2e partie : Adressage IP

Modules 11 - 13

AVIGNON UNIVERSITÉ

Module 11 : Adressage IPv4

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

Système binaire

192	168	10	10
11000000	10101000	00001010	00001010

192.168.10.10 est une adresse IP attribuée à un ordinateur.

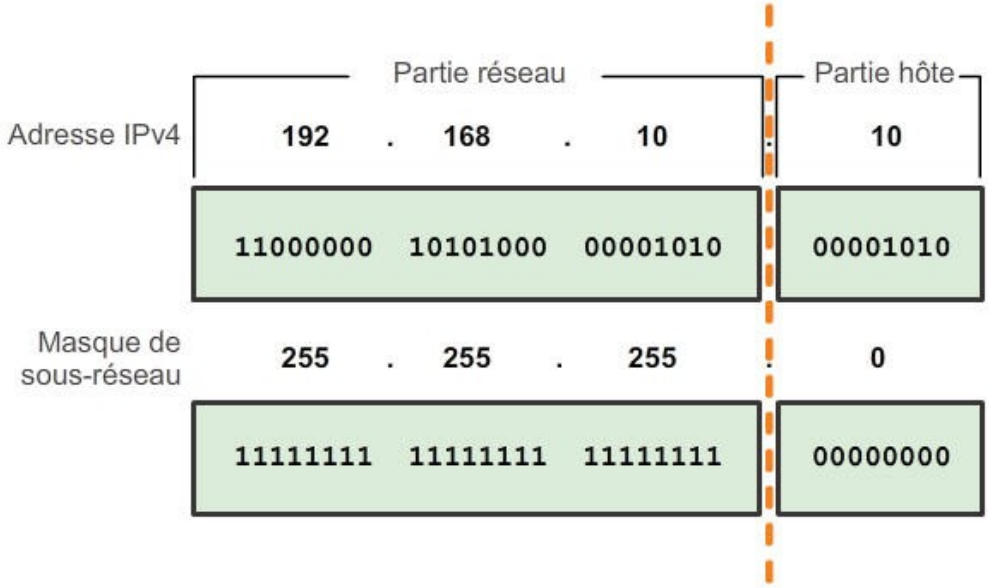
Adresse décimale | **Octets** | **Adresse 32 bits**

Base	2	2	2	2	2	2	2	2
Exposant	7	6	5	4	3	2	1	0
Valeurs des bits de l'octet	128	64	32	16	8	4	2	1
Adresse binaire	1	1	0	0	0	0	0	0
Valeurs binaires des bits	128	64	0	0	0	0	0	0

Ajouter les valeurs binaires des bits

128 + 64 = 192

La partie réseau et la partie hôte d'une adresse IPv4



- Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent un modèle 32 bits distinct appelé masque de sous-réseau
- Le masque de sous-réseau ne contient pas réellement le réseau ou la partie hôte d'une adresse IPv4 ; il indique simplement où rechercher ces parties dans une adresse IPv4 donnée

Opération ET au niveau du bit

Adresse IPv4	192 .	168 .	10 .	10
	11000000	10101000	00001010	00001010
Masque de sous-réseau	255 .	255 .	255 .	0
	11111111	11111111	11111111	00000000
Adresse réseau	192 .	168 .	10 .	0
	11000000	10101000	00001010	00000000

1 ET 1 = 1 1 ET 0 = 0 0 ET 1 = 0 0 ET 0 = 0

Examen de la longueur du préfixe

	Décimale à point	Bits significatifs affichés en binaire
Adresse réseau	**10.1.1.0/24**	**10.1.1.00000000**
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.254	10.1.1.11111110
Adresse de diffusion	10.1.1.255	10.1.1.11111111
Nombre d'hôtes: 2^8 - 2=254 hôtes		

Adresse réseau	**10.1.1.0/25**	**10.1.1.00000000**
Première adresse d'hôte		
Dernière adresse d'hôte		
Adresse de diffusion		
Nombre d'hôtes:		

Adresse réseau	**10.1.1.0/26**	**10.1.1.00000000**
Première adresse d'hôte		
Dernière adresse d'hôte		
Adresse de diffusion		
Nombre d'hôtes:		

Examen de la longueur du préfixe

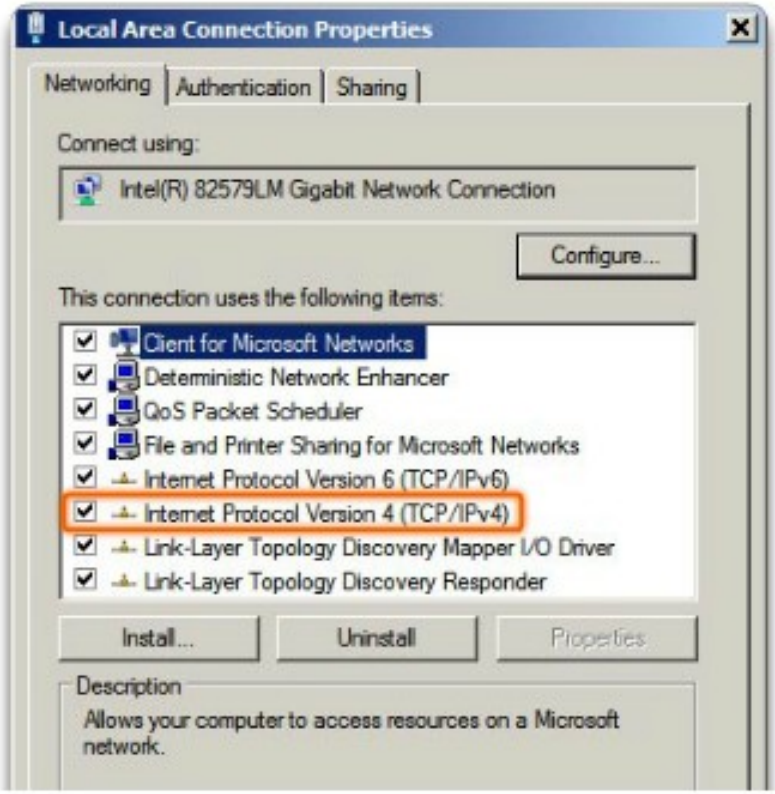
	Décimale à point	Bits significatifs affichés en binaire
Adresse réseau	**10.1.1.0/24**	**10.1.1.00000000**
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.254	10.1.1.11111110
Adresse de diffusion	10.1.1.255	10.1.1.11111111
Nombre d'hôtes: 2^8 - 2=254 hôtes		

Adresse réseau	**10.1.1.0/25**	**10.1.1.00000000**
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.126	10.1.1.01111110
Adresse de diffusion	10.1.1.127	10.1.1.01111111
Nombre d'hôtes: 2^7 - 2=126 hôtes		

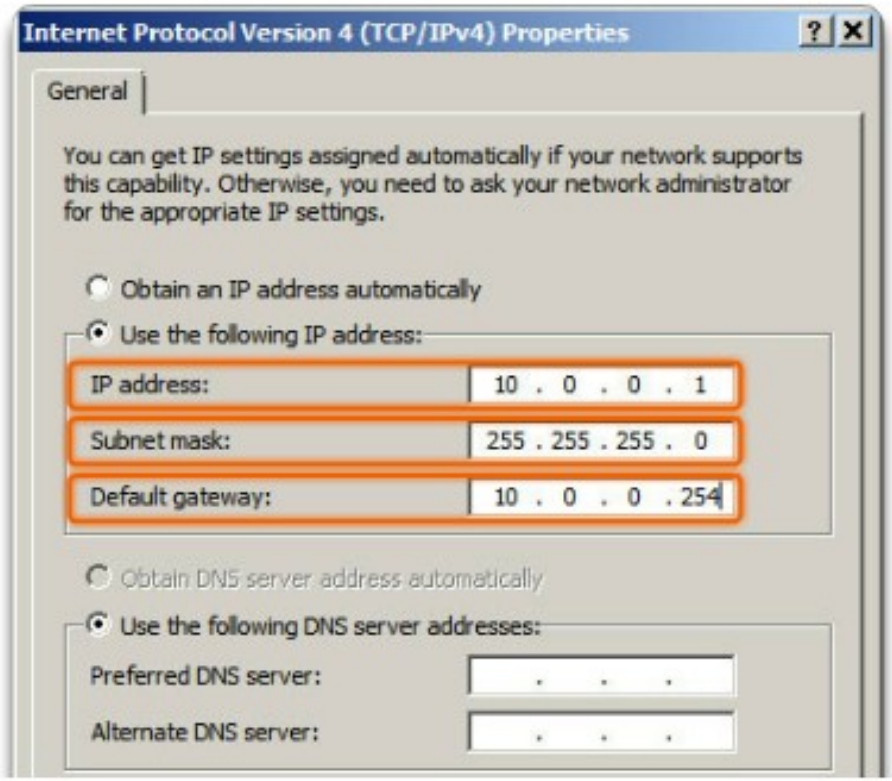
Adresse réseau	**10.1.1.0/26**	**10.1.1.00000000**
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.62	10.1.1.00111110
Adresse de diffusion	10.1.1.63	10.1.1.00111111
Nombre d'hôtes: 2^6 - 2=62 hôtes		

Attribution d'une adresse IPv4 statique à un hôte

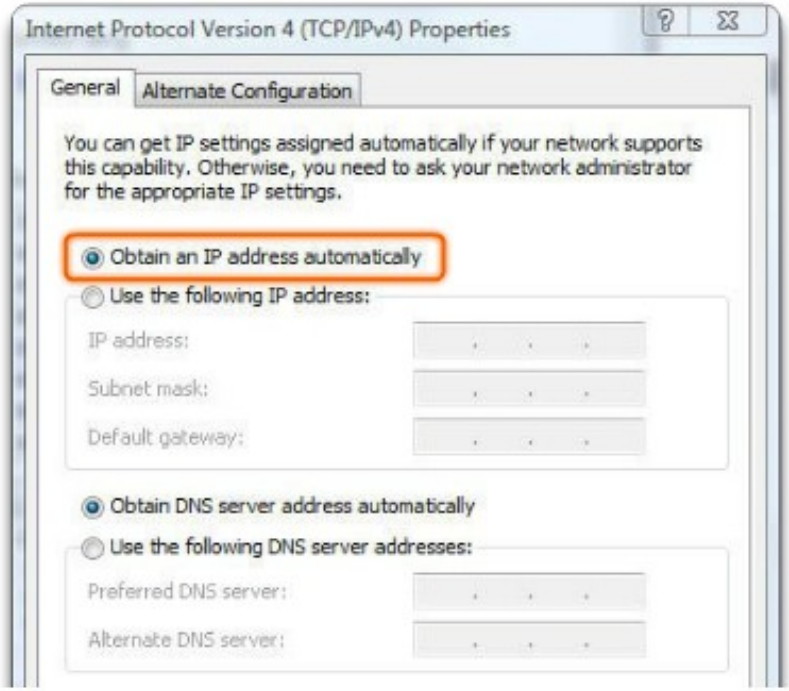
Propriétés d'interface LAN

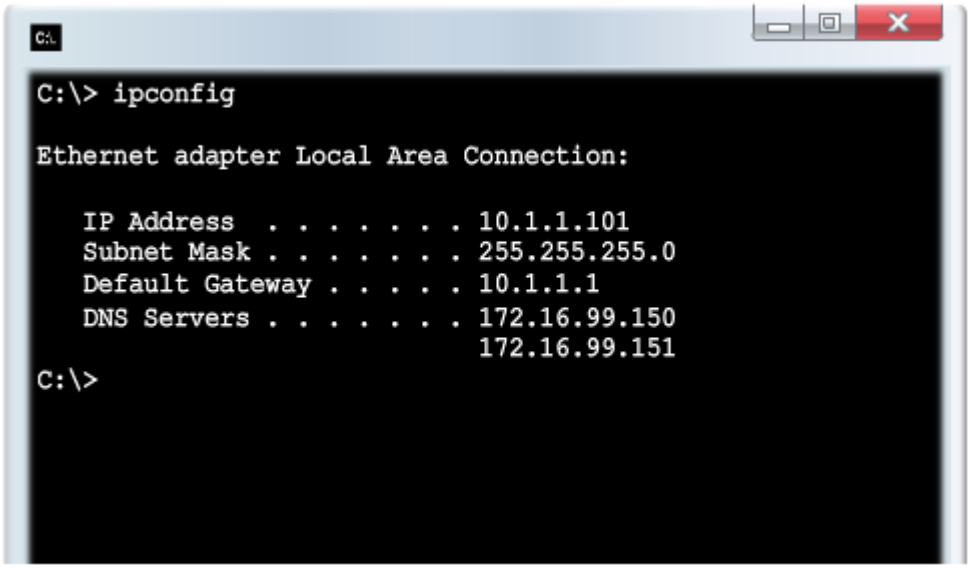


Configuration d'une adresse IPv4 statique



Attribution d'une adresse IPv4 dynamique à un hôte





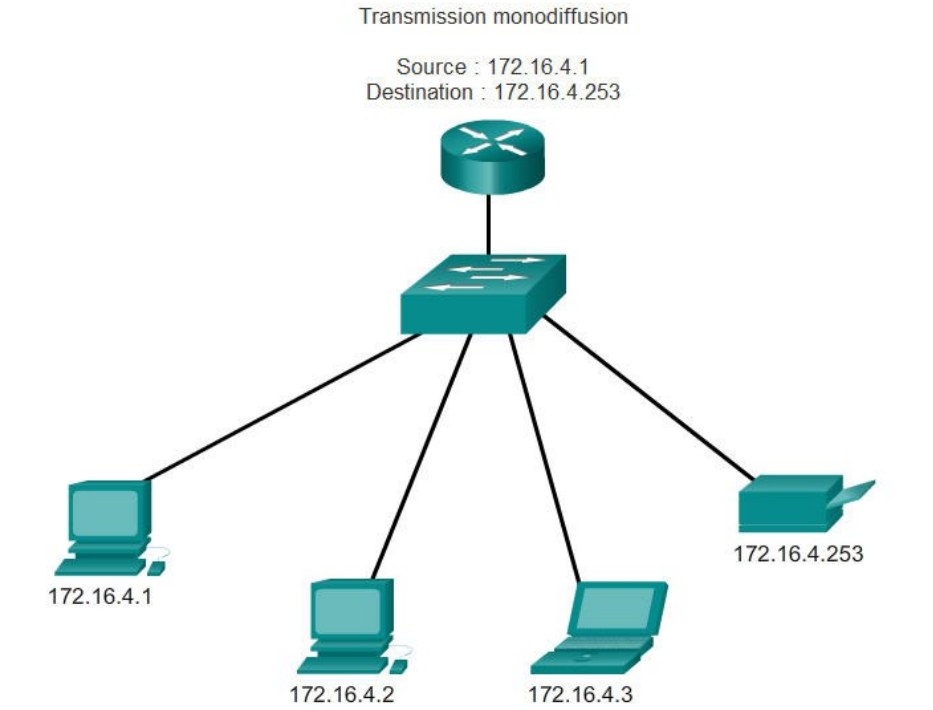
Vérification

DHCP : méthode privilégiée de « location » des adresses IPv4 aux hôtes sur les grands réseaux, car elle réduit la charge de travail de l'assistance technique et élimine presque toutes les erreurs d'entrée

Transmission en monodiffusion

Dans un réseau IPv4, les hôtes peuvent communiquer de trois façons :

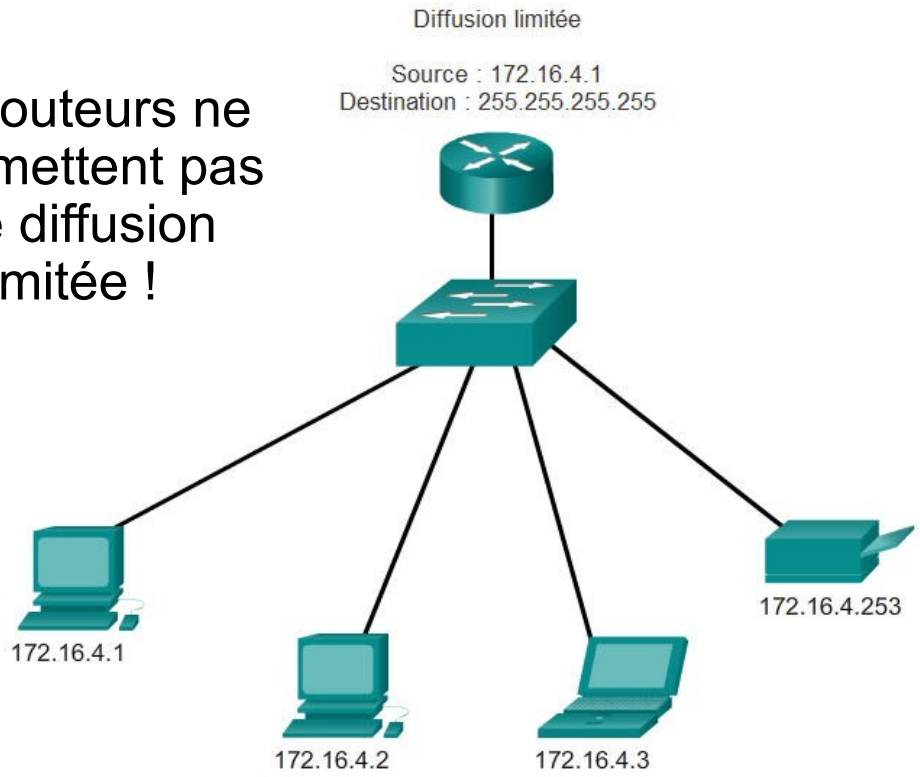
1. **Monodiffusion (unicast)** : consiste à envoyer un paquet d'un hôte à un autre



Transmission en diffusion

2. **Diffusion (broadcast)** : consiste à envoyer un paquet d'un hôte à tous les hôtes du réseau

Les routeurs ne transmettent pas une diffusion limitée !



Diffusion dirigée

- Destination 172.16.4.255
- Hôtes situés dans le réseau 172.16.4.0/24

Transmission en multidiffusion

- **Multidiffusion (multicast)** : consiste à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier, même situés dans des réseaux différents
- Réduit le trafic
- Réservé à l'adressage à des groupes de multidiffusion - de 224.0.0.0 à 239.255.255.255
- Adresses d'une étendue globale : de 224.0.1.0 à 238.255.255.255 (exemple : 224.0.1.1 a été réservée au protocole NTP)

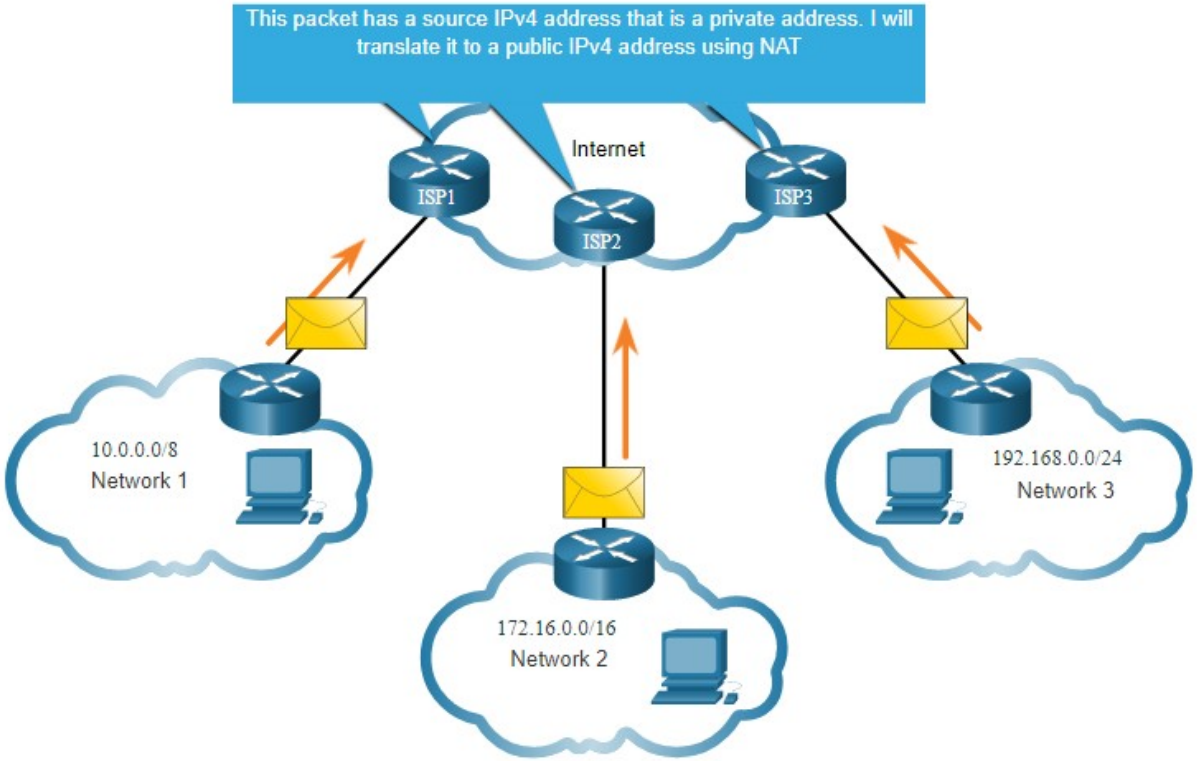
Les adresses IPv4 privées

Blocs d'adresses privées :

- 10.0.0.0 à 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 à 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 à 192.168.255.255 (192.168.0.0/16)
- Elles ne sont pas uniques et peuvent être utilisées par n'importe quel réseau interne.
- Elles ne sont pas routables globalement

Routage vers l'internet

- Le processus de traduction d'adresses réseau (NAT) convertit les adresses IPv4 privées en adresses IPv4 publiques.
- NAT est généralement activé sur le routeur périphérique qui se connecte à l'internet
- Il traduit les adresses IP privées en adresses IP publiques.



Les adresses IPv4 réservées

- **Adresses réseau et de diffusion :** dans chaque réseau, les première et dernière adresses ne peuvent pas être attribuées à des hôtes
- **Adresse de bouclage :** 127.0.0.1 est une adresse spéciale utilisée par les hôtes pour diriger le trafic vers eux-mêmes (les adresses de 127.0.0.0 à 127.255.255.255 sont réservées)
- **Adresse link-local :** les adresses de 169.254.0.0 à 169.254.255.255 (169.254.0.0/16) peuvent être automatiquement attribuées à l'hôte local
  - Plus connues sous le nom d'adresses APIPA (adressage IP privé automatique)
  - Utilisées par un client DHCP Windows pour se configurer automatiquement si aucun serveur DHCP n'est disponible

L'ancien adressage par classe

Les classes d'adresses IP

Classe de l'adresse	Plage du premier octet (décimal)	Bits du premier octet (les bits en vert ne changent pas)	Parties réseau (N) et hôte (H) de l'adresse	Masque de sous-réseau par défaut (décimal et binaire)	Nombre de réseaux et d'hôtes possibles par réseau
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128réseaux (2^7) 16777214hôtes par réseau (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16384réseaux (2^14) 65534hôtes par réseau (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2097150réseaux (2^21) 254hôtes par réseau (2^8-2)
D	224-239	11100000-11101111	ND (multidiffusion)		
E	240-255	11110000-1111 1111	ND (expérimental)		

Remarque: les adresses contenant uniquement des zéros (0) et des uns (1) ne sont pas des adresses d'hôte valides.

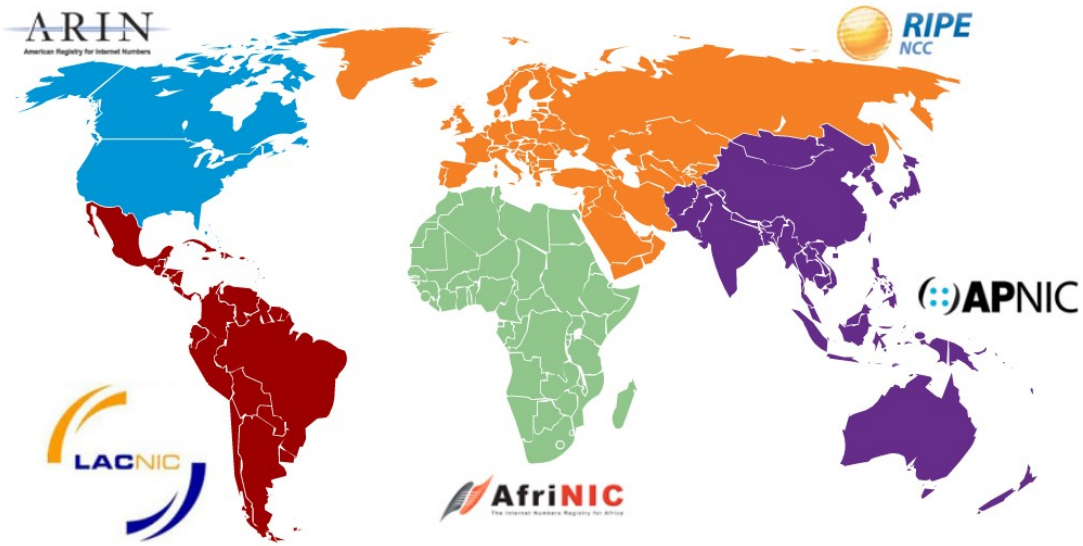
L’adressage sans classe

- Le nom officiel est Routage interdomaine sans classe (CIDR, Classless Inter-Domain Routing)
- Un nouvel ensemble de normes a été créé pour permettre aux fournisseurs de services d'allouer les adresses IPv4 sur n'importe quelle limite binaire (longueur de préfixe) plutôt que seulement avec une adresse de classe A, B ou C.

Attribution des adresses IP

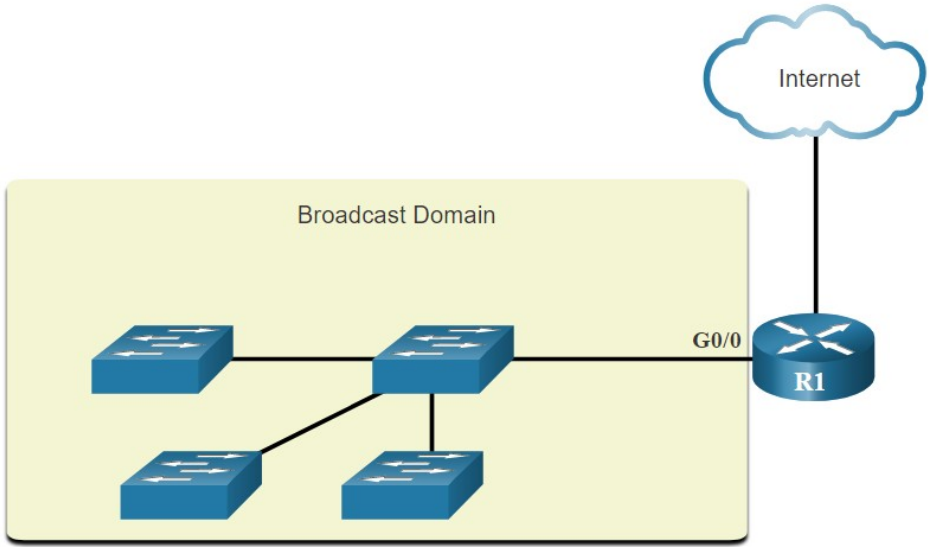
- L'IANA gère les blocs d'adresses IPv4 et IPv6 et les attribue aux organismes d'enregistrement Internet locaux (RIR).

- Les RIR sont chargés d'attribuer des adresses IP à des FAI qui, à leur tour, fournissent des blocs d'adresses IPv4 aux entreprises et aux FAI de plus petite envergure.



Domaines de diffusion et de segmentation

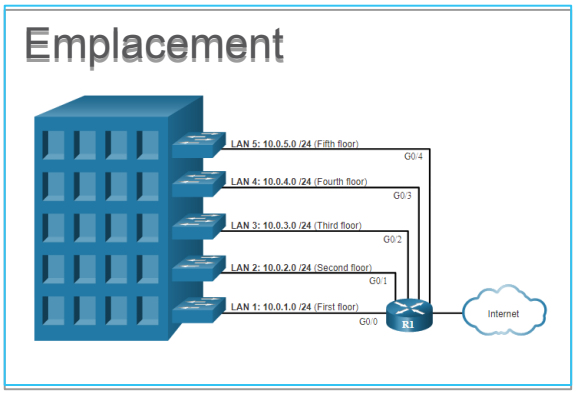
- Plusieurs protocoles utilisent des diffusions ou des multidiffusions (par exemple, ARP utilise des diffusions pour localiser d'autres périphériques, les hôtes envoient des diffusions de découverte DHCP pour localiser un serveur DHCP.)
- Les commutateurs diffusent les messages de diffusion sur toutes les interfaces, sauf celle d'où les messages proviennent.

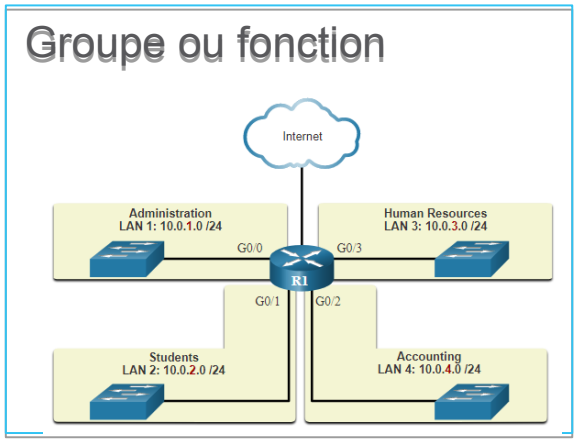


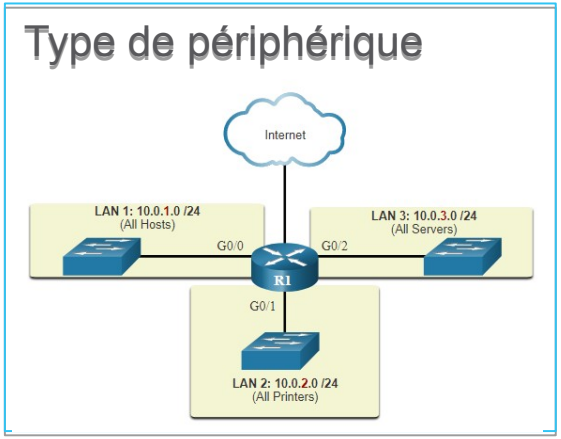
- Le seul périphérique qui arrête les diffusions est un routeur

Pourquoi créer des sous-réseaux ?

- La segmentation en sous-réseaux réduit le trafic global et améliore les performances réseau.
- Elle permet également de mettre en œuvre des politiques de sécurité entre les différents sous-réseaux.
- Le sous-réseau réduit le nombre de périphériques affectés par un trafic de diffusion anormal.
- Les sous-réseaux sont utilisés pour diverses raisons, notamment:

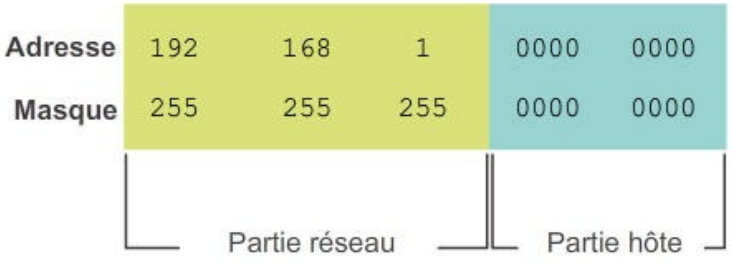


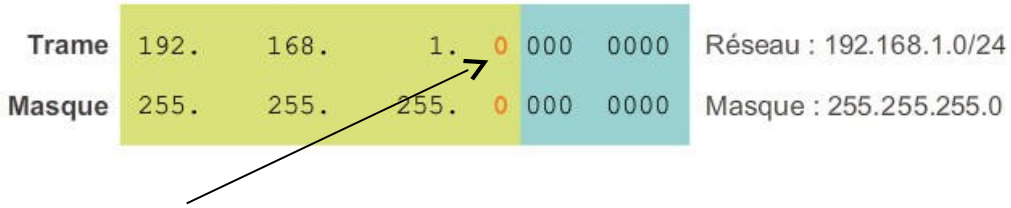




Notions de base sur les sous-réseaux

- Bits empruntés pour créer des sous-réseaux
- Emprunter 1 bit $2^1 = 2$ sous-réseaux





Emprunter 1 bit à la partie hôte crée 2 sous-réseaux avec le même masque de sous-réseau

Sous-réseau 0

Réseau : 192.168.1.**0-127**/**25**

Masque : 255.255.255.**128**

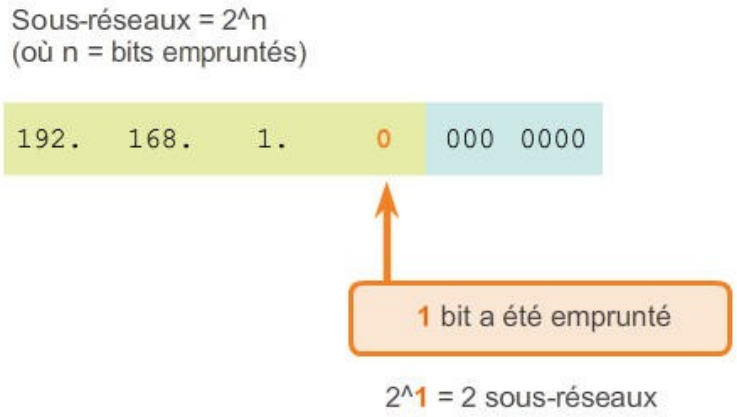
Sous-réseau 1

Réseau : 192.168.1.**128-255**/**25**

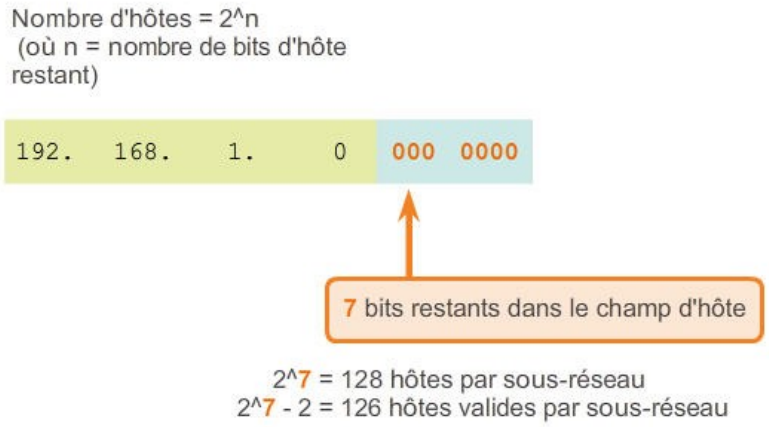
Masque : 255.255.255.**128**

Les formules de calcul des sous-réseaux

- Calculer le nombre de sous-réseaux

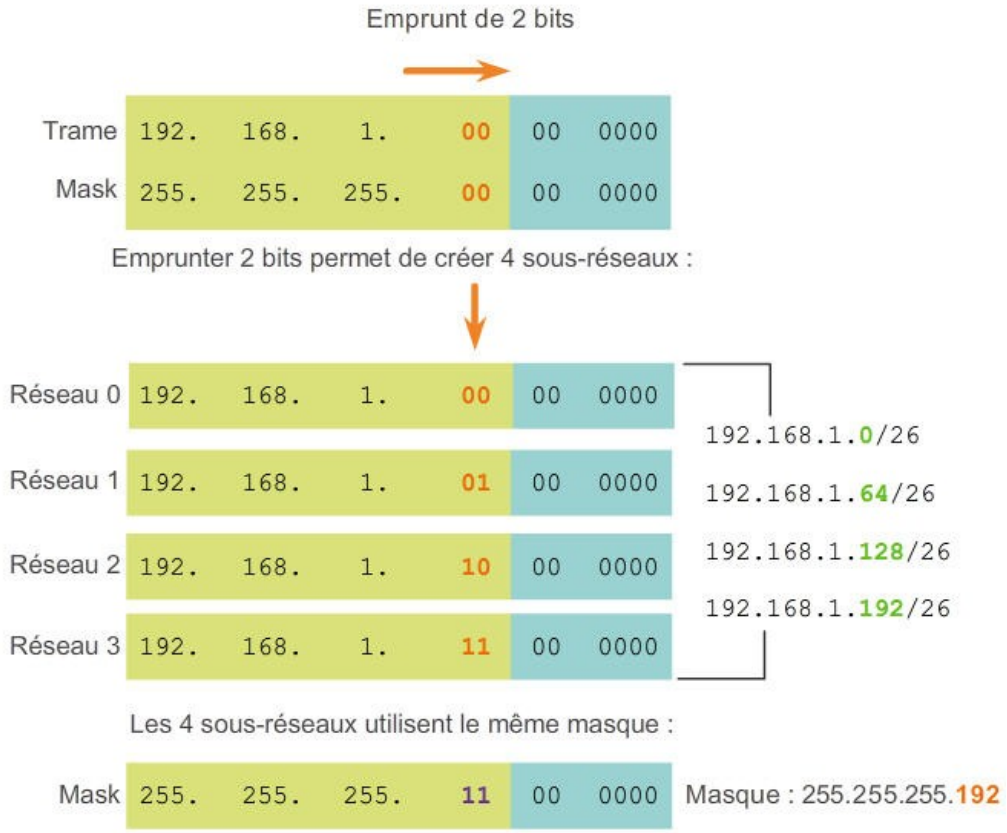


- Calculer le nombre d'hôtes



Créer 4 sous-réseaux

- Emprunter 2 bits pour créer 4 sous-réseaux **$2^2 = 4$ sous-réseaux**



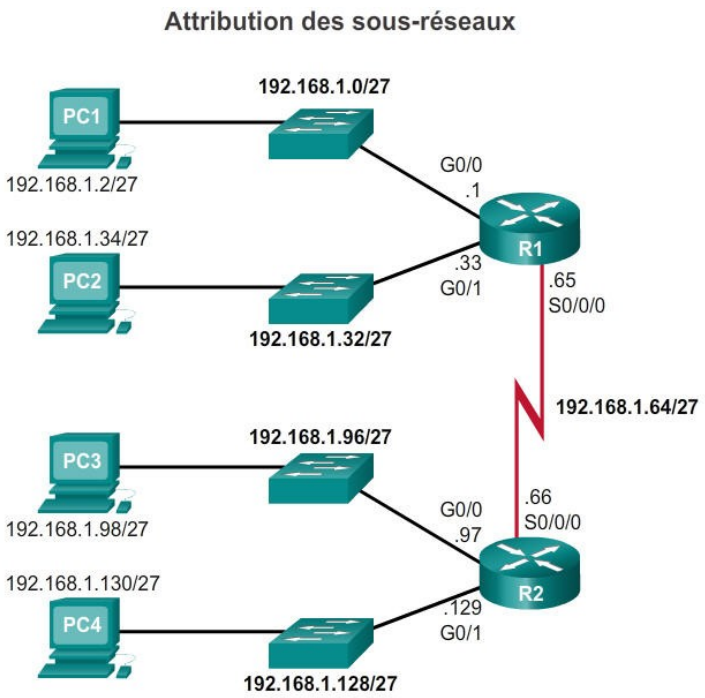
Créer 8 sous-réseaux

- Emprunter 3 bits pour créer 8 sous-réseaux **$2^3 = 8$ sous-réseaux**

Réseau 0	Réseau	192.	168.	1.	000	0	0000	192.168.1.0
	Premier	192.	168.	1.	000	0	0001	192.168.1.1
	Dernier	192.	168.	1.	000	1	1110	192.168.1.30
	Diffusion	192.	168.	1.	000	1	1111	192.168.1.31
Réseau 1	Réseau	192.	168.	1.	001	0	0000	192.168.1.32
	Premier	192.	168.	1.	001	0	0001	192.168.1.33
	Dernier	192.	168.	1.	001	1	1110	192.168.1.62
	Diffusion	192.	168.	1.	001	1	1111	192.168.1.63
Réseau 2	Réseau	192.	168.	1.	010	0	0000	192.168.1.64
	Premier	192.	168.	1.	010	0	0001	192.168.1.65
	Dernier	192.	168.	1.	010	1	1110	192.168.1.94
	Diffusion	192.	168.	1.	010	1	1111	192.168.1.95
Réseau 3	Réseau	192.	168.	1.	011	0	0000	192.168.1.96
	Premier	192.	168.	1.	011	0	0001	192.168.1.97
	Dernier	192.	168.	1.	011	1	1110	192.168.1.126
	Diffusion	192.	168.	1.	011	1	1111	192.168.1.127

Créer 8 sous-réseaux (suite)

Réseau 4	Réseau	192.	168.	1.	100	0	0000	192.168.1.128
	Premier	192.	168.	1.	100	0	0001	192.168.1.129
	Dernier	192.	168.	1.	100	1	1110	192.168.1.158
	Diffusion	192.	168.	1.	100	1	1111	192.168.1.159
Réseau 5	Réseau	192.	168.	1.	101	0	0000	192.168.1.160
	Premier	192.	168.	1.	101	0	0001	192.168.1.161
	Dernier	192.	168.	1.	101	1	1110	192.168.1.190
	Diffusion	192.	168.	1.	101	1	1111	192.168.1.191
Réseau 6	Réseau	192.	168.	1.	110	0	0000	192.168.1.192
	Premier	192.	168.	1.	110	0	0001	192.168.1.193
	Dernier	192.	168.	1.	110	1	1110	192.168.1.222
	Diffusion	192.	168.	1.	110	1	1111	192.168.1.223
Réseau 7	Réseau	192.	168.	1.	111	0	0000	192.168.1.224
	Premier	192.	168.	1.	111	0	0001	192.168.1.225
	Dernier	192.	168.	1.	111	1	1110	192.168.1.254
	Diffusion	192.	168.	1.	111	1	1111	192.168.1.255



Segmenter le réseau en sous-réseaux en fonction des besoins des hôtes

Deux considérations sont à prendre en compte lors de la planification de sous-réseaux :

- Nombre de sous-réseaux nécessaires
- Nombre d'adresses d'hôte nécessaires
- Formule pour déterminer le nombre d'hôtes utilisables

2^n-2

2^n (où n est le nombre de bits d'hôte restant) est utilisé pour calculer le nombre d'hôtes

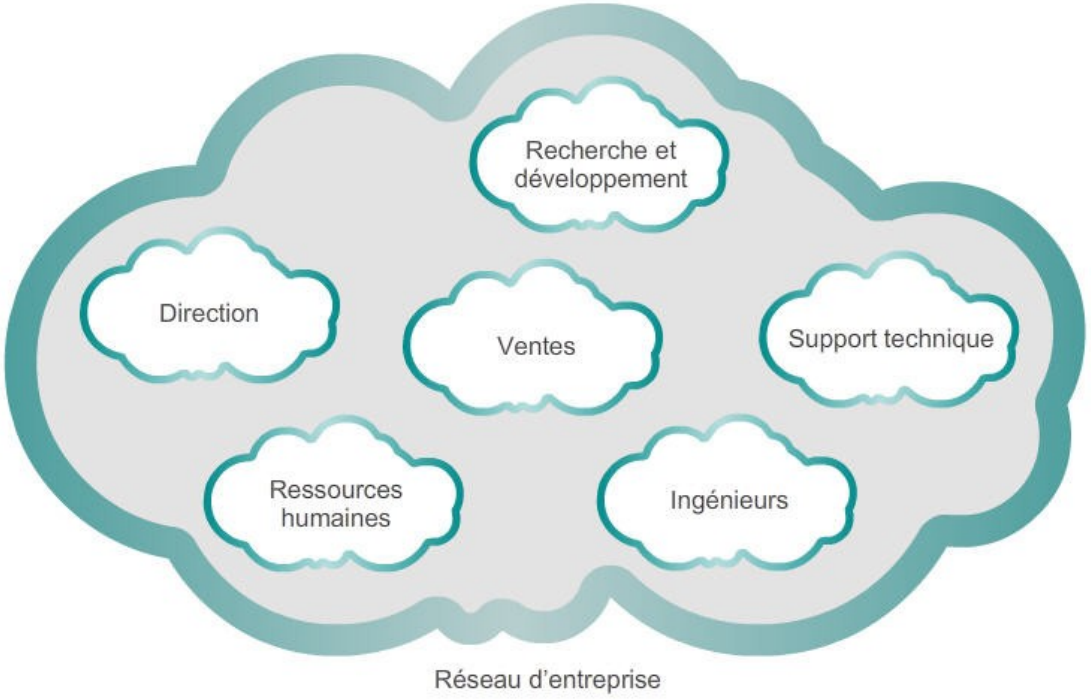
-2 L'ID de sous-réseau et l'adresse de diffusion ne peuvent pas être utilisés sur chaque sous-réseau

Segmenter le réseau en fonction des besoins de celui-ci

Calculer le nombre de sous-réseaux

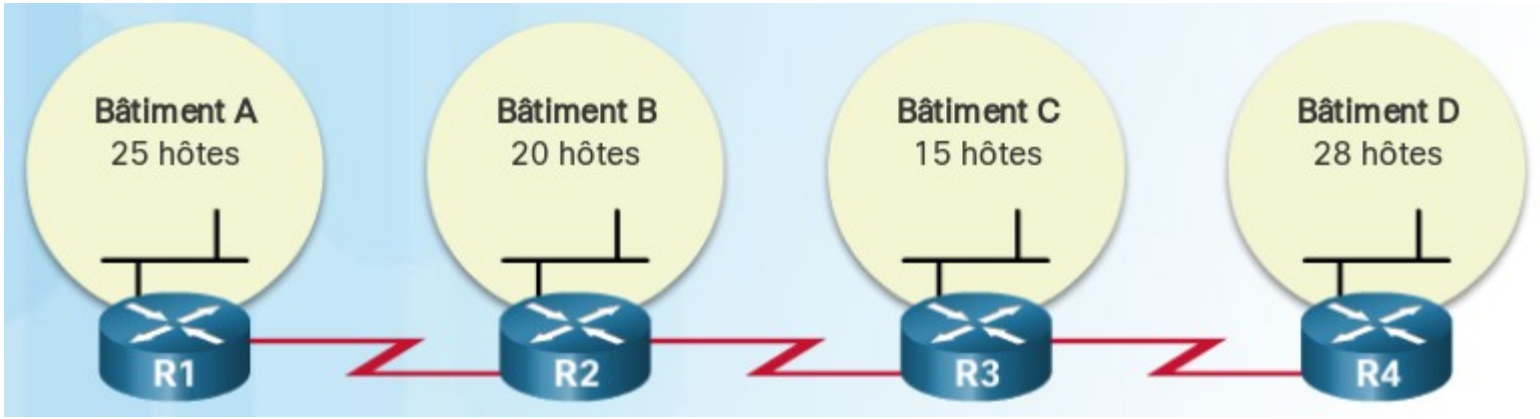
- Formule **2^n** (où n est le nombre de bits empruntés)

- Sous-réseau nécessaire pour chaque service du schéma



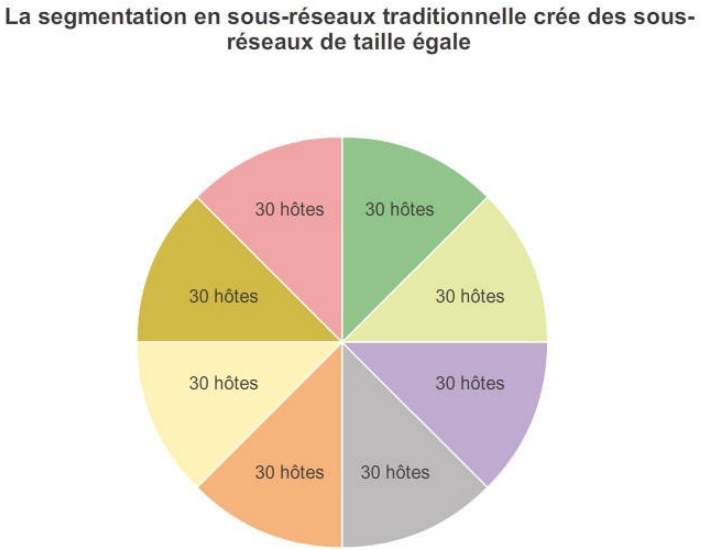
Segmenter le réseau en fonction des besoins de celui-ci

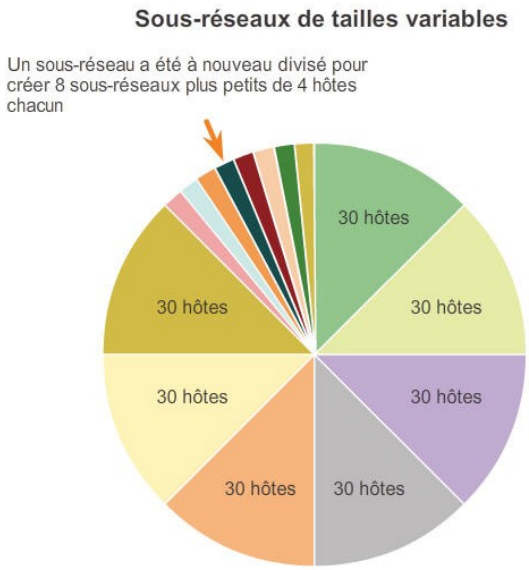
- Il est important d'équilibrer le nombre de sous-réseaux nécessaires et le nombre d'hôtes nécessaires pour le plus grand sous-réseau
- Il faut que le schéma d'adressage puisse accueillir le nombre maximal d'hôtes pour chaque sous-réseau
- Prévision de croissance dans chaque sous-réseau



La segmentation traditionnelle en sous-réseaux entraîne un gaspillage d'adresses

- Segmentation traditionnelle : le même nombre d'adresses est attribué à chaque sous-réseau.
- Les sous-réseaux qui n'ont pas besoin de la totalité ont des adresses inutilisées (gaspillées). Par exemple, les liaisons WAN n'ont besoin que de 2 adresses.
- Les masques de sous-réseau de longueur variable (VLSM, Variable Length Subnet Mask) ou la segmentation d'un sous-réseau optimisent l'utilisation des adresses.





Les masques de sous-réseau de longueur variable (VLSM)

- La technique VLSM permet de décomposer un espace réseau en parties inégales.
- Le masque de sous-réseau varie alors selon le nombre de bits ayant été empruntés pour un sous-réseau particulier.
- Le réseau est segmenté en premier, puis les sous-réseaux sont divisés à leur tour.
- Cette opération est répétée autant de fois que nécessaire pour créer des sous-réseaux de différentes tailles.

Planification de l'adressage réseau

L'attribution des adresses réseau doit être planifiée et documentée pour :

- Éviter la duplication des adresses
- Fournir et contrôler l'accès
- Contrôler la sécurité et surveiller les performances

Adresses pour les clients : généralement attribuées de manière dynamique à l'aide du protocole DHCP (Dynamic Host Configuration Protocol)

Exemple de plan d'adressage réseau

Réseau: 192.168.1.0/24		
Utilisation	**Premier**	**Dernier**
Périphériques hôtes	.1	.229
Serveurs	.230	.239
Imprimantes	.240	.249
Périphériques intermédiaires	.250	.253
Passerelle (interface LAN du routeur)	.254	

Résumé

- Décrire la structure d'une adresse IPv4, y compris la partie hôte, la partie réseau et le masque de sous-réseau
- Comparer les caractéristiques et les utilisations des adresses IPv4 de monodiffusion, de diffusion et de multidiffusion
- Expliquer les adresses IPv4 publiques, privées et réservées
- Expliquer comment la segmentation d'un réseau permet d'améliorer la communication
- Calculer les sous-réseaux IPv4

Module 12 : Adressage IPv6

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

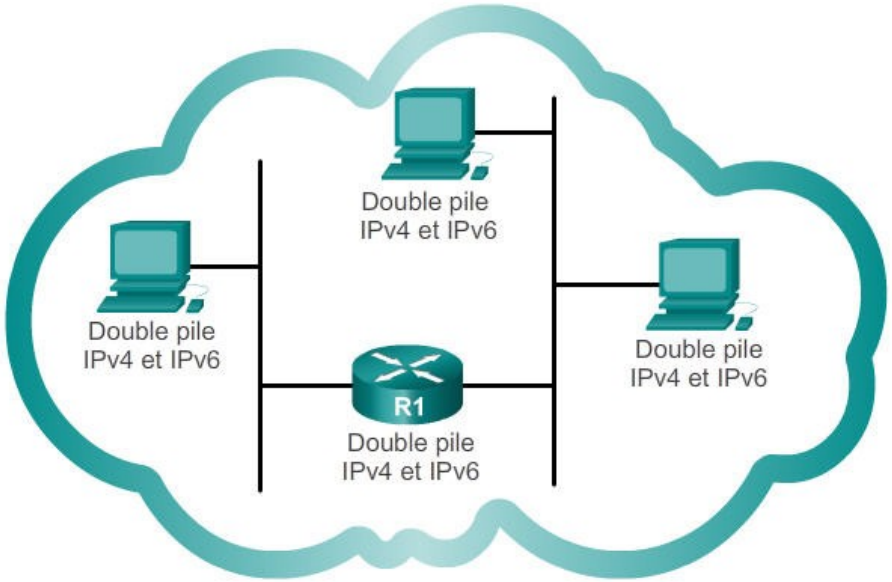
La nécessité du protocole IPv6

- IPv4 dispose d'un maximum théorique d'adresses de 4,3 milliards, plus les adresses privées en combinaison avec NAT
- L'espace d'adressage IPv6 de 128 bits est bien plus étendu et fournit 340 undécillions d'adresses (340.10^{36})
- IPv6 élimine les problèmes de limitation d'IPv4 et apporte d'autres améliorations, notamment ICMPv6
  - **Espace d'adressage plus important**
  - **Traitement plus efficace des paquet** – l'en-tête a été simplifié et comporte moins de champs.
  - **Traduction d'adresses réseau inutile** — grâce au grand nombre d'adressage, il n'est plus nécessaire d'utiliser une adressage privée interne et d'être mappé à une adresse publique partagée.

La coexistence des protocoles IPv4 et IPv6

Les techniques de migration peuvent être classées en trois catégories :

1

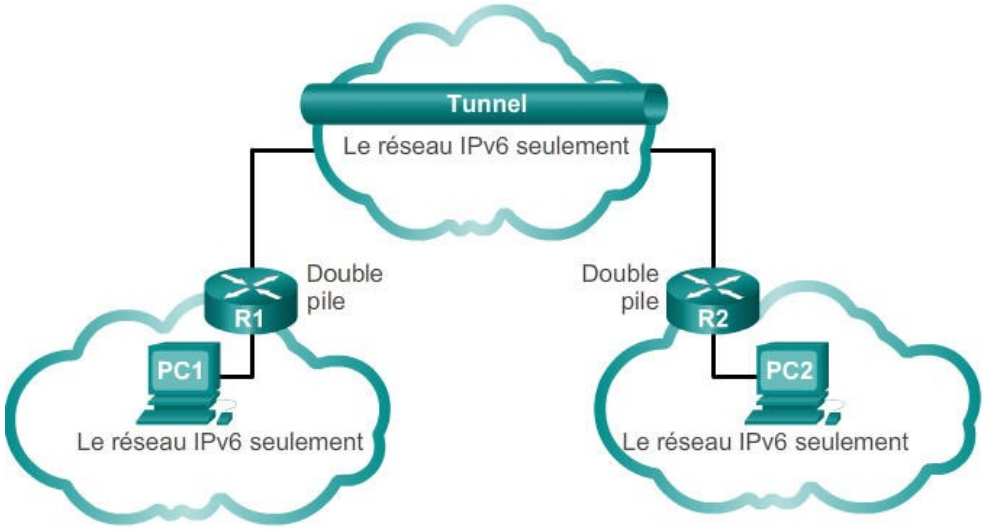


Dual-stack : permet la coexistence IPv4/IPv6 sur le même réseau. Les périphériques utilisent les deux piles de protocoles, IPv4 et IPv6, en même temps.

La coexistence des protocoles IPv4 et IPv6

Les techniques de migration peuvent être classées en trois catégories :

2

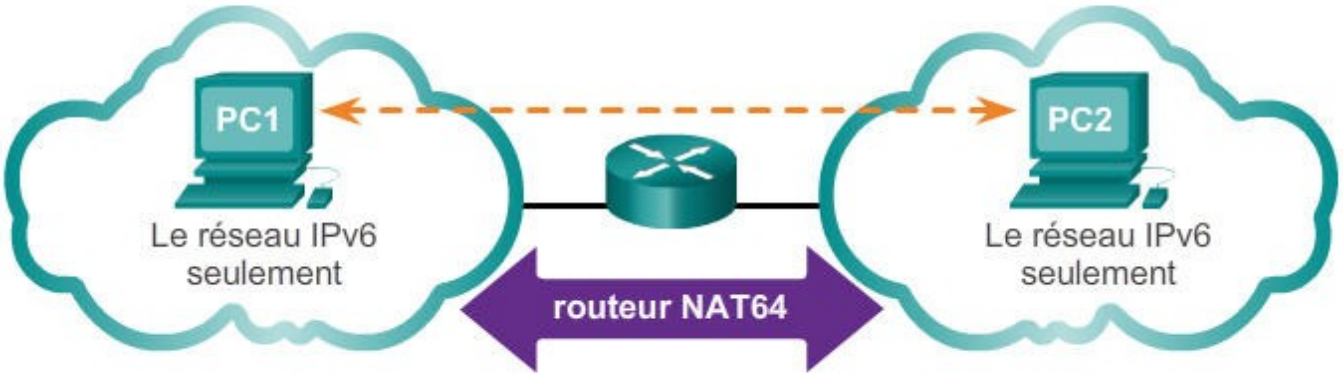


Tunneling : méthode qui consiste à transporter un paquet IPv6 sur un réseau IPv4 en l'encapsulant dans un paquet IPv4.

La coexistence des protocoles IPv4 et IPv6

Les techniques de migration peuvent être classées en trois catégories :

3



Traduction : le NAT64 (Network Address Translation 64) permet aux périphériques IPv6 de communiquer avec des périphériques IPv4 à l'aide d'une technique de traduction analogue au NAT pour IPv4. Un paquet IPv6 est converti en paquet IPv4, et inversement.

La représentation des adresses IPv6

- Comportent 128 bits, sous la forme d'une chaîne de valeurs hexadécimales
- Dans l'adressage IPv6, 4 bits représentent un seul chiffre hexadécimal, 32 valeurs hexadécimales = adresse IPv6

```
2001:0DB8:0000:1111:0000:0000:0000:0200
FE80:0000:0000:0000:0123:4567:89AB:CDEF
```

- Un hextet fait référence à un segment de 16 bits ou quatre hexadécimales
- Peuvent être écrites en minuscules ou en majuscules

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

- Première règle pour réduire les adresses IPv6 : les zéros (0) du début d'une section de 16 bits (ou hextet) peuvent être omis
- 01AB est équivalent à 1AB
- 09F0 est équivalent à 9F0
- 0A00 est équivalent à A00
- 00AB est équivalent à AB

Recommandé	2001:0DB8:000A:1000:0000:0000:0000:0100
Sans zéros en début de segment	2001: DB8: A:1000: 0: 0: 0: 100

Règle n°2 - Omettre toutes les séquences de zéros

- Une suite de deux deux-points (::) peut remplacer toute chaîne unique et continue de deux ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros
  - C'est ce qu'on appelle le *format compressé*
- Cette suite (::) ne peut être utilisée qu'une seule fois dans une adresse, sinon celle-ci devient ambiguë
  - 2001:0db8::abcd::1234 est incorrecte
- :: ne doit pas être utilisée pour remplacer un seul hextet à 0 (RFC 5952)
  - 2001:db8:0:1:1:1:1:1 est correcte, 2001:db8::1:1:1:1:1 n’est pas correcte

Règle n°2 - Omettre toutes les séquences de zéros

- Exemples

1

	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Sans zéros en début de segment	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compressé	2001:DB8::ABCD:0:0:100
ou	
Compressé	2001:DB8:0:0:ABCD::100

Une seule suite :: peut être utilisée.

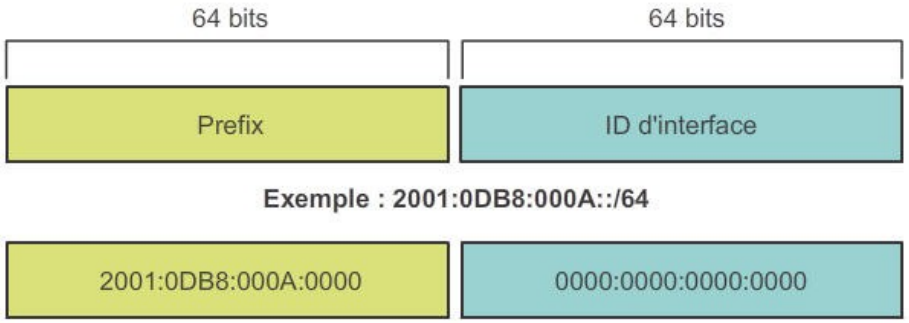
Pour 2 suites de même longueur, on préfère compresser la 1re suite

2

	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Sans zéros en début de segment	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressé	FE80::123:4567:89AB:CDEF

La longueur du préfixe IPv6

- IPv6 n'utilise pas la notation décimale à point du masque de sous-réseau.
- La longueur de préfixe indique la partie réseau d'une adresse IPv6 au format suivant :
  - Adresse IPv6/longueur de préfixe
  - La longueur de préfixe peut aller de 0 à 128
  - La longueur de préfixe est généralement /64



Types d'adresses IPv6

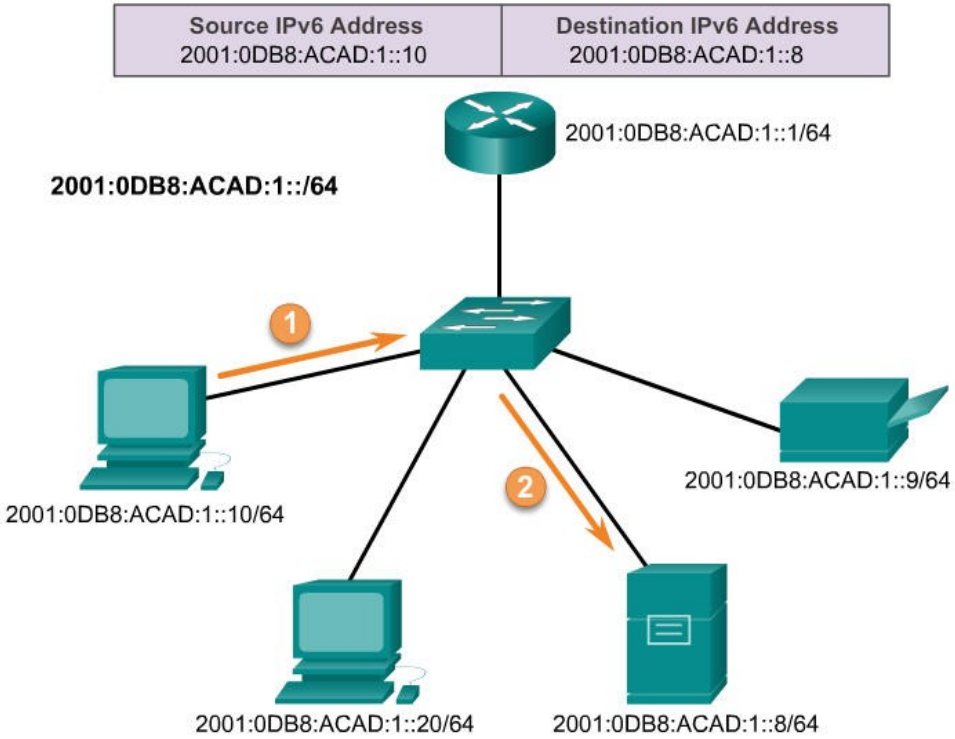
Il existe trois grands types d'adresses IPv6 :

- **Monodiffusion** : une adrese pour un hôte
- **Multidiffusion** : une adresse pour plusieurs hôtes
- **Anycast** : une adresse pour un hôte parmi plusieurs (ex : sélection par un algorithme de routage d'un hôte parmi plusieurs récepteurs potentiels)

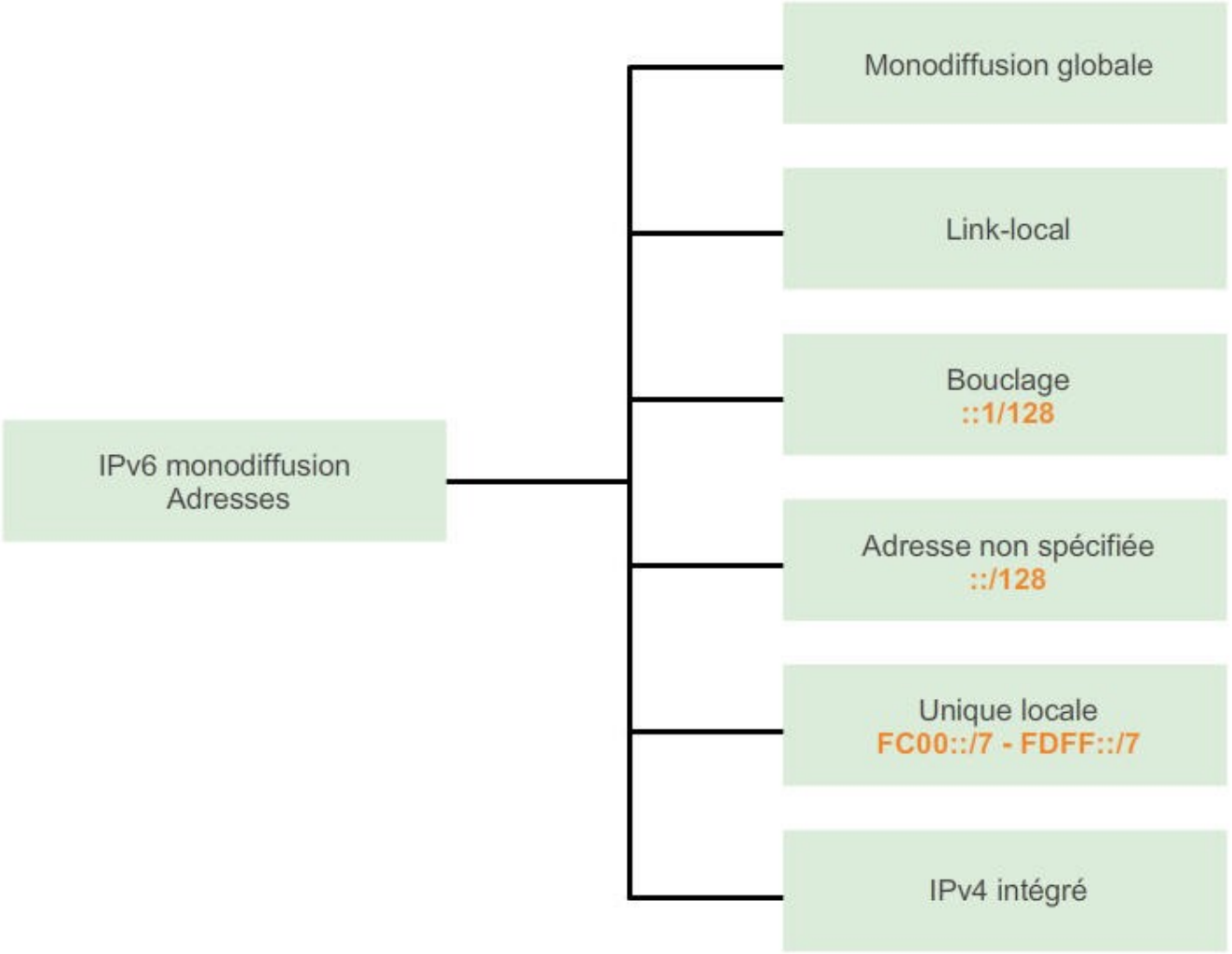
Remarque : IPv6 n'a pas d'adresses de diffusion réservée dans chaque sous-réseau, mais a des adresses de multidiffusion au comportement similaire

Les adresses IPv6 de monodiffusion

- **Monodiffusion**
  - Identifie de façon unique une interface sur un périphérique Ipv6
  - Un paquet envoyé à une adresse de monodiffusion est reçu par l'interface correspondant à cette adresse.



Les adresses IPv6 de monodiffusion



Les adresses IPv6 de monodiffusion

- **Monodiffusion globale**
  - Similaire à une adresse IPv4 publique
  - Globalement unique
  - Adresses routables sur Internet
  - Peuvent être configurées pour être statiques ou attribuées dynamiquement
- **Link-local**
  - Pour communiquer avec les autres périphériques sur la même liaison locale
  - Restriction à une seule liaison - non routables au-delà de la liaison

Les adresses IPv6 de monodiffusion

- **Envoi en boucle**
  - Permet à un hôte de s'envoyer un paquet à lui-même ; pas d'attribution à une interface physique
  - Envoyez une requête ping à l'adresse de bouclage pour tester la configuration TCP/IP de l'hôte local
  - Seulement des 0, sauf pour le dernier bit – adresses avec la syntaxe ::1/128 ou juste ::1
- **Adresse non spécifiée**
  - Adresse contenant uniquement des 0 – Représentée sous la forme ::/128 ou juste ::
  - Ne peut pas être attribuée à une interface et est utilisée uniquement comme adresse source
  - Une adresse non spécifiée est utilisée comme adresse source lorsque le périphérique n'a pas encore d'adresse IPv6 permanente ou lorsque la source du paquet est inappropriée pour la destination

Une remarque à propos de l’adresse locale unique

Les **adresses locales uniques** IPv6 (plage fc00::/7 à fdff::/7) présentent une certaine similitude avec les **adresses privées** RFC 1918 pour IPv4, mais il existe des différences.

- Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites.
- Les adresses locales uniques peuvent être utilisées pour les périphériques qui n'auront jamais besoin d'être accessibles sur un autre réseau.
- Les adresses locales uniques ne sont pas routées globalement ou traduites en adresse IPv6 globale.

Remarque: de nombreux sites utilisent la nature privée des adresses RFC 1918 pour tenter de sécuriser ou de cacher leur réseau des risques potentiels de sécurité. Cela n'a jamais été l'utilisation prévue des ULA.

IPv6 GUA (adresses de diffusion globales)

- Adresses **globalement uniques** et routables sur le réseau Internet IPv6
- L'équivalent des adresses IPv4 **publiques**
- Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000::/3 sont attribuées

IPv6 GUA : structure

Préfixe de routage global:

- Le préfixe de routage global est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un ISP) à un client ou à un site. Le préfixe de routage global varie en fonction des stratégies du fournisseur de services Internet.

ID de sous-réseau

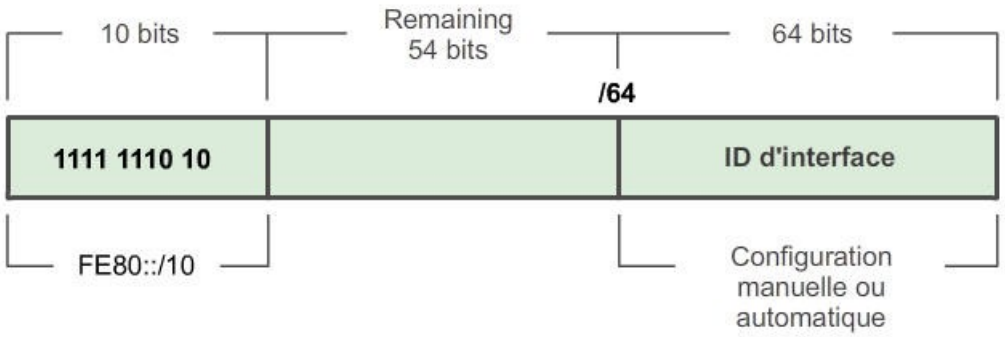
- Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface. L'ID de sous-réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site.

ID d'interface

- L'ID d'interface IPv6 est l'équivalent de la partie hôte d'une adresse IPv4. Dans la plupart des cas, il est fortement recommandé d'utiliser des sous-réseaux /64, qui crée un ID d'interface de 64 bits.

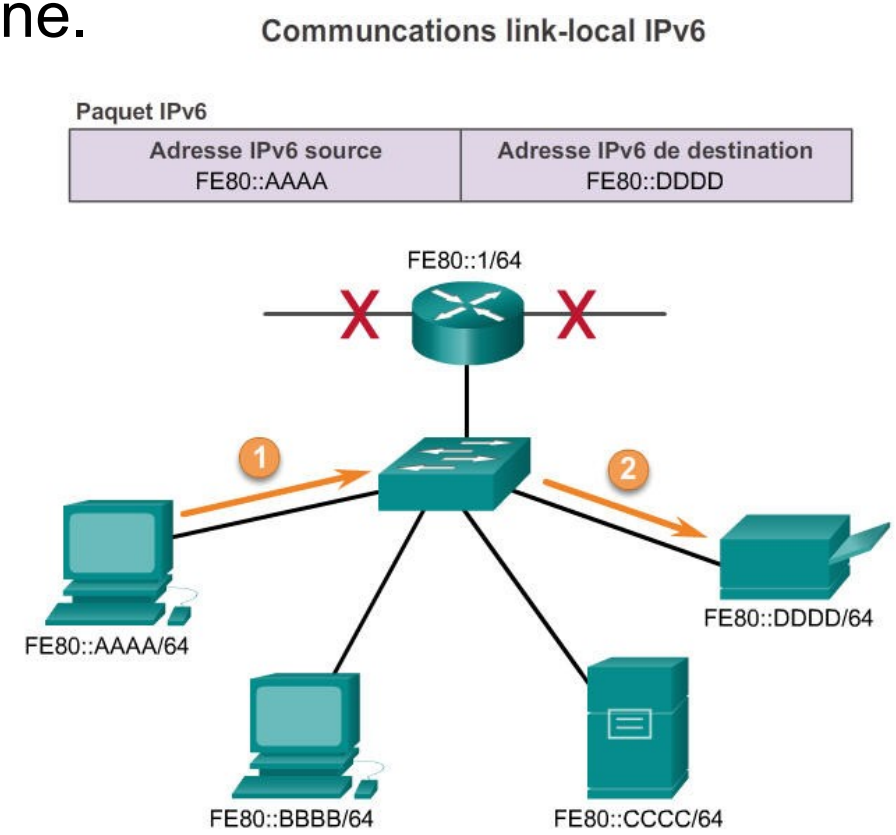
Les adresses de monodiffusion link-local IPv6 (LLA)

- Chaque interface réseau IPv6 DOIT avoir une adresse link-local
- Permet à un périphérique de communiquer avec les autres périphériques IPv6 sur la même liaison et seulement sur celle-ci (le sous-réseau)
- Plage FE80::/10, les 10 premiers bits étant 1111 1110 10xx xxxx
- 1111 1110 10**00 0000** (FE80) - 1111 1110 10**11 1111** (FEBF)



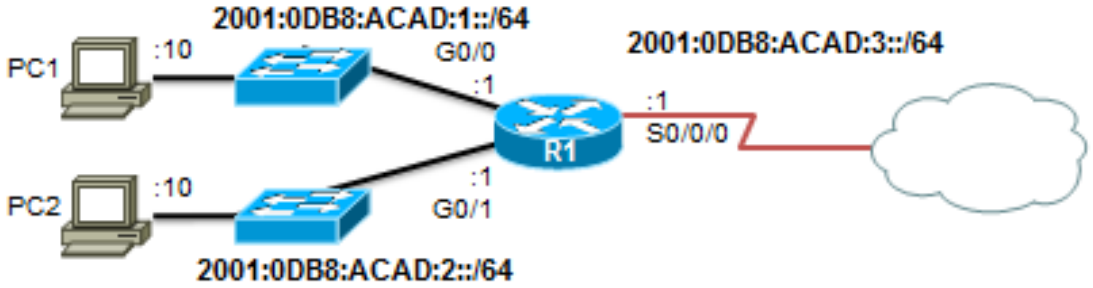
Les adresses de monodiffusion link-local IPv6

- Les paquets associés à une adresse link-local source ou de destination ne peuvent pas être acheminés au-delà de leur liaison d'origine.



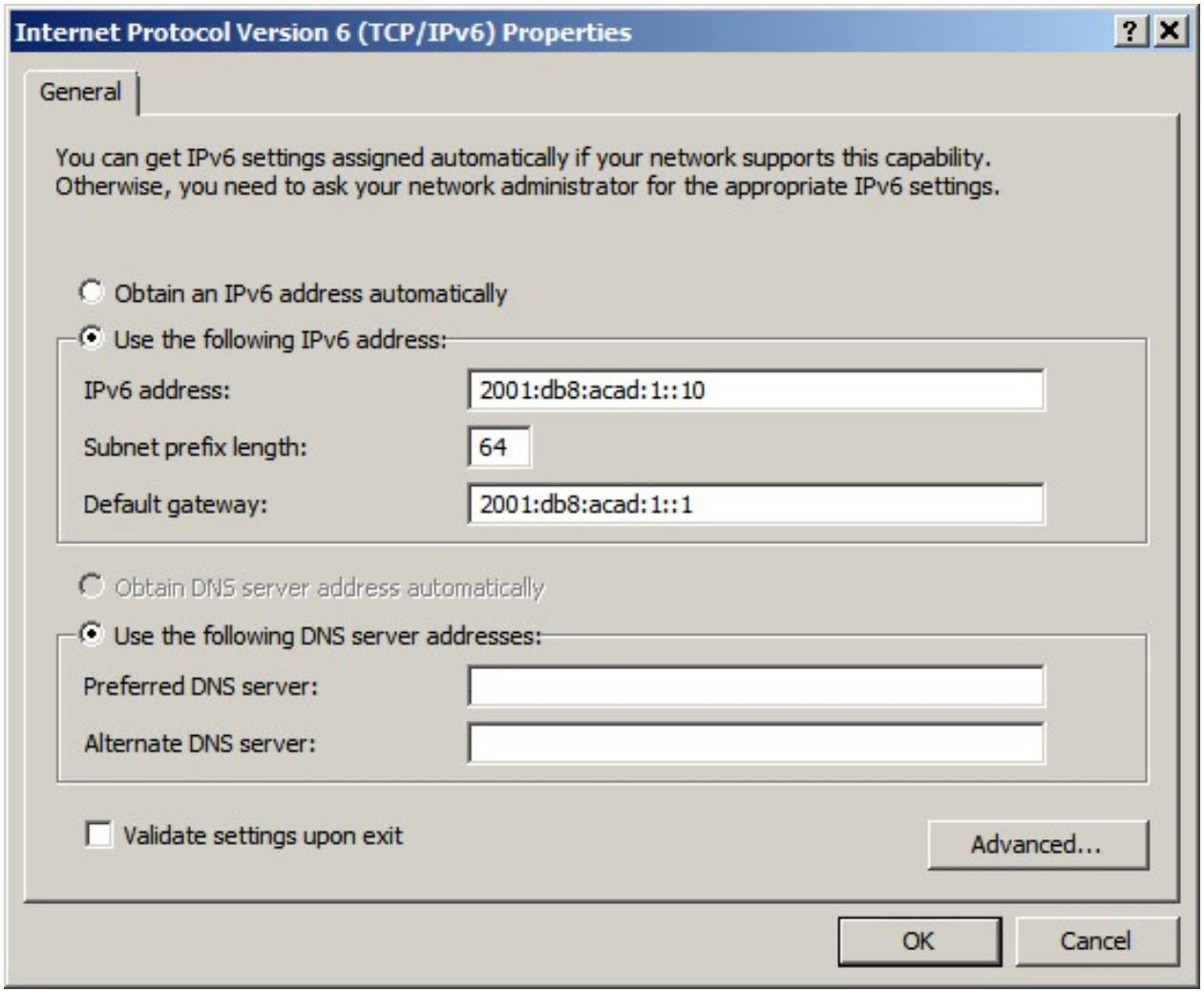
Les adresses de monodiffusion IPv6

La configuration statique d'une adresse de monodiffusion globale




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```

La configuration statique d'une adresse de monodiffusion globale IPv6



Adressage dynamique pour les IPv6 GUA

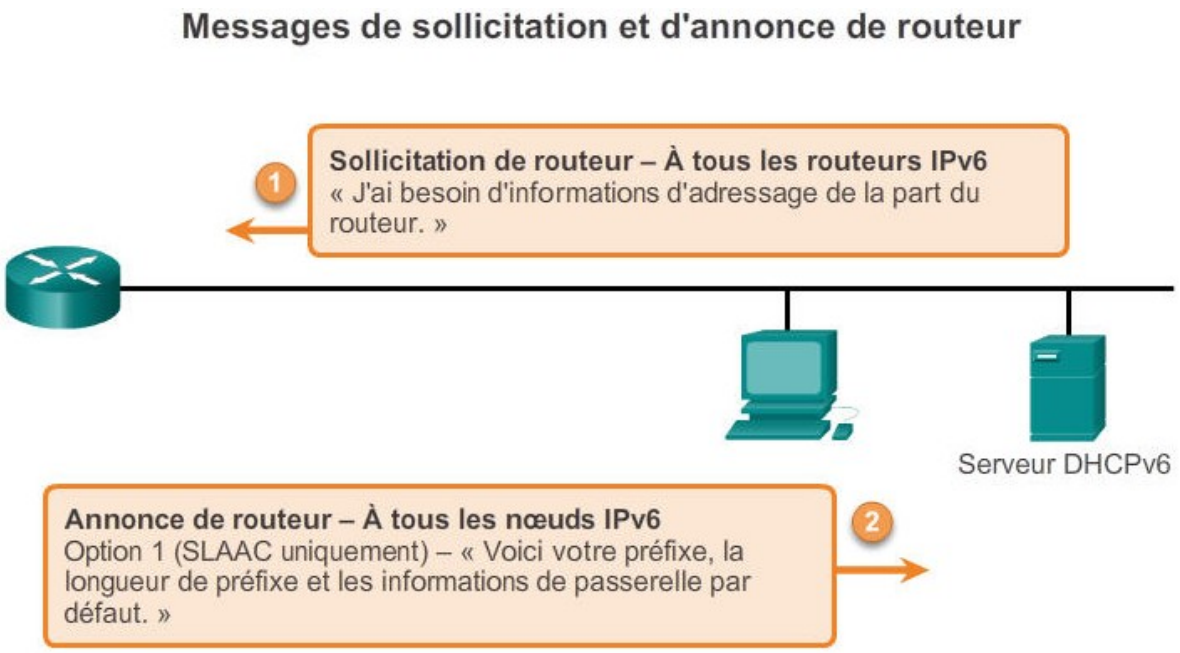
Messages RS et RA

- Les périphériques obtiennent des adresses GUA dynamiquement via les messages **ICMPv6** (*Internet Control Message Protocol* version 6)
  - Les messages de **sollicitation de routeur** (RS) sont envoyés par les périphériques hôtes pour découvrir les routeurs IPv6
  - Les messages de **publicité de routeur** (RA) sont envoyés par les routeurs pour informer les hôtes sur la façon d'obtenir une GUA IPv6 et fournir des informations réseau utiles telles que :
    - Préfixe réseau et longueur du préfixe
    - Adresse de la passerelle par défaut
    - Adresses DNS et nom de domaine
- Il existe trois méthodes pour configurer une IPv6 GUA
  - SLAAC
  - SLAAC avec serveur DHCPv6 apatride
  - DHCPv6 avec état (pas de SLAAC)

Adressage dynamique pour les IPv6 GUA

Méthode 1 : SLAAC

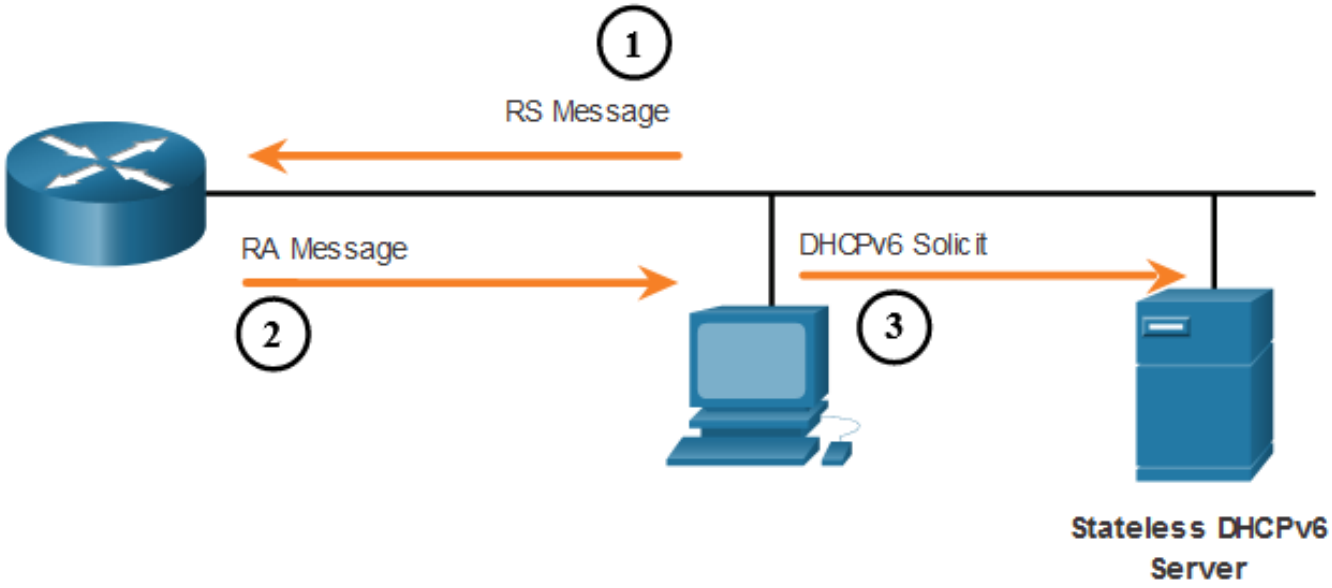
- SLAAC permet à un périphérique de configurer une GUA sans les services de DHCPv6.
- Les périphériques obtiennent les informations nécessaires pour configurer une GUA à partir des messages RA ICMPv6 du routeur local.
- Le préfixe est fourni par le RA et le périphérique utilise soit la méthode EUI-64, soit la méthode de génération aléatoire pour créer un ID d'interface.



Méthode 2 : SLAAC et DHCP sans état

Le message RA suggère que les appareils utilisent les éléments suivants :

- SLAAC pour créer sa propre IPv6 GUA
- l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut.
- un serveur DHCPv6 sans état pour obtenir d'autres informations telles que l'adresse d'un serveur DNS et un nom de domaine

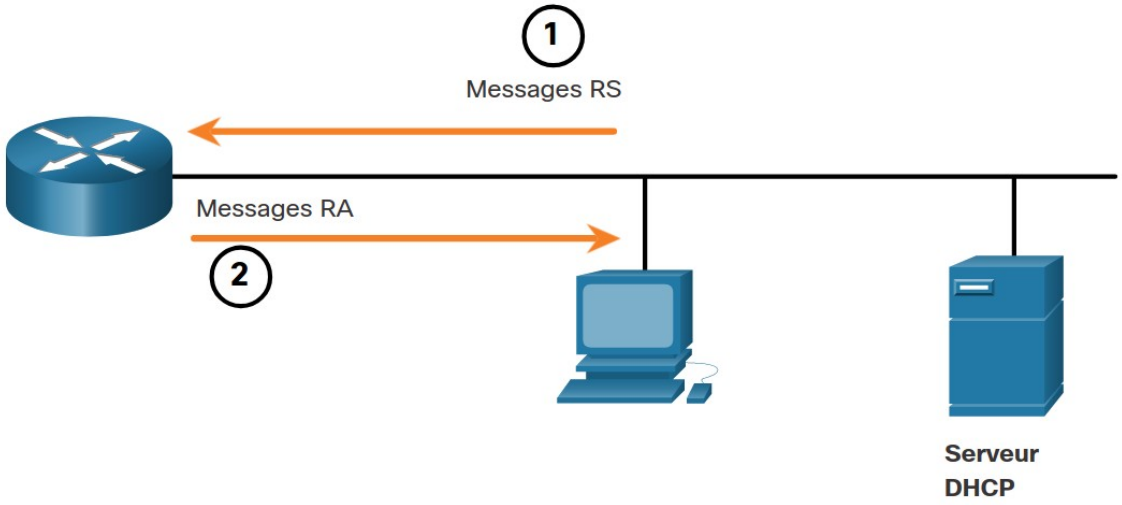


Méthode 3 : DHCPv6 avec état

DHCPv6 avec état est similaire à DHCP pour IPv4. Un périphérique peut recevoir automatiquement une GUA, une longueur de préfixe et les adresses des serveurs DNS à partir d'un serveur DHCPv6 avec état.

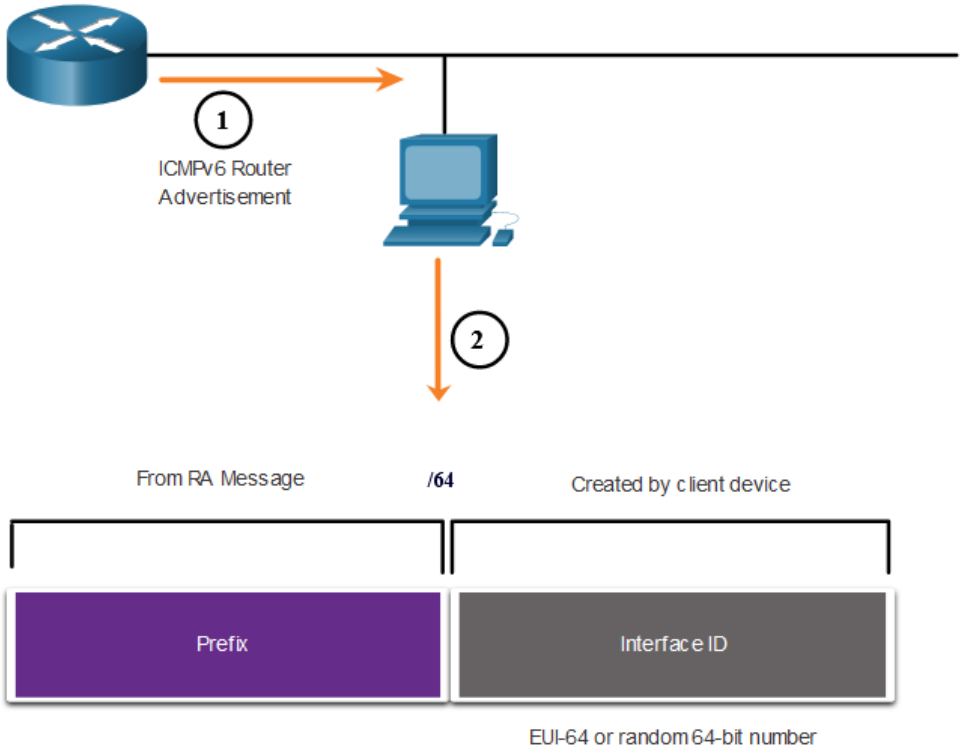
Le message RA suggère que les appareils utilisent les éléments suivants :

- l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut.
- un serveur DHCPv6 avec état pour obtenir une adresse de diffusion globale, l'adresse d'un serveur DNS, un nom de domaine et toutes les autres informations.



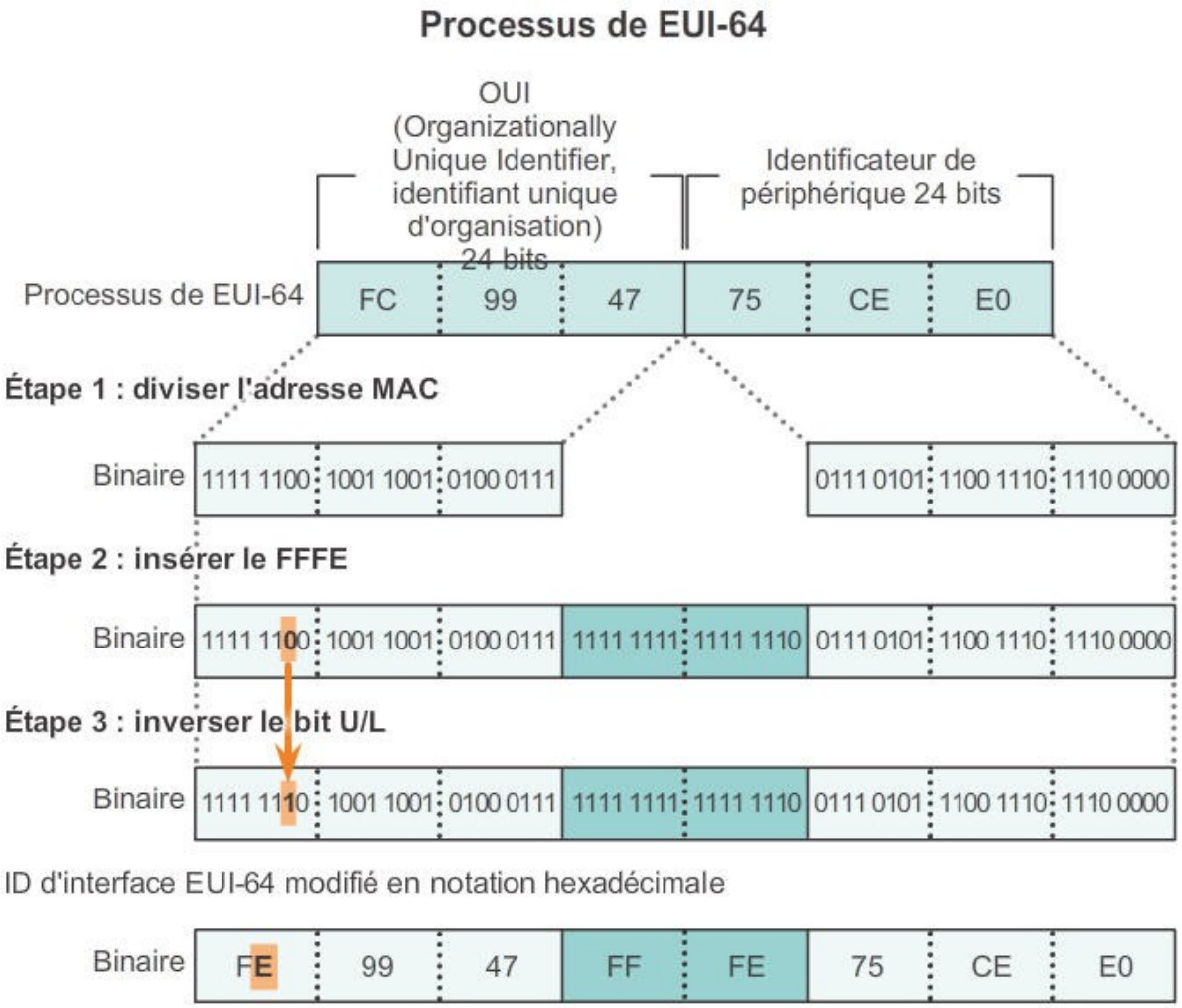
Génération aléatoire ou à l'aide de la méthode EUI-64

- Lorsque le message d'annonce de routeur est la SLAAC seule ou la SLAAC avec DHCPv6 sans état, le client doit générer lui-même son ID d'interface.
- L'interface ID peut utiliser la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement.



Adressage dynamique pour les IPv6 GUA

Génération aléatoire ou à l'aide de la méthode EUI-64



Génération aléatoire ou à l'aide de la méthode EUI-64

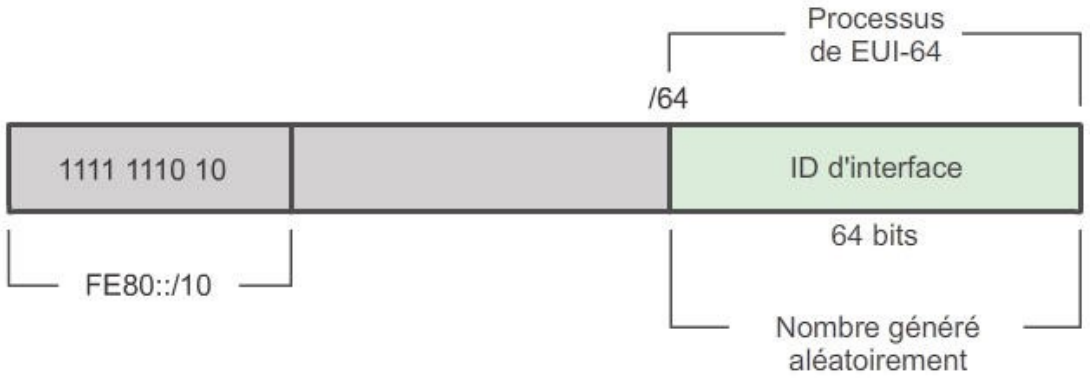
ID d'interface générés aléatoirement

- Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement plutôt que l'adresse MAC et le processus EUI-64
- À partir de Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec EUI-64
- Windows XP et les systèmes d'exploitation précédents utilisaient EUI-64

LLA dynamiques

Attribution dynamique

- L'adresse link-local est créée dynamiquement à l'aide du préfixe FE80::/10 et de l'ID d'interface



LLA dynamiques sous Windows

Les systèmes d'exploitation, tels que Windows, utiliseront généralement la même méthode pour une GUA créée par SLAAC et une LLA attribuée dynamiquement.

ID d'interface généré par la méthode EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . .: fe80::1
C:\ >
```

ID d'interface généré aléatoirement sur 64 bits

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . .: fe80::1
C:\ >
```

LLA dynamiques sur les routeurs

Les routeurs Cisco créent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée à l'interface. Par défaut, les routeurs Cisco IOS utilisent la méthode EUI-64 pour générer l'ID d'interface de toutes les adresses link-local sur des interfaces IPv6.

Voici un exemple d'un LLA configuré dynamiquement sur l'interface G0/0/0 de R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640  (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

Adresses link-local statiques

La configuration des adresses link-local

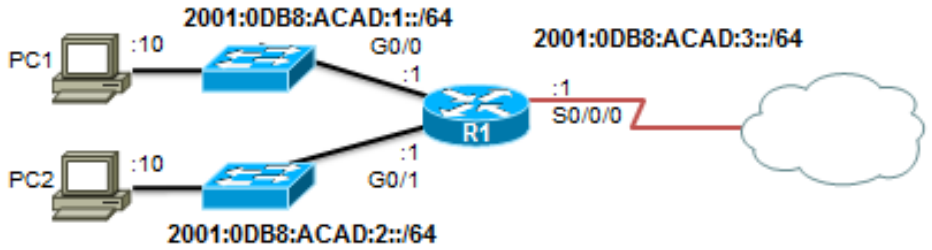
```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

Vérifier la configuration des adresses IPv6

Chaque interface possède deux adresses IPv6 -

1. l'adresse de monodiffusion globale qui a été configurée
2. une adresse de monodiffusion link-local commençant par FE80 est automatiquement ajoutée




```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

Les adresses de multidiffusion IPv6

- Les adresses de multidiffusion IPv6 ont le préfixe FF00::/8
- Il existe deux types d'adresses de multidiffusion IPv6 :
  - Les adresses de multidiffusion attribuées
  - Les adresses de multidiffusion de nœud sollicité

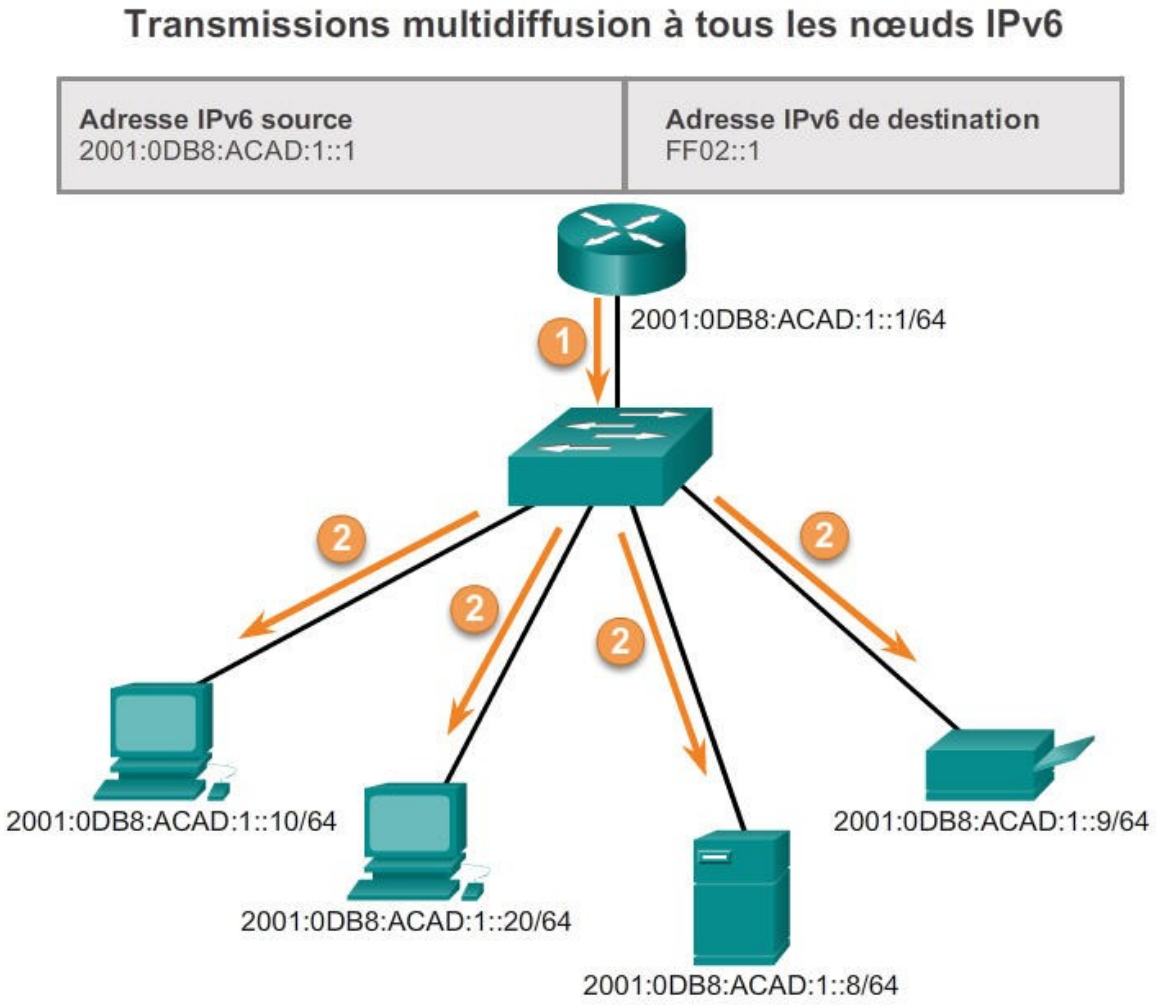
Remarque: les adresses de multidiffusion ne peuvent être que des adresses de destination et non des adresses source

Les adresses de multidiffusion IPv6 attribuées

Les deux groupes suivants de multidiffusion IPv6 attribuée sont les plus courants :

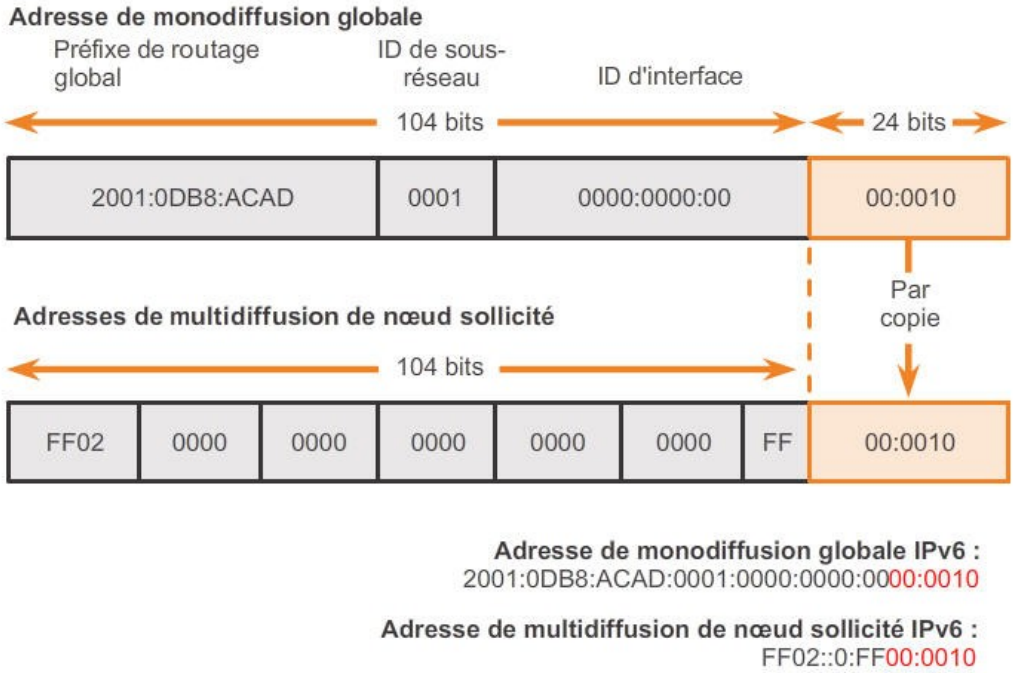
- **FF02::1 Groupe de multidiffusion avec tous les nœuds** –
  - Tous les périphériques IPv6 sont inclus
  - Même effet qu'une adresse de diffusion IPv4
- **FF02::2 Groupe de multidiffusion avec tous les routeurs** –
  - Tous les routeurs IPv6 sont inclus
  - Un routeur devient un membre de ce groupe 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 situés sur la liaison ou le réseau

Les adresses de multidiffusion IPv6 attribuées



Les adresses de multidiffusion IPv6 de nœud sollicité

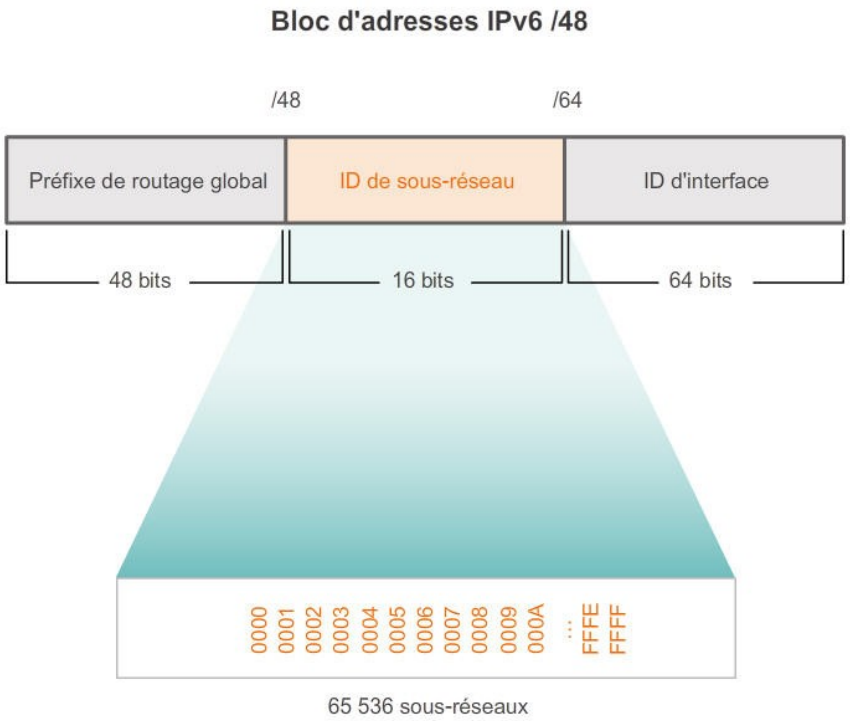
- Utilisées par NDP pour obtenir l'adresse physique

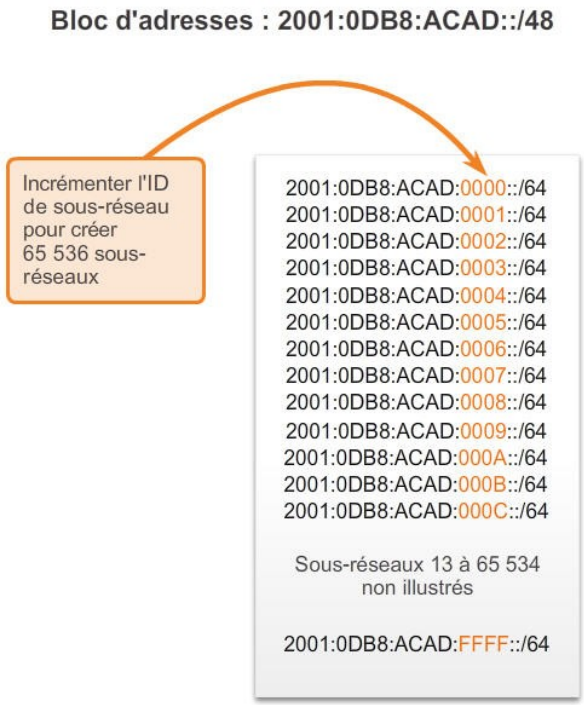


- Sont créées automatiquement lorsque la monodiffusion globale ou les adresses de monodiffusion link-local sont attribuées
- Permettent d'envoyer à tous les nœuds d'adresses IPv6 finissant par les 24 bits de l'adresse de nœud solicité
- Forment une solution efficace : la trame a une adresse de multidiffusion correspondant à l'adresse de multidiffusion IPv6

Segmenter le réseau en sous-réseaux à l'aide des ID

Un espace réseau IPv6 est segmenté en sous-réseaux afin de prendre en charge la conception hiérarchique et logique du réseau





Segmenter un réseau IPv6 en sous-réseaux

Attribution de sous-réseaux IPv6

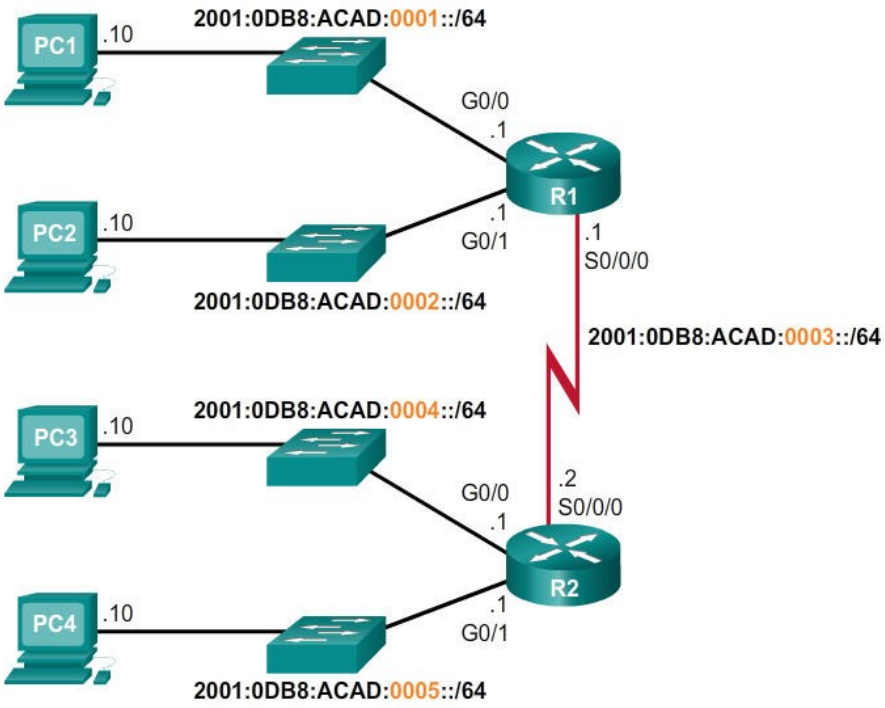
Sous-réseau IPv6

Bloc d'adresses : 2001:0DB8:ACAD::/48

5 sous-réseaux attribués parmi 65 536 sous-réseaux disponibles

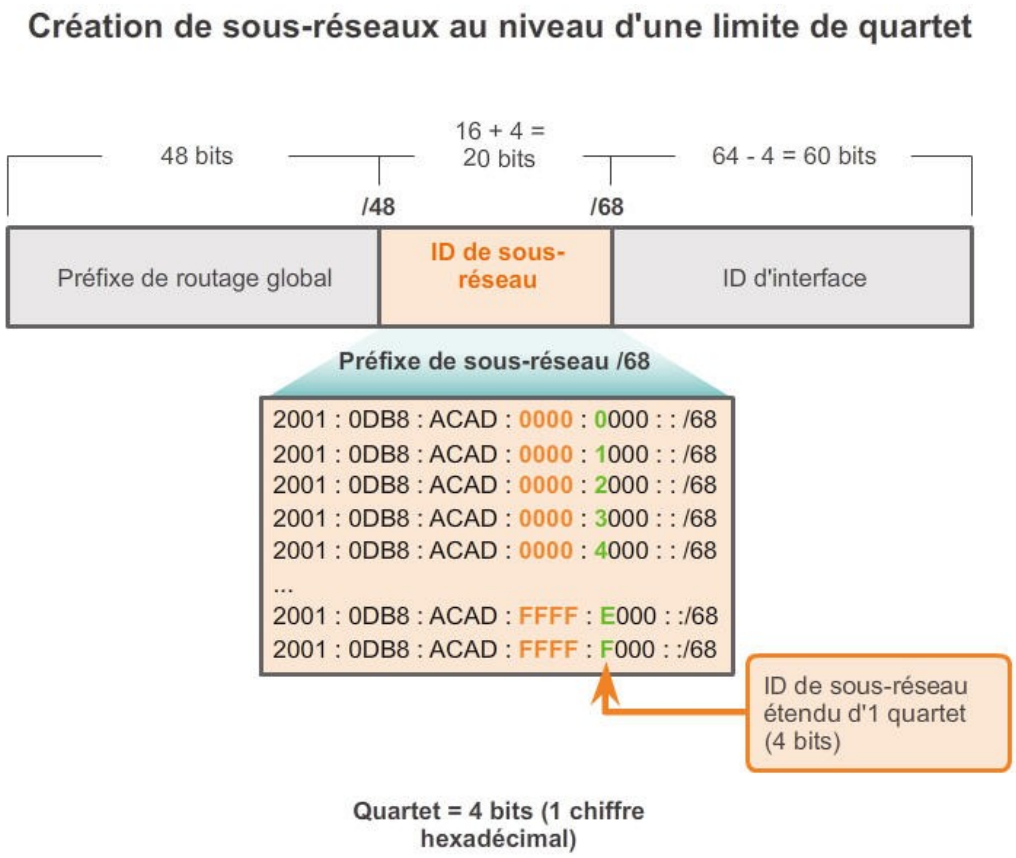
2001:0DB8:ACAD:0000::/64
2001:0DB8:ACAD:0001::/64
2001:0DB8:ACAD:0002::/64
2001:0DB8:ACAD:0003::/64
2001:0DB8:ACAD:0004::/64
2001:0DB8:ACAD:0005::/64
2001:0DB8:ACAD:0006::/64
2001:0DB8:ACAD:0007::/64
2001:0DB8:ACAD:0008::/64
:
2001:0DB8:ACAD:FFFF::/64

Attribution de sous-réseaux IPv6



Segmentation en sous-réseaux à partir de l'ID d'interface

Les bits IPv6 peuvent être empruntés à l'ID d'interface pour créer des sous-réseaux IPv6 supplémentaires



Résumé

- Expliquer la nécessité de l'adressage Ipv6
- Expliquer comment les adresses IPv6 sont représentées
- Comparer les types d'adresses réseau Ipv6
- Expliquer comment configurer des adresses de réseau IPv6 statiques de type monodiffusion globale et link-local
- Configurer les adresses de monodiffusion globale d'une façon dynamique
- Configurez dynamiquement les adresses lien-local
- Identifier des adresses Ipv6
- Mettre en œuvre un schéma d'adressage IPv6 divisé en sous-réseaux

Module 13 : ICMP

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

Les messages ICMPv4 et ICMPv6

- ICMP (*Internet Control Message Protocol*) fournit des commentaires sur les problèmes liés au traitement des paquets IP sous certaines conditions
- ICMPv4 est le protocole de message des réseaux IPv4. ICMPv6 est le protocole de messagerie pour IPv6 et inclut des fonctionnalités supplémentaires
- Les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants:
  - Accessibilité de l'Hôte
  - Destination ou service inaccessible
  - Délai dépassé

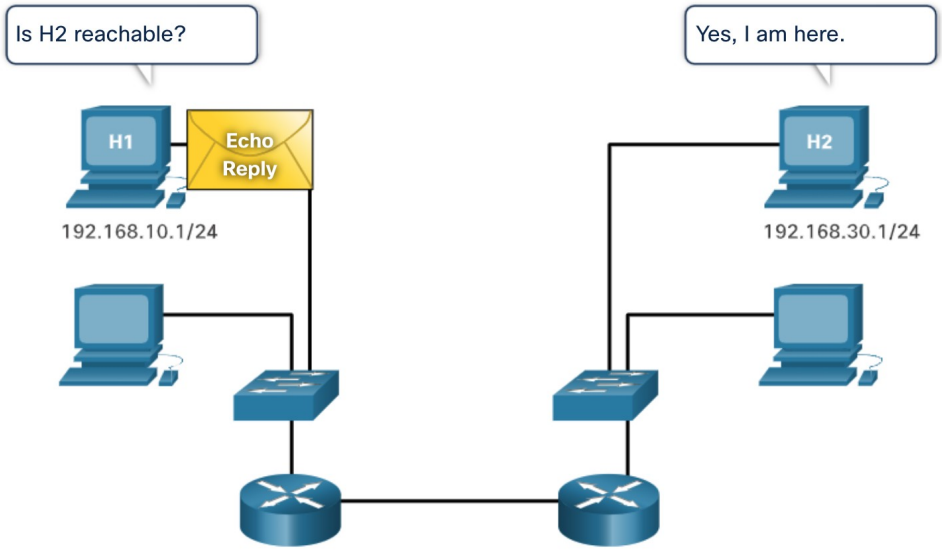
Remarque : les messages ICMPv4 ne sont pas obligatoires et ne sont souvent pas autorisés au sein d'un réseau pour des raisons de sécurité

Accessibilité de l’hôte

ICMP *Echo Message* peut être utilisé pour tester l'accessibilité d'un hôte sur un réseau IP.

Dans l'exemple:

- L’hôte local envoie un message ICMP *Echo Request* (Demande d’écho) à un autre hôte.
- Si l'hôte est disponible, l'hôte de destination répond en envoyant une réponse d'écho.



Accessibilité de l'hôte

- Un message ICMP Destination Inaccessible peut être utilisé pour avertir la source qu'une destination ou un service est inaccessible.
- Ce message comprend un code indiquant pourquoi le paquet n'a pas pu être livré.

Certains des codes de Destination Inaccessible pour l'ICMPv4 sont:

- 0 - Réseau inaccessible
- 1 - Hôte inaccessible
- 2 - Protocole inaccessible
- 3 - Port inaccessible

Certains des codes de Destination Inaccessible pour l'ICMPv6 sont:

- 0 - Pas de route vers la destination
- 1 - La communication avec la destination est interdite administrativement (p. ex., pare-feu)
- 2 - Au-delà de la portée de l'adresse source
- 3 - Adresse inaccessible
- 4 - Port inaccessible

Remarque: ICMPv6 a des codes similaires mais légèrement différents pour les messages "Destination Inaccessible".

Délai dépassé

- Lorsque le champ Durée de vie (TTL) d'un paquet est décrémenté à 0, un message ICMPv4 Délai dépassé est envoyé à l'hôte source.
- ICMPv6 envoie également un message Délai dépassé. Au lieu du champ TTL IPv4, ICMPv6 utilise le champ *Hop Limit* IPv6 pour déterminer si le paquet a expiré.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Messages ICMPv6

ICMPv6 dispose de nouvelles fonctionnalités et fonctionnalités améliorées introuvables dans ICMPv4, y compris quatre nouveaux protocoles dans le cadre du *Neighbor Discovery Protocol* (ND ou NDP).

La messagerie entre un routeur IPv6 et un périphérique IPv6, y compris l'allocation d'adresses dynamique, est la suivante:

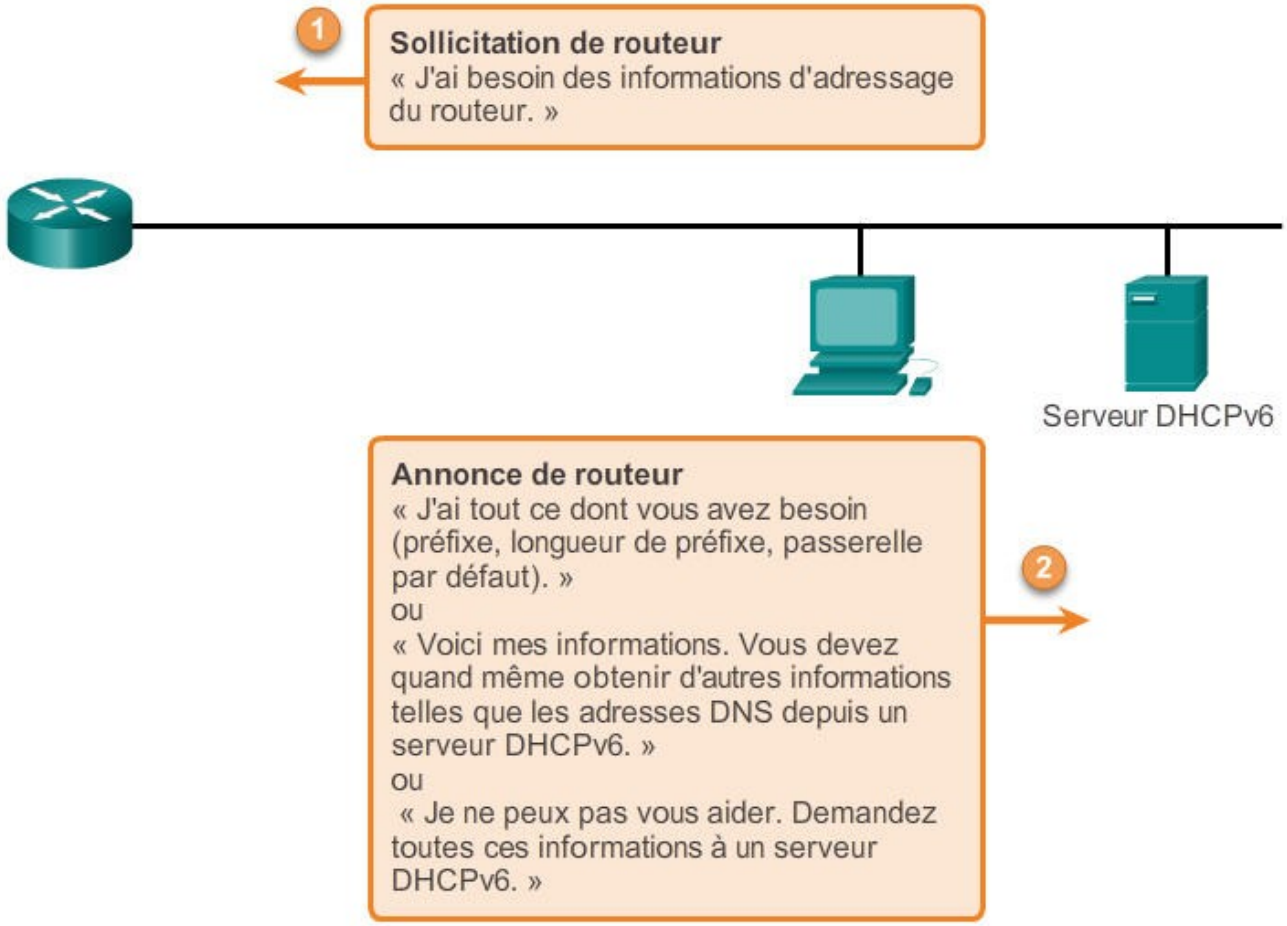
- Message de sollicitation de routeur (RS)
- Message d'annonce de routeur (RA)

La messagerie entre les périphériques IPv6, y compris la détection d'adresses en double et la résolution d'adresses, est la suivante:

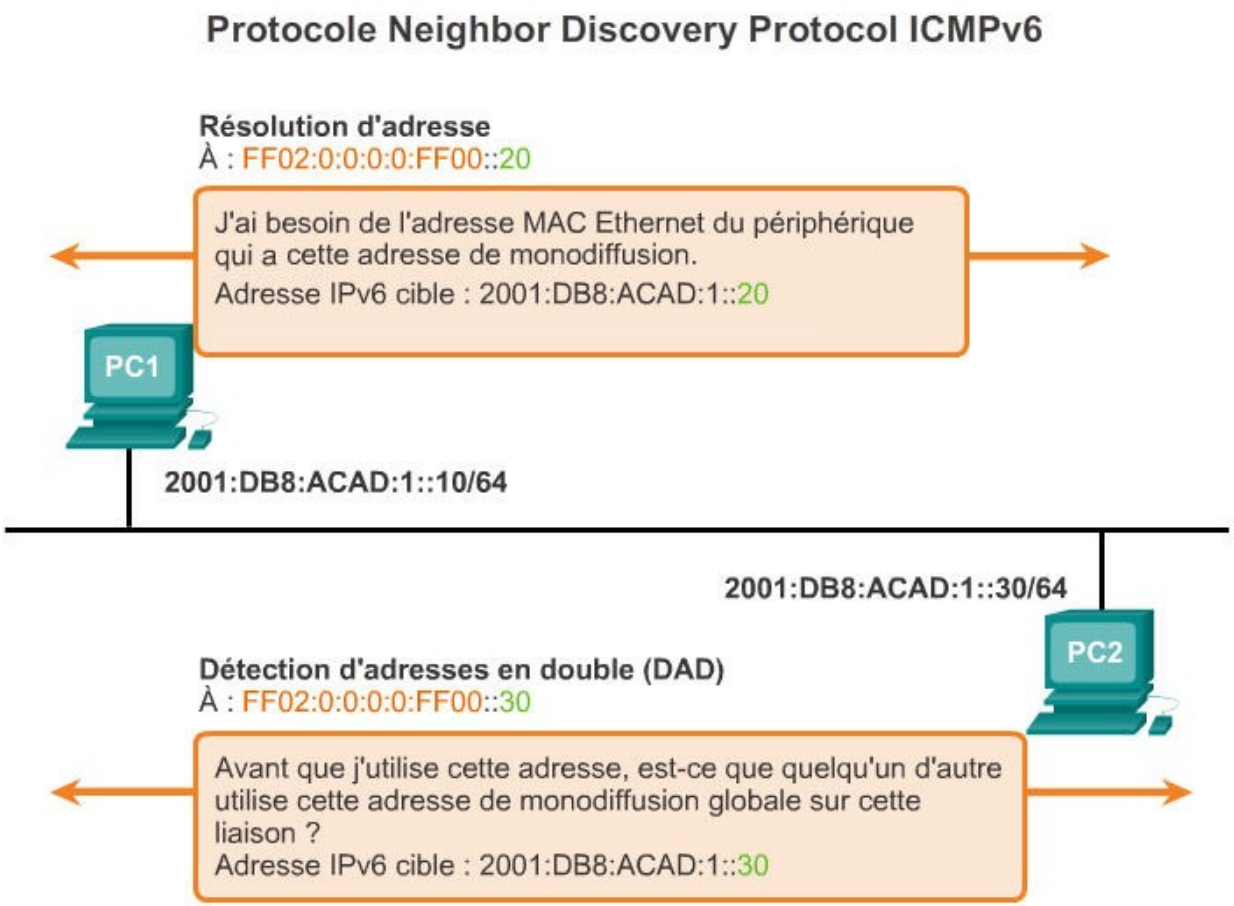
- Message de sollicitation de voisin (NS)
- Messages d'annonce de voisin (NA)

Remarque: ICMPv6 ND inclut également le message de redirection, qui comporte une fonction similaire au message de redirection utilisé dans l'ICMPv4.

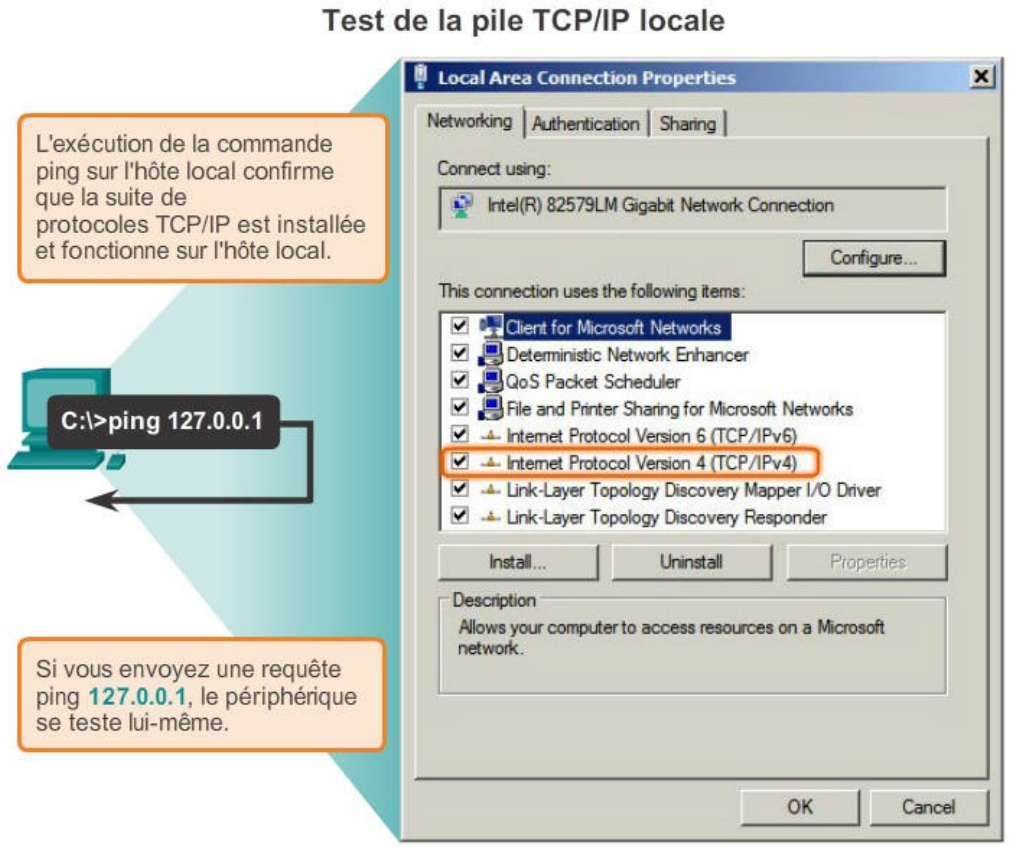
Les messages de sollicitation et d'annonce de routeur ICMPv6



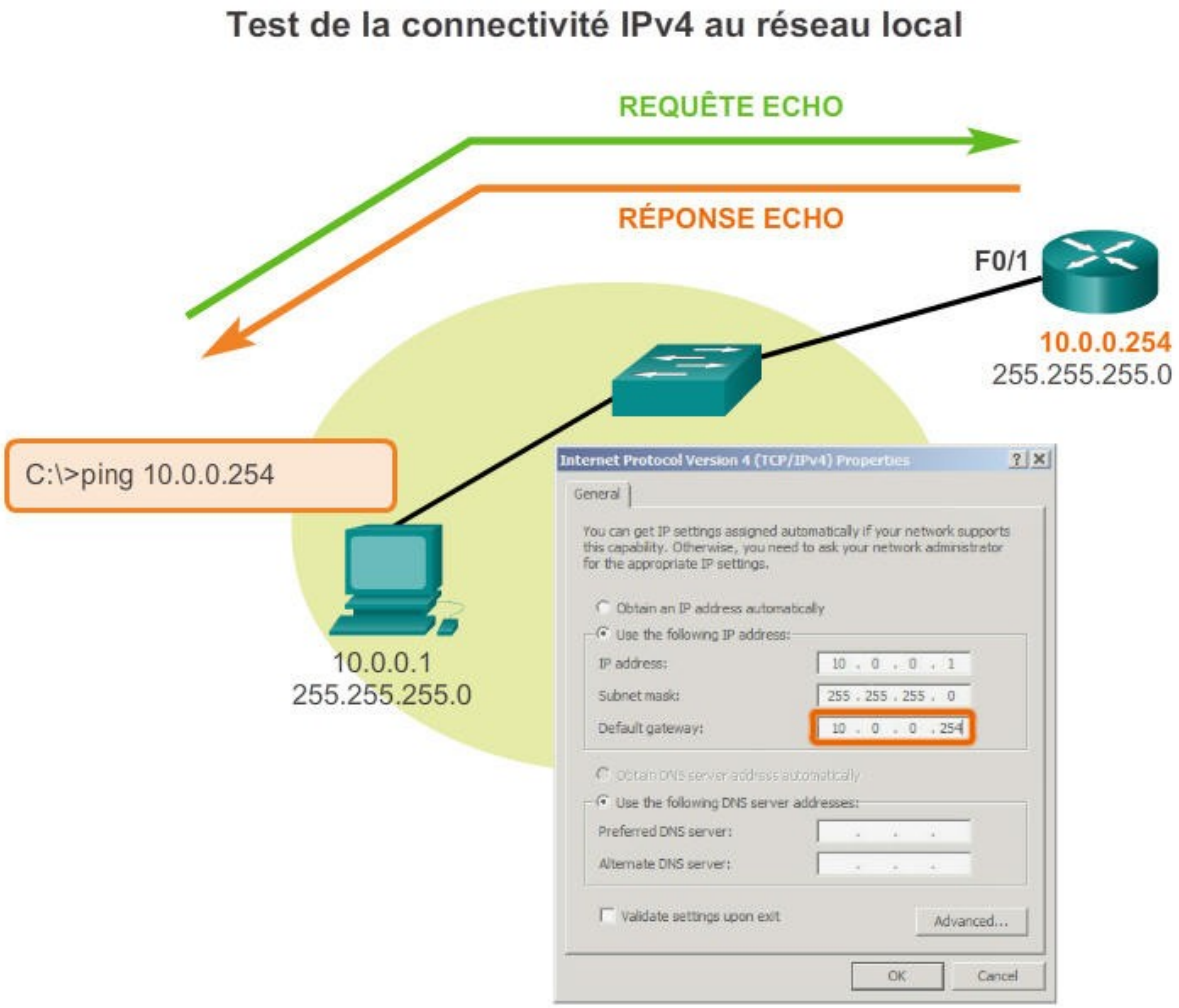
Les messages de sollicitation et d'annonce de voisin ICMPv6



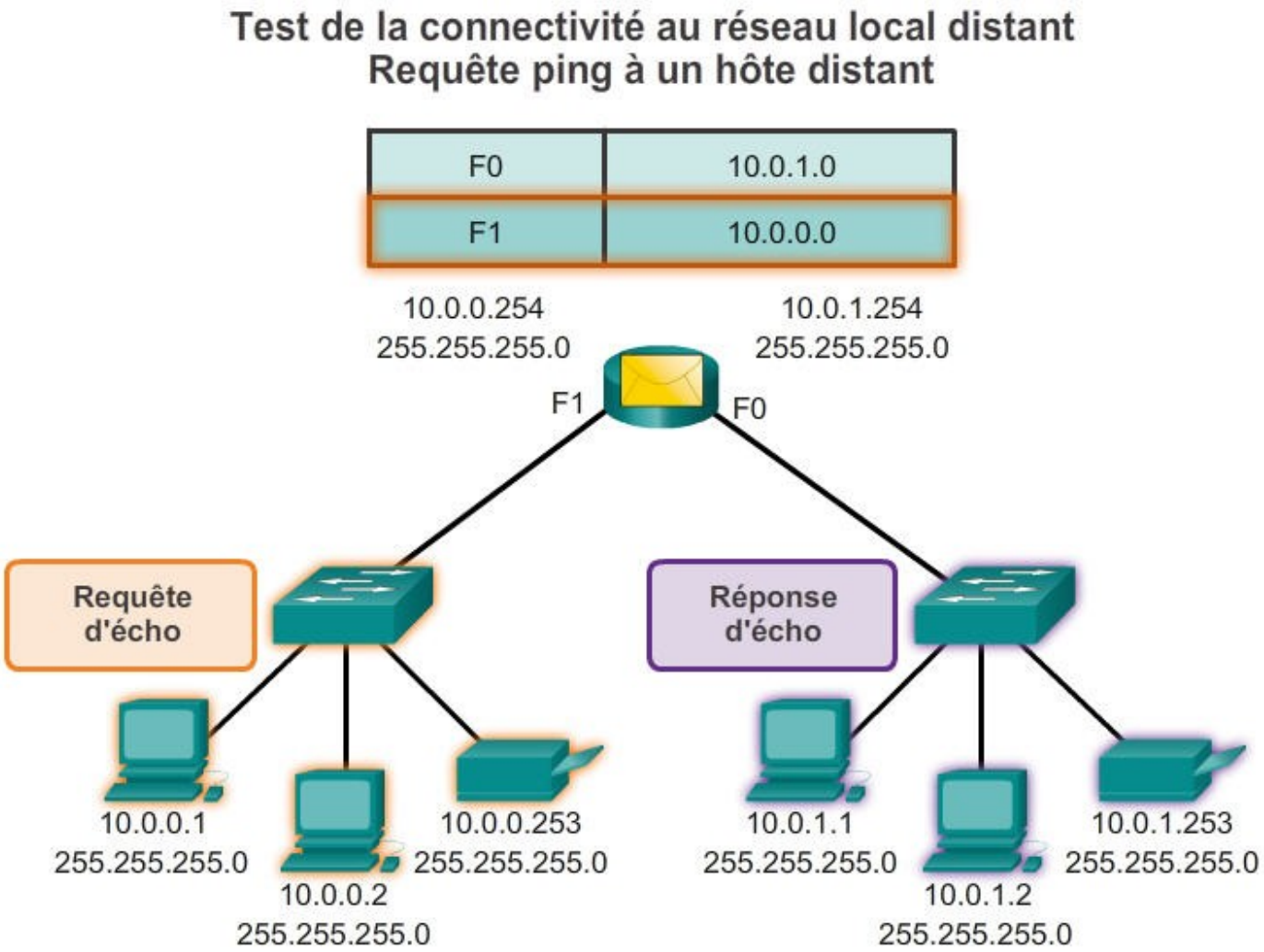
Ping - Tester la pile locale



Ping – Tester la connectivité au réseau local



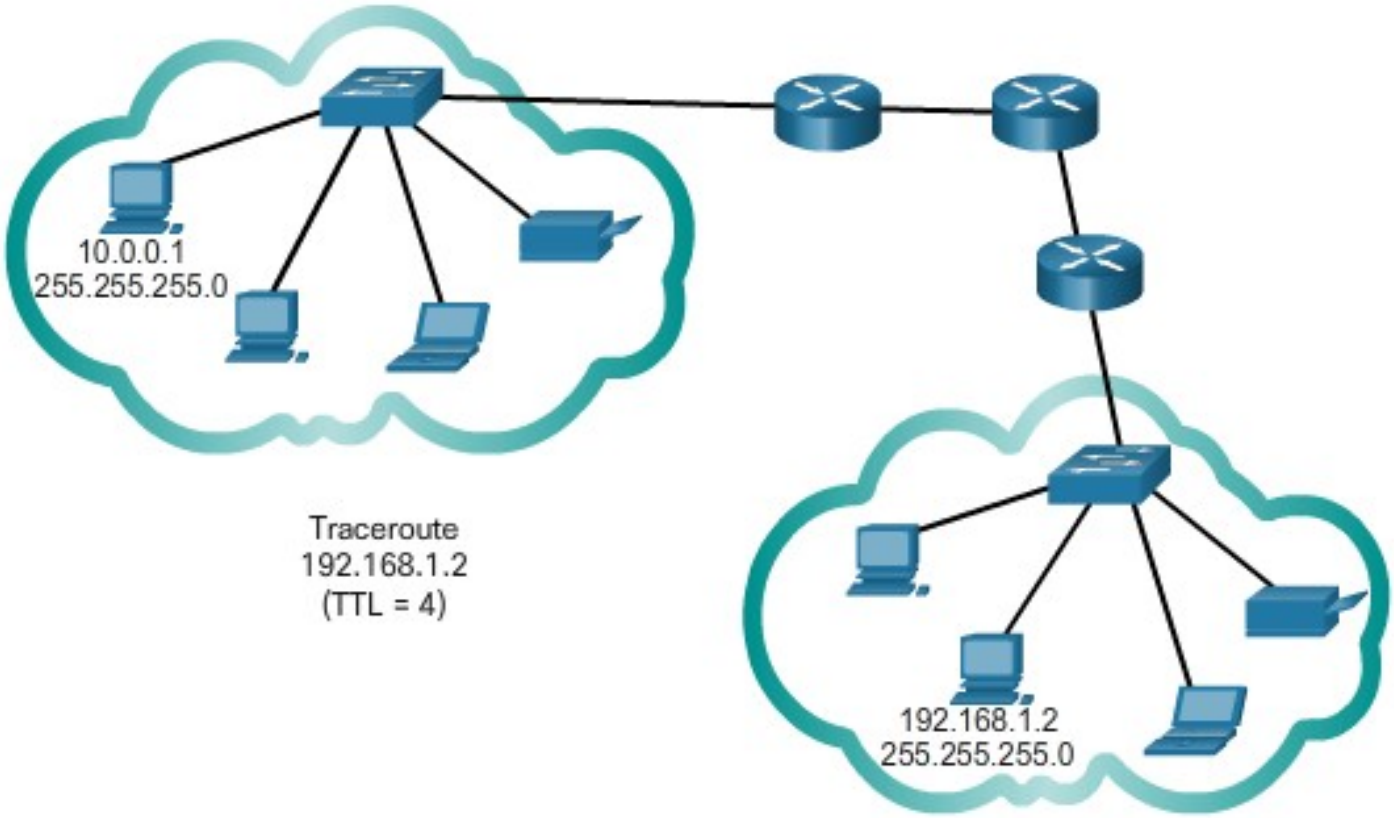
Ping – Tester la connectivité à distance



Traceroute – Tester le chemin

Traceroute (tracert sous Windows)

- Durée de transmission ou RTT (Round Trip Time)
- TTL IPv4 et limite du nombre de tronçons IPv6



Résumé

- Expliquer comment le protocole ICMP sert à tester la connectivité du réseau
- Utiliser les utilitaires Ping et Traceroute pour tester la connectivité du réseau