

Sommaire

CHAPITRE 1 NOTIONS DE BASE IPV6	2
INTRODUCTION	2
I-LIMITATIONS DES ADRESSES IPV4	ERREUR ! SIGNET NON DEFINI.
II-PRESENTATION DES ADRESSES IPV6	2
LA COEXISTENCE ET LA TRANSITION IPV6 -IPV4.....	16

Chapitre 1 Notions de base IPv6

Objectif général

Objectifs spécifiques

À l'issue de ce chapitre, les étudiants seront en mesure de :

- Identifier et écrire les adresses ipv6,

Plan d'adressage

- Définitions des plans d'adressage
- Plan d'adressage agrégé
- Réseaux de test et de production

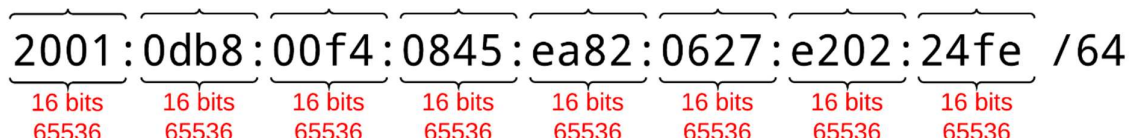
- Adressage
 - Format des adresses IPv6 et notation
 - Adresses unicast/multicast/anycast
 - Adresses locales/globales/ULA, préfixes particuliers

II-Historique et normalisation

Présentation des adresses IPv6

les adresses IPv6 sont des identifiants uniques d'interfaces :

- codés sur 128 bits
- et notés en hexadécimal en 8 mots de 16 bits (4 hexas) séparés par des ":".

The diagram shows the IPv6 address 2001:0db8:00f4:0845:ea82:0627:e202:24fe /64. Each of the eight hexadecimally represented 16-bit segments is bracketed and labeled '16 bits' and '65536' in red text below it. The final segment is followed by a slash and the number 64, indicating the prefix length.

Exemple d'adresse IPv6 Global Unicast

- ✓ Le **masque** identifie la partie fixe d'une adresse qui correspond aussi au numéro de réseau de 64 bits (le préfixe).

- ✓ Le **préfixe** est l'élément commun à toutes les adresses d'une même plage (au sein d'un réseau).

Par exemple, pour l'adresse "Global

Unicast" 2001:0db8:00f4:0845:ea82:0627:e202:24fe/64 dans son écriture extensive :

2001:0db8:00f4:0845:ea82:0627:e202:24fe/64							
-----	-----	-----	-----	-----	-----	-----	-----
16b	16b	16b	16b	16b	16b	16b	16b
-----	-----	-----	-----	-----	-----	-----	-----
Préfixe				Interface ID		Masque	

1. Avantages

IPv6 répond aux exigences de plus en plus complexes de l'adressage hiérarchique qu'IPv4 ne fournit pas. Les principaux avantages et caractéristiques d'IPv6 sont les suivants :

- **Espace d'adressage étendu** : Un espace d'adresses de 128 bits représente environ 340 trillions de trillions de trillions d'adresses.
- **Auto-configuration stateless de l'adresse** : IPv6 fournit aux périphériques hôtes une méthode pour générer leurs propres adresses IPv6 routables. IPv6 prend également en charge la configuration dynamique à l'aide de DHCPv6.
- **Élimine le besoin de NAT/PAT** : NAT/PAT a été conçu dans le cadre de la solution de l'épuisement des adresses IPv4. Avec IPv6, l'épuisement des adresses n'est plus un problème. NAT64, cependant, joue un rôle important dans la rétrocompatibilité avec IPv4.
- **En-tête plus simple** : Un en-tête plus simple offre plusieurs avantages par rapport à IPv4:
 - ✓ Meilleure efficacité de la performance et l'évolutivité du routage et du débit de transfert
 - ✓ Pas de diffusion et, par conséquent, pas de menace potentielle de tempêtes de diffusion.
 - ✓ Aucune exigence pour le traitement des sommes de contrôle
 - ✓ Mécanismes d'extension d'en-tête plus simples et plus efficaces
- **Mobilité et sécurité** : La mobilité et la sécurité contribuent à assurer la conformité aux normes IP mobile et IPsec :

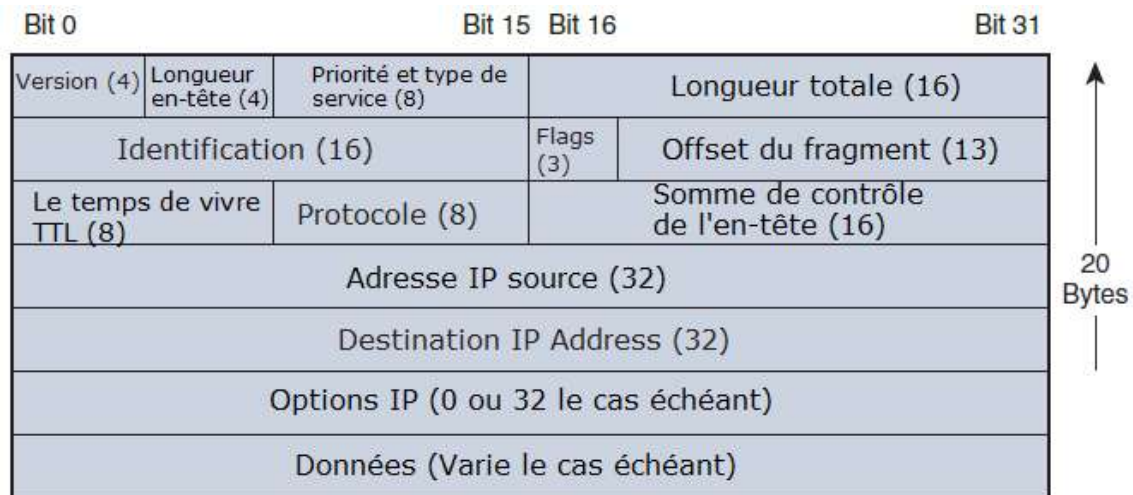
- ✓ IPv4 ne permet pas automatiquement aux appareils mobiles de se déplacer sans interruption des connexions réseau établies.
- ✓ Dans IPv6, la mobilité est intégrée, ce qui signifie que n'importe quel nœud IPv6 peut utiliser la mobilité si nécessaire.
- ✓ IPsec est activé sur chaque nœud IPv6 et peut être utilisé, ce qui rend l'Internet IPv6 plus sécurisée.
- **Stratégies de transition :** Vous pouvez incorporer les capacités IPv4 existantes avec les fonctionnalités supplémentaires d'IPv6 de plusieurs façons :
 - ✓ Vous pouvez implémenter une méthode de double pile, avec IPv4 et IPv6 configurés sur l'interface d'un périphérique réseau.
 - ✓ Vous pouvez utiliser le tunneling, qui deviendra de plus en plus important à mesure que l'adoption d'IPv6 augmentera.

I. Comparaison ipv4 vers ipv6

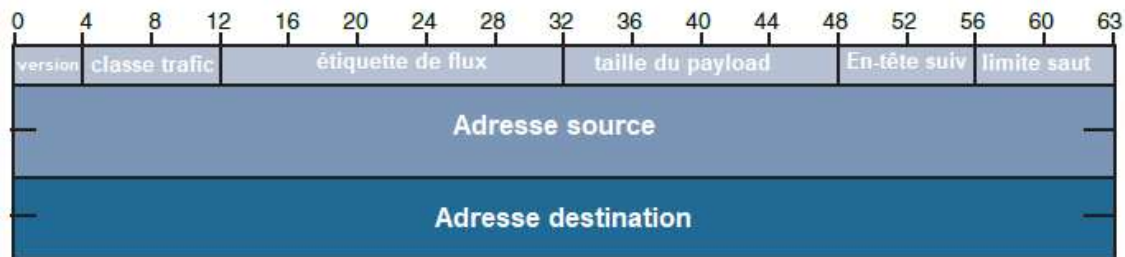
Tableau A : Comparaison d'adresses IPv4 et IPv6

	IPv4 (4 Octets)	IPv6 (16 Octets)
Représentation binaire	11000000.10101000.00001010.01100101	10100101.00100100.01110010.11010011.00101100.
Représentation alphanumérique	192.168.10.101	A524:72D3:2C80:DD02:0029:EC7A:002B:EA73
Nombre total d'adresses IP	4,294,967,296 or 2^{32}	$3.4 * 10^{38}$ or 2^{128}

En-tête IPv4



En-tête IPv6



REMARQUE : Référez-vous à la RFC 2460 pour la spécification complète d'IPv6.

paquets sur le réseau IP :

Champs	Description
Version	Contient la version du protocole IP selon laquelle le paquet IP a été créé.
Classe de trafic (traffic class)	Définit les priorités (8 bits)
Identificateur de flux (flow label)	Les paquets avec le même identificateur de flux sont traités de la même manière (20 bits)
Longueur des données utiles (payload length)	Donne la longueur du contenu du paquet, y compris les extensions mais sans les données d'en-tête (16 bits)

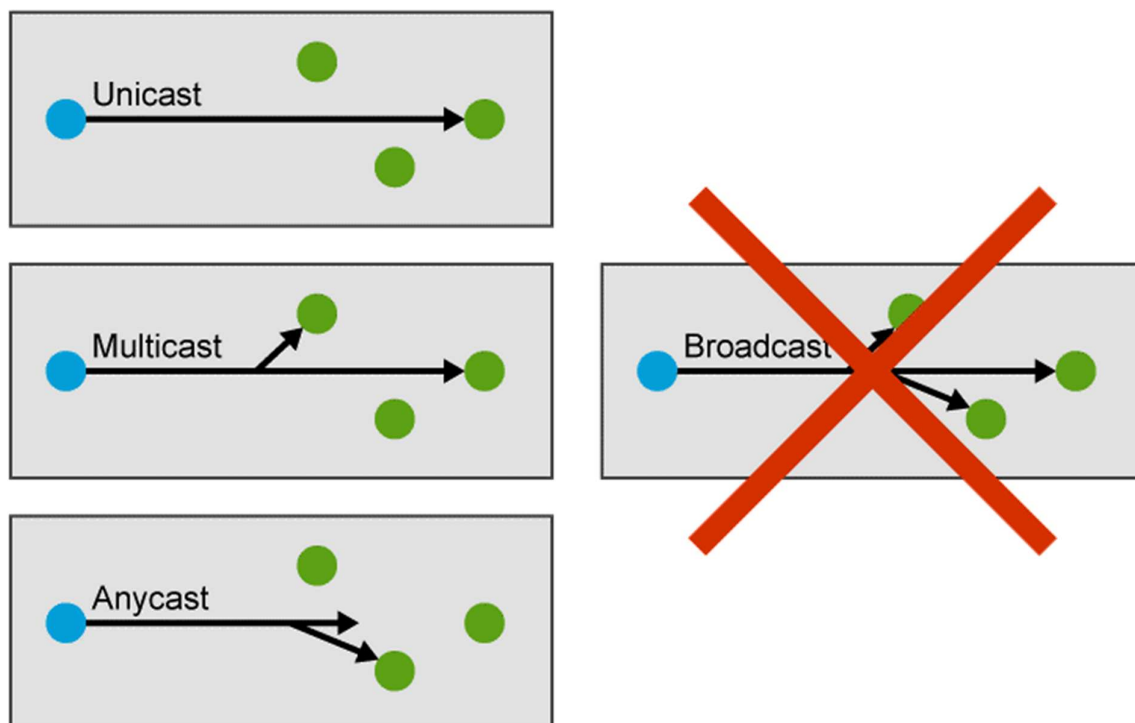
Champs	Description
En-tête suivant (next header)	Indique le protocole de la couche de transport supérieure (8 bits)
Sauts maximum (hop limit)	Indique le nombre de sauts maximal pour les étapes intermédiaires (routeurs), sur lesquelles un paquet peut passer avant d'expirer (8 bits)
Adresse IP source (Source IP address)	Comprend l'adresse de l'expéditeur (128 bits)
Adresse IP destination (destination IP address)	Comprend l'adresse du destinataire (128 bits)

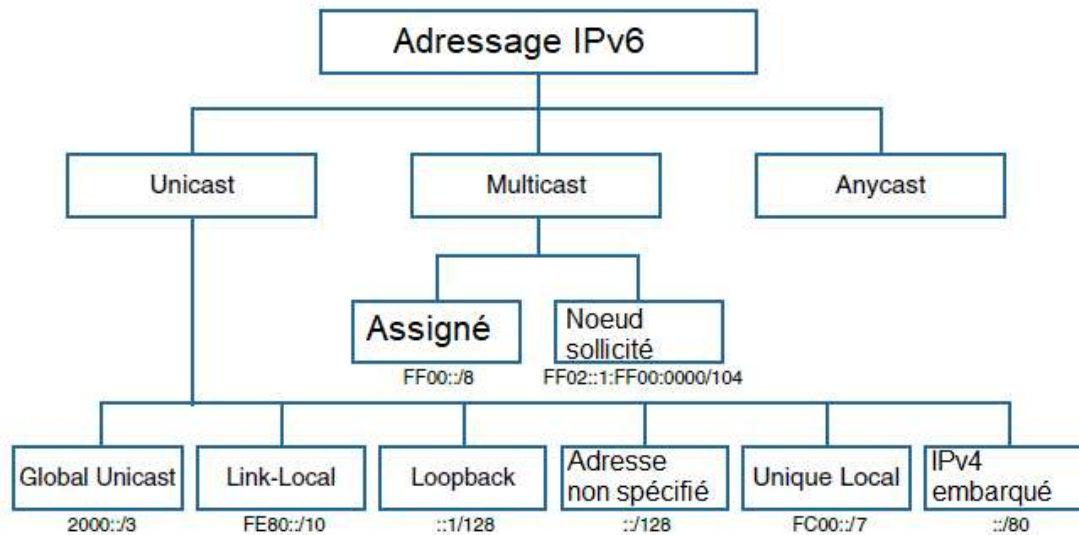
II. Types adresses ipv6

IPv4 a trois types d'adresses : unicast, multicast et broadcast.

IPv6 utilise unicast, multicast et anycast.

IPv6 n'utilise pas de diffusion.





Unicast

Une adresse unicast identifie de manière unique une interface sur un périphérique IPv6.

Un paquet envoyé à une adresse unicast est reçu par l'interface qui lui est affectée.

Multidiffusion

La multidiffusion est une technique utilisée pour qu'un appareil envoie un seul paquet à plusieurs destinations simultanément.

Une adresse IPv6 multicast définit un groupe de périphériques connu sous le nom de groupe multicast et est équivalent 224.0.0.0/4 en IPv4.

Les adresses IPv6 multicast ont le préfixe FF00::/8.

Deux types d'adresses de multidiffusion IPv6 sont utilisés :

- Multidiffusion assignée
- Multidiffusion à Nœud sollicité (Solicited node multicast)

Multidiffusion assignée

Les adresses de multidiffusion assignées sont utilisées dans le contexte de protocoles spécifiques.

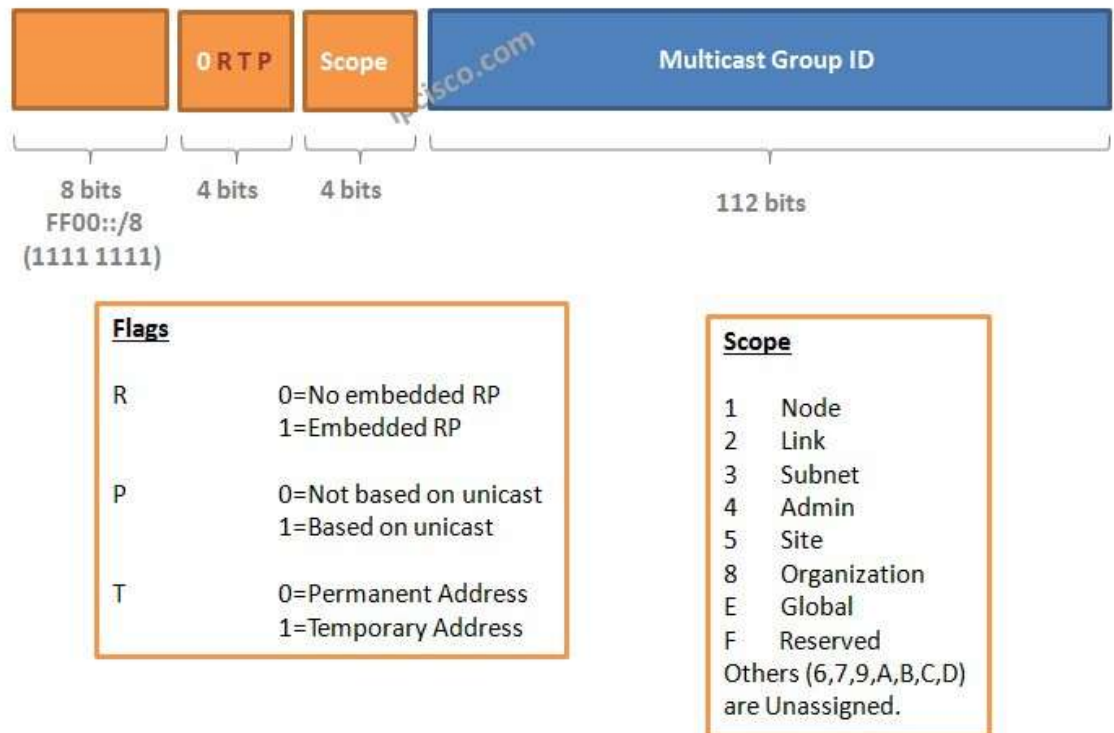
Deux groupes de multidiffusion IPv6 les plus courants sont les suivants :

- **Groupe multicast All-nodes FF02::1:** Il s'agit d'un groupe multicast auquel se joignent tous les périphériques compatibles IPv6.

Par exemple, un routeur qui envoie une annonce de routeur (RA: Router Advertisement) ICMPv6 utilise l'adresse All-nodes FF02::1. Les périphériques compatibles IPv6 peuvent ensuite utiliser les informations RA pour connaître les informations d'adresse du lien telles que le préfixe, la longueur du préfixe et la passerelle par défaut.

- **Groupe multidiffusion tous routeurs FF02::2:** Il s'agit d'un groupe multicast auquel tous les routeurs IPv6 se joignent. Un routeur devient membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 avec la commande de configuration globale `ipv6 unicast-routing`. Un paquet envoyé à ce groupe est reçu et traité par tous les routeurs IPv6 sur le lien. Par exemple, les périphériques compatibles IPv6 envoient des messages de sollicitation de routeur ICMPv6 (RS) à l'adresse multicast all-routers demandant un message RA.

IPv6 Multicast Address



Multidiffusion à nœud sollicité (Solicited-Node Multicast)

En plus de chaque adresse unicast affectée à une interface, un périphérique possède une adresse multicast spéciale connue sous le nom d'adresse multicast de nœud sollicité.

Ces adresses de multidiffusion sont automatiquement créées à l'aide d'un mappage spécial de l'adresse unicast du périphérique avec le préfixe de multidiffusion par nœud sollicité `FF02:0:0:0:0:0:1:FF00::/104`.

l'adresse de multidiffusion par nœud sollicité se compose de deux parties :

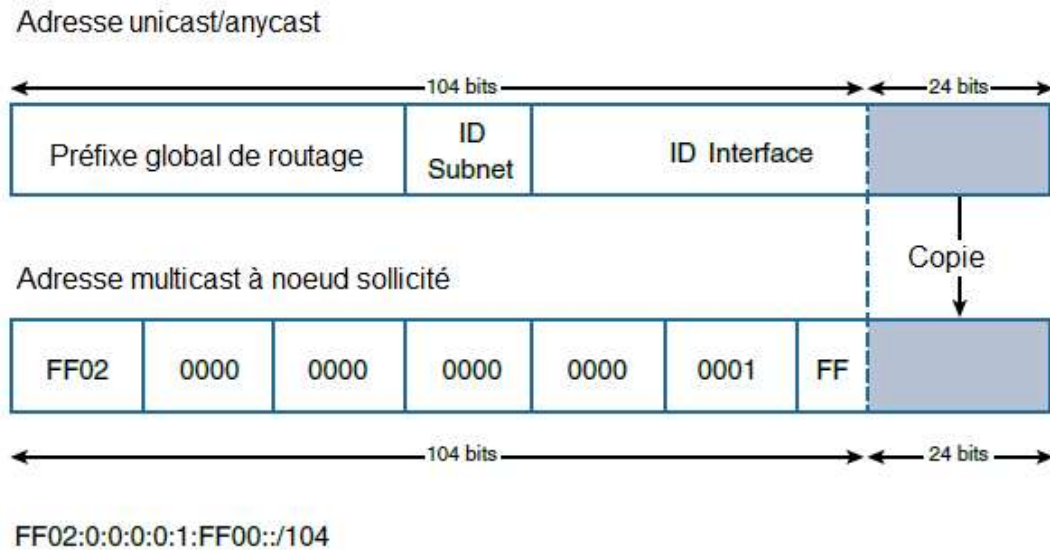


Figure : Structure d'adresses de multidiffusion à nœud sollicité

IPv6 Solicited-Node Multicast Address



Le préfixe multicast FF02:0:0:0:0:0:0:1:FF00::/104 : Il s'agit des 104 premiers bits de toute l'adresse de multidiffusion par nœud sollicité.

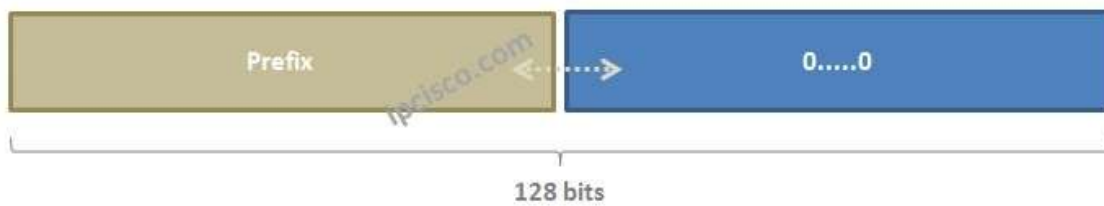
Les 24 bits Moins significatif : Ces bits sont copiés à partir des 24 bits de l'extrême droite de l'adresse unicast globale ou de l'adresse unicast locale de l'appareil.

Anycast

Il s'agit d'une adresse qui peut être affectée à plusieurs appareils ou interfaces.

Un paquet envoyé à une adresse anycast est routé vers le périphérique "le plus proche" qui est configuré avec l'adresse anycast,

IPv6 Anycast Address



Exemple :

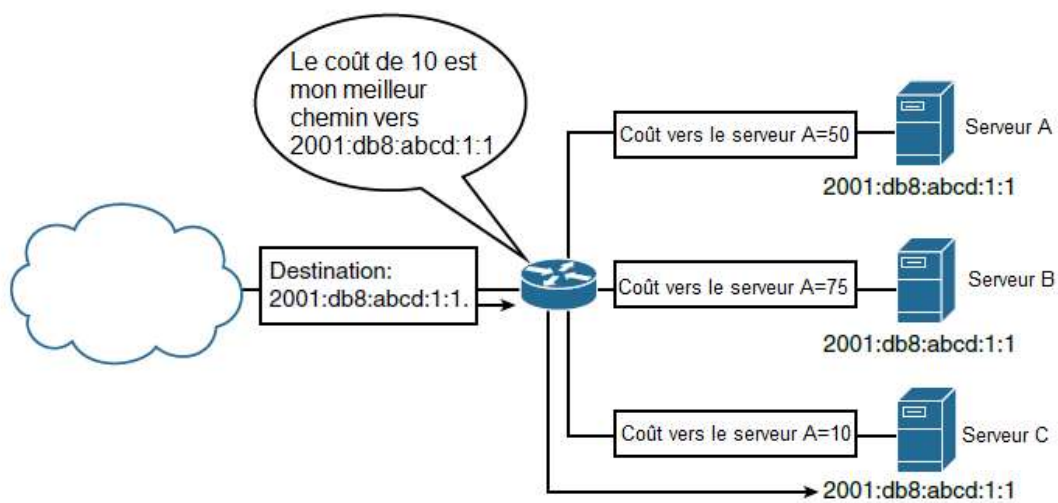
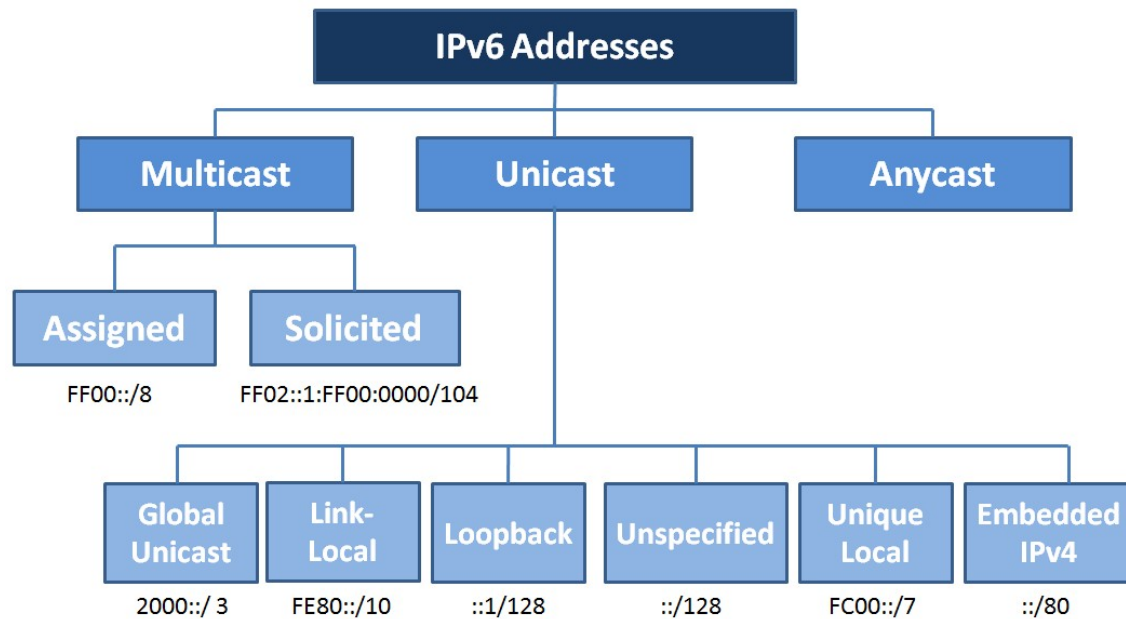


Figure : Exemple d'adressage Anycast

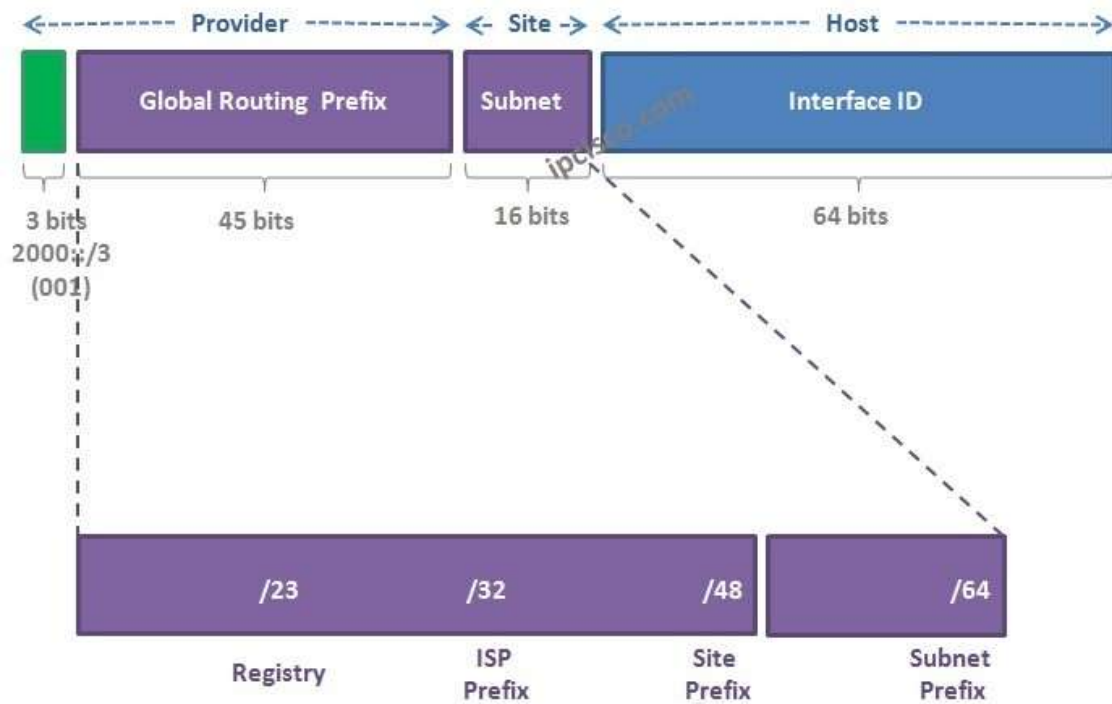
III. Types adresses ipv6 unicast



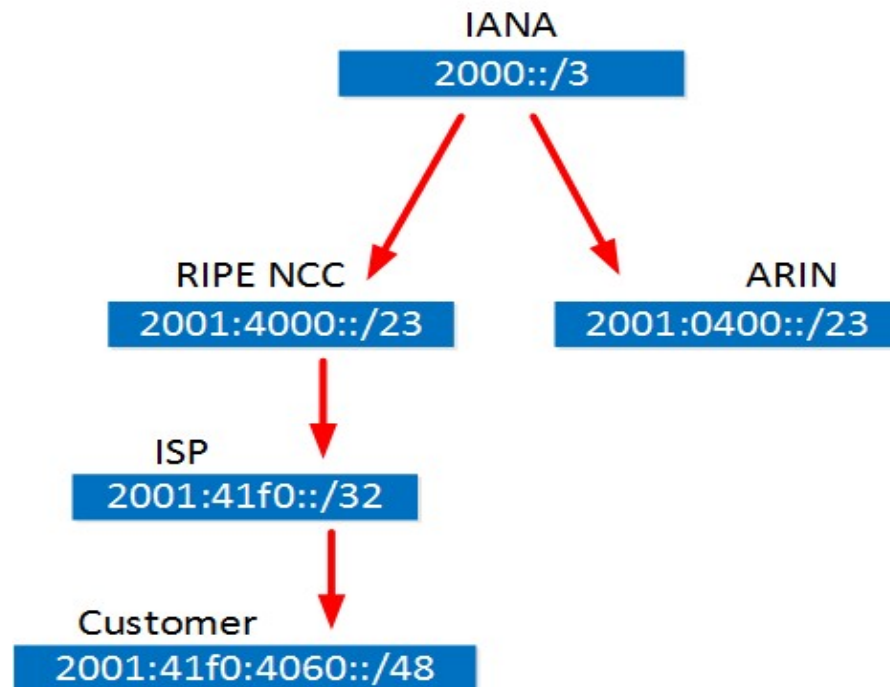
Adresse ipv6 Unicast global

Les adresses unicast globales, qui ont la même fonction que les adresses unicast, sont des adresses routables sur un réseau public. C'est le même principe que les adresses IPv4 publiques.

Global Unicast IPv6 Address



Exemple :



Adresse ipv6 Link-Local

- Une adresse Link-Local est obligatoire sur chaque interface activée en IPv6.
- Elle est générée automatiquement et elle est censée être unique sur le lien.
- On la reconnaît par son préfixe fe80::/10 ou ses dix premiers bits à 1111111010.
- Cette destination est purement locale sur la liaison de l'interface. Les routeurs IPv6 ne transfèrent pas cette destination.
- Leurs durées de vie Valid Lifetime et Preferred Lifetime sont infinies.
- Configurées sur les interfaces leur masque est obligatoirement /64.

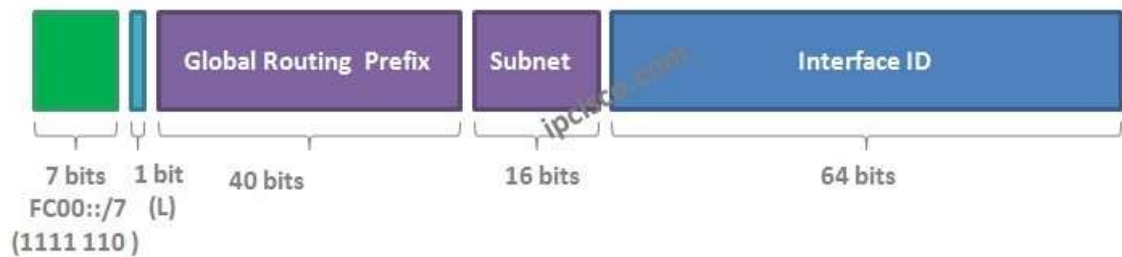
Link-Local Unicast IPv6 Address



1. Adresse ipv6 unique local

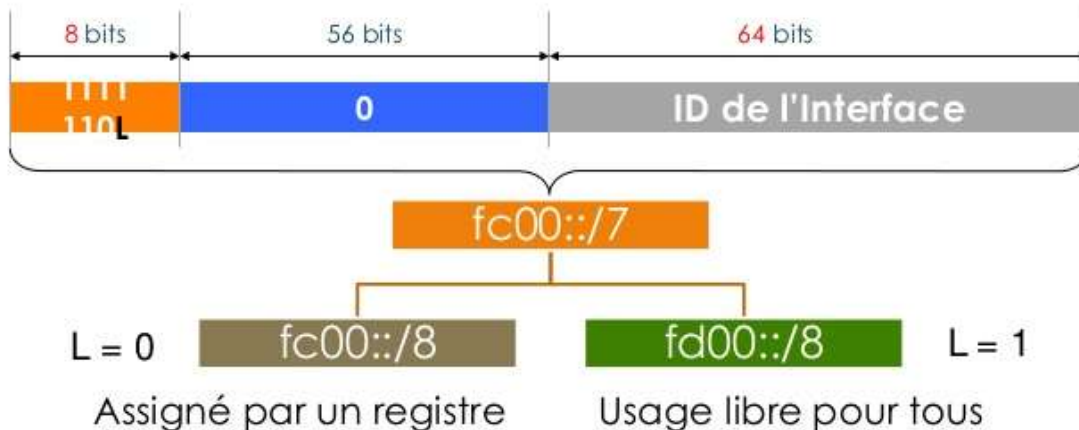
- Comparables aux adresses privées IPv4 RFC1918 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16 dans le sens où elles **ne sont pas** "globalement routables".
- Elles ne connaissent pas de destination dans l'Internet public.
- Elles permettent aux sites privés de s'interconnecter entre eux en réduisant la probabilité de conflits sur des blocs d'adresses non uniques qui se chevauchent.
- En cas de fuite DNS, il y a peu de risque de conflit avec d'autres adresses.
- Cet adressage privé IPv6 est censé être unique afin d'éviter un chevauchement d'adresses identiques à chaque extrémité d'une connexion VPN par exemple.
- On les reconnaît par leur préfixe FD00::/8 dont les 40 bits suivants ont été générés aléatoirement pour compléter un préfixe /48.

Unique-Local Unicast IPv6 Address



Exemple :

On peut les utiliser pour identifier des destinations privées entre des sites distants entre Paris et Lille, entre Bruxelles et Londres ou entre le bâtiment de la rue du commerce et celui du Boulevard du Nord ... à travers des connexions dédiées ou Internet sécurisées par IPSEC



2. Adresse de bouclage

l'adresse 0 :0 :0 :0 :0 :0 :0 :1 équivalente à 127 .0.0.1 en IPv4 ayant le préfixe ::1/128 est d'une validité limitée à l'hôte.

3. Adresse indéterminée

(0 :0 :0 :0 :0 :0 :0 :0) cette adresse est utilisée par des protocoles d'initiations d'interfaces.

IV. Les règles d'adressage

- La notation impose un regroupement par 16 bits ou 2 octets.
- Les zéros leaders (du poids fort) de chaque bloc peuvent être omis.
- Les groupes consécutifs de zéros peuvent être substitués par des zéros.

- L'écriture selon le principe de CIDR: adresse/**longueur_prefixe**.
- L'abréviation «::» ne peut apparaître qu'une fois au plus dans une adresse.

Exemple :

L'adresse **0080:0000 :0000 :0000 :0023 :4567 :89AB :CDEF** est équivalente à celles-ci, comme les règles d'adressages permettent de supprimer les zéros leaders : **80:0000 :0000 :0000 : 23 :4567 :89AB :CDEF** .

Il est également possible de remplacer un groupe de zéros consécutifs par un zéro :

80: 0 : 0 : 0 :23 :4567 :89AB :CDEF

Les octets vides peuvent être omis, et donc l'adresse précédente devient :

80 :: 23 :4567 :89AB :CDEF

Il est important de noter que dans certains cas il n'est pas possible de supprimer tous les octets vides. Pour l'adresse suivante : **2001:db8:0:12b0:0:0:54c:13ab**

Si on supprime tous les octets vides il nous sera impossible de savoir combien d'octets ont été raccourcis sur chaque côté. L'adresse équivalente sera : **2001:db8:0:12b0::54c:13ab**

La coexistence et la transition IPv6 -IPv4

Toutefois, un basculement total vers l'IPv6 est inenvisageable en raison du nombre des organismes et des entités impliqués dans l'Internet, ainsi une longue phase de cohabitation entre IPv4 et IPv6 est prévue pour durer longtemps, mais l'incompatibilité entre les deux versions du protocole nécessite des mécanismes adaptés, dans ce sens, plusieurs mécanismes existent pour assurer la cohabitation IPv6/IPv4 que l'on peut regrouper selon les catégories suivantes:

Dual-Stack : les équipements (Machines, Serveurs, Routeurs) disposent des deux adresses IPv4 et IPv6 et peuvent gérer les deux piles protocolaires.

Le tunneling (les tunnels) : ils permettent aux systèmes avec IPv6 de communiquer en utilisant une infrastructure en IPv4, il consiste à encapsuler les datagrammes IPv6 dans IPv4. deux types de Tunnel existent, les tunnels statiques comme GRE et MCT, et les tunnels dynamiques comme 6to4, ISATAP et Teredo.

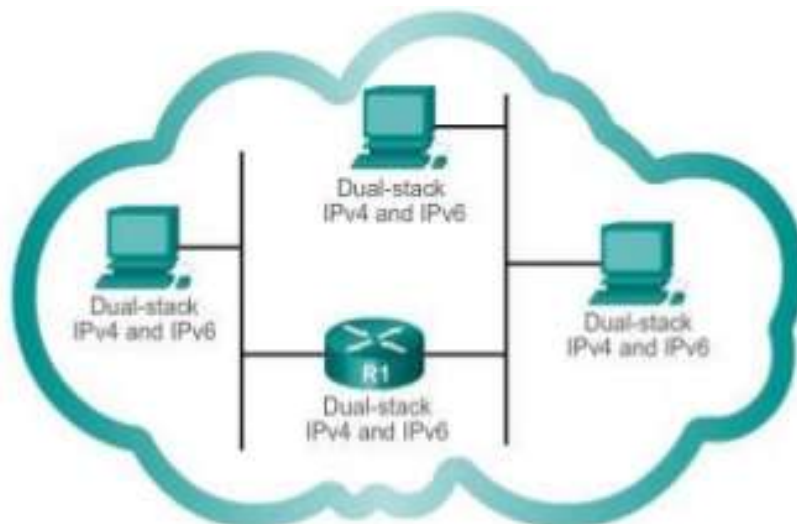
Les protocoles de Transition (NAT): permet à des équipements appartenant à des réseaux natifs IPv4 ou IPv6 de communiquer à travers un nœud de translation, parmi ces mécanismes on trouve NAT-PT et NAT64.

La solution 6PE/6VPE : qui permet d'interconnecter des clients IPv6 tout en conservant le réseau backbone IP/MPLS en IPv4 et profiter en même temps des avantages du MPLS.

Chacun des mécanismes de la cohabitation IPv4/IPv6 apporte des avantages, mais présente également des limitations qui rend son utilisation seul inefficace, et même avec la transition vers l'IPv6,

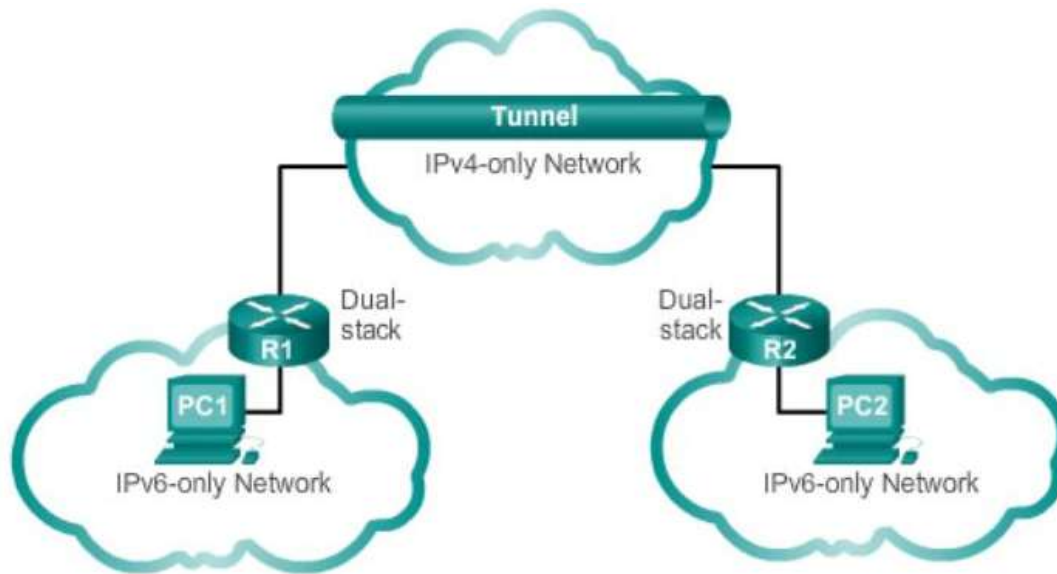
- **La double pile ou Dual-Stack** : l'utilisation de la double pile est la technique la plus simple, elle consiste à doter les nœuds d'une pile IPv6 et d'une autre IPv4.

L'avantage principal de cette méthode est de pouvoir se connecter aux applications IPv4 existantes via IPv4, tout en ayant accès aux applications IPv6 via le réseau IPv6. Cependant, comme les deux protocoles fonctionnent simultanément sur une machine, cela peut être coûteux en termes de performance et d'utilisation CPU.



- **Les tunnels d'encapsulation des datagrammes** : créer des tunnels pour transporter IPv6 dans IPv4 ou l'inverse.

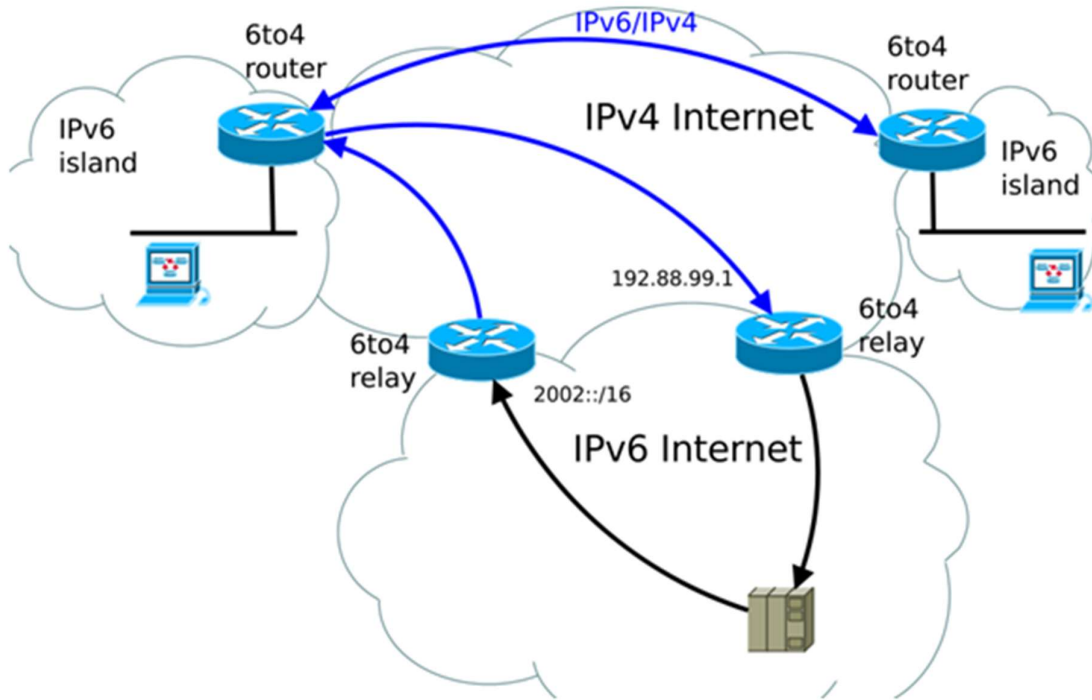
La passerelle d'accès au réseau vérifie si le datagramme d'arrivée correspond ou non au protocole transit. Si le datagramme ne correspond pas au protocole, il sera encapsulé dans un datagramme du réseau transit pour qu'il puisse être acheminé comme tout autre paquet qui correspond nativement au réseau de transit. Les tunnels automatiques servent à joindre une machine IPv6 à un réseau IPv4. Les deux machines établissant le tunnel doivent disposer d'une pile IPv4/IPv6. Contrairement à la destination qui ne peut être que la machine destinataire du paquet, la source d'un paquet dans le tunnel peut être la machine émettrice du paquet ou un routeur. Dans le cas où la source est un routeur, il faudra que la machine source possède une adresse IP compatible.



- **La translation 6to4** : le mécanisme 6to4 permet d'interconnecter des sites 6to4 entre eux à travers un réseau IPv4.

Ce mécanisme nécessite, pour les routeurs, une adresse IPv4 publique (de préférence fixe) et une double pile IP. Chaque routeur se crée un préfixe IPv6 unique et l'utilise sur tout son site. Le préfixe est construit en ajoutant l'adresse IP du routeur au préfixe 2002 ::/16.





	IPv4	IPv6
Historique	Septembre 1981	Décembre 1998
Norme	<i>RFC 791</i>	RFC: 2460
Adresse	32 bits (4 octets)	128 bits (16 octets)
Fragmentation de paquets	Routeurs et hôtes d'envoi	Envoi d'hôtes uniquement
Configuration d'adresse	Manuel ou via DHCP	Autoconfiguration d'adresse sans état (SLAAC) à l'aide du protocole ICMPv6 (Internet Control Message Protocol) version 6 ou DHCPv6
Enregistrements DNS	Adresse (A) enregistrements, noms d'hôtes cartes Enregistrements de pointeur (PTR), Domaine DNS IN- ADDR.ARPA	Enregistrements d'adresse (AAAA), noms d'hôtes cartes Enregistrements de pointeur (PTR), Domaine DNS IP6.ARPA
IPSec	en option, externe	Champs obligatoires
Taille de paquet	576 octets requis, fragmentation facultative	1280 octets requis sans fragmentation
Résolution IP vers MAC	diffusion ARP	Sollicitation Voisin Multicast