Cours réseaux

Serveur NAT et protocole IPv6 et comparaison avec IPv4

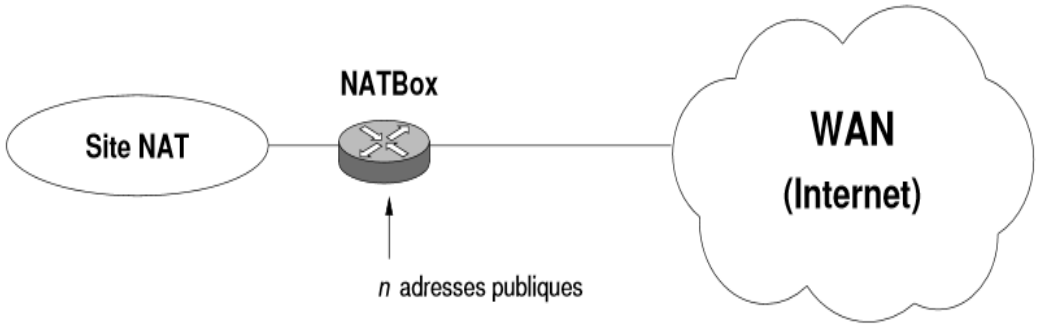
Serveur NAT

Network Address Translation (NAT)

- C’est un système qui fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables.
- Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.
- La fonction NAT dans un routeur de service intégré (ISR) traduit une adresse IP source interne en adresse IP globale.

Principe de la traduction d'adresse

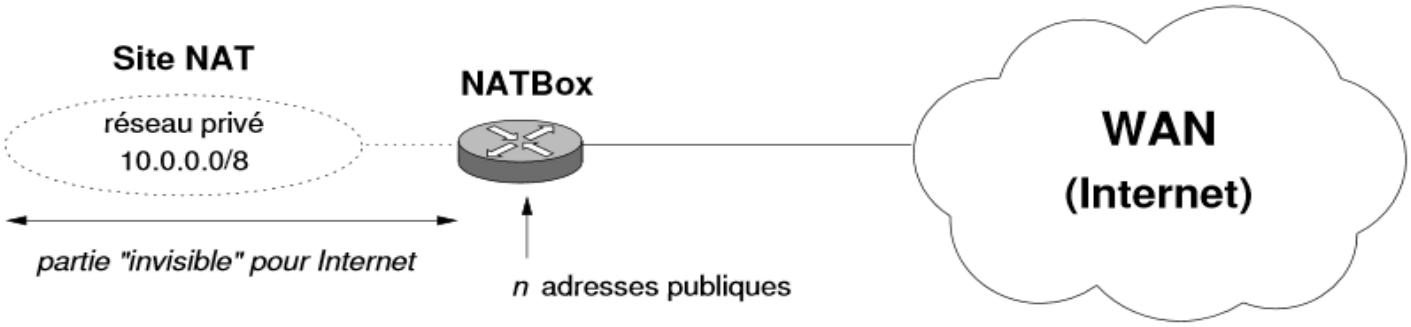
- Permettre à n adresses publiques d'être partagées par un grand nombre m de stations (périphériques réseau)



- il faut placer une NATBox qui doit être le seul point de passage entre le Site NAT (réseau de l'organisation) et le WAN (Internet)
- la NATBox est la seule qui possède et gère les n adresses publiques

Quelques précisions

- une NATBox est un routeur avec les fonctionnalités NAT (la plupart des routeurs, et les **box* des FAI)
- les stations du Site NAT n'ont pas connaissance des adresses publiques de la NATBox et ne les utilisent pas
- mais ont des **adresses privées** qu'il est fortement conseillé de prendre dans les plages définies par la RFC 1918 :
  - 10.0.0.0/8 soit 16 777 216 adresses (de 10.0.0.0 à 10.255.255.255)
  - 172.16.0.0/12 soit 1 048 576 adresses (de 172.16.0.0 à 172.31.255.255)
  - 192.168.0.0/16 soit 65 536 adresses (de 192.168.0.0 à 192.168.255.255)



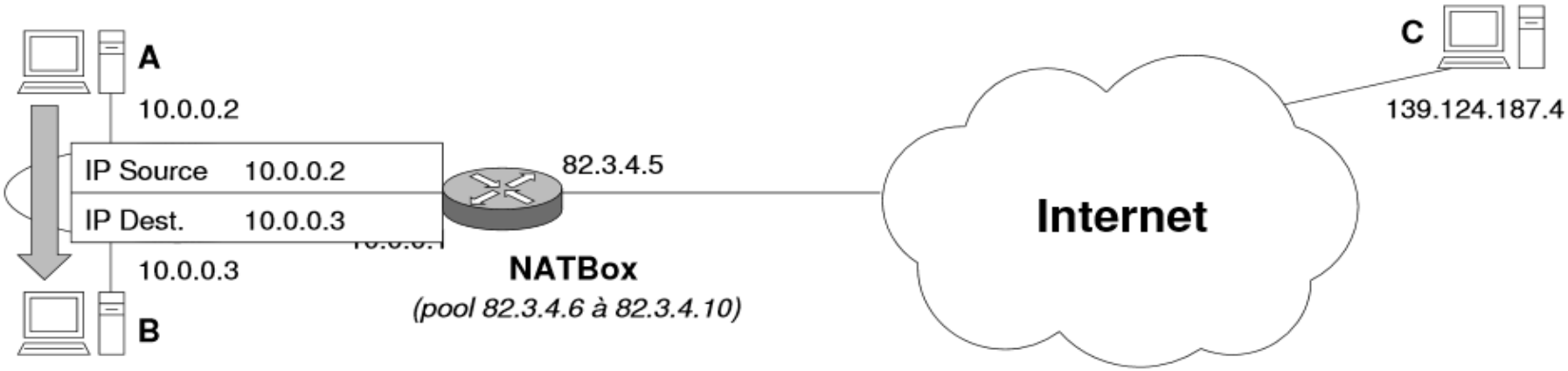
Remarque : Pour les stations du WAN, seules les n adresses de la NATBox existent et le Site NAT avec ses adresses privées est invisible

Quelques précisions

- A l’intérieur du Site NAT, les stations communiquent entre elles en utilisant leurs adresses privées (ARP)
- sans le NAT, un message envoyé à l'extérieur ne pourrait avoir de réponse car les adresses privées ne sont pas routables dans le WAN
- la NATBox doit traduire (remplacer) dans un tel message, l'adresse privée par une adresse publique, et inversement pour la réponse

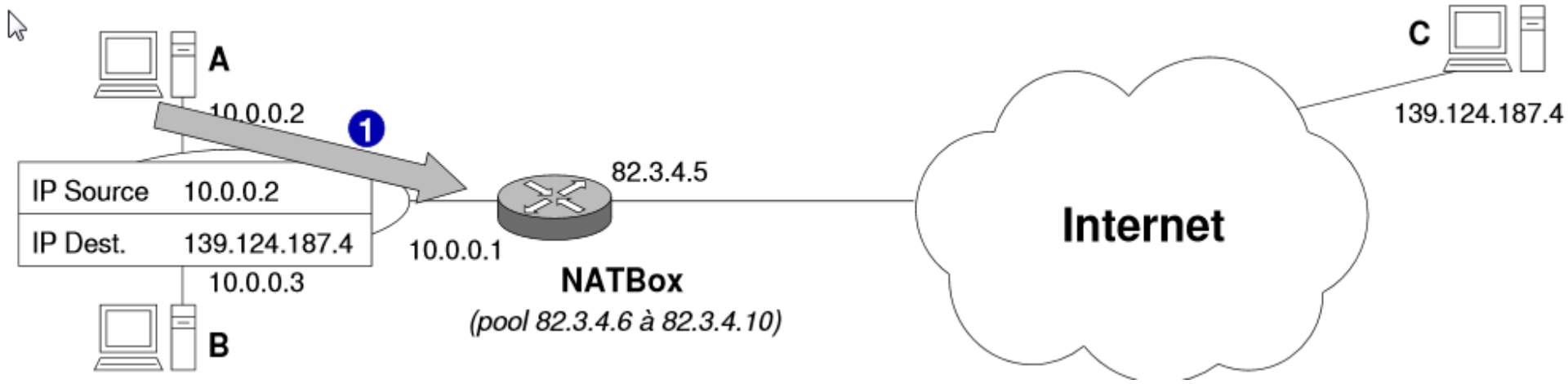
NAT et la discussion interne

- La station A (10.0.0.2) veut discuter avec la station B (10.0.0.3) :
  - le dialogue étant interne, la NATBox n'est pas concernée par ce trafic
  - les datagrammes contiennent les adresses de A et de B



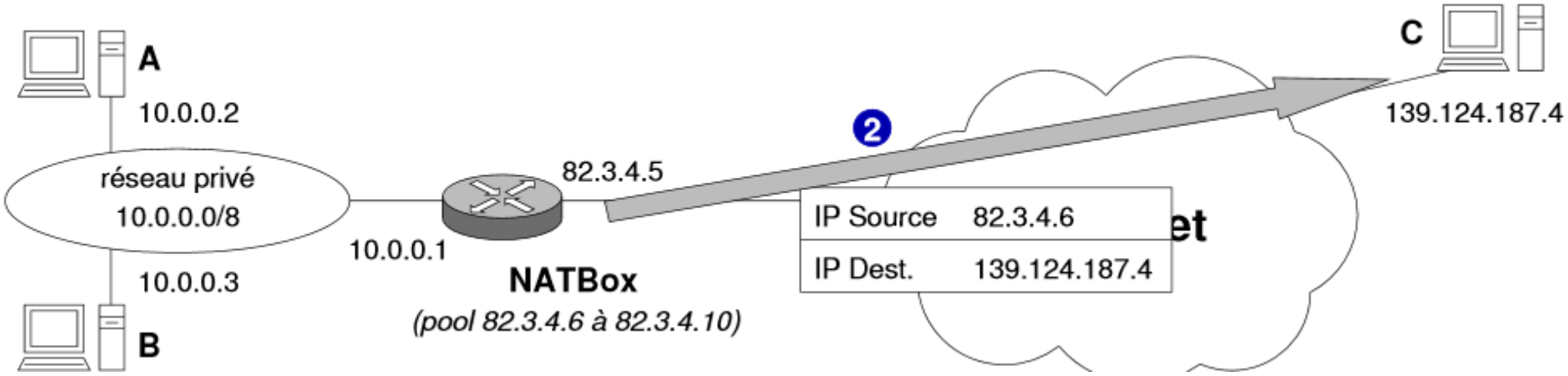
NAT et la discussion extérieur

- A (10.0.0.2) veut discuter avec la station externe C (139.124.187.4) :
  1. A envoie le datagramme qui parvient au routeur (NATBox)



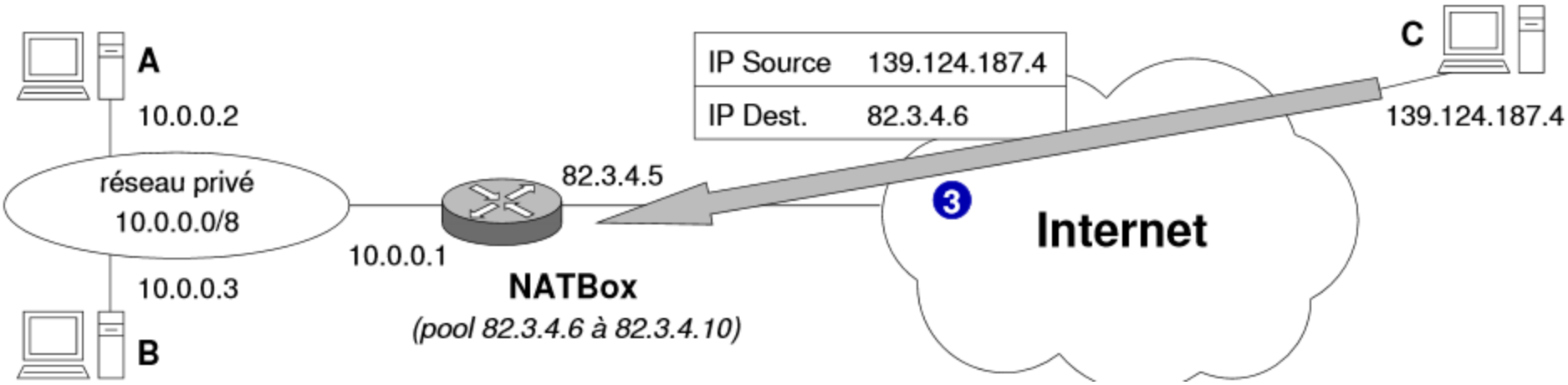
NAT et la discussion extérieur

- 2. La NATBox remplace l'adresse source (privée) par une adresse publique disponible (82.3.4.6), enregistre une association (82.3.4.6, 10.0.0.2) dans sa table de traductions , et transmet le datagramme vers C



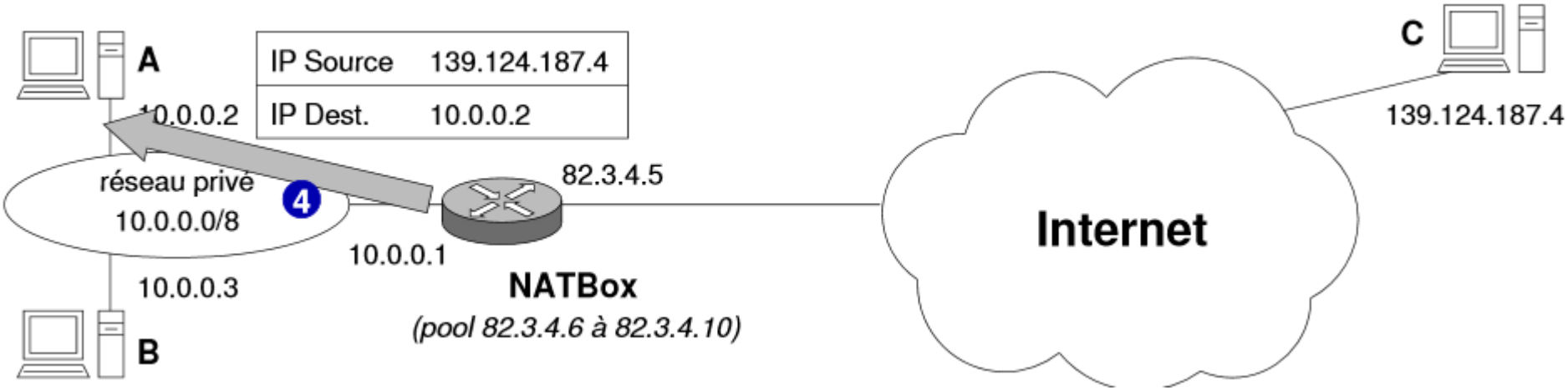
NAT et la discussion extérieur

3. C répond a l'adresse source du datagramme (82.3.4.6)



NAT et la discussion extérieur

- 4. la NATBbox reçoit le datagramme, consulte sa table de traductions, trouve l'association (82.3.4.6, 10.0.0.2), remplace l'adresse destination par 10.0.0.2 et retransmet le datagramme à A



Identification d'un processus

- Un processus peut être identifié de manière unique sur tout l'internet par un triplet qu'on appellera demi-association ayant la forme

  (

  protocole transport (TCP ou UDP)

  adresse local réseau (IP)

  processus local (numéro de port ou de service)

)
- Il existe 2 protocoles TCP et UDP
- il existe 65535 ports disponibles (moins les 1024 réservés).

Types de translation

- Translation statique
  - consiste à associer une adresse IP publique à une adresse IP privée interne au réseau
- Translation dynamique
  - Port Forwarding (extension de NAT)
    - consistant à configurer la passerelle pour transmettre à une machine spécifique du réseau interne, tous les paquets reçus sur un port particulier ex: serveur web

IPv4 vs IPv6

L’adresse IPv4

- **Qu'est-ce qu'une adresse IPv4 ?**
  - ***194.153.205.206***

- **Comment déchiffrer une adresse IP**
  - **[xxx]^{1}.[xxx.xxx.xxx]^{2}**
    - ^{1}*netID* (partie reseaux)
    - ^{2}*host-ID* (partie ordinateur)

Les problèmes d'IPv4

- Espace d'adressage trop petit
- Explosion des tables de routage
- Nouvelles fonctionnalités mal intégrées :
  - Multicast
  - Sécurité
  - Mobilité

Mesures d’urgence

- Les adresses Internet sont utilisées en interne
- Agrégation de réseaux en un préfixe (CIDR)
- Utilisation de NAT pour sortir sur Internet

IPsec

- Algorithme de cryptographie (RSA)
- IPsec opère à la couche réseau (couche 3 du modèle OSI) , donc indépendant des application (couche 7)
- Les utilisateurs n'ont pas besoin de configurer chaque application
- IPsec est souvent un composant de VPN (Virtual Private Network)
- Uniquement les données qui sont chiffrées, pas l'entête sinon problème pour traverser un serveur NAT(Network address translation)

Ce que les mesures d'urgence ont permis

- De gagner du temps pour définir une nouvelle version d'IP, IPv6
- IPv6 conserve les principes qui font le succès d'IP (modèle de bout en bout, le best Effort…)
- Corriger certains problèmes d'IPv4

Protocole IPv6

Documentation

- Les RFC, documents officiels :

  ftp://ftp.inria.fr/pub/rfc

- "IPv6" du collectif "Gisèle Cizault" chez 0'Reilly. Ouvrage en français de référence.
- De nombreux sites Web comme

  http://fr.wikipedia.org/wiki/IPv6

Introduction à IPv6

- **Un plus grand espace d'adressage** Supporter des milliards d'ordinateurs, en se libérant de l'inefficacité de l'espace des adresses IP actuelles,

  IPv4 : 32 bits, soit 2^{32} adresses = 4.3 10^{9} = 4 milliards

  IPv6 : 128 bits soit 2^{128} adresses = 344 10^{36}

  = 344 milliards de milliards de milliards

  La terre fait environ 510 millions de km², cela donne :

  674 10^{15} adresses par mm²,

  y compris sur les océans

- Simplifier le protocole, pour permettre aux routeurs de router les datagrammes plus rapidement, Réduire la taille des tables de routage,

Introduction à IPv6

- Fournir une meilleure sécurité (chiffrement, authentification et confidentialité) que l'actuel protocole IP,
- IPsec fait partie des spécifications de base du protocole
- Accorder plus d'attention au type de service, et notamment aux services associés au trafic temps réel, faciliter la diffusion multi-destinataire en permettant de spécifier l'envergure,

Introduction à IPv6

- **L’auto configuration,** protocole de découverte des voisins. L’auto-configuration permet à un équipement de devenir complètement «plug-and-play».
- Donner la possibilité à un ordinateur de se déplacer sans changer son adresse, permettre au protocole une évolution future.
- Accorder à l'ancien et au nouveau protocole une coexistence pacifique.

Introduction à IPv6

- Le protocole **IPv6** maintient les meilleures fonctions d'IPv4, en écarte ou minimise les mauvaises, et en ajoute de nouvelles quand elles sont nécessaires.
- IPv4 entête comprend 14 champs, alors que IPv6, à une entête comprend 7 champs

➔permet aux routeurs de traiter les datagrammes plus rapidement et améliore globalement leur débit.

Notation

- Les adresses IPv6 sont notées en hexadécimal doublement pointée :

  6453:9A32:E456:FFFF:2:34E3:23:4E3

- Pour le détail de la structure, voir :

http://www.iana.org/ipaddress/ipv6-allocation-policy-26jun02

Rappel IPv4

32 bits				
Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)	
Identification (16 bits)			Drapeau (3 bits)	Décalage fragment (13 bits)
Durée de vie (8 bits)		Protocole (8 bits)	Somme de contrôle en-tête (16 bits)	
Adresse IP source (32 bits)				
Adresse IP destination (32 bits)				
Données				

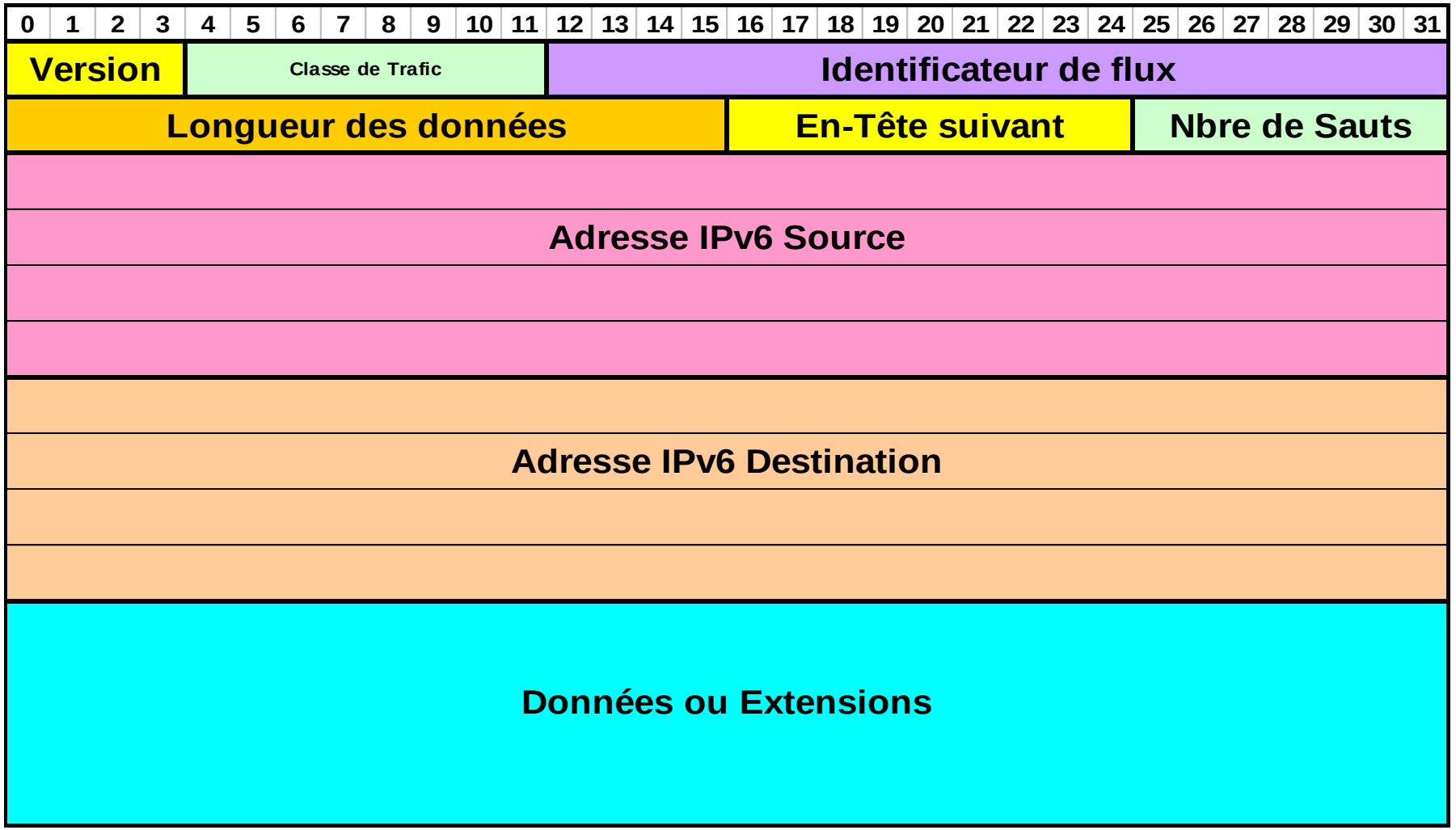
Rappel IPv4 suite

- **Version** (4 bits) : il s'agit de la version du protocole IP que l'on utilise (0100 : IPv4 et 0110 : IPv6)
- **Longueur d'en-tête**, ou *IHL* pour *Internet Header Length* (4 bits) : il s'agit du nombre de mots de 32 bits constituant l'en-tête (nota : la valeur minimale est 5).
- **Type de service** (8 bits) : il indique la façon selon laquelle le datagramme doit être traité.
- **Longueur totale** (16 bits): il indique la taille totale du datagramme en octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.
- **Identification, drapeaux (flags) et déplacement de fragment** sont des champs qui permettent la fragmentation des datagrammes.

Rappel IPv4 Suite

- **Durée de vie appelée aussi TTL**, pour *Time To Live* (8 bits) : ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus.
- **Protocole** (8 bits) : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme
  - ICMP : 1 , IGMP : 2 , TCP : 6 , UDP : 17
- **Somme de contrôle de l'en-tête**, ou en anglais *header checksum* (16 bits) : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête
- **Adresse IP source** (32 bits) , **Adresse IP destination** (32 bits)

IPv6


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version
Classe de Trafic
Identificateur de flux
Longueur des données
En-Tête suivant
Nbre de Sauts
Adresse IPv6 Source
Adresse IPv6 Destination
Données ou Extensions

Datagramme de IPv6

- **Le champ Version** (4 bits), les routeurs devront examiner ce champ pour savoir quel type de datagramme ils routent.

- **Le champ Classe de trafic** (codé sur 8 bits) est utilisé pour distinguer les sources qui doivent bénéficier du contrôle de flux des autres équivalent type service pour IPv4. Les valeurs de 0 à 7 sont affectées aux sources capables de ralentir leur débit en cas de congestion (1 pour les news, 4 pour ftp, 6 pour telnet, etc.) et les valeurs de 8 à 15 sont assignées aux trafics temps réel (audio, vidéo, etc.)

- **Le champ Identificateur de flux** (Flow label sur 20 bits) contient un numéro unique choisi par la source qui a pour but de faciliter le travail des routeurs et de permettre la mise en œuvre les fonctions de qualité de services

- **Le champ Longueur des données utiles** (*payload 16 bits*) sur deux octets, ne contient que la taille des données utiles, sans prendre en compte la longueur de l'en-tête.

Datagramme de IPv6

- **Le champ En-tête suivant** (Next header 8 bits) a une fonction similaire au champ *protocole* du paquet IPv4 : Il identifie tout simplement le prochain en-tête (dans le même datagramme IPv6). Il peut s'agir d'un protocole (de niveau supérieur ICMP, UDP, TCP, ...) ou d'une extension

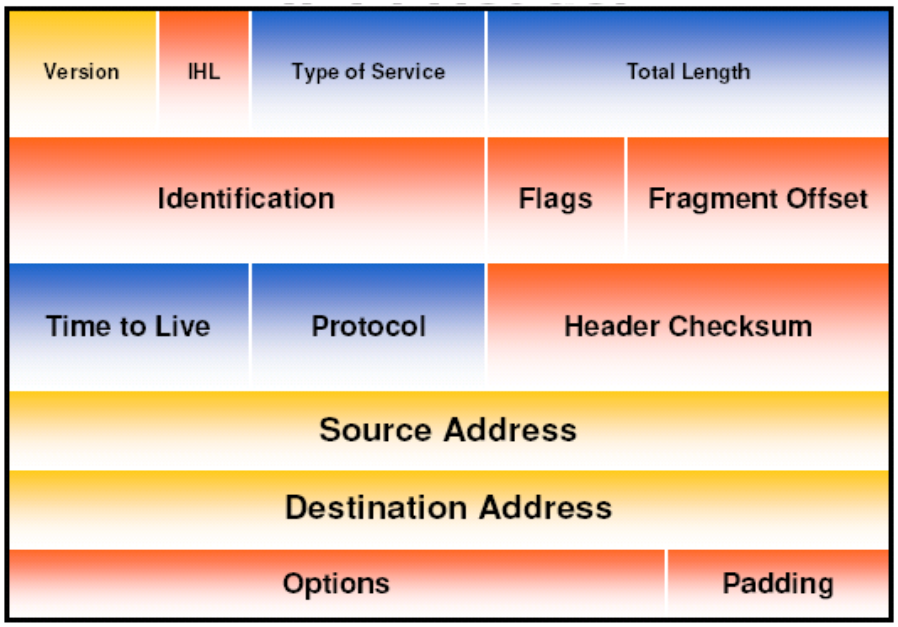
  - 01 - 00000001 - ICMP
  - 02 - 00000010 - IGMP
  - 06 - 00000110 - TCP
  - 17 - 00010001 - UDP
  - 58 - 00111010 - ICMPV6

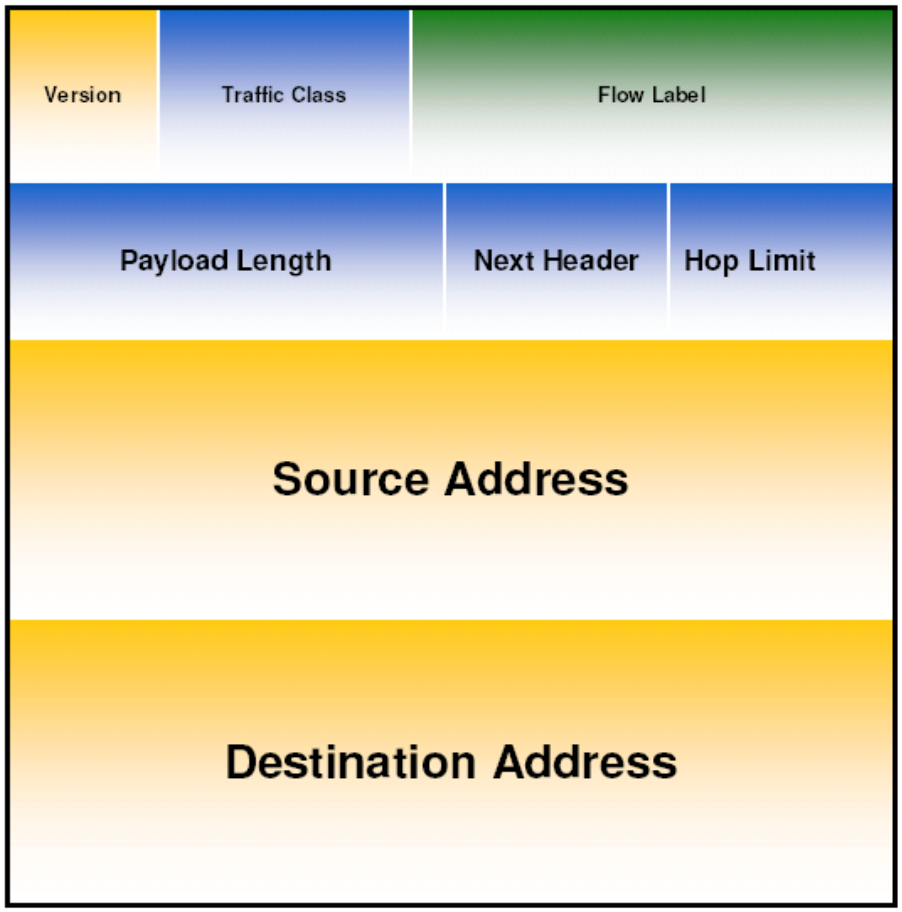
  - 00 - Option Sauts après sauts
  - 60 - Option Destination
  - 43 - Option Routage
  - 44 - Option Fragmentation
  - 51 - Option AH
  - 50 - Option ESP

- **Le champ Nombre de sauts** (Hop limit sur 8 bits) remplace le champ *"TTL"* (*Time-to-Live*) en IPv4. Sa valeur (sur 8 bits) est décrémentée à chaque nœud traversé. Si cette valeur atteint 0 alors que le paquet IPv6 traverse un routeur, il sera rejeté avec l'émission d'un message ICMPv6 d'erreur. Il est utilisé pour empêcher les datagrammes de circuler indéfiniment.

- **Adresse source** et **Adresse de destination sur 16 octets (128 bits)**

IPv4 vs IPv6





Legend

- field's name kept from IPv4 to IPv6
- fields not kept in IPv6
- Name & position changed in IPv6
- New field in IPv6

IPv4 vs IPv6

- La taille de l'en-tête est fixe, le champ IHL (IP Header Length) est donc inutile.
- Le champ *Time to Live* (TTL) est renommé en *Hop Limit*, reflétant la pratique .
- Il n'y a pas de somme de contrôle sur l'en-tête. En IPv4, cette somme de contrôle inclut le champ TTL et oblige les routeurs à le recalculer dans la mesure où le TTL est décrémenté. Ceci simplifie le traitement des paquets par les routeurs.
- Le champ *Payload length* n'inclut pas la taille de l'en-tête standard (ni des en-têtes optionnels qui suivent), contrairement au champ *Total length* d'IPv4.

IPv4 vs IPv6

- Tous les champs relatifs à la fragmentation ont été retirés, parce qu'IPv6 a une approche différente de la fragmentation.
- La fragmentation se fait au niveau de la source et non plus au niveau du routeur
- tous les ordinateurs et routeurs conformes à IPv6 doivent supporter les datagrammes de 576 octets. Si un routeur ne support pas cette taille, retourne un message d'erreur à la source

Notation IPv6

- Adresse IPv6

  8000:0000:0000:0000:0123:4567:89AB:CDEF

- Optimisation

  8000::123:4567:89AB:CDEF

- Insensible à la casse

  8000::123:4567:89ab:cdEF

- Ecriture des **URL:**

  http://[2002:400:2A41:378::34A2:36]:8080

Adressage

- Ecriture d’une adresse IPv4 en notation IPv6
  ::192.31.254.46
- Comme exception spéciale à la notation des adresses IPv6, les adresses correspondant à l'IPv4 sont communément représentées avec leurs 32 bits significatifs notés comme en IPv4.
- ➔::ffff:c000:280 sera souvent noté ::ffff:192.0.2.128 .

Les types d’adresse IPv6

IPv6 reconnaît 3 types d'adresses

- ✓ L'adresse UNICAST, est une adresse classique.
  Elle correspond à une interface.
  Le paquet sera remis à une et une seule interface.
- ✓ L'adresse ANYCAST

  Elle correspond à une ensemble d'interfaces mais le paquet n'est délivré qu'à une seule interface (la plus proche en général). Elle permet d'obtenir une information détenue par plusieurs interfaces (routeurs par exemple).
- ✓ Le BROADCAST d'IPv4 disparaît dans IPv6 (envoyer la même trame à toutes les machines d’un même sous réseau).

IPv6 Multicast

- ✓ L'adresse MULTICAST
  Elle correspond à un ensemble d'interfaces.
  Le paquet sera remis à toutes les interfaces qui peuvent être n'importe où sur l'Internet. Une interface peut rejoindre un groupe ou le quitter.
  «one – to – many » ou « many – to – many »

- **Historique**
  - **IPv4 – 1985 – RFC966**
  - **Multicast – 1991 – Steve Deering – thèse**
  - **« AUDIOCAST » – 1992 – réunion IETF**

IPv6 Multicast

- **Pourquoi le Multicasting ?**
  - **un groupe d'utilisateurs**
    - Applications Multimédia (télévision sur internet)
    - Partage de ressources
    - Gestion de bases de données distribuées
  - **une seule adresse IP**
    - Minimiser l 'utilisation des ressources du réseau
    - Meilleure gestion du groupe

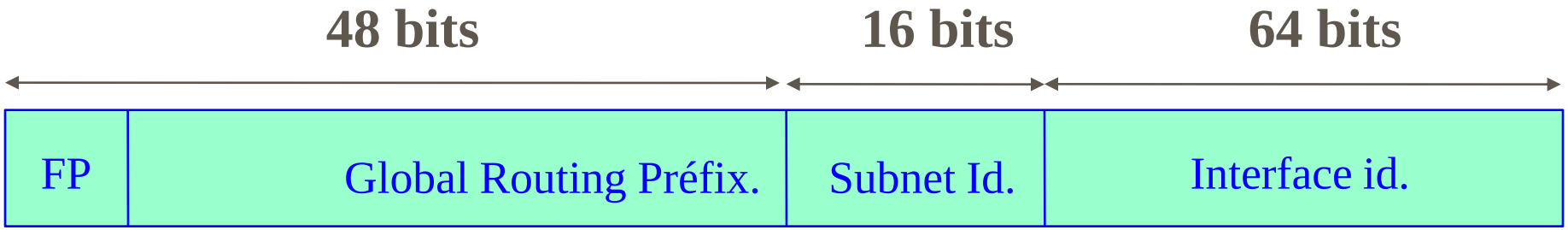
Le fonctionnement d'IPv6 est très similaire à celui d'IPv4

- Les protocoles TCP et UDP sont pratiquement inchangés. Ceci est résumé par la formule « 96 bits de plus, rien de magique »
- Les réseaux sont notés en utilisant la notation CIDR : la première adresse du réseau est suivie par une barre oblique et un nombre qui indique la taille en bits du réseau. La partie commune des adresses est appelée *préfixe*.

Le plan d'adressage global de IPv6 unicast et anycast

Les adresses Unicast globales affectées aux organismes régionaux

Défini dans le RFC 3587, il est subdivisée comme suit :



<préfixe-ipv6> / <longueur du préfixe>

2001:660:7401::/48 représente un réseau

2001:660:7401:202::66/64 représente une machine

Le plan d’adressage global de IPv6

- Le Global Routing Prefix est attribué par un organisme officiel et identifie le site. Ce préfixe est, en général, de longueur 48 pour un site final.
- La partie subnet ID de l’adresse sur 16 bits est de la responsabilité du site, elle offre la possibilité de subdiviser le site en 65534 sous réseaux.
- La dernière partie, en général sur 64 bits, est l’identifiant d’interface et permet d’identifier la machine dans un réseau donné. Elle identifie plus exactement une interface d’un équipement.

Structure des adresse IPv6

Dans l'ordre, de gauche à droite :

- *préfixe* (3 bits: 010) : identification de l'adressage (unicast fournisseur, unicast géographique, locale, multicast, ..)
- *registry ID* (5 bits) : identification de l'autorité régionale dont dépend le fournisseur d'accès (actuellement, trois registres ont été définis : Amérique du nord, Europe et Asie-Pacifique)

Chaque autorité affecte les 15 octets restants :

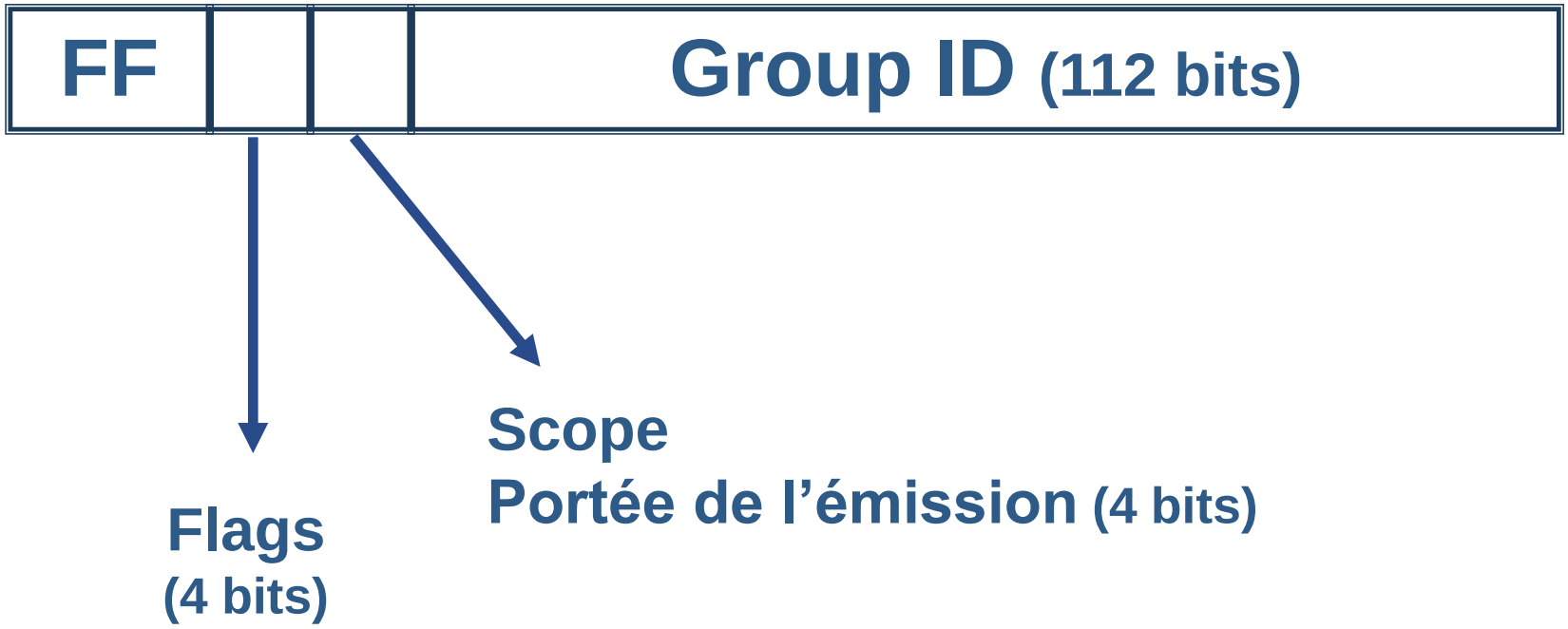
- *provider ID* (9 bits) : identification du fournisseur d'accès
- *subscriber ID* (16 bits) : identification du site de l'abonné

- *subnetwork ID* (16 bits) : identification du sous-réseau

- *interface ID* (64 bits) : identification de l'interface

Adresse multicast IPv6

- **Préfixe ff00:/8**



Les types d’adresse IPv6

- Certains préfixes d'adresses IPv6 jouent des rôles particuliers

Type d'adresses IPv6	
Préfixe	**Description**
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques
fe80::/10	Adresses locales lien
ff00::/8	Adresses multicast

Quelques préfixes

- Le préfixe 2001:db8:1f89::/48 représente des adresses de
  2001:db8:1f89:0:0:0:0:0 et finit à 2001:db8:1f89:ffff:ffff:ffff:ffff:ffff.

- Le préfixe 2000::/3 représente les adresses de :

2000 en binaire 0010 0000

Adresse de début : 0010 0000…00000000 ou 2000:0:0:0:0:0:0:0

Adresse de fin : 00111111…11111111 ou 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- Le préfixe fc00::/7 représente les adresses de
  fc00:0:0:0:0:0:0:0 à fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- Le préfixe fe80::/10 représente les adresses de
  fe80:0:0:0:0:0:0:0 à febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Quelques adresses particulières

- ::1/128 est l'adresse de loopback (équivalente à l'adresse 127.0.0.1) :

  0:0:0:0:0:0:0:1 ou ::1

- ::/128 est l'adresse non spécifiée, adresse indéterminée pendant l'initialisation (DHCPv6) d'une adresse IPv6 :

  0:0:0:0:0:0:0:0 ou ::

Identifiant d’interface

L'IEEE (Institut for Electrical and Electronics Engineers) propose actuellement 3 identificateurs universels :

- MAC-48 (couche 2)
- EUI-48
- EUI-64

MAC = *Media Access Control*

EUI = Extended Unique Identifier

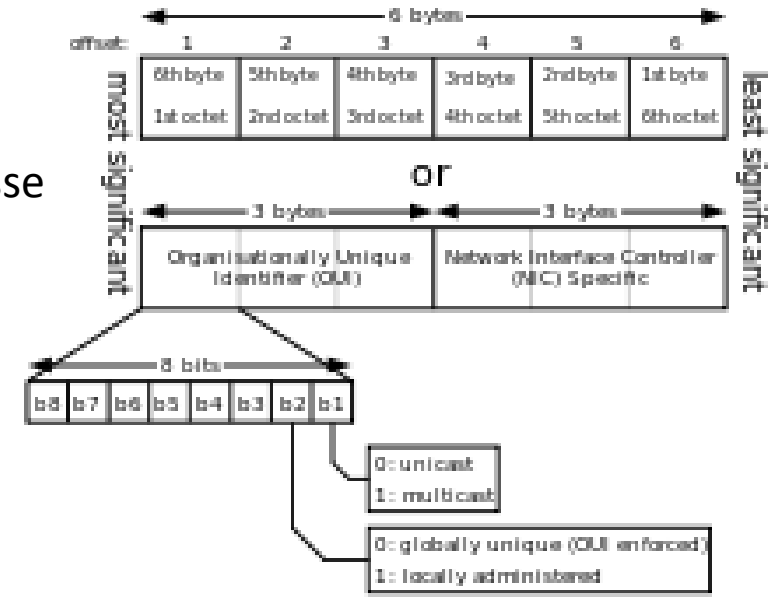
Identifiant d’interface

- Le format EUI-48 et le format MAC-48 sont sur 48 bits et sont sémantiquement identiques.
- Le format EUI-48 est par contre un identificateur plus général pouvant identifier des logiciels comme des périphériques divers.

Identifiant d'interface

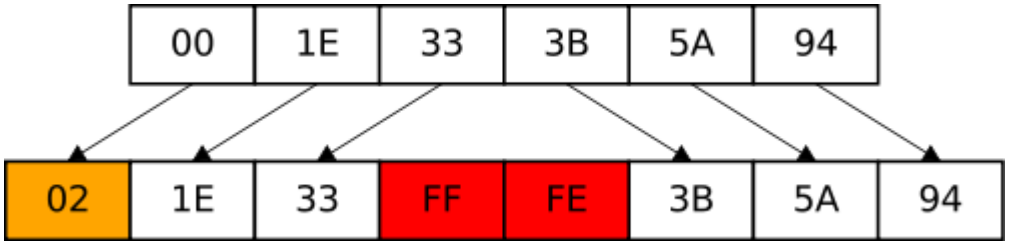
- Cet identifiant d'interface ou EUI-64 est codé sur 64 bits
- Il facilite l'auto-configuration.
- Cet identifiant est créé à partir d'une adresse MAC (48 bits, définie par l'IEEE) selon le mécanisme suivant :
- Les 3 premiers octets de la MAC adresse identifient le constructeur et les 3 derniers le matériel.

22 bits réservés : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur ;



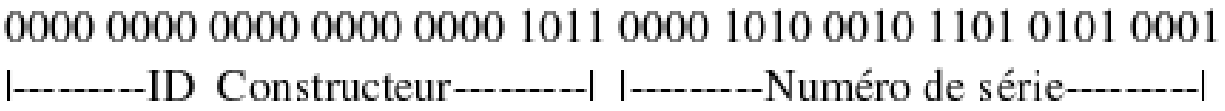
Identifiant d'interface

- On insère FFFE (notation hexadécimale) entre l'identifiant constructeur et l'identifiant matériel.
- Le « Universal/Local-Bit » (7^{ième} bit) est positionné à 1 et indique un identifiant d'interface globalement unique conformément à la norme IEEE (EUI-64).



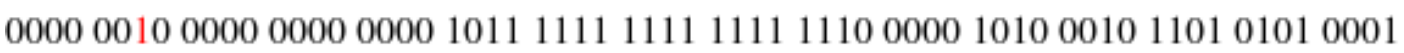
Exemple

- Soit l'adresse MAC suivante : 0000:0B0A:2D51
- En binaire



- On insère FFFE

- Bit U/L positionné à 1 (7ème bit) :



- Résultat EUI-64 : 0200:0BFF:FE0A:2D51

IPv6 : adressage automatisé

- Configuration manuelle : l'administrateur fixe l'adresse (Les adresses constituées entièrement de 0 ou de 1 ne jouent pas de rôle particulier en IPv6).
- DHCPv6 Stateful : exactement le même principe que le DHCPv4, non utilisation de l’adresse MAC
- DHCP Stateless: autoconfiguration sans état (DHCP fournit uniquement les options (serveur DNS, ..)
- Adressage Stateless, le routeur annoncent le préfixe, les clients peuvent composer eux même leur adresse

Attribution des adresses IPv6

Dans les deux dernières méthodes, la machine qui se configure ne reçoit que, au maximum les 64 premiers bits de l'adresses IPv6.

Les 64 derniers bits de son adresse complète sont générés selon :

- le format EUI-64, basé sur l'adresse MAC de l'interface ethernet utilisée
- une procédure aléatoire

Internet Control Message Protocol v6 (ICMPv6)

- ICMPv6 à vu son champ d'action élargi par rapport à la version 4
  - Les message Neighbor Discovery (ND) remplace ARP
  - Les messages ND sont envoyés en multicast
  - Les messages ND prennent également les rôles tenus par ICMP Router Discovery and ICMP Redirect en IPv4
- ICMPv6 est également impliqué dans l'auto configuration d'adresse Stateless

Neighbor Discovery Protocol (NDP)

- NDP remplit une série importante de fonctionnalités:
  - Détection de doublons dans l'adressage
  - Annonce de l'adresse link-local
  - Découverte du voisinnage
  - Résolution d'adresses
  - etc.

Neighbor Discovery Protocol (NDP):

- *Duplicate Address Detection* : détermine si un autre hôte utilise la même adresse IP,
- *Router Discovery* : les hôtes peuvent détecter les routeurs sur les liens auxquels ils sont connectés,
- *Address Autoconfiguration* : assignation automatique d'adresse sans état,
- *Address Resolution* : établissement de la correspondance entre adresse IP et adresse MAC,
- *Next-hop determination* : détermination du routeur pour une destination déterminée,
- *Neighbor Unreachability Detection* : détermine qu'un hôte n'est plus accessible,
- *Redirect* : information qu'un autre routeur sur le lien fournit un meilleur *next hop*.

Migration

Migration progressive des réseaux IPv4 vers IPv6. Trois méthodes vont être utilisées principalement :

- Une pile double (dual stack) IPv4/IPv6 dans le réseau cœur et les terminaux mobiles. Le choix est basé sur le résultat de la requête DNS ou de la préférence de l’application
- L'utilisation de tunnels automatiques et configurés comme 6to4 encapsulation des paquets IPv6 dans IPv4.
- Un protocole de traduction d'IPv4 à IPv6 dans le réseau comme NAT-PT.

Les commandes et fonctionnalités IPv6

- Commande ping6
  - ping6 -I eth0 ::1 # ping de l'adresse de bouclage
  - ping6 -I eth0 ff02::1 # permet de voir tous les hôtes actifs sur le lien
  - ping6 -I eth0 fe80::20e:35ff:fe8f:6c99 #ping de l'adresse IPv6 d'un autre poste
- Affichage
  - ifconfig |grep inet6 # affiche uniquement les adresse IPv6
- Montage et démontage des interface
  - # ip link set dev interface up# ip link set dev interface down

Les commandes et fonctionnalités IPv6

- Configurer manuellement une adresse IPv6
  - # ifconfig eth0 inet6 add 3ffe:ffff:0:f101::1/64
  - # ip -6 add 3ffe:ffff:0:f101::1/64 dev eth0
  - # ip -6 del 3ffe:ffff:0:f101::1/64 dev eth0
- Affichage de la table de routage
  - # ip -6 route show [dev peripherique]
  - # ip -6 route show
  - # route -A inet6 # route -A inet6 |grep eth0
  - # pour afficher seulement ce qui concerne l'interface eth0

Les commandes et fonctionnalités IPv6

- Commande traceroute6
  - # traceroute6 www.6bone.net
  - # traceroute6 2001:5c0:0:2::24
- Commande tracepath6
  - # tracepath6 2001:5c0:0:2::24
- Commande d'affichage du voisinnage
  - ip -6 neigh show [dev péripherique]