

TCP/IP-Overzicht

Inhoud

[Inleiding](#)

[TCP/IP-technologie](#)

[TCP](#)

[IP](#)

[Routing in IP-omgevingen](#)

[Binnenlandse routingprotocollen](#)

[RIP](#)

[IGRP](#)

[EINDTIJD](#)

[OSPF](#)

[Geïntegreerd IS-IS](#)

[Buitenkant-routingprotocollen](#)

[EGP](#)

[BGP](#)

[Cisco TCP/IP-implementatie](#)

[Toegangsbeperkingen](#)

[Tunneling](#)

[IP-multicast](#)

[Netwerkinformatie onderdrukken](#)

[Administratieve afstand](#)

[Routing Protocol-herdistributie](#)

[Ondersteuning voor Serverless Network](#)

[Netwerkbewaking en -verwijdering](#)

[Samenvatting](#)

[Gerelateerde informatie](#)

[Inleiding](#)

In de twee decennia sinds hun uitvinding is de heterogeniteit van netwerken verder toegenomen met de implementatie van Ethernet, Token Ring, Fibre Distributed Data Interface (FDDI), X.25, Frame Relay, Switched Multimegabit Data Service (SMDS), Integrated Services Digital Network (ISDN) en onlangs, Asynchronous Transfer Mode (ATM). De Internet-protocollen zijn de best bewezen benadering van het internet van deze uiteenlopende reeks LAN- en WAN-technologieën.

De Internet Protocol-reeks omvat niet alleen lagere specificaties, zoals Transmission Control Protocol (TCP) en Internet Protocol (IP), maar specificaties voor dergelijke gemeenschappelijke toepassingen zoals elektronische post, eindemulatie en bestandsoverdracht. [Afbeelding 1](#) toont de TCP/IP-protocolreeks met betrekking tot het OSI-referentiemodel. [Afbeelding 2](#) toont een aantal belangrijke Internet-protocollen en hun relatie met het OSI-referentiemodel. Raadpleeg voor

informatie over het OSI-referentiemodel en de rol van elke laag de basisbeginselen van de internetworking-documentatie.

De Internet protocollen zijn de meest algemeen uitgevoerde multitivendor protocolreeks die vandaag in gebruik is. Ondersteuning voor ten minste een deel van de Internet Protocol-reeks is beschikbaar bij vrijwel elke computerverkoper.

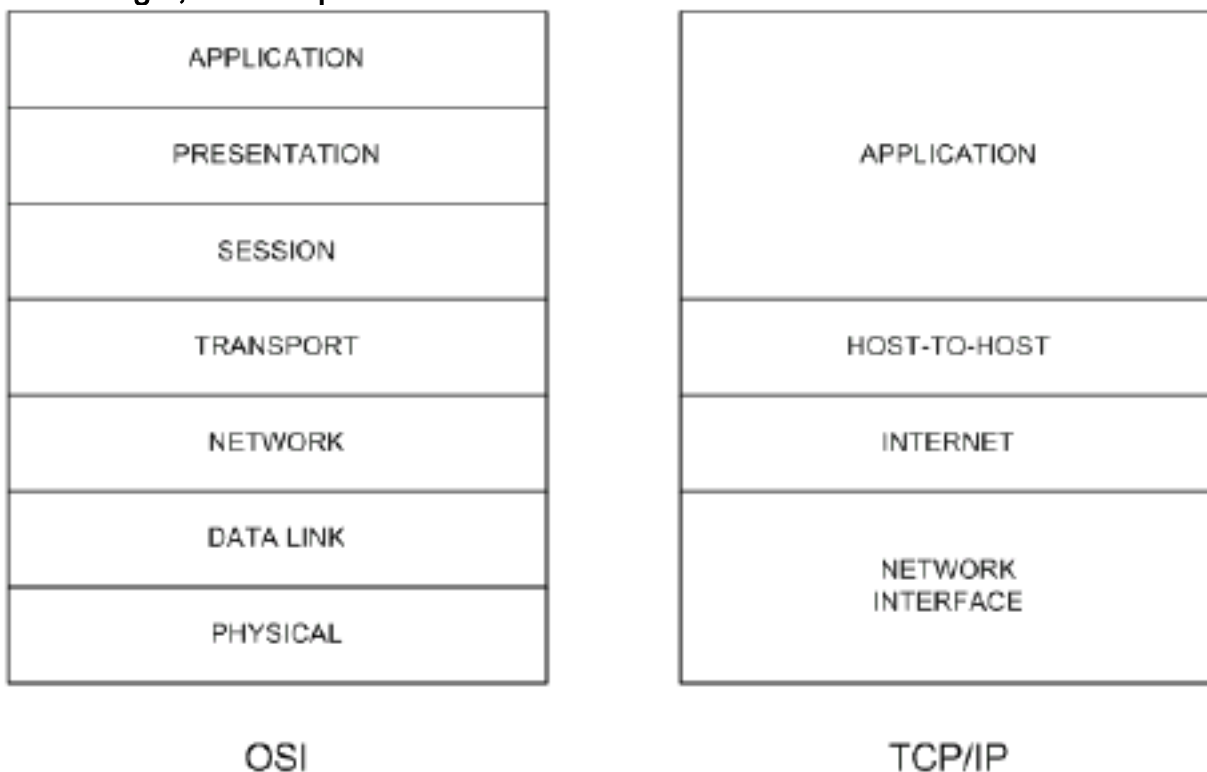
TCP/IP-technologie

In deze sectie worden de technische aspecten van TCP-, IP-, verwante protocollen en de omgevingen beschreven waarin deze protocollen werken. Omdat de primaire focus van dit document het routing (een Layer 3 functie) is, zal de discussie van TCP (een Layer 4 protocol) relatief kort zijn.

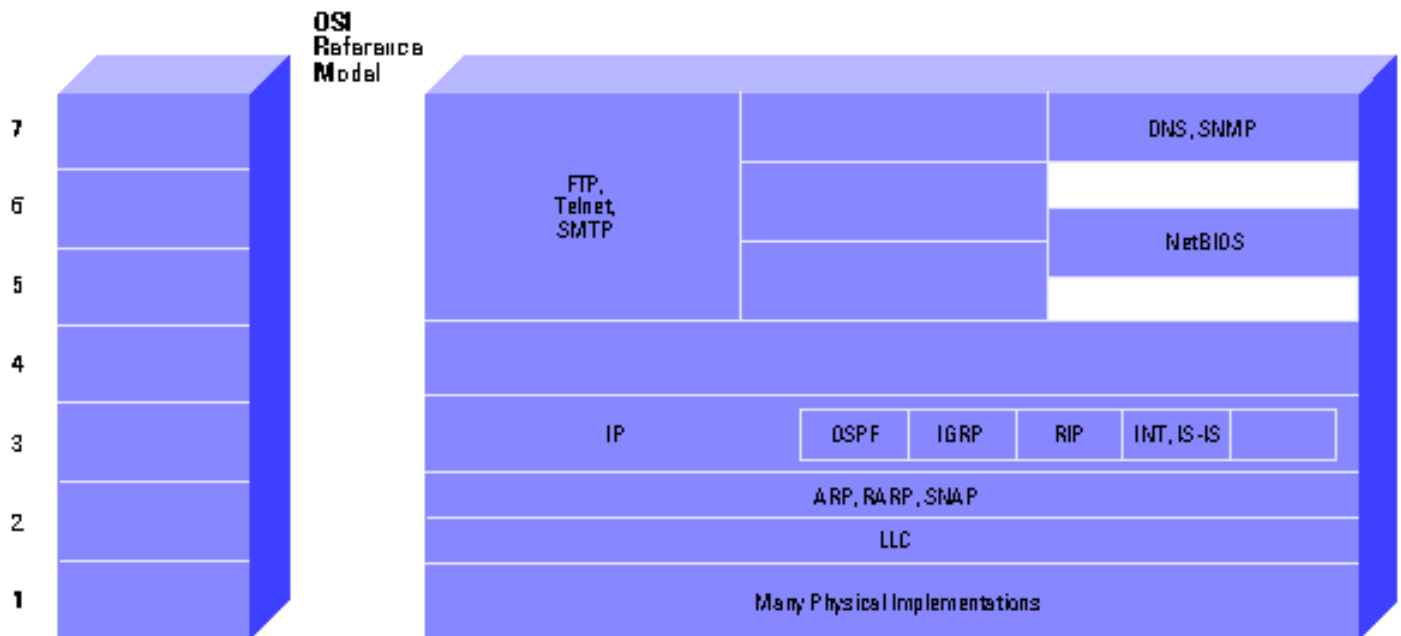
TCP

TCP is een op verbinding gericht transportprotocol dat gegevens als een niet-gestructureerde stroom bytes stuurt. Door sequentienummers en ontvangstberichten te gebruiken, kan TCP een verzendend knooppunt voorzien van leveringsinformatie over pakketten die naar een doelknooppunt worden verzonden. Waar gegevens verloren zijn gegaan in doorvoer van bron naar bestemming, kan TCP de gegevens opnieuw verzenden totdat een tijdelijke toestand is bereikt of totdat een succesvolle levering is bereikt. TCP kan ook dubbele berichten herkennen en zal deze op de juiste manier verwerpen. Als de verzendende computer te snel uitzendt voor de ontvangende computer, kan TCP stroomregelmechanismen gebruiken om gegevensoverdracht te vertragen. TCP kan ook leveringsinformatie naar de bovenlaagprotocollen en toepassingen communiceren die het ondersteunt. Al deze kenmerken maken TCP een end-to-end betrouwbaar transportprotocol. TCP wordt gespecificeerd in [RFC 793](#).

Afbeelding 1, TCP/IP-protocolreeks in relatie tot het OSI-referentiemodel



Afbeelding 2, belangrijke internetprotocollen in verband met het OSI-referentiemodel



Raadpleeg het [TCP](#)-gedeelte van [internetprotocollen](#) voor meer informatie.

IP

IP is het primaire Layer 3 protocol in de Internet suite. Naast routing tussen netwerken biedt IP, naast rapportage van fouten en fragmentatie en hermontage van informatie-eenheden met de naam datagrammen voor transmissie via netwerken met verschillende maximale gegevenseenheden. IP vormt het hart van de Internet Protocol-reeks.

Opmerking: de term IP in het hoofdstuk verwijst naar IPv4, tenzij anders expliciet vermeld.

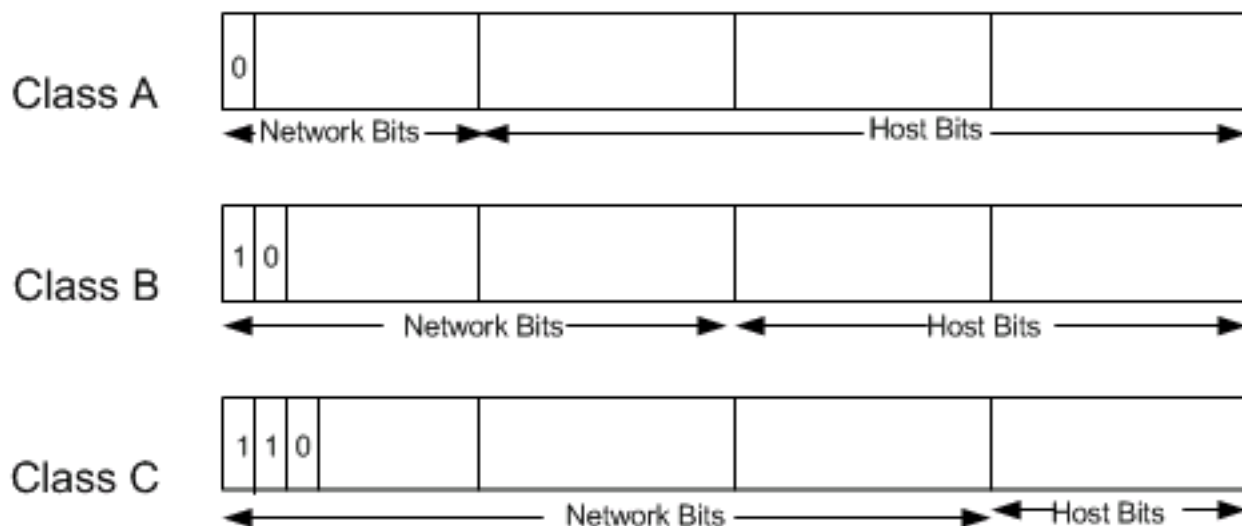
IP-adressen zijn wereldwijd uniek, 32-bits getallen toegewezen door het Network Information Center. Wereldwijd unieke adressen maken IP-netwerken overal in de wereld mogelijk om met elkaar te communiceren.

Een IP-adres is in twee delen verdeeld. Het eerste deel wijst het netwerkadres aan terwijl het tweede deel het host-adres aanwijst.

De IP-adresruimte is verdeeld in verschillende netwerkklassen. De netwerken van de klasse A zijn vooral bedoeld voor gebruik met een paar zeer grote netwerken, omdat zij slechts 8 bits voor het veld van het netwerkadres leveren. De netwerken van de klasse B wijzen 16 bits toe, en de netwerken van de Klasse C wijzen 24 bits voor het veld van het netwerkadres. De netwerken van klasse C verstrekken slechts 8 bits voor het gastveld, dus het aantal hosts per netwerk kan een beperkende factor zijn. In alle drie de gevallen geeft de meest linkse bit(s) de netwerkklasse aan. IP-adressen worden in decimale notatie met punten geschreven; Bijvoorbeeld, 34.0.0.1.

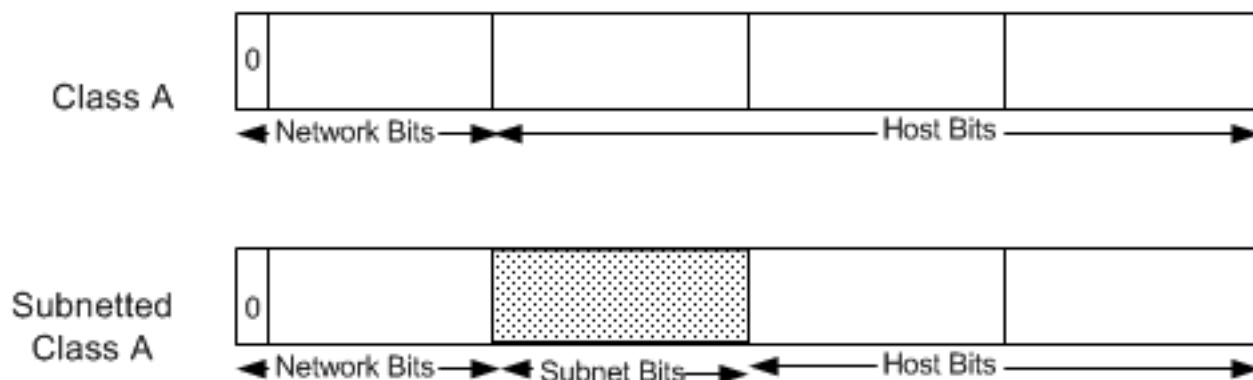
[Afbeelding 3](#) toont de adresformaten voor netwerken van klasse A, B, en C IP.

Afbeelding 3, adresformaten van klasse A, B en C IP-netwerken



IP-netwerken kunnen ook worden verdeeld in kleinere eenheden die subnetwerken of "subnetwerken" worden genoemd. Subnetten bieden extra flexibiliteit voor de netwerkbeheerder. Ga er bijvoorbeeld van uit dat een netwerk een Klasse A adres is toegewezen en alle knooppunten op het netwerk gebruiken een Klasse A adres. Ga er verder van uit dat de decimale weergave met punten van het adres van dit netwerk 34.0.0.0 is. (Alle nullen in het host veld van een adres geven het gehele netwerk aan.) De beheerder kan het netwerk onderverdelen onder subnetting. Dit wordt gedaan door "te lenen" bits van het host-gedeelte van het adres en het gebruik ervan als een subnetveld, zoals weergegeven in [afbeelding 4](#).

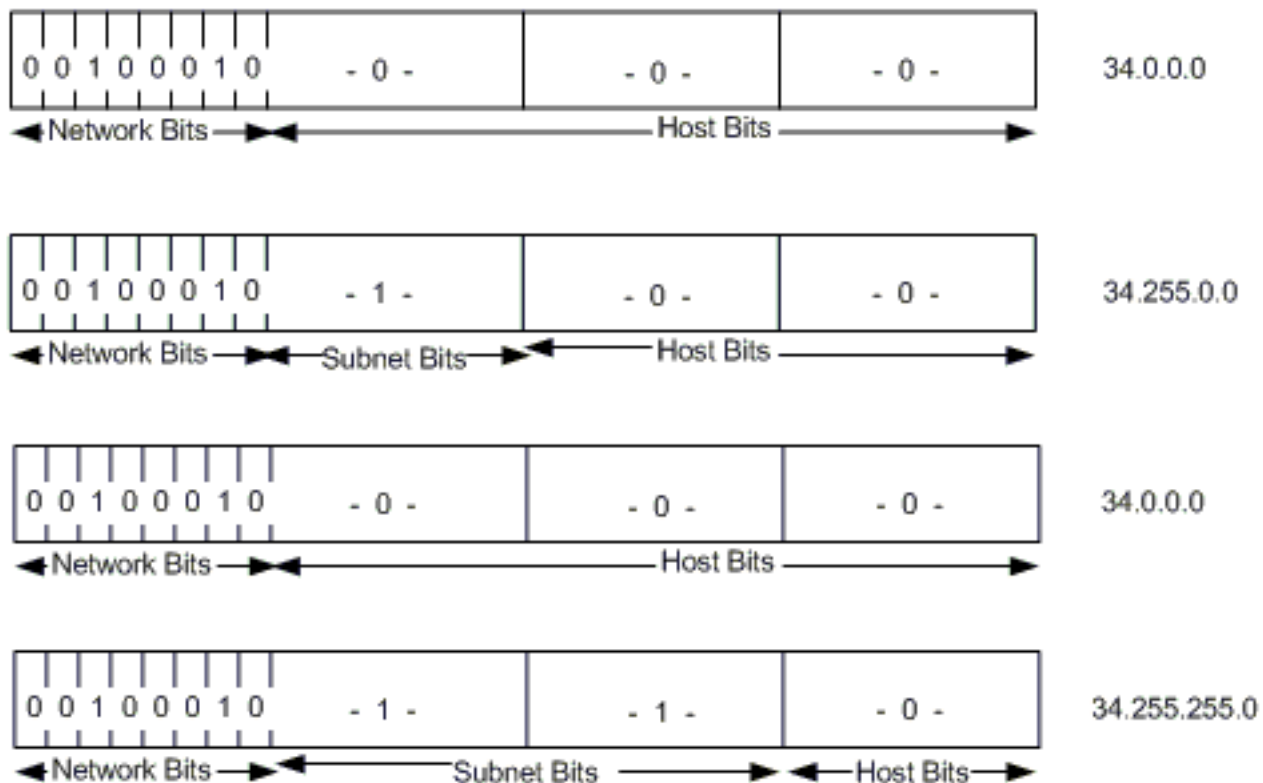
Afbeelding 4 β "Borrowing"-



Als de netwerkbeheerder heeft gekozen om 8 bits van subnetting te gebruiken, verstrekt het tweede octet van een Klasse A IP adres het Subnetnummer. In ons voorbeeld verwijst adres 34.1.0.0 naar netwerk 34, Subnet 1; adres 34.2.0.0 verwijst naar netwerk 34, Subnet 2, etc.

Het aantal bits dat voor het subnetadres kan worden geleend varieert. Om te specificeren hoeveel bits worden gebruikt om het netwerk en het netto gedeelte van het adres te vertegenwoordigen, verstrekt IP SUBNET masker. Subnetmaskers gebruiken de zelfde formaat en representatietechniek als IP adressen. Subnet maskers hebben in alle bits behalve die welke het host veld specificeren. Bijvoorbeeld, het SUBNET masker dat 8 bits van subnetting voor Klasse A adres 34.0.0.0 is 255.255.0.0 specificceert. Het SUBNET masker dat 16 bits van subnetting voor Klasse A adres 34.0.0.0 is 255.255.255.0. Beide van deze maskers zijn [Afbeelding 5](#). Subnetmaskers kunnen op bestelling door een netwerk worden doorgegeven zodat nieuwe knooppunten kunnen leren hoeveel bits van subnetting op hun netwerk worden gebruikt.

Afbeelding 5 subnetmaskers



Traditioneel, gebruikten alle subnetten van het zelfde netwerkaantal het zelfde SUBNET masker. Met andere woorden, een netwerkmanager zou een achtbits masker voor alle subnetten in het netwerk kiezen. Deze strategie is makkelijk te beheren voor zowel netwerkbeheerders als routingprotocollen. In deze praktijk wordt echter de ruimte in bepaalde netwerken beperkt. Sommige subnetten hebben veel hosts en sommige hebben slechts een paar, maar elk verbruikt een volledig subnummer. Seriéle lijnen zijn het meest extreme voorbeeld, omdat elk slechts twee hosts heeft die via een seriële lijneubnet kunnen worden aangesloten.

Aangezien IP subnetten zijn gegroeid, hebben de beheerders manieren gezocht om hun adresruimte efficiënter te gebruiken. Een van de resulterende technieken wordt variabele Lengte Subnet maskers (VLSM) genoemd. Met VLSM kan een netwerkbeheerder een lang masker op netwerken met weinig gastheren en een kort masker op subnetten met vele gastheren gebruiken. Deze techniek is echter complexer dan het maken ervan tot één formaat, en adressen moeten zorgvuldig worden toegewezen.

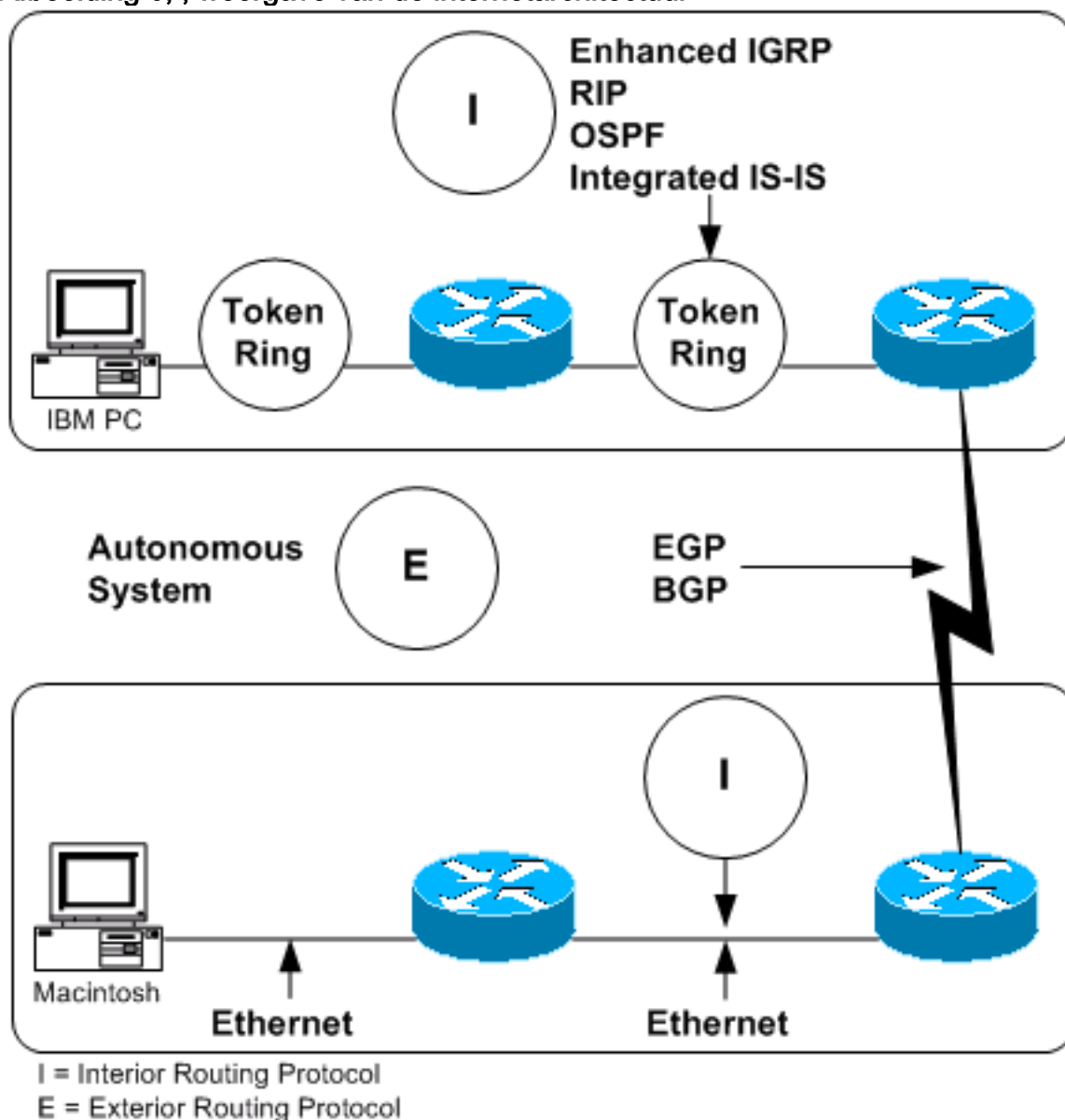
Natuurlijk moet een netwerkbeheerder om VLSM te gebruiken een routeringsprotocol gebruiken dat het ondersteunt. Cisco-routers ondersteunen VLSM met Open Shortest Path First (OSPF), Geïntegreerd Intermediate System to Intermediate System (Integrated IS-IS), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) en statische routing. Raadpleeg [IP-adressering en -subnetting voor nieuwe gebruikers](#) voor meer informatie over IP-adressering en -subnetting.

Op sommige media, zoals IEEE 802 LAN's, worden IP-adressen dynamisch ontdekt door het gebruik van twee andere leden van de Internet-protocolreeks: Address Resolutie Protocol (ARP) en Reverse Address Resolutie Protocol (RARP). ARP gebruikt uitgezonden berichten om het hardware (MAC-laag) adres te bepalen dat overeenkomt met een bepaald netwerklaagadres. ARP is voldoende generiek om het gebruik van IP met vrijwel elk type onderliggend media-toegangsmechanisme mogelijk te maken. RARP gebruikt uitzending berichten om het netwerklaag adres te bepalen verbonden aan een bepaald hardwareadres. RARP is in het bijzonder belangrijk voor onklankbare knooppunten, waarvoor de netwerklaagadressen gewoonlijk onbekend zijn bij de laars.

Routing in IP-omgevingen

Een "internet" is een groep onderling verbonden netwerken. Het internet daarentegen is de verzameling netwerken die de communicatie tussen de meeste onderzoeksinstellingen, universiteiten en veel andere organisaties in de hele wereld mogelijk maakt. De routers binnen het internet worden hiërarchisch georganiseerd. Sommige routers worden gebruikt om informatie door één bepaalde groep netwerken te verplaatsen onder dezelfde administratieve autoriteit en controle. (Een dergelijke entiteit wordt een autonoom systeem genoemd.) De routers die worden gebruikt voor informatie-uitwisseling binnen autonome systemen worden interieurrouters genoemd, en zij gebruiken een verscheidenheid aan binnenlandse gateways (IGP's) om dit doel te bereiken. Routers die informatie tussen autonome systemen verplaatsen, worden buitenrouters genoemd; zij gebruiken het Exterior Gateway Protocol (EGP) of Border Gateway Protocol (BGP). [Afbeelding 6](#) toont de internetarchitectuur.

Afbeelding 6, , weergave van de internetarchitectuur



Routing protocols die gebruikt worden met IP zijn dynamisch in aard. Dynamische routing vereist de software in de routingapparaten om routes te berekenen. Dynamische routingalgoritmen passen aan veranderingen in het netwerk aan en selecteren automatisch de beste routes. In tegenstelling tot dynamische routing, roept het statische routeren naar routes om door de netwerkbeheerder te worden ingesteld. Statische routes veranderen niet totdat de

netwerkbeheerder ze wijzigt.

IP-routingtabellen bestaan uit doeladres/volgende hoppers. Deze steekproef die tabel routeert van een router van Cisco toont dat de eerste ingang als betekenis "om aan netwerk 34.1.0.0 te krijgen (netto 1 op netwerk 34) wordt geïnterpreteerd, is het volgende eind het knooppunt op adres 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#
```

Zoals we hebben gezien, specificeert IP routing dat IP-datagrammen door een internetwork één router-hop tegelijk reizen. De gehele route is aan het begin van de reis niet bekend. In plaats daarvan, bij elk stop, wordt de volgende router hop bepaald door het doeladres binnen het datagram aan te passen met een ingang in de routingtabel van het huidige knooppunt. De betrokkenheid van elk knooppunt in het routingproces bestaat alleen uit het verzenden van pakketten die zijn gebaseerd op interne informatie. IP voorziet niet in de teruggave van fouten aan de bron wanneer zich routeringsanomalieën voordoen. Deze taak wordt overgelaten aan een ander Internet-protocol het Internet Control Message Protocol (ICMP).

ICMP voert een aantal taken uit binnen een IP internetwork. Naast de belangrijkste reden waarom het is gecreëerd (het melden van routingfouten aan de bron), biedt ICMP een methode om de bereikbaarheid van knooppunten via het internet te testen (de ICMP-Echo- en antwoordberichten), een methode om de routingefficiëntie te vergroten (het ICMP-bericht van herleiding), een methode om bronnen te informeren dat een datagram de toegewezen tijd om binnen een internet te bestaan (het ICMP-bericht van meer) heeft overschreden, en andere nuttige berichten. In totaal is ICMP een integraal deel van om het even welke IP implementatie, vooral die in routers. Zie de [verwante informatie](#)