

TCP/IP 개요

목차

[소개](#)

[TCP/IP 기술](#)

[TCP](#)

[IP](#)

[IP 환경에서 라우팅](#)

[내부 라우팅 프로토콜](#)

[RIP](#)

[IGRP](#)

[EIGRP](#)

[OSPF](#)

[통합 IS-IS](#)

[외부 라우팅 프로토콜](#)

[EGP](#)

[BGP](#)

[Cisco의 TCP/IP 구현](#)

[액세스 제한](#)

[터널링](#)

[IP 멀티캐스트](#)

[네트워크 정보 억제](#)

[관리 거리](#)

[라우팅 프로토콜 재배포](#)

[서버를 사용하지 않는 네트워크 지원](#)

[네트워크 모니터링 및 디버깅](#)

[요약](#)

[관련 정보](#)

소개

이러한 네트워크가 발명된 이후 20년 동안 이더넷, 토큰 링, FDDI(Fiber Distributed Data Interface), X.25, Frame Relay, SMDS(Switched Multabit Data Service), ISDN(Integrated Services Digital Network) 및 가장 최근에 ATM(Asynchronous Transfer Mode)을 구축하여 다양한 네트워크 환경을 더욱 확장했습니다. 인터넷 프로토콜은 이와 같이 다양한 LAN 및 WAN 기술을 상호 연결하는 가장 검증된 접근 방식입니다.

인터넷 프로토콜 제품군에는 TCP(Transmission Control Protocol) 및 IP(Internet Protocol)와 같은 하위 수준의 사양뿐 아니라 전자 메일, 터미널 에뮬레이션, 파일 전송과 같은 일반적인 애플리케이션에 대한 사양도 포함됩니다. [그림 1](#)은 OSI 참조 모델과 관련된 TCP/IP 프로토콜 제품군을 보여줍니다. [그림 2](#)는 중요한 인터넷 프로토콜 및 OSI 참조 모델과의 관계를 보여줍니다. OSI 참조 모델 및 각 레이어의 역할에 대한 자세한 내용은 Internetworking Basics 문서를 참조하십시오.

인터넷 프로토콜은 현재 가장 널리 구현된 멀티벤더 프로토콜 제품군입니다. 거의 모든 컴퓨터 공급 업체에서 Internet Protocol 제품군 중 적어도 일부를 지원합니다.

TCP/IP 기술

이 섹션에서는 TCP, IP, 관련 프로토콜 및 이러한 프로토콜이 작동하는 환경의 기술적 측면에 대해 설명합니다. 이 문서의 주요 초점은 라우팅(레이어 3 기능)이므로 TCP(레이어 4 프로토콜)에 대한 논의는 비교적 간략합니다.

TCP

TCP는 데이터를 비구조화된 바이트 스트림으로 전송하는 연결 지향 전송 프로토콜입니다. 시퀀스 번호 및 승인 메시지를 사용하여 TCP는 대상 노드로 전송된 패킷에 대한 전달 정보를 전송 노드에 제공할 수 있습니다. 소스에서 대상으로의 전송 중에 데이터가 손실된 경우 TCP는 시간 제한 조건에 도달하거나 성공적으로 전달될 때까지 데이터를 재전송할 수 있습니다. 또한 TCP는 중복 메시지를 인식할 수 있으며 적절하게 폐기합니다. 전송 컴퓨터가 수신 컴퓨터에 너무 빨리 전송되면 TCP는 흐름 제어 메커니즘을 사용하여 데이터 전송을 느리게 할 수 있습니다. TCP는 전달 정보를 지원하는 상위 계층 프로토콜 및 애플리케이션에 전달할 수도 있습니다. 이러한 모든 특성을 통해 TCP는 엔드 투 엔드 신뢰성 있는 전송 프로토콜이 됩니다. TCP는 [RFC 793](#)에 지정됩니다.

그림 1 OSI 참조 모델과 관련된 TCP/IP 프로토콜 제품군

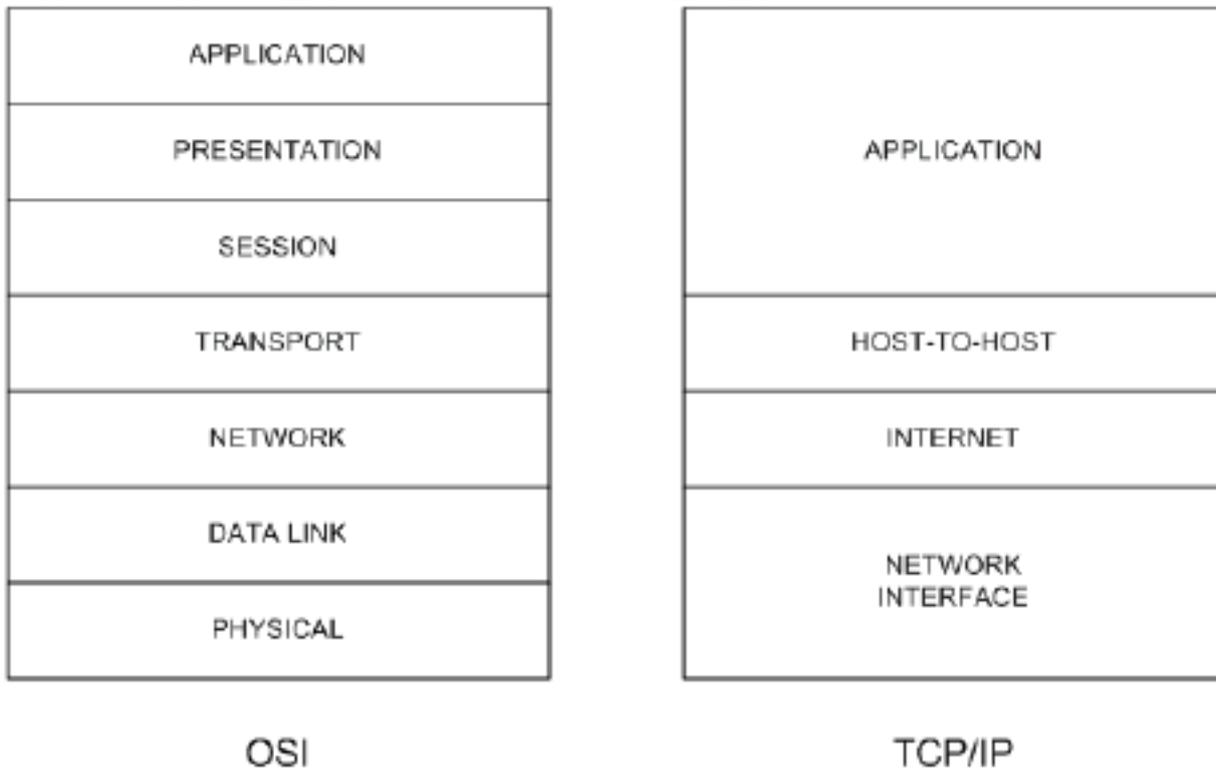
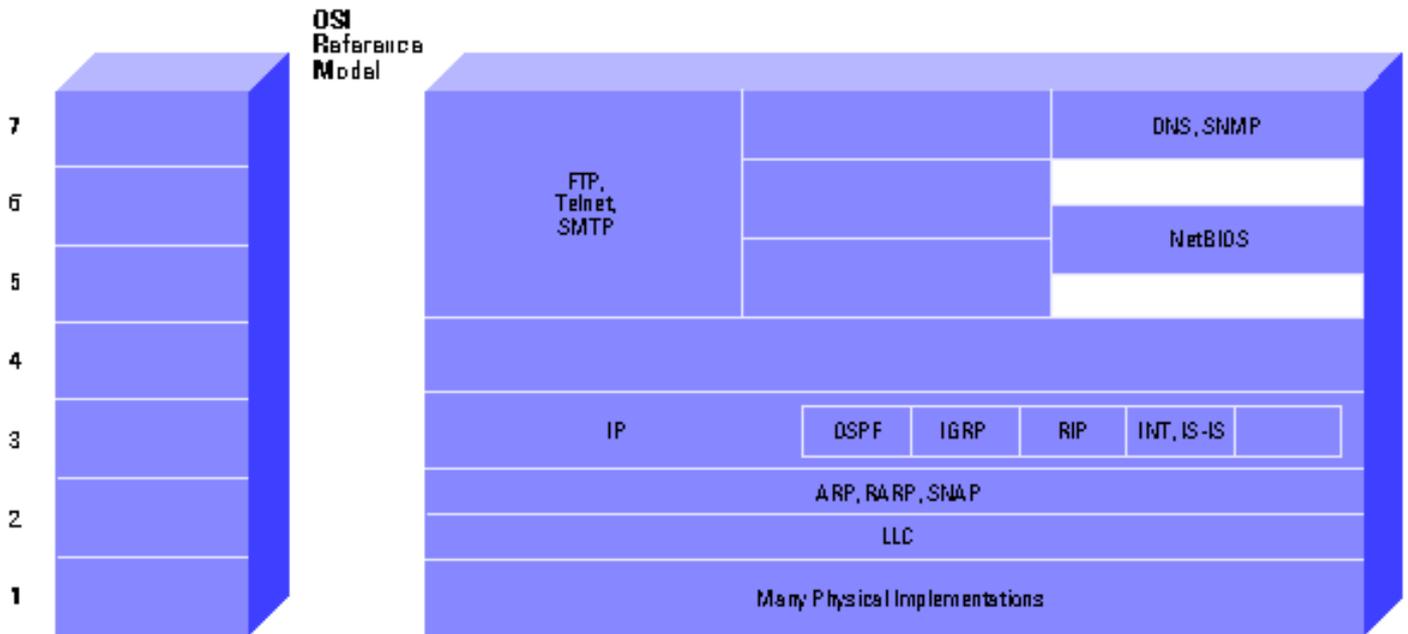


그림 2 OSI 참조 모델과 관련하여 중요한 인터넷 프로토콜



자세한 내용은 [인터넷 프로토콜의 TCP](#) 섹션을 참조하십시오.

IP

IP는 인터넷 제품군의 기본 레이어 3 프로토콜입니다. IP는 네트워크 간 라우팅 외에도 최대 데이터 단위 크기가 다른 네트워크를 통해 전송하기 위해 데이터그램이라는 정보 단위의 오류 보고 및 프래그먼트화 및 리어셈블리를 제공합니다. IP는 Internet Protocol 제품군의 핵심입니다.

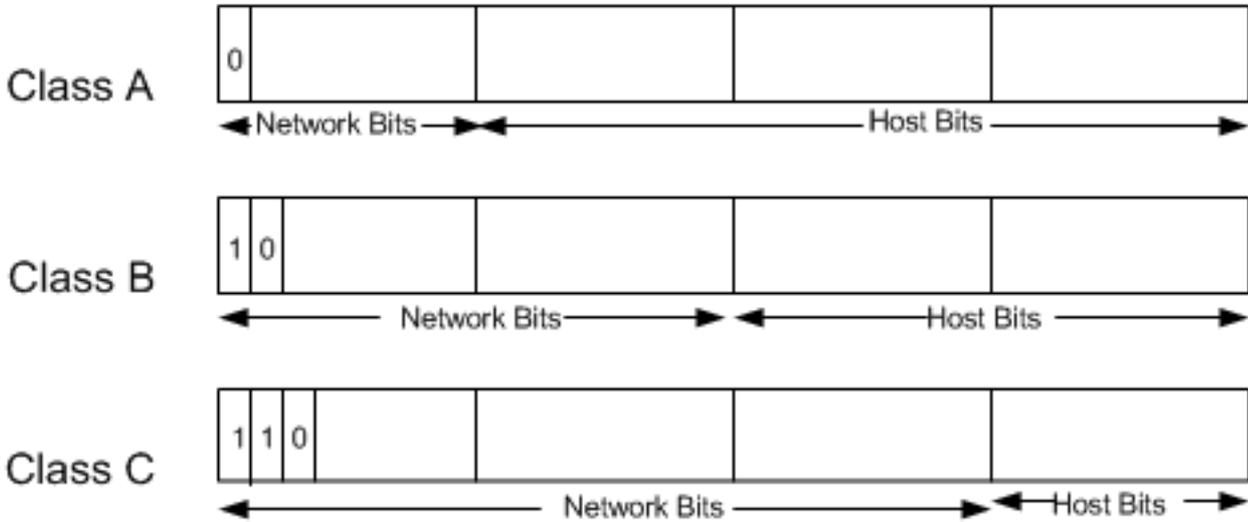
참고: 이 섹션의 IP라는 용어는 명시적으로 명시되지 않는 한 IPv4를 참조합니다.

IP 주소는 Network Information Center에서 할당된 32비트 숫자로서 전체적으로 고유합니다. 전역적으로 고유한 주소를 사용하면 전 세계 어디서나 IP 네트워크가 서로 통신할 수 있습니다.

IP 주소는 두 부분으로 구분됩니다. 첫 번째 부분은 네트워크 주소를, 두 번째 부분은 호스트 주소를 지정합니다.

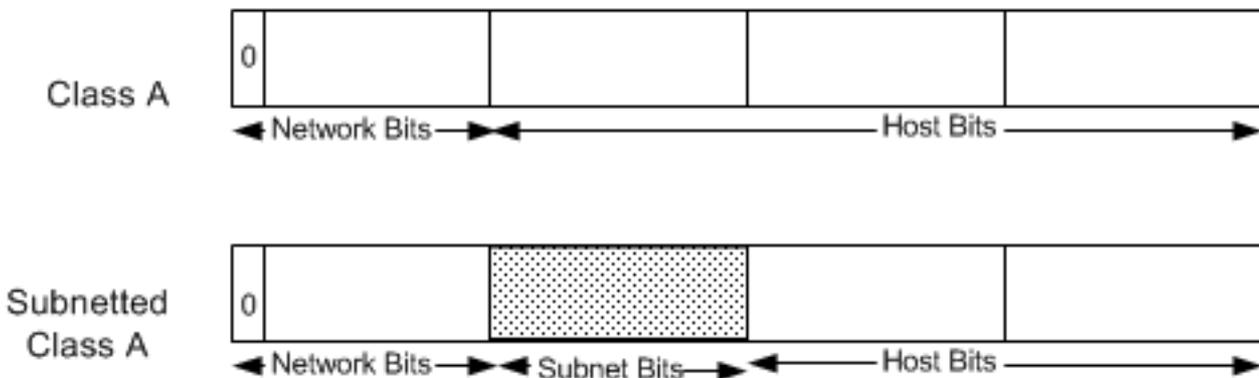
IP 주소 공간은 서로 다른 네트워크 클래스로 구분됩니다. 클래스 A 네트워크는 주로 네트워크 주소 필드에 8비트만 제공되므로 몇 개의 매우 큰 네트워크에서 사용할 수 있습니다. 클래스 B 네트워크는 16비트를 할당하고 클래스 C 네트워크는 네트워크 주소 필드에 24비트를 할당합니다. 그러나 클래스 C 네트워크는 호스트 필드에 8비트만 제공하므로 네트워크당 호스트 수가 제한 요소가 될 수 있습니다. 세 가지 경우 모두, 가장 왼쪽에 있는 비트는 네트워크 클래스를 나타냅니다. IP 주소는 점으로 구분된 십진수 형식으로 작성됩니다. 예를 들어 34.0.0.1. [그림 3](#)은 클래스 A, B 및 C IP 네트워크의 주소 형식을 보여줍니다.

그림 3 클래스 A, B 및 C IP 네트워크의 주소 형식



또한 IP 네트워크는 하위 네트워크 또는 "서브넷"이라는 작은 단위로 나눌 수 있습니다. 서브넷은 네트워크 관리자에게 추가적인 유연성을 제공합니다. 예를 들어, 네트워크에 클래스 A 주소가 할당되었고 네트워크의 모든 노드에서 클래스 A 주소를 사용한다고 가정합니다. 또한 이 네트워크 주소의 점으로 구분된 십진수 표현이 34.0.0.0이라고 가정합니다. 주소의 호스트 필드에 있는 모든 0은 전체 네트워크를 지정합니다. 관리자는 서브넷을 사용하여 네트워크를 세분화할 수 있습니다. 이 작업은 [그림 4](#)에 나와 있는 것처럼 주소의 호스트 부분에서 "차입" 비트를 서브넷 필드로 사용하여 수행됩니다.

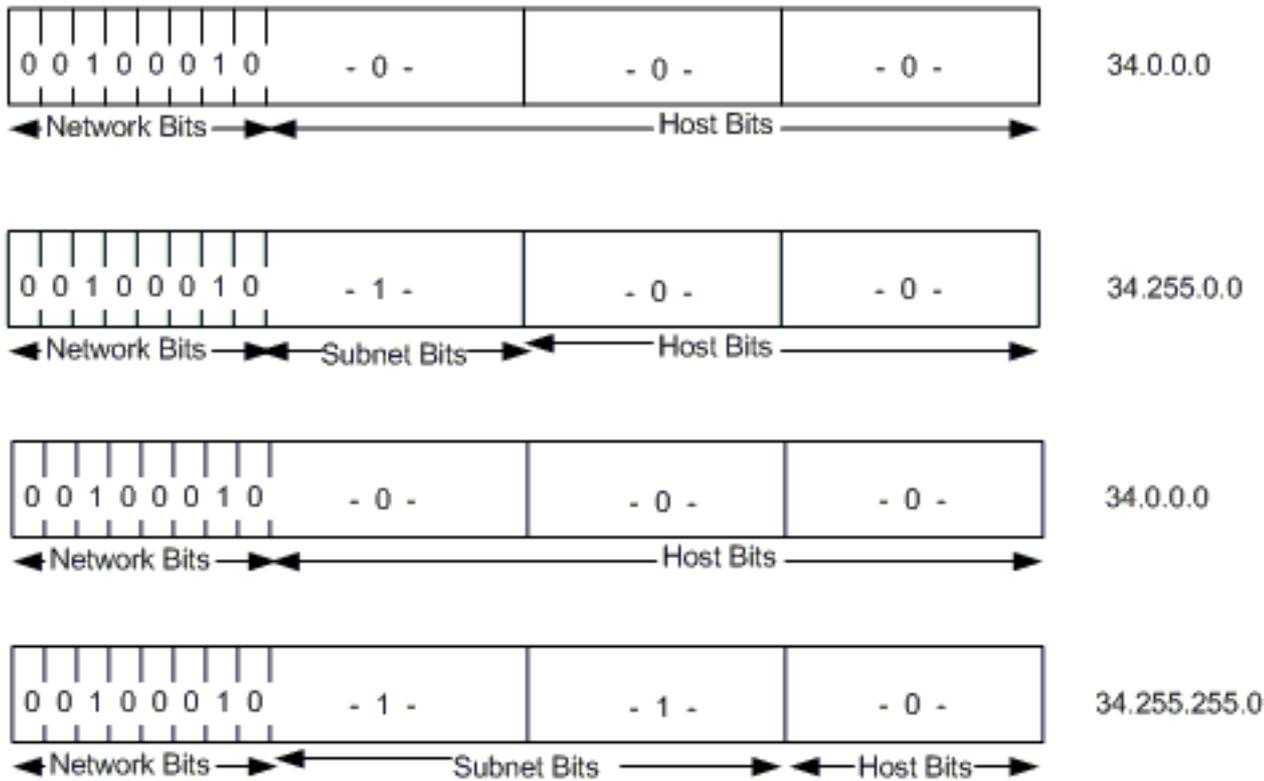
그림 4 "차입" 비트



네트워크 관리자가 8비트 서브넷 사용을 선택한 경우 클래스 A IP 주소의 두 번째 8진수는 서브넷 번호를 제공합니다. 이 예에서 주소 34.1.0.0은 네트워크 34, 서브넷 1, 주소 34.2.0.0은 네트워크 34, 서브넷 2 등을 나타냅니다.

서브넷 주소에 대해 빌릴 수 있는 비트 수는 다릅니다. 네트워크 및 주소의 서브넷 부분을 나타내는데 사용되는 비트 수를 지정하려면 IP에서 서브넷 마스크를 제공합니다. 서브넷 마스크는 IP 주소와 동일한 형식 및 표현 기술을 사용합니다. 서브넷 마스크에는 호스트 필드를 지정하는 것을 제외한 모든 비트 단위의 마스크가 있습니다. 예를 들어, 클래스 A 주소 34.0.0.0에 대해 8비트의 서브넷 마스크를 지정하는 서브넷 마스크는 255.255.0.0입니다. 클래스 A 주소 34.0.0.0에 대해 16비트를 지정하는 서브넷 마스크는 255.255.255.0입니다. [그림 5](#)에 이러한 서브넷 마스크가 표시되어 있습니다. 서브넷 마스크는 온디맨드 방식으로 네트워크를 통해 전달될 수 있으므로 새 노드가 네트워크에서 사용되는 서브넷 네팅 비트의 수를 알 수 있습니다.

그림 5 서브넷 마스크



일반적으로 동일한 네트워크 번호의 모든 서브넷이 동일한 서브넷 마스크를 사용했습니다. 즉, 네트워크 관리자는 네트워크의 모든 서브넷에 대해 8비트 마스크를 선택합니다. 이 전략은 네트워크 관리자와 라우팅 프로토콜 모두에 대해 쉽게 관리할 수 있습니다. 그러나 이러한 관행은 일부 네트워크의 공간을 낭비합니다. 일부 서브넷에는 호스트가 많고 일부는 몇 개만 있지만, 각 서브넷은 전체 서브넷 번호를 사용합니다. 직렬 회선은 가장 극단적인 예입니다. 각 회선에는 직렬 회선 서브넷을 통해 연결할 수 있는 호스트가 2개만 있기 때문입니다.

IP 서브넷이 증가함에 따라 관리자는 주소 공간을 보다 효율적으로 사용할 방법을 모색했습니다. 그 결과 얻은 기술 중 하나는 VLSM(Variable Length Subnet Masks)입니다. VLSM을 사용하면 네트워크 관리자가 호스트가 적은 네트워크에서 긴 마스크를 사용하고 호스트가 많은 서브넷에서 짧은 마스크를 사용할 수 있습니다. 그러나 이 방법은 모든 크기를 하나로 만드는 것보다 복잡하며 주소를 신중하게 할당해야 합니다.

물론 VLSM을 사용하려면 네트워크 관리자가 이를 지원하는 라우팅 프로토콜을 사용해야 합니다. Cisco 라우터는 OSPF(Open Shortest Path First), Integrated Intermediate System to Intermediate System(Integrated IS-IS), Enhanced IGRP(Interior Gateway Routing Protocol) 및 고정 라우팅을 지원하는 VLSM입니다. IP 주소 지정 및 서브넷에 대한 자세한 내용은 [새 사용자](#)의 IP 주소 지정 및 서브넷을 참조하십시오.

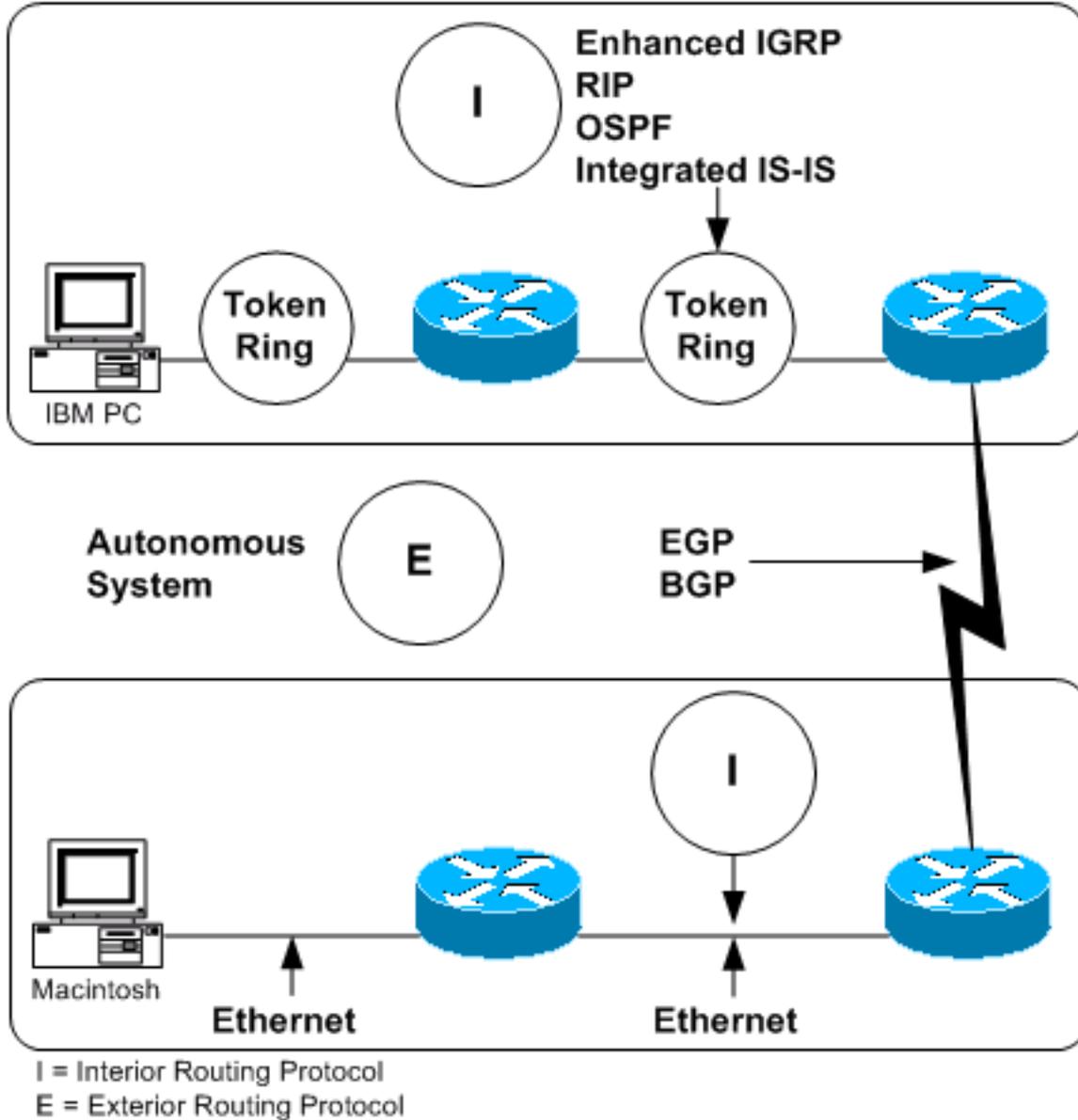
IEEE 802 LAN과 같은 일부 미디어에서는 인터넷 프로토콜 제품군의 다른 두 멤버를 사용하여 IP 주소를 동적으로 검색합니다. ARP(Address Resolution Protocol) 및 RARP(Reverse Address Resolution Protocol)는 브로드캐스트 메시지를 사용하여 특정 네트워크 레이어 주소에 해당하는 하드웨어(MAC 레이어) 주소를 결정합니다. ARP는 거의 모든 유형의 기본 미디어 액세스 메커니즘에서 IP를 사용할 수 있도록 충분히 일반적입니다. RARP는 브로드캐스트 메시지를 사용하여 특정 하드웨어 주소와 연결된 네트워크 레이어 주소를 결정합니다. RARP는 일반적으로 부팅 시 알 수 없는 네트워크 레이어 주소가 있는 디스크 없는 노드에 특히 중요합니다.

IP 환경에서 라우팅

"인터넷"은 상호 연결된 네트워크의 그룹입니다. 반면에 인터넷은 대부분의 연구 기관, 대학 및 전 세계 많은 다른 조직 간의 통신을 허용하는 네트워크의 모음입니다. 인터넷 내의 라우터는 계층적

로 구성됩니다. 일부 라우터는 동일한 관리 권한 및 제어 하에 하나의 특정 네트워크 그룹을 통해 정보를 이동하는 데 사용됩니다. 이러한 엔티티를 자동 시스템이라고 합니다. 자동 시스템 내에서 정보 교환에 사용되는 라우터를 내부 라우터라고 하며, 이를 위해 다양한 IGP(interior gateway protocol)를 사용합니다. 자동 시스템 간에 정보를 이동하는 라우터를 외부 라우터라고 합니다. EGP(Exterior Gateway Protocol) 또는 BGP(Border Gateway Protocol)를 사용합니다. [그림 6](#)은 인터넷 아키텍처를 보여줍니다.

그림 6 인터넷 아키텍처의 표현



IP와 함께 사용되는 라우팅 프로토콜은 본질적으로 동적입니다. 동적 라우팅에서는 라우팅 디바이스의 소프트웨어가 경로를 계산해야 합니다. 동적 라우팅 알고리즘은 네트워크의 변화에 적응하며 최적의 경로를 자동으로 선택합니다. 동적 라우팅과 달리 네트워크 관리자가 설정할 경로에 대한 정적 라우팅 통화입니다. 고정 경로는 네트워크 관리자가 변경할 때까지 변경되지 않습니다.

IP 라우팅 테이블은 대상 주소/next hop 쌍으로 구성됩니다. Cisco 라우터의 이 샘플 라우팅 테이블에서는 첫 번째 항목이 "네트워크 34.1.0.0(네트워크 34의 서브넷 1)에 도달하기 위해 다음 중지란 주소 54.34.23.12의 노드"로 해석되는 것을 보여줍니다.

```
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#

앞서 살펴본 것처럼 IP 라우팅은 IP 데이터그램이 한 번에 하나의 라우터 홉을 통해 인터넷워크 간에 이동하도록 지정합니다. 여행 초기에 전체 경로를 알지 못합니다. 대신 각 중지에서 다음 라우터 홉은 데이터그램 내의 대상 주소와 현재 노드의 라우팅 테이블의 항목을 일치시켜 결정합니다. 라우팅 프로세스에 각 노드가 참여하는 것은 내부 정보를 기반으로 패킷을 전달하는 것으로만 구성됩니다. 라우팅 변칙 발생 시 IP는 소스에 대한 오류 보고를 제공하지 않습니다. 이 작업은 다른 인터넷 프로토콜인 ICMP(Internet Control Message Protocol)로 남습니다.

ICMP는 IP 인터넷워크 내에서 여러 작업을 수행합니다. ICMP는 생성된 주요 사유(라우팅 오류를 소스로 다시 보고)와 더불어 인터넷을 통해 노드 연결 가능성을 테스트하는 방법(ICMP Echo 및 Reply 메시지), 라우팅 효율성을 높이기 위한 방법(ICMP Redirect 메시지), 데이터그램이 인터넷 내에 존재하기 위해 할당된 시간을 초과했음을 소스(ICMP Time Exceeded 메시지) 및 기타 유용한 메시지를 제공합니다. 무엇보다도, ICMP는 모든 IP 구현, 특히 라우터에서 실행되는 IP 구현의 필수 요소입니다. 관련 [정보 참조](#)