

**ATTENTION : il n'est pas autorisé de mettre en ligne ce fichier, merci. [promotion 2018/2019]**

# Administration des Réseaux Informatiques

PDF cours : [donné pendant le cours]



## Contenu

- Théorie
  - Les techniques d'interconnexion de réseaux locaux
    - Les VLANs
  - Les protocoles de routage intra domaine à vecteur de distance
    - RIP
  - Le protocole de routage intra-domaine à état de liens
    - OSPF
  - Les protocoles de routage inter-domaine
    - BGP
  - Traduction des noms de domaine
    - mise en œuvre de DNS
  - La configuration automatique des stations IP et de leurs adresses
    - DHCP

## Ce cours en chiffres..

- **12 h** : de cours magistraux – CM (6x2h)
- **4 h** : de travaux dirigées – TD (2x2h)
- **16 h** de travaux pratiques – TP (8x2h)
- Responsable du module :
  - Tayeb Lemlouma
    - Tayeb.Lemlouma@irisa.fr
    - Tayeb.Lemlouma@univ-rennes1.fr

## Contenu

- Pratique
  - Découverte des LAN, gestion des VLAN
  - Introduction au routage, routage statique
  - Routage dynamique : RIP
  - Routage dynamique, le protocole OSPF
  - Routage inter-domaine, le protocole BGP
  - Installation d'un système DNS
  - Installation du système DHCP

### 1.

## Interconnexion de réseaux locaux : Les VLAN

2h



- Répéteurs, amplificateur, interface, commutateur
- Pont (bridge)
- Aiguilleur (Routeur)
- Passerelle (Gateway)

Tayeb LEMLOUMA. Administration des Réseaux Informatiques, ISTIC, 2016-2017

6

## Les équipements et le modèle OSI

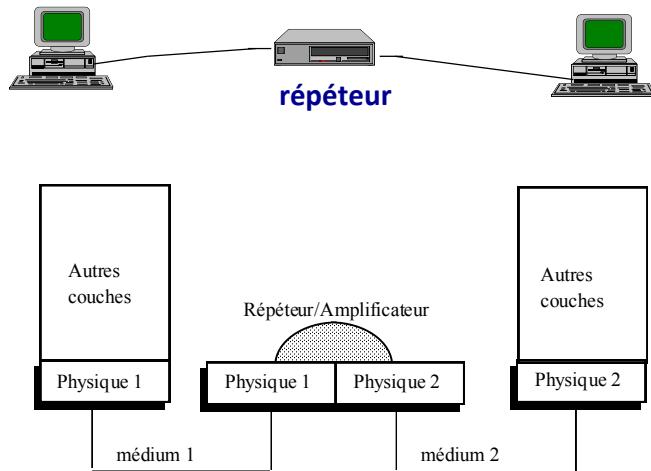
Équipement téléinformatique	Protocoles TCP/IP	Couches ISO
Passerelle	Telnet, SMTP,NFS, etc	Application
Routeur	TCP/UDP	Présentation
Pont	IP	Session
Supports physiques, Hub, Concentrateurs	802.2, PPP, Slip,HDLC	Transport
	Physique	Réseau
		Liaison
		Physique

## Interconnexion - répéteur

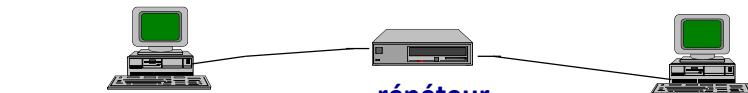


- Le répéteur et l'amplificateur sont des équipements téléinformatiques qui **relient deux médiums physiques entre eux**
- Le répéteur génère de nouveau **un signal** à partir du signal reçu .
- L'amplificateur consiste à **augmenter** la puissance du signal

## Interconnexion - répéteur



## Interconnexion - répéteur



### Avantages :

- coût;
- implantation facile.
- grand nombre de produits disponibles

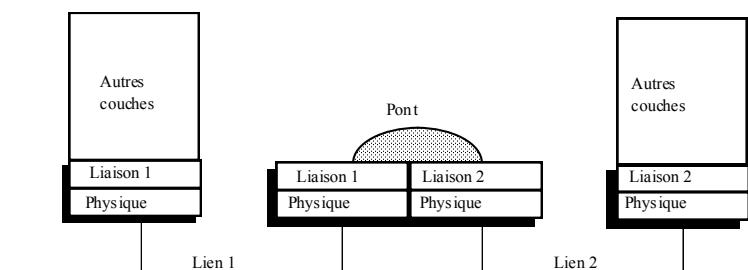
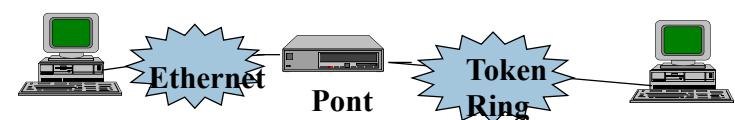
### Inconvénients :

- dépendance au réseau physique;
- sécurité faible;
- isolation des fautes faibles;
- peu de gestion et de contrôle;
- redondance très difficile.

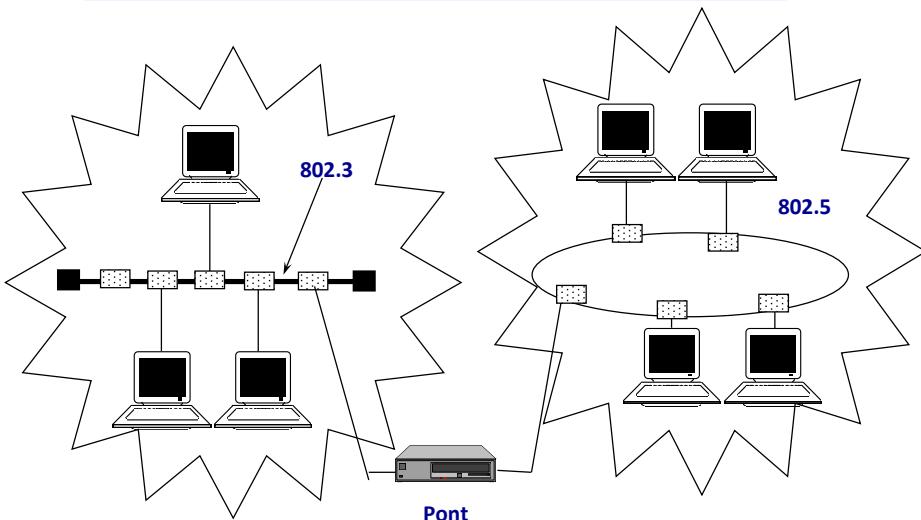
## Interconnexion – le pont

- Le pont **relie** deux réseaux identiques ou deux parties de même réseau.
- Le pont **relie** deux réseaux **au niveau de la couche Liaison**.
- Le pont agit comme **un relai** au niveau des trames et permet donc aux deux éléments qu'il relie de fonctionner indépendamment
- Sa présence permet d'optimiser les performances des réseaux et d'autoriser les utilisateurs d'un réseau à **accéder à toutes les ressources** disponibles sur l'autre réseau.
- Le pont ayant pour fonction de filtrer les trames, pour cela il possède des fonctions d'adressage qui lui permettent de **décider quelles trames il faut filtrer et lesquelles il ne faut pas filtrer**.

## Interconnexion – le pont



## Interconnexion – le pont



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

13

## Interconnexion – le pont

### • Avantages :

- grand nombre de produits disponibles;
- indépendance des protocoles;
- performance;
- implantation facile;
- isolation complète des segments;

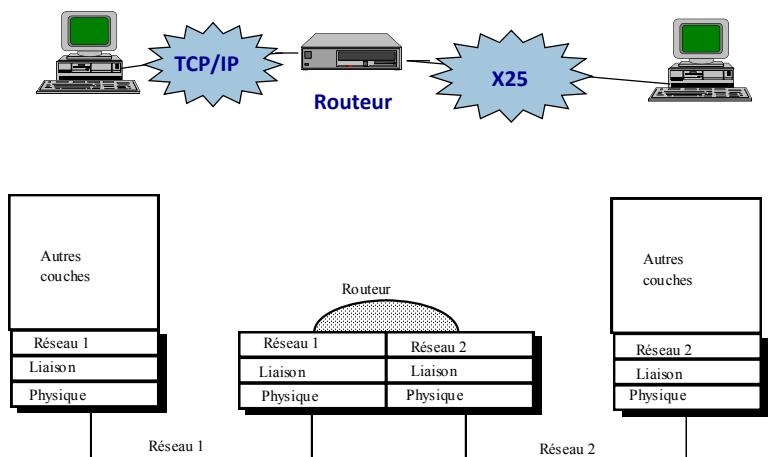
### ■ Inconvénients :

- rapport performance/coût moyen;
- gestion et sécurité très variable;
- redondance difficile;
- dépendant du réseau physique.

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

14

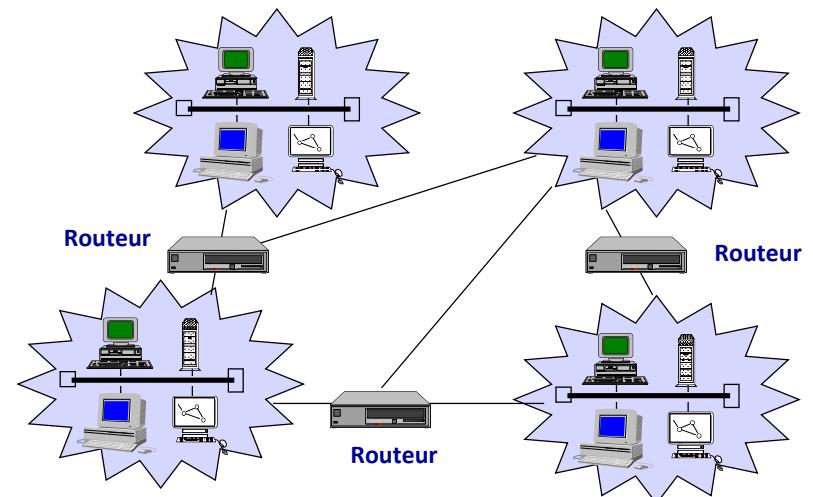
## Interconnexion – Routeur



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

15

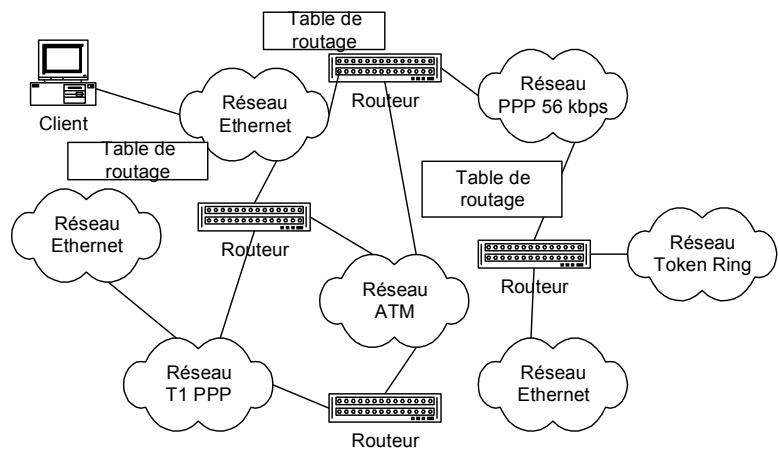
## Interconnexion – Routeur



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

16

## Interconnexion – Réseau



## Interconnexion – routeur

### ■ Avantages :

- isolation complète des “réseaux”;
- performance;
- indépendance du réseau physique.

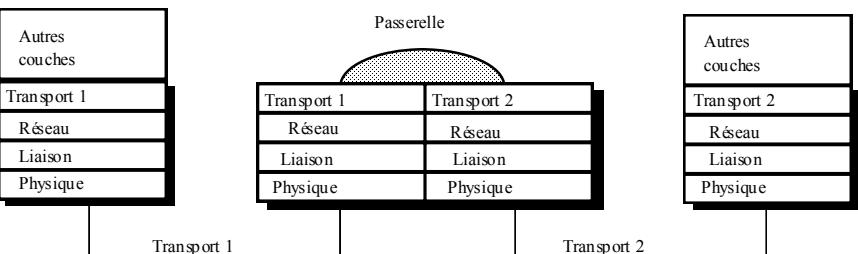
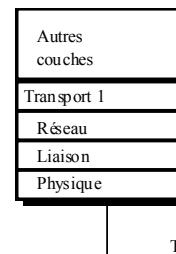
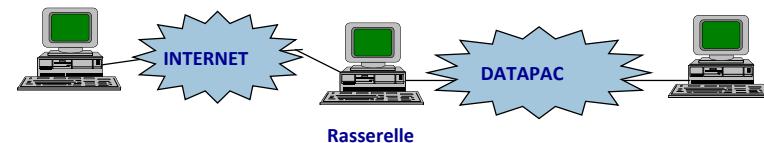
### • Inconvénients :

- délais de transmission élevés;
- rapport performance/coût mauvais;
- implantation et gestion complexe;
- dépendance des protocoles.

## Interconnexion – passerelle

- La passerelle relie deux entités de la couche **transport**, voire **des couches supérieures**.
- La passerelle relie deux réseaux différents voies incompatibles.
- Pour celà, elle dispose des **fonctions d'adaptation** et de conversion de **protocoles à travers plusieurs couches** de communication jusqu'à la couche Application.
- En un mot la passerelle relie **des réseaux hétérogènes**, et de constructeurs différents.

## Interconnexion – passerelle



## Interconnexion – passerelle

- Pont, routeur ou passerelle ?
- Critères
  - Coût
  - Interconnexion (les protocoles en jeu)
  - Routage
  - Performance
  - Sécurité (firewall)

## Interconnexion et VLAN

- Objectif

L'objectif de cette partie est de présenter la notion de vlan et introduire le routage inter-vlans.

A la fin de ce cours, vous aurez les connaissances nécessaires pour concevoir une architecture avancée d'un réseau d'entreprise.

Différents points seront abordés :

- Le principe des vlans.
- Introduction du routage inter-vlans.
- L'impact des vlans sur le schéma physique.

## Interconnexion et VLAN

- Contenu

- 1.Rappels sur la fonction switch.
- 2.Configuration de vlans sur un switch.
- 3.Les liens multi-vlans.
- 4.Routage inter vlans.
- 5.Architecture de base.
- 6.Notion d'architecture logique/physique.

## la fonction de « switch »

- Rappel sur la fonction switch



Cisco WS-C2960-8TC-L (225,68 € HT)  
Switch Cisco Catalyst 2960, niveau 2, format compact, 8 ports 10/100 + 1 port double Gigabit Base-TX

## la fonction de « switch »

- Un switch en action !



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

25

## la fonction de « switch »

### ➤ Il est composé :

- ↳ D'une CPU Central Processing Unit (intelligence ?).
- ↳ D'une RAM Random Access Memory (mémorisation dans le temps).
- ↳ D'un OS Operating System (intelligence ?).
- A l'heure actuelle, tous les switchs professionnels sont configurables en ligne de commande ou par l'intermédiaire d'un navigateur Web.
- Quand on veut avoir un accès physique au switch, on utilise le port console (liaison série).



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

27

## la fonction de « switch » (commutateur)

- Le switch ou commutateur est
  - un équipement réseau largement déployé dans les réseaux locaux des entreprises (LAN)
  - Aussi, chez les particulier



- Vous l'avez chez vous !
  - Votre box est un modem/routeur/switch.
  - Derrière la box se trouve plusieurs ports sur lesquels vous pouvez brancher vos
    - PC,
    - Imprimante réseau,
    - Console de jeux
    - TV



- Le switch n'a besoin que des couche 2 pour fonctionner (et par conséquent de la couche 1)



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

26

## la fonction de « switch »

### ➤ La "fonction switch" est un mécanisme appartenant à la **couche 2**.

- Modèle OSI : des tâches (fonctions/programmation) associées à des couches
- Modèle organisé en 7 couches

Envoi de message

Couche 7: Application  
Couche 6: Présentation  
Couche 5: Session  
Couche 4: Transport  
Couche 3: Réseau (acheminement : routage)  
**Couche 2: Liaison de données**  
Couche 1: Physique

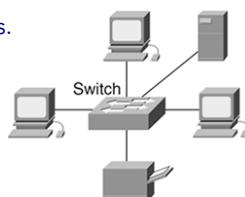
- Une couche peut communiquer avec les couches directement adjacentes
- Les protocoles définis : façons de décrire comment la communication doit se faire

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

28

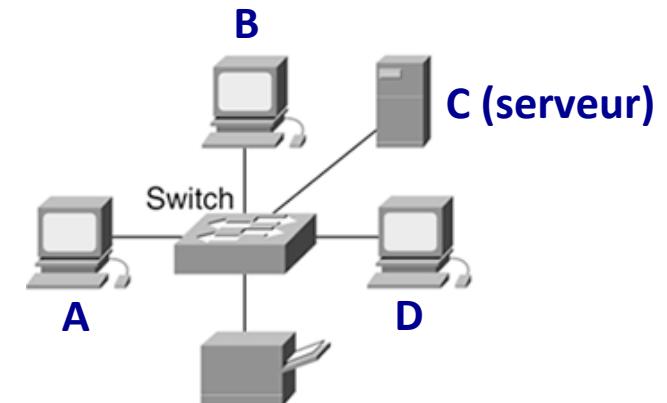
## la fonction de « switch »

- Le switch construit par **apprentissage** une table de correspondance entre @MAC et ses numéros de ports.
- Cette table est rafraîchie à intervalles réguliers pour prendre en compte d'éventuels changements (déplacement de câble, changement de carte réseau).
- C'est le standard courant pour les LANs qui utilisent une topologie physique en étoile.
- Le switch dispose :
  - ↳ De plusieurs ports servant à connecter les machines.
  - ↳ De ports spécialisés pour le configurer.



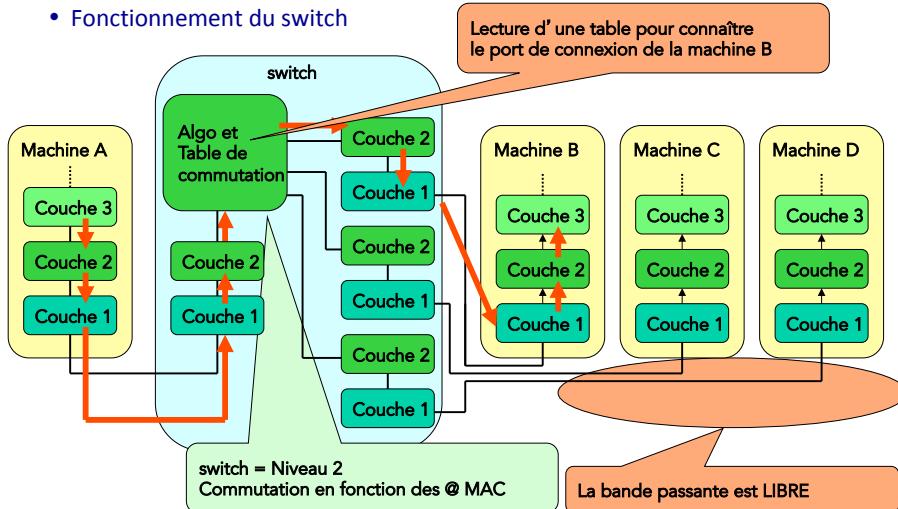
## la fonction de « switch »

- Fonctionnement du switch



## la fonction de « switch »

- Fonctionnement du switch



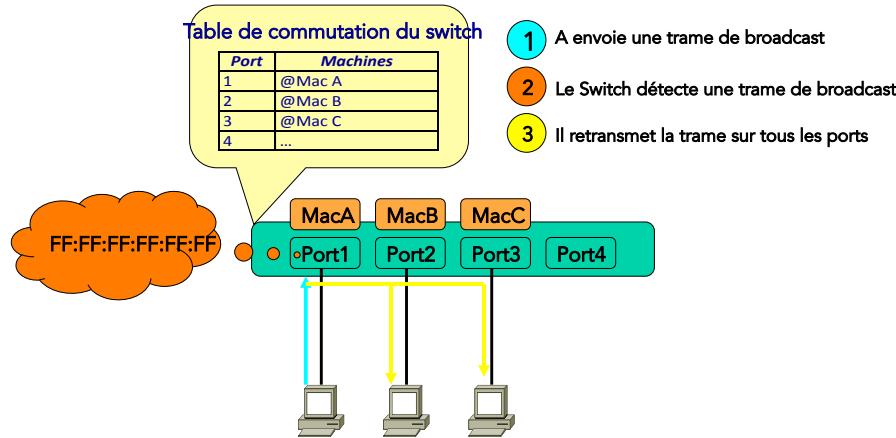
## la fonction de « switch »

- Fonctionnement du switch

- Le commutateur construit **dynamiquement** une table qui associe des adresses MAC avec des ports correspondants.
- Lorsqu'il reçoit une trame **destinée à une adresse présente** dans cette table, le commutateur renvoie la trame sur le port correspondant.
  - Si le port de destination est le même que celui de l'émetteur, la trame n'est pas transmise.
- Si l'adresse du destinataire **est inconnue** dans la table, alors la trame est traitée comme un **broadcast**, c'est-à-dire qu'elle est transmise à tous les ports du commutateur à l'exception du port d'émission.

## la fonction de « switch »

Traitement d'une trame (paquet) envoyé en « broadcast »



## la fonction de « switch »

### • Remarques

- On dit que le switch a “convergé” quand sa table MAC **contient toutes les adresses MAC** de son réseau
- La table MAC :
  - est effacée à chaque reboot du switch
  - a une taille finie (ex. sur un Cisco 2950 = 8000 entrées!)
- Ce fonctionnement d'apprentissage des adresses MAC est vulnérable à certaines attaques (ex. la saturation de table MAC)
- Pour visualiser le contenu de la table sur un switch Cisco:
  - `Switch# show mac-address-table`

## Interconnexion et VLAN

### • Contenu

- 1.Rappels sur la fonction switch.
- 2.Configuration de vlans sur un switch.
- 3.Les liens multi-vlans.
- 4.Routage inter vlans.
- 5.Architecture de base.
- 6.Notion d'architecture logique/physique.

## Configuration de VLAN sur un switch

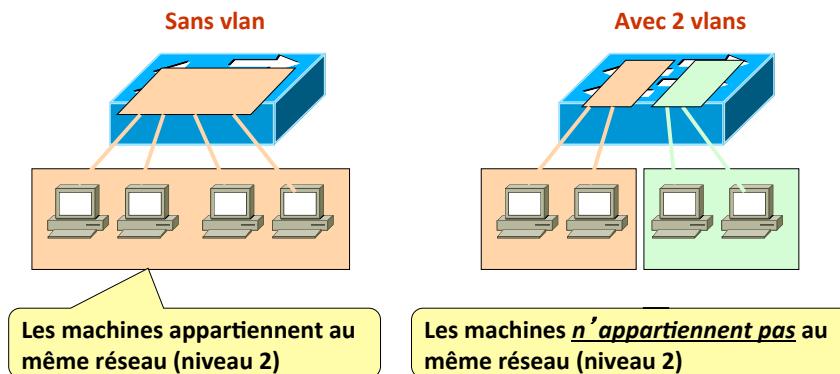
### Définition

VLAN signifie "**Virtual Local Area Network**".

- C'est un groupement logique de machines ou d'utilisateurs d'un réseau
- Limite la diffusion des informations qu'entre les membres de ce même groupe
- Virtuel : car les machines restent physiquement connectés entre elles
- Les VLANS sont mis en place par l'intermédiaire des switchs.
- Chaque port du switch est affecté à un VLAN soit en statique soit en dynamique.
- On peut gérer plusieurs réseaux IP sur un même switch (c'est à dire plusieurs domaines de broadcast), alors que dans un câblage traditionnel, toutes les machines connectées à un switch appartiennent au même réseau IP.

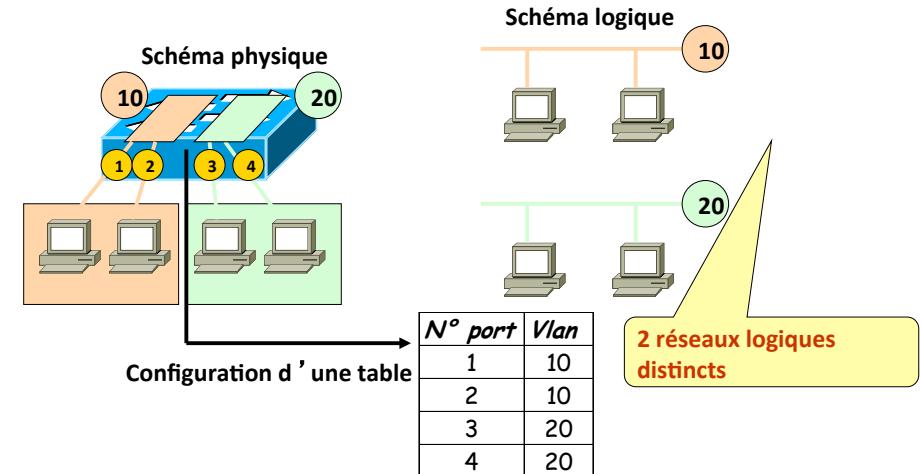
## Configuration de VLAN sur un switch

### Conception de vlans à l'aide de switch



## Configuration de VLAN sur un switch

### Schéma physique et logique



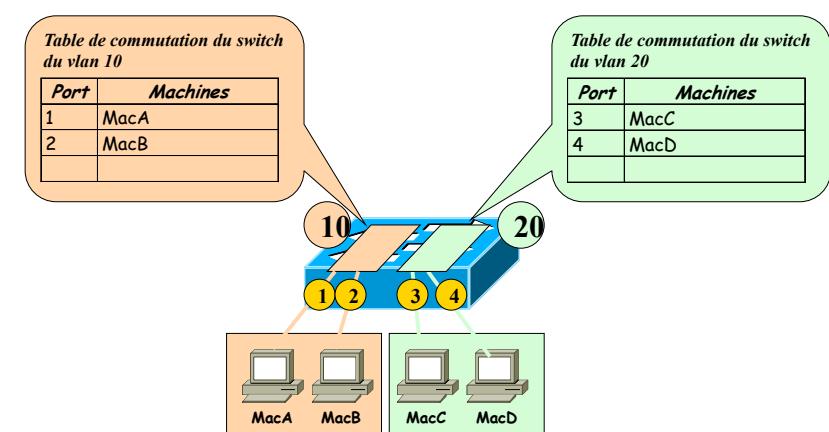
## Configuration de VLAN sur un switch

### Conséquences sur le fonctionnement du switch

- Une table par VLAN
- Le switch tient à jour une **table de commutation** pour chacun des **VLANs**.
  - si une trame arrive sur un **port appartenant au VLAN3**, le switch consultera la **table de commutation du VLAN3**.
- Un port est sur un VLAN
  - Si un port se voit attribuer un numéro de VLAN, par exemple 4, et qu'une trame de source inconnue arrive, l'@Mac source de cette trame sera ajoutée dans la **table de commutation du VLAN4**.
- On ne communique –au niveau 2- que dans le même VLAN
  - Pour qu'une trame **en provenance du VLAN4 soit transmise**, il faut que l'**@MAC destination appartienne au VLAN4** (en l'absence de routage).
- Un broadcast de niveau 2 (FF:FF:FF:FF:FF:FF) est transmis sur tous les machines du VLAN auquel appartient la machine.

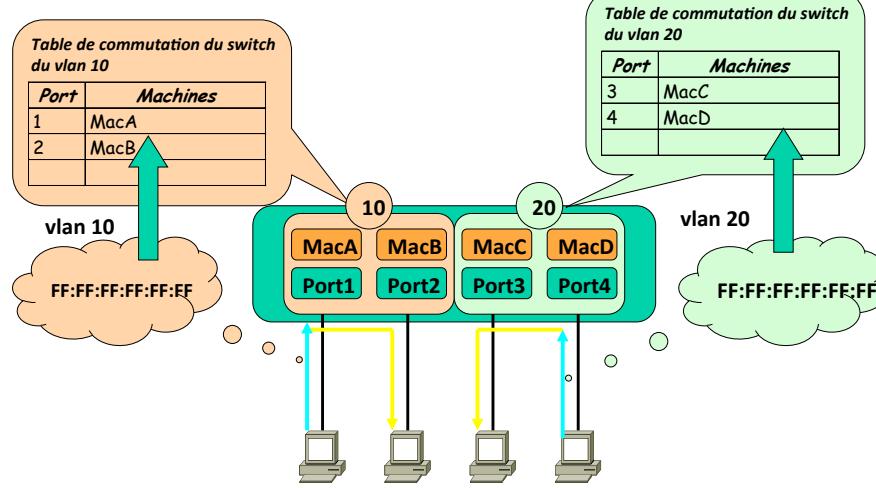
## Configuration de VLAN sur un switch

### Une table de commutation par VLAN



## Configuration de VLAN sur un switch

Traitement d'une trame de Broadcast



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

41

## Configuration de VLAN sur un switch

### Configuration des vlans

- Les machines ou les utilisateurs sont regroupés par **fonction, département ou application**, etc.

↳ Tous les ordinateurs et les serveurs utilisés par un groupe de travail feront partie du même VLAN ceci **quelque soit l'endroit** où ils se trouvent dans l'entreprise.

↳ Un PC appartenant au VLAN X ne pourra communiquer (directement au niveau 2) qu'avec les machines du VLAN X. C'est la fonction **routeage** qui va permettre de réaliser une connectivité inter-VLANS.

➤ La configuration ou reconfiguration des VLANS se fait **d'une manière logicielle**

↳ Il n'est donc **plus nécessaire** de déplacer les machines ou de refaire le câblage quand on veut réorganiser l'entreprise.

### Deux types différents de Vlans

↳ Statique.

↳ Dynamique.

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

42

## Configuration de VLAN sur un switch

### Configuration des vlans en statique (1 VLAN = {ports})

- Encore appelés VLANs axés sur le port (port-based VLAN).
  - ↳ L'administrateur réseau **configure** le switch **port par port**.
- Chaque **port est associé à un VLAN** particulier. Donc tous les utilisateurs connectés à ces ports appartiendront au même VLAN.
  - ↳ Les utilisateurs ignorent leur appartenance au VLAN.
  - ↳ L'administrateur devra **changer manuellement la configuration** si on déplace les machines (ceci permet de ne pas changer le câblage).
  - ↳ Facilité de gestion pour l'administrateur car la **configuration est simple**.

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

43

## Configuration de VLAN sur un switch

### Configuration des vlans en dynamique (1 VLAN = {@mac})

- ↳ Les ports chargent automatiquement leur configuration **en fonction de l'@MAC** de la machine (et éventuellement **d'autres paramètres**) qui vient de se connecter
- ↳ Le switch **utilise une base de données** (table de correspondance entre @MAC et numéro de VLAN par exemple). Bien sûr, cette base de données a été préalablement renseignée par l'administrateur réseau ou par un logiciel (annuaire par exemple) !
- ↳ L'administrateur réseau devra **modifier la base de données** en cas de changement de carte réseau ou d'achat de nouvelles machines.

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

44

## Interconnexion et VLAN

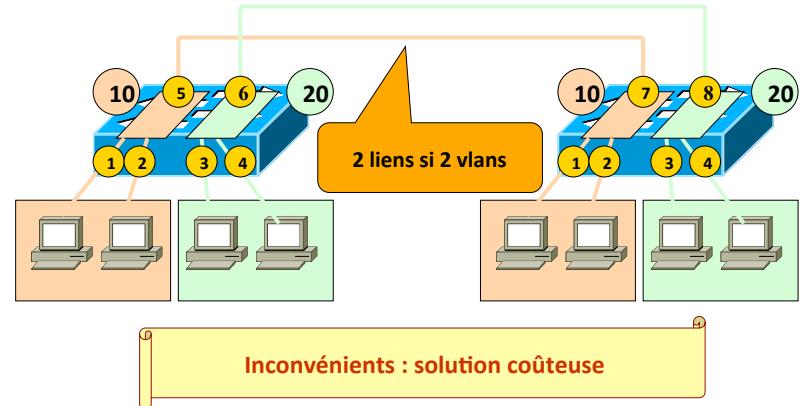
### • Contenu

1. Rappels sur la fonction switch.
2. Configuration de vlans sur un switch.
3. Les liens multi-vlans.
4. Routage inter vlans.
5. Architecture de base.
6. Notion d'architecture logique/physique.

## Les liens multi-vlans

### Connexion "classique" de 2 switchs

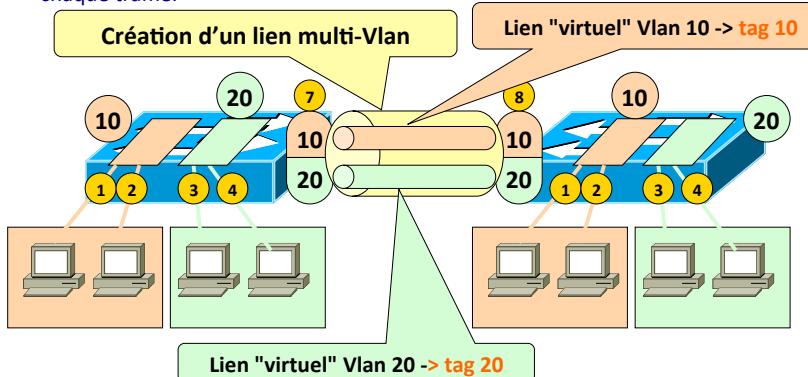
Quand on désire connecter 2 switchs configurés avec des Vlans, la première solution consiste à utiliser "un lien par Vlan" :



## Les liens multi-vlans

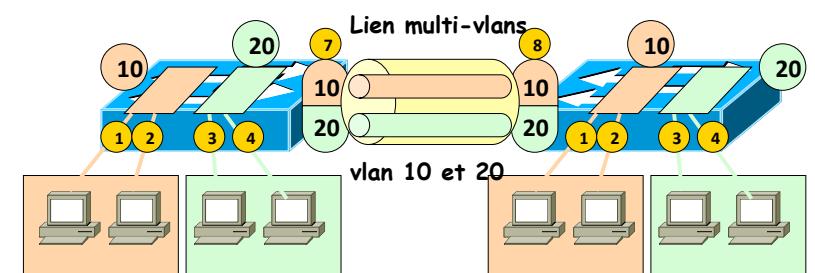
### Configuration d'un lien multi-vlans

- Pour pouvoir utiliser un seul lien, il faut pouvoir faire passer plusieurs Vlans sur un unique lien
- ✓ idée : utilisation d'une étiquette (tag) pour identifier de quel Vlan provient chaque trame.



## Les liens multi-vlans

### Les liens multi-vlans



Pour identifier une trame, un drapeau (étiquette/tag) est ajouté pour identifier le VLAN à laquelle elle appartient. Cette méthode d'identification est appelée marquage de trame "frame tagging".

Dans le cas du standard "802.1q", le marquage "tag" est inséré dans la trame.

## Les liens multi-vlans

### Fonctionnement

- Un **identifiant unique "tag"** est placé dans l'**entête** de chaque trame quand elle est expédiée sur les **liens multi-vlans** (i.e. le réseau *backbone*).
- Cet identifiant est compris et examiné par **chaque switch** avant toute transmission
- Quand la trame quitte le backbone, le switch **retire cet identifiant** avant de la transmettre à la machine finale
- Le **marquage** de trames fonctionne au niveau de la **couche 2** et demande peu de ressources processeur.
- Le standard "802.1q" appelé encore "dot1q" (point 1 Q) est le plus répandu à l'heure actuelle.
- Certains fabricants ont développé des marquages de trames propriétaires (ex. *l'encapsulation ISL propriétaire Cisco*), mais ils sont peu à peu abandonnés au profit du "802.1q".

## Les liens multi-vlans

### Format des trames

Trame non taggée :

@MAC dst	@MAC Src	Type de trame (0x0800 pour IP)	Données
6 octets	6 octets	2octets	

Trame taggée :

@MAC dst	@MAC Src	Type de trame (0x8100 pour 802.1q)	Champ Vlan	Type de trame (0x0800 pour IP)	Données
6 octets	6 octets	2octets	2 octets	2octets	

Champ 802.1q

## Les liens multi-vlans

### Format des trames

Exemple de capture de trame :

```
Frame 2 (64 bytes on wire, 64 bytes captured)
Ethernet II, Src: 00:04:75:ee:22:11, Dst:
ff:ff:ff:ff:ff:ff
802.1q Virtual LAN
 000. .... .... = Priority: 0
  ...0 .... .... .... = CFI: 0
  .... 0000 0000 0011 = ID: 3
Type: ARP (0x0806)
Trailer: 00000000000000000000000000000000...
Address Resolution Protocol (request)
```

## Les liens multi-vlans

### Format des trames

#### Priority:

On dispose de 3 bits donc de priorités variant de 0 à 7. On peut donc **fixer une priorité aux trames d'un VLAN relativement aux autres VLANs**.

#### CFI:

Ce champ codé sur 1 bit assure la **compatibilité entre les adresses MAC Ethernet et Token Ring**. Un commutateur Ethernet fixera toujours cette valeur à 0.

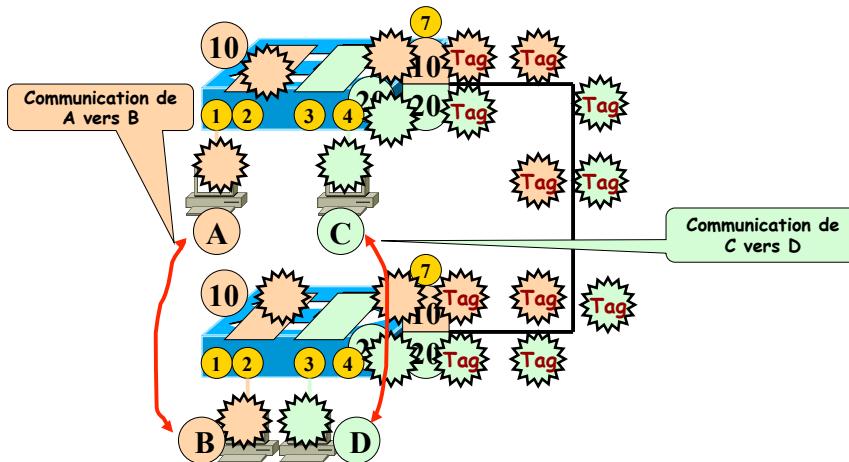
#### ID:

**Identifiant de vlan** (numéro variant de 1 à 4095)

## Les liens multi-vlans

### Exemple

Communication entre deux machines appartenant au même vlan via deux switchs.



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

53

## Interconnexion et VLAN

### • Contenu

1. Rappels sur la fonction switch.
2. Configuration de vlans sur un switch.
3. Les liens multi-vlans.
4. Routage inter vlans.
5. Architecture de base.
6. Notion d'architecture logique/physique.

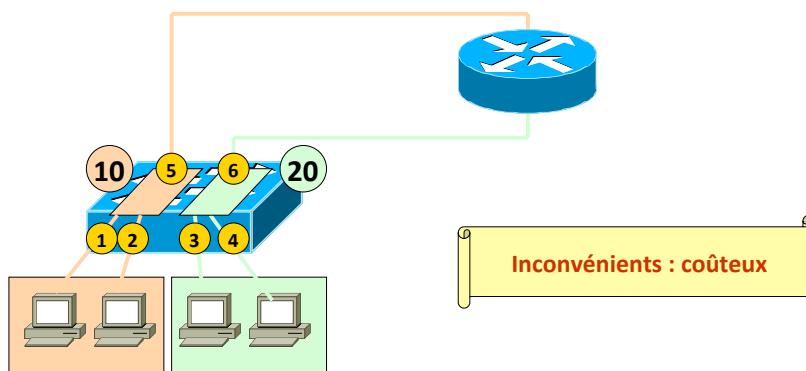
Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

54

## Routage inter-vlans

### Connexion "classique" entre switch et routeur

Quand on désire connecter un switch configuré avec des vlans à un routeur, la première solution consiste à utiliser "un lien par Vlan" :



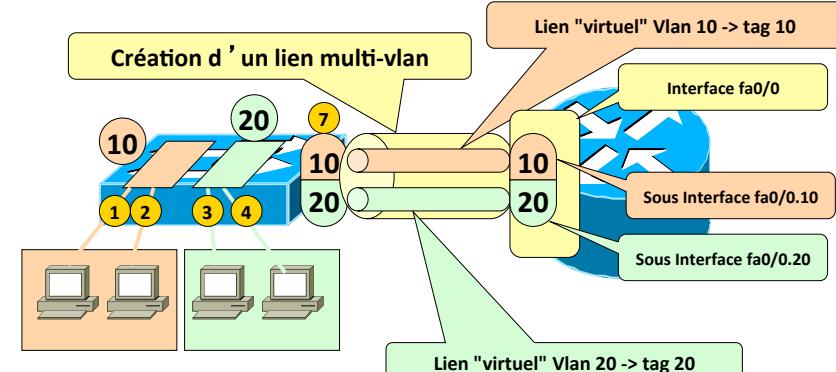
Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

55

## Routage inter-vlans

### Configuration d'un lien multi-vlans

Pour pouvoir utiliser un seul lien, il faut pouvoir  
↳ Configurer deux "sous interfaces" (car deux Vlans) sur une interface du routeur.  
↳ Le routeur va gérer lui aussi un tag pour identifier de quel Vlan provient chaque trame.



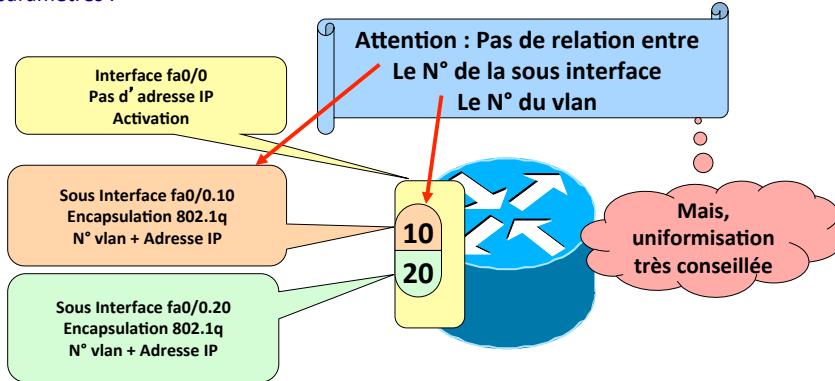
Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

56

## Routage inter-vlans

### Configuration des sous interface du routeur

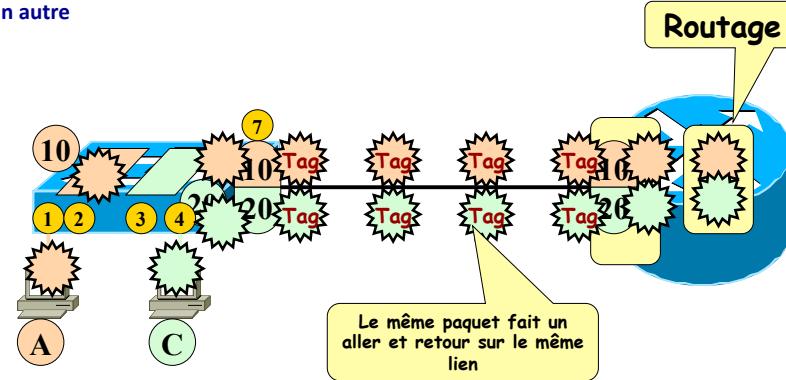
- Pour chaque sous interface du routeur, il faut configurer un certain nombre de paramètres :



## Routage inter-vlans

### Exemple

- Communication d'un paquet de la machine A vers la machine C.
- Le paquet circule "taggé" sur le lien multi-vlans. Le routeur assure le passage d'un VLAN à un autre



## Routage inter-vlans

### Evolution des technologies

- Certains switchs récents disposent de fonctionnalités de niveau supérieur et sont désignés comme "switchs de niveau 3 (ou plus)" par abus de langage.
  - Exemple : Les HP ProCurve 2626 de chez Hewlett Packard peuvent assurer un routage simple inter-Vlans si l'**option est configurée**.
  - Par défaut, seule la fonction de base du switch est validée (**commutation**).
- Par souci de rigueur, nous devrions dire que le HP2626 assure les fonctions de commutation standards et un routage simple et non pas le désigner sous le nom de switch.
- C'est pour cela qu'il faut plutôt parler :
  - De la fonction de *commutation* (switch).
  - De la fonction de *routage*.



## Routage inter-vlans

### Conclusion

- Les trames à l'arrivée et au départ des machines ne sont pas taggées.
- Les "tags" sont ajoutés ou enlevés par les **switchs ou le routeur**.
- Seul le routeur (fonction routage) permet la **communication inter-Vlans**.
- Certaines **cartes réseau** peuvent gérer le protocole **802.1q**
  - C'est le cas sur la plupart des cartes réseau des machines **serveurs**
- Dans ce cas, il faut un **lien multi Vlans** entre le switch et les cartes des machines supportant ce protocole.

## Interconnexion et VLAN

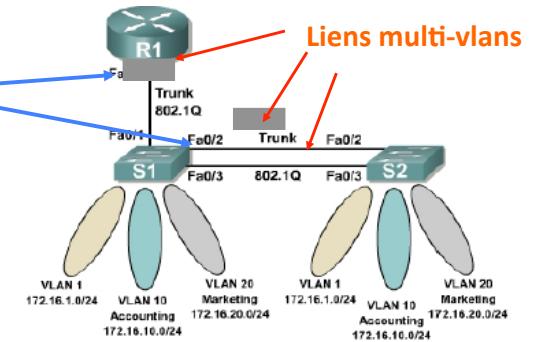
### • Contenu

1. Rappels sur la fonction switch.
2. Configuration de vlans sur un switch.
3. Les liens multi-vlans.
4. Routage inter vlans.
- 5. Architecture de base.**
6. Notion d'architecture logique/physique.

## Architecture de base

### Architecture de base

↳ Quand on utilise le protocole 802.1q et le routage inter-vlans, on obtient l'architecture réseau de base suivante :



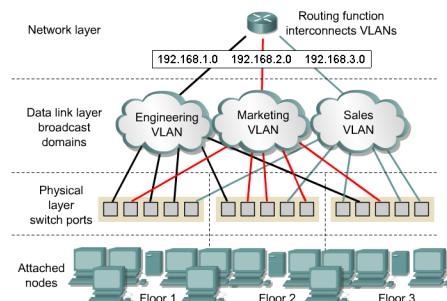
↳ Chaque lien physique transporte les 3 vlans  
→ on minimise les coûts :  
il n'est pas nécessaire  
d'utiliser une interface  
par vlan

## Architecture de base

### Les atouts

Il est facile :

- ↳ D'ajouter des hôtes sur les LANs.
- ↳ De changer la configuration des LANs
- ↳ De contrôler le trafic sur le réseau.
- La sécurité est renforcée grâce à la possibilité de contrôler l'accès aux ports.



## Interconnexion et VLAN

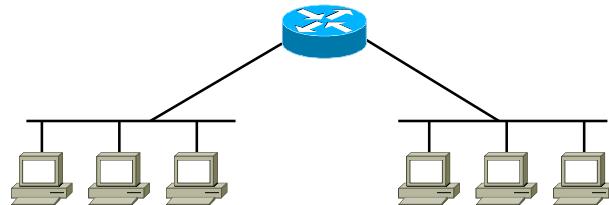
### • Contenu

1. Rappels sur la fonction switch.
2. Configuration de vlans sur un switch.
3. Les liens multi-vlans.
4. Routage inter vlans.
5. Architecture de base.
- 6. Notion d'architecture logique/physique.**

## Notion d'architecture logique/physique

### Exemple d'un petit cahier des charges

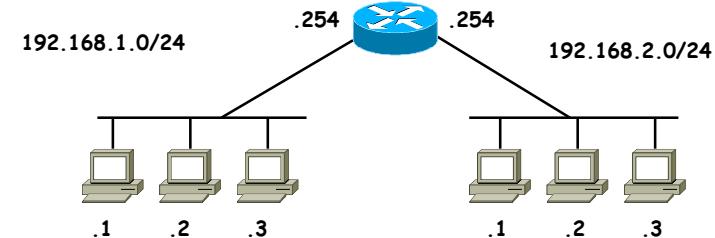
Vous souhaitez mettre en place un réseau constitué de deux sous-réseaux :



## Notion d'architecture logique/physique

### Schéma logique de votre réseau

- ↳ Le schéma logique du réseau est un schéma qui
  - doit présenter les différents réseaux,
  - avec la notion de routage (pour interconnecter les réseaux).
  - Il ne doit y avoir aucune indication de la technologie utilisée pour regrouper les différentes machines d'un réseau.
  - Un maximum d'adresses logiques doivent être présentes.

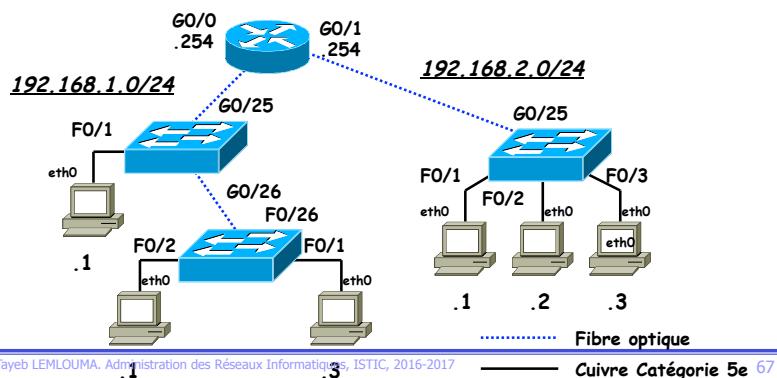


## Notion d'architecture logique/physique

3 h

### Schéma physique de votre réseau – Forme 1

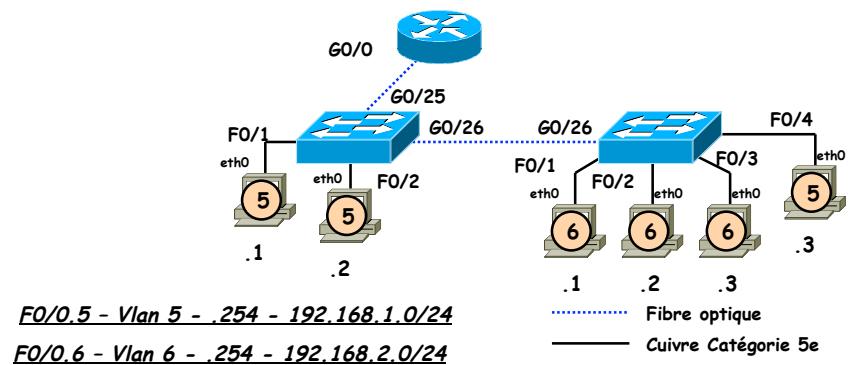
- ↳ Le schéma physique du réseau est un schéma qui doit
  - présenter les différents éléments utilisés pour effectuer le câblage de votre réseau,
  - le maximum d'information (@IP/mask, équipements, nom interfaces/ports, type de câbles, etc.)
  - Il doit à la fois être le plus complet possible et être le plus clair possible
  - Un débutant doit être en mesure de retrouver le même réseau avec votre schéma



## Notion d'architecture logique/physique

### Schéma physique de votre réseau – Forme 2

- ↳ Le schéma physique du réseau est un schéma qui doit présenter les différents éléments utilisés pour effectuer le câblage de votre réseau, avec le maximum d'information. Il doit à la fois être le plus complet possible et être le plus clair possible.

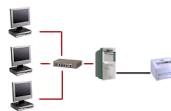


## Introduction et principes de base du routage

### 2.

#### Protocoles de routage intra domaine à vecteur de distance : RIP

2h

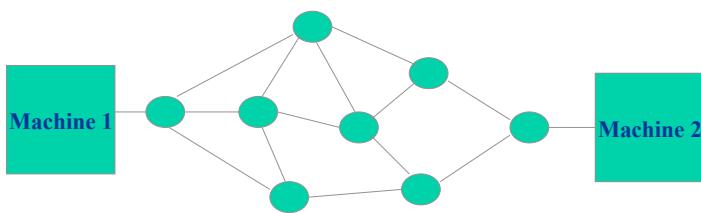


- Le besoin d'échanger des messages : **inévitable** en local ou en distribué
- Un réseau informatique permet aux processus de s'échanger des messages
- **Comment ?** définir des règles d'échange normalisées pour chaque type d'application → **PROTOCOLE**
- n'importe qui peut définir un protocole
- pour la standardisation : il faut se faire **accepté** par la communauté scientifique et industrielle & faire **les preuves** du protocole

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

70

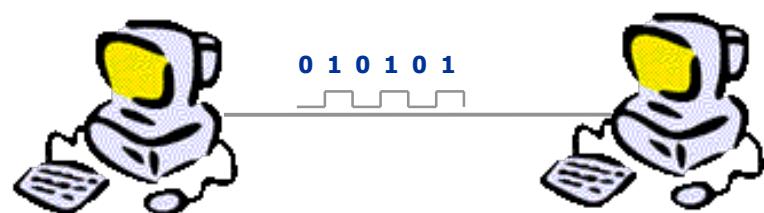
## Introduction et principes de base du routage



- Deux machines reliées au réseau, communiquent grâce aux autres **noeuds du réseau** qui routent de manière **coopérative** sur la base de l'adresse destinataire

Coopérative ?

## Introduction et principes de base du routage



- Un **noeud** est une entité tel qu'un ordinateur, routeur ou autre, un transfert dans un réseau est **un ensemble** de transferts « **point à point** »
- Quel autre type de transfert peut-on avoir?



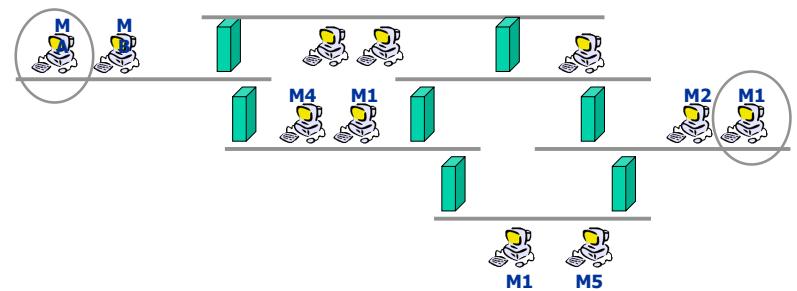
Il faut donc définir les **matériels** et **procédures** nécessaires à un échange entre deux noeuds

# Introduction et principes de base du routage

Dans un réseau il est nécessaire de normaliser :

Fonction	Protocole
Les échanges entre processus	http, ftp, smtp
Les services de transfert	Tcp , udp
Les techniques et algorithmes de routage	Ip, x25
Les procédures d'échange entre deux machines	HdLC, lap, ppp
Les composants nécessaires à la connexion des machines	Carte réseau, modem

## Transfert entre machines



L'interconnexion pose certains problèmes :

- Ambiguïté possible dans les adresses
- Plusieurs routes possibles
- Contrôle des échanges : fiabilité, erreurs

## Le Routage

- OSI : des tâches associées à des couches
- Modèle organisé en 7 couches

Envoi de message

Couche 7: Application  
Couche 6: Présentation  
Couche 5: Session  
Couche 4: Transport  
Couche 3: Réseau (acheminement : routage)  
Couche 2: Liaison de données  
Couche 1: Physique

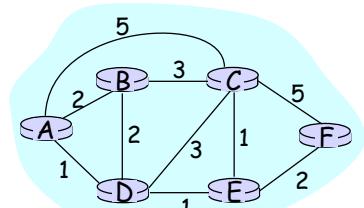
- Une couche peut communiquer avec les couches directement adjacentes
- **Les protocoles définis** : façons de décrire comment la communication doit se faire

## Le Routage

Protocole de routage  
Objectif : choisir un « bon chemin » (suite de routeurs) dans le réseau de la source à la destination.

Abstraction du réseau en graphe

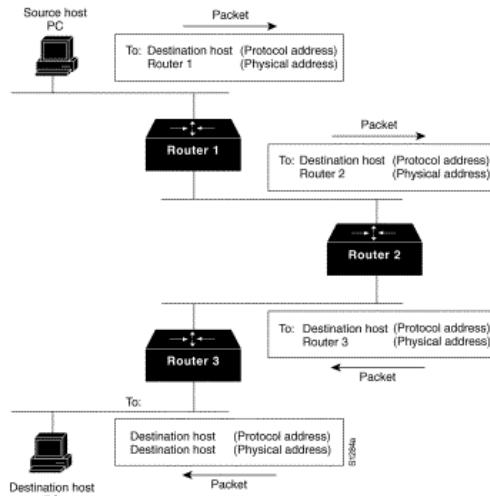
- Les nœuds sont des routeurs
- Les liens sont les liaisons physiques
  - Coût du lien : délai, prix du lien ou niveau de congestion



• «Bon chemin» :

- Typiquement un chemin de coût minimal
- Autres définitions possibles

## Le Routage, exemple de trajet



## Routage

### Définition de la stratégie de routage

=  
processus permettant à un paquet d' être acheminé vers le destinataire lorsque celui-ci n' est pas sur le même réseau physique que l' émetteur (en fonction de la politique choisie)

Le **routeur** réalise le choix du chemin en appliquant un algorithme particulier à partir de **tables de routage**.

Il existe différents manières de router les paquets :

- non adaptatif (fixe, inondation)
- adaptatif (isolé, centralisé, distribué)
- mixte

## Algorithm

### Algorithme de routage :

♦ Extraire l' adresse IP destination,

♦ Pour chaque ligne de la table :

    Calculer l' adresse du réseau destination en appliquant le masque

    Si le résultat = adresse de réseau d'une ligne existante alors router le paquet vers l' adresse passerelle

♦ Si aucune ligne ne permet le routage et s' il existe une route par défaut router le paquet vers la passerelle par défaut

♦ Sinon déclarer une erreur de routage

## Routage statique

- Le routage consiste à faire circuler de routeur en routeur les paquets de données
- L'administration d'un routeur consiste à configurer les routes d'un routeur
- Une route est définie par un *réseau de destination* et *l'adresse d'un routeur voisin*, i.e. prochaine étape vers le réseau de destination
- Les tables de routage contiennent des listes de routes utilisée par le routeur pour prendre des décisions quant à la direction à donner pour un paquet reçu sur l'une de ses interfaces
- Le routage statique par opposition au routage dynamique, consiste à saisir (configurer) **manuellement** toutes les routes dans le routeur

## Routage statique

- Il faut indiquer manuellement sur chaque entité de routage un minimum d'information :
  - Les adresses des réseaux que l'on cherche à atteindre,
  - L'interface correspondante sur le routeur à configurer ou adresse IP du routeur voisin

### Problèmes et difficultés

## Routage dynamique



L'homme ou la machine ?

plutôt que de centraliser la configuration du routage dans les mains d'un **individu** dont le temps de réaction est fatallement long et les risques d'erreurs importants, **la tâche est répartie au niveau des routeurs**

- En effet, chaque routeur connaît les réseaux qui lui sont directement connectés ainsi que l'état de ses interfaces.

## Routage statique

### Difficultés

- Lorsque le réseau global est complexe, la configuration peut être **fastidieuse** et source d'**erreurs**
- Scalabilité** : Dès qu'un réseau est ajouté, il faut reconfigurer l'ensemble
- Fiabilité** : afin de prévenir tout dysfonctionnement, il faut surveiller en permanence le réseau pour reconfigurer chaque routeur en cas de ligne coupée, panne de routeur etc.
- Tolérance aux pannes (défaillance)** : Quand la panne est réparée, il faut rétablir la configuration précédente ...

### En conclusion, avec le routage statique :

- Les « protocoles » de routage n'ont pas le choix de leurs routes (c'est fixé)
- Cette technique convient bien aux petits réseaux ne subissant pas de d'évolutions ou de changements fréquents
- Il ne s'agit pas vraiment d'un protocole de routage au sens où cela peut être pris pour le routage dynamique

## Routage dynamique

```
Lab_A#show ip route
Codes: [C - connected] S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

R    210.93.105.0/24 [120/3] via 201.100.11.2, 00:00:21, Serial0/0
C    205.7.5.0/24 is directly connected, FastEthernet0/1
R    219.17.100.0/24 [120/1] via 201.100.11.2, 00:00:21, Serial0/0
R    199.6.13.0/24 [120/1] via 201.100.11.2, 00:00:21, Serial0/0
R    204.204.7.0/24 [120/2] via 201.100.11.2, 00:00:21, Serial0/0
C    192.5.5.0/24 is directly connected, FastEthernet0/0
R    223.8.151.0/24 [120/2] via 201.100.11.2, 00:00:21, Serial0/0
C    201.100.11.0/24 is directly connected, Serial0/0
S*   0.0.0.0/0 is directly connected, Serial0/0
```

Figure. Visualisation de la **table de routage** sur un routeur Cisco

## Routage dynamique

4h

City# show ip interface brief						
Interface	IP-Address	OK?	Method	Status	Protocol	
FastEthernet0/0	192.168.12.48	YES	manual	up	up	
FastEthernet0/1	192.168.12.65	YES	manual	up	up	
Serial0/0	192.168.12.121	YES	manual	up	up	
Serial0/1	unassigned	YES	unset	up	up	
Serial0/1.102	192.168.12.125	YES	manual	up	up	
Serial0/1.103	192.168.12.129	YES	manual	up	up	
Serial0/1.104	192.168.12.133	YES	manual	up	up	

City#

Figure. Visualisation de l'état des interfaces sur un routeur Cisco

## Routage dynamique

- Les protocoles de routage dynamiques répondent à d'autres besoins et en particulier dès que les topologies des réseaux deviennent **complexes**
- Dans une configuration de routage dynamique, un protocole particulier est mis en oeuvre pour **construire dynamiquement les chemins entre routeurs**
- Exemple**
- Le protocole **RIP** (*Routing Information Protocol*) est un des protocoles **d'échange dynamique des tables de routage IP sur un réseau local**
- Le protocole RIP permet à un routeur **d'échanger** des informations de routage **avec les routeurs avoisinants**

## Routage dynamique



L'homme ou la machine ?

- De manière **générale** :



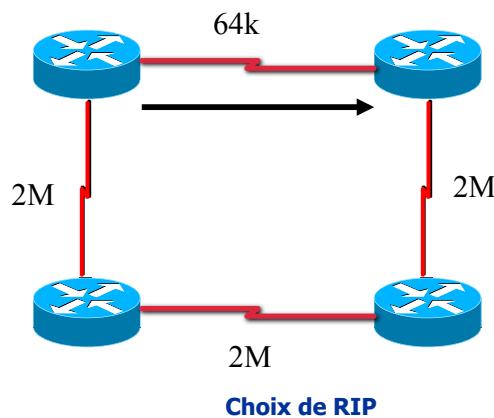
- Chaque routeur transmet ces informations à ses **voisins** et de proche en proche elles se **répandent** à tout le réseau.
- L'intervention humaine se situe en amont dans **la définition de règles** à appliquer par les routeurs pour la diffusion des routes.

## La métrique

### Choix d'une route et métrique :

- Pour déterminer une route à utiliser, un routeur va se baser sur "**métrique**"
- Cette valeur est déterminée par un ou plusieurs critères
- Le protocole RIP ne prend en compte que le **nombre de sauts** (hop) pour déterminer le chemin le plus court. (sa **métrique**)
- D'autres protocoles peuvent prendre en compte **d'autres paramètres** comme la charge, le nombre de sauts, la bande passante, le délai, la charge...

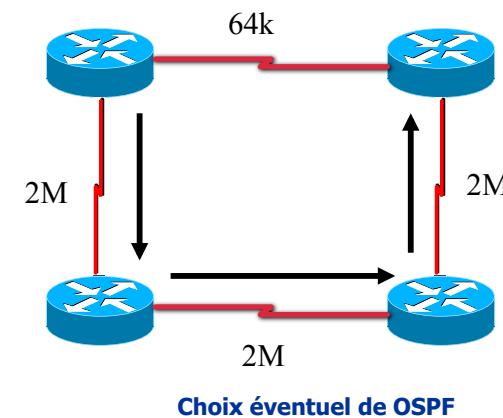
## La métrique



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

89

## La métrique



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

90

## Routage dynamique

- RIP - Protocole de routage à vecteur de distance.**
- IGRP - Protocole de routage à vecteur de distance de Cisco.**
- OSPF - Protocole de routage à état de liens. (Open Shortest Path First)**
- EIGRP - Protocole de routage hybride symétrique.**

**EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) sont des protocoles de routage inter AS.**

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

91

## Classification

- Information globale ou locale ?**
  - Statique ou dynamique ?**
    - Statique :**
      - Les routes ne changent pas dans le temps
    - Dynamique :**
      - Les routes changent régulièrement
        - Mise à jour régulière
        - En réponse aux changements de coût des liens

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

92

# Classification

## I - Les algorithmes Vector-Distance :

- Algorithmes simples
- Pas de diffusion d'un extrait des meilleurs chemins
- Diffusion sous forme d'un *vecteur* où une distance est associée à chaque entrée
- Diffusion entre voisins direct (de saut en saut)
- Les protocoles qui utilisent cet algorithme (**exemple RIP**), se basent sur le nombre de sauts (hop) comme métrique pour sélectionner un chemin
- Le routage à vecteur de distance détermine la direction (le vecteur) et la distance par rapport à une liaison du réseau
- Un routeur diffuse régulièrement (toutes les 30 secondes) à ses voisins les routes qu'il connaît
- Une route est composée d'une adresse destination, d'une adresse de passerelle et d'une métrique indiquant le nombre de sauts nécessaires pour atteindre la destination
- Une passerelle qui reçoit ces informations compare les routes reçues avec ses propres routes connues et met à jour sa propre table de routage
- Le problème vient souvent du fait que la taille des tables de routage est proportionnelle au nombre de routeurs du domaine et que cela génère très vite une charge importante sur le réseau en plus de la convergence qui peut être lente

# Classification

## I - Les algorithmes Vector-Distance :

- **Algorithme (+ protocole) :**
  - vecteur de distance ("distance vector algorithm")
  - algorithme réparti de calcul du plus court chemin
  - décrit par [Bellman & Ford - 1957]
  - amélioré par [Ford & Fulkerson – 1962]
  - **différent de l'algorithme** centralisé de calcul du plus court chemin décrit par Dijkstra - 1959 ("Shortest Path First")
- **Implémentation :**
  - première apparition : RIP du réseau XNS de Xerox
  - RIP-1 : RFC 1058 - juin 1988
  - RIP-2 : RFC 1388 - juin 1993.

# Classification-

## II - Les algorithmes Link state (état de liens) :

- Deux phases :
  1. Diffusion à tous de la connaissance sur les liaisons locales
  2. Calcul local des meilleurs chemins sur les informations ainsi rassemblées
- L'algorithme Link State, est basé sur la technique "Shortest Path First" (SPF)
- Les routeurs maintiennent une carte complète du réseau et calculent les meilleurs chemins localement en utilisant cette topologie
- Ils ne communiquent pas, comme dans l'algorithme "Vector Distance" la liste de toutes les destinations connues
- Les routeurs valident l'état des liens qui les relient et communiquent cet état aux routeurs voisins
- Cette technique recrée un état du réseau. Elle utilise en premier le plus court chemin d'abord mais peut utiliser d'autres paramètres
- Les routeurs mettent à jour leur carte et recalculent localement pour chaque lien modifié, la nouvelle route selon l'algorithme de Dijkstra shortest path algorithm qui détermine le plus court chemin pour toutes les destinations à partir d'une même source

# Classification

## III - Les techniques hybrides :

Ce sont des protocoles qui utilisent les deux techniques de routages, comme le protocole EIGRP de Cisco.

## Exemple : RIP

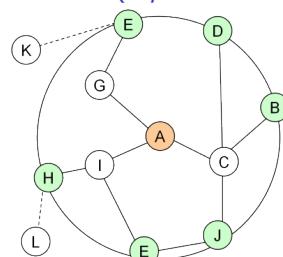
- Dès qu'un routeur est informé d'une modification quelconque de la configuration sur les réseaux (telle que l'arrêt d'un routeur), il transmet ces informations aux routeurs avoisinants
- Les routeurs envoient également des paquets de diffusion générale RIP périodiques (30s) contenant toutes les informations de routage dont ils disposent (Cisco : **timers basic update invalid holddown flush**)
- Ces diffusions générales assurent la synchronisation entre tous les routeurs
- Avec un protocole comme RIP, on peut considérer que les tables de routages des routeurs et passerelles sont constituées et mises à jour automatiquement

## Le protocole de routage RIP

- Protocole **RIP** : Routing Information Protocol (RFC 1058, juin 1988 - RFC 2453, version 2, novembre 1998)
- Protocole permettant à un routeur d'échanger des informations de routage avec un autre routeur, afin de mieux déterminer les chemins à suivre sur le réseau
- Un protocole de type Vecteur Distance (*Vector Distance*), c'est-à-dire que chaque routeur communique aux autres routeurs la distance qui les sépare (le nombre de saut qui les sépare)
- Mais ... pourquoi les distances ?!
- Distance : concept de métrique fondamental dans le domaine du routage.
- Il est fréquent (c'est même recherchée) que le réseau ait une topologie maillée pour des raisons de tolérance aux pannes => plusieurs chemins mènent à la même destination. Le routeur doit alors choisir le chemin qu'il considère le meilleur vers une destination donnée

## Le protocole de routage RIP

- La seule métrique utilisée par RIP est la distance correspondant au nombre de hôtes ou routeurs à traverser (*hop* ou nombre de sauts) avant d'atteindre un réseau
- Pour chaque chemin, RIP calcule la distance. Ensuite, si des chemins redondantes apparaissent, RIP retient celui qui traverse le moins de routeurs (donc avec la distance la plus faible)
- La longueur d'un chemin (et donc le diamètre du réseau) est limitée. La norme limite la distance maximale d'une route à 15 ( $>15 = \text{"infinie"}$  pour RIP) => deux réseaux ne peuvent être éloignés de  $> 15$  routeurs.



## L' algorithme RIP appliqué

- Lors de l'initialisation du routeur, celui-ci détermine l'adresse réseau de ses interfaces puis envoie sur chacune une demande d'informations (table RIP complète) aux routeurs voisins
- Lors de la réception d'une demande, le routeur envoie sa table complète ou partielle suivant la nature de cette demande.
- Lors de la réception d'une réponse, il met à jour sa table si besoin :
  - pour une **nouvelle** route, il incrémenté la distance, vérifie que celle-ci est strictement inférieure à 15 et diffuse immédiatement le vecteur de distance correspondant
  - pour une **route existante** mais avec une distance plus faible, la table est mise à jour. La nouvelle distance et, éventuellement, l'adresse du routeur si elle diffère sont intégrées à la table
  - si le routeur reçoit une route dont la **distance est supérieure à celle déjà connue**, RIP l'ignore. Ensuite, à intervalles réguliers (les cycles durent 30 secondes environ), la table RIP est diffusée qu'il y ait ou non des modifications (pourquoi ? Réponse dans le slide suivant ! )

## L'algorithme RIP appliqué

- Une route doit être retirée de la table gérée par RIP dans deux cas :

1) Un noeud immédiatement connecté devient inaccessible (panne de l'interface, de la ligne, modification de la topologie..) :

- Les routeurs RIP reliés à ce noeud **affectent** dans leur tables une distance "**infinie**" (16 !) à cette route
- **Conservée pendant un délai** (de "maintien" ou garbage collect) puis supprimée
- Pendant ce délai, **le vecteur est diffusé**. Un routeur qui reçoit un vecteur avec une distance de 16 comprend : "*il faut que tu retires cette route de ta table car elle est devenue invalide !*". De proche en proche, cette information se propage

1) Un routeur du réseau tombe en panne :

- Comment le savoir ? RIP considère qu'un routeur qui n'a pas donné de nouvelles depuis 3 minutes est hors-service. A chaque réception d'un vecteur de distance déjà présent dans la table, le time-out associé à la route est réinitialisé
- Si un autre routeur connaît une route menant vers un des noeud que l'on vient de retirer, la nouvelle route sera re-intégrée (**tolérance de panne**)

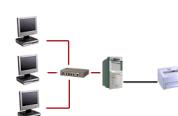
Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

101

3.

## Protocoles de routage intra-domaine à état de liens : OSPF

2h



## RIP version 2 (RFC 2453)

- Inconvénients :
  - faiblesse des algorithmes à vecteurs de distance que l'on appelle "**problème de la convergence lente**"
  - transmissions mutuelles inutiles et propagations d'informations contradictoires en particulier dans le cas de pannes
- Améliorations :
  - "**split horizon**" : une information de routage reçue d'une interface n'est jamais retransmise sur celle-ci
  - "**poison reverse**" (temporisateur de maintien) et "triggered update" : une panne est immédiatement diffusée sans attendre le prochain cycle de diffusion des tables => réduire le délai de convergence
- Version 2 :
  - diffusion des masques de sous-réseaux associés aux adresses réseaux (dans la version 1, on utilisait que les masques réseau par défaut)
  - utilisation d'adresses multicast pour diffuser les vecteurs de distance au lieu d'adresses de broadcast, ce qui réduit l'encombrement sur le réseau
  - l'authentification crypté avec MD5
  - interopérabilité entre protocoles de routage en diffusant des routes apprises à partir d'autres protocoles

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

102

## Le protocole de routage OSPF

- Le protocole **OSPF** (*Open Short Path First*) a été défini par IETF pour résoudre les problèmes posés par l'utilisation de RIP et entre autres le temps de convergence
- Actuellement, ce temps de convergence est d' environ d'une minute avec l'utilisation d'un protocole tel que OSPF
- Beaucoup plus complexe que RIP. Il est décrit dans la volumineuse (224 pages) **RFC-2328 (version 2-avril 1998. Versions 2 antérieures : 2178, 1583, 1247 et la première version 1131, voir ietf.org)**
- **Caractéristiques et fonctionnement du protocole OSPF**
- OSPF présente des caractéristiques importantes :
  - C'est un protocole ouvert (pas de copyright)
  - Il utilise l'algorithme SPF (Short Path First) dans ses calculs de route pour déterminer le plus court chemin
  - Principe d'adjacence : deux routeurs sont dits adjacents s'ils ont synchronisé leurs bases de données topologiques

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

104

## Le protocole de routage OSPF

- Le protocole OSPF fait partie de la seconde génération de protocole de routage (**Link-state** Protocole)
- Beaucoup plus complexe que RIP mais ses performances et sa stabilité sont supérieures
- Le protocole OSPF utilise une **base de données distribuées** qui permet de garder en mémoire l'état des liaisons
- Ces informations forment une **description de la topologie** du réseau et de l'état de l'infrastructure
- OSPF est un protocole de routage intra-domaine, c'est-à-dire qu' il ne diffuse les informations de routage qu' entre les routeurs appartenant à un **même système autonome** (*un ensemble de réseaux qui utilisent un protocole de routage commun et qui dépend d'une autorité d'administration unique*)

## Le protocole de routage OSPF

- La **base d'information topologique** d'un système autonome décrit un **graphe orienté**. Les  **noeuds** du graphe sont des **routeurs** ou bien des réseaux tandis que les **liens** représentent les **connexions** physiques.
- Les réseaux sont dits de **transit** si plusieurs routeurs y sont connectés ou **terminaux** dans le cas contraire.
- A chaque réseau est associé une **adresse IP** et un **masque réseau**.
- Une machine seule (*host*) est considérée comme un réseau terminal avec un masque égal à 0xFFFFFFFF.

## Le protocole de routage OSPF

- **Le problème :** dans les systèmes de routage, si le réseau est trop grand
  - overhead du traffic dans le réseau,
  - calculs trop longs,
  - dimensionnement mémoire trop grand
- **La solution :** routage hiérachique
  - découpage du réseau en parties indépendantes (Areas)
  - reliées par un BackBone (Area BackBone)
- **La fonctionnalité**
  - chaque area constitue un réseau indépendant
    - la table des liaisons ne contient que les liaisons de l' Area,
    - le protocole d' inondation s' arrête aux frontières de l' Area,
    - les routeurs ne calculent que des routes internes à l' Area
  - certains routeurs (*area border routers*) appartiennent à plusieurs Areas (en général une Area inférieure et une Area BB) et transmettent les informations récapitulatives des Areas qu' ils relient.

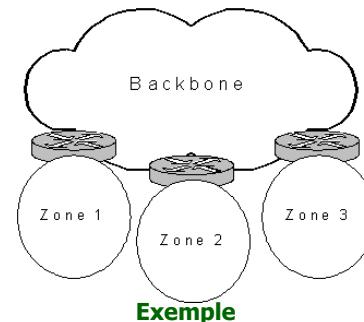
## Le protocole de routage OSPF

- **L' intérêt de définir des zones :**
  - **Limiter le trafic de routage**
  - **Réduire la fréquence des calculs du plus court chemin par l' algorithme SPF**
  - **Avoir une table de routage plus petite, ce qui accélère la convergence de celle-ci**

## Le protocole de routage OSPF

- Un système autonome géré par le protocole OSPF est donc divisé en plusieurs zones (area) de routages qui contiennent des routeurs et des hôtes
- Cette division du système autonome en plusieurs zones introduit ce que l'on appelle le **routage hiérarchique**
- Chaque zone possède sa propre topologie et ne connaît pas les topologies des autres zones du système autonome
- La zone appelée « **zone backbone** » est une zone particulière. Elle est constituée de plusieurs routeurs interconnectés et doit être le centre de toutes les zones
- => Toutes les zones doivent être connectées physiquement au backbone

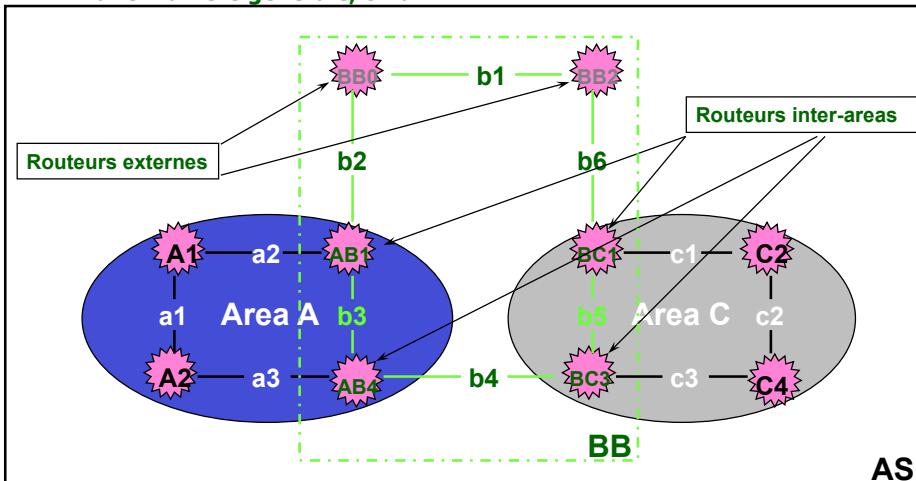
## Le protocole de routage OSPF



- le système autonome est découpé en trois zones plus le backbone
- les routeurs de la zone1 ne connaissent pas les routeurs de la zone(D), ni ceux de la zone3

## Le protocole de routage OSPF

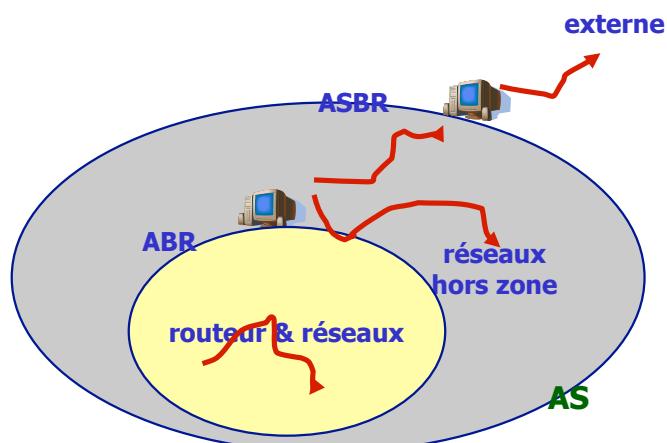
D'une manière générale, on a :



## Le protocole de routage OSPF

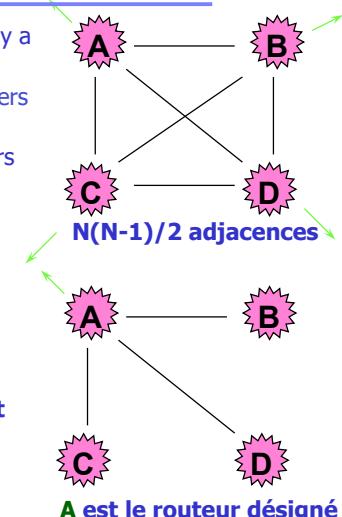
- **Routeurs OSPF :**
  - Routeurs internes
  - Routeurs backbones
  - Routeurs frontières de zone
    - **ABR** : Area Border Router
  - **Routeurs frontières de système autonome**
    - **ASBR** : Autonomous System Border Router
- Dans une phase d'initialisation, les routeurs OSPF échangent des informations avec les routeurs voisins d'un même réseau
- Des résumés des bases de données topologiques seront échangés périodiquement

## Le protocole de routage OSPF



## Le protocole de routage OSPF

- Le problème: Sur un réseau où il y a N routeurs il y a  $N*(N-1)/2$  adjacences.
  - Chaque routeur doit annoncer N-1 liaisons vers les autres routeurs
  - Chaque routeur doit annoncer ses routes vers un «réseau terminal»
  - soit  $N^2$  annonces (problème du carré de N)



## Le protocole de routage OSPF

- Dans les réseaux gérés par OSPF,
  - Un des routeurs connectés sur le réseau doit donc être élu **routeur désigné** (DR pour Designated Router)
  - Un autre routeur doit être élu routeur **désigné de secours** (BDR pour Backup Designated Router)
- Ces élections de routeurs permettent ainsi de réduire le trafic de mise à jour de routage
- Le **DR** et le **BDR** agissent comme un point central de contact pour les échanges d'informations d'état de lien
- Plutôt que les routeurs échangent leurs informations d'état de lien avec tous les autres routeurs, chaque routeur doit établir une communication avec le DR et le BDR
- Le **DR** et le **BDR** utilisent ensuite un processus d'inondation pour renvoyer ces informations à tous les autres routeurs
- Le **BDR** remplit exactement les mêmes tâches que le DR mais seulement si celui-ci tombe en panne (**tolérance aux pannes**)

## Le protocole de routage OSPF

Pour élire le DR et le BDR, les routeurs comparent leur priorité durant le processus d'échange des paquets Hello.

Le routeur avec la priorité la plus grande est élu DR et le deuxième routeur avec la priorité la plus haute est élu BDR

En ce qui concerne les sous protocoles, OSPF en compte trois, à savoir **Hello**, **échange** et **inondation**

Le protocole Hello a pour but de :

- Vérifier que les liaisons sont toutes opérationnelles
- Permet aux routeurs voisins d'établir une adjacence
- Assurer une communication bidirectionnelle avant d'échanger des informations d'état de lien

## Le protocole de routage OSPF

Les paquets **Hello** sont envoyés périodiquement par les routeurs

Ils contiennent comme informations : l'identifiant du routeur, l'intervalle Hello, les voisins avec lesquelles le routeur a une adjacence, l'identifiant de la zone dans laquelle se trouve le routeur, et enfin la priorité du routeur

## Le protocole de routage OSPF

masque réseau		
Intervalle hello	option	priorité
deadline		
routeur désigné		
routeur désigné de secours		
routeur voisin #1		
routeur voisin #n		

## Le protocole de routage OSPF

### Le protocole d' **inondation** :

Intervient lorsqu' un état de lien a changé dans le réseau

Un routeur prévient les autres d' un changement en leur envoyant des paquets **LSU** (Link State Update) qui comprennent les entrées mises à jour

Les routeurs qui reçoivent les paquets LSU mettent à jour leurs bases de données topologiques

## Le protocole de routage OSPF



### Le protocole d' **échange** :

C' est le mécanisme utilisé pour **découvrir les routes du réseau**

Il est réalisé pour que les routeurs passent dans le statut « *full state* » (état complet ou terminé) de communication

Pendant ce protocole d' échange, les routeurs s' envient un ou plusieurs paquets de **description de bases de données topologiques**

A la fin du processus d' échange, les routeurs adjacents sont considérés synchronisés et avec le statut « *full state* »

A ce moment là, les routeurs ont tous une **base de données d' état de lien identique**

## Le protocole de routage OSPF

### Sélection des routes OSPF :

La métrique OSPF par défaut est la bande passante

Chaque liaison reçoit une valeur de métrique basée sur sa bande passante

La métrique d'un lien est l'inverse de la bande passante du lien

Généralement, le coût dans les routeurs Cisco est calculé en utilisant la formule suivante :  $10\exp8 / \text{bande passante}$

Le coût d'un chemin est la somme de toutes les métriques des liaisons parcourues

Le plus court chemin pour aller d'un routeur à une destination est calculé à partir de l'algorithme de Diskjtra

L'algorithme place le routeur à la racine d'un arbre et calcule le plus court chemin pour atteindre chaque destination

## Le protocole de routage OSPF

### Quelques commandes :

**ip ospf cost** : permet de modifier les coûts d'état de lien

**show ip ospf neighbor** : indique les routeurs voisins au routeur sur lequel est exécuté la commande

**show ip route** : donne la table de routage d'un routeur

**ping et tracert** : permet de vérifier la connectivité entre les hôtes de sorte que tous les chemins de routage soient vérifiés

## Le protocole de routage OSPF

### Avantages du protocole OSPF :

Contrairement au protocole RIP, le protocole OSPF n'envoie pas à ses voisins le nombre de sauts qui les sépare mais l'état de la liaison qui les sépare

Chaque routeur est capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour transmettre un message donné

Evite aux routeurs intermédiaires d'avoir à incrémenter le nombre de sauts ce qui se traduit nécessairement par une information moins abondante et donc une meilleure bande passante disponible qu'avec le protocole RIP

## Le protocole de routage OSPF

### Inconvénients du protocole OSPF :

L'algorithme utilisé par OSPF pour ses calculs de routes est extrêmement gourmand en ressources processeurs

Plus une zone est importante et plus le nombre de calculs exécutés est conséquent, les problèmes de performances sont donc accrus

Lorsque des modifications interviennent sur le réseau, les routeurs ayant de nombreux de voisins ont beaucoup de travail à accomplir

Pour éviter ces problèmes de performances, il existe une solution :

Il est conseillé de limiter à cinquante le nombre de routeurs par zone

## Un peu de simulation/pratique

- **Routage statique, configuration**
- Mot de passe (le même que celui dans le fichier zebra.conf) => mode de visualisation de la configuration du routeur
- Passage en mode de configuration (mode privilégié) : *R2(Zebra)> enable*
- Ajout d'une route => passage en mode «terminal de configuration» :  
*Rt1(Zebra)# configure terminal*
- L'ajout : *Rt1(Zebra)(config)# ip route 192.168.1.0/24 100.0.0.1*
- Vérification de l'ajout : *route*
- Prises en compte des routes statiques à chaque démarrage :  
*R2(Zebra)# copy running-config startup-config*  
*Configuration saved to /etc/zebra/zebra.conf*
- ? la liste contextuelle des commandes

## Un peu de simulation/pratique

- **Routage dynamique, configuration**

Routage dynamique : il est indispensable d'installer les démons de routage dynamique tel que rip.conf ou ospf.conf

Exemple du protocole OSPF :

Création du fichier de configuration du démon (nécessaire au démarrage du démon et permet l'authentification d'accès en telnet)

/etc/quagga/ospfd.conf :  
hostname ospfd  
password ospfd  
enable password ospfd

Lancement du démon de routage sur les différents routeurs : Configuration avec le paquetage Quagga

## Un peu de simulation/pratique

- **Routage dynamique, configuration**

/etc/quagga/démons spécifie la liste des démons à utiliser :

```
# This file tells the quagga package which daemons to start.  
#  
# Entries are in the format: <daemon>=(yes|no|priority)  
# 0, "no" = disabled  
# 1, "yes" = highest priority  
# 2 .. 10 = lower priorities  
zebra=yes  
bgpd=no  
ospfd=yes  
ospf6d=no  
ripd=no  
ripngd=no  
isisd=no
```

## Un peu de simulation/pratique

- **Routage dynamique, configuration**

Lancement : R1 # /etc/init.d/quagga start

Configuration du protocole : connecter via telnet sur le port 2604

```
R1 # telnet localhost 2604  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
  
Hello, this is zebra
```

User Access Verification

```
Password:  
Rt1(OSPF) >
```

## Un peu de simulation/pratique

- **Routage dynamique, configuration**
  - Activer le mode privilégié, passer dans le terminal de configuration et enfin, entrer dans la configuration du routeur OSPF :  
`Rt1(OSPF) > enable` (passer en mode "super-utilisateur" de façon à pouvoir configurer le routeur)  
`Rt1(OSPF)# configure terminal` (passer en mode configuration terminal de façon à avoir plus de droits)  
`Rt1(OSPF)(config)# router ospf` (indique au routeur le type de routage à effectuer, dans notre cas OSPF)  
`Rt1(OSPF)(config-router)# redistribute connected` (indique que le routeur doit envoyer aux autres routeurs les routes qui utilisent les interfaces qui lui sont directement connectées)  
`Rt1(OSPF)(config-router)# network @ip/masque` (indique le/les réseaux sur lesquels on doit envoyer les routes)  
`Rt1(OSPF)(config-router)# end`  
`Rt1# write` (sauvegarde la configuration)
- Relancer les démons : `/etc/init.d/quagga restart`

## Un peu de simulation/pratique

### Commandes OSPF (Cisco)

- `area default-cost`
- `default-metric`
- `ip ospf authentication-key`
- `ip ospf cost`
- `ip ospf dead-interval`
- `ip ospf hello-interval`
  - `ip ospf priority`
  - `ip ospf retransmit-interval`
  - `ip ospf transmit-delay`
  - `neighbor (OSPF)`
  - `network area`
  - `show ip ospf`
  - `show ip ospf database`
  - `show ip ospf interface`
  - `show ip ospf neighbor`
  - `show ip ospf retransmission-list`
  - `timers spf`

⇒ [http://www.cisco.com/en/US/docs/ios/11\\_3/np1/command/reference/1rospf.html](http://www.cisco.com/en/US/docs/ios/11_3/np1/command/reference/1rospf.html)

⇒ **BGP** : [http://www.cisco.com/en/US/docs/ios/11\\_3/np1/command/reference/1rbgp.html](http://www.cisco.com/en/US/docs/ios/11_3/np1/command/reference/1rbgp.html)

## Un peu de simulation/pratique

### Commandes RIP (Cisco)

- `auto-summary`
- `default-information originate`
- `default-metric`
- `ip rip authentication key-chain`
- `ip rip authentication mode`
- `ip rip receive version`
- `ip rip send version`
- `ip split-horizon`
- `neighbor (IGRP and RIP)`
- `network (RIP)`
- `offset-list`
- `output-delay`
- `router rip`
- `timers basic`
- `validate-update-source`
- `version`

⇒ [http://www.cisco.com/en/US/docs/ios/11\\_3/np1/command/reference/1rrip.html](http://www.cisco.com/en/US/docs/ios/11_3/np1/command/reference/1rrip.html)

6 h

## 4.

### Protocoles de routage inter-domaine :

#### BGP

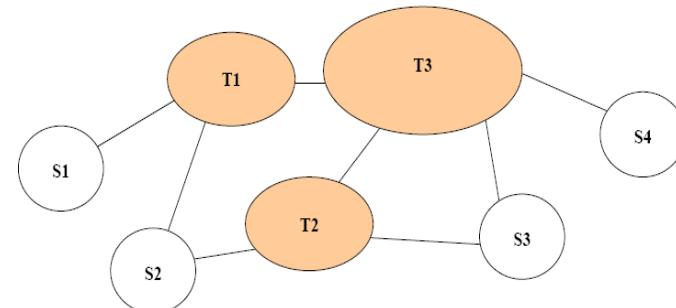


## BGP : Border Gateway Protocol

- Routage des paquets dans l'Internet global
  - Internet est composé de plus de 10.000 domaines de routage
  - Qu'est-ce qu'un domaine ?
    - Un ensemble de routeurs, liaisons, terminaux, réseaux locaux
    - Qui sont administrés par une même autorité
  - Quelle est la taille d'un domaine ?
    - En nombre d'adresses IP, un domaine peut contenir
      - » Quelques dizaines d'adresses pour les plus petits
      - » Quelques dizaines de millions d'adresses pour les plus grands
  - Comment sont interconnectés les domaines ?
    - Pour permettre à tout paquet émis d'être transmis vers tout destinataire
    - En général, un paquet devra traverser plusieurs domaines pour atteindre son destinataire final

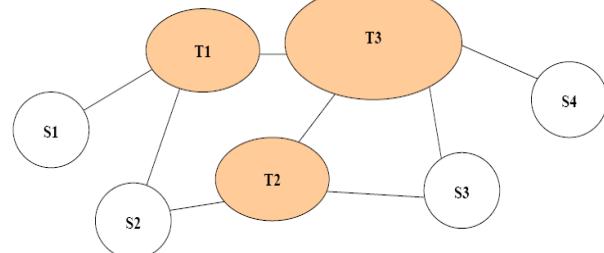
## BGP : Border Gateway Protocol

- Domaine de transit / Transit domain
  - Permet à un domaine externe d'utiliser son infrastructure réseau pour transmettre des paquets vers d'autres domaines



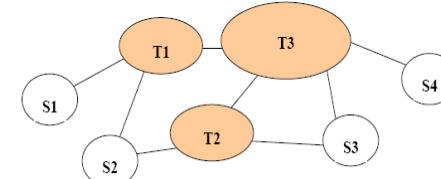
## BGP : Border Gateway Protocol

- Stub Domain
  - Ne permet pas à un domaine externe d'utiliser son infrastructure réseau pour transmettre des paquets vers d'autres domaines
  - Est connecté à au moins un domaine de transit pour communiquer avec l'extérieur



## Types de stub-domains

- Différents types
  - En fonction de leurs modes de connexion
    - *Single-homed* : connecté à un domaine de transit
    - *Double-homed* : connecté à deux domaines de transit
  - En fonction des services offerts
    - *Content-rich* : domaines comportant d'importants serveurs Web (Yahoo, Google, etc.)
    - *Access-rich* : domaines d'ISP (Internet Service Provider) offrant par exemple des accès ADSL à l'Internet global



## Exemple de stub-domain : RENATER

Le Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche

### • La communauté des utilisateurs

- Plus de 600 établissements raccordés ayant une activité dans les domaines de la recherche, de l'enseignement et de la culture

### • Le réseau RENATER

- Est maintenant dans sa troisième génération
- Utilise largement les technologies optiques de multiplexage
  - DWDM : Dense Wavelength Division Multiplexing
- Est essentiellement maillé par des liaisons à 2,5 Gbit/s
  - Interconnectant les réseaux de collecte régionaux développés avec le soutien des collectivités territoriales.
- Possède un cœur de réseau à 80 Gbit/s en région Île-de-France

## Exemple de stub-domaine : RENATER

### • Liaisons internationales

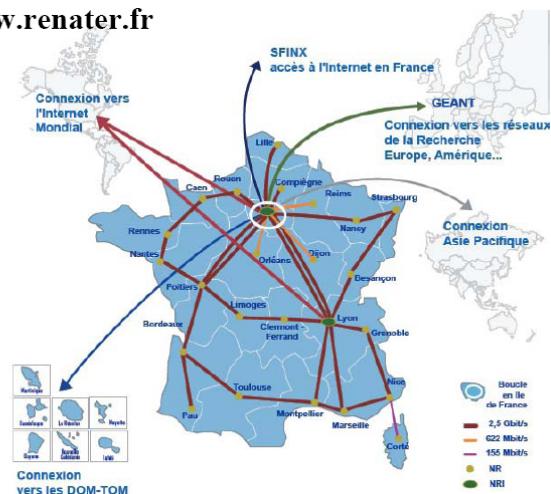
- RENATER est interconnecté à 10 Gbit/s
  - Aux autres réseaux de recherche européens et américains via le réseau européen GEANT
- Une liaison à 155 Mbit/s aboutissant en Corée
  - Assure la communication avec les réseaux de la recherche de la zone Asie-Pacifique

### • Liaisons avec l'Internet

- En France la communication avec l'Internet est réalisée
  - Par le nœud d'échange SFINX (lien à 3\*1 Gbit/s avec plus de 80 opérateurs)
- La communication avec l'Internet dans le reste du monde
  - Assurée par le raccordement de RENATER à 5 Gbit/s à l'épine dorsale Internet mondiale OpenTransit de France Télécom

## Exemple de stub-domaine : RENATER

[www.renater.fr](http://www.renater.fr)



## Exemple de transit-domaine : GEANT

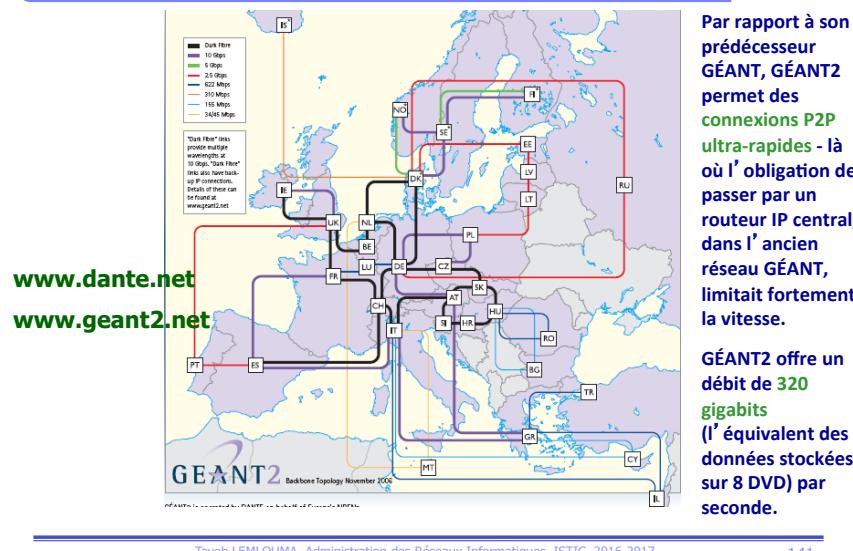
### • La communauté des utilisateurs

- Interconnecte à travers l'europe 26 réseaux nationaux pour l'éducation et la recherche (National Research and Education Networks ou NRENs)
- Réseau opérationnel le 1 décembre 2001, sa deuxième génération (GEANT2) étant en cours de développement

### • Liaisons internationales

- Connexion à 12 Gbps vers l'Amérique du nord
- Connexion à 2.5 Gbps avec le Japon
- Connexion avec les réseaux de recherche
  - ALICE : pour l'Amérique du Sud
  - EUMEDCONNECT : pour les pays de la région méditerranéenne
  - TEIN2 : pour les pays de l'asie et du pacifique

## Exemple de transit-domaine : GEANT



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

141

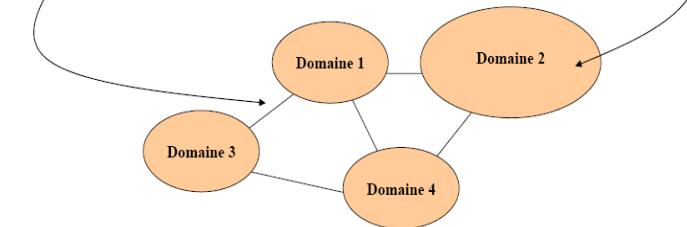
## Les protocoles de routage

### • Interior Gateway Protocol (IGP)

- Permet le routage des paquets à l'intérieur d'un domaine
- Ne connaît que la topologie du domaine qui le concerne

### • Exterior Gateway Protocol (EGP)

- Permet le routage de paquets entre différents domaines
- Ne connaît pas la topologie des domaines interconnectés (un domaine est vu comme une boîte noire)



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

142

## Types IGP

### • A vecteur de distance / Distance vector routing

- Routing Information Protocol (RIP)
  - Encore très utilisé dans les petits domaines malgré ses limitations nombreuses

### • A états de liens / Link state routing

- Open Shortest Path First (OSPF)
  - Très utilisé par les entreprises
- Intermediate System to Intermediate System (IS-IS)
  - Très utilisé par les opérateurs (Internet Service Provider)

## Routage inter-domaines

### • Objectif

- Permettre le transfert de paquets IP vers leurs destinataires
  - A travers les domaines de transits nécessaires
  - En suivant le meilleur chemin possible, i.e. le moins coûteux
  - En prenant en compte les politiques de routage (routing policies) des domaines de transit
  - Sans connaître les topologies internes des domaines de transit

### • Politique de routage

- Définie au niveau de chaque domaine
  - Les services de transport qu'il souhaite offrir
  - Les méthodes qu'il utilise pour sélectionner les meilleurs chemins

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

143

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

144

# Systèmes Autonomes

## • Définition

- Autre terme utilisé pour désigner un domaine
  - *Même si on considère parfois qu'un domaine peut-être composé de plusieurs AS*
- Un ensemble de routeurs interconnectés
  - *Gérés par une seule unité administrative*
  - *Présentant une image cohérente des réseaux destinations qu'ils peuvent permettre d'atteindre*
- Tout système autonome sera identifié par un numéro
  - *AS number défini sur 16 bits (32 bits dans un futur proche)*
  - *Exemple : AS702 (cf [www.cidr-report.org/autnums.html](http://www.cidr-report.org/autnums.html))*
  - *Remarque : certains domaines ne possèdent pas de numéro d'AS (petits domaines n'utilisant pas BGP)*



# Systèmes Autonomes

**AS294 FRANCE-IP-NET-AS** Institut National de Recherche en Informatique et Automatique

**AS1301 FR-EDFDPT3** Electricite de France

**AS1304 FR-RENATER** FR

**AS1938 FR-RENATER-IRISA** Irisa/Inria Rennes

**AS1264 USACESPK-AS** - United States Army Corps of Engineers

**AS1942 FR-CICG-GRENOBLE** FR

**AS47206 RENNES-TELECOM-AS** Rennes Metropole Telecom

Liste complète avec des entrée Whois sur : <http://www.cidr-report.org/autnums.html>

# Connexions inter-domaines

## • Deux types de connexion

- Connexion privée / private peering
  - *Via une ligne louée directe*
  - *Exemple : RENATER avec GEANT, connexion entre deux ISP internationaux, etc.*
- Connexion à un point d'interconnexion publique / public peering
  - *Via un LAN / Switch Ethernet à hautes performances connectant plusieurs routeurs (de domaines différents)*
  - *Exemple : SFINX pour la connexion de RENATER à l'Internet en France (avec 80 opérateurs)*
  - *Dans ce cas, on parle également de NAP (Network Access Point)*

# Politiques de routage

## • Deux classes principales

### ➤ Customer-Provider peering

- *C est un domaine qui achète à P sa connectivité à Internet*
  - » P accepte de transmettre les paquets venant de C vers n'importe quelle destination (ou un ensemble de destinations à préciser)
  - » P accepte de transmettre à C et à ses clients les paquets venant d'autres domaines

### ➤ Shared-cost peering

- *X et Y sont des domaines de même taille*
  - » X accepte de Y les paquets qui sont destinés à X ou aux clients de X
  - » X envoie à Y les paquets qui sont destinés à Y ou aux clients de Y
  - » Et inversement ...

## Import/Export entre les domaines

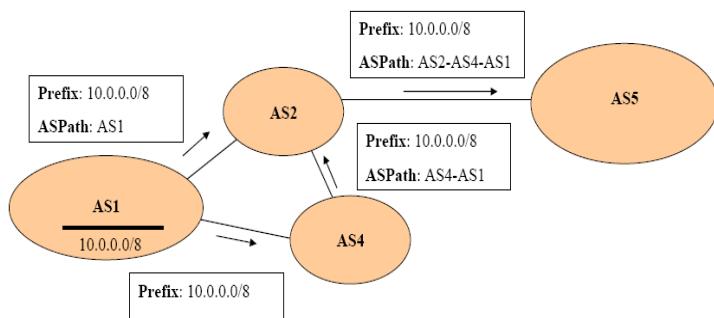
- Un domaine spécifie sa politique de routage par
  - Des règles d'export
    - Précisant les routes qu'il va annoncer à ses pairs
  - Des règles d'import
    - Précisant les routes qu'il va accepter de ses pairs
- Comment spécifier ses règles d'import / export ?
  - RPSL (Routing Policy Specification Language)
    - Défini dans la RFC2622 avec des exemples dans la RFC2650
    - Utilisé par de nombreux ISP
  - Exemples
    - Import: from AS# accept List-Of-AS | ANY
    - Export: to AS# announce List-Of-AS | ANY

## BGP : Border Gateway Protocol

- Tout routeur BGP
  - Commence par établir des sessions BGP avec ses voisins
    - Au dessus de connexions TCP pour garantir une bonne transmission des routes transmises
  - Transmet les routes actives à ses voisins
    - Routes apprises de ses voisins (routeurs BGP)
    - Routes internes configurées en statique
      - » Inconvénient : nécessite une intervention manuelle
      - » Avantage : permet de transmettre un ensemble stable de préfixes
    - Routes internes apprises (via un protocole de routage interne)
      - » Inconvénient : risque de transmettre des ensembles de préfixes instables si le protocole IGP utilisé connaît des perturbations
      - » Avantage : permet de prendre en compte automatiquement des modifications internes au domaine (ex: nouveau plan d'adressage, nouveau sous-réseau)
  - Transmet de manière incrémentale
    - Les nouvelles routes apprises ou nouvelles meilleures routes
    - Les routes qui ne sont plus accessibles

## BGP : Path Vector Protocol

- Contenu des vecteurs de chemins échangés
  - Préfixe / adresse destination
  - Chemin ou AS-path à suivre pour atteindre la destination
    - Permet de détecter les boucles si un domaine reçoit un vecteur avec un chemin où il apparaît



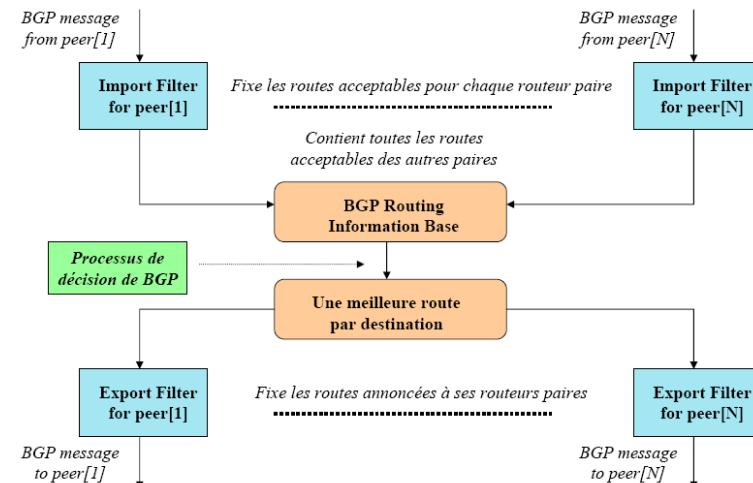
## BGP : Objectifs

- Échanger des routes (trafic) entre des organismes indépendants
  - Opérateurs
  - fournisseurs de services Internet
- Implémenter la politique de routage de chaque organisme
  - Respect des contrats passés entre les organismes
  - Sûreté de fonctionnement
- Minimiser le trafic induit sur les liens
- Donner une bonne stabilité au routage

## BGP : Politique de routage

- Tout routeur BGP choisit lui-même
  - La route qu'il va suivre pour rejoindre une destination donnée
    - La route choisie n'est pas nécessairement la plus courte (en nombre de domaines à traverser)
    - La route choisie est celle qui va être annoncée aux domaines ou routeurs voisins
  - Les routes qu'il va annoncer à ses voisins
    - Un routeur n'annonce pas nécessairement toutes les routes qu'il connaît
    - Les routes annoncées sont fonction de règles d'export

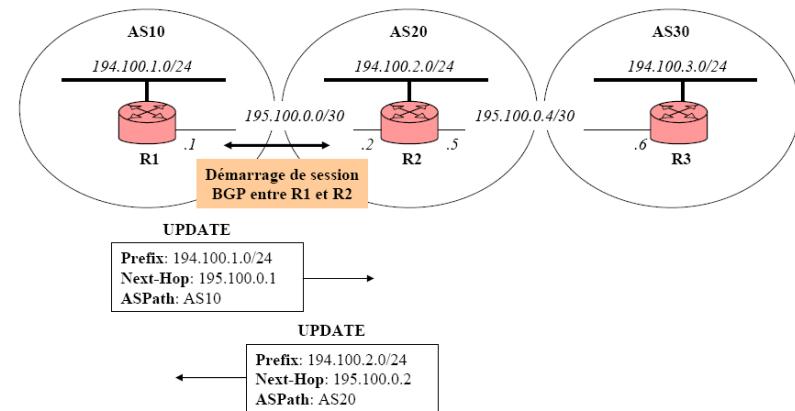
## BGP : Fonctionnement



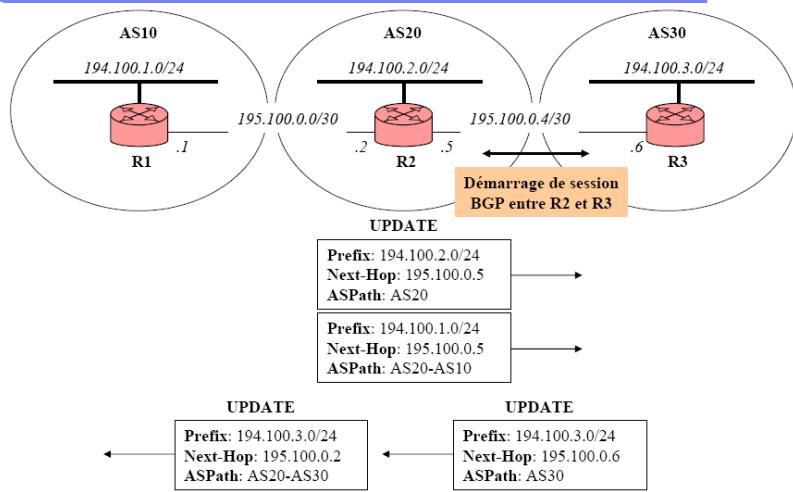
## BGP : Types de messages

- Types principaux
  - OPEN message
    - Pour établir une session BGP au dessus d'une connexion TCP (port 179)
  - KEEPALIVE message
    - Transmis périodiquement pour vérifier qu'une session BGP est toujours en état de fonctionnement
  - UPDATE message
    - Pour annoncer une route
      - Informations transmises
        - » Préfixe / adresse destination
        - » Chemin ou AS-path à suivre pour atteindre la destination
        - » Prochain saut (next-hop) annonçant la route
  - WITHDRAW message
    - Pour demander de retirer une route qui n'est plus utilisable
    - Informations transmises
      - » Préfixe / adresse destination plus joignable par une route

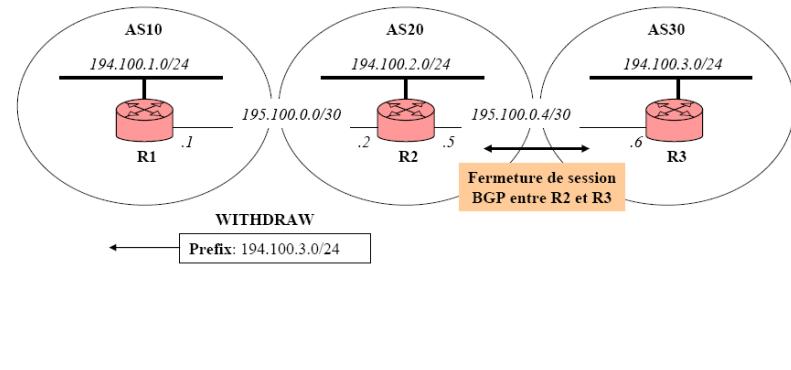
## BGP : Exemple



## BGP : Exemple

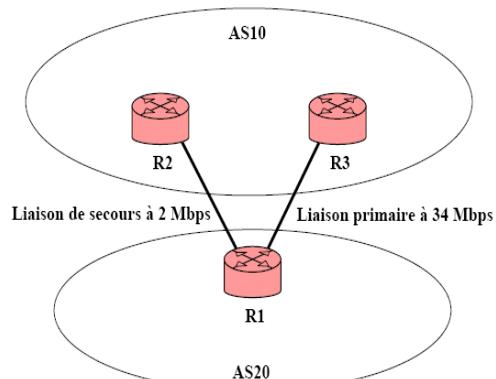


## BGP : Exemple



## BGP : Les préférences

- Comment privilégier certaines routes ?
  - Dans le cas où des liaisons primaire et de secours sont en concurrence



## BGP : Solution

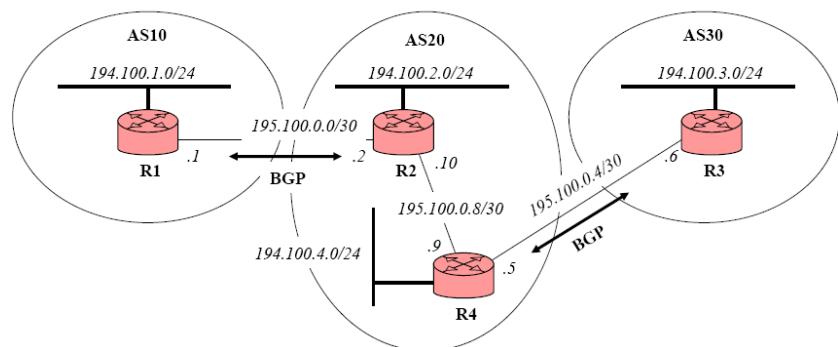
- Au niveau des règles d'import
  - Ajout de valeurs d'attribut « local-pref » aux messages BGP acceptés
    - Local-pref = 100 pour une route annoncée de qualité normale*
    - Local-pref = 200 pour une route annoncée de meilleure qualité que la normale*
    - Local-pref = 50 pour une route annoncée de moins bonne qualité que la normale*
- Au niveau des routeurs BGP
  - Modification du processus de sélection des meilleures routes
    - Commencer par prendre les routes avec la valeur de local-pref la plus élevée*
    - En cas d'égalité de local-pref entre plusieurs routes, prendre la route la plus courte (en terme d'ASPath)*

## BGP : Les préférences en pratique

### • Pour des raisons économiques

- Par ordre de croissant, une AS préfère
  - *Les routes annoncées par ses clients*
    - » Pour ne pas passer par des domaines de transit, alors que ce n'est pas nécessaire, et que le client a payé
  - *Les routes annoncées par les AS paires*
    - » Car en relation de shared-cost, les coûts d'acheminement sont normalement peu élevés
  - *Les routes annoncées par les AS qui lui fournissent un service*
    - » Pour limiter les coûts s'ils sont estimés en fonction des volumes transportés

## BGP : Un problème à résoudre !



Comment R2 (resp. R4) peut annoncer à R4 (resp. R2) les routes apprises de AS10 (resp. de AS30) ?

## BGP : Solution 1

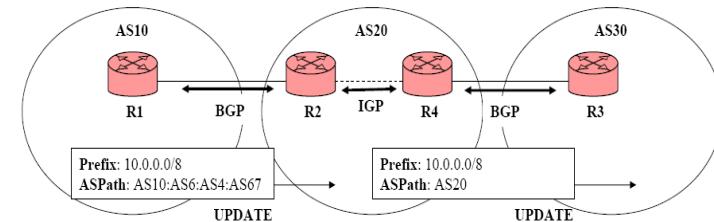
### • Utilisation de IGP

- Transport / distribution des routes apprises à travers des protocoles de routage interne
  - *Tels que OSPF, RIP, etc.*
- Avantages
  - *Pas de nouveaux protocoles à configurer en interne*
  - *Pas de trafic supplémentaire en interne*
- Inconvénients
  - *IGP peut ne pas être armé pour supporter autant de routes que celles annoncées par BGP*
  - *IGP ne peut pas transporter des attributs spécifiques à BGP tels que ASPath*

## BGP : Solution 1

### • Problème posé

- Toutes les routes annoncées par R1 à R2 via BGP
  - *Quelles que soient leur longueur (en nombre de domaines)*
- Sont ensuite transmises par R2 à R4 via IGP
  - *Sans attributs propres à BGP (ASPath)*
- Puis de R4 à R3 via BGP
  - *Comme si elles étaient internes à AS20 (donc accessibles en un saut)*



## BGP : Solution2

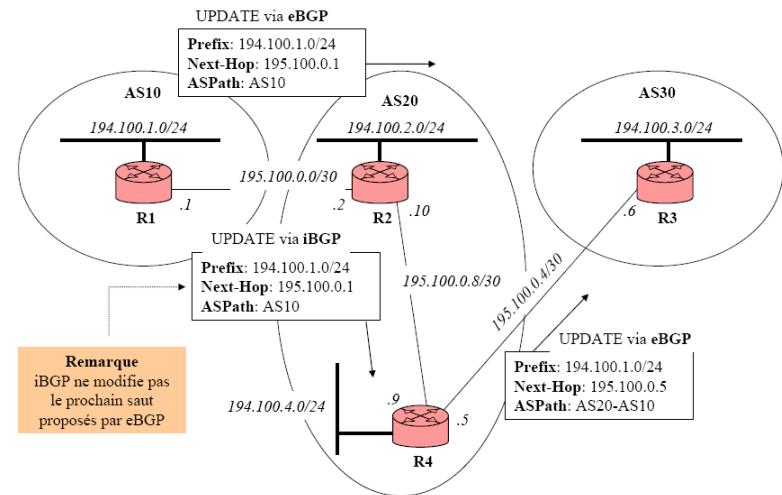
### • Utilisation de iBPG et eBGP

- (e)xterior-BGP étant utilisé entre routeurs de domaines différents
- (i)nterior-BGP étant utilisé entre routeurs d'un même domaine

### • Différences entre eBGP et iBGP

- Les préférences (attribut « local-pref ») sont transportés dans les messages iBGP
  - Ce qui n'est pas le cas pour les messages eBGP
- A travers un session iBGP
  - Un routeur annonce seulement les routes apprises de sessions eBGP
  - Une route apprise à travers une session iBGP n'est jamais annoncée à travers une autre session iBGP
  - En général, aucune règles de filtrage n'est mise en œuvre

## BGP : Solution2



## BGP : Processus de sélection



### • Quelle est la meilleure route ?

1. Ignorer celles pour lesquelles le prochain saut n'est pas joignable
2. Préférer celles avec la valeur la plus élevée de « local-pref »
3. Préférer les routes avec le « ASPath » le plus court
4. Préférer les routes avec le « MED » le plus faible
  - MED = Multi-Exit-Discrimination attribute
5. Préférer les routes annoncées par eBGP plutôt que par iBGP
6. Préférer les routes avec le prochain saut le plus proche
7. Préférer les routes annoncées par les routeurs de plus petit identifiants (adresses IP de loopback)

#### Remarque

- Le MED est utilisé entre nœuds eBGP, il indique aux voisins extérieurs le chemin préféré à l'intérieur de l'AS
- Le LOCAL\_PREF influence le trafic sortant d'un AS, le MED influence le trafic rentrant d'un AS

## BGP : Un résumé technique

### Procédure et messages :

#### • Acquisition des voisins (neighbor acquisition)

- Un routeur veut échanger des infos
  - Envoi d'un message **Open**
  - Si l'autre routeur accepte la requête : envoi d'un message **Keepalive**

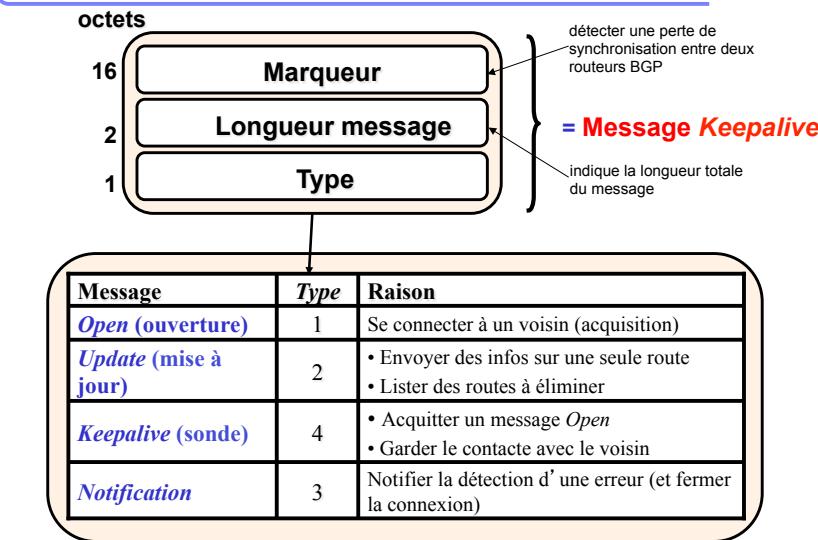
#### • Garder le contact avec les voisins (neighbor reachability)

- Envoi d'un message **Keepalive** avant expiration d'un temporisateur

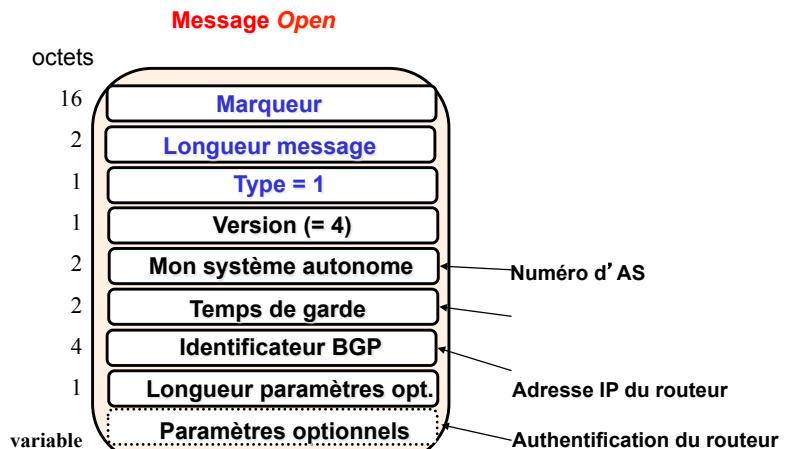
#### • Connectivité avec les réseaux (network reachability)

- Chaque routeur a une base de données de réseaux qu'il peut atteindre + une route préférée vers chaque réseau
  - Si la base de données change : envoi d'un message **Update**

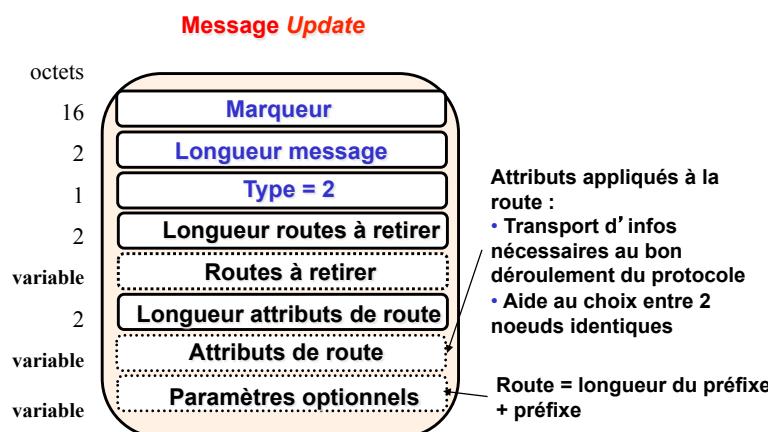
## BGP : Format de l' entête des messages



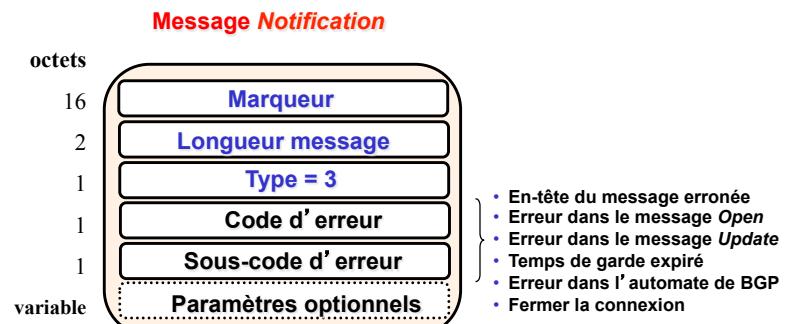
## BGP : Format de l' entête des messages (Suite)



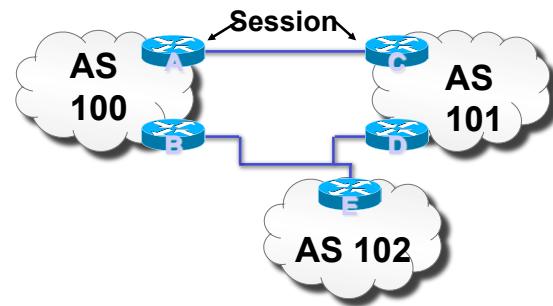
## BGP : Format de l' entête des messages (Suite)



## BGP : Format de l' entête des messages (Suite)

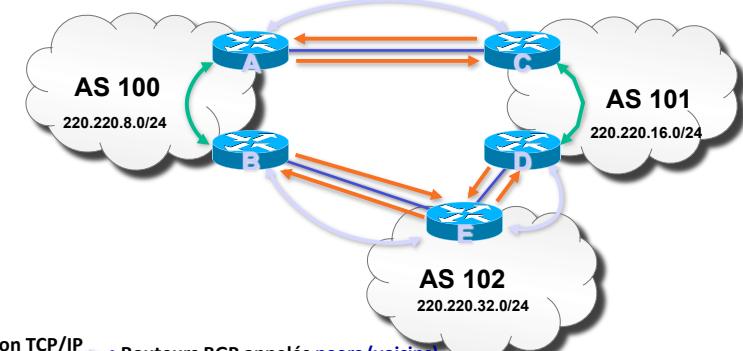


## BGP : Un résumé technique



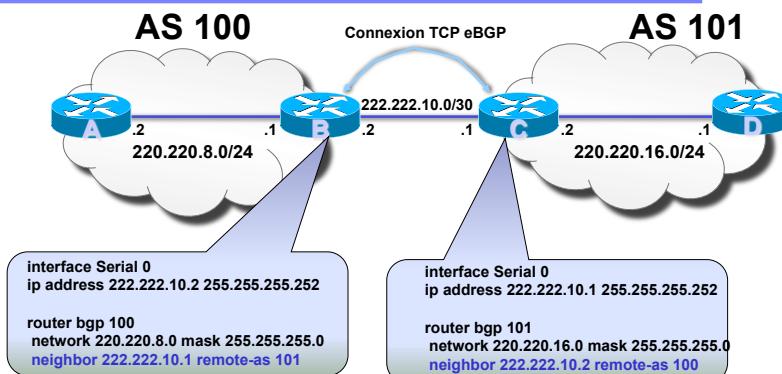
- BGP est utilisé entre AS**  
si vous n'êtes raccordé qu'à un seul AS vous n'avez pas besoin de BGP
- BGP est transporté par le protocole TCP**
- Les mises à jours sont incrémentielles**
- BGP conserve le chemin d'AS pour atteindre un réseau cible**

## BGP : Un résumé technique - Sessions



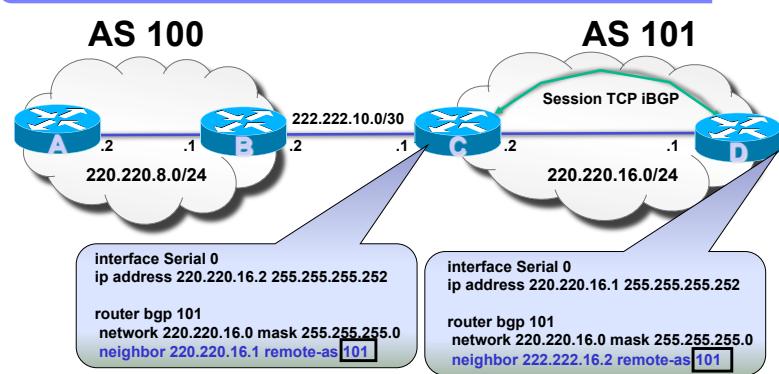
- Connexion TCP/IP eBGP
- Routeurs BGP appelés **peers** (**voisins**)
  - Session entre 2 AS différents = External BGP
- Connexion TCP/IP iBGP
- Les voisins d'un même AS sont appelés des voisins internes (**internal peers**)
  - Les voisins BGP s'échangent des messages contenant des préfixes (NLRI : Network Layer Reachability Information : (mask/@Rx), e.g. /25, 204.149.16.128)
- Message de mise à jour BGP

## BGP : Un résumé technique – Config.



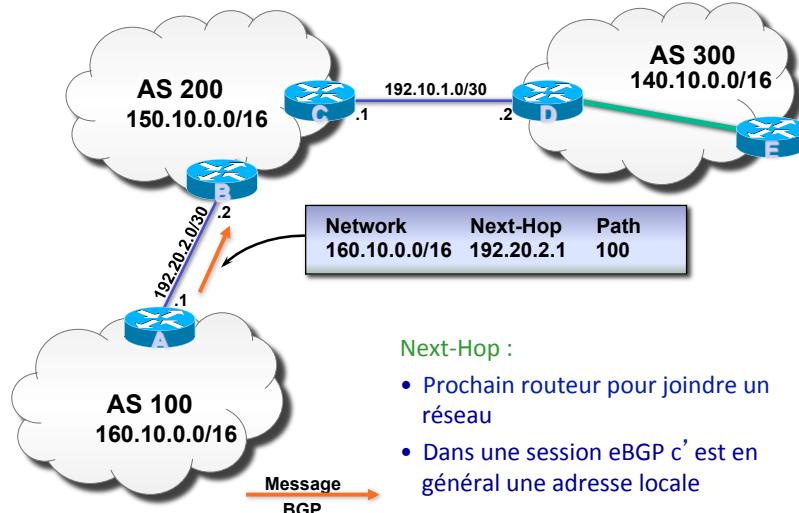
- Lorsque les numéros d'AS sont différents il s'agit d'une session BGP Externe (eBGP)
- Les sessions BGP sont établies en utilisant la commande BGP "neighbor" du routeur

## BGP : Un résumé technique – Config.



- Les sessions BGP sont établies en utilisant la commande BGP "neighbor" du routeur
  - Numéros d'AS différents -> BGP Externe (eBGP)
  - Numéros d'AS identiques -> BGP Interne (iBGP)

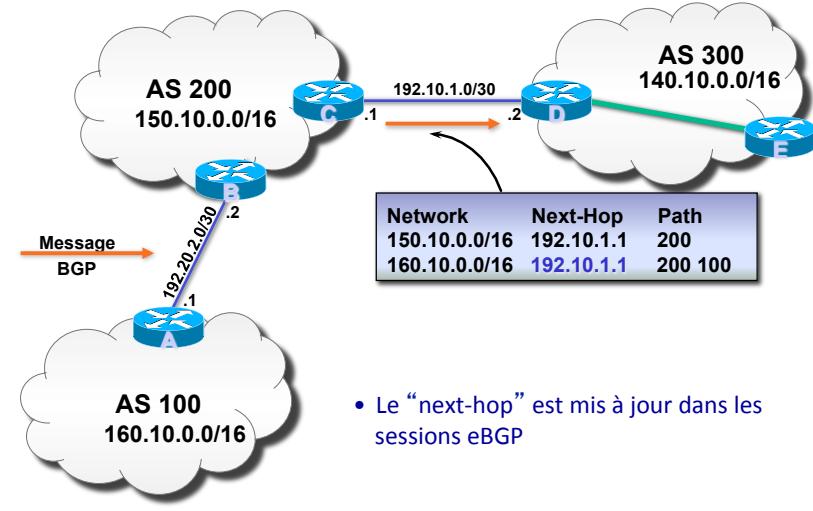
## BGP : Un résumé technique – Config. (next hop)



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

177

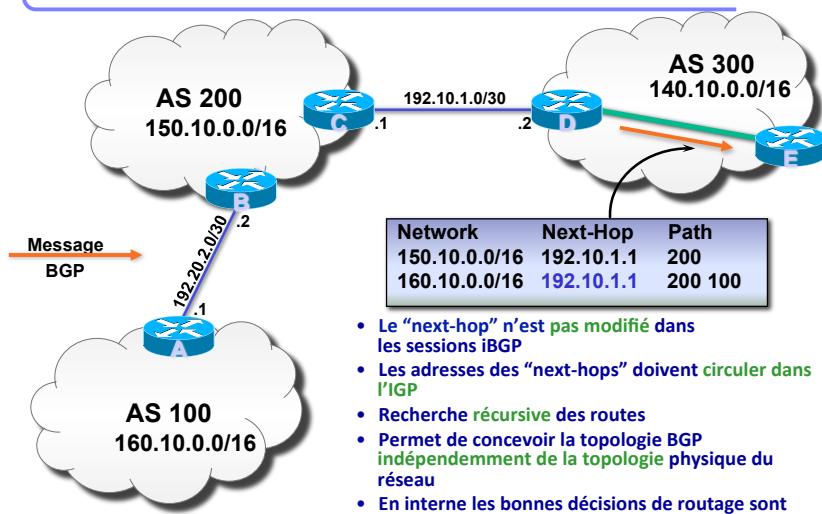
## BGP : Un résumé technique – Config. (next hop)



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

178

## BGP : Un résumé technique – Config. (next hop)



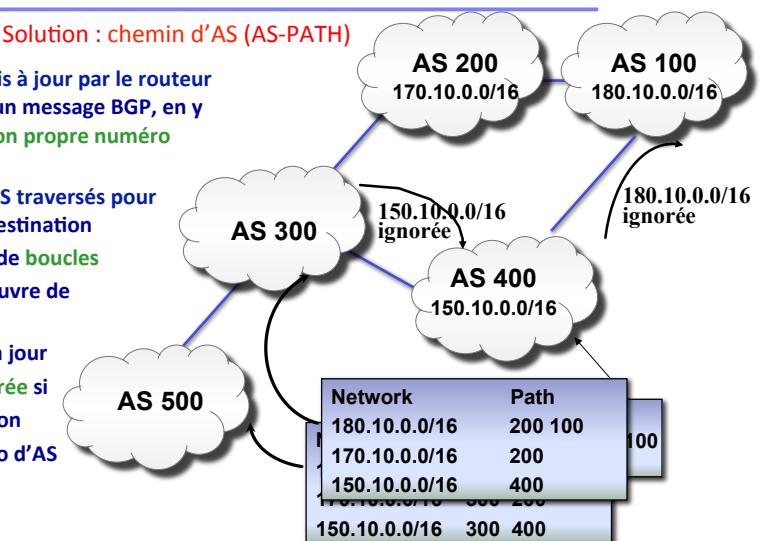
Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

179

## BGP : Un résumé technique – Problème : Détection de Boucle

AS-PATH :

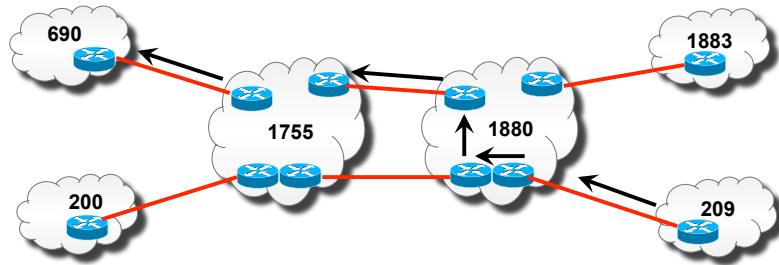
- Attribut mis à jour par le routeur envoyant un message BGP, en y ajoutant son propre numéro d'AS
- Lister les AS traversés pour arriver à destination
- Détection de boucles
- Mise en œuvre de politiques
- Une mise à jour reçue est ignorée si elle contient son propre numéro d'AS



Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

180

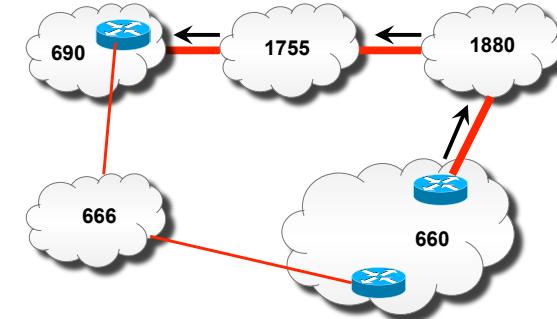
## BGP : Un résumé technique – Problème : meilleur chemin?



Solution : MED (Multi-Exit-Discriminator)

- attribut Non-transitif
  - Donne la préférence relative des points d'entrée
  - Comparable si chemins de mêmes AS
- route-map: set metric { metric | internal}

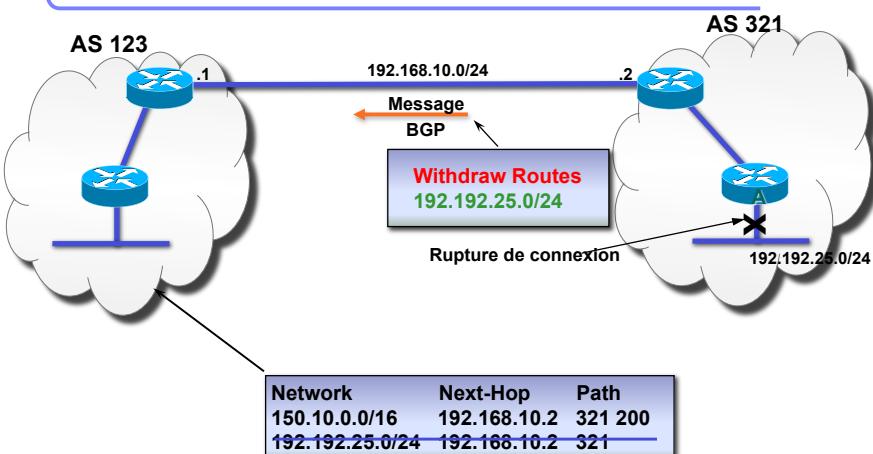
## BGP : Un résumé technique – Problème : As-path ou MED?



Solution : "Local preference :

- Attribut local à un AS - obligatoire pour des mises à jour d'iBGP
- route-map override: set local-preference

## BGP : Un résumé technique – Suppression d'une route



- Permet de retirer un réseau de la liste des réseaux accessibles
- Chaque route supprimée est composée de : son Préfixe et la longueur du masque

## BGP : derniers mots..

- **BGP versus IGP**
  - Dans un domaine, IGP redistribue sa topologie interne
  - Entre domaines, BGP permet de distribuer les routes vers l'extérieur en indiquant par quels domaines de transits passer
- **iBGP versus eBGP**
  - eBGP distribue les routes vers l'extérieur entre domaines
  - iBGP distribue les routes vers l'extérieur à l'intérieur d'un domaine
- **Processus de décision**
  - Complexité relative liée à l'existence de nombreux critères de sélection (local-pref, ASPath, MED, etc.)

## BGP : derniers mots..

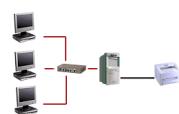
- Pas d'authentification requise des pairs
  - Par défaut la seule barrière est la négociation TCP
  - Authentification MD5 par secret partagé optionnelle
- Pas de validation des informations
  - Nécessité de faire confiance à ses voisins sur les préfixes qu'il annonce
    - Possibilité (très recommandée) de filtrer
    - Mais très difficile quand on se rapproche du cœur du réseau...
  - Impossible de vérifier la validité du message en terme d'insertion, modification, *replay*
- Pas de confidentialité
- Autres vulnérabilités récentes, voir Sources (prochain transparent!)

## BGP : Sources

- RFC 1771
  - Quatrième version de BGP
- RFC 2622 & 2650
  - RPSL (Routing Policy Specification Language)
- Ouvrages
  - Routing TCP/IP, vol. 2, Cisco Press
  - BGP4: interdomain routing in the Internet, Addison Wesley
- Web : [www.bgp4.as](http://www.bgp4.as)
- Vulnérabilités récentes :
  - S. G. D. N, Agence nationale de la sécurité des systèmes d'information, exemple : Multiples vulnérabilités dans le routage BGP des équipements Cisco  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-304/CERTA-2009-AVI-304.html> (30 juillet 2009)

## 5.

### Traduction des noms de domaine : mise en oeuvre de DNS



## Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
6. Mécanisme de résolution de noms
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Introduction

### Utilité de la résolution de nom

- Rôle des adresses MAC : permettre à deux machines dans le même réseau de communiquer directement.
- Rôle des adresses IP : permettre à deux machines dans le monde (directement connectées à Internet) de communiquer.
  - ↳ Inconvénient des adresses IP : difficile à mémoriser pour un utilisateur. Il est beaucoup plus facile de mémoriser des noms de sites plutôt que des numéros.
- Dans ce cas, il faut disposer d'un système d'annuaire permettant de transformer un nom de site en adresse IP (et inversement).

## Introduction

### Utilité de la résolution de nom

- Les noms symboliques sont plus faciles à mémoriser que des numéros ou des adresses IP.
- En TCP/IP les adresses ne sont manipulées que par la couche 3 de la pile
- Il est plus facile pour la couche application d'utiliser des noms symboliques.
- Un mécanisme de résolution de noms permettra de jouer le rôle d'annuaire.

## Introduction

### Méthodes de résolution de noms

- Attention : ne pas confondre la résolution de noms et le DNS :
  - ↳ La résolution de nom est le mécanisme qui tourne sur une machine pour gérer les correspondances entre noms et adresse IP.
  - ↳ Pour faire cette correspondance, il existe différentes méthodes, qui peuvent fonctionner en même temps. Le DNS est l'une de ces méthodes.
- Différentes méthodes de résolution de noms :
  - ↳ Table de correspondance locale.
  - ↳ Service NIS sous Linux.
  - ↳ Service WINS sous Windows.
  - ↳ Le DNS.

## Introduction

### La résolution de nom locale

La résolution de noms locale consiste, sur chaque machine, à établir une table de correspondance permettant d'associer un nom symbolique à une adresse IP.

Cette table est mémorisée dans un fichier texte :

- ↳ Sous Linux : /etc/hosts
- ↳ Sous Windows : C:\Windows\System32\drivers\etc\hosts

#### Exemple pour Windows :

```
# Copyright (c) 1993-1999 Microsoft Corp.  
# Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP pour Windows.  
# Ce fichier contient les correspondances des adresses IP aux noms d'hôtes. Chaque entrée doit être sur une ligne  
# propre. L'adresse IP doit être placée dans la première colonne, suivie par le nom d'hôte correspondant. L'adresse  
# IP et le nom d'hôte doivent être séparés par au moins un espace.  
# De plus, des commentaires (tels que celui-ci) peuvent être insérés sur des lignes propres ou après le nom  
# d'ordinateur. Ils sont indiqués par le symbole '#'.  
# Par exemple:  
# 102.54.94.97 rhino.acme.com # serveur source  
# 38.25.63.10 x.acme.com # hôte client x
```

## Introduction

### La résolution de nom locale

- ↳ S'il y a un grand nombre de machines -> le fichier doit être rempli pour chaque machine et de façon identique !
  - ↳ S'il y a un changement quelconque -> ce changement doit être répercuté sur toutes les machines du réseau !
- Conclusion :** la méthode de résolution de noms locale devient très vite fastidieuse en cas de grand nombre de machines et de changements.
- ↳ De plus, cette méthode est inutilisable à l'échelle mondiale, car dès qu'il y a un changement dans un nom ou une adresse IP à l'autre bout du monde, il faudrait mettre à jour ses fichiers localement.

## Introduction

### Service NIS sous Linux et WINS sous Windows

Deux méthodes pour éviter ces difficultés :

- ↳ Sur unix, utilisation d'une liste complète accessible par toutes les machines : il s'agit du service NIS (NIS +) ou pages jaunes (yellow pages) mis au point par SUN.
- ↳ Sur les machines Windows, des machines particulières (appelées contrôleur principal de domaine et contrôleur maître de segment) sont chargées de centraliser les listes de résolution et de les fournir aux autres machines. Soit tous les domaines et contrôleurs de domaines sont inscrits dans le fichier LMHOSTS de chaque contrôleur principal, soit ils sont fournis par le service appelé WINS.

## Introduction

### Service NIS sous Linux et WINS sous Windows

- ↳ Ces solutions sont plus faciles d'emploi que la résolution locale, car il y a très peu de reconfiguration à faire en cas de changement à effectuer.
- ↳ Cette solution est utilisable dans les réseaux locaux mais est inutilisable avec Internet et les réseaux interconnectés car le volume d'information à mémoriser serait colossal.

## Introduction

### Le DNS

Solution :

- ↳ Listes (base de données) réparties et hiérarchisées au niveau mondial avec un système de nommage unique et normalisé et une syntaxe normalisée
- ↳ Un protocole d'interrogation, réPLICATION, de mise à jour normalisé

## Mécanisme de résolution de noms et DNS

L'objectif de cette partie est :

- ↳ De vous présenter le mécanisme de résolution de noms qui permet, sur les postes clients, de transformer un nom et adresse IP.
- ↳ De vous présenter le principe, le fonctionnement et la configuration d'un service DNS.

Différents points seront abordés :

- Le fonctionnement du mécanisme de résolution de noms.
- Le principe de l'architecture de nommage DNS.
- Le principe de configuration de fonctionnement du DNS.

## Le DNS

### Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
6. Mécanisme de résolution de noms
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Présentation de la résolution de noms DNS

### L'espace de noms hiérarchisé

- Les organismes de normalisation d'Internet ont normalisé une structure en arbre dont les feuilles sont les machines (ordinateurs).
- Le niveau le plus haut (la racine ou root) est représenté par un point (.), la racine se subdivise en TLDs (Top Level Domains) qui comprennent :
  - ↳ Les TLD « historiques » .com .edu .gov .mil .org .net
  - ↳ Les nouveaux TLD .aero .coop .museum .biz .info .name .pro
  - ↳ Un TLD par pays
  - ↳ Un pseudo TLD appelé arpa pour la résolution inverse (cf plus loin)

## Présentation de la résolution de noms DNS

### L'espace de noms hiérarchisé

- A chaque division des branches de l'arbre (nœud) et à chaque feuille de l'arbre sont associés un nom (63 caractères maxi.) et un ensemble de ressources. Exemples de noms :

- ↳ univ-rennes1
- ↳ istic
- ↳ edf
- ↳ google
- ↳ fr
- ↳ edu
- ↳ gtr04

## Présentation de la résolution de noms DNS

### L'espace de noms hiérarchisé

- Le nom complet d'un nœud est la suite des noms de domaines (en remontant à la racine) séparés par un point. Exemple de nom complet :
  - ↳ mail.istic.univ-rennes1.fr
  - ↳ www.google.fr
  - ↳ urec.cnrs.fr.
- Le nommage peut être relatif si l'origine du nom est connue et définie comme origine courante. Par exemple :
  - ↳ gtr04.iut-lannion peut être utilisé si l'origine courante est univ-rennes1.fr.
- Deux machines peuvent avoir le même nom si elles se trouvent dans des domaines différents

## Présentation de la résolution de noms DNS

### Syntaxe des noms de domaines

- ↳ Syntaxe définie dans le RFC 1032.
- ↳ 63 caractères maximum, A..Z, a..z, 0..9, -,
- ↳ Il peut y avoir un nombre minimum de caractères.
- ↳ Doit commencer par une lettre.
- ↳ Le gérant du domaine englobant le vôtre doit assurer l'unicité des noms à l'intérieur de ce domaine (sous-domaine).

### La notion de domaine est administrative

- Il n'y pas correspondance systématique entre adresse ip et nom de domaine.
- ↳ Deux sites d'une même entreprise (ayant enregistré un nom de domaine unique) peuvent avoir des plans d'adressage ip complètement disjoints.
- ↳ Les noms de domaines sont hiérarchisés contrairement aux @ip.

## Présentation de la résolution de noms DNS

### Administration des noms de domaines

- Le Network Information Center (NIC) aux Etats-Unis est responsable de la coordination mondiale : c'est l'AUTORITE mondiale.
- Pour les domaines attachés aux pays, il délègue la gestion des noms par zone géographique :
  - ↳ C'est le RIPE-NCC qui est l'AUTORITE pour l'Europe.
  - ↳ Celle-ci délègue à son tour la gestion des noms par pays.
  - ↳ C'est l'AFNIC qui est l' AUTORITE pour la France (domaine fr.)
- Chaque administrateur de domaine (Universités, entreprises, associations, entités administratives ...) gère son propre domaine. Il est l'AUTORITE pour son domaine et est responsable de l'unicité des noms de son domaine.

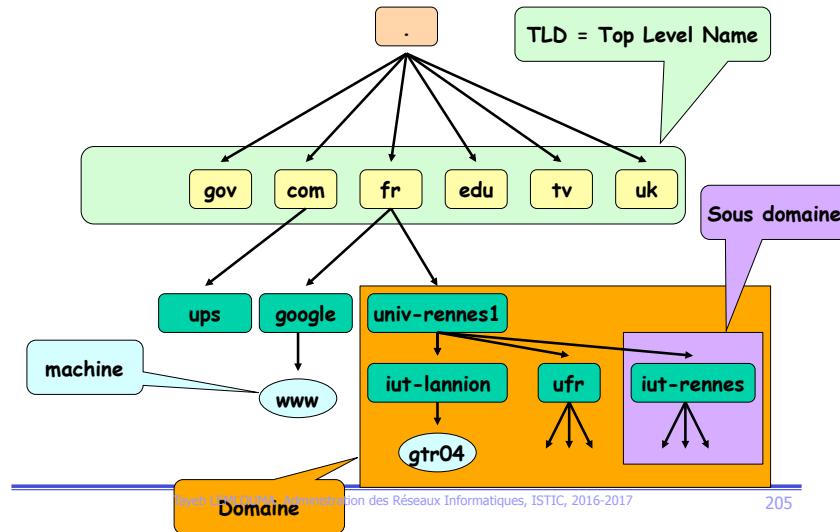
## Le DNS

### Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
6. Mécanisme de résolution de noms
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Hiérarchie de noms du DNS

Arbre de nommage : résolution de nom directe



## Hiérarchie de noms du DNS

### Domaines et nommage

- istic.univ-rennes1.fr est un sous-domaine du domaine univ-rennes1.fr qui est lui-même un sous-domaine du domaine fr
- mail.istic.univ-rennes1.fr est un ordinateur du domaine istic.univ-rennes1.fr
- Le point à la fin du nom complet qui représente la racine est omis la plupart du temps (sauf au niveau des fichiers de configuration du DNS).

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

206

## Hiérarchie de noms du DNS

### Résolution de noms inverse

- Pour des raisons de sécurité, un certain nombre d'applications (courrier électronique par exemple) vérifie que l'expéditeur d'un message est bien celui qu'il prétend être et que le domaine auquel il appartient est bien enregistré auprès des instances qui ont AUTORITE.
  - ↳ Ces applications demandent donc l'adresse ip de l'expéditeur (à partir du nom symbolique qui apparaît dans le message).
- Il existe dans l'arbre de nommage mondial une branche dévolue à la résolution inverse. Cette branche (TLD) a comme nom "arpa" et pour la résolution inverse des adresses Internet, le nœud suivant s'appelle in-addr.

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

207

## Hiérarchie de noms du DNS

### Résolution de noms inverse

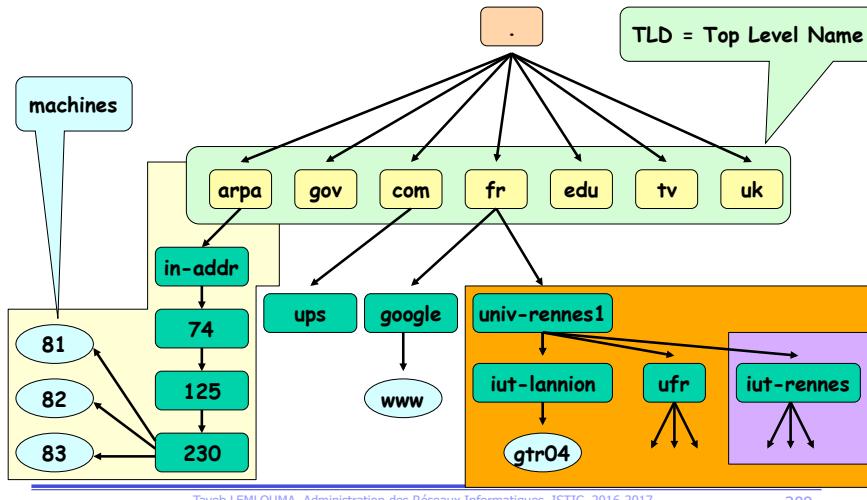
- ↳ Les nœuds suivants sont répartis en 3 niveaux (1 niveau par octet de l'adresse ip).
- ↳ Chacun de ces niveaux se ramifie en 256 branches. Les noms des nœuds, contrairement aux noms de domaine sont les chiffres (de 0 à 254) de la numérotation ip.

Tayeb LEMLOUMA, Administration des Réseaux Informatiques, ISTIC, 2016-2017

208

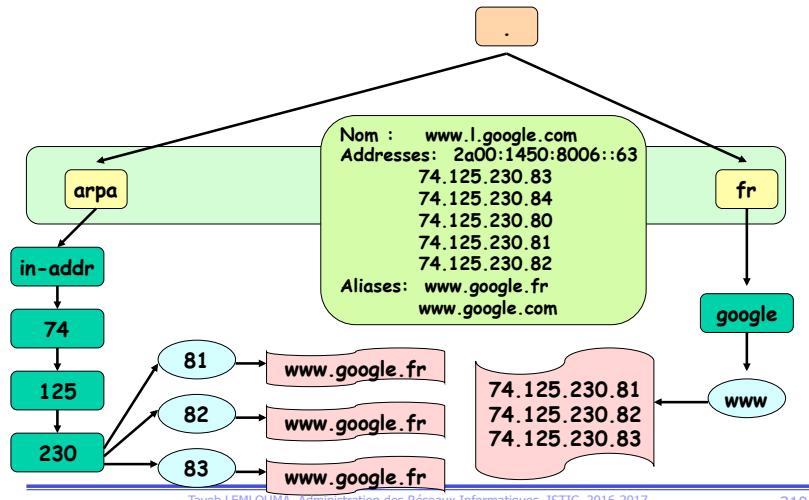
## Hiérarchie de noms du DNS

### Arbre de nommage : résolution de nom inverse



## Hiérarchie de noms du DNS

### Arbre de nommage : association nom – adresse IP



## Le DNS

### Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
- 4. Les serveurs DNS**
5. Gestion des requêtes
6. Mécanisme de résolution de noms
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Les serveurs DNS

### Notion de "Resource Records"

- La base de données du DNS comporte, entre autres, des enregistrements correspondants à chaque "machine" ou "feuille de l'arbre" de la zone administrée.
- Ces informations s'appellent Resource Records.
- Ces RRs sont enregistrés et regroupés sur des machines qui jouent le rôle de serveur DNS pour les autres machines du réseau .
- Un seul serveur DNS ne suffit pas à gérer la totalité des RRs au niveau mondial. Les enregistrement RRs sont répartis sur un nombre important de machines de manière structurée et hiérarchisée.
- Chaque serveur DNS possède une partie des informations. Ces serveurs sont accessibles à travers un service fonctionnant suivant le principe du client/serveur.

## Les serveurs DNS

### Notion de zone

- L'espace des noms de domaine est découpé en ZONES administratives.
  - ↳ Chaque serveur DNS (Name Server ou NS) a "autorité" sur au moins une partie de l'arbre de nommage appelée "zone".

### Hiérarchie des serveurs DNS

- Il existe au niveau mondial un nombre limité de serveurs DNS (une dizaine) qui ont autorité sur la zone ". ". Ces serveurs, appelés "**serveurs racines**", gèrent uniquement les TLD (Top Level Name).
- L'autorité qu'un NS a sur une partie de l'arbre, lui a été **déléguee** par le serveur de niveau supérieur dans la hiérarchie.

## Les serveurs DNS

### Hiérarchie des serveurs DNS

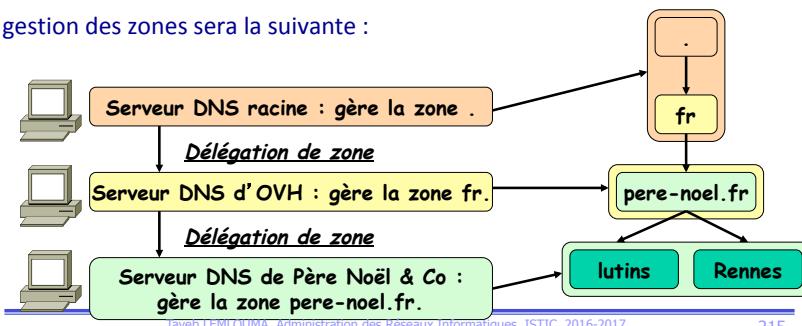
- Un serveur DNS peut organiser comme il veut la ou les zones sur la ou lesquelles il a autorité :
  - ↳ Il peut **déléguer** à son tour son autorité pour une partie des sous-zones dont il a la charge sur des serveurs de noms de niveau inférieur.
- Attention : une zone peut recouvrir exactement un domaine (ou sous-domaine) mais ce n'est pas une obligation
- Une zone peut contenir plusieurs (sous) domaines ou n'administrer qu'une partie d'un (sous) domaine. Dans ce dernier cas, il délègue alors l'administration des autres parties à des serveurs délégués.

## Les serveurs DNS

### Exemple d'organisation de zone

- L'entreprise "Père Noël & Co" désire faire un site Web avec le nom de domaine "pere-noel.fr".
  - ↳ Pour cela, elle achète auprès de l'hébergeur OVH de sites Web le nom de domaine.
  - ↳ OVH a délégation de l'AFNIC pour gérer les TLD ".fr".
  - ↳ L'entreprise décide de gérer elle-même les sous domaines "lutins" et "rennes" du domaine "pere-noel.fr".

La gestion des zones sera la suivante :



## Les serveurs DNS

### Fiabilisation du système : Notion de Zone primaire et secondaire

- La résolution de noms est un service clef d'un réseau.
- Dans la hiérarchie des serveurs présentée dans les diapos qui précédent, un seul serveur gère une zone.
  - ↳ Et s'il tombe en panne ?
- Il est nécessaire de fiabiliser le service par redondance de la base de données associées
- Pour cela, il existe la notion de zone primaire et secondaire : une même zone peut être gérée par plusieurs serveurs DNS :
  - ↳ Un seul serveur gérera une zone en primaire : le serveur possédera l'original de la base, il pourra répondre aux requêtes DNS concernant cette zone. C'est le seul qui aura AUTORITE sur la zone (c'est sur ce poste que l'on modifierra la zone).

## Les serveurs DNS

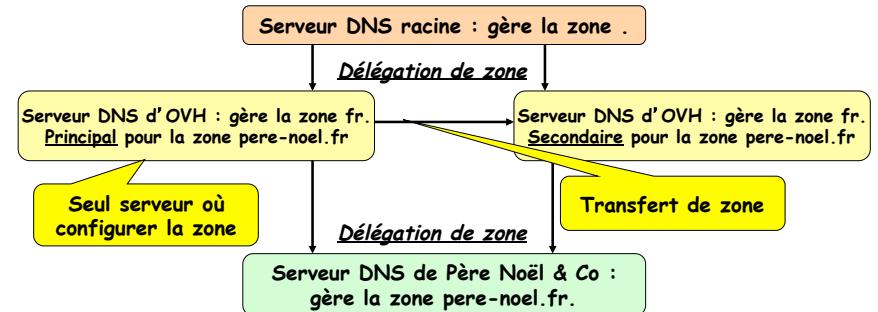
### Fiabilisation du système : Notion de Zone primaire et secondaire

- ↳ Plusieurs serveurs pourront gérer la zone en secondaire : le serveur ne possédera qu'une copie de la base de données, mais pourra répondre aux requêtes DNS concernant cette zone.
- Bonne pratique :
  - ↳ Mettre un serveur secondaire physiquement dans un endroit distant du primaire (bâtiment différent par exemple)

## Les serveurs DNS

### Fiabilisation du système : Notion de Zone primaire et secondaire

- Dans le cas où l'on doit modifier les enregistrements dans la zone, il faudra le faire obligatoirement sur le serveur qui est "principal" pour la zone".
- Les autres serveurs qui sont "secondaires" pour la zone transféreront à intervalle régulier (par exemple chaque 24 heures) la base de données de la zone pour en avoir une copie la plus "récente" possible.



## Le DNS

### Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
6. Mécanisme de résolution de noms
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Gestion des requêtes

### Informations stocké dans une zone de recherche

- Pour chaque zone de recherche directe ou inverse, le serveur DNS peut mémoriser :
  - ↳ Les @ip et noms des machines de sa (ses) zone(s)
  - ↳ Les @ip et noms d'autres ressources de sa (ses) zone(s)., par exemple : le serveur de mail, le serveur d'authentification (pour les réseauxWindows).
  - ↳ Les @ip et noms des NS des zones incluses (quand il fait de la délégation pour un sous domaine à un autre serveur DNS).
- En plus, le serveur DNS gère les NS (adresses IP) des serveurs racine (qui gèrent la zone "root" ou "."). Un administrateur réseau se doit donc de suivre l'évolution de la liste des serveurs racines de manière à ce que ses serveurs DNS soient à jour.

## Gestion des requêtes

### Fonctionnement d'un serveur DNS par rapport aux requêtes

➤ Un serveur DNS doit :

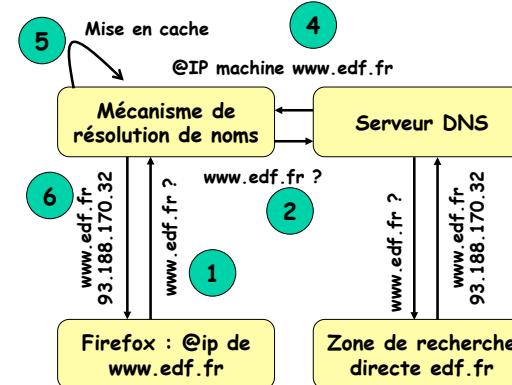
- ↳ Répondre aux requêtes de résolution directe et inverse reçues concernant des ressources de sa (ses) zone(s).
- ↳ Répondre à des requêtes de résolution directe et inverse concernant d'autres zones en questionnant d'autres serveurs DNS (fonctionnement en récursif). Dans ce cas, il va en plus mémoriser les informations pour ne pas avoir à chaque fois à les redemander (mise en cache).
- ↳ Donner au demandeur le moyen d'obtenir une réponse qu'il n'a pas ou questionner les autres serveurs au nom du demandeur (fonctionnement en itératif).

## Gestion des requêtes

### Réponse à des requêtes concernant des zones qu'il gère

A partir d'une machine d'un bureau de l'EDF :

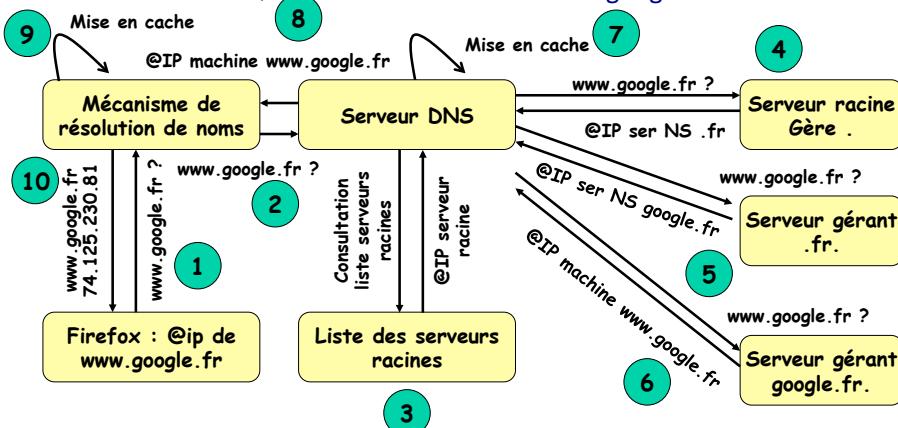
- ↳ Quelle est l'adresse IP de www.edf.fr ?



## Gestion des requêtes

### Réponse à des requêtes concernant des zones qu'il ne gère pas

En mode récursif : Quelle est l'adresse IP de www.google.fr ?



## Gestion des requêtes

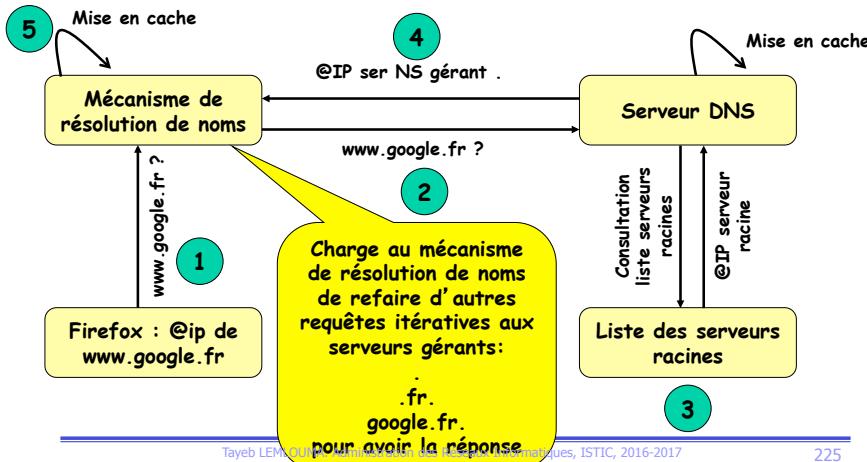
### Question en mode récursif : les réponses possibles du serveur

- Mode facultatif précisé par un drapeau dans la requête. Logiquement, tous les serveurs gèrent maintenant ce mode, à condition de le valider.
- Par souci de performance, les routeurs racines ainsi que ceux qui gèrent les .xx. ne fonctionnent pas en mode récursif.
- Deux réponses possibles :
  - ↳ L'information demandée s'il la connaît par son cache, ou parce qu'il a autorité sur la zone indiquée dans la demande et qu'il a cette information
  - ↳ Une indication d'erreur s'il n'a pas la réponse ni sur la (les) zone(s) pour laquelle il a autorité et s'il n'a pas obtenu de réponse des autres serveurs qu'il a interrogé pour le compte de son client

## Gestion des requêtes

### Réponse à des requêtes concernant des zones qu'il ne gère pas

En mode itératif : Quelle est l'adresse IP de www.google.fr ?



## Gestion des requêtes

### Question en mode itératif : les réponses possibles du serveur

- Pour un serveur DNS, c'est le mode minimal et obligatoire.
- Il fournira 3 réponses possibles :
  - ↳ L'information demandée s'il la connaît.
  - ↳ Une indication d'erreur s'il devrait avoir la réponse et qu'il ne l'a pas (il a délégation de la zone, mais ne trouve pas la réponse).
  - ↳ L'adresse d'un ou plusieurs NS qui gère une partie du chemin pour accéder au nom de domaine s'il ne gère pas la zone DNS recherchée sur le domaine indiqué dans la demande.

## Gestion des requêtes

### Fonctionnement en mode cache

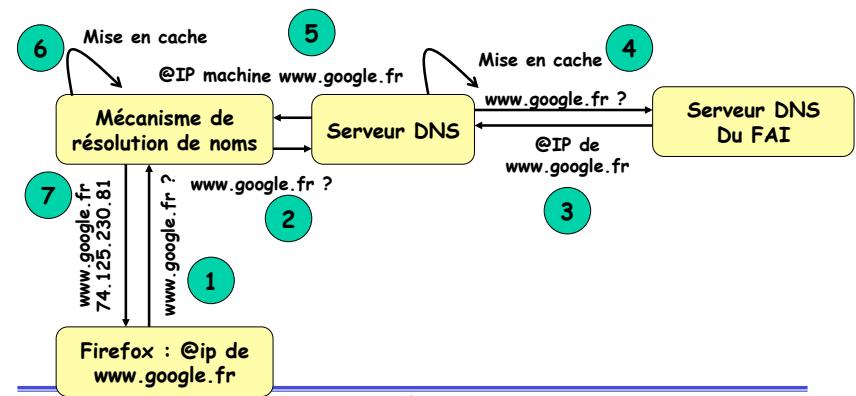
- C'est la fonction minimale d'un serveur de nom (appelé alors serveur cache).
- Un serveur cache :
  - ↳ S'il connaît la réponse grâce au cache, donne la réponse.
  - ↳ S'il ne connaît pas la réponse :
    - ✓ Soit il construit une (des) requêtes pour les NS successifs en mode généralement itératif (en commençant par ceux de la zone Root) et transmet la réponse au client qu'elle soit positive ou négative (erreur).
    - ✓ Soit retransmet la question à un "Forwarder", généralement à son fournisseur d'accès pour avoir une réponse.
- Enfin, il mémorise pendant un temps fini la correspondance nom symbolique <--> adresse IP obtenue.

## Gestion des requêtes

### Réponse à des requêtes d'un serveur cache

Configuration avec un Forwarder :

- ↳ Quelle est l'adresse IP de www.google.fr ?



# Le DNS

## Plan

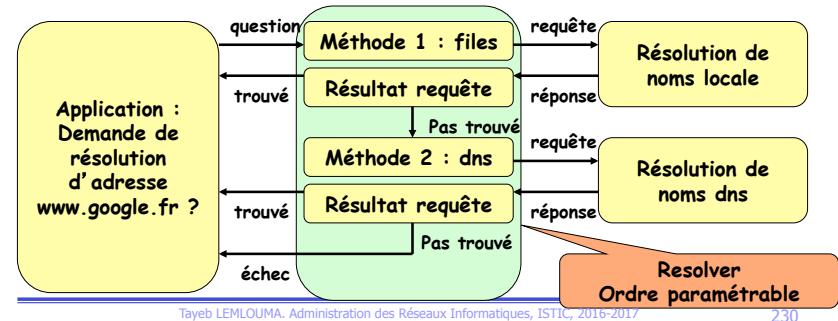
1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
- 6. Mécanisme de résolution de noms**
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Mécanisme de résolution de noms

### Présentation du mécanisme de résolution de noms

➤ Le "resolver" est le mécanisme qui, sur un poste client, gère la résolution de nom.

↳ Il faut le configurer de manière à choisir quelle méthode de résolution de nom on va utiliser et dans quel ordre. C'est la fonction minimale d'un serveur nom (appelé alors serveur cache).



## Mécanisme de résolution de noms

### Configuration du resolver sous Unix

- Sous Unix, le resolver applique une stratégie de recherche définie au niveau de la machine dans les fichiers "/etc/nsswitch.conf".
- Le fichier "nsswitch.conf" précise dans quel ordre et par quelle méthode faire la résolution des noms. Il existe en effet plusieurs méthodes utilisables sur une même machine.
- Rappel :
- ↳ Résolution locale.
  - ↳ Le protocole NIS.
  - ↳ Le protocole DNS

## Mécanisme de résolution de noms

### Le fichier "/etc/nsswitch.conf"

➤ Sous Unix le fichier "/etc/nsswitch.conf" contient, en autres, l'ordre dans lequel doit se faire la résolution de noms.

↳ Exemple : Extrait d'un fichier "nsswitch.conf" :

```
...
hosts: files dns
passwd: nis files
group: nis files
...
```

Dans l'exemple ci-dessus, le "resolver" commence la résolution de nom "locale" par la lecture du fichier "/etc/hosts", puis s'il ne trouve pas la réponse, le "resolver" fait une requête au serveur DNS.

**Remarque :** Ce fichier ci-dessus ne sert pas uniquement à la résolution de noms.

## Mécanisme de résolution de noms

### La résolution de noms "locale" sous Unix

- Le fichier "/etc/hosts" est obligatoire sur une machine.
- Il contient au minimum l'adresse de la "loopback" (127.0.0.1) et le nom de la machine elle-même.
- Il sert en l'absence d'autres méthodes de résolution ou quand la machine est non connectée au réseau ou pour l'adresse de loopback pour faire fonctionner certains services

### La résolution de noms "NIS" sous Unix

- Le protocole NIS permet de résoudre facilement les adresses dans un réseau local.
- Il centralise le fichier "/etc/hosts" d'une machine spécifique du réseau qui aura alors un rôle de serveur NIS. Il y aura éventuellement un serveur secondaire. Les autres machines du réseau seront alors clientes.
- Le NIS permet aussi de centraliser de nombreux autres informations réseaux (comptes utilisateurs par exemple)

## Mécanisme de résolution de noms

### Fonctionnement du fichier "resolv.conf" :

```
domain tp1.gtr.fr
search tp1.gtr.fr gtr.fr
nameserver 10.254.0.254
nameserver 10.12.1.1
```

- Un nom comme "**w10**" sera étendu automatiquement à "**w10.tp1.gtr.fr.**".
- La recherche sera faite avec cette extension puis en cas d'échec avec l'extension "gtr.fr." (**w10.gtr.fr.**).
- En donnant le nom "**www.google.fr.**", le nom ne sera pas étendu et la demande sera uniquement faite sous cette forme
- En l'absence de la directive search la recherche de **w10** partira de l'extension avec le domaine local complet puis son domaine parent

## Mécanisme de résolution de noms

### La résolution de noms "DNS" sous Unix

- Le fichier "/etc/resolv.conf" fournit :
  - ↳ Le nom du domaine auquel appartient la machine.
  - ↳ La ou les manières de compléter un nom incomplet pour en faire une recherche de résolution inverse.
  - ↳ Le nom des serveurs DNS qu'il pourra contacter.

#### Exemple de fichier resolv.conf

```
domain tp1.gtr.fr
search tp1.gtr.fr gtr.fr
nameserver 10.254.0.254
nameserver 10.12.1.1
```

Information non obligatoire si le nom de domaine de la machine est spécifié ailleurs

Information non obligatoire

information non obligatoire

## Le DNS

### Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
6. Mécanisme de résolution de noms
- 7. Le dialogue entre client et serveur DNS**
8. Fichiers de configuration d'un serveur DNS

## Le dialogue entre client et serveur DNS

### Service et protocole DNS

- Sous debian, le nom du service DNS est "/etc/init.d/bind9".
- Pour les échanges entre les clients et les serveurs DNS, le port d'écoute est le N° 53 en UDP.
- Pour les transferts de zones entre un serveur principal et les serveurs secondaires, le port d'écoute est le N° 53 en TCP.

### Format des messages échangés

- Le protocole fonctionne en binaire entre le client et le serveur.
- Chaque message échangé est composé de 5 parties :

- ↳ Header : entête
- ↳ Question : la question
- ↳ Answer : la ou les réponses
- ↳ Authority : la ou les NS qui ont autorité pour donner la réponse (un cache n'a pas autorité)
- ↳ Additional : la ou les informations supplémentaires (adresses des serveurs par exemple)

## Le dialogue entre client et serveur DNS

### Infos les plus courantes contenues dans la BDD d'un serveur DNS

- La liste suivante contient les informations les plus courantes contenues dans les fichiers de configuration d'un serveur DNS.

SOA	: Start Of Authority	: début de description de zone sur laquelle le serveur a autorité.
A	: Address	: relation nom --> adresse (IPv4)
PTR	: PointeR	: relation adresse-->nom
MX	: Mail eXchanger	: nom d'un serveur de messagerie
CNAME	: Canonical Name	: relation alias --> nom officiel
HINFO	: Host Information	: information sur une machine
NS	: Name Server	: nom d'un serveur de nom

## Le dialogue entre client et serveur DNS

### Format de la partie HEADER des messages

- Il comprend de nombreuses informations dont :
- ↳ Le type d'opération (question ou réponse).
  - ↳ Le type de requête (directe ou inverse).
  - ↳ Si la réponse vient d'une entité qui a autorité ou non.
  - ↳ Si le message est tronqué ou non.
  - ↳ Si la récursion est désirée ou non par le client (celui qui fait la demande).
  - ↳ Si la récursion est disponible ou non par le serveur.
  - ↳ Un code d'erreur (réponse).
  - ↳ Le nombre de questions (1 pour une requête).
  - ↳ Le nombre de champs dans la réponse.
  - ↳ Le nombre de champs de NS primaires et secondaires (serveur de nom).
  - ↳ Le nombre de champ d'informations supplémentaires (adresses des serveurs par exemple).

## Le dialogue entre client et serveur DNS

### Format d'un Resource Record

{nom/numéro} {Durée} Classe Type Données

- nom/numéro = nom de la machine (RR de type A ou MX ou CNAME) ou numéro ip (RR de type PTR) ou nom de domaine servi (RR de type NS)
  - ↳ si vide et RR de type NS le nom est le dernier nom de domaine défini dans le fichier.
  - ↳ si RR de type A ou MX ou CNAME, le nom est donné en absolu s'il est terminé par le ". " sinon le nom est relatif au domaine courant.
  - ↳ si RR de type PTR le numéro est donné en absolu ou est automatiquement complété par le numéro indiqué dans le nom de la zone (écrit à l'envers).
- durée (time to live) = temps pendant lequel un serveur cache doit garder l'information avant de la détruire ou de la redemander.
  - ↳ définies en secondes.
  - ↳ si vide valeur définit dans le SOA.
- classe = une seule est effectivement utilisée : IN (pour Internet).
- type = SOA,A,PTR,NS...
- données = valeur(s) de la ressource (nom symbolique, adresse ...).

## Le dialogue entre client et serveur DNS

### Les enregistrements SOA

- Le champ données du Resource Record SOA comprend plusieurs informations :
  - ↳ Le nom de la machine qui a autorité sur le zone concernée.
  - ↳ Le nom de la boîte aux lettres du gérant de la zone.
  - ↳ Le numéro de série de la description de la zone.
  - ↳ La fréquence de mise à jour (pour les serveurs secondaires).
  - ↳ Le temps d'attente pour faire un nouvel accès au serveur principal après un échec de remise à jour (pour un serveur secondaire).
  - ↳ Le temps au bout duquel un serveur secondaire doit détruire les informations qu'il a acquises lorsqu'il ne peut obtenir de rafraîchissement.
  - ↳ Valeur par défaut du TTL minimum pour les ressources.
- Les durées sont données par défaut en secondes.

## Le dialogue entre client et serveur DNS

### Format des champs de réponses

- Ils sont d'une structure sensiblement identique et contiennent toutes les informations contenues dans les RRs correspondants en particulier le TTL (durée) :

{nom/numéro} {Durée} Classe Type Données

- Les noms symboliques sont réduit à la valeur minimum si le nom complet peut être retrouvé par le client avec les informations qu'il possède

## Le DNS

### Plan

1. Introduction
2. Présentation de la résolution de noms DNS
3. Hiérarchie de noms du DNS
4. Les serveurs DNS
5. Gestion des requêtes
6. Mécanisme de résolution de noms
7. Le dialogue entre client et serveur DNS
8. Fichiers de configuration d'un serveur DNS

## Fichiers de configuration d'un serveur DNS

### Fichier de configuration "named.conf"

```
// Boot file for LAND-5 name server
options {
    directory "/var/named";
};

zone "." {
    type hint;
    file "root.hints";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "zone/127.0.0";
};

zone "land-5.com" {
    type master;
    file "zone/land-5.com";
};

zone "177.6.206.in-addr.arpa" {
    type master;
    file "zone/206.6.177";
};
```

## Fichiers de configuration d'un serveur DNS

### Fichier des serveurs de la zone racine (extrait) "root.hints"

```
; formerly NS.INTERNIC.NET
.          3600000 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4 ;
; formerly NS1.ISI.EDU
.          3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 128.9.0.107
; formerly C.PSI.NET
.          3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
; formerly TERP.UMD.EDU
.          3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A 128.8.10.90
; formerly NS.NASA.GOV
.          3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10
```

## Fichiers de configuration d'un serveur DNS

### Exemple de fichier de zone locale (inverse)

```
@      IN  SOA   land-5.com. root.land-5.com. (
                     199609203 ; Serial
                     28800 ; Refresh
                     7200  ; Retry
                     604800 ; Expire
                     86400 ) ; Minimum TTL
                  NS    land-5.com.

1      PTR   localhost.
```

## Fichiers de configuration d'un serveur DNS

### Exemple de fichier de zone directe

```
@ IN SOA land-5.com. root.land-5.com. (
         199609206 ; serial
         8H          ; refresh, seconds
         2H          ; retry, seconds
         1W          ; expire, seconds
         1D)         ; minimum, seconds
      NS land-5.com.
      NS ns2.psi.net.
      MX land-5.com.
      TXT "LAND-5 Corporation"
localhost A 127.0.0.1
land-5.com. A 206.6.177.2
ns2.psi.net. A 207.152.17.5
www A 207.159.141.192
ftp    CNAME land-5.com.
mail   CNAME land-5.com.
```

## Fichiers de configuration d'un serveur DNS

### Exemple de fichier de zone inverse

```
@ IN SOA land-5.com. root.land-5.com. (
         199609206 ; Serial
         28800 ; Refresh
         7200  ; Retry
         604800 ; Expire
         86400 ) ; Minimum TTL
      NS land-5.com.
      NS ns2.psi.net.

; Servers
;
1      PTR   router.land-5.com.
2      PTR   land-5.com.
2      PTR   funn.land-5.com.
```

## Fichiers de configuration d'un serveur DNS

### Exemple de délégation de zone

```
; Definition de la zone parent.fr
@ IN SOA serveur1.parent.fr. e-mail.machine.fr. (
;       etc...
)
; Avec deux serveurs de noms dans la zone
IN      NS   serveur1.parent.fr.
IN      NS   serveur2.parent.fr.
; Normalement
IN      MX   10 relais.parent.fr.

; Delegation de la zone fille.parent.fr
; Avec un serveur de noms propre a cette
zone ( primaire)
;
) ; et un serveur de noms commun a la zone
parente
fille    IN   NS  serveur3.fille.parent.fr.

IN      NS   serveur2.parent.fr.

; Suite de la definition de la zone parent.fr
serveur1 IN   A   192.10.20.30
serveur2 IN   A   192.10.20.40
; Fin
```

## Fichiers de configuration d'un serveur DNS

### Caractères spéciaux et mots réservés courants

.	: Domaine courant
@	: Origine courante
()	: Données associées sur plusieurs lignes
;	: Commentaires
*	: N'importe quelle chaîne de caractères
\$INCLUDE	<i>nom de fichier</i> : inclusion d'un fichier
\$ORIGIN	<i>nom de domaine</i> : définition de l'origine par défaut des noms symboliques

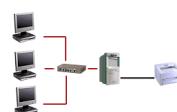
Sous Windows :

Installer un serveur DNS sous Windows compatible Windows Server 2008 :

☞ <http://idum.fr/spip.php?article175>

## 6.

# Configuration automatique des stations IP et de leurs adresses : DHCP



## Le protocole DHCP

### Objectif

L'objectif de ce cours est de vous présenter le protocole DHCP qui permet d'allouer, automatiquement pour l'utilisateur, la configuration réseau du poste client.

### Différents points seront abordés :

- Le protocole DHCP.
- Le format des échanges.
- Les cas particuliers du protocole.
- La notion de serveur DHCP relais.

# Le protocole DHCP

1. Présentation
2. Étude du protocole DHCP
3. Cas particulier du protocole
4. Le service DHCP sous linux
5. Le serveur DHCP Relais

## Présentation

### Définition

- ↳ DHCP signifie "Dynamic Host Configuration Protocol".
- ↳ Il s'agit d'un protocole qui permet à un ordinateur, qui se connecte sur un réseau local, d'obtenir dynamiquement et automatiquement sa configuration IP.
- ↳ **But principal :** Simplification de l'administration d'un réseau.
- ↳ Grâce à la centralisation de la configuration IP des équipements sur un serveur.
- Cette partie vous présente ce protocole pour les adresses IPv4.
- Le protocole DHCP fonctionne aussi pour l'IPv6, mais le fonctionnement est relativement différent

### Avantages

- Simplification de l'administration d'un réseau.
- ↳ Facilités de changement et d'évolution.
- Permet de pouvoir disposer de plus de machines que d'adresses IP (par exemple, pour un fournisseur d'accès).

## Présentation

### Fonctionnement général

- Le protocole DHCP fonctionne sur le modèle client – serveur
- Il est nécessaire d'avoir sur le réseau :
  - Au moins un serveur DHCP :
    - ↳ Le serveur, qui détient la politique d'attribution des configurations IP, envoie une configuration donnée pour une durée précise à un client : typiquement, une machine qui vient de démarrer.
    - ↳ Le serveur va servir de base pour toutes les requêtes DHCP (il les reçoit et y répond). **Il doit donc avoir une configuration IP fixe.**
  - Un poste client :
    - ↳ Le poste client sera configuré afin d'obtenir "automatiquement" (c'est le terme utilisé par Windows sur les postes clients) une configuration réseau.
    - ↳ En fait, **ce n'est pas "automatique"**. Le poste client sera configuré pour "demander" à un serveur DHCP une configuration réseau afin de pouvoir se connecter sur le réseau.

## Présentation

### Historique : le protocole Bootp

- Le protocole DHCP est une grande évolution du protocole Bootp.
- Le protocole bootp était utilisé surtout pour donner une adresse IP à équipement (l'adresse IP, masque et passerelle par défaut) et faire du client léger (machine cliente sans disque dur, donc dans possibilité de sauvegarde locale)
- Ce protocole avait de nombreuses limitations :
  - ↳ La durée du bail n'était pas configurable et prenait souvent une valeur infinie.
  - ↳ Le serveur Bootp devait avoir connaissance de l'adresse MAC du client Bootp pour être autorisé à lui répondre, et disposer des paramètres IP qui lui sont associés.
  - ↳ Une table faisant correspondre pour chaque client Bootp son adresse MAC et les paramètres IP associés doivent donc être manuellement renseignés pour chaque équipement. **Ce mécanisme était difficile à administrer.**

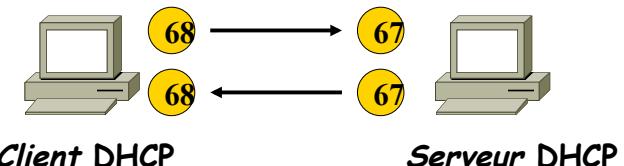
## Le protocole DHCP

1. Présentation
2. Étude du protocole DHCP
3. Cas particulier du protocole
4. Le service DHCP sous linux
5. Le serveur DHCP Relais

## Le protocole DHCP

### Transport des messages DHCP

- Les messages DHCP sont transportés par le protocole UDP. Pour l'IPv4, les numéros de ports sont :
  - ↳ Le port côté client est le 68.
  - ↳ Le port côté serveur est le 67.
- Ce n'est donc pas une relation client-serveur classique (port client >1024 temporaire, port serveur <1024 fixe).



## Le protocole DHCP

Attribution d'une adresse IP : un échange en 4 trames



**Important :** Le serveur et les postes clients doivent se situer dans le même réseau, car le protocole fonctionne avec des trames de Broadcast.

↳ N'oubliez pas que les trames de broadcast ne sont pas routées.

## Le protocole DHCP

Attribution d'une adresse IP : un échange en 4 trames

La trame "DHCP Discovery" :

- Quand un client désire avoir une adresse IP, il émet une trame "DHCP Discovery" qui permet de localiser les serveurs DHCP disponibles.

Protocole	Adresse source	Adresse destination
MAC	@ MAC station	FF:FF:FF:FF:FF
IP	0.0.0.0	255.255.255.255

La trame "DHCP Offer" :

- Si le serveur DHCP est capable de satisfaire la demande, il répond en émettant une trame "DHCP Offer".

Protocole	Adresse source	Adresse destination
MAC	@ MAC serveur	@ MAC station
IP	@ ip serveur	@IP_donnée_au_client

## Le protocole DHCP

### Attribution d'une adresse IP : un échange en 4 trames

➤ La norme suggère au serveur DHCP :

- ↳ D'être capable de vérifier que l'adresse IP proposée n'est pas déjà utilisée sur le réseau (par des échos ICMP request par exemple).
- ↳ De laisser le choix à l'administrateur d'activer ou non cette vérification.

➤ Il est obligatoire d'enregistrer cette offre dans un fichier de "lease", afin :

- ↳ De ne pas proposer la même adresse à plusieurs clients.
- ↳ De retrouver l'état actuel des adresses IP attribuée en cas de redémarrage du serveur DHCP.
- ↳ De satisfaire la législation qui impose aux fournisseurs d'accès de savoir qui a eu telle adresse IP à telle heure.

➤ Important :

- ↳ Il existe un fichier de lease sur le client et le serveur. **Il est nécessaire, en cas de très grands changements de configuration du serveur, de vider ces fichiers** (en prenant soin de sauvegarder le fichier du serveur pour des aspects légaux).

## Le protocole DHCP

### Attribution d'une adresse IP : un échange en 4 trames

➤ La norme recommande de respecter la stratégie suivante pour l'attribution d'une adresse IP :

- ↳ S'il existe déjà une entrée dans le fichier de "lease" pour ce client, et qu'elle est en cours de validité, le serveur attribue la même adresse IP que celle mentionnée dans l'entrée.

- ↳ S'il existe déjà une entrée dans le fichier de "lease", mais qu'elle n'est plus valide (le bail a expiré, ou elle a été préalablement libérée par le client), le serveur attribue la même adresse IP que celle mentionnée dans l'entrée, à condition que celle-ci soit encore valide et qu'elle n'ait pas été réattribuée.

- ↳ S'il n'existe pas d'entrée dans le fichier de "lease", le serveur attribue une adresse IP choisie à partir d'un pool d'adresses renseigné administrativement.

## Le protocole DHCP

### Attribution d'une adresse IP : un échange en 4 trames

#### La trame "DHCP Request" :

Le client reçoit l'offre d'adresse IP venant d'un serveur DHCP ou de plusieurs serveurs. Il va choisir l'une des offres. Il signifie son accord au serveur DHCP dont il retient l'offre, par une trame "DHCP Request". Cette trame est émise en Broadcast afin de permettre à tous les serveurs DHCP qui ont proposés une adresse de savoir quelle serveur a été retenu :

Protocole	Adresse source	Adresse destination
MAC	@ MAC station	FF:FF:FF:FF:FF:FF
IP	0.0.0.0	255.255.255.255

## Le protocole DHCP

### Attribution d'une adresse IP : un échange en 4 trames

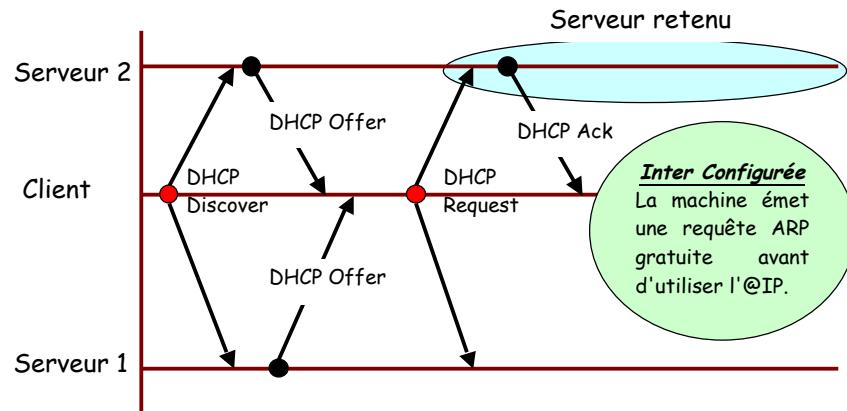
#### La trame "DHCP Ack" :

➤ Le serveur qui a proposé une adresse IP au poste client répond par une trame "DHCP Ack". Cette trame va transporter tous les renseignements complémentaires concernant la configuration réseau de la machine :

- ↳ @ IP du serveur DHCP (pour le renouvellement de bail).
- ↳ La durée de bail.
- ↳ Le masque de sous réseau.
- ↳ Le nom de domaine.
- ↳ L'adresse IP d'un routeur.
- ↳ L'adresse IP d'un serveur DNS.
- ↳ Et plus des 100 autres paramètres possibles.

## Le protocole DHCP

Attribution d'une adresse IP : un échange en 4 trames



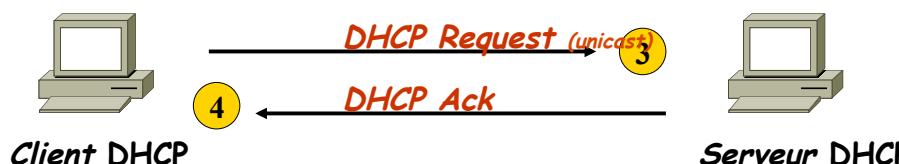
## Le protocole DHCP

1. Présentation
2. Étude du protocole DHCP
3. Cas particulier du protocole
4. Le service DHCP sous linux
5. Le serveur DHCP Relais

## Cas particuliers

### Le renouvellement de bail

- Un client qui souhaite renouveler le bail de son adresse IP, envoie un message "DHCP Request", mais :
  - ↳ En précisant, l'adresse IP qui lui a été préalablement attribuée. Le message est envoyé par **unicast** au serveur qui a préalablement attribué l'adresse IP, et qui enverra en retour un **unicast** d'acquittement.



## Cas particuliers

### Le renouvellement de bail

- Le client qui a été configuré par DHCP a reçu, en argument du message DHCP Ack, deux timers T1 (50% du bail par défaut) et T2 (75% du bail par défaut).
  - ↳ T1 est le temps au bout duquel le client demande une extension de son bail.
  - ↳ S'il n'y a pas eu de renouvellement d'adresse IP à la fin de la durée du bail, le client perd sa connectivité réseau.
- Mécanisme de renouvellement du bail :
  - ↳ Au bout du temps T1, le client émet une trame "DHCP Request" adressée au serveur qui lui a attribué son adresse IP. Il renseigne dans celle-ci son adresse IP courante.
  - ↳ Si le client ne reçoit pas de message d'acquittement au bout de T2, il envoie une trame "DHCP Request" par broadcast à tous les serveurs.
  - ↳ Si le client DHCP ne reçoit pas de trame d'acquittement avant l'expiration de son bail ( $T1 < T2 <$  Durée de bail), il passe à l'état INIT et recommence le processus de configuration IP en émettant une trame de découverte DHCP.

## Cas particuliers

### Stratégie de réglage de la durée du bail

- Les 2 timers sont configurables par le serveurs.
- Mais quelle valeur mettre comme durée de bail ?
  - ↳ Une durée trop petite occupe un peu plus le réseau (mais, cela ne représente que 2 petits échanges à chaque moitié de la durée du bail).
  - ↳ Une durée trop grande est problématique quand on veut modifier le configuration des postes clients.
- Stratégie de réglage :
  - ↳ Une des solutions est de mettre environ 12 heures comme durée. Grâce à cette valeur, une modification de la configuration du serveur DHCP le jour J sera au plus tard opérationnelle à 8h00 le jour suivant.
  - ↳ Par exemple, si on veut arrêter un serveur DNS, on modifie la configuration DHCP le jour J et le lendemain il est possible d'arrêter le serveur DNS, car il ne sera plus utilisé par les postes clients.

## Cas particuliers

### La libération d'adresse IP

- Un client qui souhaite libérer son adresse IP peut envoyer au serveur DHCP un message "DHCP Release".
- ↳ L'envoi de ce message n'est pas systématique, mais est de plus en plus fait par les systèmes actuels.

### Le refus de la configuration proposée par le serveur

- Un client peut refuser une configuration IP envoyée par le serveur. Dans ce cas, il va envoyer un DHCP refuse au serveur.
- ↳ C'est souvent le cas en cas d'erreur dans la configuration IP envoyée par le serveur (par exemple, si la route par défaut n'est pas en remise directe).

## Cas particuliers

### Adresse dynamique ou fixe

- Un serveur DHCP peut être configuré pour fournir des adresses fixes à certaines machines du réseau, comme par exemple :
  - ↳ Un serveur tftp.
  - ↳ Les imprimantes.
- Les avantages d'une attribution fixe sont :
  - ↳ La gestion centralisée des configurations des postes.
  - ↳ Proposer toujours la même adresse IP aux équipements, donc la supervision du réseau est facilitée.
  - ↳ Toutes les options : DNS, passerelle etc. restent configurées dynamiquement, ce qui vous évitera d'avoir à intervenir sur les machines si vous changez la topologie de votre réseau.

## Cas particuliers

### Négociation DHCP excluant l'adresse IP

- Lorsqu'un client DHCP a reçu une adresse IP par un moyen externe (configuration manuelle de l'administrateur), il émet une trame "DHCP Inform" contenant l'adresse IP qu'il souhaite utiliser pour obtenir le reste de sa configuration IP.
- Les serveurs répondent au client par un unicast d'acquittement, adressé à l'adresse IP demandée :
  - ↳ Sans allouer de nouvelle adresse.
  - ↳ Ni vérifier l'adresse demandée.
  - ↳ Sans inclure de durée de bail.
- La norme recommande toutefois au serveur DHCP de vérifier que l'adresse annoncée par le client n'est pas déjà utilisée.

## Le protocole DHCP

1. Présentation
2. Étude du protocole DHCP
3. Cas particulier du protocole
4. Le service DHCP sous linux
5. Le serveur DHCP Relais

## Le protocole DHCP

1. Présentation
2. Étude du protocole DHCP
3. Cas particulier du protocole
4. Le service DHCP sous linux
5. Le serveur DHCP Relais

## Le service DHCP sous Linux

### Configuration du service

- Sous linux, le service DHCP s'appelle isc-dhcp-server.
- Le fichier de configuration est dhcpd.conf. Sa structure est :

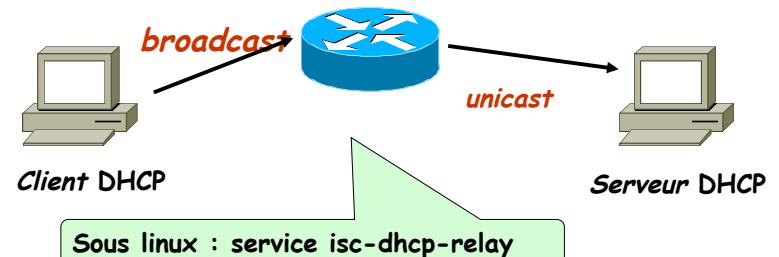
```
01 ddns-update-style none ;  
02 subnet adresse_réseau netmask masque_réseau {  
03   option routers adresse_IP_passerelle_par_défaut ;  
04   option subnet-mask masque_réseau ;  
05   option broadcast-address adresse_broadcast ;  
06   range dynamic-bootp adresse_IP_début1 adresse_IP_fin1 ;  
07   default-lease-time valeur_en_s ;  
08   max-lease-time valeur_en_s ;  
09   host M {  
10     hardware ethernet adresse_MAC_M;  
11     fixed-address adresse_IP_M ;  
12   }  
13 }
```

- Si le réseau à desservir se trouve uniquement derrière un routeur, il faudra au moins un subnet (qui peut être vide) pour un réseau qui lui est directement connecté au serveur. Sinon, le service refuse le démarrage.

## Le protocole DHCP Relais

Cas où le serveur DHCP se trouve dans un autre réseau que les postes clients -> pour un routeur Linux

- Si le serveur DHCP se trouve sur un autre réseau que les postes clients, il est obligatoire d'implémenter sur le routeur un service de DHCP Relais :

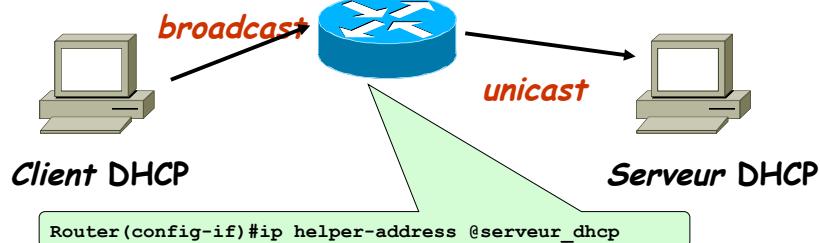


- Le fonctionnement est complètement transparent pour le poste client.

## Le protocole DHCP Relais

Cas où le serveur DHCP se trouve dans un autre réseau que les postes clients -  
> pour un routeur Cisco

- Sur un routeur CISCO, cette fonction de DHCP relais se fait par la commande "ip helper-address", appliquée sur l'interface qui reçoit les trames de broadcast :



Merci