Introduction Aux Réseaux

Contents

Introduction

Qu'est-ce qu'un réseau ?

Un réseau est une interconnexion de devices.

un device est utilisé pour comminuquer avec les autres devices via un **médium**. Ils échangent donc des **messages** en suivant des règles qui gouvernent comment les messages sur le réseau. ces règles sont appelées **protocols**.

En ce qui concerne les protocoles réseaux, toutes les activités de communication sont basées sur des normes et des standards.

Une communication oritntée connexion commence par une **ouverture de connexion**, puis une **transmission de données** et enfin une **fermeture de conexion**.

Transmission Simplex : transmission dont le sens de transmission va uniquement d'une source vers un récepteur.

Communication Full Duplex : permets aux deux participants dêtre à la fois émétteurs et récepteurs simultanément.

Application opportuniste : application qui s'adapte aux ressources réseaux disponnibles.

Communication de circuit : réservation du canal de transmission durant toute la Communication.

WPAN : Wireless Personnal area Network

Quels sont les caractéristiques d'un bon réseau ?

Un bon réseau est caractérisé par sa capacité à résister aux pannes (**fault tolerance**). Il doit pouvoir être étendu (**scalabilité**). Il doit fournir des services avec une certaine qualité (**quality of service**). il doit être **sécurisé**

Pour achever ces différentes choses, il est plus facile de procéder si le réseau est hierarchisé et fonctionne suivant des standards et protocols.

Quality of Service

La Quality Of service est une méthode de priotité des paquets réseaux. On priviligie généralement les applications qui ont besoin de plus de bande passante. On effectue une prioritisation des paquets réseaux en augmentant la fréquence d'émission de ceux-ci. (ex : des mails sont moins importants en terme de fluidité qu'une conversation skype).

LAN vs WAN

LAN : Local Area Network (Maison, Bâiment, campus)
WAN : Wide Area Network (LAN's séparées par une distance géographique)

Si leur limite peut sembler floue, il est assez facile de repérer et différencier un lan d'un wan. Malgré une forte ressemblance, ils se différencient par leurs différents **responsables de gestion**, leurs **débits** et leurs **appareils représentatifs** (switch vs router)

Modèle OSI VS TCP/IP

Les avantages de la définition d'un modèle commun pour la création des réseaux réside dans le *design*, l'*upgradabilité* et l'*uniformité* des segments composant les réseaux.

PDU (Protocol Data Unit) et l'encapsulation

Le pdu et l'encapsulation définissent comment une donnée doit être "entourée" d'information supplémentaire pour pouvoir voyager dans une couche suivant un standard bien précis.

Le modèle OSI

Le modèle OSI (et leurs PDU):

- Application : "les données" : "Contient les protocols applicatifs"
- Présentation : "les données" : "Syntaxe et sémantique, traduction"
- Session : "les données" : "Synchronisation source et destination, gestion des points de reprises"
- Transport : "Le segment" : "La transmission correcte de données (corriger, réordonner, acquitter)"
- Network : "Le paquet" : "Routage et transmission de bout en bout (source vers destination)"
- Data link : "La trame" : "Transfert fiable de données entre éléments actifs du réseau"
- Physical : "le bit" : "Transmission de bits"

Le modèle TCP/IP

Le modèle TCP/IP :

- Application : représente les données jusqu'à l'utilisateur plus l'encodage et le contrôle de dialogue.

- Transport : Supporte la communication entre divers devices au travers de réseaux diverses.
- Internet : Détermine le meilleur chemin à travers le réseau (routage , communication de bout en bout, ...).
- network access : Contrôle le hardware et le media qui constitue le réseau (wifi, bluetooth, ...).

Cependant un modèle parfait est impossible à atteindre mais il au plus le réseau tend vers le modèle au plus il se rapproche de ce qu'il peut effectuer de mieux.

Les différents rôles du modèle en couche

Le rôle du modèle en couche est de fournir une approche universelle au transport de données. chaque couche de données possède la possibilité d'encapsuler les données.

Ainsi, les données envoyées d'un device vers un autre seront encapsulées à mesure de leur descente dans le modèle, pour arriver au niveau 1 (couche physique) ou il sera transporté avant d'être "désencapsulé"" par l'autre device.

Couche 1 : Couche physique

Cette couche gère la **Mise en Oeuvre Matérielle**

La couche physique regroupe le support (cable en cuivre, fibre optique, ...) et la manière dont l'information est transportée (ex : en amplitude, en fréquence, ...)

Modulation : adapter un signal digital pour le convertir en un signal analogique.

WDM : *WaveLength division multiplexing* : transmettre plusieurs signaux simultanément sur des fibres multimodes.

STP : Shielded twisted pair **UTP** : Unshielded twisted pair

ISDN(RNIS)

Dans une connexion ISDN(RNIS). On a deux canaux B à 64Kb/s et un canal D à 16Kb/s et permets de gérer l'ouverture et la fermeture de connexion

Representation d'un signal sur un support

Pour représenter un signal sur un support, il existe une série de méthodes dont les varation d'**amplitude**, de **fréquence** et de **phase**

L'horloge

L'horloge est une fréquence d'un système utilisée pour permettre la synchronisation d'une communication entre l'émetteur et le récepteur. Ajouter un cable supplémentaire pour l'horloge pourraît être une bonne idée mais cette méthode ajouterait un cable (plus cher) et ne serait pas optimale. Actuellement, le hardware est capable de gérer sa fréquence directement.

Le bit

Dans cette couche, les données sont représentées sous la forme de bits, certaines suites spécifiques de bits indiquent le début et la fin d'une transmission de données.

Problèmes de transmission

L'atténuation : perte d'énergie du signal pendant sa propagation

La **distorsion** : suite à l'utilisation de différentes fréquences il est possible que l'une altère l'autre en se chevauchant même un cours instant

Le **bruit** : tout signal indésirable qui livre au récepteur une information incohérente.

Le signal parfait n'existe donc pas, il faut dés lors mettre en place des systèmes qui permettent de déceler les erreurs.

Bande passante

La **bande passante** est la capacité théorique d'un réseau en bits/sec.

Le **débit** de données correspond aux performances réeles d'un réseau.

Le **débit applicatif** est une mesure du transfert de données utilisables après suppression du trafic de surcharge du protocole.

Matériaux et technologies

- Fibre optique : coeur de verre qui transporte le signal sous forme de lumière
  - Monomode : 1 seul rayon (transmission longue distances)
  - Multimode : plusieurs rayons différents
- Cuivre : transmission de données sous la forme d'un signal éléctrique
  - RJ45
  - COAXIAL
- Sans-Fil : transfert via ondes électromagnétiques
  - Bluetooth
  - Wifi
  - GSM

Cable Coaxial

Le câble coaxial est composé de :

- la gaine (ext.): protège le câble de l'environnement extérieur (caoutchouc, . . .);
- blindage: enveloppe métallique entourant le câble qui protège le données transmises sur le support des parasites;
- l'isolant: permet d'éviter tout contact entre le blindage et le conducteur (pas de court-circuit possible);
- fil de cuivre (âme): a la tâche du transport des données et est composé généralement d'un seul fil de cuivre ou de plusieurs brins torsadés.

Le théorème de Nyquist

On peut transmettre le signal sans erreur aucune si on le mesure avec une fréquence qui est le double de la fréquence maximale du signal de départ

Couche 2 : Data link layer

La **Couche 2** gère la mise en oeuvre matérielle et Logicielle.

Une **trame** est le nom donnée aux données qui transites par la couche 2.

Cette couche à pour but de gérer l'accès au support. elle fait le lien entre le hardware et le software de la couche 1. Un bon exemple de la couche 2 est la carte réseau.

Gérer l'accès au média Désigne la préparation de la communication pour la transmission sur un média spécifique. Une espèce de formatage de la trame pour l'adapter au média

Gérer l'accès au réseau désigne les stratégies mises en place pour la communication (en étoile , maitre-esclave, tour par tout, acces simultané (attention aux collisions))

Les transmissions émises via la technologie **Courant Porteur en Ligne** sont sujettent aux interférences car les câbles électriques ne sont pas torsadés

Piconet : Réseau bluetooth qui est composé d'*un maitre* et de *plusieurs esclaves*.

protocols déterministes : Token Bus, Token Ring, FDDI, Fiber channel.

Accès aléatoire : solution pour un accès multiple au canal de transmission.

WaveLength Division Multiplexing : partage

Transmision STP

Transmission STP : port racine et ports désignés actifs.

Le STP désactive logiquement les liens physique dans un réseau cmposé de switch pour éviter des boucles.

IEEE

802.1D : Spanning tree protocol

30 à 60 microSec pour la création d'un arbre

802.3 : Ethernet

Optimiste en CSMA/CD. Le temps de référence pour éviter les collisions est de 51.2 microSec.

802.4 : Token Bus

Deterministe

802.5 : Token Ring

Déterministe, capture de jeton, anneau logique et un anneau physique

802.11b : Wlan Wifi

Optimiste en CSMA/CA

On évite les collisions via le Virtual carrier pass : RTS/CTS

802.15 : Bluetooth

Sa spécification correspond à un usage particulier.

802.16 : WIMAX

Traitements

A la réception, une **trame** est considérée **correcte** si elle est composée d'un **délimiteur de début**, est composée d'un **délimiteur de fin**, de **longueur correcte** (telle qu'annoncée dans la trame), a une **somme de contrôle correcte**

Il existe deux méthodes au niveau de la couche *liaison de données* afin de traiter les *retransmissions*.

Arbitrated loop : 3 architectures gérées par le Fiber channel.

Arbre de recouvrement

Un réseau est un arbre de recouvrement si il ne contient pas de boucles et est suffisant que l'on puisse atteindre toutes les stations du réseau (délai de mise en oeuvre d'un arbre minimum est compris entre 30 et 60).

Go Back N

L'idée derrière le principe de **Go-Back-N** est de *recommencer* la transmission à la trame *perdue* en « ignorant » que l'on a déjà transmis certaines trames et ce même si celles-ci ont bien été *reçues*.

On retransmet donc la trame perdue et toutes celles que l'on avait déjà transmises. Ceci a comme avantage de ne pas demander de *ressources* particulières du côté du receveur et est *facile* à implémenter. Comme désavantage on notera une baisse de rapide de *la performance* dés que *le taux d'erreurs* sur la ligne physique augmente.

Selective Repeat

La 2ème méthode, **Selective Repeat**, est basé sur le fait que ne seront retransmises que *les trames* perdues et uniquement les trames *perdues*. On évite donc de retransmettre inutilement des trames déjà transmises et reçues correctement à la destination. *Selective Repeat* a donc de meilleures performances que *Go-Back-N* lorsque la couche physique est mauvais.

L'implémentation en est plus complexe : le récepteur devant *stocker* dans un buffer les trames reçues hors séquence et les réordonner avant de les *délivrer* à la couche supérieure.

MAC adress

MAC : Medium access card : 6 bytes (type : XX:XX:XX:XX:XX:XX).

L'exemple de L'ethernet

Dans le protocol ethernet, on identifie chaque device du réseau par sa **mac adresse**.

A l'origine, les réseaux ethernet étaient disposées en bus. Le transfert de données en bus est une communication autour d'un médium (ex :coaxial) partagé par plusieurs pc. Ils fonctionnenet en CSMA/CD que plusieurs pc se partagaient. c'est à dire que quand un pc voulaient communiquer avec les autres, il devait :

- vérifier que personne ne transmettait de données avant d'en émettre.
- Puis émettre publiquement en spécifiant le destinataire en ayant confiance dans le fait qu'il n'y ait que l'utilisateur à qui le message est destiné qui lise celui-ci.
- Si deux communications venaienet à entrer en collision, les 2 devices lancent un timer aléatoire et réesayeront quand celui-ci sera terminé.

> *10 base 2* et *10 base 5* représentent respectivement le thin et le thick internet qui sont de 200m de cable à 500m de cable pour le thick.

Le bus sous la forme d'un cable à ensuite été remplacé par un hub. qui fonctionnait sur le même principe mais qui offrait des coûts bien plus avantageux.

——— image bus de communication

Le désavantage de ce système de communication logique en bus est l'impossibilité de communiquer à plusieurs à la fois et de ne pas savoir émettre et recevoir. cet ancien modèle (**half duplex**) à fait place au modèle 10 base T (t pour twisted pair) qui est un full duplex. qui utilise aussi le CSMA/CD.

Sans fil Wifi

2 types architectures : * infrastructure * Wifi

CSMA

CSMA/CD

Collision detection. EX 802.11g ### CSMA/CA collision avoidance

Switch

Un Switch est un équipement réseau lié à la *couche 2* qui permets la mise en oeuvre de plusieurs domaines de collision.

Un switch fonctione comme un hub à la différence prêt qu'il est capable de fonctionner en full duplex grâce à une table de correspondance des macs adresse et de ses ports physiques permettant une transmission en simultané entre plusieurs devices sans envoyer à tout le monde les messages.

transfert d'informations sur un médium

- Unicast : 1 à 1
- Multicast : 1 à plusieurs
- Broadcast : 1 à tous (s'étend jusqu'à rencontrer un router)

Remplissage de la Mac Table

1. La mac table est vide

2. Un ordinateur émet (la table ajoute la mac et son port physique) (**Learning**)
3. On broadcast sur le réseau(**Floading**) (si le message nous est destiné, on envoie une réponse(**Selective Forwarding**). On drop le message si ce n'est pas le cas.)

La forte tolérance aux pannes du protocole FDDI est dûe principalement à la double boucle contrarotative

Méthode d'accès optimistes ou aléatoires

- CSMA/

Types de protocols d'accès multiples au canal de transmission

Il existe trois types de protocole d'accès multiple au canal de transmission :

```
Le [partage / partitionnement du canal de transmission
L'accès aléatoire (CSMA/CD, [CSMA/CA, ...)
La [rotation (l'attente de son tour ou du jeton)
```

Il est aussi possible de différencier ces accès multiples au canal de transmission selon que la solution soit statistique ([optimiste) ou [déterministe (pessimiste).

Pour ce qui des solutions [optimistes, on laisse les ordinateurs transmettre plus ou moins à [leur guise en espérant qu'un seul ne transmettra à la fois. Cet algorithme est distribué et est conçu pour résoudre le problème des [collisions (qui seront inévitables).

D'un autre côté, pour les solutions [déterministes, on veut à tout prix éviter que deux ordinateurs ne transmettent en même temps. Une [autorisation à émettre est donnée, le jeton, pour qu'un seul appareil ne transmette à la fois. Cet algorithme est aussi [distribué et permet de gérer [l'anneau et le jeton.

La capacité à se mouvoir entre plusieurs points d'accès disposés de telle sorte que les clients puissent se déplacer sur toute la zone de couverture de manière invisible et sans perte de connexion s'appelle le **roaming**.

Le mécanisme de retransmission "Selective Repeat" a comme fonction de redemander la transmission de toutes les trames transmises depuis la dernière bien reçue en séquence. –> faux Redemander uniquement les trames non ou mal reçue.

Avant de transmettre une trame, une station participant à un réseau 802.5 Token Ring doit d'abord écouter le canal de transmission et ensuite capturer le jeton.– faux : Pas d'écoute du canal de transmission pour les protocoles déterministes

Au niveau des protocoles de la couche Liaison de Données, à quoi sert le timer associé à l'échange des trames ? A détecteur les erreurs de transmission

La méthode permettant de profiter d'une trame de données dans une communication bidirectionnelle pour acquitter (ACK) une trame de données du sens inverse est nommée Piggy-Back.

La méthode d'accès de type CSMA/CA fait partie des méthodes d'accès optimistes au canal de transmission.

Le champ [ACK présent dans une trame de données sert A acquitter une trame précédemment reçue

Une trame 802.3 Ethernet doit avoir une longueur minimale permettant ainsi de détecter les collisions pendant sa transmission sur le canal de transmission.

La technologie Courant Porteur en Ligne utilise comme canal de transmission ; le câblage électrique

Dans la cadre du protocole 802.5 et son anneau physique, une station a un rôle particulier dans la gestion de l'anneau. Elle se nomme le moniteur

Non répondue Noté sur 1,00 Marquer la question Texte de la question

Avant de transmettre une trame, une trame participant à un réseau 802.4 Token Bus doit d'abord écouter le canal de transmission. – > faux

Trunking : agréggation de plusieurs vlans sur une même ligne.

Le switch utilise la mac source contenue dans la tramme pour compléter sa mac table. Il permets de créer différents vlans sur base de leurs ips

Couche 3 : Network

Une **paquet** est le nom donnée de données qui transites par la couche 3.

Le routeur est l'appareil représentatif de cette couche

L'objectif principal de la couche réseau est d'acheminer les paquets de la source à la destination.

ARP : Le protocole qui permet d'obtenir une adresse MAC sur base d'une adresse IP
ICMP : Le protocole qui permet de gérer les erreurs de la couche Internet
BGP-4 : protocole de type Exterior Gateway Protocol et permet le routage de paquets IP entre Autonomous System **IP** : Le protocole qui permet le transfert de la source à la destination (de bout en bout) d'un paquet
OSFP : Le protocole qui permet l'établissement dynamique de tables de routage sur base du principe du "Etat de liaisons". **RIP** : Le protocole qui permet l'établissement dynamique de tables de routage sur base du principe du "vecteur de distance"

IP Header + Segment = paquet

Taille adresse IPV4 : 32 bits = 4 bytes Taille adresse IPV6: 128 bits = 16 bytes

En IPv4, une adresse IP est constituée d'une partie "réseau" et d'une partie "hôte" le tout sur une longueur de 32 bits.

Dans un paquet IPv4, les champs "Drapeau" (flag) et "Position relative" (offset) servent à réordonner à destination les fragments d'un même paquet.

Le routage dynamique qui établit le plus court chemin entre deux hôtes sur base du nombre de saut (hop) est le routage par vecteur de distance.

Le protocole BGP-4 est un protocole de type Exterior Gateway Protocol et permet le routage de paquets IP entre Autonomous System.

L'échange de messages LSP est une des étapes nécessaires pour établir des tables de routage selon le principe du routage par Etat de liaisons

Lorsque le champ Time-To-Live (TTL) d'un paquet IPv4 est égal à 0 (zéro) : il est jeté par le routeur

NAT : Network address Translation. Un des procédés mis en place pour pallier au manque d'adresse IPv4 et dont le principe est de "traduire" une adresse IPv4 privée en une adresse IPv4 routable sur Internet.

ConnexionLess (Sans connexion)

Aucune connexion n'est établie avant d'envoyer les paquets de données

L'expéditeur ne sait pas:

- si le récepteur est actif et Présent
- si le récepteur est arrivé
- si le récepteur sait lire le message

Le récepteur ne sait pas: quand le message arrive

Best Effort (au mieux)

Rien n'est fait pour garantir la réception des paquets. Son but est de garantir le transport le plus rapide possible avec le moins de pertes possibles.

Indépendance par rapport au média

Peu importe le média physique utilisé. > > fibre optique, cuivre, ethernet, ...

L'importance des réseaux et sous-réseaux

La subdivision permets de **faciliter l'administration** réseau. Elle influence aussi les **performances** et la **sécurité**. En subdivisant, on réduit le domaine de broadcast et celà nous permets de mettre en place des mesures de protection (ex : firewalls)

Adresses IPV4

XXX-XXX-XXX-XXX sur 32 bits (reseau)-(reseau)-(sousréseau)-(hôte)

Routage et commutation

Le routeur et le commutateur (ex : switch) se diffèrent par leur implication dans le transport de données

Fonction	Router	commutateur
Vitesses	Lent	Rapide
couches OSI	Couche 3	Couche 2
Adresses	IP	MAC
Broadcast	Bloqués	Transmis
Sécurité	Elevées	Faible

Rôle des périphériques intermédiaires : l'importance de la paserelle

La paserelle fait la liaison entre deux réseaux (internet et local). Une **route** est un *réseau de destination*, un *masque* et *la gateway (paserelle).*

Flux de données

Lors de l'arivée dans un noeud du reseau :

1. supprime l'encapsulation de couche 2
2. Extraction de l'ip de destination
3. Recherche de correspondance dans la table de routage
4. Si le Reseau est trouvé
5. Réencapsulation
6. Envoi

Recherche dans la table de routage:

- trouves : ok
- trouves pas: on vérifie la Porte par défaut :
- Oui : Ok
- non : On abandonne

Adressage IP

Classes

- classe A : ### Le Masque

Deux organisations existent au sein de la couche réseau. La première est la vision des opérateurs de téléphonie classique qui se base sur le principe « orienté connexion et fiable ». Cette organisation nécessite une ouverture de connexion à laquelle est associée une négociation de paramètres de connexion. Une communication bidirectionnelle complétée du respect de la séquence des paquets émis constitue le transfert de données. Le contrôle de flux et la fermeture de connexion sont d'autres éléments qui caractérisent cette organisation de la couche réseau. Il s'agit d'un réseau à commutation de circuits ou à circuits virtuels

La deuxième organisation, sans connexion et non fiable, est le choix fait pour Internet. Cette approche permet de limiter la complexité de la couche réseau qui

implique de facto des pertes de données, des données dupliquées ou réordonnées. Si besoin est d'une certaine fiabilité, celle-ci sera assumée au mieux soit par la couche transport ou par la couche application. Il s'agit ici d'un réseau à datagramme ou à commutation de paquets.

La deuxième méthode d'établissement dynamique de table de routage est basée sur le principe "Etat de liaisons". L'objectif est obtenir une topologie complète du réseau. Quatre étapes sont nécessaires pour obtenir les tables de routage permettant d'acheminer les paquets par le meilleur chemin.

Il est donc nécessaire, pour un routeur, de découvrir ses voisins: ceci est réalisé via l'envoi d'un message "Hello" sur tous ses liens. Il est aussi nécessaire de déterminer le délai pour atteindre ces voisins : le message "Hello" et sa réponse permettent de déterminer cet élément. Un point est à garder en mémoire : doit-on ou non tenir compte de la charge de la ligne en faisant passer le message "Hello" en tête ou en fin du buffer d'envoi ?

Ces informations (reprenant une topologie partielle du réseau) sont assemblées en un message spécifique (Link State Packet) envoyé à tous les autres routeurs du réseau par le principe de flooding.

Les routeurs récoltent ainsi les LSP et les assemblant chacun pour obtenir une topologie complète du réseau et établir via l'algorithme de Dijkstra (Théorie des graphes) les tables de routage.

Que ce soit un réseau à circuits virtuels ou commutation de paquets, il est nécessaire d'avoir un adressage unique pour permettre une communication entre tous les équipements participants au réseau.

Dans un réseau basé sur le protocole IP, que ce soit en IPv4 ou en IPv6, il est difficile de retenir une adresse IP. C'est pourquoi un nom peut-être associé à une adresse IP afin d'en faciliter la mémorisation et donc l'utilisation. Des protocoles applicatifs seront donc mis en place pour permettre de gérer la distribution d'adresses IP ainsi que la résolution du nom en une adresse IP.

Une adresse IPv4 est constituée de 32 bits dont la notation est décimale par octets séparés par un point (.). Il est donc théoriquement possible d'adresser plus de 4 milliards d'hôtes.

Une adresse IPv6 est quant à elle constituée de 128 bits avec une notation hexadécimale par 16 bits séparé par un double point (:). Il est possible via ces 16 octets d'adresser plus de 3.4 x 10 exposant 38 hôtes.

—

Il est nécessaire que l'établissement dynamique des tables de routage puisse se faire avec un niveau de convergence très bas et en étant capable de s'adapter aux événements du réseau : ajout de liens, de routeurs ou pannes.

Pour la méthode "vecteur de distance", les routeurs détectant une panne d'une ligne enverront un vecteur de distance annonçant une distance infinie pour les destinations utilisant cette ligne.

Néanmoins cette méthode a ses limites (si plusieurs pannes) : les routeurs concernés risquent de s'annoncer l'un l'autre la possibilité d'atteindre la destination en augmentant à chaque itération la distance pour arriver à destination. Un comptage infini en est le résultat.

Pour pallier à cet effet non désiré, il est possible d'utiliser l'horizon partagé avec ou sans empoisonnement. Le principe de base est identique : ne pas avoir un vecteur par routeur mais bien un vecteur par ligne active. Ligne active sur laquelle on n'annonce pas les destinations que l'on peut atteindre via cette ligne (sans empoisonnement) ou avec une distance infinie (avec empoisonnement).

—

Le routage, au niveau de la couche réseau, est un élément important dont l'objectif est d'acheminer les paquets depuis la source jusqu'à la destination. Ceci ne peut être réaliser que s'il est possible d'établir le meilleur chemin entre les source et destination.

Il est donc nécessaire de mettre en place au sein des routeurs, de manière statique ou dynamique, des tables de routages au plus proche de la réalité du terrain.

Statiquement il est effectivement possible d'établir des tables de routage mais seulement dans un environnement réseau maitrisé.

En ce qui concerne le routage dynamique deux méthodes existent : vecteur de distance et état de liaisons.

Pour la méthode vecteur de distance, le routeur envoie à intervalle régulier un vecteur contenant les informations "adresse de destination" et "distance jusqu'à cette adresse". Le vecteur reçu par un routeur est complété des meilleures informations à disposition du routeur et envoyé aux autres routeurs du réseau. L'assemblage des divers vecteurs de distance via l'algorithme de Ford-Bellman (théorie des graphes) permet de déterminer les meilleures routes et de facto les tables de routages.

Chapitre 4 : Couche transport

Pas d'appareils représentatifs.

Le but de la triple poignée de mains pour l'ouverture de connexion TCP est de synchroniser les numéros de séquence, les numéros d'acquit et d'échanger la taille des fenêtres TCP.

Le contrôle de flux associé au protocole TCP est aussi appelé le principe de Fenêtre glissante

La couche transport offre deux types de services : sans connexion non-fiable et orienté connexion fiable.

L'adressage utilisé au niveau de la couche transport, le port, peut avoir une valeur entre 1 à 65535. Un certain nombre de ces ports est réservé pour les ports "bien connus" (Well Known ports). Lequels ? Les 1024 premiers

A chaque envoi d'un segment un temporisateur est enclenché afin de s'assurer de la bonne réception du segment par la destination.

La retransmission des segments TCP (TPDUs) perdus peut se faire via le principe du GO-BACK-N ou Selective Repeat

Slow Start : mécanisme de résolution pour pallier au problème de congestion qui peut survenir entre la source et la destination lors de l'utilisation de TCP.

Le protocole UDP n'apporte aucune garantie de service.

Le protocole UDP, recommandé mais pas obligatoire, peut-être considéré comme un simple dispatcheur entre la couche réseau et la couche application.

Le valeur du temporisateur de retransmission dans le cadre de TCP est basé sur le RTT et sur l'estimation de sa variance, la valeur du timer est donc variable

La **problématique des 2 armées** se pose lors de la fermeture asymétrique d'une connexion.

La charge maximale d'un segment UDP (quantité de données transmises) est de 512 bytes.

Afin de garantir un bon compromis entre délais et attente d'envoi pour TCP, il est nécessaire de définir quand il est judicieux d'envoyer un segment de données ou un acquit.

En ce qui concerne les acquits, on pourrait soit le faire dés qu'un segment TCP est reçu, soit en profitant de la méthode Piggyback.

Le compromis mis en place pour l'envoi des acquits est le suivant : si le segment TCP est reçu est en séquence et si c'est le seul segment TCP à acquitter, on attend soit l'envoi d'un segment TCP de données (Piggyback) soit l'expiration d'un timer de non réception de nouveaux segments. Par ailleurs, s'il y a déjà un autre segment en attente d'acquittement, on envoie l'acquit immédiatement.

Si le segment TCP est reçu hors séquence, on envoie immédiatement un acquit.

Pour ce qui est de l'envoi d'un segment de données, un compromis est aussi trouvé entre délai et surcharge d'entête. Un nouveau segment TCP contenant l'ensemble des données non transmises est envoyé si ce segment TCP a la taille maximale (MSS bytes de données) et si il n'y a pas actuellement de données en attente d'acquittement.

Afin de numéroter les segments TCP de manière unique, les 2 participants à la transmission se basent sur une horloge monotone (compteur incrémenté de manière continue et monotone)

Le protocole TCP (Transmission Controll Protocol) s'appuie directement sur le service fourni par la couche réseau.

Le principe de la fenêtre glissante dans le cadre de la couche transport fiable et orienté connexion, permet d'assujettir l'émetteur à la capacité de traitement des segments (TPDUs) du récepteur.

Le but primaire de TCP est de fournir un circuit logique fiable ou un service de connexion entre paires de process. Il ne contrôle pas la fiabilité des protocoles sous-jacents (comme IP), donc TCP doit fournir des garanties.

TCP se préoccupe du transfert d'un flux continu de bytes (données) à destination d'une application au travers du réseau.

TCP regroupe donc les bytes dans les segments qui sont passés à la couche Internet (IP) qui les acheminera à la destination.

TCP décide lui-même comment segmenter les données qu'il transmet à son propre rythme. Dans certains cas, une application a besoin de s'assurer que toutes les données actuellement fournies à la couche transport (TCP) sont bel et bien arrivées à destination. Pour cette raison, une fonction push est définie : cela permet de « pousser » les segments TCP se trouvant encore dans les buffers vers la destination

La fonction de fermeture normale de connexion utilise cette fonction push.

Le protocole TCP est un protocole fiable orienté connexion. Le protocole UDP est un protocole non fiable sans connexion

Pour construire un protocole transport fiable et orienté connexion, on peut se baser sur les mécanismes des protocoles de la couche de liaison de données.

Le réseau entre l'émetteur et le récepteur est à considérer comme une « mémoire distribuée »:

```
les stations stockent des segments TCP avant de les transmettre;
les lignes stockent des segments TCP en fonction de son délai;
les routeurs intermédiaires contiennent des buffers
etc.
```

Lorsque les bufferssont pleins, il est nécessaire de supprimer des paquets. La perte de paquets est un indication de congestion du réseau.

Il est don nécessaire de mettre en place des mécanismes de détection et de contrôle de congestion.

Pour TCP, les algorithmes de contrôle de congestion empêchent à un émetteur de surcharger le réseau, adaptent le débit de l'émetteur à la capacité du réseau et essayent d'empêcher l'apparition de situations de congestion.

Les 4 améliorations suivantes implémentées de concert ou non permettent la mise en place du contrôle de congestion : Slow Start, Congestion Avoidance, Fast Retransmit et Fast Recovery. # 5. application

Le protocole HTTP est un protocole conçu pour transférer des documents de type HTML.

Le but des protocoles de type "Remote Execution" est de faire exécuter une tâche, un script, une commande, etc. sur un ordinateur distant.

Les applications qui ont des contraintes de débits (bande passante) sont des applications dites à flux tendus.

Les applications opportunistes (appelées aussi élastiques) s'adaptent dynamiquement à la bande passante (débit) disponible.

Le protocole FTP permet de transférer un fichier entre deux équipements distants sur le réseau.

FTP : protocole qui permet un échange de fichier sur base de TCP
SSH : le protocole qui permet une exécution à distance sécurisée
LDAP : le protocole qui permet la gestion d'annuaires
HTTP : le protocole qui permet le transfert de fichier HTML
NFS : le protocole natif sous UNIX qui permet l'accès aux fichiers distants
CIFS : le protocole natif sous Windows qui permet l'accès aux fichiers distants
RTP : le protocole qui permet de transmettre du contenu multimédia au travers du réseau en s'appuyant sur une couche transport non fiable (UDP) **RTCP** : le protocole qui permet de rapporter sur la qualité des transmissions de contenus multimédia **SNMP** : le protocole qui permet de gérer les équipements réseau
TFTP : le protocole qui permet un échange de fichier sur base d'UDP
TELNET le protocole d'exécution à distance base sur le principe du Network Virtual Terminal **NTP** : le protocole qui permet de synchroniser les horloges systèmes **POP3** : Le protocole qui permet de relever ou de gérer sa boîte aux lettres

Les protocoles qui permettent de gérer les équipements actifs du réseau : **SNMP**, **RMON**

TELNET, REXEC, RSH, SSH : Les protocoles vus au cours et traitant de la problématique de l'exécution à distance

Pour permettre la transmission de contenusmultimédia dans de bonnes conditions, il est nécessaire d'utiliser des algorithmes de compression.

Il existe deux catégoriesd'algorithmes de compression :

```
les algorithmes avec perte : certaines données "inutiles" sont supprimées afin de gagner en
les algorithmes sans perte : il n'y a ici aucune perte de données avant et après compressio
```

En ce qui concerne l'audio, on pourra aussi réduire le nombre d'échantillonsou leur taille, supprimer les silencesou tenir compte des caractéristiques de nos oreilles(son faible après son fort).

Pour ce qui est de la vidéo, on diminuera le nombre de bitspar image, la taille des images ou le nombre de couleursainsi que le nombre d'images par seconde. On pourra, de plus, aussi tenir compte de "l'imperfection" de l'œil humain : changement doux de couleurs ou les changementsvifs.

MIME (Multipurpose Internet Mail Extension) n'est pas un protocole mais une spécificationde formats de messages multimédia sur Internet.

MIME permet d'introduire dans les messages SMTPdes données multimédia car SMTP ne peut transmettre autre chose que des caractères ASCII 7 bits.

Pour remédier aux inconvénientsde SMTP, MIME permet donc de transmettre de façon transparente pour SMTP du texte enrichi (Gras, Italique, Souligné, Couleur, ...). Mais aussi des images, du son, des fichiers. Bien que réservé au départ pour SMTP, il est aussi possible d'utiliser MIME avec HTTP.

Le fait que le protocole de transport UDP supporte le multicast est bien un atout pour la transmission de contenus multimédia

Caractéristiques communes à POP et IMAP:

Les deux protocolessupportent des opérations hors ligne, le courrier étant est délivré, par ailleurs, à un serveur partagé et toujours actif via le protocole SMTP.

Les messages sont ainsi accessiblesdepuis une variété de plates-formes clientes et en tout point du réseau.

Ce sont deux protocoles, ouvertset définis par des RFCs spécifiques, qui servent à gérer l'accès aux boites aux lettres.

Les avantages du protocole POP sont :

```
Sa simplicité. L'implémentation de POP en donc est facilitée.
Un nombre élevé de logiciels clientssont actuellement disponibles.
```

Les avantages du protocole IMAP sont :

de permettre la manipulation de drapeauxd'état des messages.
de pouvoir stockerles messages et les récupérer.
de pouvoir accéder à et gérer de multiplesboîtes aux lettres.
de permettre l'accès et la mise à jourconcurrentielle de boîtes aux lettres partagées.

Vertus et défauts de SMTP

Ce protocole a la vertu d'être particulièrement robustemais il est un peu ancien et il lui manque quelques fonctionnalitésqui seraient bien utiles aujourd'hui :

La sécurisationde la transmission.
Les possibilités de transmettre autre chose que du texte brut.

Ces deux limites peuvent être contournées:

En chiffrantson message,

En utilisant un artifice pour encoder tout type de document de telle manière que SMTP ne tra

Par ailleurs, les messages SMTP sont :

Limitésà du texte ASCII 7bits

Composés de lignesde 1000 caractères maximum

Limités à une taille maximum totale

La spécification MIMEpermet de palier à ce type de limites

Les protocoles de la couche application s'appuient soit sur une couche transport fiable-orienté connexion soit sur une couche transport sans-connexion-non fiable.

Le principe VoIP (Voice over IP) est de transmettre de la voix sur un réseau de données àcommutations de paquets.

Le protocole SMTP est le protocole qui permet d'envoyer un courrier à partir d'un MUA et de le transférer de MTA en MTA jusqu'au MDA.