Chapitre 2: Pile de protocoles TCP/IP et adressage IP

2.1 Présentation du protocole TCP/IP

2.1.1 Origine et évolution du protocole TCP/IP
2.1.2 La couche application
2.1.3 La couche transport
2.1.4 La couche Internet
2.1.5 La couche d'accès au réseau
2.1.6 Comparaison des modèles OSI et TCP/IP
2.1.7 L'architecture d'Internet

2.2 Les adresses Internet

2.2.1 L'adressage IP
2.2.2 Conversion binaire et décimale
2.2.3 Adressage IPv4
2.2.4 Adresses IP de classe A, B, C, D et E
2.2.5 Adresses IP réservées
2.2.6 Adresses IP publiques et privées
2.2.7 Introduction aux sous-réseaux
2.2.8 Comparaison entre IPv4 et IPv6

2.3 Obtention d'une adresse IP

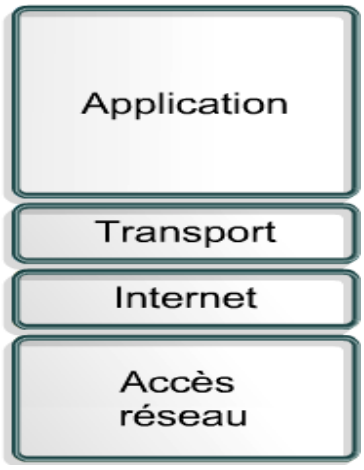
2.3.1 Obtention d'une adresse Internet
2.3.2 Attribution statique d'une adresse IP
2.3.3 Attribution d'une adresse IP à l'aide du protocole RARP
2.3.4 Attribution d'une adresse IP à l'aide du protocole BOOTP
2.3.5 Gestion des adresses IP à l'aide du protocole DHCP
2.3.6 Problèmes liés à la résolution d'adresses
2.3.7 Protocole ARP (Address Resolution Protocol)

Internet a été créé dans le but de fournir un réseau de communication capable de fonctionner en cas de guerre. Malgré la considérable évolution de son objectif premier, il repose toujours sur la pile de protocoles TCP/IP. Le protocole TCP/IP s'avère parfaitement adapté aux exigences de robustesse et de décentralisation liées à Internet. En outre, la plupart des protocoles standard s'appuient sur le modèle TCP/IP à quatre couches.
Il est conseillé de disposer de connaissances sur les modèles de réseau OSI et TCP/IP. Chacun des modèles fait appel à sa propre structure pour décrire le mécanisme d'un réseau. Néanmoins, ils se recoupent beaucoup. Les administrateurs système doivent connaître ces modèles afin de saisir le mécanisme d'un réseau.
Pour échanger des données sur Internet, un équipement doit obligatoirement disposer d'un identificateur unique. Cet identificateur correspond à l'adresse IP, car les routeurs utilisent le protocole de couche 3 appelé «protocole IP» pour déterminer le meilleur chemin pour cet équipement. IPv4 est la version du protocole IP actuellement utilisée sur Internet. Celle-ci a été élaborée avant la forte augmentation du besoin en adresses. Face à la croissance démesurée d'Internet, le nombre d'adresses IP disponibles a dangereusement diminué. Pour répondre à cette pénurie d'adresses, des solutions ont été proposées : les sous-réseaux, le système NAT (*Network Address Translation*) et les adresses privées. Le protocole IPv6 apporte des améliorations à la version IPv4 et fournit un espace d'adressage beaucoup plus important. Cette version IPv6 permet aux administrateurs d'intégrer les méthodes disponibles dans la version IPv4, ou de les supprimer.
Pour se connecter à Internet, un ordinateur doit comporter une adresse MAC physique et une adresse IP unique. L'adresse IP unique est également appelée « adresse logique ». Il existe plusieurs façons d'attribuer une adresse IP à un équipement. Certains équipements possèdent toujours la même adresse statique, tandis que d'autres se voient attribuer une adresse différente à chaque connexion au réseau. L'allocation dynamique d'adresses IP peut s'effectuer de plusieurs manières différentes.
Pour que des données soient correctement acheminées d'un équipement à un autre, les problèmes liés, par exemple, à l'utilisation d'adresses en double doivent être résolus.

2.1 Présentation du protocole TCP/IP

2.1.1 Origine et évolution du protocole TCP/IP

Le ministère américain de la Défense (*DoD*) a développé le modèle de référence TCP/IP, car il avait besoin d'un réseau pouvant résister à toutes les situations. Imaginez en effet un monde quadrillé de connexions de toutes sortes : fils, micro-ondes, fibres optiques et liaisons satellites. Imaginez maintenant que des données doivent être transmises quel que soit l'état d'un nœud ou d'un réseau spécifique. Le ministère américain de la Défense nécessitait une transmission réseau fiable, pour toute destination des données et en toute circonstance. La création du modèle TCP/IP a contribué à la réalisation de ce projet. Depuis lors, le modèle TCP/IP s'est imposé comme la norme Internet.



Examinez les couches du modèle TCP/IP par rapport à l'objectif initial d'Internet afin d'éclaircir la situation. Les quatre couches du modèle TCP/IP sont les suivantes: la couche application, la couche transport, la couche Internet et la couche d'accès au réseau. Certaines couches du modèle TCP/IP portent le même nom que celles du modèle OSI. Il est essentiel de ne pas confondre les fonctions des couches, car ces dernières jouent des rôles différents dans chaque modèle. La version actuelle du protocole TCP/IP a été normalisée en septembre 1981.

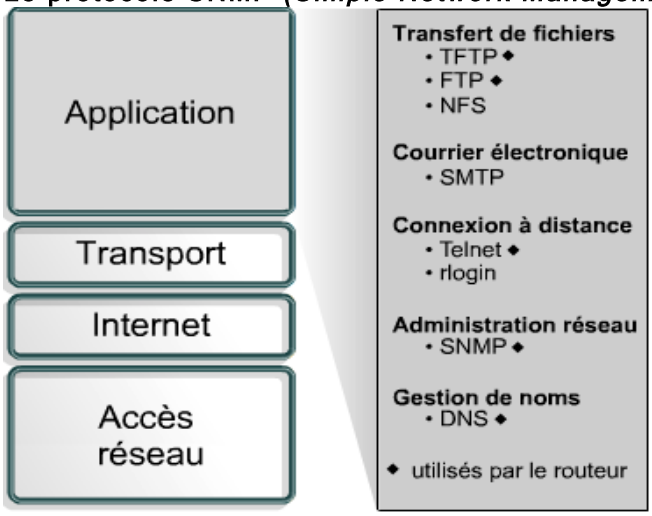
2.1.2 La couche application

La couche application gère les protocoles de niveau supérieur, les représentations, le code et le contrôle du dialogue. La pile de protocoles TCP/IP regroupe en une seule couche la totalité des aspects liés aux applications et vérifie que les données sont préparées de manière adéquate pour la couche suivante. Le protocole TCP/IP contient des spécifications relatives aux couches transport et Internet, notamment IP et TCP, et d'autres relatives

aux applications courantes. Outre la prise en charge du transfert de fichiers, du courrier électronique et de la connexion à distance, le modèle TCP/IP possède des protocoles prenant en charge les services suivants:

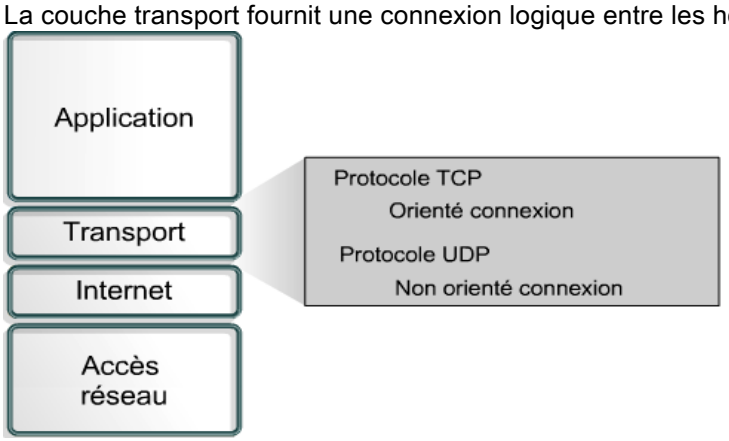
- **Le protocole FTP *(File Transfer Protocol)*:** ce protocole est un service fiable orienté connexion qui utilise le protocole TCP pour transférer des fichiers entre des systèmes qui le prennent en charge. Il gère les transferts bidirectionnels des fichiers binaires et ASCII.
- **Le protocole TFTP *(Trivial File Transfer Protocol)*:** ce protocole est un service non orienté connexion qui utilise le protocole de datagramme utilisateur UDP (*User Datagram Protocol*). Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP dans un environnement stable.
- **Le protocole NFS *(Network File System)*:** ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur, dans un réseau.
- **Le protocole SMTP *(Simple Mail Transfer Protocol)*:** ce protocole régit la transmission du courrier électronique sur les réseaux informatiques. Il ne permet pas de transmettre des données autres que du texte en clair.
- **Telnet:** ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes. Un client Telnet est qualifié d'hôte local. Un serveur Telnet est qualifié d'hôte distant.

Le protocole SNMP *(Simple Network Management Protocol)*: ce protocole permet de surveiller



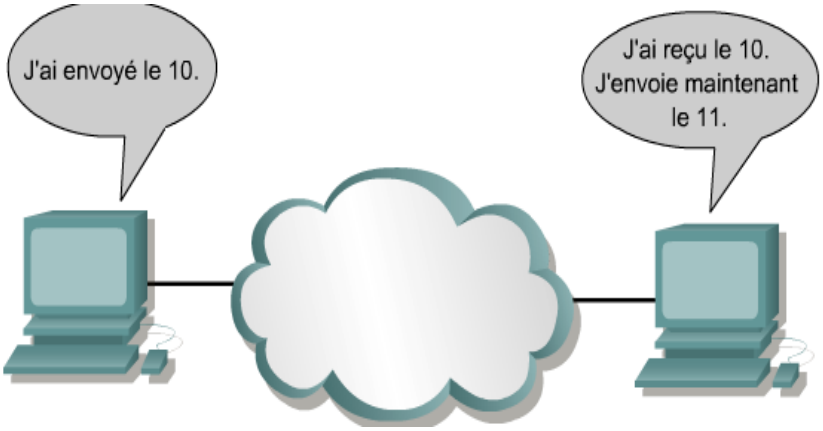
2.1.3 La couche transport

La couche transport fournit une connexion logique entre les hôtes source et de destination.

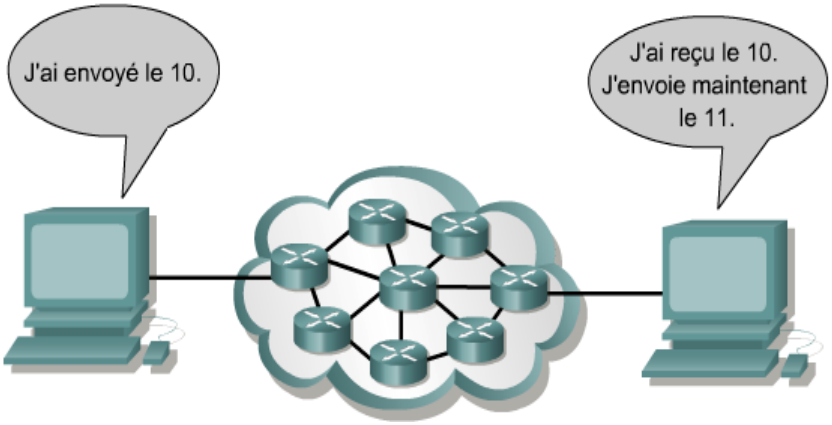


Les protocoles de transport segmentent et rassemblent les données envoyées par des applications de couche supérieure en un même flux de données, ou connexion logique, entre les deux points d'extrémité.

Internet est souvent représenté par un nuage. La couche transport envoie des paquets de données d'une source à une destination à travers ce nuage.



Le rôle principal de la couche transport est d'assurer une fiabilité et un contrôle de bout en bout lors du transfert des données à travers ce nuage. Les fenêtres glissantes, les numéros de séquençage et les accusés de réception permettent d'obtenir ce résultat. La couche transport définit également une connectivité de bout en bout entre les applications hôtes. Les protocoles de la couche transport incluent les protocoles TCP et UDP.



Le rôle des protocoles TCP et UDP est le suivant:

- Segmenter les données d'application de couche supérieure.
- Envoyer des segments d'un équipement à un autre.

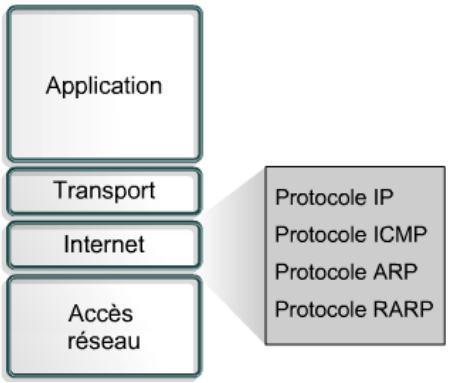
Le rôle du protocole TCP est le suivant:

- Etablir une connexion de bout en bout.
- Assurer le contrôle de flux à l'aide des fenêtres glissantes.

Assurer la fiabilité du réseau à l'aide des numéros de séquençage et des accusés de réception.

2.1.4 La couche Internet

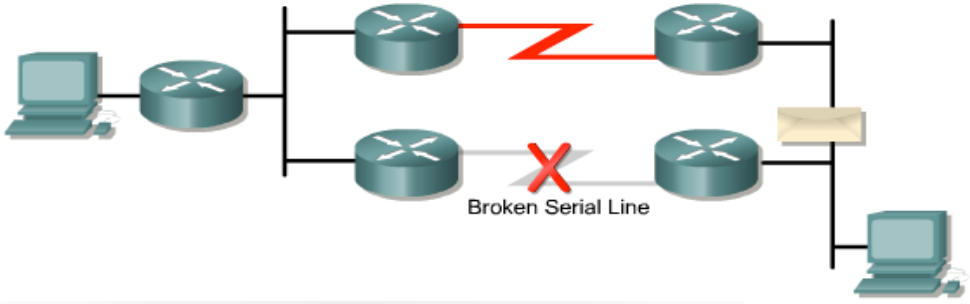
Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau. Le principal protocole de cette couche est le protocole IP. La détermination du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.



Les protocoles ci-dessous s'exécutent au niveau de la couche Internet du protocole TCP/IP:

- Le protocole IP assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion. Il ne se préoccupe pas du contenu des paquets, mais il recherche un chemin pour les acheminer à destination.
- Le protocole ICMP (*Internet Control Message Protocol*) offre des fonctions de messagerie et de contrôle.

- Le protocole ARP (*Address Resolution Protocol*) détermine les adresses de la couche liaison de données ou les adresses MAC pour les adresses IP connues.
- Le protocole RARP (*Reverse Address Resolution Protocol*) détermine l'adresse IP pour une adresse MAC connue.



Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau.

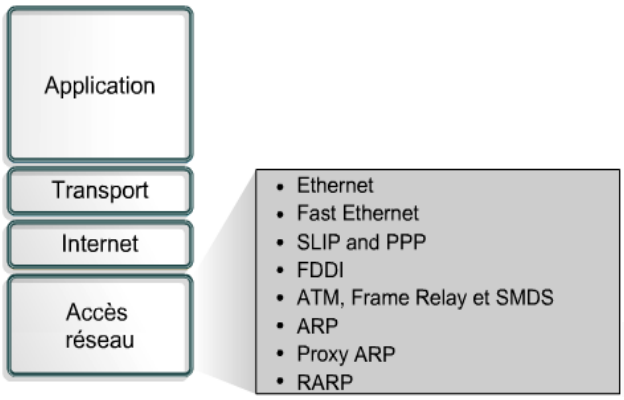
Le protocole IP effectue les opérations suivantes:

- Il définit un paquet et un système d'adressage.
- Il transfère des données entre la couche Internet et la couche d'accès au réseau.
- Il achemine des paquets à des hôtes distants.

Le protocole IP est parfois qualifié de protocole non fiable. Cela ne signifie pas qu'il n'envoie pas correctement les données sur le réseau, mais qu'il n'effectue aucune vérification d'erreurs et ne fournit aucun service de correction. Ces fonctions sont disponibles uniquement dans les protocoles de couche supérieure des couches application ou transport.

2.1.5 La couche d'accès au réseau

La couche d'accès au réseau permet à un paquet IP d'établir une liaison physique avec un média réseau. Cela comprend les détails sur les technologies LAN et WAN, ainsi que toutes les informations contenues dans les couches physique et liaison de données du modèle OSI.



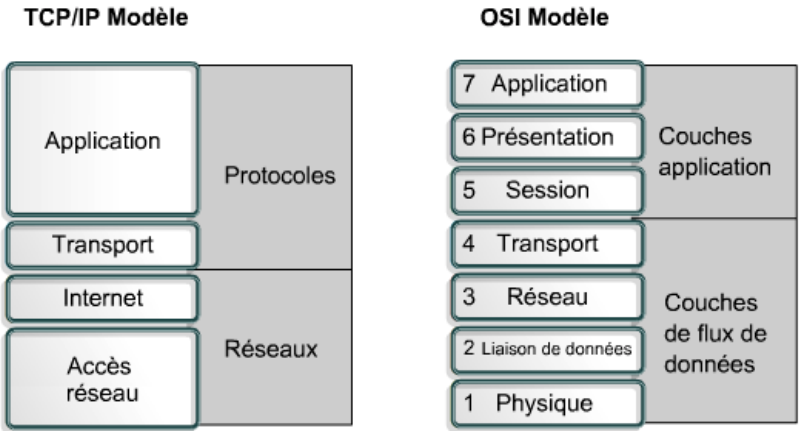
Les protocoles ARP et RARP se situent au niveau des couches d'accès réseau et Internet.

Les pilotes d'application, les cartes modem et les autres équipements s'exécutent au niveau de la couche d'accès au réseau. Cette dernière définit les procédures utilisées pour communiquer avec le matériel réseau et accéder au média de transmission. Les protocoles de modem, à savoir les protocoles SLIP (*Serial Line Internet Protocol*) et PPP (*Point-to-Point Protocol*) sont utilisés pour accéder au réseau par modem. Plusieurs protocoles sont nécessaires pour déterminer les caractéristiques matérielles, logicielles et de transmission au niveau de cette couche. Cela peut entraîner une certaine confusion dans l'esprit des utilisateurs. La plupart des protocoles facilement reconnaissables s'exécutent au niveau des couches Internet et transport du protocole TCP/IP.

En outre, les protocoles de la couche d'accès au réseau mappent les adresses IP avec les adresses matérielles physiques et encapsulent les paquets IP dans des trames. La couche d'accès au réseau définit la connexion au média physique en fonction de l'interface réseau et du type de matériel utilisés.

Voici un exemple de configuration de la couche d'accès au réseau faisant appel à une installation système Windows et à une carte réseau tierce. Certaines versions de Windows détectent automatiquement la carte réseau et installent ensuite les pilotes appropriés. Avec des versions plus anciennes de Windows, l'utilisateur doit indiquer le pilote de la carte réseau. Les fabricants de cartes réseau fournissent ces pilotes sur des disques ou des CD-ROM.

2.1.6 Comparaison des modèles OSI et TCP/IP



Les modèles OSI et TCP/IP présentent un grand nombre de similitudes:

- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services différents.
- Tous deux comportent des couches réseau et transport comparables.
- Tous deux s'appuient sur un réseau à commutation de paquets, et non sur un réseau à commutation de circuits.
- Les professionnels des réseaux doivent connaître les deux modèles.

Ils présentent également quelques différences:

- TCP/IP intègre les couches application, présentation et session du modèle OSI dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données du modèle OSI dans sa couche d'accès au réseau.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Lorsque la couche transport du protocole TCP/IP utilise le protocole UDP, la transmission des paquets n'est pas fiable tandis qu'elle est toujours fiable avec la couche transport du modèle OSI.

Les protocoles TCP/IP constituent la norme à partir de laquelle s'est développé Internet. Aussi, le modèle TCP/IP a-t-il bâti sa réputation sur ses protocoles. En règle générale, le modèle OSI ne permet pas de créer des réseaux. Il est utilisé pour aider les étudiants à comprendre le processus de communication.

2.1.7 L'architecture d'Internet

Internet permet d'envoyer des données de façon quasi instantanée à partir de n'importe quel point du globe, et ce à tout moment.

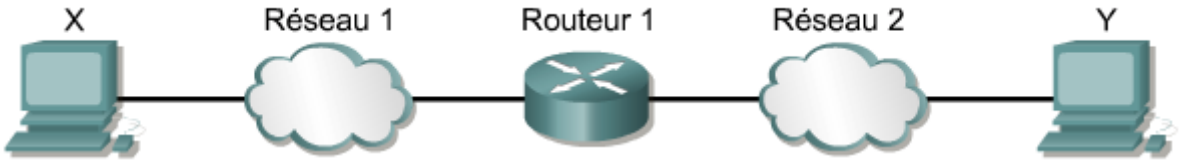
On appelle LAN les réseaux qui desservent une zone géographique limitée. Cependant, les LAN ne sont pas très évolutifs. Malgré les progrès techniques réalisés pour accélérer les communications, grâce notamment au réseau optique Metro et aux réseaux Gigabit et 10-Gigabit Ethernet, la distance reste un problème.

Afin d'obtenir une vue d'ensemble de l'architecture d'Internet, les étudiants analyseront les communications entre les ordinateurs source et de destination (ou les ordinateurs intermédiaires) au niveau de la couche application. Des instances identiques d'une application peuvent être installées sur tous les ordinateurs d'un réseau afin de faciliter l'acheminement des messages. Toutefois, ce système n'est pas très évolutif. Pour chaque nouveau logiciel, une nouvelle application doit alors être installée sur l'ensemble des ordinateurs du réseau et le logiciel doit être modifié afin d'éviter tout problème matériel. La défaillance d'un ordinateur intermédiaire ou d'une application installée sur un ordinateur pourrait interrompre la transmission des messages.

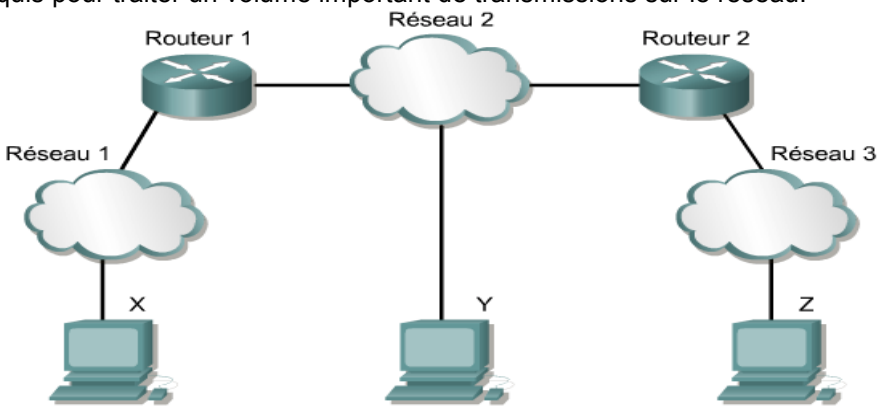
Internet fait appel au principe d'interconnexion de la couche réseau. L'objectif est de développer les fonctionnalités du réseau dans des modules séparés. Cela permet d'utiliser différentes technologies LAN pour les couches 1 et 2 du modèle OSI et différentes applications pour les couches 5, 6 et 7. Le modèle OSI offre un système dans lequel les caractéristiques des couches supérieures et inférieures sont indépendantes. Dès lors, les équipements de réseau intermédiaires auront la permission de relayer le trafic sans avoir de détails sur le LAN.

Ce qui nous amène au concept d'interréseaux, ou de réseaux composés de plusieurs réseaux. Un réseau qui comprend plusieurs réseaux s'appelle un interréseau. Le réseau sur lequel le Web (www) s'exécute s'appelle Internet. Les interréseaux doivent être modulables en fonction du nombre de réseaux et d'ordinateurs qui leur sont associés. En outre, les interréseaux doivent être capables de gérer l'acheminement des données sur de longues distances. Un interréseau doit être relativement flexible pour pouvoir assimiler les continuelles évolutions technologiques. Il doit être capable de s'adapter aux conditions dynamiques du réseau. Par ailleurs, les

interréseaux doivent se révéler économiques. Ils doivent être conçus de manière à autoriser tout utilisateur à envoyer des données vers n'importe quelle destination, et ce à tout moment.

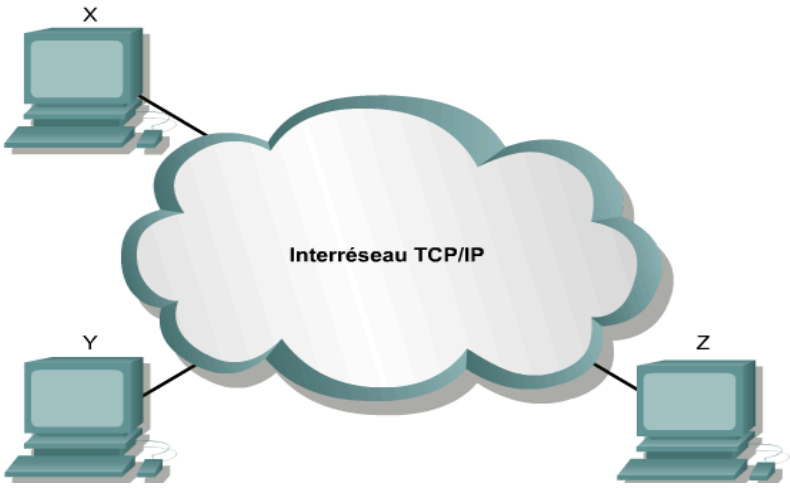


La figure présente brièvement la connexion d'un réseau physique à un autre par l'intermédiaire d'un ordinateur spécifique appelé «routeur». Ces réseaux sont directement connectés au routeur. Les routeurs servent à prendre les décisions d'acheminement nécessaires à la communication entre deux réseaux. Plusieurs routeurs sont requis pour traiter un volume important de transmissions sur le réseau.

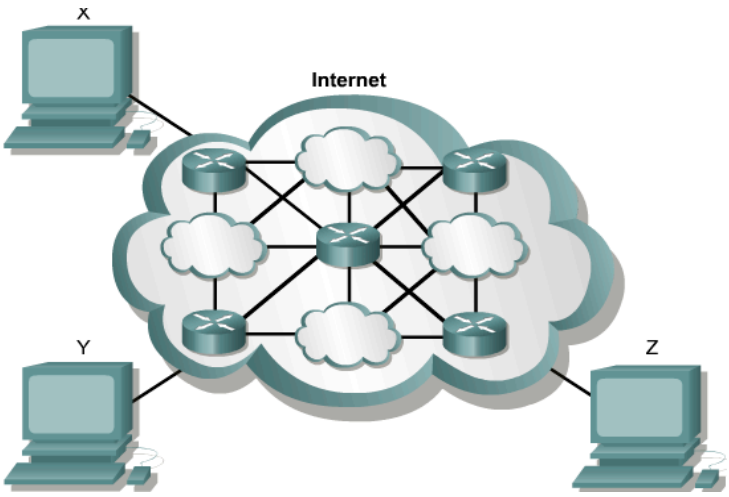


La figure illustre trois réseaux physiques connectés par l'intermédiaire de deux routeurs. Ceux-ci prennent des décisions complexes afin de permettre aux utilisateurs de tous les réseaux de communiquer avec chacun d'entre eux. Les réseaux ne sont pas tous directement connectés entre eux. Par conséquent, les routeurs doivent définir une méthode pour gérer cette situation.

L'une des solutions consiste pour le routeur à établir une liste répertoriant tous les ordinateurs et leur chemin d'accès. Le routeur sélectionne ensuite la méthode d'envoi des paquets de données en fonction de cette table de référence. Les paquets sont alors envoyés en fonction de l'adresse IP de l'ordinateur de destination. Néanmoins, plus le nombre d'utilisateurs connectés au réseau augmente, plus cette solution s'avère compliquée. La notion d'évolutivité apparaît lorsque le routeur détient une liste de tous les réseaux, mais qu'il laisse la responsabilité de l'acheminement local aux réseaux physiques locaux. Dans ce cas, les routeurs transmettent les messages à d'autres routeurs. Chaque routeur partage des informations relatives à son réseau connecté.



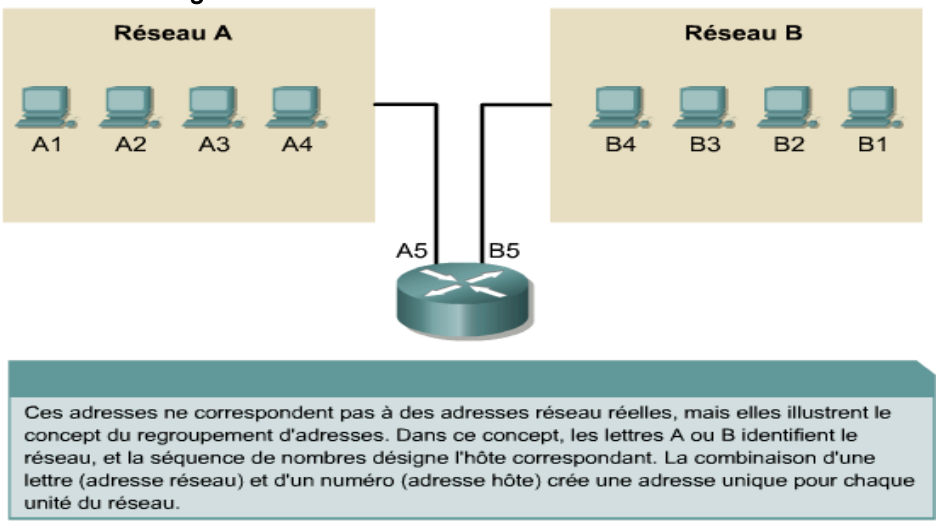
La figure présente la transparence du système requise par les utilisateurs. Néanmoins, les structures physiques et logiques qui composent le nuage Internet peuvent se révéler particulièrement complexes, comme l'illustre la figure . Internet a évolué rapidement, acceptant de plus en plus d'utilisateurs. Sa capacité d'évolution (plus de 90 000 routes principales et 300 000 000 utilisateurs finaux) traduit l'efficacité de son architecture.



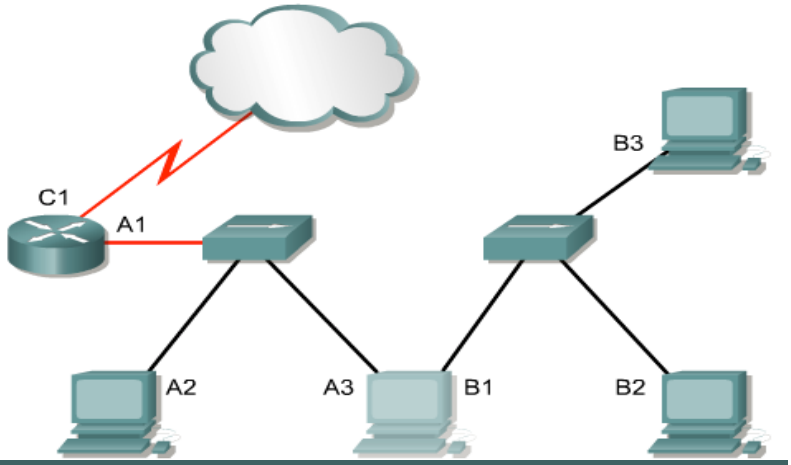
Deux ordinateurs placés à deux endroits différents de la planète peuvent communiquer de façon fiable si tant est qu'ils respectent certaines exigences en matière de protocole et de configuration matérielle et logicielle. Internet a été rendu possible grâce à la normalisation des techniques de transmission des données sur les réseaux

2.2 Les adresses Internet

2.2.1 L'adressage IP



Lorsque deux systèmes veulent échanger des données, chacun d'eux doit pouvoir identifier et localiser l'autre. Les adresses indiquées dans la figure ne correspondent pas à des adresses réseau réelles, mais elles illustrent le concept du regroupement d'adresses.



Fenêtre contextuelle (pop up)

Voici l'exemple d'un ordinateur connecté à deux réseaux différents. Pour cela, il dispose de deux cartes réseau. Il est alors désigné sous le nom d'unité à liaison double. Il est important de retenir que les deux interfaces de l'ordinateur se trouvant sur des réseaux totalement différents, elles disposent chacune d'un identificateur réseau distinct pour l'adresse. De plus, l'ordinateur ne transfère pas de données, à moins qu'il n'ait été configuré pour cette action, car il a simplement accès aux deux réseaux.

Un ordinateur peut être connecté à plusieurs réseaux. Si tel est le cas, le système doit recevoir plusieurs adresses. Chaque adresse identifie la connexion d'un ordinateur à un réseau différent. Chaque point de connexion, ou interface, d'un équipement dispose d'une adresse associée à un réseau. Cela permet à d'autres ordinateurs de localiser cet équipement sur un réseau spécifique. La combinaison d'une adresse réseau et d'une adresse hôte crée une adresse unique pour chaque équipement du réseau. Tout ordinateur appartenant à un réseau TCP/IP doit disposer d'un identificateur unique, ou adresse IP. Cette adresse, qui intervient au niveau de la couche 3, permet à un ordinateur de localiser un autre ordinateur sur le réseau. Tous les ordinateurs possèdent également une adresse physique unique, également appelée «adresse MAC». Celle-ci est attribuée par le fabricant de la carte réseau. Les adresses MAC opèrent au niveau de la couche 2 du modèle OSI.

Une adresse IP est une séquence de 32 bits composée de 1 et de 0. La figure donne un exemple de nombre 32 bits. Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous la forme de quatre nombres décimaux séparés par des points. Voici, par exemple, l'adresse IP d'un ordinateur : 192.168.1.2. Un autre ordinateur disposera de l'adresse : 128.10.2.1. Il s'agit de la notation entière avec des points de séparation. Chaque élément d'une adresse s'appelle un octet (toutes les adresses se composent de huit chiffres binaires). Par exemple, l'adresse IP 192.168.1.8 correspond à la valeur 11000000.10101000.00000001.00001000 en notation binaire. La notation entière avec des points de séparation est plus simple à comprendre que la méthode des 1 et des 0 binaires. En outre, elle permet d'éviter un grand nombre d'erreurs de transposition liées à l'utilisation des nombres binaires.

Binaire : 11000000.10101000.000000001.00001000 et 11000000.10101000.00000001.00001001

Décimale : 192.168.1.8 et 192.168.1.9

Les nombres binaires et décimaux représentent les mêmes valeurs, mais les valeurs décimales permettent une meilleure visibilité. Il s'agit d'un des problèmes les plus fréquemment rencontrés lorsque des nombres binaires sont directement utilisés. La longue chaîne de 1 et de 0 répétés est propice aux omissions et aux transpositions.

La figure représente la même valeur sous les formes binaire et décimale. On constate que cette valeur est plus facile à lire exprimée à l'aide de la notation entière avec des points de séparation. Il s'agit d'un des problèmes les

plus fréquemment rencontrés avec les nombres binaires. Les longues chaînes de 1 et de 0 répétés sont plus propices aux erreurs.
Au contraire, les adresses exprimées à l'aide de la notation entière avec des points de séparation, telles que 192.168.1.8 et 192.168.1.9, permettent de discerner plus facilement les relations entre les chiffres.

2.2.2 Conversion binaire et décimale

Il existe plusieurs façons de convertir les nombres décimaux en nombres binaires. Cette page décrit l'une de ces méthodes.
Certains étudiants considèreront peut-être que cette méthode n'est pas la plus simple ; tout est question de préférence personnelle.

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Lors de la conversion d'un nombre décimal en nombre binaire, vous devez rechercher la puissance de deux la plus proche possible du nombre décimal à convertir, sans dépasser celui-ci. Dans le cadre d'un processus informatisé, il est plus logique de commencer par les valeurs les plus élevées pouvant être contenues dans un ou deux octets. Comme nous l'avons vu précédemment, le regroupement standard est de huit bits, soit un octet. Cependant, il arrive que la valeur la plus élevée pouvant être contenue dans un octet ne soit pas suffisante par rapport aux valeurs requises. Pour pallier à ce problème, les octets sont regroupés. Au lieu d'avoir deux nombres de huit bits chacun, un seul nombre de 16 bits est créé. Au lieu d'avoir trois nombres de huit bits chacun, un seul nombre de 24 bits est créé. La même règle que celle des nombres de huit bits s'applique. Vous devez ensuite multiplier la valeur de la position précédente par deux pour obtenir la valeur de la colonne actuelle.

Puissance de la position	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
Valeur décimale	6783	6783	6783	6783	2687	639	639	127	127	63	31	15	7	3	1
Valeur de la position	32768	16384	8192	4096	2048	1024	512	256	128	32	16	8	4	2	1
Compte binaire	0	0	0	1	1	0	1	0	0	1	1	1	1	1	1
Reste	6783	6783	6783	2687	639	639	127	127	127	31	15	7	3	1	0

Conversion du nombre décimal 6783 en nombre binaire 000110100

Dans la mesure où le traitement informatique est souvent référencé par des octets, il est plus facile de commencer par définir des plages d'octets et d'effectuer le calcul à partir de ces valeurs. Entraînez-vous à l'aide, par exemple, de la valeur 6 783. Ce nombre étant supérieur à 255 (valeur maximale pour un seul octet), deux octets sont utilisés. Commencez le calcul à 2^{15}. L'équivalent binaire de la valeur 6 783 est 00011010 01111111.
Le second exemple utilise la valeur 104. Ce nombre étant inférieur à 255, il peut être représenté par un seul octet. L'équivalent binaire de la valeur 104 est 01101000.

Puissance de la position	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
Valeur décimale	104	104	40	8	8	0	0	0
Valeur de la position	128	64	32	16	8	4	2	1
Compte binaire	0	1	1	0	1	0	0	0
Reste	104	40	8	8	0	0	0	0

Conversion du nombre décimal 104 en nombre binaire 01101000.

Cette méthode est valable pour tous les nombres décimaux. Prenons l'exemple du nombre décimal un million. Sachant qu'un million est supérieur à la valeur maximale pouvant être contenue dans deux octets (soit 65 535), au moins trois octets sont nécessaires. En procédant à des multiplications par deux jusqu'à ce que vous atteigniez 24 bits (soit trois octets), vous obtenez la valeur 8 388 608. Autrement dit, la valeur la plus élevée pouvant être contenue dans 24 bits est 16 777 215. Ainsi, en prenant la valeur 24 bits comme point de départ,

suivez ce processus jusqu'à atteindre la valeur zéro. En effectuant la procédure décrite, un million (valeur décimale) correspond à 00001111 01000010 01000000 (valeur binaire).
La figure comprend des exercices de conversion de nombres décimaux en nombres binaires.
Pour convertir un nombre binaire en nombre décimal, il suffit d'effectuer l'opération en sens inverse. Placez la valeur binaire dans le tableau. Si un 1 est situé dans une position de colonne, ajoutez cette valeur au total.

Puissance de la position	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
Valeur décimale	0	0	0	0	0	0	1024	1024	1024	1024	1024	1024	1040	1040	1052	1052
Valeur de la position	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1
Compte binaire	0	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1
Reste	0	0	0	0	0	1024	1024	1024	1024	1024	1024	1040	1048	1052	1052	1053

Convertissez le nombre 00000100 00011101 en représentation décimale. La bonne réponse est: 1 053.

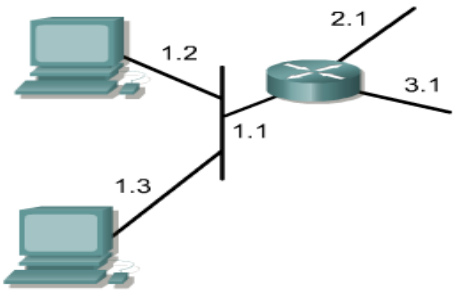
Nombre binaire	Nombre décimal
11101110	
Essayez un autre nombre.	Vérifiez votre réponse.

La figure comprend des exercices de conversion de nombres binaires en nombres décimaux.

2.2.3 Adressage IPv4

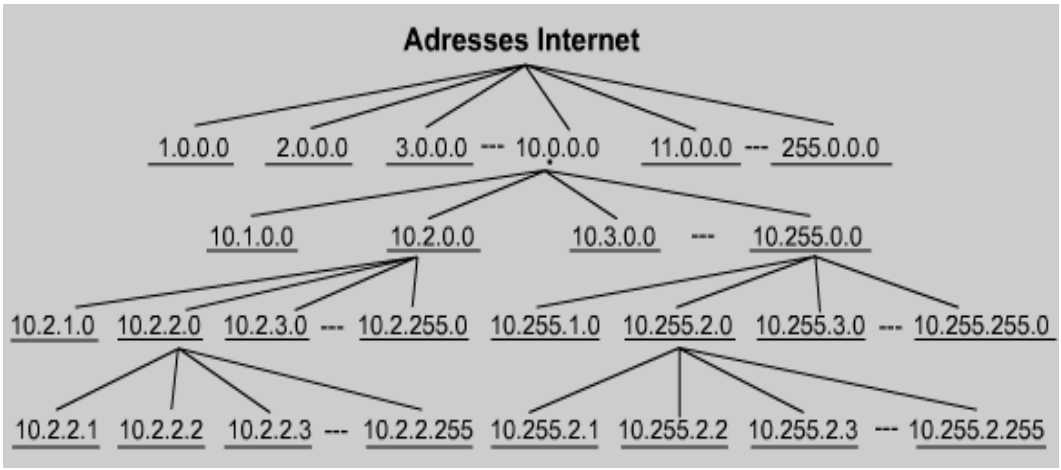
Cette page traite de l'adressage IPv4.

Un routeur fait appel à une adresse IP pour transmettre des paquets du réseau d'origine vers le réseau de destination. Les paquets doivent comporter un identificateur pour les réseaux source et de destination. Un routeur utilise l'adresse IP du réseau de destination afin de remettre le paquet au réseau approprié. Lorsque le paquet atteint un routeur connecté au réseau de destination, ce routeur localise l'ordinateur sur le réseau à l'aide de l'adresse IP. Ce système fonctionne pratiquement de la même manière que le système postal national. Une fois le courrier envoyé, le code postal est utilisé pour remettre le courrier au bureau de poste de la ville de destination. Le bureau de poste utilise ensuite la rue pour localiser la destination finale au niveau de la ville.



Réseau	Hôte
1	1 2 3
2	1
3	1

Chaque adresse IP comporte également deux parties. La première partie identifie le réseau auquel le système est connecté et la seconde partie identifie le système. Comme l'illustre la figure, chaque octet représente une valeur comprise entre 0 et 255. Chacun des octets est subdivisé en 256 groupes, qui se divisent à leur tour en 256 sous-groupes avec 256 adresses chacun. Lorsque vous faites référence à l'adresse d'un groupe directement au-dessus d'un autre groupe de la hiérarchie, tous les groupes qui en dérivent peuvent être référencés en tant qu'une seule et même unité.



On parle dans ce cas de système d'adressage hiérarchique, car il contient plusieurs niveaux. Chaque adresse IP regroupe ces deux identificateurs en un seul nombre. Ce nombre doit être unique, faute de quoi l'acheminement échoue. La première partie identifie l'adresse réseau du système. La seconde, appelée «partie hôte», identifie la machine sur le réseau.

Les adresses IP sont réparties en classes afin de définir des réseaux de grande taille, de taille moyenne et de petite taille. Les adresses IP de classe A sont affectées aux réseaux de grande taille. Les adresses de classe B sont utilisées pour les réseaux de taille moyenne et les adresses IP de classe C pour les réseaux de petite taille. Pour déterminer la partie de l'adresse qui correspond au réseau et celle qui correspond à l'hôte, vous devez d'abord identifier la classe de l'adresse IP.

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

* La plage d'adresses 127.x.x.x est réservée en tant qu'adresse en mode bouclé, utilisée pour les tests et les diagnostics.

Les étudiants peuvent utiliser l'activité de média interactive pour mieux appréhender les différentes classes d'adresses.

Classe d'adresses IP	Bits de valeur supérieure	Plage d'adresses du premier octet	Nombre de bits de l'adresse réseau
Classe A	0	0 - 127 *	8
Classe B	10	128 - 191	16
Classe C	110	192 - 223	24
Classe D	1110	224 - 239	28

* La plage d'adresses 127.x.x.x est réservée en tant qu'adresse en mode bouclé, utilisée pour les tests et les diagnostics.

La page suivante fournit des informations supplémentaires sur les adresses IP de classe A, B, C, D et E.

2.2.4 Adresses IP de classe A, B, C, D et E

Classe A	Réseau	Hôte		
Octet	1	2	3	4

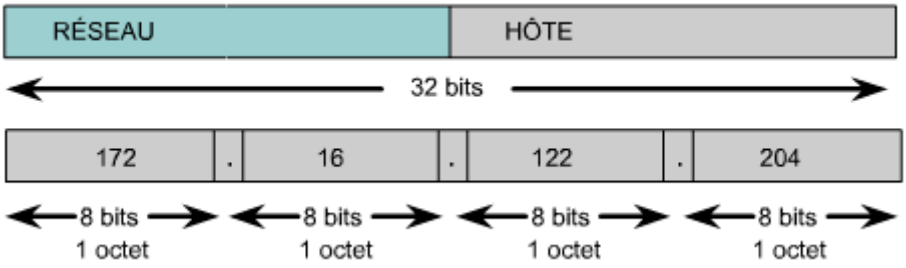
Classe B :	Réseau		Hôte	
Octet	1	2	3	4

Classe C	Réseau			Hôte
Octet	1	2	3	4

Classe D	Hôte			
Octet	1	2	3	4

Les adresses de classe D sont utilisées pour les groupes de multicast. Il n'est pas nécessaire d'allouer des octets ou des bits pour séparer les adresses réseau et hôte. Les adresses de classe E sont réservées à la recherche.

Les adresses IP sont regroupées en classes afin de permettre l'adaptation à des réseaux de différentes tailles et de faciliter leur classification. Cette opération est connue sous le nom d'adressage par classes. Chaque adresse IP complète de 32 bits est fractionnée en une partie réseau et une partie hôte.



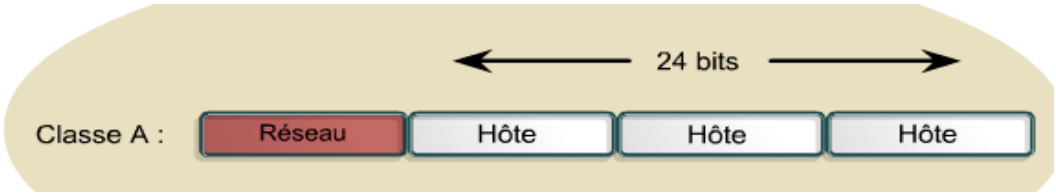
Une adresse IP comporte toujours une partie réseau et une partie hôte. Dans un modèle d'adressage par classe, cette distinction est effectuée au niveau des frontières entre les octets.

Un bit, ou une séquence de bits, situé en début d'adresse détermine la classe de l'adresse. Il existe cinq classes d'adresses IP, comme l'illustre la figure

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

Déterminez la classe d'après le premier octet.
* 127 (011111111) est une adresse de classe A réservée aux tests en mode bouclé et elle ne peut pas être attribuée à un réseau.

L'adresse de classe A est réservée aux réseaux de très grande taille, avec plus de 16 millions d'adresses hôte disponibles. Les adresses IP de classe A utilisent uniquement le premier octet pour indiquer l'adresse réseau. Les trois octets suivants sont utilisés pour définir les adresses hôte.



Le premier bit d'une adresse de classe A est toujours 0. Par conséquent, le nombre le plus faible pouvant être représenté est 00000000 (0 en décimal) et le plus élevé est 01111111 (127 en décimal). Les valeurs 0 et 127 sont réservées et ne peuvent pas être utilisées comme adresses réseau. Toute adresse commençant par une valeur comprise entre 1 et 126 dans le premier octet est une adresse de classe A.

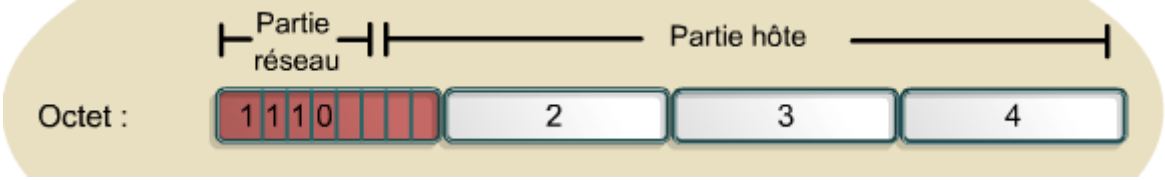
Le réseau 127.0.0.0 est réservé pour les tests en bouclage. Les routeurs ou les ordinateurs locaux peuvent utiliser cette adresse pour s'envoyer des paquets. Par conséquent, ce nombre ne peut pas être attribué à un réseau.

L'adresse de classe B est réservée aux réseaux de taille moyenne ou grande. Les adresses IP de classe B utilisent les deux premiers octets (sur quatre) pour indiquer l'adresse réseau. Les deux octets suivants sont utilisés pour les adresses hôte.

Les deux premiers bits du premier octet d'une adresse de classe B sont toujours 10. Les six bits suivants peuvent être des 1 ou des 0. Par conséquent, dans une classe B, le nombre le plus faible pouvant être représenté est 10000000 (128 en décimal) et le plus élevé est 10111111 (191 en décimal). Toute adresse commençant par une valeur comprise entre 128 et 191 dans le premier octet est une adresse de classe B.

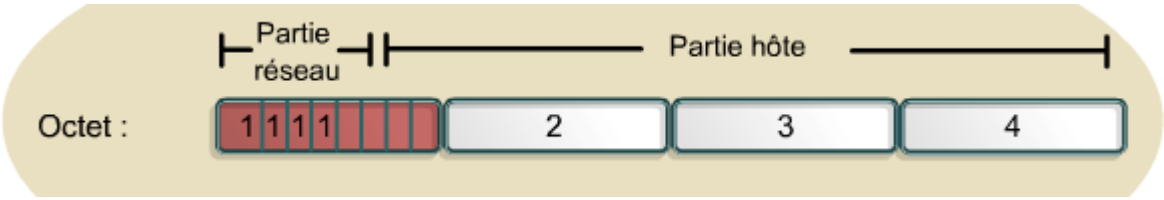
La classe C constitue l'espace le plus utilisé des classes d'adresses initiales. Cet espace d'adressage est réservé aux réseaux de petite taille (254 hôtes maximum).

Une adresse de classe C commence par la valeur binaire 110. Par conséquent, le nombre le plus faible pouvant être représenté est 11000000 (192 en décimal) et le plus élevé est 11011111 (223 en décimal). Toute adresse contenant un nombre compris entre 192 et 223 dans le premier octet est une adresse de classe C.



L'adresse de classe D est réservée à la diffusion multicast d'une adresse IP. Une adresse de multicast est une adresse réseau unique qui achemine les paquets associés à une adresse de destination vers des groupes prédéfinis d'adresses IP. Ainsi, une station peut transmettre simultanément un même flux de données vers plusieurs destinataires.

L'espace d'adressage de classe D, tout comme les autres espaces, est lié à des contraintes mathématiques. Les quatre premiers bits d'une adresse de classe D doivent correspondre à 1110. Par conséquent, le premier octet d'une adresse de classe D est compris entre 1100000 et 11101111 (soit 224 et 239 en décimal). Toute adresse IP commençant par une valeur comprise entre 224 et 239 dans le premier octet est une adresse de classe D.



Une adresse de classe E a été définie. Toutefois, le groupe IETF (*Internet Engineering Task Force*) utilise ces adresses à des fins expérimentales. Aucune adresse de classe E n'est disponible sur Internet. Les quatre premiers bits d'une adresse de classe E sont toujours des 1. Par conséquent, le premier octet d'une adresse de classe E est compris entre 11110000 et 11111111 (soit 240 et 255 en décimal).

La figure 8 indique la plage d'adresses IP du premier octet (sous forme binaire et décimale) de chaque classe d'adresse IP.

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

Déterminez la classe d'après le premier octet.
* 127 (011111111) est une adresse de classe A réservée aux tests en mode bouclé et elle ne peut pas être attribuée à un réseau.

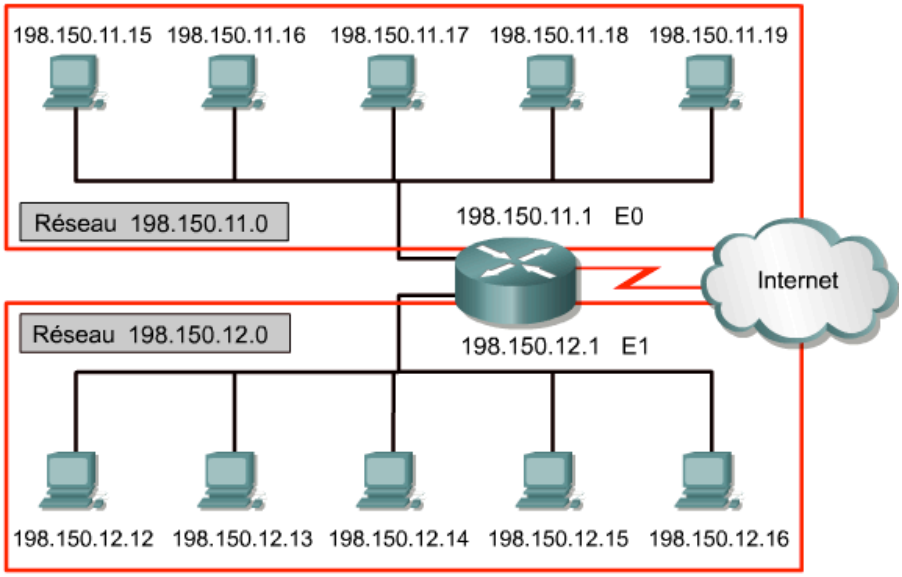
2.2.5 Adresses IP réservées

Certaines adresses hôte sont réservées et ne peuvent pas être affectées aux équipements du réseau. Les adresses hôte réservées se composent des éléments suivants:

- **Une adresse réseau** – pour identifier le réseau lui-même.

Fenêtre contextuelle (pop up)

La section identifiée par la zone supérieure représente le réseau 198.150.11.0. Les données envoyées à un hôte de ce réseau, de 198.150.11.1 à 198.150.11.254, sont affichées en dehors du réseau local 198.159.11.0. Les numéros d'hôte ne sont pris en compte que lorsque les données se trouvent sur le réseau local. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son numéro de réseau est 198.150.12.0.

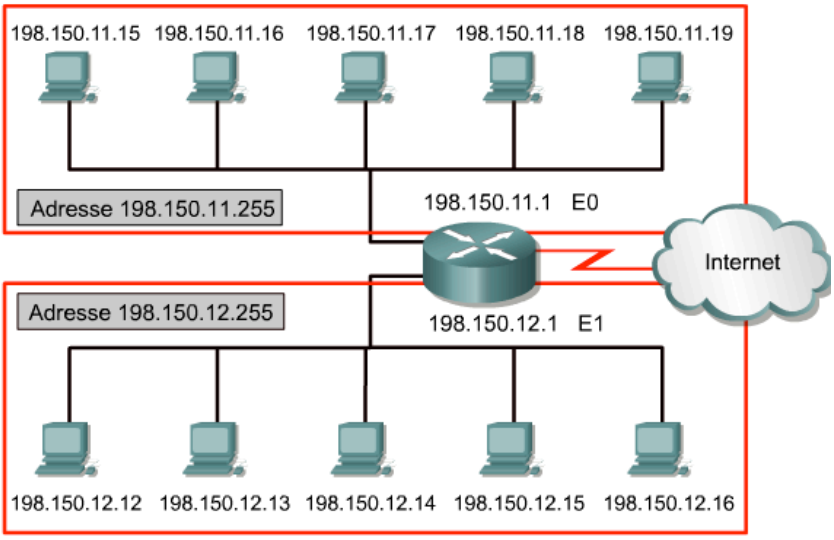


Dans la figure, la section identifiée par la zone supérieure représente le réseau 198.150.11.0. Les données envoyées à un hôte de ce réseau, de 198.150.11.1 à 198.150.11.254, seront visibles en dehors du réseau local sous la forme 198.159.11.0. Les numéros d'hôte ne sont pris en compte que lorsque les données se trouvent sur le réseau local. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son numéro de réseau est 198.150.12.0.

- **Une adresse de broadcast** – pour diffuser des paquets vers tous les équipements d'un réseau.

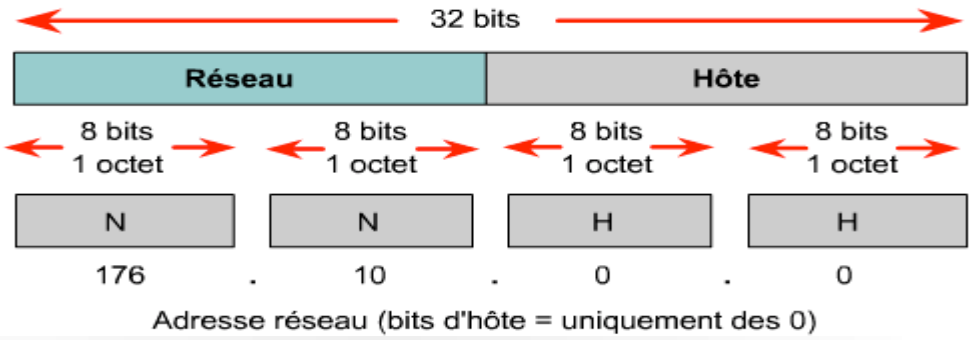
Fenêtre contextuelle (pop up)

La section identifiée par la zone supérieure représente l'adresse de broadcast 198.150.11.255. Les données envoyées à l'adresse de broadcast seront lues par un hôte du réseau, de 198.150.11.1 à 198.150.11.254. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son adresse de broadcast est 198.150.12.255.



Dans la figure, la section identifiée par la zone supérieure représente l'adresse de broadcast 198.150.11.255. Les données envoyées à l'adresse de broadcast seront lues par tous les hôtes du réseau, de 198.150.11.1 à 198.150.11.254. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son adresse de broadcast est 198.150.12.255.

Une adresse IP dont tous les bits hôte sont occupés par des 0 binaires est réservée pour l'adresse réseau. Dans un réseau de classe A, 113.0.0.0 est l'adresse IP du réseau (également connue sous le nom d'ID réseau) comprenant l'hôte 113.1.2.3. Un routeur utilise l'adresse IP du réseau pour acheminer des données sur Internet. Dans un réseau de classe B, l'adresse 176.10.0.0 est une adresse réseau, comme l'illustre la figure



Adresse réseau (bits d'hôte = uniquement des 0)

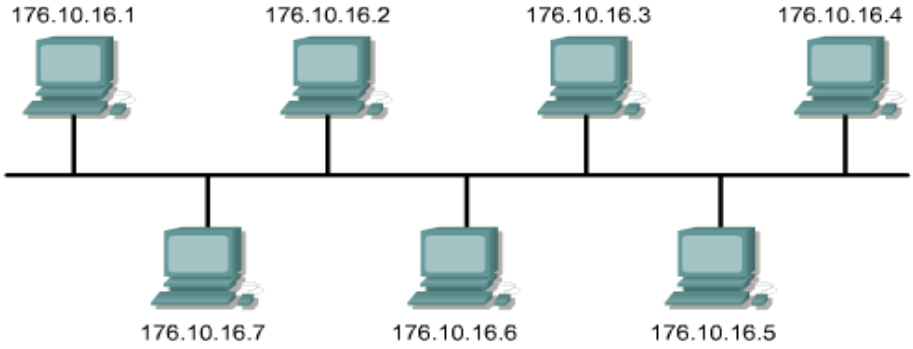
Cette adresse de classe B ne comporte que des bits définis sur 0. C'est pourquoi elle est identifiée en tant qu'adresse réseau.

Dans une adresse réseau de classe B, les deux premiers octets constituent la partie réseau. Les deux derniers octets contiennent des 0, parce que ces 16 bits sont des numéros d'hôtes et sont utilisés pour identifier les équipements reliés au réseau. L'adresse IP, 176.10.0.0, est un exemple d'adresse réseau. Cette adresse n'est jamais affectée comme adresse hôte. L'adresse hôte d'un équipement sur le réseau 176.10.0.0 peut être 176.10.16.1. Dans cet exemple, «176.10» représente la partie réseau, tandis que « 16.1 » représente la partie hôte.

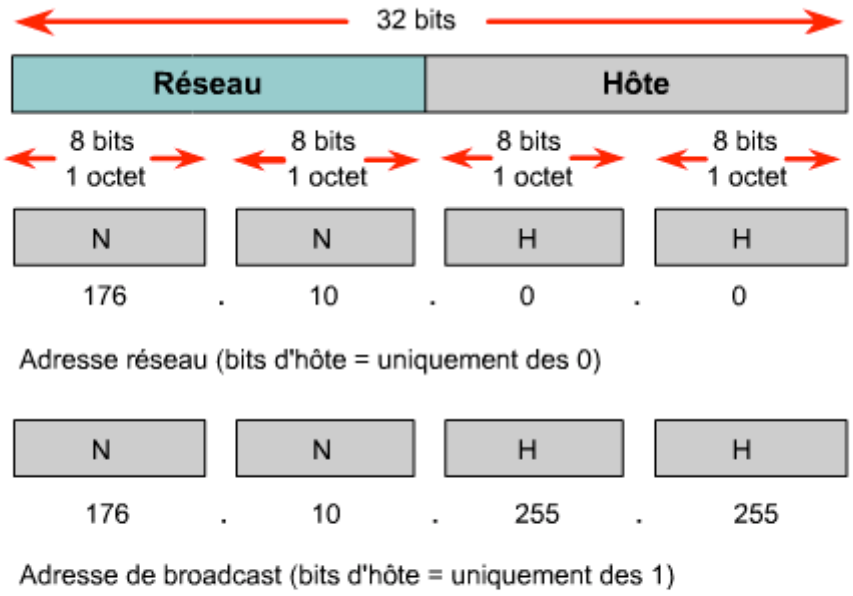
Fenêtre contextuelle (pop up)
L'ordinateur 176.10.16.1 va utiliser une transmission Unicast pour communiquer avec l'ordinateur 176.10.16.3.
L'ordinateur 176.10.16.1 prépare les données à transmettre et vérifie le câble réseau pour détecter s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, le premier ordinateur doit attendre, car un seul ordinateur à la fois peut transmettre des données. Le câble est disponible et l'ordinateur 176.10.16.1 peut effectuer la transmission.
L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.
Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.
Les trames ne sont plus prises en compte par les ordinateurs, à l'exception de l'ordinateur 176.10.16.3, car elles ne correspondent pas à l'adresse MAC de destination des trames entrantes. C'est pourquoi cette transmission est appelée transmission Unicast. Seul l'ordinateur dont l'adresse correspond continue à traiter la trame, et chaque adresse IP étant unique, un seul ordinateur va accepter les données.
L'ordinateur 176.10.16.3 traite les données provenant des trames de données de l'ordinateur 176.10.16.1 et prépare une réponse pour l'ordinateur 176.10.16.1. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.
L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du même segment analysent les trames entrantes.

Les trames sont destinées à l'ordinateur 176.10.16.1. Tous les autres ordinateurs ne prennent alors plus en compte les trames entrantes. Le cycle de la transmission Unicast entre deux ordinateurs est ainsi terminé. Il est important de remarquer que tous les ordinateurs d'un segment Ethernet examinent toujours la totalité du trafic du segment et ne le traitent que s'il leur est destiné.



Une adresse de broadcast est requise afin de pouvoir envoyer les données à tous les équipements d'un réseau. On parle de broadcast lorsqu'une source envoie des données à tous les équipements d'un réseau. Pour vérifier que tous les équipements d'un réseau traitent un tel message de broadcast, la source doit utiliser une adresse IP que tous les équipements peuvent reconnaître et traiter. Les adresses IP de broadcast se terminent par des 1 binaires dans toute la partie hôte de l'adresse.



Cette adresse de classe B est l'adresse de broadcast de ce réseau. Lorsque des paquets sont reçus avec cette adresse de destination, les données sont traitées par chaque ordinateur.

Dans l'exemple 176.10.0.0, les 16 derniers bits forment le champ hôte (ou partie hôte) de l'adresse. Le broadcast envoyé à tous les équipements du réseau comporterait l'adresse de destination 176.10.255.255, sachant que 255 correspond à la valeur décimale d'un octet contenant 11111111.

L'ordinateur 176.10.16.1 va utiliser une transmission de broadcast pour rechercher un serveur DNS. En général, un broadcast est utilisé pour localiser une unité ou un service spécifique. Il peut s'agir d'un serveur DNS, d'un serveur DHCP ou d'autres types d'unités.

L'ordinateur 176.10.16.1 prépare le paquet de broadcast à transmettre et vérifie le câble réseau pour détecter s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, le premier ordinateur doit attendre, car un seul ordinateur à la fois peut transmettre des données. Le câble est disponible et l'ordinateur 176.10.16.1 peut effectuer la transmission.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

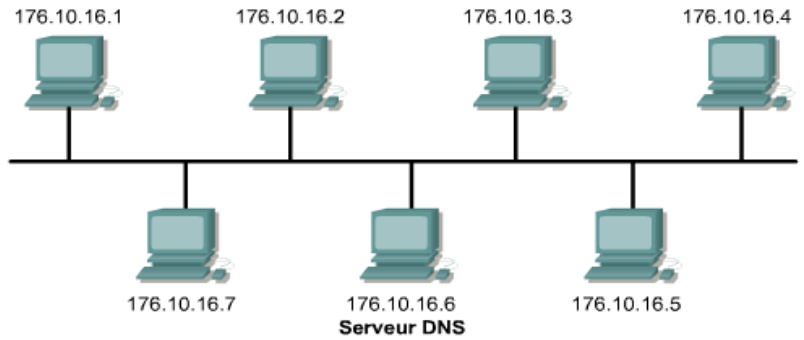
Étant donné qu'il s'agit d'une transmission de broadcast, tous les ordinateurs acceptent la transmission et la traitent. La transmission de broadcast est utilisée afin que tous les hôtes du segment traitent les données. L'ordinateur qui procède au traitement décide également de la suite à donner à la transmission. Dans le cas présent, le broadcast recherchant un serveur DNS, seule cette unité va répondre. Si plusieurs serveurs DNS reçoivent ce broadcast, ils doivent tous répondre.

L'ordinateur 176.10.16.6 traite la requête provenant de la transmission de l'ordinateur 176.10.16.1 et prépare une réponse Unicast pour l'ordinateur 176.10.16.1. L'adresse de l'unité à l'origine de la requête étant connue, la réponse peut être envoyée directement à cette unité. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.

L'ordinateur 176.10.16.6 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du même segment analysent les trames entrantes.

Les trames sont destinées à l'ordinateur 176.10.16.1. Tous les autres ordinateurs ne prennent alors plus en compte les trames entrantes. Le cycle de la transmission Unicast entre deux ordinateurs est ainsi terminé. Il est important de remarquer que tous les ordinateurs d'un segment Ethernet examinent toujours la totalité du trafic du segment et ne le traitent que s'il leur est destiné.

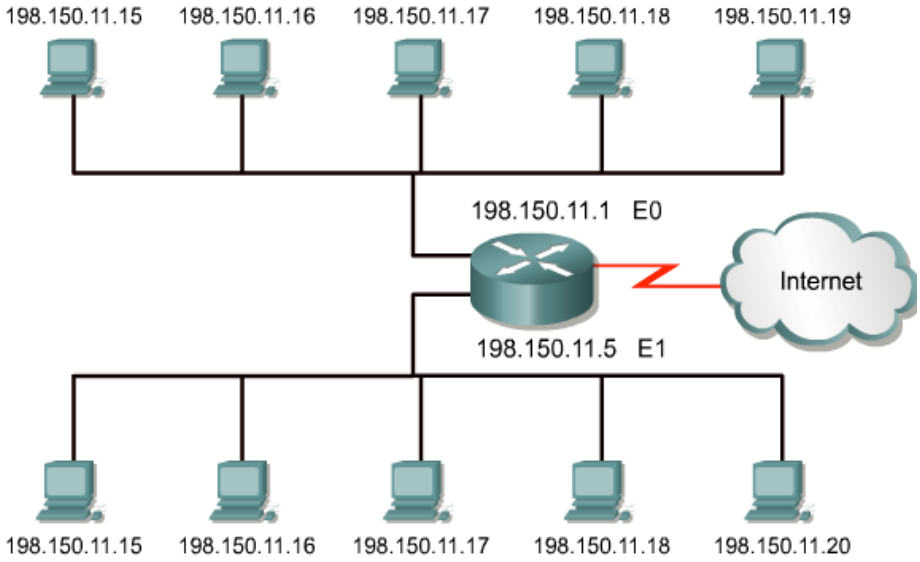


La page suivante traite des adresses IP publiques et privées.

2.2.6 Adresses IP publiques et privées

Fenêtre contextuelle (pop up)

Le modèle d'adressage réseau est incorrect. L'adresse réseau des deux réseaux est 198.150.11.0. Dans cet exemple, lorsque les transmissions de données atteignent le routeur, comment ce dernier doit-il les orienter ? Si cette action était autorisée, le trafic du réseau serait considérablement plus important et irait à l'encontre de la fonction de base du routeur. L'adresse de chaque unité d'un réseau doit être unique.



La stabilité d'Internet découle directement de l'unicité des adresses réseau publiques. Dans la figure, le modèle d'adressage réseau est incorrect. En effet, l'adresse 198.150.11.0 est la même pour les deux réseaux. Dès lors, le routeur n'est pas capable de transférer correctement les paquets de données. L'utilisation d'adresses IP réseau identiques double empêche le routeur de sélectionner le meilleur chemin. L'adresse de chaque équipement d'un réseau doit être unique.

Il fallait donc trouver un moyen de veiller à cela. À l'origine, un organisme portant le nom d'InterNIC (*Internet Network Information Center*) était chargé de cette vérification. Celui-ci n'existe plus et a été remplacé par l'IANA (*Internet Assigned Numbers Authority*). L'IANA gère scrupuleusement les adresses IP disponibles afin de garantir qu'une même adresse publique n'est pas utilisée deux fois. En cas de doublons d'adresses, Internet devient instable et ses capacités à transmettre des datagrammes sur le réseau sont compromises.

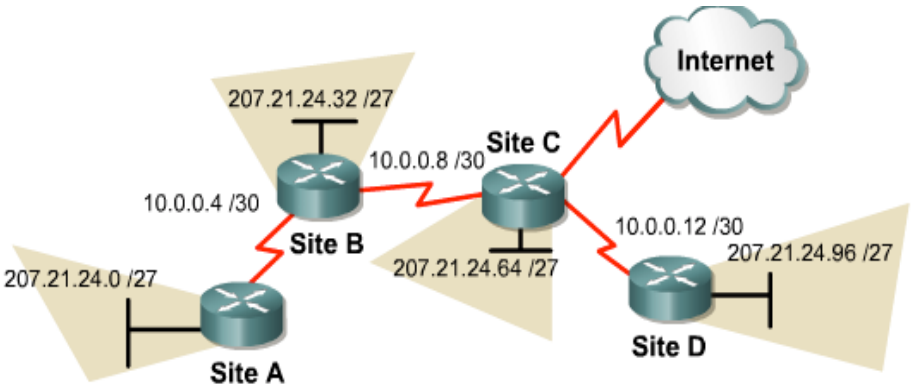
Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique. Les adresses IP publiques sont mondiales et normalisées. Tous les ordinateurs connectés à Internet se conforment au système. Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI) ou d'un registre moyennant une participation.

Avec la croissance rapide d'Internet est apparu le problème de pénurie d'adresses IP publiques. Pour résoudre ce problème, de nouveaux systèmes d'adressage, notamment le routage CIDR (*Classless interdomain routing*) et la norme IPv6, ont été développés. Ces systèmes seront traités ultérieurement dans le cours.

Classe	Plage d'adresses internes RFC 1918
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Les adresses IP privées constituent une solution de rechange au problème de pénurie des adresses IP publiques. Comme précédemment indiqué, les hôtes d'un réseau public doivent disposer d'une adresse IP unique. Néanmoins, les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle

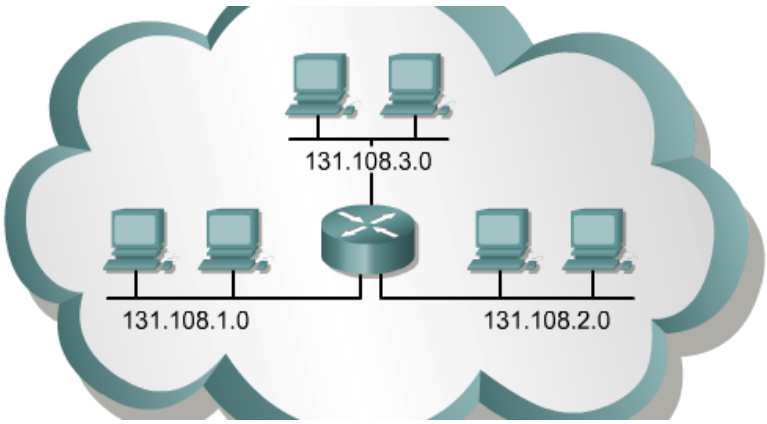
adresse hôte, dès lors que chacun des hôtes du réseau privé est unique. Un grand nombre de réseaux privés coexistent avec les réseaux publics. Cependant, il est vivement déconseillé d'avoir recours à un réseau privé utilisant une adresse quelconque, car ce réseau peut être connecté à Internet. La spécification RFC 1918 réserve trois blocs d'adresses IP pour une utilisation privée et interne. Ceux-ci se composent d'une classe A, d'une plage d'adresses de classe B et d'une plage d'adresses de classe C. Les adresses contenues dans ces plages ne sont pas acheminées sur les routeurs du backbone d'Internet. Ces routeurs Internet les rejettent immédiatement. Dans le cadre de l'adressage d'un intranet non public, d'un TP ou d'un réseau domestique, ces adresses privées peuvent être utilisées à la place d'adresses uniques mondiales. Les adresses IP privées peuvent être mélangées aux adresses publiques, comme indiqué dans le graphique. Ainsi, le nombre d'adresses utilisées pour les connexions internes sera le même.



Les adresses privées peuvent être utilisées pour prendre en charge les liaisons série point-à-point sans gaspiller les adresses IP réelles.

La connexion d'un réseau à Internet par le biais d'adresses publiques nécessite la conversion des adresses privées en adresses publiques. Ce processus de conversion est appelé «NAT» (*Network Address Translation*). L'équipement chargé d'exécuter le système NAT est généralement un routeur. Le système NAT, ainsi que le routage CIDR et la norme IPv6 seront abordés plus tard dans le cursus.

2.2.7 Introduction aux sous-réseaux



Le découpage en sous-réseaux constitue l'une des solutions de gestion des adresses IP. Cette méthode, basée sur la fragmentation de classes d'adresses réseau entières en composants plus petits, a permis d'éviter la pénurie d'adresses IP. Il est impossible de traiter du protocole TCP/IP sans aborder la question des sous-réseaux. En tant qu'administrateur système, il est primordial d'appréhender la notion de découpage en sous-réseaux afin de pouvoir subdiviser un LAN et y identifier les différents réseaux. Dans le cas de réseaux de petite taille, il n'est pas toujours utile de créer des sous-réseaux. En revanche, dans le cadre des réseaux de grande à très grande taille, cette opération s'impose. Le découpage d'un réseau en sous-réseaux implique l'utilisation du masque de sous-réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces. On pourrait établir une comparaison avec le système téléphonique américain qui se compose d'un indicatif régional, d'un indicatif de central et de numéros locaux.

L'administrateur système doit réfléchir aux problèmes suivants lors de l'évolution d'un réseau: il est essentiel de définir le nombre de sous-réseaux ou de réseaux requis, ainsi que le nombre d'hôtes requis par réseau. En utilisant des sous-réseaux, le réseau n'est pas limité aux masques de réseau de classe A, B ou C par défaut. En outre, la conception du réseau est plus flexible.

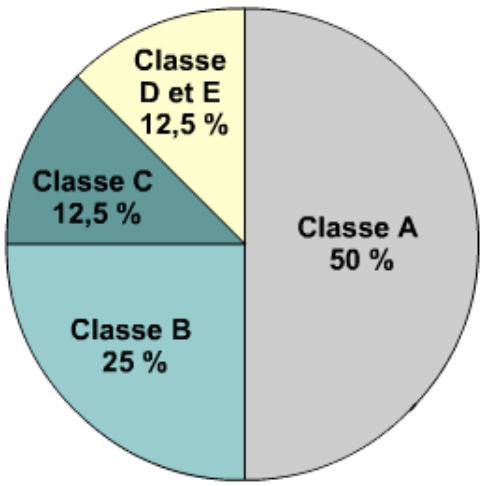
Les adresses de sous-réseau contiennent une partie réseau, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine pour l'ensemble du réseau. L'administrateur réseau jouit d'une grande souplesse d'adressage dans la mesure où il peut déterminer la façon dont la partie hôte d'origine sera subdivisée pour créer les nouveaux champs de sous-réseau et d'hôte.

Nombre de bits emprunté au champ hôte pour créer des sous-réseaux	Nombre de sous-réseaux	Nombre d'hôtes de classe A par sous-réseau	Nombre d'hôtes de classe B par sous-réseau	Nombre d'hôtes de classe C par sous-réseau
2	2	4,194,302	16,382	62
3	6	2,097,150	8,190	30
4	14	1,048,574	4,094	14
5	30	524,286	2,046	6
6	62	262,142	1,022	2
7	126	131,070	510	-
8	254	65,534	254	-

Pour créer une adresse de sous-réseau, l'administrateur réseau emprunte des bits au champ d'hôte et les désigne comme champ de sous-réseau. Le nombre minimal de bits pouvant être empruntés est deux. Lors de la création d'un sous-réseau pour lequel un seul bit a été emprunté, le numéro de réseau est .0, tandis que le numéro de broadcast est le réseau .255. Le nombre maximal de bits pouvant être empruntés est égal à tout nombre laissant au moins deux bits disponibles pour le numéro d'hôte.

2.2.8 Comparaison entre IPv4 et IPv6

Lors de son adoption dans les années 80, le protocole TCP/IP s'appuyait sur un système d'adressage à deux niveaux. Ses possibilités d'évolution étaient alors parfaitement adaptées. Malheureusement, ses concepteurs ne pouvaient pas prévoir qu'il allait soutenir un réseau mondial dédié à l'information, aux échanges commerciaux et au divertissement. Dans les années 80, la stratégie d'adressage proposée par la version IPv4 s'avérait relativement évolutive. Néanmoins, elle ne réussit pas à satisfaire les exigences liées à l'attribution des adresses.



Les adresses de classe A et B étant pratiquement toutes utilisées, les adresses de classe C (12,5 % de l'espace total) peuvent être attribuées aux nouveaux réseaux.

Les adresses de classe A et B représentent 75% de l'espace d'adresses IPv4. Toutefois, moins de 17 000 organisations peuvent recevoir un numéro de réseau de classe A ou B. Le nombre d'adresses réseau de

classe C est nettement plus important que celui des adresses de classe A et B, bien qu'il ne représente que 12,5 % des quatre milliards d'adresses IP disponibles.

Malheureusement, seuls 254 hôtes utilisables sont disponibles sur un réseau de classe C. Ce nombre ne permet pas de satisfaire les besoins des organisations plus importantes qui ne peuvent pas obtenir d'adresses de classe A ou B. S'il existait davantage d'adresses de classe A, B et C, un nombre trop élevé d'adresses réseau risquerait de provoquer l'arrêt des routeurs, du fait du volume trop important des tables de routage requises pour stocker les routes permettant d'atteindre les différents réseaux.

Dès 1992, le groupe IETF (*Internet Engineering Task Force*) a identifié deux problèmes :

- La diminution inquiétante des adresses réseau IPv4 disponibles. À l'époque, l'espace d'adresses de classe B était sur le point d'être saturé.
- La hausse importante et rapide du volume des tables de routage d'Internet en raison de l'augmentation du nombre de connexions des réseaux de classe C. Ce déferlement de nouvelles informations réseau constituait une menace pour le bon fonctionnement des routeurs Internet.

Au cours des deux dernières décennies, plusieurs extensions de la norme IPv4 ont été développées. Celles-ci étaient spécifiquement con��ues pour optimiser l'espace des adresses 32 bits. Deux des plus significatives, à savoir les masques de sous-réseau et le routage CIDR (*Classless interdomain routing*), feront l'objet d'une étude plus approfondie dans les leçons suivantes.

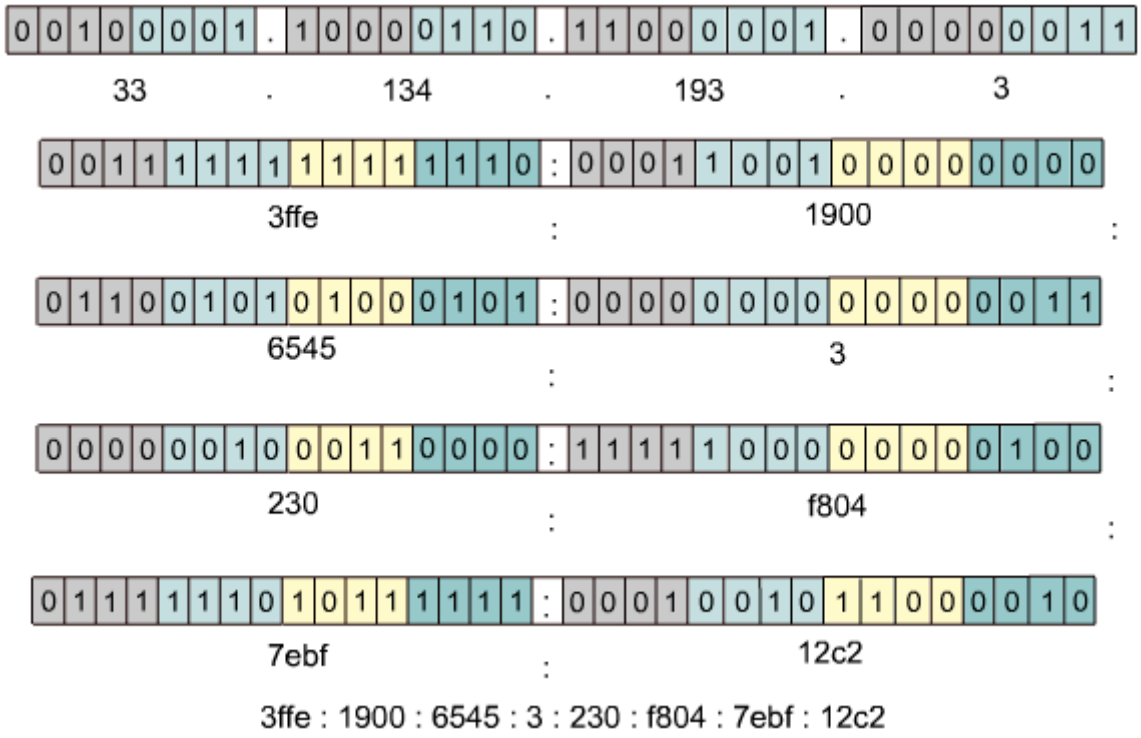
Version 4 du protocole IP (IPv4)	4 octets
11010001.11011100.11001001.01110001	
209.156.201.113	
4 294 467 295 adresses IP	

Version 6 du protocole IP (IPv6)	16 octets
11010001.11011100.11001001.01110001.11010001.11011100	
110011001.01110001.11010001.11011100.11001001	
01110001.11010001.11011100.11001001.01110001	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3,4 x 10^{38} adresses IP	

Entre-temps, une version encore plus flexible et évolutive de la norme IP (IPv6) a fait son apparition. IPv6 encode les adresses sur 128 bits au lieu de 32 (en utilisant des nombres hexadécimaux), ce qui porte le nombre d'adresses possibles à 340 x 10^{36}. Cette version devrait ainsi couvrir l'intégralité des besoins en communication pour les années à venir.

Fenêtre contextuelle (pop up)

Les adresses IPv4, qui sont les plus fréquentes, ont une longueur de 32 bits et sont exprimées en notation décimale avec des points de séparation. Toutefois, les adresses IPv6 ont une longueur de 128 bits et sont exprimées au format hexadécimal avec deux-points de séparation. Les deux-points séparent les champs de 16 bits. Les zéros de tête peuvent être omis dans chaque champ, comme dans l'exemple ci-dessus, où " 0003 " est écrit " 3 ".



La figure présente les adresses IPv4 et IPv6. Les adresses IPv4 ont une longueur de 32 bits et sont exprimées en notation décimale avec des points de séparation. Les adresses IPv6 ont une longueur de 128 bits et constituent un identifiant pour une interface ou un ensemble d'interfaces. Les adresses IPv6 sont affectées à des interfaces et non à des nœuds. Dans la mesure où chaque interface appartient à un nœud unique, toutes les adresses d'unicast attribuées aux interfaces du nœud peuvent être utilisées comme identifiant du nœud. Les adresses IPv6 sont exprimées au format hexadécimal avec des deux-points de séparation. Les champs IPv6 ont une longueur de 16 bits. Afin de faciliter la lecture des adresses, il est possible d'omettre les zéros de tête dans chaque champ. Le champ «0003» est écrit «3». La représentation abrégée IPv6 de 128 bits consiste en huit nombres de 16 bits, représentés par quatre chiffres hexadécimaux.

Après des années de planification et de développement, IPv6 s'implante doucement sur les réseaux et devrait progressivement supplanter le protocole IPv4.

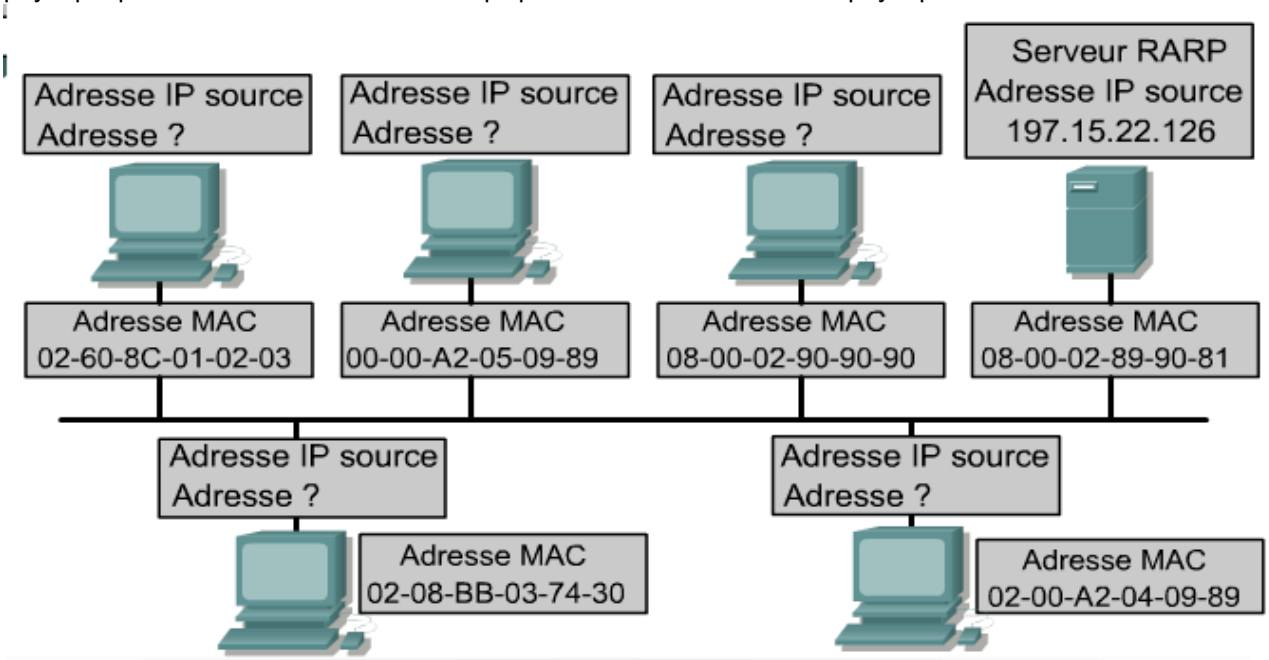
2.3 Obtention d'une adresse IP

2.3.1 Obtention d'une adresse Internet

Un hôte réseau doit se procurer une adresse unique mondialement afin de se connecter à Internet. L'adresse physique ou MAC d'un hôte n'est significative que localement, car elle identifie l'hôte sur le réseau local. Cette adresse opérant au niveau de la couche 2, le routeur ne l'utilise pas pour transmettre des données au-delà du réseau local.

Les adresses IP sont les adresses les plus fréquemment utilisées pour les communications Internet. Ce protocole, basé sur un système d'adressage hiérarchique, permet d'associer des adresses individuelles entre elles et de les traiter en tant que groupes. Ce groupement d'adresses assure un transfert efficace des données sur Internet.

Les administrateurs réseau font appel à deux méthodes différentes pour affecter les adresses IP. Il s'agit des méthodes statique et dynamique. L'adressage statique ainsi que trois variantes d'adressage dynamique seront abordés ultérieurement dans cette leçon. Quelle que soit la méthode choisie, deux interfaces ne peuvent jamais avoir la même adresse IP. Lorsque deux hôtes utilisent la même adresse IP, ils risquent de ne pas fonctionner correctement en raison d'un conflit d'adresses. Comme l'illustre la figure, les hôtes sont dotés d'une adresse physique par le biais de la carte réseau qui permet d'accéder au média physique.



Les hôtes bénéficient d'une adresse physique car ils comportent une carte réseau qui permet d'accéder au média physique. Les adresses IP doivent être attribuées à l'hôte selon l'une des méthodes possibles. L'attribution des adresses IP peut être statique ou dynamique.

2.3.2 Attribution statique d'une adresse IP

L'attribution statique convient particulièrement aux réseaux de petite taille qui subissent peu de changements. L'administrateur système effectue manuellement les opérations d'affectation et de suivi des adresses IP pour chaque ordinateur, imprimante ou serveur de l'intranet. La tenue d'archives est essentielle pour prévenir les conflits d'adresses IP. Toutefois, cette technique n'est possible que dans le cas où peu d'équipements sont connectés au réseau.

Les serveurs doivent recevoir une adresse IP statique de sorte que les stations de travail et les autres équipements puissent toujours accéder aux services requis. Imaginez combien il serait complexe d'appeler une entreprise qui change quotidiennement de numéro de téléphone.

Les autres équipements nécessitant des adresses IP statiques sont les imprimantes réseau, les serveurs d'applications et les routeurs.

2.3.3 Attribution d'une adresse IP à l'aide du protocole RARP

Le protocole RARP associe des adresses MAC connues à des adresses IP. Cette association permet à certains ��quipements d’encapsuler les données avant de les envoyer sur le réseau. Un équipement réseau, tel qu'une station de travail sans disque dur local, peut connaître son adresse MAC mais ignorer son adresse IP. Le protocole RARP permet à l'équipement de lancer une requête afin de connaître son adresse IP. Les équipements utilisant le protocole de résolution inverse d'adresses requièrent un serveur RARP pour répondre aux requêtes de ce protocole.

Examinons l'exemple d'un équipement source qui souhaite envoyer des données à un autre équipement. L'équipement source connaît sa propre adresse MAC, mais il ne trouve pas son adresse IP dans la table ARP. Pour que l'équipement de destination puisse récupérer les données, les transférer aux couches supérieures du

modèle OSI et répondre à l'équipement source, ce dernier doit indiquer son adresse MAC et son adresse IP. L'équipement source lance alors un processus appelé «requête RARP». Cette requête permet d'aider le matériel source à détecter sa propre adresse IP. Les requêtes RARP sont diffusées sur le LAN et c'est le serveur RARP, habituellement un routeur, qui y répond.

Le protocole de résolution inverse d'adresses utilise le même format de paquet que le protocole ARP. Cependant, dans une requête RARP, les en-têtes MAC et le code de fonctionnement sont différents de ceux d'une requête ARP. La structure du paquet RARP contient des champs pour les adresses MAC des équipements d'origine et de destination. Le champ de l'adresse IP d'origine est vide. Le message de broadcast est envoyé à tous les équipements du réseau. Les figures illustrent l'adresse MAC de destination sous la forme FF:FF:FF:FF:FF:FF. Les stations de travail exécutant le protocole de résolution inverse d'adresses comportent des codes en mémoire ROM qui déclenchent le processus RARP. Les figures ndiquent avec précision le processus RARP.

2.3.4 Attribution d'une adresse IP à l'aide du protocole BOOTP

Le protocole BOOTP fonctionne dans un environnement client-serveur et ne requiert qu'un seul échange de paquet pour obtenir des informations sur le protocole IP. Contrairement au protocole RARP, les paquets BOOTP peuvent contenir l'adresse IP, l'adresse du routeur, l'adresse du serveur ainsi que des informations spécifiques du fournisseur.

L'un des problèmes du protocole BOOTP est de ne pas avoir été conçu pour l'attribution dynamique d'adresses. Il permet à un administrateur réseau de créer un fichier de configuration qui définit les paramètres de chaque équipement. L'administrateur doit ajouter les hôtes et tenir à jour la base de données BOOTP. Bien que les adresses soient attribuées de manière dynamique, il existe une relation biunivoque entre le nombre d'adresses IP et le nombre d'hôtes. Autrement dit, à chaque hôte du réseau doit correspondre un profil BOOTP comportant une adresse IP. Deux profils ne peuvent pas partager une même adresse IP. Ces profils pourraient être utilisés simultanément, ce qui signifierait que deux hôtes disposent d'une même adresse IP.

Un équipement utilise le protocole BOOTP au démarrage pour obtenir une adresse IP. BOOTP utilise la couche UDP pour transporter les messages. Le message UDP est encapsulé dans un paquet IP. Un ordinateur utilise le protocole BOOTP pour envoyer un paquet IP de broadcast en utilisant une adresse IP de destination constituée de tous les 1 binaires (255.255.255.255 en notation décimale séparée par des points). Un serveur BOOTP reçoit le message de broadcast, puis en envoie un à son tour. Le client reçoit une trame et vérifie l'adresse MAC. Si le client trouve sa propre adresse MAC dans le champ d'adresse de destination et une adresse de broadcast dans le champ de destination IP, il enregistre et stocke l'adresse IP ainsi que toutes les informations fournies dans le message de réponse BOOTP. Les figures indiquent avec précision le processus BOOTP.

2.3.5 Gestion des adresses IP à l'aide du protocole DHCP

Le protocole DHCP a été proposé pour succéder au protocole BOOTP. Contrairement au protocole BOOTP, le protocole DHCP permet à un hôte d'obtenir une adresse IP de manière dynamique sans que l'administrateur réseau ait à définir un profil pour chaque équipement. Avec le protocole DHCP, il suffit qu'une plage d'adresses IP soit définie sur un serveur DHCP. Lorsque les ordinateurs se connectent, ils communiquent avec le serveur DHCP et demandent une adresse. Le serveur DHCP choisit une adresse et l'affecte à l'ordinateur hôte. Grâce au protocole DHCP, la configuration réseau tout entière d'un ordinateur peut être obtenue dans un seul message.Cela comprend les données fournies par le message BOOTP, plus une adresse IP allouée et un masque de sous-réseau.

Le protocole DHCP dispose d'un avantage majeur sur le protocole BOOTP, car il permet aux utilisateurs d'être mobiles. Les utilisateurs peuvent changer de connexion réseau d'un emplacement à l'autre, et ce en toute liberté. Il n'est plus nécessaire d'utiliser un profil fixe pour chaque équipement relié au réseau, comme cela était le cas avec le système BOOTP. Cette évolution revêt une importance particulière dans la mesure où le protocole DHCP peut octroyer une adresse IP à un équipement, puis utiliser cette même adresse pour un autre utilisateur lorsque le premier ne s'en sert plus. Autrement dit, le protocole DHCP offre une relation «un à plusieurs» pour les

adresses IP. De plus, une adresse est disponible pour quiconque se connectant au réseau. Les figures indiquent avec précision le processus DHCP.

2.3.6 Problèmes liés à la résolution d'adresses

L'une des principales difficultés liées au réseau est d'arriver à communiquer avec les autres équipements du réseau. Lors des échanges TCP/IP, un datagramme appartenant à un réseau local doit comporter une adresse MAC et une adresse IP de destination. Ces adresses doivent être valides et elles doivent correspondre aux adresses MAC et IP de destination de l'équipement hôte. Si elles ne correspondent pas, le datagramme est rejeté par l'hôte de destination. Pour échanger des données dans un segment LAN, deux adresses sont requises. Une solution de mappage automatique des adresses IP avec des adresses MAC est également requise. Le mappage manuel de ces adresses se révélerait beaucoup trop long. La pile de protocoles TCP/IP comprend un protocole appelé «ARP» (*Address Resolution Protocol*) qui peut obtenir automatiquement les adresses MAC pour la transmission locale. Plusieurs problèmes apparaissent lors de l'envoi des données à l'extérieur du réseau local.

Pour échanger des données entre deux segments LAN, un élément supplémentaire est requis. Les adresses IP et MAC sont nécessaires à l'hôte de destination et à l'équipement de routage intermédiaire. Proxy ARP est une variante du protocole ARP qui fournit l'adresse MAC d'un équipement intermédiaire pour la transmission de données vers un autre segment du réseau en dehors du LAN.

2.3.7 Protocole ARP (Address Resolution Protocol)

Dans un réseau TCP/IP, un paquet de données doit contenir une adresse MAC de destination et une adresse IP de destination. Si l'une ou l'autre est manquante, les données qui se trouvent au niveau de la couche 3 ne sont pas transmises aux couches supérieures. Ainsi, les adresses MAC et IP se contrôlent et s'équilibrent mutuellement. Une fois que les équipements ont déterminé les adresses IP des équipements de destination, ils peuvent ajouter les adresses MAC de destination aux paquets de données.

Certains tiennent à jour des tables contenant les adresses MAC et IP des autres équipements connectés au même réseau local. Ces tables sont appelées «tables ARP». Elles sont stockées dans la mémoire RAM, où les informations en mémoire cache sont mises à jour automatiquement dans chaque équipement. Il est très rare qu'un utilisateur ait à entrer manuellement des informations dans une table ARP. Tout équipement du réseau met à jour sa propre table ARP. Si un équipement cherche à envoyer des données sur le réseau, il utilise les informations contenues dans la table ARP.

Lorsqu'une source détermine l'adresse IP d'une destination, elle consulte la table ARP pour trouver l'adresse MAC de destination. Une fois l'entrée recherchée trouvée dans sa table (adresse IP de destination correspondant à l'adresse MAC de destination), elle associe l'adresse IP à l'adresse MAC et l'utilise pour encapsuler les données. Le paquet de données est alors envoyé à l'équipement de destination via le média réseau.

Les équipements disposent de deux méthodes pour obtenir les adresses MAC à ajouter aux données encapsulées. L'une d'elles consiste à surveiller le trafic existant sur le segment du réseau local. Toutes les stations du réseau Ethernet analysent le trafic afin de déterminer si la transmission leur est destinée. Une partie de ce processus consiste à enregistrer les adresses source IP et MAC du datagramme dans une table ARP. Ainsi, les paires d'adresses sont intégrées à la table ARP lors de l'envoi des données sur le réseau. L'autre solution qui permet d'obtenir une paire d'adresses pour la transmission des données consiste à diffuser une requête ARP.

L'ordinateur qui a besoin d'une paire d'adresses IP et MAC diffuse une requête ARP. Tous les autres équipements du réseau local analysent ensuite cette requête. Si l'un des équipements correspond à l'adresse IP de la requête, il renvoie une réponse ARP avec sa paire d'adresses IP/MAC. Si l'adresse IP appartient au réseau local, mais que l'ordinateur est introuvable ou hors tension, aucune réponse n'est faite à la requête ARP. Dans ce cas, l'équipement source génère une erreur. Si la requête appartient à un réseau IP différent, un autre processus doit être utilisé.

Les routeurs ne transmettent pas les paquets de broadcast. Lorsque la fonction est activée, le routeur exécute une requête via Proxy ARP. Proxy ARP est une variante du protocole ARP. Dans cette variante, un routeur envoie une réponse ARP, qui contient l'adresse MAC de l'interface qui a reçu la requête, à l'hôte demandeur. Le routeur répond avec ses adresses MAC aux requêtes dont l'adresse IP n'appartient pas à la plage d'adresses du sous-réseau local.

Une autre solution pour envoyer des données à l'adresse d'un équipement situé sur un autre segment du réseau, consiste à configurer une passerelle par défaut. Une passerelle par défaut est une option « host » dans laquelle l'adresse IP de l'interface du routeur est enregistrée dans la configuration réseau de l'hôte. L'hôte source compare l'adresse IP de destination à sa propre adresse IP afin de déterminer si les deux adresses sont situées sur le même segment. Si l'hôte de destination ne se trouve pas sur le même segment, l'hôte d'origine envoie les données en utilisant l'adresse IP actuelle de destination et l'adresse MAC du routeur. Cette dernière a été extraite de la table ARP à l'aide de l'adresse IP du routeur.

Si la passerelle par défaut de l'hôte ou la fonction Proxy ARP du routeur n'est pas configurée, aucune donnée ne peut quitter le réseau local. L'une ou l'autre est nécessaire pour établir une connexion avec une machine située à l'extérieur du réseau local.

Résumé

Le modèle de référence TCP/IP développé par le ministère américain de la défense (*DoD*) comporte quatre couches : la couche application, la couche transport, la couche Internet et la couche d'accès au réseau. La couche application gère les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue. La couche transport offre des services de transport de l'hôte à la destination. Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transmettre les paquets sur le réseau. La couche d'accès au réseau est responsable de l'établissement d'une liaison physique à un support réseau.

Bien que certaines couches du modèle de référence TCP/IP correspondent aux sept couches du modèle OSI, des différences existent. Le modèle TCP/IP intègre la couche présentation et la couche session dans sa couche application. Le modèle TCP/IP regroupe les couches physique et liaison de données du modèle OSI dans sa couche d'accès au réseau.

Les routeurs utilisent l'adresse IP pour acheminer les paquets de données d'un réseau à un autre. Les adresses IP ont une longueur de trente deux bits (dans la version 4 du protocole IP) et sont divisées en quatre octets de huit bits. Ils fonctionnent au niveau de la couche réseau (couche 3) du modèle OSI, qui est la couche Internet du modèle TCP/IP.

L'adresse IP d'un hôte est une « adresse logique », ce qui signifie qu'elle peut être modifiée. L'adresse MAC (*Media Access Control*) de la station de travail est une adresse physique de 48 bits. Elle est généralement inscrite de manière indélébile sur la carte réseau. La seule façon de la modifier est de remplacer la carte réseau. Afin de transmettre des données TCP/IP dans un segment LAN, une adresse IP de destination et une adresse MAC de destination sont requises. Bien que l'adresse IP soit unique et routable sur Internet, elle doit pouvoir être mappée avec une adresse MAC lors de la réception d'un paquet sur le réseau de destination. La pile de protocoles TCP/IP comprend un protocole appelé «ARP» (*Address Resolution Protocol*) qui peut obtenir automatiquement les adresses MAC pour la transmission locale. Une variante du protocole ARP, appelée « Proxy ARP », fournit l'adresse MAC d'un équipement intermédiaire pour la transmission de données à un autre segment du réseau.

Il existe cinq classes d'adresses IP (de A à E). Seules les trois premières classes sont utilisées commercialement. En fonction de la classe, les parties réseau et hôte de l'adresse occupent un nombre différent de bits. Les adresses de classe D sont utilisées pour les groupes de multicast. Les adresses de classe E sont utilisées à des fins expérimentales.

Une adresse IP dont tous les bits hôte sont occupés par des 0 binaires est utilisée pour identifier le réseau lui-même. Une adresse dont tous les bits hôte sont occupés par des 1 correspond à une adresse de broadcast. Elle est utilisée pour diffuser des paquets vers tous les équipements d'un réseau.

Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique. Les adresses IP publiques sont mondiales et normalisées. Les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse hôte, dès lors que chacun des hôtes du réseau privé est unique. Trois blocs d'adresses IP sont réservés pour une utilisation privée et interne. Ces blocs se composent d'une classe A, d'une plage d'adresses de classe B et d'une plage d'adresses de classe C. Toutes les adresses appartenant à ces plages sont rejetées par les routeurs et ne sont pas acheminées sur le backbone d'Internet.

Le découpage en sous-réseaux représente une solution de rechange pour subdiviser un LAN et y identifier des réseaux distincts. La subdivision d'un réseau en sous-réseaux implique l'utilisation du masque de sous-réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces. Les adresses de sous-réseau contiennent une partie réseau, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine pour l'ensemble du réseau.

Une version encore plus flexible et évolutive de la norme IP (IPv6) a fait son apparition. Il s'agit d'IPv6 qui encode les adresses sur 128 bits au lieu de 32 (en utilisant des nombres hexadécimaux). Le protocole IPv6 s'implante sur certains réseaux et devrait finir par supplanter le protocole IPv4.

Les adresses IP sont attribuées aux hôtes comme suit:

- **De façon statique** (manuellement) – par l'administrateur réseau.

De façon dynamique (automatiquement) – à l'aide des protocoles RARP, BOOTP ou DHCP.