

Réseaux : Architecture

Sławek Staworko

Univ. Lille3

1^{er} décembre 2017

Plan

- 1 Introduction
- 2 Typologie
- 3 Modèles en couches et abstractions
- 4 Niveau physique et liaison de données
- 5 Couche réseau
- 6 Transport des données

Besoins : pourquoi faire un réseau ?

Deux grandes classes d'applications

Pourquoi échanger de l'information ?

- ① Communiquer
 - ▶ Échanger, partager des documents
 - ▶ Diffuser de la musique, des vidéos
 - ▶ Discuter, laisser des messages, ...
- ② Partager des ressources
 - ▶ de calcul
 - ▶ de stockage
 - ▶ des imprimantes, ...

Jusqu'au milieu des années 80

- Centres de calcul.
- L'ordinateur coûte cher, il est fragile, est volumineux.
- Un ordinateur central, des terminaux asservis.
- Architecture maître esclaves.
- Le modèle persiste par exemple pour les caisses enregistreuses

Années 90

- Réduction des coûts.
- Augmentation de la puissance des ordinateurs de bureau.
- Intégration des deux mondes bureau et centre de calcul.
- Notion de service offert à des clients : modèle Client-serveur.
- Clients lourds.
- Repose sur une explosion des réseaux locaux.

Historique

Années 2000

- Ordinateur dans la sphère privée.
- Exploitation commerciale d'internet.
- Adoption des protocoles d'internet en entreprise.
- Clients légers.
- Calcul distribué.
- Organisation pair à pair (P2P, peer to peer)

Années 2010

- Informatique ubiquitaire : n'est plus cantonnée aux ordinateurs
- Nomadisme
- Cloud computing : externalisation des services et machines.

Plan

- 1 Introduction
- 2 Typologie**
- 3 Modèles en couches et abstractions
- 4 Niveau physique et liaison de données
- 5 Couche réseau
- 6 Transport des données

Organisation des réseaux

Plusieurs dimensions pour établir une typologie

- la taille des réseaux : PAN, LAN, MAN, WAN
- l'abstraction : niveau physique, du routage, du transport, des applications.
- la portée : intranet, extranet, internet
- l'organisation : réseaux décentralisés/centralisés, maître/esclave, client/serveur
- l'usage : réseaux d'entreprise, réseaux privés, réseaux sociaux.

Caractères remarquables

- Utilisation de nombreux langages : protocoles, codes.
- Besoin important d'interopérabilité de bout en bout.

Les tailles de réseau I

PAN : Réseaux Personnels

- Connecter des équipements : claviers, souris, casque, micro
- Un dispositif maître, plusieurs esclaves en périphérie.
- Technologie avec fil : usb , et autres ports de la machine
- Technologie sans fil : bluetooth, infrarouge.

LAN : Réseaux locaux

- Connecter des ordinateurs,
- En général localisé à un étage de bâtiment,
- Souvent interconnectés pour construire de plus grands réseaux
- Extension géographique avec des VLANs (virtuels)

Les tailles de réseau II

Au delà

- MAN : réseaux métropolitains de dimension d'une grande société, une université,...
- WAN : grands réseaux e.g. internet.

Les grands réseaux sont des interconnexions de réseaux locaux.

Plan

- 1 Introduction
- 2 Typologie
- 3 Modèles en couches et abstractions**
- 4 Niveau physique et liaison de données
- 5 Couche réseau
- 6 Transport des données

Le rôle de l'abstraction

Abstraire = simplifier

- Des couches d'abstractions successives
- Couches basses proches du signal et du matériel
- Couches hautes proches de l'application et de l'utilisateur
- Chaque couche a un rôle précis et fourni des fonctionnalités
- Chaque couche repose sur les fonctionnalités de la couche inférieure.

Modèles

- Modèle OSI normalisé par l'ISO

Application
Présentation
Session
Transport
Réseau
Liaison
Physique

Le rôle de l'abstraction

Abstraire = simplifier

- Des couches d'abstractions successives
- Couches basses proches du signal et du matériel
- Couches hautes proches de l'application et de l'utilisateur
- Chaque couche a un rôle précis et fournit des fonctionnalités
- Chaque couche repose sur les fonctionnalités de la couche inférieure.

Modèles

- Modèle OSI normalisé par l'ISO
- Internet : TCP/IP

Application
Transport TCP
Réseau : IP
Liaison
Physique

Le rôle de l'abstraction

Abstraire = simplifier

- Des couches d'abstractions successives
- Couches basses proches du signal et du matériel
- Couches hautes proches de l'application et de l'utilisateur
- Chaque couche a un rôle précis et fourni des fonctionnalités
- Chaque couche repose sur les fonctionnalités de la couche inférieure.

Modèles

- Modèle OSI normalisé par l'ISO
- Internet : TCP/IP
- On ne présente que TCP/IP

Plan

- 1 Introduction
- 2 Typologie
- 3 Modèles en couches et abstractions
- 4 Niveau physique et liaison de données**
- 5 Couche réseau
- 6 Transport des données

Au niveau physique et liaison

Le transport d'un signal

- Par l'électricité (câbles de cuivre)

Connexions filaires

- Câbles dédiés : paire de fils de cuivre, blindés pour éviter les interférences et champs magnétiques qui perturbent le signal
- Distance moyenne (centaine de mètres)
- Rapide : en Giga bits par secondes
- Bonne qualité de transmission : peu de pertes
- Sûr : il faut être branché...
- Coût moyen : plusieurs équipements, nécessite de gros travaux et un suivi de la pose des câbles

Au niveau physique et liaison

Le transport d'un signal

- Par l'électricité (câbles de cuivre)

Connexions filaires

- Câbles existants : Courant porteur en ligne (CPL) sur le réseau électrique, ADSL sur les lignes téléphoniques
- Bon marché
- Distance assez faible en CPL et longue en ADSL (plusieurs kilomètres)
- Moins rapide : en Mega bits par secondes
- Interférence, pollution par ondes électromagnétiques
- Moins sûr car on ne contrôle pas tout le réseau

Au niveau physique et liaison

Le transport d'un signal

- Par l'électricité (câbles de cuivre)
 - Par les ondes (micro ondes, satellite, ...)
-
- Ondes électromagnétiques
 - Nécessité d'une politique de sécurité
 - Moins rapide : en Mega bits par secondes
 - Qualité variable selon la distance, l'équipement

Au niveau physique et liaison

Le transport d'un signal

- Par l'électricité (câbles de cuivre)
 - Par les ondes (micro ondes, satellite, ...)
 - Par la lumière (infrarouge, fibres optiques)
-
- Fibre optique
 - Très rapide, très haut débit : en Giga bits par seconde.
 - Adapté aux longues distances (entre bâtiments), aux architectures centrales (backbone)
 - Bonne qualité, mais assez cher.
 - Tendance à arriver jusqu'au domicile (FTTH).

Équipements

Terminologie

Carte réseau maintenant disponible dans tous les ordinateurs et autres dispositifs : connecte un hôte au réseau.

Répéteur le signal qui s'est affaibli sur la distance est répété pour augmenter la distance de transmission

Concentrateur ou hub genre de multiprise réseau qui sert à construire des réseaux en étoile

Commutateur ou switch : comme un hub intelligent qui transmet les informations vers son correspondant et non toutes les machines.

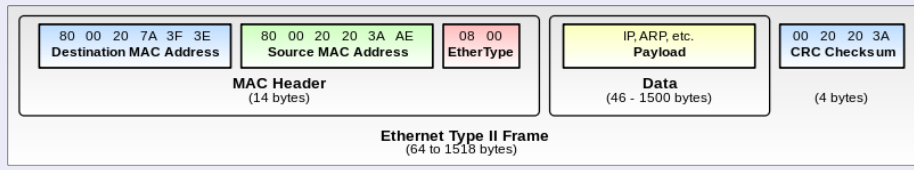
Passerelle Une machine qui permet d'interconnecter plusieurs réseaux et de router les communications.

Routeur comme une passerelle mais entre réseaux homogènes.

Protocole au niveau Physique et Liaison

Ethernet

- Protocole pour les réseaux locaux, au niveau physique et liaison.
- Le plus courant aujourd'hui .
- Proche du matériel donc doit être implanté dans les matériels (on achète des cartes compatibles avec ethernet).
- Commutation de paquets : les messages sont d'abord découpées en **trames** (normalisées).



Ethernet

Principes du protocole

- Très proche de ce qui se passe en société !
- CSMA/CD : Détection de porteuse, accès multiple, détection de collision.
- Chaque hôte écoute s'il peut émettre (CSMA)
- Il émet et tente de relire son message. En cas d'échec une collision a été détectée (CD).

Autres principes

- Chaque carte réseau compatible ethernet possède un numéro unique : numéro MAC de 48 bits donné par le constructeur.
- Les trames contiennent les numéros de l'émetteur et du destinataire.
- Toutes les machines écoutent le réseau et donc déterminent si la trame leur est destinée.
- Autres fonctionnalités pour le contrôle, la détection d'erreurs, ...

Plan

- 1 Introduction
- 2 Typologie
- 3 Modèles en couches et abstractions
- 4 Niveau physique et liaison de données
- 5 Couche réseau**
 - Routage
 - Résolution de noms
 - Configuration d'un hôte de réseau
- 6 Transport des données

Bilan

- Limitation à un réseau local avec peu de machines : sinon trop de collisions.
- On peut facilement espionner les communications si on se trouve dans le réseau local
- Un switch peut lire les trames et envoyer les messages aux bons destinataires, pas un simple commutateur

Comment passer à de grands réseaux ?

- Les protocoles de LAN ne s'étendent pas
- Adresses MAC difficilement adaptées à un grand réseau
- Mais les LANs fonctionnent bien

IP : Internet Protocol

Interconnexion de LAN

- Les LANs sont reliés par des passerelles et routeurs.
- On se repose sur les réseaux locaux pour la livraison finale
- Une adaptation des protocoles est nécessaire pour router les messages entre les LANs

Objectifs

Dans une interconnexion de réseaux locaux, il faut assurer en priorité

- Le routage
- Le contrôle

Institutions

Organisation hiérarchique

- ICANN régule l'internet international. Institution de droit américain. Remise en question et récemment concurrencée.
- L'IANA qui fait partie de l'ICANN, délègue ensuite aux registres régionaux RIRs (grandes zones mondiales).
- Les RIRs délèguent aux registres locaux LIR, (institutions nationales, FAIs fournisseurs d'accès à internet).
- Le complément de l'adresse pour construire l'adresse complète est donné par le responsable du réseau local.

Attribution

- L'adresse (et autres paramètres) est enregistrée de façon statique dans la configuration de la machine.
- L'adresse (et autres paramètres) est distribuée dynamiquement par le protocole DHCP.

Passage à IPV6

IPV4 et IPV6

- Épuisement des adresses IPV4 (février?)
- Limites des tables de routage qui deviennent trop complexes sur les routeurs en IPV4.
- Nécessité de nouvelles fonctionnalités pour les communications cryptées, les flux comme le streaming et la vidéo conférence.

Difficultés

- Mettre à jour les routeurs, adapter l'infrastructure réseau.
- Mettre à jour les clients, donc de nombreux ordinateurs et de nombreux programmes.

Protocole IP

Acheminement des paquets

- Les paquets de la couche inférieure sont augmentés de méta-données (entêtes) pour être acheminés.
- La route n'est pas fixée à l'avance, mais doit être calculée pour chaque paquet (indépendamment).

Adresses

- 32 bits en IPV4, 128 bits en IPV6.
- Identifient des réseaux, sous-réseaux et des hôtes (machines).
- Chaque hôte doit avoir une adresse IP.
- Une machine peut avoir plusieurs adresses IP (plusieurs cartes réseau)
- Une adresse peut être associée à plusieurs machines (anycast).
- Quelques adresses sont réservées : diffusion à un réseau, identification d'un réseau, adresses non routables, ...

Types de diffusion

- Unicast : de 1 à 1.
- Broadcast : de 1 à tous.
- Multicast : de 1 à plusieurs.
- Anycast : de 1 à plusieurs mais un seul est choisi finalement.

Plan

5 Couche réseau

- Routage
- Résolution de noms
- Configuration d'un hôte de réseau

Exemple IPV4

Table de routage IP du noyau

Destination	Passerelle	Genmask	Iface
194.254.132.0	0.0.0.0	255.255.255.0	eth1
192.168.1.0	0.0.0.0	255.255.255.0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	eth0
0.0.0.0	194.254.132.254	0.0.0.0	eth1

- Si on s'adresse au réseau 194.254.132.0 on reste dans le réseau local sur l'interface eth1.
- Si on s'adresse aux réseaux 192.168.1.0 et 169.254.0.0 on reste dans le réseau local sur l'interface eth0.
- Sinon, pour toute autre adresse, on transfère à la passerelle via l'interface eth1.

Passerelle et routeurs

Rôles de la passerelle

- Interconnecte deux réseaux ou plus.
- Accueille souvent le service de translation d'adresses (NAT)
 - ▶ Moyen de contourner la limite d'adresses IPV4
 - ▶ Les adresses IPV4 privées s'adressent à ce service pour accéder à internet.
- Accueille souvent un routeur.

Rôle du routeur

- Tient à jour une table de routage (cf exemple ci-dessus)
- Accueille souvent des services de filtrage : exclure des ports (voir TCP), exclure des contenus (filtre parental, ...)
- Accueille souvent des services de journalisation des échanges : surveillance, historique, ...
- Accueille souvent des services de tampons et redirections d'échanges : cache, proxy.

Plan

5 Couche réseau

- Routage
- Résolution de noms
- Configuration d'un hôte de réseau

Nommer des machines et des réseaux

Constats et objectifs

- ❶ Retenir les adresses IP n'est pas possible
- ❷ Associer des noms intelligibles aux adresses
- ❸ Permettre de retrouver un numéro par son nom et vice-versa.
- ❹ Distribuer cet annuaire dans un réseau

Le fichier des hôtes

Le système d'exploitation d'une machine peut contenir un simple fichier qui remplit les objectifs 2 et 3.

Un exemple /etc/hosts d'unix

```
127.0.0.1 localhost.localdomain localhost
192.168.1.254 pingus grappa www sgbd printserv cups www.grappa.univ-
194.254.132.192 www.grappa.univ-lille3.fr grappa.univ-lille3.fr
192.168.1.5 lp1
192.168.1.6 lp2
```

Distribution dans un réseau

NIS, WINS, LDAP, Active directory, ...

Ces systèmes d'annuaire réseau peuvent distribuer ces adresses/noms dans un réseau local.

À l'échelle d'internet

- La DNS assure ce service de distribution
- La DNS contient aussi la table de correspondances entre adresses et noms.

Ordre de résolution

- Pour une machine dans un réseau local, tous les services peuvent être interrogés.
- Un ordre fixe les conflits possibles.

DNS : Domain name system

Organisation hiérarchique des noms

- Racine, puis domaines de premier niveau, TLD : .fr, .org, ...
- puis sous-domaines : univ-lille3, openstreetmap.org, ...
- éventuellement des sous-sous-domaines (de plus en plus rare), et ainsi de suite.
- FQDN (fully qualified domain name) : grappa.univ-lille3.fr

Résolution de noms

- Serveurs de DNS : répondent aux requêtes d'annuaire.
- La **résolution des noms** suit cette structure hiérarchique : seulement 13 serveurs racine propagent les requêtes aux serveurs concernés.
- Les serveurs DNS possèdent un tampon (cache) qui permet d'accélérer le processus.
- Serveurs primaires par nom de domaine et un secondaire pour la tolérance aux pannes.

Faiblesses

- Sécurité : pas de cryptage des échanges. Attaques de type man in the middle
- 13 serveurs racine traitant des milliards de requêtes par jour, tenus par des organisation ou des sociétés. On déjà résisté à plusieurs attaques.

Autres services des serveurs DNS

Distribution des IP ou noms de serveurs plusieurs services à l'intérieur d'un domaine (serveur de mail, serveur web, serveur de temps, ...)

Institutions d'attribution des noms

- L'ICANN attribue les noms de domaine.
- Depuis peu les noms peuvent être écrits en unicode.
- Elle délègue en France à l'AFNIC pour le .fr.

Exemples

Commandes

```
moi@ici> host univ-lille3.fr
univ-lille3.fr has address 194.254.131.151
univ-lille3.fr mail is handled by 10 mx1.univ-lille3.fr.
```

```
moi@ici> host google.fr
google.fr has address 209.85.143.104
google.fr has address 209.85.143.99
google.fr has IPv6 address 2a00:1450:400b:c00::68
google.fr mail is handled by 10 google.com.s9a1.psmtp.com.
google.fr mail is handled by 10 google.com.s9a2.psmtp.com.
google.fr mail is handled by 10 google.com.s9b1.psmtp.com.
google.fr mail is handled by 10 google.com.s9b2.psmtp.com.
```

```
moi@ici> host 194.254.132.12
12.132.254.194.in-addr.arpa domain name pointer
podcast.univ-lille3.fr.
```

Plan

- 5 Couche réseau
 - Routage
 - Résolution de noms
 - Configuration d'un hôte de réseau

Configuration d'une machine

Le nécessaire pour accéder à internet

- Une adresse IP (comprenant le sous-réseau)
- La passerelle

L'adresse d'un serveur DNS n'est pas nécessaire, mais quand même très utile.

Deux approches

- Configuré en dur dans la machine (maintenant désuet)
- Attribution dynamique de ces paramètres : DHCP pour dynamic host configuration protocol.

Principe

Une machine qui veut obtenir son adresse IP et autres paramètres

- Le client dhcp envoie une requête à toutes les machines du réseau local (broadcast)
- le serveur dhcp identifie la demande et attribue une IP selon une politique
- La machine s'auto-configure avec éléments reçus
- IPV6 a des mécanismes d'attribution. DHCP peut ne plus être nécessaire.

Exemple

```
moi@ici> ifconfig eth0
eth0 Link encap:Ethernet  HWaddr 00:16:3e:ed:47:68
      inet adr:192.168.1.254  Bcast:192.168.1.255  Masque:255.255.255.255
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:12644430 errors:0 dropped:0 overruns:0 frame:0
      TX packets:14478214 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:1000
      RX bytes:3337337100 (3.1 GiB)  TX bytes:10968979382 (10.2 GiB)

moi@ici> cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 212.27.40.241
nameserver 212.27.40.240
nameserver 2a01:e00::2
```

En vrac

- WOL : wake up on lan. Allumer un PC à travers un réseau.
- PXE : Démarrage sur serveur distant (boot réseau).

La boîte à la maison

Les rôles

- modem ADSL
- switch,
- routeur, passerelle
- serveur dhcp, point d'accès wifi,
- parfois d'autres services applicatifs (Voip, SIP, NAS, WOL,...).

Plan

- 1 Introduction
- 2 Typologie
- 3 Modèles en couches et abstractions
- 4 Niveau physique et liaison de données
- 5 Couche réseau
- 6 Transport des données**

Transport : TCP/UDP

Objectifs

Assurer le transport de données : données brutes, éviter les pertes, ordonner les réceptions, ...

Un numéro de **port** est ajouté aux adresses.

TCP

- Protocole avec connexion,
- Sûr (sans perte)
- Utilisé pour la plupart des applications d'internet (Web, ftp, ...).

UDP

- Protocole sans connexion.
- Moins sûr que TCP (pertes possibles).
- Très rapide.
- Utilisé pour la DNS, les jeux en réseau, le streaming.

Les ports

C'est quoi ?

- Un numéro qui complète une adresse IP
- Comme un numéro de quai dans un port, ou un numéro de porte dans un immeuble.

Pourquoi compléter les adresses IP ?

- Une machine peut assurer ou être cliente de plusieurs services.
- Les données doivent être acheminées au bon processus (programme) dans la machine.

Attribution

- Les numéros de port sont attribués par le système d'exploitation.
- L'IANA fixe les numéros pour de nombreux services et applications :
Exemple 80 pour le Web.
- Le fichier `/etc/services` contient ces numéros normalisés.

Exemple : chat en TCP

Serveur

```
>>> from socket import *
>>> s = socket(AF_INET, SOCK_STREAM)
>>> s.bind(('',50000))
>>> s.listen(1)
>>> c,a = s.accept()
>>> d = c.recv(1000)
...
>>> d
'coucou'
>>> c.close()
```

Client

```
>>> from socket import *
>>> s = socket(AF_INET, SOCK_STREAM)
>>> serv = ('xxx.xxx.xxx.xxx',50000)
>>> s.connect(serv)
>>> s.send('coucou')
6
```

Exemple : chat en UDP

Serveur

```
>>> from socket import *
>>> s = socket(AF_INET, SOCK_DGRAM)
>>> s.bind(('',50000))
>>> d = s.recv(1000)
...
>>> d
'coucou'
>>> c.close()
```

Client

```
>>> from socket import *
>>> s = socket(AF_INET, SOCK_DGRAM)
>>> serv = ('xxx.xxx.xxx.xxx',50000)
>>> s.sendto('coucou',serv)
6
```