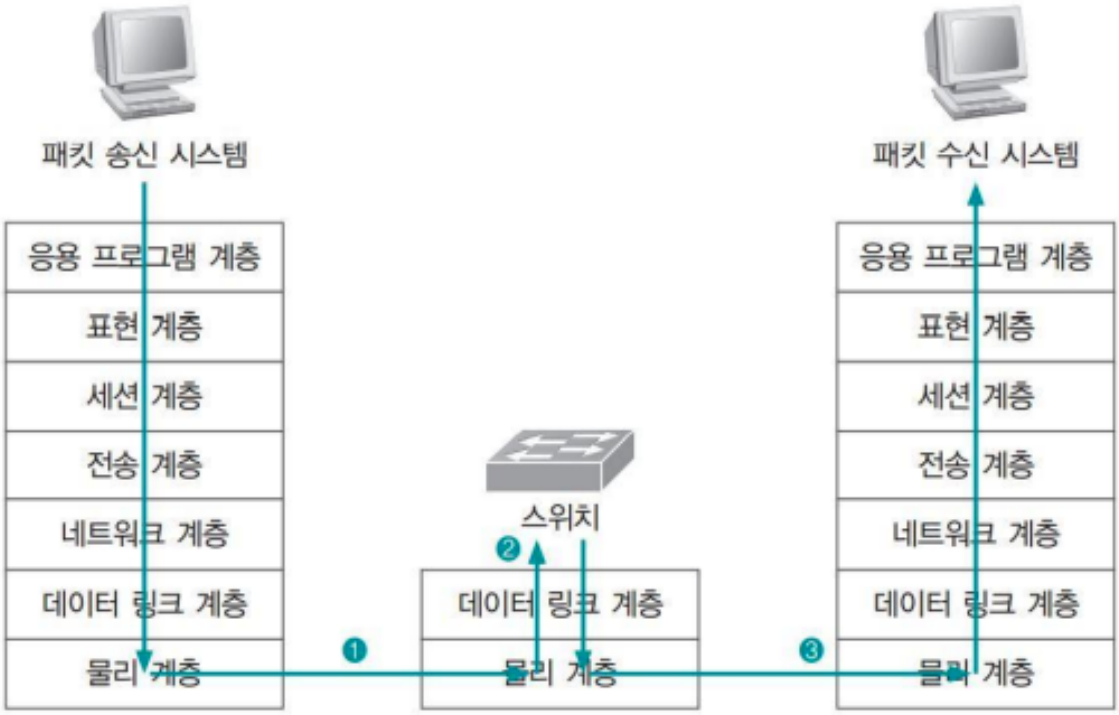
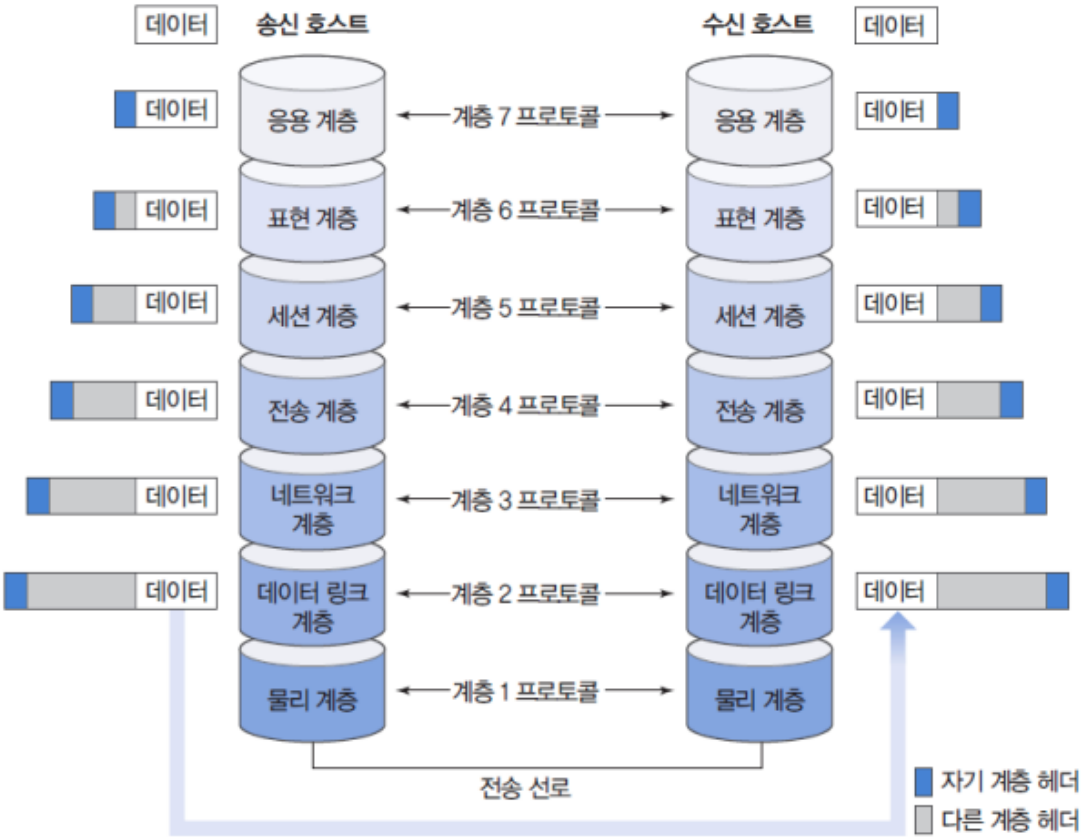
3 / 30

- 학습 목표
  - OSI 7계층의 세부 동작을 이해한다.
  - 네트워크와 관련된 해킹 기술의 종류와 방법을 알아본다.
  - 네트워크 해킹을 막기 위한 대응책을 알아본다.
  - 무선 네트워크에서 벌어지는 공격과 이에 대한 보안을 알아본다.
- 네트워크의 이해
  - OSI 7계층의 이해
    - 국제 표준화 기구(ISO)는 다양한 네트워크 간의 호환을 위해 만든 표준 네트워크 모델
  - 7계층(응용 프로그램 계층)
    - 응용 프로세스와 직접 관계하여 일반적인 응용 서비 수행
  - 6계층 (표현 계층)
    - 코드 간의 번역을 담당하는 계층, 사용자 시스템에서 데이터 구조를 통일하여 응용 프로그램 계층에서 데이터 형식의 차이로 인해 발생하는 부담을 덜어줌
  - 5계층 (세션 계층)
    - 양 끝단의 응용 프로세스가 통신을 관리하는 방법 제공
  - 4계층 (전송 계층)
    - 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해줌
  - 3계층 (네트워크 계층)
    - 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

- 2계층 (데이터 링크 계층)
  - 두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층. 16진수 12개로 구성된 MAC주소 사용
- 1계층 (물리 계층)
  - 실제 장치를 연결하기 위한 전기적, 물리적 세부 사항을 정의한 계층으로 랜선 등이 포함됨




데이터
송신 호스트
수신 호스트
데이터
응용 계층
계층 7 프로토콜
응용 계층
표현 계층
계층 6 프로토콜
표현 계층
세션 계층
계층 5 프로토콜
세션 계층
전송 계층
계층 4 프로토콜
전송 계층
네트워크 계층
계층 3 프로토콜
네트워크 계층
데이터 링크 계층
계층 2 프로토콜
데이터 링크 계층
물리 계층
계층 1 프로토콜
물리 계층
전송 선로
자기 계층 헤더
다른 계층 헤더

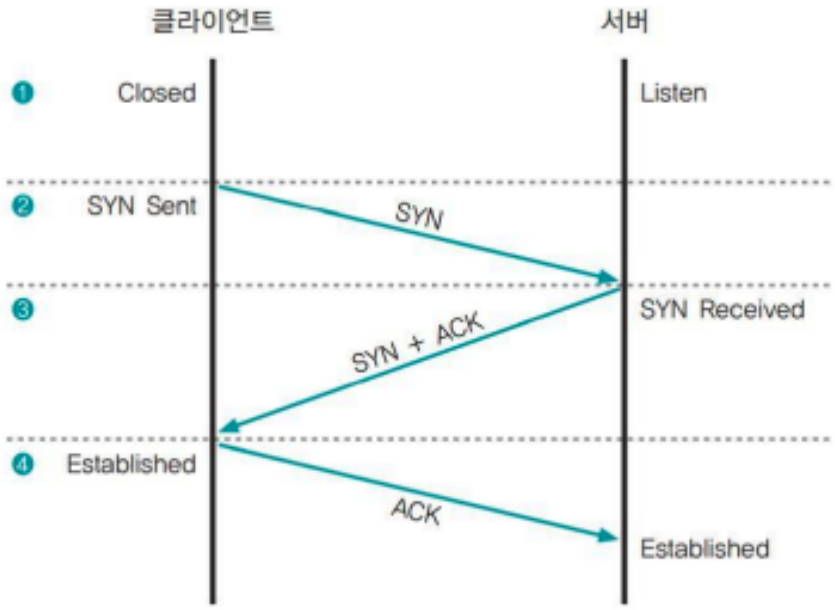


그림 3-13 TCP의 연결 설정 과정

- 서비스 거부 공격
  - 정상적인 서비스을 방해하는 공격
  - 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
      - TCP 취약점 악용
      - 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 (Seq No. 변조)
- 보잉크, 봉크, 티어드롭은 공격 대상이 반복적인 재요청과 수정을 계속하게 함으로써 시스템 자원을 고갈시킴
- 티어드롭은 패킷의 시퀀스 넘버와 길이를 조작하여 패킷 간의 데이터 부분이 겹치거나 빠진 상태로 패킷을 전송하는 공격 방법
- 해결 방안
    - 패치관리를 통해 과부하가 걸리거나 계속 반복되는 패킷을 무시하고 버리도록 처리

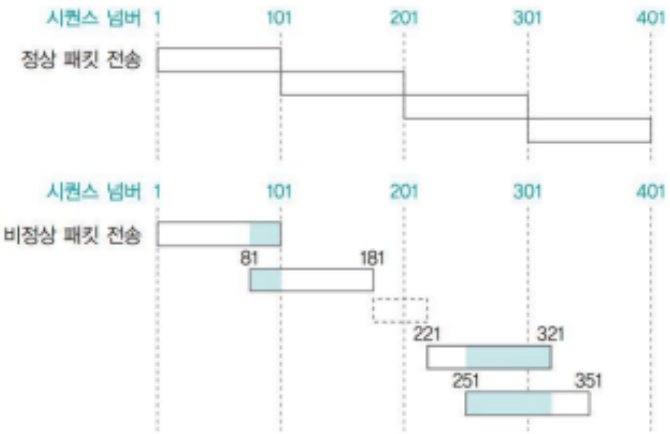


그림 3-17 티어드롭 공격 시 패킷의 배치

표 3-5 티어드롭 공격 시 패킷의 시퀀스 넘버

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

- 랜드 공격(src = dst)

- land의 뜻 → 땅, 착륙하다 이외에 (나쁜 상태에) 빠지게 하다.라는 뜻
- 패킷을 전송할 때 출발지 IP주소와 목적지 IP 주소의 값을 똑같이 만들어서 공격 대상에게 보내는 것
- 이 공격법은 SYN 플러딩처럼 동시 사용자 수를 점유하고, CPU 부하를 올려서 시스템이 금방 지쳐버리게 만듬
- 랜드 공격에 대한 보안 대책은 주로 운영체제의 패치 관리를 통해 마련

- Ping 공격
  - NetBIOS 해킹과 함께 시스템을 파괴하는 데 가장 흔히 쓰인 초기의 DoS 공격 방법
  - 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
- SYN 플러딩 공격
  - 네트워크에서 서비스를 제공하는 시스템에는 동시 사용자 수 제한이 있는데 이를 이용한 공격
  - 존재하지 않는 클라이언트가 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 함
  - TCP의 연결 과정인 3-Way 핸드셰이킹의 문제점을 악용하는 것
  - 특정 웹 서버의 접속자가 폭주하여, 서버 접속이 되지 않고 마비되는 경우도 이 공격을 받은 상황과 유사
  - 공격 대응책은 SYN Received의 대기 시간을 줄이는 것
  - 침입 방지 시스템과 같은 보안 시스템으로도 공격을 쉽게 차단할 수 있음.

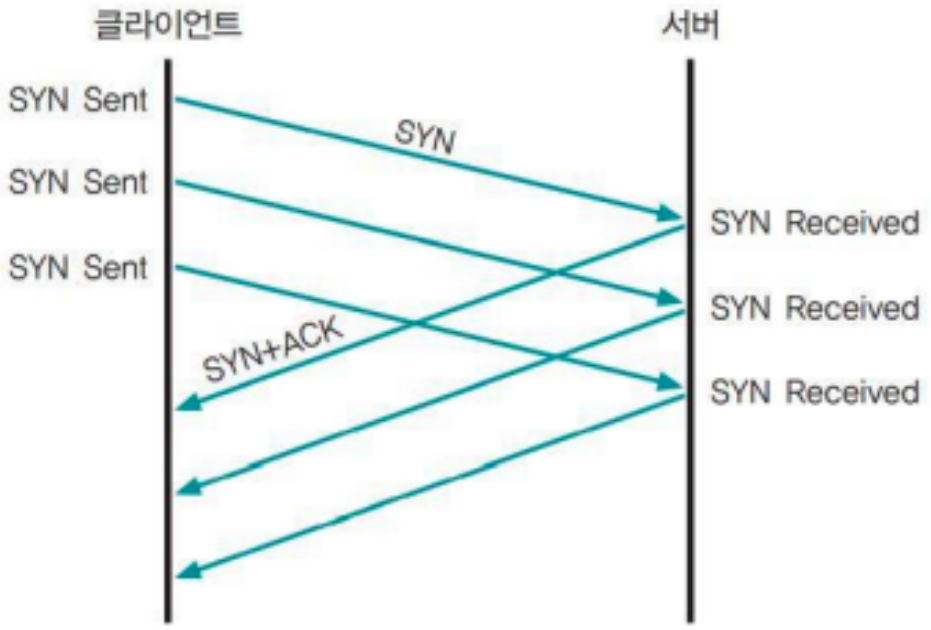


그림 3-21 SYN 플러딩 공격 시 3-웨이 핸드셰이킹

- HTTP 공격
  - HTTP GET Flooding 공격
    - 공격 대상 시스템에 TCP 3-웨이 핸드셰이킹 과정으로 정상 접속한 뒤 HTTP의 GET 메소드로 특정 페이지를 무한대로 실행하는 공격
    - 공격 패킷을 수신하는 웹 서버 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 HTTP요청 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 때 까지 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
- 스머프 공격
    - ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용하여, 패킷을 확장함으로써 서비스 거부 공격을 수행
    - 다이렉트 브로드캐스트를 악용하는 것으로 공격 방법이 간단
    - 스머프 공격 예시 : 거짓말 쟁이 스머프는 공격자 / 멀뚱이 스머프는 공격 대상
    - 다이렉트 브로드캐스트
        - 기본적인 브로드 캐스트는 목적지 IP 주소 255.255.255.255를 가지고 네트워크의 임의 시스템에 패킷을 보내는 것
        - 브로드 캐스트는 기본적으로 네트워크 계층 장비인 라우터를 넘어가지 못함
        - 라우터를 넘어가서 브로드 캐스트를 해야 하는 경우에는 클라이언트의 IP 주소 부분에 브로드 캐스트 주소인 255를 채움 (예 : 공격자가 172.16.0.255)
    - ICMP request를 받은 172.16.0.0 네트워크는 패킷의 위조된 시작 IP주소로 ICMP request ICMP request ICMP reply를 재전송
    - 공격 대상은 수많은 ICMP reply를 받게 되고, 수많은 패킷이 시스템을 과부하 상태로 만듬
    - 대응책

- 라우터에서 다이렉트 브로드 캐스트를 막아서 대응함.

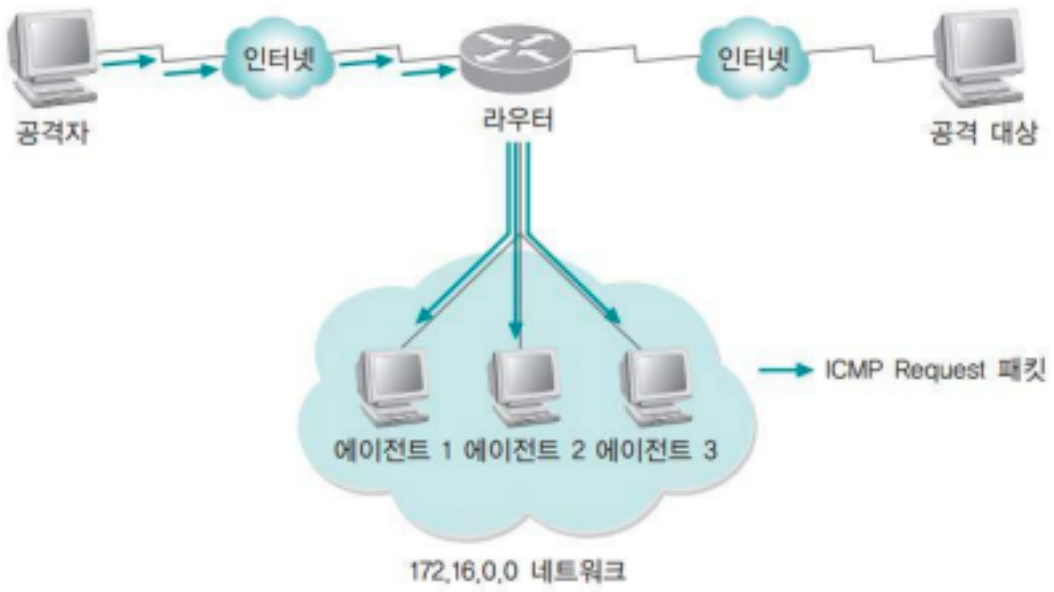


그림 3-23 공격자에 의한 에이전트로의 브로드캐스트

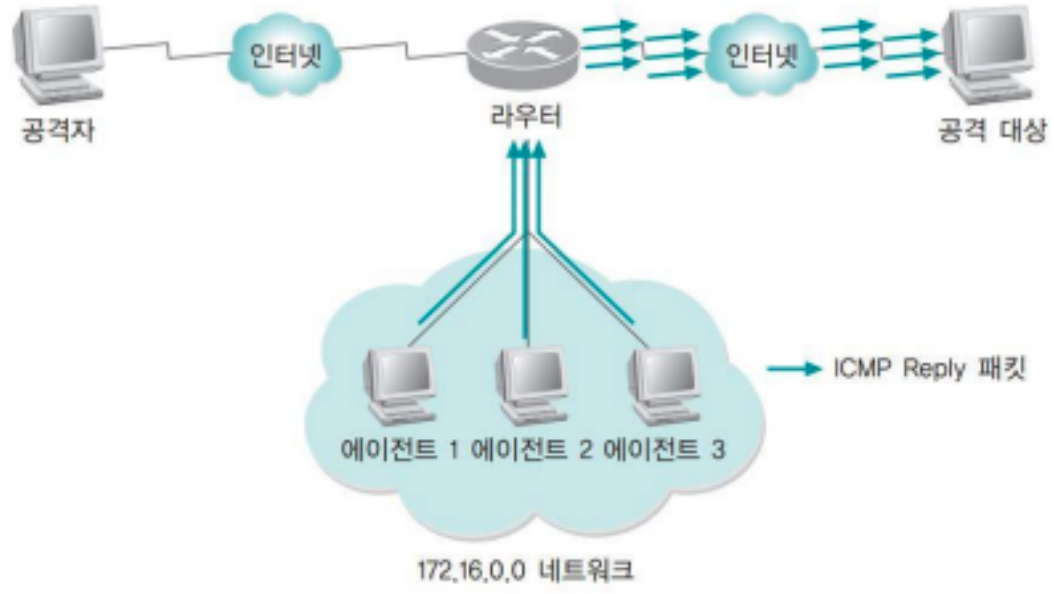
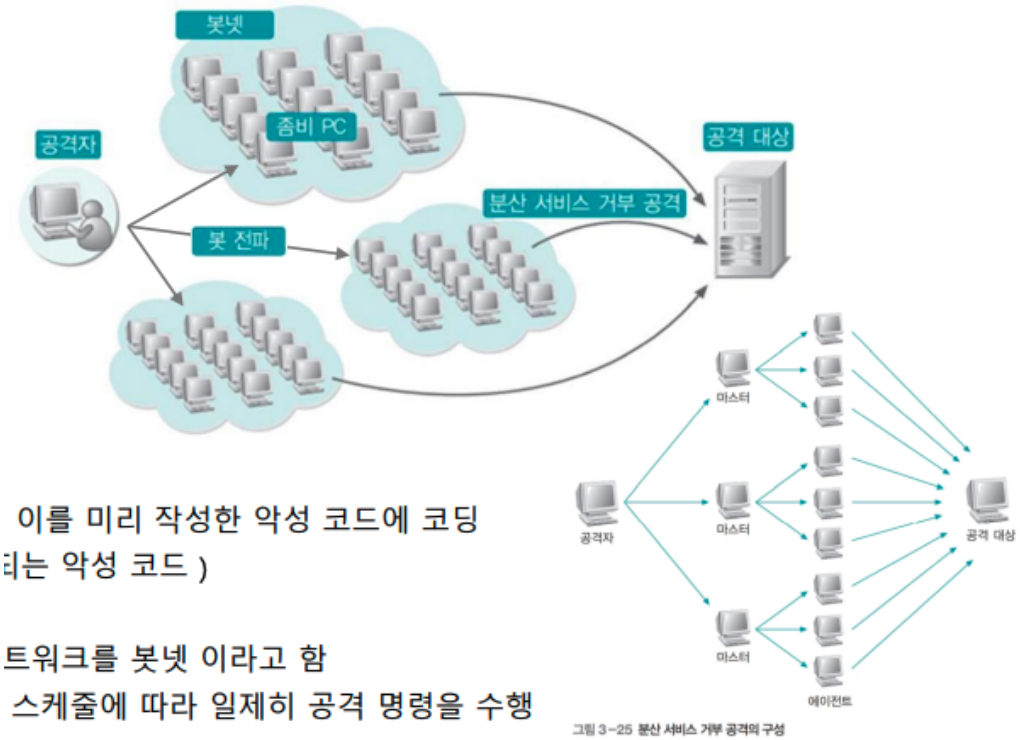


그림 3-24 에이전트에 의한 스머프 공격 실행

- 분산 서비스 거부 공격 (DDOS)
  - 사례
    - 1999년 미네소타대학에서 처음 발생하여 야후, NBC, CNN 서버의 서비스를 중지
  - 아직까지 확실한 대칙이 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
  - 에어전트 → 직접 공격을 가하는 시스템
  - 데몬 프로그램 → 에이전트 시스템의 역할 을 수해하는 프로그램
  - 마스터와 에이전트가 중간자인 동시에 피해자
- 분산 서비스 공격 과정
  1. PC에서 전파가 가능한 형태의 악성 코드를 작성
  2. 분산 서비스 거부 공격을 위해 사전 공격 대상과 스케줄을 정한 뒤 이를 미리 작성한 악성 코드에 코딩
  3. 인터넷을 통해 악성 코드를 전파, 전파 과정에서는 별다른 공격 없이 잠복, 악성코드에 감염된 PC를 좀비 PC라고 하며, 좀비 PC끼리 형성된 네트워크를 봇넷이라고 함
  4. 공격자가 명령을 내리거나 봇넷을 형성한 좀비 PC들이 정해진 공격 스케줄에 따라 일제히 공격 명령을 수행



이를 미리 작성한 악성 코드에 코딩
는 악성 코드)

트워크를 봇넷 이라고 함
스케줄에 따라 일제히 공격 명령을 수행

그림 3-25 분산 서비스 거부 공격의 구성

    - 자원 고갈 공격형
        - 네트워크 대역폭이나 시스템의 CPU, 세션 등의 자원을 소모시키는 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
- Sniffing 공격
    - 스니핑 공격의 원리
        - 네트워크 카드는 패킷의 IP 주소와 MAC 주소를 인식하고 자신의 버퍼에 저장할지를 결정
        - 네트워크 카드에 인신된 데이터 링크 계층과 네트워크 계층의 정보가 자신의 것과 일치하지 않는 패킷을 무시
        - 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 프로미스큐어스 모드로 변경 (참고 : 자신 MAC아니면 버림)
            - 프러미스큐어스 모드
                - 데이터 링크 계층과 네트워크 계층의 필터링을 해제하는 랜 카드의 모드
    - 스니핑 공격의 종류
        - 스위치 재밍 공격 (MACOF 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 초과시킴 (고가의 스위치는 MAC 테이블의 캐시와 연산자가 쓰는 캐시가 독립적으로 나뉘어 있어 통하지 않음)
        - SPAN 포트 태핑 공격
            - 침입 탐지 시스템을 설치하거나 네트워크 모니터링을 할 때 또는 로그 시스템을 설치할 때 많이 사용 (포트 미러링 기능 이용)
            - SPAN 포트는 기본적으로 네트워크 장비에서 간단한 설정으로 활성화 되나, 포트 태핑은 하드웨어 장비를 이용

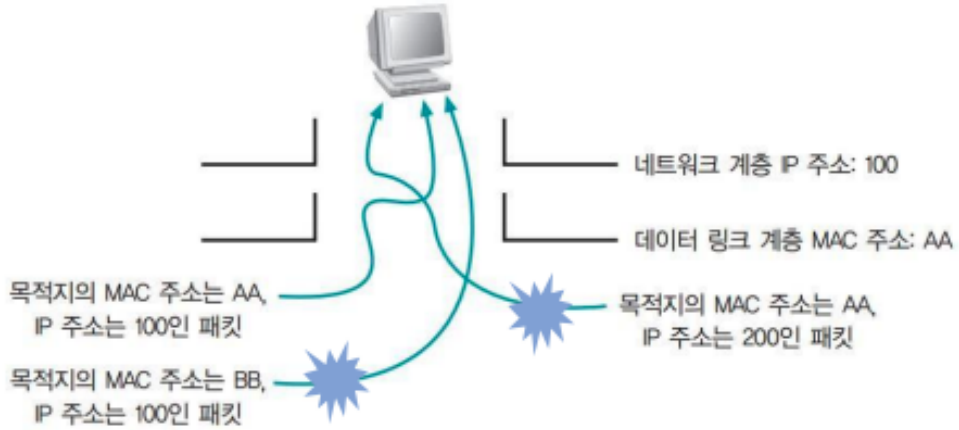


그림 3-31 네트워크 필터링 해제 상태(프러미스큐어스 모드)의 예

- 스니핑 공격의 탐지
  - 특성
    - action을 취하지 않으면 반응하지 않는 특성(감지 모드로 동작 / 도청)
  - 탐지 원리
    - 프러미스큐어스 모드에서 작동한다는 점을 이용
  - ping을 이용한 스니퍼 탐지
    - TCP/IP에서 동작하기 때문에 request를 받으면 response를 전달
    - 의심이 가는 호스트에 네트워크에 존재하지 않는 MAC 주소를 위장해서ping을 보냈을 때, ICMP echo reply를 받으면 해당 호스트가 스니핑을 하고 있는 것으로 판단
  - ARP를 이용한 스니퍼 탐지
    - 위조된 ARP request를 보냈을 때 ARP response 오면 프러미스큐어스 모드로 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
  - 유인을 이용한 스니퍼 탐지

    - 스니핑 공격을 하는 공격자의 주요 목적은 아이디와 패스워드 획득
    - 보안 관리자는 이 점 을 이용하여 가짜 아이디와 패스워드를 네트워크에 계속 뿌림
    - 공격자가 이 아이디와 패스워드로 접속을 시도할 때 스니퍼를 탐지
- ARP watch를 이용한 스니퍼 탐지
    - ARP watch
        - MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링 하여 이를 변하게 하는 패킷이 탐지되면 관리자에게 알려주는 툴
    - 대부분의 공격 기법은 위조된 ARP를 사용하기 때문에 쉽게 탐지할 수 있음

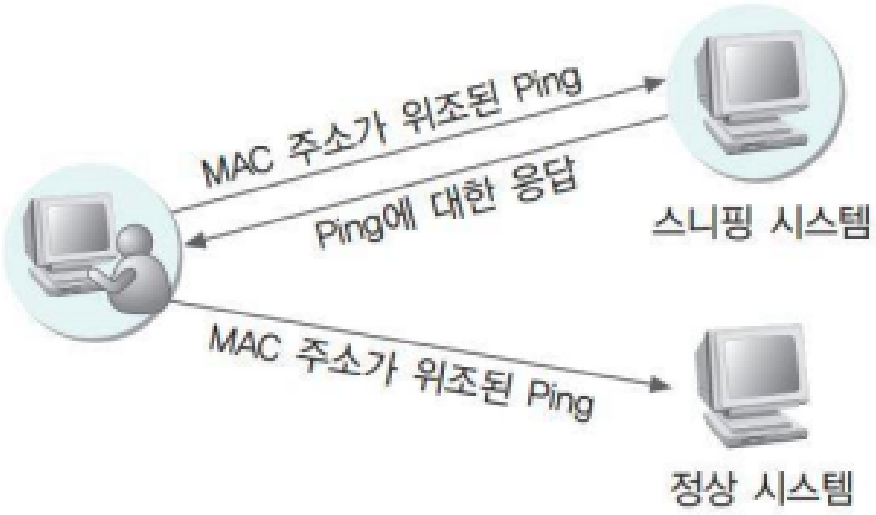
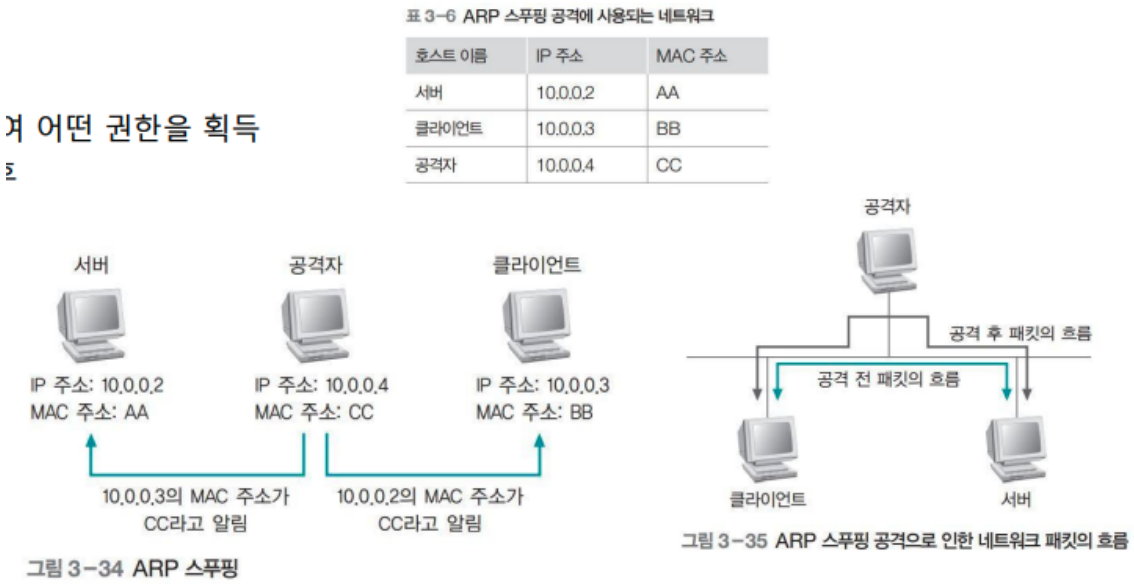


그림 3-33 ping을 이용한 스니퍼 탐지

- Spoofing 공격
    - ARP 스푸핑
        - 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 Table 변조

- IP 스푸핑
  - IP 주소를 속이는 것으로, 다른 사용자의 IP를 강탈하여 어떤 권한을 획득
  - 트러스트를 맺고 있는 서버와 클라이언트를 확인한 후 클라리언트에 서비스 거부 공격을 하여 연결을 끊음
  - 클라이언트의 IP주소를 확보하여 실제 클라이언트처럼 패스워드 없이 서버에 접근
- iCMP 리다이렉트
  - 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알려 패킷의 흐름을 바꾸는 공격
  - ICMP 리다이렉트의 동작



- DNS 스푸핑
  - 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 쇼핑몰이나 포르노 사이트가 뜨는 경우
  - DoS 공격이 되지만, 이를 조금만 응용하면 웹 스푸핑이 됨

- 자신의 웹 서버를 하나 만들고, 공격 대상이 자주 가는 사이트를 하나 골라스 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

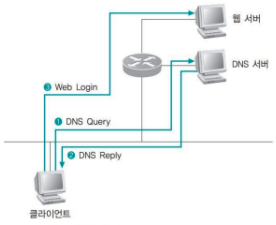


그림 3-41 정상적인 DNS 서비스

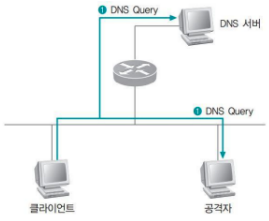


그림 3-42 DNS 스푸핑 공격: DNS Query

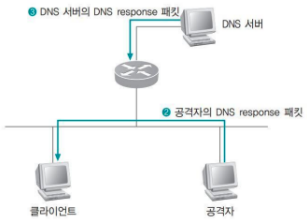
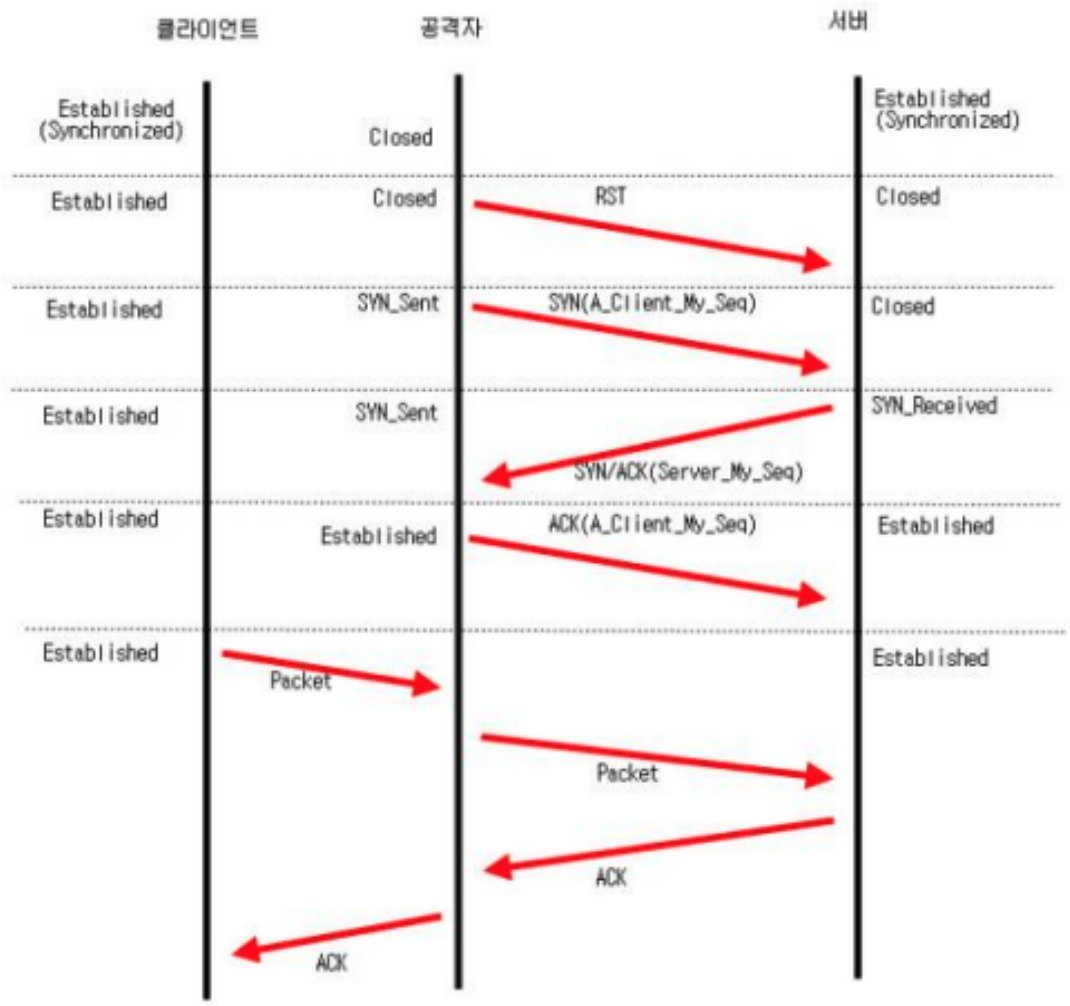


그림 3-43 DNS 스푸핑 공격: 공격자와 DNS 서버의 DNS response

- Session hijacking 공격
  - TCP 세션 하이재킹
    - TCP 세션에 대한 탈취 가로채기
  - TCP 세션 하이재킹의 기본적인 단계
    1. 클라리언트와 서버 사이의 패킷을 통제. ARP 스푸핑 등을 통해 클라이언트와 서버 사이의 통신 패킷이 전부 공격자를 지나가게 함
    2. 서버에 클라이언트 주소로 연결을 재설정하기 위한 RSTreset패킷을 보냄. 서버는 패킷을 받아 클라이언트의 시퀀스 넘버가 재설정된 것으로 판단하고 다시 TCP 3-웨이 핸드셰이킹을 수행
    3. 공격자는 클라이언트 대신 연결되어 있는 TCP 연결을 그대로 물려받음
  - MAC 주소를 고정하는 방법
    - ARP 스푸핑을 막아주기 때문에 결과적으로 세션 하이재킹을 막을 수 있음



- 무선 네트워크 공격
  - 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 수십 m에서 길게는 1 ~ 2 Km까지도 가능

시기	프로토콜	주요 사항	설명
2014년	802.11ad	60GHz	최대 속도가 7Gb/s다. 기존 2.5GHz/5GHz 대신 60GHz 대역을 사용하여 데이터를 전송하는 방식으로, 대용량 데이터나 무압축 HD 비디오 등 높은 비트레이트 동영상 스트리밍에 적합하다. 60GHz는 장애물을 통과하기 어려워서 10m 이내 같은 공간 내에서 근거리 기기에만 사용할 수 있다.
2017년	802.11ah	1GHz 미만 주파수 대역(일반적으로 900Mhz 대역)	와이파이 할로우(HaLow). TV 대역을 제외한 비허가(license-exempt) 네트워크 운영을 정의한다. 세부 주파수는 국가마다 다르다. 802.11ah의 목적은 최대 347Mbps의 데이터 전송 속도로 2.4GHz와 5GHz 영역의 일반적인 네트워크보다 더 먼 거리까지 와이파이 네트워크를 확장하는 것이다. 에너지 소비 절감에도 초점을 두고 있어 많은 에너지를 사용하지 않으면서 원거리 통신이 필요한 사물 인터넷 기기에 적합하여 블루투스 기술과도 경쟁한다.
	802.11ay	60GHz	차세대 60GHz로도 알려진 표준 프로토콜. 60GHz 주파수 내에서 20Gbps 이상의 최대 처리량을 제공하고(현재 802.11ad는 최대 7Gbps) 거리와 안정성도 개선하는 것을 목표로 한다.

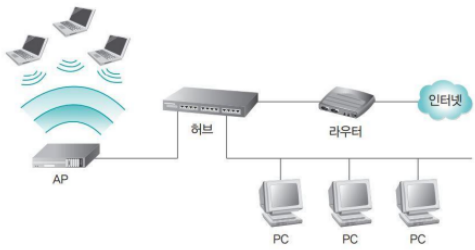


그림 3-46 유선 네트워크에 연결된 AP로 무선 랜까지 확장된 네트워크

- 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 브로드캐스팅 금지
  - SSID: 무선 랜 네트워크를 검색시 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

- 무선 랜 통신의 암호화
  - 무선 랜은 통신 과정에서 데이터 유출을 막는 것뿐 아니라 네트워크에 대한 인증을 위해서도 암호화를 수행
- WEP
  - 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용
  - 1987년에 만들어진 RC 4 암호화 알고리즘을 기본으로 사용
  - 64비트와 128비트를 사용할 수 있는데 64비트는 40비트, 128비트는 104비트의 RC 4키를 사용
  - WEP는 암호화 과정에서 암호화 키와 함께 Key(24비트의 IV)를 사용
- WPA-PSK
  - 802.11i 보안 표준의 일부분으로 WEP 방식 보안의 문제점을 해결하기 위해 만들어 짐
  - 802.11i에는 WPA-1과 WPA-2 규격이 포함되어 있는데 이는 암호화 방식에 따른 분류
  - 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

- EAP와 802.1x 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

[별첨] 유무선 통합 인증 구조

▪ 802.1x/EAP와 RADIUS 서버를 이용한 무선 랜 사용자 인증

❶ 클라이언트가 AP에 접속을 요청함, 이때 클라이언트와 AP는 암호화되지 않은 통신을 수행.
(클라이언트가 AP와 연결된 내부 네트워크로 접속하는 것은 AP에 의해 차단)

❷ RADIUS 서버는 클라이언트에 인증 Challenge를 전송

❸ 클라이언트는 Challenge에 대한 응답으로 맨 처음 전송받은 Challenge 값, 계정, 패스워드에 대한 해시 값을 구하여 RADIUS 서버로 전송

❹ RADIUS 서버는 사용자 관리 DB 정보에서 해당 계정의 패스워드를 확인
(연결 생성을 위해 최초로 전송한 Challenge의 해시 값을 구하여 클라이언트로부터 전송받은 해시 값과 비교)

❺ 해시 값이 일치하면 암호화 키를 생성

❻ 생성한 암호화 키를 클라이언트에 전달

❼ 전달받은 암호화 키를 이용하여 암호화 통신을 수행

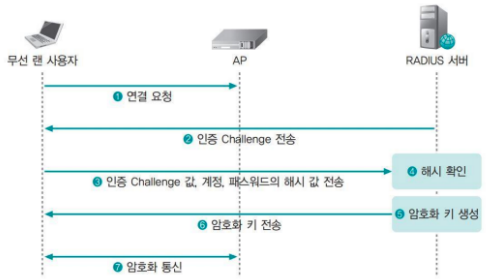


그림 3-54 RADIUS와 802.1x를 이용한 무선 랜 인증