

## Cours 2 : Protocoles et routage

Rabii El Ghorfi

## 1. Introduction

- Administration réseau
- Internet et le modèle TCP/IP

## 2. Rootage et Passerelle

- Principes de base
- Quelques commandes

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

# Contenu

- ★ Routage et passerelle :
  - ▶ Configuration d'une passerelle.
  - ▶ Configuration d'un réseau privé : NAT (**N**etwork **A**ddress **T**ranslation), IP masquerading ...
- ★ Sécurité dans les réseaux:
  - ▶ Configuration de pare-feu (*firewall*):
    - Manipulation des tables *iptables*.
    - Règles de filtrage.
    - ...
  - ▶ Outils de diagnostic :
    - *nmap*
    - ...
- ★ Configuration et manipulation de services spécifiques :
  - ▶ Gestion d'utilisateurs distants (NIS)
  - ▶ Un annuaire fédérateur (LDAP)
  - ▶ Transfert de fichiers et autres (FTP, TFTP, NFS, SMB)
  - ▶ Connexions à distance (telnet, rlogin, ssh, X11, ...)
  - ▶ Les serveurs de noms (DNS)

# Le visage de l'Internet (1)

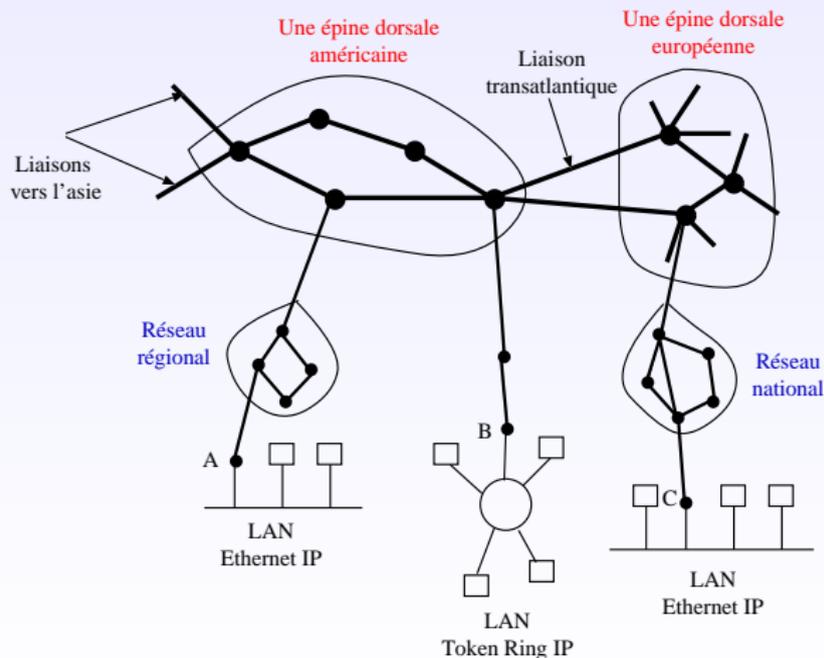
- ★ Un réseau de réseaux
- ★ Un ensemble de logiciels et de protocoles
- ★ Basé sur l'architecture TCP/IP
- ★ Fonctionne en mode Client/Serveur
- ★ Offre un ensemble de services (e-mail, transfert de fichiers, connexion à distance, WWW, ...)
- ★ Une somme « d'inventions » qui s'accumulent
  - ▶ mécanismes réseau de base (TCP/IP)
  - ▶ gestion des noms et des adresses
  - ▶ des outils et des protocoles spécialisés
  - ▶ le langage HTML

# Le visage de l'Internet (2)

- ★ Une construction à partir du « bas »
  - ▶ réseau local (laboratoire, département)
  - ▶ réseau local (campus, entreprise)
  - ▶ réseau régional
  - ▶ réseau national
  - ▶ réseau mondial
  
- ★ 3 niveaux d'interconnexion
  - ▶ postes de travail (ordinateur, terminal...)
  - ▶ liaisons physiques (câble, fibre, RTC...)
  - ▶ routeurs (équipement spécialisé, ordinateur...)

# Le visage de l'Internet (3)

Un ensemble de sous-réseaux indépendants (Autonomous System) et hétérogènes qui sont interconnectés (organisation hiérarchique)



# L'architecture de TCP/ IP (1)

Une version simplifiée du modèle OSI

**Application** FTP, WWW, telnet, SMTP, ...

**Transport** TCP, UDP (entre 2 processus aux extrémités)

- ★ TCP : transfert fiable de données en mode connecté
- ★ UDP : transfert non garanti de données en mode non connecté

**Réseau** IP (routage)

**Physique** transmission entre 2 sites

**TCP** → **T**ransport **C**ontrol **P**rotocol

**UDP** → **U**ser **D**atagram **P**rotocol

**IP** → **I**nternet **P**rotocol

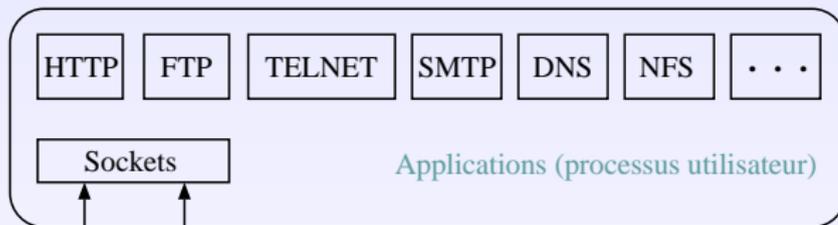
# L'architecture de TCP/ IP (2)

OSI

7

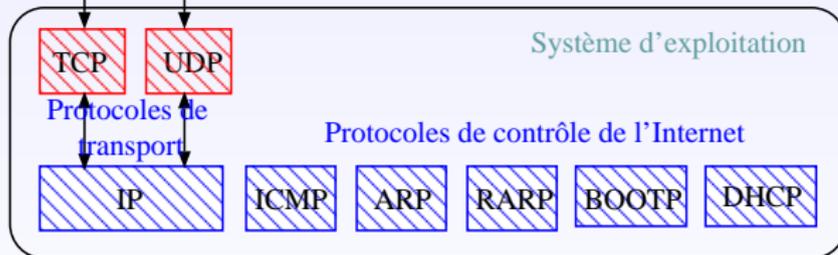
6

5



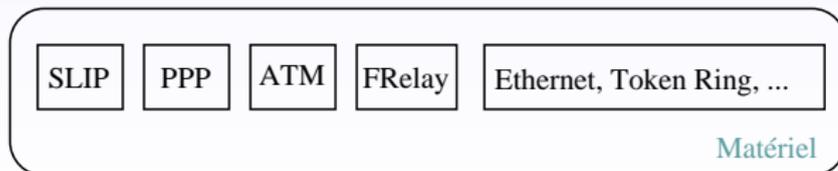
4

3



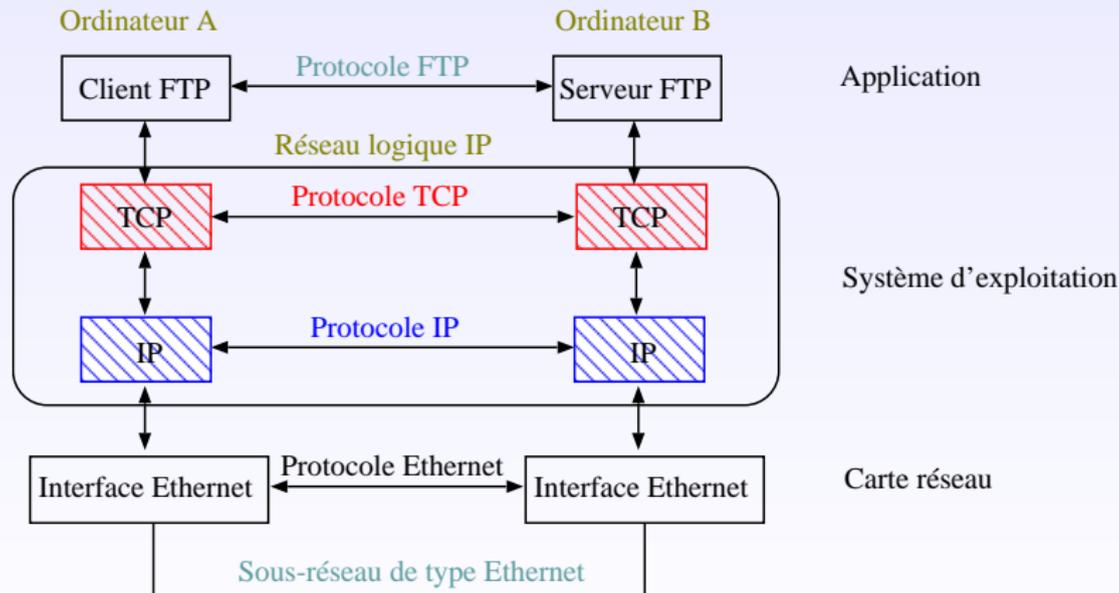
2

1



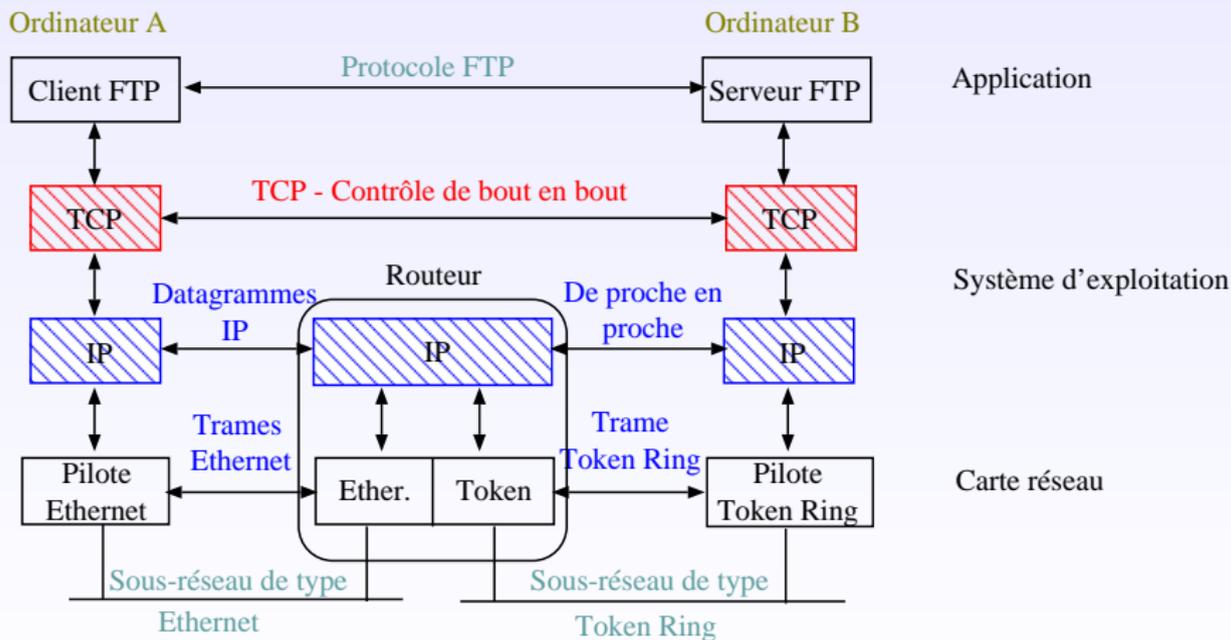
# L'architecture de TCP/ IP (3)

## Deux machines sur un même sous-réseau IP



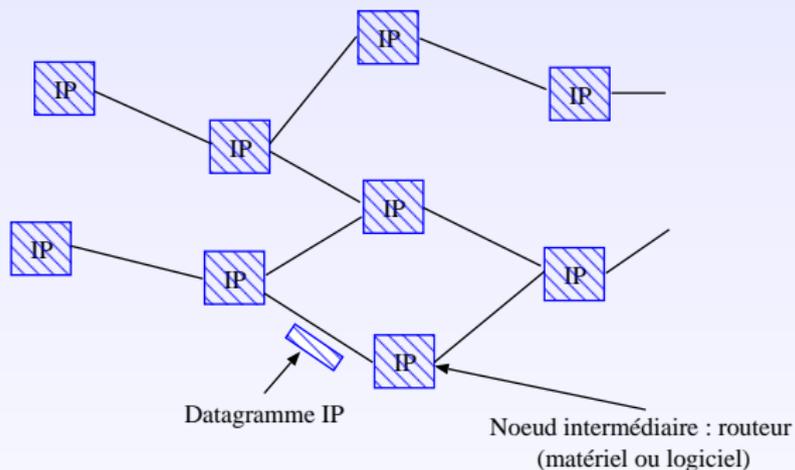
# L'architecture de TCP/ IP (4)

## Prise en compte de l'hétérogénéité



# L'architecture de TCP/IP (5)

## Couche réseau : communications entre machines

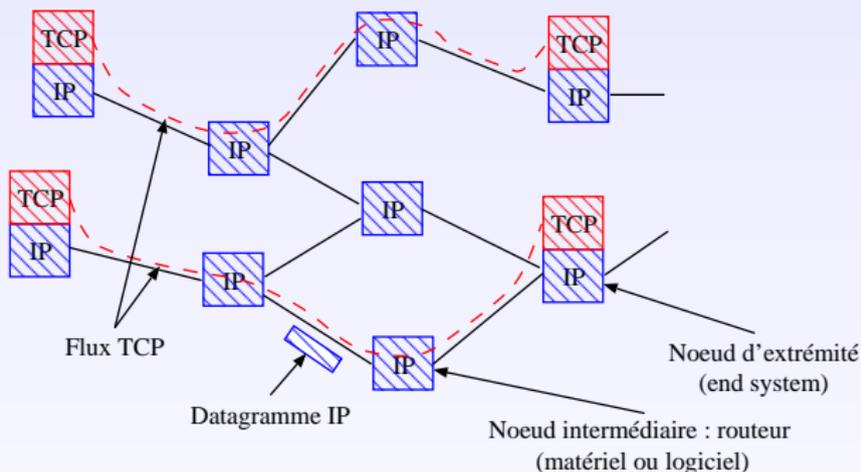


IP - protocole d'interconnexion, best-effort

- ★ acheminement de **datagrammes** (mode **non connecté**)
- ★ peu de fonctionnalités,
- ★ pas de garanties simple mais robuste (défaillance d'un noeud intermédiaire)

# L'architecture de TCP/IP (6)

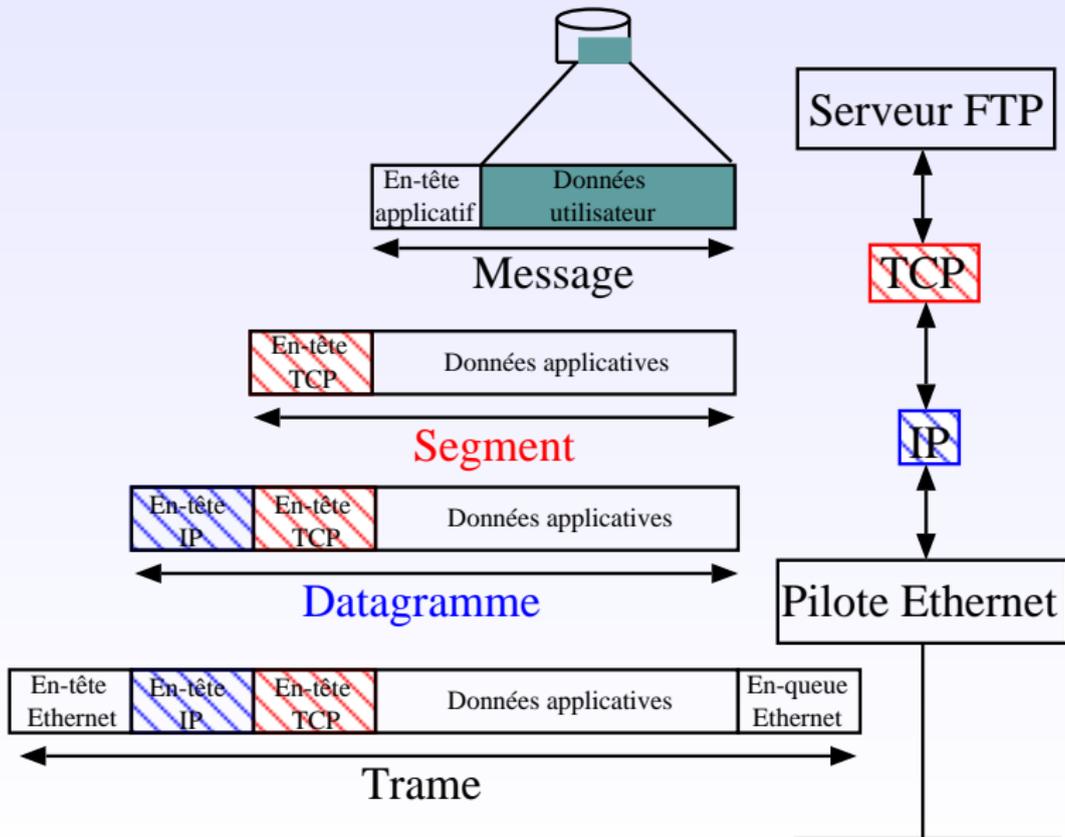
## Couche transport : communications entre applications



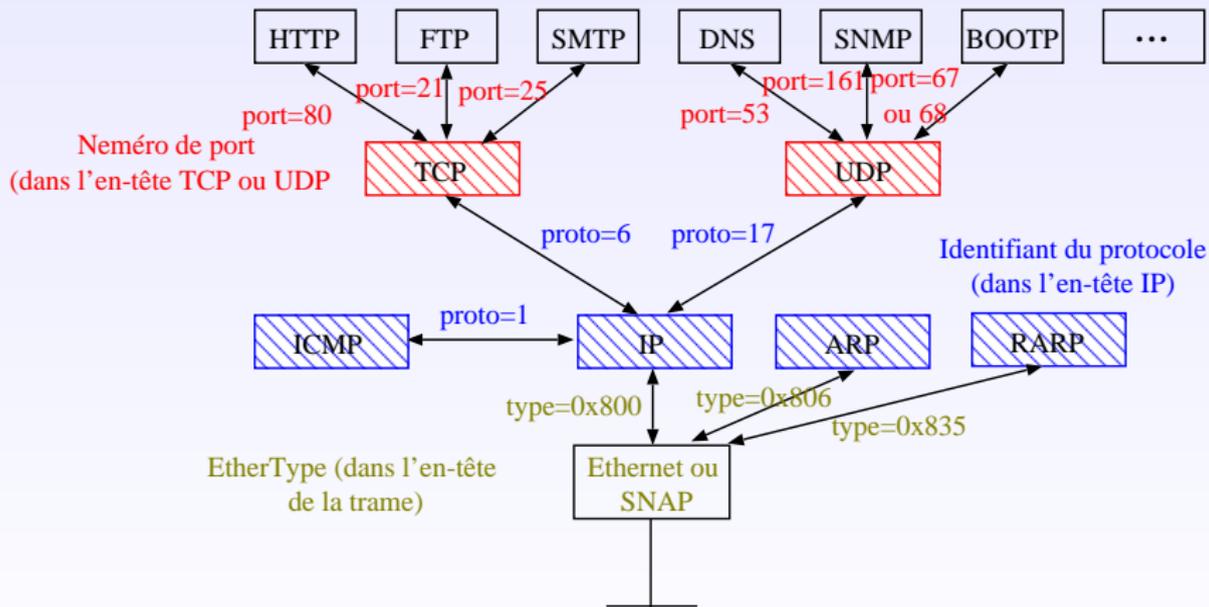
TCP - protocole de transport **de bout en bout**

- ★ uniquement présent aux **extrémités**
- ★ transport **fiable** de **segments** (mode **connecté**)
- ★ protocole complexe (retransmission, gestion des erreurs, séquençement, ...)

# L'architecture de TCP/IP (7)



# Identification des protocoles (1)



## Identification des protocoles (2)

- ★ Une adresse de transport = une adresse IP + un numéro de port (16 bits) → adresse de socket
- ★ Une connexion s'établit entre une socket source et une socket destinataire → une connexion = un quintuplé (proto, src, port src, dest, port dest)
- ★ Deux connexions peuvent aboutir à la même socket
- ★ Les ports permettent un multiplexage ou démultiplexage de connexions au niveau transport
- ★ Les ports inférieurs à 1024 sont appelés **ports réservés**

# Le protocole UDP

- ★ Performance sans garantie de délivrance
- ★ Souvent utilisé pour les applications multimédias
  - ▶ tolérantes aux pertes
  - ▶ sensibles au débit
- ★ Autres utilisations d'UDP
  - ▶ applications qui envoient peu de données et qui ne nécessitent pas un service fiable
  - ▶ exemples : DNS, SNMP, BOOTP/DHCP

## Transfert fiable sur UDP

- ▶ ajouter des mécanismes de compensation de pertes (reprise sur erreur) au niveau applicatif
- ▶ mécanismes adaptés à l'application

# Le protocole TCP

Transport Control Protocol (RFC 793, 1122, 1323, 2018, 2581)

Attention: les RFCs ne spécifient pas tout - beaucoup de choses dépendent de l'implémentation

Transport fiable en mode connecté

- ★ point à point, bidirectionnel : entre deux adresses de transport (@IP src, port src) → (@IP dest, port dest)
- ★ transporte un flot d'octets (ou flux)
  - ▶ l'application lit/écrit des octets dans un tampon
- ★ assure la délivrance des données en séquence
- ★ contrôle la validité des données reçues
- ★ organise les reprises sur erreur ou sur temporisation
- ★ réalise le contrôle de flux et le contrôle de congestion (à l'aide d'une fenêtre d'émission)

# Exemples de protocole applicatif

## HTTP - HyperText Transport Protocol

- ★ protocole du web
- ★ échange de requête/réponse entre un client et un serveur web

## FTP - File Transfer Protocol

- ★ protocole de manipulation de fichiers distants
- ★ transfert, suppression, création, ...

## TELNET - TELetypewriter Network Protocol

- ★ système de terminal virtuel
- ★ permet l'ouverture d'une session distante

## DNS - Domain Name System

- ★ assure la correspondance entre un nom symbolique et une adresse Internet (adresse IP)
- ★ bases de données réparties sur le globe

# Sous-réseaux

## Définition :

- ★ Un sous-réseau est un sous-ensemble d'un réseau de classe

## Intérêts :

- ★ diviser un réseau de grande taille en plusieurs réseaux physiques connectés par des routeurs (locaux ou distants)
- ★ possibilité de faire coexister des technologies de réseaux différentes
- ★ diminution de la congestion du réseau par redirection du trafic et réduction des diffusions

## Comment ?

- ★ ID sous-réseau en séparant les bits d'ID d'hôtes en plusieurs sections

# Linux : Positionner/Modifier une adresse IP

La manipulation des adresses IP se fait à l'aide de l'utilitaire *ifconfig*.

## Syntaxe :

```
ifconfig interface @IP netmask masque ...
```

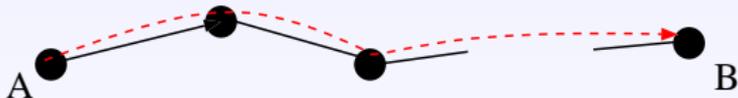
## Exemples :

- ★ `ifconfig eth0` (consulter la configuration de l'interface eth0)
- ★ `ifconfig eth0 192.168.0.1 netmask 255.255.255.0`  
(configurer l'interface eth0)
- ★ `ifconfig eth0 down` (Suppression de la configuration de l'interface eth0)

# Problématique du routage

**Objectif** : Acheminer des datagrammes IP d'une machine source A vers une machine destination B.

**Problématique** : Comment atteindre la machine B en connaissant son adresse IP?



→ Nécessité d'identifier toutes les machines intermédiaires.

# Routage IP : principe de base

## Définition :

- ★ Processus de choix des chemins par lesquels les paquets sont transmis à la machine destinataire
- ★ Processus basé sur une table de routage *IP routing table* contenant les informations relatives aux différentes destination possibles et à la façon de les atteindre
- ★ Exemple : netstat -r (sous UNIX)

## Principe de base :

- ★ L'émetteur ne connaît pas la route complète mais l'adresse du prochain site IP qui le rapprochera de la destination (prochain saut)
- ★ Simplicité des tables de routage
- ★ Changements dynamiques possibles (en cas de pannes par exemple)

# Tables de routage IP dans Linux

La consultation/modification de la table de routage peut être faite avec la commande `route`.

Exemple :

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
147.210.20.0	*	255.255.255.0	U	0	0	0	eth0
default	vlan2.labri.fr	0.0.0.0	UG	0	0	0	eth0

Cette table de routage montre que :

- ★ Notre hôte peut dialoguer directement avec les machines faisant partie du réseau 147.210.20.0/24
- ★ La route par défaut le fait passer par la passerelle `vlan2.labri.fr`

# Tables de routage IP dans Linux

La consultation/modification de la table de routage peut être faite avec la commande **route**.

Exemple :

```
route add default gw @passerelle (ajouter une route par défaut)
```

```
route add -host @hôte gw @passerelle dev iface (ajouter une route utilisant l'interface réseau iface vers un hôte particulier)
```

```
route add -net @réseau netmask masque dev iface gw @passerelle (ajouter une route utilisant l'interface iface vers un réseau particulier)
```

Pour les suppressions de route, il suffit de remplacer l'opération **add** par **del**.

# Analyse de la route

**traceroute.** montre le chemin vers des machines distantes en indiquant chaque 'hop' (saut) que fait un paquet sur la route vers la destination.

Exemple :

```
traceroute to vivaldi.emi.u-bordeaux.fr  
(147.210.13.225), 30 hops max, 40 byte  
packets
```

```
 1 vlan2.labri.fr (147.210.20.254)  
  5.579 ms 1.697 ms 6.420 ms  
 2 b3a1.labri.fr (147.210.9.254)  
  1.840 ms 4.924 ms 2.615 ms  
 3 labri-reaumur.u-bordeaux.fr  
  (147.210.246.190) 4.527 ms 5.561  
  ms 2.050 ms  
 4 vivaldi.emi.u-bordeaux1.fr  
  (147.210.13.225) 8.491 ms 2.448  
  ms
```

**pathchar, pchar, bing, ...** Outils de mesure de bande passante.

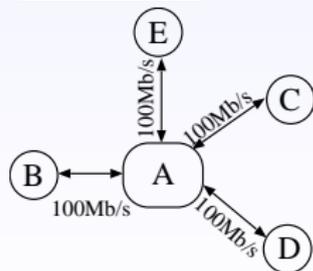
# Comment connecter des machines entre elles?

**Concentrateur (*hub*)** ★ Partage de bande passante entre les hôtes raccordés.

**Commutateur (*switch*)** ★ Pas d'interférences entre connexions simultanées.

**Routeur** ★ Pas d'interférences entre des connexions simultanées.  
 ★ Possibilité de communication entre 2 réseaux logiques différents.

Exemple :



		Type de A		
		Hub	Switch	Routeur
Débit (C→D) lorsque (B→E)		50 Mb/s	100 Mb/s	100 Mb/s
Comm. entre B et C si B et C sont dans deux réseaux différents		impossible	impossible	possible