IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

UE PRIP

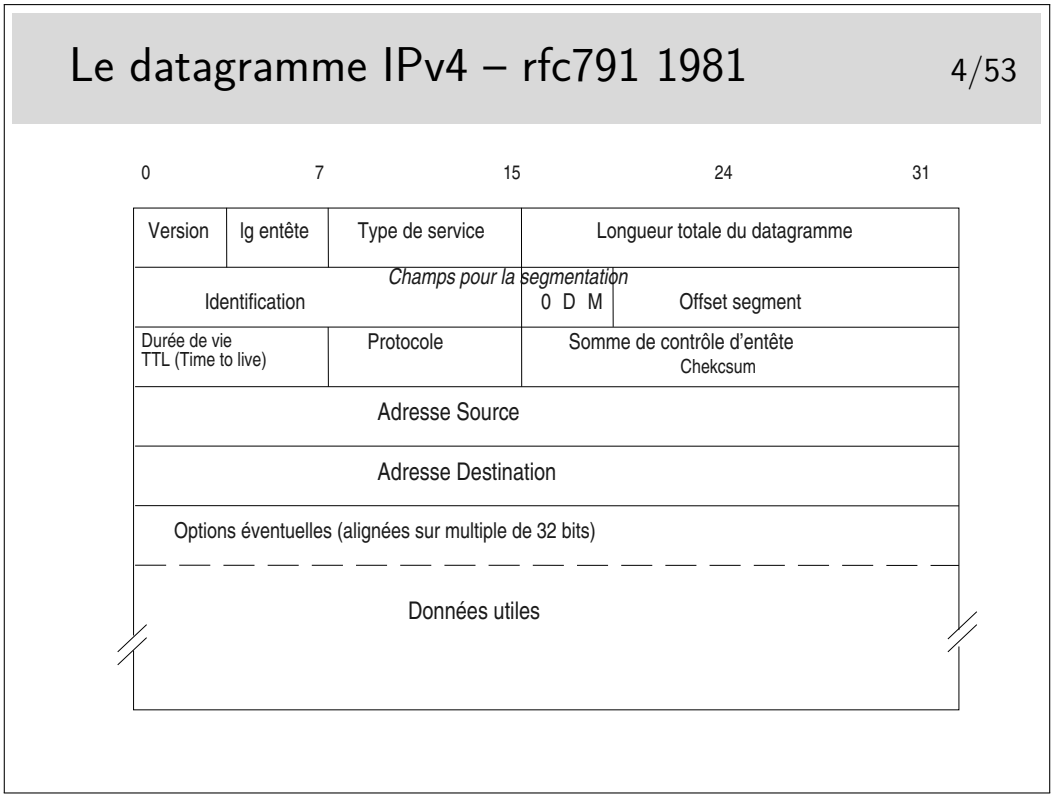
Principe des Réseaux Informatiques par la Pratique

La couche réseau

Automne 2023

1 Le datagramme IP

1.1 Le datagramme IPv4



Longueur d'entête : en nombre de mots de 32 bits ; si supérieur à 5, indique la présence d'options (40 octets max d'options : 10 mots max de 4 octets)

Type de service : peu utilisé par le passé, permet aujourd'hui, entre autres, de coder le DSCP (DiffServ Code Point). Voir pages suivantes.

Champs pour la segmentation : on recommande d'éviter la segmentation avec TCP. Elle n'existe plus que pour UDP si les unités de données fournies ont une taille supérieure au MTU de l'interface

bit D : *Don't fragment* : interdit la fragmentation du segment s'il est à 1

bit M : *More* : indique la présence de fragments complémentaires, si le segment d'origine a été fragmenté.

Si le champ Offset est à 0 ainsi que le bit M, le segment est celui d'origine

TTL : durée de vie ; décrémenté de 1 par chaque routeur. Si le résulat passe à 0, le datagramme est jeté et un message ICMP est envoyé à la machine émettrice

Protocole : indique le protocole supérieur véhiculé (TCP, UDP, ICMP voire même IP en cas d'encapsulation IP dans IP piour tunnelling)

Somme de contrôle d'entête : contient la somme des mots de 16 bits constituant l'entête. Permet à l'arrivée de vérifier l'intégrité de celle-ci. Si une erreur est détectée le datagramme est jeté sans autre forme d'action. On ne peut même pas envoyer un message d'erreur à l'émetteur car l'adresse source qui indique ce dernier peut être corrompue. Comme l'indique le nom de ce champ le contrôle d'intégrité n'est fait que sur l'entête.

Adresses : source et destination, sur 32 bits ; information fondamentale, au moins en ce qui concerne la destination car elle sert au routage.

Le champ Type de Service

5/53

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

Priorité (précédence)			Type de service				0
Par défaut à 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

111 - Network Control (protocole de type HELLO)

110 - Internetwork Control (protocoles de routage)

101 - CRITIC/ECP

100 - Flash Override

011 - Flash

010 - Immediate

001 - Priority

000 – Routine (priorité la plus faible)

RFC 791 et 795

Le champ Type de Service en version DiffServ

6/53

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

DiffServ signifie Différentiation de Service (en anglais aussi). C'est un mécanisme relativement récent permettant de marquer les paquets afin qu'ils soient traités de manière différentiée dans les routeurs. C'est un mécanisme de qualité de service.

Les options IPv4

7/53

- 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.

L'option LSR permet d'indiquer la route à suivre mais si un routeur intermédiaire ne sait pas comment utiliser une des indications contenue dans l'option, il peut alors utiliser sa table de routage normale.

L'option SSR est plus stricte car le paquet est rejeté si un routeur ne sait pas l'orienter vers une direction indiquée.

Il y a encore l'option Traceroute, obsolète car dangereuse, EEOL et NOP pour indiquer la

fin de la liste et du bourrage d'alignement sur 32 bits.

L'option RTALT est utilisée par IGMP et par RSVP, ces protocoles nécessitent des traitements particuliers dans les routeurs. Ces traitements sont effectués par des entités applicatives des routeurs. Ces derniers ne doivent donc pas effectuer le routage rapide des paquets munis de cette options mais ils doivent les diriger vers les entités applicatives.

`http://www.iana.org/assignments/ip-parameters`

1.2 Le datagramme IPv6

Le datagramme IPv6 – rfc8200 I

9/53

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Payload...                           |
```

Première standardisation de IPv6 : rfc1883 en 1995, mis à jour par le rfc2460 en 1998, lui-même remplacé par le rfc8200 de 2017, à priori bien stabilisé maintenant et qui intègre toutes les réajustement qui ont été discutés toutes ces années.

Le datagramme IPv6 II

- 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 !)

Next Header

- 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       |
+---------------+----------------+-----------------+-----------------
```

2 Adressage

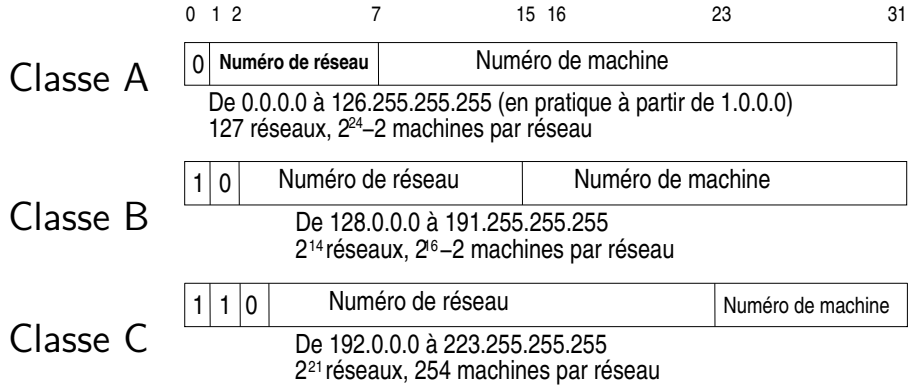
2.1 Structuration machines / réseau

Structuration machines / réseau 14/53

- Besoin : tables de routages compactes
- Structurer-aggréger les adresses pour repérer les destinations qui sont dans le même “endroit” du réseau
- Comme sur une adresse postale : pays / ville / rue / maison
- Solution : spécifier sur une addresse IP quelle partie désigne un numéro de réseau, et quelle partie désigne un numéro de machine dans ce réseau

2.2 Les adresses IPv4

Les classes historiques d’adresses IPv4 I 16/53



- Note : concept facile à comprendre mais obsolète depuis 1992, cf CIDR plus loin

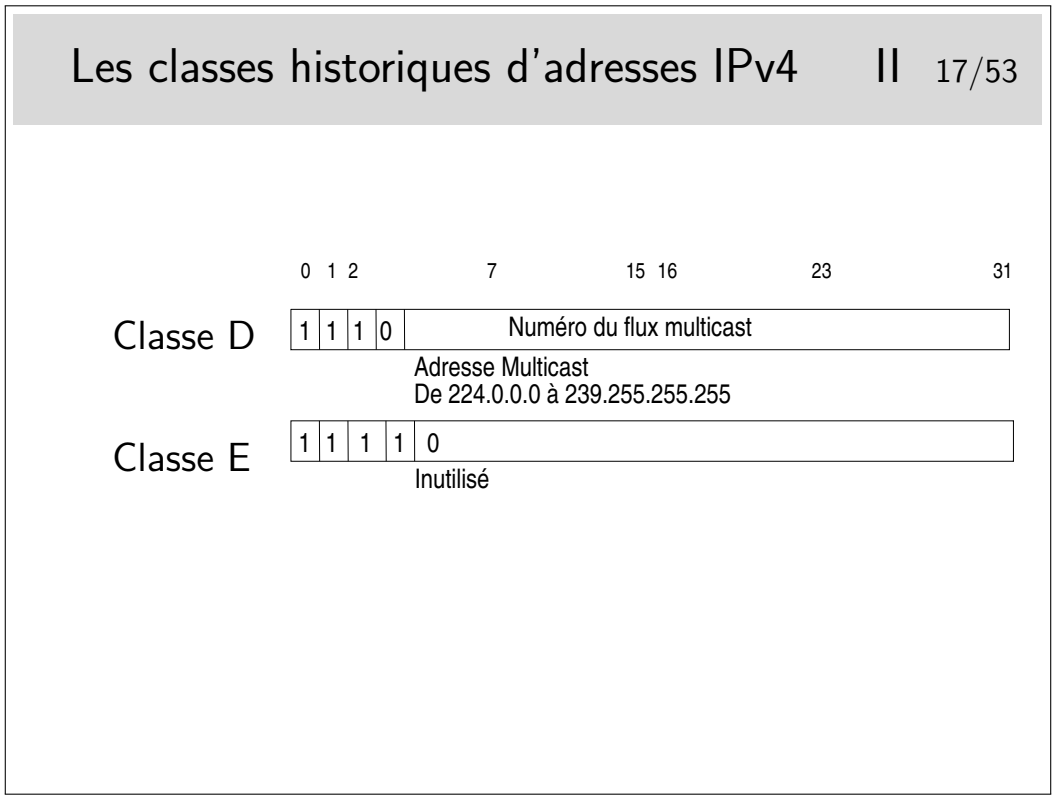
Une interface IP doit être munie d’une adresse pour pouvoir fonctionner. En général, pour des machines de bureau standard en réseau local, l’interface IP correspond à une carte réseau

de type Ethernet.

L'interface IP peut aussi être correspondre à une couche complètement logicielle, c'est le cas des interfaces de niveau 2 réalisées avec le protocole PPP qui s'interpose entre IP et une interface physique comme un port série ou un port USB relié à un modem ADSL (l'empilement des couches protocolaires est alors très complexe).

Une interface matérielle peut être munie de plusieurs adresses IP, sous Unix et Linux en particulier. On a alors, par exemple, les interfaces eth0:0, eth0:1, eth0:2, etc.

A noter que les adresses de classe A de la gamme 0.0.0.0 à 0.255.255.255 ne peuvent pas être utilisées, bien qu'elles ne correspondent pas à une fonction particulière.



Le multicast...

Permet d'envoyer des paquets IP à un certain nombre de machines mais pas à toutes. Des machines sur le réseau peuvent être sources de trafic multicast, elles peuvent émette par exemple à l'adresse 224.5.6.7. Il suffit que d'autres machines soient «au courant» de ce fait pour se mettre en écoute en lançant une application spécifique. Cette application demande explicitement à écouter le flux en envoyant un message du protocole IGMP (RFC-3376 pour la version 3) vers l'Internet. Ce message est relayé par les routeurs vers les sources, chaque routeur rencontré s'insère alors dans un arbre de diffusion multicast (préalablement configuré). Les paquets du flux applicatif peuvent arriver ainsi aux récepteurs ayant fait la requête.

Il faut que les routeurs soient configurés, ce n'est pas automatique.

Il existe un réseau mondial multicast, appelé le MBONE. Les sources potentielles diffusent des annonces de session à l'adresse SAP.MCAST.NET (224.2.127.254) (en UDP, port 9875).

L'outil sdr (pour unix/linux ou windows) permet d'écouter ce flux et afficher les informations de sessions.

(mot clé MBONE ; un lien : `http://www-itg.lbl.gov/mbone/`)

Les adresses particulières

18/53

- 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

La fonction de NAT est mise en œuvre dans un routeur muni d'une interface configurée avec une adresse officielle (pouvant donc être routée dans l'Internet). Les paquets sortant sont modifiés, le champ «adresse source» est remplacé par l'adresse officielle de l'interface de sortie du routeur. Ce dernier mémorise l'opération pour effectuer la modification inverse pour les paquets en retour.

Des extensions du concept peuvent affecter aussi les ports TCP ou UDP.

Le mécanisme pose un problème pour les protocoles tels que ftp. En effet, ftp demande la création d'une connexion «entrante» pour réaliser les transferts de fichiers, les paquets de demande de connexion doivent être corrélés avec la connexion sortante existante. Les traitements sont alors plus complexes que pour les connexions simples comme celle pour le Web par exemple). Ces concepts demandent de comprendre ce qu'est une connexion au niveau supérieur (il n'y a pas de connexion IP). Ce point sera abordé plus loin dans le chapitre sur TCP.

Sous linux, les mécanismes de translation d'adresse sont directement intégrés au noyau. Une commande permet d'en paramétrer les caractéristiques, il s'agit de iptables qui peut bien plus encore en ce qui concerne les opérations de filtrage pour la sécurité.

Les adresses particulières pour la diffusion

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 adresses de réseaux

- 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

Le *subnetting*

21/53

- 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 lasse C par exemple

Avec le masque 255.255.255.224 on prend 3 bits de la partie machine. On pourra créer 8 sous réseaux à partir du numéro 192.168.100.0 :

— `192.168.100.0`
— `192.168.100.32`
— `192.168.100.64`
— `192.168.100.96`
— `192.168.100.128`
— `192.168.100.160`
— `192.168.100.192`
— `192.168.100.224`

Question : à quel sous réseau appartient la machine de numéro `192.168.100.72` ?

Le netmask général et ses notations

22/53

- 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

Dans le dernier exemple, l'adresse donnée est une adresse de réseau et non une adresse de machine. Avec une telle adresse (et son masque) on pourra adresser deux fois 128-2 machines : de 192.168.100.1 à 192.168.100.126 (broadcast 192.168.100.127) et de 192.168.100.129 à 192.168.100.254 (broadcast 192.168.100.255).

La notation classique (255.255...) reste très répandue. La notation CIDR peut se rencontrer sous quelques Unix (BSD, Linux, ???), elles est plus commode d'utilisation.

Affectation d'adresse à une interface IP

23/53

- «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 protocole PPP est utilisé par exemple dans les connexions aux fournisseurs de service IP via des modems et le réseaux téléphonique général.

Dans les connexions via ADSL, c'est aussi PPP qui est utilisé pour affecter l'adresse à la

machine qui se connecte mais le mécanisme est beaucoup plus complexe.

Le protocole DHCP permet de fournir une adresse IP, le netmask associé, le routeur par défaut pour l'interface en cours de configuration, le nom de domaine DNS ainsi que le ou les serveurs DNS. Tout ceci pour une période de temps configurée par le gestionnaire du serveur DNS. Les clients doivent renouveler leur demande d'adresse à la fin du temps alloué.

2.3 Les adresses IPv6

Adresses IPv6 – RFC 4291

25/53

- 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`

Sous-réseaux

26/53

- 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::`

Exemples de préfixes

27/53

- 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`

Exemples d'adresses

28/53

- 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 `::`

Affectation d'adresses à une interface IP

29/53

- 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

3 Protocole ARP / NDP

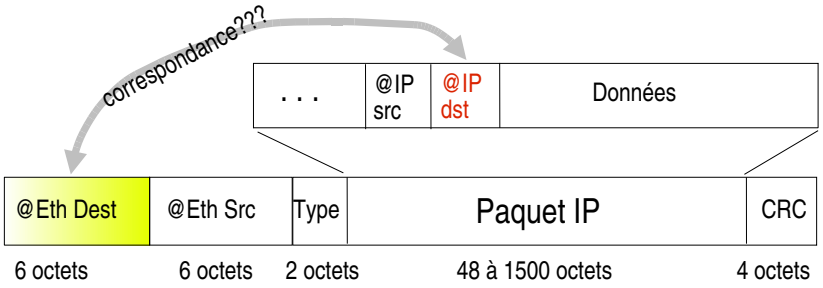
Relation entre adresse IP et adresse MAC dans les réseaux locaux

31/53

- 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)

...Adresses MAC et adresses IP... 32/53

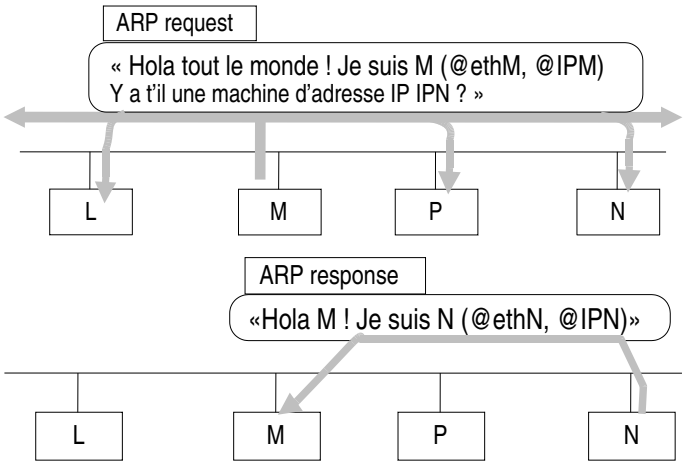
- Problème : une machine M doit émettre un paquet IP vers une machine N voisine dont on ne connaît que le numéro IP (sur le même LAN)
- Si on est sur Ethernet le paquet IP sera véhiculé par une trame telle que celle-ci



Comment la machine M peut elle retrouver l'adresse Ethernet de la machine N en ne connaissant que l'adresse IP de N ?

Adresses MAC et adresses IP : la solution ARP (IPv4) 33/53

- Adress Resolution Protocol - rfc826



Soyez curieux : la commande `arp`

Sur un réseau local, sous Windows ou Unix/Linux, ouvrez une fenêtre de commande et tapez : `arp -a` pour voir la table de résolution arp instantanée. Si vous ne voyez pas la machine de votre voisin et que vous connaissez son adresse IP (ou son nom), faites un «ping» dessus : ping 192.168.100.5 par exemple.

Si la réponse du ping est positive, refaites alors immédiatement `arp -a`, vous verrez apparaître la résolution concernant la machine voisine.

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

34/53

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

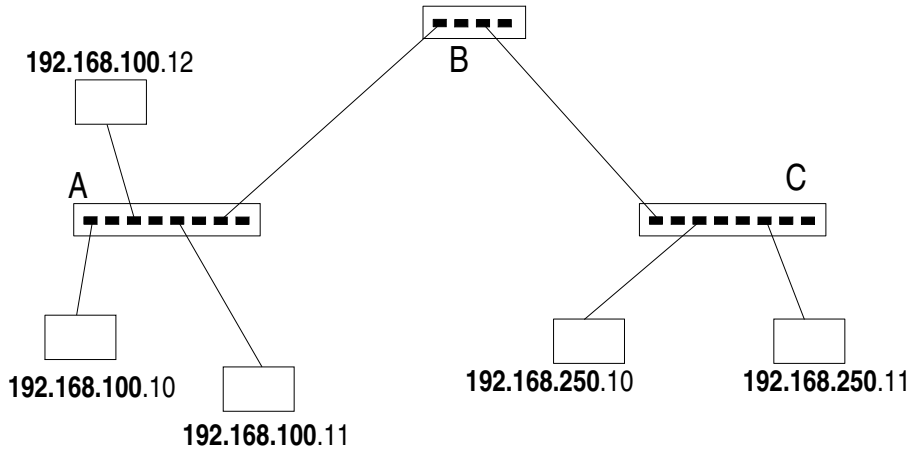
Soyez curieux : la commande `ip neigh`

4 Principe du routage

Question...

36/53

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



Vous avez le choix entre trois types d'organes :

— des hubs,

— des switches ou commutateurs ou pont multiports

— des routeurs

Aide technique : le netmask est standard pour la classe d'adresses IP utilisée...

Et cette classe est la classe ?????....

???

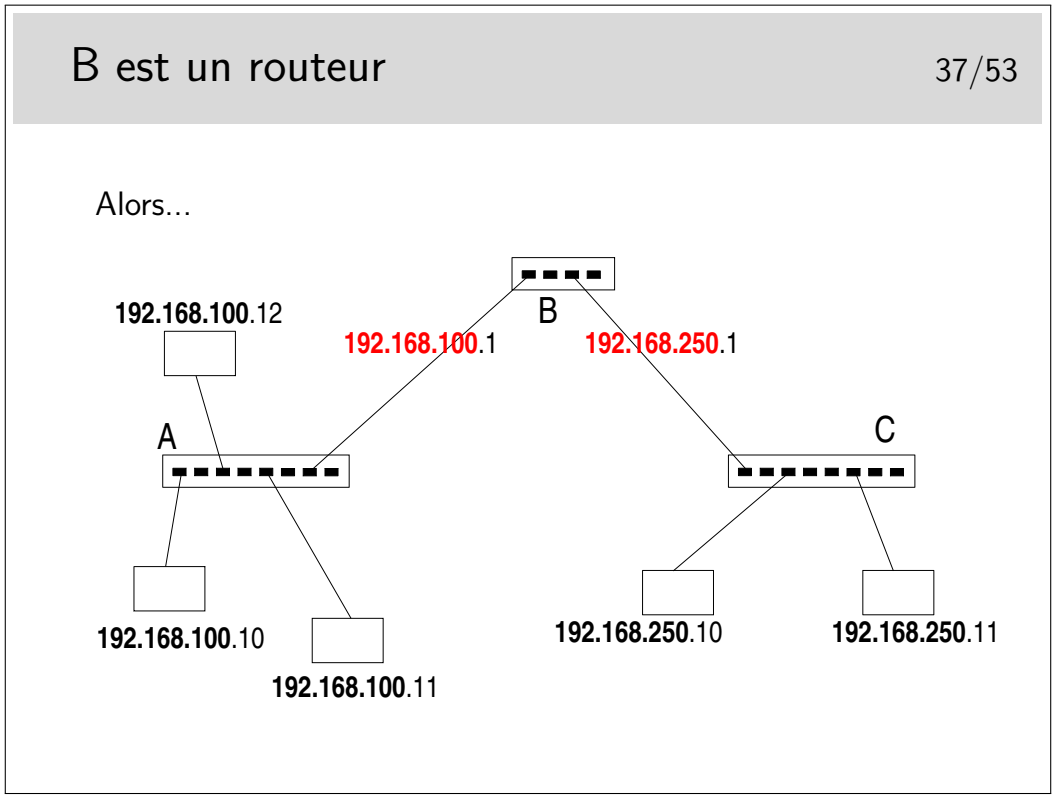
???

...C !

Ce sont des adresses de classe C...

Or les parties «Réseau» ne sont pas identiques entre la partie droite du schéma et la partie gauche...

Donc... Il ne s'agit pas de mêmes «Réseaux». Donc, forcément B est un... et A et C sont des ... ou des ...



Réponse à la question... A et B sont des hubs ou des commutateurs (ou switches ou ponts multiports). Même si fondamentalement les fonctionnalités des hubs et des commutateurs sont différentes (hubs : répéteurs, organes physiques, niveau 1 ISO – switches : niveau 2 ISO) on ne peut pas faire la différence sur le schéma.

B est un routeur. Il raccorde des réseaux dont les machines sont identifiées par des numéros IP de classe C dont la partie réseau est différente. Il raccorde dont des réseaux. Il fonctionne au niveau 3 ISO.

B est un routeur, donc chacun de ses ports est identifié par une adresse IP dont la partie réseau identifie le réseau auquel ce port est raccordé.

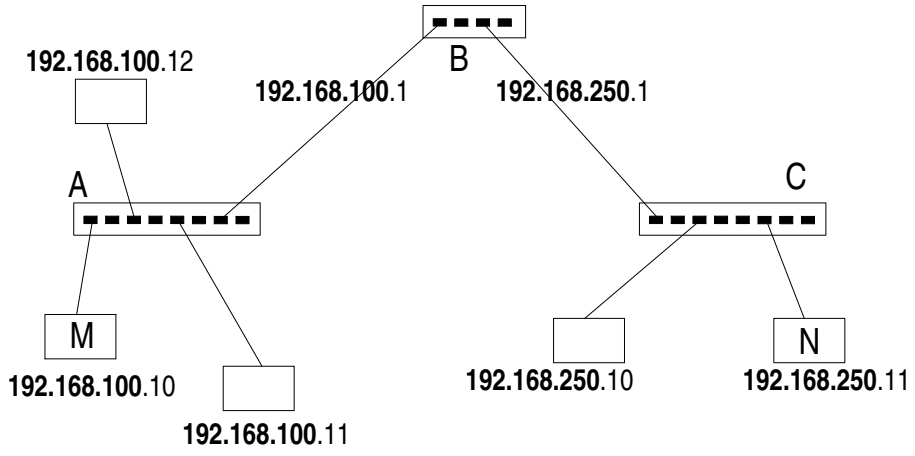
Le premier port de B est raccordé sur le réseau 192.168.100.0, on lui donnera donc une adresse libre de ce réseau (ici .1). Un autre port est sur le réseau 192.168.250.0, on lui donnera par exemple l'adresse .1 sur ce réseau.

Ce n'est pas pour faire joli, c'est vraiment fonctionnel. Si on ne le fait pas le réseau ne peut pas fonctionner.

Routage IP en réseau local

38/53

Comment envoyer un paquet de M vers N ?



Rien n'est magique... L'application sur M qui désire envoyer un message à une application sur N doit savoir que N existe. Sur M on doit connaître l'adresse IP de N.

On doit aussi savoir par où on passe. En M on doit savoir que pour atteindre N il faut passer par le routeur B.

Mais B est identifié par deux adresses IP !!!

En M, nous sommes sur un réseau local, nous ne pouvons atteindre que des machines se trouvant sur le même réseau local que nous. Nous ne pouvons donc atteindre le routeur que par son port qui est situé sur le même réseau physique, celui identifié par le préfixe IP 192.168.100.

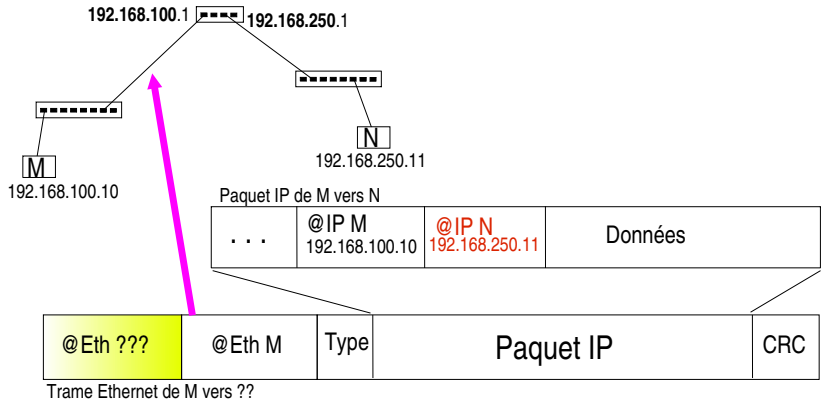
...Comment faire ?...

À suivre...

Paquet IP de M vers N, et son porteur... I

39/53

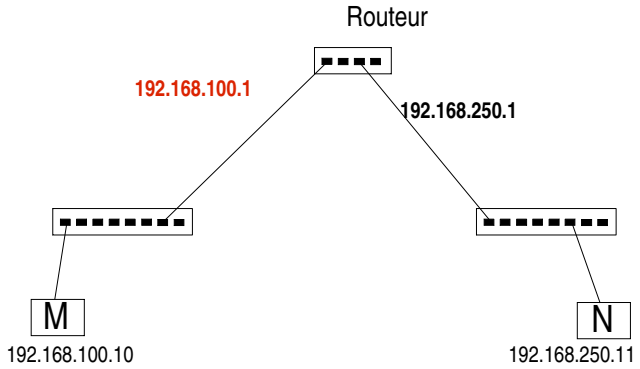
En réseau local



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

Table de routage I

40/53

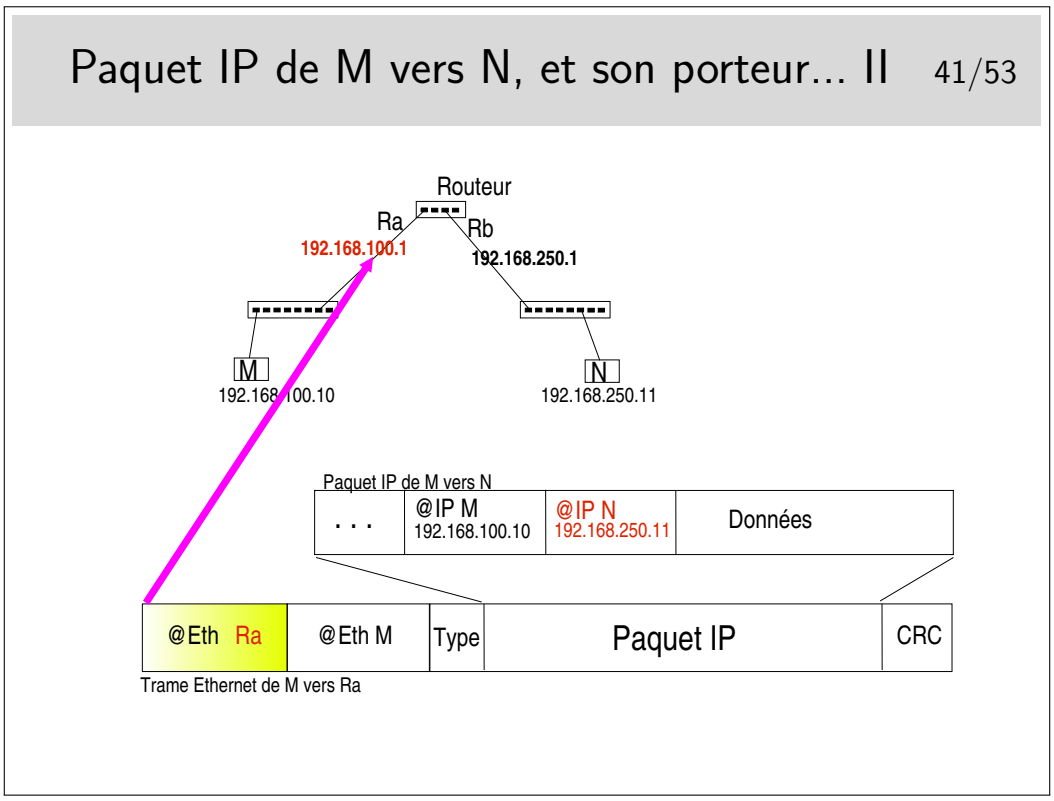


En M il faut une table de routage qui dit : « pour aller en 192.168.250.11 passer par 192.168.100.1 »
À l'aide de cette table il sera facile de faire une résolution ARP pour trouver l'adresse MAC du routeur. L'adresse destination de la trame Ethernet sera celle du routeur

Il faut une table de routage en M. Donc dans la machine terminale !!!

Chaque machine, quelle soit terminale ou intermédiaire, travaillant en IP incorpore des fonctions de routage.

Cela ne signifie pas que chaque machine terminale soit un routeur... Pour qu'une machine puisse joue le rôle de routeur il faut qu'elle possède au moins deux interfaces munies d'adresses IP (autres que 127.0.0.1, correspondant à l'interface boucle locale) et que son module IP soit autorisé à effectuer la fonction de relayage (forwarding).



Quand on disait qu'affecter une adresse à chaque interface de routeur n'était pas un effet de cosmétique...

Si en M on ne connaît pas l'adresse IP de l'interface du routeur qui est du même coté que M (sur le même réseau) alors la résolution ARP ne peut se faire.

Il ne suffit pas que l'interface du routeur et M soient «du même coté», il faut aussi qu'ils soient sur le même réseau local pour que ARP fonctionne (on rappelle que la requête ARP est transmise par broadcast Ethernet et que ce type de message ne passe pas les routeurs).

Ici la notion de réseau local est celle qui a été vue dans la partie précédente du cours, à savoir un réseau où la diffusion est possible vers toutes les machines. Ce pourrait être un VLAN car ce type de topologie définit des domaines de broadcast.

Lorsque des machines sont reliées entre-elles via des liaison point-à-point, il n'y a pas de résolution ARP.

Table de routage II

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
    - ...

Les directions sont spécifiées par des numéros de réseaux indiqués sur 4 octets et accompagnés de leur netmask, par exemple 192.168.10.0 255.255.255.0, ou en notation CIDR 192.168.10.0/24.

Une direction peut être une machine, dans ce cas l'adresse IP de la machine est indiqué directement et le netmask vaut 255.255.255.255.

Les indications de route peuvent être données en indiquant l'adresse IP du routeur par lequel il faut envoyer les paquets pour la direction correspondante. Plus précisément il s'agit de l'adresse IP de l'interface du routeur immédiatement accessible. C'est absolument obligatoire dans le cas ou l'interface du routeur en question est sur un réseau local classique.

Dans le cas ou l'interface du routeur est sur une liaison point-à-point, on peut ne donner que le nom de l'interface locale. Voir transparent suivant.

Le coût correspond à la notion de «plus court chemin». Moins le coût est grand meilleur semble le chemin (ce n'est pas toujours vrai, un chemin peut être plus court en vraie distance (moins de sauts par exemple) et cependant moins efficace en débit).

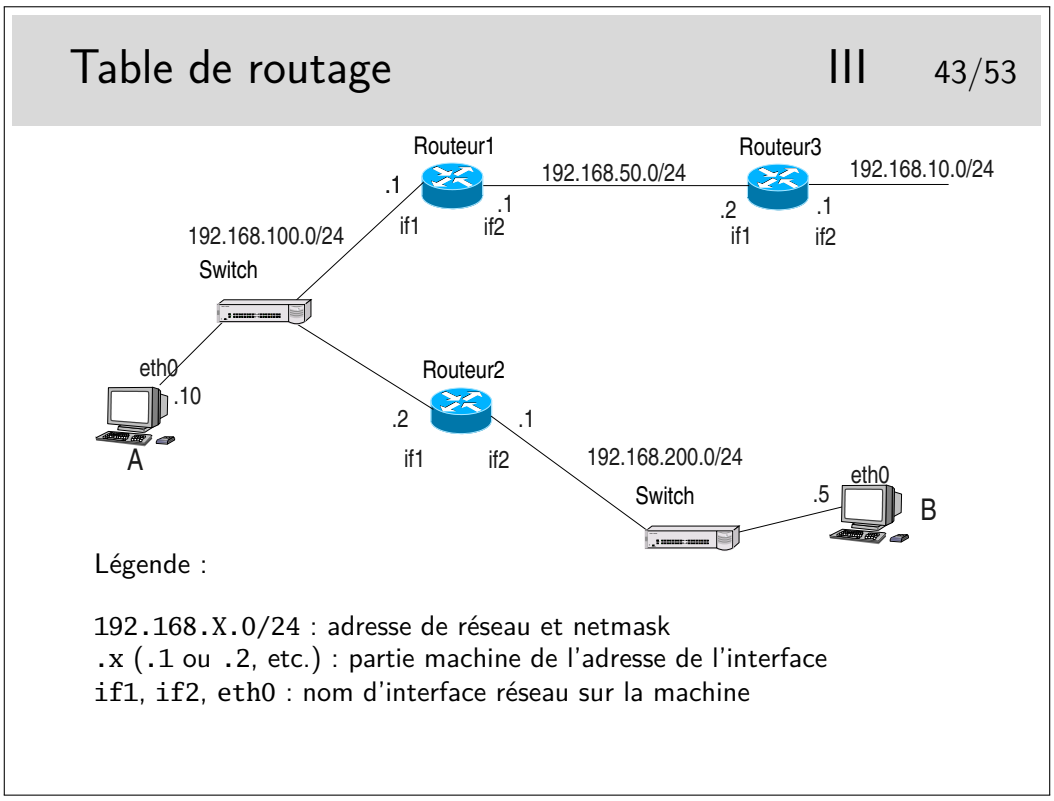


Table de routage en A

direction	netmask	gateway	interface
192.168.100.0	255.255.255.0	192.168.100.10	eth0
192.168.200.0	255.255.255.0	192.168.100.2	eth0
default	0.0.0.0	192.168.100.1	eth0

Rq : ici la mention de l'interface n'est pas très importante, elle est redondante car il n'y a qu'une seule interface physique (il y a quand même l'interface boucle locale qu'on n'a pas fait figurer dans la table de routage, mais qui exite et provoque des entrées spécifiques dans la table)

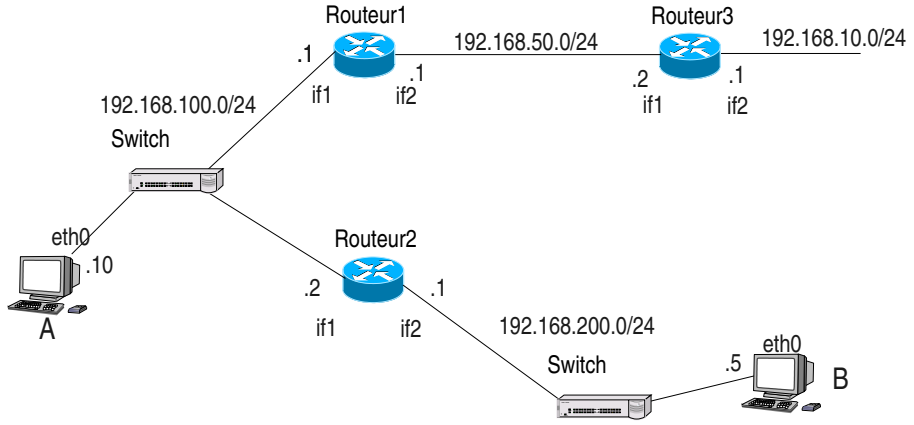
Table de routage en Routeur1

direction	netmask	gateway	interface
192.168.50.0	255.255.255.0	192.168.50.1	if2
192.168.100.0	255.255.255.0	192.168.100.1	if1
192.168.200.0	255.255.255.0	192.168.100.2	if1
default	0.0.0.0	192.168.50.2	if2

Rq : dans la ligne par défaut, la seule mention de l'interface suffirait car le lien entre les routeurs 1 et 2 est de type point-à-point.

Compléter pour le routeur 2 et la machine B...

Table de routage IV 44/53



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 ?*

On suppose la table de routage en A partiellement remplie. L'interface if1 du routeur2 est accessible, une commande ping, depuis A, vers l'adresse de cette interface fonctionne. Donc on peut supposer (et on a raison) que cette interface est «visible» depuis A. Cependant si on tente de créer en A une route via cette interface la commande doit échouer. Pourquoi ?

Exemple de table de routage sous Windows 45/53

```
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
===========================================================
```

Quelle est le numéro de l'interface de boucle locale (interface interne non raccordée à un réseau physique) ?

Quelle sont les adresses de broadcast possibles ?

Par quelle interface sont acheminés les paquets de broadcast ?

Que pouvez vous déduire de tout ceci concernant l'adresse de la machine en question ?

Que se passe-t'il si une application de cette machine envoie un paquet IP vers une autre application de la même machine ? Quel chemin est emprunté par le paquet ?

Quelle adresse code la destination par défaut ?

Et votre système dans tout ça... 46/53

Quel est votre paramétrage ?

- Sous Windows (Ouvrez une fenêtre de commande et testez les commandes suivantes:)
  - `ipconfig` (`winipcfg` 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`)

Et n'oubliez pas la commande ping... C'est la première commande à utiliser quand le réseau ne va pas très bien... «Mon voisin est-il joignable ? Alors :

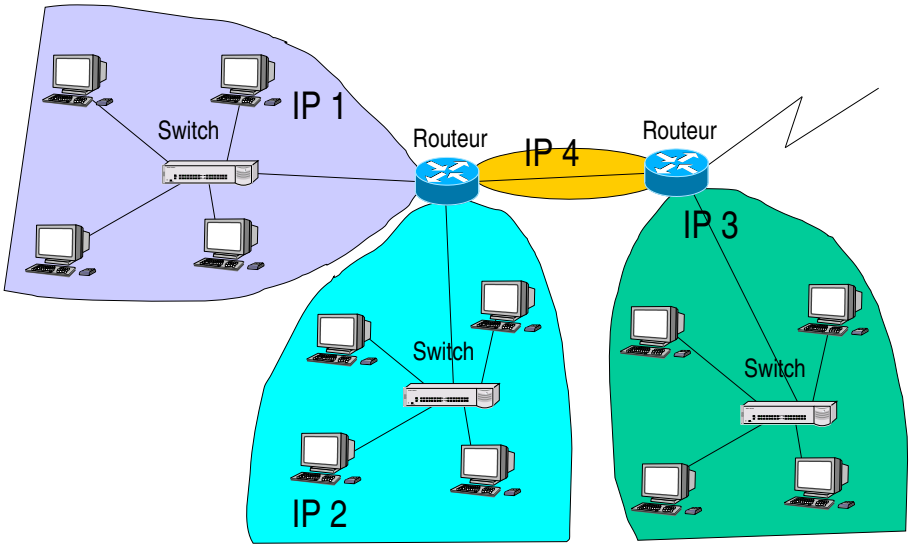
`ping mon_voisin` (plutôt `adresse_IP_de_mon_voisin`)

Note : Vous remarquerez peut être que Windows affiche plus de routes que Linux. En fait Linux gère plusieurs tables de routage et a pour habitude de n'afficher que la table `main`, sauf si on lui demande gentiment. (Pour avoir la liste des tables de routage : `cat /etc/iproute2/rt_tables` ; pour afficher la table principale : `ip route show table main` ; pour afficher la table avec les règles pour le multicast et le broadcast : `ip route show table local` ; etc.)

5 Les routeurs

Le réseau IP de l'entreprise

48/53



Ce que l'on va appeler le «réseau local» de l'entreprise est en réalité un réseau de niveau 3 composé de routeurs interconnectant des réseaux locaux séparés physiquement ou logiquement (VLANs).

L'adressage pourra être de type «privé», avec une seule adresse officielle en sortie et une fonction de type NAT dans le routeur de sortie.

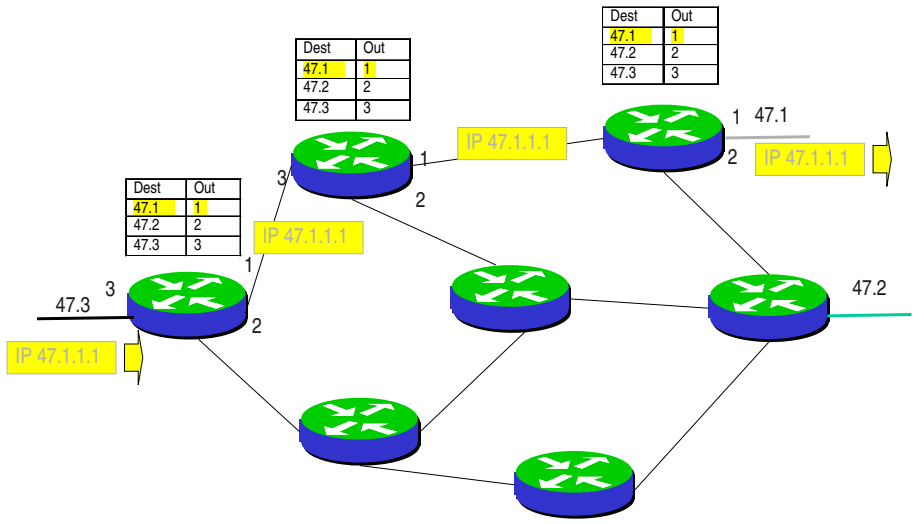
Fonctions des routeurs

49/53

- 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 *cheksum* doit être recalculé à chaque fois

Acheminement bond par bond

50/53



6 Gestion des erreurs avec ICMP

Le protocole ICMP (IPv4)

52/53

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

La commande `ping` n'utilise que ICMP (porté par IP).

La commande `traceroute` (`tracert` sous Windows) joue sur le dépassement de la durée de vie. Un premier paquet est créé «à la main» et son champ ttl est mis à 1. Il contient un paquet UDP à destination d'un port inconnu. Le paquet est routé, il atteint le premier routeur qui décrémente alors le ttl. Le résultat valant 0 le paquet est jeté et un message ICMP est émis

vers la source du paquet jeté. Le message est véhiculé par un paquet IP comportant l'adresse du routeur, ce qu'on attend dans traceroute. On peut alors afficher l'identité de ce routeur ainsi que le temps mesuré entre l'envoi du paquet initial et le l'arrivée du message ICMP. On fait cela trois fois pour avoir une estimation du temps moyen d'aller et retour puis on recommence en mettant cette fois le ttl à 2.

Le protocole ICMPv6 (IPv6)

53/53

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.