Niveau Réseau
"Network Layer"

Le protocole IP
"Inter-network Protocol"

Introduction.

IP version 4.

IP version 6.

Routage IP et protocoles annexes.

Conclusion.

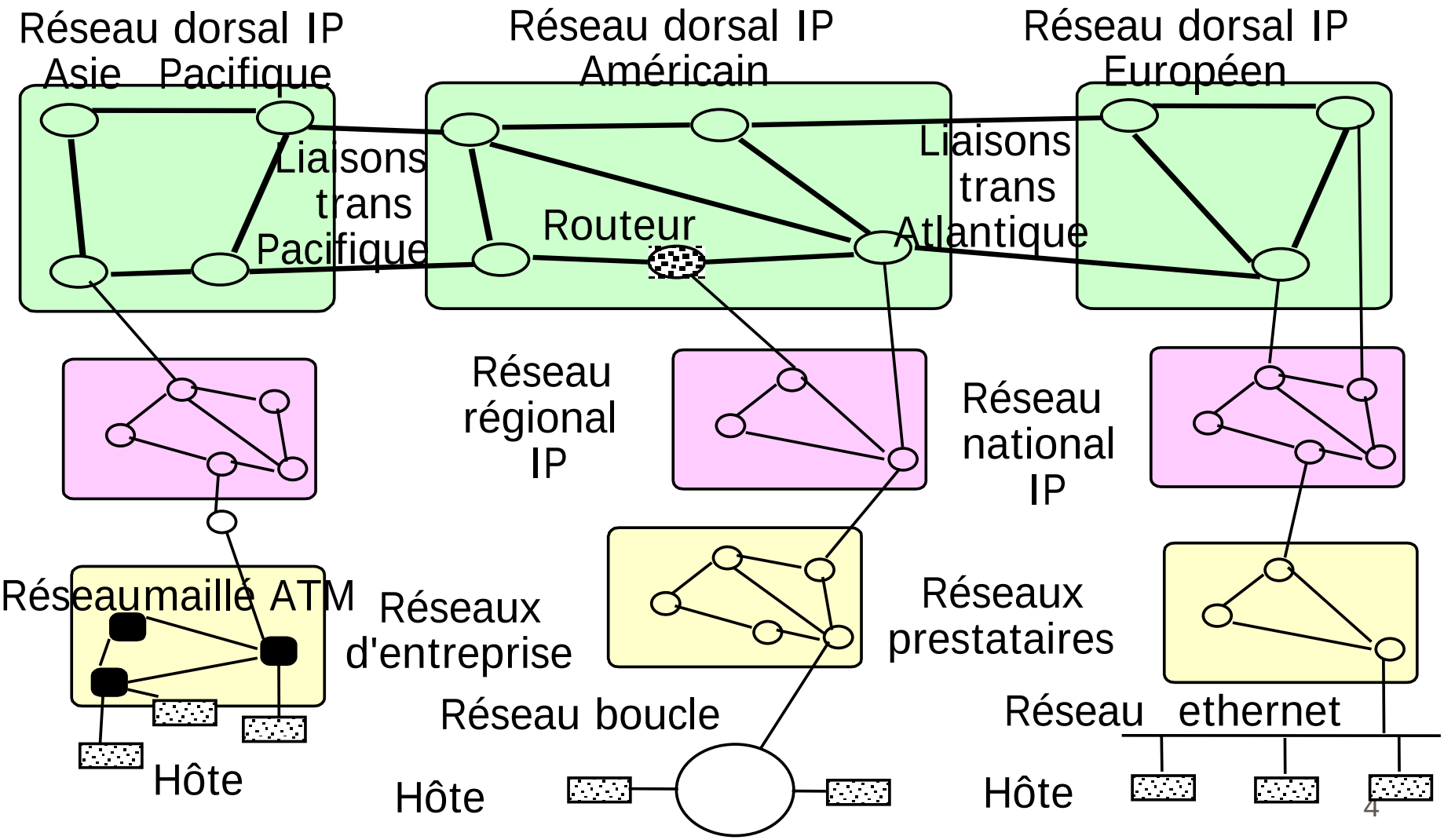
IP

Introduction - Généralités

Objectifs généraux de IP

- **IP : un réseau de réseaux**.
  - Protocole d'interconnexion de réseaux locaux ou généraux.
- **Fonctionnement en mode datagrammes** (pas de circuits virtuels).
- **En version de base pas de qualité de service temporelle**
  - **Fonctionnement au mieux ("best effort")**
  - **Existence de protocoles additionnels** pour la qualité de service.
- **Recherche d'une optimisation globale** des infrastructures de communication disponibles.
- **Robustesse** d'acheminement.
  - Reconfiguration automatique en cas de panne.

IP: un réseau mondial de plus en plus hiérarchisé

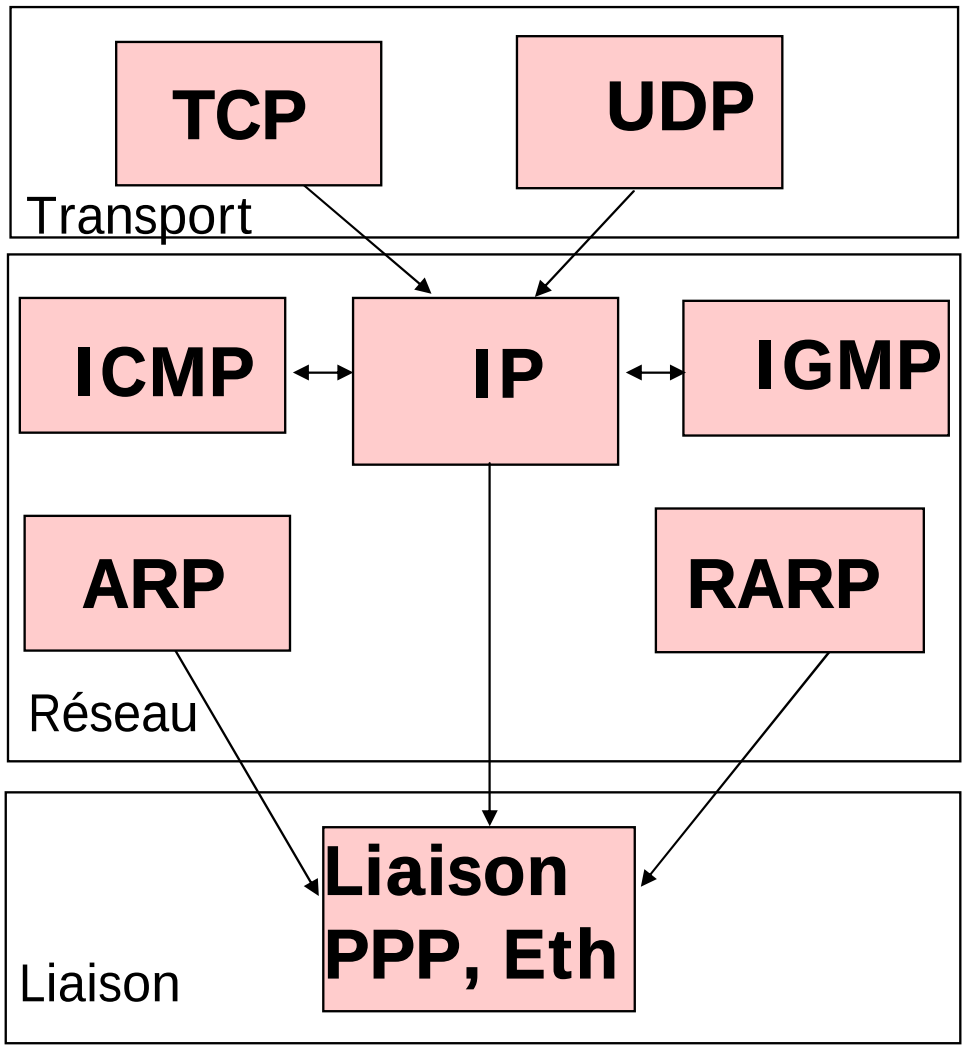


Fonctions réalisées par IP

- **Communications au niveau 3 sans connexion.**
  - Fonction de routage
  - Mode datagramme (pas d'information d'état).
- **Adressage universel.**
  - Assurant l'accès à n'importe quel type d'hôte.
- **Communications sans contrôle d'erreur, de flux, de séquence.**
  - Mode datagramme : envoi de paquets **sans contrôle.** Quelques cas d'erreurs sont détectées (sur l'entête, insuffisance de tampons) IP transmet un paquet ICMP**.**
  - => Contrôle d'erreur, de flux ... à la charge de TCP.
- **Fragmentation / Réassemblage.**
  - Adaptation de la taille des datagrammes aux possibilités offertes par les différentes couches liaisons.

La suite des protocoles TCP/IP en version 4

Diagramme des principaux protocoles en version 4



Définition simple des différents modules

- **ICMP : "Internet Control Message Protocol"**
  - Fonctions annexes au routage et traitement d'erreurs.
- **IGMP : "Internet Group Management Protocol"**
  - Gestion des groupes pour la diffusion.
- **ARP, RARP** : **"Address Resolution Protocol" , "Reverse Address Resolution Protocol "**
  - Correspondance d'adresses liaison et d'adresses IP.
- **Couche liaison** (encapsulation des paquets IP).
  - Sur liaison point à point : **"PPP Point to Point Protocol"**
  - Sur réseaux locaux : **Ethernet/DIX, "LLC/SNAP Logical Link Control/Sub Network Access Protocol".**

IP : Historique

- **Travaux sur les réseaux**: Protocole TCP -> Nombreux contributeurs (Article IEEE 1974 TCP Vinton Cerf, Robert Kahn) mais aussi Jon Postel : adoption RFC **IP** (RFC 760 janvier 1980)
- **Protocole IP** : séparé de TCP, Codage à partir de 1978.
- **Différentes améliorations** : **Stabilisation => IP Version 4 (RFC 791** septembre 1981**)**.
- **Diffusion significative :** à partir du début des années 1980.
- **Grande importance du couple UNIX-TCP/IP** : ensemble cohérent permettant de faire du réseau à coût raisonnable (UNIX Berkeley sur DEC/VAX 1983 - Université de Californie).
- **Développement des protocoles annexes**: protocoles de routage, support de la qualité de service, de la sécurité .....
- **Restructuration importante** de l'adressage pour suivre le développement mondial: **toujours en cours IP V6** (1995).

Le contrôle de l'Internet : Principaux organismes

- **ISOC "Internet Society"**
  - Organisation principale chargée de la croissance, de l'évolution technique, des aspects sociaux, politiques, …
- **IAB "Internet Architecture Board"**
  - Définition de l'architecture du réseau et de ses protocoles. Arbitrage des conflits.
- **IESB "Internet Engineering Steering Group"**
  - Administre les normes sur proposition de l'IETF.
- **IETF "Internet Engineering Task Force"**
  - Définition, expérimentation des protocoles, groupes de travail par domaines.
  - **RFC "Request For Comments" :** normes de l'Internet.
- **IRTF "Internet Research Task Group"**
  - Recherche à long terme.

Le contrôle de l'Internet : Gestion des noms, adresses et paramètres

- **IANA "Internet Assigned Number Authority"**
- **Puis ICANN "Internet Corporation for Assigned Names and Numbers"**
  - **Organisme chargé de l'affectation** des adresses, mot-clés, paramètres, ... pour l'ensemble des protocoles Internet
  - **Politique de gestion** : adresses, noms de domaines, définition des MIB ("Management Information Base")... etc
- **Délégation de certains responsabilités** (espace d'adresses)
  - **Amérique : INTERNIC** "Internet Network Information Center".
  - **Europe : RIPE NCC** "Réseaux IP Européens Network Computing Center"
  - **Asie : APNIC** "Asia Pacific Network Information Center".

IP

Chapitre I
Le protocole IP en version 4

Structure des datagrammes

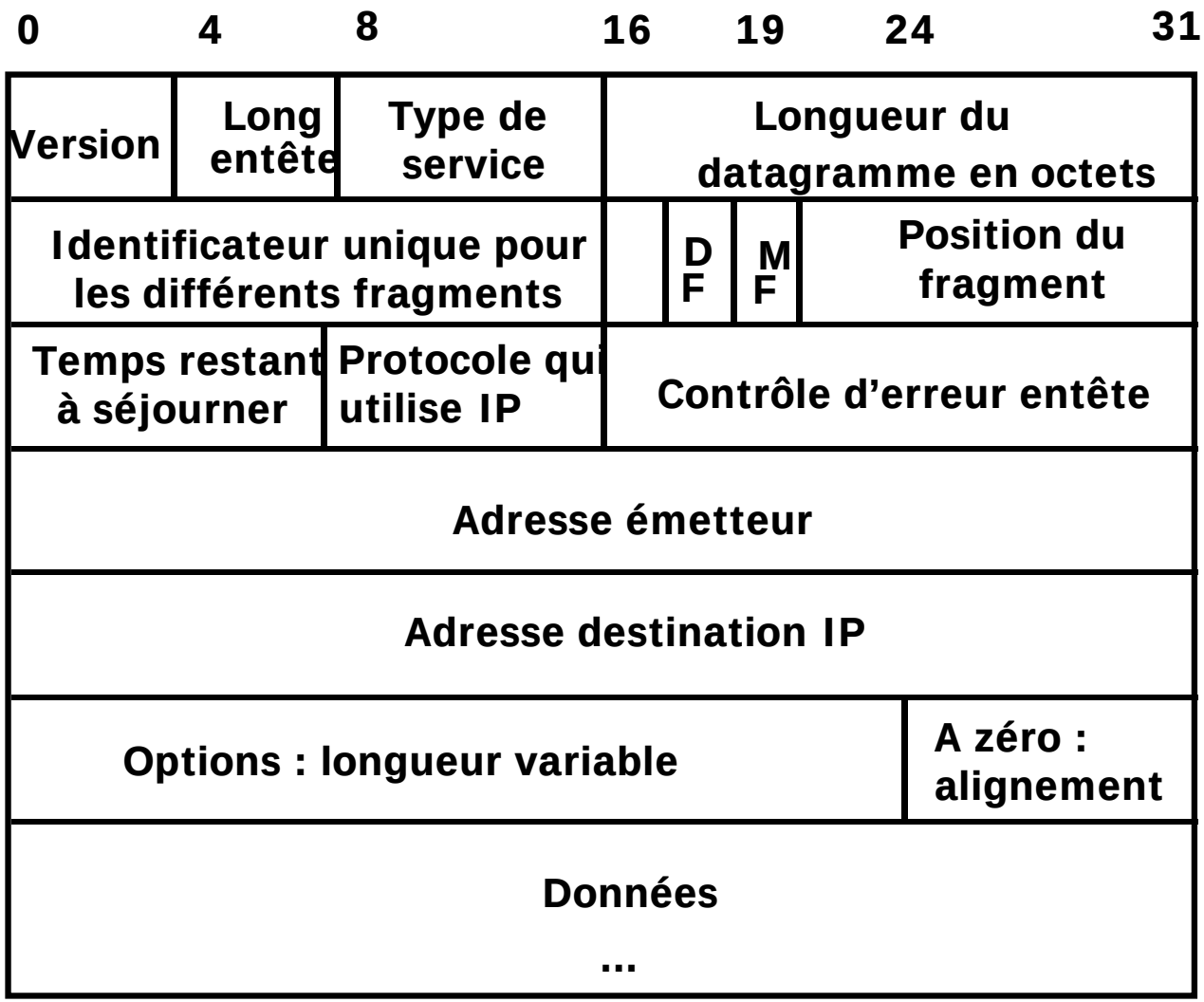
Fragmentation

Adressage

IP Version 4

I.1
Structure des datagrammes

Format du datagramme IP V4



Convention :
Transmission grand boutiste 'big endian'
Le bit 0 est envoyé en tête.

Détail des différents champs (1)

- **Numéro de version IP** "IP version number" : **4 bits** Ici IP v4
- **Longueur de l'entête** "IP Header Lenght" : **4 Bits**

  Longueur de l'entête en mots de 32 bits (Min 5 -> Max 15)

  Option: au plus 40 octets (entête standard 20 + option = 60).
- **Type de service** TOS "Type Of Service") : **8 bits**

  Qualité de service

00	**01**	**02**	**03**	**04**	**05**	**06**	**07**
Precedence			D	T	R	M	

- 3 bits ("Precedence") Priorité 0 normal à 7 contrôle réseau

- 4 bits indicateurs ("Flags" D T R M) + Un bit inutilisé

D "Delay" minimiser le délai T "Throughput" maximiser le débit

R "Reliability"max de fiabilité M "Monetary" min de coût

Redéfinition du TOS : QOS Multimédia => Diffserv.

Détail des différents champs (2)

- **Longueur datagramme (16 bits)** "Total lenght"

  . Longueur totale du datagramme en octets incluant entête et données => Longueur au maximum 65535.
- **Identificateur unique (16 bits)** "Ident field"

  . Valeur entière utilisée pour regrouper les différents fragments d'un message fragmenté.

  . Un datagramme peut être fragmenté à l'émission: un routeur qui détecte qu'un datagramme est trop long pour la voie de sortie le fragmente.
- **Ne pas fragmenter (1 bit)** DF "Don't Fragment"

  . Le datagramme même ne doit pas être fragmenté.

  . Le destinataire ne peut traiter les fragments.

  Ex : téléchargement de code en une fois.

Détail des différents champs (3)

- **Dernier fragment MF** "More Fragment" **: 1 bit.**

  . Indique le dernier fragment d'un message fragmenté (0)

  . ou un fragment courant (1).

- **Position du fragment** "Fragment Offset" **: 13 bits.**

  . Détermine la position d'un fragment dans un message (8192 fragments possibles).

  . Chaque fragment sauf le dernier comprend un nombre entier de groupes de 8 octets.

- **Temps restant à séjourner TTL** "Time To Live“ : **8 bits**

  . Ancienne version (RFC 791) :Mesure du temps de séjour dans le réseau en secondes depuis l'émission (255 s max).

  . Actuellement: Initialisé à une valeur entière (par ex 30).

  Décrémenté par chaque routeur => Le paquet est détruit lorsque le compteur passe à zéro (pour éviter les boucles).

Détail des différents champs (4)

- **Protocole utilisateur "Protocol" : 8 bits**

  . Protocole qui utilise IP. Nombreuses valeurs normalisées pour le démultiplexage des paquets entrants

  . Exemples ICMP=1, TCP=6, UDP=17

- **Contrôle d'erreur entête** "Header Checksum" **: 16 bits**

  . Contrôle d'intégrité sur l'entête du paquet.

  . Un paquet d'entête erronée est détruit pour éviter des erreurs de délivrance.

Méthode de calcul

- L'entête est considérée comme une suite de mots de 16 bits.
- On fait la somme des mots de 16 bits en complément à 1.
- On prend le complément à 1 du résultat.

=> A chaque traversée de commutateur: comme il n'y a que la zone TTL qui change de un, le calcul de la nouvelle somme de contrôle est simple.

Détail des différents champs (5)

- **Adresse source** "Source address" **: 32 bits**

  . Adresse IP de l'émetteur.

- **Adresse destination "**Destination address" **: 32 bits**

  . Adresse IP du destinataire.

- **Données "Data"**

. Zone de donnée utilisateur d'une taille maximum de 64 K octets.

Zone des options

- **Utilisée pour spécifier des compléments de protocole** qui n'ont pas à être toujours présents.
- **Utilisation des options** : beaucoup moins forte en IPV4 qu'en IPV6.
- **Longueur variable** : de 4 à 40 octets.
- **Alignement sur des frontières de mots de 32 bits** => Bourrage si le dernier mot n'est pas complètement utilisé.
- Les options **ne sont pas toutes traitées** par certains routeurs.

Les cinq classes d'options en IPV4

- **Protocoles de sécurité : IPSEC** "IP Security"
- **Enregistrement** de la route suivie "Record Route".
- **Enregistrement de la route et estampillage** par la date de traversée de tous les routeurs "Record and Timestamp".
- **Routage par la source non contraint** "Loose Source Routing" : définition d'une liste partielle de routeurs devant être visités.
- **Routage par la source contraint** "Strict Source Routing" : liste stricte des routeurs à visiter.

IP Version 4

I.2
Fragmentation
(ou segmentation)

Solutions pour la fragmentation (Segmentation)

- **Objectif: adapter la taille des datagrammes** à la taille maximum des trames de liaison (taille médium).
- **MTU** (‘Maximum Transfer Unit’) : pour une voie donnée la taille maximum des trames (souvent 1500 octets Ethernet).

Solutions de fragmentation non retenues en IP V4.

- **Fragmentation transparente 1 = fragmentation et réassemblage pour chaque saut** : le routeur émetteur sur une voie fragmente si nécessaire et le routeur destination réassemble s’il y a eu fragmentation.
- **Fragmentation transparente 2 = fragmentation de bout en bout** : on ne fragmente qu’à l’entrée du réseau et on ne réassemble qu’à la sortie => implique l’apprentissage du MTU de chemin (path MTU) plus petit MTU d’un chemin.

Fragmentation en IP V4 : Une fragmentation non transparente

- **Pour un réseau donné** (une voie de communication) un émetteur (ou un routeur) fragmente un datagramme si nécessaire et les **fragments poursuivent** jusqu'au destinataire qui est le seul à réassembler.
- **Il peut donc y avoir plusieurs fragmentations successives sans réassemblage** (sauf au terme).

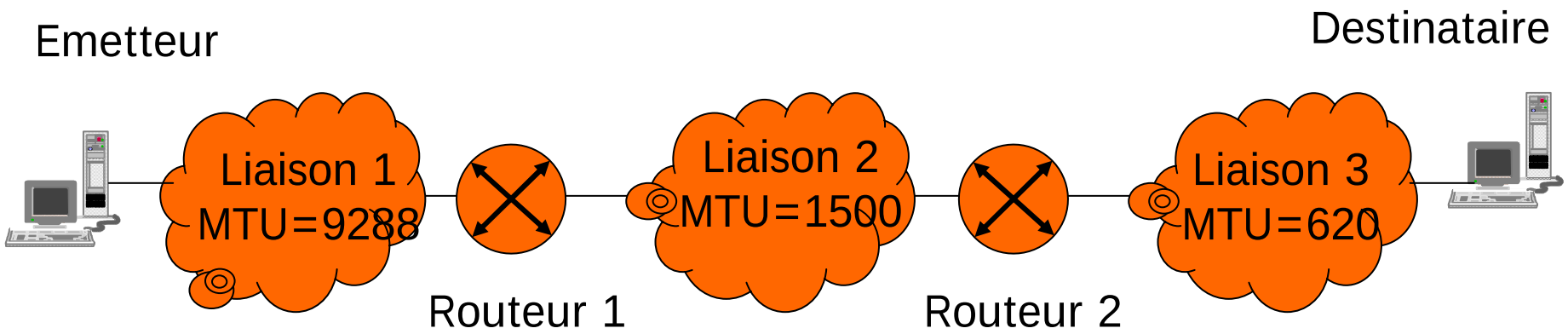
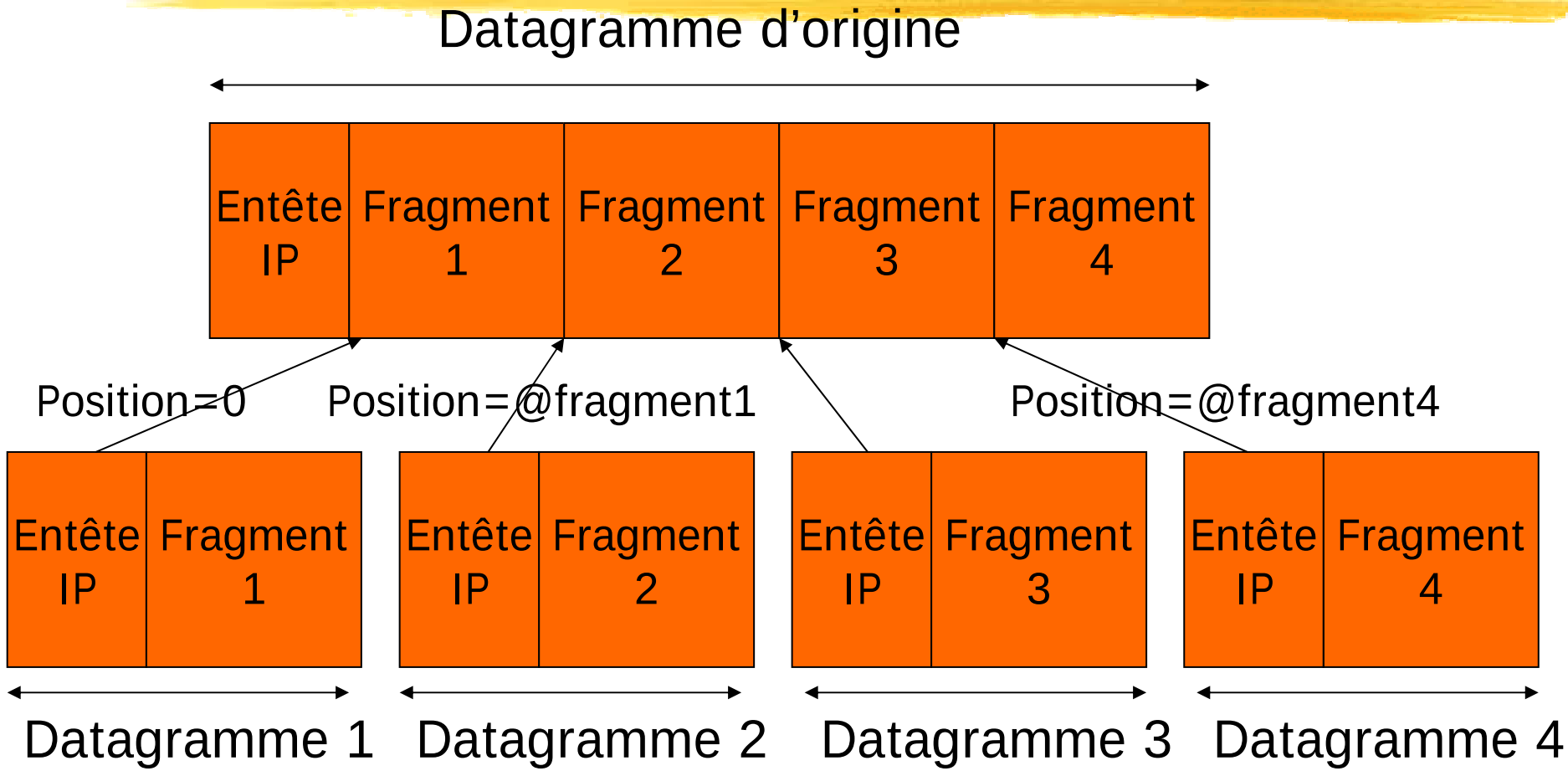


Schéma général de la fragmentation



Suite des datagrammes associés à une fragmentation :
la position (offset) permet de reconstruire le datagramme d'origine

Fragmentation IP V4 : exemple d'école de fonctionnement

- **Datagramme à fragmenter**

I=3204	P=0	M=0	L=41	Message A Transmettre

- **Après fragmentation pour un MTU=28**

I=3204	P=0	M=1	L=28	Message

I=3204	P=1	M=1	L=28	A transm

I=3204	P=2	M=0	L=25	ettre

- **Entête IPV4** : informations pour la fragmentation

  I : Identificateur de fragment. P : Position d'un fragment dans le datagramme origine (offset). M : Indicateur dernier fragment ('more'). L : Longueur du datagramme (avec entête 20 octets).

- **Attention** : P la position ('offset') est en multiple de huit octets.

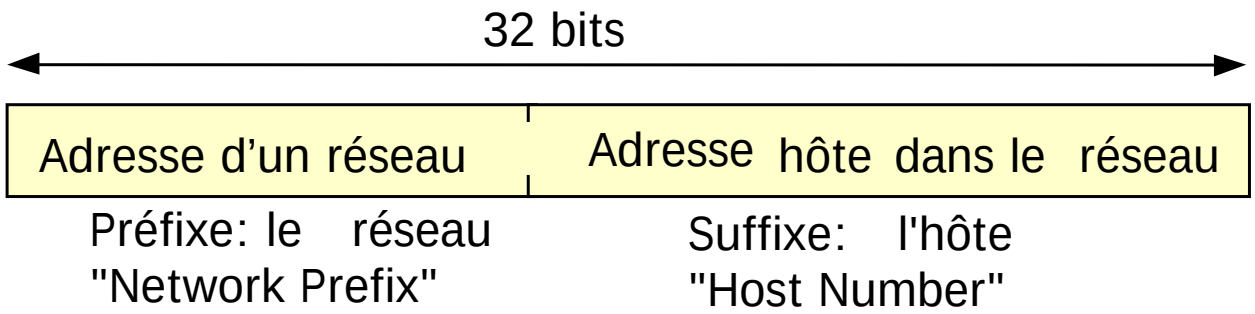
IP Version 4

I.3
Adressage

A) Par classes (‘Classfull’)
B) Avec Sous réseaux (‘Subnetting’)
C) Avec masque variable (‘Variable lenght mask’)
D) Sans classes (‘Classless’)
E) Mécanismes additionnels

Introduction : Adressage dans IP un réseau de réseaux

- **Toute machine connectée à IP appartient à un réseau**
  - Notion d'adresse de réseau et d'adresse hôte à l'intérieur d'un réseau



- **Cadre général de l'adressage IPV4**

  - **Adressage uniforme au moyen d'adresses universelles sur 32 bits** - 4 octets.

  - **Notation "Décimale Pointée"** ('dotted decimal') 4 octets d'une adresse : a.b.c.d Exemple d'adresse: 192.200.25.1

  - Transmission des adresses : **grand boutiste (big endian)**

Evolution de l'adressage IP

- **Améliorations** successives pour faire face:

  - Demande d'adresses IP à satisfaire (croissance très rapide).

  - Nombre de réseaux IP également en croissance : taille des tables de routage.

- **Solution : Hiérarchiser de plus en plus** l'adressage en relation avec le routage => Quatre étapes successives.
  - **Hiérarchisation à deux niveaux :**

  Adressage par classes 'Classfull'
  - **Hiérarchisation à trois niveaux :**

  Adressage IP par sous réseaux 'Subnetting'
  - **Hiérarchisation complète à n niveaux de l'adresse d'hôte:**

  Adressage IP avec masque variable VLSM ('Variable lenght Subnet mask')
  - **Hiérarchisation complète à n niveaux de l'adresse IP**

  Adressage IP sans class CIDR ('Classless Inter Domain Routing').

Utilisation des adresses IP dans le routage

- **Table de routage (ensemble de routes)**

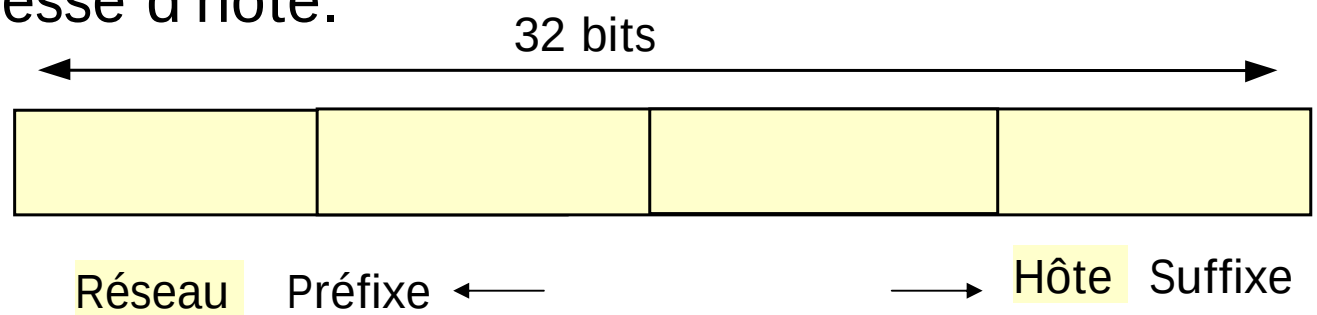
Adresse destination	Différents champs	Direction d'envoi
163.173.0.0 (réseau)	xxxxxxxxxxxxxxx	/dev/eth0
.....	.....	.....

- **Datagramme à router**
  - Adresse destination e.g.h.i (par ex 136.173.36.60).
  - A partir du préfixe détermination de l'adresse réseau par application d'un masque (adresse avec un préfixe de bits à 1 par exemple 16 bits à 1 soit 255.255.0.0)

    => adresse réseau 136.173.0.0.
  - Comparaison de l'adresse réseau de destination avec les destinations des différentes routes dans la table.

A) L'adressage IP V4 par classes "IP Classfull" RFC 791 (1981)

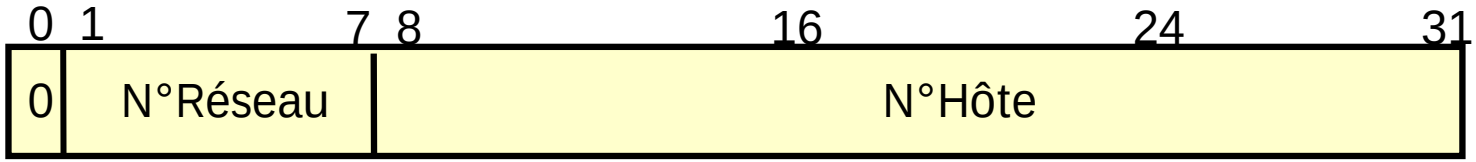
- **Hiérarchisation de base des adresses avec deux niveaux**
- **Réseaux de types et de tailles très différentes**: idée de distinction de trois classes A, B, C selon les tailles de réseau => Trois frontières différentes entre adresse de réseau et adresse d'hôte.



- **Une répartition des adresses entre les trois classes** qui permet automatiquement de déterminer la classe (la taille du préfixe) => donc de trouver l'adresse du réseau d'appartenance (par analyse de l'octet de fort poids).

Classe A : Grands réseaux

- Préfixe sur 8 bits, suffixe sur 24 bits.
- 126 Réseaux de 16777214 = 2**24 -2 hôtes.
- La moitié de l'espace d'adressage.



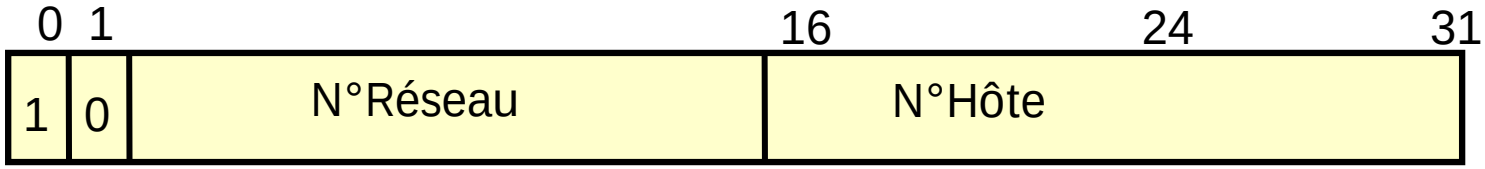
N°de Réseau: a de 1 à 126 (0 et 127 sont réservés).

N°d'hôte: a.0.0.0 et a.255.255.255 réservés.

- Plan d'adressage réservé aux très grands groupes => gestion stricte.

Classe B : Réseaux moyens

- Préfixe sur 16 bits, suffixe sur 16 bits.
- 16384 Réseaux de 65534 = 2**16 -2 hôtes.
- Le quart de l'espace d'adressage.



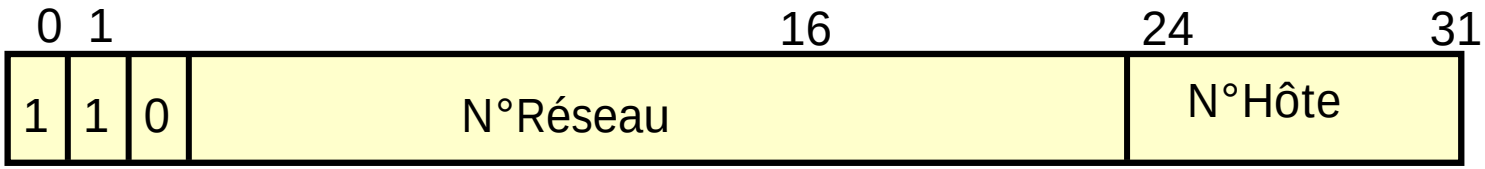
N°de Réseau: a.b de 128.0 à 191.255.

N°d'hôte: 1 à 65534 (a.b.0.0 et a.b.255.255 réservés)

- Plan d'adressage pour entreprises moyennes => gestion laxiste au départ.

Classe C : Petits Réseaux

- Préfixe sur 24 bits, suffixe sur 8 bits.
- 2097152 Réseaux de 254 = 2**8 - 2 hôtes.
- Le huitième de l'espace d'adressage.



N°de Réseau: a.b.c de 192.0.0 à 223.255.255

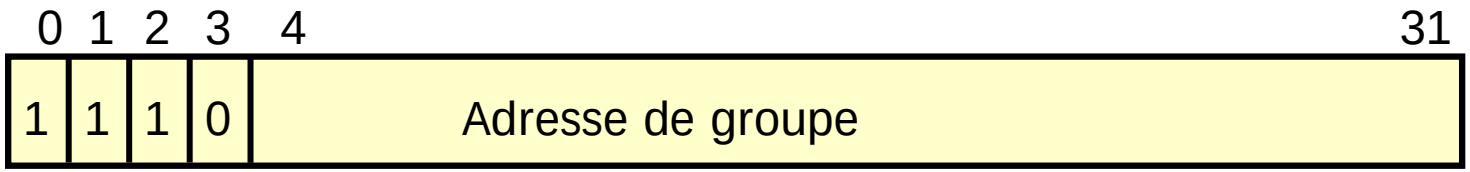
N°d'hôte: 1 à 2544 (a.b.c.0 et a.b.c.255 réservés)

- Plan d'adressage peu demandé au départ

=> utilisation avec la croissance du réseau.

Adresses de classe D : Diffusion sur groupe ("Multicast" IP)

- **Préfixe 4 bits 1110**, suffixe 28 bits: identifiant de groupe (adresse) de diffusion.
- Adresses de 224.0.0.0 à 239.255.255.255



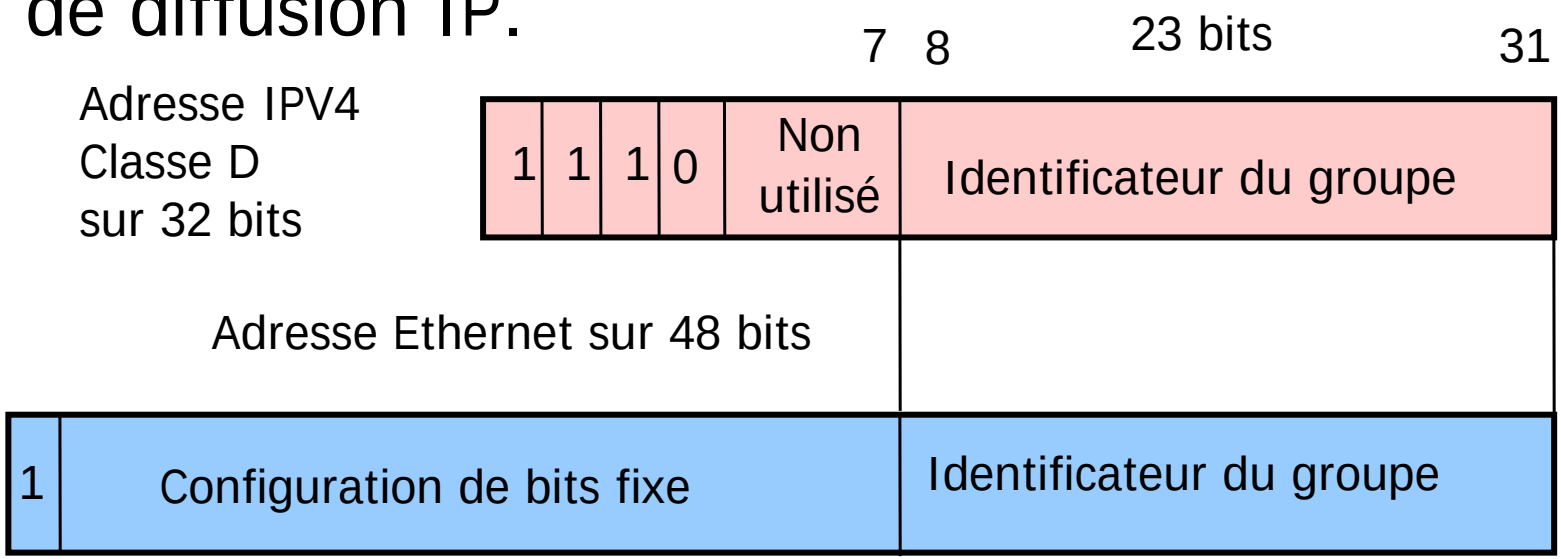
- **Groupes permanents 224.x.y.z (224/8)**

  224.0.0.2 tous les routeurs d'un sous-réseau

  224.0.1.1 groupe "Network Time Protocol"
- **Autres groupes** non permanents : 225 à 239.
- **Pour mémoire classe E** : Réservée Préfixe 11110

Adresses de classe D : Diffusion sur IP et sur Ethernet

- **Transformation** d'une adresse de groupe IP en une adresse de groupe Ethernet.
- **Pour déterminer automatiquement** une adresse de diffusion Ethernet à partir d'une adresse de diffusion IP.



Adresses particulières IPV4 : Adresses point à point (RFC 1340)

- **Adresse point à point ('unicast'):** atteindre un seul destinataire.
- **Adresse destination dans un réseau : une adresse de destination dans une table de routage (atteindre un hôte dans un réseau)**

  - On note le préfixe adresse de réseau suivi de 0 en partie hôte (xyz.00).

  - Autre notation la notation a.b.c.d/n (/n indique un préfixe sur n bits)

    Exemple: a.b.0.0 <=> a.b.c.d/16

  - 0.0.0.0 : L'Internet => l'adresse **destination** par défaut (atteindre un hôte qui se trouve dans l'Internet).
- **Adresse destination moi-même (l'hôte courant): 127/8**

  - 127/8 Comme adresse de destination le même hôte (pour permettre à deux utilisateurs sur le même site de communiquer par IP).

  - Adresse de rebouclage "Loopback"

  - Toutes les adresses classe A "127.a.b.c" sont affectées à cette fonction.

  => Utilisation habituelle de l'adresse : 127.0.0.1 ("localhost").
- **Adresse source moi-même (l'hôte courant): 0.0.0.0 ou 000.xyz**

  - **0.0.0.0 : Adresse source** d'une station qui ne connaît pas son adresse (utilisable également 000.xyz l'hôte xyz dans son réseau).

Adresses particulières v4 : Adresses de diffusion générale

- **Idée de diffusion générale ('Broadcast') :** atteindre tous les hôtes d'un réseau IP donné.
- **En IPV4 pour construire une adresse de diffusion : mettre** des 1 partout dans la partie adresse hôte.
- **Cas de l'adressage par classe : Adresses destination: a.255.255.255 , a.b.255.255 et a.b.c.255:**

  Diffusion à tous les hôtes du réseau a.0.0.0 (classe A) ou a.b.0.0 (classe B) ou a.b.c.0 (classe C)
- **Cas particulier : Adresse dest 255.255.255.255**

  - Idée naturelle au départ diffusion à tout l'Internet

  => abus.

  - Ensuite diffusion limitée au sous-réseau de l'hôte émetteur (non délivré hors du contexte local).

Conclusion : Adressage IPV4 par classes

- **Gaspillage d'adresses dans les années 1980.**

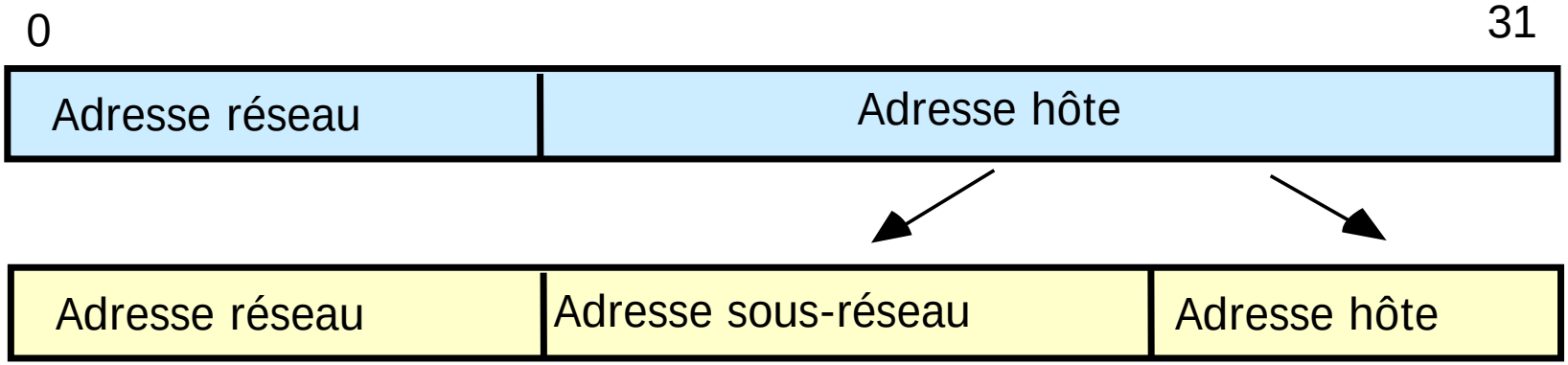
  - L'espace d'adressage paraissant très suffisant,
  - Le réseau était confidentiel

  => Les adresses ont été distribuées sans prévoir.
- **Les besoins exprimés par les entreprises** sont souvent supérieurs à la classe C sans justifier la classe B

  Si attribution de plusieurs classes C : gonflement des tables de routage **=> Attribution de classe B**
- **L'adressage IPV4 par classes sur 32 bits** (4 294 967 296 adresses) **est devenu tout à fait inadapté**
- **Mais les attributions anciennes ont été préservées** dans les plans d'adressages ultérieurs.

B) Adressage par sous-réseaux “IP Subnetting” RFC 950 (1985)

- **Hiérarchisation à trois niveaux:**
  - Possibilité offerte de structurer l’espace d'adressage interne à un réseau de classe A, B ou C en deux niveaux
  - Trois notions : réseau, sous-réseau et hôte.



- **Pour quoi faire** :
  - Mieux structurer un espace d’adressage interne.
  - Sans impact sur l’Internet mondial.
  - Eviter des demandes de blocs d’adresses

Adressage par sous-réseaux : Notion de masque ("Subnet Mask")

- **Souplesse souhaitée**: La frontière entre adresse sous-réseau et adresse d'hôte est variable selon les besoins de l'entreprise (définie par l'administrateur du réseau).
- **Nécessité de fournir** le découpage retenu à chaque machine d'un sous réseau et aux routeurs.
- **Le masque :** permet le filtrage des adresses destination pour trouver l'adresse du sous-réseau d'appartenance.
- **C'est une configuration de bits à 1 que l'on applique en et logique** sur une adresse IP pour sélectionner la partie adresse réseau + sous réseau
- **Exemple** un réseau de classe B : 135.28/16
  - On souhaite le découpage de l'espace interne 10 bits pour l'adresse de sous-réseau et 6 bits pour l'adresse d'hôte :
  - Valeur du masque : **255.255.255.192 ou en notation de** préfixe étendu ***/26*** (ou encore en héxadécimal 0xFFFFFFC0).

Conclusion IPV4 et les sous-réseaux

Avantages

- **Les tables de routages de l'Internet ne croissent pas en taille** (seuls les routeurs internes gèrent les sous-réseaux)
- **L'espace d'adressage privé est mieux géré** (lors de la création de nouveaux réseaux on évite de demander des adresses).
- **Si un réseau modifie sa structure interne il n'est pas nécessaire de modifier les routes** dans l'Internet

Inconvénients

- **Il faut gérer le masque** en plus de l'adresse.
- **On ne définit qu'une seule façon de hiérarchiser** les adresses : **rigidité du découpage** (un seul pour toute l'entreprise => difficile à changer).

C) Masques de longueur variable VLSM Variable Length Subnet Mask

- **Besoin: créer des sous réseaux de taille différente.**

Exemple

- Classe B 135.8.0.0/16 découpé par le masque 255.255.254.0 ou /23 (soit 2**7 = 128 sous-réseaux de 2**9 – 2 = 510).
- Il se créé un nouveau sous_réseau de 15 hôtes (extension prévisible à 50).
  - Si on lui attribue une adresse de sous-réseau /23 on va perdre environ 500 adresses.
  - Il serait par contre très intéressant de lui attribuer une adresse /26 d'un sous réseau de 64 – 2 = 62 hôtes.

- **La solution : VLSM Variable Length Subnet Mask (RFC 1009 en 1987) :** masques de taille variable.

Problèmes posés par VLSM : 1) Gestion des masques

- **Chaque sous-réseau** possède sa propre **taille.**
  - Pour déterminer **correctement le numéro de réseau** quelque soit sa taille.
  - **Le protocole de routage interne doit utiliser un masque** (un préfixe étendu) différent pour chaque sous-réseau
  - **Il doit transférer ces masques dans chaque route.**

=> **Modifier les protocoles de routage**

- **RIP V2** (‘Routing Information Protocol’ RFC1388) La version 2 permet de déployer VLSM.
- **OSPF** (‘Open Shortest Path First’)

Problèmes posés par VLSM : 2) Correspondance la plus longue

- **Recherche de "correspondance la plus longue"** (‘Longest Match based forwarding algorithm’)
  - Au cas ou plusieurs routes sont dans une table,
  - La route de plus long préfixe est la plus précise
- **La route de plus long préfixe doit être sélectionnée et utilisée.**
- **Exemple :** datagramme vers l'hôte 136.1.6.5 avec 3 routes vers les destinations suivantes :
  - 136.1.0.0/16 : 10001000 00000001
  - 136.1.4.0/22 : 10001000 00000001 000001
  - 136.1.6.0/23 : 10001000 00000001 0000011

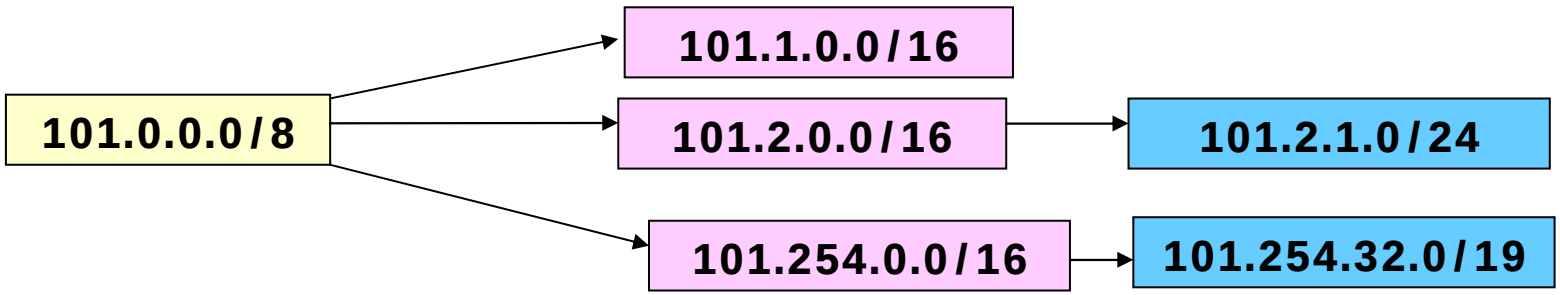
  =>Les trois routes conduisent au but

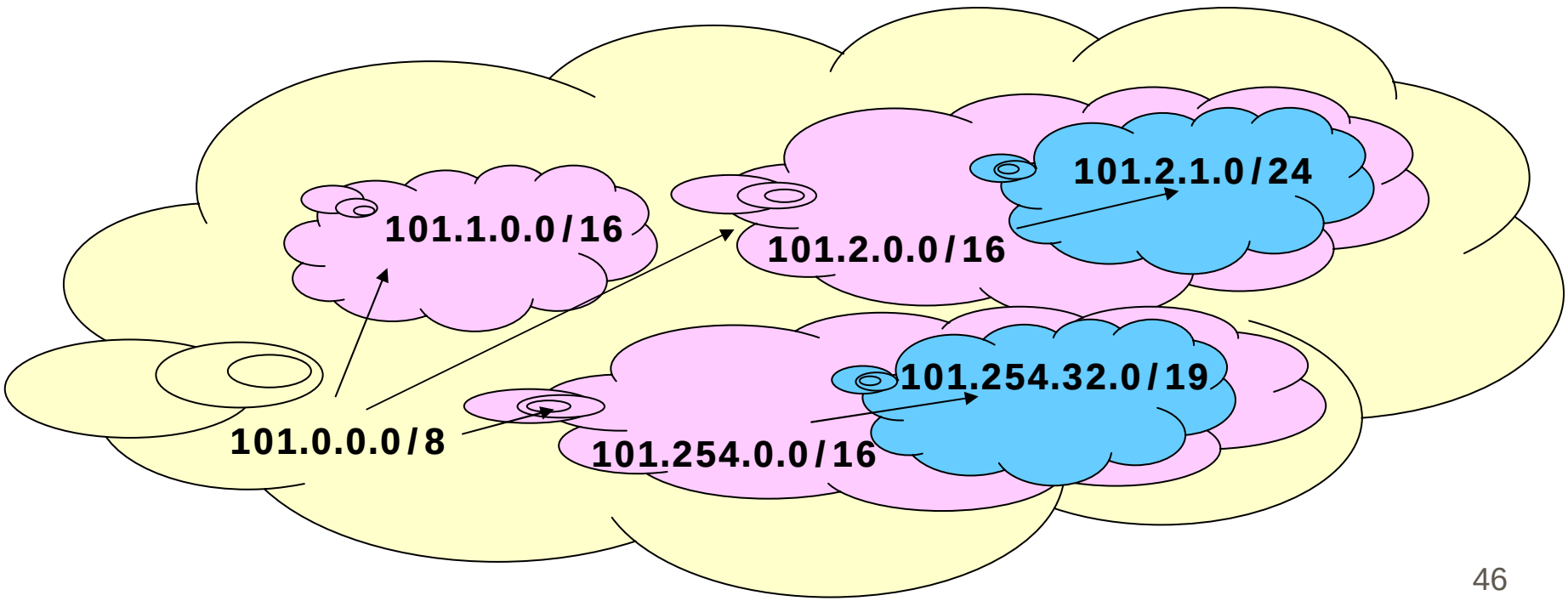
  =>Le routeur choisit la route 136.1.6.0/23.

Problèmes posés par VLSM : 3) Agrégation des routes

- **Déploiement d'un réseau VLSM => Pour l'agrégation des routes les adresses doivent être assignées 'topologiquement '.**
  - Les blocs d'adresses sont découpés hiérarchiquement.
  - Les blocs d'adresses sont attribuées selon la topologie du réseau
- **On réduit la quantité d'information dans les tables de routage** => on peut agréger en une seule route, les routes pour l'ensemble des blocs contenus dans un bloc destination.
- **On diminue le temps de recherche en table** => amélioration des performances du routage.

Exemple de gestion d'adresse avec agrégation 'topologique' en VLSM





Conclusion : IPV4 avec VLSM

Avantages

- **L'utilisation de plusieurs masques permet un usage plus efficace de l'espace d'adressage attribué à une organisation** : il n'est pas nécessaire de se conformer à la taille unique des sous-réseaux.
- **On réduit le volume des tables nécessaires au routage** au niveau dorsal ('backbone') d'une organisation.

Inconvénients

- **Nécessite l'adaptation des protocoles de routage** pour échanger les masques: RIPV1 -> RIPV2
- **Ne permet de structurer correctement que le domaine d'adresse privé** d'une organisation.

D) Routage sans classe : CIDR ‘Classless Inter Domain Routing’

- **Problème récurrent après 1990 (web) en IP v4:**
  - Saturation de l'espace d'adressage et croissance de la taille des tables de routage (aux plus haut niveaux).
- **Solution : Hiérarchisation complète des adresses V4.**

=> Extension de l’approche VLSM à tout l’espace d’adressage de l’Internet.

=>Suppression des frontières établies par l’adressage en classes (classless)

- **Prolongation importante de l’adressage V4.**
  - En améliorant l’utilisation des adresses encore disponibles.
  - En diminuant le volume des tables de routage par agrégation des routes.
- **Solution CIDR : RFC1517 à 1520 (1993).**

Contraintes pour le déploiement de CIDR

Hôtes et routeurs doivent supporter l'adressage CIDR et ses conséquences

- **Mêmes conséquences** que VLSM.
- **Les adresses de destination doivent être échangées** par les protocoles de routage avec leur préfixe (qui peut être de taille quelconque).
- **Les routeurs doivent implanter** un algorithme de "correspondance la plus longue".
- **Les adresses doivent être distribuées** sur une base topologique pour agréger les routes.

Distribution des adresses IP dans l'adressage sans classe

- **Attribution d'adresses par blocs** dont la taille est toujours sur **n bits soit 2^n adresses à chaque fois.**
- **L'utilisation d'un bloc d'adresses libres** de n bits doit correspondre à une adresse de réseau valide sur 32-n bits.
- **Notation en CIDR :**
  - Un bloc d'adresses en CIDR: 212.37.24.160/27
  - Utilisable comme une adresse de réseau:

    L'adresse de réseau en binaire :

    11010100.00100101.00011000.101 | 00000
  - Le masque comporte 27 bits à 1 en tête, et 5 bits à 0 à la fin.

    11111111111111111111111111 | 00000
  - On peut donc aussi noter le masque en notation décimale pointée :

    11111111.11111111.11111111.111 | 00000

    Soit : 255.255.255.224

Exemple de distribution

- **Construction d'un nouveau réseau IP** : comprenant environ 2000 adresses.
- **On doit attribuer un bloc de 2**11** : soient 2048>2000 adresses =>11 bits adresse hôte masque /21.
- **On dispose du bloc libre :** 194.16.32.0/19

  => On peut attribuer les blocs
  - Réseau (1) 194.16.32.0/21 ou 11000010 00010000 00100|000 00000000
  - Réseau (2) 194.16.40.0/21 ou 11000010 00010000 00101|000 00000000
  - Réseau (3) 194.16.48.0/21 ou 11000010 00010000 00110|000 00000000
  - Réseau (3) 194.16.56.0/21 ou 11000010 00010000 00111|000 00000000
  - Exemple: réseau (2) Première adresse d'hôte utilisable 194.16.40.1

    Dernière adresse 194.16.47.254
- **On ne peut pas faire d'autre choix** : car ce ne seraient pas des adresses de réseaux avec préfixe /21 sur 21 bits et suffixe sur 11 bits.

Application de CIDR : distribution des adresses de classe C restantes

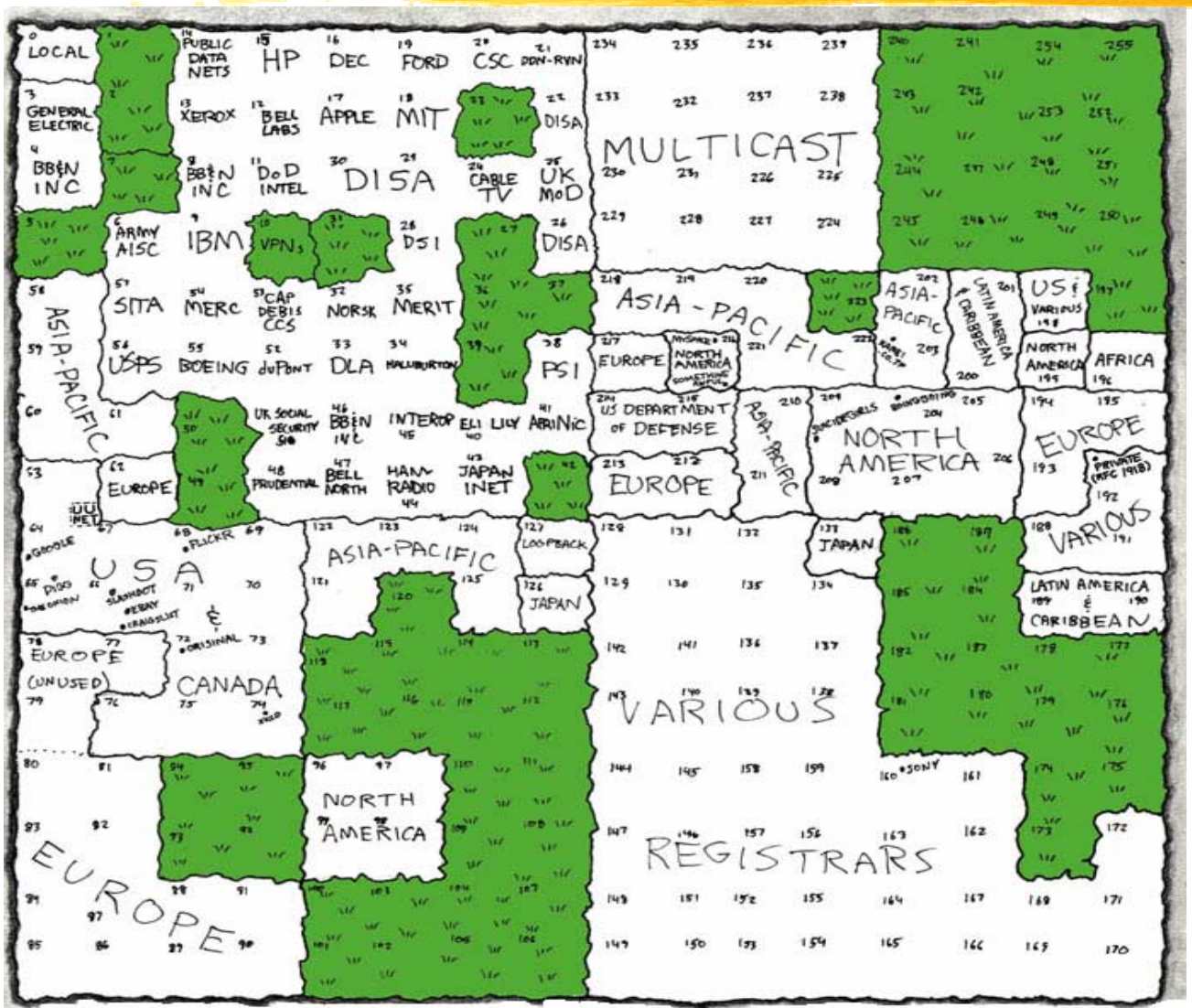
- **Adresses restantes** : dans la classe C (peu de demandes).
- **Solution d'administration**: séparer les classe C restantes en quatre catégories administrées par continent.
  - 194.0.0.0 - 195.255.255.255 Europe RIPE
  - 198.0.0.0 - 199.255.255.255 Amérique nord et sud ARIN
  - 200.0.0.0 - 201.255.255.255 //
  - 202.0.0.0 - 203.255.255.255 Asie Pacifique APNIC
- **Distributions indépendantes** par région de blocs de taille quelconque aux FAI.
- **Agrégation de routes**: une adresse 194.x.y.z doit être envoyée sur un routeur européen.

Conclusion IPV4 avec CIDR

- **CIDR alloue efficace des adresses v4**
  - CIDR permet de **coller** assez finement aux demandes.
  - **Récupération** d'anciennes adresses A, B ou C.
  - Un prestataire Internet ‘ISP’ **attribue librement** ses adresses.
  - La découpe peut opérer à tous les niveaux.
- **CIDR permet d'agréger les routes à tous les niveaux**
  - **Contrôle de la taille** des tables de routage.
  - **Facilite l'administration** des routeurs.

- **CIDR présente les inconvénients de la hiérarchisation**: Si une organisation souhaite changer de prestataire sans changer d’adresse on doit créer une route d’exception ce qui est coûteux (autre solution voir plus loin NAT).

Carte de l'Internet : occupation de l'espace IPV4 en 2006



Adressage IP Version 4

E) Mécanismes additionnels pour l'adressage (économiser et faciliter l'administration)

1. Liaisons dénumérotées
2. Adresses publiques et privées
3. Traduction d'adresses (NAT)
4. Distribution d'adresses (DHCP)

E1) Liaisons dénumérotées (RFC 1812)

- **Toute carte réseau est identifiée par une adresse IP unique.**
- **Pour une liaison point-à-point, il faut attribuer un numéro de réseau pour une voie qui ne contient que deux interfaces** => perte d'adresses IPv4.
- **Solution : Notion de liaison point-à-point dénumérotée et de routeur virtuel.**
  - On supprime les adresses des interfaces réseau pour une liaison dénumérotée en contradiction avec la notion de route (adresse IP à atteindre "next hop")
  - Les deux routeurs situés aux deux extrémités de la liaison sont des demi routeurs qui forment un seul routeur virtuel (la liaison point à point est en fait interne au routeur virtuel).
- **Avantages** : gain de deux adresses, gestion simplifiée
- **Inconvénients** : on ne supporte pas les cas compliqués à plusieurs routeurs, les routeurs virtuels sont complexes et non standardisés.

E2) Adresses publiques et adresses privées (RFC 1918)

- **Les organisations qui veulent créer un Internet privé peuvent utiliser sans demande les adresses réservées:**
  - 10/8 (10.0.0.0 à 10.255.255.255)
  - 172.16/12 (172.16.0.0 à 172.31.255.255)
  - 192.168/16 (192.168.0.0 à 192.168.255.255)
- **Les adresses privées ne sont routées que dans les réseaux privés (non routées dans l'Internet mondial).**

Avantages

- On évite ainsi **beaucoup de demandes d'adresses.**
- On a **moins de risque d'une utilisation 'sauvage' d'adresses publiques** dans des réseaux privés.

Inconvénient

- **On ne peut pas communiquer avec l'Internet mondial.**

E3) Traducteurs d'adresses IP : NAT Network Address Translation RFC 1631

- **Motivation : l'économie des adresses IP mais aussi :**
  - **Une entreprise ayant créé un Internet privé** (RFC 1918) souhaite avoir ensuite accès à l'Internet mondial.
  - **Une entreprise souhaite cacher au monde extérieur** son plan d'adressage interne.
  - **Une entreprise souhaite se rendre indépendante** des adresses fournies par son fournisseur d'accès Internet.
- **La solution NAT : modification des adresses dans les datagrammes**
  - **Traduction des adresses IP** (dans un routeur ou dans un équipement de transit par exemple mur pare feux 'firewall').
  - **Basée sur l'acquisition** du datagramme, la **consultation** de table, la **modification** d'adresse, la **retransmission.**

NAT : Traduction statique et dynamique

- **Traduction statique (Static NAT) :**
  - Traduction d'une adresse IP d'entreprise vers une adresse IP extérieure
  - => **Toujours la même traduction réalisée.**
  - Typiquement adresse privée interne vers adresse publique du réseau mondial (facilite l'administration)

- **Traduction dynamique (Dynamic NAT) :**
  - Traduction d'une adresse IP d'entreprise (privée) vers une adresse IP publique prise dans une réserve
  - => **Un hôte n'a pas toujours la même adresse IP.**
  - Facilite l'administration et économise les adresses

NAT : Les quatre approches de traduction (1)

- **NAT avec traduction pour des transactions en sortie uniquement (unidirectionnel en sortie).**
  - Traduction NAT classique des adresses IP internes en adresses IP externes.
- **NAT avec transactions dans les deux sens (NAT unidirectionnel en sortie et unidirectionnel en entrée) :**
  - **Cas précédent ou des hôtes internes requièrent des serveurs externes** (traduction unidirectionnelle en sortie)
  - **Cas ou des clients externes requièrent des serveurs internes :** NAT en relation avec le DNS donne une adresse publique d'un serveur interne et transforme cette adresse en adresse privée (traduction unidirectionnelle en entrée).

NAT : les quatre approches de traduction (2)

- **NAT Bidirectionnel (avec traduction dans les datagrammes des adresses sources et destination) :**
  - Cas ou les espaces d'adressage internes et externes se recouvrent (adresses privées ou usage anormal d'adresses publiques). Exemple: mise en relation NAT de deux réseaux privés construits sur le bloc 10.0.0.0/8.
- **Traduction d'adresse et de numéro de port**
  - **NAT surchargé 'Overloaded'** ou encore **NAT with PAT 'Port Address Translation.**
  - Traduction du couple (adresse IP, numéro de port TCP ou UDP) vers un autre couple (adresse, numéro de port).

  => **Une adresse IP dans une réserve et un numéro de port sur 16 bits sont donc réattribués**.

  => **La solution la plus utilisée.**

Exemple : NAT unidirectionnel avec traduction de numéro de port

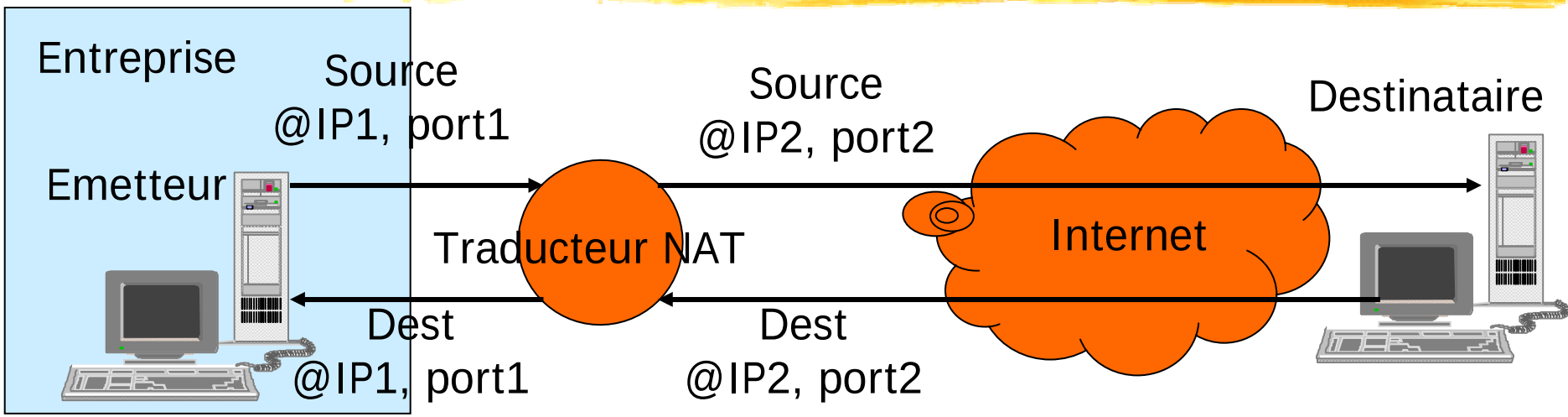


Table du traducteur

@IP1 , port 1	@IP2 , port 2

- L'adresse @IP1 peut être privée.
- L'adresse @IP2 doit être publique : un seule adresse peut servir 65536 – 4096 = 61440 applications (numéro de port sur 16 bits et les 4096 premiers numéros sont réservés aux ports bien connus).

Conclusion NAT

- **Solution simple, peu coûteuse et très efficace** : la solution qui a assuré la survie de l'adressage IP V4
- **NAT une solution qui pose aussi des problèmes**
  - Ne respecte pas le principe: chaque interface une adresse IP (problème d'identification des sources)
  - Le mode datagramme IP devient plus ou moins connecté.
  - NAT: uniquement prévu pour TCP et UDP, viole le principe d'indépendance des couches (mélange réseau/transport).
  - Si des applications placent des adresses IP dans les datagrammes il faudrait que NAT modifie à deux endroits.
  - Problème des mécanismes de sécurité avec chiffrement de charges utiles encapsulant des datagrammes donc des adresses IP.
  - NAT retarde le déploiement de IP V6.

E4) Distribution des adresses IP : La solution de base RARP

- **Problème : Attribution à un site d'une adresse IP.**
- **RARP 'Reverse Address Resolution Protocol' RFC 903**
  - Une solution pour la correspondance entre adresses MAC et IP.
  - Utilisée pour les machines sans disques et facilite l'administration.
- **Solution sur réseau local.**
  - Chaque hôte dispose d'une adresse IP fixe.
  - Un hôte qui démarre demande son adresse IP fixe.
  - Diffusion sur Ethernet de requête RARP en donnant son adresse MAC.
  - Un serveur RARP fournit l'adresse IP correspondant à l'adresse MAC.
- **Problèmes**
  - Ne fonctionne qu'avec des adresse IP fixes.
  - RARP ne gère que la distribution d'adresses IP.
  - Nécessite un serveur RARP sur chaque tronçon (ou mise en œuvre de serveurs proxy, relais de requêtes).

Distribution des adresses IP: La solution BOOTP

- **BOOTP ‘Bootstrap Protocol’ RFC 951, 1048, 1084**
  - Faire un outil pour le démarrage des stations sans disques.
  - Utiliser UDP et le routage IP pour avoir un seul serveur par entreprise.
  - Fournir différentes informations à l’initialisation (routeur par défaut, masque, serveur de fichiers de boot pour station sans disque ...).
- **Solution BOOTP pour les adresses IP sur UDP.**
  - Protocole avec différents formats de messages au dessus de UDP.
  - Un hôte qui démarre diffuse une demande d’adresse IP en UDP sur le port serveur bootp 67 (réponse en diffusion sur le port client 68).
- **Problèmes**
  - Ne fonctionne qu’avec des adresse IP fixes.

Attribution dynamique d'adresses : DHCP (RFC 941)

- **DHCP 'Dynamic Host Configuration Protocol'**
  - Une solution de **distribution d'adresses sur réseau local**.
  - Utilise les **formats** de message du protocole **BOOTP**.
  - Requête d'adresse IP en diffusion sur réseau local: **DHCPDISCOVER.**
  - Réponse d'un serveur DHCP proposant une adresse: **DHCP OFFER.**
  - Acceptation d'une adresse offerte par le client: **DHCPREQUEST.**
  - Acquittement par le serveur: attribution d'adresse: **DHCPACK.**
- **Gestion de bail** : location d'adresse IP pour une période limitée pour récupérer les adresses inutilisées.
- **Comme Bootp** : fourniture d'autres informations utiles.
- **Possibilité de déclarer des relais DHCP** sur des routeurs pour atteindre d'autres tronçons.

Conclusion : DHCP

- **Principal avantage :**
  - **Administration simplifiée des adresses (administration centralisée).**
  - **Pas de problèmes d'erreurs dues à l'utilisation de la même IP.**
- **Deux solutions**

  A) Un hôte reçoit **toujours la même** adresse IP: IP fixe comme en Bootp (pour des serveurs).

  B) Un hôte reçoit **une adresse IP prise** dans un ensemble d'adresses disponibles.
  - Une même adresse peut servir à désigner **des hôtes différents dans le temps.**
  - Il n'est pas nécessaire **d'avoir autant d'adresses que d'abonnés** si tous les abonnés ne se connectent pas en même temps.

Conclusion Adressage IPv4

- **Les problèmes de l'adressage IPv4** : tarissement des adresses, grossissement des tables de routage, trop grande centralisation de distribution.
- **Ont reçus des solutions astucieuses qui permettent à IPV4 de durer** : CIDR, NAT, DHCP ...

- **Le plan d'adressage Internet IPv4 devrait néanmoins tôt ou tard arriver à saturation**

  - Incertitude très grande sur la date effective

  - Liée au développement des services Internet consommateurs d'adresses: Internet fixe, mobile, téléphonie, commerce électronique, domotique...

  - Et à la façon de régler les problèmes d'adressage dans tous ces cas
- **Les difficultés prévisibles de l'adressage IPV4 ont amené à spécifier une version nouvelle de IP IP Version 6.**

IP

Chapitre II

Le protocole IP en version 6

Généralités IPV6

Structure des datagrammes

Adressage

Introduction IPv6

- **Besoin d'un nouveau protocole** qui apporte des réponses aux **limitations du plan d'adressage v4.**
- **Incorporer** aussi les évolutions technologiques (**sécurité, performances, administration**)
- **Etude à partir des années 1990** : différentes propositions pour un futur IP baptisé tout d'abord: IP NG
- **Processus de choix difficile à l'IETF** => Choix techniques principaux = adoption des RFC **1994-1995**.
  - IP v5 : Protocole ST2 RFC 1819: multimédia, en connexion
  - IP v7 : Réseau OSI sans connexion CLNP
  - **IP v6** : choix/fusion entre propositions CATNIP, TUBA, SIPP
- **Décision définitive 1998**
- **Implantations disponibles** en cours à partir de 1995-1996, routeur IPV6 2001 depuis phase d'expérimentation/déploiement.

Critères de conception IPv6

Adressage / Routage

- **Grand espace d'adressage hiérarchisable**.
  - Adressage pour au moins un milliard de réseaux.
- **Autorisant un routage hiérarchisé.**
  - Diminution des tailles des tables
- **Distribution d'adresses facilitée** en répartissant les possibilités d'attribution.

Déploiement

- **Une transition 'sans jour j'.**
- **Tous les changements à effectuer sur tous les types d'appareils doivent être précisés** (protocoles annexes ICMP/IGMP, hôtes, routeurs, administration réseau, ...).

Modifications par rapport à IPV4

- **Capacité d'adressage quadruplée**
  - 128 bits soit 16 octets (au lieu de 32 bits).
- **Simplification du format d'entête standard**
  - Optimisation pour un routage simplifié.
  - Suppression des champs inutiles au routage.
  - Alignement sur des frontières de mots
- **Etiquette de flot**
  - Identifier des flots d'octets pour permettre la réservation de ressource => qualité de service.
- **Pas de somme de contrôle d'entête**
- **Amélioration des extensions et des options**
  - Sous forme d'extensions à l'entête minimum.

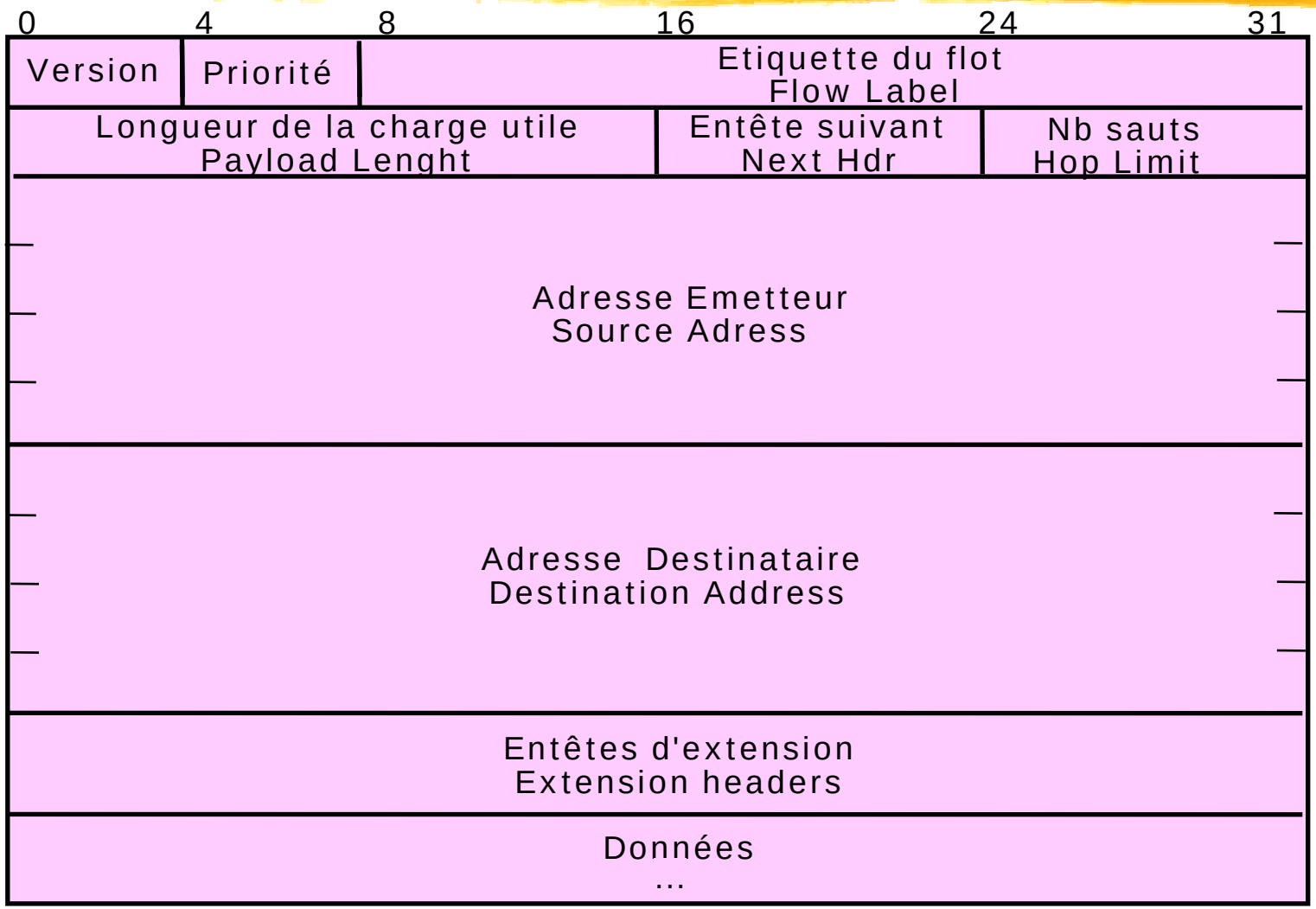
Fonctionnalités requises pour IPv6

- **Support de l'autoconfiguration** ('plug and play')
- **Support de mécanismes de sécurité** (confidentialité, authentification, intégrité)
- **Support de la qualité de service temporelle** (existence de mécanismes pour la réservation de ressources).
- **Support du mode diffusion.**
- **Support de la mobilité.**
- **Support d'artères à tous les débits**.

IP Version 6

Structure du datagramme

Format du datagramme IPv6



Détails concernant les champs IPv6 (1)

- **Numéro de version IP (4 bits) "IP version number"**

  Ici valeur 6 (IPv6).

- **Classe de trafic (4 bits) "Traffic Class" "Priority"**

Permet la définition de la priorité entre les flots de datagrammes.

Valeurs de 0 à 7 pour les flots pouvant ralentir en cas de congestion.

0 Pas de priorité particulière	**4 Trafic en rafale attendu ("ftp")**
1 Trafic de fond ("news")	**5 Réservé pour usage futur**
2 Trafic non attendu ("mail")	**6 Trafic interactif et (X11)**
3 Réservé pour usage futur	**7 Commandes: routage, admin**

Valeurs de 8 à 15 trafic "temps réel" non susceptible de ralentir (multimédia)

Remarque : Problème de la QOS temps réel: encore en développement. Autre découpage proposé: Traffic Class plus riche sur 8 bits et étiquette de flot seulement 20 bits.

Détails concernant les champs IPv6 (2)

- **Etiquette de flot (24 bits) "Flow label"**

  - En relation avec l'adresse émetteur une étiquette de flot identifie un flot de données:

  => On peut allouer des ressources à ce flot pour lui assurer un certaine qualité de service.

  - Utilisation en liaison avec RSVP "Resource Reservation Protocol".

- **Longueur de la charge utile (16 bits) "Payload Lenght"**

  - A la différence de IPv4 on ne compte pas les 40 octets de l'entête.

Détails concernant les champs IPv6 (3)

- **Prochain entête "Next Header"**

  - De nombreux entêtes d'extension sont prévus pour compléter l'entête de base selon les besoins.
  - Les entêtes forment une liste.
  - Cette zone détermine le type du premier entête.
  - Le dernier entête définit le protocole utilisateur.
    - 0 Informations de routage saut par saut
    - 4 Protocole internet
    - 6 Protocole TCP
    - 17 Protocole UDP
    - 43 Entête de routage
    - 44 Entête de fragmentation (par la source)
    - 45 Protocole de routage inter domaine
    - 46 Protocole de réservation (RSVP)
    - 50 Confidentialité de la charge
    - .....

Détails concernant les champs IPv6 (4)

- **Nombre de sauts max (8 bits) "Hop Limit"**

  - Comme dans IPv4 le nombre maximum de commutateurs pouvant être traversés (ancienne zone 'Time To Live' avec un nouveau nom qui correspond à la fonction).

  - Le diamètre du réseau 256 est jugé trop faible par certains commentateurs.

- **Adresse source (128 bits) ("Source address")**

  - Adresse IP de l'émetteur.

- **Adresse destination (128 bits) ("Destination address")**

  - Adresse IP du destinataire.

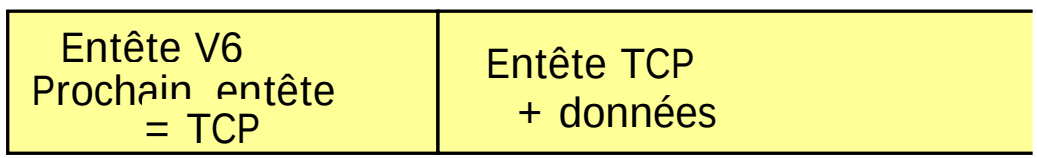
- **Données "Data"**

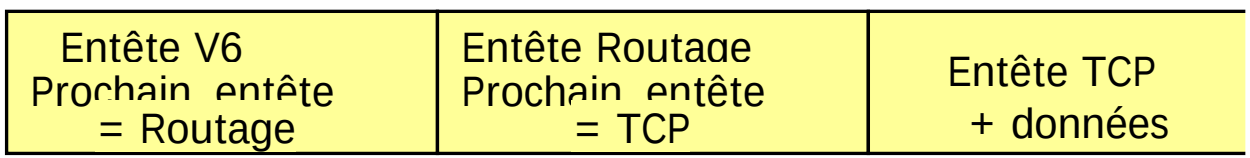
  - Zone de donnée d'une taille max de 64 Ko.

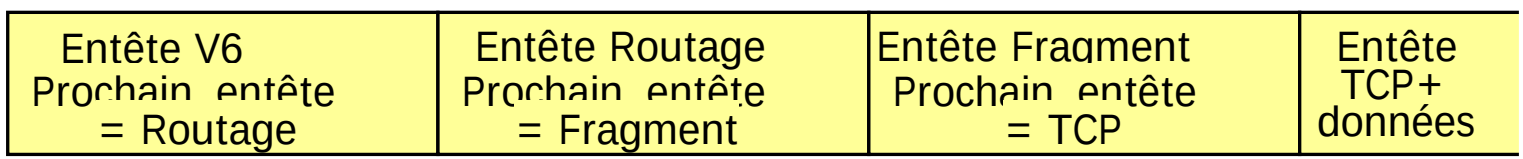
  - Une entête d'extension particulière permet de définir des longueurs sur 32 bits jumbograms.

IPV6 : Les entêtes d'extension "Extension Headers" RFC 1883

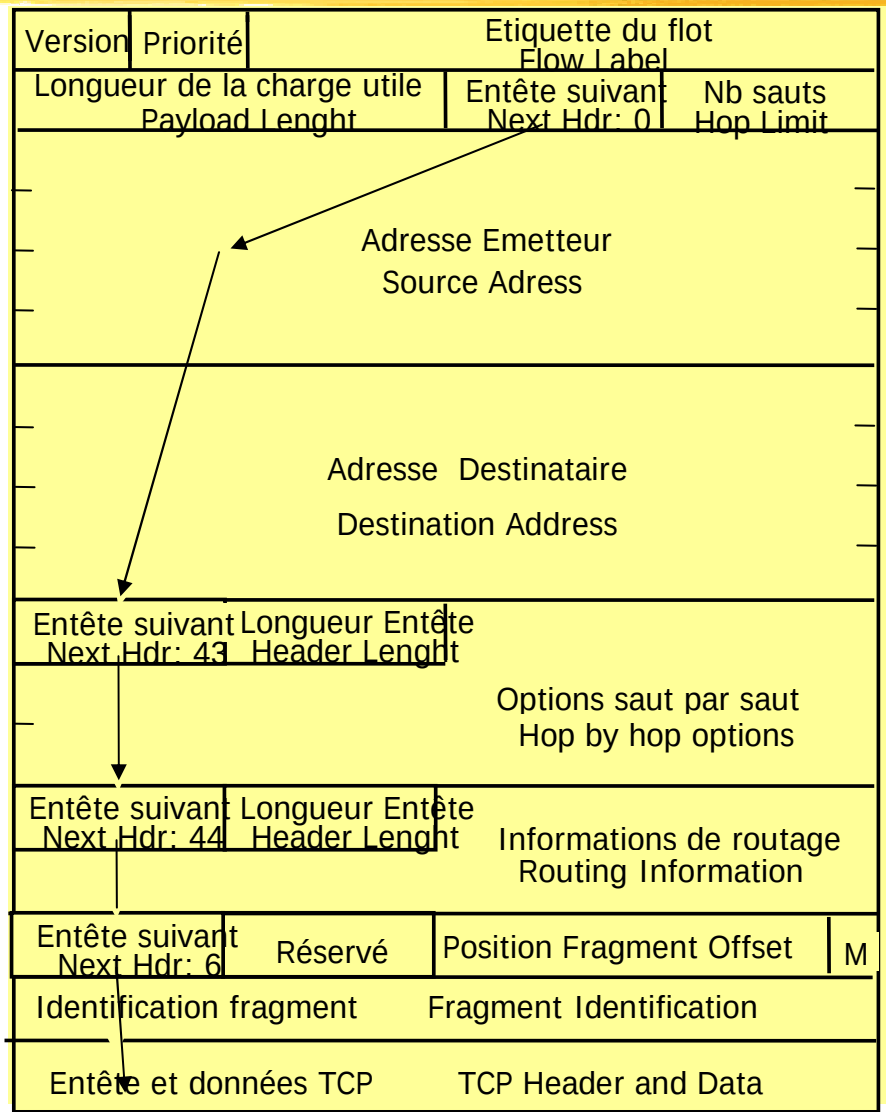
- **Nombreuses options prévues par le protocole** codées dans un nombre variable de champs d'extension en début.
- **Les extensions ne sont pas traitées par les routeurs** sauf l'extension infos "pour chaque saut" ("Hop by hop").
- **Les entêtes forment une liste.**







IPV6 : Les entêtes d'extension
Autre présentation de la liste



Description de quelques entêtes d'extension (1)

- **Les champs d'extension et leur ordre**
  - Une extension ne peut apparaître qu'une fois.
  - On doit rencontrer les extensions dans l'ordre suivant
- **Infos saut par saut 0 "Hop-by-hop header"**
  - Définit des informations pour chaque routeur rencontré par le datagramme.
  - Différents types d'informations sont précisées sur un octet.
  - En particulier le code 194 " Jumbo Payload Lenght" définit un paquet dont la taille dépasse 64K (jusqu'à 32 bits)
- **Routage 43 "Routing Header"**
  - Définit un routage par la source comme en IPV4.

Description de quelques entêtes d'extension (2)

- **Authentification 51 "Authentication Header"**
  - La méthode proposée par défaut par IPV6 utilise une clé secrète connue de l'émetteur et du destinataire.
  - La clé combinée avec le paquet transmis est compressée avec l'algorithme MD5 ("Message Digest 5").
  - Beaucoup d'autres approches de sécurité IPSEC.
- **Pas de prochaine entête 59 "No next header"**

Entêtes de fragmentation (2)

- **Généralités**
  - **La fragmentation ne dispose plus** d'informations toujours présentes dans l'entête de tous les datagrammes.
  - **Part non fragmentable**: entête de base plus quelques extensions (routage).
  - **Part fragmentable** : les autres extensions et les données
- **Entête 44 "Fragment Header"**
  - Définit une fragmentation avec des paramètres voisins de ceux de V4
  - Bit M, identificateur, déplacement (offset) du fragment.
- **Solution de fragmentation transparente** (bout en bout).
- **Découverte du MTU de chemin** :
  - Le plus grand MTU possible qui ne conduise pas à une fragmentation sur le parcours.
  - L'émetteur émet un paquet avec le bit Don't Fragment (taille du paquet inférieure ou égale au MTU local; prise en compte aussi du MSS Maximum Segment Size taille max définie pour les messages TCP).
  - Si le MTU nécessite une fragmentation dans un routeur intermediaire
    - Ce routeur transmet un message ICMP "I can't fragment"
    - L'émetteur recommence avec une taille plus petite.

IP Version 6

Adressage

IPv6 : Choix d'une adresse 128 bits

- **Rappel des principes de base**
  - Une adresse IP v6 adresse une interface (pas à un hôte).
  - C'est un identifiant unique pour une interface
  - C'est un moyen de localisation de cette interface.
- **Adressage IP V6 : ambition à terme** d'être le principal système d'adressage au niveau mondial => **effet grille-pain**
- **Choix** : entre des adresses de taille fixe (plus rapide à traiter) et des adresses de taille variable => **Taille fixe grande**
- **Choix 128 bits :** un choix de compromis entre 64 bits (jugé trop faible) et 160 bits adresse OSI (trop grand ou trop OSI).
  - A priori 3.9 * 1018 adresses par mètre carré de surface terrestre.
  - Si l'on utilise très mal les adresses disponibles (comme dans le téléphone) => 1500 adresses par mètre carré.

IPv6 : Trois catégories d'adresses

- **Adressage "Unicast" point à point.**

  - Une adresse pour un seul destinataire => le paquet est délivré à l'interface identifiée par l'adresse (comme en IP v4).

- **Adressage "Multicast" diffusion**

  - Une adresse pour un ensemble de destinataires => le paquet est délivré à toutes les interfaces du groupe identifié par l'adresse (comme en IP v4).

- **Adressage "Anycast"**

  - Une adresse pour un ensemble de destinataires => le paquet est délivré à l'une quelconque des interfaces appartenant au groupe identifié par l'adresse

  - Utilisation possible, accès à un seul serveur appartenant à un groupe de serveurs (exemple trouver un serveur au moins).

IPv6 : Représentation des adresses

- **Notation en hexadécimal** par groupes de 16 bits avec des deux points comme séparateurs.

  128 bits = 32 chiffres hexadécimaux = 8 groupes de 4 chiffres

  0ECD:AB56:0000:0000:FE34:98BC:7800:4532

Deux raccourcis d'écriture sont prévus

- **Omission des zéros en tête de groupe**.

  ECD:AB56:0:0:FE34:98BC:7800:4532

- **Plusieurs groupes de 16 bits à zéro peuvent être remplacés par ::**

L'abréviation :: ne peut apparaître qu'une fois dans une adresse.

ECD:AB56::FE34:98BC:7800:4532

IPv6 : Adresses particulières

- **Adresses de réseaux**

  - **Adressage de type CIDR** => Tout découpage réseau/ sous réseau est possible (selon des plans d'adressages).

  - La notation **adresse_Ipv6/n** définit la valeur du masque (les n bits en fort poids forment l'adresse de réseau, les autres bits sont à 0).

- **Adresse non spécifiée ("Unspecified")**

  - Pour un site en initialisation qui demande à un serveur son adresse réelle (seulement utilisable comme adresse source).

  0:0:0:0:0:0:0:0 ⇔ ::

- **Adresse de rebouclage ("Loopback")**

  - L'adresse pour s'envoyer des messages (ne peut circuler sur le réseau).

  0:0:0:0:0:0:0:1 ⇔ ::1

IPv6 : Plans d'adressage
Adresses de plus haut niveau

0::/8	00000000	Adresses IPv4
200::/7	0000001	Adresses OSI CLNP
400::/7	0000 010	Adresses Novell IPX
2000::/3	001	Adresses agrégées
4000::/3	010	Adresses prestataires
8000::/3	100	Adresses géographiques
FE80::/10	1111111010	Adresses locales lien
FEC0::/10	1111111011	Adresses locales site
FF00::/8	1111 1111	Adresses de diffusion

Récupération de la base existante OSI-CLNP, Novell

- **Protocoles de réseaux existants non IP**
  - CLNP "ConnectionLess Network Protocol"
  - IPX "Internetwork Packet Exchange"
- **Le plan d'adressage v6 propose au moyen de préfixes de reprendre ces adresses réseaux existantes**

  => migration facilitée pour ces protocoles.
- **Conversions d'adresses**

  - IPX 80 bits (10 octets) à compléter à 121 bits

  - Problème pour les adresses CLNP-NSAP "Network Service Access Point" 20 octets=160 bits à faire rentrer dans 121 bits ....

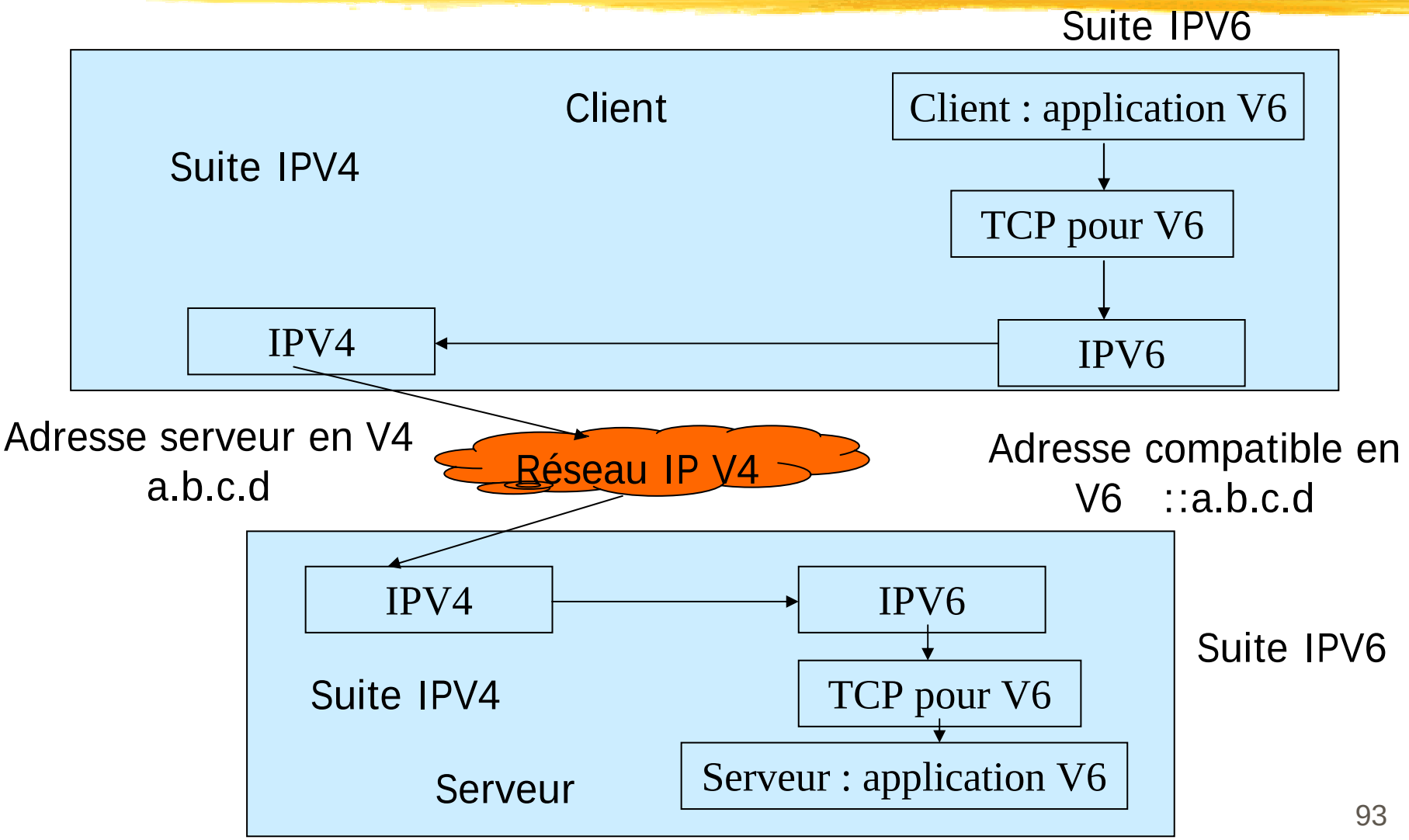
Adresses IPV6 compatibles IPV4 Transition par encapsulation

- **Phase de transition IPV4 vers IPV6:** situation ou l'on communique encore en IPV4 pour démarrer IP V6.
- **Solution d'encapsulation ("tunnelling")** de datagrammes IP v6 dans des datagrammes IP v4 (IPV6 acheminé par IP v4 et délivré à distance à une pile IP v6 après désencapsulation).
- **Adresse IPV6 compatible IPv4** "IPv4 Compatible address"

  Un hôte IP à une adresse IPV4 et une adresse IP v6 en rajoutant des 0 devant l'adresse ipv4 pour en faire de l'IP v6.

  Forme: 0:0:0:0:0:0:a.b.c.d soit ::a.b.c.d
- **Un site IP v6 souhaitant communiquer** avec un autre site IP v6 **au moyen de IP v4** utilise une suite IPV4, une adresse IP V4 et une adresse IP v6 compatible IP v4.

Encapsulation IPV6 dans IPV4

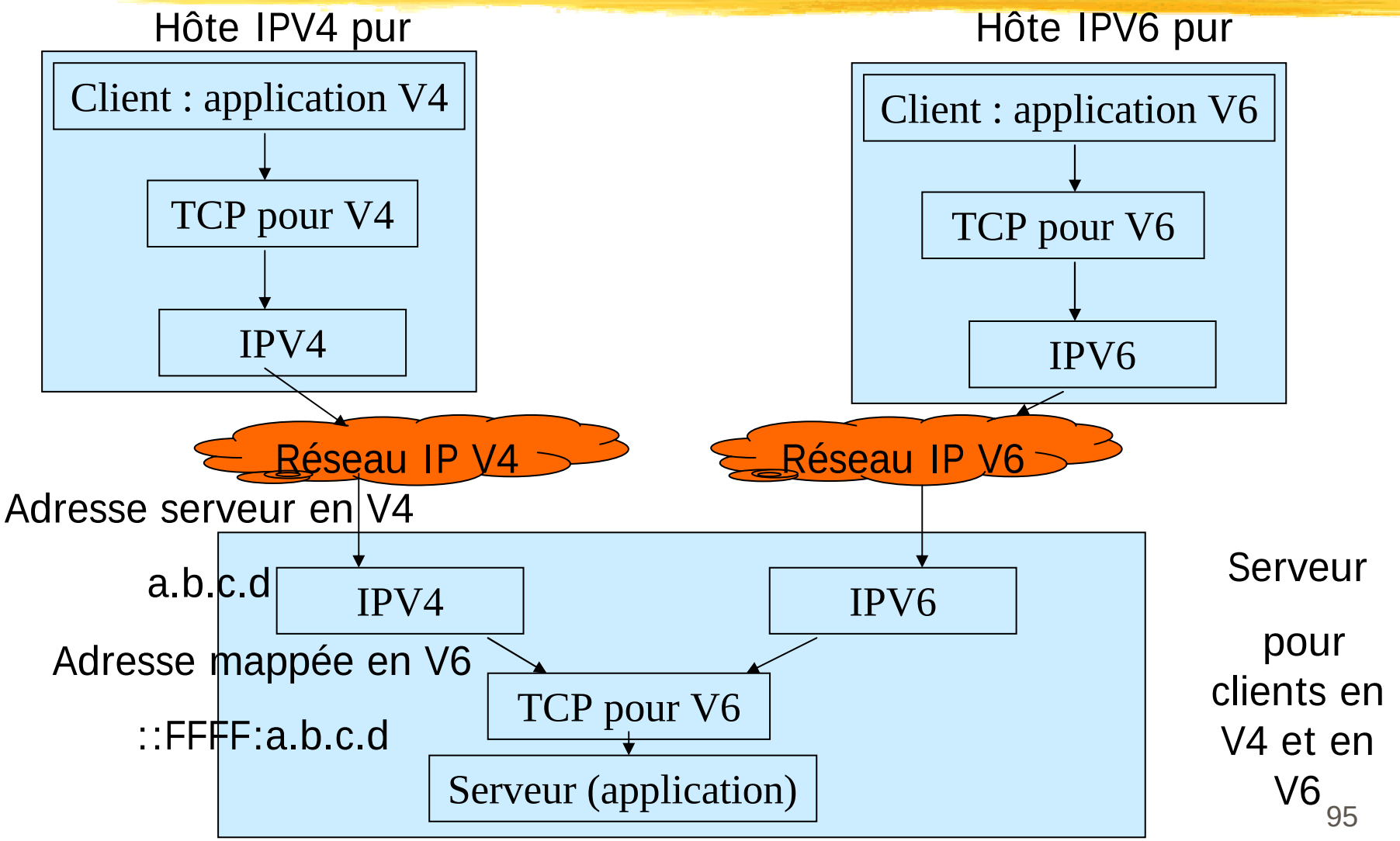


Adresses IPV4 représentées en IPV6 (‘mapped’)

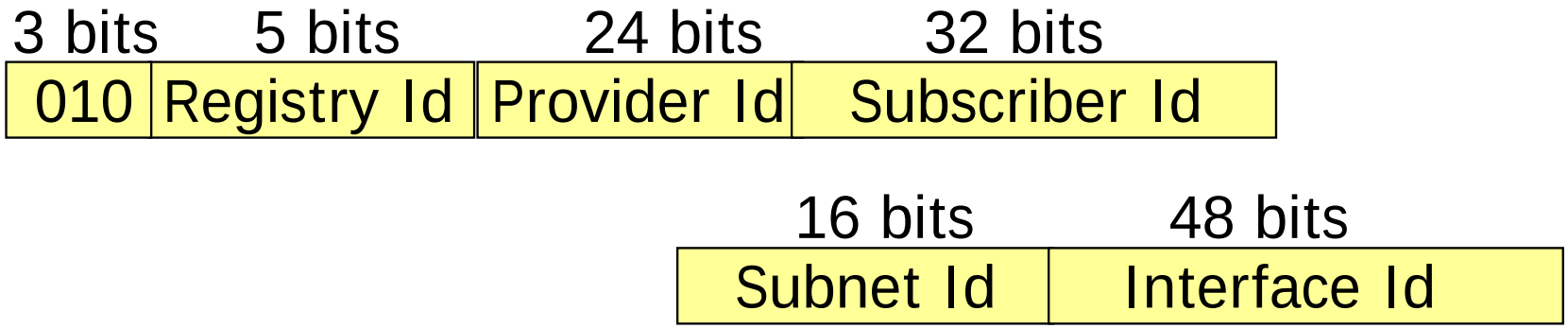
- **Transition IPV4-> IPV6 par transformation (mappage)**
  - En **émission** une requête de transmission pour un datagramme avec une adresse IP v4 représentée en IP v6 est **traité par une pile IP v4.**
  - En réception, le datagramme reçu par IP v4 est présenté à son destinataire (TCP) comme s'il s'agissait **d'un datagramme arrivé en IP v6 avec une adresse mappée**.
- **Adresse IPV4 représentée par une adresse IPV6** "IPv4 mapped IPv6 address"

  0:0:0:0:0:FFFF:a.b.c.d soit ::FFFF:a.b.c.d
- **Seul un trafic Ipv6 acheminé par IPV4** peut utiliser une adresse IP V6 mappée.
- **On peut communiquer à partir de sites IP V4 vers des sites IPV6** comme si l'on se trouvait dans le domaine d'adressage IP V6.

Adresses IPV4 représentées en IPV6 (‘mapped’)



IPV6 : Plan d'adressage prestataire 'Provider based unicast address'



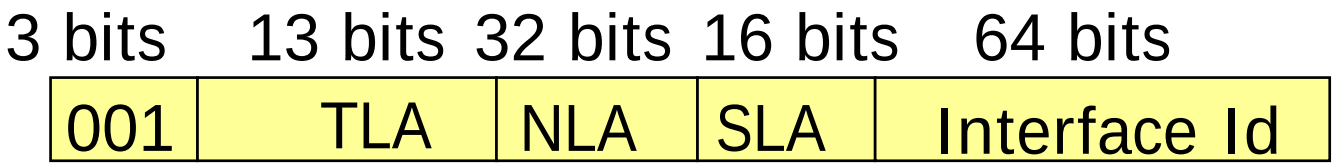
- **Quatre autorités ("Registry") prévues**
  - IANA Internet Assigned Numbers Authority
  - RIPE-NCC Réseaux IP Européens Network Coordination Center
  - INTERNIC Inter Network Information Center
  - APNIC Asia Pacific Network Information Center
- **Non utilisé** : trop dépendant des prestataires à tous niveaux (changement de prestataire => changement d'adresse).

IPV6: Plan d'adressage géographique ‘Geographic based unicast address'

3 bits	x bits	y bits	z bits
100	Id région géog	Id sous-réseau	Id Interface

- **Ces adresses seraient distribuées** selon des contraintes géographiques (pays, région, ...).
- **Les opérateurs / les monopoles de Télécom** devraient jouer un rôle majeur.
- **Beaucoup de problèmes de mise en œuvre :** répartition d'entreprises sur différentes zones géographiques.
- **Non utilisé**

IPV6 : Plan d'adressage agrégé 'Aggregatable global addresses'



- **Préfixe** 2000::/3 (3bits)
- **TLA ('Top Level Aggregator') (13 bits)**

  Agrégation de plus haut niveau: ce niveau représente de très grands ensembles d'adresses (ex: grands opérateurs internet)
- **NLA ('Next Level Aggregator') (32 bits)**

  Agrégation de niveau intermédiaire: ce niveau représente des ensembles d'adresses de taille intermédiaire (prestataires de service moyens). Ce niveau est hiérarchisable.
- **SLA ('Site Level Aggregator') (16 bits)**

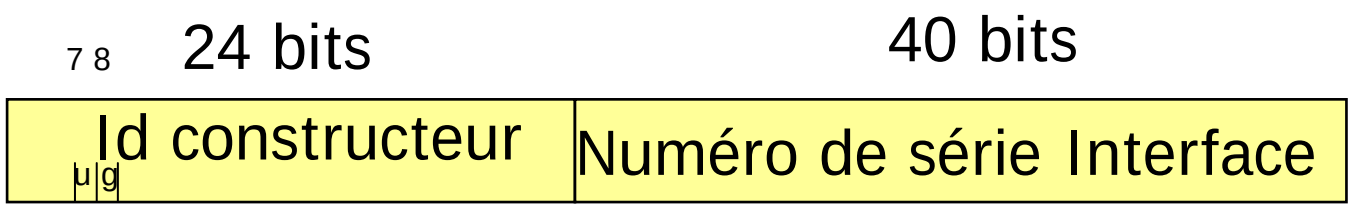
  Agrégation au niveau d'un site (ex une entreprise). Ce niveau est hiérarchisable.
- **Le plan d'adressage actuellement en service.**

Identificateur d'interface 64 bits 'Interface Identifier'

- **IEEE** : normalisation des identificateurs d'interface sur 64 bits

=> Format EUI 64: identifier toutes les interfaces de réseaux (IEEE 802, Appletalk, ..)

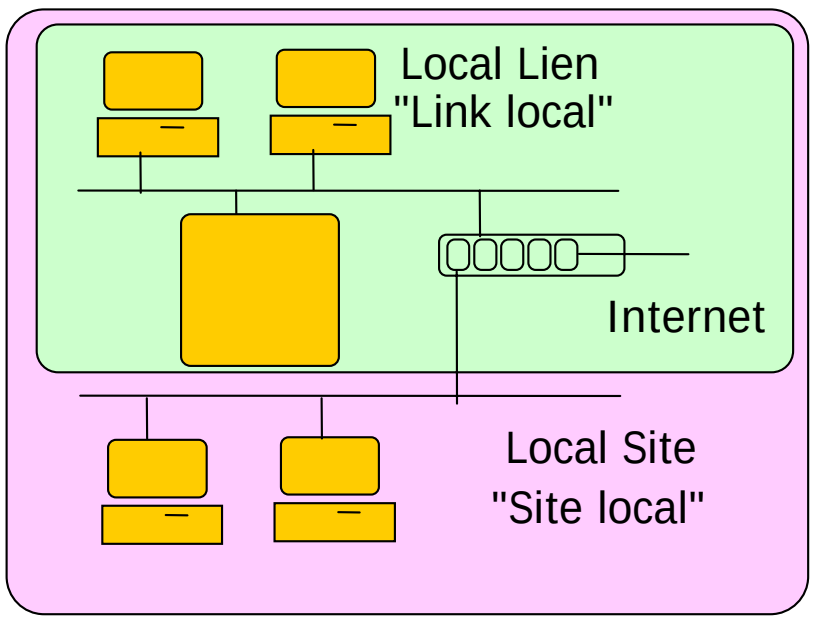
Format d'identificateur d'interface pour IP v6 (dérivé de EUI 64)



- **Bit u (universel) :** 1 => l'adresse est unique, 0 sinon (bit inversé en EUI)
- **Bit g (group) :** 1 => adresse d'un groupe ; 0 => adresse individuelle.
- **Identifiant constructeur** : 24 bits comme pour les adresses MAC IEEE
- **Numéro de série interface:** 40 bits (par exemple on porte de 24 bits à 40 bits la partie numéro de série des adresses IEEE802 en ajoutant FFFE).

IPV6 : Adresses locales

- **Adresses de portée locale**
  - Ces adresses ne sont pas valides à l'extérieur d'une certaine portée
  - => Les routeurs ne les acheminent pas.
- **Permettent de construire des réseaux Internet privés** (à l'abri d'un mur anti feu) comme dans le cas des adresses réservées IP v4.
- **Deux portées locales**
  - Locale site
  - Locale lien ou tronçon



IPV6 : Format des adresses locales

- **Portée locale site (préfixe FEC0::/10)**

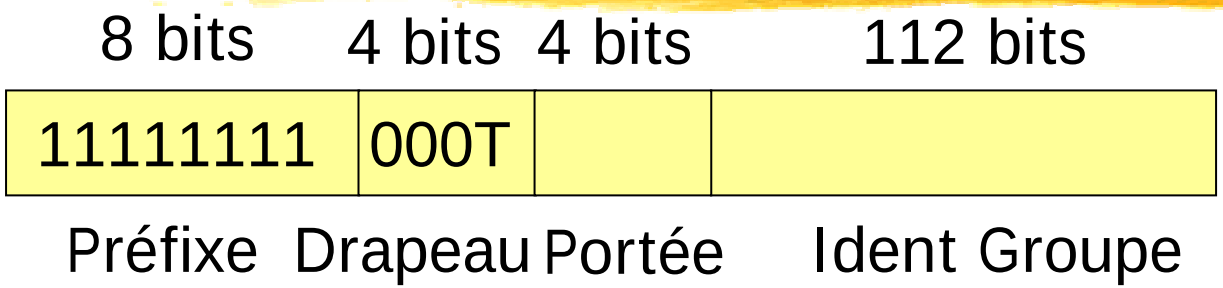
10 bits	n bits	m bits	118-n-m bits
1111111011	0		

- **Portée locale lien (un tronçon de réseau local) (préfixe FE80::/10)**

10 bits	n bits	118-n bits
1111111010	0	Interface Id

  - On doit mettre une adresse d'interface unique.
  - On prend l'adresse IEEE de la carte réseau accédant au réseau local.

IPV6 : Les adresses de diffusion



- **Préfixe (‘Prefix) :** FF/8 **soient** 8 bits à 1 => 11111111
- **Drapeau (‘Flag’) :** 4 bits 000T

  T=1 adresse permanente ; T=0 adresse temporaire
- **Portée (‘Scope’) :** 4 bits XXXX Valeurs de portée de diffusion
  - 1 Diffusion limitée à un seul système
  - 2 Diffusion limitée à une seule liaison locale
  - 5 Diffusion limitée à un seul site
  - E Diffusion de portée globale à l’Internet
- **Identifiant de groupe (‘Group Id’) :** 112 bits

IPV6 : Exemple de quelques adresses de groupes prédéfinies

- **1 : L'ensemble des systèmes**

  FF05::1 Portée de site local

  FF02::1 Portée lien local.

- **2 : L'ensemble des routeurs**

  FF05::2 Portée de site local

  FF02::2 Portée lien local.

- **C : L'ensemble des serveurs de configuration DHCP** "Dynamic Host Configuration Protocol"

  FF02::C Portée lien local (tous les serveurs DHCP sur un tronçon, utilisation type de DHCP).

Conclusion IP V6

- **IP V6 : une amélioration certaine par rapport à IPV4**
  - Surtout pour ce qui concerne l'adressage
  - Mais aussi pour la prise en compte d'améliorations techniques diverses (sécurité, extensions ...).
- **Mais démarrage très lent à grande échelle**.
  - **Très nombreux détails à régler**
  - **IPV6 constitue un effort de portage** que les utilisateurs n'ont pas envie de supporter tant que l'adressage IP V4 tient.
  - **On demande beaucoup plus à IPV6 qu'à IPV4.**
- **Développé depuis 1995**
  - Transition prévue au départ sur 15 ans.
  - Chaque année le lancement à grande échelle est annoncé.
  - Chaque année IP V6 se développe un peu.
- **Attente de l'application consommatrice d'adresses IP qui forcera la migration vers IPV6.**

Bibliographie IP V6

- RFC1752 'Recommendation for the IP Next Generation Protocol' 1/95
- RFC1809 'Using the Flow Label in IPv6' 6/95
- RFC1881 'IPv6 Address Allocation Management' 12/95
- RFC1883 'Internet Protocol, Version 6 Specification' 12/95
- RFC1884 'IP Version 6 Addressing Architecture' 12/95
- RFC1885 'Internet Control Message Protocol (ICMPv6)' 12/95
- RFC1886 'DNS Extensions to Support IPv6‘ 12/95
- RFC1887 'An Architecture for IPv6 Unicast Address Allocation' 12/95
- RFC1897 'IPv6 Testing Address Allocation' 12/95
- RFC1924 'A Compact Representation of IPv6 Addresses' 4/96
- RFC1933 'Transition Mechanisms for IPv6 Hosts and Routers' 4/96
- RFC1825 'Security Architecture for the Internet Protocol' 8/95

IP

Chapitre III
Le routage IP

Généralités

Routage statique

Routage dynamique

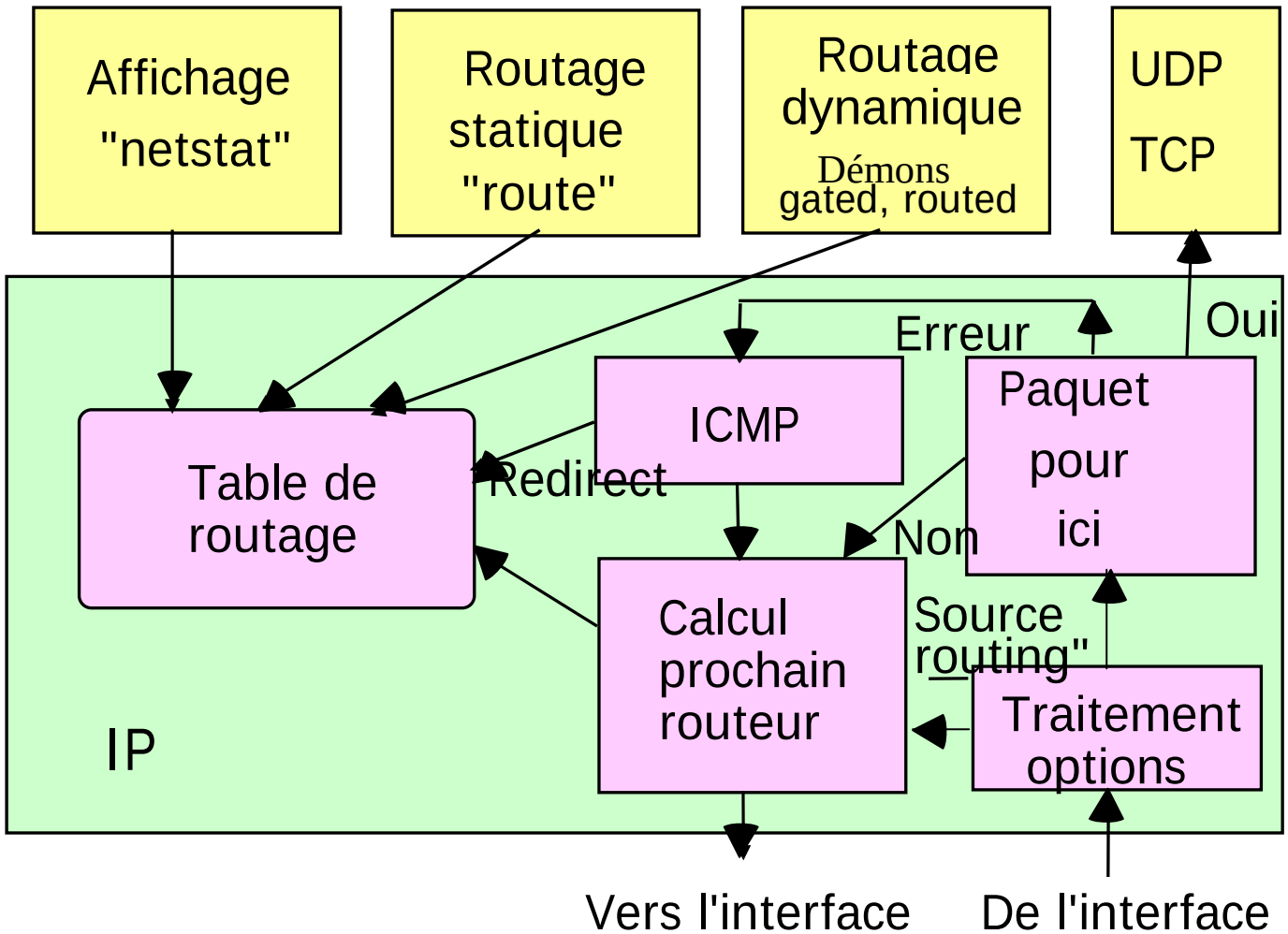
Introduction : Rappel du problème de routage

- **Objectif du routage point à point :** Atteindre un seul hôte destinataire en masquant la traversée d'une série de **réseaux et de routeurs intermédiaires**.
- **Routage multipoint (‘multicast’) :** Atteindre tous les hôtes d’un groupe destinataire.
- **Notion d’hôtes** (**"Hosts")**
  - Un hôte ne **relaie pas** de messages (il dispose en général d’une seule interface et d'une table de routage simplifiée).
- **Notion de routeurs ("Routers" "Gateways")**
  - Un routeur possède plusieurs interfaces.
  - **Il retransmet un message d'une interface entrante à une interface sortante** s'il dispose des informations suffisantes pour le routage (sinon il note le message 'non délivrable‘).

Routage statique et dynamique

- **Routage statique** : Définition manuelle des routes (une fois pour toute).
- **Routage dynamique :** Mise en œuvre d'un protocole de communication entre routeurs pour l'apprentissage 'automatique' des meilleurs routes (selon des critères de coûts).

Organisation générale du routage IP



Etapes d'une opération de routage

- **Choix d'une route**
  - **Recherche des routes** pour la destination d'un paquet.
  - Choix de **correspondance la plus longue** *longest Match*
  - Eventuellement : choix entre des routes équivalentes selon la qualité de service **(TOS)** et la **métrique** de la route.
  - Eventuellement **répartition de charge**.
- **Transmission**
  - Si le site à atteindre est connecté directement au site courant (par une liaison point à point ou en réseau local)

    => Obtention de **l'adresse liaison** destinataire (ARP)

    => Le message est **envoyé directement**.
  - Sinon **transmission au prochain routeur** (next hop) qui reprend à son compte l'acheminement.

Gestion de la table de routage : A) Liste d'une table

Informations associées à une route (UNIX)

- **Adresse IP destination**
  - Généralement une adresse de réseau (la zone Host-id est à zéro).
- **Adresse du prochain routeur ("Gateway")**
  - A emprunter pour atteindre la destination.
- **Indicateurs ("flags")**
  - U chemin opérationnel,
  - G chemin vers un routeur,
  - H chemin vers un hôte,
  - D chemin créé par une redirection,
  - M chemin modifié par une redirection ....
- **Nombre de références**
  - Nombre de connexion utilisant le chemin (connexions TCP, UDP).
- **Métrique (de la route)**
- **Nombre de paquets envoyés**
- **Interface ("device")** (pilote et carte sur lesquels envoyer le paquet).

Table de routage pour un hôte: Exemple de liste en LINUX

- **Commande route (autre possibilité netstat –r)**

kirov::/users/ensinf/gerard _16 /sbin/route
Table de routage IP du noyau

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
163.173.128.0	*	255.255.252.0	U	0	0	0	eth0
loopback	*	255.0.0.0	U	0	0	0	lo
default	bigiron.cnam.fr	0.0.0.0	UG	0	0	0	eth0

kirov::/users/ensinf/gerard _17

- **Commentaire : table de routage d'un hôte = >** trois routes principales
  - **La boucle locale** : loopback (127.0.0.1) pour les messages qui ne sortent pas.
  - **L'accès aux hôtes** sur le même réseau Ethernet : ici 163.173.128.0
  - **L'accès à un routeur par défaut** qui ouvre sur le reste de l'Internet : default (en fait 0.0.0.0). Indicateur G route vers un routeur.

Table de routage pour un routeur: Exemple de liste sur routeur CISCO

mgs>**show ip route**
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default.4/9
Gateway of last resort is 193.51.128.81 to network 0.0.0.0
10.0.0.0 255.255.0.0 is subnetted, 1 subnets
S 10.35.0.0 [1/0] via 192.108.119.147
C 192.168.100.0 is directly connected, Ethernet5
C 192.168.101.0 is directly connected, Ethernet5
C 192.168.55.0 is directly connected, Ethernet3
C 192.168.0.0 is directly connected, Ethernet1
193.51.128.0 255.255.255.248 is subnetted, 1 subnets
C 193.51.128.80 is directly connected, Ethernet2
C 192.168.200.0 is directly connected, Ethernet4
S 192.168.201.0 [1/0] via 192.168.200.61
..... liste coupée ici .... etc .....

Gestion de la table de routage : B) Initialisation Statique (1)

- **Pour créer manuellement une route**
  - **Pour délivrer des datagrammes** sur un réseau local.
  - **Pour atteindre un routeur distant (ex type default).**
- **Exemple en UNIX : Commande ifconfig configure les paramètres du pilote de carte réseau**
  - A chaque définition d'une interface la table de routage est initialisée automatiquement en conséquence.
  - **Exemple** : /etc/ifconfig eth0 kirov up déclare un coupleur ethernet eth0 actif (up) . Différentes autres options
    - "netmask" : définition du masque de sous-réseau.
    - etc ...;

Exemple de liste de paramètres d'interface

```
kirov::/users/ensinf/gerard _16 /sbin/ifconfig eth0
eth0    Lien encap:Ethernet  HWaddr 00:09:3D:00:A9:7F
        inet adr:163.173.129.17  Bcast:163.173.131.255 Masque:255.255.252.0
        adr inet6: fe80::209:3dff:fe00:a97f/64 Scope:Lien
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:214175639 errors:0 dropped:0 overruns:0 frame:0
        TX packets:147434433 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 lg file transmission:1000
         RX bytes:158285671425 (150952.9 Mb)  TX bytes:87060146495
                                                        (83027.0 Mb)
         Interruption:25
kirov::/users/ensinf/gerard _17
```

Gestion de la table de routage: Initialisation Statique (2)

- **Exemple en UNIX : Commande route**
  - **Déclaration explicite d'une route** vers un réseau distant :

route add -net 192.56.76.0 netmask 255.255.255.0 dev eth0

  - **Les routes initialisées statiquement** sont contenues dans un fichier de configuration :
    - Exemples AIX /etc/rc.net, SUNOS /etc/rc.local, SOLARIS 2 /etc/rc2.d/S69inet

Gestion de la table de routage: C) Redirection par ICMP

- **Modification des tables de routage par découverte de chemins :** ICMP protocole additionnel qui achemine des informations de routage et des messages d'erreur pour IP
- **Utilisation des diagnostics ICMP d'erreurs pour améliorer le routage**
  - Exemple: routeur A envoie un message à un routeur B pour atteindre C.
  - B s'aperçoit qu'il ne peut atteindre C
  - B indique par un message ICMP à A ce problème ("host unreachable").
- **Messages ICMP de maintenance des tables**
  - ICMP peut diffuser des demandes de routes (en diffusion totale ou mieux en diffusion sur groupes) "router sollicitation message"
  - Les routeurs à l'écoute répondent : "router advertisement message"

Gestion de la table de routage: D) Routage dynamique

- **Routages dynamiques :**
  - **Les routes dans les tables sont modifiées** par des processus qui implantent des protocoles d'échange de routes.
  - Le routage dynamique permet **l'apprentissage des routes et l'adaptativité aux variations de charge**.
  - **Les tables de routages sont exploitées** de la même façon pour la commutation par IP (qu'elles soient initialisées statiquement ou dynamiquement).
- **Nombreuses possibilités de routage dynamique en IP.**
- **IP : Routage hiérarchisé à deux niveaux (au moins)**
- **Notion de domaine ou AS "Autonomous Systems":**
  - Un domaine correspond à un ensemble de sites, administrés par une seule et même entité (grande entreprise, campus).
- **Deux types de routage: intra et inter domaine.**

Liste de principaux protocoles de routage dynamique en IP

- **Protocoles de routage intra-domaine (IGP "Interior Gateway Protocol") :**
  - **RIP :** “Routing Information Protocol”.
  - **IGRP, EIGRP :** “Enhanced Interior Gateway Routing Protocol”.
  - **OSPF :** “Open Shortest path First”.
  - **Integrated IS-IS :** “Integrated Intermediate System to Intermediate System”.
- **Protocoles de routage inter-domaine (IRP "Interdomain Routing Protocol") :**
  - **EGP :** “Exterior Gateway Protocol“.
  - **BGP :** "Border Gateway Protocol“.

1) Routage dynamique: RIP Routing Information Protocol (RFC 1028)

- **Routage dynamique par échange périodique** de tables entre voisins **("Distance Vector").**
- **Initialisation du protocole**
  - **Emission d'une requête** de demande de table sur toutes les interfaces avec une liste de destination (**Code commande 1).**
  - **Réponse**: S'il y a une route pour la destination =>métrique de la route
    Sinon => métrique = valeur infinie (ex 30) (**Code commande 2).**
- **Fonctionnement en mode établi ('message request')**
  - **Mise à jour périodique** : émission vers tous les voisins systématiquement toute les x secondes (typiquement 30).
  - **Si une route n'a pas été rafraîchie** pendant y minutes elle est portée à infini (pour invalidation, y typiquement 3 minutes)
  - **Mise à jour de route** sur événement (changement de métrique).

RIP Routing Information Protocol : Informations complémentaires

- **Métrique d'une route :** nombre de sauts ("hops").
- **Protocole utilisé UDP :** pour échanger les informations avec les autres routeurs.
- **Nom du démon en UNIX: "Routed"**
- **RIP V2 RFC 1388:** extensions dans des champs inutilisés par RIP V1 (diffusion, identification de domaine, échange du masque)
- **Sous UNIX :** commande pour obtenir les informations de routage d'un routeur distant (code commande poll 5) :
  ripquery -n "nom de routeur"
- **Solution de moins en moins utilisée**

2) Routage dynamique: OSPF Open Shortest Path First (RFC 1247)

- **OSPF : remplaçant de RIP**
  - RIP est insuffisant pour les grands réseaux.
  - Déploiement progressif de OSPF après 1990.
- **Solution à état de liaison ("link state").**
  - Collecte par chaque routeur de l'état des liaisons adjacentes.
  - Echange de ces états (plusieurs approches, solution de base inondation).
  - Calcul par tous les routeurs des tables de routage optimales par l'algorithme de Dijsktra ("Shortest Path First").

OSPF : Caractéristiques

- **OSPF: un routage intra domaine mais hiérarchisé à deux niveaux**
  - OSPF permet de gérer à l'intérieur d'un domaine des régions ("areas")
  - OSPF calcule des routes intra-régions, inter régions.
  - Une région particulière permet de connecter les autres ("backbone" "area 0").
  - Pour la maitrise des grands domaines ("autonomous system").
- **OSPF propose une grande variété de métriques**
  - Débit, délai aller-retour, ...
  - Une métrique peut-être attribuée par type de service.
- **Calcul de plusieurs routes possibles** par type de service.
  - Si deux routes sont de coût équivalent: distribution de charge.
- **Echange des informations** de routage OSPF: protocole IP .
- **Nom du démon UNIX**: "Gated« .

Principaux messages OSPF

Type de message	Description
Hello	Découverte des voisins immédiats
Link state update	Diffusion aux voisins
Link state ack	Acquittement réception
Database description	Annonce des états dont dispose un routeur
Link state request	Demande informations à un routeur

3) Routage dynamique: BGP Border Gateway Protocol (RFC 1267, 1268)

- **Protocole de routage Inter-domaine.**
- **Autorise des politiques de routage** spécifique aux grandes organisations
- **Objectif :** contrôler l'acheminement par une organisation (interdire du traffic en transit , orienter le traffic, ...).
- **Trois types de domaines** (identifiés par des entiers 16 bits):
  - **Domaine souche ("stub") :** un seul lien avec l'exterieur
  - **Domaine de transit ("transit AS"):** plusieurs liens avec l'extérieur, et autorise le passage d'informations extérieures à son trafic local (transit)
  - **Domaine multi-liens ("multi homed AS"):** plusieurs liens avec l'extérieur, mais n'autorise pas le passage.
- **Solution par échange de tables** entre voisins comme RIP ("Distance vector", Mac Quillan)
- **Echange des informations de routage** : TCP.

Routage IP : Conclusion

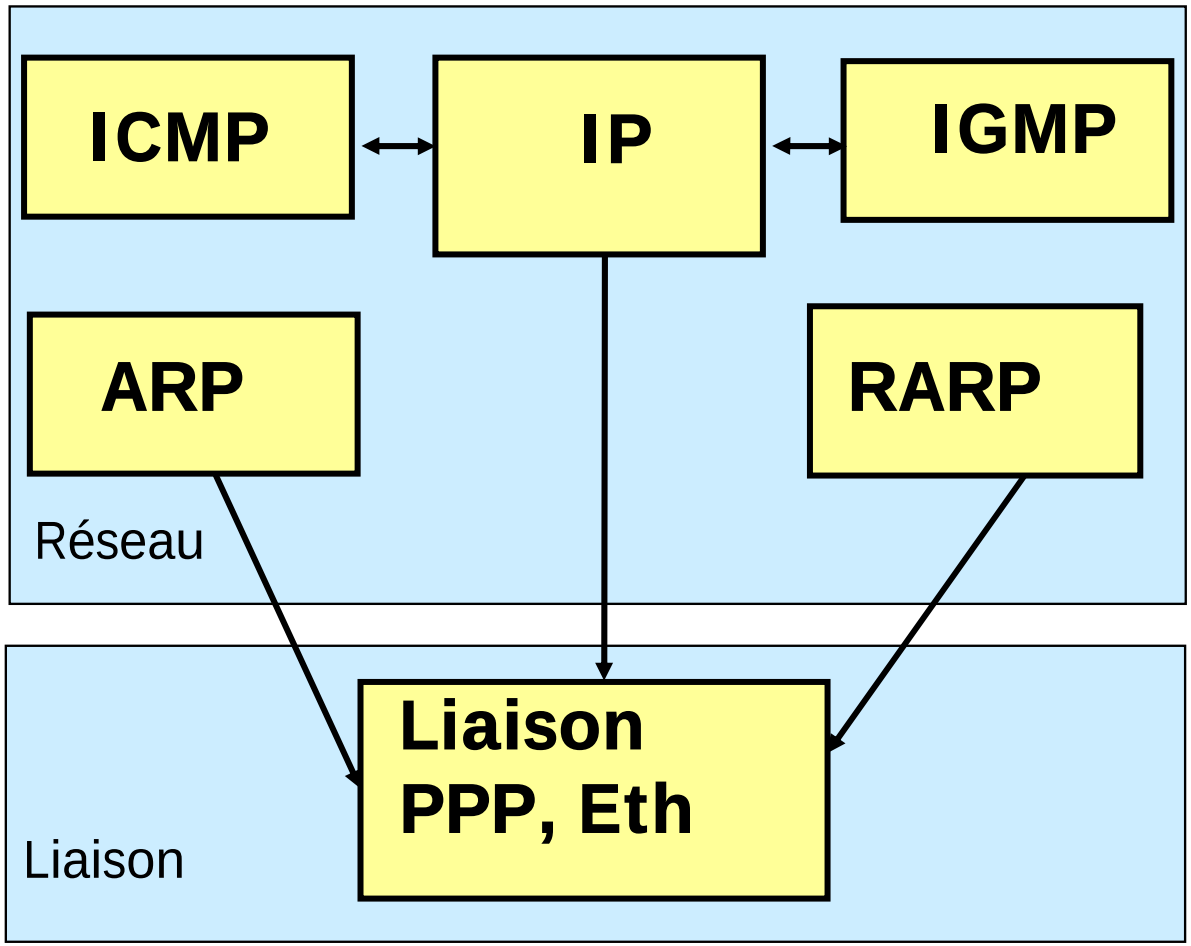
- **Hiérarchisation du routage :** le routage IP est devenu suffisamment hiérarchique avec les notions de sous-réseaux, les domaines (AS), les régions (areas) (mais le réseau Internet est très grand et en développement rapide).
- **Agrégation des routes :**
- **Rôle majeur des opérateurs, des grandes organisations et des fournisseurs de service :** qui administrent le routage pour des domaines importants.
- **Introduction de IP V6 :** Les algorithmes de routages sont basés exactement sur les mêmes principes (OSPF, BGP4) avec un espace d'adresses suffisant.

IP

Chapitre IV

Protocoles complémentaires de IP

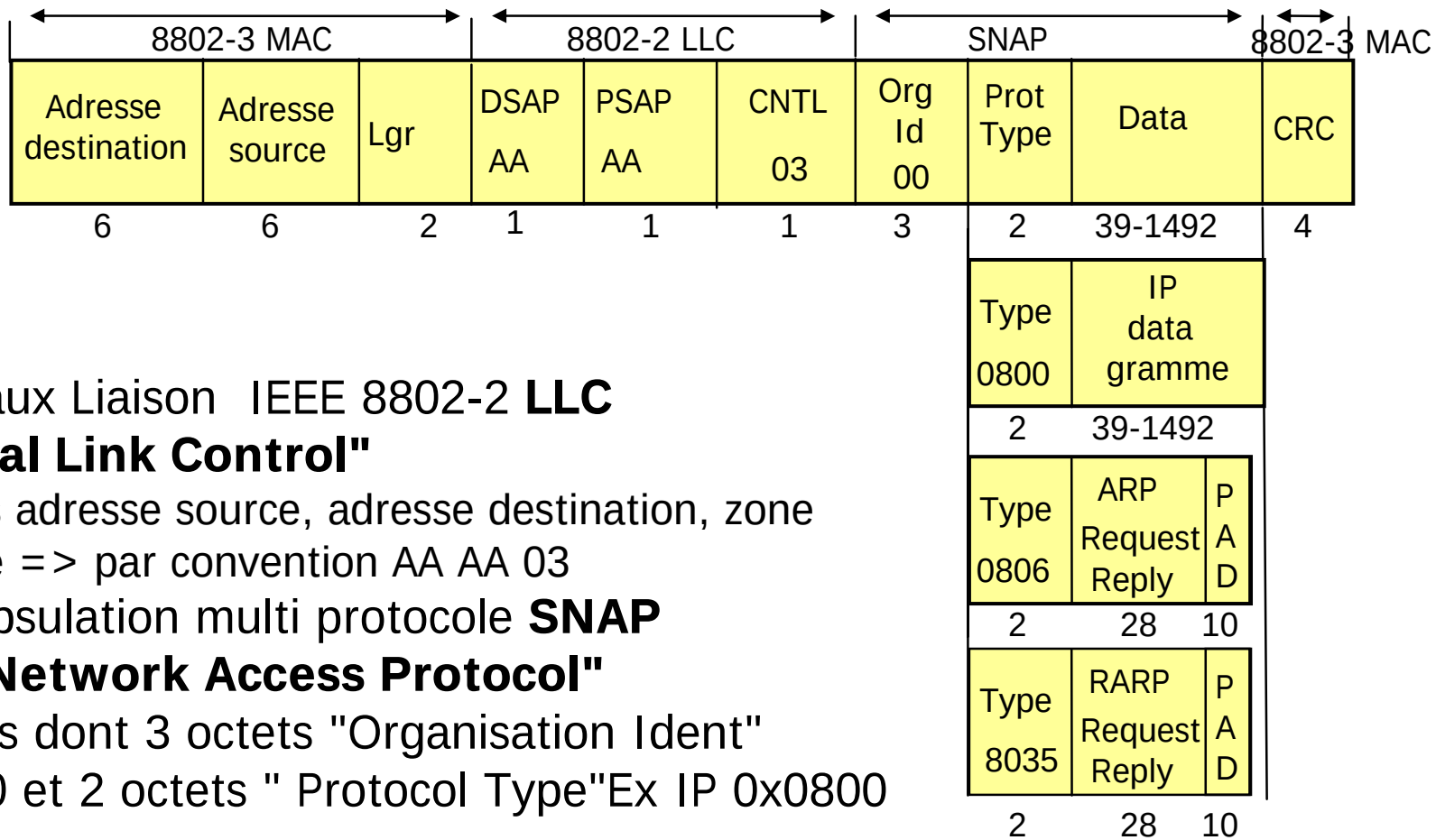
Introduction : rappel des protocoles annexes de IP



A) Couche liaison : Encapsulation Multiplexage

- **Problème abordé:**
  - Encapsuler des paquets IP dans des trames au niveau liaison.
  - Supporter conjointement sur le même réseau local différents protocoles de niveau 3 (IP, IPX, DECNET, CLNP, AppleTalk, ...).
- **Existence de différents protocoles de liaison.**
- **Cas des liaisons spécialisées : protocole PPP**
  - Encapsulation PPP => déjà vue
- **Cas des réseaux locaux : Protocoles Ethernet DIX ou IEEE 802**
  - Encapsulation **Ethernet/DIX ou LLC/SNAP**

Encapsulation IEEE 802



- Niveaux Liaison IEEE 8802-2 **LLC**

"**Logical Link Control**"

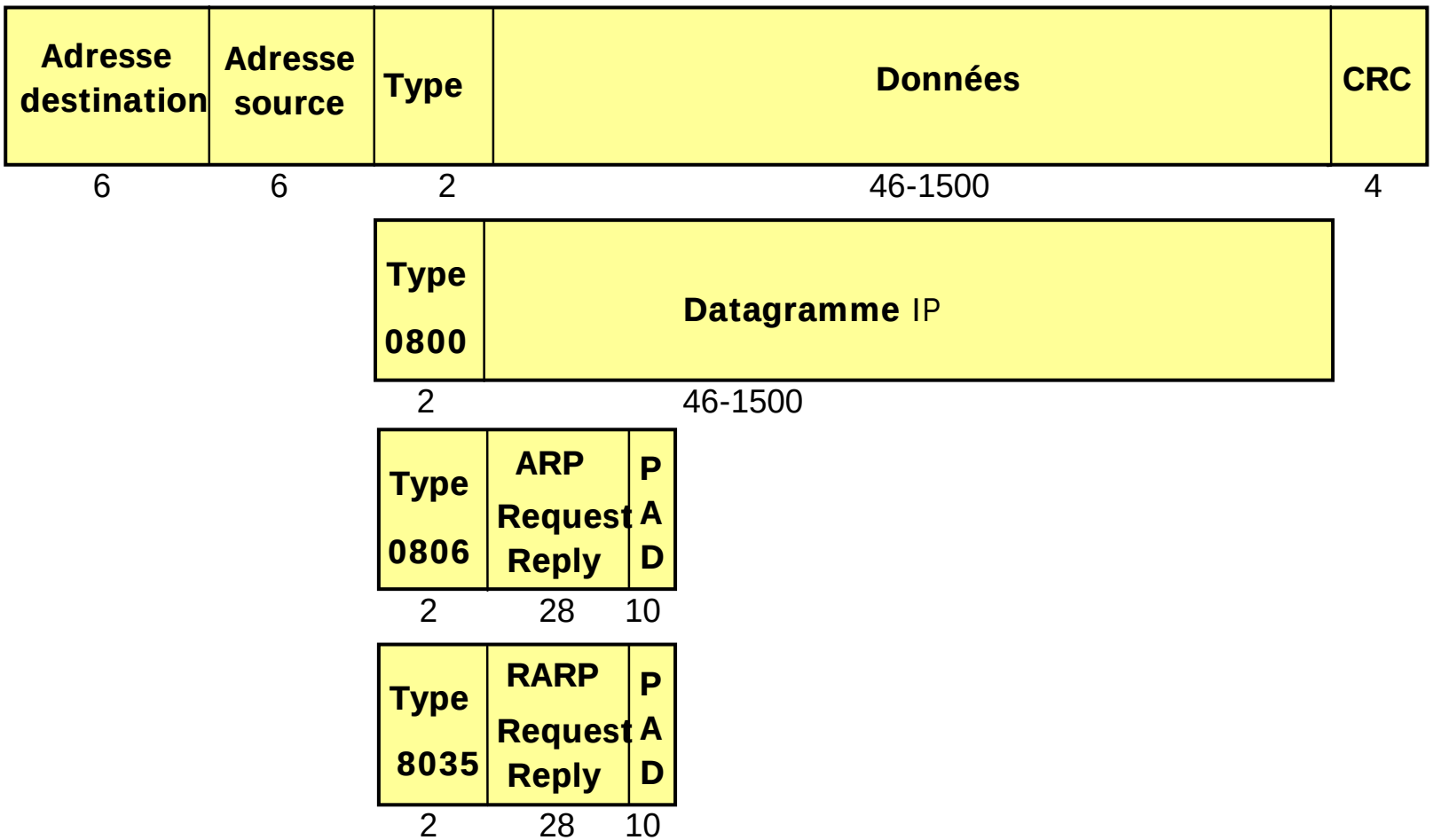
3 octets adresse source, adresse destination, zone contrôle => par convention AA AA 03

- Encapsulation multi protocole **SNAP**

"**Sub-Network Access Protocol**"

5 octets dont 3 octets "Organisation Ident" 000000 et 2 octets " Protocol Type"Ex IP 0x0800

Encapsulation Ethernet DIX



B) Relation entre adresses liaison et réseau: solutions statiques

- **Objectif : Etablir la correpsondance** entre adresses liaison (adresses MAC) et adresses réseau (adresses IP):
  - **Adresse Internet** <=> **Adresse Ethernet**

    @IP @MAC

- **Solutions statiques**
- **A) Gérer dans chaque site une table statique**

  => Mais modification obligatoire de la table à chaque changement de configuration.

  => Solution très lourde.
- **B) Utiliser des adresses IP et des adresses MAC qui se déduisent l'une de l'autre 'facilement'**

  => Solution IP V6.

Relation entre adresses liaison et réseau: Solutions dynamiques

- **Solution dynamique: gestion d'annuaire**
  - Existence de sites serveurs qui connaissent la relation d'adressage**.**
  - Utiliser un protocole client-serveur pour interroger ces serveurs et déterminer dynamiquement les relations entre adresses.
  - Très utile si le réseau est souvent reconfiguré (retrait, installation fréquente de stations de travail).
- **Eviter de renseigner sur chaque site les adresses des serveurs:** utilisation du mode diffusion des réseaux locaux.

B1) Protocole ARP : "Address Resolution Protocol"

- **Problème :** connaître l'adresse Ethernet connaissant l'adresse IP
- **Cas d'utilisation :** communication dans l'Internet sur le même réseau local
  - A sur le même réseau local que B doit dialoguer avec B (@IpB, @MacB).
  - A ne connaît que l'adresse réseau Internet @IpB.
  - A veut connaître l'adresse liaison Ethernet @MacB.
- **Fonctionnement de la recherche locale : Mécanisme de Cache d'adresse (cache ARP)**
  - Table sur chaque site qui conserve les résolutions d'adresses effectuées.
  - A cherche dans son cache local l'adresse MAC de B : si succès fin de ARP et communication avec B.
- **Fonctionnement de la recherche distante: chaque site fonctionne comme serveur de sa propre adresse.**

(1) Diffusion d'un paquet requête ARP contenant @ IpB

(2) Tous les sites du réseau reçoivent le paquet ARP et comparent l'adresse Internet proposée avec leur propre adresse

(3) B répond seul (réponse ARP) en envoyant @MacB.

(4) A dialogue avec B.

Protocole ARP : Compléments de gestion du cache

- **A ayant reçu une réponse de B :** mémorise dans son cache la correspondance (@IpB, @MacB)
- **B dans le message requête à appris la correspondance** (@IpA, @MacA) **:** apprentissage dans le cache
- **Tous les autres hôtes ont reçu la requête :** entrée si nécessaire dans leur cache (@IpA, @MacA).
- **A sa mise en marche une station diffuse une requête ARP sur sa propre adresse:** apprentissage de tout le réseau (ARP gratuit).
- **Les entrées du cache sont invalidées après une durée paramétrable :** gestion dynamique de cache pour tenir compte des modifications de l'architecture.
- **Remarque :** prolongation possible des requêtes de diffusion ARP **notion de proxy ARP** un routeur qui retransmet les requêtes ARP sur ses différentes interfaces de réseau.

Protocole ARP : Exemple (fonctionnement en UNIX)

tulipe::/users/ensinf/gerard _23 /usr/sbin/arp -a
Net to Media Table

Device	IP Address	Mask	Flags	Phys Addr
le0	mac-florin.cnam.fr	255.255.255.255		00:00:94:22:ac:74
le0	cisco-for-turbigo	255.255.255.255		aa:00:04:00:1f:c8
le0	kendatt	255.255.255.255		08:00:20:7d:72:08
le0	savitri.cnam.fr	255.255.255.255		08:00:20:04:3a:04

< Longue liste de toute la table>

tulipe::/users/ensinf/gerard _25 /usr/sbin/ping rita
rita.cnam.fr is alive

tulipe::/users/ensinf/gerard _26 /usr/sbin/arp -a
Net to Media Table

Device	IP Address	Mask	Flags	Phys Addr
le0	mac-florin.cnam.fr	255.255.255.255		00:00:94:22:ac:74
le0	cisco-for-turbigo	255.255.255.255		aa:00:04:00:1f:c8
le0	kendatt	255.255.255.255		08:00:20:7d:72:08
le0	**rita.cnam.fr**	**255.255.255.255**		**08:00:20:12:bd:d5**
le0	savitri.cnam.fr	255.255.255.255		08:00:20:04:3a:04

< Longue liste de toute la table>

B2) Protocole RARP : "Reverse Address Resolution Protocol"

- **Objectif : Déterminer une adresse IP avec une adresse Ethernet**
- **Cas d'utilisation:** une machine qui boute
  - Cas d'une machine sans disque: boute à partir du réseau (coupleur boute = coupleur Ethernet).
  - Nécessité pour utiliser un transfert de fichier simple (TFTP) de connaître l'adresse IP locale ou envoyer le binaire.
  - En ROM coupleur son adresse MAC => obtention de l'adresse IP.

- **Fonctionnement RARP**
  - La station qui amorce diffuse son adresse Ethernet sur le réseau local.
  - Un serveur RARP (nécessaire sur chaque réseau) retourne l'adresse IP.
  - Absence de réponse : retransmissions (nombre limité).
  - Tolérance aux pannes : plusieurs serveurs RARP.

- **En IPv6 ARPet RARP sont intégrés à ICMP.**

C) Protocole ICMP : "Internet Control Message Protocol" (1)

- **Objectif : réaliser différents échanges orientés administration de réseaux** (15 types de messages)
  - Messages d'erreurs.
  - Acquisition d'informations.
- **Requête-Réponse de masque (d'un sous-réseau)**
  - Pour une station sans disque qui souhaite le connaître lors de son initialisation.
- **Requête-Réponse demande de l'heure d'un site distant**
  - Pour développer une synchronisation d'horloge.
- **Acheminement de messages d'erreurs**
  - Durée de vie dépassée => paquet détruit
  - Site inaccessible ("port unreachable error") 16 diagnostics d'échec.
- **Messages ICMP de maintenance des tables de routage**
  - ICMP redirect ou messages de demande routes.

ICMP : Utilitaire ping

- **Requête-Réponse ICMP:** envoi d'un message à un hôte distant et attente d'une réponse (si le répondeur est activé).
  - **Message ICMP type ECHO_REQUEST**
  - **Message ICMP type ECHO_REPLY**
- **Commande Unix: ping**
  - ping "adresse IP" ou "nom de domaine DNS d'un hôte"
  - "nom de station" is alive et/ou statistiques de temps d'aller retour
- **Utilisation:**
  - Hôte distant opérationnel (en fait sa couche IP fonctionne).
  - Le réseau Internet permet d'atteindre un hôte distant.
  - Détection d'un réseau (ou d'un hôte distant) surchargé.
- **Autre option : ping -R** pour "record route" : chaque routeur enregistre son adresse dans le paquet.
  - Utilisation pour tracer les routes (courtes).
  - Ping n'est pas toujours disponible et longueur maximum de la route 9.

Exemple : utilitaire ping

$ping ulysse.cnam.fr

Envoi d'une requête 'ping' sur ulysse.cnam.fr [163.173.136.36] avec 32 octets de données :

Réponse de 163.173.136.36 : octets=32 temps=60 ms TTL=115
Réponse de 163.173.136.36 : octets=32 temps=50 ms TTL=115
Délai d'attente de la demande dépassé.
Réponse de 163.173.136.36 : octets=32 temps=50 ms TTL=115

Statistiques Ping pour 163.173.136.36:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),
Durée approximative des boucles en millisecondes :
    minimum = 50ms, maximum = 60ms, moyenne = 40ms
$

ICMP : Utilitaire traceroute

- **Objectif :** tracer ou tester une route de longueur arbitraire.
- **Solution :**
  - Emettre des datagrammes IP vers un destinataire avec une valeur de la durée de vie TTL Time To Live croissante (1, 2, 3, jusqu'à une valeur max).
  - A chaque expérience ICMP retourne un diagnostic d'erreur ICMP à l'envoyeur lorsque le TTL passe à 0 => apprentissage du routeur visité sur la route vers le destinataire
- **Commande Unix: traceroute "adresse IP" ou "nom de domaine"**
  - Permet de connaître le chemin emprunté et la durée pour atteindre chaque routeur (trois expériences pour chaque routeur).
- **Autre possibilité : traceroute -g "adresseIP"**
  - Permet également de tester les possibilités de routage par la source
  - -g routage faible : on force IP à emprunter quelques routeurs spécifiés.
  - -G routage strict : on force IP à parcourir strictement une route.

Exemple : utilitaire traceroute

```
$/usr/etc/traceroute cyr.culture.fr
    traceroute to cyr.culture.fr (143.126.201.251), 30 hops max, 40 byte packets
     1  internet-gw                    (163.173.128.2)   0 ms     0 ms     0 ms
     2  renater-gw                     (192.33.159.1)    0 ms    10 ms     0 ms
     3  danton1.rerif.ft.net           (193.48.58.113)   110 ms   80 ms    90 ms
     4  stlamb3.rerif.ft.net           (193.48.53.49)    100 ms  130 ms  100 ms
     5  stamand1.renater.ft.net        (192.93.43.115)   90 ms    60 ms    50 ms
     6  stamand3.renater.ft.net        (192.93.43.17)    70 ms   100 ms    90 ms
     7  rbs1.renater.ft.net            (192.93.43.170)   130 ms  120 ms     *
     8  Paris-EBS2.Ebone.NET           (192.121.156.226) 110 ms   90 ms  100 ms
     9  icm-dc-1.icp.net               (192.121.156.202) 220 ms  110 ms  220 ms
    10  icm-dc-1-F0/0.icp.net          (144.228.20.101)  200 ms  230 ms  290 ms
    11  Vienna1.VA.Alter.Net           (192.41.177.249)  250 ms  210 ms  240 ms
    12  Falls-Church4.VA.ALTER.NET(137.39.100.33)    330 ms  220 ms  180 ms
    13  Falls-Church1.VA.ALTER.NET(137.39.8.2)       270 ms  290 ms  230 ms
    14  Amsterdam2.NL.EU.net           (134.222.35.1)    380 ms  410 ms  460 ms
    15  Amsterdam1.NL.EU.net           (193.242.84.1)    350 ms  380 ms  310 ms
    16  134.222.30.2                   (134.222.30.2)    150 ms  490 ms  530 ms
    17  Rocquencourt.FR.EU.net         (193.107.192.18)  340 ms  340 ms  330 ms
    18  143.126.200.203                (143.126.200.203) 300 ms  410 ms     *
    19  cyr.culture.fr                 (143.126.201.251)  460 ms  220 ms  290 ms
$
```

D) Protocole IGMP : "Internet Group Management Protocol"

- **Objectif :** Utiliser les capacités de transmission IP pour réaliser des diffusions sur groupe => Deux problèmes à résoudre :

  => **Disposer d'un protocole d'appartenance à un groupe:** messages vers les routeurs pour entrer et sortir d'un groupe de diffusion

  => **Construire un routage en diffusion** : exemple de protocoles de routage en diffusion sur groupe DVMRP, PIM=>Notion de routeur diffuseur
- **Protocole d'appartenance à un groupe dans l'Internet: IGMP.**
  - **Rappel :** Adresses IPV4 de groupes (classe D) ou Adresse IPV6 (FF/8)
  - **Association à un groupe (abonnement) :** en émettant une requête à son routeur (diffuseur) de rattachement comportant l'identificateur du groupe et l'interface qui doit recevoir les messages.
  - **Désassociation (désabonnement) :** autre requête.
  - **Surveillance :** un routeur diffuseur émet une requête périodique sur toutes les interfaces ou il doit délivrer des messages diffusés pour vérifier l'opérationnalité.
  - **Maintenance de table :** utilisant ces requêtes et ces réponses un routeur gère sa table locale des groupes.
- **En IPv6 IGMP est intégré à ICMP.**

IP

Conclusion

Succès du protocole IP

- **Un protocole de niveau 3 en expansion considérable:** HTTP, SMTP puis les applications puis la téléphonie et la TV.
- **IP couvre les besoins d'interconnexion** : pour des réseaux de transmission de données numériques => **IP est devenu le réseau par excellence d'intégration de services.**
- **IP intègre** toutes les nouvelles offres de moyens de communication physique.
- **Les routeurs IP ont été améliorés en performances** et IP est complété par un protocole de commutation rapide à circuits virtuels (MPLS)
- **IP possède une version 6 :** pour supporter le développement en termes d'adressage et de hiérarchisation.

Compte tenu de son extension et de son adéquation IP devrait continuer d'être utilisé comme protocole unificateur de niveau 3 pendant très longtemps.

Incertitudes

- **Est ce que IPV6 va réussir à se déployer** dans de bonnes conditions en même temps que IPv4 va régresser?
- **Est ce que IP va pouvoir s'ouvrir à l'ensemble large et divers d'usagers et de besoins qui sont visés:**
  - Support de la qualité de service pour des application variées multimédias.
  - Dans le cadre d'un développement énorme => passage à l'échelle.
- **Comment IP et plus généralement l'Internet va gérer son propre effet sur la société?**

Bibliographie Internet Protocol

- W.R. Stevens "**TCIP/IP Illustrated, The protocols**" , Addison Wesley
- S.A. Thomas "**IPng and the TCP/IP protocols**" Wiley
- A.S. Tannenbaum "**Computer Networks**" Prentice Hall
- Cisco "**Internetworking Technology**" Publication interne