# SOMMAIRE

## 1. Adresses réseau IPV4 :

### 1.1 Adresses IPV4 :

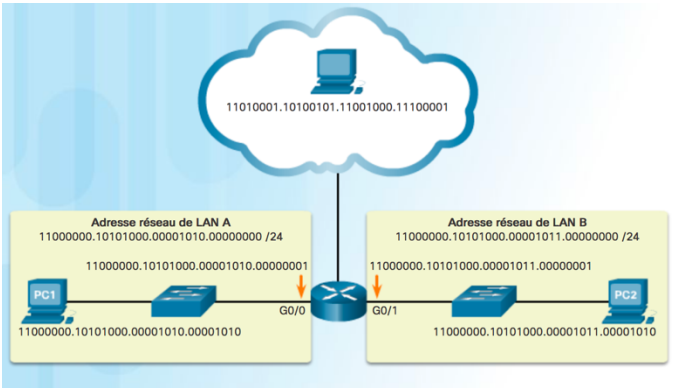



figure 1

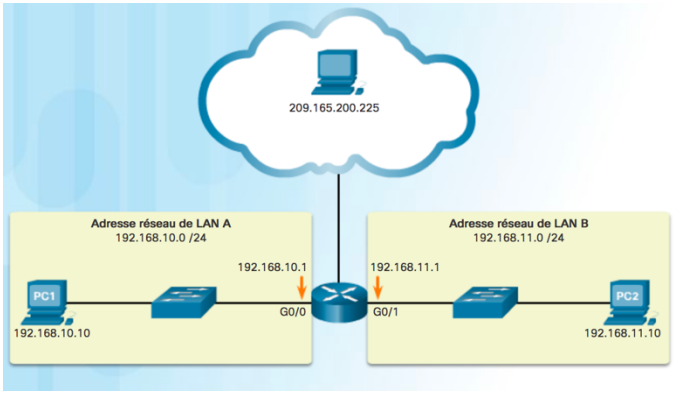



figure 2

Le format binaire est un système de numération utilisant les chiffres 0 et 1 qui sont appelés des *bit*. Le système de numération décimal utilise 10 chiffres, de 0 à 9.

Il est important de comprendre le système binaire puisque les hôtes, les serveurs et les périphériques réseau utilisent l'adressage binaire. Plus précisément, ils utilisent des adresses IPv4 binaires pour s'identifier, comme le montre la figure 1.

Chaque adresse est une chaîne de 32 bits divisée en quatre parties appelées *octets*. Chaque octet contient 8 bits séparés par un point. Par exemple, sur la figure, l'adresse IPv4 de PC1 est 11000000.10101000.00001010.00001010. L'adresse de sa passerelle par défaut serait celle de l'interface Gigabit Ethernet de R1, 11000000.10101000.00001010.00000001. Il peut être difficile de s'en sortir avec les nombres binaires. Pour simplifier leur utilisation, les adresses IPv4 sont souvent exprimées en notation décimale à point, comme à la figure 2. L'adresse IPv4 de PC1 est 192.168.10.10 et celle de sa passerelle par défaut est 192.168.10.1.

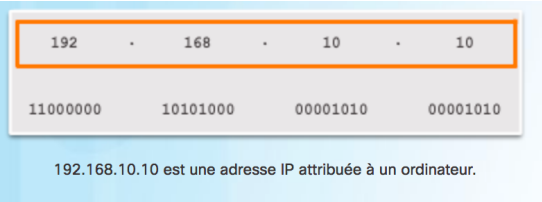
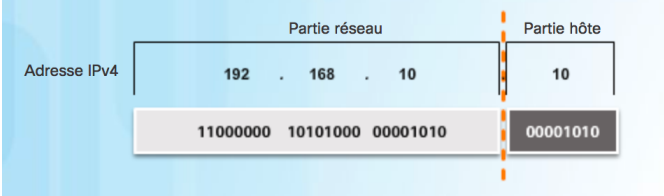



figure 3

La figure 3 compare l'adresse de PC1 au format décimal à point et au format binaire 32 bits. Pour bien comprendre l'adressage réseau, il est important de connaître l'adressage binaire et de s'entraîner à convertir des adresses IPv4 entre le format binaire et le format décimal à point.

## 1.2 Parties réseau et hôte :

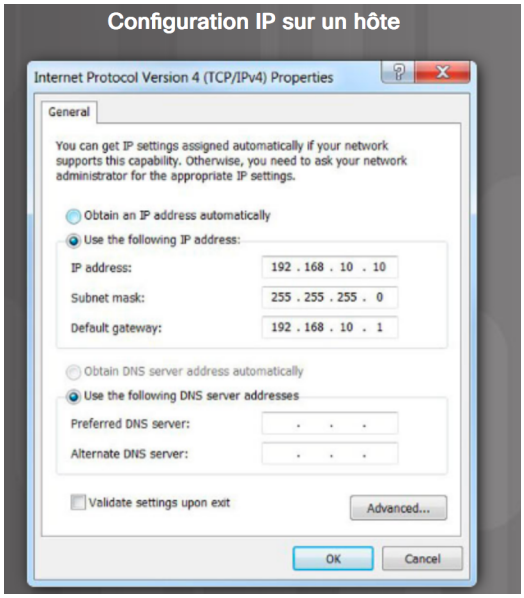


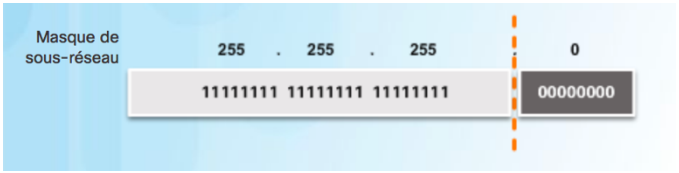

Il est important de comprendre la notation binaire pour déterminer si deux hôtes se trouvent sur le même réseau. Rappelez-vous qu'une adresse IPv4 est une adresse hiérarchique qui se compose d'une partie réseau et d'une partie hôte. Lorsque vous déterminez la partie réseau et la partie hôte, il est nécessaire d'examiner le flux de 32 bits. Dans le flux de 32 bits, une partie des bits constitue la partie réseau et une autre partie des bits compose la partie hôte, comme le montre la figure ci-contre.

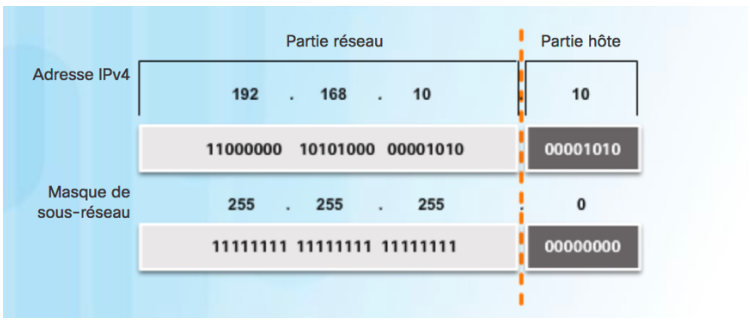
Les bits de la partie réseau de l'adresse doivent être identiques pour tous les périphériques installés sur le même réseau. Les bits de la partie hôte de l'adresse doivent être uniques, pour identifier un hôte spécifique dans un réseau. Si la partie réseau du flux de 32 bits est la même sur deux hôtes, ces deux hôtes résident sur le même réseau.

Mais comment les hôtes repèrent-ils la portion du flux de 32 bits qui représente la partie réseau par rapport à celle qui représente la partie hôte ? Le *masque de sous-réseau* permet de le savoir.

## 1.3 Masque de sous-réseau :




Comme le montre la figure de gauche, la configuration IPv4 d'un hôte comprend trois adresses IPv4 décimales à point :

- **l'adresse IPv4**, qui est l'adresse IPv4 unique de l'hôte,
- **le masque de sous-réseau**, qui sert à identifier la partie réseau et la partie hôte d'une adresse IPv4,
- **la passerelle par défaut**, qui indique la passerelle locale (c'est-à-dire l'adresse IPv4 de l'interface du routeur local) permettant d'atteindre les réseaux distants.

Lorsqu'une adresse IPv4 est attribuée à un périphérique, le masque de sous-réseau est utilisé pour déterminer l'adresse du réseau auquel le périphérique appartient. L'adresse réseau représente tous les périphériques du même réseau.

La figure en haut, à droite indique l'adresse au format décimal à point et le masque de sous-réseau 32 bits. Notez que le masque de sous-réseau est en fait une séquence de bits 1 suivie d'une séquence de bits 0.

Pour identifier les parties réseau et hôte d'une adresse IPv4, chaque bit du masque de sous-réseau est comparé à l'adresse IPv4, de gauche à droite, comme le montre la figure en bas, à droite. Les 1 dans le masque de sous-réseau représentent la partie réseau, et les 0 représentent la partie hôte. Notez que le masque de sous-réseau ne contient pas réellement la partie réseau ou hôte d'une adresse IPv4 : il indique uniquement à l'ordinateur où rechercher ces parties dans une adresse IPv4 donnée.

En réalité, le processus utilisé pour identifier la partie réseau et la partie hôte est appelé l'opération AND.

### 1.4 Longueur de préfixe :

| Masque de sous-réseau | Adresse 32 bits | Longueur de préfixe |
|---|---|---|
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

Il peut devenir fastidieux d'exprimer les adresses réseau et les adresses d'hôtes avec l'adresse du masque de sous-réseau au format décimal à point. Heureusement, il existe une méthode plus rapide d'identification du masque de sous-réseau, appelée la longueur de préfixe.

En fait, la longueur de préfixe correspond au nombre de bits définis sur 1 dans le masque de sous-réseau. Elle est notée au moyen de la « notation de barre oblique », soit le signe « / » suivi du nombre de bits définis sur 1. Il suffit donc de compter le nombre de bits du masque de sous-réseau et d'y ajouter une barre oblique.

Pour voir un exemple, reportez-vous au tableau ci-contre. La première colonne contient la liste des masques de sous-réseau qui peuvent être utilisés avec une adresse d'hôte. La deuxième colonne indique l'adresse binaire 32 bits convertie. La dernière colonne affiche la longueur de préfixe obtenue.

Nous verrons plus tard pourquoi différents types de longueur de préfixe sont utilisées. Pour l'instant, nous allons nous concentrer sur le masque de sous-réseau /24, c'est-à-dire (255.255.255.0).

## 1.5 Adresses réseau, d'hôte et de diffusion :

Chaque adresse réseau contient (ou identifie) des adresses d'hôtes et une adresse de diffusion, comme décrit à la figure 1.

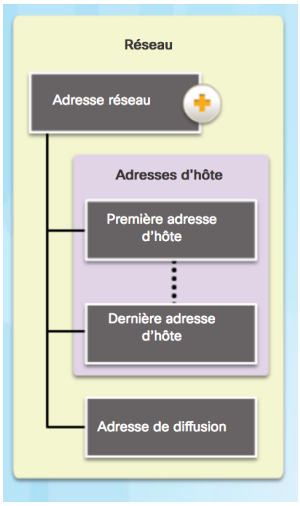



figure 1

La figure 2 dresse la liste des adresses du réseau 192.168.10.0 /24 et les décrit.
Pour étudier un autre exemple, consultez les figures 3 à 7. Sur ces figures, notez que la partie réseau des adresses reste inchangée, contrairement à la partie hôte.

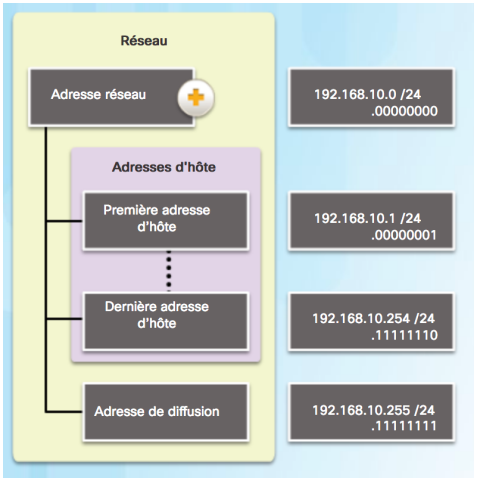



figure 2

La figure 3 illustre l'adresse réseau 10.1.1.0 /24. Les bits d'hôte sont tous des 0.

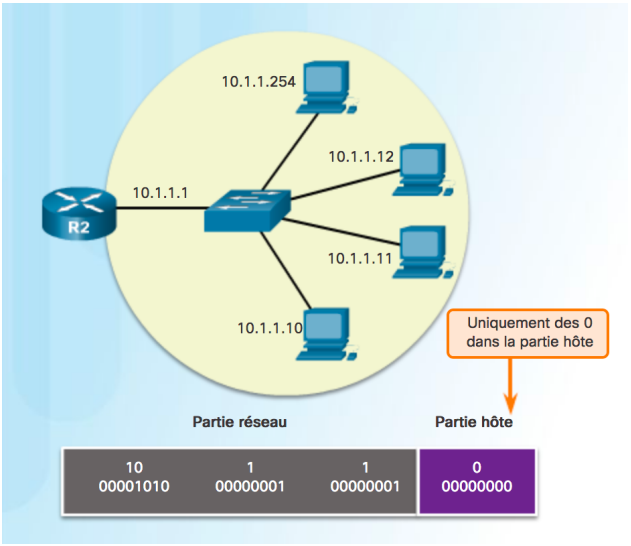



figure 3

La figure 4 illustre l'adresse d'hôte IPv4 10.1.1.10. Les bits d'hôte sont des 0 et des 1.

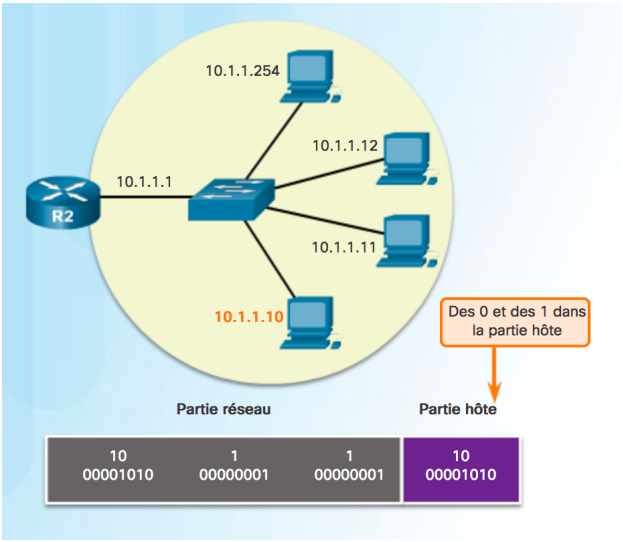



figure 4

La figure 5 illustre l'adresse IPv4 du premier hôte, 10.1.1.1. Les bits d'hôte sont tous des 0 sauf un. Notez qu'elle est attribuée à l'interface du routeur et deviendrait donc la passerelle par défaut de tous les hôtes sur ce réseau.

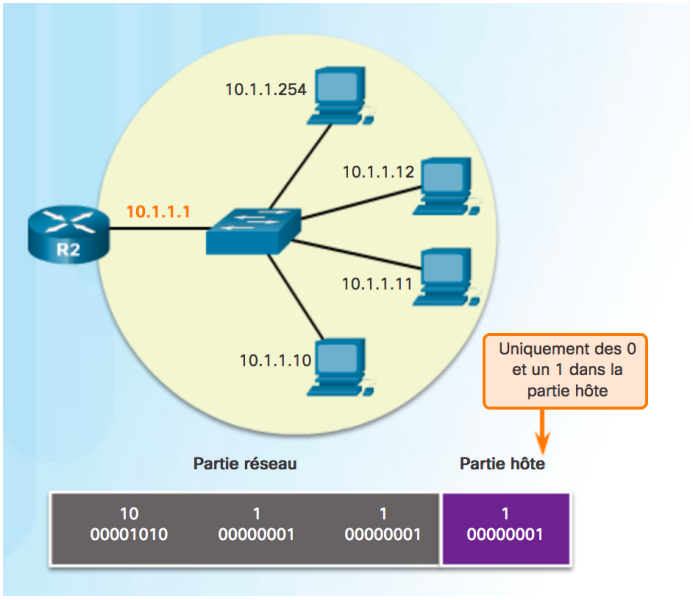



figure 5

La figure 6 illustre l'adresse IPv4 du dernier hôte, 10.1.1.254. Les bits d'hôte sont tous des 1 sauf un.

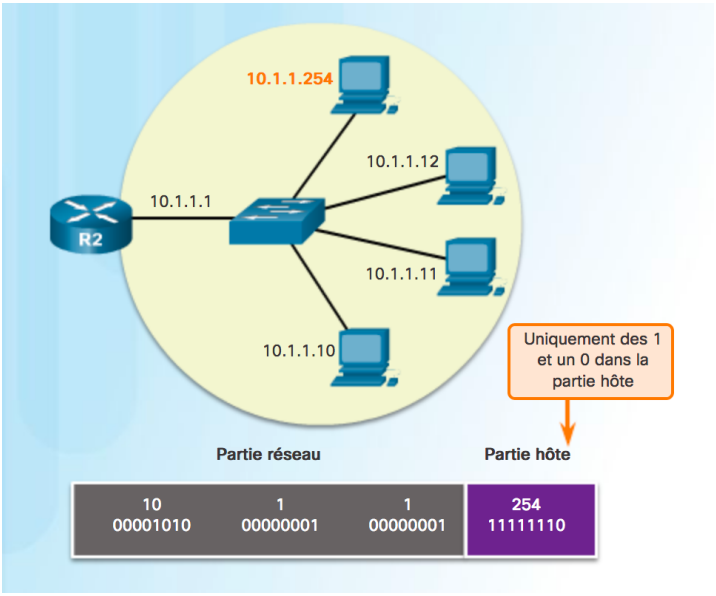



figure 6

La figure 7 illustre l'adresse de diffusion, 10.1.1.255. Les bits d'hôte sont tous des 1.
Les concepts abordés dans ce sujet constituent la base de l'adressage IPv4. Assurez-vous de bien comprendre comment une adresse réseau identifie une partie réseau et une partie hôte à l'aide du masque de sous-réseau ou de la longueur de préfixe et de l'opération AND. Notez également les différents types d'adresses réseau présentes dans un réseau.

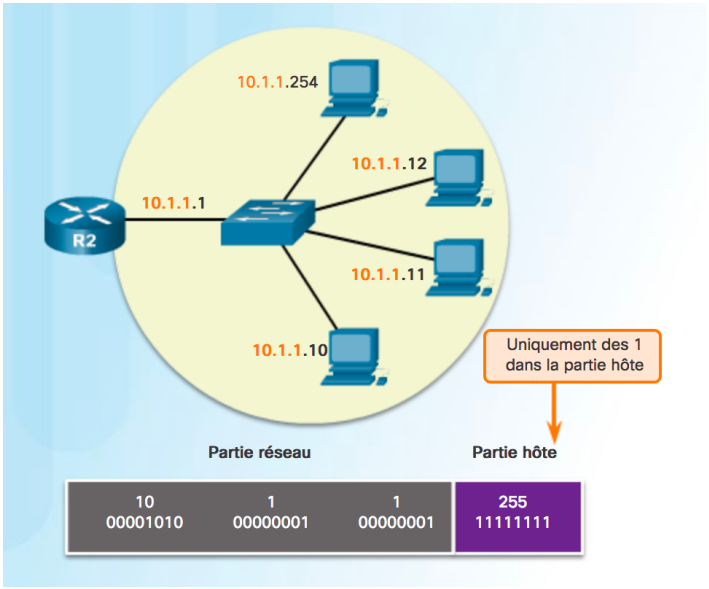
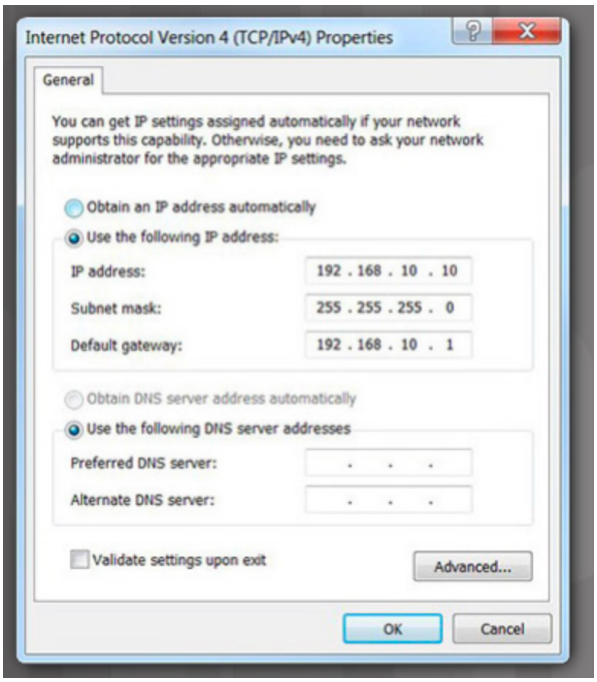



figure 7

### 1.6 Attribution d'une adresse IPV4 statique à un hôte.

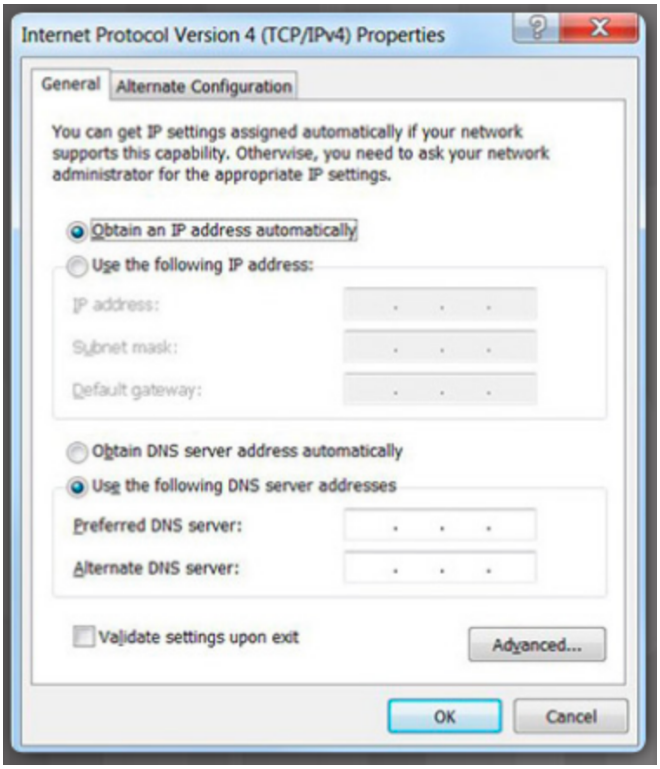



Les adresses IP peuvent être attribuées aux périphériques de manière statique ou dynamique.

Sur les réseaux, certains périphériques doivent avoir une adresse IP fixe. Par exemple, les imprimantes, serveurs et périphériques réseau doivent conserver la même adresse IP. De ce fait, une adresse IP statique leur est généralement attribuée.

Il est également possible d'attribuer une adresse IPv4 statique à un hôte, comme l'illustre la figure ci-contre. L'attribution d'adresses IP statiques aux hôtes est une pratique acceptable dans les petits réseaux. Toutefois, il serait fastidieux de saisir des adresses statiques sur chaque hôte d'un grand réseau. Il est important de tenir à jour une liste exacte des adresses IP statiques attribuées à chaque périphérique.

### 1.7 Attribution d'une adresse IPV4 dynamique à un hôte.




Dans la plupart des réseaux de données, les hôtes sont principalement des ordinateurs, des tablettes, des smartphones, des imprimantes et des téléphones IP. Bien souvent, les utilisateurs et leurs périphériques changent fréquemment. Il serait donc impossible d'attribuer des adresses IPv4 statiques à chaque périphérique. C'est pourquoi on leur attribue des adresses IPv4 de manière dynamique à l'aide du protocole DHCP (Dynamic Host Configuration Protocol).

Comme illustré sur la figure, un hôte peut obtenir automatiquement des informations d'adressage IPv4. L'hôte est un client DHCP qui demande des informations d'adresse IPv4 à un serveur DHCP. Le serveur DHCP lui fournit une adresse IPv4, un masque de sous-réseau, une passerelle par défaut et d'autres informations de configuration.

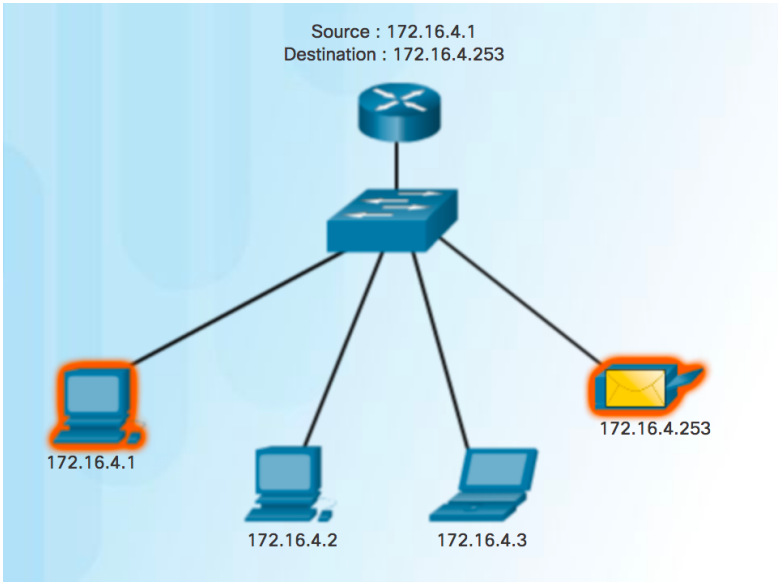
Sur les grands réseaux, la méthode DHCP est généralement privilégiée pour l'attribution des adresses IPv4. L'autre avantage de cette méthode réside dans le fait que les adresses ne sont pas attribuées aux hôtes de manière permanente, elles sont uniquement « louées » pour une certaine durée. Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée. Cela est particulièrement intéressant pour les utilisateurs mobiles qui se connectent et se déconnectent d'un réseau.

## 1.8 Transmission monodiffusion.

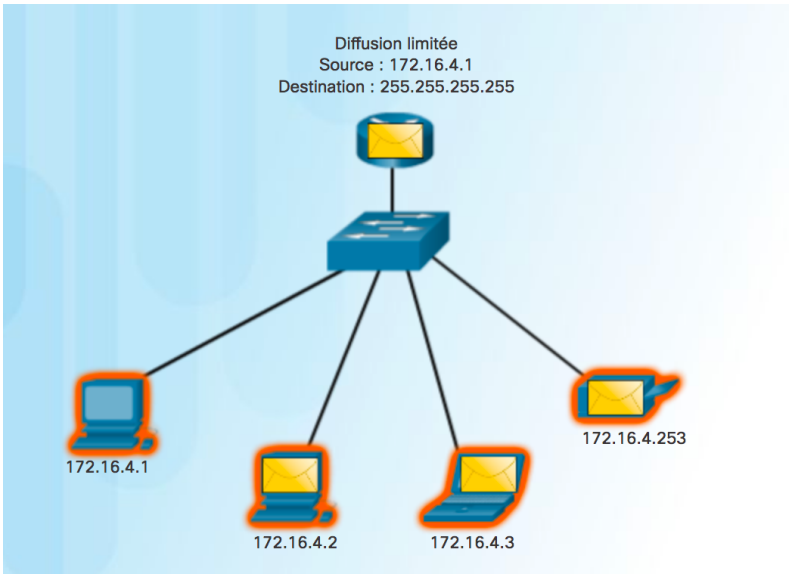
Un hôte connecté à un réseau peut communiquer avec les autres périphériques de trois façons :

- **la monodiffusion** : processus consistant à envoyer un paquet d'un hôte à un autre.
- **la diffusion** : processus consistant à envoyer un paquet d'un hôte à tous les autres hôtes du réseau.
- **la multidiffusion** : processus consistant à envoyer un paquet d'un hôte à un groupe d'hôtes spécifique (qui peuvent se trouver sur différents réseaux).

Ces trois types de communication sont utilisés à des fins différentes dans les réseaux de données. Dans les trois cas, l'adresse IPv4 de l'hôte émetteur est placée dans l'en-tête du paquet comme adresse source.




## 1.9 Transmission de diffusion.

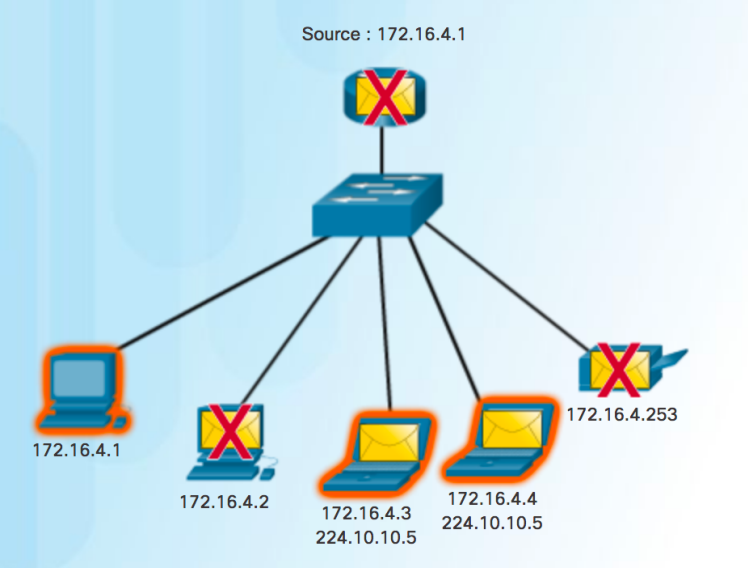


Le trafic de diffusion est utilisé pour envoyer des paquets à tous les hôtes du réseau grâce à l'adresse de diffusion du réseau. En diffusion, le paquet contient une adresse IPv4 de destination avec uniquement des un (1) dans la partie hôte. Cela signifie que tous les hôtes se trouvant sur ce réseau local (domaine de diffusion) recevront le paquet et le regarderont. De nombreux protocoles réseau, tels que DHCP, utilisent les diffusions. Lorsqu'un hôte reçoit un paquet envoyé à l'adresse de diffusion du réseau, il traite le paquet comme s'il s'agissait d'un paquet adressé à son adresse de monodiffusion.

La diffusion peut être dirigée ou limitée. Une diffusion dirigée est envoyée à tous les hôtes d'un réseau particulier. Par exemple, un hôte sur le réseau 172.16.4.0/24 envoie un paquet à 172.16.4.255. Une diffusion limitée est envoyée à 255.255.255.255. Par défaut, les routeurs ne transfèrent pas les diffusions.

Lorsqu'un paquet est diffusé, il utilise les ressources du réseau et est traité par chaque hôte destinataire sur le réseau. Ainsi, le trafic de diffusion devrait être limité de sorte qu'il ne réduise pas les performances du réseau ou des périphériques. Dans la mesure où les routeurs séparent les domaines de diffusion, la création de sous-réseaux peut améliorer les performances du réseau en éliminant le trafic de diffusion excessif.

## 1.10 Transmission de multidiffusion.



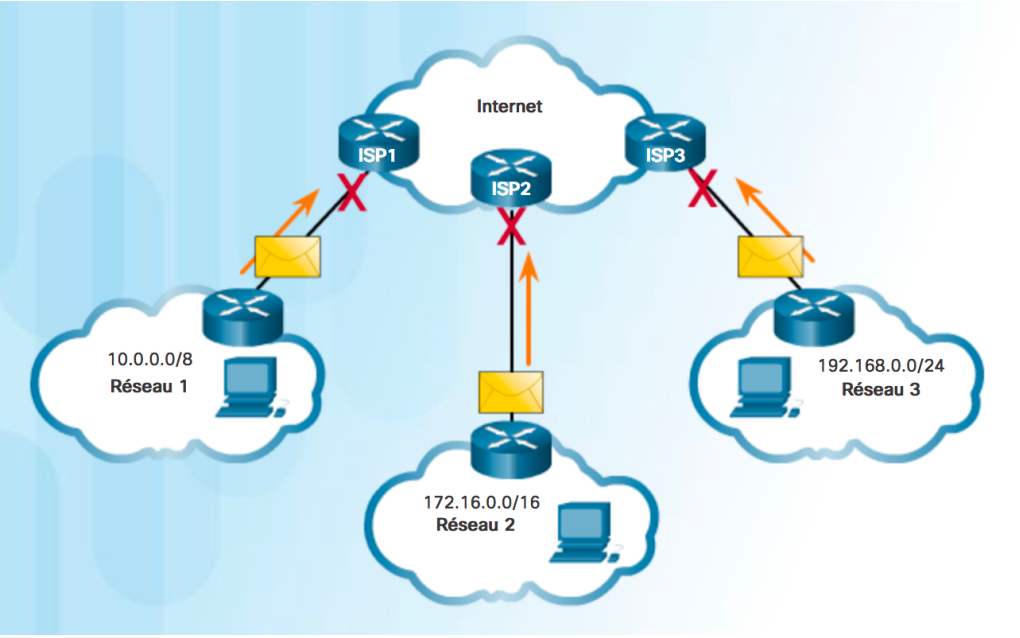

La transmission multidiffusion réduit le volume du trafic en permettant à un hôte d'envoyer un seul paquet à un groupe d'hôtes désigné inscrits à un groupe de multidiffusion.

IPv4 a réservé les adresses 224.0.0.0 à 239.255.255.255 comme plage de multidiffusion. Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 à 224.0.0.255 sont réservées à la multidiffusion sur le réseau local uniquement. Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local. Un routeur connecté au réseau local sait reconnaître que ces paquets sont adressés à un groupe de multidiffusion d'un réseau local et ne les transmet jamais. Les adresses de multidiffusion de réseau local réservées s'appliquent principalement aux protocoles de routage qui utilisent la transmission multidiffusion pour échanger des informations de routage. Par exemple, 224.0.0.9 est l'adresse de multidiffusion utilisée par le protocole RIP (Routing Information Protocol) version 2 pour communiquer avec d'autres routeurs RIPv2.

Les hôtes qui reçoivent des données multidiffusion spécifiques sont appelés des « clients multidiffusion ». Ces derniers font appel à des services demandés par un programme client pour s'abonner au groupe de multidiffusion.

Chaque groupe de multidiffusion est représenté par une seule adresse de destination multidiffusion IPv4. Lorsqu'un hôte IPv4 s'abonne à un groupe de multidiffusion, il traite les paquets envoyés à cette adresse de multidiffusion, ainsi que ceux destinés à son adresse de monodiffusion, qui a été attribuée à lui seul.

## 1.11 Adresses IPV4 publiques et privées.




Les adresses ne sont pas routables sur internet

Les adresses IPv4 publiques sont acheminées de manière globale entre les routeurs des FAI (fournisseurs d'accès à Internet). Toutefois, toutes les adresses IPv4 disponibles ne peuvent pas être utilisées sur Internet. Certains blocs d'adresses nommés *adresse privée* sont utilisés par la plupart des entreprises pour attribuer des adresses IPv4 aux hôtes internes. Les adresses IPv4 privées ont été créées au milieu des années 1990 en raison de la pénurie d'espace d'adresses IPv4. Les adresses IPv4 privées ne sont pas uniques et peuvent être utilisées par un réseau interne.

Les blocs d'adresses privées sont les suivants :

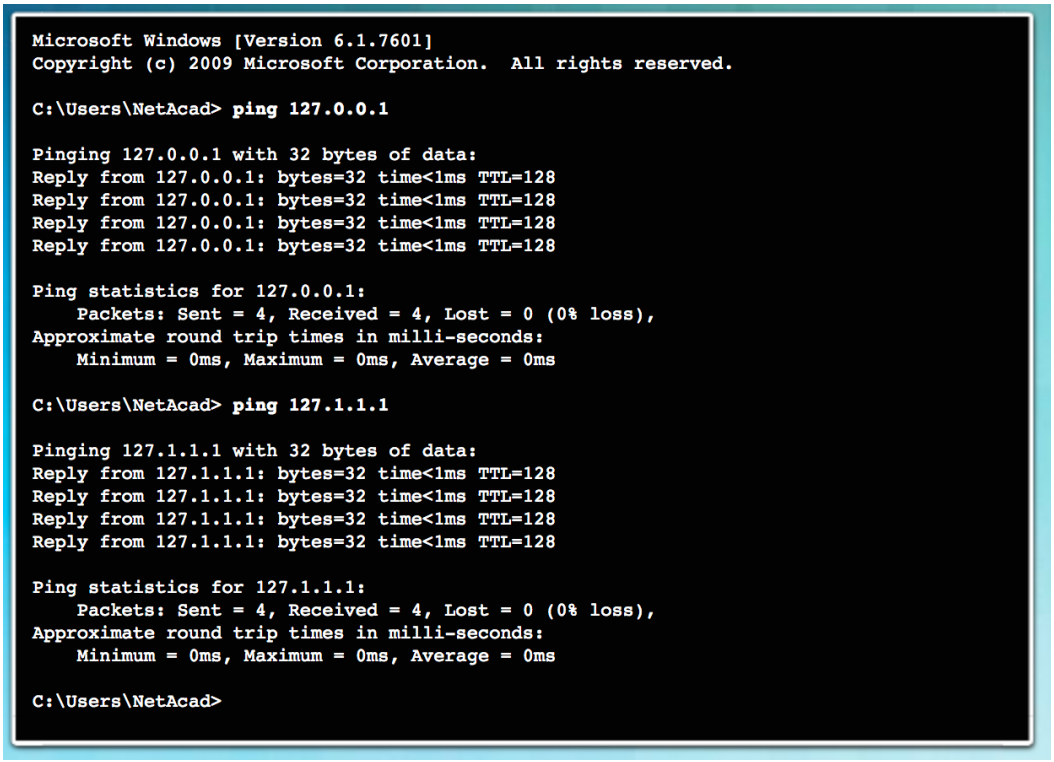
- **10.0.0.0 /8** ou **10.0.0.0** à **10.255.255.255**
- **172.16.0.0 /12** ou **172.16.0.0 à 172.31.255.255**
- **192.168.0.0 /16** ou **192.168.0.0 à 192.168.255.255**

Il est important de savoir que les adresses appartenant à ces blocs ne sont pas autorisées sur Internet et doivent être filtrées (rejetées) par les routeurs Internet. Par exemple, dans la figure ci-contre, les utilisateurs des réseaux 1, 2 ou 3 envoient des paquets à des destinations éloignées. Les routeurs du fournisseur d'accès à Internet (FAI) voient que les adresses IPv4 source dans les paquets sont des adresses privées et rejettent donc les paquets.

**Remarque** : les adresses privées sont définies dans le document RFC 1918.
La plupart des entreprises utilisent des adresses IPv4 privées pour leurs hôtes internes. Toutefois, ces adresses RFC 1918 ne sont pas routables via Internet et doivent être traduites en adresses IPv4 publiques. La traduction d'adresses réseau (NAT) est utilisée pour convertir les adresses IPv4 privées en adresses IPv4 publiques. Généralement, cette opération s'effectue sur le routeur qui connecte le réseau interne à celui du FAI.

Les routeurs domestiques assurent la même fonction. Par exemple, la plupart des routeurs domestiques attribuent des adresses IPv4 à leurs hôtes filaires et sans fil à partir de l'adresse privée 192.168.1.0 /24. Une adresse IPv4 publique utilisée sur Internet est attribuée à l'interface du routeur domestique qui se connecte au réseau du FAI.

## 1.12 Adresses IPV4 d'utilisateur spéciales.




Certaines adresses, telles que l'adresse réseau et l'adresse de diffusion ne peuvent pas être attribuées à des hôtes. Il existe également des adresses spéciales qui peuvent être attribuées aux hôtes, mais des restrictions s'appliquent sur les interactions de ces hôtes sur le réseau.

- **Adresses de bouclage (127.0.0.0 /8 ou 127.0.0.1 à 127.255.255.254) :** couramment appelées 127.0.0.1, ces adresses spéciales sont utilisées par des hôtes pour diriger le trafic vers eux-mêmes. Par exemple, elles peuvent être utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle, comme le montre la figure ci-contre. Notez que l'adresse de bouclage 127.0.0.1 répond à la commande ping. Notez également que n'importe quelle adresse de ce bloc envoie les paquets en boucle à l'hôte local, comme le montre le résultat de la deuxième commande ping sur la figure ci-contre.

- **Adresses locales-liens (169.254.0.0 /16 ou 169.254.0.1 à 169.254.255.254) :** plus connues sous le nom d'adresses APIPA (adressage IP privé automatique), elles sont

utilisées par un client DHCP Windows pour se configurer automatiquement si aucun serveur DHCP n'est disponible. Elles sont utiles dans une connexion peer-to-peer.

- **Adresses TEST-NET (192.0.2.0/24 ou 192.0.2.0 à 192.0.2.255)** : ces adresses sont réservées à des fins pédagogiques et utilisées dans la documentation et dans des exemples de réseau.

**Remarque** : il existe également des adresses expérimentales dans le bloc 240.0.0.0 à 255.255.255.254 qui sont réservées pour une utilisation future (RFC 3330 de l'IETF).

## 1.13 Ancien système d'adressage par classe.

En 1981, les adresses IPv4 Internet étaient attribuées à l'aide de l' *adressage par classe* tel que défini dans la RFC 790 de l'IETF, Assigned Numbers. Les clients ont reçu une adresse réseau basée sur l'une des trois classes, A, B ou C. Le RFC a divisé les plages monodiffusion en classes spécifiques, respectivement appelées :

- **Classe A (0.0.0.0/8 à 127.0.0.0/8)** : créée pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte. Elle utilisait un préfixe /8 fixe avec le premier octet identifiant l'adresse réseau et les trois derniers octets identifiant les adresses d'hôte. Toutes les adresses de classe A nécessitaient que le bit de poids fort du premier octet soit un zéro, pour créer 128 réseaux de classe A au total. La figure 1 résume la classe A.

| Spécifications de la classe A | |
|---|---|
| Bloc d'adresses | 0.0.0.0 – 127.0.0.0 |
| Masque de sous-réseau par défaut | /8 (255.0.0.0) |
| Nombre maximal de réseaux | 128 |
| Nombre d'hôtes par réseau | 16 777 214 |
| Bit d'ordre haut | 0xxxxxxx.___.___.___ |

* 0.0.0.0 et 127.0.0.0 sont réservées et ne peuvent pas être attribuées

- **Classe B (128.0.0.0 /16 à 191.255.0.0 /16)** : créée pour répondre aux besoins des réseaux de taille moyenne ou de grande taille comportant jusqu'à 65 000 adresses d'hôtes environ. Elle utilisait un préfixe /16 fixe avec les deux octets d'ordre haut pour indiquer l'adresse réseau et les trois derniers octets identifiant les adresses d'hôte. Les deux bits de poids fort de l'octet d'ordre haut doivent être 10 pour créer plus de 16 000 réseaux. La figure 2 résume la classe B.

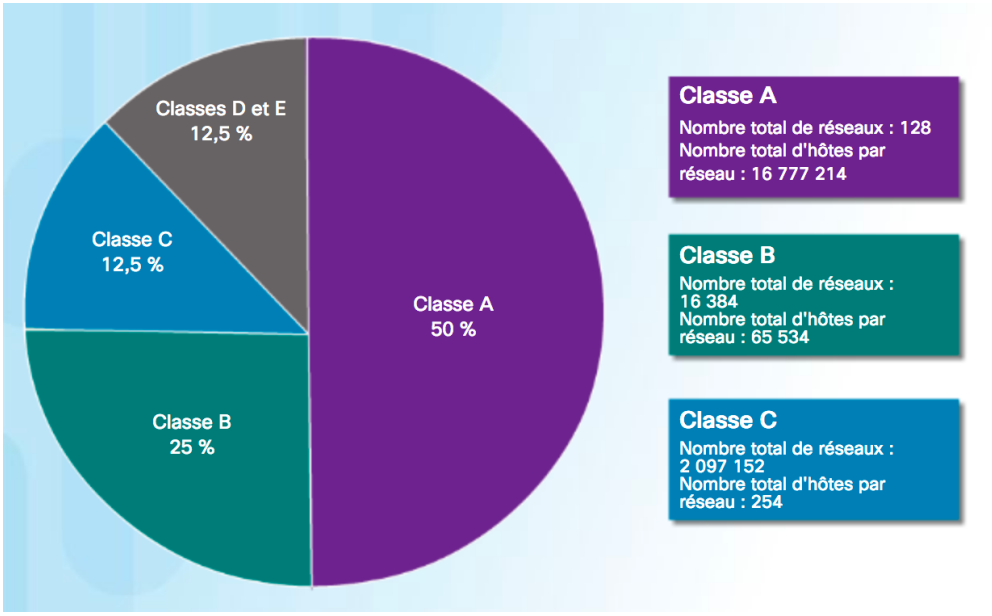
| Spécifications de la classe B | |
|---|---|
| Bloc d'adresses | 128.0.0.0 à 191.255.0.0 |
| Masque de sous-réseau par défaut | /16 (255.255.0.0) |
| Nombre maximal de réseaux | 16 384 |
| Nombre d'hôtes par réseau | 65 534 |
| Bit d'ordre haut | 10xxxxxx.___.___.___ |

- **Classe C (192.0.0.0 /24 à 223.255.255.0 /24)** : créée pour répondre aux besoins des réseaux de petite taille comportant 254 hôtes maximum. Elle utilisait un préfixe /24 fixe avec les trois premiers octets identifiant le réseau et l'octet restant identifiant les adresses d'hôte. Les trois bits de poids fort de l'octet d'ordre haut doivent être 110 pour créer plus de 2 millions de réseaux. La figure 3 résume la classe C

| Spécifications de la classe C | |
|---|---|
| Bloc d'adresses | 192.0.0.0 à 223.255.255.0 |
| Masque de sous-réseau par défaut | /24 (255.255.255.0) |
| Nombre maximal de réseaux | 2 097 152 |
| Nombre d'hôtes par réseau | 254 |
| Bit d'ordre haut | 110xxxxx.___.___.___ |

**Remarque** : il existe également un bloc d'adresses de multidiffusion de classe D de 224.0.0.0 à 239.0.0.0 et un bloc d'adresses expérimentales de classe E de 240.0.0.0 à 255.0.0.0.

## 1.14 Adressage sans classe.




Comme le montre la figure, le système sans classe a attribué 50 % des adresses IPv4 disponibles aux 128 réseaux de classe A, 25 % des adresses aux réseaux de classe B, et la classe C a ensuite partagé les 25 % restants avec les classes D et E. Malheureusement, cette distribution a gaspillé de nombreuses adresses et épuisé les adresses IPv4 disponibles. Les besoins de certaines entreprises n'étaient pas toujours couverts par l'une de ces trois classes. Par exemple, une entreprise dont le réseau comptait 260 hôtes devait obtenir une adresse de classe B avec plus de 65 000 adresses, gaspillant ainsi 64 740 adresses.

L'adressage par classe a été abandonné à la fin des années 1990 au profit du système d'adressage sans classe plus récent et toujours d'actualité. L'adressage par classe a pourtant laissé quelques vestiges dans les réseaux actuels. Par exemple, lorsque vous attribuez une adresse IPv4 à un ordinateur, le système d'exploitation examine l'adresse pour déterminer si elle appartient à la classe A, B ou C. Le système d'exploitation devine ensuite le préfixe utilisé par cette classe et attribue le masque de sous-réseau par défaut.

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). En 1993, l'IETF a créé un nouvel ensemble de normes permettant aux fournisseurs de services d'attribuer des adresses IPv4 sur n'importe quelle limite binaire (longueur de préfixe) au lieu d'utiliser uniquement les classes A, B ou C. L'objectif était de retarder la pénurie voire l'épuisement des adresses IPv4.

L'IETF savait que le CIDR était uniquement une solution temporaire et qu'un nouveau protocole IP devait être développé pour s'adapter à la croissance rapide du nombre d'utilisateurs d'Internet. En 1994, l'IETF a commencé à chercher un successeur à l'IPv4, à savoir le futur protocole IPv6.
Mais qui gère et attribue ces adresses IP ?

## 1.15 Attribution des adresses IP.


Pour que les entreprises ou organisations puissent prendre en charge les hôtes réseau (par exemple les serveurs web) accessibles depuis Internet, elles doivent disposer d'un bloc d'adresses publiques. N'oubliez pas que les adresses publiques doivent être uniques et que l'utilisation des adresses publiques est régulée et dépend de chaque organisation. Cela vaut pour les adresses IPv4 et IPv6.

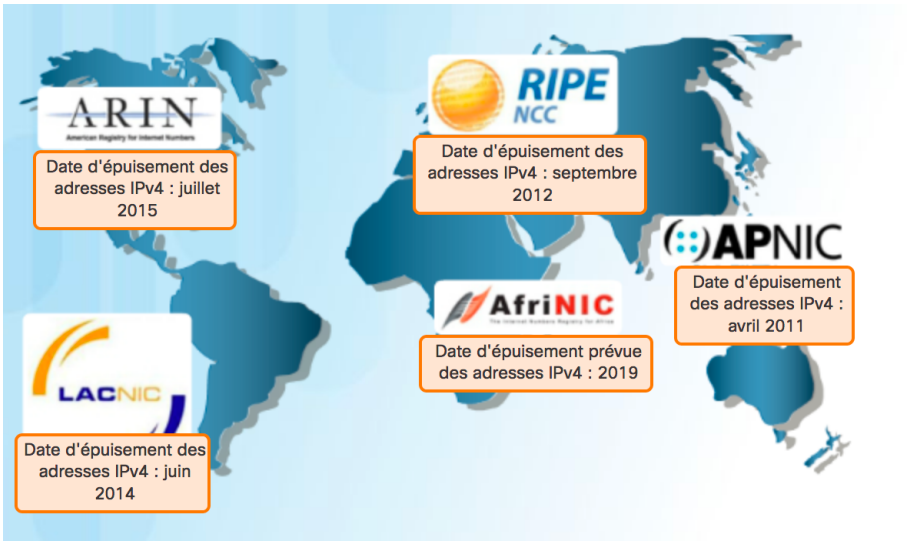
Elles sont gérées par l'IANA (Internet Assigned Numbers Authority,http://www.iana.org). L'IANA gère les blocs d'adresses IP et les attribue aux organismes d'enregistrement Internet locaux (RIR).

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. Les entreprises peuvent obtenir leurs adresses directement auprès d'un organisme d'enregistrement Internet local selon la politique appliquée par celui-ci.

La figure représente une carte du monde sur laquelle se trouvent les organismes d'enregistrement Internet locaux chargés d'attribuer des adresses IP notamment : ARIN en Amérique du Nord ; LACNIC en Amérique du Sud ; RIPE en Europe ; APNIC en Asie, sur les îles du Pacifique, en Nouvelle-Zélande et en Australie ; et AfriNIC en Afrique.

## 2. Adresses réseau IPV6 :

### 2.1 Ce qui rend IPV6 nécessaire.




Le protocole IPv6 est conçu pour être le successeur de l'IPv4. L'IPv6 possède un plus grand espace d'adressage (128 bits) pour un total de 340 sextillions d'adresses disponibles (c'est-à-dire 340, suivi de 36 zéros). Toutefois, l'IPv6 ne se limite pas à la multiplication des adresses. Lorsque l'IETF a commencé à développer un successeur à l'IPv4, l'organisme a utilisé cette opportunité pour corriger les limites de l'IPv4 et améliorer ce protocole. Par exemple, l'ICMPv6 (Internet Control Message Protocol version 6) inclut la configuration automatique et la résolution d'adresse, fonctions inexistantes dans le protocole ICMP pour l'IPv4 (ICMPv4). L'ICMPv4 et l'ICMPv6 seront étudiés plus loin dans ce chapitre.

**Nécessité du protocole IPv6**

Le manque d'espace d'adressage IPv4 a été le facteur le plus décisif pour la transition vers l'IPv6. À mesure que les connexions à Internet augmentent en Afrique, en Asie et dans d'autres parties du monde, les adresses IPv4 deviennent insuffisantes pour prendre en charge cette croissance. Comme l'illustre la figure, quatre des cinq RIR se sont trouvés à court d'adresses IPv4.
Théoriquement, l'IPv4 est limité à 4,3 milliards d'adresses. Les adresses privées, en association avec la traduction d'adresses réseau (NAT), ont été utilisées pour ralentir le manque d'espace d'adressage IPv4. Toutefois, la fonction NAT endommage de nombreuses applications et comporte des restrictions qui gênent fortement les communications peer-to-peer.

**Internet of Everything**

Par rapport au dernière décennies, l'Internet d'aujourd'hui est sensiblement différent. Désormais, Internet est principalement utilisé pour les e-mails, les pages web et le transfert de fichiers entre ordinateurs. Internet évolue pour devenir un « Internet des objets ». Les appareils pouvant accéder à Internet ne sont plus seulement des ordinateurs, des tablettes et des smartphones. Demain, les appareils connectés et équipés de capteurs concerneront tous les objets du quotidien, notamment les automobiles, les équipements biomédicaux, l'électroménager et même les écosystèmes naturels.

Avec l'utilisation croissante d'Internet, un espace limité d'adresses IPv4, des problèmes liés à la fonction NAT et l'Internet of Everything, le moment est venu d'entamer la transition vers IPv6.

## 2.2 Coexistence des protocoles IPV4 et IPV6.

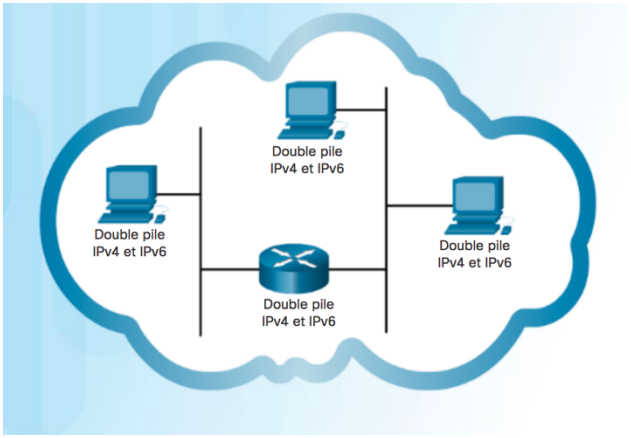



Figure 1

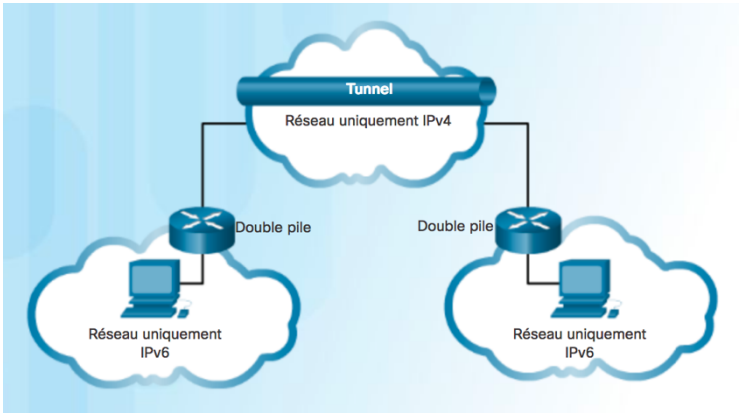



figure 2

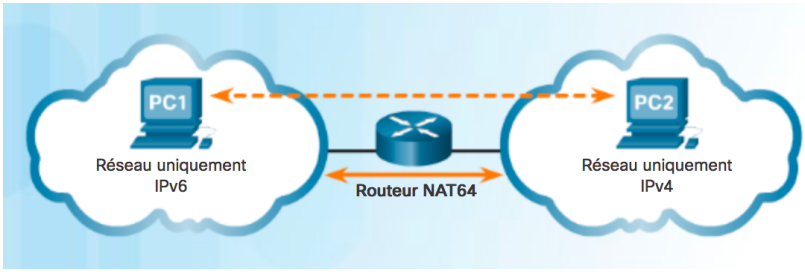



figure 3

La transition vers l'IPv6 n'aura pas lieu à une date fixe. Dans un futur proche, l'IPv4 et l'IPv6 vont continuer à coexister. La transition vers l'IPv6 durera probablement plusieurs années. L'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6. Les techniques de migration peuvent être classées en trois catégories :

- **la double pile** : comme l'illustre la figure 1, la double pile permet à l'IPv4 et à l'IPv6 de coexister sur le même segment de réseau. Les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément.

- **le tunneling** : comme l'illustre la figure 2, le tunneling est une méthode de transport des paquets IPv6 via un réseau IPv4. Les paquets IPv6 sont encapsulés dans des paquets IPv4, de la même manière que d'autres types de données.
- **la traduction** : comme l'illustre la figure 3, les périphériques IPv6 peuvent utiliser la traduction d'adresses réseau 64 (NAT64) pour communiquer avec les périphériques IPv4 à l'aide d'une technique de traduction similaire à la NAT pour l'IPv4. Un paquet IPv6 est traduit en un paquet IPv4, et inversement.

**Remarque** : le tunneling et la traduction sont utilisés uniquement lorsque nécessaire. L'objectif doit être de communiquer de manière native via le protocole IPv6 depuis la source jusqu'à la destination.

### 2.3 Représentation de l'adresse IPV6.

Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique ; pour un total de 32 valeurs hexadécimales, comme l'illustre la figure 1. Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.

**Format privilégié**

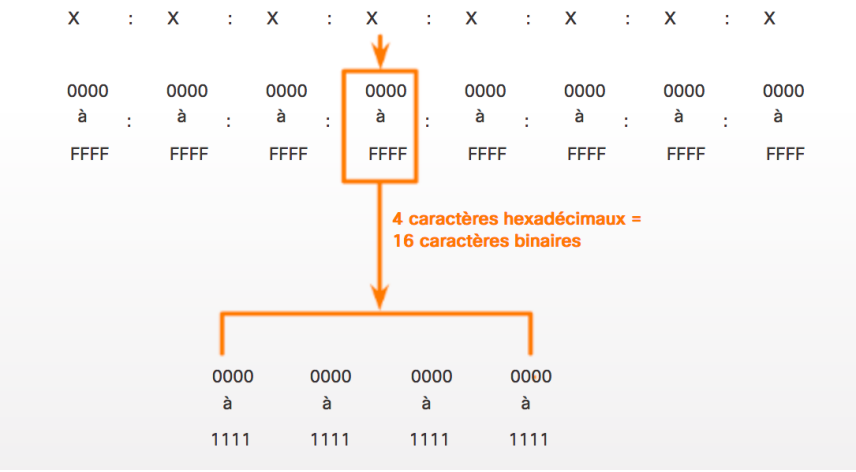



figure 1

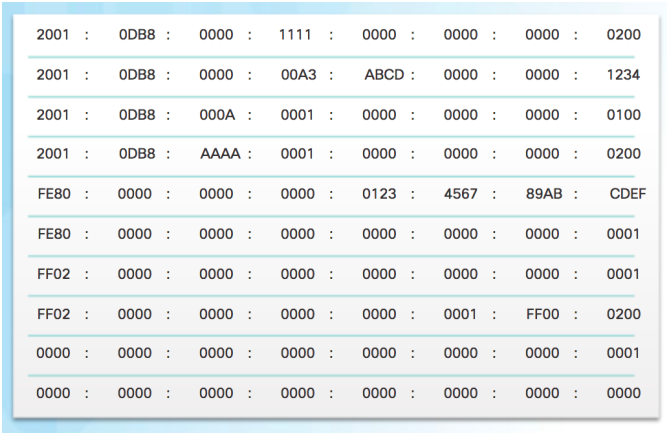
Comme l'illustre la figure 1, le format privilégié pour noter une adresse IPv6 est x:x:x:x:x:x:x:x, où chaque « x » est constitué de quatre valeurs hexadécimales. Pour faire référence aux 8 bits d'une adresse IPv4, nous utilisons le terme « octet ». Pour les adresses IPv6, « hextet » est le terme officieux qui désigne un segment de 16 bits ou de quatre valeurs hexadécimales. Chaque « x » équivaut à un hextet, 16 bits, ou à quatre caractères hexadécimaux.

Le format privilégié implique que l'adresse IPv6 soit écrite à l'aide de 32 caractères hexadécimaux. Cela ne signifie pas nécessairement que c'est la solution idéale pour représenter une adresse IPv6. Dans les pages suivantes, nous verrons deux règles permettant de réduire le nombre de chiffres requis pour représenter une adresse IPv6.

La figure 2 passe en revue la relation entre les formats décimal, binaire et hexadécimal. La figure 3 présente des exemples d'adresses IPv6 au format privilégié.

| Décimal | Binaire | Hexadécimal |
|---|---|---|
| 0 | 0000 | 0 |
| 1 | 0001 | 1 |
| 2 | 0010 | 2 |
| 3 | 0011 | 3 |
| 4 | 0100 | 4 |
| 5 | 0101 | 5 |
| 6 | 0110 | 6 |
| 7 | 0111 | 7 |
| 8 | 1000 | 8 |
| 9 | 1001 | 9 |
| 10 | 1010 | A |
| 11 | 1011 | B |
| 12 | 1100 | C |
| 13 | 1101 | D |
| 14 | 1110 | E |
| 15 | 1111 | F |

figure 2



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2001 | 0DB8 | 0000 | 1111 | 0000 | 0000 | 0000 | 0200 |
| 2001 | 0DB8 | 0000 | 00A3 | ABCD | 0000 | 0000 | 1234 |
| 2001 | 0DB8 | 000A | 0001 | 0000 | 0000 | 0000 | 0100 |
| 2001 | 0DB8 | AAAA | 0001 | 0000 | 0000 | 0000 | 0200 |
| FE80 | 0000 | 0000 | 0000 | 0123 | 4567 | 89AB | CDEF |
| FE80 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0001 |
| FF02 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0001 |
| FF02 | 0000 | 0000 | 0000 | 0000 | 0001 | FF00 | 0200 |
| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0001 |
| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |

figure 3

La figure 1 montre le format d'une adresse IPv6, qui se compose de huit ensembles de quatre valeurs hexadécimales séparées par des signes deux-points. Un ensemble de quatre valeurs hexadécimales est appelé hextet. La figure 2 représente un tableau qui répertorie les équivalents au format binaire et décimal des 16 chiffres hexadécimaux. La figure 3 présente des exemples d'adresses IPv6 au format privilégié. Le format privilégié répertorie les 32 chiffres hexadécimaux, chaque hextet étant séparé par un signe deux-points. Par exemple, 2001:0DB8:0000:1111:0000:0000:0000:0200.

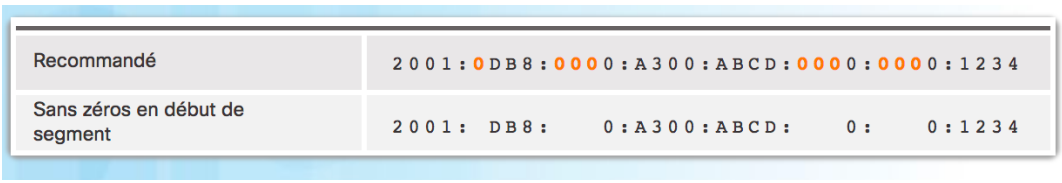
**Règle n° 1 : omettre les zéros en début de segment.**

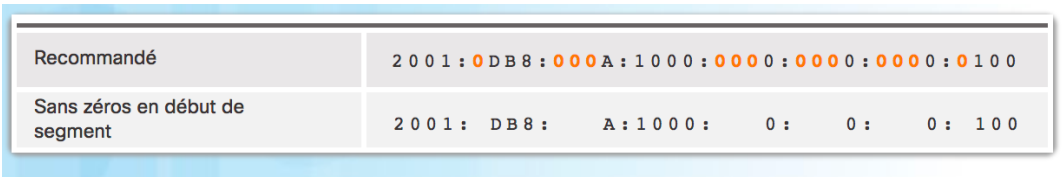
La première règle pour réduire la notation des adresses IPv6 consiste à omettre les zéros (0) du début d'une section de 16 bits (ou hextet). Par exemple :

- 01AB est équivalent à 1AB
- 09F0 est équivalent à 9F0
- 0A00 est équivalent à A00
- 00AB est équivalent à AB

Cette règle s'applique uniquement aux zéros de début de segment et NON aux zéros de fin. L'omission de ces derniers rendrait l'adresse ambiguë. Par exemple, l'hextet « ABC » peut être « 0ABC » ou « ABC0 », mais ce sont deux valeurs différentes.

Les figures suivantes contiennent plusieurs exemples où les zéros de début de segment sont omis pour réduire la taille des adresses IPv6. Pour chaque exemple, le format privilégié est indiqué. Notez que l'omission des zéros en début de segment entraîne un raccourcissement de l'adresse dans la plupart des cas.


**Règle nº 2 : omettre les séquences composées uniquement de zéros.**

La deuxième règle permettant d'abréger la notation des adresses IPv6 est qu'une suite de deux fois deux points (::) peut remplacer toute chaîne unique et contiguë d'un ou plusieurs segments de 16 bits (hextets) composés uniquement de zéros.

Une suite de deux fois deux points (::) peut être utilisée une seule fois par adresse : sinon, il serait possible d'aboutir sur plusieurs adresses différentes. Lorsque l'omission des zéros de début de segment est utilisée, la notation des adresses IPv6 peut être considérablement réduite. Il s'agit du « format compressé ».

Adresse non valide :
2001:0DB8::ABCD::1234

Extensions possibles des adresses ambiguës compressées :

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

Les figures suivantes illustrent plusieurs exemples de l'utilisation de deux fois deux points (::) et d'omission des zéros de début de segment pour réduire la taille d'une adresse IPv6.

| | |
|---|---|
| Recommandé | 2001:0DB8:0000:1111:0000:0000:0000:0200 |
| Sans zéros en début de segment | 2001: DB8: 0:1111: 0: 0: 0: 200 |
| Compressé | 2001:DB8:0:1111::200 |

| | |
|---|---|
| Recommandé | 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 |

:: peut être utilisé une seule fois.

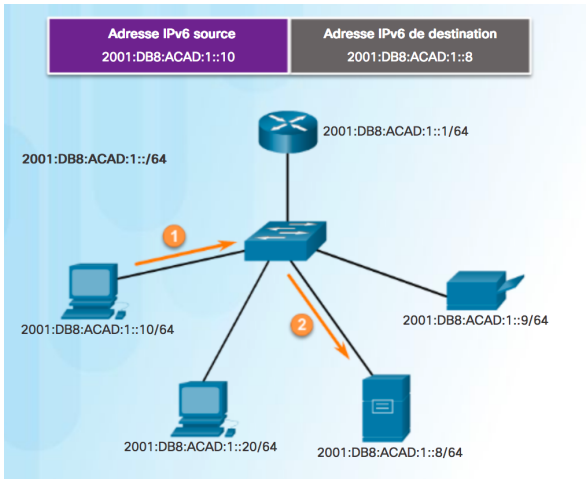
| | |
|---|---|
| Recommandé | FE80:0000:0000:0000:0123:4567:89AB:CDEF |
| Sans zéros en début de segment | FE80: 0: 0: 0: 123:4567:89AB:CDEF |
| Compressé | FE80::123:4567:89AB:CDEF |

| | |
|---|---|
| Recommandé | FF02:0000:0000:0000:0000:0000:0000:0001 |
| Sans zéros en début de segment | FF02: 0: 0: 0: 0: 0: 0: 1 |
| Compressé | FF02::1 |

| | |
|---|---|
| Recommandé | 0000:0000:0000:0000:0000:0000:0000:0001 |
| Sans zéros en début de segment | 0: 0: 0: 0: 0: 0: 0: 1 |
| Compressé | ::1 |

| | |
|---|---|
| Recommandé | 0000:0000:0000:0000:0000:0000:0000:0000 |
| Sans zéros en début de segment | 0: 0: 0: 0: 0: 0: 0: 0 |
| Compressée | :: |

## 2.4 Types d'adresses IPV6.

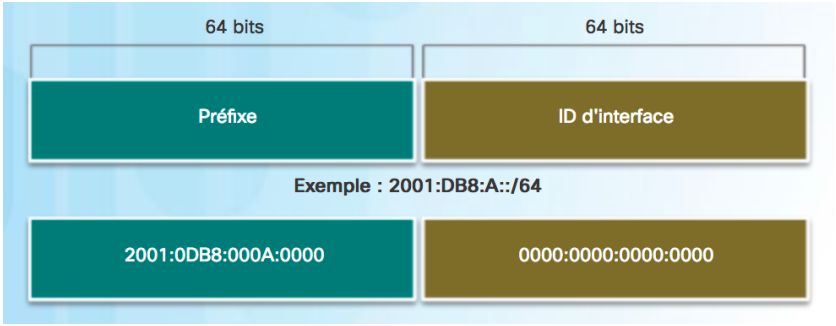



Il existe trois types d'adresses IPv6 :

- **monodiffusion** : une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique. Comme le montre la figure ci-contre, une adresse IPv6 source doit être une adresse de monodiffusion.
- **multidiffusion** : une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.
- **anycast** : une adresse anycast IPv6 est une adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse. Les adresses anycast sortent du cadre de ce cours.

Contrairement à l'IPv4, l'IPv6 n'a pas d'adresse de diffusion. Cependant, il existe une adresse de multidiffusion destinée à tous les nœuds IPv6 et qui offre globalement les mêmes résultats.

## 2.5 Longueur de préfixe IPV6.




Souvenez-vous que le préfixe (ou la partie réseau) d'une adresse IPv4 peut être identifié par un masque de sous-réseau en notation décimale à point ou une longueur de préfixe (notation de barre oblique). Par exemple, l'adresse IPv4 192.168.1.10 et le masque de sous-réseau en notation décimale à point 255.255.255.0 correspondent à 192.168.1.10/24.

L'IPv6 utilise la longueur de préfixe pour représenter le préfixe de l'adresse. Le protocole IPv6 n'utilise pas la notation décimale à point du masque de sous-réseau. La longueur de préfixe est utilisée pour indiquer la partie réseau d'une adresse IPv6 à l'aide de la notation adresse IPv6/longueur de préfixe.

La longueur de préfixe peut être comprise entre 0 et 128. La longueur de préfixe IPv6 standard pour les réseaux locaux et la plupart des autres types de réseau est /64. Cela signifie que le préfixe ou la partie réseau de l'adresse a une longueur de 64 bits, ce qui laisse 64 bits pour l'ID d'interface (partie hôte) de l'adresse.

## 2.6 Adresses de monodiffusion IPV6.

Une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique. Un paquet envoyé à une adresse de monodiffusion est reçu par l'interface correspondant à cette adresse. Comme c'est le cas avec l'IPv4, une adresse source IPv6 doit être une adresse de monodiffusion. L'adresse IPv6 de destination peut, quant à elle, être une adresse de monodiffusion ou de multidiffusion.

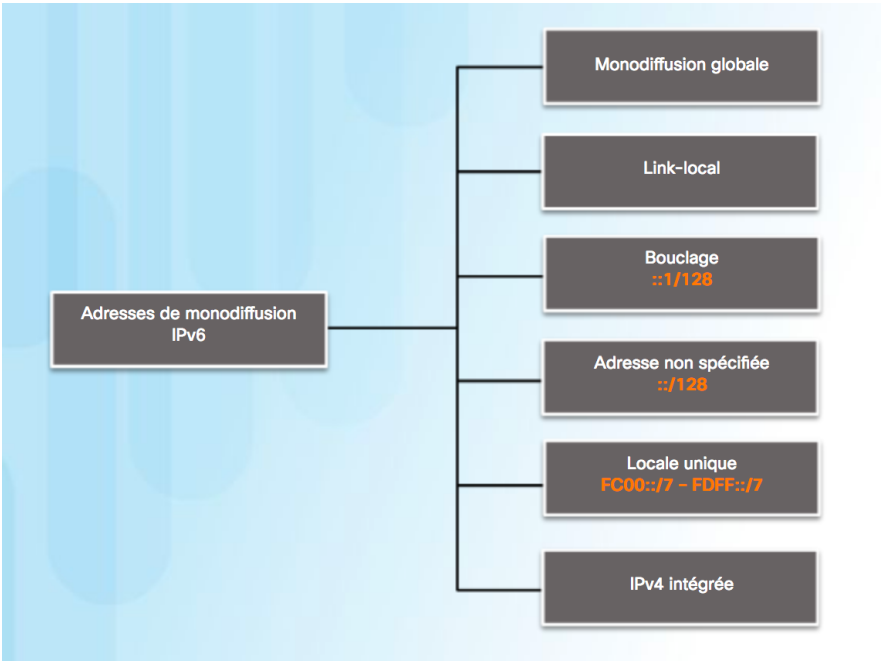
Les types d'adresses de diffusion IPv6 les plus courants sont les **adresses de diffusion globale** et les **adresses de monodiffusion link-local.**

**Monodiffusion globale**
Une adresse de diffusion globale est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet. Les adresses de diffusion globale peuvent être configurées de manière statique ou attribuées dynamiquement.

**Link-local**
Les adresses link-local sont utilisées pour communiquer avec d'autres périphériques sur la même liaison locale. Dans le cadre de l'IPv6, le terme « link » (ou liaison) fait référence à un sous-réseau. Les adresses link-local sont confinées à une seule liaison. Leur caractère unique doit être confirmé uniquement sur cette liaison, car elles ne sont pas routables au-delà de la liaison. En d'autres termes, les routeurs ne transmettent aucun paquet avec une adresse source ou de destination link-local.

**Adresse locale unique**
L'adresse de monodiffusion locale unique est un autre type d'adresse de monodiffusion. Les adresses IPv6 locales uniques ont certains points communs avec les adresses privées RFC 1918 utilisées dans l'IPv4, mais présentent également d'importantes différences. Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites. Ces adresses ne doivent pas être routables sur le réseau IPV6 global et ne doivent pas être traduites en adresses IPv6 globales. Les adresses locales uniques sont comprises entre FC00::/7 et FDFF::/7.

Avec l'IPv4, les adresses privées sont associées aux fonctions NAT/PAT pour fournir une traduction « plusieurs vers un seul » d'adresses privées en adresses publiques. Cette opération est effectuée en raison du caractère restreint de l'espace d'adressage IPv4. De nombreux sites utilisent également le caractère privé des adresses RFC 1918 pour sécuriser ou masquer leur réseau et limiter les risques. Cependant, ce n'est pas le but premier de ces technologies et l'IETF a toujours recommandé que les sites prennent les précautions de sécurité nécessaires au niveau de leur routeur connecté à Internet. Les adresses locales uniques peuvent être utilisées pour les périphériques qui n'auront jamais besoin d'être accessibles sur un autre réseau.




## 2.7 Les adresses de monodiffusion link-local IPV6.

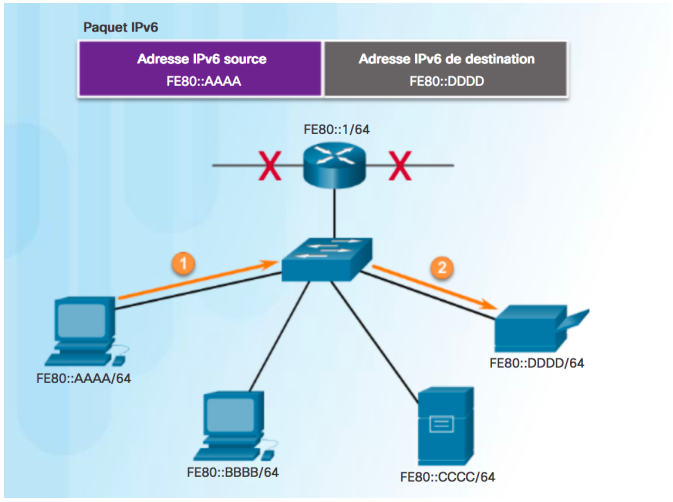



figure 1

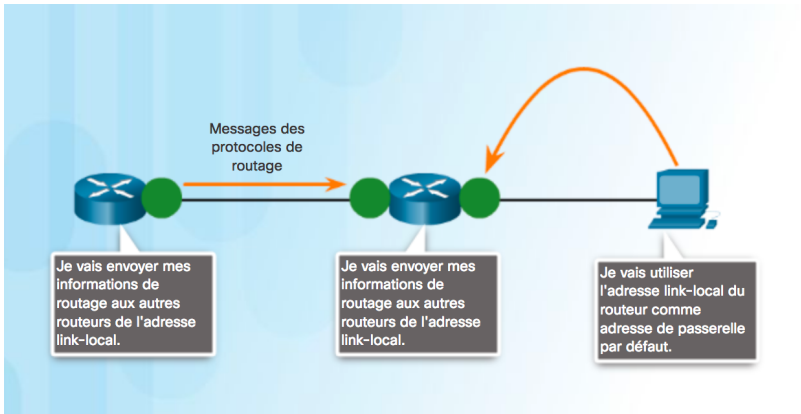



figure 2

Une adresse link-local IPv6 permet à un périphérique de communiquer avec d'autres périphériques IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau). Les paquets associés à une adresse link-local source ou de destination ne peuvent pas être acheminés au-delà de leur liaison d'origine.

L'adresse de diffusion globale n'est pas obligatoire. Toutefois, chaque interface réseau IPv6 doit avoir une adresse link-local.

Si une adresse link-local n'est pas configurée manuellement sur une interface, le périphérique crée automatiquement sa propre adresse sans communiquer avec un serveur DHCP. Les hôtes IPv6 créent une adresse link-local IPv6 même si aucune adresse de monodiffusion globale IPv6 n'a été attribuée aux périphériques. Cela permet aux périphériques IPv6 de communiquer avec d'autres périphériques IPv6 sur le même sous-réseau. Cela inclut la communication avec la passerelle par défaut (routeur).

Les adresses link-local IPv6 se trouvent dans la plage FE80::/10. /10 Indique que les 10 premiers bits sont 1111 1110 10xx xxxx. Le premier hextet dispose d'une plage comprise entre 1111 1110 10**00 0000** (FE80) et 1111 1110 10**11 1111** (FEBF).

La figure 1 présente un exemple de transmission à l'aide d'adresses link-local IPv6.
La figure 2 présente quelques utilisations des adresses link-local IPv6.

**Remarque** : en règle générale, c'est l'adresse locale-lien du routeur et non l'adresse de diffusion globale qui est utilisée comme passerelle par défaut pour les autres périphériques sur la liaison.

### 2.8 La structure d'une adresse de monodiffusion globale IPV6.


figure 1

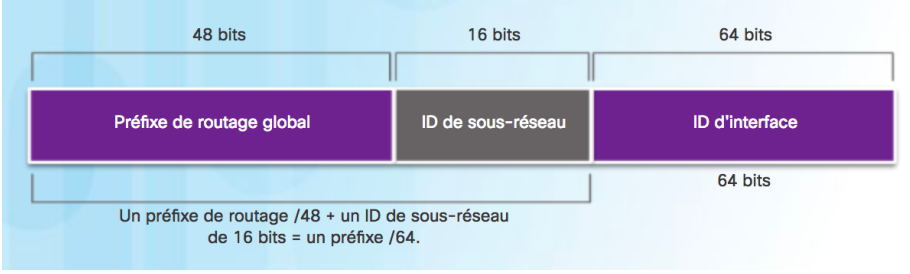



figure 2

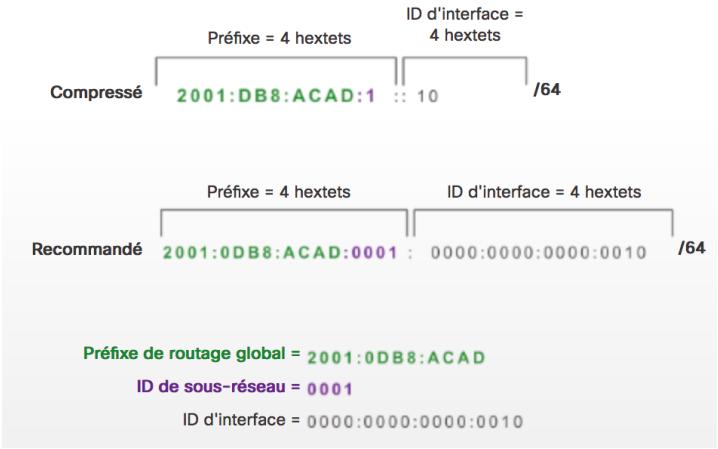



figure 3

Les adresses de diffusion globale (GUA) IPv6 sont uniques au monde et routables (Internet IPv6). Ces adresses sont équivalentes aux adresses publiques IPv4. L'ICANN (Internet Committee for Assigned Names and Numbers), opérateur de l'IANA, attribue des blocs d'adresses IPv6 aux cinq organismes d'enregistrement Internet locaux. Actuellement, seules des adresses de diffusion globale dont les trois premiers bits sont 001 ou 2000::/3 sont attribuées. En d'autres termes, le premier chiffre hexadécimal d'une adresse de diffusion globale (GUA) commence par 2 ou par 3. C'est uniquement 1/8e de l'espace d'adressage IPv6 total disponible : seule une infime partie est exclue pour les autres types d'adresse de monodiffusion et de multidiffusion.

**Remarque** : l'adresse 2001:0DB8::/32 a été réservée à des fins de documentation, notamment pour être utilisée dans des exemples.

La figure 1 illustre la structure et la plage d'adresses de diffusion globale.

Une adresse de diffusion globale se compose de trois parties :

- Préfixe de routage global
- ID de sous-réseau
- ID d'interface

**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 FAI) à un client ou à un site. Généralement, les RIR attribuent le préfixe global de routage /48 aux clients, à savoir tous les clients potentiels, des réseaux d'entreprise aux réseaux de particuliers.

La figure 2 illustre la structure d'une adresse de diffusion globale utilisant le préfixe de routage global /48. Les préfixes /48 sont les préfixes de routage global les plus couramment attribués et seront utilisés dans la plupart des exemples de ce cours.
Par exemple, l'adresse IPv6 2001:0DB8:ACAD::/48 a un préfixe indiquant que les 48 premiers bits (3 hextets) (2001:0DB8:ACAD) constituent le préfixe ou la partie réseau de l'adresse. La suite de deux fois deux points (::) avant la longueur de préfixe /48 signifie que le reste de l'adresse contient uniquement des 0.

La taille du préfixe global de routage détermine la taille de l'ID de sous-réseau.

**ID de sous-réseau**

L'ID de sous-réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site. Plus l'ID de sous-réseau est un nombre important, plus il y a de sous-réseaux disponibles.

**ID d'interface**

L'ID d'interface IPv6 est l'équivalent de la partie hôte d'une adresse IPv4. Le terme ID d'interface est utilisé, car un hôte unique peut avoir plusieurs interfaces, chacune dotée d'une ou de plusieurs adresses IPv6. Dans la plupart des cas, il est fortement recommandé d'utiliser des sous-réseaux /64, c'est-à-dire un ID d'interface 64 bits, comme illustré à la figure 2.

Remarque : contrairement à l'adressage IPv4, avec IPv6, les adresses d'hôte contenant uniquement des 0 ou uniquement des 1 peuvent être attribuées à un périphérique. L'adresse contenant uniquement des 1 peut être attribuée, puisque les adresses de diffusion ne sont pas utilisées dans IPv6. L'adresse contenant uniquement des 0 peut également être utilisée, mais elle est réservée comme adresse anycast de routeur de sous-réseau, et elle ne doit être attribuée qu'aux routeurs.

Un moyen simple de lire la plupart des adresses IPv6 consiste à compter le nombre d'hextets. Comme l'illustre la figure 3, dans une adresse de diffusion globale /64, les quatre premiers hextets sont réservés à la partie réseau de l'adresse, le quatrième hextet indiquant l'ID de sous-réseau. Les quatre hextets restants sont réservés à l'ID d'interface.

La figure 1 montre que les trois premiers bits d'une adresse de monodiffusion globale IPv6 sont définis sur 001. La figure montre la plage de bits au format binaire du premier hextet, qui va de 2000 à 3FFF. La figure 2 montre le préfixe de routage global IPv6 de /48. Les premiers 48 bits servent de préfixe de routage global et les 16 bits suivants servent d'identifiant de sous-réseau. Le préfixe de routage /48 combiné à l'identifiant de sous-réseau de 16 bits forment le préfixe /64. Les 64 bits restants sont l'identifiant de l'interface. La figure 3 montre comment lire une adresse de monodiffusion globale. L'adresse est d'abord listée comme une adresse compressée, 2001:DB8:ACAD:1::10/64. Les quatre premiers hextets sont le préfixe et les quatre derniers hextets sont l'identifiant de l'interface.

La forme étendue est 2001:0DB8:ACAD:0001:0000:0000:0000:0010 /64. Le préfixe de routage global est 2001:0DB8:ACAD. L'ID du sous-réseau est 0001 et l'ID de l'interface est 0000:0000:0000:0200.

## 2.9 Configuration statique d'une adresse de diffusion globale.

### Configuration de routeur

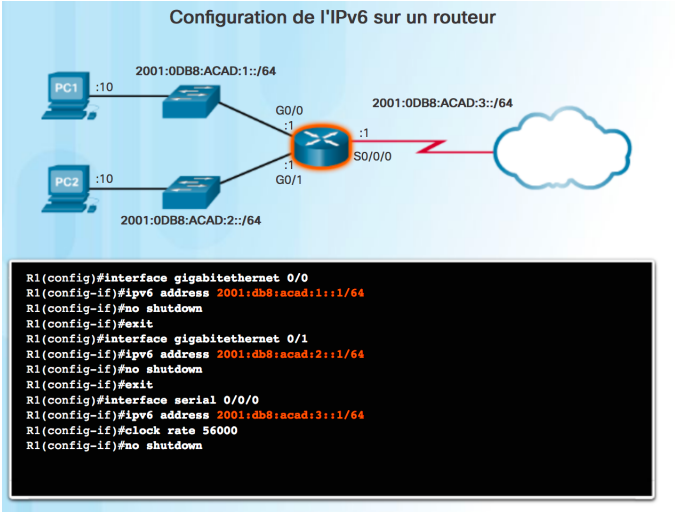



figure 1

La plupart des commandes de configuration et de vérification IPv6 de Cisco IOS sont semblables à celles utilisées pour l'IPv4. Dans de nombreux cas, la seule différence est l'utilisation d'**ipv6** au lieu d'**ip** dans les commandes.

La commande permettant de configurer une adresse de monodiffusion globale sur une interface est **ipv6 address** *(adresse IPv6/longueur du préfixe).*
Notez qu'il n'y a pas d'espace entre *l'adresse IPv6* et *la longueur du préfixe.*
La configuration utilisée en exemple utilise la topologie de la figure 1 et les sous-réseaux IPv6 suivants :

- 2001:0DB8:ACAD:0001:/64 (*ou* 2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (*ou* 2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (*ou* 2001:DB8:ACAD:3::/64)

La figure 1 indique également les commandes nécessaires pour configurer l'adresse de diffusion globale IPV6 sur les interfaces GigabitEthernet 0/0, GigabitEthernet 0/1 et Série 0/0/0 de R1.

### Configuration des hôtes

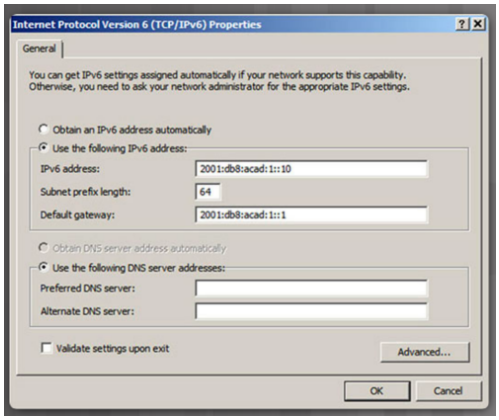



figure 2

La configuration manuelle de l'adresse IPv6 sur un hôte est similaire à celle d'une adresse IPv4.

Comme le montre la figure 2, l'adresse de la passerelle par défaut configurée pour PC1 est 2001:DB8:ACAD:1::1. Il s'agit de l'adresse de diffusion globale de l'interface GigabitEthernet de R1 sur le même réseau. L'adresse de la passerelle par défaut configurée peut également être celle de l'adresse link-local de l'interface GigabitEthernet. Ces deux configurations fonctionnent.

Tout comme avec l'IPv4, la configuration des adresses statiques sur les clients ne convient pas aux environnements de grande taille. Pour cette raison, la plupart des administrateurs de réseaux IPv6 utilisent l'attribution dynamique des adresses IPv6.

Un périphérique peut obtenir automatiquement une adresse de diffusion globale IPv6 de deux façons :

- la configuration automatique des adresses sans état (SLAAC)
- DHCPv6 avec état

**Remarque** : lorsque la méthode DHCPv6 ou SLAAC est utilisée, l'adresse link-local du routeur local est automatiquement définie comme étant l'adresse de la passerelle par défaut. La figure 1 illustre une topologie avec un routeur connecté à deux LAN et un WAN. Chaque réseau est identifié avec une adresse réseau IPv6. Sous la topologie, une fenêtre de commande montre la configuration des interfaces du routeur avec les adresses IPv6 : 2001:db8:acad:1::1/64, 2001:db8:acad:2::1/64 et 2001:db8:acad:3::1/64. La figure 2 montre la fenêtre Propriétés TCP/IPv6 de Windows. L'adresse IPv6, la longueur du préfixe de sous-réseau et la passerelle par défaut sont configurés.

## 2.10 Configuration dynamique SLAAC.

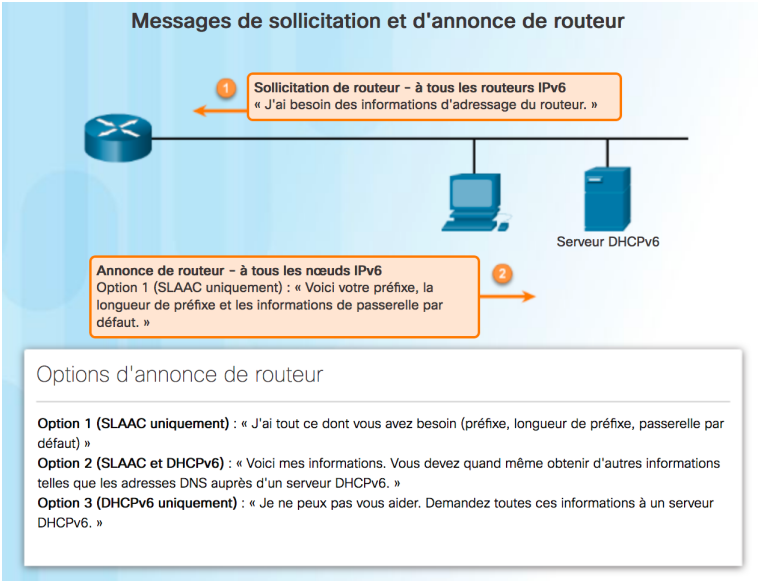



figure 1

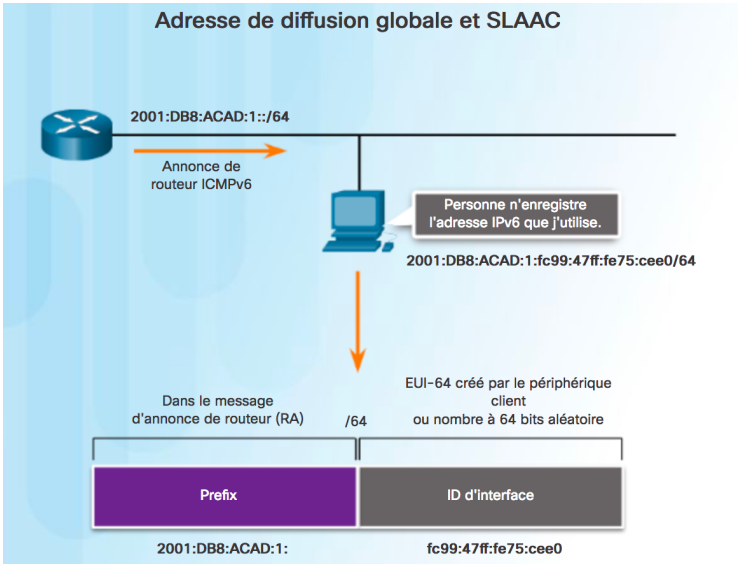



figure 2

La configuration automatique des adresses sans état (SLAAC) est une méthode qui permet à un périphérique d'obtenir son préfixe, la longueur de préfixe, l'adresse de la passerelle par défaut et d'autres informations à partir d'un *routeur Ipv6* sans utiliser un serveur DHCPv6. Lorsque la SLAAC est utilisée, les périphériques se basent sur les messages d'annonce de routeur ICMPv6 du routeur local pour obtenir les informations nécessaires.

Les routeurs IPv6 envoient des messages d'annonce de routeur ICMPv6 toutes les 200 secondes à tous les périphériques IPv6 du réseau. Un message d'annonce de routeur est également envoyé en réponse à un hôte qui envoie un message de sollicitation de routeur ICMPv6.

Le routage IPv6 n'est pas activé par défaut. Pour sélectionner l'IPv6 sur un routeur, la commande de configuration globale **ipv6 unicast-routing** doit être utilisée.
**Remarque** : des adresses IPv6 peuvent être configurées sur un routeur qui n'est pas un routeur IPV6.

Le message d'annonce de routeur ICMPv6 indique à un périphérique comment obtenir une adresse de diffusion globale IPv6. La décision finale revient au système d'exploitation de l'appareil. Le message d'annonce de routeur contient les éléments suivants :

- **le préfixe de réseau et la longueur de préfixe**, qui indiquent au périphérique le réseau auquel il appartient.
- **l'adresse de la passerelle par défaut**, qui est une adresse link-local et l'adresse IPv6 source du message d'annonce de routeur.
- **les adresses DNS et le nom de domaine**, c'est-à-dire les adresses des serveurs DNS et un nom de domaine.

Comme l'illustre la figure 1, il existe trois options de messages d'annonce de routeur :
- Option 1 : SLAAC
- Option 2 : SLAAC avec un serveur DHCPv6 sans état
- Option 3 : DHCPv6 avec état (pas de SLAAC)

**Option d'annonce de routeur 1 : SLAAC**

Par défaut, le message d'annonce de routeur suggère au périphérique récepteur d'utiliser les informations qu'il contient pour créer sa propre adresse de diffusion globale IPv6 et à d'autres fins. Les services d'un serveur DHCPv6 ne sont pas nécessaires.
La SLAAC étant sans état, aucun serveur central (par exemple un serveur DHCPv6 avec état) n'assure l'attribution des adresses de diffusion globale et la tenue à jour d'une liste des périphériques et de leurs adresses. Avec la SLAAC, le périphérique client utilise les informations du message d'annonce de routeur pour créer sa propre adresse de diffusion globale. Comme le montre la figure 2, les deux parties de l'adresse sont créées comme suit :

- **le préfixe**, reçu dans le message d'annonce de routeur
- **l'ID d'interface**, qui utilise la méthode EUI-64 ou est obtenu par la génération d'un nombre à 64 bits aléatoire

La figure 1 illustre le processus de sollicitation de routeur avec un ordinateur qui envoie une demande d'informations d'adressage IPv6 à partir de tous les routeurs IPv6. La figure montre également un message d'annonce de routeur envoyé par un routeur. Ce message peut être l'une des trois options configurées. L'option 1 fournit toutes les informations d'adressage nécessaires. L'option 2 définit des options d'adressage, mais se repose sur un serveur DHCPv6 pour certains paramètres. Enfin, l'option 3 se repose uniquement sur un serveur DHCPv6 pour toutes les informations d'adressage. Dans la figure, l'annonce de routeur utilise l'option 1 et indique à l'ordinateur le préfixe, la longueur de préfixe et la passerelle par défaut à utiliser. La figure 2 montre un exemple de SLAAC. Un ordinateur utilise l'adresse de monodiffusion globale du routeur pour construire sa propre adresse de monodiffusion globale. L'ordinateur utilise le préfixe de l'adresse du routeur, soit 2001:DB8:ACAD:1 dans l'exemple. Ensuite, l'ordinateur utilise EUI-64 ou génère un nombre à 64 bits aléatoire pour compléter la partie ID de l'interface de l'adresse.

## 2.11 Configuration dynamique DHCPV6.

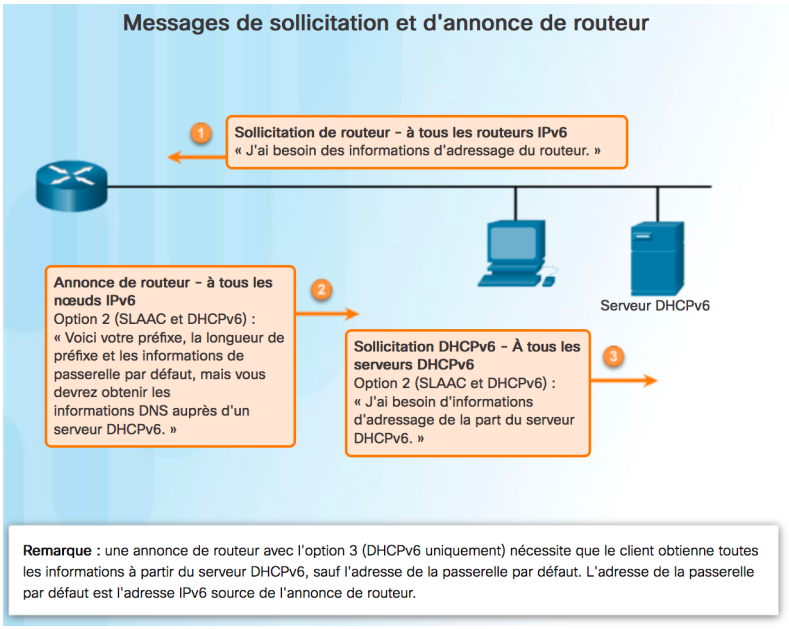



figure 1

Par défaut, le message d'annonce de routeur est l'option 1 : SLAAC uniquement. L'interface du routeur peut être configurée pour envoyer une annonce de routeur à l'aide des méthodes SLAAC et DHCPv6 sans état, ou uniquement de la méthode DHCPv6.

**Option 2 d'annonce de routeur : SLAAC et DHCPv6 sans état**

Avec cette option, le message d'annonce de routeur suggère aux périphériques d'utiliser :

- la SLAAC pour créer sa propre adresse de diffusion globale IPv6.
- 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.

Un serveur DHCPv6 sans état distribue les adresses des serveurs DNS et les noms de domaine. Il n'attribue pas les adresses de diffusion globale.

**Option d'annonce de routeur 3 : DHCPv6 sans état**

DHCPv6 avec état est similaire à DHCP pour IPv4. Un périphérique peut recevoir automatiquement ses informations d'adressage, y compris une adresse de diffusion globale, la longueur du préfixe et les adresses des serveurs DNS à l'aide des services d'un serveur DHCPv6 avec état.

Avec cette option, le message d'annonce de routeur suggère aux périphériques d'utiliser :

- 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.

Un serveur DHCPv6 avec état attribue les adresses IPv6 aux périphériques et tient à jour une liste de ces attributions. DHCP pour IPv4 est une méthode avec état.

**Remarque** : l'adresse de la passerelle par défaut peut uniquement être obtenue de manière dynamique à partir du message d'annonce de routeur. Le serveur DHCPv6 avec ou sans état ne fournit pas l'adresse de la passerelle par défaut.

La figure montre un message d'annonce de routeur envoyé par un routeur en réponse à un message de sollicitation de routeur. Dans la figure, l'annonce de routeur utilise l'option 2 et indique à l'ordinateur le préfixe, la longueur de préfixe et la passerelle par défaut à utiliser. Elle utilise également la configuration des adresses sans état et indique à l'ordinateur qu'un serveur DHCPv6 est requis pour les informations DNS. L'ordinateur envoie ensuite une demande de sollicitation DHCPv6 pour rechercher des informations DNS.

## 2.12 Méthode EUI-64 et génération aléatoire.

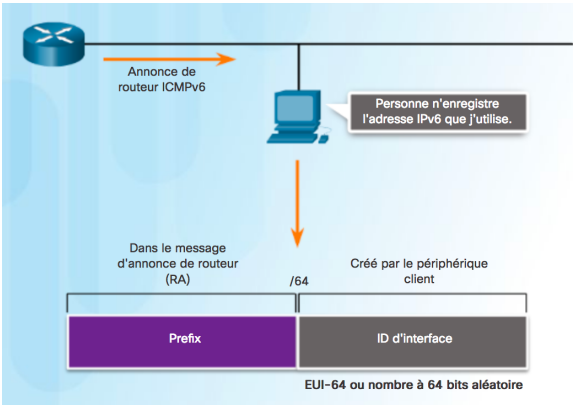



figure 1

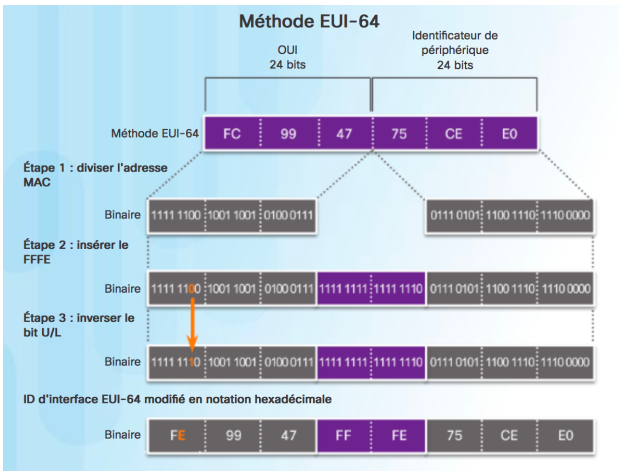



figure 2


figure 3


figure 4

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. Le client connaît la partie préfixe de l'adresse grâce au message d'annonce, mais il doit créer son ID d'interface. Pour cela, il peut utiliser la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement, comme le montre la figure 1.

**Méthode EUI-64**

L'IEEE a défini l'identifiant unique étendu (EUI), ou format EUI-64 modifié. Ce processus utilise l'adresse MAC Ethernet à 48 bits d'un client et insère 16 autres bits au milieu de cette adresse MAC pour créer un ID d'interface de 64 bits.
Les adresses MAC Ethernet sont généralement représentées au format hexadécimal et sont constituées de deux parties :

- **l'identifiant unique d'entité (OUI)** : un code de fournisseur de 24 bits (6 caractères hexadécimaux) attribué par l'IEEE.
- **l'ID de périphérique** : une valeur unique de 24 bits (6 caractères hexadécimaux) contenue dans un OUI standard.

Un ID d'interface EUI-64 est représenté au format binaire et comprend trois parties :

- le code OUI sur 24 bits, provenant de l'adresse MAC du client, mais dont le septième bit (universellement/localement, U/L) est inversé. Cela signifie que si le septième bit est un 0, il devient un 1, et vice versa.
- La valeur de 16 bits FFFE intégrée (au format hexadécimal).
- ID de périphérique de 24 bits de l'adresse MAC du client.

Le processus EUI-64 est présenté à la figure 2, avec l'adresse MAC GigabitEthernet FC99:4775:CEE0 de R1.

**Étape 1** : coupez l'adresse MAC au niveau de la séparation entre l'OUI et l'ID de périphérique.

**Étape 2** : insérez la valeur hexadécimale FFFE, à savoir 1111 1111 1111 1110 en binaire.

**Étape 3** : convertissez les 2 premières valeurs hexadécimales de l'OUI en binaire et inversez le bit U/L (bit 7). Dans cet exemple, le 0 du bit 7 devient un 1.

Il en résulte un ID d'interface généré à l'aide de la méthode EUI-64, FE99:47FF:FE75:CEE0.
**Remarque** : l'utilisation du bit U/L et les raisons de son inversion sont expliquées dans le RFC 5342.

À la figure 3, l'adresse de diffusion globale IPv6 de PCA est créée dynamiquement à l'aide des méthodes SLAAC et EUI-64. Il est simple de savoir si une adresse a été créée via la méthode EUI-64 : il suffit d'analyser la valeur FFFE située dans l'ID d'interface (voir la figure 3).

L'avantage de la méthode EUI-64 est que l'adresse MAC Ethernet peut être utilisée pour déterminer l'ID d'interface. Elle permet également aux administrateurs réseau de suivre facilement une adresse IPv6 jusqu'à un périphérique final en utilisant une adresse MAC unique. Toutefois, cela entraîne des problèmes de confidentialité pour de nombreux utilisateurs. Ces derniers s'inquiètent du fait qu'il soit possible de remonter jusqu'à l'ordinateur physique en analysant les paquets. Pour éviter ce problème, un ID d'interface généré aléatoirement peut également être utilisé.

### 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 la version Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec le processus EUI-64. Windows XP et les systèmes d'exploitation précédents utilisaient la méthode EUI-64.

Une fois l'ID d'interface créé via la méthode EUI-64 ou aléatoirement, il peut être combiné avec un préfixe IPv6 dans le message d'annonce de routeur pour créer une adresse de diffusion globale, comme le montre la figure 4.

Remarque : pour s'assurer que les adresses de monodiffusion IPv6 sont uniques, le client peut utiliser le processus de détection d'adresse dupliquée (DAD). Le principe est similaire à une requête ARP pour sa propre adresse. En l'absence de réponse, l'adresse est unique.

## 2.13 Adresses link-local dynamiques.

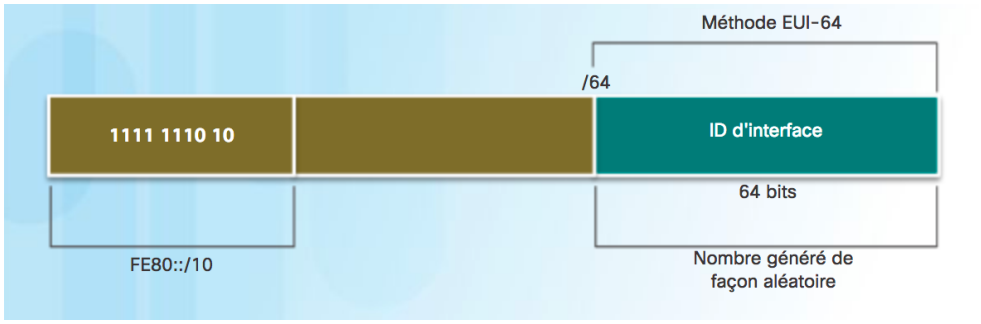



figure 1

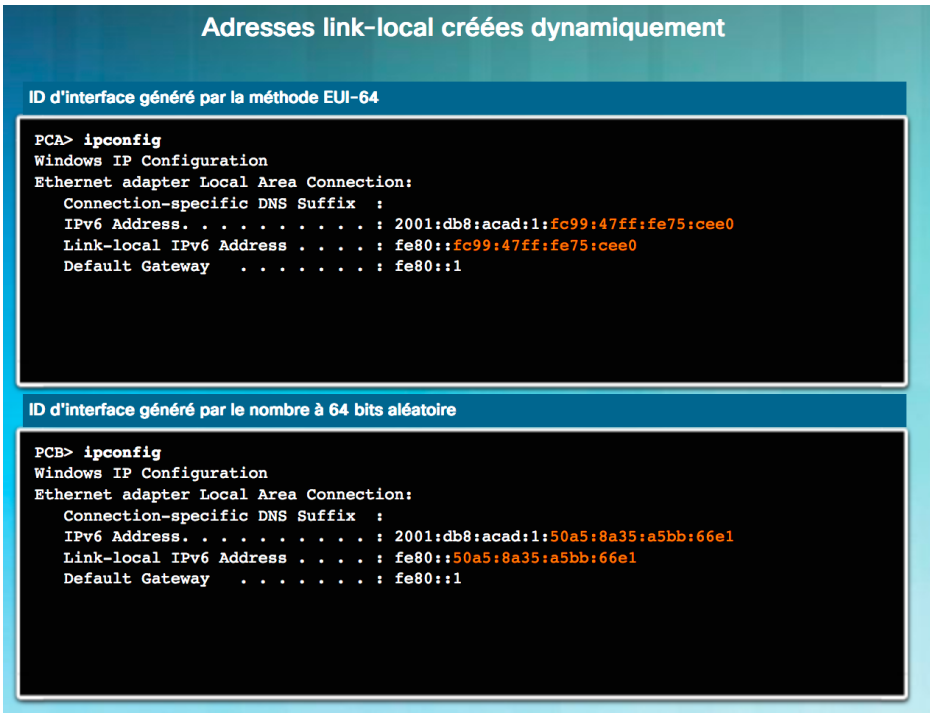



figure 2

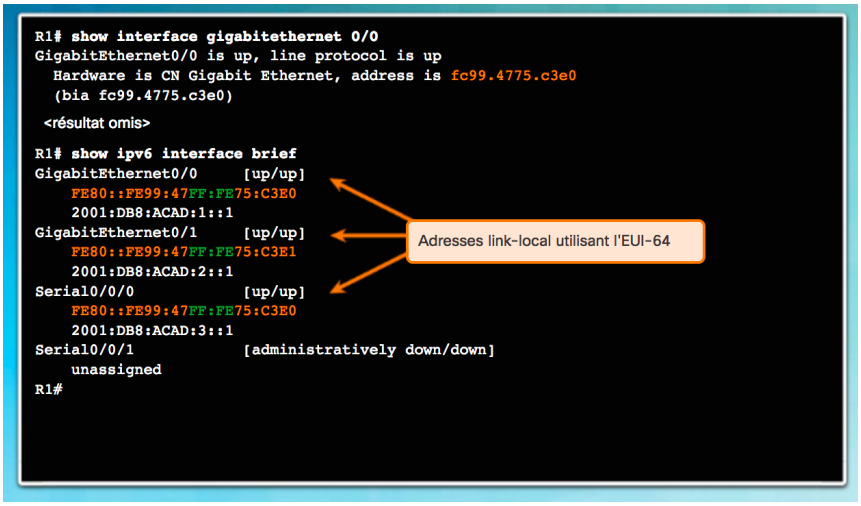



figure 3

Tous les périphériques IPv6 doivent avoir une adresse link-local IPV6. Une adresse link-local peut être établie dynamiquement ou configurée manuellement comme adresse link-local statique.

La figure 1 montre que l'adresse link-local est créée dynamiquement à partir du préfixe FE80::/10 et de l'ID d'interface à l'aide de la méthode EUI-64 ou d'un nombre à 64 bits généré aléatoirement. Les systèmes d'exploitation utilisent généralement la même méthode pour une adresse de diffusion globale créée par une SLAAC et pour une adresse link-local attribuée dynamiquement, comme le montre la figure 2.

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. Pour les interfaces série, le routeur utilise l'adresse MAC d'une interface Ethernet. Souvenez-vous qu'une adresse link-local doit être unique seulement sur sa liaison ou son réseau. Toutefois, un inconvénient de l'utilisation de l'adresse locale-lien attribuée dynamiquement est son long ID d'interface : il est en effet difficile d'identifier et de mémoriser les adresses attribuées. La figure 3 indique l'adresse MAC sur l'interface GigabitEthernet 0/0 de R1. Cette adresse est utilisée pour créer l'adresse link-local sur la même interface.

Pour simplifier l'identification et la mémorisation de ces adresses sur les routeurs, il est courant de configurer les adresses link-local IPv6 de manière statique sur les routeurs.
La Figure 1 illustre le format d'une adresse link-local IPv6. La figure met en évidence les dix premiers bits au format binaire définis sur 1111111010, qui est FE80::/10 10. Les 54 bits restants dans le préfixe sont normalement définis sur zéro. L'ID d'interface de 64 bits peut être dérivée via la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement. La figure 2 présente deux fenêtres de ligne de commande Windows. Les deux fenêtres montrent la sortie de la commande « ipconfig ». Dans la fenêtre supérieure, l'adresse link-local a été générée à l'aide de la méthode EUI-64. Dans la fenêtre inférieure, l'adresse link-local a été créée à l'aide d'un nombre à 64 bits généré aléatoirement pour l'ID d'interface. La figure 3 présente la sortie de la commande « show interface gigabitethernet 0/0 » sur un routeur. L'adresse MAC fc99.4775.c3e0 est mise en surbrillance. La deuxième commande exécutée est « show ipv6 interface brief ». La sortie de cette commande vérifie que le routeur utilise la même adresse link-local sur les trois interfaces IPv6 actives. L'adresse link-local a été générée à l'aide de la méthode EUI-64.

## 2.14 Adresses link-local statiques.

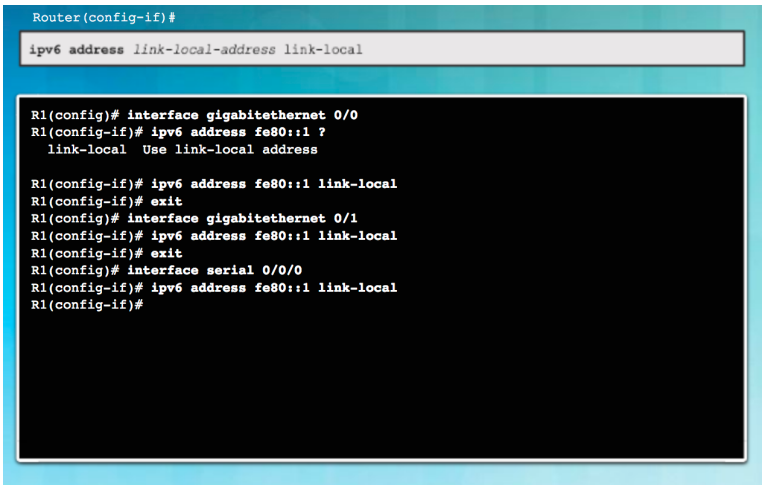



figure 1

La configuration manuelle de l'adresse link-local permet de créer une adresse qui est reconnaissable et plus facile à mémoriser. Il est généralement nécessaire de créer des adresses locales-liens reconnaissables sur les routeurs. Cela est avantageux dans la mesure où les adresses locales-liens du routeur sont utilisées comme des adresses de passerelle par défaut, ainsi que lors du routage des messages d'annonce.

Les adresses link-local peuvent être configurées manuellement avec la même commande d'interface que celle utilisée pour créer des adresses de diffusion globale IPv6. Cependant, dans ce cas, le paramètre **link-local** doit également être utilisé. Lorsqu'une adresse commence par cet hextet dans la plage FE80 à FEBF, le paramètre link-local doit suivre l'adresse.

La figure ci-contre montre la configuration d'une adresse link-local à l'aide de la commande d'interface **ipv6 address**. L'adresse link-local FE80::1 est utilisée pour indiquer clairement qu'elle appartient au routeur R1. La même adresse link-local IPv6 est configurée sur toutes les interfaces du routeur R1. L'adresse FE80::1 peut être configurée sur chaque liaison, car elle ne doit être unique que sur cette liaison.

Tout comme le routeur R1, le routeur R2 serait configuré avec FE80::2 comme adresse link-local IPv6 sur toutes ses interfaces.

## 2.15 Vérifier la configuration des adresses IPV6.

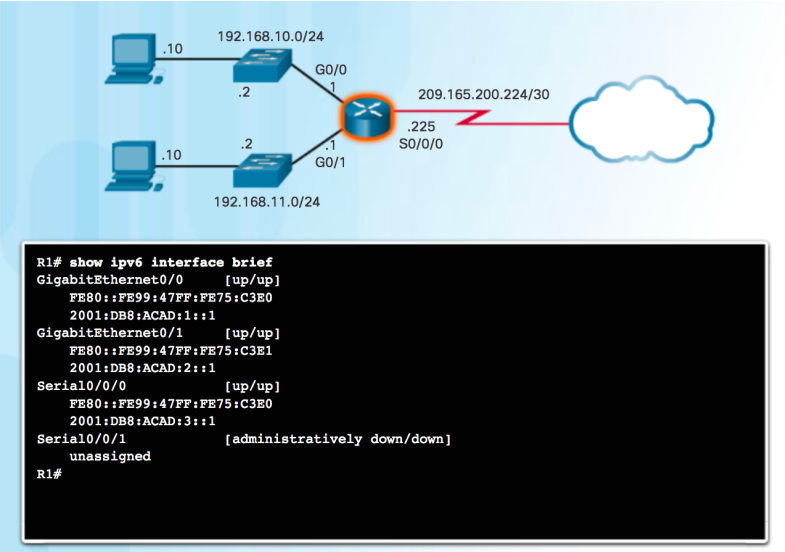



figure 1

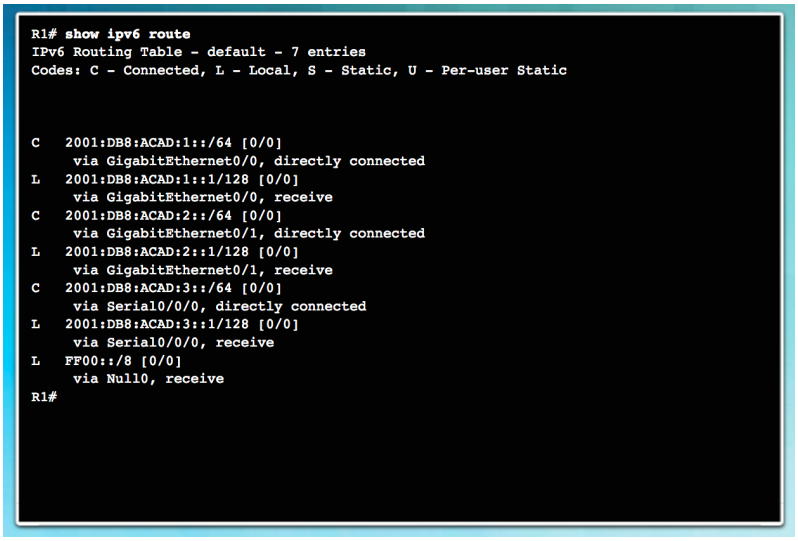



figure 2

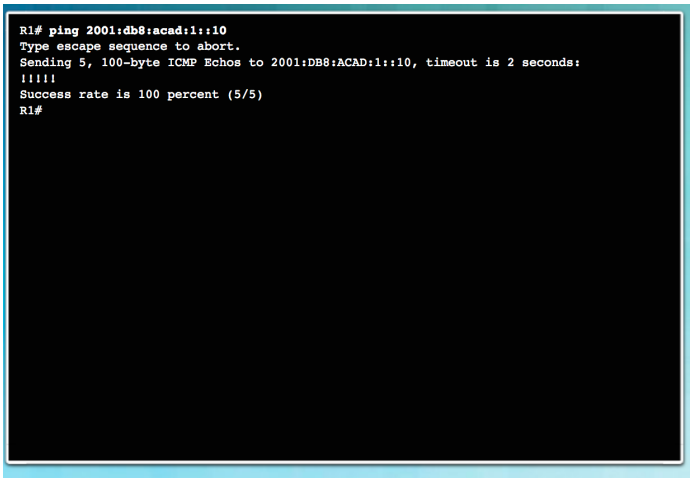



figure 3

Comme l'illustre la figure 1, la commande permettant de vérifier la configuration de l'interface IPv6 est comparable à la commande utilisée pour l'IPv4.

La commande **show interface** affiche l'adresse MAC des interfaces Ethernet. Le processus EUI-64 utilise cette adresse MAC pour générer l'ID d'interface de l'adresse link-local. En outre, la commande **show ipv6 interface brief** affiche des résultats abrégés pour chacune des interfaces. Les termes **[up/up]** sur la même ligne que l'interface indiquent l'état de l'interface de couche 1/couche 2. Ces états correspondent aux colonnes **Status** et **Protocol** de la commande IPv4 équivalente.

Notez que chaque interface possède deux adresses IPv6. La deuxième adresse de chaque interface est l'adresse de diffusion globale qui a été configurée. La première adresse, celle qui commence par FE80, est l'adresse de monodiffusion link-local de l'interface. Souvenez-vous que l'adresse link-local est automatiquement ajoutée à l'interface lorsqu'une adresse de diffusion globale est attribuée.

Notez également que l'adresse link-local de l'interface série 0/0/0 du routeur R1 est identique à celle de l'interface GigabitEthernet 0/0. Les interfaces série n'ont pas d'adresse MAC Ethernet. Cisco IOS utilise donc l'adresse MAC de la première interface Ethernet disponible. Cela est possible, car les interfaces link-local ne doivent être uniques que sur une liaison.

L'adresse link-local de l'interface du routeur est généralement l'adresse de la passerelle par défaut des périphériques sur cette liaison ou sur ce réseau.

Comme l'illustre la figure 2, la commande **show ipv6 route** peut être utilisée pour vérifier que les adresses des interfaces IPv6 spécifiques et des réseaux IPv6 ont été insérées dans la table de routage IPv6. La commande **show ipv6 route** n'affiche que les réseaux IPv6 et non les réseaux IPv4.

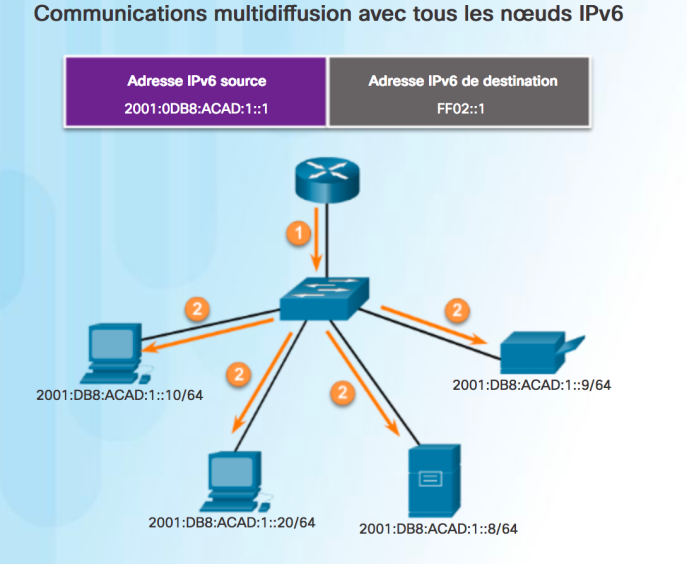
Dans la table de routage, la lettre **C** placée en regard d'une route indique qu'il s'agit d'un réseau connecté directement. Lorsque l'interface de routeur est configurée avec une adresse de diffusion globale et que son état est « up/up », le préfixe IPv6 et la longueur de préfixe sont ajoutés à la table de routage IPv6 en tant que route connectée.
**Remarque** : le **L** indique une route locale, l'adresse IPv6 attribuée à l'interface. Il ne s'agit pas d'une adresse locale-lien. Les adresses locales-liens ne sont pas incluses dans la table de routage du routeur car il ne s'agit pas d'adresses routables.

L'adresse de diffusion globale IPv6 configurée sur l'interface est également insérée dans la table de routage en tant que route locale. Le préfixe de la route locale est /128. Des routes locales sont utilisées par la table de routage pour traiter efficacement les paquets dont l'adresse de destination est l'adresse de l'interface du routeur.

La commande **ping** pour l'IPv6 est identique à la commande utilisée avec l'IPv4, excepté qu'une adresse IPv6 est utilisée. Comme l'illustre la figure 3, cette commande permet de vérifier la connectivité de couche 3 entre le routeur R1 et l'ordinateur PC1. Lorsqu'un utilisateur envoi une requête ping à une adresse link-local à partir d'un routeur, Cisco IOS l'invite à entrer l'interface de sortie. Comme l'adresse link-local de destination peut être sur une ou plusieurs de ses liaisons ou sur un ou plusieurs de ses réseaux, le routeur doit savoir à quelle interface envoyer la requête ping.

La figure 1 illustre une topologie dans laquelle un routeur est connecté à deux LAN et un WAN. Sous la topologie, la fenêtre de commande affiche la sortie de la commande « show ipv6 interface brief ». Les trois interfaces sont signalées comme « up » et « up », c'est-à-dire activées. La figure 2 présente la sortie de la commande « show ipv6 route » avec trois réseaux connectés répertoriés, ainsi que leur réseau local. Le réseau FE00::/8 est aussi listé. La figure 3 présente la fenêtre de commande du routeur 1 avec l'envoi réussi d'une requête ping vers l'un des ordinateurs sur un LAN connecté à R1. La figure 4 est un exercice avec un vérificateur de syntaxe qui permet à l'étudiant de mettre en pratique l'exécution de commandes pour vérifier la configuration d'adresse IPv6.

## 2.16 Les adresses de multidiffusion IPV6 attribuées.




Les adresses de multidiffusion IPv6 sont semblables aux adresses de multidiffusion IPv4. Rappelez-vous qu'une adresse de multidiffusion est utilisée pour envoyer un même paquet à un ou plusieurs destinataires (groupe de multidiffusion). Les adresses de multidiffusion IPv6 ont le préfixe FF00::/8.

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

Il existe deux types d'adresses de multidiffusion IPv6 :

- Les adresses de multidiffusion attribuées
- les adresses de multidiffusion de nœud sollicité

### Adresses de multidiffusion attribuées

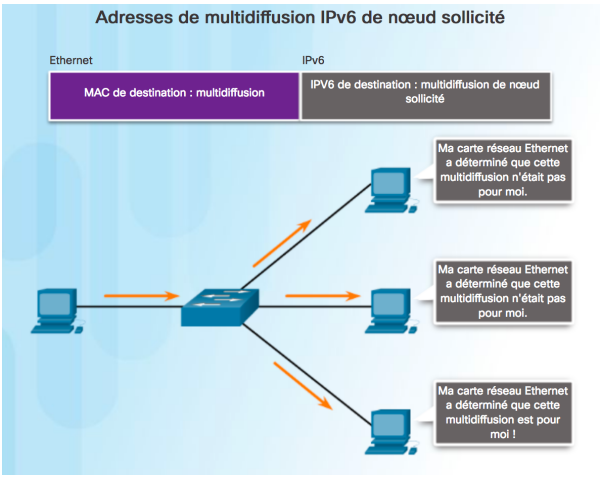
Les adresses de multidiffusion attribuées sont des adresses de multidiffusion réservées à des groupes ou périphériques prédéfinis. Une adresse de multidiffusion attribuée est une adresse unique utilisée pour joindre un groupe de périphériques exécutant un service ou un protocole commun. Les adresses de multidiffusion attribuées sont utilisées avec des protocoles spécifiques, tels que DHCPv6.

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

- **Groupe de multidiffusion vers tous les nœuds FF02::1** - il s'agit d'un groupe de multidiffusion que tous les périphériques IPv6 peuvent rejoindre. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau. Cette opération a le même effet qu'une adresse de diffusion IPv4. La figure illustre un exemple de communication via l'adresse de multidiffusion à tous les nœuds. Un routeur IPv6 envoie des messages d'annonce de routeur ICMPv6 au groupe de multidiffusion à tous les nœuds. Le message d'annonce de routeur indique à tous les périphériques IPv6 du réseau les informations d'adressage telles que le préfixe, la longueur du préfixe et la passerelle par défaut.
- **Groupe de multidiffusion vers tous les routeurs FF02::2** il s'agit d'un groupe de multidiffusion que peuvent rejoindre tous les routeurs IPv6. 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 périphériques IPv6 envoient des messages de sollicitation du routeur ICMPv6 (RS) à l'adresse de multidiffusion à tous les routeurs. Le message RS demande un message d'annonce au routeur IPv6 (RA) pour faciliter la configuration de l'adresse du périphérique.

## 2.17 Adresses de multidiffusion IPV6 de nœud sollicité.




Une adresse de multidiffusion de nœud sollicité est comparable à une adresse de multidiffusion à tous les nœuds. Elle offre l'avantage d'être mappée à une adresse de multidiffusion Ethernet spéciale. Cela permet à la carte réseau Ethernet de filtrer la trame en examinant l'adresse MAC de destination sans l'envoyer au processus IPv6 pour voir si le périphérique est la cible prévue du paquet IPV6.

## 3. Vérification de la connectivité :

### 3.1 ICMPV4 et ICMPV6.

Bien que le protocole IP tâche de réaliser ses promesses, la suite TCP/IP permet d'envoyer des messages si certaines erreurs se produisent. Ces messages sont envoyés via les services du protocole ICMP. Ces messages ont pour objectif de fournir des commentaires sur les problèmes liés au traitement de paquets IP dans certaines circonstances. Les messages ICMP ne sont pas obligatoires et sont souvent interdits sur les réseaux pour des raisons de sécurité.

Le protocole ICMP est disponible pour IPv4 et IPv6. ICMPv4 est le protocole de message des réseaux IPv4. ICMPv6 fournit également ces services pour l'IPv6, en ajoutant d'autres fonctionnalités. Dans ce cours, le terme ICMP fait référence à l'ICMPv4 et à l'ICMPv6.
Il existe différents types de message ICMP, et les raisons pour lesquelles ils sont envoyés sont très diverses. Nous décrirons les messages les plus courants.

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)

**Host Confirmation (Confirmation de l'hôte)**

Un message ICMP Echo (Écho ICMP) permet de déterminer si un hôte est fonctionnel. 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. Sur la figure ci-contre, cliquez sur le bouton Lecture pour lancer une animation sur les requêtes et les réponses d'écho ICMP. L'utilisation de messages ICM Echo est à la base de l'utilitaire ping.

**Destination or Service Unreachable (destination ou service inaccessible)**

Lorsqu'un hôte ou une passerelle ne peut pas acheminer un paquet reçu, il ou elle peut utiliser un message ICMP de destination inaccessible pour avertir la source que la destination ou le service est inaccessible. Ce message comprend un code indiquant pourquoi le paquet n'a pas pu être acheminé.

Certains des codes de destination inaccessible pour l'ICMPv4 sont :

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

**Remarque** : les codes des messages de destination inaccessible utilisés par l'ICMPv6 diffèrent légèrement.

**Dépassement du délai**

Un message de dépassement de délai ICMPv4 est utilisé par un routeur pour indiquer qu'il ne peut pas transférer un paquet, car le champ TTL de durée de vie du paquet a atteint 0. Si un routeur reçoit un paquet et décrémente le champ TTL de durée de vie du paquet IPv4 jusqu'à atteindre zéro, il abandonne le paquet et envoie un message de dépassement de délai à l'hôte source.

Si le routeur ne peut pas transmettre un paquet IPv6 parce que celui-ci a expiré, le protocole ICMPv6 envoie également un message de dépassement de délai. Les paquets IPv6 n'ont pas de champ de durée de vie TTL : le champ de limite de nombre de tronçons est utilisé pour déterminer si le paquet a expiré.

La figure est une animation présentant un ordinateur avec une adresse IPv4 192.168.10.1 qui envoie une requête d'écho ICMP à un ordinateur avec une adresse IPv4 192.168.30.1. Le message part de l'ordinateur expéditeur et passe par un commutateur pour atteindre ensuite un routeur. Ce routeur envoie la requête à un autre routeur, puis à un commutateur et enfin à l'ordinateur de destination. L'ordinateur récepteur renvoie alors un de réponse d'écho ICMP.

### 3.2 Messages de sollicitation et d'annonce de routeur ICMPV6.

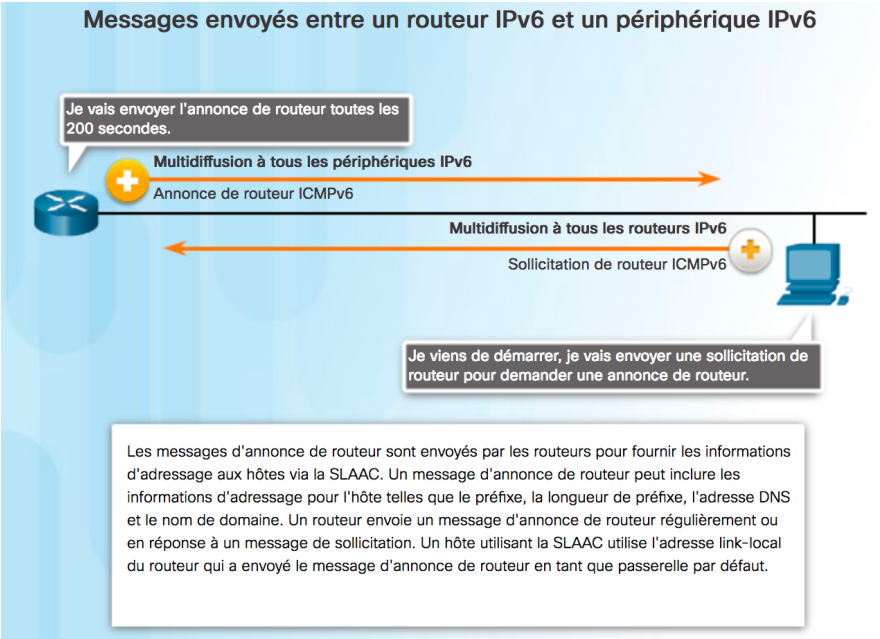



figure 1

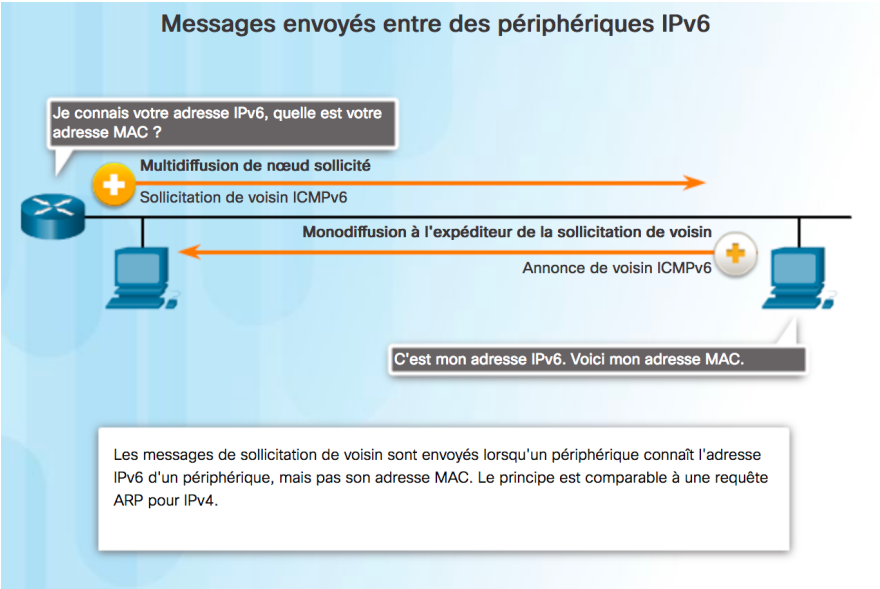



figure 2

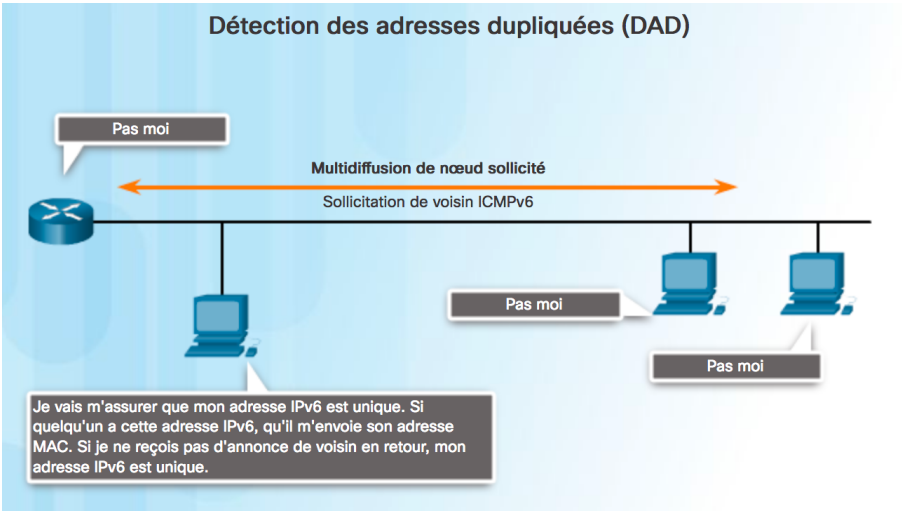



figure 3

Les messages d'informations et d'erreur du protocole ICMPv6 ressemblent fortement aux messages de contrôle et d'erreur mis en œuvre par le protocole ICMPv4. Cependant, l'ICMPv6 offre de nouvelles fonctions et fonctionnalités avancées qui n'existent pas dans l'ICMPv4. Les messages ICMPv6 sont encapsulés dans l'IPv6.

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

- Messages envoyés entre un routeur IPv6 et un périphérique IPv6 :
- Message de sollicitation de routeur (RS)
- Message d'annonce de routeur (RA)
- Messages envoyés entre des périphériques IPv6 :
- Message de sollicitation de voisin
- Messages d'annonce de voisin

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

La Figure 1 illustre un exemple d'échange de messages de sollicitation et d'annonce de routeur entre un ordinateur et un routeur. Cliquez sur chaque message pour obtenir plus d'informations.

Les messages de sollicitation et d'annonce de voisin sont utilisés pour la résolution d'adresse et la détection d'adresse dupliquée (DAD).

**Résolution d'adresse**

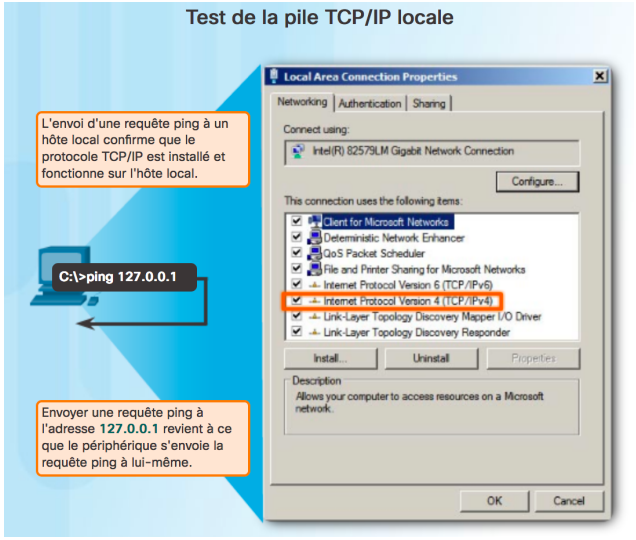
La résolution d'adresse est utilisée lorsqu'un périphérique du réseau local (LAN) connaît l'adresse de monodiffusion IPv6 d'une destination, mais pas son adresse MAC Ethernet. Pour déterminer l'adresse MAC de destination, le périphérique envoie un message de sollicitation de voisin à l'adresse du nœud sollicité. Le message inclut l'adresse IPv6 (ciblée) connue. Le périphérique portant l'adresse IPv6 ciblée répond par un message d'annonce de voisin qui inclut son adresse MAC Ethernet. La Figure 2 illustre deux ordinateurs échangeant des messages de sollicitation et d'annonce de voisin. Cliquez sur chaque message pour obtenir plus d'informations.

**Détection des adresses dupliquées**
Lorsqu'une adresse de monodiffusion globale ou de monodiffusion link-local est attribuée à un périphérique, il est recommandé d'utiliser la détection d'adresse dupliquée pour s'assurer que l'adresse est unique. 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, comme le montre la Figure 3. Si cette adresse est attribuée à un autre périphérique du réseau, ce dernier répond en envoyant un message d'annonce de voisin. Ce message informe le périphérique expéditeur que l'adresse est utilisée. Si aucun message d'annonce de voisin n'a été renvoyé au bout d'un certain temps, l'adresse de monodiffusion est unique et peut être utilisée.

**Remarque** : la détection d'adresse dupliquée n'est pas obligatoire, mais le RFC 4861 recommande de l'utiliser sur les adresses de monodiffusion.

La figure 1 montre un ordinateur qui démarre et envoie une sollicitation de routeur (RS) demandant une annonce de routeur (RA). Le routeur envoie des annonces de routeur toutes les 200 secondes. Cliquez sur les deux types de messages pour afficher des informations complémentaires. Dans la figure 2, un ordinateur connaît l'adresse IPv6 d'un autre ordinateur, mais pas l'adresse MAC. Il envoie un message de sollicitation de voisin (NS) sous la forme d'un message à multidiffusion de nœud sollicité. L'ordinateur répond en envoyant un message de monodiffusion NS. La figure 3 illustre un processus DAD avec un ordinateur utilisant un message de multidiffusion de nœud sollicité pour s'assurer que les autres ordinateurs ne sont pas en train d'utiliser l'adresse IPv6 que l'ordinateur veut utiliser.

### 3.3 Tester la pile locale.




La commande ping est un utilitaire de test qui utilise des messages de requête et de réponse d'écho ICMP pour tester la connectivité entre les hôtes. Le ping fonctionne avec les hôtes IPv4 et IPv6.

Pour tester la connectivité avec un autre hôte sur un réseau, une requête d'écho est envoyée à l'adresse d'hôte au moyen de la commande ping. Si l'hôte à l'adresse spécifiée reçoit une requête d'écho, il répond en envoyant une réponse d'écho. Chaque fois qu'une réponse d'écho est reçue, la commande ping vous informe du temps qui s'écoule entre l'envoi de la requête et la réception de la réponse. Cela peut être utilisé pour mesurer les performances réseau.

La commande ping intègre un délai d'attente de la réponse. Si aucune réponse n'est reçue dans ce délai, la commande ping indique dans un message que la réponse n'a pas été reçue. Cela signale généralement un problème, mais cela peut également indiquer que des fonctions de sécurité de blocage des messages ping sont activées sur le réseau.

Une fois toutes les requêtes envoyées, l'utilitaire ping affiche un résumé qui inclut le taux de réussite et la durée de transmission moyenne à destination.

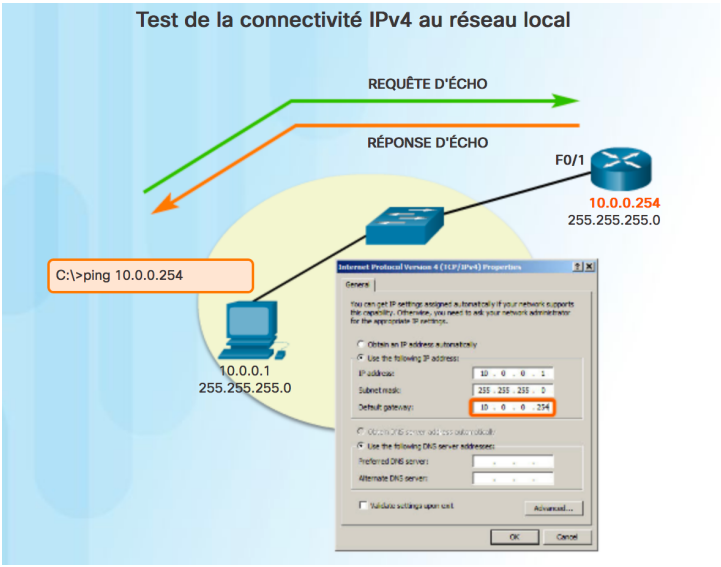
**Envoi d'une requête ping sur le bouclage local**

La commande ping s'utilise également dans certaines activités de test et de vérification. Par exemple, dans un test de la configuration interne IPv4 ou IPv6 sur l'hôte local. Pour réaliser ce test, nous exécutons la commande ping sur l'adresse de bouclage locale 127.0.0.1 pour l'IPv4 (et ::1 pour l'IPv6). Le test de bouclage IPv4 est illustré dans la figure ci-contre.

Une réponse provenant de l'adresse 127.0.0.1 pour l'IPv4 ou ::1 pour l'IPv6 indique que le protocole IP est correctement installé sur l'hôte. Cette réponse provient de la couche réseau. Toutefois, elle n'indique pas que les adresses, les masques ou les passerelles sont correctement configurés. Par ailleurs, elle n'indique rien sur l'état de la couche la plus basse de la pile réseau. Elle teste uniquement la configuration IP via la couche réseau du protocole IP. Si un message d'erreur est généré, cela indique que la suite TCP/IP ne fonctionne pas sur l'hôte.

La figure présente l'utilitaire de ligne de commande permettant de tester la pile TCP/IP locale sur un ordinateur exécutant IPv4. La commande est ping 127.0.0.1.

### 3.4 Ping – tester la connectivité avec le réseau local.




Vous pouvez également utiliser la commande ping pour tester la capacité d'un hôte à communiquer sur le réseau local. Cela consiste généralement à envoyer une requête ping à l'adresse IP de la passerelle de l'hôte. Une requête ping à la passerelle indique si l'hôte et l'interface du routeur qui sert de passerelle sont opérationnels sur le réseau local.

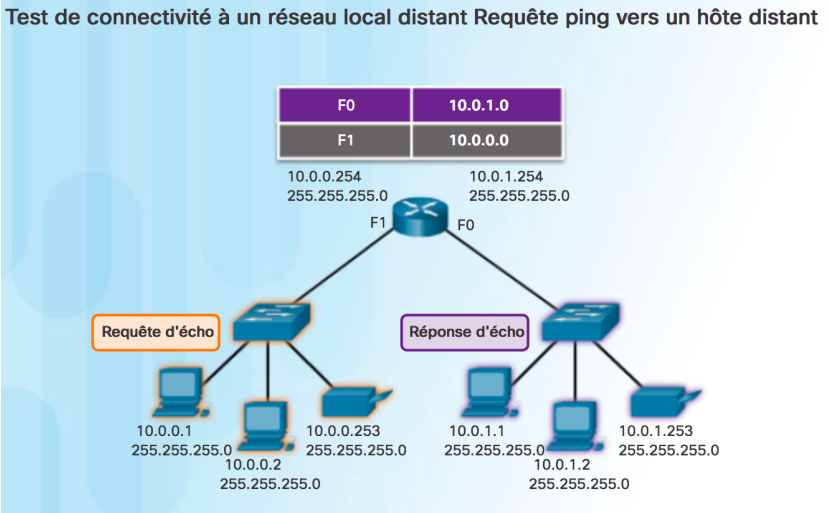
Pour ce test, l'adresse de la passerelle est souvent utilisée, car le routeur est, en principe, toujours opérationnel. Si l'adresse de la passerelle ne répond pas, une requête ping peut être envoyée à l'adresse IP d'un autre hôte qui est opérationnel sur le réseau local.

Si une réponse est obtenue, soit de la passerelle, soit d'un autre hôte, cela signifie que l'hôte local peut communiquer sans problème sur le réseau local. Si la passerelle ne répond pas, mais qu'un autre hôte répond, cela peut indiquer un problème sur l'interface du routeur qui sert de passerelle.

Il se peut qu'une adresse de passerelle incorrecte ait été configurée sur l'hôte. Peut-être que l'interface du routeur est fonctionnelle, mais qu'une règle de sécurité en vigueur l'empêche de traiter des requêtes ping ou d'y répondre.

La figure montre un routeur avec un commutateur connecté à son port FastEthernet 0/1. L'adresse IPv4 du port est 10.0.0.254. Un ordinateur est connecté au commutateur. Son adresse IPv4 est 10.0.0.1. L'ordinateur teste la connectivité au routeur, qui est la passerelle par défaut, en utilisant une commande ping pour envoyer une demande d'écho au port du routeur. La commande utilisée est ping 10.0.0.254. Le routeur envoie une réponse d'écho en retour.

### 3.5 Ping – tester la connectivité à distance.




La commande ping peut aussi être utilisée pour tester la capacité d'un hôte local à communiquer sur un interréseau. L'hôte local peut envoyer une requête ping à un hôte IPv4 opérationnel sur un réseau distant, comme présenté dans la figure ci-contre.

Si cette requête ping aboutit, le fonctionnement d'une grande partie de l'interréseau peut être vérifié. Une requête ping réussie sur un interréseau confirme la communication sur le réseau local, le fonctionnement du routeur qui sert de passerelle et le fonctionnement de tous les autres routeurs sur le chemin entre le réseau local et le réseau de l'hôte distant.
En outre, la fonctionnalité de l'hôte distant peut être vérifiée. Si l'hôte distant ne peut pas communiquer en dehors de son réseau local, il ne répond pas.

**Remarque** : de nombreux administrateurs réseau limitent ou interdisent l'entrée des messages ICMP dans le réseau d'entreprise. Par conséquent, l'absence d'une réponse ping peut être due à des restrictions de sécurité.

### 3.6 Traceroute – test du chemin.

La commande ping permet de tester la connectivité entre deux hôtes, mais ne fournit pas d'informations sur les détails des périphériques entre les hôtes. Traceroute (tracert) est un utilitaire qui génère la liste des tronçons empruntés sur le chemin. Cette liste peut fournir d'importantes informations pour la vérification et le dépannage. Si les données parviennent à destination, la commande affiche la liste des interfaces de tous les routeurs situés entre les hôtes. Si les données restent bloquées au niveau d'un tronçon, l'adresse du dernier routeur ayant répondu à la commande peut fournir une indication sur l'endroit où se situe le problème ou sur d'éventuelles restrictions de sécurité.

**Durée de transmission ou RTT (Round Trip Time)**

L'exécution de la commande traceroute fournit la durée de transmission sur chacun des tronçons rencontrés sur le chemin et indique si un tronçon n'a pas répondu. La durée de transmission correspond à la durée nécessaire à un paquet pour atteindre l'hôte distant, plus le temps mis par l'hôte pour répondre. Un astérisque (*) indique un paquet perdu ou sans réponse.

Cette information permet de localiser un routeur problématique sur le chemin. Si un tronçon est associé à des temps de réponse longs ou à une perte de données, cela indique que les ressources du routeur ou que ses connexions sont saturées.

**TTL IPv4 et limite du nombre de tronçons IPv6**

La commande traceroute utilise une fonction du champ TTL du protocole IPv4 et le champ de limite de nombre de tronçons du protocole IPv6 dans les en-têtes de couche 3, ainsi que le message ICMP de dépassement de délai.

La première séquence des messages envoyés par traceroute contient un champ TTL égal à 1. Cela entraîne l'expiration du champ TTL de durée de vie du paquet IPv4 au niveau du premier routeur. Ce routeur répond ensuite en envoyant un message ICMPv4. L'utilitaire traceroute dispose à présent de l'adresse du premier tronçon.

Puis, il incrémente progressivement le champ TTL (2, 3, 4, etc.) pour chaque séquence de messages. Cela permet d'obtenir l'adresse de chaque tronçon, à mesure que les paquets expirent sur le chemin restant. Le champ TTL est incrémenté jusqu'à ce que la destination soit atteinte ou jusqu'à une valeur maximale prédéfinie.

Après que la destination finale a été atteinte, l'hôte répond par un message ICMP Port Unreachable (port inaccessible) ou ICMP Echo Reply (réponse d'écho), à la place du message ICMP Time Exceeded (délai dépassé).