제9주차 1교시

강의주제 IPv6의 개념과 체계

학습목표

1. IPv6의 개념을 정의할 수 있다.
2. 네트워크 계층 프로토콜의 개념을 정의할 수 있따.
3. 주소 변환 프로토콜(ARP)을 설명할 수 있다.
4. 역주소 변환 프로토콜(RARP)을 설명할 수 있다.

학습내용

1. IPv6의 개념
2. 네트워크 계층 프로토콜의 개념
3. 주소 변환 프로토콜(ARP)
4. 역주소 변환 프로토콜(RARP)

사전학습

기존 IPv4가 존재하는데도 불구하고 IPv6가 필요한 이유는 무엇이라고 생각하나요?

본 학습

1. IPv6의 개념

1) IPv6 도입 필요성

- 한 조직이 A 클래스의 주소를 할당받으면 호스트 1,600만 개를 할당받을 수 있음
- 그러나 C클래스는 주소를 256개만 할당받을 수 있는데 이 수는 충분치 못함
- 또한 D 클래스와 E 클래스에서도 주소 수백만 개가 낭비되고 있음
- IPv4는 산술적으로 주소를 43억 개 할당할 수 있지만 클래스별 주소 분류 방식 때문에 사용하지 않는 주소가 많음
- 4차 산업혁명 시대에는 단말기마다 IP가 부여되는 환경이 필요하므로 IPv4를 사용하면 IP 주소가 부족하게 됨
- 인터넷의 폭발적인 성장으로 32비트로 구성된 IPv4 주소 공간(약 40억 개)은 이미 고갈 상태
- IPv6는 전 세계 60억 인구가 1인당 53,731,028개의 주소를 할당받을 수 있기 때문에 주소 부족 현상이 일어나지 않을 것임
- IPv6는 128비트로 구성되며, 긴 주소를 쉽게 읽을 수 있도록 16비트씩 콜론(:)으로 나누어 각 필드를 16진수로 표현하는 방법을 사용
- 기존의 IPv4 주소도 하위 32비트는 IPv4 주소를 그대로 채우고 상위 비트는 모두 0으로 채워 IPv6 주소로 표현할 수 있음

2) IPv6의 특징

- IPv6 주소의 길이는 128비트(32비트인 IPv4 주소와 비교하면 주소 공간 길이가 4배 증가)
- IPv6는 옵션을 기본 헤더에서 분리하여 필요할 때마다 기본 헤더와 상위 계층 데이터 간에 새로운 확장 헤더를 삽입해서 사용
- 대부분의 옵션은 라우터로 검사할 필요가 없으므로 라우팅이 더 빠름
- IPv6의 경우 새로운 기술이나 응용 분야에서 요구되는 프로토콜의 확장을 허용하도록 설계
- 서비스 유형 필드를 삭제하고 플로우 레이블 항목을 추가하여 송신자가 패킷에 특별한 처리를 요청할 수 있음
- 암호화와 인증 옵션 기능 등 IPv4보다 향상된 보안 환경 제공

3) IPv4와 IPv6 주소 체계 비교

- ipconfig 명령을 실행하여 IP 주소 확인

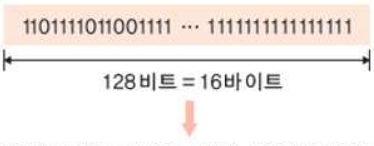
```
C:₩Users₩Administrator>ipconfig

Windows IP 구성

이더넷 어댑터 이더넷:

   연결별 DNS 접미사. . . . :
   링크-로컬 IPv6 주소 . . . . : fe80::14ba:a8:263d:ac43%4
   IPv4 주소 . . . . . . . . . . : 192.168.0.2
   서브넷 마스크 . . . . . . . . : 255.255.255.0
   기본 게이트웨이 . . . . . . . : 192.168.0.1
```

- 링크-로컬 IPv6 주소
  - 현재 사용 중인 fe80::으로 시작하는 주소
  - LAN 세그먼트 내에서만 유효한 IPv6 주소
  - DHCP 서버 등이 없어도 자동으로 설정되는 주소
  - 동일한 링크 내에서만 유효한 자동설정 주소
  - 기존 IPv6구조와 다름

4) IPv6 주소

(1) 주소 체계

- IPv6 주소의 128비트는 2바이트의 영역 8개로 구분
- 16진수 표기법에서 2바이트는 16진수 4개로 나타낼 수 있으므로 IPv6 주소는 16진수 32개로 표현
- IPv6 주소에서 앞의 64비트 : 네트워크 주소
- IPv6 주소에서 뒤의 64비트 : 네트워크에 연결된 통신 장비 등에 할당되는 인터페이스 주소



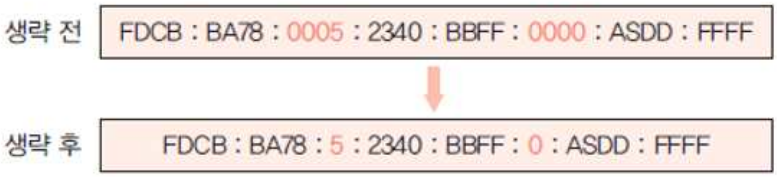
	/0~/16	~/32	~/48	~/64	~/80	~/96	~/112	~/128
16진수 표기법	0000:	0000:	0000:	0000:	0000:	0000:	0000:	0000:
기술적 경계	64비트 네트워크 주소				인터페이스 주소			

- IPv6의 주소 필드는 네트워크 프리픽스 부분(fe80::) 64비트와 인터페이스 ID 부분 64비트로 구성
- IPv6에서는 IP 주소의 후반부를 호스트 ID가 아닌 인터페이스 ID라고 부름
- 인터페이스 ID는 고정 길이(64비트)이며 일반적으로 EUI-64 주소를 사용
- 이더넷에서는 48비트 MAC 주소를 시작 부분 24비트와 끝부분 24비트로 나누고 그 사이에 FFFE를 삽입
- 인터페이스 ID 부분에는 MAC 주소를 기반으로 한 EUI-64 주소 이외에도 다양한 주소를 이용하여 인터페이스를 지정할 수 있음
- 이더넷의 MAC 주소를 ipconfig/all 명령으로 확인

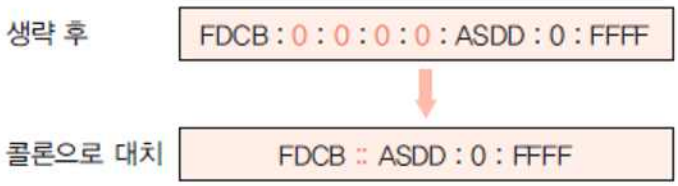
```
연결별 DNS 접미사. . . . :
설명. . . . . . . . . . . : Realtek PCIe GbE Family Controller
물리적 주소 . . . . . . . : FC-AA-14-EC-7F-32
DHCP 사용 . . . . . . . . : 예
자동 구성 사용. . . . . . : 예
링크-로컬 IPv6 주소 . . . . : fe80::14ba:a8:263d:ac43%4(기본 설정)
IPv4 주소 . . . . . . . . : 192.168.0.2(기본 설정)
서브넷 마스크 . . . . . . : 255.255.255.0
임대 시작 날짜. . . . . . : 2022년 9월 15일 목요일 오후 3:32:20
임대 만료 날짜. . . . . . : 2022년 9월 15일 목요일 오후 7:23:59
기본 게이트웨이 . . . . . : 192.168.0.1
DHCP 서버 . . . . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . . . : 234662420
DHCPv6 클라이언트 DUID. . . : 00-01-00-01-29-EE-A2-0B-FC-AA-14-EC-7F-32
DNS 서버. . . . . . . . . : 210.220.163.82
                            219.250.36.130
Tcpip를 통한 NetBIOS. . . . : 사용
```

  - 위 규칙에 따라 변환한 EUI-64 주소 : FCAA:14FF:FEEC:7F32
  - 실제 주소(링크-로컬 IPv6 주소) : fe80::14ba:a8:263d:ac43%4가 인터페이스 ID로 사용
  - EUI-64 주소와 실제 주소가 불일치

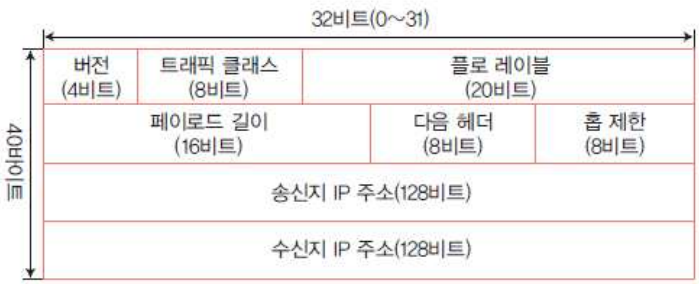
- 윈도우를 비롯해 최근의 운영체제에서는 인터페이스 ID에 MAC 주소를 기반으로 생성된 EUI-64 주소를 사용하지 않을 때가 있음
  - 기기 고유의 MAC 주소를 사용하여 인터페이스 ID를 지정하면 IP 주소를 통해 간단하게 기기를 확인할 수 있기 때문에 보안상의 이유로 해시 함수를 이용하여 일시적으로 생성된 익명 IPv6 주소를 디폴트로 인터페이스 ID로 지정하고 있음
- 128비트의 IP 주소는 두 콜론 사이에 있는 4개의 수(섹션)에서 앞쪽의 0을 생략함으로써 줄여서 표현 가능
  - 이와 같은 생략 방식을 이용하면 0056은 56으로, 000D는 D로, 0000은 0으로 나타낼 수 있음



- 연속된 0으로만(2바이트 이상) 구성된 섹션은 0을 모두 지우고 콜론 2개로 대치할 수 있는데 이는 주소당 한 번만 허용
  - 예를 들어 섹션 2개에 0이 있다면 그 중 주소 하나에만 생략 방식 적용 가능



(2) IPv6 헤더



- IPv6의 각 패킷은 기본 헤더와 페이로드로 구성
- 원칙적으로 IPv4의 기본적인 형식을 계승하고 있으나 IPv4에서 별로 사용되지 않았던 기능은 제거
- IPv6의 헤더는 고정 길이 40바이트로 형식이 간단
- IPv6 기본 헤더의 종류
  - 버전(4비트): IP 버전을 나타내며 값은 6
  - 트래픽 클래스(8비트): IPv4의 TOS 필드 명칭이 바뀐 것으로 QoS용 필드로 0이 들어감
  - 플로 레이블(20비트): 미사용 필드로 일반적으로 0이 들어감
  - 페이로드 길이(16비트): IPv4의 전체 길이 필드 명칭이 바뀐 것으로 기본 헤더를 제외한 IP 데이터그램의 전체 길이를 규정
  - 다음 헤더(8비트): IPv4의 프로토콜 필드 명칭이 바뀐 것으로 데이터그램에서 기본 헤더의 다음 헤더를 정의

- 다음 헤더 코드(필드 값)

코드	다음 헤더	코드	다음 헤더
00	홉-바이-홉 옵션	44	분할 헤더 옵션
02	IGMP	50	ESP 헤더
06	TCP	51	인증 헤더
17	UDP	59	헤더 없음
43	라우팅 헤더 옵션	60	수신지 옵션 헤더

- 홉 제한(8비트): IPv4의 라이프 타임 필드 명칭이 바뀐 것으로 중계 가능한 라우터의 수를 나타내며, 중계할 때마다 값이 줄어들고 0이 되면 패킷을 폐기
- 송신지 IP 주소(128비트): 송신지의 IPv6 주소를 지정
- 수신지 IP 주소(128비트): 수신지의 IPv6 주소를 지정

● IPv6 확장 헤더의 종류

- 홉-바이-홉 옵션 헤더 : 경로상의 각 홉에서 배달 또는 전달 처리 옵션을 지정하기 위해 사용
- 목적지 옵션 헤더 : 패킷의 목적지에서 배달 또는 전달 처리 옵션을 지정하기 위해 사용
- 라우팅 헤더 : 패킷이 목적지에 가는 동안 경유해야 할 라우터를 지정
- 단편화 헤더 : 요청한 페이로드가 MTU보다 크면 IPv6 송신지에서 페이로드를 조각내고, 단편화 옵션 헤더를 사용하여 리어셈블 정보를 제공하여 Destination Node가 재결합
- AH 헤더 : IPSec의 인증 헤더
- ESP 헤더 : IPSec의 인증 및 암호화 헤더

(3) IPv6 주소의 장점

● 확대된 주소 공간 : 주소의 길이가 128비트로 증가하여 2,128개의 주소를 생성할 수 있음
● 단순해진 헤더 포맷 : IPv4 헤더의 불필요한 필드를 제거하여 보다 빠른 처리가 가능
● 간편해진 주소 설정 기능 : IPv6 프로토콜에 내장된 주소 자동 설정 기능을 이용하여 플러그 앤드 플레이 설치가 가능
● 강화된 보안 기능 : IPv6에서는 IPSec 기능을 기본 사항으로 제공
● 개선된 모바일 IP : IPv6 헤더에서 이동성을 지원

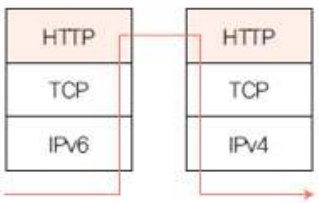
5) IPv4에서 IPv6로의 전환 기술

(1) 전환기술 개요

● 전환 기술은 IPv4 네트워크망과 IPv6 네트워크망 간에 주소 변환기를 이용하여 IP를 상호 연동시키고, 게이트웨이를 이용하여 IPv4와 IPv6 주소 체계를 호환하는 기술
● 전환 기술은 어떤 계층을 거쳐서 변환하는지에 따라 응용 계층 게이트웨이 방식, 전송 계층 릴레이 방식, 헤더 변환 방식으로 구분

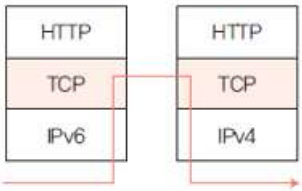
(2) 응용 계층 게이트웨이 방식(응용 계층)

● 변환(트랜잭션) 서비스를 위한 ALG(응용 수준 게이트웨이)
● 웹 사이트 정보를 숨기고 캐시 메커니즘으로 서비스의 성능을 향상하는데 사용
● 응용 계층 게이트웨이 방식은 응용 계층에서 변환됨



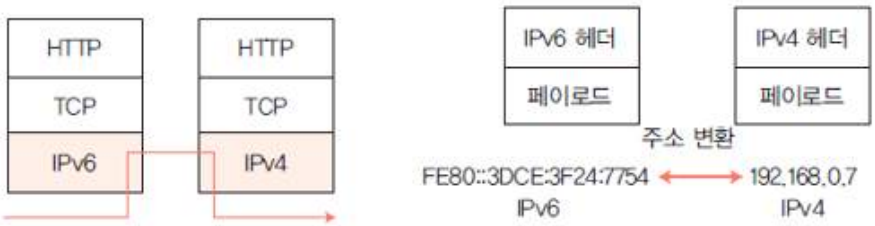
(3) 전송 계층 릴레이 방식(전송 계층)

- TCP/UDP의 IPv4 세션과 TCP/UDP의 IPv6 세션을 중간에서 릴레이



(4) 헤더 변환 방식(네트워크 계층)

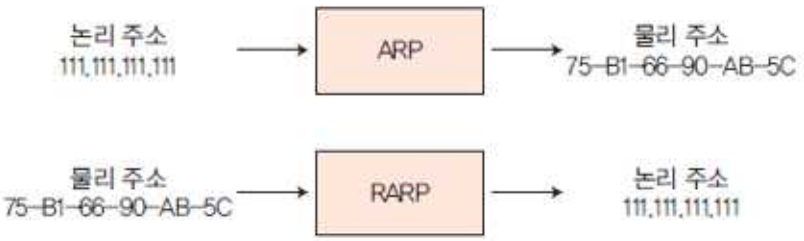
- 네트워크 계층(IP)에서 IPv6 패킷 헤더를 IPv4 패킷 헤더로 또는 IPv4 패킷 헤더를 IPv6 패킷 헤더로 변환하는 것
- 인터넷은 대부분 IPv6를 사용하므로 헤더 변환이 필요 없지만 IPv4를 사용할 때는 헤더 변환이 필요
- 송신 측에서는 IPv6를 사용하려 하는데 수신 측이 이것을 이해하지 못한다면 수신 측이 이해할 수 있는 IPv4 형식으로 패킷의 헤더 형식을 변환
- 헤더 변환은 IP 계층에서의 변환을 의미



2. 네트워크 계층 프로토콜의 개념

1) 개요

- TCP/IP에서 네트워크 계층 프로토콜은 IP, ARP, ICMP, IGMP로 구성
- 전송 계층의 패킷은 세그먼트 형태로 네트워크 계층에 전송
- 네트워크 계층의 데이터는 IP 헤더가 추가된 IP 데이터그램으로 동작
- 송신 측 시스템이 수신 측 시스템으로 패킷을 전송할 때 이 패킷은 물리적인 네트워크를 통과하므로 패킷이 수신 측 시스템에 도착하려면 수신 측의 논리 주소뿐만 아니라 물리 주소도 알아야 함
- ARP는 IP 주소를 받아 네트워크 카드의 물리 주소인 MAC 주소로 변환하는 프로토콜
- RARP(Reverse ARP)는 물리 주소인 MAC 주소를 IP 주소로 변환하는 역주소 변환 프로토콜



3. 주소 변환 프로토콜(ARP)

1) 개요

- IP 프로세스는 물리 주소인 MAC 주소를 모르기 때문에 최종 수신지 호스트까지 신호를 전송하려면 기본 게이트웨이에서 수신지 IP 주소와 관련이 있는 네트워크 카드(LAN 카드)의 MAC 주소를 알아야 함
- 이때 논리 주소인 IP 주소를 물리 주소인 MAC 주소로 매핑하는 것이 바로 주소 변환 프로토콜 ARP임
- 네트워크 카드의 물리 주소는 제조업체에서 생산할 때 결정되므로 네트워크 카드를 교체하면 MAC 주소도 변경됨
- 하지만 IP 주소는 네트워크 카드를 교체해도 동일한 주소를 사용할 수 있음
- 송신지 호스트에서 수신지 호스트로 신호를 전송할 때 수신지 게이트웨이까지는 MAC 주소를 알 필요가 없으나 수신지 게이트웨이에 도달한 후 수신지 호스트까지 신호를 전송하려면 ARP가 동작해야 함
- ARP의 신호 전송은 두 가지 동작으로 완성
  - 하나는 수신지 호스트의 MAC 주소를 알아내는 것
  - 또 하나는 해당 MAC 주소로 데이터를 전송하는 것
- ARP 요청: 특정 IP주소에 대해 MAC주소를 요구, MAC 주소를 알지 못하기 때문에 브로드 캐스트로 전송
- ARP 응답: 요청한 MAC 주소 정보를 유니캐스트로 전송

4. 역주소 변환 프로토콜(RARP)

1) 개요

- 호스트 컴퓨터의 물리 주소를 알고 있을 때 IP 주소를 알아내는데 사용
- RARP는 컴퓨터를 네트워크에 처음 연결할 때나 디스크가 없는 컴퓨터를 부팅할 때 사용하는 프로토콜로 이더넷, 토큰링, FDDI 등 근거리 통신망에서 사용할 수 있음
- RARP 요청: MAC정보를 담고있는 RARP 정보를 브로드 캐스트로 전송
- RARP 응답: 요청자의 IP 주소를 담은 RARP 응답을 유니캐스트로 전송

학습정리

1. IPv6 : IPv6 주소의 길이는 128비트이며 새로운 기술이나 응용 분야에서 요구되는 프로토콜의 확장을 허용하도록 설계
2. IPv6 주소 체계 : IPv6 주소에서 앞의 64비트는 네트워크 주소, IPv6 주소에서 뒤의 64비트는 네트워크에 연결된 통신 장비 등에 할당되는 인터페이스 주소
3. IPv6 헤더 : IPv6의 각 패킷은 기본 헤더와 페이로드로 구성
4. 응용 계층 게이트웨이 방식(응용 계층) : 변환(트랜잭션) 서비스를 위한 ALG(응용 수준 게이트웨이)
5. 주소 변환 프로토콜(ARP) : 논리 주소인 IP 주소를 물리 주소인 MAC 주소로 매핑하는 것
6. 역주소 변환 프로토콜(RARP) : 호스트 컴퓨터의 물리 주소를 알고 있을 때 IP 주소를 알아내는데 사용

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제9주차 2교시

강의주제 IP, ARP 덤프 분석

학습목표

1. 인터넷 제어 메시지 프로토콜(ICMP)을 설명할 수 있다.
2. 인터넷 그룹 메시지 프로토콜(IGMP)을 설명할 수 있다.
3. IP, ARP 덤프 분석을 수행하고 분석 결과를 제시할 수 있다.

학습내용

1. 인터넷 제어 메시지 프로토콜(ICMP)
2. 인터넷 그룹 메시지 프로토콜(IGMP)
3. IP, ARP 덤프 분석

사전학습

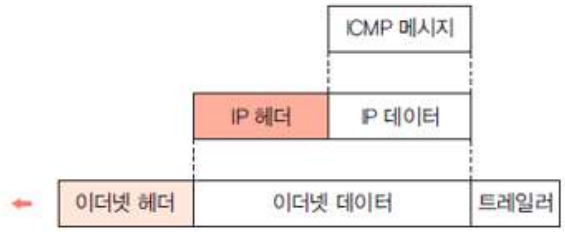
네트워크의 호스트나 라우터에서는 예상치 못한 상황이나 오류가 발생할 수도 있는데, 이러한 상황에서 가장 우선적으로 처리해야 하는 일은 무엇이라고 생각하나요?

본 학습

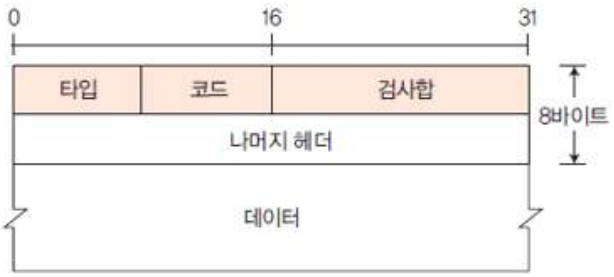
1. 인터넷 제어 메시지 프로토콜(ICMP)

1) 개요

- 네트워크의 호스트나 라우터에서는 예상치 못한 상황이나 오류가 발생할 수도 있음
- 인터넷 제어 메시지 프로토콜 ICMP은 라우터에서 발생한 오류를 송신 측으로 전송하는 데 사용하는 프로토콜
- ICMP는 네트워크 계층에서 상주하지 않고 IP 데이터그램에 캡슐화되어 인터넷으로 전송
- ICMP는 수신지 호스트나 라우터가 도달 가능한지 결정
- 시간을 초과한 IP 데이터그램이나 헤더의 부적합한 정보가 있는 데이터그램 등 잘못된 IP 데이터그램을 수신하고 있다는 것을 통지하여 메시지를 상호 교환



- ICMP의 처음 4바이트는 모든 메시지가 동일한 형식이고 나머지 부분은 메시지에 따라 달라짐
  - 타입: ICMP 메시지의 15개 종류 중 무엇인지 명시
  - 코드: 메시지의 종류를 타입보다 좀 더 세분화하는 추가적인 코드
  - 검사합: 메시지의 오류를 검사
  - 나머지 헤더: 타입과 코드 값에 따라 변경



2) ICMP 질의 메시지

- ICMP는 질의하거나 응답하여 정보를 구하는 데 사용할 수 있는데 이러한 유형을 질의 메시지라고 함
- ICMP 질의 메시지의 일반적인 유형

- 에코 요청 및 응답
  - 현재 ping 프로토콜을 구현하는 데 사용하는 메시지
  - 에코 요청 메시지는 어떤 컴퓨터의 ICMP 소프트웨어로도 전송할 수 있음
  - 이후 ICMP 소프트웨어는 에코 요청 메시지에 대해 에코 응답 메시지를 전송할 것을 요청받음

- 타임 스탬프 요청 및 응답
  - 호스트나 라우터에서 현재 날짜와 시간을 지시하는 메시지
  - 여러 가지 상황에서 경과 시간을 측정하는 도구로 사용
  - 두 시스템 간에 IP 데이터그램이 오고 가는 데 필요한 왕복 시간(round trip time)을 결정
- 주소 마스크 요청 및 응답
  - 호스트의 서브넷 마스크를 알아보는 데 사용
- 라우터 요청 및 응답
  - 다른 네트워크의 호스트에 데이터를 전송할 때 자신의 네트워크에 연결된 라우터의 주소를 요청하기 위해 사용

3) ICMP 오류 메시지

- 가장 일반적인 ICMP 메시지
- 전송을 시도할 때나 IP 데이터그램을 전송하는 도중에 발생하는 다양한 형태의 오류 상태를 통보
- ICMP 오류 메시지의 일반적인 발생 유형

- 목적지 도달 불가능
  - 데이터그램을 최종 목적지로 전달할 수 없을 때 라우터는 데이터그램을 생성한 호스트에 목적지 도달 불가능 메시지를 전송
  - 이 메시지에는 지정 목적지 호스트에 도착할 수 없는 이유 또는 목적지가 부착된 네트워크에 도착할 수 없는 이유를 명시
  - 목적지 도달 불가능 메시지는 라우터가 원격 시스템으로 가는 경로를 찾지 못할 때, 목적지 시스템의 특정 포트 번호가 현재 응답할 수 없을 때, 기타 여러 가지 문제가 발생했을 때 생성

① Network Unreachable(네트워크에 도달할 수 없음)
- 오류를 보고하는 라우터의 라우팅 테이블에서 수신지 네트워크의 경로를 찾지 못할 때 이 오류 메시지가 생성
- 사용자를 인터넷에서 라우팅할 수 없는 사설 주소에 연결할 때, 손상되거나 오래된 라우팅 테이블이 있는 라우터에 데이터그램을 전송할 때 발생

② Host Unreachable(호스트에 도달할 수 없음)
- IP 데이터그램을 최종 수신지 시스템에 전송하지 않았음을 나타냄
- 최종 단계의 라우터가 수신지 시스템에 이르는 방법을 찾지 못할 때 이 오류 메시지가 생성

③ Protocol Unreachable(프로토콜에 도달할 수 없음)
- 수신지 시스템에서 특정 전송 프로토콜을 사용할 수 없음을 나타냄
- 사용자가 비표준 전송 프로토콜을 사용하여 프로그램을 지원하지 않는 다른 호스트와 통신할 때 이 오류 메시지가 생성

④ Port Unreachable(포트에 도달할 수 없음)
- 수신지 시스템에서 특정 수신지 포트 번호를 사용하지 않았음을 나타냄
- 대부분 UDP 때문에 이 오류 메시지가 생성
- TCP는 원격 시스템과 연결하는 데 3-way 핸드셰이킹을 사용하므로, 수신지 시스템에 해당 포트를 사용하는 응용 프로그램이 없으면 수신지 시스템의 TCP 스택은 TCP 리셋 플래그를

사용하여 연결 요청을 거부

⑤ Source Route Failed(송신지 라우팅을 수행할 수 없음)

- 다음 단계의 라우터가 유효 하지 않거나 라우터가 다음 단계의 라우터에 데이터그램을 전송하지 못할 때 이 오류메시지가 생성

● 송신지 억제

▪ 송신지 시스템이 너무 많은 데이터를 전송하면 수신지 시스템은 송신지 시스템에 ICMP 송신지 억제(Source Quench) 오류 메시지를 보내 전송 속도를 줄일 것을 요구

▪ 이때 송신지 시스템이 전송 속도를 늦추지 않으면 혼잡으로 일부 패킷을 분실할 가능성이 큼

▪ 송신지 억제 메시지는 서버에 혼잡이 발생했다고 송신지 시스템에 알리고 전송 속도를 늦출 것을 요구

▪ 이러한 메시지는 집중적인 트래픽 흐름을 제어하는 데 효과적임

● 재지정

▪ 라우터가 다른 네트워크로 가는 패킷을 송신해야 할 때는 적절한 다음 라우터의 주소를 알아야 함

▪ 송신 측 노드에 적합하지 않은 경로를 설정했다고 판단하면 노드를 재지정하는 오류 메시지를 전송

▪ 이 오류 메시지에는 지정 호스트 변경이나 네트워크 변경을 명시

● 시간 초과

▪ 라우터가 데이터그램에 있는 라이프 타임 필드를 0으로 감소시킬 때마다 라우터는 데이터그램을 소멸시키고 시간 초과 메시지를 보냄

▪ 또한 주어진 데이터그램에서 모든 단편이 도착하기 전에 재조립 타이머가 끝나면 호스트는 시간 초과 메시지를 보냄

① Time-to-live Exceeded in Transit

- IP 데이터그램을 최종 수신지에 전송하기도 전에 데이터그램의 활성화 시간 값이 0에 도달했을 때 이 오류 메시지를 사용
- 라이프 타임 필드는 데이터그램이 거칠 수 있는 최대 단계의 수를 나타내므로 라우터는 활성화 시간 값이 0인 데이터그램을 전송하지 못함
- 이때는 데이터그램을 소멸시켜야 하며, 송신자에게 삭제했음을 알림

② Fragment Reassembly Time Exceeded

- 수신지 시스템이 주어진 시간(유닉스에서는 대부분 60초로 설정) 내에 모든 단편을 수신하지 못했을 때 이 오류 메시지를 사용
- 일반적으로 이 오류 메시지는 전송 과정에서 어떤 단편을 분실했으며, 모든 단편이 지정된 시간 내에 도착하지 않았음을 알림

● 매개변수 문제

▪ 라우터나 호스트는 데이터그램의 IP 헤더 매개변수에서 문제를 발견하면 데이터그램을 폐기

4) ICMP 오류 메시지를 생성하지 않을 때

● ICMP 오류 메시지를 전송하는 데이터그램에서는 오류 메시지를 생성하지 않음

● 멀티캐스트 주소가 있는 데이터그램에서는 오류 메시지를 생성하지 않음

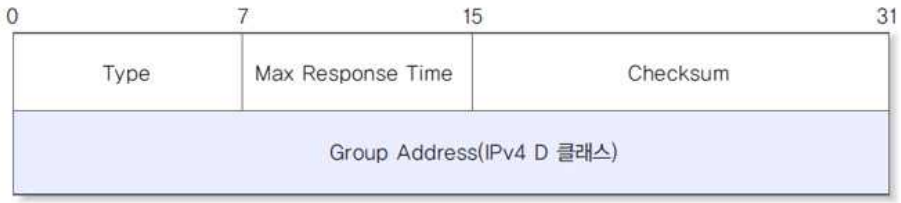
● 127.0.0.0이나 0.0.0.0 등 특수한 주소가 있는 데이터그램에서는 오류 메시지를 생성하지 않음

2. 인터넷 그룹 메시지 프로토콜(IGMP)

1) 개요

- IGMP(Internet Group Management Protocol): 인터넷에 연결한 컴퓨터가 멀티캐스트 그룹을 주위의 라우터에 알릴 수 있는 수단을 제공하는 프로토콜
- 하나의 라우터와 여러 호스트 컴퓨터로 구성된 서브 네트워크에서 라우터와 호스트 컴퓨터가 어떤 멀티캐스트 그룹에 속하는지 알려줌
- IGMP는 IP 패킷에 캡슐화되어 보내짐
- 멀티캐스팅은 네트워크의 한 호스트 컴퓨터가 미리 지정된 다수의 컴퓨터에 메시지를 보낼 수 있도록 허용
  - 멀티캐스팅 : 특정 그룹의 모든 호스트에 메시지를 전송하는 방식
  - 멀티캐스트 라우팅 : 멀티캐스팅에 필요한 라우팅 알고리즘멀티캐스트 그룹에 가입하거나 탈퇴할 때 사용하는 프로토콜
- 멀티캐스트 그룹에 가입한 호스트와 라우터 사이에 멤버 정보를 교환하는 용도
- 질의 메시지 : 멀티캐스트 라우터가 그룹 정보를 얻기 위하여 호스트에 전달
- 보고 메시지 : 질의의 응답으로 호스트가 보고 메시지를 회신
- 그룹 관리
  - 그룹 관리의 주요 기능 : 그룹의 생성·제거, 전송 호스트의 그룹 참가·탈퇴 등
  - 멀티캐스팅 기능
    - 다중 호스트를 표시하는 멀티캐스트 그룹 주소 표기 방법의 통일
    - 라우터가 멀티캐스트 주소와 이 그룹에 속하는 호스트 사이의 연관성 처리
    - 멀티캐스트 라우팅 알고리즘은 그룹의 모든 멤버에게 가장 짧은 경로를 선택하는 기능 제공

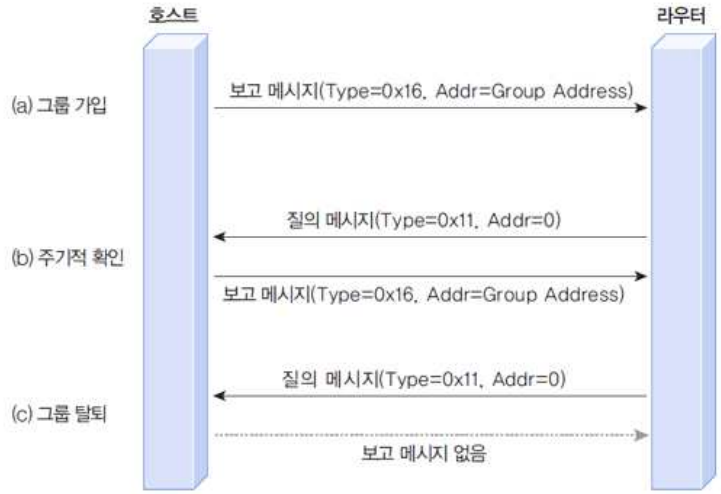
2) IGMP 헤더 구조



- Type(유형)
  - 0x11 : 멀티캐스트 라우터가 전송한 질의 메시지
  - 0x16 : 호스트가 전송하는 보고 메시지
  - 0x17 : 그룹 탈퇴에 관한 메시지
- Max Response Time(최대 응답 시간) : 질의에 대한 보고 메시지가 전송되는 최대 응답시간
- Checksum(체크섬) : IP 프로토콜에서 사용하는 알고리즘과 동일한 방식 (오류 검출용으로 이용)
- Group Address(그룹 주소)
  - 질의 메시지는 0
  - 보고 메시지에는 호스트가 가입을 원하는 그룹 주소 표기

3) IGMP 동작 과정

- 그룹 가입 : 해당 멀티캐스트 주소를 표기한 IGMP 보고 메시지를 전송
- 그룹 유지 : IGMP 보고 메시지를 사용해 IGMP 질의에 응답해야함
- 그룹 탈퇴 : 라우터의 질의 메시지에 대해 호스트의 보고 메시지 응답이 없음



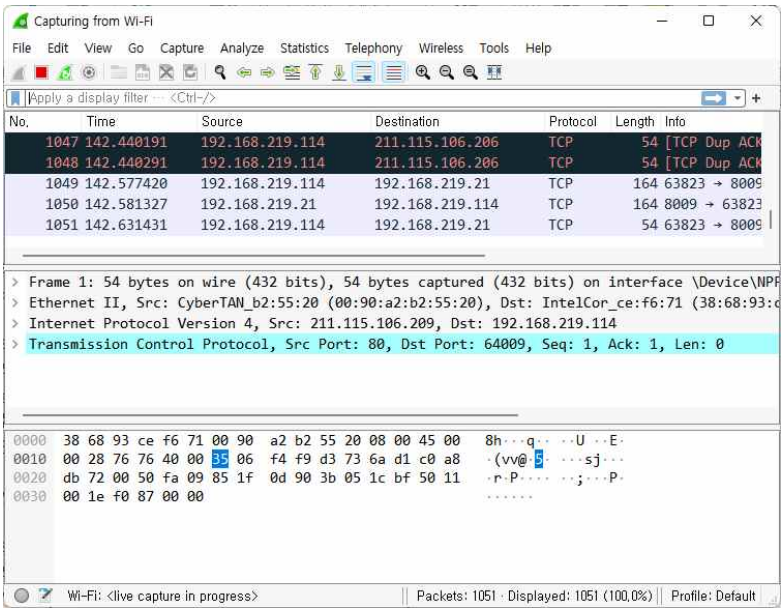
3. IP, ARP 덤프 분석

1) 네트워크 분석 도구 설치

① 와이어샤크 홈페이지(https://www.wireshark.org/)에 접속
② <Download>를 클릭한 후 ' Windows Installer(64-bit)'를 선택, 만약 32비트 윈도우 운영체제를 사용하고 있다면 ' Windows Installer(32-bit)'를 선택
③ 와이어 샤크 설치 화면에서 <NEXT>를 클릭
④ 라이선스 동의 화면에서 <I Agree>를 클릭
⑤ 설치할 컴포넌트를 선택한 후 <Next>를 클릭, 기본적으로 선택된 컴포넌트대로 진행
⑥ 추가할 태스크가 있으면 선택하고 <Next>를 클릭
⑦ 인스톨할 경로 선택, 'Destination Folder'에 설치할 위치 경로를 입력하거나 <Browse...>를 클릭하여 설치 위치를 선택
⑧ WinPcap을 설치할지 여부를 확인하는 화면이 나타나며 ' Install WinPcap 4.1.3'에 체크한 뒤 <Next>를 클릭하면 와이어샤크 설치가 진행
⑨ 와이어샤크를 설치하는 도중에 WinPcap 설치 화면이 나오면 <Next>를 클릭
⑩ 라이선스 동의 화면이 나타나면 <I Agree>를 클릭
⑪ WinPcap 설치 옵션을 설정, 컴퓨터가 부팅될 때 WinPcap도 자동으로 시작하도록 기본적으로 체크가 되어 있으며 <Install>을 클릭하면 WinPcap 설치가 시작
⑫ WinPcap 설치가 끝나면 <Finish>를 클릭
⑬ WinPcap 설치가 끝나면 와이어샤크 설치 진행 화면으로 돌아가며. 와이어샤크 설치가 완료되면 <Completed>가 표시되고, <Next>를 클릭하면 와이어샤크 설치 완료 화면이 나타남
⑭ 와이어샤크 설치 완료 화면이 나타나면 <Finish>를 클릭

2) 와이어샤크 실행

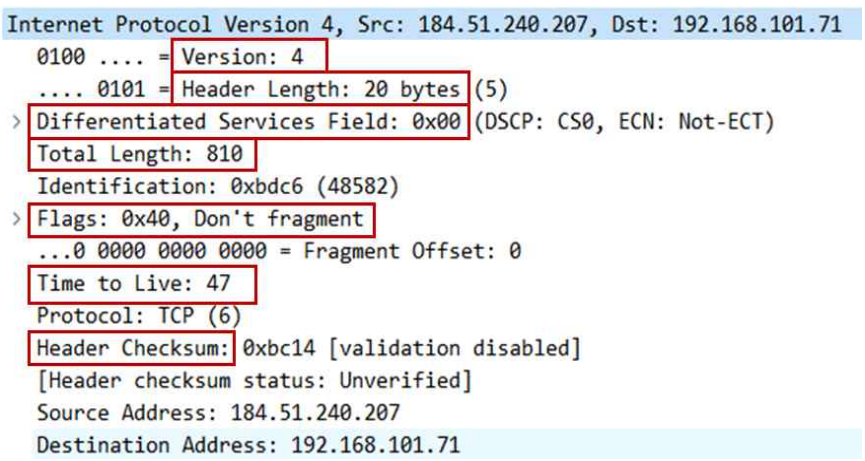
① 와이어샤크가 설치되면 [시작] 메뉴에서 와이어샤크 실행
② 와이어샤크가 실행되면 와이어샤크에서 인식된 LAN 카드가 목록에 나타나며, 그중에서 캡처하려는 이더넷(네트워크 인터페이스)을 클릭하면 패킷 캡처가 시작



- 와이어샤크로 패킷을 분석할 때 패킷의 헤더 구성을 살펴보는 것이 좋음
- 각 헤더에 등장하는 주소의 경우 Ethernet II 헤더에는 MAC 주소, IP 헤더에는 IP 주소, TCP 헤더에는 포트 번호, HTTP 헤더에는 URI가 사용
- 프로토콜은 각 헤더에서 어떤 필드 값을 표시할지, 어떤 것을 주소로 사용할지에 대한 일정한 규칙이며, Ethernet II, IP, TCP, HTTP가 겹겹이 쌓여 있어 이를 프로토콜 스택이라고도 함
- 각각의 프로토콜은 주소를 가지고 있고 층별로 기능이 나뉘어 있음
- 층을 나눔으로써 주소가 복잡해지지 않고 층별로 하드웨어나 소프트웨어를 준비할 수 있음
- 덤프 분석 시 주의 사항
  - 윈도우는 웹 브라우저를 열고 웹 페이지를 검색하지 않더라도 제어용 패킷으로 시작해서 네트워크 통신을 수행하기 때문에 많은 패킷이 섞여 있음
  - 패킷이 다수 캡처되더라도 필터 툴바의 텍스트 박스에 'tcp or http or arp' 등을 입력하고 클릭하면 해당 패킷만 확인할 수 있음

3) IP 덤프 분석

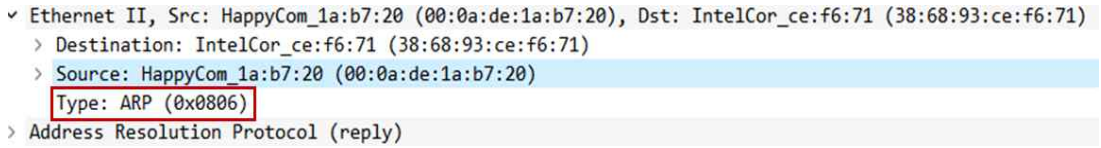
- Internet Protocol의 헤더 부분을 확인
  - 패킷 리스트 영역에 있는 프레임을 선택한 후 패킷 상세 영역에서 Internet Protocol의 › 기호를 클릭



- IP 헤더의 처음에 있는 Version 필드는 4비트이고 Version: 4는 패킷이 IPv4임을 나타냄
- Header Length는 20바이트
- Differentiated Services Field에는 1바이트 값이 표시되며 패킷의 대역을 제어하는 QoS에 사용
- Total Length 필드에는 IP 패킷의 전체 크기가 2바이트로 표시
- Flags 필드
  - 큰 IP 패킷을 한 번에 보낼 수 없을 때 여러 개의 IP 패킷으로 분할하거나 재결합하는 단편화와 재조립에 사용됨
  - Don't fragment 비트가 1(ON)이 되면 단편화가 금지되고 단편화가 발생하면 패킷이 파기
- Time to live(TTL)
  - IP 패킷의 수명을 나타내는 1바이트 필드
  - 송신 측에서 처음 설정되고 라우터 등의 중계 장치를 통과할 때마다 1씩 감소하고 통신 도중에 TTL 값이 0이 되면 해당 패킷이 폐기
- Protocol 필드
  - IP 다음 레이어의 헤더를 1바이트로 나타냄
  - Protocol 필드의 대표적인 값[프로토콜(프로토콜 번호)]은 ICMP(1), TCP(6), UDP(17) 등임
- Header checksum은 IP 헤더의 내용을 확인하기 위한 필드로, 헤더에 오류가 없는지 검사하는 데 사용

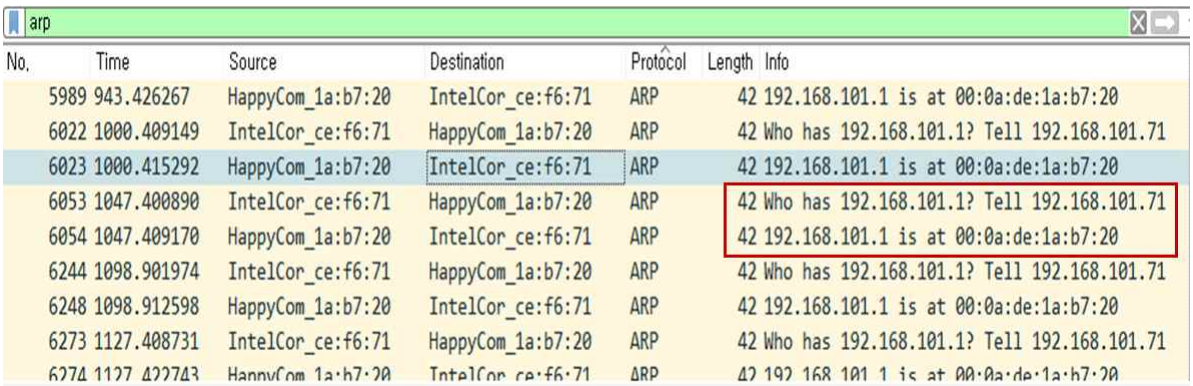
4) ARP 덤프 분석

- Ethernet II 헤더 뒤에 ARP 헤더가 캡슐화되어 송신되는 ARP 패킷은 Ethernet II 프레임의 최소 크기인 64바이트
- ARP 패킷을 송신할 때 Ethernet II 헤더의 타입에는 0x0806이 사용



- ARP 시퀀스
  - Info 열에 Who has...로 표시된 패킷이 ARP 요청 프레임
  - ...is at...으로 표시된 프레임이 ARP 응답 프레임

⇒ 이 두 패킷을 ARP 시퀀스라고 함



학습정리

1. 인터넷 제어 메시지 프로토콜(ICMP) : 인터넷 제어 메시지 프로토콜 ICMP은 라우터에서 발생한 오류를 송신 측으로 전송하는 데 사용하는 프로토콜
2. ICMP 질의 메시지 : ICMP는 질의하거나 응답하여 정보를 구하는 데 사용하는 메시지
3. ICMP 오류 메시지 : 목적지 도달 불가능, 송신지 억제, 재지정, 시간 초과, 매개변수 문제
4. 인터넷 그룹 메시지 프로토콜(IGMP) : 인터넷에 연결한 컴퓨터가 멀티캐스트 그룹을 주위의 라우터에 알릴 수 있는 수단을 제공하는 프로토콜
5. 멀티캐스팅 : 특정 그룹의 모든 호스트에 메시지를 전송하는 방식
6. 멀티캐스트 라우팅 : 멀티캐스팅에 필요한 라우팅 알고리즘멀티캐스트 그룹에 가입하거나 탈퇴할 때 사용하는 프로토콜

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제10주차 1교시

강의주제 TCP 프로토콜

학습목표

1. 전송계층의 기능을 설명할 수 있다.
2. TCP 프로토콜을 설명할 수 있다.
3. TCP 프로토콜을 이용한 데이터 전송 방식을 설명할 수 있다.

학습내용

1. 전송계층의 기능
2. TCP 프로토콜
3. TCP 프로토콜을 이용한 데이터 전송

사전학습

통신 네트워크 구성에서 전송계층이 필요한 이유는 무엇이라고 생각하나요?

본 학습

1. 전송계층의 기능

1) 개요

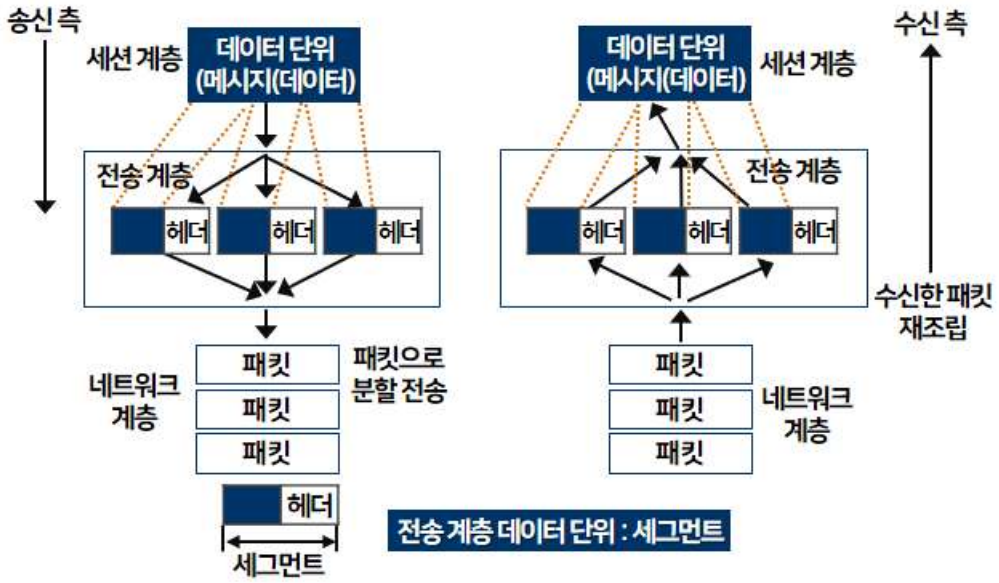
- 전송 계층
  - 수신지에 신뢰할 수 있는 데이터를 전송하기 위해 필요한 계층
  - 오류를 점검하는 기능이 있기 때문에 데이터에 오류가 발생하면 재전송을 요청할 수 있음
- 네트워크 계층에서는 수신지까지 데이터를 전송하고, 전송 계층에서는 데이터가 제대로 도착했는지 확인
- 전송 계층은 전송된 데이터의 수신지가 어떤 애플리케이션인지 식별하는 기능이 있음
  - 수신지에 데이터가 도착했을 때 그 데이터가 어떤 응용 프로그램에서 사용하는 것인지 판단해야 함
  - 전송 계층은 웹 페이지에서 사용하는 데이터가 도착하면 어떤 애플리케이션(예: 크롬, 아웃룩)에 전송해야 하는지 알려줌

2) 전송계층의 특징

- 프로토콜(TCP, UDP)과 관련된 계층으로 오류 복구와 흐름 제어 등을 담당하며, 두 시스템 간에 신뢰성 있는 데이터를 전송
- 네트워크 계층에서 온 데이터를 세션 계층의 어느 애플리케이션에 보낼 것인지 판독하고, 네트워크 계층으로 전송할 경로를 선택
- OSI 참조 모델 7계층 중 전송 계층은 네 번째 계층으로 시스템 종단 간에 투명한 데이터를 양방향으로 전송하는 계층
- 네트워크 계층에서 전송한 데이터와 실제 운영체제의 프로그램이 연결되는 통신 경로라고 할 수 있음

3) 전송계층의 데이터 단위

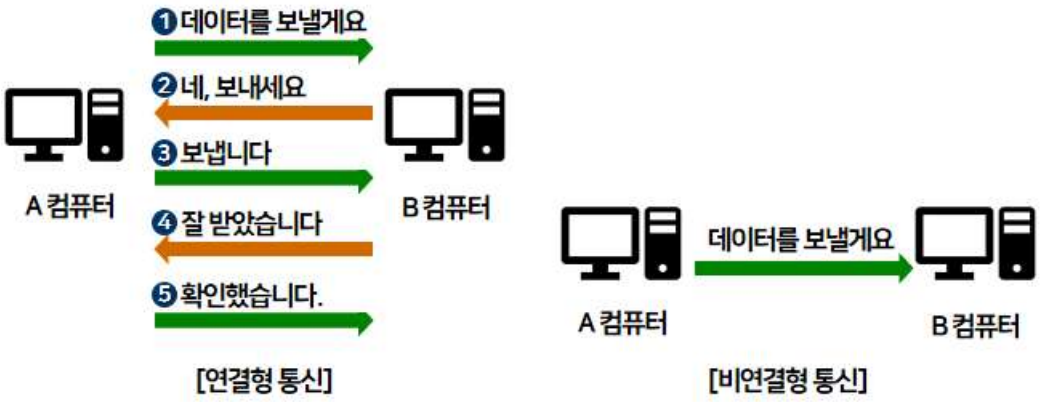
- 전송 계층, 네트워크 계층, 세션 계층의 관계



- 전송 계층의 데이터 헤더에는 포트 주소, 소켓 주소, 순서 번호 등이 포함
- 전송 계층은 세션 계층에서 온 데이터를 수신할 때 데이터를 전송할 수 있는 세그먼트로 나누고, 수신 측에서 재조립할 수 있도록 헤더에 순서를 표시
- 네트워크 계층은 전송해야 하는 시스템에 각 패킷을 전송하는 역할을 하고, 전송 계층은 해당 시스템의 응용 프로그램에 모든 데이터를 전송하는 역할을 수행
- 전송 계층의 기능
  - 연결 제어: 패킷을 하나의 경로로 보낼 것인지 결정
  - 수신지로 데이터 전송: 수신지에서 데이터의 모든 패킷 전송과 도착을 검사
  - 단편화: 데이터를 전송 가능한 단편(세그먼트)으로 나누고 순서 번호를 기록
  - 재조립: 수신지의 전송 계층에서 순서 번호에 따라 데이터를 올바르게 재조립
- TCP를 사용하는 전송 계층의 예
  - 송신 측에서 데이터(01001100)를 보내면 TCP의 포트 번호 80번을 이용하여 수신 측으로 데이터를 안전하게 전송

4) 전송 계층의 통신 방식

- 연결형(TCP) 통신
  - 신뢰할 수 있고 데이터를 정확하게 전송하는 통신
  - 신뢰성이 우선이므로 데이터를 전송할 때 여러 번 확인하고 전송
- 비연결형(UDP) 통신
  - 효율적으로 데이터를 전송하는 통신
  - 효율성이 우선이므로 확인 절차 없이 일방적으로 데이터를 전송



2. TCP 프로토콜

1) 개요

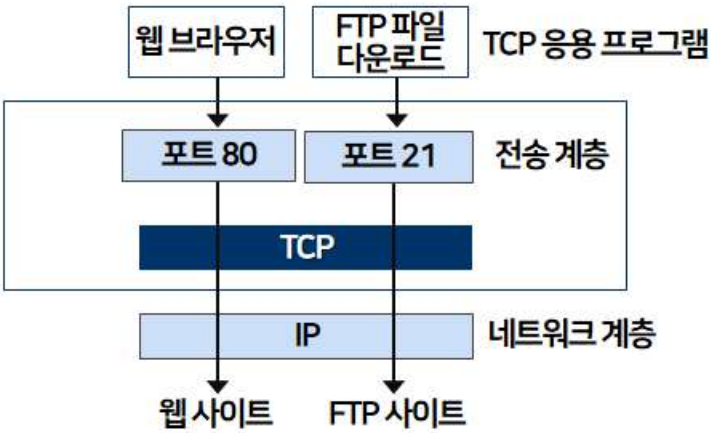
- 연결 지향형 프로토콜인 TCP는 신뢰성 있는 바이트 스트림 서비스를 제공
  - 연결 지향이란 응용 프로그램이 데이터를 교환하기 전에 서로 TCP 연결을 확립해야 함을 의미함
  - 신뢰성이 있다는 말은 데이터를 성공적으로 수신했거나 오류가 발생했음을 알려주는 것을 의미
- 신뢰성 있게 순차적으로 데이터를 전송하는 서비스를 '연결형 서비스'라고 함
- 연결형 서비스는 송신 측 전송 계층 프로세스와 수신 측 전송 계층 프로세스 간에 연결이라는 논리적 관계를 설정하는 것임
- 전송 계층 프로토콜은 신뢰성 있고 순차적인 데이터 전송 서비스를 지원하는 데 필요한 제어 기능을 수행

2) TCP 연결형 데이터 서비스

- 데이터 전송 서비스는 두 통신 프로세스 간에 양방향으로 동시에 데이터를 전송할 수 있는 전이중 방식 서비스를 말함
- 전이중 방식은 동시에 데이터를 송수신하는 것으로, 전화를 대표적인 예로 꼽을 수 있음
- 연결 지향형 프로토콜은 송신 측 컴퓨터와 수신 측 컴퓨터가 데이터를 전송하기 전에 먼저 데이터를 송수신할 수 있는 연결 통로를 만들고 데이터를 전송하는 프로토콜
- 연결 지향형 프로토콜은 신뢰성 있는 데이터 전송을 보장하며, 오류가 발생하면 수신자에게 알려줌
- TCP는 대표적인 연결 지향형 프로토콜

3) 포트 번호

- 포트는 TCP가 상위 계층으로 데이터를 전송하거나 상위 계층에서 TCP로 데이터를 전송할 때 상호 간에 사용하는 데이터의 이동 통로를 말함
- 상위 계층 프로토콜과 하위 계층 프로토콜이 같은 포트를 사용해야만 통신할 수 있음
- 통신할 때 여러 웹 사이트에서 동시에 파일을 다운로드할 수 있음
  - TCP 프로토콜이 포트를 여러 개 사용하여 상위 계층의 프로그램과 각각 따로 통신하기 때문에 동시에 파일을 다운로드할 수 있는 것임
- TCP 포트를 이용한 통신



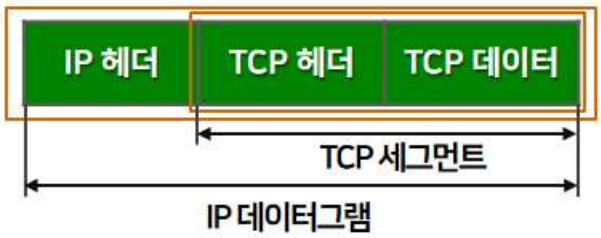
- 웹 브라우저로 서버에 접속하여 웹 페이지의 내용을 보는 과정
  - 웹 브라우저에서 접속하려는 서버의 IP 주소를 입력한 후 해당 서버에 액세스
  - 서버가 웹 서비스를 위해 열어놓은 포트(수신지 포트)를 이용하여 웹 서비스를 담당하는 상위 계층의 서버 프로그램에 웹 페이지의 내용을 요청
  - 웹 서비스를 하는 서버가 포트 80번을 웹 서비스용으로 사용하는 경우, 서버에 접속하려는 클라이언트도 포트 80번으로 접속해야 함
- 서버에 접속을 요청할 때 사용하는 포트 번호는 클라이언트의 포트 번호와 서버의 포트 번호임
- 서버가 클라이언트에 웹 페이지의 내용을 전송할 때 사용하는 포트 번호도 서버의 포트 번호와 클라이언트의 포트 번호임
- 신호를 보내는 입장에서 보낸 신호의 응답을 받을 포트 번호를 '소스 포트 번호'라 하고, 연결을 요청할 포트 번호를 '수신지 포트 번호'라 함
- 포트 번호는 0~65535번을 사용할 수 있음
- 주요 인터넷 서비스에 정해놓은 포트 번호를 '잘 알려진 포트 번호'라고 하며 0~1023번이 할당되어 있음

포트 번호	애플리케이션	포트 번호	애플리케이션
21	FTP	80	HTTP
25	SMTP	110	POP3
53	DNS	443	HTTPS

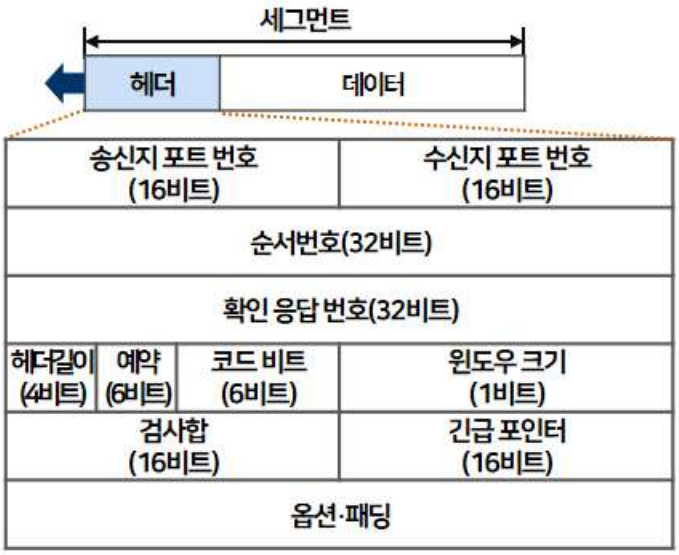
- 웹 서비스는 HTTP 프로토콜을 사용하므로 포트 번호는 80번
  - 우리가 웹 브라우저를 사용하여 웹 서버에 접속할 때 포트 번호를 입력하지 않아도 자동으로 80번이 할당
  - 웹 페이지의 포트 번호를 80번이 아닌 다른 번호로 할당하면 해당 포트 번호를 아는 사람만 웹 페이지에 접속할 수 있어 어느 정도 보안이 유지됨
- 어떤 애플리케이션이 사용되고 있는지 구분하려면 TCP는 포트 번호가 필요함

4) TCP 세그먼트

- TCP 프로토콜은 전송을 위해 바이트 스트림을 세그먼트 단위로 나눔
- 세그먼트 : TCP를 이용하여 두 장치 간에 전달하는 데이터의 단위
- 캡슐화된 TCP 세그먼트



- TCP 세그먼트 형식과 각 필드 구성



  - 송신지 포트 번호: 세그먼트를 전송하는 송신지 호스트에 있는 응용프로그램의 포트 번호
  - 수신지 포트 번호
    - 수신지 호스트에서 수행하는 프로세스가 사용하는 포트 번호
    - 클라이언트가 수신지 호스트를 요청하는 서버라면 대부분은 잘 알려진 포트 번호
  - 순서 번호
    - 세그먼트에 포함된 데이터의 첫 번째 바이트에 부여된 것

- 32비트의 부호 없는 번호이며 TCP는 신뢰성 있는 연결을 보장하기 위해 전송하는 바이트마다 번호를 부여하고, 순서 번호는 수신지 TCP에 세그먼트의 첫 번째 바이트가 순서 번호에 해당하는 바이트라는 것을 알려줌

▪ 확인 응답 번호
- 세그먼트를 수신하는 노드가 상대편 노드에서 수신하려는 바이트의 번호이며 이 번호는 성공적으로 수신한 마지막 바이트의 순서 번호+1임

▪ 헤더 길이 : TCP 헤더 길이를 4바이트 워드 값으로 나타내며, 헤더 길이는 20~60바이트

▪ 예약 : 나중에 사용하기 위해 예약된 필드

▪ 코드 비트
- 연결의 제어 정보가 기록되는 코드 비트는 비트별로 역할이 정해져 있음
- 초깃값이 0이고 비트가 활성화되면 1이 됨
- 데이터를 전송할 때 연결을 확립하려면 코드 비트 중 연결 요청을 하는 SYN과 확인 응답을 하는 ACK가 필요

코드 비트	설명
URG	긴급하게 처리할 데이터가 들어 있음
ACK	응답 확인 번호 사용
PSH	TCP가 받은 데이터를 상위 계층에 전달
RST	연결 재설정
SYN	연결을 초기화하려고 순서 번호 동기화
FIN	데이터 송신 종료

URG	ACK	PSH	RST	SYN	FIN
0	1	0	0	1	0
1비트	**1비트**	**1비트**	**1비트**	**1비트**	**1비트**

3. TCP 프로토콜을 이용한 데이터 전송

1) 개요

● 데이터를 전송하기 전에 연결을 확립하기 위해 패킷 요청을 세 번 교환하는 것을 3-way 핸드셰이킹이라고 함

● 핸드셰이킹은 우리가 상대방을 확인하고 악수를 하는 것처럼 네트워크 통신에서도 확실하게 데이터가 전송되었는지 확인하면서 이루어지는 통신 방식

● SYN과 ACK를 사용한 3-way 핸드셰이킹 과정

① 네트워크 통신을 하려면 수신 측 컴퓨터의 허락을 받아야 하므로 먼저 송신 측 컴퓨터는 수신 측 컴퓨터에 연결 확립 허가를 받기 위한 SYN 요청을 보냄

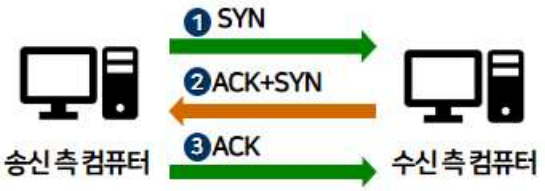
② 수신 측 컴퓨터는 송신 측 컴퓨터가 보낸 요청을 받은 후 허가한다는 응답을 회신하기 위해 연결 확립 응답인 ACK를 보냄

▪ 동시에 수신 측 컴퓨터는 송신 측 컴퓨터로부터 데이터 전송 허가를 받기 위해 연결 확립 요청인 SYN을 보냄

▪ 이때 연결을 확립하기 위해 코드 비트의 SYN과 ACK가 1로 활성화됨

③ 수신 측 컴퓨터의 요청을 받은 송신 측 컴퓨터는 수신 측 컴퓨터에 허가한다는 응답으로 연결 확립 응답인 ACK를 보냄

- 연결 확립 과정



1 연결 확립 요청 (1로 활성화)

URG	ACK	PSH	RST	SYN	FIN
0	0	0	0	1	0

2 연결 확립 응답 + 연결 확립 요청

URG	ACK	PSH	RST	SYN	FIN
0	1	0	0	1	0

3 연결 확립 응답

URG	ACK	PSH	RST	SYN	FIN
0	1	0	0	0	0

- 연결 종료 과정

① 송신 측 컴퓨터는 수신 측 컴퓨터로 연결 종료 요청(FIN)을 보냄

②, ③ 수신 측 컴퓨터는 송신 측 컴퓨터로 연결 종료 응답(ACK)을 반환하고 수신 측 컴퓨터는 송신 측 컴퓨터로 연결 종료 요청(FIN)을 보냄

④ 송신 측 컴퓨터는 수신 측 컴퓨터로 연결 종료 응답(ACK)을 반환

1 연결 종료 요청 (1로 활성화)

URG	ACK	PSH	RST	SYN	FIN
0	0	0	0	0	1

2 연결 종료 응답

URG	ACK	PSH	RST	SYN	FIN
0	1	0	0	0	0

3 연결 종료 요청

URG	ACK	PSH	RST	SYN	FIN
0	0	0	0	0	1

4 연결 종료 응답

URG	ACK	PSH	RST	SYN	FIN
0	1	0	0	0	0

2) TCP 전송 방식

- TCP는 데이터를 분할해서 전송하는데, 이때 데이터에 일련번호, 즉 순서 번호를 부여하면 수신 측은 몇 번째 데이터를 받았는지 알 수 있음
- 확인 응답 번호는 수신 측이 몇 번째 데이터를 수신했는지 송신 측에 알려주는 데 사용하며 다음 번호의 데이터를 요청할 때도 사용됨
  예) 50번 데이터를 수신하면 51번 데이터를 수신 측에 요청하는데 이를 확인 응답이라고 함
- 윈도우 크기 : 상대방이 유지해야 하는 바이트 단위의 윈도우 크기를 정의하며 필드의 길이가 16비트이므로 윈도우의 최대 크기는 65,535바이트
- 검사합(Checksum) : 의사 헤드를 포함한 헤드 부분의 오류를 검출하는 검사합 계산이 포함

- 검사합 수행 과정(송신측)
  ① 데이터 단위를 각각 n(보통 16)비트인 섹션 m개로 나눔
  ② 모든 섹션은 합을 만들기 위해 1의 보수를 사용하여 서로 더함
  ③ 합이 보수화되어 검사합이 됨
  ④ 검사합의 값을 데이터와 함께 보냄
- 검사합 수행 과정(수신측)
  ① 데이터 단위를 각각 n비트인 섹션 m개로 나눔
  ② 모든 섹션은 합을 만들기 위해 1의 보수를 사용하여 서로 더함
  ③ 합이 보수화됨
  ④ 결과가 0이면 오류가 없는 것이고, 그렇지 않으면 오류가 발생한 것임
- 검사합 수행 예제
  - 16비트 블록을 8비트 검사합을 사용하여 전송

```
          10101001
          00111001
-------------------
합: 11100010
검사합: 00011101
```

전송 데이터: 10101001 00111001 00011101
수신 데이터: 10101001 00111001 00011101

  - 섹션 3개를 모두 더한 후 1의 보수가 0인지 확인

```
          10101001
          00111001
          00011101
-------------------
결과: 1  11111111
1의 보수: 0000000
```

3) TCP 연결 관리

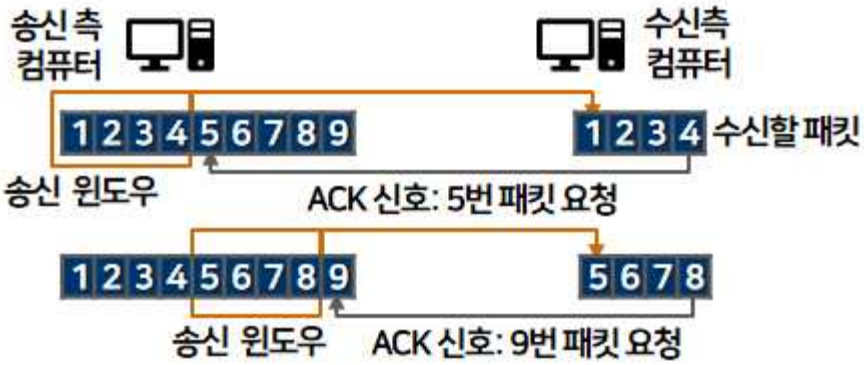
- 네트워크 통신의 흐름 예시
  - 포트 번호만 사용하여 응용 프로그램을 식별하는 UDP와 달리 TCP는 연결을 사용하여 응용 프로그램을 식별

  - 데이터를 전송하기 전 단계에서 3-way 핸드셰이킹으로 연결 수립이 이루어질 때 해당 통신에 사용하는 순서 번호인 5001번과 확인 응답 번호인 6001번이 결정
  - 순서 번호 5001번은 지금 전송하는 300바이트 데이터의 첫 번째 바이트 번호이고, 확인 응답 번호는 다음에 전송하길 바라는 데이터의 첫 번째 바이트 번호
    ① 송신 측 컴퓨터는 수신 측 컴퓨터로 300바이트의 데이터를 전송
    ② 수신 측 컴퓨터는 300바이트를 수신하고 다음에 수신하고자 하는 데이터의 번호를 확인 응답 번호에 넣으며 다음에 수신하고자 하는 데이터는 5001 + 300 = 5301이므로 5301번부터 전송해달라고 요청
    ③ 송신 측 컴퓨터는 수신 측 컴퓨터로 5301번부터 300바이트의 데이터를 전송
    ④ 수신 측 컴퓨터는 300바이트를 수신하고 다음에 수신하고자 하는 데이터의 번호를 확인 응답 번호에 넣으며 다음에 수신하고자 하는 데이터는 5301 + 300 = 5601이므로 5601번부터 전송해달라고 요청
  - 데이터 전송이 완료될 때까지 ① ~ ④를 반복하며 전송된 데이터에 오류가 발생했을 때는 순서 번호와 확인 응답 번호를 사용하여 일정 시간 대기한 후 데이터를 재전송

4) TCP 흐름 제어

- 패킷을 전송할 때 네트워크 상황에 따라 패킷의 도착 순서가 바뀔 수도 있고 도중에 패킷이 사라질 수도 있으므로 TCP는 패킷 번호를 사용하여 신뢰성 있는 데이터를 전송함
- 패킷을 한 번에 하나씩 송수신하는 것보다 여러 패킷을 한 번에 송수신한 후 확인 응답 신호를 전송하는 것이 효율적
- 윈도우 크기
  - 확인 응답을 하나하나 하지 않고 연속해서 송수신할 수 있는 데이터 크기
  - 데이터를 전송할 때 한 번에 전송할 수 있는 전체 패킷의 크기를 'TCP 윈도우 크기'라고 하는데, 윈도우 크기가 크면 한 번에 여러 패킷을 전송할 수 있음
- 송수신 측 컴퓨터가 상대방의 윈도우 크기를 확인함으로써 오버플로가 발생하지 않게 데이터를 전송할 수 있음

- 슬라이딩 윈도우
  - 가정: 송신 측 컴퓨터에서 한 번에 전송할 송신 윈도우 크기가 패킷 4개 크기



- 송신 측 컴퓨터는 윈도우 크기에 따라 1~4번 패킷을 전송
- 수신 측 컴퓨터에서 수신 확인 ACK 신호를 수신하면 ACK 신호에서 요청한 5번 패킷 위치로 송신 윈도우를 옮김
- 다시 윈도우 안의 패킷을 전송하고, 수신 측 컴퓨터에서 ACK 신호를 수신하면 ACK 신호에서 요청한 9번 패킷 위치로 송신 윈도우를 옮김
- 이처럼 송신 버퍼 역할을 위해 송신 윈도우를 이동하는 방식을 '슬라이딩 윈도우라고 함

학습정리

1. 전송계층 : 프로토콜(TCP, UDP)과 관련된 계층으로 오류 복구와 흐름 제어 등을 담당하며, 두 시스템 간에 신뢰성 있는 데이터를 전송
2. 전송 계층의 데이터 헤더 : 포트 주소, 소켓 주소, 순서 번호
3. TCP 프로토콜 : 연결 지향형 프로토콜인 TCP는 신뢰성 있는 바이트 스트림 서비스를 제공
4. 포트 번호 : TCP가 상위 계층으로 데이터를 전송하거나 상위 계층에서 TCP로 데이터를 전송할 때 상호 간에 사용하는 데이터의 이동 통로
5. TCP 세그먼트 : TCP를 이용하여 두 장치 간에 전달하는 데이터의 단위
6. 핸드셰이킹 : 우리가 상대방을 확인하고 악수를 하는 것처럼 네트워크 통신에서도 확실하게 데이터가 전송되었는지 확인하면서 이루어지는 통신 방식

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제10주차 2교시

강의주제 전송계층

학습목표

1. UDP 프로토콜을 설명할 수 있다.
2. RTP 프로토콜을 설명할 수 있다.
3. OSI TP 프로토콜을 설명할 수 있다.

학습내용

1. UDP 프로토콜
2. RTP 프로토콜
3. OSI TP 프로토콜

사전학습

인터넷과 같이 데이터 통신 속도가 중요한 곳에서 사용하는 통신 프로토콜은 어떠한 특징이 있다고 생각하나요?

본 학습

1. UDP 프로토콜

1) 개요

- UDP(User Datagram Protocol, 사용자 데이터그램 프로토콜) : 프로토콜 중 구조가 가장 간단
- UDP는 RFC 768 문서에 정의된 비연결 지향 프로토콜
- TCP(연결 지향 프로토콜)와 달리 패킷이나 흐름 제어, 단편화 및 전송 보장 등의 기능을 제공하지 않음
- UDP 통신은 요청 메시지와 응답 메시지만으로 구성되고 주로 적은 양의 데이터 전송에 사용
- UDP를 사용하는 대표적인 응용 계층 프로토콜은 DNS, DHCP, SNMP 등이 있음
- 헤더와 전송 데이터에 대한 체크섬 기능을 제공
- Best Effort 전달 방식을 지원
- 신뢰성이 떨어지지만 프로토콜을 처리하는 기능이 작아 TCP보다 데이터 처리가 빠르므로 데이터 전송 시간에 민감한 응용 환경에서는 UDP를 사용하는 것이 유리

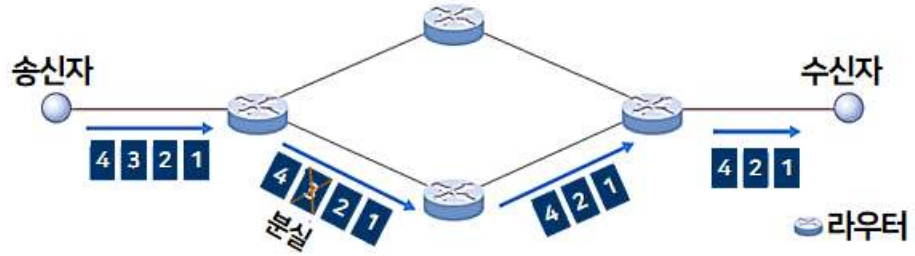
2) UDP 헤더 구조

- 프로토콜의 오버헤드가 작은 편임

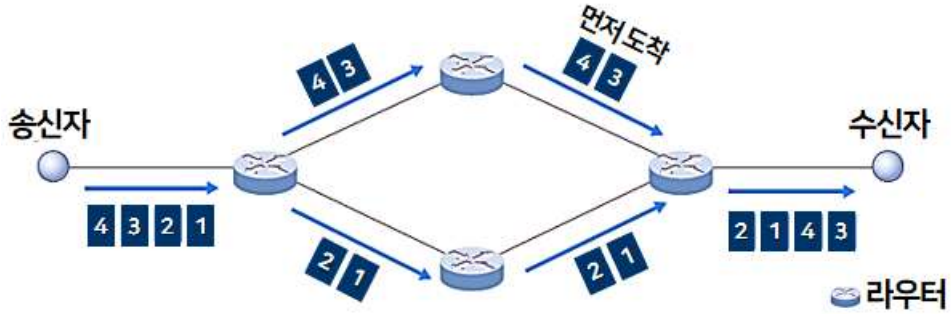
- 송신지 포트 번호
  - 데이터 영역의 데이터 정보를 만든 전송 시스템의 프로세스나 응용 프로그램
  - TCP 헤더의 송신지 포트와 같은 기능을 수행
- 수신지 포트 번호
  - 데이터 영역의 데이터 정보를 처리할 수신 시스템의 프로세스나 응용 프로그램
  - TCP 헤더의 수신지 포트와 같은 기능을 수행
- 전체 길이
  - UDP 헤더와 데이터의 길이를 바이트 단위로 표현한 것
  - UDP 메시지에 얼마나 많은 데이터 정보가 포함되었는지를 나타냄
- 검사합
  - 수신 측에서는 16비트인 검사합을 사용하여 UDP 헤더와 데이터 및 IP 헤더의 오류를 검사함
  - UDP 표준에서는 검사합이 선택 사항이며, 이 영역을 사용하지 않으면 UDP 패킷의 영역은 값이 0
- 데이터
  - 송신지 포트의 응응 계층 프로세스가 만든 데이터 정보로 크기가 가변적

3) UDP의 데이터그램 전송

- 비연결형 서비스를 이용하여 데이터그램을 전송
- 흐름 제어 기능이 없어 버퍼 오버플로에 의한 데이터 분실 오류가 발생할 수 있음
- 오류 유형
  - 데이터가 목적지에 도착하지 못하는 데이터그램 분실



  - 데이터그램의 도착 순서가 바뀌는 도착 순서 변경



  - UDP에서의 데이터그램 분실 : 데이터의 순서 번호 기능이 없음

4) 전송 계층 기타 프로토콜

(1) SPX

- NetWare의 연결 지향 프로토콜
- 패킷 접수 통지, 흐름 제어 등 TCP와 유사한 기능 제공
- NetWare 서버는 프린트 큐 사이에서 프린트 서버와 프린터 간의 통신에 SPX를 주로 사용하고 인터넷 통신에는 거의 사용하지 않음
- SPX 헤더구조

  - 연결 제어 : 8비트이며 제어 기능 메시지를 포함
  - 데이터 스트림 유형 : 8비트이며 데이터 영역의 정보 데이터 유형이나 연결 종료 과정에서 사용하는 코드 등을 포함
  - 송신지 연결 : 16비트이며 송신지 시스템이 현재의 연결을 구별하는 데 사용하는 수를 포함
  - 수신지 연결 : 16비트이며 수신지 시스템이 현재의 연결을 구별하는 데 사용하는 수를 포함

- 순서 번호 : 16비트이며 일련의 데이터 패킷 중에서 패킷의 위치를 지정
- 확인 일련번호 : 16비트이며 수신 시스템이 다음에 받을 패킷의 일련번호를 포함
- 위치 번호 : 16비트이며 수신 시스템이 사용할 수 있는 패킷 수신 버퍼의 크기를 나타냄
- 데이터 필드 : 응용 프로그램이나 상위 계층 프로토콜이 만든 데이터 정보로 크기가 가변적

(2) NCP

- NCP는 NetWare 클라이언트와 서버 간의 파일 공유 등 다양한 네트워크 기능을 담당
- NCP는 워낙 다양한 기능을 수행하기 때문에 NCP 프로토콜에 해당하는 OSI 계층을 하나로 규정하기는 어려움
- NCP 요청 메시지

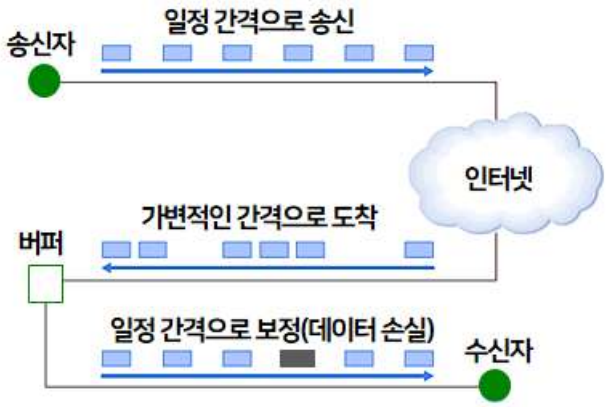
8비트	16비트
요청 유형	
일련 번호	연결 번호 로
직업 번호	연결 번호 하이
요청 코드	

- 요청 유형 필드 : 16비트이며 요청 메시지의 종류로 서비스 연결 생성과 파일 서버 요청
- 일련번호 필드 : 8비트이며 현재 메시지의 순서
- 연결 번호로 필드 : 8비트이며 NetWare 서버에 연결된 클라이언트의 수
- 작업 번호 필드 : 8비트의 유일한 값으로, 서비스를 요청하는 작업이 무엇인지 구분
- 연결 번호 하이 필드 : 8비트이며 현재 사용하지 않음

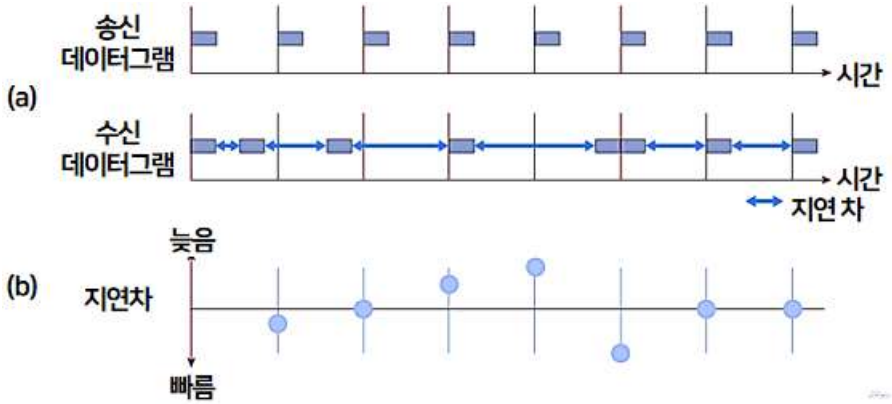
2. RTP 프로토콜

1) 개요

- RTP(Real Time Protocol) : 실시간 멀티미디어 데이터의 전송을 지원하며 유니캐스팅뿐 아니라 멀티캐스팅도 지원
- 불규칙한 데이터의 순서를 정렬하기 위해 타임스탬프 방식을 사용
- ALF(Application Level Framing) 방식으로 응용 환경이 요구하는 알고리즘에 따라 버퍼 크기를 개별적으로 조절 가능
- 실시간 요구 사항
  - 데이터 변형/분실 오류를 복구하는 기능이 상대적으로 덜 중요함
  - 도착 순서, 패킷의 지연 간격, 데이터 압축 등이 중요
- 버퍼의 역할
  - 네트워크에서 데이터의 시간 간격이 불규칙적으로 변함
  - 수신 프로세스의 버퍼를 이용하여 시간 간격이 일정하도록 보정



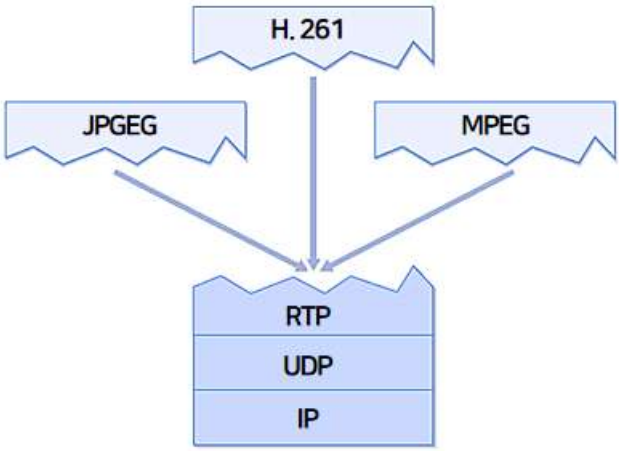
- 지터
  - 지터(Jitter) 분포 : 데이터그램의 도착 시간을 측정하였을 때 각 데이터그램의 도착 시간이 불규칙적으로 도착하는 정도를 나타냄



2) RTP의 데이터 전송

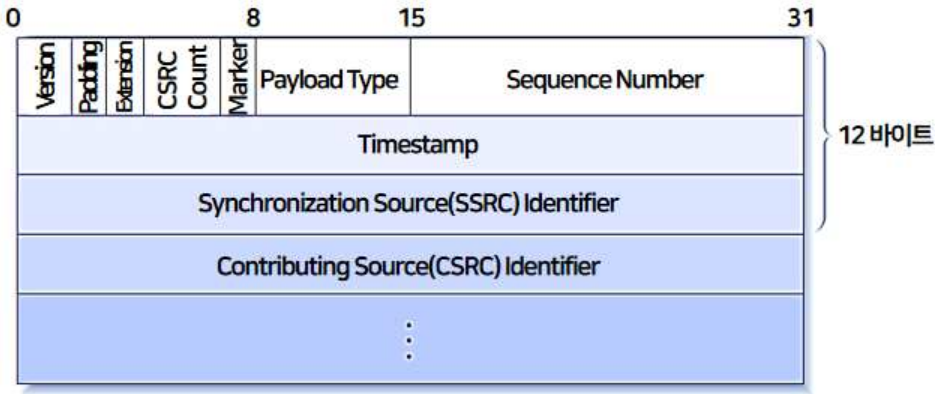
- 실시간 서비스를 위해 작고 빠른 전송 기능을 제공하는 UDP 위에서 구현
  - 데이터그램 분실이나 도착 순서 변경과 같은 전송 오류는 RTP 자체에서 해결
  - 송수신 프로세스 간의 연결을 관리
- 하나의 완전한 프로그램 단위로 구현되지 않고, 기능별로 개별로 구현
- 다수의 사용자가 하나의 세션에 참여, 서로 실시간 데이터 전송을 지원
- 두 종류의 RTP 릴레이(Relay)를 지원
  - 릴레이는 데이터 전송 과정에서 송수신 프로세스가 데이터를 직접 전송할 수 없는 상황이 발생했을 때, 데이터를 중개하는 기능
- 믹서(Mixer) : RTP 데이터그램 스트림을 받아 이들을 적절히 조합하여 새로운 데이터그램 스트림을 생성
- 트랜슬레이터(Translator) : 입력된 각 RTP 데이터그램을 하나 이상의 출력용 RTP 데이터그램으로 만들어주는 장치

- RTP 구조



3) RTP 헤더 구조

- 응용 환경과 관련된 가변 크기의 헤더를 추가할 수 있음
- CSRC 구분자 목록은 믹서에 의해 추가되는 경우에 사용
- 멀티캐스트 전송 가능
  - RTP 데이터 형식에 송신 구분자 필드 존재
  - Timestamp 필드 지원



- RTP 헤더에 정의된 각 필드의 의미
  - Version(버전) : RTP의 버전 번호
  - Padding(패딩) : RTP 페이로드의 마지막에 패딩 데이터가 존재하는지 여부
  - Extension(확장) : 고정 헤더의 마지막에 확장 헤더가 하나 더 이어짐을 의미
  - CSRC Count(CSRC 개수) : CSRC 구분자의 개수를 표시
  - Marker(표식) : 임의의 표식, 페이로드 유형에 따라 값의 의미가 결정됨
  - Payload Type(페이로드 유형) : 헤더 다음에 이어지는 RTP 페이로드의 유형
  - Sequence Number(순서 번호) : Timestamp 필드 값이 동일한 페이로드에 대해 패킷 손실이나 순서 변경과 같은 오류 검출
  - Timestamp(타임스탬프) : RTP 페이로드에 포함된 데이터의 생성 시기
  - SSRC Identifier(SSRC 구분자) : 임의의 세션 내에서 RTP 페이로드의 발신지가 어디인지를 구분하는 고유 번호
  - CSRC Identifier(CSRC 구분자) : SSRC 외에 추가된 스트림에 대한 식별자

- RTP 1890에서 권고한 표준 오디오/비디오 인코딩

페이로드	인코딩
0	PCMU audio
1	1016 audio
2	G.721 audio
3	GSM audio
4	audio
5	DV14 audio
6	DV14 audio
7	LPC audio
8	PCMA audio
9	G.722 audio

페이로드	인코딩
10	L16 audio
11	L16 audio
12~13	audio
14	MPA audio
15	G.728 audio
16~23	audio
24	video
25	CelB video
26	JPEG video
27	

페이로드	인코딩
28	nv video
31	H.261 video
32	MPV video
33	MP2T video
34~71	
72~76	Reserved
77~95	
96~127	Dynamic

4) RTP 제어 프로토콜

- QoS(Quality of Service)와 혼잡 제어 : 데이터 분배 과정에서 발생하는 서비스 품질에 관한 피드백 기능을 지원
- Identification(구분자) : RTCP 송신 프로세스에 관한 구분자 정보가 포함, 서로 다른 세션에서 발신된 스트림 정보들을 서로 연관시키는 근거를 제공
- 세션 크기 : 전체 세션 트래픽의 5% 이내로 유지되도록 알고리즘이 동작
- 패킷의 종류와 역할
  - Sender Report / Receiver Report : 데이터 전송 품질을 피드백하기 위한 용도로 사용
  - Source Description : 송신 프로세스가 자신에 대한 정보를 더 많이 제공하는 용도로 이용
  - Goodbye : 송신 프로세스가 더 이상 존재하지 않음을 의미하고, 이는 수신 프로세스가 송신 프로세스를 무한정 기다리지 않도록 함
  - Applicationdefined Packet : 응용 환경에 따른 기능을 점검하기 위해 제공

3. OSI TP 프로토콜

1) 개요

- OSI TP 프로토콜이 제공하는 서비스
  - 클래스 0이 구조가 가장 단순, 클래스 번호가 커질수록 기능이 추가

클래스	제공하는 서비스
클래스 0	기본 기능
클래스 1	기본 오류 복구 기능
클래스 2	멀티플레싱 기능
클래스 3	오류 복구, 멀티플렉싱 기능
클래스 4	오류 검출, 오류 복구, 멀티플렉싱 기능

- OSI TP의 서비스 프리미티브
  - 연결형 서비스 : 연결 설정(T-CONNECT), 연결 해제(T-DISCONNECT), 일반 데이터(T-DATA), 긴급 데이터(T-EXPEDITED-DATA)
  - 비연결형 서비스 : 데이터 전송을 위한 T–UNITDATA 프리미티브만 존재

프리미티브	제공 서비스
T-CONNECT.request	연결 설정
T-CONNECT.indication	연결 설정
T-CONNECT.response	연결 설정
T-CONNECT.confirm	연결 설정
T-DISCONNECT.request	연결 해제
T-DISCONNECT.indication	연결 해제

프리미티브	제공 서비스
T-DATA.request	데이터 전송
T-DATA.indication	데이터 전송
T-EXPEDITED-DATA.request	긴급 데이터 전송
T-EXPEDITED-DATA.indication	긴급 데이터 전송
T-UNITDATA.request	비연결형 데이터 전송
T-UNITDATA.indication	비연결형 데이터 전송

2) OSI TP의 데이터 전송

- T-DISCONNECT(연결 해제)
  - 어느 한쪽이라도 연결 해제를 원하면 해제
  - 네트워크 내부에 특별한 상황이 발생시 해제

학습정리

1. UDP 프로토콜 : 프로토콜 중 구조가 가장 간단하며 RFC 768 문서에 정의된 비연결 지향 프로토콜
2. UDP 헤더 구조 : 송신지 포트 번호, 수신지 포트 번호, 전체 길이, 검사합, 데이터
3. SPX : NetWare의 연결 지향 프로토콜이며 패킷 접수 통지, 흐름 제어 등 TCP와 유사한 기능 제공
4. NCP : NetWare 클라이언트와 서버 간의 파일 공유 등 다양한 네트워크 기능을 담당
5. RTP 프로토콜 : 실시간 멀티미디어 데이터의 전송을 지원하며 유니캐스팅뿐 아니라 멀티캐스팅도 지원
6. 트랜슬레이터(Translator) : 입력된 각 RTP 데이터그램을 하나 이상의 출력용 RTP 데이터그램으로 만들어주는 장치
7. OSI TP 프로토콜의 연결형 서비스 : 연결 설정(T-CONNECT), 연결 해제(T-DISCONNECT), 일반 데이터(T-DATA), 긴급 데이터(T-EXPEDITED-DATA)

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제11주차 1교시

강의주제 인터넷 서비스의 이해

학습목표

1. 웹 서비스 구조를 이해하고 설명할 수 있다.
2. APM(Apache, PHP, MySQL)의 연동 방식을 설명할 수 있다.
3. 웹 서비스(HTTP, WWW)를 설명할 수 있다.
4. 웹의 진화과정과 발전 방향에 대해 말할 수 있다.

학습내용

1. 웹 서비스 구조
2. APM(Apache, PHP, MySQL)의 연동 방식
3. 웹 서비스(HTTP, WWW)
4. 웹의 진화 과정과 발전 방향

사전학습

미래의 웹은 어떠한 방향으로 발전될 것이라고 생각하나요?

본 학습

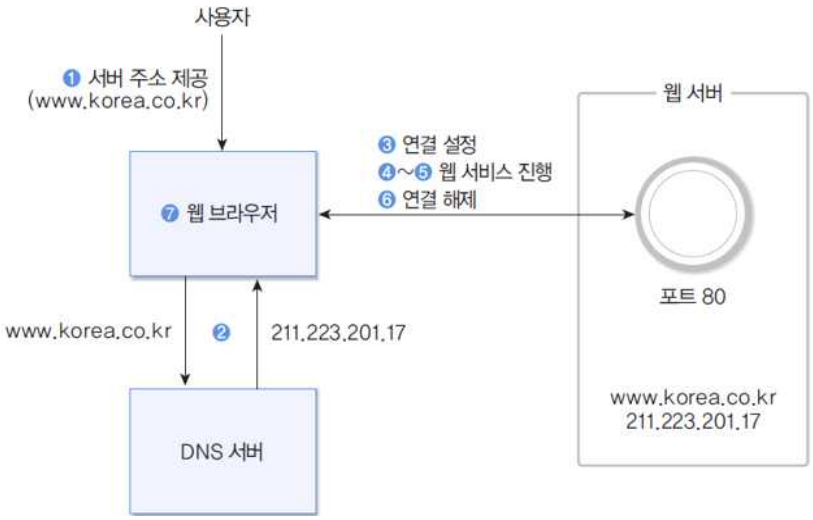
1. 웹 서비스 구조

1) 개요

- 웹(WWW, World Wide Web) 서버의 TCP 포트 번호 : 80번으로 지정
- 클라이언트-서버 모델
  - URL(Uniform Resource Locator) : 웹 서버를 지칭하며 프로토콜, 연결하는 서버의 호스트 이름, 서버 내부의 파일 경로명으로 표현
    예) http://www.korea.co.kr/welcome.html
  - 유닉스, 리눅스 시스템
    - 로그인 이름 : hong
    - 홈 디렉토리 : /public_html/index.html
      예) http://www.korea.co.kr/~hong

2) 웹 서비스 동작 원리

① 웹 브라우저에 URL 주소를 입력
② 클라이언트는 서버 호스트 이름을 DNS 서버에 전송, 웹 서버의 IP 주소 얻음
③ IP 주소와 Well-known 포트 80번을 사용하여 웹 서버와 TCP 연결을 시도
④ TCP 연결이 설정되고 클라이언트가 서버에 GET 명령을 전송
⑤ 서버가 요청한 웹 문서를 웹 브라우저에 회신
⑥ 둘 사이의 TCP 연결을 해제
⑦ 웹 브라우저는 해당 파일의 내용을 사용자가 볼 수 있게 화면에 표시



2. APM(Apache, PHP, MySQL)의 연동 방식

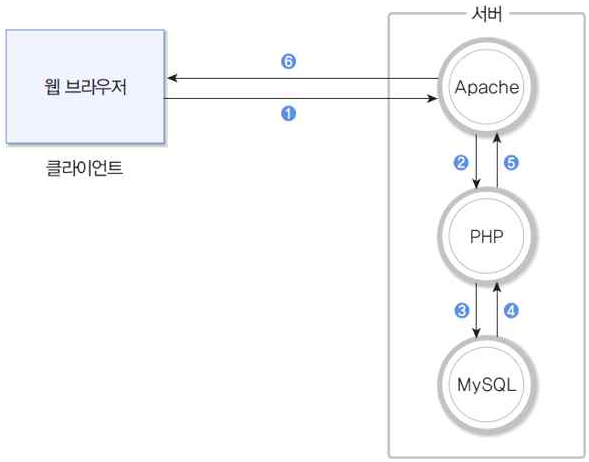
1) APM의 웹 서비스 구조

- APM(Apache, PHP, MySQL)
  - PHP : 유닉스나 리눅스 환경에서 주로 사용
  - 아파치 : 웹 서버 프로그램
  - MySQL : 데이터베이스

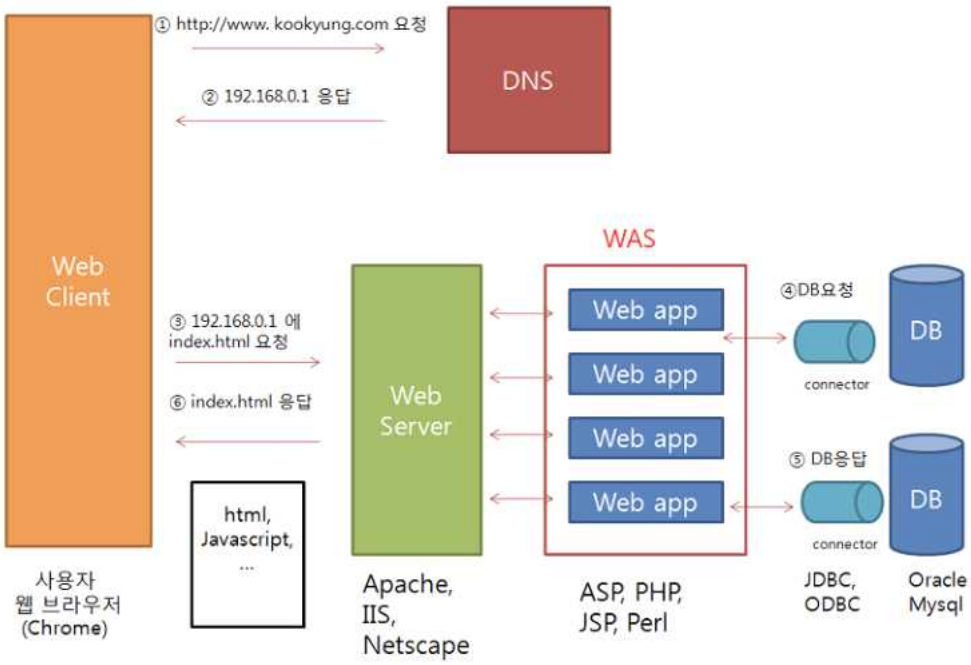
- PHP
  - HTML 언어의 기능을 보완, 문서 내부에 PHP 코드를 추가하는 형식으로 사용
  - 모든 종류의 운영체제에서 지원
  - 공개용 데이터베이스인 MySQL과도 연동이 쉬움

2) APM의 동작 원리

① 웹 브라우저가 Apache에 웹 문서 요청
② PHP 코드 처리 필요 시 PHP에 요청
③ 데이터베이스 처리 필요 시 MySQL에 요청
④ 데이터베이스 결과 회신
⑤ PHP가 실행 결과인 HTML 코드 회신
⑥ 웹 문서를 웹 브라우저에 회신



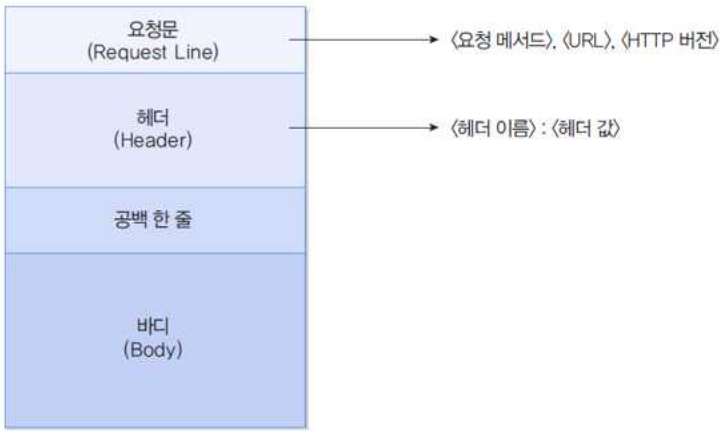
3) 웹 구조



3. 웹 서비스(HTTP, WWW)

1) HTTP(HyperText Transfer Protocol)

- 웹 문서를 전송하는 프로토콜이며 TCP 포트 80번
- HTTP의 요청과 응답
  - RFC 2616으로 발표된 HTTP 1.1 버전
    - 클라이언트의 요청과 서버의 응답에 의해 동작하는 간단한 프로토콜
    - HTTP 클라이언트가 서버에 요청을 전송, 요청 메서드, URL, HTTP 버전과 기타 부가 정보 포함
    - HTTP 서버가 요청의 결과인 응답 코드가 포함된 정보를 회신
- 비상태 연결
  - 요청과 응답 이후, 연결이 끊어지므로 비상태 프로토콜
- MIME 유사 메시지
  - HTTP의 요청·응답 메시지는 MIME(Multipurpose Internet Message Extensions) 유사 구조를 사용해 데이터를 전송
- 요청 메시지 구조



- 요청 메서드 : 클라이언트가 서버에 실행을 요구하는 명령을 기술
- 요청 메서드의 명령
  - GET
    - URI(URL)이 가진 정보를 검색하기 위해 서버 측에 요청하는 형태로 보통 리소스를 조회할 때 사용함
    - 서버에 전달하고 싶은 데이터는 query를 통해서 전달
  - POST
    - 데이터 요청을 처리하고, 메시지 바디를 통해 서버로 데이터를 전달함
    - 요청 URI(URL)에 양식 입력을 처리하기 위해 구성한 서버 측 스크립트(ASP, PHP, JSP 등) 혹은 CGI 프로그램으로 구성되고 Form Action과 함께 전송됨
    - 이때 헤더 정보에 포함되지 않고 데이터 부분에 요청 정보가 들어가게 됨
  - PUT
    - 리소스가 있으면 대체하고 리소스가 없으면 생성함
    - POST처럼 정보를 서버로 제출하는 것이지만 덮어쓴다고 보면 됨
  - DELETE : 웹 리소스를 제거할 때 사용

- HEAD
  - HEAD 요청 방식은 GET과 유사한 방식이나 웹 서버에서 헤더 정보 이외에는 어떤 데이터도 보내지 않음
  - 웹 서버의 다운 여부 점검(Health Check)이나 웹 서버 정보(버전 등)등을 얻기 위해 사용
- OPTIONS : 해당 메소드를 통해 시스템에서 지원되는 메소드 종류 확인
- CONNECT : 웹 서버에 프록시 기능을 요청할 때 사용
- TRACE : 원격지 서버에 Loopback 메세지를 호출하기 위해 사용

● 응답 메시지 구조

● HTTP 상태 코드

- 1XX (Informational: 조건부 응답) : 프로토콜을 교체해도 된다거나 계속 요청을 보내도 된다거나하는 식의 정보성을 띄고 있는 상태

응답코드	설명
101 (Continue)	- 요청자는 요청을 계속해야 함 - 서버는 이 코드를 제공하여 요청의 첫 번째 부분을 받았으며 나머지를 기다리고 있음을 나타냄
102 (Processing)	- 사용자가 수신 요청을 해 처리하고 있지만, 아직은 제대로 된 응답을 할 수 없는 상태

- 2XX (Success: 성공) : 클라이언트가 요청한 동작을 수신하여 이해했고 승낙했으며 성공적으로 처리했음을 가리킴

응답코드	설명
200 (Success)	성공적으로 처리된 경우
202 (Accepted)	요청이 받아들여졌지만 처리가 되지 않았음
204 (No Content)	성공적으로 처리했지만 콘텐츠를 제공하지 않음
206 (Partial Content)	콘텐츠의 일부분만 제공

- 3XX (Redirection: 리다이렉션 완료) : 이 요청을 완료하기 위해서는 리다이렉션이 이루어져야 한다는 의미

응답코드	설명
301 (Moved Permanentely)	영구적으로 콘텐츠가 이동했을 때 사용
302 (Found)	일시적으로 콘텐츠가 이동했을 때 사용
304 (Not Modified)	200 다음으로 자주보는 상태, 이 경우 브라우저에 캐시되어 있는 버전을 사용

- 4XX (Client error: 클라이언트 에러) : 400번대의 코드들은 클라이언트가 서버에게 보낸 요청이 잘못된 경우를 의미

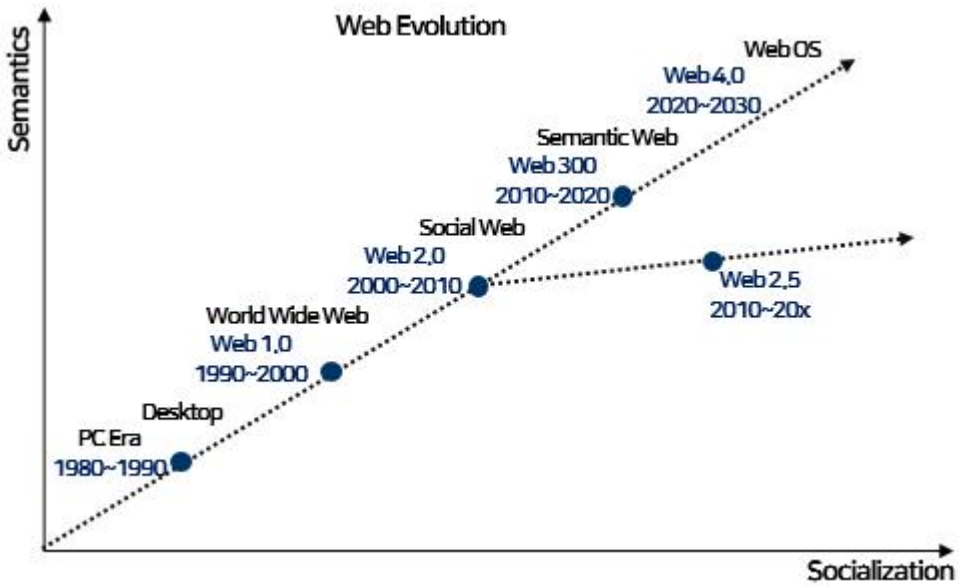
응답코드	설명
400 (Bad Request)	- 요청 자체가 잘못되었을 때 사용됨
401 (Unauthorized)	- 인증이 필요한 리소스에 인증없이 접근한 경우 발생 - 이 응답코드를 사용할 때에는 반드시 브라우저에 어떤 인증방식을 이용할 것인지를 보내야 함
402 (Payment Required)	- 결제가 필요한 리소스에 결제없이 접근했을 경우 발생
403 (Forbidden)	- 서버가 요청을 거부할 때 발생함 - 관리자가 해당 사용자를 차단했거나 서버에 index.html이 없는 경우에도 발생함
404 (Not Found)	- 찾는 리소스가 없다는 뜻
406 (Not Acceptable)	- 요청은 정상이나 서버에서 받아들일 수 없는 요청일시 사용하는 코드 - 보통 웹 방화벽에 걸리는 경우 이 코드가 반환됨
408 (Request Timeout)	- 요청 중 시간이 초과되었을때 사용하는 코드
409 (Conflict)	- 사용자의 요청이 서버의 상태와 충돌하여 응답하는 코드
410 (Gone)	- 찾는 리소스가 영원히 사라진 경우 사용하는 코드 - 404가 그런 게 없어서 못 찾는 경우라면, 410은 있었던 것이 없어져서 못 찾는 것
429 (Too Many Requests)	- 일정 시간 동안 너무 많은 요청을 보냈을 때 이를 거부하기 위해 사용
451 (Unavailable For Legal Reasons)	- 국가 검열 등, 법적인 이유로 차단되었을 경우 사용할 수 있도록 정의된 코드

- 5XX (Server Error: 서버 오류) : 올바른 요청에 대해 서버가 응답할 수 없다는 의미

응답코드	설명
500 (Internal Server Error)	- 서버에 오류가 발생해 작업을 수행할 수 없을 때 사용
501 (Not Implemented)	- 서버가 요청을 수행하는데 필요한 기능을 지원하지 않는 경우 사용
502 (Bad Gateway)	- 게이트웨이가 연결된 서버로부터 잘못된 응답을 받았을 때 사용
503 (Service Temporarily Unavailable)	- 서비스를 일시적으로 사용할 수 없을 때 사용 - 주로 웹서버 등이 과부하로 다운되었을 때 볼 수 있음
504 (Gateway Timeout)	- 게이트웨이가 연결된 서버로부터 응답을 받을 수 없었을 때 사용
508 (Loop Detected)	- 서버가 요청을 처리하는 동안 무한 루프를 발견하였을 때 뜨는 응답코드
511 (Network Authentication Required)	- 사용자가 네트워크 엑세스 권한이 필요한 경우 뜨는 응답코드 - 보통 네트워크에 엑세스할 때 로그인이 필요한 경우

4. 웹의 진화 과정과 발전 방향

1) 웹의 진화 과정



① 웹 1.0

- 웹 2.0이 유행하기 전의 월드 와이드 웹 상태
- 1990년부터 2000년까지의 기간에 있던 대부분의 웹사이트가 이에 해당
- 기본적인 개념은 디렉터리 검색
  - 모든 자료는 체계적으로 분류되어 있으며, 사용자들은 해당 카테고리를 통해 자료를 검색

② 웹 2.0
- 용량이 큰 동영상이나 이미지 파일도 큰 제약 없이 쉽게 업로드
- 키워드로 검색하는 웹 엔진
- 키워드가 길거나 키워드로 검색할 수 없는 정보라면 원하는 정보를 찾을 수 없음

③ 웹 3.0
- 언제 어디서든 원하는 정보를 찾아 개인별 맞춤 서비스가 가능한 지능형 웹
- 사용자가 원하는 정보를 정확히 찾아주는 시맨틱웹 기반의 지능형 웹 서비스
- 분산 컴퓨팅을 실현할 수 있는 신기술이라는 기대가 컸지만, 시장에서의 실효성 때문에 많이 보급되지는 않음

④ 웹 4.0
- '웹 OS'로 규정(인터넷이 사람의 두뇌를 대체한다는 뜻)
- 시맨틱웹 기술로 인간을 대신하는 에이전트(로봇, 인공지능 등)가 인간의 질문을 이해하고, 방대한 정보를 검색하고 편집한 후 적절한 답안을 스스로 추론하여 제공하는 것이 목표인 시스템
- 인간과 기계 또는 기계와 기계를 연결하는 역할을 수행할 전망
- 기계와 기계, 기계와 인간이 의사소통하는 웹 환경을 구현

2) 웹 언어의 진화와 발전 방향
- CGI 언어
  - 서버와 외부 데이터, 응용 프로그램 간의 인터페이스
  - 브라우저에서 서버로 보낸 데이터를 가공하여 응용 프로그램에 전달
  - 응용 프로그램에서 받은 데이터를 가공하여 서버를 통해 브라우저로 전달
  - ASP, PHP, JSP 등
- 마크업 언어
  - 웹 서버에 저장된 문자, 그림, 표, 음성, 동영상 등을 포함한 문서를 클라이언트가 내려받아 웹 브라우저에 표현할 때 사용
  - SGML, HTML 순으로 발전
  - XML은 SGML과 HTML의 단점을 보완해 등장한 언어
  - SGML
    - 기기나 처리 시스템에 독립적이고, 문헌을 구조화시켜 그 내용이 물리적인 형태와 별도로 유지
    - 융통성 있고 확장이 가능하며 다양한 응용에 사용할 수 있음
    - 기능이 복잡해 SGML을 지원하는 소프트웨어를 개발하기 쉽지 않으며, 비용도 많이 발생
  - HTML
    - 표준 웹 언어, 일반적인 웹 페이지를 작성하면 인터넷 익스플로러 같은 웹 브라우저에서 인식
    - 단순성, 이식성, 사용의 용이성이 장점
    - 태그 집합이 제한적이라 문서의 다양한 특성을 반영할 태그가 충분치 않음
  - XML
    - 1996년 W3C에서 제안
    - 웹에서 구조화된 문서를 전송할 수 있도록 내용(XML)과 구조(DTD), 표현(XSL)이 분리된 구조적 문서
    - 데이터베이스 조작이나 환경 설정, 서비스 관련 설정을 더 쉽게 처리할 수 있음
    - XML 문서 작성은 구조인 DTD와 XML 스키마 작성도 포함
    - DTD : 접근하기 쉽지만 정보의 구조까지는 제어할 수 없음
    - XML 스키마 : 정보의 구조까지 제어할 수 있음, 규칙이 엄격해 웹 서비스를 자동으로 구현하기 용이하나 접근이 어려움

- AJAX
  - 대화식 웹 응용 프로그램을 제작하기 위해 여러 기술을 조합하여 만든 웹 개발 기법
  - 웹에 있는 DHTML, CSS, XML과 마이크로소프트 객체인 XMLHttpRequest 기술을 합쳐 만든 것
  - DHTML, 자바스크립트, CSS 등 기존 웹 기술을 그대로 이용할 수 있음
- jQuery
  - HTML의 클라이언트 사이드 조작을 단순화하도록 설계된 크로스 플랫폼의 자바스크립트 라이브러리
  - 존 레식이 2006년 뉴욕시 바캠프에서 공식적으로 소개
- HTML5
  - 차세대 웹 표준으로 2014년 10월 28일에 W3C가 발표
  - HTML이 멀티미디어 등 다양한 애플리케이션까지 표현 및 제공하도록 진화
  - 오디오, 비디오, 그래픽의 처리, 위치정보 제공 등 다양한 기능을 제공
  - 홈페이지에서 사용한 시맨틱 태그를 사용한 레이아웃을 다른 곳에서 검색하고 의미를 알아내기 쉬움
  - 기존의 웹 콘텐츠의 경우, One source, One Device로 운영되었으나, HTML5가 적용됨에 따라 비로소 표준을 따르는 대부분의 브라우저를 수용하는 환경이 됨

3) 사물 인터넷

- 각종 사물에 컴퓨터 칩과 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미
- 기술 요소는 크게 하드웨어 기술과 소프트웨어 기술로 구분
- 다양한 분야에 적용 가능(스마트 홈, 헬스케어, 원격검침, 스마트 카 등)
- 다양한 산업에 융합되어 사용 가능(농축, 건설, 에너지, 자동차, 교통, 물류, 환경, 디지털 콘텐츠 산업 등)
- 사물인터넷 구현 기술요소
  - 센싱기술 : 각종 센서, RFID, 태그기술, GPS, 자이로스코프, 가속도계 등
  - 유무선 통신 기술 : 지그비, NFC, 블루투스, 로라, LAN, WAN 등
  - 서비스 인터페이스 기술 : 미들웨어
  - 보안기술 : 암호화, 해킹방지, 정보유출 방지

학습정리

1. URL(Uniform Resource Locator) : 웹 서버를 지칭하며 프로토콜, 연결하는 서버의 호스트 이름, 서버 내부의 파일 경로명으로 표현
2. HTTP(HyperText Transfer Protocol) : 웹 문서를 전송하는 프로토콜이며 TCP 포트 80 번
3. 웹의 진화 과정 : 웹 1.0 → 웹 2.0 → 웹 3.0 → 웹 4.0
4. CGI 언어 : 서버와 외부 데이터, 응용 프로그램 간의 인터페이스
5. 마크업 언어 : 웹 서버에 저장된 문자, 그림, 표, 음성, 동영상 등을 포함한 문서를 클라이언트가 내려받아 웹 브라우저에 표현할 때 사용
6. 사물 인터넷 : 각종 사물에 컴퓨터 칩과 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제11주차 2교시

강의주제 FTP외 SMTP의 이해

학습목표

1. 파일 전송 서비스(FTP)를 설명할 수 있다.
2. 메일 서비스(SMTP)를 설명할 수 있다.
3. FTP 덤프 분석을 수행할 수 있다.

학습내용

1. 파일 전송 서비스(FTP)
2. 메일 서비스(SMTP)
3. FTP 덤프 분석

사전학습

기존 www 서비스가 존재함에도 불구하고 파일 전송을 위한 별도의 프로토콜이 필요한 이유는 무엇이라고 생각하나요?

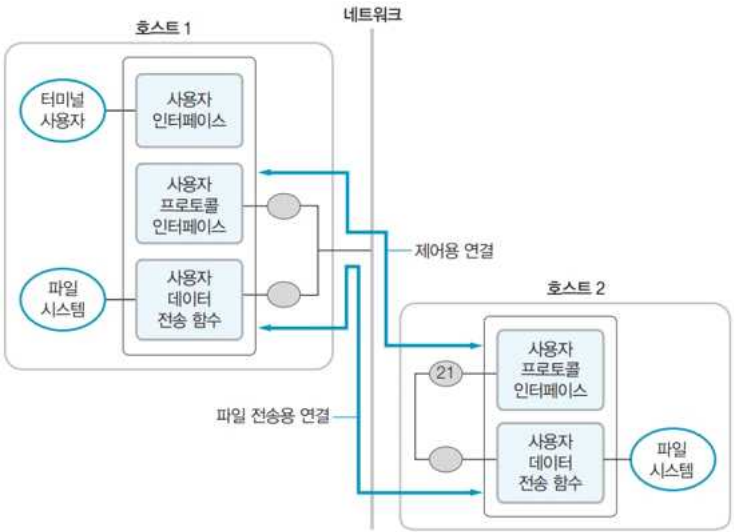
본 학습

1. 파일 전송 서비스(FTP)

1) 개요

- TCP/IP 프로토콜의 응용 계층에 속함
- TCP/IP 프로토콜을 가지고 서버와 클라이언트 사이의 파일 전송을 위한 프로토콜
- HTTP 프로토콜을 통해 접속되는 WWW(World Wide Web) 방식이 주된 방식
- WWW는 일반 문서를 비롯하여 사진·음악·동영상 콘텐츠까지 간편하게 사용할 수 있고, 네이버 클라우드, 구글 드라이브 등 간편하고 빠른 웹 하드 서비스를 쉽게 접할 수 있음
  → 큰 데이터의 파일을 한 번에 주고받기 어렵다는 단점이 있음
- FTP의 장점
  - FTP는 파일 전송 전용 서비스라는 특징과 인터넷을 통한 파일 송수신만을 위해 고안된 서비스(프로토콜)이기 때문에 동작방식이 단순하고 직관적임
  - 사용법이 간단하고 빠른 속도로 많은 파일을 주고받을 수 있음
- 빠른 파일 전송이 주된 목적이기 때문에 사진이나 음악, 동영상 등의 멀티미디어 콘텐츠는 내려받기가 완료된 다음에 확인할 수 있음(스트리밍 서비스 미지원)

2) FTP 동작 원리



- FTP 서비스를 제공하는 서버와 여기에 접속하는 클라이언트 사이에 두 개의 연결(세션)이 생성됨
- 21번 포트 : 데이터 전송을 제어하기 위한 신호를 주고받기 위한 포트
- 20번 포트 : 실제 데이터(파일) 전송에 사용되는 포트
- FTP 서버에 접속할 때는 사용자 계정과 암호를 입력하는데, 이러한 정보들은 데이터 제어 신호를 통해서 주고받게 됨
- 실제 파일 송수신 작업은 데이터 전송(20번 포트)에서 처리
- FTP 클라이언트 프로그램은 여러 파일을 연속으로 송수신해야 하므로 서버와의 지속적인 응답 메시지 전송을 통해 연결 상태(세션)를 유지
- FTP통신은 TCP통신을 하므로, 처음 3-way-handshaking 과정을 거친 후 클라이언트가 명령어를 입력하면, 서버는 숫자 코드로 응답

- 동작 순서

① 서버는 FTP의 포트 21을 개방하고, 클라이언트가 접속하기 까지 대기
② 클라이언트는 연결 제어를 하기 위해 TCP 포트 21을 개방
③ 클라이언트는 연결된 제어를 이용해 파일 전송을 요청
④ 서버는 FTP의 21 포트로 클라이언트와 연결을 설정
⑤ 서버는 연결을 이용해 클라이언트에 파일을 전송
⑥ 파일 전송 후 서버는 연결을 해제
⑦ 원하는 파일을 전부 수신했으면 클라이언트는 연결을 해제
⑧ 서버는 다른 서비스 요청이 있을 때까지 잠시 대기

(1) FTP 보안 취약점

- 사용자 인증정보에서 암호화 부재
- 계정 로그인의 인증 취약점을 악용한 Brute force 공격
  - 무차별 대입(Brute Force) 공격
    - 인증 정보(사용자 이름과 비밀번호)를 알아내기 위해 공격자가 반복적으로, 체계적으로 매번 다른 사용자 이름과 비밀번호를 입력하는 방식의 공격임
    - 단순하지만 리소스를 많이 소비하는 시행착오 기반의 접근 방식임
    - 보통 자동화된 툴이나 스크립트 또는 봇을 사용해 액세스 권한을 회득할 때까지 가능한 모든 조합을 대입
- Sniffing 공격으로 인한 인증정보 유출
  - Sniffing : 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미하며 네트워크 트래픽을 도청(eavesdropping)하는 과정
- 익명(Anonymous) FTP 취약
- FTP 바운스 공격 : 명령 채널과 파일 전송 채널이 별도로 존재하므로 실제 파일을 전송받는 클라이언트가 바뀔 수 있다는 취약점이 존재

3) FTP 통신

- FTP는 데이터(파일)를 전송함에 있어, 수동 모드(Passive Mode)와 능동 모드(Active Mode) 두 가지를 지원
- Active Mode : 이 모드로 데이터 전송을 할 때에는 서버는 20번 포트 사용
- Passive Mode : 이 모드로 데이터 전송을 할 때에는 서버는 1024~65535 사이의 랜덤한 비특권 포트를 사용

(1) 능동모드(Active Mode)

- 수행과정

① 클라이언트에서 FTP 서버의 21번 포트로 접속을 시도하고, 사용할 두 번째 포트를 서버에 알려줌
② 서버는 ACK로 응답
③ 서버의 20번 포트는 클라이언트가 알려준 두 번째 포트로 접속을 시도
④ 마지막으로 클라이언트가 ACK로 응답

- 최초 접속 요청
  - 클라이언트는 서버의 21번 포트로 접근하여 로그인을 요청
  - 서버는 정상적인 접근일 경우 그에 대한 승인을 하고 로그인이 이루어짐

- 데이터 전송을 위한 절차
  - 클라이언트가 로그인을 하게 되면 서버에게 "데이터 전송을 위해서 내 쪽의 xxxx포트로 접속해"를 알려줌
  - 이에 서버는 20번 포트를 이용하여 클라이언트가 알려준 포트로 접속을 하고 데이터를 전송
- 문제점
  - TCP/IP의 특징인 '클라이언트가 서버에 접속을 시도하는 것'이 아니라 '서버가 클라이언트에 접속을 시도한다'는 것 때문에 클라이언트 PC에 내부적인 환경요인(방화벽)과 외부적인 환경요인(FTP를 제대로 인지하지 못하는 공유기)으로 FTP가 접속이 제대로 되지 않음
  - 접속이 되더라도 이후 데이터 목록을 받아오지 못하는 에러가 발생할 수 있음

(2) 수동모드(Passive Mode)

- 수행과정
  - 서버가 클라이언트에 접속을 시도하는 비정상적인 능동모드에 대한 문제점을 해결하기 위해 수동모드(Passive Mode) 등장

① 클라이언트가 21번 포트로 접속을 시도
② 서버에서는 서버가 사용할 두 번째 포트를 알려줌
③ 클라이언트는 다른 포트를 열어 서버가 알려준 이 포트로 접속을 시도
④ 이에 서버는 ACK로 응답

- 임의의 비특권 포트를 사용
  - 수동 모드에서는 두 번째 data포트로써 능동모드에서 사용했던 20번 포트를 사용하지 않고 1024 ~ 65535 사이의 임의의 비특권 포트를 사용
- 최초 접속 요청
  - 능동 모드와 동일한 절차를 거쳐 로그인
  - 서버의 21번 포트로 접속을 하게 되고 서버는 승인을 함
- 데이터 전송을 위한 절차
  - 데이터 전송 시 능동모드와 달리 클라이언트는 서버 쪽에서 알려준 임의포트와 연결하여 데이터를 송수신

4) 익명(Anonymous) FTP

(1) 익명 FTP 취약점과 보안 문제점

- FTP를 설치하게 되면 default로 Anonymous FTP가 실행
- 하지만 보안 절차를 거치지 않고 익명으로 사용하는 사용자에게 FTP 서버 접근을 허용하는 경우 여러가지 보안 문제점이 발생
- Anonymous FTP 서버로 사용자들이 데이터를 upload 할 수 있는 기능을 제공하는 경우 악의를 가진 사용자가 문제가 있는 소프트웨어를 upload하면 심각한 문제를 유발할 수도 있음
- Anonymous FTP 서버에 침입자가 침입하여 루트 권한을 획득할 경우 서버에 있는 모든 자료들을 수정할 수 있기 때문에 서버가 신뢰하는 자료를 가지고 있다고 보기 어려움

(2) 익명 FTP 보안 대책

- 호스트에서 제공할 서비스와 사용할 계정을 고려
  - Anonymous FTP 서비스만 제공하는 호스트를 구축
  - FTP 외에 다른 서비스를 같이 제공하는 호스트를 구축할 경우 다른 서비스들에 대한 차단을 할 수 없는 경우가 많기 때문에 호스트의 보안을 설정하는데 많은 문제점을 야기할 수 있음
  - 불필요한 계정은 만들지 않으며 대부분의 Anonymous FTP 서버에는 일반 사용자 계정을 두지 않는 것이 관례

- 사용자에 대한 최소한의 정보만 유지
  - ftp/etc 디렉터리에는 passwd와 group 파일을 만들어 주게 되는데, 이 파일의 용도는 익명의 사용자가 ls -l 등을 이용할 때 그 파일의 소유주나 그룹을 보여 주는 역할만을 할 뿐임
  - 실제로 유닉스의 /etc/passwd나 /etc/group 파일이 이용되는 것과 같은 용도로는 사용되지는 않음
  - 그러므로 보안 수준을 높이고 싶다면 이 파일을 만들지 않는 방법이 추천되고 있음
  - 사용자들에게 좀 더 좋은 인터페이스를 제공하기 위해서 이 파일들을 가져다 놓게 될 경우, /etc/passwd 나 /etc/group 파일을 그대로 복사하여 가져다 놓을 수 있음
  - 이는 그 호스트의 사용자와 그룹의 정보를 유출시킬 수 있기 때문에 불필요한 사용자들을 지워버리는 것이 좋음
- 권한의 설정
  - 최소한의 서비스를 위한 권한만 사용자에게 제공
  - 익명 사용자가 로그인했을 때 루트가 되는 디렉터리를 ftp라고 하면 이 디렉터리의 소유주는 반드시 루트가 되어야 함
    - 퍼미션(permission)은 555(user, group, other에게 쓰기권한을 주지 않음)로 해야 함
  - ftp/bin 디렉터리에는 FTP 서비스 시에 이용될 수 있는 프로그램들을 가져다 놓게 되는데 이 때 소유주는 루트로 하고 퍼미션은 111(noread, nowrite, execute)로 해줌
    - 여기에 가져다 놓게 되는 프로그램들 또한 위와 같은 소유주와 퍼미션을 주는 것이 좋음
  - ftp/etc의 소유주도 루트로 해주며, 이 퍼미션도 111로 설정
  - 다운로드 할 수 있는 파일들을 보관하는 ftp/pub 디렉터리의 소유주는 이 FTP를 관리할 사람의 권한으로 해주고, 퍼미션은 555로 설정
  - ftp/incoming과 같이 누구나 파일을 업로드할 수 있게 해줄 수 있는 권한을 줄 디렉터리는 소유주는 root, 퍼미션은 777로 해줌
    - 조금 더 보안의 수준을 높이고 싶다면 이 디렉터리만을 위한 새로운 파일 시스템을 만들어 줌
  - ftp 밑에 .rhost나 .forward 파일을 만들되, 파일의 크기를 0으로 하여 소유주는 root, 권한은 000(noread, nowrite, noexecute)으로 설정
- 정기적인 점검
  - 정기적으로 ftpd 데몬에 의해서 만들어지는 로그 파일을 분석함으로써 불필요한 접근이나 명령어의 시도가 있었는지를 감시

5) FTP Bounce Attack(FTP 바운스 공격)

(1) FTP Bounce Attack

- FTP 서버가 클라이언트가 지시한 곳으로 자료를 전송할 때 그 목적지가 '어떤 곳'인지를 검사하지 않는 FTP 프로토콜 구조의 허점을 이용한 공격 방법
- FTP 클라이언트가 실행되는 호스트가 아닌 다른 호스트를 지정하더라도 서버는 충실하게 지정된 곳으로 정보를 보냄

(2) FTP 바운스 공격 예시

- 포트 스캐닝
  - 클라이언트가 자료 전송을 요청할 때, 지정한 포트가 열리지 않으면 실패 메시지가, 성공하면 성공 메시지가 출력되는데 이러한 메시지를 이용한 포트 스캐닝 스크립트에 이용할 수 있음
- 거짓 편지(Fake mail)
  - 메일의 정보를 가진 부분을 헤더라고 하는데, FTP 바운스 공격을 이용하면 이러한 정보가 허위로 입력된 거짓 편지를 만들어 보낼 수 있음
  - 임의의 메일을 텍스트 형태의 파일로 만들어 바운스 공격을 통하여 서버에 전송
  - 서버는 이 fake mail을 지정된 목적지로 전송

- 바운스 공격을 통해 전송된 메시지는 익명성을 가지며 송신지를 알 수 없음
- FTP 서버의 주소는 알 수 있지만 여러 경로를 통하기 때문에 공격자를 거의 찾을 수 없음

● 방화벽을 넘어 접근하기

- 방화벽의 내부에 외부에서 익명 접근이 가능한 FTP 서버가 있다면 FTP 서버는 방화벽의 내부에 존재하기 때문에 방화벽의 Packet Filtering을 완전히 무시하고 여러 가지 작업을 수행할 수 있음

(3) FTP 바운스 공격 대응책

● FTP가 자료를 전송할 때 1024번보다 낮은 포트(port)로 접속하지 않도록 설정
● 클라이언트와 다른 호스트로 접속하지 않도록 설정
● FTP 외의 다른 서비스들이 20번 포트로부터는 접속을 받아들이지 않도록 설정
● 최신 버전의 FTP server를 설치

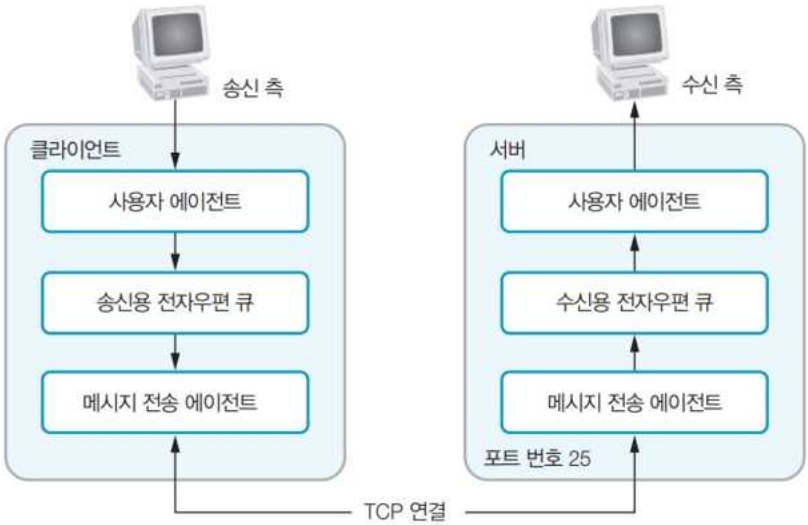
2. 메일 서비스(SMTP)

1) 개요

● SMTP(Simple Mail Transfer Protocol), 전자우편 서비스를 사용할 수 있는 프로토콜
● 하위 계층에서 TCP 프로토콜을 사용하며, 전자우편을 송수신하려고 사용자 에이전트와 메시지 전송 에이전트를 사용
● 사용자의 메시지 접수방법, 사용자 인터페이스 구성방법, 사용자의 메시지 저장 방법 등은 지정하지 않음
● TCP/IP 네트워크 환경에서 인터넷 메일 서비스를 담당하는 응용 계층의 프로토콜은 POP3와 SMTP이며 인터넷에서 클라이언트가 메일을 송수신하려면 다음과 같은 서비스가 필요

- SMTP 전송 서비스
  - 메일 서버는 일종의 우체국 역할을 수행하며 일단 전송된 메일을 분류함
  - 자신의 클라이언트에 보내는 메일은 자신의 메일 서버에도 저장하고, 다른 메일 서버로 전송되는 메일은 해당 메일 서버로 전송
- SMTP 수신 서비스
  - 메일 서버는 클라이언트가 메일을 수신할 수 있도록 해야 하며 이 서비스는 우편물을 넣는 우체통 기능을 수행
- POP3 서비스
  - TCP/IP 네트워크 환경에서 POP3 서비스는 클라이언트에 발송한 메일을 해당 메일 서버가 자동으로 전송하는 것이 아니라 클라이언트가 직접 네트워크(메일 서버)에 접속해서 다운로드할 수 있게 해주는 서비스
  - 이 서비스는 우편물을 받을 사람이 우체국에 직접 가서 우편물을 찾아가는 것에 비유할 수 있음

2) SMTP 동작 원리



① 송신 측에서 메일 명령을 수행
② 송신 측에서 SMTP에 규정된 전자우편 형식에 따라 내용을 작성
③ 송신 측에서 송신용 메일 큐나 스풀에 송신할 내용의 전자우편을 미리 저장
④ 송신 측에서 수신용 메일 큐에 전자우편을 검색, 있으면 헤더를 참조해 SMTP 규정에 따라 수신 측으로 발송
⑤ 수신 측에서 수신용 메일 큐에 전자우편이 있으면 전자우편을 읽음

3) SMTP 기본 명령어

- HELO: 클라이언트 자체를 식별하기 위해 클라이언트에서 보냄
- MAIL FROM: 메시지를 보낸 사람을 식별
- RCPT TO: 메시지 받는 사람을 식별
- SIZE: SMTP 서버에서 지원되는 최대 메시지 크기를 표시할 수 있는 메커니즘
- DATA: 클라이언트에서 메시지 내용 전송을 초기화하기 위해 보냄
- RSET: 전체 메시지 트랜잭션을 무효화하고 버퍼를 다시 설정
- QUIT: 세션을 종료

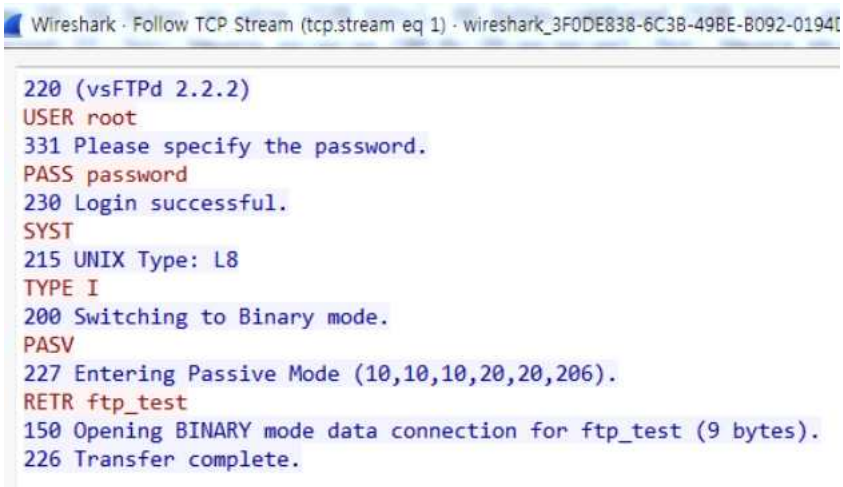
4) SMTP 응답 코드

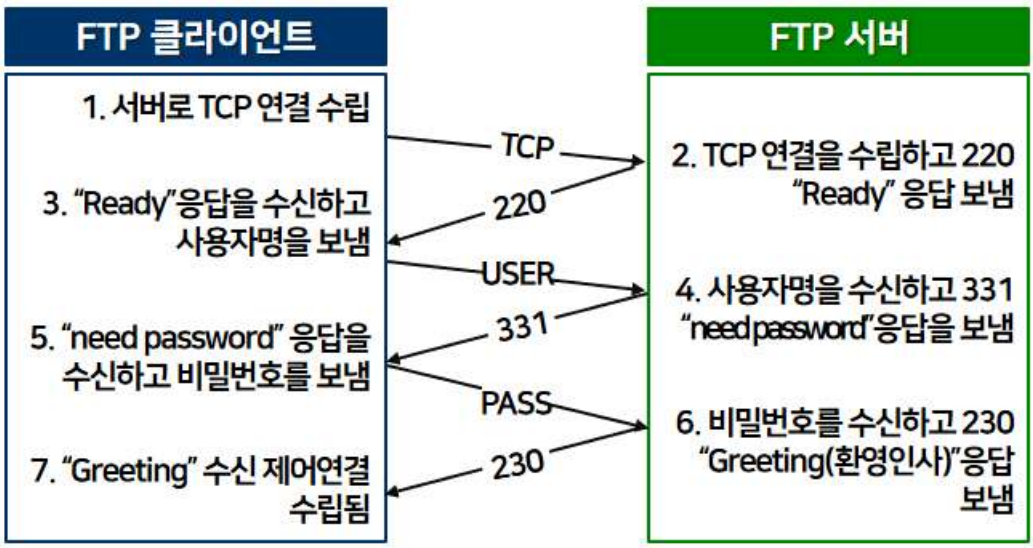
- 211: 서버 상태 메시지
- 214: help 명령을 실행할 때 나오는 코드 메시지
- 220: 메일 서버 호스트가 SMTP서비스 가능한 상태
- 250: 접속 종료 응답 코드
- 251: 로컬상에 존재하지 않는 주소일 경우 포워드 주소로 포워딩될 때
- 354: 상대방 서버가 메일 데이터를 받을 준비된 상태
- 421: 요청한 서비스 이용 불가능하여 접속 종료 시
- 450: 메일박스를 사용할 수 없어 요청한 작업이 실행되지 않을 때
- 451: 로컬상 처리 도중에 에러로 인하여 요청한 작업이 중단될 때
- 452: 계정 공간 부족으로 인하여 요청한 작업이 실패할 경우
- 500: 인식할 수 없는 명령이나 syntax 오류 시

- 501: 파라미터 또는 아그먼트로 인한 syntax 오류 시
- 502: 특정 명령이 서버에 따라 실행되지 않을 때
- 503: 명령 순서가 잘못되었을 때
- 504: 명령에 사용되는 파라미터가 해당 서버에서는 적용되지 않을 때
- 521: 메일을 받지 못할 때
- 530: 접근 거부 시
- 550: 요청한 작업이 실행되지 않을 때
- 551: 로컬 상의 주소가 아닐 경우 수동으로 메일이 포워딩되어야 할 때
- 552: 디스크 공간 부족으로 인하여 요청한 작업이 취소될 때
- 553: 부적절한 메일박스로 인하여 요청한 작업이 실행되지 않을 때
- 554: Transaction이 실패될 때

3. FTP 덤프 분석

1) 개요





- FTP 명령에 사용하는 일반적인 포트 번호는 21이지만 다른 포트 번호로 구성하여 동작하게 할 수 있음
- 데이터는 20번 포트를 사용하거나 PASV 또는 PORT 명령 프로세스를 통해 설정된 포트를 사용

- 수동 모드 데이터 전송에는 PASV 명령을 사용하고, 데이터 전송 연결은 FTP 클라이언트가 FTP 서버로 설정
- FTP는 사용자가 put 명령을 입력하면 STOR 명령을 생성하고, 사용자가 get 명령을 입력하면 RETR 요청을 전송

학습정리

1. 파일 전송 서비스(FTP) : TCP/IP 프로토콜을 가지고 서버와 클라이언트 사이의 파일 전송을 위한 프로토콜
2. FTP는 데이터(파일)를 전송함에 있어, 수동 모드(Passive Mode)와 능동 모드(Active Mode) 두 가지를 지원
3. 익명(Anonymous) FTP : FTP를 설치하게 되면 default로 Anonymous FTP가 실행되는데 보안 절차를 거치지 않고 익명으로 사용하는 사용자에게 FTP 서버 접근을 허용하는 경우 여러가지 보안 문제점이 발생
4. FTP Bounce Attack : FTP 서버가 클라이언트가 지시한 곳으로 자료를 전송할 때 그 목적지가 '어떤 곳'인지를 검사하지 않는 FTP 프로토콜 구조의 허점을 이용한 공격 방법
5. 메일 서비스(SMTP) : 전자우편 서비스를 사용할 수 있는 프로토콜

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제12주차 1교시

강의주제 네트워크 관리의 이해

학습목표

1. 네트워크 관리의 개념 및 필요성을 이해하고 설명할 수 있다.
2. 네트워크 관리 기능을 설명할 수 있다.
3. 네트워크 분석 도구를 설명할 수 있다.

학습내용

1. 네트워크 관리의 개념 및 필요성
2. 네트워크 관리 기능
3. 네트워크 분석 도구

사전학습

네트워크를 관리해야 하는 가장 중요한 이유는 무엇이라고 생각하나요?

본 학습

1. 네트워크 관리의 개념 및 필요성

1) 네트워크 관리의 필요성

- 네트워크는 인터넷의 보편화와 함께 급속도로 번지고 있음
- 데이터망과 기존 통신망의 통합과 서로 다른 시스템, 네트워크 장비, 운영체계, 통신규약(Protocol) 등이 복잡하게 묶여 있으며 이를 사용하는 서비스와 사용자가 급격하게 증가하여 점점 규모가 커지고 있음
- 따라서 안정적이고 효율적인 네트워크 환경을 제공하기 위해서 네트워크 상에 존재하는 다양한 자원들을 모니터링하고 제어하는 네트워크 관리의 개념이 필요하게 되었음
- 네트워크를 관리하면 네트워크 모니터링, 트러블 슈팅, 유지·보수 등을 능률적으로 수행할 수 있음
- 네트워크 관리 도구는 네트워크 관리자가 직접 컴퓨터를 살펴보지 않아도 하드웨어와 소프트웨어를 평가하는 기능을 제공
- 중앙 관리 콘솔을 이용하여 원격지에서 업데이트 등 기본적인 컴퓨터 유지 작업을 할 수 있으며, 디스크 공간 문제나 쿨링팬 결함 문제 등도 자동으로 관리자에게 보고됨

2) 네트워크 관리의 개념

- 전산 자원의 중요성이 커짐
  - 네트워크와 분산된 전산 자원들은 그 단체에서 가장 중요한 역할을 수행할 뿐만 아니라 자산으로서도 중요성이 커지게 되어 전산자원 자체도 효율적인 관리를 필요로 하게 됨
- 복잡해진 네트워크 관리 구조
  - 다양한 네트워크 구성요소와 인터페이스, 프로토콜의 사용과 서비스로 인해 네트워크가 한층 복잡해져 관리가 어려워짐
- 서비스 개선
  - 네트워크를 이용하는 규모가 커지고 이에 따라 자원과 정보가 증가함에 따라 안정적인 고속 서비스를 원하게 됨
- 사용자의 다양한 요구 충족
  - 성능, 가동율(Availability), 보안(Security) 등에서 사용자의 다양한 요구를 만족시켜야 함
- 자원의 활용성(Utilization) 증대
  - 네트워크에 소요되는 경비를 조절하기 위해 분산된 네트워크 자원의 활용성을 모니터링하고 제어하는 것이 필요해짐

3) 네트워크 관리 시스템 개요

- 네트워크 관리는 제한된 인력과 비용을 활용하여 네트워크의 효율성과 생산성을 높일 수 있도록 복잡한 네트워크를 제어하는 일련의 과정
- 네트워크에 분산된 각종 자원을 분배·관리·분석·평가하는 기능이 포함됨
- 효율적으로 자원 사용을 극대화함과 동시에 서비스 품질의 측면에서 가용성과 신뢰성을 최상의 상태로 유지하고 응답 시간을 단축하는 시스템
- 자원 사용의 효율성 측면에서는 네트워크 시스템의 처리 능력인 처리율과 이용률을 극대화하는 것이 중요함

- 네트워크 관리 프로세스

4) 네트워크 관리 시스템 구성

- NMS는 에이전트(Agent)와 매니저(Manager)로 나뉘어지며 NME와 NMA로 구성됨
- NME(Net work Management Entity)
  - 실제 에이전트의 역할을 수행하는 객체
  - 네트워크 자원들에 대한 직접적인 관리를 수행
  - 워크스테이션(Workstation), 브리지(Bridge), 라우터, PC를 비롯해서 기타 관리되는 시스템에 존재
  - 네트워크와 관련된 정보를 수집하여 저장하고 매니저로부터 요청이 들어오면 자신이 관리하는 정보를 보내줌
- NMA(Network Management Application)
  - 매니저의 역할을 수행하는 응용프로그램
  - 에이전트가 관리하는 객체의 내용들을 수집해서 전체 네트워크를 관리
  - 에이전트와 통신을 할 때는 다양한 종류의 네트워크로 인해 표준화된 프로토콜(SNMP, CMIP)을 사용하여 정보를 교환
- Proxy
  - 매니저와 에이전트가 서로 다른 프로토콜을 사용하거나 표준에 맞지 않는 자체적인 관리 인터페이스를 가지는 경우 중간에 프록시(Proxy)를 둠
  - 프록시는 매니저의 표준 프로토콜을 받아 상대 시스템에 맞는 형태로 변환시켜서 전달하고, 상대 시스템에서 되돌아온 결과를 표준 프로토콜로 바꾸어 매니저에게 전달

5) 네트워크 모니터링

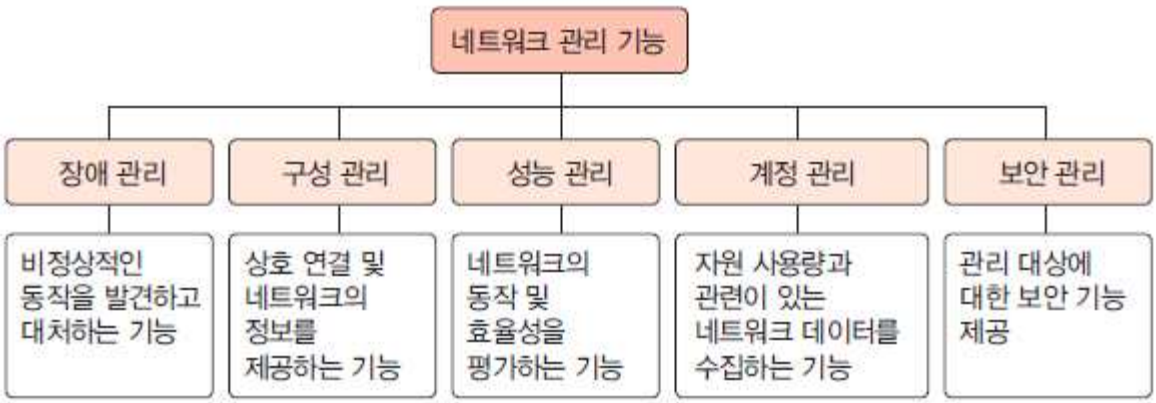
- NMS를 이용하여 네트워크 자원들의 상태를 관찰하여 분석하는 것
- 모니터링 정보의 분류
  - 네트워크 모니터링에서 얻는 정보는 크게 정적 정보, 동적 정보, 통계 정보로 구분
  - 정적 정보(Static Information) : 네트워크의 구성과 구성 요소와 같이 쉽게 변하지 않는 정보(예 : 포트 번호)
  - 동적 정보(Dynamic Information) : 네트워크의 상태와 이벤트에 의해서 변하는 정보(예 : 패킷의 전송량, 에러 개수)
  - 통계 정보(Statistical Information) : 동적 정보의 통계치(평균 전송량)
- 모니터링 방법
  - 에이전트의 내용을 매니저에게 전달하는 방법에는 폴링(Polling)과 이벤트 보고(Event Reporting)가 있음
  - 폴링
    - 요청에 의한 응답(Request-Response) 방식
    - 매니저가 에이전트에게 원하는 정보를 요구(Request)하면 에이전트는 매니저가 원하는 정보를 찾아서 응답(Response)해주고, SNMP(Simple Network Management Protocol)에서 정보를 교환하는 주된 방버
    - 구현은 쉽지만 네트워크에 부하를 많이 주는 단점이 있음

- 이벤트 보고
  - 에이전트가 매니저의 요구가 없어도 매니저에게 정보를 보내는 방법
  - 상태나 속성 값이 자주 바뀌지 않는 경우에 폴링 방식보다 효율적임
  - 특별한 이벤트가 발생했을 경우에 주로 사용되며 SNMP에서는 트랩(Trap)이라고 함

2. 네트워크 관리 기능

1) 개요

- OSI 표준에서는 효율적인 네트워크 관리를 위해 장애 관리, 구성 관리, 성능 관리, 계정 관리, 보안 관리기능을 제안
- 이 외에도 운영 환경을 고려하여 유지·보수, 자산 관리, 사용자 관리, 문서화, 백업 등 부수적인 관리 기능을 다양하게 실행할 수 있음



2) 네트워크 관리 기능의 종류

(1) 장애 관리

- 장애 관리는 네트워크 구성 요소에 문제가 발생하거나 비정상적으로 작동할 때 이를 검출하여 격리·기록·조사·분석·정정함으로써 복잡한 네트워크가 원활하게 작동하도록 하는 것
- 장애가 발생한 시점을 기준으로 사전 장애 관리와 사후 장애 관리로 구분
- 네트워크에 장애가 발생했을 때 문제점을 파악하므로 사전 장애 관리보다는 사후 장애 관리의 의미가 더 크다고 볼 수 있음
  - 사전 장애 관리 : 장애 발생을 억제하는 것으로, 관리 대상을 지속적으로 모니터링하며, 사전에 정의된 규칙이나 정책 등을 이용하여 장애 발생 원인을 사전에 파악하고 처리하는 과정
  - 사후 장애 관리 : 장애가 발생한 시점부터 장애를 처리하여 정상적인 상태로 전환될 때까지의 과정
- 장애 처리 과정

① 장애가 발생한 위치를 파악함(Detect)
② 장애가 발생한 부분을 다른 부분으로부터 격리함(Isolate)
③ 장애의 영향을 최소화하기 위해 네트워크를 변경해서 재구성함(Reconfigure)
④ 장애를 일으킨 구성 요소를 수리하거나 교체함(Repair)

  - 이런 장애 관리를 위해서는 로깅(Logging), 이벤트 보고, 연결 테스트 기능이 필요
  - 로깅 기능은 중요한 사건들과 에러를 기록하는 기능으로서 로그 데이터의 분석을 통해 결함을 발견할 수 있음
  - 이벤트 보고 기능은 어떤 사건이 발생하면 바로 관리자에게 보고하는 기능

- 진단 기능은 연결 테스트(예: traceroute), 프로토콜의 무결성, 응답시간검사(Response Time Check), 생존 검사(예 : ping), 루프백(loop-back) 등을 검사하는 기능

● 모니터링 기법

- SLM(Service Level Management) 이란 네트워크, 시스템 및 어플리케이션까지 포함해 'IT 서비스' 차원의 관리 기능을 제공한다는 개념임
- SLA(Service Level Agreement)에서 정의한 서비스에 대해 정확히 성과를 측정/평가하고 그 결과를 바탕으로 더 나은 서비스가 이루어지도록 개선방안을 마련하는 일련의 과정
- SLM의 기능
  - SLM을 통해 네트워크, 시스템 어플리케이션 등의 상호작용관계를 정의함으로써 문제가 발생했을 때 그 문제의 근본원인을 찾아내고 이것이 다른 자원에 어떤 영향을 미치는지 자동 분석을 수행
- SLM은 장애 정보 항목에 승인과 시간 체크 항목을 추가함으로써
  - 실제로 장애가 발생했을 때 관리자의 인지 여부를 파악하는 항목과 파악 당시의 시간을 기록 ⇒ 장애 발생부터 관리자의 인지 및 처리까지 걸린 시간에 대한 SLA 수치를 기록 및 관리할 수 있음
- 관리 항목은 관리 시스템이 자동으로 탐지한 노드 중에서 선택하거나 관리자가 수동으로 생성
- 관리 항목을 생성한 후 관리 시스템은 각 노드에 대한 장애를 탐지하기 위해 모니터링을 시작
- 모니터링 방식

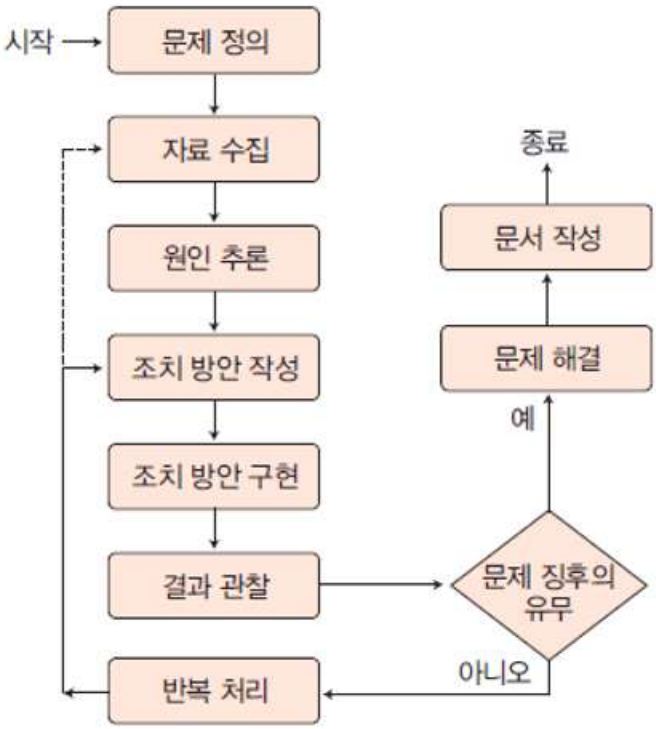
CMIP	- Common Management Information Protocol - 조직적이고 규모가 큰 망관리를 위한 프로토콜 - TCP/IP 기반의 중소규모의 망관리를 위한 SNMP와는 달리, OSI 프로토콜 스택(stack)상에서 동작하는 대규모의 통일화된 망관리 프로토콜
SNMP	- Simple Network Management Protocol - 네트워크 관리를 위해, 관리 정보 및 정보 운반을 위한 단순 망관리 프로토콜 - UDP / IP 상에서 동작하는 비교적 단순한 형태의 메시지 교환형 네트워크 관리 프로토콜
ICMP의 이용하는 방식	- ICMP: Internet Control Message Protocol - 해당 호스트가 없거나, 해당 포트에 대기중에 서버 프로그램이 없는 등의 에러 상황이 발생할 경우 IP헤더에 기록되어 있는 출발지 호스트로 이러한 에러에 대한 상황을 보내주는 역할을 수행

  - 그 외 업체 특유의 프로토콜이나 소켓(Socket) 프로그램에 의해 모니터링 하는 방법

● 트러블 슈팅

- 네트워크 또는 시스템에 장애가 발생했을 때 원인을 빠르게 규명하고 장애를 복구하는 일련의 작업
- 트러블 슈팅을 하려면 많은 장애 요인을 고려하여 다양한 각도에서 접근해야 하므로 다양한 활용 사례가 도움이 됨
- 트러블 슈팅 작업 단계
  - 문제 정의, 자료 수집, 원인 추론, 조치 방안 작성, 조치 방안 구현으로 나눌 수 있음
  - 문제 정의 단계
    - 현상을 파악하고 원인을 찾아내기 전에 시스템의 문제를 명확히 규정하는 단계
    - '웹 서버에 접속이 불가능하다', '라우터로 Ping이 되지 않는다' 등의 현상을 파악

- 자료 수집
  - 정의된 문제의 전체적인 점검 항목과 내용을 결정하고 적합한 해결책을 선정하여 자료를 수집하는 단계
  - 문제 유형(반응 시간 등)에 맞는 해결책을 선택하여 수집하는 방법을 결정하는 것이 중요
- 원인 추론
  - 수집된 자료를 바탕으로 문제 장비나 환경 등을 추론하는 단계
  - 수집한 정보를 체계적으로 분석하여 신속하게 원인을 규명하는 것이 중요



(2) 구성 관리

- 네트워크 구성에 관한 정보를 수집하고 이러한 정보를 바탕으로 장치의 구성을 업데이트하여 최신 정보를 유지하고 보고서를 작성하는 기능을 담당
- 구성 관리의 목적은 시스템의 구성을 최적의 상태로 유지하는 것으로, 하드웨어와 소프트웨어의 구성 내역을 관리하는 기법을 사용
- 사용자의 요구와 네트워크 상황이 계속 변하기 때문에 응용프로그램의 변화와 사용자의 요구 사항을 유연하게 수용하려면 지속적으로 구성을 관리해야 함
- 모니터링
  - 성능 개선이나 장애 방지를 목적으로 CPU, 메모리, 버퍼 등의 주요 구성 요소를 지속적으로 모니터링하는 기능
  - 이 기능이 없다면 다양한 네트워크 상황을 파악할 때 설계 도면을 살펴보아야 할 것이지만 네트워크 상황이 수시로 변하기 때문에 도면만으로는 현재의 네트워크 상태를 정확하게 판단할 수 없음
  - 네트워크 관리 시스템의 구성 관리 기능을 통해 현재 네트워크의 구성을 정확하게 파악할 수 있을 뿐 아니라 현재 네트워크 장치의 회선 속도와 같은 정보도 파악할 수 있음
  - 원격으로 해당 장치를 액세스하여 인터페이스의 구성 정보를 살펴봄으로써 문제 해결에도 도움이 됨

- 변경 관리
  - 관리 시스템의 구성 관리 기능만으로 장치의 동작 상태를 변경하여 구성을 쉽게 바꿀 수 있음
  - 네트워크 장치 설정 및 변경, 가입 변경 시 구성 정보 변경, 네트워크 장치 구성 정보의 버전 관리, 네트워크 관리 체계 소프트웨어의 백업 등이 해당
- 주소 관리
  - 구성 관리의 핵심 기능 중 하나로, 모든 네트워크 장치에는 고유한 주소가 있으므로 종합적으로 관리를 수행해야 함
  - 사용자에게 부여하는 주소 체계의 관리, 사용자 호스트의 IP 주소 및 라우터 주소 관리 등이 해당

(3) 성능 관리
- 성능 관리의 목적은 성능 저하가 장애로 이어지지 않도록 방지하는 데 있음
- 통계 정보를 수집하고, 시스템 상태 이력 기록을 유지·검사하며, 시스템 성능을 측정하고, 지연 시간과 대역폭 사용률, 패킷 처리율 등을 단계별 또는 시간별로 관리
- 성능 관리 고려사항
  - 용량 활용도(Capacity Utilization)가 얼마나 높은가?
  - 과도한 흐름(Excessive Traffic)이 있는가?
  - 처리량(Throughput)이 줄어들었는가?
  - 어디서 병목(Bottleneck)이 일어나는가?
- 성능 관리 모니터링 기능
  - 성능 측정(Performance Measurement): 실제 트래픽을 측정하는 기능으로 에이전트에 의해 수행
  - 성능 분석(Performance Analysis): 에이전트들이 측정한 통계치를 모아서 분석하는 기능으로 매니저에 의해 수행
  - 테스트 트래픽 생성(Synthetic Traffic Generation): 인위적으로 트래픽을 생성하여 성능을 측정하는데 사용

(4) 계정 관리
- 개방 시스템에서 일어나는 활동에 따라 소비하는 자원에 관한 모든 정보를 관리
- 자원 사용량과 관련이 있는 네트워크 데이터를 수집
- 네트워크 자원에 접근하는 사용자의 권한을 관리하고, 네트워크 자원에 접근하려는 사용자가 정당한 사용자인지 인증하며, 인증되지 않은 사용자라면 네트워크 자원에의 접근을 차단하는 기능 수행
- 네트워크 자원의 사용에 따라 사용료를 부과하고 네트워크 관리 대상 요소의 사용에 따른 비용을 산출

(5) 보안 관리
- 보안 관리는 위험을 방지하여 네트워크 관리가 올바로 이루어지게 하고, 네트워크 자원과 정보를 보호하며, 패스워드와 인증, 접근 제어 정보를 관리 및 분배하는 역할 수행
- 보안관리 기능
  - 데이터를 암호화하는 기능
  - 암호화에 필요한 키를 생성하고 분산시켜 관리하는 기능 사용자를 인증할 수 있는 기능
  - 네트워크 자원에 대한 접근 권한을 제어하는 기능
  - 보안정보와 감사정보(Audit Records or Security Logs)를 모아 저장하고 점검하는 기능

● 네트워크 관리 기능과 용도

구분	장애 관리	구성 관리	성능 관리	계정 관리	보안 관리
신속한 장애 회복	○	○			
사용자 정보 보호		○			○
성능 약화 방지	○	○	○		
설비 최적 가동		○	○		
운영 및 보수 비용 절감	○	○	○		○
공정한 비용 부담				○	

3. 네트워크 분석 도구

1) 개요

- 네트워크의 정보 수집과 분석을 자동으로 처리하는 도구
- 네트워크를 지속적으로 모니터링
- 네트워크 구성 자원의 상태를 표시
- 응답 시간, 과도한 회선 오류 등의 네트워크 문제를 분석
- 성능과 용량 관리를 위한 보고서 작성 등의 정보 제공

2) 네트워크 분석 도구의 유형

(1) 유형 1

- 네트워크의 특정 세그먼트에 접속해서 사용하는 유형
- 문제가 발생했을 때 원인을 진단하는 데 필요한 모니터링 기능으로 개발
- 이 유형에는 원격 네트워크를 모니터링하는 RMON, Expert Sniffer 등의 프로토콜 분석기가 있음
- 모든 세그먼트를 감시하려면 세그먼트마다 분석기를 설치해야 함
  → 이렇게 하면 비용이 많이 들어 전체 네트워크 분석용으로는 적합한 방식이 아님
- 네트워크에 문제가 발생했을 때 집중적으로 분석할 수 있어 문제를 해결하는 용도로는 가장 적합
- 이러한 유형에 속하는 네트워크 분석기는 네트워크 감시, 데이터 해석, 트래픽 생성 등의 기본적인 기능을 처리
- 모니터링 기능
  - 트래픽 부하 측정, 사용하는 프로토콜 확인, 오류 통계, 모니터링 결과 보고서 작성 기능 등을 제공
  - 대표적인 모니터링으로는 전송 프레임의 유형과 길이 분석을 들 수 있음
  - 모니터링은 실시간 또는 비실시간 분석을 제공
    - 실시간 모니터링 기능을 사용하면 트래픽 수준을 실시간으로 살펴볼 수 있음
    - 비실시간 모니터링 기능을 사용하면 트래픽 동향을 분석하여 문제가 발생하는 시점을 확인할 수 있음
- 해석 기능
  - 네트워크에서 전송하는 프레임을 수집한 후 프레임 헤더에 있는 정보를 이용하여 프레임의 내용을 해석
  - TCP/IP, 이더넷, IPX/SPX 등 서로 다른 유형의 프로토콜 패킷을 속성별로 해석할 수 있음

- 트래픽 생성 기능
  - 브리지나 라우터, 서버 등의 트래픽 부하를 측정하기 위해 트래픽을 생성
  - 실제 네트워크 트래픽을 정확하게 측정하기 위해 다른 유형의 프레임을 생성하거나 프레임 길이, 프레임 발생 빈도, 송수신지 주소 등을 조정할 수 있음

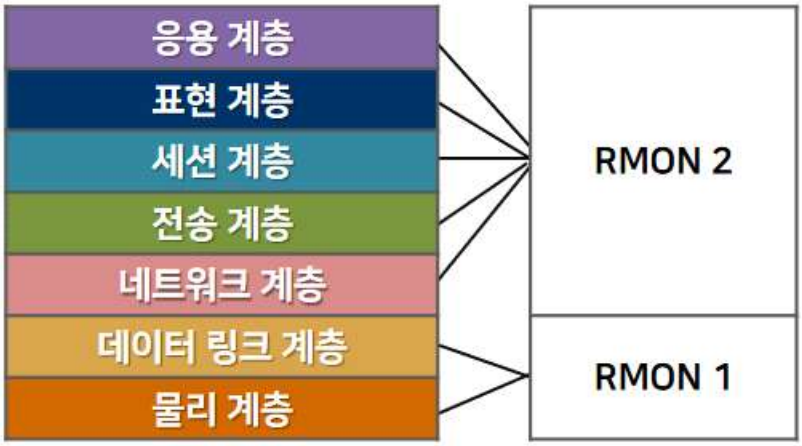
(2) 유형 2

- 이 유형의 도구는 허브, 브리지, 라우터 등 네트워크 장비에 있는 에이전트에서 데이터를 수집하여 분석하는 기능을 제공
- 유형 1보다 비교적 단순하고 비용이 저렴
- 광범위한 네트워크도 지속적으로 분석하고 경제적으로 분석 시스템을 구축할 수 있기 때문에 가장 많이 사용하는 네트워크 분석 도구
- 유형 2는 분석 정보를 제공하는 에이전트와 분석 기능을 처리하는 네트워크 분석 소프트웨어로 구성
- 에이전트와 분석 소프트웨어 간에는 주로 SNMP 프로토콜을 이용하여 정보를 교환
- 네트워크 분석 도구
  - 네트워크 분석 소프트웨어: SNMP 장치의 구성과 장애, 성능을 모니터링함
  - 시스템 관리 소프트웨어: 서버와 클라이언트 등 각종 시스템을 관리함
  - 응용프로그램 분석 소프트웨어: 응용 프로그램 차원의 트래픽 이동 경로와 특성을 파악

3) RMON

- RMON(The Remote Network Monitoring)은 SNMP의 확장 형태로, 네트워크 곳곳에 설치되어 있는 장비로부터 오가는 트래픽을 분석하고 감시
- RMON은 SNMP에 기반을 둔 RMON 매니저와 프로브 probe로 구현
- SNMP는 에이전트가 있는 장비 상태의 처리 결과를 알려주는 데 반해, RMON은 전체 네트워크의 구획에서 발생한 트래픽을 알려줌
- RMON MIB가 제공하는 정보는 통계, 히스토리, 경보, 호스트, HostTopN, 트래픽 매트릭스, 필터, 패킷 캡처, 이벤트 등
  - MIB(Management Information Base) : 망관리를 위해 사용되는 체계화된 관리 정보로 망 관리 자원 정보를 구조화시킨, 대규모 관리 정보 집합
- 단점: RMON은 한 세그먼트의 트래픽을 감시하는 용도로는 적당하지만 MAC 계층까지만 분석이 가능함
- 이에 RMON에 프로토콜별 분포 현황, 네트워크 계층인 IP, IPX, DECnet, 애플토크 등의 호스트별 트래픽 수집 기능을 추가한 RMON 2가 발표됨
- RMON 2의 등장으로 네트워크 관리자는 OSI 참조 모델 7계층을 모두 관찰할 수 있으나 에이전트의 시스템 자원이 충분하고 성능이 좋아야 하며 단독 장비를 구성해야 한다는 부담이 있음
- 따라서 스위치로 네트워크 구획을 분리하여 스위치의 각 포트에 연결된 허브에 RMON을 탑재하는 방안이 대두

- OSI 참조모델 7계층과 RMON



학습정리

1. 네트워크 관리 시스템(Network Management System) : 효율적으로 자원 사용을 극대화함과 동시에 서비스 품질의 측면에서 가용성과 신뢰성을 최상의 상태로 유지하고 응답 시간을 단축하는 시스템
2. 네트워크 모니터링 : NMS를 이용하여 네트워크 자원들의 상태를 관찰하여 분석하는 것
3. 네트워크 관리 기능 : OSI 표준에서는 효율적인 네트워크 관리를 위해 장애 관리, 구성 관리, 성능 관리, 계정 관리, 보안 관리기능을 제안
4. 네트워크 분석 도구 유형 1 : 네트워크의 특정 세그먼트에 접속해서 사용하는 유형
5. 네트워크 분석 도구 유형 2 : 광범위한 네트워크도 지속적으로 분석하고 경제적으로 분석 시스템을 구축할 수 있기 때문에 가장 많이 사용하는 네트워크 분석 도구
6. RMON(The Remote Network Monitoring) : SNMP의 확장 형태로, 네트워크 곳곳에 설치되어 있는 장비로부터 오가는 트래픽을 분석하고 감시

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제12주차 2 교시

강의주제 네트워크 관리 프로토콜

학습목표

1. 네트워크 관리 프로토콜을 설명할 수 있다.
2. 네트워크 관리 명령어를 설명할 수 있다.
3. 트러블 슈팅을 이해하고 수행할 수 있다.

학습내용

1. 네트워크 관리 프로토콜
2. 네트워크 관리 명령어
3. 트러블 슈팅

사전학습

사이트 연결 오류가 발생되었을 때 문제의 원인을 찾기 위한 방안은 무엇이라고 생각하나요?

본 학습

1. 네트워크 관리 프로토콜

1) 개요

- TCP/IP 환경의 네트워크를 처음 사용할 당시에는 주로 ICMP를 이용하여 네트워크 장비 간의 연결 상태 등을 관리
  - ICMP(Internet Control Message Protocol)
    - TCP/IP의 IP 계층에서 추가적으로 필요한 기능들을 수행하기 위한 프로토콜
    - IP 패킷을 처리할 때 발생되는 문제를 알리거나, 그와 같은 문제의 진단 등을 수행하고 IP와 하나의 쌍을 이루며 동작
- ICMP는 상대방 호스트의 동작 여부와 응답 시간 측정 등 단순한 기능만 제공하므로, 인터넷 사용자가 증가하고 네트워크의 구성이 복잡해지면서 표준화된 새로운 프로토콜의 필요성이 대두
- 1980년대 후반 SNMP가 표준 프로토콜로 등장하면서 대부분의 네트워크 관리 제품이 SNMP를 지원하기 시작
  - SNMP(Simple Network Management Protocol) : UDP/IP를 사용하여 이더넷 연결을 통해 네트워크 관리 작업을 수행하는 응용 계층 프로토콜
- 네트워크 시스템을 관리하는 프로토콜로는 SNMP, CMIP를 주로 사용
- SNMP는 구현하기 쉽고 간편하여 현재 가장 일반적인 네트워크 관리 프로토콜
- CMIP는 구현이 복잡하고 방대하여 아직 네트워크 관리의 중심에 자리 잡지 못한 실정
  - CMIPCommon Management Information Protocol) : 조직적이고 규모가 큰 망관리를 위한 프로토콜

2) SNMP(UDP 포트 : 161)

(1) SNMP 개요

- SNMP는 현재 가장 많이 사용하는 프로토콜로 구현하기 쉽고 간편한 것이 장점
- 관리 시스템과 에이전트의 분산구조를 사용하여 관리 서비스를 수행
- SNMP를 사용하려면 SNMP 에이전트와 SNMP 매니저가 필요
  - SNMP Manager : Agent에 필요한 정보를 요청하는 모듈
  - SMAP Agent : 관리 대상 시스템에 설치되어 필요한 정보를 수집하고 Manager에게 전달해주는 역할을 수행하는 모듈
- 관리해야 할 특정 정보나 자원을 '개체'라 하고, 이 개체를 모아놓은 집합체를 'MIB'라 함
- 네트워크 관리를 위한 목적으로 주로 서버나 네트워크 장비에서 SNMP를 설정한 MRGT 프로그램을 이용하여 트래픽 관리 등을 위해 사용
  - MRTG(Multiple Router Traffic Grapher) : SNMP 기반의 장비 모니터링 프로그램으로 주 용도는 네트워크 트래픽 사용량 모니터링이지만 벤더에서 제공하는 SNMP MIB값을 사용하여 다양한 정보를 수집할 수 있음
- SNMP는 OSI 7계층의 Application 계층 프로토콜이며, 메시지는 단순히 요청과 응답 형식의 프로토콜에 의해 교환되기 때문에 전송계층 프로토콜로 UDP 프로토콜을 사용
- SNMP는 가장 많이 사용하는 네트워크 시스템 관리 프로토콜이지만 IP 네트워크에만 특화되어 있음
- 방대한 양의 데이터 정보를 가져오기에는 효율이 떨어지고 보안 기능이 취약하여 이러한 문제를 해결하기 위해 등장한 프로토콜이 바로 SNMP v2

- SNMP v2에서는 분산 관리의 도입과 한 번의 요청으로 여러 데이터 값을 읽어오는 것이 가능하고, SNMP v1의 가장 큰 문제였던 보안 기능도 향상

(2) SNMP 동작방식

- 관리 시스템(Manager)은 162/udp 포트를 이용하고 Agent는 161/udp 포트를 이용
  - Manager : Agent에 필요한 정보를 요청하는 역할
  - Agent : Agent가 설치된 시스템의 정보나 네트워크 정보 등을 수집하여 MIB 형태로 보관, Manager에 전달해주는 역할 수행
- 관리 시스템과 대행자간에 통신하기 위해서는 최소 다음 3가지 사항이 일치되어야 함
  - SNMP 버전 : Manager와 Agent간 SNMP 버전이 일치해야 함
  - Community String : 상호간에 설정한 Community String이 일치해야 함
  - PDU(Protocol Data Unit) : 통신하기 위한 메시지 유형
- PDU 타입
  - Get Request : 관리시스템이 에이전트로 원하는 객체의 특정 정보를 요청
  - Get Next Request : 관리시스템이 에이전트로 이미 요청한 정보의 다음 정보를 요청
  - Set Request : 관리 시스템이 에이전트로 특정한 값을 설정하기 위해 사용
  - Get Response : 에이전트가 관리시스템에 해당 변수 값을 전송
  - Trap : 에이전트가 관리 시스템에 어떤 정보를 비동기적으로 알리기 위해 사용하며 notify라고 하며, 콜백 함수와 같은 역할
- SNMP 데이터 수집 방식
  - Polling 방식 : Manager가 Agent에게 정보를 요청하면 응답해주는 방식으로 Agent가 161/udp 포트를 사용
  - Event Reporting 방식 : Agent가 이벤트 발생 시 이를 Manager에게 알리는 방식으로 Manager가 162/udp 포트를 사용

3) CMIP(TCP)

- CMIS는 네트워크를 관리하기 위해 각 네트워크 구성 요소로 제공하는 일반적인 서비스를 정의
  - CMIS(Common Management Information Service) : CMIP 환경하에서 망관리 정보를 공유하기 위한 방법을 제시하고 OSI 시스템상의 망관리를 위하여 제공하는 서비스들을 정의함
- CMIP는 이러한 CMIS 서비스를 구현하는 프로토콜
- 시스템 관리를 수행하는 응용 프로그램을 'CMISE(Common Management Information Service Element)'라고 함
- CMIP는 인증, 접근 제어, 보안 로그 등 네트워크 관리 정보에 보안 체계를 갖춘 프로토콜
- 이러한 특성 때문에 SNMP를 채택한 관리 시스템보다 안정성이 뛰어나다고 할 수 있음
- 관리대상에서 장애가 발생하면 그 내역을 CMIP의 서비스 중 하나인 이벤트 리포트 기능을 이용하여 전송하면 되므로 CMIP를 채택하면 SNMP보다 더 능률적으로 네트워크를 관리할 수 있음
- CMIP를 사용하면 관리 정보가 손실되지 않음
- CMIP는 SNMP보다 기능이 많고 OSI 참조 모델 7계층의 통신 프로토콜에서 동작하기 때문에 프로세스 자체가 무거울 뿐만 아니라 시스템 자원도 많이 소모
- 비용이 많이 들고 구현하기도 어렵기 때문에 아직까지는 SNMP를 대체하지 못하고 있는 실정

2. 네트워크 관리 명령어

1) 개요

- 네트워크 관리 명령어를 사용하여 네트워크 상태를 모니터링하고 네트워크 문제를 진단할 수 있음
- [시작] 메뉴의 검색 화면에서 'cmd'를 입력하면 명령 프롬프트 창이 나타나며 이곳에 네트워크 명령어 입력 가능

2) 명령어

(1) nbtstat

- nbtstat - A
  - 컴퓨터를 사용하다 보면 가끔 IP 주소가 충돌했다는 경고 메시지가 나타남
  - DHCP를 사용하여 IP 주소를 관리하는 곳(가정)에서는 잘 발생하지 않음
  - 하지만, 네트워크 관리자가 수동으로 고정 IP 주소를 설정하는 네트워크 환경(학교)에서는 하나의 IP 주소를 컴퓨터 두 대에 입력하면 충돌 메시지가 발생
  - 이럴 때 nbtstat –A는 충돌하는 컴퓨터를 찾아줌
  - IP 주소 충돌 메시지가 나타나면 컴퓨터를 종료한 후 다른 컴퓨터에서 nbtstat 명령어로 중복된 IP 주소를 사용하는 컴퓨터의 이름을 확인하고(nbtstat -A 중복된 IP 주소) 충돌하는 컴퓨터의 IP 주소를 바꾸면 됨
  - nbtstat -n 명령어를 입력하면 NetBIOS가 사용하는 통계 및 이름 정보를 확인할 수 있음
  - **nbtstat –a 명령어 예시**

```
C:₩Users₩jack5>nbtstat -a
      192.168.101.71
Bluetooth 네트워크 연결 :
노드 IpAddress: [0.0.0.0] 범위 ID: []
        호스트를 찾을 수 없습니다.
Wi-Fi:
노드 IpAddress: [192.168.101.71]
      범위 ID: []
        호스트를 찾을 수 없습니다.
로컬 영역 연결 * 1:
노드 IpAddress: [0.0.0.0] 범위 ID: []
        호스트를 찾을 수 없습니다.
```

  - **nbtstat –n 명령어 예시**

```
C:₩Users₩jack5>nbtstat -n
Bluetooth 네트워크 연결 :
노드 IpAddress: [0.0.0.0] 범위 ID: []
      캐시에 이름 없음
Wi-Fi:
노드 IpAddress: [192.168.101.71]
      범위 ID: []
      NetBIOS 로컬 이름 테이블
      이름                유형     상태
---------------------------------------
LAPTOP-OKSHN32P<20>  UNIQUE   등록됨
LAPTOP-OKSHN32P<20>  UNIQUE   등록됨
WORKGROUP<00>        GROUP    등록됨

로컬 영역 연결 * 1:
노드 IpAddress: [0.0.0.0] 범위 ID: []
      캐시에 이름 없음
```

(2) netstat

- netstat
  - 시스템에서 TCP 전송 프로토콜의 상태를 보여주는 명령어
  - 네트워크에서 현재 열려 있는 포트를 모두 확인할 수 있음

명령 프롬프트 - netstat

```
C:₩Users₩jack5>netstat

활성 연결

  프로토콜  로컬 주소          외부 주소              상태
  TCP    127.0.0.1:49669        LAPTOP-OKSHN32P:49670  ESTABLISHED
  TCP    127.0.0.1:49670        LAPTOP-OKSHN32P:49669  ESTABLISHED
  TCP    127.0.0.1:49671        LAPTOP-OKSHN32P:49672  ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-OKSHN32P:49671  ESTABLISHED
  TCP    127.0.0.1:53710        LAPTOP-OKSHN32P:64032  ESTABLISHED
  TCP    127.0.0.1:64032        LAPTOP-OKSHN32P:53710  ESTABLISHED
  TCP    192.168.101.71:49409   20.198.119.143:https   ESTABLISHED
```

- netstat -p
  - 특정 전송 프로토콜의 상태를 보여주는 명령어

```
C:₩Users₩jack5>netstat -p tcp

활성 연결

  프로토콜  로컬 주소          외부 주소              상태
  TCP    127.0.0.1:49669        LAPTOP-OKSHN32P:49670  ESTABLISHED
  TCP    127.0.0.1:49670        LAPTOP-OKSHN32P:49669  ESTABLISHED
  TCP    127.0.0.1:49671        LAPTOP-OKSHN32P:49672  ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-OKSHN32P:49671  ESTABLISHED
  TCP    127.0.0.1:53710        LAPTOP-OKSHN32P:64032  ESTABLISHED
  TCP    127.0.0.1:64032        LAPTOP-OKSHN32P:53710  ESTABLISHED
  TCP    192.168.101.71:49409   20.198.119.143:https   ESTABLISHED
  TCP    192.168.101.71:50163   27.0.238.140:https     ESTABLISHED
  TCP    192.168.101.71:50455   a23-200-152-10:https   CLOSE_WAIT
  TCP    192.168.101.71:53493   121.53.203.203:https   ESTABLISHED
  TCP    192.168.101.71:53718   211.115.106.206:http   CLOSE_WAIT
```

- netstat - an
  - 컴퓨터에 트로이 목마 등 백도어 해킹 프로그램 등이 설치되어 정보를 빼내지는 않는지 확인할 수 있음
  - -an 옵션은 주소와 포트 번호를 숫자 형식으로 표시
  - netstat -an은 현재 서비스를 대기하고 있는 'LISTENING 정보'와 TCP 통신을 하는 'ACTIVE 서비스'의 연결 상태를 도메인 정보 없이 보여줌
  - ESTABLISHED는 다른 컴퓨터와 연결된 상태를, CLOSE_WAIT는 연결이 종료된 상태를, TIME_WAIT는 연결은 종료되었지만 소켓은 열어놓은 상태를 나타냄
  - 컴퓨터의 사용 포트를 확인하여 불필요한 포트가 열려 있다면 외부에서 해킹 중인지 의심해보아야 함

명령 프롬프트

```
C:₩Users₩jack5>netstat -an

활성 연결

  프로토콜  로컬 주소          외부 주소          상태
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:808            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9001           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:14430          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:14440          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:21300          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:42235          0.0.0.0:0              LISTENING
```

- netstat - e 5
  - 윈도우의 NetBIOS는 TCP 포트 139를 이용하여 다양한 정보를 넘겨주는 API가 있어 보안에 취약함
    → 인증되지 않은 사용자가 ID나 패스워드 인증 없이도 원격 컴퓨터의 정보를 가져갈 수 있음
  - 악성 코드, 케이블 불량, 허브의 포트 불량 등으로 송수신 속도가 느릴 때 5초 주기로 이더넷 인터페이스의 데이터 송수신을 계속 표시
    → 악성 코드나 기타 바이러스 때문에 트래픽이 증가하지는 않는지 확인할 수 있음

명령 프롬프트 - netstat -e 5

```
C:₩Users₩jack5>netstat -e 5
인터페이스 통계

                           받음                보냄

바이트                   227608784          112779376
유니캐스트 패킷            3268480             619000
비유니캐스트 패킷            99032               7688
버림                             0                  0
오류                             0                  0
알 수 없는 프로토콜              0
인터페이스 통계
```

- netstat -r
  - 로컬 호스트의 라우팅 테이블을 보여주는 명령어
  - 라우팅 테이블을 통해 호스트의 알려진 모든 경로 상태를 확인

```
명령 프롬프트
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:₩Users₩jack5>netstat -r
===========================================================================
인터페이스 목록
  5...38 68 93 ce f6 72 ......Microsoft Wi-Fi Direct Virtual Adapter
  8...3a 68 93 ce f6 71 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 17...38 68 93 ce f6 71 ......Intel(R) Wi-Fi 6 AX201 160MHz
  7...38 68 93 ce f6 75 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 경로 테이블
===========================================================================
활성 경로:
네트워크 대상       네트워크 마스크     게이트웨이       인터페이스    메트릭
          0.0.0.0          0.0.0.0    192.168.101.1   192.168.101.71     35
        127.0.0.0        255.0.0.0            연결됨         127.0.0.1    331
        127.0.0.1  255.255.255.255            연결됨         127.0.0.1    331
  127.255.255.255  255.255.255.255            연결됨         127.0.0.1    331
```

- netstat -s
  - IP, ICMP, TCP, UDP에 대한 프로토콜 통계를 보여주는 명령어
  - 통계를 이용하여 프로토콜에 문제가 있는 영역을 확인

```
명령 프롬프트

C:₩Users₩jack5>netstat -s

IPv4 통계

  받은 패킷                          = 114612
  받은 헤더 오류                     = 0
  받은 주소 오류                     = 0
  전달된 데이터그램                    = 0
  알 수 없는 프로토콜 받음           = 0
  받은 패킷 버림                     = 10444
  받은 패킷 배달됨                     = 118996
  출력 요청                          = 83400
  라우팅 버림                        = 0
  버린 출력 패킷                   = 0
  무경로 출력 패킷                   = 3
  리어셈블리 필요                    = 0
  리어셈블리 성공                    = 0
  리어셈블리 실패                    = 0
  성공적으로 조각화된 데이터그램         = 0
  조각화에 실패한 데이터그램             = 0
  만든 조각                          = 0
```

- netstat -e
  - 컴퓨터의 송수신 패킷 관련 정보를 확인

```
명령 프롬프트

C:₩Users₩jack5>netstat -e
인터페이스 통계

                           받음                보냄

바이트                    228556840          113525712
유니캐스트 패킷             3270112             620408
비유니캐스트 패킷            100880               7784
버림                            0                  0
오류                            0                  0
알 수 없는 프로토콜             0
```

- netstat -f
  - 특정 주소 그룹의 패킷 전송과 관련된 통계를 확인

```
명령 프롬프트 - netstat -f
C:₩Users₩jack5>netstat -f

활성 연결

  프로토콜  로컬 주소          외부 주소              상태
  TCP    127.0.0.1:49669     LAPTOP-0KSHN32P:49670  ESTABLISHED
  TCP    127.0.0.1:49670     LAPTOP-0KSHN32P:49669  ESTABLISHED
  TCP    127.0.0.1:49671     LAPTOP-0KSHN32P:49672  ESTABLISHED
  TCP    127.0.0.1:49672     LAPTOP-0KSHN32P:49671  ESTABLISHED
  TCP    127.0.0.1:53710     LAPTOP-0KSHN32P:64032  ESTABLISHED
  TCP    127.0.0.1:64032     LAPTOP-0KSHN32P:53710  ESTABLISHED
```

(3) ping

- ping 사이트 주소
  - 원격의 호스트 컴퓨터, 서버 장비, 네트워크 장비와 통신이 잘되고 있는지 확인하는 명령어
  - ping을 실행하면 ICMP 프로토콜에서 지정한 호스트 컴퓨터로 데이터그램을 전송하여 응답을 요청
  - ICMP는 TCP/IP 네트워크에서 오류 처리를 담당하는 프로토콜이며, ping 명령어를 사용하여 원격의 호스트 컴퓨터에 IP가 연결되어 있는지 확인할 수 있음
  - 집에서 작업하다 사무실의 컴퓨터를 끄고 왔는지 확인하고 싶다면 ping 명령어를 이용
    - 사무실의 컴퓨터가 꺼져 있다면 ' Request timed out(요청 시간이 만료되었습니다.)'이라는 메시지가 출력
    - 누군가가 컴퓨터로 인터넷을 사용하고 있다면 'Reply from 163.152.19.114: bytes=32times‹10ms TTL=128'이라는 메시지가 출력
    - 'Request timed out' 메시지는 상대방의 컴퓨터가 꺼져 있거나, IP 주소가 잘못되었거나, 케이블 연결이 잘못되었거나, 인터넷에 연결되지 않았음을 나타냄

```
명령 프롬프트

C:₩Users₩jack5>ping 192.168.101.71

Ping 192.168.101.71 32바이트 데이터 사용:
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128

192.168.101.71에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

- ping - n count 사이트 주소
  - count 옵션은 보낼 에코 요청의 수
  - count에 3을 입력하면 사이트에 에코 요청을 세 번 수행

```
C:₩Users₩jack5>ping -n 3 192.168.101.71

Ping 192.168.101.71 32바이트 데이터 사용:
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128

192.168.101.71에 대한 Ping 통계:
    패킷: 보냄 = 3, 받음 = 3, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

- ping - t 사이트 주소
  - -t 옵션은 중지할 때까지 지정한 호스트에 ping을 실행(중지하려면 ^c 를 클릭)

```
명령 프롬프트

C:₩Users₩jack5>ping -t 192.168.101.71

Ping 192.168.101.71 32바이트 데이터 사용:
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128

192.168.101.71에 대한 Ping 통계:
    패킷: 보냄 = 6, 받음 = 6, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms
Control-C
^C
```

- ping - f - l size 사이트 주소
  - -f 옵션은 패킷 조각화하지 않고 플래그를 설정(라인 테스트용)
  - -size 옵션은 전송할 버퍼 크기를 의미

```
C:₩Users₩jack5>ping -f -l 64 192.168.101.71

Ping 192.168.101.71 64바이트 데이터 사용:
192.168.101.71의 응답: 바이트=64 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=64 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=64 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=64 시간<1ms TTL=128

192.168.101.71에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

(4) route

- 서버나 방화벽 장비에 LAN 카드를 여러 개 설치할 때 route 명령어를 이용하여 패킷이 전달되는 경로를 확인하거나 지정할 수 있으며, route print는 라우팅 테이블을 보여줌
- 라우팅 테이블은 라우터나 다른 네트워크 장치에 저장된 데이터베이스이며 네트워크의 특정 수신지까지 경로를 계속 저장하기 위해 사용

명령 프롬프트

```
C:₩Users₩jack5>route print
===========================================================================
인터페이스 목록
  5...38 68 93 ce f6 72 ......Microsoft Wi-Fi Direct Virtual Adapter
  8...3a 68 93 ce f6 71 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 17...38 68 93 ce f6 71 ......Intel(R) Wi-Fi 6 AX201 160MHz
  7...38 68 93 ce f6 75 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 경로 테이블
===========================================================================
활성 경로:
네트워크 대상       네트워크 마스크     게이트웨이       인터페이스    메트릭
          0.0.0.0          0.0.0.0    192.168.101.1   192.168.101.71     35
        127.0.0.0        255.0.0.0            연결됨          127.0.0.1    331
        127.0.0.1  255.255.255.255            연결됨          127.0.0.1    331
  127.255.255.255  255.255.255.255            연결됨          127.0.0.1    331
    192.168.101.0    255.255.255.0            연결됨     192.168.101.71    291
   192.168.101.71  255.255.255.255            연결됨     192.168.101.71    291
  192.168.101.255  255.255.255.255            연결됨     192.168.101.71    291
        224.0.0.0        240.0.0.0            연결됨          127.0.0.1    331
        224.0.0.0        240.0.0.0            연결됨     192.168.101.71    291
  255.255.255.255  255.255.255.255            연결됨          127.0.0.1    331
  255.255.255.255  255.255.255.255            연결됨     192.168.101.71    291
===========================================================================
영구 경로:
  없음
```

(5) tracert 사이트 주소

- 인터넷은 원격의 컴퓨터 또는 서버와 직접 연결되어 있지 않고 라우터 등의 네트워크 장비를 거쳐 접속

- tracert 명령어
  - 최종 수신지 컴퓨터에 도달하기까지 중간에 거치는 라우터 여러 개의 경로 및 응답 속도를 보여줌
  - 갑자기 특정 웹 사이트와의 접속이 느릴 때 tracert 명령어로 내부 네트워크나 회선 구간 등을 확인할 수 있음
  - 전용 회선 관리나 장애 복구에도 이 명령어를 많이 사용
- tracert 뒤에 수신지 서버의 이름이나 IP 주소를 입력하면 1행씩 중계 라우터의 수, 즉 1부터 시작하는 hop 수, 지연 시간, IP 주소 또는 이름순으로 수신지 서버까지의 경로를 보여줌
- 통신 오류가 발생했을 때는 지연 시간이 *로 나타남

```
명령 프롬프트

C:₩Users₩jack5>tracert www.google.com

최대 30홉 이상의
www.google.com [142.250.207.100](으)로 가는 경로 추적:

  1     *        *        *     요청 시간이 만료되었습니다.
  2   120 ms     7 ms     6 ms  14.42.53.254
  3     5 ms     4 ms     4 ms  121.163.119.33
  4     3 ms     3 ms     2 ms  112.188.85.9
  5     6 ms     4 ms    10 ms  112.188.78.69
  6     *        *        *     요청 시간이 만료되었습니다.
  7    12 ms    13 ms    13 ms  112.174.90.2
  8    12 ms    21 ms    11 ms  112.174.84.70
  9    36 ms    44 ms    39 ms  72.14.210.6
 10    35 ms    35 ms    35 ms  142.251.61.113
 11    35 ms    35 ms    35 ms  108.170.242.177
 12    35 ms    34 ms    58 ms  209.85.246.83
 13    37 ms    38 ms    39 ms  142.250.229.250
 14    37 ms    37 ms    39 ms  108.170.243.65
 15    36 ms    39 ms    36 ms  142.251.70.23
 16    37 ms    37 ms    37 ms  kix06s11-in-f4.1e100.net [142.250.207.100]

추적을 완료했습니다.
```

(6) arp - a, arp - s, arp – d

- ARP에서 사용하는 인터넷 IP 주소에서 물리 주소로 변환된 값을 확인하고 수정(관리자 권한)할 수 있음
- 관리자 권한으로 명령 프롬프트를 사용하려면 [시작] 메뉴의 [명령 프롬프트]에 마우스 커서를 놓고 오른쪽 버튼을 클릭하여 [관리자 권한으로 실행]을 선택

```
명령 프롬프트

C:₩Users₩jack5>arp -a

인터페이스: 192.168.101.71 --- 0x11
  인터넷 주소           물리적 주소           유형
  192.168.101.1         00-0a-de-1a-b7-20     동적
  192.168.101.255       ff-ff-ff-ff-ff-ff     정적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.251           01-00-5e-00-00-fb     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
```

- ARP 표에 새로운 ARP 항목 추가
  - 항목 추가: arp -s 163.152.19.114 00-aa-00-62-c6-09
  - ARP 표 표시: arp –a
- ARP 표에서 ARP 항목 삭제
  - 항목 삭제: arp –d 163.152.19.114
- 사무실에 있는 한 컴퓨터가 ARP 스푸핑(트로이 목마) 등 악성 코드에 감염되면
  - 이 컴퓨터는 사무실에 있는 모든 컴퓨터의 ARP 값을 변조하며 악성 코드에 감염된 컴퓨터 때문에 ARP 값이 변조되어 네트워크가 되지 않는 컴퓨터는 ARP 값을 초기화하여 해결

→ 명령 프롬프트 창에 'arp -d'를 입력하면 ARP 표의 정보가 초기화

3. 트러블 슈팅

1) 개요

- 트러블 슈팅과 계층의 관계
  - 트러블 슈팅을 하려면 층별로 장애의 원인을 조사하여 문제가 발생한 곳을 찾아내고 장애를 분리하는 것이 중요
  - 트러블 슈팅은 통신 매체부터 시작하여 하위 계층에서 상위 계층으로 진행하는 것이 좋음
  - 장애를 분리할 때는 상위 계층에서 하위 계층 순으로 분리하고, 동일 계층이라면 가까운 곳에서 먼 곳 순으로 분리

계층	주요 프로토콜	트러블 원인
응용 계층	HTTP	소프트웨어
전송 계층	TCP	운영체제(소켓)
네트워크 계층	IP	운영체제(소켓)
네트워크 접속 계층	EthernetII	하드웨어
통신 매체		케이블

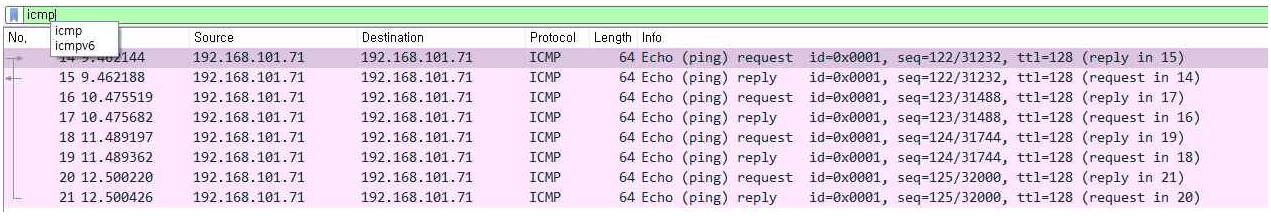
2) Ping 테스트 패킷 캡처

- Ping 테스트를 실행하기 전에 먼저 패킷 캡처를 시작
- 패킷 캡처가 진행되면 Ping 테스트를 실행하여 결과를 확인

```
C:₩Users₩jack5>ping 192.168.101.71

Ping 192.168.101.71 32바이트 데이터 사용:
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128
192.168.101.71의 응답: 바이트=32 시간<1ms TTL=128

192.168.101.71에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms
```

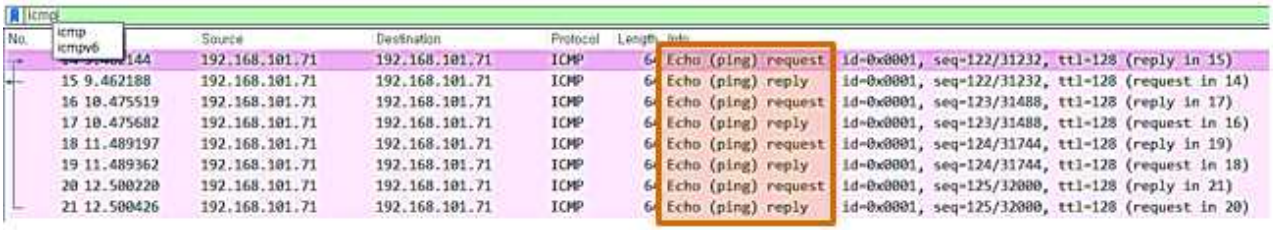
12 3.511621	fe80::d411:5467:dc6…	ff02::1:3	LLMNR	85	Standard query 0xbee6 ANY LAPTOP-0KSHN32P
13 3.511795	192.168.101.71	224.0.0.252	LLMNR	65	Standard query 0xbee6 ANY LAPTOP-0KSHN32P
14 9.462144	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) request id=0x0001, seq=122/31232, ttl=128 (reply in 15)
15 9.462188	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) reply id=0x0001, seq=122/31232, ttl=128 (request in 14)
16 10.475519	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) request id=0x0001, seq=123/31488, ttl=128 (reply in 17)
17 10.475682	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) reply id=0x0001, seq=123/31488, ttl=128 (request in 16)
18 11.489197	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) request id=0x0001, seq=124/31744, ttl=128 (reply in 19)
19 11.489362	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) reply id=0x0001, seq=124/31744, ttl=128 (request in 18)
20 12.500220	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) request id=0x0001, seq=125/32000, ttl=128 (reply in 21)
21 12.500426	192.168.101.71	192.168.101.71	ICMP	64	Echo (ping) reply id=0x0001, seq=125/32000, ttl=128 (request in 20)
22 13.142498	127.0.0.1	127.0.0.1	TLSv1.2	222	Application Data
23 13.142548	127.0.0.1	127.0.0.1	TCP	44	64032 → 53829 [ACK] Seq=241 Ack=357 Win=8371 Len=0

- 필터 표시 기능을 사용하여 Ping에 이용되는 ICMP 패킷만 필터링
  - ICMP 패킷 중에서 Echo (ping) request로 표시된 것은 ICMP 에코 요청 패킷
  - Echo (ping) reply로 표시된 것은 ping 에코 응답 패킷

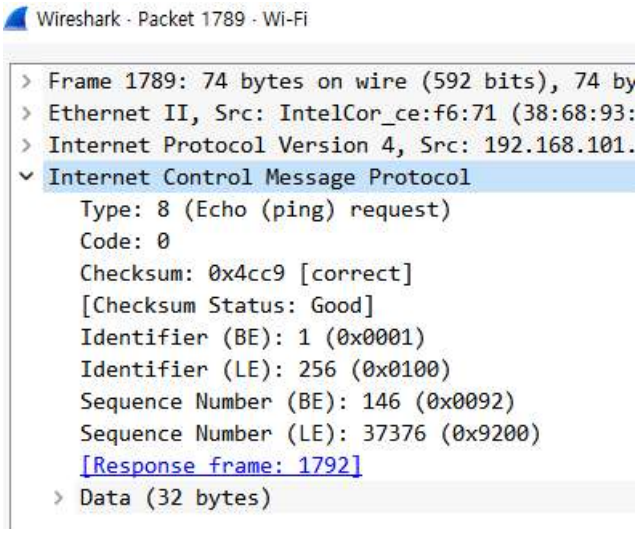


3) ICMP 덤프 분석

- ICMP는 IP 접속 테스트를 위한 프로토콜
- 에코 요청과 에코 응답 등의 메시지 종류가 정의되어 있는 ICMP는 네트워크 상태를 확인하는 데 사용
- Echo (ping) request, Echo (ping) reply로 표시된 패킷 2개 덤프 분석



- Echo (ping) request 패킷



- Type: ICMP 패킷의 종류, 에코 요청이므로 8로 지정
- Code: 회신 에코 테스트이므로 0으로 지정, Ping은 에코 요청과 에코 응답 패킷을 송수신함으로써 접속을 확인
- Checksum: ICMP 메시지가 도중에 변형되지 않도록 데이터의 내용을 검사하기 위해 사용
- Identifier: ICMP 메시지가 여러 개 있을 때 각각을 구별하기 위한 필드
- Sequence number: 비트열의 상위부터 하위 방향으로 오른쪽 정렬하여 비트를 나열해 가는 빅엔디언(BE)과 하위부터 상위 방향으로 왼쪽 정렬하여 비트를 나열해가는 리틀엔디언(LE)으로 표시
- Request frame: ICMP 에코 요청의 패킷 번호로의 링크를 연결
- Response time: Ping 패킷의 왕복 지연 시간(RTT)
- Data: Ping에서 사용하는 메시지의 초기 크기는 윈도우에서는 32바이트, 유닉스에서는 64바이트인 경우가 많음

학습정리

1. 네트워크 관리 프로토콜 : TCP/IP 환경의 네트워크를 처음 사용할 당시에는 주로 ICMP를 이용하여 네트워크 장비 간의 연결 상태 등을 관리
2. SNMP(Simple Network Management Protocol) : UDP/IP를 사용하여 이더넷 연결을 통해 네트워크 관리 작업을 수행하는 응용 계층 프로토콜
3. CMIP(TCP) : CMIS는 네트워크를 관리하기 위해 각 네트워크 구성 요소로 제공하는 일반적인 서비스를 정의하며 CMIP는 이러한 CMIS 서비스를 구현하는 프로토콜
4. 트러블 슈팅 : 트러블 슈팅을 하려면 층별로 장애의 원인을 조사하여 문제가 발생한 곳을 찾아내고 장애를 분리하는 것이 중요

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제13주차 1교시

강의주제 네트워크 보안의 이해

학습목표

1. 네트워크 보안을 정의할 수 있다.
2. 크래커와 불법 공격을 설명할 수 있다.
3. 악성 프로그램을 설명할 수 있다.
4. 네트워크 보안 기법을 설명할 수 있다.

학습내용

1. 네트워크 보안의 개요
2. 크래커와 불법 공격
3. 악성 프로그램
4. 네트워크 보안 기법

사전학습

네트워크 보안을 강화하기 위해 가장 중요한 요소는 무엇이라고 생각하나요?

본 학습

1. 네트워크 보안의 개요

1) 개요

- 보안은 크게 컴퓨터 보안과 네트워크 보안으로 구분
  - 컴퓨터 보안 : 컴퓨터 자체의 데이터를 보호하는 것
  - 네트워크 보안 : 컴퓨터 간에 데이터를 안전하게 전송하는 것
- 해킹 : 정보 시스템이나 정보통신 시스템에 허가받지 않고 침투하는 행위
- 방화벽 : 인터넷과 내부 네트워크 간에 일종의 세관 역할을 수행
- 외부 네트워크에서는 네트워크 전면에 있는 방화벽만 보이고, 그 뒤에 놓인 내부 네트워크는 보이지 않음
  ⇒ 따라서 해커가 침입하더라도 갈 수 있는 한계는 방화벽까지며, 그 뒤의 내부 네트워크와는 격리됨
- 보통 방화벽 자체에는 중요한 정보가 없는데, 외부의 접근을 차단하여 해킹 위험을 방지하는 것임
- 보안 정책 : 보안 수준을 결정하는 것
  - 4차 산업혁명 시대에 보안은 중요한 요소이며 기술이 발전해가는 만큼 해킹기술도 발전하고 있으며, 이에 따라 보안 기술도 발전할 수밖에 없음

2) 보안의 종류

- 네트워크 보안
  - 하드웨어와 소프트웨어를 모두 사용해 코어 네트워크의 물리적 요소 및 가상 요소에서 네트워크 활용성과 데이터 무결성을 보호
  - 효율성을 위해 네트워크 보안은 사용자, 디바이스 및 데이터의 네트워크 액세스를 관리
  - 위협을 감지하고 결정적으로 분석한 후 네트워크에 액세스하거나 확산하는 것을 완화, 또는 방지
- 애플리케이션 보안
  - 'AppSec'이라고도 함
  - 데이터 또는 코드가 오용, 도난 또는 피해를 당하지 않도록 앱 수준에서 적용되는 보안 조치의 모음
  - 애플리케이션 개발, 설계 및 구축 과정에서 보안 문제를 해결하고 공격으로 이어질 수 있는 보안 취약성을 방지하는 데 사용되는 포괄적인 접근 방식
  - 종종 위험과 취약성을 최소화하기 위한 보안 소프트웨어와 하드웨어 기기가 혼합되어 있음
- 시스템 보안
  - 네트워크에 연결된 시스템의 운영체제(Operating System), 응용 프로그램, 서버 등의 취약점을 이용해 해커들이 침입해서 컴퓨터 시스템을 이용하는 것을 방지하는 것

3) 네트워크 보안의 요구사항

- 기밀성 : 인가된 자만이 정보에 접근
- 무결성 : 불법 접근에 의해 정보가 변경되지 않음
- 가용성 : 필요시 언제든 자원 사용
- 인증 : 정당한 사용자임을 확인
- 부인 방지 : 송수신 사실 부인 막기
- 책임 추적성 : 보안사고 발생 시 책임 소재와 방법 파악
- 접근 통제 : 화이트리스트/블랙리스트

4) 보안의 3가지 방법

기술적 보안	▪ 식별과 인증 ▪ 접근 통제 ▪ 감시 추적
물리적 보안	▪ 물리적 접근 차단 ▪ 위험 환경 요소 제거 ▪ 화재 및 수해 예방
관리적 보안	▪ 분류와 소유권 관리 ▪ 요원 관리, 보안사고 관리 ▪ 조직과 자원, 보안 행정 절차 통제

2. 크래커와 불법 공격

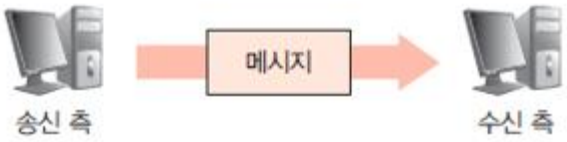
1) 개요

- 크래커(Cracker)
  - 불법적이고 악의적인 목적을 가진 해킹을 크래킹(Cracking)이라 부르며 크래킹하는 사람을 크래커라고 부름
  - 크래커 : 다른 사람의 컴퓨터 시스템에 무단으로 침입해 정보를 훔치거나 프로그램을 훼손하는 불법 행위를 하는 사람
  - 행하는 불법 공격의 유형 : 방해, 가로채기, 변조, 위조 등
- 화이트 햇(White-Hat)
  - 보통 화이트 해커로 부름
  - 선의의 목적을 가지고 해킹을 하는 사람들이며 보안전문가로도 불림
  - 화이트 햇은 기업에 고용되어 시스템의 취약점을 찾아내기 위해 해킹을 시도하고 취약점이 발견되면 이에 대한 대응 전략이나 방안을 제시하기도 함
- 블랙 햇(Black-Hat)
  - 보통 블랙 해커로 부름
  - 이 부류의 해커는 악의적인 목적을 가지고 해킹을 하는 사람들, 크래커들을 말함
  - 이들은 기업의 정보나 개인의 정보를 탈취하기 위해 시스템에 침입하고, 악성코드를 유포하여 시스템을 파괴하고, 상용 소프트웨어를 변조하여 대중에 유포하는 등의 불법적인 행위를 수행
- 그레이 햇(Gray-Hat)
  - 보통 그레이 해커로 부름
  - 이 부류의 해커는 음지에서 활동하는 화이트 해커
  - 그레이 햇은 선의의 목적을 가지고 허가 없이 타인의 시스템에 침입
  - 시스템에 침입한 후에는 해악을 끼치는 행위를 하지 않고, 오히려 보안 취약점을 고쳐주고 나가기도 함
  - 그레이 햇은 시스템에 침입한 흔적을 지우므로 시스템에 침입했는지 안했는지 잘 모르는 경우가 대부분임
- 스크립트 키디(Script Kiddie)
  - 줄여서 스키디(Skiddie)라고 부름
  - 스키디는 특별한 해킹기술을 가지고 있지 않으며 해커들이 만들고 공유한 해킹 도구를 이용하여 타인의 시스템에 해악을 끼치는 사람들

- 스키디는 해커도 크래커도 아니며, 악의적인 프로그램을 활용하여 불법적인 행위를 저지르는 사람들을 의미함

2) 불법 공격의 유형

- 정상적인 전송상태



- 전송 차단 : 송신 측과 수신 측 사이에 있는 제삼자가 데이터를 전송할 수 없다는 메시지를 만들어 송신 측에 전송하는 것

- 가로채기 : 송신 측과 수신 측이 데이터를 주고받는 사이에 제삼자(공격자)가 도청하는 것

- 변조
  - 송신 측이 수신 측으로 전송할 데이터를 제삼자가 가로채서 데이터의 일부 또는 전부를 변경하여 잘못된 데이터를 수신 측에 전송하는 것
  - 수신 측은 송신 측이 잘못된 데이터를 전송한 것으로 오인하게 됨

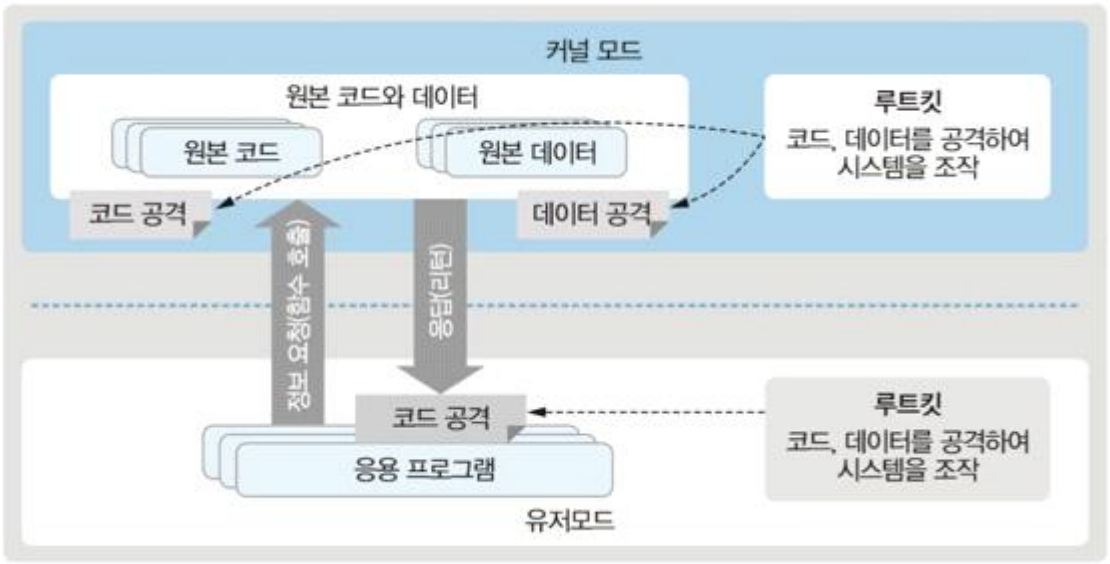
- 위조
  - 제삼자가 메시지를 위조하여 송신 측이 전송한 것처럼 수신 측으로 전송하는 것
  - 이때 변조와 달리 송신 측이 전송하지 않은 메시지를 수신 측으로 전송하는 문제가 발생함

3. 악성 프로그램

1) 개요
- 악성 소프트웨어, 줄여서 말웨어, 또는 악성코드라고도 함
- 악의적인 목적을 위해 작성된 실행 가능한 코드
- 컴퓨터 바이러스
  - MS 워드나 엑셀처럼 컴퓨터에서 실행되는 프로그램의 일종
  - 자기 복제를 하며, 컴퓨터 시스템을 파괴하거나 작업을 지연 및 방해
- 웜
  - 실행 코드 자체로 번식하며, 주로 PC에서 실행
  - 1999년 들어 전자우편을 이용해 다른 사람에게 전달되는 형태
- 트로이 목마
  - 컴퓨터 사용자의 정보를 빼 가는 악성 프로그램
  - 목마 속에서 나온 그리스 병사가 트로이를 멸망시킨 것에 비유
  - 유틸리티 프로그램에 악의적인 코드를 내장하거나 그 자체를 유틸리티 프로그램으로 위장
  - 컴퓨터 바이러스나 웜과는 달리, 보통 다른 파일에 삽입되거나 스스로 전파되지 않음
- 백도어
  - 시스템 보안이 제거된 비밀 통로
  - 시스템 설계자가 서비스 기술자의 접근 편의를 위해 일부러 만들어 놓은 시스템의 보안 구멍
  - 정상적인 인증 절차를 거치지 않고, 컴퓨터와 암호 시스템 등에 접근할 수 있도록 하는 방법
- 스파이웨어
  - 스파이(spy)와 소프트웨어(software)의 합성어
  - 다른 사람의 컴퓨터에 잠입하여 개인정보를 추적, 모니터 및 소유하며, 제3자에게 유출시키는 프로그램

2) 루트킷

(1) 개요
- 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램들의 모음
- 트로이 목마 설치, 내부사용 흔적 삭제, 관리자 권한 획득, 원격접근, 백도어 등



(2) 루트킷 공격으로 발생할 수 있는 피해

- 멀웨어 감염
  - 루트킷은 멀웨어로써 시스템에 설치될 경우 탐지하기 매우 어려움
  - 사용자와 백신 프로그램의 감시를 피해 시스템에 추가적인 멀웨어를 다운로드 받을 수 있도록 허용해줌
  - 사용자가 인지 못 하게 백신 프로그램을 원격으로 강제 종료하여 사이버 공격에 취약하게 만들 수 있음
- 정보 탈취
  - 해커들이 민감성 정보와 기밀정보를 탈취하는데 활용
  - 루트킷은 멀웨어이기 때문에 찾기 어려우며 유저명, 비밀번호, 신용카드 정보 그리고 금융정보와 같은 민감정보를 훔치는데 용이
- 파일 삭제
  - 운영체제에 비인가 엑세스 권한을 주는 루트킷을 활용
  - 디렉토리, 인증키 그리고 다양한 파일을 삭제할 수 있게 되며 심지어 운영체제의 시스템 코드까지 삭제할 수 있음
- 도청
  - 개인정보와 사용자 간의 대화를 도청 및 유출하는 데 활용
  - 사용자의 메시지와 이메일 등을 훔쳐보고 배포할 수 있음
- 파일 원격 실행
  - 백신 프로그램의 감시를 우회하기 때문에 탐지되지 않은 상태에서 원격으로 파일을 실행시킬 수 있음
- 원격 액세스
  - 시스템 구성을 변조할 수 있게 함
  - 방화벽(Firewall) 안에서 TCP포트를 열 수 있으며 시스템 시작 스크립트를 변경할 수 있음
  - 이를 통해 원격 접근권한을 얻고 시스템을 악용

(3) 루트킷의 종류

- 사용자 모드(user-mode)/애플리케이션(application) 루트 킷
  - 컴퓨터에 있는 파일을 감염된 파일로 변경하며 응용 프로그램 또는 API표준 행동을 수정시킴

- 영향을 받는 프로그램의 종류에는 MS 오피스, 메모장, 그림판 등이 있음
- 해커는 사용자가 프로그램을 실행하면 컴퓨터에 무단 액세스할 기회를 얻게 됨
- 다행히도 안티바이러스 프로그램과 같은 응용계층에서 실행되기 때문에 발견하기 쉬운 편임

● 커널모드(kernel mode) 루트킷
- 해커들이 시스템의 모든 프로세스를 제어하고 시스템 동작 방식을 변조하기 위해 사용
- 운영체제의 커널 모듈에 설치되어 발견하기 쉽지 않음
- 시스템 퍼포먼스에 악영향을 미치며 해커들은 이를 이용하여 개인정보를 탈취하고 도용

● 하이브리드(hybrid) 루트킷
- 유저모드의 안정성과 커널모드의 탐지하기 어려운 특성을 조합한 것
- 해커들이 공격하는데 가장 흔하게 사용되는 루트킷

● 부트킷(bootkit)
- 커널모드의 변형으로 컴퓨터의 마스터 부트 레코드(MBR) 계층에서 사용
- 사용자가 컴퓨터를 실행할 때마다 PC는 운영체제의 연산 시스템을 확인하기 위해 MBR에 접근하는데 감염된 컴퓨터는 사용자가 전원을 켜 MBR에 접근할 때 부트킷이 실행되며 컴퓨터의 운영체제가 완전히 작동하기 전에 실행되어 사용이 가능해짐

● 펌웨어(firmware) 루트킷
- 하드웨어를 디바이스에서 사용하기 위해 제공되는 하드웨어 제어 소프트웨어인 펌웨어에 숨어있는 루트킷
- 사용자가 디바이스를 종료할 때 펌웨어에 숨어있다가 다시 켤 때 실행되는 것이 특징임
- 펌웨어 루트킷을 제거하는 것은 매우 어려운데 그 이유는 탐지기를 통해 발견하고 삭제한다고 하더라도 디바이스를 재실행하게 된다면 다시 실행되기 때문임

● 가상(virtual) 루트킷
- 가상머신을 사용해 운영체제를 제어하는 방식으로 작동
- 가상머신은 하나의 운영체제에 다수의 운영체제를 실행시키기 위해 사용
- 가상머신은 사용자의 운영체제에서 작동하기 때문에 별도의 운영체제에 설치가 되더라도 결과적으로 시스템 전체에 대한 제어권을 얻을 수 있게 됨
- 가상 루트킷은 다른 루트킷보다 상위레벨에서 작동하며 컴퓨터의 자체 OS와는 별도로 실행되기 때문에 탐지하기 매우 어려움

(4) 루트킷 공격을 막는 법

● 루트킷 스캐너(rootkit scanner)와 제거 프로그램 사용
- 스캐너는 시스템의 모든 구성 요소를 분석하여 루트킷을 발견

● 피싱(phishing) 공격에 속지 말 것
- 이메일을 통해 사용자가 감염된 프로그램을 다운받도록 속이므로 출처를 알 수 없는 이메일 또는 메시지의 위험성에 대해 경고

● 지속적인 소프트웨어 업데이트
- 모든 소프트웨어는 해커들이 악용할 수 있는 보안 취약점이 없도록 주기적으로 업데이트해야 함

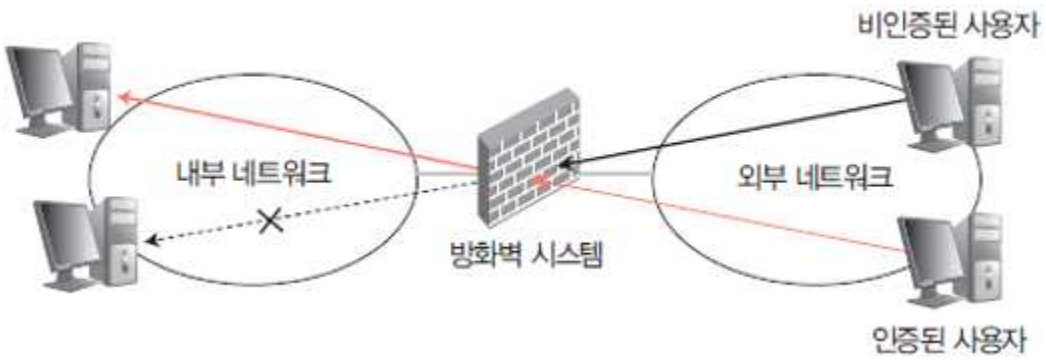
● 고급 백신 프로그램 사용
- 악성 프로그램과 루트킷 공격이 더욱 발전함에 따라 증가하는 보안 위협을 막기 위해 보안도 함께 발전해야 함

● 네트워크 트래픽 모니터링
- 네트워크 패킷을 분석하는 것은 기업의 보안에 영향을 주는 악성 트래픽을 발견하는 데 도움이 되며 손상된 네트워크 세그먼트를 격리해 공격이 퍼지고 추가적인 피해를 입는 것을 방지

4. 네트워크 보안 기법

1) 개요

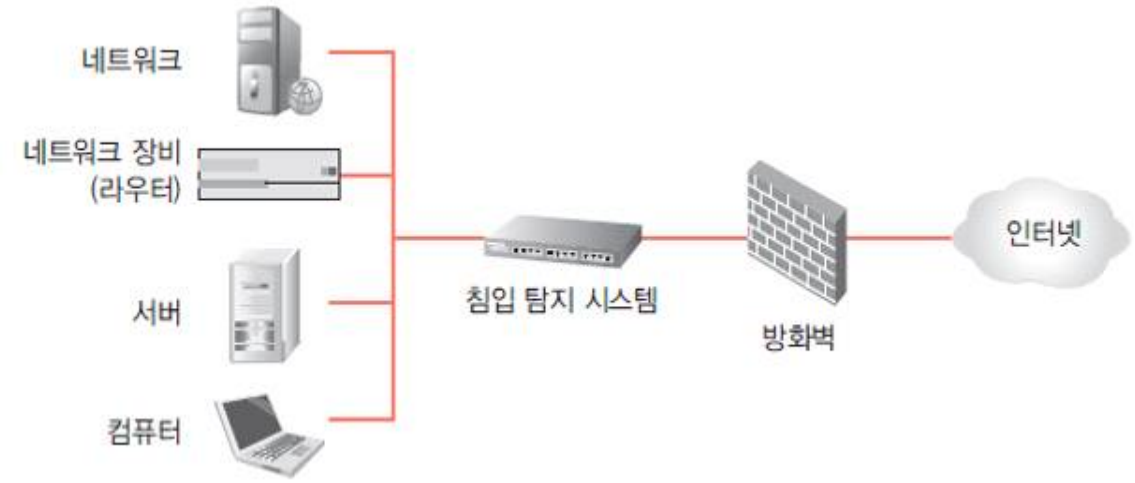
- 방화벽
  - 내부 네트워크와 외부 네트워크 사이에 있는 하드웨어와 소프트웨어로 구성
  - 보통은 라우터나 서버 등에 위치하는 소프트웨어



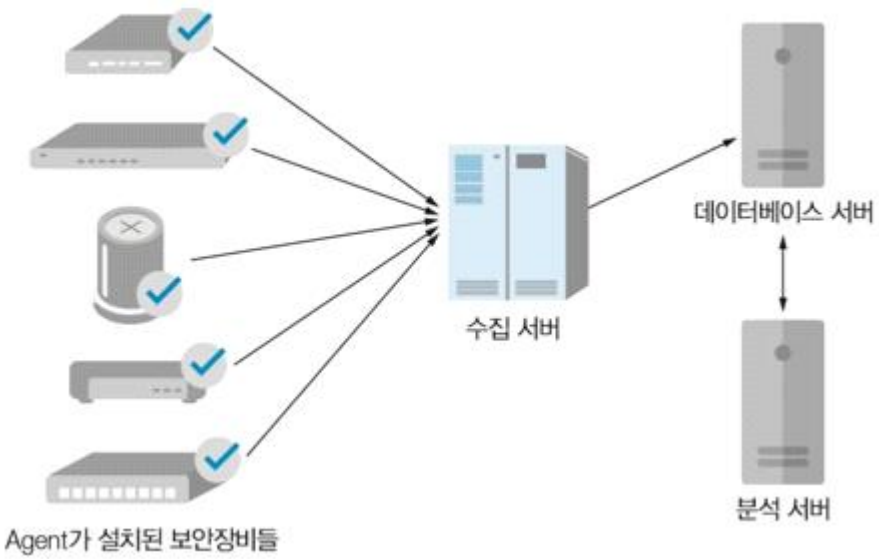
- 방화벽의 기본 구성 요소 : 네트워크 정책, 방화벽 사용지 인증 시스템, 패킷 필터링, 응용계층 게이트웨이
- 방화벽의 종류

종류	설명
스크리닝 라우터 (Screening Router)	▪ 네트워크에서 사용하는 프로토콜의 형태, 송신지 주소와 수신지 주소, 프로토콜의 제어 필드, 통신에 사용하는 포트 번호를 분석 → 내부 네트워크에서 외부 네트워크로 나가는 패킷 트래픽의 진입을 허가 또는 거절하거나 외부 네트워크에서 내부 네트워크로 진입하는 패킷 트래픽의 진입을 허가 또는 거절하는 라우터
배스천 호스트	▪ 보호된 네트워크에서 유일하게 외부의 공격에 노출된 컴퓨터 시스템 ▪ 내부 네트워크와 외부 네트워크 간에 게이트웨이 역할을 수행 ▪ 네트워크 보안상 가장 중요한 위치를 차지하므로 관리자가 철저하게 감시하며, 불법적인 침입 의도로 접속한 모든 시스템의 기록을 주기적으로 검사

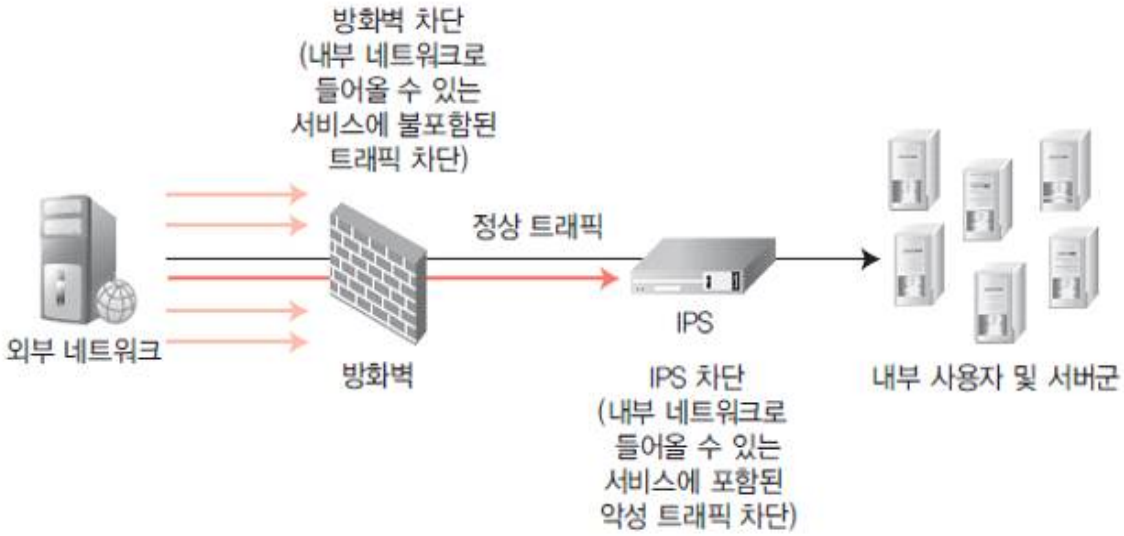
- 침입탐지 시스템(IDS)
  - 시스템이나 네트워크에 인증 절차를 거치지 않고 불법으로 침입한 사용자를 찾아내는 시스템
  - 단순한 접근제어 기능을 넘어 네트워크 시스템을 실시간으로 모니터링하고 비정상적인 침입을 탐지하는 보안 시스템



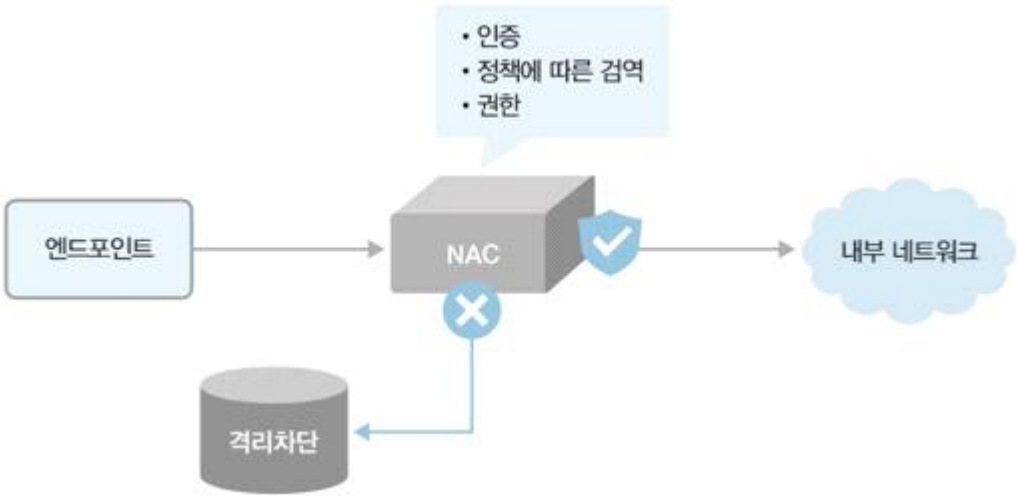
- 가상 사설망(VPN)
  - 게이트웨이 사이에서 물리적으로 통신하되, 암호화 통신은 논리적으로 하는 방식
  - 주로 단말과 단말 사이에 통신하는 패킷을 압축·암호화하여, 이 패킷을 터널링 기술을 이용해 전송
  - 기존 사설망에 비해 훨씬 저렴한 비용으로 더욱 연결성이 뛰어나며 안전한 망을 구성할 수 있음
- ESM(통합 보안관리)
  - 방화벽, 침입탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모은 통합 보안관리 시스템
  - 보안관리 프로세스의 효율성과 보안성을 향상시키기를 위한 보안관제, 운영 및 관리를 지원하는 통합보안관리 체계



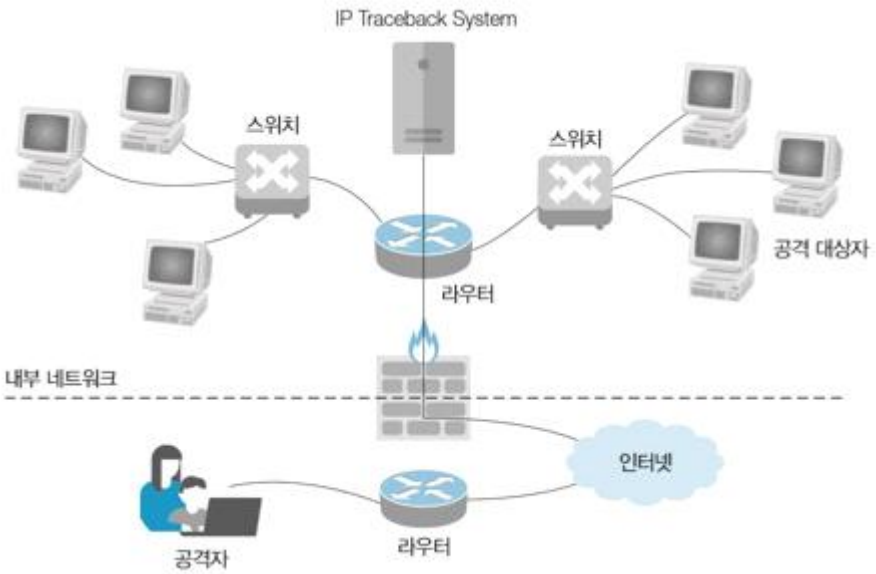
- IPS(침입방지시스템)
  - 침입탐지 시스템의 탐지와 방화벽의 차단 능력을 결합한 보안 방식
  - 비정상적인 트래픽을 능동적으로 차단하고 격리하는 등 방어 조치를 취하는 보안 솔루션



- NAC(네트워크 접근제어)
  - 허가되지 않거나 악성코드에 감염된 컴퓨터나 모바일 기기 등을 네트워크에 접속하는 것을 원천적으로 차단하여 시스템 전체를 보호하는 보안 솔루션
  - 사전 방어적인 목적



- 역추적 시스템
  - 공격을 시도하는 공격자의 위치와 네트워크상 실제 위치가 서로 다르다 하더라도 실제 공격자의 근원지를 실시간으로 추적하는 기술
  - 사람에 의한 역 추적, TCP 연결 역추적, IP 패킷 역추적이 있음



- TCP/IP 보안
  - IPSEC : 네트워크 계층에서 IP 패킷을 보호하는 인터넷 표준 방식
  - ESP : IP 페이로드를 암호화하여 데이터 기밀성을 제공하고, 제3 자가 데이터를 캡처하는 것으로 데이터를 보호
  - AH : 인증 데이터와 순서 번호를 가져서 송신자를 확인하고, 메시지를 송신하는 동안 수정하지 않았음을 보장하며, 데이터의 암호화는 제공하지 않음
- 무선 LAN 보안
  - 무선 인터넷 이용 환경을 구축하기 위해서는 무선 공유기 등 무선 접속장치가 필요

학습정리

1. 네트워크 보안 : 하드웨어와 소프트웨어를 모두 사용해 코어 네트워크의 물리적 요소 및 가상 요소에서 네트워크 활용성과 데이터 무결성을 보호
2. 네트워크 보안의 요구사항 : 기밀성, 무결성, 가용성, 인증, 부인 방지, 책임 추적성, 접근 통제
3. 크래커(Cracker) : 불법적이고 악의적인 목적을 가진 해킹을 크래킹(Cracking)이라 부르며 크래킹 하는 사람을 크래커라고 부름
4. 불법 공격의 유형 : 전송 차단, 가로채기, 변조, 위조
5. 악성 프로그램 : 컴퓨터 바이러스, 웜, 트로이 목마, 백도어, 스파이웨어
6. 루트킷 : 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램들의 모음
7. 방화벽 : 내부 네트워크와 외부 네트워크 사이에 있는 하드웨어와 소프트웨어로 구성
8. ESM(통합 보안관리) : 방화벽, 침입탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모은 통합 보안관리 시스템

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제13주차 2교시

강의주제 네트워크 위협

학습목표

1. 스미싱을 설명할 수 있다.
2. 랜섬웨어를 설명할 수 있다.
3. 공유기 보안 위협을 설명할 수 있다.
4. 네트워크 공격 기술을 설명할 수 있다.

학습내용

1. 스미싱
2. 랜섬웨어
3. 공유기 보안 위협
4. 네트워크 공격 기술

사전학습

최근 인터넷 환경에서 해커의 공격으로 피해를 입은 사례가 무엇이 있었는지 생각해 보세요.

본 학습

1. 스미싱

1) 개요

- 스미싱(smishing)은 문자 메시지(SMS)와 피싱(phising)의 합성어
- SMS에 포함된 URL을 클릭하면 악성 앱이 설치되고, 개인정보나 금융정보 등을 탈취하여 금전적인 피해를 입히거나 이차 공격 도구로 활용
- 스미싱 동작 과정

① 해커가 악성 앱을 제작하여 사용자가 다운로드하도록 클라우드 서비스에 업로드
② 해커가 사용자에게 스미싱 문자 메시지를 발송
③ 사용자가 문자 메시지에 포함된 URL을 클릭하면 악성 앱 설치 파일인 APK 파일이 자동으로 다운로드
④ 다운로드된 APK 파일을 사용자가 클릭하면 악성 앱이 설치
⑤ 설치된 악성 앱을 실행
⑥ 개인정보, 금융정보 등이 해커가 지정한 공격자 서버로 전송

2) 스미싱의 특징

- 스마트폰에 많이 설치되는 정상 어플(ex. 플레이스토어, 크롬, 모바일 백신 등)을 사칭하여 악성 앱 설치를 유도
- 크롬, 모바일 뱅킹 등 특정 앱이 실행되면 '업데이트 파일입니다'와 같은 안내 메시지를 띄워 사용자가 악성 앱을 다운로드하도록 유도
- 사용자가 악성 앱을 설치하도록 유도하기 위해 관심을 끄는 다양한 형태의 SMS(청첩장, 돌잔치 초대장, 배송 지연이나 수령 확인 등의 택배 사칭, 지인 사칭 등)를 전송
- URL은 단축 서비스를 사용하여 사용자가 사이트의 정보를 알기 어렵고, 정상적인 사이트와 매우 유사하게 제작된 피싱 사이트로 연결
- 최근에는 정상적인 사이트와 유사한 인터넷 주소를 사용하는 경우도 있으므로 주의

3) 스미싱의 예방

- 출처가 불분명한 APK 파일이 다운로드 되어 악성 앱이 설치되는 것을 방지하려면 스마트폰 환경 설정에서 '알 수 없는 출처 앱 설치' 기능을 해제
- 스미싱 차단 앱을 설치하면 스미싱으로 의심되는 SMS를 사전에 차단할 수 있음
- 모바일 백신을 설치하여 스마트폰의 보안 상태를 주기적으로 점검하고, 설치된 앱에 악성코드가 포함되었는지 확인
- 스마트폰 운영체제를 항상 최신 버전으로 업데이트하여 보안상 취약점이 없도록 관리
- 보호되지 않는 무선 공유기의 사용을 금지

4) 주요 용어

- APK 파일 : 안드로이드 응용 프로그램 패키지의 확장자로 안드로이드 애플리케이션 설치 파일
- 애플리케이션 : 응용 소프트웨어의 준말로 운영체제 위에서 동작하는 모든 소프트웨어를 뜻하고 더 줄여서 앱(App)이라고도 표현
- 애플리케이션 권한 : 애플리케이션이 실행될 때, 애플리케이션이 스마트폰 안에 들어있는 여러 가지 정보에 대한 접근을 가능하게 하는 정보
- 애플리케이션 마켓
  - 스마트폰 사용자가 앱 개발자로부터 구매하여 설치 및 관리를 할 수 있도록 환경을 제공하는 앱
  - 마켓은 제조사나 통신사 등에서 운영하여 앱에 대한 검증 및 관리하는 공식 마켓과 특정 조직이나 업체에서 관리를 하지 않는 그 외에 마켓으로 구별됨
- 캡챠코드
  - 사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용하는 방법
  - 컴퓨터가 쉽게 인지하지 못하게 의도적으로 숫자나 문자를 비틀거리나 덧칠하면서 해당 내용을 물어보는 방법
- 루팅 : 안드로이드 운영체제의 기반이 된 리눅스 환경에서 모든 파일과 프로그램에 접근할 수 있는 권한을 비정상적인 방법으로 획득하여 슈퍼유저로 설정
- 탈옥 : 애플社의 아이폰 잠금장치를 해킹하여, 멀티태스킹 등 다양한 기능을 사용하고 유료 앱을 무료로 이용할 수 있도록 함

2. 랜섬웨어

1) 개요

- 랜섬웨어는 몸값(ransom)과 소프트웨어(software)의 합성어
- 시스템을 잠그거나 데이터를 암호화하여 사용할 수 없게 하고 이를 인질로 금전을 요구하는 악성 프로그램
- 랜섬웨어는 신뢰할 수 없는 사이트, 스팸메일, 파일 공유 사이트, 네트워크를 통해 유포

2) 감염 경로

- 신뢰할 수 없는 사이트: 단순한 사이트 방문만으로도 감염될 수 있으며 드라이브 바이 다운로드 drive-by-download 기법을 통해 유포
  - 드라이브 바이 다운로드(Drive by download) : 취약한 사이트에 방문했을 때 사용자 모르게 악성 스크립트가 동작하여 취약점을 유발하는 코드가 실행
    ⇒ 악성코드가 다운로드 및 실행되어 사용자의 컴퓨터를 감염시키는 기법
- 파일 공유 사이트 : 토렌트, 웹하드 등의 P2P 사이트에서 동영상 등의 파일을 다운로드하여 실행하면 악성코드에 감염될 수 있음

- SNS: 페이스북, 인스타그램 등의 SNS에 업로드된 단축 URL과 이미지를 통해 유포
- 네트워크망: 네트워크를 통해 최신 보안 패치가 적용되지 않은 컴퓨터를 스캔하여 악성코드를 감염

3) 랜섬웨어의 종류

- 워너크라이(WannaCry)
  - 17년 5월 12일 스페인, 영국, 러시아 등을 시작으로 전 세계에서 피해가 보고된 악성코드
  - 다양한 문서 파일(hwp, ppt, doc)과 파일을 암호화
  - 윈도우 운영체제의 SMB(Sever Message Block)를 이용하여 악성코드를 감염시킨 후 해당 컴퓨터 또는 서버에서 접속 가능한 IP를 스캔하여 네트워크로 전파 시킴
  - 파일을 암호화하여 바탕화면을 변경하고 확장자를 .wncry 또는 .wncryt로 변경
  - 변종이 지속적으로 발견되고 있으며, 미진단 변종이 존재할 수 있으므로 MS 윈도우 최신보안 패치를 반드시 적용
- 로키(Locky)
  - 16년 3월 이후 수신자를 속이기 위해 Invoice, Refund 등의 제목을 붙인 이메일을 통해 유포
  - 자바스크립트 파일이 들어 있는 압축 파일을 첨부하여 수신자가 이를 실행하면 감염
  - 감염되면 파일이 암호화되고 확장자가 .locky로 변경되며, 바탕화면과 텍스트 파일로 복구 관련 메시지를 출력
  - 최근에는 연결 IP 정보를 동적으로 복호화하고 특정 파라미터를 전달해서 실행하는 경우만 동작
- 크립트XXX(CryptXXX)
  - 16년 5월 해외 백신사의 복호화 툴 공개 이후에 취약한 암호화 방식을 보완한 크립트XXX 3.0 버전이 유포됨
  - 크립트XXX에 감염되면 파일 확장자가 .crypt 등으로 변경되고, 바탕화면에 복구 안내 메시지인 비트코인 지불 안내 페이지가 한글로 번역되어 나타남
  - 실행 파일(exe)이 아닌 동적 링크 라이브러리 DLL 형태로 유포
  - 정상 rundll32.exe를 svchost.exe 파일로 복사한 후 동작
  - 최신 버전은 네트워크 연결 없이도 파일을 암호화할 수 있음
- 케르베르(CERBER)
  - CERBER는 말하는 랜섬웨어로 유명
    - 감염 시에 "Attention! Attention! Attention!? Your documents, photos, databases and other important files have been encrypted" 음성 메시지 출력
  - 웹사이트 방문 시 취약점을 통해 감염되며, 감염되면 파일을 암호화하고 확장자를 .cerber로 변경, 최근 이메일 통해 유포되는 정황 발견
  - 악성코드 내에 저장되어있는 IP 주소와 서브넷 마스크값을 사용하여 UDP 패킷을 전송, 네트워크가 연결되지 않더라도 파일은 암호화
  - 윈도우즈 볼륨 쉐도우(Windows Volume Shadow)를 삭제하여 윈도우 시스템 복구가 불가능하게 만듦
- 크립토락커(CryptoLocker)
  - '13년 9월 최초 발견된 랜섬웨어의 한 종류로 자동실행 등록 이름이 크립토락커(CryptoLocker)로 되어 있는 것이 특징
  - 웹사이트 방문 시 취약점을 통해 감염되거나, E-Mail 내 첨부파일을 통해 감염되며, 확장자를 encrypted, ccc로 변경
  - 파일을 암호화한 모든 폴더 내에 복호화 안내 파일 2종류를 생성(DECRYPT_INSTRUCTIONS.* / HOW_TO_RESTORE_FILES.*)
  - 윈도우즈 볼륨 쉐도우(Windows Volume Shadow)를 삭제하여 윈도우 시스템 복구가 불가능하게 만듦

- 테슬라크립트(TeslaCrypt)
  - '15년 국내에 많이 유포된 랜섬웨어로 '16년 5월경 종료로 인해 마스터키가 배포되었음
  - 취약한 웹페이지 접속 및 이메일 내 첨부파일로 유포되며, 확장자를 ecc, micr등으로 변경
  - 드라이브 명에 상관없이 고정식 드라이브(DRIVE_FIXED)만을 감염 대상으로 지정하며, 이동식 드라이브나 네트워크 드라이브는 감염 대상에서 제외
  - 악성코드 감염 시 (Howto_Restore_FILES.*)와 같은 복호화 안내 문구를 바탕화면에 생성

4) 랜섬웨어 예방
- 모든 소프트웨어는 최신 버전으로 업데이트하여 사용
- 백신 소프트웨어를 설치하고 최신 버전으로 업데이트
- 출처가 불명확한 이메일과 URL 링크는 실행하지 않음
- 파일 공유 사이트 등에서 파일을 다운로드하여 실행할 때 주의
- 중요 자료는 정기적으로 백업

5) 랜섬웨어 복구
- 한국인터넷진흥원(KISA) 제공 랜섬웨어 복구프로그램
- NMR(No More Ransom) 제공 랜섬웨어 복구프로그램
- 이스트시큐리티 제공 랜섬웨어 복구프로그램
- 안랩 제공 랜섬웨어 복구프로그램
- 랜섬웨어 침해 대응센터 복구프로그램 안내
- 카스퍼스키 제공 랜섬웨어 복구프로그램
- 트랜드마이크로 제공 랜섬웨어 복구프로그램

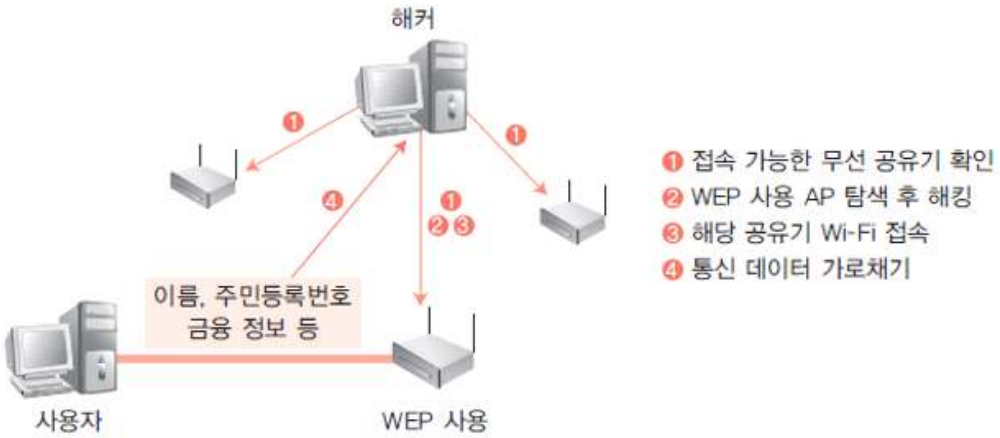
3. 공유기 보안 위협

1) 개요
- 보안 설정이 되어 있지 않은 무선 LAN은 외부에서 무선 공유기를 무단으로 사용할 수 있고, 해커가 접속하여 해킹 및 개인 정보 유출 등의 다양한 보안 위협을 유발
- 공유기 사용자는 무선 인증 패스워드를 기본으로 설정하거나 취약한 인증 방식을 사용하고 있기 때문에 해커는 해당 공유기를 통해 제공되는 무선 네트워크에 접속할 수 있음
- 해커는 ARP 스푸핑(spoofing) 등의 공격 기법을 통해 평문으로 전송되는 사용자의 계정, 금융정보 등의 개인정보를 탈취

2) 무선 공유기의 보안 기술

구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
인증	사전 공유된 비밀키 사용 (64비트, 128비트)	사전에 공유된 비밀키를 사용하거나 별도의 인증서버 이용	사전에 공유된 비밀키를 사용하거나 별도의 인증서버 이용
암호방법	고정 암호키 사용 RC4 알고리즘 사용	암호키 동적 변경(TKIP) RC4 알고리즘 사용	암호키 동적 변경 AES 등 강력한 암호 알고리즘 사용
보안성	가장 취약하여 널리 사용되지 않음	WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	가장 강력한 보안기능 제공

- 무선 공유기 개인 정보 탈취
  - 일부 공유기는 유지·보수를 위해 텔넷 포트를 이용하는데, 관리의 편의성 때문에 쉬운 계정이나 추측하기 쉬운 패스워드를 사용하는 경우가 많음
  - 해커는 감염된 다수의 공유기를 통한 통신사 DDoS 공격 등 다양한 공격을 할 수 있음
  - 개인정보 탈취 과정



- DNS 주소 변조 과정
  - 인터넷에서 접속 가능한 공유기의 DNS 주소를 변조하는 방법으로 공유기 사용자에게 사칭 앱 유포, 금융정보 유출 등의 피해를 입힐 수 있음
  - DNS 주소 변조 과정

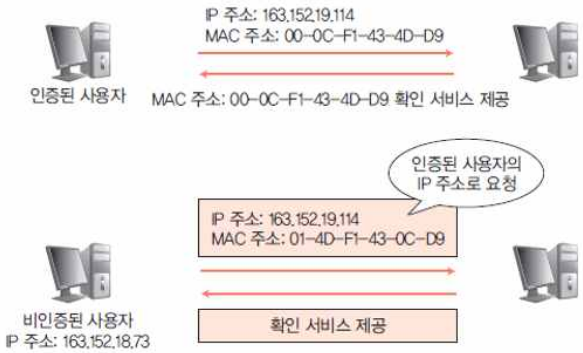
- 공유기 보안 위협 예방
  - 불필요한 외부 접속 포트나 FTP, 텔넷 등의 서비스를 비활성화
  - 필요한 경우에는 패스워드를 설정
  - 무선 암호화 방식은 보안 강도가 높은 WPA2가 기본으로 설정
  - 공유기 펌웨어를 업데이트할 때 파일 고유 해시값을 비교하여 변조 여부에 대한 무결성 검증을 실시
  - 무결성 인증 시 SHA-256 이상의 암호화 알고리즘을 사용

4. 네트워크 공격 기술

1) IP 스푸핑

(1) 개요

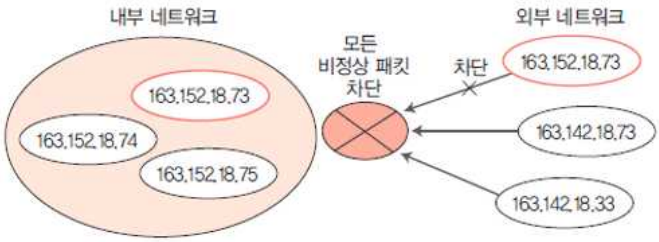
- IP 스푸핑(IP Spoofing)은 IP 주소를 속이는 행위를 말함
- '스푸핑'은 외부 네트워크 공격자가 임의로 웹사이트를 구성하여 일반 사용자의 방문을 유도하고, 인터넷 프로토콜인 TCP/IP의 구조적인 결함을 이용하여 사용자 시스템 권한을 획득한 후 정보를 빼가는 해킹 수법



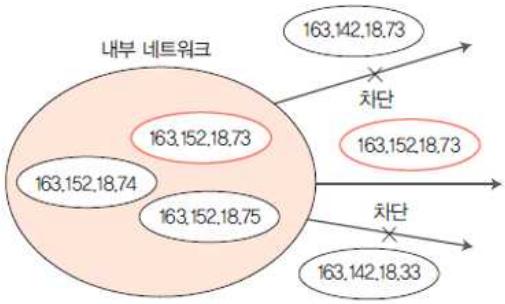
(2) IP 스푸핑 차단 방법

- 액세스 제어
  - 내부 네트워크에 있는 송신지 주소를 가진 외부 네트워크의 패킷을 모두 거부함으로써 IP

스푸핑 공격을 줄일 수 있음



- 필터링
  - 내부 네트워크의 IP 주소 범위에서 송신지 주소를 보유하지 않은 패킷이 외부로 나가는 것을 차단함으로써 사용자가 다른 네트워크를 스푸핑하는 것을 막을 수 있음



- 암호화
  - IP 스푸핑을 차단하는 가장 좋은 방법은 패킷을 암호화하는 것임

2) IP 스니핑

(1) 개요

- 스니핑(Sniffing)은 '코를 킁킁거리다' 또는 '냄새를 맡다'는 뜻으로 네트워크를 이용하여 전송하는 데이터를 엿듣는 일종의 도청 행위를 말함
- TCP/IP 프로토콜은 인터넷이 시작되기 전부터 설계된 프로토콜이기에 패킷 암호화 및 인증 등을 고려하지 않아 데이터 통신 보안의 기본 요소 중 비밀성과 무결성을 보장할 수 없음
- 특히 스니핑은 비밀성을 해치는 대표적인 공격 방법 중 하나임

(2) 스니핑 피해 감소 방법

- 가상 LAN 작게 나누기
  - 스니핑은 동일한 가상 LAN에서 가능하기 때문에 가상 LAN을 작게 나누면 피해를 줄일 수 있음
  - 하나의 C 클래스가 하나의 가상 LAN으로 구성되어 있다면 그만큼 스니핑 당할 수 있는 범위가 넓어짐
  - 반대로 서비스에 따라 가상 LAN을 세분하면 그만큼 피해 범위를 줄일 수 있음
- 암호화 전송 프로토콜
  - 기본적으로 스니핑은 텔넷이나 FTP, POP3 등이 평문으로 전송되는 트래픽을 모니터링하여 ID나 패스워드를 빼내는 것이므로, 암호화 전송 프로토콜을 이용하면 중간에서 패킷을 가로채도 분석하기 어려움
  - 최근에는 텔넷 대신 SSH, HTTP 대신 HTTPS, POP3 대신 POP3S 등의 프로토콜을 이용하는 추세
  - 프로토콜마다 별도의 암호화 전송 프로토콜과 응용 프로그램을 사용해야 하는 등 현실적으로 불편하기 때문에 VPN을 이용하는 방법을 권고함
  - 종류

종류	설명
SSL	▪ HTTP, POP3, SMTP, 텔넷 등에 SSL을 적용하여 HTTPS, POP3S, SMTPS, 텔넷 등으로 대치 ▪ HTTP에 가장 많이 활용하며 이를 적용하여 ID와 패스워드 암호화 가능
SSH	▪ 암호화 통신을 제공하여 FTP, 텔넷 대치 가능
VPN	▪ 스니핑 피해가 우려되는 네트워크에 전용선을 직접 연결함으로써 도청 방지 ▪ 인터넷 회선을 이용하여 사설망의 효과를 낼 수 있으며 각 VPN 장비 간의 암호화를 이용하여 도청 방지

※ SSL(Secure Sockets Layer), SSH(Secure Shell), VPN(Virtual Private Network)

학습정리

1. 스미싱 : SMS에 포함된 URL을 클릭하면 악성 앱이 설치되고, 개인 정보나 금융 정보 등을 탈취하여 금전적인 피해를 입히거나 이차 공격 도구로 활용
2. 랜섬웨어 : 시스템을 잠그거나 데이터를 암호화하여 사용할 수 없게 하고 이를 인질로 금전을 요구하는 악성 프로그램
3. 랜섬웨어의 종류 : 워너크라이(WannaCry), 로키(Locky), 크립트XXX(CryptXXX), 케르베르(CERBER), 크립토락커(CryptoLocker), 테슬라크립트(TeslaCrypt)
4. 무선 공유기의 보안 기술 : WEP(Wired Equivalent Privacy), WPA(Wi-Fi Protected Access), WPA2(Wi-Fi Protected Access2)
5. IP 스푸핑 : '스푸핑'은 외부 네트워크 공격자가 임의로 웹사이트를 구성하여 일반 사용자의 방문을 유도하고, 인터넷 프로토콜인 TCP/IP의 구조적인 결함을 이용하여 사용자 시스템 권한을 획득한 후 정보를 빼가는 해킹 수법
6. IP 스니핑 : 스니핑(Sniffing)은 '코를 킁킁거리다' 또는 '냄새를 맡다'는 뜻으로 네트워크를 이용하여 전송하는 데이터를 엿듣는 일종의 도청 행위를 말함

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제14주차 1교시

강의주제 4차 산업과 네트워크 기술

학습목표

1. 4차 산업 혁명 시대의 배경을 이해하고 개요를 설명할 수 있다.
2. ICBM(IoT/Cloud/Big Data/Mobile)의 특징을 이해하고 설명할 수 있다.

학습내용

1. 4차 산업 혁명 시대의 개요
2. ICBM(IoT/Cloud/Big Data/Mobile)

사전학습

최근 이슈가 되고 있는 4차 산업 혁명이 무엇이라고 생각하나요?

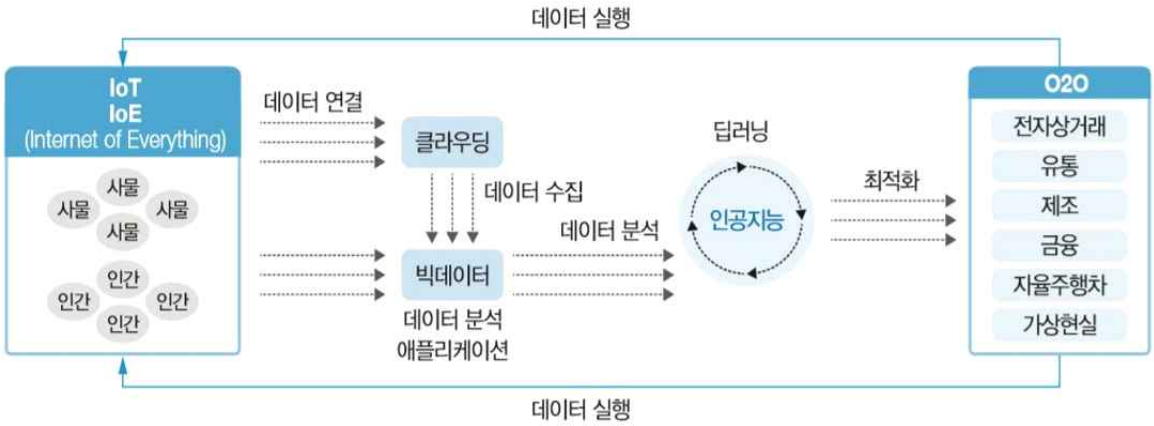
본 학습

1. 4차 산업 혁명 시대의 개요

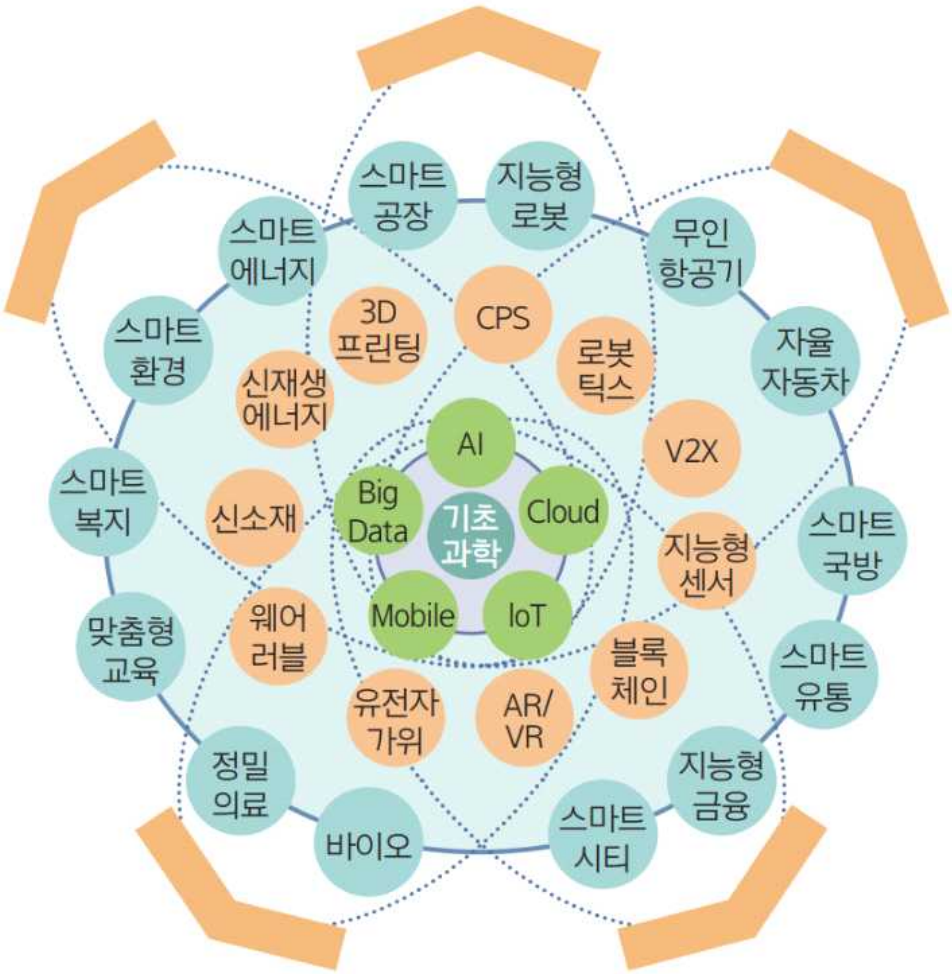
1) 개요

- 정보통신 기술을 기반으로 한 공간의 융합과 변화가 특징
- 사물인터넷(IoT), 클라우드 컴퓨팅 기술, 빅데이터 기술, 5G(또는 6G) 이동통신 기술 등이 주요 기술
- 산업혁명의 4단계

- 4차 산업 혁명 시대의 정보통신 기술과 서비스 작동 원리
  - 사물인터넷 기술로 빅데이터를 얻고, 그 내용을 클라우드에 저장하며, 이 저장된 빅데이터를 인공지능 기술로 분석하고 활용



● 4차 산업혁명 관련 과학-기술-산업 간 연계도



2. ICBM(IoT/Cloud/Big Data/Mobile)

1) ICBM 개요

- 4차 산업혁명이라는 새로운 환경에 원천이 되는 대표적인 정보통신 기술
- 사물인터넷(IoT), 클라우드, 빅데이터, 모바일 기술 등

2) 사물인터넷(IoT)

- 각종 사물에 컴퓨터 칩과 통신 기능을 내장하여 인터넷에 연결하는 기술
- 다양한 산업에 융합되어 사용가능
- 사물인터넷의 참조 모델
  - ITU-T의 규정을 기반으로 정의

구분	설명
응용 계층	▪ 다양한 사물인터넷 응용들을 의미
서비스 지원 및 응용지원계층	▪ 공통지원 기능: 다양한 사물인터넷 응용들에게 공통으로 필요한 기능으로 정보 처리 및 정보 저장 기능 등을 포함 ▪ 특정 응용 지원 기능: 특정한 응용에 특화된 기능으로 다양한 응용을 지원하기 위해 다양한 기능 그룹이 존재할 수 있음

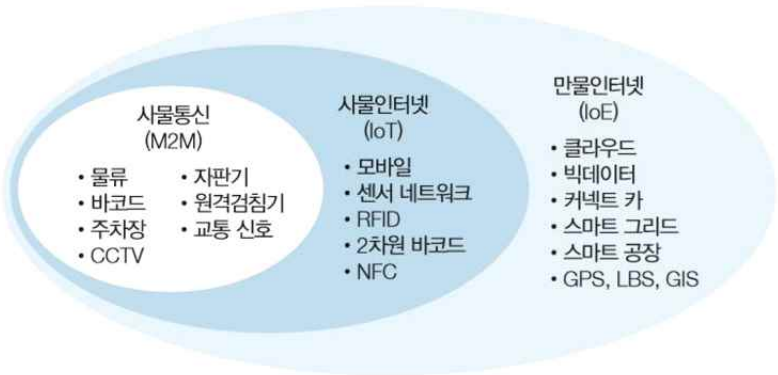
구분	설명
네트워크 계층	▪ 네트워킹 기능 : 자원제어, 이동성 관리, AAA(Authentication, Authorization and Accounting) 등 네트워크 연결을 위한 제어기능을 수행 ▪ 전송 기능 : 사물인터넷 서비스 및 응용과 관련된 정보, 제어 정보, 관리 정보의 전달을 위한 연결 기능 수행
디바이스 계층	▪ 디바이스 기능 - 네트워크와 직접통신 - 게이트웨이의 기능을 활용한 네트워크와 간접 통신 - 애드혹 네트워킹 - 슬립 및 웨이크 업 ▪ 게이트웨이 기능 - 다양한 인터페이스 지원 - 프로토콜 변환
관리기능	▪ 장애, 구성, 과금, 성능 및 보안에 필요한 관리 기능을 모두 포함 ▪ 공통관리 기능 - 디바이스 관리 - 로컬 네트워크 토폴로지 관리 - 트래픽 관리 ▪ 특정 관리 기능 - 스마트 그리드 전력선 관리 등 특정 응용의 요구 사항과 밀접하게 관련된 기능
보안기능	▪ 응용 계층에서 권한, 인증, 응용 데이터 기밀성 및 무결성 보호, 개인정보보호, 보안 감사 및 안티 바이러스 ▪ 네트워크 계층에서 권한, 인증, 사용자 데이터 및 시그널링 데이터의 데이터의 기밀성 및 무결성 보호 ▪ 디바이스 계층에서 권한, 인증, 장치 무결성 검증, 엑세스 제어, 데이터 기밀성 및 무결성 보호

● 사물인터넷의 진화

▪ 사물통신 : 통신장비와 사람과의 통신을 주목적

▪ 사물인터넷(IoT) : 사물끼리도 통신을 함

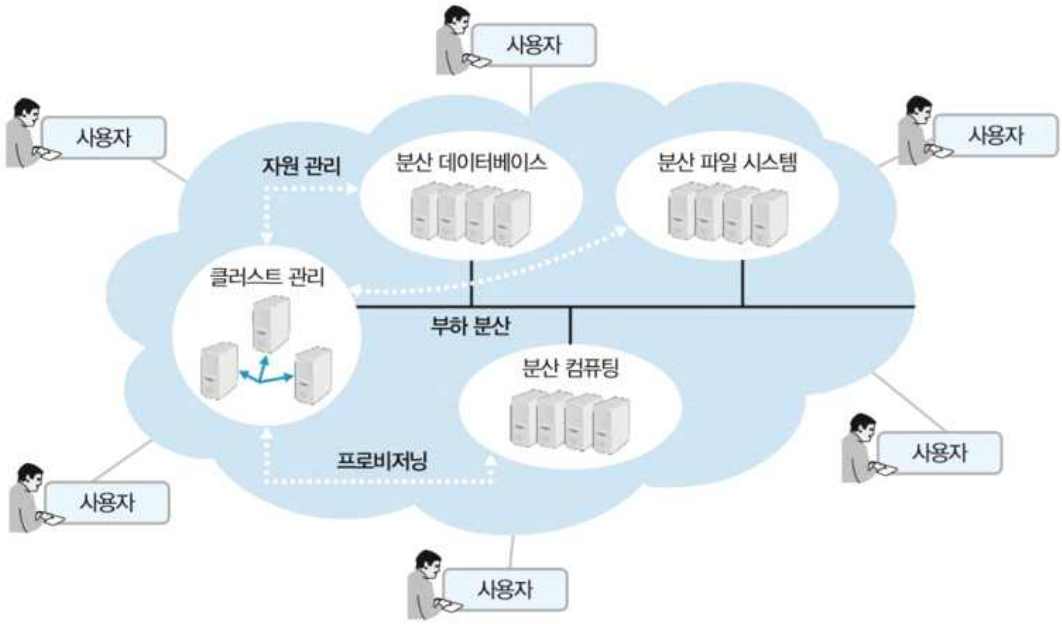
▪ 만물인터넷(IoE) : 프로세스와 데이터가 독립적인 개체로 서로 연결



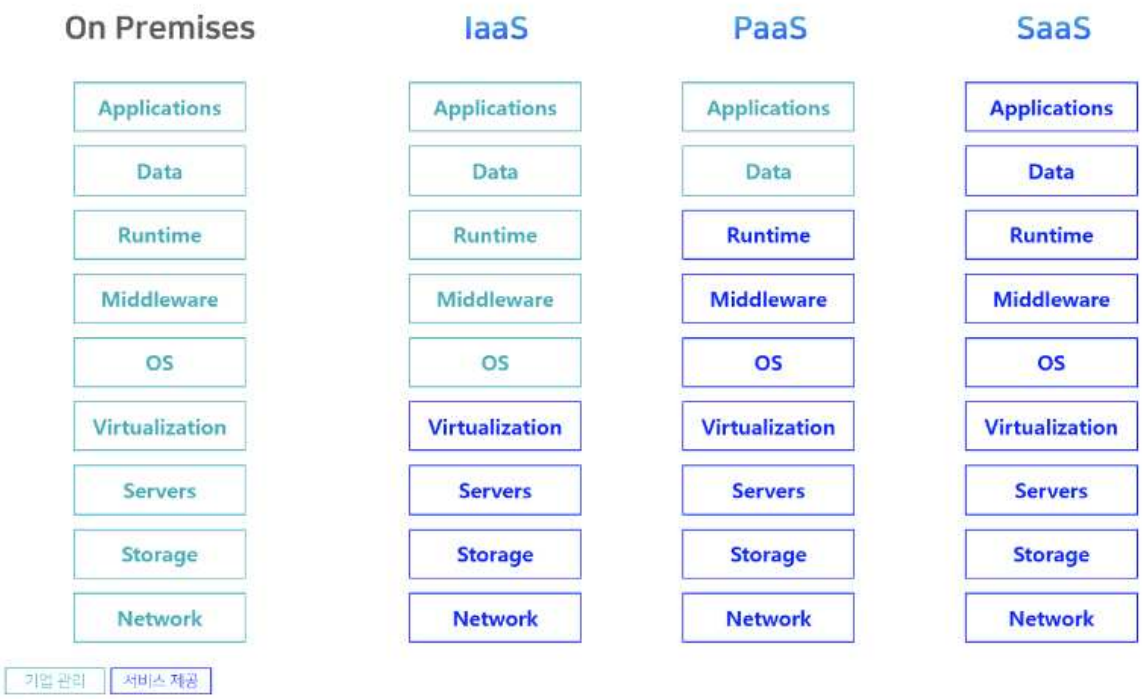
3) 클라우드(Cloud)

(1) 개요

- 정보처리, 저장, 관리, 유통, 분석 등의 작업을 제3의 공간(웹하드)에서 수행하는 컴퓨팅 시스템
- 인터넷 접속이 가능한 단말기 등을 통해 언제 어디서나 데이터를 불러와 작업하는 사용자 환경
- 클라우드 컴퓨팅의 개념도



(2) 클라우드 컴퓨팅의 서비스 유형



- IaaS (Infrastructure as a Service)
  - 가상화 기술과 물리적 자원, 즉 인프라만 제공
  - Amazon AWS, MS Azure, Google GCP 등

- PaaS (Platform as a Service)
  - 개발에 필요한 환경, 즉 플랫폼까지만 빌려주고 앱과 데이터는 기업이 직접 운영
  - AWS Elastic Beanstalk, Heroku, Red Hat OpenShift 등
- SaaS (Software as a Service)
  - 전통적인 IT 솔루션 (사용자의 하드웨어·소프트웨어)을 모두 서비스
  - Dropbox, Salesforce, Google Drive, Naver MYBOX 등

(3) 클라우드 운영 유형

- Public Cloud (공용 클라우드)
  - 타사 클라우드 서비스 공급자가 소유하고 운영하며, 인터넷을 통해 제공하는 방식
  - 기업이 사용료를 내고 이용하지만, 기업 뿐만 아니라 외부 사용자도 이용할 수 있음
  - 확장성 (필요시 자원 할당 가능)
  - 비용 절감 (HW·SW 구매 불필요)
  - 유지 관리 불필요
  - 안정성 (공용이므로 광대하고 탄탄한 네트워크가 받쳐야 함)
  - 상대적으로 보안에 취약
  - 주로 웹 서비스·개인정보 취급 서비스·동영상 서비스처럼 외부에 제공하는 시스템 등
- Private Cloud (사설 클라우드)
  - 주로 기업 내부에 구축된 인프라를 운영하는 방식으로, 방화벽으로 보호된 인프라는 단일 고객만 사용
  - 조직의 데이터 센터에 있을 수도, 타사 클라우드 서비스 공급자가 호스팅할 수도 있음
  - 유연성 (조직의 요구 조건에 알맞는 사용자 지정 수준의 설계)
  - 보안 향상
  - 기업 내부에서 유지 관리가 필요하며, 외부 접속이 불필요하고 보안에 민감한 내부 서비스(그룹웨어 등)에 적합
- Hybrid Cloud (혼용 클라우드)
  - 필요에 따라 혼용하여 운영하는 방식
  - 1개 이상의 Public Cloud + 1개 이상의 Private Cloud
  - 2개 이상의 Public (혹은 Private) Cloud
  - 1개 이상의 Public(혹은 Private) Cloud에 연결되는 Bare-Metal 혹은 가상 환경
  - 공용 서비스를 위한 WEB에 내부 DB 서비스를 연결하는 등의 복합적인 환경에 필요

4) 빅데이터(Big Data)

(1) 개요

- 기존의 데이터 처리방법으로는 감당하기 힘들 정도로 방대한 분량의 데이터
- 데이터 하나하나가 모여 의미와 가치가 있는 단위로 묶인 데이터 덩어리
- "빅데이터 프로세싱(Big data processing)"을 포함하여 일컫는 말
- 대용량 데이터가 뭉친 형태를 일컫는 말
- 정형 데이터(Structured data)
  - 일반적으로 수치만으로 파악이 쉬운 데이터들
  - 예) age : 25, weight : 65 등
- 비정형 데이터(Unstructured data)
  - 정해진 규칙이 없어서 값의 의미를 쉽게 파악하기 힘든 데이터들
  - 예) 텍스트, 음성, 영상 등

(2) 빅데이터 등장 배경
- 기술 발전에 따른 데이터 저장, 처리 비용의 감소
- 실시간 서비스, SNS 서비스 등으로 디지털 정보량의 기하급수적 증가
- 기존의 데이터 저장, 관리, 분석, 기법의 한계

(3) 정의
- 기존의 데이터베이스 관리 도구, 관리 시스템의 능력을 넘어 대량의 정형, 비정형 데이터 세트, 이를 포함한 데이터로부터 분석하여 의미있는 가치를 추출하고 결과를 분석하는 기술
- 위키피디아 : 데이터베이스 등 기존의 데이터 처리 응용 소프트웨어(data-processing application software)로는 수집·저장·분석·처리하기 어려울 정도로 방대한 양의 데이터를 의미
- 국가정보화전략위원회 : 대용량 데이터를 활용, 분석하여 가치있는 정보를 추출하고, 생성된 지식을 바탕으로 능동적으로 대응하거나 변화를 예측하기 위한 정보화 기술
- 삼성경제연구소 : 기존의 관리 및 분석 체계로는 감당할 수 없을 정도의 거대한 데이터의 집합
- 맥킨지(Mckinsey) : 기존 시스템의 데이터 수집, 저장, 관리, 분석 역량을 넘어서는 데이터셋(Dataset, 1개 단위로 취급하는 데이터의 집합) 규모로 빅데이터의 분량 기준은 산업 분야에 따라 상대적이며 앞으로도 계속 변화될 것

(4) 특징
- 3V : 규모(Volume), 다양성(Variety), 속도(Velocity)
- 5V : 규모(Volume), 다양성(Variety), 속도(Velocity), 정확성(Veracity), 가치(Value)
- 규모(Volume) : 기술 및 ICT 발전, 디지털 정보량 급증, 제타바이트(ZB) 시대 진입
- 다양성(Variety) : 텍스트 외 음성, 영상 등 비정형 데이터 종류 증가
- 속도(Velocity) : IoT 및 실시간 정보 증가, 데이터 생성 및 이동 증가, 실시간 데이터 처리 분석 위한 속도의 중요성
- 정확성(Veracity) : 방대한 데이터의 질이 데이터 분석 정확도에 영향을 미침
- 가치(Value) : 빅데이터가 추구하는 것이 바로 가치이며 빅데이터 분석, 통찰력 제공, 기업의 현실문제 해결에 도움

(5) 빅데이터 분석과정
- 데이터 인식 : 데이터가 어디있는가 데이터 소스를 인식하는 단계
  - 내부데이터 : 해당 조직이 자체적으로 보유한 각종 데이터(예: 현재 및 과거의 매출정보, 고객정보, 제품정보 등)
  - 외부 데이터 : 인터넷 등으로 연결되어 조직 외부에 존재하는 각종 비정형 데이터(예: 소셜 미디어 데이터 등)
- 수집 : 데이터를 모으는 행위
  - 검색, 수집, 변환을 통해 정제된 데이터를 확보
  - 데이터웨어하우스 : 데이터분석을 위한 데이터
  - ETL(Extraction, Transformation, Loading)
  - 웹 크롤링(Web Crawling) 등
- 저장 : 데이터를 어딘가에 저장
  - 빅데이터를 위한 데이터베이스
  - 예) Hadoop, NoSQL 등 비정형 데이터베이스
- 처리 : 분석 가능한 상태로 처리
  - 일괄처리: 쌓인 데이터를 여러 서버로 분산해 나누어 처리, 이를 다시 모아 결과를 정리
  - 실시간처리: 데이터가 들어오는 대로 일련의 처리 업무들을 수행하여 그 결과를 연속적으로 제공
- 분석 : 데이터 안의 정보 및 지식을 추출
  - 대량의 데이터로부터 사실, 추세, 관계, 패턴 등 알려지지 않은 정보, 또는 지식을 찾아내는 과정

- 통계 분석(Statstical Analysis), 데이터 마이닝(Data Mining), 텍스트 마이닝(Text Mining), 소셜 네트워크 분석(Social Network Analysis) 등
- 표현 : 분석결과를 활용하여, 의사결정 혹은 다양한 여러분야에 활용
- 데이터 분석 결과를 쉽게 이해할 수 있도록 시각적인 수단으로 정보를 전달하는 과정
- 예) 시간 시각화, 분포 시각화, 관계 시각화, 인포그래픽 등

5) 모바일(Mobile)

(1) 개요

- 스마트폰과 태블릿 PC 등과 같이 이동 중 사용이 가능한 컴퓨터 환경
- 5세대 이동통신(5G) : 국제전기통신연합의 전파부문 이동통신작업반 회의에서 합의된 IMT-2020
- 6세대 이동통신(6G) : 2030년이면 현재 5G의 20Gbps보다 50배 빠른 1Tbps 최대 전송용량과 10배 우수한 1Gbps 사용자 체감속도, 통신 서비스가 나올 것으로 전망
- 7세대 이동통신(7G) : 2040년경에 이루어질 전망, 사람이 존재하는 모든 공간 자체가 네트워크화 될 것, 지구에 존재하는 모든 산업과 인프라가 조 단위의 센서로 연결되는 '초연결' 생태계가 조성될 전망

학습정리

1. 사물인터넷(IoT) : 각종 사물에 컴퓨터 칩과 통신 기능을 내장하여 인터넷에 연결하는 기술
2. 클라우드(Cloud) : 정보처리, 저장, 관리, 유통, 분석 등의 작업을 제3의 공간(웹하드)에서 수행하는 컴퓨팅 시스템
3. 빅데이터(Big Data) : 기존의 데이터베이스 관리 도구, 관리 시스템의 능력을 넘어 대량의 정형, 비정형 데이터 세트, 이를 포함한 데이터로부터 분석하여 의미있는 가치를 추출하고 결과를 분석하는 기술
4. 빅데이터 분석과정 : 데이터 인식 – 수집 – 저장 – 처리 – 분석 - 표현
5. 5세대 이동통신(5G) : 국제전기통신연합의 전파부문 이동통신작업반 회의에서 합의된 IMT-2020

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)

제14주차 2교시

강의주제 차세대 네트워크 프로토콜

학습목표

1. 5G와 6G 기술을 이해하고 설명할 수 있다.
2. 지능형 초연결망을 이해하고 발전 방향을 설명할 수 있다.
3. IoT 기술 및 프로토콜을 설명할 수 있다.

학습내용

1. 5G와 6G
2. 지능형 초연결망
3. IoT 기술 및 프로토콜

사전학습

지능형 초연결망의 핵심 기술은 무엇이라고 생각하나요?

본 학습

1. 5G와 6G

1) 5G 개요

- 통신 산업은 '80년 1세대 아날로그 이동통신 서비스가 시작된 이래 10년을 주기로 진화를 거듭해오고 있으며, '19년 4월 국내 최초 상용화를 기점으로 5세대 이동통신 시대 개막
- 1G/2G 시대는 사람들 사이의 무선음성 서비스를 제공
- 3G/4G 시대는 사람들 사이의 무선 데이터 서비스를 제공
- 5G 이동통신은 4G 대비 초고속, 저지연, 초연결을 제공하는 통신기술로 이를 활용하여 스마트시티, 자율주행차, 지능형 CCTV 등 다양한 서비스 제공이 가능

2) 5G 기술 진화 방향

- 초광대역 서비스(eMBB: enhanced Mobile Broadband)
  - UHD 기반 AR/VR 및 홀로그램 등 대용량 전송이 필요한 서비스를 감당하기 위해 더 큰 주파수 대역폭을 사용하고 더 많은 안테나를 사용
  - 사용자당 100Mbps에서 최대 20Gbps까지 훨씬 빠른 데이터 전송속도 제공을 목표로 함
  - 15GB(Giga-Byte) 사이즈의 고화질 영화 1편을 다운로드할 때 500 Mbps 속도의 최신 4G는 240초 소요되는 반면 20 Gbps 속도의 5G에서는 6초가 소요됨
  - 특히 기지국 근처에 신호가 센 지역 뿐만 아니라 신호가 약한 지역 (Cell Edge)에서도 100Mbps급의 속도를 제공하는 것을 목표로 하고 있음
  - 이렇게 되면 한 장소에 수만 명이 오가는 번화가나, 주요 경기가 열리는 경기장 같이 사용자가 밀집된 장소에서도 끊김없는 고화질 스트리밍 서비스가 가능할 것임
- 고신뢰/초저지연 통신(URLLC: Ultra Reliable & Low Latency Communications)
  - 로봇 원격 제어, 주변 교통 상황을 통신을 통해 공유하는 자율주행차량, 실시간 interactive 게임 등 실시간 반응 속도가 필요한 서비스를 대비하기 위한 것
  - 기존 수십 밀리 세컨드 (1ms = 1/1000 초) 걸리던 지연 시간을 1ms 수준으로 최소화하는 것을 목표로 하고 있음
  - 이를 위해 무선자원관리 분야나 네트워크 설계 등의 최적화를 진행하고 있음
  - 시속 100Km/h 자율 주행 차량이 긴급 제동 명령을 수신하는 데 걸리는 시간을 예로 들면 4G에서 50ms 지연 가정 시 1.4m 차량 진행 후 정지신호 수신하는 반면 5G에서 1ms 지연 가정 시 2.8cm 차량 진행 후 정지신호 수신하게 됨
- 대량연결 (mMTC: massive Machine-Type Communications)
  - mMTC는 수많은 각종 가정용, 산업용 IoT 기기들이 상호 연결되어 동작할 미래 환경을 대비하기 위한 것
  - 1km2 면적 당 1백만개의 연결(connection)을 지원하는 것을 목표로 기술 개발 및 표준화가 진행 중임
  - 참고로 4G LTE도 초기 상용화 시점 (2010년경) 당시에는 최대 속도가 75Mbps에 불과하여 4G의 최종 목표인 1Gbps 대비 1/10 도 안 되는 수준이었음(=7.5% 수준)
  - 최근에야 1Gbps를 지원하는 단말 칩이 출시되어 2018년에 1Gbps 상용이 가능했음

- 4G와 5G 특징 비교

기능	분류	4G	5G
초광대역 서비스(eMBB: enhanced Mobile Broadband)	최대 전송속도	1 Gbps	20 Gbps
고신뢰/초저지연 통신(URLLC: Ultra Reliable & Low Latency Communications)	전송지연	10 ms	1 ms
대량연결 (mMTC: massive Machine-Type Communications)	최대 기기 연결수	10^5 / km^2	10^6 / km^2

- Ericsson에 따르면 향후 관련 시장이 폭발적으로 성장하여 5G 산업의 활성화가 예상되는 '26년경 5G 기반의 ICT 산업 글로벌 매출이 U$1.3조에 달할 것으로 전망됨

3) 5G 기술 종류

(1) 빔포밍 기술

- 초고주파는 이전에 국제적으로 사용 빈도가 크지 않았었기 때문에 각 국가별로 광대역 확보가 상대적으로 용이하지만 물리적 특성상 낮은 주파수에 비해서 멀리까지 전파되지 못하고 장애물 등을 통과하는 투과력이 상대적으로 약한 특성이 있음
- 이러한 초고주파의 물리적 특성을 극복하기 위해 수십 개 이상의 많은 안테나를 활용하는 빔포밍(beamforming) 기술을 5G 표준 기술로 도입함
- 빔포밍(beamforming) 기술 특징
  - 많은 수의 안테나에 실리는 신호를 각각 정밀하게 제어하여 특정 방향으로 에너지를 집중시키거나, 또는 반대로 특정 방향으로 에너지가 나가지 않도록 조절이 가능한 기술
  - 전파의 에너지를 집중시켜 거리를 늘리고 빔(Beam)간에는 간섭을 최소화 시킬 수가 있음
  - 안테나를 많이 사용할수록 빔의 모양이 예리(sharp)해져서 에너지를 더 집중 시킬 수 있음
  - 단말이 빠르게 이동하는 경우 이렇게 예리한 빔을 계속 정확하게 추적(tracking)해야 하는 것이 기술적 관건이 됨

(2) Massive MIMO

- 4G에서도 MIMO 기술이 사용되었으나 적은 수의 안테나를 사용하여 빔이 예리하지 못해 사용자 구분에 한계가 있었음
- 1차원(1D) 안테나 배열을 사용하였기 때문에 자유도(degree of freedom)가 낮아 수평방향(horizontal)사용자만 구분하는데 그침
- 5G에서는 수십 개 이상의 안테나를 2차원(2D)으로 배치해 수직-수평(horizontal & vertical) 방향 모두 사용자를 구분할 수 있어 더 많은 다중사용자를 동시에 지원할 수 있는 규격을 제공함

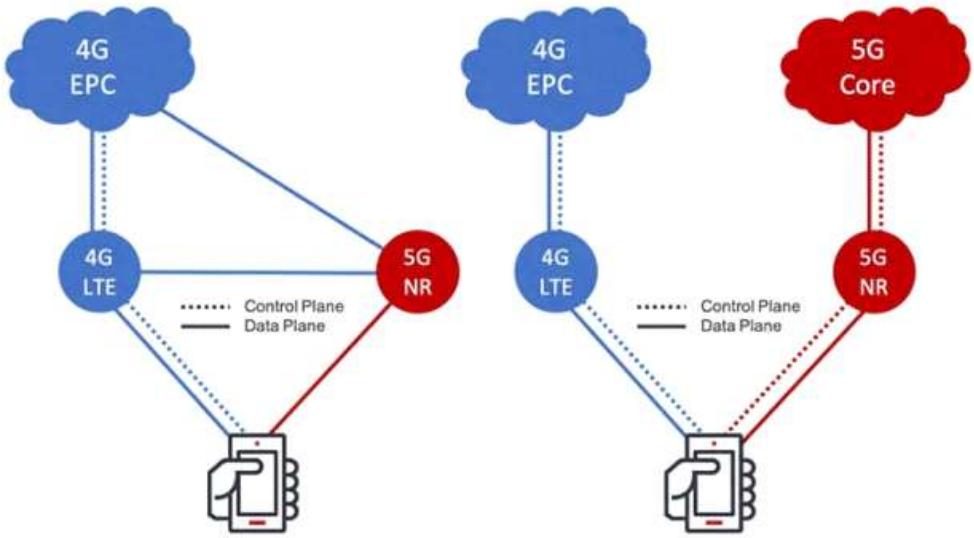
(3) Network Slicing

- 5G 표준에서는 네트워크 슬라이싱(Network Slicing) 기능과 품질(QoS: Quality-of-Service) 보장 기능을 통해서 서비스별 차별화를 제공함
- 4G에서는 Voice와 Data 서비스로 구분해서 Voice에 대해서만 별도의 QoS를 제공함
- Data 서비스 내에서는 모든 서비스들이 하나의 자원을 공유하므로 개별 서비스 간의 품질(QoS) 차별화가 불가능했음
- 5G에서는 네트워크 슬라이싱을 통해, 각각의 Data 서비스들도 독립적인 네트워크 자원 할당이 가능하고 따라서 각 서비스 별로 다른 서비스의 영향을 받지 않으면서 품질을 보장할 수 있음
- 특히, 이러한 독립적인 네트워크 자원할당을 통해 시간지연에 민감한 서비스(Mission Critical

Service)들의 품질을 보장할 수 있게 되어 이동통신 사업자는 특화 서비스에 대한 별도의 과금체계도 도입할 수 있음

(4) NSA(Non-Standalone) 구조와 SA(Standalone)

- 5G 표준에서는 4G에서 5G로의 진화를 위한 코어 네트워크를 NSA(Non-Standalone) 구조와 SA(Standalone) 구조를 모두 고려함
- NSA(Non-Standalone)
  - 초기 상용망에 구현될 것으로 예상되는 구조
  - 단말의 이동성(mobility) 관리 등을 담당하는 제어 플레인(control plane)의 동작은 4G LTE 망을 활용하면서 사용자 플레인(User plane/Data plane)에 해당하는 데이터 트래픽은 5G망으로 주고받음
- SA(Standalone) : 제어채널이나 데이터 채널 모두 5G의 자체 구조를 사용하는 구조
- 비자립형(NSA)형/자립형(SA) 구성도



4) 5G 통신망 분류 체계

- 이동통신망 : 무선접속망과 코어망으로 구성되며, 그 기능에 따라 5G 코어, 엣지컴퓨팅, 기지국, 무선 프론트홀/백홀, 중계기, 스몰셀, 테스트장비로 구분
  - 5G 코어
    - 5G 이동통신시스템의 코어망
    - 5G System Architecture에서 사용자 단말, 무선접속망, 데이터망을 제외한 전체 또는 일부 기능을 포함
  - 엣지컴퓨팅
    - 기지국에 분산 클라우드 컴퓨팅을 적용하여 다양한 서비스를 이용자 단말에 가까이 전개하여 시간 지연을 최소화하는 기술
  - 기지국
    - 5G 이동통신 기지국 장비로 5G 단말과 무선으로 연결되어 5G 코어망과의 통신 중계 역할을 함
    - 송수신기, RF/안테나 등으로 구분
  - 무선 프론트홀/백홀
    - 무선 백홀은 5G 이동통신망에서 기지국과 코어망 간 무선 데이터 전송을 제공하는 장비
    - 무선 프론트홀은 기지국의 RU와 DU 간 무선 데이터 전송을 제공하는 장비

- 중계기 : 이동통신 서비스가 제공되지 않는 전파 음영지역에 설치해 기지국과 단말기를 연결하는 장비
- 스몰셀 : 통상 수 km의 광대역 커버리지를 지원하는 매크로셀과는 달리 수십~수백m 정도의 소출력 커버리지를 갖는 소형 기지국
- 테스트장비 : 5G 시스템의 물리적 특성, 네트워크 대역폭, 전류 흐름 및 전기 신호를 측정하고 테스트하는데 사용되는 장비

● 전달망 : 분리형 기지국의 CU/DU와 코어망을 연결하는 백홀 네트워크로 광 전송장비, 패킷 교환장비, 광모듈/소재로 구분

- 광 전송장비
  - 광섬유 또는 공간 등을 전송매체로 하여 정보를 광으로 변환 후 한 곳에서 다른 곳으로 전송하는 방식을 사용하는 장치
- 패킷 교환장비 : 다수의 네트워크간 패킷 기반 전달 장비
- 광모듈/소재 : 광학 원시/검지기, 탐지기 등의 송수신 모듈과 광통신의 전송을 위해 사용되는 광섬유와 이를 이용한 케이블 등

● 액세스망 : 분리형 기지국의 AU/RU와 CU/DU를 연결하는 프론트홀 네트워크와 전화, 인터넷 등 유선 가입자의 단말장치로부터 통신국사를 연결하는 유선 액세스 장비로 구분

- 프론트홀 광전송장비 : 기지국의 무선 셀 사이트 장치 또는 무선 장치를 데이터 센터의 중앙에 있는 디지털 장치에 연결하는 광전송 장비
- 유선 액세스 장비 : 유선 가입자의 단말장치로부터 통신 국사를 연결하는 통신망 장비

5) 6G 개요

● 5G 성능 고도화, 네트워크 완전 지능화, 통신 커버리지 초월을 통해 가상과 현실을 시공간 제약 없이 연결하는 지능형 통신 인프라

● 6G 구현을 위해서는 5G의 요구사항인 초고속, 초저지연, 초연결의 확장과 함께 초공간, 초지능, 초신뢰라는 기술 특성이 더해짐

● 5G의 20GBPS 전송속도보다 50배 빠른 속도를 구현(1000GBPS) 할 수 있으며 1초당 1기가 바이트 데이터 전송 가능

● 5G와 6G 활용방안 비교

구분	5G	6G
실감 콘텐츠	모바일 AR, VR 방송	비대면 홀로그램 회의
자율주행차	차량 간 초저지연 통신	6G 위성으로 플라잉카 초저지연 통신
스마트시티	우체국 드론 택배	물류-교통 이동체에 대한 완전한 디지털 관제
스마트공장	유선 기반 제조설비라인의 무선화	산업형장 빅데이터 기반 설비 자동 정밀 제어
디지털 헬스케어	모바일을 통한 실시간 건강관리	원거리 원격 수술

2. 지능형 초연결망

1) 개요

● 4차 산업혁명시대는 센서, 단말기, 자율이동체 등 다양한 사물이 네트워크에 연결되어 방대한 데이터가 수집, 전송될 것으로 예상

- 단순연결을 넘어 엄청난 수의 사물, 사람, 데이터와 지능이 연결되는 네트워크의 초연결성이 중요한 핵심 기술임
- 지능형 초연결망은 4차 산업혁명의 핵심인프라로서 5G, IoT, SDN 등 신기술을 아우르는 네트워크 환경을 조성
- 일상생활에 필요한 모든 정적 및 동적객체를 연결하여 새로운 비즈니스를 창출하고 사회혁신을 촉진

2) 정의

- 지능형 초연결망은 모든 사람·사물을 신경망과 같이 유기적으로 구축하여 혁신적 서비스창출을 지원하는 초연결 네트워크
- 5G, IoT, Wi-Fi, vCPE(가상네트워크장비) 등의 네트워크 신기술이 SDN/NFV 기반의 지능형기술을 기반으로 제어 및 관리됨
- 신경망과 같이 모든 만물에서 대량의 정보를 지연없이 효율적이고 안전하게 지능정보시스템(AI/빅데이터/클라우드)와 연계

3) 필요성

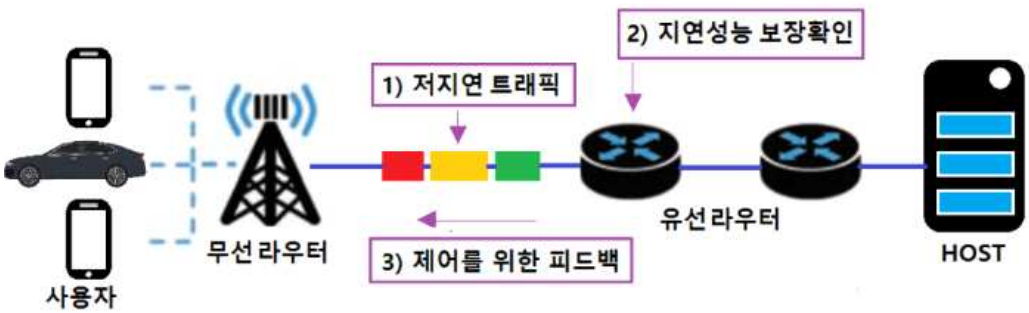
- 4차 산업혁명시대에 중요한 기반 인프라는 네트워크이며, 이를 위한 네트워크의 초연결성, 초고속/초저지연, 초지능화가 요구됨
- 소프트웨어 기반의 자동제어 및 운영이 가능하고, 언제 어디서나 유·무선 네트워크를 통해 사람과 사물을 연결해야 함
- 기하급수적으로 증가하는 네트워크 연결수요와 모바일트래픽을 관련기술의 개발 및 지원을 통해 경제적으로 처리해야 함
- 현실과 가상세계, 원격지와 근거리에서 촉각(1ms)수준의 동시반응을 구현하고, 인공지능으로 분석된 정보를 신속하게 적용 필요
- 초연결 네트워크를 통해 수많은 ICT인프라가 연결됨으로써, 우리의 삶을 획기적으로 변화시킬 새로운 융합서비스의 등장 요구

4) 구성 기술

- 초지능형 초연결망은 SDN(Software-Defined Networking), NFV(Network Functions Virtualization), 네트워크 지능기술, 초저지연/시간확정형 네트워크 기술, 양자정보통신기술, 전달망기술 등이 포괄적으로 포함
- SDN 기술
  - 소프트웨어기술을 활용하여 네트워크를 지능화하고 중앙에서 제어하거나 프로그래밍 할 수 있는 네트워크 아키텍처 기술
  - 네트워크의 제어부(Control Plane)와 전송부(Data Plane)를 분리하고 네트워크 장치는 전송부의 기능만 유지하고, 범용서버에 제어부의 기능을 분리 부여하여 여러 개의 네트워크 장치를 제어
  - 개방형 API를 사용하여 소프트웨어적으로 네트워크를 제어함으로써 다양한 융복합 서비스를 위한 최적화된 환경을 구축

- SDN 기술 개념도

- NFV 기술
  - 기존에 하드웨어에서 실행되었던 라우터, 방화벽(Firewall)이나 로드밸런서 (Load Balancer) 같은 네트워크 장비를 가상화
  - 네트워크 기능을 가상화함으로써, 하나의 물리적인 네트워크 기능을 여러 사용자 또는 장치가 나누어 사용할 수 있음
  - 통신사업자들이 사용하고 있는 네트워크 장비내의 네트워크 서비스기능을 하드웨어 전용장비로부터 범용서버로 분리
  - 소프트웨어적으로 유연하게 제어 및 관리가 가능함으로써 안정성 및 상호 운용성 향상
- 네트워크 지능기술
  - 융합 네트워크가 실시간으로 다양한 기능을 동시에 수행함에 따라, 개별·수동제어방식에서 자율성 기반의 자동운용으로 변화 필요
  - 인공지능기술을 이용하여 자율의사/정책결정(Self-Decision/Policy Making) 방식을 통해 네트워크 자원(물리/가상)을 자동적으로 설정, 제어, 관리하는 기술
  - 수동적 네트워크 제어, 운용 및 관리기술을 인공지능기술을 기반으로 자율의사 결정방법에 따라 완전 자동화방식으로 변환
  - 다양한 데이터의 분석을 통해 네트워크 및 IT 자원을 항상 최적으로 유지하여 비용절감과 동시에 신규 비즈니스 발굴도 용이
- 초저지연 및 시간확정형 네트워크 기술
  - 일반 트래픽이 혼재된 패킷 네트워크에서 실시간 민감형 통신 및 원격제어, 계측 등을 위해 패킷전달 지연시간을 확정할 수 있는 통신기술
  - 청각, 시각적 신호의 전달을 넘어 촉각 등 공감각적인 Tele-presence가 가능한 실감형 서비스를 제공하기 위해 초저지연 트래픽의 QoS를 만족시킬 네트워크 필요
  - 실시간 정밀한 작업이 요구되는 스마트공장 원격제어, 원격의료, 원격드론제어, 원격가상현실, 홀로그램 등 미래 실감통신 분야에서 활용
  - 저-지연을 위한 네트워크 피드백 구조



- 양자 정보통신기술(Quantum IT)
  - 양자적 특성을 정보통신에 적용하여 보안, 초고속 연산 등 기존 정보통신의 한계를 극복할 수 있는 차세대 정보통신기술
  - 양자역학적 특성을 이용하여 양자암호의 양자 암호키분배(QKD: Quantum Key Distribution)를 통한 안전하고 신뢰성 있는 통신
  - 양자역학적 상태를 이용해 통신보안 수준을 고도화 한 양자암호통신, 초고속 연산이 가능한 양자컴퓨터 부문으로 발전
  - 양자정보통신의 개념

- 전달망 기술
  - 메트로 및 장거리 통신망에서 L0에서 L2까지의 전송 및 스위칭 기술
  - 기간통신망 요구수준의 대용량 광전송 및 망 관리/유지보수, 장애 시 50㎳이내 복구, 고정밀 망 동기 등이 지원되는 네트워크 기술

3. IoT 기술 및 프로토콜

1) 개요

- IoT 서비스는 디바이스(Device)/센서(Sensor), 네트워크(Network), 플랫폼(Platform), 클라이언트(Client)/서비스(Service)로 구성
- 사물인터넷 서비스는 각종 센서(디바이스)에서 시작
- 센서를 통해 측정된 다양한 데이터는 Wi-Fi 및 이동통신 등의 네트워크 통신 기술을 통해 플랫폼(미들웨어) 서버에 전달
- 플랫폼 서버는 센서를 통해 수집한 데이터를 취합, 분류, 분석하여 의미있는 정보를 생성
- 이를 고객(Client) 혹은 응용 서비스(Service)에 제공
- IoT 서비스/기술 구성 요소 (D-N-P-C)

2) IoT 프로토콜

(1) 저전력, 단거리 네트워크

- 저전력, 단거리 네트워크는 가정, 사무실, 기타 소규모 환경에 적합
- 소형 배터리가 필요한 경향을 보이며 일반적으로 작동 비용이 저렴
- Bluetooth : 고속 데이터 전송에 적합한 Bluetooth는 음성 및 데이터 신호를 최대 10미터까지 전송
- NFC : 4cm(1.5인치) 이하의 거리에서 두 전자 디바이스 간에 통신할 수 있게 해주는 통신 프로토콜 세트
- Wi-Fi/802.11
  - Wi-Fi는 작동 비용이 저렴하여 가정과 사무실에서 표준이 되고 있으나 범위가 제한되어 있ㅇ,ㅁ
  - 연중무휴로 에너지를 소비하기 때문에 모든 시나리오에 적합하지는 않을 수도 있음
- Z-Wave : 저에너지 전파를 사용하여 어플라이언스 간에 통신하는 메시 네트워크
- Zigbee : 소형 저전력 디지털 라디오를 사용하여 개인 영역 네트워크를 만드는 데 사용되는 고급 통신 프로토콜 모음에 대한 IEEE 802.15.4 기반 사양

(2) LPWAN(저전력 광역 네트워크)

- LPWAN은 최소 500미터 범위에서 통신할 수 있게 해주며 최소한의 전력이 필요하고 대부분 IoT 디바이스에 사용
- 4G LTE IoT : 높은 용량과 짧은 대기 시간을 제공하는 이 네트워크는 실시간 정보나 업데이트가 필요한 IoT 시나리오에 적합
- 5G IoT : 5G IoT 네트워크는 지정된 지역에서 더 많은 디바이스에 훨씬 더 빠른 다운로드 속도와 연결을 제공
- Cat-0 : LTE 기반 네트워크로 가장 저렴한 비용 옵션으로, 2G를 대체할 기술인 Cat-M의 토대를 마련
- Cat-1 : 셀룰러 IoT에 대한 표준으로 기존 3G를 대체
- LoRaWAN : LoRaWAN(장거리 광역 네트워크)은 배터리로 작동하는 양방향 보안 모바일 디바이스를 연결
- LTE Cat-M1 : LTE 네트워크와 완전히 호환되며, IoT 애플리케이션용으로 특별히 설계된 2세대 LTE 칩에서 비용과 전력을 최적화
- 협대역 또는 NB-IoT/Cat-M2 : NB-IoT/Cat-M2는 DSSS(직접 시퀀스 확산 스펙트럼) 변조를 사용하여 서버에 직접 데이터를 보냄으로써 게이트웨이의 필요성을 없애줌
- Sigfox
  - Cellular 및 WiFi 속성을 모두 포함하는 최고의 대체 기술 중 하나
  - 낮은 수준의 데이터를 전송하기 위해 초당 10~1000비트의 속도를 유지하고 50마이크로와트의 전력만 소비

(3) 애플리케이션 계층에서의 IoT 프로토콜

- AMQP(고급 메시지 큐 프로토콜)
  - 메시징 미들웨어 간의 상호 운용성을 만드는 소프트웨어 계층
  - 이 계층을 통해 다양한 시스템과 애플리케이션이 함께 작동하여 산업형 규모에서 표준화된 메시징을 만들 수 있음
- CoAP(제한된 애플리케이션 프로토콜)
  - 용량이 제한된 디바이스가 머신 간 통신에서 연결하도록 설계된 제한된 대역폭 및 제한된 네트워크 프로토콜
- DDS(데이터 분산 서비스)
  - 소형 디바이스를 실행하는 것부터 고성능 네트워크를 연결하는 것까지 모든 작업을 수행하는

다목적 피어 투 피어 통신 프로토콜

- MQTT(메시지 큐 원격 분석 전송)
  - 경량 머신 간 통신용으로 설계된 메시징 프로토콜
  - 주로 원격 위치에 대한 저대역폭 연결에 사용되며 MQTT는 게시자-구독자 패턴을 사용하며 효율적인 대역폭과 배터리 사용이 필요한 소형 디바이스에 적합

학습정리

1. 5G : 4G 대비 초고속, 저지연, 초연결을 제공하는 통신기술로 이를 활용하여 스마트시티, 자율주행차, 지능형 CCTV 등 다양한 서비스 제공이 가능
2. 5G 기술 진화 방향 : 초광대역 서비스(eMBB: enhanced Mobile Broadband), 고신뢰/초저지연 통신(URLLC: Ultra Reliable & Low Latency Communications), 대량연결 (mMTC: massive Machine-Type Communications)
3. 5G 기술 종류 : 빔포밍 기술, Massive MIMO, Network Slicing, NSA(Non-Standalone) 구조와 SA(Standalone)
4. 6G : 5G 성능 고도화, 네트워크 완전 지능화, 통신 커버리지 초월을 통해 가상과 현실을 시공간 제약 없이 연결하는 지능형 통신 인프라
5. 지능형 초연결망 : 모든 사람·사물을 신경망과 같이 유기적으로 구축하여 혁신적 서비스창출을 지원하는 초연결 네트워크
6. 지능형 초연결망 구성 기술 : SDN(Software-Defined Networking), NFV(Network Functions Virtualization), 네트워크 지능기술, 초저지연/시간확정형 네트워크 기술, 양자정보통신기술, 전달망 기술

참고문헌

- 컴퓨터 네트워크(이재광, 김봉한, 생능출판, 2021년)
- 네트워크 개론(진혜진, 한빛아카데미, 2019년)