


EL-3017 Réseaux avancés

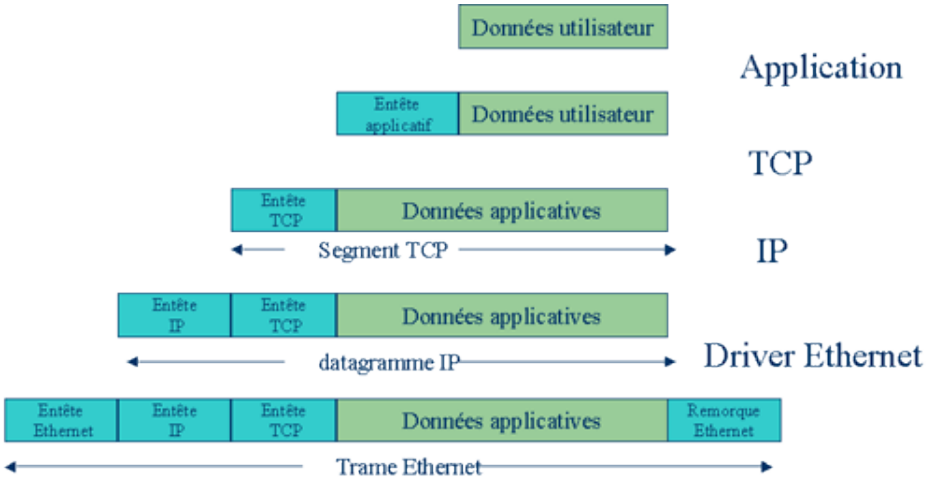
Internet Protocol v6 (IPv6)

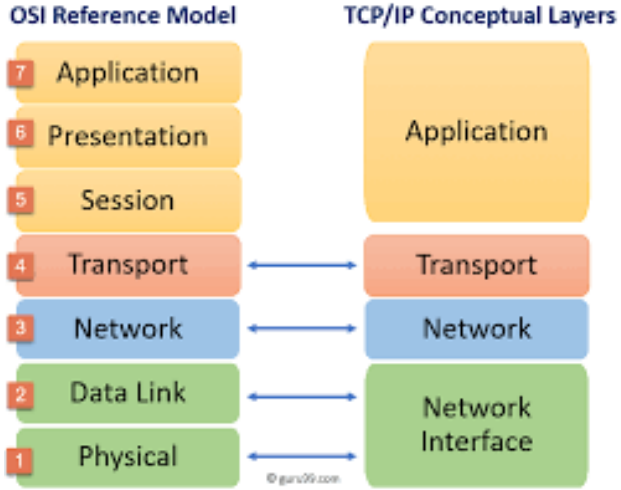
Sofiane Imadali, PhD sofiane.imadali@orange.com


Sommaire

- **Définitions et terminologie**
- **Adressage**
  - Format et scope (portée) d'une adresse
  - Configuration
  - Unicast, Multicast, Anycast
- **ICMPv6 et DHCPv6**
  - **Neighbor discovery**
- **Sécurité**
- **Transition et cohabitation de l'IPv6 et IPv4**

Quelques fondamentaux





Définitions et terminologie

- 1981 : RFC IPv4
- Au début gaspillage important d'adresse : par exemple assignation d'une classe A à une entreprise
- 1993 : épuisement des classes B
- Prévision de saturation pour 1994 !
- Mesures d'économie avec le CIDR
- Naissance de IPv6 en 1996

Définitions et terminologie

- Début des années 1990: CIDR (Classless Internet Domain Routing)
  - Réseau = préfixe/longueur
  - Moins de gâchis d'adresses
  - Permet l'agrégation d'adresses dans les tables de routages: moins de routes

    Exemple: 192.0.1/24 et 192.0.0/24 peut devenir 192.0.0/23
  - Allouer dans les anciennes classes A & B
- NAT et adressage privé
- Cela a permis de gagner du temps pour définir et déployer une nouvelle version de IP (version 6)

Définitions et terminologie

- 1996: Premiers routeurs traitant IPv6 dans Internet (6Bone) et en France dans Renater (G6Bone)
- 2004: Premiers serveurs DNS racine accessible en IPv6. Puis très rapidement serveur des domaines .jp, .kr et .fr
- 2007: Free offre IPv6 natif à ses abonnés
- 2008 : Google accessible en IPv6
- 2010 : Facebook et Youtube accessible en IPv6
- 2011 : épuisement des adresses IPV4 en Asie : fin 2011 , en Europe fin 2012

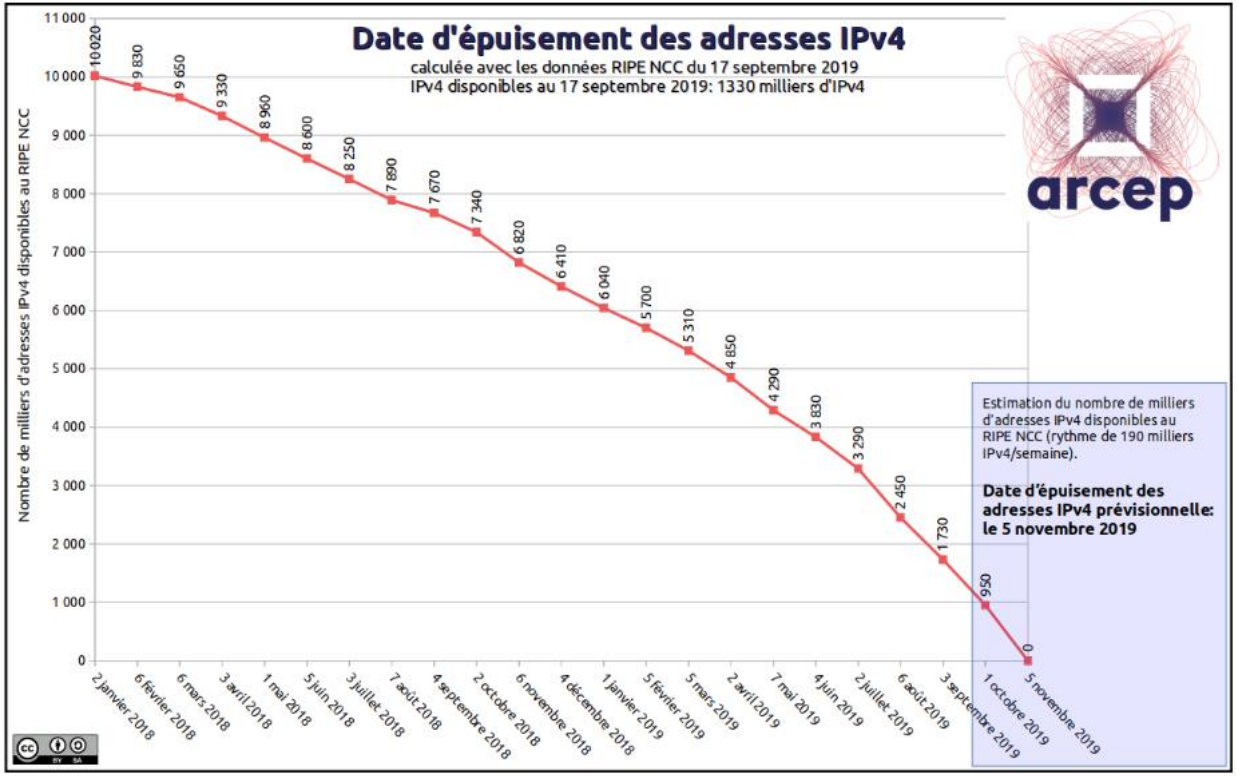
Accès à Google en IPV6 :

- Début 2012 : 0,5 %
- 2015: 5%

Définitions et terminologie

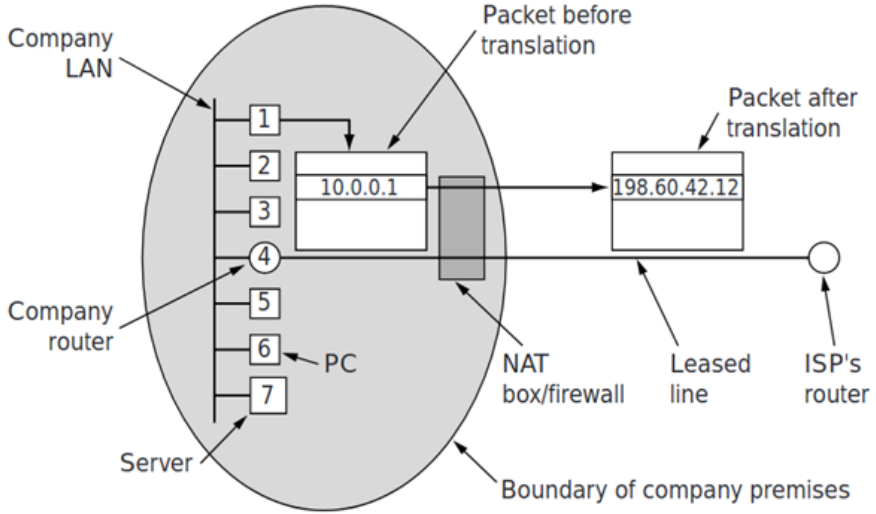
- Adresse sur 16 octets (128 bits)
  - 6,67. 10^17 adresses au millimètre carré de la surface terrestre en théorie
  - En pratique plus de 1500 au m2
- Simplification de l'entête
- Assignation de la partie machine automatique
- Changement de protocole de découverte d'adresse de niveau liaison de donnée (ARP)

Épuisement global et continue des adresses Ipv4



NAT à la rescousse

Problème du nombre limité d'adresses
=> adresse privée + NAT (Network Adresse Translation)



NAT à la rescousse

- Casse la structure pair-à-pair d'Internet très problématique pour certaines applications(VoIP, ...)
- Donne une fausse impression de sécurité :Certaines attaques sont possibles même dans cette configuration
- Semble être une des (mauvaises) raisons du ralentissement de passage à IPv6
- Carrier-grade NAT (CGN) : l'internet mobile est principalement proposé par les opérateurs sous ce mode dégradé.

Questions de compréhension

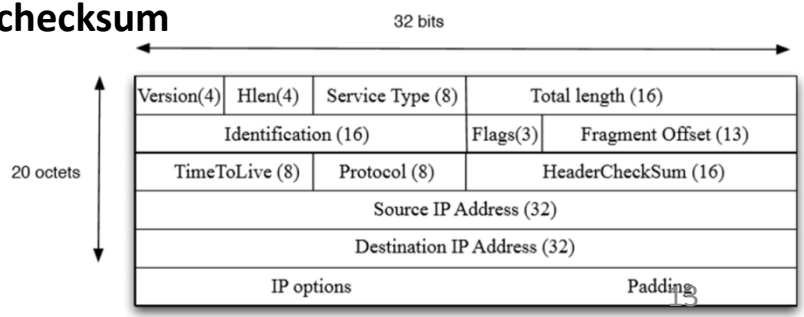
- Quel organisme de normalisation définit le protocole IPv6 ?
- Quelles mesures ont permis de ralentir l'épuisement des adresses IPv6 ?

Sommaire

- Définitions et terminologie
- **Adressage**
  - Format et scope (portée) d'une adresse
  - Configuration
  - Unicast, Multicast, Anycast
- **ICMPv6 et DHCPv6**
  - **Neighbor discovery**
- **Sécurité**
- **Transition et cohabitation de l'IPv6 et IPv4**

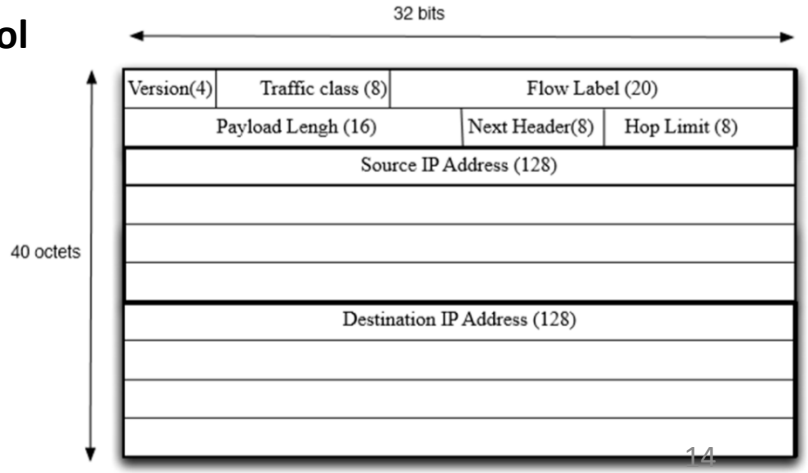
Format des paquets

- **Version : 4 , Hlen : longueur de l'entête (options possibles)**
- **Service type : 6 bits, différentier des classes de service et donner des priorités de traitement**
- **Total Length : nombre d'octets de données plus entête IPV4**
- **Identification: identifie un paquet IP (identique pour tous les fragments éventuels)**
- **Flags : Deux bits nécessaires à la fragmentation (More Fragment, Don't fragment)**
- **Fragment Offset : position du fragments dans le paquet (en nombre de mots de 8 octets)**
- **TTL : Nombre de routeur pouvant être traversés (décrémenté par chaque routeur)**
- **Protocol : définit le protocole de niveau supérieur (ICMP, UDP, TCP)**
- **Header Checksum : détection d'erreur sur l'entête IP par checksum**
- **Source et destination adresses : chacune sur 4 octets**



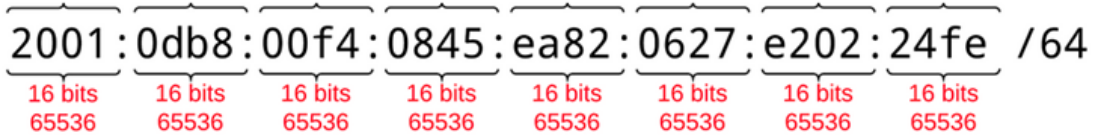
Format des paquets

- **Version : 6**
- **Traffic Class : utilisé pour la gestion des qualités de service**
- **Flow Label : permet le marquage des flux pour des traitements différenciés dans les routeurs**
- **Payload Length: nombre d'octets de données**
- **Next Header : définit le protocole de niveau supérieur (ICMP, UDP, TCP) de la même façon que le champ Protocol d'IPv4**
- **Hop Limit : Nombre de routeur pouvant être traversés, comme le champ TTL d'IPV4**
- **Source et destination adresses: chacune sur 16 octets**



Adresse IPv6

- 128 bits codée en hexadécimal en 8 mots de 16 bits (4 hexas) séparés par des “:”.



- Exemple

  2001:0db8:0000:85a3:0000:0000:ac1f:8001

- Possibilité de supprimer les 0 non significatifs par groupes de 1 à 3

  2001:db8:0:85a3:0:0:ac1f:8001

- Voire par blocs entiers de 4

  2001:db8:0:85a3::ac1f:8001

- Exemple d’URL: http://[2002:400:2A41:378::34A2:36]:8080

- Exemples de subnet:

  2001:660:3000:3210/64

  3000:E334::/48 ou encore: 3000:E334::/60

Capacité d'un subnet IPv6

2001:0db8:00f4:0845:0000:0000:0000:0000 /64

2001:0db8:00f4:0845:ffff:ffff:ffff:ffff /64

---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --

16b 16b 16b 16b 16b 16b 16b 16b

---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --

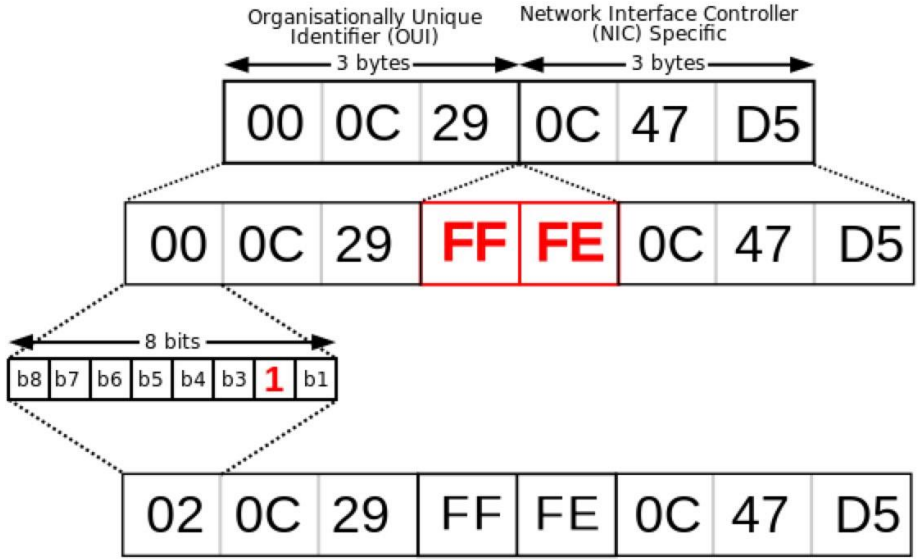
Préfixe Interface ID Masque

Configuration d'une adresses IPv6

- Une adresse IPv6 attribuée à une interface est constituée d'un préfixe de 64 bits et d'un identifiant d'interface de 64 bits.
- Un identifiant d'interface peut être créé de manière statique :
  - statiquement : 2001:db8:14d6:1::1/64, 2001:db8:14d6:1::254/64, fe80::101, par exemple.
- Ou dynamique par autoconfiguration en utilisant l'une de ces trois méthodes :
  - MAC EUI-64, par défaut (RFC 4291)
  - Pseudo-aléatoire, par défaut chez Microsoft, Ubuntu, Mac OSX (RFC 4941)
- Ou dynamique parDHCPv6 (RFC 3315) stateful, si le client est installé et activé (par défaut sur Microsoft Windows et Mac OSX)

Configuration d'une adresses IPv6

- Transformer une adresse MAC48 vers un EUI64



Architecture d'adressage IPv6

- Définie dans le RFC4291, où on détaille tout ce qu'un hôte IPv6 devrait posséder et reconnaitre :
  - Avoir une adresse Link-local sur chaque interface fe80::/10
  - Des adresses Unicast ou Anycast qui ont été configurées sur les interfaces du nœud, 2000::/3
  - L'adresse de Loopback (node-local) ::1/128
  - Les adresses All-Nodes Multicast.
  - L'adresse Solicited-Node Multicast pour chacune des adresses Unicast ou Anycast.
  - Les adresses Multicast des groupes joints par le noeud.

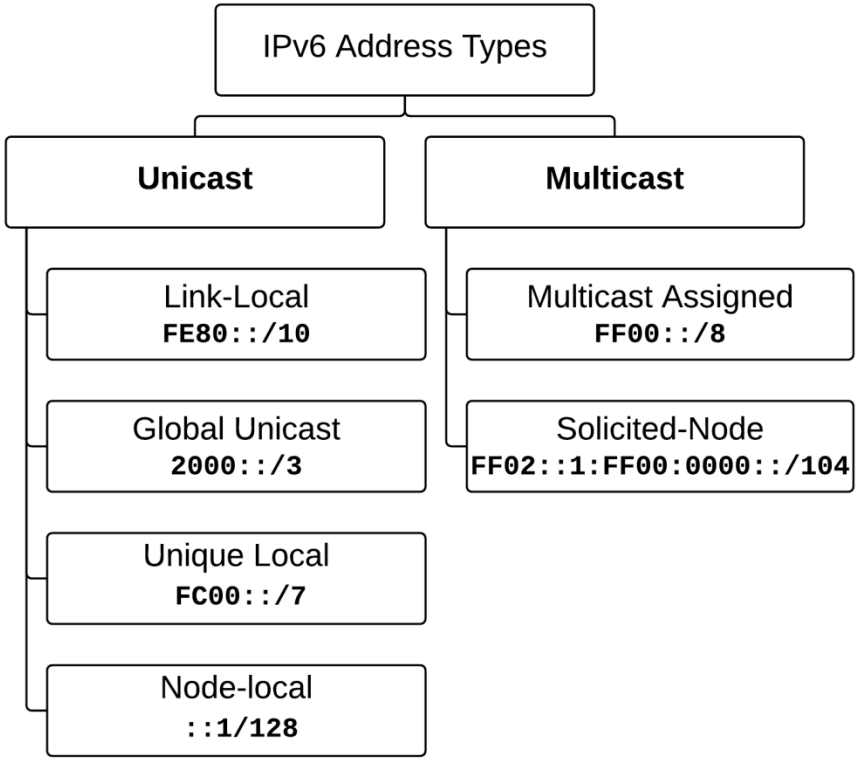
Adresses unicast IPv6

- 0000::/8 Reserved by IETF [RFC4291]
- 0100::/8 Reserved by IETF [RFC4291]
- 0200::/7 Reserved by IETF [RFC4048]
- 0400::/6 Reserved by IETF [RFC4291]
- 0800::/5 Reserved by IETF [RFC4291]
- 1000::/4 Reserved by IETF [RFC4291]
- 2000::/3 Global Unicast [RFC4291]
- 4000::/3 Reserved by IETF [RFC4291]
- c000::/3 Reserved by IETF [RFC4291]
- e000::/4 Reserved by IETF [RFC4291]
- f000::/5 Reserved by IETF [RFC4291]
- F800::/6 Reserved by IETF [RFC4291]
- fc00::/7 Unique Local Unicast [RFC4193]
- fe00::/9 Reserved by IETF [RFC4291]
- fe80::/10 Link Local Unicast [RFC4291]
- fec0::/10 Reserved by IETF [RFC3879]
- ff00::/8 Multicast [RFC4291]

Adresses multicast IPv6

- ff02:0:0:0:0:0:0:1 All Nodes Address (link-local scope)
- ff02:0:0:0:0:0:0:2 All Routers Address
- ff02:0:0:0:0:0:0:5 OSPF IGP
- ff02:0:0:0:0:0:0:6 OSPF IGP Designated Routers
- ff02:0:0:0:0:0:0:9 RIP Routers
- ff02:0:0:0:0:0:0:fb mDNSv6
- ff02:0:0:0:0:0:1:2 All-dhcp-agents
- ff02:0:0:0:0:1:ffxx:xxxx Solicited-Node Address
- ff05:0:0:0:0:0:1:3 All-dhcp-servers (site-local scope)

Types d’adresses IPv6



Préfixe	Description
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques
fe80::/10	Adresses liens locaux
ff00::/8	Adresses multicast

Questions de compréhension

- Quelle est la taille normale d'une adresse IPv6 ?
- Quelles sont les différentes manières d'obtenir une adresse IPv6 ?
- A combien d'adresses a droit un hôte IPv6 ?
- Quels sont les types d'adresses IPv6 ?

Sommaire

- Définitions et terminologie
- Adressage
  - Format et scope (portée) d'une adresse
  - Configuration
  - Unicast, Multicast, Anycast
- **ICMPv6 et DHCPv6**
  - **Neighbor discovery**
- **Sécurité**
- **Transition et cohabitation de l'IPv6 et IPv4**

ICMPv6

- Ce protocole agrège les propriétés de ARP et ICMP pour IPv4
- Permet de découvrir les adresses MAC des hôtes voisins
- Découverte des routeurs voisins pour une route donnée
  - automatiquement
  - Redirection
- Découverte de prefix (adresse globale)
- Découverte de paramètre (par exemple le MTU)
- Auto-configuration d'adresse: permet de récupérer une adresse IPv6 globale
- Résolution d'adresse : Adresse IPv6 -> adresse MAC (équivalent à ARP)
- Détection d'adresse multiple
- Détermination du routeur pour une destination donnée

ICMPv6 pour la gestion des erreurs

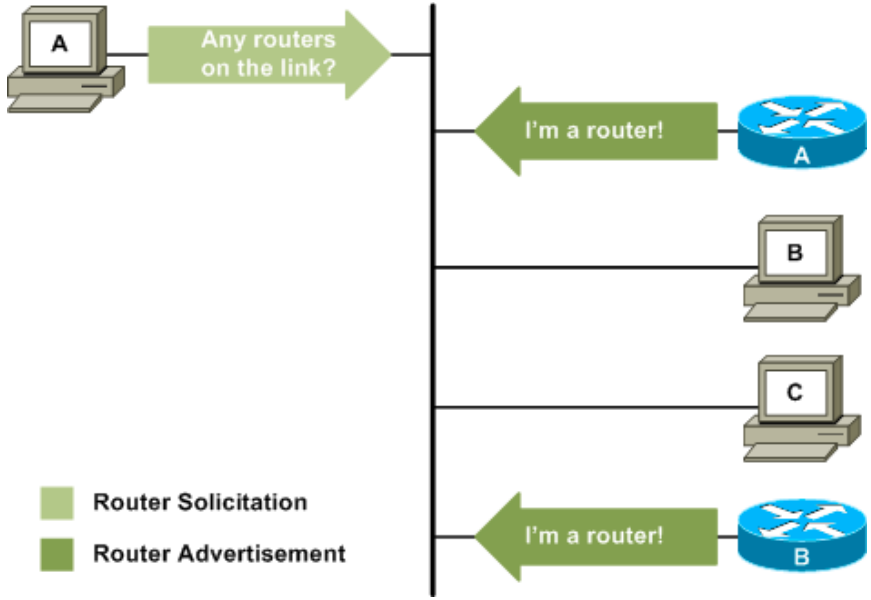
Type	Name	Reference
1	Destination Unreachable	[RFC4443]
2	Packet Too Big	[RFC4443]
3	Time Exceeded	[RFC4443]
128	Echo Request	[RFC4443]
129	Echo Reply	[RFC4443]
133	Router Solicitation	[RFC4861]
134	Router Advertisement	[RFC4861]
135	Neighbor Solicitation	[RFC4861]
136	Neighbor Advertisement	[RFC4861]
151	Multicast Router Advertisement	[RFC4286]
152	Multicast Router Solicitation	[RFC4286]
153	Multicast Router Termination	[RFC4286]
157	Duplicate Address Request	[RFC6775]
158	Duplicate Address Confirmation	[RFC6775]
160	Extended Echo Request	[RFC8335]
161	Extended Echo Reply	[RFC8335]

ICMPv6

- Deux concepts sont importants et novateurs dans l'ICMPv6 par rapport à son cousin en IPv4
  - L'autoconfiguration d'adresse avec le coupe de messages Router Advertisement/Router Solicitation
  - La sollicitation de voisins pour la découverte d'adresse MAC (remplacement de la même fonctionnalité en ARP): Neighbor solicitation/Neighbor advertisement
- Il est à noter que pendant longtemps la configuration de l'adresse était la seule possible avec ICMPv6 Router Advertisement. Depuis la RFC 8106 (IPv6 Router Advertisement Options for DNS Configuration), il est possible de joindre l'adresse du DNS dans ce message lorsqu'il n'y a pas d'alternatives

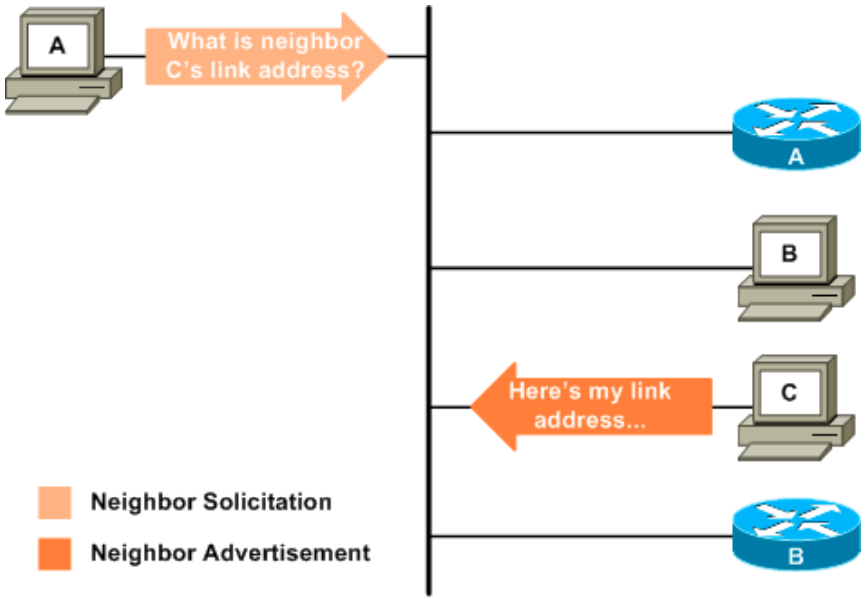
ICMPv6: Autoconfiguration

- Un routeur configuré avec un prefix IPv6 annonce ce préfixe de manière périodique sur le lien: Router Advertisement (RA)
- Ce message contient le prefix qu'un hôte pourrait utiliser pour s'attribuer la partie Interface ID (EUI64, random…)
- Une configuration automatique nécessite la vérification de l'unicité de l'adresse sur le lien (par exe, Neighbor solicitation).
- Si le message RA tarde à être annoncé sur le lien, un nouveau nœud sur le lien peut soliciter tous les routeurs en envoyant un Router Solicitation à ff02::2



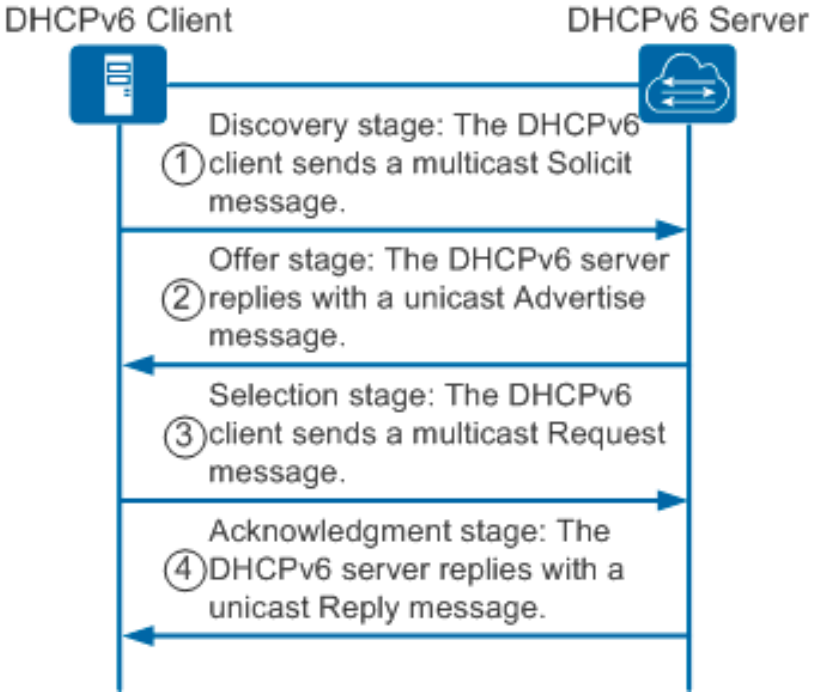
ICMPv6: Recherche de voisins

- Dans un réseau local, un nœud pourrait avoir besoin de connaitre l'adresse MAC d'un voisin pour:
  - Déterminer si une adresse est libre d'utilisation et sans collision
  - Délivrer un paquet réseau
- Un message Neighbor solicitation est envoyé sur le lien réseau à une adresse multicast quand on cherche à déterminer l'adresse link-layer (MAC) et elle est unicast lorsqu'on cherche à valider la joignabilité d'un voisin
- Neighbor adverstisement est la réponse à ce message



DHCPv6

- Protocole qui pratiquement identique au fonctionnement de DHCP en IPv4
- Donne une configuration réseau complète: Adresse, subnet, gateway, dns, et plus.
- Utilise le port UDP 546 du côté client et le port UDP 547 du côté serveur.
- Un client DHCPv6 peut également demander une délégation de préfix du serveur pour qu'il agisse entant que serveur sur un réseau réduit
- La RFC en cours pour ce protocole est rfc8415



Questions de compréhension

- Quel est le mécanisme de découverte des voisins en IPv6 et à quoi il sert ?
- Comment configure-t-on une adresse de manière autonome en IPv6 ? A-t-on besoin d'une information supplémentaire au préfixe pour aller sur Internet dans ce cas ?
- Quelles sont les autres fonctions possibles du protocole ICMPv6 ?

Sommaire

- Définitions et terminologie
- Adressage
  - Format et scope (portée) d'une adresse
  - Configuration
  - Unicast, Multicast, Anycast
- ICMPv6 et DHCPv6
  - Neighbor discovery
- **Sécurité**
- **Transition et cohabitation de l'IPv6 et IPv4**

Sécurité

- Les faiblesses du protocole IPv6 sont sommes toutes très similaires à celles de l'IPv4:
  - Usurpation d'adresse IP source triviale
  - Pas d'authentification ou de chiffrement par défaut
  - Attaques par déni de service et force brute
  - Attaques contre les protocoles de transport ou contre les applications
  - Protocoles de résolution d'adresses sur le réseau local différents (ARP vs. NDP) mais posant des problèmes similaires
  - Protocoles de routage

- Cependant, l'IPv6 apporte quand-mêmes des menaces idoines et qu'il est important de comprendre afin de sécuriser un déploiement

Sécurité

- IPv6 peut amener des difficultés particulières donc:
  - Messages RA d'attaquants. En introduisant des Router Advertisements erronés ou avec des prefixes inexistant s et on amène une machine victime à avoir cette config ou a flooder d'adresses
  - Espionnage sur la vie privée et pistage. Ceci vient principalement de l'adresse IPv6 initialement définie avec une partie de l'adresse issue de l'adresse MAC de l'interface qui est unique.
  - Rétablissement du peer-to-peer dans IPv6 et donc exposition supplémentaire, car on est plus derrière un NAT.
  - Comptage des adresses dans un subnet pour la même raison.
  - Beaucoup d'attaques existent aussi: utiliser un outil spécialisé pour le diagnostic et le pentesting comme: https://www.si6networks.com/tools/ipv6toolkit/

Sécurité

- Une entreprise peut amener ses propres problèmes en migrant des solutions IPv4 en IPv6, ou en essayant d'avoir des politiques équivalentes dans les deux protocoles
  - Par exemple, il peut être difficile d'avoir des règles firewall identique dans les deux protocoles

- Beaucoup d'administrateurs pensent que le NAT et le proxy sont les seules protections sérieuses et basent leur stratégie de sécurité là-dessus.
  - La conséquence est que les société en général désactivent IPv6 considéré comme pas gérable, ce qui ralentit son déploiement

Sommaire

- Définitions et terminologie
- Adressage
  - Format et scope (portée) d'une adresse
  - Configuration
  - Unicast, Multicast, Anycast
- ICMPv6 et DHCPv6
  - Neighbor discovery
- Sécurité
- **Transition et cohabitation de l'IPv6 et IPv4**

Transition IPv4/IPv6

- Double pile ou dual stack
- Doter chaque équipement du réseau d'une double pile protocolaire avec une adresse IPv4 et/ou IPv6 à chaque interface réseau.
- Il s'applique à tous les segments d'un réseau. En contrepartie, ce mécanisme ne prend pas en compte les problèmes de pénurie d'adresses IPv4.
- Tous les équipementiers de coeur de réseaux supportent ce mécanisme, qui permet rapidement d'acheminer du trafic IPv6 dans une infrastructure IPv4 existante.
- Le déploiement de ce mécanisme peut être progressif et ne concerner qu'une partie du coeur de réseau dans un premier temps.

Transition IPv4/IPv6

- 6PE (MPLS)

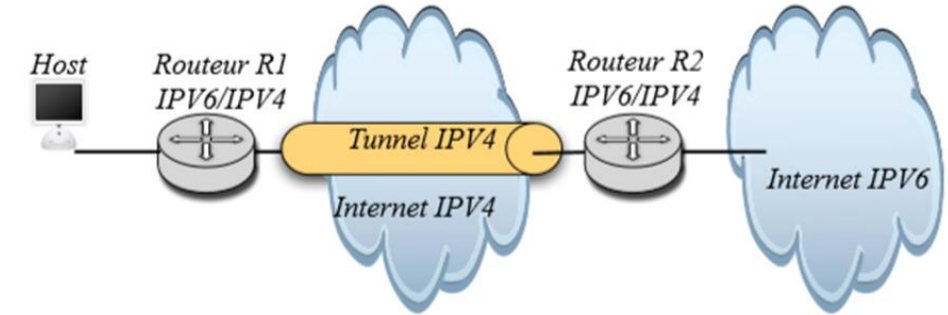
- Profite de la commutation de MPLS (Multi Protocol Label Switching) selon l'étiquette insérée dans un paquet, pour rendre un réseau capable de transporter des paquets IPv6 sans avoir à en modifier tous les équipements.

- Le coeur du réseau MPLS (les équipements P : Provider) reste inchangé. 6PE permet à un opérateur / ISP, dont le coeur de réseau s'appuie sur la technologie MPLS pour acheminer le trafic IPv4, de ne faire évoluer que la partie périphérique de son réseau (les équipements de périphérie : PE : Provider Edge) pour pouvoir transporter aussi le trafic IPv6 de ses usagers.

- Le routage IPv6 est réalisé par les équipements de périphérie (PE) qui attribuent une étiquette à chaque paquet IPv6.

Transition IPv4/IPv6

- Tunnel IPv6 et encapsulation 6to4
- Plusieurs variantes de tunnelisation de traffic IPv6 dans des paquets IPv4 existent
- Il s'agit d'encapsuler le trafic de l'origine du tunnel à sa fin



Prise en charge d'IPv6

- Les systèmes d'exploitation modernes sont tous (ou presque) capables de supporter l'IPv6 et l'IPv4
  - Toute taille d'équipement, de l'IoT au cœur de réseau

- Les applications sont normalement développées de manière agnostique à la génération du protocole IP
  - Les langages de programmation sont normalement prêts depuis longtemps et les librairies existent

- Les fournisseurs d'accès Internet sont normalement tous capables à minima de donner une adresse IPv6 à leurs clients
  - Les déploiements pour les clients entreprises peuvent se faire en IPv6 de bout-en-bout

Prise en charge d'IPv6

- Il est cependant important de dire que malgré les progrès réalisés ces dernières années sur le déploiement d'IPv6, des limitations existent

    - Soit à cause de la sécurité et de la résistance des sysadmin un peu partout
    - Le déploiement n'est pas end-to-end donc, une cassure IPv6 se produit à un moment donnée obligeant le fallback en IPv4
    - Peu d'applications ou de services réseaux sont proposés qui profitent des fonctionnalités de base d'IPv6 (comme le multicast, anycast…)