GTI611

Chapitre 3: Protocole IPv6

Chargée de cours: Souad Hadjres

Protocole IPv6

- **Rappel IPv4**
- **Protocole IPv6**
  - En-tête IPv6
  - Adresses IPv6
  - En-têtes d’extension
- **Protocole NDP**
- **Déploiement de IPV6 avec IPv4**

IPv4

- Taille des adresses limitée à 32 bits

  - épuisement des adresses (dernier espace non-assigné alloué en février 2011 à un registre régional)

- Limitation au niveau: sécurité, QoS, mobilité, etc.

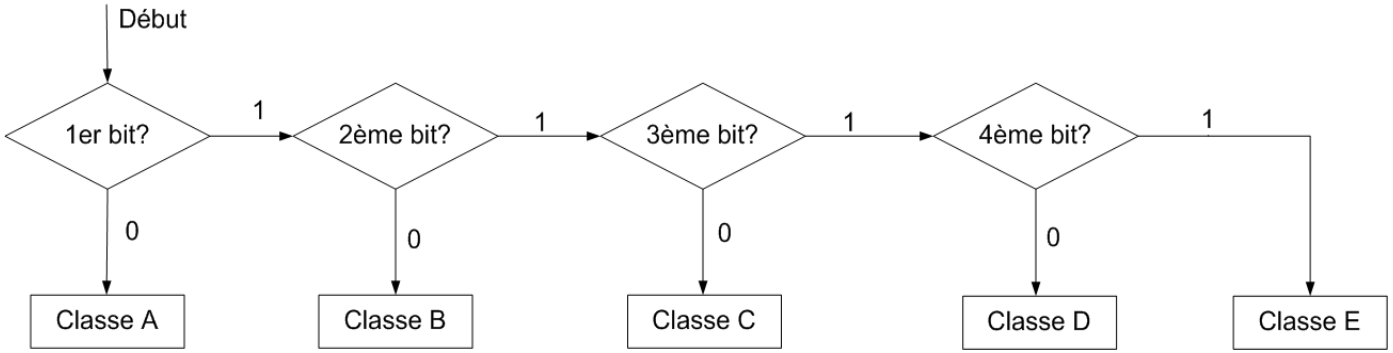
IPv4 - Rappel

- Deux types de notations:
  - Binaire: 10000000 00001011 00000011 00011111
  - Décimal: 128.11.3.31
- L'espace d'adresse IP est divisé en 5 classes:

Source : B. A. Forouzan

IPv4

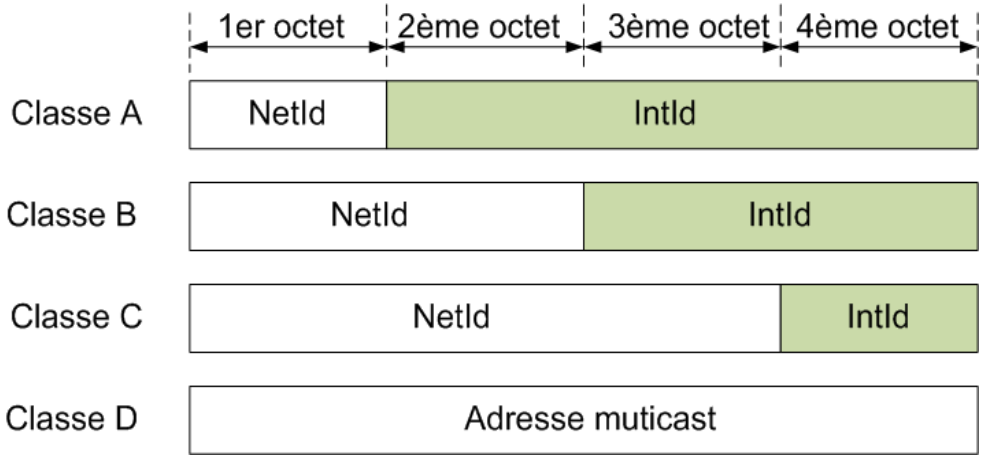
- Procédure de vérification de la classe d'adresse



- Exemple: Trouvez la classe des adresses suivantes:
  - 10100001 00001011 00011011 11101111
  - 222.5.15.111
- Les adresses des classes A, B et C sont utilisées pour les communications unicast.
- Les adresses de la classe D sont utilisées pour les communications multicast.
- Les adresses de la classe E sont réservées pour un usage futur.

IPv4

- Identificateurs de réseaux et d'interfaces:



- La classe A compte jusqu'à 2^7 réseaux, possédant chacun jusqu'à 2^{24} (16 777 216) interfaces. Nombre des adresses d'interfaces très large.
- La classe B compte jusqu'à 2^{14} réseaux, chacun d'une capacité de 2^{16} (65536) interfaces. Nombre des adresses d'interfaces large.
- La classe C permet d'identifier jusqu'à 2^{21} réseaux, chacun d'une capacité de 2^8 interfaces. Nombre des adresses d'interfaces limité à 254.

Adressage– Protocoles d’adressage

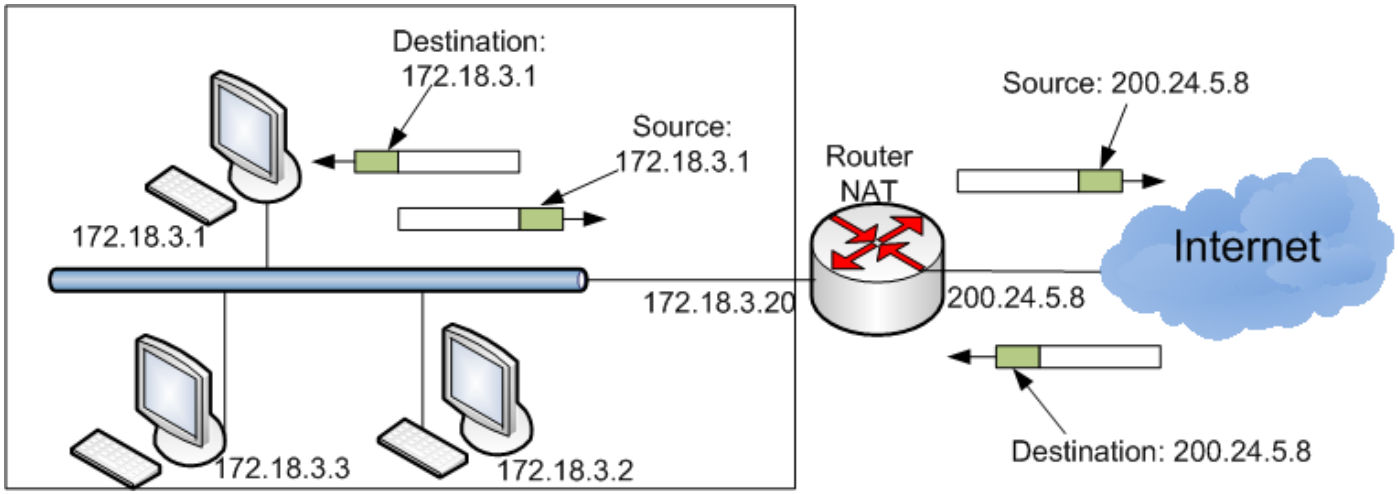
- Classes d’adresses non flexibles par rapport à la taille de la plupart des organisations.
- Manque d’adresses.
- Solution court terme:
  - Allocation flexible des adresses CIDR (Classless interdomain routing)
  - Adressage privé et translation NAT (Network address translation)
  - Partage dans le temps DHCP (Dynamic host configuration protocol).

Adressage - CIDR

- CIDR (Classless interdomain routing): allocation flexible des adresses
  - NetId peut-être de n'importe quelle taille.
  - Forme de l'adresse *a.b.c.d/x*, avec x nombre de bits NetId.
  - Exemple:
    - une entreprise comptant 2000 ordinateurs peut ainsi utiliser 2^{11} (2048) adresses de la forme *a.b.c.d/21*.
    - Elle peut subdiviser ce groupe de 11 bits à l'aide de la procédure de subdivision en sous-réseau (subnetting) afin de créer des réseaux internes.
  - Routage complexe.

Adressage – NAT

- NAT : adressage privé et translation
  - Permet de créer plusieurs adresses à l'intérieur d'un réseau et auxquelles correspondent une ou plusieurs adresses à l'extérieur de ce même réseau.
  - Trois sortes d'adresses peuvent être utilisées pour des réseaux privés:
    - 10.0.0.0 à 10.255.255.255 , total 2^{24} adresses.
    - 172.16.0.0 à 172.31.255.255, total 2^{20} adresses.
    - 192.168.0.0 à 192.168.255.255, total 2^{16} adresses.



Source: B. A. Forouzan

Adressage – DHCP

- DHCP: partage d'adresses dans le temps
  - permet à un équipement terminal d'obtenir une adresse IP de manière automatique ainsi que différentes informations utiles telles que l'adresse du routeur de premier bond et de celle de son serveur DNS (Domain name Server).
  - est qualifié de protocole 'Plug and play' permettant à un équipement terminal d'obtenir une adresse permanente ou temporaire.
  - Exemple:
  - Soit un fournisseur d'accès internet ayant 2000 clients résidentiels, parmi lesquels au plus 400 personnes peuvent se connecter simultanément.
  - Avec un serveur DHCP et une assignation d'adresses dynamique temporaire, seulement 2^9 (512) adresses suffisent pour desservir ces personnes. Adresse du type 200.23.30.0/23.

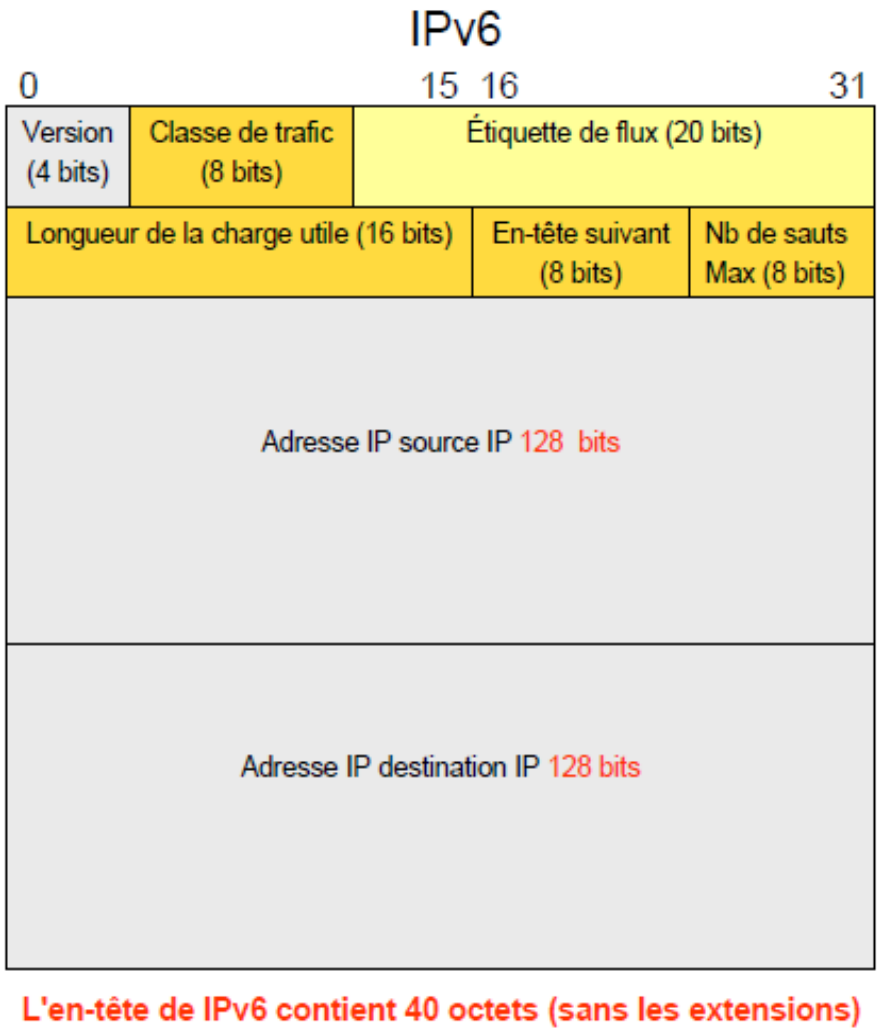
IPv6 - Introduction

- IPv6 a été conçu pour remplacer IPv4 en supprimant certains des problèmes de la version 4 qui date de 1981 (RFC 791)
- Le déploiement d'IPv4 étant très large, IPv6 doit permettre une transition facile, sans interruption ou problème administratif. Les dernières publications relatives à IPv6 concernent les problèmes de transition.
- Le développement exponentiel des appareils pouvant se brancher à l'Internet (cellulaire, télévision, …) et le développement d'applications qui fonctionnent difficilement avec une adresse privée imposent aujourd'hui d'accélérer le déploiement d'IPv6.
  - Téléphonie cellulaire 3G et 4G : 3.3 milliards d'abonnements
  - Nouvelles applications: VoIP, vidéoconférence, etc.

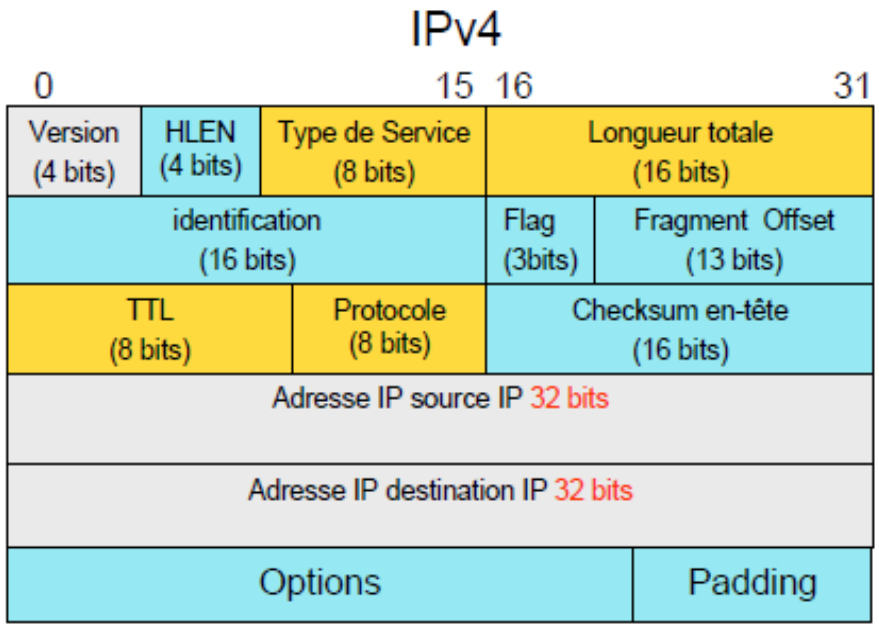
IPv6 - Objectifs

- Supporter la connexion de milliards d'équipements: Augmentation de la taille des adresses de 32 à 128 bits
  - IPv4: $2^{32}=4x10^{9}$, 4 milliards d'adresses
  - IPv6: $2^{128}=3.4 \times 10^{38}$, $7x10^{23}$ adresses par m^2 sur la planète
- Simplifier l'en-tête pour faciliter l'acheminement de paquets
  - Des champs IPv4 ont été supprimés ou sont optionnels
  - Malgré une taille des adresses de 16 octets, l'en-tête ne dépasse pas les 40 octets
- Fournir plus d'options pour plus de flexibilité
  - QoS
  - Sécurité
  - Mobilité

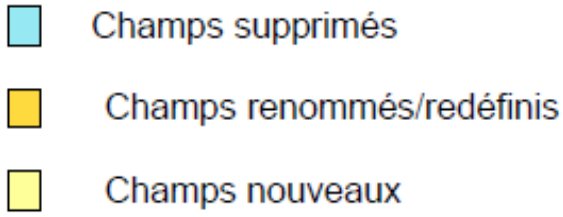
IPv6



L'en-tête de IPv6 contient 40 octets (sans les extensions)



L'en-tête de IPv4 contient 20 octets (sans les options)



Champs en-tête IPv6

- Version (4 bits): version 6 pour IPv6
- Traffic class (Classe de trafic: 8 bits): identifie différentes classes ou priorités pour la QoS (DiffServ). Équivalent de ToS dans IPv4
- Flow label (Étiquette de flux: 20 bits): La source peut utiliser ce champ pour marquer un ensemble de paquets appartenant au même flot (RFC 3697). Peut être utilisé afin établir une correspondance avec les réseaux niveaux 2 (ex. MPLS) pour classer et donner des priorités aux paquets IP.
- Payload Length: Longueur de charge utile uniquement, (dans IPv4 header+payload, les options sont considérées comme faisant partie de la charge utile).

Champs en-tête IPv6

- Next Header (en-tête suivant: 8 bits): équivalent du champ protocole dans IPv4. Utilisé pour identifier le protocole contenu dans le champ de données (TCP/UDP, ICMP, extension d'en-tête, etc.)
- Nombre de sauts limite: Équivalent au TTL dans IPv4

Fragmentation: avec IPv6, le Path MTU est découvert au préalable. La source est le seul nœud pouvant fragmenter un paquet. Chaque nœud doit ajuster ses paquets en fonction du plus petit MTU sur le chemin. Si la découverte du Path MTU n'est pas activée dans un réseau IPv6, le RFC 2460 recommande de se limiter à un Path MTU minimal qui est de 1280 octets.

ICMP: Internet Control Message Protocol, NDP: Neighbor Discovery Protocol

Champs en-tête IPv6

Simplifications IPv6:

- Format fixe des en-têtes: Header Length de IPv4 n'est plus nécessaire. Le champ option remplacé par les extensions de l'en-tête
- Fragmentation:
  - Les champs *Identification*, *Flag* et *Fragment Offset* ne sont plus nécessaires
  - Les hôtes IPv6 doivent utiliser la découverte de MTU (RFC 1981)
  - Pas de fragmentation aux nœuds intermédiaires pour IPv6. Transfert rapide des paquets IP
- Header Checksum
  - Avec IPv4, le Checksum nécessite d'être recalculé à chaque changement de TTL.
  - Pas de header Checksum pour IPv6. Traitement rapide des paquets IP.

IPv6: schéma d'adressage

- Le RFC 4291 de 2006 définit le schéma d'adressage IPv6
- Il existe trois types d'adresses:
  - **Unicast**: Une adresse unicast est un identificateur pour une seule interface. Le paquet est transmis à l'interface possédant cette adresse.
  - **Anycast**: une adresse anycast est un identificateur pour un ensemble d'interfaces appartenant à différents nœuds. Le paquet est transmis à une de ces interfaces, celle qui est la plus proche.
  - **Multicast**: Une interface multicast est un identificateur pour un ensemble d'interfaces appartenant à différents nœuds. Le paquet est transmis à toutes les interfaces identifiées par cette adresse. Il n' y a plus d'adresse broadcast en IPv6. Cette fonction (broadcasting) est assurée par le multicast.

IPv6: schéma d'adressage

- Une adresse est assignée à une interface, pas à un nœud. Une adresse unicast d'une interface peut être utilisée pour identifier le nœud.
- Une interface doit avoir au moins une adresse unicast. Elle peut également avoir plusieurs adresses de chaque type (unicast, anycast et multicast).
- Les adresses IPv6 sont assignées d'une manière hiérarchique
  - Un usager obtient une adresse IPv6 de son Fournisseur d'Accès Internet (FAI)
  - Un FAI obtient un espace d'adressage du Registre Internet Local (RIL), du Registre Internet National (RIN) ou du Registre Internet Régional (RIR)
  - L'organisation IANA alloue un espace adressage aux différents registres RIR:
    - AFRINIC: RIR pour la région d'Afrique
    - APNIC: RIR pour la région Asie/Pacifique
    - ARIN: RIR pour le Canada, USA
    - LACNIC: RIR pour l'Amérique latine
    - RIPE NCC: RIR pour l'Europe, Moyen-Orient et Asie centrale

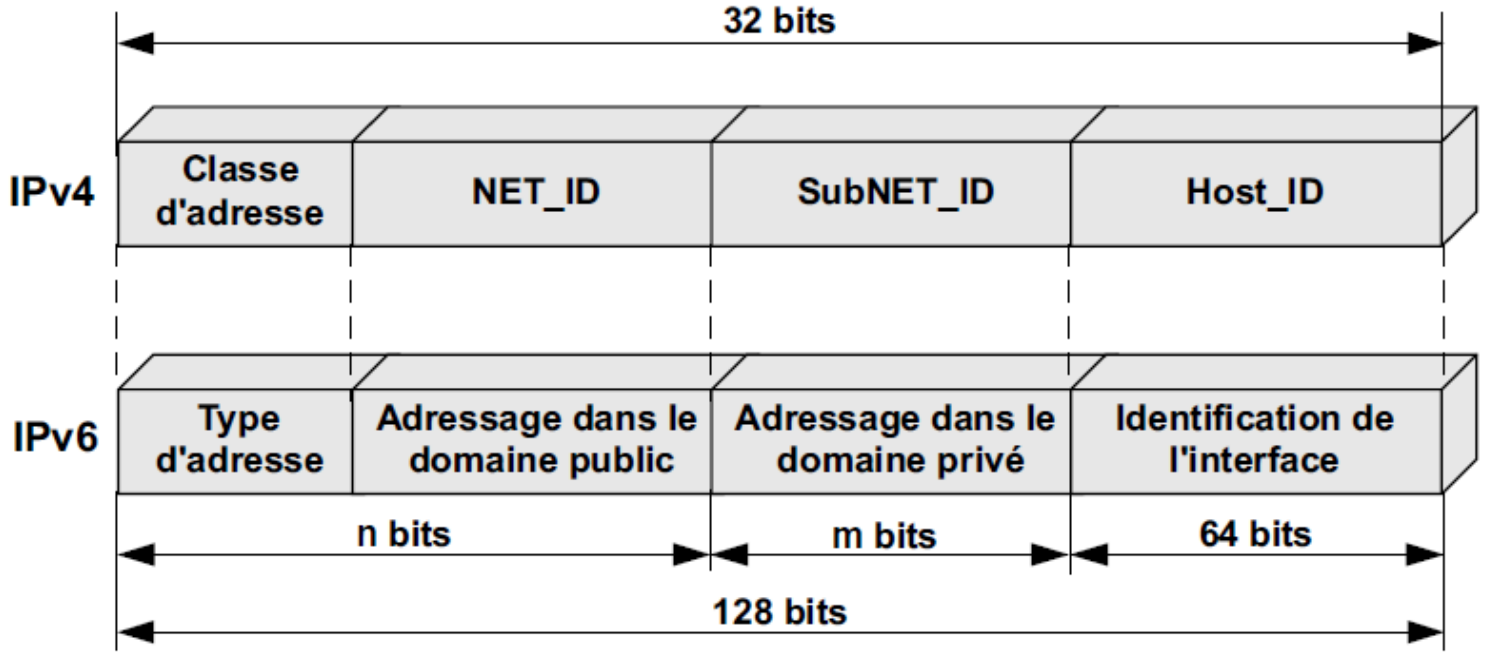
IANA: Internet Assigned Numbers Authority

Source: www.iana.org

Représentation des adresses

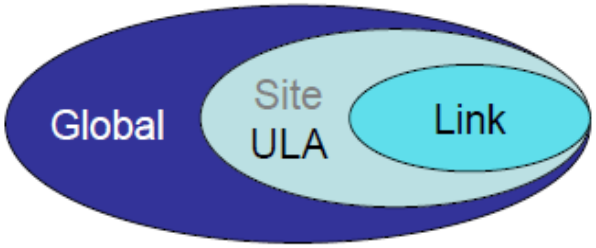
- Il existe trois formes conventionnelles pour la représentation des adresses IPv6 (RFC4291)
  - Forme x:x:x:x:x:x:x:x, où x est la valeur hexadécimale de 16 bits
    - 2001:BA98:7654:3210:FEDC:BA98:7654:3210
    - 2001:0:0:0:8:800:200C:417A
  - Forme de zéros compressés: il sera commun de retrouver une longue chaîne de 0. '::' indique un ou plusieurs groupes de 16 bits de 0. '::' peut apparaître seulement une fois dans une adresse
    - 2001:0000:0000:0000:8:800:200C:417A
    - 2001:0:0:0:8:800:200C:417A
    - 2001**::**8:800:200C:417A
  - Forme combinée: pour les environnements, mixte IPv4 et IPv6. Les 4 derniers octets sont des valeurs décimales
    - 0:0:0:0:0:0:192.168.10.5→::192.168.10.5 IPv6 compatible IPv4 (obsolète)
    - 0:0:0:0:0:FFFF:129.144.52.38 → ::FFFF:129.144.52.38 IPv4 mappée en IPv6
  - Dans les URL: http://[2001:0:0:0:8:800:200C:417A]:8080

Représentation des adresses



Représentation des adresses

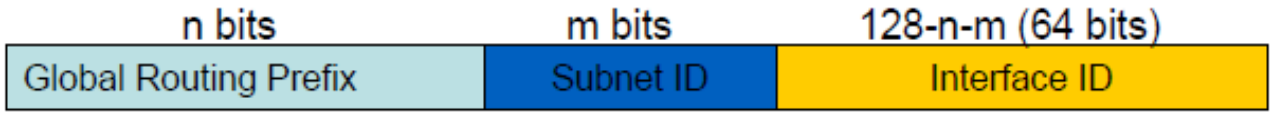
- **Le type d'adresse est identifié par des bits de haut niveau**
  - 0:0:0:0:0:0:0:0/128 — Adresse non spécifiée
  - 0:0:0:0:0:0:0:1/128 — Adresse de bouclage (loopback)
  - FE80::/10 — Adresse unicast locale à un lien
  - FC00::/7 — Adresse unicast local unique (VPN)
  - FF00::/8 — Adresse multicast
  - Autre — Adresse unicast globale
- Les adresses anycast sont prises dans l'espace unicast
- RFC 6164 recommande d'utiliser un préfixe de longueur /127 pour liaisons point à point
  - Raison: Limiter les attaques issues par NDP (Neighbor Discovery Protocol)
- **Les adresses ont une signification:**
  - Globale
  - Locale unique (Locale à un site)
  - Locale à un lien



ULA: Unique Local Address

Adresse unicast globale

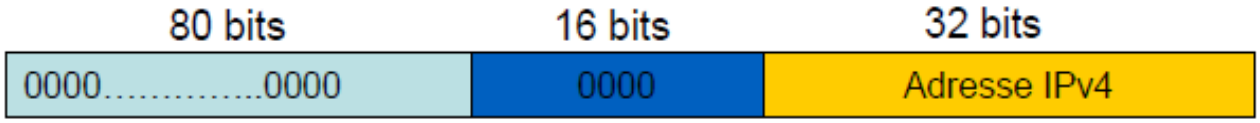
Format général



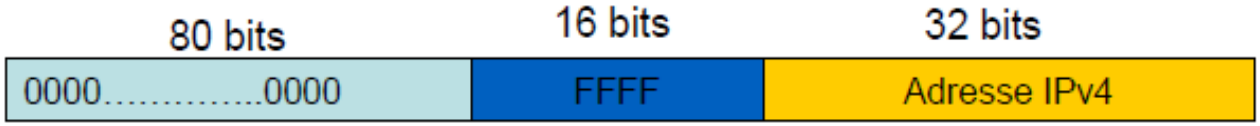
Toutes les adresses, à l'exception de celles commençant par 000, ont un champ Interface ID de 64 bits

Un exemple d'adresse globale commençant par 000 → Adresse IPv6 avec adresse IPv4 incorporée

Format avec IPv4 incorporé



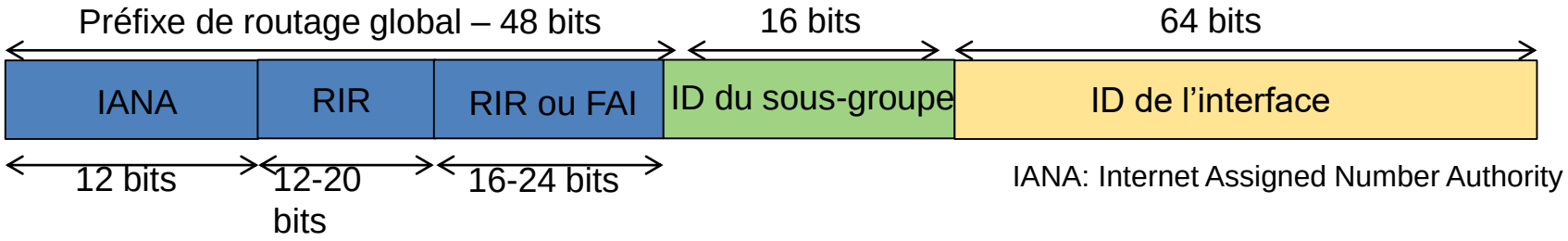
Adresse IPv6 compatible IPv4. Adresse assignée à un nœud IPv6 pour tunneliser les paquets IPv6 sur un réseau ne supportant qu'IPv4



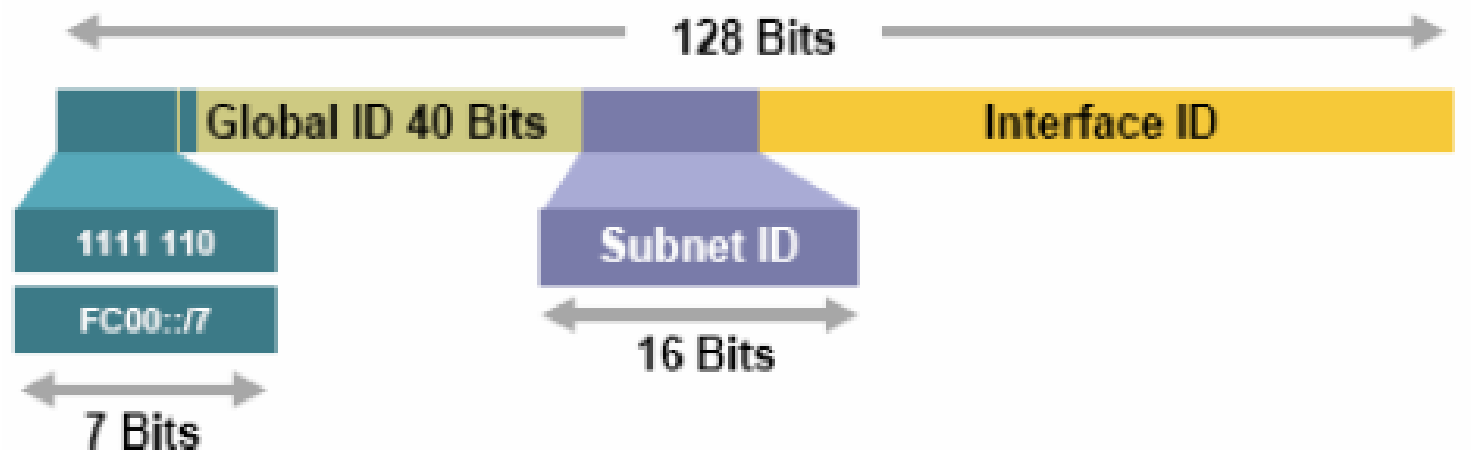
Représente une adresse IPv4 dans une adresse IPv6. Ainsi un paquet IPv4 peut être acheminé sur une infrastructure IPv6.

Adresse unicast globale

- Adresse routable sur Internet
- Subnet ID: C'est un identificateur d'un lien dans un site
- Global routing prefix:
  - Ce préfixe est une valeur assignée à un site (une grappe de sous-réseau/liens).
  - Deux types:
    - Adresse IPv6 dépendante du fournisseur d'accès Internet (Dépendante du FAI - DFAI)
    - Adresse IPv6 indépendante du fournisseur d'accès Internet (Indépendante du FAI - IFAI)
  - L'adresse assignée par un FAI est de type DFAI. C'est une adresse temporaire, car elle doit être modifiée lors du changement du FAI
  - L'adresse assignée par les registres Internet Régionaux (RIR) est du type IFAI
  - Les 3 premiers bits de ce préfixe ont été fixés par IANA à 001 (espace d'adressage unicast global 2000::/3)

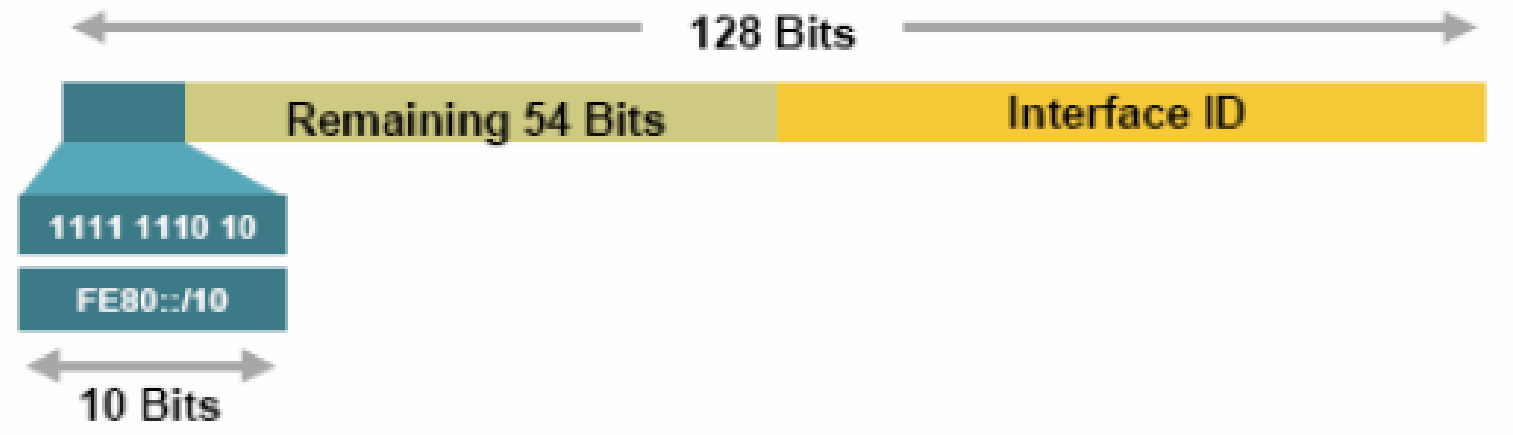


Adresse unicast locale unique



- Identificateur global est généré pseudo-aléatoirement
- Peut être utilisée dans un site pour les réseaux IPv6 privés (pas au niveau de l'internet global)
- Traverse les routeurs, mais uniquement dans un seul site (ces adresses sont routables uniquement dans les sites)
- Peut-être utilisée inter-sites VPN
- Équivalentes aux adresses IPv4 privées
- Adresses: 1111 110 donc FC00::/7

Adresse unicast locale à un lien



- Adresse unicast avec signification locale et unique sur le lien. Elle est générée automatiquement et utilisée pour la configuration d'adresse et la détection de voisins (découverte des voisins et des routeurs)
- N'est valide que sur un lien (elle ne traverse pas les routeurs)
- Adresses: 1111 1110 10 donc FE80::/10

Auto Configuration d'une adresse d'une interface

- Interface ID:
  - utilisé pour identifier une interface sur un lien. Cet identifiant est unique dans un sous-réseau.
  - Configuration de cet identifiant: Statique, via DHCPv6 ou autoconfiguration sans état SLAAC (Stateless Address Autoconfiguration)
  - Configuration SLAAC
    - Disponible sur les interfaces de routeurs compatibles IPv6
    - Permet d'obtenir automatiquement une adresse unique (les informations du routeur par défaut sont fournies via ICMPv6)
    - Adresse construite grâce au 48 bits du nombre MAC des cartes réseau (ex. adresse MAC de 00:E0:4C:39:B2:A9 donne 02E0:4CFF:FE39:B2A9)
      - Adresse dérivée du format IEEE EUI-64
      - Passage de l'adresse MAC Ethernet à une adresse EUI-64 bits
        - 24 premiers bits de l'EUI-64 pour l'identification du constructeur avec inversion du 7e bit
        - 16 bits de valeur FFFE
        - 24 bits suivants identifient le numéro de série.

EUI: Extended Unique Identifier, DHCP:Dynamic Host Configuration Protocol, ICMP: Internet Control Message Protocol, NDP: Neighbor Discovery Protocol

Exemples

root@debian:~# **ifconfig**

Eth0 Link encap:Ethernet Hwaddr b8:27:eb:59:70:f3 => **adresse MAC de 48bits**

Inet adr:192.168.1.119 Bcast:192.168.1.255 Masque:255.255.255.0 => **IPv4**

Adr inet6: fd26:44e1:8c70:fd00:ba27:ebff:fe59:70f3/64 **Scope: site local**

Adr inet6: fe80::ba27:ebff:fe59:70f3/64 **Scope: local Lien**

Adr inet6: 2001:db8:acaf:fd00:ba27:ebff:fe59:70f3/64 **Scope:Global**

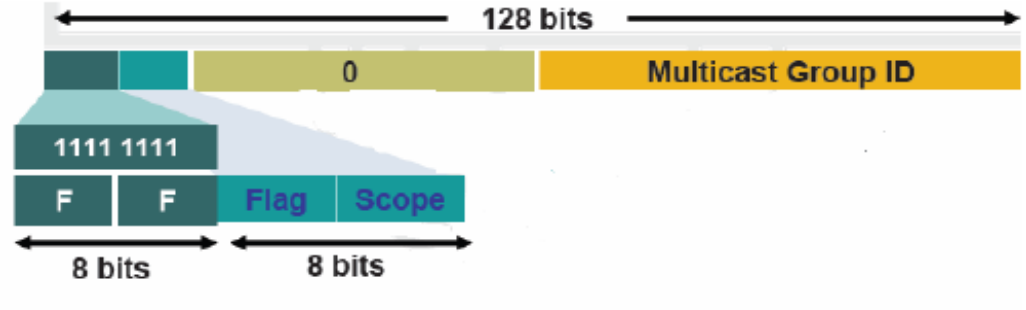
```
R1(config)# interface FastEthernet 0/0
R1(config-if)# ipv6 enable
R1(config-if)# ipv6 address 2001:DB8:0:1::/64 eui-64
R1# show ipv6 interface FastEthernet 0/0
   FastEthernet0/0 is uo, line protocol is up
      IPv6 is enabled. link-local address is FE80::E23F:49FF:FE45:9D7B
      No Virtual link-local address(es):
      Global unicast address(es):
        2001:DB8:0:1::E23F:49FF:FE45:9D7B, subnet is 2001:DB8:0:1::/64 [EUI]
```

Adresse Anycast

- Utilisée pour transmettre un paquet à l'interface, la plus proche, ayant cette adresse
- Une adresse anycast a la même forme qu'une adresse unicast
- Lorsque plusieurs interfaces ont la même adresse, celle-ci devient anycast.
- Un nœud doit être en mesure de distinguer ces adresses
- Ne peut être utilisée comme adresse source.

Adresse multicast

- Identificateur pour un groupe d'interface
- Une interface peut appartenir à plusieurs groupes de multicast

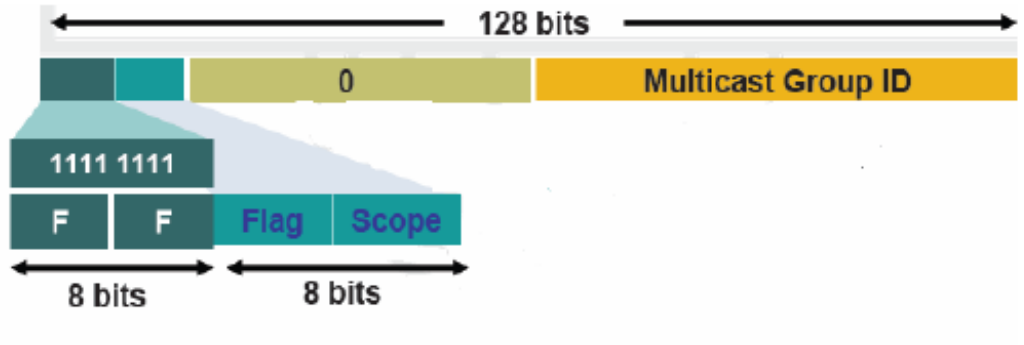


Flag		
	0	If Permanent
	1	If Temporary

Scope		
	1	Node
	2	Link
	5	Site
	8	Organization
	E	Global

- Flag ou champ drapeau = 000T , 000=réservé, T= 0 = Adresse permanente, T = 1 = Adresse temporaire
- Scope ou la portée: utilisé pour limiter l'étendue d'un groupe
- Adresses: 1111 1111 ou FF00::/8
- Exemples:
  - FF02::1 permanente et désigne tous les nœuds du lien
  - FF05::2 permanente et désigne tous les routeurs du site

Adresse multicast



Flag		
	0	If Permanent
	1	If Temporary

Scope		
	1	Node
	2	Link
	5	Site
	8	Organization
	E	Global

- Une adresse multicast permanente a un sens quelque soit son étendue.
- Son identifiant de groupe est réservé pour toutes les portées.
- Exemple: l'identifiant 0x101 est réservé pour les serveurs NTP (Network Time Protocol), donc:

ff01::101 représente tous les serveurs NTP de la même interface que l'émetteur

ff02::101 représente tous les serveurs NTP du même lien que l'émetteur

ff05::101 représente tous les serveurs NTP du même site que l'émetteur

ff0E::101 représente tous les serveurs NTP de l'Internet

Planification adressage IPv6

- Pour une organisation, la planification de l'adressage IPv6 revient le plus souvent à l'affectation des 16 bits de l'ID du sous-réseau
- Types d'affectations
  - Affectation d'adresse selon le nombre de sites
  - Affectation d'adresse au sein d'un site
  - Affectation d'adresse basée sur les fonctions d'un site
  - Affectation d'adresse basée sur l'emplacement de site (site contenant des sous-sites)

Affectation d'adresses selon le nombre de sites

Préfixe de routage global	Nombre de sites
/48	1
/44	16
/40	256
/36	4096
/32	65536

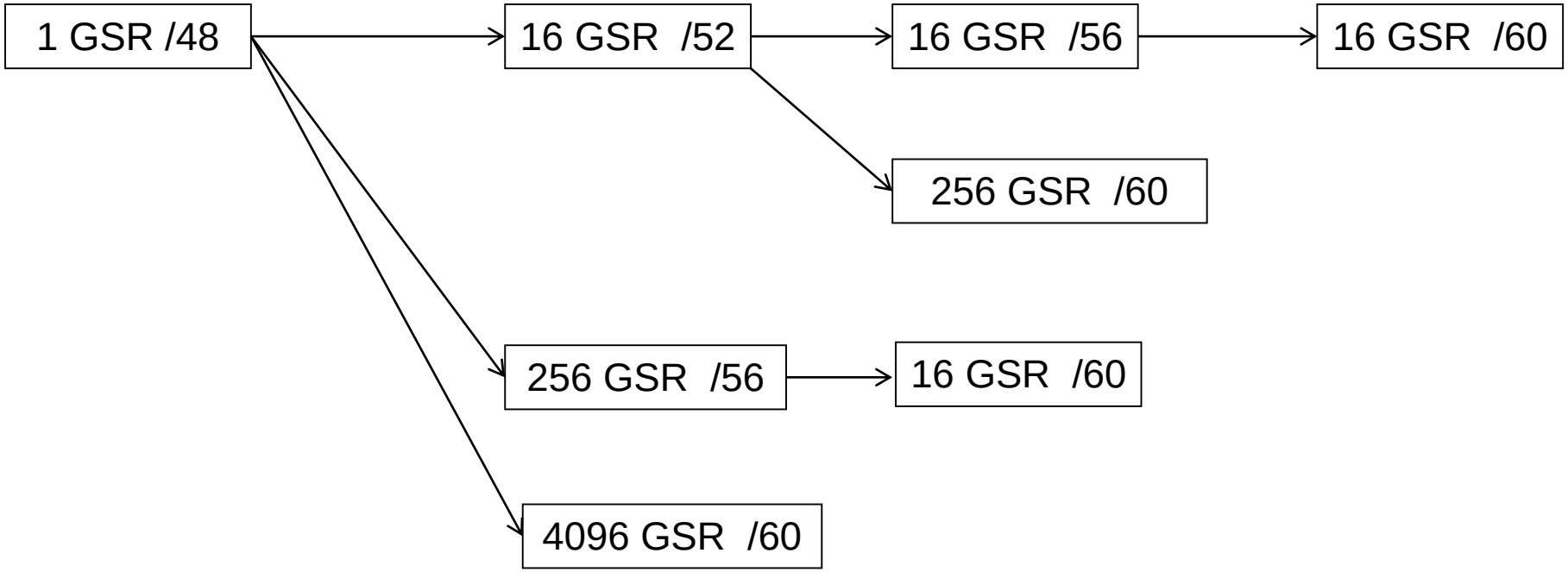
- Peu de chances qu'une organisation demande plus de 65536 sites
- Tailles des préfixes de routage global choisies sont des multiples de 4 bits pour avoir un préfixe plus lisible.

Affectation d'adresses au sein d'un site

- On peut avoir 1 sous-réseau (SR)/site ou des groupes de sous-réseaux (GSR)/site
  - Vu le nombre important de sous-réseaux, il est judicieux de définir des GSR pour faciliter l'agrégation du routage, l'application de la sécurité, la gestion et l'opération d'infrastructures réseau
  - Le nombre de GSR dépend de la croissance prévue pour une organisation. Un espacement intermédiaire de 4 bits doit être prévu pour faire face à cette croissance
  - La taille et l'affectation d'adresses des GSR sont basées sur la fonction et l'emplacement du SR pour lequel l'adressage est fourni.

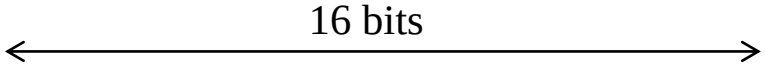
Préfixe de routage global	Nombre de GSR	Nombre de SR
/48	1	65536
/52	16	4096
/56	256	256
/60	4096	16

Affectation de GSR au sein d'un site /48



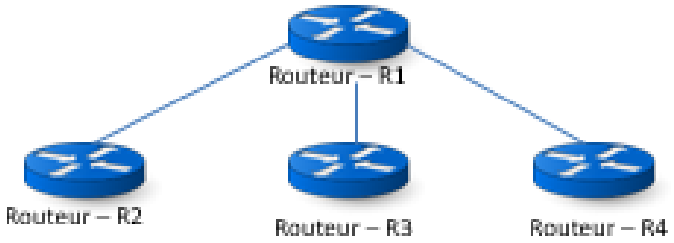
Affectation d'adresses basée sur les fonctions d'un site

- Dans un site, il est généralement souhaitable d'affecter une signification fonctionnelle à un groupe de sous-réseaux (GSR)
- Le nombre de bits alloués à un tel GSR dépend du nombre de fonctions identifiées
- Exemple: 2001:abcd:db12:YYYYXXXXXXXXXXXXXX::/52.
  le champ YYYY représente des bits qui désignent une fonction et X les bits non encore assignés



Affectation d'adresses basée sur les fonctions d'un site

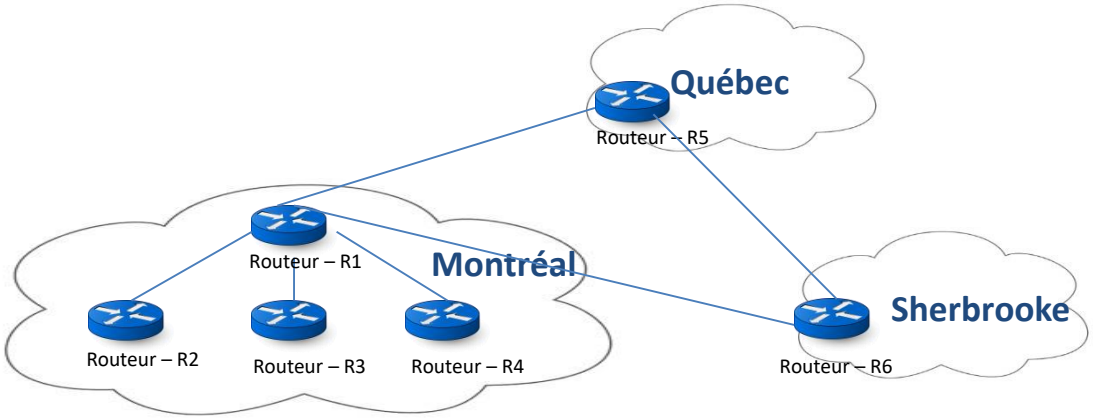
- **Exemple 1** : On veut créer un plan d'adressage pour un réseau d'entreprise subdivisé en sous-réseaux (SR). Chaque SR prend en charge une fonction particulière de l'entreprise. L'entreprise prévoit ajouter des SR supplémentaires pour un usage ultérieur. Proposez un plan d'adressage pour cette entreprise
  - Les fonctions planifiées: 1) VoIP, 2) Surveillance Vidéo, 3) Données, 4) Réseau sans fil privé, 5) Réseau sans fil publique, 6) Infrastructure, Usage futur.
  - Emplacement de l'entreprise: Montréal
  - Adresse IPv6 assignée: 2001:abcd:db0::/48
  - L'infrastructure réseau de l'entreprise est illustrée ci-dessous



- 2001:abcd:db0::/48

Affectation d'adresse basée sur les fonctions – cas de plusieurs sites

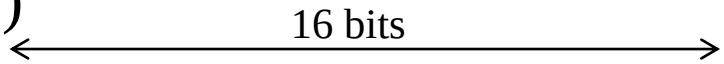
- **Exemple 2**: On suppose que l'entreprise, décrite dans l'exemple 1, possède 3 sites: le siège social à Montréal et 2 succursales une à Québec et une à Sherbrooke. Proposez un plan d'adressage pour cette nouvelle configuration.
  - Fonctions planifiées pour chaque site: 1) VoIP, 2) Surveillance Vidéo, 3) Données, 4) Réseau sans fil privé, 5) Réseau sans fil public, 6) Infrastructure, Usage futur.
  - Adresse IPv6 assignée: 2001:abcd:db0::/44



- 2001:abcd:db0::/44

Affectation d'adresse basée sur l'emplacement de site

- Un site peut être subdivisé en sous-sites. Dans ce cas, il est généralement souhaitable d'affecter une signification liée à l'emplacement au groupe de sous-réseaux (GSR)
- Deux champs sont identifiés: un pour l'emplacement (Z) et l'autre pour la fonction (Y)
- Exemple: 2001:abcd:db12:ZZZZYYYYXXXXXXXX::/52 va me représenter le préfixe alloué à l'emplacement.



le champ ZZZZ représente des bits qui désignent un emplacement et YYYY sont des bits qui désignent une fonction

  - 2^4 emplacements
  - 2^4 fonctions
  - 2^8 sous-réseaux par fonction

Protocole NDP

- Fonctions du protocole NDP (Neighbor Discovery Protocol)
  - Utilise des messages ICMPv6 pour découvrir les adresses IPv6 des voisins connectés aux extrémités des interfaces ou encore leurs adresses MAC (équivalent au protocole ARP)
  - Découverte de routeurs et du préfixe
  - Découverte de MTU et le nombre maximal de sauts
  - Impliqué dans l'autoconfiguration des adresses sans état SLAAC (Stateless Address Autoconfiguration)
  - Détection d'adresses dupliquées

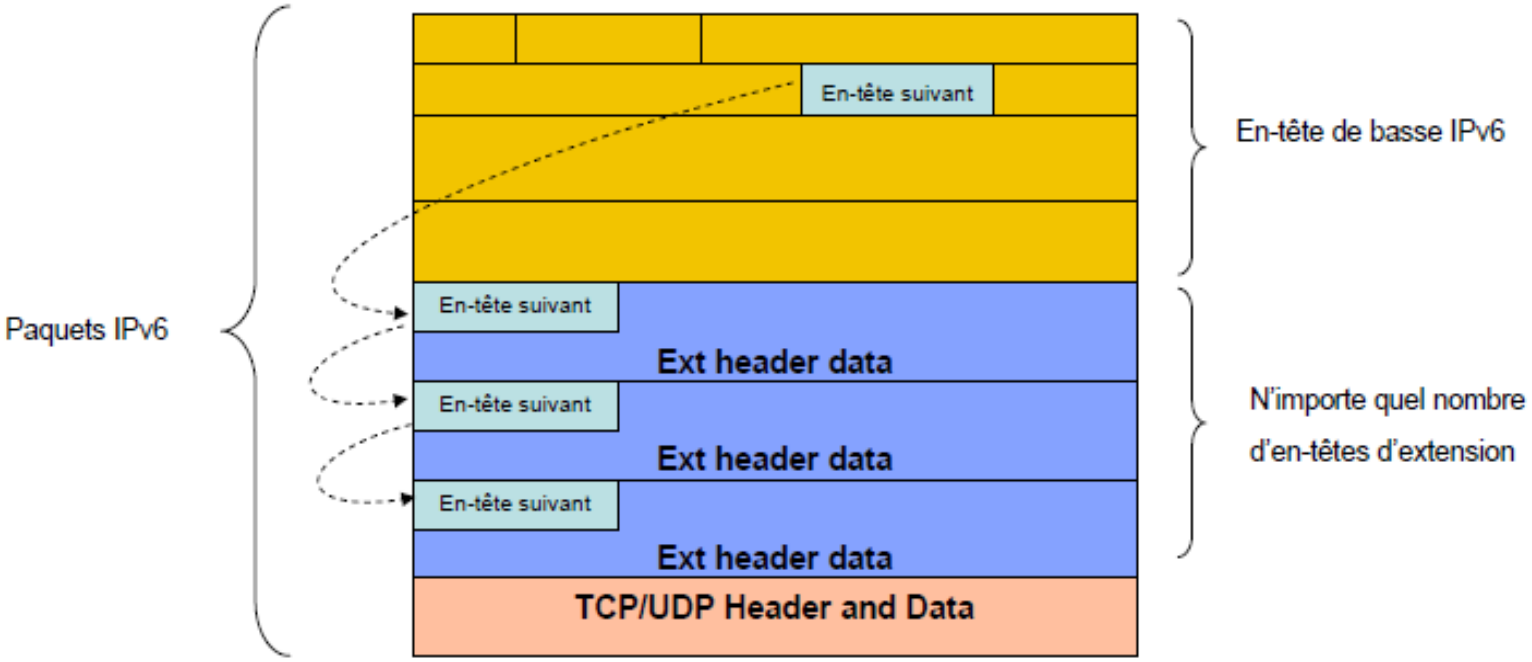
ICMP: Internet Control Message Protocol

Protocole NDP

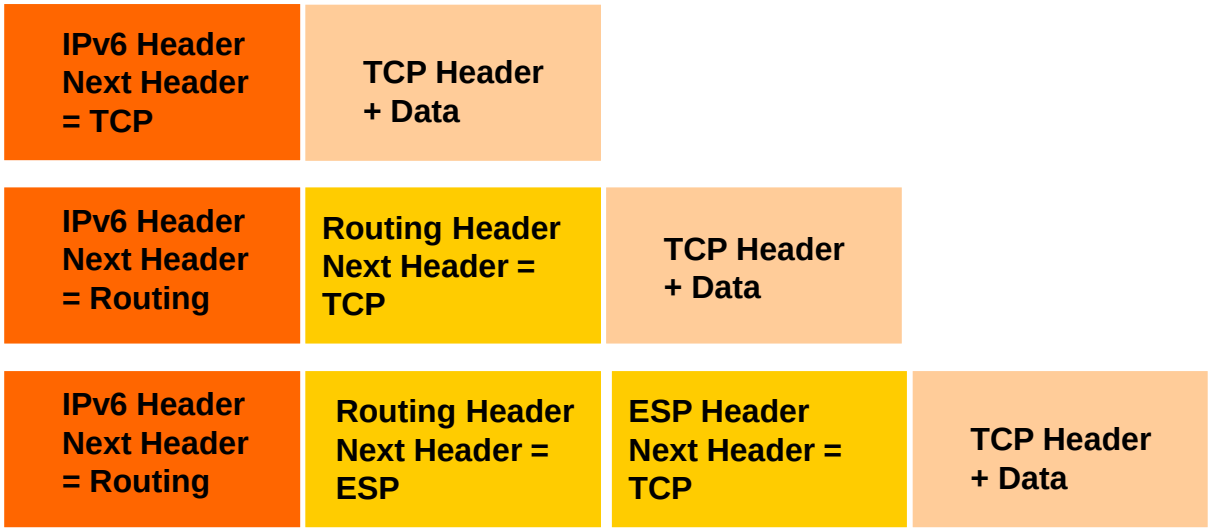
- Les types de messages NDP(Neighbor Discovery Protocol)
  - Message **NA (Neighbor Advertisement)**: Annonce d'un voisin. Messages périodiques de présence envoyés par les nœuds et contenant les adresses couche liaison
  - Message **NS (Neighbor Solicitation):** message envoyé par un nœud pour la découverte d'une adresse couche liaison d'un voisin (résolution d'adresse couche 3 à couche 2)
  - Message **RA (Router Advertisement):** message envoyé par un routeur soit périodiquement soit en réponse à un message RS et destiné à tous les nœuds connectés à lui. Il distribue les paramètres nécessaires à la configuration automatique des adresses IP et au routage (MTU, nombre max de sauts…)
  - Message **RS (Router Solicitation):** message envoyé par un hôte pour demander à tous les routeurs du réseau d'envoyer des annonces RA.
  - Message **DAD (Duplicate Addresss Detection):** message envoyé par un nœud permettant de détecter des adresses dupliquées (cas d'adressage combiné statique et SLAAC)

En-tête d'extension IPv6

- Avec IPv6 les informations optionnelles sont:
  - encodées dans des en-têtes séparés
  - enchainées entre l'en-tête de base de IPv6 et l'en-tête de transport

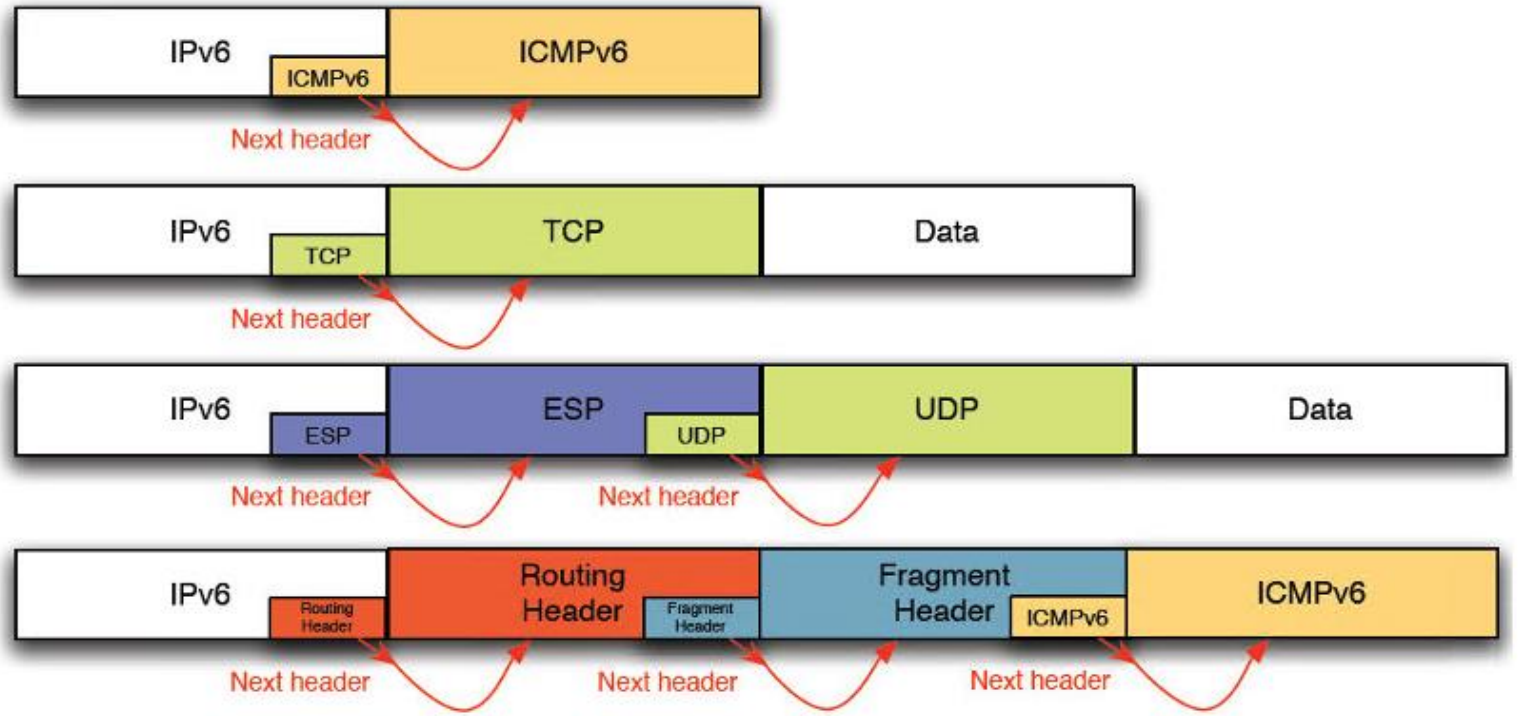


En-tête d'extension IPv6



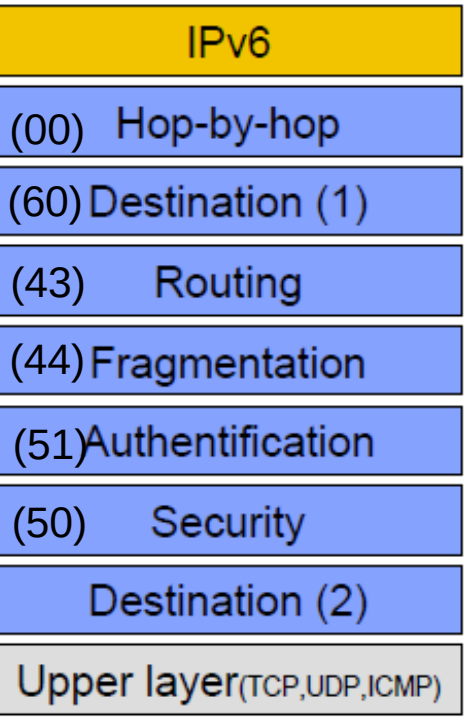
- À part une exception, les en-têtes ne sont traités que par le ou les nœuds (multicast) de destination.
- Le premier en-tête est traité et une information permet de savoir s'il faut traiter l'en-tête suivant. Les en-têtes sont donc traités selon l'ordre de transmission.

ESP: Encapsulating Security Payload


IPv6
ICMPv6
ICMPv6
Next header
IPv6
TCP
TCP
Data
Next header
IPv6
ESP
ESP
UDP
UDP
Data
Next header
Next header
IPv6
Routing Header
Routing Header
Fragment Header
Fragment Header
ICMPv6
ICMPv6
Next header
Next header
Next header

En-tête d'extension IPv6

- Une implantation complète de IPv6 comprend les en-têtes d'extensions suivants dans l'ordre:



Options spéciales exigeant un traitement saut par saut (*Next Header* =00)

Données facultatives devant être vérifiées par le nœud de destination (*Next Header* =60)

Routage étendu imposant à un paquet une route différente (*Next Header* =43)

Fragmentation et réassemblage (*Next Header* =44)

Authentification et intégrité des données (*Next Header* =51)

Chiffrement des données à protéger - Encapsulating Security Payload (*Next Header* =50)

»

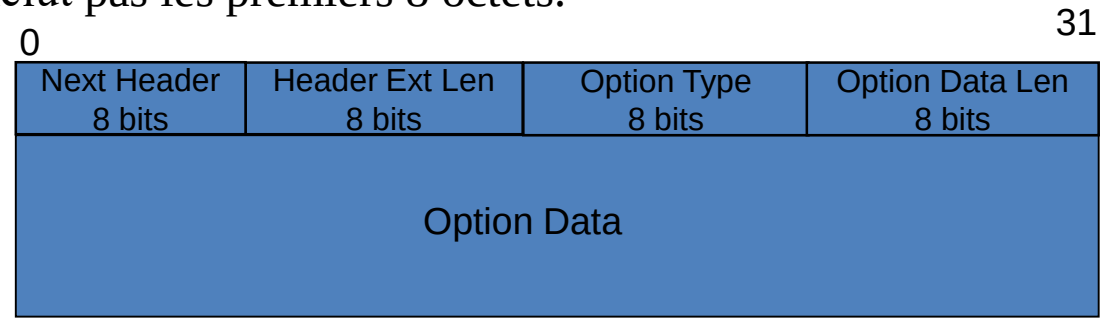
Chaque en-tête d'extension a une longueur multiple de 8 octets

En-tête extension Hop-by-hop et destination

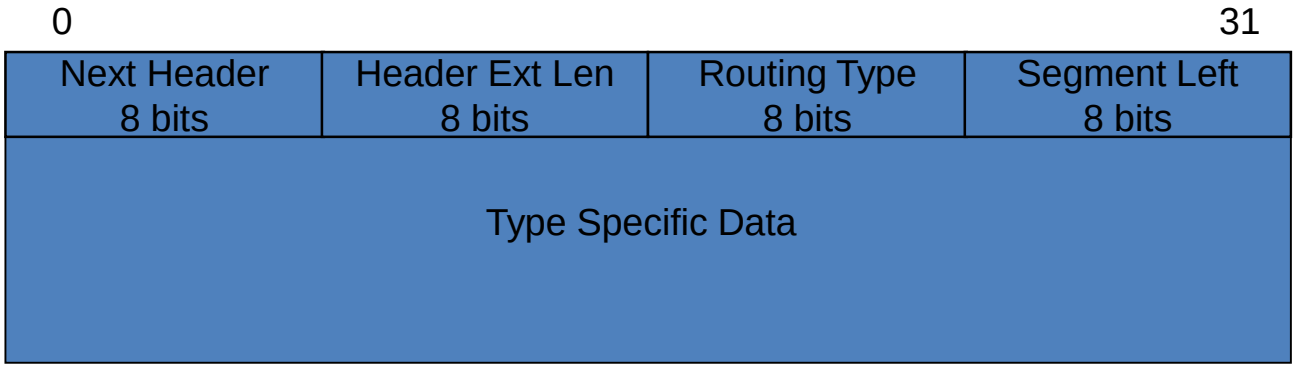
- **En-tête extension <u>Hop-by-Hop</u>**
  - Il s'agit de l'exception à la règle. Cet en-tête est traité par tous les nœuds, incluant la source et la destination
  - Cet en-tête doit suivre immédiatement l'en-tête IPv6. Sa présence est indiquée par la valeur 0 du champ *Next Header* de l'en-tête IPv6
  - Exemple: transport des Jambo-grams (paquet de taille > 2^{16}) et messages d'alerte de routeurs (ex. Multicast Listener Discovery – MLD et RSVP IPv6)
- **En-tête extension <u>destination</u>**
  - Sa présence est indiquée par la valeur 60 du champ *Next Header* de l'en-tête IPv6
  - Exemple: support de la mobilité IPv6.

Next Header: identifie le prochain type d'en-tête qui est inclus dans le paquet IPv6

Header Ext. Len.: Longueur de l'en-tête *Options* en multiple de 8 octets. Cette longueur n'inclut pas les premiers 8 octets.

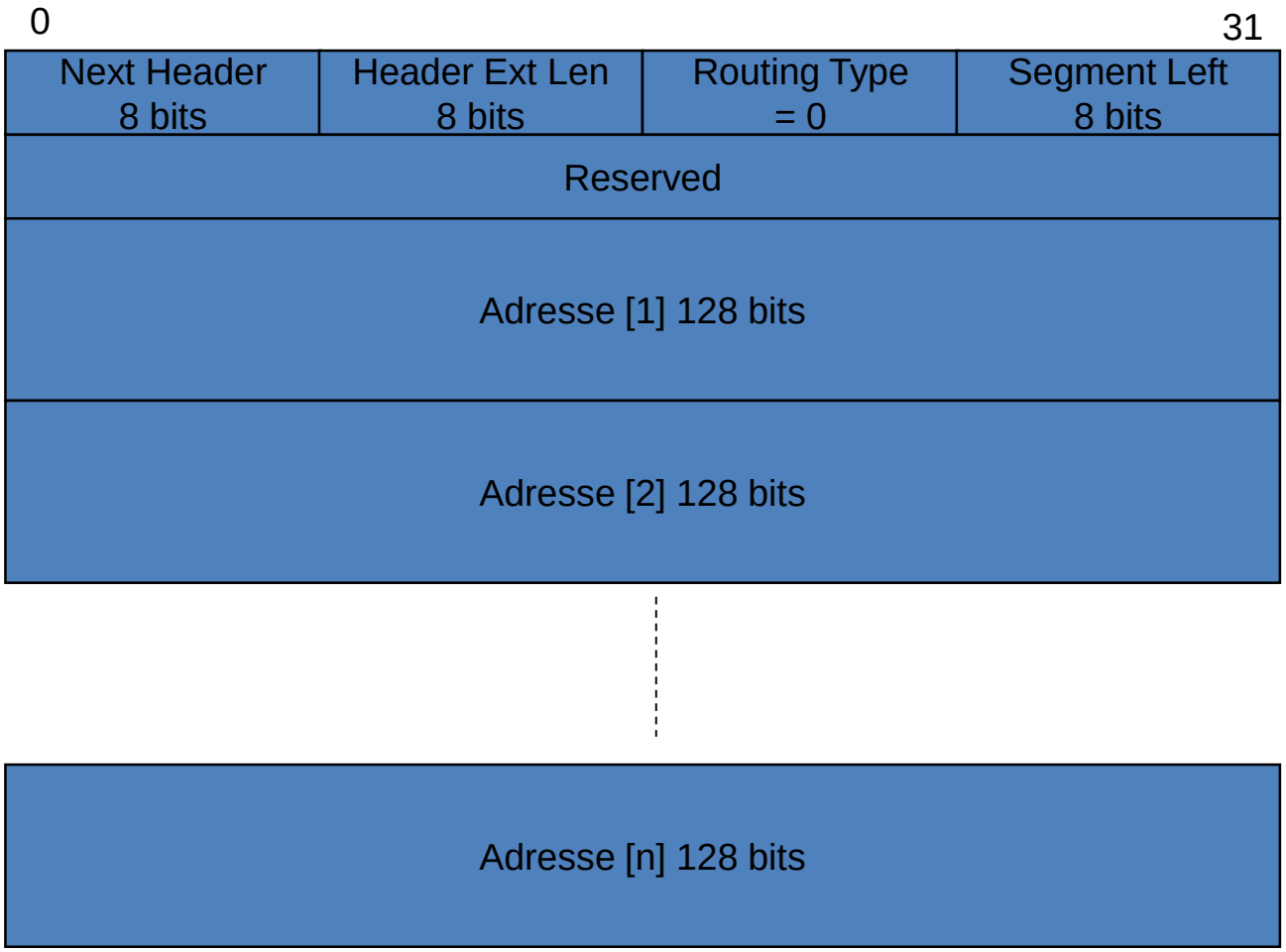


En-tête extension Routing

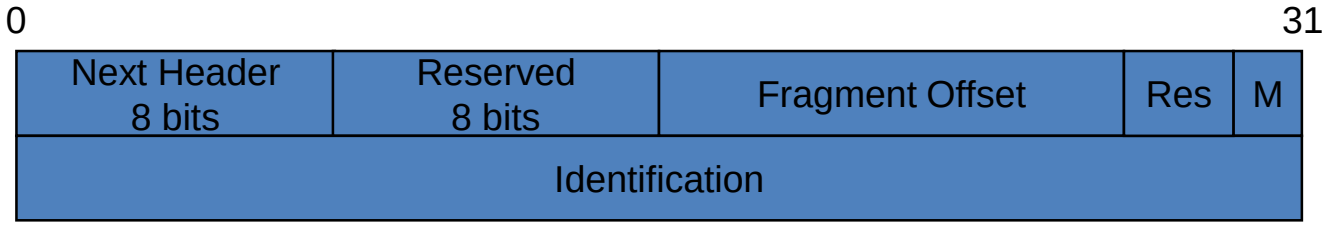


- Identifié par la valeur Next Header = 43 dans l'en-tête précédent.
- Utilisé par la source pour spécifier les nœuds intermédiaires devant être visités sur le chemin vers la destination.
- Pour s'assurer que le paquet passe par les nœuds intermédiaires, l'adresse de destination est modifiée pour le prochain nœud à visiter.
- Routing Type : Identifie une variante particulière de l'en-tête Routing
- Segment Left : Nombre de segments de route restant. Nombre de nœuds intermédiaires à visiter avant d'atteindre la destination finale.
- Type-Specific Data : Format déterminé par le *routing type*. Longueur variable, multiple de 8 octets.

En-tête extension Routing

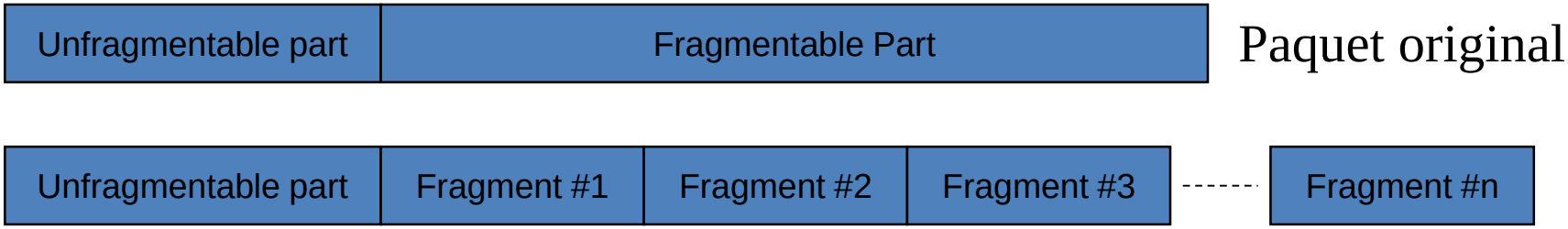


En-tête extension Fragment

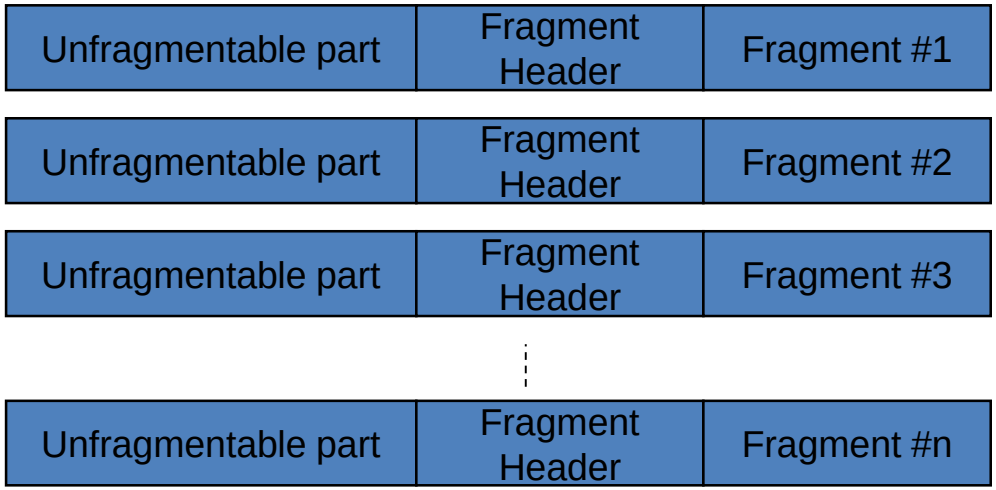


- Identifié par la valeur Next Header = 44 dans l'en-tête précédent.
- Utilisé par la source IPv6 pour transmettre un paquet plus large que le *Path MTU*.
- La fragmentation est réalisée uniquement par la source, pas par les routeurs.
- Fragment Offset (13 bits) : L'offset, en multiple de 8 octets, des données qui suivent cet en-tête, relativement au début de la partie fragmentable du paquet d'origine.
- Res (2 bits) : Reserved
- M (1 bit) : More bit, 1 = More fragment, 0 = Last fragment
- Identification : Tous les fragments d'un même paquet original ont la même valeur d'identification.

En-tête extension Fragment



- La partie non fragmentable contient l'en-tête IPv6 et les en-têtes d'extension traités sur le chemin.



En-têtes extension: Authentification (AH) et Sécurité (ESP)

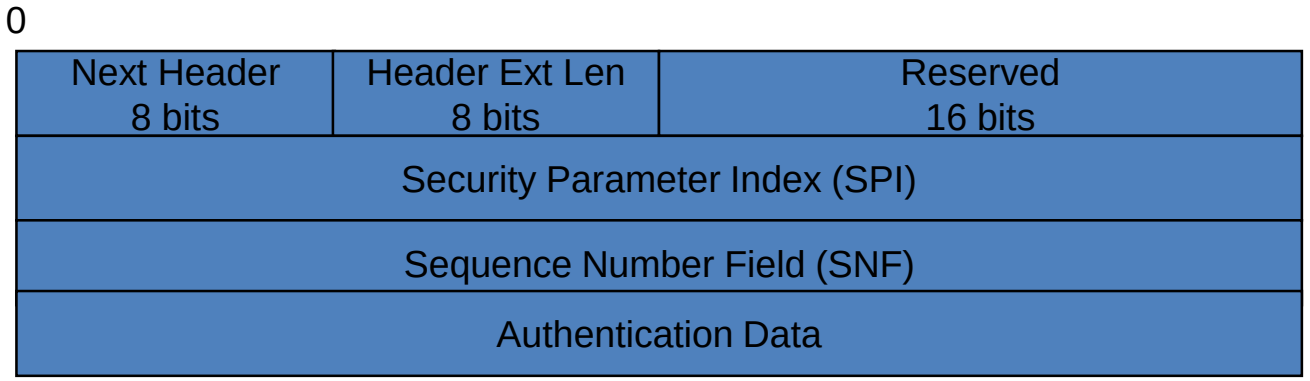
- Pour la protection contre les attaques actives (falsification de données et de transactions) l'authentification de message est utilisée.

L'authentification de message est une procédure permettant à des usagers en communication de vérifier que les messages reçus sont authentiques. Autrement dit:

  - Le message provient d'une source authentique
  - Le message n'a pas été altéré

- Pour la protection contre les attaques passives, le cryptage est utilisé. Il permet de rendre illisible le message pour celui qui ne possède pas la clef.

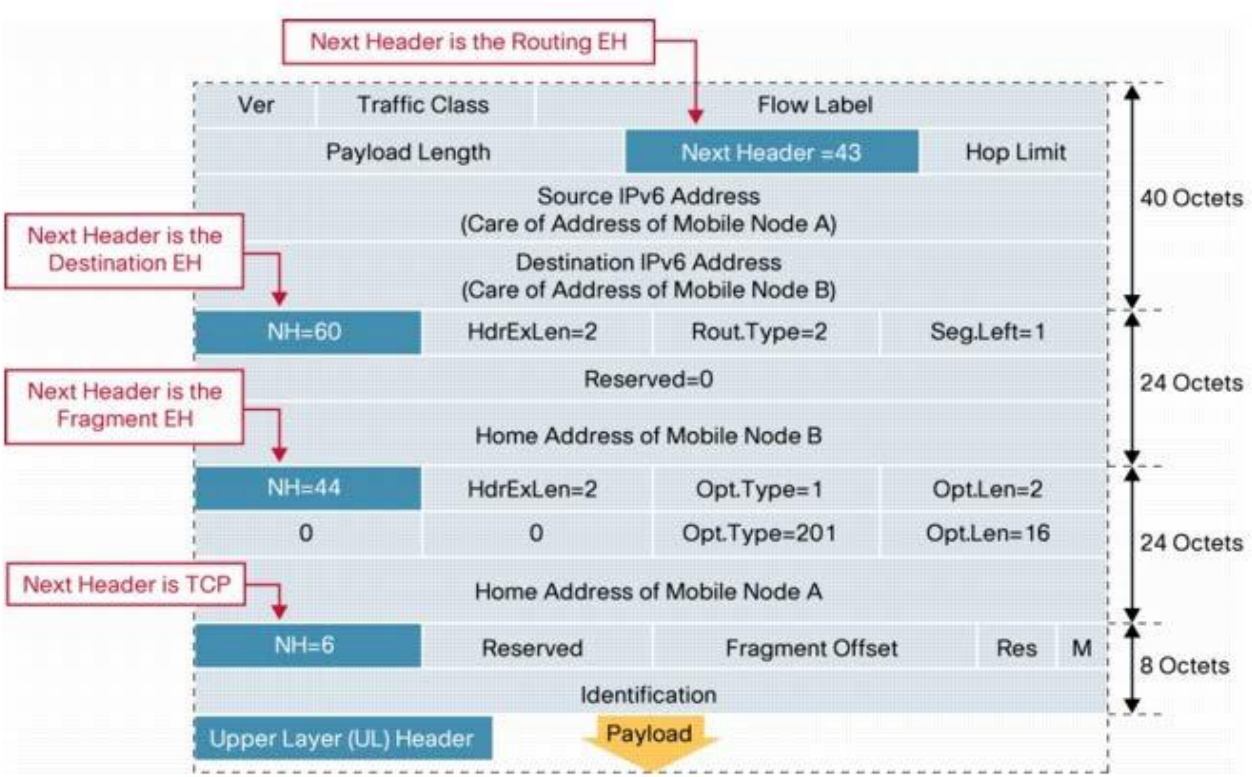
En-tête extension Authentification



- SPI : la combinaison du SPI avec l'adresse de destination forme un identificateur unique pour l'association de sécurité.
  - Entre une même source et une destination, il pourrait exister plus d'un échange authentifié. Chaque échange utilise une clé différente et/ou une façon distincte de calculer l'authentification.
- SNF : Utilisé pour éviter des attaques de type rejouer ou un attaquant tenterait de transmettre un paquet qu'il a capté.
- Authentification Data : Contient la valeur *Integrity Check Value* calculée par la source. La longueur de ce champ dépend de la technique d'authentification utilisée.

En-têtes extensions Exemple

Dans cet exemple (Cisco Systems), le paquet est envoyé du Mobile Node A au Mobile Node B à travers dialogue TCP (6), utilisant l'extension Routing (43) et l'extension Destination Options (60). Il est envoyé à travers un chemin ayant un Maximum Transmission Unit (MTU) plus petit que les liaisons physiques des Mobile Nodes (MNs) et utilise l'extension Fragmentation (44).



IPv4 / IPv6

- **Déploiement**
  - Le déploiement d'IPv6 est encore limité
  - Compliqué en raison de l'incompatibilité des adresses IPv4 et IPv6
  - Progression de IPv6 surtout dans le cœur d'Internet

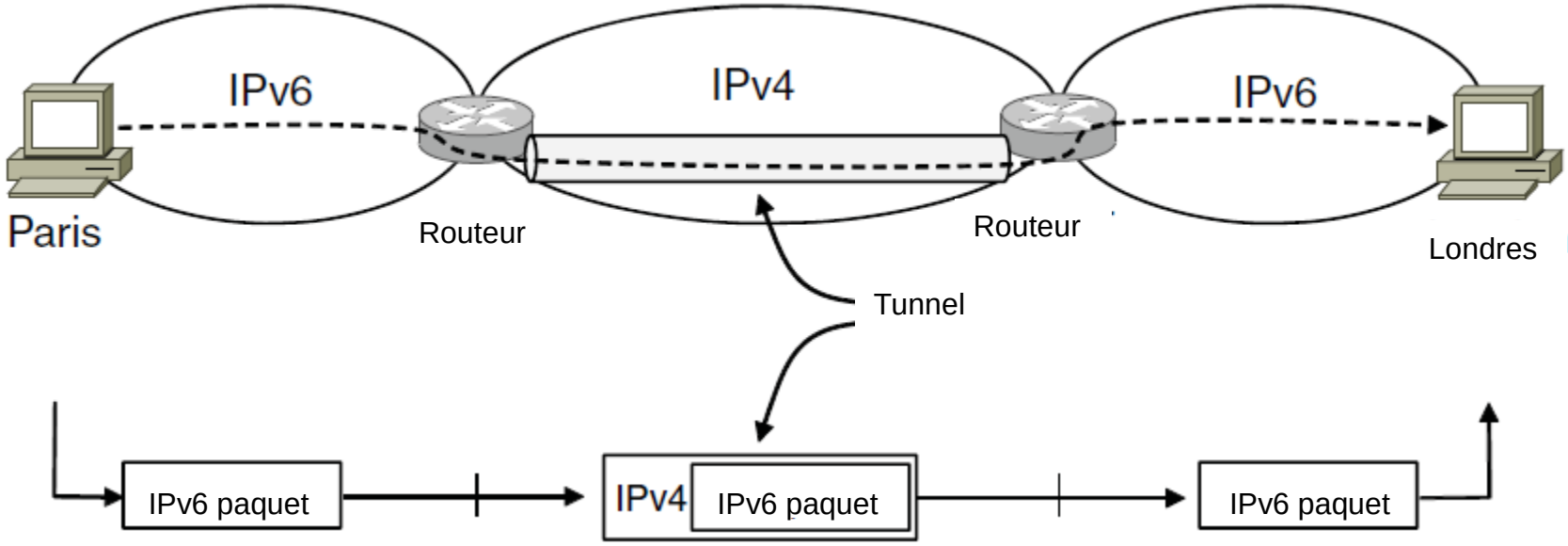
  > Systèmes d'exploitation des hôtes/machines usagers viennent maintenant avec IPv6

https://www.google.com/intl/en/ipv6/statistics.html

IPv4 / IPv6

- **Techniques:**
  - Transport de paquet IPv6 d'une périphérie à une périphérie, en passant par un réseau cœur IPv4
  - Conversion de paquet IPv4 en IPv6 et vice versa à la périphérie

IPv4 / IPv6



- Technique : Envoyer les paquets IPv6 dans des tunnels IPv4
  Paquets IPv6 encapsulés dans des paquets IPv4
  - Requis
    Les 2 bouts du tunnel doivent supporter aussi bien IPv4 que IPv6
  - Applicabilité
    IPv4 au cœur et double pile à la périphérie

IPv4/IPv6

- **Technique: Double pile de protocoles: IPv6 / IPv4**
  - Une interface de programmation d'application (API) qui supporte aussi bien IPv4 que IPv6
  - Requis
    - Mise à jour de toute l'infrastructure
    - Deux types d'adressage
    - Deux types de gestion de réseau
    - Deux types de table de routage
  - Applicabilité
    - Infrastructure spécifique avec un mixage IPv4, IPv6
      - Réseau universitaire
      - Points de présence des fournisseurs d'accès Internet

IPv4/IPv6

- **Technique: Traduction IPv4/IPv6:**
  - Deux possibilités
    - Pas de changement à la couche réseau (IPv4 / IPv6)
      - Mécanisme de relais niveau TCP ou UDP
        - » Serveur dédié avec une double pile (IPv4/IPv6)
        - » Deux connexions au niveau transport: Connexion IPv4 et Connexion IPv6
    - Changements à IPv6 / IPv4
      - Couche logicielle au-dessus de IPv6 ou IPv4 pour interagir avec la couche transport
        - » Mappage d'adresse
        - » Traduction et autres
  - Applicabilité
    - Exemple
      - Continuer à exécuter des applications IPv4 quand tout sera IPv6

Conclusion

- Augmentation de la taille d’adressage
- Plusieurs changements dans l’en-tête IPv6
- Plusieurs simplifications pour un transfert et un traitement rapides
- IPv6 est une évolution du protocole IP