

03 - Complements

Gaétan Richard
gaetan.richard@info.unicaen.fr

DNR2I - M1

I. Rappels

Le modèle OSI ...

7-Application	Communique avec l'application
6-Présentation	Mets en forme les informations échangées
5-Session	Assure l'ouverture et la fermeture d'une session
4-Transport	Assure le transfert des données et la fragmentation
3-Réseau	Assure l'acheminement ou le routage
2-Liaison	Assure le transfert des trames sur une ligne
1-Physique	Transmet les bits sur le support physique

Important :

- ▶ Chaque couche communique uniquement avec la couche immédiatement supérieure et inférieure.
- ▶ Chaque élément est standardisé.

...et la réalité

Application
Transport
Réseau
Liaison - Physique

ex : *DNS, IMAP, POP3, SMTP, HTTP, ...*

ex : *TCP / UDP*

ex : *IPv4 (ICMP)*

ex : *Wifi, ethernet, ppp, ...*

Rôle : assure une connexion entre deux machines reliées “physiquement”.

À retenir :

- ▶ Adresse **MAC** ;
- ▶ Somme de contrôle ;
- ▶ ...

Rôle : Assure l'acheminement par l'intermédiaire de **tables de routage** qui indiquent où envoyer les paquets.

À retenir :

- ▶ Sous-réseaux, masque ;
- ▶ Adresses privées / publiques ;
- ▶ Principes du routage ;
- ▶ Tables de routage ;
- ▶ ICMP ;
- ▶ ...

Table de routage

Exemple :

```
$ /sbin/route -n
```

```
Table de routage IP du noyau
```

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
10.0.2.0	0.0.0.0	255.255.255.0	U	1	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	eth0
0.0.0.0	10.0.2.2	0.0.0.0	UG	0	0	0	eth0

ARP (Address Resolution Protocol)

Rôle : Permet de transformer les adresses IP en adresses MAC.

Fonctionnement : ARP envoie des demandes à tout le réseau local pour connaître qui possède une adresse IP.
La machine concernée répond.

Rôle : Assure la connexion et le transport des données d'un point à un autre du réseau.

À retenir :

- ▶ Notion de **port** ;
- ▶ Principe de l'acquittement ;
- ▶ Établissement et clôture d'une connexion TCP ;
- ▶

DNS (Domain Name System)

Rôle : Associer à chaque nom un adresse IP (et inversement).

ex : `www.info.unicaen.fr` \Leftrightarrow 193.55.128.20

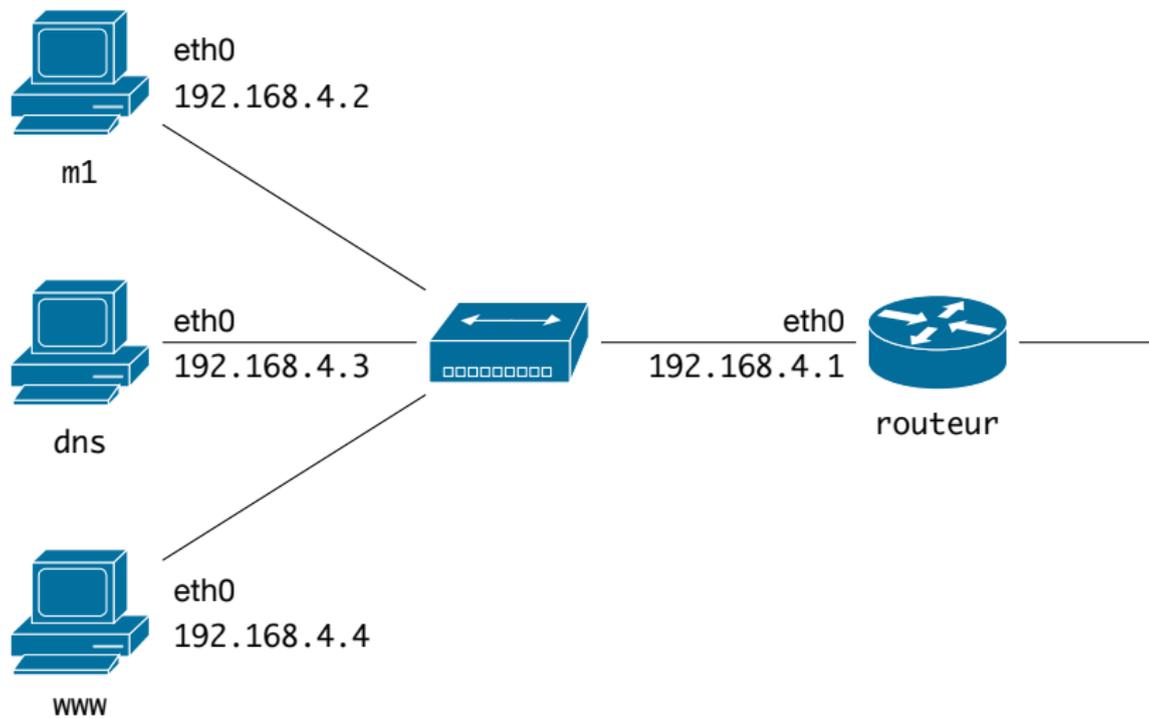
Application

Rôle : Transporte les informations du programme.

À retenir :

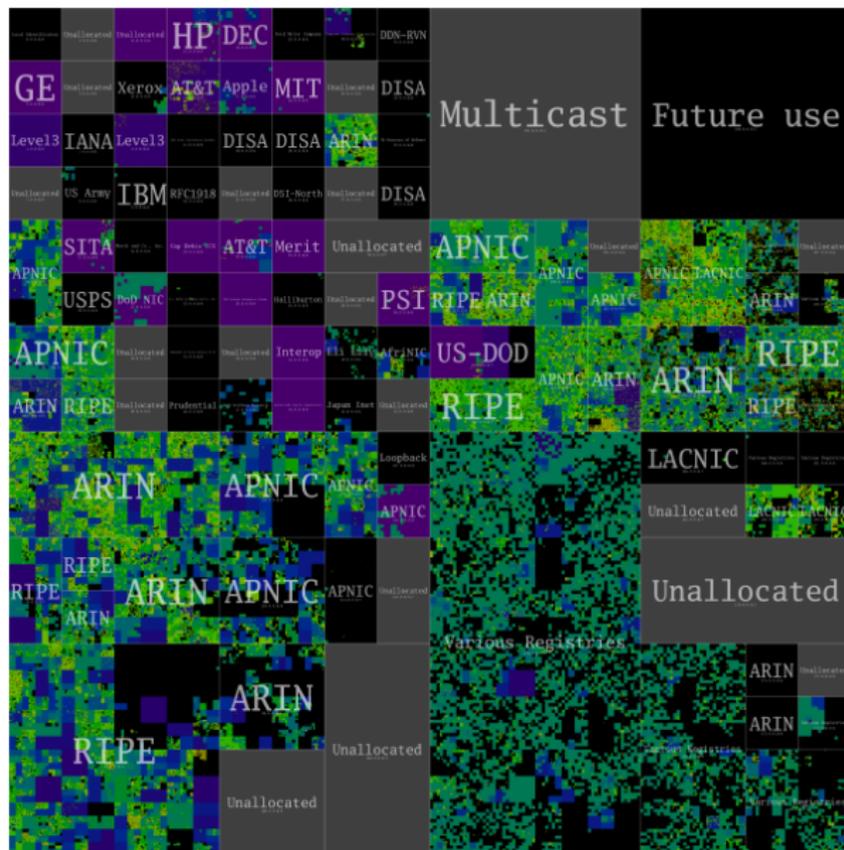
- ▶ *RFCs* ;
- ▶ Variété des protocoles ;
- ▶ Ports usuels ;
- ▶ Principe du client / serveur ;
- ▶ ...

Récapitulatif : lire un site web



2. IPv6

Attribution des adresses IPv4 (2008)



Ressources limités : les adresses IPv4 sont épuisés depuis le 31 janvier 2011 (IANA) et le 15 avril 2011 (APNIC).

Que faire ?

Adresse IPv6 :

- ▶ 4×4 octets (128 bits);
- ▶ Représenté par 8 nombres en hexadécimal séparés par des `:`
(ex :
`FE80 :0000 :0000 :0000 :0000 :0000 :0000 :0001`);
- ▶ Les deux derniers champs peuvent être représenté comme une adresse IPv4
(ex : `FE80 :0000 :0000 :0000 :0000 :0000 :0.0.0.1`);
- ▶ On ignore les 0 non significatifs
(ex : `FE80 :0 :0 :0 :0 :0 :0 :1`);
- ▶ On peut omettre **une** fois une suite de 0 consécutive avec `::`
(ex : `FE80 ::1`).

Comparaison

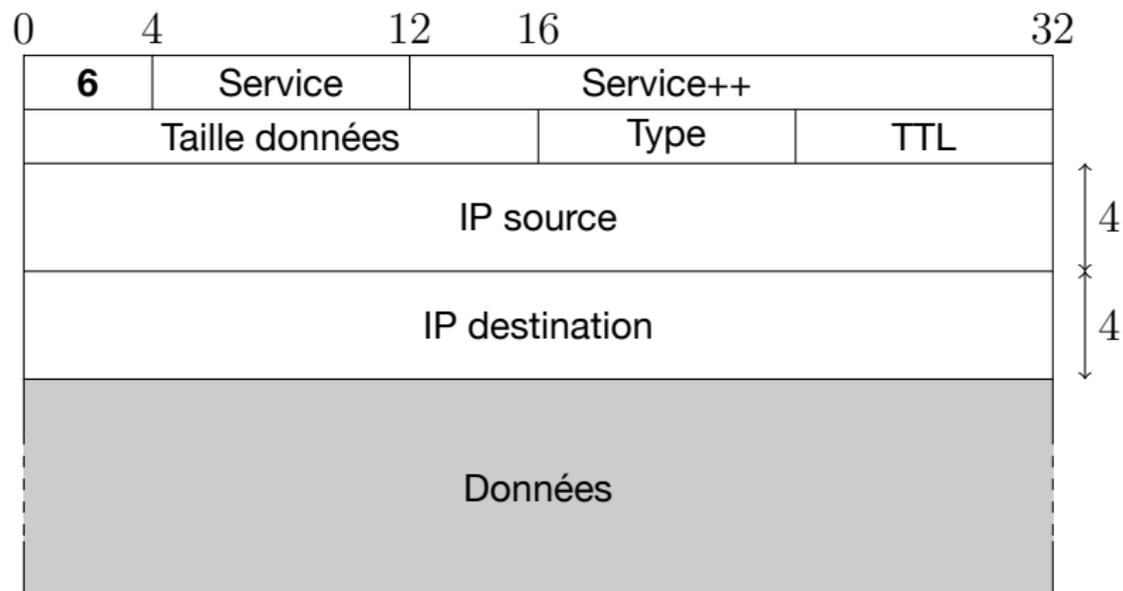
Avantages :

- ▶ Plus d'adresses ;
- ▶ incorpore ICMP ;
- ▶ permet la configuration automatique d'adresses ;
- ▶ profite de l'expérience d'IPv4 (plus clair / mieux adapté) ;
- ▶ ...

Inconvénients :

- ▶ Manque encore quelques points (DNS automatique ?) ;
- ▶ besoin d'une transition ;
- ▶ ...

Structure :



3. Filtrage

Adressage privé

Certaines adresses sont réservées pour un usage privé (*c-à-d* local) et peuvent être utilisées librement.

Les classes privées :

- ▶ 127.0.0.1 (*localhost*)
- ▶ 10.0.0.0 – 10.255.255.255
- ▶ 172.16.0.0 – 172.31.255.255
- ▶ 192.168.0.0 – 192.168.255.255

Question : Comment faire pour connecter ces machines à l'internet.

Proxy applicatif

Principe : Une machine sert de relais au niveau applicatif (couche application) pour donner accès au service.

Exemple : Proxy web.

Avantage : On peut tirer parti de la connaissance du protocole applicatif (cache, ...).

NAT (Network address translation)

Principe : Une machine sert de relais au niveau de la couche réseau.

Fonctionnement : On remplace l'adresse privé par l'adresse publique de la machine servant de passerelle et on utilise les ports pour se souvenir de la connexion.

Accessibilité :

- ▶ On peut aller de l'intérieur vers l'extérieur ;
- ▶ On ne peut pas faire le contraire.

Mise en place :

Sous Linux, on utilise l'ensemble [netfilter](#) et notamment la commande **iptables**.

Filtrage

Principe : On observe en détail le trafic et on choisit les actions à effectuer.

Type de trafic :

- ▶ Entrant (INPUT);
- ▶ Sortant (OUTPUT);
- ▶ En transit (FORWARD).

Effet :

- ▶ Accepter (ACCEPT);
- ▶ Refuser en envoyant un message (REJECT);
- ▶ Ignorer (DROP);
- ▶ Loguer (LOG).

Transfert de port

Principe : Rediriger le trafic entrant sur un port fixé vers une autre ordinateur.

Utilité : Permettre d'avoir un service accessible sur une machine avec un IP privée.

4. Réseaux virtuels

Protection : Afin de protéger les communications et d'assurer la sécurité du réseau, on le sépare en sous-réseaux *indépendants*.

Question : Comment faire lorsque le câblage est déjà fait ?

Protection : Afin de protéger les communications et d'assurer la sécurité du réseau, on le sépare en sous-réseaux *indépendants*.

Question : Comment faire lorsque le câblage est déjà fait ?

Solution : Utiliser des réseaux virtuels (**VLAN**).

Virtual LAN : Créer un sous-réseaux virtuel à l'intérieur d'un réseau.

- ▶ Fonctionne au niveau des trames Ethernet ;
- ▶ Standard IEEE 802.1Q ;
- ▶ Il existe aussi un protocole propriétaire *Cisco*.

Datagramme :

- ▶ Ajoute un champ **Tag** ;
- ▶ Recalcule la CRC.

Configuration :

- ▶ Transparent pour la machine ;
- ▶ Se configure sur le switch ;
- ▶ Configuration par *port* du switch.

Documentation :

Voir la documentation du constructeur.

Virtual Private Network

- ▶ Permet de créer des réseaux privés virtuels au travers d'Internet ;
- ▶ Encapsule les communications (possibilité d'utiliser des adresses privées) ;
- ▶ Crypte les communications.

Configuration :

- ▶ De nombreuses options ;
- ▶ Utilisation de **ssh** et **ppp** ;
- ▶ Utilisation via un navigateur web ;
- ▶ ...