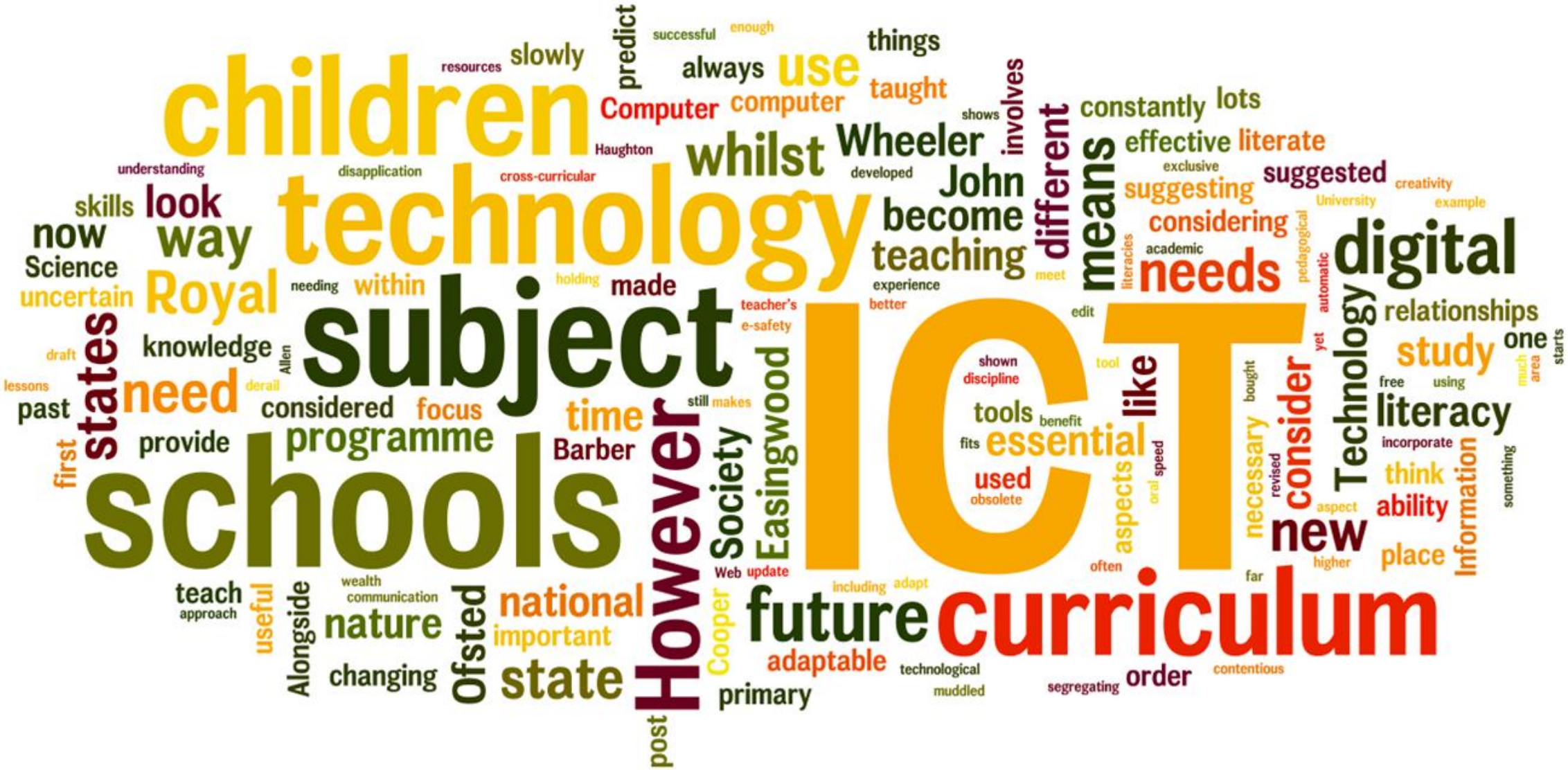
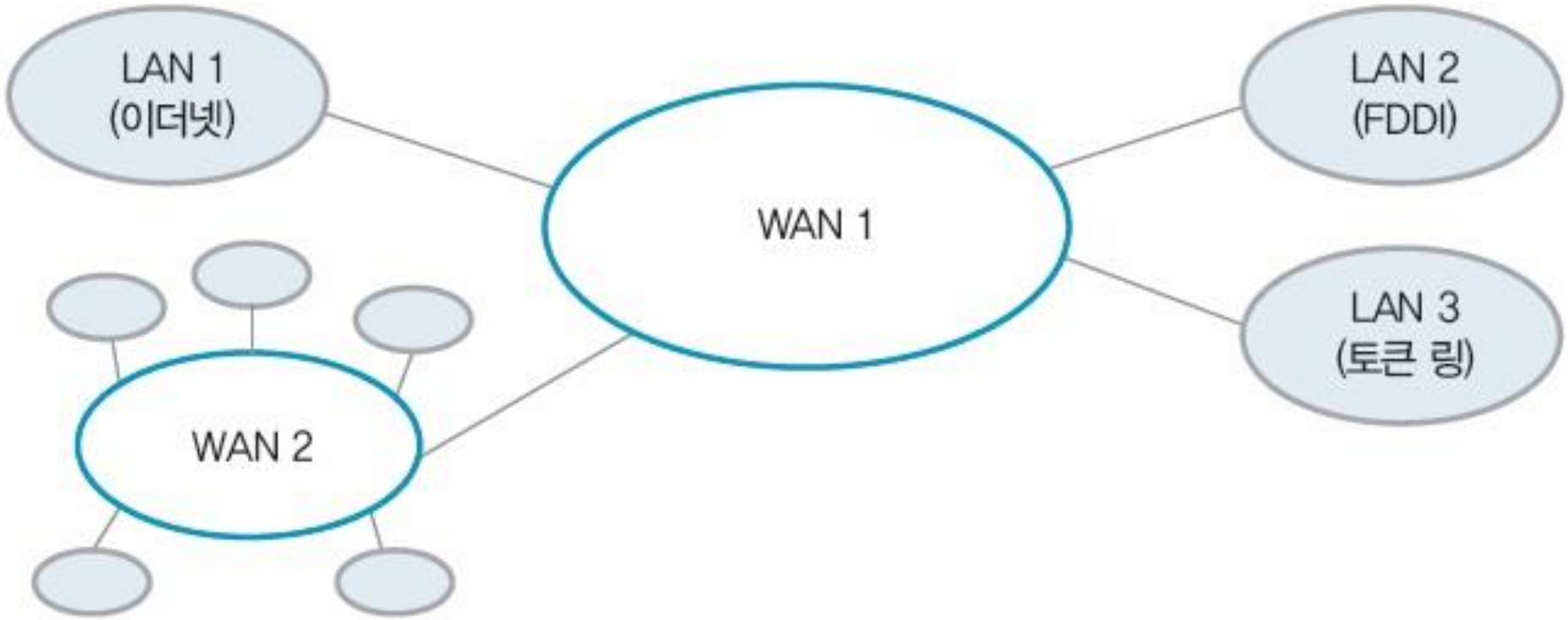

predict
successful
enough
things
slowly
resources
always
use
children
Computer
computer
taught
involves
shows
constantly
lots
Haughton
whilst
Wheeler
different
means
effective
literate
understanding
disapplication
cross-curricular
developed
John
suggested
creativity
skills
look
technology
suggesting
University
example
now
way
become
considering
Science
teaching
digital
needs
uncertain
Royal
needing
within
holding
made
experience
meet
literacies
pedagogical
automatic
teacher's
better
edit
relationships
subject
ICT
e-safety
one
study
draft
knowledge
Allen
shown
discipline
tool
yet
lessons
states
need
derail
bought
consider
Technology
free
using
much
area
starts
past
considered
focus
time
still
makes
tools
benefit
like
literacy
provide
programme
Barber
Easingwood
Society
fits
essential
incorporate
first
used
obsolete
speed
oral
aspects
necessary
revised
think
ability
aspect
schools
However
new
place
higher
Information
something
often
far
Web
update
including
adapt
teach
approach
wealth
communication
useful
Alongside
nature
national
Ofsted
Cooper
future
curriculum
important
adaptable
technological
muddled
segregating
order
contentious
changing
state
primary
post

07 인터넷

인터네트워크(Internetwork)

- LAN이나 WAN 등 독립적인 네트워크를 상호 연결하여 만든 복잡한 네트워크

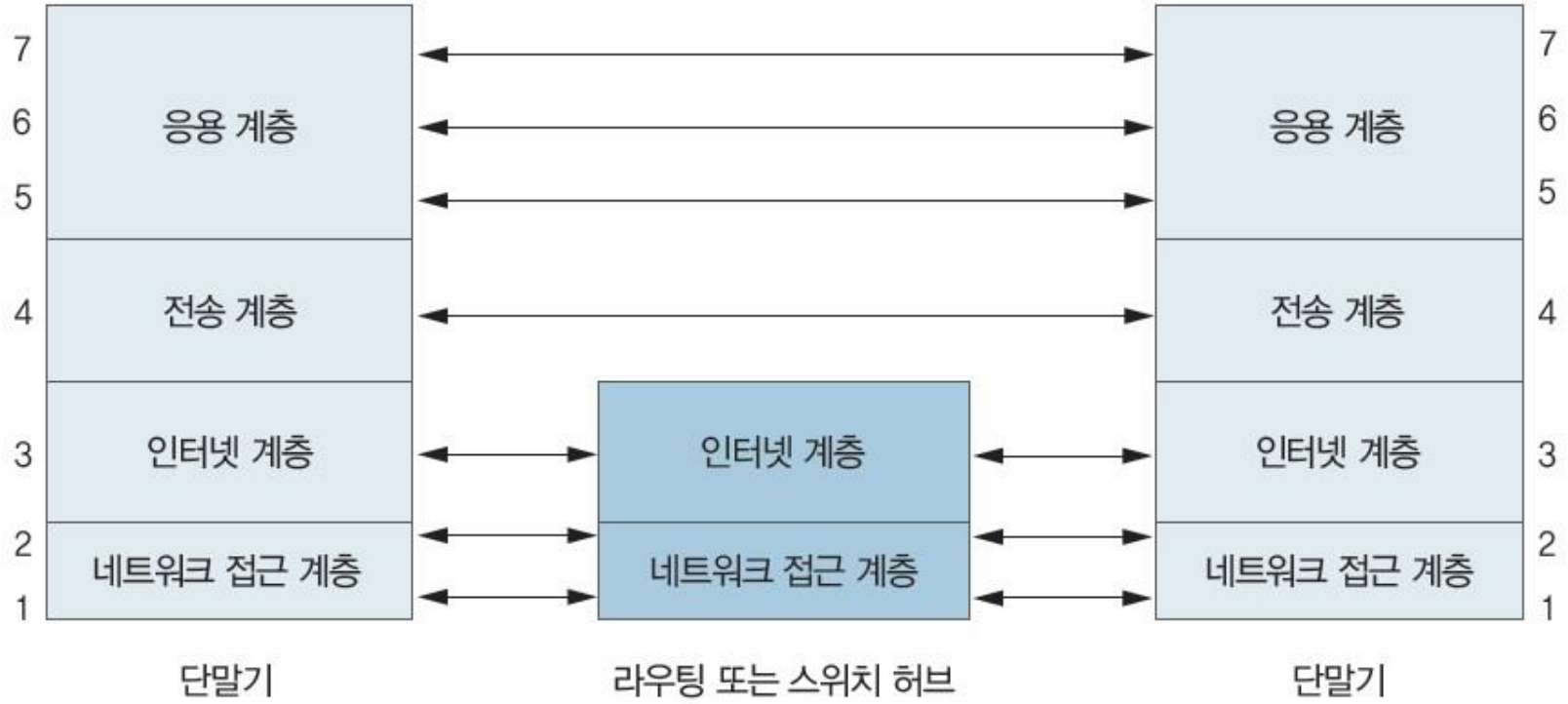


인터네트워킹(Internetworking)

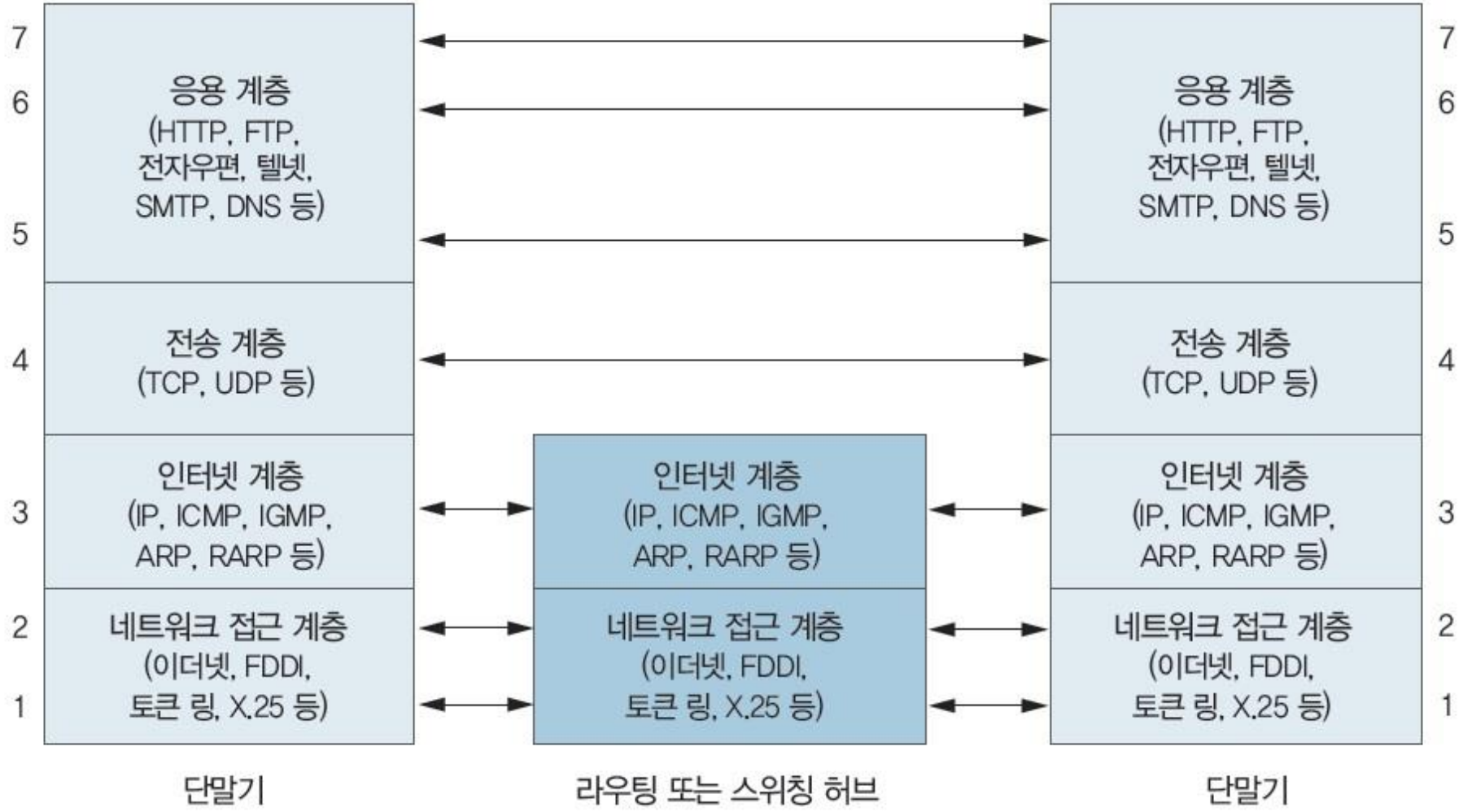
- 인터네트워크를 연결하는 과정이나 방법
- 하나의 통신 기준을 바탕으로 종류가 다른 네트워크를 서로 연결하므로, 다양한 하드웨어와 소프트웨어 기술이 필요
- 관련 장비로는 리피터, 브리지, 라우터, 게이트웨이 등이 있음
- 인터네트워킹으로 구성된 대표적인 네트워크가 바로 인터넷(Internet)

인터넷 프로토콜

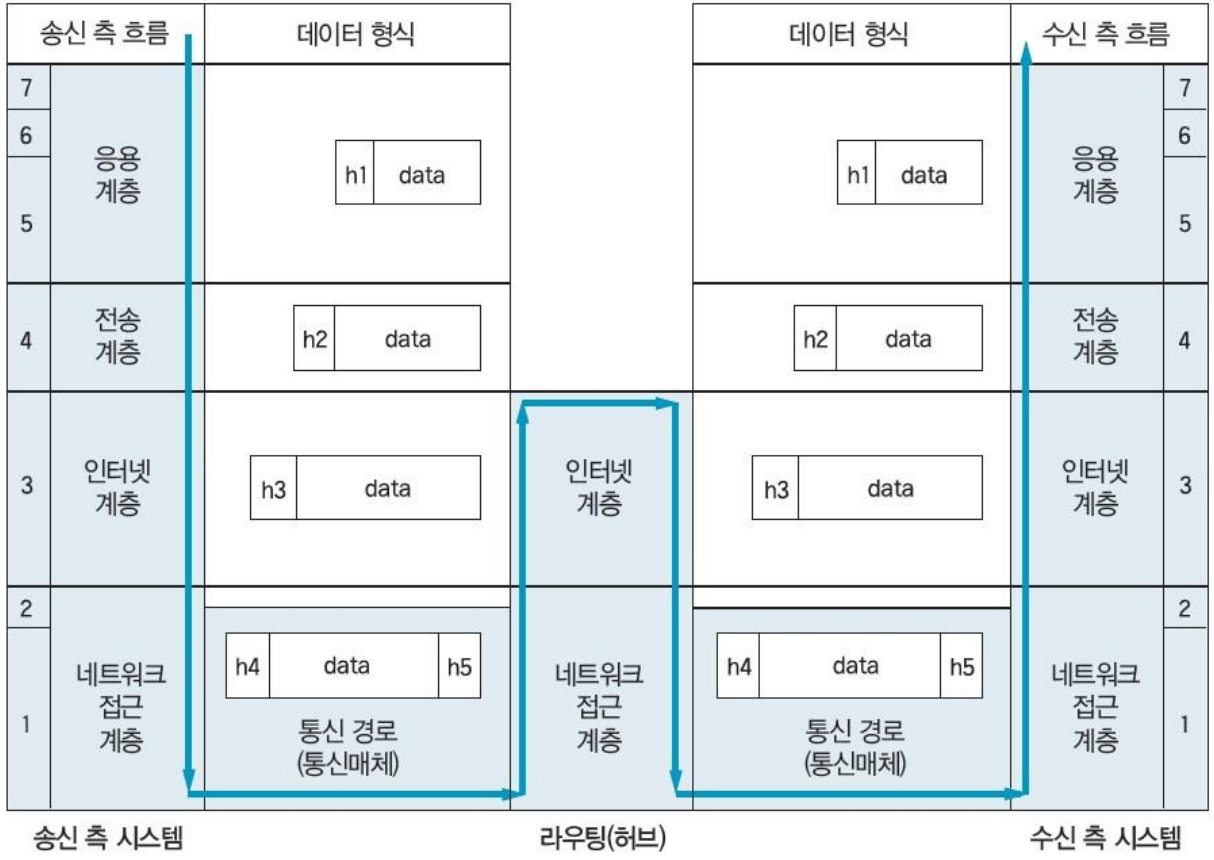
- TCP/IP는 인터넷에 기반을 둔 프로토콜
- 가정과 대학교 캠퍼스, 기업, 정부 연구기관 등을 서로 연결하여 전 세계적 규모의 인터넷을 구성하는 기반을 만듦



인터넷의 계층별 대표 프로토콜



인터넷에서 데이터를 전송하는 과정



※ TCP/IP일 때

- h1 : 응용 헤더
- h2 : TCP 헤더
- h3 : IP 헤더
- h4 : 이더넷 헤더
- h5 : 이더넷 트레일러

인터넷에서 데이터를 전송하는 과정

① 송신 측의 최상위 계층(응용 계층)에서 발생한 데이터는 헤더 정보를 추가한 후 아래 계층으로 전달됨

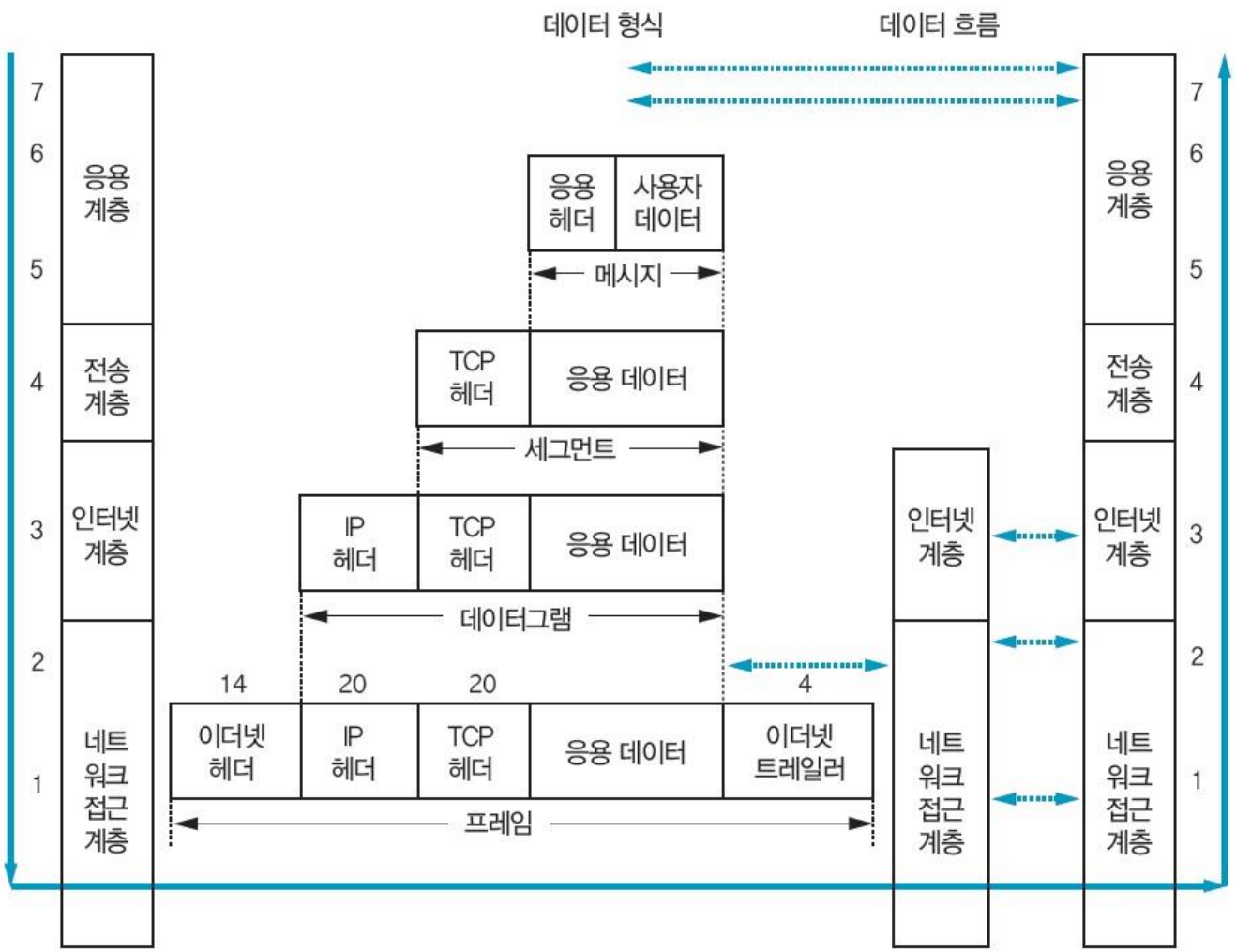
② 송신 측에 있는 최하위 계층에는 원래 데이터에 헤더를 여러 개 씌운 형태로 존재 → 캡슐화

③ 송신 측 최하위 계층에서는 이 데이터를 전기 신호로 변환하여 전송

④ 송신 측 각 계층은 헤더에 해당되는 부분을 벗겨내어 수신 측의 최상위 계층으로 전달 → 캡슐해제

⑤ 수신 측의 최상위 계층에서는 송신 측의 최상위 계층에서 보낸 원래 데이터가 정확하게 전달됨

인터넷에서 데이터를 전송하는 과정



IP와 인터넷 도메인

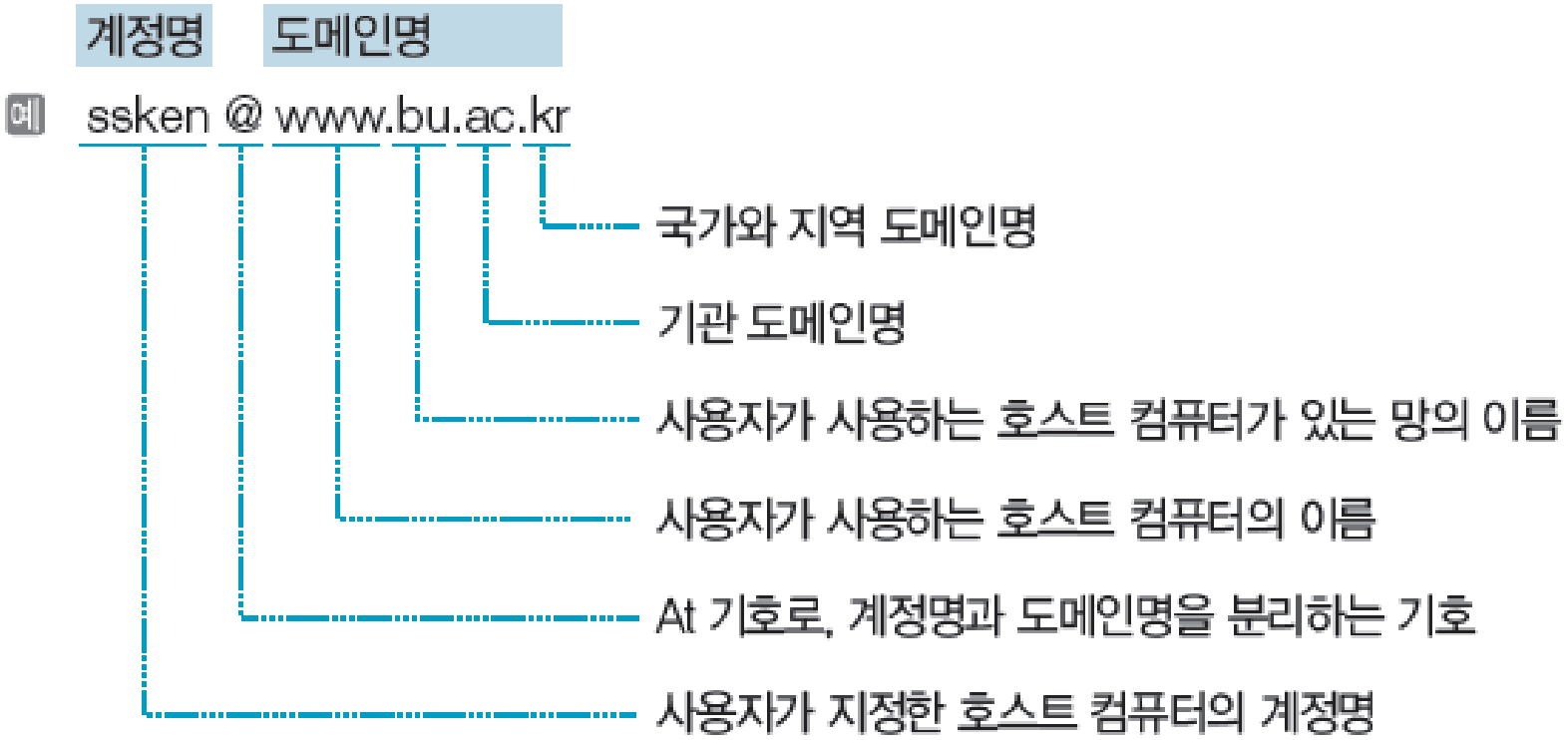
- IP 주소 체계 : 컴퓨터가 인식할 수 있는 주소 체계
- 인터넷 도메인 : 사람이 인식할 수 있는 주소 체계
  → IP 주소나 인터넷 도메인 모두 인터넷 계층은 IP에서 정의 및 처리함

인터넷 주소 관리 기관

- IANA : 전 세계 인터넷 주소 자원을 총괄 관리
- APNIC : 아/태 지역 총괄 관리
- NIDA(한국인터넷진흥원) : 우리나라의 인터넷 주소 자원을 관리
  - 국내에서 인터넷 도메인을 등록하려면 한국인터넷진흥원의 한국인터넷정보센터 (KRNIC)에서 주소를 할당받아야 함

도메인(Domain)의 개념

- 영문자나 .(마침표)를 혼합해 주소를 표현하는 것
- 국가는 최상위 도메인, 기관은 서브 도메인이라고 함



도메인명(Domain Name)

국가명	도메인명	국가명	도메인명	국가명	도메인명
Argentina	AR	Egypt	EG	Korea(North)	KP
Australia	AU	Finland	FI	Korea(South)	KR
Austria	AT	France	FR	New Zealand	NZ
Belgium	BE	Germany	GE	Norway	NO
Beliuze	BZ	Hong Kong	HK	Poland	PL
Canada	CA	Italy	IT	Taiwan	TW
China	CN	Japan	JP	United Kingdom	UK

도메인명(Domain Name)

도메인명	기관	사용 예
ac 또는 edu	학교(ACademy) 또는 학술기관	cheonan.ac.kr
co 또는 com	회사(COmpany)	samsung.com
go 또는 gov	정부기관(GOvernment)	bluehouse.go.kr
re	연구소(REsearch)	etri.re.kr
net	네트워크(NETwork) 관련기관	hitel.net
nm	네트워크 운영기관(Network Management)	hana.nm.kr
org	특수 사설기관(ORGanization)	www.ieee.org

도메인명의 조합 규칙

- 도메인명의 길이는 최대 256자까지 가능
- 도메인명은 숫자(0~9)나 영문자(A~Z), 영문자와 숫자의 조합으로 구성
- ,(쉼표)나 _(언더바) 등은 사용할 수 없음, -(하이픈)은 사용 가능
- 전 세계적으로 중복되지 않은 고유 주소를 사용해야 함

IP 주소의 개념

- IP 주소는 전 세계 모든 컴퓨터에 부여된 고유의 식별 주소
- 현재 사용 중인 버전은 IPv4이며, 차세대 버전은 IPv6
- 보통 IP 주소라 하면 IPv4를 뜻함
- IP 주소는 10진수 4개와 .(점)으로 표현, 실제로는 32비트로 구성됨
- 각 10진수 숫자는 0~255까지 사용할 수 있으며, 숫자가 256개인 8비트가 필요
- 하므로 전체적으로는 32비트가 필요

IP 주소 체계

- 네트워크 번호와 그 네트워크에 접속해서 부여하는 호스트 번호로 구성
- IP 주소 체계는 클래스 A~E까지 다섯 종류
- 첫 번째부터 네 번째 비트까지 번호를 할당하여 클래스를 구분

IP 주소 체계

- 클래스 A
  - 첫 번째 비트가 0인 주소로, 범위는 1.X.X.X~127.X.X.X
  - 주소가 64.X.X.X라면 64.0.0.0과 64.255.255.255는 특수 목적으로 사용되고, 나머지 주소는 망에 있는 호스트 주소로 사용
  - 즉, 호스트 주소의 개수는 16,777,214(256×256×256-2)개, 64.0.0.0은 서브망의 주소
- 클래스 B
  - 첫 번째와 두 번째 비트가 각각 1과 0인 주소로, 범위는 128.X.X.X~191.255.X.X
  - 주소가 149.11.X.X라면 149.11.0.0과 149.11.255.255는 특수 목적으로 사용되고, 나머지 주소는 망에 있는 호스트 주소로 사용
  - 즉, 호스트 주소의 개수는 65,534(256×256-2)개, 149.11.0.0은 서브망의 주소

IP 주소 체계

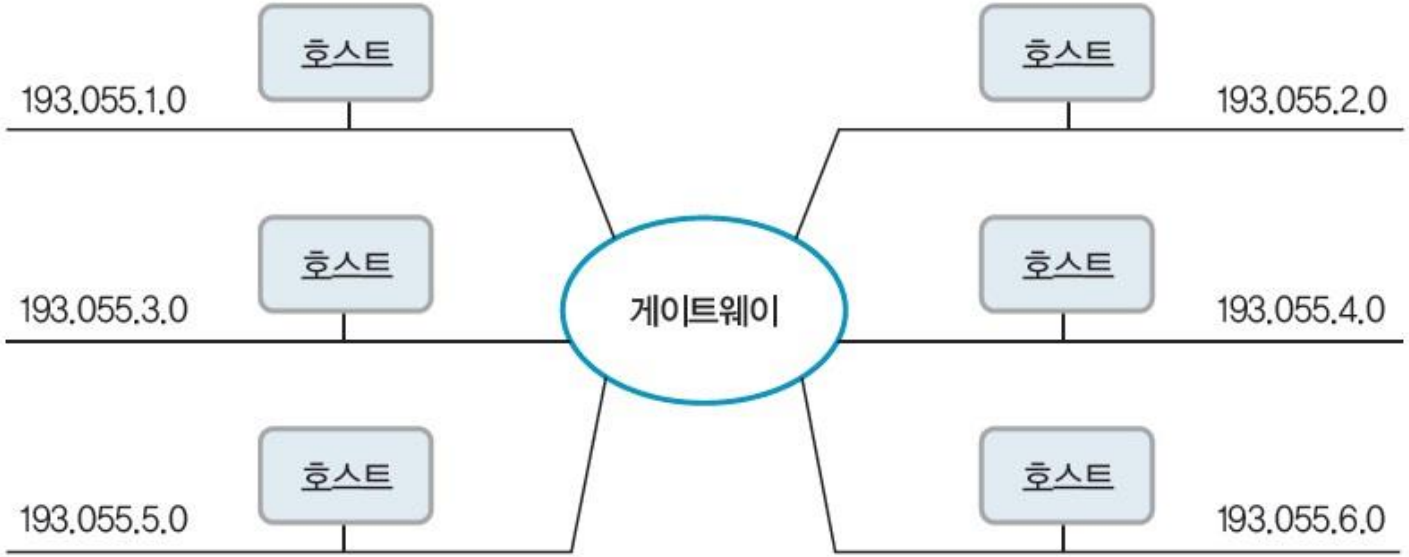
- 클래스 C
  - 첫 번째에서 세 번째 비트가 각각1 , 1, 0인 주소로, 범위는 192.X.X.X~223.255.255.255
  - 주소가 249.11.1.X라면 249.11.1.0과 249.11.1.255는 특수 목적으로 사용되고, 나머지 주소는 망에 있는 호스트 주소로 사용
  - 즉, 호스트 주소의 개수는 254(256-2)개,249.11.1.0은 서브망의 주소
- 클래스 D
  - 첫 번째에서 네 번째 비트가 각각 1, 1, 1, 0인 주소로 나머지 28비트를 멀티캐스트용으로 사용한다
  - 범위는 224.X.X.X~239.255.255.255
- 클래스 E
  - 첫 번째에서 네 번째 비트가 각각 1, 1, 1, 1인 주소
  - 향후 사용하려고 남겨둔 예비·실험용 주소
  - 범위는 240.X.X.X~247.255.255.255

IP 주소 관리 방식과 서브네팅

- 서브넷 주소는 IP 주소를 네트워크 번호와 호스트 번호로만 구분하지 않고 호스트 번호 부분을 서브넷 번호와 호스트 번호로 세분하는 방식
- 서브넷 주소는 IP 주소의 비트를 더욱 효율적으로 사용하는 방법
- 예를 들어 클래스 B에 서브넷을 적용하면 254(28-2)개의 서브넷과 서브넷당 254개(28-2)의 호스트를 만들 수 있음

IP 주소 관리 방식과 서브네팅

- 서브넷 주소를 사용하면 외부 라우터가 내부 네트워크 조직에 대해 모르게 할 수 있으며, 라우팅 테이블의 크기를 줄이는 효과도 얻을 수 있음
- 서브넷 마스크는 서브넷과 호스트 부분을 구분해 주는 역할을 함
- 각 클래스의 디폴트 서브넷 마스크는 클래스 A는 (255.0.0.0), 클래스 B는 (255.255.0.0), 클래스 C는 (255.255.255.0)



IP 주소 관리 방식과 서브네팅

클래스 C 네트워크를 26개의 서브넷으로 나누고, 각 서브넷에는 4~5개의 호스트를 연결하려고 한다. 이러한 서브넷을 구성하기 위해서는 서브넷 마스크 값을 얼마로 해야 하는가?

- 클래스 C에서 서브넷 마스크를 적용해야 할 부분은 맨 마지막 8비트
- 이 중에서 4~5개의 호스트를 연결하려면 적어도 3비트가 필요
- 나머지 5비트를 가지고 최대 32(25)개의 서브넷을 만들 수 있음
- 처음 다섯 비트는 서브넷 번호로 사용하고 이후 세 비트는 호스트 번호로 사용
- 서브넷 번호로 사용할 비트는 1을 할당하고 나머지 비트는 0을 할당한 값은 11111000으로, 이를 10진수로 바꾸면 248
- 최종적으로 서브넷을 구성하기 위한 서브넷 마스크 값은 255.255.255.248

도메인 네임 시스템(DNS, Domain Name System)

- 인터넷 도메인명과 IP 주소를 대응시켜 주는 거대 규모의 분산 시스템
- IP 주소 같이 숫자로 되어 있는 주소 정보를 문자열 정보로 변환하여 관리하는 서버이며, 주로 인터넷에서 사용

URL(Uniform Resources Locator)

- 인터넷에서 자원의 위치를 통일적으로 표현하는 주소
- 웹 브라우저에 URL을 입력하면 그 URL이 가리키는 웹 서버에 있는 하이퍼미디어 문서를 불러올 수 있음

네트워크 접근 계층 프로토콜

- 네트워크 접근 계층은 네트워크 매체와 인터페이스에서 하드웨어의 세부사항을 처리하며, 상위 계층의 데이터를 수용하여 연결된 다른 네트워크로 전송
- 네트워크 인터페이스 카드(NIC)의 디바이스 드라이버처럼 하드웨어 관련 프로그램이 있음 (여기서 전달되는 데이터를 프레임이라고 함)
- 대표 프로토콜로 이더넷, FDDI, 토큰 링, X.25 등 여러 가지가 있음

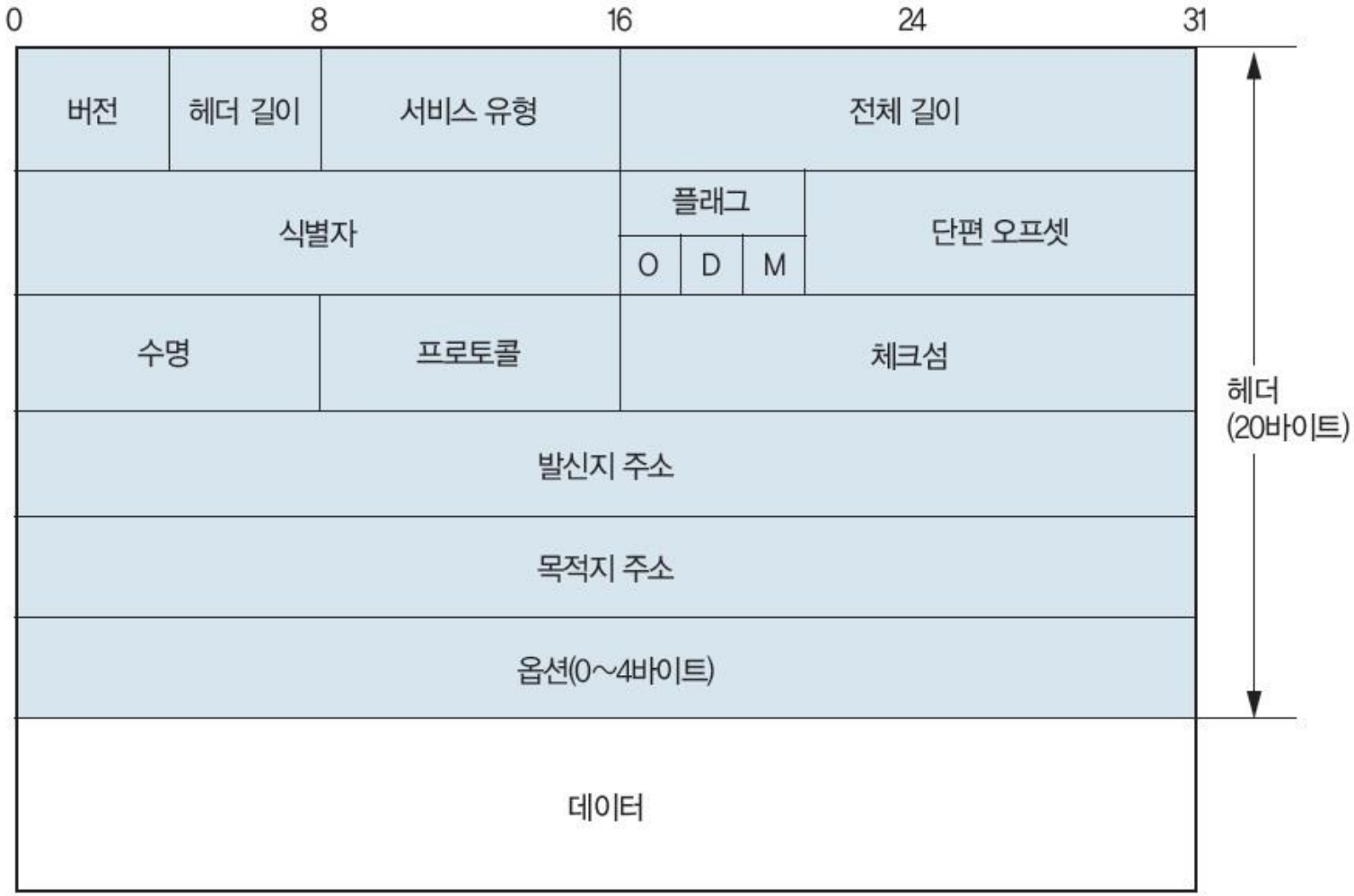
인터넷 계층 프로토콜

- 인터넷 계층은 발신지에서 목적지로 데이터를 전송하는 일을 함
- 주소 지정, 패키징(Packaging), 라우팅(Routing) 등의 기능을 제공(여기서 전달되는 데이터를 데이터그램이라고 함)
  - 주소 지정 : 인터넷 계층 프로토콜은 비연결형으로 신뢰성이 없고, 오류 검사나 추적을 하지 않음
  - 패키징 : 데이터에 헤더를 추가하는 것(헤더에는 발신지, 목적지 IP 주소, 전송 프로토콜, 체크섬, 생존 시간 등의 정보가 들어 있음)
  - 라우팅 : 발신지와 목적지 IP 호스트가 원격지의 네트워크에 있다면 라우팅 테이블을 검색하여 최적의 경로를 찾음

IP(Internet Protocol)

- 인터넷 계층에서 가장 중요한 프로토콜
- 다양한 네트워크로 구성된 인터넷을 이용해 발신지에서 목적지까지 데이터그램을 전송할 수 있도록 라우팅 기능을 수행
- 여기에는 오류와 상황 보고, 경로를 제어하는 정보 전달 기능 등은 포함되어 있지 않음

IP 헤더


0
8
16
24
31
버전
헤더 길이
서비스 유형
전체 길이
식별자
플래그
O
D
M
단편 오프셋
수명
프로토콜
체크섬
발신지 주소
목적지 주소
옵션(0~4바이트)
데이터
헤더
(20바이트)

IP 헤더

항목	길이	설명
버전(Version)	4	• IP 헤더 형식을 나타내는 것으로 현재는 4, 차세대는 6. 여기서 4는 IPv4를, 6은 IPv6를 의미
헤더 길이(Header Length)	4	• 4바이트(또는 옥텟, Octet)의 배수로 표시 • 선택 항목을 제외하면 20바이트(20옥텟=5×4)
서비스 유형 (TOS, Type Of Service)	8	• 우선순위, 지연 시간, 처리 능력, 신뢰성 등 바람직한 QoS(Quality Of Service) 표시 • 총 8비트 중에서 상위 3비트는 사용하지 않고, 나머지 5비트 중 4비트만 설정하여 사용 • 마지막 비트값은 0으로 지정
전체 길이(Total Length)	16	• IP 데이터그램의 총 길이로, 데이터의 시작 위치 명시 • IP 데이터그램의 최대 길이는 65,535바이트로, 최소 길이는 576바이트(512+64(프로토콜 오버헤드))
식별자(Identification)	16	• 각 데이터그램을 식별 • IP 단편화에 이용
플래그(Flag)	3	• 단편화와 관련된 항목으로, 단편화 여부와 마지막 조각인지 표시

IP 헤더

항목	길이	설명
단편 오프셋 (FO, Fragment Offset)	13	• 단편의 시작 바이트를 8로 나눈 값을 저장 • 데이터 항목의 시작 위치 표시
수명(TTL, Time To Live)	8	• 데이터그램이 활동할 수 있는 최대 시간을 초 단위로 나타냄 • 이 항목이 0이 되면 타이머 완료 • 통과할 수 있는 라우터의 수 제한
프로토콜(Protocol)	8	• IP로 데이터를 보낸 프로토콜 명시
체크섬	16	• IP 데이터그램의 오류를 검사하는 것으로 데이터를 제외한 헤더 부분을 검사
발신지 주소	32	• 데이터그램을 송신한 장치의 논리적 주소
목적지 주소	32	• 데이터그램을 수신한 장치의 논리적 주소
옵션		• 필요하면 옵션(경로 설정, 정렬, 타이밍 등) 사용 • 평소에는 잘 사용하지 않음

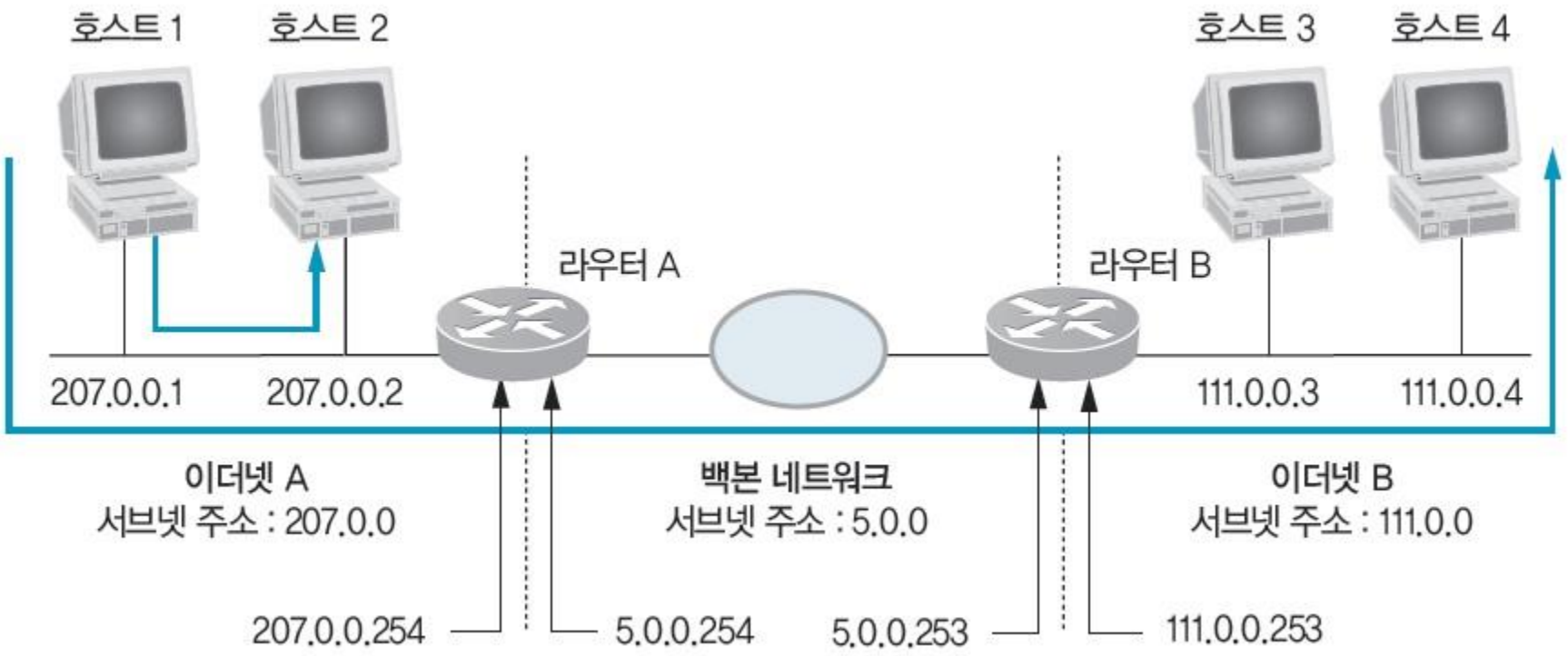
IP 라우팅

- 송신지에서 목적지로 패킷을 전송할 경로를 직접 연결하지 않고, 중간 노드를 경유하여 연결하는 기능(이 기능을 수행하는 장비가 라우터)

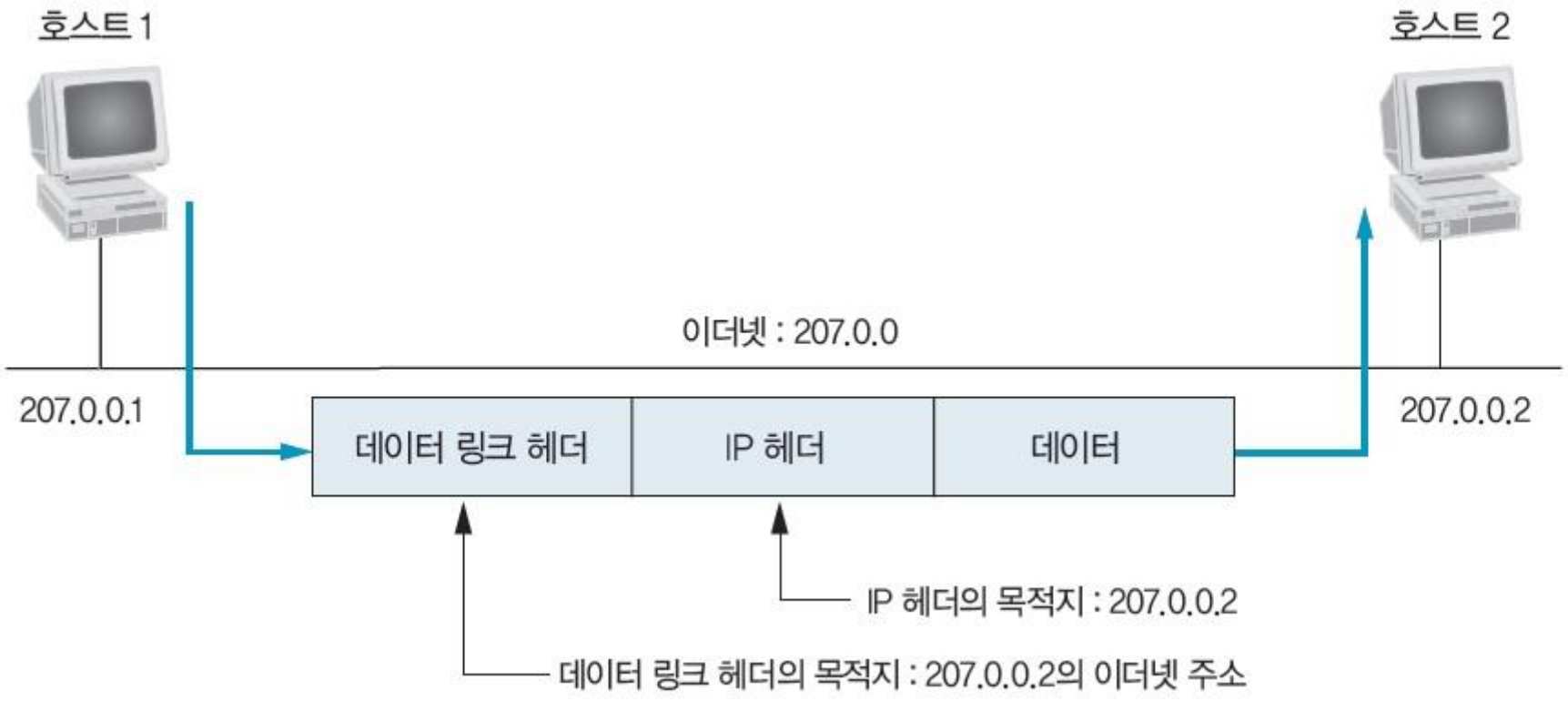
라우팅 프로토콜과 라우팅 테이블

- 라우터가 경로를 결정하는 데 사용하는 규칙을 라우팅 프로토콜이라고 함
- 라우팅은 경로 결정과 스위칭 기능으로 구성
- 결정된 경로는 라우팅 테이블에 저장
- 한번 결정한 경로는 대부분 결정한 경로가 유효한지 계속 확인

IP 라우팅의 예


호스트 1
호스트 2
호스트 3
호스트 4
라우터 A
라우터 B
207.0.0.1
207.0.0.2
111.0.0.3
111.0.0.4
이더넷 A
서브넷 주소 : 207.0.0
백본 네트워크
서브넷 주소 : 5.0.0
이더넷 B
서브넷 주소 : 111.0.0
207.0.0.254
5.0.0.254
5.0.0.253
111.0.0.253

IP 라우팅의 예


호스트 1
호스트 2
이더넷 : 207.0.0
207.0.0.1
207.0.0.2
데이터 링크 헤더
IP 헤더
데이터
IP 헤더의 목적지 : 207.0.0.2
데이터 링크 헤더의 목적지 : 207.0.0.2의 이더넷 주소

IPv6(Internet Protocol version 6)

- IPv6는 주소 부족, 보안성 취약, 실시간 전송의 문제점 등을 가지고 있는 IPv4의 주소 체계를 개선한 차세대 인터넷 프로토콜
- 1990년대 초부터 인터넷 기술 작업반(IETF, Internet Engineering Task Force)에서 연구와 표준화 작업을 수행
- 주소 공간은 128비트로, 32비트인 IPv4보다 주소 공간이 4배 확대됨

IPv6의 헤더 구조

0
8
16
24
31
버전
우선순위
흐름 라벨
페이로드 길이
다음 헤더
홉 한계
발신지 주소
목적지 주소
옵션
데이터
40바이트

IPv6의 헤더 구조

항목	길이	설명
버전(Version)	4	프로토콜의 버전 표시로 값은 고정값인 6
우선순위(Priority)	8	우선순위 표시
흐름 라벨(Flow Label)	20	송신지와 수신지의 고유 특성과 요구사항 설정
페이로드 길이(Payload Length)	16	40바이트 다음 바이트의 정보를 알려줌
다음 헤더(Next Header)	8	IPv6의 확장 헤더나 TCP/UDP처럼 상위 계층 헤더의 종류 표시
홉 한계(Hop Limit)	8	패킷이 영원히 있는 것을 방지하는 것으로 값이 0이면 폐기
발신지 주소(Source Address)	128	발신지 주소 표시
목적지 주소(Destination Address)	128	목적지 주소 표시

IPv6의 특징

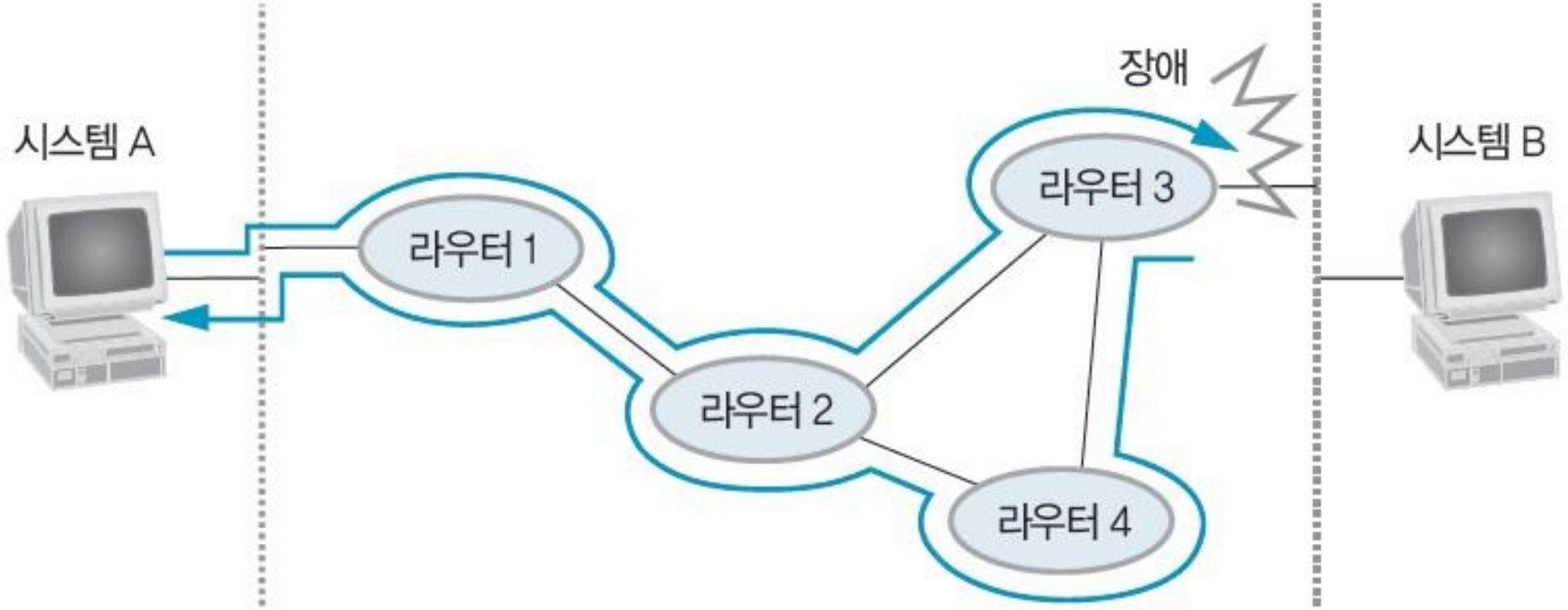
- IPv6의 주소 공간은 128비트로, 32비트인 IPv4보다 주소 공간이 4배 확대
- 기본 헤더와 확장 헤더가 분리되어 구조가 매우 유연해 쉽게 변경 추가 가능
- IPv4의 헤더 구조보다 단순하며, IPv4의 옵션 필드를 확장 헤더로 구현

IPv6의 주소 유형

- 유니캐스트(Unicast) : 단일 인터페이스 형식의 주소, 주소에 해당하는 인터페이스에만 전달됨
- 애니캐스트(Anycast) : 멀티 인터페이스 형식의 주소, 주소에 해당하는 인터페이스 중 하나에 전달됨
- 멀티캐스트(Multicast) : 멀티 인터페이스 형식의 주소, 주소에 해당하는 모든 인터페이스에 전달됨

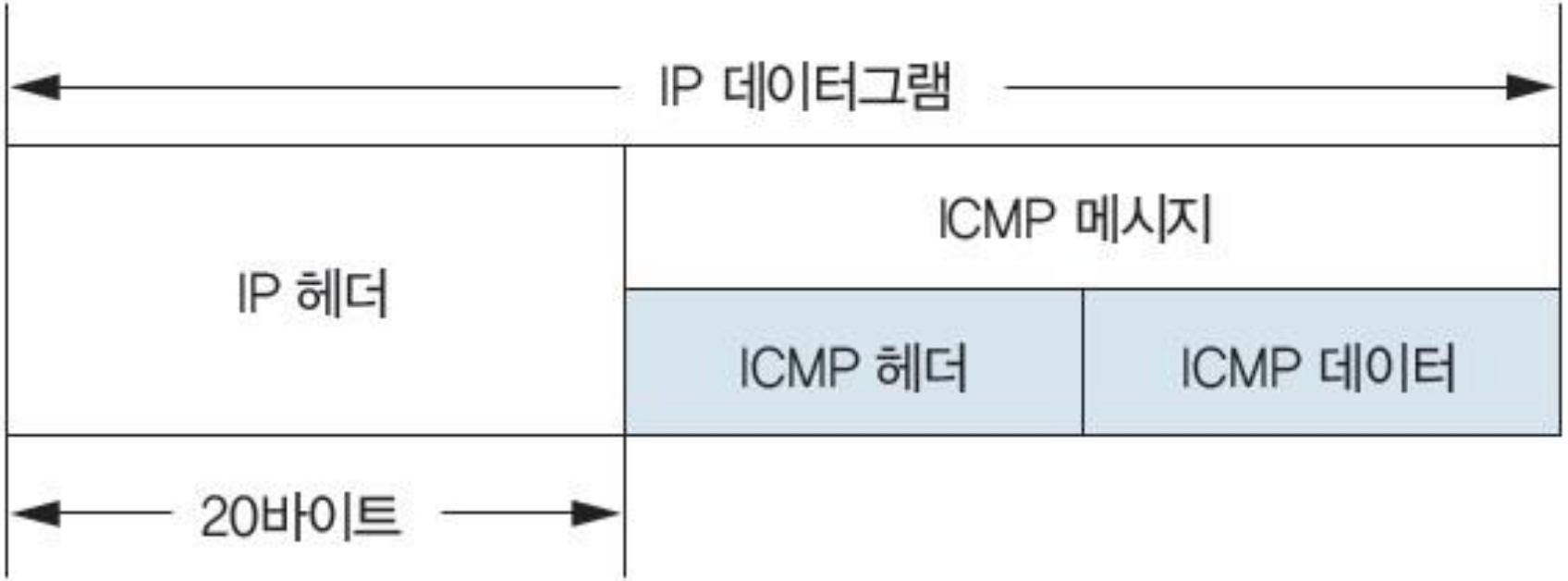
ICMP(Internet Control Message Protocol)

- IP에서 발생하는 문제를 처리하기 위한 프로토콜
- 오류 보고, 상황 보고, 경로를 제어하는 정보 전달 기능 등이 있음



ICMP 메시지의 캡슐화

- ICMP 메시지는 인터넷과 라우터를 거쳐 운반되므로 IP로 캡슐화해야 함
- IP로 캡슐화하더라도 ICMP를 상위 계층 프로토콜로 간주하지는 않음



ICMP 메시지의 형식

ICMP 헤더의 항목

항목	길이	설명
타입(Type)	8	ICMP 메시지의 종류 표시
코드(Code)	8	각 메시지 타입에서 코드값 표시(0~5)
체크썸(Checksum)	16	ICMP 메시지 자체(헤더+데이터)에서 오류를 검사하는 필드
기타 헤더	32	타입과 코드에 따라 달라지는 부분

멀티캐스트

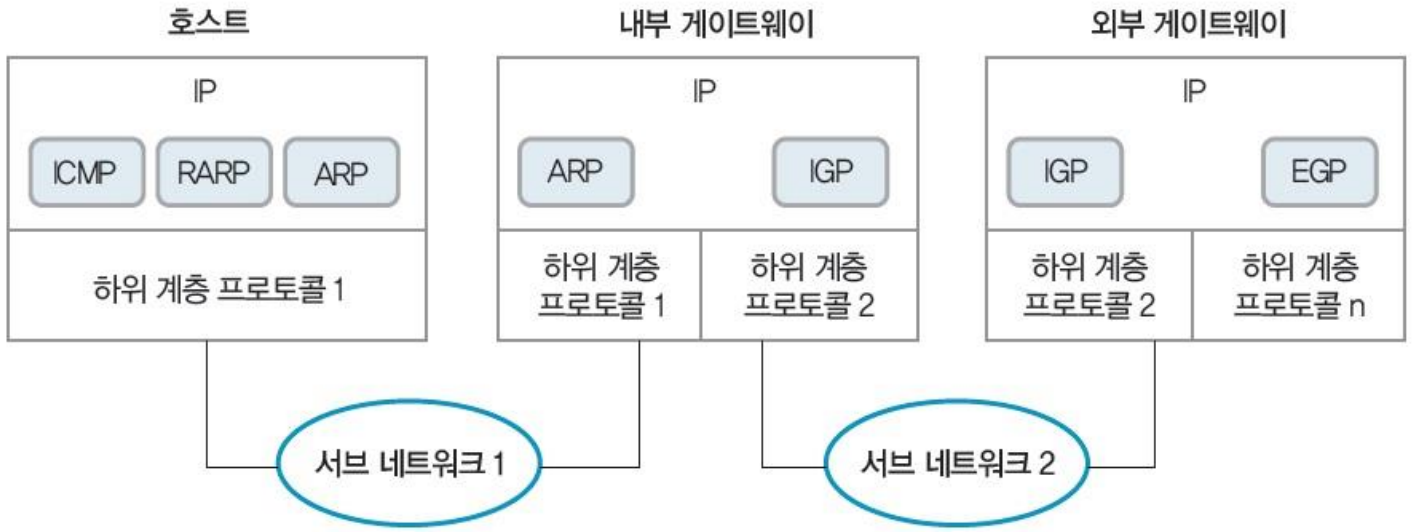
- 하나의 송신 노드가 네트워크에 연결된 하나 이상의 수신 노드에 데이터를 전송하는 것
- 송신 노드는 수신될 노드를 미리 지정함
- 전자우편에서 주소록을 미리 등록하여 보내는 방식이 대표적인 예

IGMP Internet Group Message Protocol

- 멀티캐스트 기능을 수행하는 프로토콜
- 네트워크의 멀티캐스트 트래픽을 자동으로 조절하고 제한
- 수신자 그룹에 메시지를 동시에 전송하는 데 사용
- 멀티캐스트 트래픽을 제어할 때 쿼리(Query)와 리포트(Report) 메시지 이용
  - 쿼리 메시지 : 라우터 같은 네트워크 장비가 보내는 메시지
  - 리포트 메시지 : 메시지를 보냈을 때 그것을 받은 호스트가 대답하는 메시지

인터넷 라우팅 프로토콜

- 자율시스템 구성요소가 라우팅 정보를 저장·관리하고, 사용하는 프로토콜
- 자율시스템 : 네트워크 내부의 라우팅이나 네트워크 관리를 독자적으로 운영함
  - 내부 게이트웨이 : 자율시스템 내부에 위치한 게이트웨이
  - 외부 게이트웨이 : 자율시스템을 연결하는 게이트웨이
  - 내부 게이트웨이 프로토콜(IGP) : 내부 게이트웨이에서 동작하는 라우팅 프로토콜
  - 외부 게이트웨이 프로토콜(EGP) : 외부 게이트웨이에서 동작하는 라우팅 프로토콜

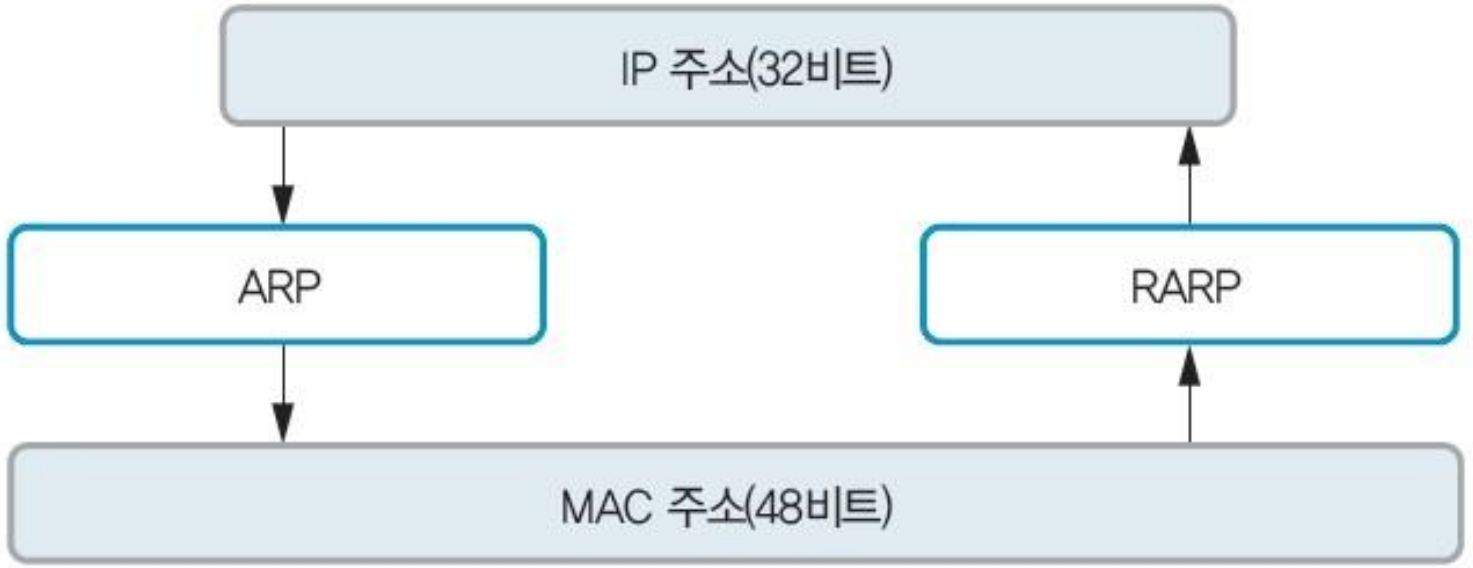


주소 결정 프로토콜ARP, Address Resolution Protocol

- IP 주소를 네트워크 인터페이스 카드(NIC)의 물리적 주소인 이더넷 주소로 변환
- IP와 관련된 LAN 카드의 물리 주소를 알아내는 프로토콜
- ARP는 RFC 826 규격

역주소 결정 프로토콜RARP, Reverse Address Resolution Protocol

- 네트워크 인터페이스 카드(NIC)의 물리적 주소인 이더넷 주소를 IP 주소로 변환
- RFC 903 규격



내부 게이트웨이 프로토콜IGP, Interior Gateway Protocol

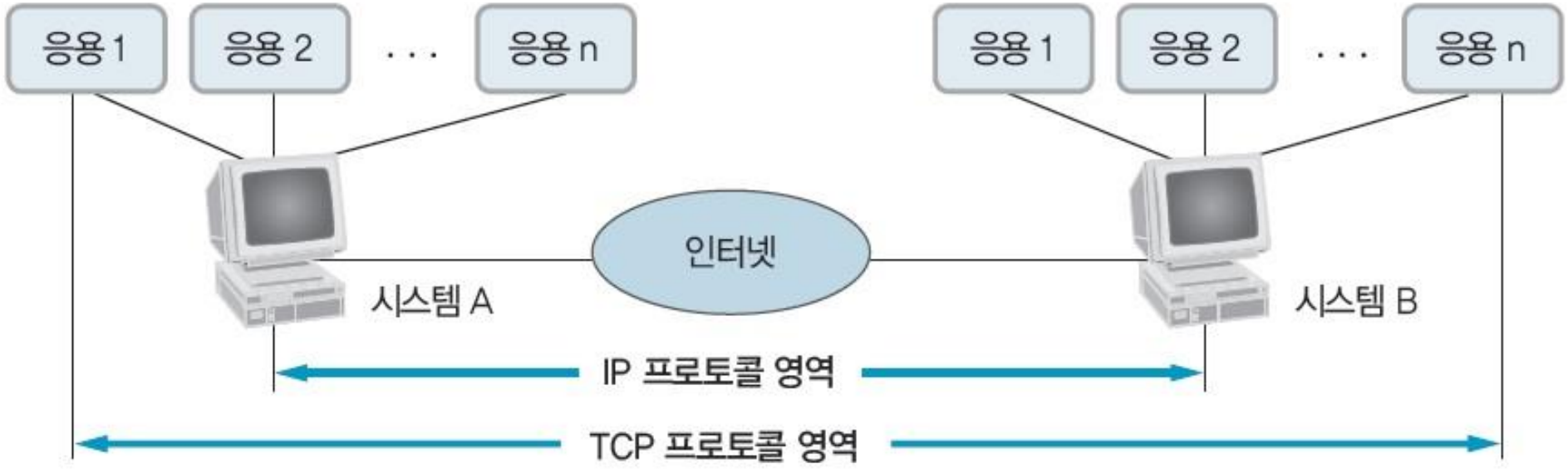
- 내부 게이트웨이와 외부 게이트에 위치
- 자율시스템 내부에서 작동

외부 게이트웨이 프로토콜EGP, Exterior Gateway Protocol

- 외부 게이트에 위치
- 서로 다른 자율시스템 사이에서 작동

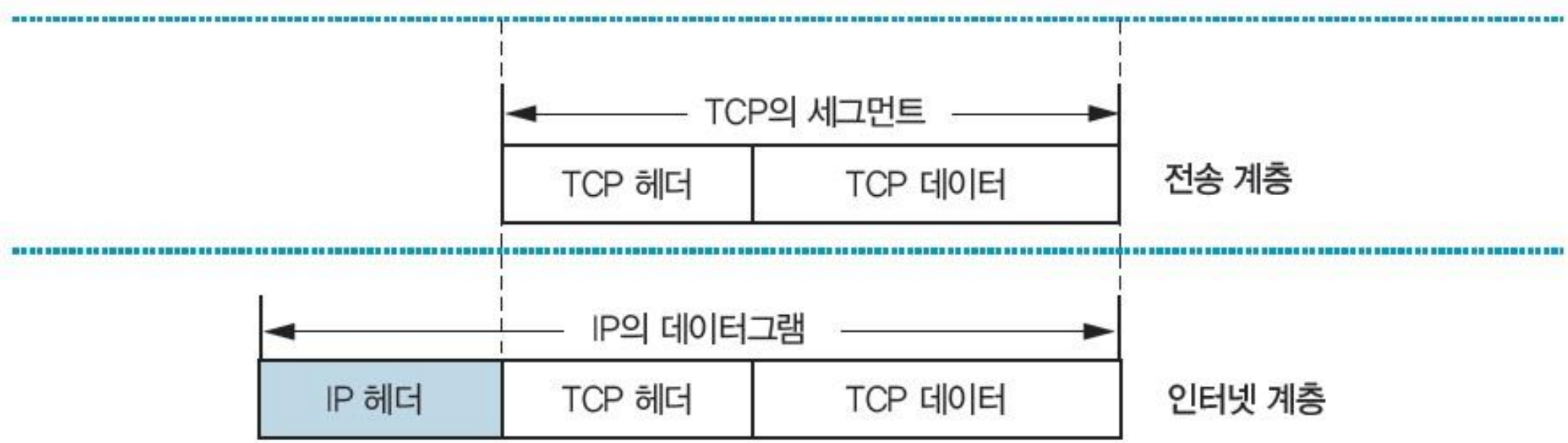
TCP Transmission Control Protocol

- 두 종단 간의 연결을 설정한 후 데이터를 8비트의 바이트 스트림으로 교환하는 연결형 프로토콜
- 응용 프로그램(프로세스) 간에 메시지를 전달하며 이를 위해 포트 번호를 이용
- 세그먼트 : TCP에서 전달되는 데이터



TCP의 캡슐화

- 세그먼트는 인터넷과 라우터를 거치기 때문에 IP가 캡슐화하여 전송



TCP 헤더의 구조

0
8
16
24
31
발신지 포트
목적지 포트
순서 번호
수신 확인 번호
헤더 길이 (HLEN)
예약 (Reserved)
URG
ACK
PSH
RST
SYN
FIN
윈도 크기
체크섬
긴급 포인터
옵션
데이터
TCP 헤더 : 20바이트

TCP 헤더의 항목

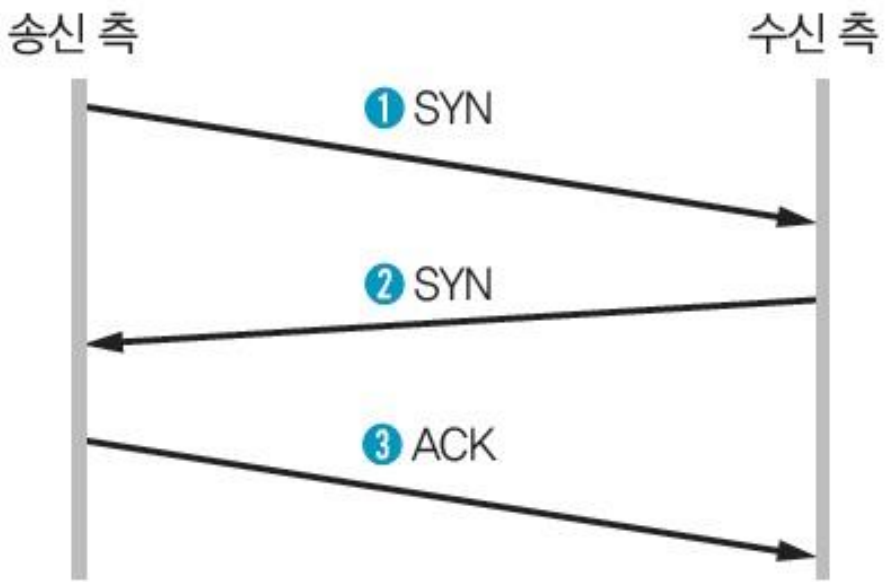
항목	길이	설명
발신지 포트(Source Port)	16	세그먼트를 보낸 호스트의 프로세스에 할당된 포트 번호
목적지 포트(Destination Port)	16	세그먼트를 받는 호스트의 프로세스에 할당된 포트 번호
순서 번호(Sequence Number)	32	세그먼트에 포함된 데이터의 첫 번째 바이트에 부여된 번호 표시. TCP는 신뢰성 있는 스트림 전달 프로토콜이므로 전달하는 바이트마다 번호 부여. 이 번호는 난수 발생기를 사용하여 초기 순서 번호를 만들고, 각 방향에 따라 다른 번호 사용. 순서 번호는 목적지 TCP에 세그먼트의 첫 번째 바이트가 이 순서 번호에 해당되는 바이트임을 알려줌
수신 확인 번호(Acknowledge Number)	32	상대편 호스트에서 받으려는 바이트의 번호 정의
헤더 길이(HLEN)	4	TCP 헤더의 길이를 4바이트 워드 개수로 표시
예약(Reserved)	6	나중에 사용하려고 예약한 필드

TCP 헤더의 항목

항목	길이	설명
플래그 비트	6	서로 다른 제어 비트 6개를 표시 • URG : 긴급 플래그 • ACK : 수신 확인 플래그 • PSH : 푸시 플래그 • RST : 리셋 플래그 • SYN : 동기화 플래그 • FIN : 종료 플래그
윈도 크기	16	송수신 측의 버퍼 크기. 16비트이므로 최대 크기는 65,535
체크섬(Checksum)	16	데이터를 포함한 세그먼트 전체의 오류를 검사하는 필드
긴급 포인터(Urgent Pointer)	16	긴급 데이터이므로 우선 처리하라고 수신 측에 알려주는 필드
옵션	32	최대 40바이트의 정보를 선택할 수 있고, 수신지에 추가 정보를 전달

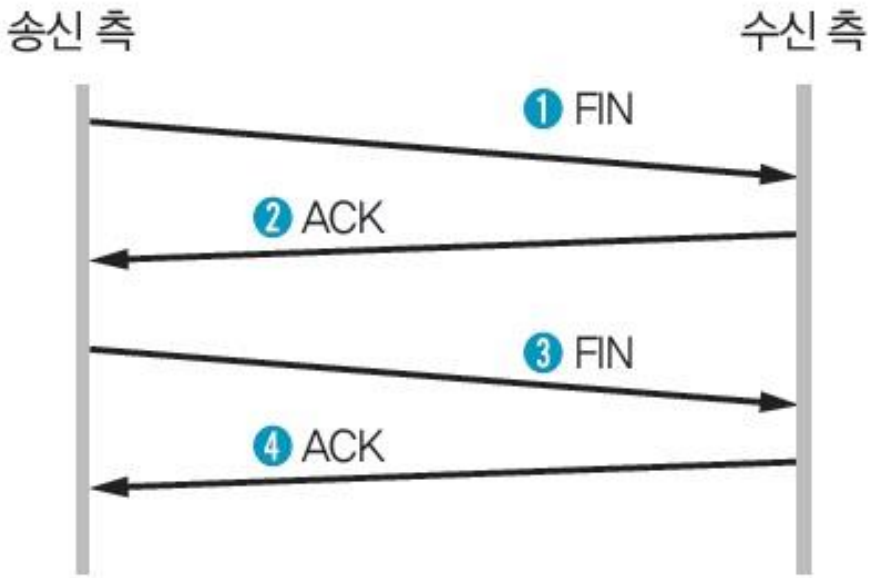
TCP의 연결 설정과 해제

- TCP는 송신 측과 수신 측을 서로 연결·설정하기 위해 신호를3 단계로 교환
  - ① 송신 측이 수신 측에 SYN 세그먼트를 보내 연결 설정을 요청
  - ② 수신 측이 송신 측에 수신 확인으로 SYN 세그먼트를 전송
  - ③ 송신 측이 수신 측에 응답 세그먼트의 확인 응답으로A CK를 보냄



TCP의 연결 설정과 해제

- TCP는 송신 측과 수신 측의 연결을 해제하기 위해 신호를4 단계로 교환
  - ① 송신 측이 수신 측에 FIN 세그먼트를 보내 연결 해제를 요청
  - ② 수신 측이 송신 측에 확인 응답으로 ACK 세그먼트를 전송
  - ③ 수신 측이 송신 측에 FIN 세그먼트를 전송하여 연결 해제를 요청
  - ④ 송신 측이 수신 측에 응답 세그먼트의 확인 응답으로 ACK를 보냄



TCP의 특징

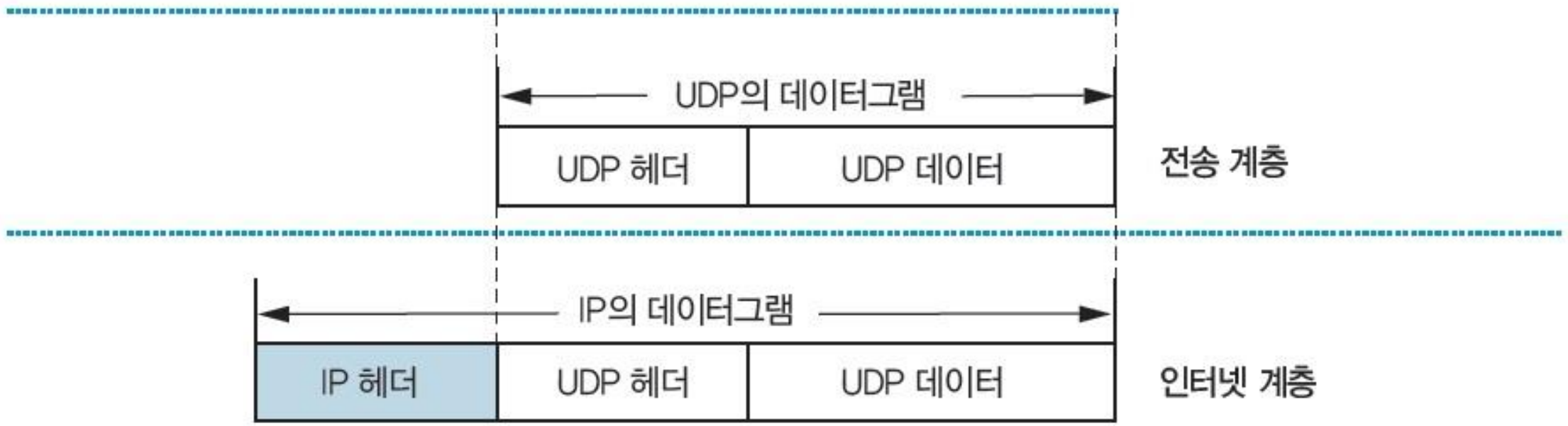
- 상위층이 넘겨준 데이터를 세그먼트 단위로 쪼개어 가공한 후 하위층으로 넘김
- 쪼개진 세그먼트에 순서를 부여한 후 전송·수신하여 순서가 뒤바뀌지 않게 함
- 순번이 뒤바뀌어도 다시 복구하여 상위층이 신뢰할 수 있는 연결 방식을 제공
- TCP의 연결지향형 방식을 스트림 서비스(Reliable Stream Service)라고도 함

UDP(User Datagram Protocol)

- 두 종단 간에 연결을 설정하지 않고 데이터를 교환하는 비연결형 프로토콜
- 사용자 데이터를 데이터그램에 포함해 전송

UDP의 캡슐화

- UDP 패킷은 인터넷과 라우터를 거쳐 전달되기 때문에 IP가 캡슐화하여 운반



UDP의 헤더 구조

UDP 헤더의 항목

항목	길이	설명
발신지 포트(Source Port)	16	데이터그램을 보낸 호스트의 프로세스에 할당된 포트 번호
목적지 포트(Destination Port)	16	데이터그램을 받는 호스트의 프로세스에 할당된 포트 번호
전체 길이(Total Length)	16	헤더와 데이터를 합한 사용자 데이터그램의 전체 길이로, 범위는 0~65,535
체크섬(Checksum)	16	데이터그램의 헤더와 데이터 전체의 오류 검사에 사용

UDP의 특징

- 수신 측이 데이터가 제대로 도착했는지 확인하지 않는 비신뢰성 서비스를 제공
- 매우 빠른 전달 서비스를 제공하는 대신 신뢰성이 없음

TCP와 UDP의 특징 비교

프로토콜의 기능	TCP	UDP
데이터 전송 단위	세그먼트	블록 형태의 데이터그램
서비스 형태	연결형	비연결형
수신 순서	송신 순서와 일치	송신 순서와 불일치
오류와 흐름 제어	있음	없음

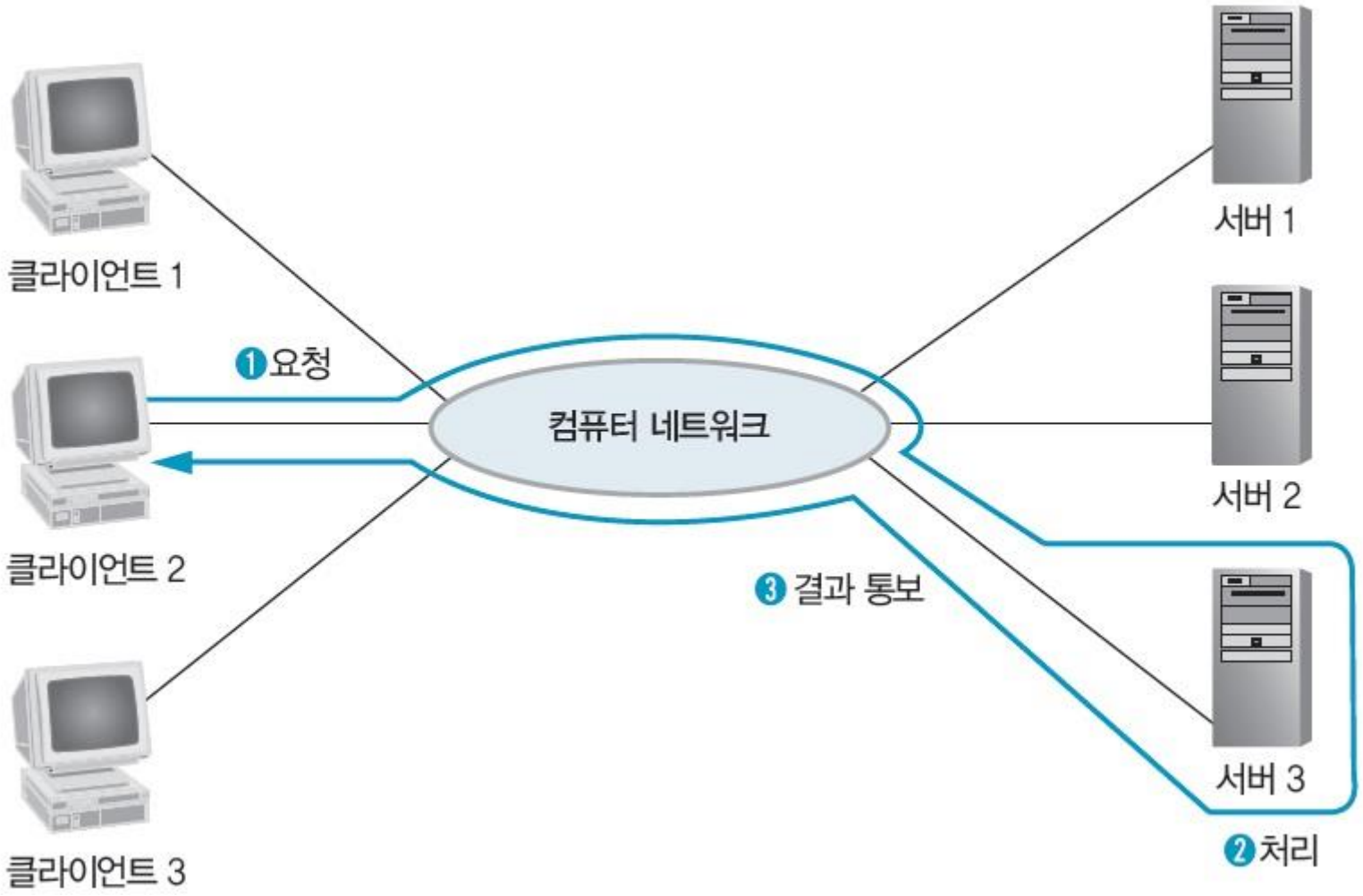
응용 계층 프로토콜

- 응용 계층 프로토콜의 대부분은 클라이언트와 서버 모델로 구현됨
- 클라이언트와 서버의 협동 처리(Cooperative Processing)를 통해 작업이 진행
- 클라이언트와 서버 모델은 연결 방식에 따라 연결형과 비연결형으로 분류
  - 연결형 : TCP/IP 프로토콜
  - 비연결혈 : UDP/IP 프로토콜을 사용

클라이언트와 서버 모델 동작 원리

- 대기 상태와 요청 : 서버 프로세스는 클라이언트의 요청을 기다리는 대기 상태, 클라이언트가 서버에 연결을 요청
- 처리 : 서버가 클라이언트의 요청에 해당하는 서비스를 처리
- 결과 통보 : 처리 결과를 클라이언트에 통보하는 응답을 함

클라이언트와 서버 모델 동작 원리



전송 계층의 프로토콜에 따른 응용 계층의 프로토콜 종류

전송 계층의 프로토콜	응용 계층의 프로토콜
TCP 사용	HTTP, FTP, 텔넷, SMTP 등
UDP 사용	SNMP 등

HTTP HyperText Transfer Protocol

- 인터넷에서 하이퍼텍스트 문서를 교환하는 데 사용하는 통신 규약
- 1989년 팀 버너스 리(Tim Berners Lee)가 처음 설계
- 인터넷을 이용한 월드 와이드 웹(WWW, World Wide Web)에 기반을 두고 전 세계적으로 정보를 공유할 수 있게 함
- ‘http://www...’는 www로 시작되는 URL인 인터넷 주소에서 하이퍼 텍스트 문서의 교환을 http 통신 규약으로 처리하라는 뜻
- HTTP의 특징
  - 웹(Web)에서 HTML 문서를 송수신하는 데 사용
  - 텍스트, 이미지, 멀티미디어 파일 등 다양한 형태의 데이터를 전송할 수 있음

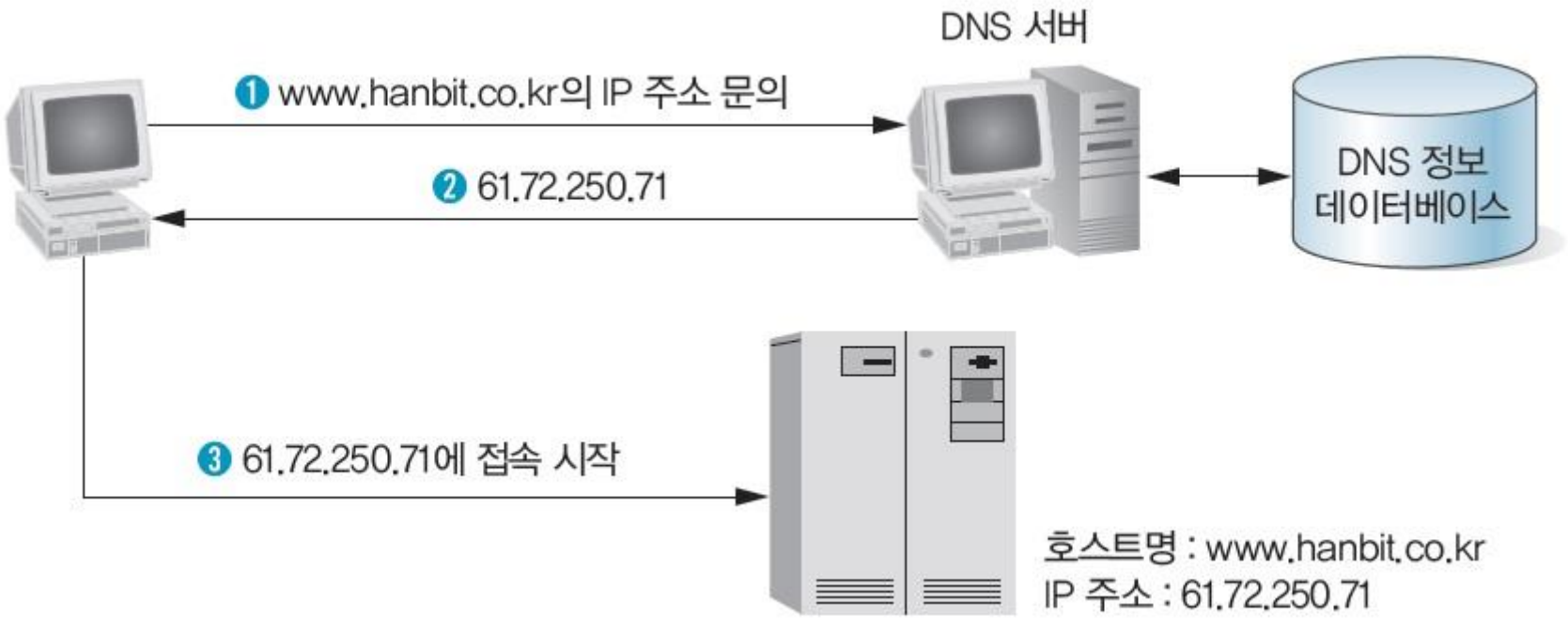
HTTP의 특징

- 웹(Web)에서 HTML 문서를 송수신하는 데 사용
- 텍스트, 이미지, 멀티미디어 파일 등 다양한 형태의 데이터를 전송할 수 있음

HTTP의 동작 원리와 예

- 클라이언트와 서버 방식을 이용
  - 클라이언트의 웹 브라우저가 서비스를 요구하면 하나의 TCP 연결을 생성
  - 웹 브라우저에서 요구한 URL 도메인명에 해당하는 컴퓨터 서버에 접근하여 URL 경로의 HTML 파일을 찾아 클라이언트에게 보여줌

도메인명을 IP 주소로 변환하는 과정



IP 주소를 받은 클라이언트의 웹 브라우저 동작 과정

① 웹 브라우저는 응답 받은 IP 주소에 포트 80번으로 TCP를 연결하여 설정

② 클라이언트가 설정된 연결을 이용해 '/book/test.html'을 요청하는 명령어를 보냄

③ www.hanbit.co.kr 서버가 test.html 파일을 클라이언트에 보냄

④ www.hanbit.co.kr이 TCP 연결을 해제

⑤ test.html을 수신한 웹 브라우저는 텍스트 정보를 먼저 보여주고 이미지 정보를 보냄

HTML과 보완 기술

- HTML은 텍스트 위주 웹 문서는 적합하지만 동적인 효과를 표현하기는 부적합
- 플래시(Flash), VRML(ViRtual Markup Language), 자바 애플릿, 자바 스크립트 등은 모두 HTML의 한계를 보완하려고 만든 기술

웹 브라우저와 웹 페이지

- 웹 브라우저 : HTML 언어로 생성된 문서를 읽을 수 있는 프로그램, 마이크로소프트의 인터넷 익스플로러를 가장 많이 사용
- 웹 페이지 : 웹에서 페이지 단위로 상호 연결된 HTML 형식의 웹 문서

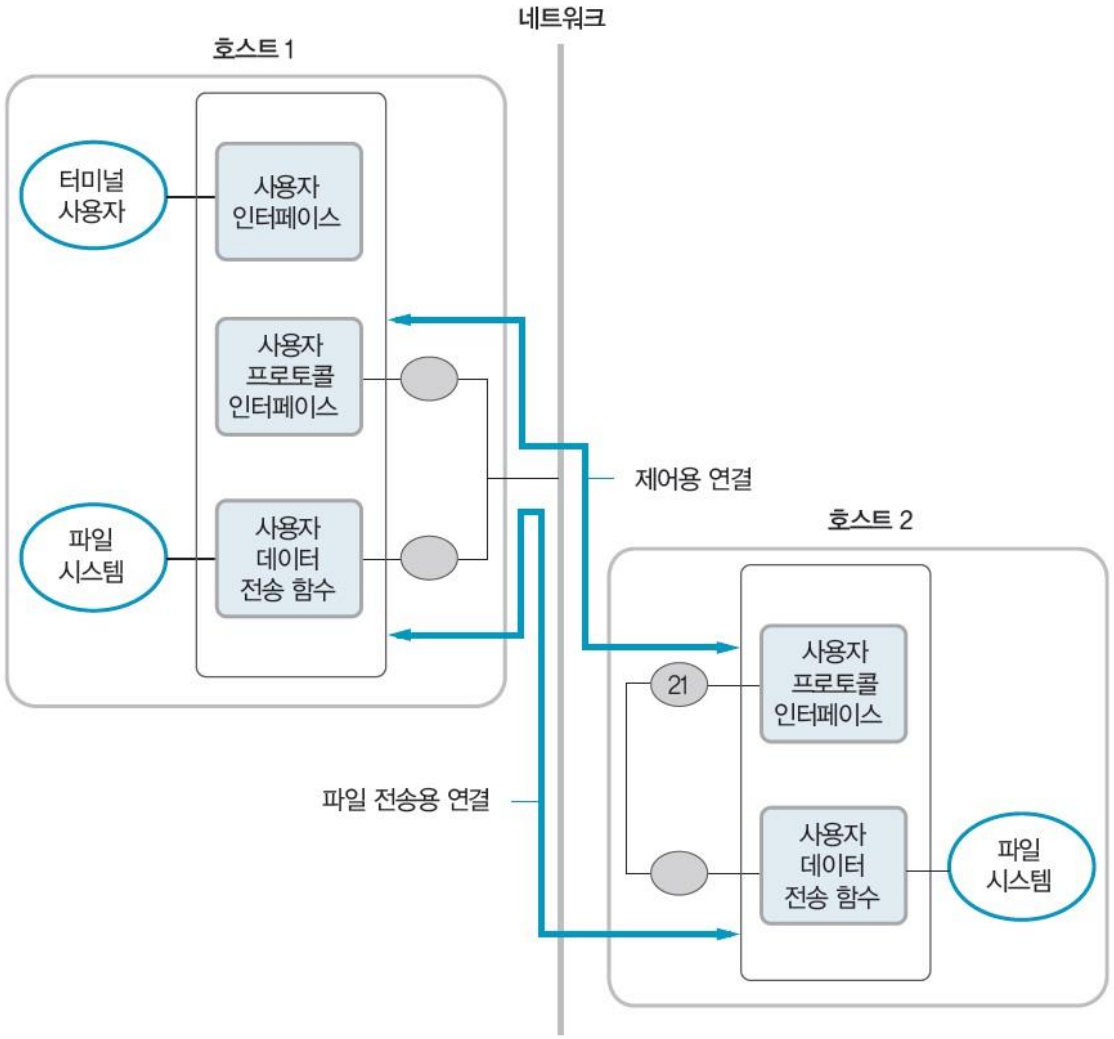
FTP File Transmission Protocol

- 파일을 효율적으로 주고받을 수 있는 파일 전송 프로토콜
- FTP의 특징
  - 원하는 프로그램이나 각종 데이터를 무료나 저렴한 가격에 살 수 있음
  - 용량이 큰 파일도 빠르게 송수신할 수 있음
  - 사용자로 등록하지 않고서도 익명 ID와 패스워드로 자신의 전자우편 주소를 설정하면 원격지 호스트에 접속하여 파일을 쉽게 송수신할 수 있음

FTP의 동작 원리와 예

- FTP는 두 개의 연결 중에서 하나는 파일 전송용, 다른 하나는 제어용으로 사용
- 파일 전송용 : 클라이언트 쪽에서 서버 쪽으로 파일을 전송할 때마다 생성해서 사용
- 제어용 : 클라이언트 쪽에서 서버 쪽으로 명령을 내리고 서버에 응답하려고 사용
  ① 서버는 FTP의 포트 21을 개방하고, 클라이언트가 접속하기 까지 대기
  ② 클라이언트는 연결 제어를 하기 위해 TCP 포트 21을 개방
  ③ 클라이언트는 연결된 제어를 이용해 파일 전송을 요청
  ④ 서버는 FTP의 21 포트로 클라이언트와 연결을 설정
  ⑤ 서버는 연결을 이용해 클라이언트에 파일을 전송
  ⑥ 파일 전송 후 서버는 연결을 해제
  ⑦ 원하는 파일을 전부 수신했으면 클라이언트는 연결을 해제
  ⑧ 서버는 다른 서비스 요청이 있을 때까지 잠시 대기

FTP의 동작 원리와 예


네트워크
호스트 1
터미널
사용자
사용자
인터페이스
사용자
프로토콜
인터페이스
파일
시스템
사용자
데이터
전송 함수
제어용 연결
호스트 2
21
사용자
프로토콜
인터페이스
파일 전송용 연결
사용자
데이터
전송 함수
파일
시스템

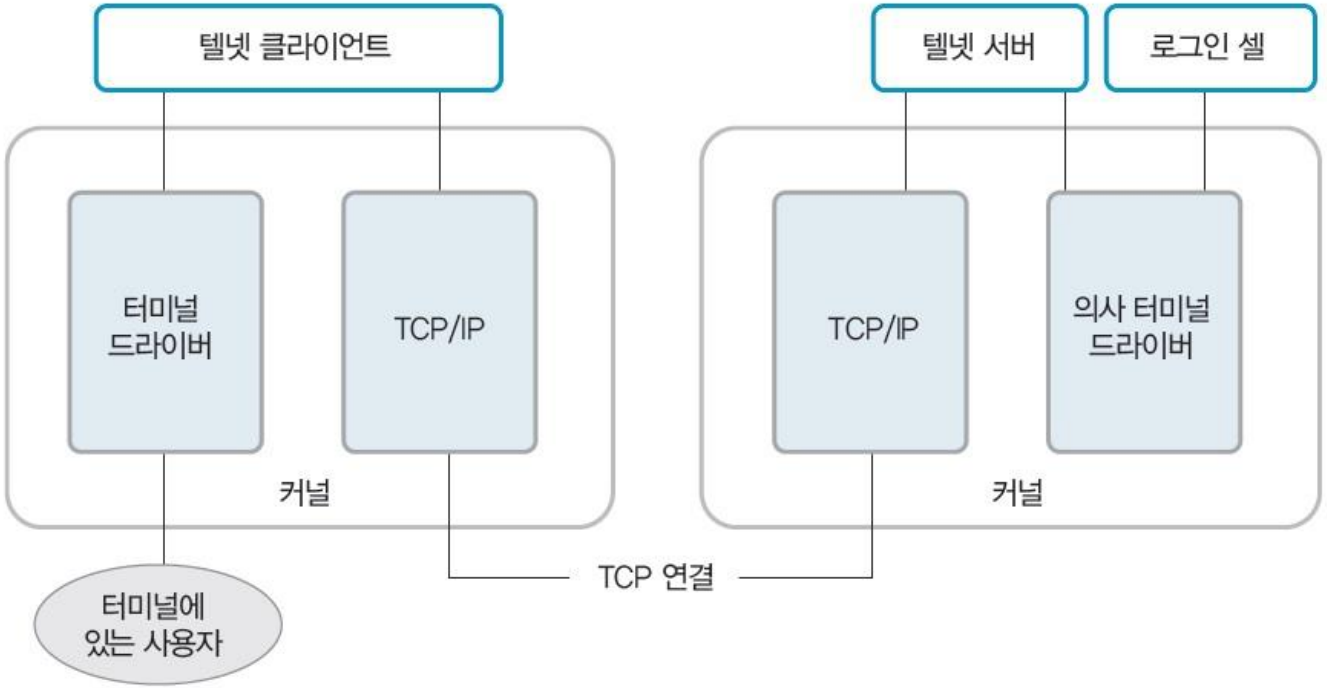
텔넷Telnet

- 원격지에서 컴퓨터를 이용한 가상 단말 기능을 구현하는 프로토콜
- 원격지에 위치한 호스트 컴퓨터를 로컬 컴퓨터처럼 사용할 수 있음

- 텔넷의 특징
  - 텔넷을 이용해 전 세계에 있는 다양한 온라인 서비스를 제공받을 수 있음
  - 클라이언트와 서버 모델을 사용
  - 서버는 의사 단말(Pseudo Terminal)로 처리

텔넷의 동작 원리와 예

① 터미널에 있는 사용자는 로그인하려는 호스트와 TCP 연결을 설정
② 서버는 연결을 이용해 사용자에게 가상의 터미널을 제공
③ 사용자는 가상의 터미널을 실제 터미널처럼 이용



SMTP Simple Mail Transfer Protocol

- 전자우편 서비스(E-mail Service)를 사용할 수 있는 프로토콜

- SMTP의 특징
  - 하위 계층에서 TCP 프로토콜을 사용
  - 전자우편 송수신을 위해 사용자 에이전트와 메시지 전송 에이전트를 사용
  - 전자우편 메시지가 통과하는 로컬 메인 시스템하고만 정보를 교환
  - 사용자의 메시지 접수방법, 사용자 인터페이스 구성방법, 사용자의 메시지 저장 방법 등은 지정하지 않음

SMTP 동작 원리와 예

① 송신 측에서 메일 명령(Mail Command) 수행

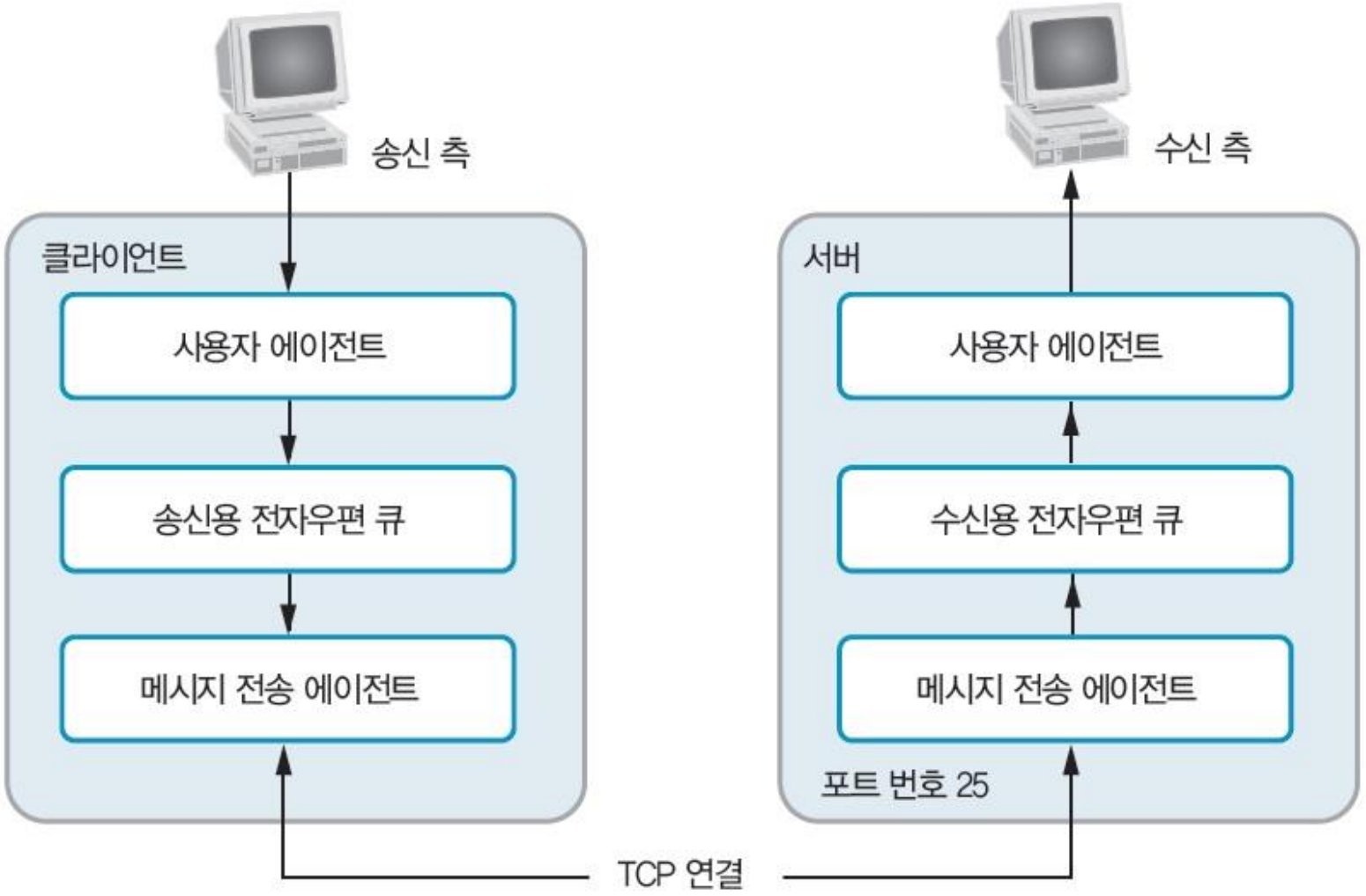
② 송신 측에서 SMTP에 규정된 전자우편 형식에 따라 내용을 작성

③ 송신 측에서 송신용 메일 큐나 스풀에 송신할 내용의 전자우편을 미리 저장

④ 송신 측에서 수신용 메일 큐에 전자우편이 있는지 검색하여, 있으면 헤더를 참조해 SMTP 규정에 따라 수신 측으로 발송

⑤ 수신 측에서 수신용 메일 큐에 전자우편이 있으면 전자우편을 읽음

SMTP 동작 원리와 예


송신 측
수신 측
클라이언트
사용자 에이전트
송신용 전자우편 큐
메시지 전송 에이전트
서버
사용자 에이전트
수신용 전자우편 큐
메시지 전송 에이전트
포트 번호 25
TCP 연결

SNMP Simple Network Management Protocol

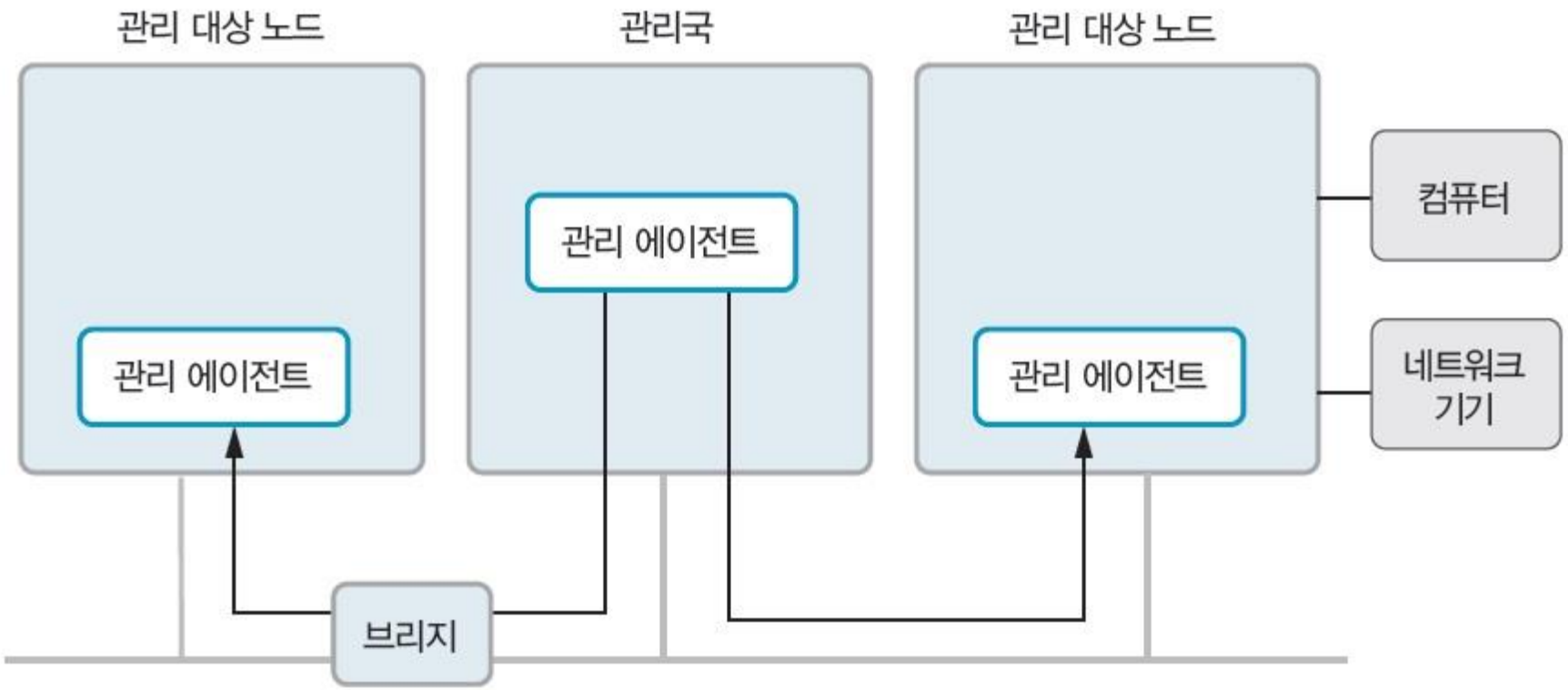
- 인터넷에서 네트워크를 관리하는 프로토콜
- 네트워크 관리 정보를 교환하는 데 사용

- SNMP의 특징
  - 관리자 프로세스와 관리 프로세스 간에 정보를 주고받을 수 있는 기능만 지원하므로, 자신을 통과하는 관리 정보는 알 수 없음
  - SNMP는 하위 계층에서 UDP 프로토콜을 사용

SNMP의 동작 원리와 예

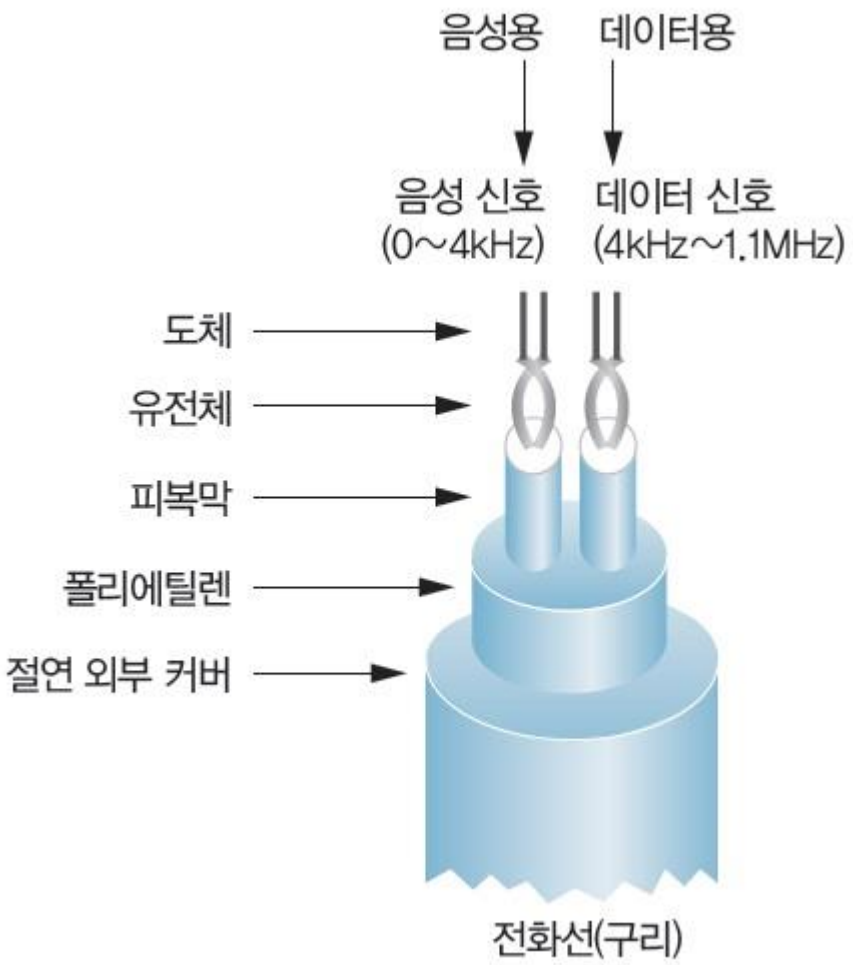
- 관리국이 에이전트에서 관리 정보를 가져오고 설정하며, 오류 등 이상이 발생하면 에이전트가 관리국에 알리는 일련의 과정
  - 관리 에이전트 : 관리국과 관리 대상 노드에 있고, 기기의 상태나 이력 공간인 데이터베이스를 관리하며, 기기의 조작에도 영향을 줌
  - 관리국 : 관리 에이전트와 SNMP 프로토콜로 통신, 관리 대상 노드의 상태를 조회하고 변경시킬 수 있음
  - 관리 대상 노드 : 일종의 디바이스로 관리 에이전트가 동작하는 공간, 호스트, 프린터, 라우터, 브리지 등 외부에 상태 정보 통신 능력이 있음

SNMP의 동작 원리와 예



xDSL(x Digital Subscriber Line)

- 일반 전화망의 주파수 대역 중 사용하지 않는 대역을 고속으로 데이터를 전송하는 데 사용하는 새로운 전송 기술



xDSL의 역사

- 우리나라는 1997년부터 xDSL 기술을 개발

연도	설명
1972년	미국 AT&T 벨연구소에서 DMT(Discrete MultiTone) 변복조 기술 특허
1980년	미국에서 V.38 변복조 기술로 ISDN 기술 개발
1988년	미국에서 2B1Q(2-Bit 1-Quaternary) 변복조 기술로 HDSL(High-bit-rate Digital Subscriber Line) 기술 개발
1989년	미국 벨코어(Bellcore)에서 xDSL 기술 개발
1990년	인터넷 기술과 함께 xDSL 기술 부각
1992년	ANSI에서 xDSL의 QAM(Quadrature Amplitude Modulation)/CAP(Carrierless Amplitude Phase Modulation)/DMT 기술 표준화
1993년	ANSI에서 RADSL(Rate Adaptive Digital Subscriber Line) 기술 표준화

전송속도에 따른 xDSL의 분류

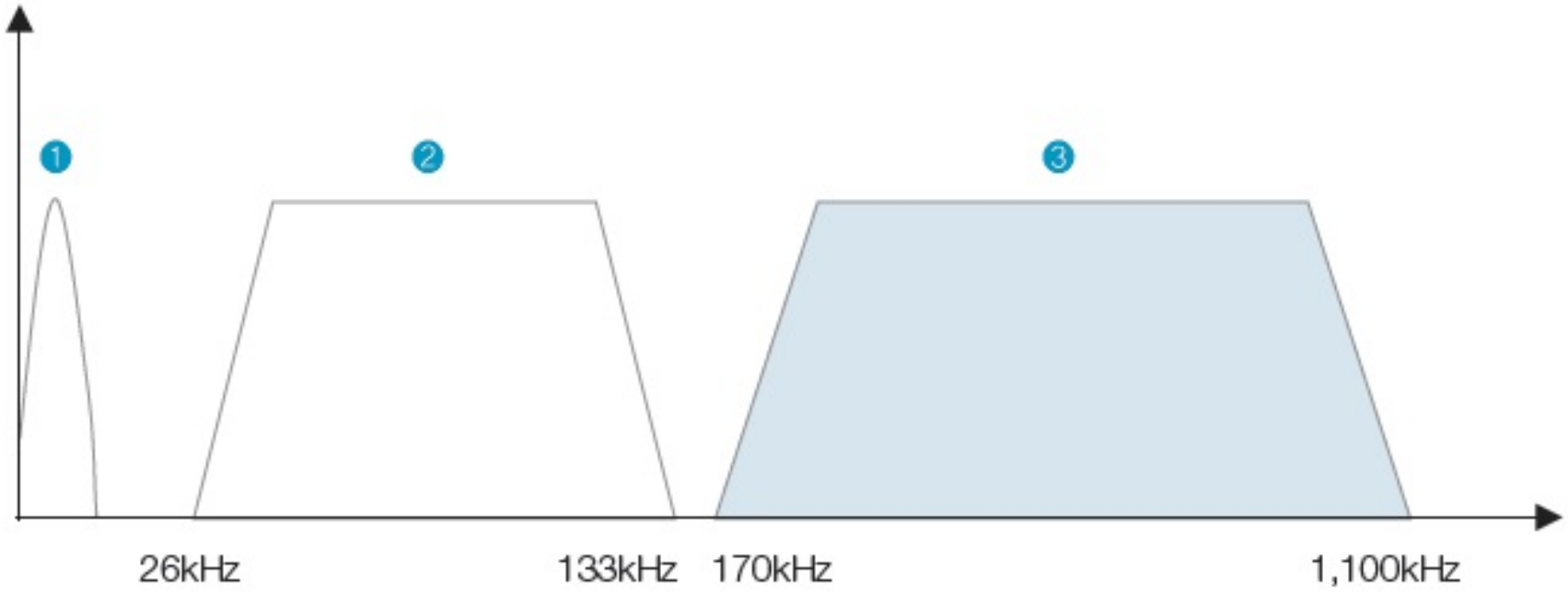
- 보통 대칭형보다 비대칭형 기술을 더 많이 사용

종류	설명
SDSL(Symmetric DSL) : 대칭형 디지털 가입자 회선	• 데이터의 전송속도는 양방향이 똑같은 대칭형 • 원격교육과 화상회의 등에서 연결용으로 주로 사용
MSDSL/MDSL(Multirate DSL) : 다중률 디지털 가입자 회선	• SDSL보다 수신속도 향상
HDSL(High-bit-rate DSL) : 고속 디지털 가입자 회선	• 영국의 통신회사 BT가 개발한 2B1Q 방식의 기술을 바탕으로 개발 • 데이터의 전송속도는 양방향이 똑같은 대칭형
ADSL(Asymmetric DSL) : 비대칭형 디지털 가입자 회선	• 한 전화회선에서 전화는 낮은 주파수를, 데이터는 높은 주파수를 사용 • 데이터의 전송속도는 양방향이 다른 비대칭형 • 정보 검색이나 대량의 데이터 수신에 적합
RADSL(Rate-Adaptive DSL) / UADSL (Universal ADSL) : 속도 적응 비대칭형 디지털 가입자 회선/보급형 비대칭형 디지털 가입자 회선	• 데이터의 전송속도가 양방향이 다른 비대칭형 • 전화회선의 전송속도를 조절할 수 있는 소프트웨어가 있음 • 웨스텔(Westell)의 ADSL 기술
VDSL(Very-high speed DSL) : 초고속 디지털 가입자 회선	• 비교적 가까운 거리에 더 빠른 속도를 보장하는 기술 • 1991년 미국에서 광섬유와 동축 케이블을 혼합한 망에서 고속의 인터넷 서비스를 제공하려고 개발 • 범용성은 떨어지나 ATM 장비 등 트렁크에 주로 연결 • VoD, HDTV, 대화형 멀티미디어 서비스 등에 주로 이용

변조 방식에 따른 xDSL의 분류

종류	설명
QAM	• 직교 진폭 변조 방식, 1980년대 중반 미국의 AT&T 벨연구소에서 최초로 개발 • ANSI와 ETSI 등에서 표준으로 채택
CAP	• 1993년 미국 AT&T의 벨 아틀랜틱에서 최초로 상용화한 방식, 30kHz~1MHz의 고주파 대역을 변복조함 • ADSL에서 음성은 3~4kHz, 데이터는 1.1MHz까지 전송하기 때문에 전화나 데이터 서비스를 동시에 사용할 수 있음
DMT	• 미국 스탠포드 대학교에서 개발한 ADSL의 선로 부호 방식의 일종 • 1993년 미국 벨코어에서 최초로 상용화, 1995년 ADSL의 변복조 방식으로 전송하는 다중 반송파 변조 방식
2B1Q	• 영국의 통신회사 BT가 개발한 변조 기술로, 단형파의 진폭을 변조하여 보내는 방식 • 속도가 대칭되는 전송 장비 등에 사용하는 디지털 전송 방식
DWMT	• DMT 기술과 비슷하며, 다중 반송파 변조 방식 • 초고속 디지털 가입자 회선(VDSL)에 사용

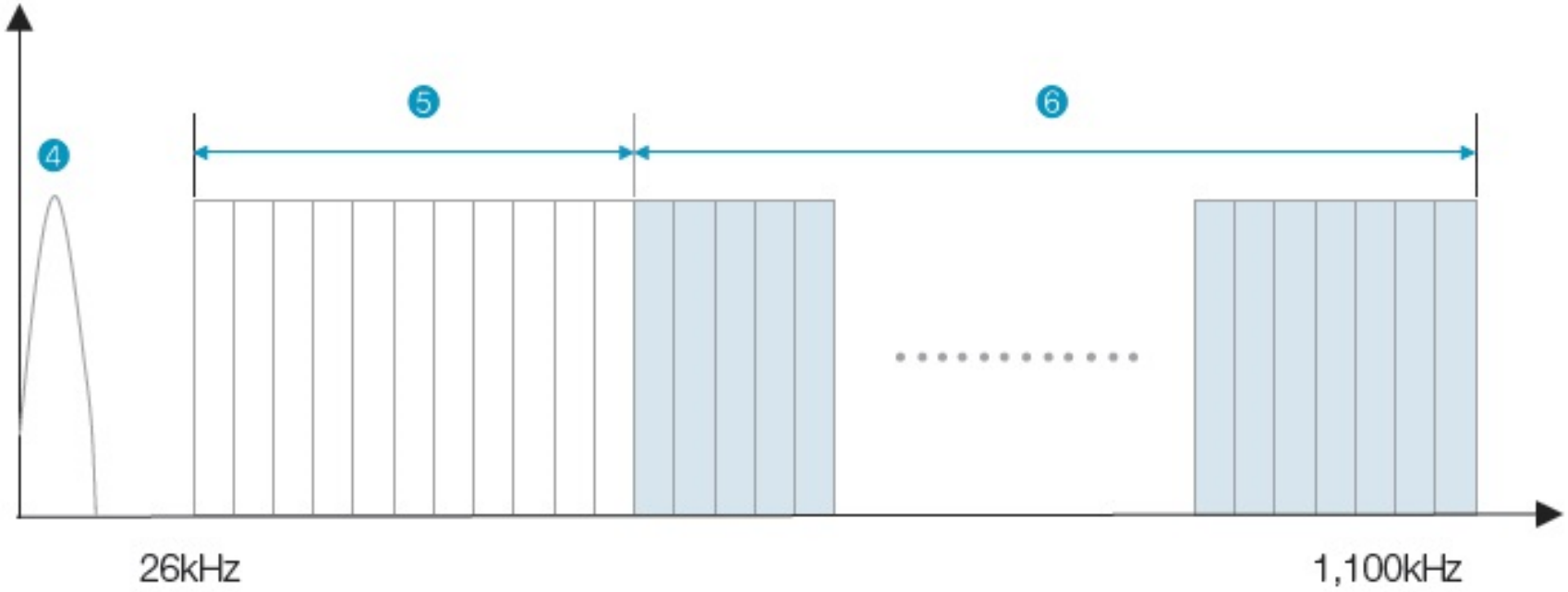
xDSL니 회선의 변복조 방식(CAP)



❶ 음성전화대역(POTS)
❷ 상향 데이터 전송 대역(Upstream)
❸ 하향 데이터 전송 대역(Downstream)

(a) CAP 방식

xDSL니 회선의 변복조 방식(DMT)



4 음성전화대역(POTS)
5 상향 데이터 전송 대역(Upstream)
6 하향 데이터 전송 대역(Downstream)

(b) DMT 방식

부가가치망VAN, Value Added Network

- 회선을 직접 보유하거나 통신사업자의 회선을 임차(또는 이용)하고 단순히 전송하는 기능 이상의 부가가치를 부여하여, 음성이나 데이터 정보를 제공하는 데이터 통신망
- 1973년 미국 연방통신위원회(FCC)가 프로토콜을 변환할 수 있는 패킷 교환 서비스를 사업으로 인가하면서 등장
- Telenet과 Tymnet 등이 여기에 해당
- 패킷 교환 방식을 사용
- 일본에서는 1985년 실현됨

VAN의 기능

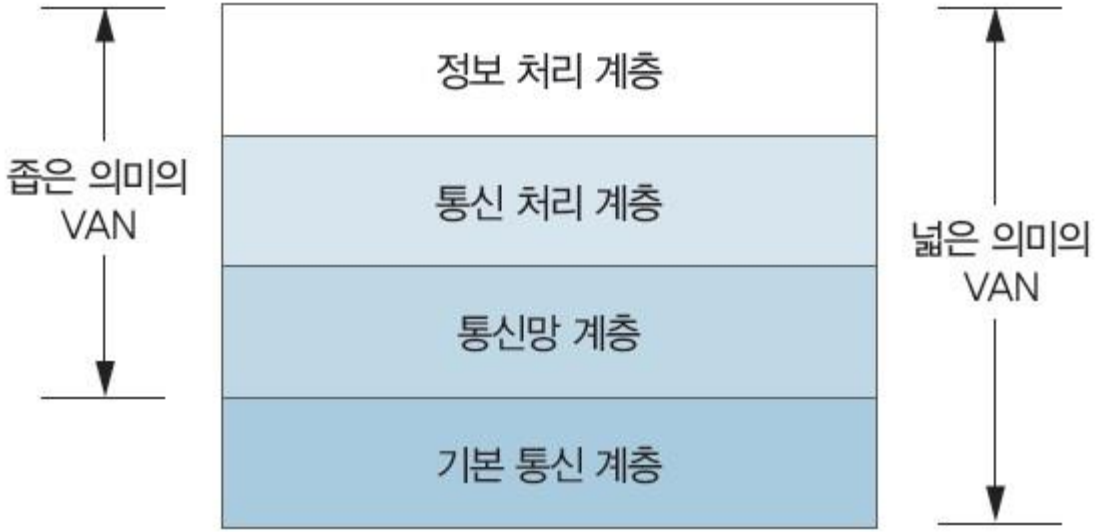
기능	설명
전자사서함	상대방이 부재 중일 때 메시지 몇 개를 통신망에 일시적으로 축적하였다가 나중에 송신
데이터 교환	데이터의 축적 기능을 이용해 송수신자 사이의 데이터 교환 수행
동보통신	축적 기능을 이용해 단말기 여러 개나 모든 단말기에 메시지를 동시에 송신
정시 집신	VAN이 정보 송신국에서 정해진 시간에 정보를 꺼냄
송신 기능	VAN에 축적되어 있는 정보를 수신국에 송신

VAN의 사용 목적

- 다른 업종이나 기업 간의 접속으로 새로운 사업을 발굴하려는 목적에서 이용
- 데이터 통신의 효율성 향상과 통신 비용 절감
- 회선을 확장하거나 운용하려는 목적

VAN의 계층 구조와 기능

- 정보 처리 계층 : 응용 서비스를 제공하는 계층, 재고 관리, 구매 관리, 급여 관리 등을 처리
- 통신 처리 계층 : 통신 과정에서 축적 교환, 속도 교환, 미디어 변환 등을 수행, 회선의 접속, 각종 제어 절차 등 프로토콜 변환 기능도 수행
- 통신망 계층 : 통신 방식을 규정한 계층으로, 패킷 교환 방식 사용



VAN의 서비스 범위

전송	전송/교환		부가가치 통신	정보 검색	정보 처리
전용회선	회선 교환	패킷 교환, 메시지 교환	메시지 축적	데이터베이스 서비스, 비디오텍스 서비스	정보 처리 서비스
			코드/프로토콜 변환		

좁은 의미의 VAN 서비스

넓은 의미의 VAN 서비스

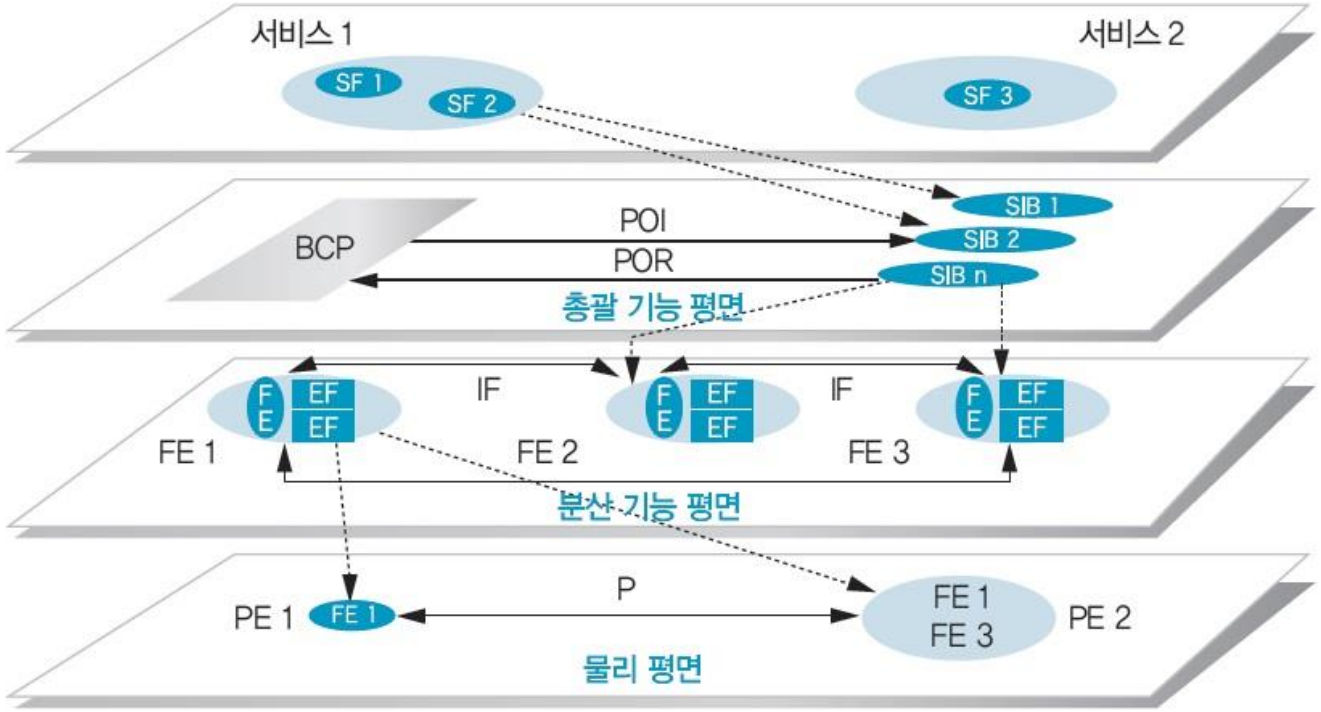
지능망(IN, Intelligent Network)

- 기존 통신망에 No.7 공통선 신호망을 이용해 컴퓨터와 고속 대용량의 데이터베이스를 접속한, 수직적 망 개념을 도입한 것
- 통신망 유형에 따라 PSTN, PSDN, N-ISDN, B-ISDN 등 다양한 망에 적용 가능
- 1984년 미국 AT&T에서 분리된 BOC(Bell Operating Company)가 독자적인 데이터베이스를 구축하여 800 서비스를 제공하면서 시작됨

지능망의 구조

- 지능망의 개념 모델은 지능망 구조를 설계하는 프레임워크로, 평면 4개로 구성
- 서비스 평면 : 사용자 관점의 서비스, 사용자에게 보여지는 것처럼 망이 제공하는 서비스 관련 행위를 인식
- 총괄 기능 평면 : 지능망을 하나의 실체로 모형화
- 분산 기능 평면 : 지능망을 분산 개념으로 모형화
- 물리 평면 : 지능망에 물리적 특질을 모형화, 실제 지능망에 있는 물리실체와 프로토콜을 규정

지능망의 개념 모델



- SF : Service Flow
- BCP : Basic Call Process
- POI : Point Of Initiation
- POR : Point Of Return

---------- ► 포인터

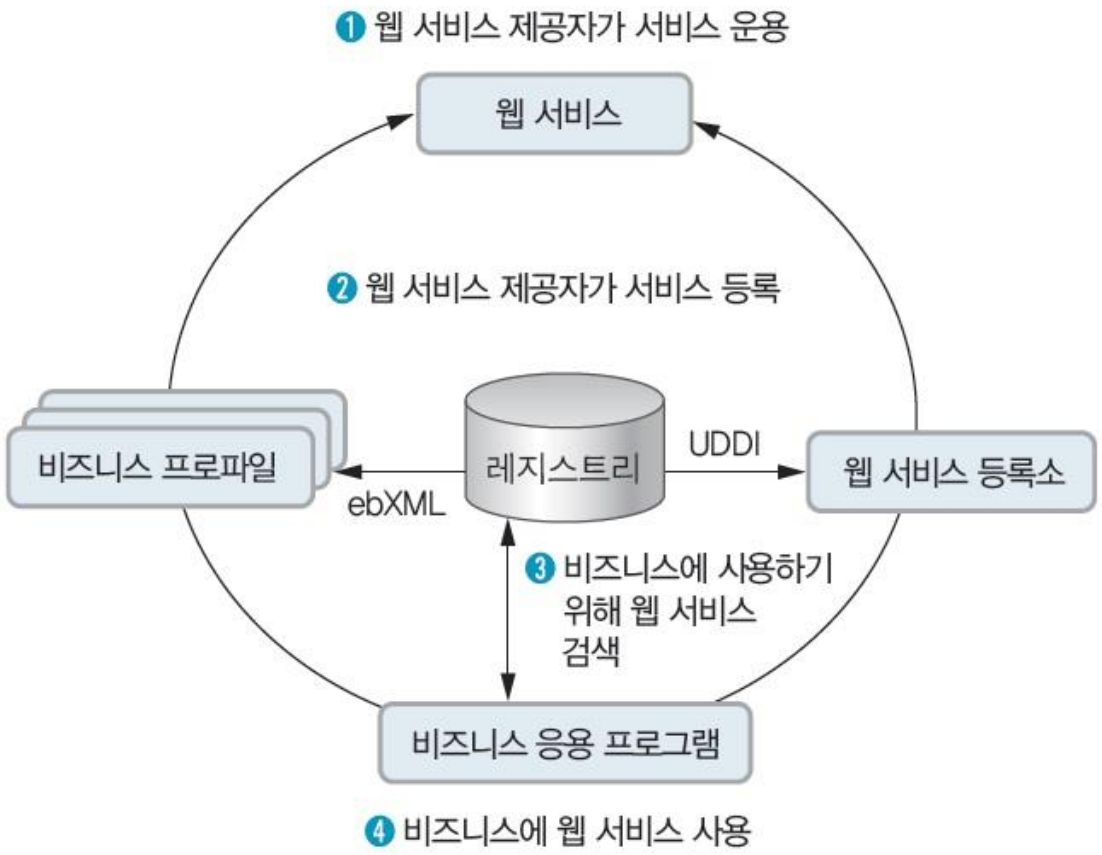
- SIB : Service Independent Building block
- FE : Functional Entity
- EF : Elementary Function
- PE : Physical Entity
- P : Protocol

지능망의 구성 요소

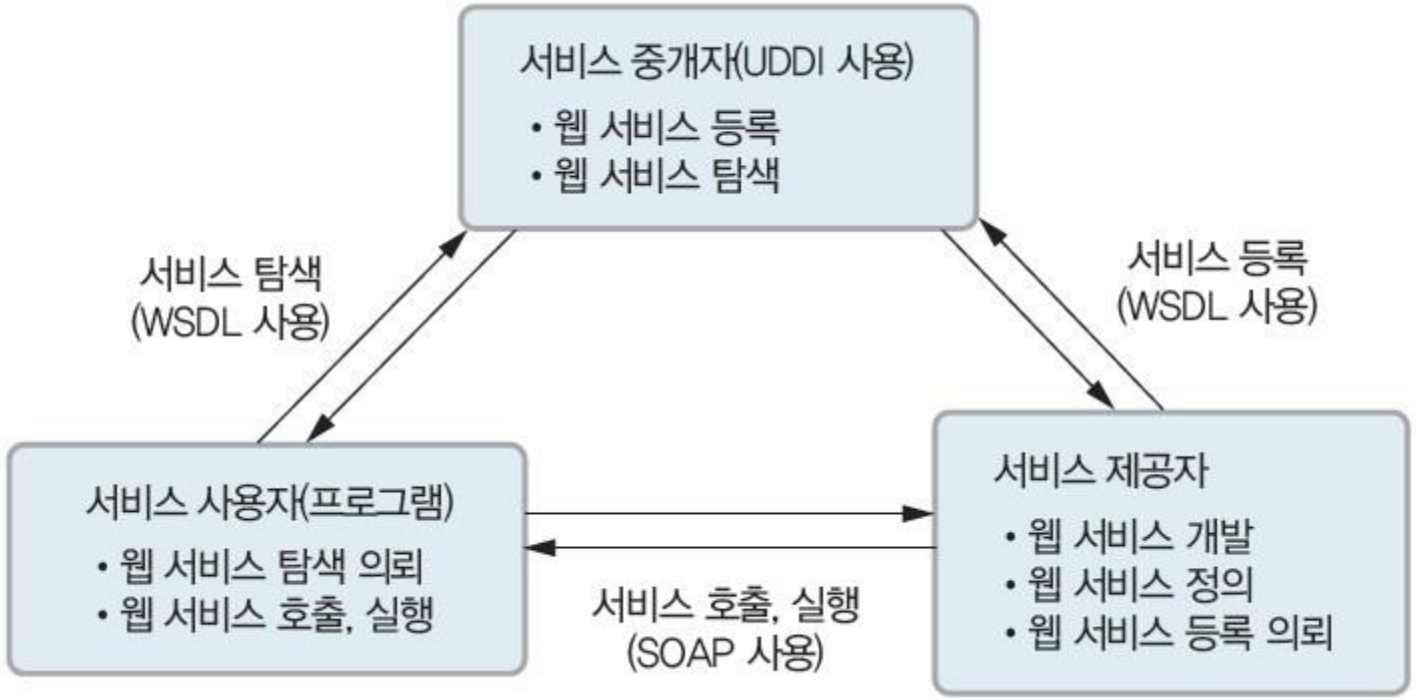
구성요소	역할
서비스 제어 시스템 (SCP, Service Control System)	지능망 서비스의 가장 중요한 요소이다. 서비스를 제공하는 서비스 로직과 서비스와 관련된 데이터를 가지고 있다. 예를 들면, 가입자에 대한 정보를 저장하고 있다.
서비스 관리 시스템 (SMS, Service Management System)	서비스 관리 기능을 수행한다.
서비스 교환기 (SSP, Service Switching System)	서비스 이용자와 지능망 사이를 연결하는 특수한 형태의 전자 교환기이다.
No.7 공통선 신호망	SCP와 SSP 사이의 정보를 전달하는 데 사용되는 프로토콜이며 ITU-T에서 제정하였다.

웹 서비스(Web Service)

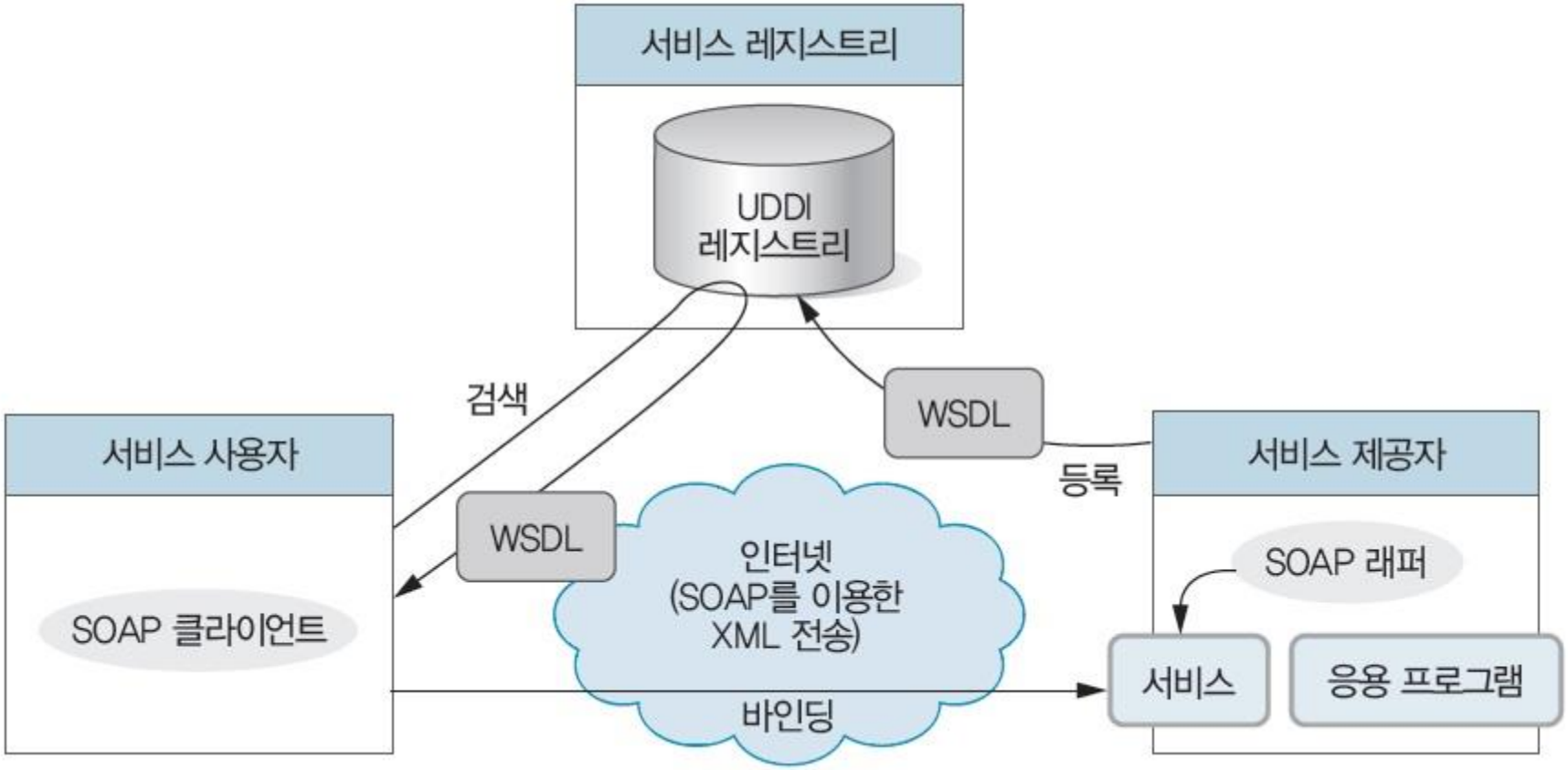
- 여러 시스템을 플랫폼에 독립적으로 연계하고, 통합과 자원을 공유할 목적으로 만든 표준화된 웹 기술
- 근간이 되는 기술로는 XML, SOAP, UDDI, WSDL 등이 있음
- 모든 메시지를 XML로 변환하여 상호 운용성이 높음



웹 서비스의 구성요소


서비스 중개자(UDDI 사용)
• 웹 서비스 등록
• 웹 서비스 탐색
서비스 탐색
(WSDL 사용)
서비스 등록
(WSDL 사용)
서비스 사용자(프로그램)
• 웹 서비스 탐색 의뢰
• 웹 서비스 호출, 실행
서비스 호출, 실행
(SOAP 사용)
서비스 제공자
• 웹 서비스 개발
• 웹 서비스 정의
• 웹 서비스 등록 의뢰

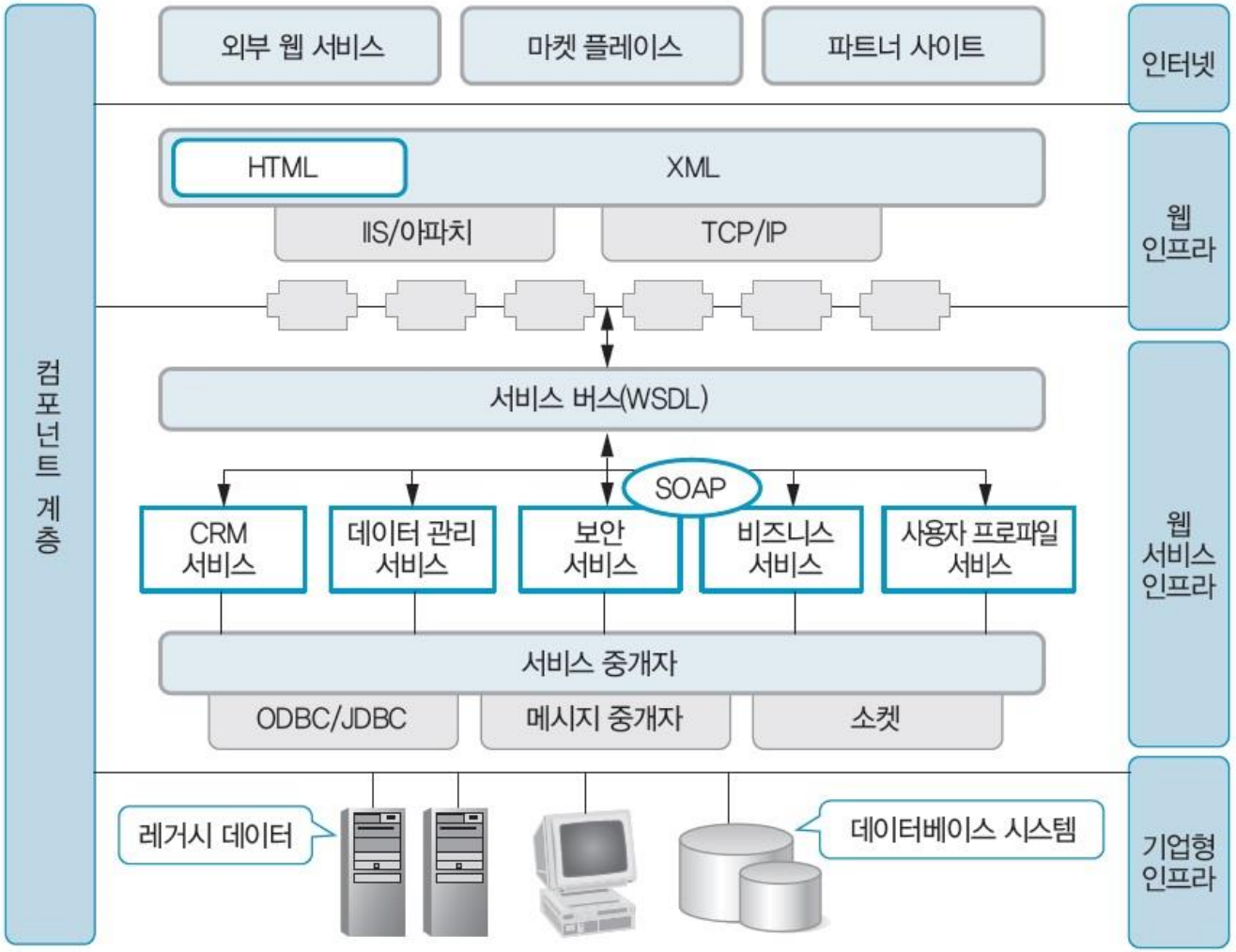
웹 서비스의 동작 원리


서비스 레지스트리
UDDI
레지스트리
검색
WSDL
등록
서비스 사용자
서비스 제공자
WSDL
인터넷
(SOAP를 이용한
XML 전송)
SOAP 래퍼
SOAP 클라이언트
서비스
응용 프로그램
바인딩

웹 서비스의 동작 원리

- SOAP(Simple Object Access Protocol)
  - HTTP, HTTPS, SMTP 등을 사용해 XML 형식의 메시지를 컴퓨터 네트워크에서 교환하는 프로토콜
  - 웹 서비스에서 기본 메시지를 전달하는 기반이 됨
  - 보통 원격 프로시저 호출(RPC, Remote Procedure Call) 메시지 패턴
  - XML을 근간으로 헤더와 바디를 조합하는 디자인 패턴으로 설계
- UDDI(Universal Description, Discovery and Integration)
  - 인터넷에 있는 전 세계 비즈니스 목록에 자신을 등재하는 XML 기반의 레지스트리
- WSDL(Web Services Description Language)
  - 특정 비즈니스가 제공하는 서비스를 설명하고, 개인이나 회사가 그 서비스에 전자적으로 접근하는 방법을 제공할 때 사용하는 XML 기반 언어
  - 마이크로소프트, IBM, 아리바(Ariba) 등이 주도한 UDDI의 기본이라고 할 수 있음

웹 서비스의 계층 구조

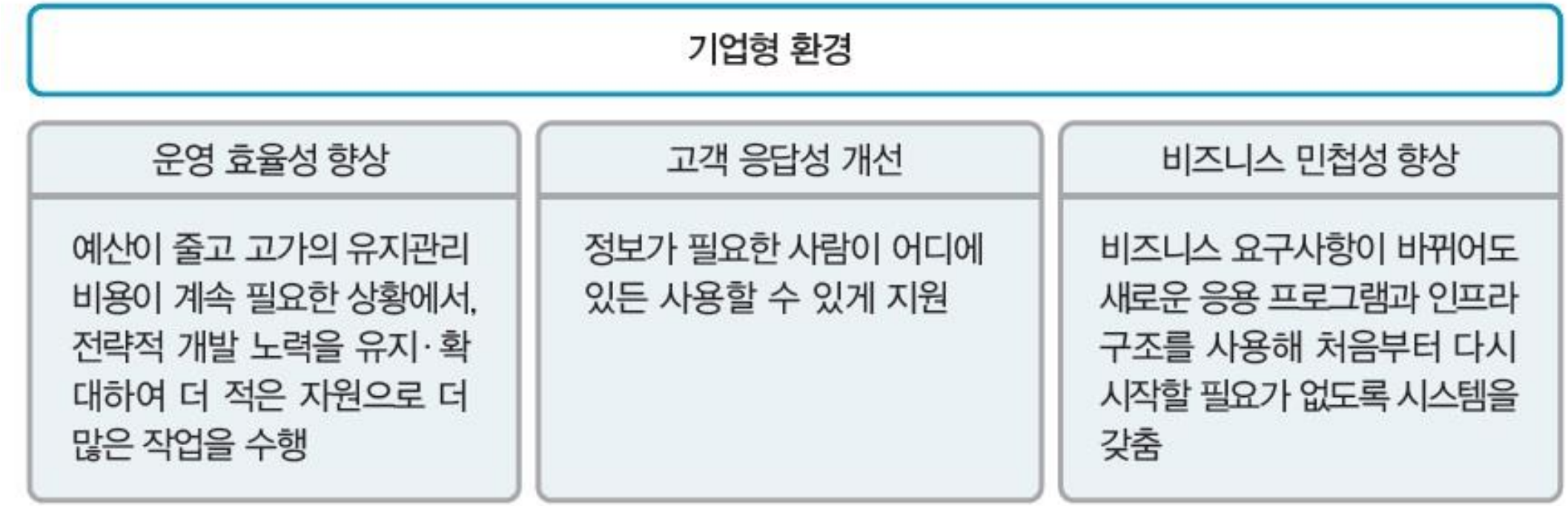

컴포넌트 계층
외부 웹 서비스
마켓 플레이스
파트너 사이트
인터넷
HTML
XML
IIS/아파치
TCP/IP
웹 인프라
서비스 버스(WSDL)
SOAP
CRM 서비스
데이터 관리 서비스
보안 서비스
비즈니스 서비스
사용자 프로파일 서비스
웹 서비스 인프라
서비스 중개자
ODBC/JDBC
메시지 중개자
소켓
레거시 데이터
데이터베이스 시스템
기업형 인프라

웹 서비스의 진화

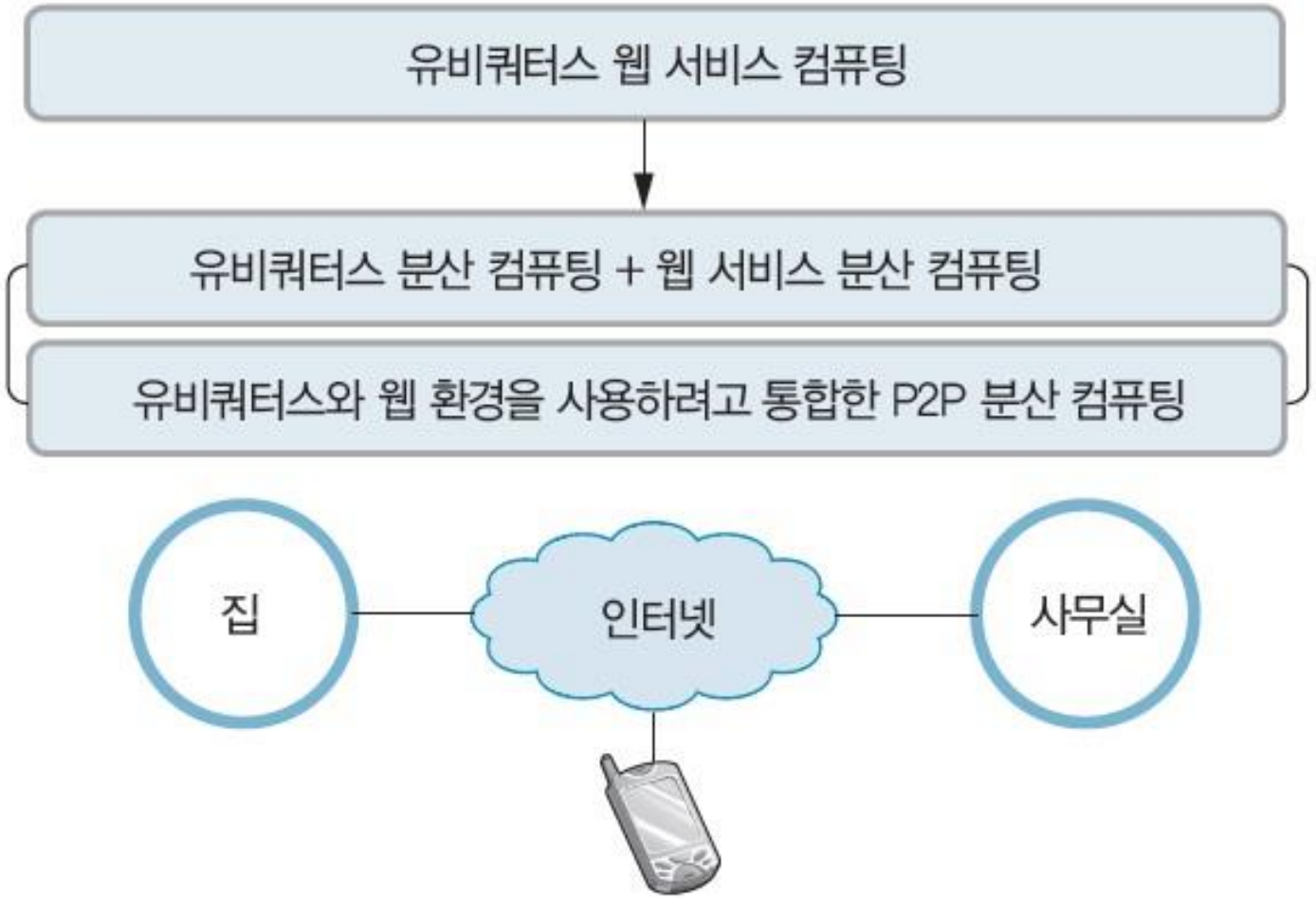
구성요소	주요 적용 기술	
제1세대 : 웹 서비스의 출현	• 웹 브라우저를 기반으로 이용 • 사용자 중심	• 콘텐츠, 응용 프로그램 지향 • URL을 이용해 수동으로 접근
제2세대 : 현재의 웹 서비스	• 응용 프로그램을 기반으로 이용 • 사용자, 응용 프로그램 중심	• 서비스 지향 • 레지스트리를 이용한 검색, 바인딩
제3세대 : 시맨틱 웹 서비스	• 에이전트를 기반으로 이용 • 사용자, 응용 프로그램 기반	• 목적 지향 • 온토폴로지 기반의 서비스 검색, 실행, 조합

SOA(서비스 지향 아키텍처)

- 기업형 응용 프로그램에 포함된 개별 기능을 서비스 지향적으로 분리하여 동적 비즈니스 요구사항에 따라 신속하게 조립하고 재사용해 상호 운영할 수 있도록 표준 기반 서비스로 구성하는 IT 전략



유비쿼터스 웹 서비스 컴퓨팅



XML

- CGI(Common Gate Interface) 언어
  - 서버와 외부 데이터, 응용 프로그램 간의 인터페이스
  - 사용자와 이용 시간대에 따라 내용과 표현이 달라지는 동적인 정보를 다룸
- 마크업 언어(Markup Language)
  - 웹 서버에 저장된 문자, 그림, 표, 음성, 동영상 등을 포함한 문서를 클라이언트가 내려받아 웹 브라우저에 표현할 때 사용
  - SGML → HTML 순으로 발전
  - XML은 SGML과 HTML의 단점을 보완해 등장한 언어

XML

- SGML
  - 기기나 처리 시스템에 독립적, 문헌을 구조화시켜 내용이 물리적인 형태와 별도로 유지
  - 융통성 있고 확장이 가능하며 다양한 응용에 사용할 수 있음
  - 기능이 복잡해 SGML을 지원하는 소프트웨어를 개발하기 쉽지 않음
- HTML
  - 표준 웹 언어
  - 단순성, 이식성, 사용의 용이성이라는 장점이 있음
  - 태그 집합이 제한적이라 문서의 다양한 특성을 반영할 태그가 충분치 않음
- XML
  - 1996년 W3C에서 제안
  - 단순하고, 구조성과 융통성을 유지하면서 확장이 가능해 HTML보다 표현력이 좋음
  - SGML의 실용적인 기능만 모은 부분집합이라고 할 수 있음

SGML, HTML, XML의 비교

구분	SGML	HTML	XML
등장 시기	1986년	1991년	1998년
목적	정보의 구조화	정보의 표현	정보의 구조화
문법	엄격하고 복잡	느슨	엄격하나 단순
사용 가능한 태그	확장 가능	확장 불가능	확장 가능
정보 검색	트리 검색	텍스트 검색	트리 검색
재사용	쉬움	매우 어려움	쉬움

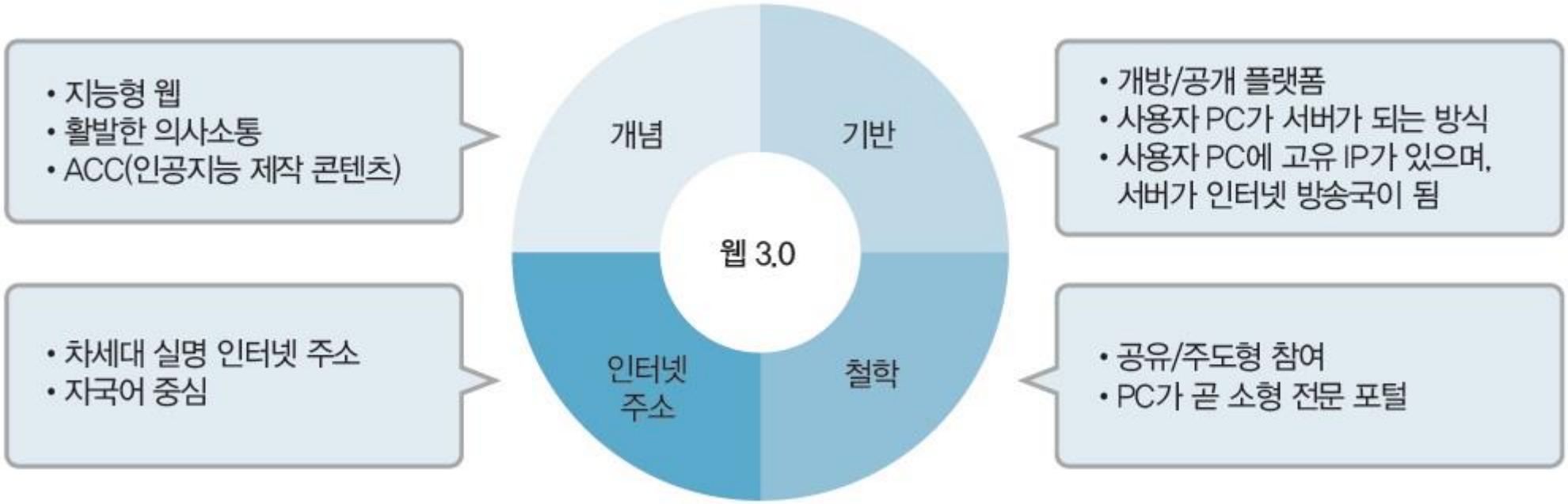
AJAX(Asynchronous JAvascript and XML)

- 대화식 웹 응용 프로그램을 제작하려고 여러 기술을 조합하여 만든 웹 개발 기법
- 비동기 자바스크립트와 XML을 의미
- 웹에 있는 DHTML, CSS, XML과 마이크로소프트 객체인 XMLHttpRequest 기술을 합쳐 만든 것
- 웹 페이지의 사용성, 접근성, 응답성이 향상됨
- DHTML, 자바스크립트, CSS 등 기존 웹 기술을 그대로 이용할 수 있음

웹의 진화

구분	1995년~2000년	2005년~2010년	2015년~2020년
	WWW	웹 2.0	웹 3.0
의사소통	일방적(단방향 정보 제공)	고정 공간, 즉 포털에서 양방향 정보 제공	자유로움
콘텐츠	생산 주체가 사용자에게 일방적으로 제공	사용자 스스로 참여	웹 자체가 지능화되어 사용자가 원하는 정보 제공
검색	검색엔진 내부에서만 가능	여러 사이트에 있는 자료 개방 (오픈 API)	사용자 맞춤형 검색

웹의 진화


• 지능형 웹
• 활발한 의사소통
• ACC(인공지능 제작 콘텐츠)
개념
기반
• 개방/공개 플랫폼
• 사용자 PC가 서버가 되는 방식
• 사용자 PC에 고유 IP가 있으며, 서버가 인터넷 방송국이 됨
웹 3.0
• 차세대 실명 인터넷 주소
• 자국어 중심
인터넷 주소
철학
• 공유/주도형 참여
• PC가 곧 소형 전문 포털

지능형 웹 서비스

- 시맨틱 웹 에이전트 기술을 웹 서비스에 접목하는 시도
- 컴퓨터가 이해할 수 있는 형태의 새로운 언어로 표현해 기계끼리 의사소통을 할 수 있는 지능형 웹

시맨틱 웹

- 인간을 대신하는 에이전트(로봇이나 인공지능일 수 있음)가 인간의 질문을 이해하고, 방대한 정보를 검색하고 편집한 후 적절한 답안을 스스로 추론하여 제공하는 것이 목표인 시스템

시맨틱 웹의 구성 요소

- 시맨틱 웹 언어
  - 시맨틱 웹 언어 표준이 주로 구문 구조(Syntax) 위주로 정의되어 있음
  - 앞으로는 구문 구조에 의미(Semantics)를 부여하는 방향으로 연구해야 함
- 기반 구조
  - 프로토콜이나 전송 방법 등을 의미
- 온톨로지
  - 시맨틱 웹에서 가장 중심에 있는 개념
  - 응용 프로그램이 통신할 때 단어에서 동의를 이끌어내는 데 중요
- 휴먼 인터페이스
  - 사용자 인터페이스 : 시맨틱 웹 기술을 이용해 사람이 통신하는 소프트웨어와 하드웨어를 의미
  - 조직 인터페이스 : 그룹 사이의 상호작용에 필요한 인터페이스를 의미

모바일 웹

- 스마트폰을 비롯한 고성능의 휴대폰에서 시작
- 모바일 웹의 표준화가 매우 중요한 과제

미래의 인터넷

- 인터넷 환경과 모바일 기기의 진화로 웹 세상과 현실세계의 경계가 없어질 것
- 특히 증강현실(AR, Augmented Reality)기술은 우리 신체와 현실을 확장할 예정