

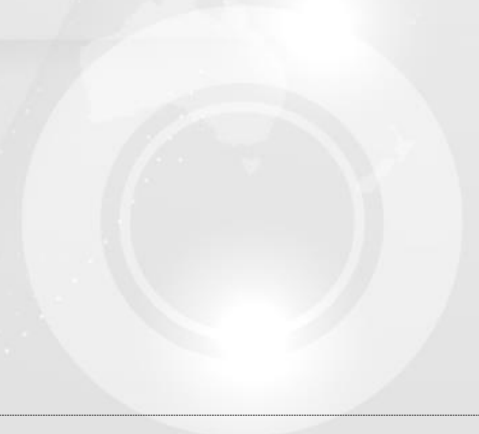
네트워크 취약점 이해 및 대응

Contents

- I. 네트워크 기초
- II. 네트워크 스캐닝
- III. 스니핑 공격 기법의 이해 및 대응
- IV. 스푸핑 공격 기법의 이해 및 대응
- V. 네트워크 보안
- VI. DoS, DDoS 공격 유형과 특징

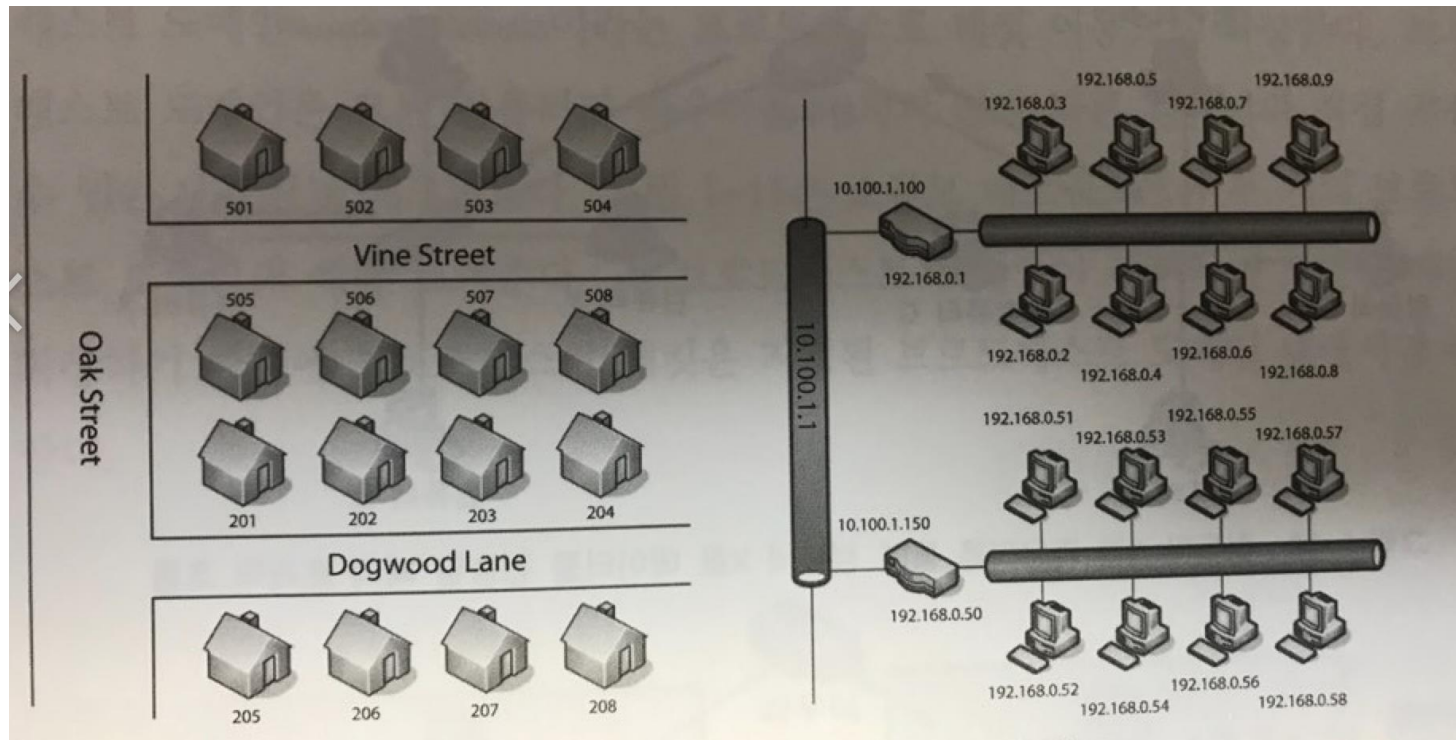
I. 네트워크 기초

1. 네트워크의 이해
2. OSI 7 Layer & TCP/IP
3. 응용, 표현, 세션 계층
(Application, Presentation, Session)
4. 전송 계층(Transport)
5. 네트워크 계층(Network)
6. 데이터링크 계층(Datalink)
7. 물리 계층(Physical)



1 네트워크의 이해

- 서로 떨어져 있는 컴퓨터끼리 연결하는 도로(망)
- Key Concepts:
프로토콜, 네트워크 계층(OSI 7 Layer, TCP/IP Layer), 네트워크 장비
- 네트워크 해킹 단계: 정찰, 스캐닝, 침투



1 네트워크의 이해 - 프로토콜(Protocol)

- 컴퓨터 사이에 메시지를 주고받기 위한 통신방법에 대한 규칙과 약속
- 프로토콜의 본래 의미는 외교에서 의례 또는 의정서
- RFC Editor : <https://www.rfc-editor.org/standards>

Internet Standards

STD #	Number	Files	Title	Authors	Date	More Info	Status
STD 3	RFC 1122	ASCII, PDF	Requirements for Internet Hosts - Communication Layers	R. Braden, Ed.	October 1989	Errata , Updates RFC 793, Updated by RFC 1349, RFC 4379, RFC 5884, RFC 6093, RFC 6298, RFC 6633, RFC 6864, RFC 8029	Internet Standard
STD 3	RFC 1123	ASCII, PDF	Requirements for Internet Hosts - Application and Support	R. Braden, Ed.	October 1989	Errata , Updates RFC 822, RFC 952, Updated by RFC 1349, RFC 2181, RFC 5321, RFC 5966, RFC 7766	Internet Standard
STD 5	RFC 791	ASCII, PDF	Internet Protocol	J. Postel	September 1981	Errata , Obsoletes RFC 760, Updated by RFC 1349, RFC 2474, RFC 6864	Internet Standard
STD 5	RFC 792	ASCII, PDF	Internet Control Message Protocol	J. Postel	September 1981	Errata , Obsoletes RFC 777, Updated by RFC 950, RFC 4884, RFC 6633, RFC 6918	Internet Standard
STD 5	RFC 950	ASCII, PDF	Internet Standard Subnetting Procedure	J.C. Mogul, J. Postel	August 1985	Updates RFC 792, Updated by RFC 6918	Internet Standard
STD 5	RFC 1112	ASCII, PDF	Host extensions for IP multicasting	S.E. Deering	August 1989	Obsoletes RFC 988, RFC 1054, Updated by RFC 2236	Internet Standard
STD 5	RFC 919	ASCII, PDF	Broadcasting Internet Datagrams	J.C. Mogul	October 1984		Internet Standard
STD 5	RFC 922	ASCII, PDF	Broadcasting Internet datagrams in the presence of subnets	J.C. Mogul	October 1984		Internet Standard
STD 6	RFC 768	ASCII, PDF	User Datagram Protocol	J. Postel	August 1980		Internet Standard
STD 7	RFC 793	ASCII, PDF	Transmission Control Protocol	J. Postel	September 1981	Errata , Obsoletes RFC 761, Updated by RFC 1122, RFC 3168, RFC 6093, RFC 6528	Internet Standard
STD 8	RFC 854	ASCII, PDF	Telnet Protocol Specification	J. Postel, J.K. Reynolds	May 1983	Errata , Obsoletes RFC 764, Updated by RFC 5198	Internet Standard
STD 8	RFC 855	ASCII, PDF	Telnet Option Specifications	J. Postel, J.K. Reynolds	May 1983	Obsoletes NIC 18640	Internet Standard
STD 9	RFC 959	ASCII, PDF	File Transfer Protocol	J. Postel, J. Reynolds	October 1985	Errata , Obsoletes RFC 765, Updated by RFC 2228, RFC 2640, RFC 2773, RFC 3659, RFC 5797, RFC 7151	Internet Standard

RFC: 793

TRANSMISSION CONTROL PROTOCOL

DARPA INTERNET PROGRAM
PROTOCOL SPECIFICATION

September 1981

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

by

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90231

September 1981

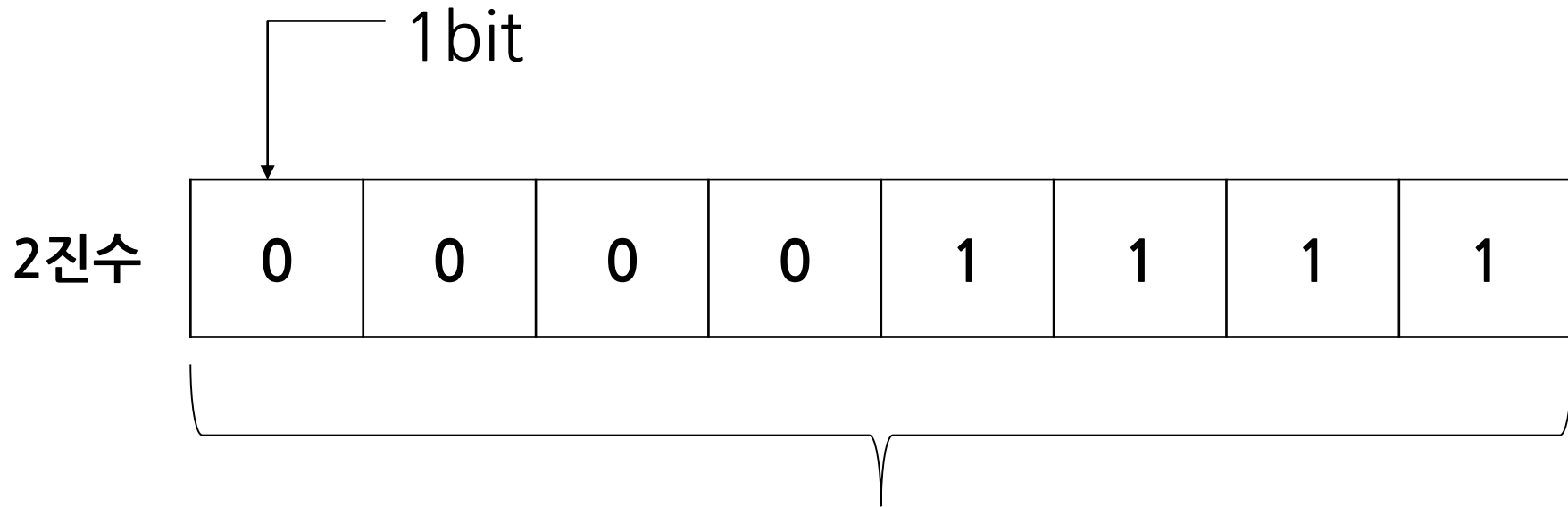
Transmission Control Protocol

1 네트워크의 이해 - 2진수, 10진수, 16진수

- 컴퓨터는 기본적으로 2진수를 사용
 - 2진수는 0,1로 이루어져 있음
 - 10진수는 0~9로 이루어져 있음
 - 16진수는 0~F로 이루어져 있음

2진수	0 (8)	0 (4)	0 (2)	0 (1)		1 (8)	1 (4)	1 (2)	1 (1)
10진수	0				~	15			
16진수	0					F			

1 네트워크의 이해 - Bit(Binary Digit) & Byte



10진수

15

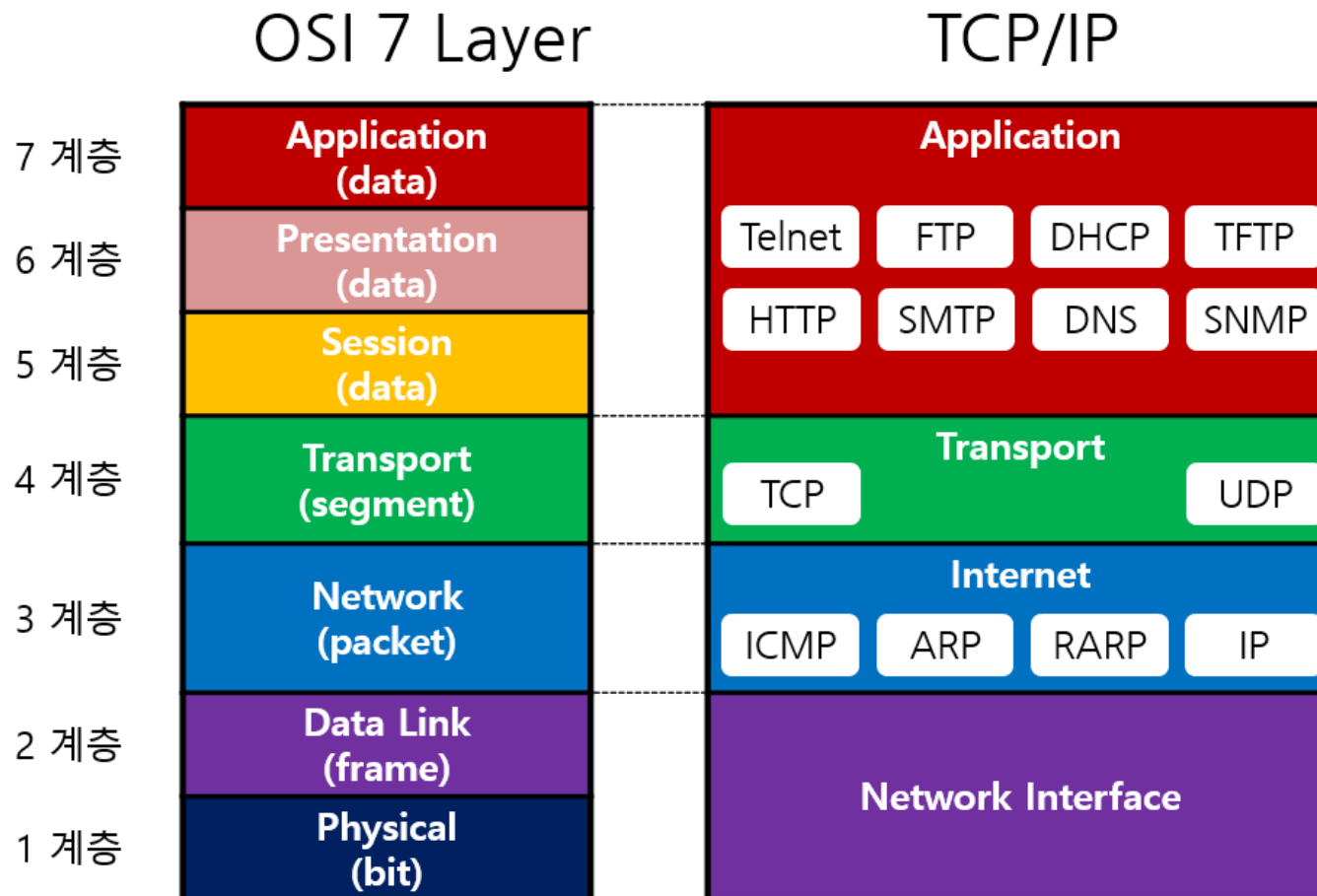
16진수

0

F

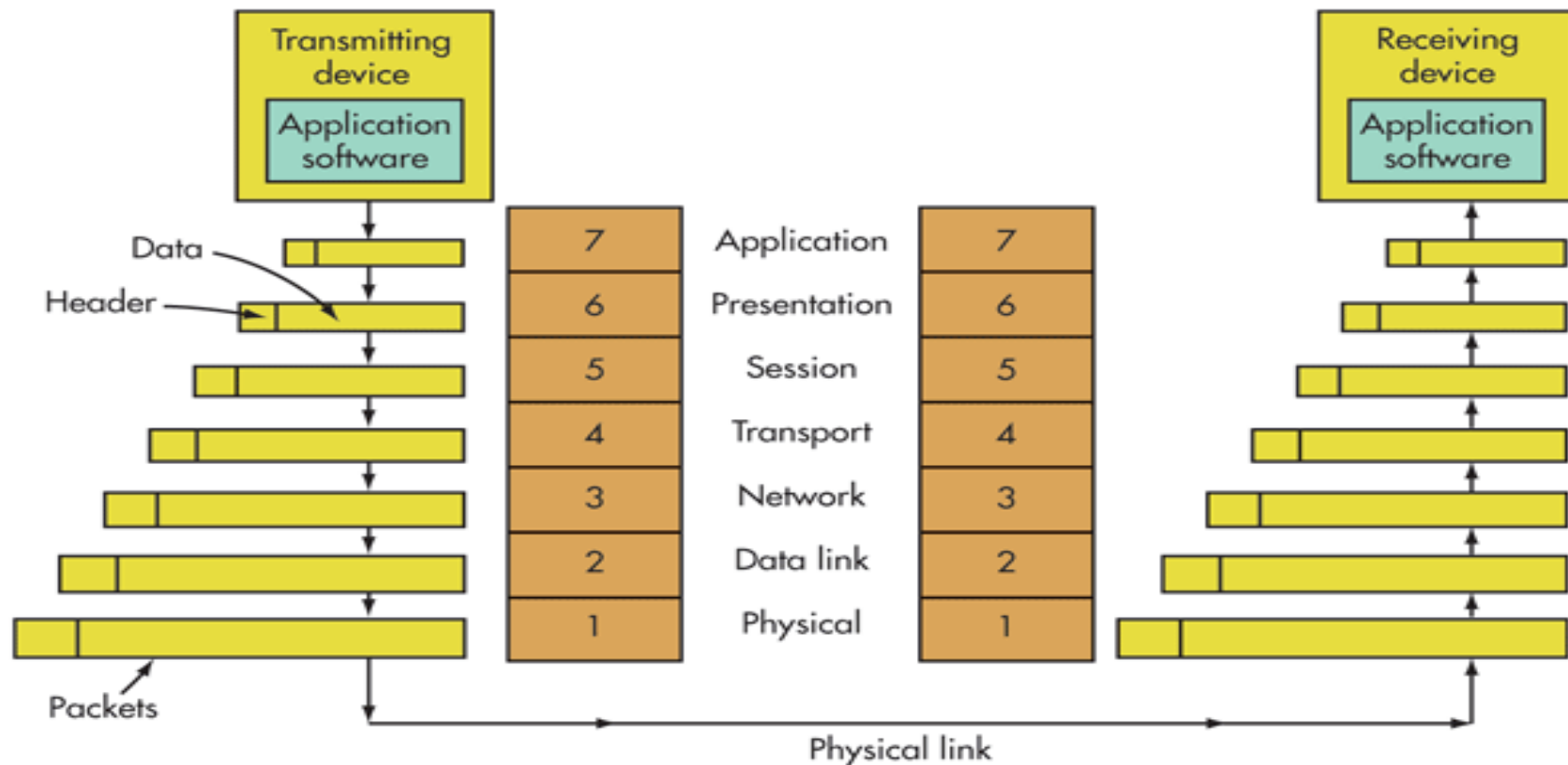
2 OSI 7 Layer & TCP/IP

- 국제표준화기구(ISO : International Organization for Standardization)는 다양한 네트워크의 호환을 위해 OSI 7계층이라는 표준 네트워크 모델을 설계함



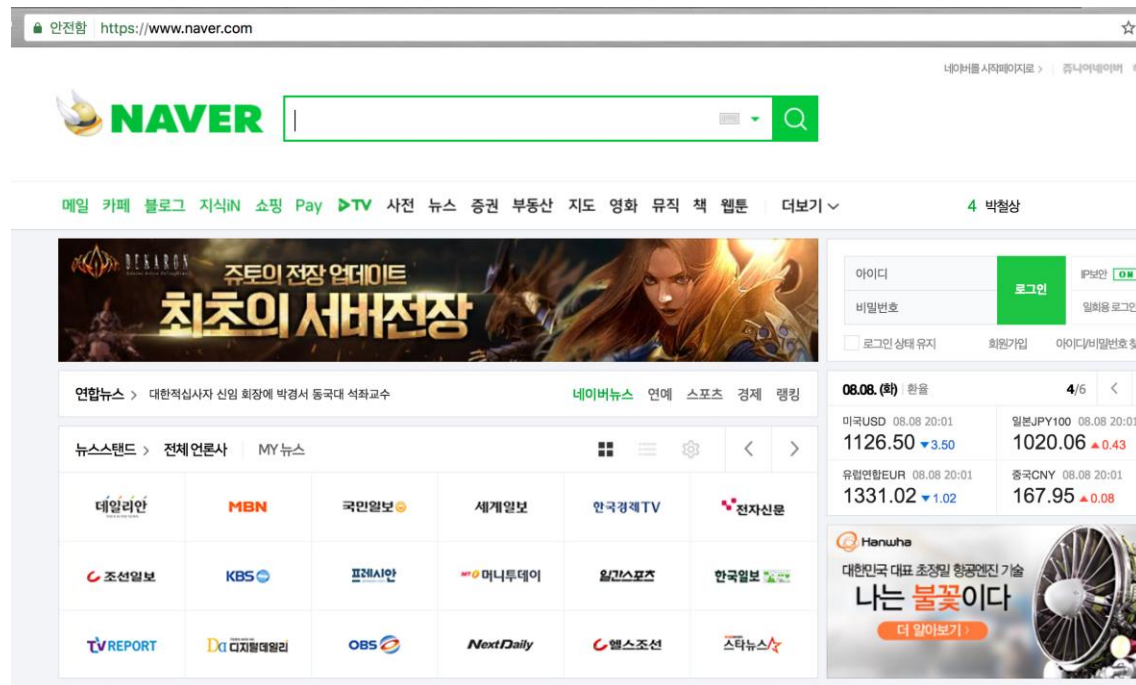
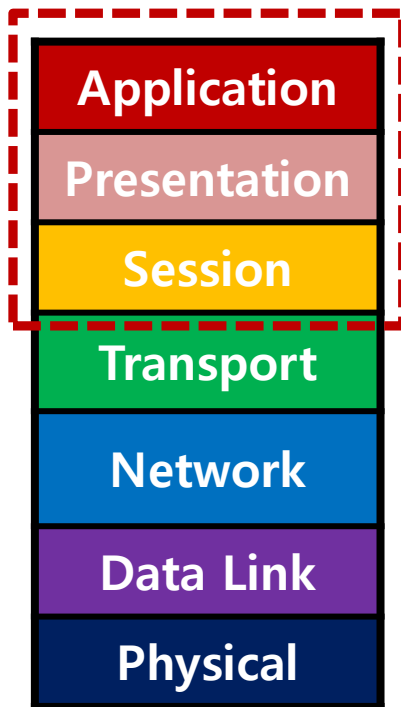
2 OSI 7 Layer & TCP/IP

- 패킷을 생성할 때는 OSI 7 Layer 위층에서부터 아래층으로 진행
- 패킷을 해석할 때는 OSI 7 Layer 아래층에서 위층으로 진행



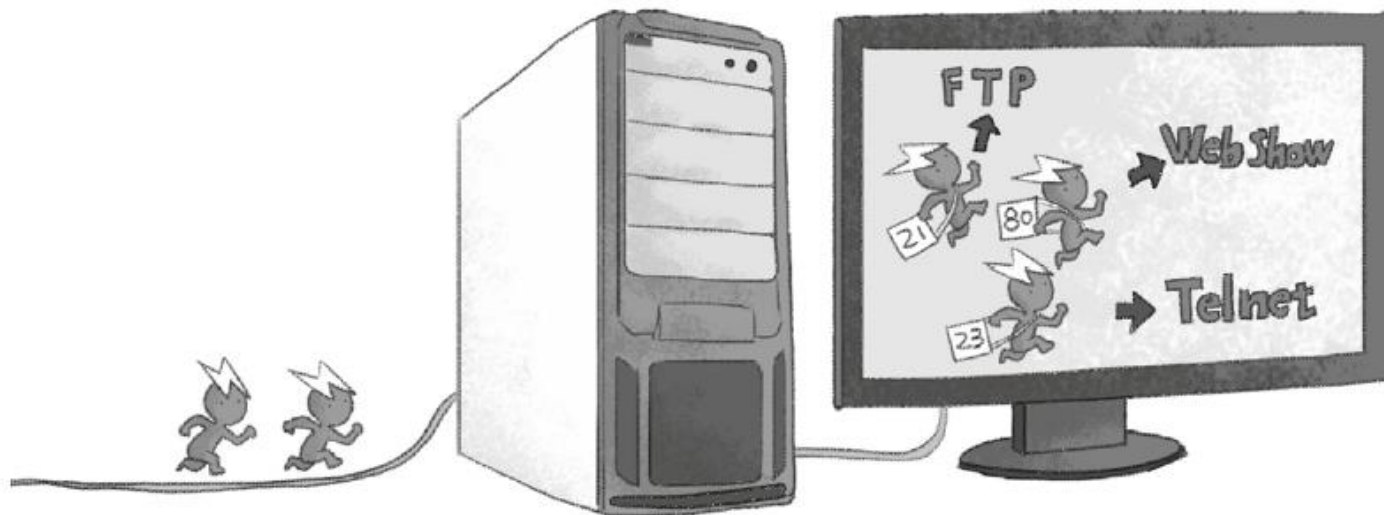
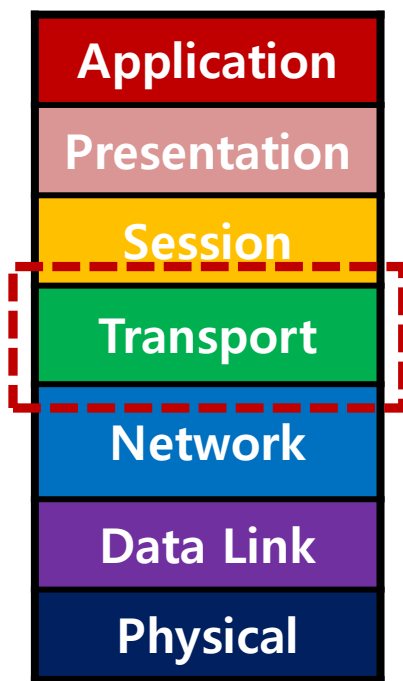
3 응용, 표현, 세션 계층

- 네트워크 통신을 하기 위해 사용되는 응용 프로그램이 구동하는 계층
 - FTP (File Transfer Protocol) : 파일 전송을 위해 사용되는 프로토콜
 - HTTP (Hypertext Transfer Protocol) : 웹 통신을 하기 위해 사용되는 프로토콜
 - Telnet : 원격 접속 서비스를 위해 사용되는 프로토콜
 - SMTP (Simple Mail Transfer Protocol) : 메일 서비스를 위해 사용되는 프로토콜



4 전송 계층

- 통신 양 끝단(Host to Host) 사용자들이 신뢰성 있는 데이터를 주고 받을 수 있도록 함
 - TCP(Transmission Control Protocol)
 - TCP도 별도의 주소를 가지고 있는데, 이를 포트(Port)라고 함
 - 포트는 시스템에 도착한 후 패킷이 찾아갈 응용 프로그램과 통하는 통로 번호
 - UDP(User Datagram Protocol)는 신뢰성 있는 전송을 보장하지 않음



4 전송 계층 - 포트(Port)

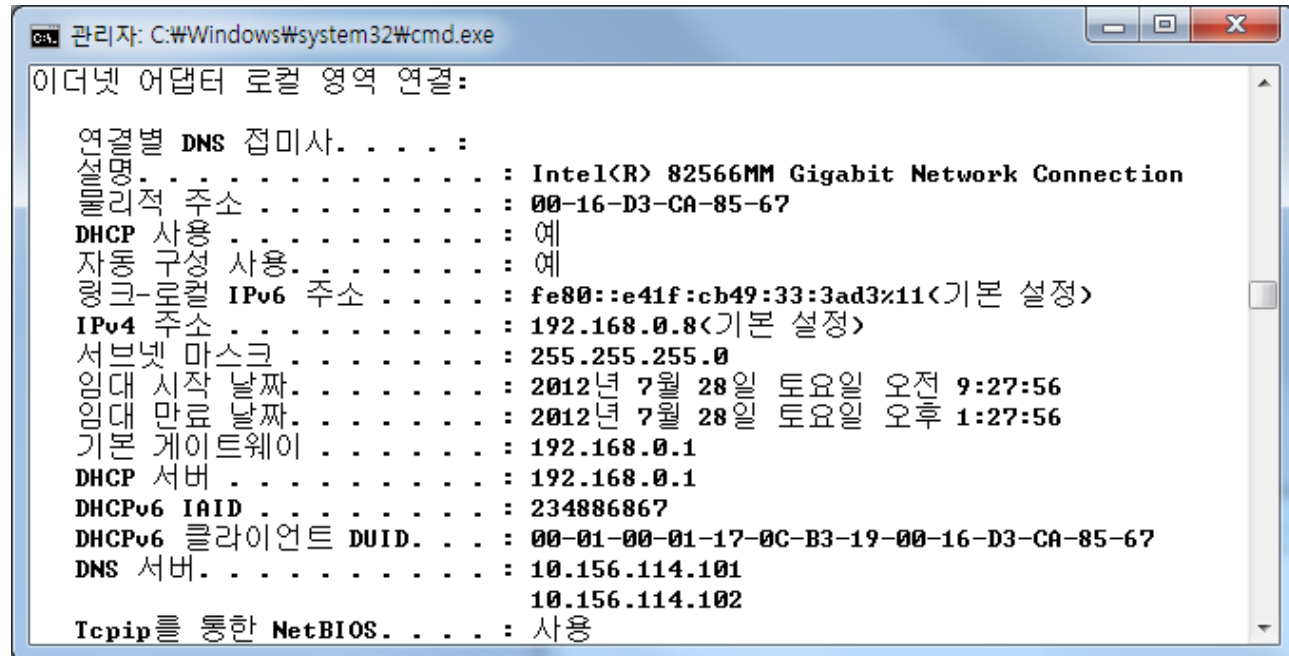
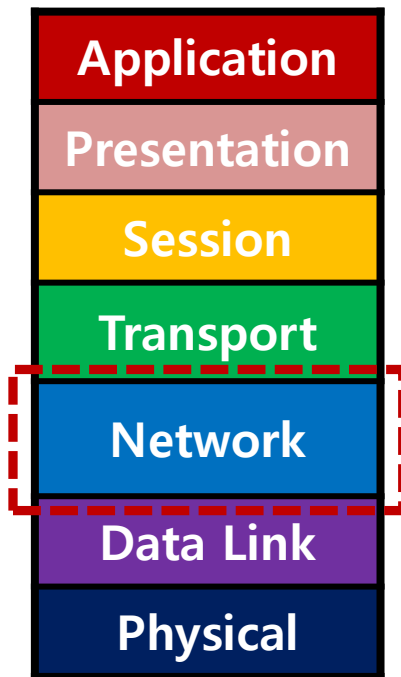
- 호스트 내 실행되고 있는 프로그램을 구분하기 위한 주소(서비스 번호)
 - 잘 알려진 포트(Well Known Ports) : 0 ~ 1023 - 예약 영역
 - 등록된 포트(Registered Ports) : 1024 ~ 49151 - 서버 소켓
 - 동적 포트(Dynamic Ports) : 49152 ~ 65535 - 동적

포트	Pro	설명
20	TCP	FTP (File Transfer Protocol) - 데이터 포트
21	TCP	FTP (File Transfer Protocol) - 제어 포트
22	TCP	SSH (Secure Shell) - ssh scp, sftp 같은 프로토콜 및 포트 포워딩
23	TCP	텔넷 (Telnet) 프로토콜
25	TCP	SMTP (Simple Mail Transfer Protocol) - 이메일 전송에 사용
53	TCP UDP	DNS (Domain Name System)
67		DHCP (Dynamic Host Configuration Protocol) 서버
68		DHCP (Dynamic Host Configuration Protocol) 클라이언트
80	TCP UDP	HTTP (HyperText Transfer Protocol) - 웹 페이지 전송
88	TCP	커베로스(Kerberos) - 인증 에이전트

포트	Pro	설명
123	UDP	NTP (Network Time Protocol) - 시간 동기화
135	TCP	RPC (Remote Procedure Call)
139	TCP	넷바이오스(NetBIOS) 세션
161	UDP	SNMP (Simple Network Management Protocol) - Agent 포트
162	UDP	SNMP (Simple Network Management Protocol) - Manager 포트
443	TCP	HTTPS - HTTP over SSL (암호화 전송)
445	TCP	Microsoft-DS SMB 파일 공유
1433	TCP	Microsoft SQL Server(MS-SQL)
3343	TCP	클러스터 서비스(Windows Clustering/Failover Cluster)
3389	TCP	터미널 서비스(원격 데스크톱)

5 네트워크 계층

- 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 수행
 - 다양한 길이의 데이터를 네트워크를 통해 전달하며 그 과정에서 라우팅, 흐름 제어, 세그멘테이션(segmentation/desegmentation), 오류 제어 등을 수행
 - 네트워크 계층에서 여러 개의 노드를 거쳐 경로를 찾기 위한 주소는 IP로 대표됨
 - 윈도우: ipconfig 명령어로 확인, 유닉스/리눅스/MacOS: ifconfig 명령어로 확인



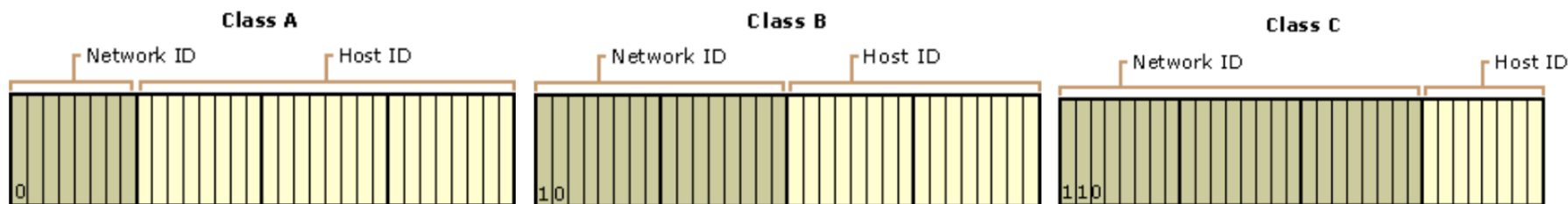
```
관리자: C:\Windows\system32\cmd.exe
이더넷 어댑터 로컬 영역 연결:

   연결별 DNS 접미사. . . . . : 
   설명. . . . . : Intel(R) 82566MM Gigabit Network Connection
   물리적 주소. . . . . : 00-16-D3-CA-85-67
   DHCP 사용. . . . . : 예
   자동 구성 사용. . . . . : 예
   링크-로컬 IPv6 주소. . . . . : fe80::e41f:cb49:33:3ad3%11<기본 설정>
   IPv4 주소. . . . . : 192.168.0.8<기본 설정>
   서브넷 마스크. . . . . : 255.255.255.0
   임대 시작 날짜. . . . . : 2012년 7월 28일 토요일 오전 9:27:56
   임대 만료 날짜. . . . . : 2012년 7월 28일 토요일 오후 1:27:56
   기본 게이트웨이. . . . . : 192.168.0.1
   DHCP 서버. . . . . : 192.168.0.1
   DHCPv6 IAID. . . . . : 234886867
   DHCPv6 클라이언트 DUID. . . : 00-01-00-01-17-0C-B3-19-00-16-D3-CA-85-67
   DNS 서버. . . . . : 10.156.114.101
   : 10.156.114.102
   Tcpip를 통한 NetBIOS. . . . . : 사용
```

5 네트워크 계층 - IP(Internet Protocol) 주소

• 인터넷에 연결된 기기의 주소

- 현재는 IPv4를 사용(8bit의 수 4개로 구성 = 32bit)
- 0.0.0.0 ~ 255.255.255.255(단, 0.0.0.0은 모든 IP를 의미)



구분	IP 주소	사용 가능 컴퓨터 수	지정된 사설 네트워크	주요 사용
A 클래스	1~126.xxx.xxx.xxx	16,777,214	10.0.0.0 ~ 10.255.255.255	국가나 대형망

127.0.0.1~127.255.255.255 는 loopback과 diagnostic functions으로 예약되어 있음.

B 클래스	128~191.aaa.xxx.xxx	65,534	172.16.0.0 ~ 172.31.255.255	학교 등 중대규모
C 클래스	192~223.aaa.bbb.xxx	254	192.168.0.0 ~ 192.168.255.255	소규모 회사
D 클래스	224~239.aaa.bbb.xxx	Reserved for Multicasting		

5 네트워크 계층 - IP(Internet Protocol) 주소

- 네트워크 주소와 호스트 주소로 구성
 - 서브넷 마스크를 이용해서 구분
- Prefix 표기법을 이용해 서브넷 마스크 표기 가능

192 . 168 . 56 . 1

IP 주소

11000000	10101000	00111000	00000001
----------	----------	----------	----------

서브넷 마스크

11111111	11111111	11111111	00000000
----------	----------	----------	----------

255 . 255 . 255 . 0

네트워크 주소

호스트 주소

192.168.56.1 255.255.255.0 = 192.168.56.1/24

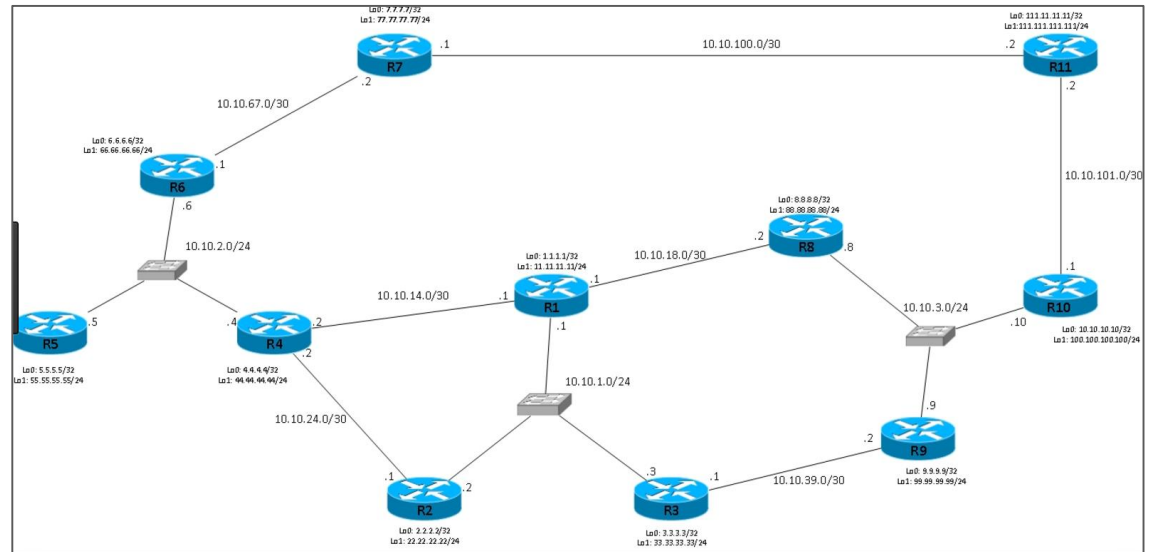
5 네트워크 계층 - IP 조회

• IP 조회하기

- (Check) wq.apnic.net에서 101.1.1.1 조회 → 차이나텔레콤
- (Check) whois.kisa.or.kr에서 1.234.0.0 조회 → SK브로드밴드 (A Class)
- (Check) ping www.dhs.gov → 23.62.232.56
whois.arin.net 에서 조회 → 23.32.0.0 - 23.67.255.255 (A Class) , AKAMAI
- (Check) ping www.korea.ac.kr → 163.152.x.x (B Class)
- (Check) ping www.onesecurity.kr
→ 211.43.212.0 - 211.43.212.255 (가비아, C Class)

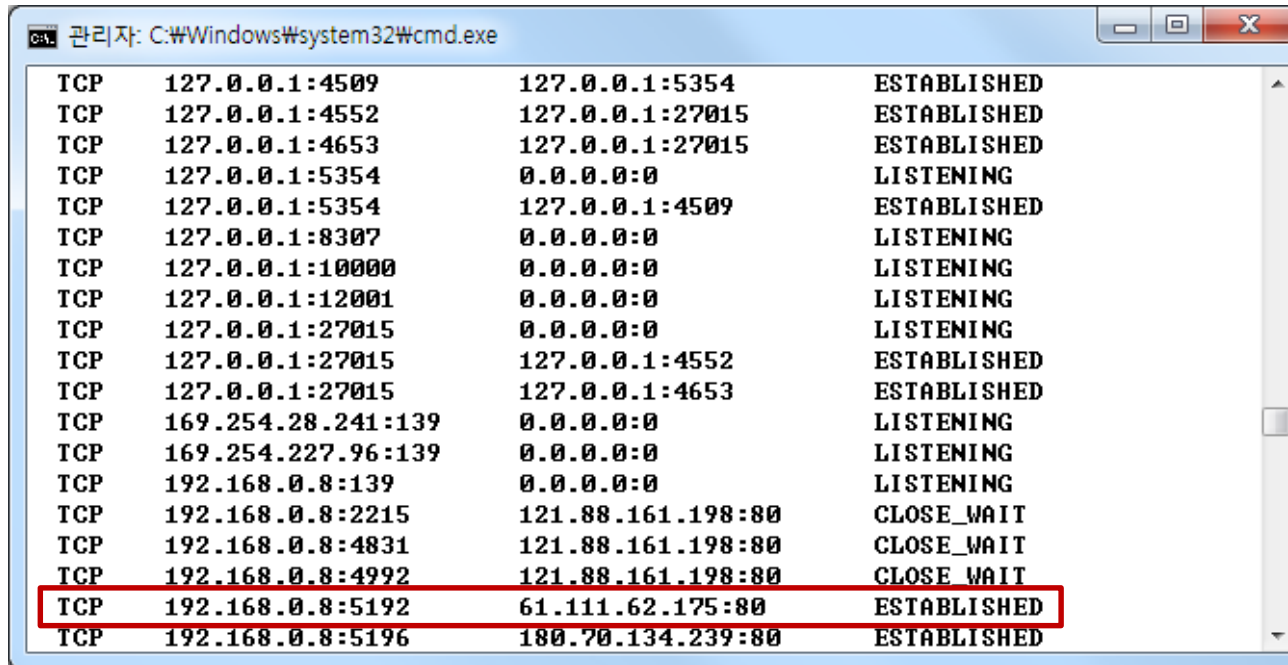
5 네트워크 계층 - 라우터

- 네트워크 계층의 대표적인 장비는 '라우터'(또는 '게이트웨이' 라고도 함)
 - 라우터의 가장 중요한 기능은 패킷의 최적 경로를 찾기 위한 라우팅 테이블을 구성
 - 라우팅 테이블에 따라 패킷을 목적지까지 가장 빠르게 보내는 길잡이 역할을 수행

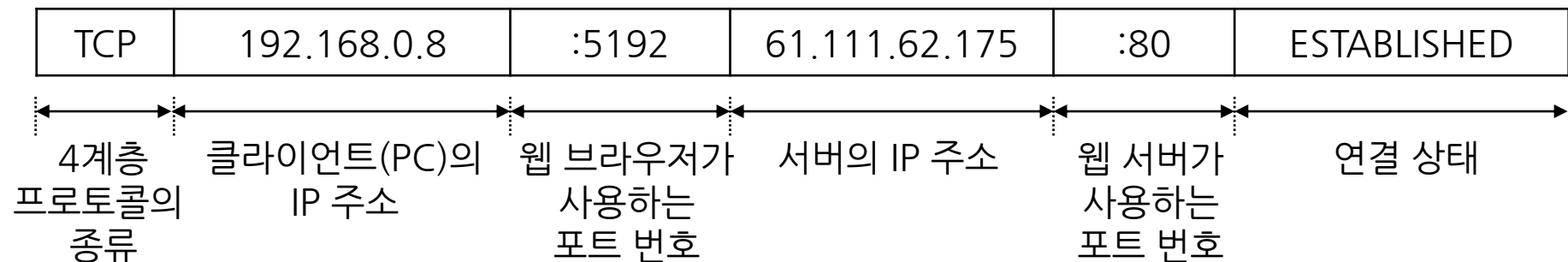


5 네트워크 계층 - 연결 상태 확인

- 네트워크 계층과 전송 계층은 `netstat -an` 명령어로 확인 할 수 있음

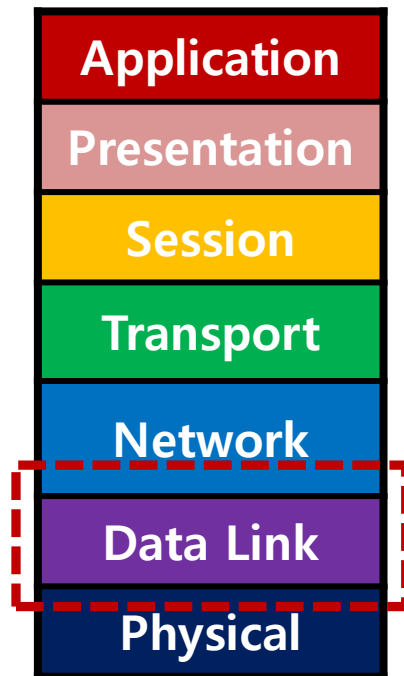


```
관리자: C:\Windows\system32\cmd.exe
TCP    127.0.0.1:4509      127.0.0.1:5354      ESTABLISHED
TCP    127.0.0.1:4552      127.0.0.1:27015     ESTABLISHED
TCP    127.0.0.1:4653      127.0.0.1:27015     ESTABLISHED
TCP    127.0.0.1:5354      0.0.0.0:0           LISTENING
TCP    127.0.0.1:5354      127.0.0.1:4509      ESTABLISHED
TCP    127.0.0.1:8307      0.0.0.0:0           LISTENING
TCP    127.0.0.1:10000     0.0.0.0:0           LISTENING
TCP    127.0.0.1:12001     0.0.0.0:0           LISTENING
TCP    127.0.0.1:27015     0.0.0.0:0           LISTENING
TCP    127.0.0.1:27015     127.0.0.1:4552      ESTABLISHED
TCP    127.0.0.1:27015     127.0.0.1:4653      ESTABLISHED
TCP    169.254.28.241:139  0.0.0.0:0           LISTENING
TCP    169.254.227.96:139  0.0.0.0:0           LISTENING
TCP    192.168.0.8:139     0.0.0.0:0           LISTENING
TCP    192.168.0.8:2215    121.88.161.198:80    CLOSE_WAIT
TCP    192.168.0.8:4831    121.88.161.198:80    CLOSE_WAIT
TCP    192.168.0.8:4992    121.88.161.198:80    CLOSE_WAIT
TCP    192.168.0.8:5192    61.111.62.175:80     ESTABLISHED
TCP    192.168.0.8:5196    180.70.134.239:80    ESTABLISHED
```



6 데이터링크 계층

- End to End 상호 통신을 위해 MAC 주소를 할당
 - MAC(Media Access Control) 주소는 ipconfig /all 명령을 실행해 확인할 수 있음



```
관리자: C:\Windows\system32\cmd.exe
이더넷 어댑터 로컬 영역 연결:

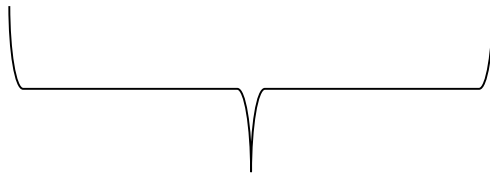
연결별 DNS 접미사. . . . . : 
연결별 . . . . . : Intel(R) 82566MM Gigabit Network Connection
물리적 주소 . . . . . : 00-16-D3-CA-85-67
DHCP 사용 . . . . . : 예
자동 구성 사용 . . . . . : 예
링크-로컬 IPv6 주소 . . . . : fe80::e41f:cb49:33:3ad3%11<기본 설정>
IPv4 주소 . . . . . : 192.168.0.8<기본 설정>
서브넷 마스크 . . . . . : 255.255.255.0
임대 시작 날짜 . . . . . : 2012년 7월 28일 토요일 오전 9:27:56
임대 만료 날짜 . . . . . : 2012년 7월 28일 토요일 오후 1:27:56
기본 게이트웨이 . . . . . : 192.168.0.1
DHCP 서버 . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 234886867
DHCPv6 클라이언트 DUID. . . : 00-01-00-01-17-0C-B3-19-00-16-D3-CA-85-67
DNS 서버 . . . . . : 10.156.114.101
                        10.156.114.102
Tcpip를 통한 NetBIOS. . . . : 사용
```

6 데이터링크 계층 - MAC 주소

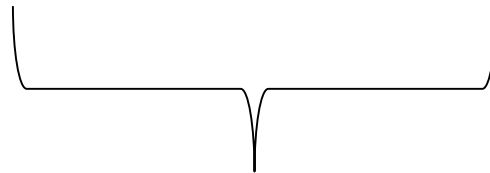
- 인터페이스 카드(NIC, Network Interface card)를 제조할 때 할당
 - 물리적인 주소
 - 16진수로 표현
- 고유의 주소이므로 세상에 한개 밖에 없음
 - But, MAC 주소는 논리적으로 변경 가능!



a4 : 5e : 60 : cd : 4f : 0d



제조업체 식별코드



업체 랜카드 정보

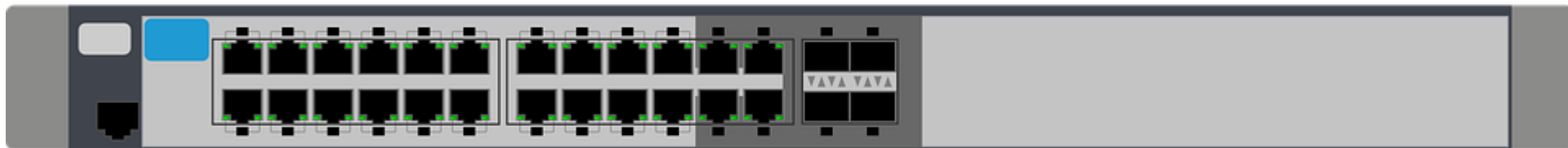
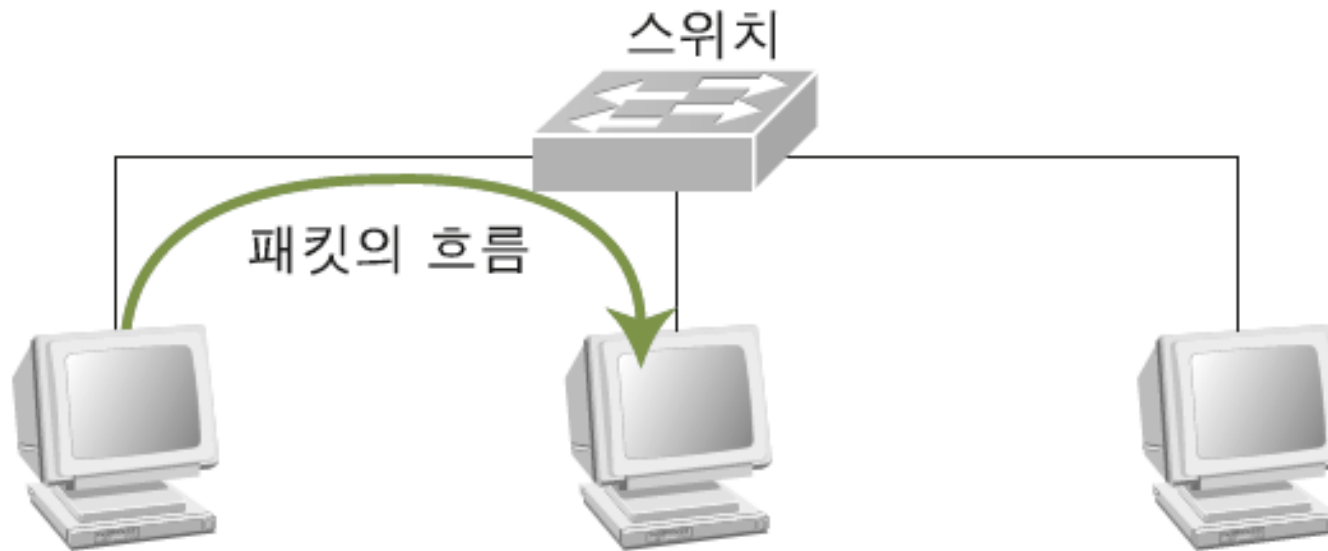
Search results for "a4:5e:60"

MAC	Vendor
A45E60	Apple, Inc.

<https://hwaddress.com/>

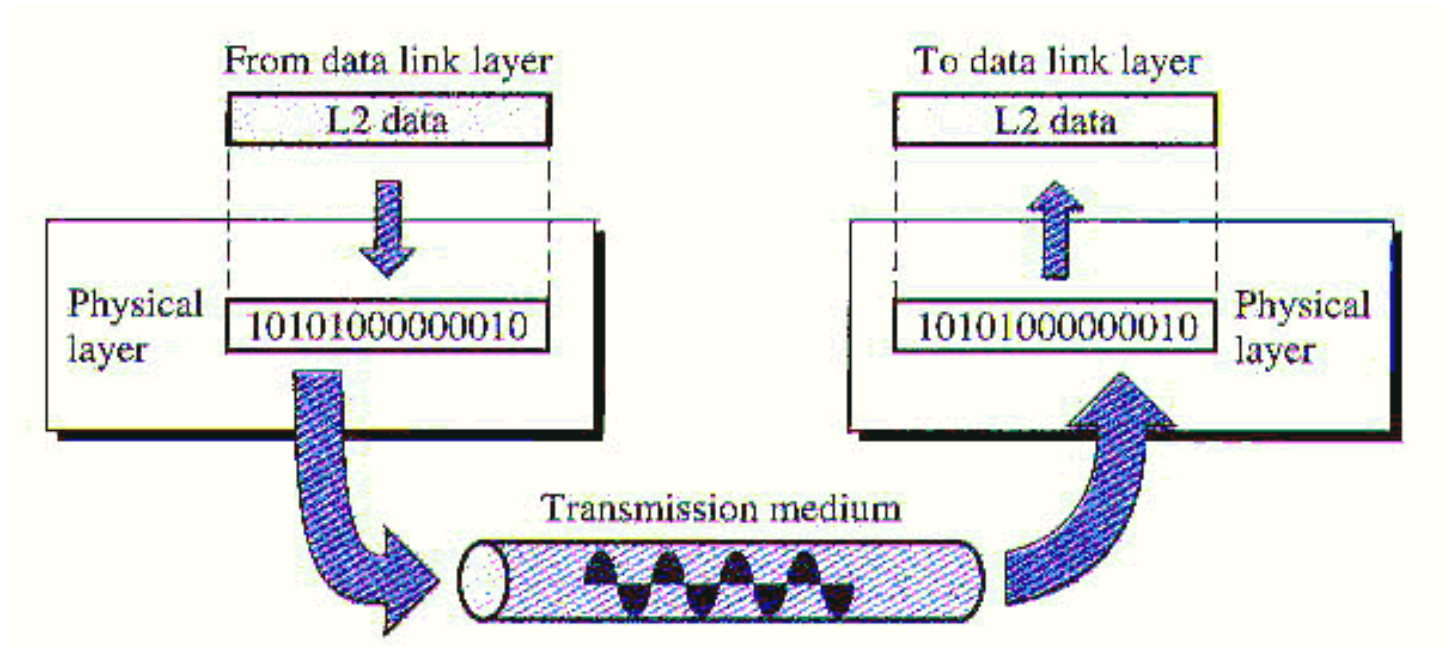
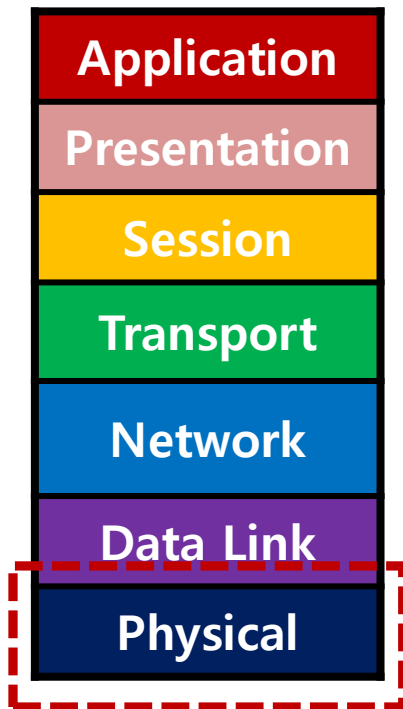
6 데이터링크 계층 - 스위치

- 데이터링크 계층의 대표적인 장비로는 ‘스위치’가 있음



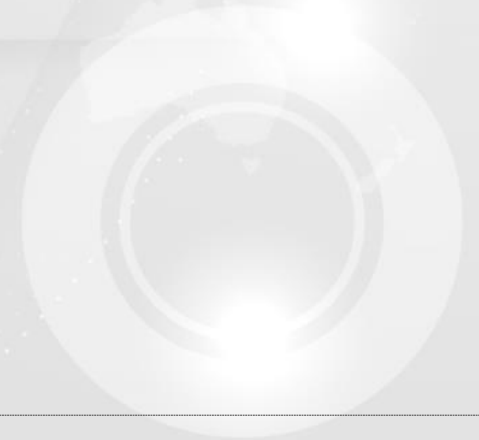
7 물리 계층

- 랜 케이블, 동축 케이블, 광 케이블 등 시스템 간의 물리적 연결을 위한 계층



II . 네트워크 정보수집

1. SSDP
2. IP 주소 Tracking
3. Network Scanning



1 SSDP (Simple Service Discovery Protocol)

- 네트워크 서비스나 정보를 찾기 위해서 사용하는 네트워크 프로토콜
 - SSDP는 HTTPU(UDP 기반의 HTTP)를 이용. 모든 데이터는 text로 통신
 - 사용하는 포트는 UDP 1900이며, IP multicast 주소를 이용.
 - IPv4에서 멀티캐스트 주소는 239.255.255.250
 - <https://wiki.wireshark.org/SSDP>,
<https://tools.ietf.org/html/draft-cai-ssdp-v1-00>,

No. ↓	Time	Source	Destination	Protocol	Info
508	23.452661	128.100.20.52	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
509	23.463234	128.100.20.52	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
510	23.472439	128.100.20.52	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
511	23.481717	128.100.20.52	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
513	23.571197	128.100.170.29	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
583	26.571177	128.100.170.29	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
861	35.019794	128.100.170.113	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
935	38.015690	128.100.170.113	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
976	41.015147	128.100.170.113	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
1360	55.020106	128.100.170.113	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1

⊞ Frame 511 (386 bytes on wire (386 bytes captured))

⊞ Ethernet II, Src: SamsungE_26:1c:6f (00:15:99:26:1c:6f), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

⊞ Internet Protocol, Src: 128.100.20.52 (128.100.20.52), Dst: 239.255.255.250 (239.255.255.250)

⊞ User Datagram Protocol, Src Port: 1024 (1024), Dst Port: ssdp (1900)

⊞ Hypertext Transfer Protocol

⊞ NOTIFY * HTTP/1.1\r\n

Request Method: NOTIFY

Request URI: *

Request Version: HTTP/1.1

HOST: 239.255.255.250:1900\r\n

CACHE-CONTROL: max-age=60\r\n

LOCATION: http://128.100.20.52:5200/Printer.xml\r\n

NT: urn:schemas-upnp-org:service:PrintBasic:1\r\n

NTS: ssdp:alive\r\n

SERVER: Network Printer Server UPnP/1.0 OS 1.03.04.02 12-21-2007\r\n

USN: uuid:Dell-Printer-1_0-dsi-secretariat::urn:schemas-upnp-org:service:PrintBasic:1\r\n\r\n

2 IP 주소 Tracking

- 공격 또는 취약점 진단을 하고자 하는 대상 네트워크 범위 식별
 - ping www.korea.ac.kr → 163.152.6.10
 - ping portal.korea.ac.kr → 163.152.6.19
 - whois 163.152.6.19 → inetnum: 163.152.0.0 - 163.152.255.255
 - ping yonsei.ac.kr → 165.132.13.38
 - whois 165.132.13.38 → inetnum: 165.132.0.0 - 165.132.255.255
- 특정 네트워크 대역에 있는 호스트 중 웹 서비스를 구동 중인 호스트 식별
 - nmap 163.152.6.1/24 -p 80,443 -oN 163.152.6.1-255.nmap -vv
- 내부 네트워크 대역에 있는 호스트 중 살아있는 호스트 식별
 - fping -q -a -s -g 192.168.219.0/24

2 IP 주소 Tracking

- <https://dev.maxmind.com/geoip/legacy/geolite/>

Downloads

Database	Download links				
	Binary / gzip	Binary / xz	CSV / gzip	CSV / zip	CSV / xz
GeoLite Country	Download	Gzip only	Zip only	Download	Zip only
GeoLite Country IPv6	Download	Gzip only	Download	Gzip only	Gzip only
GeoLite City	Download	Download	Zip and xz only	Download	
GeoLite City IPv6 (Beta)	Download	Gzip only	Download	Gzip only	
GeoLite ASN	Download	Gzip only	Zip only	Download	
GeoLite ASN IPv6	Download	Gzip only	Zip only	Download	

1.0.0.0	1.0.0.255	16777216	16777471	AU	Australia
1.0.1.0	1.0.3.255	16777472	16778239	CN	China
1.0.4.0	1.0.7.255	16778240	16779263	AU	Australia
1.0.8.0	1.0.15.255	16779264	16781311	CN	China
1.0.16.0	1.0.31.255	16781312	16785407	JP	Japan
1.0.32.0	1.0.63.255	16785408	16793599	CN	China
1.0.64.0	1.0.127.25	16793600	16809983	JP	Japan
1.0.128.0	1.0.255.25	16809984	16842751	TH	Thailand
1.1.0.0	1.1.0.255	16842752	16843007	CN	China
1.1.1.0	1.1.1.255	16843008	16843263	AU	Australia
1.1.2.0	1.1.63.255	16843264	16859135	CN	China
1.1.64.0	1.1.127.25	16859136	16875519	JP	Japan
1.1.128.0	1.1.255.25	16875520	16908287	TH	Thailand
1.2.0.0	1.2.2.255	16908288	16909055	CN	China
1.2.3.0	1.2.3.255	16909056	16909311	US	United State
1.2.4.0	1.2.127.25	16909312	16941055	CN	China
1.2.128.0	1.2.255.25	16941056	16973823	TH	Thailand
1.3.0.0	1.3.255.25	16973824	17039359	CN	China
1.4.0.0	1.4.0.255	17039360	17039615	AU	Australia
1.4.1.0	1.4.127.25	17039616	17072127	CN	China
1.4.128.0	1.4.255.25	17072128	17104895	TH	Thailand
1.5.0.0	1.5.255.25	17104896	17170431	JP	Japan
1.6.0.0	1.7.255.25	17170432	17301503	IN	India
1.8.0.0	1.8.255.25	17301504	17367039	CN	China
1.9.0.0	1.9.255.25	17367040	17432575	MY	Malaysia

The GeoLite Legacy databases may also be downloaded and updated with our [GeoIP Update program](#).

2 IP 주소 Tracking

- ip-tracker.org (163.152.6.19)

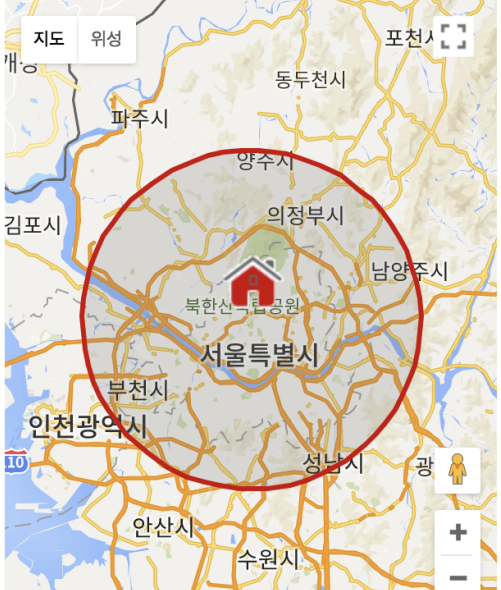
www.ip-tracker.org/locator/ip-lookup.php?ip=163.152.6.19

163.152.6.19

Lookup IP Address With IP Lookup

Advertisements

Ads by Google IP Check Address Tracing Location Finder

Advertisements	IP Locator & IP Lookup Basic Tracking Info
IP Lookup Result From IP Locator on IP Map 	IP Address: 163.152.6.19 IP Blacklist Check
	Reverse DNS: 19.6.152.163.in-addr.arpa Hostname: portal.korea.ac.kr
	Nameservers: e.dns.kr >> 202.30.124.100 b.dns.kr >> 61.74.75.1 d.dns.kr >> 203.83.159.1 f.dns.kr >> 218.38.181.90 c.dns.kr >> 203.248.246.220 g.dns.kr >> 202.31.190.1
	Lookup IP Address Location For IP: 163.152.6.19
	Continent: Asia (AS)
	Country: Korea, Republic of 🇰🇷 (KR)
	Capital: Seoul
	State: Seoul-t'ukpyolsi
	City Location: Seoul
	ISP: Korea University
	Organization: Korea University
	AS Number: AS9452 Korea University

2 IP 주소 Tracking

- ip-tracker.org (23.62.232.56)

www.ip-tracker.org/locator/ip-lookup.php?ip=23.62.232.56

23.62.232.56

Lookup IP Address With IP Lookup

Advertisements

Ads by Google

IP Check

Address Tracing

Location Finder

Advertisements

IP Locator & IP Lookup Basic Tracking Info

IP Lookup Result From IP Locator on IP Map



IP Address: 23.62.232.56
[\[IP Blacklist Check\]](#)

Reverse DNS: 56.232.62.23.in-addr.arpa


Hostname: a23-62-232-56.deploy.static.akamaitechnologies.com

ns6-32.akamaistream.net >> 95.100.168.32
p7.akamaistream.net >> 95.101.36.32
p8.akamaistream.net >> 23.74.25.32
p6.akamaistream.net >> 95.100.175.32
ax2.akamaistream.net >> 95.100.174.35

Nameservers: ns2-32.akamaistream.net >> 2.22.230.32
p5.akamaistream.net >> 193.108.88.66
ax3.akamaistream.net >> 96.7.49.32
ax0.akamaistream.net >> 72.246.46.32
ns3-32.akamaistream.net >> 23.61.199.32
ax1.akamaistream.net >> 184.26.161.32

Lookup IP Address Location For IP: 23.62.232.56

Continent: North America (NA)

Country: United States  (US)

Capital: Washington

State: Massachusetts

City Location: Cambridge

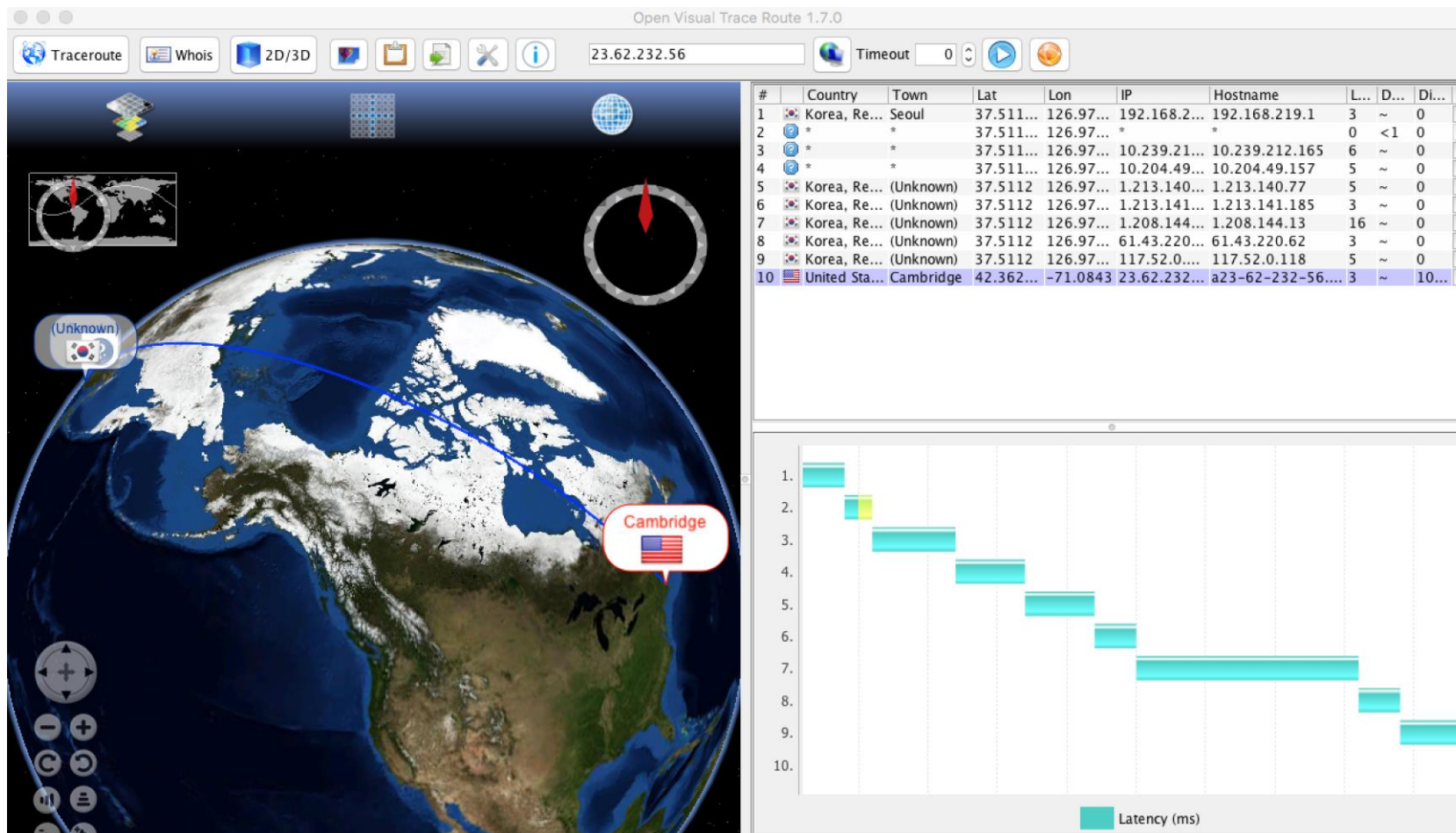
Postal: 02142

Area: 617

- Check IP
 - 175.45.179.68
 - 223.166.0.0

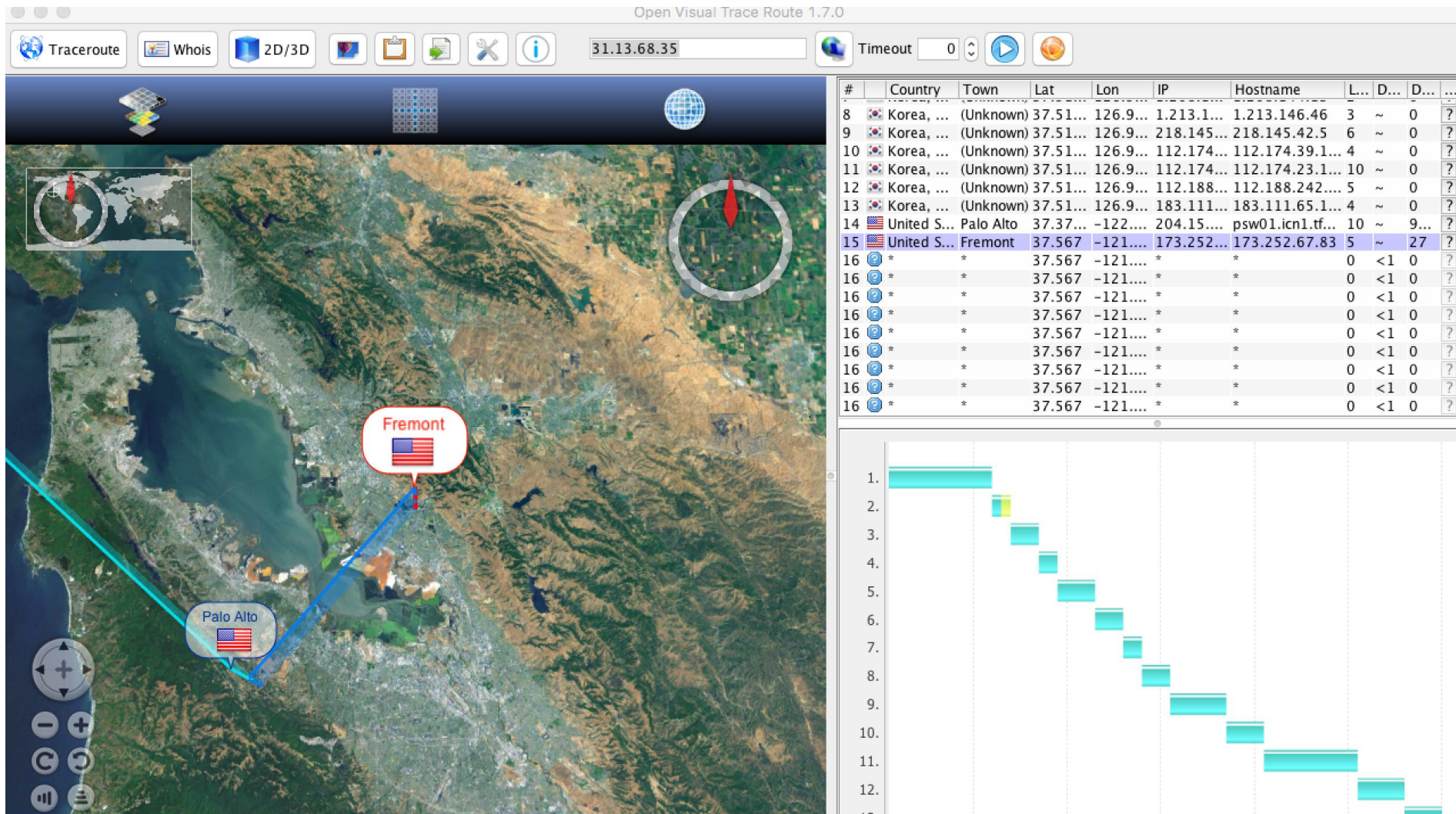
2 IP 주소 Tracking

- <https://www.visualtraceroute.net/>
- Open Visual Trace Route (23.62.232.56)



2 IP 주소 Tracking

- Open Visual Trace Route (31.13.68.35 - facebook.com)



3 Network Scanning

- 공격자가 목표에 대한 네트워크나 시스템의 자세한 정보를 수집하기 위함
 - 시스템에 실행되고 있는 TCP, UDP 서비스들
 - 시스템 및 운영체제 종류
 - 그외 다양한 정보
- 국내에서는 스캐닝만으로도 불법이 될 수 있음

제48조(정보통신망 침해행위 등의 금지)

- ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
- ② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.
- ③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

3 Network Scanning - TCP

- TCP(Transmission Control Protocol)는 **3 Way-Handshake** 과정을 거쳐 **세션을 성립**하고 패킷을 전송하는 **“연결” 지향형 프로토콜**로서 패킷 전송 중 발생하는 손실과 중복, 오류를 검출하고 해결하는 기능을 가지고 있다. 웹(HTTP)과 같은 신뢰성을 요구하는 통신에 사용된다.

Source Port(16bits)								Destination Port(16bits)							
Sequence Number(32bits)															
Acknowledgment Number(32bits)															
Data Offset (4bits)	Reserved (4bits)	Flags(8bits)								Window Size (16bits)					
		C	E	U	A	P	R	S	F						
		W	C	R	C	S	S	Y	I						
		R	E	G	K	H	T	N	N						
Checksum(16bits)								Urgent Pointer(16bits)							
Options and Padding															

3 Network Scanning - TCP

Source Port(16bits)							Destination Port(16bits)						
Sequence Number(32bits)													
Acknowledgment Number(32bits)													
Data Offset (4bits)	Reserved (4bits)	Flags(8bits)								Window Size (16bits)			
		C	E	U	A	P	R	S	F				
		W	C	R	C	S	S	Y	I				
		R	E	G	K	H	T	N	N				
Checksum(16bits)							Urgent Pointer(16bits)						
Options and Padding													

Source Port : 패킷을 송신하는 출발지의 포트번호

Destination Port : 패킷을 수신할 도착지의 포트번호

Sequence Number : 세그먼트(패킷)의 순서 표기

Acknowledgment Number : 수신한 데이터에 대한

확인 응답으로 SEQ+1 값 전송

Data Offset : TCP 헤더와 데이터를 포함한 전체 길이

Reserved : 미래를 위해 예약된 필드. 항상 0

Window Size : 도착지에서 한번에 수신 가능한 버퍼의 크기

Checksum : 데이터가 전송 중 손상되지 않았는지 검사

Urgent Pointer : Urgent 데이터의 마지막 바이트(Urgent Flag가 1로 설정시 동작)

Options and Padding : 최대 40byte, TCP 헤더 외에 추가적인 정보를 송신할때 사용

3 Network Scanning - TCP

Source Port(16bits)							Destination Port(16bits)						
Sequence Number(32bits)													
Acknowledgment Number(32bits)													
Data Offset (4bits)	Reserved (4bits)	Flags(8bits)								Window Size (16bits)			
		C	E	U	A	P	R	S	F				
		W	C	R	C	S	S	Y	I				
		R	E	G	K	H	T	N	N				
Checksum(16bits)							Urgent Pointer(16bits)						
Options and Padding													

CWR : 송신자가 자신의 Window Size를 줄임 PSH : 수신측은 버퍼의 데이터를 즉시

ECE : 혼잡 감지 시 ECE 플래그 설정 후 어플리케이션 계층에 전송

송신자에게 알림

RST : 강제 세션 종료

URG : Urgent Pointer 사용

SYN : 세션 시작

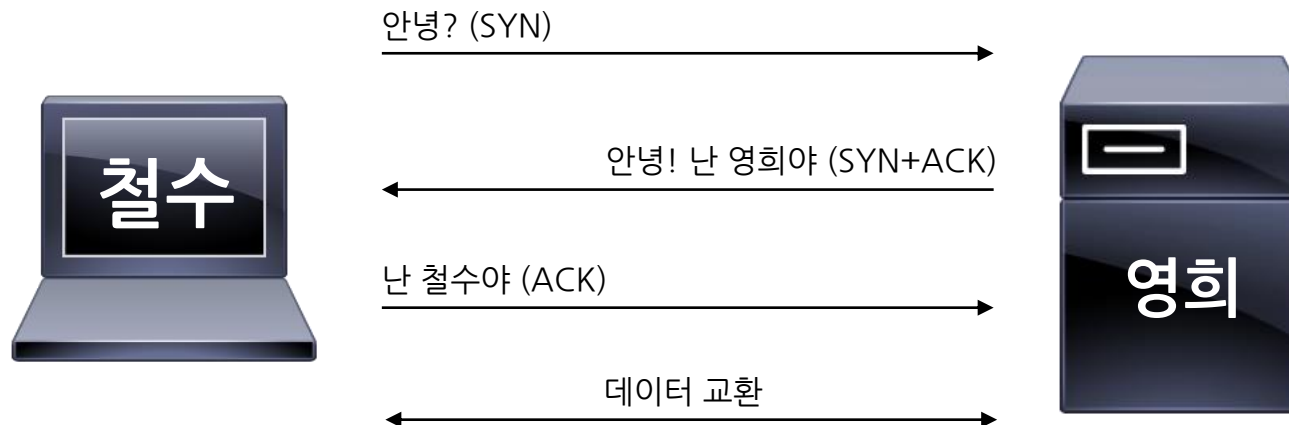
ACK : SYN에 대한 확인

FIN : 세션 종료

3 Network Scanning - TCP

• TCP 세션 연결(3 Way-Handshake)

- 처음 만난 철수(클라이언트)와 영희(서버)가 나누는 인사로 비교할 수 있다.
- 이 과정을 거쳐 두 사람은 악수(세션 형성)를 통해 친구(패킷 전송)가 된다.

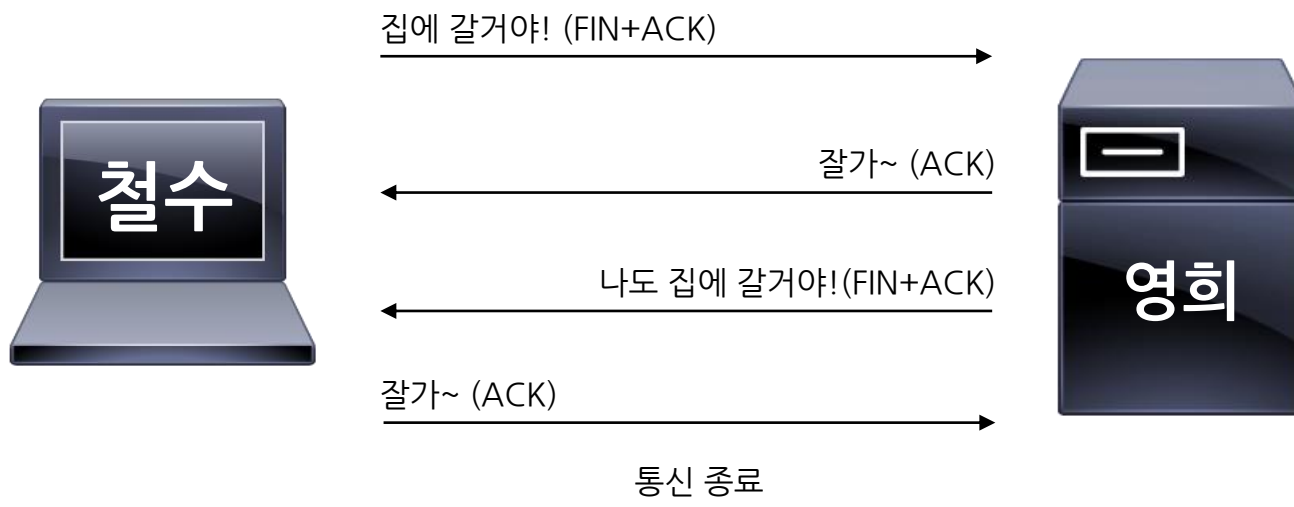


Source	Destination	Protocol	Length	Info
192.168.0.2	147.46.10.58	TCP	66	2265 → 80 [SYN] Seq=0 win=8192 Len=0 M
147.46.10.58	192.168.0.2	TCP	66	80 → 2265 [SYN, ACK] Seq=0 Ack=1 win=5
192.168.0.2	147.46.10.58	TCP	54	2265 → 80 [ACK] Seq=1 Ack=1 win=65700

3 Network Scanning - TCP

- TCP 세션 해제

- 대화(데이터 교환)가 끝난 철수(클라이언트)와 영희(서버)가 작별인사를 하는 과정에 비교할 수 있다.
- 이 과정을 거쳐 두 사람은 작별인사(세션 종료)를 하고 헤어진다.



Source	Destination	Protocol	Length	Info
218.159.68.104	192.168.0.2	TCP	60	8000 → 2637 [FIN, ACK] Seq=280 Ack=533 win=6912 Len=0
192.168.0.2	218.159.68.104	TCP	54	2637 → 8000 [ACK] Seq=533 Ack=281 win=65960 Len=0
192.168.0.2	218.159.68.104	TCP	54	2637 → 8000 [FIN, ACK] Seq=533 Ack=281 win=65960 Len=0
218.159.68.104	192.168.0.2	TCP	60	8000 → 2637 [ACK] Seq=281 Ack=534 win=6912 Len=0

3 Network Scanning - TCP

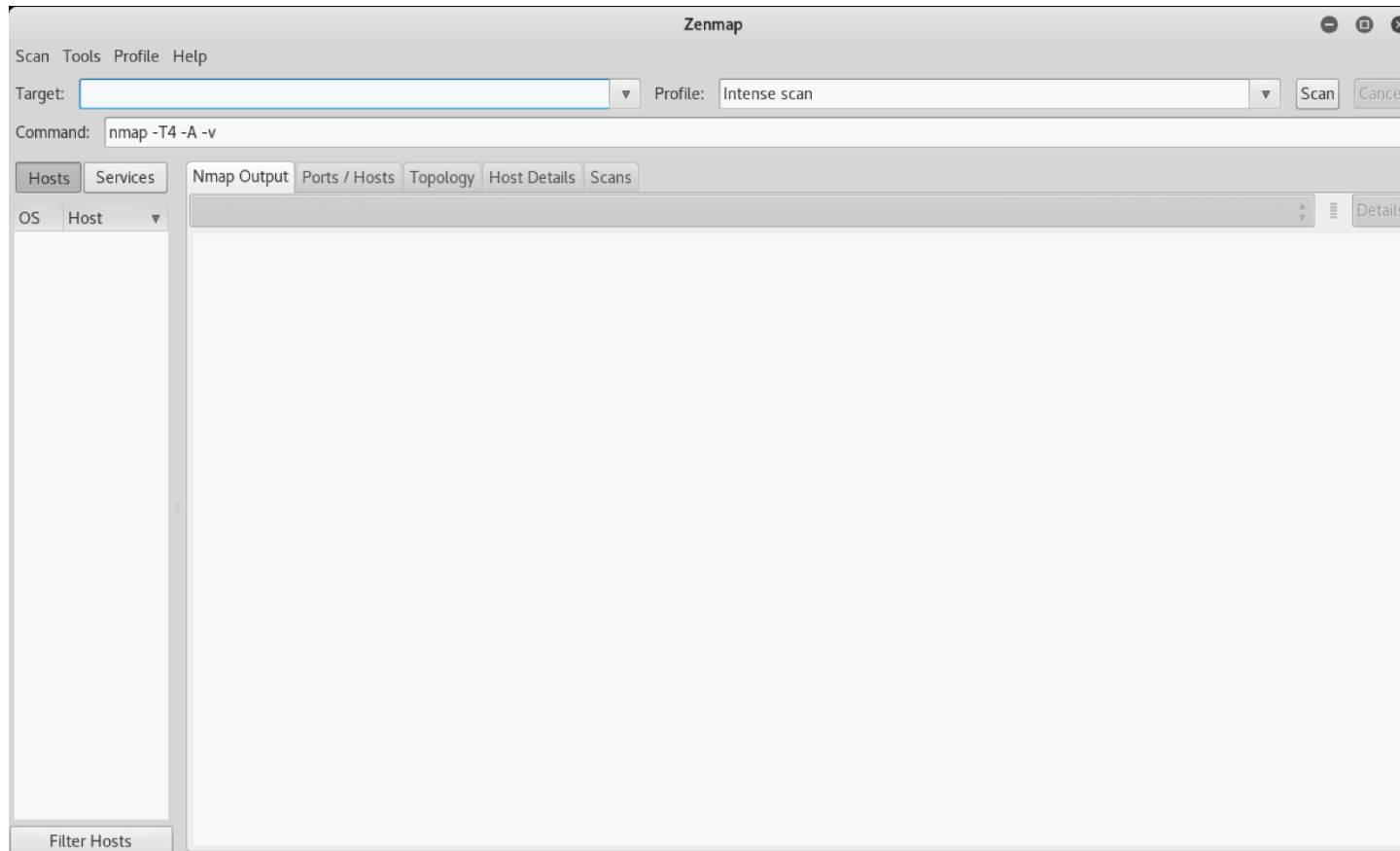
- Port Scanning 기법에는 정상적인 세션을 맺어 스캔하는 TCP 스캔부터 서버의 탐지를 우회하기 위한 Stealth 스캔 등 다양한 종류의 기법이 있다.

1. TCP (Connect) Scan
2. SYN Scan
3. FIN Scan
4. X-mas Scan
5. Null Scan

※ 현재는 Stealth 스캔 방법이 오히려 더 탐지하기 쉽다.

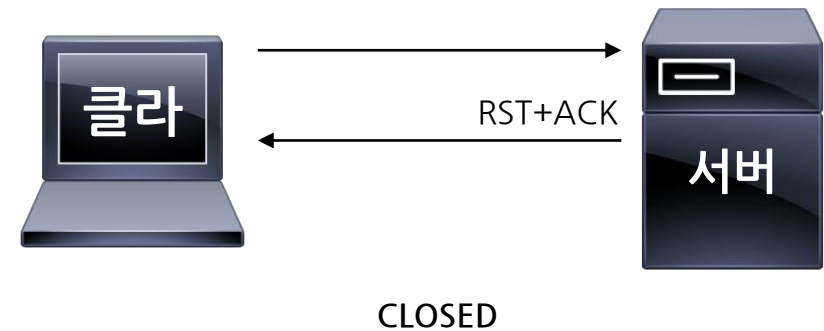
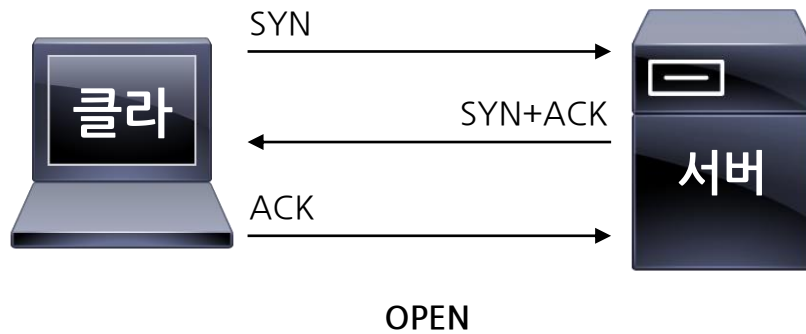
3 Network Scanning - TCP

- Nmap - 대표적인 Network Scanning 도구
- Zenmap은 Nmap의 GUI



3 Network Scanning - TCP (Connect) Scan

- 3 Way-Handshake으로 세션을 맺은 후 스캔을 하기 때문에 서버에 로그가 남는다. 닫힌 경우 RST, ACK 응답을 받는다.



3 Network Scanning - TCP (Connect) Scan

nmap -sT [IP Address]

```
nmap -sT 192.168.56.2
```

PORT	STATE	SERVICE
80/tcp	open	http

OPEN

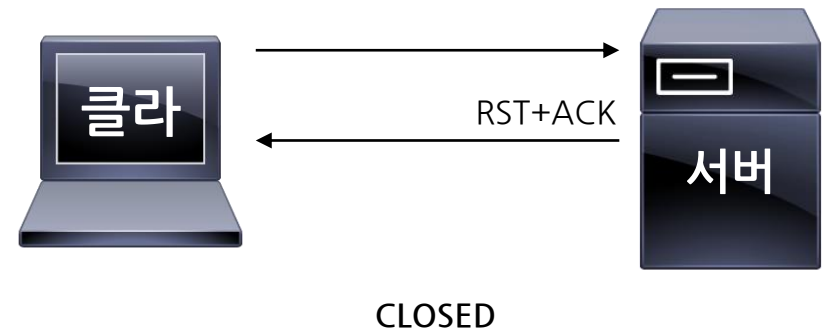
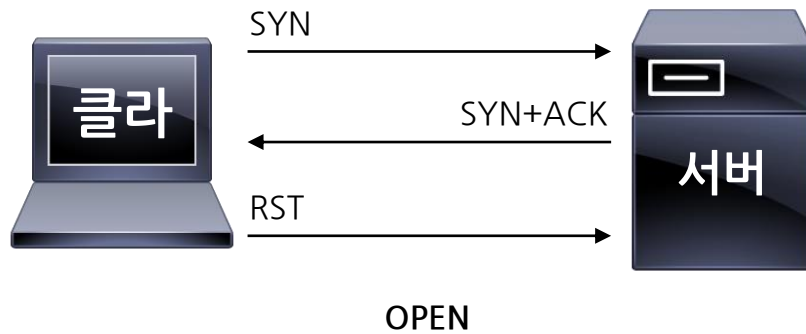
Source	Destination	Protocol	Length	Info
192.168.56.101	192.168.56.2	TCP	74	37748 → 80 [SYN] Seq=0
192.168.56.2	192.168.56.101	TCP	74	80 → 37748 [SYN, ACK] S
192.168.56.101	192.168.56.2	TCP	66	37748 → 80 [ACK] Seq=1

CLOSED

Source	Destination	Protocol	Length	Info
192.168.56.101	192.168.56.2	TCP	74	56258 → 8888 [SYN] Seq=
192.168.56.2	192.168.56.101	TCP	60	8888 → 56258 [RST, ACK]

3 Network Scanning - SYN Scan

- 3 Way-Handshake 과정 중 처음의 SYN 패킷만 전송해 열린 포트를 확인하고 RST 패킷으로 연결을 종료하기 때문에 로그를 남기지 않는다.
달한 경우 RST, ACK 응답을 받는다. Half-Open 스캔으로 부르기도 한다.



3 Network Scanning - SYN Scan

nmap -sS [IP Address]

```
nmap -sT 192.168.56.2
```

PORT	STATE	SERVICE
80/tcp	open	http

OPEN

Source	Destination	Protocol	Length	Info
192.168.56.101	192.168.56.2	TCP	58	51378 → 80 [SYN] Seq=
192.168.56.2	192.168.56.101	TCP	60	80 → 51378 [SYN, ACK]
192.168.56.101	192.168.56.2	TCP	54	51378 → 80 [RST] Seq=

CLOSED

Source	Destination	Protocol	Length	Info
192.168.56.101	192.168.56.2	TCP	58	51378 → 8888 [SYN] Seq=
192.168.56.2	192.168.56.101	TCP	60	8888 → 51378 [RST, ACK]

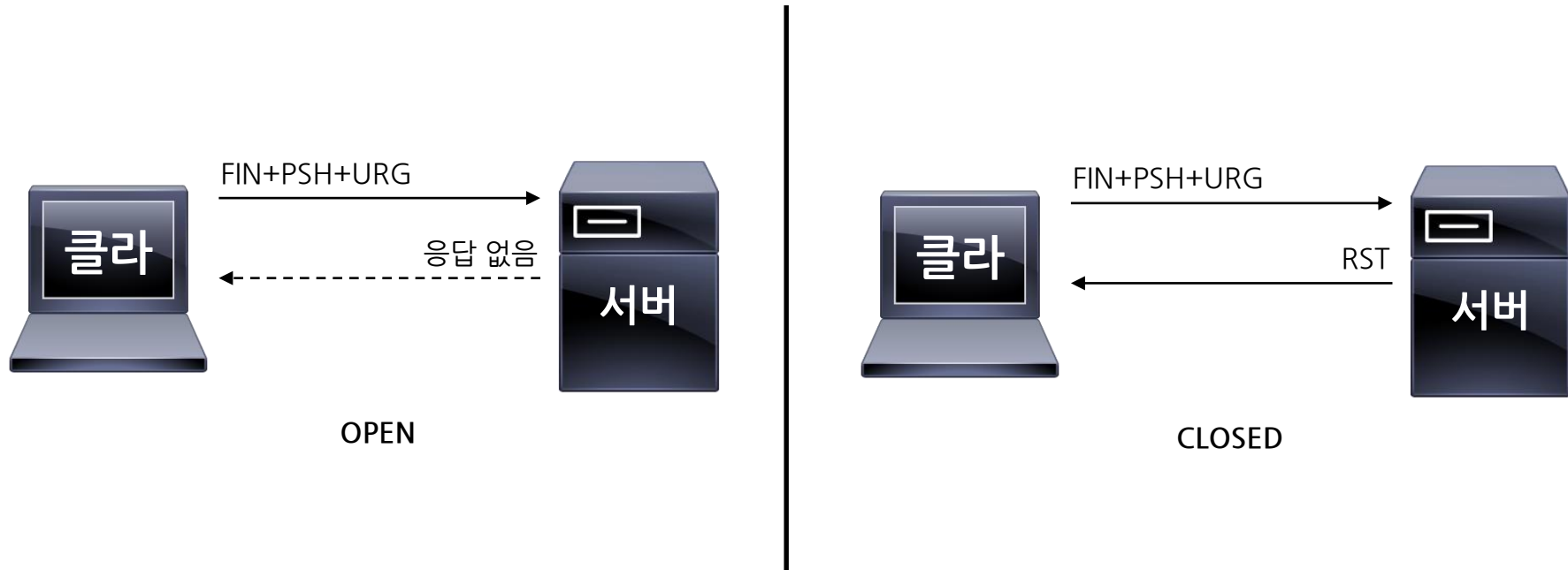
3 Network Scanning - FIN Scan

- 공격자는 TCP 패킷의 FIN 플래그를 설정한 패킷을 전송 해 열린 포트를 확인한다. 포트가 열려있는 경우 아무 응답이 오지 않는다.
닫힌 경우 RST 응답을 받는다.



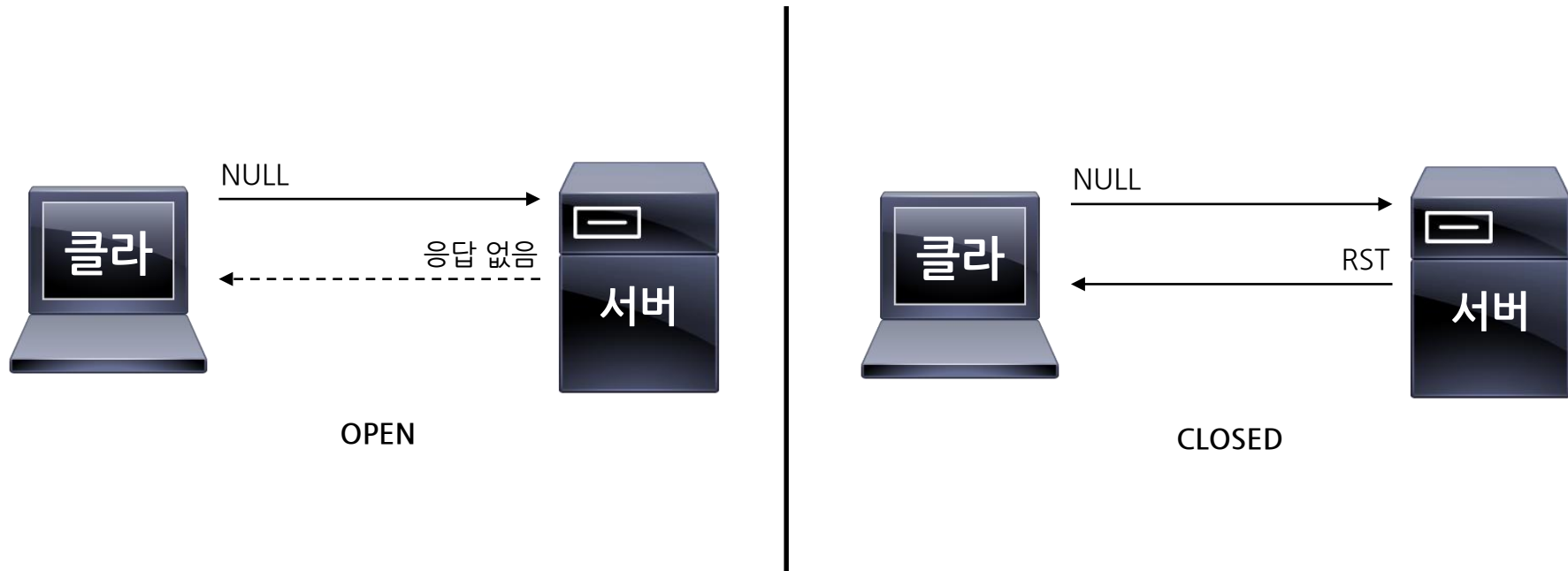
3 Network Scanning - X-mas Scan

- 공격자는 FIN, PSH, URG 패킷을 전송 해 열린 포트를 확인한다.
포트가 열려있는 경우 아무 응답이 오지 않는다. 닫힌 경우 RST 응답을 받는다.



3 Network Scanning - NULL Scan

- 공격자는 TCP 패킷의 아무 플래그도 설정하지 않은 Null 패킷을 전송해 열린 포트를 확인한다. 포트가 열려있는 경우 아무 응답이 오지 않는다. 닫힌 경우 RST 응답을 받는다.



3 Network Scanning - UDP

- UDP는 “비연결” 지향형 프로토콜로서 단순 오류 검출 기능만을 가지고 있다.
따라서 TCP보다 패킷 구조가 단순하고 오버헤드가 적다.
DNS와 같은 소량의 데이터 전송 시 이용한다.

Source Port(16bits)	Destination Port(16bits)
Total Length(16bits)	Checksum(16bits)

Source Port : 패킷을 송신하는 출발지의 포트번호

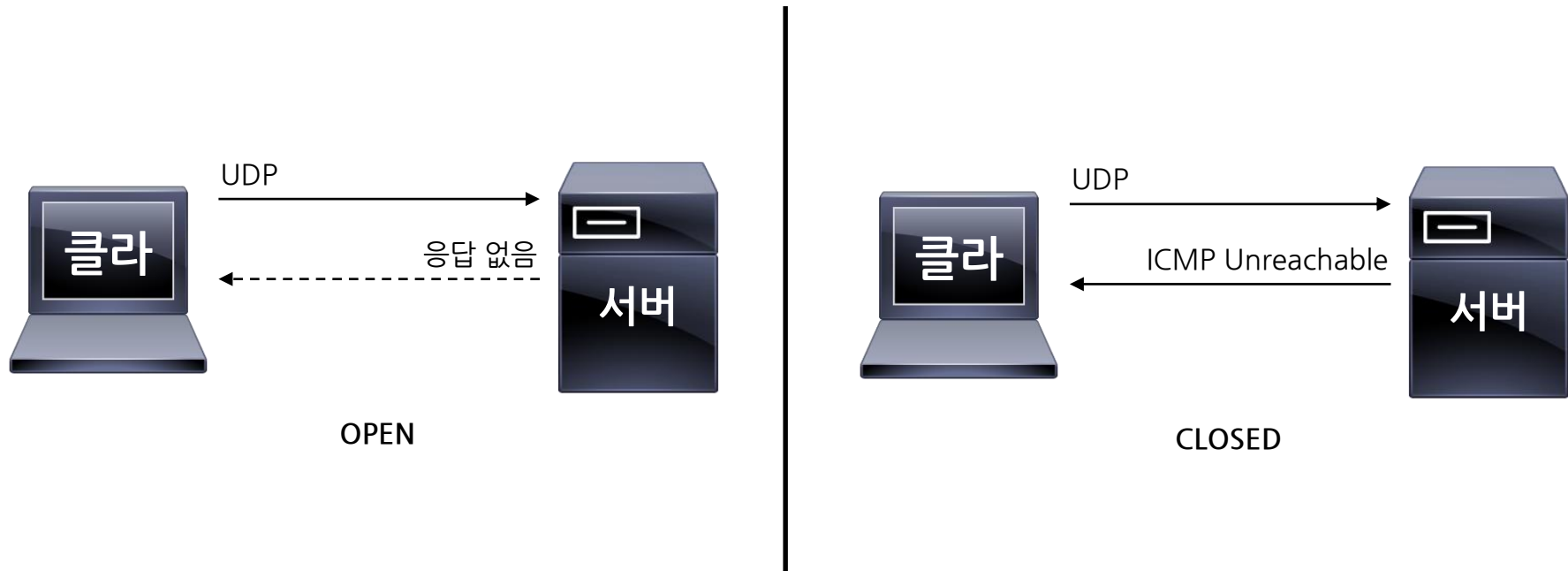
Destination Port : 패킷을 수신할 도착지의 포트번호

Total Length : UDP 헤더와 데이터를 포함한 전체 길이

Checksum : 데이터가 전송 중 손상되지 않았는지 검사

3 Network Scanning - UDP SCAN

- 공격자는 UDP 패킷을 전송 해 열린 포트를 확인한다.
포트가 열려있는 경우 아무 응답이 오지 않는다.
닫힌 경우 ICMP Unreachable 응답을 받는다.



Q & A