MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

Présenté en vue de l'obtention
du Diplôme d'Ingénieur d'Etat en Electronique

Option : Contrôle

Thème:
Optimisation et réalisation d'un réseau local sécurisé au sein de l'IAP de BOUMERDES

Proposé par : Mme F.Kehila
Dirigé par : Mr M.Lahdir

Présenté par :
- **NESNAS Ouerdia**
- **ZIKIOU Nadia**

Année universitaire **2008/2009**

Soutenu le : 01-07-2009

Remerciements :

Nous tenons à remercier en premier lieu, M^{r} LAHDIR notre promoteur pour la qualité de son encadrement.

Nos vifs remerciements vont ensuite à :

- M^{me} TIAR pour son orientation et son entière collaboration
- M^{elle} F.CHARIF et M^{r} A.KHELLAF pour leur précieuse aide et disponibilité au niveau de SONATRACH
- M^{me} F.Mezari et M^{r} Salem pour leurs conseils et assistance
- M^{me} F.KEHILA, l'encadreur de BOUMERDES
- Tous nos enseignants de nos cursus scolaires
- Nos remerciements vont également à tous ceux qui, de prés ou de loin ont aidés à élaborer ce travail

O.NESNAS et N.ZIKIOU

Je dédie ce modeste travail :

- ✓ Aux deux personnes qui m'ont soutenu depuis que j'ai vu le jour. Pour leur patience, leur amour et leur réconfort, à mes parents
- ✓ A mon très cher frère « Abdellah »
- ✓ A mes sœurs adorées : Samia, Souad, Yasmine, Romayssa et mon amie Aldjia
- ✓ A toute ma famille
- ✓ A mon amie Ouerdia ainsi que sa famille
- ✓ A toutes mes amies
- ✓ A tous ceux que j'aime et je respecte.

Je dédie cet humble travail à :

- ✓ A mes chers parents qui ont toujours été là pour moi, que j'espère ne jamais décevoir
- ✓ A la mémoire de ma grand-mère paternelle « Ouerdia »
- ✓ A ma grand-mère maternelle « Wiza » qui j'espère sera présente à toutes mes réussites
- ✓ A ma grande sœur « Salima » qui n'a jamais cessé de m'aider et de m'épauler. A son futur mari « Kader ».
- ✓ Mon adorable petite sœur « Radia » qui a su être là pour moi dans les moments difficiles
- ✓ Au petit cadet « Said », l'être que j'aime le plus au monde
- ✓ A ma binôme « Nadia » qui est plus qu'une simple binôme à mes yeux, ainsi qu'à toute sa famille
- ✓ Mes oncles « M^{d} Arezki », « Hamid » et à mon cousin « Yahia »
- ✓ A toutes mes tantes, à tous mes cousins
- ✓ A mes amies fideles : Fatiha, Fazia, Houria, Hassina, Lilia, Nassima que je ne remercierai jamais assez pour leur présence et leur soutien.
- ✓ A tous ce que j'ai connu.

O.NESNAS

Sommaire

Sommaire

Introduction générale :

Une gestion sécurisée des systèmes d'information pour une entreprise devient de plus en plus nécessaire. Beaucoup d'efforts ont été déployés dans ce sens pour garantir l'amélioration des performances et des services. Un grand pas a été franchi au niveau de l'IAP (SONATRACH de BOUMERDES), le travail qui nous a été confié au sein de cette dernière entre dans ce contexte.

Le réseau informatique de la SONATRACH représente un réseau local de type client/serveur avec une topologie en étoile et une architecture à multi niveau dont l'hiérarchie doit représenter des niveaux de plus en plus sécurisés. Ce réseau doit centraliser un maximum de fonctions et de services sur son serveur en attribuant un répertoire personnel pour chaque utilisateur, rendre des répertoires du serveur accessible par les utilisateurs, faire le partage de ressources matériel et mise en place et configuration de diverses applications. Cependant pour assurer un bon déroulement de toutes ces tâches dans le réseau, il faut garantir sa sécurité, et faire de notre serveur un pare-feu qui assure la sécurité de notre réseau sans pour autant affecter le débit et le coût et assurer une gestion d'information meilleure sur les serveurs d'application.

Ainsi, nous devons proposer une architecture optimale en termes de sécurité, fiabilité et rapidité, en lui injectant des systèmes d'exploitation qui répondent aux exigences tracées. Notre réseau contient trois zones différentes :

- ✓ Réseau externe : représente l'Internet
- ✓ Zone DMZ : contient les serveurs d'applications de notre réseau
- ✓ Réseau interne : doit être protégé contre toute attaque de l'extérieur, nous devons lui assurer une sécurité maximale.

Pour aboutir aux objectifs tracés, notre mémoire sera réparti en cinq chapitres. Le premier sera consacré aux généralités des réseaux informatiques en vu d'approfondir nos connaissances dans ce domaine. Le deuxième à la sécurité réseau qui portera un aperçu sur les attaques et les techniques de protection. Le troisième aux généralités Internet. Le dernier chapitre à l'analyse et la réalisation sur lequel nous développerons l'application, et enfin nous terminons par une conclusion générale.

1-1 Introduction :

La mise en place d'un réseau informatique suggère de nombreuses tâches et procédures à vérifier. Dans ce chapitre nous allons présenter différentes généralités sur lesquelles sont basées la réalisation d'un réseau local et le bon fonctionnement de ses éléments.

1-2 Définition d'un réseau informatique :

Un réseau informatique est la connexion de deux ordinateurs ou plus par des supports de transmission afin de partager des données et des ressources entre eux.

- Si la transmission (l'échange de l'information) se fait par câble, on parle de réseau filaire.
- Si elle se fait par l'intermédiaire des ondes (hertziennes, acoustiques) on parle de réseau sans fils.

1-3 Topologie :

Représente la manière dont les éléments de réseau sont reliés entre eux.
L'arrangement physique de ces éléments est appelé la topologie physique, il en existe plusieurs, parmi lesquels on cite:

- La topologie en bus.
- La topologie en étoile.
- La topologie en anneau.
- La topologie maillée.

Le choix de l'une des quatre topologies s'appuie essentiellement sur :

- Le bilan des équipements informatiques existants.
- La disposition géographique des équipements et des locaux.

- L'analyse des besoins immédiats et futurs.
- Le coût d'investissement.

La façon avec laquelle les données transitent dans les câbles est appelée la topologie logique, on cite :

- Ethernet.
- Token Ring.
- FDD

1-3-1 Topologie en bus :

Figure 1-1 : topologie en bus

C'est la topologie la plus simple d'un réseau. Cette topologie utilise un seul câble, généralement en câble coaxial pour relier les ordinateurs sur une ligne unique. Un terminateur (bouchon) est raccordé sur chaque extrémité de la ligne pour éviter la réflexion du signal.
L'avantage de cette organisation est qu'un ordinateur en panne ne perturbe pas l'ensemble du réseau auquel il appartient. Par contre le signal est perdu quand on dépasse une longueur du câble supérieur à 500m (dépend du câble utilisé) et sa rupture, sur n'importe quel point du réseau provoque l'arrêt du réseau.

1-3-2 Topologie en étoile :

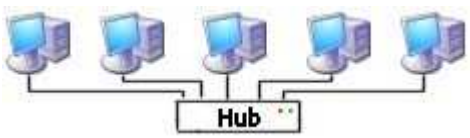

Figure 1-2 : topologie en étoile

Cette topologie consiste à avoir des ordinateurs tous concentrés à un concentrateur qui fait office d'un objet intermédiaire permettant aux postes de communiquer. Lorsqu'un ordinateur a une donnée à émettre celle-ci passe d'abord par le concentrateur qui se charge de l'envoyer vers le destinataire.

Cette topologie est facile à réaliser et à surveiller. La rupture d'un câble n'affecte pas le fonctionnement du réseau, par contre le bon fonctionnement du réseau est étroitement lié au bon fonctionnement du concentrateur. Si le concentrateur tombe en panne, rien ne pourra fonctionner. Cette technologie nécessite un nombre élevé de câble quand le réseau est de grande taille.

1-3-3 Topologie en anneau :

Figure 1-3 : topologie en anneau

Cette topologie est identique à la topologie en bus si on relie les deux extrémités entre elles, formant ainsi une boucle. Les données transitent de l'ordinateur émetteur à un autre jusqu'au destinataire, chaque ordinateur recevant un message de son voisin le réexpédie vers l'ordinateur suivant. Pour que le message ne tourne pas indéfiniment dans la boucle, l'ordinateur émetteur retire le message dés qu'il lui revient. Le droit d'émetteur des informations (car il se peut que plusieurs ordinateurs émettent en même temps) est donné par un répartiteur (appelé MAU : Multi Station Access Unit) qui va gérer la communication en impartissant à chaque ordinateur un temps de parole.

Dans cette topologie, le dysfonctionnement d'un ordinateur de la boucle anéanti le réseau en totalité. Ce problème est particulièrement pallié par la boucle qui fait circuler les données dans un sens opposé.

1-3-4 Topologie maillée

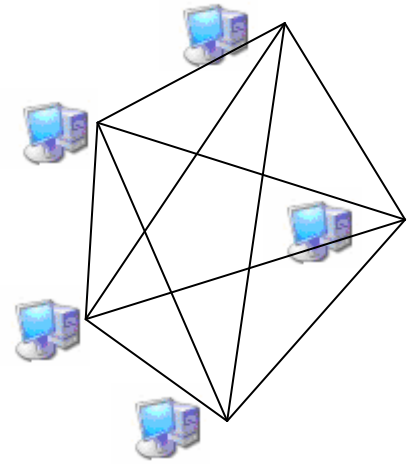

Figure 1-4 : topologie en maille

Dans le maillage régulier, l'intersection est totale ce qui assure une fiabilité optimale du réseau, par contre c'est une solution coûteuse en câblage physique. Si l'on allège le plan de câblage, le maillage devient irrégulier, la fiabilité peut rester élevé mais nécessite un routage de message selon des algorithmes parfois complexes.

Il existe d'autres topologies fréquentes dans les réseaux comme les réseaux en satellite.

1-4 Les composants d'un réseau :

1-4-1 Supports physiques de transmission :

Le support de transmission est un câble qui relie deux ordinateurs ou plus. Il est physique car il est concret et on distingue :

1-4-1-1 Le câble coaxial :

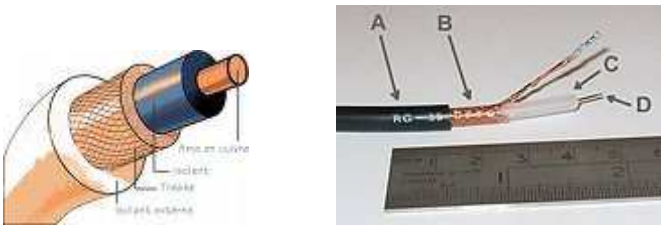

Figure 1-5 : câble coaxial

Proche du câble qui relit le téléviseur à son antenne, est constitué au centre d'un fils de cuivre qui est le conducteur du signal électrique. Le fil de cuivre est entouré d'une couche d'isolant et au pourtour se trouve une couche protectrice qui permet de protéger les données transmises contre les bruits extérieurs constitué d'une tresse métallique en cuivre ou en aluminium. L'ensemble : tresse métallique, isolant et câble conducteur sont entourés d'une gaine isolante en matière plastique. On cite deux types de câble coaxial :

- Câble Ethernet fin : souple, moins cher et transportant le signal jusqu'à 200m
- Câble Ethernet épais : flexible et transportant le signal jusqu'à 500m.

Le câble coaxial présente une bonne immunité aux bruits extérieurs, mais son prix plus élevé rend la paire torsadée plus compétitive.

1-4-1-2 Le câble à paire torsadée :

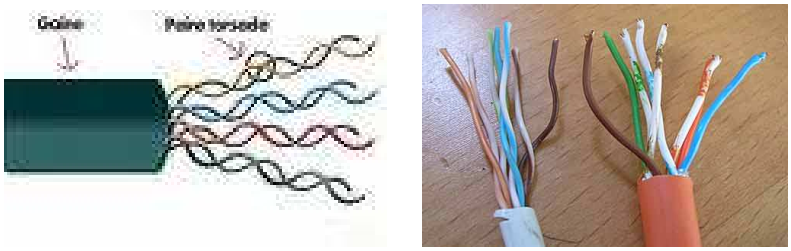

Figure 1-6 : câble à paire torsadée

Il se compose d'une ou plusieurs paires de câble en cuivre fin de 1mm de diamètre entouré d'isolant, et l'ensemble des paires est refermé dans une gaine protectrice.

Se divise en deux types :

- STP (Sheilded Twiseted Pair), la paire torsadée blindée : est plus immunisée contre les bruits car elle contient un blindage à l'intérieur de la gaine.
- UTP (Unshieldes Twiseted Pair), la paire torsadée non blindée : ne contient pas de blindage, elle est moins cher et plus utilisable dans les réseaux locaux.

Il en existe 6 catégories et cat5 est la plus utilisée dans les réseaux actuels. Elle offre une transmission jusqu'à 100Mbs.

1-4-1-3 Le câble en fibre optique :

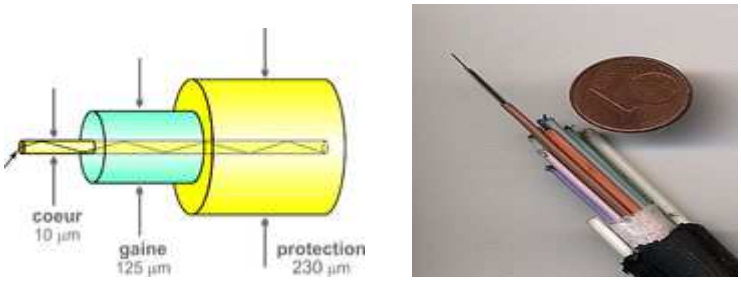

Figure 1-7 : câble en fibre optique

Le câble à fibre optique ressemble au câble coaxial sans tresse métallique. Au centre du câble on trouve un cœur de verre qui est entouré d'une gaine également en verre et à l'extérieur un revêtement en plastique. La transmission se fait en trois parties :

- Emetteur de lumière (source), constitué d'une diode électroluminescente ou d'un laser qui convertit le signal électrique en signal lumineux.

- Le média de transmission (la fibre optique), se comporte comme un tube, guidant la lumière de la source vers la destination.

- Le détecteur (récepteur du signal), constitué d'une photodiode qui génère une impulsion électrique dès qu'une impulsion de lumière la frappe.

La fibre optique est très performante en matière de sécurité et de débit élevé qu'elle peut atteindre sur des longues distances sans affaiblissement du signal. Les inconvénients de la fibre optique sont :

- Sa cherté
- Assez délicate à mettre en place et demande un personnel spécialisé.
- La transmission est unidirectionnelle, il en faut donc deux pour avoir une transmission bidirectionnelle.

1-4-2 Les connecteurs :

Les connecteurs permettent la jonction mécanique entre l'ordinateur (par le biais de la carte réseau) et le câble de transmission. On distingue :

1-4-2-1 Le connecteur RJ45 : (RJ : Rectangular Jack) :

Figure 1-8 : connecteur RJ45

Ce type de connecteur est le plus familier. Il est utilisé dans le câblage à paire torsadée**,** les connecteurs RJ45 servent dans les réseaux Ethernet 10Mbps, 100Mbps et 1000Mbps.

1-4-2-2 Les connecteurs BNC :

Figure 1-9 : connecteur BNC

Le câble coaxial fin et le câble coaxial épais utilisent tous les deux des connecteurs BNC (British Naval Connector), il existe plusieurs types :

- Connecteur BNC en T : sert à connecter la carte réseau de l'ordinateur au câble.
- Connecteur BNC en I : relie deux segments de câble coaxial pour en faire un câble plus long.
- Connecteur de terminaison BNC : ferme chaque extrémité du câble d'un bus.

1-4-2-3 Connecteur pour fibre optique :

Figure 1-10 : connecteur pour fibre optique

Il existe deux types :

- La connectique pour les standards 10BaseF est de type ST.
- La connectique utilisée pour les standards 100BaseFX, 1000BaseSX et 1000BaseLX est de type SC.

1-4-3 Carte réseau :

Figure 1-11 : carte réseau

Pour communiquer en réseau, les ordinateurs doivent être équipés d'une carte réseau, généralement installée sur l'un des connecteurs d'extension (slot) de l'ordinateur. Elle comporte un port où se fiche un câble terminé par un connecteur (un connecteur RJ45 ou BNC) pour connecter l'ordinateur au câblage du réseau. Chaque carte réseau est munie d'un identifiant mondial unique c'est l'adresse MAC.

1-4-4 Les concentrateurs :

Ils peuvent être des hubs (répéteurs) ou des switchs (commutateurs).

1-4-4-1 1es hubs :

Figure 1-12 : hub

Un hub, se présente sous la forme d'une boite allongée, où se trouve plusieurs ports (ou connecteurs), auxquels se connectent les différents câbles du réseau. La face avant du hub donne des informations concernant l'état de chaque port, la densité du trafic dans le réseau et même les collisions. A chaque fois que le hub reçoit une requête sur l'un de ses ports, il la fait renvoyer sur tous les autres ports qui lui sont connectés. Le signal est en général amplifié avant d'être renvoyé sur tous les autres ports.

1-4-4-2 Les switchs :

Figure 1-13 : switch

Contrairement au hub, un switch n'émet pas les trames sur l'ensemble des ports, mais analyse les adresses MAC des trames Ethernet qui le traversent, dirige ces trames uniquement aux ports destinataires. Ainsi, s'il reçoit une trame pour l'ordinateur X, il ne l'envoie qu'à l'ordinateur X, les autres ordinateurs connectés au switch ne verront pas les données qui ne leurs sont pas destinées. Il commute (il branche) l'entrée des données vers la sortie où est l'ordinateur concerné. Un switch améliore donc les performances réseau ainsi que la sécurité des données transmises. Il travaille au niveau 2 du modèle OSI.

1-4-5 Les ponts :

Un pont, se présente sous forme de boîtier muni d'un nombre fini de ports. Il permet d'interconnecter des réseaux de même type (c'est-à-dire des réseaux qui ont la sous-couche MAC compatible, exemple réseau Ethernet, réseau Token Ring). Les ponts fonctionnent selon la couche liaison du modèle OSI, inspectent les données qui leur arrivent et doivent décider s'ils les envoient sur l'autre réseau ou pas. Cette décision se fait en fonction de l'adresse MAC dans le cas des réseaux Ethernet. En d'autres termes, un pont filtre les trames et ne transmet que les trames dont l'adresse correspond à un ordinateur situé sur le réseau raccordé. En plus du filtrage, un pont transforme la trame pour l'adapter au réseau raccordé.

1-4-6 Les routeurs :

Comme pour les ponts, les routeurs permettent d'interconnecter plusieurs réseaux entre eux (pas forcément de même type). Ils sont considérés comme des appareils de la couche 3 du modèle OSI. Le rôle du routeur est d'inspecter chaque paquet envoyé par l'émetteur, et de déterminer la meilleure route (chemin jugé optimal) pour les envoyer à d'autres routeurs. Le paquet passera ainsi d'un routeur à l'autre jusqu'au destinataire.

1-4-7 Les passerelles :

Les passerelles à la différence des ponts et des routeurs, sont souvent des ordinateurs dédiés. Les passerelles doivent assurer toutes les conversions de protocoles pour garantir les échanges entre deux réseaux et ce sont les seules qui travaillent jusqu'à la couche 7 du modèle OSI.

En raison de cette conversion de protocole, chaque réseau croit que l'autre réseau lui est identique, alors qu'ils sont différents. C'est ainsi que les passerelles permettent à des ordinateurs hétérogènes de communiquer.

1-5 Classification des réseaux :

On distingue différents types de réseau selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue.
Les réseaux sont classés en trois grandes structures :

1-5-1 Réseau LAN : Local Area Network ou RLE (Réseau Local d'Entreprise)

Est un réseau privé dont la taille ne dépasse pas quelques kilomètres. Les débits de ces réseaux peuvent aller de quelques mégabits à plusieurs centaines de mégabits par seconde. Le nombre d'utilisateurs (ordinateurs) peut varier dans la plage de 100à 1000.

1-5-2 Réseau MAN : Métropolitan Area Network (réseau métropolitain) :

Consiste à interconnecter les réseaux locaux par des lignes spécialisées afin d'agrandir ou de permettre à ces réseaux de communiquer. Le réseau MAN peut atteindre des surfaces importantes (ville : d'où son nom, ou campus,…) sans pour autant affecter la vitesse de transfert.

1-5-3 Réseau WAN : Wide Area Network (réseau étendu) :

C'est le même principe qu'un réseau MAN sur des distances beaucoup plus importantes, à l'échelle d'un pays ou d'un continent ou même du monde entier (Internet : plus grand réseau WAN).

1-5-4 Réseau VPN : (Réseau Privé Virtuel) :

Il est dit virtuel car il relie deux réseaux locaux par l'intermédiaire d'Internet et privé car seuls les ordinateurs faisant partie du réseau VPN peuvent accéder aux données.
Lorsqu'on ne peut pas se permettre de relier deux réseaux locaux par une ligne spécialisée (en raison de cherté), une solution existe. Celle de relier par support de transmission qui est l'Internet.
Sur Internet, les données sont facilement captées et écoutées, ce qui nuit à la sécurité et la confidentialité de l'entreprise. D'où l'utilité de placer un Proxy (faisant souvent office d'un firewall) sur chacun des réseaux locaux à relier. Ainsi lorsqu'un ordinateur envoie un message d'une partie d'un VPN vers une autre partie, il passe d'abord par un Proxy qui va crypter le message (par des algorithmes de cryptage). Il l'envoie ensuite au Proxy correspondant à l'autre partie. Celui-ci décrypte le message et le remet à son destinataire.

1-5-5 Réseau WIFI : (réseau sans fils) :

C'est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Il est basé sur une liaison utilisant les fréquences radio qui éliminent les câbles, partage une connexion Internet et permet l'échange des ondes radioélectriques. Ces réseaux offrent à l'utilisateur la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus au moins étendu. La communication entre équipements terminaux peut s'effectuer directement ou par le biais de station de base. La communication entre les bornes s'effectue de façon hertzienne ou par câble. Les débits de tels réseaux peuvent atteindre jusqu'à plusieurs mégabits par seconde.

1-6 Transmission de données :

1-6-1 Codage :

Le codage consiste à faire correspondre à chaque caractère du message une suite d'éléments binaires (0ou1). Pour cela, on utilise des codes qui ont été normalisés afin de rendre compatibles des équipements informatiques d'origines diverses.

L'étape de transmission intervenant après le codage, il est nécessaire de transformer les informations binaires en signal électrique. Exemple : on associe à : "0" la valeur "v0", "1" la valeur "v1", ainsi le signal électrique obtenu prend la forme d'une impulsion.
Les principaux codes utilisés sont :

- ***Code ASCII*** : code à 7 bits, utilisé par la plupart des claviers et imprimantes, il constitue l'alphabet d'ordinateur type PC.
- ***Code EBCDIC*** : code à 8 bits, normalisé par IBM pour ses propres équipements informatiques.

1-6-2 Transmission en bande de base :

La transmission en bande de base consiste à transmettre les signaux numériques directement sur le support de transmission. Il existe plusieurs codeurs bande de base :
Manchester, NRZ, Bipolaire, Miller…

1-6-3 Transmission parallèle et transmission série :

La transmission des bits sur un support de transmission peut s'effectuer suivant une transmission parallèle ou une transmission série :

1-6-3-1 Transmission parallèle :

Les bits sont envoyés sur des fils métalliques distincts pour arriver ensemble à destination.

1-6-3-2 Transmission série :

Pour les transmissions sur de longues distances, la transmission série s'impose car la transmission parallèle demande beaucoup de fils (autant de bits que de fils), alors que la transmission série nécessite un seul support de transmission. Les bits sont envoyés l'un derrière l'autre de façon synchrone ou asynchrone.

- Une suite de données est synchrone si le temps qui sépare les instants significatifs est un multiple d'un cycle d'horloge (les bits se suivent d'une façon régulière sans séparation entre les intervalles).

- Une suite de données est asynchrone si l'émetteur produit des caractères d'une façon irrégulière et le temps séparant les caractères est aléatoire. Exemple : les caractères tapés sur un clavier.

1-6-4 Mode d'exploitation d'un support de transmission :

On associe dans cette session : E : émetteur.
R : récepteur.

Si la communication se fait :
De E vers R la transmission est dite simplex.
De E vers R et de R vers E alternativement, la transmission est dite half duplex.
De E vers R et de R vers E simultanément, la transmission est dite full duplex.

1-6-5 Technique de commutation :

Le mécanisme mis en œuvre pour le transport de données s'appelle la commutation. Il existe des techniques utilisées dans les réseaux pour transporter les données d'un utilisateur vers un autre.

1-6-5-1 Commutation de circuits :

Un chemin physique est établi avant même la communication (connexion existante). Une fois la communication en place, elle est conservée tant que les deux entités communiquantes ne la libèrent pas. Exemple : le réseau téléphonique.

Si les deux parties n'ont plus de données à s'échanger pendant un certain temps, la ligne est inutilisée, d'où l'idée de concentrer plusieurs nœuds sur une même liaison.

1-6-5-2 Commutation de message :

Consiste à envoyer un certain nombre d'informations (message) d'un émetteur vers un récepteur en passant par plusieurs nœuds de commutation (commutateurs). Chacun de ces nœuds attend la réception complète du message avant de remettre au nœud suivant. Cela demande des buffers sur chaque équipement et un contrôle de flux pour éviter les engorgements. La facturation se fait par rapport à la distance et la durée.

1-6-5-3 Commutation par paquet :

C'est l'optimisation de la commutation de message qui consiste à découper le message en plusieurs paquets pouvant être acheminés (par une table de routage) plus vite et indépendamment les uns des autres.

Il est à noter qu'en cas d'erreurs, seuls les paquets erronés sont retransmis, par contre en commutation de message, le message est intégralement retransmis. La facturation se fait par rapport au volume d'informations transmises.

1-7 Le modèle OSI :

Développé par ISO (International Standardisation Organisation), ce modèle est OSI (Open System Interconnexion), qui a pour but de créer un modèle idéal où chaque couche effectue une tache définie et dépend des services de la couche inférieure. Il repose sur l'empilement de sept couches pour communiquer entre elles. Les quatre premières couches sont dites basses et les couches 5, 6 et 7 sont dites hautes. Le choix des frontières entre couches doit minimiser le flux d'informations aux interfaces. Ces couches sont les suivantes :

Couche application
Couche présentation
Couche session
Couche transport
Couche réseau
Couche liaison
Couche physique

Figure 1-14 : Couche du modèle OSI

1-7-1 Couche physique :

Détermine comment le support de transmission doit être connecté à l'ordinateur. Elle indique également comment les informations électriques doivent circuler au sein du réseau. Ses fonctions principales sont :

- La spécification de règles mécaniques, électriques, optiques ou autres, fonctionnelles liées aux circuits de données telles que la durée d'un bit, la possibilité de transmission dans les deux sens, le nombre de broches que possède le connecteur…
- L'initialisation de la connexion, son maintien, et le relâchement quand les deux côtés ont fini.

1-7-2 Couche liaison de données :

Subdivise les données en sous groupes pour le transfert au sein du réseau. Ses fonctions principales sont :

- Détection de la correction des erreurs de transmission.
- Etablissement des connexions logiques entre les entités qui désirent s'échanger des données.

- Résolution des problèmes posés par les trames endommagées, perdues et dupliquées.
- Emploi de mécanismes de régulation entre l'émetteur et le récepteur.

1-7-3 Couche réseau :

Elle identifie les ordinateurs connectés au réseau et détermine comment les informations transférées doivent être dirigées. Les protocoles les plus connus sont X25 et IP.

1-7-4 Couche transport :

Corrige les erreurs de transmissions et vérifie que les informations ont été acheminées sans erreurs. Ses fonctions principales sont :

- A l'émission, le découpage des messages longs en morceaux plus petits pour être adaptés aux possibilités du réseau utilisé.
- A la réception, rassemblement de ces différents morceaux pour reconstituer le message sans erreurs et sans duplication.
- Elle gère l'établissement et le relâchement des connexions sur le réseau.

Les protocoles utilisés sont TCP et UDP.

1-7-5 Couche session :

Détermine comment les ordinateurs et les périphériques configurés en réseau doivent communiquer. Elle offre plusieurs services tels que la gestion du dialogue et la synchronisation de ce dernier.

1-7-6 Couche présentation :

Met en forme les informations de telle sorte qu'elles soient lisibles pour les applications logicielles. Elle permet aussi d'effectuer une compression des données pour réduire le nombre de bits transmis.

1-7-7 Couche application :

Elle gère les échanges de données entre les programmes fonctionnant sur l'ordinateur et les autres services du réseau. Ses fonctions principales sont :

- Elle offre des moyens permettant à l'utilisateur d'accéder à l'environnement OSI.
- Elle offre des services et des processus d'application de tout type (Le transfert des fichiers, le courrier électronique, la consultation des annuaires et l'exécution des travaux).

1-8 Le protocole TCP/IP :(Transport Control Protocol/Internet Protocol) :

TCP/IP désigne une architecture réseau qui contient 4 couches, et dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils constituent l'implémentation la plus courante. Il est inspiré du modèle OSI et reprend l'approche modulaire.

Protocole TCP/IP	**Modèle OSI**
Application	**Application**
	Présentation
	Session
Transport TCP	**Transport**
Internet IP	**Réseau**
Accès réseau	**Liaison**
	Physique

Figure 1-15 : couche du modèle TCP/IP

Les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que celles du modèle OSI. Certaines d'entre elles correspondent à plusieurs couches de ce dernier.

1-8-1 L'encapsulation des données :

Dans le modèle TCP/IP, les données de l'application constituent des messages, ceux-ci sont transportés dans des segments qui seront émis sur le réseau sous forme de datagrammes.
L'unité de transport élémentaire est la trame qui consiste au niveau physique un train de bits.

1-8-2 Couches du modèle TCP/IP :

1-8-2-1 La couche application :

Elle prend en charge les protocoles d'adressage et d'administration réseau. Elle comporte des protocoles assurant le transfert de fichiers, le courrier électronique et la connexion à distance. Les principaux protocoles de cette couche sont : FTP, http, SMTP,…

1-8-2-2 La couche transport :

Elle permet de segmenter plusieurs applications de couches supérieures pour les placer dans le même flux de données. Elle assure donc le service de transport et elle fournie deux protocoles :

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

1-8-2-2-a Le protocole TCP :

Il assure le contrôle de flux au moyen de fenêtres glissantes et fournit des numéros de séquences et des accusés de réception. Il représente l'avantage de garantir la transmission des segments et permet d'effectuer une tache importante : multiplexage/ démultiplexage, c'est-à-dire faire transiter sur une même ligne des données provenant d'applications diverses.

Le format des données sous TCP :

<table>
<tr><td colspan="3">Port source</td><td>Port destination</td></tr>
<tr><td colspan="4">Numéro de séquence</td></tr>
<tr><td colspan="4">Numéro d’acquisition</td></tr>
<tr><td>DO</td><td>Réservé</td><td>Code</td><td>Fenêtre</td></tr>
<tr><td colspan="3">Checksum</td><td>Pointeur d’urgence</td></tr>
<tr><td colspan="3">Option</td><td>Bourrage</td></tr>
<tr><td colspan="4">Données à envoyer</td></tr>
</table>

Figure 1-16 : Le format d’un fragment

- Port source : codé sur 16 bits et correspond au port relatif à l’application en cours sur la machine source.

- Port destination : codé sur 16 bits et correspond au port relatif à l’application en cours sur la machine de destination.

- Numéro de séquence : est codé sur 32 bits et correspond au numéro du paquet. Cette valeur permet de situer le paquet arrivé par rapport aux autres.

- Numéro d’acquittement : codé sur 32 bits et définit un acquittement pour les paquets reçus.

- Data Offset : codé sur 4 bits et définit le nombre de mots de 32 bits dans l’entête TCP, il indique alors où les données commencent.

- Réservé : inutilisé actuellement mais prévu pour l’avenir.

- Code :

URG	SYN	ACK	RST	PSH	FIN

URG : pointeur de données urgent utilisé
SYN : pour la synchronisation des numéros de séquences
ACK : numéro de séquence d'acquittement validé
RST : demande de la réinitialisation de la connexion
PSH : indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons.
FIN : fin de transmission.

1-8-2-2-b Le protocole UDP :

Il est non orienté connexion et non fiable car il ne fournit pas d'accusés de réception. Le trafic sur le réseau est plus faible, ce qui accélère le transfert.

1-8-2-3 La couche Inter Réseau :

Elle est la couche la plus importante car elle définit les datagrammes, et gère les notions d'adressage IP.

Le protocole IP :

Un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP, mais n'assure pas la livraison.

version	**Longueur**	**TOS**	**Longueur totale**	
Identification			**Drapeaux**	**Position du fragment**
Durée de vie	**Protocole**		**Checksum de l'en-tête**	
Adresse IP source				
Adresse IP destination				
Option éventuelle			**Bourrage**	
Données à envoyer				

Figure 1-17 : Format d'un datagramme

Version : la version du protocole IP.

Longueur : le nombre des mots de 32 bits sur lesquels est réparti l'en-tête.

TOS : il indique la façon dans laquelle le datagramme doit être traité.

Longueur totale : il indique la taille totale du datagramme en octets.

Identification, fragment et position du fragment : ils permettent la fragmentation des datagrammes.

Durée de vie : indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer.

Protocole : permet de savoir de quel protocole est issu le datagramme.

Somme de contrôle de l'en-tête : permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été alerté pendant la transmission.

Adresse IP source : représente l'adresse IP de la machine émettrice et permet au destinataire de répondre.

Adresse IP destinataire : adresse IP du destinataire de message.

1-8-2-4 La couche accès réseau :

Le datagramme IP issu la couche inter réseau, ne peut être émis directement sur le câble réseau, car il n'offre aucun moyen de reconnaître son début ou sa fin. Pour effectuer la transmission, la couche accès au réseau utilise des trames (comme les trames Ethernet par exemple) afin d'encapsuler le datagramme dans une trame, et permettre ainsi la reconnaissance du début et de la fin.

1-8-2-4-a Adresse IP :

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points.

L'originalité de ce format d'adresse réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau est commune à l'ensemble des hôtes d'un même réseau, appelée aussi ID réseau.

- La partie hôte est unique à l'intérieur d'un même réseau, appelée ID hôte.

Exemple : 192.168.5.12
ID réseau = 192.168.5
ID hôte = 12

1-8-2-4-b Classes d'adresses :

Une classe définit le nombre de réseaux et le nombre d'hôtes autorisés par réseau. Il existe 5 possibilités de classes selon la taille :

Classe A :

0				

Cette classe peut comporter :

- 128 (2 puissance 7) réseaux.
- 16 millions (2 puissance 24) d'hôtes.

Classe B :

10				

Cette classe peut comporter :

- 16384 (2 puissance 14) réseaux.
- 65536 (2 puissance 16) hôtes.

Classe C :

110				

Cette classe peut comporter :

- millions (2 puissance 21).
- 256 (2 puissance 8) hôtes.

Les classes D et E sont réservées à des actions spécifiques.

L'ID réseau w=127 est réservée aux diagnostics. L'adresse 127.0.0.1 appelée boucle locale (loopback), est destinée à tester la machine locale. Un ping 127.0.0.1 sur chaque machine permet de savoir si l'interface réseau fonctionne correctement.

1-8-2-4-c Quelques règles d'affectation d'adresse IP :

- Ne pas utiliser l'ID réseau w=127.
- L'ID réseau et l'ID hôte ne peuvent pas être tous égaux à 1 ou 0.
- Ne pas mettre un ID hôte pour un ID réseau.
- Pour communiquer entre eux, tous les hôtes d'un même réseau doivent avoir le même ID réseau.

1-8-2-4-d Notion de masque :

C'est une adresse qui a le même format que l'adresse IP et qui permet de fixer une partie de l'adresse IP. Il est ainsi possible de maîtriser le nombre d'adresses IP utilisées dans un réseau.

Exemple :

255.255.255.0 Précise que seule la dernière valeur de l'adresse IP peut changer.

255.255.0.0 Précise que seules les deux dernières valeurs de l'adresse IP peuvent changer, on peut avoir plus de combinaisons et donc plus d'hôtes dans le réseau.

1-9 Types de réseaux locaux :

D'un point de vue fonctionnel, les réseaux locaux se divisent en deux catégories :

- Réseaux poste à poste.
- Réseau à serveur dédié (réseaux client/serveur).

Pour comprendre le concept de base des deux architectures, on définit quelques termes :

Client : programme ou ordinateur utilisant une ressource partagée fournie par un autre ordinateur appelé serveur.

Serveur : généralement c'est une machine très puissante en termes de capacité d'entrée/sortie, accomplissant une opération sur la demande d'un client.

Requête : c'est le message qu'envoie le client au serveur, et qui décrit l'opération à exécuter pour le compte du client.

Réponse : c'est le message envoyé par le serveur au client suite à l'exécution d'une opération contenant les valeurs de retours de l'opération.

Middleware : c'est le logiciel qui assure les dialogues entre les clients et les serveurs souvent hétérogènes.

1-9-1 Réseau poste à poste :

Chaque ordinateur est capable de fonctionner comme client, serveur, ou les deux à la fois selon les ressources utilisées.

Tous les ordinateurs sont à pied d'égalité d'où l'appellation anglaise : peer to peer ce qui signifie égal à égal.

Ce type d'architecture convient aux réseaux :

- Où les ressources (fichiers, application,…) ne sont pas volumineuses.
- Où la sécurité n'est pas le souci majeur.

Les ressources importantes ralentissent le travail de l'utilisateur qui les détient quand un autre utilisateur sollicite ces ressources.

Certainement, on peut penser à répartir les ressources d'une façon intelligente sur l'ensemble des machines mais cette solution nécessite parfois un maintien sous tension de tous les ordinateurs ce qui n'est pas intéressant.

Il n'existe aucune politique de sécurité sur l'ensemble du réseau. Chaque utilisateur est responsable de la sécurité de sa machine.

On en conclue que cette architecture est mieux adaptée pour les réseaux de petite taille.

1-9-2 Réseau à serveur dédié :

Un réseau à serveur dédié permet d'hiérarchiser le réseau : les applications et données sont centralisées sur les serveurs. Les serveurs ont pour seul rôle de servir les autres ordinateurs du réseau (les clients).

Un client ayant besoin d'une donnée ou autre consulte uniquement le serveur en émettant une requête vers le serveur grâce à son adresse 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 client et son port.

De nombreuses applications fonctionnent selon ce modèle car il présente des avantages très importants, on cite :

- Pas d'obligation de maintenir tous les postes sous tension, du moment que toutes les données sont centralisées sur les serveurs (qui doivent être allumés bien sur).
- Les périphériques partagés sont accessibles en performance car obligatoirement le serveur est très performant.
- C'est une architecture évolutive, on peut supprimer et ajouter des clients ou même des serveurs sans perturber le bon fonctionnement du réseau.
- Le nombre de points d'accès étant réduit, la sécurité est meilleure.
- Gère les ressources communes, comme une base de donnée centralisé afin d'éviter le problème de redondance et de contradiction.

Un tel type de réseau convient parfaitement aux grandes entreprises exigeant une haute sécurité, et ayant affaire à des données importantes et intensives.

Le réseau à serveur dédié présente plusieurs architectures :

- *Architecture à deux niveaux :*

C'est l'architecture la plus simple. Le client demande une ressource au serveur et le serveur la lui apporte, sans passer par un autre chemin.

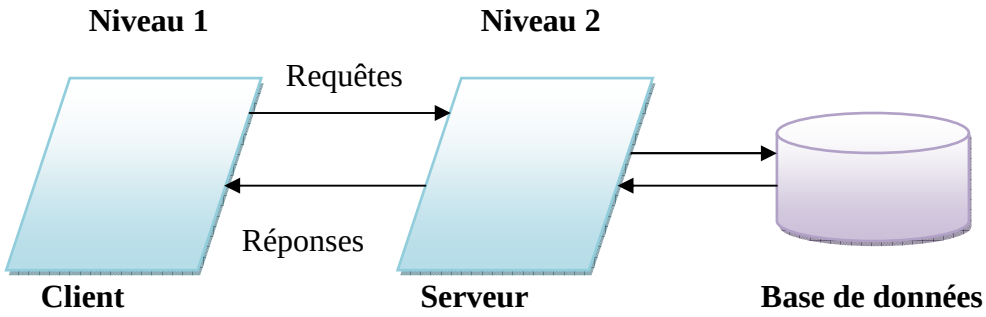

Figure 1-18 : Architecture client/serveur à deux niveaux

➢ *Architecture à trois niveaux :*

Ici, le serveur ne va pas satisfaire le client directement. Il se comporte lui-même comme client, en envoyant la même requête pour un serveur intermédiaire qui va à son tour envoyer sa réponse au premier serveur. Celui-ci la ramène enfin au client.

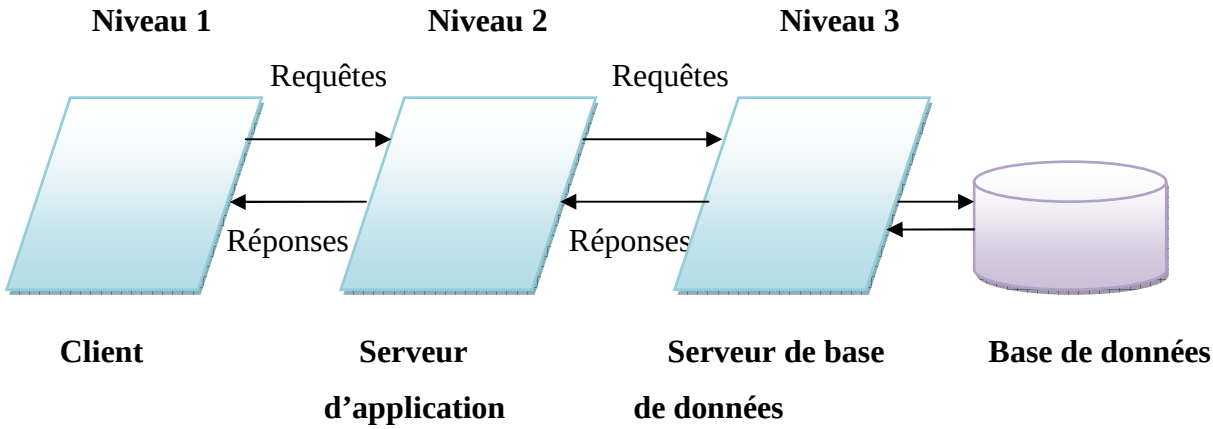

Figure 1-19 : Architecture client/serveur à trois niveaux

Le réseau à serveur dédié présente quand même certains inconvénients :

- Un coût élevé dû à la technicité du serveur.

- Un maillon (serveur), étant donné que tout le réseau est architecturé autours de lui et gère toutes les ressources, sa fiabilité est très importante sinon tout le réseau est anéanti en cas de panne (c'est pour cela que le serveur est une machine très performante et a une grande tolérance pour les pannes grâce par exemple au système RAID).

1-9-3 Comparaison entre les deux types d'architecture :

Dans l'architecture à deux niveaux, le serveur est polyvalent, c'est-à-dire qu'il est capable de fournir directement l'ensemble des ressources demandées par le client. Dans l'architecture à trois niveaux par contre, les applications au niveau serveur sont délocalisées, chaque serveur est spécialisé dans une tâche (serveur web, serveur de base de données,…).

On en conclue que l'architecture à trois niveaux offre :

- Une plus grande souplesse / flexibilité ;
- Une plus grande sécurité (la sécurité est souvent définie pour chaque service) ;
- De meilleures performances (les tâches sont partagées).

1-10 Réseau Ethernet :

La norme IEEE 802.3 a pour origine ALOHA de l'université d'Hawaï. Dans ce système, les données sont transmises de façon sourde, c'est-à-dire sans savoir si le support est prêt ou pas. Le problème majeur posé par cette technique est les collisions, c'est-à-dire quand plusieurs stations émettent en même temps. Pour améliorer la technique ALOHA, la société XEROX a mis au point la méthode d'accès CSMA/CD. On construit donc un réseau CSMA/CD à 2,94 Mbps, fonctionnant sur un câble d'un km de langueur, et permettant de connecter 100 stations de travail. Ce système fut appelé Ethernet.

1-10-1 Méthode d'accès CSMA/CD :

Quand un ordinateur veut émettre une trame, il commence par écouter le support de transmission. S'il n'y a pas de signal donc le canal est libre, alors il envoie sa trame qui sera diffusée mais qui ne sera traitée que par l'ordinateur destinataire (sauf pour une trame de diffusion qui sera traitée par tous les ordinateurs).

Il peut arriver que deux ordinateurs émettent au même moment. Alors les deux signaux se mélangent, c'est " la collision". Tous les ordinateurs peuvent détecter la collision, ceux qui l'ont généré arrêtent la transmission et attendent un temps aléatoire (méthode dite d'accès aléatoire) avant de réémettre leurs données. Ce temps est calculé par un algorithme de telle manière que le temps de réémission soit différent pour chacun des ordinateurs émetteurs qui ont provoqué la collision.

1-10-2 Format Ethernet :

Le bloc de données transporté sur un réseau Ethernet appartient à la famille des trames car il contient un champ capable de déterminer son début et sa fin :

PRE	SFD	DA	SA	LEN	DATA	PAD	FCS

Figure 1-20 : format de la trame Ethernet.

PRE : sur 7 octets, permet aux horloges des récepteurs de se synchroniser avec celle de l'émetteur.

SFD : sur 1 octet, permet de délimiter le début réel de la trame.

DA : sur 6 octets, contient l'adresse MAC de la machine destinataire.

SA : sur 6 octets, contient l'adresse MAC de la machine source.

LEN : sur 2 octets, précise le nombre d'octets contenus dans le champ suivant (DATA).

DATA : de 0 à 1500 octets, contient les données à envoyer sur le réseau issu de la couche supérieure.

PAD : de 0 à 46 octets, si le champ DATA est inférieur à 46 octets, la trame doit être complétée par des bits de remplissage (de bourrage) dans le champ PAD pour atteindre la longueur minimale imposée par le protocole.

FCS : sur 4 octets**,** sert à effectuer la détection des erreurs de transmission.

1-10-3 Adressage Ethernet :

Cause de la diffusion, il fallait mettre une technique pour que chaque ordinateur puisse reconnaître les trames qui lui sont adressées, c'est ce qu'on appelle adressage Ethernet.

C'est la sous couche MAC de la couche liaison qui s'occupe des adressages physiques. Les adresses MAC sont administrées par l'IEEE. A chaque carte réseau, est affectée d'un numéro unique au niveau mondial.

1-10-4 Différents types de réseaux Ethernet :

Ces types sont :

Ethernet 10 Mbps : de la forme 10 Base X

10 : correspond au débit en Mbps

Base : le réseau est en bande de base

X : indique, si c'est un nombre la distance maximale, si c'est une lettre le type du câble utilisé.

.

Il existe 4 types d'Ethernet 10 Mbps :

10 Base 5 :-câble coaxial épais
-topologie en bus
-distance de 500m.

10 Base 2 :-câble coaxial fin
-topologie en bus
-distance de 200m.

10 Base T :-câble à paires torsadées non blindées
-topologie en étoile
-distance de 100m.

10 Base F :-fibre optique
-topologie en étoile
-distance de 2km.

Ethernet 100 Mbps :(Fast Ethernet) : groupe de travail IEEE 802.3u, une évolution de 10 Mbps, ces types :

100 Base TX :-câble torsadé non blindé Cat 5
-topologie en étoile
- Distance de 100m.

100 Base T4 :-câble à paires torsadées non blindées Cat 3 à 5
-topologie en étoile
-distance de 100m.

100 Base FX :-fibre optique
-2km

Gigabits Ethernet :

Dernière version, le groupe de travail IEEE. 3z, ces types :

100 Base CX :-support coaxial

-25m.

100 Base BX :-fibre optique

100 Base T :-câble à paires torsadées Cat 5.

1-10-5 Les systèmes d'exploitation sur un réseau ETHERNET :

De nombreux systèmes d'exploitation réseaux fonctionnent sur un réseau ETHERNET :

- Les systèmes MICROSOFT :
  - WINDOWS 95 et 98
  - WINDOWS NT WORKSTATION
  - WINDOWS NT SERVER
  - LAN MANAGER
  - WINDOWS for WORKGROUP
- Le système NETWARE de NOVELL
- Le système LAN SERVER d'IBM
- Le système APPLESHARE de APPLE COMPUTER
- Les systèmes UNIX, BSD, LINUX

1-10-6 Diamètre de réseau et timeslot Ethernet :

Le diamètre de réseau est la distance qui sépare les deux stations les plus éloignées dans un domaine de broadcast (diffusion générale). Celles-ci peuvent être interconnectées à l'aide de hubs, de répéteurs, de commutateurs ou de ponts. Pour les réseaux Ethernet 802.3 une collision doit pouvoir être détectée dans un intervalle requis pour transmettre la plus petite trame Ethernet autorisée (64 octets).

Le temps pris par une trame pour couvrir le diamètre du réseau est appelé timeslot Ethernet.

1-10-7 Trame unicast, multicast et broadcast :

Une station dispose de trois méthodes pour adresser les trames q'elle souhaite transmettre :

1. ***Adressage broadcast*** : la trame est envoyée à toutes les stations du domaine du broadcast.
2. ***Une adresse broadcast Ethernet*** : est une adresse de destination de 48 bits particulière dont tous les bits sont positionnés à 1, c'est-à-dire dont la valeur hexadécimal de chaque octet est ff.
3. ***Une station*** : qui souhaite transmettre une trame à toutes les autres stations sur son segment, place cette adresse dans le champ d'adresse de destination. L'inconvénient dans ce type d'adressage est que certaines stations doivent traiter des trames qui ne les concernent pas.

1-10-8 Adressage unicast :

La trame est envoyée à une station spécifique. Lorsque le trafic se destine à un nombre limité de stations, voire à une seule, recourir à l'adressage brodcast ou multicast devient inefficace en terme de performances. L'adressage unicast permet à l'émetteur d'envoyer une trame directement à l'adresse Ethernet de la station concernée. Dans ce cas, seule cette dernière reçoit la trame et traite son contenu.

1-11 Réseau Token Ring (IEEE 802.5) :

Créé par IBM et développé par IEEE, sous le nom IEEE 802.5, sa topologie logique est en anneau qui utilise une méthode d'accès par jeton. Ce réseau représente les caractéristiques suivantes :

- Débit de 4 à 16 Mbps

- Transmission en bande de base
- Topologie en anneau
- Méthode d'accès par jeton
- La taille maximale d'une trame est 5000 octets
- Support de type paires torsadées ou fibre optique.

1-11-1 Méthode d'accès par jeton :

Basé sur une petite trame appelé jeton, cette méthode consiste à générer un jeton (par la station superviseur de l'anneau) qui circule dans le réseau. L'ordinateur qui veut envoyer attend jusqu'à l'arrivée de ce jeton qui est marqué "libre", le retire en le marquant "occupé", lui attache le bloc de données à transmettre et le passe à la station suivante jusqu'atteindre sa destination. Celle-ci copie les données qui ont été transmises et marque la trame lue. Quand l'expéditeur reçoit la trame de nouveau, il vérifie si elle était bien reçue puis marque le jeton libre de nouveau et l'envoie sur la ligne.

1-11-2 Le format de la trame Token Ring :

La trame est constituée de la manière suivante :

- Un en-tête :
  - Un délimiteur de début de trame
  - Un contrôle d'accès pour indiquer la propriété de la trame, pour signaler s'il s'agit du jeton ou d'une trame de données
  - Un contrôle de trame
  - L'adresse réceptrice du destinataire
  - L'adresse émettrice de l'expéditeur
- Les données
- La queue :
  - Une séquence de contrôle de trame, le CRC
  - Un délimiteur de fin de trame

- Un état de la trame, pour indiquer si la trame a été reconnue, copiée, ou si l'adresse de destination était indisponible…

1-12 Notion d'intranet :

L'intranet est un réseau interne à une entreprise ou organisation, utilisant des infrastructures privées propres à elle et où tous les utilisateurs sont identifiés. Il ne doit pas nécessairement être relié à Internet. Si c'est le cas, il est primordial de sécuriser le réseau contre les différentes menaces.

Pour contrôler des informations, chaque fonction d'intranet est prise en charge par un serveur qui offre notamment :

- ✓ Un accès au web ;
- ✓ Un accès au courrier électronique ;
- ✓ Un accès à des groupes de discussion et à des services de conversion ;
- ✓ Permet aux utilisateurs dans le réseau de partager des informations et des ressources ;
- ✓ Accès rapide à l'information

1-13 Extranet :

Un Extranet est un réseau reliant des intranets entre eux par l'intermédiaire de l'Internet. Un Extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau de manière sécurisée (authentification par nom d'utilisateur et mot de passe).c'est l'exemple une entreprise qui veut donner à ses clients un accès privilégié à certaines ressources informatiques par l'intermédiaire d'une interface web.

1-14 Conclusion :

Ce chapitre était consacré à l'étude des réseaux informatiques ainsi qu'à leurs principes de fonctionnement pour avoir une bonne compréhension de leurs services. A mesure que nous progressons, nous serons à même de comprendre les divers problèmes qui se posent à leurs

niveaux, tels que la sécurité des accès et des communications, ce qui sera l'objectif de notre prochain chapitre.

2-1 Introduction :

Ce chapitre introduit les principales caractéristiques de la sécurité informatique.

Différents types de sécurité :

Cinq types de sécurité ont été définis :

1- la confidentialité :

La confidentialité est la capacité à garder un secret. Elle a comme rôle la protection des données contre les attaques non autorisées, ce qui assure l'arrivée du message envoyé au destinataire.

2-l'authentification :

L'authentification permet de s'assurer de l'identité des processus communicants, ce qui assure que le message envoyé a été reçu par le bon destinataire.

3-l'intégrité :

L'intégrité assure la non modification des données, c'est-à-dire que les données émises et celles reçues sont identiques.

4-la non répudiation :

La non répudiation permet pour un message donné de bien spécifier l'émetteur et le récepteur, c'est-à-dire que ni l'émetteur ni le récepteur ne peuvent contester respectivement l'émission ou la réception d'un message donné.

5- le contrôle d'accès :

Le contrôle d'accès comme son nom l'indique adjoint à l'accès à des ressources données des conditions d'accès, et permet cet accès à des utilisateurs bien spécifiés.

2-2 Les mécanismes de sécurité :

Plusieurs mécanismes ont été définis pour réaliser les différents types de sécurité cités précédemment. Parmi ces divers mécanismes on cite :

2-2-1 Le chiffrement :

Chiffrer un texte en clair veut dire protéger son contenu en lui affectant des transformations (ou encore des algorithmes de chiffrements) s'appuyant sur l'utilisation d'une ou plusieurs clés de chiffrement. Ceci permet d'obtenir un texte chiffré dont seul celui qui possède les clés de déchiffrement pourra accéder à ce texte, en effectuant des transformations inverses (ou encore des algorithmes de déchiffrement).

La taille des clés de chiffrement dépond de la sensibilité des données à protéger. Plus ces clés sont longues plus le nombre de possibilités de clés est important, par conséquent il sera difficile de deviner la clé qui a été utilisée (cette difficulté réside dans la puissance et le temps nécessaire pour deviner la clé).

Les algorithmes de chiffrement se devisent en deux catégories. Selon qu'ils peuvent être exécutés dans les deux sens, auquel cas on parle d'algorithmes symétriques, ou qu'ils ne puissent être exécutés que dans un seul sens, auquel cas on parle d'algorithmes asymétriques.

2-2-1-1 Chiffrement symétrique :

Dans ce cas de chiffrement, l'émetteur et le récepteur utilisent la même clé secrète qu'ils appliquent à un algorithme donné pour chiffrer ou déchiffrer un texte. Si la transformation utilisée pour chiffrer un texte est la fonction f, celle pour le déchiffrer est la fonction f-1. Ces deux fonctions s'effectuent à l'aide de la même clé, d'où la notion du chiffrement symétrique.

2-2-1-2 Chiffrement asymétrique :

Ces systèmes se caractérisent par la présence d'une entité pour chaque interlocuteur désirant communiquer des données. Chaque interlocuteur possède une bi-clé ou couple de clés calculées l'une en fonction de l'autre.

Une première clé, visible, appelée clé publique (clé verte dans la figure) est utilisée pour chiffrer un texte en clair.

Une deuxième clé, secrète, appelée clé privée (clé rouge dans la figure) est connue seulement par le destinataire, qui l'utilise pour déchiffrer le texte.

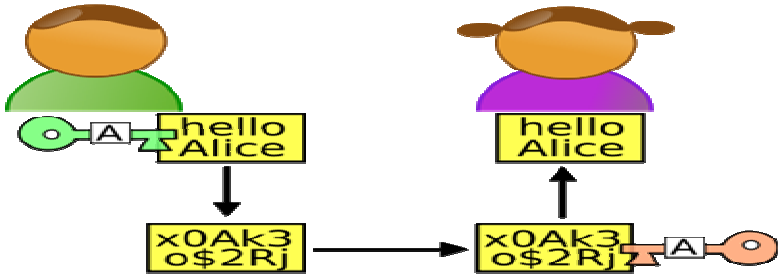

Figure 2-1 : chiffrement asymétrique

Il est clair qu'il faut connaitre la clé publique de ses partenaires pour pouvoir leur envoyer des données. Ces clés publiques sont obtenues auprès d'une autorité de gestion de clés.

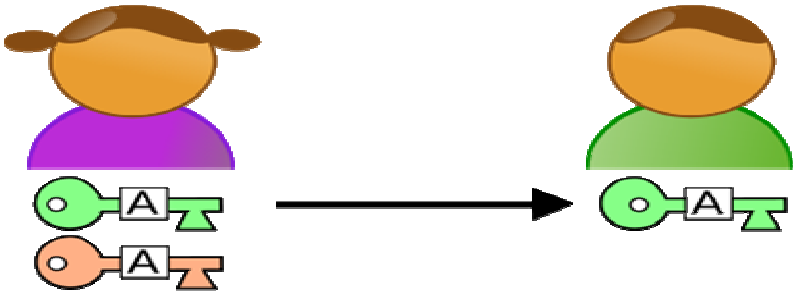

Figure 2-2 : génération de clés publique

2-2-1-3 Principaux algorithmes symétriques :

- l'algorithme DES (Data Encryption Standard) adopté par le NIST (National Institute Of Standard and Technologie) et ses différentes variantes Triple DES, DESX, GDES, RDES.
- Les algorithmes RC2, RC4 et RC5 développés par R.RIVEST et diffusées par la société RSA Security Inc.
- L'algorithme IDEA (International Data Encription Algorithm) développé par des chercheurs de l'Ecole Polytechnique Fédérale de Zurich et de la société Ascom.
- L'algorithme BLOWFISH développé par B.Schneier.

2-2-1-4 Principaux algorithmes asymétriques :

- L'algorithme RSA pour R.Rivest, A.Shamir, L.Adelman.
- L'algorithme Diffie-Hellman.
- L'algorithme El Gamal.

2-2-2 La signature digitale :

C'est un mécanisme permettant à la fois l'authentification de l'émetteur et la non répudiation d'un envoi. Il consiste à signer électroniquement un document, en utilisant un algorithme de chiffrement à clé publique. Cela se fait en trois étapes :

- L'émetteur doit adjoindre le message à envoyer d'une signature qui n'est qu'un petit texte ou message de déclaration d'identité chiffré avec sa clé privée.
- Chiffrer l'ensemble message et signature en utilisant la clé publique du destinataire, puis envoyer le message.
- Le destinataire déchiffrera le message qu'il reçoit avec sa clé privée, puis détachera la signature qu'il déchiffrera avec la clé publique de l'émetteur.

On voit bien que ce mécanisme est performant, mais il possède également des failles, comme par exemple pouvoir constituer une signature digitale à la place du partenaire lui-même après lui avoir volé sa clé privée.

2-2-3 L'enveloppe digitale :

Les systèmes de chiffrement vus précédemment possèdent des inconvénients :

- La lenteur de traitement des messages de taille importante pour les systèmes à chiffrement asymétriques.
- Le problème de distribution et de gestion des clés secrètes pour les systèmes à chiffrement symétriques.

La méthode des l'enveloppe digitale consiste à combiner ces deux systèmes pour éliminer ces deux inconvénients. Le principe est simple :

- La génération par l'un des partenaires de la communication d'une clé valide pendant la durée de communication, qu'on appelle clé de session.
- En appliquant cette clé de session à un algorithme de chiffrement symétrique, on chiffre le message à émettre.
- Chiffrer la clé de session en utilisant la clé publique du destinataire, pour obtenir ce qu'on appelle l'enveloppe 'digitale du message'.

- ❖ Envoyer ensuite le message et son enveloppe au destinataire.
- ❖ Viens ensuite le destinataire qui déchiffrera l'enveloppe avec sa clé privée, lui permettant de déterminer la clé de session qu'il utilisera ensuite pour déchiffrer le message.

2-2-4 La certification :

Ce mécanisme permet d'assurer à la fois l'authentification et la non répudiation. Il s'agit d'une entité,

- ✓ Générant des bi-clés (constituées de clé publique et de clé secrète) pour chaque station du réseau.
- ✓ Permettant la gestion de ces bi-clés.
- ✓ Diffusant les clés publiques aux ressources qui la solliciteraient et qui seraient habituées à l'obtenir.
- ✓ Certifiant ces clés publiques.

L'organisme permettant la gestion des clés publiques s'appelle tiers de confiance. C'est une autorité de certification de clés.

Ce tiers de confiance pourra également enregistrer officiellement toutes les actions et transactions réalisées entre prestataires, pour la véracité des échanges. Ceci assure en quelque sorte la non répudiation.

2-3 La sécurité Internet :

La sécurité dans le réseau Internet consiste à protéger les applications telle que la messagerie, les services d'information tel que le Web et les accès aux ressources informatiques.

Les attaques dans le réseau Internet appartiennent à de nombreuses familles. Ci-dessous sont donnés quelques exemples d'attaque et les parades possibles.

2-3-1 Les attaques par Internet :

Divers types d'attaque existent, ainsi que leur solutions. Ci-dessous sont définis brièvement quatre types d'attaque :

2-3-1-1 Les attaques par dictionnaire :

Ces attaques consistent à découvrir les mots de passe qui sont généralement choisis dans un dictionnaire en utilisant un automate qui va les essayer tous.

Une solution simple à ce type d'attaque consiste à rendre les mots de passe plus complexes en leur ajoutant des caractères spéciaux tel que !, ?, etc.

2-3-1-2 Les attaques ICMP :

Les données envoyées sur le réseau Internet sont sous forme de paquets contenant les données de l'utilisateur ainsi que les adresses source et destination des paquets. À partir de ces adresses les routeurs exécutent leur fonction.

ICMP (Internet Control Message Protocol) utilisé par les routeurs, pour créer des messages véhiculés par le protocole Internet liés au contrôle de l'acheminement des paquets de données IP.

Pour inonder un serveur, il suffit de lui envoyer des messages de type Ping, lui demandant au de renvoyer une réponse. Il existe également d'autres types de message de contrôle ICMP pouvant être utilisés dans le même but. Cette inondation rend le réseau inutilisable et entraîne certains dénis de service.

Une solution consiste à configurer les routeurs de sorte qu'il ne puisse pas générer plus d'un certain nombre de message ICMP durant une période de temps donnée.

On peut également s'appuyer sur la fonction de surveillance des systèmes de gestion de réseaux, en générant une alarme lors de la détection d'un taux de charge anormal (c'est-à-dire un nombre très important de message ICMP).

2-3-1-3 Les attaques par cheval de trois :

Le cheval de trois est un petit programme introduit par le pirate dans la station terminale et permettant de mémoriser l'identification d'un utilisateur ainsi que son mot de passe. Une fois mémorisées, ces informations sont envoyées vers l'extérieur par un message sur une boite aux lettres anonymes, ce petit programme peut se substituer au programme permettant d'effectuer

le login, comme il peut être un programme pirate qui espionne ce qui se passe dans le terminal.

2-3-3-4 Les attaques TCP :

Le protocole TCP utilise des numéros de ports qu'il concatène avec les adresses IP pour construire ce qu'on appelle des sockets qui sont des points d'accès au réseau. A chaque application correspond un numéro de port consistant à l'utilisation, par un pirate, des numéros de ports affectés à l'échange de données, en substituant à l'ordinateur (client) et un serveur, il y aura une piste de cette communication par le pirate, qu'il va ensuite communiquer avec le serveur.

Le pirate pourra également prolonger les réponses vers l'utilisateur pour que ce dernier ne puisse pas se douter de quelque chose.

Une solution consiste de bien configurer le Firewall pour qu'il puisse empêcher le passage de paquets IP ayant des adresses IP internes et arrivant sur des ports de communication externe.

On peut également utiliser les fonctions de chiffrement dans la procédure d'authentification des Firewall pour assurer plus d'efficacité.

2-3-3-5 Les spywares :

Pour éviter l'immense majorité des virus, il a lieu de respecter trois règles clefs :

- Mise à jour régulière à l'aide de Windows Update
- Suppression systématique avant l'ouverture du courrier électronique d'origine inconnu
- Utilisation d'un antivirus fréquemment mise à jour

Mais le respect de ces règles ne prémunit l'utilisateur contre un risque nouveau, les "spywares" !

Un spyware est un logiciel qui s'installe à l'insu de l'utilisateur dans le but de diffuser de la publicité ou obliger à utiliser tel ou tel service payant pour rapporter de l'argent à son créateur.

Comme les virus, ils s'installent souvent à l'insu de l'utilisateur. Toutefois une caractéristique les différencie. Les spywares ne cherchent pas à se reproduire.

De manière générale, on dénombre deux moyens de contamination pour les spywares :

- Internet : de nombreux sites web proposent beaucoup de services. Mais avant d'accéder aux contenus, ils demandent d'accepter l'installation d'un composant ActiveX. Le navigateur en acceptant, non seulement va donner ses clés à l'éditeur du site Web pour y installer ce qu'il veut, mais bien souvent le site Web n'offre même pas ce qu'il a promis.
- Le mode de « diffusion » des spywares est aussi le plus répandu et le plus efficace : plusieurs logiciels gratuits sont accompagnés, le plus souvent de manière invisible, d'un spyware qui s'active à l'installation. À l'utilisation du programme (voir même à tout moment) de la publicité est affichée. Cette publicité permet à la société éditrice du spyware d'engranger des revenus.

L'action la plus couramment entreprise par un spyware consiste à modifier la page de démarrage et la page de recherche du navigateur. Une action un peu plus vicieuse consiste à ajouter une extension au navigateur. Le spyware dispose ainsi de toutes les libertés pour envoyer une fenêtre de publicité même si le navigateur Web n'est pas ouvert. Comme il peut aussi (et en cela il se rapproche du virus), utiliser la connexion Internet de la machine sur laquelle il est installé pour envoyer des courriers électroniques non désirés (spam) à d'autres internautes.

Certains spywares modifient parfois le fichier "hosts" de Windows. C'est un fichier très sensible dans la mesure où il indique aux navigateurs Internet comment convertir une adresse web (http://www.mabanque.com) en adresse IP (192.231.12.18). Imaginant un spyware qui fait croire au navigateur qu'il est sur le site de sa banque alors qu'il navigue en fait sur une copie de celui-ci.

L'utilisation périodique d'un logiciel antispyware est bien entendu recommandée pour s'assurer que la machine n'a pas été récemment infestée par un spyware.

2-4 Zone démilitarisée ou la DMZ :

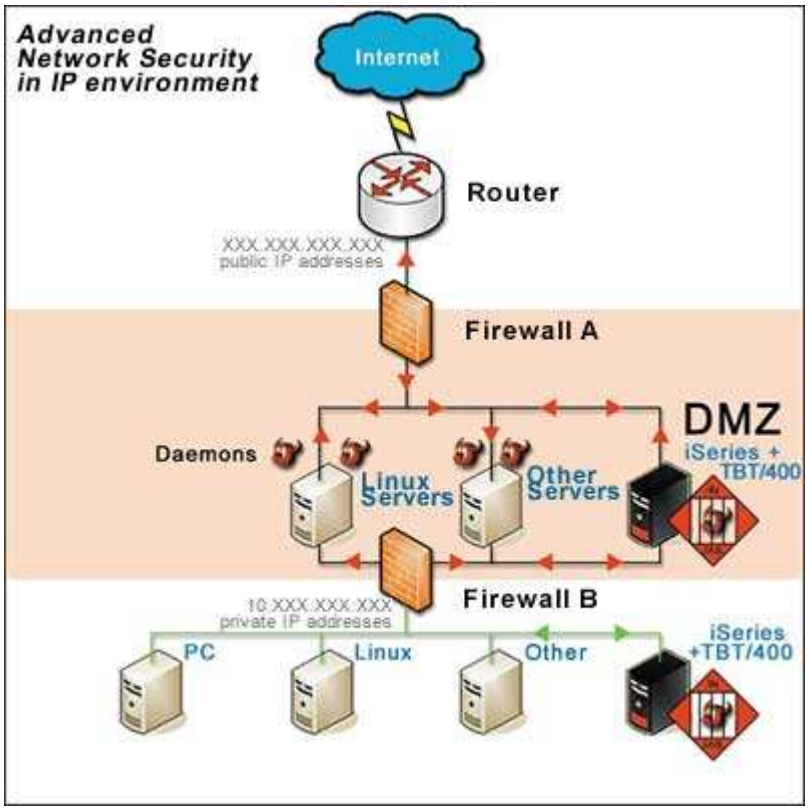

Figure 2-3 : zone DMZ

En informatique, une DMZ est un sous réseau isolé par un pare feu. Ce sous réseau contient des machines se situant entre un réseau interne (LAN, poste client) et un réseau externe (Internet).

La DMZ permet à ses machines d'accéder à Internet et/ou de publier des services sur Internet sous le contrôle du pare-feu externe. En cas de compromission d'une machine de la DMZ, l'accès vers le réseau local est encore contrôlé par le pare-feu interne.

2-5 Proxy :

Un serveur proxy est à l'origine une machine qui fait fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet.

2-5-1 Fonctionnement :

Lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête.

Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

2-5-2 Fonctionnalité d'un serveur proxy :

1. ***La fonction cache*** : c'est la capacité à garder en mémoire (en cache) les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible.

2. ***Le filtrage :*** il est possible d'assurer un suivi de connexions via la construction de journaux d'activité, en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet ; il est ainsi possible de filtrer la connexion à Internet en analysant d'une part les requêtes clientes, d'autre part les réponses des serveurs.

3. ***Le reverse proxy :*** c'est un proxy-cache "monté à l'envers", c'est-à-dire un serveur proxy permettant non pas aux utilisateurs d'accéder au réseau Internet, mais aux utilisateurs d'Internet d'accéder indirectement à certain réseau serveurs internes.

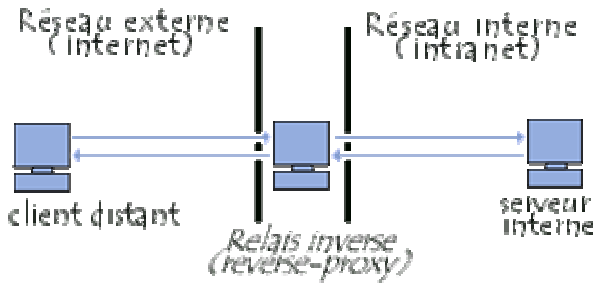

Figure 2-4 : fonctionnement d'un reverse proxy

La fonction de cache du reverse-proxy peut permettre de soulager la charge du serveur pour lequel il est prévu. C'est la raison pour laquelle un tel serveur est parfois « accélérateur ».

2-5-3 Mise en place d'un proxy :

Le proxy le plus répandu est sans nul doute Squid, un logiciel disponible sur de nombreuses plates-formes dont Windows de Linux.

- Sous Windows il existe plusieurs logiciels permettant de réaliser un serveur proxy à moindre coût.
- Wingate est la solution la plus courante (mais non gratuite).
- La configuration d'un proxy avec Java Server devient de plus en plus courante.
- Windows 2000 intègre Microsoft proxy Server (MSP), complété par Microsoft Proxy Client, permettent de réaliser cette opération.

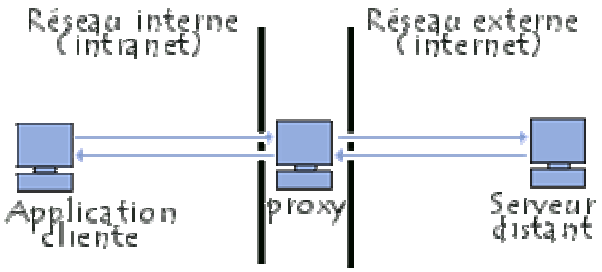

Figure 2-5 : fonctionnement d'un proxy

2-6 Firewall (pare feu) :

Le terme firewall est un terme qui prête parfois à confusion. En effet, il regroupe tous les systèmes de sécurité qui fonctionnent en connexion avec un réseau. Il en existe différents types.

2-6-1 Définition d'un firewall :

Un pare-feu est un système physique (matériel) ou logique (logiciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3,4 et 7 du modèle OSI. Il s'agit donc d'une machine (machine spécifique dans le cas d'un firewall matériel ou d'un ordinateur sécurisé hébergeant une application particulière de pare-feu) qui comporte au minimum deux interfaces réseaux :

- Une interface pour le réseau à protéger (réseau interne)
- Une interface pour le réseau externe

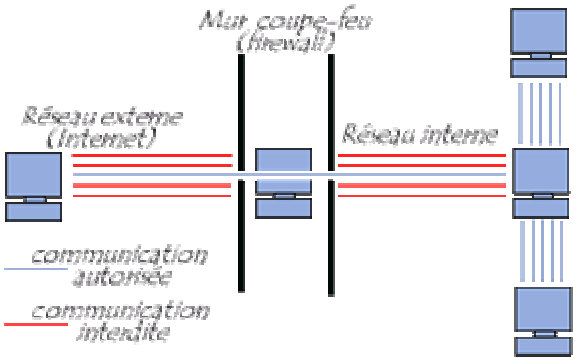

Figure 2-6 : principe de fonctionnement d'un firewall

La politique de sécurité définit l'ensemble des règles de filtrage à implémenter sur le pare-feu. Deux stratégies de configurations de pare-feu existent :

- ✓ Tout ce qui n'est pas explicitement interdit est autorisé
- ✓ Tout ce qui n'est pas explicitement permis est interdit

La première stratégie est dangereuse à utiliser d'un point de vue de la sécurité. En effet, par défaut, tous les services TCP/IP sont autorisés. De la sorte, il suffit qu'à l'installation d'un nouveau service, l'officier de sécurité oublie de modifier la configuration du pare-feu pour que le pare-feu devienne une vraie passoire. C'est pourquoi la seconde stratégie est préférée à la première et est souvent implémentée par défaut.

2-6-2 Filtrage simple de paquets :

Le pare feu fonctionne sur le principe de filtrage simple de paquets. Il analyse les en-têtes des paquets de données échangées entre une machine du réseau interne et une machine du réseau externe. Les paquets échangés possèdent les en-têtes suivants :

- Adresse IP de la machine émettrice ;
- Adresse IP de la machine réceptrice ;
- Type de paquet (TCP,UDP,etc) ;
- Numéro de port (rappel : un port est un numéro associé à un service ou une application réseau) ;

On en distingue deux types de filtrage simple : filtrage de paquets sans état (ne gardent aucun contexte en mémoire), filtrage de paquets avec état (gardent un contexte en mémoire)

Les adresses IP contenues dans des paquets permettent d'identifier la machine émettrice et la machine cible. Tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue). Le port 23 est par exemple souvent bloqué par défaut par le dispositif pare-feu car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance. Les administrateurs lui préfèrent généralement le protocole SSH, réputé sur et fournissant les mêmes fonctionnalités que Telnet.

2-6-3 Filtrage dynamique :

De nombreux services initient une connexion sur un port statique mais ouvrent dynamiquement un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. De cette manière, à partir du moment où la machine située de l'autre côté du pare-feu ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Mais le filtrage dynamique ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

2-6-4 Filtrage applicatif :

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simples (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application. Un firewall qui effectue le filtrage applicatif est appelé Proxy (passerelle applicative).

Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse finie des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

2-6-5 Installation d'un Firewall :

Le smoothwall est en effet un firewall (pare-feu) distribué sous licence GNU/GPL, avec son code source. Il est basé sur un noyau Linux 2.19. Le smoothwall, une fois installé, n'a vraiment besoin que d'un PC, sans clavier, sans souris, sans écran. Le smoothwall supporte les cartes réseau les plus courantes (3COM, real tek, NE 2000) et les modes de connexion Internet les plus courantes (Modem, ISDN, USBADSL, ADSL Ethernet). Sur le firewall on peut créer trois zones réseau différentes à l'aide de trois cartes réseaux (RED, ORANGE, GREEN).

La configuration requise pour le smoothwall est vraiment minimale :

- Processeur 468DX4.
- 16Mo de RAM.
- Disque dur de 200Mo (smoothwall n'occupe qu'environ 60Mo).
- Carte réseau 100Mb.

Ceci est le minimum pour faire fonctionner une connexion par Modem. Pour une configuration multiutilisateur (partage de connexion) et l'ADSL, il faudra étoffer un peu de cette configuration.

2-7 Conclusion :

Dans ce chapitre, on a fait un rappel des différents types d'attaques ainsi que les techniques de sécurité utilisées sur les réseaux informatiques tels que la cryptographie. Ceci consiste une base d'information à laquelle on référera tout au long du développement de notre application.

Introduction :

Des réseaux hétérogènes (de type différents) se sont développés aux quatre coins du globe, des chercheurs décidèrent donc de relier ces réseaux entre eux (entre universités, centres de recherche, les services de renseignements…).

Les protocoles ont évolués pour permettre la communication de tous ces réseaux formant petit à petit une gigantesque toile d'araignée (Web)**,** qui contient tous les réseaux et qu'on appelle désormais « Internet ».

Internet est un ensemble de réseaux à l'échelle mondiale, dont chacun est une interconnexion d'ordinateurs se communiquant en utilisant le protocole TCP/IP.

3-2 Se connecter à Internet :

La carte réseau est l'élément de l'ordinateur qui permet de se connecter à un réseau par des lignes spécialement prévues pour faire transiter des informations numériques. Le modem permet de se connecter à un réseau par l'intermédiaire d'une ligne téléphonique.

Une carte réseau possède une adresse IP qui la caractérise. Nous pouvons toute fois avoir accès à un réseau Internet en contactant un ordinateur relié d'un côté à une ou plusieurs lignes téléphoniques (pour recevoir l'appel) et de l'autre côté à un réseau par l'intermédiaire d'une carte réseau. Cet ordinateur appartient généralement au fournisseur d'accès à Internet (FAI). Lorsqu'il nous connecte par son intermédiaire, il nous prête une adresse IP que nous garderons le temps de la connexion. A chaque connexion de notre part, il nous attribuera arbitrairement une des adresses IP libres qu'il possède. Celle-ci n'est donc pas une adresse IP fixe.

3-3 Service d'Internet :

Le réseau Internet offre une large gamme de services, les services Internet les plus utilisés sont :

- Les courriers électroniques permettant d'envoyer ou de recevoir sur un poste de travail des messages textuels ;
- Le file transfer protocol ou le FTP qui est conçu pacifiquement pour transférer des fichiers d'un ordinateur à un autre.

- Les forums de discussions usenet (new groups) qui sont les forums publics où chacun peut exprimer différents opinions sur différents thèmes.
- La téléphonie qui permet une communication directe entre utilisateurs en ayant à leur disposition une carte de son, un microphone et un haut parleur.
- I R Chat ou Internet Reley Chat, grâce auquel les utilisateurs peuvent s'envoyer des messages en temps réel.
- Worlrd Wide Web ou WWW, ajoute en plus des différents services cités ci-dessus, des liens vers d'autres ressources et des facilités multimédias telles que la vidéo, le son,…etc.

3-4 Domaine Name System (DNS) :

3-4-1 Définition :

Il permet aux utilisateurs de travailler avec des noms de la forme http://yahoo.fr au lieu des adresses numériques du genre 192.153.200.20. Ainsi TCP/IP permet aux utilisateurs de travailler avec des noms de stations explicites appelés adresses FQDN (Fully Qualified Domain) ou domaine totalement qualifié.

Une adresse FQDN est composée d'un nom d'hôte, d'un point et d'un nom de domaine, ce dernier ayant lui-même deux composantes, la première correspond au nom de l'organisation et la seconde à la classification du domaine.

Exemple : www.avg.fr (Hôte.organisation.domaine)

On appelle résolution de nom du domaine (ou résolution d'adresse), la corrélation entre les adresses IP et le nom de domaine associé.

Signification de quelques domaines d'Internet :

Nom de domaine	Signification
Com	Entreprise commerciale
Edu	Etablissement d'enseignement
Gou	Etablissement gouvernementaux
Mil	Groupe militaire
net	Site réseau d'importance majeure

3-4-2 Serveur DNS :

Il permet d'établir la correspondance entre le nom du domaine et l'adresse IP sur les machines d'un réseau, chaque domaine possède son serveur de nom de domaine, lui-même relié à un serveur de nom de domaine de plus haut niveau. Ainsi on peut dire que ce système de nom se présente sous la forme d'une architecture distribuée car on a pas d'organisme unique qui se charge de l'ensemble des noms des domaines, c'est-à-dire qu'il n'existe pas d'organisme ayant à charge l'ensemble des noms de domaine. Par contre, il existe un organisme « Inter NIC » pour les noms de domaine en « .com », « .net », « .org », et « .edu ».

Le système de nom de domaine est transparent pour l'utilisateur, néanmoins il ne faut pas oublier les points suivants :

- Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelé Domain Name Server (lorsqu'on installe le kit de connexion d'un fournisseur d'accès Internet, celui-ci va automatiquement modifier nos paramètres pour prendre en compte cette transformation) ;
- L'adresse IP d'un second Domain Name Server peut également être introduite : il peut relayer le premier en cas de panne ;
- Le nom d'un serveur de nom ne peut certainement pas être donné.

3-5 URL : (uniform ressource locator)

Un URL est un format de nommage universel pour désigner une ressource sur Internet, il s'agit d'une chaine de caractères ASCII imprimable qui se décompose en 4 champs :

- Le nom du protocole : c'est-à-dire le langage utilisé pour communiquer sur Internet. Le protocole le plus largement utilisé est le protocole http (Hyper Text Tranfer Protocol), le protocole permettant d'échanger des pages web aux formats html. De nombreux autres protocoles sont utilisables (FTP, New, Mailto, Gopher,..etc.
- Le nom du serveur : il s'agit d'un nom de domaine de l'ordinateur hébergeant la ressource demandée. Notons qu'il est toute fois possible d'utiliser l'adresse IP de celui-ci, mais l'url devient tout de suite beaucoup moins lisible.

- Le numéro de port : il s'agit d'un numéro associé à un service permettant au serveur de savoir quel type de ressource est demandé. Le port associé par défaut au protocole est le port 80, ce qui signifie que si le service web est associé au port 80, ce numéro de port étant facultatif.
- Le chemin d'accès à la ressource : ce chemin donne l'emplacement exacte de la ressource demandée, c'est-à-dire le répertoire et le nom de fichier demandé.

Un url a donc la structure suivante :

Protocole	Nom du serveur	Port (facultatif)	Chemin
http://	www.monsiteweb.com	:80	/sommaire/sommaire.html

Les protocoles peuvent être utilisés par l'intermédiaire d'une url sont les suivants :

- http
- ftp
- telnet
- mailto
- wais
- gopher

Le nom de ficher dans l'URL peut être suivie d'un point d'interrogation, puis de données au format ASCII, il s'agit de données supplémentaires envoyées en paramètre d'une application sur le serveur (un script CJI par exemple).

3-6 Les ports :

De nombreux programmes TCP/IP peuvent être exécutés simultanément par Internet (on peut ouvrir plusieurs navigateurs simultanément ou bien naviguer sur html tout en téléchargeant un fichier par FTP). Chacun de ces programmes travaillent avec un protocole, toute fois l'ordinateur doit pouvoir distinguer les différentes sources de données. Ainsi, pour faciliter ce processus chacune de ces applications se voit attribuer une adresse unique sur la machine, codé sur 16 bits (port). La combinaison adresse IP+port est alors une adresse unique

au monde, elle est appelée socket. Lorsque l'ordinateur reçoit une requête sur un port, les données sont envoyées vers l'application correspondante.

3-6-1 La fonction de multiplexage :

Le processus qui fait transiter sur une connexion les informations provenant de diverses applications s'appelle le multiplexage. De même le fait d'arriver à mettre en parallèle (répartir sur les diverses applications) le flux de données s'appelle le démultiplexage, ces opérations sont réalisées grâce aux ports.

3-6-2 Assignation par défaut :

Il existe plusieurs ports (ceux-ci sont codés sur 16 bits, il y'a 65536 possibilités), c'est pourquoi une assignation standard a été mise au point afin d'aider à la configuration du réseau.

Quelques assignations par défaut :

port	Service ou application
21	FTP
23	Telnet
25	SMTP
53	DNS
80	http
110	POP3
119	NNTP

Les ports 0 à 1023 sont des ports reconnus, un administrateur réseau peut toute fois lier des services aux ports de son choix, Les ports 1024 à 49151 sont appelés ports enregistrés (Registred Ports), les ports 49152 à 64535 sont les ports dynamiques ou privés.

Les ports d'un serveur sont généralement compris entre 0 et 1023, du côté du client, le port est choisit aléatoirement parmi ceux disponible par le système d'exploitation.

Ainsi, les ports du client ne seront jamais compris entre 0 et 1023 car cet intervalle de valeur représente les ports connus.

3-7 Les protocoles Internet :

Un protocole est une méthode qui permet la communication entre deux machines, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe beaucoup, selon ce que l'on attend de la communication. Certains protocoles sont spécialisés dans l'échange de fichier (FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP),Etc.

Sur Internet, les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles reliés entre eux. Cette suite de protocoles s'appelle TCP/IP.

Elle contient les protocoles suivants :

- http
- ARP
- IP
- UDP
- NNTP
- FTP
- ICMP
- TCP
- SMTP
- TELNET

3-7-1 Protocole http :

Le protocole http est le protocole le plus utilisé sur Internet depuis 1990. La version 0.9 était uniquement destinée à transférer des données sur Internet. La version 1.0 du protocole permet de transférer des messages avec des en-têtes décrivant le contenu du message en utilisant un codage de type MIME. Le but du protocole http est de permettre un transfert de fichiers (essentiellement en format html) localisé grâce à une chaine de caractères appelée URL entre un navigateur (le client) et un serveur web (appelé httpd).

3-7-2 Communication entre navigateur et serveur :

La communication entre le navigateur et le serveur se fait en deux temps :

- Le navigateur effectue une requête http
- Le serveur traite la requête puis envoie une réponse http.

En réalité la communication s'effectue en plus de temps si on considère le traitement de la requête par le serveur. Etant donné que l'on s'intéresse uniquement au protocole http.

3-8 Langages d'implémentation :

3-8-1 HTML :

Le HTML n'est pas un langage de programmation, c'est un simple fichier texte contenant des balises permettant de mettre en forme le texte, les images ou autre contenus dans des pages web. Le HTML « Hyper Text Markup Language » est un système qui formalise l'écriture d'un document avec des balises de formatage indiquant la façon dont doit être présenté le document et les liens qu'il établit avec les autres documents. Il permet, entre autre, la lecture de documents sur Internet à partir de machines différents grâce au protocole http.

En effet le web est une énorme archive de textes formatés, d'images, de sons, de vidéo,…etc. Ces documents sont organisés autour d'une page d'accueil qui guide le visiteur vers d'autres pages HTML grâce à des liens « hypertexte ». Une balise est une commande encadrée par le caractère inferieur (<) et le caractère supérieur (>). Par exemple <H1> est une balise.

3-8-1-1 Page HTML :

Une page HTML est un simple fichier texte commençant par <HTML> et finissant par </HTML>. Il contient un en-tête décrivant le titre de la page, puis un corps dans lequel on place le contenu de la page. L'en-tête est délimité par les balises <HEAD> et </HEAD> le corps est délimité par les balises <BODY> et </BODY>. Ainsi le code source d'une page html sera :

```
<HTML>
    <HEAD>
        <TITLE>Le titre </TITLE>
    </HEAD>
    <BODY>
        Contenu de la page
    < /BODY>
</HTML>
```

3-8-1-2 Les marqueurs :

Les marqueurs peuvent être uniques par exemple
 qui signifie un retour à la ligne ou par paire pour agir sur le texte qu'ils encadrent (le marqueur de fin est alors précédé d'un /) :

<marqueur>notre texte formaté</marqueur>

ce texte est en gras

3-8-1-3 Liens hypertextes :

Les liens hypertextes (appelés aussi ancrage) sont des endroits de la page (généralement en bleus et soulignés) qui amène dans un autre endroit lorsqu'on clique dessus, c'est ce qui permet de lier les pages WEB entre elles. Ils permettent de naviguer :

- ✓ Vers un autre endroit du document
- ✓ Vers un autre fichier HTML situé sur le même disque
- ✓ Vers une autre machine

L'attribut principal des liens hypertextes est HREF, il s'écrit sous la forme :

..

3-8-1-3-A Liens externes :

il crée un lien vers une page dont on spécifie l'URL par exemple :

commentaire ?

3-8-1-3-B Liens internes :

On peut créer un lien vers une page située sur le même ordinateur en remplaçant l'URL par le fichier cible, ce lien peut être fait d'une façon relative ; si le fichier cible est "fich.html" situé dans le répertoire parent, son lien s'écrira : …

Ce lien peut aussi être fait de façon absolue, en écrivant l'adresse du fichier cible de façon locale :

<a href=file:///c:/rep/fich.html…

3-8-1-4 Les signets :

On peut créer un signet dans une page c'est-à-dire marquer un endroit précis d'une page pour s'y rendre par hypertexte. Cela se fait grâce à l'attribut NAME ou ID, à titre d'exemple

« … ; » sera appelé grâce au lien suivant :…, on peut ainsi se déplacer à un endroit précis sur une autre page :

….

3-8-1-5 Les images en html :

Les images peuvent être sur le même ordinateur que la page ou bien ailleurs sur un autre site. Il y'a grossièrement deux formats d'images que nous pouvons inclure dans une page WEW :

- Les images JPEG (JPG) : les images ayant un grand nombre de couleurs seront bien compressées
- Les images JIF : leur taille est faible dans le cas d'images avec peu de couleurs. Ce format permet en outre d'avoir des images entrelacées (qui s'affichent progressivement) et des images dont on définit une couleur comme transparente

On utilise le marqueur <IMG> pour inclure une image. Ses trois principaux attributs sont ;

- **SRC :** indique l'emplacement de l'image (il est obligatoire)
- **ALIGN :** spécifie l'alignement de l'image par rapport au texte adjacent et peut prendre les valeurs TOP, MIDDLE et BOTTOM (au dessus, au milieu et en dessous)
- **ALT :** permet d'afficher un texte lorsque l'image ne s'affiche pas.

Ainsi pour insérer une image, il faudra saisir un marqueur du genre :

<IMG SRC="url/image.gif ou url/image.jpg" ALT="texte remplaçant l'image">

3-8-2 PHP :

Personal Home Page (PHP) est conçu initialement pour quelques fonctions permettant la mise en place d'un site internet, d'un livre d'or ou d'un compteur. Cet outil a évolué pour devenir un véritable langage de script. Php fonctionne sur de nombreuses plates formes Microsoft et Linux et facilite l'accès à un grand nombre de données. Pour développer le php, il suffit de créer une page html dont on change l'extension en (.php) et dans laquelle on pourra insérer des scripts pour réaliser les tâches désirées, telles que l'accès aux bases de données via le web. Quatre technologies sont utilisées pour insérer des scripts dans les pages php :

< ?php …… ?> ;< ?.....le script…….. ?> ;

<script language=PHP>……le script…….</script>

Ou

< ?echo(…….le script……) ;%>

3-9 Outil d'implémentation Dreamweaver 8 :

Dreamweaver 8 est un éditeur visuel professionnel pour la création et la gestion de pages web. Dreamweaver permet de créer aisément des pages compatibles avec une sérié de plates formes et de navigateurs. Dreamweaver permet également d'utiliser certaines fonctions du format html dynamique, tels que les claques et le comportement animés. Le système de ciblage de navigateur vérifie le travail pour détecter d'éventuels problèmes de comptabilité

avec les plates-formes et les navigateurs les plus répandus. Avec Dreamwever, on peut créer des applications Web dynamiques reposant sur des bases de données à l'aide de langage serveur tel que PHP.

3-10 Le world wide web :

3-10-1 Définition :

Le web est un ensemble global de documents et de fichiers interconnectés qui résident sur les serveurs web dans le monde.

Les documents web, appelés également pages web sont composées de textes, d'images, de sons et de clips vidéo. Ils offrent aussi des liens hypertexte sur lesquels on peut cliquer pour pouvoir accès à d'autres pages web.

Son cadre d'exécution et son langage sont ceux du modèle client/serveur. Le client dialogue avec le serveur selon le protocole http et le serveur fournit la réponse structurée en code html. Le serveur web est en permanence à l'écoute des requêtes formulées par le client web.

3-10-2 Navigateur web :

Les navigateurs web sont des logiciels permettant d'accéder et de visualiser des documents présents sur le web en interprétant le langage html dans lequel ils sont écrits. Les navigateurs les plus connus sont Netscape Communicator, Internet explorer, Mozilla Firefox.

3-10-3 Serveur web :

Un serveur web est un programme spécifique situé sur l'une des machines de l'Internet qui attend qu'une interface de navigation se connecte et lui présente une requête. Une fois reçue, le serveur localise le fichier et procède à son envoi.

Parmi les serveurs les plus utilisés, on site le serveur Apache, NCSA et le serveur IIS.

3-10-4 Site web :

Un site web est un ensemble d'un ou plusieurs fichiers prenant place sur un serveur connecté par Internet. Il débute par une page d'accueil contenant des liens hypertexte qui donne accès aux différents sous pages.

3-10-5 Page web :

Une page web est un ensemble de mots disposés linéairement et d'objets graphiques, sons, vidéo,..etc. qui sont regroupés en un document qui sera affiché en un seul bloc. Elle contient également des liens hypertexte.

On distingue des pages web statiques invariantes proposées à l'avance et des pages dynamiques créées à une réponse d'une requête d'utilisateur.

3-11 Conclusion :

A travers ce chapitre, nous avons résumé certaines définitions concernant le réseau Internet et son fonctionnement. Ainsi nous pourrons compléter nos informations préparées pour résoudre la problématique de l'application.

4-1 Introduction :

La mise en œuvre d'un réseau local en interconnectant des ordinateurs et assurer leur communication ouvre des perspectives diverses. En effet, le système informatique du service d'exploration de la SONATRACH est composé de plusieurs machines partageant des ressources communes. Dans ce chapitre, nous allons détailler différents traitements pour aboutir à l'amélioration de la gestion de l'information.

4-2 Cahier des charges :

Dans cette partie, nous allons décrire les étapes d'implémentation d'un réseau local ayant les caractéristiques suivantes :

- une architecture en étoile.
- type Ethernet.
- le protocole utilisé est le TCP/IP.
- à serveur dédié.
- système d'exploitation : on utilise :

Pour serveur : un serveur comme contrôleur de domaine et un autre pour serveur d'applications

Pour client : 4 PC utilisateurs.

- Un firewall

Problématique :

Le réseau informatique de la SONATRACH représente un réseau local de type client/serveur avec une topologie en étoile, et une architecture à multi niveau dont l'hiérarchie doit représenter des niveaux de plus en plus sécurisés. Ce réseau doit centraliser un maximum de fonctions et de services sur son serveur en attribuant un répertoire personnel pour chaque utilisateur, rendre des répertoires du serveur accessible par les utilisateurs, faire le partage de ressources matérielles et permettre la mise en place et configuration de diverses applications. Cependant pour assurer un bon déroulement de toutes ces tâches dans le réseau, il faut garantir sa sécurité. Le schéma de base du travail demandé est le suivant :

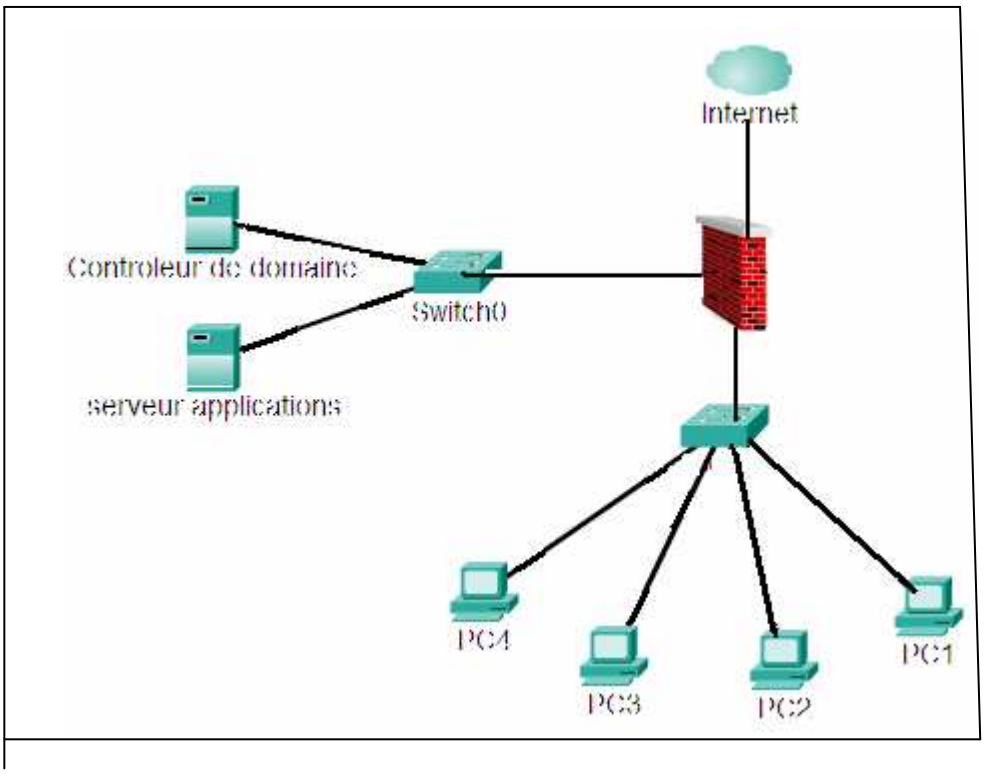

Figure 4-1 : Schéma de base du réseau à réaliser

4-3 VMware :

Dans cette partie, nous utiliserons un logiciel de virtualisation permettant de visualiser les étapes d'installation des différents systèmes d'exploitation et leurs configurations. Ainsi, l'installation de différents logiciels, programmes et tâches qui peuvent être exécutées sur un PC. Nous testerons donc toute la partie logicielle du réseau à réaliser.

4-3-1 Historique :

VMware, Inc. est une société filiale d'EMC Corporation, fondée en 1998, qui propose plusieurs produits propriétaires liés à la virtualisation d'architectures x86. C'est aussi par extension le nom d'une gamme de logiciels de virtualisation. Parmi ces produits nous citons : VMware Workstation, VMware Ace, VMware Player, VMware Fusion,…etc.

4-3-2 VMware Workstation :

C'est la version station de travail du logiciel. Sa toute première version VMware Workstation 1.0 est née en 1999. La version actuelle est VMware Workstation 6.0 que nous allons utiliser au cours de notre travail.

VMware Workstation 6.0 est une application de virtualisation permettant d'émuler de nombreux systèmes d'exploitation (excepté MaxOS). Une fois le programme lancé, il permettra d'installer une distribution sur une machine virtuelle. Elle constitue la référence absolue en matière de virtualisation pour poste de travail et ordinateurs portables.

VMware Workstation 6.0 :

- Assure l'exécution de plusieurs systèmes d'exploitation sur un même ordinateur
- Est compatible avec 19 versions de Windows et 26 versions de Linux pour postes de travail et serveurs
- Permet de basculer entre différents environnements informatiques d'un simple clic
- Permet de paramétrer des configurations et réseaux n-tiers
- Crée plusieurs snapshots de machines virtuelles en toute simplicité
- Ne limite plus la taille des disques virtuels à 2 Go, gère l'USB, les lecteurs DVD et les graveurs CD-R/RW
- Gère jusqu'à trois cartes réseau et neuf ports Ethernet virtuels
- Permet de créer et d'exécuter plusieurs machines virtuelles simultanément sur un même ordinateur

Il est possible de relier la machine virtuelle au réseau local

4-3-3 Fonctionnement :

Le logiciel de virtualisation VMware Workstation alloue les ressources physiques aux ressources logiques de la machine virtuelle. Ainsi, chaque machine virtuelle dispose d'un processeur, d'une mémoire, de disques et de périphériques E/S qui lui sont propres, exactement comme un ordinateur x86 standard. Aucun redémarrage ou partitionnement du disque dur n'est nécessaire pour basculer entre les machines virtuelles.

Lorsqu'une VM s'exécute dans un mode qui nécessite une émulation, VMware traduit dynamiquement le code privilégié en un code équivalent en mode utilisateur, le place dans un endroit libre de la mémoire, le rend invisible et inaccessible au code d'origine et l'exécute à la place. Lorsqu'une machine virtuelle fait appel à un périphérique, VMware intercepte la demande et la traduit pour qu'elle soit gérée par le système hôte. Bien que les machines virtuelles tournent en mode utilisateur, VMware nécessite d'installer plusieurs pilotes de périphériques privilégiés dans le noyau du système hôte.

VMware assure l'émulation de la carte vidéo, la carte réseau, le lecteur de CD-ROM, le bus USB, les ports séries et parallèles et le disque dur de type SCSI ou IDE. Ce dernier étant un fichier extensible d'une taille voisine de la place occupée sur la machine virtuelle ou fixe pour davantage de performance. Ce fichier contenant le contenu du disque peut être copié sur un autre hôte et exécuté par un ordinateur. Pour l'ordinateur virtuel, tous les périphériques sont identiques, même si le système hôte est totalement différent, car c'est VMware qui caractérise les périphériques.

4-3-4 Avantages du VMware :

- Réduction des coûts matériels par l'exécution de plusieurs systèmes physiques en tant que machines virtuelles sur un même ordinateur
- Augmentation de la productivité par la réduction du délai d'approvisionnement, de déploiement et de reconfiguration des machines physiques
- Optimisation des ressources par l'accès aux données et applications à partir du système d'exploitation d'un ordinateur unique
- Elimination des risques par le test isolé des correctifs et logiciels d'application, et préservation de l'état des machines virtuelles pour la sauvegarde ou la redistribution

4-3-5 Manipulation du VMware Workstation 6.0:

Au démarrage du logiciel VMware Workstation 6.0 on clique sur l'icône du bureau, une page d'accueil s'affiche proposant :

- New Virtual Machine
- New team

- Open Existing VM or team

New virtual machine : permet de créer une nouvelle VM, en suivant les étapes :

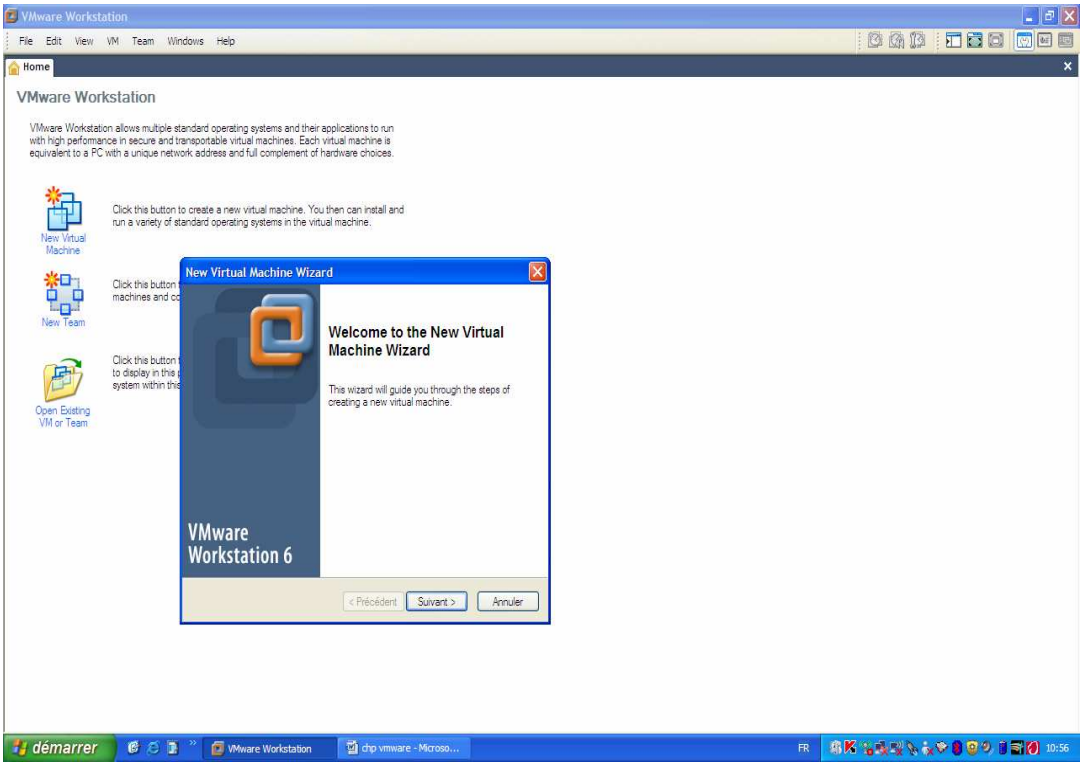

Figure 4-2 : Démarrage d'installation d'une VM

- ✓ Cliquer sur ***Suivant***
- ✓ Choisir entre une configuration standard: ***Typical*** (celle qu'on va utiliser tout au long du travail) ou une configuration personnalisée ***Custom***
- ✓ Choisir le système d'exploitation qu'on veut installer dans la VM ainsi que sa version
- ✓ Choisir l'emplacement de la VM sur la machine physique
- ✓ Sélectionner le type de réseau auquel appartient la VM
- ✓ Choisir la taille qu'occupe la VM sur le disque dur

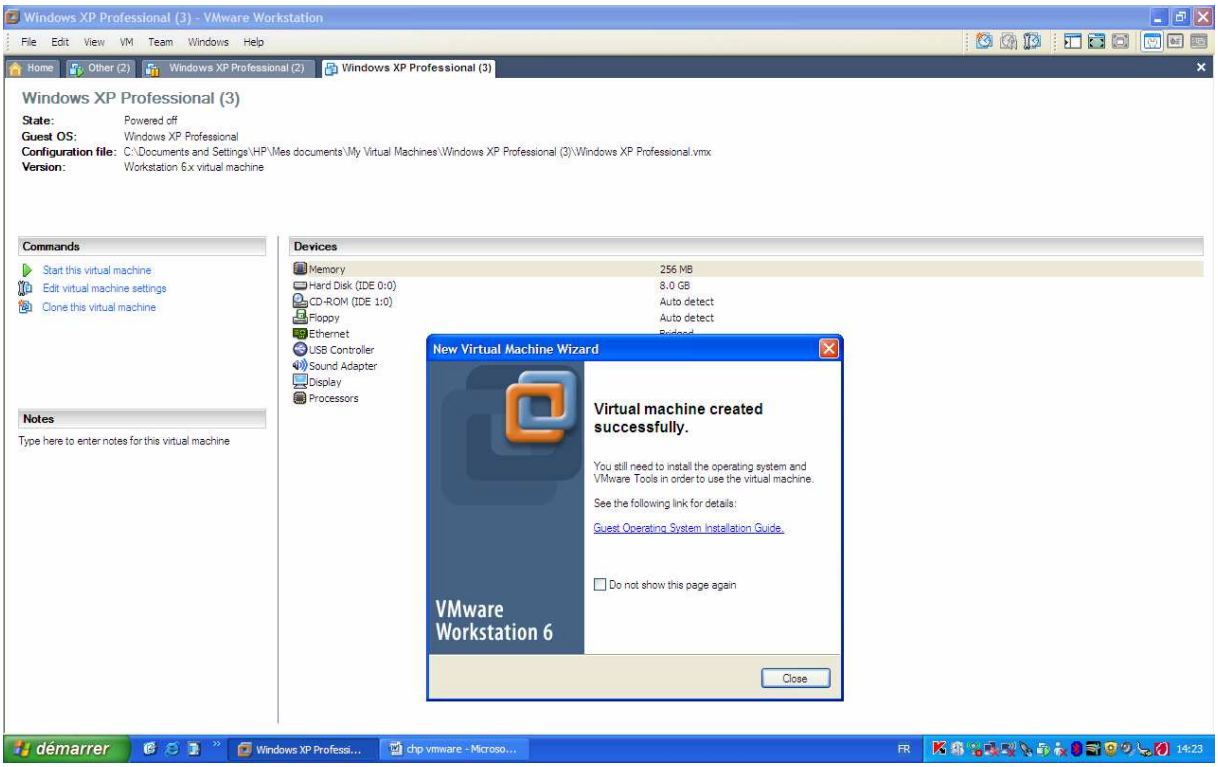

Figure 4-3 : Fin des étapes d'installation d'une VM

- ✓ Fermer la fenêtre

Il suffit d'insérer le CD correspondant au système d'exploitation choisi au départ et cliquer sur ***start this virtual machine*** pour que la machine démarre normalement.

New team : Pour créer un nouveau groupe, on peut ajouter des VM et les connecter sous un réseau privé

Open Existing VM or team : Pour ouvrir les VM et groupes déjà crées .

4-4 Choix des systèmes d'exploitation :

Le choix du système d'exploitation de la machine est une tâche très importante. Dans cette partie nous prendrons en considération pour ces choix les exigences posées dans le cahier des charges, afin d'assurer le bon fonctionnement du réseau. Tout le travail qu'on désire réaliser pour répondre à ces conditions sera traité sur VMware Workstation.

4-4-1 Définition d'un système d'exploitation (SE):

Le système d'exploitation est un ensemble de programmes qui remplissent deux grandes fonctions :

- Il gère les ressources de l'installation matérielle, en assurant leur partage entre un ensemble plus au moins grand d'utilisateurs.
- Il assure un ensemble de services, en présentant aux utilisateurs une interface mieux adaptée à leur besoin que celle de la machine physique.

4-4-2 Le SE Microsoft Windows 2000 Server :

Il existe environ 1000 utilisateurs réseau au niveau de la SONATRACH, qui sont répartis selon le travail demandé en services et sous services. Le serveur doit donc assurer l'administration de ces organisations et la gestion des droits d'accès des utilisateurs. L'utilitaire Active Directory conçu pour Microsoft Windows 2000 et 2003 serveurs, est une bonne solution pour ordonner toutes ces bases de données présentes.

4-4-2-1 Installation du Microsoft Windows 2000 server :

L'installation peut se faire en plusieurs manières :

- à partir d'un CD bootable.
- en utilisant les 4 disquettes de boot (créer à partir du dossier makeboot).
- copie d'image.

L'installation de Windows 2000 server sera présentée dans l'annexe.

4-4-2-2 Configuration de Windows 2000 server :

L'administration d'un réseau d'une entreprise sous Windows 2000 server, consiste à représenter sa structure interne sous forme d'arborescence (hiérarchie) de domaine dans Active Directory.

4-4-2-2-A Installation d'Active Directory :

-cliquer sur ***Démarrer*** puis ***Exécuter***

-dans la zone de texte taper ***DCPROMO***

-cliquer sur ***OK***

Et l'assistant d'Active Directory s'affiche

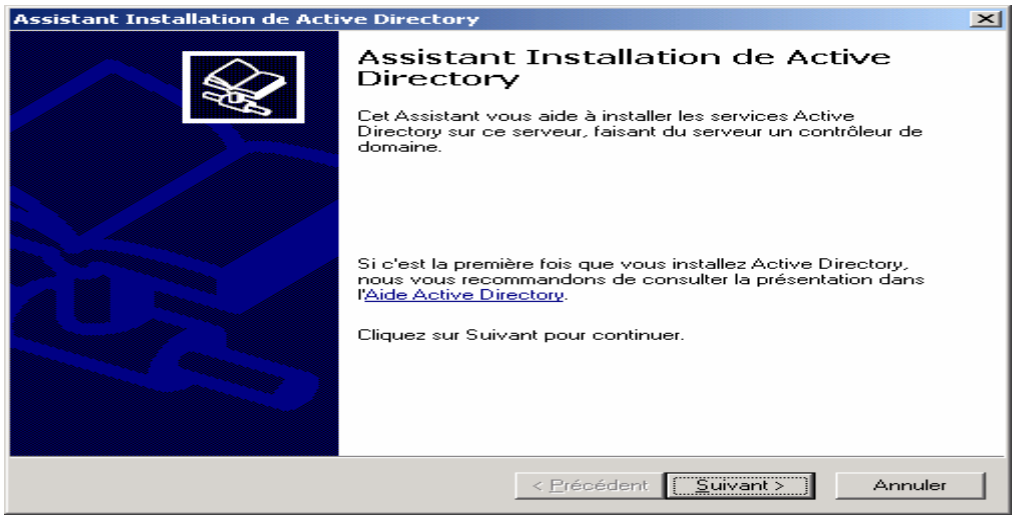

Figure 4-4 : Assistant d'installation d'Active Directory

-Cliquer sur ***Suivant*** pour continuer.

-Dans notre cas, ceci étant le premier serveur de notre réseau, nous devons créer un ***Contrôleur de domaine pour un nouveau domaine.*** L'autre option sera utilisée pour un serveur supplémentaire. Cliquer sur ***Suivant***

-la deuxième partie c'est de créer une arborescence de domaine ou un nouveau domaine enfant dans une arborescence de domaine existante.

- puisque aucun domaine n'existe sur notre réseau, cocher sur ***Créer une nouvelle arborescence de domaine***. Cliquer sur ***Suivant.***

-Comme c'est le premier serveur, nous allons créer une nouvelle forêt. Cliquer sur ***suivant***

-L'étape suivante consiste à de donner *un nom DNS* à notre nouveau nom de domaine. Il doit être de la forme ***Nom.extention.*** Cliquer sur ***Suivant***

-Une fois le nom de domaine est spécifié, nous devons lui donner un nom ***NetBIOS*** pour permettre la connexion de stations utilisant d'anciennes versions de Windows.

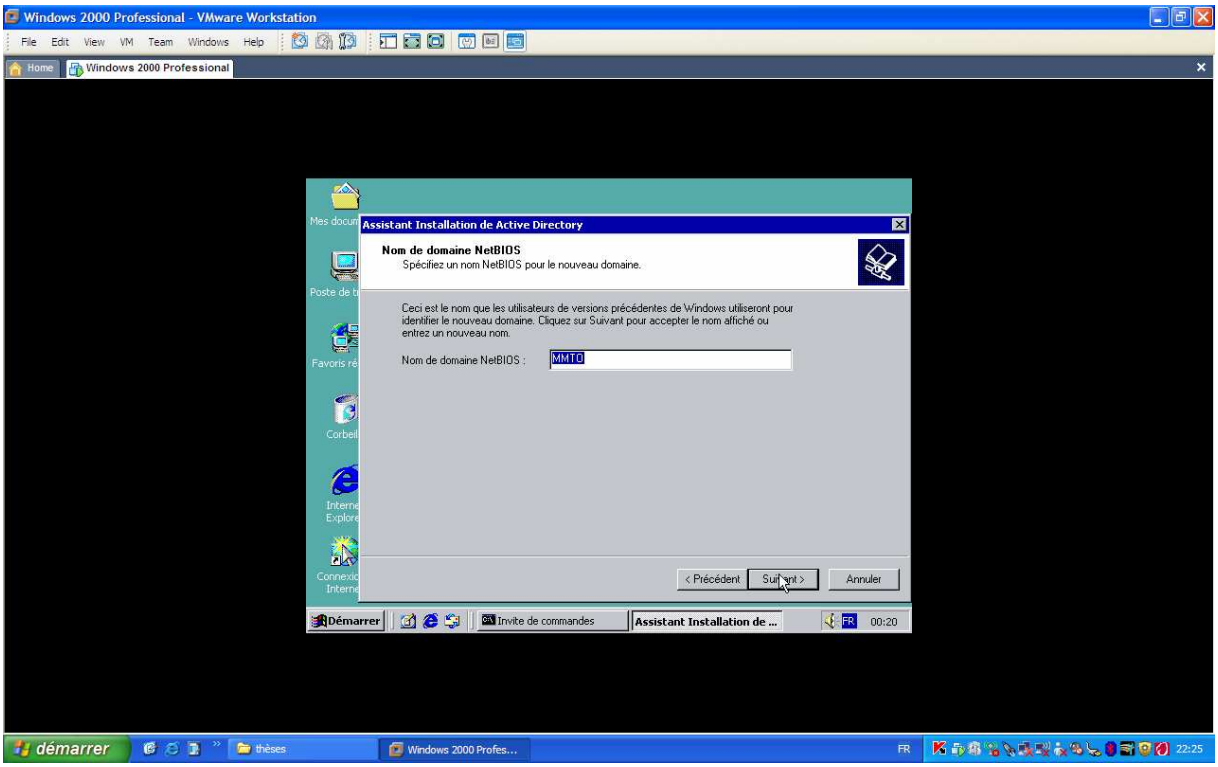

Figure 4-5 : Nom du domaine NetBios

-Cliquer sur ***Suivant***

-L'étape suivante consiste à créer les différents dossiers de stockage pour l'annuaire, avant d'essayer de se connecter sur un contrôleur de domaine existant. Laisser les dossiers proposés. Cliquer sur ***Suivant***

-Demande de l'installation du ***service DNS***

-Notre réseau ne contient pas de clients NT4, Windows 95, 98 ou Me, cliquez sur Autorisations compatibles uniquement avec les systèmes d'exploitation serveurs Windows 2000 ou Windows Server 2003. Cliquez sur ***Suivant***

-Spécifier le mot de passe d'administrateur à utiliser lors du démarrage de l'ordinateur**.**

-Cliquer sur ***Suivant***

-résumé de l'installation demandée. Cliquer sur ***Suivant***

-démarrer l'installation demandée

-Fin de l'installation d'Active Directory.

-Cliquer sur ***Terminer*****.**

4-4-2-2-B Création des comptes utilisateurs :

Dans le menu ***démarrer,*** pointer sur ***programme*** puis sur ***Outils d'administration*****.** Cliquer alors sur ***Utilisateurs et ordinateurs Active Directory***.

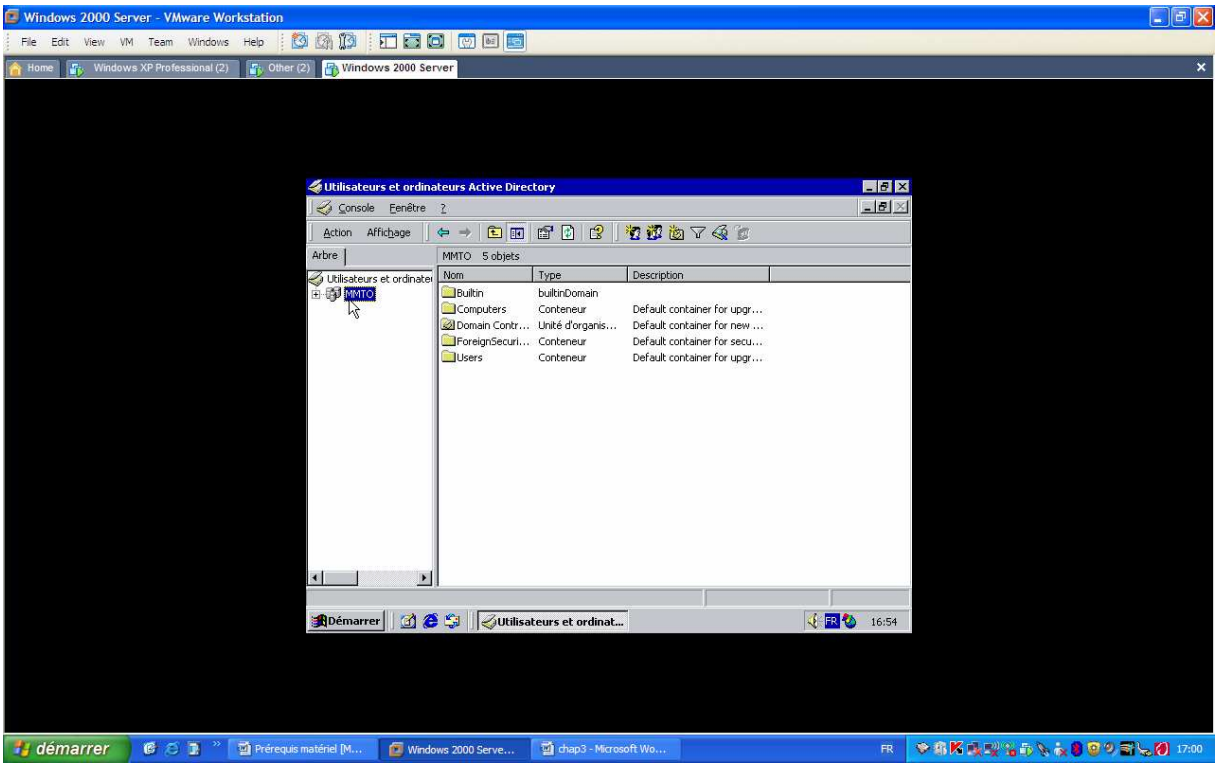

Figure 4-6 : Création de comptes utilisateurs

Cliquer avec le bouton droit sur le domaine ***MMTO.dz,*** cliquer sur ***Nouveau*** puis cliquer sur ***Unité d'organisation***

Dans la zone de texte taper le nom de cette unité. Cliquer sur ***OK***

4-4-2-2-C Création d'unités d'organisation :

Cliquer avec le bouton droit sur unité d'organisation créée préalablement, pointer le curseur sur ***Nouveau*** puis cliquer sur ***Unité d'organisation.*** Cliquer sur ***OK***

De même on peut créer de nouveaux ordinateurs, utilisateurs et groupes. Notre configuration est la suivante :

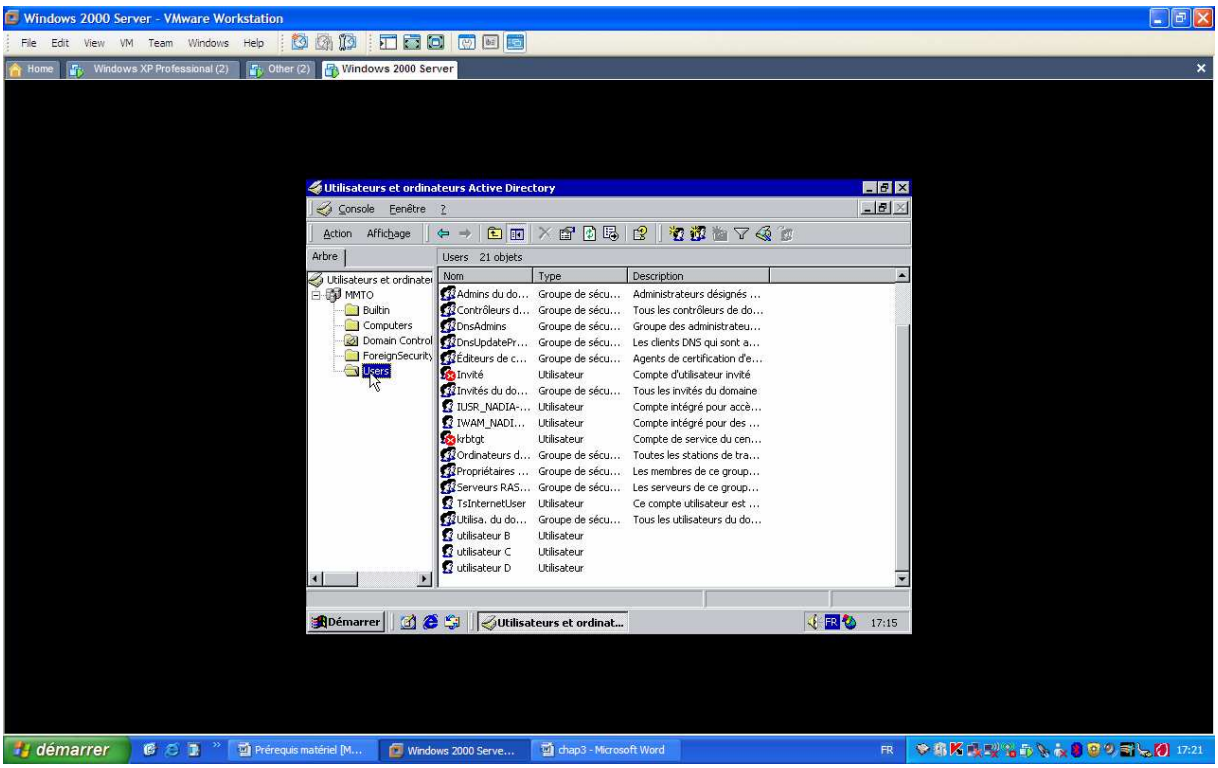

Figure 4-7 : Fin de création des comptes utilisateurs

4-4-2-3 Partage de ressources et affectation des droits d'accès :

Eu tant qu'administrateur, on doit assurer que les utilisateurs peuvent accéder aux ressources dont ils ont besoin pour leur travail.

Pour améliorer la sécurité, une possibilité de contrôler les personnes qui auront accès à ces dossiers partagés existe.

Pour créer un dossier partagé, dans l'explorateur Windows, cliquer avec le bouton droit sur le dossier, puis cliquer sur ***Partager*.**

Dans l'onglet ***Partage*** configurer les options suivantes :

- sélectionner l'option ***Partager ce dossier,*** donner un nom du partage puis une description (commentaire).
- cocher sur ***Autorisation*** pour définir les autorisations sur le dossier partagé.
- cliquer sur ***Ajouter***
- sélectionner les comptes utilisateurs auxquels on veut accorder les droits d'accès puis cliquer sur ***Ajouter***
- cliquer sur ***OK***
- sélectionner les utilisateurs et cocher ***Autorisé***
- cliquer sur ***Appliquer*** puis ***OK.***

4-4-2-4 Avantages et inconvénients :

Le système d'exploitation Windows 2000 server a les avantages suivants :

- La logithèque
- La stabilité
- Simplicité d'utilisation

Mais tout de même, il a des inconvénients tels que :

- Un système trop fermé
- Cher
- Et son plus grand inconvénient est au niveau de la sécurité.

4-4-3 Le SE linux Open1SUSE :

LINUX peut être utilisé comme serveur Intranet/Internet, la plupart des distributions de LINUX contiennent tous les logiciels nécessaires pour réaliser un serveur Intranet/Internet complet. Cela inclut les fonctionnalités :

- ✓ De transfert et de distribution de courrier électronique
- ✓ De serveur web ou FTP
- ✓ De serveur de nom de machine DNS ainsi DHCP

La version Open SUSE offre une grande facilité d'administration, de configuration des différents services et une grande immunité contre les virus. Ainsi, nous préférons à notre serveur d'application cette version de linux afin d'assurer plus de performance et de sécurité lors du lancement de nos applications.

4-4-3-1 Installation d'OpenSUSE :

Il existe deux possibilités pour installer Linux :

- L'installer depuis Windows, une fois fait on aura un choix au démarrage. L'avantage est de pouvoir désinstaller facilement, son inconvénient est qu'il sera moins performant, et nécessitera plus de mémoire (512Mo). On adoptera la méthode suivante.
- redémarrer l'ordinateur avec le CD de linux dans le lecteur.

Les étapes d'installation d'OpenSUSE seront présentées dans l'annexe.

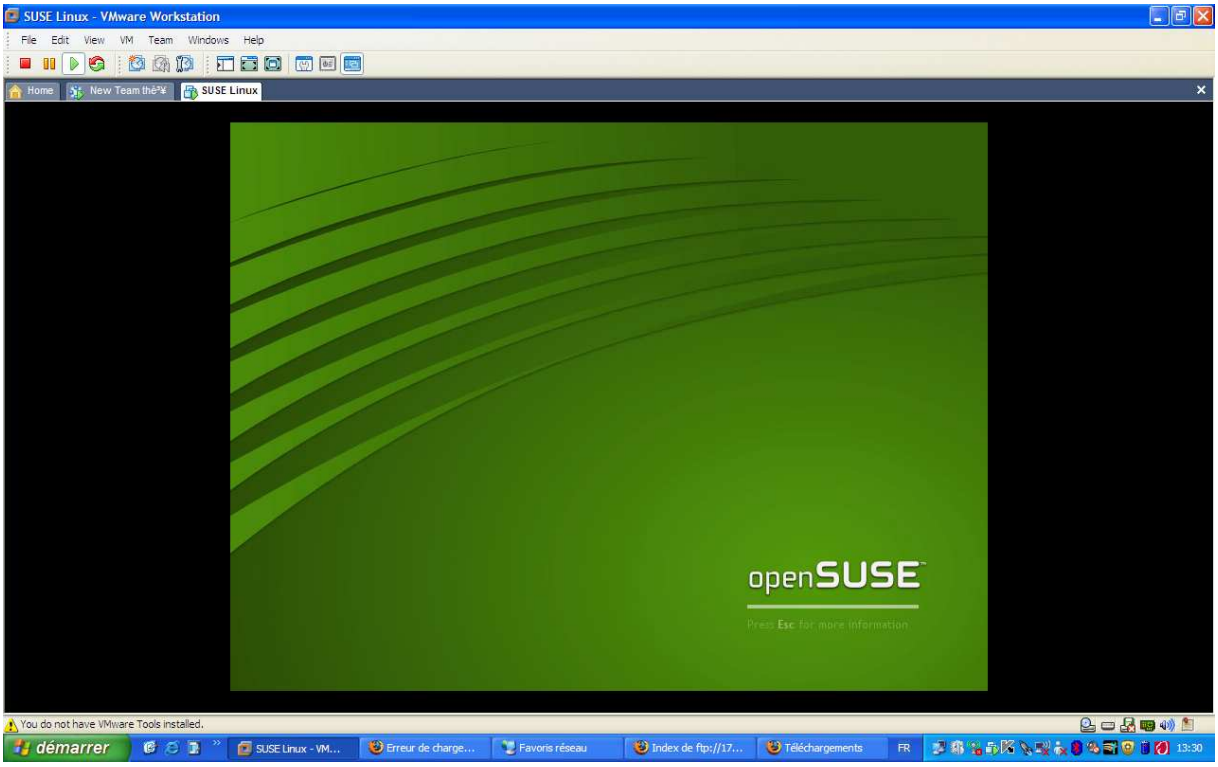

Figure 4-8 : Installation d'OpenSUSE.

4-4-3-2 Configuration d'OpenSUSE :

La majorité des distributions Linux prennent en charge l'installation des pilotes matériels, de plusieurs utilitaires et logiciels qui facilitent les tâches des utilisateurs. De même pour l'OpenSUSE, ces pilotes ont été installés par défaut. Plusieurs applications peuvent être installées sur ce serveur, nous avons choisis d'installer un serveur web.

4-4-3-2-1 Le serveur Web Apache :

Le serveur http Apache est le fruit de travail d'un groupe volontaire « the Apache group » sous forme de logiciel libre. La première version est apparue en décembre 1995. Par la suite des centaines d'utilisateurs ont contribué à son amélioration. Il engloba plusieurs avantages et c'est le serveur Web le plus utilisé au monde actuellement par le fait qu'il :

- Soit un serveur gratuit
- ait un niveau de performance élevé pour des besoins matériels modestes
- Soit extensible, modulaire, configurable et robuste
- Soit portable (Linux, Windows,…) contrairement à IIS (Internet Information Service)

4-4-3-2-2 Installation du serveur apache :

La version Open SUSE contient plusieurs logiciels par défaut, parmi ces logiciels on trouve Apache2. Pour le lancer, il faut lui installer les package qui lui sont compatibles dans son CD de boot. Aller à l'installation logicielle, sélectionner les logiciels à utiliser et confirmer l'installation.

Pour vérifier cette installation, aller au repertoire ***etc*** et retrouver le repertoire ***Apache2*** et pour l'activer le service Apache, taper la commande '***service apache2'*** dans le terminal.

4-4-3-3 Caractéristiques d'OpenSUSE :

S i openSUSE est livrée avec beaucoup de logiciels similaires à d'autres distributions, certaines caractéristiques lui sont bien spécifiques. Parmi lesquelles, on cite:

- Le centre de contrôle YaST
- Le gestionnaire de paquets ZYpp
- Le service de compilation public openSUSE Build Service
- Le menu Slab — maintenant inclu en amont dans KDE, mais toujours unique dans la version GNOME d'openSUSE et SLED
- L'installation par défaut de nombreux logiciels
- Les forums officiels très actifs
- La participation directe dans le développement de GNOME et KDE
- Le choix du bureau par défaut laissé libre à l'utilisateur
- Le *polissage* incomparable du bureau
- L'installation en un clic (One-click install)
- La boîte en vente - une voie aisée pour les débutants qui commencent avec openSUSE
- La très bonne intégration de Mono
- Les dépôts logiciels disponibles dans le Build Service
- Le choix de l'image DVD avec beaucoup de logiciels ou des Live-CD avec une sélection minimale
- la très bonne implémentation dual-architecture x86_64
- Le support serveur - openSUSE convient très bien pour une utilisation serveur

- Et comme tous les systèmes linux, il présente une grande immunité contre les virus, il est libre et ouvert, diffusé gratuitement ou à faible coût et disposant d'un excellent support de protocoles et applications Internet.

4-4-4 Pour postes clients :

Nous allons utiliser :

- Microsoft Windows XP : il est doté de plusieurs fonctionnalités tel que :
  - Destiner à grand public
  - Une gestion des comptes d'utilisateurs simplifiée permettant de créer plusieurs comptes et d'affecter à chacun un mot de passe
  - Le partage de fichiers et de ressources matérielles avec les autres utilisateurs du réseau
  - Contient un assistant configuration réseau qui paramètre automatiquement la plupart des options

- Linux Ubuntu : nous avons choisi cette version au vu des nombreux avantages qui la caractérisent. Citons quelques uns :
  - Destiner à grand public
  - Centralisation des applications
  - Une gestion système plus sécurisée en imposant une fenêtre login pour vérifier l'identité et mot de passe
  - une immunité contre les virus

4-5 Mise en place d'un firewall:

Un firewall est une nécessité dans tous les réseaux informatiques (même dans PC personnel), on peut se le procurer dans beaucoup de magasins d'informatiques, ou simplement avec une simple vielle machine grâce au smoothwall. Dans notre réseau, nous avons une zone interne qui est constituée du réseau utilisateurs, de deux serveurs dont le premier est un contrôleur du domaine et le deuxième pour bases de données. Tout l'ensemble

doit bénéficier d'Internet. Sur le smoothwall on peut avoir jusqu'à trois cartes réseaux afin de définir trois zones déférentes :

- Une verte sur laquelle seront relié le réseau local et le serveur de fichiers par exemple
- Une orange sur laquelle serons reliés le serveur web et serveur de jeu en réseaux

- Une rouge sur laquelle sera relié le modem Ethernet.

Le firewall dont est muni le Smoothwall permet de bloquer les connections de la carte rouge vers la carte verte, c'est à dire de bloquer les intrusions depuis internet vers notre réseau. La troisième carte nommée "carte orange" permet de créer une DMZ (zone démilitarisée) dans la quelle on peut placer des serveurs qui doivent être accessibles depuis internet à certaines conditions seulement. Par exemple pour un serveur web, le passage de la carte rouge vers la carte orange sera autorisé sur le port TCP 80 uniquement. Les machines installées sur la carte orange peuvent quand à elles "sortir" librement en direction d'internet mais ne peuvent se connecter à votre réseau, à moins de créiez une règle spéciale (déconseillé). Evidement les machines du réseau interne (zone verte) peuvent se connecter sans restrictions à celles de la zone orange ou "sortir" sur internet.

4-5-1 Installation du smoothwall:

Les étapes d'installation du smoothwall seront présentées dans l'annexe.

Une fois l'installation terminée, on peut passer à sa configuration en utilisant une interface web à partir de l'un des ordinateurs présents dans le réseau. Taper le lien : http://192.168.0.1 :81 (192.168.0.1 étant l'adresse IP du smoothwall)

4-5-2 Configuration du smoothwall :

About your smoothie :

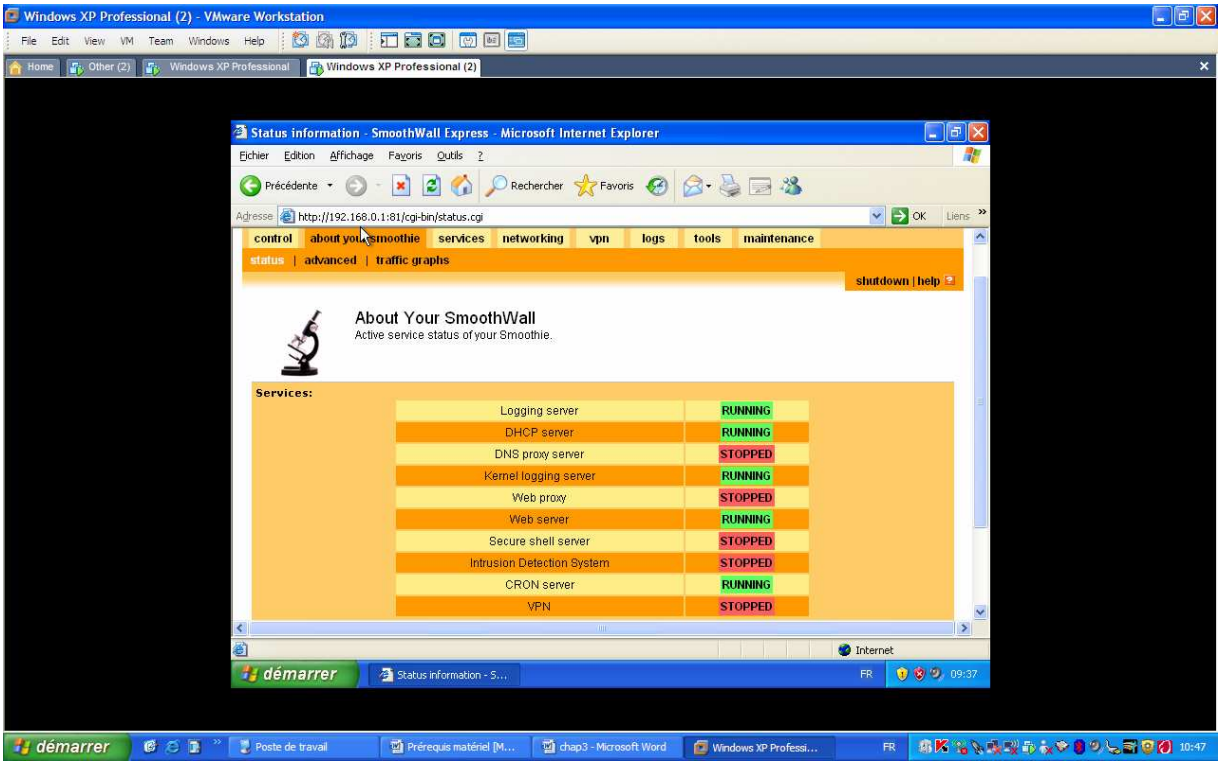

Figure 4-8 : Les services configurés sur smoothwall

Services :

- Vérifier que le système de détection d'intrusions est en route
- Secure shell server (pour connecter par sftp, scp ou ssh)
- Web proxy (configuration obligatoire des navigateurs qui utilisent le proxy ou non)
- Serveur DHCP : permet de demander au smoothwall d'attribuer une adresse IP aux machines du réseau interne
- Trafic graphs : c'est un contrôleur de flux c'est-à-dire le trafic dans le réseau

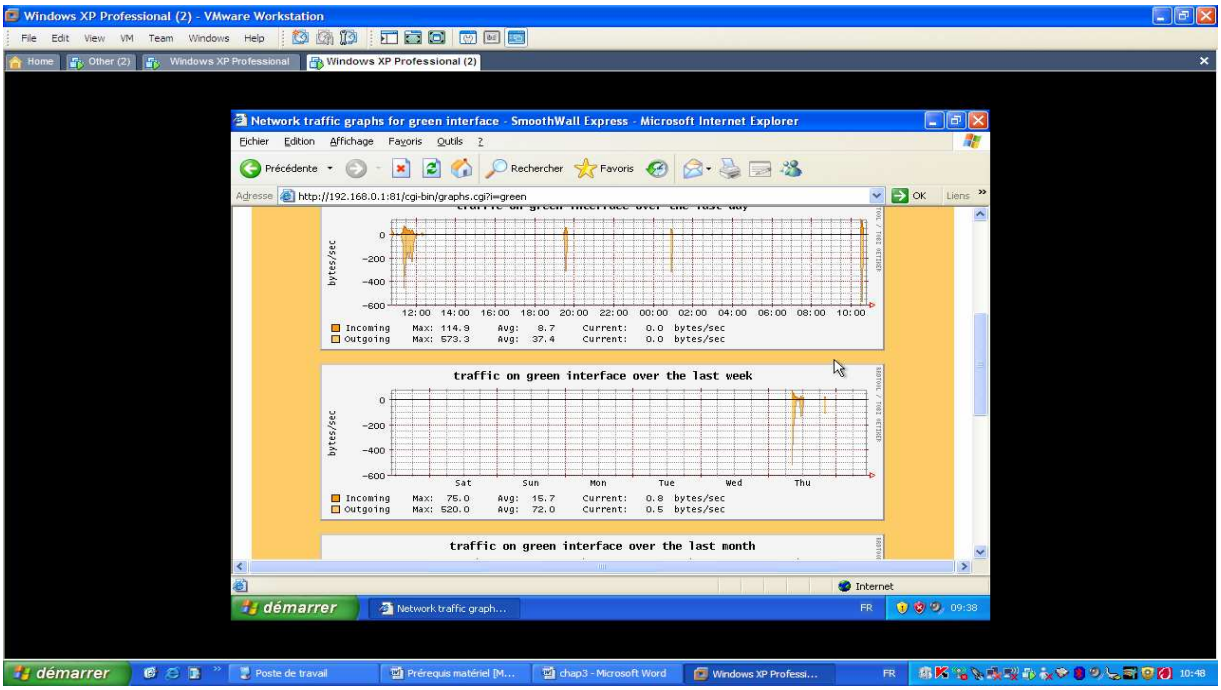

Figure 4-10 : contrôleur du trafic réseau

Networking : permet de paramétrer les règles de filtrage :

- Port forwarding : autorise des connexions depuis Internet vers le smoothwall (déconseillé sauf ssh si on veut administrer le smoothwall depuis internet)
- External service access : permet d'ouvrir un port pour des connections depuis internet vers la DMZ (orange). par exemple : pour rendre le serveur web accessible de l'extérieur, ouvrir le port 80.
- DMZ pinholes : permet d'ouvrir des ports pour des connections de la DMZ vers la zone interne (verte).
- ppp settings : permet de configurer le modem de secours branché sur le port série
- IP block : permet de définir les adresses IP qu'on veut bloquer et la manière de le faire
- Advanced : permet d'affiner le comportement du firewall par rapport à certains événements, mais peut poser problème à MSN.

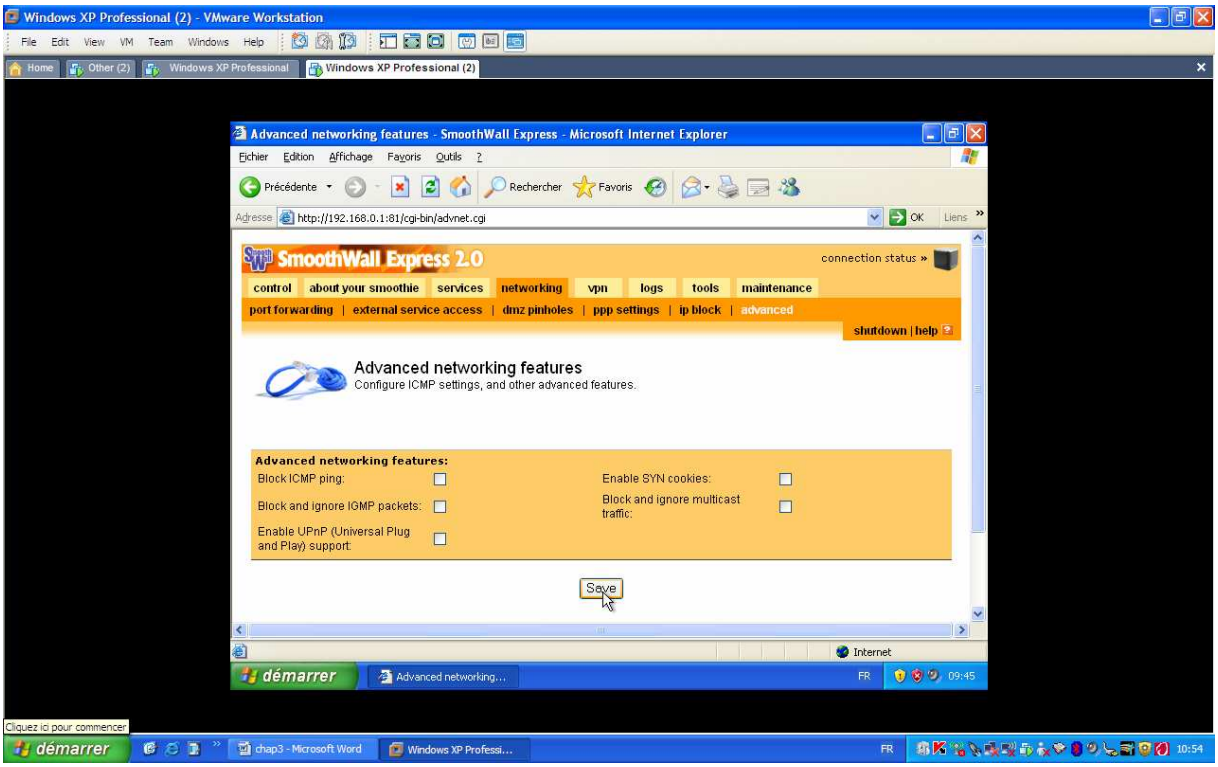

Figure 4-11 : Services Networking

Service/Time : Pour la mise à l'heure du smoothwall

Shutdown : pour fermer le smoothwall il suffit de cliquer sur « shutdown » et pour le redémarrer cliquer sur « reboot ».

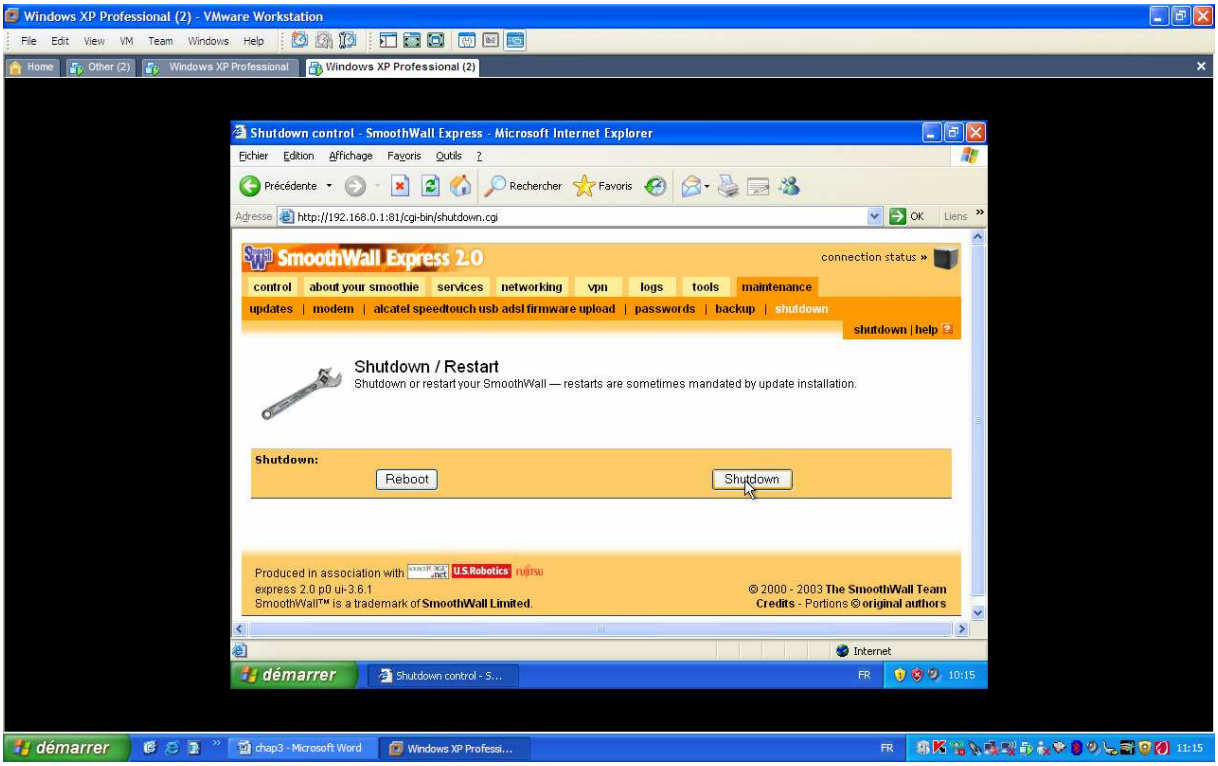

Figure 4-12 : Services maintenances

4-6 Simulation de l'application :

Après avoir installé les systèmes d'exploitation choisis pour serveurs et clients, et configuré le smoothwall selon les objectifs désirés (3 cartes réseaux, serveur DHCP et un maximum de performance), nous allons simuler notre travail dans un environnement virtuel en lançant les VM configurées comme serveurs et postes utilisateurs dans VMware Workstation 6.0. Ceux-ci serons reliés automatiquement en réseau local dans ce logiciel.

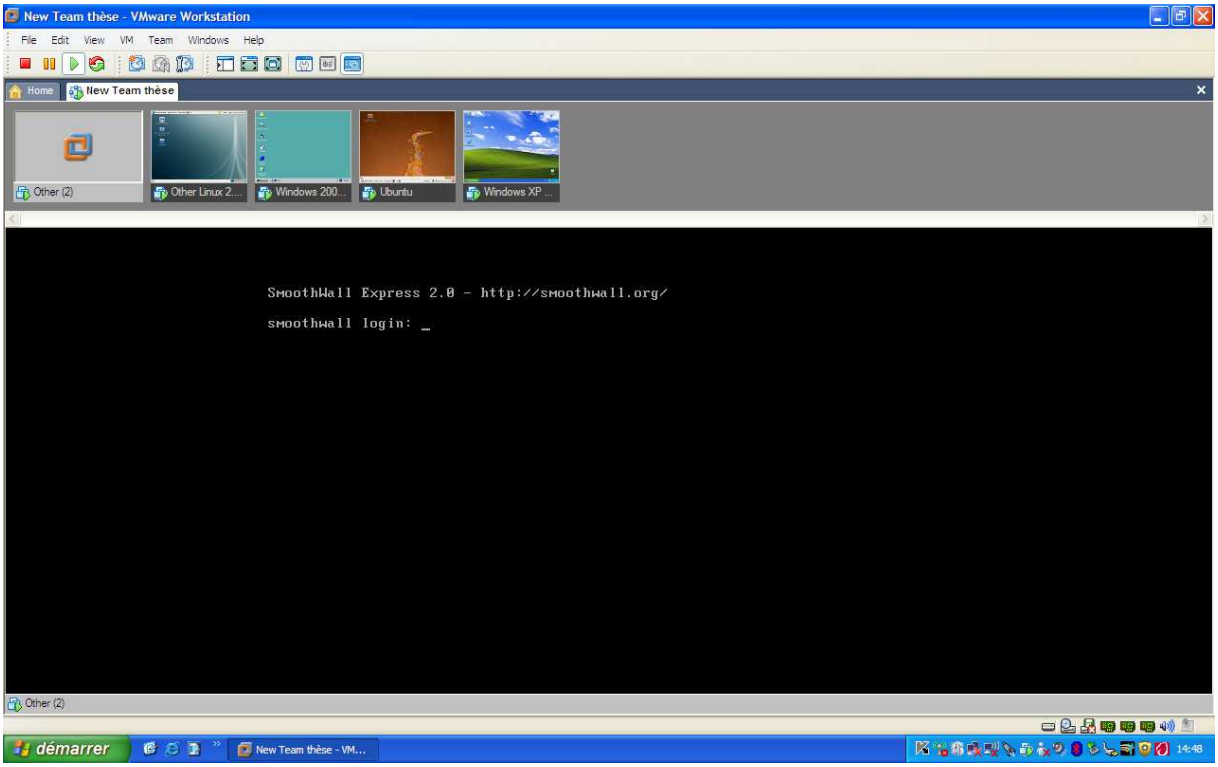

Figure 4-13 : Simulation de l'application

Cet espace virtuel va permettre de vérifier la totalité des applications réalisées dans un réseau réel tel que :

- Envoyer des signaux d'échos (Ping) pour vérifier la présence des machines dans le réseau
- Accéder à partir des postes utilisateurs au smoothwall et apporter des modifications si nécessaire
- Accéder à la page web injectée dans le serveur web
- Faire le partage des fichiers et des ressources matérielles
- Gérer les droits d'accès à partir du contrôleur du domaine

4-7 Réalisation de l'application

Lors de la mise en place d'un réseau local, il est utile de faire une étude préalable sur ce réseau. Une fois fait, nous allons essayer de mettre en évidence ces connaissances pour dégager quelques recommandations qui pourront aider les responsables de déploiement à faire la meilleure conception possible et d'utiliser le matériel nécessaire pour tirer le meilleur profit de leurs réseaux.

4-7-1 Plan d'action adopté :

Installation du réseau LAN selon l'architecture suivante :

1. Installation du smoothwall selon la configuration vue précédemment
2. Placer le serveur web dans la zone DMZ, celui-ci peut accéder à l'extérieur à travers la carte RED
3. Placer le contrôleur de domaine et les postes clients dans le réseau interne afin d'assurer sa sécurité, cette zone peut accéder aux autres zones mais ne peut être accédée.

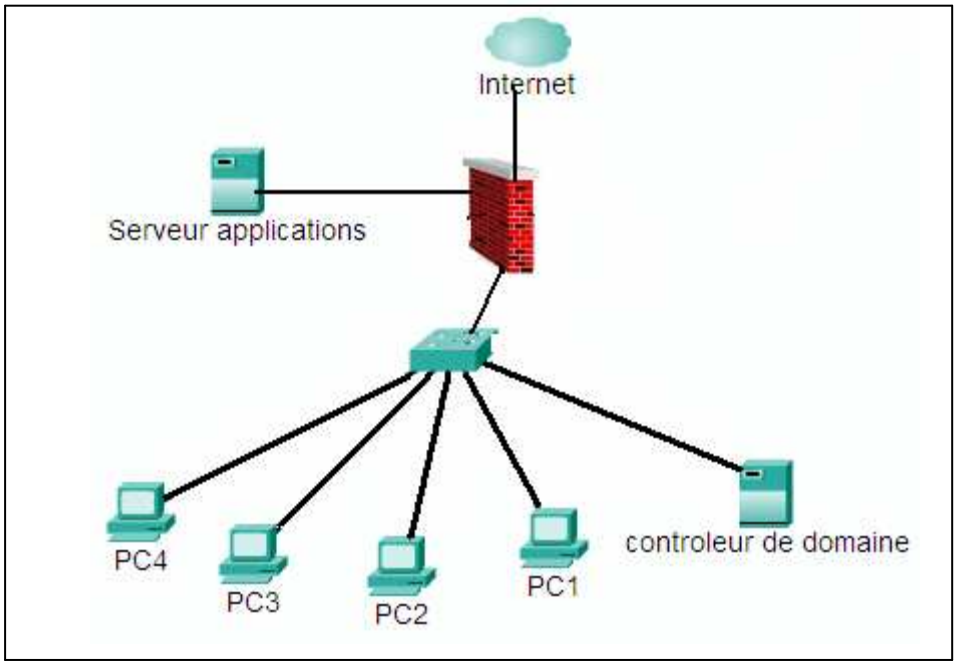

Figure 5-1 : Schéma de travail adopté

4-7-2 Outils nécessaires :

- 7 PC qui sont équipés de cartes réseau de type Ethernet 10/100 Mbits/s.
- Les cartes sont placées dans le slot d'extension PCI de chaque PC, et ils sont équipés d'un connecteur de type RJ45.
- un Switch nécessaire pour un réseau en topologie étoile, doté de 8ports répondant à la norme Ethernet 10/100Mbits/s.
- câbles à paire torsadées UTP Cat 5 (obligation pour un réseau Fast Ethernet)

4-7-3 Présentation de la page web réalisée :

Après installation du serveur Apache et version PHP conçus pour UNIX, et vu les possibilités qu'offre Dreamweaver nous l'avons utilisé pour créer notre page web.

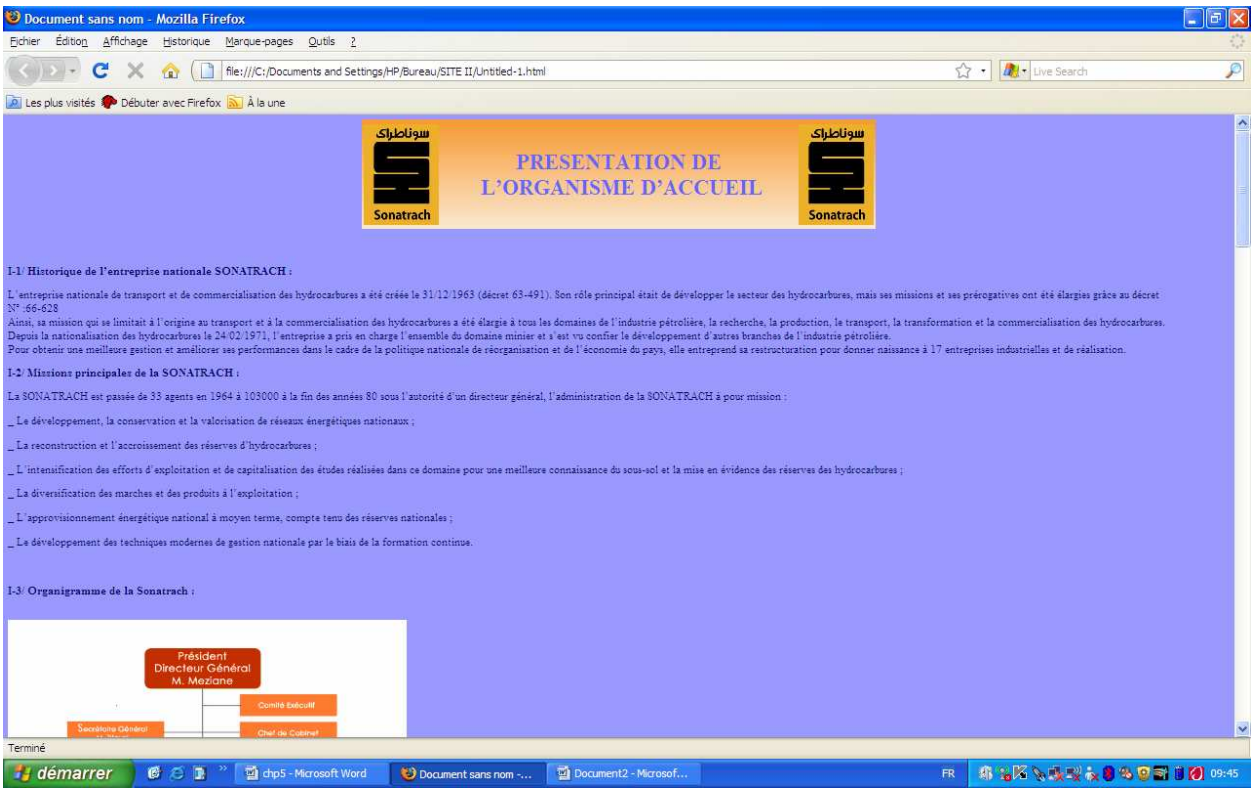

Figure 5-2 : présentation de l'historique de la Sonatrach

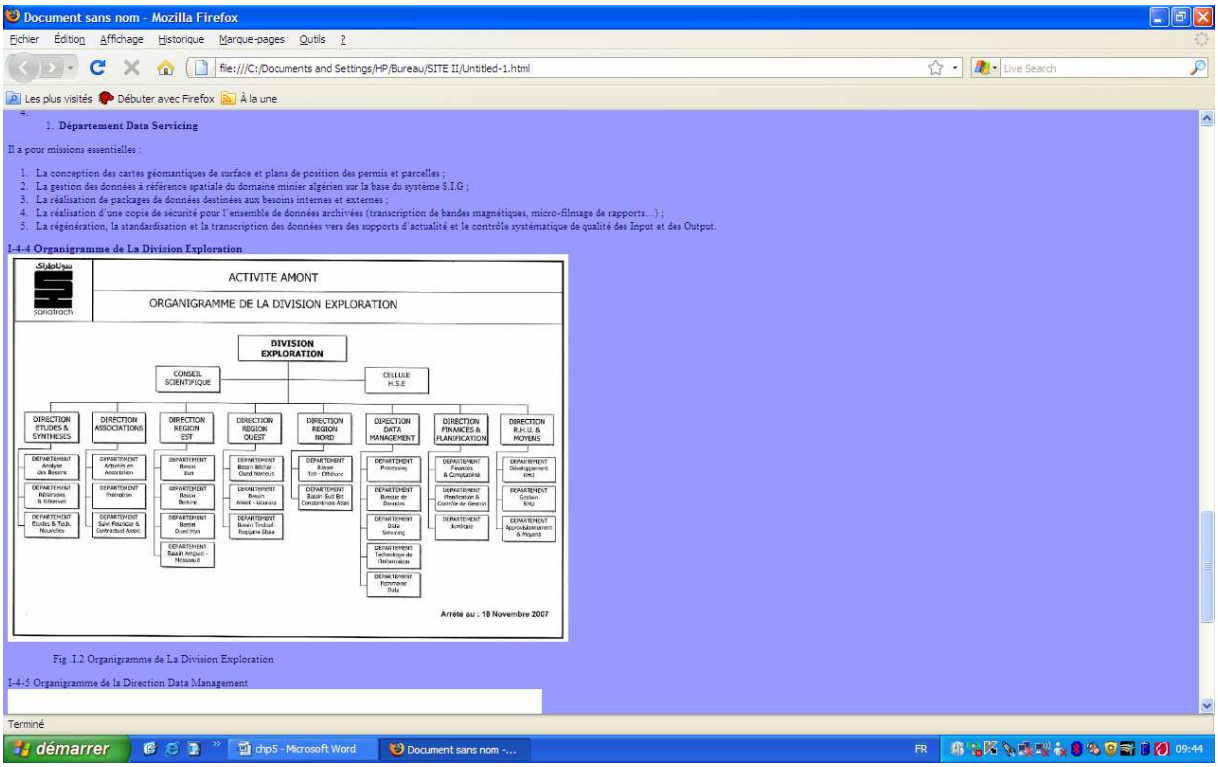

Figure 5-3 : Organigramme de la division Exploration

Cette page web va être placée dans le fichier ***httdocs*** du document ***www*** du fichier ***srv***. Il faut tout de même activer le serveur apache2 à chaque utilisation.

4-7-4 Accès à la page web :

Pour qu'on puisse accéder à cette page on doit configurer le serveur apache, en modifiant ***listen80*** qui se place dans le fichier ***httpd.conf*** de ***apache2,*** ce dernier se trouve dans le fichier ***etc*** en ***listen * :80.***

Pour accéder à cette page web à partir de n'importe quel poste du réseau, il faut préciser l'adresse de la machine ainsi le chemin du dossier hébergeant cette page.

4-8 Conclusion :

Ce chapitre s'est porté sur la présentation des différents outils utilisés lors de la réalisation de notre réseau ainsi que les déférentes fonctionnalités qu'il offre. Ceci était simulé sur un logiciel de virtualisation appelé VMware qui nous a permis de tester la performance de notre réseau avant de l'exécuter concrètement sur des machines physiques. Nous avons aussi porté un accent sur la réalisation d'une page Web accessible depuis les postes de notre réseau.

Conclusion générale :

Dans le cadre de ce travail, notre but était d'assurer une sécurité meilleure au réseau réalisé en respectant les exigences tracées dans le cahier des charges. Nous avons pu installer sur les postes de ce réseau différents systèmes d'exploitation Microsoft et Linux, non seulement pour se familiariser avec ces systèmes mais aussi pour faire le choix convenable selon les nécessités imposées.

Dans la première partie de notre application, nous avons utilisé un logiciel de virtualisation pour tester toutes les étapes d'installation, de configuration et de communication entre tous les éléments du réseau.

Nous avons configuré le smoothwall avec trois cartes réseau, une verte pour notre réseau interne, une orange pour la DMZ et une rouge pour l'accès à internet. La zone DMZ a l'accès à Internet ce qui la rend exposée aux déférentes attaques extérieures. Ainsi, nous lui avons préférer une version Linux qui a une grande immunité contre les virus et plus de performance pour la gestion de l'information.

Cependant, notre contrôleur de domaine doit gérer les droits d'accès, administrer les comptes utilisateurs et garantir une confidentialité des informations. Ce qui nécessite une stratégie sévère pour assurer sa sécurité à cent pour cent. Ainsi, nous l'avons placé dans la partie interne de notre réseau, sachant que cette partie peut accéder aux autres parties sans qu'elle soit accessible par ces dernières.

Ce travail nous a permis de manipuler certains outils dans le domaine d'informatique, ce qui nous ouvrira des perspectives diverses. Nous considérons que l'essentiel de notre but est atteint, même s'il reste à parfaire certaines notions dans le domaine de la sécurité. Nous espérons que ce travail apportera aux étudiants d'avantages de savoir et de connaissances.

1-Etapes d'installation de Windows 2000 Server :

Après avoir partitionner et partager le disque dur, l'installation sera lancée :

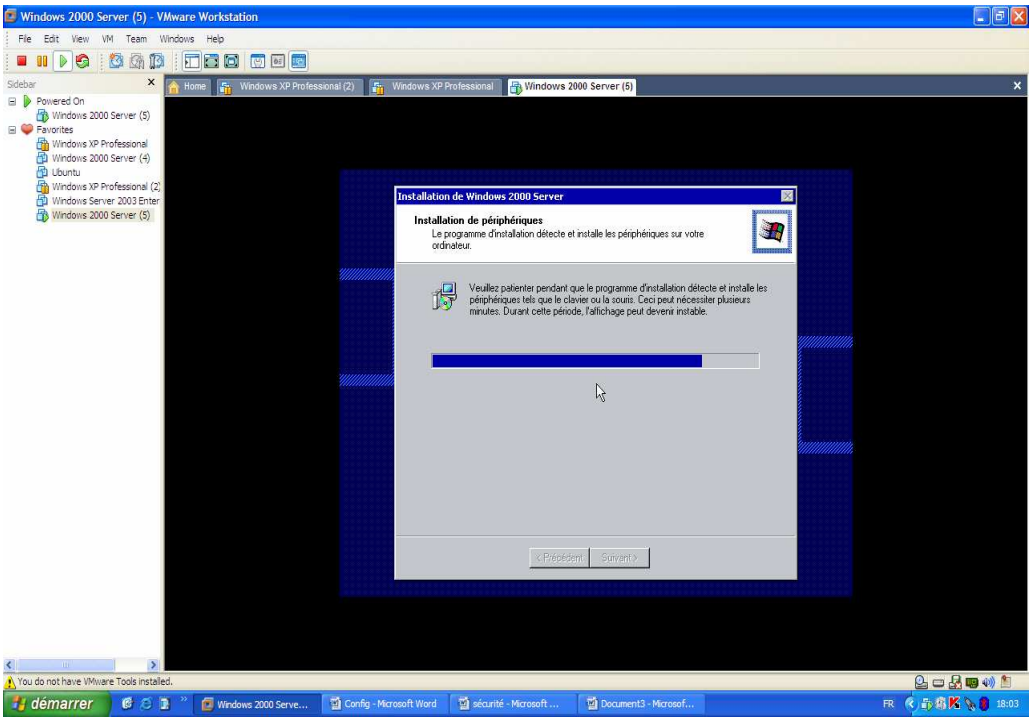

Figure 1 : Lancement d'installation de Windows 2000

Les étapes d'installation sont les suivantes :

- ✓ Cliquer sur ***suivant***
- ✓ Entrer la clé du produit
- ✓ Taper le nom d'utilisateur et son mot de passe
- ✓ Choisir les composants Windows 2000
- ✓ Régler la date et l'heure
- ✓ Choisir les paramètres de gestion de réseau
- ✓ Désigner le nom du domaine auquel appartient cet ordinateur, cliquer ***non*** s'il n'appartient à aucun domaine
- ✓ Fin d'installation.

2-Etapes d'installation de la Fedora 8.0 :

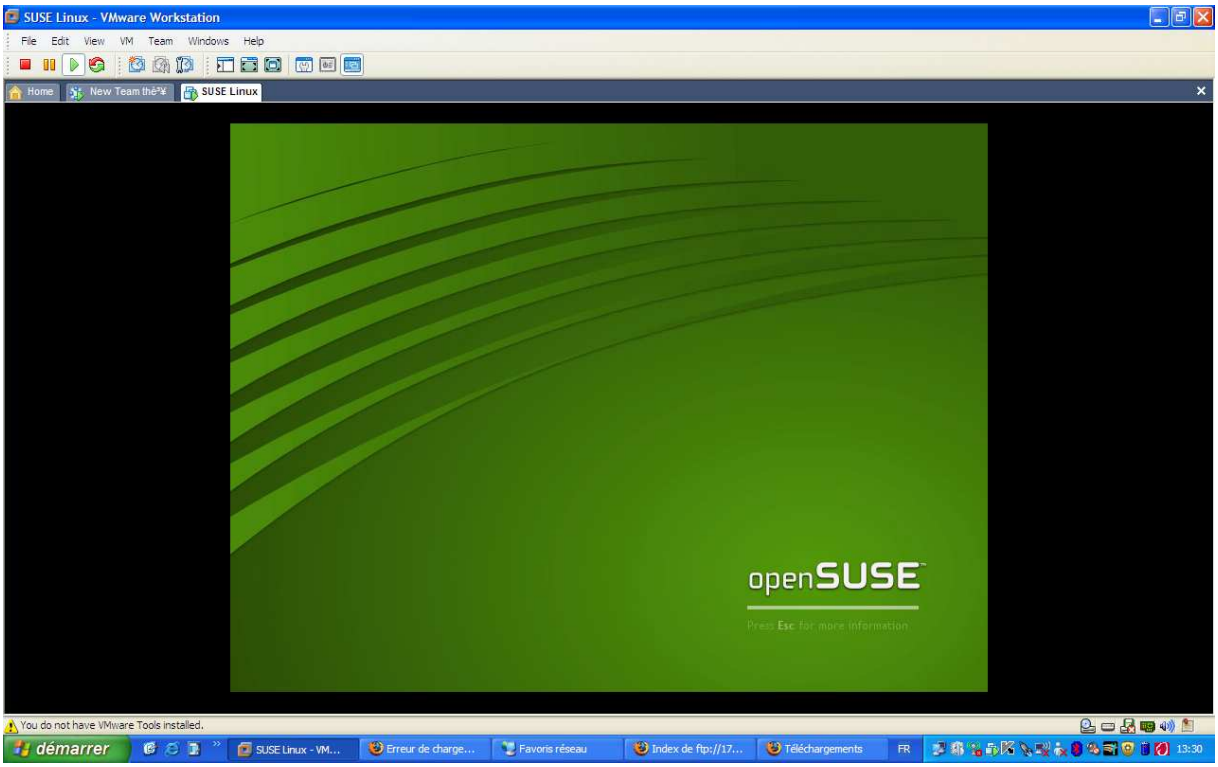

Figure 2 : lancement d'installation de Linux Fedora 8.0

Les étapes d'installation sont les suivantes :

- ✓ Lancer le démarrage de l'installation
- ✓ Cliquer ***suivant***
- ✓ Choisir la langue
- ✓ Cliquer sur suivant pour continuer l'installation
- ✓ Demande de partitionnement, on choisit partition par défaut
- ✓ Installation de packages
- ✓ Cliquer sur ***suivant***
- ✓ Configurer le firewall
- ✓ Régler la date et l'heure
- ✓ Créer un compte utilisateur, et taper le mot de passe
- ✓ Fin de l'installation.

1-Etapes d'installation du smoothwall :

Télécharger l'image ISO et la graver sur CD. Booter dessus et suivre les étapes d'installation suivantes :

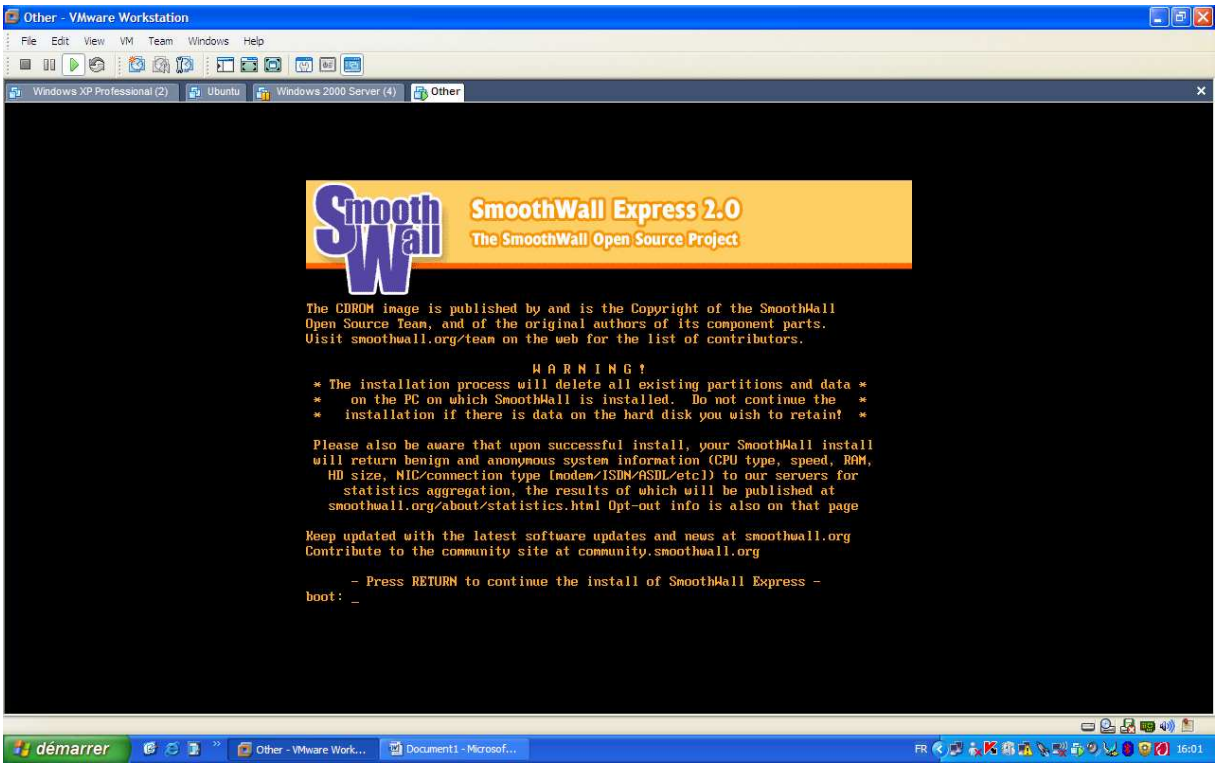

Figure 3 : lancement d'installation du smoothwall

- Choix du langage
- Fenêtre de bienvenu
- Choix du mode d'installation (CD ROM)
- Préparation du disque dur (partitions et formatage : toutes les données présentes sont effacées)
- Configuration réseau (carte verte : IP statique 192.168.0.1)
- Installation de smoothwall
- Hostname (le nom donné au firewall)
- Configuration USB ADSL
- Configuration Ethernet

Adresse MAC : nombre unique de 48bits assigné à la carte réseau par son constructeur également appelée adresse physique.

Balise html : mécanisme principal de mise en forme de page Web, les balises html précisent au navigateur ce qu'il soit faire.

Blindage : couverture entourant certains types de câbles et protègent les données transmises par les signaux parasites appelés bruit.

BNC : Britsh Control Connector, connecteur pour câble coaxial

Broadcast : consiste à envoyer une information à tous les ordinateurs du réseau

Cache : espace de stockage à accés rapide utilisé pour accélerer le transfert d'information

CSM/CD : Carrier Sense Multiple Acces/ Collision Detection, méthode d'acces multiple dans laquelle chaque station vérifie que le canal est libre avant de commencer une émission, puis écoute pendant l'émission pour détecter une éventuelle collision. Cette méthode s'utilise couramment dans les réseau locaux du type Ethernet.

En-tête de paquet : partie d'un paquet contenant les données de control.

Ethernet : type de réseau local parmi les plus utilisé, initialement dévellopé par Xerox. Il utilise la technique CSMA/CD et correspond à la norme IEEE802.3.

Hypertexte :type de navigation. Un document hypertexte est composé de texte, mais aussi d'un structure logique permettant de fairer des références (explicitement sélectionnable) à d'aures parties du document ou à d'aures documents

ICMP : Internet Control message Control, protocole d'envoi de message de test et de contrôle, permettant aux ordinateurs du réseau d'échanger des informations relatives aux erreurs et aux anomalies de fonctionnement. Il est employé par PING qui détermine si un ordinateur distant est accessible ou non.

IEEE : Institut of Electrical and Electronics Engineer, instance de normalisation internationnal situé aux états unis. Elle comporte un groupe de normalisation qui travaille dans le domaine de l'informatique.l'IEEE est essentiellement connu par ses publication de la norme IEEE 802 qui est une norme clé des réseaux locaux et qui a été repris par l'ISO

Localhost : (127.0.0.1) c'est l'adresse de la machine hors réseau

Mono : désigne le plan qui consiste à introduire la plate-forme .NET comme système libre

Norme : document établi au consensus et approuvé par un organisme de normalisation reconnu (IEEE, ISO,…)

Plug and play : fonction de Windows permettant la reconnaissance et l'installation automatique de périphérique connecté à l'ordinateur.

Port : point d'entrée et de sortie logique par lequel les services d'une machine peuvent être accessibles et réciproquement une machine peut émettre des données depuis ce port.

PPPOE : Point-to-Point Protocol Over Ethernet est un protocole d'encapsulation PPP sur Ethernet mis au point par la société RedBack

Protocole : ensemble de règles permettant à des équipements informatiques d'échanger des informations d'un type donné.

Smoothwall : un firewall logique ou qui peut être configuré avec trois cartes réseaux

Snaphot : possibilité d'enregistrer l'état d'une VM (disque et mémoire vive).

Socket : point de communication par lequel un processus donné pourra émettre et recevoir des données et le représenter par une adresse IP et un port.

VM : une machine virtuelle offre un espace virtuel qui permet l'exécution de toutes les fonctionnalités d'une machine physique.

Yast : est un outil d'installation et de configuration conçu pour la version OpenSUSE de Linux constitué d'une multitude d'outils pour paramétrer l'ordinateur. Les différents modules sont classés par catégories.

http://www.pcplaisir.eu

http://www.memoireonline.com

http://fr.wikibooks.org/wiki/acceuil

http://www.developpez.com

http://www.metz.supelec/Vialle

http://www.laissus.fr/cours/cours.html

http://www.themanualpage.org/

http://www.commentçamarche.com

http://www.guill.net

http://www.siteduzero.com

http://www.wikipedia.org/

Réseaux locaux sous Windows et linux de messieurs M.Lahdir et R.Mezari.

Réseaux, Architectures, Protocoles, Applications de Andro Tanenbaum ; InterEdition 1995

Initiation aux réseaux informatiques et à Internet de Jerom Alet