1. OSI 모델
   1. 데이터 통신의 단계 구성도
   2. 데이터 통신을 단계로 나누어 각 단계의 순서를 명확히 함.
   3. 이 모델에 따라 프로토콜을 정의
   4. 각 계층 -> 위의 계층 지원, 특정 기능 수행
2. 네트워크 기초
   1. 네트워크는 컴퓨터와 컴퓨터가 그물망처럼 통신 매체로 연결되어 데이터를 운반하는 것
   2. 네트워크 인터페이스 카드(NIC)를 통해 연결됨
   3. NIC는 물리적 계층에서 작동
   4. Mac주소
      1. Ip주소와 반대되는 물리적 주소
      2. NiC에서 16진수로 할당됨
      3. 네트워크 내의 식별에 사용되는 레이어2의 주소
   5. DNS서버
      1. 도메인 이름(URL)을 IP주소로 변환
   6. 허브
      1. 가장 간단한 네트워크 연결 장치
      2. 간단한 네트워크 생성
      3. 레이어 1 장치(물리적 레이어)
   7. 스위치
      1. 허브에서 진화된 형태
      2. 의도한 컴퓨터에게만 패킷을 전송한다
      3. 계층 2 장치(링크 계층)
   8. 라우터
      1. 스위치에서 더 발전
      2. 의도된 네트워크의 트래픽을 제한가능
      3. 계층 3장치(네트워크 계층)
   9. 데이터 전송 방법
      1. 패킷이 전송됨
         1. 패킷(데이터그램)
            1. 바이트로 구성
            2. 헤더와 바디로 나뉨

헤더

패킷이 어디로 가는지 알려줌

네트워크 기기 -> 헤더 읽어 패킷 전송 위치 결정

헤더 구성 요소(IP)

버전 – IPv4, IPv6

IP 헤더의 길이

서비스 유형 – DSCP

데이터그램의 크기

ID 정보 – 패킷의 ID

IP계층에서 패킷이 쪼개질 수 있다

쪼개질 때 구분하는 값 – ID정보

플래그

프래그먼트 오프셋

생존 기간

프로토콜 번호

헤더 체크섬

보낸 사람 IP주소

받는 사람 IP주소

옵션

* 1. 프로토콜
     1. 네트워크 및 인터넷 통신을 제어하는 규칙
        1. IETF(국제 인터넷 표준화 기구)가 프로토콜을 관리한다
     2. 용도별로 다른 규칙이 있다
     3. 이러한 개념 의사소통 규칙과 유사, (부모님과 소통하는 방식과 친구들과 소통하는 방식이 다른 것 처럼)
     4. TCP(전송 제어 프로토콜)는 Connection Oriented
        1. 1:1로 연결 상태를 유지하여 통신
     5. IP(인터넷 프로토콜), UDP(사용자 데이터그램 프로토콜)는 Connectionless
        1. 연결 상태 유지 X
        2. 주소를 가지고 다음 라우터나 목적지로 전달만 하여 데이터그램에 관여 X
        3. TCP와 UDP차이점
           1. TCP는 통신하는 컴퓨터와 REQUEST와 RESPONSE를 주고받아(THREE WAY HANDSHAKE) 정확, 확실하게 통신함
           2. UDP는 RESPONSE를 받을 때까지 기다리지 X
           3. UDP는 시계 설정 등에 매우 적합
     6. ICMP(인너텟 저어 메시지 프로토콜)는 네트워크상의 문제를 장치에 알릴 때 사용
  2. 포트
     1. 연결점
        1. 컴퓨터의 물리적 포트가 아님(USB단자 이런게 X)
     2. 통신 경로의 숫자로 이루어진 목적지
     3. 프로토콜이 통신하기 위해 사용

1. 인터넷
   1. 인터넷에 연결하기 위해서는 ISP(인터넷 서비스 공급자, KT같은 것)에 등록해야함
   2. ISP는 다른 ISP와 연결하거나 BACKBONE제공자(세계적인 수준의 ISP)와 연결한다.
   3. 또 BACKBONE제공자는 또다른BACKBONE제공자와 연결
   4. IP(인터넷 프로토콜) 주소
      1. 인터넷 탐색에 필요
      2. 고유 식별자
      3. 보통 이진수로 표현
      4. 10진수로 구분된 4개의 옥텟(섹션)으로 구성
   5. 공용 IP 주소 VS 개인 IP 주소
      1. 공용 주소는 인터넷에서 라우팅 할 수 있다.
         1. 라우팅 - 어떤 네트워크 안에서 통신 데이터를 보낼 때 최적의 경로를 선택하는 과정
         2. ISP에서 임대해야 함.
      2. 개인 주소는 인터넷에서 라우팅 할 수 X
         1. PRIVATE 네트워크 내에서만 사용
   6. 네트워크 클래스
      1. IP주소의 각 옥텟은 특정한 것을 의미
      2. 첫번째 옥텟은 IP가 속하는 클래스를 정의
   7. IP주소의 효용성
      1. IP주소는 무한대로 존재하지 X
      2. IPv4는 IPv6로 대체된다
      3. 서브넷
         1. 커다란 네트워크 안에 작은 네트워크를 만들 수 있는데 이렇게 분할된 작은 네트워크를 말함
         2. 서브넷 마스크는 어디까지가 서브넷 번호인지를 설명한다.
   8. IPv6
      1. 128bit의 주소
      2. IPv4대비 헤더의 크기가 켜졌으며 사라진 요소와 바뀐 요소 새로 생긴 요소가 있다.
   9. URL(Uniform Resource Locator)
      1. 웹 사이트를 쉽게 기억할 수 있는 방법
      2. DNS(Domain Name Server)에 의해 IP로 번역되어 웹사이트에 연결
      3. 웹사이트에서 오류메세지를 보낼 수 있다.
         1. 오류메세지
            1. 100 대 시리즈 – 정보
            2. 200 대 시리즈 – 연결의 성공을 의미하기에 평소에는 보이지 X
            3. 300 대 시리즈 – 웹사이트로의 재연결
            4. 400 대 시리즈 – 클라이언트 오류
            5. 500 대 시리즈 – 서버 오류
2. 기본 네트워크 유틸리티
   1. Ipconfig
      1. 시스템에 대한 정보 제공
         1. ip주소
         2. 서브넷 마스트
         3. 기본 게이트웨이
      2. cmd에 ipconfig 입력
      3. 다른 커맨더 사용하려면
      4. Ipconfig -?을 입력하면 다른 옵션들이 보임
      5. Ipconfig/all이 가장 흔함
   2. Ping
      1. 시스템이 네트워크에 연결되어 있는지의 여부를 알려줌
      2. 패킷이 대상 호스트에 도착하는 시간 알려줌
      3. 해커는 어떤 사용자에게 해킹을 할 수 있는 지 결정할 때 씀.
   3. Tracert
      1. Ping의 고급 버전
      2. Ping과 동일한 구문을 사용한다
      3. 호스트와 대상 주소 사이의 모든 hop을 표시
         1. Hop - 출발지와 목적지 사이에 위치한 경로의 한 부분
      4. 기술자와 해커 모두에게 유용한 툴
3. 다른 네트워크 기기
   1. 방화벽
      1. 하드웨어 또는 소프트웨어로 존재
      2. 패킷이 네트워크에 진입할 때 필터링을 함
      3. 허용되지 않는 패킷은 거부함
   2. 프록시 서버
      1. 네트워크를 위장하는 데 사용
      2. 인터넷에 접속하는 다른 호스트의 ip주소로 대체