Cours Réseau – C. Lang

2015-2016

Ce que vous savez :

- Plan IP

- IPv6

- Routage dans la pratique

- NAT, Proxy, ACL, VLAN

Le cours de M1 : aller vers des notions précises, des technos particulières.

Le cours de M2 : développer votre culture des réseaux en reprenant les techniques déjà éprouvées et en créant le lien entre elles.

Dans cette partie de cours :

- Les protocoles de niveau 2 : Ethernet, Wifi.

- Leurs caractéristiques

- Leur gestion du medium physique

- Les réseaux d’accès : ADSL, Fibre et encore Wifi

- Les grands réseaux : RENATER

Préambule : replacer cela dans le contexte de l’OSI.

# Les couches OSI

Il y en a 7 !!!

Voir diapos

C’est un standard qui permet de comprendre et de construire les réseaux. Il définit les étapes d’encapsulation des données.

Le réseau c’est :

* Encapsuler les données (modèle OSI qui fait référence)
* Les acheminer à destination (Routage/Commutation)

Nous allons nous intéresser plus particulièrement aux 4 premières couches du modèle, à savoir les couches qui concernent l’encapsulation pour le transport.

Les 3 couches supérieures sont liées à l’application (initiation du dialogue, chiffrement éventuel, langage commun, …).

Si on se penche plus particulièrement sur les couches 2 et 3. La couche paquet est surtout utile pour l’identification globale (par exemple IP). La couche 2 change en fonction du sous-réseau que l’on traverse.

On a appliqué cela à une discussion entre Joris et Ibrahim, sur l’exemple de TCP/IP.

En général les données de la couche paquet ne sont pas transformées par les équipements intermédiaires (routeurs, switches, …). Il se peut toutefois que certains protocoles aient besoin de casser les paquets en deux (ou plus), pour être compatibles avec leurs caractéristiques.

Une fois que les paquets/trames sont fabriqués, il faut les acheminer.

# Commutation/routage

C’est le principe d’envoyer les paquets à destination. Les trames n’ont pas de besoin de routage simplement de la commutation locale en Ethernet.

## Routage de paquets

Il y a le routage statique et dynamique.

Dynamique :

* RIP : Routing Internet Protocol. Protocole à vecteur de distances. RIP n’est plus très utilisé, il a subi de nombreuses mises à jour pour combler ses lacunes (rebond, comptage à l’infini). RIP ne gère pas les sous-réseaux de tailles différentes.
* OSPF : Open Shortest Path First. Probablement le plus utilisé. Protocole à états de liaisons. On organise le routage en sous-aires pour limiter les échanges entre les routeurs.

Sur internet, on structure les domaines de routage en AS (Autonomous Systems) qui sont des domaines indépendants. Cela optimise les échanges pour le routage. Entre deux AS on utilise des protocoles de routage inter-domaines (EGP, BGP).

Voir diapos sur les protocoles de routage.

Pour mémoire, les routeurs vont donc analyser chaque trame (on enlève la partie trame, on regarde l’adresse IP, on regarde la table de routage, on reconstruit la trame et on envoie).

Ces opérations sont coûteuses en temps. Il faut que les routeurs soient optimisés au niveau calcul et au niveau mémoire. Ceci se fait en fonction des protocoles qu’on va gérer. On peut ainsi prévoir le nombre de cœurs et la mémoire flash par exemple.

Ces protocoles de routage, et les routeurs en général sont bons pour du best effort. C’est essentiellement bon pour du Web (pages Web) et des applications qui utilisent des buffers.

## Commutation

Elle peut être en local : Ethernet. Ou à longue distance : ATM.

La commutation longue distance est optimisée pour les flux multimedia : vidéo, son, …

C’est donc utilisé notamment dans la diffusion de la télévision par Internet.

## Commutation de circuits

C’est le principe de construire le chemin physiquement pour réserver un canal pour la communication : téléphonie analogique ou téléphonie mobile.

# Le niveau 2

## A quoi sert le niveau 2 ?

La couche 2 est l’une des 7 (muy importante) couches OSI. C’est elle qui permet de gérer l’hétérogénéité des réseaux en faisant l’interface entre IP et le niveau physique. Les couches 3 et 4 sont chargées de gérer la communication de bout en bout. La couche 2 va gérer chacune des étapes de cette communication.

Par exemple, on va garder le protocole IP depuis la source jusqu’à la destination alors que l’on peut traverser des niveaux physiques très différents : Wifi, Paires Torsadées, Fibre optique, …

Exemple de protocoles de niveau 2 :

- ATM

- Ethernet

- Liaison série

…

## Adressage

On se place dans le cadre classique : Ethernet, Wifi.

Mac address. Pas de structuration de réseau. Ces adresses sont assignées au matériel réseau. Normalement uniques mais on peut modifier par voie logicielle.

Pour pouvoir faire une correspondance entre IP et Mac. Chaque élément du réseau maintient une table de correspondances IP-MAC. Cette table est remise à jour régulièrement.

Le protocole qui gère cette correspondance s’appelle ARP :

Comment ça marche ?

* Quand un ordinateur veut communiquer avec une IP, il regarde si celle-ci est dans sa table
* Si ce n’est pas le cas, il envoie une requête ARP en diffusion. Requête qui veut dire en gros : « A qui appartient cette IP ? »
* L’élément du réseau qui a cette IP répond en envoyant sa Mac Address
* L’ordi d’origine met à jour sa table. Le switch aussi.
* S’il a déjà cette correspondance dans sa table, il envoie directement avec la Mac address.
  + Attention à bien choisir la bonne. Si l’ordi est sur le réseau local, il envoie directement avec la mac address de l’ordi
  + S’il ne l’est pas, il envoie sur la mac address de la passerelle.

En Ethernet, sur un medium partagé (coaxial) ou en Wifi en medium partagé, celui qui voit passer la trame qui possède sa mac address la récupère.

Quand on est en réseau switché, de toutes manières la trame n’est envoyée que sur le bon destinataire. A part si le message envoyé est un broadcast.

## La sous-couche MAC

C’est celle qui est responsable de communiquer avec la couche physique. Du coup elle est responsable de voir si on peut « balancer » l’info sur la couche physique en question.

En TD, on a vu CSMA/CD. Le principe : le temps de transmission d’une trame doit être au moins égal à 2 fois le temps nécessaire pour parcourir la distance qui sépare les 2 points les plus éloignés du réseau.

CSMA/CD est utilisé pour le réseau Ethernet, pour le Wifi, il s’agit de CSMA/CA que nous verrons dans la partie Wifi.

C’est utile dans le cadre des réseaux Ethernet partagés, pas dans le cas de l’Ethernet switché.

Voir diapo.

La norme initiale d’Ethernet : 10 Mbits/s, 64 octets pour une trame, 200 000 km/s de vitesse de propagation, longueur max du réseau : 5 km.

## Le support physique

En Ethernet on utilise des câbles RJ45 ou paires torsadées. C’est du full duplex (on peut communiquer dans les 2 sens en même temps).

Bande passante s’exprime en Hertz. C’est l’amplitude de fréquences supportées par le câble. Plus on peut mettre de fréquences différentes, plus on a une capacité maximale qui sera grande.

C = W Log2(1+S/B).

W : bande passante en Hertz

S/B : rapport signal/bruit en db

C = bits/s

Quand on achète un câble dit à 100 Mbits/s, on suppose qu’il n’y a pas de perturbation.

Le rapport S/B exprime le contexte dans lequel le câble se trouve. Par exemple si vous faites passer votre câble près d’une source électro-magnétique (exemple des enceintes de chaine Hifi) vous risquez de perdre en capacité maximale.

Le débit effectivement observé sera dépendant de cette capacité maximale mais aussi des débits des cartes réseaux concernées. On prendra le minimum des équipements impliqués.

Débit effectif = min(capacité maximale, débit émetteur, débit récepteur)

En Wifi on utilise les ondes hertziennes qui obéissent aux mêmes lois physiques.

## Transmission de l’info sur le support physique

Concernant Ethernet, il faut maintenant transformer les 0 et les 1 en électricité. On utilise ce qu’on appelle la bande de base qui consiste à faire varier une tension sur un câble. En Ethernet cela s’appelle Code Manchester. L’idée est d’appliquer un changement de tension sur le câble pour indiquer les 0 ou les 1.

Concernant l’ADSL ou le Wifi, on utilise des sinusoïdes. On peut jouer sur la fréquence, sur la phase ou l’amplitude pour modifier ce signal et donc envoyer des 0 ou des 1.

## Les règles de dialogue

C’est le principe d’indiquer que la communication démarre et qu’elle s’arrête. Plusieurs cas :

* On est dans une communication série, on va utiliser des drapeaux de début et de fin.
  + C’est typiquement une communication entre un ordi et une imprimante par exemple
  + On va transmettre des bits sans structuration aucune, comme un flux. On va utiliser des drapeaux de début et de fin pour indiquer le début et la fin de la comm. Le drapeau sera 01111110. Le problème se pose si on veut transmettre le drapeau en tant que donnée. L’algo est le suivant :
    - Après 5 x 1 transmis, l’émetteur insère systématiquement un 0.
    - Après 5 x 1 reçus, le récepteur supprime systématiquement un 0.
    - Sauf sur les drapeaux de début et de fin.
  + On peut aussi transmettre des octets en hexa (souvent le cas de la comm avec les imprimantes). On va utiliser un caractère de début qui est 02 (STX), un caractère de fin qui est 03 (ETX) et un caractère de transparence 10 (DLE). L’émetteur va mettre le DLE devant les caractères qui seraient ambigus : 02, 03, 10. Le récepteur enlève systématiquement le 10 et garde ce qu’il y a derrière.
* On est dans une communication de type Ethernet, on sait reconnaître un début de trame et comme on connaît la dimension de la trame, on sait quand elle s’arrête.

# Le Wifi

C’est un protocole de niveau 2, il s’appuie sur IP pour le niveau 3 et sur TCP ou UDP pour le niveau 4. Il s’occupe de la comm locale, donc c’est bien du niveau 2. Il gère aussi l’accès au medium partagé que sont les ondes hertziennes, c’est bien du niveau 2.

## Généralités

On dit LE Wifi.

On parle de WLAN : Wireless LAN.

Fréquences utilisées : 2,4 Ghz mais aussi 5 Ghz pour les protocoles plus récents.

But : favoriser le nomadisme, limiter le câblage.

En aucun cas, il est destiné à remplacer le réseau filaire.

## Les normes et le débit

802.11b -> 11 Mbits/s. Dès qu’on était plus de deux sur la borne : 1 Mbits/s

802.11g -> 54 Mbits/s

802.11n -> multi antennes. Free pour sa box a pris un bout de cette norme, le bout en question concernait l’aspect multi-antennes.

802.11ac -> fréquences entre 5 et 6 Ghz -> 1,3 Gbits/s et 7 Gbit/s en MIMO.

## Fonctionnement

Les clients sont appelés des Wireless Stations.

Les bornes : Access Points

Un ensemble Access point + WS = BSS Basic Service Set

On peut faire du Wifi sans borne, on parle alors de mode adhoc. On passe dans un schéma maitre-esclave (point à point).

Le Hand Over, c’est la technique qui permet de passer d’une borne à l’autre sans perte (trop visible) de connexion.

## Protocole

Pour se connecter à un WIFI, il faut d’abord détecter le SSID et tenter une première connexion à la borne

* Ecoute passive : la borne elle balance son SSID pour que les équipements puissent le détecter
* Ecoute active : souvent quand la borne cache son SSID.

Une fois que le SSID est connu on se synchronise, on échange les informations d’authentification chiffrées et on commence la communication.

## Accès au medium partagé

Par définition, il faut se synchroniser pour accéder à la borne sans perturber les autres.

Le protocole CSMA/CD ? Difficile à mettre en place car on ne peut pas détecter les collisions comme on le fait sur un réseau Ethernet.

Le protocole utilisé est un protocole centralisé par la borne CSMA/CA (Collision Avoidance).

Algo :

Ecoute de l’ordi pour savoir s’il y a une émission proche.

Si pas d’émission, il écrit à la borne pour savoir s’il peut causer avec elle. La borne renvoie un ack en cas d’accord.

## Sécurité

WEP ? clé partagée. Protocole extrêmement fragile.

WPA2/PSK (Pre-Shared Key) : la clé bouge dans le temps.

WPA : la norme 802.1X (on parle aussi de serveur Radius). C’est le principe d’associer une ou des bornes à un CAS (Central Authentification Service). Il n’y a pas de clé partagée, on contacte le serveur, on s’identifie et là la communication peut commencer.

Le serveur Radius peut, en fonction de l’identité de la personne, donner accès à telle ou telle portion du réseau ou donner accès à tel ou tel protocole.

Eduroam est basé sur ce CAS. Il a accès aux comptes des utilisateurs des autres universités. Quand vous vous connectez sur Eduroam, le serveur CAS vous place en DMZ (Zone démilitarisée).

En entreprise, on utilise ce genre de choses pour segmenter les réseaux et ainsi protéger les données.

# Bluetooth

Protocole d’échange de données, à courte portée et sans fil.

Théorie : 1 à 30m. Pratique : 10m, c’est pas mal. Débit usuel 1 Mbits/s.

Petits équipements à connecter : manettes de jeu, oreillettes, transfert ponctuel entre téléphones, entre PC et téléphone.

Pourquoi le bluetooth : facile à mettre en œuvre, ne nécessite pas d’infrastructure, protocole économe en énergie.

Sécurité ? On utilise une clé partagée de 64 bits. Clé de longueur plutôt faible mais les échanges sont souvent courts et la distance limite les risques.

# Réseaux d’accès

Ce sont les protocoles et les infrastructures qui permettent d’accéder au cœur du réseau.

* Wifi : déjà vu plus haut
* Ethernet qui est à cheval entre accès et cœur
* ADSL
  + Asymetric Digital Suscriber Line
  + ADSL (2 Mbits/s -> 8 mbits/s, 5 km maxi du NRA), ADSL 2+ (20 Mbits/s, en dessous des 3 kms). Pour un plus haut débit on augmente la fréquence mais plus elle est élevée moins elle supporte la distance.
  + Re-ADSL : Reach Extended ADSL -> 7 km. On va utiliser des fréquences basses, supporte mieux la distance mais le débit est du coup plus faible. 2 mbit/s maxi.
  + VDSL : Very High-rate Dig Subs Line. VDSL 1 en dessous d’un km et on peut prétendre à 60 mbits/s. VDSL 2, 3 bornes, protocole amélioré on peut aller jusqu’à 100 mbits/s
  + Sur le câble qu’est-ce qui passe ? Signal sinusoïdal. Cela supporte mieux la distance et c’est moins perturbé par l’électro-magnétisme.
* 3G/4G : réseau via le hertzien.
* Fibre : c’est le principe d’arriver avec de la fibre jusqu’au plus proche du domicile. Cela peut être en bas de l’immeuble, le reste du chemin peut être effectué via le câble TV ou la prise téléphonique (VDSL).
* Câble : utilisation du câble TV. Utilisé aussi dans la distribution de la fibre.
* Satellites : utilisation directe du satellite. Les offres sont chères, c’est assez lent et c’est limité en quantité de données.
* Wimax : Wifi longue distance. Utilisé pour arroser un village avec le réseau mais débit faible et peu fiable en fonction des conditions météo.
* CPL : courant porteur en ligne. Au domicile, ce n’est pas un réseau local. Par contre il existe le CPL longue distance : utilisation des lignes à haute tension.
* Lifi : Wifi par les Leds. Distance faible mais haut débit et possibilité d’un grand nombre d’utilisateurs.