La couche physique

Débit réseau vs débit constaté (affiché par la machine)

- En réseau, le débit se mesure en bits/seconde
- En informatique, on travail par paquet de 8 bits (= 1 octet)
- Une capacité de stockage est donc mesurée en nombre d'octets
- Un débit dans une application (navigateur internet) se fait aussi en octet.

Débit informatique = Débit Réseau / 8

Débit de 16 Mbits/s annoncé par un fournisseur d'accès = 2 Mo constaté en téléchargement.

Mo != Mio

- 1 Ko = 1000 octets
- 1Kio = 2^10 = 1024 octets
- 50 000 000 000 octets = 50 Go = 46,56 Gio

Le cablage : paire torsadée

- Issu du monde de la téléphonie
- Peut supporter un débit jusqu'à 1 Gbits/s
- Longueur maximale : 100 mètres
- Architecture physique en etoile (à l'aide de hub ou switch).
- Prise RJ45

Le cablage : coaxial

- Similaire à celui de la télévision
- Câble coaxial fin (couleur noire) 10Base2 10Mbits/s sur 200m avec des terminaison de 50 Ohm
- Câble coaxial épais (couleur jaune) 10Base5 10Mbits/s sur 500m.
- Pour le coaxial l'achitecture physique est en Bus les machines se suivent.
- Prise BNC

Le cablage : la fibre multimode et monomode

- Avantages:
  - Trés haut débit,
  - Longue distance (multimode 500m, 1Gbits/s et monomode 5 KM, 1Gbits/s)
  - Insensible au perturbation électromagnétique
  - Difficile à pirater
  - Liaison inter-bâtiment (problème de Terre)
- Inconvénients:
  - coût élevé (installation, elements actifs ....)
  - difficile à mettre en oeuvre
  - difficile à tester (matériel coûteux)
- Prise spécifique fibre

Le concentrateur

- Permet de connecter plusieurs machines entre elles au niveau Ethernet
- Toute information qui arrive sur un port est diffusée sur les autres ports
- Dispose d'un nombre variable de ports (4, 24 par exemple)
- Les ports d'un concentrateur ne disposent pas d'adresse MAC ni d'adresse IP
- Les ports in croisent les paires de fils torsadés.
- Le port out n'est pas croisé pour permettre la liaison d'un autre concentrateur.
- Sur un réseau 10 Mbit/s, pas plus de 5 segments (cables) entre deux terminaux (donc 4 concentrateurs).
- On parle de réseau Ethernet partagé.
- **Plus utilisé en filaire, existe toujours dans les technologies sans fil**

Les commutateurs (switch)

- Les terminaux sont reliés à un port du commutateur
- Le commutateur enregistre les adresses MAC des terminaux connectés pour n'envoyer les trames reçues que sur le bon port (table de commutation).
- Moins de problèmes de collision
- La diffusion (broadcast) est toujours possible sur les commutateurs
- Par défaut, on évitera de mettre des machines de réseaux différents sur un même commutateur.
- Des commutateurs spécifiques existent pour garantir la sécurité de réseaux différents sur un même appareil (VLAN port, MAC, IP)

Les routeurs (passerelles IP)

- Ressemblent à des concentrateurs ou des commutateurs de l'extérieur (prises RJ45)
- **Contrairement à ceux ci, les prises RJ45 sont associées à une adresse MAC et une adresse IP**
- Permet de gérer finement le traffic réseau entre sous-réseaux (table de routage)
- C'est un ordinateur administrable depuis le réseau.

Le cablage en paire torsadée

- Cable droit : relie une interface réseau (prise RJ45 avec adresse MAC et IP) avec une 'multiprise pour cable RJ45" (concentrateur ou commutateur).
- Cable croisé : relie directement deux interfaces réseau (deux ordinateurs, un ordinateur et un routeur).
- Les matériels récents sont capables de gérer automatiquement le croisement des paires torsadées sur leur prise RJ45.
- Possibilité d'alimenter électriquement les terminaux (Power over Ethernet, PoE) : téléphonie sur IP par exemple.

Le domaine de collision

- Un seul terminal peut émettre à un moment donné sur le réseau partagé.
- Avant d'envoyer une trame, le terminal vérifie que la ligne est libre.
- Cette vérification ne fonctionne pas pour les trames émises mais pas encore reçues (temps de parcours sur le réseau).
- Si deux terminaux émettent en même temps, une collision se produit.
- La détection peut se faire en comparant le signal émit et le signal reçu par l'envoyeur.
- Si une collision est détectée, chaque terminal attend un temps aléatoire avant de re-émettre.
- Après un nombre d'essais, l'emission est annulée.

Approche Carrier Sense Multiple Access (CSMA)

Le proxy

- Un intermédiaire entre deux machines
  - Les deux machines ne communiquent pas directement
  - Chaque machine ne connaît que l'intermédiaire
- Usages (proxy HTTP squid à l'université) :
  - Mise en cache des pages web souvent consultées
  - Journalisation des accès
  - Contrôle des accès

Le pare-feu

- Protège un réseau interne des intrusions externe
- Fonctionne généralement au niveau 4 (transport : TCP/UDP)
  - filtrage des ports
  - filtrage des adresses IP
- Problème des ports dynamiques : nécessite d'analyser le contenu des trames (niveau applicatif)

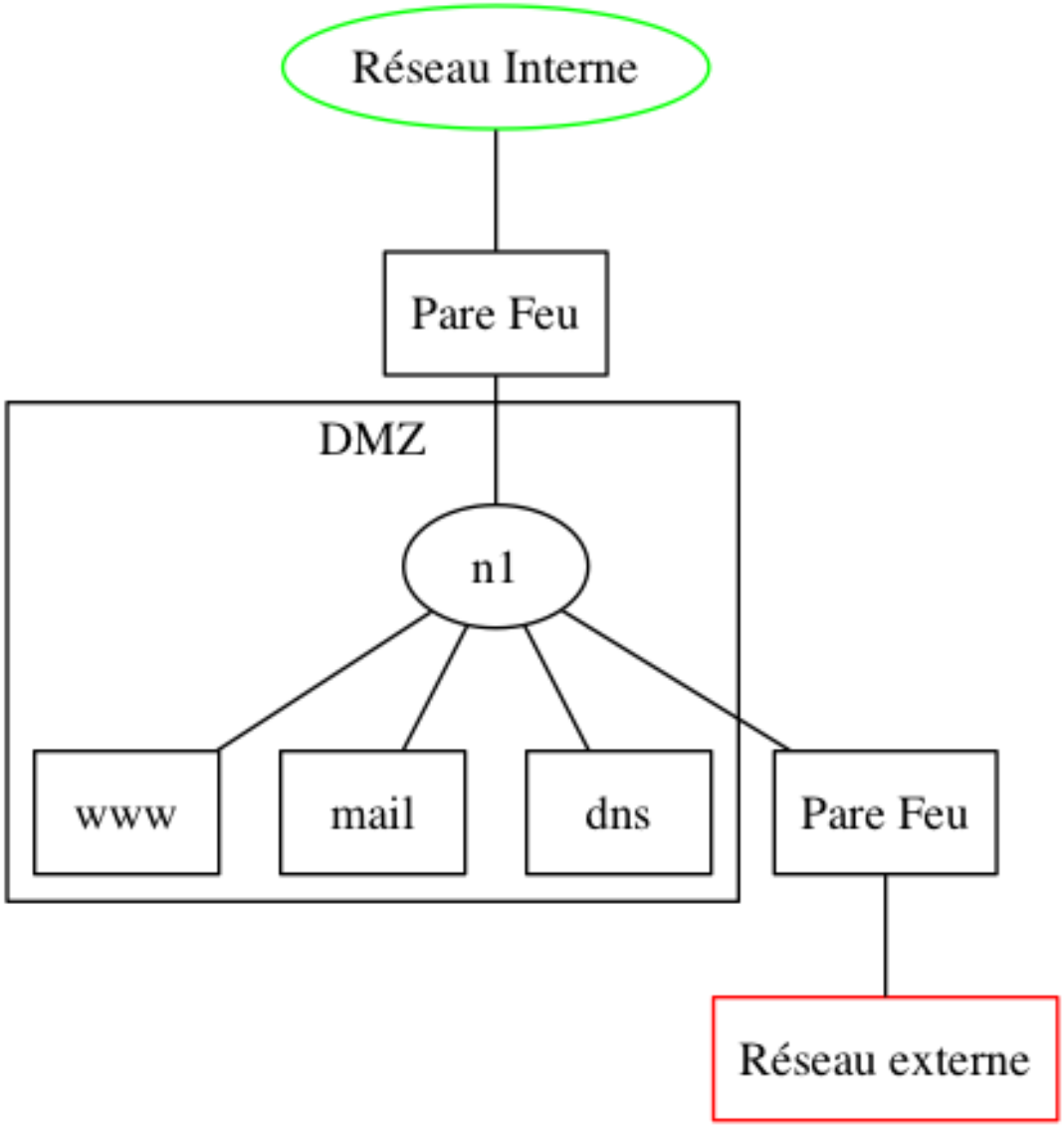
Le futur : des matériels génériques configurables

- Les commutateurs et routeurs font de plus en plus de choses
- *in fine* il s'agit d'ordinateurs spécialisés
- D'où l'idée de brancher des boitiers génériques et de configurer leurs fonctionnalités de manière logicielle **Software Defined Networking**
- Le contrôle (calcul des routes) est alors découplé des données (le routage des paquets)
- OpenFlow est un protocole pour créer des réseaux logiciels.

Architecture : la DMZ

- Certaines machines doivent être visibles du réseau public (web, mail, DNS) et du réseau interne.
- Ces machines sont regroupées dans un sous-réseau particulier appelé DMZ
- L'accès entre le réseau interne et la DMZ est protégé par un pare-feu
- L'accès entre la DMZ et le réseau public est aussi protégé par un pare-feu

Exemple de DMZ



Pour terminer

Quels services de l'université se trouvent dans notre DMZ ?

Comment le vérifier ?

De 194.254.23.3:80 à www.univ-artois.fr

- Les utilisateurs “normaux” d’Internet n’utilisent pas d’adresses IP
- Les adresses IP sont remplacées par des noms
- Les ports associés aux services courants sont normalisés
  - 22 SSH
  - 23 telnet
  - 25 SMTP
  - 80 HTTP
  - 110 POP3
  - 143 IMAP
- Les ports sont donc souvent cachés par les outils

Pour faciliter l’usage du réseau, des noms sont associés aux adresses IP

Noms de domaines

- composé d'une **extension** (.fr, .net, .com, .edu, .info, .biz etc) appelée nom de domaine de premier niveau (*Top Level Domain, TLD*)
  - TLD nationaux/géographiques (fr, en, eu, it, us)
  - TLD génériques originaux (com, org, net, edu, gov, mil)
  - Création en 1998 de l' Internet Corporation for Assigned Names and Numbers (ICANN) pour gérer les nouveaux TLD (aero, biz, coop, info, museum, name, pro en 2000
  - TLD sponsorisés (edu, gov, mil) vs non sponsorisés (com, org, net)
- le nom de **domaine de second niveau** précède le TLD
- le préfixe qui désigne un service (`www` pour le web)
- tout ce qui se trouve entre le nom de second niveau et le préfixe représente des sous-domaines du domaine de second niveau.

Exemples de noms de domaine

- `www.univ-artois.fr`
- `wmail.univ-artois.fr`
- `foad.univ-artois.fr`
- `ent.univ-artois.fr`

`fr` est un TLD national, `univ-artois` un nom de domaine de second niveau et `www`, `wmail`, `foad`, `ent` sont des préfixes représentant des services de l'universités.

- `www.impots.gouv.fr`
- `www.education.gouv.fr`
- `www.diplomatie.gouv.fr`

`fr` est un TLD national, `gouv` un nom de domaine de second niveau correspondant à l'état français, `impots`, `education` et `diplomatie` sont des sous domaines représentant les différentes administrations de l'état et `www` représente pour ces administrations leur site web.

Louer un nom de domaine secondaire

- Il est facile de louer un nom de domaine secondaire si il est libre
- Des restrictions peuvent exister : TLD géographiques ou sponsorisés, noms secondaires correspondant à des marques.
- En france, c'est l'AFNIC qui gère les noms de domaines secondaires du TLD fr (et aussi `re` Ile de la Réunion, `pm` Saint-Pierre et Miquelon, `tf` Terres australes et antarctiques Françaises, `wf` Wallis et Futuna, `yt` Mayotte)
- Pour connaître le locataire d'un nom de domaine, on utilise le service `whois`.

Association statique locale

- Sous Unix, l'association se fait dans le fichier `/etc/hosts`

```
$ more /etc/hosts
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1       localhost
255.255.255.255 broadcasthost
::1             localhost
fe80::1%lo0     localhost
192.168.33.10  preview.localhost
```

- Au début d'Internet, un fichier complet d'associations était maintenu par un organisme (Network Information Center) et recopié sur les machines connectées à Internet

Domain Name System

- Depuis le milieu des années 80, un système hiérarchique, dynamique et distribué voit le jour : le DNS.
- L'association (nom, adresse IP) est gérée par des serveurs de noms (Name Server)
- Système hiérarchique : les sous domaines sont gérés par des serveurs de noms internes, les domaines secondaires sont gérés par au moins deux serveurs de noms, les TLD sont gérés par des organismes.
- Les serveurs de nom sont souvent gérés par un logiciel qui s'appelle BIND (Berkeley Internet Name Domain)
- On peut utiliser la commande `dig` pour connaître les serveurs de noms associés à un nom de domaine.

Résolution inverse

- Permet de retrouver le nom de domaine associé à une adresse IP
- On transforme pour cela l'adresse IP en un domaine particulier
  - on renverse l'adresse IP
  - on ajoute l'extension in-addr.arpa
  - `194.254.23.3` devient `3.23.254.194.in-addr.arpa`
- La commande `host` permet de faire de la résolution inverse

```
host 194.254.23.3
3.23.254.194.in-addr.arpa domain name pointer srv-arras-23-3.u
```

Questions relatives au cours de la semaine précédente

Pour chacune des affirmations suivantes, indiquer si elle est vrai ou fausse

- 192.168.34.123:8080 représente l'adresse IP 192.168.34.123 et le masque de réseau 8080
- UCP est un protocole connecté fiable
- TCP est une protocole non connecté rapide
- Les noms de domaine de premier niveau sont toujours géographiques/nationaux
- Dans le nom `3.23.254.194.in-addr.arpa`, `arpa` est un domaine de premier niveau (TLD) et `in-addr` est un domaine de second niveau