

# Vue d'ensemble de TCP/IP

## Contenu

[Introduction](#)

[Technologie TCP/IP](#)

[TCP](#)

[IP](#)

[Routage dans les environnements IP](#)

[Protocoles de routage intérieurs](#)

[RIP](#)

[IGRP](#)

[EIGRP](#)

[OSPF](#)

[IS-IS intégré](#)

[Protocoles de routage extérieurs](#)

[EGP](#)

[BGP](#)

[Implémentation TCP/IP de Cisco](#)

[Restrictions d'accès](#)

[Tunnellisation](#)

[multicast IP](#)

[Suppression des informations réseau](#)

[Distance administrative](#)

[Redistribution du protocole de routage](#)

[Support réseau sans serveur](#)

[Surveillance et débogage du réseau](#)

[Résumé](#)

[Informations connexes](#)

## Introduction

Au cours des deux décennies qui ont suivi leur invention, l'hétérogénéité des réseaux s'est poursuivie avec le déploiement d'Ethernet, de Token Ring, de l'Interface de données distribuées sur fibre optique (FDDI), des protocoles X.25, de Frame Relay, du Switched Multimegabit Data Service (SMDS), du Réseau numérique à intégration de services (RNIS) et, plus récemment, du Mode de transfert asynchrone (ATM). Les protocoles Internet sont la meilleure approche éprouvée pour l'interconnexion de cette gamme diversifiée de technologies LAN et WAN.

La suite de protocoles Internet inclut non seulement des spécifications de niveau inférieur, telles que TCP (Transmission Control Protocol) et IP (Internet Protocol), mais également des spécifications pour des applications courantes telles que la messagerie électronique, l'émulation de terminal et le transfert de fichiers. [La Figure 1](#) illustre la suite de protocoles TCP/IP par rapport

au modèle de référence OSI. [La Figure 2](#) présente certains des protocoles Internet importants et leur relation avec le modèle de référence OSI. Pour obtenir des informations sur le modèle de référence OSI et le rôle de chaque couche, reportez-vous au document Notions de base sur l'interconnexion de réseaux.

Les protocoles Internet sont la suite de protocoles multifournisseurs la plus répandue aujourd'hui. La prise en charge d'au moins une partie de la suite de protocoles Internet est disponible auprès de pratiquement tous les fournisseurs d'ordinateurs.

## Technologie TCP/IP

Cette section décrit les aspects techniques du protocole TCP, du protocole IP, des protocoles associés et des environnements dans lesquels ces protocoles fonctionnent. Étant donné que le principal objectif de ce document est le routage (une fonction de couche 3), la discussion sur le protocole TCP (un protocole de couche 4) sera relativement brève.

### TCP

TCP est un protocole de transport orienté connexion qui envoie des données sous forme de flux non structuré d'octets. En utilisant des numéros d'ordre et des messages d'accusé de réception, TCP peut fournir à un noeud émetteur des informations de remise sur les paquets transmis à un noeud de destination. Lorsque des données ont été perdues en transit de la source à la destination, le protocole TCP peut retransmettre les données jusqu'à ce qu'une condition de délai d'attente soit atteinte ou jusqu'à ce que la livraison ait réussi. Le protocole TCP peut également reconnaître les messages en double et les supprime de manière appropriée. Si l'ordinateur émetteur transmet trop rapidement pour l'ordinateur récepteur, le protocole TCP peut utiliser des mécanismes de contrôle de flux pour ralentir le transfert de données. Le protocole TCP peut également communiquer des informations de livraison aux protocoles et applications de couche supérieure qu'il prend en charge. Toutes ces caractéristiques font du protocole TCP un protocole de transport fiable de bout en bout. TCP est spécifié dans [RFC 793](#) .

**Figure 1 - Suite de protocoles TCP/IP par rapport au modèle de référence OSI**

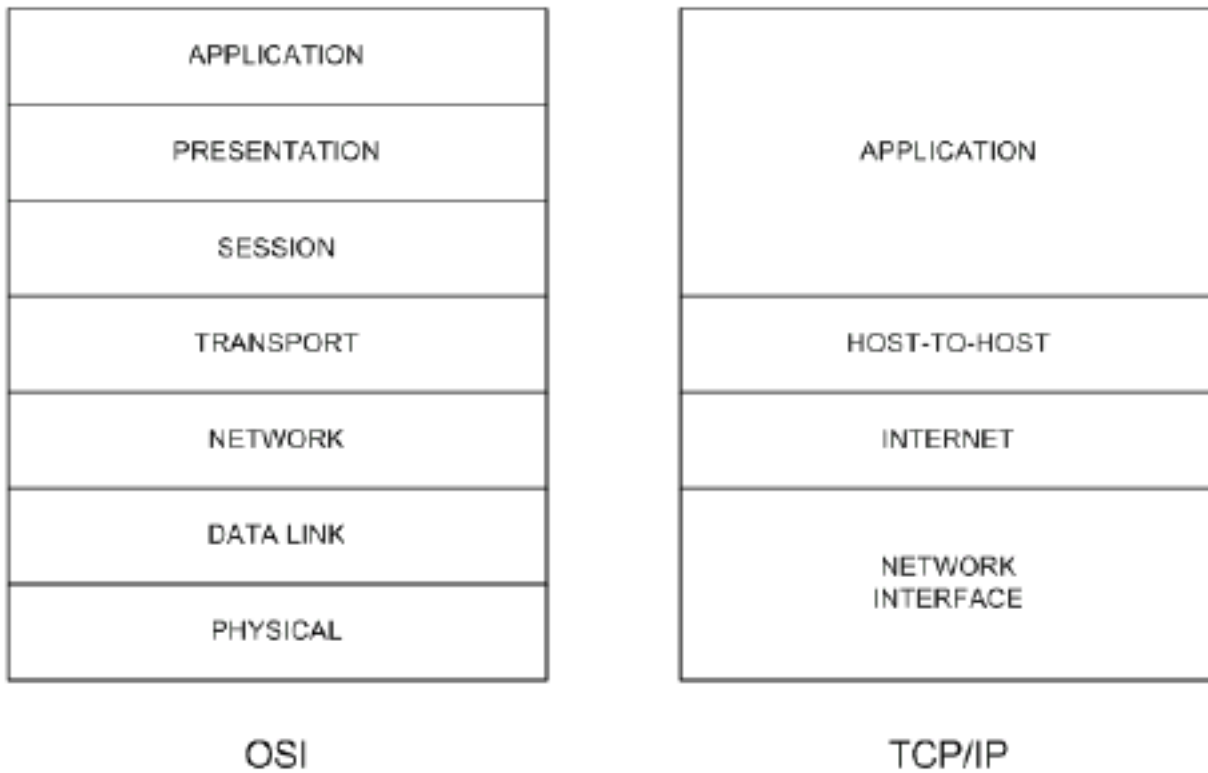
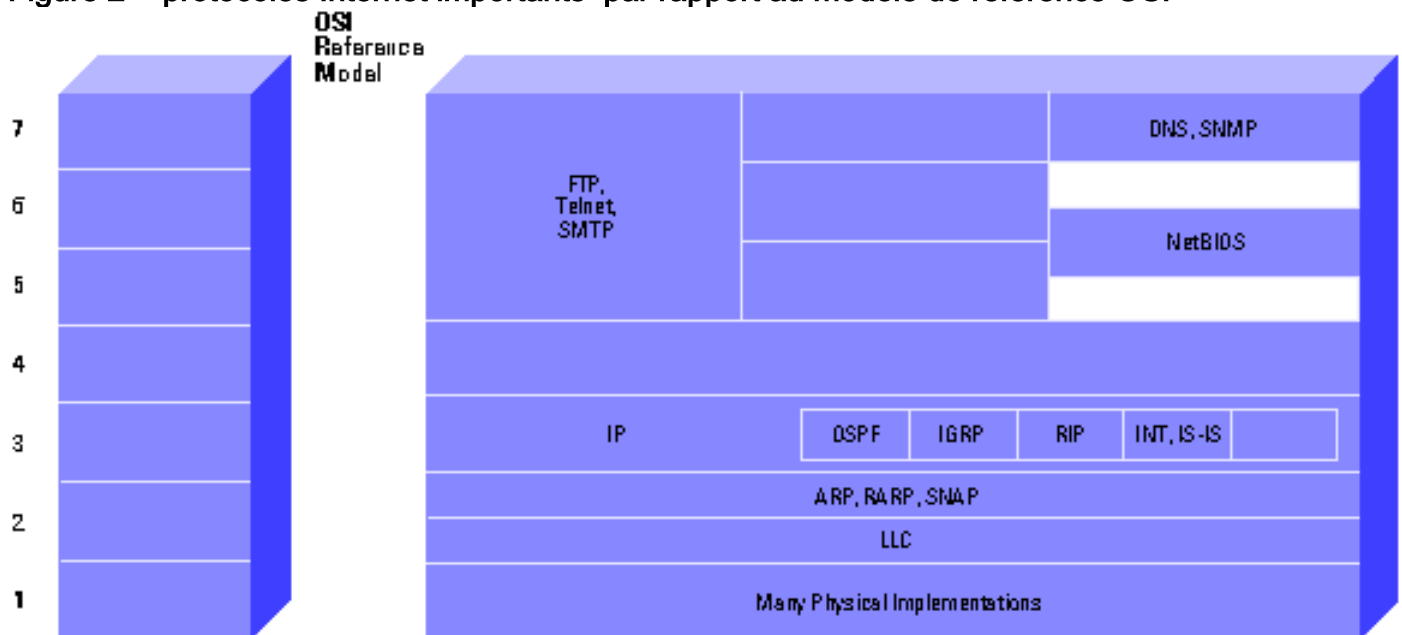


Figure 2 - protocoles Internet importants par rapport au modèle de référence OSI



Référez-vous à la section [TCP](#) des [protocoles Internet](#) pour plus d'informations.

## IP

IP est le protocole de couche 3 principal de la suite Internet. En plus du routage interréseau, IP fournit des rapports d'erreurs, la fragmentation et le réassemblage d'unités d'information appelées datagrammes pour la transmission sur des réseaux de tailles d'unités de données maximales différentes. IP représente le coeur de la suite de protocoles Internet.

**Remarque :** le terme IP de la section fait référence à IPv4, sauf indication contraire explicite.

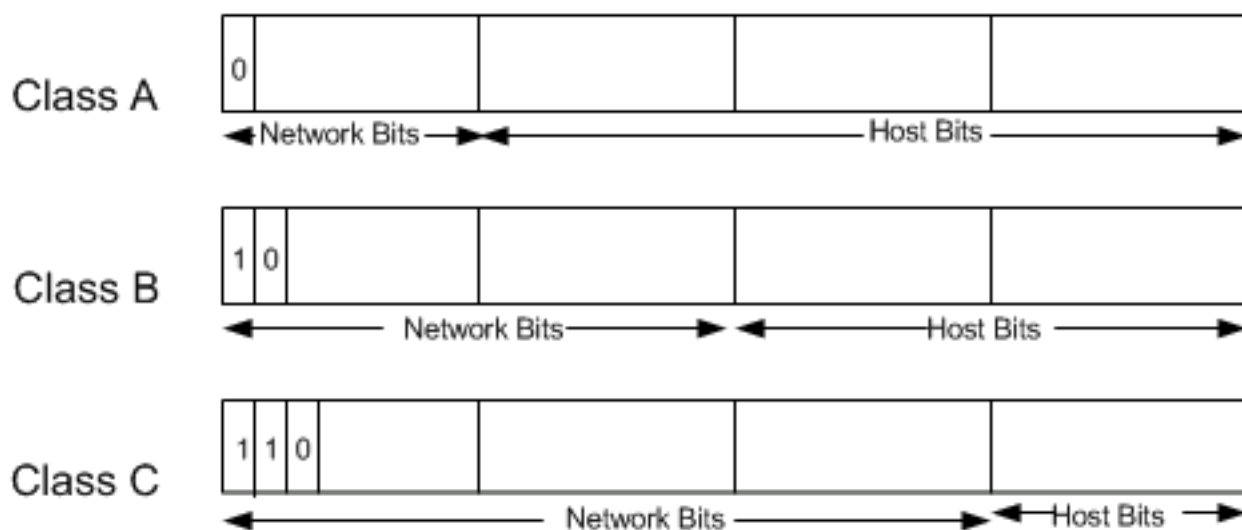
Les adresses IP sont des numéros 32 bits uniques au niveau mondial, attribués par le Centre d'informations réseau. Les adresses uniques à l'échelle mondiale permettent aux réseaux IP de

communiquer entre eux n'importe où dans le monde.

Une adresse IP est divisée en deux parties. La première partie désigne l'adresse réseau tandis que la seconde partie désigne l'adresse hôte.

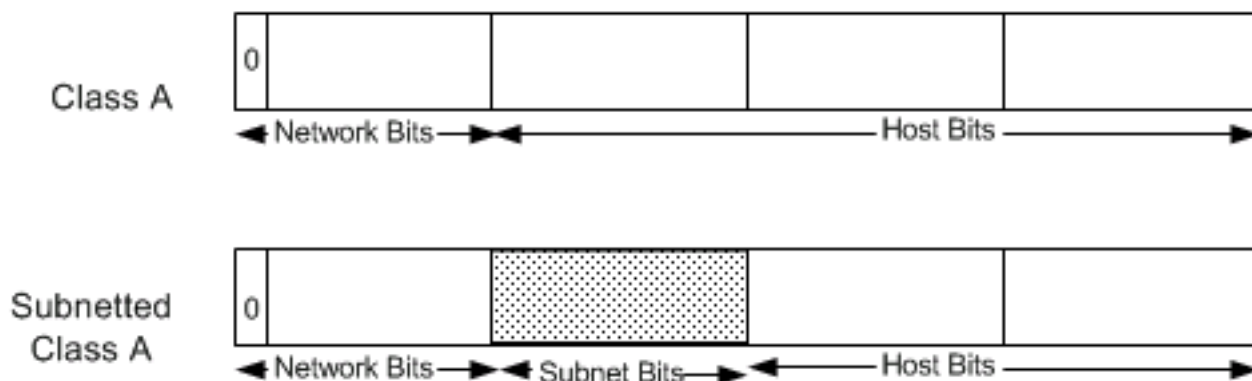
L'espace d'adressage IP est divisé en différentes classes de réseau. Les réseaux de classe A sont principalement destinés à être utilisés avec quelques très grands réseaux, car ils ne fournissent que 8 bits pour le champ d'adresse réseau. Les réseaux de classe B allouent 16 bits et les réseaux de classe C attribuent 24 bits pour le champ d'adresse réseau. Toutefois, les réseaux de classe C ne fournissent que 8 bits pour le champ d'hôte, de sorte que le nombre d'hôtes par réseau peut être un facteur limitatif. Dans les trois cas, le ou les bits les plus à gauche indiquent la classe de réseau. Les adresses IP sont écrites en notation décimale à point ; par exemple, 34.0.0.1. [La Figure 3](#) présente les formats d'adresse des réseaux IP de classe A, B et C.

**Figure 3 - Formats d'adresses pour les réseaux IP de classe A, B et C**



Les réseaux IP peuvent également être divisés en unités plus petites appelées sous-réseaux ou sous-réseaux. Les sous-réseaux offrent une flexibilité supplémentaire à l'administrateur réseau. Par exemple, supposons qu'une adresse de classe A a été attribuée à un réseau et que tous les noeuds du réseau utilisent une adresse de classe A. Supposez en outre que la représentation décimale à point de l'adresse de ce réseau est 34.0.0.0. (Tous les zéros du champ hôte d'une adresse spécifient l'ensemble du réseau.) L'administrateur peut subdiviser le réseau en sous-réseaux. Pour ce faire, vous empruntez des bits à la partie hôte de l'adresse et les utilisez comme champ de sous-réseau, comme illustré à la [Figure 4](#).

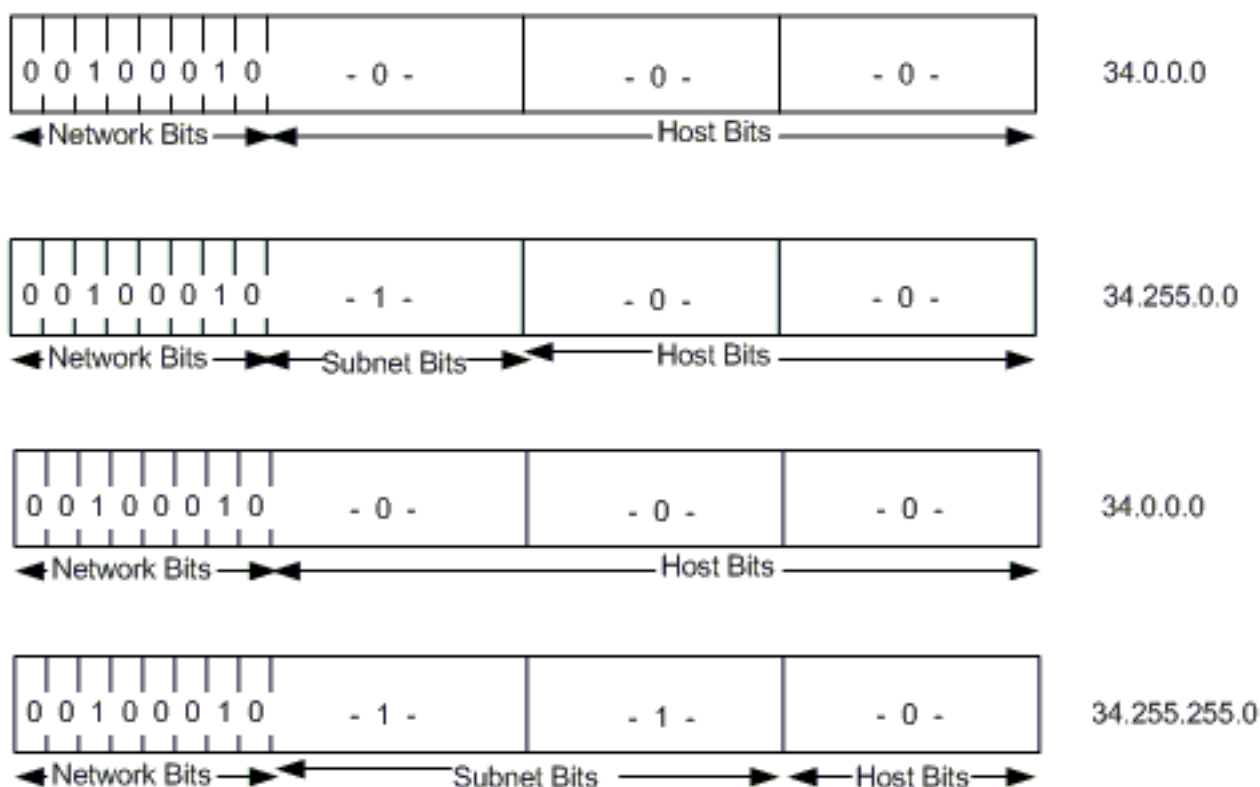
**Figure 4 - bits d'emprunt**



Si l'administrateur réseau a choisi d'utiliser 8 bits de découpage en sous-réseaux, le deuxième octet d'une adresse IP de classe A fournit le numéro de sous-réseau. Dans notre exemple, l'adresse 34.1.0.0 fait référence au réseau 34, sous-réseau 1 ; adresse 34.2.0.0 fait référence au réseau 34, au sous-réseau 2, etc.

Le nombre de bits pouvant être empruntés pour l'adresse de sous-réseau varie. Pour spécifier le nombre de bits utilisés pour représenter le réseau et la partie sous-réseau de l'adresse, IP fournit des masques de sous-réseau. Les masques de sous-réseau utilisent le même format et la même technique de représentation que les adresses IP. Les masques de sous-réseau ont des 1 dans tous les bits, à l'exception de ceux qui spécifient le champ d'hôte. Par exemple, le masque de sous-réseau qui spécifie 8 bits de découpage en sous-réseaux pour l'adresse de classe A 34.0.0.0 est 255.255.0.0. Le masque de sous-réseau qui spécifie 16 bits de découpage en sous-réseaux pour l'adresse de classe A 34.0.0.0 est 255.255.255.0. Ces deux masques de sous-réseau sont illustrés à la [Figure 5](#). Les masques de sous-réseau peuvent être transmis sur un réseau à la demande afin que les nouveaux noeuds puissent apprendre combien de bits de découpage en sous-réseaux sont utilisés sur leur réseau.

**Figure 5 - Masques de sous-réseau**



Traditionnellement, tous les sous-réseaux du même numéro de réseau utilisaient le même masque de sous-réseau. En d'autres termes, un administrateur réseau choisit un masque de huit bits pour tous les sous-réseaux du réseau. Cette stratégie est facile à gérer pour les administrateurs réseau et les protocoles de routage. Cependant, cette pratique gaspille de l'espace d'adressage dans certains réseaux. Certains sous-réseaux ont de nombreux hôtes et d'autres n'en ont que quelques-uns, mais ils consomment tous un numéro de sous-réseau. Les lignes série en sont l'exemple le plus extrême, car chacune ne comporte que deux hôtes pouvant être connectés via un sous-réseau de ligne série.

À mesure que les sous-réseaux IP se développent, les administrateurs cherchent des moyens d'utiliser leur espace d'adressage de manière plus efficace. Une des techniques qui en a résulté est appelée masques de sous-réseau de longueur variable (VLSM). Avec VLSM, un administrateur réseau peut utiliser un masque long sur les réseaux comportant peu d'hôtes et un

masque court sur les sous-réseaux comportant de nombreux hôtes. Cependant, cette technique est plus complexe que de ne les faire toutes de taille unique, et les adresses doivent être attribuées avec soin.

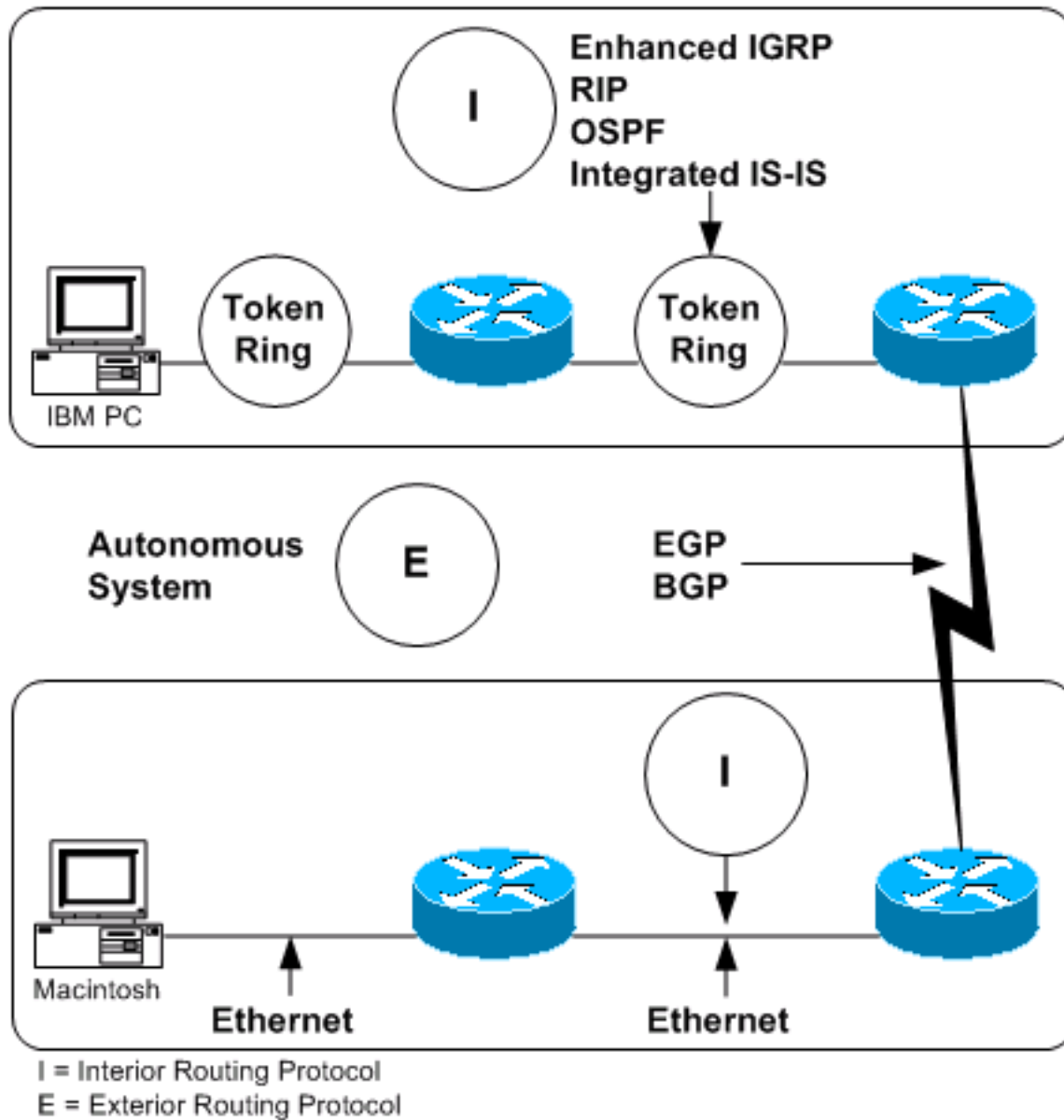
Bien sûr, pour utiliser VLSM, un administrateur réseau doit utiliser un protocole de routage qui le prend en charge. Les routeurs Cisco prennent en charge VLSM avec Open Shortest Path First (OSPF), Integrated Intermediate System to Intermediate System (Integrated IS-IS), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) et le routage statique. Référez-vous à [Adressage IP et création de sous-réseaux pour les nouveaux utilisateurs](#) pour plus d'informations sur l'adressage IP et la création de sous-réseaux.

Sur certains supports, tels que les réseaux locaux IEEE 802, les adresses IP sont découvertes dynamiquement à l'aide de deux autres membres de la suite de protocoles Internet : ARP (Address Resolution Protocol) et RARP (Reverse Address Resolution Protocol). Le protocole ARP utilise des messages de diffusion pour déterminer l'adresse matérielle (couche MAC) correspondant à une adresse de couche réseau particulière. Le protocole ARP est suffisamment générique pour permettre l'utilisation d'IP avec pratiquement n'importe quel type de mécanisme d'accès au support sous-jacent. Le protocole RARP utilise des messages de diffusion pour déterminer l'adresse de couche réseau associée à une adresse matérielle particulière. Le protocole RARP est particulièrement important pour les noeuds sans disque, pour lesquels les adresses de couche réseau sont généralement inconnues au moment du démarrage.

## [Routage dans les environnements IP](#)

Un « Internet » est un groupe de réseaux interconnectés. Internet, en revanche, est un ensemble de réseaux qui permettent la communication entre la plupart des institutions de recherche, des universités et de nombreuses autres organisations dans le monde. Les routeurs d'Internet sont organisés de manière hiérarchique. Certains routeurs sont utilisés pour déplacer des informations sur un groupe particulier de réseaux sous la même autorité administrative et le même contrôle. (Cette entité est appelée système autonome.) Les routeurs utilisés pour l'échange d'informations au sein de systèmes autonomes sont appelés routeurs intérieurs et utilisent divers protocoles IGP (Interior Gateway Protocol) pour atteindre cet objectif. Les routeurs qui déplacent des informations entre des systèmes autonomes sont appelés routeurs externes ; ils utilisent le protocole EGP (Exterior Gateway Protocol) ou le protocole BGP (Border Gateway Protocol). [La Figure 6](#) illustre l'architecture Internet.

### **Figure 6 - Représentation de l'architecture Internet**



Les protocoles de routage utilisés avec IP sont de nature dynamique. Le routage dynamique nécessite le logiciel des périphériques de routage pour calculer les routes. Les algorithmes de routage dynamique s'adaptent aux changements du réseau et sélectionnent automatiquement les meilleures routes. Contrairement au routage dynamique, le routage statique demande que les routes soient établies par l'administrateur réseau. Les routes statiques ne changent pas tant que l'administrateur réseau ne les modifie pas.

Les tables de routage IP se composent de paires adresse de destination/saut suivant. Cet exemple de table de routage d'un routeur Cisco montre que la première entrée est interprétée comme signifiant « pour accéder au réseau 34.1.0.0 (sous-réseau 1 sur le réseau 34), le prochain arrêt est le noeud à l'adresse 54.34.23.12 » :

```
R6-2500# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
```

```
34.0.0.0/16 is subnetted, 1 subnets
O 34.1.0.0 [110/65] via 54.34.23.12, 00:00:51, Serial0
   54.0.0.0/24 is subnetted, 1 subnets
C 54.34.23.0 is directly connected, Serial0
R6-2500#
```

Comme nous l'avons vu, le routage IP spécifie que les datagrammes IP traversent un interrèseau saut par saut. L'itinéraire complet n'est pas connu au début du voyage. Au lieu de cela, à chaque arrêt, le saut de routeur suivant est déterminé en faisant correspondre l'adresse de destination dans le datagramme avec une entrée dans la table de routage du noeud actuel. L'implication de chaque noeud dans le processus de routage consiste uniquement à transmettre des paquets en fonction des informations internes. Le protocole IP ne permet pas de signaler les erreurs à la source lorsque des anomalies de routage surviennent. Cette tâche est laissée à un autre protocole Internet le protocole ICMP (Internet Control Message Protocol).

Le protocole ICMP effectue un certain nombre de tâches au sein d'un interrèseau IP. En plus de la raison principale pour laquelle il a été créé (rapport des échecs de routage à la source), ICMP fournit une méthode pour tester l'accessibilité des noeuds sur un Internet (les messages d'écho et de réponse ICMP), une méthode pour augmenter l'efficacité du routage (le message de redirection ICMP), une méthode pour informer les sources qu'un datagramme a dépassé le temps alloué à exister dans un Internet (message ICMP Time Exceeded), et d'autres messages utiles. Dans l'ensemble, le protocole ICMP fait partie intégrante de toute mise en oeuvre IP, en particulier de celles qui s'exécutent sur les routeurs. Voir les [informations connexes](#)