

S1, Maîtrise de l'ordinateur
Unité de module 631-2
Introduction aux réseaux

Initiation aux réseaux

Chapitre 8. Adressage IP

- 8.1 Adresses réseau IPv4
- 8.2 Les adresses réseau IPv6
- 8.3 Vérification de la connectivité

Objectifs



- Décrire la structure d'une adresse IPv4.
- Décrire le rôle du masque de sous-réseau.
- Comparer les caractéristiques et les utilisations des adresses IPv4 de monodiffusion, de diffusion et de multidiffusion.
- Comparer l'utilisation de l'espace d'adressage public et de l'espace d'adressage privé.
- Expliquer le besoin d'adressage IPv6.
- Décrire la représentation d'une adresse IPv6.
- Décrire les types d'adresses réseau IPv4 et IPv6.
- Configurer les adresses de monodiffusion globale.
- Décrire les adresses de multidiffusion.
- Décrire le rôle du protocole ICMP dans un réseau IP (IPv4 et IPv6 inclus).
- Utiliser les utilitaires ping et traceroute pour tester la connectivité réseau.

Table des matières



8.1 Adresses réseau IPv4

8.1.1 *Structure de l'adresse IPv4*

8.1.1.2 Système binaire

8.1.1.3 Conversion d'une adresse binaire en adresse décimale

8.1.1.4 Exercice – Conversion de nombres binaires en nombres décimaux

8.1.1.5 Conversion de nombres décimaux en nombres binaires

8.1.1.7 Exercice - Conversion de nombres décimaux en nombres binaires

8.1.2 *Masque de sous-réseau IPv4*

8.1.2.1 Partie réseau et partie hôte d'une adresse IPv4

8.1.2.2 Examen de la longueur du préfixe

8.1.2.3 Réseau, hôte et adresses de diffusion IPv4

8.1.2.4 Première et dernière adresses d'hôte

8.1.2.5 Opération AND au niveau du bit

8.1.2.6 Importance de l'opération AND

8.1.2.8 Travaux pratiques – Conversion des adresses IPv4 en binaire

8.1.2.9 Exercice – Utilisation de l'opération AND pour déterminer l'adresse réseau

8.1.3 *Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion*

8.1.3.3 Transmission monodiffusion

8.1.3.4 Transmission de diffusion

8.1.3.5 Transmission multidiffusion

8.1.3.7 Exercice – Calcul des adresses réseau, de diffusion et d'hôte

Table des matières (suite)



8.1.4 Les types d'adresses IPv4

8.1.4.1 Adresses IPv4 publiques et adresses IP privées

8.1.4.3 Les adresses IPv4 réservées

8.1.4.4 L'ancien système d'adressage par classe

8.1.4.5 L'attribution des adresses IP

8.2 Les adresses réseau IPv6

8.2.1 Les problèmes liés au protocole IPv4

8.2.1.1 Ce qui rend IPv6 nécessaire

8.2.1.2 La coexistence des protocoles IPv4 et IPv6

[8.2.1.3 Exercice – Problèmes liés au protocole IPv4 et solutions](#)

8.2.2 Adressage IPv6

8.2.2.2 Représentation de l'adresse IPv6

8.2.2.3 Règle n° 1 - Omettre les zéros en début de segment

8.2.2.4 Règle n° 2 - Omettre les séquences composées uniquement de zéros

[8.2.2.5 Exercice - Entraînement sur les représentations d'adresses IPv6](#)

8.2.3 Les types d'adresses IPv6

8.2.3.1 Types d'adresses IPv6

8.2.3.2 Longueur de préfixe IPv6

8.2.3.3 Les adresses de monodiffusion globale IPv6

Table des matières (suite)



8.2.3.4 Les adresses de monodiffusion link-local IPv6

8.2.3.5 Exercice - Identifier les types d'adresse IPv6

8.2.4 Les adresses de monodiffusion globale IPv6

8.2.4.1 La structure d'une adresse de monodiffusion globale IPv6

8.2.4.2 La configuration statique d'une adresse de monodiffusion globale

8.2.4.3 La configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

8.2.4.4 La configuration dynamique d'une adresse de monodiffusion globale avec la méthode DHCPv6

8.2.4.5 La génération aléatoire ou à l'aide de la méthode EUI-64

8.2.4.6 Les adresses link-local dynamiques

8.2.4.7 Adresses Link-Local statiques

8.2.4.8 Vérifier la configuration des adresses IPv6

8.2.5 Les adresses de multidiffusion IPv6

8.2.5.1 Les adresses de multidiffusion IPv6 attribuées

8.2.5.2 Les adresses de multidiffusion IPv6 de nœud sollicité

8.2.5.3 Packet Tracer : configuration de l'adressage IPv6

8.2.5.4 Travaux pratiques - Identifier les adresses IPv6

8.2.5.5 Travaux pratiques - Configurer les adresses IPv6 sur des périphériques réseau

Table de matières (suite)



8.3 Vérification de la connectivité

8.3.1 ICMP

8.3.1.1 Les messages ICMPv4 et ICMPv6

8.3.1.2 Les messages de sollicitation et d'annonce de routeur ICMPv6

8.3.1.3 Les messages de sollicitation et d'annonce de voisin ICMPv6

8.3.2 Test et vérification

8.3.2.1 Ping - Tester la pile locale

8.3.2.2 Ping - Tester la connectivité au réseau local

8.3.2.3 Ping - Tester la connectivité à distance

8.3.2.4 Traceroute - Tester le chemin

S1, Maîtrise de l'ordinateur
Unité de module 631-2
Introduction aux réseaux (C1b)

Initiation aux réseaux

Chapitre 8. Adressage IP

8.1 Adresses réseau IPv4

8.2 Les adresses réseau IPv6

8.3 Vérification de la connectivité

8.1 Adresses réseau IPv4

8.1.1 Structure de l'adresse IPv4

8.1.1.2 Système binaire

Une adresse IPv4 est constituée de 32 bits, regroupés en 4 blocs de 8 bits (octet).

110000001010100000000000100001011

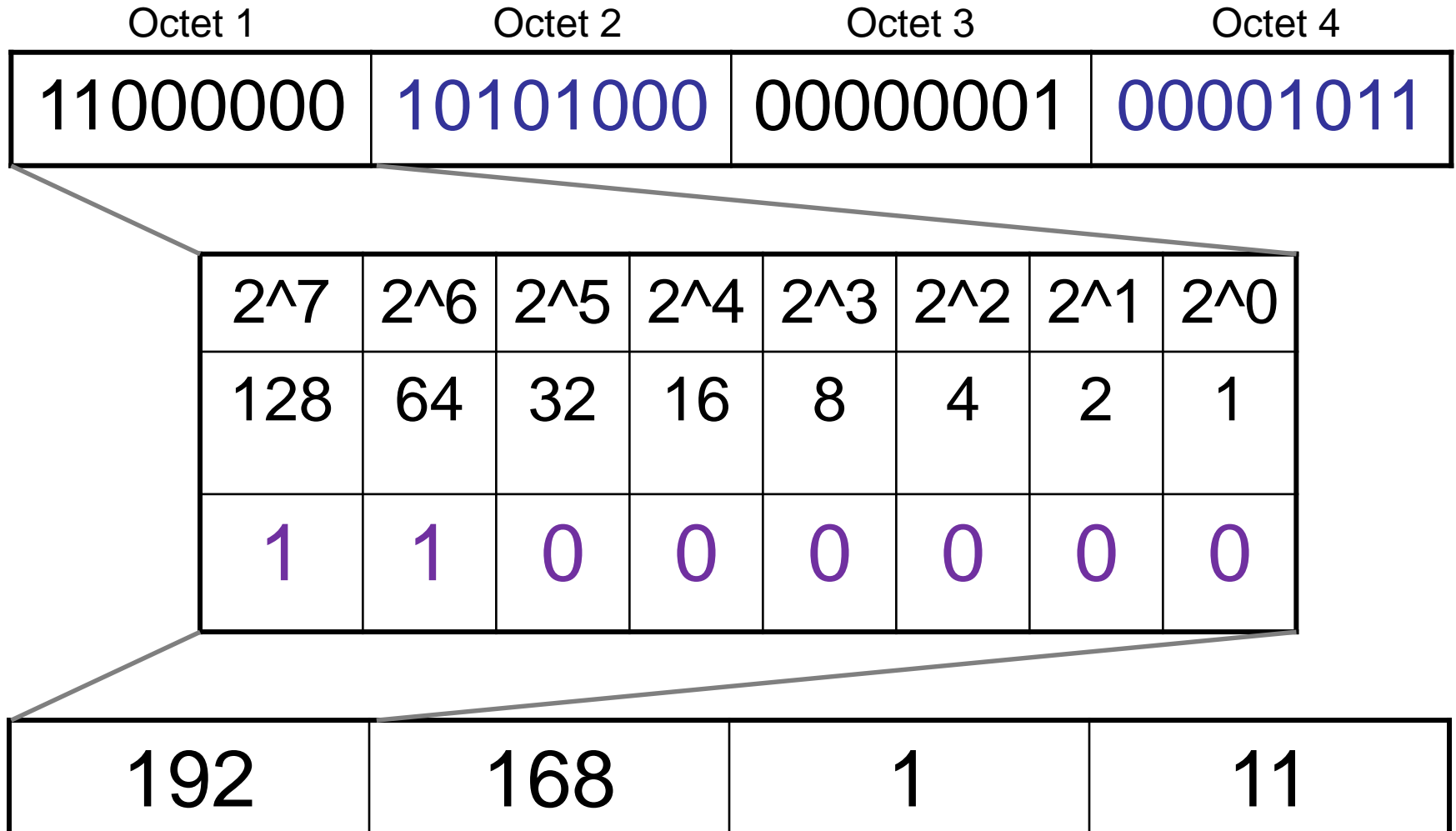
Elle est représentée dans le format décimal et chaque bloc est séparé par un point.

192.168.1.11

L'adresse est composée de deux parties, la partie réseau et la partie hôte

192	168	1	11
Réseau			Hôte

8.1.1.3 Conversion d'une adresse binaire en adresse décimale



8.1.1.5 Conversion de nombres décimaux en nombres binaires

Octet 1	Octet 2	Octet 3	Octet 4
192	168	1	11

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

11000000	10101000	00000001	00001011
----------	----------	----------	----------

8.1.2 Masque de sous-réseau IPv4

8.1.2.1 Partie réseau et partie hôte d'une adresse IPv4

Une adresse IPv4 :

192	168	1	11
Réseau			Hôte

Le masque de sous-réseau correspondant :

255	255	255	0
-----	-----	-----	---

8.1.2.2 Examen de la longueur du préfixe

Un ordinateur utilise un masque pour déterminer les portions réseau et hôte d'une adresse IP.

Un masque est un nombre binaire de 32 bits et a pour objectif de définir la structure d'une adresse IP, en représentant la partie hôte par des bits à 0 et la partie réseau par des 1.

Il existe deux formats de masques de sous-réseau :

- La notion décimale pointée
- La notion préfixée

Le préfixe réseau indique la longueur de la partie réseau soit le nombre de bits qui la compose, comme par exemple : / 24 .

C'est une manière différente d'exprimer le masque de sous-réseau

Un préfixe /24 correspond à un masque de sous-réseau de 255.255.255.0

8.1.2.3 Réseau, hôte et adresses de diffusion IPv4

8.1.2.4 Première et dernière adresses d'hôte

Il y a trois types d'adresses :

- Adresse réseau
- Adresse hôte
- Adresse de diffusion (broadcast)

L'adresse réseau fait référence au réseau. C'est la plus petite adresse de la plage. La partie hôte est constituée que de 0.

Les adresses d'hôtes sont les adresses attribuées aux périphériques finaux sur le réseau. Elles se situent entre l'adresse de réseau et de diffusion.

L'adresse de diffusion est utilisée pour envoyer les données à tous les hôtes du réseau. C'est la plus grande adresse de la plage. La partie hôte est constituée que de 1.

8.1.2.5 Opération AND au niveau du bit

8.1.2.6 Importance de l'opération AND

Le résultat de l'opération booléenne AND (ET) permet de trouver l'adresse réseau à partir d'une adresse IP et d'un masque de sous-réseau. Cette opération logique consiste à comparer deux bits et donne le résultat suivant :

$$1 \text{ AND } 1 = 1$$

$$1 \text{ AND } 0 = 0$$

$$0 \text{ AND } 1 = 0$$

$$0 \text{ AND } 0 = 0$$

Un hôte source utilise l'opération AND pour déterminer si un paquet doit être envoyé directement à un hôte du réseau local ou dirigé vers la passerelle.

8.1.2.8 Conversion des adresses IPv4 en binaire

8.1.2.9 Utilisation de l'opération AND pour déterminer l'adresse réseau

192	168	1	36	/ 24
-----	-----	---	----	------

Adresse IP

Masque de sous-réseau

Opérateur AND et on trouve l'adresse réseau

11000000	10101000	00000001	00100100
11111111	11111111	11111111	00000000
-----	-----	-----	-----
11000000	10101000	00000001	00000000

8.1.2.8 Conversion des adresses IPv4 en binaire

8.1.2.9 Utilisation de l'opération AND pour déterminer l'adresse réseau

192	168	1	36	/ 24
255	255	255	0	
192	168	1	0	/ 24
réseau			hôte	

Adresse IP hôte : 192.168.1.36 /24

Adresse réseau: 192.168.1.0 /24

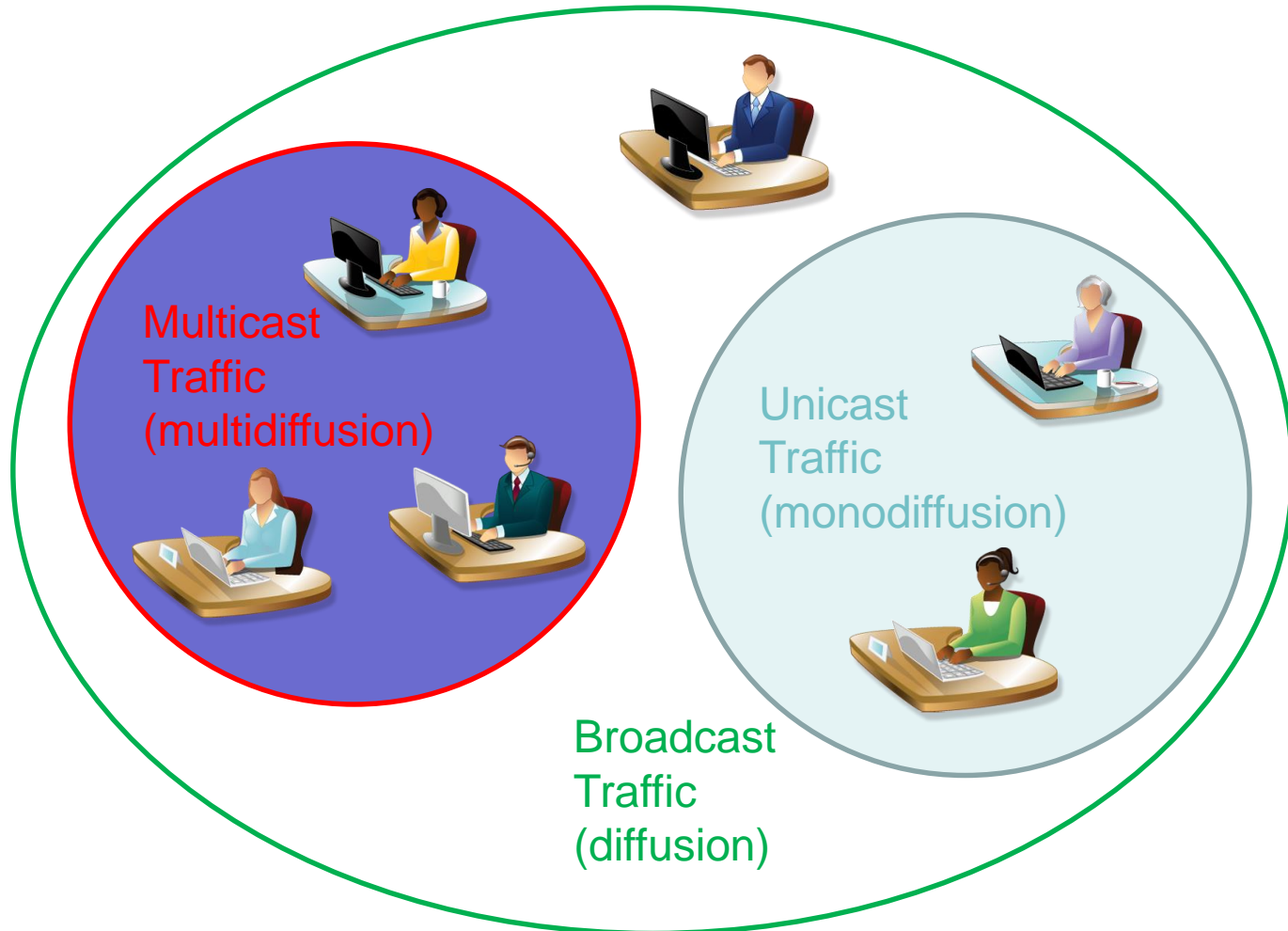
Adresse de diffusion: 192.168.1.255/24

8.1.3 Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion


8.1.3.3 Transmission monodiffusion

8.1.3.4 Transmission de diffusion

8.1.3.5 Transmission multidiffusion



8.1.3.7 Exercice – Calcul des adresses réseau, de diffusion et d'hôte

Exemple: 172.165.14.36 / **22** 

Adresse IP :	10101100	10100101	00001110	00100100
Masque :	11111111	11111111	11111100	00000000
Op AND :	10101100	10100101	00001100	00000000

On trouve l'adresse réseau : 172.165.12.0 / 22

Pour trouver l'adresse de diffusion on met tout les bits de la partie hôte à 1.

Diffusion:	10101100	10100101	00001111	11111111
------------	----------	----------	----------	----------

L'adresse de diffusion est : 172.165.15.255 / 22

Résumé : caractéristiques du réseau 172.165.12.0 / 22

Adresse réseau : 172.165.12.0

Adresse de diffusion : 172.165.15.255

Plage d'hôtes : 172.165.12.1 à 172.165.15.254

8.1.4 Les types d'adresses IPv4

8.1.4.1 Adresses IPv4 publiques et adresses IP privées

Chaque ordinateur connecté à l'Internet a besoin d'une adresse IP unique non dupliquée appelée adresse publique pour communiquer.

Les adresses privées sont un ensemble d'adresses destinées aux réseaux qui ne sont pas reliés à l'Internet et l'espace d'adressage privé est défini dans la RFC 1918.

Adresses privées

- Classe A : 10.0.0.0 à 10.255.255.255 (10.0.0.0 /8)
- Classe B : 172.16.0.0 à 172.31.255.255 (172.16.0.0 /12)
- Classe C : 192.168.0.0 à 192.168.255.255 (192.168.0.0 /16)

Note : Le routeur ou le périphérique pare-feu, en périphérie de ces réseaux privés, doivent bloquer ou traduire ces adresses.

La traduction d'une adresse privée en une adresse publique est effectuée par le protocole NAT (Network Address Translation)

8.1.4.3 Les adresses IPv4 réservées

Adresses spéciales

- Bouclage : 127.0.0.1
Il s'agit d'une adresse que les hôtes utilisent pour diriger le trafic vers eux-mêmes.
- Adresses link-local : 169.254.0.0/16
Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation
- Adresses TEST-NET : 192.0.2.0/24
Ce bloc d'adresses est réservé à des fins pédagogiques et peuvent être utilisées dans la documentation et dans des exemples de réseau.

8.1.4.4 L'ancien système d'adressage par classe

L'espaces d'adresses IPv4 a été subdivisés en cinq classes de la classe A à la classe E

Classe A : réseaux de grandes tailles
partie réseau : premier octet (8bits)
partie hôte : les trois octets suivants (24 bits)
le premier bit est toujours égal à 0
masque de sous-réseau : 255.0.0.0
préfixe : /8



Classe B : réseaux de tailles moyennes
partie réseau : deux premiers octets (16bits)
partie hôte : les deux octets suivants (16bits)
les deux premiers bits sont toujours égaux à 10
masque de sous-réseau : 255.255.0.0
préfixe : /16

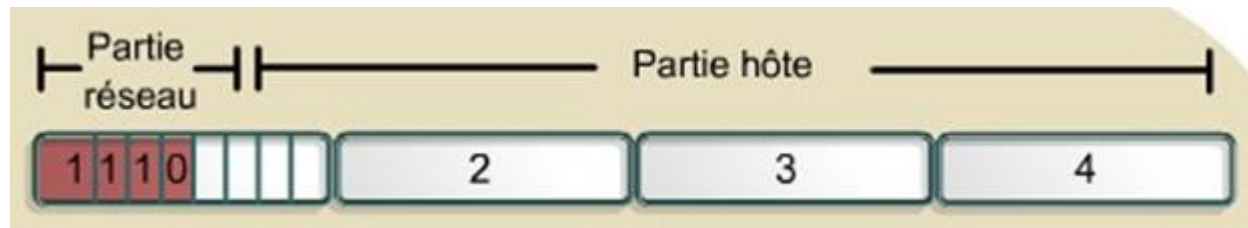


8.1.4.4 L'ancien système d'adressage par classe

Classe C : réseaux de petites tailles
partie réseau : trois premiers octets (24bits)
partie hôte : le dernier octet (8 bits)
les deux premiers bits sont toujours égaux à 110
masque de sous-réseau : 255.255.255.0
préfixe : /24

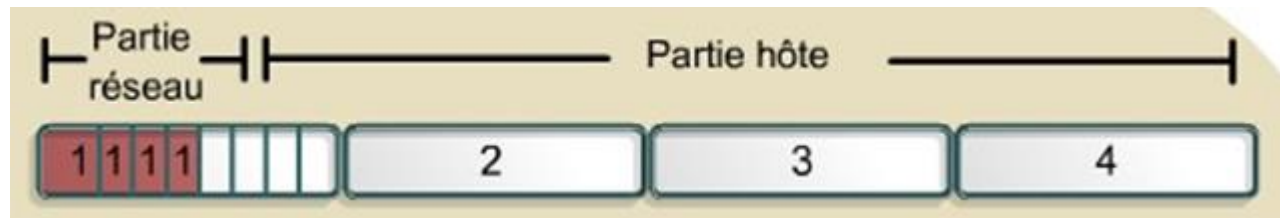


Classe D : adresses de multidiffusion (multicast)
partie réseau : les quatre premiers bits
partie hôte : le reste (28 bits)
les quatre premiers bits correspondent à 1110



8.1.4.4 L'ancien système d'adressage par classe

Classe E : adresses expérimentales utilisées pour la recherche
partie réseau : les quatre premiers bits
partie hôte : le reste (28 bits)
les quatre premiers bits correspondent à 1111



Adressage sans classe

Le système utilisé aujourd'hui porte le nom d'adressage sans classe. Son nom formel est le routage CIDR (Classless Inter-Domain Routing, routage interdomaine sans classe).

8.1.4.4 L'ancien système d'adressage par classe

Classe d'adresses IP	Plage d'adresses IP (premier octet)
Classe A	1-126 (00000001-01111110) *
Classe B :	128-191 (10000000-10111111)
Classe C	192-223 (11000000-11011111)
Classe D	224-239 (11100000-11101111)
Classe E	240-255 (11110000-11111111)

Classe de l'adresse	Nombre de réseaux	Nombre d'hôtes par réseau
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (multicast)	S.O.	S.O.

8.1.4.5 L'attribution des adresses IP

La stratégie d'affectation des adresses IPv6 peut être résumée comme suit :

- Les adresses publiques IPv6 sont groupées numériquement suivant les principes de zones géographiques
 - Dans chaque zone géographique, l'espace d'adressage est subdivisé suivant les FAI
 - Enfin, l'espace adressable de chaque FAI est à nouveau subdivisé suivants les clients
-
- L'Internet Corporation for Assigned Network Numbers (ICANN) est responsable de la gestion du processus d'affectation des adresses IP.
 - Elle affecte un ou plusieurs blocs d'adresses IPv6 à chaque RIR (Regional Internet Registry)
 - Les cinq RIR connus subdivisent leur espace adressable en plus petits blocs et assignent des préfixes au FAI et à d'autres RIR, dépendant d'eux.
 - Les FAI sont regroupés hiérarchiquement et affectent des blocs d'adresses encore plus petit à leurs clients.

8.1.4.5 L'attribution des adresses IP

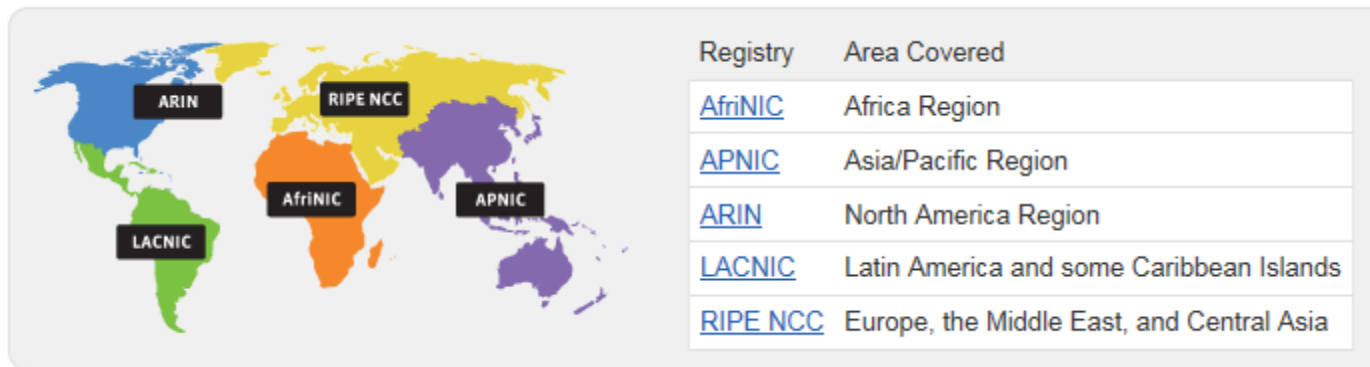
Extrait plages attribuées à RIPE

Prefix	Designation	Date	Whois	Status
2001:0000::/23	IANA	1999-07-01	whois.iana.org	ALLOCATED
2001:0600::/23	RIPE NCC	1999-07-01	whois.ripe.net	ALLOCATED
2001:0800::/23	RIPE NCC	2002-05-02	whois.ripe.net	ALLOCATED
2001:0A00::/23	RIPE NCC	2002-11-02	whois.ripe.net	ALLOCATED
2001:1400::/23	RIPE NCC	2003-02-01	whois.ripe.net	ALLOCATED
2001:1600::/23	RIPE NCC	2003-07-01	whois.ripe.net	ALLOCATED
2001:1A00::/23	RIPE NCC	2004-01-01	whois.ripe.net	ALLOCATED
2001:1C00::/22	RIPE NCC	2001-05-04	whois.ripe.net	ALLOCATED
2001:2000::/20	RIPE NCC	2001-05-04	whois.ripe.net	ALLOCATED
2001:3000::/21	RIPE NCC	2001-05-04	whois.ripe.net	ALLOCATED
2001:3800::/22	RIPE NCC	2001-05-04	whois.ripe.net	ALLOCATED
2001:4000::/23	RIPE NCC	2004-06-11	whois.ripe.net	ALLOCATED
2001:4600::/23	RIPE NCC	2004-08-17	whois.ripe.net	ALLOCATED
2001:4A00::/23	RIPE NCC	2004-10-15	whois.ripe.net	ALLOCATED
2001:4C00::/23	RIPE NCC	2004-12-17	whois.ripe.net	ALLOCATED
2001:5000::/20	RIPE NCC	2004-09-10	whois.ripe.net	ALLOCATED

<http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.txt>

8.1.4.5 L'attribution des adresses IP

Prefix	Designation	Date	Whois	Status
2002:0000::/16	6to4	2001-02-01		ALLOCATED
2003:0000::/18	RIPE NCC	2005-01-12	whois.ripe.net	ALLOCATED
2400:0000::/12	APNIC	2006-10-03	whois.apnic.net	ALLOCATED
2600:0000::/12	ARIN	2006-10-03	whois.arin.net	ALLOCATED
2610:0000::/23	ARIN	2005-11-17	whois.arin.net	ALLOCATED
2620:0000::/23	ARIN	2006-09-12	whois.arin.net	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	ALLOCATED
2A00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	ALLOCATED
2C00:0000::/12	AfriNIC	2006-10-03	whois.afrinic.net	ALLOCATED
2D00:0000::/8	IANA	1999-07-01		RESERVED
2E00:0000::/7	IANA	1999-07-01		RESERVED
3000:0000::/4	IANA 1999-07-01			RESERVED



Création de sous-réseaux

La création des sous-réseaux permet de créer plusieurs réseaux logiques à partir d'un seul bloc d'adresses.

Les sous-réseaux sont créés au moyen d'un ou plusieurs bits d'hôte en tant que bits réseau (emprunts).

Formule de calcul des sous-réseaux

2^n où n = le nombre de bits empruntés dans la partie hôte

Exemple : en empruntant 2 bits, on peut définir 4 sous-réseaux

Formule de calcul du nombre d'hôtes utilisables

$2^m - 2$ où m = le nombre de bits restants dans la partie hôte

L'étape suivante consistera au découpage d'un sous-réseau, ce qui reviendra à utiliser des masques de sous-réseau de longueur variable VLSM (Variable Length Subnet Mask), permettant ainsi d'optimiser l'efficacité de l'adressage.

S1, Maîtrise de l'ordinateur
Unité de module 631-2
Introduction aux réseaux

Initiation aux réseaux

Chapitre 8. Adressage IP

8.1 Adresses réseau IPv4

8.2 Les adresses réseau IPv6

8.3 Vérification de la connectivité

8.2 Les adresses réseau IPv6

8.2.1 Les problèmes liés au protocole IPv4

8.2.1.1 Ce qui rend IPV6 nécessaire

Les raisons du passage à IPv6

Le pool des nombres diminue pour les raisons suivantes :

- Croissance de la population
- Utilisateurs mobiles
- Transport
- Électronique grand public

L'internet que nous connaissions est entrain d'évoluer vers l'Internet des objets. Aujourd'hui, par exemple, les automobiles sont aussi connectées

8.2.1.2 La coexistence des protocoles IPv4 et IPv6

Plusieurs mécanismes de transition sont disponibles :

- **Double pile**

La double pile permet la coexistence d'IPv4 et d'IPv6

- **Le Tunneling**

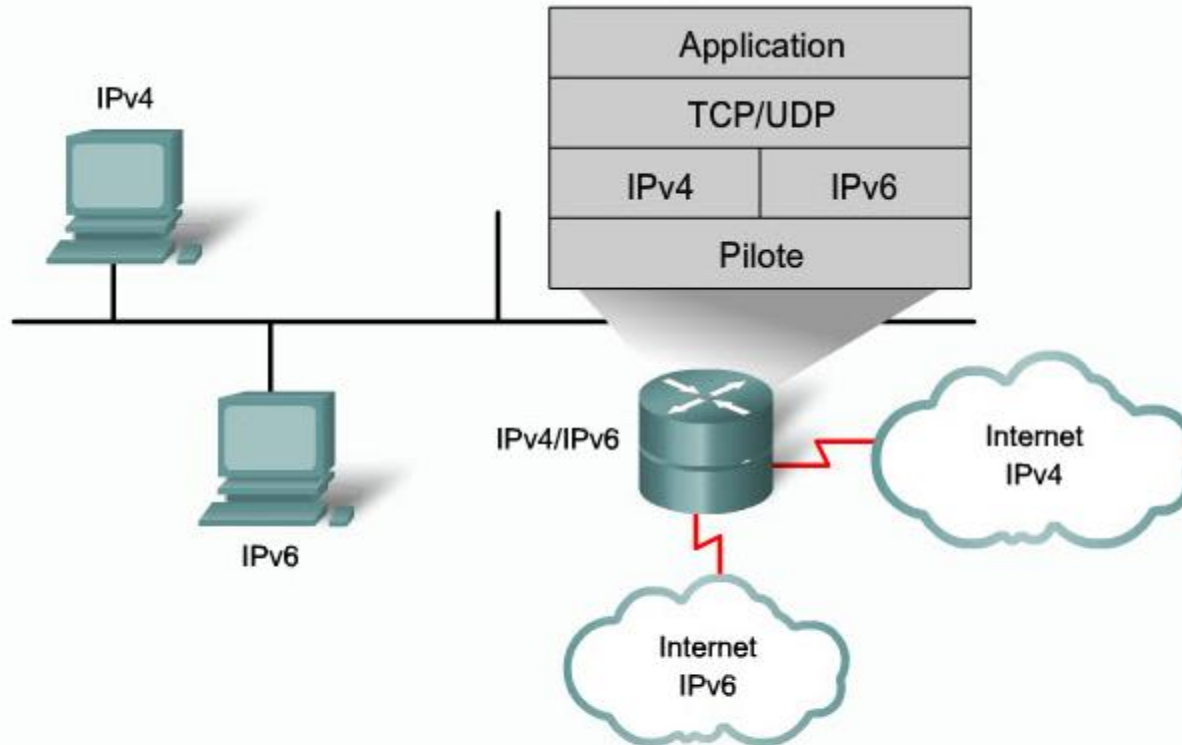
Les paquets IPV6 sont encapsulés dans des paquets IPv4

Il existe plusieurs possibilités de tunnels comme le tunnel manuel, le tunnel 6to4 (Préfixe : 2002::/16), le tunnel ISATAP ou le Tunnel Teredo (Préfixe : 2001:0000::/32)

- **La traduction**

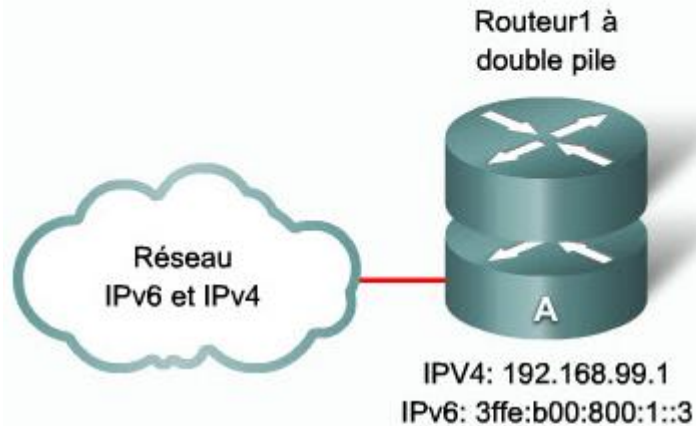
Similaire à la traduction NAT IPv4, vous allez traduire des adresses sources IPV6 en adresses source IPv4

8.2.1.2 La coexistence des protocoles IPv4 et IPv6



Le mode double pile est une méthode d'intégration dans laquelle un nœud a une mise en œuvre et une connectivité à un réseau IPv4 et IPv6.

8.2.1.2 La coexistence des protocoles IPv4 et IPv6

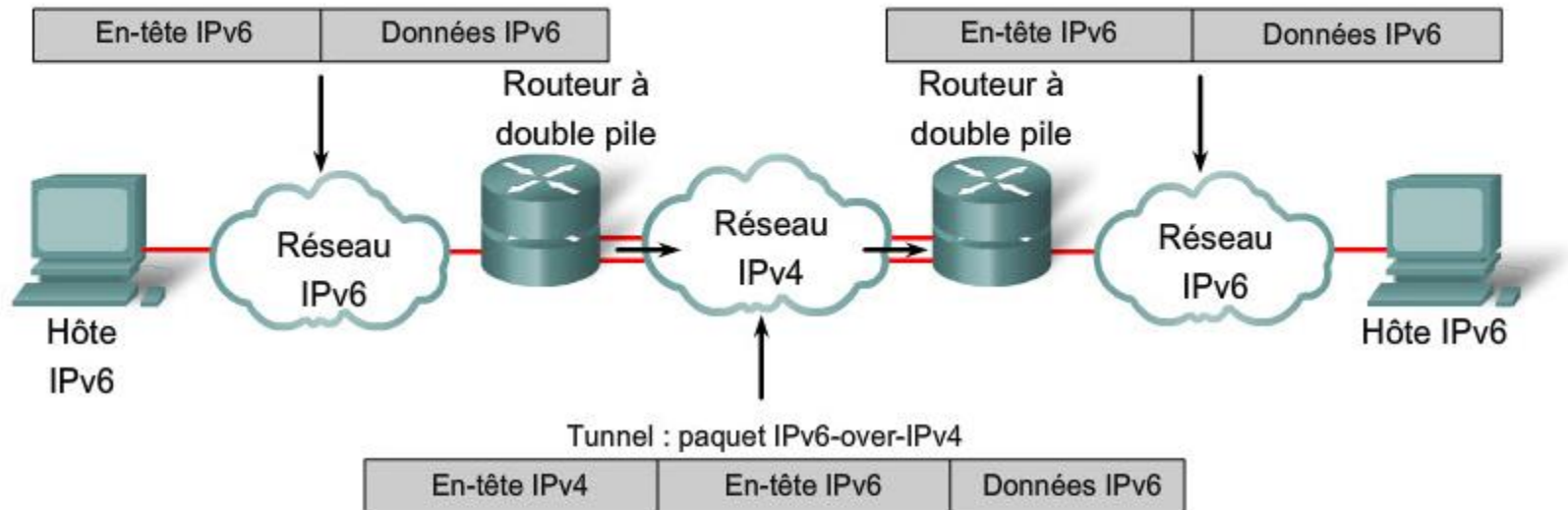


```
conf t
ipv6 unicast-routing

interface ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 3ffe:b00:c18:1::3/127
```

Lorsque IPv4 et IPv6 sont tous deux configurés sur une interface, l'interface est considérée comme à double pile.

8.2.1.2 La coexistence des protocoles IPv4 et IPv6

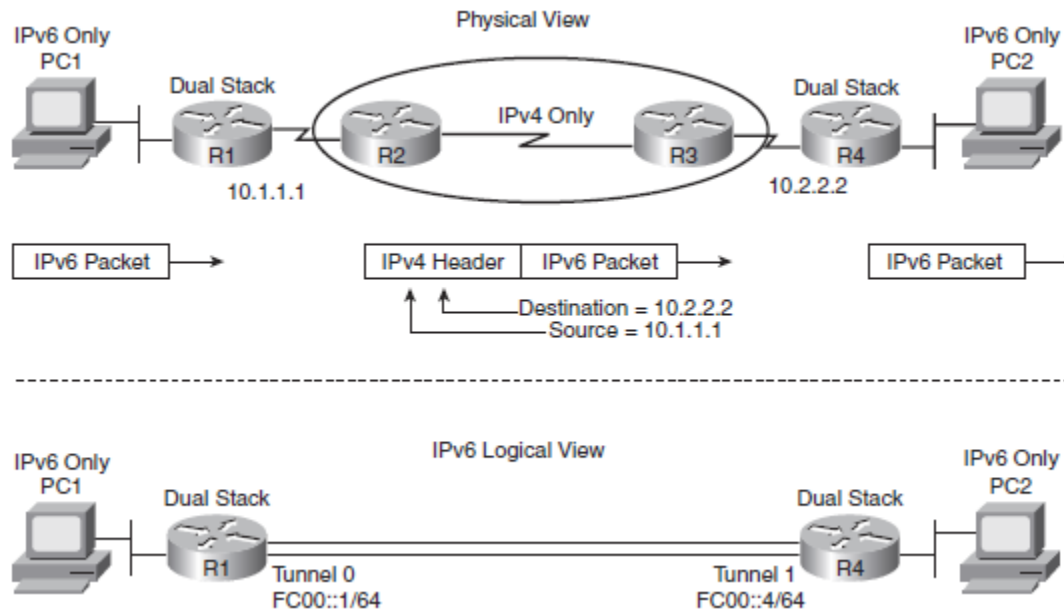


La transmission tunnel est une méthode d'intégration dans laquelle un paquet IPv6 est encapsulé dans un autre protocole, par exemple IPv4. Cette méthode d'encapsulation :

- comprend un en-tête IPv4 de 20 octets sans options, un en-tête IPv6 et des données utiles ;
- nécessite des routeurs à double pile.

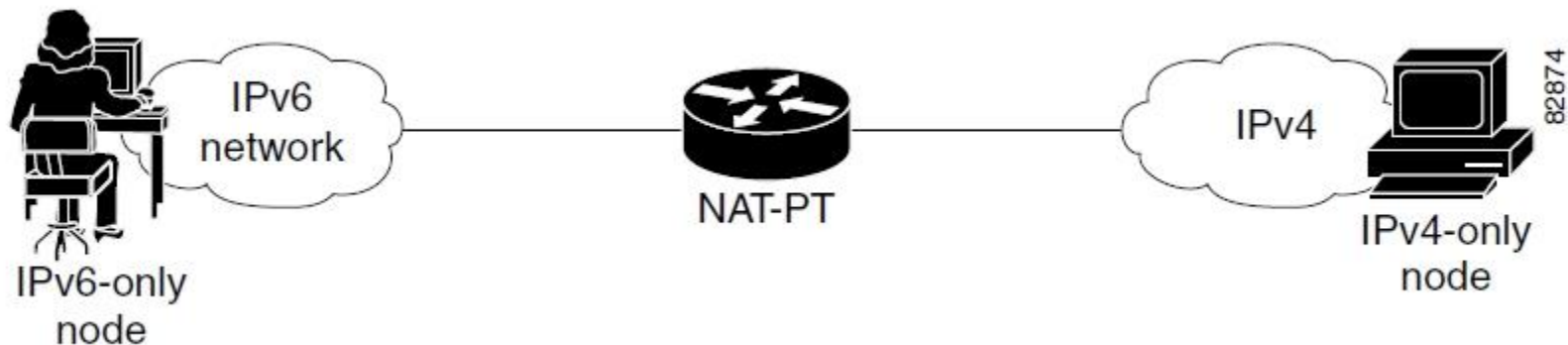
8.2.1.2 La coexistence des protocoles IPv4 et IPv6

Il en existe plusieurs types mais, ici le tunnel prend un paquet IPv6 envoyé par l'hôte et l'encapsule dans un paquet IPv4. Celui-ci est alors envoyé sur un réseau IPv4 existant et à l'arrivée, le destinataire le décapsule pour restituer le paquet IPv6 original. Le concept ressemble à un tunnel VPN.



8.2.1.2 La coexistence des protocoles IPv4 et IPv6

La version 12.3(2)T de Cisco IOS et les versions ultérieures (avec le jeu de fonctions approprié) comprennent également NAT-PT entre IPv6 et IPv4. Cette traduction permet aux hôtes qui utilisent différentes versions du protocole IP de communiquer directement. Ces traductions sont plus complexes que la fonction NAT d'IPv4. À l'heure actuelle, cette méthode de traduction constitue l'option la moins favorable et ne doit être utilisée qu'en dernier recours.



8.2.2 Adressage IPv6

8.2.2.2 Représentation de l'adresse IPv6

Une adresse IPv6 est une valeur binaire longue de 128 bits, pouvant être affichée sous forme d'écriture hexadécimale à 32 chiffres.

IPv6 : 16 octets
11010001.11011100.11001001.01110001.11011100. 11001100.01110001.11010001.11011100.11001001. 11010001.11011100.11001001.01110001
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73
3,4 x 10 ³⁸ adresses IP

L'écriture d'une adresse IPv6 à l'aide des 32 caractères s'appelle le format privilégié

8.2.2.3 Règle n°1 – Omettre les zéros en début de segment

❑ Dans un champ, les zéros de tête sont facultatifs.

Par exemple : le champ 09C0 est équivalent à 9C0
 le champ 0000 est équivalent à 0.

2031 : 0000 : 130F : 0000 : 0000 : 09C0 : 876A : 130B

Evolue en :

2031 : 0 : 130F : 0000 : 0000 : 9C0 : 876A : 130B

8.2.2.4 Règle n°2 – Omettre les séquences composées uniquement de zéros

❑ Des champs successifs de zéros peuvent être représentés comme deux signes deux-points (::)

Restriction : vous ne pouvez cependant utiliser cette abréviation qu'une seule fois dans une même adresse.

2031: 0:130F:0000:0000: 9C0:876A:130B

2031: 0:130F: : 9C0:876A:130B

au final : 2031:0:130F::9C0:876A:130B

❑ Une adresse indéterminée est écrite comme ceci : « :: ». En effet, elle ne contient que des zéros.

8.2.3 Les types d'adresses IPv6

8.2.3.1 Types d'adresses IPv6

IPv6 prend en charge trois types d'adresses :

Monodiffusion

Une adresse de monodiffusion identifie une interface unique dans l'étendue du type d'adresse de monodiffusion. Avec la topologie de routage de monodiffusion appropriée, les paquets adressés à une adresse de monodiffusion sont remis à une seule interface. Pour s'adapter aux systèmes à équilibrage de la charge, la RFC 3513 autorise plusieurs interfaces à utiliser la même adresse du moment qu'elles apparaissent en tant qu'interface unique pour l'implémentation IPv6 sur l'hôte.

Multidiffusion

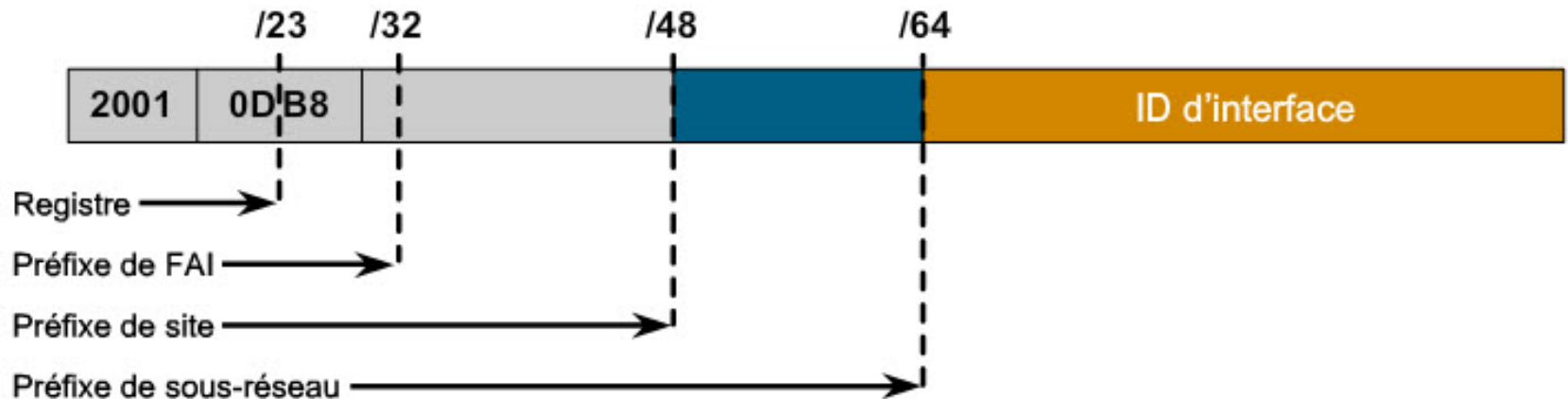
Une adresse de multidiffusion identifie plusieurs interfaces. Avec la topologie de routage de multidiffusion appropriée, les paquets adressés à une adresse de multidiffusion sont remis à toutes les interfaces identifiées par l'adresse. Une adresse de multidiffusion est utilisée pour la communication un-à-plusieurs, avec la remise à plusieurs interfaces.

Anycast

Une adresse anycast identifie plusieurs interfaces. Avec la topologie de routage appropriée, les paquets adressés à une adresse anycast sont remis à une seule interface, la plus proche identifiée par l'adresse. Il s'agit de l'interface la plus proche en terme de distance de routage. Une adresse anycast est utilisée pour la communication un-à-un-sur plusieurs, avec la remise à une seule interface.

8.2.3.2 Longueur de préfixe IPv6

La longueur du préfixe peut aller de 0 à 128. La grandeur standard est /64 cela veut dire que la partie hôte (ID d'interface) est également de 64 bits



8.2.3.3 Les adresses de monodiffusion globale IPv6

Il existe six types d'adresse de monodiffusion IPv6 :

Adresse de monodiffusion globale IPv6 (Global unicast, 2000::/3)

- Ces adresses sont similaires aux adresses publiques IPv4

Adresse de monodiffusion de liaison locale (Link-Local, fe80::/10)

- Ces adresses se retrouvent uniquement sur votre réseau local et ne sont pas routable

Adresse de bouclage (Loopback, ::1/128 ou ::1)

- Cette adresse est utilisée par un hôte pour s'envoyer un paquet à lui-même

Adresse indéterminée ou non spécifiée (Unspecified, ::/128)

- Cette adresse est utilisée lorsqu'un hôte ne possède pas encore son adresse

Adresse locale unique, RFC 1918 (ULAs, fc00::/7)

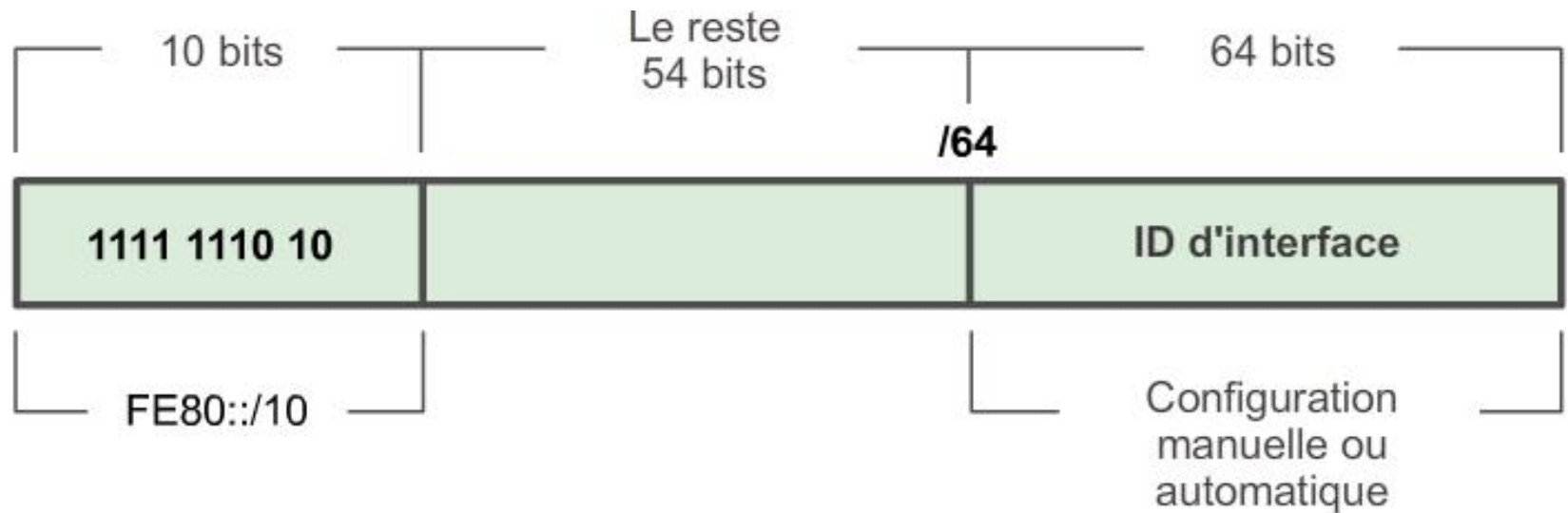
- Ces adresses ressemblent aux adresses privées IPv4 et ne doivent être routées sur le réseau global (public) IPv6

Adresse IPv4 intégré (IPv4-Mapped, ::ffff/96)

- Ces adresses sont utilisées pour faciliter la transition IPv4 vers IPv6

8.2.3.4 Les adresses de monodiffusion link-local IPv6

Chaque interface réseau IPv6 doit avoir une adresse link-local



8.2.4 Les adresses de monodiffusion globale IPv6

8.2.4.1 La structure d'une adresse de monodiffusion globale IPv6

Les adresses de monodiffusion globales comprennent généralement un préfixe de routage global de 48 bits et un ID de sous-réseau de 16 bits.

An example of the resulting format of global unicast address under the 2000::/3 prefix that is currently being delegated by the IANA and consistent with the recommendations in [RFC 3177](#) is:

3	45 bits	16 bits	64 bits
001	global routing prefix	subnet ID	interface ID

L'adresse de monodiffusion globale actuelle qui est attribuée par l'IANA utilise la plage d'adresses qui commence par la valeur binaire 001 (2000::/3)

2000::/3

2000:0000:0000:0000:0000:0000:0000:0000/3

L'IANA alloue l'espace d'adressage IPv6 dans les plages de [2001::/16](#) aux cinq organismes d'enregistrement Internet locaux (ARIN, RIPE, APNIC, LACNIC et AfriNIC). L'adresse 2001:DB8::/32 a été réservée à des fins de documentations.

Adressage IPv6

Vous pouvez attribuer un ID d'adresse IPv6 de façon statique ou dynamique :

- a) Attribution statique à l'aide d'un ID d'interface manuel
- b) Attribution statique à l'aide d'un ID d'interface EUI-64
- c) Configuration automatique sans état
- d) DHCP pour IPv6 (DHCPv6)

8.2.4.2 La configuration statique d'une adresse de monodiffusion globale

Vous pouvez attribuer un ID d'adresse IPv6 à une interface de façon statique :

- a) A l'aide d'un ID d'interface manuel

Commande: **ipv6 address** *adresse-ipv6* [/longueur-préfixe]

Exemple :

RouterX(config)# interface gigabitethernet 0/0

RouterX(config-if)# ipv6 address 2001:DB8:2222:7272::72/64

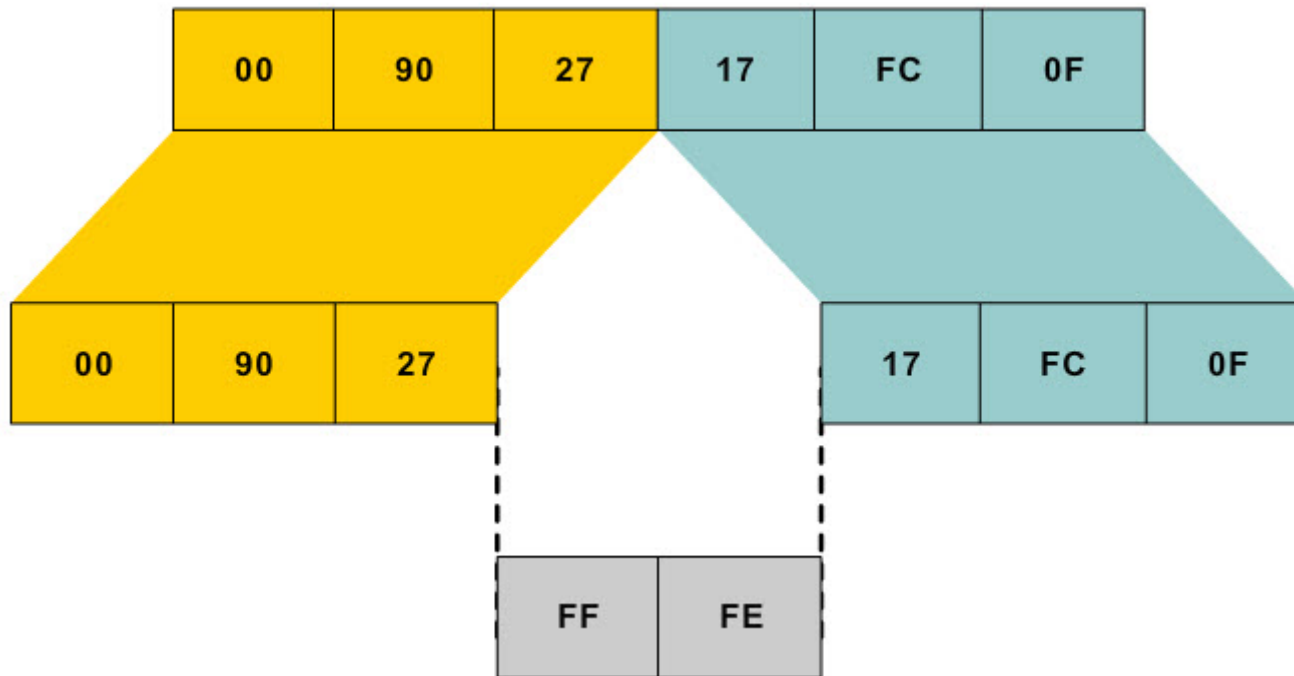
RouterX(config-if)# no shutdown

8.2.4.2 La configuration statique d'une adresse de monodiffusion globale

- b) A l'aide d'un ID d'interface EUI-64

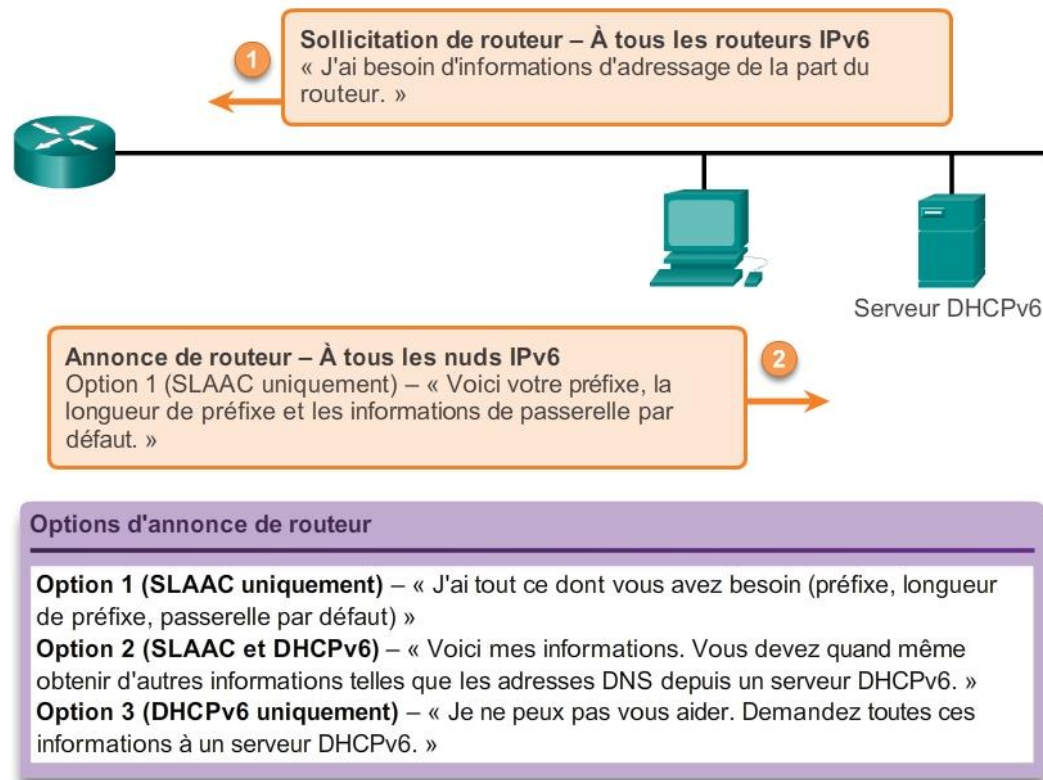
Commande : **ipv6 address** *préfixe-ipv6/longueur-préfixe* eui-64

RouterX(config-if)#ipv6 address 2001:DB8:2222:7272::**64** eui-64

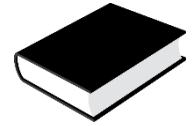


8.2.4.3 La configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

La configuration automatique des adresses sans état (SLAAC) est une méthode permettant à un périphérique d'obtenir son préfixe, la longueur de préfixe, et l'adresse de la passerelle par défaut depuis un routeur IPv6, sans l'intervention d'un serveur DHCPv6.



Adressage IPv6

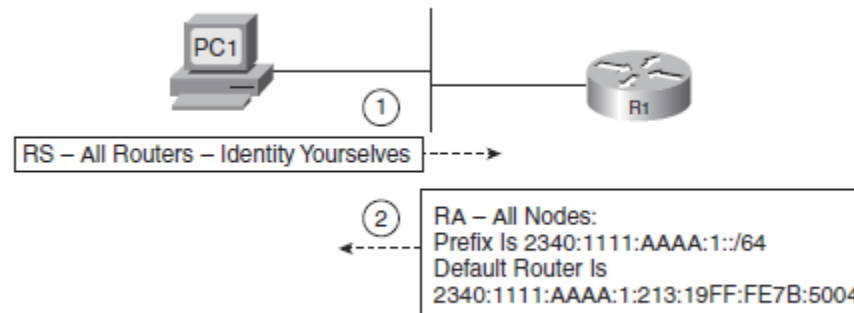


c) Vous pouvez attribuer un ID d'adresse IPv6 de façon dynamique :

■ Configuration automatique sans état

Avec l'auto-configuration sans état, un hôte apprend dynamiquement le préfixe /64 utilisé par les sous-réseaux et calcule le reste de son adresse en utilisant l'ID d'interface au format EUI-64 de l'adresse MAC de sa carte réseau. Il utilise une des nombreuses fonctionnalités du protocole de découverte des voisins, *Neighbor Discovery Protocol* (NDP) d'IPv6, pour trouver le préfixe utilisé sur le LAN. L'auto-configuration sans état utilise deux messages NDP :

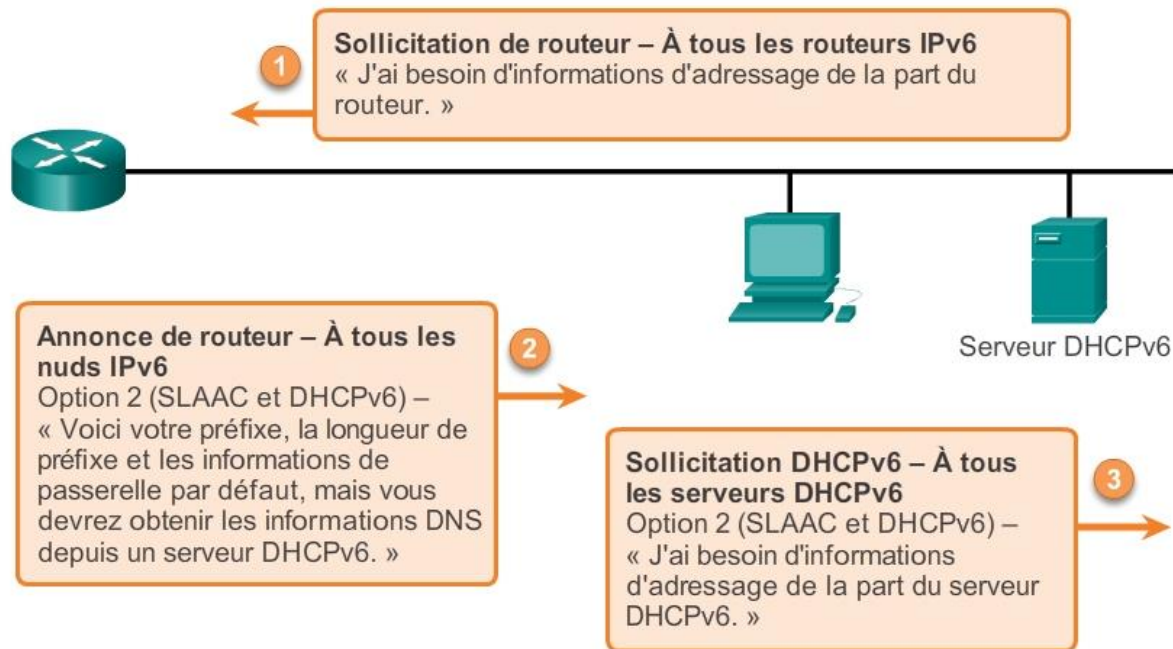
- ☐ Sollicitation de routeur, ou Router Solicitation (RS) [FF02::2]
- ☐ Annonce de routeur, ou Router Advertisement (RA) [FF02::1]



Note : L'auto-configuration sans états ne permet pas de récupérer l'adresse IP du serveur DNS ni le nom de domaine.

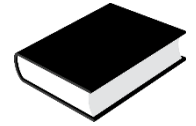
8.2.4.4 La configuration dynamique d'une adresse de monodiffusion globale avec la méthode DHCPv6

L'IPv6 permet à plusieurs adresses IPV6, appartenant au même réseau, d'être configurées sur la même interface, ceci de façon statique ou dynamique



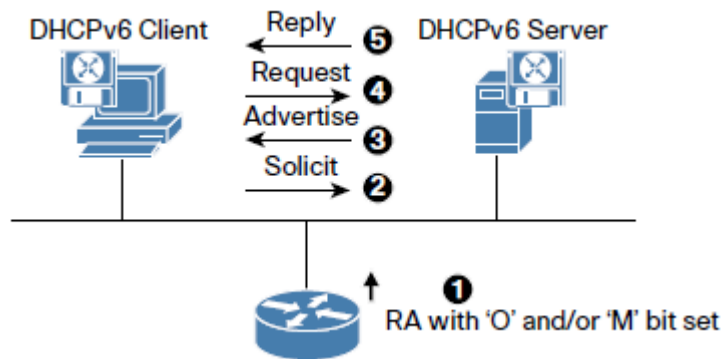
Remarque : une annonce de routeur avec l'option 3 (DHCPv6 uniquement) nécessite que le client obtienne toutes les informations à partir du serveur DHCPv6.

Adressage IPv6



d) Vous pouvez attribuer un ID d'adresse IPv6 de façon dynamique :

- DHCP pour IPv6 (DHCPv6)



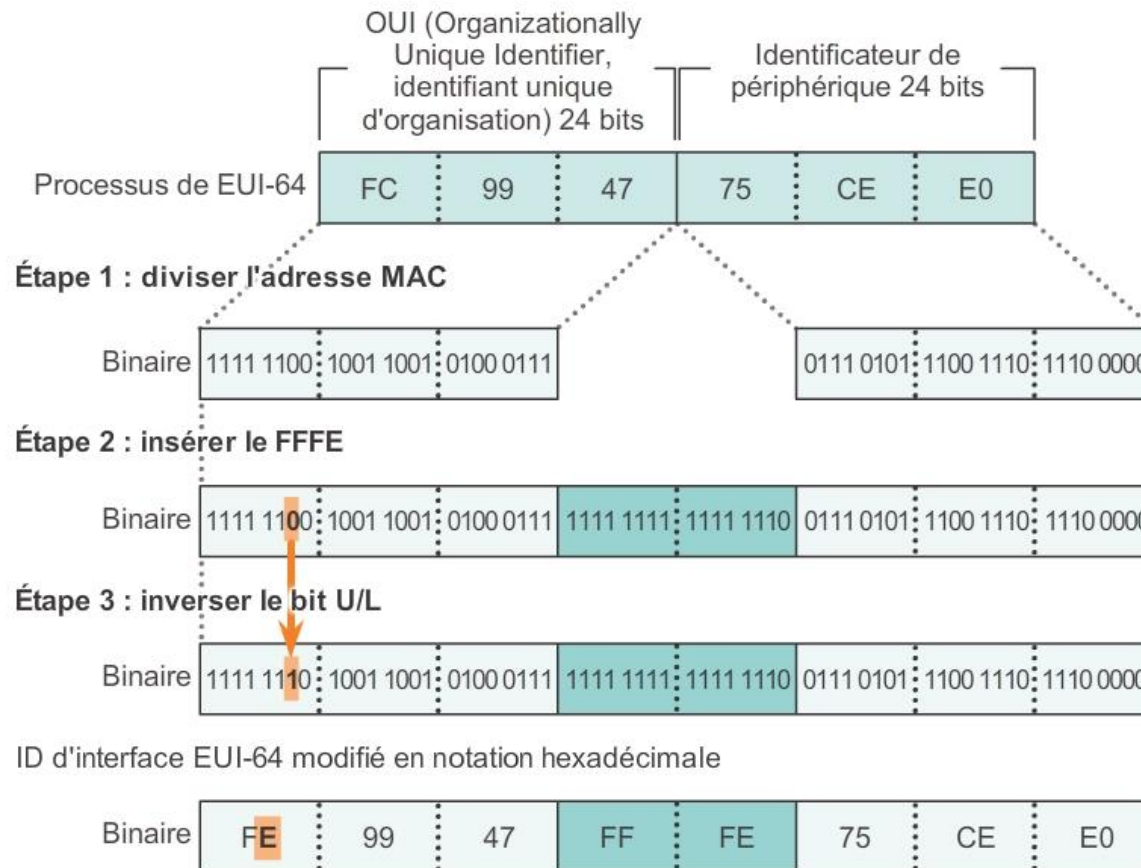
DHCPv6 Message Type	DHCPv4 Message Type
SOLICIT (1)	DHCPDISCOVER
ADVERTISE (2)	DHCPOFFER
REQUEST (3), RENEW (5), REBIND (6)	DHCPREQUEST
REPLY (7)	DHCPACK/DHCPNAK
RELEASE (8)	DHCPRELEASE
INFORMATION-REQUEST (11)	DHCPINFORM
DECLINE (9)	DHCPDECLINE
CONFIRM (4)	none
RECONFIGURE (10)	DHCPFORCERENEW
RELAY-FORW (12), RELAY-REPLY (13)	none

Advertisement (RA) available for this purpose:

- 'O' bit—When this bit is set, the client can use DHCPv6 to retrieve Other configuration parameters (ie: DNS addresses)
- 'M' bit—When this bit is set, the client may use DHCPv6 to retrieve a Managed IPv6 address from a DHCPv6 server

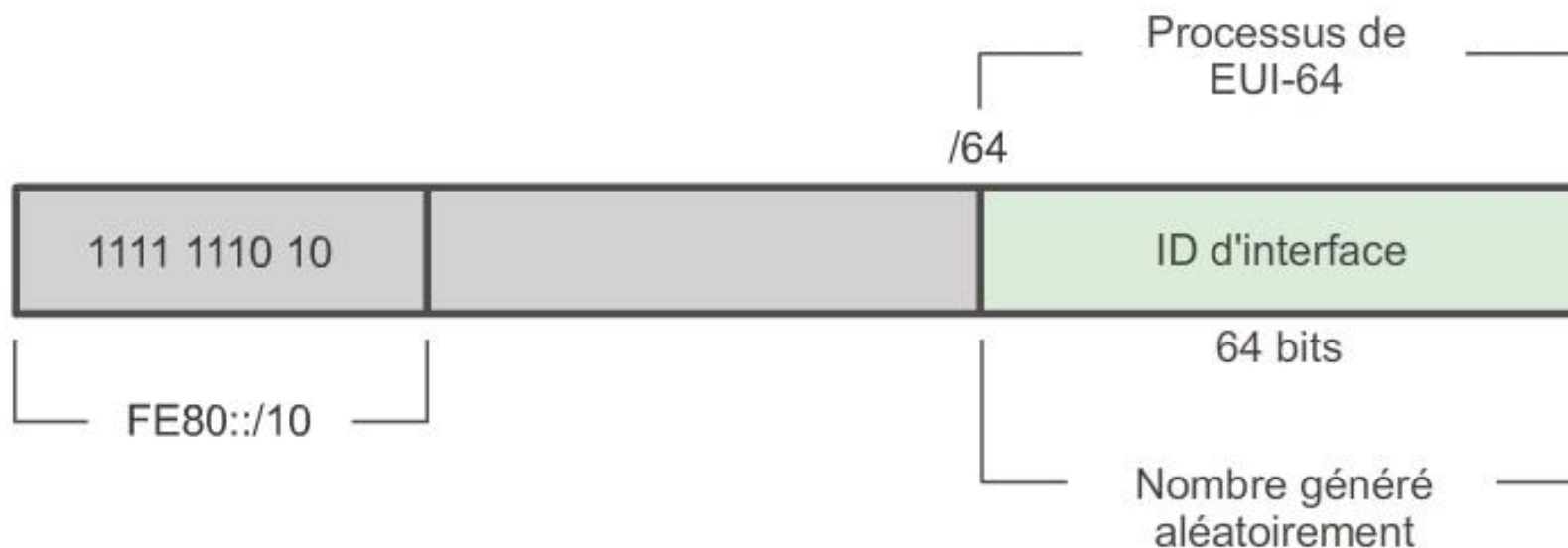
8.2.4.5 La génération aléatoire ou à l'aide de la méthode EUI-64

L'EUI (Extended Unique Identifier), ou format EUI-64 modifié utilise l'adresse MAC d'un client et insère 16 autres bits au milieu, avec une modification du bit U/L au passage, pour créer l'ID interface



8.2.4.6 Les adresses link-local dynamiques

Une fois qu'une adresse de monodiffusion globale est attribuée à une interface, le périphérique IPv6 génère automatiquement son adresse link-local. Elles servent comme passerelle par défaut, lors de l'échange des mises à jour de routage, comme adresse IP de saut suivant dans une table de routage



8.2.4.7 Adresses Link-Local statiques

Configuration d'une adresse de lien local de façon statique :

Exemple :

```
RouterX(config)# interface gigabitethernet 0/0
```

```
RouterX(config-if)# ipv6 address fe80::1 link-local
```

8.2.4.8 Vérifier la configuration des adresses IPv6

Pour vérifier vos configurations, vous adapterez les ordres bien connus en IPv4. Vous substituerez «IP» par «IPv6» dans la majorité des cas.

Ordres IPv4

```
show ip interface brief  
show ip route  
ping 192.168.1.1
```

Ordres IPv6

```
show ipv6 interface brief  
show ipv6 route  
ping 2001:db8:acad::11
```

8.2.5 Les adresses de multidiffusion IPv6

8.2.5.1 Les adresses de multidiffusion IPv6 attribuées

Les adresses de multidiffusion IPv6 ont le préfixe FF00::/8

Il existe deux types d'adresses de multidiffusion IPv6 :

Les adresses de multidiffusion attribuées

Elles sont réservées à des groupes ou périphériques prédéfinis

Les plus courants sont :

Groupe de multidiffusion à tous les nœuds FF02::1. Ces messages sont traités par tous les périphériques du réseau local

Groupe de multidiffusion à tous les routeurs FF02::2. Ces messages sont traités par tous les routeurs du réseau local

Les adresses de multidiffusion de nœud sollicité

8.2.5.2 Les adresses de multidiffusion IPv6 de nœud sollicité

Une adresse de multidiffusion de nœud sollicité IPv6 est créée automatiquement lorsque l'adresse de monodiffusion globale ou l'adresse link-local est attribuée.

L'adresse de multidiffusion de nœud sollicité comprend deux parties :

- Le préfixe de multidiffusion FF02:0:0:0:0:1:FF00::/104 : les 104 premiers bits de l'adresse de multidiffusion de nœud sollicité.
- Les 24 bits les moins significatifs : il s'agit des 24 derniers bits de l'adresse de multidiffusion de nœud sollicité. Ces bits sont copiés à partir des 24 derniers bits de l'adresse de monodiffusion globale ou de l'adresse de monodiffusion link-local du périphérique.

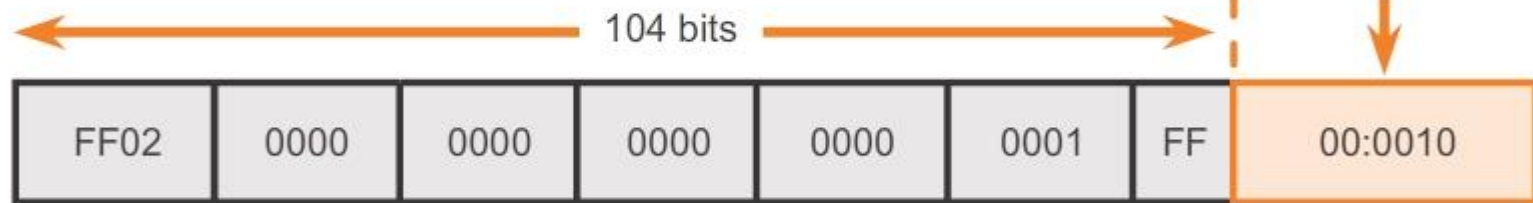
Elles sont semblables à une adresse de multidiffusion à tous les nœuds, mais seront traitées seulement par les périphériques ayant les 24 derniers bits identiques.

8.2.5.2 Les adresses de multidiffusion IPv6 de nœud sollicité

Adresse de monodiffusion globale



Adresses de multidiffusion de nud sollicité



Par copie

Adresse de monodiffusion globale IPv6 :
2001:0DB8:ACAD:0001:0000:0000:0000:0000:0010

Adresse de multidiffusion de nud sollicité IPv6 :
FF02::0:FF00:0010

S1, Maîtrise de l'ordinateur
Unité de module 631-2
Introduction aux réseaux

Initiation aux réseaux

Chapitre 8. Adressage IP

8.1 Adresses réseau IPv4

8.2 Les adresses réseau IPv6

8.3 Vérification de la connectivité

8.3 Vérification de la connectivité

8.3.1 ICMP

8.3.1.1 Les messages ICMPv4 et ICMPv6

La suite TCP/IP permet d'envoyer des messages, via les services du protocole ICMP, si certaines erreurs se produisent. Ces messages ont pour objectif de fournir des commentaires sur les problèmes liés au traitement de paquets IP dans certaines circonstances.

Les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants :

- Host confirmation (Confirmation de l'hôte)
- Destination or Service Unreachable (destination ou service inaccessible)
- Time exceeded (Délai dépassé)
- Route redirection (Redirection de la route)

8.3.1.2 Les messages de sollicitation et d'annonce de routeur ICMPv6

ICMPv6 inclut quatre nouveaux protocoles dans le cadre du protocole Neighbor Discovery Protocol (ND ou NDP) :

- Message de sollicitation de routeur
- Message d'annonce de routeur
- Message de sollicitation de voisin
- Message d'annonce de voisin

Messages de sollicitation de routeur

Lorsqu'un hôte est configuré pour obtenir ses informations d'adressage à l'aide de la configuration automatique des adresses sans état (SLAAC), celui-ci envoie un message de sollicitation au routeur.

Messages d'annonce de routeur

Ces messages sont envoyés par les routeurs pour fournir les informations d'adressage aux hôtes via la SLAAC

8.3.1.3 Les messages de sollicitation et d'annonce de voisin ICMPv6

Les messages de sollicitation de voisin et d'annonce de voisin sont utilisés pour :

- La résolution d'adresse
- La détection d'adresses en double (DAD)

Résolution d'adresse

La résolution d'adresse est utilisée lorsqu'un périphérique du réseau local (LAN) connaît l'adresse de monodiffusion IPv6 d'une destination, mais pas son adresse MAC Ethernet.

Pour déterminer l'adresse MAC de destination, le périphérique envoie un message de sollicitation de voisin à l'adresse du nœud sollicité.

Détection d'adresses en double

Pour vérifier le caractère unique d'une adresse, le périphérique envoie un message de sollicitation de voisin avec sa propre adresse IPv6 comme adresse IPv6 ciblée. Si cette adresse est attribuée à un autre périphérique du réseau, ce dernier répond en envoyant un message d'annonce de voisin.

8.3.2 Test et vérification

La commande **ping** (Packet Internet Groper) est un utilitaire qui permet de tester la connectivité IP entre des hôtes. Elle utilise un protocole de couche 3 qui fait partie de la suite de protocoles TCP/IP appelée ICMP (Internet Control Message Protocol).

Un message de requête écho ICMP Echo Request est envoyé vers une adresse IP de destination. Si l'hôte, à l'adresse spécifiée, reçoit cette demande, il répond par un message ICMP Echo Reply. Pour chaque paquet envoyé, la commande ping mesure la durée de réception de la réponse.

8.3.2.1 Ping - Tester la pile locale

Pour réaliser ce test, nous exécutons la commande ping sur l'adresse de bouclage locale 127.0.0.1. Une réponse indique que le protocole IP est correctement installé sur l'hôte.

8.3.2.2 Ping - Tester la connectivité au réseau local

Si cette requête ping aboutit, le fonctionnement d'une grande partie de l'interréseau peut être vérifié.

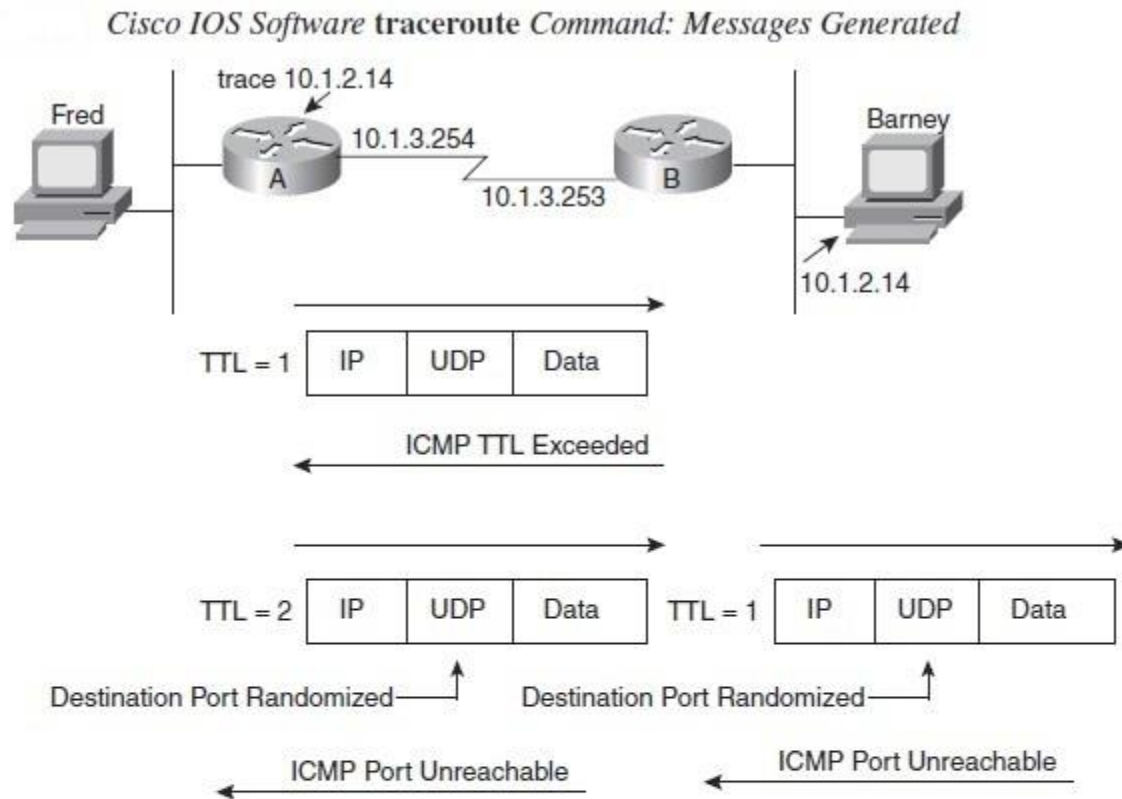
8.3.2.3 Ping - Tester la connectivité à distance

Une requête ping à la passerelle indique que l'hôte et l'interface du routeur qui sert de passerelle sont fonctionnels (ou non) sur le réseau local.

8.3.2.4 Traceroute - Tester le chemin

Le programme **Traceroute** (tracert sous windows) nous permet de visualiser la route empruntée par le datagramme IP d'une machine vers une autre. Il fait appel à la fonction du champ TTL (Time To Live) qui d'empêche les datagrammes de se perdre dans des boucles infinies. Lorsque un routeur reçoit un datagramme IP dont le champ TTL est à 1, il ne doit pas le transmettre.

8.3.2.4 Traceroute - Tester le chemin



Example 7-1 ICMP debug on Router B When Running the traceroute Command on Router A

```
RouterA#traceroute 10.1.2.14

Type escape sequence to abort.
Tracing the route to 10.1.2.14

 1 10.1.3.253 8 msec 4 msec 4 msec
 2 10.1.2.14 12 msec 8 msec 4 msec
RouterA#
```