

# 정보보호와 시스템 보안

## 3. 네트워크 보안 개요

전은아

# 목차

1. 네트워크에 대한 이해
2. 서비스 거부(Dos) 공격
3. 스니핑 공격
4. 스푸핑 공격
5. 세션 하이재킹 공격
6. 무선 네트워크 공격과 보안

# 학습목표

- OSI 7 계층의 세부 동작을 이해한다.
- 네트워크와 관련된 해킹 기술의 종류와 방법을 살펴본다.
- 네트워크 해킹을 막기 위한 대응책을 알아본다.

# 01 네트워크에 대한 이해

## ■ OSI 7계층

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



[그림 1] OSI 7계층

# 01 네트워크에 대한 이해

## ■ 물리 계층(1계층)

- 인터넷 이용시의 랜 케이블, 전화선, 동축 케이블 또는 광 케이블 등의 시스템간의 물리적인 연결매체

[표 1] CAT별 특성

구분	최대 속도	용도
CAT 1	1Mbps 미만	<ul style="list-style-type: none"><li>• 아날로그 음성(일반적인 전화 서비스)</li><li>• ISDN 기본률 접속(Basic Rate Interface)</li><li>• Doorbell Wiring</li></ul>
CAT 2	4Mbps	<ul style="list-style-type: none"><li>• 주로 IBM의 토큰링 네트워크에 사용된다.</li></ul>
CAT 3	16Mbps	<ul style="list-style-type: none"><li>• 10BASE-T 이더넷상의 데이터 및 음성</li></ul>
CAT 4	20Mbps	<ul style="list-style-type: none"><li>• 16Mbps 토큰 링에서 사용. 많이 사용되지는 않는다.</li></ul>
CAT 5	100Mbps	<ul style="list-style-type: none"><li>• 옥내 수평 및 간선 배선망(100MHz)</li><li>• 4/16Mbps 토큰 링(IEEE 802.5)</li><li>• 10/100 BASE-T(IEEE 802.3)</li><li>• 155Mbps ATM</li></ul>
CAT 6	250Mbps	<ul style="list-style-type: none"><li>• 옥내 수평 및 간선 배선망(250MHz)</li><li>• 4/16Mbps 토큰 링(IEEE 802.5)</li><li>• 10/100/1000 BASE-T(IEEE 802.3)</li><li>• 155/622Mbps ATM</li><li>• Gb 이더넷</li></ul>
CAT 7	10Gbps	<ul style="list-style-type: none"><li>• 10Gb 이더넷</li></ul>

# 01 네트워크에 대한 이해

## ■ 물리 계층(1계층)

[표 2] 케이블 선의 분류

구분	내용
UTP(Unshielded Twisted Pair)	제품 전선과 피복만으로 구성되어 있으며, 두 선 사이의 전자기 유도를 줄이기 위해 절연의 구리선이 서로 꼬여 있다.
FTP(Foil Screened Twisted Pair Cable)	알루미늄 은박이 4가닥의 선을 감싸고 있다. UTP보다 절연 기능이 탁월해 공장 배선용으로 많이 사용된다.
STP(Shielded Twisted Pair Cable)	연선으로 된 전선 겉에 외부 피복 또는 차폐재가 추가된 케이블(섀드 처리)이다. 이때 차폐재는 접지의 역할을 하므로 외부의 노이즈를 차단하거나 전기적 신호의 간섭에 탁월하다.

- 일반적으로 인터넷에 쓰는 랜 케이블은 UTP 케이블 중 CAT 5 또는 CAT 6에 해당되는 10/100/1000 BASE-T(IEEE 802.3) 선에 RJ 45 커넥터를 사용.

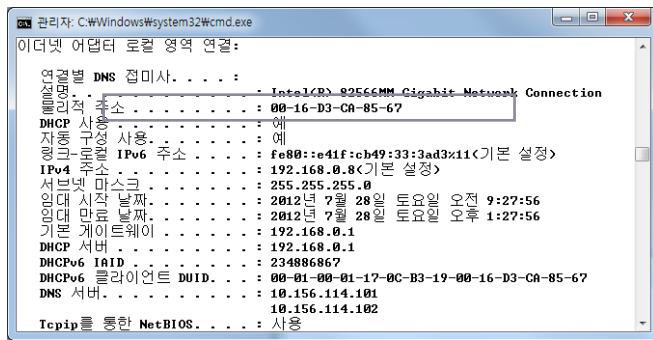


[그림 2] RJ 45 커넥터

# 01 네트워크에 대한 이해

## ■ 데이터 링크 계층(2계층)

- 2계층인 데이터 링크 계층은 두 포인트(Point to Point) 간 신뢰성 있는 전송을 보장하기 위한 계층.
- 상호 통신을 위해 MAC 주소를 할당받는데, MAC 주소는 ipconfig /all 명령을 실행해 확인할 수 있음.



[그림 3] MAC 주소의 확인

- MAC 주소는 총 12개의 16진수 숫자로 구성.
  - 앞쪽 6개의 16진수는 네트워크 카드를 만든 회사를 나타내는 것으로 OUI(Organizational Unique Identifier)라고 함.
  - 뒤쪽 6개의 16진수는 각 회사에서 임의로 붙이는 일종의 시리얼을 나타내는 것으로 Host Identifier라고 함.

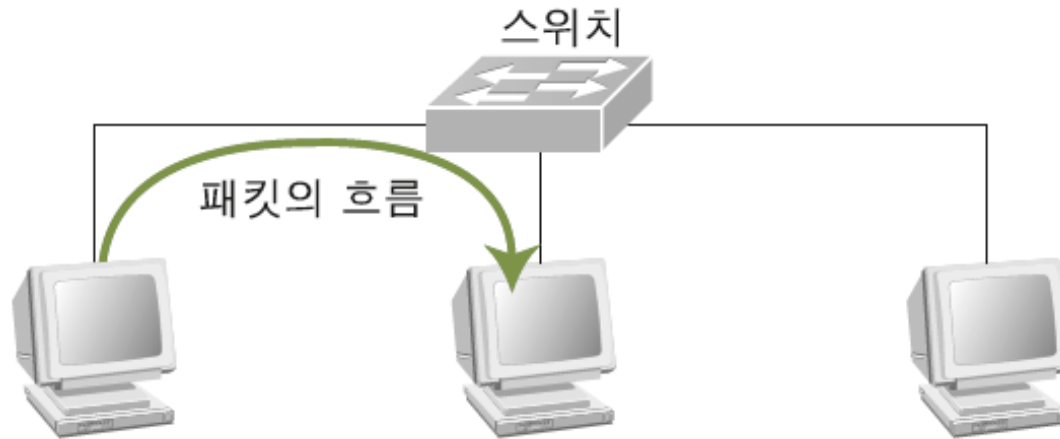


[그림 4] MAC 주소의 형태

# 01 네트워크에 대한 이해

## ■ 데이터 링크 계층(2계층)

- 1계층과 2계층만을 사용하는 네트워크 통신



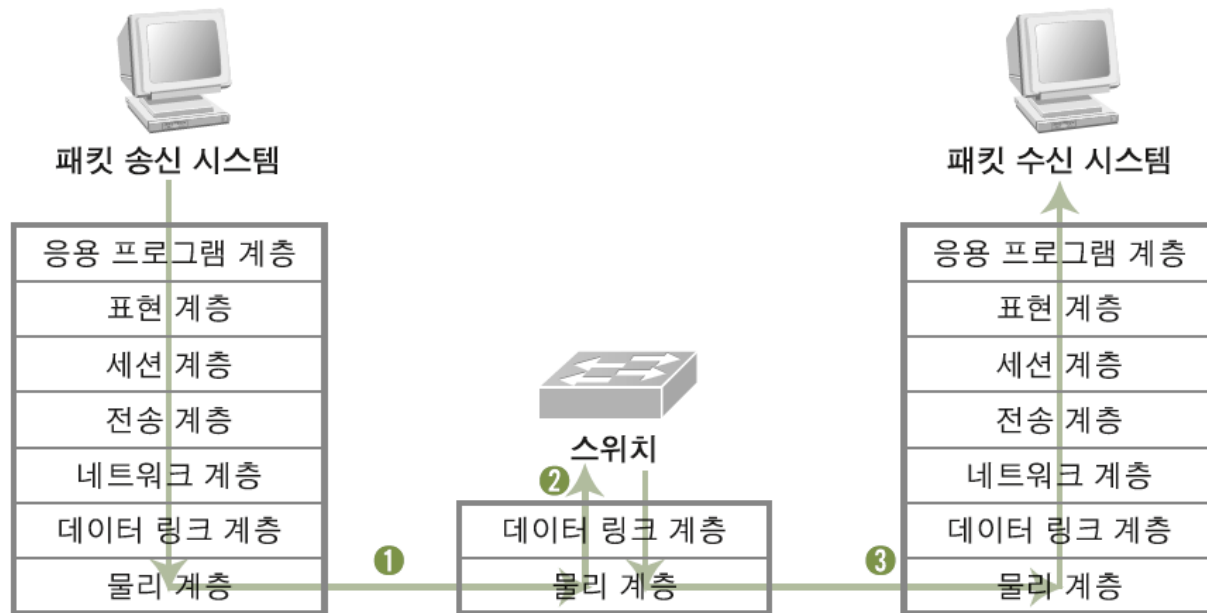
[그림 5] 2계층에서 패킷의 흐름



# 01 네트워크에 대한 이해

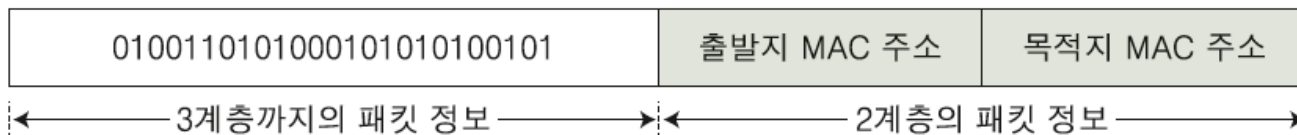
## ■ 데이터 링크 계층(2계층)

- 패킷의 흐름을 다시 OSI 7계층에 따른 패킷의 흐름으로 나타내 보자.



[그림 6] 2계층에서의 OSI 계층의 패킷 흐름

- ①, ②, ③ 각 단계에서 흘러가는 패킷은 다음과 같은 구조를 갖는다.



# 01 네트워크에 대한 이해

## ■ 데이터 링크 계층(2계층)

- 스위치의 동작 원리
  - 스위치에 안방 컴퓨터만이 연결되어 있을 경우

1번 포트	
2번 포트	안방 컴퓨터의 MAC 주소
3번 포트	
4번 포트	

- 스위치에 작은방의 컴퓨터를 연결할 경우

1번 포트	
2번 포트	안방 컴퓨터의 MAC 주소
3번 포트	작은방 컴퓨터의 MAC 주소
4번 포트	

- 일반적으로 잘못 이해할 수 있는 스위치의 메모리 구조

1번 포트	
192.168.0.100	안방 컴퓨터의 MAC 주소
192.168.0.101	작은방 컴퓨터의 MAC 주소
4번 포트	

# 01 네트워크에 대한 이해

## ■ 네트워크 계층(3계층)

- 3계층인 네트워크 계층은 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층.
- 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.

```
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
```

[그림 7] ipconfig/all 명령을 실행한 결과

# 01 네트워크에 대한 이해

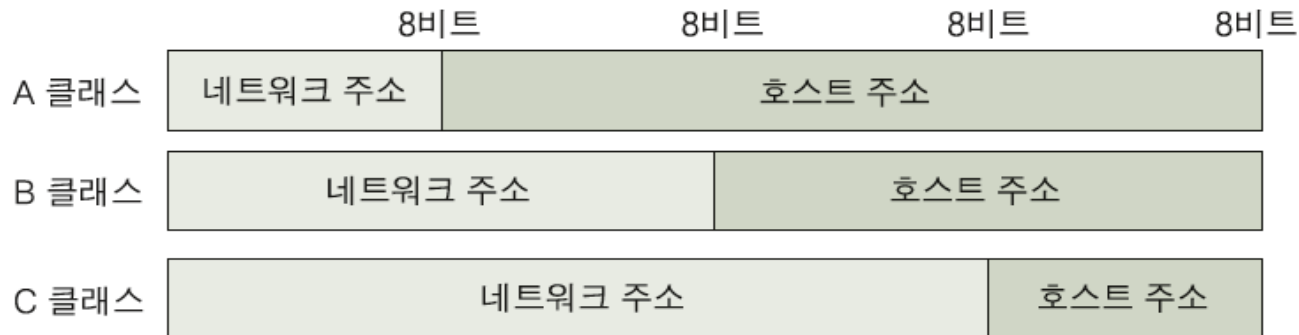
## ■ 네트워크 계층(3계층)

- IP주소는 8비트의 수 4개로 구성 (32 자리의 2 진수로 8 자리마다 점을 찍어 구분)

11000000 . 10101000 . 00000000 . 00001000

- IP주소는 A,B,C,D,E 클래스로 구분

- A 클래스 : 첫 번째 자리가 네트워크 주소, 나머지 세 자리가 호스트 주소
- B 클래스 : 두 번째 자리까지가 네트워크 주소, 나머지 두 자리가 호스트 주소
- C 클래스 : 세 번째 자리까지가 네트워크 주소, 나머지 한 자리가 호스트 주소



[그림 8] IP 주소 클래스

# 01 네트워크에 대한 이해

## ■ 네트워크 계층(3계층)

[표 3] 네트워크 클래스의 구분

시작 주소	구분	내용
0	A 클래스	<ul style="list-style-type: none"><li>• 00000000번부터 01111111(127)번까지의 네트워크이다.</li><li>• A 클래스는 모두 2<sup>8</sup> (128)개가 가능하고, 하나의 A 클래스 안에 256<sup>3</sup>(16,777,216)개의 호스트가 존재할 수 있다.</li></ul>
10	B 클래스	<ul style="list-style-type: none"><li>• 10000000(128)번부터 10111111(191)번까지의 네트워크이다.</li><li>• B 클래스는 2<sup>16</sup> * 256(16,384)개가 가능하고, 하나의 B 클래스 안에 256<sup>2</sup>(66,536)개의 호스트가 존재할 수 있다.</li></ul>
110	C 클래스	<ul style="list-style-type: none"><li>• 11000000(192)번부터 11011111(223)번까지의 네트워크이다.</li><li>• C 클래스는 2<sup>24</sup> * 256<sup>2</sup>(2,097,152)개가 가능하고, 하나의 B 클래스 안에 256개의 호스트가 존재할 수 있다.</li></ul>
1110	D 클래스	<ul style="list-style-type: none"><li>• 11100000(224)번부터 11101111(239)번까지의 네트워크이다.</li><li>• 멀티미디어 방송을 할 때 자동으로 부여된다.</li></ul>
E 클래스		<ul style="list-style-type: none"><li>• 11110000(240)번부터 11111111(255)번까지의 네트워크이다.</li><li>• 테스트를 위한 주소 대역으로, 사용하지 않는다.</li></ul>

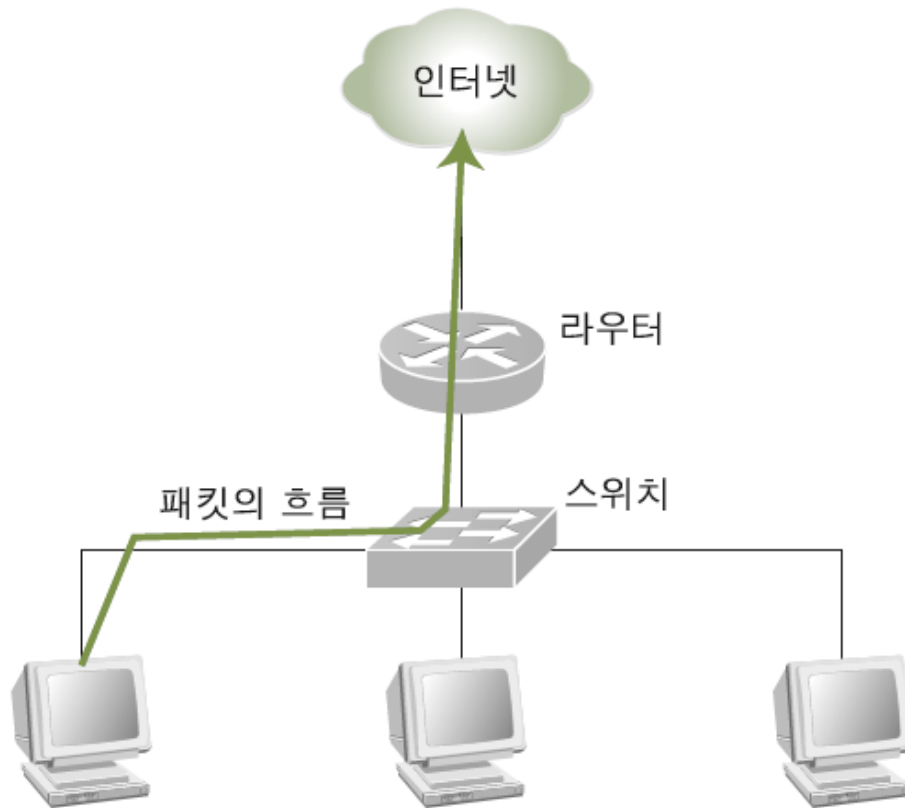
[표 4] 클래스별 네트워크 범위

구분	지정된 사설 네트워크
A 클래스	10.0.0.0 ~ 10.255.255.255
B 클래스	172.16.0.0 ~ 172.31.255.255
C 클래스	192.168.0.0 ~ 192.168.255.255

# 01 네트워크에 대한 이해

## ■ 네트워크 계층(3계층)

- 2, 3계층에서의 패킷의 흐름

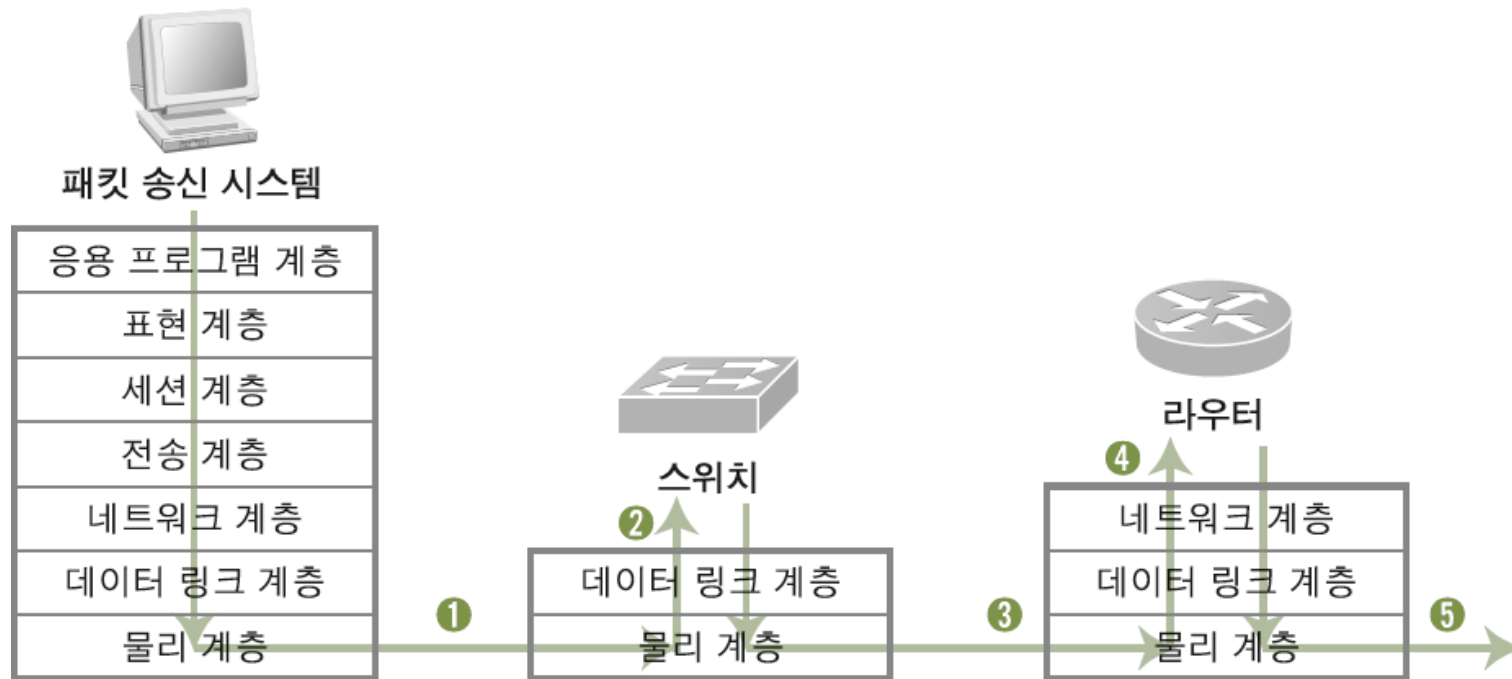


[그림 9] 2계층 및 3계층에서의 패킷의 흐름

# 01 네트워크에 대한 이해

## ■ 네트워크 계층(3계층)

- 패킷의 흐름을 OSI 7계층에서 살펴보자.



[그림 10] 2계층 및 3계층에서의 OSI 레벨의 패킷 흐름

# 01 네트워크에 대한 이해

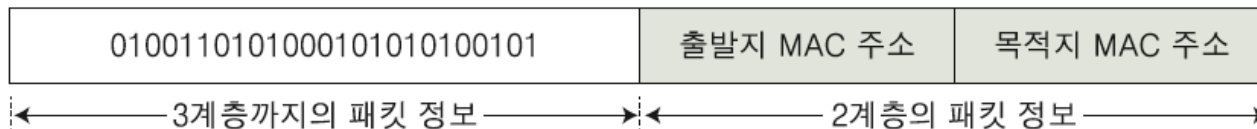
## ■ 네트워크 계층(3계층)

- 네트워크 계층에서의 패킷 전달 구조
  - 2, 3계층 에서의 패킷의 흐름 예

- 패킷 송신 시스템의 IP : 172.16.0.100
- 라우터의 랜쪽 포트의 IP(게이트웨이) : 172.16.0.1
- 패킷 송신 시스템의 MAC 주소 : AA-AA
- 라우터의 랜쪽 포트의 MAC 주소(게이트웨이) : BB-BB
- 라우터의 인터넷쪽 포트의 MAC 주소 : CC-CC
- 스위치의 메모리에 존재하는 MAC 주소 테이블

1번 포트	BB-BB(라우터 케이블 연결 포트)
2번 포트	AA-AA(컴퓨터 연결 포트)
3번 포트	
4번 포트	

- 인터넷에 전송하는 패킷의 기본 구조

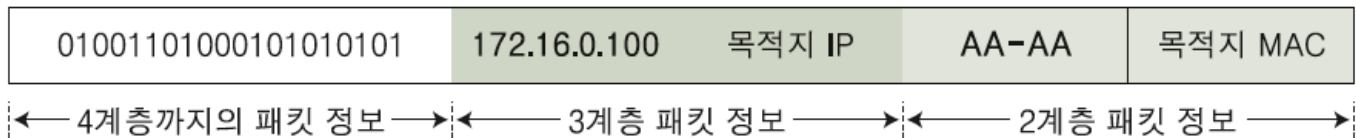




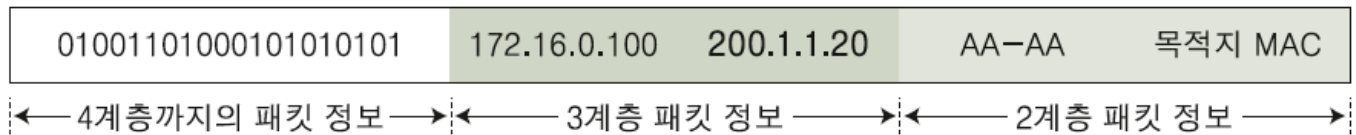
# 01 네트워크에 대한 이해

## ■ 네트워크 계층(3계층)

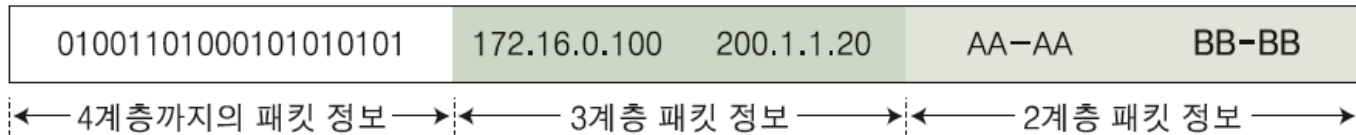
- 네트워크 계층에서의 패킷 전달 구조
  - 출발지의 IP와 MAC 주소가 기록됨.



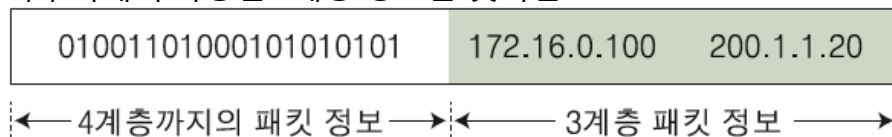
- 목적지 IP 주소 입력



- 목적지 MAC 주소에는 랜을 벗어나기 위한 가장 일차적인 목적지, 즉 게이트웨이의 MAC 주소 입력 (ARP 프로토콜 이용)



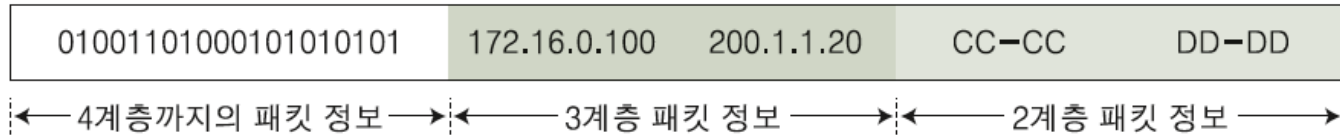
- 라우터에서 사용한 2계층 정보를 벗겨냄.



# 01 네트워크에 대한 이해

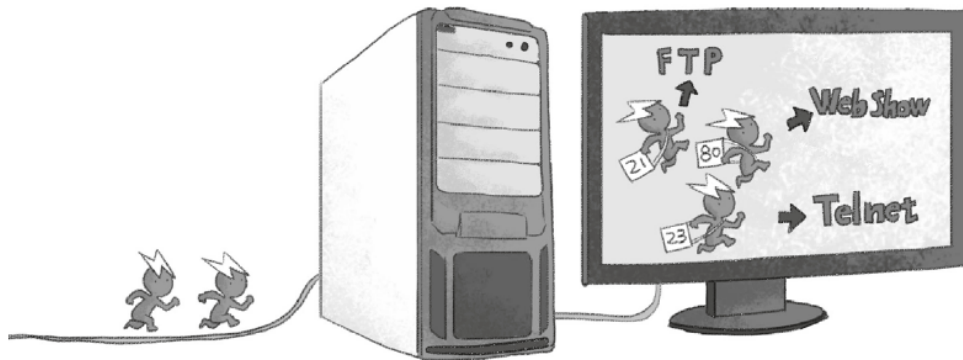
## ■ 네트워크 계층(3계층)

- 네트워크 계층에서의 패킷 전달 구조
  - 다음 라우터까지의 2계층 정보를 패킷에 덧씌움.



## ■ 전송 계층(4계층)

- 4계층인 전송 계층은 양 끝단(End to end)의 사용자들이 신뢰성 있는 데이터를 주고받을 수 있도록 함으로써, 상위 계층들이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않도록 해줌.
- 가장 잘 알려진 전송 프로토콜은 TCP(Transmission Control Protocol)
- MAC 주소가 네트워크 카드의 고유 식별자이고 IP가 시스템의 주소라면, 포트는 시스템에 도착한 후 패킷이 찾아갈 응용 프로그램과 통하는 통로 번호라 생각할 수 있음.



[그림 11] 포트의 개념

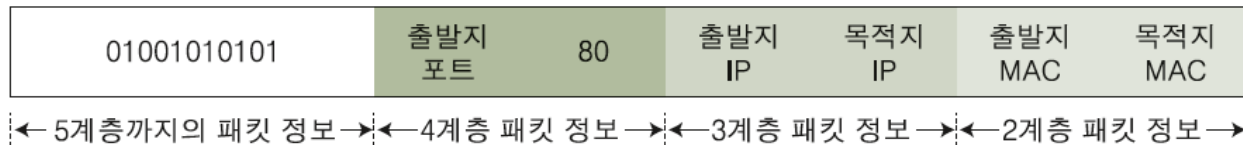
# 01 네트워크에 대한 이해

## ■ 전송 계층(4계층)

- 시스템에서 구동되는 응용 프로그램들은 네트워킹을 하기 위해 자신에게 해당되는 패킷을 식별할 필요가 있음.
  - 이때 사용하는 것이 포트이며, 포트는 0번부터 65,535( $2^{16}$ )번까지 존재함.
  - 4계층까지 생각한 패킷의 구조



- 출발지 포트는 운영체제나 응용 프로그램마다 조금씩 다르나 보통 1,025번부터 65,535번 사이의 포트 중에서 사용하지 않는 임의의 포트를 응용 프로그램별로 할당하여 사용, 웹 서버의 서비스 포트는 보통 80번이니 패킷의 구조가 다음과 같음.



- 출발지 포트는 시스템에서 임의로 정해짐. 3,000번 대의 임의의 포트가 할당되면 다음과 같을 수 있음.



# 01 네트워크에 대한 이해

## ■ 전송 계층(4계층)

이런 기본적인 포트번호와 서비스는 꼭 알고있어야함(시험문제)

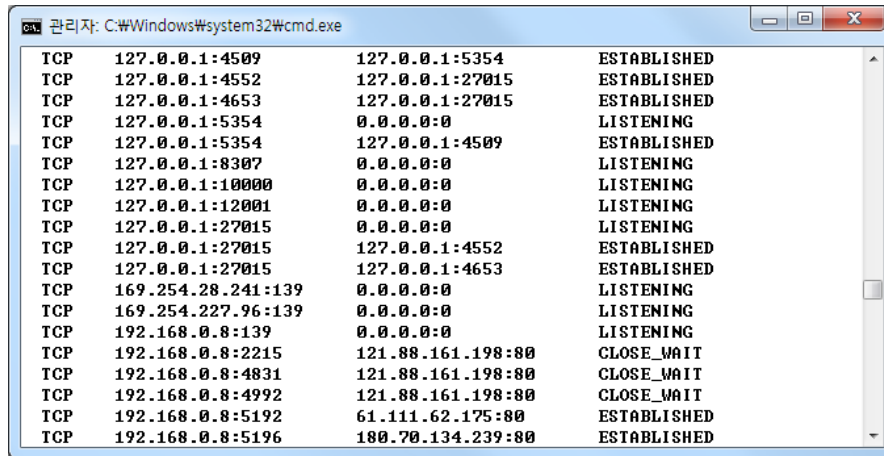
[표 5] 주요 포트와 서비스

포트 번호	서비스	설명
20	FTP	<ul style="list-style-type: none"><li>• File Transfer Protocol-Datagram</li><li>• FTP 연결 시 실제로 데이터를 전송한다.</li></ul>
21	FTP	<ul style="list-style-type: none"><li>• File Transfer Protocol-Control</li><li>• FTP 연결 시 인증과 제어를 한다.</li></ul>
23	Telnet	<ul style="list-style-type: none"><li>• 텔넷 서비스로, 원격지 서버의 실행창을 얻어낸다. 요샌거의안씀 보안상의문제로 (막아놓음거의)</li></ul>
25	SMTP	<ul style="list-style-type: none"><li>• Simple Message Transfer Protocol</li><li>• 메일을 보낼 때 사용한다.</li></ul>
53	DNS	<ul style="list-style-type: none"><li>• Domain Name Service</li><li>• 이름을 해석하는 데 사용한다.</li></ul>
69	TFTP	<ul style="list-style-type: none"><li>• Trivial File Transfer Protocol</li><li>• 인증이 존재하지 않는 단순한 파일 전송에 사용한다.</li></ul>
80	HTTP	<ul style="list-style-type: none"><li>• Hyper Text Transfer Protocol</li><li>• 웹 서비스를 제공한다.</li></ul>
110	POP3	<ul style="list-style-type: none"><li>• Post Office Protocol</li><li>• 메일 서버로 전송된 메일을 읽을 때 사용한다.</li></ul>
111	RPC	<ul style="list-style-type: none"><li>• Sun의 Remote Procedure Call</li><li>• 원격에서 서버의 프로세스를 실행할 수 있게 한다.</li></ul>
138	NetBIOS	<ul style="list-style-type: none"><li>• Network Basic Input Output Service</li><li>• 윈도우에서 파일을 공유할 수 있게 한다.</li></ul>
143	IMAP	<ul style="list-style-type: none"><li>• Internet Message Access Protocol</li><li>• POP3와 기본적으로 같으나, 메일이 확인된 후에도 서버에 남는다는 것이 다르다.</li></ul>
161	SNMP	<ul style="list-style-type: none"><li>• Simple Network Management Protocol</li><li>• 네트워크 관리와 모니터링을 위해 사용한다.</li></ul>

# 01 네트워크에 대한 이해

## ■ 전송 계층(4계층)

- 3계층과 4계층의 정보는 netstat -an 명령으로 쉽게 확인할 수 있음.



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

[그림 12] netstat -an 명령을 실행한 결과

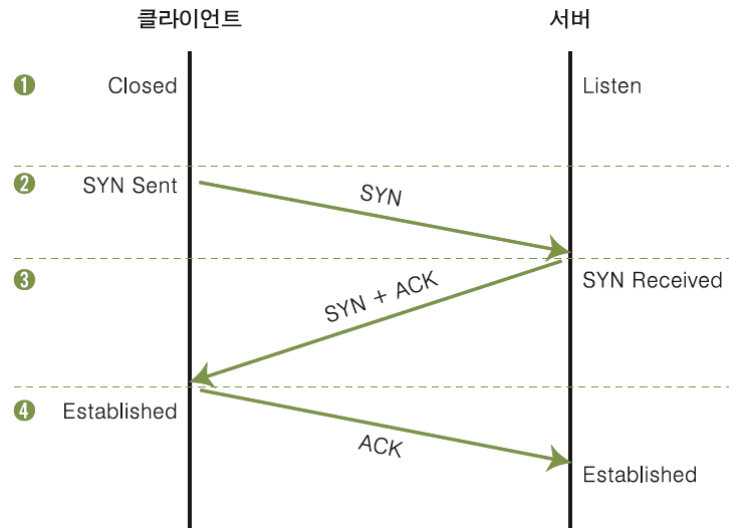
- netstat -an 명령을 실행한 결과는 각각 다음의 정보를 담고 있다.

TCP	172.168.10.93	:7780	61.97.70.9	:80	ESTABLISHED
4계층 프로토콜의 종류	클라이언트(PC)의 IP 주소	웹 브라우저가 사용하는 포트 번호	서버의 IP 주소	웹 서버가 사용하는 포트 번호	연결 상태

# 01 네트워크에 대한 이해

## ■ 전송 계층(4계층)

- '3웨이 핸드셰이킹(way handshaking)'



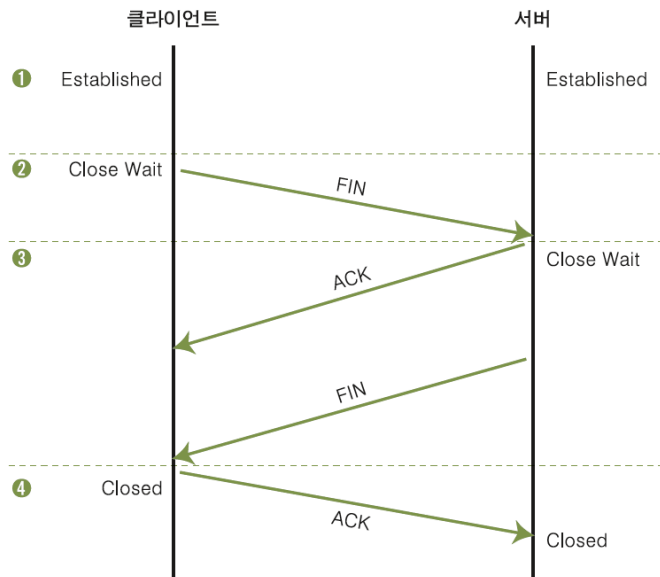
[그림 13] TCP에서 연결 설정 과정

- ① 단계 : 두 시스템이 통신을 하기 전에, 클라이언트는 포트가 닫힌 Closed 상태, 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태
- ② 단계 : 처음 클라이언트가 통신을 하고자 하면, 임의의 포트 번호가 클라이언트 프로그램에 할당되고 클라이언트는 서버에 연결하고 싶다는 의사 표시로 SYN Sent 상태가 됨.
- ③ 단계 : 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 되고 클라이언트에게 연결을 해도 좋다는 의미로 SYN+ACK 패킷을 보냄.
- ④ 단계 : 마지막으로 클라이언트는 연결을 요청한 것에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버에 보냄.

# 01 네트워크에 대한 이해

## ■ 전송 계층(4계층)

### ■ TCP 세션의 종료



[그림 14] TCP에서 연결 해제 과정

- ① 단계 : 통신을 하는 중에는 클라이언트와 서버 모두 Established 상태
- ② 단계 : 통신을 끊고자 하는 클라이언트가 서버에 FIN 패킷을 보냄. 이때 클라이언트는 Close Wait 상태가 됨.
- ③ 단계 : 서버는 클라이언트의 연결 종료 요청을 확인하고 클라이언트에게 응답으로 ACK 패킷을 보냄. 서버도 클라이언트의 연결을 종료하겠다는 의미로 FIN 패킷을 보내고 Close Wait 상태가 됨.
- ④ 단계 : 마지막으로 클라이언트는 연결 종료를 요청한 것에 대한 서버의 응답을 확인했다는 의미로 ACK 패킷을 서버에 보냄.

# 01 네트워크에 대한 이해

## ■ 전송 계층(4계층)

- TCP와 UDP
  - **TCP** : 연결 지향형 프로토콜로서 수신측이 데이터를 흘려버리지 않게 데이터 흐름 제어(Flow Control)와 전송 중 에러가 발생할 경우 자동으로 재전송하는 에러 제어(Error Control) 등의 기능을 통해 데이터의 확실한 전송을 보장함. 하지만 완전하지는 않아 해커들에게 많은 공격을 받게 됨.
  - **UDP(User Datagram Protocol)** : TCP와는 달리 데이터의 신뢰성 있는 전송을 보장하지는 않음. 그러나 신뢰성이 매우 높은 회선을 사용하거나 데이터의 확실한 전송을 요구하지 않는 통신을 하거나 한 번에 많은 상대방에게 메시지를 전송하고자 하는 경우에는 전송 경로 확립을 위한 번잡함을 생략하고 시간을 절약할 수 있어 UDP가 더 효과적임.



# 01 네트워크에 대한 이해

## ■ 세션 계층(5계층)

- 5계층인 세션 계층은 양 끝단의 응용 프로세스가 통신을 관리하기 위한 방법을 제공
- 전송 계층이 종단간에 논리적인 설정을 담당한다면 세션 계층은 이런 연결에 정보 교환을 효과적으로 할 수 있게 추가 서비스를 함.

## ■ 표현 계층(6계층)

- 6계층인 표현 계층은 코드 간의 번역을 담당.
- 즉 사용자 시스템에서 데이터의 구조를 하나의 통일된 형식으로 표현함으로써, 응용 계층의 데이터 형식 차이로 인한 부담을 덜어줌.

## ■ 응용 프로그램 계층(7계층)

- 7계층인 응용 프로그램 계층은 사용자나 응용 프로그램 사이에 데이터의 교환이 가능하게 하는 계층
- 예를들어 HTTP, FTP, 터미널 서비스, 메일 프로그램, 디렉터리 서비스 등을 제공

## 02 서비스 거부(Dos) 공격

### ■ 일종의 웨방

한국인터넷진흥원



[그림 15] 포장마차에 행해지는 서비스 거부 공격

## 02 서비스 거부(Dos) 공격

### ■ 취약점 공격형

#### ■ Boink, Bonk, TearDrop 공격

- TCP의 신뢰성 있는 연결을 위한 기능
  - 패킷의 순서가 올바른지 확인
  - 중간에 손실된 패킷은 없는지 확인
  - 손실된 패킷의 재전송 요구
- 프로토콜은 이러한 사항이 확인되지 않는 데이터 전송에 대해 신뢰도를 확보하기 위해 반복적인 재요청과 수정을 함.
- Boink, Bonk, TearDrop은 모두 이러한 반복적인 재요청과 수정을 공격 대상이 계속하게 함으로써 시스템의 자원을 고갈시키는 공격임.
- TCP 패킷 안에는 각 패킷이 데이터의 어느 부분을 포함하고 있는지를 표시하기 위하여 시퀀스 번호가 기록되어 있는데, 이러한 공격들은 시스템의 패킷 재전송과 재조합(Reassembling)에 과부하가 걸리도록 이 시퀀스 번호를 속임.
- 시퀀스 번호가 조작된 패킷의 흐름은 공격 대상에게 절대로 풀 수 없는 퍼즐을 던져주는 것과 같음. 이러한 취약점은 패치를 통해서 제거되어 있음. 과부하가 걸리거나 계속 반복되는 패킷은 무시하고 버리도록 처리함.

## 02 서비스 거부(Dos) 공격

### ■ 취약점 공격형

- Boink, Bonk, TearDrop 공격

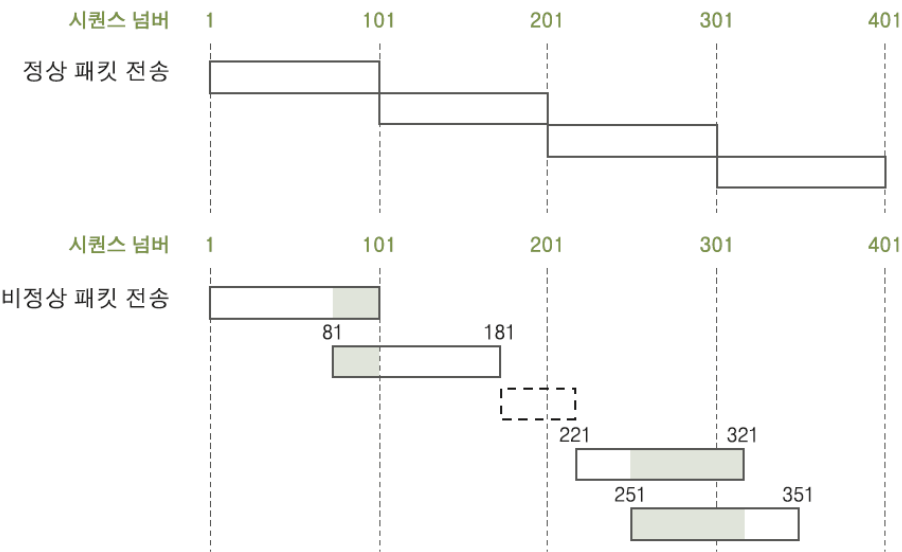


[그림 16] Bonk 공격

# 02 서비스 거부(Dos) 공격

## ■ 취약점 공격형

### ▪ Boink, Bonk, TearDrop 공격



[그림 17] TearDrop 공격 시 패킷의 배치

[표 6] TearDrop 공격 시 패킷의 시퀀스 번호

패킷 번호	정상 패킷의 시퀀스 번호	공격을 위한 패킷의 시퀀스 번호
1	1~101	1~101
2	101~201	81~181
3	201~301	221~321
4	301~401	251~351

## 02 서비스 거부(Dos) 공격

### ■ 취약점 공격형

#### ▪ Land 공격

- 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소값을 똑같이 만들어서 공격 대상에게 보내는 공격.
- 이 때 조작된 IP 주소값은 공격 대상의 IP 주소여야 함.
- Land 공격에 대한 보안 대책은 주로 운영체제의 패치 관리를 통해 마련하거나, 방화벽과 같은 보안 솔루션을 이용



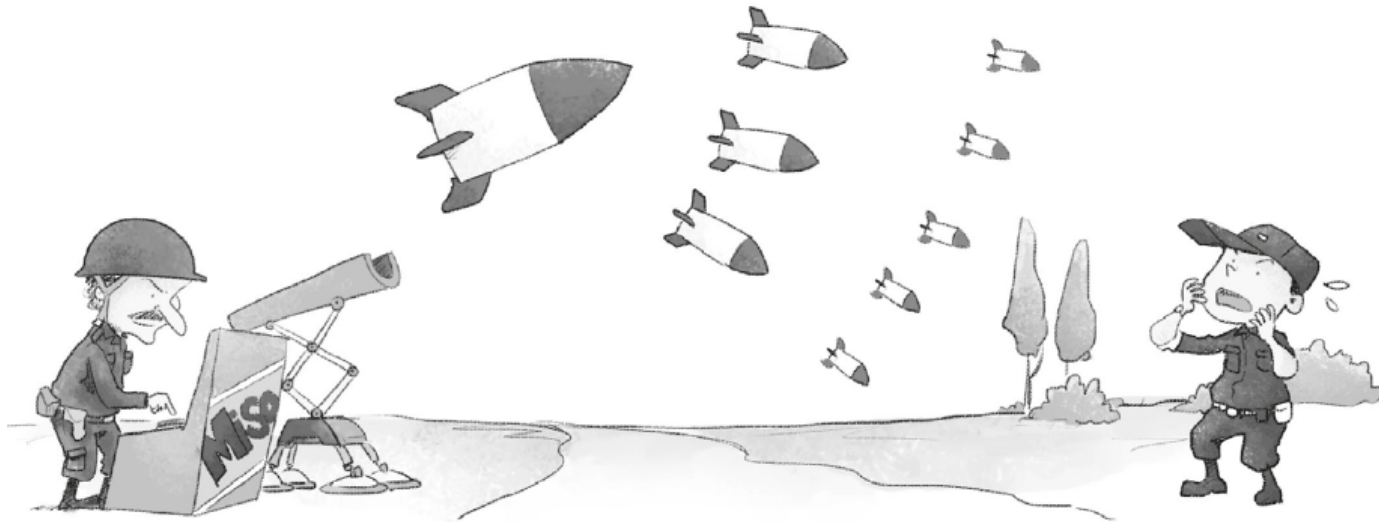
[그림 18] Land 공격

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ Ping of Death 공격

- 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것.
- 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내짐.



[그림 19] Ping of Death 공격

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ SYN Flooding 공격

- 네트워크에서 서비스를 제공하는 시스템에는 동시 사용자 수에 대한 제한이 있음.
- SYN Flooding은 존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서버의 서비스를 제공받지 못하게 하는 공격.



[그림 20] SYN Flooding 공격

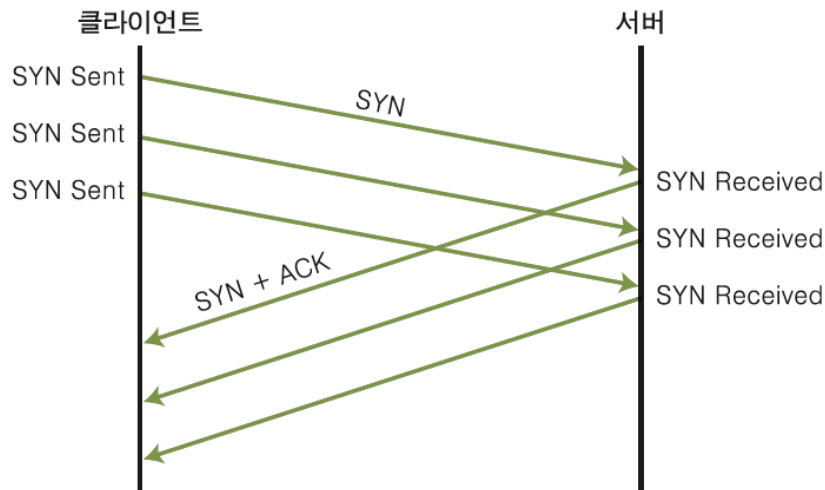


## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ SYN Flooding 공격

- 서버는 클라이언트가 ACK패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있음.



[그림 17] SYN Flooding 공격 시 3 웨이 핸드셰이킹

- 이 공격은 SYN Received의 대기 시간을 줄이는 방법으로 쉽게 해결할 수 있음.
- 침입 방지 시스템(IPS)과 같은 보안 시스템을 통해서도 이러한 공격을 쉽게 차단할 수 있음.

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ HTTP GET Flooding 공격

- 피공격 시스템에 TCP 3-웨이 핸드셰이킹 과정을 통해 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것.

```
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
.....
```

- 공격 패킷을 수신하는 웹 서버는 정상적인 TCP 세션과 함께 정상적으로 보이는 HTTP Get 요청을 지속적으로 요청하게 되므로, 시스템에 과부하가 걸림.

#### ■ HTTP CC 공격

- HTTP 1.1 버전의 CC(Cache-Control) 헤더 옵션은 자주 변경되는 데이터에 대해 새롭게 HTTP 요청 및 응답을 요구하기 위하여 캐시(Cache) 기능을 사용하지 않게 할 수 있음.
- 서비스 거부 공격 기법에 이를 응용하기 위해 'Cache-Control: no-store, mustrevalidate' 옵션을 사용하면 웹 서버는 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가하게 됨

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ 동적 HTTP Request Flooding 공격

- 동적 HTTP Request Flooding은 웹 방화벽을 통해 특징적인 HTTP 요청 패턴 차단 기법을 우회하기 위해 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청하는 기법

#### ■ Smurf 공격

- Smurf(스머프) 공격은 ICMP 패킷과 네트워크에 존재하는 임의의 시스템들을 이용하여 패킷을 확장시켜서 서비스 거부 공격을 수행하는 방법
- 네트워크를 공격할 때 많이 사용



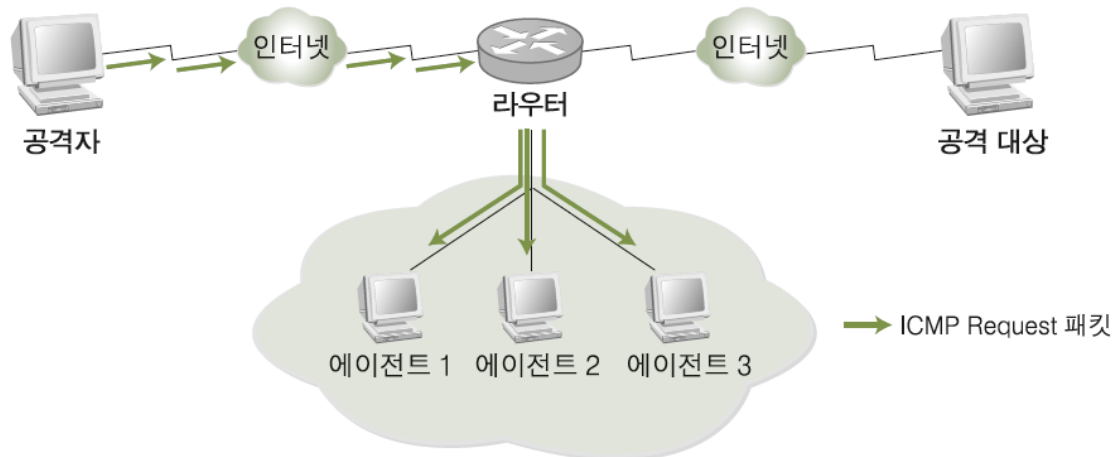
[그림 22] smurf 공격

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ Smurf 공격

- 다이렉트 브로드캐스트(Direct Broadcast)의 이해
  - 기본적인 브로드캐스트는 255.255.255.255의 목적지 IP 주소를 가지고 네트워크의 임의의 시스템에 패킷을 보내는 것으로, 3계층 장비(라우터)를 넘어가지 못함.
  - 172.16.0.255와 같이 네트워크 부분(172.16.0)에 정상적인 IP를 적어주고, 해당 네트워크에 있는 클라이언트의 IP 주소 부분에 255, 즉 브로드캐스트 주소로 채워서 원격지의 네트워크에 브로드캐스트를 할 수 있는데 이를 다이렉트 브로드캐스트라고 함.
  - 공격자가 172.16.0.255로 다이렉트 브로드캐스트를 하면 패킷이 다음과 같이 전달됨.



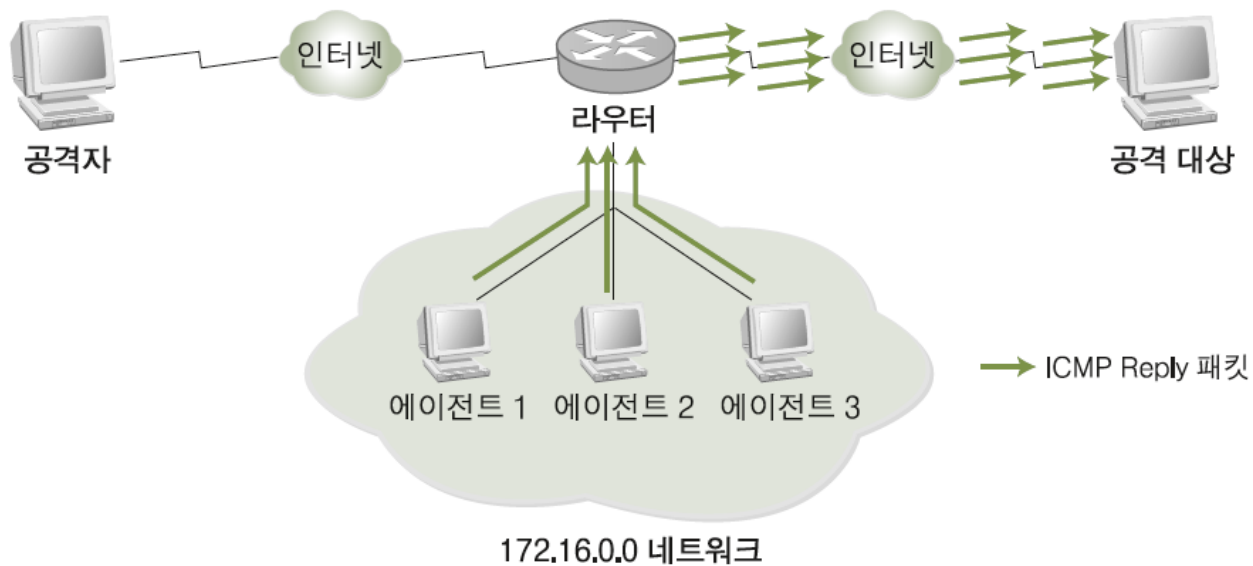
[그림 23] 공격자에 의한 에이전트로의 브로드캐스트

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ Smurf 공격

- ICMP Request를 받은 172.16.0.0 네트워크는 ICMP Request 패킷의 위조된 시작 IP 주소로 ICMP Reply를 다시 보냄.
- 결국 공격 대상은 수많은 ICMP Reply 를 받게 되고 Ping of Death처럼 수많은 패킷이 시스템을 과부하 상태로 만듦.



[그림 24] 에이전트에 의한 스머프 공격의 실행

## 02 서비스 거부(Dos) 공격

### ■ 자원 고갈 공격형

#### ■ Mail Bomb 공격

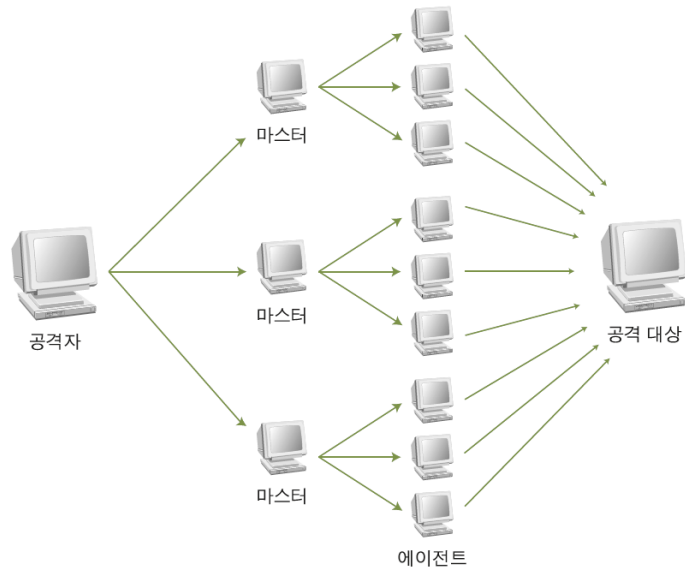
- 흔히 폭탄 메일이라고 함. 스팸 메일도 여기에 해당
- 메일 서버는 각 사용자에게 일정한 양의 디스크 공간을 할당하는데, 메일이 폭주하여 디스크 공간을 가득 채우면 정작 받아야 하는 메일을 받을 수 없음. 즉 스팸 메일도 서비스 거부 공격이 될 수 있음.

### ■ 분산 서비스 거부(DDoS) 공격

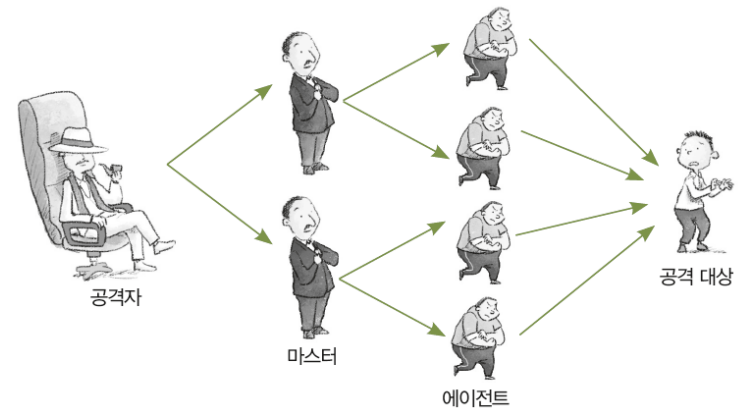
- 1999년 8월 17일 미네소타 대학에서 발생한 것으로 알려져 있음.
- 야후, NBC, CNN 서버의 서비스를 중지시킴. 피해가 상당히 심각하며 이에 대한 확실한 대책 역시 없고 공격자의 위치와 구체적인 발원지를 파악하는 것도 거의 불가능에 가까움.
- 특성상 대부분의 공격이 자동화된 툴을 이용.
- 공격의 범위가 방대하며 DDoS 공격을 하려면 최종 공격 대상 이외에도 공격을 증폭시켜주는 중간자가 필요함.
- 분산 서비스 거부 공격에 사용되는 구성
  - 공격자(Attacker) : 공격을 주도하는 해커의 컴퓨터
  - 마스터(Master) : 공격자에게 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리함
  - 핸들러(Handler) 프로그램 : 마스터 시스템의 역할을 수행하는 프로그램
  - 에이전트(Agent) : 공격 대상에 직접 공격을 가하는 시스템
  - 데몬(Daemon) 프로그램 : 에이전트 시스템의 역할을 수행하는 프로그램

## 02 서비스 거부(Dos) 공격

### ■ 분산 서비스 거부(DDoS) 공격



[그림 25] 분산 서비스 거부 공격도

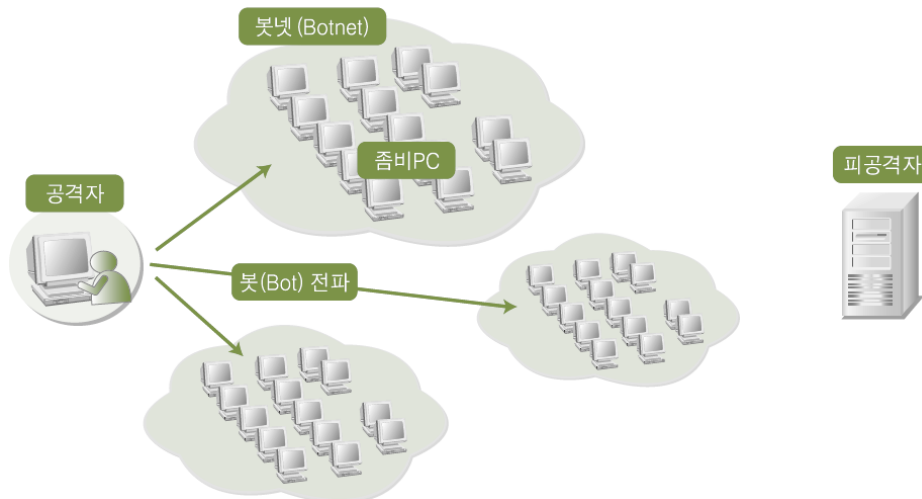


[그림 26] 분산 서비스 거부 공격의 개념도

## 02 서비스 거부(Dos) 공격

### ■ 분산 서비스 거부(DDoS) 공격

- 최근의 분산 서비스 거부 공격은 악성코드와 결합하는 형태
  - PC에서 전파가 가능한 형태의 악성코드를 작성
  - 분산 서비스 거부 공격을 위해 사전에 공격 대상과 스케줄을 정한 뒤 이를 작성한 악성코드에 코딩
  - 악성코드(분산 서비스 거부 공격에 사용되는 악성코드를 봇(Bot)이라고 한다.)가 인터넷을 통해 전파되도록 함.
    - 전파 과정에서는 별다른 공격이 이뤄지지 않도록 잠복함.
  - 악성코드에 감염된 PC를 좀비 PC라고 부르며, 좀비 PC끼리 형성된 네트워크를 '봇넷(Botnet)'이라고 부름.
  - 공격자가 명령을 내리거나 정해진 공격 스케줄에 따라 봇넷으로 형성된 좀비 PC들이 일제히 공격 명령을 수행하여 대규모의 분산 서비스 거부 공격이 가능해짐.

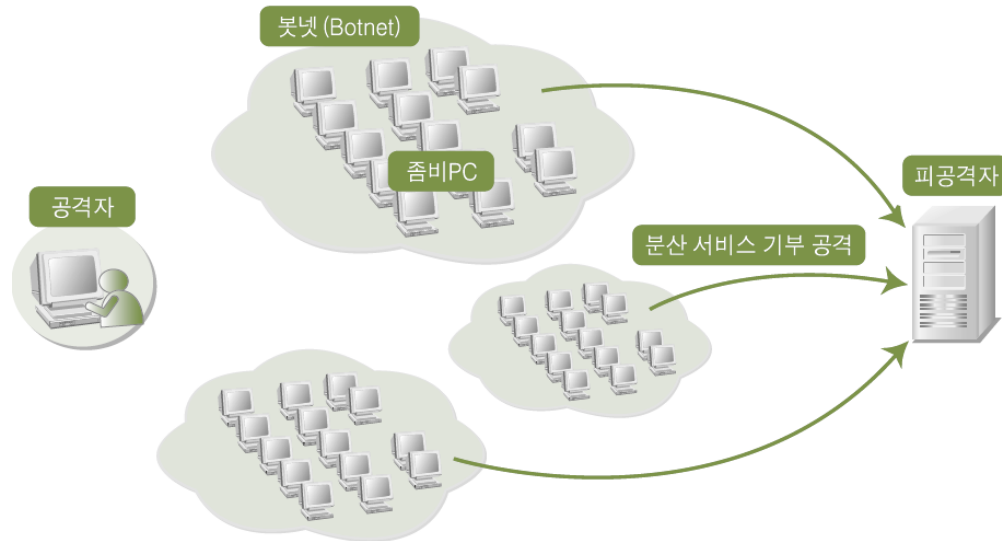


[그림 27] 악성코드(봇)에 의한 분산 서비스 거부 공격 에이전트 전파



## 02 서비스 거부(Dos) 공격

### ■ 분산 서비스 거부(DDoS) 공격



[그림 28] 좀비 PC에 의한 분산 서비스 거부 공격 수행

## 03 스니핑 공격

### ■ 스니핑(Sniffing)

- 수동적(Passive) 공격이라고도 함.
- 스니핑 공격의 종류
  - 드라마에서 주인공이 문 앞에서 다른 이의 대화를 엿듣는 것
  - 도청(Eavesdropping)
  - 전화선이나 UTP(Unshielded Twisted Pair)에 태핑(Tapping)을 해서 전기적 신호를 분석해 정보를 찾아내는 것
  - 전기적 신호를 템페스트(Tempest) 장비를 이용해 분석하는 것

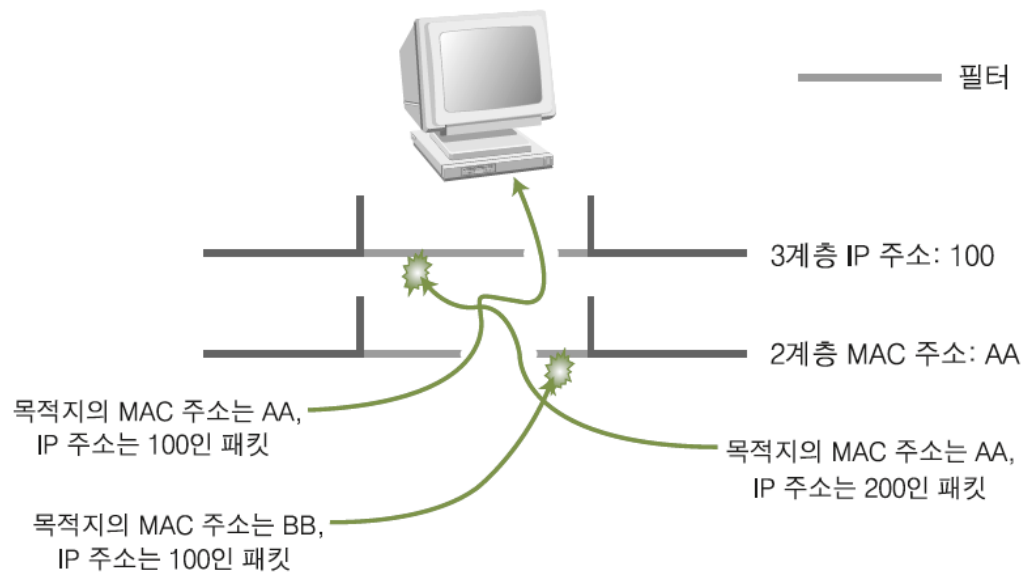


[그림 29] 스니핑 공격

## 03 스니핑 공격

### ■ 스니핑 원리

- 네트워크에 접속하는 모든 시스템은 설정된 IP 주소값과 고유한 MAC 주소값을 가지고 있음.
- 통신을 할때 네트워크 카드는 이 두 가지 정보(2계층의 MAC 정보와 3계층의 IP)를 가지고 자신의 랜 카드에 들어오는 프로토콜 형식에 따른 전기적 신호의 헤더 부분, 즉 주소값을 인식하고 자신의 버퍼에 저장할지를 결정함.
- 네트워크 카드에 인식된 2계층과 3계층 정보가 자신의 것과 일치하지 않는 패킷은 무시함.

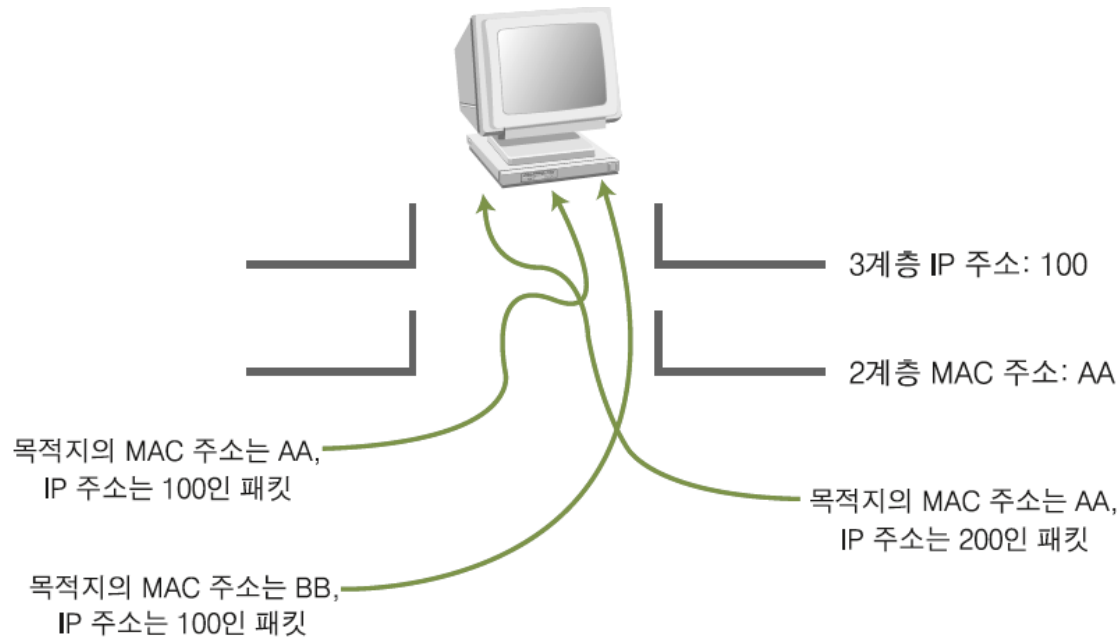


[그림 30] 정상적인 네트워크 필터링

## 03 스니핑 공격

### ■ 스니핑 원리

- 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하기 때문에 2계층과 3계층 정보를 이용한 필터링은 방해물임.
- 이럴 때 2, 3계층에서의 필터링을 해제하는 랜 카드의 모드를 프러미큐어스(Promiscuous) 모드라고 함.



[그림 31] 네트워크 필터링 해제 상태(프러미스큐어스 모드)

## 03 스니핑 공격

### ■ 스위치 재밍 공격

- 스위치의 주소 테이블의 기능을 마비시키는 공격. MACOF 공격이라고도 함.
- 스위치에 랜덤한 형태로 생성한 MAC을 가진 패킷을 무한대로 보내면, 스위치의 MAC 테이블은 자연스레 저장 용량을 넘게 되고, 스위치의 원래 기능을 잃고 더미 허브처럼 작동하게 됨.

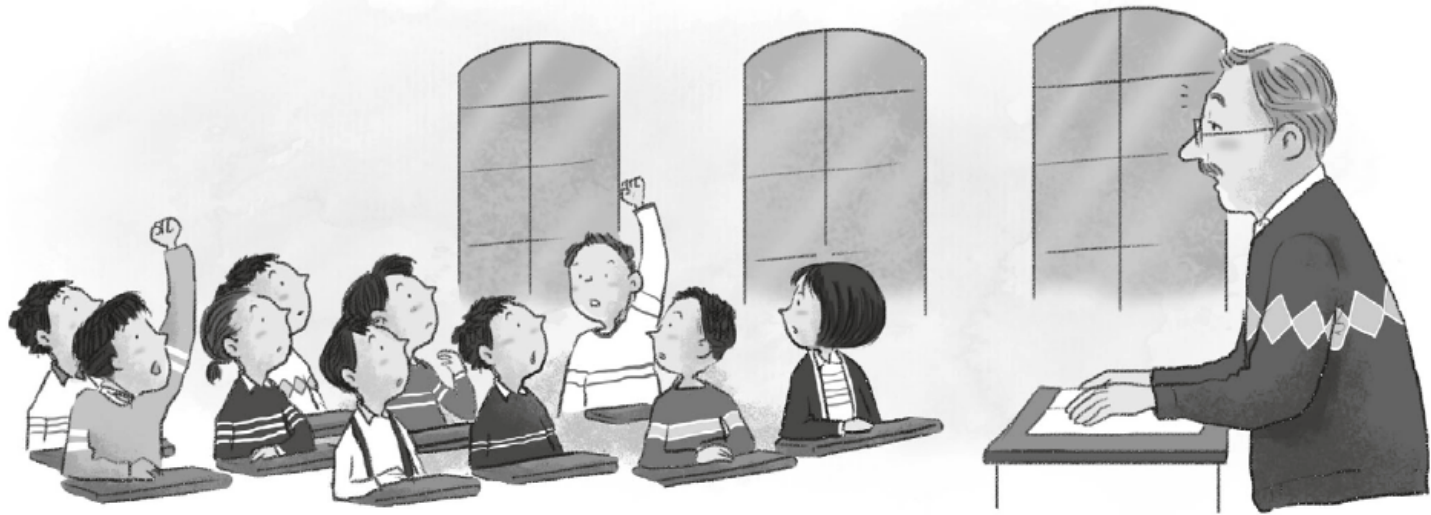
### ■ SPAN 포트 태핑 공격

- SPAN은 포트 미러링(Port Mirroring)을 이용한 것.
- 포트 미러링이란 각 포트에 전송되는 데이터를 미러링하고 있는 포트에도 똑같이 보내주는 것.
- SPAN 포트는 기본적으로 네트워크 장비에서의 하나의 설정 사항으로 이뤄지지만, 포트 태핑(Tapping)은 하드웨어적인 장비로 제공되고 이를 스플리터(Splitter)라고 부르기도 함.

## 03 스니핑 공격

### ■ 스니퍼의 탐지

- 자신의 이름이 아닌데도 아무 이름에나 받아들여 대답하다가 교수님께 걸리는 프리미스큐어스 모드의 학생.



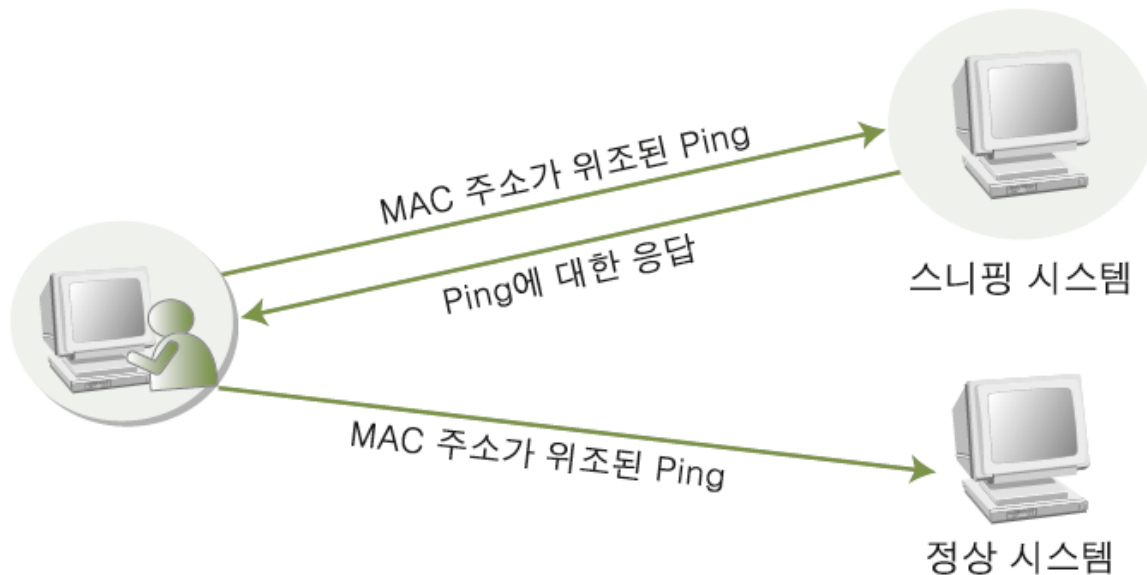
[그림 32] 대출이 들키는 상황

## 03 스니핑 공격

### ■ 스니퍼의 탐지

#### ■ Ping을 이용한 스니퍼 탐지

- 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 Request를 받으면 Response를 전달. 이를 이용해 의심이 가는 호스트에 ping을 보내면 되는데, 네트워크에 존재하지 않는 MAC 주소를 위장하여 보냄.
- 만약 ICMP Echo Reply를 받으면 해당 호스트가 스니핑을 하고 있는 것임.



[그림 33] Ping을 이용한 스니퍼 탐지

## 03 스니핑 공격

### ■ 스니퍼의 탐지

#### ■ ARP를 이용한 스니퍼 탐지

- ping과 유사한 방법으로, 위조된 ARP Request를 보냈을 때 ARP Response가 오면 프러미스큐어스 모드로 설정되어 있는 것

#### ■ DNS를 이용한 스니퍼 탐지

- 일반적으로 스니핑 프로그램은 사용자의 편의를 위해 스니핑한 시스템의 IP 주소에 DNS에 대한 이름 해석 과정(Inverse-DNS lookup)을 수행
- 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지

#### ■ 유인(Decoy)를 이용한 스니퍼 탐지

- 스니핑 공격을 하는 공격자의 주요 목적은 ID와 패스워드의 획득에 있음.
- 가짜 ID와 패스워드를 네트워크에 계속 뿌리고 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지

#### ■ ARP watch를 이용한 스니퍼 탐지

- ARP watch는 MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여, 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려주는 툴.
- 대부분의 공격 기법이 위조된 ARP를 사용하기 때문에 쉽게 탐지할 수 있음.



## 04 스푸핑 공격

### ■ ARP 스푸핑 공격

- ARP(Address Resolution Protocol) 스푸핑은 MAC 주소를 속이는 것. 즉, MAC 주소를 속여 랜에서의 통신 흐름을 왜곡시킴.

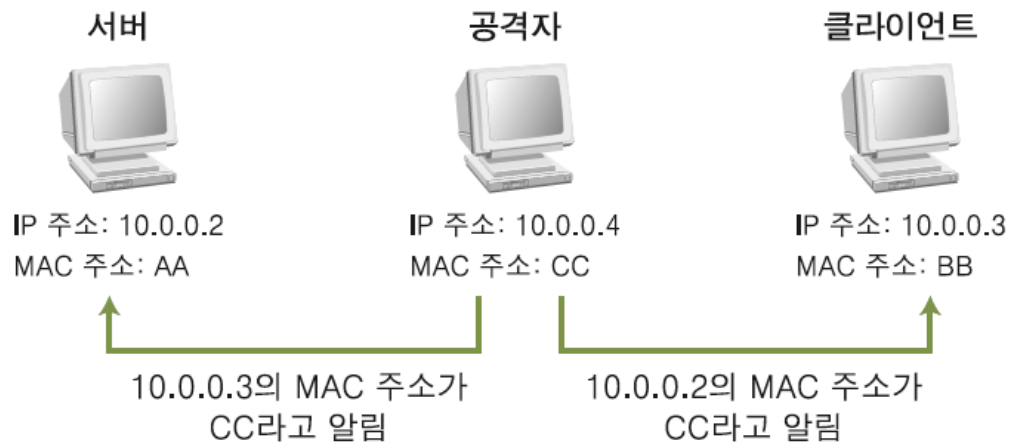
[표 7] ARP 스푸핑 공격 예에 사용되는 네트워크

호스트 이름	IP 주소	MAC 주소
서버	10.0.0.2	AA
클라이언트	10.0.0.3	BB
공격자	10.0.0.4	CC

## 04 스푸핑 공격

### ■ ARP 스푸핑 공격

- 공격자가 서버와 클라이언트의 통신을 스니핑하기 위해 ARP 스푸핑 공격을 시도해보자.



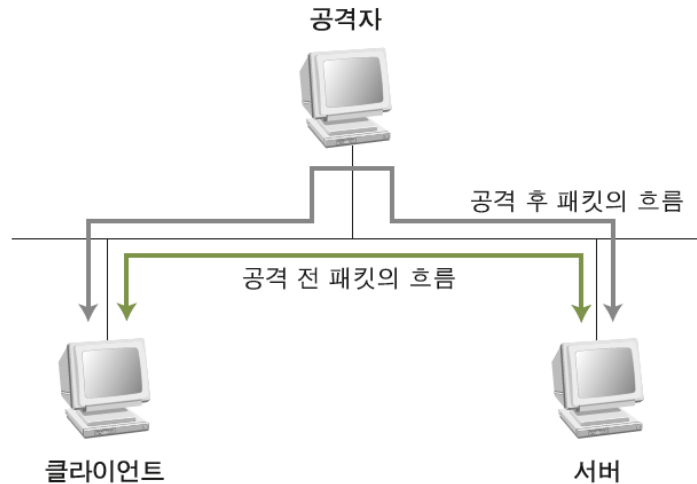
[그림 34] ARP 스푸핑

- 공격자는 서버의 클라이언트에게 10.0.0.2에 해당하는 가짜 MAC 주소 CC를 알리고, 서버에게는 10.0.0.3에 해당하는 가짜 MAC 주소 CC를 알림.
- 공격자가 서버와 클라이언트 컴퓨터에 서로 통신하는 상대방을 공격자 자기 자신으로 알렸기 때문에 서버와 클라이언트는 공격자에게 각각 패킷을 보냄.
- 공격자는 각자에게 받은 패킷을 읽은 후 서버가 클라이언트에 보내고자 하던 패킷을 클라이언트에게 정상적으로 보내주고, 클라이언트가 서버에게 보내고자 하던 패킷을 서버에게 보내줌.

## 04 스푸핑 공격

### ■ ARP 스푸핑 공격

- ARP 스푸핑 공격 후 패킷 결과



[그림 35] ARP 스푸핑 공격에 따른 네트워크 패킷의 흐름

- 윈도우에서는 arp -a 명령을 이용해 현재 인지하고 있는 IP와 해당 IP를 가지고 있는 시스템의 MAC 주소 목록을 다음과 같이 확인할 수 있음. 이것을 'ARP 테이블'이라고 함.

```
C:\Windows\system32\cmd.exe
C:\W>arp -a

인터페이스: 192.168.0.8 --- 0xb
인터넷 주소      물리적 주소      유형
192.168.0.1       00-26-66-d4-ac-e4  동적
192.168.0.255     ff-ff-ff-ff-ff-ff  정적
224.0.0.22        01-00-5e-00-00-16  정적
224.0.0.252       01-00-5e-00-00-fc  정적
239.255.255.250   01-00-5e-7f-ff-fa  정적
255.255.255.255   ff-ff-ff-ff-ff-ff  정적
```

[그림 36] arp-a 명령의 실행 결과

## 04 스푸핑 공격

### ■ ARP 스푸핑 공격

- ARP 스푸핑 공격을 당하기 전에 `arp -a` 명령을 실행한 결과

```
Internet Address Physical Address Type  
10.0.0.2 AA Dynamic
```

- ARP 스푸핑을 당한 후 `arp -a` 명령을 실행한 결과

```
Internet Address Physical Address Type  
10.0.0.2 CC Dynamic
```

- ARP 스푸핑에 대한 대응책

- ARP 테이블이 변경되지 않도록 `arp -s [IP 주소][MAC 주소]` 명령으로 MAC 주소 값을 고정시키는 것

```
arp -s 10.0.0.2 AA
```

- `-s(static)`는 고정시킨다는 의미. 이 명령으로 Type 부분이 Dynamic에서 Static으로 바뀌게 됨. 하지만 이 대응책은 시스템이 재부팅될 때마다 수행해주어야 하는 번거로움이 있음.
- 어떤 보안 툴은 클라이언트의 ARP 테이블의 내용이 바뀌면 경고 메시지를 보내기도 하지만 사실 ARP 스푸핑은 TCP/IP 프로토콜 자체의 문제로 근본적인 대책은 없음.

## 04 스푸핑 공격

### ■ IP 스푸핑 공격

- IP 스푸핑은 쉽게 말해 IP 주소를 속이는 것
- 트러스트 : 파티에 초대된 사람 중 친분이 있는 사람은 초대장을 확인하지 않고 그냥 들여보내주는 것과 같은 개념



[그림 37] 파티 주최자와의 트러스트를 이용해 인증 없이 파티에 참석하는 모습

## 04 스푸핑 공격

### ■ IP 스푸핑 공격

- 유닉스 계열에서는 트러스트 인증법을 주로 사용.
- 윈도우에서는 트러스트 대신 액티브 디렉토리 (Active Directory)를 주로 사용.
- 트러스트 설정을 해주려면 유닉스에서는 /etc/host.equiv 파일에 다음과 같이 클라이언트의 IP와 접속 가능한 아이디를 등록해 주어야 함.

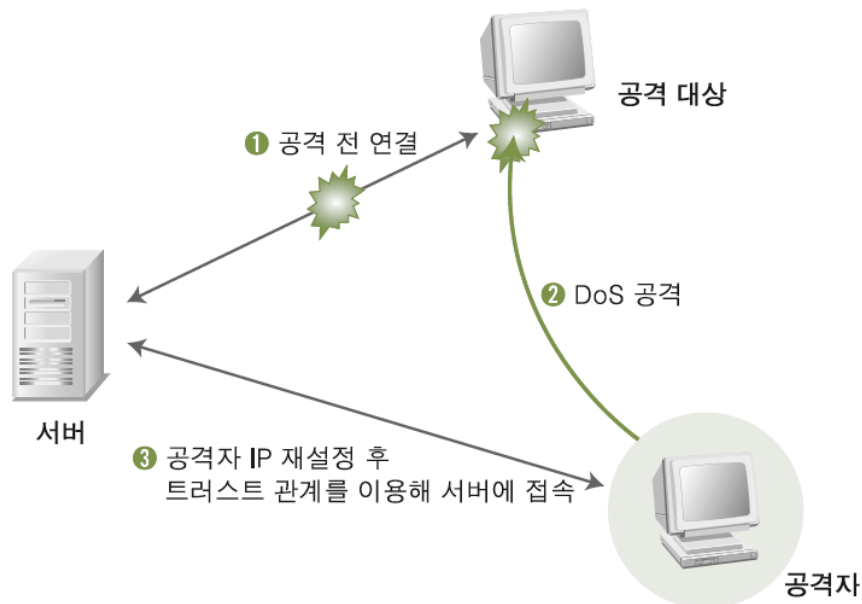
```
❶ 200.200.200.200 root
❷ 201.201.201.201 +
```

- ❶은 200.200.200.200에서 root 계정이 로그인을 시도하면 패스워드 없이 로그인을 허락하라는 의미
- ❷는 201.201.201.201에서는 어떤 계정이든 로그인을 허락하라는 것으로 +는 모든 계정을 의미
  - 만일 ++라고 적힌 행이 있으면 IP와 아이디에 관계없이 모두 로그인을 허용하라는 의미

## 04 스푸핑 공격

### ■ IP 스푸핑 공격

- 트러스트를 이용한 접속은 네트워크에 패스워드를 뿌리지 않기 때문에 스니핑 공격에 안전한 것처럼 보임.
- 하지만 인증이 IP를 통해서만 일어나기 때문에 공격자가 해당 IP를 사용해서 접속하면 스니핑을 통해서 패스워드를 알아낼 필요성 자체가 없어지는 문제점이 있음.
- 실제로 공격은 트러스트로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어짐.
- 공격자는 패스워드 없이 서버에 로그인할 수 있음.

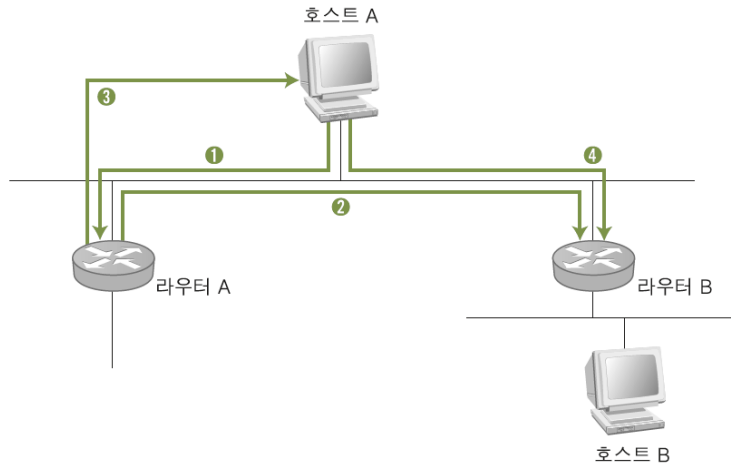


[그림 38] IP 스푸핑을 이용한 서버 접근

## 04 스푸핑 공격

### ■ ICMP 리다이렉트 공격

- ICMP 리다이렉트는 3계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격



[그림 39] ICMP 리다이렉트 개념도

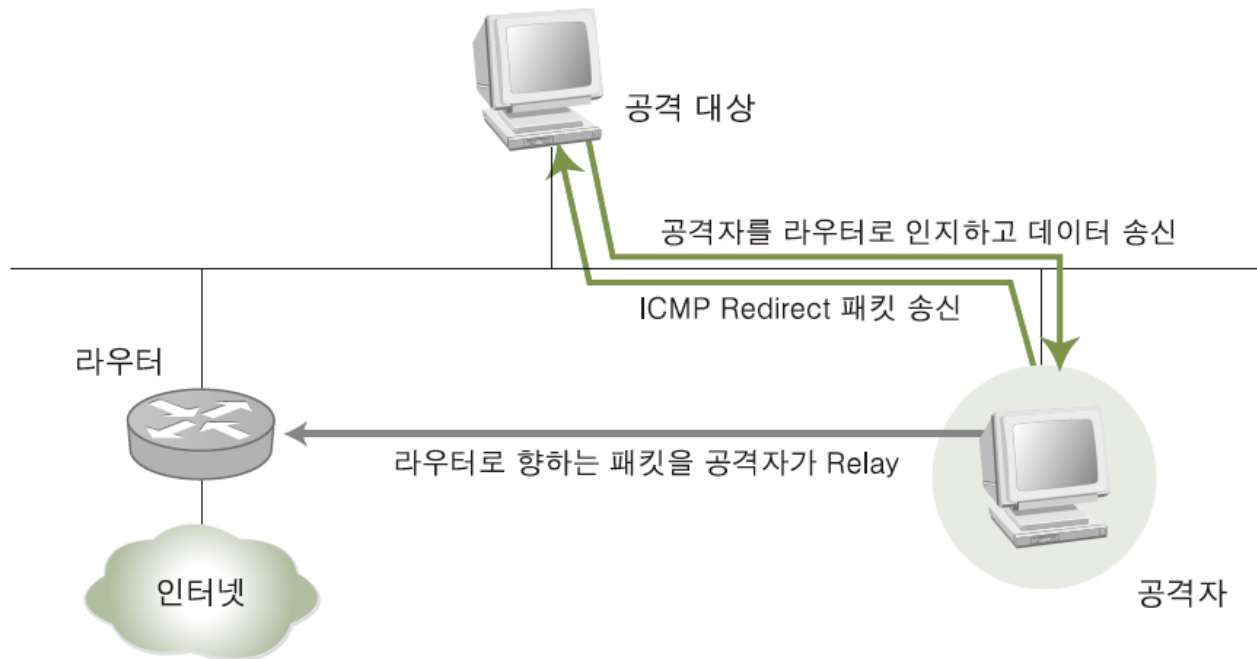
- 1 호스트 A에 라우터 A가 기본으로 설정되어 있기 때문에, 호스트 A가 원격의 호스트 B로 데이터를 보낼 때 패킷을 라우터 A로 보낸다.
- 2 라우터 A는 호스트 B로 보내는 패킷을 수신한다. 그리고 라우팅 테이블을 검색하여 호스트 A에게 자신을 이용하는 것보다 라우터 B를 이용하는 것이 더 효율적이라고 판단하여 해당 패킷을 라우터 B로 보낸다.
- 3 라우터 A는 호스트 B로 향하는 패킷을 호스트 A가 자신에게 다시 전달하지 않도록, 호스트 A에 ICMP 리다이렉트 패킷을 보내서 호스트 A가 호스트 B로 보내는 패킷이 라우터 B로 바로 향하도록 한다.
- 4 호스트 A는 라우팅 테이블에 호스트 B에 대한 값을 추가하고, 호스트 B로 보내는 패킷은 라우터 B로 전달한다.



## 04 스푸핑 공격

### ■ ICMP 리다이렉트 공격

- 공격자가 라우터 B가 되어 ICMP 리다이렉트 패킷도 공격 대상에게 보낸 후 라우터 A에게 다시 릴레이시켜주면 모든패킷을 스니핑할 수 있음

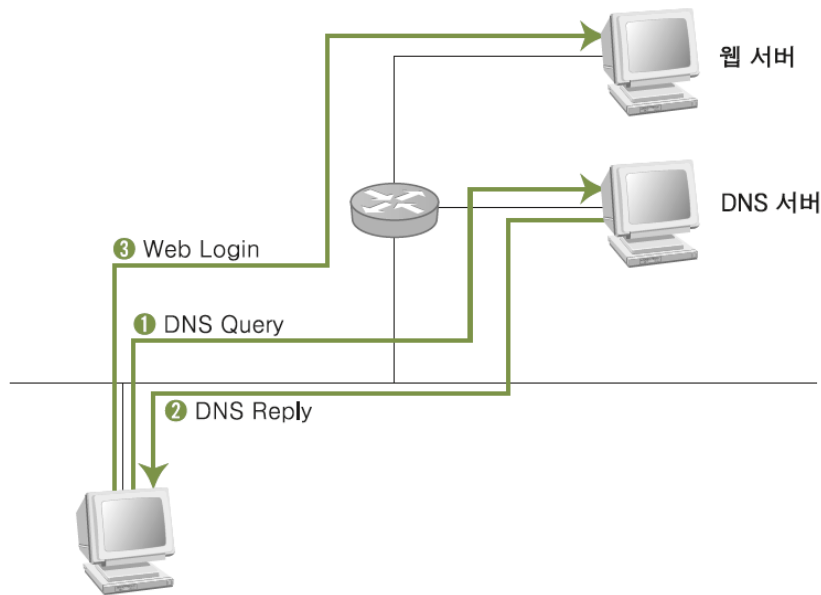


[그림 40] ICMP 리다이렉트 공격 개념도

## 04 스푸핑 공격

### ■ DNS 스푸핑 공격

- 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격



[그림 41] 정상적인 DNS 서비스

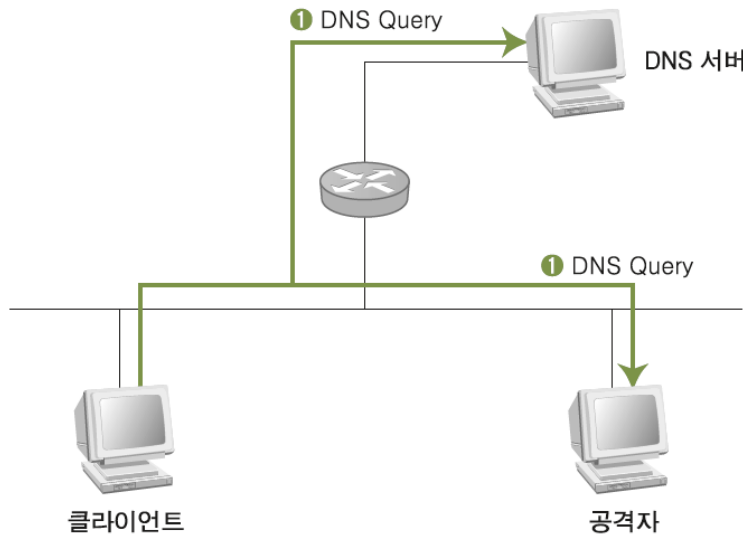
- 1 클라이언트가 DNS 서버에게 접속하고자 하는 IP 주소(www.wishfree.com과 같은 도메인 이름)를 물어봄. 이때 보내는 패킷은 DNS Query
- 2 DNS 서버가 해당 도메인 이름에 대한 IP 주소를 클라이언트에게 보내줌.
- 3 클라이언트가 받은 IP 주소를 바탕으로 웹 서버를 찾아감.

## 04 스푸핑 공격

### ■ DNS 스푸핑 공격

① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인.

- 스위칭 환경일 경우에는 클라이언트 DNS Query 패킷을 보내면 이를 받아야 하므로 ARP 스푸핑과 같은 선행 작업이 필요함.
- 만약 허브를 쓰고 있다면 모든 패킷이 자신에게도 전달되므로 클라이언트가 DNS Query 패킷을 보내는 것을 자연스럽게 확인할 수 있음.

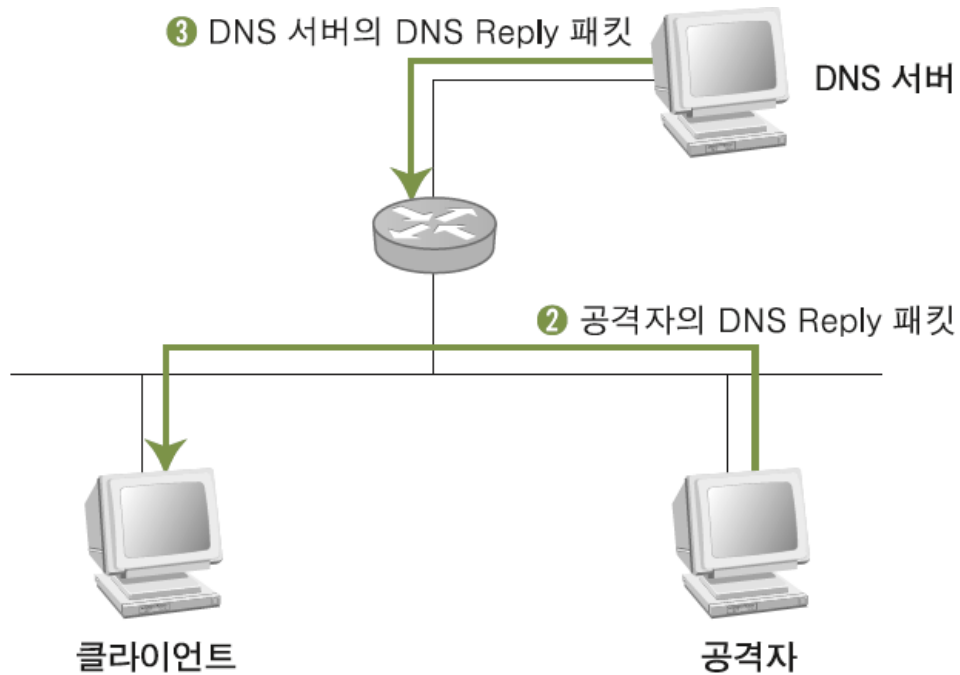


[그림 42] DNS Query

## 04 스푸핑 공격

### ■ DNS 스푸핑 공격

- ② 공격자는 로컬에 존재하므로 DNS 서버보다 지리적으로 가까움.
  - DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 클라이언트에게 위조된 DNS Response 패킷을 보낼 수 있음.

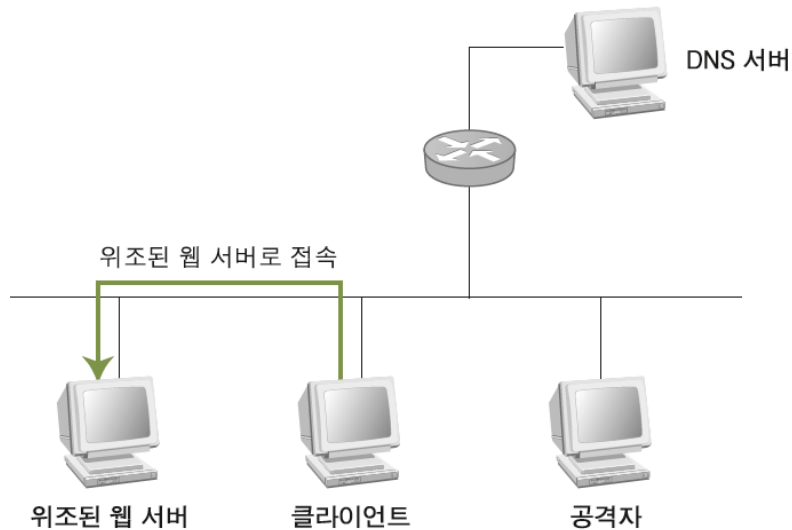


[그림 43] 공격자와 DNS 서버의 DNS Response

## 04 스푸핑 공격

### ■ DNS 스푸핑 공격

- ③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고, 웹에 접속.
  - 지리적으로 멀리 떨어져 있는 DNS 서버가 보낸 DNS Response 패킷은 버림.



[그림 44] 공격 성공 후 도착한 DNS 서버의 DNS Response

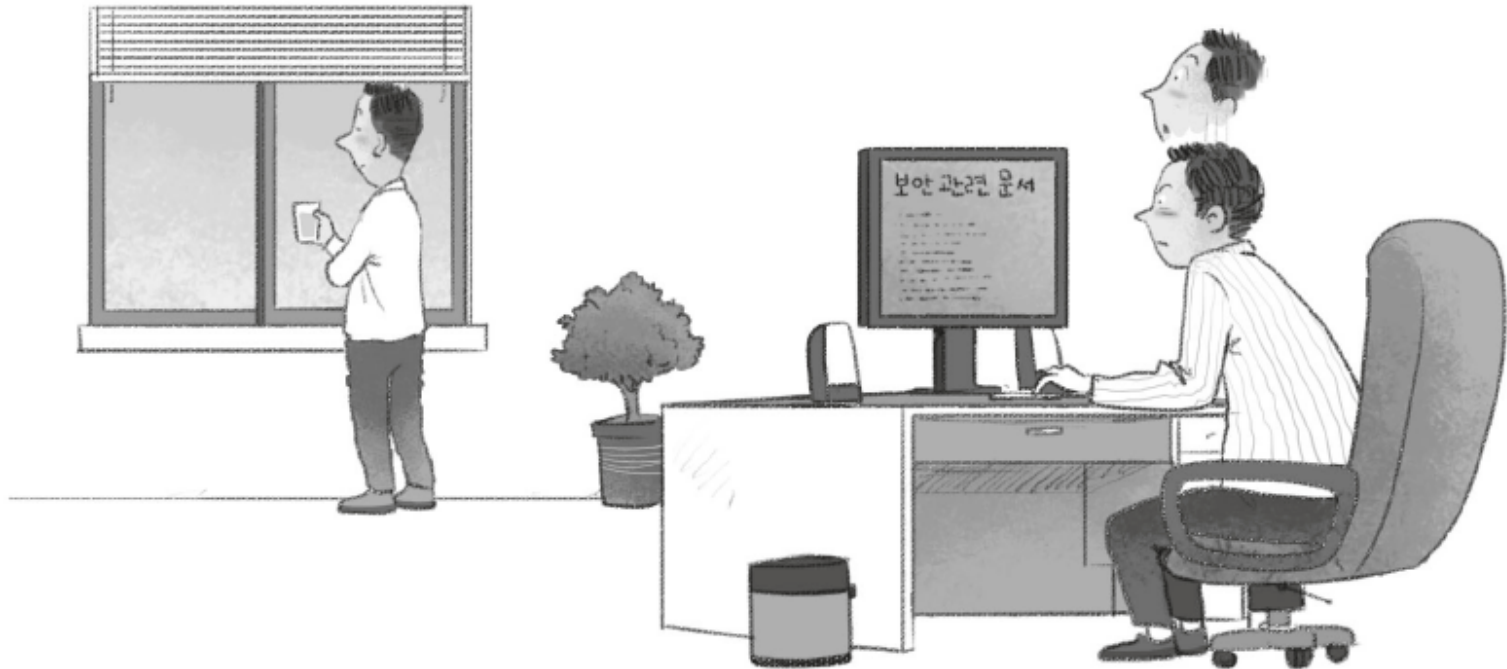
- hosts 파일에는 URL과 IP 정보가 등록되어 있음.

```
127.0.0.1 localhost
200.200.200.123 www.wishfree.com
201.202.203.204 www.sysweaver.com
```

## 05 세션 하이재킹 공격

### ■ 세션 하이재킹(Session Hijacking)의 정의

- 세션(Session) : 사용자와 컴퓨터, 또는 두 대의 컴퓨터 간의 활성화된 상태
- 세션 하이재킹 : 두 시스템 간 연결이 활성화된 상태, 즉 로그인(Login)된 상태를 가로채는 것을 뜻함.



[그림 45] 자리 가로채기

## 05 세션 하이재킹 공격

### ■ TCP 세션 하이재킹

- TCP가 가지는 고유한 취약점을 이용해 정상적인 접속을 빼앗는 방법.
- TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 번호를 사용함. 이 시퀀스 번호가 잘못되면 이를 바로 잡기 위한 작업을 하는데, TCP 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 번호를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식.
  - ① 클라이언트와 서버 사이의 패킷을 통제. ARP 스푸핑 등을 통해 클라이언트와 서버 사이의 통신 패킷이 모두 공격자를 지나가게 하도록 하면 됨.
  - ② 서버에 클라이언트 주소로 연결을 재설정하기 위한 RST(Reset) 패킷을 보냄. 서버는 해당 패킷을 받고, 클라이언트의 시퀀스 번호가 재설정된 것으로 판단하고, 다시 TCP 쓰리웨이 핸드셰이킹을 수행.
  - ③ 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받음.

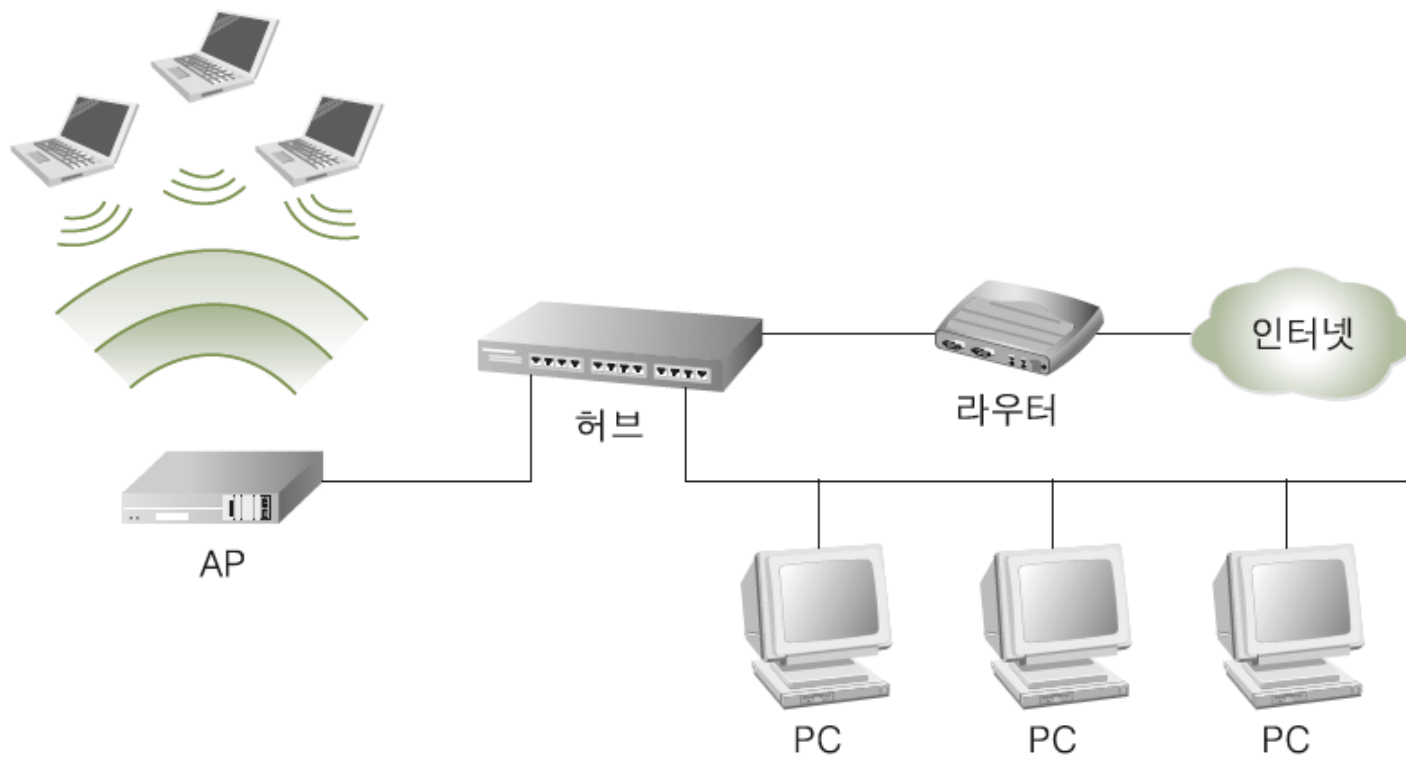
### ■ 세션 하이재킹 공격에 대한 대응책

- SSH와 같이 세션에 대한 인증 수준이 높은 프로토콜을 이용해서 서버에 접속해야 함.
- 클라이언트와 서버 사이에 MAC 주소를 고정시켜주는 줌. 주소를 고정시키는 방법은, 앞서도 언급했지만 ARP 스푸핑을 막아주기 때문에 결과적으로 세션 하이재킹을 막을 수 있음.

## 06 무선 네트워크 공격과 보안

### ■ 무선 랜

- 기본적으로 Ethernet Like 개념으로서, 보통 내부 네트워크의 확장으로서 이용됨. 무선 랜을 사용하기 위해서는 내부의 유선 네트워크에 AP(Access Point) 장비를 설치해야 함.



[그림 46] 유선 네트워크에 연결된 AP로 무선 랜까지 확장된 네트워크



## 06 무선 네트워크 공격과 보안

### ■ 무선 랜

[표 8] 안테나의 종류와 수신 가능 거리

안테나의 종류	수신 가능 거리
무지향성 안테나	200~300m
지향성 안테나	1Km
무지향성 증폭 안테나	(200mW)2~3Km
접시형 안테나	수Km
접시형 안테나 + 지향성 증폭 안테나	50~60Km

- 무지향성 안테나
  - 주로 봉의 형태
  - 전파 수신에 일정한 방향성이 없어 AP의 위치에 상관없이 동작
- 지향성은 다시 수직과 수평인 것으로 나누어짐.
  - 대부분의 무방향성 안테나는 수평면에 대한 무지향성을 지원
  - 지향성 안테나는 목표 방향을 지정해 그 방향으로만 전파를 탐지
    - 지향성 안테나는 보통 쟁반이나 접시 모양



[그림 47] 무지향성 안테나



[그림 48] 지향성 안테나

## 06 무선 네트워크 공격과 보안

### ■ 무선 랜

[표 9] 무선 랜 주요 프로토콜

시기	프로토콜	주요 사항	특징
1997.7	802.11	2.4GHz/2Mbps	최초의 무선 랜 프로토콜
1999.9	802.11b	2.4GHz/11Mbps	위피(WiFi)라고도 하며, WEP 방식의 보안을 구현할 수 있음
	802.11a	5GHz/54Mbps	위피5(WiFi 5)라고도 하며, 전파 투과성과 회절성이 떨어져 통신 단절 현상이 심하며, 802.11b와 호환이 되지 않음
2003.6	802.11g	2.4GHz/54Mbps	802.11b에 802.11a의 속도 성능을 추가한 프로토콜, 802.11b와 호환이 되나 네트워크 공유시 데이터 처리 효율이 현격히 줄어드는 문제점이 있음
2004.6	802.11i	802.11b와 동일	802.11b 표준에 보안성을 강화한 프로토콜
2007	802.11n	5GHz, 2.4GHz	최대 600Mbps의 속도. 여러 개의 안테나를 사용하는 다중 입력/다중 출력(MIMO) 기술과 대역폭 손실의 최소화

## 06 무선 네트워크 공격과 보안

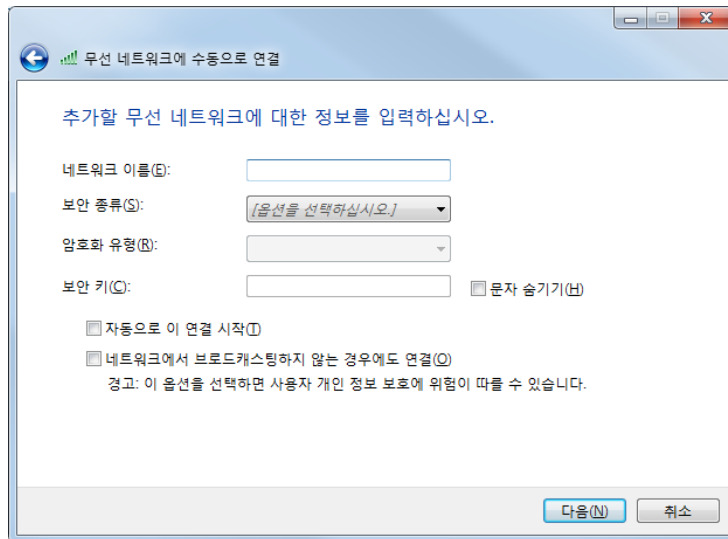
### ■ AP 보안

#### ■ 물리적인 보안 및 관리자 패스워드 변경

- AP 보호를 위한 첫 번째 사항은 물리적인 보안
- AP는 전파가 건물 내에 한정되도록 전파 출력을 조정하고, 건물 안쪽의 중심부의 눈에 쉽게 띄지 않는 곳에 설치
- 설치한 후에 AP의 기본 계정 패스워드는 반드시 재설정해야 함.

#### ■ SSID 브로드캐스팅 금지

- AP를 탐색하면 나타나는 각 AP의 이름이 바로 SSID(Service Set Identifier)임. 무선 랜에서 가장 설정하기 쉬운 보안 사항은 이 SSID가 AP 탐색에 쉽게 노출되지 않도록 SSID의 브로드캐스팅을 막는 것.



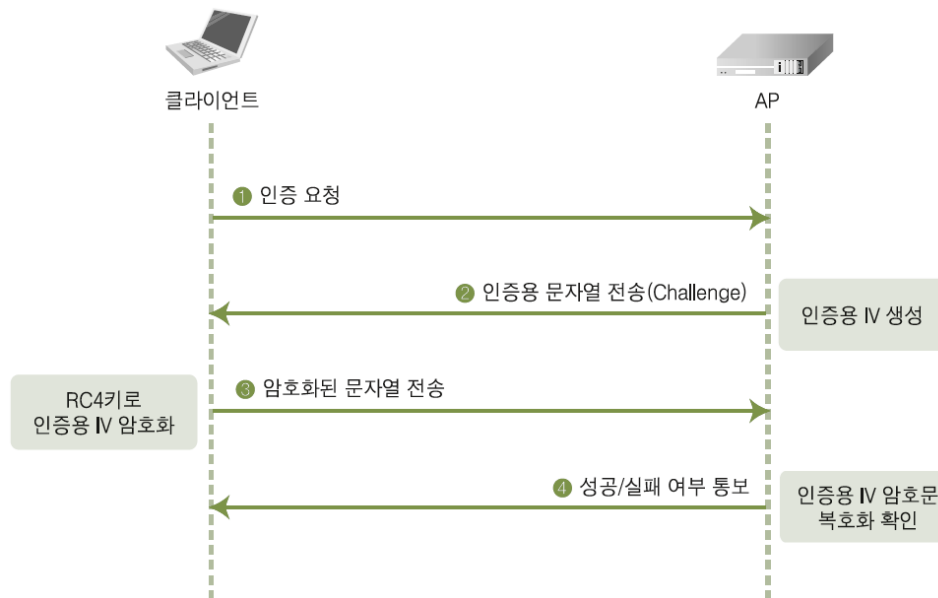
[그림 51] [제어판]-[네트워크 및 인터넷]-[무선 네트워크 관리]에서 추가

## 06 무선 네트워크 공격과 보안

### ■ 무선 랜 통신 암호화

#### ■ WEP의 암호화

- 무선 랜을 암호화하는 가장 기본적인 방법



[그림 53] WEP 암호화 세션의 생성 과정

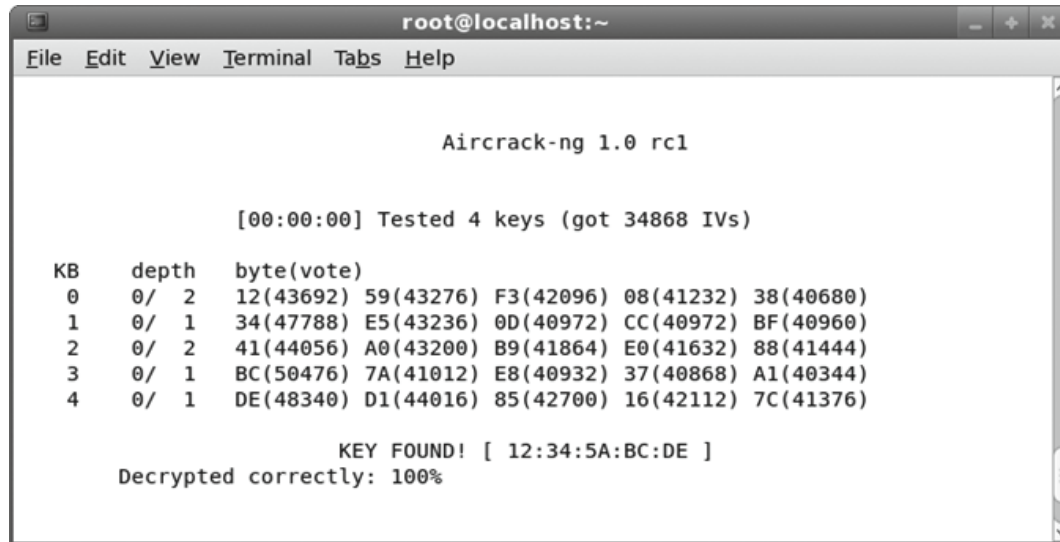
- ① 클라이언트에서 AP에 인증을 요청한다.
- ② AP는 무작위로 IV(Initial Vector)를 생성하여 클라이언트에 전달한다.
- ③ 클라이언트는 전달받은 IV를 본인이 알고 있는 WEP 키(RC4 키)로 암호화하여 AP에 전송한다.
- ④ AP는 전달받은 암호문을 WEP 키로 복호화하여 본인이 최초 전송한 IV와 일치하면 연결을 허락한다.

## 06 무선 네트워크 공격과 보안

### ■ 무선 랜 통신 암호화

#### ■ WEP의 암호화

- WEP 키를 이용한 무선 랜 암호화 통신의 보안성은 그다지 높지 않음.
- 통신 과정에서 IV는 무작위로 생성되어 암호화 키에 대한 복호화를 어렵게 하지만, 24비트의 IV는 24비트의 짧은 길이로 인해 반복되어 사용되기 때문



```
root@localhost:~  
File Edit View Terminal Tabs Help  
  
Aircrack-ng 1.0 rc1  
  
[00:00:00] Tested 4 keys (got 34868 IVs)  
  
KB    depth  byte(vote)  
0     0/ 2    12(43692) 59(43276) F3(42096) 08(41232) 38(40680)  
1     0/ 1    34(47788) E5(43236) 0D(40972) CC(40972) BF(40960)  
2     0/ 2    41(44056) A0(43200) B9(41864) E0(41632) 88(41444)  
3     0/ 1    BC(50476) 7A(41012) E8(40932) 37(40868) A1(40344)  
4     0/ 1    DE(48340) D1(44016) 85(42700) 16(42112) 7C(41376)  
  
KEY FOUND! [ 12:34:5A:BC:DE ]  
Decrypted correctly: 100%
```

[그림 54] 복호화된 WEP 키

## 06 무선 네트워크 공격과 보안

### ■ 무선 랜 통신 암호화

#### ■ WPA, WPA-PSK의 암호화

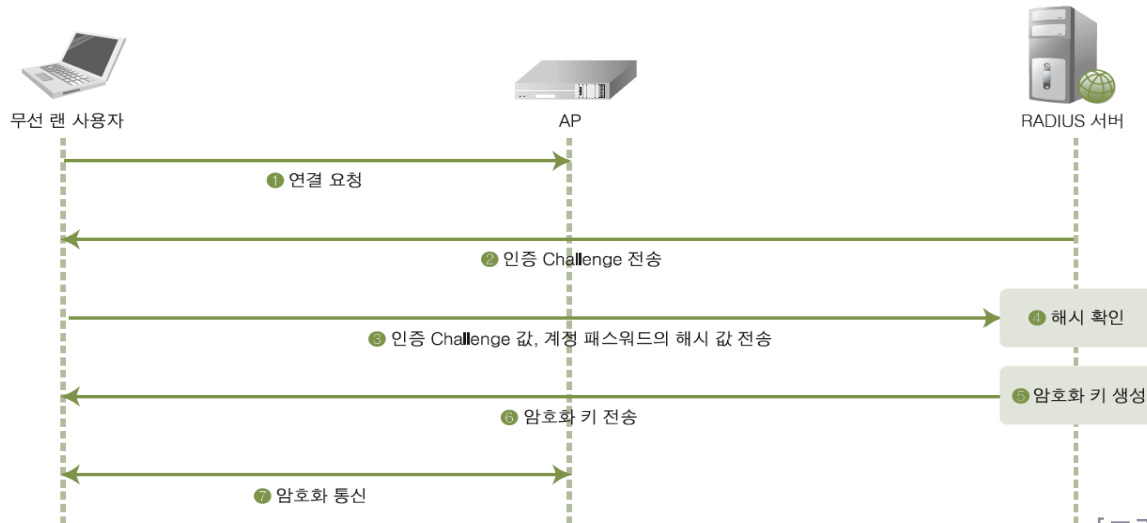
- WPA(WiFi Protected Access)는 키값이 쉽게 깨지는 WEP의 취약점을 보완하기 위해 개발됨.
- 데이터 암호화를 강화하기 위해 TKIP(Temporal Key Integrity Protocol)라는 알고리즘을 사용.
- WEP와 달리 WPA는 단순한 패킷 수집을 통해서 크랙이 이루어지지 않지만, 최초 인증 과정에서 인증 패킷이 노출 될 경우 간단한 패스워드는 몇 시간~몇 일만에 크래킹됨.

### ■ EAP와 802.1x의 암호화

- WPA-EAP로 불리는 WPA Enterprise 방식은 인증 및 암호화를 강화하기 위해 다양한 보안 표준 및 알고리즘을 채택
- 그중 가장 중요하고 핵심적인 사항은 유선 랜 환경에서 포트 기반 인증 표준으로 사용되는 IEEE 802.1x 표준과 함께, 다양한 인증 메커니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택한 것
- 802.1x/EAP(Extensible Authentication Protocol)이 개인 무선 네트워크의 인증 방식과 비교해 추가된 사항
  - 사용자에 대한 인증을 수행
  - 사용 권한을 중앙 관리
  - 인증서, 스마트카드 등의 다양한 인증을 제공
  - 세션별 암호화 키를 제공

## 06 무선 네트워크 공격과 보안

### ■ EAP와 802.1x의 암호화



[그림 55] RADIUS와 802.1x를 이용한 무선 랜 인증

- ① 클라이언트는 AP에 접속을 요청한다. 이때 클라이언트와 AP는 암호화되지 않은 통신을 수행한다. 그러나 클라이언트가 AP와 연결된 내부 네트워크로 접속하는 것은 AP에 의해 차단된다.
- ② RADIUS 서버는 클라이언트에 인증 Challenge를 전송한다.
- ③ 클라이언트는 Challenge에 대한 응답으로서 최초로 전송받은 Challenge 값, 계정, 패스워드에 대한 해시 값을 구하여 RADIUS 서버에게 전송한다.
- ④ RADIUS 서버는 사용자 관리 DB 정보에서 해당 계정의 패스워드를 확인한다. 그리고 연결 생성을 위해 최초로 전송한 Challenge의 해시 값을 구하여 클라이언트에서 전송받은 해시 값과 비교한다.
- ⑤ 해시 값이 일치하면 암호화 키를 생성한다.
- ⑥ 생성한 암호화 키를 클라이언트에게 전달한다.
- ⑦ 전달받은 암호화 키를 이용하여 암호화 통신을 수행한다.

*Q&A*