TCP/IP Network Protocols
제2장 – 인터넷의 동작 절차 이해

박승철교수
한국기술교육대학교

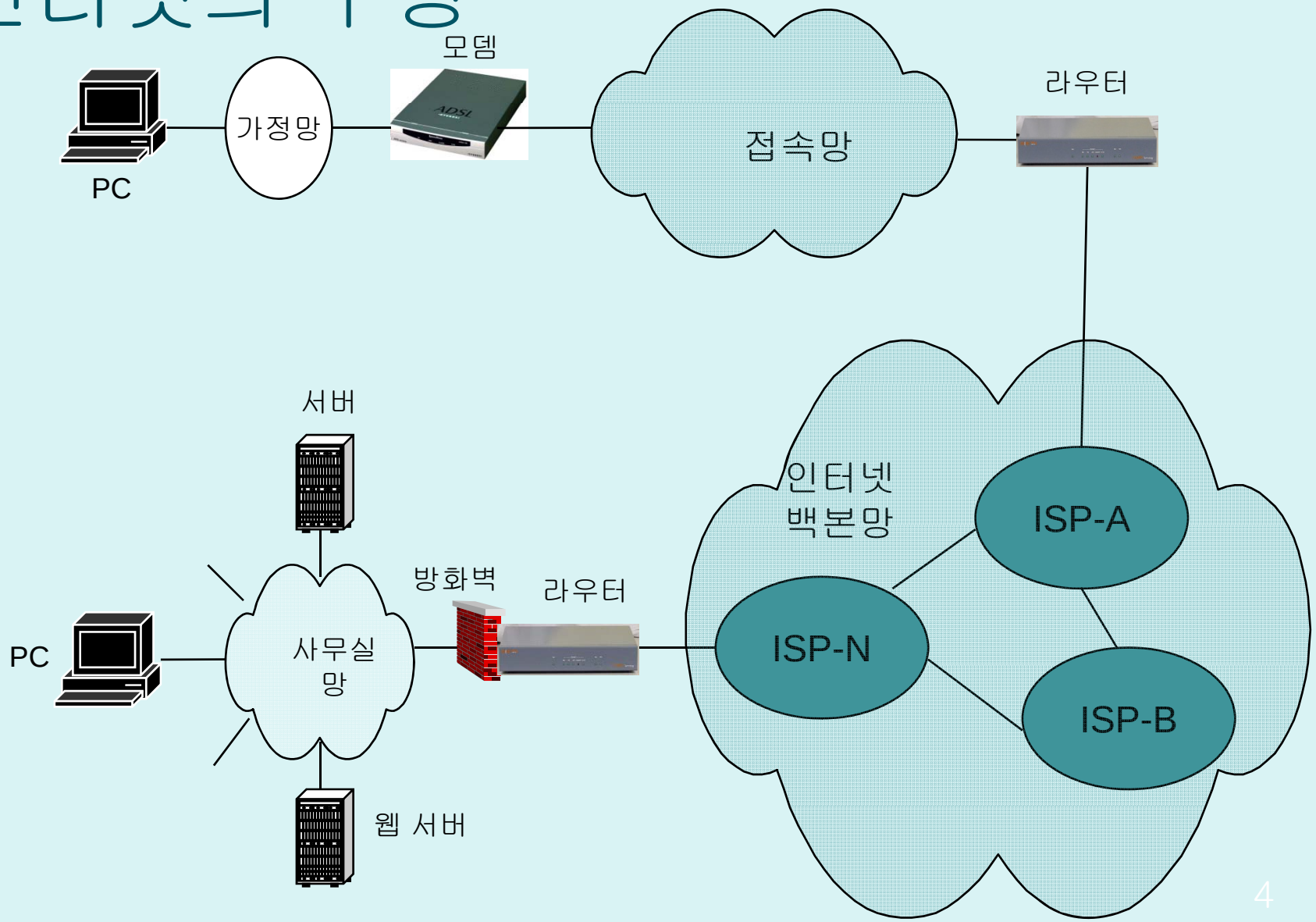
제2장의 강의 목표

- 인터넷을 구성하는 호스트와 데이터 통신망들이 인터넷 서비스를 제공하기 위해 동작하는 절차를 전반적으로 이해하고
- 인터넷에서 사용되고 있는 프로토콜들의 연관 관계를 이해하고
- 호스트-접속망-백본망-사무실망의 데이터 전달 절차를 이해함
-

제2장의 구성

- 개요
- 인터넷 서비스를 위한 호스트의 동작 절차
  - HTTP에 의한 웹 페이지 전송
  - TCP에 의한 신뢰적인 데이터 전송
  - IP에 의한 인터넷 데이터 전달
- 인터넷 서비스를 위한 접속망의 동작 절차 : DSL 접속망
  - 접속망의 데이터 전달 과정
  - DSL 모뎀과 DSLAM에 의한 데이터 전송
- 인터넷 서비스를 위한 백본망의 동작 절차
  - 인터넷 백본망의 데이터 전달 과정
  - 인터넷의 지연시간과 데이터 손실
  - 인터넷의 차등화된 데이터 전달
- 인터넷 서비스를 위한 사무실망의 동작 절차
  - 이더넷 기반 사무실망의 데이터 전달 과정
  - 스패닝 트리 프로토콜
  - 방화벽과 인터넷 보안
  - 웹 서버 접속

인터넷의 구성


모뎀
라우터
PC
가정망
ADSL
접속망
서버
인터넷
백본망
ISP-A
방화벽
라우터
PC
사무실
망
ISP-N
ISP-B
웹 서버

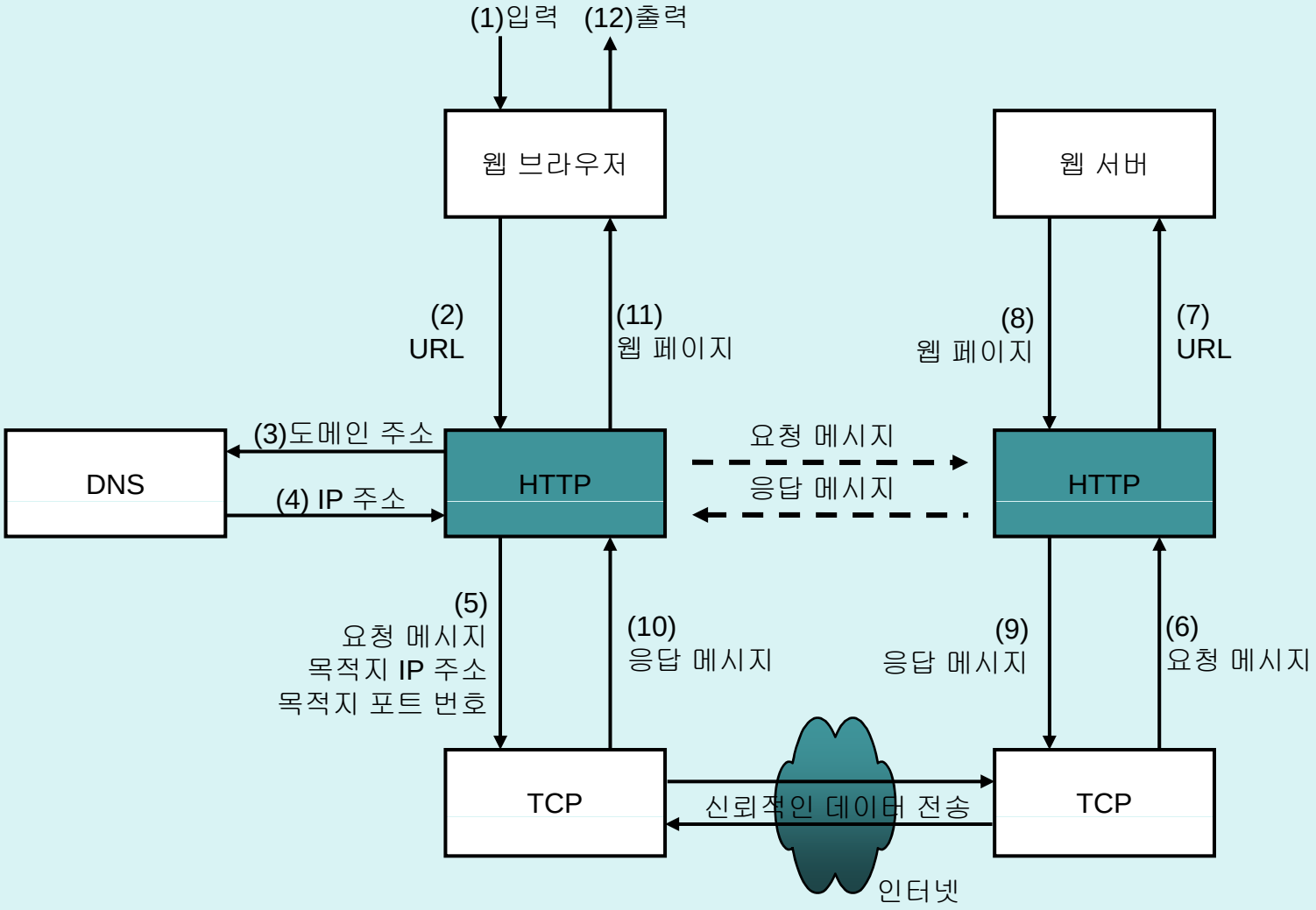
개요

- 접근 방법
  - 특정 인터넷 서비스(웹 서비스) 실현을 위해 인터넷을 구성하는 요소들이 상호 작용하는 과정 소개함으로써 인터넷의 전반적인 동작 원리를 이해할 수 있게 함
- 인터넷에서의 통신
  - 특정 표현 방식으로 실시간으로 생성되거나 미리 저작되어 일정한 장소(서버) 저장되어 있는 정보를 정해진 규약에 따라 신속하고 안전하게 제공 받는 것
- 인터넷 응용 서비스
  - 인터넷 통신을 응용하여 사용자에게 제공하는 서비스
  - 웹 서비스, 파일 전송 서비스, 이메일 서비스, 인터넷 전화, 화상 회의, VoD, IPTV 등

개요

- 응용 프로토콜(Application Protocol)
  - 사용자가 특정 유형의 정보를 인터넷을 통해 효율적으로 이용할 수 있도록 정의한 정보 전송 규칙
  - 응용 서비스를 위해 교환할 정보의 유형과 정보 교환 절차를 정의
  - 응용 프로토콜 정보 유형 : 사용자 정보(데이터) + 제어 정보
- 응용 프로토콜 종류
  - 웹 서비스 : HTTP(Hyper Text Transfer Protocol)
  - 파일 전송 서비스 : FTP
  - 이메일 서비스 : SMTP, POP3
- 웹 서비스를 중심으로 인터넷 동작 절차 설명
  - 웹 브라우저가 웹 서버를 접근하기까지의 전체 과정을 설명함으로써 인터넷의 전반적인 동작 절차를 이해하고자 함.

HTTP에 의한 웹 페이지 전송 절차



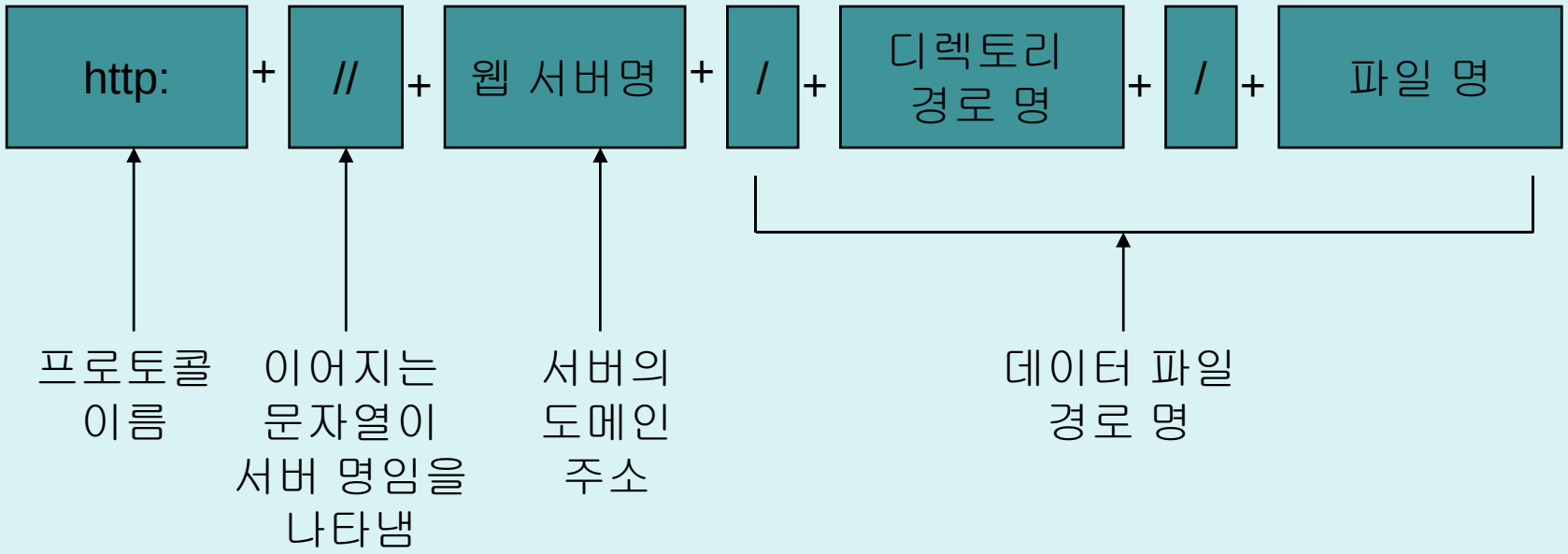
HTTP(Hyper Text Transfer Protocol)

- HTTP의 역할
  - 웹 브라우저와 웹 서버간에 교환할 메시지의 유형과 메시지 교환 절차를 정의한 프로토콜
- HTTP 메시지
  - 요청 메시지(Request Message)
  - 응답 메시지(Response Message)
- 요청 메시지
  - 웹 페이지의 URL
  - 요청의 종류(method)
  - 처리 가능 미디어와 문자 집합 정보 등 제어 정보
- 응답 메시지
  - 웹 페이지와 제어 정보

HTTP(Hyper Text Transfer Protocol)

- TCP(Transmission Control Protocol) 사용
  - HTTP 메시지를 신뢰적으로 전송하기 위해 TCP를 사용
  - TCP가 HTTP를 구분할 수 있도록 포트 번호(Port Number) 사용
- DNS(Domain Name System) 사용
  - 도메인 주소를 IP 주소로 변환하기 위해 DNS 사용

URL(Uniform Resource Locator)

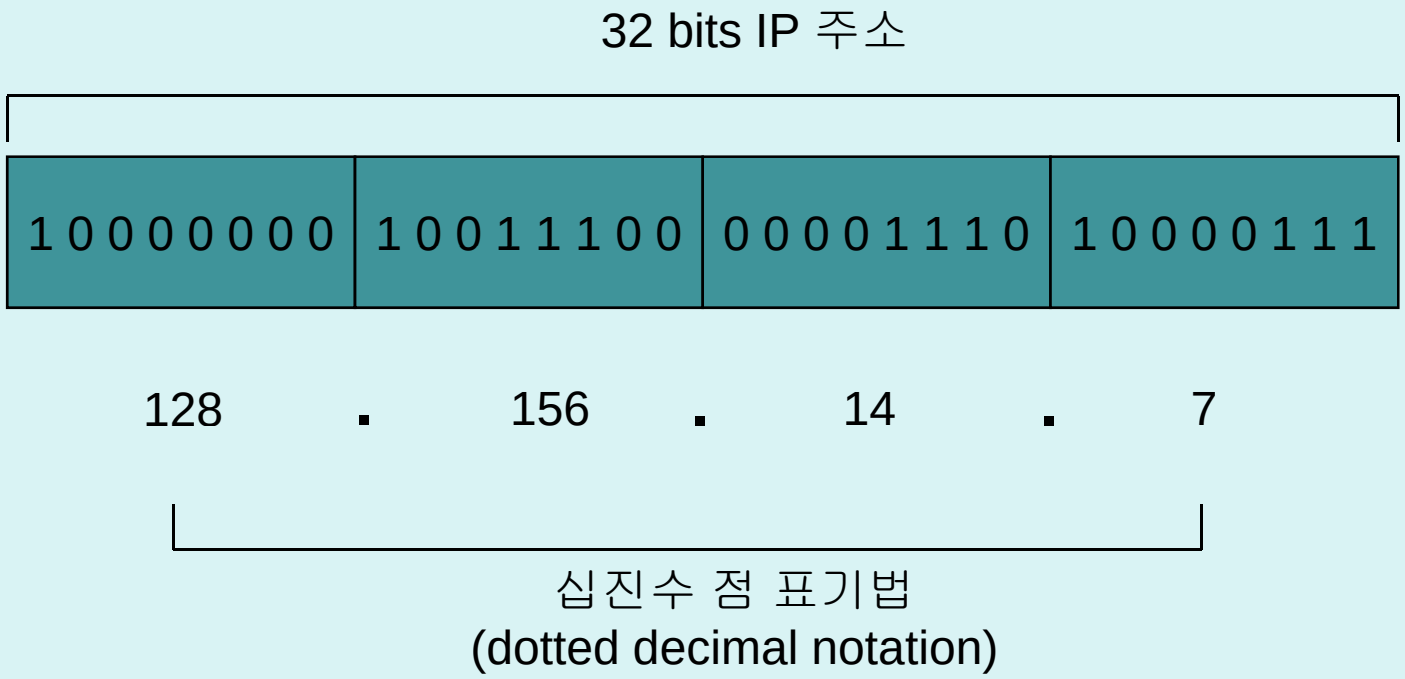


예 : http : // www.kut.ac.kr / Admission / html / index.php

한국기술교육대학교
웹 서버 도메인 명

한국기술교육대학교 웹 서버내
특정 파일 경로 명

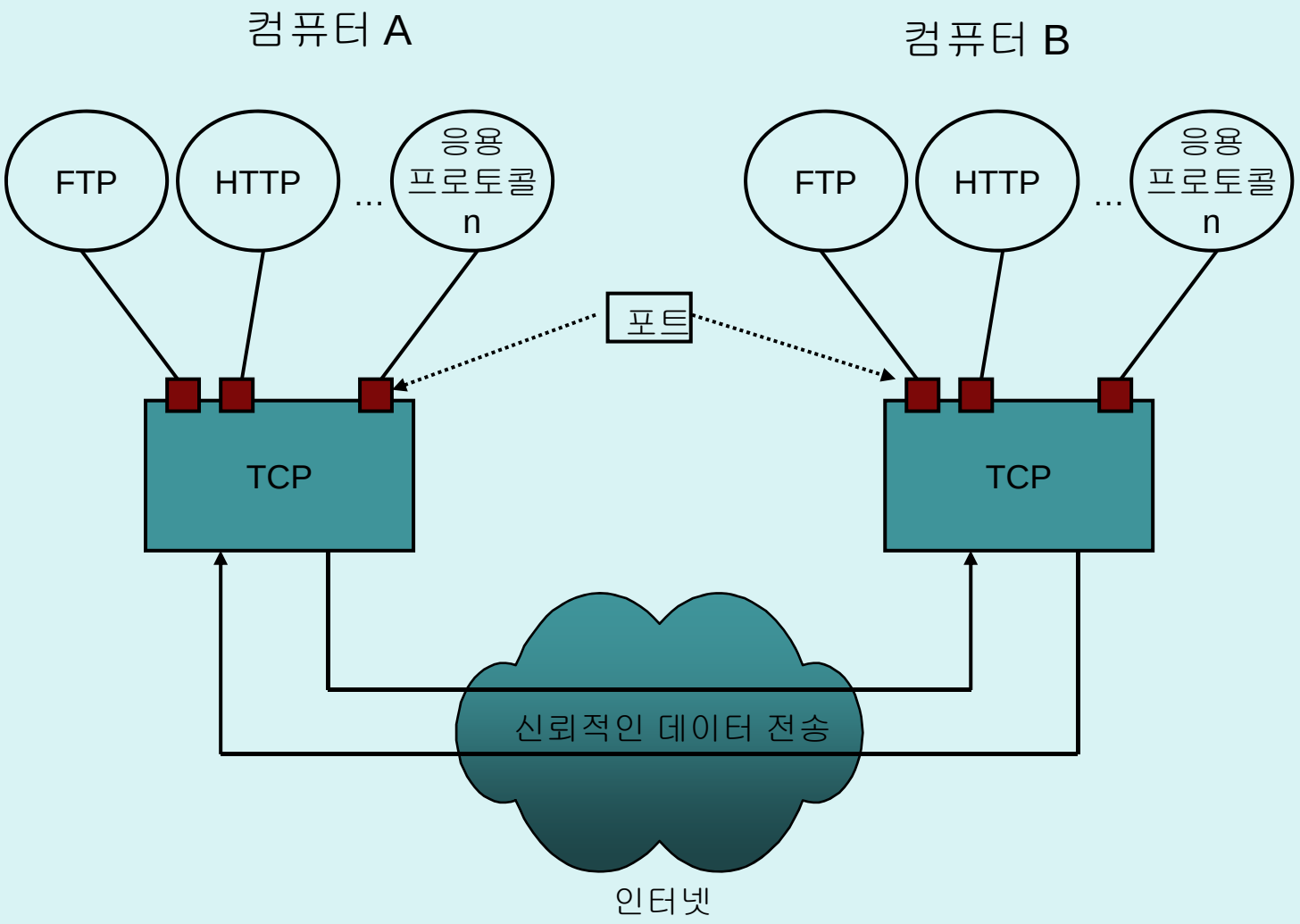
IP 주소


32 bits IP 주소
1 0 0 0 0 0 0 0
1 0 0 1 1 1 0 0
0 0 0 0 1 1 1 0
1 0 0 0 0 1 1 1
128 . 156 . 14 . 7
십진수 점 표기법
(dotted decimal notation)

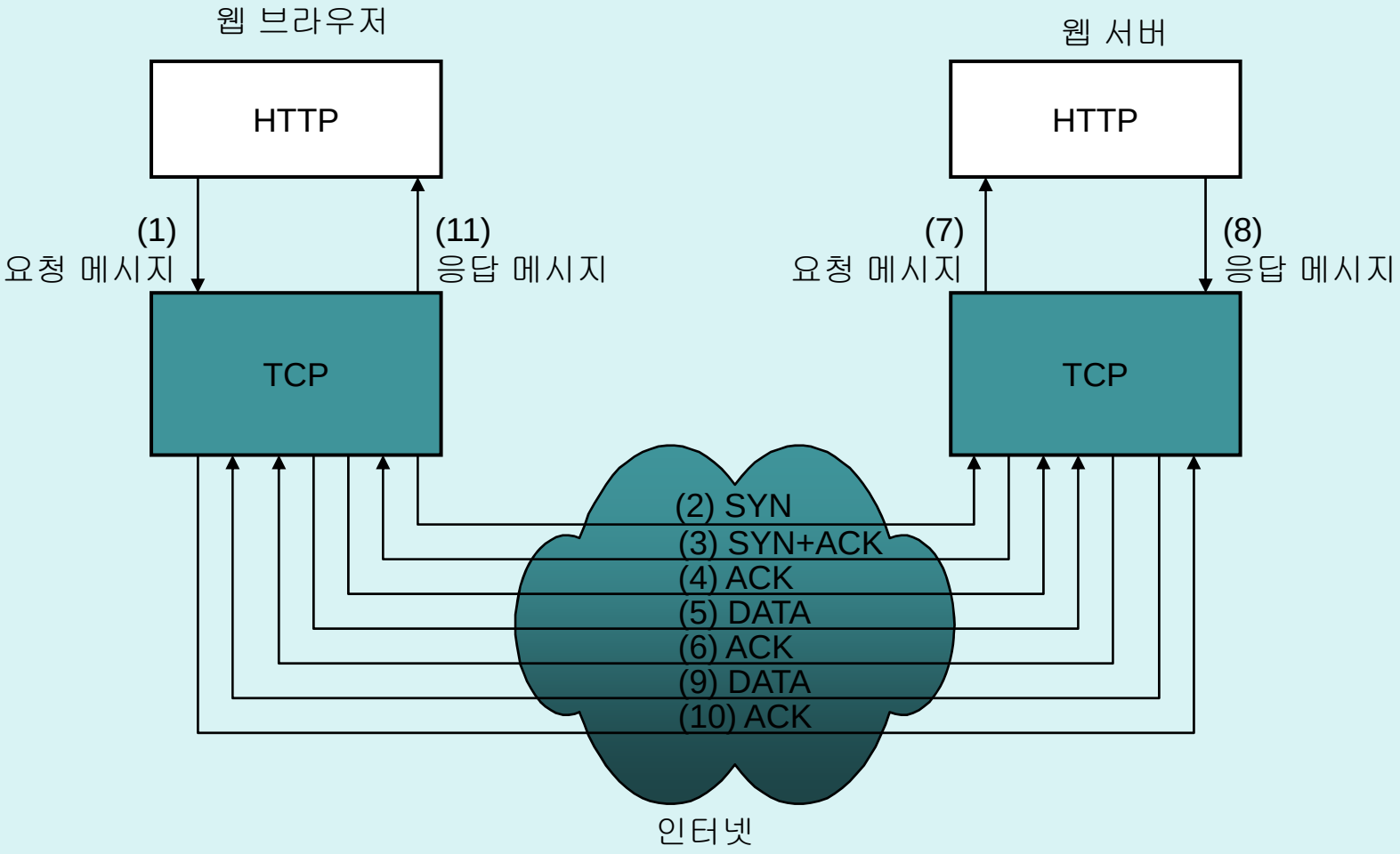
TCP(Transmission Control Protocol)

- TCP(Transmission Control Protocol)의 역할
  - 인터넷에 연결된 두 대의 통신 장치에 실행되고 있는 임의의 두 개의 응용 프로세스간에 신뢰성 있는 데이터 전송 절차를 정의
- TCP 공유
  - 다양한 응용 프로토콜이 신뢰성 있게 전송하는 방법은 동일
  - 신뢰성 있는 전송을 위한 규약을 TCP로 별도로 정의
  - 여러 응용 프로토콜이 TCP를 공유하고 응용 프로토콜 간 구분은 포트 번호 사용

TCP 공유 모델


컴퓨터 A
컴퓨터 B
FTP
HTTP
...
응용 프로토콜 n
FTP
HTTP
...
응용 프로토콜 n
포트
TCP
TCP
신뢰적인 데이터 전송
인터넷

TCP의 신뢰적인 데이터 전송 절차



TCP DATA 세그먼트 = TCP 제어 정보 + HTTP 요청/응답 메시지

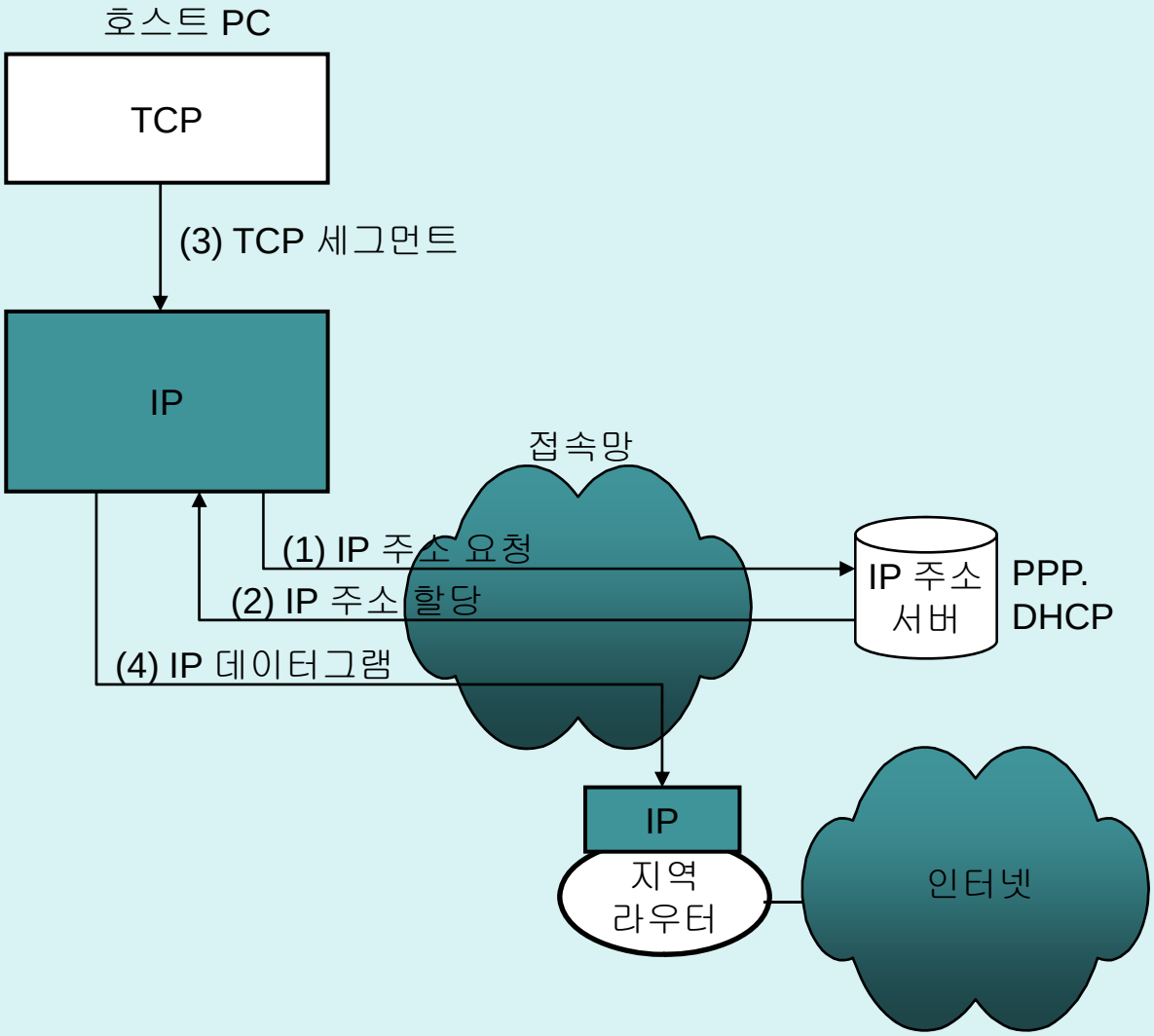
TCP의 신뢰적인 데이터 전송 절차

- 연결 설정(Connection Establishment)
  - 신뢰적인 전송을 위해 먼저 연결 설정
  - 동기화 세그먼트(SYN)의 전송과 동기화 세그먼트의 수신 확인 세그먼트(ACK)를 상호 교환함으로써 연결을 설정
  - 포트번호, 시작 순서 번호 ,수신 버퍼의 크기 등의 제어 정보 교환
- 신뢰적인 데이터 전송
  - 데이터 세그먼트(DATA) 전송과 확인 세그먼트(ACK) 수신
  - DATA 세그먼트 : 응용 프로토콜의 메시지 + 제어 정보(포트 번호, 순서 번호 등)
  - ACK 세그먼트 : 확인 순서 번호.

호스트 IP에 의한 인터넷 데이터 전달

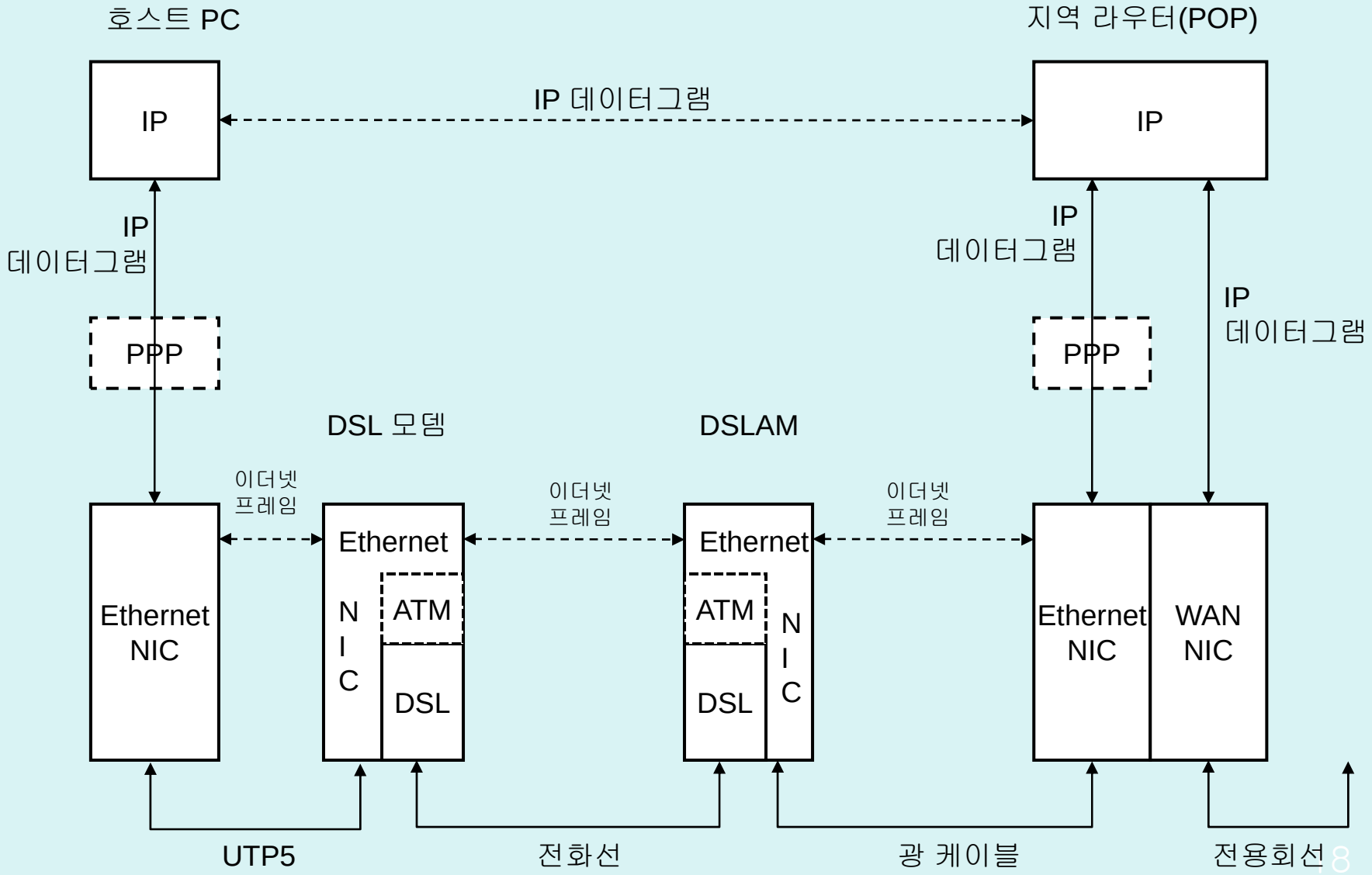
- TCP 세그먼트의 전달
  - 인터넷을 구성하는 데이터 통신망은 자체적인 주소 체계, 데이터 전송 단위, 그리고 데이터 전송 절차를 가짐
  - 하부 데이터 통신망과 독립적인 전송을 위해 IP 사용
- IP(Internet Protocol)
  - 기존 데이터 통신망과 독립적인 주소 체계(IP 주소) 정의
  - IP 데이터그램 전송 절차 정의
  - IP 데이터그램 : 데이터(TCP 세그먼트) + 제어 정보(출발지 IP 주소, 목적지 IP 주소, 단편화/재조립 관련 정보 등)
- IP 주소 할당
  - 정적 할당(고정 IP 주소)
  - 동적 할당(유동 IP 주소) : PPP(Point-to-Point Protocol), DHCP(Dynamic Host Configuration Protocol)

호스트 IP에 의한 인터넷 데이터 전달



IP 데이터그램 = IP 제어 정보 + TCP 세그먼트

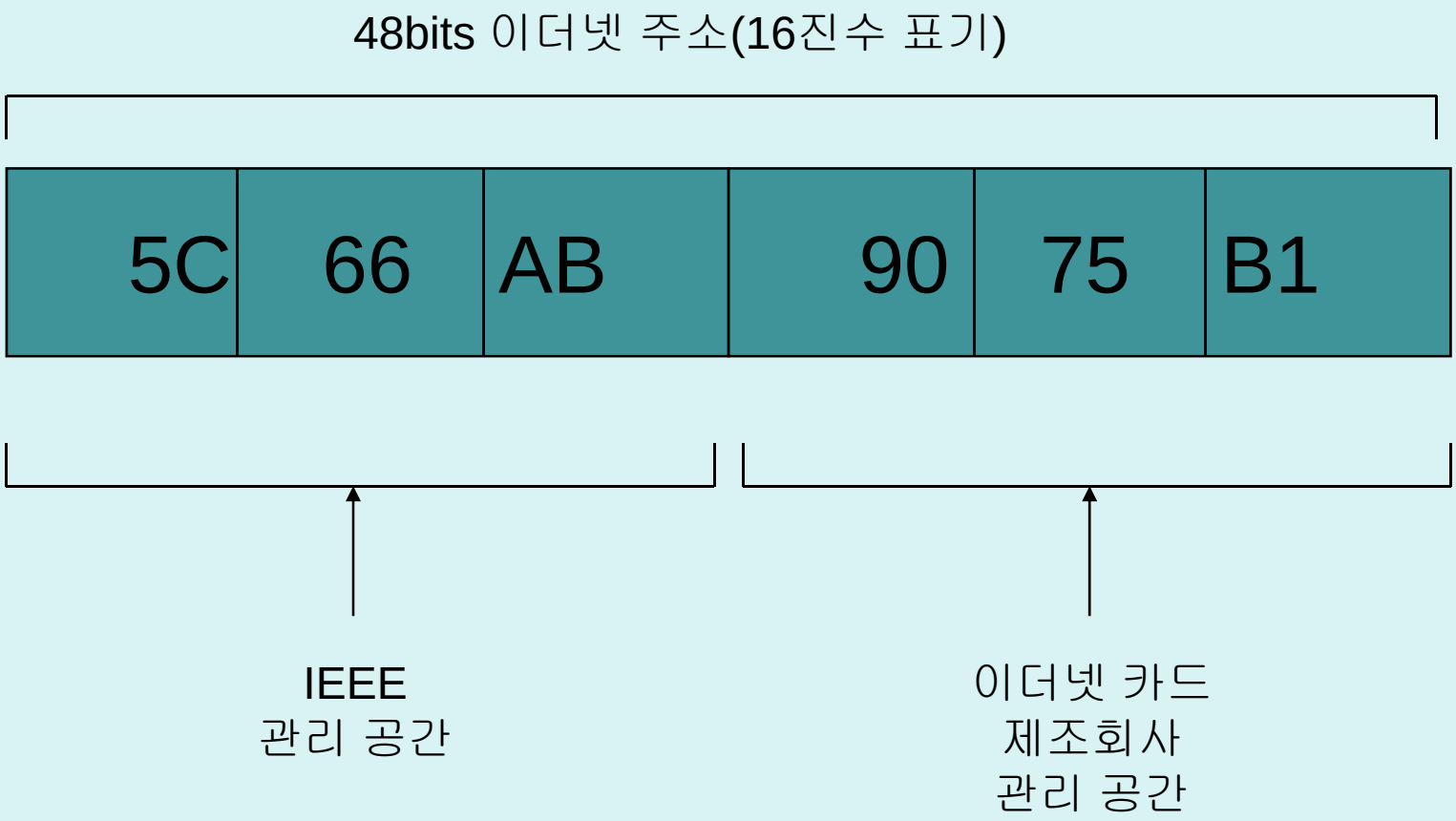
접속망의 구조: DSL망


호스트 PC
지역 라우터(POP)
IP
IP 데이터그램
IP
IP
데이터그램
IP
데이터그램
PPP
PPP
IP
데이터그램
DSL 모뎀
DSLAM
이더넷
프레임
이더넷
프레임
이더넷
프레임
Ethernet
Ethernet
Ethernet
NIC
N
I
C
ATM
DSL
ATM
DSL
N
I
C
Ethernet
NIC
WAN
NIC
UTP5
전화선
광 케이블
전용회선

접속망에 의한 IP 데이터그램 전달

- 이더넷 NIC(Network Interface Card) 사용
  - 이더넷 NIC을 사용하여 IP 데이터그램 전달
  - 이더넷 프레임으로 변환된 후 POP 라우터의 이더넷 NIC로 전달
- 이더넷 프레임(Ethernet Frame)
  - IP 데이터그램 + 이더넷 제어 정보
  - 이더넷 제어 정보 : 출발지 이더넷 주소, 목적지 이더넷 주소, 오류 탐지를 위한 부가 정보 등
- 이더넷 주소
  - 48 비트 체계
  - 생산 시에 변경되지 않는 고유한 이더넷 주소를 할당

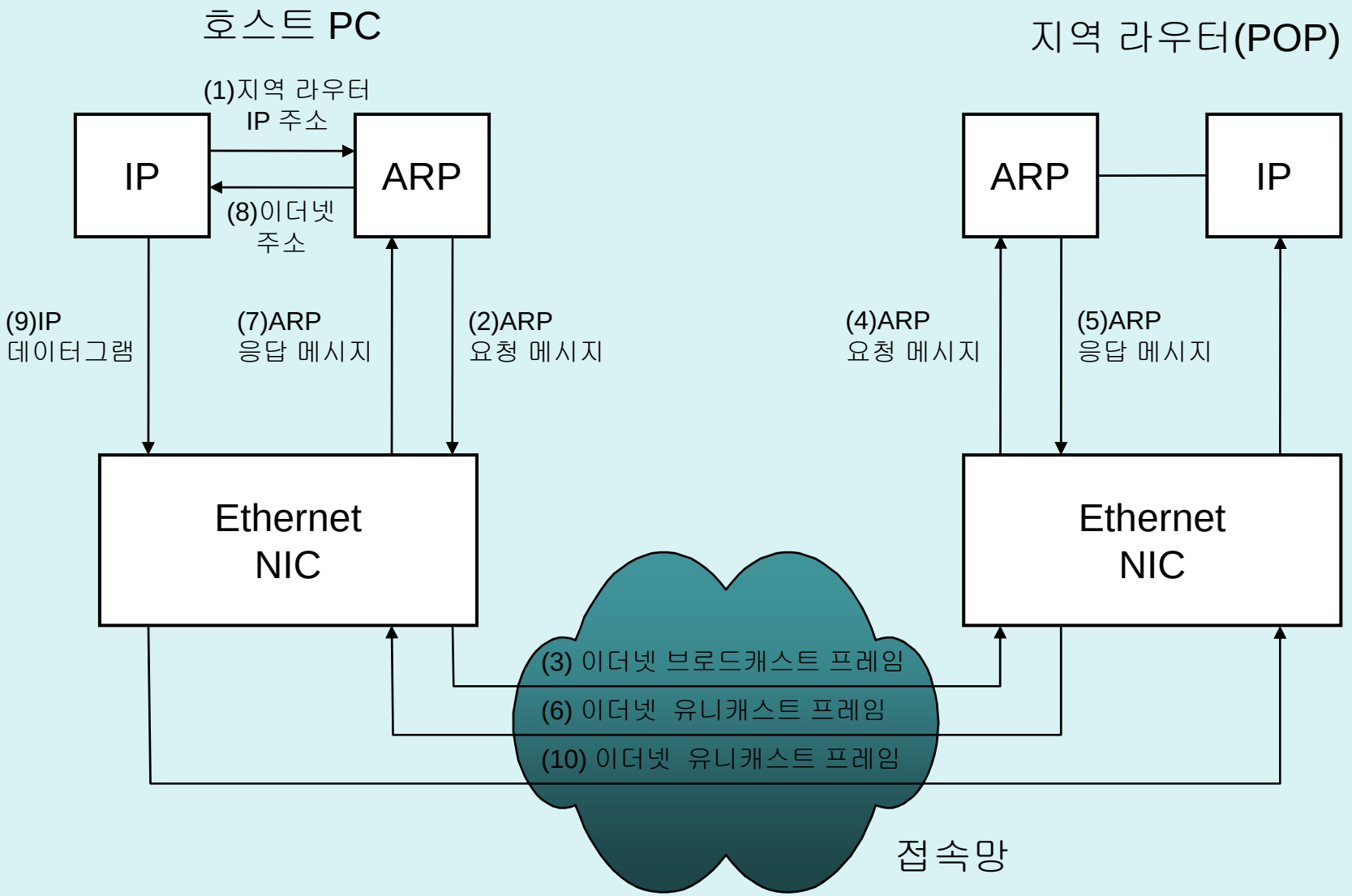
이더넷 주소 체계


48bits 이더넷 주소(16진수 표기)
5C
66
AB
90
75
B1
IEEE
관리 공간
이더넷 카드
제조회사
관리 공간

ARP(Address Resolution Protocol)

- ARP의 역할
  - 이미 알려진 IP주소를 가진 인터넷 장치(지역 라우터)의 이더넷 주소를 자동으로 알려주는 프로토콜
  - ARP 요청 메시지와 ARP 응답 메시지 사용
- ARP 요청 메시지
  - 대상의 IP 주소 포함
  - 브로트캐스팅(broadcasting)
- ARP 응답 메시지
  - 대상의 이더넷 주소 포함
  - 유니캐스팅(unicasting)

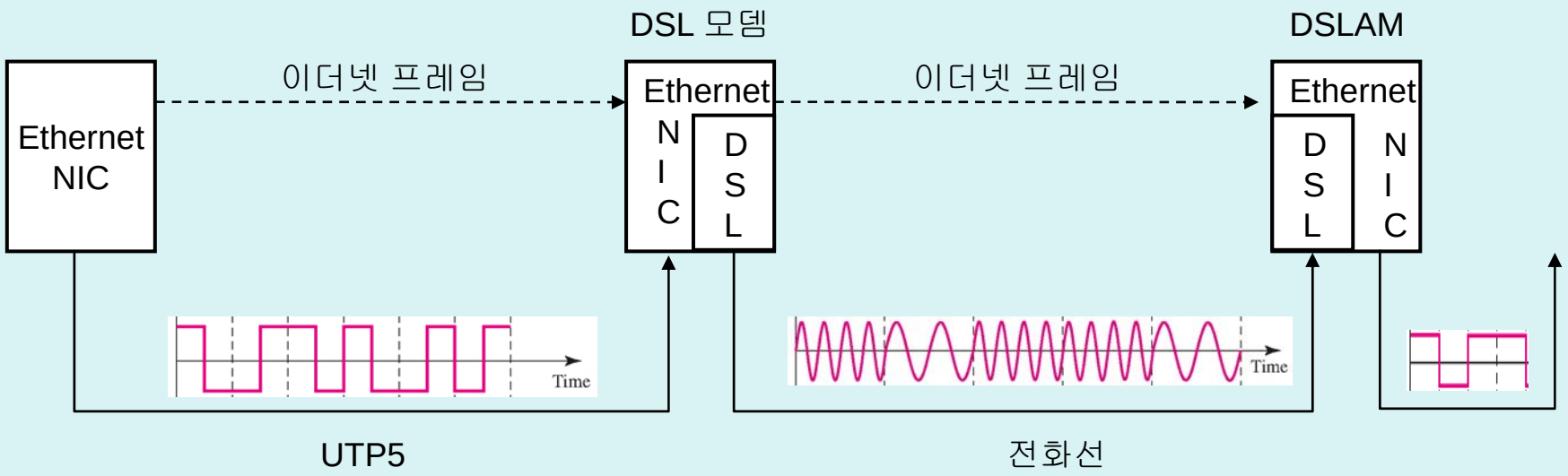
접속망에 의한 IP 데이터그램 전달 절차



DSL 모뎀에 의한 데이터 전송 과정

- DSL 모뎀의 물리적인 역할
  - PC와 UTP5로 연결
  - DSLAM 전화선으로 연결
  - UTP5 회선을 통해 수신된 디지털 신호를 전화선의 고주파 아날로그 신호(DSL 신호)로 변조(modulation)
  - 전화선의 고주파 아날로그 신호를 UTP5 회선을 통해 수신된 디지털 신호로 복조(demodulation)
- DSL 모뎀의 논리적인 역할
  - PC에 의해 생성된 이더넷 프레임을 UTP5 회선을 통해 수신한 다음 전화선을 통해 DSLAM으로 전달
  - DSLAM으로부터 전화선을 통해 수신된 이더넷 프레임을 UTP5 회선을 통해 PC로 전달
  - 이더넷 브리지(연결 포트가 2개인 이더넷 스위치) 역할 수행

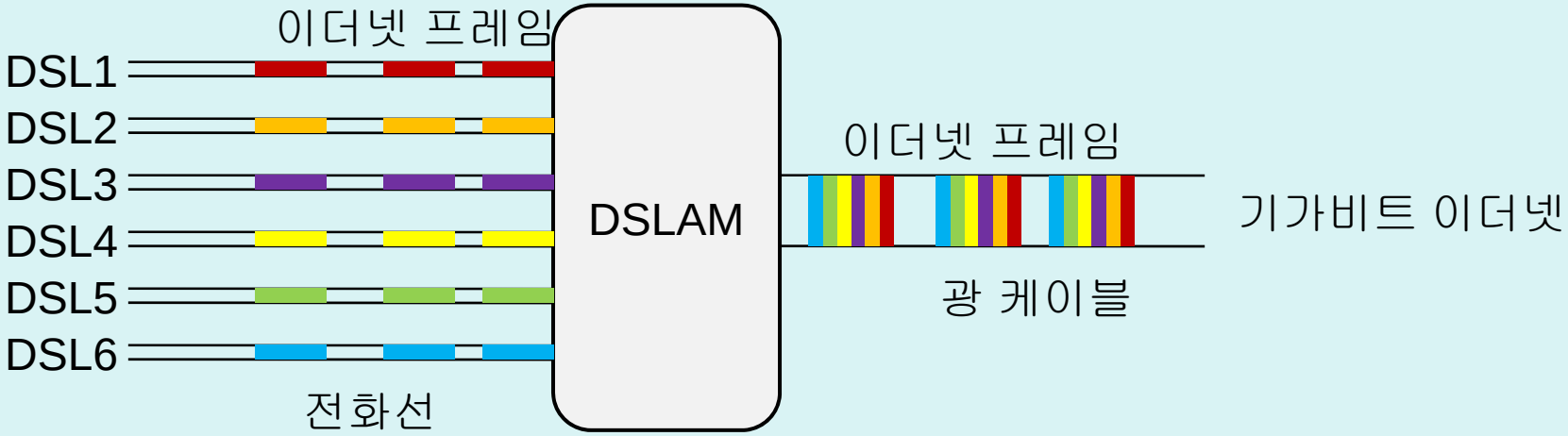
DSL 모뎀에 의한 데이터 전송 과정



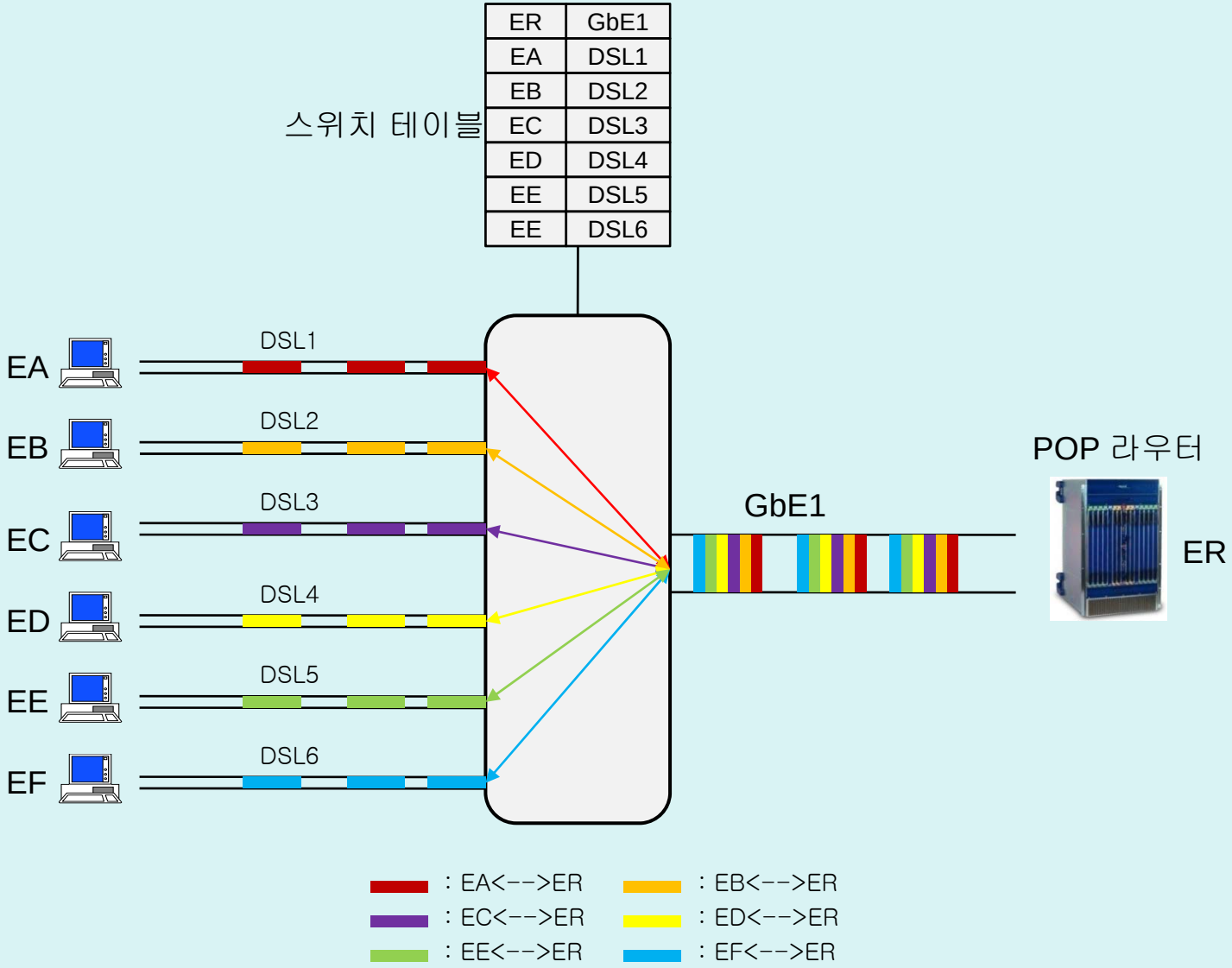
DSLAM에 의한 데이터 전송 과정

- DSLAM의 물리적인 역할
  - 가입자 모뎀이 연결된 많은 수의 DSL 회선을 POP 라우터가 연결된 기기비트 이더넷 광 케이블 회선과 연결
  - 아날로그 DSL 신호와 디지털 기가비트 이더넷 신호간 변조와 복조
- DSLAM의 논리적인 역할
  - 다수의 DSL 회선을 통해 수신된 호스트 PC의 이더넷 프레임을 다중화(multiplexing)하여 고속의 기가비트 이더넷 회선을 통해 POP 라우터로 전달
  - POP 라우터로부터 수신된 이더넷 프레임을 적절한 DSL 회선으로 역다중화(demultiplexing)하여 가입자 DSL 모뎀을 통해 호스트 PC로 전달

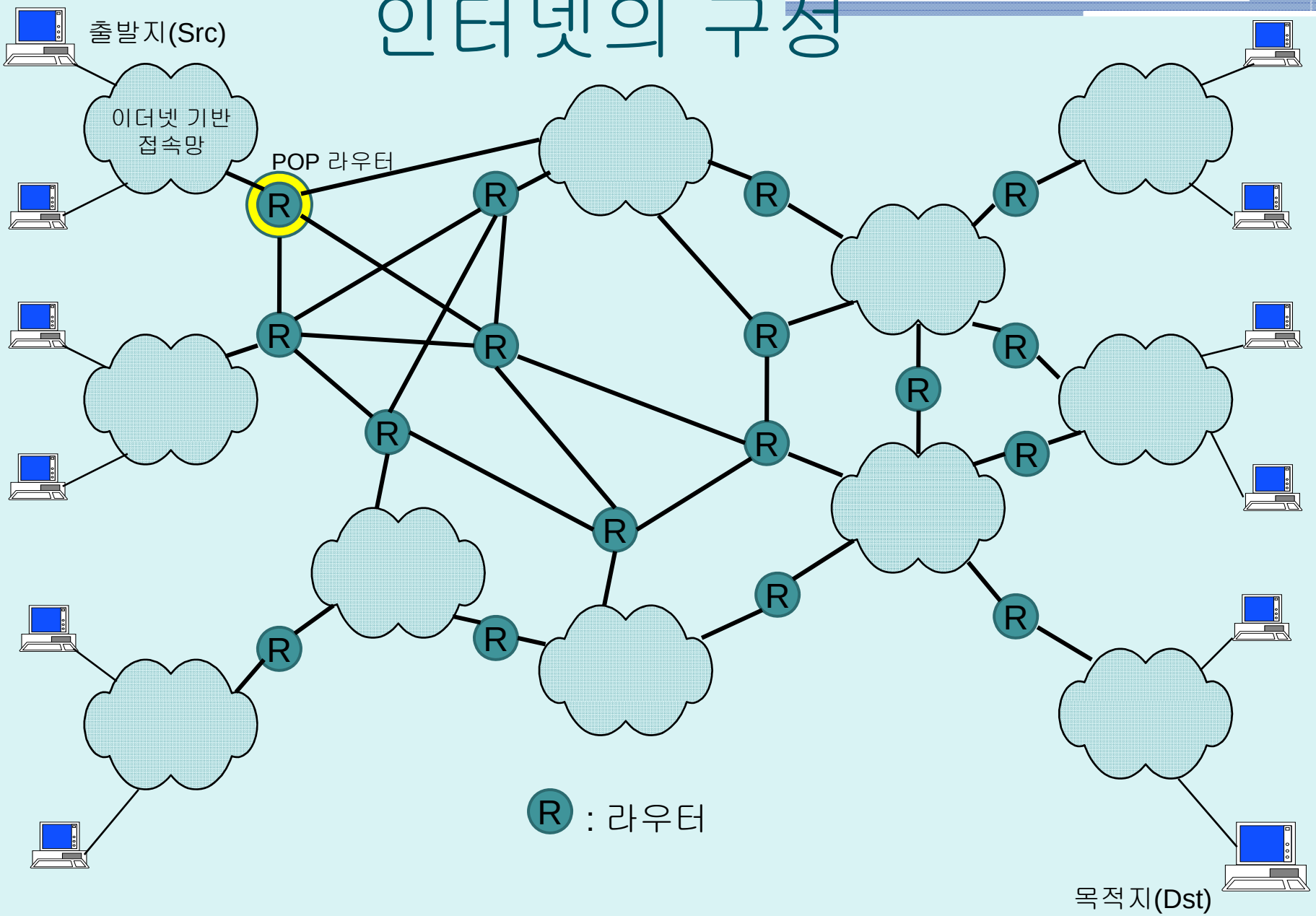
DSLAM에 의한 DSL 회선 다중화



이더넷 기반 DSLAM의 다중화 과정



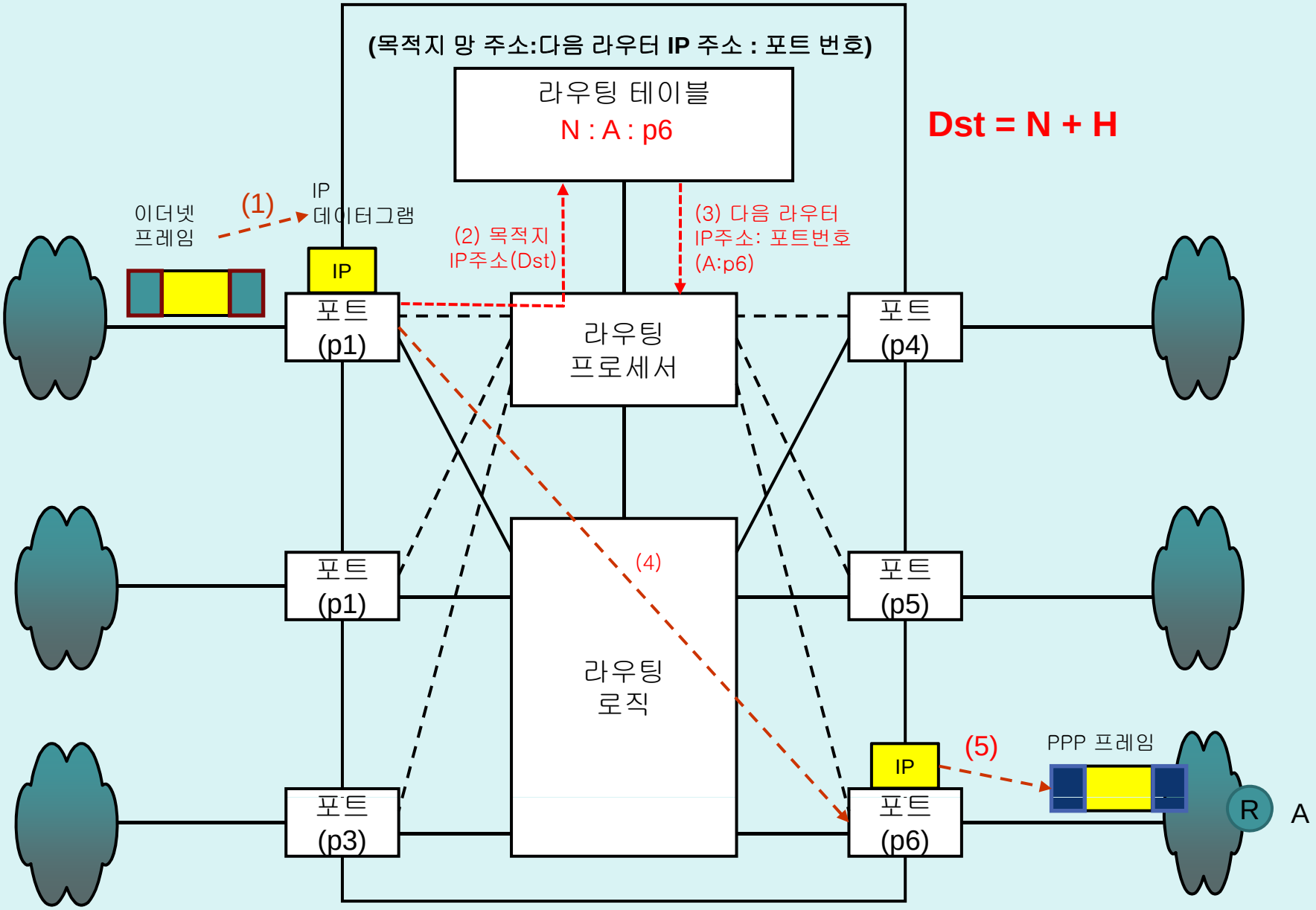
인터넷의 구성



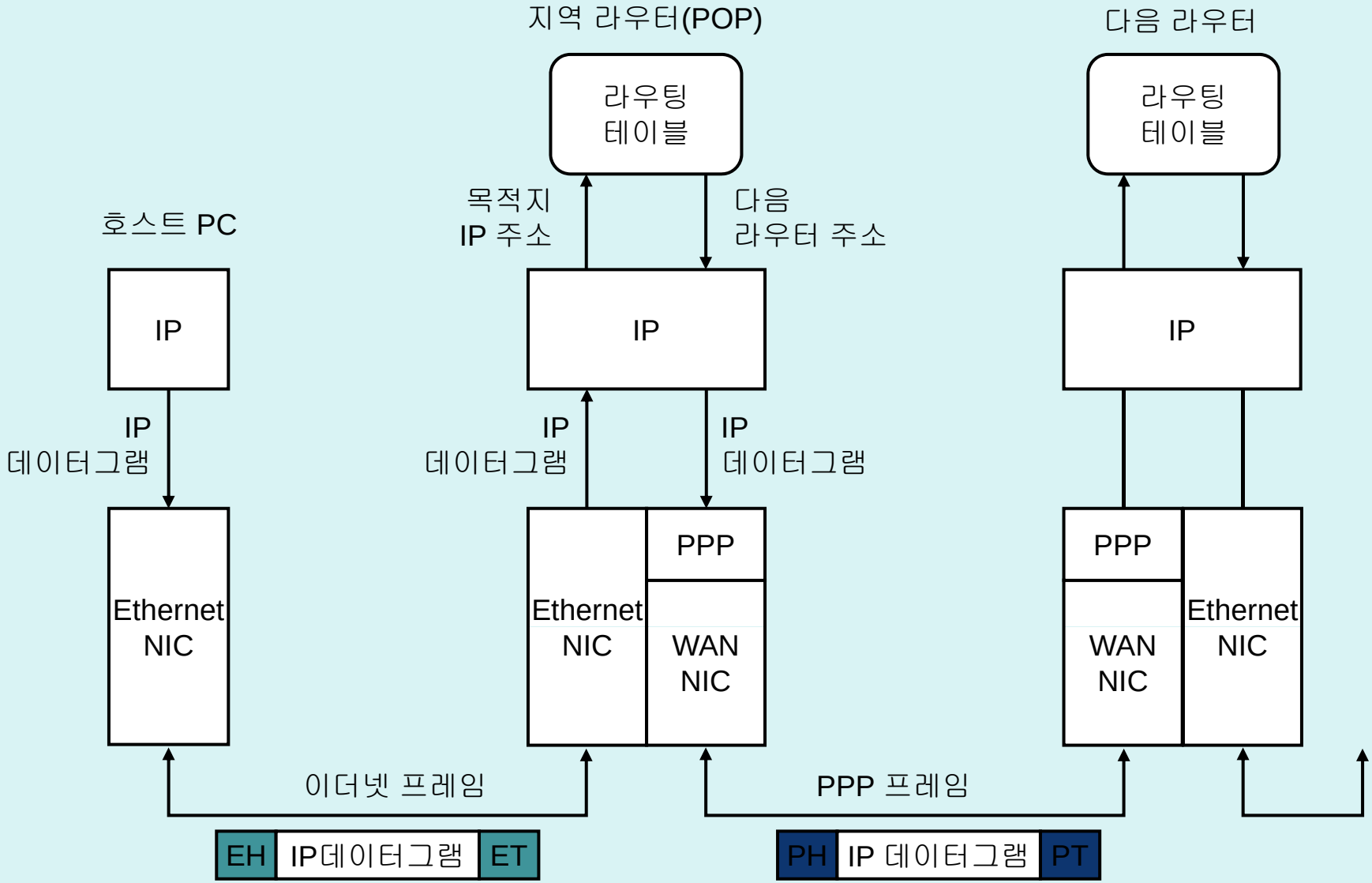
라우터

- 라우터의 역할
  - 2개 이상의 데이터 통신망을 상호 연결
  - 인터넷에 연결된 호스트와 호스트간에 가장 좋은 경로를 통해 IP 데이터그램 전달
- 라우터의 동작 절차
  - 하부 데이터 통신망으로부터 IP 데이터그램 수신 : Decapsulation
  - 라우팅 테이블을 검색하여 다음 라우터 선정
  - 하부 데이터 통신망을 사용하여 다음 라우터로 IP 데이터그램 전달 : Encapsulation

라우터의 구조 및 동작 절차

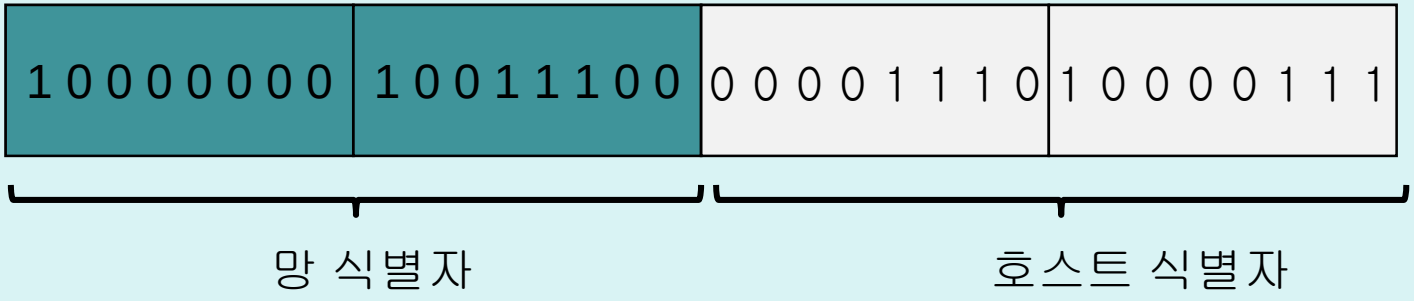


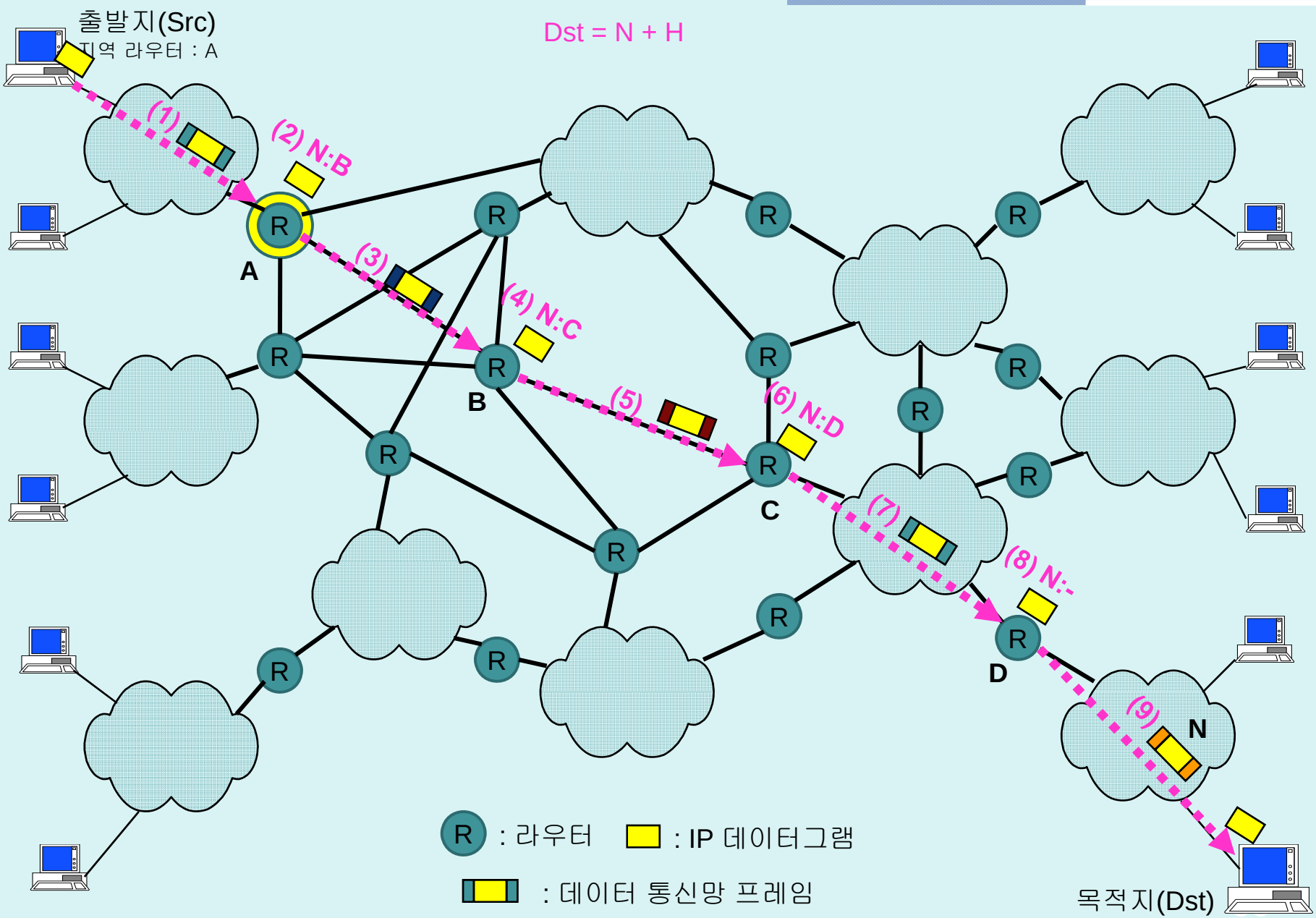
라우터에 의한 IP 데이터그램 전달 체계



인터넷 백본망의 IP 데이터그램 전달 과정

- 2단계 IP 데이터그램 전달
  - 목적지 호스트가 소속된 데이터 통신망에 연결된 라우터로 전달
  - 목적지 망의 라우터가 목적지 호스트에게 IP 데이터그램을 전달
- IP 주소(Dst = N + H)
  - 망 주소
  - 호스트 주소




출발지(Src)
지역 라우터 : A
Dst = N + H
(1)
(2) N:B
(3)
(4) N:C
(5)
(6) N:D
(7)
(8) N:-
(9)
A
B
C
D
N
R
R : 라우터
: IP 데이터그램
: 데이터 통신망 프레임
목적지(Dst)

라우팅 프로토콜(Routing Protocol)

- 라우팅 테이블 갱신
  - 정적 라우팅 테이블 갱신- 수동
  - 동적 라우팅 테이블 갱신- 자동(라우팅 프로토콜 사용)
- 라우팅 프로토콜
  - 라우터간에 최신 라우팅 정보를 교환하는 규칙을 정의
  - 자치 시스템 – 독립적으로 라우팅 정책을 수행하는 관리 단위(예, ISP)
  - 자치 시스템(Autonomous System) 내부 라우팅과 자치 시스템간 라우팅 분리
  - 내부 라우팅 – RIP(Routing Information Protocol), OSPF(Open Shortest Path First)
  - 외부 라우팅 – BGP(Border Gateway Protocol)

인터넷 지연시간(Delay)

- 종단간 지연시간(end-to-end delay)
  - 출발지에서 IP 데이터그램이 송신되는 시점으로부터 목적지에 도착하는 시점까지의 시간 간격
  - 처리 지연시간, 전송 지연시간, 전달 지연시간, 큐잉 지연시간 등 여러 가지 유형의 지연시간의 합에 의해 결정
- 처리 지연시간(processing delay)
  - 통신 장치(라우터)가 IP 데이터그램을 수신하여 전송 대기 자료 구조인 큐(queue)에 전달하는 데에 걸리는 시간 간격
  - 데이터그램 제어 정보를 해석, 라우팅 테이블을 검색, 데이터그램을 교환하는 작업 등에 소요되는 시간

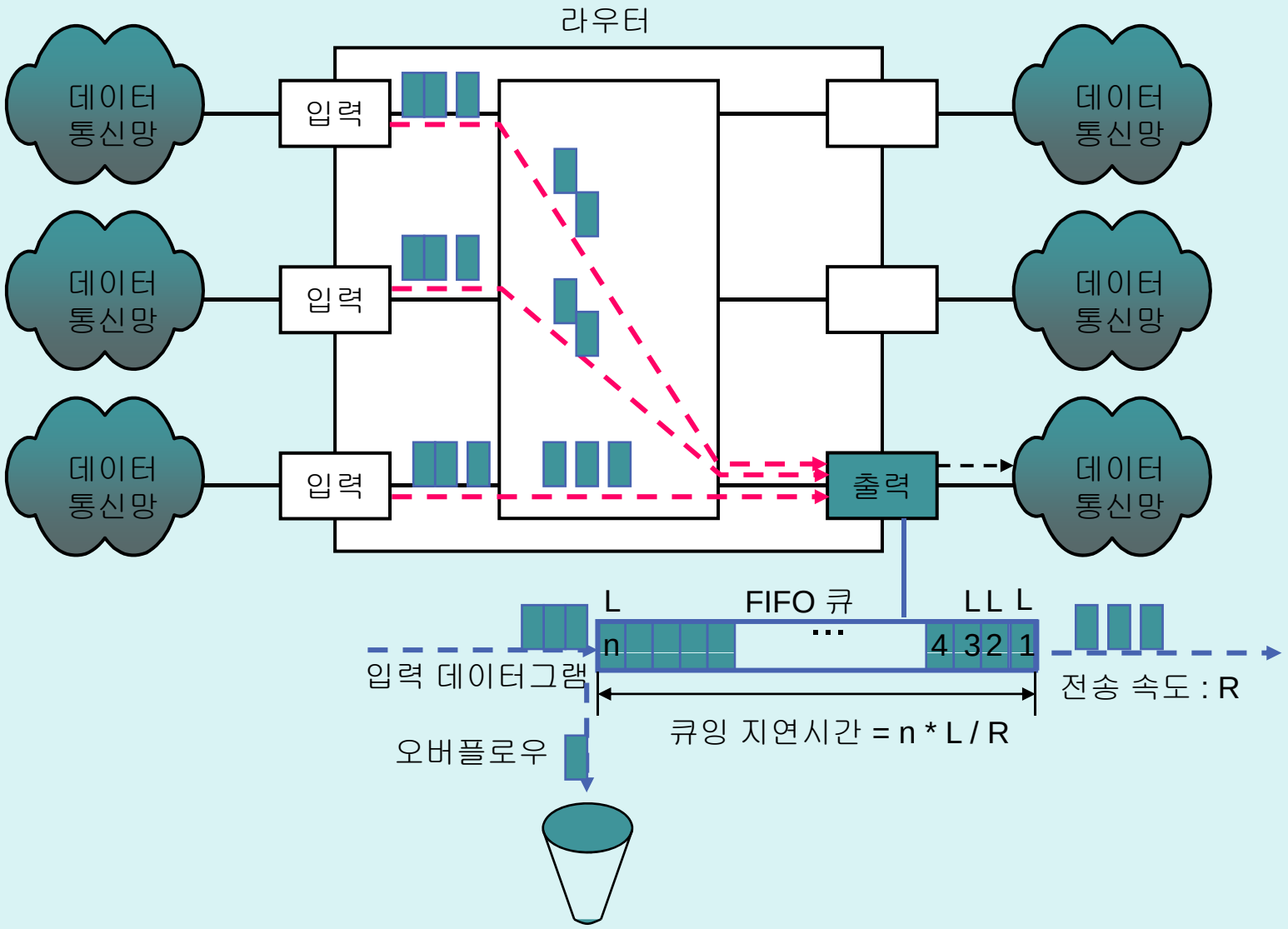
인터넷 지연시간(Delay)

- 전송 지연시간(transmission delay)
  - IP 데이터그램의 첫 번째 비트를 미리 정의된 전기적인 신호로 만들어 전송 매체에 옮기기 시작한 시점부터 마지막 비트를 옮기는 시점까지의 시간 간격
  - 데이터그램의 길이를 전송 속도로 나눈 값
- 전달 지연시간(propagation delay)
  - 하나의 비트가 전송 매체의 한쪽 끝을 출발한 시점으로부터 다른 쪽 끝에 도착하는 시점까지의 시간 간격
  - 전송 매체의 길이(L)을 해당 매체에서의 전기 신호 전달 속도(S)로 나눈 값

인터넷 지연시간(Delay)

- 큐잉 지연시간(queuing delay)
  - IP 데이터그램이 전송을 위해 큐(queue) 자료구조에 들어가는(큐잉 – queuing) 시점으로부터 전송이 종료되어 큐를 떠나는 시점까지의 시간 간격
  - 큐에 전송 대기중인 IP 데이터그램이 많고 전송 속도(대역폭)가 느린 경우 큐잉 지연시간은 커짐
  - 데이터그램의 도착율(arrival rate)과 데이터 통신망의 전송 속도의 관계에 의해 결정되는 가변적인 지연시간
  - n번째 데이터그램의 큐잉 지연시간 - n*L/R
    (통신망의 전송 속도는 R, IP 데이터그램의 크기 L)
- 라우터 혼잡(congestion) 상황
  - 큐 자료 구조 넘침(Queue Overflow)
  - 다음 도착 IP 데이터그램 손실

큐잉 지연시간과 데이터그램 손실

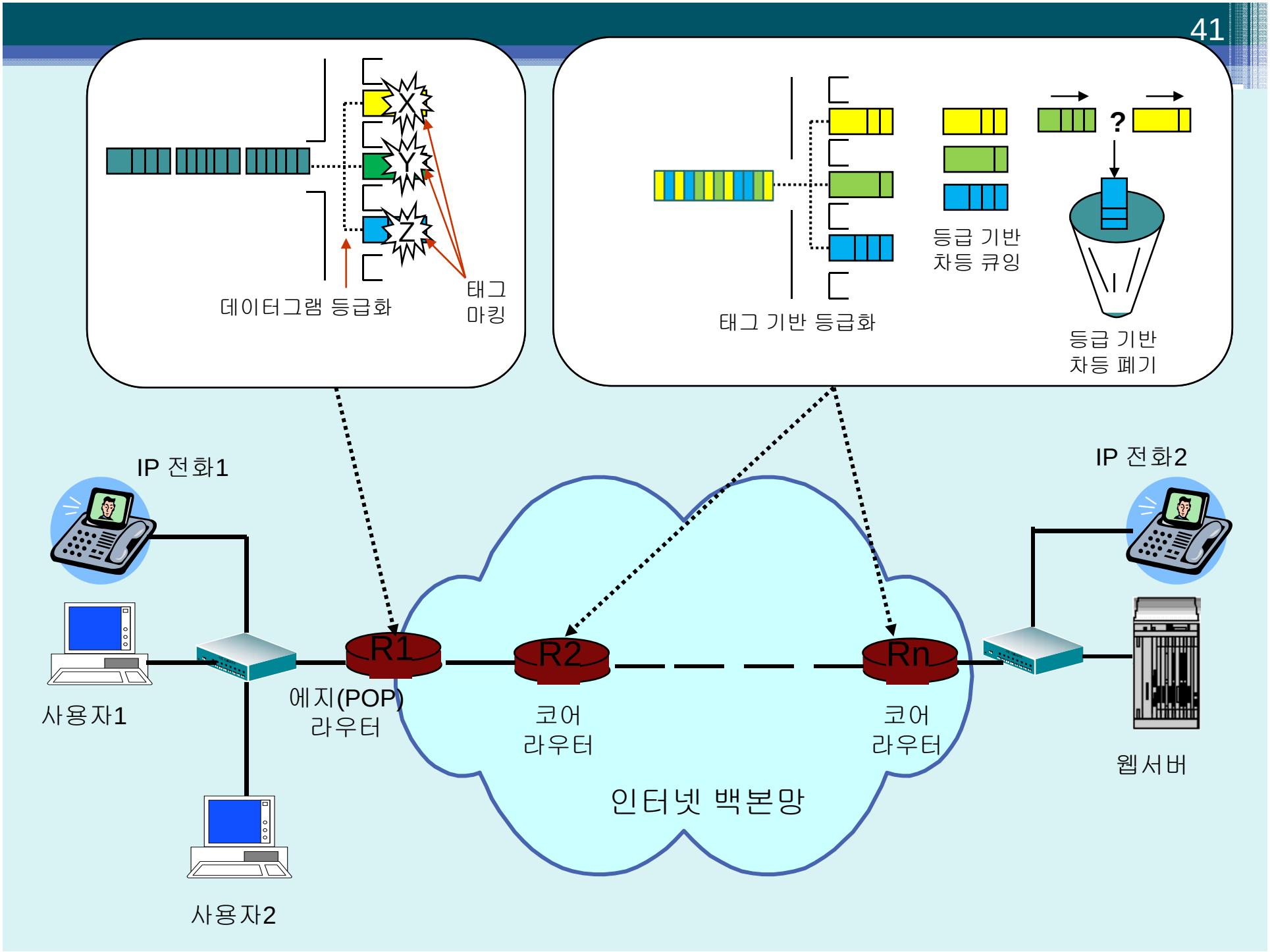


최선형 인터넷(Best-effort Internet)

- FIFO(First In First Out) 큐잉 정책
  - 도착한 순서에 따라 라우터가 최선을 다해 데이터그램 처리
  - 데이터의 속성에 맞는 서비스 품질(QoS-Quality of Service) 제공 불가
- 데이터 속성
  - IP 전화기 데이터 - 지연시간에 매우 민감
  - 비디오 스트리밍 데이터 - 지연시간과 지연시간의 편차에 민감
  - 이메일 데이터 - 지연시간과 지연시간 편차에 덜 민감
- 차등화된 QoS 요구
  - VoIP(Voice over IP), IPTV(Internet Protocol TV), VoD(Video on Demand) 등 실시간성 멀티미디어 서비스 활성화

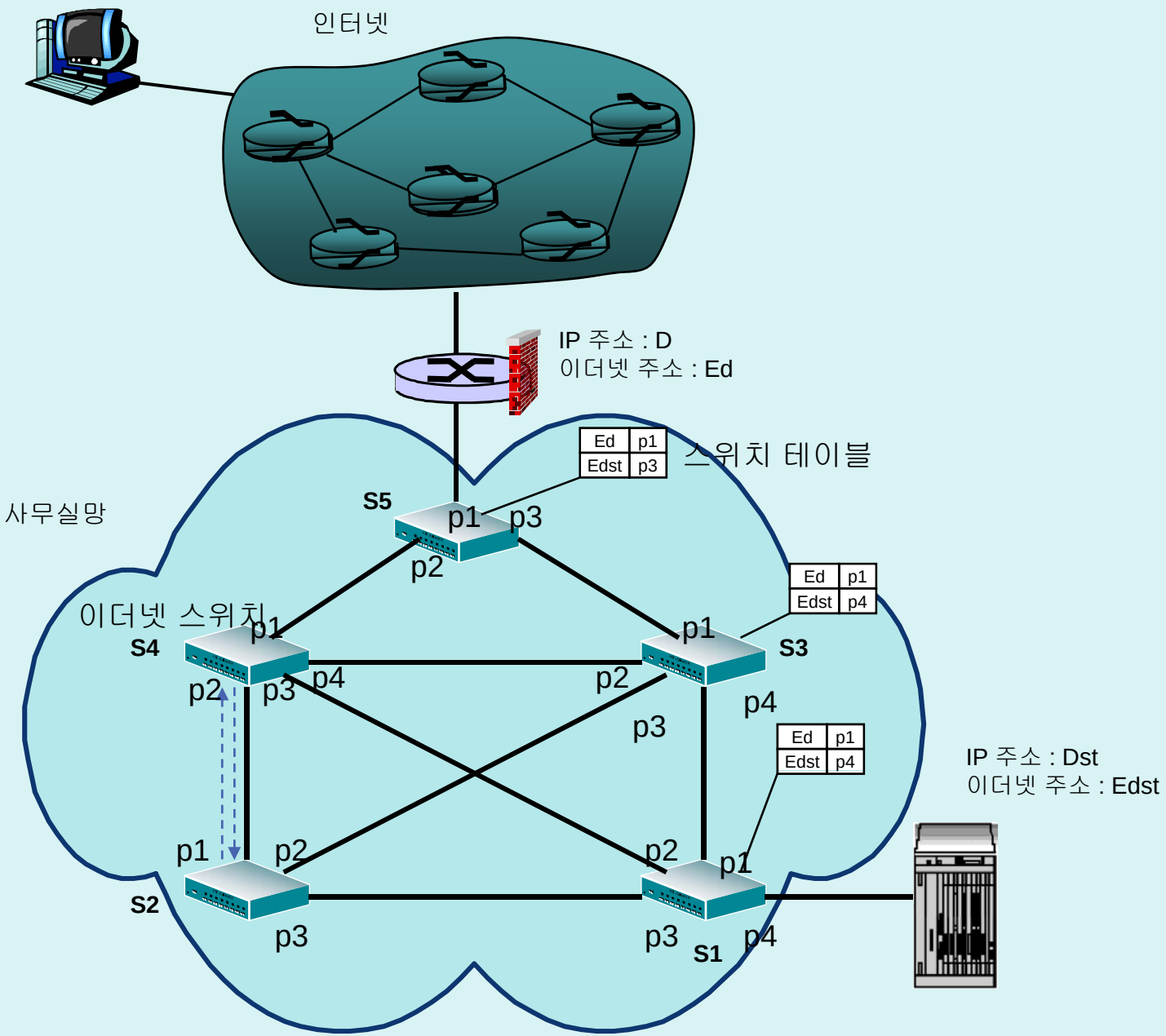
인터넷의 차등화된 데이터 전달

- 트래픽 등급화 : 가장자리 라우터(Edge Router)
  - 데이터 속성에 따른 IP 데이터그램 등급화
  - 등급에 따라 IP 데이터그램에 태그 마킹하기
- 등급에 따른 차별화된 처리 : 백본 라우터
  - 태그 기반의 등급별 데이터그램 큐잉
  - 등급별 큐에 대한 차등화된 데이터그램 전송
  - 혼잡 상황 발생 시 등급별 차등화된 데이터그램 폐기 등


데이터그램 등급화
태그
마킹
태그 기반 등급화
등급 기반
차등 큐잉
?
등급 기반
차등 폐기
IP 전화1
IP 전화2
사용자1
사용자2
에지(POP)
라우터
R1
R2
Rn
코어
라우터
코어
라우터
인터넷 백본망
웹서버

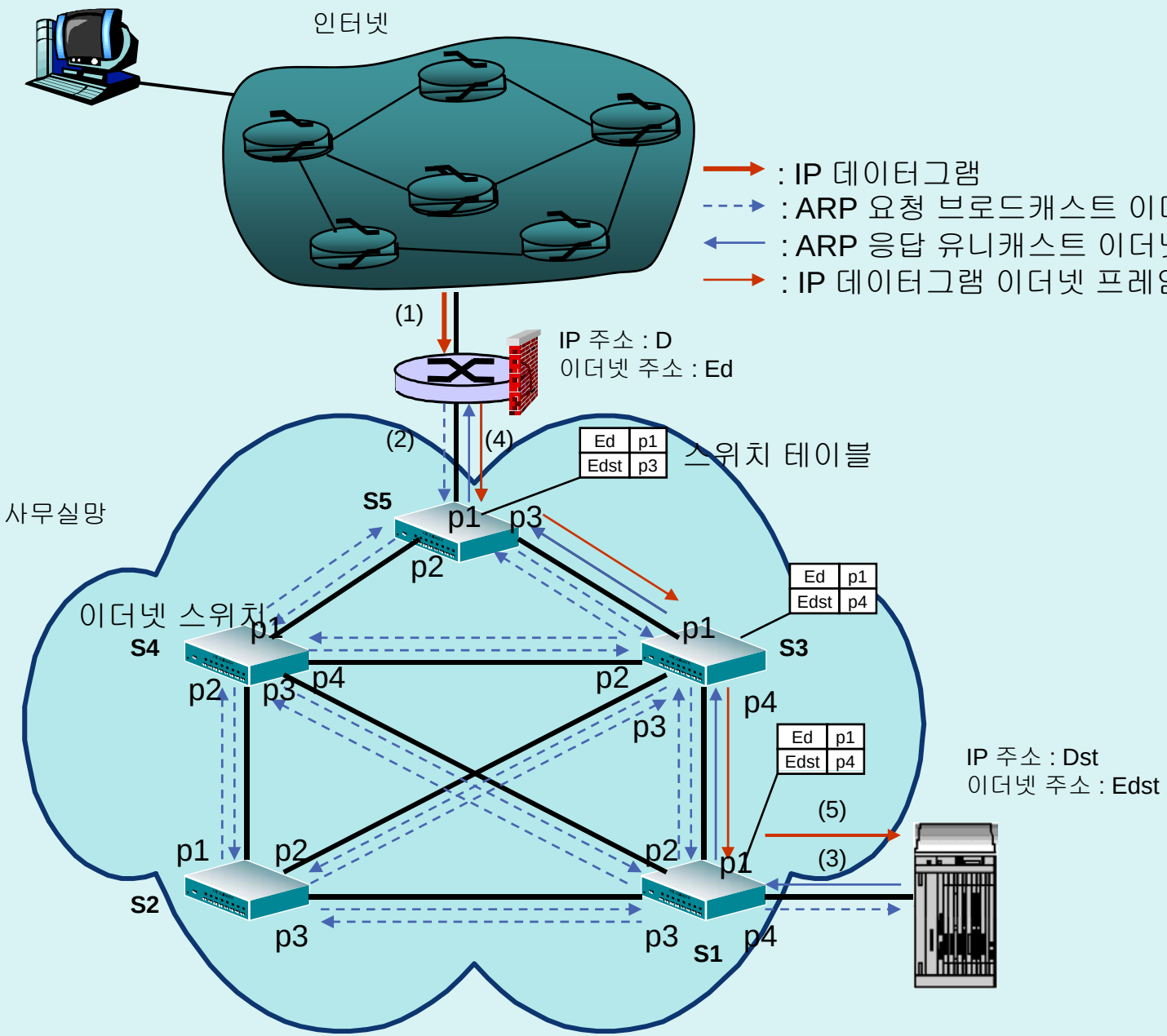
사무실망의 구성

- 이더넷 기반
  - 고속 이더넷
  - 이더넷 스위치
  - 이더넷 스위치의 상호 연결
  - (무선 LAN)
- 이더넷 스위치
  - 이더넷 프레임의 출발지 주소를 활용하여 스스로 [이더넷 주소 : 출력 포트 번호] 형식의 스위치 테이블 작성
  - 스위치 테이블을 활용하여 입력 포트로 수신된 특정 목적지 주소의 이더넷 프레임을 출력 포트로 교환
  - 스위치 테이블에 존재하지 않는 이더넷 주소를 목적지 주소로 가진 프레임은 입력 포트를 제외한 모든 포트


인터넷
IP 주소 : D
이더넷 주소 : Ed
스위치 테이블
Ed p1
Edst p3
사무실망
S5
p1
p3
p2
이더넷 스위치
S4
S3
Ed p1
Edst p4
p1
p2
p3
p4
Ed p1
Edst p4
IP 주소 : Dst
이더넷 주소 : Edst
S2
S1

사무실망의 IP 데이터그램 전달 과정

- 사무실망 라우터에 IP 데이터그램 도착
  - 라우터의 IP 주소 : D
  - 라우터의 이더넷 주소 : Ed
  - 목적지 IP 주소 : Dst
  - 목적지 이더넷 주소 : ?(Edst)
- IP 데이터그램 전달 과정
  - ARP 요청 메시지 브로드캐스팅(D → All)
  - ARP 응답 메시지 유니캐스팅(Dst → D)
  - IP 데이터그램을 이더넷 프레임으로 캡슐화
  - 이더넷 프레임 전송(Ed → Edst)
  - 이더넷 프레임으로부터 IP 데이터그램 역캡슐화


인터넷
: IP 데이터그램
: ARP 요청 브로드캐스트 이더넷 프레임
: ARP 응답 유니캐스트 이더넷 프레임
: IP 데이터그램 이더넷 프레임
(1)
IP 주소 : D
이더넷 주소 : Ed
(2)
(4)
Ed p1
Edst p3
스위치 테이블
사무실망
S5
p1
p3
p2
이더넷 스위치
S4
S3
Ed p1
Edst p4
p1
p2
p3
p4
Ed p1
Edst p4
IP 주소 : Dst
이더넷 주소 : Edst
(5)
(3)
S2
S1

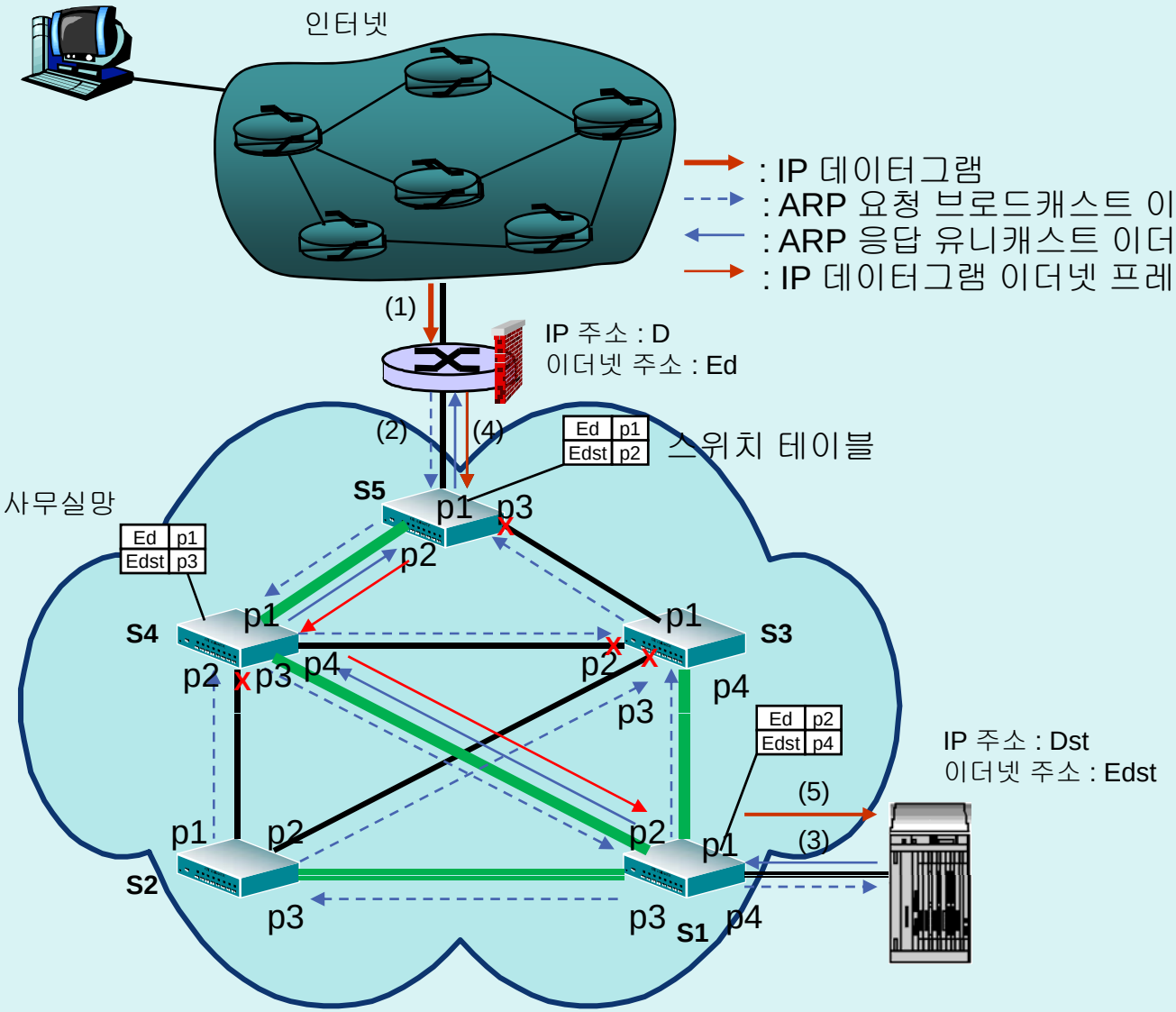
STP(Spanning Tree Protocol)

- 순환 경로(Loop)
  - 스위치와 스위치간에 중복 경로가 존재하여 자신이 전송한 프레임이 다른 경로로 다시 자신에게 되돌아올 수 있게 만드는 경로
  - S1→S2→S3→S1
  - 고장 인내력(Fault Tolerance)를 높이기 위한 의도적 구성 또는 우연한 구성
- 순환 경로의 문제점
  - 불안전한 스위치 테이블(프레임 중복 전달)
  - 브로드캐스트 폭풍(Broadcast Storm) – 브로드캐스트 프레임의 폭발적인 증가

STP(Spanning Tree Protocol)

- STP의 역할
  - 순환 경로를 자동으로 제거하는 프로토콜
  - 특정 스위치를 루트 스위치로 선정
  - 루트 스위치로부터 각 스위치로의 중복 경로 중 가장 좋은 경로를 제외한 나머지 경로는 해당 스위치의 포트를 막음(blocking)
  - S1을 루트 스위치로 선정, S3의 p2와 p3, S4의 p2, 그리고 S1의 p3 포트를 막음
  - S5와 S1간에는 S5→S4→S1 경로만 존재
  - 고장이 발생하는 경우 막혀있는 포트를 정상화하여 망을 자동적으로 복구

STP 지원 확장 이더넷


인터넷
: IP 데이터그램
: ARP 요청 브로드캐스트 이더넷 프레임
: ARP 응답 유니캐스트 이더넷 프레임
: IP 데이터그램 이더넷 프레임
(1)
IP 주소 : D
이더넷 주소 : Ed
(2)
(4)
Ed p1
Edst p2
스위치 테이블
사무실망
S5
S4
S3
S2
S1
p1
p2
p3
p4
Ed p1
Edst p3
Ed p2
Edst p4
IP 주소 : Dst
이더넷 주소 : Edst
(5)
(3)

방화벽과 인터넷 보안

- 사무실망 보안의 필요성
  - 사무실망에는 많은 사용자가 존재하고 내.외부 사용자들이 공유하는 다양한 서버(웹, 이메일, FTP 등)들이 존재
  - 사무실망에 연결된 컴퓨터에 존재하는 다양한 정보들을 불법적인 사용자의 접근으로부터 적절하게 보호
  - 사무실망 운용에 관한 통계 자료를 수집 및 부당한 침입에 대한 증거 자료를 수집
- 방화벽(firewall)
  - 내.외부의 불법적인 사용자들이 사무실망의 정보에 침입하는 것을 방지하기 위한 침입 차단 시스템
  - 주로 사무실망과 외부 인터넷의 연결 장치인 라우터에 설치

방화벽과 인터넷 보안

- 방화벽의 기능
  - 이메일 서버, 웹 서버 등 일부에 대해서만 외부 사용자가 접근이 가능하도록 제어
  - 특정 호스트 및 서비스에 대한 접근 허용 사용자 목록 지정
  - 내부 사용자에 대해서도 외부 인터넷 접근을 제어
- 패킷 필터링(packet filtering)
  - 목적지 IP 주소, 출발지 IP 주소, 출발지 포트 번호, 목적지 포트 번호 등과 같은 IP, TCP, UDP의 헤더 정보 기반의 패킷 필터링을 통해 접근 제어

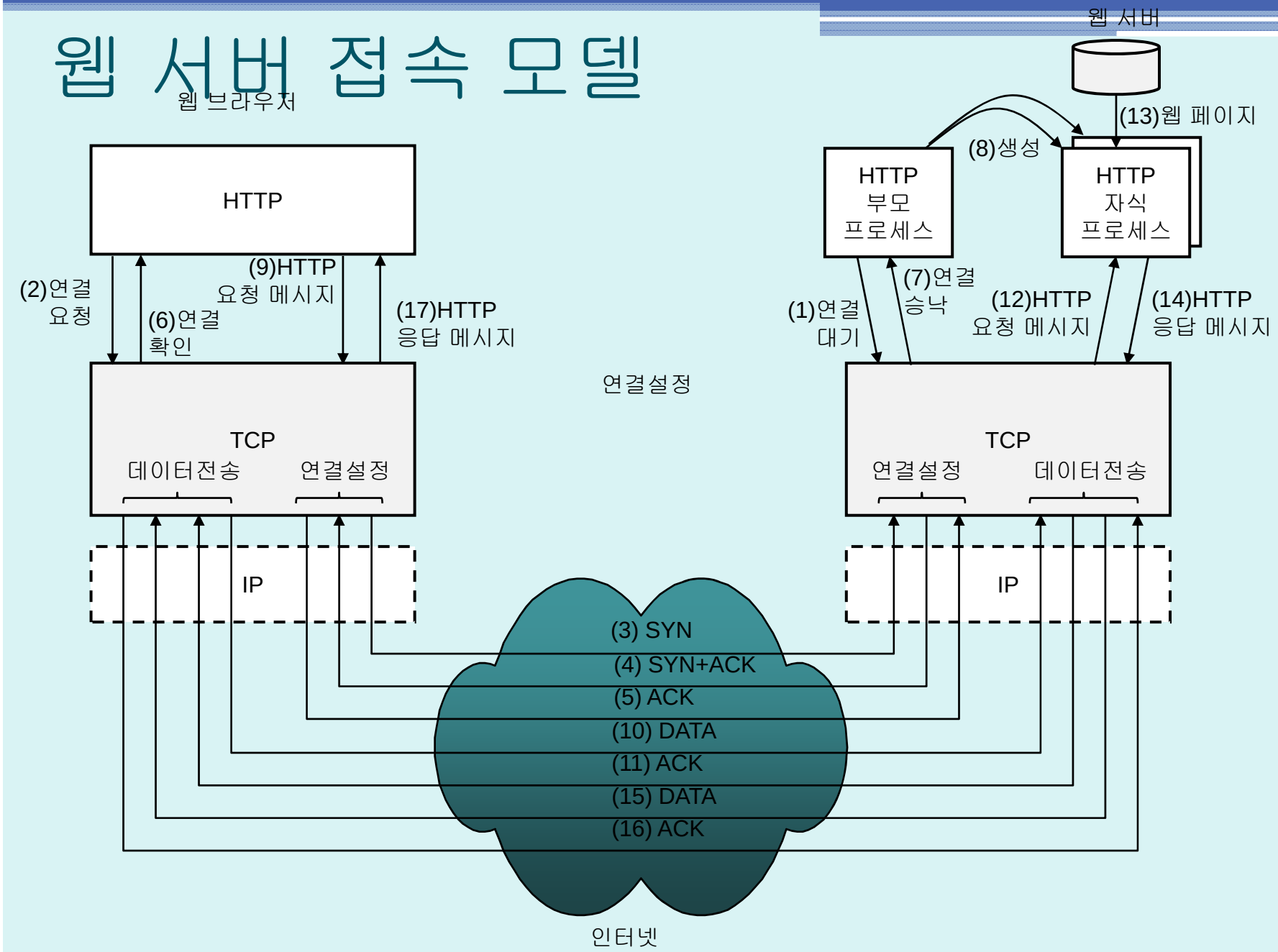
방화벽의 패킷 필터링 규칙

규칙	방향	출발지 IP 주소	목적지 IP 주소	프로토콜	출발지 포트	목적지 포트	동작
1	내부향	외부 IP1	내부 IP2	TCP	1023 이상	23	허용
2	외부향	내부 IP2	외부 IP1	TCP	23	1023 이상	허용
3	외부향	내부 IP3	외부 IP4	TCP	1023 이상	25	허용
4	내부향	외부 IP4	내부 IP3	TCP	25	1023 이상	허용
5	양방향	any	any	any	any	any	거부

인터넷 보안 강화

- 방화벽의 문제점
  - IP, TCP, UDP 등 망 계층과 트랜스포트 계층의 제어 정보에 근거하여 보안 정책을 수행함으로써 응용 서비스 수준에서 정교한 보안 서비스 제공에 한계
- 보안 수준 향상
  - 프록시 서버(proxy server)로 불리는 응용 수준의 게이트웨이(gateway) 장치를 추가로 설치
  - 프로토콜 제어 정보와 사용자 데이터를 안전하게 전송하기 위해 IPSec, PGP, S/MIME, SSL 등 인증과 암호화 기반의 다양한 수준의 보안 프로토콜 지원.

웹 서버 접속 모델


웹 서버
웹 브라우저
(13)웹 페이지
(8)생성
HTTP
부모
프로세스
HTTP
자식
프로세스
HTTP
(2)연결
요청
(9)HTTP
요청 메시지
(6)연결
확인
(17)HTTP
응답 메시지
(1)연결
대기
(7)연결
승낙
(12)HTTP
요청 메시지
(14)HTTP
응답 메시지
연결설정
TCP
데이터전송
연결설정
TCP
연결설정
데이터전송
IP
IP
(3) SYN
(4) SYN+ACK
(5) ACK
(10) DATA
(11) ACK
(15) DATA
(16) ACK
인터넷

웹 서버 접속 절차

- 웹 서버 HTTP는 맨 먼저 자신의 포트 번호(80번)로 요청되는 연결 요청을 기다리도록 TCP에게 지시
- 웹 브라우저측의 TCP는 HTTP에 의한 연결 요청에 의해 SYN 세그먼트를 웹 서버 TCP에게 송신
- 웹 서버 HTTP 프로세스는 웹 브라우저와의 통신을 담당할 자식 프로세스를 생성하고 자신은 또 다른 웹 브라우저로부터의 연결 요청을 대기
- TCP 연결 설정이 완료되면 웹 브라우저는 해당 연결을 통해 웹 서버에게 HTTP 요청 메시지를 송신
- 웹 서버 TCP는 HTTP 요청 메시지를 해당 웹 브라우저를 담당하는 HTTP 자식 프로세스에게 전달
- HTTP 자식 프로세스는 웹 서버로부터 HTTP 요청 메시지가 지시하는 URL의 웹 페이지를 읽어 HTTP 응답 메시지로 웹 브라우저에게 송신