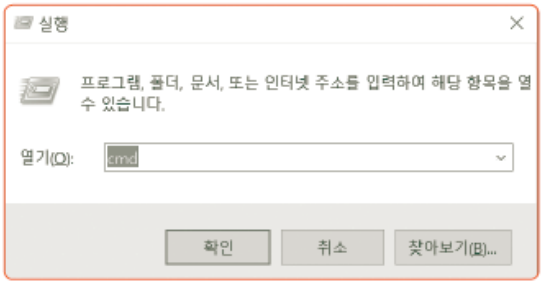
디지털보안학

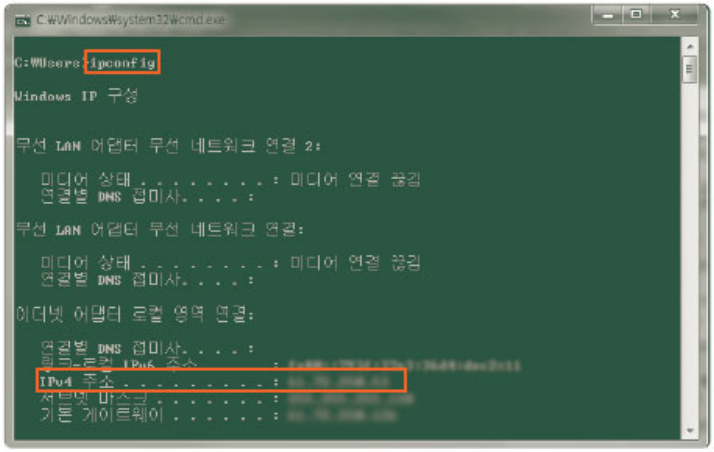
[3주차. 인터넷보안1]

우리집의 인터넷 환경을 살펴보자

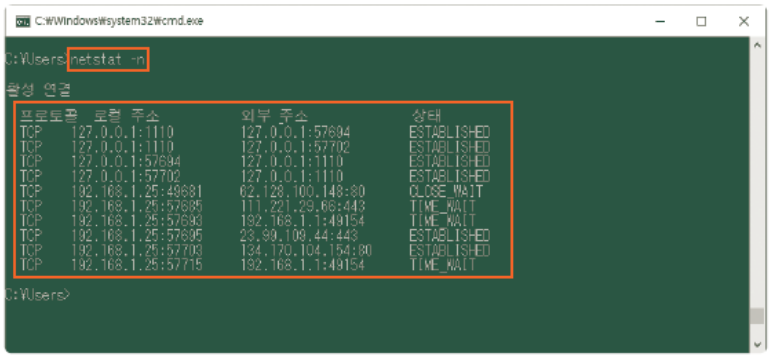
- 인터넷이 어떻게 연결되어 있으며 어떤 정보가 오고 가는지를 통해 예상되는 공격 및 예상 공격대상 파악
- IP 주소 확인
  - 윈도우에서 [Ctrl] + [Esc] 클릭
  - [프로그램 및 파일 검색] 창에 'cmd'입력 후 확인 클릭



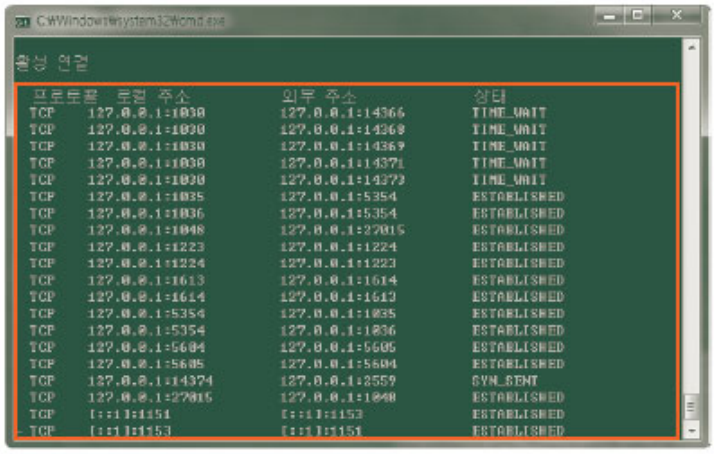
– 명령어 프롬프트에 ‘ipconfig’ 입력 후 [Enter]



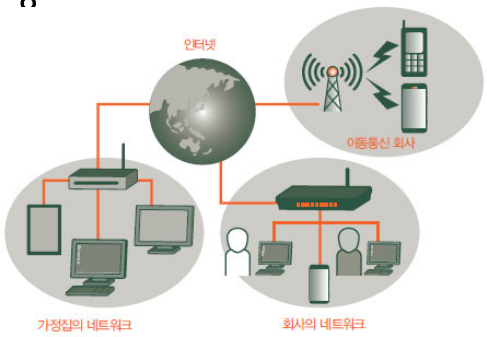
- 포트 번호 확인
  – 명령어 프롬프트에서 ‘netstat -n’ 입력하면 로컬 주소와 외부 주소 표시



- 웹 브라우저로 상명대학교 웹사이트(http://www.smu.ac.kr) 실행 후 한번 더 명령어 프롬프트에서 'netstat -n' 실행
  - ✓ 조금 전보다 표시 내용 늘어났음을 확인

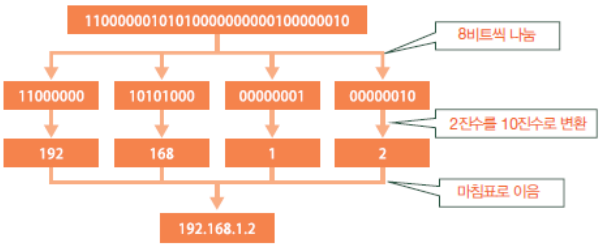


- 인터넷에는 어떻게 연결되는가?
  - IP 주소와 포트 번호
    - ✓ 네트워크란 여러 대의 컴퓨터를 케이블이나 무선으로 연결하여 정보 주고받는 것
    - ✓ 인터넷은 집, 회사 등의 작은 네트워크가 외부의 더 큰 네트워크에 연결되어 구성

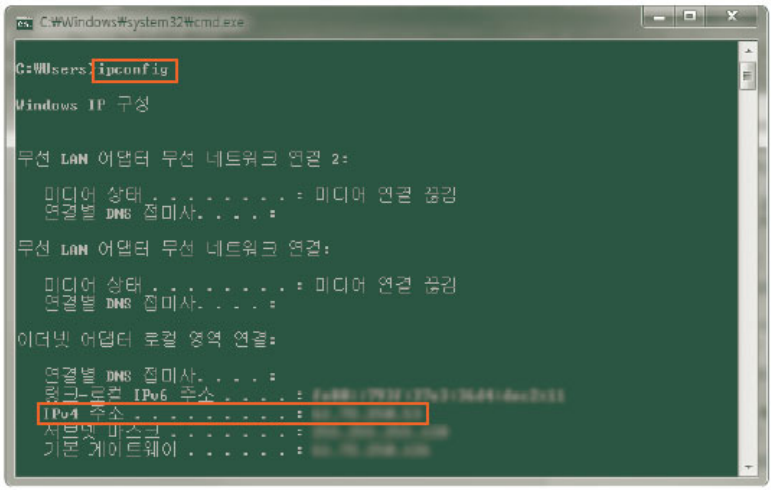


– IP 주소로써 컴퓨터의 네트워크상의 위치를 식별
  ✓ IPv4 (Internet Protocol version 4)
  ✓ IPv6 (Internet Protocol version 6)

  ✓ IP 주소는 32비트 정숫값이며, 컴퓨터 내부에서는 2진수로 처리
  ✓ 32비트 정숫값을 8비트씩 4개로 나누어 10진수로 IP주소 표시



  ✓ IP주소 확인을 위해 윈도우 PC의 명령어 프롬프트 열어 'ipconfig' 명령어 실행



- IP 주소로 컴퓨터 장소 지정한 후, 그 컴퓨터상에서 동작하는 여러 프로그램 중 어떤 것과 통신할지를 포트 번호를 통해 지정
  - ✓ IP 주소가 건물 주소라면, 포트번호는 방 번호에 해당
  - ✓ 잘 알려진 서비스 포트 (well known port) 라는, 네트워크 서비스마다 정해진 포트 번호가 존재

포트 번호	서비스 내용
20	FTP (데이터)
21	FTP (제어)
22	SSH
23	Telnet
25	SMTP
80	HTTP
110	POP3
443	HTTPS
587	Submission (이메일 발송)

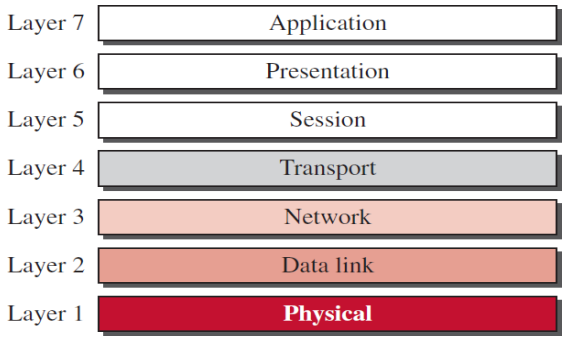
- ✓ 통신을 실행하기 위해서는 서버 측뿐 아니라 클라이언트 측도 발송 포트 번호 지정해야 함
- ✓ 발송 포트 번호는 각각 다른 번호 사용하도록 OS가 관리하는 것이 일반적
  - 임시 포트 (ephemeral port)
- ✓ 명령어 프롬프트에서 netstat 명령어 실행하여 포트 번호 확인 : netstat -n

- 통신 프로토콜 (protocol)
  - ✓ 인터넷에서 컴퓨터가 정보 주고받기 위해 표준화된 규약
  - ✓ 규칙을 정해놓음으로써 서로 다른 제조사, 서로 다른 설계 방식으로 개발된 기종 간 문제없이 정보를 교환할 수 있음

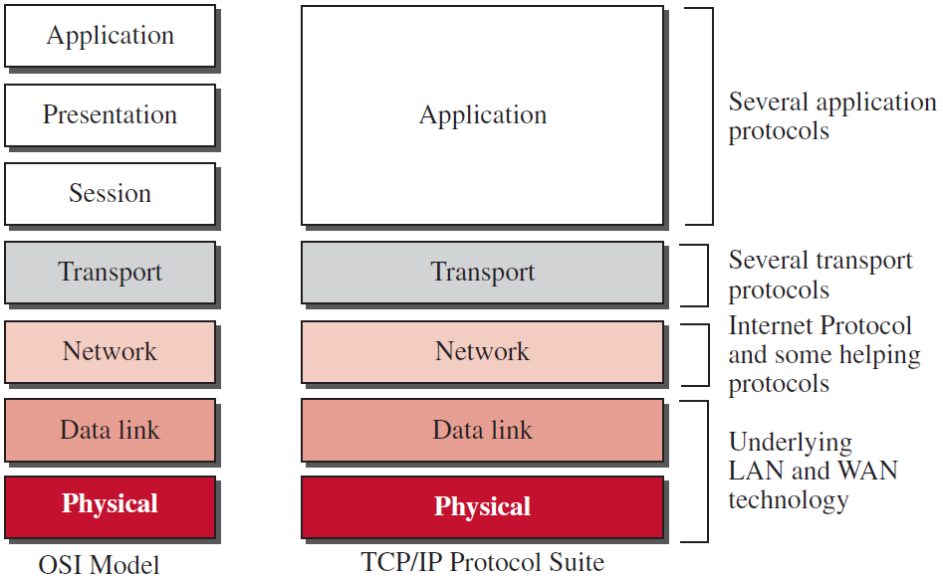
- TCP/IP

네트워크에 대한 이해

- OSI 7계층 (Open System Interconnection)
  - 국제표준화기구(ISO : International Organization for Standardization)는 다양한 네트워크의 호환을 위해 OSI 7계층이라는 표준 네트워크 모델을 만듦.

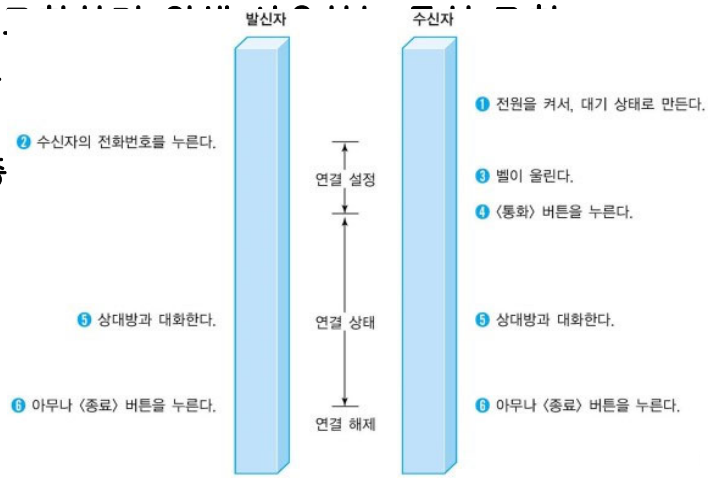


OSI vs. TCP/IP (Transmission Control Protocol/Internet Protocol)



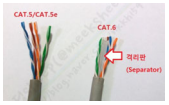
Protocol

- 통신 시스템이 데이터를 [illegible]
  - OSI 7계층 모델에서는 독립적이라고 간주
  - 따라서 계층 1에는 계층 계층 2에는 계층 2끼리



물리 [Physical]

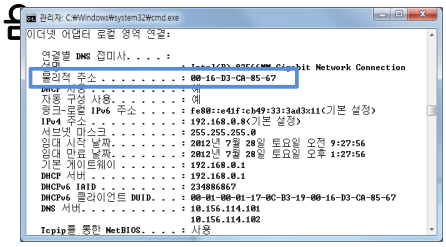
- 물리 계층은 사용자가 전송한 데이터를 장치 간 주고받을 수 있는 형태로 변환하는 계층
- 물리 계층 특성들
  - 전기적 특성 : 전압의 크기와 전압이 변하는 시점에 관련된 특성입니다
  - 기능적 특성 : 물리적으로 연결된 장치 간 데이터를 주고받을 때 쓰이는 케이블의 기능적 특성입니다
  - 절차적 특성 : 데이터를 성공적으로 전송하기 위한 규정을 말합니다
  - 물리적 특성 : 표준 케이블 사이의 물리적 연결에 대해 정의합니다
- 물리 계층은 데이터를 0과 1로 표현하는 등의 신호 전송만을 수행하는 계층이므로, 오류가 생겼는지 문제는 없는지에 관한 것에는 관여하지 않음
- 사용되는 장비로는 UDP(Unshielded Twisted Pair)와 STP(Shielded Twisted Pair) 등



데이터링크 [Data Link]

- 데이터링크 계층은 직접 연결된 2개의 네트워크 장치 사이의 데이터 전송을 담당하며, 두 포인트(Point to Point) 간 신뢰성 있는 전송을 보장하기 위한 계층
- 데이터링크 계층 기능
  - 프레이밍(Framing) : 1계층에서 수신한 데이터를 조합하여 프레임(Frame) 단위로 만들어 처리합니다. 또는 위의 계층에서 내려온 데이터를 프레임 단위로 만들어 신호로 전송합니다. 이때 각 계층별로 고정된 크기의 데이터 유닛을 일반적으로 PDU(Protocol Data Unit)이라고 합니다
  - 흐름 제어(Flow Control) : 송신 측과 수신 측 사이의 오가는 데이터가 너무 많거나 너무 적지 않도록 데이터의 흐름을 적절히 제어합니다
  - 오류 제어(Error Control) : 프레임을 전송할 때 발생한 오류를 복원하거나 재전송합니다.
  - 접근 제어(Access Control) : 네트워크 상의 통신 매체가 여럿 존재할 경우, 각 장치들의 통신 상황을 고려하여 데이터의 전송 가능 여부를 판단합니다
  - 동기화(Synchronization) : 데이터링크 계층 프로토콜에 따라 프레임을 구분하거나 전송된 프레임의 타이밍 정보를 맞추기 위해 필요한 비트 패턴을 제공합니다

- 기능들을 수행하기 위해서 데이터링크 계층에서는 헤더와 트레일러라는 것을 사용
  - 헤더에는 송신 장치 & 수신 장치의 주소
  - 트레일러에는 오류 검출을 위한 코드가 들어감
- 사용되는 장비로는 대표적으로 스위치(Switch)가 있음
- 상호 통신을 위해 MAC 주소를 할당받는데, MAC 주소는 ipconfig /all 명령을 실행해 확인할 수 있음



네트워크 [Network]

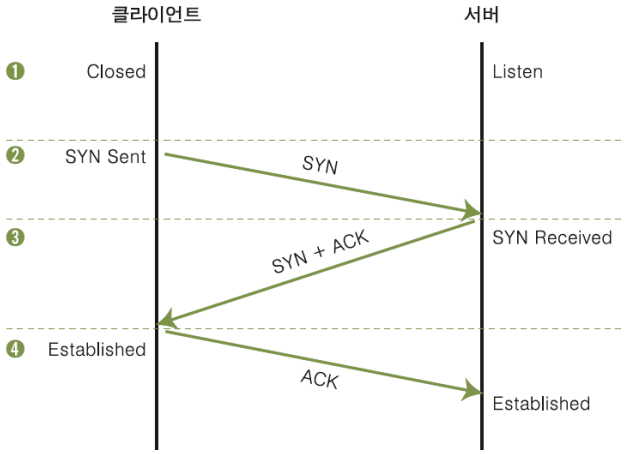
- 네트워크 계층에서는 상위 계층으로부터 받은 데이터를 패킷(Packet) 혹은 데이터그램(Datagram)이라는 단위로 규격화해서 송수신하는 역할
  - 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층.
  - 2계층에서는 MAC주소로 통신했다면 3계층에서는 IP 주소를 기반으로 통신
- 네트워크 계층의 주요 역할
  - 패킷 전달(Packet Forwarding) : 종단 간 패킷 전달을 합니다.
  - 라우팅(Routing) : 종단 간 패킷을 전송할 때, 라우팅 프로토콜을 이용하여 가장 효율적인 경로를 통해 전달송합니다.
  - 논리 주소(Logical Address) : IP 주소라는 논리적인 주소를 사용함으로써, 사용자 데이터를 목적지 장치까지 전달합니다.
- 사용되는 장치가 라우터(Router), L3 스위치(L3 Switch) 등등이 있습니다.

전송 [Transport]

- 전송 계층은 종단 간 데이터 통신을 제어하며, 세그먼트(Segment)라는 이름의 데이터 유닛을 사용
- 이전의 계층에서는 데이터를 전송하는데 의의를 두었다면 전송 계층부터는 사용자가 사용하는 서비스와 직접적으로 관련된 역할을 수행
- 전송 계층의 주요 역할
  - 종단 간 데이터 통신 보장 : 흐름 제어와 오류 제어 등을 수행함으로써 데이터의 통신을 보장합니다.
  - 지연(Delay)에 따른 문제 해결
  - 동시에 여러개의 논리적 연결 지원
  - 사용자 데이터 분할 및 재조합 : 사용자가 송신하는 데이터를 전송 가능한 고정된 크기의 세그먼트로 분할합니다. 그 후 순서 번호를 할당하고 송신합니다. 이때 수신한 데이터는 이 번호를 토대로 재조립하거나 폐기하는 역할을 합니다.

포트 번호	서비스	설명
20	FTP	• File Transfer Protocol-Datagram • FTP 연결 시 실제로 데이터를 전송한다.
21	FTP	• File Transfer Protocol-Control • FTP 연결 시 인증과 제어를 한다.
23	Telnet	• 텔넷 서비스로, 원격지 서버의 실행창을 얻어낸다.
25	SMTP	• Simple Message Transfer Protocol • 메일을 보낼 때 사용한다.
53	DNS	• Domain Name Service • 이름을 해석하는 데 사용한다.
69	TFTP	• Trivial File Transfer Protocol • 인증이 존재하지 않는 단순한 파일 전송에 사용한다.
80	HTTP	• Hyper Text Transfer Protocol • 웹 서비스를 제공한다.
110	POP3	• Post Office Protocol • 메일 서버로 전송된 메일을 읽을 때 사용한다.
111	RPC	• Sun의 Remote Procedure Call • 원격에서 서버의 프로세스를 실행할 수 있게 한다.
138	NetBIOS	• Network Basic Input Output Service • 윈도우에서 파일을 공유할 수 있게 한다.
143	IMAP	• Internet Message Access Protocol • POP3와 기본적으로 같으나, 메일이 확인된 후에도 서버에 남는다는 것이 다르다.
161	SNMP	• Simple Network Management Protocol • 네트워크 관리와 모니터링을 위해 사용한다.

- 3-웨이 핸드셰이킹(3-way handshaking)



세션 [Session]

- 세션 계층은 종단 간 통신 세션의 시작과 종료를 의미하며, 세션 계층에서부터는 데이터 유닛을 메시지(message)라고 함
- 세션 계층의 역할로는 메시지 그룹화, 데이터 전송 방향 결정, 데이터 중간 점검 및 복구를 위한 동기 점 생성과 같은 역할을 함

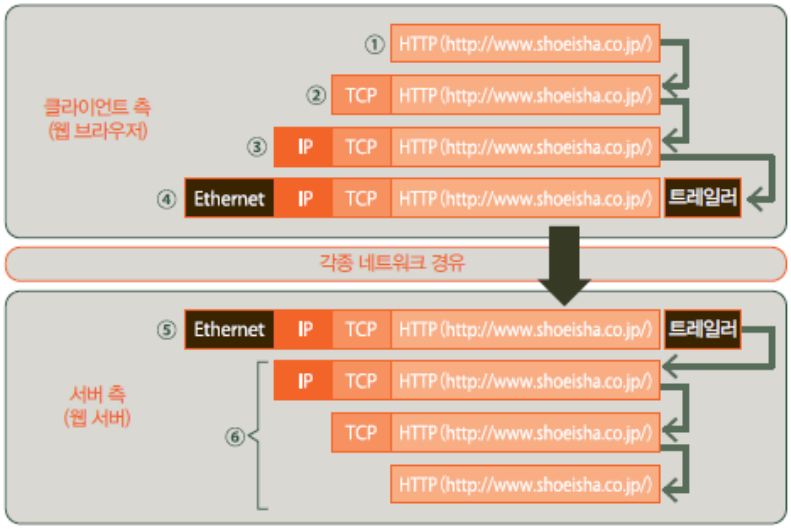
표현 [Presentation]

- 표현 계층에서는 모든 컴퓨터가 이해할 수 있도록 데이터를 변환하는 역할을 함
- 또 암호화를 통해 보안성을 높이고, 데이터 압축 기능으로 데이터가 효율적으로 전송될 수 있도록 함

응용 [Application]

- 응용 계층은 OSI의 최상위 계층으로서 주로 서비스를 나타냄
- 응용 계층의 예시로는 FTP, SMTP, SNMP, HTTP 등등이 있습니다. 즉 응용 계층은 사용자가 사용하는 UI와 비슷하다고 할 수 있음

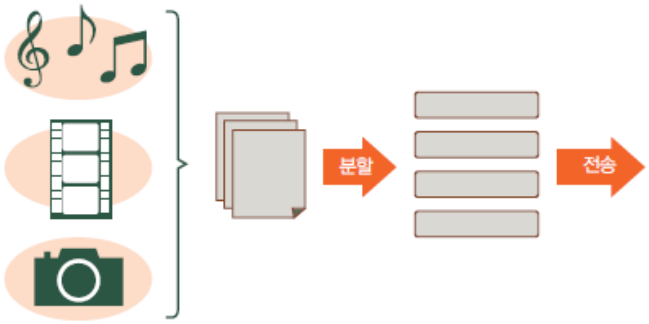
웹 브라우저에서 웹 서버에 요청 보내는 경우



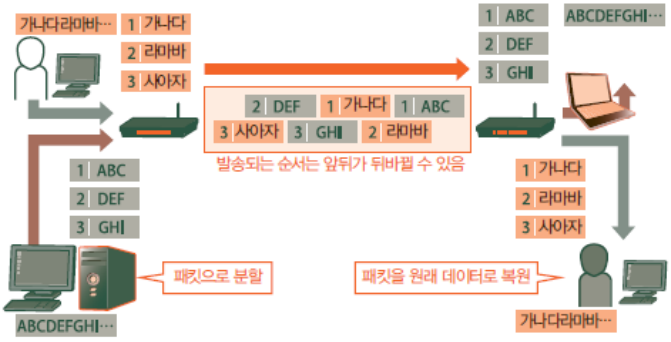
- 웹 브라우저에서 웹 서버로 보낼 데이터를 OS가 관리하는 TCP에 전달
- TCP에서는 전달받은 데이터를 일정한 사이즈로 분할한 'TCP 세그먼트' 작성. 작성한 TCP 세그먼트의 헤더에 상대방 웹 서버의 포트번호 적어서 IP에 전달
- IP에서는 통신 상대 나타내는 IP 주소를 새로운 헤더에 붙인 'IP 패킷' 만들어 이더넷으로 보냄
- 이더넷에서는 IP주소에 지정된 최종 상대와의 통신 경로상에 있는 네트워크 기기들 중 바로 다음으로 패킷 전달해야 할 기기의 MAC 주소를 헤더에 기입한 '이더넷 프레임' 송출
- 네트워크로 송출된 이더넷 프레임이 헤더에 적힌 다음 기기로 전달되면, 그 기기에서는 다음 상대의 MAC 주소를 헤더에 고쳐 적어 다시 송출. 이를 반복하여 이더넷 프레임은 최종 통신 상대의 서버에 도착.
- 서버에서는 이더넷 프레임에서 IP 패킷, TCP 세그먼트의 순서로 헤더를 벗겨내어 마지막으로 원래 애플리케이션이 보낸 데이터를 복원. 이 데이터가 TCP 세그먼트의 헤더에 기술된 수신 포트 번호의 애플리케이션으로 건네짐.

패킷 교환(패킷 통신)의 원리

- 데이터를 일정한 길이의 블록으로 분할하여 각각마다 수신자 정보를 부여
- 이를 '패킷' 형태로 만들어 발송



- 하나의 회선 안에 여러 이용자의 패키지를 주고받으며, 통신회선을 놀리지 않고 작동하기 때문에 네트워크 이용 효율이 높음
- 그림이나 음성 등 서로 다른 종류의 데이터를 같은 네트워크 안에서 보낼 수 있음
- 네트워크를 통해 원래 데이터를



– 회선이 패킷으로 붐비면 도착할 때까지 시간 걸리거나 패킷 분실될 수 있음

TCP와 UDP의 차이점

- TCP (Transmission Control Protocol)
  - 패킷의 순서를 맞추거나 도착하지 않은 패킷이 있으면 재발송 요구하는 등 제어 담당
- UDP (User Datagram Protocol)
  - '포트 번호로 프로그램 식별하기'라는 간단한 제어만을 수행
  - TCP어

	TCP	UDP
특징	• 발송 전에 커넥션을 확립 • 통신 상대마다 접속을 관리	• 커넥션을 확립할 필요 없음 • 바로 즉시 데이터 발송
장점	• 재발송, 도착순서 등을 제어할 수 있음 • 신뢰성이 높음	• 헤더 사이즈가 작음 • 부하가 작음
단점	• 헤더 사이즈가 큼 • 부하가 큼	• 패킷을 분실해도 재발송하지 않음 • 신뢰성이 떨어짐

MAC(media access control) 주소

- 네트워크 기기를 유일하게 식별할 수 있도록 할당된 물리 주소
- 48비트 정숫값으로, 앞부분 24비트는 제조사 식별번호, 뒷부분 24비트는 각 장치마다 중복되지 않도록 제조사가 할당한 번호로 되어 있음
  - (예) 12:34:56:78:9a:bc or 12-34-56-78-9a-bc