Module Réseaux et Sécurité Informatique
Medium.ip 01-01-1430

Q : C'est quoi la raison pour la quelle les télécommunications et les réseaux informatiques sont développée ?

R : Le besoin de partager les ressources, échanger les informations d'une manière simple et rapide entre systèmes, se sont les principaux raisons de développer les télécommunications et les réseaux informatiques. L'avantage est la non nécessite de la mise à disponibilité toutes les données et les applications nécessaire au travail d'une machine connectée à un réseau informatique, ce qui va éviter de dupliquer les données et les programmes dans les machines d'un seul site.

Q : Quelles sont les différentes étapes pour transmettre des données entres systèmes ?

R :

1- Etablissement de la connexion : Afin de garantir la bonne livraison des données, on vérifie la présence des deux machines, ces dernières réserve les ressources système nécessaire sur les quels le contrôle de flux est effectué. Les systèmes d'extrémités sont d'accord et près pour communiquer
2- Etablissement de la communication : Plusieurs mécanismes sont présents pour assurer le transfert des informations, ces mécanismes implémentent les différents protocoles qui s'utilisent comme des règles dans le but d'avoir le même langage d'échanger les données.
3- Fermeture de connexion : Fin du transfert, il faut libérer les ressources systèmes et réseaux allouées pour permettre à d'autres entités d'utiliser à nouveau le réseau (c'est-à-dire une nouvelle communication).

Q : Quelles sont les différentes types des réseaux informatiques ?

R : Selon plusieurs paramètres à savoir : Le débit maximum, la localisation et la distance entre terminaux et systèmes informatiques,…, on distingue 3 types des réseaux informatiques :

1- Les réseaux LAN (Local Area Network) qui sont des réseaux intra entreprise et qui sont géographiquement limité à quelques centaines de mètres. Ils ne dépendent pas d'un opérateur officiel de télécommunication. Ethernet, Fast Ethernet, FDDI et ATM sont des types de technologies utilisées dans les LANs.
2- Les réseaux MAN (Metropolitan Area Network) relient plusieurs LANs d'une même ville.
3- Les réseaux WAN (Wilde Area Network) qui dépendent d'un opérateur officiel de télécommunication, ils assurent la transmission des données sur des distances à grande échelle (Sup à 100 km).

Q : Qu'est ce qui diffère la topologie physique de la topologie logique ?

R : La topologie physique désigne la manière dont les nœuds d'un réseau sont connectés physiquement (ex : Topologie étoile, bus et anneau), mais la topologie logique est le mode de

communication qui décrit la façon dont les systèmes émettent les données sur le médium physique (ex : Ethernet, FDDI, Token Ring).

Q : Pourquoi la normalisation des technologies de l'information ?

R : Avant, chaque compagnie a développé ses propres règles pour l'échange des données, ce qui a posé un véritable problème : la communication entres les différentes dispositifs à différents protocoles est impossible. C'est pour cette raison que plusieurs organismes ont proposé de normaliser les protocoles utilisés (ex : Modèle OSI de ISO), d'où la normalisation des technologies de l'information.

Q : Qu'est ce qu'il faut définir pour avoir un concept d'architecture en couche de niveau N?

R : Trois objets sont nécessaire pour développer un concept d'architecture en couche :

1- Le service-N : Qui est un ensemble de procédures qui devant être effectuées au niveau N et qui rend un service à la couche de niveau supérieur.
2- Le protocole-N : Qui est l'ensemble de règles à respecter pour transporter et définir le format des données du niveau N au niveau N homologue, il est le responsable de réaliser le service.
3- Les points d'accès au service-N (N-SAP) : Ils sont localisés à la frontière entre deux couches adjacentes. A partir des N-SAP l'entité N fournis le service à celle de N+1.

Q : Comment déterminé un service ou protocole ?

R : Un service ou un protocole sont déterminés par trois attributs :

1- La sémantique d'association qui désigne le mode de connexion (Connecté ou non connecté).
2- La sémantique de fonctionnalité : qui regroupe l'ensemble des procédures utilisés dans le transfert.
3- La syntaxe qui caractérise le codage des primitives de service et l'unité de données de protocole (PDU).

Q : Quelles sont les quatre primitives de service ? Donner un exemple de fonctionnement de ces primitives de service.

R : Les quatre primitives de service sont :

1- Primitive de demande : N-service.REQUEST
2- Primitive d'indication : N-service.INDICATION
3- Primitive de réponse : N-service.RESPONSE
4- Primitive de confirmation : N-service.CONFIRMATION

Exemple d'application : Etablissement d'une connexion réseau

- N-service.REQUEST : Demande de la connexion réseau.
- N-service. INDICATION: Indication de la connexion réseau.
- N-service. RESPONSE: Réponse à une demande de connexion réseau.
- N-service. CONFIRMATION: Confirmation de la connexion réseau.

Q : Quelles sont les principales unités de données de services ? Quelle est la relation entre eux ?

R : Les principales unités de données de services sont :

1- PCI (Protocol Control Information)
2- SDU (Service Data Unit)
3- PDU (Protocol Data Unit)
[N-PDU = N-PCI + N-SDU]

Q : Quel est les rôles des couches du modèle OSI ?

R : Voici les rôles de chaque couche du modèle OSI :

1- La couche physique [3 ARGS] : Elle décrit les caractéristiques physiques et électroniques de la connexion, et elle s'occupe de la transmission des données bit par bit sur le canal de transfert. Les données sont représentées sous forme des impulsions électriques ou lumineuses.

2- La couche Liaison [6 ARGS] : Elle est composée de deux sous couches principales : LLC et MAC. Elle est responsable de l'établissement et de la libération de la connexion, elle fractionne et envoi les données d'émetteur en trames et gère les trames d'acquittement du récepteur. Un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Elle assure aussi un contrôle de flux ce qui évite l'engorgement et la surcharge du récepteur. La couche liaison doit aussi déterminer la méthode d'accès au support (ex : Token Ring, CSMA/CD).

Couche Liaison de données	LLC (IEEE 802.2)
	MAC (IEEE 802.x)

Le Medium Access Control ou MAC spécifie comment des stations se partagent sur le médium. Le 802.3 propose par exemple une méthode d'accès au médium appelée Carrier Sense Multiple Access with Collision Detection (CSMA/CD) tandis que les normes IEEE 802.4, 802.5 et FDDI font appel à des passages de jeton.
Le Logical Link Control veille à la fiabilité de la connexion physique. Le 802.2 fait office de lien logique de contrôle. Le PPP (Point to Point Protocol) travaille à ce niveau.

3- La couche réseau [2 ARGS] : Elle assure l'acheminement des données à travers les routeurs ce qui garantie le routage des paquets. Elle effectue aussi un contrôle de congestion tel qu'il adapte la taille des blocs de données aux capacités du sous réseau physique utilisé. A ce niveau, interviennent aussi les protocoles de routage ex : Routing Information Protocol (RIP).

4- La couche transport [3 ARGS]: Elle contrôle le transport de bout en bout ce qui garantie que le récepteur reçoit exactement ce que lui a été envoyé, elle assure le découpage des données en segments en cas d'émetteur, et le réassemblage des

segments en bon ordre en cas de récepteur et aussi il s'occupe de la cohérence des données.

5- La couche session [1 ARGS] : Elle assure la synchronisation du dialogue entre les hôtes en ouvrant des sessions pour chaque application ce qui va permettre à plusieurs applications d'utiliser la même interface pour communiquer simultanément.

6- La couche présentation [2 ARGS] : Elle permet de mettre en forme les données dans un format compréhensible par les 2 systèmes, elle assure également les fonctions de cryptage et de compression des données.

7- La couche application [1 ARGS] : Elle est constituée des applications qui se servent du réseau (ex : Navigateur Web, …).

Q : Y a-t-il une différence entre une communication avec connexion et celle sans connexion ?

R : Oui, il existe une grande différence entre une communication avec connexion et une communication sans connexion :

La communication orienté connexion garantit la bonne livraison des données et effectue un control de flux fiable et elle nécessite des confirmations (ACK) de la part du récepteur, par contre la communication sans connexion est plus simple est plus facile mais elle ne contrôle pas les flux des données et elle n'a pas besoin de vérifier la présente ou non de la machine destinatrice ce qui assure pas le transfert des informations.

Q : Fait une comparaison entre le TCP et l'UDP.

R : Les deux protocoles TCP et UDP sont implémentés dans la couche de niveau 4 du modèle OSI, mais leur fonctionnement est différent :

TCP (Transmission Control Protocol) est un protocole fiable, orienté connexion. Il garantit l'ordre et la mise des paquets et la réussite de la livraison de données. Ce protocole exige également que le récepteur lui renvoi des accusés de réception des données (ACK).

UDP (Unit Datagram Protocol) est un complément du protocole TCP qui offre un service sans connexion qui ne garantit ni la remise ni l'ordre des paquets délivrés.

Q : Quel est le rôle et le principe des protocoles ARP et RARP ?

R :

ARP (Address Résolution Protocol) est un protocole de résolution d'adresse MAC ou physique à partir d'un adresse IP, il fonctionne au niveau 3 du modèle OSI. Pour que deux machines de même réseau puissent se communiquer, chacune d'eux doit connaître l'adresse physique de l'autre, c'est pour cette raison qu'on a besoin d'une table qui contient l'adresse IP et sa correspondance physique. Cette table est nommée ARP, elle se met à jour automatiquement ou manuellement.

RARP (Reverse Address Resolution Protocol) fait le travail inverse du protocole ARP, il traduit une adresse physique en adresse logique.

Q : Pour définir la qualité d'un service, quels paramètres le permettent ?

R : Les paramètres qui permettent de définir la qualité d'un service sont :

1- Le délai d'établissement et de la libération d'une connexion.
2- Probabilité d'échec de l'établissement ou libération d'une connexion.
3- Le débit lors de transfert de données.
4- Le taux d'erreurs.$

Q : Quelle est la différence entre le contrôle d'erreurs, de flux et d'échange ?

1- Le contrôle d'erreurs s'effectue par un protocole déterminé qui assure la détection et la correction d'erreurs et s'il utilise les acquittements, alors il s'occupe de les envoyer à l'émetteur pour lui indiquer la bonne réception ou non de l'information. Le contrôle est effectué par des clés calculées en appliquant des techniques comme: VRC, LCR, CRC et FCS

2- Le contrôle de flux adapte le débit d'envoi de l'entité émettrice à la vitesse de traitement et les ressources disponibles du récepteur afin d'éviter la congestion et le surcharge de celui-ci. Sans ce mécanisme de contrôle de flux, les données arrivent plus rapidement que la capacité de traitement du récepteur ce qui va remplir ses tampons et puis il y aura des pertes des données.

3- Le contrôle d'échange est réaliser à l'aide de deux compteurs Ns et Nr qui compte le nombre de blocs d'informations envoyés (Send) et reçus (Receive). Un protocole à anticipation est présent pour gérer les acquittements des trames reçus en respectant le crédit d'émission (la fenêtre d'anticipation). HDLC est un exemple de protocole employé pour contrôler l'échange d'informations.

Q : Pourquoi un modèle en couche ?

R : Un modèle en couche réduit la complexité, uniforme les services, assure l'interopérabilité de la technologie, facilite l'enseignement et l'acquisition des connaissances.

Q : Dans un réseau Ethernet :

- Quelle est la structure d'une trame ?
  [Préambule][@Mac Dest] [@Mac Source][Type][Données][Clé Calculée (CRC, FCS)]

- Quel est le protocole d'accès au médium ? Décrivez-le.
  Le protocole utilisé pour l'accès au médium en Ethernet est le CSMA/CD (Carrier Sense with Multiple Access / Collision Detection), ce dernier vérifie la présence ou non de porteuse et permet aux systèmes d'émettre les données sur le support une fois qu'il est libre, ce qui permet d'interdire d'autres émission simultanément et par

conséquent d'éviter des collisions. En cas de collision, CSMA/CD bloque l'accès au support pour un délai aléatoire.

Q : Quelle est la différence entre un commutateur et un concentrateur ?

R : Les deux matériels sont des équipements de raccordement actifs, ils permettent de mettre en place une topologie physique en étoile. Le concentrateur copie le signal d'entré et le diffuse sur tous les autres ports actifs, il est repéré au niveau 1, la zone de collusion est une seule pour toutes les machine connecté à cet équipement. Le commutateur fonction au niveau 2 (il existe actuellement des commutateurs allant jusqu'au niveau 3 qui traitent les IP), il effectue une analyse de la trame reçue pour déterminer sur quel port il va la diriger en se basant sur l'adresse MAC de la destination. Il crée pour chaque port une zone de collusion et il évite de partager la bande passante ce qui améliore le transfert.

Q : Quel est le rapport entre la Notion de fanion et celle de transparence lors de la délimitation des blocs de données échangées ?

R : Le fanion est une combinaison binaire qui sert à délimiter et synchroniser la transmission de données. La notion de transparence vient pour renforcer les fanions en les distinguant des données brutes par des caractères d'échappement (ex : Transparence binaire).

Q : Donner les principales étapes du traitement de la transparence binaire au cours de la transmission de la chaine binaire : **001101111110010101111011**.

R : Soient le fanion : **01111110,** et Le caractère d'échappement : **0**
Dans la machine émettrice :
Traitement de la transparence binaire : **00110111110100101011111 0 011**
Message émis : **01111110**00110111110**0**10010101111**0**011**0**1111110
Dans la machine réceptrice : La démarche en inverse.

Q : C'est quoi le rôle et le principe du protocole HDLC ?

R : HDLC (High Level Data Link Control) est un protocole utilisé pour contrôler l'échange de données, il offre un service de transfert de données fiable et efficace entre deux systèmes adjacents, il travail au mode connecté, il se base sur deux compteurs Ns et Nr qui compte respectivement le nombre de blocs envoyés et reçus dans chaque transmission. Il utilise trois types de trames :

- Trame d'information (I) : caractérisée par le bit de rang 0 à 0 du champ de commande dont il se trouve deux champs : Ns le numéro de la trame courante et Nr le numéro de la trame d'information attendue, ainsi qu'un troisième champ sur un seul bit qui dépend de type d'échange. La trame I est utilisée pour échanger les données.

- Trame de supervision (S) : caractérisée par les bits 1,0 dans les rangs 0,1 du champ de commande dont il y n'a pas de bits réservés au Ns. Elle transporte les commandes ou les réponses liées au contrôle d'erreurs, et au contrôle de flux.

- Trame non numéroté (U) : caractérisée par les bits 1,1 dans les rangs 0,1 du champ de commande, ce dernier ne contient pas les champs des compteurs. Cette trame est utilisée pour établir ou libérer une liaison.

Q : Quelle sont les différentes classes d'adresses ? Donnez pour chacune la plage des adresses privées et publics ainsi que le masque de réseau par défaut.

R :

Classe	Adresse réseau	Adresse réseau Privées	Masque
A	0.0.0.0 - 127.255.255.255	10.0.0.0 - 10.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	172.16.0.0 - 172.31.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	192.168.0.0 - 192.168.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	? - ?	255.255.255.255

Q : A quoi sert un masque de réseau ? Comment l'utiliser ?

R : Le masque sous réseau permet d'extraire l'adresse réseau à partir d'un IP de hôte en faisant un ET logique de l'adresse IP machine et son masque réseau.

Q : A quoi sert le Subnetting ? Comment obtenir des sous réseaux ?

R : La segmentation en sous réseaux réduit l'encombrement et le trafic, elle limite les diffusions, elle renforce la sécurité en isolant un réseau d'un autre, et elle optimise l'espace réservé à une adresse IP et surtout dans le cas des adresses publics car il nous permet de crée à partir d'une seule adresse réseau plusieurs sous réseaux, ce qui va agrandir le réseau. Pour avoir des sous réseaux, on réserve selon le besoin un nombre bien fixé de bits de poids forts dans le premier octet des octets d'ID machine, pour les ajouter au ID réseau.

Ex : @réseau : 10.0.0.0/8 et j'ai besoin de 2 sous réseaux, donc je réserve un seul bit, et voila les sous réseaux résultants : 10.0.0.0/10, 10.128.0.0/10

Q : Quelle est la différence entre le routage direct et indirect ?

R : Le routage direct s'agit de livrer un datagramme à une machine raccordée au même LAN, mais le routage indirect s'effectue lorsque le destinataire n'est pas sur le même site, alors il est absolument nécessaire de franchir une passerelle connue d'avance ou d'employer un chemin par défaut.

Q : Quelle est la différence entre le routage statique et dynamique ?

R : Le routage statique est réalisé si on fait rentrer les routes manuellement ce qui est un peu très fatiguant et non-pratique, c'est pour cela que plusieurs algorithmes (ex : RIP, OSPF) sont

développés pour s'occuper de la détermination des chemins dynamiquement ce qui permet d'avoir des routes toujours optimisées, c'est ce qu'on appel le routage dynamique.

Q : Quelles sont les principales algorithmes de routage ? Donner des exemples de protocoles utilisés.

R : Les algorithmes de routage se divisent en deux principales familles :

- Algorithme à vecteur de distance : Il détermine la direction (vecteur) et la distance vers les nœuds distants. Ex : RIP, EGP.

  RIP (Routing Information Protocol) : est un protocole de routage dynamique qui permet l'échange d'informations de routage sur un inter-réseau. Chaque routeur fonctionnant avec RIP échange les identificateurs des réseaux qu'il peut atteindre, ainsi que la distance qui le sépare de ce réseau *(nb de sauts=nb de routeurs à traverser).* Ainsi chacun dispose de la liste des réseaux et peut proposer le meilleur chemin.

- Algorithme à état de lien : Il décrit la topologie exacte de l'ensemble de l'inter-réseau. Ex : OSPF.

  OSPF (Open Shortest Path First) :

  - est un protocole de routage à état de lien, il effectue un routage dynamique qui permet l'échange d'informations de routage entre les routeurs voisins.
  - Il s'agit d'un protocole de type protocole route-link (que l'on pourrait traduire par Protocole d'état des liens), cela signifie que, contrairement à RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare.

Q : Quelles sont les cinq principaux objectifs à garantir quant on parle de la sécurité informatique ?

R : La sécurité informatique entraine cinq objectifs :

1- L'intégrité : Les informations ne doit pas être modifier au cours d'une transmission.
2- La confidentialité : Les informations envoyées doit être cryptées.
3- L'authentification : Garantir les identités des entités communicantes.
4- La non-répudiation : Prouver l'intégrité et l'origine des données.
5- Le contrôle d'accès : Sauf les utilisateurs autorisés ont le droit d'utiliser le système et ses ressources alors l'accès au système doit être bien contrôlé.

Q : Quelles sont les différentes techniques d'attaque ?

R : les techniques d'attaques sont :

1- Flux normal : C'est une attaque directe.
2- L'interruption : Destruction de tous les messages destinés à un nœud particulier ce qui lui rend indisponible.
3- L'interception : Espionnage et vol d'information enlève la confidentialité.
4- La modification : Modifier le contenu d'un message.
5- La fabrication : Modifier la direction et/ou l'origine d'un message.

Q : Quelle est la différence entre une menace active et une autre passive ?

R : Les menaces passives n'influence pas ni sur le fonctionnement du système ni sur les informations transmises (ex : Espionnage), par contre les menaces actives effectuent des modifications sur les données et le travail du réseau (ex : Interruption).

Q : Quel est le principe de chiffrement ?

R : Le chiffrement est une technique qui consiste à rendre un message illisible en se basant sur deux éléments : Une clé sous forme d'une suite binaire, et un algorithme qui va combiner la clé et l'information pour la crypter (ex : Chiffrement de César).

Q : Quelles sont les différents systèmes de cryptographie ? Donner des exemples d'algorithmes de chiffrement utilisés.

R : Les systèmes de cryptographie sont séparés en deux catégories :

1- Système symétrique : également dit à clé secrète, est la plus ancienne forme de chiffrement. La clé utilisée permet de chiffrer et déchiffrer les messages. Il présente l'avantage d'être rapide mais il présente un certain nombre d'inconvénients comme l'augmentation du nombre de clé en fonction des utilisateurs. Ex : DES.

   DES (Data Encrypting Standard) : c'est un algorithme de chiffrement par blocs utilisant une clé de 56bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit. L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés individuelles de 56 bits, représentées par 64 bits (avec un bit de chaque octet servant pour le contrôle de parité). D'une manière générale, on peut dire que DES fonctionne en trois étapes :
   a. permutation initiale et fixe d'un bloc.
   b. le résultat est soumis à 16 itérations d'une transformation, ces itérations dépendent à chaque ronde d'une autre clé partielle de 48 bits. Cette clé de ronde intermédiaire est calculée à partir de la clé initiale de l'utilisateur. Lors de chaque ronde, le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre. Le bloc de 32 bits ayant le poids le plus fort subira une transformation.
   c. le dernier résultat de la dernière ronde est transformé par la fonction inverse de la permutation initiale.

2- Système asymétrique : est un système de chiffrement qui utilise généralement une clé publique pour coder le message, et une autre clé privée qui permet de décoder le message ce qui assure l'authentification de l'émetteur et la confidentialité de données. Ex : RSA.

RSA : La méthode repose sur un constat très simple : il est facile d'effectuer la multiplication de deux nombres premiers, mais il est très difficile de retrouver les facteurs quand le résultat est grand. La clé publique est donc constituée du produit n de deux nombres premiers p et q, choisis très grands. La clé secrète dépend directement de p et q et ne peut donc être déduite de la clé publique.

Q : Donner les caractéristiques principales d'un algorithme cryptographique.

R :

- Réversibilité : L'algorithme doit être réversible pour permettre au destinataire d'appliquer la transformation inverse afin de retrouver le clair du message crypté. Sans cette option, il est impossible de décrypter le message.
- Symétrie : L'algorithme utilisant une même clé pour chiffrer et déchiffrer l'information, est appelé algorithme symétrique. Sinon, si le chiffrement et le déchiffrement s'effectuent par deux clés qui sont en relation, alors dans ce cas l'algorithme est asymétrique.
- Mode de chiffrement : Le chiffrement est réalisé par deux méthodes : Le chiffrement par blocs (Application de l'algorithme bloc par bloc) et celui par flux (Chaque élément binaire est chiffré).
- Résistance : Un algorithme de chiffrement doit être résistant à toutes menaces des décrypteurs, la résistance est liée au temps nécessaire pour trouver déchiffrer un message.
- Publication : Tous le monde peut se servir du service fournis par cet algorithme.
- Implémentation : l'implémentation d'un algorithme sous forme d'un logiciel, garantie la portabilité.
- Autorisation de mise en œuvre.

Q : C'est quoi un pare-feu, un système IDS et une zone DMZ ?

R :

Le pare-feu ou le Firewall est un outil qui contrôle le trafic réseau et qui fonctionne aux niveaux 3 et 4 du modèle OSI et aide à bien sécurisé les réseaux locaux. Il permet de filtrer les adresses IP en se basant sur plusieurs paramètres : IP source, IP destination, port source, port destination, protocole de niveaux 3 et 4.

Les IDS se sont des systèmes de surveillance qui sont capable de détecter des activités anormales et les intrusions soit au niveau réseau (NIDS) soit au niveau hôte (HIDS).

La zone DMZ est un espace très protégé par plusieurs composantes de sécurité à savoir les pare-feu, les systèmes de détection d'intrusion IDS et les hyperviseurs de sécurité.

MTU (Maximum Transfer Unit) : le nombre de blocs d'informations qu'un média supporte. MTU doit être respecté dans chaque transmission

ICMP (Internet Control Message Protocol) : est un protocole de maintenance utilisé pour les tests, qui véhicule des messages de contrôle. IL permet à deux systèmes d'un réseau IP de partager des informations d'état et d'erreur (ex: La commande PING utilise les paquets ICMP).

Ethernet (IEEE802.3) est le standard de transmission de données pour les réseaux locals basé sur le principe suivant: Tous les machines du réseau Ethernet sont connectées par le meme support physique (ex: 10baseT, 100baseTX, 100baseFX, 1000baseT…). Les communications dans un réseau Ethernet sont gérées par le CSMA/CD qui évite que deux stations utilise le medium physique simultanément. Un réseau Ethernet est donc un réseau à caractère probabiliste car il n'y a pas de chef d'orchestre pour synchroniser les émissions ce qui indique qu'il n'y a pas de priorité.

Le TTL ou "Time To Live" (8 bits) est l'expression en secondes de la durée maximale de séjour du paquet dans un réseau. La plupart des routeurs se contentent de décrémenter le TTL d'une unité. Si le TTL devient nul, son paquet IP n'est plus relayé : c'est souvent l'indication d'une erreur de paquet qui boucle. La valeur TTL recommandée est comprise entre 40 et 64

Chiffre de césar :

Le code César est la méthode de cryptographie la plus ancienne, il consiste à une substitution mono alphabétique où la substitution est définie par un décalage de lettre. Par exemple A devient F,B devient G,… l'inconvénient c'est qu'il ya 25 décalage possible ce qui rend le déchiffrement d'un information cryptée par le chiffre de césar très facile.

Chiffre de Vignère :

c'est un système qui utilise la substitution ploy alphabétique. Son principe est: Dans un tableau dit carré de Vignère, on remplace la lettre de message à chiffrer par celle obtenu à l'intersection de la colonne repérée par cette lettre, et de la ligne définie par la lettre de la clé associée à la lettre du message.

Algorithme de vernam?

Les paramètres qui rend une connexion unique: {Protocole, @Dest, @Source, P.Dest, P.Source}

Objets de sécurité:

- L'information
- Le système
- Le réseau

Un mécanisme de sécurité est conçu pour détecter, prévenir et lutter contre une attaque de sécurité.

• Interruption: vise la disponibilité des informations
• Interception: vise la confidentialité des informations
• Modification: vise l'intégrité des informations
• Fabrication: vise l'authenticité des informations

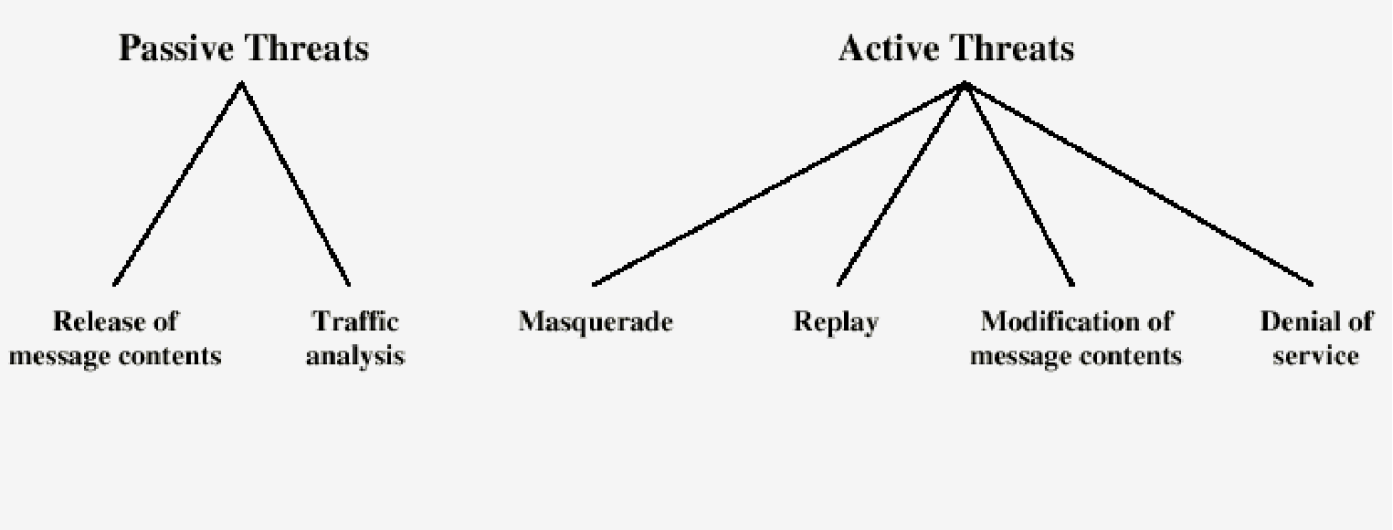

Figure 1.2 Active and Passive Security Threats

Services de Sécurité
• Confidentialité : les données (et l'objet et les acteurs) de la communication ne peuvent pas être connues d'un tiers non-autorisé.
• Authenticité : l'identité des acteurs de la communication est vérifiée.
• Intégrité : les données de la communication n'ont pas été altérées.
• Non-répudiation : les acteurs impliqués dans la communication ne peuvent nier y avoir participé.

• Disponibilité : les acteurs de la communication accèdent aux données dans de bonnes conditions.

Mécanismes de défense
• Chiffrement : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
• Signature numérique: données ajoutées pour vérifier l'intégrité ou l'origine des données.
• Bourrage de trafic : données ajoutées

• Antivirus : logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
• Le pare-feu : un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
• Détection d'intrusion : repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs.
• Journalisation ("logs") : Enregistrement des activités de chaque acteur.

Quelle est la fonction d'un firewall ?
Un firewall est un (ou plusieurs) dispositif(s) qui assure(nt) le respect d'une politique de sécurité entre un réseau privé et l'Internet. En ce sens, il est plus évolué que le routeur qui lui transmet juste les données. L'objectif d'un firewall est double, il permet :
De protéger le réseau interne contre les tentatives d'intrusion provenant de l'extérieur.
De limiter et vérifier les connexions provenant du réseau interne vers l'extérieur.
À l'origine, un firewall est un système comportant au minimum deux interfaces réseau permettant ainsi la sécurisation d'un réseau interne. On distingue alors l'interface externe (Reliée à l'Internet) et l'interface interne (reliée au réseau local).

Le serveur doit créer un socket, lui attacher un numéro de port et attendre une connexion.
La couche session est la responsable de l'ouverture et la fermeture des ports.

Commande de configuration réseau :

```
Router> en
Router# configure
Router (config) # interface eth0
Router (config-if) # ip address @ip @masque
Router (config-if) # no shutdown
```

Router (config) # router rip
Router (rip) # network @ address 1
Router (rip) # network @ address 2
Router (rip) # network @ address n

Router (config) # ip route @cible @masque @sortie
Router (config) # ip route 0.0.0.0 0.0.0.0 @sortie
Router (config) # no ip route @cible @masque @sortie

Ifconfig : permet d'afficher la configuration réseau de l'interface
arp -s (ajouter une entrée statique), exemple : **arp** -s 192.168.1.2 00:40:33:2D:B5:DD
arp -d (supprimer une entrée), exemple : **arp** -d 192.168.1.2

route:
Le routage définit le chemin emprunté par les paquets entre son point de départ et son point d'arrivée.

route add [net | host] addr [gw passerelle] [métric coût] [netmask masque] [dev interface]
route add 152.1.25.0 addr 192.168.0.2.3 4   255.255.255.0 eht0
route add default gw 192.186.2.3

ip route 0.0.0.0 0.0.0.0 @gw
route add -net 192.56.76.0 netmask 255.255.255.0 eth0   (UNIX)

La commande traceroute permet d'afficher le chemin parcouru par un paquet pour arriver à destination

Les fichiers de configuration

Les fichiers de configuration

Nom fichier	Description
`/etc/hosts`	Correspondance entre adresses IP et noms de machine
`/etc/inetd.conf`	Liste des services TCP/IP et ports associés
`/etc/protocols`	Liste des protocoles installés sur la machine
`/etc/networks`	Correspondance entre adresses IP et noms de réseaux
`/etc/netmasks`	Masque de l'adresse IP pour définir les sous-réseaux
`/etc/services`	Liste des services TCP/IP

Le fichier `/etc/hosts`

Le fichier `hosts` donne un moyen d'assurer la résolution de noms, de donner un nom FQDN à un hôte

Exemple de fichier `hosts`

```
127.0.0.1  localhost localhost.localdomain
192.168.1.1  uranus.foo.org uranus
```

Le fichier `/etc/networks`

Il permet d'affecter un nom logique à un **réseau**

```
localnet   127.0.0.0
foo-net 192.168.1.0
```

Cette option permet par exemple d'adresser un réseau sur son nom, plutôt que sur son adresse.

route `add` ***foo-net*** au lieu de **route** `add -net` ***192.168.1.0***.

Le fichier `/etc/host.conf`

Il donne l'ordre dans lequel le processus de résolution de noms est effectué. Voici un exemple de ce que l'on peut trouver dans ce fichier :

```
order hosts,bind
```

La résolution est effectuée d'abord avec le fichier `host`s, en cas d'échec avec le DNS.

Le fichier `/etc/resolv.conf`

Il permet d'affecter les serveurs de noms.

Exemple

```
Nameserver 192.168.1.1
Nameserver 192.168.1.2
Nameserver 192.168.1.3
```

Ici le fichier déclare le nom de domaine et les 3 machines chargées de la résolution de noms.

Les fichiers de configuration des interfaces réseau

Vous trouverez ces fichiers dans `/etc/network/interfaces`. Voici un exemple qui contient 3 interfaces.

```
# /etc/network/interfaces -- configuration file for ifup(8), ifdown(8)
```

```
# The loopback interface
# automatically added when upgrading

auto lo eth0 eth1

iface lo inet loopback

iface eth0 inet static
        address 192.168.90.1
        netmask 255.255.255.0
        network 192.168.90.0
        broadcast 192.168.90.255
        gateway 192.168.90.1

iface eth1 inet static
        address 192.168.0.1
        netmask 255.255.255.0
        network 192.168.0.0
        broadcast 192.168.0.255
```