# 4. La couche réseaux

- BUT :
  - La couche réseaux se charge d'acheminer des paquets tout au long d'un parcours, d'une source jusqu'à un destinataire.
  - Gère le trafic à travers les nœuds de communication intermédiaire.

# Fonctions principales

Pour acheminer un paquet d'un émetteur vers un destinataire, il est impératif de connaître précisément la localisation de l'émetteur et du destinataire.
Pour ce faire, la couche réseau introduit la notion d'***adressage***.

## Fonctions principales

Une fois la destination connue, il faut déterminer le chemin à parcourir pour s'y rendre.

La couche réseau introduit donc la notion de ***routage***.

Le routage est le choix du meilleur chemin à prendre pour aller à la destination.

## Fonctions principales

Le réseau global peut être vu comme un réseau routier. Par conséquent, il est sensible aux mêmes problèmes d'embouteillages.

La couche réseau assure le ***contrôle de flux*** et le ***contrôle de congestion*** pour limiter les dégâts de ces embouteillages.

## Le service à la couche transport

Les service offerts à la couche 4 doivent respecter les objectifs suivants :

- les services doivent être indépendants des technologies de routeur mises en œuvre sur le sous-réseau
- la couche réseau doit être indépendante du nombre et du type des routeurs, ainsi que de la topologie du réseau
- les adresses de réseau mises à la disposition de la couche transport doivent faire partie d'un plan de numérotation qui doit rester uniforme.

## Le service à la couche transport

Compte tenu de ces critères, les concepteurs de la couche réseaux avaient ***beaucoup de liberté*** pour rédiger les spécifications.

Cette liberté donna lieu à d'assez grandes ***divergences*** :

- certains voulaient un service orienté connexion pour assurer une certaine qualité de service
- d'autres voulaient un service sans connexion, argumentant le fait que c'est aux stations d'assurer le service de connexion

## Service sans connexion

- Dans ce mode, les paquets sont injectés dans le sous-réseau ***individuellement***, et routés ***indépendamment*** les uns des autres.
- Dans ce contexte les paquets sont souvent appelés ***datagrammes***
- Il est possible que les paquets n'arrivent pas dans l'ordre initialement émis ou n'arrive pas du tout

## Service avec connexion

- Un chemin doit être établi au préalable du routeur source jusqu'au routeur de destination avant que les paquets ne soient envoyés
- Cette connexion est appelée ***Circuit Virtuel***
- Il n'est dès lors plus nécessaire de prendre une décision de routage pour chaque paquet

## Couche réseau dans Internet

- 10 principes fondamentaux sont décrits dans la RFC 1958.
  1. s'assurer que tout fonctionne
  2. privilégier la simplicité
  3. faire des choix
  4. exploiter la modularité (faite des couches)
  5. anticiper l'hétérogénéité (plus c'est grand, plus il y a des éléments différents qui composent)
  6. éviter les options et les paramètres statiques

## Couche réseau dans Internet

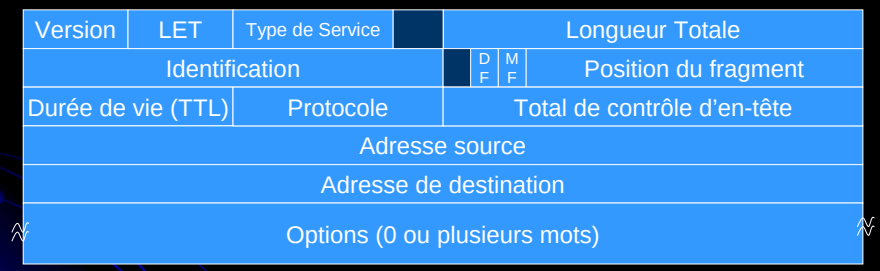
7. rechercher une conception efficace, mais pas parfaite
8. être sévère lors de l'envoi et tolérant lors de la réception
9. penser à l'évolutivité
10. considérer les performances et les coûts

# IP - Plan

- Le format de datagramme IP
- L'adressage
- La fonction de routage

# IP – Le format de datagramme

- Entête :



## Vocabulaire

- ***Little endian*** = lecture des informations de droite à gauche, soit le bit de poids faible en premier
  Exemple : un octet 10100111
  est transmis 11100101
- ***Big endian*** = lecture des informations de gauche à droite, soit le bit de poids fort en premier
  Exemple : un octet 10100111
  est transmis 10100111

## IP – Le format de datagramme

- L'***entête*** est transmise sous forme big endian (adresse « d'abord »)
- ***Version*** : indique le numéro de version du protocole. Ainsi, on peut avoir plusieurs version de IP au même moment sur le réseau.
  Actuellement, la version est IPv4.
  Une transition vers IPv6 est en cours.

## IP – Le format de datagramme

- ***LET*** : la Longeur de l'En-Tête est précisée ici sous la forme d'un nombre de mots de 32 bits.
  La valeur minimale est 5, sans options.
  La valeur maximale est de 15, soit 60 octets au maximum pour l'en-tête IP.

## IP – Le format de datagramme

- ***Type de Service*** : sert à distinguer les différentes classes de services (combinaisons de fiabilité et de débit).
  A l'origine, ces 6 bits représentaient :
  - 3 bits de priorité (0 = normale, 7 = haute)
  - 1 bit D(elay) = importance sur le délais
  - 1 bit T(hroughput) = importance sur le débit
  - 1 bit R(eliability) = importance sur la fiabilité

Dans la pratique actuelle, le type de service est *ignoré* par les routeurs

## IP – Le format de datagramme

- ***Longueur totale*** : donne la longueur totale du datagramme (en-tête + données)
  Actuellement, le maximum est 65.535 octets.
  Ce nombre risque de devenir trop petit dans les futurs réseaux Gigabits.
- ***Identification*** : permet à l'hôte destinataire de déterminer à quel datagramme appartient un fragment reçu. Tous les fragments d'un datagramme contiennent la même valeur d'identification.

## IP – Le format de datagramme

- ***DF (Don't Fragment)*** : un bit qui permet de demander aux routeurs intermédiaires de ne pas fragmenter le datagramme. Dans certains cas, le destinataire n'est pas en mesure de recomposer les datagrammes qui seraient fragmentés.
- ***MF (More Fragments)*** : ce bit est positionné à 1 pour tous les fragments sauf le dernier.

## IP – Le format de datagramme

- ***Position de Fragment*** : indique la position (déplacement, offset) du fragment dans le datagramme courant (même identification).
  Tous les fragments (à l'exception du dernier) doivent avoir un multiple de 8 octets.
  Ce champ contient 13 bits, soit une valeur maximale de 8.192 (= $2^{13}$) fragments par message (unité du niveau 4).
  8.192 x 8 = 65.536 octets au total.

## IP – Le format de datagramme

- ***Durée de Vie*** (TTL Time To Live) : compteur qui sert à limiter la durée de vie des datagrammes.
  Lorsqu'un datagramme traverse un routeur, celui-ci décrémente la valeur du TTL.
  Ceci permet d'empêcher que des datagrammes n'errent sans fin (boucle sans fin) dans le réseau.
- En effet, un paquet pourrait « jouer » au ping-pong entres routeurs et ce en fonction des informations de routage que ces derniers possèdent (état des lignes, métriques, …)

## IP – Le format de datagramme

- ***Protocole*** : spécifie à quel processus de la couche transport doit on passer le datagramme
  La numérotation des protocoles est globale sur l'internet (fixée par la RFC1700) et consultable sur le site **http://www.iana.org**

## IP – Le format de datagramme

- ***Total de contrôle d'en-tête*** : permet de détecter les erreurs générées par des mots mémoire erronés dans un routeur.
- Ce total de contrôle doit être recalculé dans chaque routeur. Pourquoi ?
  - car au moins le TTL change à chaque passage dans un routeur.

## IP – Le format de datagramme

- L'*adresse source* et l'*adresse destination* : contiennent respectivement les adresses IP des machines source et destination. Ces adresses seront détaillées ultérieurement.

## IP – Le format de datagramme

- *Options* : le champ options a été prévu pour introduire de nouveaux éléments dans le protocole sans devoir revoir complètement la spécification.
  On peut également placer dans les options des éléments rarement exploitables.

## IP – Le format de datagramme

- Les options sont de longueur variables, et sont constituées de :
  - un champ de code d'option
  - un champ de longueur d'option (facultatif)
  - un ou plusieurs octets de données
- Le champ option doit être un multiple de 4 octets

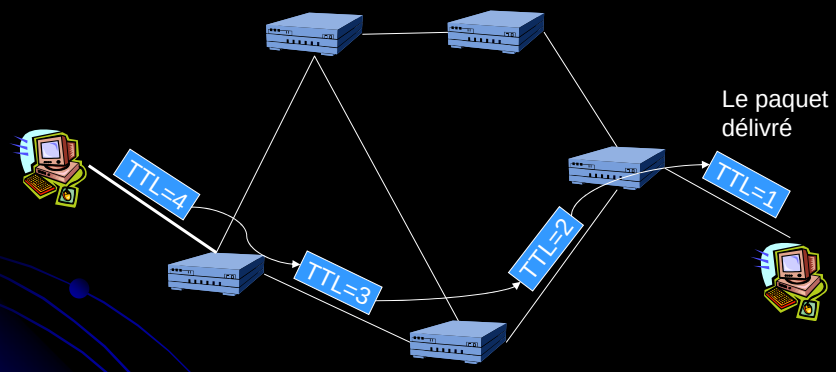
## IP – Le format de datagramme

- ***5 options*** on été définies au départ :
  - ***Sécurité*** : renseigne sur le degré de confidentialité des données, par exemple pour interdire le routage de paquets confidentiels au travers de certains pays. En pratique, c'est ignoré
  - ***Routage strict par la source*** : Le chemin entre la source et la destination est écrit, et le datagramme doit suivre ce chemin. Utile pour envoyer des messages lorsque les tables de routage sont corrompues

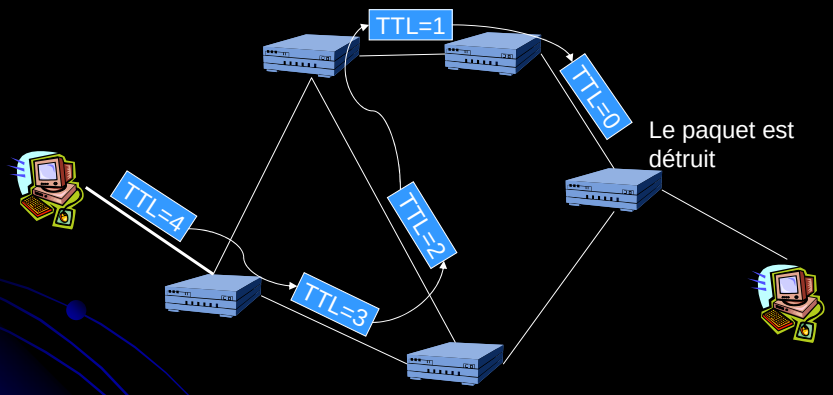
# IP – Le format de datagramme

- ***Routage lâche par la source*** : Permet de spécifier quelques routeurs que le datagramme doit traverser pour rejoindre sa destination. Utile par exemple pour éviter de traverser certains pays en demandant un passage par d'autres
- ***Enregistrement de route*** : Demande aux routeurs intermédiaires d'insérer leur adresse IP dans le champ d'option pour que l'administrateur puisse déterminer le parcourt du datagramme
- ***Horodatage*** : chaque routeur intermédiaire doit introduire une date et heure pour permettre un debuggage du parcours effectué par le datagramme

# Time To Live



## Time To Live




## IP – Les adresses

- Chaque carte réseau possède une adresse MAC unique au monde, constituée de 48 bits.
- Malheureusement, il n'y a aucune logique dans la localisation des adresses MAC : l'adresse 00-90-4B-72-0D-58 peut se trouver à Luxembourg et l'adresse 00-90-4B-72-0D-59 se trouver à New York
- Il est donc impossible d'utiliser ces adresses pour acheminer les datagramme au niveau mondial.

## IP – Les adresses

- A chaque ordinateur, routeur, … connecté à l'Internet on va attribuer au moins une adresse IP.
- Une adresse IP est constituée de 32 bits et contient :
  - Un numéro de réseau
  - Un numéro d'hôtes
- A chaque carte réseau peut-être associée une adresse IP.

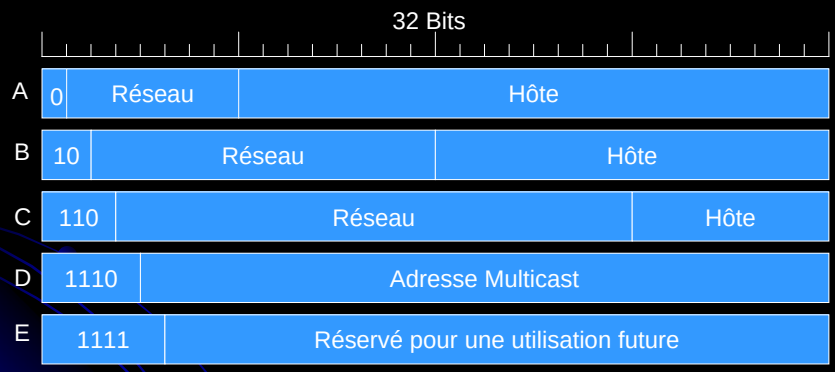
## IP – Les adresses

- Pendant plusieurs décennies, les adresses IP ont été divisées en 5 classes :

**L'adressage par classes**

Le tableau suivant reprend les 5 classes :

# IP – Les adresses




# IP – Les adresses

- ***Classe A*** :
  - Adresses de 1.0.0.0 à 127.255.255.255
  - 128 réseaux différents
  - 16 millions d'hôtes différents par réseau
- ***Classe B*** :
  - Adresses de 128.0.0.0 à 191.255.255.255
  - 16384 réseaux différents
  - 65536 d'hôtes différents par réseau
- ***Classe C*** :
  - Adresses de 192.0.0.0 à 223.255.255.255
  - Plus de 2 millions de réseaux
  - 256 d'hôtes différents par réseau

## IP – Les adresses

- *Classe D* :
  - Adresses de 224.0.0.0 à 239.255.255.255
  - Adresses multicast utilisées pour envoyer des datagrammes à plusieurs destinataires simultanément.
- *Classe E* :
  - Adresses de 240.0.0.0 à 255.255.255.255
  - Réservé pour un usage ultérieur

## IP – Les adresses

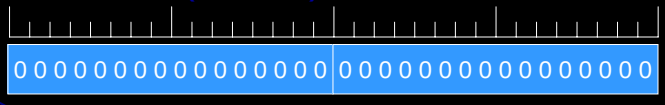
- La gestion des adresses IP au niveau mondial est faite par l'*ICANN* (*Internet Corporation for Assigned Names and Numbers*)
- S'occupe de veiller à ce qu'une adresse IP (routable) ne soit pas utilisée 2 fois sur la planète
- Délégation de la gestion de groupes d'adresses à des autorités régionales
  Exemple : RESTENA – 158.64.0.0

# IP – Les adresses

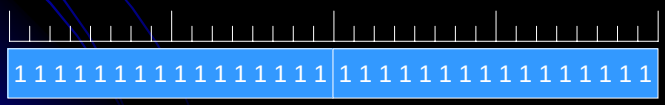
- Représentation d'une adresse IP :
  - *Notation décimale pointée*
    Exemple : 158.64.1.25
  - Les 4 octets qui constituent l'adresse sont séparés par un point
  - Chaque octet peut prendre une valeur de 0 à 255.
  - Exemple :
    1100 0000 0010 1001 0000 0110 0001 0100
    C0 29 06 14
    192.41.6.20

# IP – Les adresses

- Certaines adresses ont une signification particulière :
  - Cet hôte : adresse utilisée au démarrage de la machine (0.0.0.0)

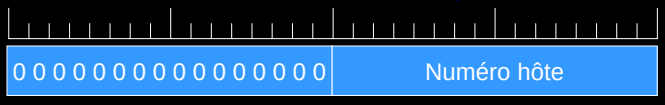



  - *Broadcast* : adresse utilisée pour diffuser un paquet à toutes les stations d'un LAN

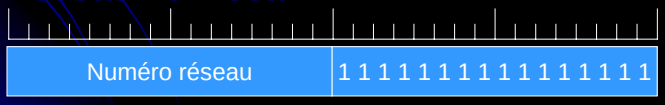


# IP – Les adresses

- Un hôte sur ce réseau : permet de désigner un hôte sans tenir compte du numéro du réseau local (NB : il faut quand même connaître la classe du réseau)

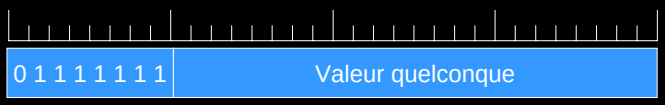



- ***Diffusion broadcast*** sur réseau distant : permet d'envoyer un paquet en broadcast sur un réseau non local.




# IP – Les adresses

- ***Bouclage*** : permet d'effectuer un test de fonctionnement de la pile de protocoles sans utiliser le réseau physique




= 127

- 127.0.0.1 = localhost

## IP – Les sous-réseaux

- Tous les hôtes appartenant à un même réseau doivent avoir le même numéro de réseau
- Cependant, l'utilisation d'une classe A ou B pose rapidement un ***problème*** : on ne peut pas stocker 60.000 hôtes ou plus dans un espace physique adressable par un réseau Ethernet (en coaxial, la limite des 4 répéteurs est rapidement atteinte)

## IP – Les sous-réseaux

- Il est donc nécessaire de faire une légère modification au système d'adressage : ***partitionner le réseau*** en plusieurs entités à ***usage interne***.
- Vu de l'extérieur, rien ne change : le réseau est toujours vu comme une seule entité.
- Exemple : RESTENA dispose d'une classe B (158.64.0.0), et ***attribue des parties*** de cette classe aux lycées luxembourgeois.

## IP – Les sous-réseaux

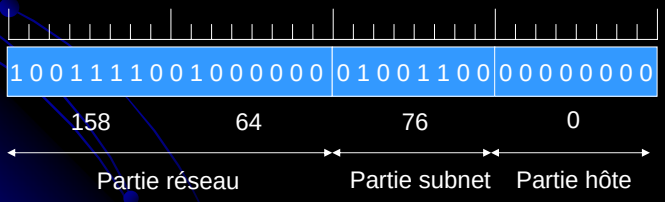
- Les réseaux résultant du partitionnement sont appelés des « ***sous-réseaux*** » ou « ***subnets*** »
- Comment un routeur d'entrée peut-il transmettre un paquet qui arrive pour une machine appartenant à un subnet ?

## IP – Les sous-réseaux

- ***Première solution*** : Tenir en mémoire une table de tous les hôtes des différents subnets.
  Cette solution n'a pas été retenue, car elle implique une table volumineuse en mémoire et un travail de maintenance important (ajout, déplacement, retrait de stations).

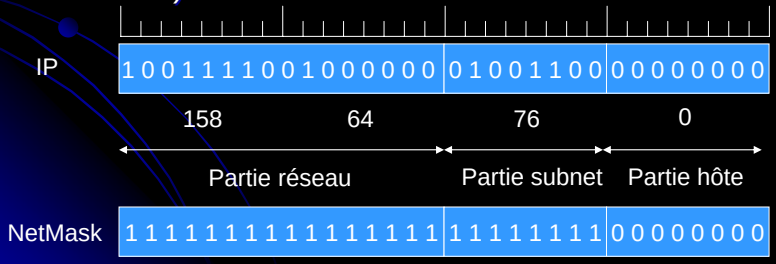
# IP – Les sous-réseaux

- ***Seconde solution*** : utiliser des bits de la partie « hôte » de l'adresse IP pour déterminer le subnet.
  Exemple : RESTENA dispose d'une classe B (158.64.0.0) subdivisée en subnet pour les instituts d'enseignement. Ici pour l'IST (158.64.76.0)




# IP – Les sous-réseaux

- Cette implémentation requiert l'utilisation d'un « **masque de sous-réseau** » ou « ***Subnet mask*** ».
  Il identifie les portions numéro de réseau / numéro de sous-réseau (tous les bits à 1) et le numéro d'hôte. (tous les bits à 0)

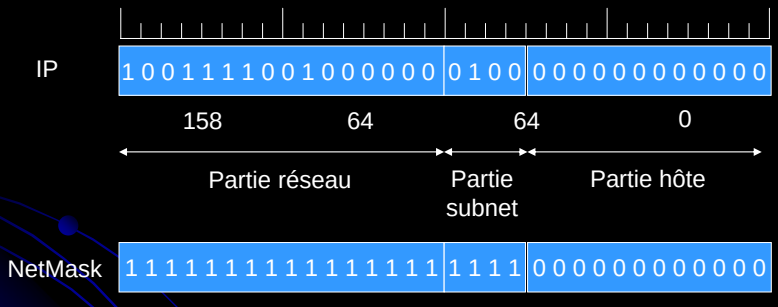


# IP – Les sous-réseaux

- Remarque : dans notre exemple, le masque de sous réseau comporte 24 bits à 1, ce qui est équivalent à une adresse de classe C.
  Dans la réalité, le masque de sous réseau peut prendre un nombre quelconque de bits à 1 :
  - ***corollaire*** : si le nombre de subnets augmente, le nombre de machines dans ceux-ci diminue

# IP – Les sous-réseaux

- Exemple :




Dans ce cas, les adresses IP du sous réseau vont de 158.64.64.0 à 158.64.79.255

## IP – Les sous-réseaux

- Le masque de sous réseau peut se représenter de 2 manières différentes :
  - Sous la même forme qu'une ***adresse IP***
    Pour l'exemple précédent : 255.255.240.0
  - Sous la forme d'un ***nombre de bits*** à 1 placé à coté de l'adresse du réseau
    Pour l'exemple précédent : 158.64.64.0 / 20

## IP – Les sous-réseaux

- Pour un sous réseau, certaines valeurs des adresses ont une signification particulière :
  - ***Adresse réseau*** : constituée d'un numéro réseau et d'un numéro d'hôte égal à 0.
    Elle donne la référence du sous réseau.
  - ***Adresse broadcast*** : constituée d'un numéro de réseau et d'un numéro d'hôte dont tous les bits sont à 1.
    Elle permet d'envoyer un paquet à toutes les machines du sous réseau.

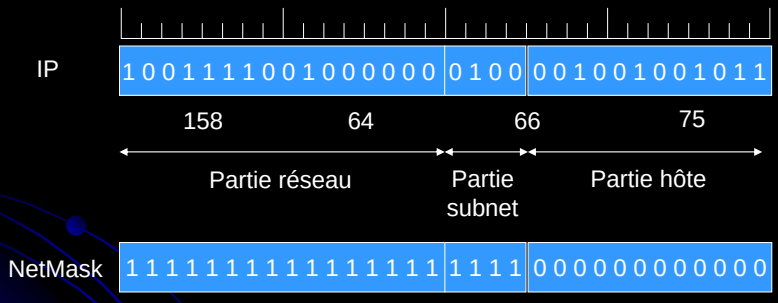
# IP – Les sous-réseaux

- Calcul :
  - Adresse IP : 158.64.66.75
  - Masque de sous réseau : 255.255.240.0

  - Quelle est l'adresse du réseau ?
  - Quelle est l'adresse de broadcast ?
  - Combien de machines peut-on adresser dans ce sous réseau ?

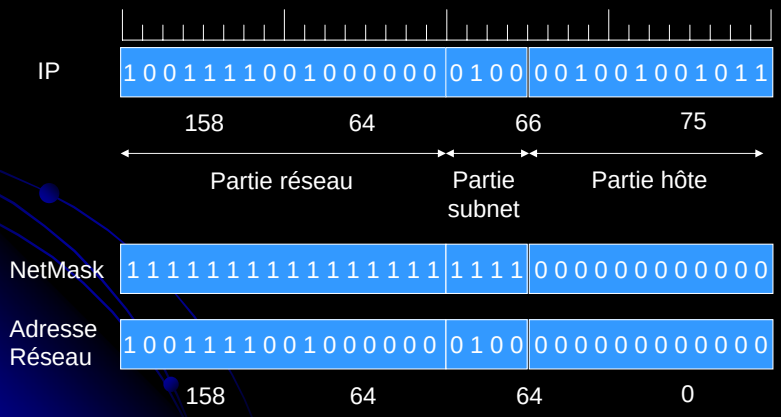
# IP – Les sous-réseaux

- Représentation de l'exercice :



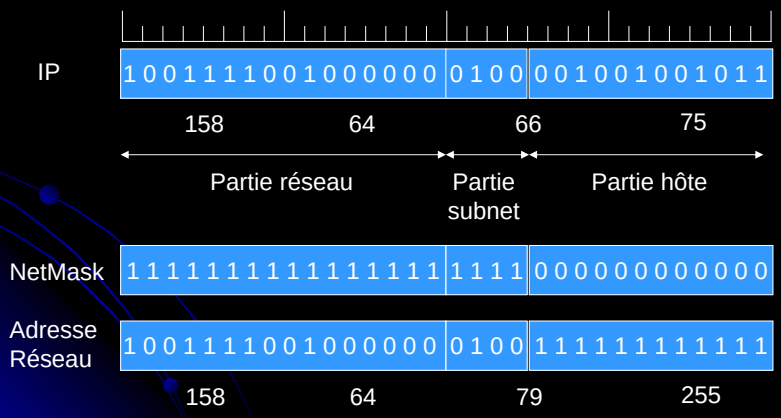
# IP – Les sous-réseaux

- Pour calculer *l'adresse du réseau*, il faut mettre tous les bits de la partie hôte à 0.




# IP – Les sous-réseaux

- Pour calculer *l'adresse broadcast*, il faut mettre tous les bits de la partie hôte à 1.



## IP – Les sous-réseaux

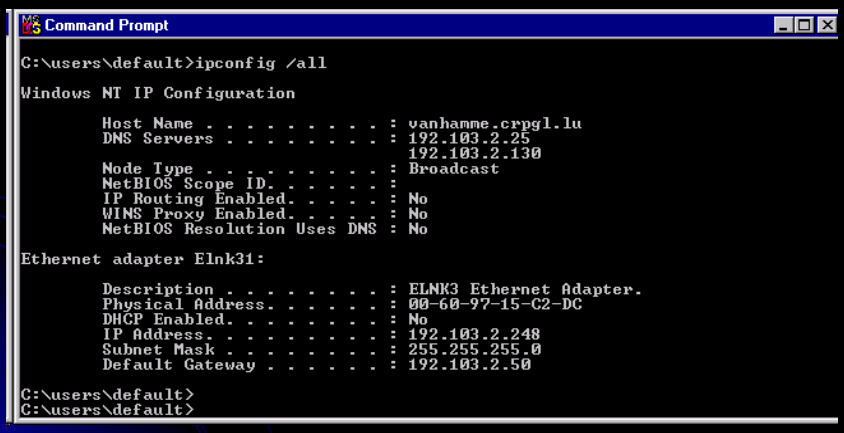
- Le ***nombre de machines*** que l'on peut adresser dans le sous réseau est égal au nombre d'adresses IP différentes (avec la même partie réseau) moins l'adresse réseau et l'adresse broadcast.
  Cela revient à ***calculer le nombre de nombres*** que l'on peut écrire avec les bits de la partie hôte, puis soustraire 2.
  - 12 bits pour la partie hôte (32 – 20)
  - 4096 nombres différents avec ces 12 bits
  - Donc, 4094 hôtes dans le sous réseau

## IP – Les sous-réseaux

- Exercices :
  Calculez l'adresse réseau, l'adresse broadcast et le nombre de machine par sous réseau pour les adresses suivantes.
  - 192.168.101.25/25
  - 164.23.17.56/20
  - 10.65.45.23/12

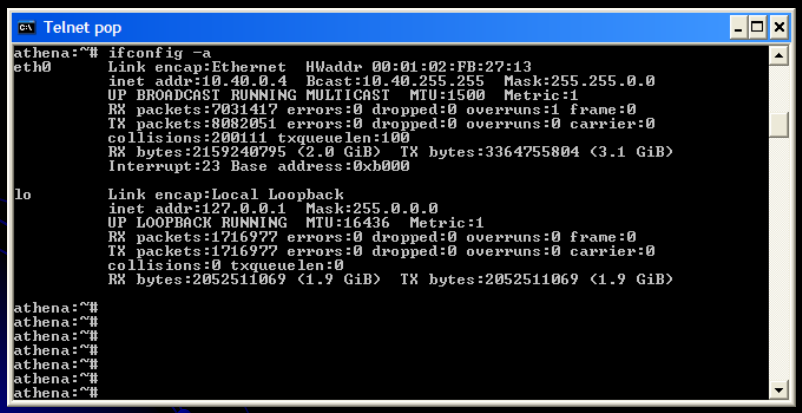
# IP – En pratique

- Déterminer l'adresse IP d'une machine Windows :




# IP – En pratique

- Déterminer l'adresse IP d'une machine Unix :

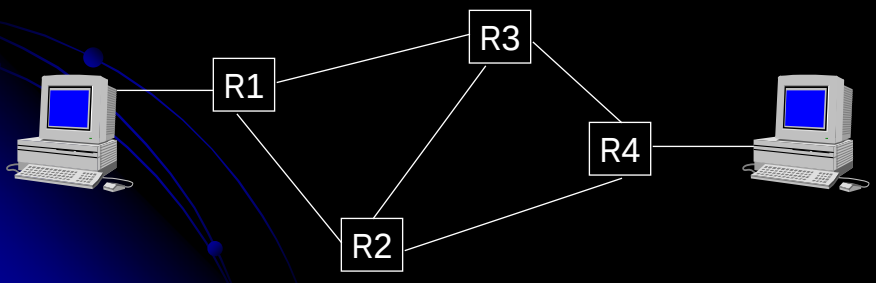


## Routage : Introduction

- Comme nous l'avons vu, la couche réseau a pour but d'acheminer les paquets (datagrammes) d'un hôte émetteur vers un hôte destinataire (distant).

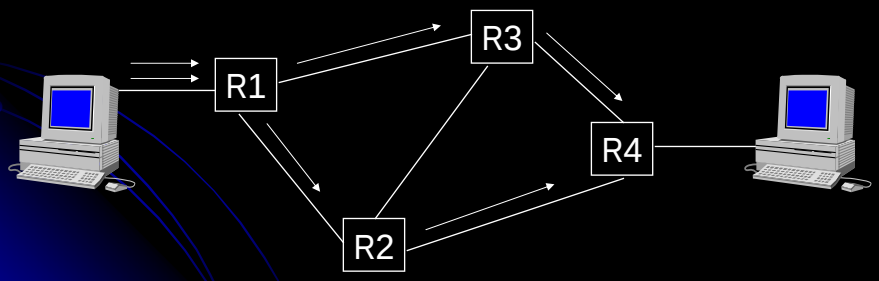
## Routage : Introduction

- Le réseau global peut être vu comme suit : deux machines distantes sont reliées par un ensemble de routeurs formant un maillage complexe.



# Routage : Introduction

- En conséquence, il existe plusieurs chemins pour un datagramme pour aller de l'émetteur vers le récepteur.

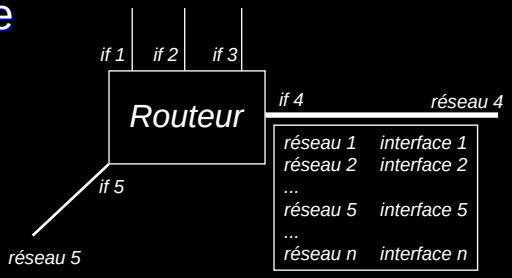



# Routage : Introduction

- Le ***routeur*** est un dispositif qui permet de déterminer la **route** qu'un datagramme doit suivre pour arriver à destination.
- Ce processus s'appelle ***routage***.

# Routage : Introduction

- Globalement, le routeur peut être vu comme une boite noire avec un certain nombre d'interface.
- Chaque interface pourra être connectée à un réseau (local)




# Routage : Introduction

- A l'intérieur du routeur, un algorithme examine chaque datagramme en provenance d'une interface.
- En fonction de la **table de routage** et de **l'adresse de destination**, il détermine l'interface que le datagramme doit emprunter pour continuer sa route vers sa destination.

## Routage : table de routage

- La table de routage est une liste contenant un certain nombre de combinaisons :
  - Adresse IP (réseau, 0 ou réseau, hôte)
  - Masque de sous réseau
  - Interface de sortie
- Cette liste permet de déterminer quelle interface de sortie doit emprunter un datagramme qui arrive au routeur.
- Nous allons montrer comment le routage fonctionne au travers d'un exemple :

## Routage : exemple

- Soit 3 universités qui demandent un accès à l'Internet :
  - Cambridge demande 2000 adresses IP et reçoit le bloc d'adresses de 194.24.0.0 à 194.24.7.255 avec le masque 255.255.248.0
  - Oxford demande 4000 adresses IP et reçoit le bloc d'adresses de 194.24.16.0 à 194.24.32.255 avec le masque 255.255.240.0 Un bloc de 4096 adresses doit être aligné sur la valeur 4096.

# Routage : exemple

- Edimbourg demande 1000 adresses IP et reçoit le bloc d'adresses de 194.24.8.0 à 194.24.11.255 avec le masque 255.255.252.0
- Dans le tableau suivant, on constate donc qu'un ensemble d'adresse IP sont disponibles de 194.24.12.0 à 194.24.15.255

# Routage : Exemple

| Université | Première adresse | Dernière adresse | Nombre d'adresses | Masque de sous réseau |
|---|---|---|---|---|
| Cambridge | 194.24.0.0 | 194.24.7.255 | 2048 | 255.255.248.0 |
| Edimbourg | 194.24.8.0 | 194.24.11.255 | 1024 | 255.255.252.0 |
| (Disponible) | 194.24.12.0 | 194.24.15.255 | 1024 | 255.255.252.0 |
| Oxford | 194.24.16.0 | 194.24.32.255 | 4096 | 255.255.240.0 |

# Routage : Exemple

- Les tables de routage des routeurs sont mises à jour avec ces informations.
  Dans chaque routeur on trouvera l'adresse réseau et le masque de sous réseau :

| Université | Adresse réseau | Masque de sous réseau |
|---|---|---|
| Cambridge | 11000010 00011000 00000000 00000000 | 11111111 11111111 11111000 00000000 |
| Edimbourg | 11000010 00011000 00001000 00000000 | 11111111 11111111 11111100 00000000 |
| Oxford | 11000010 00011000 00010000 00000000 | 11111111 11111111 11110000 00000000 |

- Y associer le port de sortie

# Routage : Exemple

- Voyons ce qui se passe lorsqu'un routeur reçoit un paquet dont l'adresse de destination est 194.24.17.4

  En binaire, cette adresse est :
  11000010 00011000 00010001 00000100
- Le routeur va effectuer un ***ET logique*** avec les masques de chaque ligne de la table de routage.

## Routage : Exemple

- Pour la première ligne (Cambridge) :

  11000010 00011000 00010001 00000100
  11111111 11111111 11111000 00000000
  ---
  11000010 00011000 00010000 00000000

- Cette adresse ***ne correspond pas*** à l'adresse IP du réseau de Cambridge.

## Routage : Exemple

- Pour la seconde ligne (Edimbourg) :

  11000010 00011000 00010001 00000100
  11111111 11111111 11111100 00000000
  ---
  11000010 00011000 00010000 00000000

- Cette adresse ***ne correspond pas*** à l'adresse IP du réseau de Edimbourg.

## Routage : Exemple

- Pour la troisième ligne (Oxford) :

  11000010 00011000 00010001 00000100
  11111111 11111111 11110000 00000000
  ---
  11000010 00011000 00010000 00000000

- Le résultat ***correspond*** à l'adresse du réseau de Oxford.

## Routage : Exemple

- Si aucune correspondance plus longue n'est trouvée, le datagramme est envoyé par l'interface correspondante pour la ligne trouvée dans la table de routage.

## Routage : Exemple

- Prenons ensuite le cas d'un routeur situé à Omaha, au Nebraska. Ce routeur ne dispose que de 4 interfaces vers :
  - Minneapolis
  - New York
  - Dallas
  - Denver

## Routage : Exemple

- Lorsque ce routeur prend connaissance des 3 nouvelles lignes à insérer dans sa table de routage, il constate qu'il peut les combiner en une seule règle :
  194.24.0.0 / 19 vers l'interface New York.
  L'adresse :
  11000010 00011000 00000000 00000000
  Le masque de sous réseau :
  11111111 11111111 11100000 00000000

## Routage : Exemple

- Cette entrée dit d'envoyer tous les paquets destinés à n'importe quelle des 3 universités à New York
- En combinant ces entrées, le routeur de Omaha simplifie sa table de routage et donc améliore ses performances.
- On appelle cette technique l'***agrégation de routes***.

## Routage : Exemple

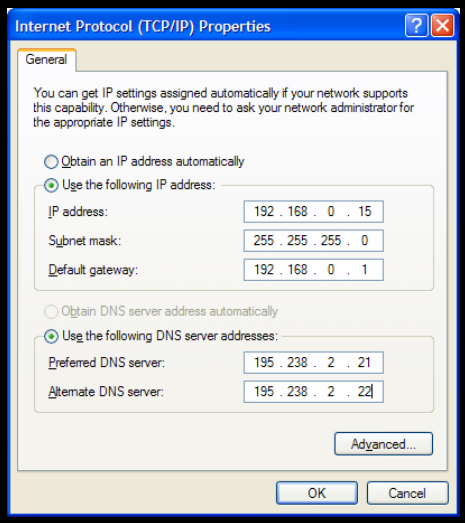
- L'entrée agrégée du routeur de Omaha dirige aussi vers New York les datagrammes destinés aux adresses non assignées.
- Si ces adresses étaient attribuées à l'université de Californie, il faudrait ajouter une entrée supplémentaire :
  Exemple : 194.24.12.0 / 22 vers Dallas

# Routage : LAN ou WAN ?

- Le même principe du ET logique est utilisé par les stations d'un LAN pour déterminer si le datagramme qu'elles envoient doit être délivré sur le LAN ou envoyé à un routeur pour une expédition sur un WAN.

# Routage : LAN ou WAN ?

- Exemple : voici la configuration d'une machine.
- IP : 192.168.0.15
- Netmask : 255.255.255.0
- Gateway : 192.168.0.1



## Routage : LAN ou WAN ?

- Cette machine envoie un datagramme vers 192.168.0.33.
- On effectue un ET logique entre l'adresse de destination et le masque de sous réseau.
- 11000000 01000100 00000000 00100001
  11111111 11111111 11111111 00000000
  ---
  11000000 01000100 00000000 00000000
- Cette adresse correspond à l'adresse réseau calculée à partir de l'adresse IP de la machine.
- Le datagramme doit donc être délivré sur le LAN.

## Routage : LAN ou WAN ?

- Cette machine envoie un datagramme vers 192.168.100.33.
- On effectue un ET logique entre l'adresse de destination et le masque de sous réseau.
- 11000000 01000100 01100100 00100001
  11111111 11111111 11111111 00000000
  ---
  11000000 01000100 01100100 00000000
- Cette adresse ne correspond pas à l'adresse réseau calculée à partir de l'adresse IP de la machine.
- Le datagramme doit donc être délivré au routeur

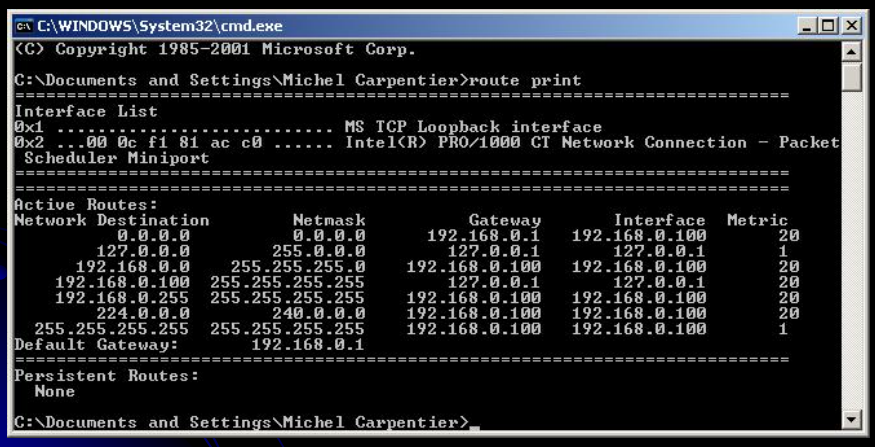
## Routage : la gateway

- La default gateway notée dans la configuration de la machine exemple est en fait la destination par défaut pour tous les datagrammes ne trouvant pas une ligne qui leur correspond.
  On peut assimiler cela au panneau « Toutes directions ».
- Il s'agit d'une entrée de la table de routage

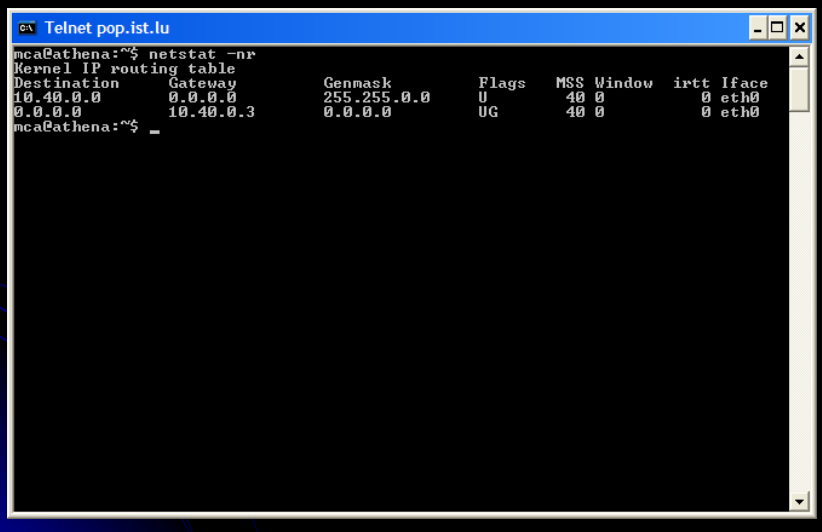
## Routage : les outils

- Consultation de la table de routage sous Windows :
  - Route print
  - Netstat -nr
- Consultation de la table de routage sous Unix :
  - Netstat –nr
  - Route (nécessite les droits root)

# Routage : les outils

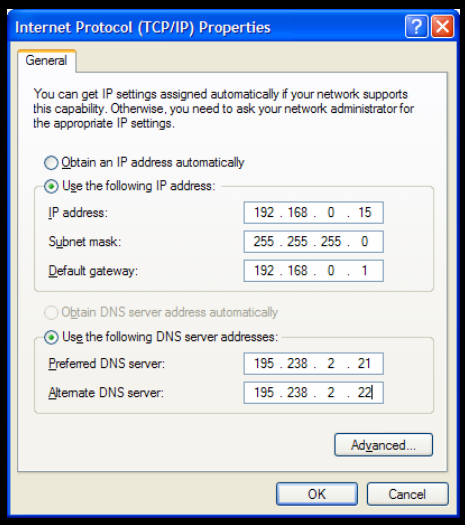



# Routage : les outils



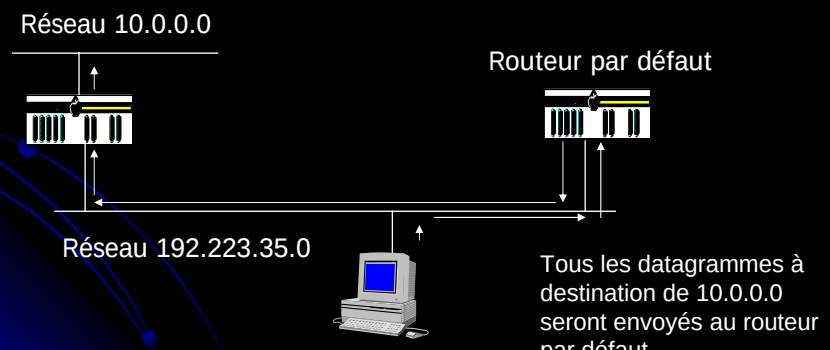
# Routage : Modifications

- Au niveau de la configuration d'une machine, il n'y a qu'une seule route par défault (default gateway).




# Routage : Modifications

- Dans certains cas, cela peut poser des problèmes. Exemple :



## Routage : Modifications

- Pour modifier la table de routage d'un PC Windows :
  - Ajout d'une route :

    route add 192.168.76.0 mask 255.255.255.0 192.168.0.4
  - Suppression d'une route :

    route delete 192.168.76.0 mask 255.255.255.0 192.168.0.4
  - Plus d'infos : « route /? »

## Routage : Modifications

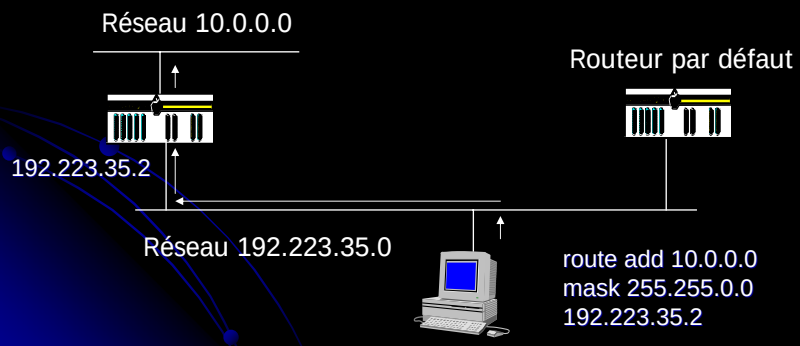
- Pour modifier la table de routage d'une machine Unix :
  - Ajout d'une route :

    route add -net 192.56.76.0 netmask 255.255.255.0 dev eth0
  - Suppression d'une route :

    route del -net 192.56.76.0 netmask 255.255.255.0 dev eth0
  - Plus d'infos : « man route »

# Routage : Modifications

- En modifiant la table de routage du PC, on peut router directement les datagrammes vers le routeur du réseau 10.0.0.0




# Routage : Modifications

- Dans les deux cas (Windows et Unix), les modifications apportées de la sorte aux tables de routage ne seront valides que pour la session courante.
- Pour une modification permanente, il faut ajouter ces lignes dans les scripts de démarrage de la machine.

## Liaison couche 2 & 3

- Nous avons vu précédemment que la couche 2 utilise des adresses MAC pour transmettre des informations d'une station à une autre.
- Avec l'arrivée de la couche 3, nous avons introduit les adresses IP pour assurer l'acheminement mondial des datagrammes.
- Comment effectuer le lien entre adresse MAC et adresse IP ?

## ARP

- Ce lien va être assuré par ARP (Address Resolution Protocol).
- ARP va convertir les adresses IP en adresse MAC (ethernet ou token ring)
- La machine source envoie un paquet en broadcast sur le LAN. Ce paquet contient l'adresse MAC source, l'adresse IP source et l'adresse IP destination.

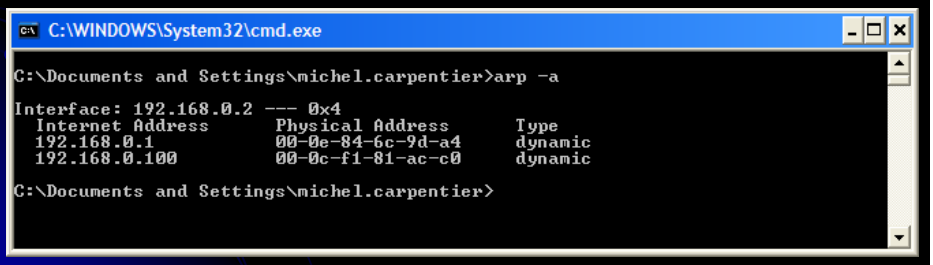
# ARP

- Chaque machine connectée au réseau local reçoit ce paquet, mais seule la machine dont l'adresse IP est spécifiée correspond à l'adresse IP destination du paquet répond.  Cette machine envoie alors à l'adresse MAC source trouvée dans le paquet, l'information demandée : son adresse MAC.

# ARP

# ARP

- Les informations ainsi obtenues sont stockées dans une mémoire temporaire
- On peut consulter ces informations à l'aide de la commande : arp -a




# Routage : Exercice

- Donnez, pour chaque segment impliqué
  - la valeur des adresses ethernet source et destination
  - la valeur des adresses IP source et destination

  utilisées pour une communication entre PC1 et PC2, puis PC1 et PC3, PC1 et PC4.
- Vous utiliserez la notation suivante :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|

# Routage : Exercice

- Le tableau suivant reprend les adresses des machines :

| Nom de machine | Adresse IP | Adresse MAC |
|---|---|---|
| PC1 | 199.27.35.1 | @PC1 |
| PC2 | 199.27.35.2 | @PC2 |
| PC3 | 200.25.148.3 | @PC3 |
| PC4 | 129.46.12.15 | @PC4 |
| R1 interface 1 | 198.28.25.250 | @R1-1 |
| R1 interface 2 | 199.27.35.250 | @R1-2 |
| R1 interface 3 | 129.46.12.250 | @R1-3 |
| R2 interface 1 | 198.28.25.251 | @R2-1 |
| R2 interface 2 | 200.25.148.250 | @R2-2 |

# Routage : Exercice

- Les tableaux suivants reprennent les tables de routage

| PC1 | | |
|---|---|---|
| Adresse & Masque | Interface | Gateway |
| 0.0.0.0 / 0 | Eth0 | 199.27.35.250 |
| 199.27.35.0 / 24 | Eth0 | |

| PC2 | | |
|---|---|---|
| Adresse & Masque | Interface | Gateway |
| 0.0.0.0 / 0 | Eth0 | |
| 199.27.35.0 / 24 | Eth0 | 199.27.35.250 |

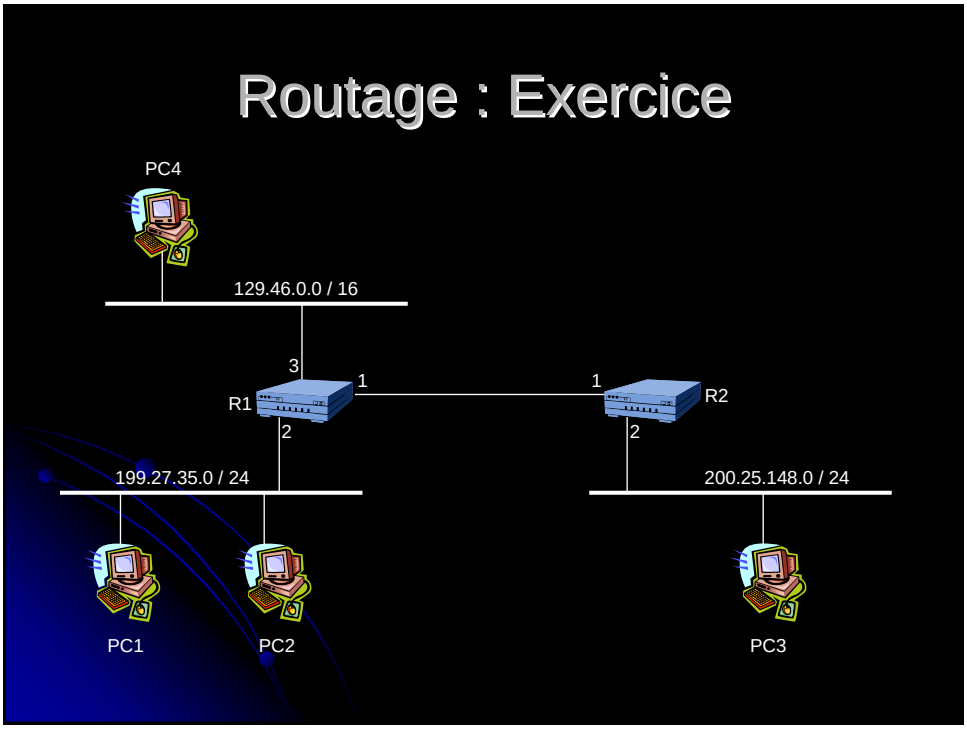
| PC3 | | |
|---|---|---|
| Adresse & Masque | Interface | Gateway |
| 0.0.0.0 / 0 | Eth0 | 200.25.148.250 |
| 200.25.148.0 / 24 | Eth0 | |

| PC4 | | |
|---|---|---|
| Adresse & Masque | Interface | Gateway |
| 0.0.0.0 / 0 | Eth0 | 129.46.12.250 |
| 129.46.0.0 / 16 | Eth0 | |

| R1 | | |
|---|---|---|
| Adresse & Masque | Interface | Gateway |
| 199.27.35.0 / 24 | 2 | |
| 129.46.0.0 / 16 | 3 | |
| 0.0.0.0 / 0 | 1 | 198.28.25.251 |

| R2 | | |
|---|---|---|
| Adresse & Masque | Interface | Gateway |
| 200.25.148.0 / 24 | 2 | |
| 0.0.0.0 / 0 | 1 | 198.28.25.250 |

# Routage : Exercice




# Routage : Exercice

- Transmission de datagramme de PC1 à PC2.
  - On effectue un ET logique entre l'adresse IP de destination et le masque du sous réseau de la première entrée de la table de routage de PC1 : 199.27.35.2 ET 0.0.0.0 = 0.0.0.0
    La route convient, mais on continue à parcourir la table de routage pour trouver une éventuelle meilleure solution.
  - La seconde ligne nous donne le calcul suivant : 199.27.35.2 ET 255.255.255.0 = 199.27.35.0
    La route convient également. De plus, la correspondance est plus longue (plus de bits correspondants), elle est donc privilégiée.

# Routage : Exercice

- On recherche donc l'adresse MAC de PC2 en envoyant un paquet ARP en broadcast sur le LAN.
- La station PC2 répond en donnant son adresse MAC @PC2.
- Le paquet peut donc circuler sur le LAN avec les informations suivantes :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|
| @PC1 | @PC2 | 199.27.35.1 | 199.27.35.2 |

# Routage : Exercice

- Transmission d'un datagramme de PC1 à PC3.
  - Parcours de la table de routage de PC1 :
    200.25.148.3 ET 0.0.0.0 = 0.0.0.0
    La route convient. On continue…
  - 200.25.148.3 ET 255.255.255.0 = 200.25.148.0
    La route ne convient pas, car l'adresse trouvée ne correspond pas à l'entrée.
  - La première ligne est donc utilisée. Elle renseigne qu'il faut envoyer le datagramme à la gateway 199.27.35.250
  - On recherche donc l'adresse MAC de ce routeur via ARP. L'adresse nous est fournie : @R1-2

# Routage : Exercice

- On obtient donc :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|
| @PC1 | @R1-2 | 199.27.35.1 | 200.25.148.3 |

- Le datagramme arrive donc dans R1 par l'interface 2.
- Le routeur consulte sa table de routage pour déterminer le traitement à apporter à ce datagramme.
- 200.25.148.3 ET 255.255.255.0 = 200.25.148.0
  La route ne convient pas.
- 200.25.148.3 ET 255.255.0.0 = 200.25.0.0
  La route ne convient pas.

# Routage : Exercice

- 200.25.148.3 ET 0.0.0.0 = 0.0.0.0
  La route convient et on est arrivé au bout de la table de routage.
- La ligne en question indique qu'il faut transmettre le datagramme à la gateway 198.28.25.251 via l'interface 1 du routeur
- En utilisant ARP, on détermine l'adresse MAC correspondant à cette adresse IP : @R2-1
- Le datagramme est donc transmis :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|
| @PC1 | @R1-2 | 199.27.35.1 | 200.25.148.3 |
| @R1-1 | @R2-1 | 199.27.35.1 | 200.25.148.3 |

# Routage : Exercice

- Le datagramme arrive dans R2 par l'interface 1
- Le routeur consulte sa table de routage pour déterminer le traitement à apporter à ce datagramme.
- 200.25.148.3 ET 255.255.255.0 = 200.25.148.0
  La route convient.
- 200.25.148.3 ET 0.0.0.0 = 0.0.0.0
  La route convient, mais la correspondance est plus courte, on conserve donc la première ligne comme route à utiliser.
- Cette ligne nous indique d'utiliser l'interface 2 pour transmettre le datagramme
- En utilisant ARP, on détermine l'adresse MAC correspondant à cette adresse IP : @PC3

# Routage : Exercice

- Le datagramme est donc transmis :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|
| @PC1 | @R1-2 | 199.27.35.1 | 200.25.148.3 |
| @R1-1 | @R2-1 | 199.27.35.1 | 200.25.148.3 |
| @R2-2 | @PC3 | 199.27.35.1 | 200.25.148.3 |

- Le datagramme est arrivé à destination.

# Routage : Exercice

- Transmission d'un datagramme de PC1 à PC4.
  - Parcours de la table de routage de PC1 :
    129.46.12.15 ET 0.0.0.0 = 0.0.0.0
    La route convient. On continue…
  - 129.46.12.15 ET 255.255.255.0 = 129.46.12.0
    La route ne convient pas, car l'adresse trouvée ne correspond pas à l'entrée.
  - La première ligne est donc utilisée. Elle renseigne qu'il faut envoyer le datagramme à la gateway 199.27.35.250
  - On recherche donc l'adresse MAC de ce routeur via ARP. L'adresse nous est fournie : @R1-2

# Routage : Exercice

- On obtient donc :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|
| @PC1 | @R1-2 | 199.27.35.1 | 200.25.148.3 |

  - Le datagramme arrive donc dans R1 par l'interface 2.
  - Le routeur consulte sa table de routage pour déterminer le traitement à apporter à ce datagramme.
  - 129.46.12.15 ET 255.255.255.0 = 129.46.12.0
    La route ne convient pas.
  - 129.46.12.15 ET 255.255.0.0 = 129.46.0.0
    La route convient. On continue…

# Routage : Exercice

- 129.46.12.15 ET 0.0.0.0 = 0.0.0.0
  La route convient et on est arrivé au bout de la table de routage. Cependant, la précédente solution est plus longue, donc utilisée.
- La ligne en question indique qu'il faut utiliser l'interface 3 pour délivrer le datagramme sur le LAN.
- En utilisant ARP, on détermine l'adresse MAC correspondant à cette l'adresse IP de PC4 : @PC4
- Le datagramme est donc transmis :

| adresse ethernet source | adresse ethernet destination | adresse IP source | adresse IP destination |
|---|---|---|---|
| @PC1 | @R1-2 | 199.27.35.1 | 200.25.148.3 |
| @R1-3 | @PC4 | 129.46.12.250 | 129.46.12.15 |

# Routage : Exercices

- Conseils pour la réalisation :
  - Attention aux tables de routage !
  - Ne pas se focaliser sur le schéma du réseau
  - Travailler de manière méthodique en suivant l'algorithme de routage.

## NAT

- Les adresses IP sont devenues une denrée rare de nos jours
- Une solution consiste à allouer des adresses de manière temporaire aux personnes qui se connectent à l'Internet par une ligne téléphonique.
  Cette solution n'est malheureusement pas miraculeuse car les entreprises veulent une connexion permanente, de même que les clients au service ADSL.

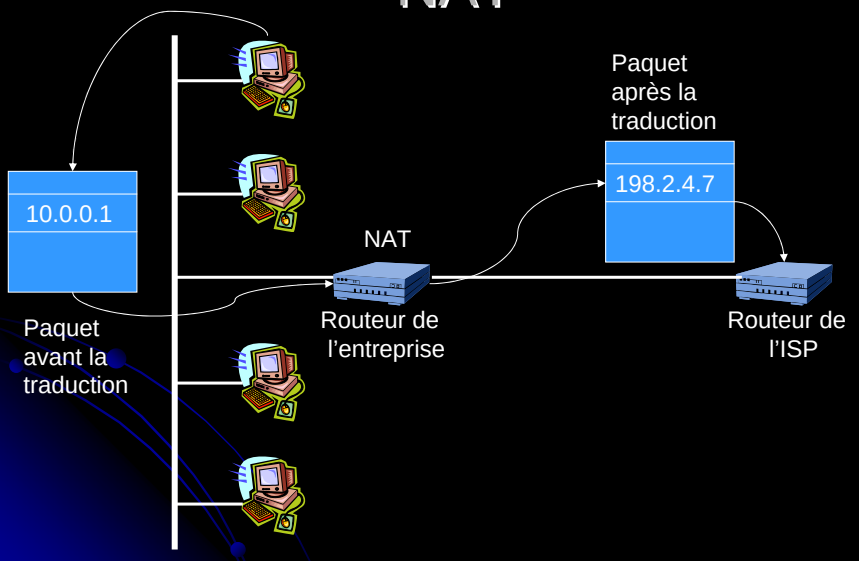
## NAT

- C'est pour cela qu'est née la technique de **traduction d'adresses de réseau** (***Network Address Translation - NAT***)
- On assigne à chaque organisation une seule adresse IP (ou un petit groupe).
- Tous les ordinateurs reçoivent une adresse unique interne.  Lorsqu'un datagramme doit être envoyé sur le réseau externe, la traduction d'adresse intervient.

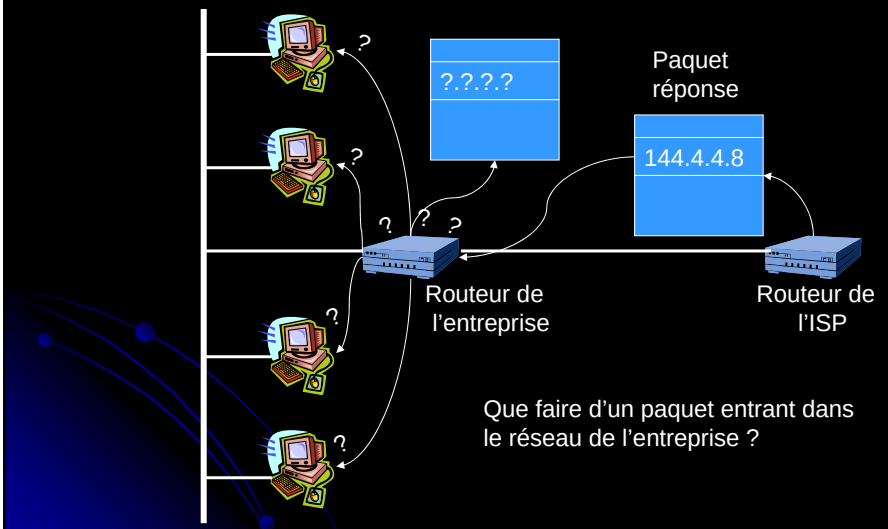
# NAT

- Pour réaliser cela, 3 plages d'adresses IP ont été réservées :
  - 10.0.0.0 / 8 16 777 216 hôtes
  - 172.16.0.0 / 12 1 048 576 hôtes
  - 192.168.0.0 / 16 65 536 hôtes
- Ces adresses peuvent être utilisées librement à la condition qu'aucune d'elle ne doit être transmise sur Internet.

# NAT



# NAT




# NAT

- On ne peut modifier l'entête IP pour y ajouter une information pour NAT, et il ne reste plus qu'un seul bit disponible !
- Les concepteurs de NAT ont constaté que la majorité des paquets IP incluent une charge utile TCP ou UDP.

## NAT

- Nous verrons plus tard (cours 1081) que TCP et UDP utilise un numéro de port source et un numéro de port destination pour orienter les paquets vers les bons processus (tant chez l'émetteur que le récepteur).
- Les numéros de 0 à 1023 sont réservés à des services identifiés.
  Exemple : le port http est 80.
- Ces numéros de port sont codés sur 16 bits.

## NAT

- Par analogie, on pourrait comparer ces numéros de ports aux extensions téléphoniques d'une entreprise.
  Le numéro de la centrale serait l'adresse IP, tandis que les extensions des employés seraient les numéros de ports.

## NAT

- Lorsqu'un paquet est envoyé à l'extérieur, il traverse le dispositif NAT :
  - L'adresse IP interne (10.0.0.1) est remplacée par l'adresse publique de la société (198.2.4.7)
  - Le champ port source TCP (ou UDP) est remplacé par une référence à une entrée dans une table de traduction de 65 536 adresses du dispositif NAT.

## NAT

- Cette table contient :
  - Le numéro IP de la machine source
  - Le numéro de port de la machine source
- Les sommes de contrôle sont recalculées et le paquet est transmis.
- Il est impératif de remplacer le port source par un port choisi, car au sein du réseau, deux machines pourraient établir une communication vers l'extérieur avec le port 5000 comme source au même moment.

## NAT

- Lorsque la réponse arrive au dispositif NAT de l'extérieur, le port TCP (ou UDP) est extrait du paquet et utilisé pour retrouver dans la table de correspondance du dispositif NAT, le numéro de port et l'adresse IP de la machine destinatrice.
- Une fois l'entrée localisée, le paquet reconstitué (avec recalcul des sommes de contrôle), il peut être envoyé au destinataire.

## NAT

- Cette technique a cependant ses problèmes :
  - NAT ne respecte pas le modèle architectural qui dit que chaque machine est identifiée par son adresse IP
  - NAT altère le réseau en faisant d'un réseau sans connexion une sorte de réseau avec connexions.
    En cas de plantage du routeur toutes les connexions en cours sont perdues.

## NAT

- NAT enfreint la règle la plus essentielle de l'organisation en couches : la couche k n'est absolument pas concernée par ce que la couche k+1 place dans son champ de données.
  La version 2 de TCP risque de poser beaucoup de problèmes.
- Les processus de l'Internet ne sont pas strictement obligés d'utiliser TCP ou UDP. Avec NAT, ils perdent cette liberté.

## NAT

- Certaine application insèrent des adresses IP dans le corps des données transmises. Le récepteur peut ensuite les extraire pour s'en servir.  Exemple : FTP, H323.
- Étant donné que le champ port source est codé sur 16 bits, un maximum de 65 536 machines peuvent être associées.  Ceci peut être contourné en réalisant le NAT avec plusieurs adresses externes.

## Les protocoles de contrôle

- Outre IP qui sert à la transmission de données, l'Internet dispose d'un certain nombre de protocoles destinés au contrôle du réseau :
  - ICMP – Internet Control Message Protocol
  - ARP – Address Resolution Protocol
  - RARP – Reverse Address Resolution Protocol
  - BOOTP - Bootstrap
  - DHCP – Dynamic Host Configuration Protocol

## ICMP

- ICMP (Internet Control Message Protocol) sert à :
  - Signaler des événement inattendus sur le réseau
  - Tester le fonctionnement du réseau
- Une dizaine de messages ICMP ont été définis et peuvent être transmis au sein d'un paquet IP.

# ICMP

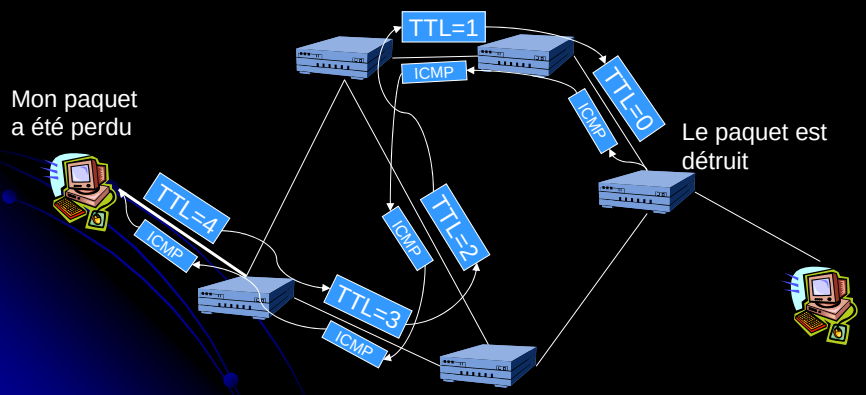
| *Type de message* | *Description* |
|---|---|
| Destination inaccessible | Le paquet n'a pas pu être délivré |
| Délai expiré | Le champ d'entête TTL a atteint 0 |
| Problème de paramètre | Champ d'entête invalide |
| Ralentissement de la source | Paquet de rétention |
| Redirection | Indication d'une meilleure route |
| Demande d'écho | Demande à une machine si elle est active |
| Envoi d'écho | La machine distante est active |
| Demande d'horodate | Identique à une demande d'écho, mais inclus en plus une horodate |
| Envoi d'horodate | Identique à un envoi d'écho, mais inclus en plus une horodate |

# ICMP

- **Destination inaccessible** est utilisé lorsque le sous réseau, ou un routeur ne parvient pas à localiser la destination. Ce paquet peut également être envoyé par un routeur qui ne peut transmettre une donnée pour laquelle le champ DF de l'entête est positionné à 1.

# ICMP

- **Délai expiré** est émis lorsqu'un paquet est éliminé car son compteur de durée de vie a atteint la valeur 0.




# ICMP

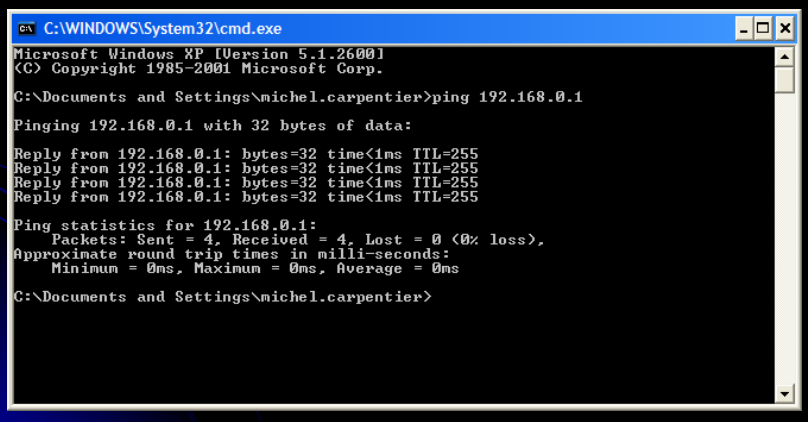
- **Problème de paramètre** indique qu'une valeur illégale a été détectée dans un champ d'entête. Il signifie un bug dans un logiciel IP.
- **Ralentissement de source** était destiné initialement à ralentir l'émetteur trop rapide. Il n'est plus utilisé car le contrôle de flux est maintenant assuré en couche 4. (Cours 1081)

# ICMP

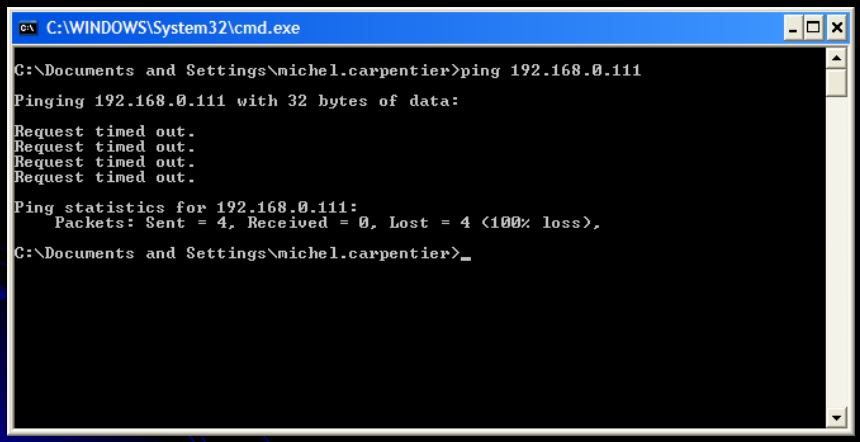
- **Redirection** est émis par un routeur lorsqu'il lui semble qu'un paquet n'est pas correctement routé. Il signale à l'hôte émetteur la probabilité d'une erreur.
- Les messages **demande d'écho** et **envoi d'écho** permettent de déterminer si une destination donnée est accessible et active.

# Ping

- Ping permet d'utiliser ces paquet ICMP demande d'écho et envoi d'écho.

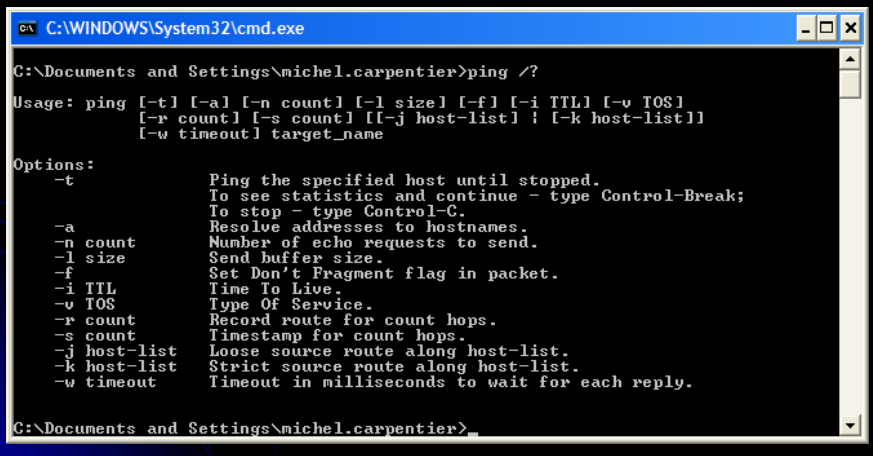


# Ping




# Ping

- Ping possède quelques options interessantes…



## ICMP

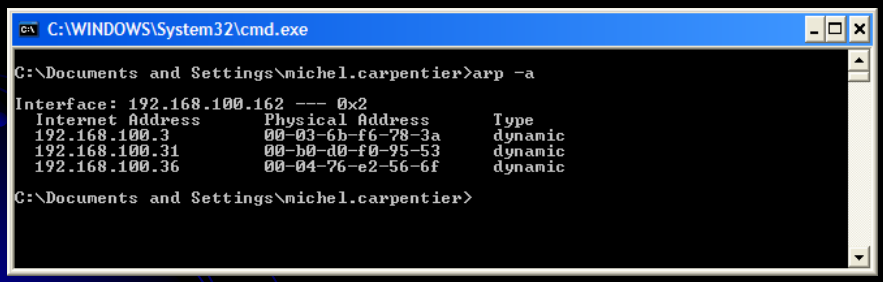
- D’autres messages on été définis.
  Leur liste se trouve maintenue à l’adresse
  http://www.iana.org/assignments/icmp-parameters

## ICMP & ARP : Exercice

- Comment déterminer l’adresse MAC d’une station distante ?
- Solution en 2 étapes :
  - Effectuer un PING vers la station
  - Consulter la table d’adresses MAC via ARP.

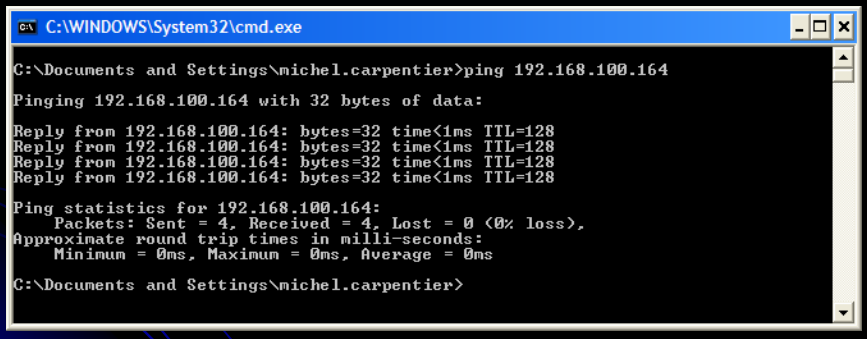
# ICMP & ARP : Exercice

- Quelle est l'adresse MAC de la station 192.168.100.164 ?
  Cette adresse n'est pas en mémoire :



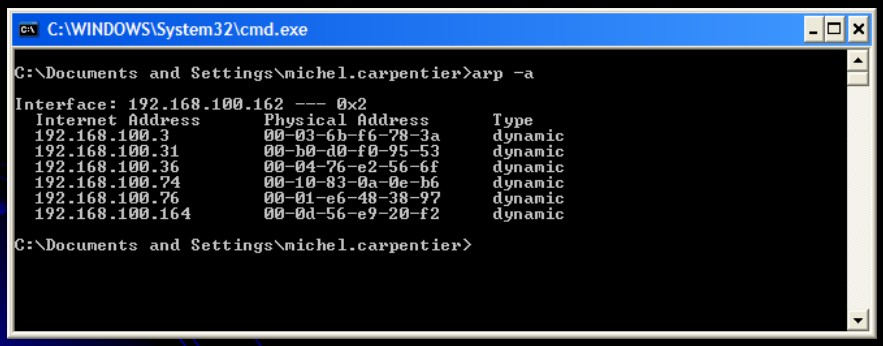

# ICMP & ARP : Exercice

- On effectue un PING vers cette station :



# ICMP & ARP : Exercice

- On regarde le contenu de la table ARP :



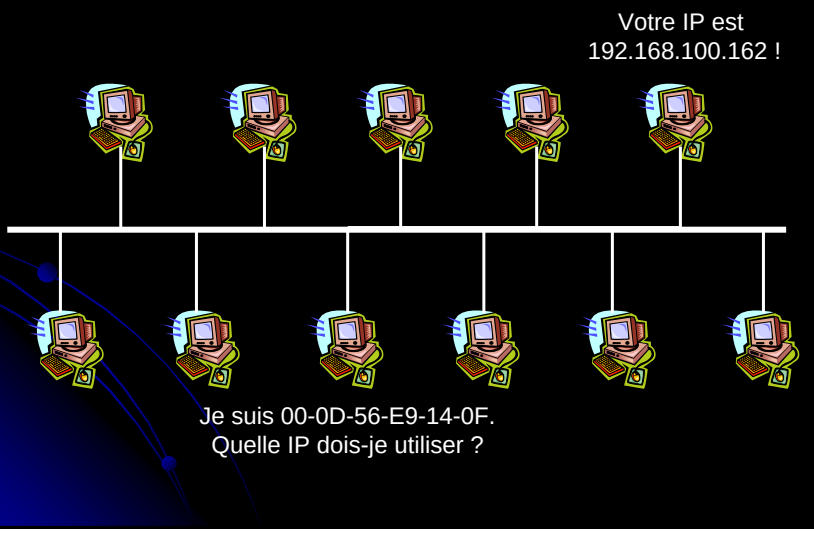

# RARP

- Nous avons vu que ARP permet de découvrir l'adresse MAC d'une station dont on connaît l'adresse IP
- Dans certains cas, l'inverse est également intéressant : certaines stations « disk-less » doivent demander au réseau l'attribution d'une adresse IP, connaissant leur adresse MAC.

# RARP

- RARP (Reverse Address Resolution Protocol) assure cette fonction.
- RFC 903
- Une station effectue une requête RARP en broadcast avec sa propre adresse MAC.
- Le serveur RARP répond en donnant l'adresse IP qu'il souhaite attribuer à cette station

# RARP



## RARP

- Inconvénient :
  - Le broadcast est effectué en plaçant tous les bits de l'adresse de destination à 1.
    Une telle frame ne traverse pas le routeur qui délimite le segment de la station émettrice.
  - En conséquence, il faut un serveur RARP par segment de réseau.

## BOOTP

- BOOTP (Bootstrap) contourne l'inconvénient de RARP en utilisant des messages UDP pour effectuer les requêtes.
- Dès lors, les routeurs peuvent être franchis.
- RFC 951, 1048, 1084

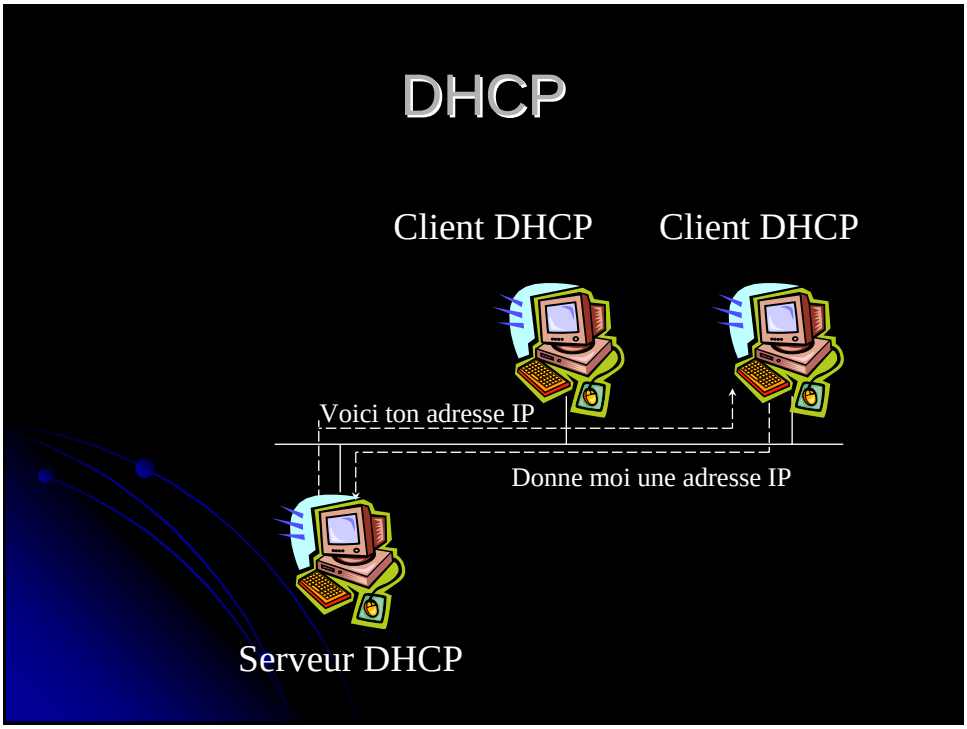
## BOOTP

- Inconvénient :
  - Sur le serveur BOOTP, chaque station doit être décrite sous la forme :
    - Adresse ethernet -> Adresse IP
  - La gestion d'une telle table est source de lourdeur et de risque potentiels de mauvaise configuration.

## DHCP

- En répondant à ce dernier inconvénient, le protocole BOOTP a changé de nom : DHCP (Dynamic Host Configuration Protocol).
- Basé sur RFC 2131 et RFC 2132
- Le fonctionnement est basé sur le mode client – serveur.

# DHCP




# DHCP

- Un serveur DHCP peut envoyer des informations diverses :
  - adresse IP
  - masque de sous-réseau
  - valeurs optionelles :
    - routeur par défaut
    - serveur(s) DNS
    - options spécifiques au client.

# DHCP

- Lorsque l'attribution d'adresses se fait automatiquement, il faut s'assurer que les adresses qui ne sont plus utilisées sont restituées au serveur.
- Pour assurer cela, on utilise le mécanisme du bail (leasing)
- Chaque adresse est « prettée » pour une certaine période. A la fin de cette période, elle peut être renouvelée ou remise à disposition.

# DHCP

- **Il existe plusieurs formes de requêtes DHCP :**
  - **DHCPDISCOVER** (pour localiser les serveurs DHCP disponibles)
  - **DHCPOFFER** (réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres)
  - **DHCPREQUEST** (requête diverse du client pour par exemple prolonger son bail)
  - **DHCPACK** (réponse du serveur qui contient des paramètres et l'adresse IP du client)
  - **DHCPNAK** (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
  - **DHCPDECLINE** (le client annonce au serveur que l'adresse est déjà utilisée)
  - **DHCPRELEASE** (le client libère son adresse IP)
  - **DHCPINFORM** (le client demande des paramètres locaux, il a déjà son adresse IP)

# DHCP

Le serveur envoie une proposition au client

Client DHCP

Client DHCP

DHCPOFFER
IP : 158.64.76.4
Mask : 255.255.255.0
Lease : 48h
Mac client : 00-10-C6-2A-C8-AC
IP Server : 158.64.76.1

DHCPDISCOVER
Source : 0.0.0.0
Destin. : FF.FF.FF.FF

Le poste client demande une adresse IP au(x) serveur(s) DHCP

Serveur DHCP

# DHCP

Le serveur confirme l'attribution de l'adresse

Client DHCP

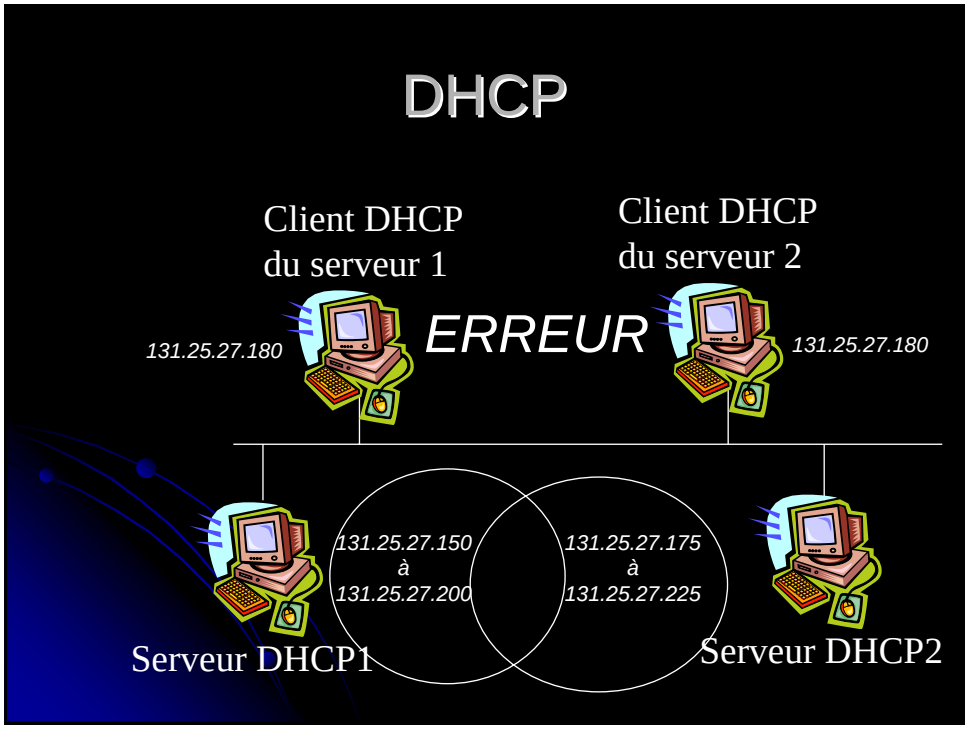
Client DHCP

DHCPACK
IP : 158.64.76.4
Mask : 255.255.255.0
Lease : 48h
Mac client : 00-10-C6-2A-C8-AC
IP Server : 158.64.76.1

DHCPREQUEST
Source : 0.0.0.0
Destin. : FF.FF.FF.FF
IP : 158.64.76.4
…

Le poste client accepte la première proposition qu'il a reçue en informant tous les serveurs.

Serveur DHCP


DHCP
Client DHCP
du serveur 1
Client DHCP
du serveur 2
131.25.27.180
ERREUR
131.25.27.180
131.25.27.150
à
131.25.27.200
131.25.27.175
à
131.25.27.225
Serveur DHCP1
Serveur DHCP2