

네트워크 보안

[참고자료 – 정보보안개론 한빛아카데미(주)]

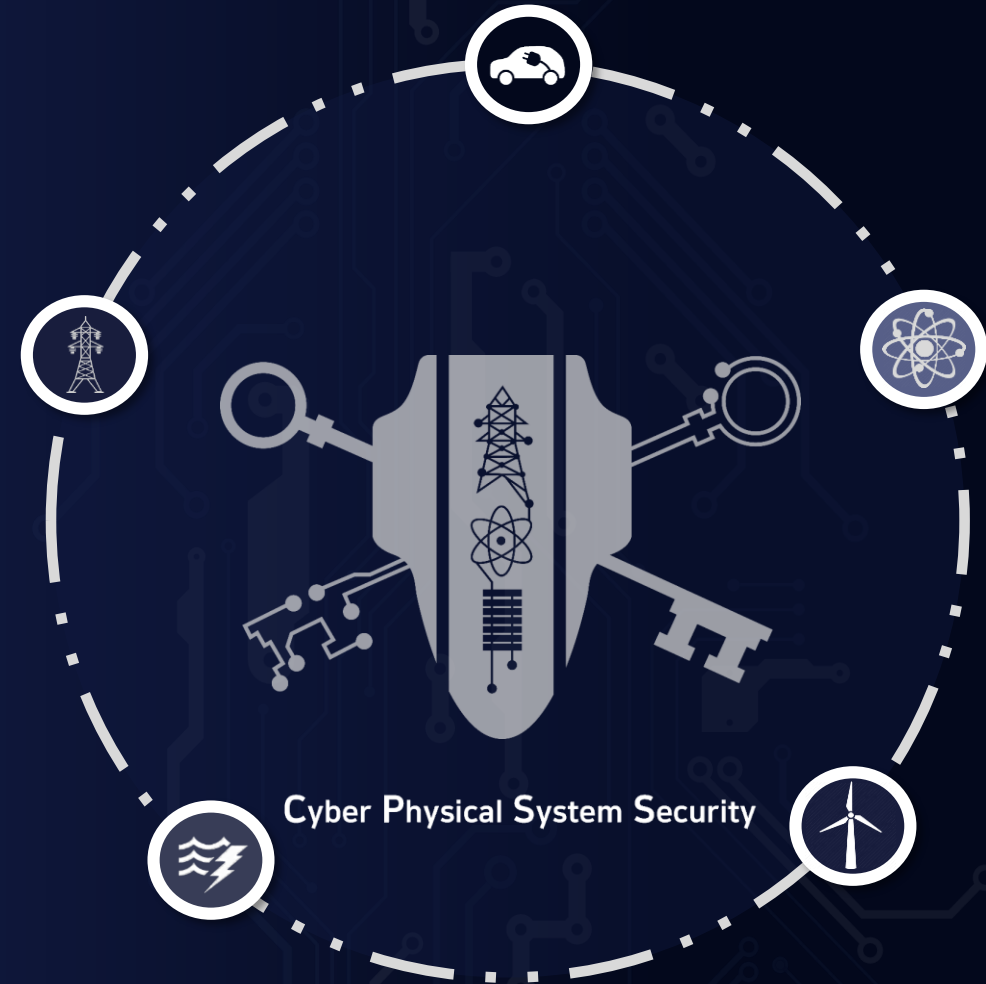
서정택

가천대학교 컴퓨터공학부 스마트보안전공 교수

가천대학교 CPS보안연구센터 센터장

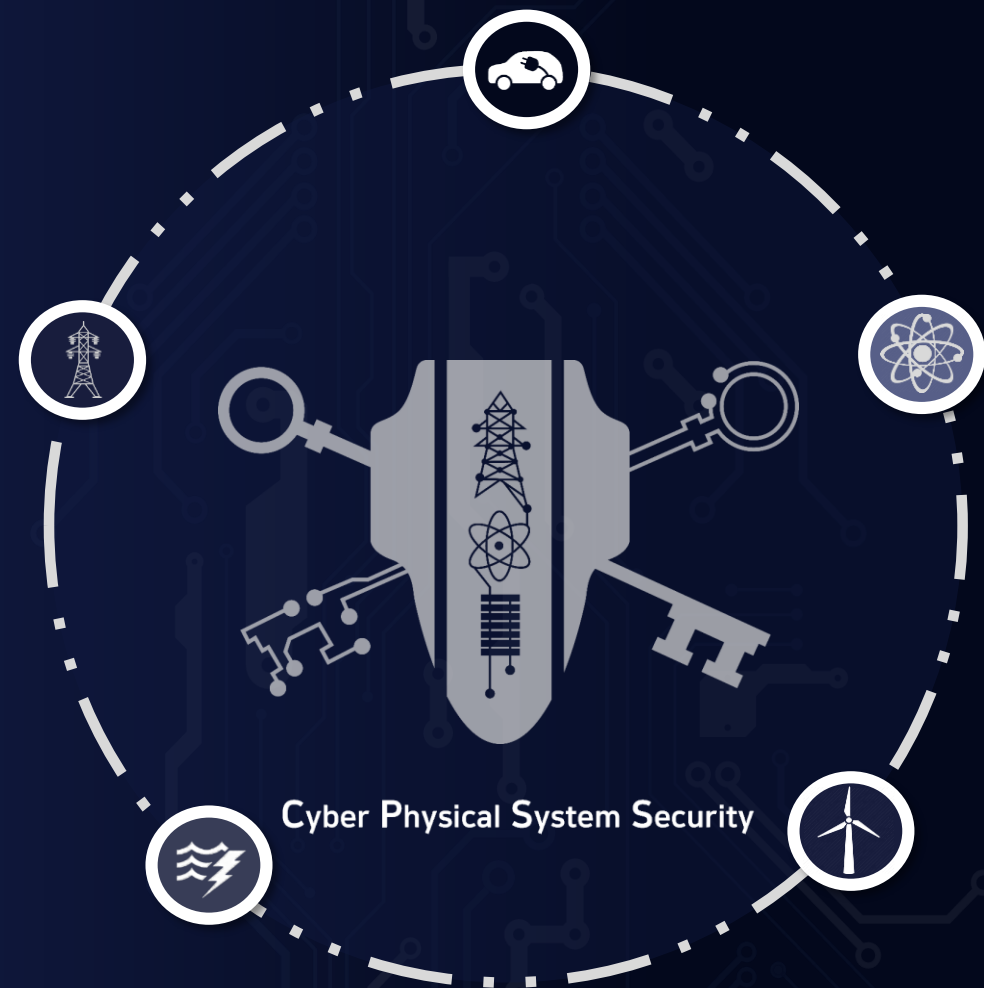
한국정보보호학회 CPS보안연구회 위원장

seojt@gachon.ac.kr



CONTENTS

- 01 네트워크에 대한 이해
- 02 서비스 거부(Dos) 공격
- 03 스니핑 공격
- 04 스푸핑 공격
- 05 세션 하이재킹 공격
- 06 무선 네트워크 공격과 보안



01. 네트워크에 대한 이해



OSI 7계층

- 국제표준화기구(ISO : International Organization for Standardization)에서 다양한 네트워크의 호환을 위해 만든 표준 네트워크 모델

계층	OSI 7 계층 모델 [PDU]	내용
7계층	응용 계층 [Data] (Application Layer)	<ul style="list-style-type: none"> 사용자에게 서비스 제공 역할 DHCP, DNS, SMTP, FTP, HTTP 등 사용자가 원하는 최종 목표에 해당
6계층	표현 계층 [Data] (Presentation Layer)	<ul style="list-style-type: none"> 데이터의 인코딩/디코딩, 압축/해제, 암호화/복호화 담당
5계층	세션 계층 [Data] (Session Layer)	<ul style="list-style-type: none"> 통신하는 프로세스 사이의 대화 제어 및 동기화 담당 연결 세션에서 데이터 교환과 에러 발생 시 복구 담당
4계층	전송 계층 [TCP - Segment, UDP - Datagram] (Transport Layer)	<ul style="list-style-type: none"> 종단 간 신뢰성 있는 데이터 전송을 담당 오류 검출, 복구, 흐름제어, 중복검사 수행 데이터 전송을 위해 Port 번호를 사용
3계층	네트워크 계층 [Packet] (Network Layer)	<ul style="list-style-type: none"> 종단 간 전송을 위한 경로 설정을 담당(IP주소 사용) 호스트로 도달하기 위한 최적의 경로를 라우팅 알고리즘을 통해 선택하고 제어
2계층	데이터링크 계층 [Frame] (Datalink Layer)	<ul style="list-style-type: none"> 인접한 노드 간의 신뢰성 있는 데이터 전달 신뢰성을 위해 흐름제어, 오류제어, 회선제어 수행 MAC 주소를 통해서 통신
1계층	물리 계층 [Bit] (Physical Layer)	<ul style="list-style-type: none"> 물리매체를 통해 bit 흐름 전송 물리적으로 연결된 노드 간의 신호 전송

물리 계층(1계층)

- 인터넷 이용시의 랜 케이블, 전화선, 동축 케이블 또는 광 케이블 등의 시스템 간의 물리적인 연결매체
- Cat별 특성

구분	최대 속도	사용주파수(MHz)	용도
CAT 1	1Mbps 미만	음성주파수	<ul style="list-style-type: none">• 아날로그 음성(일반적인 전화 서비스)• 전화망(2Pair)에 사용
CAT 2	4Mbps	4	<ul style="list-style-type: none">• Multi Pair 통신케이블에 사용
CAT 3	16Mbps	16	<ul style="list-style-type: none">• 전화망 및 전산망에 사용
CAT 4	20Mbps	20	<ul style="list-style-type: none">• 전산망 전송속도가 증가하고 손실이 적어짐
CAT 5	100Mbps	100	<ul style="list-style-type: none">• 옥내 수평 및 간선 배선망(100MHz)• 디지털 전화망 및 전산망에 사용• 저손실, 광대역폭 케이블에 사용
CAT 6	250Mbps	200	<ul style="list-style-type: none">• 옥내 수평 및 간선 배선망(250MHz)• Gigabyte 이더넷• 영상신호 전송에 적합
CAT 7	10Gbps	500	

물리 계층(1계층)

케이블 선의 분류

구분	내용
UTP(Unshielded Twisted Pair)	<ul style="list-style-type: none">제품 전선과 피복만으로 구성두 선 사이의 전자기 유도를 줄이기 위해 절연의 구리선이 서로 꼬여 있음
FTP(Foil Screened Twisted Pair Cable)	<ul style="list-style-type: none">알루미늄 은박이 4가닥의 선을 감싸고 있음UTP보다 절연 기능이 탁월해 공장 배선용으로 많이 사용
STP(Shielded Twisted Pair Cable)	연선으로 된 전선 겉에 외부 피복 또는 차폐재가 추가된 케이블(шил드 처리)이다. 이때 차폐재는 접지의 역할을 하므로 외부의 노이즈를 차단하거나 전기적 신호의 간섭에 탁월하다.

커넥터에도 여러 가지 표준이 존재

- 랜 케이블의 연결 커넥터 : RJ 45
- 전화선의 연결 커넥터 : RJ 11



< RJ 45 >



< RJ 11 >

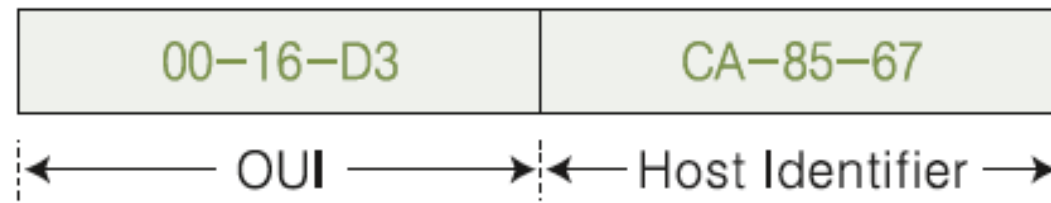
데이터링크 계층(2계층)

- 두 포인트 간의 신뢰성 있는 전송을 보장하기 위한 계층

- 네트워크 위의 개체 간에 데이터를 전달
- 물리 계층에서 발생할 수 있는 오류를 찾아내고 수정하는 데 필요한 기능적, 절차적 수단을 제공

MAC 주소

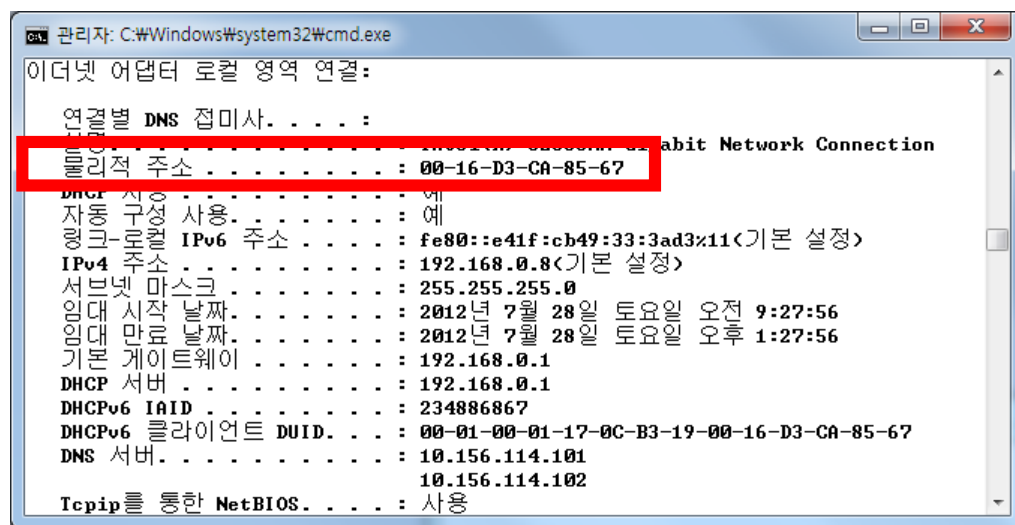
- 데이터 링크 계층에서는 상호 통신을 위해 MAC 주소를 할당 받음
- MAC 주소는 윈도우 명령 창에서 `ipconfig /all` 명령을 실행하여 확인
- MAC 주소는 총 12개의 16진수로 구성
- 앞쪽 6개의 16진수는 네트워크 카드를 만든 회사를 나타내는 것으로 OUI(Organizational Unique Identifier)라고 함
- 뒤쪽 6개의 16진수는 각 회사에서 임의로 붙이는 일종의 시리얼을 나타내는 것으로 Host Identifier 라고 함



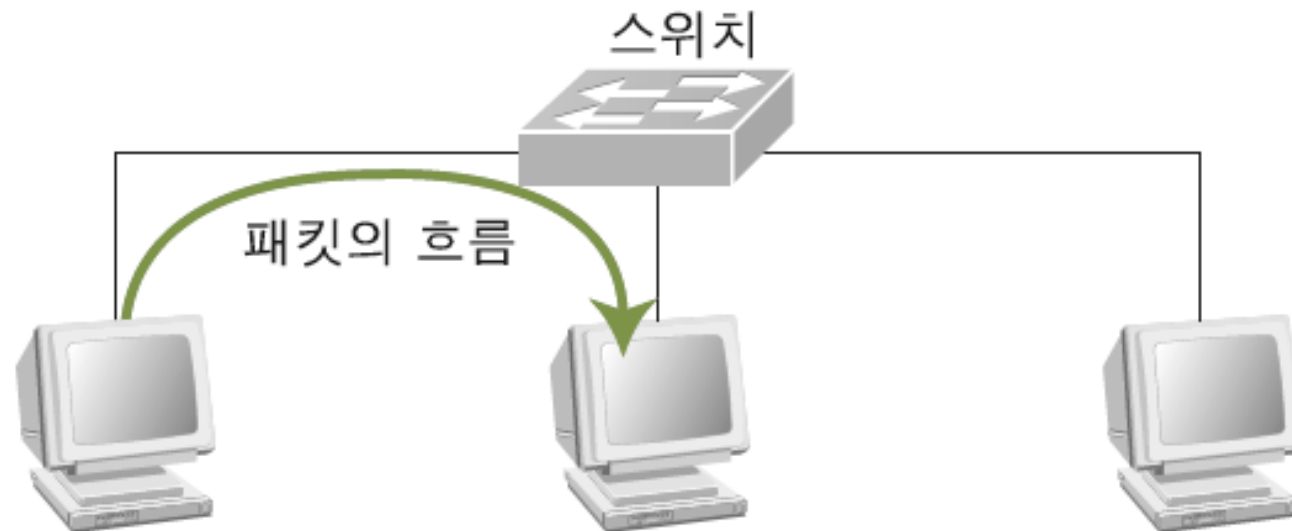
데이터링크 계층(2계층)

데이터링크 계층의 패킷 흐름

- 데이터 링크 계층의 대표적인 네트워크 장비는 스위치
- MAC 계층에서 동작하는 대표적인 프로토콜은 이더넷



[cmd에서 확인한 MAC 주소]



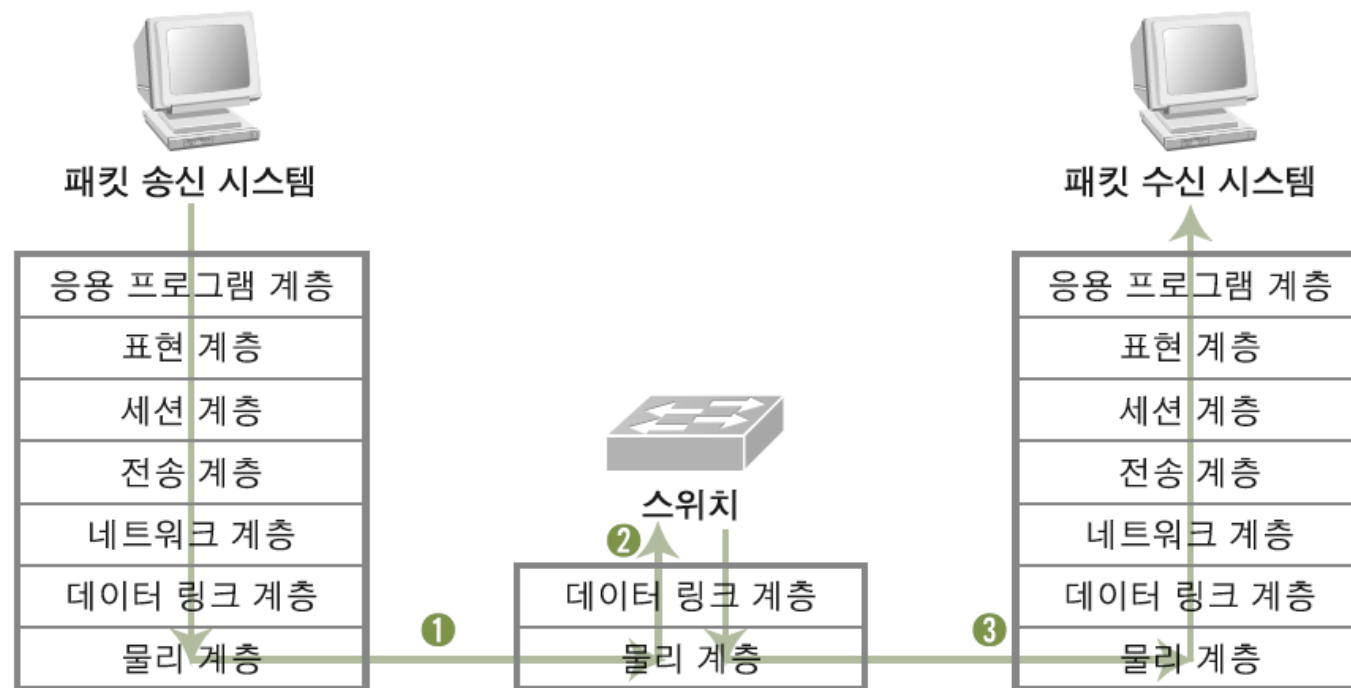
[데이터링크 계층의 패킷 흐름]

01. 네트워크에 대한 이해 – OSI 7계층

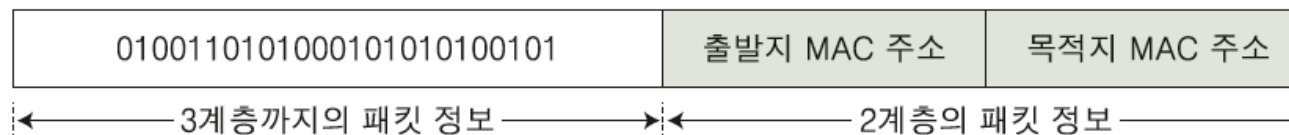


데이터링크 계층(2계층)

- 2계층에서의 OSI 계층의 패킷 흐름



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



네트워크 계층(3계층)

- 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층
 - 다양한 길이의 데이터를 네트워크를 통해 전달
 - 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::11f:eb49:33:3ad3::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
```

네트워크 계층(3계층)

IP 주소의 클래스

- IP주소는 A, B, C, D, E 클래스로 구분
 - A 클래스 : 첫 번째 자리가 네트워크 주소, 나머지 세 자리는 호스트 주소
 - B 클래스 : 두 번째 자리가 네트워크 주소, 나머지 두 자리는 호스트 주소
 - C 클래스 : 세 번째 자리가 네트워크 주소, 나머지 한 자리는 호스트 주소

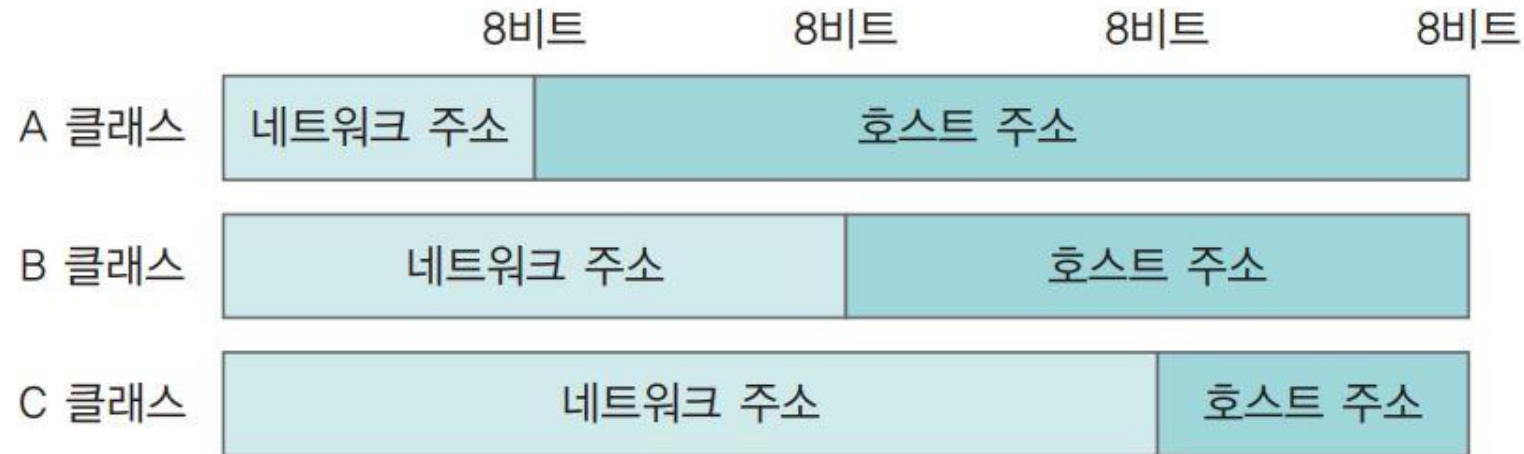


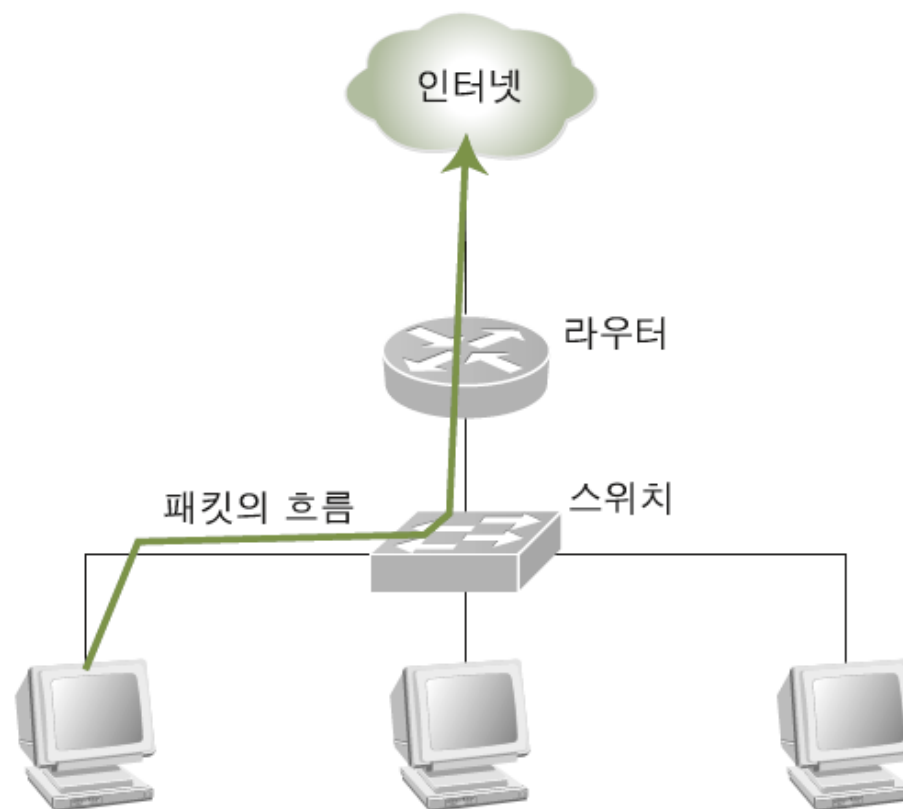
그림 3-8 IP 주소의 클래스

01. 네트워크에 대한 이해 – OSI 7계층



네트워크 계층(3계층)

- 2, 3계층에서의 패킷의 흐름

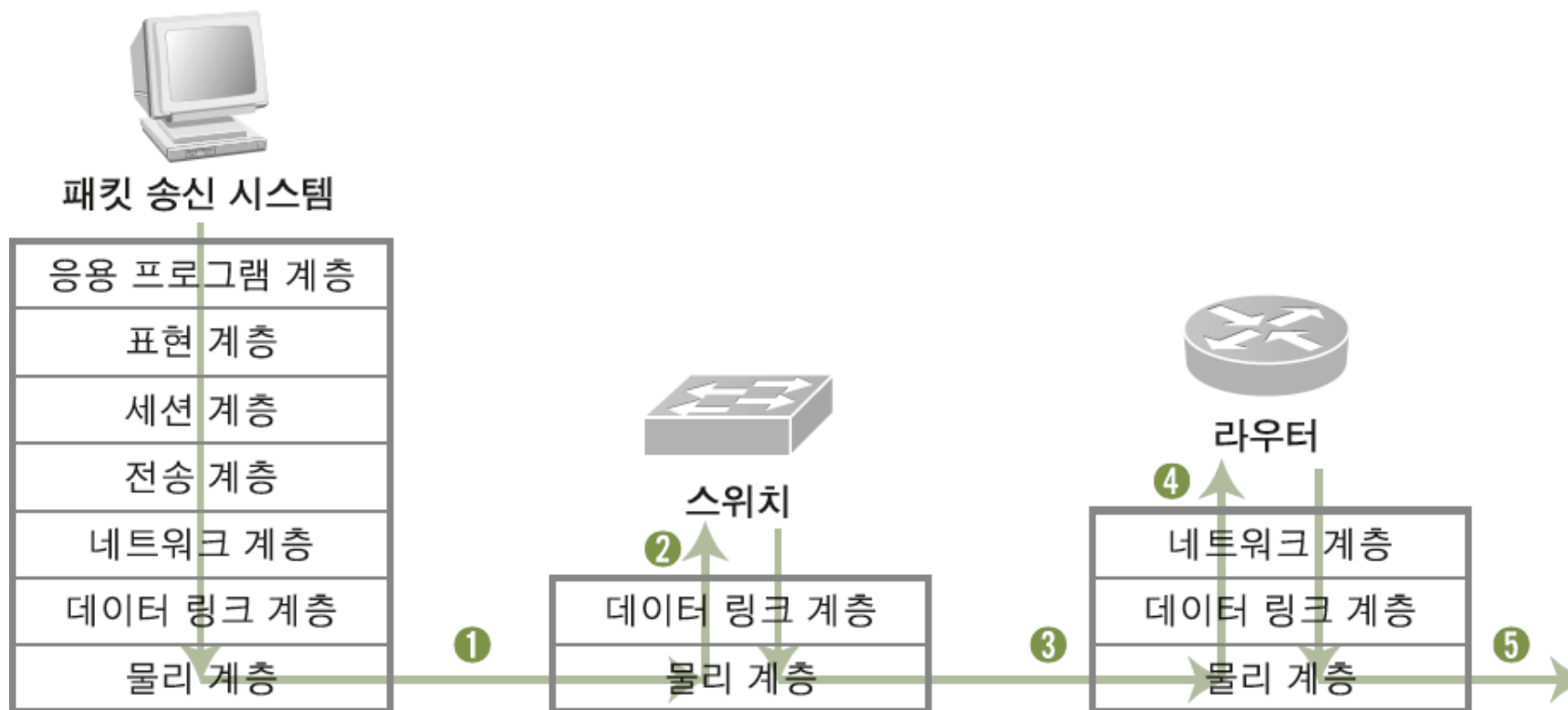


01. 네트워크에 대한 이해 – OSI 7계층



네트워크 계층(3계층)

- 2, 3계층에서의 패킷의 흐름 – OSI 7계층



네트워크 계층(3계층)

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

- 패킷 송신 시스템의 IP: 172.16.0.100
- 라우터 랜 쪽 포트의 IP(게이트웨이): 172.16.0.1
- 패킷 송신 시스템의 MAC 주소: AA-AA
- 라우터 랜 쪽 포트의 MAC 주소(게이트웨이): BB-BB
- 라우터 인터넷 쪽 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	

- 인터넷으로 전송하는 패킷의 기본 구조

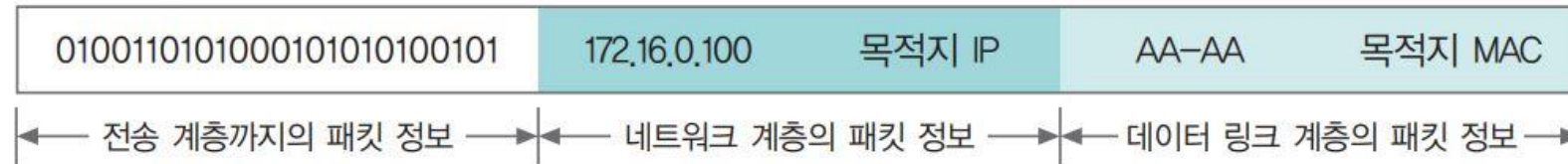


01. 네트워크에 대한 이해 – OSI 7계층

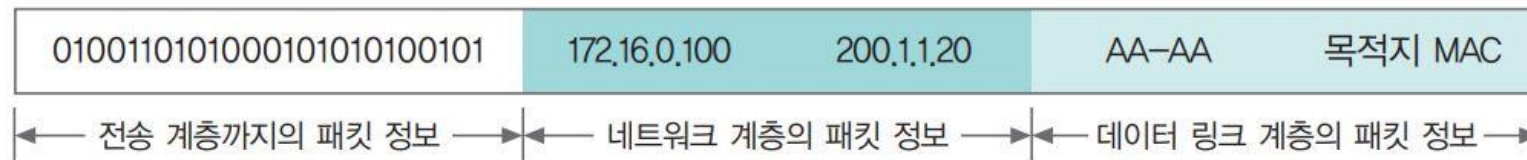
네트워크 계층(3계층)

네트워크 계층에서의 패킷 전달 구조

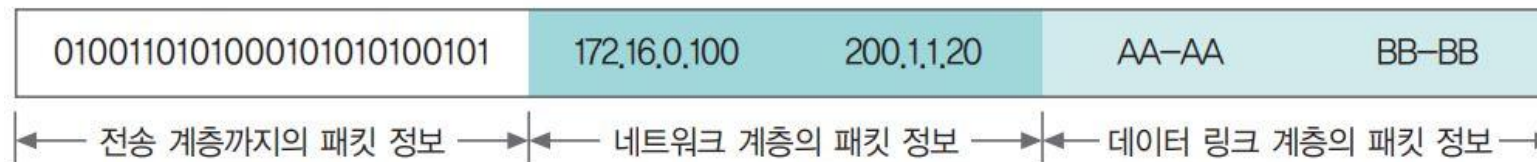
- 출발지의 IP와 MAC 주소가 기록됨



- 목적지 IP 주소 입력



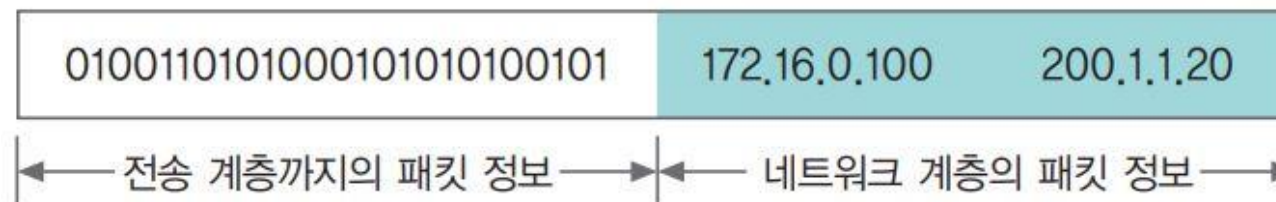
- 목적지 MAC 주소에는 랜을 벗어나기 위한 가장 일차적인 목적지, 즉 게이트웨이의 MAC 주소 입력
 - ARP 프로토콜 이용



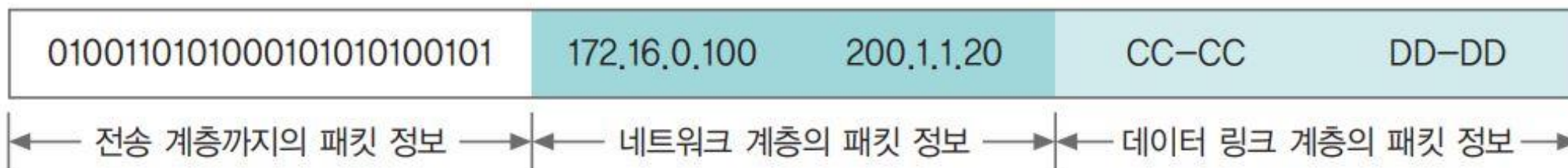
네트워크 계층(3계층)

네트워크 계층에서의 패킷 전달 구조

- 라우터에서 사용한 데이터 링크 계층 정보를 벗겨냄



- 다음 라우터까지의 데이터 링크 계층 정보를 패킷에 덧씌움



■ 전송 계층(4계층)

- 양 끝단(End to end)의 사용자들이 신뢰성 있는 데이터를 주고받을 수 있도록 함
 - 상위 계층이 데이터 전달의 유효성이나 효율성을 신경쓰지 않게해줌
 - 가장 잘 알려진 전송 프로토콜은 TCP(Transmission Control Protocol)
- **포트**
 - 시스템에 도착한 후 패킷이 찾아갈 응용 프로그램으로 통하는 통로 번호
 - 시스템에서 구동되는 응용 프로그램은 네트워킹을 하기 위해 자신에게 해당되는 패킷을 식별 할 때 사용
- 포트의 패킷 구조



전송 계층(4계층)

TCP

- 연결형(connection-oriented) 서비스로 연결이 성공해야 통신이 가능
- 데이터의 경계를 구분하지 않음, 이것을 바이트 스트림 서비스라고 함
- 데이터의 순서 유지를 위해 각 바이트 마다 번호를 부여하여 데이터의 전송 순서를 보장
- Sequence Number, Ack Number를 통한 신뢰성 보장하여 신뢰성 있는 데이터를 전송
- 수신자 버퍼 오버플로우(Overflow) 방지를 위해 데이터 흐름 제어
- 패킷 수의 과도하게 증가하는 현상 방지를 위한 혼잡 제어
- 연결의 설정(3-way handshaking)과 해제(4-way handshaking)
- 전이중(Full-Duplex), 점대점(Point to Point) 서비스
- UDP보다 전송속도가 느림

전송 계층(4계층)

TCP – 3 Way Handshake 방식 (SYN, ACK)

- TCP 통신을 위한 네트워크 연결은 3 way handshake 이라는 방식으로 연결
- 서로의 통신을 위한 관문(port)을 확인하고 연결하기 위하여 3번의 요청 및 응답 후에 연결
- 이 과정에서 가장 많은 시간이 소요되어 UDP방식보다 속도가 느려지는 주요 원인이 됨

전송 계층(4계층)

TCP 연결 과정 (3-Way Handshaking)

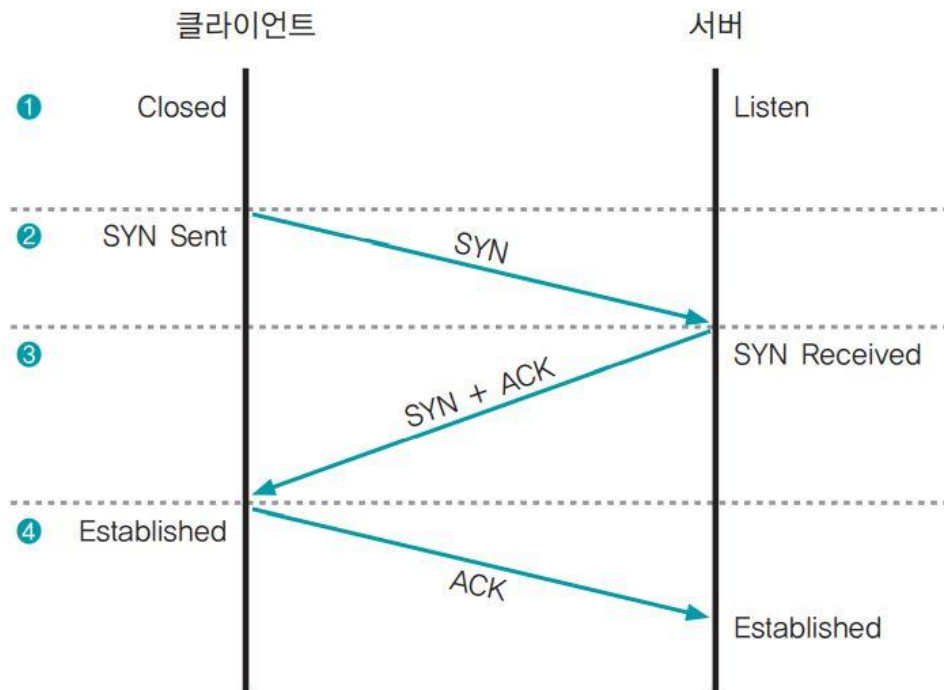


그림 3-13 TCP의 연결 설정 과정

- 1 두 시스템이 통신을 하기 전에 클라이언트는 포트가 닫힌 **Closed** 상태
서버는 해당 포트에 항상 서비스를 제공할 수 있는 **Listen** 상태
 - 2 클라이언트가 처음 통신을 하려면 임의의 포트 번호가 클라이언트 프로그램에 할당
클라이언트는 서버에 연결하고 싶다는 의사 표시로 **SYN Sent** 상태가 됨
 - 3 클라이언트의 연결 요청을 받은 서버는 **SYN Received** 상태가 됨
클라이언트에 연결을 해도 좋다는 의미로 **SYN + ACK** 패킷을 보냄
 - 4 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 표시로 **ACK** 패킷을 서버로 보냄
- 위와 같이 3번의 통신이 정상적으로 이루어지면, 서로의 포트가 **ESTABLISHED** 되면서 연결

전송 계층(4계층)

TCP 연결 해제 과정

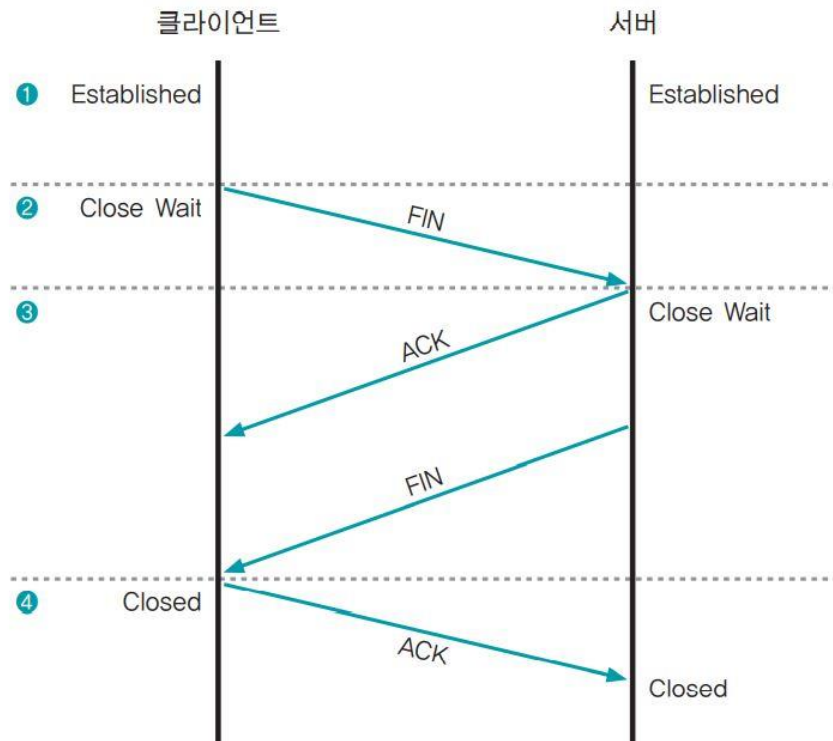


그림 3-14 TCP의 연결 해제 과정

- 1 통신 중에는 클라이언트와 서버 모두 Established 상태
- 2 통신을 끊으려는 클라이언트가 서버에 FIN 패킷을 보내고 클라이언트는 Close Wait 상태가 됨
- 3 서버는 클라이언트의 연결 종료 요청을 확인하고 응답으로 클라이언트에 ACK 패킷을 보내면 서버도 클라이언트의 연결을 종료하겠다는 의미로 FIN 패킷을 보내고 Close Wait 상태가 됨
- 4 클라이언트는 연결 종료를 요청한 것에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버에 보냄

전송 계층(4계층)

UDP

- 비연결형 서비스(Connectionless)로 연결 없이 통신이 가능하며 데이터그램 방식을 제공
- 데이터 경계를 구분
- 정보를 주고 받을 때 정보를 보내거나 받는다는 신호 절차를 거치지 않음
- 데이터 재전송과 데이터 순서 유지를 위한 작업을 하지 않아 신뢰도가 떨어짐
- 느린 선로로 보낸 패킷이 나중에 도착할 경우 유실이 발생할 수 있어 패킷 관리가 필요
- 패킷 오버헤드가 적어 네트워크 부하가 감소되는 장점을 가짐
- 상대적으로 TCP보다 전송속도가 빠름

전송 계층(4계층)

TCP 와 UDP 공통점

TCP와 UDP의 공통점
포트 번호를 이용하여 주소를 지정
데이터 오류 검사를 위한 체크섬 존재

01. 네트워크에 대한 이해 – OSI 7계층

전송 계층(4계층)

TCP 와 UDP 차이점

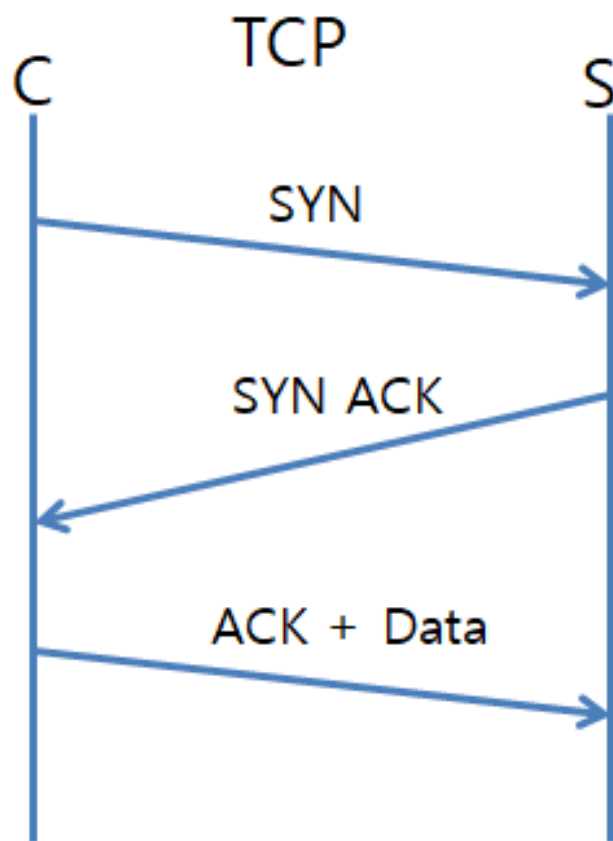
	TCP	UDP
연결방식	연결형서비스	비 연결형 서비스
패킷 교환 방식	가상 회선 방식	데이터그램 방식
전송 순서	전송 순서 보장	전송 순서가 바뀔 수 있음
수신 여부 확인	수신 여부를 확인함	수신 여부를 확인하지 않음
통신 방식	1:1 통신만 가능	1:1 / 1:N / N:N 통신 모두 가능
신뢰성	높음	낮음
속도	느림	빠름

01. 네트워크에 대한 이해 – OSI 7계층



전송 계층(4계층)

통신 그림 비교



전송 계층(4계층)

출발지 포트 결정

- 출발지 포트는 보통 1,025 ~ 65,535번 중에서 사용하지 않는 임의의 포트를 응용 프로그램 별로 할당하여 사용
- 예시) 웹 서버에 접속할 경우
 - 웹서버의 서비스 포트



- 출발지 포트로 할당된 3000번대의 임의 포트



01. 네트워크에 대한 이해 – OSI 7계층

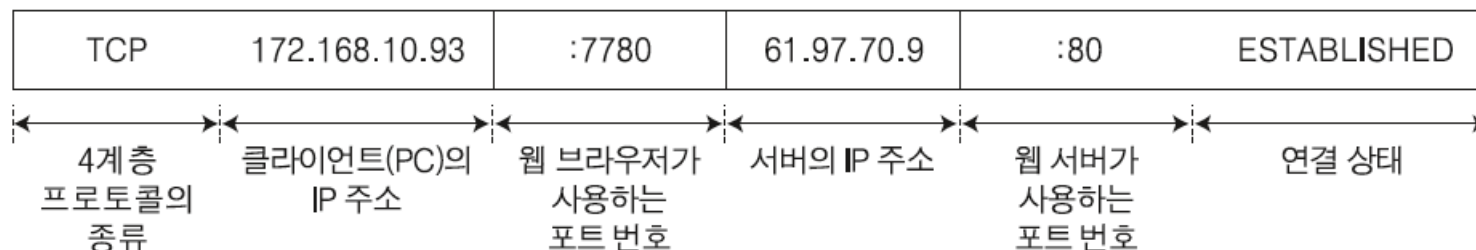


전송 계층(4계층)

- 3계층과 4계층 정보는 netstat -an 명령으로 쉽게 확인 가능

```
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
```

- Netstat -an 명령을 실행한 결과 각각 다음의 정보를 담고 있음



전송 계층(4계층)

주요 포트와 서비스

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

세션 계층(5계층)

- 종단 호스트 프로세스 간에 세션을 생성, 유지, 종료하는데 필요한 여러 기능을 제공
 - 세션 키(Session Key) : 하나의 논리적 연결 세션 동안 만 유효한 암호 키
- 대화 관리 (dialogue manage)
 - 세션 계층은, 토큰을 사용함으로써 대화를 관리
 - 성립된 세션을 통한 상호 대화 관리를 하는 양단간 응용 개체를 위해 토큰 개념이 정의
 - 누가 언제 통신 하였는지를 결정하며 토큰을 교환함으로써 구현
 - 프로세스는 토큰을 가졌을 때 전송할 수 있음
 - 토큰(Token)은 어떤 서비스의 실행을 기동하는 권리를 표현하는 것
- 다중화 (multiplexing)
 - 여러 세션들이 효율을 높이기 위해 1개의 같은 전송 계층 접속을 사용할 수 있음
 - 반대로 1개 세션이 속도 등을 위해 다수의 전송 계층 접속들을 사용할 수도 있음
 - 전송 계층과 같이 세션 계층에서도 상향, 하향 다중화가 가능
- 사용되는 곳
 - 네트워크 지원용 API : 소켓, RPC, NFS, SMB, NetBIOS 등
 - 데이터베이스 쿼리용 : SQL

표현 계층(6계층)

- 하나의 통일된 구문 형식으로 변환시키는 기능을 수행하는 계층
 - 네트워크 상의 여러 이기종 시스템들이 저마다 다른 데이터 표현 방식을 사용
 - 두 응용 계층 프로토콜 개체가 서로 통신할 때 양쪽 개체 간의 메시지가 같은 뜻으로 (공통의 어휘로) 교환되어야 함
 - 번역기 / 변환기 역할을 수행
- 응용 계층(7 Layer)의 다양한 표현 양식(Syntax)을 공통의 형식으로 변환
- 암호화 (Encryption)
- 압축 (Compression)
- 코드 변환
 - 서로 다른 상이한 형태의 코드 변환(ASCII, EBCDIC, binary 등), 파일 변환, 문장 축소화 등의 기능 수행
- 사용되는 곳
 - ASN.1, BER(Basic Encoding Rule) 등

응용 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
- 사용되는 곳
 - 전자메일, 가상단말, 파일 송수신, 웹 응용 등
- 관련 프로토콜
 - OSI 프로토콜 : FTAM, CMIP 등
 - TCP/IP 프로토콜 : FTP(파일전송), SMTP(메일전송), HTTP(웹문서전송), TELNET(문자단말) 등

02. 서비스 거부(DoS) 공격



서비스 거부 공격 (DoS)

● 다른 해킹에 비해 비교적 간단한 것으로 일종의 훼방

- 예를 들면 갱패가 노점상의 장사를 방해하는 것
- 집기를 부수거나 식재료의 공급을 끊거나 나쁜 재료를 음식에 몰래 섞는 것



그림 3-15 노점상에 행해지는 서비스 거부 공격

서비스 거부 공격 (DoS)

● 취약점 공격형

- 특정 형태의 오류가 있는 네트워크 패킷의 처리 로직에 문제가 있을 때 공격 대상이 그 문제점을 이용하여 오작동을 유발하는 형태
- 보잉크/봉크/티어드롭 공격, 랜드 공격

● 자원 고갈 공격형

- 네트워크 대역폭이나 시스템의 CPU, 세션 등의 자원을 소모 시키는 형태
- 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

보잉크/붕크/티어드롭 공격

- 프로토콜의 오류 제어 로직을 악용하여 시스템 자원을 고갈시키는 방식
- TCP 프로토콜이 제공하는 오류 제거 기능
 - 패킷의 순서가 올바른지 확인
 - 중간에 손실된 패킷이 없는지 확인
 - 손실된 패킷의 재전송을 요구
- TCP는 데이터 전송 시 신뢰를 확보하기 위해 패킷 전송에 문제가 있으면 반복적으로 재요청과 수정을 함
- 보잉크, 붕크, 티어드롭은 공격 대상이 반복적인 재요청과 수정을 계속하게 함으로써 시스템 자원을 고갈시킴

랜드 공격

- 'land'를 영어사전에서 찾아보면 '땅', '착륙하다'라는 뜻 외에 '(나쁜 상태에) 빠지게 하다'라는 뜻
- 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만들어서 공격 대상에게 보내는 것
- 이 공격법은 SYN Flooding처럼 동시 사용자 수를 점유하고 CPU 부하를 올려서 시스템이 금방 지쳐버리게 만듦
- land 공격에 대한 보안 대책은 주로 운영체제의 패치 관리를 통해 마련

죽음의 핑 공격 – Ping of Death

- NetBIOS 해킹과 함께 시스템을 파괴하는 데 가장 흔히 쓰인 초기의 DoS 공격 방법
 - NetBIOS : OSI 모형의 세션 계층에 관련된 서비스들을 제공하여 개개의 컴퓨터의 애플리케이션들이 근거리 통신망을 통해 통신할 수 있게 도와주는 서비스
- 네트워크의 연결 상태를 점검하는 ping 명령을 보낼 때 공격 대상에게 패킷을 최대한 길게 보내 패킷을 쪼갬
- 공격 대상 시스템은 대량의 작은 패킷을 수신하느라 네트워크가 마비
- 죽음의 핑 공격을 막으려면 ping이 내부 네트워크에 들어오지 못하도록 방화벽에서 ICMP를 차단해야 함
 - ICMP: ping이 사용하는 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 오류를 알려주는 프로토콜

■ 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

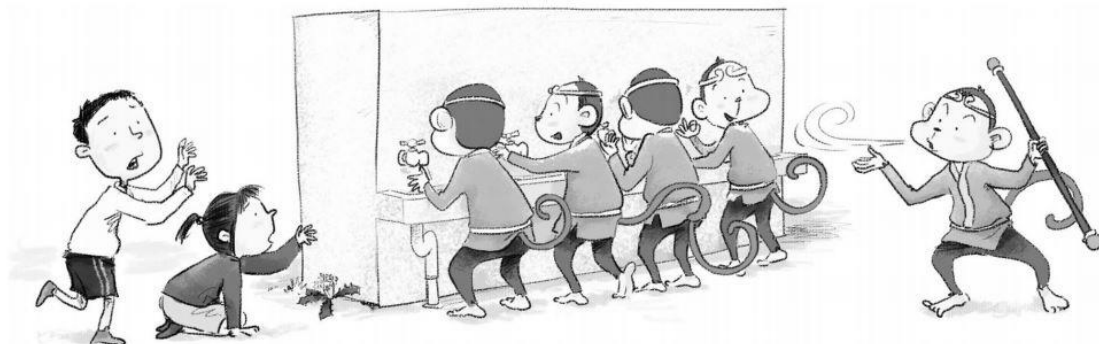


그림 3-20 SYN 플러딩 공격

■ 자원 고갈 공격형

● SYN Flooding 공격

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

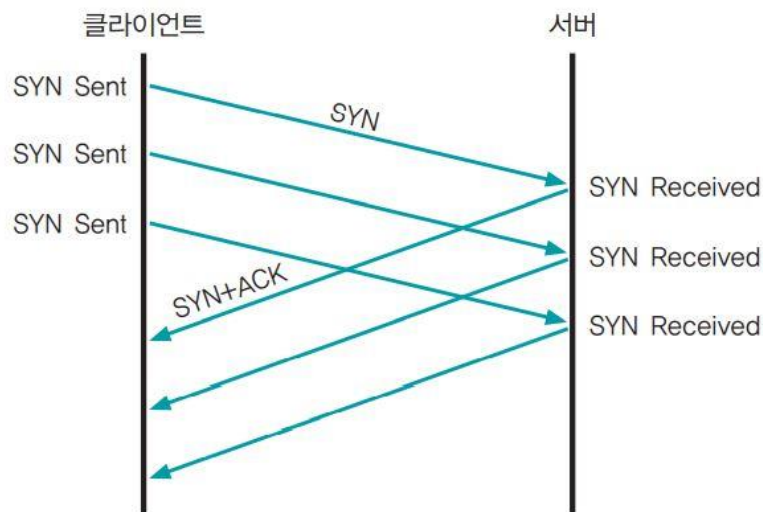


그림 3-21 SYN 플러딩 공격 시 3-웨이 핸드셰이킹

SYN Flooding 공격 대응방법

- 이 공격은 SYN Received의 대기 시간을 줄이는 방법으로 쉽게 해결할 수 있음
- 침입 방지 시스템(IPS)과 같은 보안 시스템을 통해서도 이러한 공격을 쉽게 차단 가능
 - 의심 패킷에 대한 차단 정책을 추가하는 방식으로 대응
 - 예를 들어 공격이 시도되고 있는 포트로 유사 패킷이 1초당 10개를 초과할 경우 차단
 - Snort, iptable 등을 이용하여 Rule 작성
 - 예시
 - `# iptables -A INPUT -p TCP --dport 80 --syn -m limit 10/second -j ACCEPT`
 - `# iptables -A INPUT -p TCP --dport 80 --syn -j DROP`
- SYN Cookie를 사용
 - 연결 수립에 필요한 정보들을 Cookie를 통해 보냄으로써 SYN Backlog Queue를 사용하지 않음
 - SYN Backlog Queue : 3-Way-Handshake를 위해 연결이 진행중인 요청을 담아두는 큐
 - ACK이 올 경우 쿠키값을 검증하여 제대로 된 값인 경우 연결을 형성
 - 이 기능을 리눅스나 유닉스에 입력하여 활성화
 - 예시
 - `sysctl -w net.ipv4.tcp_syncookies=1`

❏ 자원 고갈 공격형

● HTTP GET Flooding 공격

- 공격 대상 시스템에 TCP 3-Way Handshaking 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
- 요청 예시

```
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
www.gachun.ac.kr/list.php?page=1&search=test  
.....
```

자원 고갈 공격형

동적 HTTP GET Flooding 공격

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

Smurf 공격

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

자원 고갈 공격형

HTTP CC 공격

- HTTP 1.1 버전의 CC 헤더 옵션은 자주 변경되는 데이터에 새로운 HTTP 요청 및 응답을 요구하기 위해 캐시 기능을 사용하지 않을 수 있음
- 서비스 거부 공격에 이를 응용하려면 'Cache-Control: no-store, must-revalidate' 옵션을 사용
 - Cache-Control: no-store : 어떠한 요청도 캐시로 저장하지 않음
 - Must-revalidate : 캐시를 사용하기 이전에 기존 리소스 상태를 반드시 확인하며 만료된 리소스는 사용하지 않음
- 이 옵션을 사용하면 웹 서버가 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가함

동적 HTTP Request Flooding 공격

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

스머프 공격 (smurf)

- ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용하여 패킷을 확장함으로써 서비스 거부 공격을 수행
- 다이렉트 브로드캐스트를 악용하는 것으로 공격 방법이 간단
- 스머프 공격 예시
 - 스머프 마을에서 거짓말쟁이 스머프가 확성기를 들고 "마을에 가가멜이 나타났어요. 가가멜이에요!"라고 소리침
 - 온 동네 스머프를 다 깨운 뒤 옆에 있던 멀뚱이 스머프에게 확성기를 쥐어줌
 - 스머프들이 확인해보니 거짓말 이었는데, 모두 확성기를 가지고 있던 멀뚱이 스머프가 한 짓으로 생각함
 - 거짓말쟁이 스머프는 '공격자' / 멀뚱이 스머프는 '공격 대상'



그림 3-22 스머프 공격

• 스머프 공격

- 다이렉트 브로드캐스트

- 기본적인 브로드캐스트는 목적지 IP 주소 255.255.255.255를 가지고 네트워크의 임의 시스템에 패킷을 보내는 것
- 브로드캐스트는 기본적으로 네트워크 계층 장비인 라우터를 넘어가지 못함
- 라우터를 넘어가서 브로드캐스트를 해야 하는 경우에는 클라이언트의 IP 주소 부분에 브로드캐스트 주소인 255를 채움

- 공격자가 172.16.0.255로 다이렉트 브로드캐스트를 할 경우

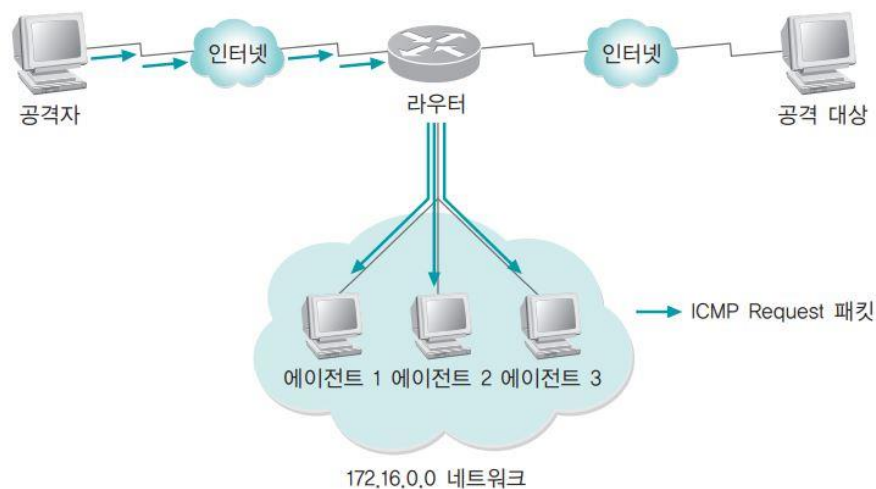


그림 3-23 공격자에 의한 에이전트로의 브로드캐스트

■ 자원 고갈 공격형

● Smurf 공격

■ 다irect 브로드캐스트(Direct Broadcast)의 이해

- 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 다irect 브로드캐스트라고 함
- 공격자가 172.16.0.255로 다irect 브로드캐스트를 하면 패킷이 다음과 같이 전달됨

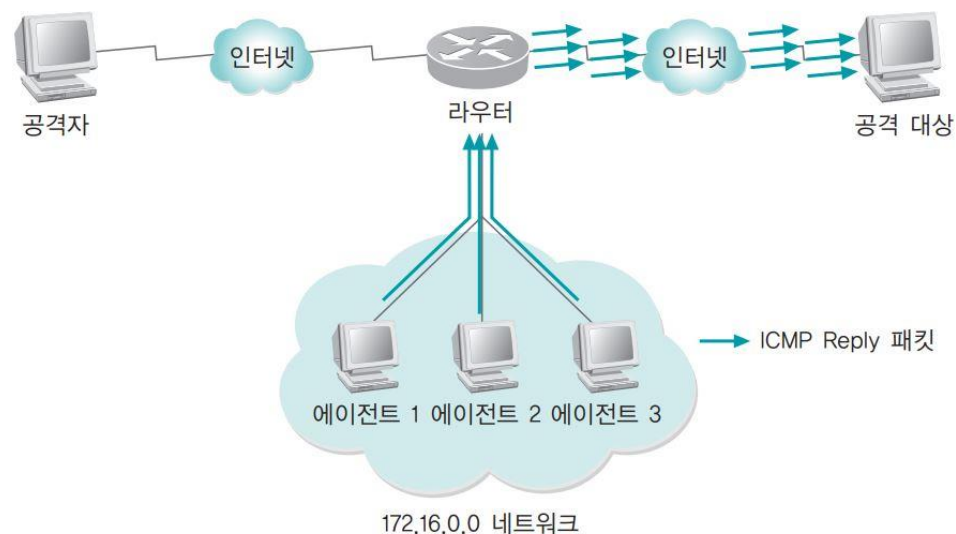


그림 3-24 에이전트에 의한 스머프 공격 실행

자원 고갈 공격형

Mail Bomb(메일 폭탄) 공격

- 메일 폭탄은 스팸 메일과 같은 종류
- 익명의 발신자로 위장하여 메시지를 무한정 보내면, 서버의 시스템은 메일을 받아 하드디스크 스푼(Spool)에 저장하며 디스크자원과, 서버의 전자우편 프로세스를 낭비하며 과부하를 주는 공격
- 발생원인
 - 클라이언트의 전자우편 주소에 대량의 이메일을 전송하여 메일 서버를 다운되게 함으로써 업무를 마비시키는 용도로 사용
 - 전자우편 주소로 전송된 스팸 메일을 열람했을 시 사용자에게 대란 정보가 노출되어 공격자의 표적이 되므로 메일 서버내의 기능을 통해 스팸차단 & 스팸신고 & 수신거부 기능 사용
 - 서버용 스팸메일 차단 프로그램을 사용하여 자체 스팸정책을 마련하여 기술적 보안 조치 필요

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

■ 분산 서비스 거부(DDoS) 공격

● 기본 구성

- 구조는 폭력 조직과 비슷하여 공격자를 폭력 조직의 두목, 마스터를 행동대장, 에이전트를 졸개에 비유
- 과거의 분산 서비스 거부 공격에서는 마스터와 에이전트가 중간자인 동시에 피해자

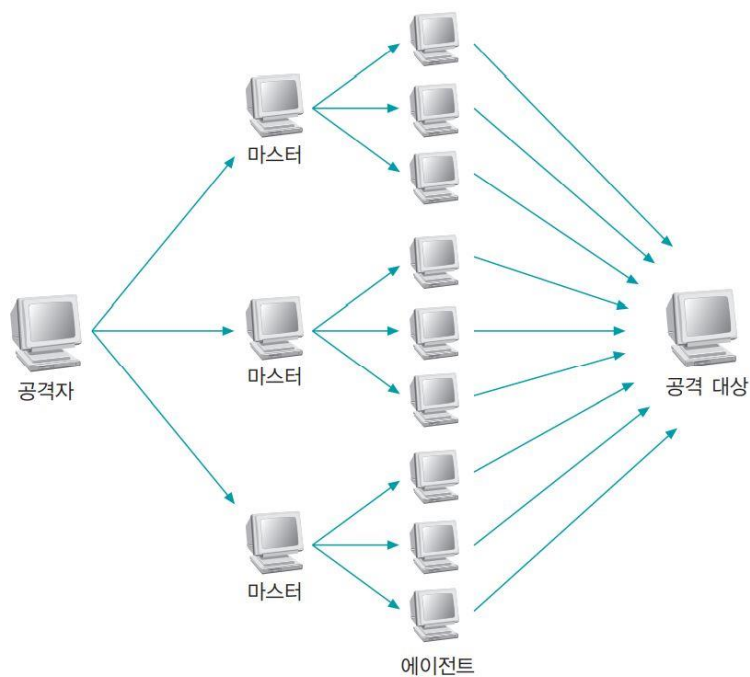


그림 3-25 분산 서비스 거부 공격의 구성

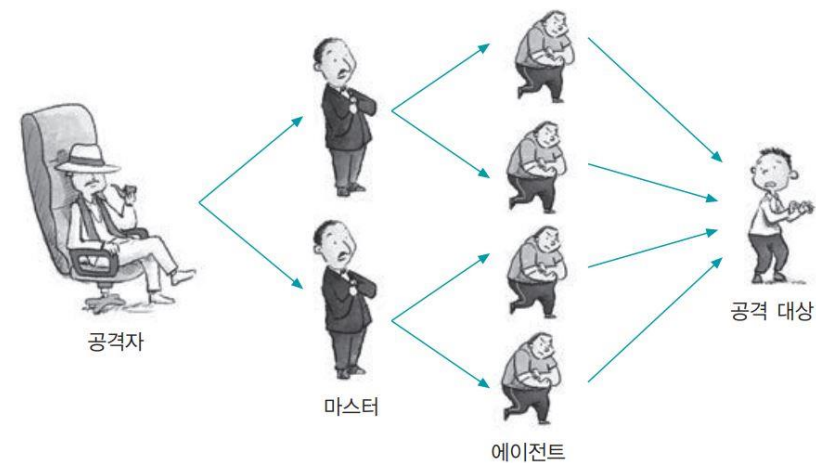


그림 3-26 분산 서비스 거부 공격의 개념

분산 서비스 거부(DDoS) 공격

● 최근에 발생하는 분산 서비스 공격 과정

- ① PC에서 전파가 가능한 형태의 악성 코드를 작성
- ② 분산 서비스 거부 공격을 위해 사전에 공격 대상과 스케줄을 정한 뒤 이를 미리 작성한 악성 코드에 코딩
- ③ 인터넷을 통해 악성 코드를 전파 (봇: 분산 서비스 거부 공격에 사용되는 악성 코드)
전파 과정에서는 별다른 공격 없이 잠복
악성 코드에 감염된 PC를 좀비 PC라고 하며, 좀비 PC끼리 형성된 네트워크를 **봇넷**(Botnet) 이라고 함

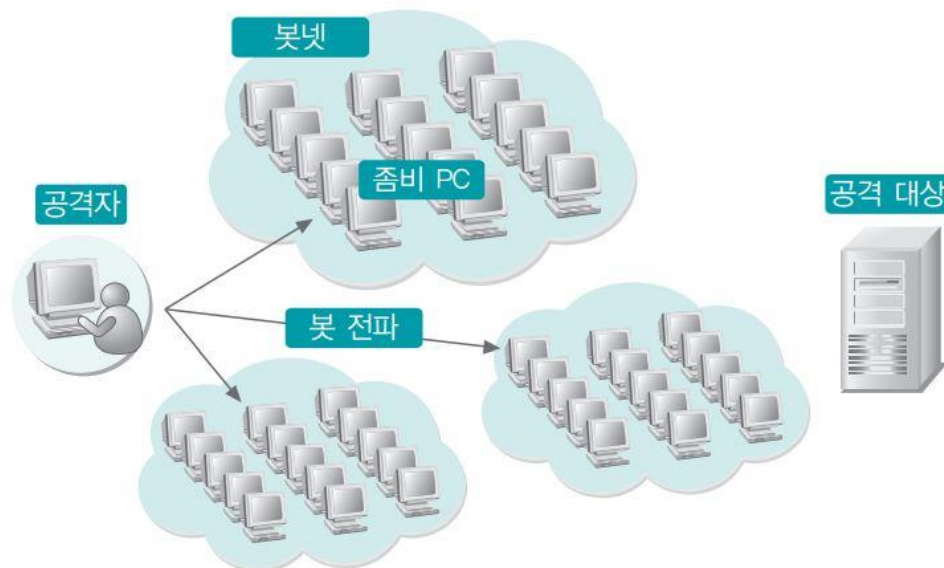


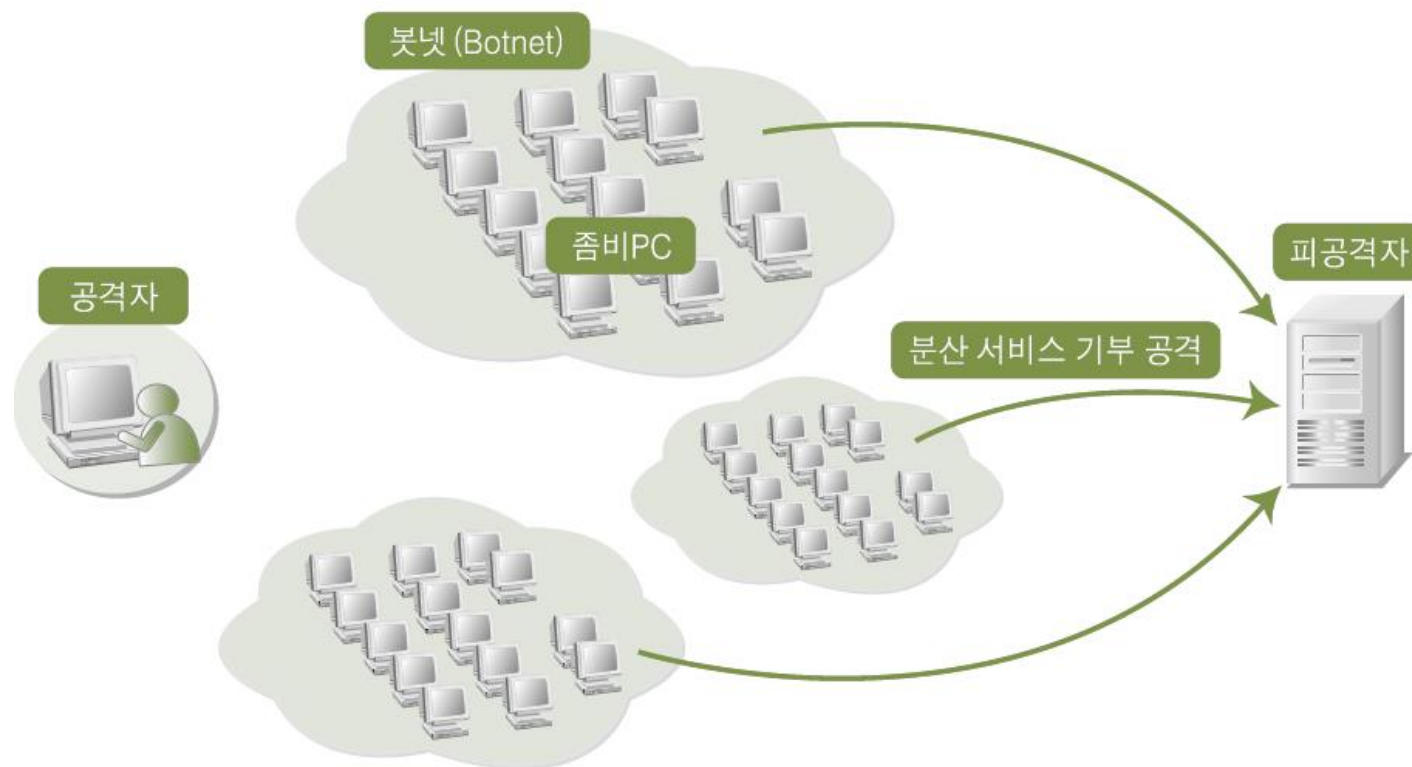
그림 3-27 악성 코드(봇)에 감염된 에이전트

02. 서비스 거부(DoS) 공격



분산 서비스 거부(DDoS) 공격

- 좀비 PC에 의한 분산 서비스 거부 공격 수행



03. 스니핑 공격



스니핑(Sniffing)

수동적(Passive) 공격이라고도 함

스니핑 공격의 개요

- 코를 킁킁거리면서 음식을 찾는 동물처럼 데이터 속에서 정보를 찾는 것
- 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 충분하기 때문에 수동적 공격이라고도 함
 - 다른 사람의 대화를 엿듣거나 도청하는 행위
 - 전화선이나 UTP에 태핑(Tapping)을 해서 전기적 신호를 분석하여 정보를 찾아내는 것
 - 전기적 신호를 템페스트(Tempest) 장비로 분석하는 것



[템페스트 도청 장치]



[스니핑 개요]

스니핑(Sniffing) 원리

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

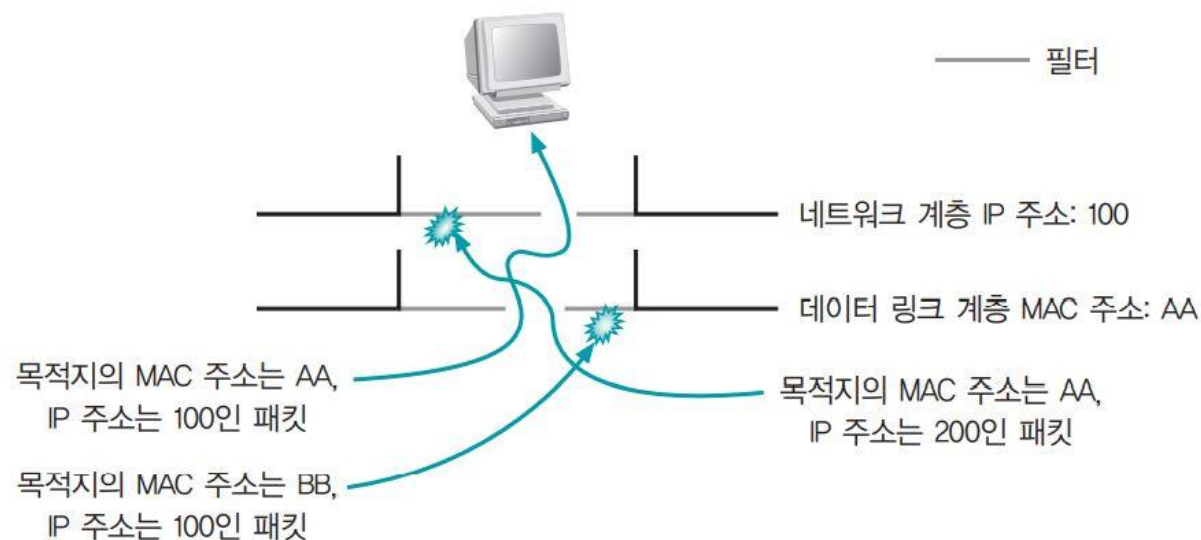


그림 3-30 정상적인 네트워크 필터링의 예

스니핑(Sniffing) 원리

- 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 **프러미스큐어스 모드 (Promiscuous Mode)로 변경**
 - 프러미스큐어스 모드: 데이터 링크 계층과 네트워크 계층의 필터링을 해제하는 랜 카드의 모드

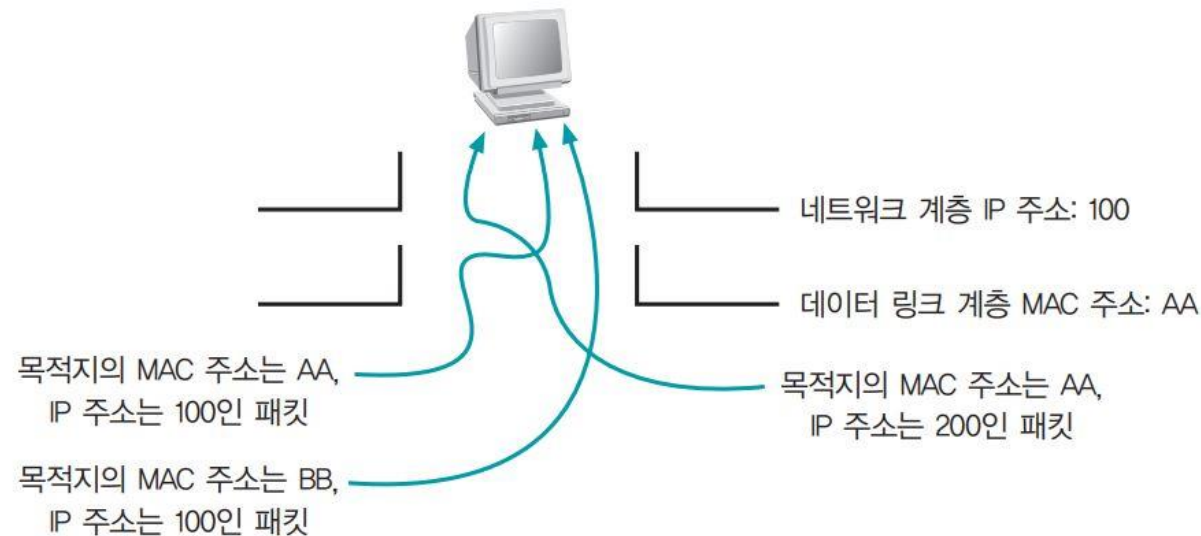


그림 3-31 네트워크 필터링 해제 상태(프러미스큐어스 모드)의 예

스니핑 재밍 공격

- 스위치의 주소 테이블의 기능을 마비시키는 공격. **MACOF 공격**이라고도 함
- 스위치에 랜덤한 형태로 생성한 MAC을 가진 패킷을 무한대로 보내면, 스위치의 MAC 테이블은 자연스레 저장용량을 넘게 되고, 스위치의 원래 기능을 잃고 더미 허브처럼 작동하게 됨
- 스위치가 더미 허브와 똑같이 동작하면 공격자는 ARP 스푸핑이나 ICMP 리다이렉트처럼 패킷이 굳이 자기에게 오게 할 필요가 없어 스니핑 공격 자체가 쉬워짐
- 고가의 스위치는 MAC 테이블의 캐시와 연산자가 쓰는 캐시가 독립적으로 나뉘어져 있어 스위치 재밍 공격이 통하지 않음

SPAN 포트 태핑 공격

- SPAN(Switch Port Analyzer)은 **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
- 스니핑 공격에 악용

스니퍼의 탐지

- 스니퍼를 설치한 이후에는 네트워크에 별다른 이상 현상을 일으키지 않기 때문에 사용자가 인지하기 어려움
- 스니퍼를 쉽게 탐지하려면 스니퍼가 프러미스큐어스 모드에서 작동한다는 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 프러미스큐어스 모드인 학생은 교수에게 들리게 됨

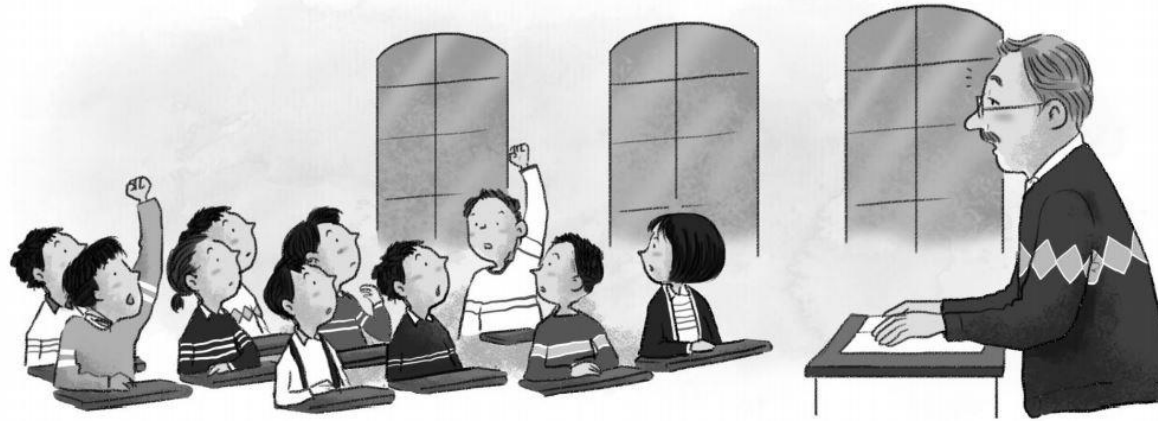


그림 3-32 스니퍼가 탐지되는 상황

스니퍼의 탐지

● Ping을 이용한 스니퍼 탐지

- 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 request를 받으면 response를 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

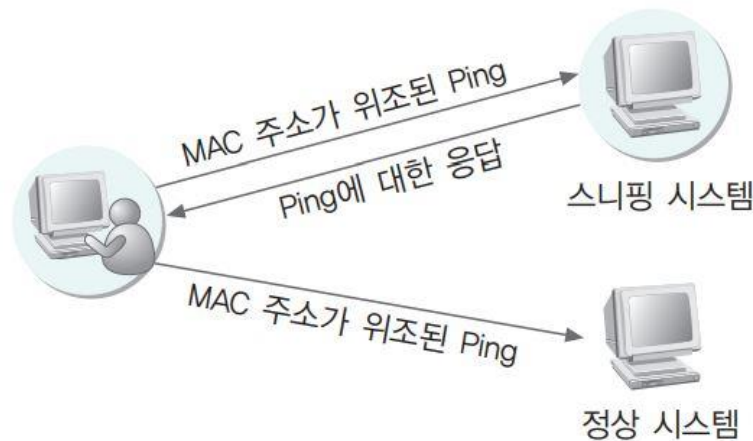


그림 3-33 ping을 이용한 스니퍼 탐지

스니퍼의 탐지

● ARP를 이용한 스니퍼 탐지

- 위조된 ARP request를 보냈을 때 ARP response 오면 프로미스큐어스 모드(Promiscuous mode)로 설정되어 있는 것

● DNS를 이용한 스니퍼 탐지

- 일반적인 스니핑 프로그램은 스니핑한 시스템의 IP 주소에 DNS의 이름 해석 과정인 Reverse-DNS lookup을 수행
- 대상 네트워크로 ping sweep를 보내고 들어오는 Reverse-DNS lookup을 감시하면 스니퍼 탐지 가능
 - Reverse-DNS : SpamMail 여부를 확인할 때 IP에 해당하는 도메인을 검사하는 것

● 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 스푸핑의 개요

- ARP 스푸핑은 MAC 주소를 속이는 것
 - 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

ARP 스푸핑 과정



그림 3-34 ARP 스푸핑

표 3-6 ARP 스푸핑 공격에 사용되는 네트워크

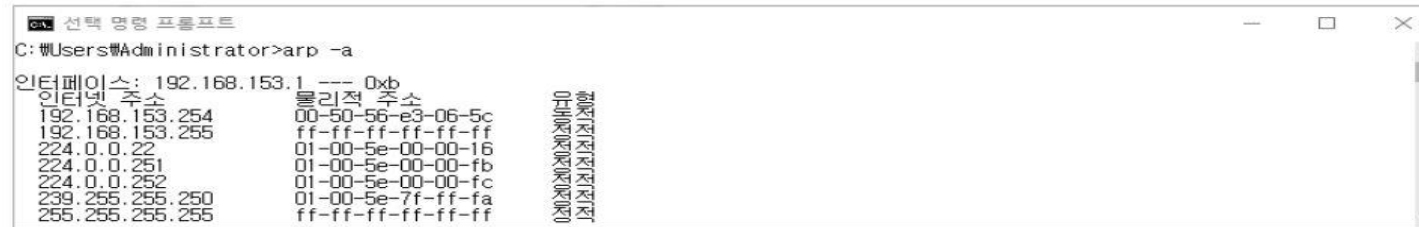
호스트 이름	IP 주소	MAC 주소
서버	10.0.0.2	AA
클라이언트	10.0.0.3	BB
공격자	10.0.0.4	CC

- 공격자는 서버의 클라이언트에 10.0.0.2에 해당하는 가짜 MAC 주소 CC를 알리고 서버에는 10.0.0.3에 해당하는 가짜 MAC 주소 CC를 알림
- 공격자가 서버와 클라이언트 컴퓨터에 서로 통신하는 상대방을 자기 자신으로 알렸기 때문에 서버와 클라이언트는 각각 공격자에게 패킷을 보냄
- 공격자는 서버와 클라이언트로부터 받은 패킷을 읽은 후, 서버가 클라이언트에 보내려던 패킷은 클라이언트에 보내주고 클라이언트가 서버에게 보내려던 패킷은 서버에 보냄

ARP 스푸핑 공격

ARP 테이블

- 윈도우에서는 **arp -a** 명령을 이용하여 현재 인지하고 있는 IP와 해당 IP를 가지고 있는 시스템의 MAC 주소목록을 확인할 수 있음



```
선택 명령 프롬프트
C:\Users\Administrator>arp -a

인터넷 주소: 192.168.153.1 --- 0xb
인터넷 주소 물리적 주소
192.168.153.254 00-50-56-e3-06-5c
192.168.153.255 ff-ff-ff-ff-ff-ff
224.0.0.22 01-00-5e-00-00-16
224.0.0.251 01-00-5e-00-00-fb
224.0.0.252 01-00-5e-00-00-fc
239.255.255.250 01-00-5e-7f-ff-fa
255.255.255.255 ff-ff-ff-ff-ff-ff
```

그림 3-36 arp -a 명령 실행 결과

- 위 예의 클라이언트에서 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 실행하면 결과가 변경

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

ARP 스푸핑 공격 후 패킷

- 클라이언트와 서버 사이의 패킷을 공격자가 훔쳐볼 수 있게 됨

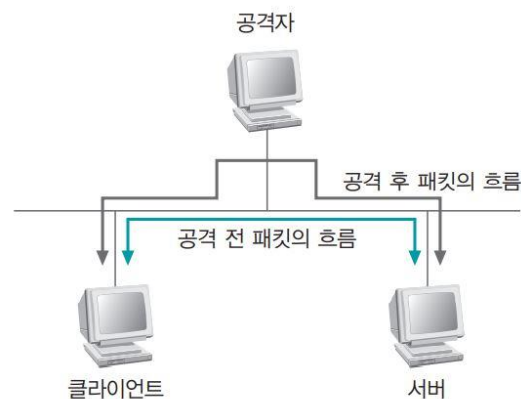


그림 3-35 ARP 스푸핑 공격으로 인한 네트워크 패킷의 흐름

ARP 스푸핑에 대한 대응책

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

```
arp -s 10.0.0.2 AA
```

- s(static)는 고정시킨다는 의미. 이 명령으로 Type 부분이 Dynamic에서 Static으로 바뀌게 됨. 하지만 이 대응책은 시스템이 재부팅 될 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

IP 스푸핑 공격

IP 스푸핑의 개요

- 쉽게 말해 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

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 가능 아이디를 등록해 주어야 함.

```
① 200.200.200.200 root
② 201.201.201.201 +
```

① 200.200.200.200에서 root 계정이 로그인을 시도하면 패스워드 없이 로그인을 허락하라는 의미

② 201.201.201.201에서는 어떤 계정이든 로그인을 허락하라는 것

- + 는 모든 계정을 의미
- ++라고 적힌 행이 있으면 IP와 아이디에 관계없이 모두 로그인을 허용

IP 스푸핑 공격

IP 스푸핑의 서버 접근

- 공격자가 해당 IP를 사용하여 접속하면 스니핑으로 패스워드를 알아낼 필요가 없음
 - 공격자는 제로 트러스트(Zero Trust)로 접속한 클라이언트에 서비스 거부 공격을 수행하여 클라이언트의 IP의 네트워크 출연을 막음
 - 그 후 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 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 패스워드를 알아낼 필요성 자체가 없어지는 문제점이 있음
- 실제로 공격은 트러스트로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어짐
- 공격자는 패스워드 없이 서버에 로그인할 수 있음

ICMP(Internet Control Message Protocol) 리다이렉트(Redirect)

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

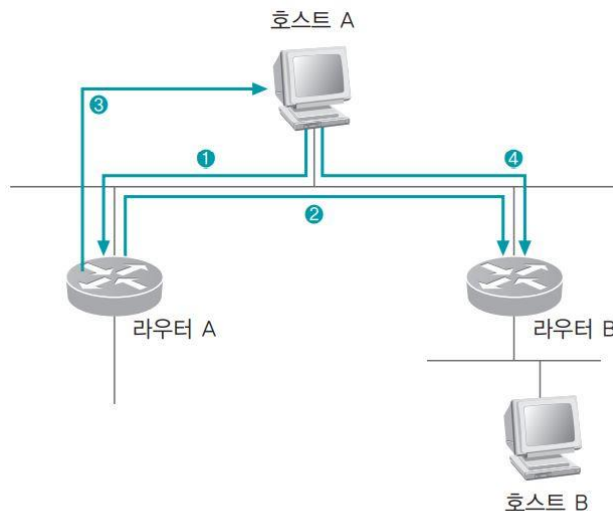


그림 3-39 ICMP 리다이렉트의 동작

- 호스트 A에 라우터 A가 기본으로 설정되어 있기 때문에 호스트 A가 원격의 호스트 B로 데이터를 보낼 때 패킷을 라우터 A로 전송
- 라우터 A는 호스트 B로 보내는 패킷을 수신, 그 후 라우팅 테이블을 검색하여 호스트 A가 자신보다 라우터 B를 이용하는 것이 더 효율적이라고 판단하여 해당 패킷을 라우터 B로 전송
- 라우터 A는 호스트 B로 향하는 패킷을 호스트 A가 자신에게 다시 전달하지 않도록, 호스트 A에 ICMP 리다이렉트 패킷을 보내어 호스트 A가 호스트 B로 보내는 패킷이 라우터 B로 바로 향하게 함
- 호스트 A는 라우팅 테이블에 호스트 B에 대한 값을 추가하고 호스트 B로 보내는 패킷은 라우터 B로 전달

ICMP(Internet Control Message Protocol) 리다이렉트(Redirect)

- ICMP 리다이렉트를 이용해 공격하면 공격자가 라우터 B가 됨
- ICMP 리다이렉트 패킷도 공격 대상에게 보낸 후 라우터 A에 다시 연결하면 모든 패킷을 스니핑할 수 있음
- ICMP 리다이렉트는 데이터링크 계층의 공격이 아니기 때문에 잘 응용하면 로컬의 랜이 아니라도 공격이 가능

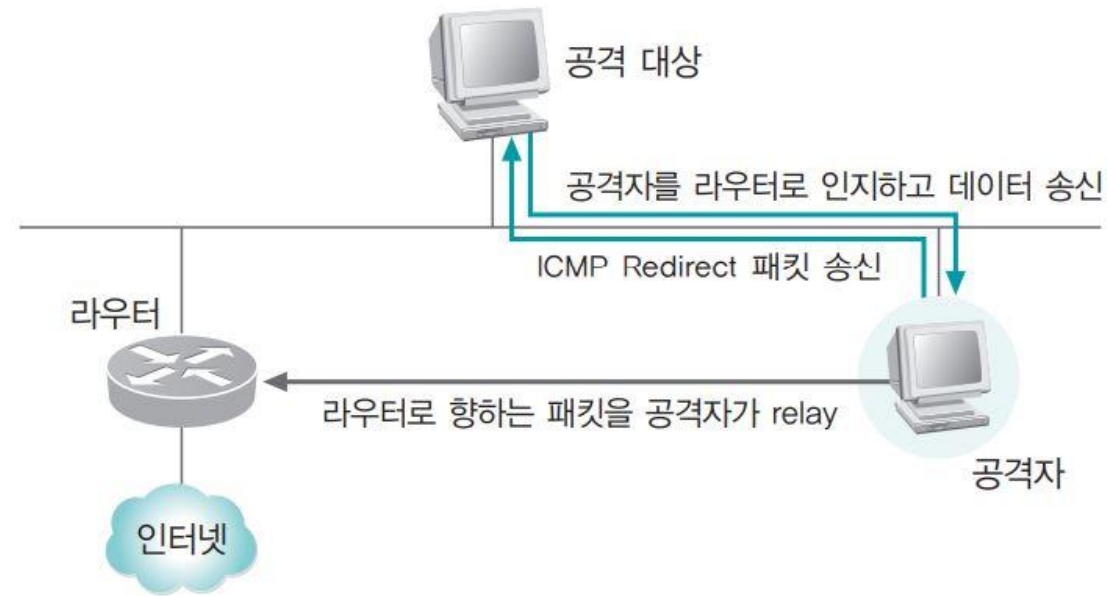


그림 3-40 ICMP 리다이렉트 공격

DNS 스푸핑 공격

- 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격
 - 인터넷 익스플로러에 사이트 주소를 입력하고 Enter를 눌렀을 때 쇼핑몰이나 음란 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

정상적인 DNS 통신 과정

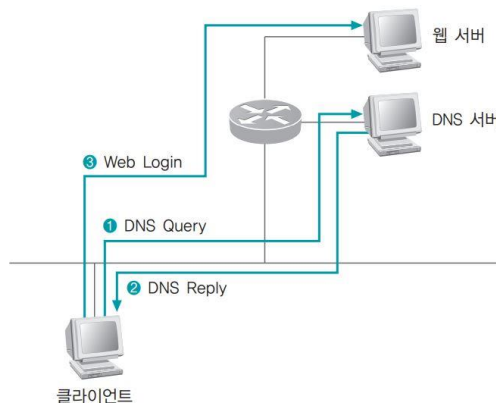


그림 3-41 정상적인 DNS 서비스

- 1 클라이언트가 DNS 서버에 접속하고자 하는 IP 주소(www.gachun.ac.kr과 같은 도메인 이름)를 물어볼 때 보내는 패킷은 DNS query
- 2 DNS 서버가 해당 도메인 이름에 대한 IP 주소를 클라이언트에 전송.
- 3 클라이언트가 받은 IP 주소를 바탕으로 웹 서버를 찾아감

■ DNS 스푸핑 공격 단계

- 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

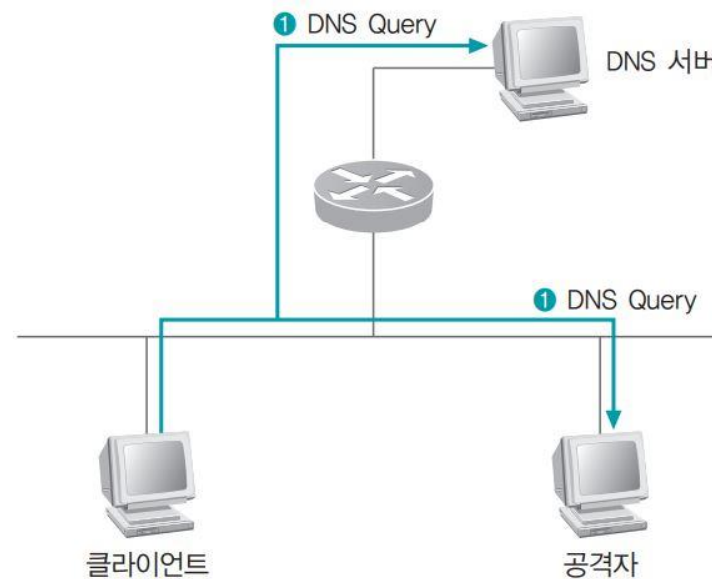


그림 3-42 DNS 스푸핑 공격: DNS Query

DNS 스푸핑 공격 단계

② 공격자는 로컬에 존재하므로 DNS 서버보다 지리적으로 가까움.

- DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 클라이언트에게 위조된 DNS Response 패킷을 보낼 수 있음
- 클라이언트는 공격자가 보낸 DNS response 패킷을 올바른 패킷으로 인식하고 웹에 접속

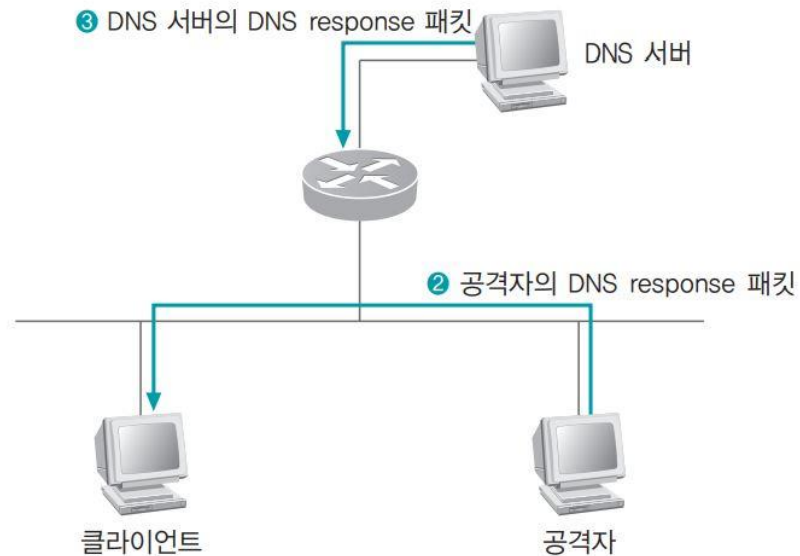


그림 3-43 DNS 스푸핑 공격: 공격자와 DNS 서버의 DNS response

DNS 스푸핑 공격 단계

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

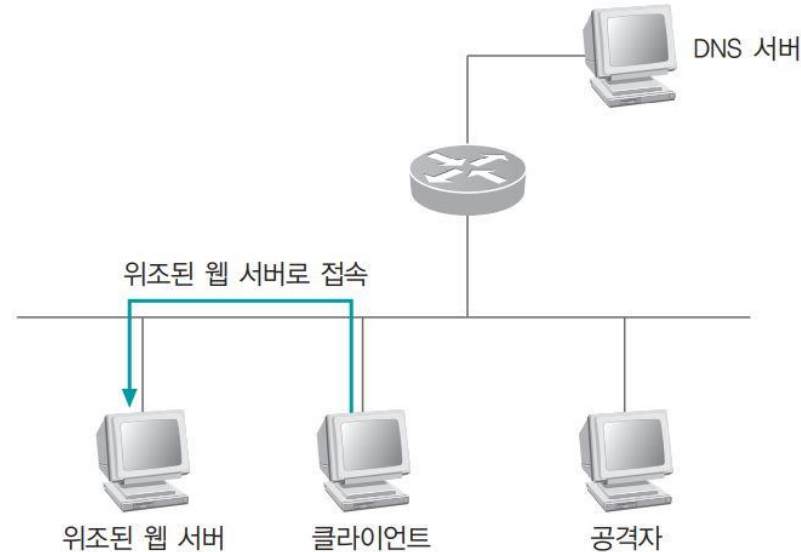


그림 3-44 DNS 스푸핑 공격: 위조된 웹 서버로 접속하는 클라이언트

- hosts 파일에는 URL과 IP 정보가 등록되어 있음. – 중요서버의 URL에 대한 IP를 hosts 파일에 등록

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


DNS 스푸핑 공격 대응책

● DNS 스푸핑 공격을 막으려면 중요 서버에 대해 DNS query를 보내지 않으면 됨

- 먼저 시스템 메모리의 정보를 확인하고 그 다음 hosts 파일에 등록된 정보를 확인
- hosts 파일에는 URL과 IP 정보가 등록

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

- **중요 접속 서버의 URL에 대한 IP 를 hosts 파일에 등록**해 놓으면 되지만, 모든 서버의 IP를 등록하는 것은 무리이므로 모든 서버에 대한 DNS 스푸핑을 막기는 어려움

05. 세션 하이재킹 공격



■ 세션 하이재킹(Session Hijacking) 공격

● 개요

- 1995년에 케빈 미트닉이 시스템 관리자인 시모무라 쓰토무의 컴퓨터를 공격한 기술
- 말 그대로 '세션 가로채기'를 의미
 - 세션: '사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 상태'
 - 세션 하이재킹은 두 시스템 간의 연결이 활성화된 상태, 즉 로그인된 상태를 가로채는 것
 - 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 충족돼야함
 - 대상이 자리를 비움, 화면 잠금을 설정하지는 않음, 내가 접속하고자 하는 세션에 접속한 채로 자리를 비움

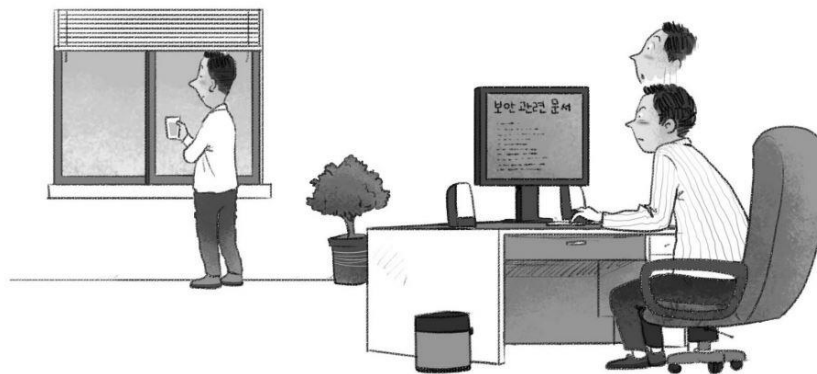


그림 3-45 자리 가로채기

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 번호**를 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 3-way Handshaking 수행
 - ③ 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받음
 - 3단계를 거치면 공격자는 클라이언트가 텔넷 등을 통해 열어놓은 세션을 아이디와 패스워드 입력 없이 그대로 획득 가능

세션 하이재킹 공격에 대한 대응책

- SSH와 같이 세션에 대한 인증 수준이 높은 프로토콜을 이용해서 서버에 접속해야 함
- 클라이언트와 서버 사이에 MAC 주소를 고정시켜줌
 - 주소를 고정시키는 방법은, 앞서도 언급했지만 ARP 스푸핑을 막아주기 때문에 결과적으로 세션 하이재킹을 막을 수 있음
- 토큰의 암호화를 통해 공격자가 토큰을 추측하기 어렵게 하기 위해 쿠키 값을 암호화하여 저장
- HTTPS 통신 활용하여 SSL 인증 기술을 이용하여 암호화 프로토콜인 HTTPS를 이용하여 전송
- 쿠키 정보 만료 시간을 짧게 설정하고 사용자가 로그아웃 버튼을 누르지 않아도 일정 시간 후에 자동으로 로그아웃을 진행

06. 무선 네트워크 공격과 보안

무선 랜

무선 랜의 개요

- 유선 랜의 네트워크를 확장하려는 목적으로 사용
- 이를 위해서는 내부의 유선 네트워크에 AP 장비를 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

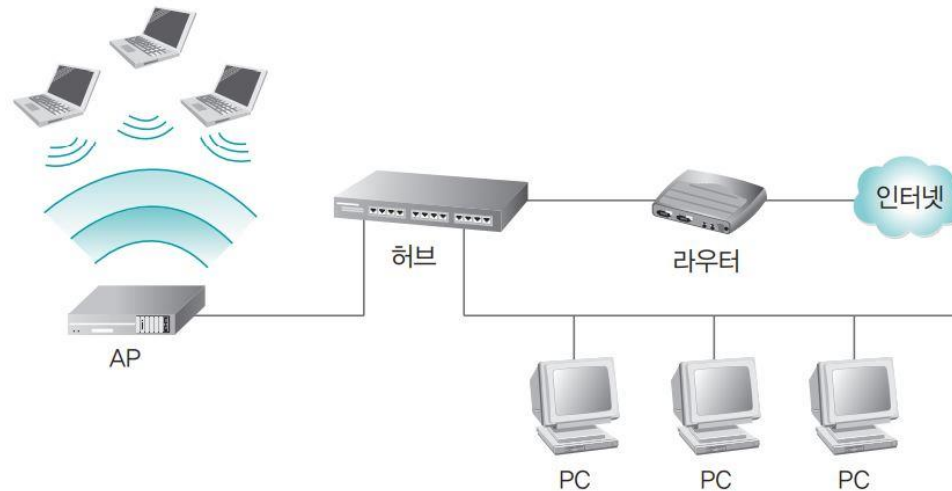


그림 3-46 유선 네트워크에 연결된 AP로 무선 랜까지 확장된 네트워크

무선 랜

● 무지향성 안테나

- 주로 봉의 형태이며, 전파 수신에 일정한 방향성이 없어 AP의 위치에 상관없이 동작
 - 4개 이상의 방향성이 있다고 말하는 편이 더 정확
- 여러 방향을 지원하므로 수평면에 대해 무지향성

● 지향성 안테나

- 수직과 수평으로 나뉨
- 목표 방향을 지정하여 그 방향의 전파만 탐지하기 때문에 통신 거리가 더 긴 편
- 지향성 안테나는 보통 쟁반 또는 접시 모양

● 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	수 KM
접시형 안테나 + 지향성 증폭 안테나	50 ~ 60Km

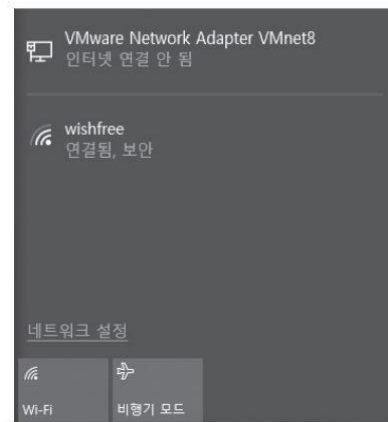
AP 보안

물리적인 보안 및 관리자 패스워드 변경

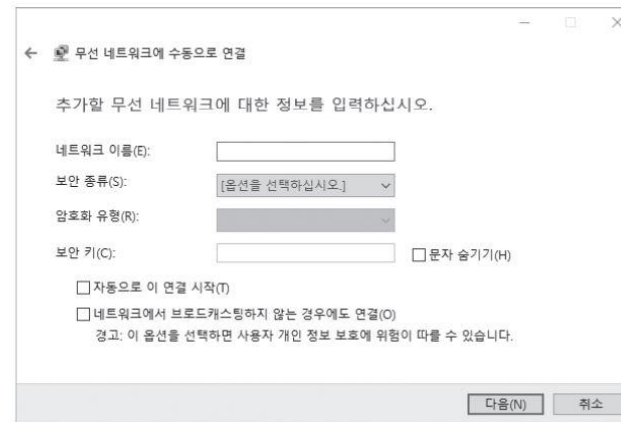
- AP는 전파가 건물 내에 한정되도록 전파 출력을 조정
- 창이나 외부에 접한 벽이 아닌 건물 안쪽 중심부의 눈에 쉽게 띄지 않는 곳에 설치
- 설치 후에는 AP의 기본 계정과 패스워드를 반드시 재설정

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 접속할 수 있게 해야함
- 높은 수준의 보안 권한이 필요한 무선 랜은 대부분 SSID 브로드캐스팅을 차단



(a) AP 목록: SSID 브로드캐스팅을 금지하지 않은 경우



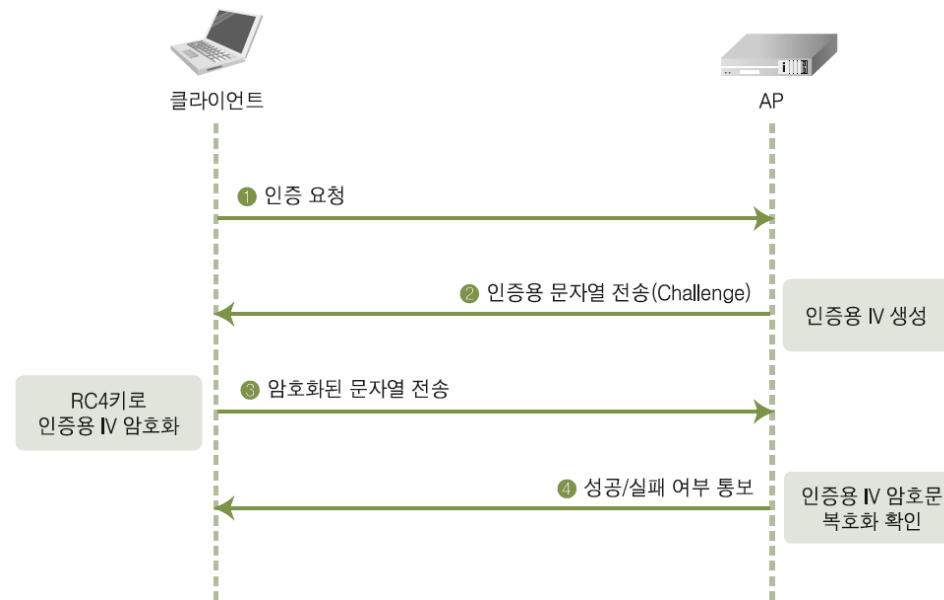
(b) SSID를 직접 입력하여 AP에 접속: SSID 브로드캐스팅을 금지한 경우

그림 3-49 AP 접근 방법

무선 랜 통신의 암호화

WEP

- 무선 랜을 암호화하는 가장 기본적인 방법



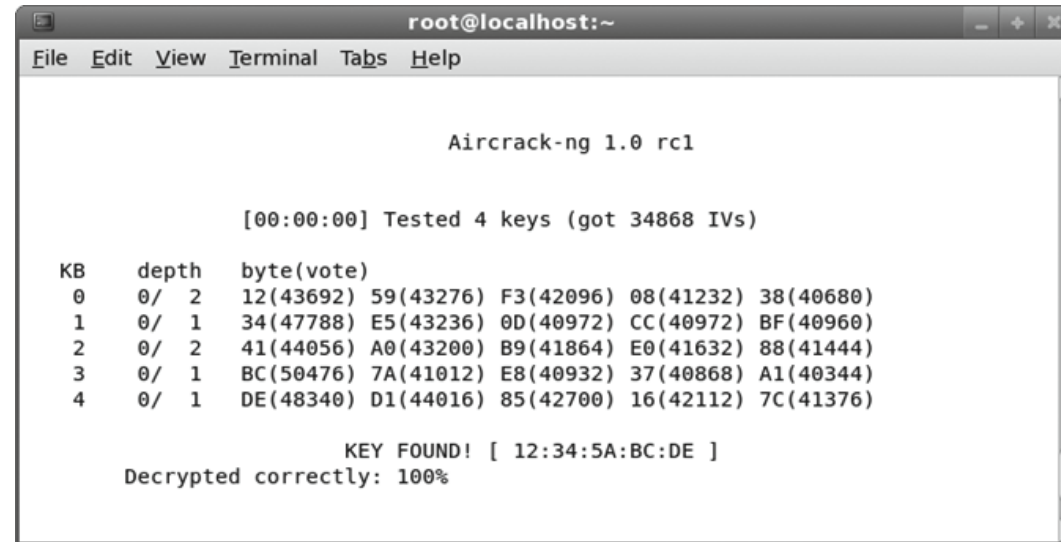
[그림 3-53] WEP 암호화 세션의 생성 과정

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

무선 랜 통신의 암호화

WEP

- 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 3-54] 복호화된 WEP 키

무선 랜 통신의 암호화

WPA-PSK

- 802.11i 보안 표준의 일부분으로 WEP 방식 보안의 문제점을 해결하기 위해 만들어짐
- 802.11i에는 WPA-1과 WPA-2 규격이 포함되어 있는데 이는 암호화 방식에 따른 분류
- WPA 규격은 WPA-개인, WPA-엔터프라이즈로 규정되어 있는데 무선 랜 인증 방식에 사용되는 모드에 따른 구분

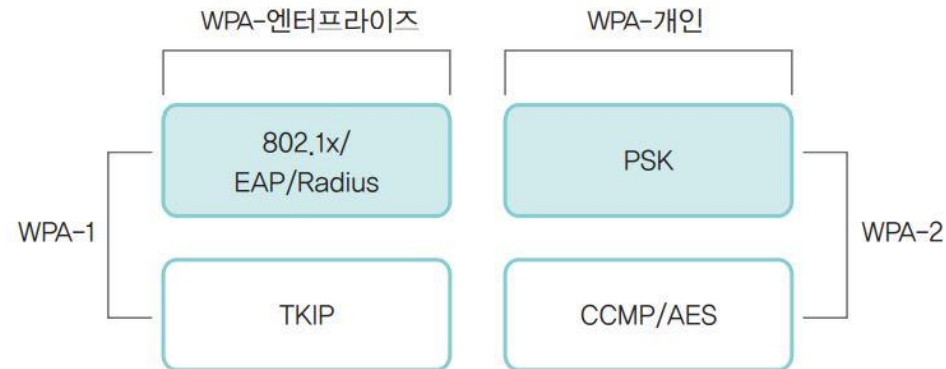


그림 3-53 WPA 규격의 구조

- 무선 전송 데이터의 암호화 방식 중에서 TKIP(WPA-1) 방식은 WEP의 취약점을 해결하기 위해 제정된 표준
- CCMP(WPA-2)는 128비트 블록 키를 사용하는 CCM모드의 AES 블록 암호 방식을 사용
- TKIP가 RC 4를 암호에 사용하는 반면 CCMP는 AES를 기반으로 함

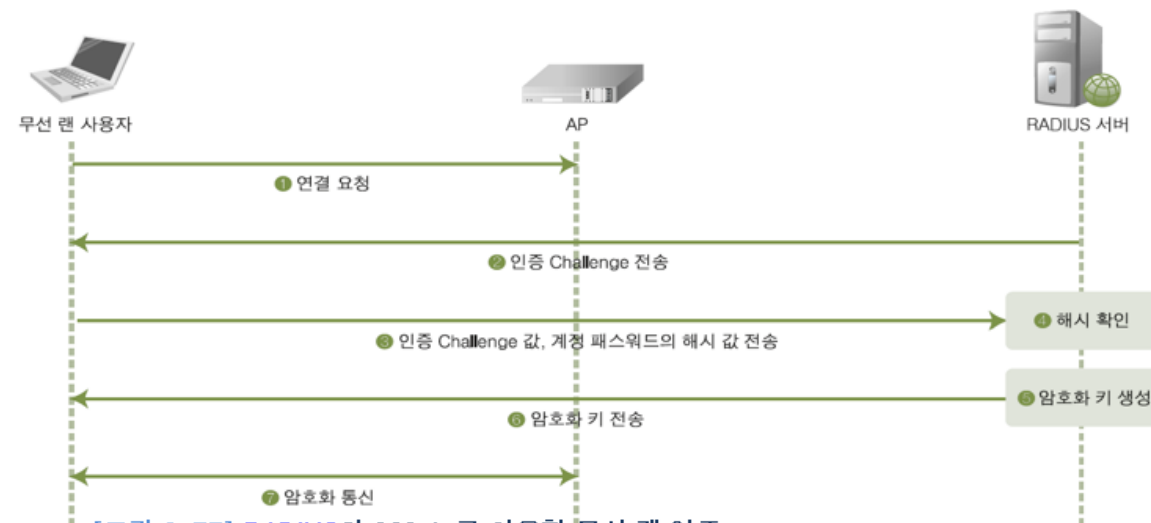
무선 랜 통신의 암호화

EAP와 802.1x의 암호화

- WPA-엔터프라이즈(EAP)는 인증 및 암호화를 강화하기 위해 다양한 보안 표준과 알고리즘을 채택
- 그 중 가장 중요하고 핵심적인 사항은 IEEE 802.1x 표준과 IETF의 EAP 인증 프로토콜을 채택한 점
- 802.1x/EAP는 개인 무선 네트워크의 인증 방식에 비해 다음과 같은 기능이 추가
 - 사용자 인증을 수행
 - 사용 권한을 중앙에서 관리
 - 인증서, 스마트카드 등 다양한 인증을 제공
 - 세션별 암호화 키를 제공
- WEP 또는 WPA-PSK가 802.1x/EAP와 근본적으로 다른 차이점
 - 아이디와 패스워드를 통한 사용자 인증
 - 무선 랜 연결(세션)별로 재사용이 불가능한 다른 암호화 키를 사용

무선 랜 통신의 암호화

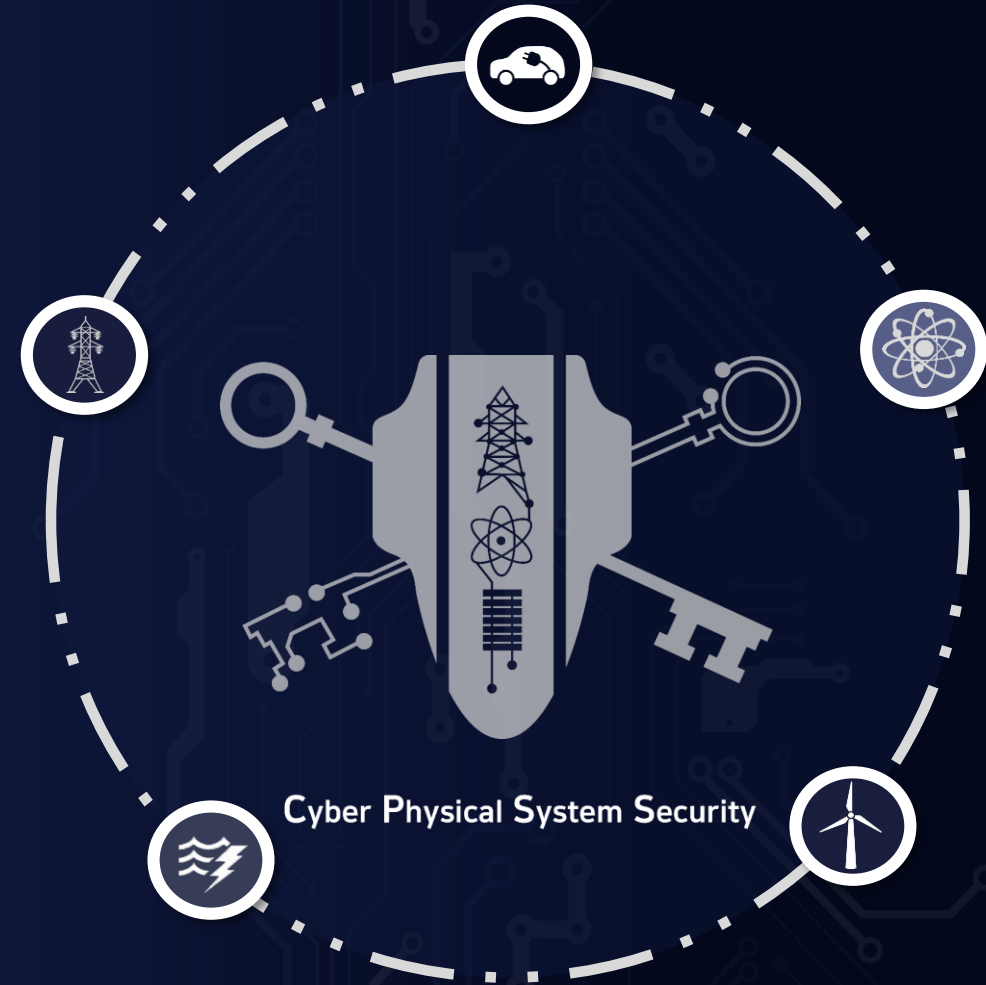
EAP와 802.1x의 암호화 방법



[그림 3-55] 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 서버**는 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



Thank You

