propage toujours I à défaut de mise à jour de la part de A ou d'une autre source.

Les méthodes de diffusion de proche en proche employées par les protocoles introduisent tous les délais de diffusion de l'information à la totalité des routeurs.
Le nombre croissant de réseaux augmente les mises à jour, les délais et les problèmes de cohérence.

Une table de routage mémorise pour chaque réseau connu des informations du type suivant : l'adresse IP réseau, la voie de sortie associé ou l'adresse du routeur suivant, le compteur de liaison qui indique le nombre de liaisons existant entre le routeur et la destination, la temporisation exprime le temps écoulé depuis la dernière mise à jour de l'entrée.

Selon le protocole de routage, le coût associé à chaque lien est fourni par l'administrateur, calculé par le routeur de façon statique ou dynamique ou bien est basé sur une combinaison des deux approches. Une adresse IP est souvent affectée à l'adresse de boucle locale pour disposer d'une adresse stable indépendante de la coupure d'un lien.

III.3. Concepts de base

Une couche minimale de routage fonctionne sur chaque station de travail, elle détermine pour chaque fragment à émettre si le réseau destinataire est local ou distant. Une comparaison entre les adresses réseaux locale et destinataire l'indique. Pour un destinataire local la délivrance sera directe, alors que pour un destinataire distant, la pile IP envoie au routeur de sortie. L'adresse IP du routeur par défaut est connue par paramètre ou par DHCP, son adresse MAC est connue par ARP. Des routes statiques sont également définies sur station à l'aide de la commande route. ARP, Mécanisme qui fait correspondre une adresse MAC niveau 2 et une adresse IP niveau 3.

Le choix d'une route se pose seulement s'il existe plusieurs sorties.
Beaucoup de routeurs sont positionnés en impasse et ne disposent que d'une seule entrée-sortie, ils ne nécessitent donc pas l'échange de tables de routage, cette fonctionnalité sera donc invalidée pour éviter de surcharger inutilement le réseau et éviter des facturations inutiles pour les lignes facturées à l'utilisation.

III.4. Les principaux protocoles de routage interne

- RIP : ce premier protocole de routage associé aux réseaux TCP/IP favorise l'interopérabilité des routeurs ;
- RIP détermine le chemin le plus court à suivre par un paquet pour atteindre sa destination finale à travers des routeurs en comptant le nombre de sauts nécessaires ;
- IGRP : ce protocole de routage es développé par Cisco pour ses routeurs multi-protocoles. Le désavantage d'IGRP est qu'il est propriétaire et que certaines de ses fonctionnalités sont protégées par des brevets ;
- OSPF : ce protocole de routage sécurisé pour les réseaux IP est spécifié par l'IETF est le routage interne normalisé par l'OSI.

III.5. Adressage IP

III.5.1. Qu'est-ce qu'un adressage IP

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP, qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, 194.153.205.26 est une adresse IP donnée sous une forme technique.
Ces dresses servent aux ordinateurs du réseau pour communiquer entre-eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau. C'est l'ICANN, remplaçant l'IANA depuis 1998 qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public Internet.

III.5.2. Déchiffrement d'une adresse IP

Une adresse IP est une adresse de 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP :

Une partie des nombres à gauche désigne le réseau et est appelée ID de réseau en anglais netID,

Les nombres de droite désignent les ordinateurs de ce réseau et est appelée ID d'hôte en anglais host-ID.

III .5.3 Caractéristiques de IP

- une adresse IP est un nombre de 32 bits codés sur 4 octets ;
- Pour l'usage humain, cette adresse est représentée sous la forme décimale pointée W.X .Y.Z par exemple, 192.168.0.12, cette adresse est normalement sous format binaire, sauf qu'elle est par convention représentée sous format décimale afin qu'elle soit facilement retenue. Exemple : IP 212.217.0.1 correspond à la notation binaire : 11010100. 11011001. 00000000. 00000001
- Chaque numéro dans le champ d'adresse doit être compris entre 0 et 225(2^8=256 nombres).

Selon que l'adresse est de classe A, B ou C, les premiers champs à partir de la gauche désignent le réseau, les champs à droite désignent la machine.

III.5.4 Les classes

Les réseaux TPC/IP se divisent en trois grandes classes qui ont des tailles prédéfinies, ces 3 classes de réseau sont notées A, B et C et se différencient par le nombre d'octets désignant le réseau,
Dans une adresse IP, la partie Net ID peut être codée sur 1, 2 ou 3 octets. Les trois bits de poids fort du premier octet déterminent la classe de l'adresse et définissent ainsi implicitement le nombre d'octets utilisés pour le codage de l'identifiant réseau.

Classe A

Dans une adresse IP de classe A, l'adresse réseau est désignée par le premier octet qui doit être d'une valeur inférieure à 128, le réseau composé de 0 uniquement n'existe pas, et le réseau 127 désigne l'ordinateur local.

La plage utilisable est comprise entre 1.0.0.0. et 126.0.0. 0 car 2^7 donc allant de 1 à 128-2.
Ce réseau peut contenir 16646144 ordinateurs.

Classe B

Dans une adresse IP de classe B, l'adresse réseau est désignée par les deux premiers octets. La plage utilisable est comprise entre 128.0.0.0 et 191.255.0.0 et peut contenir 65024 ordinateurs.

Classe C

Dans une adresse IP de classe C, l'adresse réseau est désignée par les trois premiers octets. La plage utilisable est comprise entre 192.0.0.0 et 233.255.255.0 et peut contenir 254 ordinateurs. On peut assigner à un hôte une adresse IP statique ou une adresse IP dynamique. Elle est statique quand on affecte une adresse figée (fixe) qu'il utilise à chaque fois qu'il se connecte au réseau, elle est dynamique quand on utilise un serveur DHCP qui affecte aléatoirement des adresses IP aux différentes machines au sein des réseaux, cette méthode est mieux préférée lors de l'adressage pour éviter les conflits d'adresses.

III.5.5. Masque de réseau

Pour comprendre ce qu'est un masque, il peut-être intéressant de consulter la section « assembleur » qui parle du masquage en binaire. En résumé, on fabrique un masque contenant des 1 aux emplacements des bits que l'on désire conserver, et des 0 pour ceux que l'on veut annuler. Une fois ce masque créé, il suffit de faire un ET logique entre la valeur que l'on désire et annuler le reste.

Ainsi, un masque réseau, en anglais netmask se présente sous la forme de 4 octets séparés par des points comme une adresse IP, il comprend dans sa notation binaire des zéros au niveau des bits de l'adresse IP que l'on veut annuler et des 1 au niveau de ceux que l'on désire conserver.

III.5.5.1. Intérêt d'un masque de sous réseau

Le premier intérêt d'un masque de sous-réseau est de permettre d'identifier simplement le réseau associé à une adresse IP.

En effet, le réseau est déterminé par un certain nombre d'octets de l'adresse IP, 1 octet pour les adresses de classe A, 2 pour les adresses de classe B, et 3 octets pour la classe C. Or, un réseau est noté en prenant le nombre d'octets qui le caractérisent, puis en complétant avec des 0, le réseau associé à l'adresse 34.56.123.12 est par exemple 34.0.0.0. car il s'agit d'une adresse IP de classe A. Par exemple pour connaître l'adresse du réseau associé à l'adresse IP 34.56.123.12, il suffit donc d'appliquer un masque dont le premier octet ne comporte que des 1 soit 255 en notation décimale, puis des 0 sur les octets suivants.
Le masque est :
11111111.00000000.00000000.00000000
Le masque associé à l'adresse IP 34.208.123.12 est donc 255.0.0.0.
La valeur binaire de 34.208.123.12 est :
00100010.11010000.01111011.00001100

Un ET logique entre Adresse IP et le masque donne ainsi le résultat suivant :
00100010.11010000.01111011.00001100
ET
11111111.00000000.00000000.00000000
00100010.00000000.00000000.00000000
Soit 34.0.0.0. Il s'agit bien du réseau associé à l'adresse 34.208.123.12.
En généralisant, il est possible d'obtenir le masque correspondant à chaque classe d'adresse :
Pour une adresse de classe A, seul le premier octet doit être conservé. Le masque possède la forme suivante :
11111111.00000000.00000000.00000000, c'est-à-dire 255.0.0.0 en notation décimale ; pour une adresse de classe B, les deux premiers octets doivent être conservés, ce qui donne le masque suivant 11111111.11111111.00000000.00000000, correspondant à 255.255.0.0. en notation décimale ;
Pour une adresse de classe C, avec le même raisonnement, le masque possédera la forme suivante 11111111.11111111.11111111.00000000 c'est-à-dire 255.255.255.0 en notation décimale.

III.6. L'adressage physique

Les adresses matérielles de la machine source et destination notées par les termes IP sont le plus souvent appelées adresses MAC. Celles-ci doivent référencer un matériel de manière unique dans le monde informatique. Ce matériel peut être un serveur, un poste de travail, une imprimante, un routeur, ...

III.7. L'adressage logique

L'adressage logique permet de référencer un matériel dans le réseau. Souvent, on parle d'adresse logique pour une machine (ordinateur...). Or, c'est un abus de langage car l'on confond l'interface réseau de la machine et la machine elle-même.
Souvent celle-ci n'a qu'une interface réseau mais il arrive aussi que certains routeurs, firewall, serveurs ..., en aient plusieurs.
Elles auront alors plusieurs adresses logiques, une par interface.
Ainsi, si l'on a deux interfaces réseaux (deux cartes réseaux), ce sera une machine, deux adresses MAC, deux adresses logiques, voire même deux noms pour la même machine.

Une autre distinction existe tout comme pour les adresses physiques entre l'adresse logique privée, et l'adresse logique publique si le réseau n'est pas un réseau interconnectés, réseau intranet par exemple, l'administrateur peut fixer les adresses à sa convenance même si elles existent déjà sur le réseau Internet, il y aura pas d'interaction ou de conflit du fait que son réseau n'est pas interconnecté. Par contre si le réseau créé doit être interconnecté, il faudra, comme pour l'dresse MAC, une adresse logique unique pour chacune des interfaces réseaux.

III.8. Les protocoles de communication

Les protocoles sont un ensemble de règles et de procédures qui règlent les échanges entre les ordinateurs, ce sont les conventions qui déterminent la façon de deux ordinateurs communiquent.
Plusieurs protocoles fonctionnent ensemble afin que les données soient préparées, transférées, réglées et traitées.

Le fonctionnement des protocoles doit être coordonné afin d'éviter des conflits ou des opérations incomplètes.
L'envoi de données est décomposé en plusieurs tâches:

- Reconnaissance des données,
- segmentation des données en paquets plus faciles à traiter.
- Ajout d'informations dans chaque paquet de données afin de :
  - Définir l'emplacement des données
  - Identifier le récepteur
  - Ajout d'informations de séquence et de contrôle d'erreurs
  - Dépôt des données sur le réseau et envoi.

LE PROTOCOLE TCP/IP.

Nom d'une famille de protocoles de communication mis au point par la défense américaine entre 1969 et 1982, date de leur mise dans le domaine public. C'est le protocole de base sur Internet, TCP est un protocole sécurisé orienté connexion conçu pour s'implanter dans un ensemble de protocoles multicouches, supportant le fonctionnement de réseaux hétérogènes.

Le protocole IP se charge du routage des informations (couche réseau) et le protocole TCP se charge du contrôle des données transmises (couche transport).
TCP/IP représente l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP.
Ses fonctions sont :

- Le fractionnement des messages en paquet
- L'utilisation d'un système d'adressage
- L'acheminement de données sur le réseau
- Le contrôle des erreurs de transmission

Il est question ici des protocoles de niveau 3 (réseau) et 4 (transport) du modèle OSI concernant les réseaux locaux et plus particulièrement Internet. Les protocoles importants de la couche réseau : la couche réseau comporte les protocoles IP, ARP,RARP.
Le protocole IP est associé à deux protocoles de la couche transport TCP et UDP. Cette association fait que l'on parle très souvent de protocoles TCP/IP ou UDP/IP comme si c'était un seul et même protocole.

Le protocole IP gère l'adressage logique, le nommage des matériels, le Routage, la fragmentation et le réassemblage des paquets. Pour cela il Utilise des datagrammes (unité de données) permettant le transit des Informations.

III.9 Principes de base du routage

III.9.1. Définition

La raison d'être IP est bien d'interconnecter des réseaux physiques hétérogènes ou non. Ce protocole de niveau 3 propose un format de paquets, un format d'adressage et une logique d'acheminement des paquets entre les réseaux physiques.
Cette dernière fonction se nomme: le routage.
Cette fonction est réalisée généralement par des équipements spécifiques appelés des routeurs. Ces routeurs appliquent tous les mêmes règles de base pour que le transfert des paquets soit cohérent. Ce sont les règles de routage.
Sur l'Internet ou au sein de toute entité qui utilise IP, les datagrammes ne sont pas routés par des machines Unix, mais par des routeurs dont c'est la fonction par définition. Ils sont plus efficaces et plus perfectionnés pour cette tâche par construction, et surtout autorisent l'application d'une politique de routage, ce que la pile IP standard d'une machine Unix ne sait pas faire. Toutefois il est courant dans les petits réseaux, ou quand le problème à résoudre reste simple, de faire appel à une machine Unix pour ce faire.
Le routage des datagrammes se fait au niveau de la couche IP, et c'est son travail le plus important. Toutes les machines multiprocessus sont théoriquement capables d'effectuer cette opération.
La différence entre un « routeur » et un « hôte » est que le premier est capable de transmettre un data gramme d'une interface à un autre et pas le deuxième.
Cette opération est délicate si les machines qui doivent dialoguer sont connectées à de multiples réseaux physiques, du point de vu idéal, établir une route pour des datagrammes devrait tenir compte d'éléments comme la charge du réseau, la taille des datagrammes, le type de service demandé.
Les délais de propagation, l'état des liaisons, le trajet le plus court, ... la pratique est plus rudimentaire.

Il s'agit de transporter des datagrammes aux travers de multiples réseaux physiques. Donc aux travers de multiples passerelles. On divise le routage en deux grandes familles :

- Le routage direct

Il s'agit de délivrer un data gramme à une machine raccordée au même LAN. L'émetteur trouve l'adresse physique du correspondant encapsule le data gramme dans une trame et l'envoie.

- Le routage indirect

Le destinataire n'est pas sur le même LAN comme précédemment. Il est absolument nécessaire de franchir une passerelle connue d'avance ou d'employer un chemin par défaut. .
En effet, toutes les machines à atteindre ne sont pas forcément sur le même réseau physique. C'est le cas le plus courant par exemple sur l'Internet qui regroupe des centaines de milliers de réseaux différents.

III.9. 2. Le routage dynamique

Il existe sur les routeurs certaines applications qui permettent aux routeurs voisins d'échanger de l'information quand à leurs tables de routage; ce sont les protocoles de routage.

III. 9. 3 Le routage statique

Dans le routage statique, l'administrateur réseau doit informer, paramétrer les routeurs pour leur donner des ordres de routage : sur quelle interface envoyer les datagrammes pour le réseau de destination d'adresse IP. C'est une modification statique de la table de routage des routeurs.

IIème PARTIE : LE SERVEUR DHCP

CHAPITRE IV : PRESENTATION GENERALE DE DHCP

IV.1. Introduction

Dynamic Host Configuration Protocol (DHCP) est une série de mots désignant un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous réseau.

Les adresses IP peuvent être statiques ou dynamiques. Les adresses statiques ne changent jamais, l'administrateur du réseau assigne des adresses IP fixes à chaque ordinateur. Les adresses dynamiques peuvent changer, quelquefois rarement, et en d'autres occasions chaque fois que l'utilisateur fait quelque chose sur le réseau; ces adresses n'ont jamais à être assignées manuellement à chaque ordinateur. Pour ce faire, il y a un programme spécial sur le réseau qui agit comme gestionnaire d'adresses IP. Ce gestionnaire donne les adresses non utilisées à chaque ordinateur demandeur; ainsi lorsqu'un ordinateur veut être connecté au réseau, il demande et reçoit une adresse unique qu'il peut utiliser pour sa « session », il se base sur l'adresse MAC pour différencier chaque machine. Ce gestionnaire d'adresses s'appelle DHCP.

La conception initiale d'IP supposait la préconfiguration de chaque ordinateur connecté au réseau avec les paramètres TCP/IP adéquats : c'est l'adressage statique. Sur des réseaux de grandes dimensions ou étendus, ou des modifications interviennent souvent, l'adressage statique engendre une lourde charge de maintenance et des risques d'erreurs. En outre les adresses assignées ne peuvent être utilisées même si l'ordinateur qui la détient n'est pas en service.

Un cas typique ou ceci pose de problèmes est celui des fournisseurs d'accès à internet qui ont en général plus de clients que d'adresses IP à leur disposition mais dont tous les clients ne sont jamais connectés en même temps.

Le serveur DHCP apporte une solution à ces deux inconvénients :

- Seuls les ordinateurs en service utilisent une adresse de l'espace d'adressage;
- Toute modification des paramètres (adresse de la passerelle, des serveurs de noms) est répercutée sur les stations lors du redémarrage;

La modification de ces paramètres est centralisée sur les serveurs DHCP.

L'affectation dynamique d'une adresse IP est l'élément fondamental, mais il y en a beaucoup d'autres comme le masque réseau, le nom d'hôte, le nom de domaine, la passerelle et les serveurs de noms. En outre, elle peut fournir d'autres informations, comme un serveur d'horloge.

De nombreuses personnes sont contre le DHCP parce qu'elles ne le voient que comme un moyen dont un Fournisseur d'Accès Internet (FAI) vous offre une adresse IP qui change. Ceci complique bien sûr l'annonce d'un serveur. Par ailleurs, DHCP peut nous épargner une bonne partie du travail de configuration permanente au sein de l'entreprise ou de l'organisation.
Le LAN a des adresses IP privées et utilise la NAT pour gérer les connexions depuis les systèmes internes vers l'Internet.

La plupart des routeurs de cette classe permettent :

- de cloner l'adresse d'un de nos ordinateurs : ce comportement vous permet de laisser le FAI penser qu'il dialogue avec un système informatique que nous avons préalablement identifié plutôt qu'un routeur auquel de multiples machines sont éventuellement connectées.

- de gérer des adresses IP statiques : cela signifie que nous pouvons choisir une adresse réseau locale et affecter des adresses spécifiques dans cette plage.
- d'affecter dynamiquement des adresses **IP** d'une plage spécifiée.

Le DHCP est un protocole réseau qui a pour but de simplifier l'administration d'un réseau. Le protocole DHCP offre un moyen de centraliser la configuration des machines du réseau, en mettant à disposition un serveur au sein d'un réseau local.

Un serveur DHCP permet, comme son nom l'indique, d'attribuer de façon dynamique une configuration. Ce serveur permet d'attribuer automatiquement des adresses :

- IP : pour chaque ordinateur à partir du moment où i sera connecté physiquement au réseau.
- Passerelle (ou gateway en Anglais) : un réseau local dispose d'une adresse **IP** privée, pour pouvoir sortir de notre réseau local et accéder à un autre réseau, on utilise une passerelle, appelé aussi routeur.
- Serveur DNS : un nom est plus facile à retenir que *83.43.23.80.* le rôle du serveur DNS est ainsi de faire correspondre un nom de domaine (ou de machine) à une adresse IP.
- serveur Windows Internet Naming Service (WINS) : il s'agit d'un serveur de nom comme DNS, mais spécifique à Windows,
- Serveur Network Time Protocol (NTP) : les serveurs NTP permettent d'attribuer une même date et une même heure à l'ensemble d'un réseau, un service spécifique d'IPCop est consacré à cela.

Ainsi le protocole DHCP permet à un ordinateur qui se connecte au sein d'un réseau d'obtenir dynamiquement sa configuration tout en évitant les conflits d'adresses, il évite également la reconfiguration des ordinateurs portables lors d'un changement de réseau, la configuration des machines clientes s'en trouve donc très simplifiée, l'administrateur peut facilement avoir un œil sur son réseau et connaître les adresses allouées aux clients DHCP.

IV.2. Les baux

Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées avec une date de début et une date de fin de validité. C'est ce qu'on appelle un « bail ».

Un client qui voit son bail arriver à terme peut demander au serveur une prolongation du bail par un DHCPREQUEST.

De même, lorsque le serveur verra un bail arriver à terme, il émettra un paquet DHCPNAK pour demander au client s'il veut prolonger son bail.

Si le serveur ne reçoit pas de réponse valide, il rend disponible l'adresse IP.
C'est toute la subtilité du DHCP, on peut optimiser l'attribution des adresses IP en jouant sur la durée des baux. Le problème est la. Si aucune adresse n'est libérée au bout d'un certain temps, plus aucune requête DHCP ne pourra être satisfaite, faute d'adresses à distribuer.
Sur un réseau ou beaucoup d'ordinateurs se branchent et se débranchent souvent, réseau d'école ou de locaux commerciaux par exemple, il est intéressant de proposer des baux de courte durée. A l'inverse, sur un réseau constitué en majorité de machines fixes, très peu souvent rebootées, des baux de longues durées suffisent.

IV.3. Fonctionnement du serveur DHCP

II faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe.

Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, *le serveur DHCP.*

.

Le mécanisme de base de la communication est BOOTP. Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP.
Pour faire cela la technique utilisée est le broadcast, pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast sur le réseau local. Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast contenant toutes les informations requises pour le client.

On pourrait croire qu'un seul paquet peut suffire à la bonne marche du protocole. En fait, il existe plusieurs types de paquets DHCP susceptibles d'être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client:

- DHCPDISCOVER pour localiser les serveurs DHCP disponibles ;
- DHCPOFFER réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres.

DHCPREQUEST : requête diverse du client pour par exemple prolonger son bail,

- DHCPACK réponse du serveur qui contient des paramètres et l'adresse IP du client,

- DHCPNAK : réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau,
- DHCPDECLINE : le client annonce au serveur que l'adresse est déjà utilisée,
- DHCPRELEASE : le client libère son adresse IP,
- DHCPINFORM : le client demande des paramètres locaux, il a déjà son adresse IP.

Le premier paquet émis par le client est un paquet de type DHCPDISCOVER. Le serveur répond par un paquet DHCPOFFER, en particulier pour soumettre une adresse IP au client. Le client établit sa configuration, puis fait un DHCPREQUEST pour valider son adresse IP. Le serveur répond simplement par un DHCPACK avec l'adresse IP pour confirmation de l'attribution.

Normalement, c'est suffisant pour qu'un client obtienne une configuration réseau efficace, mais cela peut être plus ou moins long selon que le client accepte ou non l'adresse IP :

- tout serveur DHCP ayant reçu ce datagramme, s'il est en mesure de proposer une adresse sur le réseau auquel appartient le client, diffuse une offre DHCP à l'attention du client, identifié par son adresse physique. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous-réseau qu'il propose au client. II se peut que plusieurs offres soient adressées au client.
- le client retient une des offres reçues (la première qui lui parvient), et diffuse sur le réseau un datagramme de requête DHCP. Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client. Elle a pour effet de demander.
- au serveur choisi l'assignation de cette adresse, l'envoi éventuel des valeurs des paramètres, et d'informer les autres serveurs qui ont fait une offre qu'elle n'a pas été retenus.

- le serveur DHCP choisi élabore un datagramme d'accusé de réception *DHCPack* qui assigne au client l'adresse IP et son masque de sous-réseau, la durée du bail de cette adresse, deux valeurs T 1 et T2 qui déterminent le comportement du client en fin de bail, et éventuellement d'autres paramètres.

IV.4. Renouvellement du bail

Les adresses IP dynamiques sont octroyées pour une durée limitée, qui est transmise au client dans l'accusé de réception qui clôture la transaction DHCP. La valeur Tl qui l'accompagne détermine la durée après laquelle le client commence à demander périodiquement le renouvellement de son bail auprès du serveur qui lui a accordé son adresse, couramment la moitié de la durée du bail. Cette fois la transaction est effectuée par transmission IP classique, d'adresse à adresse. Si lorsque le délai fixé par la deuxième valeur T2 est écoulé, le bail n'a pas pu être renouvelé, le client demande une nouvelle allocation d'adresse par diffusion. Si au terme du bail client n'a pu ni en obtenir le renouvellement, ni obtenir une nouvelle allocation, l'adresse est désactivée et il perd la faculté d'utiliser le réseau TCP/IP.

IV.5. Les messages DHCP

DHCP se compose de huit types de messages discrets :

Message DHCP	Description
Découvrez DHCP	UDP diffusion de client DHCP pour localiser les serveurs disponibles.
Offre DHCP	Serveur DHCP aux clients en réponse à DHCP Découvrez avec offre de paramètres de configuration.
Requête DHCP	La réaction des clients aux serveurs soit ; demandant l'offre des paramètres d'un serveur ; ce qui confirme l'exactitude de l'adresse précédemment alloués après, par exemple, le système de redémarrer la machine, ou d'étendre le bail sur une adresse réseau.
DHCPACK	serveur au client avec les paramètres de configuration
DHCPNAK	Serveur au client indiquant que l'adresse est incorrecte (par exemple, la clientèle a déménagé dans le nouveaux sous-réseau) ou le bail du client est expiré.
Baisse de DHCP	Message d'erreur du client DHCP au serveur en indiquant que l'adresse réseau est déjà en service.

Tableau IV.1. Les messages DHCP

IV.6. Renouvellement d'adresse

La première requête émise par le client est un message DHCPDISCOVER. Le serveur répond par un DHCPOFFER, en particulier pour soumettre une adresse IP au client.
Le client établit sa configuration, demande éventuellement d'autres paramètres, puis fait un DHCPREQUEST pour valider son adresse IP. Le serveur répond simplement par un DHCPACK avec l'adresse IP pour confirmation de l'attribution. Normalement, c'est suffisant pour qu'un client obtienne une configuration réseau efficace.

Mais cela peut être plus ou moins long selon que le client accepte ou non l'adresse IP ou demande des informations complémentaires...

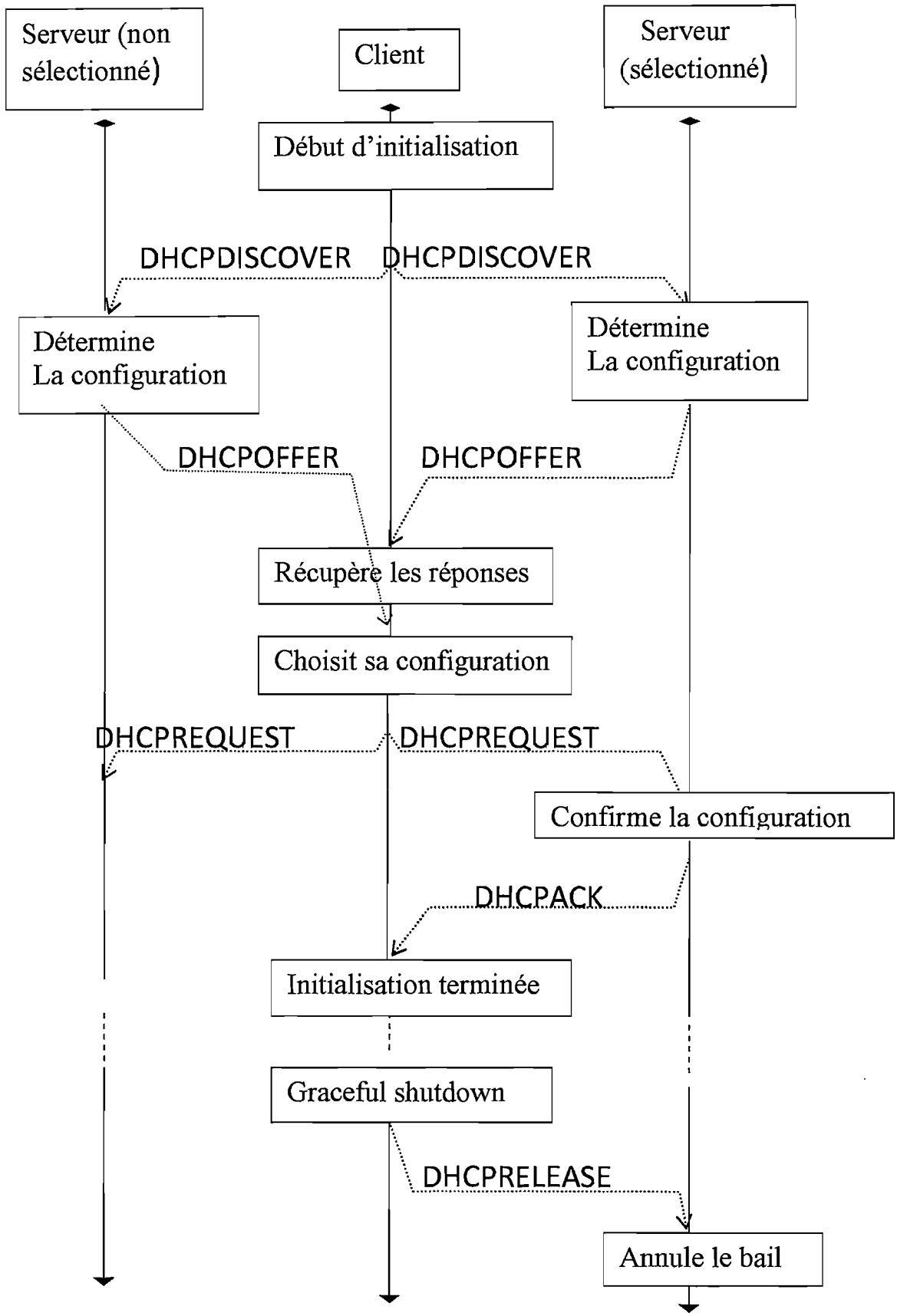

Figure IV.3: Renouvellement d'adresse

IV.6 Les dialogues DHCP

Les requêtes sont transmises du client au port du serveur. Les réponses sont transmises du serveur au port du client. Si le client ignore l'adresse du serveur, il envoie son message par un « broadcast » sur le réseau local. Comme seuls les serveurs DHCP écoutent sur le port, les autres postes de travail détruisent ce message sur réception. Le client attend ensuite sur le port pour les réponses du serveur. Certains systèmes ne permettent pas de faire un « unicast » à un client n'ayant pas d'adresse IP, même si on connait l'adresse de l'interface matérielle. Dans ce cas, le serveur doit faire un « broadcast » de sa réponse. En transmettant sur le port, on évite que les serveurs DHCP qui écoutent seulement au port doivent décoder des réponses à des requêtes.

II existe deux cheminements pour la configuration d'un client par DHCP, selon que le client connaisse ou ne connaisse pas son adresse IP.

Ces deux cheminements sont illustres par les deux figures des pages 50 et 51.

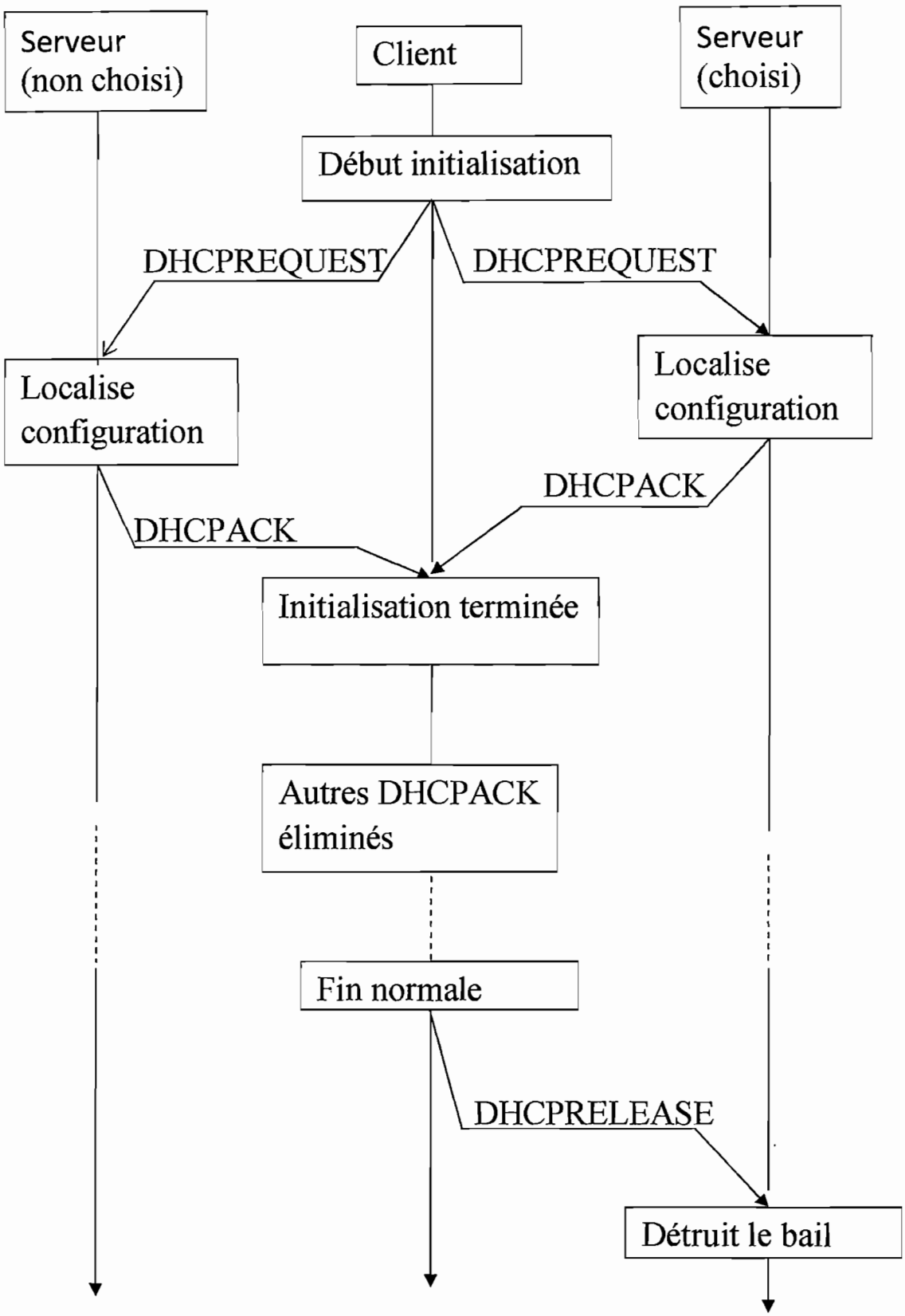

Figure IV.4 : Cheminement de la configuration d'un client DHCP lorsque le client connait son adresse IP.

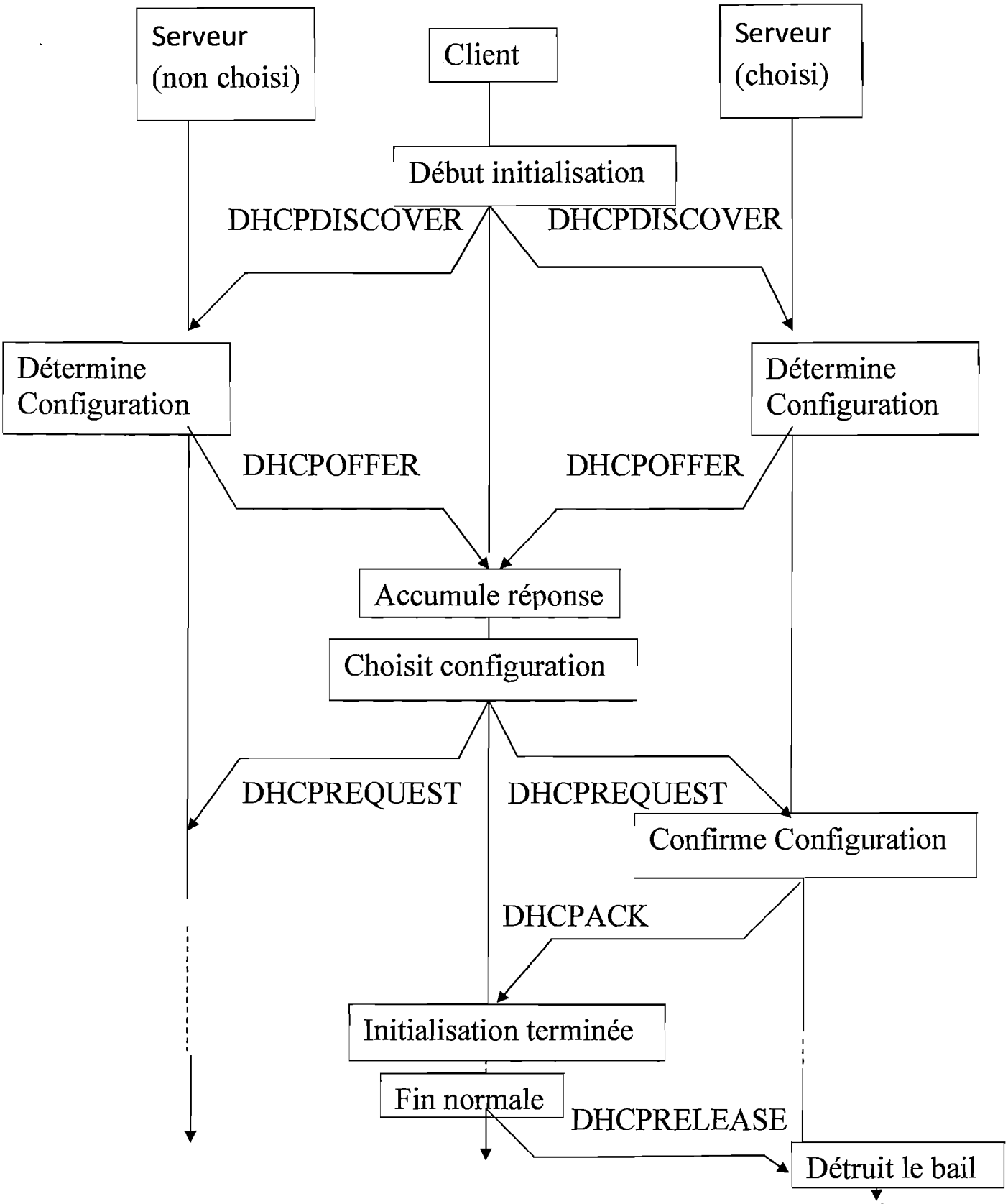

Figure IV.4 : Cheminement de la configuration d'un client DHCP lorsque le client ne connaît pas son adresse IP.

Lors de la négociation entre le client et le serveur la longueur de ce champ dépend de la longueur maximale d'un message DHCP. Cette valeur peut être augmentée avec l'option

IV. 7 Options du protocole DHCP

Ces options sont spécifiques au protocole DHCP. Elles permettent de fournir des informations de négociation entre le client et le serveur.

Requested IP Address : permet au client d'indiquer au serveur l'adresse IP qu'il désire obtenir.

IP Address Lease Time : permet au client d'indiquer le délai d'expiration désiré et au serveur d'indiquer le délai d'expiration offert.

Option Overload : indique si des options se trouvent dans les champs sname et/ou file.

DHCP Message Type : indique le type de requête ou réponse DHCP. DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE et DHCPINFORM.

Les requêtes sont les commandes transmises par le serveur: DHCPOFFER, DHCPACK, DHCPNAK.

Server Identifier : Adresse IP du serveur faisant une offre de configuration, elle sert aussi à identifier le serveur offrant lorsque le client accepte l'offre.

Parameter Request List : indique la liste des options pour lesquelles le client désire obtenir une valeur de configuration.

Message: permet au serveur de transmettre un message d'erreur au client lors d'un refus de configuration.

Maximum DHCP Message Size: permet de modifier la longueur d'un message DHCP.

Client identifier : permet de fournir un identifiant unique du client. Cet identifiant est utilisé par le serveur pour localiser l'information sur ce client dans sa base de données.

TFTP Server Name : permet de fournir le nom du serveur TFTP qui fournira l'image système au client.

Bootfile Name : permet d'identifier le nom du fichier contenant l'image système à télécharger.

IV.8 Client et serveur sur des segments différents

Lorsque le serveur DHCP et le client ne figurent pas sur le même segment Ethernet, les diffusions émises par ce dernier ne parviennent pas au serveur parce que les routeurs ne transmettent pas les diffusions générales. Dans ce cas, on utilise un agent de relais DHCP.
Cet hôte particulier est configure avec une adresse IP statique, et connait l'adresse d'un serveur DHCP auquel il transmet les requêtes DHCP qui lui parviennent sur le port. II diffuse sur son segment les réponses qu'il reçoit du serveur DHCP.

IV.9 Les avantages offerts par DHCP

Les avantages offerts par le DHCP sont :

- Configuration, gestion et optimisation simplifiant l'adressage IP.
- Sécurité accrue limitant les risques de conflits s'adressage sur le réseau.
- Permet à des utilisateurs occasionnels de se connecter a tout moment sans avoir à attendre une adresse IP de l'administrateur.

La charge de l'administrateur devient donc réduite et optimisée mais cette technique est à privilégier pour des structures importantes puisque c'est la multiplicité des postes qui rend difficile la gestion des adresses IP sur le réseau normale.

CHAPITRE V: DESCRIPTION DU CAMPUS KIRIRI, INSTALLATION DU SERVEUR DHCP ET DECOUPAGE D'UN RESEAU IP

V.1. Description du campus KIRIRI

V .1.1. Présentation du campus KIRIRI

Le campus universitaire KIRIRI est situé à l'Est de la ville de BUJUMBURA, en bordure de la chaussée Prince Louis RWAGASORE qui mène à une petite localité (centre spirituel des jésuites).

Celui-ci comporte 2 Instituts et une Faculté :

- l'Institut Technique Supérieur
- l'Institut d'Education Physique et de Sport
- la faculté des Sciences Appliquées

L'Institut Technique Supérieur est fait de 3 Départements à savoir :

- le Département de Génie civil
- le Département de génie Electromécanique.
- le Département d'aménagement et Urbanisme
- le département de l'informatique (computer science).

La faculté des sciences appliquées comporte deux départements :

- le département de Génie Electromécanique ;
- le département de Génie civil.

V.1.2. Equipement du campus universitaire KIRIRI

Le campus universitaire KIRIRI est équipe de deux salles informatiques, lesquelles salles sont utilisées pour les travaux informatiques. Il dispose aussi du matériel informatique pour les décanats de FSA/ITS et IEPS.

V.1.3. Les prévisions suite au nouveau département de l'informatique

Le décanat de la FSA/ITS vient de mettre en place un département de l'informatique au cours de l'année académique 2008-2009, de plus il envisage équiper tous les ateliers, laboratoires et les bureaux des professeurs du matériel informatique.
Grâce à cette mise en place du nouveau département, ledit décanat a mis à la disposition des étudiants qui ont embrassé ce nouveau département une salle informatique.
Toutes les machines des deux salles informatiques, laboratoires, ateliers et bureaux des professeurs auront une connexion sur Internet.

V.2. Installation du serveur DHCP

V.2.1. Introduction

Un serveur DHCP permet de donner dynamiquement une adresse IP à des ordinateurs. II peut être intégré dans un routeur ou dans une configuration serveur. Si on démarre l'installation de SBS 2003 avec deux cartes réseaux intégrés, l'une pour le réseau local, l'autre pour la connexion Internet, il est installé par défaut sur la partie locale pas pour la partie Internet utilisant une connexion sur un routeur.

V.2.2. Installation du serveur DHCP

DHCP n'est pas un composant installé par défaut lors d'une installation normale de Windows Server 2003.
On peut l'installer lors de l'installation de Windows 2003 ou ultérieurement. La procédure est la suivante :

- Cliquer sur Démarrer, Panneau de Configuration puis Ajout/Suppression de programmes ;
- Cliquer ensuite sur Ajouter ou Supprimer des composants Windows ;
- Faire un double clic sur Services de mise en réseau ;
- Cocher la case Protocole DHCP

- Cliquer sur ok, puis sur suivant, puis à la fin de l'installation cliquer sur terminer.

Si on n'a pas attribué l'adresse IP statique, l'assistant de composants Windows demandera alors de spécifier une adresse IP statique sur le serveur.

L'installation du serveur DCHP est à présent terminée.

V.3. Découpage d'un réseau IP

V.3.1. Introduction

Le Découpage d'un réseau IP consiste à utiliser une seule adresse IP pour créer d'autres sous réseaux.

V.3.2. Pourquoi les sous réseaux

- Ils permettent aux réseaux locaux physiquement à distance d'être reliés.
- un mélange des architectures de réseau peut être relié comme Ethernet sur un segment et le Token ring sur des adresses.
- Ils permettent à un nombre illimité de machines de communiquer en combinant des sous réseaux.
  Par contre, le nombre de machines sur chaque segment est illimité par le type de réseau utilisé.
- La congestion de réseau est réduite comme les diffusions et chaque trafic local de réseau est limité au segment local.

V.3.3. Caractéristiques des sous réseaux

- Un réseau IP de classe A, B, C peut être découpé en. sous réseaux
- Chaque sous réseau peut être découpé en sous réseaux et ainsi de suite.
- Chaque sous réseau a un seul identifiant réseau unique et il exige un masque de réseau pour le sous réseau.

Il est nécessaire de bien déterminer les points suivants avant de faire subnetting :

- déterminer le nombre d'identifiant réseau requis pour l'usage courant et également pour l'évolution dans le futur ;
- déterminer le nombre maximum des machines de chaque sous réseau, tenant compte encore de la croissance dans le futur ;
- définir un masque de réseau pour le sous réseau entier ;
- déterminer les identifiants sous réseau qui sont utilisables ;

- déterminer les identifiants machines valides et assigner les adresses IP aux postes de travail.

V.3.4. Echantillon de l'étude

Vu les besoins du dit campus, nous proposons le réseau IP de class C avec 2 sous réseaux : l'un pour la salle des professeurs et l'autre pour la salle des étudiants.
Ce réseau aura un NET ID : 192. 168. 1.0 avec le masque par défaut 255.255.255.0

V.3.5. Procédure de calcul des sous-réseaux

- Déterminer le nombre de bits dans la partie sous-réseau qui permet d'avoir le nombre de sous-réseaux voulus ;
- Déterminer le nombre de bits dans la partie machine qui permet d'avoir le nombre de machines ;
- Déterminer le masque qui va être utilisé pour ces sous-réseaux
- Ecrire sous forme binaire l'adresse IP initial ;
- Ecrire sous forme binaire le masque initial ;
- Ecrire sous forme binaire le nouveau masque ;
- Réduire les adresses de sous-réseaux en incrémentant la partie des sous-réseaux dans l'adresse initiale ;
- Réduire l'adresse du broadcast en remplaçant par des 1 tous les bits de la partie machine de l'adresse IP ;
- Enfin déduire les adresses utilisables.

V.3.6. Calcul des adresses avec le sous adressage

L'opération consiste à découper le réseau IP de classe C 192.168.1.0/24 avec un masque par défaut 255.255.255.0 en deux sous réseau de 62 adresses par chaque sous réseau.

V.3.6.1. Calcul du nombre de sous-réseaux

Avec un réseau IP 192.168.1.0/24 soit
11000000.01101000.00000001.00000000
11000000.01101000.00000001 est la partie réseau
00000000 est la partie machine
La masque de sous réseau par défaut est 255.255.255.0 soit
11111111.11111111.11111111.00000000
Donc, on a 256 adresses possibles, c'est-à-dire de 0 à 254 dont 0 pour la machine locale et 255 pour l'adresse de diffusion. Or dans notre travail, nous avons besoin de 62 machines par sous réseau, $62 < 2^6$ donc 6 bits pour la partie hôte et 2 bits pour la partie sous réseau, soit 11000000. Avec 256 adresses, on a le nombre de sous réseaux de 256 :64 = 4 sous-réseaux.

V.3.6.2. Calcul du masque de sous réseau

Le nouveau masque de sous réseau est 255.255.255.192 avec 2 bits pour HOST ID.

V.3.6.3. Calcul du NetID et des plages des adresses

Le premier sous réseau est : 192.168.1.0, les adresses utilisables sont dans la plage de 1 à 62 ; le deuxième sous réseau est de 192.168.1.64 les adresses utilisables sont dans la plage de 65 à 126 ; le troisième sous réseau est de 192.168.1.128 les adresses utilisables sont dans la plage de 129 à 190 ; le quatrième sous réseau est de 192.168.1.192 les adresses utilisables sont dans la plage de 193 à 254.

Comme il y a un besoin que dans chaque sous-réseau, on distribue 40 adresses et réserver 22, il faut le préciser et le déclarer lors de la configuration.

Mais le travail consistait à avoir deux sous réseaux, dans ce cas, le calcul change.

Chaque sous réseau contient 128 adresses, or 128 est codé sur 7 bits. Les 7 bits sont pour la partie host et le 1 qui reste pour la partie NetID, le nouveau masque de sous réseau devient 255.255.255.128

- Le premier sous réseau devient 192.168.1.0, les adresses utilisables sont dans la plage de 192.168.1.1 à 192.168.1.126
- Le deuxième sous réseau devient 192.168.1.128, les adresses utilisables sont de 192.168.1.129 à 192.168.1.254

Dans chaque sous réseau, il faut déclarer que 40 adresses sont allouées et que 22 sont réservées pour une extension ultérieure pour le premier sous réseau tandis que 32 adresses du second sous réseau sont allouées et 30 réservées aussi pour une extension ultérieure.

V.3.7. Adresse de diffusion

Pour obtenir l'adresse de diffusion dans chaque sous réseau, on met à 1 tous les bits de Host ID.
L'adresse de diffusion du premier sous réseau est 192.168.1.01111111, soit 192.168.1.127, l'adresse de diffusion du deuxième sous réseau est 192.168.1.225.

V.3.8. Choix des équipements d'interconnexion des machines

V.3.8.1. Concentrateur

C'est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes et de régénérer le signal.
Le concentrateur est ainsi une entité possédant un certain nombre de ports, il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32.

Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.
Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports.

Il permet ainsi de connecter plusieurs machines entre elles, parfois disposées en étoile, ce qui lui vaut le non de hub qui signifie moyeu de roue, la traduction Française exacte est répartiteur pour illustrer le fait qu'il s'agit du point de passage des communications des différentes machines.

V.3.8.1.1. Types de concentrateurs

On distingue deux catégories de concentrateurs :

- les concentrateurs dits « actifs » : ils sont alimentés électriquement et permettant de régénérer le signal sur les différents ports ;
- les concentrateurs dits « passifs » : ils ne permettent que de diffuser le signal à tous les hôtes connectés sans amplifications.

V.3.8.2. Répéteur

Sur une ligne de transmissions, le signal subit des distorsions et un affaiblissement d'autant plus important que la distance qui sépare deux éléments actifs est longue.
Généralement, deux nœuds d'un réseau local ne peuvent pas être distants de plus de quelques centaines de mètres ; c'est la raison pour laquelle un équipement supplémentaire est nécessaire au-delà de cette distance.
Un répéteur (repeater en anglais) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau afin d'étendre la distance de câblage d'un réseau.

V.3.8.3. Commutateur

Il travail sur les deux premières couches du modèle OSI, c'est-à-dire qu'il distribue les données à chaque machine destinataire alors que le hub envoie toutes les données à toutes les machines.
Conçu pour travailler sur des réseaux avec un nombre de machines légèrement plus élevé que le hub.

Il élimine les collisions de paquets éventuelles (une collision apparait lorsqu'une machine tente de communiquer avec une seconde alors qu'une autre est déjà en communication avec celle-ci).
Un commutateur est un pont multiports c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI, il analyse les trames arrivant sur les ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats. Donc le commutateur permet d'allier les propriétés du port en matière de filtrage et le concentrateur en matière de connectivité.
Lorsqu'on dispose un nombre élevé de machines à connecter sur un serveur, un hub ou un répéteur ne sont pas suffisants, il est nécessaire de recourir à un routeur ou à un commutateur.
Mais puisque nous disposons un nombre de machines qui n'est pas assez considérable, nous allons utiliser les concentrateurs et les répéteurs comme équipement de liaison comme le montre le schéma suivant :

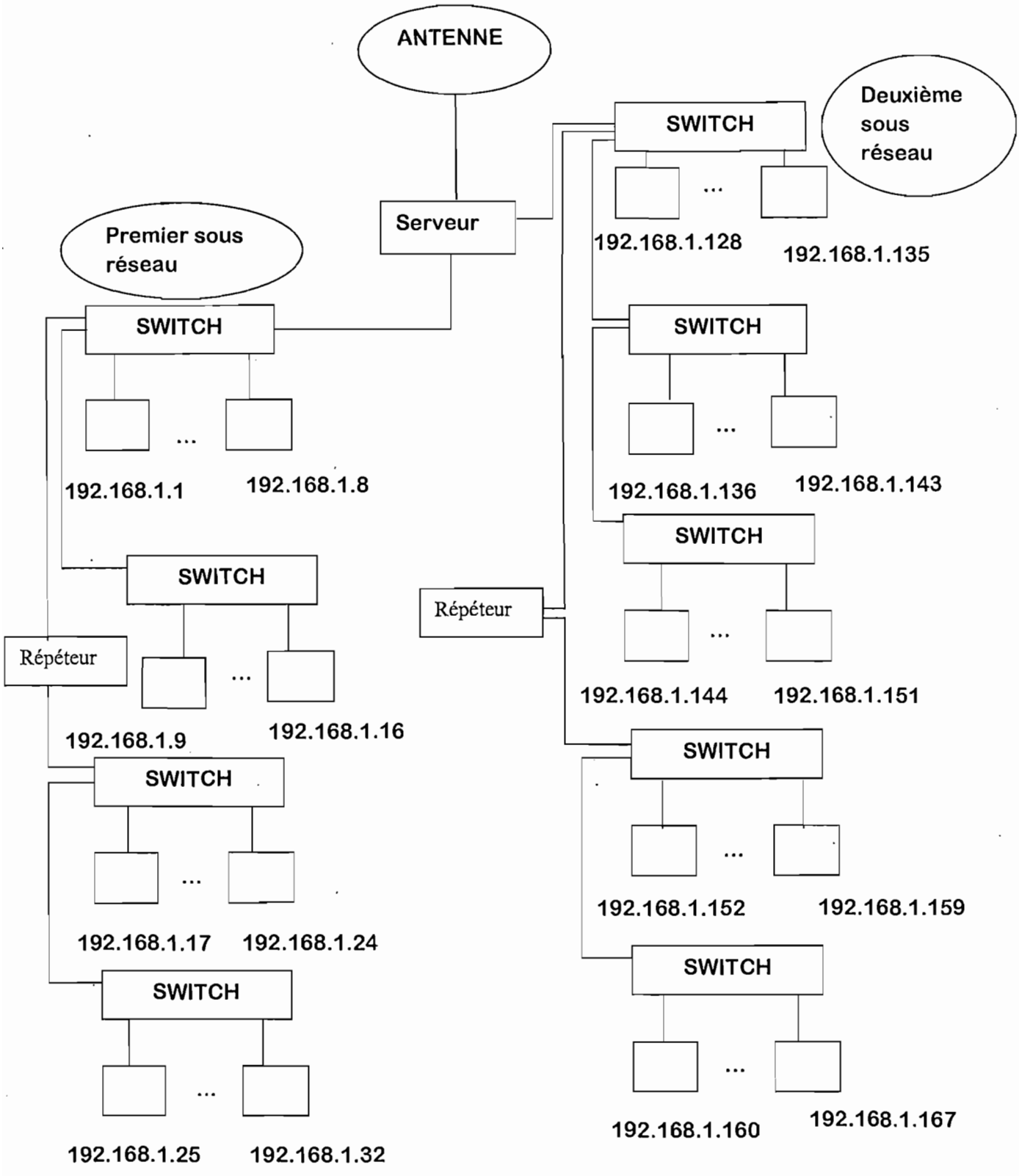

Figure V.1. Représentation schématique de l'installation des machines

CHAPITRE VI : CONFIGURATION DU SERVEUR DHCP

VI.1. Définition d'une étendue

Une étendue est une plage d'adresses IP qui peuvent être allouées aux clients DHCP sur le réseau. Il est recommandé qu'au moins une étendue ne soit pas recoupée avec d'autres étendues sur le réseau.

VI.2. Configuration des machines des deux salles informatiques

Une fois le serveur installé, on doit démarrer et configurer le serveur DHCP en créant une étendue.
Les propriétés d'une étendue sont les suivantes :

- Identificateur de réseau ;
- Masque de sous réseau ;
- Plage d'adresses IP de réseau ;
- Durée du bail ;
- Routeur (passerelle) ;
- Nom de l'étendue ;
- Plage d'exclusions.

VI.3. Création d'une nouvelle étendue

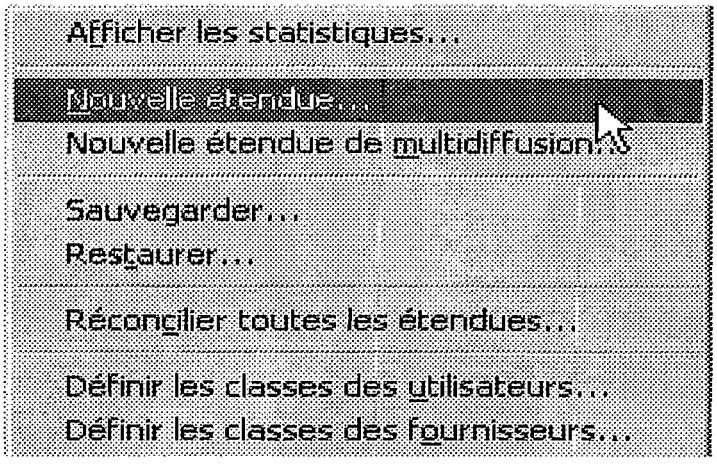

Figure VI.1 : Création d'une nouvelle étendue

Les étapes sont les suivantes :
Cliquer sur ***Démarre***r, Outils d'Administrations puis DHCP
La console DHCP s'ouvre
Cliquer avec le bouton droit sur le serveur DHCP où l'on veut créer une nouvelle étendue, puis cliquer sur ***nouvelle étendue.***

- Dans l'assistant de création d'une nouvelle étendue, cliquer sur ***suivant,***
- Entrer un nom d'étendue dans la zone ***nom***, ce nom doit être explicité. Il est recommandé de fournir une description à l'étendue,
- Cliquer sur ***suivant,***
- Saisir ensuite la plage d'adresses qui sera allouée,
- Ces adresses vont être par la suite attribuées aux clients, elles doivent être valides et ne doivent pas être déjà utilisées,
- Spécifier ensuite le masque de sous réseau choisi,
- Cliquer sur **suivant.**

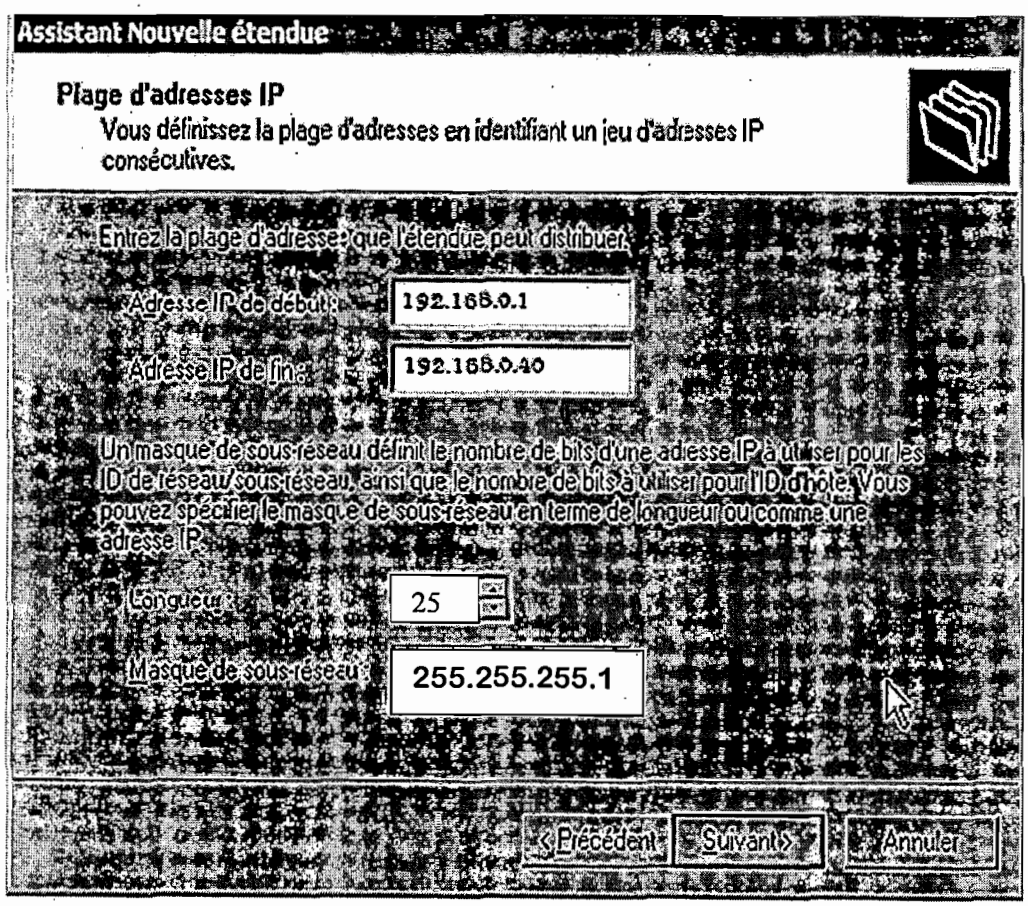

Figure VI.2 : Plage d'adresses IP

On peut ajouter différentes plages d'exclusions si on le souhaite.
Les adresses IP exclus ne seront pas attribuées par le serveur.
Les adresses exclues peuvent être destinées aux imprimantes, à des serveurs.
Cliquer sur ***suivant.***

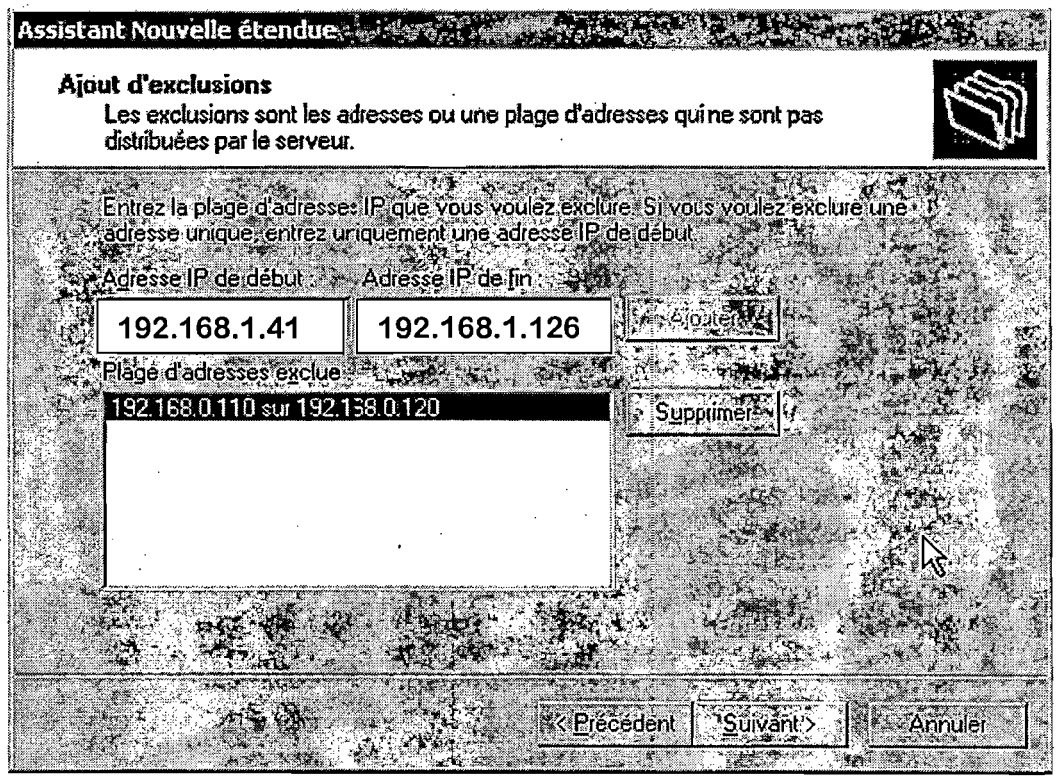

Figure VI.3 : Plage d'adresses exclues

Si on utilise un serveur DNS, on tape le nom du serveur puis on clique sur ***Résoudre***.

Enfin on clique sur **ajouter** pour inclure ce serveur dans la liste des serveurs DNS affectés aux clients DHCP

- On clique sur ***suivant***
- On fait de même si l'on doit inclure des serveurs WINS, en ajoutant son nom et son adresse IP
- On clique sur ***Oui je veux activer cette étendue maintenant*** pour activer l étendue et ainsi délivrer les baux clients de l'étendue
- On clique sur ***suivant*** puis sur ***terminer***.

Le serveur DHCP est à présent configuré

VI.4. Configuration des machines dans les laboratoires, ateliers et bureaux des professeurs

La procédure de la configuration des laboratoires, ateliers et bureaux des professeurs est la même que celle de la salle d'informatique.

Dans l'assistant nouvelle étendue, on définit la plage d'adresse en précisant l'adresse IP de début soit : 192.168.1.128 et l'adresse IP de fin soit : 192.168.1.160, on précise aussi le masque de sous-réseau soit 255.255.255.126

De plus on précise la plage d'adresses qui n'est pas distribué par le serveur soit de 192.168.1.161 à 192.168.1.254, la durée du bail dépend des besoins de l'entreprise ou bien de la société et enfin l'adresse du routeur ou les passerelles qui doivent être distribués par l'étendue.

CHAPITRE VII : EXPLOITATION ET MAINTENANCE

VII.1. Surveillance

Le service DHCP enregistre dans les fichiers journaux un ensemble d'opérations ou événements critiques tels que le démarrage ou l'arrêt du service ainsi que les requêtes d'autorisation.L'audit ainsi créé est stocké dans le répertoire de la base de données DHCP.
Les fichiers d'audits ont la nomenclature suivante : DHCP srvlog.xxx où xxx représente les trois premières lettres du jour de la semaine. L'enregistrement de l'audit DHCP est activé par défaut.Pour activer ou désactiver l'audit DHCP, on effectue un clic droit sur le serveur DHCP, ensuite on clique sur propriétés et cocher ou décocher l'option ***activer l'enregistrement d'audit DHCP***. On peut modifier l'emplacement des fichiers d'audit en cliquant sur ***l'onglet avancé***, dans le champ chemin d'accès du fichier journal d'audit et enfin on clique sur ***parcourir***.

VII.2. Statistiques

Les statistiques sont utiles pour la surveillance des étendues ou du serveur DHCP. Les statistiques informent sur un certain nombre d'informations :

- Heure de démarrage
- Temps d'activité du serveur DHCP ;
- Nombres de requêtes reçues :
  DHCPDISCOVER, DHCPREQUEST, DHCPNACK,
  DHCPDECLINE et DHCPRELEASE. ;
- Nombre de requêtes **DHCPOFFER**, DHCPACK ;
- Nombre total d'adresses IP ;
- Nombre d'adresses et pourcentage d'adresses IP actuellement utilisées ;
- Nombre et pourcentage d'adresses IP disponibles.

Pour afficher les statistiques de serveur, on fait un clic droit sur le nom du serveur, on clique sur ***afficher les statistiques.***

VII.3. Maintenance

Le protocole DHCP de Windows 2003 possède une base de données qui enregistre toutes les informations. On peut modifier le chemin d'accès à la base de données DHCP en cliquant sur l'onglet avancé dans les propriétés du serveur DHCP.

VII.3.1. Sauvegarde de la base de données

La sauvegarde de la base de données est effectuée toutes les soixante minutes. Cependant, on peut sauvegarder la base de données DHCP manuellement, pour cela on clique avec le bouton droit sur le nom du serveur DHCP puis on clique sur ***sauvegarder***, on saisit ensuite le chemin local où sauvegarder la base de données DHCP. Après avoir sauvegardé la base de données DHCP sur l'ordinateur local, il est recommandé de placer cette sauvegarde sur un support mobile dans un endroit sûr.

VII.3.2. Restauration de la base de données

On peut restaurer la base de données DHCP si celle-ci est endommagée. Dans la console DHCP, on fait un clic droit sur le nom du serveur dont on veut restaurer, on spécifie ensuite l'emplacement des fichiers de restauration puis on clique sur ***ok*** et enfin cliquer sur ***oui*** pour redémarrer le service DHCP.

VII.3.3. Compression de la base de données DHCP

Au fur du temps, la base de données DHCP change de taille lors de l'ajout et de la suppression d'enregistrement.
Afin de récupérer l'espace perdu, Windows server 2003 effectue une compression en ligne de la base de données DHCP ; cependant la compression manuelle récupère plus d'espace que la compression dynamique. Pour effectuer une compression manuelle, il faut impérativement stopper le service DHCP.

VII.4. Serveur DHCP multi-hôtes

Un serveur DHCP multi-hôtes est un ordinateur exécutant un système d'exploitation serveur Windows server 2003 qui utilise le service DHCP pour plus d'une connexion réseau.

Pour qu'un ordinateur serveur soit multi-hôte, chaque connexion réseau doit relier cet ordinateur à plus d'un réseau physique : cela nécessite l'utilisation de matériel supplémentaire sous forme d'installation de plusieurs cartes réseau sur l'ordinateur.

Un ordinateur exécutant un système d'exploitation serveur sur Windows server 2003 peut agir en tant que serveur DHCP multi-hôtes. Pour les serveurs multi-hôte le service DHCP est lié à la première adresse IP configurée de manière statique pour chaque connexion réseau utilisée.

Par défaut, les liaisons du service dépendent de la configuration dynamique ou statique de la première connexion réseau pour TCP/IP.

Selon la méthode de configuration utilisée dont les paramètres actuels apparaissent dans les propriétés de protocol Internet TCP/IP, le service de serveur DHCP effectue par défaut les liaisons de service comme suit :

- si la première connexion réseau utilise une adresse IP définie manuellement, la connexion est activée dans les liaisons de serveur. Pour cela, une valeur doit être configurée en adresse IP et l'option d'utilisation de l'adresse suivante doit être activée dans les propriétés de protocole Internet (TCP/IP). Dans ce cas, le serveur DHCP est à l'écoute des clients DHCP et leur fournit ce service.
- si la première connexion réseau utilise une adresse IP configurée en liaison dynamique, la connexion est activé dans les liaisons du serveur, c'est le cas lorsque l'option obtenir une adresse IP automatiquement est désactivée dans les propriétés de protocol Internet (TCP/IP).

Pour les ordinateurs exécutant des systèmes d'exploitation Windows server 2003, il s'agit du paramètre par défaut.

Dans ce mode, le serveur DHCP ne se met à l'écoute des clients DHCP pour leur fournir le service que lorsqu'une adresse IP est configurée.

Le serveur DHCP sera ensuite lié à la première adresse IP statique configurée sur chaque carte réseau.

VII.5. Surveillance et dépannage du serveur DHCP

VII.5.1. Utilisation de l'observateur d'événements de suivi D'activité DHCP

On peut utiliser l'outil ***observation d'événement*** situé dans le dossier ***outil d'administration*** afin de surveiller l'activité de DHCP.

L'observateur d'événement enregistre les événements qui sont enregistrés dans le système journal d'application et journal de sécurité. Le journal système contient les événements qui sont associés avec le système d'exploitation. Le journal d'exploitation stocke les événements qui se rapportent à des applications qui s'exécutent sur l'ordinateur. Les événements qui sont associés à des activités d'audit sont consignés dans le journal de sécurité. Tous les événements qui sont spécifiques à DHCP sont enregistrés dans le journal système.
Le protocole DHCP journal des événements système contient les événements qui sont associés aux activités du service DHCP et un serveur DHCP. Par exemple lorsque le serveur DHCP a démarré et arrêté, lorsque les baux DHCP sont près d'être épuisés et quand la base de données est corrompue.

VII.5.2. Utilisation du moniteur système pour surveiller l'activité DHCP

Le moniteur système d'utilité est le principal outil de suivi de la performance du système. Moniteur système permet de suivre plusieurs processus sur le système Windows en temps réel, l'utilisateur utilise un affichage graphique que l'on peut utiliser pour visualiser les données ou enregistrer des données.
On peut spécifier les éléments spécifiques ou des composants qui doivent être suivis sur ordinateur local et l'ordinateur distant, on peut déterminer l'utilisation des ressources par le suivi des tendances.

Moniteur système peut être affiché dans un graphique histogramme ou format de rapport.

Moniteur système utilise les objets, les compteurs. C'est un outil précieux lorsqu'on a besoin de contrôler et de dépanner le trafic DHCP.

Les compteurs surveillés sont :

- le processus de bail DHCP
- la longueur de la file d'attente DHCP
- DHCP server-side conflit tentatives.

Pour démarrer le moniteur système, on clique sur ***démarrer, outils d'administration*** puis cliquer sur ***performance***, lorsque le rendement console s'ouvre, on ouvre le moniteur système. Le DHCP de performance que l'on peut suivre la voie de circulation DHCP est :

- ***ACK/sec*** : indique le taux DHCPAK à laquelle les messages sont envoyés par le serveur ;
- ***Active queu length*** : indique le nombre de paquets DHCP qui sont dans la file d'attente pour le traitement par le serveur DHCP
- ***Vérifier la file d'attente des conflits longueur*** : indique le nombre de paquets DHCP qui sont dans la file d'attente de détection de conflits ;
- ***Baisses/sec*** : indique la vitesse à laquelle le serveur DHCP reçoit DHCPDECLINE messages ;
- ***Découverte/sec*** : indique la vitesse à laquelle le serveur DHCP reçoit DHCPDISCOVER messages ;
- ***Dropped doublons/sec*** : indique la vitesse à laquelle les paquets dupliqués sont reçue par le serveur DHCP ;
- ***Informations/sec*** : indique la vitesse à laquelle le serveur DHCP reçoit DHCPINFORM messages ;
- ***Millisecondes par paquets*** : indique le temps moyen que prend le serveur DHCP pour envoyer une réponse ;
- ***NACKS/sec*** : indique pour DHCPNACK les messages envoyés par le serveur DHCP ;

- ***Expired paquets /sec*** : indique la vitesse à laquelle a expiré les baux alors que les paquets sont en attente dans file d'attente du serveur DHCP ;
- ***Paquets reçus/sec*** : le taux indique que le serveur DHCP reçoit des paquets ;
- ***Communiqué de presse/sec*** : indique la vitesse à laquelle DHCPRELEASE messages sont reçus par le serveur DHCP ;
- ***Demande/sec*** : indique la vitesse à laquelle DHCPREQUEST messages sont reçus par le serveur DHCP.

VII.5.3. Utilisation du moniteur réseau pour surveiller la Circulation du bail DHCP

Le moniteur réseau est utilisé pour surveiller le trafic réseau et pour résoudre des questions ou des problèmes de réseau. Moniteur réseau fourni avec Windows server 2003 permet de surveiller l'activité réseau et d'utiliser les informations recueillies pou r gérer et optimiser le trafic, identifier les protocoles inutiles, détecter les problèmes avec les applications de réseau et de services. Afin de saisir les cadres, on doit installer le moniteur réseau et l'application pilote du moniteur réseau sur le serveur où on va exécuter le moniteur réseau.

Les deux versions du moniteur réseau sont :

- La version du moniteur réseau fourni avec Windows server 2003 : avec cette version de Network, on peut surveiller l'activité réseau uniquement sur l'ordinateur local et exécuter le moniteur réseau
- Le moniteur réseau version inclue avec Microsoft system management server : avec cette version, on peut surveiller l'activité réseau sur tous les périphériques sur un segment de réseau. On peut capturer des images à partir d'un ordinateur distant, les noms de périphériques pour résoudre des adresses MAC, et de déterminer l'utilisateur et le protocole qui consomme le plus de bande passante.

En raison de ces fonctionnalités, on peut utiliser le moniteur réseau pour surveiller et dépanner le trafic de bail DHCP ; on peut utiliser la version du moniteur réseau inclus dans Windows server DHCP. Avant qu'on puisse utiliser le moniteur réseau pour surveiller le trafic du bail DHCP, on doit d'abord installer le pilote du moniteur réseau.
Le pilote moniteur réseau est installé automatiquement lorsqu'on installe le moniteur réseau.

VII.5.3.1. Installation du moniteur réseau

1. Cliquer sur ***démarrer*** puis cliquer sur ***panneau de configuration***
2. Cliquer sur ***ajouter*** ou **supprimer des programmes** pour ouvrir l'outil ***Ajout/suppression*** de programmes boîte de dialogue
3. Cliquer sur ***Ajout/supprimer des composants Windows***
4. Sélectionner outils de gestion et cliquer sur boutons détails
5. Sur la gestion et de suivi de boîte de dialogue outils, sélectionner le moniteur réseau outils et cliquer sur ***ok***
6. Cliquer sur ***suivant*** lorsqu'on est retourné à l'assistant composant de Windows
7. Cliquer sur ***terminer*** sur l'assistant composant de Windows page.

VII.6. Les fichiers du serveur DHCP

Les fichiers du serveur DHCP sont des fichiers texte délimités, chaque entrée du journal représente une ligne de texte. L'exploitation par le biais de DHCP permet de connecter nombreux événements certains de ces événements sont :

- Serveur DHCP événement,
- Client DHCP événements,
- Crédit bail DHCP,
- Serveur DHCP voyou détection des événements,
- Active Directory autorisation.

Chaque entrée du fichier journal a son champ et chaque à un but

- ID : c'est le serveur DHCP de l'ID d'événement code ;
- Date : la date à laquelle le fichier journal de l'entrée a été connecté sur le serveur DHCP ;
- Temps : le temps ou l'entrée du fichier journal a été enregistré sur le serveur DHCP ;
- Description : il s'agit d'une description de l'événement du serveur DHCP ;
- Adresse IP : il s'agit de l'adresse IP du client DHCP
- Nom d'hôte : il s'agit du nom d'hôte du client DHCP
- Adresse MAC : c'est l'adresse MAC utilisé par le client DHCP à l'adaptateur réseau.
- Les fichiers journaux de serveur DHCP utilise l'ID d'événement réservés codes. Ces codes d'ID d'événements décrivent des informations sur les activités qui sont connectés. Le fichier journal ID d'événements décrit seulement des codes qui sont inférieur à 50. Les serveurs DHCP codes journal ID d'événements sont résumés dans le tableau ci dessous :

Codes Evénements	signification
00	Le journal a été lancé
01	Le journal a été arrêté
02	Le journal a été temporairement interrompu en raison du faible disque
10	Une nouvelle adresse IP a été louée à un client
11	Un bail a été renouvelé par un client
12	Un bail a été libéré par un client
13	Une adresse IP a été détectée pour être en cours d'utilisation sur le réseau
14	Demande de location qui ne peut être satisfaite
15	Un bail a été refusé
16	Un bail a été supprimé
17	Un bail a été dépassé
20	Bootp indique qu'une adresse a été louée à un client
21	Une adresse dynamique bootp a été louée à un client
22	Une requête bootp ne pouvant pas être satisfaite en raison de l'adresse de la piscine de la portée bootp qui est épuisé
23	Bootp indique qu'une adresse IP a été supprimée après avoir confirmé qu'elle n'était pas utilisée
24	Une adresse IP opération de nettoyage a commencé
25	Indique l'adresse IP de nettoyage statique
30	Une demande de mis a jour DNS
31	La mis a jour DNS a échoué
32	Mis à jour DNS succès

Tableau VII .1 : Codes événements

VII.7. Dépannage de la configuration du client DHCP

Le serveur DHCP existe généralement lorsque les événements suivants se produisent :

- le client DHCP ne peut pas contacter le serveur DHCP ;
- le client DHCP perd la connectivité.

Lorsque ces événements se produisent, l'une des premières tâches que l'on doit effectuer est de déterminer si les problèmes de connectivité ont eu lieu en raison de la configuration du client DHCP ou si elle s'est produite en raison d'autres problèmes de réseau.

Pour ce faire, il faut déterminer le type d'adresse de l'adresse IP du client DHCP ; pour déterminer le type d'adresse :

Il faut utiliser la commande ***IPconfig*** pour déterminer si le client a reçu un bail de l'adresse IP du serveur DHCP :

- Le client a reçu une adresse IP du serveur DHCP si la commande ***IP config/all*** sortie affiche :
  - Le serveur DHCP comme étant permis
  - l'adresse IP est affichée comme adresse IP
- On peut également utiliser la boîte de dialogue d'état de la connexion réseau pour déterminer le type d'adresse IP pour le client ;
- Pour afficher les informations, on fait une double clique sur la connexion réseau dans la boîte de dialogue connexion réseau ;
- Cliquer sur l'onglet support ;
- L'adresse IP de type doit être affichée comme étant attribuée par le DHCP.

Après les contrôles ci-dessus, on peut conclure que l'adresse IP a été attribuée au client par le serveur DHCP.

Un autre problème de réseau est à l'origine du serveur DHCP qui connaît des problèmes de connectivité.

Lorsque les clients ont l'adresse IP incorrecte, il a été probablement dû à l'ordinateur qui n'est pas en mesure de contacter le serveur DHCP.

Lorsque cela se produit, l'ordinateur attribue sa propre adresse IP par le biais de l'adressage IP privé automatique.

Les ordinateurs pourraient ne pas être en mesure de contacter le serveur DHCP pour un certain nombre de raisons :

- Un problème peut exister avec le matériel ou logiciel du serveur DHCP ;
- Une liaison de données de protocol pourrait empêcher l'ordinateur de communiquer avec le réseau.
- Le serveur DHCP et le client sont sur les différents réseaux locaux et il n'y a pas d'agent de relais DHCP, un agent de relais DHCP permet à un serveur DHCP de gérer l'adresse IP des demandes clients qui sont situés sur un LAN.
- Quand un client DHCP est attribué une adresse IP qui est utilisée actuellement par un autre client, une adresse de conflit a eu lieu.
- Le processus qui se produit à détecter des doublons d'adresses IP est le suivant :
  - Lorsque l'ordinateur démarre, le système vérifie la présence de tous les doublons d'adresse IP
  - Le protocole TCP/IP stock est désactivé sur l'ordinateur lorsque le système détecte des doublons d'adresses IP
  - Un message d'erreur s'affiche indiquant que l'adresse matérielle de l'autre système est en conflit avec cet ordinateur ;
  - On doit reconfigurer l'ordinateur en conflit avec une adresse IP unique afin que le protocole TCP/IP puisse être activé sur l'ordinateur à nouveau.
- Quand les conflits existent, un message d'avertissement s'affiche :
  - un avertissement est affiché dans la barre de l'état système ;
  - un message d'avertissement est affiché dans le journal système qu'on peut afficher dans l'observateur d'événements.

- Les adresses de conflits se produisent généralement dans les circonstances suivantes :
  - lorsqu'on a la concurrence des serveurs DHCP dans l'environnement, pour résoudre le problème de serveur DHCP concurrents, on doit localiser les serveurs DHCP voyous, enlever les voyous des serveurs DHCP et puis on vérifie qu'il n'y a pas deux serveurs DHCP pouvant attribuer l'adresse IP de location à partir de la même plage d'adresses IP
  - Un champ de redéploiement a eu lieu : on doit récupérer d'une portée de redéploiement à travers la stratégie suivante :
    - augmenter le conflit des tentatives sur le serveur DHCP
    - renouveler le client DHCP bail

- Lorsqu'un client DHCP ne peut pas obtenir une adresse IP du serveur DHCP, les stratégies de dépannage sont les suivantes :
  - Utiliser la commande IP config/renew ou le bouton de récupération de la boîte de dialogue d'état de la connexion pour rafraichir la configuration IP du client
  - Vérifier que le serveur DHCP est activé, configuré et qu'un agent de relais DHCP existe dans 'émission gamme.
  - Si le client ne peut toujours pas obtenir une adresse IP du serveur DHCP, vérifier si la connexion physique du serveur DHCP ou l'agent de relais DHCP fonctionne correctement.
  - Vérifier l'état du serveur et l'agent de relais DHCP
  - Si le problème persiste après que toutes les vérifications ci-dessus aient été effectuées, on a peut être un problème du serveur DHCP.

- Lors du dépannage du serveur DHCP, il faut vérifier que le serveur DHCP soit installé et activé, vérifier que le serveur est correctement configuré, vérifier que le serveur DHCP est autorisé. Lors du dépannage du champ d'application configuré pour le serveur DHCP, vérifier que le champ d'application est activé, vérifier aussi que toutes les adresses IP disponibles baux ont déjà été attribuées aux clients.

- Lorsqu'un client DHCP obtient une adresse IP incorrecte de la portée, les stratégies de dépannage que l'on utilise sont les suivantes :
  - tout d'abord on détermine si la concurrence existe des serveurs DHCP sur le réseau. Pour ce, on utilise le DHCPLOC.exe utilitaire fourni avec les outils de support Windows pour localiser les serveurs DHCP voyous qui font l'allocation des adresses IP aux clients.
  - Si aucun rogue DHCP serveur n'est situé à travers le DHCPLOC.exe utilité, la prochaine étape consiste à vérifier que chaque serveur DHCP attribue l'adresse IP unique
  - si on dispose plusieurs champs d'applications sur le serveur DHCP ; assigne les adresses IP aux clients sur les sous-réseaux à distance, vérifier alors que l'agent de relais qui est utilisé pour permettre la communication avec le serveur DHCP à l'adresse correcte.

VII.8. Dépannage de la configuration du serveur DHCP

Il arrive que les clients DHCP ne puissent pas obtenir les adresses IP du serveur DHCP même s'ils peuvent contacter le serveur DHCP, dans ce cas, Vérifier que le service serveur DHCP s'exécute sur un serveur particulier, Vérifier la configuration TCP/IP sur les paramètres du serveur DHCP.
Si on utilise le service d'annulaire active directory, on vérifie que le serveur DHCP est autorisé ;
Le serveur DHCP peut être configuré avec le champ d'application incorrect, on vérifie alors que le champ d'application est correct sur le serveur DHCP et qu'il est actif.

La vérification de la configuration du serveur DHCP se fait suivant la procédure suivante :

- on vérifie que le service serveur DHCP est configuré avec l'adresse IP correcte. L'ID de réseau à utiliser doit être le même pour le sous-réseau et pour le serveur DHCP qui est prévu pour attribuer les adresses IP aux clients ;
- Vérifier le réseau des liaisons du serveur DHCP, le serveur DHCP doit être lié aux sous-réseaux ;
- Vérifier que le serveur DHCP est autorisé dans ***Active directory*** afin qu'il puisse fournir les adresses IP aux clients DHCP ;
- Vérifier le champ associé à la configuration du serveur DHCP
- Vérifier que le champ d'application est activé ;
- Vérifier que le champ d'application est configuré avec l'adresse IP correcte ;
- Vérifier les adresses IP disponibles qui peuvent être attribuées aux clients DHCP ;
- Vérifier les exclusions qui sont spécifiées dans le pool d'adresses et vérifier qu'elles sont valables et nécessaires ;

- Vérifier les réserves qui sont précises, si on a un client qui ne peut pas obtenir une adresse IP réservée, vérifier si la même adresse est également définie comme une exclusion dans le pool d'adresse ;
- Vérifier que toutes les adresses IP réservées sont situées dans la plage d'adresses du champ d'application, vérifier aussi que les adresses MAC ont été enregistrées avec succès pour toutes les adresses IP qui sont réservées.

Si on a des serveurs DHCP qui contiennent de multiples champs d'application, vérifier que chacun de ces champs d'application est configurée correctement.

VII.9. Dépannage de la base de données DHCP

Le service DHCP utilise un certain nombre de fichiers de base de données qui nécessite le maintien des données ou des informations sur les adresses IP, les baux, les champs superscopes et option DHCP.
Les fichiers base de données DHCP demeurent ouverts pendant que le service est en cours d'exécution sur le serveur, on ne doit pas changer l'un des dossiers de fichiers de base de données DHCP tant que le service DHCP est en cours d'exécution. Quand on a besoin de changer le rôle du serveur DHCP et de déplacer ses fonctions à un autre serveur, il est recommandé de migrer la base de données DHCP sur un nouveau serveur DHCP. Cette stratégie empêche les erreurs qui se traduisent lorsqu'on essaie de recréer manuellement l'information dans la base de données DHCP du serveur de destination.

CONCLUSION GENERALE

Le protocole TCP /IP est rapidement devenu actuellement l'un des protocoles réseau le plus utilisé.

En effet, lorsque les postes de travail sur le réseau augmentent, la gestion des adresses peut prendre beaucoup de temps, Heureusement, on peut utiliser le serveur DHCP, un protocole de Configuration dynamique de l'hôte, qui permet la gestion des adresses IP sur le réseau et diminuer le temps qu'on passe sur les détails de la Configuration.
DHCP est un protocole commun qui permet d'établir une plage d'adresses localisées et gérées centralement pour les postes de travail clients. Après avoir établi une plage, un serveur DHCP assigne dynamiquement les adresses aux postes de travail client comme nécessaires.
La gestion des adresses TCP/IP consiste en un simple suivi des nombres assignés aux postes de travail pour assigner les adresses TCP/IP statiques, on doit visiter chaque poste de travail, on doit en plus de l'adresse, configurer les informations telles que les passerelles et les masques de sous réseau. Si on fait une erreur dans n'importe laquelle de ces entrées, le poste de travail peut être incompatible de communiquer sur le réseau.

Le DHCP résout les problèmes de configuration et d'administration TCP/IP, élimine la configuration manuelle de chaque poste de travail, alloue et réclame les adresses TCP/IP comme nécessaire donnant ainsi une manière plus efficace d'éviter les conflits d'adresses IP. Si on veut déployer le protocole TCP/IP sur le réseau, il faut un moyen de gérer facilement les adresses individuelles pour tous les postes de travail et rendre le poste de travail beaucoup plus facile.
Notre contribution est d'encourager les sociétés, entreprises, organisations, tant publiques que privées à mettre à leur disposition le serveur Dynamic Host Configuration Protocol vu la gestion centralisée des adresses IP qu'il assure dans une infrastructure réseau.

BIBLIOGRAPHIE

- SINDAYIHEBURA J.M., *le DNS et le protocole Enum*, mémoire présenté en mars, 2005, Facultés des Sciences Appliquées
- MANIRAKIZA J.M et NDAYIRAGIJE J.M., *Mise en place de la plate forme de la voix sur le protocole Internet (VOIP) dans une entreprise : « cas de l'ONATEL »* mémoire présenté en 2006, Institut Technique Supérieur
- TCP/IP et les services réseaux

LES SITES ET PAGES INTERNET

- http://www.tel.ucl.ac.be/edu/elec2920/1997/linux/slides.htm
- http://chrstian.caleca.free.fr/dhcp/serveur-dhcp.htm
- www.wanado.fr
- www.cisco.net
- www.acade.net
- www.cisco.com
- http://www.commert camarchce.net/internet/tcpip.php3
- http://www.arin.net
- www.ntfaqfr.com/dhcp.html-5k
- www.hdcp-handbook.com
- www.isc.org
- http://www.rfc-édition.org
- http://www.tout-savoir.net
- http://hauterive-developpez.com
- www.micropp.com
- file:///h:/introduction%20 aux 20 r%3%a9seaux%20informatique…
- file%:/hh:/formation%20micosoft%20windows%20 server20200
- http://www.laboratoire-microsoft.org/articles/network/conf-dhcp-win2/13/1/

- http://h:/moise 1020.htm
- http://www.piw.net/cours/windows/2003/dhcp/
- http://www.commentçamarche.net/contents/lan/concentrateur.php3