-컴퓨터 네트워크-

Layer 4 : Transport Layer

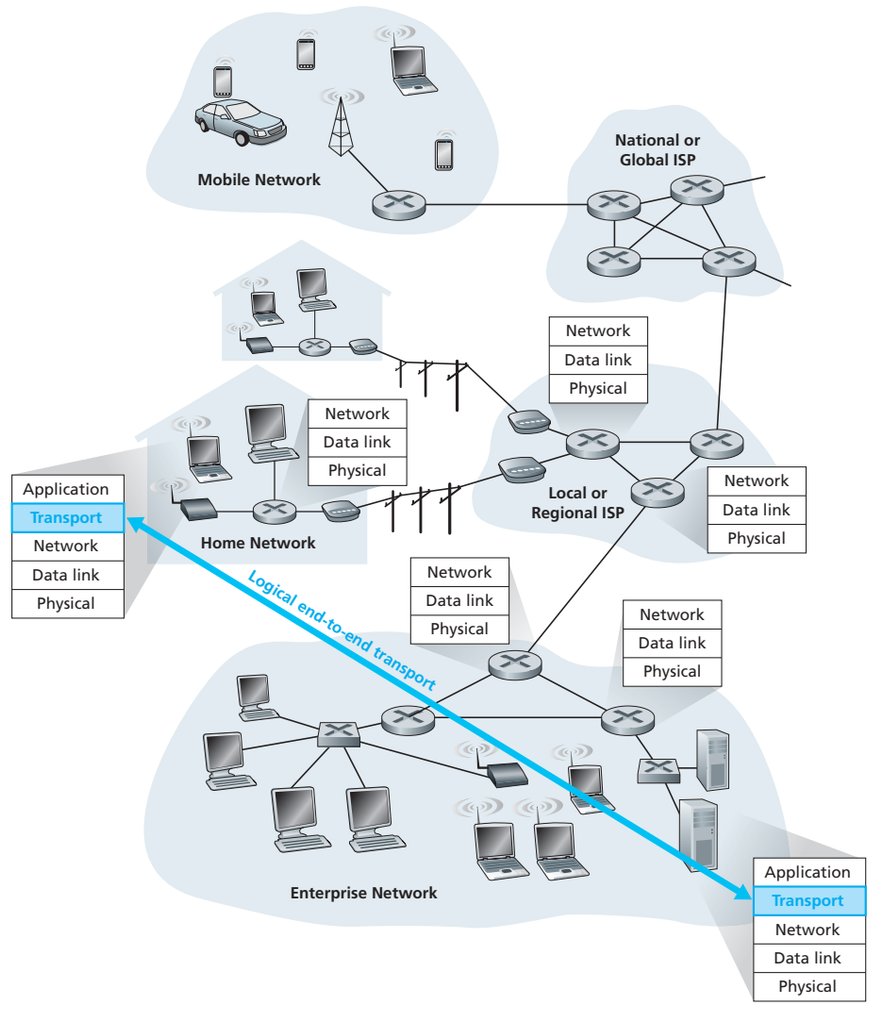
2022 Spring
Kyungseop Shin

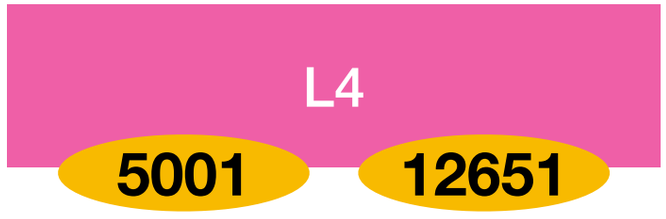
Course Outline

- Layer 4 Transport Protocol에 대해 이해
  - Transmission Control Protocol (TCP)에 대해 이해
  - User Datagram Protocol(UDP)에 대해 이해
- IP datagram 전달에 대한 다양한 제어 프로토콜에 대해 이해
  - Firewall
  - Network Address Translation (NAT)
  - Dynamic Host Configuration Protocol (DHCP)

Layer 4 Overview

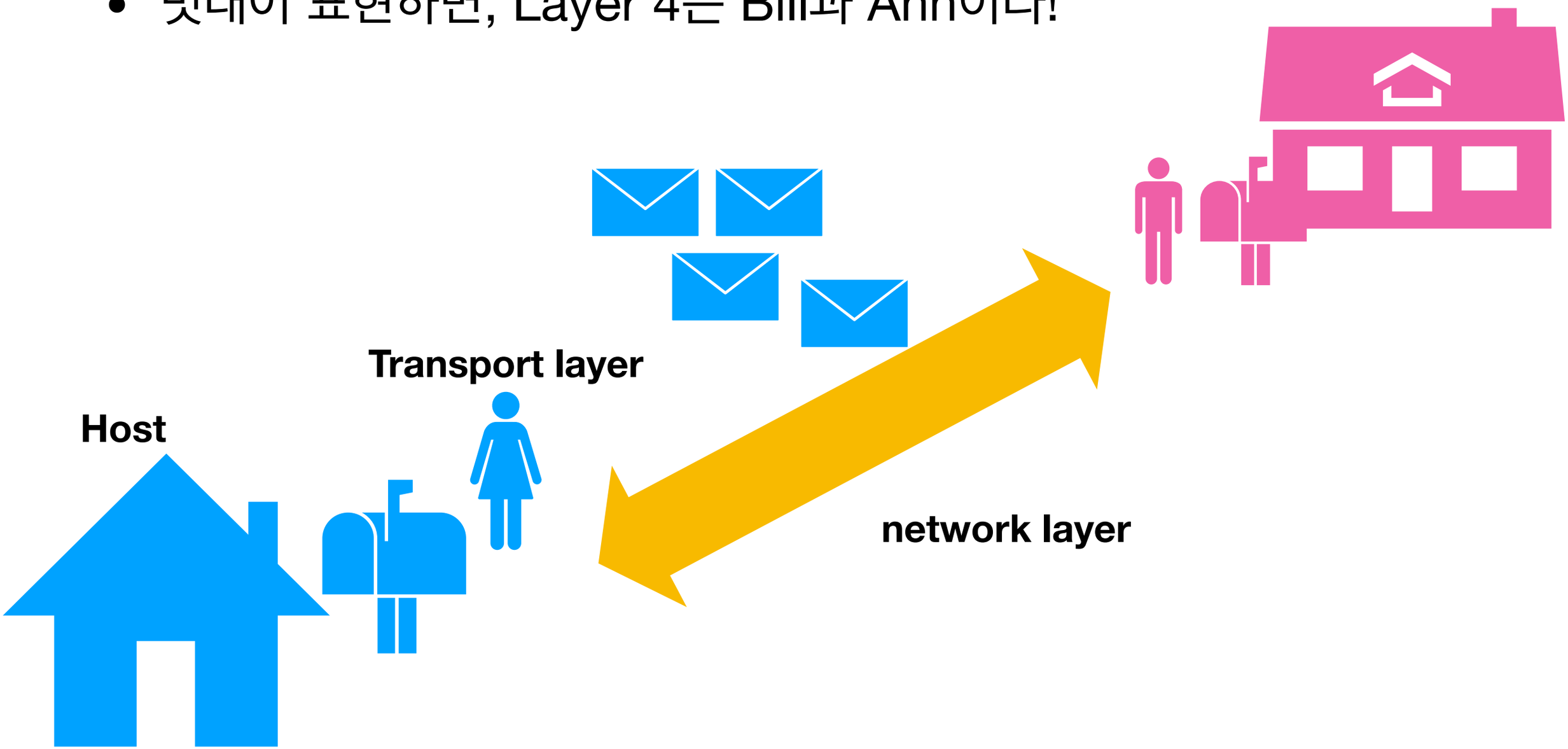
- End-to-end data 전송을 위한 logical communication 역할
  - Connection-oriented vs. connectionless
  - IP 및 Port 번호로 식별





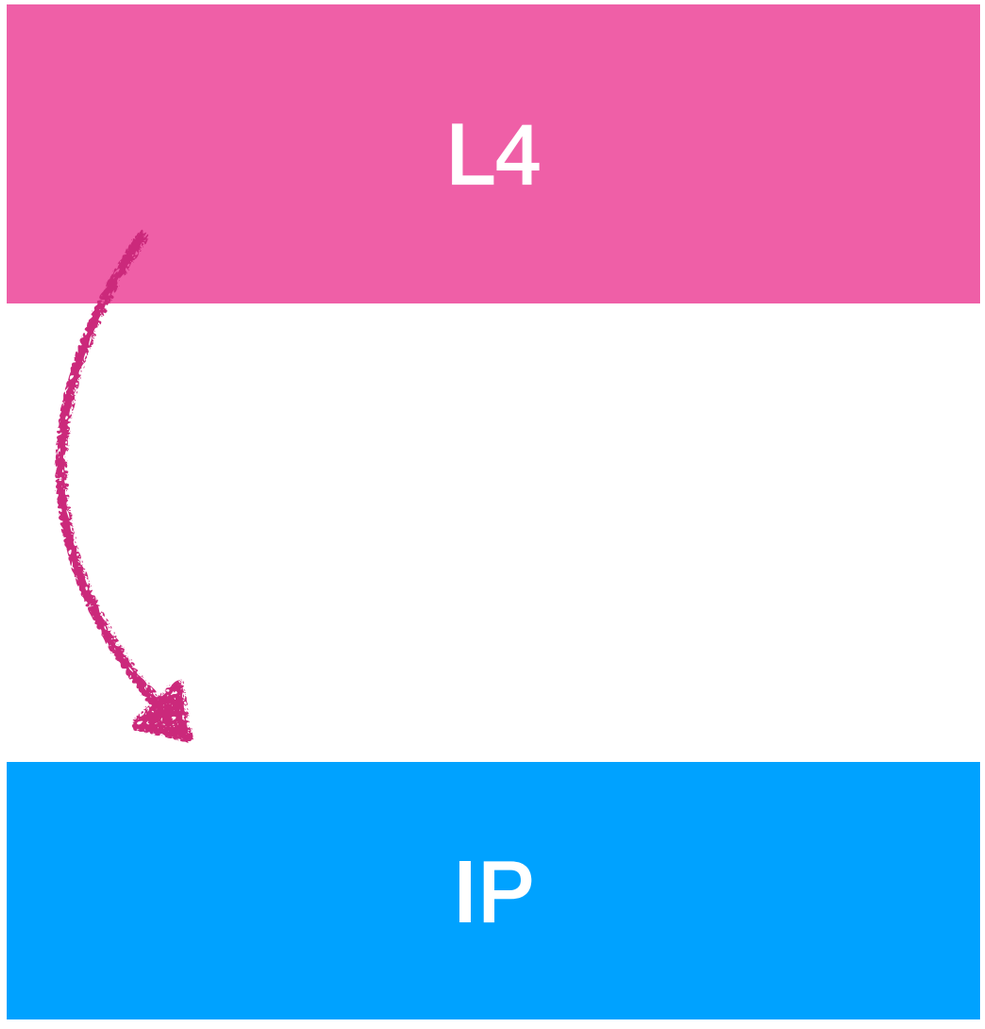
Layer 4 Overview

- 빗대어 표현하면, Layer 4는 Bill과 Ann이다!



Layer 4 Overview

- IP 계층에 대한 다양한 제어
  - 동적 IP 주소 관리
  - IP 변환
  - IP packet 흐름 제어

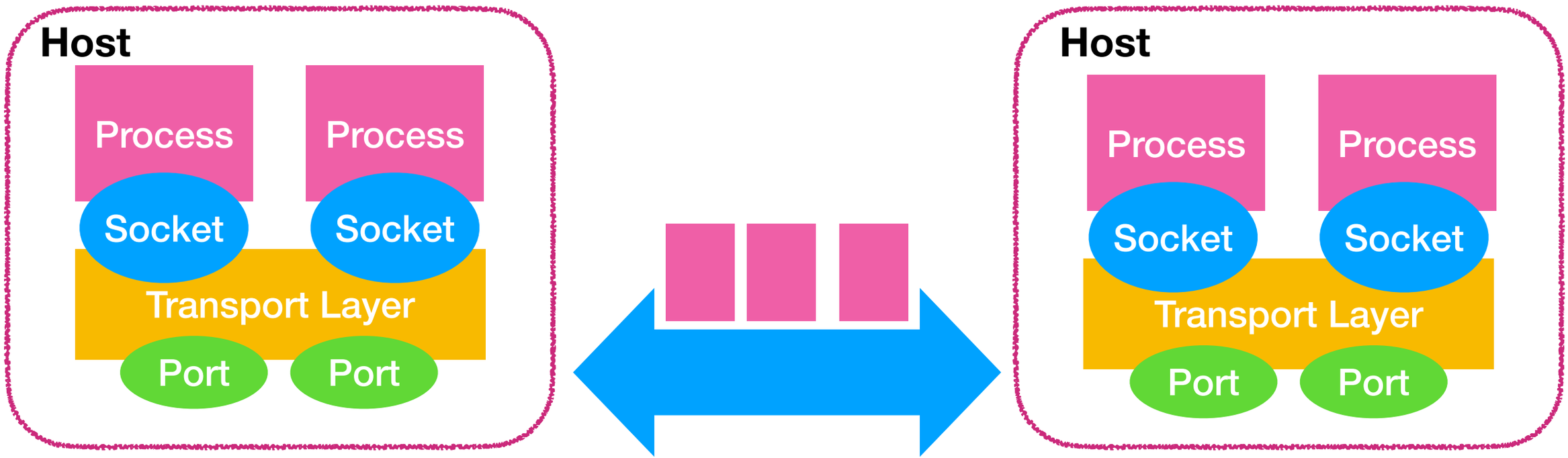


Transport Layer 종류

- Application에 따라 다음 두 프로토콜 중 한가지를 사용
    - User Datagram Protocol (UDP) : unreliable, connectionless service, transparent
    - Transmission Control Protocol (TCP) : reliable, connection-oriented service, congestion control
- 두가지 모두 IP 상위 계층 위치에서 end-to-end로 segment를 전달하는 역할을 가짐
    - Best-effort and unreliable delivery service (IP) 상에서
    - Application process에게 적절하게 packet 전달 (Socket to socket)

Transport-Layer Multiplexing

- 한 host 내 다양한 process로부터의 data 전달 역할
  - Multiplexing : 여러 socket을 통해서 SDU를 받아 전송
  - Demultiplexing : 수신된 PDU를 적절한 socket으로 전달
- Socket : process - transport layer 간 SAP
  - Transport layer에서는 Port 번호로 식별



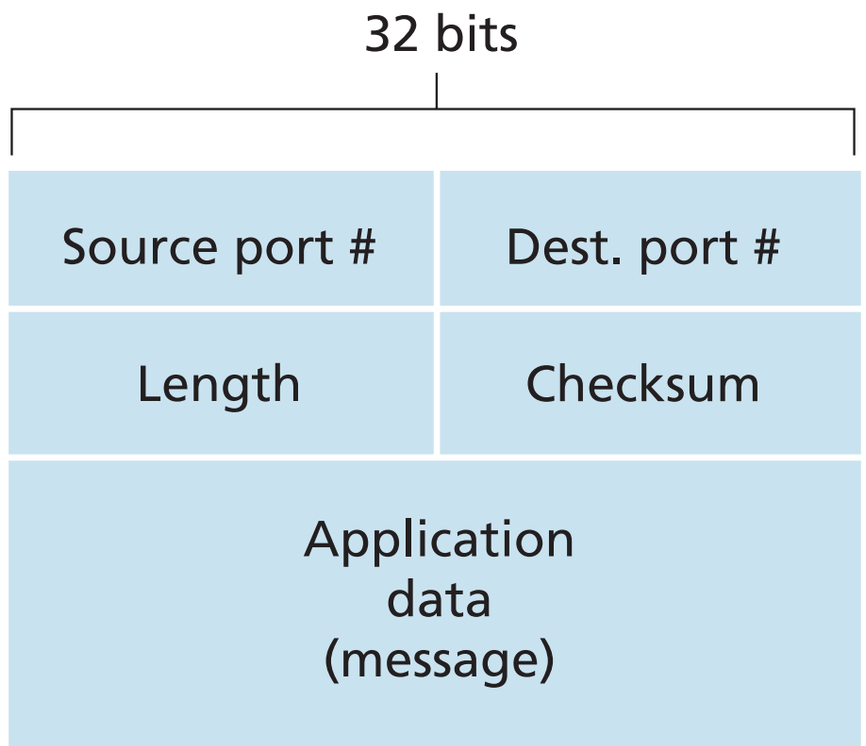
Port number

- Transport-layer에서의 식별자 역할
  - socket에 대한 식별
  - 보통 source/destination 별로 port번호 존재
- Well-known port number

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL

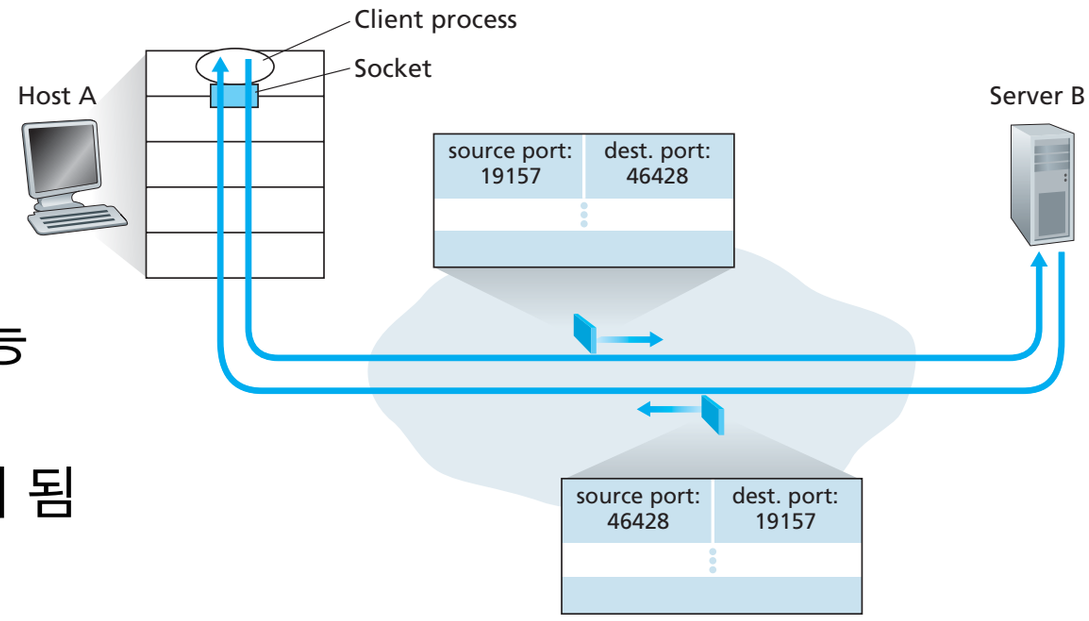
User Datagram Protocol (UDP)

- 간단한 multiplexing/demultiplexing 기능의 프로토콜
  - Port 번호와 checksum만 header로 붙음
  - 사실상 IP의 기능만 하며, application 계층에서 flow control 등 기타 기능을 구현
- Segment 전송 방식도 심플함
  - 연결 과정 없이 바로 전송 가능



User Datagram Protocol (UDP)

- UDP socket의 생성
  - Application process에서 socket 생성 즉시 transport layer에서 port 번호가 부여됨
- UDP segment 송수신
  - Two tuple : destination IP & port number
  - 상대방 host의 port가 열려있으면 항상 전송 가능
    - IP, port 번호를 지정해서 보내면 바로 전달이 됨
- Source port ?
  - Return address개념



User Datagram Protocol (UDP)

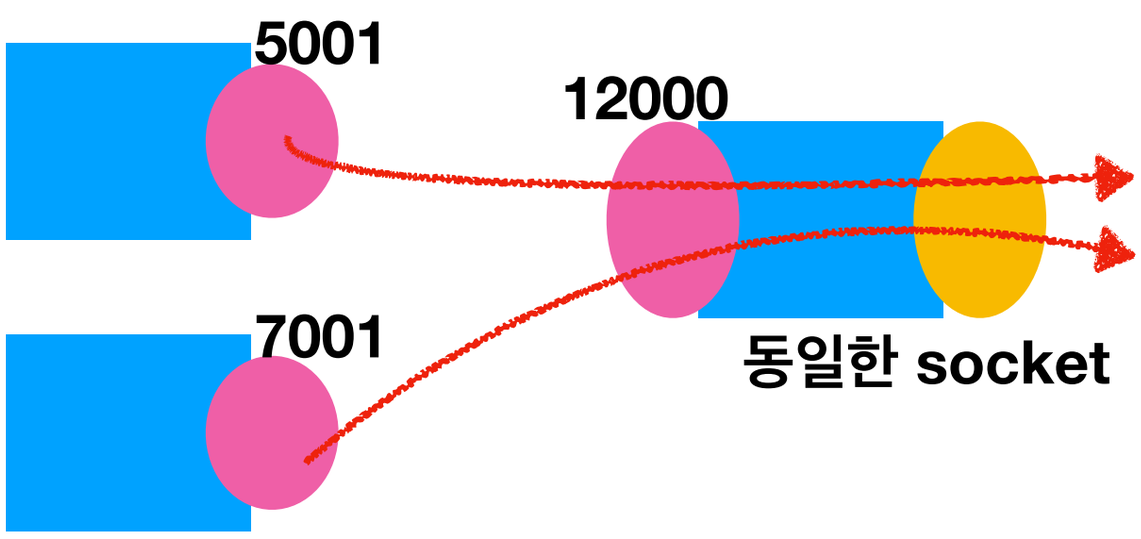
- UDP의 장점
  - application-level에서의 data 전송 제어가 손쉬움
  - Connection establishment 과정이 불필요함
  - Connection state에 대한 관리 및 관련 동작 제한이 없음
  - Packet header overhead가 적음

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Routing protocol	RIP	Typically UDP
Name translation	DNS	Typically UDP

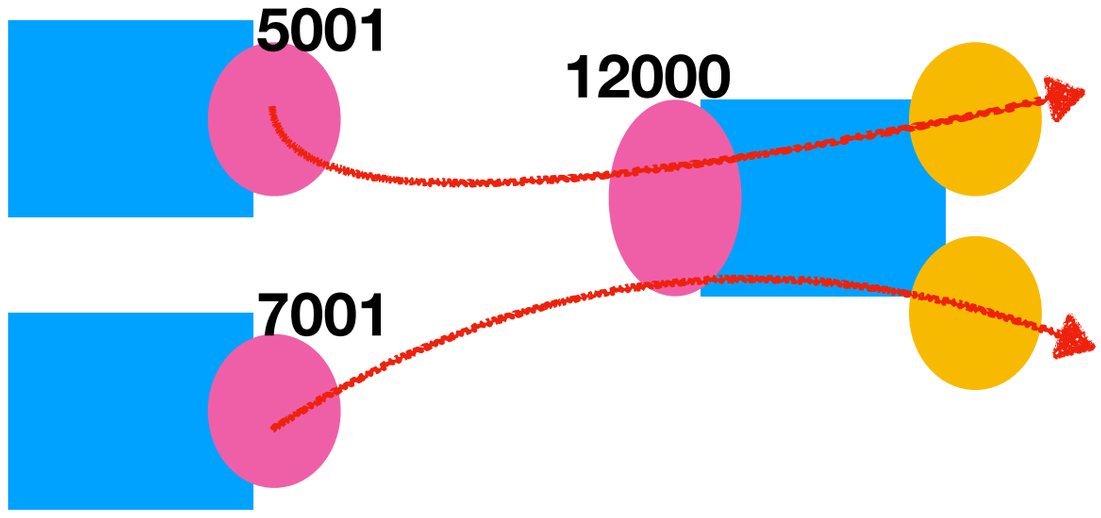
Transmission Control Protocol (TCP)

- Connection-oriented : connection establishment 과정 존재
  - connection이 존재해야 segment 전달이 가능
  - Four tuple : source IP/port number, destination IP/port number
  - source에 대한 정보까지 대조하여 socket에 mapping

UDP

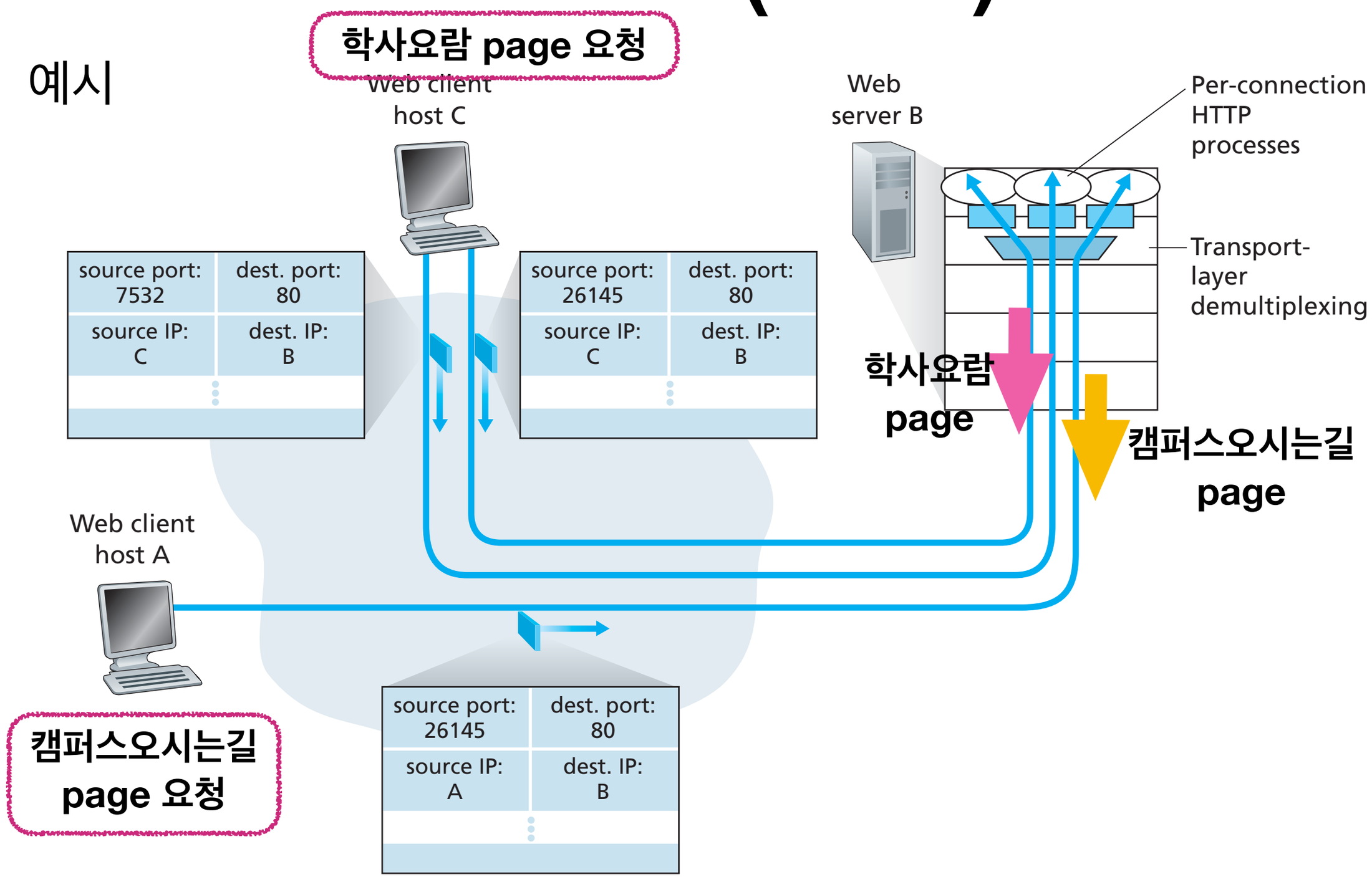


TCP 서로 다른 **socket**



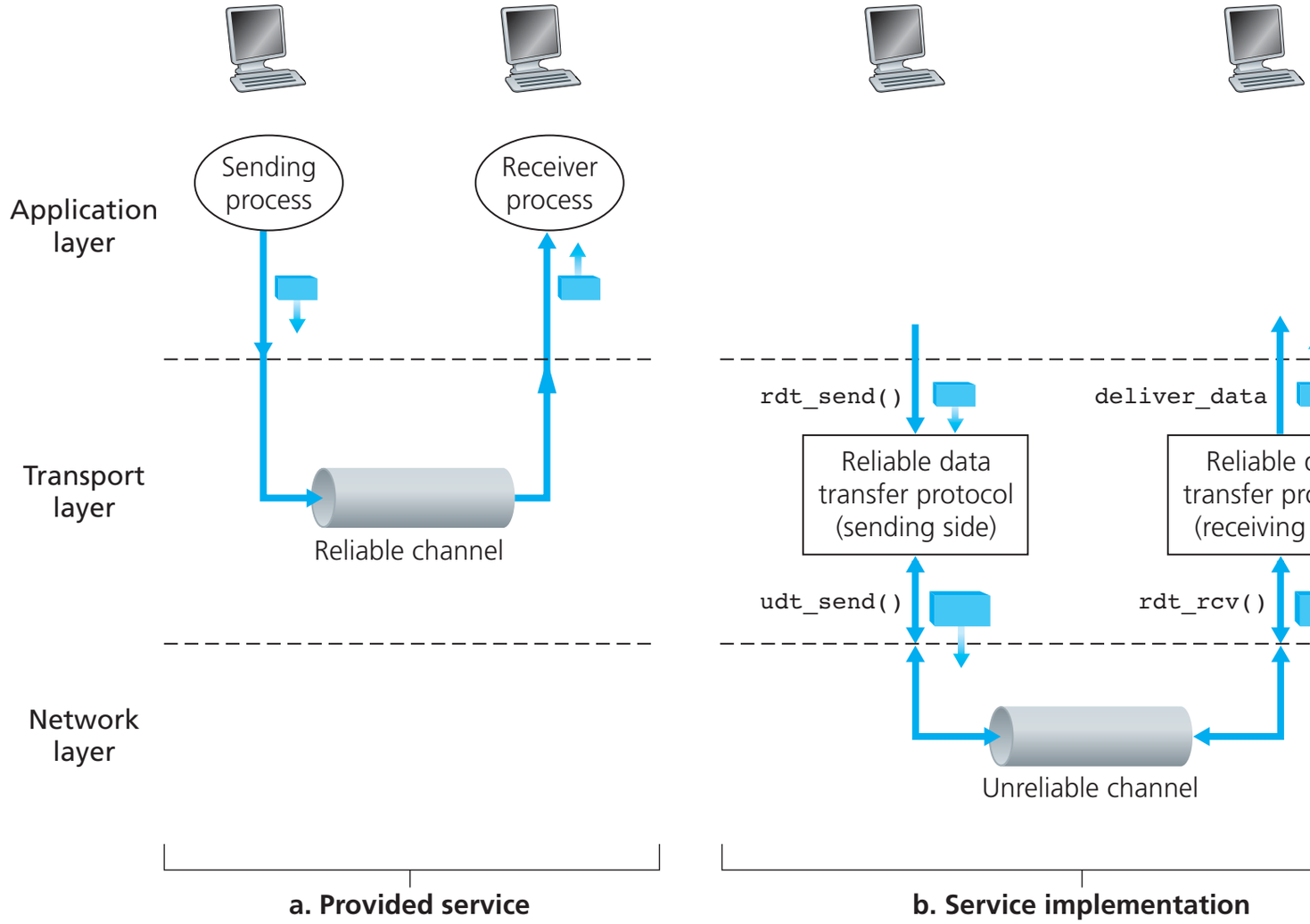
Transmission Control Protocol (TCP)

- 예시



Transmission Control Protocol (TCP)

- TCP는 reliable data transfer를 지원
  - 즉, 재전송 및 ARQ 기능을 포함

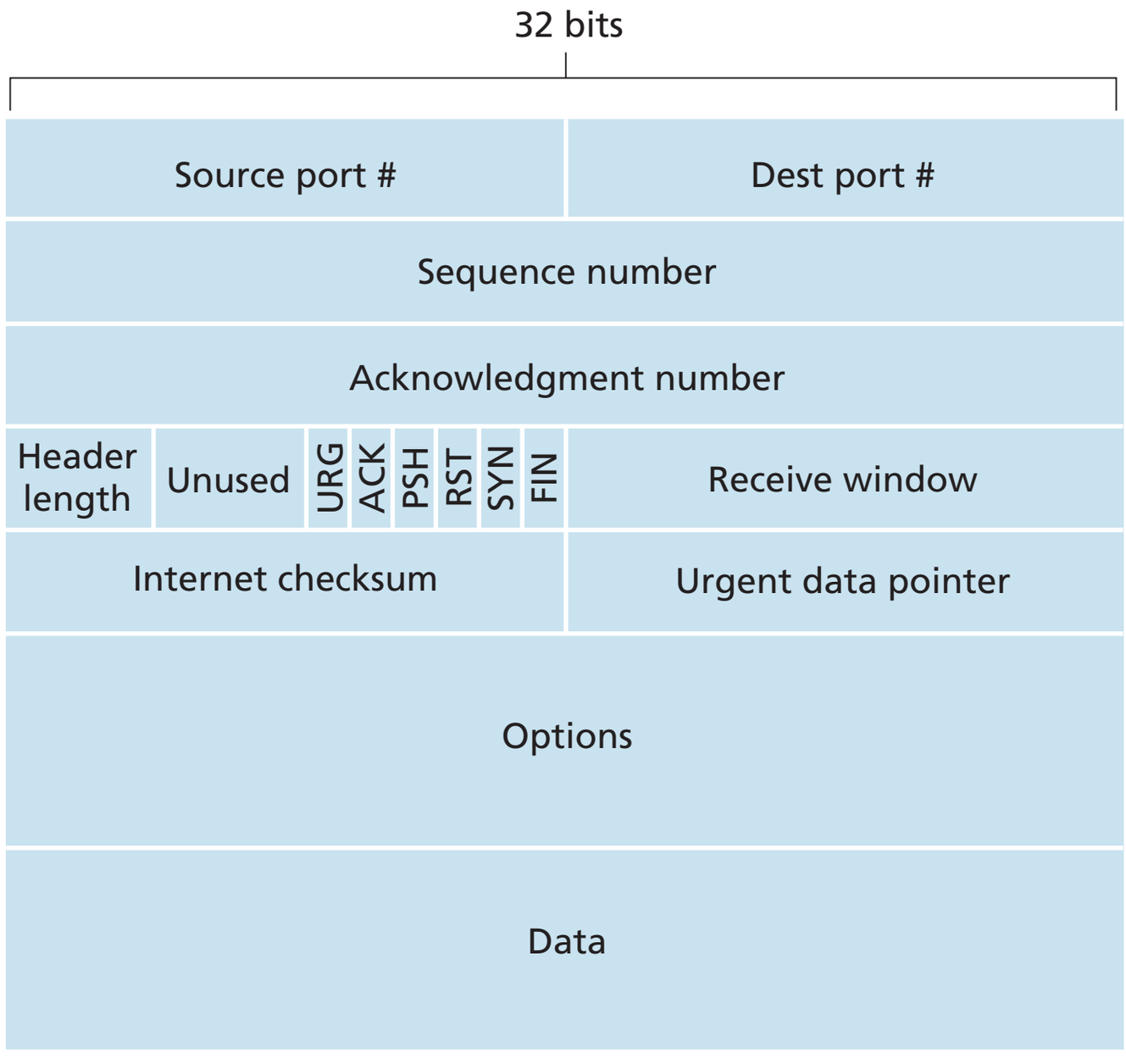


Transmission Control Protocol (TCP)

- Connection establishment : process간 three way handshake를 통해 수행
    - 특정 port로 connection establishment 메시지를 수신하고 나서 socket과 port번호가 연동됨
        - Point-to-point : single sender/receiver 간 연결됨
- client process에서 initiation을 함
    - Server process에서는 IP address/port에 대해 연결 승인
- 목적 : 상대방의 존재 알림, optional parameter 결정, transport entity resource 할당

Transmission Control Protocol (TCP)

- Segment format
  - Sequence no. : Byte 시작점
  - ACK no. : 다음번 수신을 해야 할 Byte offset



Transmission Control Protocol (TCP)

- Retransmission과 함께 flow control 수행

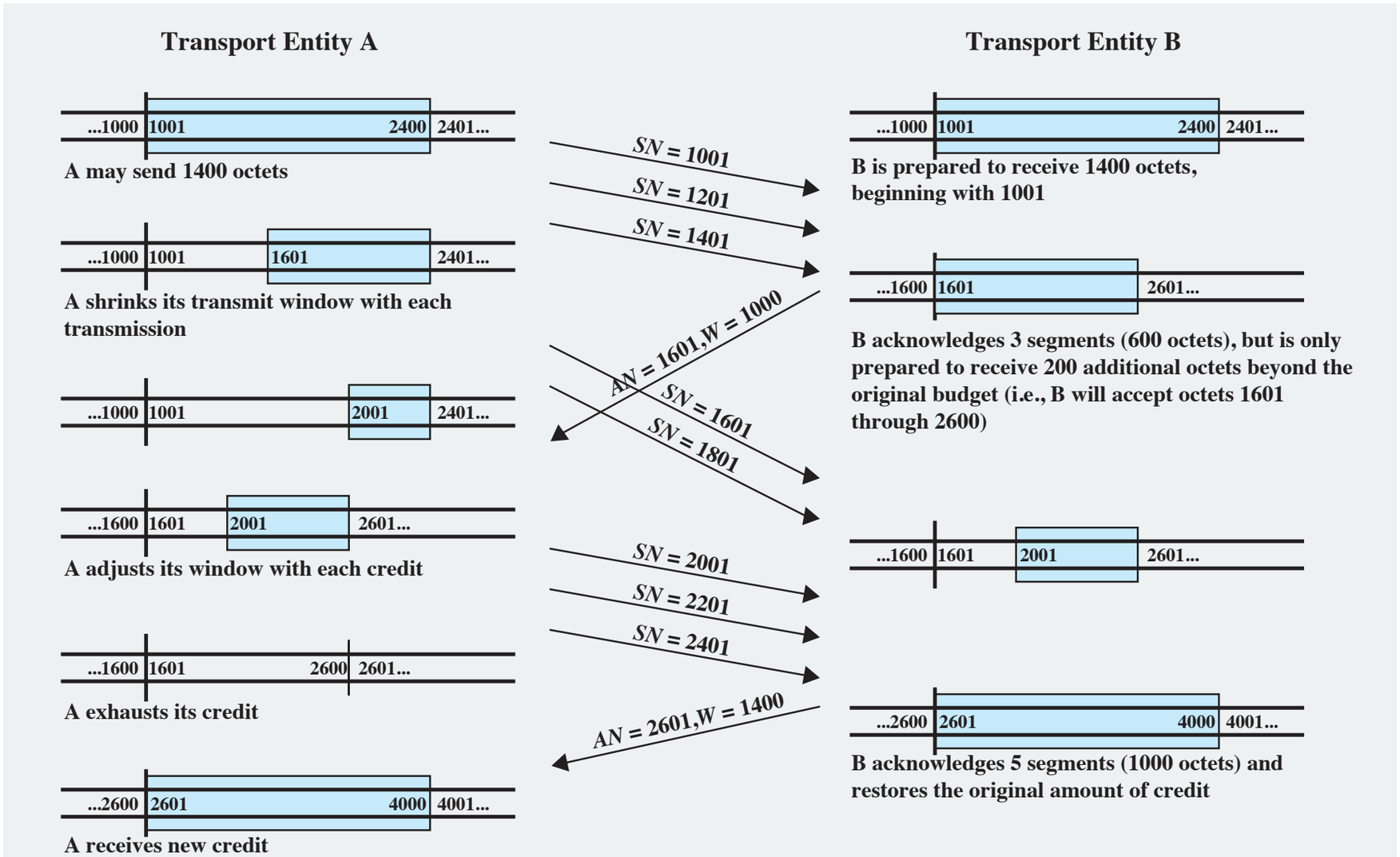


Figure 15.1 Example of TCP Credit Allocation Mechanism

Congestion Control

- UDP와 다르게 TCP는 congestion control을 수행
  - Network의 혼잡을 방지하기 위해 자체적으로 flow control 수행
    - 일시적 delay가 커질 수 있으나 network 전체 관점에서 이득
- Window management : 일반적으로 window가 크면 congestion을 유발할 가능성이 크므로 아래와 같은 규칙하에 관리
  - slow start
  - dynamic window sizing

Congestion Control

- Slot start & Dynamic window sizing
    - 정상적으로 전송-feedback으로 주고 받는 상황에서 서서히 window 크기를 확장
    - congestion 상황에서 임의로 window size를 줄임

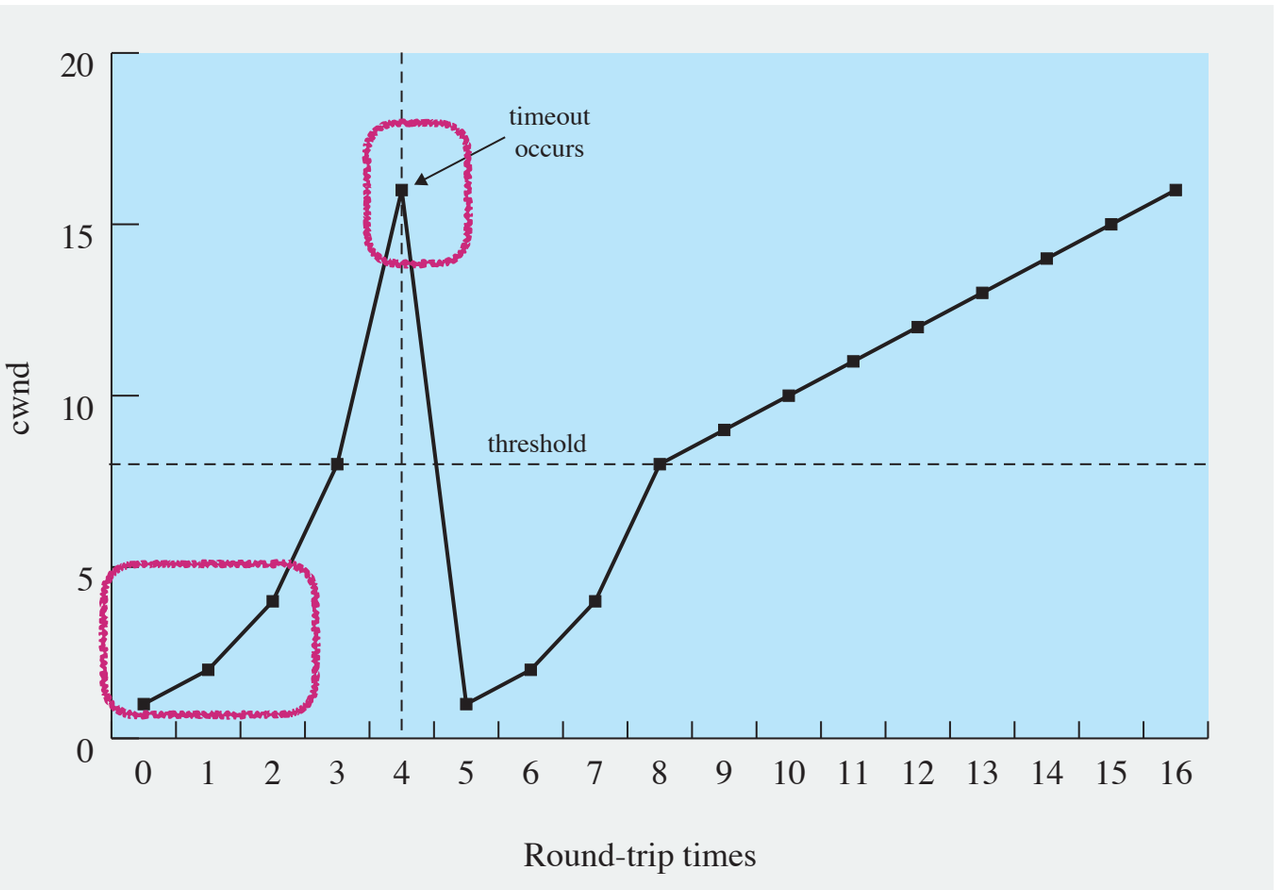


Figure 20.10 Illustration of Slow Start and Congestion Avoidance

Dynamic Host Configuration Protocol (DHCP)

- 특정 host에 대해 IP를 동적으로 할당하기 위한 프로토콜 (RFC2131)
    - 가능한 IP address pool 내에서 선택해서 요청 host에게 할당
        - 사용되지 않는 IP는 자동으로 회수
- 원래는 IP address 수가 부족한 상황을 보완하기 위한 목적으로 만들어짐
- 최근에는 WiFi나 subnet 내 불특정 다수의 host에 대한 IP address를 편리하게 부여하기 위한 용도로 사용됨

Dynamic Host Configuration Protocol (DHCP)

- 서비스 시나리오
  - 특정 host가 새로 등장
  - DHCP server로 IP 주소 요청
  - IP 주소를 할당하는 responce msg 수신

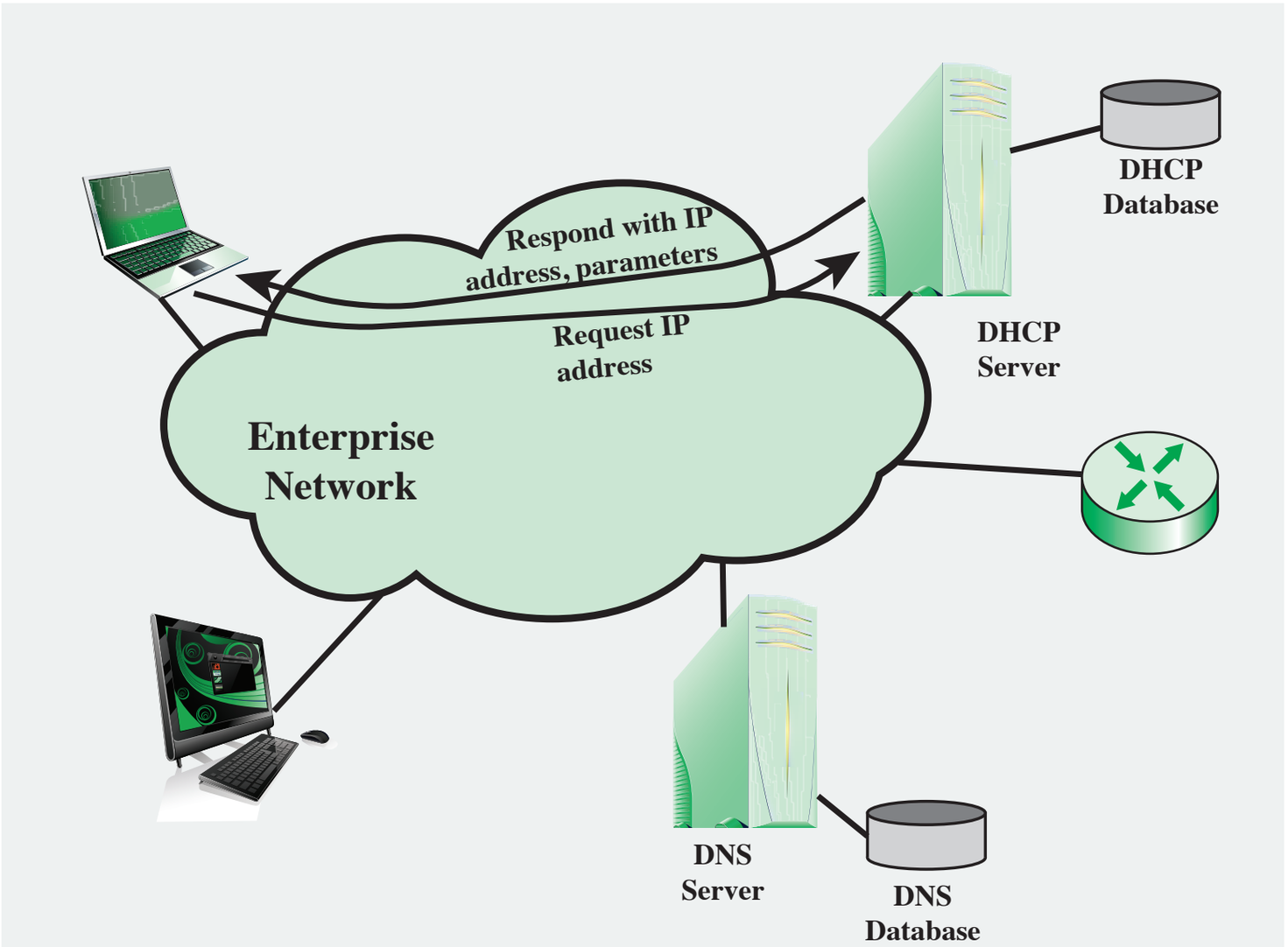


Figure 21.14 DHCP Role

Dynamic Host Configuration Protocol (DHCP)

- DHCP messages

DHCPDISCOVER
- Client broadcast to locate available servers

DHCPOFFER
- Server to client in response to DHCPDISCOVER with offer of configuration parameters

DHCPREQUEST
- Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, for example, system reboot, or (c) extending the lease on a particular network address

DHCPACK
- Server to client with configuration parameters, including committed network address

DHCPNACK
- Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease has expired

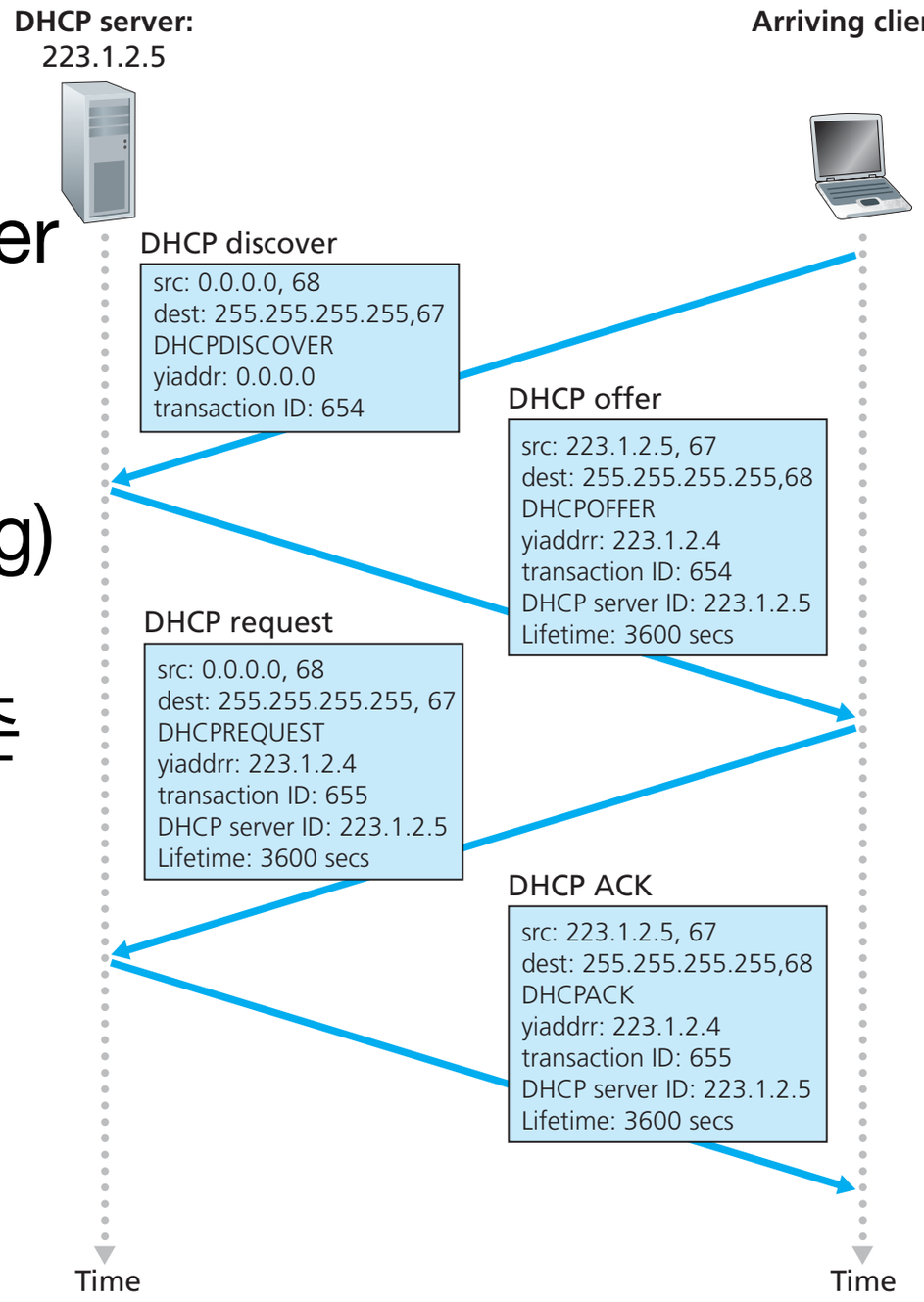
DHCPDECLINE
- Client to server indicating network address is already in use. DHCP server should then notify sysadmin

DHCPRELEASE
- Client to server relinquishing network address and canceling remaining lease

DHCPINFORM
- Client to server, asking only for local configuration parameters client already has externally configured network address

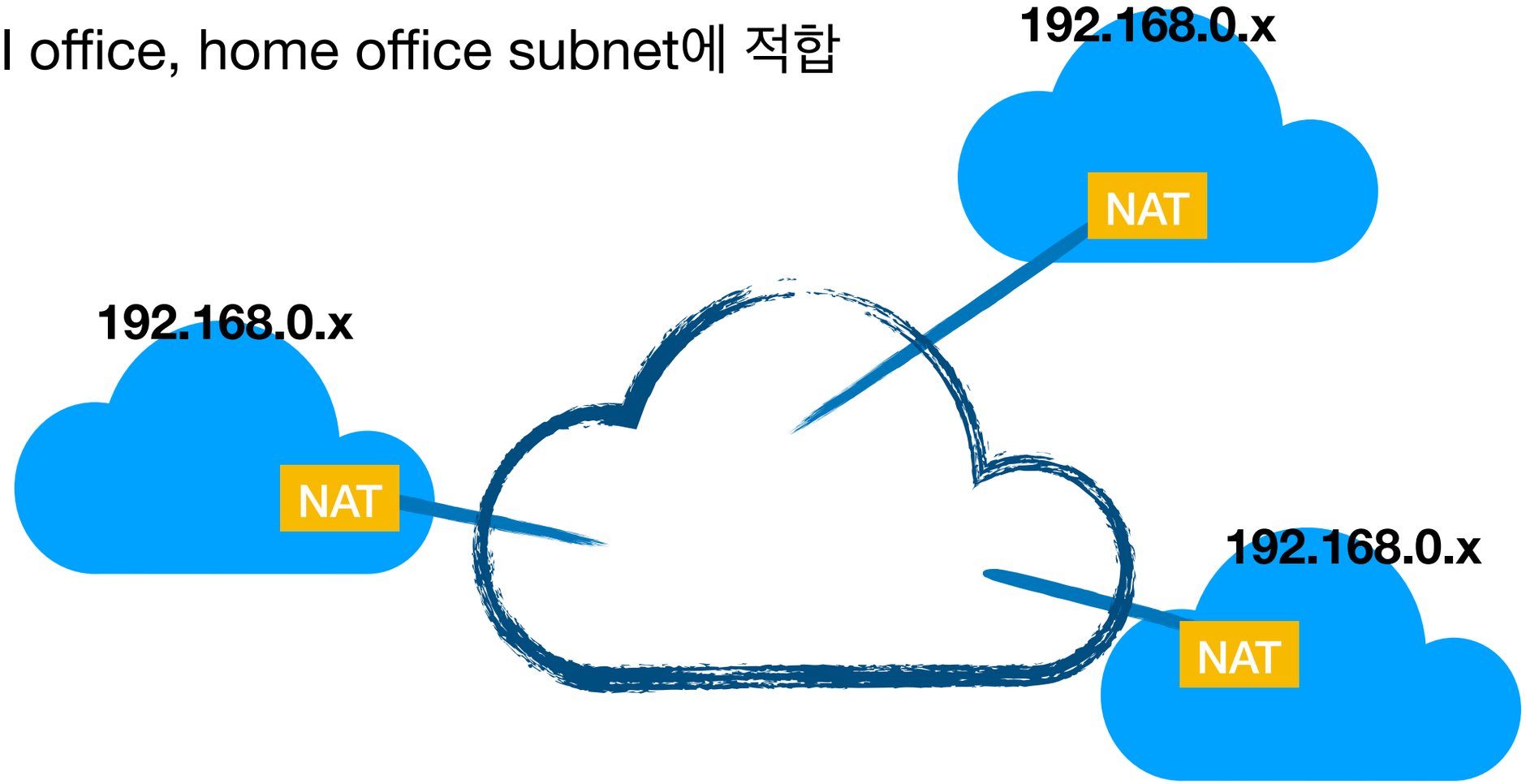
Dynamic Host Configuration Protocol (DHCP)

- 4 step scenario
  - DHCP server discovery : DHCP server 를 찾는 메시지 (UDP port 67)
    - IP : 255.255.255.255 (broadcasting)
  - DHCP server offer : server가 자신의 존재를 알림 (broadcasting)
  - DHCP request - DHCP ACK



Network Address Translation (NAT)

- IPv4를 오늘날까지 생존하게 한 프로토콜
  - 절대적으로 수가 부족한 IP address를 국지적으로 사용할 수 있게 해줌
  - Small office, home office subnet에 적합

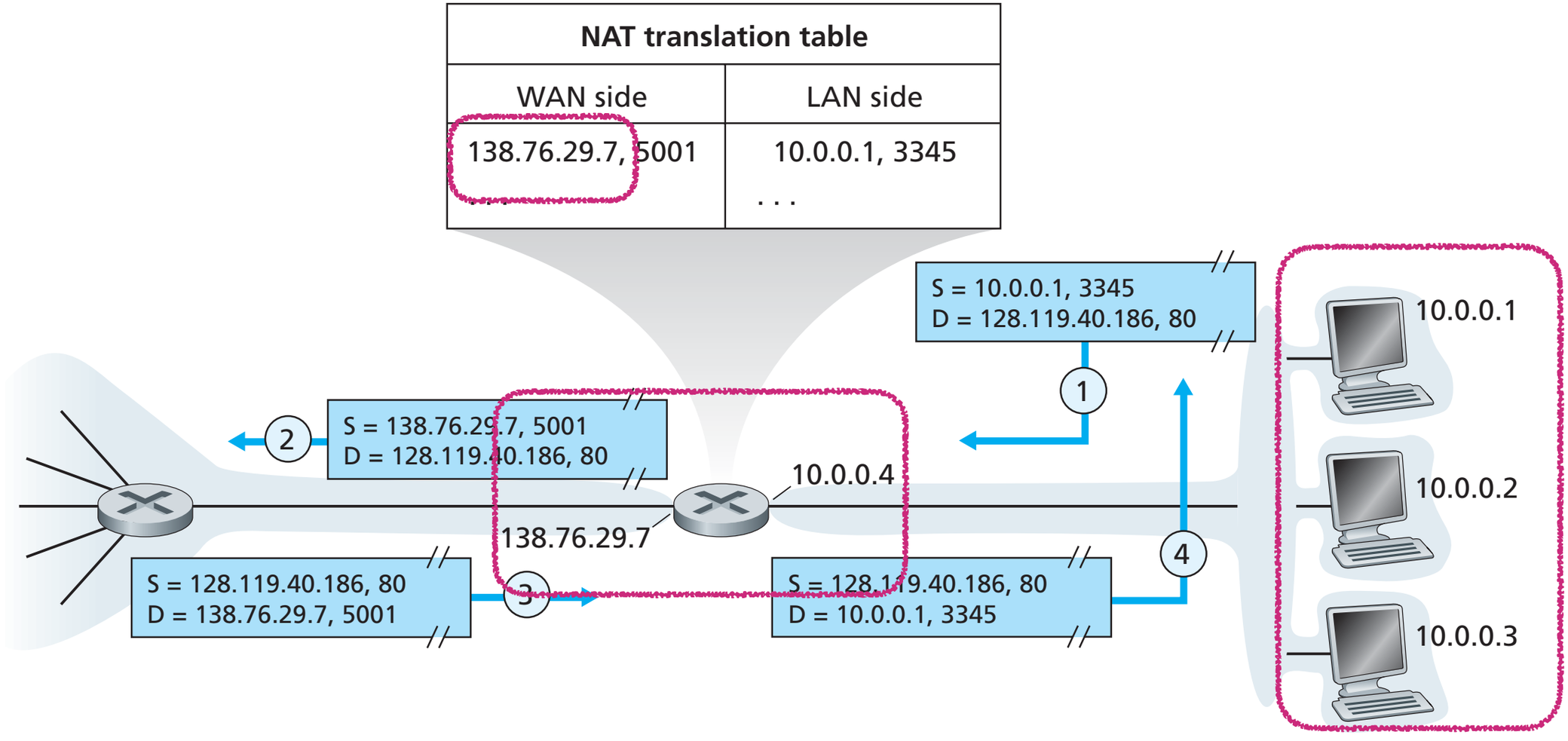


Network Address Translation (NAT)

- Small Office Home Office (SOHO)
  - 초기에는 ISP로부터 일정 IP 대역을 할당 받음
  - 이 subnet이 점점 커지면서 IP 대역을 더 많이 요구하게 되면 연속된 IP를 못받을 수 있음
- Network Address Translation
  - 하나의 IP로 할당 받아 내부의 subnet의 여러 host들에게 공통으로 서비스를 하는 방식
  - 내부적으로 IP를 따로 주면서 외부로 나갈 때 할당된 하나의 IP를 사용

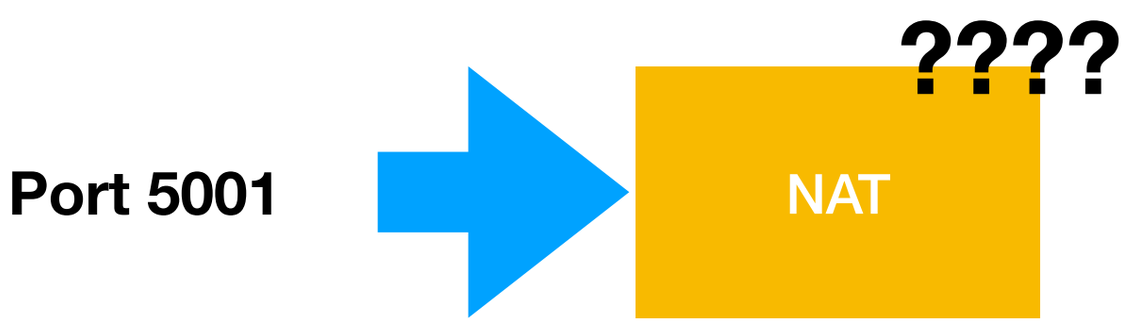
Network Address Translation (NAT)

- Out-going IP + port 번호와 내부 IP/port로 mapping
  - NAT translation table을 통해 outer->internal routing을 수행
  - 초기 Outgoing packet에 대해 translation table 항목을 생성하고 port번호 부여



Network Address Translation (NAT)

- NAT의 역할
    - 외부 IP 하나를 통해 여러 host들이 손쉽게 networking할 수 있음
        - 부족한 IP address 수에 대한 강력한 보완책이 됨
    - Internal network내 host를 감추는 역할
        - 외부에서는 어떤 host든 single IP로 밖에 보이지 않음
- 한계점
    - In-going packet으로 연결이 시작되는 서비스가 불가능



Network Address Translation (NAT)의 Issue

- Port 번호의 용도가 잘못됨
    - host를 지칭하는 것이 아닌, service를 지칭해야 함
- Layered architecture concept에 어긋남
    - IP header에 대한 관리는 L3에서만 해야 함
- IP header에 대한 생성/조작은 End-to-end 단계에서만 다루어져야함
- IPv4의 다음 기술인 IPv6이 널리 퍼지는 것을 제대로 막음
    - Networking 기술이 다음 세대로 가지 못하고 있음

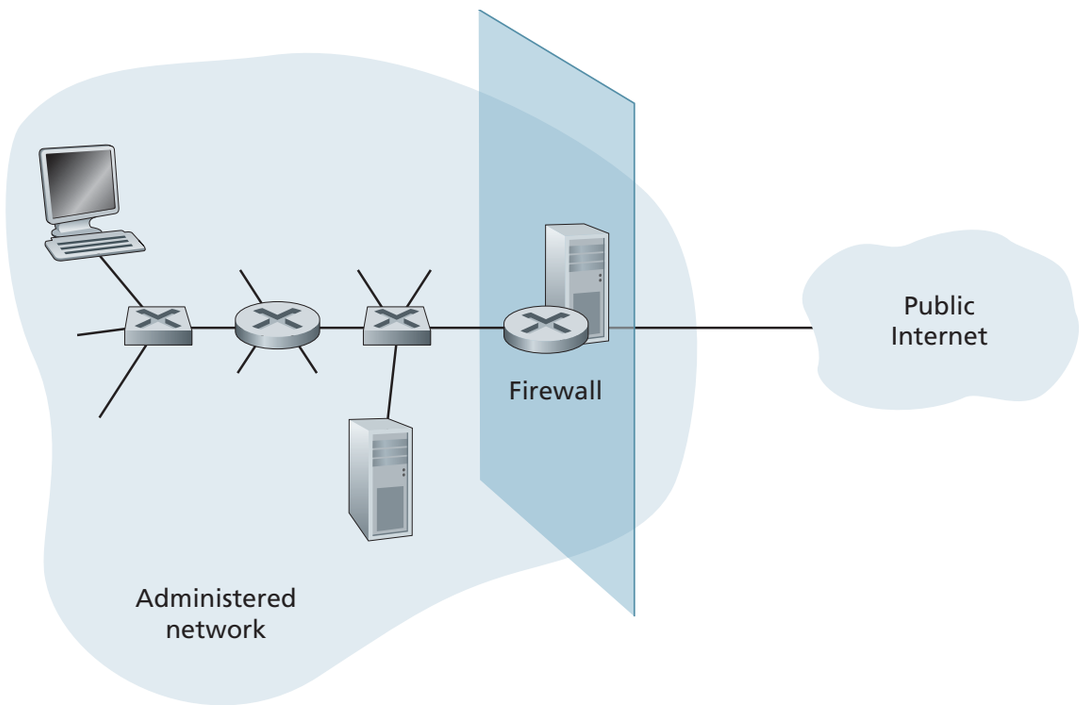
Universal Plug and Play (UPnP)

- P2P file-sharing 혹은 VoIP와 같이 외부에서 접속이 필요한 서비스를 NAT 환경에서 지원하기 위한 프로토콜

- Host가 주변 NAT와 사전 configuration 진행
  - Private IP/port와 public IP/port를 미리 지정
  - Outside node에서 해당 IP/port로 internal host에 접속 가능

Firewall

- internal network와 internet의 경계를 짓는 존재
  - Allowing some packets to pass and blocking others
  - Internal network - internet 간 대문(gateway) 역할
- Network security 측면에서의 주요 역할
  - Network 관리자가 외부 접속에 대한 관리를 가능하게 해줌



Firewall

- Three goals
  - 모든 양방향의 traffic이 firewall을 통해서 지나가도록 함
    - 외부 internet과 관리 대상인 내부 망의 boundary 역할
  - Local security policy에 의해 규정된 허용 트래픽만 통과시킴
    - 유입/유출되는 traffic에 대해 관리자가 지정한 정책에 따라 흐름을 제어
  - Firewall 자신은 보안에 매우 강해야 함
    - firewall이 공격당하기 쉬우면 차라리 없는 게 더 좋음

Categories of Firewalls : Traditional Packet Filters

- Traditional packet filters

  - Administrator-specific rule에 따라 gateway router에서 packet의 통과를 허용하거나 drop을 수행

    - IP source or destination address
    - Protocol type in IP datagram field: TCP, UDP, ICMP, OSPF, and so on
    - TCP or UDP source and destination port
    - TCP flag bits: SYN, ACK, and so on
    - ICMP message type
    - Different rules for datagrams leaving and entering the network
    - Different rules for the different router interfaces

Categories of Firewalls : Traditional Packet Filters

- 보안적인 측면과 더불어 Internal network의 용도 및 관리자의 의도에 맞게 적절히 filter를 수동으로 설정
    - IP와 port 번호를 조합해서 규칙 생성 가능

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Categories of Firewalls : Traditional Packet Filters

- 실제 firewall rule은 access control list를 설정해서 구현

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	—
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	—
deny	all	all	all	all	all	all

HTTP

DNS

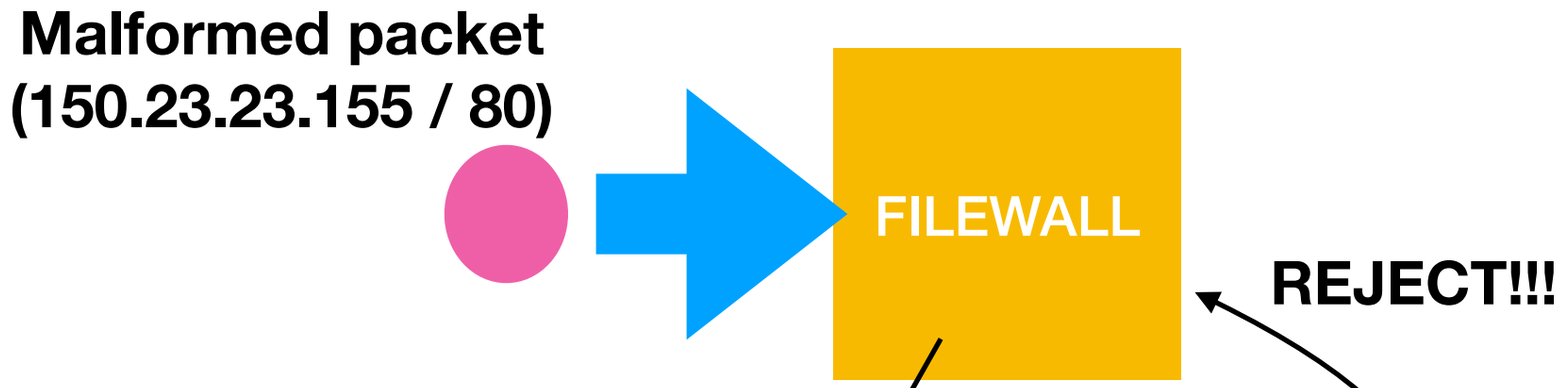
Categories of Firewalls : Stateful Packet Filter

- Stateful packet filter
  - connection 별로 filtering 규칙 적용
    - 각 packet에 대해 별도로 filtering 규칙을 적용하는 Traditional packet filter와는 다름
  - connection의 handshake 절차 등을 추적하면서 filtering을 할 수 있음

source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Categories of Firewalls : Stateful Packet Filter

- Check connection : 해당 연결에 대해 connection list까지 검토해야 함을 표시



action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	>1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	>1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	>1023	53	—	
allow	outside of 222.22/16	222.22/16	UDP	53	>1023	—	X
deny	all	all	all	all	all	all	

source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Connection table

Categories of Firewalls : Application Gateway

- Filtering이 packet 기반(IP, port number 등)이 아닌 application 수준의 상황에 따라 이루어져야 할 때가 있음
  - e.g.) 특정 internal user에게만 telnet service 허용

- Application gateway
  - Firewall과 협업해서 Packet filter를 함
  - IP/TCP/UDP 보다 윗계층에서 application data를 확인