

Protocoles & Standards

IPv6



SI-F
AfNOG 2014, Djibouti

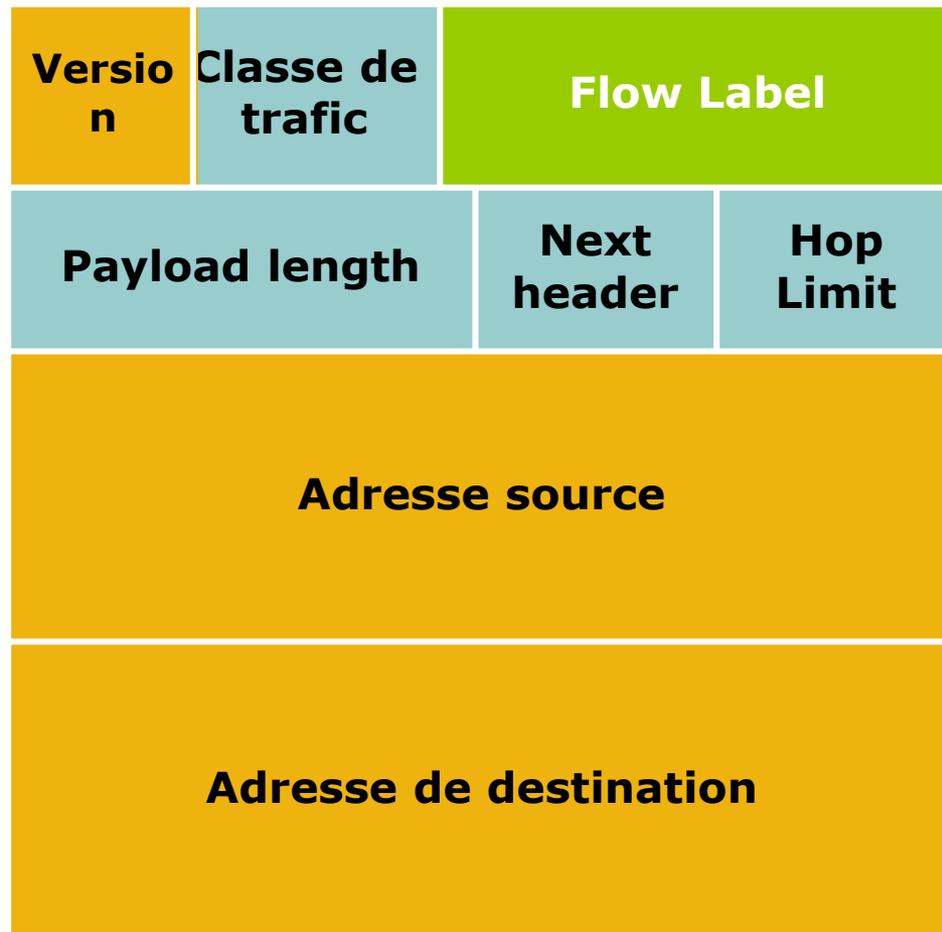
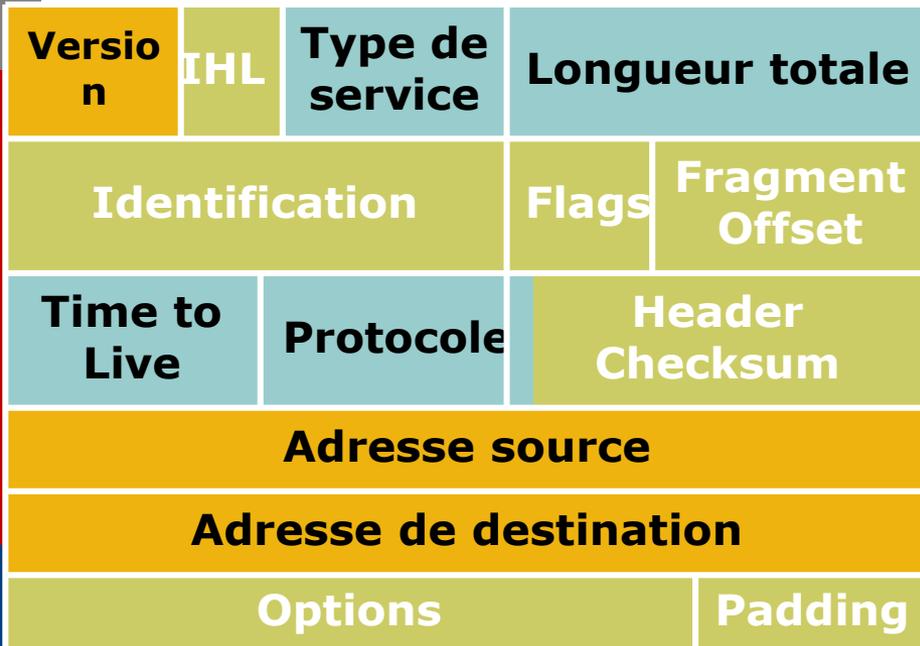
Qu'est ce qui a réellement changé?

- Un espace d'adressage plus large
 - La longueur de l'adresse est quadruplée pour atteindre 16 octets
- Simplification du format de l'entête
 - Longueur fixe, les entêtes facultatives sont chaînées
 - L'entête IPv6 est deux fois longue (40 octets) que celle d'IPv4 sans les options (20 octets)
- Pas de checksum au niveau de la couche réseau IP
- Pas de fragmentation par les routeurs intermédiaires
 - Découverte de chemin MTU
- 64 bits alignés dans le header
- Fonctions d'authentification et de confidentialité
 - Ipsec est obligatoire
- Plus de broadcast

Comparaison des entêtes IPv4 et IPv6

IPv4 Header

IPv6 Header



Légende

- Nom du champ gardé de IPv4 à IPv6
- Les champs non gardés dans IPv6
- Nom et position a changé dans IPv6
- Nouveau champ dans IPv6

Entête IPv6

- Version = valeur à 6 (champ sur 4 bits)
- Traffic Class = champ sur 8 bits
 - Remplace le champ TOS d'IPv4
- Flow Label = champ sur 20 bits
- Payload Length = champ sur 16 bits
 - La taille de la charge utile dans le paquet IPv6 en dehors de l'entête- remplace la longueur totale d'IPv4
- Next Header = champ sur 8 bits
 - Remplace le champ Protocol d'IPv4, et indique le type de l'entête suivante
- Hop Limit = champ sur 8 bits
 - Décrémenté d'un à chaque passage à un noeud IPv6 (équivalent au compteur TTL d'IPv4)
- Source address = champ sur 128 bits
- Destination address = champ sur 128 bits

Simplification du format de l'entête

- Longueur fixe

-
- Entêtes facultives chaînées

- 64 bits alignés

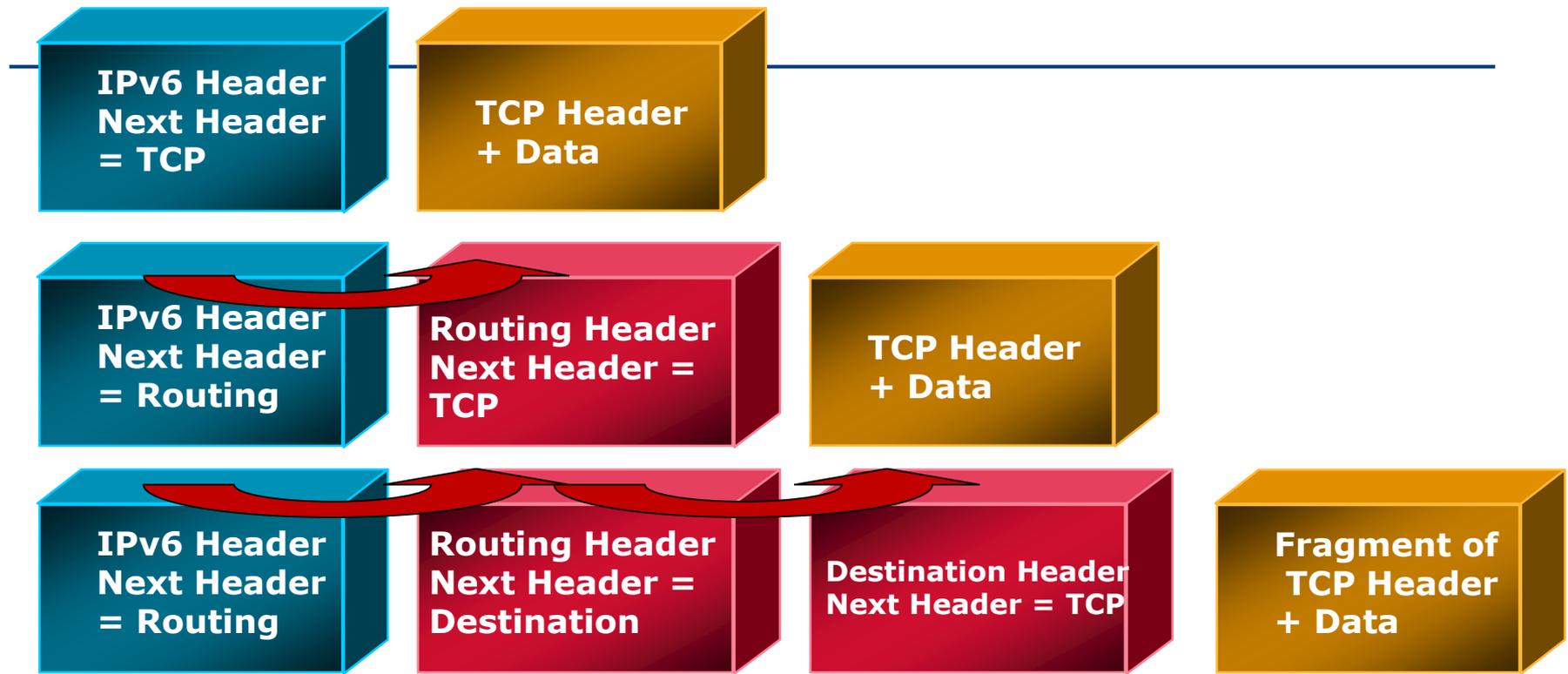
- Entête IPv6 deux fois plus longue (40 octets) que celle d'IPv4 sans les options(20 octets)

- IPv4 contient de base 10 champs dans l'entête (sans les champs d'adresse)

- IPv6 contient de base 6 champs dans l'entête (sans les champs d'adresse)

- Pas de checksum au niveau de la couche réseau IP
- Pas de fragmentation sur les noeuds intermédiaires

Format d'entête– Entête d'Extension



- ❑ Tous les champs facultatifs vont dans des entêtes d'extension
- ❑ Ces entêtes sont chaînées derrière l'entête de base
 - La dernière entête d'"extension" est en général une entete ICMP, TCP ou UDP
- ❑ Cette procédé permet d'ajouter de nouvelles fonctionnalités dans le protocole IPv6 sans changement majeur dans l'ingénierie des équipements

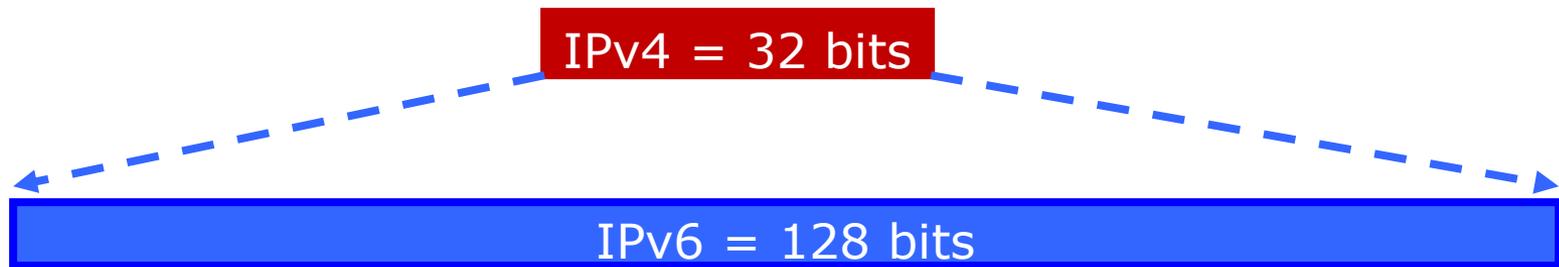
Format de l'entête– Entêtes Courantes

- Valeurs classiques du champ “Next Header”:
 - 0 Hop-by-hop option (extension)
 - 2 ICMP (payload)
 - 6 TCP (payload)
 - 17 UDP (payload)
 - 43 Source routing (extension)
 - 44 Fragmentation (extension)
 - 50 Encrypted security payload (extension, IPSec)
 - 51 Authentication (extension, IPSec)
 - 59 Null (No next header)
 - 60 Destination option (extension)

Format de l'entête – Classement des entêtes

- L'ordre est important parce que:
 - Les entêtes Hop-by-hop doivent être traitées par chaque noeud intermédiaire
 - Les entêtes de Routing doivent être traitées par les routeurs intermediaires
 - A la destination, la fragmentation doit être exécutée avant les autres entêtes
- Ceci permet de simplifier l'implémentation du traitement des entêtes traiter dans le matériel

Large espace d'adresse



- IPv4
 - 32 bits
 - = 4,294,967,296 dispositifs adressables
 - IPv6
 - 128 bits: 4 fois la taille en bits
 - = 3.4×10^{38} dispositifs adressables
 - = 340,282,366,920,938,463,463,374,607,431,768,211,456
 - $\sim 5 \times 10^{28}$ adresses par personne sur la planète

Comment la taille de l'adresse IPv6 a été choisie?

- ❑ Certains ont voulu une longueur d'adresse fixe de 64 bits
 - Idéale pour 10^{12} sites, 10^{15} noeuds, avec une efficacité d'allocation de .0001
 - ❑ (3 ordres de grandeur plus que les exigences d'IPv6)
 - Minimise la croissance de la charge d'entête par paquet
 - Efficace pour le traitement logiciel
- ❑ Certains ont voulu une longueur variable jusqu'à 160 bits
 - Compatible avec le plan d'adressage OSI NSAP
 - Assez suffisant pour l'auto-configuration utilisant les adresses IEEE 802
 - On pourrait commencer avec des adresses plus courtes que 64 bits, et augmenter au fur et à mesure
- ❑ Retenir une longueur fixe avec des adresses 128-bits

Représentation de l'adresse IPv6 (1)

- Champs de 16 bits en caractères hexadécimaux, non sensibles à la casse et séparés par :
 - 2031:0000:130F:0000:0000:09C0:876A:130B
- Les zéros à gauche dans un champs sont facultatifs a :
 - 2031:0:130F:0:0:9C0:876A:130B
- Les zéros successifs dans un champ sont représentés par ::, mais seulement une seule fois dans une adresse :
 - 2031[↑]:0:130F[↑]::9C0:876A:130B ———— est bon
 - 2031::[↑]130F[↑]::9C0:876A:130B **N'est pas** bon

- 0:0:0:0:0:0:0:1 → ::1 (loopback address)
- 0:0:0:0:0:0:0:0 → :: (unspecified address)

Représentation de l'adresse IPv6 (2)

□ Représentation ::

- RFC5952 recommande que la suite de :0: (zéros) la plus à droite soit remplacée :: pour des raisons de consistance
 - 2001:db8:0:2f::5 rather than 2001:db8::2f:0:0:0:5
- Compatible IPv4 (n'est plus utilisé)
 - 0:0:0:0:0:0:192.168.30.1
 - = ::192.168.30.1
 - = ::C0A8:1E01
- Dans un URL, l'adresse est mise entre crochets (RFC3986)
 - [http://\[2001:db8:4f3a::206:ae14\]:8080/index.html](http://[2001:db8:4f3a::206:ae14]:8080/index.html)
 - Complicé pour les utilisateurs, utilisé souvent à des fins de diagnostic
 - On utilise le fully qualified domain names (FQDN)
 - ⇒ The DNS doit fonctionner!!

Représentation de l'adresse IPv6 (3)

- Représentation du préfixe
 - La représentation du préfixe se fait comme la notation CIDR en IPv4
 - Dans cette représentation, on ajoute la longueur du préfixe
 - Exemple dans une adresse IPv4:
 - 198.10.0.0/16
 - Une adresse IPv6 est représentée de la même façon :
 - 2001:db8:12::/40

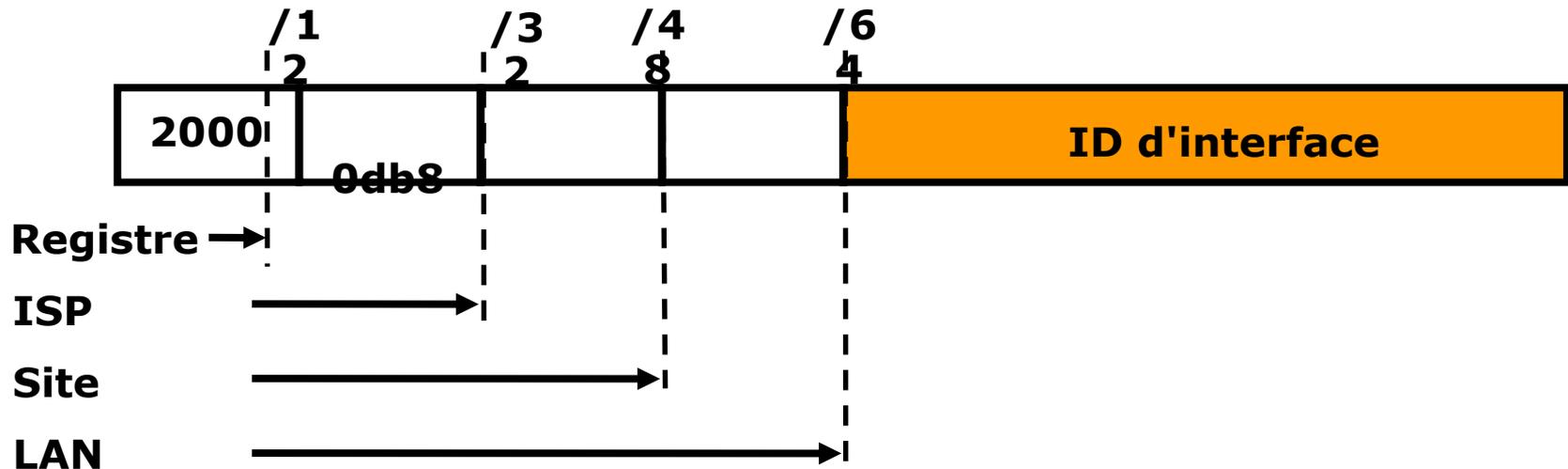
Adressage IPv6

- ❑ ~~Les règles d'adressage IPv6 sont décrites par~~ plusieurs RFC
 - L'architecture est définie dans la RFC 4291
- ❑ Les types d'adresses sont:
 - Unicast : une à une (Globale, Unique Local, Link local)
 - Anycast : Une vers la plus proche (Alloué à partir d'une adresse Unicast)
 - Multicast : Une vers un groupe
- ❑ Plusieurs adresses IPv6 de tout type (unicast, anycast, multicast) peuvent être assignées à une seule interface
 - Plus d'adresse Broadcast → les adresses Multicast sont utilisée

Adressage IPv6

Type	Binaire	Hexadécimale
Indéterminée	000...0	::/128
Loopback	000...1	::1/128
Adresse Unicast Globale	0010	2000::/3
Adresse Unicast Lien Local	1111 1110 10	FE80::/10
Adresse Unicast Unique Locale	1111 1100 1111 1101	FC00::/7
Adresse Multicast	1111 1111	FF00::/8

L'allocation des adresses IPv6



- Le processus d'allocation est le suivant:
 - L'IANA alloue dans le bloc 2000 :: / 3 pour une utilisation initiale des adresses IPv6 unicast
 - Chaque registre obtient un préfixe /12 de l'IANA
 - Le registre attribue un préfixe /32 (ou plus) à un ISP IPv6
 - La stratégie recommandée est que les ISP attribuent un préfixe /48 à chaque client final

Portée de l'adressage IPv6

- 64 bits utilisés pour l'interface ID
 - Possibilité de 2^{64} hôtes sur un réseau LAN
 - En théorie 18,446,744,073,709,551,616 hôtes
 - Arrangement pour accueillir les adresses MAC dans l'adresse IPv6
- 16 bits utilisés pour les end-site
 - Possibilité de 2^{16} réseaux sur chaque site
 - 65536 sous réseaux ce qui équivaut à un /12 en IPv4 (en supposant un /28 ou 16 hôtes par sous-réseau IPv4)

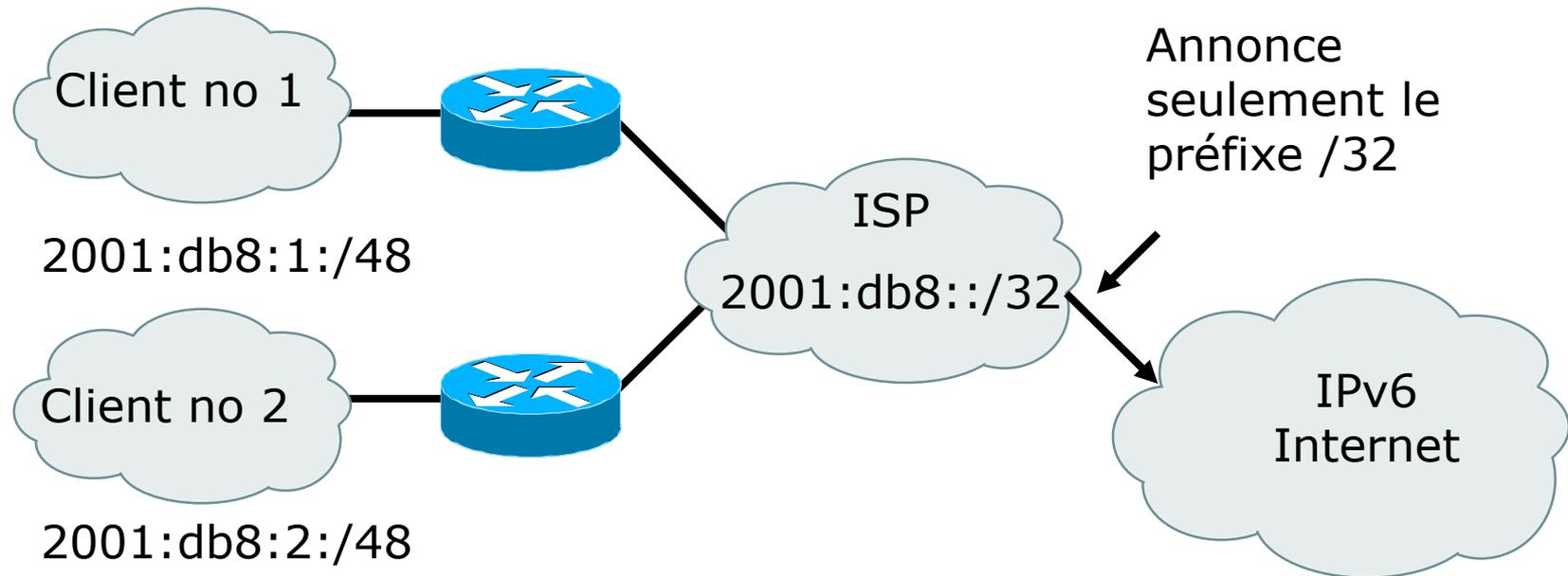
Portée de l'adressage IPv6

- 16 bits réservés pour chaque fournisseur de service
 - Possibilité d'avoir 2^{16} sites finaux par fournisseur de service
 - 65536 clients possibles: ce qui équivaut à octroyer à chaque fournisseur de service un /8 en IPv4 (en supposant un bloc d'adresse de /24 par client)
- 29 bits réservés pour tous les fournisseurs de service
 - Possibilité d'avoir 2^{29} fournisseurs de service
 - i.e. 536,870,912 réseaux de fournisseurs de service
 - Bien que certains fournisseurs de service justifient déjà l'utilisation de plus d'un /32

Comment obtenir une adresse IPv6?

-
- L'espace d'adressage IPv6 est attribué par les 5 RIRs:
 - AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
 - Les ISPs obtiennent leur espace d'adressage des RIRs
 - Les Entreprises obtiennent à leur tour leur espace d'adressage de leurs ISPs
 - Tunnels 6to4 2002::/16
 - Dernier recours seulement et de nos jours c'est jugé inutile
 - (6Bone)
 - Ce fut le réseau expérimental d'IPv6 depuis les années mi-90
 - Maintenant retiré, la fin du service était le 6 Juin 2006 (RFC3701)

Espoirs d'Aggregation



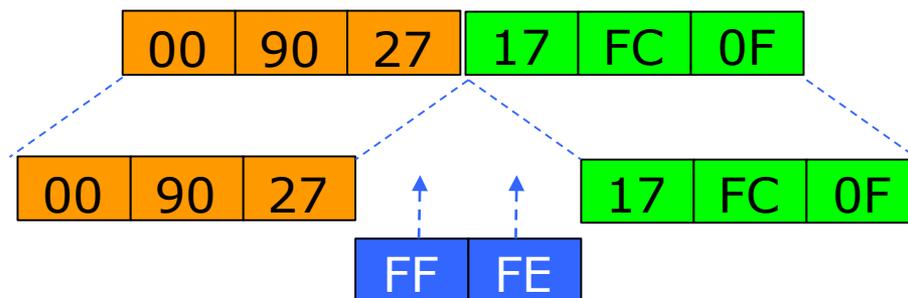
- ❑ Un espace d'adressage plus large permet l'agrégation de préfixes annoncés sur la table de routage globale sur Internet
- ❑ L'idée étant de permettre un routage plus efficace et évolutif
- ❑ **Mais la solution multihoming de l'Internet d'aujourd'hui bloque ce modèle**

IDs d'Interface

- Les 64 bits de poids le plus faible de l'adresse unicast peuvent être assignées de plusieurs façons :
 - Auto-configurés à partir d'une adresse EUI-64, généré à partir de l'adresse MAC de 48 bits (e.i., adresse Ethernet)
 - Auto-génération d'un nombre aléatoire (pour gérer les problèmes de confidentialité)
 - Assignés via un serveur DHCP
 - Manuellement configurés

EUI-64

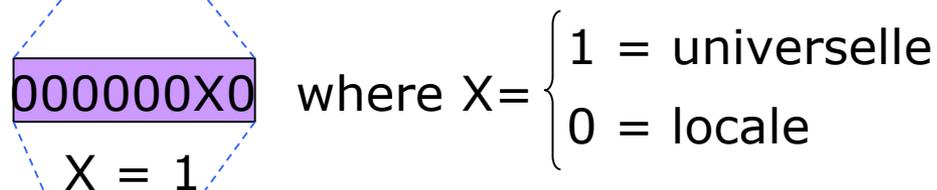
Adresse MAC Ethernet
(48 bits)



Version 64 bits



Portée de l'id EUI-64



Adresse EUI-64



- L'adresse EUI-64 est formée en insérant la séquence FFFE entre l'id de l'équipementier (**company-id**) et l'**extension du fabricant**, et en mettant le bit "u" pour indiquer la portée
 - Portée Globale: pour les adresses MAC de 48 bits IEEE
 - Portée locale: si aucune adresse MAC de 48 bits IEEE n'est disponible (e.i. serials, tunnels)

Exemples d'adresses IPv6

LAN: 2001:db8:213:1::/64

Ethernet0

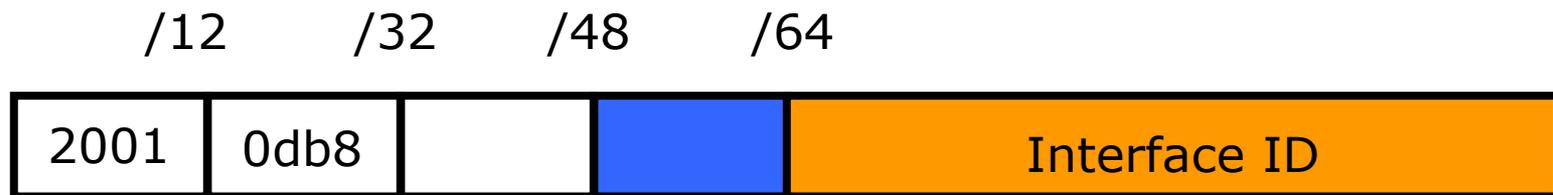


```
interface Ethernet0
  ipv6 address 2001:db8:213:1::/64 eui-64
```

Adresse MAC: 0060.3e47.1530

```
router# show ipv6 interface Ethernet0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
Global unicast address(es):
  2001:db8:213:1:260:3EFF:FE47:1530, subnet is 2001:db8:213:1::/64
Joined group address(es):
  FF02::1:FF47:1530
  FF02::1
  FF02::2
MTU is 1500 bytes
```

Confidentialité dans l'adresse IPv6 (RFC 4941)



- ❑ Adresses temporaires pour les hôtes clients IPv6 d'applications, e.e. le navigateur Web
- ❑ Destiné à inhiber le suivi d'un équipement/utilisateur mais ceci est également un problème potentiel
 - Plus difficile de scanner toutes les adresses IP d'un sous-réseau
 - Mais le scan de ports scan est identique si l'adresse est connue
- ❑ Une interface ID aléatoire de 64 bits, exécuter DAD avant de l'utiliser
- ❑ Le taux de variation dépend de la politique locale
- ❑ Implementé dans Microsoft Windows XP/Vista/7 Apple MacOS 10.7 et ultérieur

Options d'adressage IPv6 chez l'hôte

- Sans état ou Stateless (RFC4862)
 - SLAAC – Stateless Address AutoConfiguration
 - Le noeud au démarrage envoie une requête “router solicitation” pour demander en réponse un “router advertisement” pour obtenir les informations pour configurer son interface
 - Le noeud au démarrage configure sa propre adresse de type lien local
- Stateful
 - DHCPv6 – requis par la plupart des entreprises
 - Manuel – comme dans IPv4 avant DHCP
 - Adéquat pour les serveurs et routeurs d'infrastructure
 - N'est pas adapté pour les utilisateurs finaux

Renumérotation dans IPv6

□ Renumérotation des Hôtes

■ Stateless:

- La renumérotation des hôtes est effectuée en modifiant le RA pour annoncer l'ancien préfixe avec une durée de vie plus courte et le nouveau préfixe

■ Stateful:

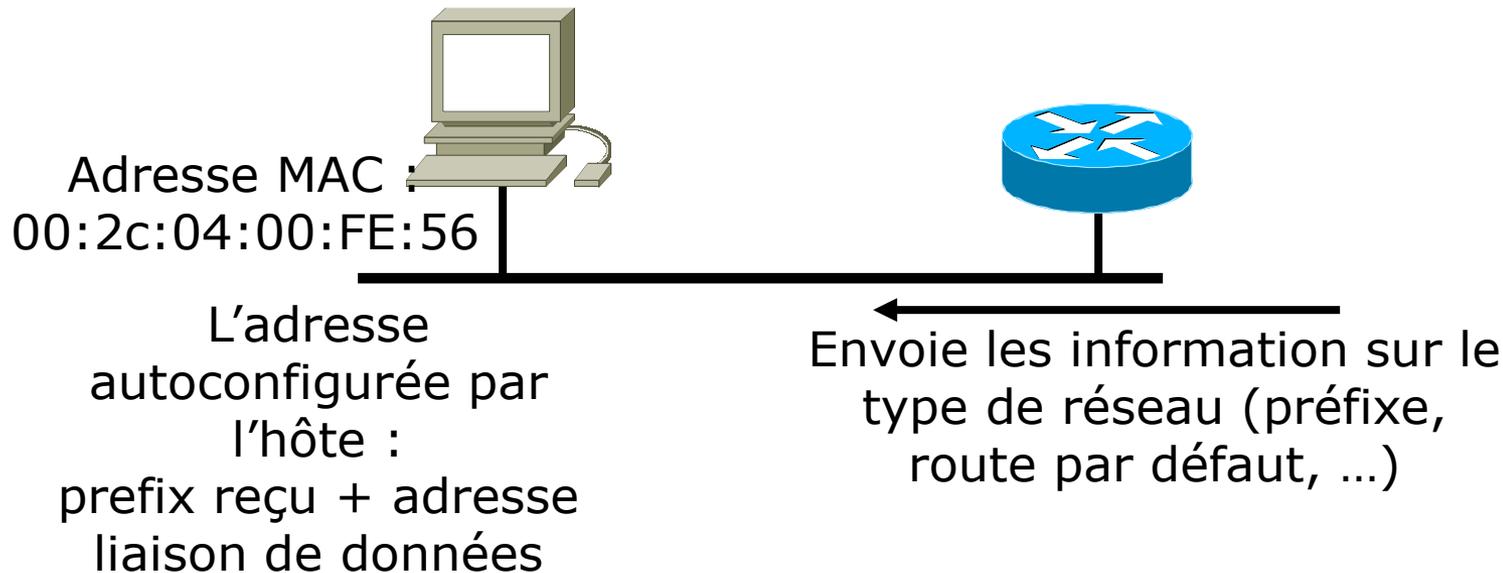
- DHCPv6 utilise le même processus que DHCPv4

□ Renumérotation des Routeurs

- Le protocole de numérotation de routeur a été développé (RFC 2894) pour permettre aux routeurs de domaine interne d'apprendre l'introduction/le retrait de préfixes

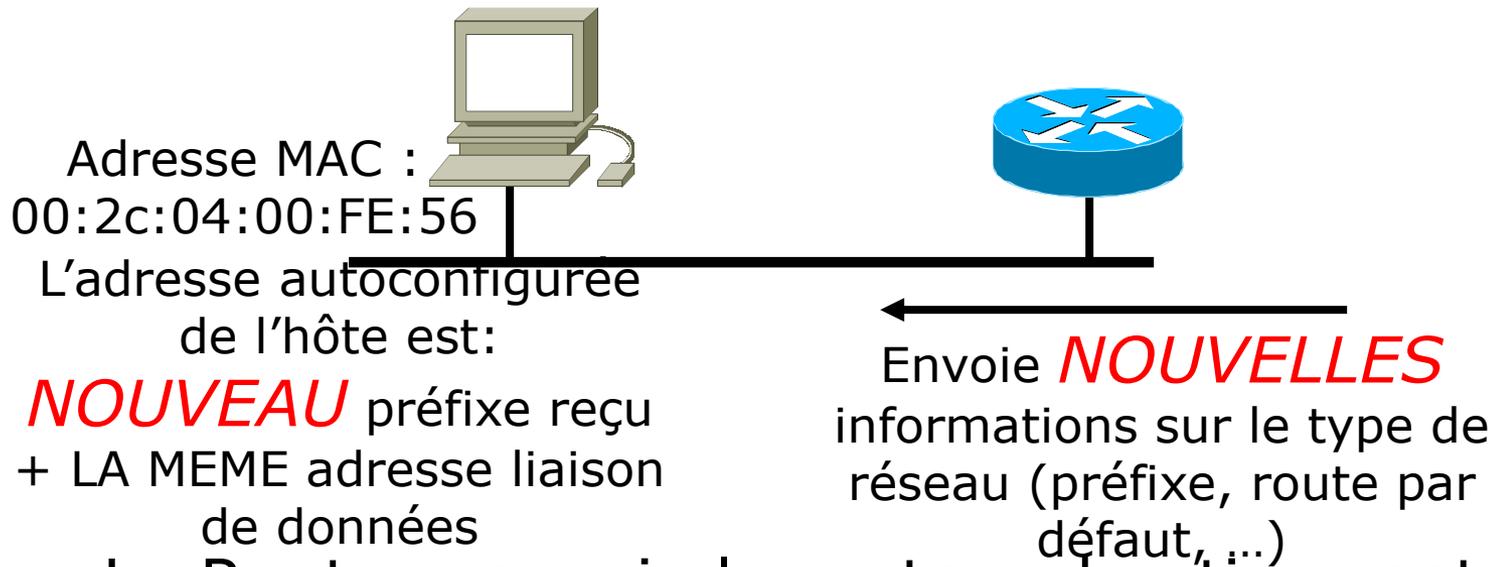
■ **Aucune implémentation connue!**

Auto-configuration



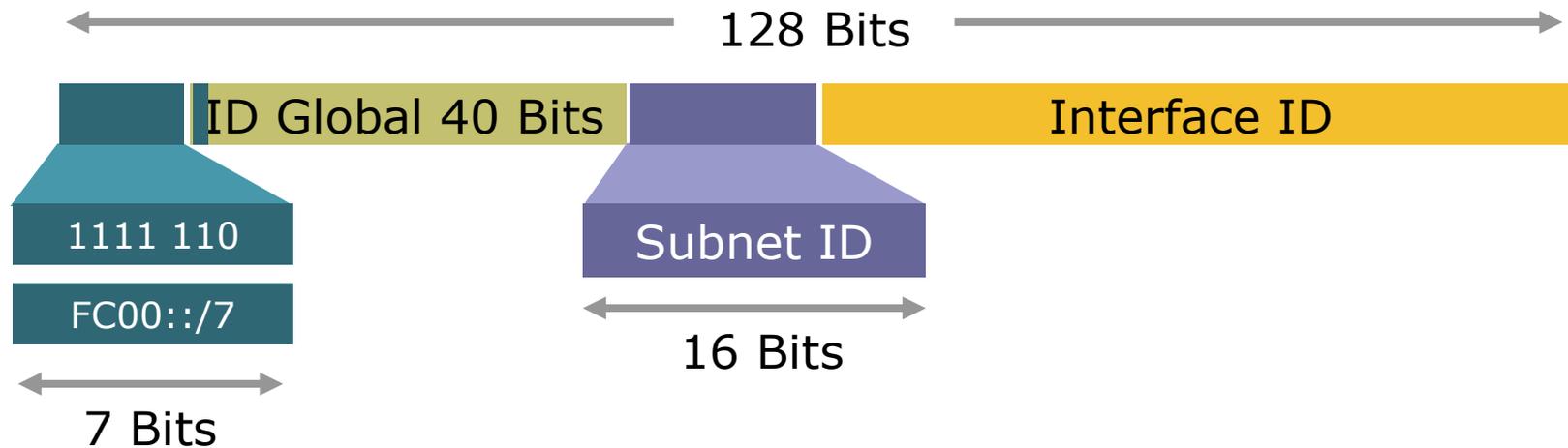
- ❑ Le PC envoie un message router sollicitation (RS)
- ❑ Le Routeur répond par un message router advertisement (RA)
 - Ceci inclut le préfixe et la route par défaut
 - La RFC6106 ajoute l'option serveur DNS
- ❑ Le PC configure son adresse IPv6 en concaténant²⁷ le préfixe reçu avec son adresse EUI-64

Renumerotation



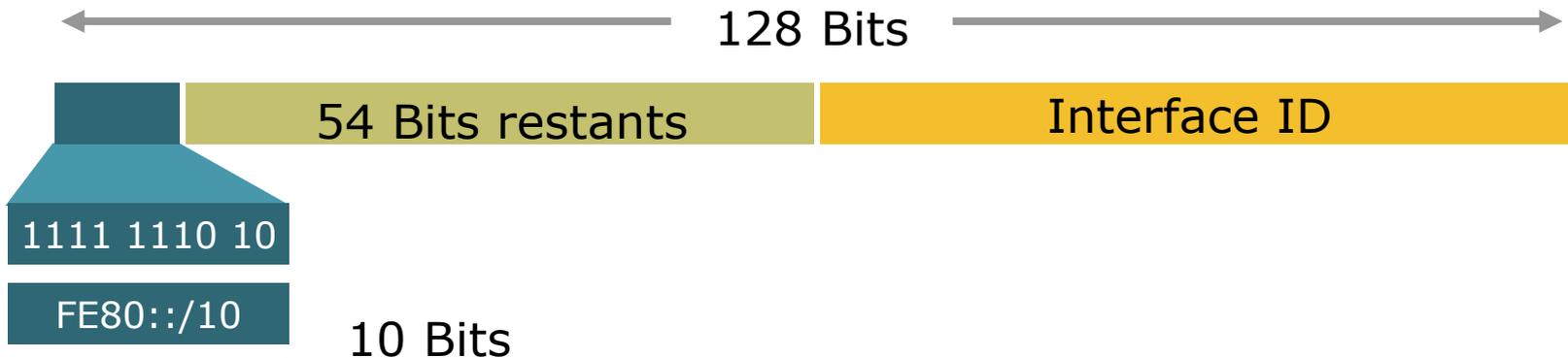
- Le Routeur envoie le router advertisement (RA)
 - Ceci inclut le nouveau préfixe et la route par défaut (et et la durée de vie restante de l'ancienne adresse)
- Le PC configure une nouvelle adresse IPv6 en concaténant le préfixe reçu avec son adresse EUI-64
 - Marque la durée de vie sur l'ancienne adresse

Adresse Unique-Locale



- ❑ Les adresses de type Unique-Local sont utilisées:
 - Communications locales & des VPNs inter-sites
 - Périphériques locaux tels que les imprimantes, téléphones, etc
 - Connectivité des systèmes de gestion réseau
- ❑ Elles ne sont pas routables sur Internet
- ❑ C'est une réinvention de la notion d'adresse site-local devenue obsolète?

Adresse Link-Local



- Les adresses de type Link-Local sont utilisées pour:
 - Communications entre deux périphériques IPv6 (comme ARP mais au niveau de la couche 3)
 - Calcul du Next-Hop dans les protocoles de Routage
- Automatiquement assigné par le routeur dès qu' IPv6 est activé
 - Adresse obligatoire
- A seulement une portée sur le lien Spécifique
- Les 54 bits restants pourraient être des zéros ou toute valeur manuellement configurée

Utilisation Multicast

□ Broadcasts dans IPv4

- Interrrompt tous les périphériques réseaux sur le LAN même si la requête était destinée à un sous-ensemble
- Peut complètement inonder le réseau (“tempête de broadcast”)

□ Broadcasts dans IPv6

- Cette notion n’est plus utilisée et est remplacée par le multicast

□ Multicast

- Permet une utilisation efficace du réseau
- La plage d’adresses Multicast est plus large

Adresse Multicast IPv6

- ▣ Les adresses multicast IPv6 ont comme préfixes FF00::8
- ▣ Le second octet définit la durée de vie et la portée de l'adresse multicast.

8-bits	4-bits	4-bits	112-bits
1111 1111	Lifetime	Scope	Group-ID

Lifetime	
0	Si Permanente
1	Si Temporaire

Scope	
1	Noeud
2	Lien
5	Site
8	Organisation
E	Global

Exemples d'adresses Multicast IPv6

□ RIPng

- L'adresse multicast pour désigner tous les routeurs RIPng (AllRIPRouters) est **FF02::9**
 - Notez que 02 signifie que c'est une adresse permanente et une portée sur le lien

□ OSPFv3

- L'adresse multicast pour désigner tous les routeurs OSPF (AllSPFRouters) est **FF02::5**
- L'adresse multicast pour désigner tous les routeurs désignés (AllDRouters) est **FF02::6**

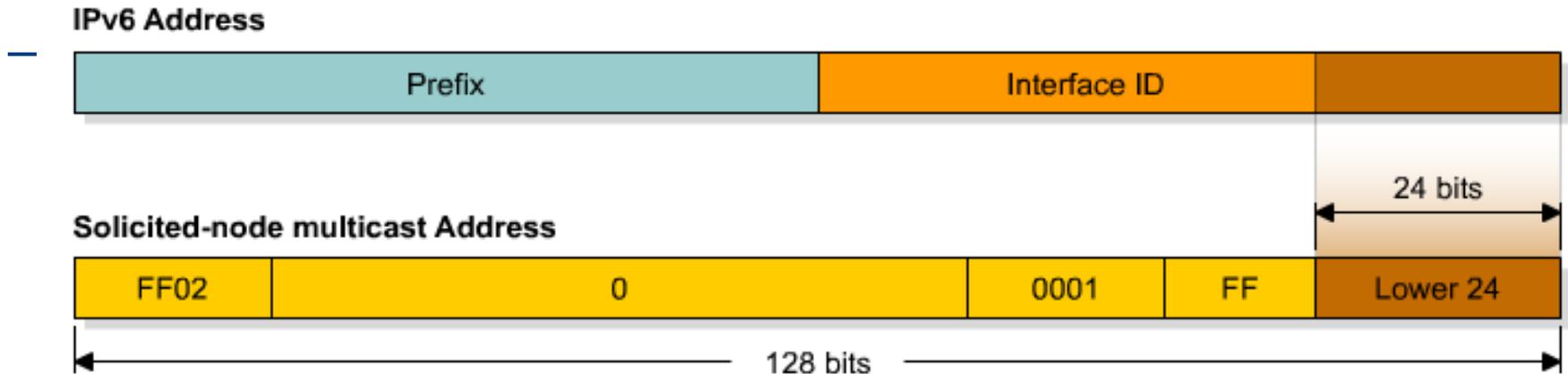
□ EIGRP

- L'adresse multicast pour désigner tous les routeurs EIGRP (AllEIGRPRouters) est **FF02::A**

Adresse Multicast de Noeud-Sollicité

- L'adresse multicast de noeud sollicité est utilisé pour la détection de conflit d'adresse (Duplicate Address Detection)
 - Fait partie du processus de découverte de voisins (Neighbour Discovery)
 - Remplace ARP
 - Des adresses IPv6 en double sur le réseaux ont rares, mais le test doit être effectué
- Pour chaque adresse unicast ou anycast configurée, il y a une adresse multicast de noeud sollicité correspondante
 - Cette n'adresse n'a de portée que sur le lien local

Adresse Multicast de Noeud-Sollicité



- L'adresse multicast de noeud-sollicité est créée avec le préfixe `FF02:0:0:0:0:1:FF::/104` auquel on ajoute les 24 bits de poids le plus faible de l'adresse IPv6 unicast ou anycast

Adresse Multicast de Noeud-Sollicité

```
R1#sh ipv6 int e0
Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::200:CFF:FE3A:8B18
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF3A:8B18
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
R1#
```

Adresse Multicast de Noeud-Sollicité



Adresse Anycast IPv6

- Une adresse anycast IPv6 est un identifiant pour un ensemble d'interfaces (appartenant à plusieurs noeuds différents)
 - Un paquet envoyé à une adresse anycast est délivrée à une des interfaces identifiées par cette adresse (le plus "proche" d'entre elles, selon la distance mesurée du protocole de routage).
 - RFC4291 décrit dans les détails l'Anycast IPv6
- En réalité, il n'y a pas eu d'implémentation connue d'anycast IPv6 Anycast selon la RFC
 - La plupart des opérateurs ont choisi d'utiliser à la place le style anycast d'IPv4

Anycast dans Internet

- Une adresse unicast globale est assignée à tous les noeuds qui doivent répondre à un service donné
 - Cette adresse est routée à partir du bloc d'adresses du parent
- Le noeud qui répond à une requête de service est celui le plus proche du demandeur selon le protocole de routage
 - Chaque noeud anycast est identique aux autres
- Utilisable au sein d'un ASN, ou de façon globale sur
- Des exemples types (IPv4) sont:
 - Serveurs racines DNS et serveurs de noms des ccTLD/gTLD
 - Serveurs de relais SMTP et les résolveurs DNS dans le système autonome d'un ISP

Limites MTU

- Le MTU minimum sur un lien dans IPv6 est 1280 octets

(alors que c'est 68 octets dans IPv4)

⇒ Sur les liens où le MTU < 1280, la fragmentation et le réassemblage spécifique au lien, doivent être utilisés
- Les implementations sont tenues d'accomplir la découverte du chemin MTU pour pouvoir envoyer les paquets supérieurs à 1280 octets
- Avec une implémentation minimale, on peut omettre la découverte PMTU aussi tant que les paquets sont ≤ 1280 octets
- Une option saut à saut supporte la transmission de “jumbograms” avec plus de 2^{32} octets de charge utile

Découverte de Voisins (ND) dans IPv6

- Le protocole définit les mécanismes pour le problèmes suivants:
 - Découverte de router
 - Découverte de préfixe
 - Découverte de Paramètres
 - Autoconfiguration d'adresse
 - Résolution d'adresse
 - Détermination du saut suivant (Next-hop)
 - Détection de l'inaccessibilité du voisin
 - Détection de conflit d'adresses
 - Redirections

Découverte de Voisins (ND) dans IPv6

- Défini dans la RFC 4861
- Protocole basé sur ICMPv6 (RFC 4443)
 - Combinaison des protocoles IPv4 (ARP, ICMP, IGMP,...)
- Entièrement dynamique, interactif entre hôtes et routeurs
- Définit 5 types de paquets ICMPv6 :
 - Sollicitation de Routeur (Router Solicitation)
 - Annonce de Routeur (Router Advertisement)
 - Sollicitation de voisin (Neighbour Solicitation)
 - Annonce de voisin (Neighbour Advertisement)
 - Redirection (Redirect)

IPv6 et DNS

- Nom d'hôte en adresse IP:

IPv4	www.abc.test.	A	192.168.30.1
------	---------------	---	--------------

IPv6	www.abc.test	AAAA	2001:db8:c18:1::2
------	--------------	------	-------------------

Tehnologie IPv6

<i>Service IP</i>	<i>Solution IPv4</i>	<i>Solution IPv6</i>
Plage d'adressage	32-bit, Network Address Translation	128-bit, portée multiples
Autoconfiguration	DHCP	Serverless, Reconfiguration, DHCP
Securité	IPSec	IPSec obligatoire, fonctionne en mode End-to-End
Mobilité	IP Mobile	IP Mobile avec routage direct
Qualité de service	Differentiated Service, Integrated Service	Differentiated Service, Integrated Service
Multicast IP	IGMP/PIM/Multicast BGP	MLD/PIM/Multicast BGP, identificateur de la portée

Que fait IPv6 pour:

□ La Sécurité

- Rien de plus qu'IPv4– IPSec est utilisé dans les deux
- Mais IPv6 rend obligatoire IPSec

□ La QoS

- Rien de plus qu'IPv4–
 - Differentiated et Integrated Services sont utilisés dans les deux
 - Jusqu'à présent, le champ "Flow label" n'a pas connu une utilisation réelle.

Sécurité IPv6

- ❑ Les standards IPsec standards s'appliquent aussi bien dans IPv4 que dans IPv6
- ❑ Toutes les implémentations doivent supporter to l'authenfication et le chiffrement des entêtes ("IPsec")
- ❑ L'authentification étant séparée du chiffrement dans les cas où le chiffrement est interdit ou couterait trop cher
- ❑ Les protocoles de distribution de clés ne sont pas encore définis (indépendent d'IP v4/v6)
- ❑ Support de la configuration des clés manuellement requis

Rappel sur la Qualité de Service sur IP

- Deux approches basiques ont été développées par IETF:
 - “Integrated Service” (int-serv)
 - Fine-grain (par flux), les promesses quantitatives (par exemple, les x bits par seconde), utilise la signalisation RSVP
 - “Differentiated Service” (diff-serv)
 - Gros grain (par classe), les promesses qualitatifs (par exemple, la priorité), aucune signalisation explicite
 - diff-serv Signalé (RFC 2998)
 - Utilise RSVP pour la signalisation avec des marques qualitatives globales à gros grains
 - Permet le contrôle de la politique sans exiger des frais généraux de l'État de charge par-routeur

Support Int-Serv dans IPv6

- Champ Flow Label sur 20-bits pour identifier des flux spécifiques ç des besoins spécifiques de QoS
 - Chaque source choisit ses propres valeurs Flow Label; les routers utilisent Source Addr + Flow Label pour identifier des flux distincts
 - La valeur 0 est affectée au Flow Label si aucune QoS n'est demandée (très souvent le cas de nos jours)
- Originellement standardisé dans la RFC 3697

Flow label IPv6

- Le champ Flow label n'a jamais été utilisé depuis qu'IPv6 est standardisé
 - Les suggestions sur son utilisation ces dernières furent incompatibles avec la spécification originelle(discussed in RFC6436)
- Spécification mise à jour dans la RFC6437
 - RFC6438 décrit l'utilisation du Flow Label des chemins multiples d'égal coût et l'aggregation de liens dans les Tunnels

Support Int-Serv dans IPv6

- Le champ Traffic Class sur 8-bits permet d'identifier des classes de paquets spécifiques à des besoins de QoS
 - Pareil à la nouvelle définition de l' octet Type-of-Service d' IPv4
 - Peut être initialisé par la source ou par le routeur intermédiaire; peut être réécrit par les routeurs intermédiaires
 - La valeur du champ Traffic Class est à 0 si aucune QoS n'est demandée (très souvent le cas de nos jours)

Standards IPv6

- Les spécifications de base IPv6 sont des standards de drafts IETF

 - bien testées & stables
 - Specifications de base IPv6, ICMPv6, Neighbor Discovery, PMTU Discovery,...
- D'autres spécifications importantes sont loin derrière pour être des normes, mais sont en bonne voie
 - IPv6 Mobile, compression de l'entête,...
 - Pour voir le statut actuel: www.ipv6tf.org
- Les standards 3GPP UMTS Rev. 5 sur les réseaux cellulaires sans fil(2002) rendent IPv6 obligatoire; également envisagée par⁵¹
3GPP?

Statut IPv6 – Standardisation

- ▣ Plusieurs éléments clés en cours d'études dans la liste les standards ...
-

Specification (RFC2460)

ICMPv6 (RFC4443)

RIP (RFC2080)

IGMPv6 (RFC2710)

Router Alert (RFC2711)

Autoconfiguration (RFC4862)

DHCPv6 (RFC3315 & 4361)

IPv6 Mobility (RFC3775)

GRE Tunnelling (RFC2473)

DAD for IPv6 (RFC4429)

ISIS for IPv6 (RFC5308)

Neighbour Discovery (RFC4861)

IPv6 Addresses (RFC4291 & 3587)

BGP (RFC2545)

OSPF (RFC5340)

Jumbograms (RFC2675)

Radius (RFC3162)

Flow Label (RFC6436/7/8)

Mobile IPv6 MIB (RFC4295)

Unique Local IPv6 Addresses (RFC4193)

Teredo (RFC4380)

VRRP (RFC5798)

- ▣ IPv6 disponible pour:

PPP (RFC5072)

FDDI (RFC2467)

NBMA (RFC2491)

Frame Relay (RFC2590)

IEEE1394 (RFC3146)

Facebook (RFC5514)

Ethernet (RFC2464)

Token Ring (RFC2470)

ATM (RFC2492)

ARCnet (RFC2497)

FibreChannel (RFC4338)

Sujets d'actualités Récents sur IPv6

- Débat sur l'épuisement des adresses IPv4
 - Pool d'adresses IANA IPv4 épuisé depuis le 3 Février 2011
 - <http://www.potaroo.net/tools/ipv4/>
- “Assistance” dans la transition IPv6
 - CGN, 6rd, NAT64, IVI, DS-Lite, 6to4, A+P...
- IPv6 Mobile
- Multihoming
 - SHIM6 “dead”, Multihoming dans IPv6 identique à celui d'IPv4
- Sécurité IPv6
 - L'industrie et les experts de la sécurité examinent de plus près la sécurité IPv6

Conclusion

- ❑ Le Protocole est “prêt”
- ❑ Les composants de base ont déjà connu plusieurs années d’expérience de terrain

The IPv6 Protocol & IPv6 Standards



SI-F

AfNOG 2014