정보보안

OSI 7계층과 프로토콜에 대한 이해

교재: 정보 보안 개론과 실습 (개정3판)
저자: 양대일
출판사: 한빛미디어

수업 목표

- 프로토콜의 필요성을 이해한다.
- 프로토콜의 다양한 기능을 이해한다.
- 네트워크 계층 구조의 필요성을 이해한다.
- 네트워크 계층 구조인 OSI 7계층을 이해한다.
- OSI 7계층의 주요 동작 원리를 이해한다.

프로토콜의 개념 (1/3)

- 본래 의미는 외교에서 의례 또는 의정서

의정서

[議定書, protocol]

요약 일반적인 조약에 비해 중요성이 덜한 부수적 성격의 조약

조약의 형식 중 하나로, 의사록과 같은 의미로 쓰이기도 하지만 본래는 국가 간의 조약을 가리킨다. 외교교섭과 국제회의의 의사 또는 사실의 공식보고에서 관계 당사자들이 서명한 것이거나 일반적인 조약에 비해 중요성이 덜한 부수적 성격의 조약을 뜻한다.

프로토콜의 개념 (2/3)

- 1965년 톰 마릴이 컴퓨터와 컴퓨터 사이에 메시지를 전달하는 과정을 프로토콜이라 부름
  - 컴퓨터가 메시지를 전달하고, 메시지가 제대로 도착했는지 확인하며, 메시지가 제대로 도착하지 않으면 메시지를 재전송하는 일련의 방법을 가리키는 '기술적 은어'라는 뜻

프로토콜의 개념 (3/3)

[그림 2-1] 통역원을 통해 이야기를 나누는 두 대통령

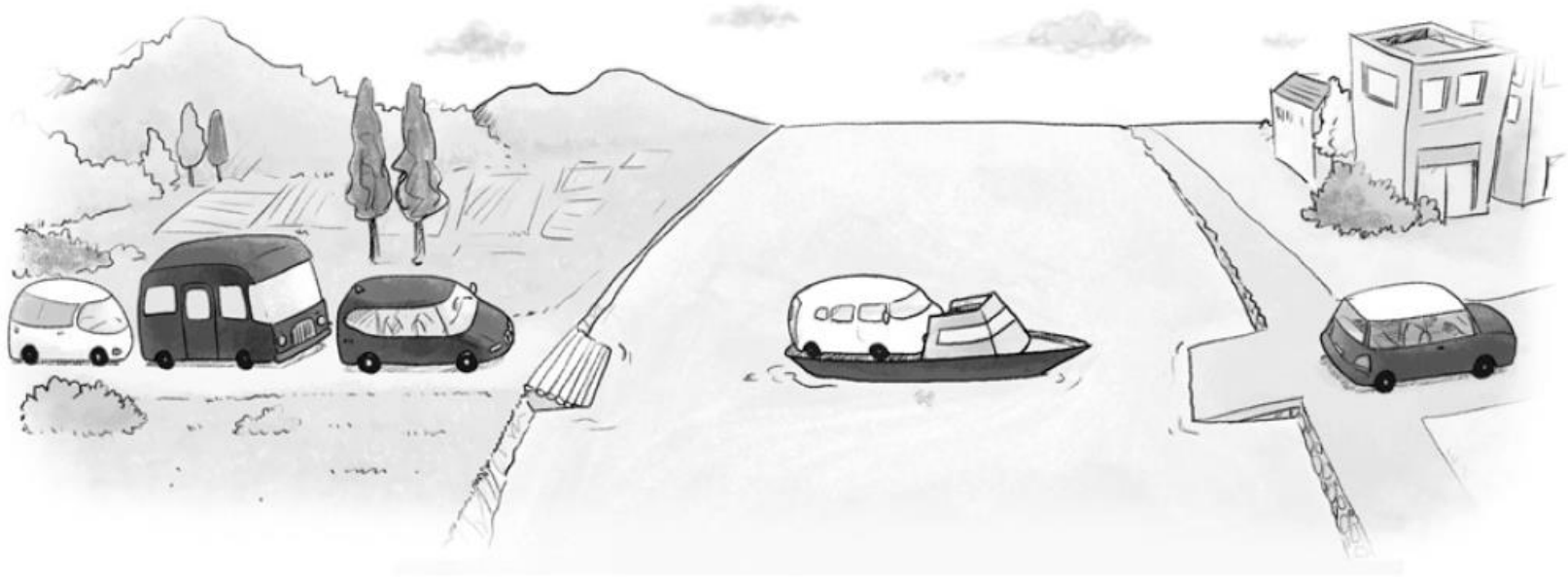
프로토콜의 세 가지 요소

- 구문(syntax)
  - 데이터의 형식이나 신호로, 부호화 방법 등을 정의
- 의미(semantics)
  - 오류 제어, 동기 제어, 흐름 제어 같은 각종 제어 절차에 관한 제어 정보 정의
- 순서(timing)
  - 송/수신자 간 혹은 양단(end-to-end)의 통신 시스템과 망 사이의 통신 속도나 순서 등을 정의

프로토콜의 기능 (1/4)

- 주소 설정(Addressing)
  - 각 전송 계층에 맞는 송신자와 수신자의 주소 지정
- 순서 제어(Sequence Control)
  - 데이터 단위가 전송될 때 보내지는 순서 명시
- 데이터 대열의 단편화 및 재조합(Fragmentation & Reassembly)
  - 전송 효율이 높은 작은 단위로 단편화 및 응용 프로그램에서 사용하기 위해 재조합
- 캡슐화(Encapsulation)
  - 데이터에 제어 정보를 덧붙임

프로토콜의 기능 (2/4)



[그림 2-2] 캡슐화

프로토콜의 기능 (3/4)

- 연결 제어(Connection Control)
  - 연결 설정, 데이터 전송, 연결 해제에 대한 통제 수행
- 흐름 제어(Flow Control)
  - 송신측 개체로부터 오는 데이터의 양이나 속도 조절
- 오류 제어(Error Control)
  - 데이터를 교환할 때 SDU(Service Data Unit)나 PCI(Protocol Control Information)에 대한 오류 검사
- 동기화(Synchronization)
  - 두 개체 간에 데이터가 전송될 때 각 개체는 특정 타이머 값이나 윈도우 크기 등을 통해 서로의 상태를 일치시킴

프로토콜의 기능 (4/4)

- 다중화(Multiplexing)
  - 여러 시스템이 동시에 통신할 수 있는 기법
- 전송 서비스
  - 우선순위 결정, 서비스 등급과 보안 요구 등을 제어

네트워크 계층 구조

- 1970년대 중앙 집중식 네트워크에서 분산형 네트워크로 변하면서 중소형 네트워크 발달
- IBM과 DEC가 대기업 네트워크의 대부분 차지, 이들은 SNA, DECnet이라는 각각의 네트워크 구조 모델 사용
- 개인 컴퓨터가 널리 보급되면서 중소형 네트워크의 필요성 제기, 업체마다 자사 제품끼리만 통신이 가능하게 만들어 이기종 통신에 문제 발생
- ISO는 여러 업체가 만든 시스템을 상호 연동 가능하게 하는 표준 네트워크 모델 제정의 필요성 요구를 수용해 1984년 OSI 네트워크 모델 발표

OSI 7계층 (1/3)

7계층	응용 프로그램 계층 (Application Layer)	사용자나 응용 프로그램 간의 데이터 교환이 가능하게 하는 계층이다. HTTP, FTP, 터미널 서비스, 여러 메일 프로그램, 디렉토리 서비스 등을 제공한다.
6계층	표현 계층 (Presentation Layer)	데이터의 구조를 하나의 통일된 형식으로 표현하고, 데이터의 압축과 암호화 기능을 수행한다.
5계층	세션 계층 (Session Layer)	두 시스템 간의 통신 중 동기화를 유지하고 데이터 교환을 관리한다. 정보 교환을 효과적으로 할 수 있도록 전송 계층에서 설정된 종단 간의 논리적인 연결에 추가 서비스를 제공한다.
4계층	전송 계층 (Transport Layer)	종단 간의 신뢰성 있고, 투명한 데이터 전송을 제공한다. 이를 위해 오류 제어, 통신량 제어, 다중화를 제공하며 응용 프로그램 간 통신을 위해 포트를 사용한다.
3계층	네트워크 계층 (Network Layer)	8비트의 숫자 4개로 구성된 IP 주소 체계로 사용하며, 경로 제어와 통신량 제어 등을 수행한다.
2계층	데이터 링크 계층 (Data Link Layer)	물리적인 링크를 통하여 동기화, 에러 제어, 흐름 제어 등을 통해 패킷을 전송한다. 16진수 12개로 만들어진 MAC 주소를 객체 간 통신에 사용하며, MAC 주소는 고유하다.
1계층	물리 계층 (Physical Layer)	기계적, 전기적, 기능적, 절차적 특성을 정의하며 비트 스트림을 물리적 매체를 통해 전송한다.

[그림 2-3] OSI 7계층 구조

OSI 7계층 (2/3)

- 물리 계층 (1계층)
  - 기계적, 전기적, 기능적, 절차적 특성을 정의하여 구조화되지 않은 비트 스트림을 물리적 매체를 통해 전송
- 데이터 링크 계층 (2계층)
  - 물리적인 링크를 통해 신뢰성 있는 정보 제공. 즉, 동기화, 오류 제어, 흐름 제어 등을 통해 프레임 전송
  - 점대점 (point-to-point)간 신뢰성 있는 전송을 보장
- 네트워크 계층(3계층)
  - 네트워크를 통한 데이터 패킷 전송 담당, 경로 제어(routing)와 흐름 제어, 단편화 등을 수행

OSI 7계층 (3/3)

- 전송 계층(4계층)
  - 양끝단 (end-to-end)의 사용자들의 신뢰성 있는 데이터 송수신
  - 이를 위해 양단간에 오류 제어, 통신량 제어, 다중화 제공
- 세션 계층 (5계층)
  - 프로세스 간의 대화 연결 확립/관리/해제하려고 체크포인트, 재시작, 차단 서비스 수행
- 표현 계층 (6계층)
  - 응용 프로그램 계층 개체 간의 정보를 표현하는 구문을 하나의 통일된 형식으로 표현
- 응용 계층 (7계층)
  - 사용자나 응용 프로그램 사이에 데이터 교환을 가능하게 함

프로토콜 계층화

- 복잡하고 다양한 유형의 통신 기능을 하나의 큰 프로토콜로 정의하기 거의 불가능하여 프로토콜 계층화
- 기능별로 계층을 구분하여 각 기능에 맞게 표준화 진행
- 네트워크의 추가, 변경, 유지 보수 등의 문제 해결 편리

인터넷 프로토콜 (TCP/IP)

[그림 3-2] OSI 7계층과 TCP/IP 4계층

물리 계층

- 1계층으로, 시스템 간의 연결선(랜 케이블, 동축 케이블, 전화선, 전자 파장 전달 공간 등)
- 실제 장치를 연결하는 데 필요한 전기적, 물리적 세부 사항 정의
- 물리 계층 장치 : 허브나 리피터

ANSI/EIA 표준 568의 데이터 속도에 따른 1계층 케이블 구분

카테고리	최대 속도	용도
CAT 1	1Mbps 미만	• 아날로그 음성(일반적인 전화 서비스) • ISDN 기본율 접속(Basic Rate Interface) • Doorbell wiring
CAT 2	4Mbps	• 주로 IBM의 토큰링 네트워크에 사용
CAT 3	16Mbps	• 10BASE-T 이더넷의 데이터 및 음성
CAT 4	20Mbps	• 16Mbps 토큰 링에서 사용. 많이 사용되지는 않음
CAT 5	100Mbps	• 옥내 수평 및 간선 배선망(100MHz) • 4/16Mbps 토큰 링(IEEE 802.5) • 10/100 BASE-T(IEEE 802.3) • 155Mbps ATM
CAT 6	250Mbps	• 옥내 수평 및 간선 배선망(250MHz) • 4/16Mbps 토큰 링(IEEE 802.5) • 10/100/1000 BASE-T(IEEE 802.3) • 155/622Mbps ATM • 기가비트 이더넷

케이블의 구분

구분	내용
UTP(Unshielded Twisted Pair)	두 선 간의 전자기 유도를 줄이기 위해 절연의 구리선이 서로 꼬여 있다. 제품 전선과 피복만으로 구성되어 있다.
FTP(Foil Screened Twisted Pair)	알루미늄 은박이 4가닥 선을 감싸고 있다. UTP보다 절연 기능이 탁월해 공장 배선용으로 많이 사용한다.
STP(Shielded Twisted Pair)	연선으로 된 케이블 겉에 외부 피복, 또는 차폐재가 추가되었다(쉴드 처리). 차폐재가 접지 역할을 하므로 외부 노이즈를 차단하거나 전기적 신호 간섭을 줄이는 데 탁월하다.

커넥터

RJ-11

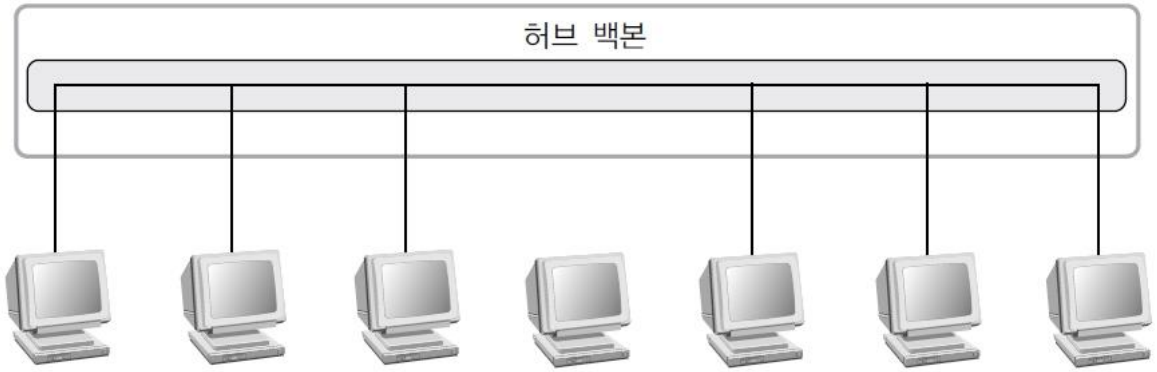
RJ-45

물리 계층 관련 장비

- 리피터(Repeater)
  - 네트워크 연장 장비
  - 거리가 일정 이상이 되면 신호 세기가 약해져서 0과 1의 디지털 신호를 분석하기 어려워진다는 점을 해결하기 위해 리피터 사용
  - 불분명해진 신호 세기를 다시 증가시키는 역할을 함

물리 계층 관련 장비

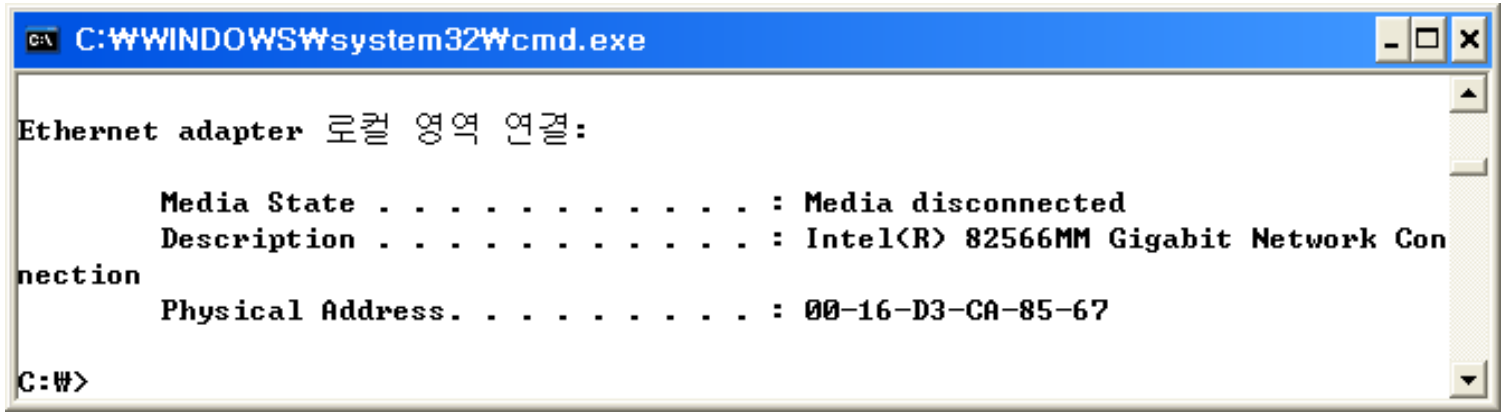
- 더미 허브(Hub)
  - 허브는 요즘에 쓰이는 스위치의 옛날 형태
  - 흔히 최근의 스위치를 스위칭 허브라고 부르고, 이전 허브를 더미 허브라 부름
  - 더미 허브는 네트워크 구조 관점에서 버스 구조를 하고 있다고 볼 수 있음



[그림 3-6] 버스 구조의 허브

데이터 링크 계층 (1/2)

- 랜 카드나 네트워크 장비의 하드웨어 주소만으로 통신하는 계층
- MAC(Media Access Control) 주소는 네트워크 카드마다 붙는 고유 이름. 윈도우 명령 창에서 ipconfig /all 명령으로 확인



- OUI

데이터 링크 계층 (2/2)

- 총 12개의 16진수로 구성. 앞쪽 6개는 네트워크 카드를 만든 회사를 나타내는 OUI(Organizational Unique Identifier) → 어느 회사에서 만든 제품인지 알 수 있음
- 뒤쪽 6개는 호스트 식별자(Host Identifier)로 각 회사에서 임의로 붙이는 일종의 시리얼 → OUI가 같은 회사도 없고, 한 회사에서 시리얼이 같은 네트워크 카드를 만들지 않기 때문에, 같은 MAC 주소는 존재하지 않음

OUI	Host Identifier
00-16-D3	CA-85-67

데이터 링크 계층 관련 장비 (1/2)

- 브리지(Bridge)
  - 초기의 랜과 랜을 연결하는 네트워크 장치
  - 데이터 링크 계층에서 통신 선로를 따라 한 네트워크에서 그 다음 네트워크로 데이터 프레임을 복사하는 역할
  - 브리지에 프레임이 들어오면 MAC 주소를 확인해 목적지 MAC 주소가 프레임이 들어온 인터페이스에 있으면 해당 패킷을 막고, 프레임이 들어온 인터페이스가 아닌 다른 인터페이스 쪽에 있으면 전달

데이터 링크 계층 관련 장비 (2/2)

- 스위치(Switch)
  - 기본적으로 L2(Layer 2), 즉 데이터 링크 계층에서 작동하는 스위치
  - L3, L4 스위치는 L2 스위치에 상위 계층의 네트워킹 기능을 추가한 것
  - L2 스위치는 스타형 네트워크로 더미 허브가 연결된 시스템이 늘어날수록 패킷 간 충돌 때문에 매우 낮은 속도로 동작하는 문제점을 해결하는 획기적인 방안

스위칭 방식 (1/2)

- 패킷 전송 방식에 따라 컷스루(cut-through) 방식, 저장 후 전송(store & forward) 방식과 인텔리전트 스위칭(intelligent switching) 방식으로 구분
- 제공 경로의 대역폭에 따라 전이중(full-duplex)과 반이중(half-duplex) 방식으로 구분
- 컷스루 방식
  - 수신한 프레임의 목적지 주소를 확인하고 목적지 주소의 포트로 프레임을 즉시 전송
  - 지연 시간이 최소화되나 수신한 패킷에 오류가 발생할 때는 목적지 장치에서 폐기

스위칭 방식 (2/2)

- 저장 후 전송 방식
  - 완전한 프레임을 수신하여 버퍼에 보관했다가 전 프레임을 수신한 후 CRC 등 오류를 확인하고 정상 프레임을 목적지 포트로 전송
  - 패킷 길이에 비례해 전송 지연이 발생하지만 브리지나 라우터보다 훨씬 신속하게 이루어짐
- 인텔리전트 스위칭 방식
  - 보통 컷스루 모드로 작동하다가 오류가 발생하면 저장 후 전송 모드로 자동 전환하여 오류 프레임을 전송하는 것을 중지
  - 오류율이 0이 되면 자동으로 다시 컷스루 방식으로 전환

네트워크 계층

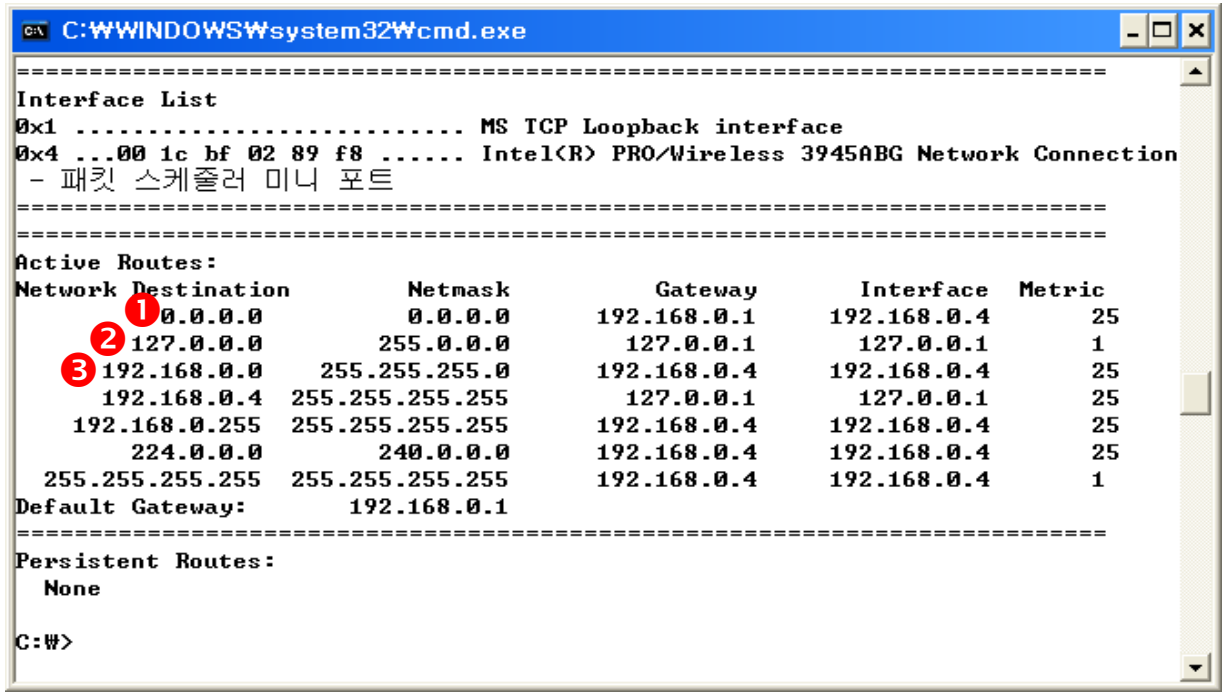
- 랜을 벗어난 통신을 하기 위해 네트워크 계층에서 IP 주소 사용
- IP 주소는 각 랜의 주소, 즉 세계에 펼쳐진 네트워크의 주소
- 라우터
  - 네트워크 계층의 대표 장비
  - 게이트웨이라고도 하는데, 게이트웨이는 원래 서로 다른 프로토콜을 사용하는 네트워크를 연결해주는 장비
  - 게이트웨이처럼 논리적으로 분리된 둘 이상의 네트워크를 연결하는 역할과 반대로 로컬 네트워크에서 브로드캐스트를 차단하여 네트워크를 분리하는 역할 수행
  - 가장 중요한 기능은 패킷 교환망에서 패킷의 최적 경로를 찾기 위한 라우팅 테이블을 구성하고, 이 라우팅 테이블에 따라 패킷을 목적지까지 가장 빠르게 보내는 길잡이 역할

라우터

소형/대형 라우터

라우팅

- 네트워크 계층 통신을 하는 모든 장치는 라우팅 테이블을 가지고 있음
- PC의 라우팅 테이블 예



PC의 라우팅 테이블 예

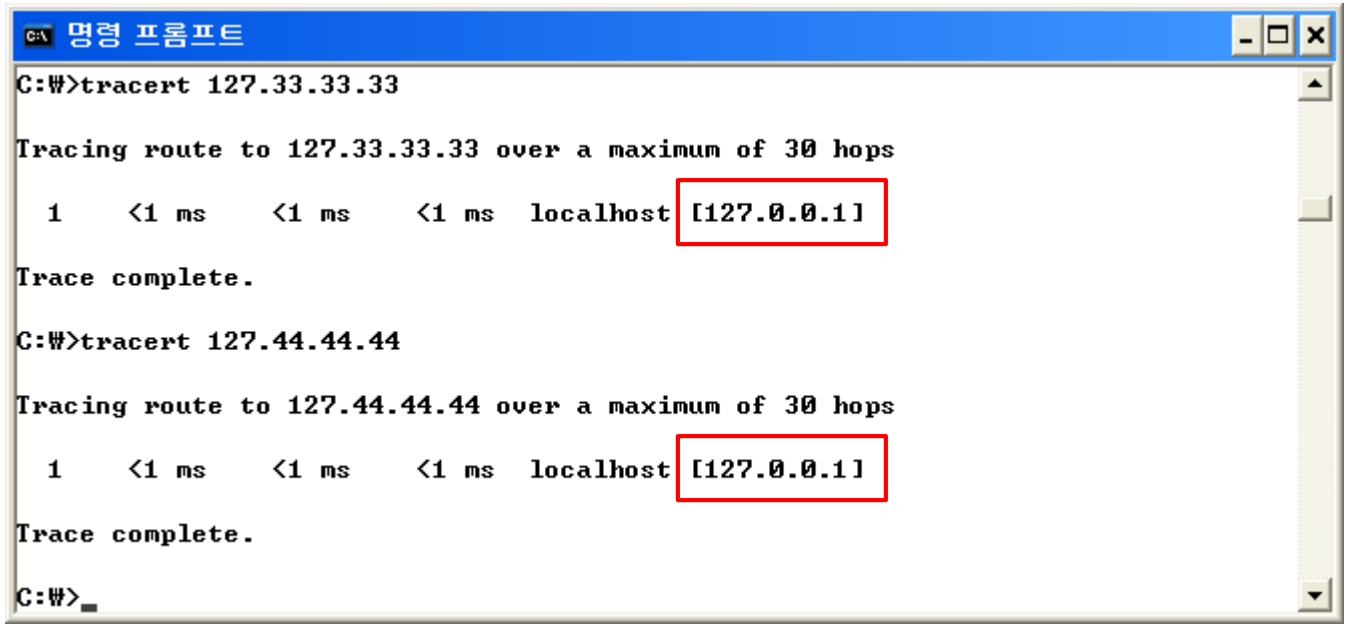
❶ 목적지 0.0.0.0은 라우팅 테이블에 목적지로 따로 명시되지 않은 모든 목적지 주소, 라우팅 테이블에서 직접 구체적으로 지정한 주소 외의 모든 목적지 주소는 192.168.0.4 인터페이스를 통해서 게이트웨이 192.168.0.1로 보내라

❷ 목적지 주소가 127로 시작하는 모든 패킷에 대해 루프백 주소인 127.0.0.1로 보내라

❸ 로컬 네트워크(LAN)에 있는 호스트이므로 192.168.0.1로 보내지 않고, LAN에서 상대방을 찾으라

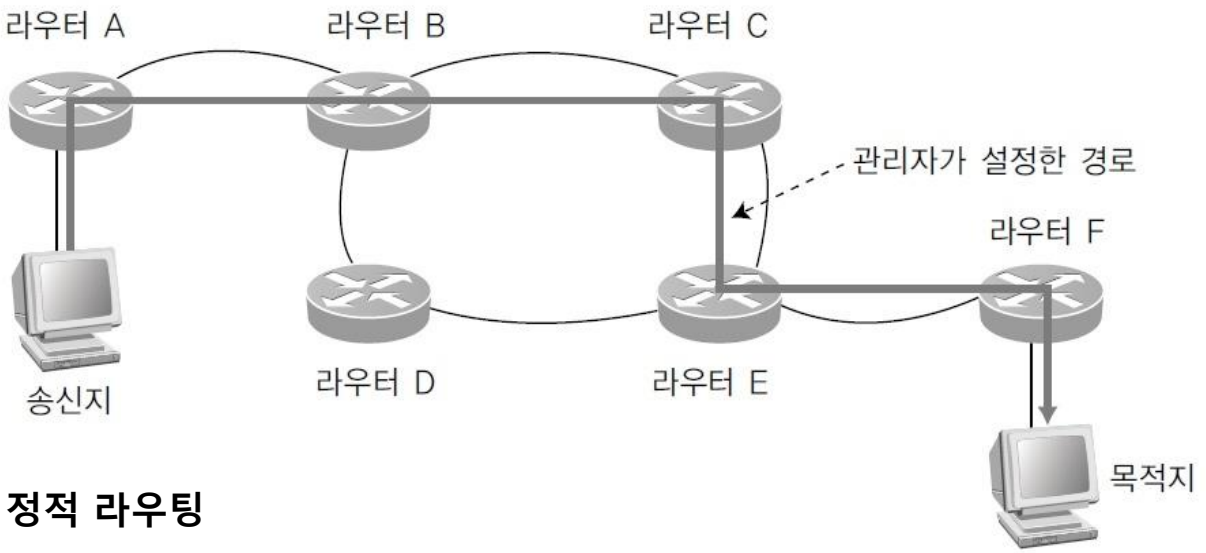
라우팅 동작 예

- tracert 명령을 사용해 127로 시작하는 경로로 ICMP 패킷 전송
  - 두 경우 모두 127.0.0.1로 패킷을 보냄



정적 라우팅 (1/2)

- 관리자의 권한으로 특정 경로를 통해서만 패킷이 지날 수 있도록 설정한 것



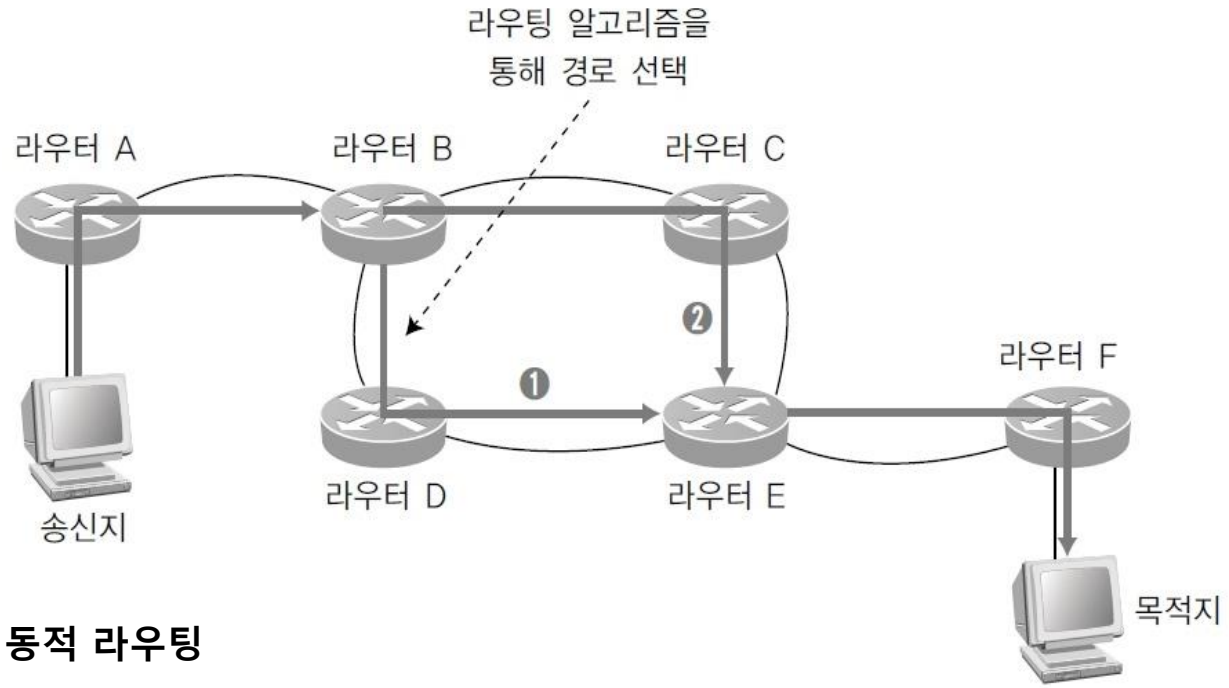
정적 라우팅

정적 라우팅 (2/2)

- 경로 설정이 실시간으로 이루어지지 않기 때문에 초기에 관리자가 다양한 라우팅 정보를 분석하여 최적의 경로 설정이 가능
- 라우팅 알고리즘을 통한 경로 설정이 이루어지지 않기 때문에 라우터의 직접적인 처리 부하가 감소
- 네트워크 환경 변화에 능동적인 대처가 어려움
- 네트워크 환경 변화 시 관리자가 새로운 라우팅 정보를 통해 경로를 재산출하여 각 라우터에 제공해야 함
- 비교적 환경 변화가 적은 형태의 네트워크에 적합

동적 라우팅 (1/2)

- 라우터가 네트워크 연결 상태를 스스로 파악하여 최적의 경로를 선택해 전송하는 방식



동적 라우팅

동적 라우팅 (2/2)

- 경로 설정이 실시간으로 이루어지기 때문에 네트워크 환경 변화에 능동적인 대처 가능
- 라우팅 알고리즘을 통해 자동으로 경로 설정이 이루어지기 때문에 관리 쉬움
- 주기적인 라우팅 정보 송수신으로 인한 대역폭 낭비 초래
- 네트워크 환경 변화 시 라우터에 의한 경로 재설정으로 라우터의 처리 부하가 증가하고 지연 발생
- 수시로 환경이 변하는 형태의 네트워크에 적합

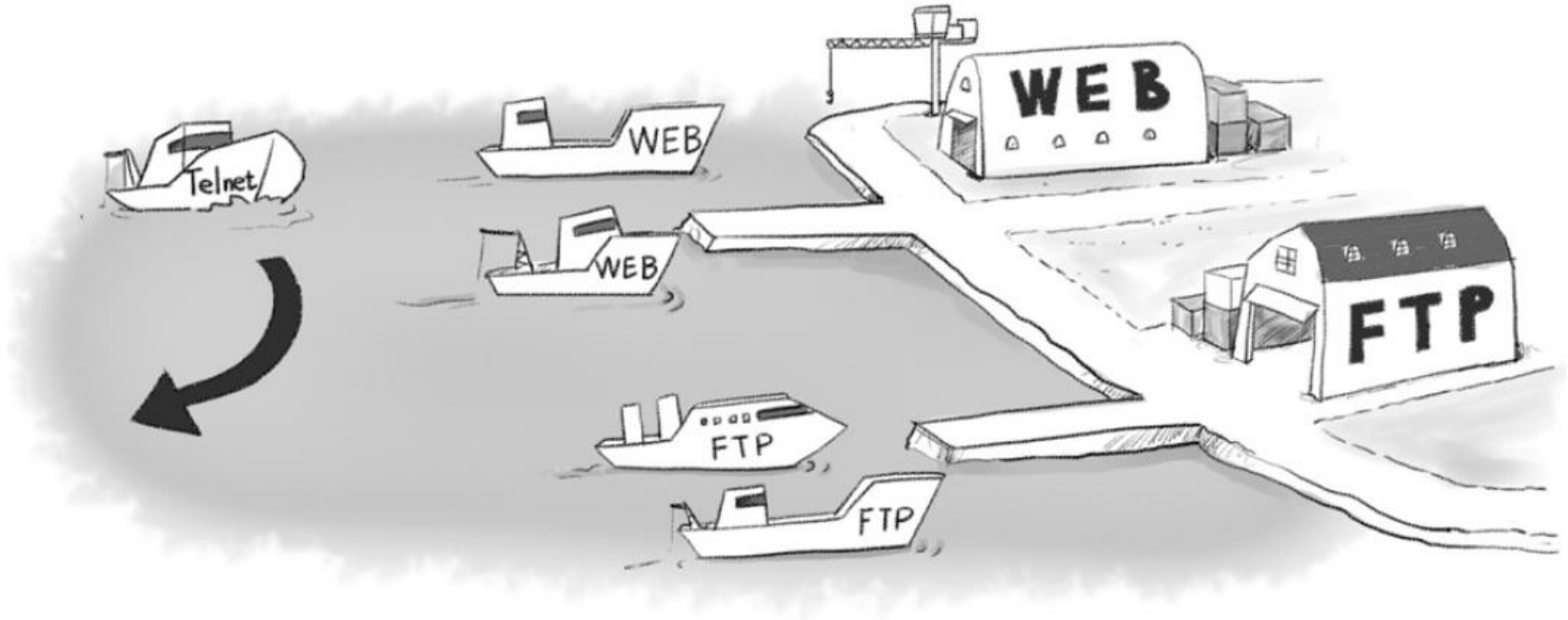
정적/동적 라우팅 비교

구분	정적 라우팅	동적 라우팅
라우팅 테이블 관리	• 수동 • 네트워크의 변화(라우터 추가/변경/회선 장애 등)에 대한 자동 인지 불가	• 자동 • 네트워크의 변화를 자동으로 인지하여 정보의 전송 경로를 재구성
처리 부하	• 라우팅 테이블의 갱신을 위한 별도의 부하 없음 • CPU와 메모리에 부하 적음 • 네트워크 장애의 실시간 관리를 위한 NMS와 각 라우터 간의 정보 전송이 많음(CPU에 부하 다소 발생)	• 라우팅 테이블의 갱신을 위해 라우터 간 정보 교환 • CPU와 메모리에 부하 많음 • 네트워크의 장애를 실시간으로 관리할 필요가 없음
백업 구성	• 백업 구성이 곤란함 • 별도의 네트워크 장비를 이용하여 회선 백업 가능	• 백업 구성이 쉬움(회선, 장비)
복구 기능	• 백업 회선이 있는 경우 회선 장애 시 수 초 내로 복구 가능 • 기타 장애 시 최소 10분 이상의 복구 시간 필요(백본 라우터의 장애 시 30분 이상 소요)	• 백업 회선이 있는 경우 수 초 내로 복구 가능
인터페이스	변경이 적을 때 유리	변경이 많을 때 유리
노드 추가/변경/확대	운영 요원이 라우팅 작업	대처 용이
중간 경로	단일 경로에 적합	다중 경로에 적합

전송 계층 (1/2)

- 대표 프로토콜은 TCP
- TCP가 가진 주소를 포트(port)라 함
  - MAC 주소가 네트워크 카드의 고유 식별자고 IP가 시스템의 논리적인 주소라면, 포트는 시스템에 도착한 후 패킷이 찾아갈 응용 프로그램과 통하는 통로 번호
  - 포트는 0~65535(216)번까지 존재하며, IP나 MAC 주소처럼 출발지와 목적지에 응용 프로그램별로 포트 번호를 가지고 통신

전송 계층 (2/2)



[그림 3-17] 포트별 정해진 응용 프로그램

주요 포트와 서비스

- 0~1,023번(1,024개)을 잘 알려진 포트(Well Known Port)라고 부름
- 보통 0번 포트는 사용하지 않으며, 1,023번 포트까지는 대부분 고유의 사용 용도가 있음

[표 3-4] 주요 포트와 서비스

포트 번호	서비스	포트 번호	서비스
20	FTP	80	HTTP
21	FTP	110	POP3
23	Telnet	111	RPC
25	SMTP	138	NetBIOS
53	DNS	143	IMAP
69	TFTP	161	SNMP

패킷 구조와 예 (1/2)

- 출발지 포트는 운영체제나 응용 프로그램마다 조금씩 다르나 보통 1,025번~65,535번 중 사용하지 않는 임의의 포트를 응용 프로그램별로 할당하여 사용

01001010101	출발지 포트	목적지 포트	출발지 IP	목적지 IP	출발지 MAC	목적지 MAC
5계층까지의 패킷 정보	4계층 패킷 정보		3계층 패킷 정보		2계층 패킷 정보	

- 클라이언트가 인터넷에 존재하는 웹 서버에 접속한다고 가정하면, 웹 서버의 서비스 포트는 보통 80번

01001010101	출발지 포트	80	출발지 IP	목적지 IP	출발지 MAC	목적지 MAC
5계층까지의 패킷 정보	4계층 패킷 정보		3계층 패킷 정보		2계층 패킷 정보	

패킷 구조와 예 (2/2)

- 출발지 포트는 시스템에서 임의로 정해져 알 수가 없으나 대략 3000번 대의 임의 포트가 할당

<table>
<tr><td>01001010101</td><td>3405</td><td>80</td><td>출발지 IP</td><td>목적지 IP</td><td>출발지 MAC</td><td>목적지 MAC</td></tr>
<tr><td>5계층까지의 패킷 정보</td><td colspan="2">4계층 패킷 정보</td><td colspan="2">3계층 패킷 정보</td><td colspan="2">2계층 패킷 정보</td></tr>
</table>

Question & Answer