TCP/IP - Übersicht

Inhalt

Einführung

In den zwei Jahrzehnten seit ihrer Erfindung hat sich die Heterogenität von Netzwerken mit der Bereitstellung von Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), X.25, Frame Relay, Switched Multimegabit Data Service (SMDS), Integrated Services Digital Network (ISDN) und zuletzt Asynchronous Transfer Mode (ATM) weiter vergrößert. Die Internetprotokolle sind der bewährteste Ansatz für das Internet dieser vielfältigen LAN- und WAN-Technologien.

Die Internet Protocol-Suite umfasst nicht nur Spezifikationen der unteren Ebene wie Transmission Control Protocol (TCP) und Internet Protocol (IP), sondern auch Spezifikationen für gängige Anwendungen wie E-Mail, Terminal-Emulation und Dateiübertragung. Abbildung 1 zeigt die TCP/IP-Protokoll-Suite in Bezug auf das OSI-Referenzmodell. Abbildung 2 zeigt einige der wichtigen Internetprotokolle und ihre Beziehung zum OSI-Referenzmodell. Weitere Informationen

zum OSI-Referenzmodell und zur Rolle jeder Ebene finden Sie im Dokument Internetworking Basics (Internetworking-Grundlagen).

Die Internetprotokolle sind die am häufigsten implementierte Protokoll-Suite mit mehreren Anbietern, die heute verwendet wird. Die Unterstützung für mindestens einen Teil der Internet Protocol-Suite ist von praktisch jedem Computeranbieter erhältlich.

TCP/IP-Technologie

In diesem Abschnitt werden technische Aspekte von TCP, IP, verwandten Protokollen und den Umgebungen beschrieben, in denen diese Protokolle ausgeführt werden. Da der Schwerpunkt dieses Dokuments auf Routing (eine Layer-3-Funktion) liegt, wird die Diskussion über TCP (ein Layer-4-Protokoll) relativ kurz gehalten.

TCP

TCP ist ein verbindungsorientiertes Transportprotokoll, das Daten als unstrukturierten Bytestrom sendet. Durch Verwendung von Sequenznummern und Bestätigungsnachrichten kann TCP einen sendenden Knoten mit Bereitstellungsinformationen für Pakete bereitstellen, die an einen Zielknoten übertragen werden. Wenn bei der Übertragung von der Quelle zum Ziel Daten verloren gegangen sind, kann TCP die Daten erneut übertragen, bis entweder eine Timeout-Bedingung erreicht ist oder bis eine erfolgreiche Bereitstellung erreicht ist. TCP kann auch doppelte Nachrichten erkennen und diese entsprechend verwerfen. Wenn der sendende Computer zu schnell für den empfangenden Computer überträgt, kann TCP Datenübertragungssteuerungsmechanismen verwenden, um die Datenübertragung zu verlangsamen. TCP kann darüber hinaus Bereitstellungsinformationen an die von ihm unterstützten Protokolle und Anwendungen der oberen Schicht weiterleiten. All diese Eigenschaften machen TCP zu einem zuverlässigen End-to-End-Transportprotokoll. TCP wird in RFC 793 angegeben.

Abbildung 1: der TCP/IP-Protokoll-Suite im Zusammenhang mit dem OSI-Referenzmodell

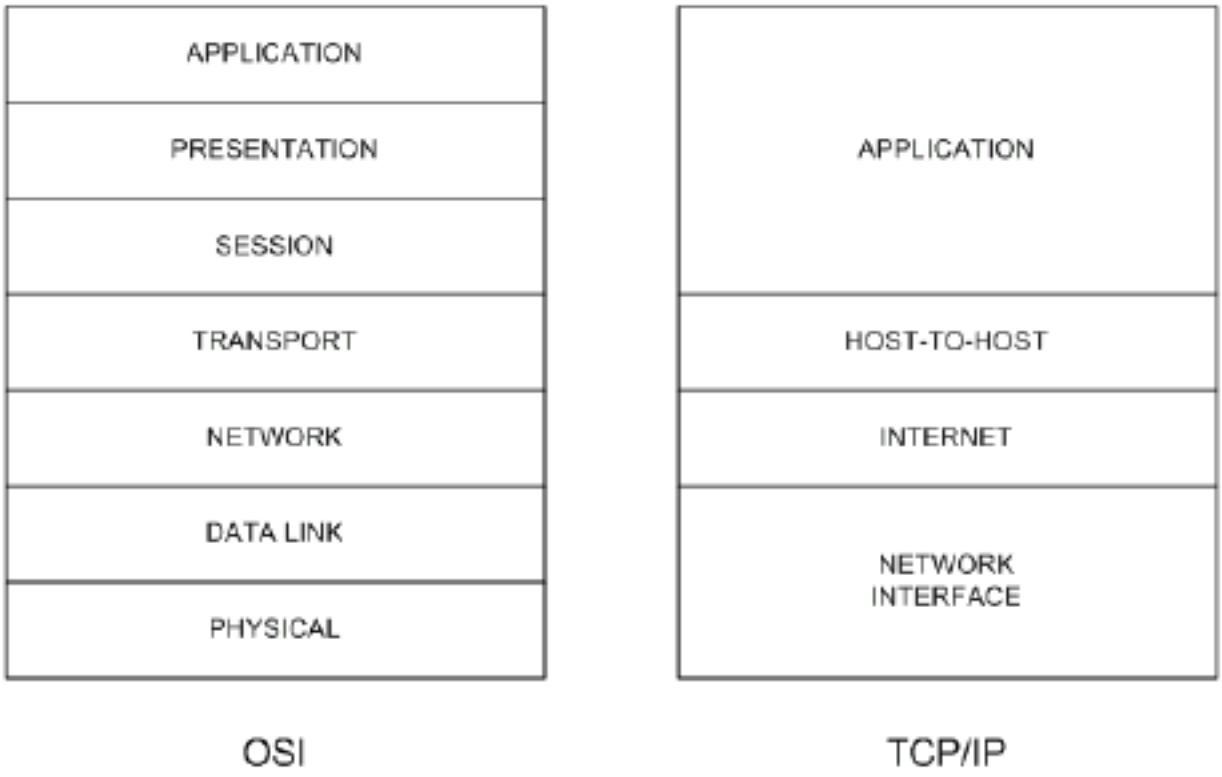
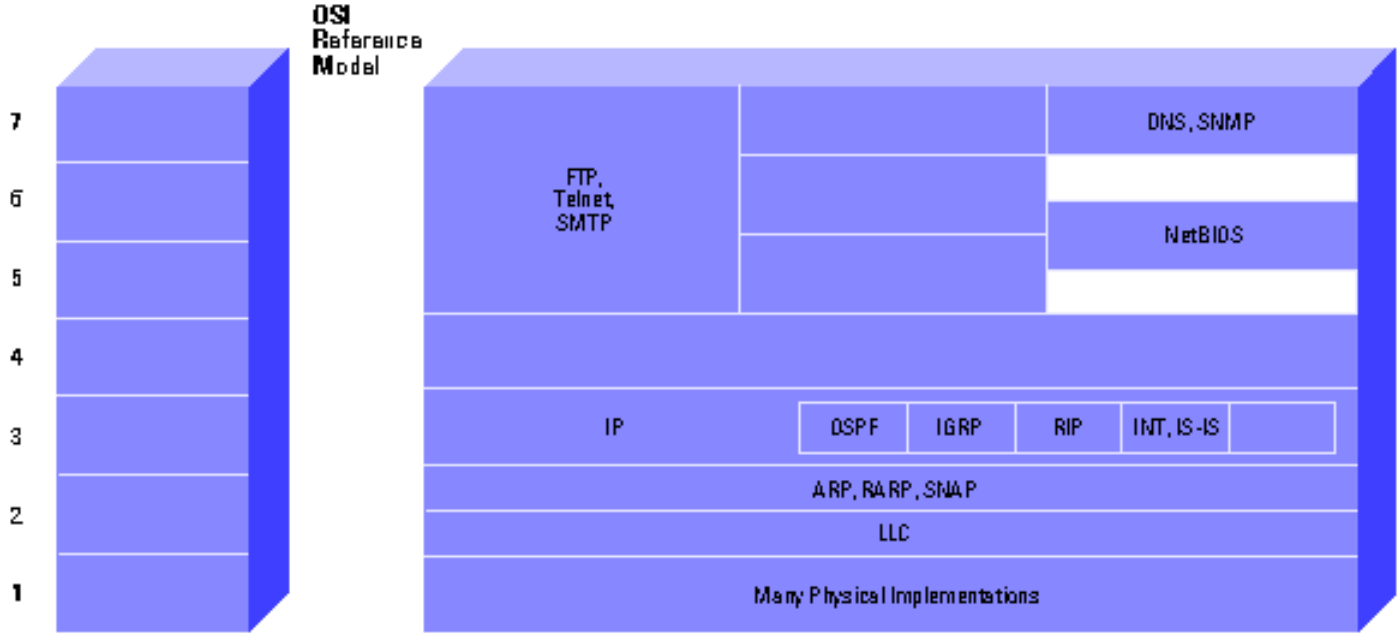


Abbildung 2: Wichtige Internetprotokolle im Zusammenhang mit dem OSI-Referenzmodell



Weitere Informationen finden Sie im TCP-Abschnitt der Internetprotokolle.

IP

IP ist das primäre Layer-3-Protokoll in der Internet-Suite. Zusätzlich zum Internetwork Routing bietet IP Fehlerberichte, Fragmentierung und Reassemblierung von Informationseinheiten, so genannten Datagrammen, für die Übertragung über Netzwerke mit unterschiedlichen maximalen Datenstückgrößen. IP stellt das Herzstück der Internet Protocol-Suite dar.

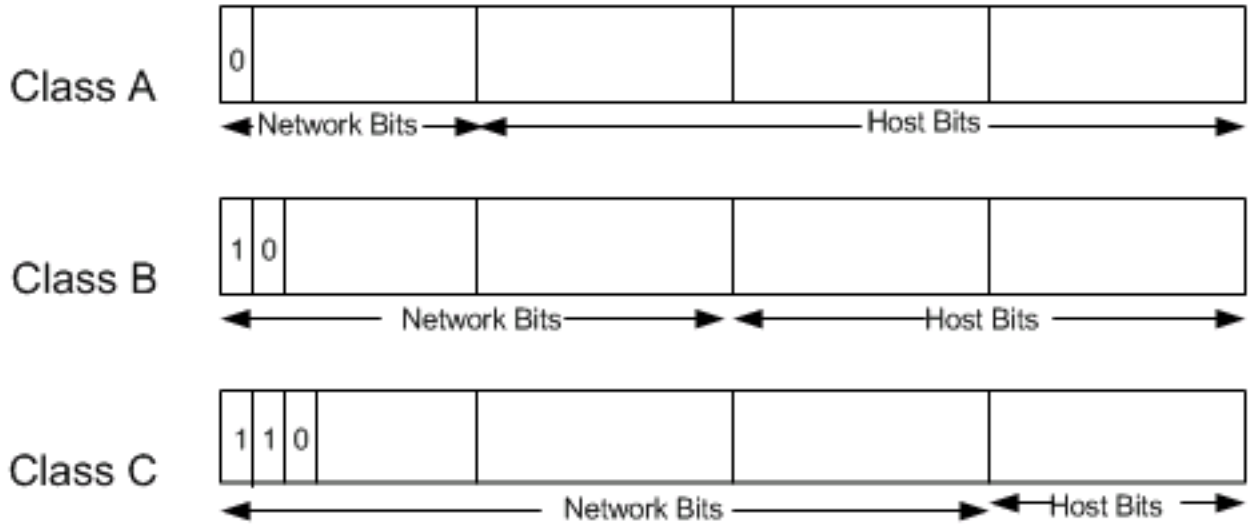
Hinweis: Der Begriff IP im Abschnitt bezieht sich auf IPv4, sofern nicht ausdrücklich anders angegeben.

IP-Adressen sind global eindeutige, vom Network Information Center zugewiesene 32-Bit-Nummern. Globale eindeutige Adressen ermöglichen die Kommunikation zwischen IP-Netzwerken an jedem beliebigen Ort der Welt.

Eine IP-Adresse ist in zwei Teile unterteilt. Der erste Teil gibt die Netzwerkadresse an, der zweite Teil die Hostadresse.

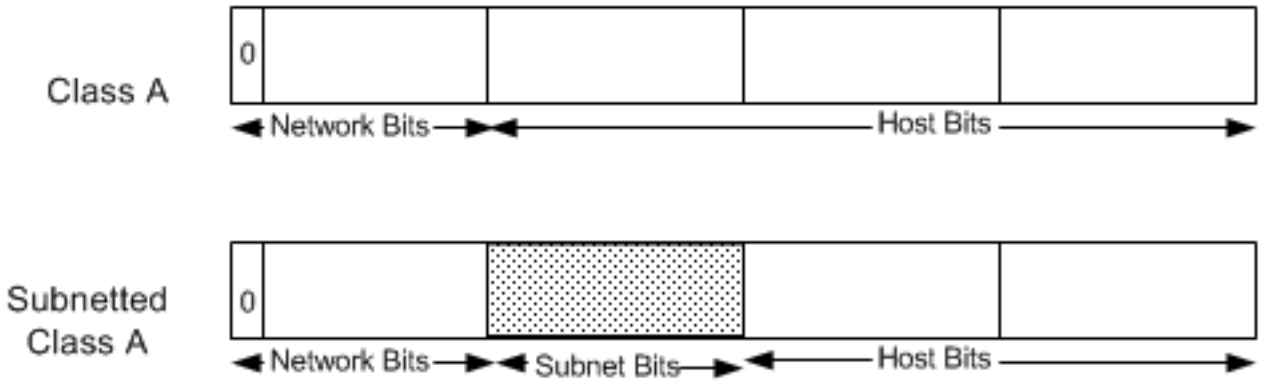
Der IP-Adressbereich ist in verschiedene Netzwerkklassen unterteilt. Klasse-A-Netzwerke sind hauptsächlich für die Verwendung mit einigen sehr großen Netzwerken vorgesehen, da sie nur 8 Bit für das Netzwerkadressfeld bereitstellen. Klasse-B-Netzwerke weisen 16 Bit zu, Klasse-C-Netzwerke 24 Bit für das Netzwerkadressfeld. Klasse-C-Netzwerke stellen jedoch nur 8 Bit für das Hostfeld bereit, sodass die Anzahl der Hosts pro Netzwerk ein begrenzender Faktor sein kann. In allen drei Fällen geben die meisten Bit-Links die Netzwerkklasse an. IP-Adressen werden im Dezimalpunktformat geschrieben. beispielsweise 34.0.0.1. Abbildung 3 zeigt die Adressformate für IP-Netzwerke der Klassen A, B und C.

Abbildung 3: -Adressformate für IP-Netzwerke der Klassen A, B und C



IP-Netzwerke können auch in kleinere Einheiten, so genannte Subnetze oder "Subnetze", unterteilt werden. Subnetze bieten dem Netzwerkadministrator mehr Flexibilität. Angenommen, einem Netzwerk wurde eine Klasse-A-Adresse zugewiesen, und alle Knoten im Netzwerk verwenden eine Klasse-A-Adresse. Weiterhin wird davon ausgegangen, dass die gepunktete Dezimaldarstellung der Netzwerkadresse 34.0.0.0 lautet. (Alle Nullen im Hostfeld einer Adresse geben das gesamte Netzwerk an.) Der Administrator kann das Netzwerk mithilfe der Subnetzfunktion unterteilen. Hierzu werden Bits vom Hostteil der Adresse "ausgeliehen" und als Subnetzfeld verwendet, wie in Abbildung 4 dargestellt.

Abbildung 4 - - "Borrowing Bits"

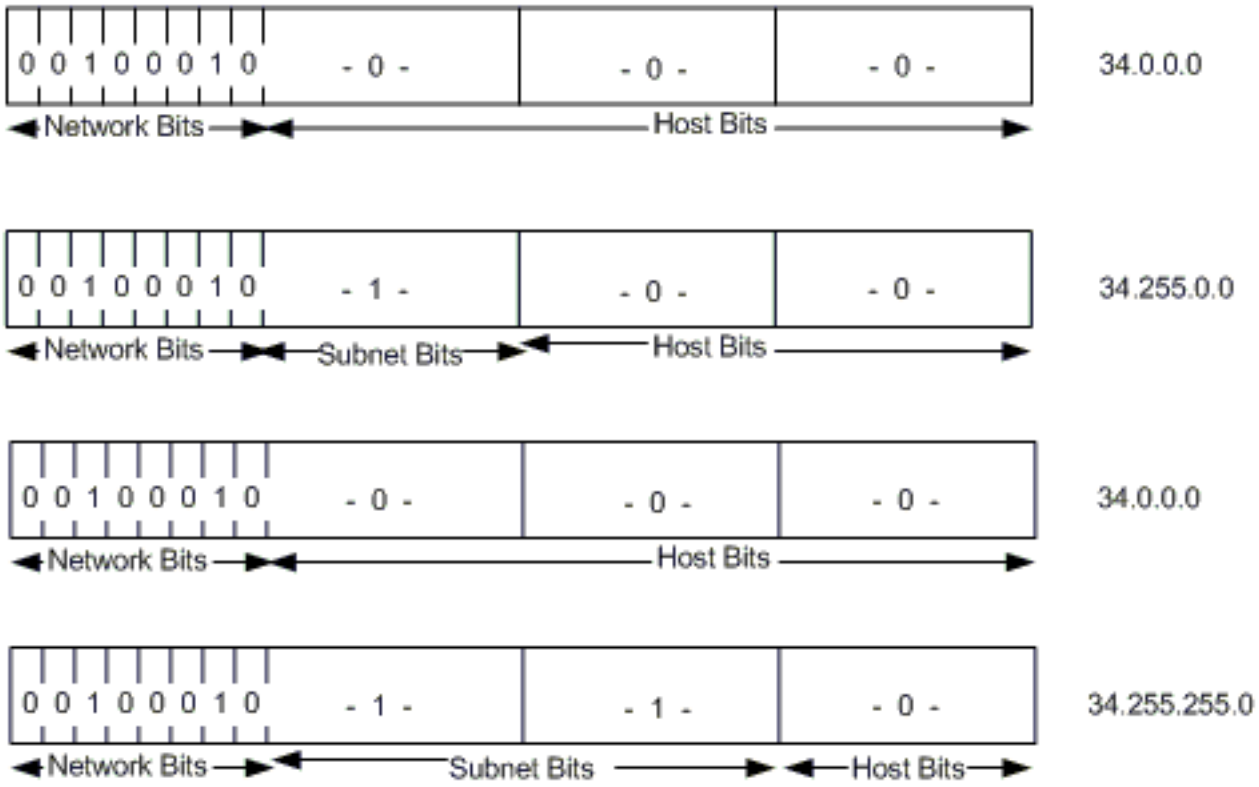


Wenn der Netzwerkadministrator die Verwendung von 8 Bit Subnetz gewählt hat, stellt das zweite Oktett einer IP-Adresse der Klasse A die Subnetznummer bereit. In unserem Beispiel bezieht sich Adresse 34.1.0.0 auf Netzwerk 34, Subnetz 1. address 34.2.0.0 bezieht sich auf Netzwerk 34, Subnetz 2 usw.

Die Anzahl der Bits, die für die Subnetzadresse ausgeliehen werden können, variiert. Um festzulegen, wie viele Bit zur Darstellung des Netzwerks und des Subnetzteils der Adresse verwendet werden, stellt IP Subnetzmasken bereit. Subnetzmasken verwenden das gleiche Format und die gleiche Darstellungstechnik wie IP-Adressen. Subnetzmasken haben eine in allen Bits, mit Ausnahme derjenigen, die das Hostfeld angeben. Beispielsweise ist die Subnetzmaske, die 8 Bit Subnetting für die Adresse der Klasse A 34.0.0.0 angibt, 255.255.0.0. Die Subnetzmaske, die 16 Bit Subnetting für die Adresse der Klasse A 34.0.0.0 angibt, ist 255.255.0. Beide Subnetzmasken sind in Abbildung 5 dargestellt. Subnetzmasken können bei Bedarf über ein Netzwerk weitergeleitet werden, sodass neue Knoten lernen können, wie viele Bits von

Subnetzwerken in ihrem Netzwerk verwendet werden.

Abbildung 5: Subnetzmasken



Bisher verwendeten alle Subnetze derselben Netzwerknummer dieselbe Subnetzmaske. Mit anderen Worten, ein Netzwerkmanager würde eine Acht-Bit-Maske für alle Subnetze im Netzwerk auswählen. Diese Strategie ist sowohl für Netzwerkadministratoren als auch für Routing-Protokolle einfach zu verwalten. Bei dieser Vorgehensweise wird jedoch Adressraum in einigen Netzwerken verschwendet. Einige Subnetze haben viele Hosts und einige nur wenige, aber jedes verwendet eine ganze Subnetznummer. Serielle Leitungen sind das extremste Beispiel, da jeder nur über zwei Hosts verfügt, die über ein Subnetz mit serieller Leitung verbunden werden können.

Im Zuge der Zunahme von IP-Subnetzen haben Administratoren nach Wegen gesucht, um ihren Adressraum effizienter zu nutzen. Eine der daraus resultierenden Techniken sind Subnetzmasken mit variabler Länge (VLSM). Mit VLSM kann ein Netzwerkadministrator in Netzwerken mit wenigen Hosts eine lange Maske und in Subnetzen mit vielen Hosts eine kurze Maske verwenden. Dieses Verfahren ist jedoch komplexer als das Erstellen aller Adressen in einer Größe, und Adressen müssen sorgfältig zugewiesen werden.

Natürlich muss ein Netzwerkadministrator zur Verwendung von VLSM ein Routing-Protokoll verwenden, das dieses unterstützt. Cisco Router unterstützen VLSM mit Open Shortest Path First (OSPF), Integrated Intermediate System to Intermediate System (Integrated IS-IS), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) und statischem Routing. Unter IP-Adressierung und Subnetting für neue Benutzer finden Sie weitere Informationen zur IP-Adressierung und Subnettierung.

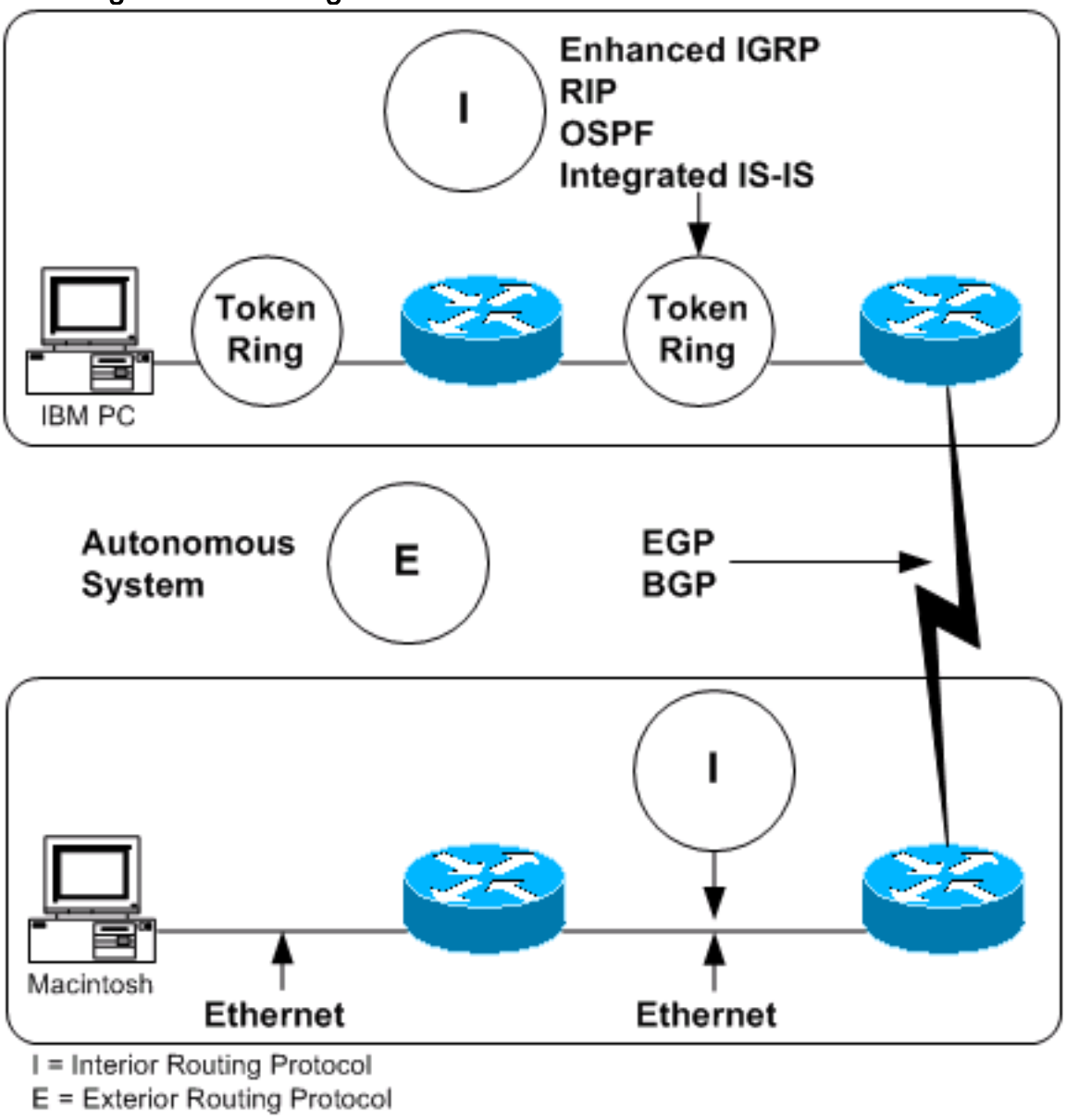
Auf einigen Medien, z. B. IEEE 802-LANs, werden IP-Adressen dynamisch mithilfe von zwei anderen Mitgliedern der Internet Protocol Suite erkannt: Address Resolution Protocol (ARP) und Reverse Address Resolution Protocol (RARP). ARP verwendet Broadcast-Nachrichten, um die Hardwareadresse (MAC-Layer) zu bestimmen, die einer bestimmten Netzwerkschichtadresse entspricht. ARP ist ausreichend allgemein gehalten, um die Verwendung von IP mit praktisch jedem zugrunde liegenden Medienzugriffsmechanismus zu ermöglichen. RARP verwendet

Broadcast-Nachrichten, um die mit einer bestimmten Hardwareadresse verknüpfte Netzwerkschichtadresse zu ermitteln. RARP ist besonders wichtig für diskless-Knoten, für die Netzwerkschichtadressen zum Zeitpunkt des Bootvorgangs normalerweise unbekannt sind.

Routing in IP-Umgebungen

Ein "Internet" ist eine Gruppe miteinander verbundener Netzwerke. Das Internet andererseits ist eine Sammlung von Netzwerken, die die Kommunikation zwischen den meisten Forschungsinstituten, Universitäten und vielen anderen Organisationen auf der ganzen Welt ermöglicht. Router im Internet sind hierarchisch organisiert. Einige Router werden verwendet, um Informationen unter der gleichen Verwaltungsbehörde und Kontrolle über eine bestimmte Gruppe von Netzwerken zu übertragen. (Eine solche Einheit wird als autonomes System bezeichnet.) Router, die für den Informationsaustausch innerhalb autonomer Systeme verwendet werden, werden als Intern-Router bezeichnet. Zu diesem Zweck verwenden sie eine Reihe von Interior Gateway Protocols (IGPs). Router, die Informationen zwischen autonomen Systemen übertragen, werden als externe Router bezeichnet. sie verwenden das Exterior Gateway Protocol (EGP) oder BGP (Border Gateway Protocol). Abbildung 6 zeigt die Internetarchitektur.

Abbildung 6 - Darstellung der Internetarchitektur



Mit IP verwendete Routing-Protokolle sind dynamisch. Für dynamisches Routing muss die

Software in den Routing-Geräten Routen berechnen. Dynamische Routing-Algorithmen passen sich an Veränderungen im Netzwerk an und wählen automatisch die besten Routen aus. Im Gegensatz zu dynamischem Routing fordert statisches Routing, dass Routen vom Netzwerkadministrator eingerichtet werden. Statische Routen ändern sich erst, wenn der Netzwerkadministrator sie ändert.

IP-Routing-Tabellen bestehen aus Zieladresse/Next-Hop-Paaren. Diese Beispiel-Routing-Tabelle von einem Cisco Router zeigt, dass der erste Eintrag als "to get to network 34.1.0.0 (Subnetz 1 in Netzwerk 34), the next stop is the node at address 54.34.23.12" interpretiert wird:

```
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#
```

Wie wir gesehen haben, gibt IP-Routing an, dass IP-Datagramme jeweils einen Router-Hop über ein Internetwork durchlaufen. Die gesamte Route ist zu Beginn der Reise nicht bekannt. Stattdessen wird an jeder Haltestelle der nächste Router-Hop bestimmt, indem die Zieladresse im Datagramm mit einem Eintrag in der Routing-Tabelle des aktuellen Knotens abgeglichen wird. Die Beteiligung jedes Knotens am Routing-Prozess besteht lediglich aus der Weiterleitung von Paketen, die auf internen Informationen basieren. IP bietet keine Fehlerberichte an die Quelle, wenn Routing-Anomalien auftreten. Diese Aufgabe wird einem anderen Internetprotokoll überlassen dem Internet Control Message Protocol (ICMP) .

ICMP führt eine Reihe von Aufgaben in einem IP-Internetwork aus. Neben dem Hauptgrund, für den sie erstellt wurde (Meldung von Routing-Fehlern an die Quelle) bietet ICMP eine Methode zum Testen der Node-Erreichbarkeit über das Internet (ICMP-Echo und Reply-Meldungen), eine Methode zur Steigerung der Routing-Effizienz (ICMP Redirect-Nachricht), eine Methode, um Quellen zu informieren, dass ein Datagram seine zugewiesene Zeit in einem Internet überschritten hat (ICMP Time Exceeded Message), und andere hilfreiche Nachrichten. Alles in allem ist ICMP ein integraler Bestandteil jeder IP-Implementierung, insbesondere derjenigen, die in Routern ausgeführt werden. Weitere Informationen