

ADMINISTRATION DES RÉSEAUX
ROUTAGE ET PASSERELLE

A. Guermouche

Introduction

Routage dans IP

- Principes de base

- Manipulation des tables de routage

Mise en place d'un réseau

- comment connecter des machines entre elles?

- Routage avec Linux

Réseaux privé

Introduction

Routage dans IP

- Principes de base

- Manipulation des tables de routage

Mise en place d'un réseau

- comment connecter des machines entre elles?

- Routage avec Linux

Réseaux privé

Adresse IP (1/2)

Adresse IPv4

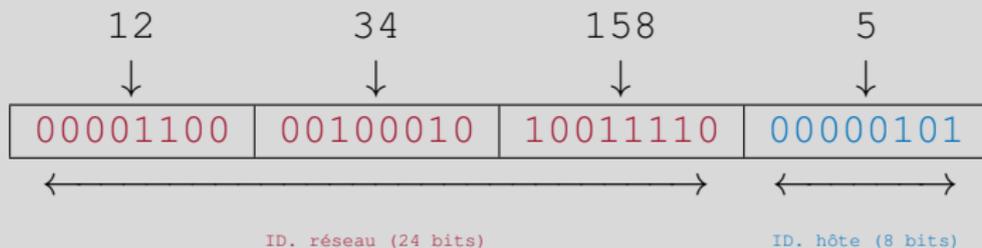
- Identifiant unique de 32 bits
- Identifie une interface réseau
- Représentée en notation décimale avec quatre nombres compris entre 0 et 255 (e.g. 12.34.158.5)



Adresse IP (2/2)

Structure de l'adresse IPv4

- L'adresse est divisée en deux parties : **réseau** et **hôte**
- 12.34.158.0/24 est un préfixe de 24 bits.



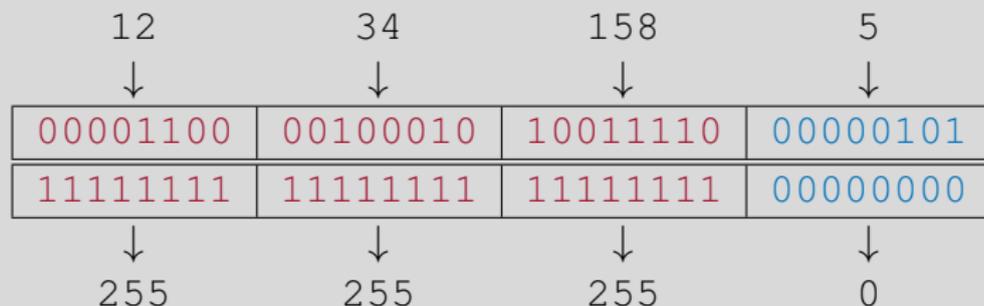
- ID réseau + zeros → adresse de réseau ¹
- ID réseau + uns → adresse de broadcast ¹
- ID réseau + ID hôte → adresse d'hôte

¹ne doit pas être attribuée à un hôte

Masque de sous-réseau

Principe

- Nombre de 32 bits
- Contenant uniquement des uns sur la partie ID réseau (et des zéros ailleurs)
- adresse IP & masque → adresse de réseau



- notation : 12.34.158.5/255.255.255.0 ou 12.34.158.5/24 (24 pour les 24 bits du masque)

Définition

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

Intérêt

- 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* ou *ip*.

Syntaxe :

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

ou

```
ip addr add @IP/masque dev interface ...
```

Exemples :

- `ifconfig eth0 up` ou `ip link set eth0 up` (activer l'interface eth0)
- `ifconfig eth0` ou `ip addr show eth0` (consulter la configuration de l'interface eth0)
- `ifconfig eth0 192.168.0.1 netmask 255.255.255.0` ou `ip addr add 192.168.0.1/24 dev eth0` (configurer l'interface eth0)
- `ifconfig eth0 down` ou `ip addr flush dev eth0` (Suppression de la configuration de l'interface eth0)

Introduction

Routage dans IP

- Principes de base

- Manipulation des tables de routage

Mise en place d'un réseau

- comment connecter des machines entre elles?

- Routage avec Linux

Réseaux privé

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` ou `ip route` (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
- Simplicité des tables de routage
- Changements dynamiques possibles (en cas de pannes par exemple)

Tables de routage IP (Linux)

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

Routage IP : algorithme de base (1/2)

1. Extraire du datagramme l'adresse IP de destination (*IPDest*)
2. Calculer l'adresse du réseau de destination (*IPRes*)
3. Si cette adresse *IPRes* correspond à l'adresse réseau du réseau local (la machine distante est dans le même réseau que l'émetteur) :
 - *IPdest* est directement accessible sur le réseau élémentaire commun
 - La couche IP locale tente la translation adresse logique *IPdest* en une adresse physique à travers la table maintenue en cache
 - Si le réseau est de type Ethernet (Tokenring, ...), le protocole ARP est utilisé pour construire les éventuelles entrées manquantes dans la table et émettra le datagramme
 - Si le réseau est d'un autre type (Transpac, ...), les adresses physiques destinataires X21 auront dû être configurées à la main au préalable

4. Sinon (ce n'est pas une adresse accessible, il faut alors consulter la table de routage IP locale)
 - Si *IPres* est dans la table alors :
 - Router le datagramme selon les indications de la table (vers un autre nœud du réseau local, avec résolution adresse IP → adresse physique, ou vers un autre routeur connecté à un réseau externe)
 - Sinon *IPres* n'est pas dans la table alors
 - Prendre la route par défaut indiquée dans la table
 - Router le datagramme selon les indications de l'entrée par défaut de la table (vers un autre nœud du réseau local, avec résolution adresse IP → adresse physique, ou vers un autre routeur connecté à un réseau externe)

Tables de routage IP dans Linux

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

Exemple

| | |
|--------------------------------|---|
| Ajout route par défaut | <code>route add default gw @passerelle</code> <code>ip route add default via @passerelle</code> |
| Ajout route vers hôte | <code>route add -host @hôte gw @passerelle dev iface</code> <code>ip route add @hôte via @passerelle dev iface</code> |
| Ajout route vers réseau | <code>route add -net @réseau netmask masque dev iface gw @passerelle</code> <code>ip route add @réseau/masque via @passerelle dev iface</code> |

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

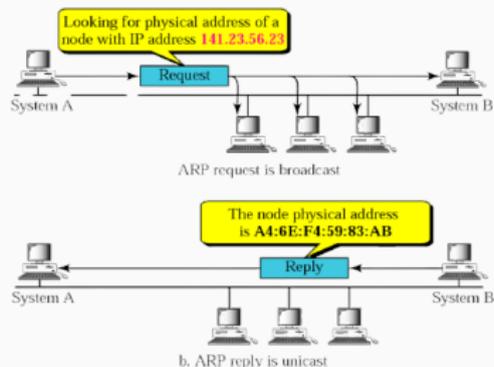
  1  vlan2.labri.fr
    (147.210.20.254) 5.579 ms 1.697
    ms 6.420 ms
  2  b3a1.labri.fr (147.210.9.254)
    1.840 ms 4.924 ms 2.615 ms
  3  labri-reaumur.u-bordeaux.fr
    (147.210.246.190) 4.527 ms 5.561
    ms 2.050 ms
  4  vivaldi.emi.u-bordeaux1.fr
    (147.210.13.225) 8.491 ms 2.448
    ms
```

pathchar, pchar, ping, ... Outils de mesure de bande passante.

ARP (Address Resolution Protocol)

Principe

- L'adresse IP sert à arriver dans un réseau mais elle ne peut pas être utilisée pour contacter la machine de destination via le réseau physique
 - Les adresses n'ont un sens que pour TCP/IP
 - Les adresses physiques sont les adresses utilisées au sein d'un réseau physique
- Nécessité de faire correspondre adresse IP et adresse physique
- ARP est basé sur un mécanisme de diffusion (broadcast)
- Utilisation d'un cache pour éviter de saturer le réseau avec les résolutions.



Introduction

Routage dans IP

- Principes de base

- Manipulation des tables de routage

Mise en place d'un réseau

- comment connecter des machines entre elles?

- Routage avec Linux

Réseaux privé

Comment connecter des machines entre elles?

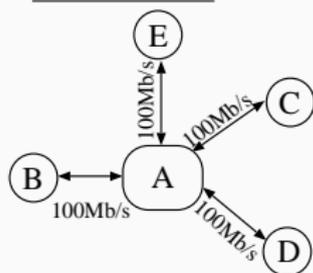
Concentrateur (*hub*) • Partage de bande passante entre les hôtes raccordés.

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

Routeur • Pas d'interférences entre des connexions simultanées.

- Possibilité de communication entre 2 réseaux logiques différents.

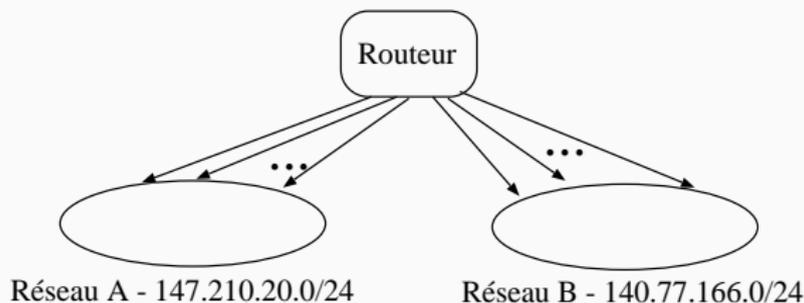
Exemple :



| | 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 |

Différences entre routeurs et passerelle

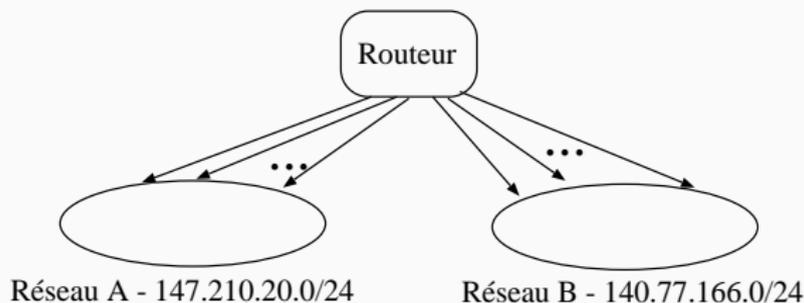
- Passerelle.** Élément faisant relais entre deux réseaux physiques utilisant des technologies différentes.
- Routeur.** Élément reliant deux réseaux différents (et les faisant communiquer).



Différences entre routeurs et passerelle

Passerelle. Élément faisant relais entre deux réseaux physiques utilisant des technologies différentes.

Routeur. Élément reliant deux réseaux différents (et les faisant communiquer).

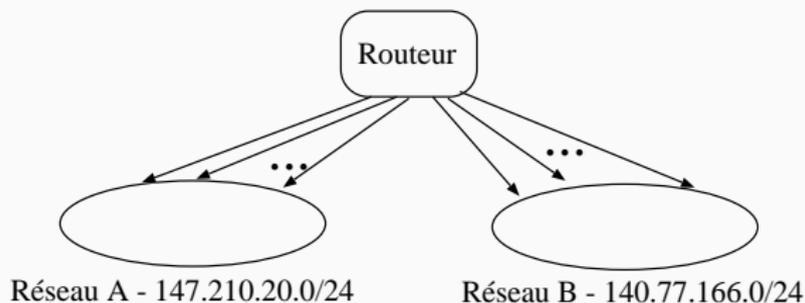


→ La différence est difficile à mettre en évidence de nos jours.

Différences entre routeurs et passerelle

Passerelle. Élément faisant relais entre deux réseaux physiques utilisant des technologies différentes.

Routeur. Élément reliant deux réseaux différents (et les faisant communiquer).



- La différence est difficile à mettre en évidence de nos jours.
- Matériels ayant "généralement" plusieurs cartes réseau.

- Support pour le routage disponible dans le noyau Linux.
 - Nécessité d'activer la fonctionnalité de "relais" dans le noyau.
Deux méthodes peuvent être utilisées :
 - Modifier "à chaud" le paramètre qui contrôle la fonctionnalité :
`echo 1 > /proc/sys/net/ipv4/ip_forward`
 - Configuration automatique à chaque démarrage :
Ajout de `net.ipv4.ip_forward=1` au fichier
`/etc/sysctl.conf`
- La machine en question fera alors office de relais entre ses différentes interfaces réseau.

Exercice

Étant données 4 machines, A,B,C et D.

Nous voulons connecter ces machines de telles sortes que A, B et C soient sur 3 sous-réseaux différents. D, quant à elle jouera le rôle de routeur.

Remarque :

Nous disposons d'un *switch* à au moins 4 ports.

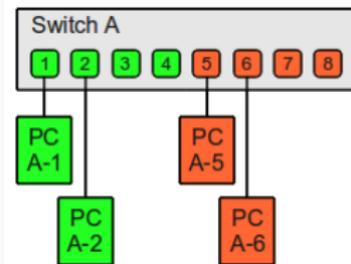
Nous considérerons les cas où D a 1 et 3 cartes réseau.

1. Déterminer les tables de routages pour les machines A, B, C et D. Montrer la séquence des commandes à lancer pour positionner les tables de routage à la bonne valeur.
2. Donner l'ensemble des étapes à effectuer au niveau de la machine D pour la configurer en routeur.

Virtual LANs (VLANs)

Principe

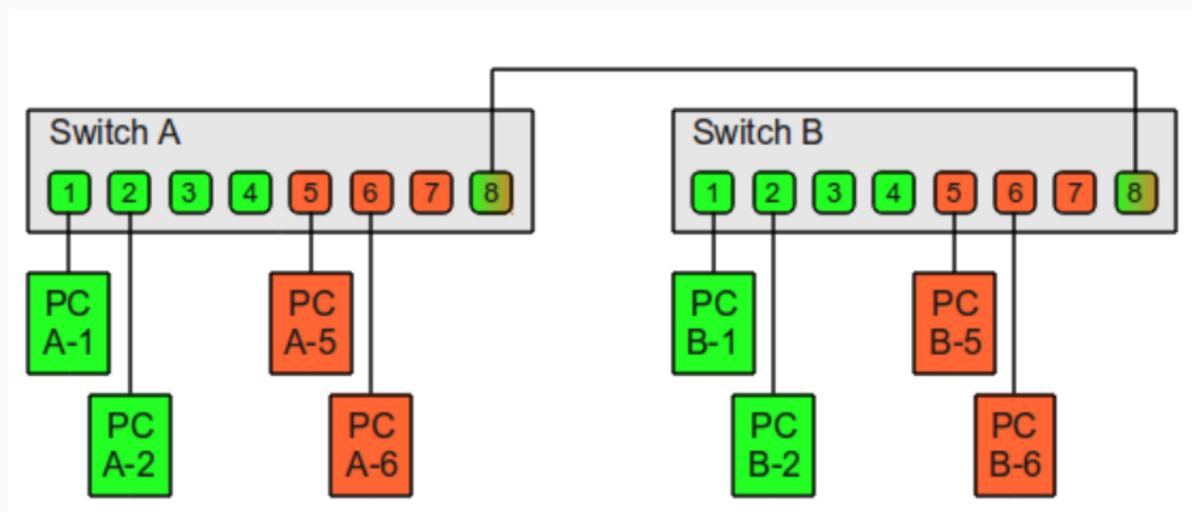
- Permet la division des switches en plusieurs switches “virtuel”
- Seuls les membres d'un VLAN peuvent en voir le trafic
 - Une communication inter-VLAN nécessite de passer par un routeur
- Les VLANs proposent une segmentation basée sur les domaines de diffusion
- 1 VLAN va correspondre à un sous-réseau IP



Principe

- Les ports du switch sont affectés à un numéro de VLAN
- Un broadcast dans un VLAN ne concerne que les ports appartenant au VLAN
- Se basent sur la norme 802.1q
 - Les paquets doivent contenir un tag VLAN
 - Qui positionne le tag?
- Deux de types de ports:
 - Ports *untagged* sont les ports pour lesquels le switch gère les tag
 - Il s'agit des Ports clients
 - Pour un paquet arrivant sur un port donné, le switch va ajouter le tag
 - Pour un paquet sortant d'un port donné, le switch va enlever le tag
 - Un port untagged ne peut appartenir qu'à un seul VLAN
 - Ports *tagged* sont les ports où le switch ne fait rien
 - Il s'agit des ports dédiés aux passerelles entre VLAN
 - Un port tagged peut appartenir à plusieurs VLAN

Fonctionnement des VLANs (2/2)



source <https://www.thomas-krenn.com/de/wiki/DE/images/4/4f/VLAN-Grundlagen-Beispiel-3.png>

Introduction

Routage dans IP

- Principes de base

- Manipulation des tables de routage

Mise en place d'un réseau

- comment connecter des machines entre elles?

- Routage avec Linux

Réseaux privé

Pourquoi avoir des adresses privées?

- Gérer la pénurie d'adresses au sein d'un réseau
- Masquer l'intérieur du réseau par rapport à l'extérieur (le réseau peut être vu comme une seule et même machine)
- Améliorer la sécurité pour le réseau interne
- Assouplir la gestion des adresses du réseau interne
- Faciliter la modification de l'architecture du réseau interne

→ Mécanisme de translation d'adresses (NAT - Network Address Translation)

Deux types de NAT :

statique. association entre n adresses publiques et n adresses privées.

dynamique. association entre 1 adresse publique et n adresses privées.