



**IMT Atlantique**

Bretagne-Pays de la Loire  
École Mines-Télécom

*Cybersécurité des systèmes*

*maritimes et portuaires*

# La couche réseau

2021

## Le datagramme IP

Adressage

Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP

Le datagramme IP

Le datagramme IPv4

Le datagramme IPv6

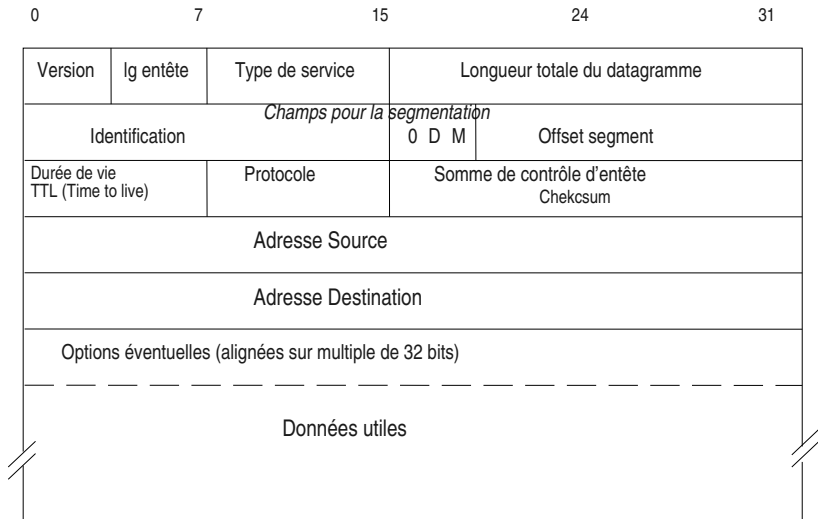
Adressage

Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP



- ▶ Encore appelé ToS (*Type of Service*) rfc1349

Priorité (précédence) Par défaut à 0	Type de service				0
	-délai	+débit	+fiabilité	-coût	

- ▶ Utilisation non généralisée
  - ▶ Précédence utilisable pour marquer des flux dans les nœuds du réseau (routeurs)
  - ▶ Les bits Type de Service peuvent être positionnés par les applications terminales (API socket sous Windows et linux)
  - ▶ Sous Linux ils peuvent être positionnés via la commande iptables selon divers critères

DSCP						0	0
1	2	3	4	5	6	7	8

- ▶ Le champ DSCP sert à coder le *PHB (Per Hop Behavior)*, paramètre fondamental de DiffServ (rfc 2474)
- ▶ Exemples de PHBs :
  - ▶ Expedited forwarding (pertes faibles, latence faible, gigue faible, bande passante assurée)
  - ▶ Assured forwarding (groupe de PHBs)
  - ▶ Best effort
  - ▶ Network control

## ▶ Format :



## ▶ Les options :

- ▶ LSR : *Loose Source Route* : permet d'indiquer la route
- ▶ SSR : *Strict Source Route*, comme précédemment en plus rigoureux
- ▶ RR : *Record Route* : les routeurs traversés rajoutent leur adresse
- ▶ RTALT : *Router Alert*, permet de passer le paquets aux couches hautes des routeurs traversés
- ▶ etc.

## Le datagramme IP

Le datagramme IPv4

Le datagramme IPv6

Adressage

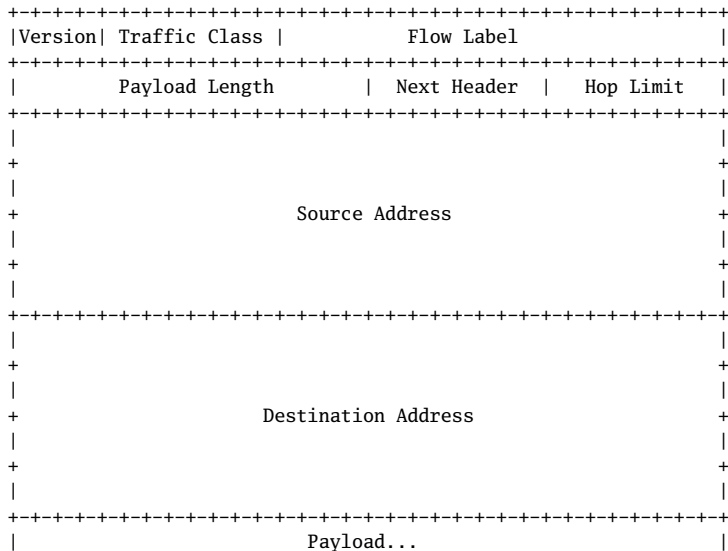
Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP





- ▶ Version : 6 (!)
- ▶ Traffic Class : typiquement Differentiated Services et Explicit Congestion Notification, comme le TOS IPv4
- ▶ Flow Label : pour tagger les paquets d'un même flux ; visiblement peu utilisé...
- ▶ Payload Length : comme son nom l'indique... (Note : dans IPv4 on a la taille *totale* du datagramme)
- ▶ Next Header : remplace le champ Protocole IPv4 et ajoute un mécanisme un peu novateur pour gérer les options (cf. slides suivants)
- ▶ Hop Limit : l'équivalent du champ TTL IPv4 (Note : contrairement à IPv4 qui compte en secondes, ici c'est bien en nombre de sauts)
- ▶ Source & Destination [Addresses](#) : sur **128 bits** (Ouf!)

- ▶ Les headers s'enchaînent dans le payload
- ▶ ...les options IPv6 diverses, puis le protocole transporté effectivement (TCP, UDP, ...)

IPv6 header	TCP header + data
Next Header =	
TCP	

IPv6 header	Routing header	TCP header + data
Next Header =	Next Header =	
Routing	TCP	

IPv6 header	Routing header	Fragment header	fragment of TCP header + data
Next Header =	Next Header =	Next Header =	
Routing	Fragment	TCP	

Le datagramme IP

**Adressage**

Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP

Le datagramme IP

Adressage

- Les adresses IPv4

- Les adresses IPv6

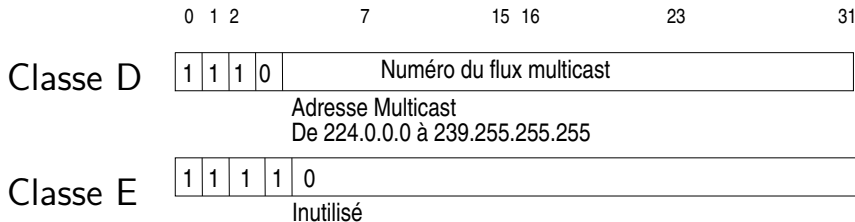
Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP

	0	1	2		7		15	16		23		31
Classe A	0	Numéro de réseau					Numéro de machine					
	De 0.0.0.0 à 126.255.255.255 (en pratique à partir de 1.0.0.0) 127 réseaux, $2^{24}-2$ machines par réseau											
Classe B	1	0	Numéro de réseau				Numéro de machine					
	De 128.0.0.0 à 191.255.255.255 $2^{14}$ réseaux, $2^{16}-2$ machines par réseau											
Classe C	1	1	0	Numéro de réseau					Numéro de machine			
	De 192.0.0.0 à 223.255.255.255 $2^{21}$ réseaux, 254 machines par réseau											



- ▶ L'adresse de boucle locale : 127.0.0.1
  - ▶ Interface lo sous Linux
- ▶ Les adresses privées : rfc-1918
  - ▶ 10.0.0.0 à 10.255.255.255
  - ▶ 172.16.0.0 à 172.16.255.255
  - ▶ 192.168.0.0. à 192.168.255.255
  - ▶ Non routables dans l'Internet
    - ▶ Les machines munies de ces adresses peuvent cependant accéder l'Internet via des passerelles réalisant une fonction de translation d'adresse appelée **NAT** pour **Network Address Translation**
  - ▶ Routables dans les réseaux privés



Différentes possibilités :

- ▶ *Broadcast* sur le réseau local : 255.255.255.255
  - ▶ Peu utilisée
- ▶ Partie réseau normale, partie machine à 255
  - ▶ Généralement l'adresse de broadcast mise en œuvre
    - ▶ Exemples :
      - ▶ 192.168.100.255
      - ▶ 172.16.255.255
  - ▶ Partie réseau normale, partie machine à 0
  - ▶ Ancienne adresse de broadcast pouvant encore être utilisées sur des machines SUN dont l'OS est SUNOS-4

- ▶ Les réseaux avec un netmask standard
  - ▶ On indique les 4 octets (entre 0 et 255), comme pour une adresse normale, les derniers octets étant à 0 (le dernier pour une classe C, les deux derniers pour ne classe B, les trois derniers pour ne classe A)
    - ▶ Exemple : 192.168.100.0
- ▶ Les réseaux «subnettés»
  - ▶ On fait figurer tous les octets (entre 0 et 255), y compris les bits de l'extension
    - ▶ Exemple : 192.168.100.32 (netmask 255.255.255.224 par exemple)
    - ▶ Voir page suivante

- ▶ Extension de la partie «Réseau» de l'adresse en empruntant quelques bits de poids forts de la partie machine
- ▶ Par exemple 255.255.255.224 pour une classe C
  - ▶ Tout à 1 sauf la partie machine (224d = 1110 0000b)
- ▶ Le masque indique quels bits
- ▶ Permet de créer des «sous» réseaux
  - ▶ Les sous réseaux sont raccordés entre eux via des routeurs, comme des réseaux «normaux»
- ▶ Il y a toujours un netmask
  - ▶ Il est standard s'il ne comporte pas d'extension de bits par rapport à la classe d'adresses : 255.255.255.0 pour une classe C par exemple

- ▶ Les adresses sans classe
  - ▶ Concept CIDR (RFC-1519) : *Classless InterDomain Routing*
  - ▶ La frontière de l'adresse réseau n'est plus figée selon la loi des classes
  - ▶ Utile pour agréger des routes dans les tables de routage des routeurs
  - ▶ Utile pour les fournisseurs de service pour affecter un sous ensemble d'adresses à un client...
  - ▶ Le netmask doit être précisé avec les adresses
- ▶ Notation
  - ▶ Classique : 255.255.255.128 (25 bits de masque)
  - ▶ Notation CIDR : /25 : exemple 192.168.100.128/25

- ▶ «À la main»
  - ▶ Selon les outils offerts par le système d'exploitation
    - ▶ À l'aide d'interfaces graphiques d'administration
    - ▶ Via des commandes spécifiques
- ▶ Dynamiquement
  - ▶ Via le protocole DHCP (*Dynamic Host Control Protocol*)
    - ▶ Un serveur est configuré pour donner l'information
  - ▶ Sur connexion via liaison point à point et le protocole PPP (Point to Point Protocol). La machine à configurer contacte un serveur situé à l'autre extrémité de la liaison. Le serveur peut lui fournir son adresse

Le datagramme IP

Adressage

Les adresses IPv4

**Les adresses IPv6**

Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP

- ▶ Adresses sur 128 bits
- ▶ Notation hexa par bloc de 16 bits  
2001:db8:cafe:deca:0:0:0:1
- ▶ Compression de zéros  
2001:db8:cafe:deca::1

- ▶ Deux parties :
  - ▶ **préfixe** ou **identifiant de sous-réseau** (subnet ID) : partie gauche de l'adresse
  - ▶ **identifiant de machine** (host ID) : partie droite
- ▶ notation CIDR :
  - ▶ 2001:db8:cafe:deca:a9e:1ff:fe6b:25c9/64
  - ▶ subnet correspondant:  
2001:db8:cafe:deca::



- ▶ Préfixe de documentation 2001:db8::/32
- ▶ Préfixe link-local fe80::/10
- ▶ Préfixe multicast ff02::/10
- ▶ Exemple de préfixe «end-user»  
2001:db8:fada:ba00:/56

- ▶ Unicast  
2001:db8:cafe:deca:a9e:1ff:fe6b:25c9/64
- ▶ Link-local  
fe80::a9e:1ff:fe6b:25c9/64
- ▶ Notation IPv4  
2001:db8::cafe:192.168.0.1 égal à  
2001:db8::cafe:c0a8:1
- ▶ Localhost ::1
- ▶ Tout les bits à 0 ::

- ▶ Il est *normal* d'avoir plusieurs adresses IPv6 à une interface (adresse de portée *lien*, de portée *globale*)
- ▶ Configuration «à la main» : plutôt rare
- ▶ Dynamiquement
  - ▶ Auto-configuration, grâce au préfixe annoncé par le router
  - ▶ Via DHCPv6

Le datagramme IP

Adressage

**Protocole ARP / NDP**

Principe du routage

Les routeurs

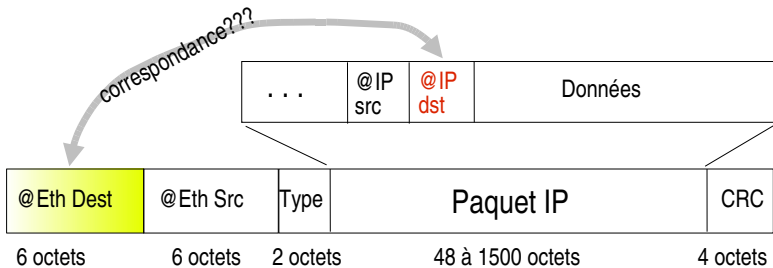
Gestion des erreurs avec ICMP

# Relation entre adresse IP et adresse MAC dans les réseaux locaux

29/51

- ▶ Concernent les machines reliées à un réseau local de type Ethernet ou 802.11
- ▶ Les adresse IP se gèrent
  - ▶ Elles sont affectées «à la main» via des outils spécifiques du système d'exploitation des machines (interfaces graphiques ou commandes telles que ifconfig sous Unix/Linux)
  - ▶ Elles peuvent être affectées automatiquement via le protocole DHCP, mais cette possibilité est configurée elle aussi à la main
- ▶ Les adresses MAC ne se gèrent pas
  - ▶ Elles sont préaffectées par le constructeur de la carte interface que l'on achète ou qui est fournie avec la machine
  - ▶ Parfois le pilote (drivers) de la carte permet que cette adresse puisse être modifiée (via ifconfig)

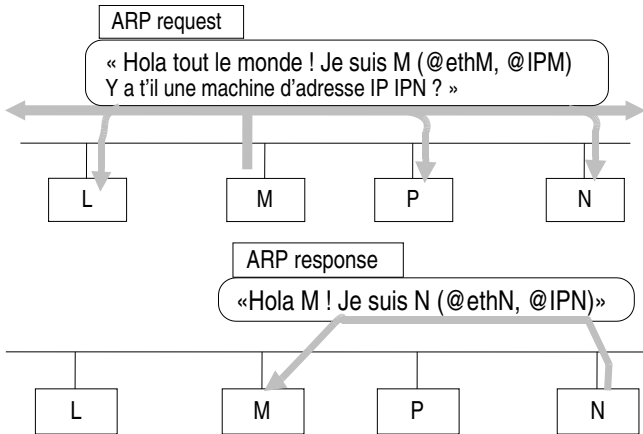
- ▶ Problème : une machine M doit émettre un paquet IP vers une machine N voisine dont on ne connaît que le numéro IP (sur le même LAN)
- ▶ Si on est sur Ethernet le paquet IP sera véhiculé par une trame telle que celle-ci



# Adresses MAC et adresses IP : la solution ARP (IPv4)

31/51

## ► Adress Resolution Protocol - rfc826



# Adresses MAC et adresses IP : Neighbor Discovery Protocol (IPv6)

32/51

- ▶ Neighbor Discovery Protocol (NDP)
- ▶ Intégré dans Internet Control Message Protocol version 6 (ICMPv6) – rfc4443
- ▶ Fonctionne de manière similaire à ARP (IPv4)



Le datagramme IP

Adressage

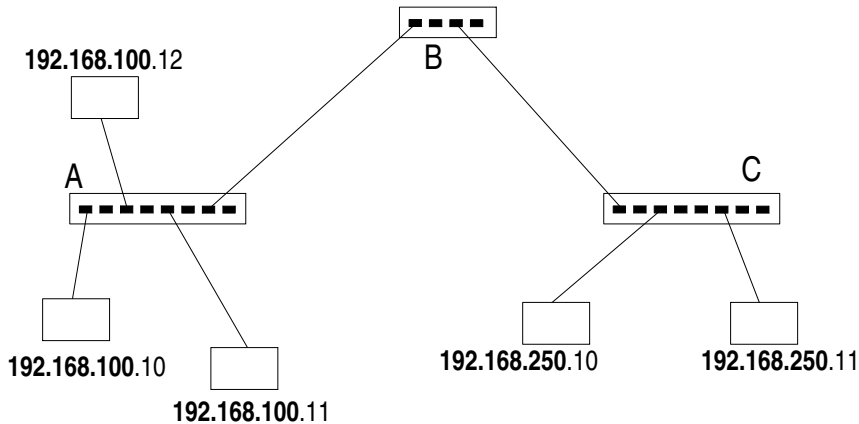
Protocole ARP / NDP

**Principe du routage**

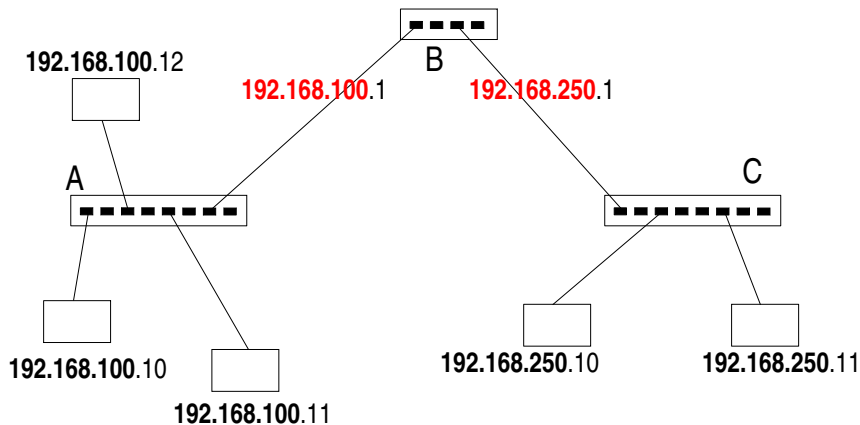
Les routeurs

Gestion des erreurs avec ICMP

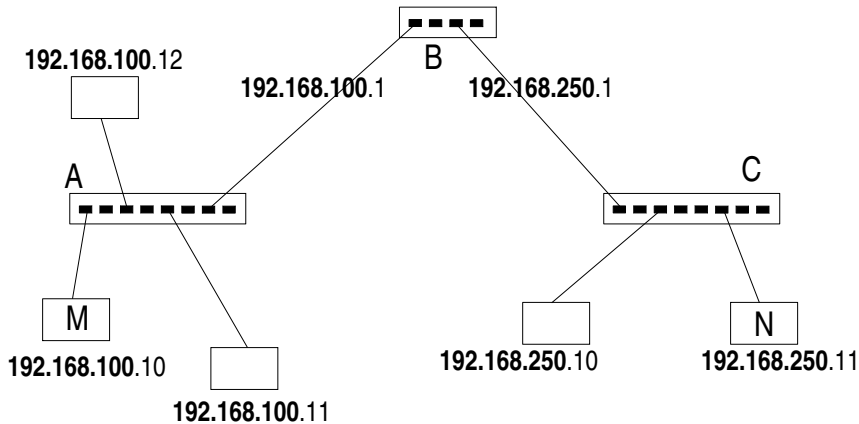
Quelle est la nature des organes A, B et C ?



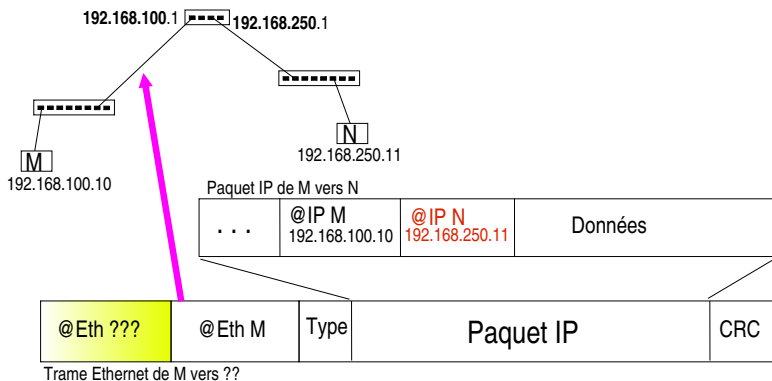
Alors...



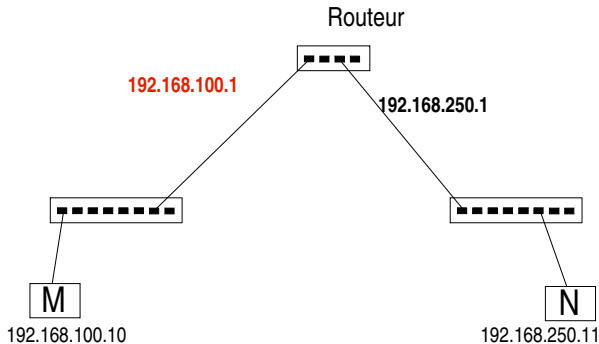
Comment envoyer un paquet de M vers N ?



En réseau local



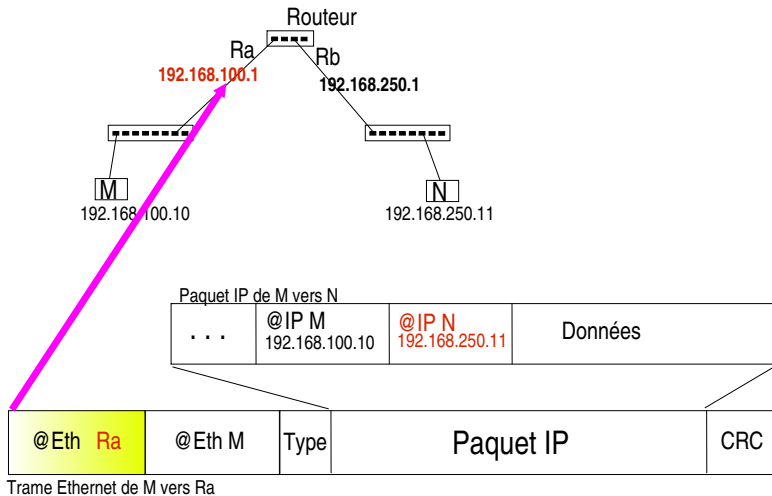
Comment, en M, déterminer l'adresse Mac de la trame Ethernet qui va emporter le paquet vers sa destination ?



En M il faut une **table de routage** qui dit : « pour aller en 192.168.250.11 passer par 192.168.100.1 »

À l'aide de cette table il sera facile de faire une résolution ARP pour trouver l'adresse MAC du routeur. L'adresse destination de la trame Ethernet sera celle du routeur

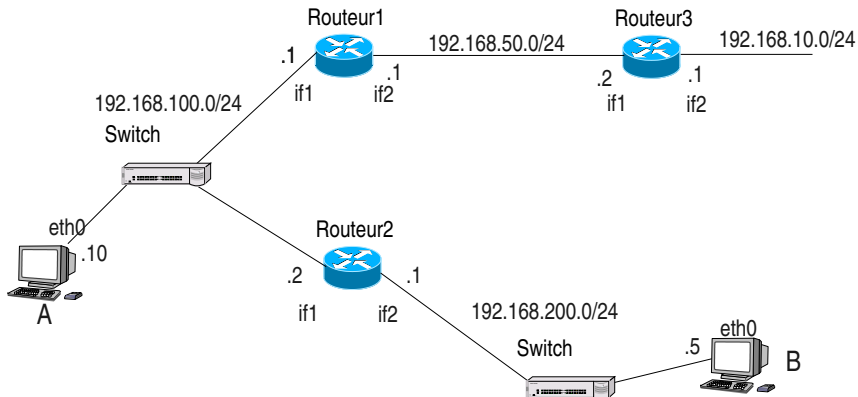
# Paquet IP de M vers N, et son porteur... II 39/51



Chaque «entrée» dans la table contient au moins

- ▶ Une direction (réseau ou machine)
- ▶ Une indication de route
  - ▶ machine par laquelle les paquets doivent être acheminés
    - ▶ Cette machine doit être accessible
  - ▶ interface locale
- ▶ Un coût
  - ▶ Notion de «distance» ou de «coût»
    - ▶ Nombre de sauts nécessaires
    - ▶ Débit
    - ▶ ...



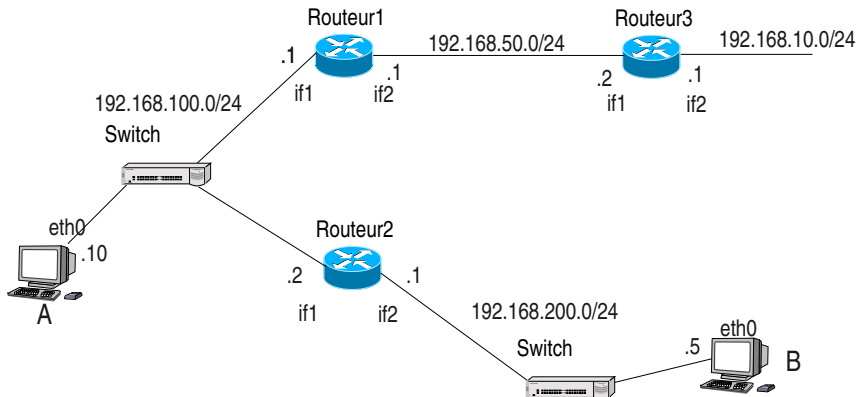


Légende :

`192.168.X.0/24` : adresse de réseau et netmask

`.x` (`.1` ou `.2`, etc.) : partie machine de l'adresse de l'interface

`if1`, `if2`, `eth0` : nom d'interface réseau sur la machine



Considérons les tables de routage correctement servies partout sauf en A  
A peut atteindre if1 de Routeur3 (192.168.50.2), mais pas if2 (192.168.10.1)  
Pourquoi **ne peut-on pas** dire en A : pour aller en 192.168.10.0/24 passer par 192.168.50.2 ? *Que faut-il dire ?*

# Exemple de table de routage sous Windows 43/51

```
C:\>route print
```

```
=====
```

Liste d'Interfaces

```
0x1 ..... MS TCP Loopback interface
```

```
0x1000003 ...00 01 02 6e 7c 46 ..... 3Com EtherLink PCI
```

```
=====
```

Itinéraires actifs:

Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique
0.0.0.0	0.0.0.0	192.44.75.1	192.44.75.184	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.44.75.0	255.255.255.0	192.44.75.184	192.44.75.184	1
192.44.75.184	255.255.255.255	127.0.0.1	127.0.0.1	1
192.44.75.255	255.255.255.255	192.44.75.184	192.44.75.184	1
224.0.0.0	224.0.0.0	192.44.75.184	192.44.75.184	1
255.255.255.255	255.255.255.255	192.44.75.184	192.44.75.184	1

Passerelle par défaut: 192.44.75.1

```
=====
```

## Quel est votre paramétrage ?

- ▶ Sous Windows (Ouvrez une fenêtre de commande et testez les commandes suivantes :)
  - ▶ `ipconfig` (`wipcfg` sous Windows 9x/ME) avec le sélecteur `/all`
  - ▶ `route print` pour afficher la table de routage
  - ▶ `nslookup` pour traduire des noms de machine en adresse IP et inversement
  - ▶ `arp -a` si vous êtes sur un LAN pour lire la table de traduction arp
  - ▶ `tracert`
- ▶ Sous Linux (Ouvrez un terminal et testez :)
  - ▶ `ifconfig` avec ou sans `-a`
  - ▶ `route` avec ou sans `-n`
  - ▶ `nslookup` ou `host`
  - ▶ `arp -a`
  - ▶ `traceroute` (avec ou sans `-n`)

Le datagramme IP

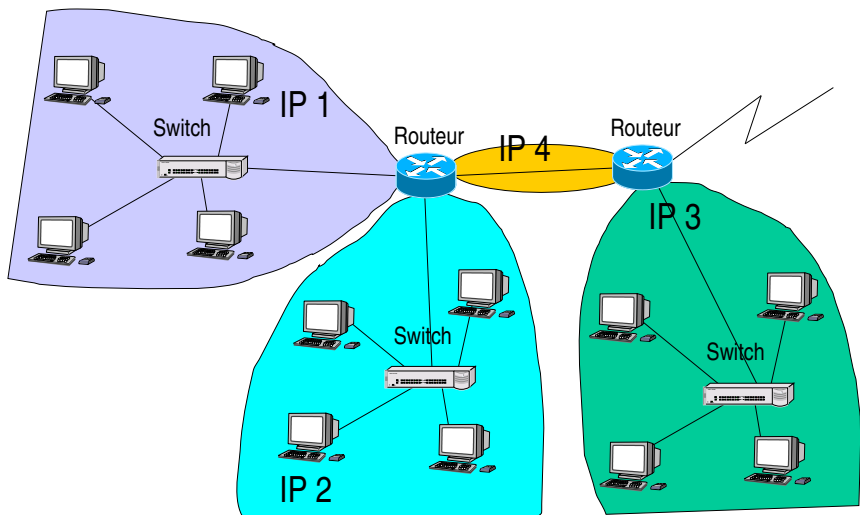
Adressage

Protocole ARP / NDP

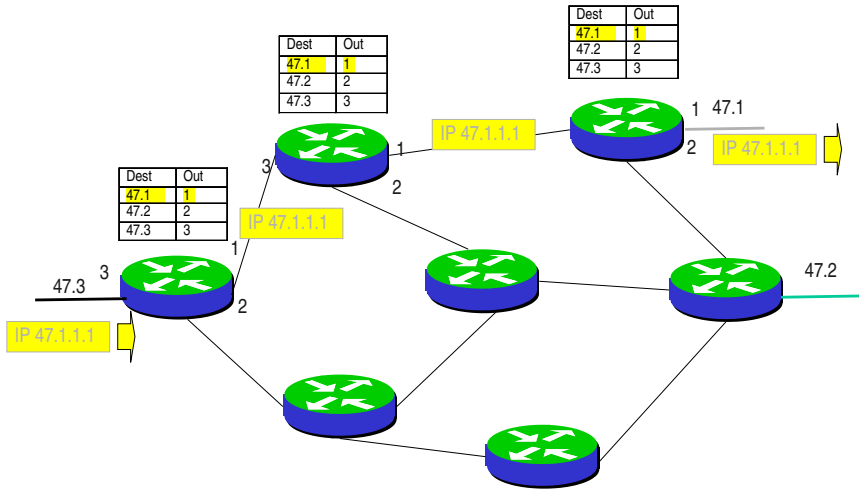
Principe du routage

**Les routeurs**

Gestion des erreurs avec ICMP



- ▶ Chaque paquet IP entrant dans le routeur voit son adresse destination examinée et comparée sur un certain nombre de bits avec le contenu d'une table (table de routage) associant des directions avec une interface de sortie
- ▶ Cette fonction est aussi mise en œuvre dans les machines terminales
- ▶ Le champ TTL est décrémenté par chaque routeur, le champ *checksum* doit être recalculé à chaque fois





Le datagramme IP

Adressage

Protocole ARP / NDP

Principe du routage

Les routeurs

Gestion des erreurs avec ICMP

## Internet Control Message Protocol (rfc 792)

- ▶ Sert à véhiculer des messages d'erreur ou de demande d'information
  - ▶ Demande d'écho et réponse (commande ping)
  - ▶ Destination non accessible
    - ▶ Le réseau ne peut être atteint
    - ▶ La fragmentation est nécessaire et le bit D est à 1 (PMTU discovery)
    - ▶ etc
  - ▶ Redirection, il existe une meilleure route
  - ▶ Durée de vie dépassé
  - ▶ etc

## Internet Control Message Protocol v6 (rfc 4443)

- ▶ Mêmes fonctions que ICMP (IPv4)
  - ▶ Erreurs diverses, ping, redirections, etc.
- ▶ En plus :
  - ▶ Neighbor Discovery Protocol (équivalent du ARP pour IPv4)
  - ▶ Router Solicitation, Router Advertisement :  
Auto-configuration de l'adresse. Au démarrage, un host recherche s'il y a un routeur présent sur LAN ; le routeur diffuse le préfixe IPv6 à utiliser ; le host se choisit une adresse dans ce préfixe.