Adressage de réseaux

5.1 Adresses IP et masques de sous-réseau

5.1.1 Rôle de l'adresse IP

Un hôte a besoin d'une adresse IP pour participer aux activités sur Internet. L'adresse IP est une adresse réseau logique qui identifie un hôte donné. Elle doit être unique et correctement configurée pour toute communication avec d'autres périphériques sur Internet.

Une adresse IP est attribuée à la connexion de l'interface réseau d'un hôte. Cette connexion se présente généralement sous la forme d'une carte réseau installée dans le périphérique. Les stations de travail, serveurs, imprimantes réseau et téléphones IP sont des exemples de périphériques utilisateurs dotés d'interfaces réseau. Certains serveurs peuvent avoir plusieurs cartes réseau, qui ont chacune leur propre adresse IP. Les interfaces du routeur fournissant des connexions à un réseau IP ont également une adresse IP.

Chaque paquet envoyé via Internet dispose d'une adresse IP source et d'une adresse IP de destination. Les périphériques réseau ont besoin de ces informations pour garantir que les informations arrivent à destination et que toutes les réponses sont renvoyées à la source.

Exercice Packet Tracer 1

Utilisez Packet Tracer pour envoyer une requête ping à différents sites Web.

5.1.2 Structure de l'adresse IP

Une adresse IP consiste simplement en une série de 32 bits binaires (des un et des zéro). Il est très difficile pour l'être humain de lire une adresse IP binaire. Pour cette raison, les 32 bits sont regroupés en quatre multiplets de 8 bits appelés octets. Avec ce format, il est difficile pour un être humain de lire, d'écrire et de mémoriser une adresse IP. Pour que l'adresse IP soit plus facile à comprendre, chaque octet est présenté dans sa valeur décimale, séparée par une virgule décimale ou un point décimal. C'est ce qu'on appelle la notation en décimale à point.

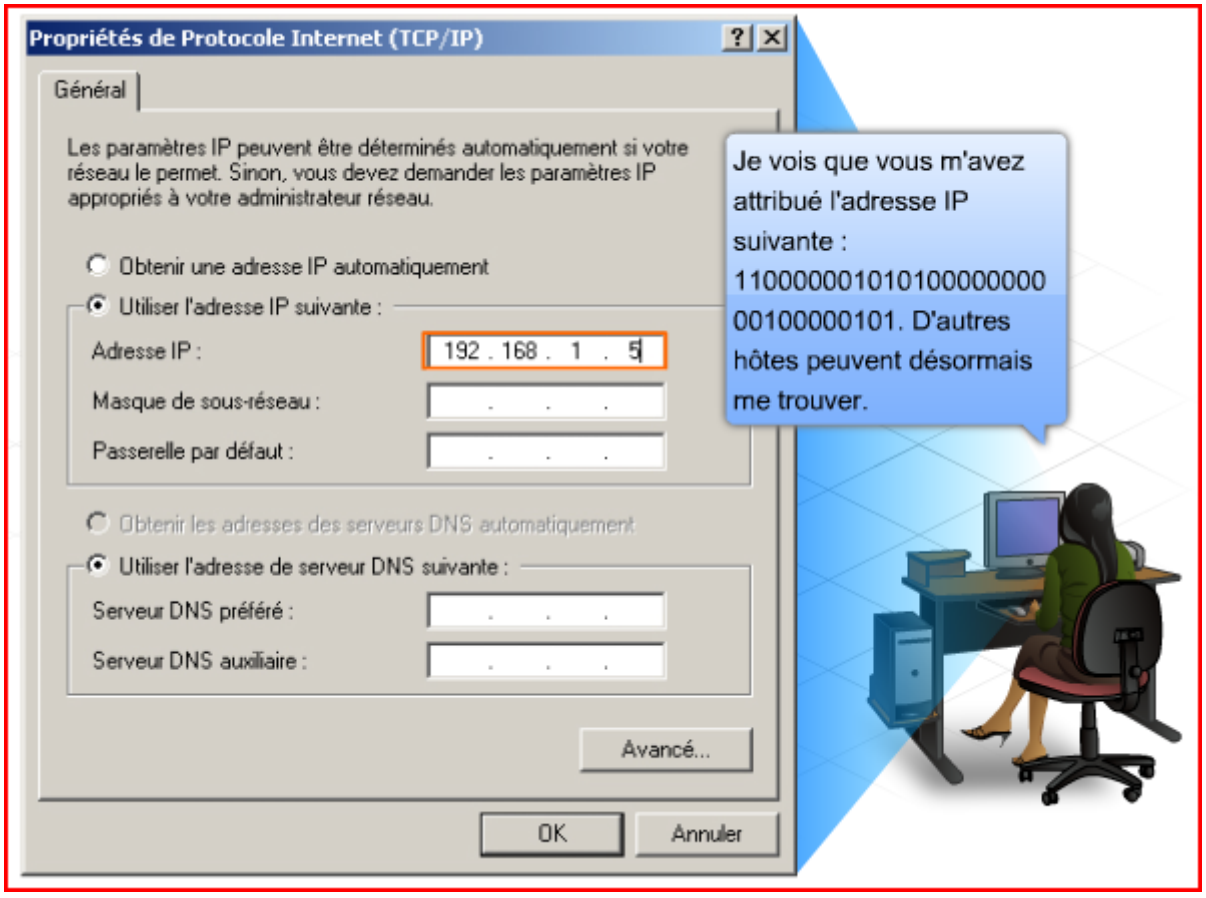
Lorsqu'un hôte est configuré avec une adresse IP, celle-ci est entrée sous la forme de nombre en décimale à point, tel que 192.168.1.5. Supposez que vous devez entrer l'équivalent binaire à 32 bits de 11000000101010000000000100000101. Si ne serait-ce qu'un bit n'est pas saisi correctement, l'adresse est différente, et l'hôte ne pourra peut-être pas communiquer sur le réseau.

L'adresse IP 32 bits est définie avec IP version 4 (IPv4).

IPv4

Internet Protocol version 4. Version actuelle du protocole Internet.

Il s'agit actuellement de la forme la plus courante d'adresse IP sur Internet. Il existe environ 4 milliards d'adresses IP possibles utilisant un système d'adressage 32 bits.



Lorsqu'un hôte reçoit une adresse IP, il regarde l'intégralité des 32 bits tels qu'ils sont reçus par la carte réseau. Les êtres humains, quant à eux, doivent convertir ces 32 bits dans leur équivalent décimal à quatre octets.

octet

Nombre décimal situé dans la plage de 0 à 255 qui représente 8 bits.

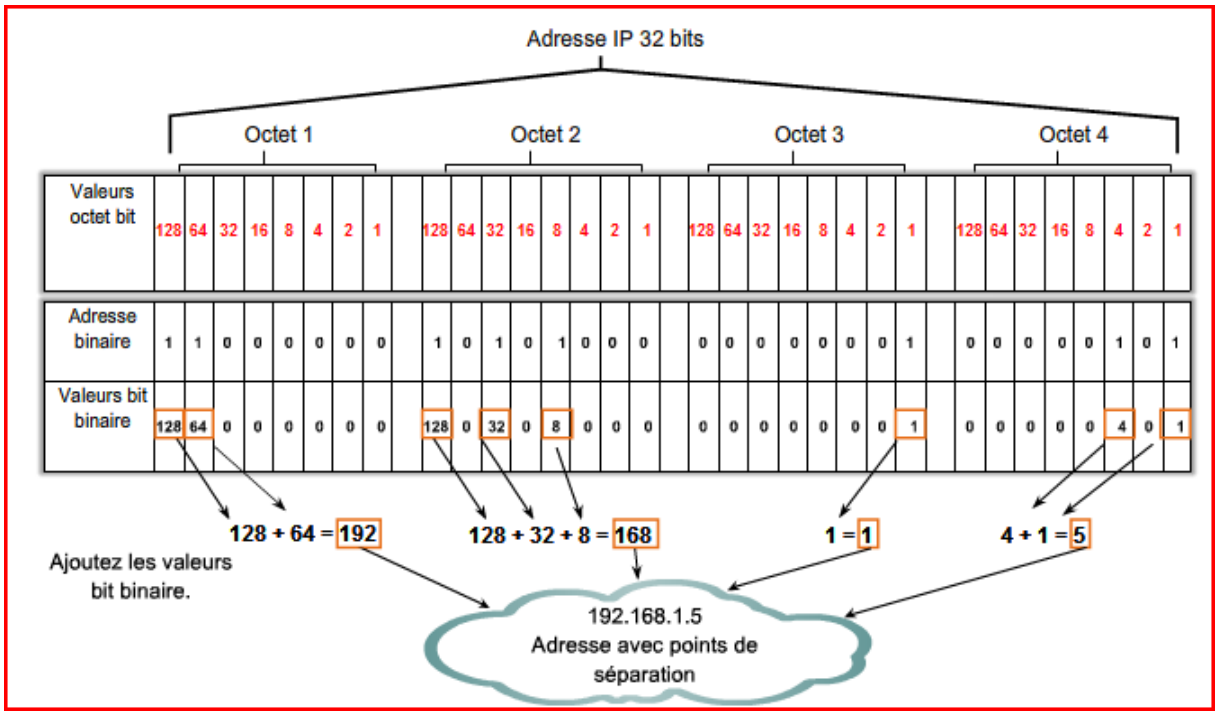
Chaque octet est constitué de 8 bits, qui ont chacun une valeur. Les quatre groupes de 8 bits ont le même ensemble de valeurs. Le bit le plus à droite dans un octet a la valeur 1, et les valeurs des bits restants sont, de droite à gauche, 2, 4, 8, 16, 32, 64 et 128.

Déterminez la valeur de l'octet en ajoutant les valeurs de positions chaque fois qu'un binaire 1 est présent.

- Si, dans un rang, la valeur est 0, n'ajoutez pas de valeur.
- Si les 8 bits sont des 0, 00000000, la valeur de l'octet est 0.
- Si les 8 bits sont des 1, 11111111, la valeur de l'octet est 255 (128+64+32+16+8+4+2+1).

- Si les 8 bits sont composés de 0 et de 1, par exemple 00100111, la valeur de l'octet est 39 (32+4+2+1).

Ainsi, la valeur de chacun des quatre octets peut aller de 0 à 255 au maximum.

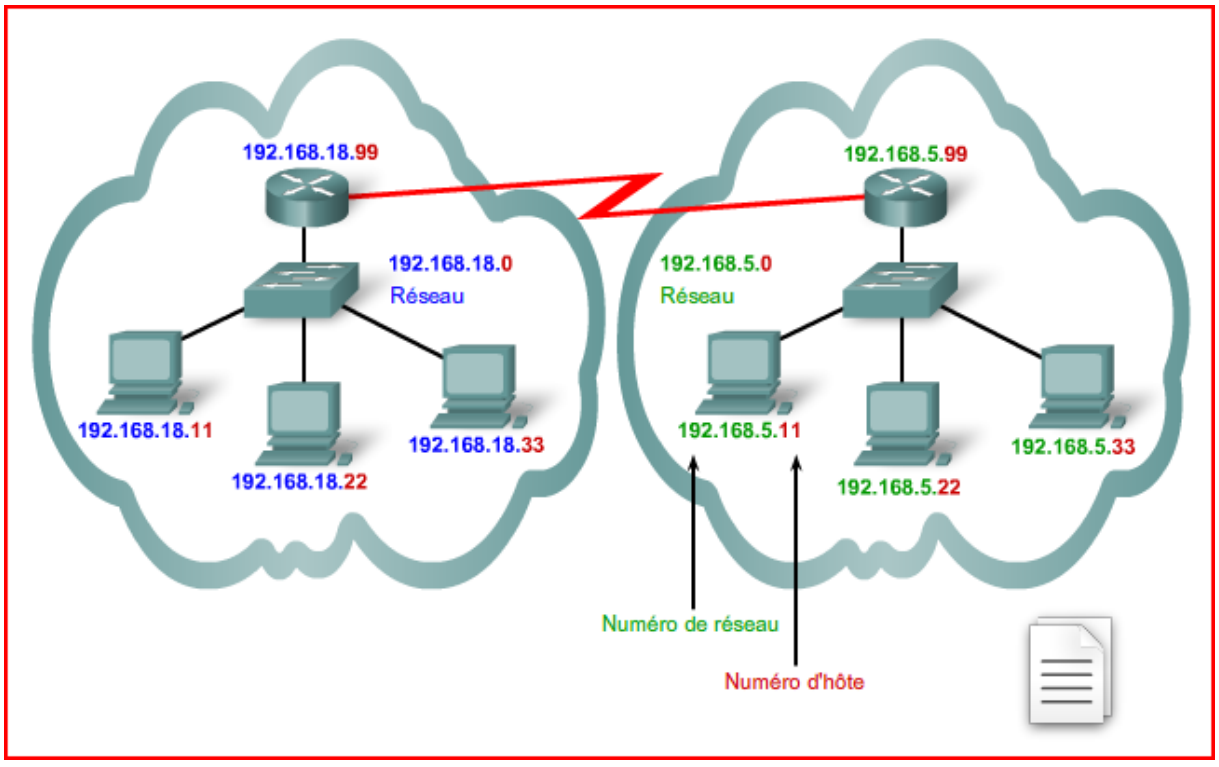


5.1.3 Parties d'une adresse IP

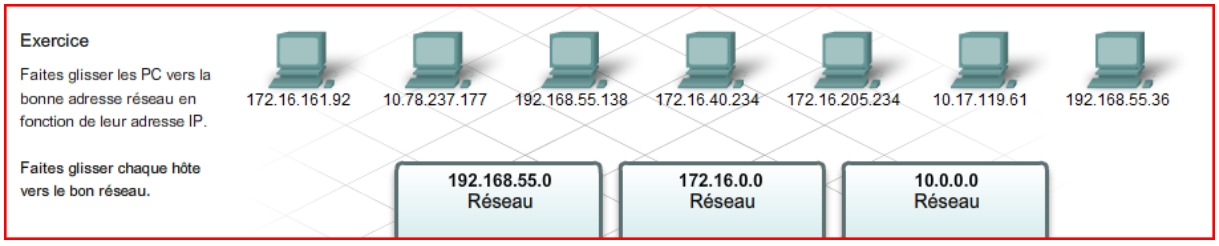
L'adresse IP logique 32 bits est hiérarchique et constituée de deux parties. La première partie identifie le réseau, et la seconde partie identifie un hôte sur ce réseau. Ces deux parties sont nécessaires à l'adresse IP.

À titre d'exemple, si un hôte a pour adresse IP 192.168.18.57, les trois premiers octets (192.168.18) identifient la partie réseau de l'adresse, et le dernier octet (57) identifie l'hôte. On parle d'adressage hiérarchique parce que la partie réseau indique le réseau sur lequel chaque adresse hôte unique se trouve. Les routeurs ont seulement besoin de savoir comment atteindre chaque réseau, sans connaître l'emplacement de chaque hôte individuel.

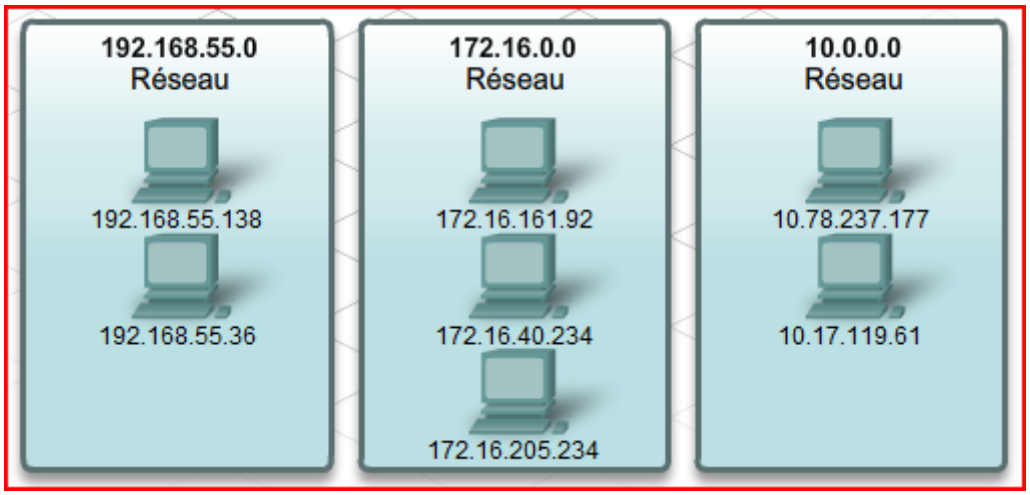
Le système téléphonique est un autre exemple de réseau hiérarchique. Dans le cas d'un numéro de téléphone, l'indicatif de pays, l'indicatif régional et le central téléphonique représentent l'adresse réseau, tandis que les chiffres restants indiquent un numéro de téléphone local.



Application



Solution



5.1.4 Comment les adresses IP et les masques de sous-réseau interagissent-ils ?

Chaque adresse IP contient deux parties. Comment les hôtes savent-ils quelle partie correspond au réseau et quelle partie correspond à l'hôte ? Le masque de sous-réseau permet de le savoir.

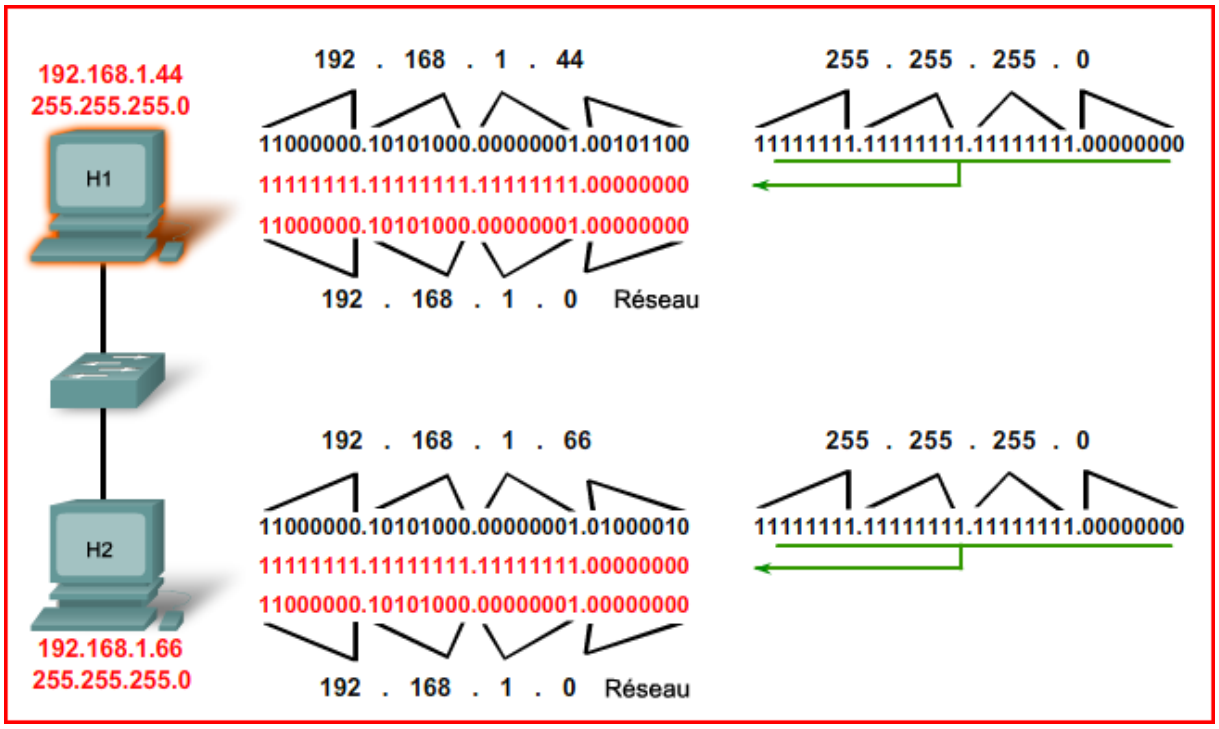
masque de sous-réseau

Masque d'adresse de 32 bits, utilisé dans le protocole IP pour indiquer les bits d'une adresse IP servant à désigner le sous-réseau. Le second groupe de nombres est une adresse IP.

Lorsqu'un hôte IP est configuré, un masque de sous-réseau est attribué avec une adresse IP. Comme l'adresse IP, le masque de sous-réseau est constitué de 32 bits. Le masque de sous-réseau indique quelle partie de l'adresse IP correspond au réseau et quelle partie correspond à l'hôte.

Le masque de sous-réseau est comparé à l'adresse IP de gauche à droite, bit par bit. Les 1 dans le masque de sous-réseau représentent la partie réseau, et les 0 représentent la partie hôte. Dans l'exemple, les trois premiers octets correspondent au réseau, tandis que le dernier octet représente l'hôte.

Lorsqu'un hôte envoie un paquet, il compare son masque de sous-réseau à sa propre adresse IP et à l'adresse IP de destination. Si les bits de réseau correspondent, l'hôte source et l'hôte de destination sont sur le même réseau, et le paquet peut être transmis localement. S'ils ne correspondent pas, l'hôte émetteur transmet le paquet à l'interface du routeur local afin qu'il soit envoyé à l'autre réseau.

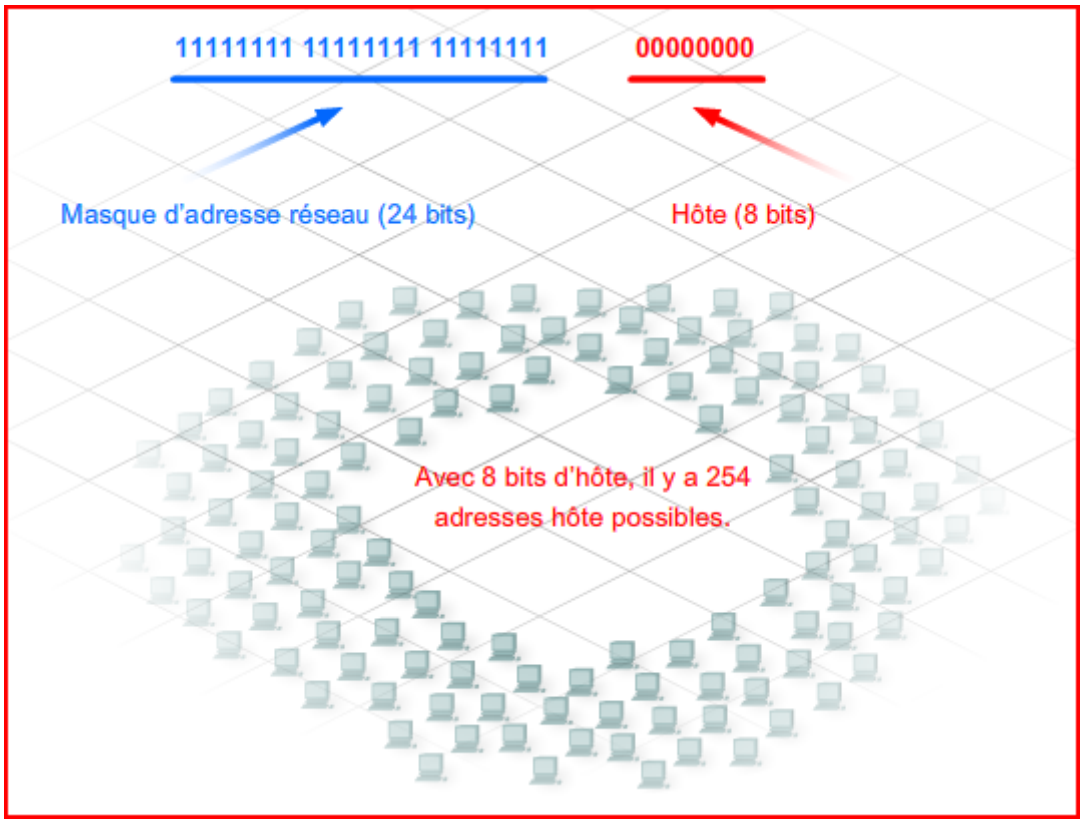


Les masques de sous-réseau rencontrés le plus souvent dans les réseaux domestiques et les réseaux des petites entreprises sont : 255.0.0.0 (8 bits), 255.255.0.0 (16 bits) et 255.255.255.0 (24 bits). Un masque de sous-réseau 255.255.255.0 (décimal) ou 11111111.11111111.1111111.00000000 (binaire) utilise 24 bits pour identifier le numéro de réseau, ce qui laisse 8 bits pour numéroter les hôtes sur ce réseau.

Pour calculer le nombre d'hôtes pouvant se trouver sur ce réseau, mettez le nombre 2 à la puissance du nombre de bits d'hôte (2 ^ 8 = 256). Soustrayez ensuite 2 de ce nombre (256-2). Il est nécessaire de soustraire 2 parce que tous les 1 de la partie hôte d'une adresse IP constituent une adresse de diffusion pour ce réseau et, à ce titre, ils ne peuvent pas être attribués à un hôte spécifique. Tous les 0 de la partie hôte indiquent l'ID réseau et, de même, ne peuvent pas être attribués à un hôte spécifique. Les puissances de 2 peuvent être aisément calculées à l'aide de la calculatrice dont est doté tout système d'exploitation Windows.

Une autre méthode pour déterminer le nombre d'hôtes disponibles consiste à ajouter les valeurs des bits d'hôte disponibles (128+64+32+16+8+4+2+1 = 255). Soustrayez 1 à ce nombre (255-1 = 254), car les bits d'hôte ne peuvent pas tous être des 1. Il n'est pas nécessaire de soustraire 2, car la valeur de tous les 0 est 0 et n'est pas comprise dans l'addition.

Avec un masque de 16 bits, 16 bits (deux octets) sont disponibles pour les adresses d'hôtes. Une adresse d'hôte pourrait avoir tous les 1 (255) dans l'un des octets. L'adresse peut, en apparence, être une diffusion, mais tant que l'autre octet n'est pas exclusivement constitué de 1, il s'agit d'une adresse d'hôte valide. N'oubliez pas que l'hôte regarde tous les bits d'hôte ensemble, et non les valeurs des octets.



Faire Labo 1

Convertissez des valeurs binaires en valeurs décimales, et inversement. Utilisez des puissances de 2 pour calculer le nombre d'hôtes disponibles avec x bits dans la partie hôte de l'adresse.

5.2 Types d'adresses IP

5.2.1 Classes d'adresses IP et masques de sous-réseau par défaut

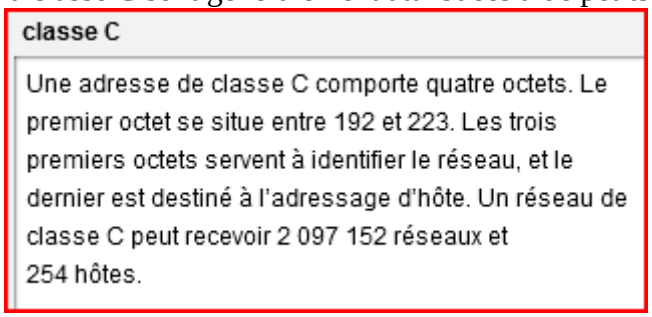
L'adresse IP et le masque de sous-réseau servent ensemble à déterminer quelle partie de l'adresse IP représente l'adresse réseau et quelle partie représente l'adresse d'hôte.

Les adresses IP se divisent en 5 classes. Les classes A, B et C correspondent à des adresses commerciales et sont attribuées à des hôtes. La classe D est réservée à la multidiffusion, et la classe E à un usage expérimental.

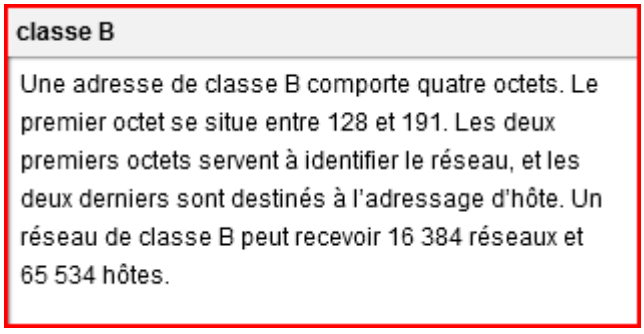
classe D
Une adresse de classe D comporte quatre octets. Le premier octet se situe entre 224 et 239. La classe D est utilisée pour la multidiffusion.

classe E
Une adresse de classe E comporte quatre octets. Le premier octet se situe entre 240 et 255. L'adressage IP de la classe E est réservé.

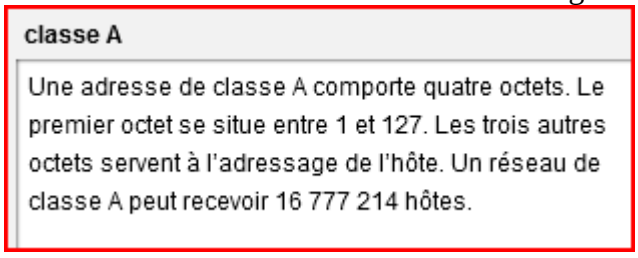
Les adresses de la classe C ont trois octets pour la partie réseau et un pour les hôtes. Le masque de sous-réseau par défaut a une longueur de 24 bits (255.255.255.0). Les adresses de la classe C sont généralement attribuées à de petits réseaux.



Les adresses de la classe B ont deux octets pour la partie réseau et deux pour les hôtes. Le masque de sous-réseau par défaut a une longueur de 16 bits (255.255.0.0). Ces adresses sont habituellement utilisées avec les réseaux de taille moyenne.



Les adresses de la classe A n'ont qu'un octet pour la partie réseau, mais elles en ont trois pour les hôtes. Le masque de sous-réseau par défaut a une longueur de 8 bits (255.0.0.0). Ces adresses sont habituellement attribuées à de grandes organisations.



La classe d'une adresse peut être déterminée par la valeur du premier octet. Par exemple, si la valeur du premier octet d'une adresse IP est comprise entre 192 et 223, l'adresse relève de la classe C. Ainsi, l'adresse 200.14.193.67 fait partie de la classe C.

Classes d'adresses IP

Classe de l'adresse	Plage du premier octet (décimal)	Bits du premier octet (les bits verts ne changent pas)	Parties réseau (R) et hôte (H) d'une adresse	Masque sous-réseau par défaut (décimal et binaire)	Nombres de réseaux et d'hôtes possibles par réseau
A	1 - 127	00000000 - 01111111	R.H.H.H	255.0.0.0 11111111 .00000000.00000000.00000000	126 réseaux (2^7-2) 16 777 214 hôtes par réseau (2^24-2)
B	128 - 191	10000000 - 10111111	R.R.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16 382 réseaux (2^14-2) 65 534 hôtes par réseau (2^16-2)
C	192 - 223	11000000 - 11011111	R.R.R.H	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150réseaux (2^21-2) 254 hôtes par réseau (2^8-2)
D	224 - 239	11100000 - 11101111	Non destiné à une utilisation commerciale comme hôte		
E	240 - 255	11110000 - 11111111	Non destiné à une utilisation commerciale comme hôte		

^^ Les adresses hôte ne comportant que des zéros (0) et que des uns (1) ne sont pas valides.

5.2.2 Adresses IP publiques et adresses IP privées

Tous les hôtes se connectant directement à Internet ont besoin d'une adresse IP publique unique.

adresse IP publique

Ensemble des adresses IP à l'exception des adresses IP privées réservées.

Il risque de ne pas y avoir suffisamment d'adresses IP, puisque le nombre d'adresses 32 bits disponibles n'est pas infini. Une solution à ce problème consiste à réserver certaines adresses privées à un usage exclusivement interne à une organisation. Cela permet aux hôtes se trouvant au sein d'une organisation de communiquer avec un autre hôte sans qu'une adresse IP publique unique soit nécessaire.

Le document RFC 1918 est une norme qui réserve plusieurs plages d'adresses dans chacune des classes A, B et C.

document RFC
Ensemble de documents utilisés comme principal moyen de communication d'informations sur Internet. Il s'agit principalement de spécifications de protocole comme Telnet et FTP, mais il peut également s'agir de documents humoristiques ou historiques. Les requêtes pour commentaires sont disponibles en ligne à partir de nombreuses sources.

Comme indiqué dans le tableau, ces plages d'adresses privées comprennent un seul réseau de classe A, 16 réseaux de classe B et 256 réseaux de classe C. Un administrateur réseau dispose ainsi d'une grande souplesse en ce qui concerne l'attribution d'adresses internes.

Un très grand réseau peut utiliser le réseau privé de classe A qui offre plus de 16 millions d'adresses privées.

Un réseau de taille moyenne peut utiliser un réseau privé de classe B qui fournit plus de 65 000 adresses.

Les réseaux domestiques et les réseaux des petites entreprises utilisent généralement une adresse privée unique de classe C qui autorise jusqu'à 254 hôtes.

Le réseau de classe A, les 16 réseaux de classe B ou les 256 réseaux de classe C peuvent être utilisés dans toute organisation, quelle que soit sa taille. Généralement, de nombreuses organisations utilisent le réseau privé de classe A.

Classe de l'adresse	Nombre de numéros de réseau réservés	Adresses réseau
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

Les adresses privées peuvent être utilisées par des hôtes au sein d'une organisation, en interne, tant que ces hôtes ne se connectent pas directement à Internet. Par conséquent, le même ensemble d'adresses privées peut être utilisé par plusieurs organisations. Les adresses privées ne sont pas routées sur Internet et sont rapidement bloquées par un routeur FAI.

L'utilisation d'adresses privées peut garantir une certaine sécurité, puisque ces adresses sont visibles uniquement sur le réseau local et que les tiers ne peuvent pas accéder directement aux adresses IP privées.

Certaines adresses privées peuvent également être utilisées pour tester et diagnostiquer des périphériques. Ce type d'adresse privée est appelé une adresse de bouclage. Le réseau 127.0.0.0 de classe A est réservé aux adresses de bouclage.

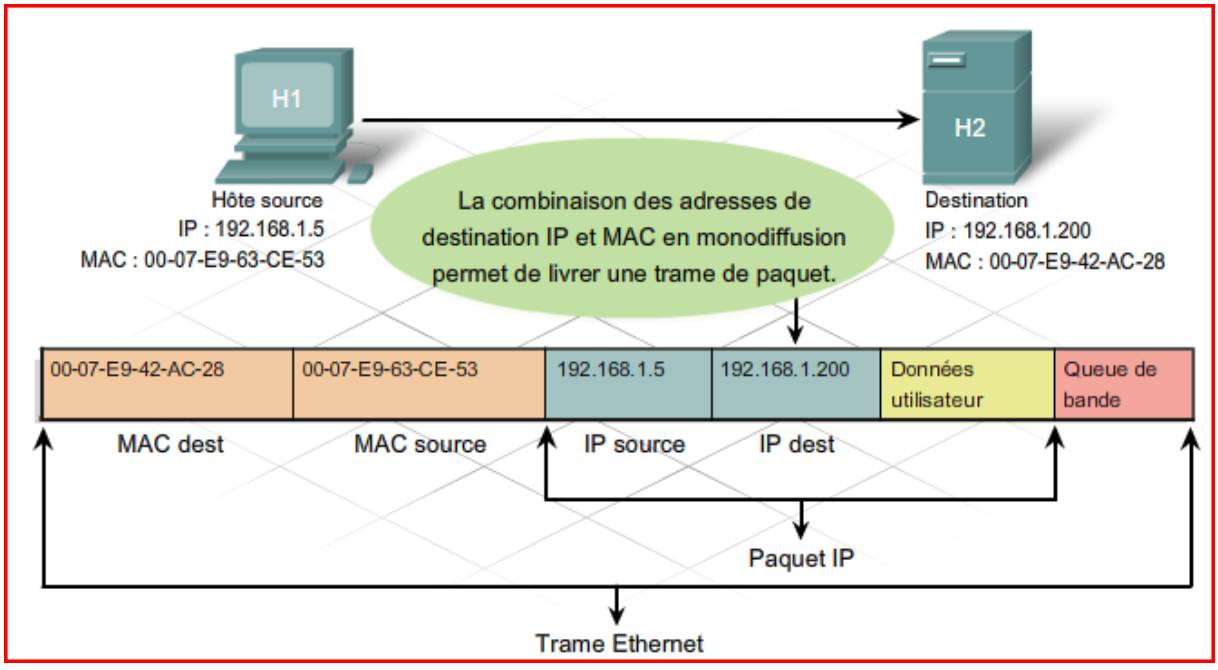
5.2.3 Adresses de monodiffusion, de diffusion et de multidiffusion

En plus des classes d'adresse, on distingue les adresses IP de monodiffusion, de diffusion et de multidiffusion. Les hôtes peuvent utiliser des adresses IP pour communiquer avec un seul destinataire (monodiffusion), plusieurs destinataires (multidiffusion) ou tous les destinataires (diffusion).

Monodiffusion

L'adresse de monodiffusion est la plus répandue sur un réseau IP. Un paquet ayant une adresse de destination monodiffusion est destiné à un hôte spécifique. Citons pour exemple un hôte ayant l'adresse IP 192.168.1.5 (source) demandant une page Web à partir d'un serveur à l'adresse IP 192.168.1.200 (destination).

Pour qu'un paquet monodiffusion soit envoyé et reçu, une adresse IP de destination doit figurer dans l'en-tête du paquet IP. Une adresse MAC de destination correspondante doit également être présente dans l'en-tête de la trame Ethernet. Les adresses IP et MAC se combinent pour transmettre les données à un hôte de destination spécifique.



Diffusion

Avec une diffusion, le paquet contient une adresse IP 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 qu'ARP et DHCP, utilisent les diffusions.

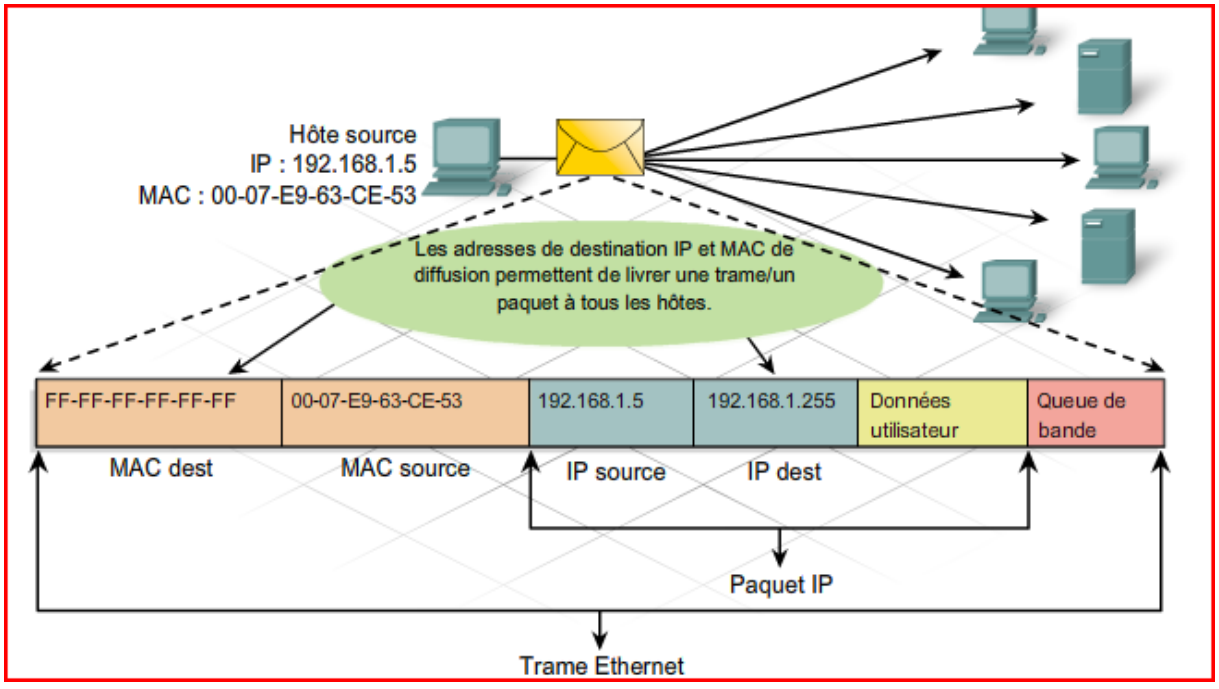
DHCP
Protocole de configuration hôte dynamique demandant et affectant une adresse IP, une passerelle par défaut et une adresse de serveur DNS à un hôte réseau.

Un réseau de classe C 192.168.1.0 ayant pour masque de sous-réseau par défaut 255.255.255.0 a pour adresse de diffusion 192.168.1.255. La partie hôte a la valeur décimale 255 ou la valeur binaire 11111111 (uniquement des 1).

Le réseau de classe B 172.16.0.0 ayant pour masque par défaut 255.255.0.0 a pour adresse de diffusion 172.16.255.255.

Le réseau de classe A 10.0.0.0 ayant pour masque par défaut 255.0.0.0 a pour adresse de diffusion 10.255.255.255.

Une adresse IP de diffusion pour un réseau a besoin d'une adresse MAC de diffusion correspondante dans la trame Ethernet. Sur les réseaux Ethernet, l'adresse MAC de diffusion contient 48 chiffres un affichés comme FF-FF-FF-FF-FF-FF hexadécimal.



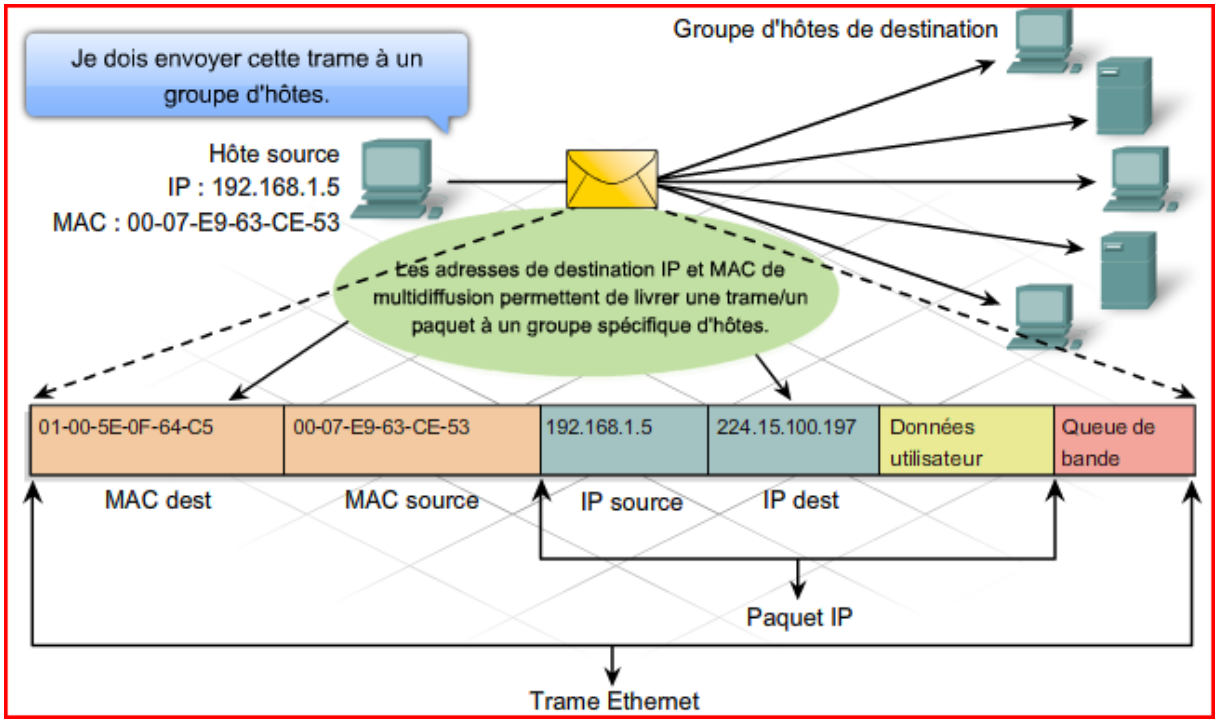
Multidiffusion

Les adresses de multidiffusion permettent à un périphérique source d'envoyer un paquet à un groupe de périphériques.

Une adresse IP de groupe de multidiffusion est attribuée aux périphériques appartenant à un groupe de multidiffusion. Les adresses de multidiffusion sont comprises entre 224.0.0.0 et 239.255.255.255. Les adresses de multidiffusion représentant un groupe d'adresses (parfois appelé groupe d'hôtes), elles ne peuvent être utilisées qu'en tant que destination d'un paquet. La source doit toujours avoir une adresse monodiffusion.

Les adresses de multidiffusion sont utilisées, par exemple, dans les jeux à distance, où plusieurs joueurs sont connectés à distance en jouant au même jeu. L'enseignement à distance par vidéoconférence, où plusieurs étudiants sont connectés au même cours, illustre également bien ce concept.

Comme avec une adresse de monodiffusion ou de diffusion, les adresses IP de multidiffusion nécessitent une adresse MAC de multidiffusion correspondante pour pouvoir transmettre des trames sur un réseau local. L'adresse MAC de multidiffusion est une valeur spéciale qui commence par 01-00-5E en hexadécimal. La valeur se termine par la conversion des 23 bits inférieurs de l'adresse IP de groupe de multidiffusion dans les 6 caractères hexadécimaux restants de l'adresse Ethernet. Comme indiqué dans le graphique, 01-00-5E-0F-64-C5 hexadécimal en est un exemple. Chaque caractère hexadécimal correspond à 4 bits binaires.



5.3 Comment obtenir des adresses IP ?

5.3.1 Attribution dynamique et attribution statique d'adresses

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

Statique

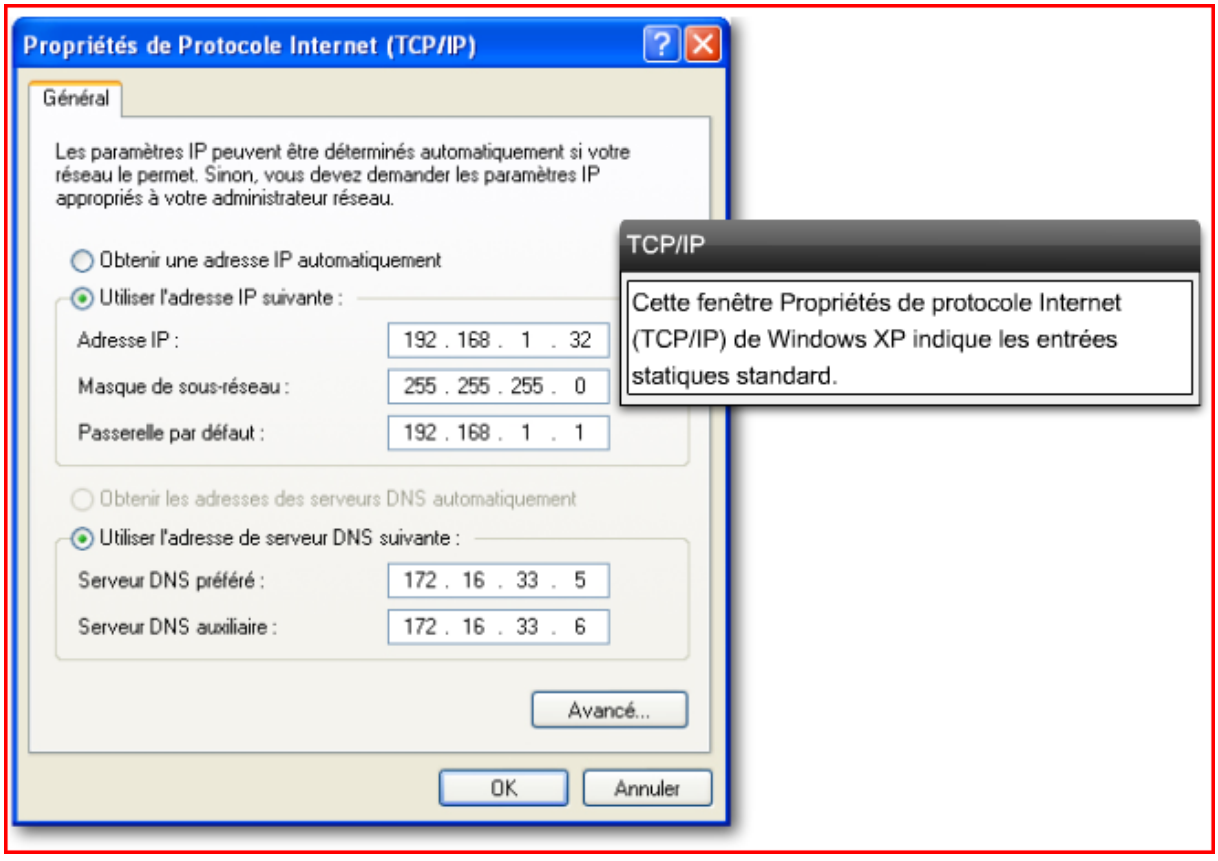
Avec une attribution statique, l'administrateur réseau doit configurer manuellement les informations réseau relatives à un hôte. Ces informations comprennent au moins l'adresse IP d'hôte, le masque de sous-réseau et la passerelle par défaut.

Les adresses statiques présentent des avantages. Par exemple, elles sont utiles pour les imprimantes, serveurs et autres périphériques réseau qui doivent être accessibles aux clients

sur le réseau. Si les hôtes accèdent normalement à un serveur avec une adresse IP particulière, cette adresse ne devrait pas être modifiée.

L'attribution statique d'informations d'adressage peut permettre de mieux contrôler les ressources réseau, mais la saisie d'informations pour chaque hôte peut prendre beaucoup de temps. Avec la saisie statique d'adresses IP, l'hôte effectue uniquement les vérifications d'erreurs de base sur l'adresse IP. Ainsi, le risque d'erreur est plus grand.

Lorsque vous utilisez l'adressage IP statique, il est important de tenir à jour une liste permettant de savoir précisément quelles adresses IP ont été attribuées à quels périphériques. En outre, ces adresses sont permanentes et ne sont normalement pas réutilisées.



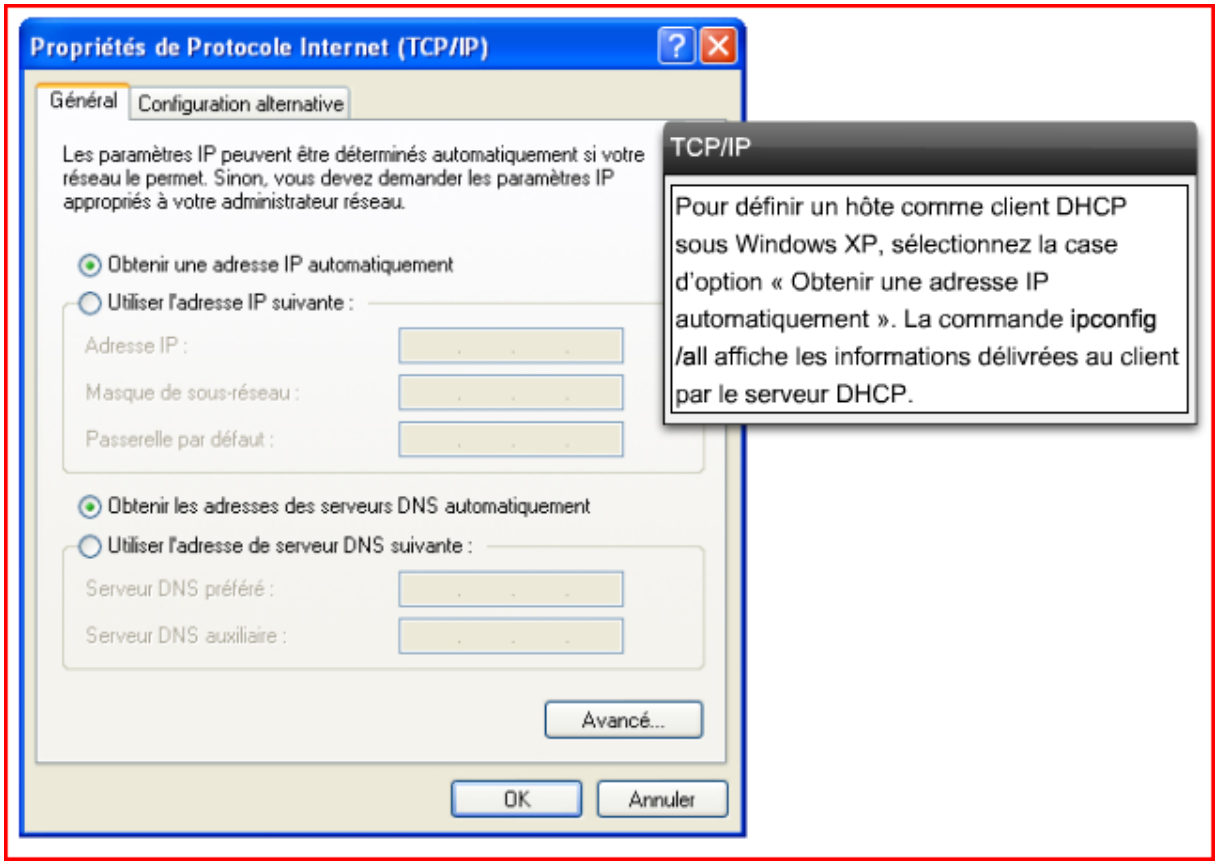
Dynamique

Sur les réseaux locaux, il n'est pas rare que les utilisateurs changent fréquemment. Les nouveaux utilisateurs arrivent avec des ordinateurs portables et ont besoin d'une connexion. D'autres ont de nouvelles stations de travail qui ont besoin d'être connectées. Plutôt que de demander à l'administrateur réseau d'attribuer des adresses IP à chaque station de travail, il est plus facile d'attribuer ces adresses automatiquement. Cette opération est réalisée à l'aide du protocole DHCP (Dynamic Host Configuration Protocol).

DHCP fournit un mécanisme qui permet d'attribuer automatiquement les informations d'adressage telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et d'autres informations relatives à la configuration.

DHCP est généralement la méthode préférée d'attribution d'adresses IP aux hôtes sur les grands réseaux, puisqu'elle réduit la charge de travail du personnel d'assistance réseau et élimine pratiquement toutes les erreurs de saisie.

Un autre avantage du protocole DHCP réside dans le fait qu'une adresse n'est pas attribuée à un hôte de manière permanente ; elle est seulement louée pour une période donnée. Si l'hôte est mis hors tension ou s'il est retiré du réseau, l'adresse est renvoyée au pool en vue d'une réutilisation. Cela est particulièrement utile avec les utilisateurs mobiles qui vont et viennent sur un réseau.



5.3.2 Serveurs DHCP

Si vous vous connectez à un point d'accès sans fil dans un aéroport ou un café-restaurant, DHCP vous permet d'accéder à Internet. Lorsque vous pénétrez dans la zone, le client DHCP de votre ordinateur portable contacte le serveur DHCP local via une connexion sans fil. Le serveur DHCP attribue une adresse IP à votre ordinateur.

serveur DHCP

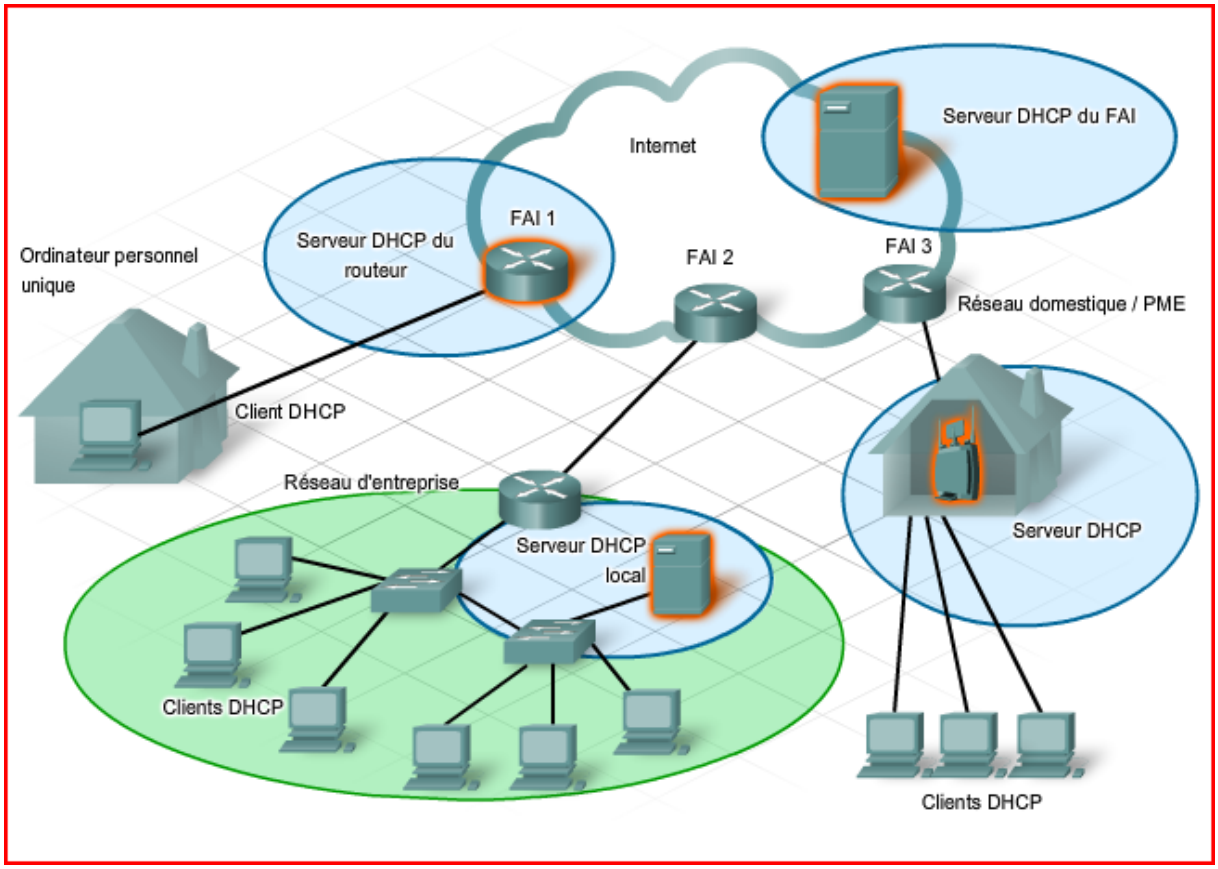
Le protocole DHCP (Dynamic Host Configuration Protocol) est un ensemble de règles qui affectent dynamiquement des adresses IP à des périphériques sur un réseau. Un serveur DHCP gère et affecte des adresses IP et garantit que toutes les adresses IP sont uniques.

Plusieurs types de périphériques peuvent servir de serveurs DHCP, tant qu'ils exécutent un logiciel de service DHCP. Sur la plupart des réseaux de taille moyenne à grande, le serveur DHCP est généralement un serveur PC local dédié.

Sur les réseaux domestiques, le serveur DHCP se trouve généralement chez le fournisseur de services Internet, qui envoie directement à un hôte sur le réseau domestique sa configuration IP.

Bon nombre de réseaux domestiques et de petites entreprises utilisent un routeur intégré pour se connecter au modem du fournisseur de services Internet. Dans ce cas, le routeur intégré est à la fois un client DHCP et un serveur. Le routeur intégré se comporte comme un client pour recevoir sa configuration IP du fournisseur de services Internet, puis comme un serveur DHCP avec les hôtes internes se trouvant sur le réseau local.

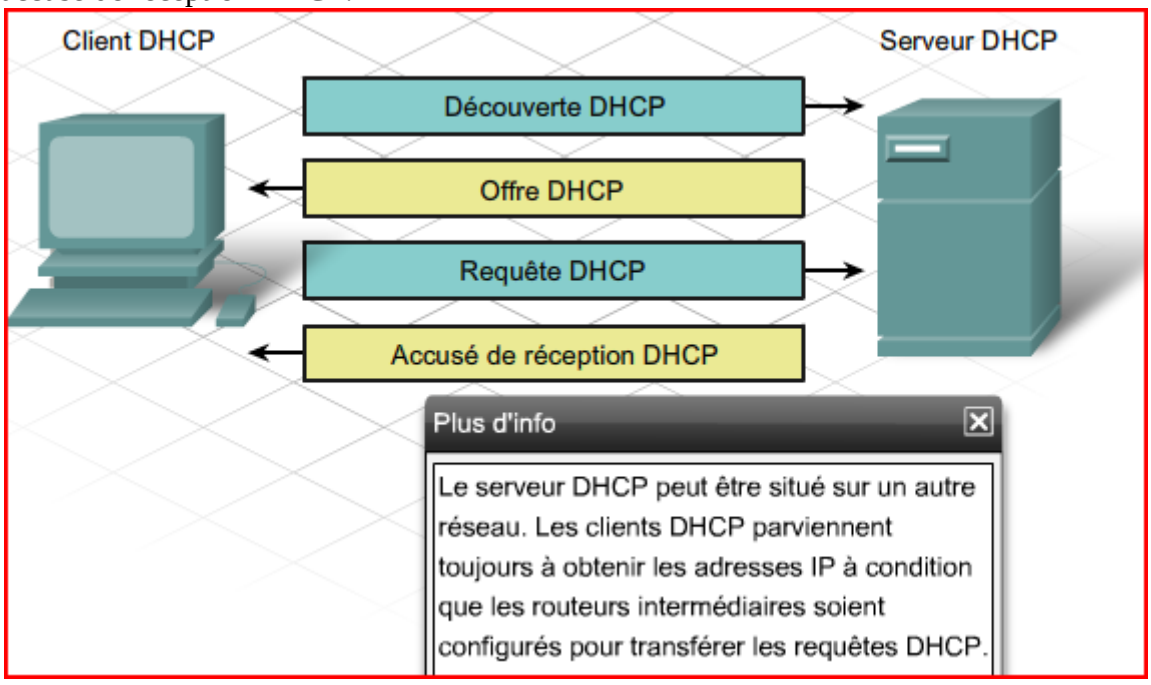
Outre les serveurs PC et les routeurs intégrés, d'autres types de périphériques réseau, tels que les routeurs dédiés, peuvent fournir des services DHCP aux clients, bien que cela ne soit pas très courant.



5.3.3 Configuration de DHCP

Lorsqu'un hôte est d'abord configuré comme client DHCP, il n'a pas d'adresse IP, de masque de sous-réseau ou de passerelle par défaut. Un serveur DHCP lui fournit ces informations, soit sur le réseau local, soit sur un réseau se trouvant chez le fournisseur de services Internet. Le serveur DHCP est configuré avec une plage ou un pool d'adresses IP pouvant être attribuées aux clients DHCP.

Un client ayant besoin d'une adresse IP envoie un message de détection DHCP, qui est une diffusion ayant l'adresse IP de destination 255.255.255.255 (32 chiffres un) et l'adresse MAC de destination FF-FF-FF-FF-FF-FF (48 chiffres un). Tous les hôtes sur le réseau reçoivent cette trame DHCP de diffusion, mais seul un serveur DHCP répond. Le serveur répond avec une offre DHCP en suggérant une adresse IP au client. L'hôte envoie ensuite une requête DHCP à ce serveur en demandant à utiliser l'adresse IP suggérée. Le serveur répond avec un accusé de réception DHCP.



Sur la plupart des réseaux domestiques et des réseaux de petites entreprises, un périphérique multifonction fournit les services DHCP aux clients du réseau local. Pour configurer un routeur sans fil Linksys, accédez à son interface graphique Web en ouvrant le navigateur et en saisissant, dans la zone Adresse, l'adresse IP par défaut du routeur : 192.168.1.1. Accédez à l'écran qui affiche la configuration DHCP.

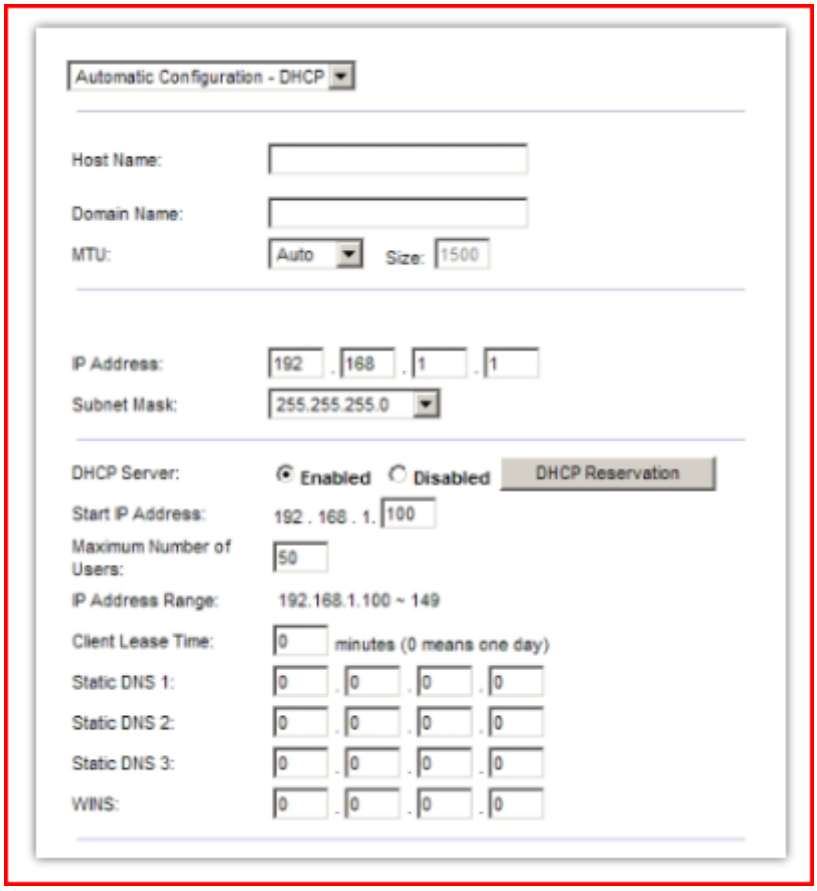
L'adresse IP 192.168.1.1 et le masque de sous-réseau 255.255.255.0 sont les adresses par défaut de l'interface du routeur interne. Ceci représente la passerelle par défaut pour tous les hôtes du réseau local, mais également l'adresse IP du serveur DHCP interne. Le serveur DHCP est activé par défaut sur la plupart des routeurs sans fil Linksys et autres routeurs intégrés domestiques.

Sur l'écran de configuration DHCP, vous pouvez vous servir de la plage DHCP par défaut ou indiquer une adresse de départ pour la plage DHCP (ne pas utiliser 192.168.1.1) ainsi que le nombre d'adresses à attribuer. La durée d'utilisation peut également être modifiée (par défaut, elle est de 24 heures). La fonction de configuration DHCP disponible sur la plupart des routeurs de services intégrés fournit des informations sur les hôtes connectés et les adresses IP, sur les adresses MAC qui leur sont associées et sur les durées d'utilisation.

plage DHCP

Gamme de protocole de configuration d'hôte dynamique. Liste contiguë d'adresses IP dans un pool DHCP.

Le tableau des clients DHCP affiche également le nom du client et indique s'il est connecté via le réseau local Ethernet ou si la connexion est sans fil (Interface).



Exercice Packet Tracer 2

Configurez un périphérique qui fera office de serveur DHCP, puis indiquez une plage d'adresses IP. Configurez un client DHCP, puis vérifiez les configurations DHCP.

5.4 Gestion des adresses

5.4.1 Frontières des réseaux et espace d'adressage

Le routeur fournit une passerelle grâce à laquelle les hôtes d'un réseau peuvent communiquer avec les hôtes se trouvant sur d'autres réseaux. Chaque interface d'un routeur est connectée à un réseau distinct.

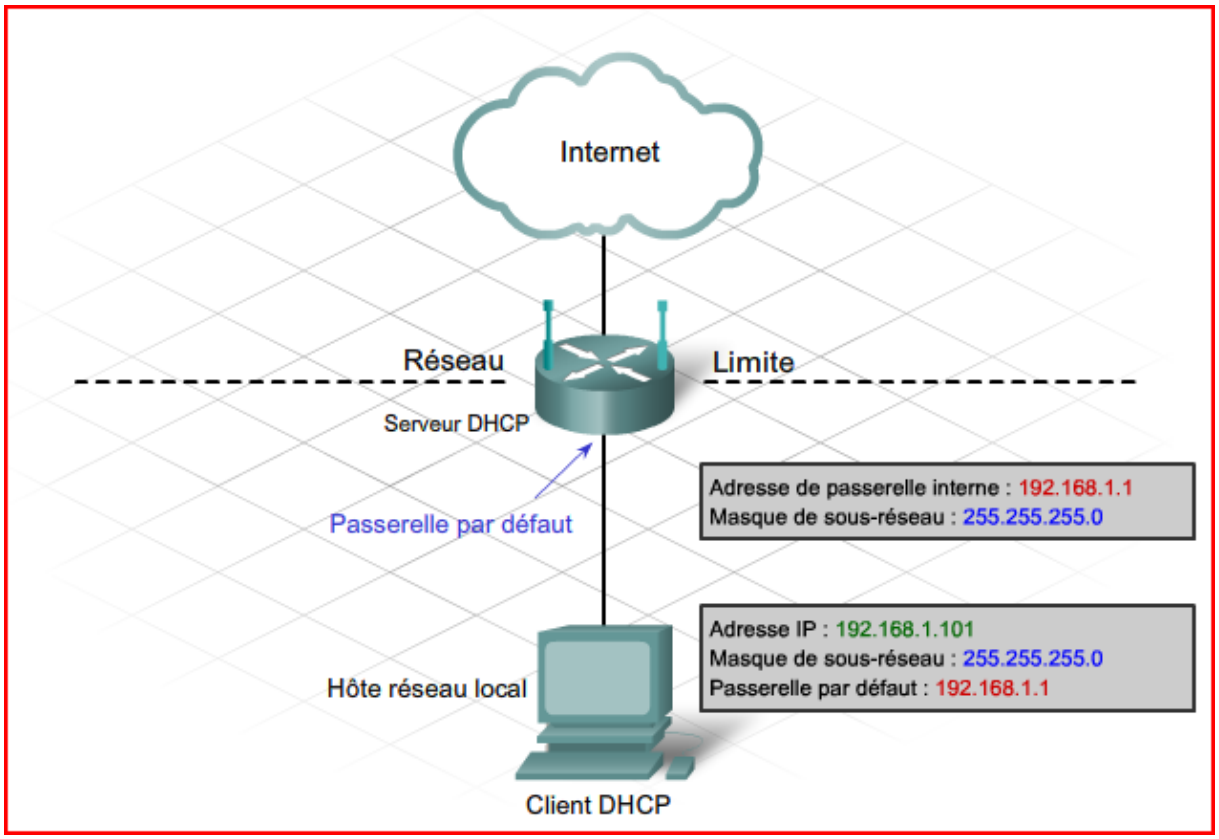
L'adresse IP attribuée à l'interface identifie le réseau local qui y est directement connecté.

Chaque hôte sur un réseau doit utiliser le routeur comme passerelle vers d'autres réseaux. Par conséquent, chaque hôte doit savoir quelle adresse IP de l'interface du routeur est connectée au réseau auquel l'hôte est relié. Cette adresse est l'adresse de la passerelle par défaut. Elle peut être configurée sur l'hôte de manière statique ou reçue de manière dynamique via DHCP.

Lorsqu'un routeur intégré est configuré comme serveur DHCP pour le réseau local, il envoie automatiquement aux hôtes la bonne adresse IP d'interface en tant qu'adresse de la passerelle par défaut. Ainsi, tous les hôtes du réseau peuvent utiliser cette adresse IP pour transférer des messages à des hôtes se trouvant chez le fournisseur de services Internet et accéder aux hôtes situés sur Internet. Les routeurs intégrés sont généralement configurés pour être des serveurs DHCP par défaut.

L'adresse IP de cette interface du routeur local devient l'adresse de la passerelle par défaut pour la configuration d'hôte. La passerelle par défaut est fournie soit de manière statique, soit via DHCP.

Lorsqu'un routeur intégré est configuré comme serveur DHCP, il fournit aux clients DHCP sa propre adresse IP interne en tant que passerelle par défaut. Il leur communique également leur adresse IP et leur masque de sous-réseau respectifs.



5.4.2 Attribution d'adresses

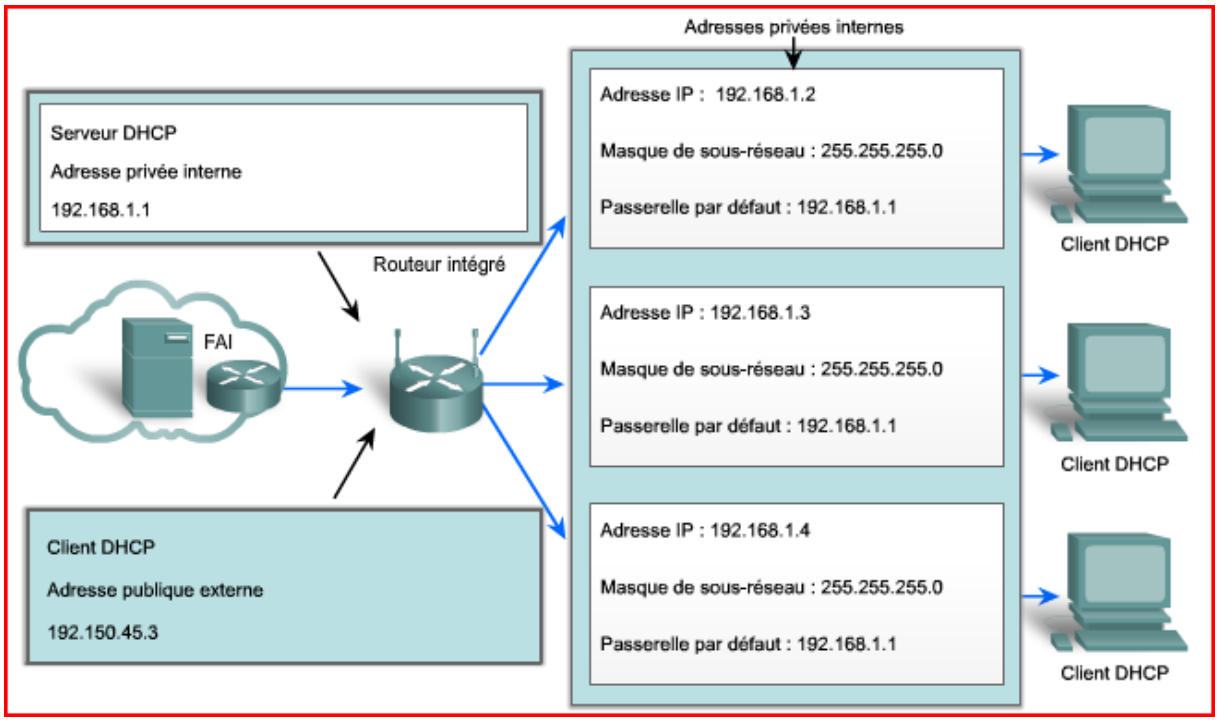
Le routeur intégré agit comme serveur DHCP avec tous les hôtes locaux qui sont connectés à lui, au moyen d'un câble Ethernet ou via une connexion sans fil. Ces hôtes locaux se trouvent sur un réseau interne. La plupart des serveurs DHCP sont configurés pour attribuer des adresses privées aux hôtes sur le réseau interne, plutôt que des adresses publiques routables sur Internet. Cela garantit ainsi que, par défaut, le réseau interne n'est pas directement accessible à partir d'Internet.

L'adresse IP par défaut configurée sur l'interface du routeur intégré local est généralement une adresse privée de classe C. Les adresses attribuées aux hôtes internes doivent se trouver dans le même réseau que le routeur intégré, avec une configuration statique ou via DHCP. Lorsqu'il est configuré comme serveur DHCP, le routeur intégré fournit des adresses dans cette plage. Il fournit également les informations relatives au masque de sous-réseau et sa propre adresse IP d'interface qui sert de passerelle par défaut.

De nombreux fournisseurs de services Internet utilisent également les serveurs DHCP pour fournir des adresses IP au côté Internet du routeur intégré installé sur les sites de leurs clients. Le réseau attribué au côté Internet du routeur intégré est appelé réseau externe.

Lorsqu'un routeur intégré est connecté au fournisseur de services Internet, il agit comme un client DHCP pour recevoir la bonne adresse IP du réseau externe pour l'interface Internet. Les fournisseurs de services Internet fournissent généralement une adresse routable sur Internet qui permet aux hôtes connectés au routeur intégré d'accéder à Internet.

Le routeur intégré sert de frontière entre le réseau interne local et Internet, à l'extérieur.



Les hôtes peuvent être connectés à un fournisseur de services Internet et à Internet de différentes manières. L'attribution ou non d'une adresse publique ou privée à un hôte individuel dépend de la manière dont celui-ci est connecté.

Connexion directe

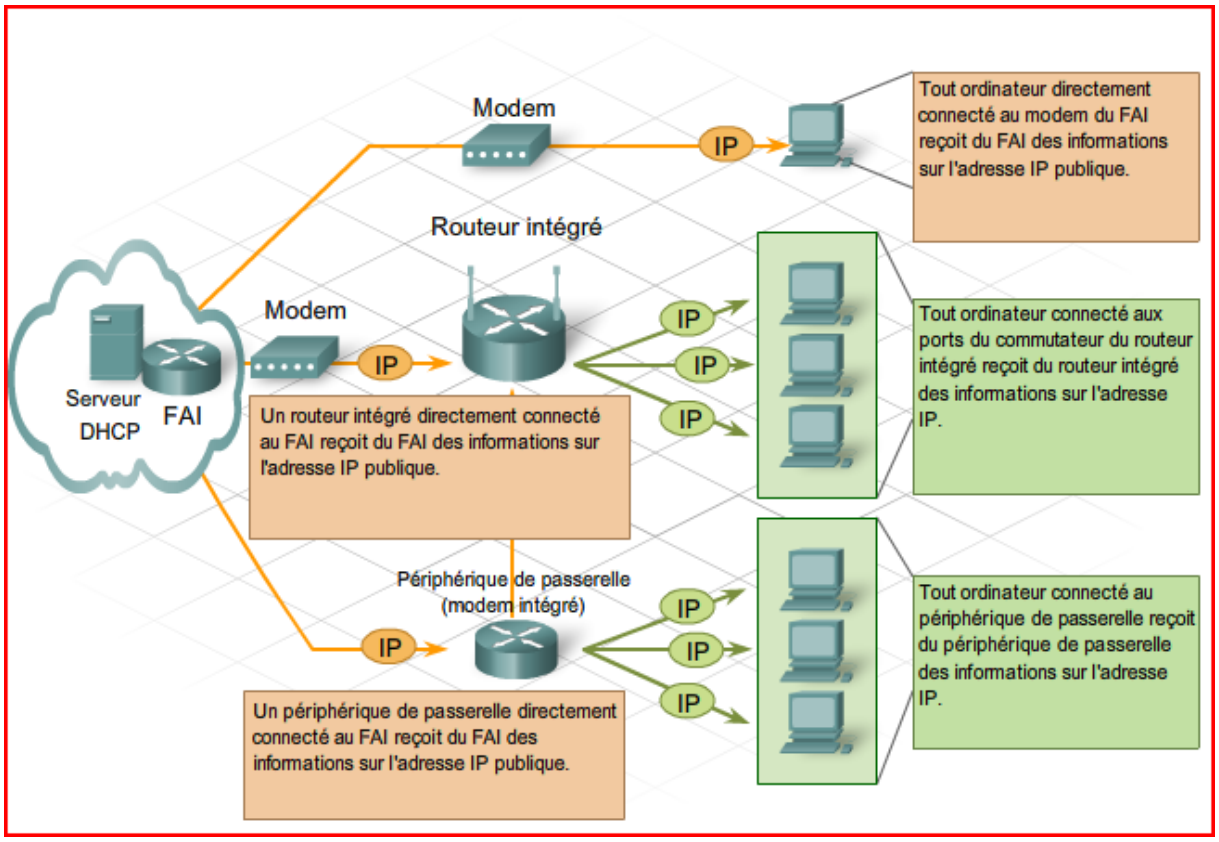
Certains clients ne disposent que d'un seul ordinateur ayant une connexion directe fournie par le fournisseur de services Internet via un modem. Dans ce cas, l'adresse publique fournie par le serveur DHCP du fournisseur de services Internet est attribuée à l'hôte unique.

Connexion avec un routeur intégré

Lorsque plusieurs hôtes ont besoin d'accéder à Internet, le modem du fournisseur de services Internet peut être directement relié à un routeur intégré, plutôt que d'être connecté directement à un ordinateur unique. Cela permet la création d'un réseau domestique ou de petite entreprise. Le routeur intégré reçoit l'adresse publique par le fournisseur de services Internet. Les hôtes internes reçoivent les adresses privées par le routeur intégré.

Connexion avec un périphérique de passerelle

Les périphériques de passerelle regroupent un routeur intégré et un modem, dans une unité, et se connectent directement au service du FAI. Comme avec les routeurs intégrés, le périphérique de passerelle reçoit une adresse publique par le FAI, et les PC internes reçoivent des adresses privées par le périphérique de passerelle.



5.4.3 Traduction d'adresses de réseau (NAT)

Le routeur intégré reçoit une adresse publique par le FAI qui l'autorise à envoyer et à recevoir des paquets sur Internet. Le routeur fournit alors des adresses privées aux clients du réseau local. Les adresses privées étant interdites sur Internet, il convient de recourir à un processus permettant de traduire les adresses privées en adresses publiques uniques, afin que les clients locaux puissent communiquer sur Internet.

Le processus utilisé pour convertir les adresses privées en adresses routables sur Internet est appelé la traduction d'adresses de réseau (NAT). La fonction NAT permet de convertir une adresse IP source (locale) privée en adresse (globale)publique. Le processus est inversé pour les paquets entrants. Grâce à la fonction NAT, le routeur intégré est capable de traduire plusieurs adresses IP internes dans la même adresse publique.

traduction d'adresses de réseau (NAT)
Procédure consistant à réécrire l'adresse source ou de destination des paquets IP lorsqu'ils transitent par un routeur ou un pare-feu. Plusieurs hôtes d'un réseau privé peuvent ainsi accéder à Internet en utilisant une seule adresse IP publique.

Seuls les paquets destinés à d'autres réseaux ont besoin d'être traduits. Ces paquets doivent traverser la passerelle, où le routeur intégré remplace l'adresse IP privée de l'hôte source par sa propre adresse IP publique.

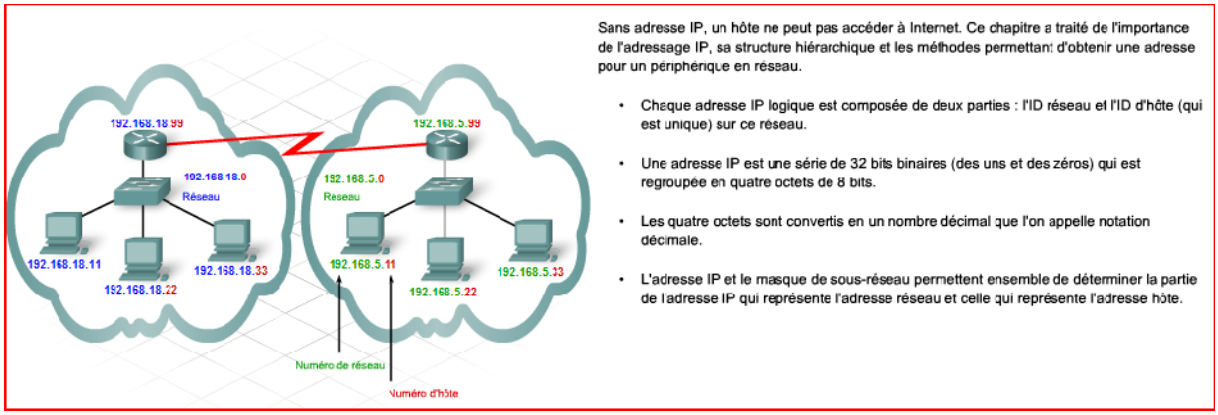
adresse IP privée
Adresse IP réservée pour usage dans un réseau interne et impossible à acheminer sur Internet. Les plages d'adresses IP sont comprises entre 10.0.0.0 et 10.255.255.255, entre 172.16.0.0 et 172.31.255.255, et entre 192.168.0.0 et 192.168.255.255.

Bien qu'une adresse IP privée unique soit attribuée à chaque hôte sur le réseau interne, les hôtes doivent partager l'unique adresse routable sur Internet attribuée au routeur intégré.

Exercice Packet Tracer 3

Configurez un périphérique multifonction en tant que serveur DHCP, puis configurez un client pour qu'il reçoive une configuration IP. Vérifiez la configuration des adresses publiques et privées.

5.5 Résumé du chapitre

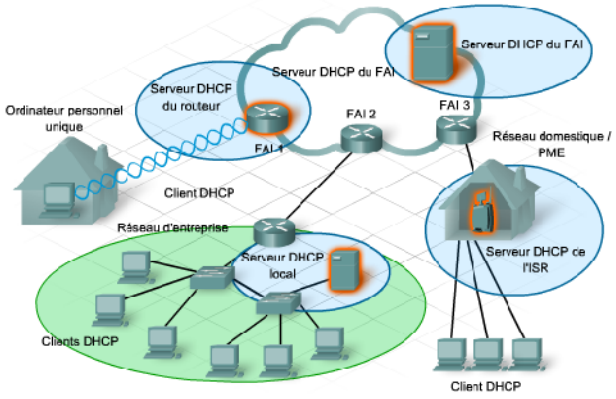


Les adresses IP sont classées de diverses façons.

- Les adresses IP sont regroupées en 5 classes. Les classes A, B et C sont commerciales. La classe D est destinée à la multidiffusion et la classe E est expérimentale.
- Chaque classe d'adresse IP dispose de son propre masque de sous-réseau par défaut.
- Les adresses IP sont également classées comme publiques ou privées. Les adresses publiques sont uniques et utilisées sur Internet.
- Les adresses privées peuvent être utilisées en interne par les hôtes d'une organisation. Les adresses privées peuvent être traduites en adresses Internet routables pour que les hôtes puissent communiquer sur Internet.
- Les hôtes peuvent utiliser les adresses IP pour communiquer en mode un-à-un (monodiffusion), un-à-plusieurs (multidiffusion) ou un-à-tous (diffusion).

Classes d'adresses IP

Classe de l'adresse	Plage du premier octet (décimal)	Bits du premier octet (les bits verts ne changent pas)	Parties réseau (R) et hôte (H) de l'adresse	Masque sous-réseau par défaut (décimal et binaire)	Nombres de réseaux et d'hôtes possibles par réseau
A	1 - 127	00000000 - 01111111	R.H.H.H	255.0.0.0 11111111.00000000.0000 0000.00000000	126 réseaux (2^7-2) 16 777 214 hôtes par réseau (2^24-2)
B	128 - 191	10000000 - 10111111	R.R.H.H	255.255.0.0 11111111.11111111.0000 0000.00000000	16 382 réseaux (2^14-2) 65 534 hôtes par réseau (2^16-2)
C	192 - 223	11000000 - 11011111	R.R.R.H	255.255.255.0 11111111.11111111.1111 1111.00000000	2 097 150 réseaux (2^21-2) 254 hôtes par réseau (2^8-2)
D	224 - 239	11100000 - 11101111	Non destiné à une utilisation commerciale comme hôte		
E	240 - 255	11110000 - 11111111	Non destiné à une utilisation commerciale comme hôte		

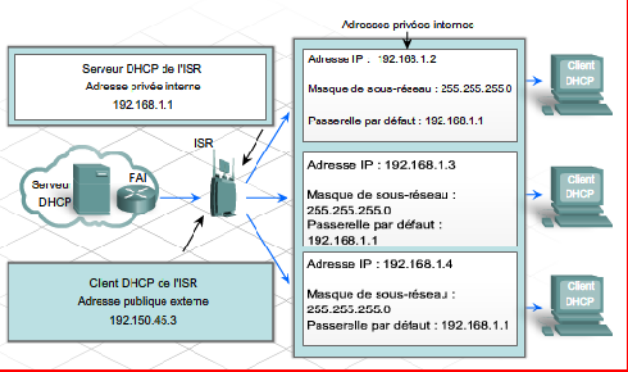


Les adresses IP peuvent être attribuées de façon statique ou dynamique.

- Si elle est attribuée de façon statique, l'adresse IP ainsi que le masque de sous-réseau et la passerelle par défaut doivent être configurés manuellement.
- Traditionnellement, les adresses statiques sont requises pour les serveurs dont l'accès se fait par Internet.
- DHCP constitue la méthode préférée d'attribution des adresses IP sur des réseaux de grande envergure car cela réduit la charge de travail des membres du support réseau.
- Le routeur de service intégré (ISR), ainsi que d'autres périphériques multifonctions, agit comme un client DHCP pour recevoir sa configuration IP unique du FAI, puis agit comme un serveur DHCP pour attribuer des adresses IP aux hôtes internes du réseau local.

Les adresses IP privées internes à une organisation doivent être traduites en adresse IP publique unique avant que le paquet n'arrive sur Internet.

- Les routeurs fournissent une frontière qui sépare les réseaux locaux d'Internet.
- La passerelle par défaut d'un hôte est l'interface de routeur connectée au réseau local qui est utilisée pour communiquer avec des destinations situées sur d'autres réseaux.
- De nombreux routeurs de passerelle traduisent des adresses IP privées de réseau local en adresses IP Internet routables à l'aide d'une fonction appelée NAT (Network Address Translation - Traduction d'adresses de réseau).
- Lorsque plusieurs adresses IP privées sont traduites en une seule adresse IP publique, le routeur mémorise toutes les adresses IP source et tous les numéros de port traduits, de sorte que le trafic de retour est correctement dirigé vers l'hôte.



5.6 Questionnaire du chapitre

Un technicien configure divers appareils. Quels sont les trois périphériques qui nécessitent une adresse IP ? (Choisissez trois réponses.)

- [ ] une imprimante avec une carte Ethernet
- [ ] une webcam reliée directement à un hôte
- [ ] un serveur avec deux cartes réseau
- [ ] un téléphone sur IP
- [ ] une station de travail autonome
- [ ] un assistant numérique personnel relié à une station de travail en réseau

Quels énoncés suivants sont vrais à propos des octets binaires ? (Choisissez trois réponses.)

- [ ] Si un bit est un zéro (0), sa valeur de colonne n'est pas comptée.
- [ ] La valeur de chaque bit d'un octet est le double de la valeur du bit à sa droite.
- [ ] Le bit le plus à droite d'un octet a une valeur de 0 lors de l'activation.
- [ ] Un hôte analyse chaque bit d'une adresse IP lors de sa réception par la carte réseau de l'hôte.
- [ ] Si tous les bits d'un octet sont définis sur un (1), la valeur de l'octet est de 256.
- [ ] Il existe 32 positions de valeur dans un octet.

Faites correspondre le numéro du premier octet à gauche avec la classe de l'adresse à droite. Notez que les premiers numéros d'octet indiqués à gauche ne sont pas tous à utiliser.

premier numéro d'octet de 0	Classe A
premier numéro d'octet de 126	Classe B
premier numéro d'octet de 130	Classe C
premier numéro d'octet de 200	
premier numéro d'octet de 224	
premier numéro d'octet de 240	

Quelle affirmation suivante à propos des adresses réseau privées est vraie ?

- Elles sont toujours acheminées sur Internet.
- Elles ne peuvent être utilisées que par une entreprise à la fois.
- Elles permettent aux utilisateurs externes d'accéder facilement aux serveurs Web internes.
- Elles sont plus sûres car elles ne sont visibles que sur le réseau local.

Combien de réseaux de classe C sont réservés à l'espace d'adresse privé ?

- 1
- 16
- 128
- 256

Quelle est l'adresse MAC de destination d'une trame Ethernet de diffusion ?

- 255.255.255.255
- 1.1.1.1
- AA-AA-AA-AA-AA-AA
- FF-FF-FF-FF-FF-FF

Faites glisser l'énoncé à gauche sur la catégorie correspondante à droite.

- utile pour les imprimantes et les serveurs
- offre un contrôle étendu des ressources réseau
- possibilité d'erreurs d'entrée
- utile pour les utilisateurs mobiles
- limité dans le temps
- adresses fournies par un serveur
- extrait automatiquement des adresses d'un pool
- les adresses ne sont pas réattribuées à un autre périphérique

Adressage IP statique

Adressage IP dynamique

Placez dans l'ordre ces messages DHCP pour qu'un hôte obtienne une adresse IP auprès d'un serveur DHCP.

Requête DHCP	
Découverte DHCP	
Offre DHCP	
Accusé de réception DHCP	

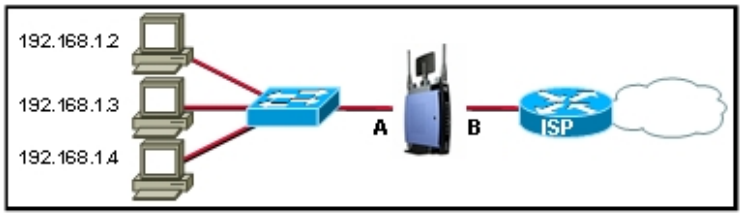
Un routeur de service intégré (ISR) dispose d'une adresse IP publique émise par le FAI. Quel est l'objectif de l'adresse IP publique ?

- permet aux hôtes internes de communiquer entre eux sur le réseau local
- permet aux hôtes internes de communiquer avec d'autres hôtes sur Internet
- permet à l'ISR de communiquer avec les hôtes locaux sur le réseau
- permet à l'ISR de communiquer avec les serveurs locaux sur le réseau

Qu'effectue la fonction NAT dans un routeur de service intégré (ISR) ?

- NAT traduit une adresse IP source en adresse de passerelle par défaut.
- NAT traduit une adresse IP locale en adresse IP source interne.
- NAT traduit une adresse IP globale interne en adresse IP source locale.
- NAT traduit une adresse IP source interne en adresse IP globale.

Observez le schéma. Quels sont les deux types d'adresses IP qui doivent être utilisés sur le routeur de service intégré (ISR) aux interfaces A et B ? (Choisissez deux réponses.)



- [ ] L'interface A doit utiliser une adresse IP privée.
- [ ] L'interface A doit utiliser une adresse IP publique.
- [ ] L'interface A doit utiliser une adresse IP source.
- [ ] L'interface B doit utiliser une adresse IP privée.
- [ ] L'interface B doit utiliser une adresse IP publique.
- [ ] L'interface B doit utiliser une adresse IP de destination.

Solution

1, 3 et 4

1, 2 et 4

premier numéro d'octet de 126

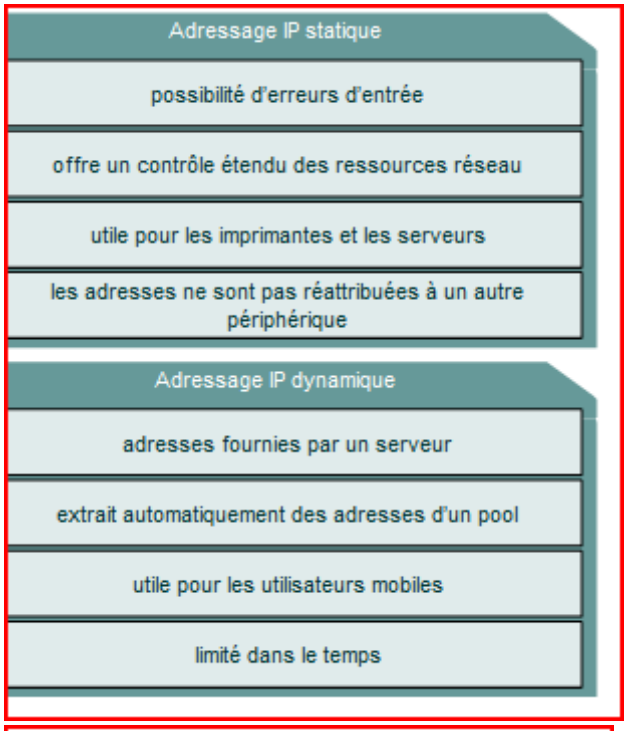
premier numéro d'octet de 130

premier numéro d'octet de 200

4

4

4



Découverte DHCP

Offre DHCP

Requête DHCP

Accusé de réception DHCP

2

4

1 et 5