BUJUMBURA INTERNATIONAL UNIVERSITY
Excellence in Education for Development
(O.M. No. 610/136, 03 FEV. 2014)

Cours : BST- 3507 Développement Internet/ BAC 3

Nombre de crédits : 4 Crédits

Titulaire du cours : BIMENYIMANA Ildegard Christian (Master)

Téléphone mobile : 257 77 485 127

Adresse électronique : barundure@gmail.com

Ier semestre, année ou IIè semestre, année

DESCRIPTION DU COURS

Ceci est le support du cours de Développement Internet de Bujumbura International University (année 2020/2021). Le chapitre I traite des transmissions de données et des réseaux en général sous l'angle de l'architecture des systèmes ouverts (modèle OSI) en traçant les grandes lignes sur le fonctionnement du modèle TCP/IP. Le chapitre 2 traite du réseau Internet et des protocoles qui lui sont associés. Les chapitres 3 et 4 sont plus orientés vers des applications pratiques visant la mise en place de services sur les réseaux.

Objectifs du cours

❖ Objectif général

L'objectif de ce cours est d'apprendre aux étudiants le niveau avancé sur le fonctionnement du réseau informatique en apprenant la configuration et l'interconnexion des réseaux sur différents niveaux (Niveaux Liaison et Réseaux) par mode Trunk et par Protocoles de routage de paquets.

Les étudiants vont apprendre comment faire la configuration et le développement de services Intranet/Internet par la mise en place serveur DNS et le système de messagerie interne au sein d'une organisation. Ils vont découvrir encore le fonctionnement des API et apprendre à créer un API REST en PHP et Mysql. Ils vont finir par les notions sur le commerce électronique et la sécurité des informations confidentielles des clients et de l'entreprise virtuelle.

❖ Objectifs spécifiques

Les objectifs spécifiques de ce cours sont :

- Configuration et créations des VLAN ;
- Création des API;
- Création des services Intranet/internet;
- Commerce électronique et sécurité des données électronique.

METHODODOLOGIE UTILISEE

a- Les ouvrages de base

(John Wiley & Sons, Inc., 2015, Les API pour les Nuls®, Édition limitée IBM, 111 River St., États-Unis)

- John Wiley & Sons, Inc., 2015, Les API pour les Nuls®, Édition limitée IBM, 111 River St., États-Unis

- Scott Empson, 2008, CCNA Portable Command Guide, Second Edition, Indianapolis, IN 46240 USA,Cisco Press

b- Méthode d'enseignement

EXIGENCES DU COURS

a- Lectures obligatoires

- Avoir des notions sur l'adressage et la segmentation du réseau informatique ;
- Avoir le niveau débutant sur la programmation web ;
- Avoir les connaissances de base sur le système d'exploitation Linux.

b- Calendrier des évaluations

(Indiquer les périodes auxquelles les évaluations auront lieu)

- Evaluations formatives (contrôle continu, travaux dirigés, travaux pratiques) : travaux dirigés
- Examen semestriel : Devoir de table

c- Système d’évaluation

Pour les programmes de baccalauréat :

- Examen semestriel : 60%
- Evaluations formatives (contrôle continu, travaux dirigés, travaux pratiques) : 30%
- Présence au cours : 10%.

PLAN DU COURS

TABLE DES MATIERES

CHAPITRE I : MODELE TCP/IP 6

I.1. Le modèle TCP/IP et son fonctionnement 6
I.2. Signification de TCP/IP 6
1.3. Différence entre TCP et IP 8
I.4. Le rôle de TCP/IP et sa façon de fonctionnement 9
I.5. Les quatre couches du modèle TCP/IP 11
I.6.Comparaison avec le modèle OSI et critique 15
I.7. Les types de connexion au réseau 17
I.8. Les différentes technologies d'accès à internet 22

CHAPITRE 2 : Routage et protocoles de routage 28

II.1. Introduction 28
II.2.Fonctionnement 28
II.3. Internetwork Operating System 29
II.3. Processus d'amorçage CISCO 29
II.4.Ports de gestion 30
II.5. Interfaces du Routeur 30
II.6. Configuration de Base 31
II.7. Table de routage 32
II.8. Réseaux directement connectés 32
II.9. Réseaux distants 33
II.10. Analogie 33
II.11. Routage Statique 34
II.12.Routage dynamique 35
II.13. Principes d'une table de routage 35
II.14. Meilleur chemin 36
II.15. Protocoles IGP et EGP 36

CHAPITRE III : LE COMMERCE ELECTRONIQUE ET SECURITE.....37

III.1. Introduction 37
III.2. Les petites entreprises devraient se tourner vers le commerce électronique 38
III.3. Les avantages des Solutions de commerce électronique 38
III.4. Mise sur pied d'un magasin virtuel 39
III.5. Les nom de domaines sécurisés 43
III.6. Options relatives au traitement des paiements 44

III.7. Sécurité et protection des renseignements personnels 49
CHAPITRE IV : LES API 53
IV.1. Introduction 53
IV.2. Définition d'un API 54
IV.3. Des API à l'économie des API 54
IV.4. Quatre catégories d'API 56
IV.5. Savoir en quoi consiste la gestion d'une API 57
IV.6. Concepteur d'API 59
IV.7. CONCLUSION 60
IV.8.References 60

CHAPITRE I : MODELE TCP/IP

I.1. Le modèle TCP/IP et son fonctionnement

Tout comme pour les individus, il est important que les ordinateurs aient un moyen commun de communiquer entre eux. De nos jours, la plupart d'entre eux le font à travers TCP/IP. TCP/IP est généralement intégré aux ordinateurs et est largement automatisé, mais il peut être utile d'en comprendre le modèle, en particulier lorsque vous configurez un ordinateur pour vous connecter à d'autres systèmes.

I.2. Signification de TCP/IP

TCP/IP signifie Transmission Control Protocol/Internet Protocol (Protocol de contrôle des transmissions/Protocole Internet).

TCP/IP est un ensemble de règles normalisées permettant aux ordinateurs de communiquer sur un réseau tel qu'Internet.

En fonctionnement autonome, un ordinateur individuel peut effectuer un nombre illimité de tâches, mais la véritable force des ordinateurs se révèle quand ils communiquent entre eux. Bien des tâches que nous réalisons en les utilisant, que ce soit envoyer des e-mails, regarder Netflix (films sur internet) ou trouver son chemin, impliquent une communication entre les ordinateurs. Ils peuvent appartenir à différentes sociétés ou être situés dans différentes parties du monde, et les individus ou les logiciels qui les utilisent peuvent parler des langues différentes ou être codés dans des langages de programmation divers.
Les interactions peuvent se produire entre deux ordinateurs ou impliquer des centaines de systèmes, mais, tout comme lors de l'acheminement d'un courrier ou d'un colis, chaque transaction se produit entre deux ordinateurs à la fois. Pour la réaliser, les deux ordinateurs doivent savoir à l'avance comment communiquer.

- Comment démarrent-ils la conversation ?
- À qui est-ce le tour de communiquer ?
- Comment chaque ordinateur soit-il que son message a été correctement transmis ?
- Comment les ordinateurs terminent-ils une conversation ?

Les ordinateurs réalisent tout cela grâce à des protocoles. Un protocole est un ensemble convenu de règles. En termes humains, nous utilisons des protocoles sociaux pour savoir

comment nous comporter et communiquer avec les autres. Les technologies ont leurs propres façons de définir des règles de communication.

C'est la même chose avec les ordinateurs mais avec des règles plus strictes. Lorsque les ordinateurs utilisent tous le même protocole, les informations peuvent être transmises. Quand ils ne le font pas, c'est le chaos.

La communication était plus compliquée lorsqu'on a commencé à échanger des informations entre ordinateurs. Chaque fabricant avait sa propre façon de faire communiquer ses ordinateurs, mais aucune ne leur permettait de communiquer avec les ordinateurs des autres fabricants. Il est rapidement devenu évident qu'une norme commune était nécessaire pour permettre aux ordinateurs de tous les fabricants de communiquer entre eux. Et cette norme est **TCP/IP**.

1.3. Différence entre TCP et IP

TCP et **IP** sont deux protocoles de réseau informatique distincts.
IP est la partie qui obtient l'adresse à laquelle les données sont envoyées. **TCP** est responsable de la livraison des données une fois que cette adresse IP a été trouvée.

Il est possible de les séparer, mais il ne sert à rien de différencier TCP et IP. Parce qu'ils sont souvent utilisés ensemble, «TCP/IP» et le «modèle TCP/IP» sont désormais des termes reconnus.

Voyez cela de la manière suivante : l'adresse IP est similaire au numéro de téléphone attribué à votre smartphone. TCP est toute la technologie faisant sonner le téléphone et vous permettant de parler à un interlocuteur sur un autre téléphone. Ils sont différents l'un de l'autre, mais ils sont également dénués de sens l'un sans l'autre.

I.4. Le rôle de TCP/IP et sa façon de fonctionnement

TCP/IP a été développé par le département américain de la Défense pour spécifier la méthode de transfert de données d'un appareil à un autre. TCP/IP met notamment l'accent sur la précision et il comporte plusieurs étapes pour garantir que les données sont correctement transmises entre les deux ordinateurs.

Voici un moyen qu'il utilise pour le faire. Si le système devait envoyer le message entier en un seul morceau et s'il devait rencontrer un problème, le message entier devrait être renvoyé. Au lieu de cela, TCP/IP décompose chaque message en paquets, et ces paquets sont ensuite réassemblés à l'autre extrémité. En fait, chaque paquet peut emprunter un itinéraire différent vers l'autre ordinateur, si le premier itinéraire n'est pas disponible ou s'il est encombré.

De plus, TCP/IP divise les différentes tâches de communication en couches. Chaque couche remplit une fonction différente. Les données passent par quatre couches individuelles avant d'être reçues à l'autre extrémité. TCP/IP parcourt ensuite ces couches

dans l'ordre inverse pour reconstituer les données et les présenter au destinataire.

Le but des couches est de garder l'ensemble standardisé, sans que de nombreux fournisseurs de matériel et de logiciels aient à gérer eux-mêmes les communications. C'est comme conduire une voiture : tous les fabricants s'accordent sur l'emplacement des pédales, ce qui représente un élément sur lequel nous pouvons compter entre les voitures. Cela signifie également que certaines couches peuvent être mises à jour, par exemple pour améliorer les performances ou la sécurité, sans avoir à mettre l'ensemble à niveau.

Figure I.1 : Partage de données entre deux ordinateurs

I.5. Les quatre couches du modèle TCP/IP

TCP/IP est un protocole de liaison de données utilisé sur Internet. Son modèle est divisé en quatre couches distinctes. Utilisées ensemble, elles peuvent également être appelées une suite de protocoles.

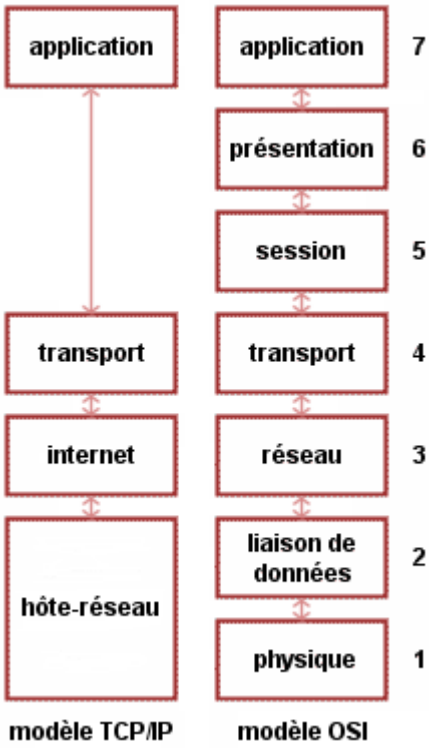


Figure I.2 : TCP/IP, un modèle en 4 couches

Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.

I.5.1. La couche hôte réseau

Cette couche est assez «étrange». En effet, elle semble «regrouper» les couches physiques et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée; la seule

contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet; Ethernet est une implémentation de la couche hôte-réseau.

I.5.2. La couche internet

Cette couche est la clé de berceau de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

I.5.3. La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charger la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

I.5.4. La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

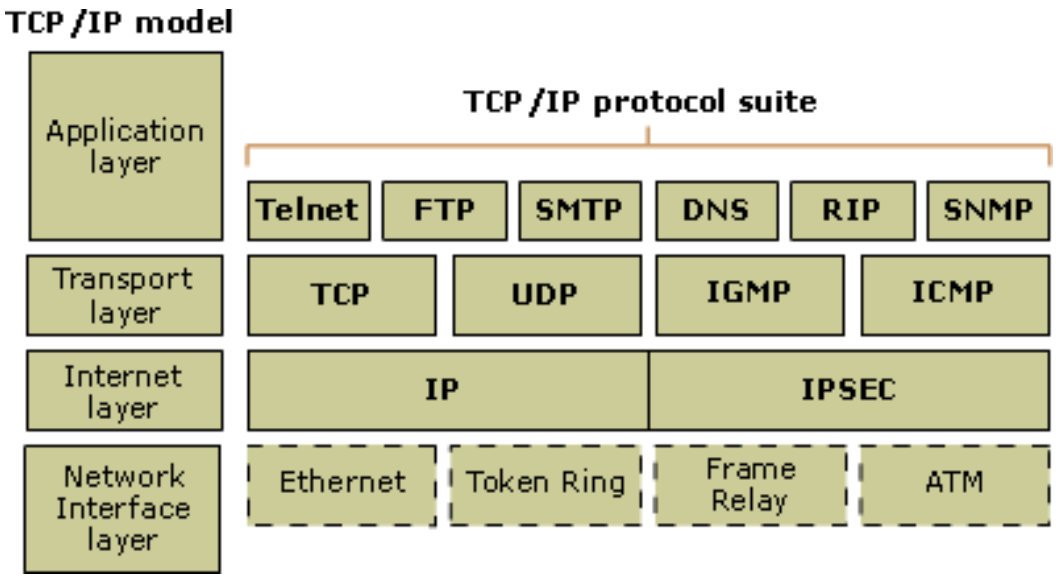


Figure I.3 : Modèle TCP/IP en détail

I.6.Comparaison avec le modèle OSI et critique

I.6.1.Comparaison avec le modèle OSI

Tout d'abord, les points communs. Les modèles OSI et TCP/IP sont tous les deux fondés sur le concept de pile de protocoles indépendants. Ensuite, les fonctionnalités des couches sont globalement les mêmes.

Au niveau des différences, on peut remarquer la chose suivante : le modèle OSI faisait clairement la différence entre 3 concepts principaux, alors que ce n'est plus tout à fait le cas pour le modèle TCP/IP. Ces 3 concepts sont les concepts de services, interfaces et protocoles. En effet, TCP/IP fait peu la distinction entre ces concepts, et ce malgré les efforts des concepteurs pour se rapprocher de l'OSI. Cela est dû au fait que pour le modèle TCP/IP, ce sont les protocoles qui sont d'abord apparus. Le

modèle ne fait finalement que donner une justification théorique aux protocoles, sans les rendre véritablement indépendants les uns des autres.

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

I.6.2. Critique du modèle TCP/IP

Une des premières critiques que l'on peut émettre tient au fait que le modèle TCP/IP ne fait pas vraiment la distinction entre les spécifications et l'implémentation : IP est un protocole qui fait partie intégrante des spécifications du modèle.

Une autre critique peut être émise à l'encontre de la couche hôte réseau. En effet, ce n'est pas à proprement parler une couche d'abstraction dans la mesure où sa spécification est trop floue. Les constructeurs sont donc obligés de proposer leurs solutions

pour « combler » ce manque. Finalement, on s'aperçoit que les couches physiques et liaison de données sont tout aussi importantes que la couche transport. Partant de là, on est en droit de proposer un modèle hybride à 5 couches, rassemblant les points forts des modèles OSI et TCP/IP :

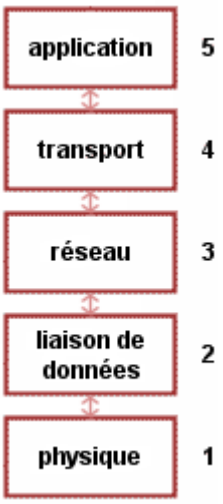


Figure I.4 : Modèle hybride de référence

C'est finalement ce modèle qui sert véritablement de référence dans le monde de l'Internet. On a ainsi gardé la plupart des couches de l'OSI (toutes, sauf les couches session et présentation) car correctement spécifiées. En revanche, ses protocoles n'ont pas eu de succès et on a du coup gardé ceux de TCP/IP.

I.7. Les types de connexion au réseau

I.7.1. Présentation

Lorsqu'on virtualise des serveurs par l'intermédiaire des machines virtuelles, on les connecte au réseau par l'intermédiaire

d'un hyperviseur de niveau 1 et de niveau 2 avec des produits comme VMware Player, VMware Workstation, VMware ESXi, Microsoft Hyper-V, Proxmox, ou encore Oracle Virtualbox.

En termes de connexion au réseau, on trouve plusieurs types de connexion au réseau, je dirais même que plusieurs méthodes sont disponibles pour se connecter au réseau de différentes manières.
Parmi ces types de connexion au réseau, on trouve :

- Bridge ;
- NAT ;
- Host-Only ;
- LAN Segment.

Maitriser cela est essentiel pour commencer dans la virtualisation et être capable de s'adapter selon la configuration et l'architecture qu'on souhaite obtenir. C'est pour cela que nous allons voir, à quoi correspondent ces types de connexion, à quoi servent-ils, comment fonctionnent-ils et quand les utiliser.

I.7.2. Le type Bridge

Ce mode est surement le plus utilisé puisqu'il permet de connecter une machine virtuelle directement sur le réseau physique sur lequel est branchée la carte réseau physique de l'hôte.

Pour cela, un bridge c'est-à-dire un pont est créé entre la carte réseau virtuelle de l'application de virtualisation et la carte réseau de votre hôte physique. C'est en quelque sorte un partage de carte réseau, où le système d'exploitation de votre hôte physique partage sa carte physique avec le système d'exploitation de votre ou vos machines virtuelles.

Si votre hôte physique dispose de plusieurs cartes réseaux, vous pouvez choisir de créer un pont avec celle que vous souhaitez, ce qui permet une flexibilité dans la configuration et dans la gestion de la connexion réseau.

Vu que la machine virtuelle se retrouvera connectée sur le même réseau que la machine physique, il lui faudra une configuration TCP/IP identique aux autres postes du réseau afin qu'elle puisse communiquer avec le reste du réseau et sortir du réseau.

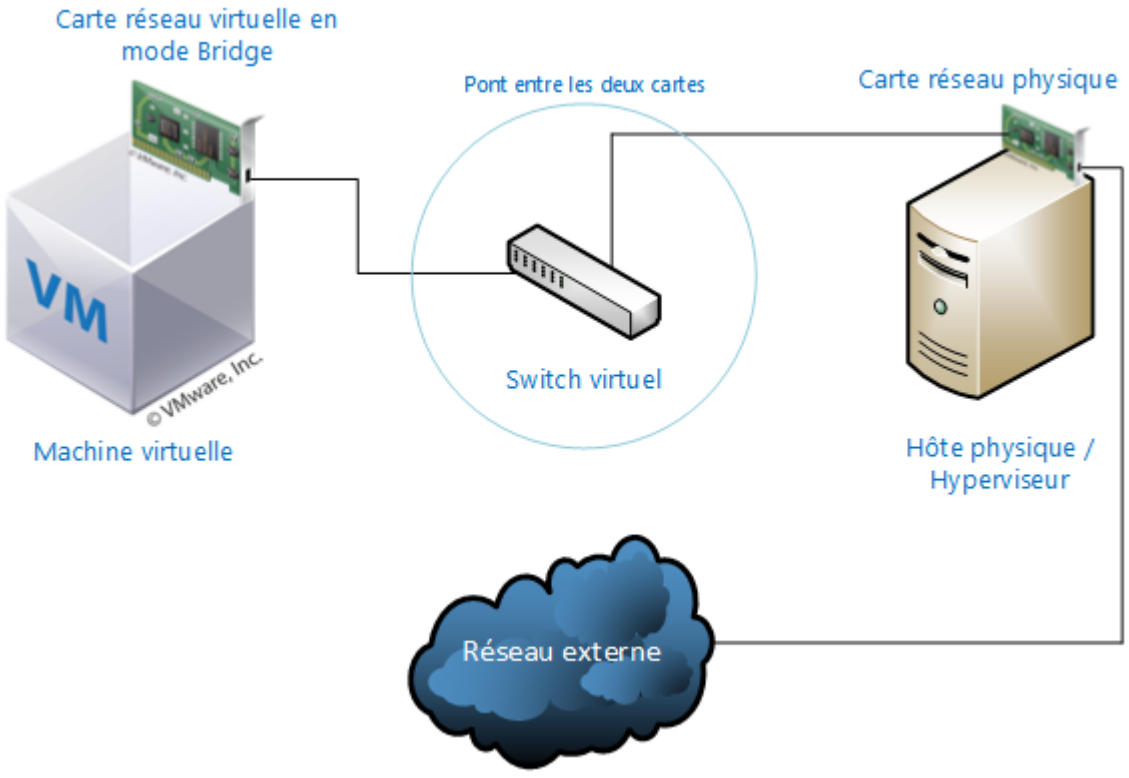


Figure I.5. Connexion au réseau par Bridge

I.7.3. Le type NAT

Ce type de connexion reprend tout simplement le principe d'une passerelle NAT, à savoir masquer l'adresse IP des clients qui lui sont connectés pour sortir sur le réseau.

Ce mode est intéressant puisqu'il permet à votre machine virtuelle d'accéder à votre réseau de façon totalement transparente puisque c'est l'adresse IP de la machine physique qui est utilisée grâce à la translation d'adresse du processus NAT.

En fait, lorsque vous sélectionnez ce mode, la machine virtuelle utilise une adresse IP distribuée par l'application de virtualisation via un serveur DHCP, puis elle utilisera votre hôte physique comme passerelle pour sortir du réseau. Comme la fonctionnalité de NAT est appliquée, vous accédez au réseau sans être visible.

Notamment, cela peut être intéressant s'il y a de la sécurité appliquée sur un port d'accès d'une salle où on autorise une seule adresse MAC définie à se connecter, puisque vous utiliserez la connexion de l'hôte physique vous ne serez pas détecté comme intrus et pourrez utiliser la liaison avec votre machine virtuelle.

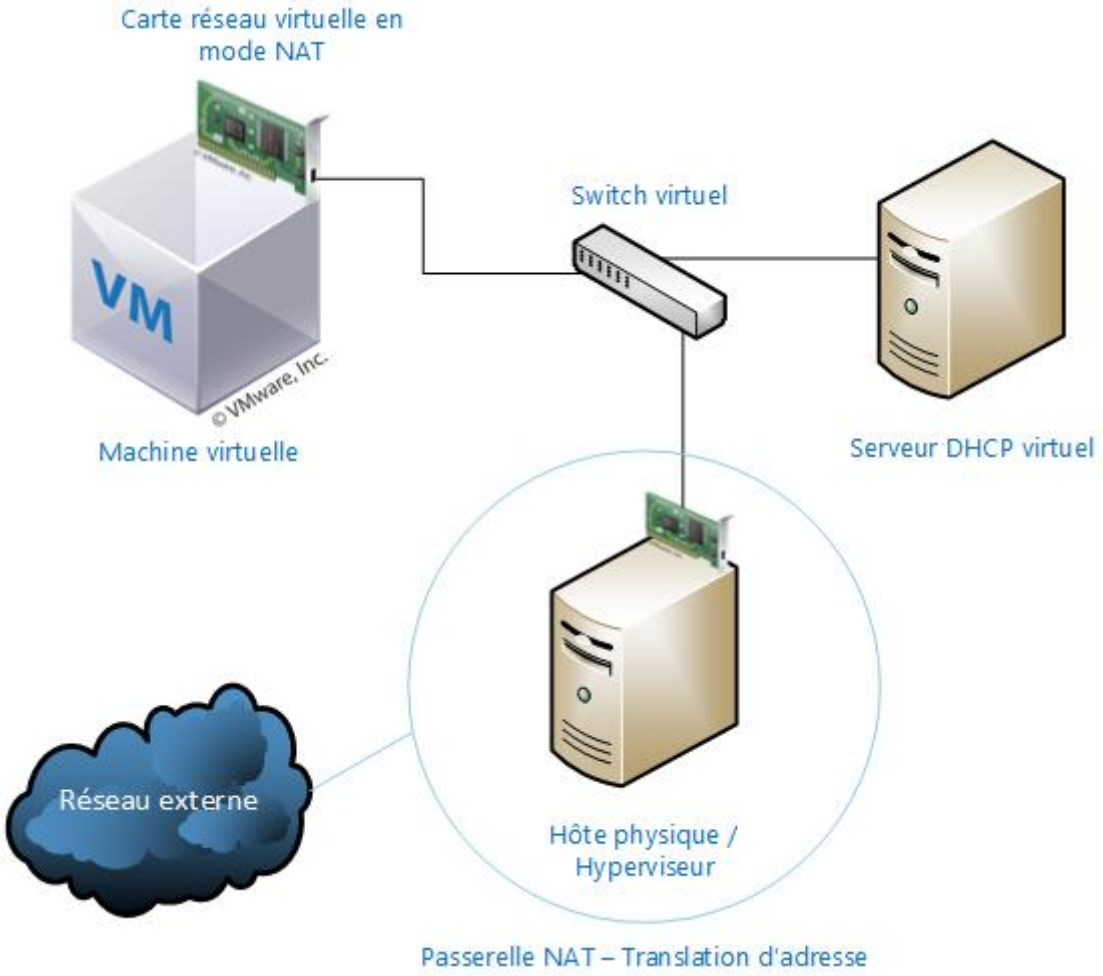


Figure I.6. Connexion au réseau par NAT

I.7.4. Le type Host-Only

Ce type de connexion ne permet pas de sortir vers un réseau extérieur, ni d'accéder au réseau local par l'intermédiaire de la carte réseau physique de la machine physique hôte.

Comme son nom l'indique, ce mode permet uniquement d'établir une connexion entre la machine virtuelle et la machine physique. Cela par l'intermédiaire de l'adaptateur virtuel de la machine virtuelle et l'adaptateur virtuel de la machine physique qui

obtiendront des adresses IP via le serveur DHCP virtuel de l'hyperviseur.

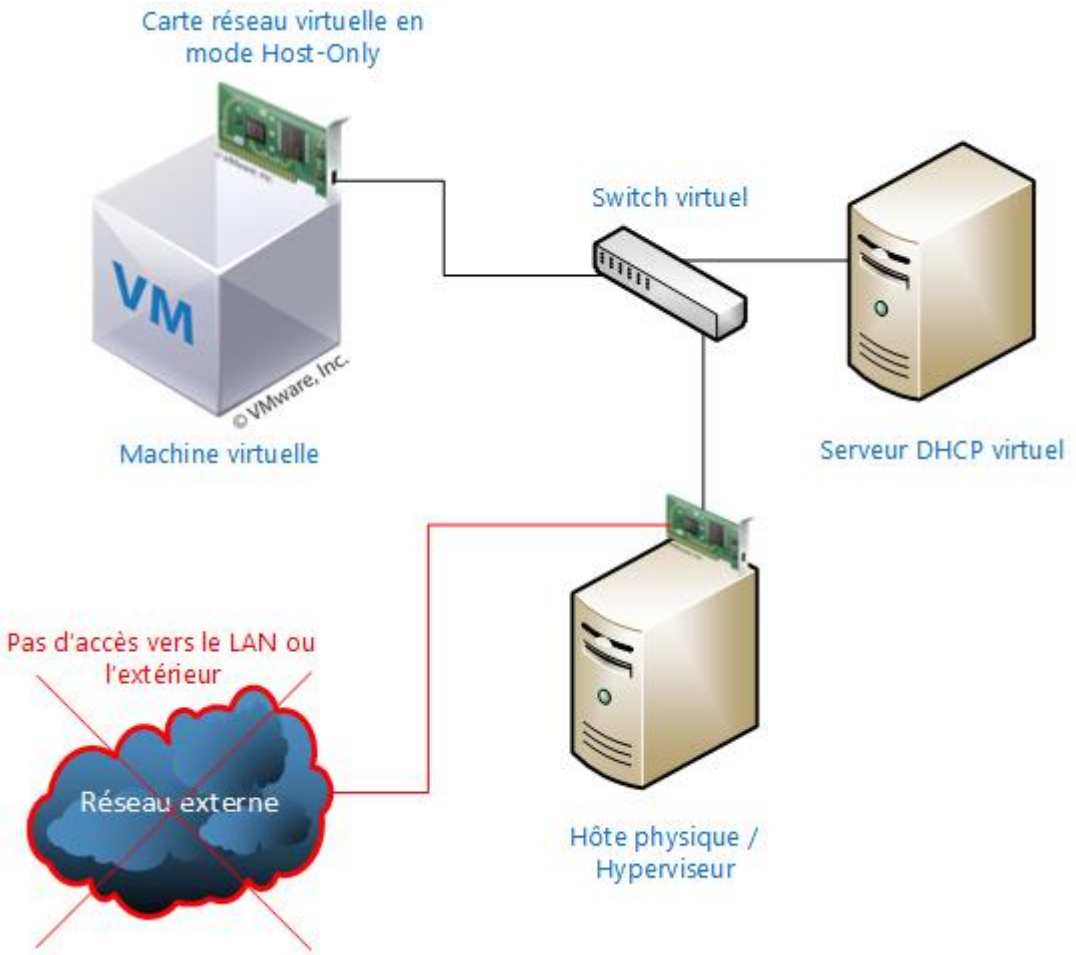


Figure I.7. Connexion au réseau par Host

I.8. Les différentes technologies d'accès à internet

I.8.1. Connexions filaires

I.8.1.1. L'ADSL

L'acronyme ADSL renvoie à «Asymetric Digital Sub-scriber Line» et désigne la liaison numérique sur la ligne de l'abonné téléphonique. Technologie de connexion de loin la plus répandue en France, l'ADSL utilise comme support le fil téléphonique

classique en cuivre pour y transporter des données qui sont numérisées et dont le débit descendant (internet vers internaute) est plus important que le débit montant. L'asymétrie permet de mieux répondre aux usages courants d'internet, qui consistent majoritairement dans la récupération plutôt que la publication de contenus.

La possibilité d'avoir en même temps une conversation téléphonique et une connexion internet haut débit sur une même ligne téléphonique est rendue possible par l'utilisation de bandes de fréquence différentes, séparées chez l'abonné ainsi qu'au central téléphonique par des filtres spéciaux.

Chez l'abonné, ce filtre est généralement un petit boitier gigogne venant s'intercaler entre la prise téléphonique murale et celle du téléphone. A l'origine en France l'ensemble des infrastructures permettant la téléphonie et l'accès internet étaient gérées par l'opérateur historique, qui les sous-louait à d'autres FAI. Rapidement est arrivé le dégroupage dit «partiel», où la téléphonie classique reste gérée par l'opérateur historique alors que les FAI peuvent utiliser une partie des centraux téléphoniques pour y installer leurs propres équipements de raccordement à internet.

Le dégroupage «total», essentiellement disponible en zone urbaine, permet quant à lui de s'affranchir totalement de l'opérateur historique et de ne plus lui payer d'abonnement. L'opérateur alternatif est alors responsable de l'ensemble de la ligne. Dans ce cas, du moins en France, les opérateurs ne proposent plus de

téléphonie classique et se limitent aux offres de téléphonie en ligne dites en Voip (Voice over Internet Protocol), offres couplées à celle de la télévision et d'internet. Des équipements de téléphonie classique dont ils devraient faire l'investissement feraient, en effet, double emploi avec la Voip. Le débit est souvent plus rapide en dégroupage total du fait de l'absence de filtres chez l'opérateur et chez l'abonné, ces derniers pouvant perturber le signal.

I.8.1.2. GLOSSAIRE

FAI: Fournisseur d'Accès Internet. Il s'agit généralement d'une société auprès de laquelle on souscrit un abonnement internet mais le FAI peut aussi être une association, voire un particulier.
Voip: La Voip, pour «Voice on IP», est une technologie permettant de se servir des réseaux IP (Internet Protocol) comme moyen de transmission des communications vocales.

I.8.2. Le Réseau Téléphonique Commuté (RTC)

Le Réseau Téléphonique Commuté que nous utilisons depuis toujours (ou presque…) pour nos conversations téléphoniques. Ces dernières y sont transmises par des signaux dits «analogiques», c'est-à-dire que l'on peut représenter par une grandeur physique. Dans les débuts de l'accès à internet pour le grand public un modulateur-démodulateur, ou modem, installé généralement dans l'ordinateur de l'internaute, opérait la conversion entre les modes analogique et numérique de réception ou d'envoi des données.

Cette technologie offre toutefois des débits très faibles, dont le maximum théorique est de 56 Kbit/s. De plus, contrairement à l'ADSL, la ligne téléphonique reste occupée et il est donc impossible de téléphoner tant que l'on est sur internet.

I.8.3. Le Câble

Présent seulement dans les agglomérations, le câble est une technologie originellement conçue pour faire transiter de l'information uniquement depuis le centre de transmission vers les abonnés. Elle était donc essentiellement dédiée à la distribution des flux télévisuels. Au fil du temps, de multiples adaptations ont permis d'augmenter la capacité montante du réseau, et donc notamment vers internet, ce qui a amené au développement d'une réelle offre haut débit.

I.8.4. La fibre optique

La fibre optique est constituée d'un fil en verre ou en plastique ayant la propriété de conduire la lumière. Elle offre un débit de transfert de données nettement supérieur à celui des câbles coaxiaux et peut donc être utilisée tout à la fois pour les liaisons téléphoniques, télévisuelles ou informatiques.
en cours de déploiement dans les grandes villes en France pour les particuliers, la fibre optique est en réalité utilisée depuis longtemps sur les «dorsales» des réseaux pour les transmissions de données sur de longues distances, y compris pour internet.

I.8.5. Connexions par ondes radio

I.8.5.1. LA 3G

Il s'agit de la 3ème génération de téléphones portables. La deuxième génération, née au début des années 1990, était basée sur le réseau GSM (Global System for Mobile communication).

La 3G est, quant à elle, basée sur l'uMTS (universal Mobile Telecommunications Systems). Entièrement différente et nécessitant de nouveaux réseaux d'antennes, la technologie 3G est essentiellement dévolue à la mobilité pour internet, soit sur un téléphone, soit sur un ordinateur au moyen d'une clé uSb 3G ou d'un modem 3G intégré.

Ce mode de connexion alternatif a, bien sûr, pour principal avantage de permettre de surfer en mobilité et en haut débit dans tout le territoire national.

I.8.5.2. Le WIMAx

Le wimax (pour Worldwide Interoperability for Microwave Access) est une technologie de transmission sans fil à haut débit et à large portée (70 Mbit/s sur une distance de 50 km, en théorie). Il se présente donc comme un relais dans les zones mal équipées pour les connexions internet en haut débit.

En ville, s'il se développe, il devrait également permettre la mise en place de réseaux à partir d'un unique point d'accès sur un large périmètre, contrairement à la multiplicité des points d'accès

actuels en Wi-Fi. Seule la « boucle locale », la connexion des particuliers au réseau, devra se faire en Wi-Fi. Fonctionnant en effet sur des bandes de fréquence bien plus élevées que celles du Wi-Fi, le wimax ne peut pas franchir les murs.

I.8.5.3. Le WI-FI

Certaines zones rurales non couvertes par l'ADSL le sont en Wi-Fi, généralement par de petits opérateurs locaux et pour desservir une zone de quelques kilomètres carrés. Ces réseaux utilisent des points de collecte en haut débit, puis une série d'émetteurs/ récepteurs jusqu'aux équipements des usagers.

I.8.5.4. Le SATELLITE

Longtemps présentée comme une alternative à l'ADSL pour les lieux isolés grâce à un débit descendant nettement plus intéressant que le RTC, cette technologie présente toutefois des temps de latence importants pour le débit montant de l'internaute vers le satellite. Les applications en temps réel telles que la téléphonie, la visioconférence ou les jeux en ligne ne peuvent donc pratiquement pas être utilisées.

I.8.5.5. Le CPL

La technologie des Courants Porteurs en Ligne permet de se connecter à internet en s'appuyant le réseau électrique existant. Elle peut être utilisée pour créer un réseau local dans un

bâtiment ou pour la réalisation d'un réseau de desserte haut débit. Dans la pratique, cette technologie est surtout fonctionnelle pour les réseaux locaux des particuliers, les dessertes plus larges en CPL impliquant de nombreuses contraintes et des coûts élevés.

CHAPITRE 2 : Routage et protocoles de routage

II.1. Introduction

Un routeur est un ordinateur comme un autre.
Il possède de nombreux composants matériels et logiciels communs avec d'autres ordinateurs :

- Processeur ;
- RAM ;
- ROM ;
- Système d'exploitation.

II.2.Fonctionnement

La fonction principale d'un routeur consiste à diriger les paquets destinés à des réseaux locaux et distants en :

- déterminant le meilleur chemin pour l'envoi des paquets ;
- transférant les paquets vers leur destination.

Pour cela, le routeur utilise sa table de routage pour déterminer le meilleur chemin pour le transfert du paquet. Lorsque le routeur reçoit un paquet, il examine son adresse IP de destination et recherche, dans la table de routage, l'adresse réseau qui lui correspond le mieux.

La table de routage contient également l'interface à utiliser pour le transfert du paquet. Une fois une correspondance trouvée, le routeur encapsule le paquet IP dans la trame de liaison de données de l'interface sortante ou de sortie, et le paquet est alors transféré vers sa destination.

II.3. Internetwork Operating System

Le logiciel du système d'exploitation utilisé dans les routeurs Cisco est appelé Cisco Internetwork Operating System (IOS). Comme tout système d'exploitation d'ordinateur, Cisco IOS gère les ressources matérielles et logicielles du routeur, notamment l'allocation de mémoire, les processus, la sécurité et les systèmes de fichiers. Cisco IOS est un système d'exploitation multitâche intégré aux fonctions de routage, de commutation, d'interconnexion et de télécommunications.

II.3. Processus d'amorçage CISCO

Le processus d'amorçage démarrage comporte quatre phases principales :

1. Test automatique de mise sous tension (POST)
2. Chargement du programme d'amorçage
3. Localisation et chargement du logiciel Cisco IOS
4. Localisation et chargement du fichier de configuration initiale ou passage en mode configuration

II.4.Ports de gestion

Pour pouvoir être gérés, les routeurs sont dotés de connecteurs physiques. Ces connecteurs sont appelés ports de gestion. Contrairement aux interfaces Ethernet et série, les ports de gestion ne sont pas utilisés pour le transfert de paquets. Le port de gestion le plus courant est le port de console. Le port de console est utilisé pour connecter un terminal ou, plus fréquemment, un PC exécutant un logiciel émulateur de terminal, afin de configurer le routeur sans qu'il soit nécessaire d'accéder au réseau. Le port de console doit être utilisé pendant la configuration initiale du routeur.

Le port auxiliaire est un autre port de gestion. Les routeurs ne possèdent pas tous un port auxiliaire. Parfois, le port auxiliaire peut être utilisé de façon similaire au port de console. Il peut également permettre de relier un modem.

II.5. Interfaces du Routeur

Sur les routeurs Cisco, le terme interface désigne un connecteur physique sur le routeur dont le rôle principal est de recevoir et de transférer des paquets. Les routeurs ont plusieurs interfaces, utilisées pour se connecter à plusieurs réseaux. Généralement, les interfaces se connectent à différents types de réseaux, ce qui veut dire que différents types de supports et de connecteurs sont nécessaires. Ainsi, un routeur nécessite souvent différents types d'interfaces. Par exemple, un routeur possède généralement des

interfaces **FastEthernet** pour les connexions aux différents réseaux locaux, et divers types d'interfaces WAN pour connecter diverses **liaisons série** comme T1, DSL et RNIS.

À l'instar des interfaces d'un PC, les ports et interfaces d'un routeur se situent à l'extérieur de celui-ci. Cela permet un branchement plus pratique des câbles réseau et des connecteurs adéquats.

Chaque interface du routeur appartient à un réseau IP différent ou en est un hôte. Chaque interface doit être configurée avec l'adresse IP et le masque de sous-réseau d'un réseau différent. Avec Cisco IOS, deux interfaces actives du même routeur ne peuvent pas appartenir au même réseau.

II.6. Configuration de Base

Lors de la configuration d'un routeur, certaines tâches de base sont effectuées :

- Attribution d'un nom au routeur ;
- Définition de mots de passe ;
- Configuration d'interfaces ;

- Configuration d'une bannière ;
- Enregistrement des modifications apportées à un routeur ;
- Vérification de la configuration de base et des opérations de routage.

II.7. Table de routage

Une table de routage est un fichier de données dans la mémoire vive servant à stocker les informations sur la route à emprunter sur les réseaux directement connectés et les réseaux distants.

La table de routage contient des associations réseau/tronçon suivant. Celles-ci informent un routeur qu'une destination donnée peut être atteinte de manière optimale en envoyant le paquet à un routeur donné, lequel représente le « tronçon suivant » sur le chemin menant à la destination finale. L'association de tronçon suivant peut également être constituée de l'interface de sortie vers la destination finale.

L'association réseau/interface de sortie peut également représenter l'adresse réseau de destination du paquet IP. Cette association se produit sur les réseaux directement connectés au routeur.

II.8. Réseaux directement connectés

Lorsqu'une interface de routeur est configurée avec une adresse IP et un masque de sous-réseau, l'interface devient un hôte sur ce

réseau connecté. L'adresse réseau et le masque de sous-réseau de l'interface, ainsi que le type et le numéro de l'interface, sont entrés dans la table de routage en tant que réseau directement connecté.

II.9. Réseaux distants

Un réseau distant n'est pas directement connecté au routeur. En d'autres termes, un réseau distant est un réseau qui peut être atteint uniquement en envoyant le paquet à un autre routeur. Les réseaux distants sont ajoutés à la table de routage grâce à un protocole de routage dynamique ou grâce à la configuration de routes statiques.

Les routes dynamiques, qui mènent à des réseaux distants, sont apprises automatiquement par le routeur et utilisent un protocole de routage dynamique. Les routes statiques mènent à des réseaux configurés manuellement par l'administrateur réseau.

II.10. Analogie

- **Routes directement connectées**: pour rendre visite à un voisin, il vous suffit de descendre la rue dans laquelle vous habitez déjà. Ce chemin est similaire à une route directement connectée car la «destination» est directement disponible via votre «interface connectée», la rue.

- **Routes statiques**: pour une route donnée, un train utilise toujours la même voie ferrée. Ce chemin est similaire à une route statique car la voie menant à la destination est toujours la même.

- **Routes dynamiques** : Lorsque vous conduisez une voiture, vous pouvez «dynamiquement» choisir une route différente, en fonction du trafic, des conditions météorologiques ou autres. Ce chemin est similaire à une route dynamique car, tout au long du trajet, vous pouvez choisir, à différents moments, de prendre une autre route.

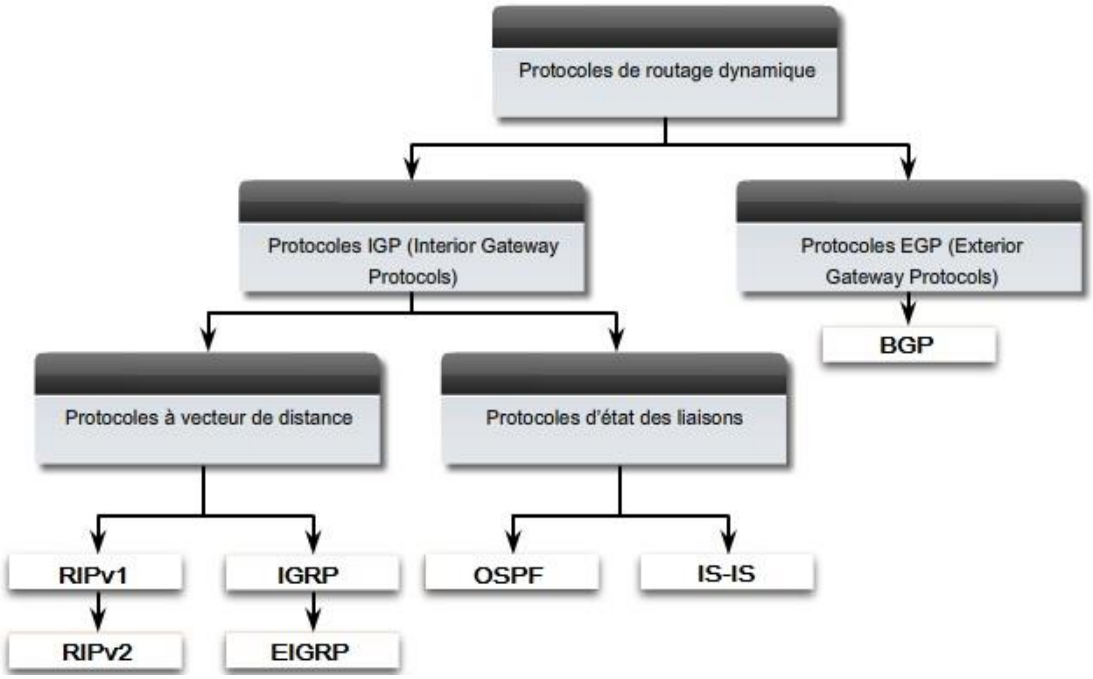
II.11. Routage Statique

Les réseaux distants sont ajoutés à la table de routage grâce à la configuration de routes statiques ou à l'activation d'un protocole de routage dynamique. Lorsque l'IOS doit atteindre un réseau distant et qu'il est informé de l'interface à utiliser, il ajoute cette route à la table de routage tant que l'interface de sortie est activée.

Une route statique inclut l'adresse réseau et le masque de sous-réseau du réseau distant, ainsi que l'adresse IP du routeur du tronçon suivant ou de l'interface de sortie. Les routes statiques sont indiquées par le code S dans la table de routage, comme illustré dans la figure. Elles sont abordées en détail au chapitre suivant.

II.12.Routage dynamique

Les protocoles de routage dynamique sont utilisés par les routeurs pour partager des informations sur l'accessibilité et l'état des réseaux distants. Les protocoles de routage dynamique effectuent plusieurs tâches, notamment :
la détection de réseaux ;
la mise à jour des tables de routage.



II.13. Principes d'une table de routage

1. Chaque routeur prend sa décision seul, en se basant sur les informations disponibles dans sa table de routage.
2. Le fait qu'un routeur ait certaines informations dans sa table de routage ne veut pas dire que les autres routeurs disposent des mêmes informations.

3. Les informations de routage liées à un chemin menant d'un réseau à un autre ne fournissent pas d'informations de routage sur le chemin inverse ou de retour.

II.14. Meilleur chemin

La détermination du meilleur chemin d'un routeur implique d'évaluer plusieurs chemins menant au même réseau de destination et de choisir le chemin optimal ou «le plus court» pour atteindre ce réseau.

Lorsqu'il existe plusieurs chemins menant au même réseau, chaque chemin utilise une interface de sortie différente sur le routeur pour atteindre ce réseau. Le meilleur chemin est sélectionné par un protocole de routage, qui utilise une valeur ou une mesure pour déterminer la distance à parcourir pour atteindre un réseau.

- le protocole **RIP**, se basent sur le nombre de sauts simples, qui représente le nombre de routeurs entre un routeur et le réseau de destination.
- le protocole **OSPF**, déterminent le chemin le plus court en examinant la bande passante des liaisons et en utilisant celles dont la bande passante est la meilleure.

II.15. Protocoles IGP et EGP

Un système autonome (SA), également appelé domaine de routage, est un ensemble de routeurs dont l'administration est

commune. Exemple: Le réseau interne d'une société, le réseau d'un fournisseur de services Internet. Dans la mesure où Internet repose sur le concept de système autonome, deux types de protocoles de routage sont nécessaires : des protocoles de routage intérieurs et extérieurs. Ces protocoles sont les suivants :

- Les protocoles IGP (Interior Gateway Protocols) sont utilisés pour le routage interne du système autonome.
- Les protocoles EGP (Exterior Gateway Protocols) sont utilisés pour le routage entre systèmes autonomes.

CHAPITRE III : LE COMMERCE ELECTRONIQUE ET SECURITE

III.1. Introduction

Le commerce électronique s'entend du processus d'achat ou de vente de produits ou de services sur Internet. Le magasinage en ligne gagne de plus en plus en popularité en raison de la rapidité et de la facilité d'utilisation qu'il offre aux clients. Les activités de commerce électronique, telles que la vente en ligne, peuvent viser les consommateurs ou d'autres entreprises.

Le commerce électronique de détail (ou commerce électronique **B2C** – sigle de **Business to Consumer**) désigne la vente en ligne de biens et de services, de même que la présentation directe de renseignements aux consommateurs. Le commerce électronique

interentreprises (ou commerce électronique **B2B** –sigle de **Business to Business**) se rapporte à la vente en ligne de produits, de services ou de renseignements d'une entreprise à une autre

III.2. Les petites entreprises devraient se tourner vers le commerce électronique

La vente en ligne peut aider votre entreprise à pénétrer de nouveaux marchés et à accroître vos ventes et vos profits. Si vous souhaitez vendre à d'autres entreprises, vous pouvez recourir à Internet pour trouver des indications de clients potentiels, publier des appels d'offres et offrir des produits par l'intermédiaire de votre site Web ou d'un cybermarché.

La recherche de produits et services en ligne peut vous faire gagner temps et argent, car vous pouvez trouver les prix les plus avantageux sans avoir à vous déplacer. De plus, vous pouvez vous servir d'Internet pour trouver de nouveaux fournisseurs, afficher des demandes de produits ou services que vous souhaitez vous procurer ou rechercher des produits et services. Les réseaux de commerce en ligne peuvent également contribuer à l'échange efficace de renseignements entre les acheteurs et les vendeurs.

III.3. Les avantages des Solutions de commerce électronique

- Meilleur service à la clientèle: Les entreprises peuvent traiter directement avec leurs clients jour et nuit.

- Élimination des intermédiaires: Les entreprises, en particulier les manufacturiers, peuvent offrir leurs produits

aux consommateurs à un prix plus bas et plus abordable en leur vendant ceux-ci directement, sans l'intervention de distributeurs et de détaillants, qui fait gonfler les prix.

- Flexibilité dans l'établissement des prix : Les étiquettes de prix peuvent être modifiées facilement et instantanément, ce qui présente un avantage pour l'entreprise et pour le client. Le commerce électronique de détail vous offre en outre la possibilité de faire de la vente croisée, de la vente incitative, d'offrir des rabais, ainsi que des coupons et autres soldes en ligne ou hors ligne.

- Image de professionnalisme: Même si votre entreprise est de petite taille, votre site de commerce électronique peut contribuer à rehausser votre réputation en projetant une image plus imposante et en vous permettant de bénéficier de conditions équitables de concurrence.

- Rayonnement accru: L'ouverture d'une vitrine virtuelle peut élargir votre présence auprès d'une clientèle potentielle appréciable, en particulier celle qui n'a pas accès à vos installations physiques locales.

III.4. Mise sur pied d'un magasin virtuel

Le présent point explique en quoi consiste la vente en ligne sur votre site Web. Trois éléments sont indispensables au traitement d'une opération de vente en ligne :

1. Le panier d'achat
2. Un serveur sécurisé
3. Le traitement des paiements

Ces trois éléments essentiels sont exposés plus amplement ci-dessous.

1. Paniers d'achat

Les logiciels «panier d'achat» retiennent les articles que l'utilisateur choisit d'acheter sur le site Web avant de passer à la «caisse». Le panier d'achat virtuel comporte trois parties :

- le catalogue de produits ;
- la liste des achats ;
- le système de caisse de sortie.

Le catalogue de produits contient tous les renseignements nécessaires pour présenter au client chaque produit offert et compléter une opération de vente en ligne. Les renseignements inclus dans la base de données de produits comprennent, en règle générale, le prix, le numéro du produit, une image ou autre représentation multimédia, les options ou choix concernant le produit.

La liste DES ACHATS (c.-à-d. la liste des produits sélectionnés) permet aux utilisateurs de retracer les articles qu'ils souhaitent acheter. On utilise habituellement une image de panier d'achat pour indiquer les articles sélectionnés par le visiteur. Pour que le

panier d'achat fonctionne correctement, l'ordinateur de l'utilisateur doit être réglé pour accepter les témoins (cookies).
Le système de caisse de sortie permet aux clients de sélectionner des produits en cliquant sur un bouton «ajouter des articles dans le panier», puis de payer les produits sélectionnés.

2. Serveur Sécurisé

Le serveur sécurisé contribue à assurer une protection contre la perte ou la modification des renseignements personnels. Le protocole SSL est la technologie la plus couramment utilisée aux fins des transactions sécurisées en ligne.

Le protocole SSL procède au cryptage (codage) de toutes les données échangées entre le serveur de la boutique et l'ordinateur du client. Ces renseignements, par exemple les numéros de carte de crédit, deviennent ainsi très difficiles à décoder pour des tiers.
Le schéma qui suit illustre la façon dont un serveur sécurisé est en mesure de protéger les renseignements qui circulent entre le consommateur et le client.

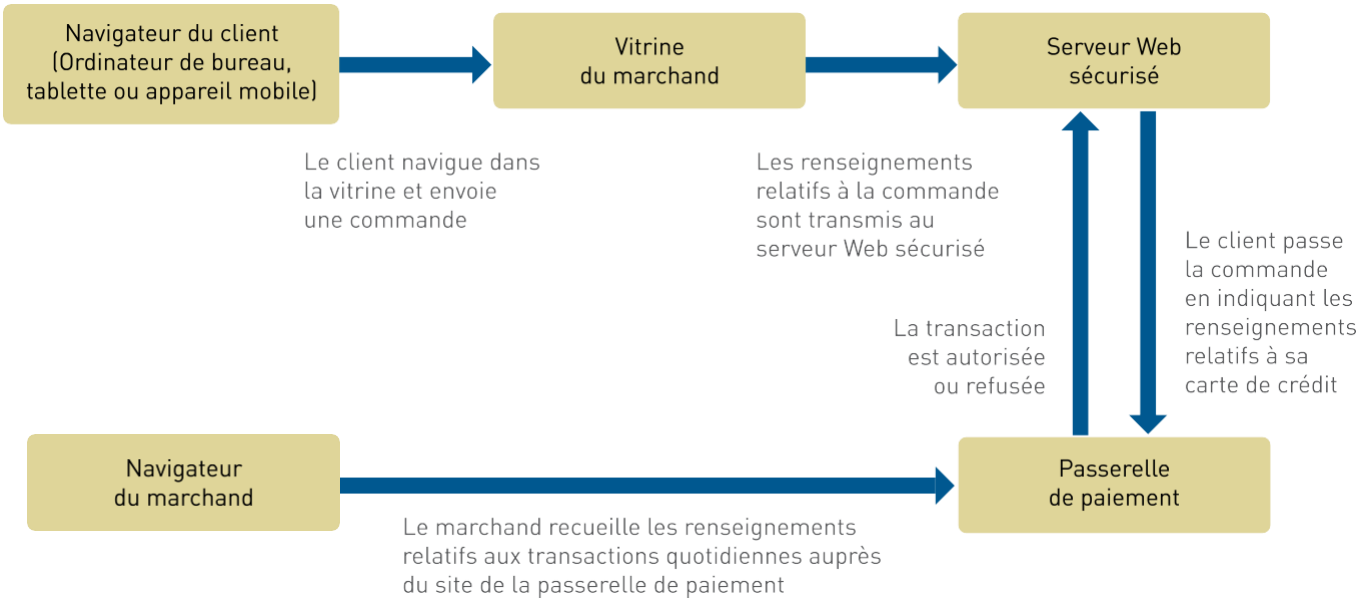


Figure III.1. La protection des renseignements relatifs aux transactions au moyen d'un serveur sécurisé

Les paniers d'achat n'ont un rôle à jouer que dans une partie de la transaction. Ils transmettent des renseignements (c.-à-d. les articles commandés par l'utilisateur) à une Passerelle de paiement.

Une passerelle de paiement est un service distinct qui relie le panier d'achat aux réseaux financiers intervenant dans la transaction. Lorsque vous choisissez un forfait de panier d'achat, assurez-vous de la compatibilité entre celui-ci et le service de passerelle de paiement. Renseignez-vous auprès du fournisseur du service de passerelle afin de connaître les forfaits de panier d'achat que celui-ci prend en charge. Les passerelles de paiement associent les transactions à des certificats d'identification commerciale et les marchands n'ont ainsi par besoin de connaître le numéro de carte de crédit de leurs clients.

Les TEMOINS sont de petits fragments logiciels qui les sites Web stockent dans l'ordinateur des utilisateurs. Ils ont de très multiples usages, dont un important consiste à savoir comment les visiteurs arrivent dans le site et comment ils utilisent celui-ci. Si votre site Web fait usage de témoins, vous devriez expliquer aux visiteurs l'usage que vous faites de ces renseignements et les raisons pour lesquelles vous les utilisez.

Les Serveurs constituent l'épine dorsale d'Internet : il s'agit d'ordinateurs reliés par des lignes de communication qui distribuent les renseignements sous forme textuelle, graphique et multimédia à des ordinateurs en ligne qui demandent des données.

III.5. Les nom de domaines sécurisés

Si vous prévoyez faire de la vente en ligne, vous devrez vous doter d'un certificat numérique pour que fonctionne la technologie SSL. Un certificat numérique est un certificat d'identité qui contribue à démontrer la crédibilité d'un site Web.

Si vous désirez effectuer des achats en ligne, comment savoir si le site Web est doté d'un serveur sécurisé?
Recherchez ce qui suit :

- L'adresse URL commence par **HTTPS://** plutôt que par **http://.**

- Le navigateur vous avise du fait que vous vous trouvez dans un site sécurisé. Plusieurs navigateurs utilisent un symbole (ex., l'icône d'un cadenas) ou un message.

III.6. Options relatives au traitement des paiements

En matière de traitement des paiements, cinq options s'offrent à vous :

A. Le traitement des paiements par un tiers

B. Le compte commercial Internet

C. Le traitement des paiements manuel (hors ligne)

D. Les passerelles de PPEF et de paiement sur demande

E. Le commerce électronique mobile avec identification par radiofréquence et communication

Les facteurs à prendre en considération au moment de choisir une option de traitement DES PAIEMENTS.

- Les coûts associés à l'option de paiement (frais de transaction, frais d'ouverture de compte, frais mensuels).
  - ✓ Prenez le temps de comprendre les caractéristiques qu'offre chaque option ainsi que le modèle de tarification ;

- ✓ Tenez compte du fait qu'il existe différents frais et différentes caractéristiques associés aux comptes commerciaux ;
- ✓ Tenez également compte des frais de rétro facturation ;
- ✓ Prenez aussi en compte les frais associés aux transactions frauduleuses.

- o **La confidentialité des données relatives à la transaction**: Si vous examinez la possibilité de louer un logiciel par l'intermédiaire d'un fournisseur de services, prenez connaissance de la politique de celui-ci en ce qui concerne la divulgation et le partage des renseignements.
- o **La protection contre la fraude**: Examinez les outils de protection contre la fraude. Les comptes commerciaux sont habituellement dotés de filtres antifraudes qui repèrent et retracent les transactions suspectes. Ces transactions peuvent être mises en attente pendant que la banque informe l'entreprise de l'activité suspecte.
- o La crédibilité générale du fournisseur de services: La crédibilité des comptes commerciaux Internet est plus grande.

A. Le traitement des paiements par un tiers

Ces services constituent une solution de rechange à l'obtention d'un compte commercial Internet. Cette solution présente l'avantage de vous permettre de commencer à vendre en ligne plus rapidement et plus facilement. Elle s'assortit de frais d'inscription, de frais de transaction et de frais mensuels. La

période de retenue avant le versement au marchand du solde des ventes peut également être plus long.

Selon Wikipédia (www.wikipedia.org), PayPal (www.paypal.com) est le fournisseur de services en ligne le plus utilisé. Selon CanadaOne www.canadaone.com, les petites entreprises recourent à des entreprises de traitement des cartes de crédit telles que PayPal (www.paypal.com), CCNow (www.ccnow.com),PsiGate(www.Psigate.com),Beanstream (www.beanstream.com) et InternetSecure (www.internetsecure.com).

Les fournisseurs de services de paiement à des tiers perçoivent des frais de transaction, y compris un pourcentage de la vente et un montant fixe par transaction. Les frais établis selon le nombre de transactions peuvent convenir aux microentreprises ou lorsque le nombre de transactions est limité.

Comment fonctionne ce type de traitement? L'argent issu de la transaction est déposé dans un compte spécial géré par le fournisseur de services. Pour obtenir son argent, le commerçant doit habituellement entreprendre le transfert. En cas de différend au sujet de la transaction, le fournisseur de services peut retenir les fonds pendant de plus longues périodes.

B. Le compte commercial Internet

Un compte commercial Internet est accordé par une institution financière et permet à l'entreprise qui en est titulaire d'accepter les paiements en ligne effectués par carte de crédit. Les entreprises doivent obtenir un compte commercial Internet distinct pour chaque type de carte de crédit qu'elles souhaitent accepter (p. ex. Visa, Mastercard, American Express).

Comment obtenir un compte commercial Internet?

Vous devez établir un compte commercial auprès d'une banque. La banque procédera à une évaluation du RISQUE de crédit. Il peut être utile de préparer un plan d'affaires. Vous pourriez être tenu de verser à la banque un dépôt de garantie substantiel. Avec ce type de compte, le processus de transfert de l'argent dans le compte approprié est automatique et rapide.

C. Le traitement manuel (hors ligne) des paiements

Vous pouvez mettre sur pied un site Web de commerce électronique dans lequel les utilisateurs peuvent passer des commandes en ligne, mais vous traitez les cartes de crédit manuellement plutôt que de recourir aux options de traitement des paiements en ligne. Avec cette option, les renseignements relatifs aux cartes de crédit peuvent être obtenus par l'intermédiaire d'un serveur sécurisé et la transaction peut être traitée manuellement. Cette option est envisageable lorsque le nombre de commandes en ligne est limité.

D. La PPEF et les passerelles de paiement sur demande

La présentation et le paiement électroniques de factures (PPEF) est un processus permettant la livraison et le paiement des factures par Internet. La PPEF est pratique pour les clients et leur permet de gagner du temps, tandis que pour le propriétaire de l'entreprise, il se traduit par des capacités de paiement accélérées. Les petites entreprises peuvent utiliser la PPEF de trois façons :

- ✓ Le service de consolidation est la possibilité offerte par de grandes organisations, telles que les banques ou le bureau de poste, de payer divers types de factures par le biais de leur site Web. Pour la petite entreprise moyenne, il s'agit davantage d'une commodité en tant qu'utilisateur du service que d'une façon d'implanter un service de PPEF pour les clients ;

- ✓ Biller Direct est un service permettant aux petites entreprises d'offrir à leurs clients la possibilité de visiter son site pour payer leurs factures par voie électronique ;

- ✓ Le paiement direct par courriel permet aux petites entreprises d'offrir à leurs clients la possibilité de régler de façon pratique et rapide leurs factures par courriel.

E. Le commerce électronique mobile avec identification par radiofréquence et communication NFC

La communication en champ proche (NFC) est une technologie sans fil recourant à l'identification par radiofréquence et permettant à des appareils de transmettre des données entre eux à des fins de commerce et de paiement mobiles. À titre d'exemple, vous pouvez maintenant payer votre repas en agitant simplement votre téléphone intelligent devant un lecteur de carte sans fil au restaurant.

Les leaders de marché tels que Google et Apple s'emploient à améliorer les capacités du commerce mobile au moyen de téléphones intelligents équipés de la technologie NFC. Pour la plupart des détaillants, l'obstacle le plus important réside dans le passage des terminaux de point de vente à cette nouvelle technologie.
Il y a aussi la courbe d'apprentissage du personnel dont il faut tenir compte. Mais de plus en plus de consommateurs recherchent des options d'achat et de paiement pratiques qui correspondent à leur mode de vie de plus en plus mobile.

III.7. Sécurité et protection des renseignements personnels

Il importe d'être conscient des questions relatives à la sécurité et la protection des renseignements personnels associées au commerce électronique. Les risques les plus courants sont l'utilisation frauduleuse des cartes de crédit, les virus informatiques, les pourriels (courriels non sollicités) et le vol d'ordinateurs ou de renseignements.

L'hameçonnage est un risque pour la sécurité qui se présente sous forme de courriel qui semble provenir d'une source officielle, mais qui contient des hyperliens redirigeant l'utilisateur vers un site factice où il est amené à divulguer des renseignements personnels. Le vol de renseignements personnels ou leur protection inadéquate constituent des menaces à la vie privée.

Voici quelques conseils pour réduire les risques liés à la sécurité et à la protection des renseignements personnels :

- ✓ Passez en revue les fonctions et les services relatifs à la sécurité offerts par votre hébergeur Web, votre fournisseur de services Internet, votre concepteur Web et votre fournisseur de logiciels;

- ✓ Soyez attentif aux alertes de sécurité et installez les correctifs de sécurité nécessaires;

- ✓ Procédez régulièrement à la mise à jour du logiciel de sécurité et à la recherche de logiciels espions et de virus;

- ✓ Faites régulièrement des copies de sauvegarde des systèmes et des données;

- ✓ La conception d'un site de commerce électronique doit réduire au minimum les risques pour la sécurité. Par

exemple, lorsque le consommateur appuie sur le bouton «Acheter», le bouton «Précédent» devrait être désactivé;

- ✓ procurez-vous un certificat numérique pour votre site Web. Ce certificat indique que les renseignements personnels transmis à votre site seront chiffrés (codés). Verisign (http://www.verisign.com) et Thawte (http://thawte.com) sont deux des principaux fournisseurs de certificats numériques sur Internet;

- ✓ évitez de stocker sur votre ordinateur l'information relative aux cartes de crédit des clients. Si vous laissez ces renseignements sur votre ordinateur, assurez-vous que ni vos employés ni les pirates informatiques n'y ont accès;

- ✓ Rédigez une politique de protection des renseignements personnels. Cette politique devrait encadrer la collecte et l'utilisation des renseignements ainsi que les procédures de sécurité utilisées pour protéger ces renseignements de la perte, du vol ou de toute modification. Vous pourriez afficher cette politique sur votre site. Vous pourriez également demander un sceau de garantie de protection des renseignements personnels. L'icône du sceau de garantie de protection des renseignements personnels s'affiche sur votre site et augmente la confiance des consommateurs.

- ✓ assurez-vous d'être muni du protocole SSL qui permet de crypter les renseignements confidentiels pendant la transmission des transactions et leur autorisation;

- ✓ assurez-vous d'avoir le matériel de sécurité nécessaire pour stocker les renseignements. Par exemple, le protocole SET (Secure Electronic Transaction) élaboré conjointement par VISA et MasterCard. Avec ce protocole, l'entreprise n'a pas accès aux renseignements sensibles et ceux-ci ne sont pas stockés sur le serveur de l'entreprise. Des coupe-feu devraient être utilisés pour protéger le réseau et les ordinateurs des virus et des pirates informatiques. Seuls les employés autorisés devraient avoir accès aux renseignements et particulièrement aux renseignements sensibles;

- ✓ passez en revue les autres outils de prévention des fraudes et évaluez leur pertinence dans le cadre de vos opérations. Par exemple, un service de vérification des adresses (AVS) compare l'adresse du client avec celle qui est inscrite dans le registre de la banque ayant émis la carte. Les grandes sociétés émettrices de cartes de crédit ont également des systèmes de vérification. Le code à trois chiffres imprimé à l'arrière des cartes de crédit peut vous aider à déterminer la validité de la carte des clients;

- ✓ vérifiez toujours l'adresse du client;

- ✓ méfiez-vous des commandes importantes ou des commandes de plusieurs exemplaires du même produit, en particulier si le client demande une livraison urgente;

- ✓ si vous vendez des articles de valeur qui peuvent se revendre facilement, vous pourriez envisager de faire appel aux services évolués de protection contre les fraudes offerts par les fournisseurs de services de passerelle (p. ex., les filtres antifraude qui détectent les activités suspectes.

CHAPITRE IV : LES API

IV.1. Introduction

Les API sont un sujet en vogue, qui fait l'objet de vifs débats entre commerciaux, responsables informatiques et développeurs. Cette agitation au sein de l'espace public porte essentiellement sur les API publiques ouvertes. Pour oser une comparaison, ne pas avoir une API publique aujourd'hui, c'est comme ne pas avoir de site Web à la fin des années 1990. Cependant, bon nombre d'entreprises considèrent les API publiques comme le cadet de leurs soucis.

Créer des solutions omnicanal, innover plus vite que la concurrence, devenir une entreprise mobile ou mettre en place un environnement de cloud hybride constituent des priorités. Pourtant, les API jouent un rôle central dans tous ces projets et bien d'autres, d'où cet intérêt de la part d'acteurs divers et variés.

Mais qu'est-ce qu'une API ? En quoi se différencie-t-elle d'une interface de programmation d'applications ancienne génération ? Et pourquoi faut-il s'en soucier ? L'acronyme API (pour Application Programming Interface) signifie Interface de programmation d'applications. Cette notion a considérablement évolué avec le temps. Les API d'aujourd'hui sont très différentes des anciennes.

IV.2. Définition d'un API

Parfois, il vaut mieux définir quelque chose en commençant par expliquer ce que cette chose n'est pas. Donc, voici ce qu'une API n'est pas :

- **Un logiciel**: un logiciel n'est pas une API (même s'il peut se présenter sous la forme d'une API pour faciliter l'utilisation de ses fonctionnalités) ;
- **Une interface utilisateur**: une interface utilisateur n'est pas une API (mais elle peut s'exécuter sur une interface utilisateur) ;
- **Un serveur**: un serveur n'est pas une API (mais il peut héberger une ou plusieurs API qui fournissent les données et fonctions mises à disposition par le serveur).

IV.3. Des API à l'économie des API

L'économie des API apparaît lorsque les API deviennent parties intégrantes du modèle économique. Les API publiques et

partenaires sont des outils stratégiques pour plusieurs modèles économiques, comme ceux de Twitter et d'Amazon.

Par exemple, les API de Twitter enregistrent dix fois plus de trafic que le site Web de Twitter. Clairement fondé sur l'interaction par les tweets, le modèle économique de cette société permet à tous ceux qui le souhaitent de proposer une expérience utilisateur.

Dès le début, Amazon a décidé de ne pas se positionner comme un simple revendeur sur Internet, mais comme un portail marchand à l'échelle mondiale. La plate-forme marchande d'Amazon s'appuie résolument sur des API qui facilitent l'intégration de nouveaux marchands.

En tant qu'outils de réseau métiers, les API ne constituent pas une nouveauté. Depuis plusieurs décennies, les banques créent des infrastructures de paiement et des chambres de compensation basées sur des API spécifiques. À ceci près que les API modernes sont explicite- ment conçues pour un écosystème ouvert (interne ou externe) et non pour des réseaux privés fermés. De plus, les modèles de consommation des API sont standardisés, privilégiant la simplicité de consommation à la facilité de création.

Certaines personnes emploient le terme API métiers pour désigner toutes les API modernes. Un terme bien choisi, dans la mesure où les API, en tant que produits, doivent faire partie intégrante de votre stratégie métier. Sachez simplement que lancer une API publique ou partenaire n'est pas la seule manière d'intégrer des

API dans votre modèle économique. Les modes d'utilisation des API consommées en interne sont nombreux, le plus connu étant la nécessité de proposer une expérience client omnicanal différente.

Que votre entreprise soit « née sur le Web » ou qu'elle existe depuis un siècle, vous vivez à l'âge du cloud, de l'analyse des données, de l'informatique mobile et des réseaux sociaux, où l'omnicanal est devenu l'enjeu principal. Pour vous démarquer de vos concurrents, vous devez proposer aux clients une expérience immédiatement agréable. Et pour ce faire, vous devez être libre d'expérimenter et d'innover.

IV.4. Quatre catégories d'API

Lorsque vous décidez de créer des API, choisir celles à créer en premier peut être compliqué. Une bonne API doit se démarquer de ce qui existe déjà. Se demander « Quelles situations métiers pourrais-je améliorer, et comment m'y prendre ? » est un bon point de départ. Trouvez la réponse à ces deux questions et vous saurez quelles API créer en premier parmi les quatre catégories proposées ci-après :

- **API de détection**: ces API vous aident à identifier les opportunités qui impliquent des clients, des employés, des partenaires et des équipements. Elles intègrent des fonctionnalités, telles que la géolocalisation mobile, la

surveillance par capteurs, l'analyse prédictive et l'observation humaine ;

- **API d'enrichissement**: ces API améliorent la compréhension de la situation grâce à des données historiques émanant de systèmes de gestion de la relation client (CRM), de fichiers de comptabilité, d'analyses démographiques, de dossiers médicaux, etc ;

- **API de perception**: ces API fournissent un contexte dynamique de la situation actuelle et vous permettent de savoir ce que pensent les personnes que vous ciblez. Il peut s'agir d'API sociales (des personnes partageant des projets futurs ou des intérêts actuels) ou de solutions d'analyse de capteurs (pour l'état global du système, comme la consommation des ressources ou la congestion du trafic) ;

- **API d'action**: ces API vous permettent d'agir en quasi-temps réel. Elles peuvent inclure des notifications push, des équipements instrumentés ou des systèmes de gestion de tâches humaines.

IV.5. Savoir en quoi consiste la gestion d'une API

Pour un consommateur d'API, un bon portail de développeurs est essentiel. Pour un fournisseur d'API, la gestion des processus

d'externalisation et de partage des API ne constitue que la partie émergée de l'iceberg (voir la figure IV.1). Les aspects métiers et informa- tiques qui facilitent la création, le déploiement et l'exploitation des API restent cachés. Ces aspects incluent le mapping des données, la sécurité, la régulation du débit, le suivi et la gestion des versions.

Non seulement une API gérée dispose d'une interface bien définie et s'adresse à un public cible, mais son fonctionnement est régi par des contrôles métiers et informatiques correctement mis en œuvre. Chaque groupe joue un rôle particulier dans la gestion des API.

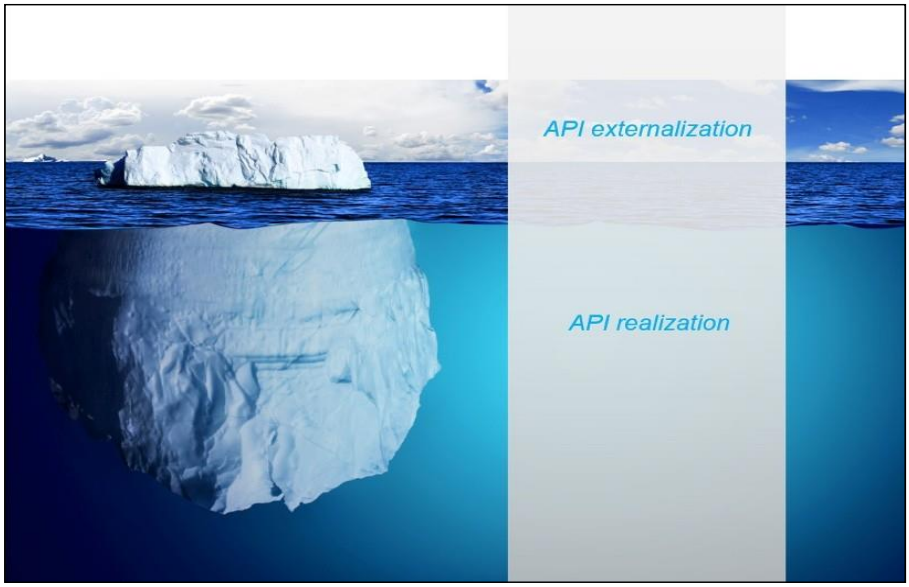


Figure IV.1 : La gestion des API ne se limite pas à leur conception et à leur externalisation

Le propriétaire d'API prend les décisions suivantes :

- ✓ Les conditions dans lesquelles l'API peut être consommée
- ✓ Les communautés avec lesquelles l'API sera partagée

- ✓ Si l'API remplit ses objectifs (en cas d'échec, le modèle économique doit être ajusté)

IV.6. Concepteur d'API

Cette personne est chargée de créer et de déployer l'API. Elle doit effectuer les opérations suivantes :

- ✓ définir l'interface de l'API;
- ✓ identifier les points de terminaison principaux capables de fournir les données ou les fonctions nécessaires pour mettre en œuvre l'API;
- ✓ configurer le mapping entre l'interface de l'API et les sources principales de données ou de fonctionnalités.

Le concepteur d'API doit être capable d'effectuer ces tâches sans générer un volume de code important. Lorsque la création d'une API repose davantage sur la génération de code que sur la configuration dynamique, le rythme d'innovation chute inévitablement, même chez les équipes de développement les plus agiles. La distinction entre la configuration d'une API et le développement de données ou de fonctionnalités est essentielle dans la réflexion sur les API.

Les API modernes ne sont pas des logiciels, mais un moyen souple de présenter des fonctionnalités à des publics extérieurs à votre équipe.

IV.7. CONCLUSION

Dans ce monde actuel où tout devient automatisé, l'administration, la connaissance du fonctionnement, la création et la configuration des réseaux informatiques parait indispensable pour un étudiant en Informatique.

Ce cours d'administration des réseaux informatiques est rédigé tout en tenant compte du niveau de compréhension des étudiants et leurs prérequis en générale. Les chapitres sont présentés dans le but de permettre aux apprentis dans le domaine de comprendre les notions de base d'administration des réseaux informatiques.

IV.8.References

[2] https://www.frameip.com/tcpip/?video=322#video-322
[3] http://www.coursnet.com/2014/12/cours-modele-tcpip.html
[4]https://www.it-connect.fr/virtualisation-les-types-de-connexion-au-reseau/
[5] https://ecommerce-platforms.com/fr/glossary/ecommerce
[6] Source: Expedite Media Group, Inc
[7] www.canadabusiness.ca
[8] John Wiley & Sons, Inc., 2015, Les API pour les Nuls®, Édition limitée IBM, 111 River St., États-Unis
[9] Scott Empson, 2008, CCNA Portable Command Guide, Second Edition, Indianapolis, IN 46240 USA,Cisco Press