



3주차: 네트워크 보안



ChulSoo Park

School of Computer Engineering & Information Technology

Korea National University of Transportation

E-Mail : pcs8321@naver.com

학습목표 (3주차)

- ISO 7계층의 세부 동작 이해.
- 네트워크 관련 해킹 기술의 종류와 방법 이해.
- 네트워크 해킹을 막기 위한 대응책.
- 무선네트워크 공격과 보안 이해.

03 CHAPTER

네트워크 보안

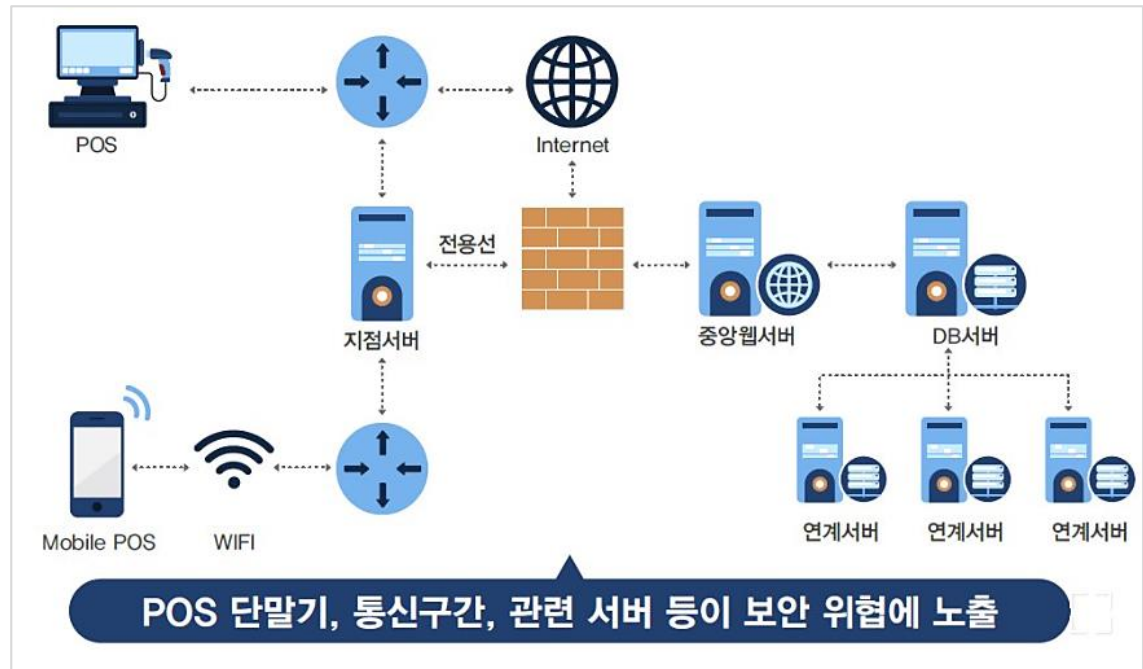


CONTENTS

1. 네트워크의 이해
2. 서비스 거부 공격 : DoS와 DDoS
3. 스니프 공격
4. 스푸핑 공격
5. 세션 하이재킹 공격
6. 무선 네트워크 공격과 보안

1. 시스템 보안

1. 시스템 보안의 이해
2. 계정 관리
3. 세션 관리
4. 접근 관리
5. 권한 관리
6. 로그 관리
7. 취약점 관리
8. 모바일 보안



1. 네트워크의 이해

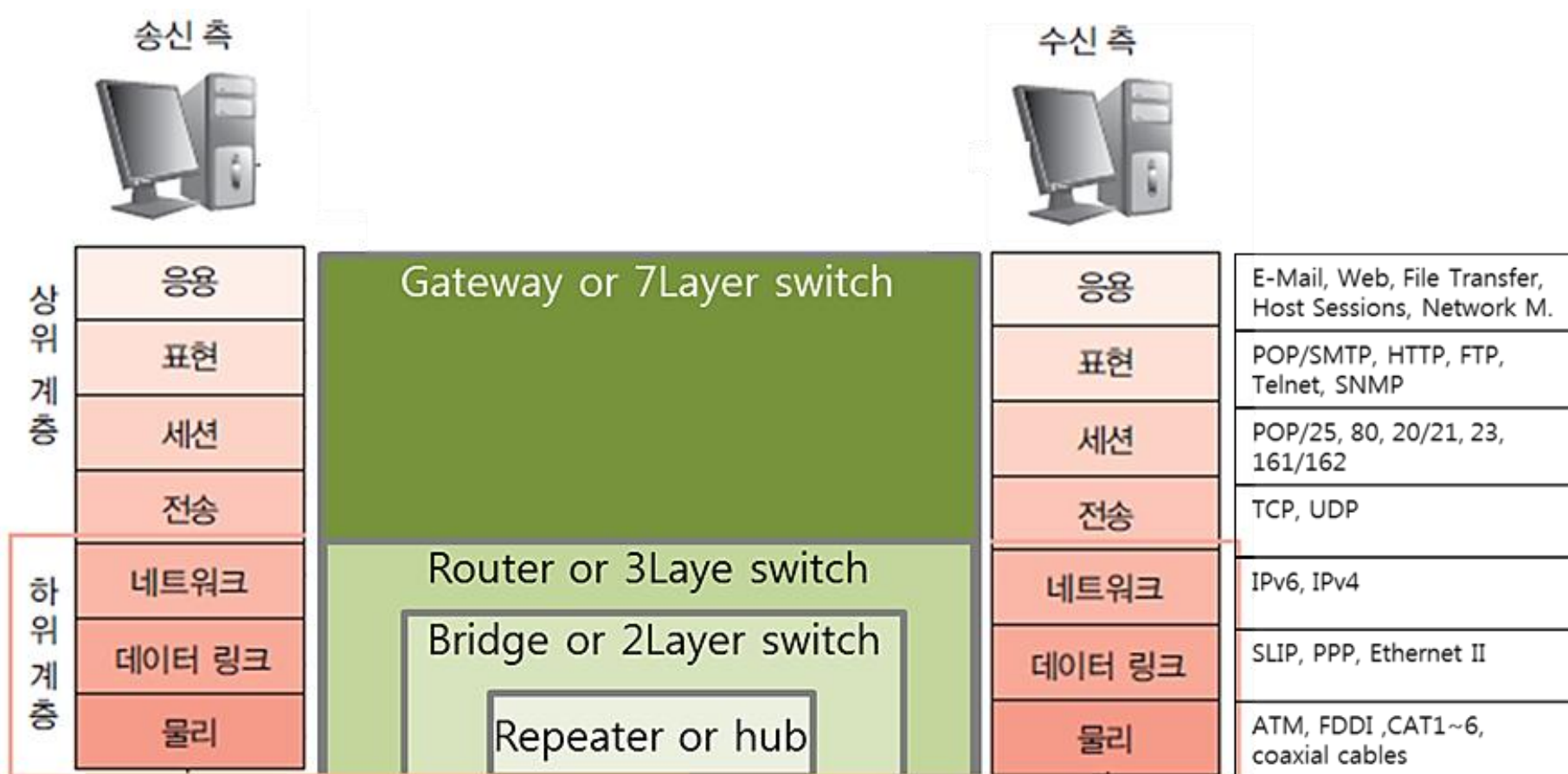
- **네트워크**는 세상의 길과 비슷한 역할을 하며 보안 분야에 많은 변화 발생
- **해커들이 네트워크를 통해** 다른 시스템에 침투하는 방법(길)을 찾음.
- 1970년대에 TCP/IP 네트워크가 본격적으로 시작, 지금도 근본적인 바뀜 없이 사용됨.
- 이장에서 다루는 스니핑, 스푸핑, 세션 하이재킹과 같은 기법은 여전히 사용됨.
- 최근에 무선랜이 발달하면서 무선랜 공격이 다양화 되어가고 있음.



1. 네트워크의 이해

1 OSI 7계층의 이해

OSI(Open Systems Interconnection) 7계층 국제표준화기구(ISO)에서 개발한 모델로, 컴퓨터 네트워크 프로토콜 디자인과 통신을 계층으로 나누어 설명한 것.



1. 네트워크의 이해

1 OSI 7계층의 이해

OSI(Open Systems Interconnection) 7계층으로 분리한 이유

- 계층을 분리함으로써 각 계층은 독립적인 역할을 수행
- 역할이 분리되면서 문제 발생시 문제의 현상을 보았을 때 어떤 계층에 문제가 생겼는지도 파악이 가능, 각 계층의 수행 역할이 다르기 때문에 이런 것이 가능.
- 각 계층은 하위 계층을 사용하고 현 계층의 기능을 포함하여 상위 계층에 제공, 따라서 계층구조는 위에서 바라보았을 때 아래층이 안보이는 구조라 볼 수 있다. 이러한 이유로 최상위 계층만 보면 그 아래 계층을 모두 포함하고 있음.



1. 네트워크의 이해

1 OSI 7계층의 이해

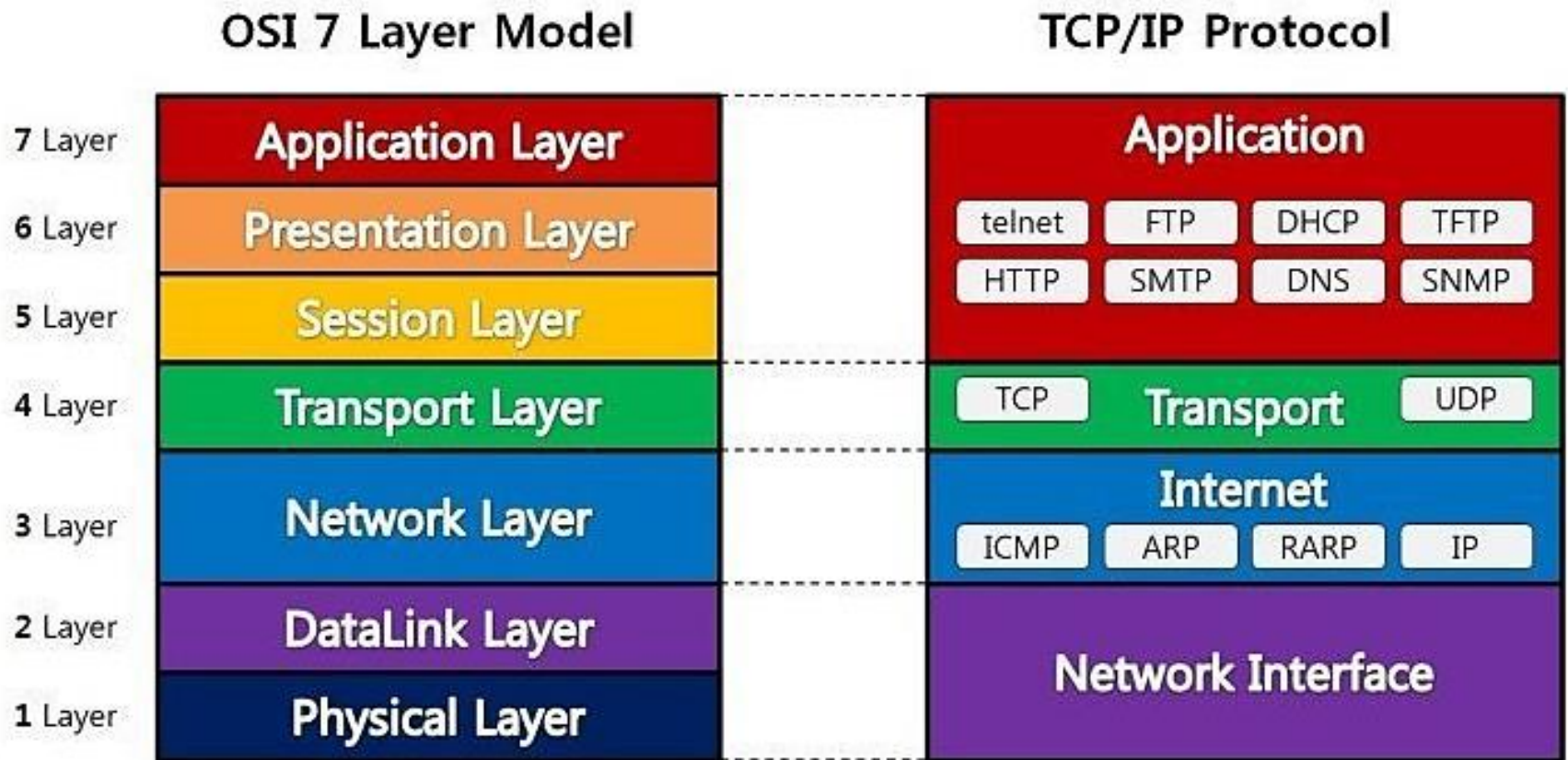
레벨	PDU	프로토콜	기능
7 응용 계층 (Application)	Data	E-MAIL, Web app. File Transfer	사용자가 네트워크에 접근할 수 있도록 해주는 계층이다. 사용자 인터페이스, 전자우편, 데이터베이스 관리 등 서비스를 제공한다.
6 표현 계층 (Presentation)	Data	HTTP, FTP, DNS, DHCP, SMTP, NFS, RTSP	코드 간의 번역을 담당하는 계층. 사용자 시스템에서 데이터 구조를 통일하여 응용 프로그램 계층에서 데이터 형식의 차이로 인해 발생하는 부담을 덜어줌. Ex. 텔넷, HTTP, SSH, SMTP, FTP
5 세션 계층 (Session)	Data	SSH, TLS, ISO8327, Apple talk, NetBIOS	양 끝단의 응용 프로세스가 통신을 관리하는 방법 제공
4 전송 계층 (Transport)	Segments	TCP, UDP, ARP, RTP, SCTP, SPX	양 끝단의 사용자들이 신뢰성 있는 데이터를 주고 받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해줌 장비. 게이트웨이, 스위치(L4)
3 네트워크 계층 (Network)	Packets	IP, ICMP, IGMP, RIP, IPX, DDP	여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층, 다양한 길이의 데이터를 네트워크를 통해 전달하고, 전송 계층이 요구하는 서비스 품질(QoS)을 위해 기능적, 절차적 수단 제공 Ex. IP(IPv4, IPv6), 장비. 라우터, 스위치(L3)
2 데이터링크 계층 (Data Link)	Frames	MAC, PPP, 무선랜, Ethernet	두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층, 16진수 12개로 구성된 MAC 주소 사용 장비. 브릿지, 스위치(L2)/ MAC 주소 16진수 12개로 구성
1 물리 (Physical)	Bits	RS-232C, Modem	물리적 매체를 연결하기 위한 전기적, 물리적 세부 사항을 정의한 계층으로 랜선 등이 포함 장비. 허브, 리피터, FDDI, CAT1~6, ATM, coaxial cables

프로토콜 데이터 단위(PDU, Protocol Data Unit)

1. 네트워크의 이해

1 OSI 7계층의 이해

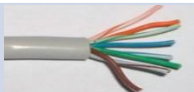


OSI 7계층과 TCP/IP의 관계



1. 네트워크의 이해

2 물리 계층(1계층)

1계층 물리 계층은 시스템 간의 물리적 연결을 의미함. (PDU : bits)

케이블 선	실체	설 명
UTP		제품 전선과 피복만으로 구성, 두선 사이의 전자 유도를 줄이기 위해 절연의 구리 선이 서로 꼬여 있음
FTP		알루미늄 은박이 네 가닥의 선을 감싸고 있으며, UTP보다 절연 기능 우수
STP		연선으로 된 전선 겉에 외부 피복 또는 차폐재가 추가된 케이블, 외부노이즈와 전기적 신호 간섭에 탁월

케이블 CAT(Category)별 특성

CAT	최대 속도	용 도
CAT1	1Mbps 미만	아날로그 음성, 초인종 등
CAT2	4Mbps	주로 IBM의 토큰 링 네트워크에 사용
CAT3	16Mbps	10BASE-T 이더넷의 데이터 및 음성 전용에 사용
CAT4	20Mbps	16Mbps 토큰 링에서 사용
CAT5	100Mbps	10/100 BASE-T, 155Mbps ATM에서 사용
CAT6	250Mbps	10/100/1000 BASE-T, Gb 이더넷
CAT7	10Gbps	10Gb 이더넷

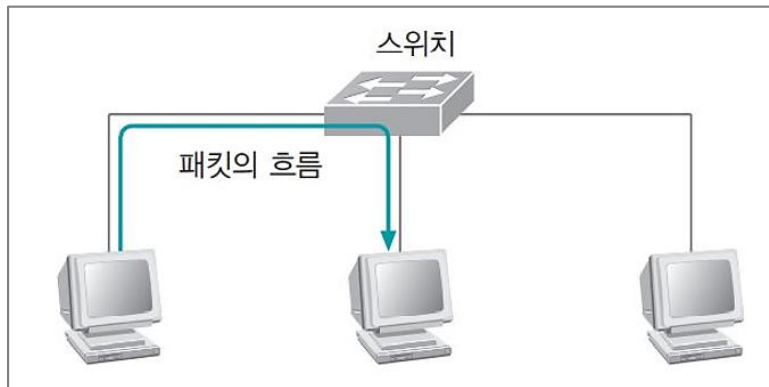
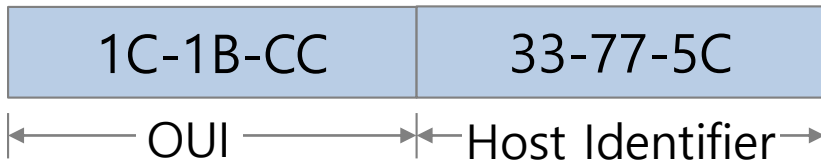
1. 네트워크의 이해

3 데이터 링크 계층(2계층)

2계층인 데이터 링크 계층은 두 포인트 간(point to point)의 신뢰성 있는 전송을 보장하기 위한 계층으로 **CRC**(cyclic redundancy check) 기반의 오류 제어 및 흐름 제어 필요.

데이터 링크 계층에서는 상호 통신을 위해 **MAC** 주소를 할당 받아 활용.

MAC 주소 구성 : 12개의 16진수로 구성



데이터 링크 계층의 패킷 흐름

1. 네트워크의 이해

3 데이터 링크 계층(2계층)

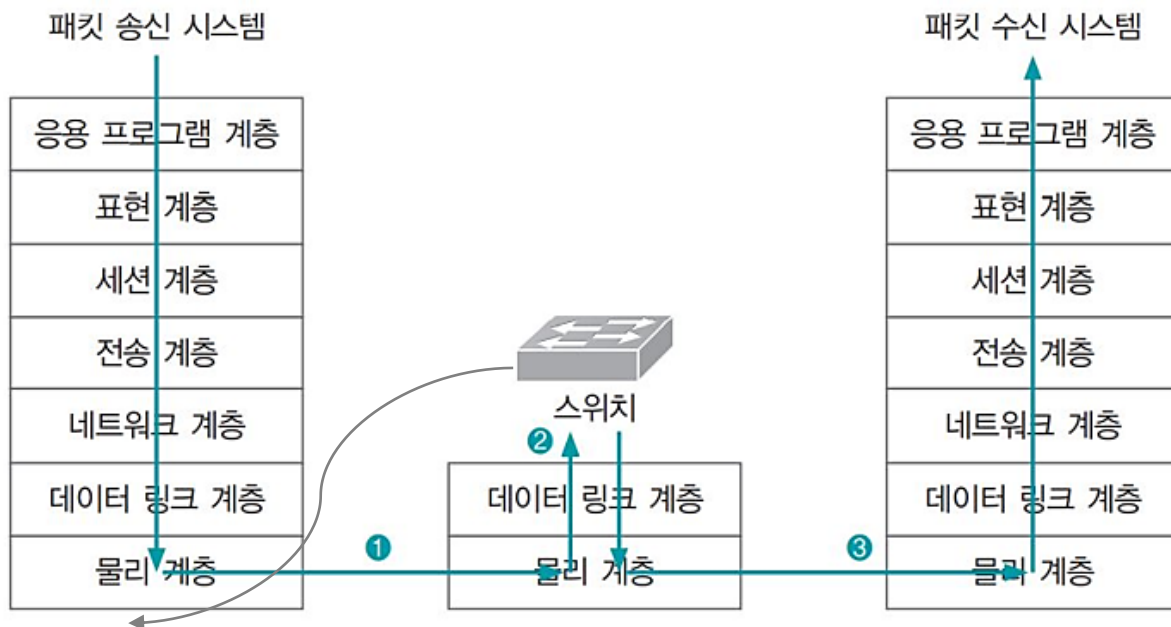
데이터 링크 계층의 패킷 흐름



거실 PC : Port 2



공부방 PC : Port 3



스위치 메모리

1번 포트	
2번 포트	거실 PC MAC 주소
3번 포트	공부방 PC MAC 주소
4번 포트	

데이터링크 계층의 패킷 구조

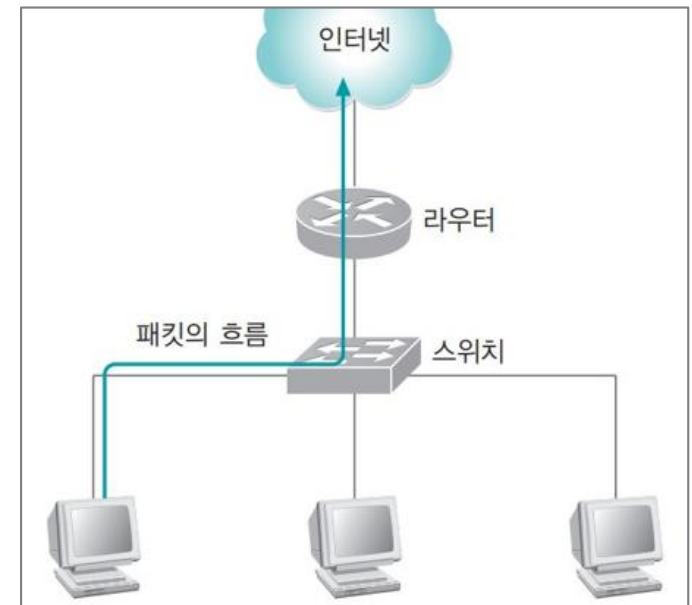
0101000011110011111111	출발지 MAC 주소	목적지 MAC 주소
------------------------	------------	------------

← 네트워크 계층까지의 패킷 정보 → ← 데이터 링크 계층의 패킷 정보 →

1. 네트워크의 이해

4 네트워크 계층(3계층)

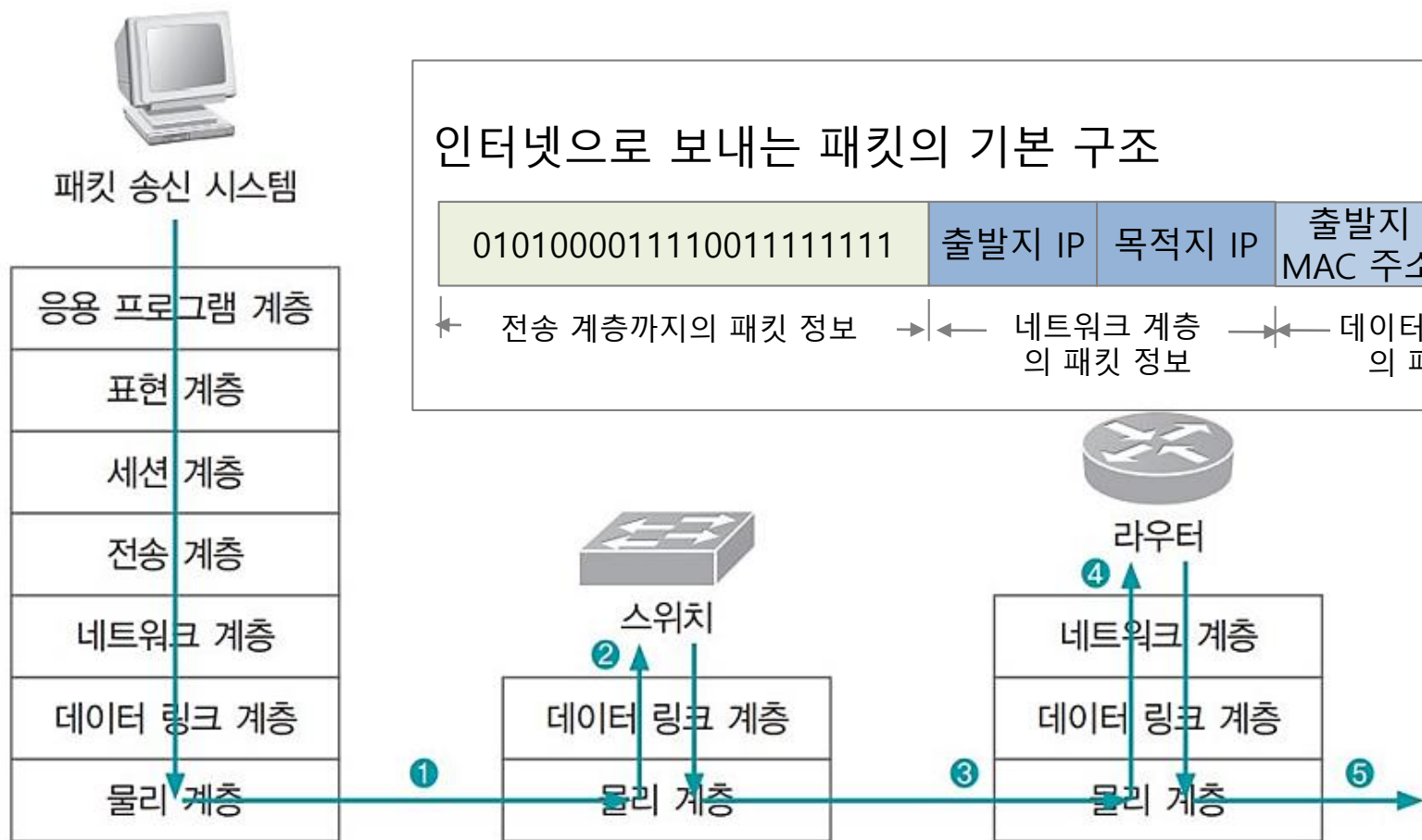
- 3계층인 네트워크 계층은 여러 개의 노드를 거칠 때마다 경로를 찾아 주는 역할을 수행
- 라우팅과 흐름 제어, 세그먼테이션, 오류 제어 등을 수행.
- 장비 : 라우터나 스위치(L3)
- 네트워크 계층에서 여러 개의 노드를 거쳐 경로를 찾기 위한 주소로는 IP를 주로 사용.
- IP는 8비트의 4개로 구성 :
(예) 11000000.10101000.00000000.01100100
- 주소의 클래스 : A,B,C,D,E



1. 네트워크의 이해

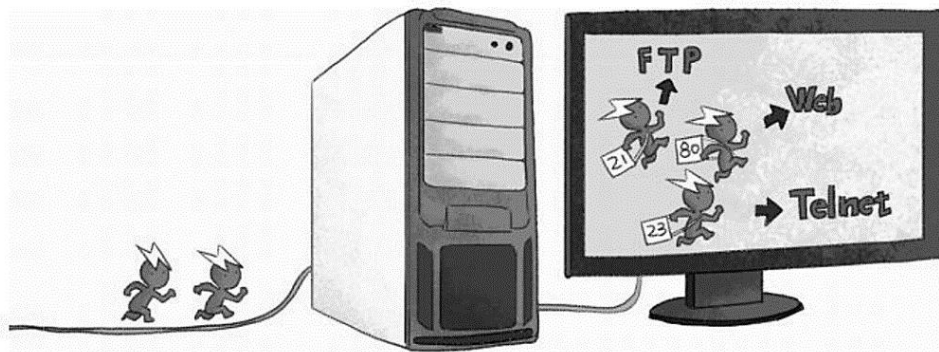
4 네트워크 계층(3계층)

네트워크 계층의 동작



1. 네트워크의 이해

- 4계층인 전송 계층은 양 끝단(end to end)의 사용자들이 신뢰성 있는 데이터를 주고 받을 수 있게 하여 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해줌.
- 대표적인 전송 프로토콜 : TCP(Transmission Control Protocol)
- MAC 주소 : 네트워크 카드의 고유 식별자, IP 시스템의 주소, **포트(Port)**는 시스템에 도착한 후 패킷이 찾아갈 응용프로그램으로 통하는 통로 번호.
- 충북 충주시 대소원면 검단리 789번지 한국교통대학교 김영희
- 충북 충주시 대소원면 검단리 789번지 한국교통대학교 소프트웨어전공 김영희(키큰)



1. 네트워크의 이해

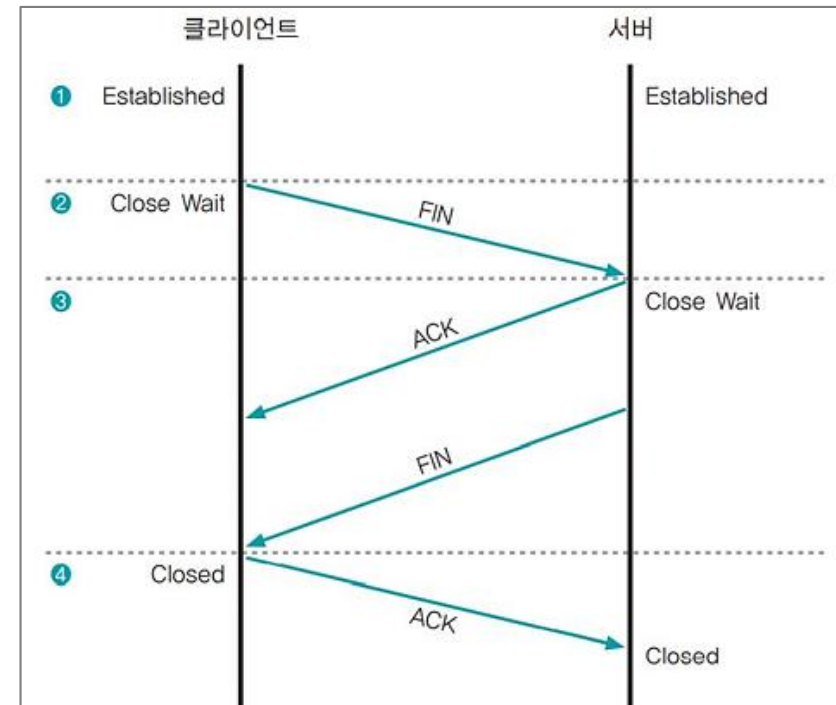
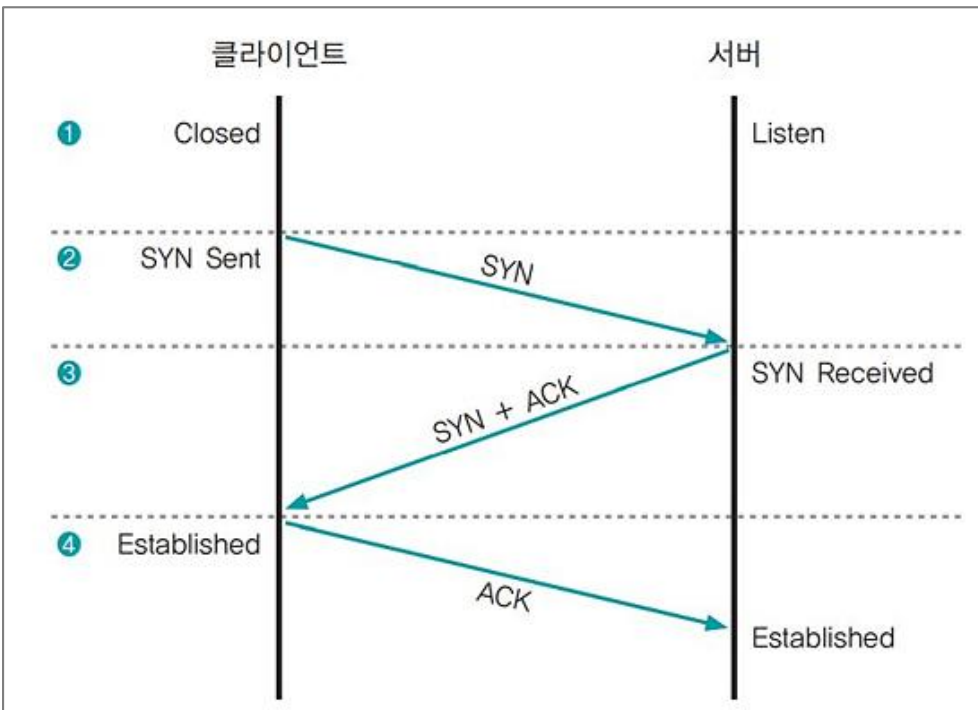
주요 포트와 서비스(과정평가형 자격증 실기 사례)

- ① 20 : FTP - DATA (FTP의 데이터 전송)
- ② 21 : FTP - CONTROL (FTP의 데이터 전송 제어)
- ③ 23 : TELNET (터미널 에뮬레이션)
- ④ 25 : SMTP (메일 메시지 전송 프로토콜)
- ⑤ 53 : DNS (DNS 질의응답)
- ⑥ 69 : TFTP (인증이 존재하지 않는 단순한 파일 전송)
- ⑦ **80 : HTTP (웹 전송)**
- ⑧ 110 : POP3 (메일 서버로 전송 된 메일을 읽을 때 사용)
- ⑨ 789 : NTP (Network Time Protocol)
- ⑩ 161 : SNMP (네트워크 관리와 모니터링을 위해 사용)
- ⑪ 179 : BGP (BGP 라우팅 프로토콜)

1. 네트워크의 이해

TCP의 연결 과정 (3-웨이 핸드셰이킹)

TCP 연결 해제 과정



TCP 기능

- 연결 지향형 프로토콜
 - ✓ 수신 측이 데이터를 흘려버리지 않도록 하는 데이터 흐름 제어 전송 중 에러가 발생하면 자동으로 재전송하는 에러 제어 기능
- 이를 통해 데이터의 확실한 전송을 보장 하지만 과정이 완전하지 않아 해커들에게 많은 공격을 받음

UDP 기능

- TCP와 달리 데이터의 신뢰성 있는 전송을 보장하지 않음
- 특정한 경우 전송 경로 확립을 위한 번잡함을 생략하고 시간을 절약할 수 있어 UDP가 더 효과적
 - ✓ 신뢰성이 매우 높은 회선을 사용하는 경우, 데이터의 확실한 전송을 요구하지 않는 경우, 한 번에 많은 상대방에게 메시지를 전송하는 경우

1. 네트워크의 이해

■ 세션 계층(5계층)

- ✓ 양 끝단의 응용 프로세스가 통신을 관리하기 위한 방법을 제공
- ✓ 동시 송수신 방식, 반이중 방식, 전이중 방식의 통신과 함께 체크 포인팅, 유휴, 종료, 다시 시작의 과정을 수행
- ✓ 전송 계층이 종단 간의 논리적인 설정을 담당한다면 세션 계층은 이런 연결에 정보 교환을 효과적으로 할 수 있게 추가 서비스를 함

■ 표현 계층(6계층)

- ✓ 코드 간의 번역을 담당, 인코딩이나 암호화 등을 6계층에서 담당
- ✓ ASN.1 방식
 - 사용자 시스템에서 데이터 구조를 하나의 통일된 형식으로 표현하여 응용 계층의 데이터 형식 차이로 인한 부담을 덜어줌
 - 응용 프로그램 계층 간의 서로 다른 표현을 인식하기 위해 정보를 정의하고 데이터의 압축과 암호화 기능을 수행

■ 응용 프로그램 계층(7계층)

- ✓ 사용자나 응용 프로그램 사이에 데이터 교환이 가능하게 하는 계층
- ✓ 응용 프로세스와 직접 관계하여 일반적인 응용 서비스를 수행
- ✓ HTTP, FTP, 터미널 서비스, 메일 프로그램, 디렉터리 서비스 등을 제공

2. 서비스 거부 공격 : DoS와 DDoS

서비스 거부 공격(DoS, **Denial** of Service)

- 다른 해킹에 비해 비교적 간단한 것으로 일종의 **훼방**
- 예를 들면 갯패가 노점상의 장사를 방해하는 것
- 집기를 부수거나 식재료의 공급을 끊거나 나쁜 재료를 음식에 몰래 섞는 것

분산 서비스 거부 공격(DDoS, **Distributed Denial** of Service)



서비스 거부 공격(DoS)

구분	설 명	공격 형태
취약점 공격형	특정 형태의 오류가 있는 네트워크 패킷의 처리 로직에 문제가 있을 때 공격 대상이 그 문제점을 이용하여 오작동을 유발하는 형태	<ul style="list-style-type: none"> ■ 보잉크 ■ 봉크 ■ 티어드롭 공격 ■ 랜드 공격
자원 고갈 공격형	네트워크 대역폭이나 시스템의 CPU, 세션 등의 자원을 소모시키는 형태	<p>랜드 공격, 죽음의 핑 공격, SYN 플러딩 공격, HTTP GET 플러딩 공격, HTTP CC 공격, 동적 HTTP 리퀘스트 플러딩 공격, 슬로 HTTP 헤더 DoS(슬로로리스) 공격, 슬로 HTTP POST 공격, 스머프 공격, 메일 폭탄 공격</p>

보잉크(Boink) / 봉크(Bonk) / 티어드롭(TearDrop) 공격



- 프로토콜의 오류 제어 로직을 악용하여 시스템 자원을 고갈시키는 방식
- 보잉크, 봉크, 티어드롭은 공격 대상이 반복적인 재요청과 수정을 계속하게 함으로써 시스템 자원을 고갈시킴
- **TCP 프로토콜이 제공하는 오류 제거 기능**
 - ✓ 패킷의 순서가 올바른지 확인
 - ✓ 중간에 손실된 패킷이 없는지 확인
 - ✓ 손실된 패킷의 재전송을 요구



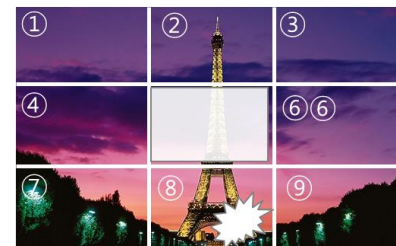
5번, 5번, 5번, 5번,...



2. 서비스 거부 공격 : DoS와 DDos

1 DoS(서비스 거부 공격)

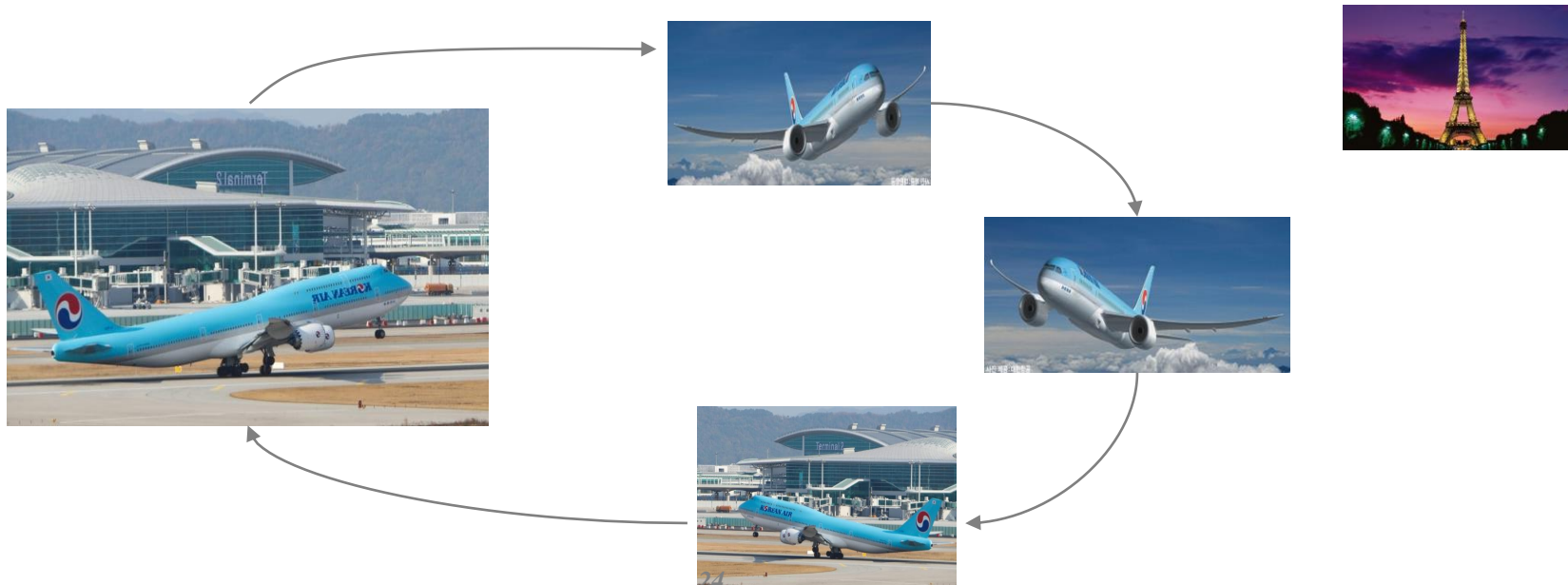
- TCP는 데이터 전송 시 신뢰를 확보하기 위해 패킷 전송에 문제가 있으면 반복적으로 재요청과 수정을 함
- 티어드롭**은 패킷의 시퀀스 넘버와 길이를 조작하여 **패킷 간의 데이터 부분이 겹치거나 빠진 상태로 패킷을 전송하는 공격 방법**
- 시퀀스 넘버가 조작된 패킷의 흐름은 공격 대상에게 **절대로 풀 수 없는 퍼즐**을 던져주는 것과 같음
- 이런 **취약점은 패치 처리를 통해 과부하가 걸리거나 계속 반복되는 패킷을 무시하고 버리도록 처리**



패킷 번호	정상 패킷의 시퀀스 넘버	공격을 위한 패킷의 시퀀스 넘버
1	1~100	1~100
2	101~200	81~180
3	201~300	230~320
4	301~400	250~340

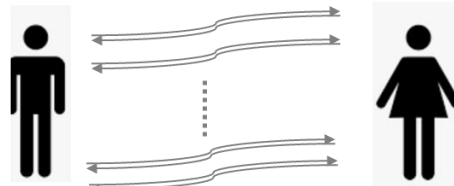
랜드(Land) 공격

- Land : '땅', '착륙하다'라는 뜻 외에 '(나쁜 상태에) 빠지게 하다'
- 패킷 을 전송할 때 출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만들어서 공격
- 이 공격법은 SYN 플러딩처럼 동시 사용자 수를 점유하고 CPU 부하를 올려서 시스템 이 금방 지쳐버리게 만듦
- 랜드 공격에 대한 보안 대책은 주로 운영체제의 패치 관리를 통해 해결(출발지 IP 주소와 목적지 IP 주소 동일한 전송 배제)



죽음의 핑(Ping) 공격

- NetBIOS 해킹과 함께 시스템을 파괴하는 데 가장 흔히 쓰인 초기의 DoS 공격 방법
- **ping 명령** : 네트워크의 연결 상태를 점검 명령어
- ping을 보낼 때 공격 대상에게 패킷을 **최대한 길게 보내 패킷을 꼬임**, 공격 대상 시스템은 대량의 작은 패킷을 수신하느라 네트워크가 마비
- 죽음의 핑 공격을 막는 방법 : ping이 내부 네트워크에 들어오지 못하도록 방화벽에서 ICMP를 차단해야 함
 - ✓ **ICMP**: ping이 사용하는 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 오류를 알려주는 프로토콜



```
C:\Users\Administrator>ping ut.ac.kr

Ping ut.ac.kr [210.119.144.5] 32바이트 데이터 사용:
요청 시간이 만료되었습니다.
요청 시간이 만료되었습니다.
요청 시간이 만료되었습니다.
요청 시간이 만료되었습니다.

210.119.144.5에 대한 Ping 통계:
패킷: 보냄 = 4, 받음 = 0, 손실 = 4 (100% 손실).

C:\Users\Administrator>ping chungju.go.kr

Ping chungju.go.kr [27.101.140.37] 32바이트 데이터 사용:
27.101.140.37의 응답: 바이트=32 시간=12ms TTL=49
27.101.140.37의 응답: 바이트=32 시간=10ms TTL=49
27.101.140.37의 응답: 바이트=32 시간=12ms TTL=49
27.101.140.37의 응답: 바이트=32 시간=13ms TTL=49

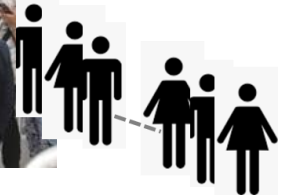
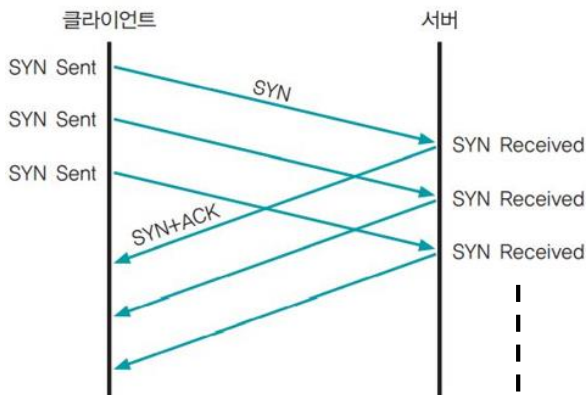
27.101.140.37에 대한 Ping 통계:
패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
최소 = 10ms, 최대 = 13ms, 평균 = 11ms
```

* NetBIOS는 Network Basic Input / Output System의 약어로 네트워킹 업계 표준

SYN 플러딩 공격

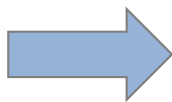
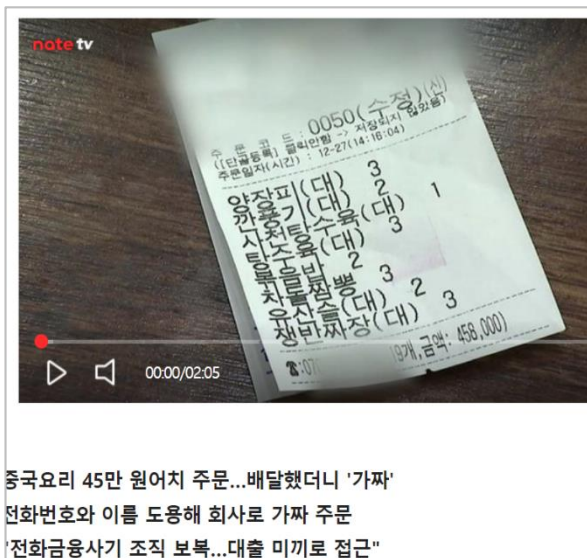
- 서비스를 제공하는 시스템에는 동시 사용자 수 제한을 이용한 공격.
- 존재하지 않는 클라이언트가 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 함.
- TCP의 연결 과정인 3-웨이 핸드셰이킹의 문제점을 악용하는 것.
- 특정 웹 서버의 접속자가 폭주, 서버 접속이 마비되는 경우도 이 공격과 유사
- 공격 대응책은 SYN Received의 대기 시간을 줄이는 것
- 침입 방지 시스템과 같은 보안 시스템으로도 공격을 쉽게 차단할 수 있음

3-웨이 핸드셰이킹



HTTP GET 플러딩 공격

- 공격 대상 시스템에 TCP 3-웨이 핸드셰이킹 과정으로 정상 접속한 뒤 HTTP의 GET 메소드로 특정 페이지를 무한대로 실행하는 공격
- 공격 패킷을 수신하는 웹 서버는 정상적인 TCP 세션과 정상으로 보이는 HTTP GET을 지속적으로 요청하므로 시스템에 과부하가 걸림



■ HTTP CC 공격

- ✓ HTTP 1.1 버전의 CC 헤더 옵션은 자주 변경되는 데이터에 새로운 HTTP 요청 및 응답을 요구하기 위해 캐시기능을 사용하지 않을 수 있음
- ✓ 서비스 거부 공격에 이를 응용하려면 'Cache-Control: no-store, must-revalidate' 옵션을 사용
- ✓ 이 옵션을 사용하면 웹 서버가 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가함

■ 동적 HTTP 리퀘스트 플러딩 공격

- ✓ 특징적인 HTTP 요청 패턴을 확인하여 방어하는 차단 기법을 우회하기 위한 공격
- ✓ 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청

■ 슬로 HTTP 헤더 DoS(슬로로리스) 공격

- ✓ 서버로 전달할 HTTP 메시지의 헤더 정보를 비정상적으로 조작
- ✓ 웹 서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지하도록 하는 공격
- ✓ 시스템 자원을 소비시켜 다른 클라이언트의 정상적인 서비스를 방해

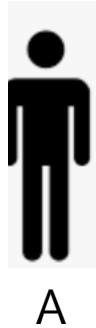
■ 슬로 HTTP POST 공격

- ✓ 웹 서버와의 커넥션을 최대한 오래 유지하여 웹 서버가 정상적인 사용자의 접속을 받아들일 수 없게 하는 공격

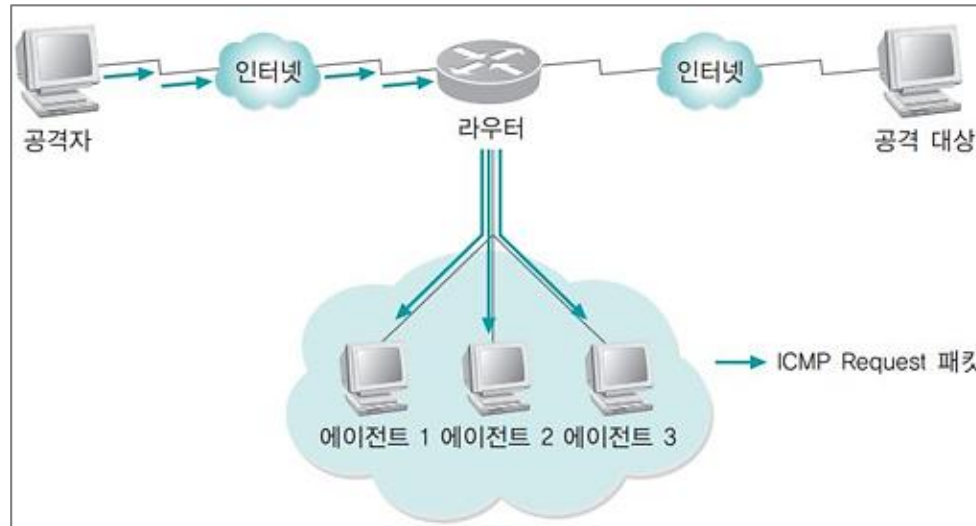
2. 서비스 거부 공격 : DoS와 DDos

1 DoS(서비스 거부 공격)

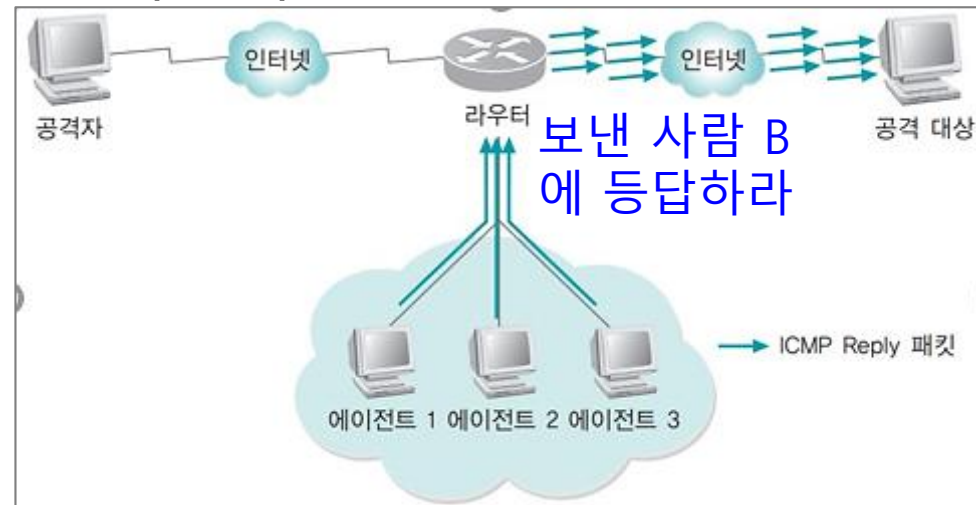
스머프 공격



브로드캐스트 개념



브로드캐스트 개념



분산 서비스 공격

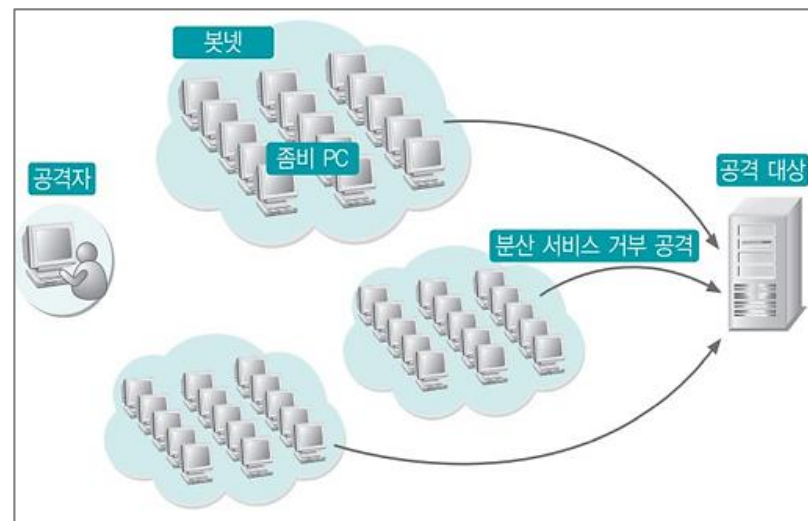
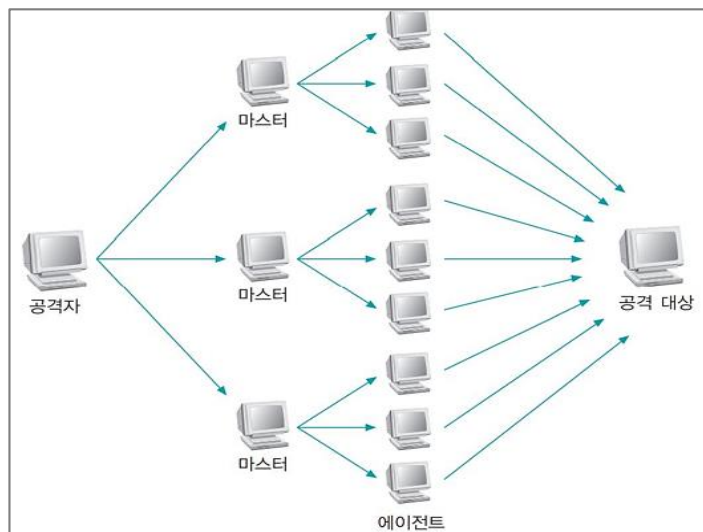
- **분산 서비스 거부 공격**(DDoS,Distributed Denial of Service attack)이란 특정 서버(컴퓨터)나 네트워크 장비를 대상으로 많은 데이터를 발생시켜 장애를 일으키는 대표적인 **서비스 거부 공격**
- 이 공격은 1999년 미네소타대학에서 처음 발생,야후, NBC, CNN 서버의 서비스를 중지
- 현재 확실한 대책이 없으며 공격자의 위치와 구체적인 발원지를 파악하는 것도 거의 불가능
- **분산 서비스의 기본 구성**
 - ✓ **공격자**: 공격을 주도하는 해커 컴퓨터
 - ✓ **마스터**: 공격자에게 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리
 - ✓ **핸들러 프로그램**: 마스터 시스템의 역할을 수행하는 프로그램
 - ✓ **에이전트** : 공격 대상에 직접 공격을 가하는 시스템
 - ✓ **데몬 프로그램**: 에이전트 시스템의 역할을 수행하는 프로그램

분산 서비스 공격과 사례(마포 경찰서)

- 분산 서비스 거부 공격을 위해 **사전에 공격 대상과 스케줄을 정한 뒤 이를 미리 작성한 악성 코드에 코딩**
- 인터넷을 통해 악성 코드를 전파 (**봇**: 분산 서비스 거부 공격에 사용되는 악성 코드)
- 전파 과정에서는 별다른 공격 없이 잠복
- 악성 코드에 감염된 PC를 **좀비 PC**라고 하며, 좀비 PC끼리 형성된 네트워크를 **봇넷**

* bot : 특정 작업을 반복 수행하는 프로그램

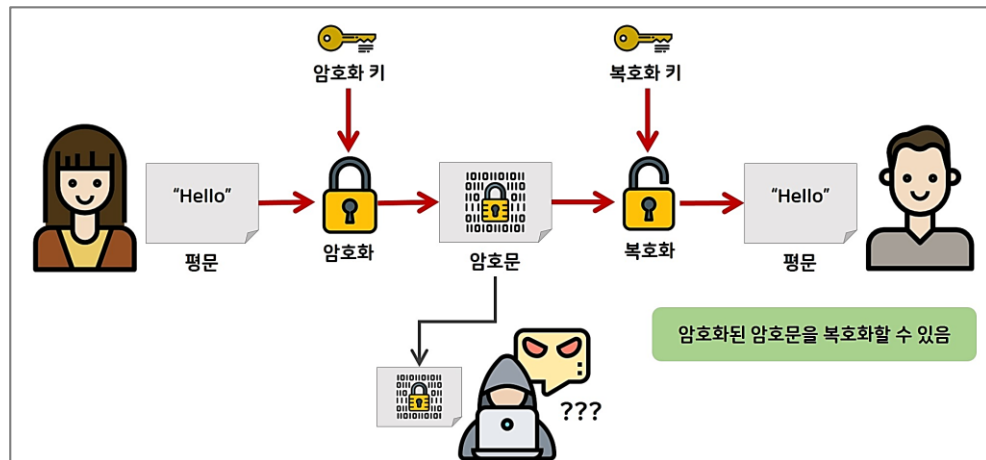
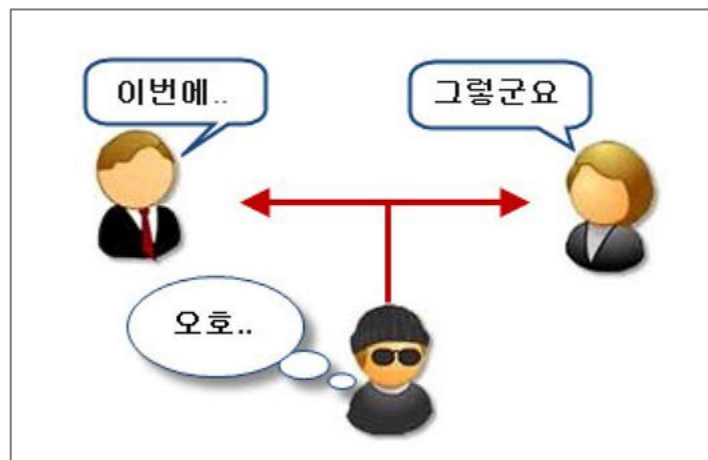
* botnet(사용자가 모르게 바이러스 같은 악성 소프트웨어의 통제를 받는 컴퓨터들)



3. 스니핑 공격

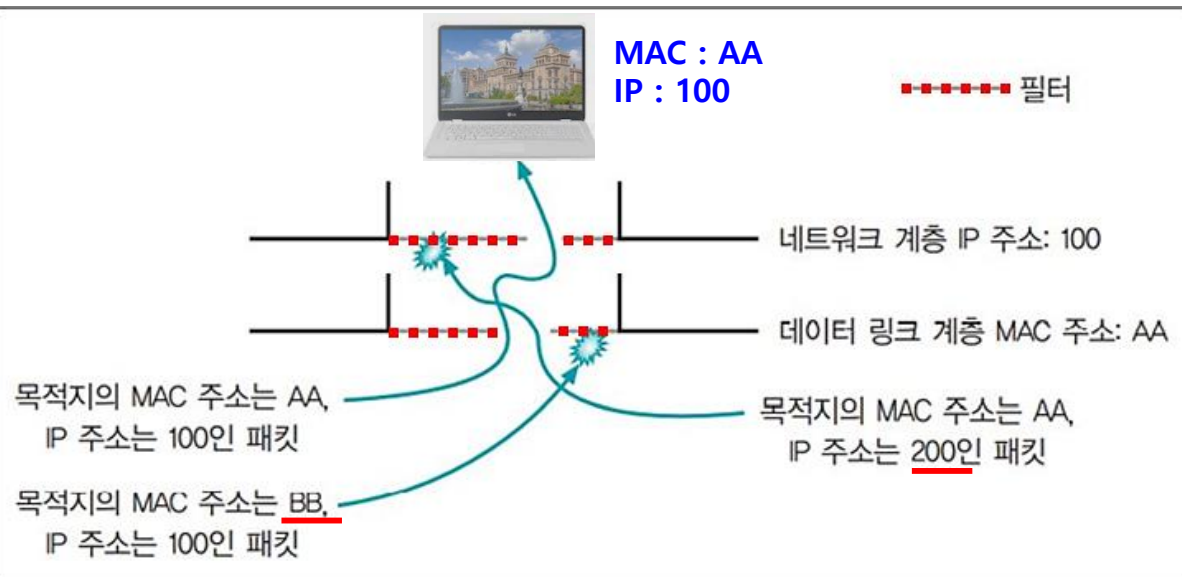
스니핑 공격 개요

- 다른 사람의 대화를 엿듣거나 **도청하는 행위**
- **공격 주요 목적 : 아이디와 패스워드 획득**
- 코를 킁킁거리면서 음식을 찾는 동물처럼 데이터 속에서 정보를 찾는 것
- 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 수동적 공격
 - ✓ 전화선이나 UTP에 태핑을 해서 전기적 신호를 분석하여 정보를 찾아내는 것
 - ✓ 전기적 신호를 템페스트 장비로 분석하는 것



스니핑 공격 개요

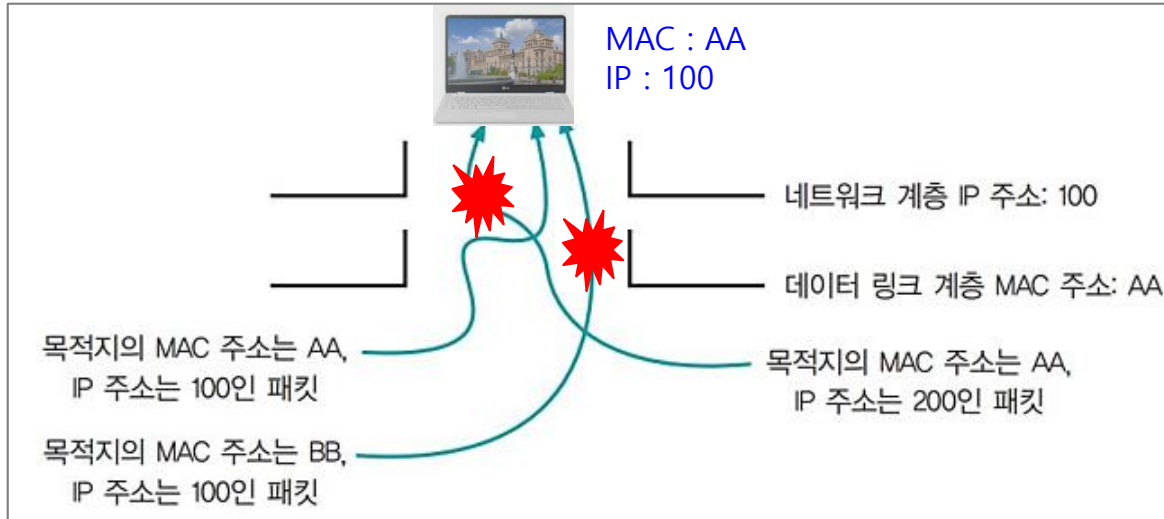
- 네트워크 카드는 패킷의 IP 주소와 MAC 주소를 인식하고 자신의 버퍼에 저장할지를 결정
- 네트워크 필터링은 네트워크 카드에 인식된 데이터 링크 계층과 네트워크 계층의 정보가 자신의 것과 일치하지 않는 패킷은 무시



정상적인 네트워크 필터링(예)

스니핑 공격 개요

- 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하므로 필터링이 방해됨
- 랜 카드의 설정 사항을 간단히 조정하거나 스니핑을 위한 드라이버를 설치하여 **프리미스큐어스** 모드로 변경



네트워크 필터링 해제 상태(프리미스큐어스 모드)(예)



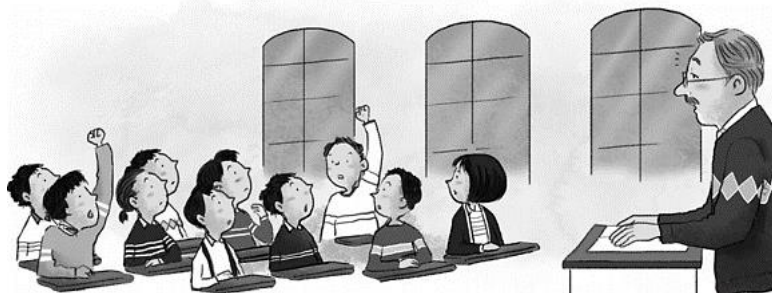
- ❖ **프리미스큐어스 모드**: 데이터 링크 계층과 네트워크 계층의 필터링을 해제하는 랜 카드의 모드

스니핑 공격 종류

- 스위치 재밍(Switch Jamming) 공격 (MACOF(MAC Flooding) 공격)
 - ✓ 스위치가 MAC 주소 테이블을 기반으로 패킷을 포트에 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격
 - ✓ 랜덤 형태로 생성한 MAC 주소를 가진 패킷을 스위치에 무한대로 보내 MAC 테이블의 저장 용량을 초과 시킴
 - ✓ 고가의 스위치는 MAC 테이블의 캐시와 연산자가 쓰는 캐시가 독립적으로 나뉘어 있어 통하지 않음
- SPAN 포트 태핑 공격
 - ✓ 스위치의 포트 미러링 기능을 이용
 - ✓ 포트 미러링이란 각 포트에 전송되는 데이터를 미러링하는 포트에도 같이 보내는 것
 - ✓ 침입 탐지 시스템을 설치하거나 네트워크 모니터링을 할 때 또는 로그 시스템을 설치할 때 많이 사용
 - ✓ SPAN 포트는 기본적으로 네트워크 장비에서 간단한 설정으로 활성화 되나 포트 태핑은 하드웨어 장비를 이용

스니핑 공격의 탐지

- 스니퍼를 설치한 이후에는 네트워크에 별다른 이상 현상을 일으키지 않기 때문에 사용자가 인지하기 어려움
- 스니퍼를 쉽게 탐지하려면 스니퍼가 **프리미스큐어스 모드에서 작동**한다는 점을 이용해야 함
- 스니퍼 탐지의 예시 (강의실에서 교수가 출석을 부를 때)
 - ✓ 친구의 출석을 대신 해주기로 한 학생은 자신의 이름이 호명되지 않았는데도 목소리를 바꿔서 대답
 - ✓ 두 명이 동시에 대답한다면 프리미스큐어스 모드인 학생은 교수에게 들리게 됨



스니핑 공격의 탐지

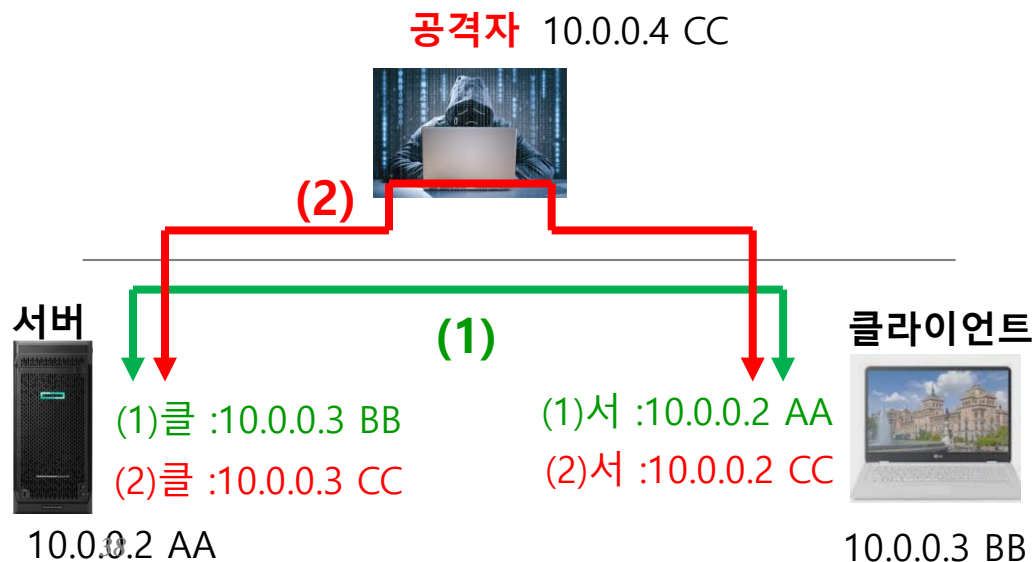
- 주소 결정 프로토콜(**ARP**, Address Resolution Protocol)은 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응(bind)시키기 위해 사용
- 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 **request**를 받으면 **response**를 전달
- 이를 이용하여 의심이 가는 호스트에 ping을 보내면 스니퍼를 탐지
- 이때 네트워크에 존재하지 않는 MAC 주소를 위장해서 전송
- 만약 ICMP echo reply를 받으면 해당 호스트가 스니핑을 하고 있는 것
- **ping을 이용한 스니퍼 탐지 종류(역으로 위조 된 자료 활용)**
 - ✓ ARP를 이용한 스니퍼 탐지 : ARP request 보내고 돌아오는 ARP reponse
 - ✓ DNS를 이용한 스니퍼 탐지 : ping sweep 보내고 돌아오는 반응 감시
 - ✓ 유인을 이용한 스니퍼 탐지 : 가짜 ID,PW 이용
 - ✓ ARP watch를 이용한 스니퍼 탐지 : 원본 IP,MAC 변경 감시

- **Spoofing 사전적 의미 '속이는 것'**
- 속이는 대상 : MAC 주소, IP 주소, 포트 등 네트워크 통신관련 모든 것.
- 목적 : 시스템 권한 얻기, 암호화된 세션 복호화, 네트워크 트래픽 흐름 변경

ARP 스푸핑의 개요

- ARP 스푸핑은 MAC 주소를 속이는 것
- 주소 결정 프로토콜(ARP, Address Resolution Protocol)은 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응(bind)시키기 위해 사용
- 로컬에서 통신하는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속임
- 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 랜의 통신 흐름을 왜곡

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



arp -a : 주소 확인

arp -s [IP 주소] [MAC 주소] : 주소 고정

C:\W>arp -a

인터페이스: 199.133.33.331 --- 0xe

인터넷 주소

199.111.11.1

199.222.22.255

10.0.0.2

224.0.0.251

224.0.0.252

239.255.255.250

255.255.255.255

C:\W>arp -a

인터페이스:

인터넷 주소

199.111.11.1

199.222.22.255

10.0.0.2

224.0.0.251

224.0.0.252

239.255.255.250

255.255.255.255

C:\W>arp -a

인터페이스: 199.133.33.331 --- 0xe

인터넷 주소

199.111.11.1

199.222.22.255

10.0.0.2

224.0.0.251

224.0.0.252

239.255.255.250

255.255.255.255

물리적 주소

04-09-a5-0c-0c-ed

ff-ff-ff-ff-ff

AA

01-00-5e-00-00-fb

01-00-5e-00-00-fc

01-00-5e-7f-ff-fa

ff-ff-ff-ff-ff

유형

동적

정적

고정

정적

정적

정적

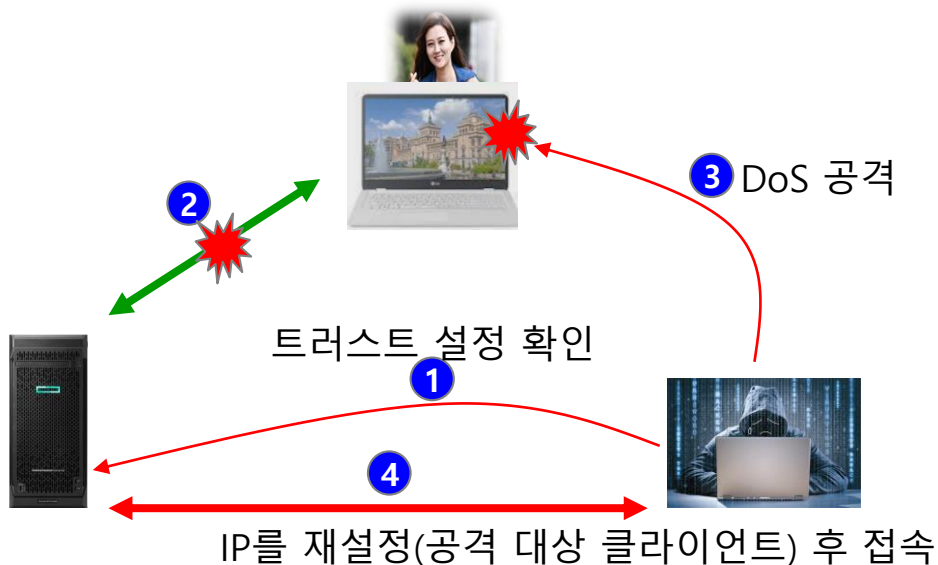
정적

■ IP 스푸핑의 개요

- IP 스푸핑은 IP 주소를 속이는 것으로, 다른 사용자의 IP를 강탈하여 어떤 권한을 획득
- 트러스트를 맺고 있는 서버와 클라이언트를 확인한 후 클라이언트에 서비스 거부 공격을 하여 연결을 끊음
- 클라이언트의 IP 주소를 확보하여 실제 클라이언트처럼 패스워드 없이 서버에 접근
- 트러스트 (신뢰 관계)
 - ✓ 클라이언트의 정보를 서버에 미리 기록함
 - ✓ 합당한 클라이언트가 서버에 접근하면 아이디와 패스워드의 입력없이 로그인을 허락하는 인증법
 - ✓ 유닉스에서는 주로 트러스트 인증법 사용, 윈도우에서는 트러스트 대신 액티브 디렉터리를 사용



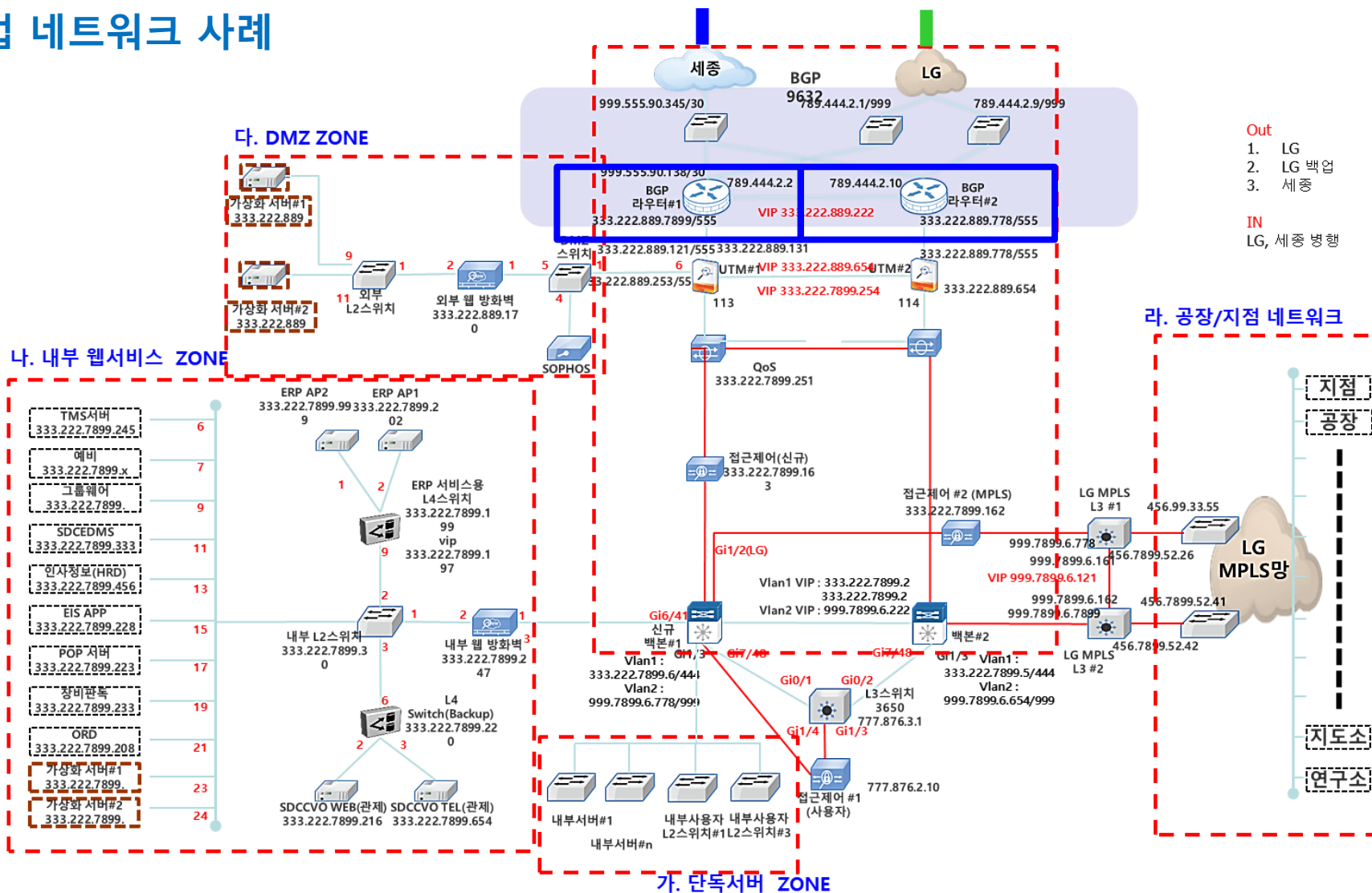
- 트러스트를 설정하려면 유닉스에서는 /etc/host.equiv 파일에 클라이언트의 IP와 접속 가능한 아이디를 등록
 - ✓ 10.0.0.3 root, 10.0.0.3 +, ++
- 공격자가 해당 IP를 사용하여 접속하면 스니핑으로 패스워드를 알아낼 필요가 없음
 - ✓ 공격자는 제로 트러스트로 접속한 클라이언트에 서비스 거부 공격을 수행하여 클라이언트의 IP의 네트워크 출연을 막음
 - ✓ 그 후 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 공격
- IP 스푸핑 공격에 대한 대응책은
트러스트를 이용하지 않는 것



4. 스푸핑 공격

3 ICMP 리다이렉트 공격

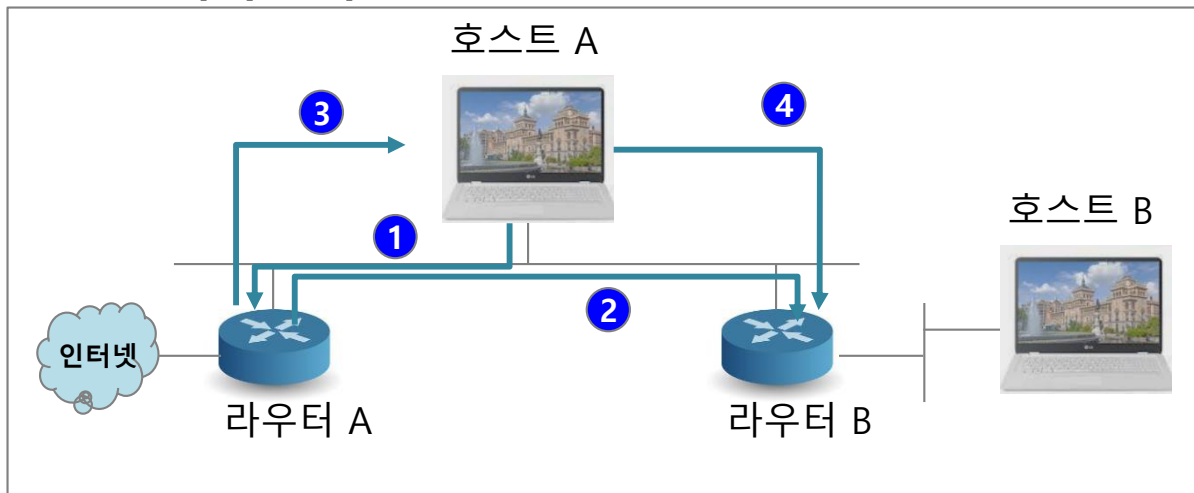
기업 네트워크 사례



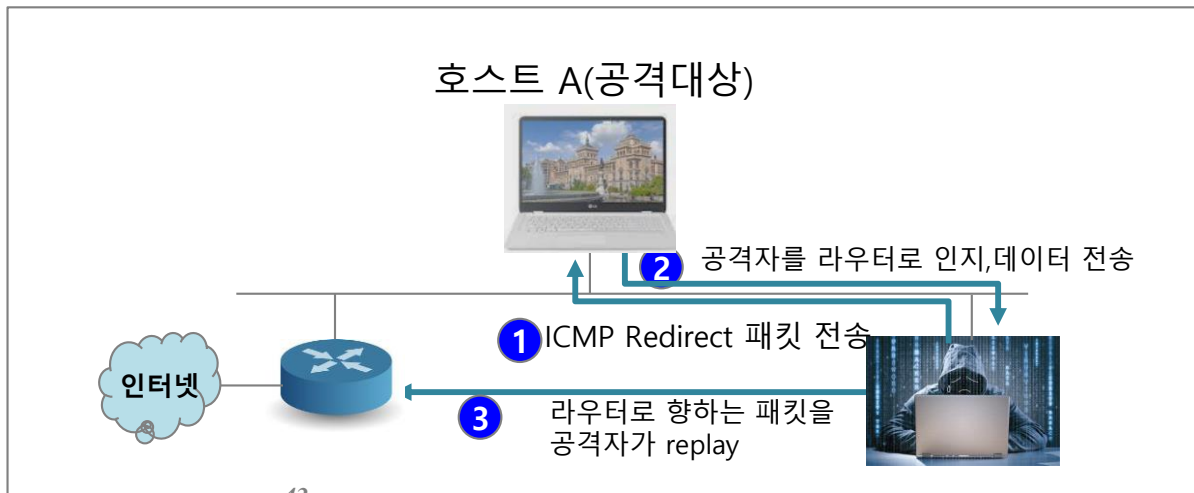
* 인터넷 제어 메시지 프로토콜(ICMP, Internet Control Message Protocol)

- 네트워크 계층에서 스푸핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알려 패킷의 흐름을 바꾸는 공격.
- ICMP 리다이렉트 동작.
- ICMP 리다이렉트 공격.

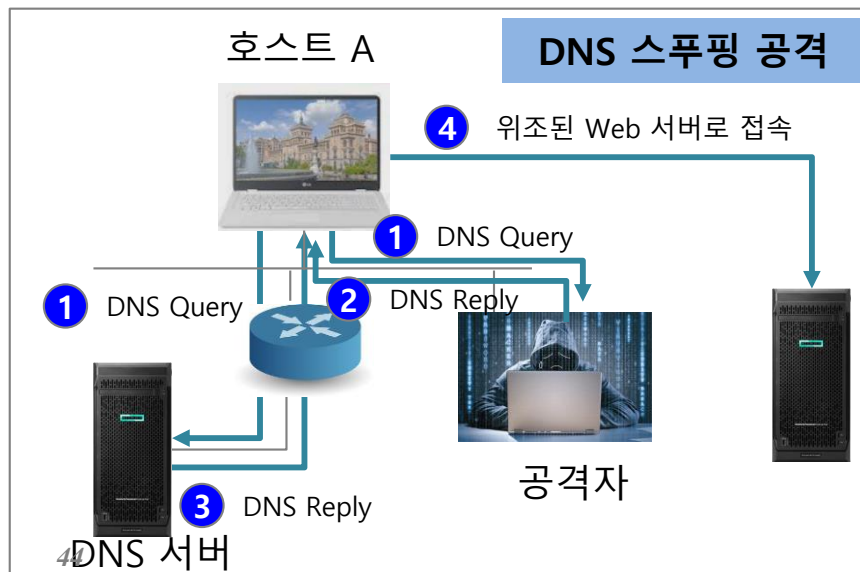
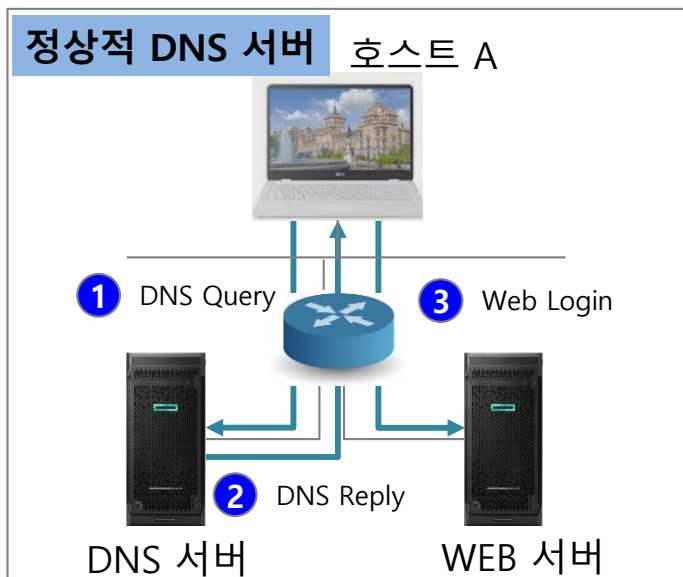
ICMP 리다이렉트 동작



ICMP 리다이렉트 공격



- 실제 DNS 서버보다 빨리 공격 대상에게 DNS response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격
- 인터넷 익스플로러에 사이트 주소를 입력하고 Enter를 눌렀을 때 다른 사이트가 뜨는 경우
- DoS 공격이 되지만 이를 조금만 응용하면 웹 스푸핑이 됨
 - ✓ 자신의 웹 서버를 하나 만들고 공격 대상이 자주 가는 사이트를 하나 골라서 웹 크롤러를 이용해 해당 사이트를 긁어옴
 - ✓ 아이디와 패스워드를 입력받아 원래 사이트로 전달해주는 스크립트를 프로그래밍
 - ✓ 공격 대상은 사이트 주소를 입력하고 자신의 아이디와 패스워드를 입력하여 해킹 당함



DNS 스푸핑을 막는 대응책

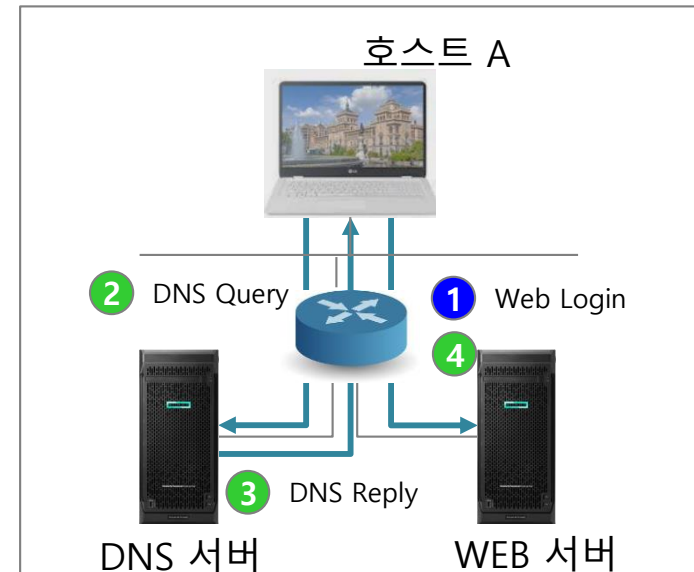
- 맨 먼저 시스템 메모리의 정보 활용
- 다음으로 다음과 같이 hosts 파일에 등록된 정보 확인
- hosts 파일에는 다음과 같은 정보 등록
- 모든 정보 등록 사실상 불가

127.0.0.1 localhost

210.119.144.25 www.ut.ac.kr

27.101.140.37 www.chungju.go.kr

210.104.148.81 www.chungbuk.go.kr



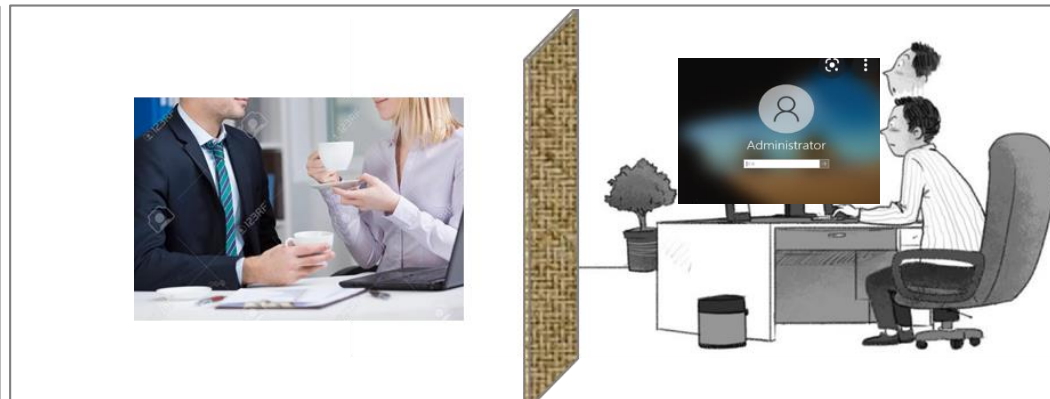
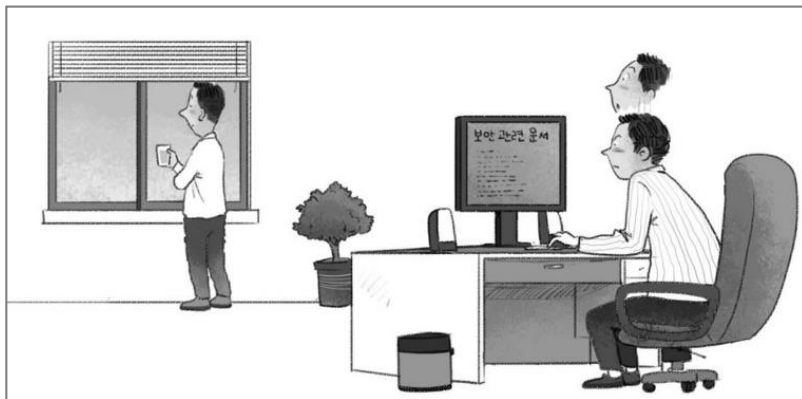
5. 세션 하이재킹 공격

세션 하이재킹 : 세션 가로채기

- 세션: 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 상태
- 세션 하이재킹은 두 시스템 간의 연결이 활성화된 상태, 즉 로그인된 상태를 가로챌
- 가장 쉬운 세션 하이재킹은 누군가 작업을 하다가 잠시 자리를 비웠을 때 몰래 PC를 사용하여 원하는 작업을 하는 것

현실 세계에서 세션 하이재킹을 하려면 몇가지 조건들이 충족되어야함

- 대상이 자리를 비움, 화면 잠금을 설정하지는 않음, 내가 접속하고자 하는 세션에 접속한 채로 자리를 비움



5. 세션 하이재킹 공격

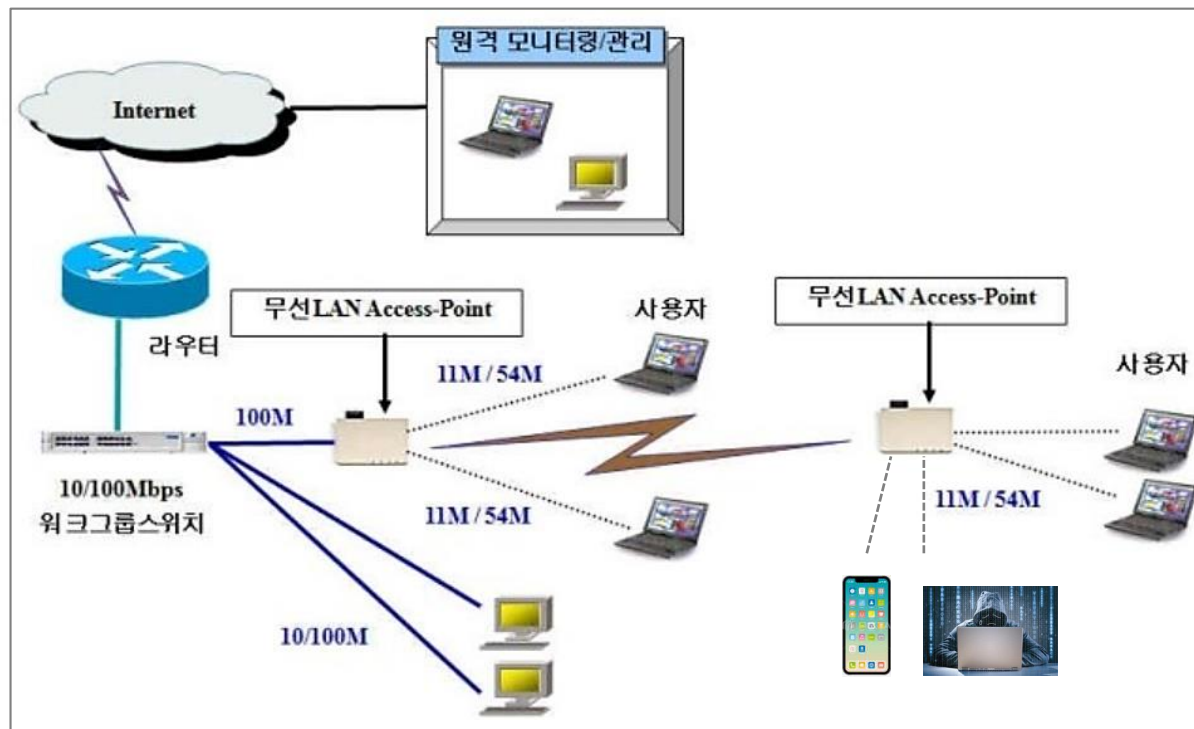
TCP 세션 하이재킹 : TCP가 가지고 있는 고유한 취약점 이용

- TCP 세션 하이재킹은 서버와 클라이언트에 잘못된 시퀀스 넘버를 혼란을 준 뒤 자신이 끼어드는 방식
- TCP 세션 하이재킹의 기본적인 단계
 - ① 클라이언트와 서버 사이의 패킷을 통제
 - ✓ ARP 스푸핑 등으로 클라이언트와 서버 간의 통신 패킷을 공격자를 지나가게 함
 - ② 서버에 클라이언트 주소로 연결을 재설정하기 위한 RST(reset) 패킷을 보냄
 - ✓ 서버는 패킷을 받아 클라이언트의 시퀀스 넘버가 재설정된 것으로 판단하고 다시 TCP 3-웨이 핸드셰이킹을 수행
 - ③ 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받음
- MAC 주소를 고정하는 방법은 ARP 스푸핑을 막아주기 때문에 결과적으로 세션 하이재킹을 막을 수 있음

6. 무선 네트워크 공격과 보안

무선 랜의 개요

- 유선 랜의 네트워크를 확장하려는 목적으로 사용(공장 적용 사례)
- 이를 위해서는 내부의 유선 네트워크에 **AP 장비**를 설치해야 함.
- 확장된 무선 네트워크는 AP를 설치한 위치에 따라 통신 영역이 결정
- **보안이 설정되어 있지 않으면** 공격자가 통신 영역 안에서 내부 사용자와 같은 권한으로 공격 가능
- 무선 랜의 전송 가능 길이는 수신 안테나의 형태에 따라 다르지만 짧게는 수십m에서 길게는 1~2Km까지도 가능

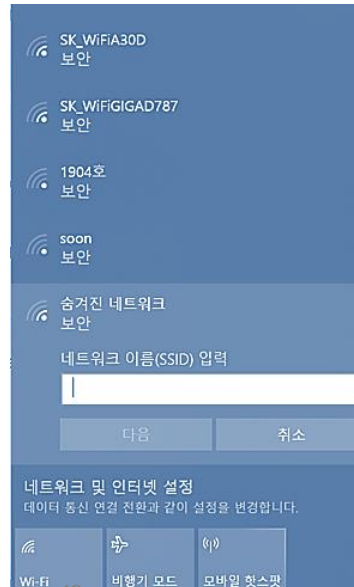
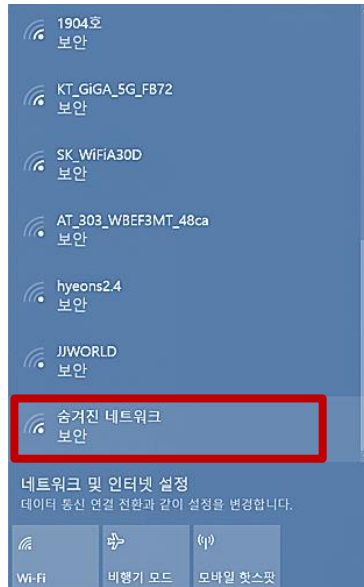


■ 물리적인 보안 및 관리자 패스워드 변경

- ✓ AP는 전파가 건물 내에 한정되도록 전파 출력을 조정
- ✓ 건물 안쪽 눈에 쉽게 띄지 않는 곳에 설치 후 AP의 기본 계정과 패스워드를 반드시 재설정

■ SSID(Service Set Identifier) 브로드캐스팅 금지

- ✓ SSID: 무선 랜 네트워크를 검색 시 확인할 수 있는 AP목록 중 이름으로 표시된 것
- ✓ 무선 랜에서 AP의 존재를 숨기고 싶으면 SSID 브로드캐스팅을 막고 사용자가 SSID를 입력해야 AP에 접속 가능하게 함, 높은 수준의 보안 권한이 필요 시 **SSID 브로드캐스팅을 차단**



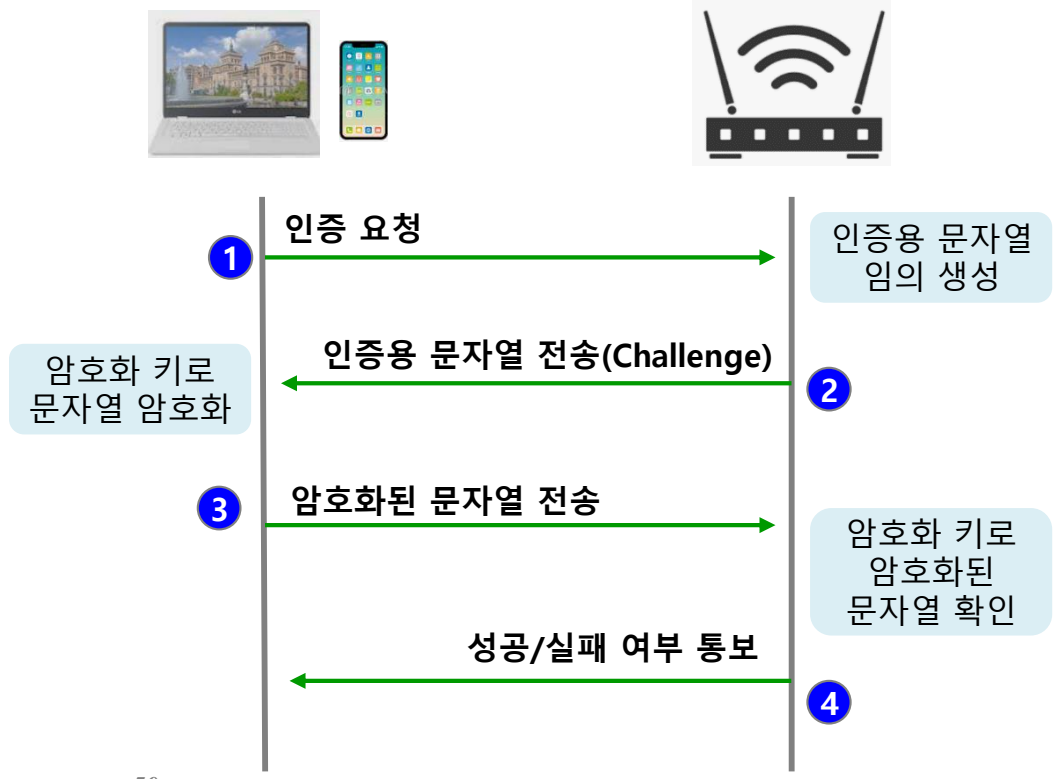
6. 무선 네트워크 공격과 보안

2 무선 랜 통신의 암호화

- 무선 랜은 통신 과정에서 데이터 유출을 막는 것뿐 아니라 네트워크에 대한 인증을 위해서도 **암호화를 수행**
- 암호화된 통신을 수행하는 네트워크에 접근을 시도하면 [네트워크 보안 키 입력] 창이 나타남



WEP 암호화 세션의 생성

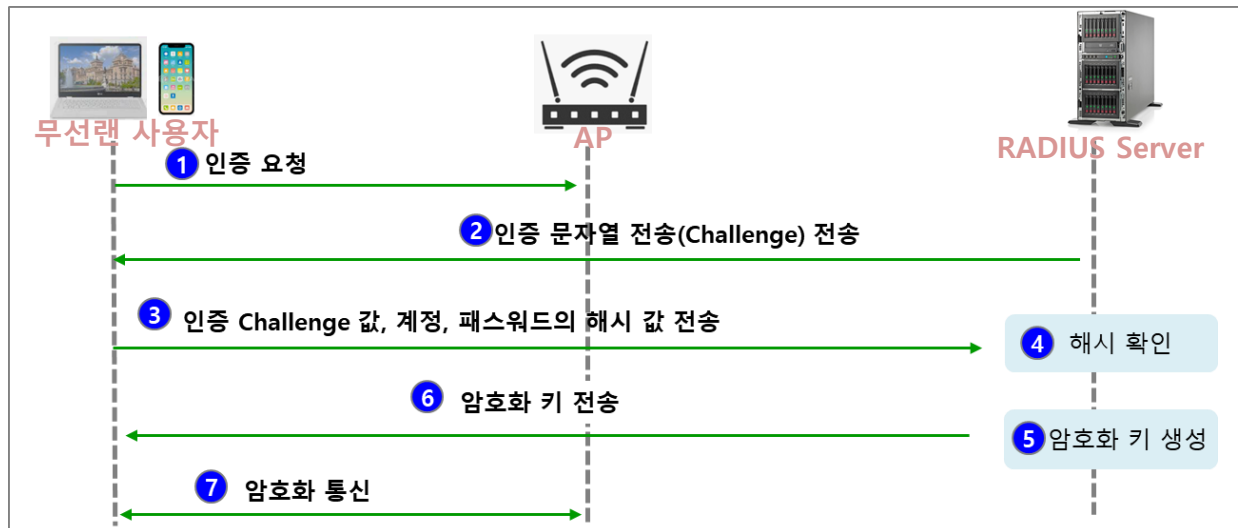


- WEP(Wired Equivalent Privacy)
- WPA-PSK
- EAP와 802.1x 암호화

6. 무선 네트워크 공격과 보안

2 무선 랜 통신의 암호화

- 물리적인 보안을 유지하고 관리자 패스워드 변경
- SSID 브로드캐스팅 금지
- WEP 암호화 : 128 비트 키까지 암호화 키를 제공
- WPA-PSK 암호화 : WEP 암호화의 취약점을 해결한 암호화 방식
- EAP와 802.1x 암호화 : EAP는 무선 랜 클라이언트와 RADIUS 서버 간의 통신을 가능하게 하는 프로토콜이고, 802.1x는 포트에 대한 접근을 통제하는 프로토콜



RADIUS와 802.1x를 이용한 무선랜 인증

* 레이드어스 서버(RADIUS Server)는 원격지 이용자의 접속 요구 시 이용자 ID나 패스워드, IP주소 등의 정보를 인증 서버에 보내어 이용자의 식별 및 인증을 실행하는 것을

6. 무선 네트워크 공격과 보안

2 무선 랜 통신의 암호화

인터넷·정보보호 실천 수칙
(스마트폰 보안수칙 10)

<https://www.kisa.or.kr/60801>

일상에서 지켜주세요

스마트폰 보안수칙 10

- 01** 스마트폰 운영체제와 모바일 백신 최신으로 업데이트하기
- 02** 공식 앱 마켓이 아닌 다른 출처의 앱 설치 제한하기 (출처를 알 수 없는 앱)
- 03** 스마트폰 앱 설치 시 과도한 권한을 요구하는 앱은 설치하지 않기
- 04** 문자 또는 SNS 메시지에 포함된 URL 클릭하지 않기
- 05** 스마트폰 보안 잠금을 설정하여 이용하기 (비밀번호 또는 화면 패턴)
- 06** 스마트폰 WiFi 연결 시 제공자 불분명한 공유기 이용하지 않기
- 07** 루팅, 탈옥 등을 통한 스마트폰 플랫폼의 구조 임의변경 금지
- 08** 스마트폰에 중요정보 저장하지 않기 (주민등록증, 보안카드 등)
- 09** 스마트폰 교체 시 개인정보 등 데이터 완전삭제 혹은 초기화 적용
- 10** 스마트폰, SNS 등 계정 로그인 2단계 인증 설정하기

국가정보원
과학기술정보통신부
KISA 한국인터넷진흥원

Thank you

INFORMATION SECURITY

