

Library Technologies:

Computer, Internet, Database, Networking

DATA COMMUNICATION AND COMPUTER
NETWORK

Contents

1. OVERVIEW

Classification of Computer Networks

Geographical Span

Inter—Connectivity

Administration

Network Architecture

Network Applications

2. TYPES OF COMPUTER NETWORKS

Personal Area Network

Local Area Network

Metropolitan Area Network

Wide Area Network

Internetwork

3. NETWORK LAN TECHNOLOGIES

Ethernet

Fast—Ethernet

Giga—Ethernet

Virtual LAN

4. COMPUTER NETWORK TOPOLOGIES

Point—to—Point

Bus Topology
Star Topology
Ring Topology
Mesh Topology
Tree Topology
Daisy Chain
Hybrid Topology

5. COMPUTER NETWORK MODEL

Layered Tasks
OSI Model
Internet Model

6. COMPUTER NETWORK SECURITY

Secret Key Encryption
Public Key Encryption
Message Digest

7. PHYSICAL LAYER INTRODUCTION

Signals
Transmission Impairment
Transmission Media
Channel Capacity
Multiplexing
Switching

8. DIGITAL TRANSMISSION

Digital-to-Digital Conversion

Line Coding

Unipolar Encoding

Polar Encoding

Bipolar Encoding

Block Coding

Analog-to-Digital Conversion

Sampling

Quantization

Encoding

Transmission Modes

9. ANALOG TRANSMISSION

Digital-to-Analog Conversion

Analog-to-Analog Conversion

10. TRANSMISSION MEDIA

Magnetic Media

Twisted Pair Cable

Coaxial Cable

Power Lines

Fiber Optics

11. WIRELESS TRANSMISSION

Radio Transmission

Microwave Transmission

Infrared Transmission

Light Transmission

12. MULTIPLEXING

Frequency Division Multiplexing

Time Division Multiplexing

Wavelength Division Multiplexing

Code Division Multiplexing

13. SWITCHING

Circuit Switching

Message Switching

Packet Switching

14. DATA LINK LAYER INTRODUCTION

Functionality of Data-link Layer

15. ERROR DETECTION AND CORRECTION

Types of Errors

Error Detection
Error Correction

16. DATA LINK CONTROL AND PROTOCOLS

Flow Control
Error Control

17. NETWORK LAYER INTRODUCTION

Layer-3 Functionalities
Network Layer Features

18. NETWORK ADDRESSING

19. NETWORK ROUTING

Unicast routing
Broadcast routing
Multicast Routing
Anycast Routing
Unicast Routing Protocols
Multicast Routing Protocols
Routing Algorithms

20. INTERNETWORKING

Tunneling

Packet Fragmentation

21. NETWORK LAYER PROTOCOLS

Address Resolution Protocol (ARP)

Internet Control Message Protocol (ICMP)

Internet Protocol Version 4 (IPv4)

Internet Protocol Version 6 (IPv6)

22. TRANSPORT LAYER INTRODUCTION

Functions

End-to-End Communication

23. TRANSMISSION CONTROL PROTOCOL

Features

Header

Addressing

Connection Management

Bandwidth Management

Error Control and Flow Control

Multiplexing

Congestion Control

Timer Management

Crash Recovery

24. USER DATAGRAM PROTOCOL

Requirement of UDP

Features

UDP Header

UDP application

25. APPLICATION LAYER INTRODUCTION

26. CLIENT–SERVER MODEL

Communication

27. APPLICATION

PROTOCOLS

Domain Name System

Simple Mail Transfer Protocol

File Transfer Protocol

Post Office Protocol (POP)

Hyper Text Transfer Protocol (HTTP)

28. NETWORK SERVICES

Directory Services

File Services

Communication Services

Application Services

I. OVERVIEW

서로 연결된 컴퓨터들과 프린터와 같은 주변기기의 시스템을 컴퓨터 네트워크라고 부른다. 이러한 상호연결을 통하여 컴퓨터들은 정보를 원활하게 공유한다. 컴퓨터들은 무선이나 유선 매체로 서로 연결될 수 있다.

1. Classification of Computer Networks

컴넷은 여러 가지 요소를 근거로 분류될 수 있으며, 그 요소들은 다음과 같다:

- . Geographical span: 지리적 범위
- . Inter-connectivity: 상호 연결성
- . Administration: 운영주체
- . Architecture: 구조

1)Geographical Span

지리적으로 넷은 다음과 같은 범주들 중의 하나라고 여겨질 수 있다;

- . 책상 위에서 블루투스 사용기기들 간에 이루어지는 2-3 미터 내의 범위
- . 모든 층을 연결하기 위한 중계기의 경우에는 건물 전체.
- . 도시 전체
- . 복수의 도시나 지역
- . 전 세계

2)Inter-Connectivity

넷의 구성요소는 연결성에 따라, 논리적, 물리적, 또는 두 가지 혼합방식으로 나눈다.

- . 모든 단일 기기는 넷망을 구성하기 위하여 넷상의 모든 다른 기기에 연결될 수 있다.
- . 지리적으로는 분리되어 있는 경우에는 버스형 구조로 만들어 모든 기기를 단일 매체에 연결할 수 있다.
- . 각 기기를 선형 구조를 만들기 위해서는 단지 그것의 왼쪽과 오른쪽에 있는 peers 에 연결되어야 한다.
- . 모든 기기가 단일기기에 함께 연결되면, 스타형 구조를 만들 수 있다.
- . 모든 기기를 하이브리드형 구조를 만들기 위해서는 모든 위의 방식으로 서로를 연결되어야 한다.

3)Administration

행정이 입장에서 넷은 하나의 독립 시스템에 속하는 사적 넷일 수 있으므로, 그것의 물리적 또는 논리적 영역 밖에서는 접근할 수 없어야 한다. 넷이 모두에 의해 접근 가능하다면 그것은 공용 넷이다.

4)Network Architecture

컴넷은 그것의 구조에 따라서, Client-Server, peer-to-peer, hybrid 와 같이 다양한 종류로 구별할 수 있다.

- . 서버로서 활동하는 하나 이상의 시스템이 있을 수 있다. 클라이언트는 리퀘스트를 처리하도록 서버에 요청한다. 서버는 클라이언트 대신에 그러한 리퀘스트를 받아서 처리한다.
- . 두 개의 시스템은 Point-to-Point 또는 back-to-back fashion 으로 연결될 수 있다. 이 두 시스템 모두는 동일한 수준에서 활동하며, peers 라 부른다.
- . 위에서 살펴본 두 가지 넷 구조 모두를 포함하는 하이브리드형 넷이 존재할 수 있다.

2. Network Applications

컴퓨터 시스템과 주변기기들은 하나의 넷을 형성하기 위하여 연결되어야 한다. 이것들의 장점은 다음과 같다

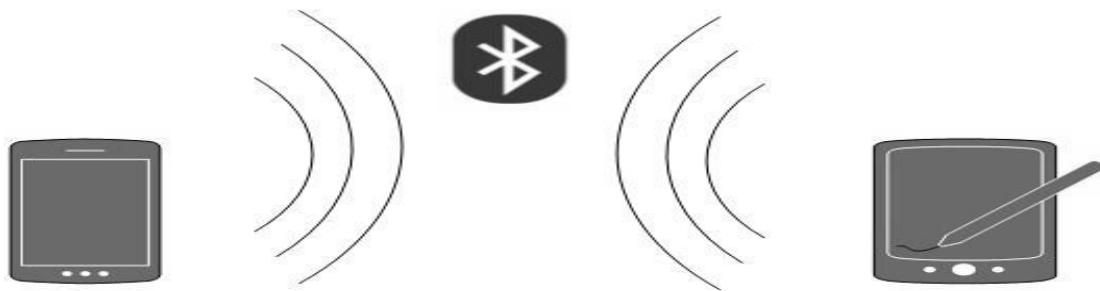
- . 프린터와 저장기와 같은 자원의 공유
- . 전자우편과 FTP 를 사용하여 정보를 교환
- . 웹이나 인터넷을 사용하여 정보를 공유
- . 역동적인 웹 페이지를 사용함으로써 다른 사람과의 의사전달
- . IP 전화
- . 비디오 회의
- . 병렬식 컴퓨팅
- . 즉시형 메시지

II. TYPES OF COMPUTER NETWORKS

일반적으로, 넷은 지리적 폭을 근거로 구분된다. 넷은 여러분의 휴대폰과 블루투스 헤드폰 사이의 거리만큼 짧을 수도 있고 전세계를 포함하는 인터넷처럼 길 수도 있다.

1. Personal Area Network

PAN은 사용자에게 매우 개인적인 가장 작은 넷이다. 이것에는 블루투스 기기나 적외선 기기와 같은 것이 포함될 수 있다. PAN은 10미터 정도의 연결 범위를 가지고 있다. PAN에는 무선 컴퓨터 키보드와 마우스, 블루투스 헤드폰, 무선 프린터, TV 리모콘 등이 포함된다.

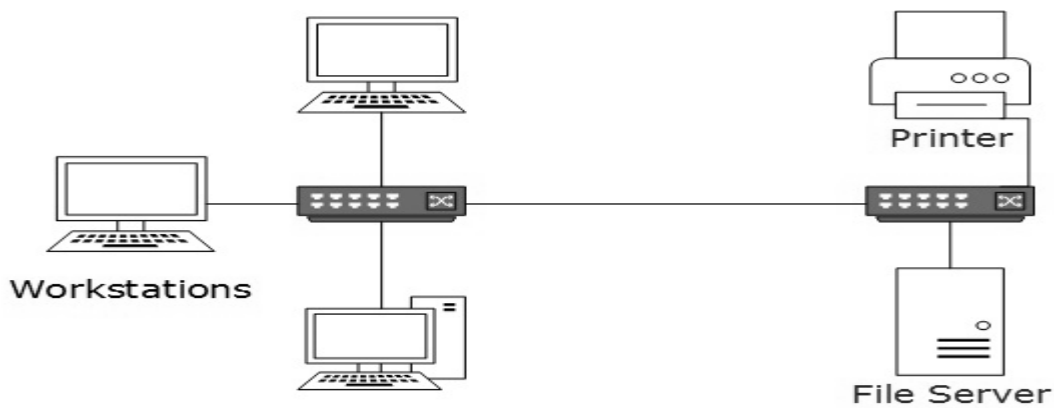


Personal Area Network

2. Local Area Network

어떤 컴넷은 그 범위가 빌딩 내부이며, LAN이라고 부르는 단일 행정 시스템에서 사용한다. 대체로, LAN은 사무실, 학교, 대학교에서 사용하고 있다. LAN에 연결된 시스템의 수는 최소한 2개에서부터 최대한 1600만개까지 다양한다.

LAN은 최종이용자들 간에 자원을 공유하는 유용한 방법을 제공한다. printers, file servers, scanners, internet과 같은 자원들은 쉽게 컴퓨터들 간에 공유될 수 있다.



Local Area Network

LAN 은 저렴한 네트워킹과 라우팅 장비로 구성된다. 여기에는 파일 저장과 기타 지엽적으로 공유된 어플을 다루는 로컬 서버가 포함되기도 한다. 이것들은 대부분이 사설 IP 어드레스에서 운영되며, heavy routing 은 이루어지지 않는다. LAN 은 그것 자체의 로컬 도메인에 따라 운영되며 중앙방식으로 통제한다.

LAN 은 Ethernet 또는 Token-ring 기술을 사용한다. 이더넷은 가장 많이 사용되는 LAN 기술이며 스타 형태를 갖추고 있으나, Token-ring 은 찾아보기가 매우 힘들다.

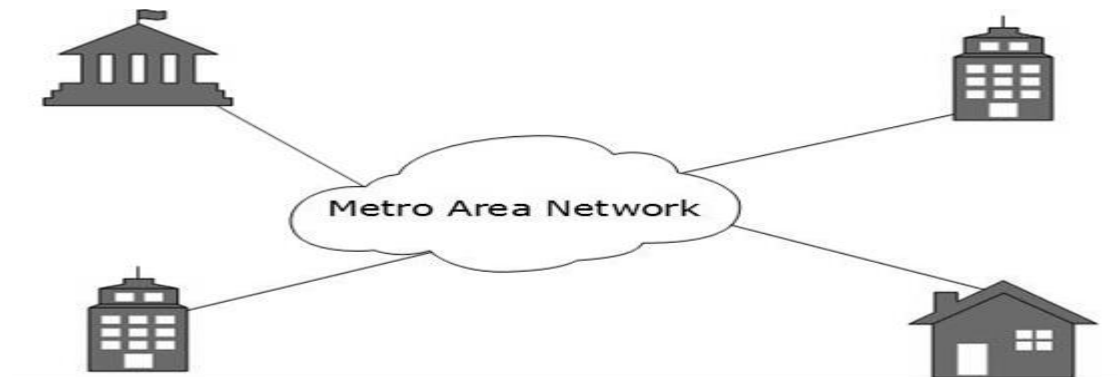
LAN 은 무선, 유선, 또는 이들 두 가지 모두를 사용할 수 있다.

3. Metropolitan Area Network

MAN 은 일반적으로 케이블 TV 네트워크처럼 한 도시 전체를 대상으로 한다. 이것은 Ethernet, Token-ring, ATM, 또는 Fiber Distributed Data Interface (FDDI)의 형태로 구성된다.

- 1) ATM(Asynchronous Transfer Mode) - 비동기전달모드로, 음성, 데이터, 비디오 신호를 전달하기 위한 표준이다. PSTN(public switched telephone network)과 ISDN(Integrated Services Digital Network)의 백본으로 사용된 핵심 프로토콜이지만, 최근에는 Internet Protocol(IP)로 인하여 쇠퇴하였다.
- 2) FDDI - 최장 200km 까지 연장이 가능한 근거리통신망의 광케이블 데이터 전송 표준이며, 토큰 링에 기반하고 있다.

Metro Ethernet 은 ISPs 에서 제공되는 서비스이다. 이 서비스를 이용하면 이용자는 자신의 LAN 을 확장시킬 수 있다. 예를 들어, MAN 은 한 도시에 있는 기업의 모든 사무실들을 연결시킬 수 있다.

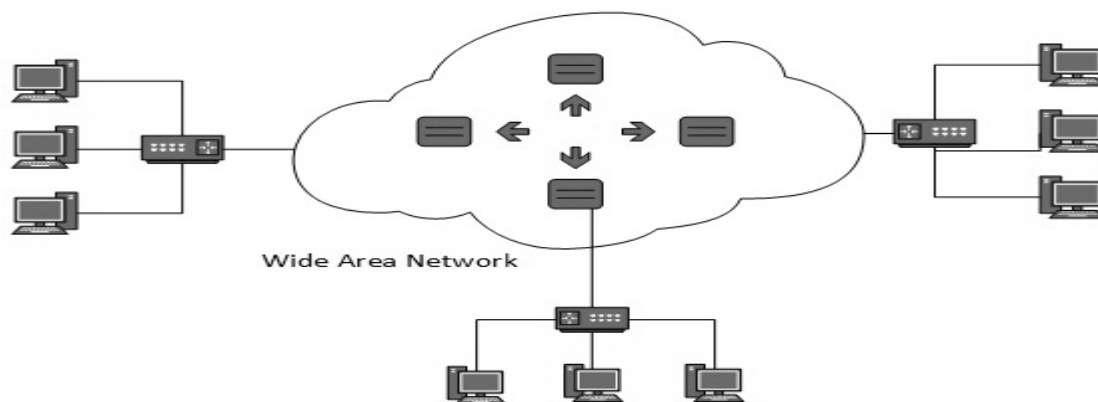


Metropolitan Area Network

MAN의 백본은 고용량이며 고속인 광섬유이다. MAN은 LAN과 WAN 사이에서 활동한다. MAN은 WANs나 인터넷으로 LANs용 uplink를 제공한다.

4. Wide Area Network

이 이름이 의미하듯이, WAN은 지역을 넘어 심지어 국가 전체를 그 범위로 설정할 만큼 넓은 지역을 담당한다. 일반적으로 텔레콤 넷은 WAN이다. 이 넷들은 MANs와 LANs으로 연결할 수 있다. 이것들은 초고속의 백본을 갖추고 있으므로, 매우 값비싼 넷 장비를 사용한다.



Wide Area Network

WAN은 Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Network (SONET)와 같은 첨단 기술을 사용하기도 한다. WAN은 복수로 관리되기도 한다.

- 3) Frame Relay – packet switching 방식을 사용하는 디지털 텔레콤 채널의 물리적 및 논리적 link layers 를 특정화시키는 표준화된 WAN 기술이다.

5. Internetwork

넷들의 넷을 인터넷이라 부른다. 이것은 지구상에 존재하는 가장 커다란 넷이다. 인터넷은 대규모로 모든 WANs 를 연결하고 있으며 LANs 와 Home 넷에도 연결될 수 있다. 인터넷은 TCP/IP protocol suite 를 사용하며 자신의 어드레싱 프로토콜로 IP 를 사용한다. 오늘날, 인터넷은 IPv4 를 널리 사용하고 있으나, Address spaces 의 단점으로 인하여, 점차적으로 IPv4 에서 IPv6 로 옮겨가고 있다.

인터넷은 사용자로 하여금 많은 양의 정보를 공유하고 접근할 수 있도록 하고 있다. 이것은 WWW, FTP, email services, audio, video streaming 등에서 사용하고 있다. 크게 보면, 인터넷은 클라이언트-서버 모델로 기동하고 있다.

인터넷은 초고속의 광섬유 백본을 사용한다. 여러 대륙을 서로 연결하기 위하여, 광섬유가 바다 속에 깔려있는데, 이것을 우리는 submarine communication cable 이라 부른다.

인터넷은 HTML linked pages 를 사용하는 WWW 서비스를 널리 채택하고 있으며, 웹 브라우저로 알려진 클라이언트 소프트웨어로 접근할 수 있다. 사용자가 웹 브라우저를 사용하여 전세계의 어디에 있는 어떤 웹 서버에 들어 있는 어떤 페이지를 요청할 때, 그 웹 서버는 적합한 HTML 페이지로 응답한다. 이것의 통신 지연을 매우 낮다.

인터넷은 많은 프로포즈를 처리하며, 우리의 삶과 많이 관련되어 있다. 이것들 중 몇 가지는 다음과 같다:

- . Web sites
- . E-mail
- . Instant Messaging
- . Blogging
- . Social Media
- . Marketing
- . Networking
- . Resource Sharing
- . Audio and Video Streaming

III. NETWORK LAN TECHNOLOGIES

다양한 LAN 기술에 대하여 간단하게 살펴보기로 한다:

1. Ethernet

이더넷은 널리 채택되고 있는 LAN 기술이다. 이 기술은 1970 년에 Bob Metcalfe & D.R. Boggs 에 의해 개발되었으며, 1980 년에 IEEE 802.3 으로 표준화되었다. 이더넷은 미디어를 공유한다. 공유된 미디어를 사용하는 넷은 데이터 충돌의 확률이 높다. 이더넷은 Carrier Sense Multi Access/Collision Detection (CSMA/CD) 기술을 사용하여 이러한 충돌을 감지한다. 이더넷에서 충돌이 발생하면, 그것의 모든 호스트들이 roll back 하여 무작위적으로 짧은 시간 동안 기다린 다음, 해당 데이터를 재전송한다.

이더넷 코넥터는 48-bits MAC address 로 된 네트워크 인터페이스이다. 이것은 다른 이더넷 기기들이 이더넷에서 원거리 기기를 식별하여 통신하는 것을 도와준다.

- 4) MAC address – Media Access Control address. 물리적 넷 세그먼트에서 통신용으로 사용되는 넷 인터페이스에 배정된 유일한 식별 코드이며, 이더넷과 와이파이에서 넷 어드레스로 사용된다.

전통적인 이더넷은 10BASE-T specifications 을 사용한다. 번호 10 은 10MBPS 속도를 의미하며, BASE 는 baseband 를 뜻하고, T 는 Thick Ethernet 를 뜻한다. 10BASE-T Ethernet 은 10MBPS 까지의 전송속도를 제공하며 RJ-5 코넥터와 더불어 동축케이블이나 Cat-5 twisted pair cable 을 사용하기도 한다. 이더넷은 세그먼트 길이가 100 미터까지인 스타형태를 갖는다. 모든 기기들은 하나의 허브/스위치에 스타 모양으로 연결된다.

- 5) Baseband – 매우 좁은 범위의 주파수를 가지고 있는 시그널

2. Fast-Ethernet

새로운 소프트웨어와 하드웨어의 기술에 의한 요구에 따라, 이더넷은 Fast-Ethernet 으로 확장되었다. 이것은 UTP(Unshielded twisted pair cable), Optical Fiber, 또는 wirelessly 로도 운영될 수 있다. 이것은 100MBPS 까지의 속도를 제공하며, 이것의 표준은 Cat-5 twisted pair cable 를 사용할 경우, IEEE 803.2 에서 100BASE-T 로 명명하였다. 이것은 이더넷 호스트들간에 공유하는 유선 미디어를 위한 CSMA/CD 기법과 무선 Ethernet LAN 을 위한 CSMA/CA (CA stands for Collision Avoidance) 기법을 사용하고 있다.

광섬유의 Fast Ethernet 는 100MBPS 까지의 속도를 제공하는 100BASE-FX standard 에서 정의하고 있다. 광섬유 이더넷은 half-duplex mode 로 100 미터까지 확대될 수 있으며, multimode fibers 와 관련된 full-duplex 로는 최대 2000 미터까지 전달할 수 있다.

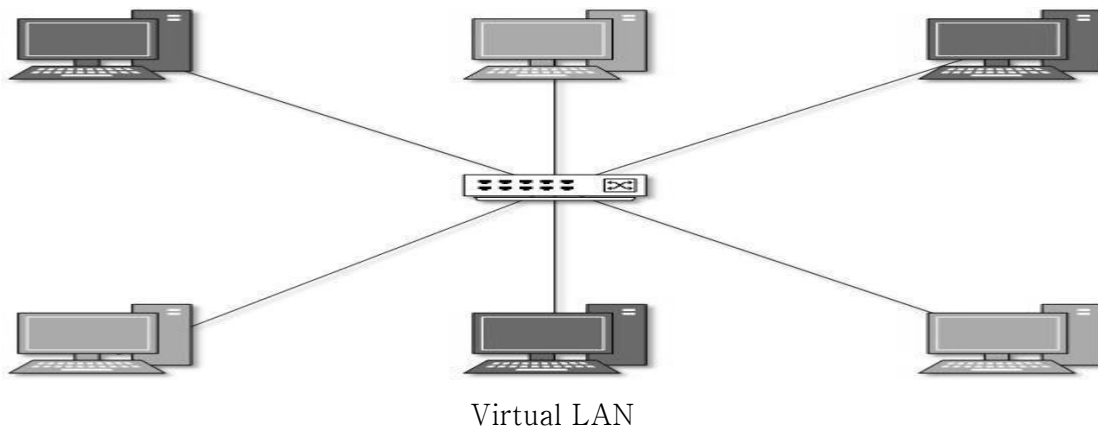
3. Giga-Ethernet

1995 년에 소개된 이래로, Fast-Ethernet 은 Giga-Ethernet 이 소개될 때까지 3 년동안 고속의 지위를 유지하고 있었다. 기가-이더넷은 1000mbit/seconds 까지의 속도를 제공한다. IEEE 802.3ab 는 Cat-5, Cat-5e 그리고 Cat-6 cables 을 사용하는 UTP 용 기가-이더넷의 표준이며, IEEE 802.3ah 에서는 Fiber 용인 기가-이더넷을 정의하고 있다.

4. Virtual LAN

LAN 은 공유된 미디어에서 순차적으로 작동하는 이더넷을 사용한다. 이더넷에서 공유된 미디어들은 a single Broadcast domain 과 a single Collision domain 을 만든다. 이더넷의 스위치들은 a single collision domain 문제를 제거하지만, 스위치에 연결된 각 기기는 각자의 독립된 collision domain 에서만 작동한다. 그렇지만 스위치라하더라도 넷을 독립된 Broadcast domains 로 쪼갤 수는 없다.

Virtual LAN 은 a single Broadcast domain 을 multiple Broadcast domains 으로 나누는 방식이다. 하나의 VLAN 에 있는 호스트는 또 다른 VLAN 에 있는 호스트에 명령할 수 없다. 초기값에 의해, 모든 호스트들은 동일한 VLAN 에 들어 있어야 한다.



위의 다이어그램에서, 서로 다른 VLAN 은 서로 다른 색깔로 표시되어 있다. 하나의 VLAN 에 있는 호스트들은 비록 동일한 Switch 에 연결되어 있다 하더라도, 다른 VLAN 에 있는 다른 호스트들을 참조하거나 명령할 수 없다. VLAN 은 이더넷에서 밀접하게 작동하는 Layer-2 기술이다. 두 개의 서로 다른 VLANs 간에 패킷츠를 라우트하기 위하여 Router 와 같은 Layer-3 기기가 필요하다.

IV. COMPUTER NETWORK TOPOLOGIES

넷 토폴로지는 어떤 컴퓨터 시스템이나 넷 기기들이 서로 연결된 형태를 말한다. 토폴로지는 넷의 물리적 또는 논리적 모습을 정의하기도 한다. 논리적 물리적 토폴로지 둘 다는 동일한 넷에서 같거나 다를 수도 있다.

1. Point-to-Point

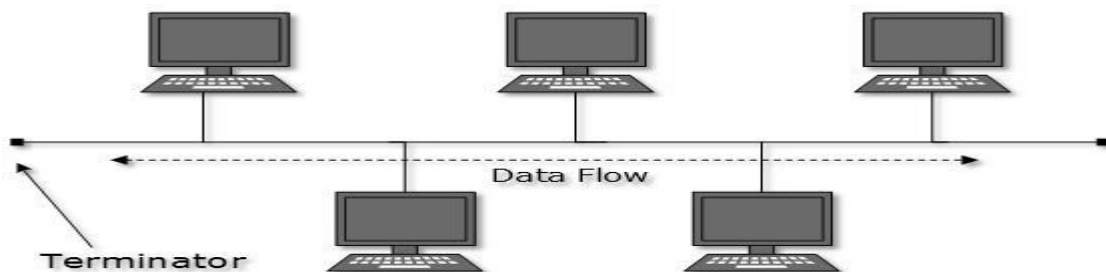


포인트-투-포인트 넷은 정확하게 컴퓨터로 된 두 개의 호스트, 스위치, 라우터 또는 한 조각의 케이블을 사용하여 백-투-백으로 연결된 서버로 구성된다. 종종 한 호스트의 수신부분이 다른 호스트 등의 송신부분에 연결되기도 한다.

만일 호스트들이 논리적으로 포인트-투-포인트로 연결되었다면, 복수의 중계기기들이 포함되기도 한다. 그렇지만, 최종 호스트들은 이러한 내용을 못하며 마치 서로가 직접 연결된 것으로 인식한다.

2. Bus Topology

버스 토폴로지의 경우에, 모든 기기들은 단일 통신선이나 케이블을 공유한다. 버스 토폴로지는 복수의 호스트가 동시에 데이터를 전송하는 경우에 문제가 있을 수 있다. 그러므로, 버스 토폴로지는 CDMA/CD 기술을 사용하거나 그러한 문제를 해결하기 위하여 하나의 호스트를 Bus Master 처럼 인식한다. 이것은 단일 기기의 잘못이 다른 기기에 영향을 끼치지 않는 가장 간단한 네트워크 형태들 중의 하나이다. 그러나 공유 통신선에 문제가 발생하면 모든 다른 기기들의 기능이 멈출 수 있다.



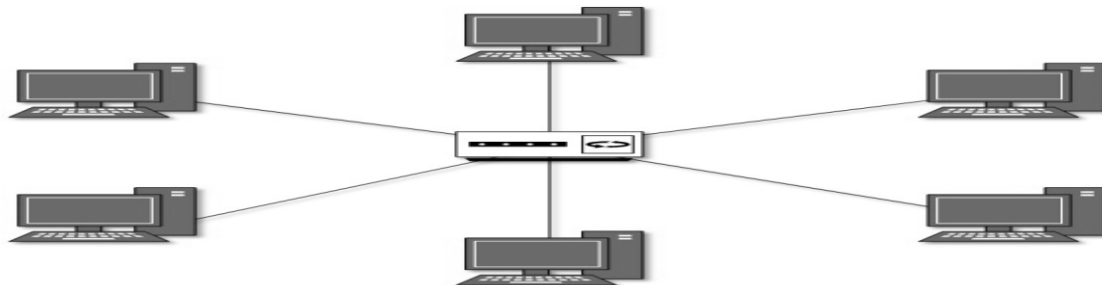
Bus Topology

공유채널의 양쪽 끝에는 line terminator 가 있다. 데이터는 단지 한 방향으로만 보내지며 그것이 양단 끝에 도달하자마자, 터미네이터는 그 통신선으로부터 온 데이터를 제거한다.

3. Star Topology

스타 토폴로지의 모든 호스트들은 포인트-투-포인트 연결방식으로 hub device 인 한 개의 중앙 기기에 연결되어 있다. 즉, 호스트들과 허브는 포인트-투-포인트 연결방식으로 존재한다. 이 허브 기기들은 다음과 같은 것들 중의 하나일 수 있다:

- . Layer-1 device such as hub or repeater
- . Layer-2 device such as switch or bridge
- . Layer-3 device such as router or gateway

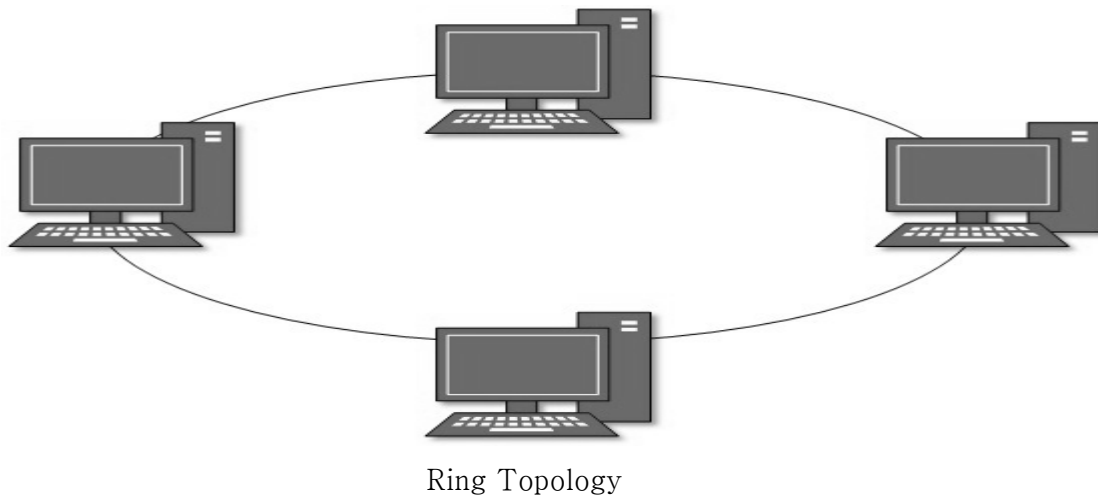


Star Topology

버스 토폴로지에서처럼, 스타형의 허브는 단일 기기처럼 행동한다. 만일 허브가 잘못된다면, 모든 호스트들의 연결에 문제가 발생한다. 호스트들간의 모든 통신은 허브만을 통해 이루어진다. 스타 토폴로지는 한 개 이상의 호스트를 연결하고, 허브와 호스트 간에는 단지 한 개의 케이블만이 필요하다. 따라서 구성도 간단하며 비싸지 않다.

4. Ring Topology

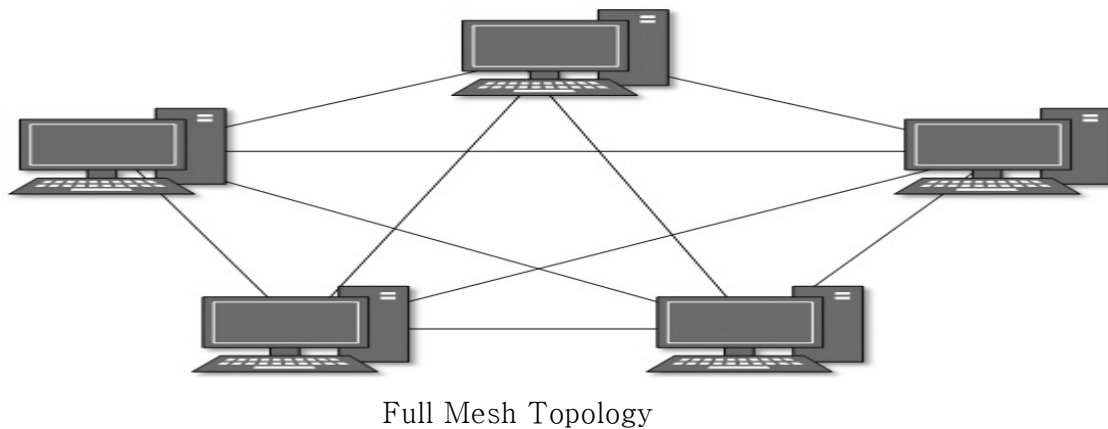
링 토폴로지에서, 각 호스트는 원형 넷 구조를 만들기 위하여 정확하게 두 개의 다른 기기에 연결된다. 한 개의 호스트가 그것에 인접해 있지 않은 또 다른 호스트에 메시지를 보내거나 통신하려고 할 때, 그 데이터는 모든 중계 호스트를 거쳐서 전달된다.



어떤 호스트의 잘못은 링 전체의 잘못을 초래한다. 그러므로, 링에 있는 각각의 호스트는 에러를 발생시키는 하나의 포인트가 될 수 있다. 따라서 한 개 이상의 백업 링을 사용하여 이러한 문제를 예방한다.

5. Mesh Topology

이런 종류의 토폴로지에서, 호스트는 한 개 또는 복수의 호스트에 연결된다. 이 토폴로지는 모든 다른 호스트들과 포인트-투-포인트로 연결된 호스트들을 가지고 있거나 소수의 호스트들과 포인트-투-포인트 방식으로 연결된 호스트들을 가질 수도 있다.



메쉬 토폴로지에서 호스트들은 직접적인 포인트-투-포인트 링크를 갖고 있지 않은 다른 호스트를 위하여 릴레이처럼 작동하기도 한다. 메쉬 토폴로지는 두 가지의 유형이 있다:

. Full Mesh(완전 메쉬):

모든 호스트가 네트워크에 있는 다른 모든 호스트에 포인트-투-포인트 방식으로 연결되어 있다. 따라서 모든 새로운 호스트를 위하여 $n(n-1)/2$ 연결횟수가 필요하다. 이것은 모든 넷 토폴로지 중에서 가장 신뢰할 수 있는 구조이다.

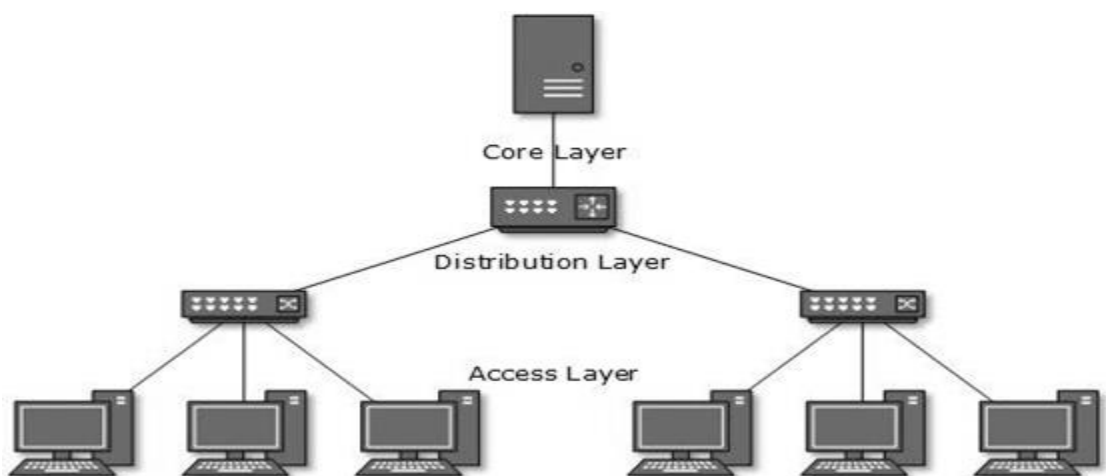
. Partially Mesh(부분 메쉬):

모든 호스트가 다른 모든 호스트에 포인트-투-포인트 방식으로 연결되어 있지는 않다. 호스트들은 임의적인 방식으로 서로 연결된다. 이 토폴로지는 모든 호스트 중에서 몇 개의 호스트들에 대해서만 신뢰성을 부여하고자 할 경우에 사용된다.

6. Tree Topology

계층적 토폴로지로 알려져 있으며, 이것은 현재 사용중인 넷 토폴로지에서 가장 일반적인 형태이다. 이 토폴로지는 확장형 스타 토폴로지처럼 보이며, 버스 토폴로지의 특성을 가지고 있다.

이 토폴로지는 네트워크를 복수의 levels/layers 로 나눈다. 주로 LANs 에서, 네트워크는 3 가지 유형의 네트워크 기기로 나눈다. 가장 낮은 쪽이 컴퓨터들이 접속하는 access-layer 이고, 중간 레이어는 distribution layer 로 알려져 있는데 이것은 위쪽 레이어와 아래쪽 레이어 간의 중계자 역할을 한다. 최상의 레이어는 core layer 라 부르며, 네트워크의 중심점이다. 다시 말해서, 모든 노드들이 갈라져 나가는 트리의 뿌리(root) 모양이다.



Tree Topology

모든 이웃 호스트들은 서로 포인트-투-포인트 방식으로 연결된다. 버스 토폴로지와 비슷하므로 만일에 루트가 다운된다면, 모든 네트워크가 비록 그것이 잘못된 단일 포인트가 아니더라도 어려움을 겪는다.

7. Daisy Chain

이 토폴로지는 모든 호스트들이 하나의 선형으로 연결되어 있다. 링 토폴로지와 비슷하게, 모든 호스트들은 단지 두 개의 호스트끼리 연결되어 있으나 최종 호스트들은 그렇지 않다. 만일 데이지 체인에 있는 최종 호스트가 연결되어 있다면, 그것은 링 토폴로지이다.

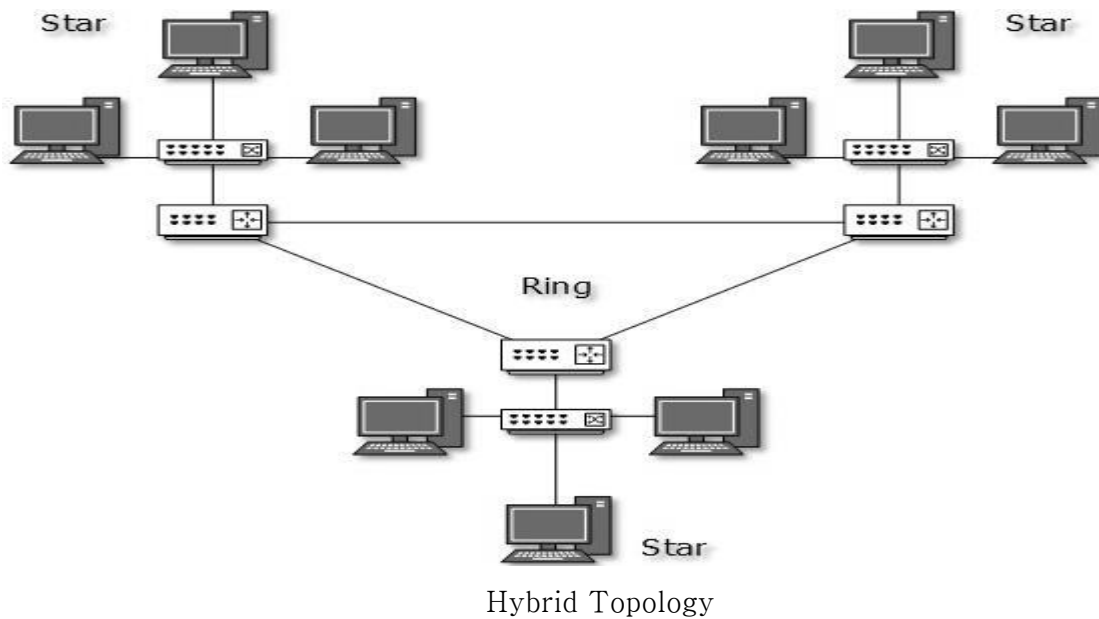


Daisy Chain Topology

데이지 체인 토폴로지의 각 링크의 에러는 단일 포인트의 잘못을 의미한다. 모든 링크의 잘못은 넷을 두 조각으로 분리시킨다. 모든 중간 호스트들은 인접 호스트들을 위한 릴레이로 기동한다.

8. Hybrid Topology

하나 이상의 토폴로지를 포함하도록 디자인된 넷 구조를 하이브리드 토폴로지라 부른다. 하이브리드 토폴로지는 그 안에 통합된 모든 토폴로지의 장단점을 갖는다.



위의 그림은 임의적인 하이브리드 토폴로지를 나타내고 있다. 서로 결합되어 있는 토폴로지들은 **스타, 링, 버스, 그리고 메시-체인 토폴로지**의 속성을 가질 수 있다. 대부분의 WANs 는 Dual-Ring 토폴로지를 사용하여 연결되어 있으며, 이것들에 연결된 넷들은 대부분 스타 토폴로지들이다. **인터넷은 가장 커다란 하이브리드 토폴로지의 가장 좋은 예이다.**

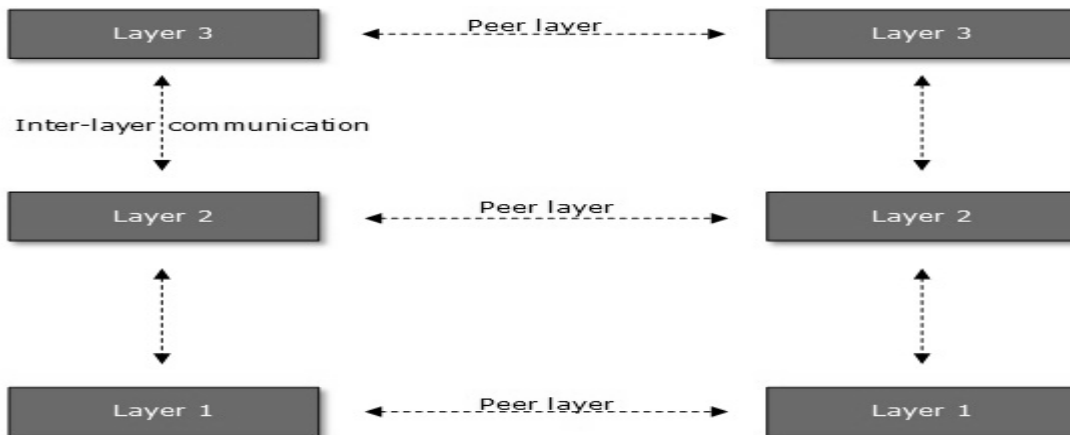
V. COMPUTER NETWORK MODEL

넷 공학은 software, firmware, chip level engineering, hardware, electric pulses 를 포함하는 복잡한 업무이다. 넷 공학을 쉽게 이해하기 위하여, 네트워킹 개념 전체를 복수의 레이어로 구분하고 있다. 각 레이어는 어떤 특별한 임무를 포함하며, 다른 모든 레이어와는 독립적이다. 그렇지만, 전체적으로 거의 모든 네트워킹 임무들은 이러한 레이어에 의존하고 있다. 레이어들은 서로 간에 데이터를 공유하며, input 을 받고 output 을 보내는 데도 서로 의존하고 있다.

1. Layered Tasks

넷 모델의 레이어 구조에서, 한 개의 넷 프로세서는 작은 임무들로 세분된다. 그 다음에 각각의 작은 임무들은 단지 그 임무만을 전문적으로 처리하는 특별한 레이어에 할당된다.

레이어화된 통신 시스템에서, 호스트의 한 레이어는 원거리 호스트에서 동일한 레벨에 있는 그것의 peer layer 에 의해 수행되는 임무를 다룬다. 그 임무는 가장 낮은 레벨에 있거나 그 위에 있는 레벨의 레이어에서 시작된다. 만일 그 임무가 최상의 레이어에서 시작된다면, 추가적인 처리를 위하여 그것의 바로 아래에 있는 레이어로 전달된다. 해당 레이어는 그 임무를 처리하여 다시 보다 낮은 레이어에 전달한다. 만일 그 임무가 가장 낮은 레이어에서 시작된다면, 역순의 과정이 이루어진다.



Layered Tasks

각각 레이어는 자신들의 임무를 수행하는데 필요한 모든 절차, 프로토콜, 그리고 방법을 가지고 있다. 모든 레이어는 encapsulation header 및 tail 의 기법으로 자신들의 상대를 식별한다.

2. OSI Model

Open System Interconnect 는 모든 통신 시스템을 위한 개방형 표준이다. OSI 모델은 ISO 에서 만들었다. 이 모델은 7 단계의 레이어로 구성되어 있다:



OSI Model

1)Application Layer:

이 레이어는 어플 이용자에게 인터페이스 제공의 책임을 진다. 이것은 직접적으로 이용자와 접속할 수 있는 프로토콜을 가지고 있다.

2)Presentation Layer:

이 레이어는 원격 호스트에 원래 포맷되어 있는 데이터가 다른 호스트의 포맷에서 표현되는 방법을 정의한다.

3)Session Layer:

이 레이어는 원격 호스트들간의 세션을 유지한다. 예를 들어, 일단 사용자/패스워드 인증이 이루어지면, 호스트는 이 세션을 유지함으로써 이 유지시간 동안 다시 인증을 요구하지 않는다.

4)Transport Layer:

이 레이어는 호스트들 간에 end-to-end 전달을 책임진다.

5)Network Layer:

이 레이어는 넷에서 호스트들의 어드레스 할당에 책임을 진다.

6)Data Link Layer:

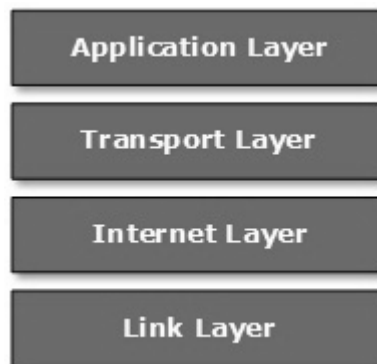
이 레이어는 통신선으로부터 전달되는 또는 통신선 상에 있는 데이터를 읽고 쓰는데 책임을 진다. 링크 에러는 이 단계에서 감지된다.

7)Physical Layer:

이 레이어는 넷을 구성하는 hardware, cabling, wiring, power output, pulse rate etc. 을 정의한다.

3. Internet Model

인터넷은 인터넷 슈트라 부르는 TCP/IP protocol suite 를 사용한다. 이것은 4 단계의 레이어로 구성된 인터넷 모델 이다. OSI 모델은 일반적인 통신 모델이지만, 인터넷 모델은 인터넷의 모든 통신에서 사용하는 모델이다. 인터넷은 그것의 기저가 되는 넷 구조 즉, 그것의 모델과는 독립적이다. 이 모델은 다음과 같은 레이어를 가지고 있다:



Internet Model

1)Application Layer:

이 레이어는 이용자가 넷에서 접속할 수 있는 프로토콜을 정의한다. 예를 들어, FTP, HTTP etc.

2)Transport Layer:

이 레이어는 어떻게 데이터가 호스트들 간에서 유통되는지를 정의한다. 이 레이어에 있는 중요한 프로토콜이 Transmission Control Protocol (TCP) 이다. 이 레이어에서는 호스트들간에 전달된 데이터의 순서가 맞는지, 그리고 end-to-end delivery 로 이루어졌는지를 확인한다.

3)Internet Layer:

IP 는 이 레이어에서 활동한다. 이 레이어는 host addressing & recognition 을 원활하게 한다. 이 레이어에서 라우팅을 정의한다.

4)Link Layer:

이 레이어는 실제적인 데이터를 송수신하는 메커니즘을 제공한다. 그것의 상대인 OSI 모델과 달리, 이 레이어는 근간이 되는 넷 구조 및 하드웨어와는 독립적이다

VI. COMPUTER NETWORK SECURITY

인터넷 초기에 이것의 사용은 연구 개발 목적으로 군대와 대학으로 제한되었다. 그 후에 모든 넷이 서로 통합되어 인터넷을 형성했을 때, 그것의 데이터는 공적인 넷을 통해 전달되었다. 일반인은 자신들의 bank credentials, username & passwords, personal documents, online shopping details, 또는 confidential documents 와 같은 매우 민감한 데이터를 보낼 수 있게 되었다.

모든 보안상의 위협은 의도적인 것이다. 다시 말해서, 그것들은 단지 고의적인 목적을 가질 때만 발생한다.

1) Interruption

인터럽션은 자원의 이용가능성을 공격하는 보안 위협이다. 예를 들어, 사용자가 웹 서버에 접근할 수 없거나 웹서버가 강탈되었다.

2) Privacy-Breach

이런 상황에서, 사용자의 프라이버시는 보장받지 못한다. 접근권한이 없는 사람이 인증된 사용자가 보내거나 받는 데이터에 침입하여 가로챌 수 있다.

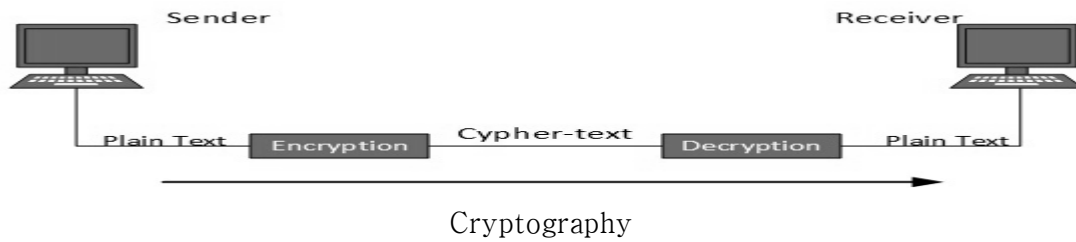
3) Integrity

이 위협에는 통신의 원래 내용을 변경하거나 조정이 포함된다. 공격자는 송신자가 보내온 데이터를 중간에서 가로챌 다음에 잘못된 데이터로 변경하거나 만들어서 수신자에게 보낸다. 수신자는 원래의 송신자가 보내고 있다는 가정하에 그 데이터를 접수한다.

4) Authenticity

이 위협은 공격자나 보안위반자가 진짜 회원으로 인정받아 자원에 접근하거나 다른 진짜 회원과 통신할 때 발생한다.

오늘날 어떠한 기술도 100% 안전하지 않다. 그러나 데이터가 안전하지 못한 넷이나 인터넷을 사용하는 동안 그것을 보호하기 위한 조치들이 취해질 수 있다. 가장 널리 사용되는 기법이 **Cryptography** 이다.



암호학은 평범한 텍스트의 데이터를 이해하거나 해석하기 어렵게 암호로 만드는 기법이다. 오늘날 이용 가능한 여러 가지 암호 알고리즘이 존재하며, 다음과 같다:

- . Secret Key
- . Public Key
- . Message Digest

1)Secret Key Encryption

송신자와 수신자 모두 한 개의 비밀 키를 갖는다. 이 비밀 키는 송신자 쪽에서 데이터를 암호화하는데 사용된다. 데이터가 암호화된 후, 이것은 공식 도메인을 통해 수신자에게 보내진다. 수신자도 비밀 키를 알고 있으므로, 암호화된 데이터 패킷을 쉽게 해독될 수 있다.

2) Public Key Encryption

이 시스템에서, 모든 사용자는 자신의 비밀 키를 가지만 그것을 공유하지 않는다. 자신의 비밀 키는 결코 공적 영역에 노출되지 않는다. 비밀 키와 더불어, 모든 사용자는 시스템에서만 사용하는 공적 키를 갖는다. 공적 키는 항상 공적으로만 사용되며 데이터를 암호화하기 위하여 송신자가 사용한다. 사용자가 암호화된 데이터를 접수했을 때, 그는 자신의 비밀 키를 사용하여 그것을 쉽게 해독할 수 있다.

3) Message Digest

이 방법에서는 실제 데이터를 보내지 않는다. 대신에 해쉬 값을 계산해서 보낸다. 상대방의 최종 이용자는 자신의 해쉬 값을 계산한 다음에 방금 접수된 것과 비교한다. 양쪽의 값이 동일하다면, 그 데이터는 접수되고 그렇지 않다면 거부된다.

- 6) Hash function - 임의적인 크기의 데이터를 고정된 크기의 데이터로 map 하는데 사용될 수 있는 함수이다. 이 함수에 의해 리턴된 값을 해쉬 값, 해쉬 코드라고 부르며, 전송된 데이터의 순수성을 확인하는데 사용한다.

VII. PHYSICAL LAYER INTRODUCTION

OSI 모델에서 물리적 레이어는 실제적인 하드웨어와 신호 메커니즘이 상호작용하도록 하는 역할을 한다. 물리적 레이어는 실제로 두 개의 서로 다른 스테이션을 물리적으로 연결시키는 OSI 의 유일한 레이어이다. 이 레이어에서 하드웨어 장비, cabling, wiring, frequencies, 이진 신호를 나타내는데 사용되는 pulses 등을 정의한다.

물리적 레이어는 Data-link 레이어에 서비스를 전달 한다. Data-link 레이어는 물리적 레이어로 프레임들을 제시한다. 물리적 레이어는 그것들을 이진 데이터로 표현되는 전기 펄스로 변경시킨다. 그런 다음에 그 이진 데이터는 유무선 매체를 통해 전달된다.

1. Signals

데이터가 물리적 매체로 보내질 때, 그것은 전자기 신호로 먼저 바뀌어야 한다. 데이터 그 자체는 인간 음성과 같은 아날로그이거나 디스크의 파일처럼 디지털일 수 있다. 아날로그와 디지털 데이터 모두 디지털이나 아날로그 신호로 표현될 수 있다.

1)Digital Signals:

디지털 신호는 성질상 이산적이며 연속된 전압 펄스를 나타낸다. 디지털 신호는 컴퓨터 시스템의 회로에서 사용된다.

2)Analog Signals:

아날로그 신호는 성질이 연속된 파형으로 되어 있으며 연속적인 전자기 파동으로 표현된다.

2. Transmission Impairment

신호가 매체로 전달된 때, 그것들이 망가지는 경우가 있다. 이것은 다음과 같은 원인으로 발생 한다:

1)Attenuation(감쇠):

수신자가 실제로 데이터를 해석하기 위해서는 그 신호가 충분히 강해야 한다. 신호가 매체를 통해 전달될 때 약해지는 경향이 있다. 거리가 늘어날수록 강도를 잃게 된다.

2)Dispersion:

신호가 매체를 통해 전달될 때, 그것은 중첩되거나 분산되는 경향이 있다. 산포의 총량은 사용된 주파수에 따라 결정된다.

3)Delay distortion:

신호는 사전에 정해진 속도와 주파수로 매체간에 보내진다. 만일 신호의 속도와 주파수가 부합되지 않는다면, 그 신호는 임의의 방식으로 목적지에 도달할 가능성이 있다. 디지털 매체에서, 어떤 비트들이 이미 보낸 것들 보다 빨리 도달한다면 이것은 매우 치명적이다.

4)Noise:

아날로그나 디지털 신호에서 임의적 방해와 불안정을 잡음이라고 말하며, 이것은 전달되는 실재정보를 왜곡시킨다. 노이즈는 아래의 유형 중에서 한가지의 특징을 가질 수 있다:

(4-1)Thermal Noise:

열은 노이즈를 유발시킬 수 있는 전도체를 뜨겁게 한다. 어느 수준까지, 열에 의한 노이즈를 피할 수는 없다.

(4-2)Intermodulation(주파수의 상호변조):

복수의 주파수를 한 매체가 공유할 때, 이것들 간의 간섭이 매체에 노이즈를 발생시킨다. 이런 노이즈는 만일 두 개의 서로 다른 주파수가 하나의 매체를 공유하여 그것들 중의 하나가 너무나 강해 올바르게 작동하지 않는다면, 그 결과로 발생하는 주파수는 기대한 것만큼 전달되지 않을 수 있다.

(4-3)Crosstalk(혼선):

이런 유형의 노이즈는 외래 신호가 매체에 끼어들 때 발생한다. 이것은 어떤 매체의 신호가 다른 매체의 신호에 영향을 끼치기 때문에 발생한다.

(4-4)Impulse(충격):

이 노이즈는 빛, 전기, 누전, 또는 불량부품과 같은 비정상적인 방해로 발생한다. 디지털 데이터는 이 노이즈에 대부분이 영향을 받는다.

3. Transmission Media

두 컴퓨터 시스템 간에 정보를 보내주는 매체를 전송 매체라 부르며, 두 가지 형태가 있다:

1) Guided Media:

모든 통신 와이어/케이블은 UTP, coaxial cables, fiber Optics 처럼 전도 매체이다. 이 매체에서, 송신자와 수신자는 직접 연결되며 그것을 통해 정보를 전송(유도)한다.

2) Unguided Media:

무선이나 공중파는 비전도 매체라 부른다. 그 이유는 송수신자 간에 어떠한 연결성도 없기 때문이다. 정보는 공중으로 날라가서 수신기를 갖고 있는 누군가에 의해 수집될 수 있다.

4. Channel Capacity

정보전송의 속도를 채널 캐퍼시티라 부른다. 이것을 디지털 분야에서는 data rate 로 계산하며, 다음과 같이 요소에 따라 결정된다:

- . Bandwidth(주파수 대역폭): 기저 매체의 물리적 한계.
- . Error-rate: 노이즈가 원인인 부정확한 정보의 입수
- . Encoding: 시그널용으로 사용된 레벨들의 번호

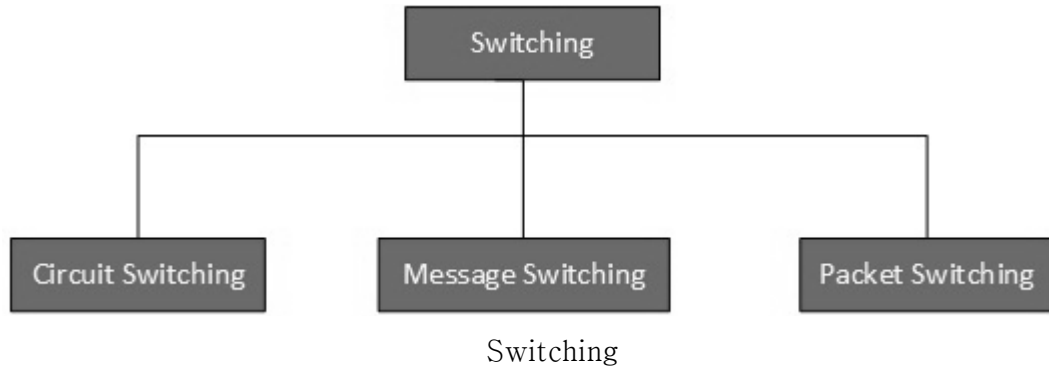
5. Multiplexing

멀티플렉싱이란 단일 매체로 복수의 데이터 스트림들을 혼합하여 보내는 기법을 말한다. 이 기법에서는 스트림들을 멀티플렉싱하기 위한 multiplexer (MUX)와 매체로부터 정보를 받아서 다른 목적지로 분산시켜주는 de-multiplexer (DMUX)와 같은 시스템 하드웨어를 필요로 한다.

6. Switching

스위칭이란 정보원에 직접 연결되지 않은 목적지로 데이터/정보를 보내는 메커니즘이다. 넷들은 직접 연결된 정보원으로부터 데이터를 받아서 그것을 저장하고 분석한 다음에, 목적지에 가장 가까이 있는 두 번째의 기기로 보내는 기기들로 구성되어 있다.

스위칭의 범주는 다음과 같다:



1)Circuit switching

서킷 스위칭이란 노드들이 통신 전에, 두 개의 노드를 넷 전용 통신 채널(서킷)로 구축하는 방법을 말한다. 서킷은 full bandwidth 를 보장하며 통신 세션이 이루어지는 동안 접속이 지속된다. 서킷에서는 해당 노드들이 물리적으로 하나의 전기회로로 연결된 것처럼 작동한다.

서킷 스위치 넷의 명확한 예로는 초기의 아날로그 전화 넷이다. 한 전화기로부터 다른 전화기로 통화가 이루어질 때, 전화교환기에 있는 스위치들은 가능한 한 오랫동안 통화가 지속되도록 두 전화기 사이에서 계속해서 유선 서킷을 만든다.

2)Message switching

메시지 스위칭은 한번에 일회 송출(one hop)로 메시지들이 텔레콤 전체로 라우트시키는 스위칭 방식이다. 이것은 대형 항공사, 은행, 철도회사에서 사용하였다.

메시지 스위칭 시스템은 현재에도 패킷 스위치 또는 서킷 스위치 넷의 대안으로 사용되고 있다. 각 메시지는 독립된 엔티티로 취급된다. 각 메시지에는 어드레싱 정보가 포함되어 있으며, 각 스위치에서 이 정보가 읽혀진 다음, 전용선으로 다음 스위치에 전달된다.

넷 조건에 따라, 여러 메시지들의 데이터가 똑 같은 통신선으로 전달되지 않기도 한다. 각 메시지는 다음 스위치로 전달되기 전에, RAM 의 한계로 인하여 대체로 하드웨어에 저장된다. 이러한 이유로 인하여, 이것을 'store-and-forward' network 라 부르기도 한다.

이메일은 메시지 스위칭을 사용하는 대표적인 어플이다. 두 컴퓨터 간에 실시간 데이터 전송이 이루어지지만, 이메일을 전달하는데는 딜레이가 허용된다.

3)Packet switching

패킷 스위칭은 동시다발적인 통신 세션에서 공유 매체를 통해 전달될 수 있도록, 모든 전송 데이터를 패킷이라고 부르는 적당한 크기의 블록으로 집단화시키는 디지털 통신

방법이다. 패킷 스위칭은 넷의 효율성과 건강성을 증대시키며, 동일한 넷에서 작동하는 많은 어플의 기술적 융합(convergence)을 가능케 한다.

패킷은 헤더와 페이로드로 구성된다. 헤더의 정보는 하드웨어에 의해, 패킷이 목적지로 직행하는데 사용되며, 페이로드는 어플에서 발췌하여 사용한다.

패킷 스위칭은 1960 년대와 1970 년대에 개발되었으며, 초기엔 X.25 와 ARPANET 에서 널리 사용되었다. 오늘날 이것은 인터넷과 대부분의 LAN 에서 사용되는 기본적 기술이다. 웹을 웹이라고 부르는 이유는 이것이 분산식(거미줄처럼)으로 상호 연결된 구조이기 때문이다.

패킷 스위칭은 데이터그램 스위칭인 connectionless(비연결) packet switching 과 virtual circuit switching 인 connection-oriented packet switching 으로 구분되기도 한다:

비연결 프로토콜의 예로는 Ethernet, Internet Protocol (IP), 그리고 User Datagram Protocol (UDP)이 있고, 연결-지향적 프로토콜로는 X.25, Frame Relay, Multiprotocol Label Switching (MPLS), Transmission Control Protocol (TCP)가 있다.

비연결 모드에서, 각 패킷에는 환전된 주소정보가 들어있다. 이 패킷들은 개별적으로 라우트 되므로, 그 결과가 때로는 서로 다른 통로를 사용하여 순차적으로 전달되지 않는다. 각 패킷은 목적지 주소, 정보원 주소, 포트 번호를 포함하고 있다. 또한 그것의 일련 번호가 포함될 수도 있다. 이것은 패킷이 목적지로 가는 데 전용선 사용의 필요성을 배제시킨다. 목적지에서, 본래의 메시지/데이터는 패킷의 순번을 근거로 올바른 순서로 재취합 된다.

연결-지향적 전송에서 어떤 패킷은 통신 패러미터의 구성을 위해, 전달되기도 전에 각각의 관련 노드에 설치절차를 요구한다. 이 패킷들은 주소정보보다는 연결 식별자를 포함하고 있으며, 엔드 포인트와 협정을 맺어서 순서대로 그리고 에러를 체크하면서 전달된다.

VIII. DIGITAL TRANSMISSION

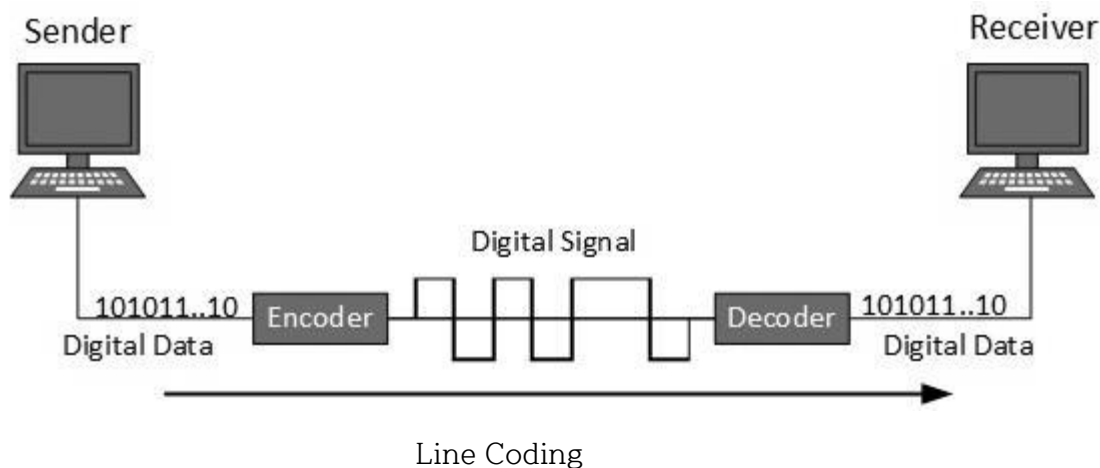
데이터나 정보는 두 가지 방법으로 저장된다: analog 와 digital. 컴퓨터에서 데이터를 사용하기 위하여는 discrete digital form 로 되어 있어야 한다. 데이터와 비슷하게, signals 또한 analog 나 digital form 이어야 한다. 데이터를 디지털로 전송하기 위해서, 먼저 디지털 형태로 그것을 변경해야 한다.

1. Digital-to-Digital Conversion

이제 디지털 데이터를 디지털 신호로 변환시키는 방법에 대해 알아보자. 두 가지 방법이 있다: line coding 과 block coding. 모든 통신에서 line coding 은 필수적이지만, block coding 은 선택적이다.

1) Line Coding

디지털 데이터를 디지털 신호로 변환시키는 절차를 Line Coding 이라 한다. 디지털 데이터는 2진 형태로 되어 있으므로, 내부적으로 1s 과 0s 연속으로 표현되거나 저장된다.



2) Block Coding

수신된 data frame 의 정확성을 보장하기 위하여, redundant bits 를 사용한다. 예를 들어, 짝수 패리티(even-parity)에서, one parity bit 를 frame even 에 있는 1 들의 계산에 추가 한다. 따라서 비트의 원래의 수가 증가한다. Block Coding 이라 부른다.

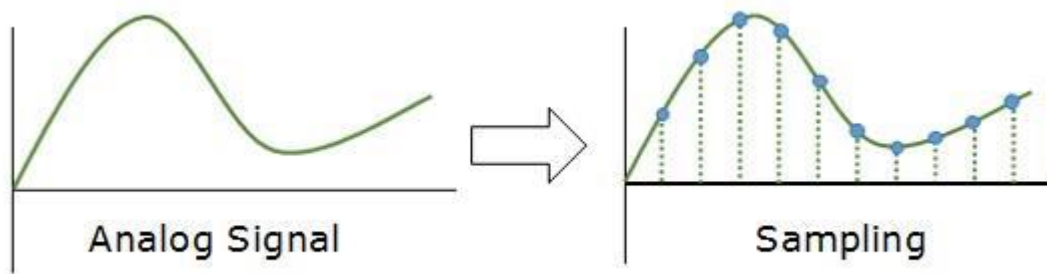
2. Analog-to-Digital Conversion

Microphones 은 analog voice 를 그리고 camera 는 analog videos 를 취급한다. 이것을 디지털 데이터로 전송하기 위해서는 디지털 변환이 필요하다.

Analog data 는 파도형의 연속 데이터인 반면에, 디지털은 이산 데이터이다. 아날로그 파형을 디지털 데이터로 변환시키기 위해서는 Pulse Code Modulation (PCM)을 사용하여야 한다. PCM 은 가장 일반적인 방법 중의 하나이며, 3 가지의 단계가 있다:

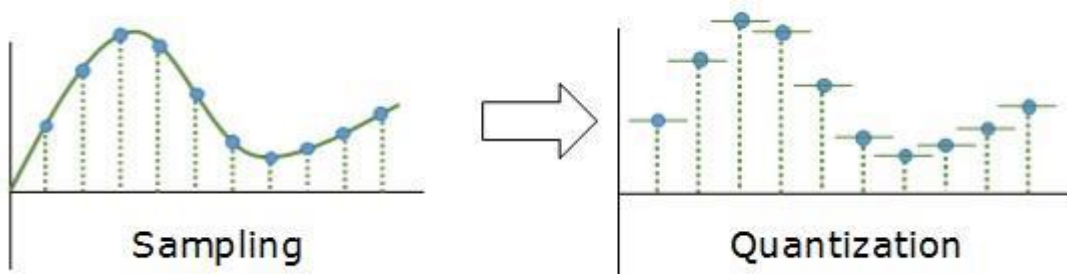
- . Sampling
- . Quantization
- . Encoding.

1)Sampling



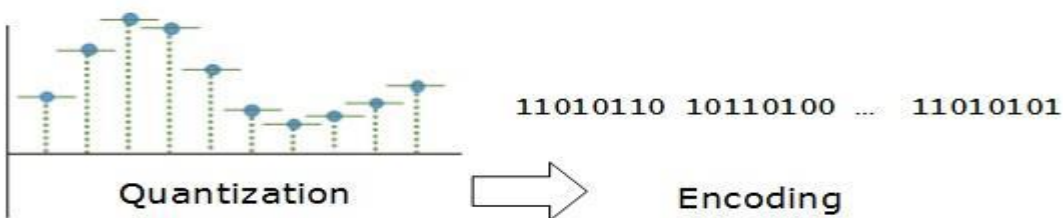
analog signal 은 모든 모든 Time interval 을 샘플링한다. 샘플링에서 가장 중요한 요소는 analog signal 을 샘플링하는 비율이다. 샘플링 비율은 적어도 signal 의 최고 빈도의 두 배가 되어야 한다.

2)Quantization



Sampling 은 연속적인 아날로그 시그널의 이산적 형태를 갖는다. 이 경우에, 모든 이산적 패턴은 아날로그 시그널을 증폭시켜 보여준다. Quantization 은 최대의 증폭 값과 최소의 증폭 값 사이에서 이루어진다. Quantization 은 instantaneous analog value 의 근사치이다.

3)Encoding



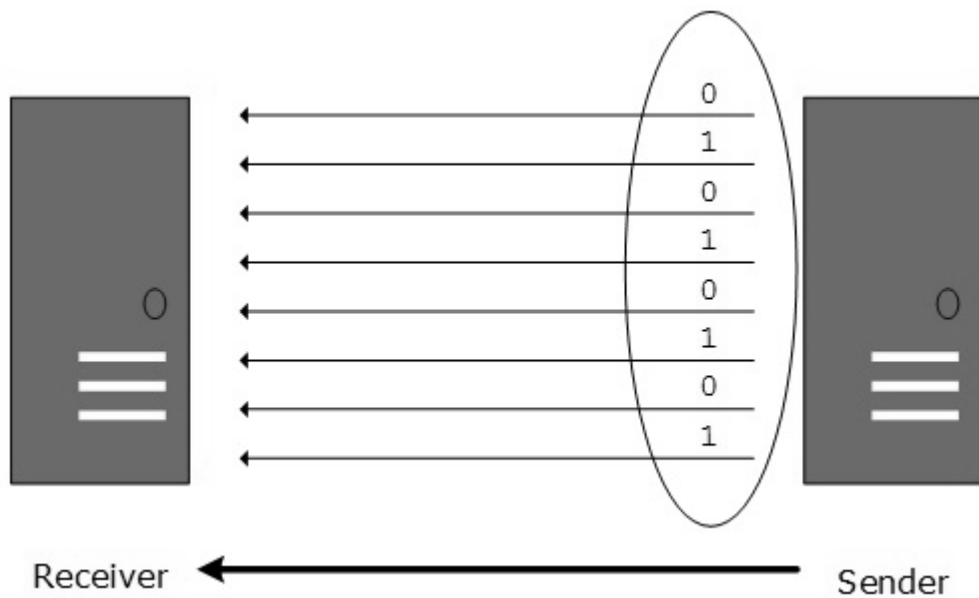
Encoding

기호화하는데 있어서, 각 근사치는 이진 포맷으로 변환된다.

3. Transmission Modes

transmission mode 에서는 두 컴퓨터 간에 데이터 전송방법을 결정한다. 1s 과 0s 로된 이진 데이터는 두 가지 모드로 보내진다: Parallel 과 Serial.

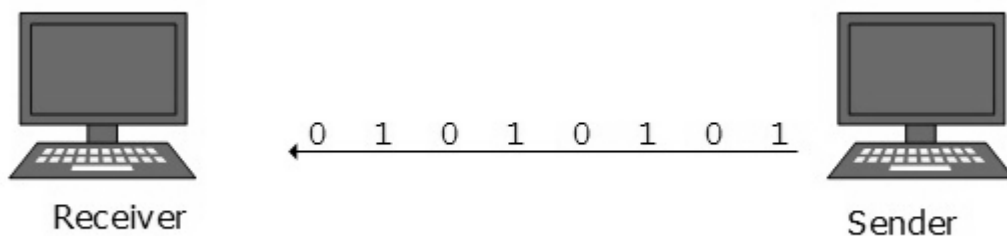
1)Parallel(병렬식) Transmission:



이진 비트는 고정된 길이의 그룹들로 조직되어 있다. 송더와 리시버 둘 다 동일한 데이터 라인의 숫자를 갖고 병렬식으로 연결되어 있다. 송더는 모든 라인으로 한번에 모든 비트를 보낸다. 그 이유는 그룹이나 데이터 프레임에 있는 비트의 수가 동일하기 때문에, 완전한 비트 그룹(데이터 프레임)을 한번에 보낼 수 있다. Parallel transmission 의 장점은 고속이란 것이며, 단점은 병렬식으로 데이터를 보내므로 wires 의 비용이 비싸다는 것이다.

2)Serial(직렬식) Transmission:

serial transmission 에서 비트는 순차적으로 나란히 보내진다. Serial transmission 에서는 단지 한 개의 통신 채널만이 필요하다:



Serial Transmission

Serial transmission 은 동기식과 비동기식으로 이루어진다.

(2-1)Asynchronous Serial Transmission:

이름이 뜻하는 것처럼, timing 이 중요하지 않는 방식이다. 데이터-비트는 특별한 패턴을 가지고 있어서 리시버가 시작과 끝 데이터 비트를 읽는데 도움을 준다. 예를 들어, 0 은 모든 데이터 바이트에 prefixed 되며, 한 개 이상의 1s 이 끝부분에 첨가된다.

(2-2)Synchronous Serial Transmission:

synchronous transmission 에서 timing 은 중요하다. 왜냐하면 시작과 끝 데이터 비트를 인식하는 메커니즘이 존재하지 않기 때문이다. 어떠한 pattern 이나 prefix/suffix method 이 없다. synchronous transmission 의 장점은 고속이며, asynchronous transmission 에서처럼 extra header 와 footer bits 에 대한 어떠한 부담도 없다는 것이다.

IX. ANALOG TRANSMISSION

아날로그 미디어로 디지털 데이터를 보내기 위해, 아날로그 시그널을 변환시켜야 한다. 데이터 포매팅에 따라 두 가지 케이스가 있다:

1. Bandpass:

필터들이 관심대상의 주파수를 필터하고 패스시키는데 사용된다. Bandpass 는 필터를 전달할 수 있는 주파수의 밴드이다.

2. Low-pass:

Low-pass 는 low frequencies signals 을 전달하는 필터이다.

디지털 데이터를 bandpass analog signal 로 변경할 때, digital-to-analog conversion 이라 부르고, low-pass analog signal 을 bandpass analog signal 로 변경할 땐 analog-to-analog conversion 이라 부른다.

X. TRANSMISSION MEDIA

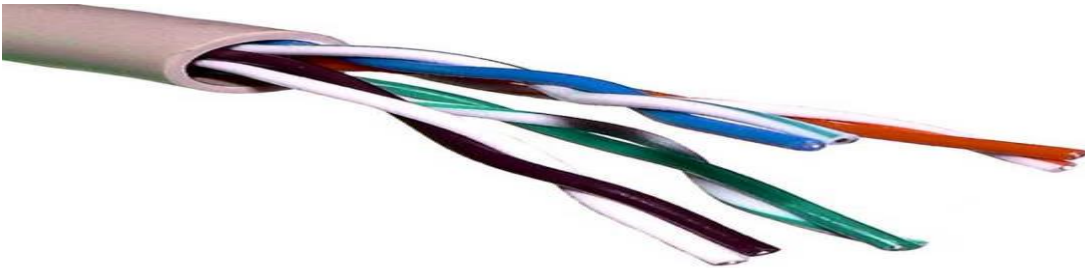
transmission media 는 컴넷 통신이 이루어지는 단지 physical media 이다.

1. Magnetic Media

컴퓨터 간에 데이터를 전송하는 가장 편리한 방법 중의 하나는 넷이 탄생하기 전에도 저장 매체에 그것을 저장한 다음, 한 스테이션에서 다른 곳으로 물리적으로 전송하는 것이다. 고속의 인터넷 시대인 오늘날 비록 구식이라 하더라도, 데이터의 규모가 클 땐, 마그네틱 매체를 사용한다: magnetic tapes 나 magnetic discs.

1) Twisted Pair Cable

twisted pair cable 은 두 개의 플라스틱으로 감싼 동선으로 되어 있으며, 두 선이 꼬여서 하나의 형태를 이루고 있다. 이 두 전선 중에서 단지 하나만 실제 신호를 전송하고, 나머지는 접지(ground reference)용으로 사용한다. 전선 간의 twists 는 noise (electro-magnetic interference) 와 crosstalk 를 줄이는데 도움이 된다.



두 종류의 twisted pair cables 이 있다:

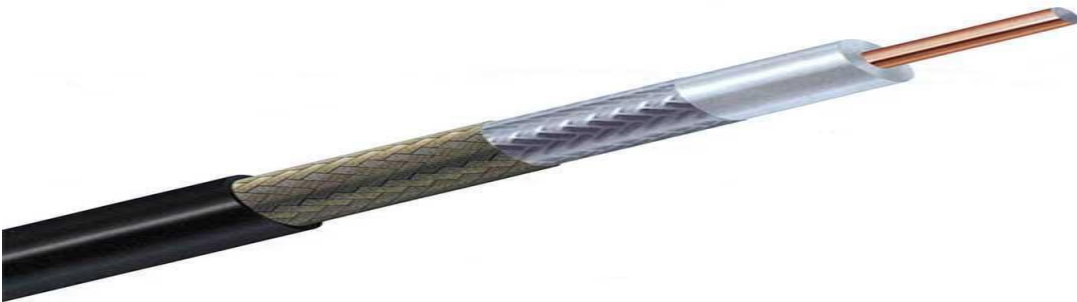
- . Shielded Twisted Pair (STP) Cable
- . Unshielded Twisted Pair (UTP) Cable

STP cables 은 금속막으로 덮인 twisted wire pair 로 되어 있으며, noise 와 crosstalk 에 대해 강하다.

UTP 는 7 개의 카테고리를 갖고 있으며, 각각은 특별한 용도에 맞춰져 있다. computer networks 에서, Cat-5, Cat-5e, 그리고 Cat-6 cables 이 가장 많이 사용되며, UTP cables 은 RJ45 connectors 에 연결된다.

2)Coaxial Cable

Coaxial cable 은 두 가닥의 구리선 이다. 중심에는 core wire 가 있으며, 고체인 도체로 덮여 있다. Core 는 절연되는 외장물질(sheath)로 감싸여 있다. 두 번째 wire 도 sheath 로 감싸져 있으며, 또한 절연 sheath 로 다시 감싸여 있다. 이것 모두는 플라스틱 피복으로 덮여 있다.



Coaxial Cable

이러한 구조로 인하여, coax cable 은 높은 주파수의 시스널을 전달할 수 있어서, twisted pair cable 보다 우수하다. 이것의 피복 구조는 noise 와 cross talk 에 우수한 방어막을 제공한다. 동축선은 고속의 450 mbps 까지의 주파수 폭이 이 가능하다.

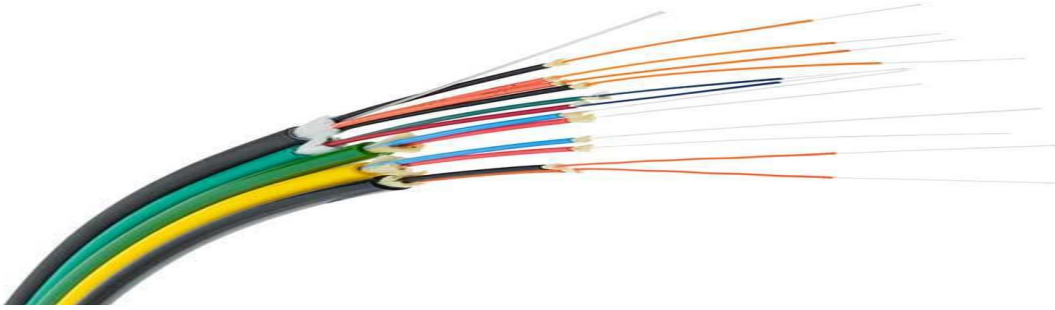
3)Power Lines

Power Line communication (PLC)는 데이터 시스널을 전송하기 위하여 전선을 사용하는 Layer-1 (Physical Layer) technology 을 사용한다. PLC 에서, modulated data 는 케이블로 보내진다. 다른 끝에 있는 리시버는 그 데이터를 de-modulates 그리고 interprets 한다.

4)Fiber Optics

Fiber Optic 는 빛의 성질로 작동한다. 빛이 임계각(critical angle)으로 비칠 때, 90 도로 굴절된다. 이러한 성질이 광섬유에서 사용되고 있다. fiber optic cable 의 핵심은 고순도의 유리나 플라스틱으로 만든다. 한 쪽 끝에서 빛이 방사되면, 선을 따라 전달된 다음, 다른 쪽 끝에 있는 빛 감지기(light detector)에서 빛줄기(light stream)를 탐지하여 전기 데이터로 변환시킨다.

Fiber Optic 는 **초고속을** 제공하며, 두 모드로 되어 있다: 하나는 single mode fiber 이고, 또 하나는 multimode fiber. Single mode fiber 는 단일 빛을 운반하는 반면에, multimode 는 복수의 빛을 전송한다.



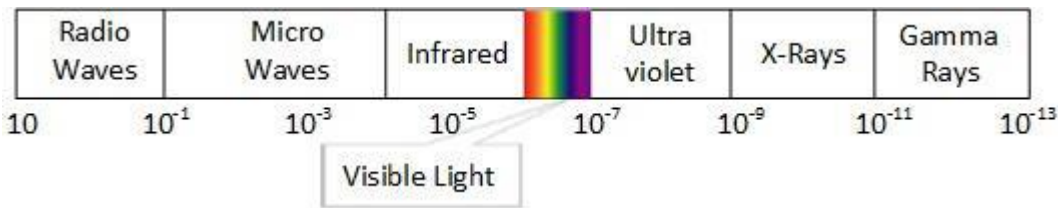
Fiber Optics

XI. WIRELESS TRANSMISSION

Wireless transmission은 unguided media의 한 형태이다. Wireless communication은 두 개 이상의 기기 사이에 설정된 어떠한 물리적 링크도 존재하지 않는다. 무선 신호는 공중으로 퍼지며, 적절한 안테나에 의해 수집되고 해석된다.

antenna가 computer나 wireless device의 전자회로에 접속할 때, digital data는 무선 신호로 바뀐 다음 주파수 범위 내에서 퍼져 나간다. 상대방에 있는 receptor가 이 신호를 받아서 다시 디지털 데이터로 변환시킨다.

electromagnetic spectrum의 조그만 부분을 wireless transmission에서 사용한다.



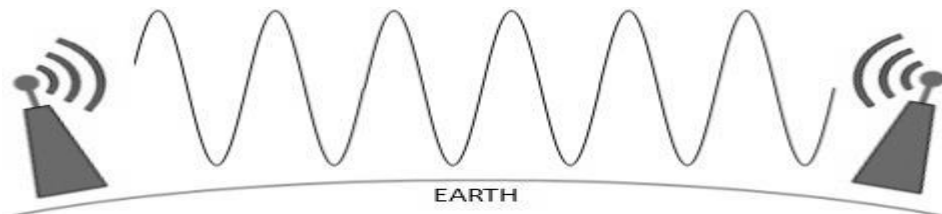
Electromagnetic Spectrum

1. Radio Transmission

Radio frequency는 생산성이 높는데, 그것의 커다란 파장(wavelength)이 벽 같은 구조물을 관통할 수 있기 때문이다. Radio waves의 범위는 1mm에서 100,000km 정도이며, 3Hz (Extremely Low Frequency)에서 300 GHz (Extremely High Frequency) 정도의 주파수 범위를 갖는다. Radio frequencies는 six bands로 다시 나뉜다.

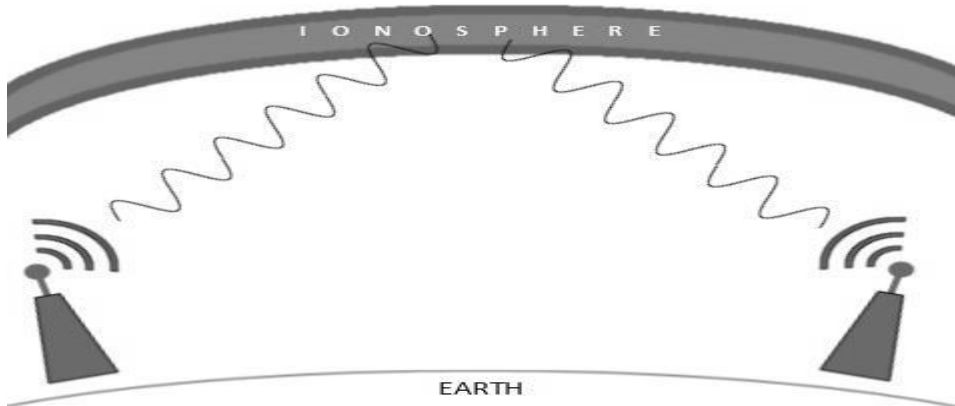
저 주파는 벽을 통과할 수 있는 반면에, 고주파는 직선으로 가며 벽에서 튕어 나온다. 저 주파수의 힘은 거리가 늘어나면 급격하게 줄어든다. 고주파는 더 많은 전력이 소비된다.

VLF, LF, MF bands와 같은 저 주파수들은 지상에서 1000 kilometers까지 전달된다.



Radio wave - grounded

고주파는 빗물이나 기타 장애물에 흡수되기 쉽다. 이것들은 전리층(ionosphere)을 이용한다. 이것들이 전리층에 도달 하면, 지상으로 다시 반사된다.

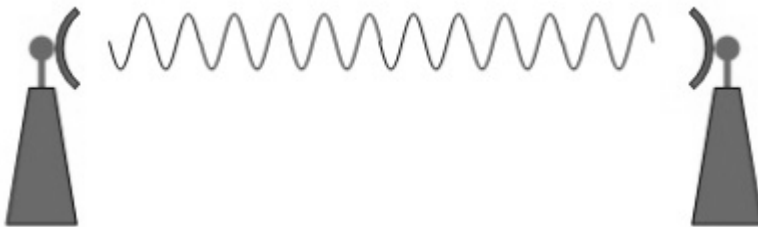


Radio wave - Ionosphere

2. Microwave Transmission

100MHz 이상의 전자기파는 직선으로 퍼지는 경향이 있으며, 이것의 시그널은 어떤 특별한 스테이션을 향해 보내지는 전파 빔으로 전송된다. Microwaves 는 직선으로만 전파되기 때문에, 센터와 리시버 둘 다 엄격하게 가시적(line-of-sight)으로 정렬되어야 한다.

Microwaves 의 길이는 1mm 에서부터 1meter 이고, 주파수는 300MHz 부터 300GHz 까지 이다.



Personal Area Network

Microwave antennas 는 빔으로 된 주파수를 모은다. 위의 그림에서처럼 다수의 안테나들을 보다 멀리 전달하게 위하여 정렬할 수도 있다. Microwaves 는 고주파이므로 장애물인 벽을 뚫을 순 없다.

Microwave transmission 은 날씨와 사용 주파수에 크게 의존한다.

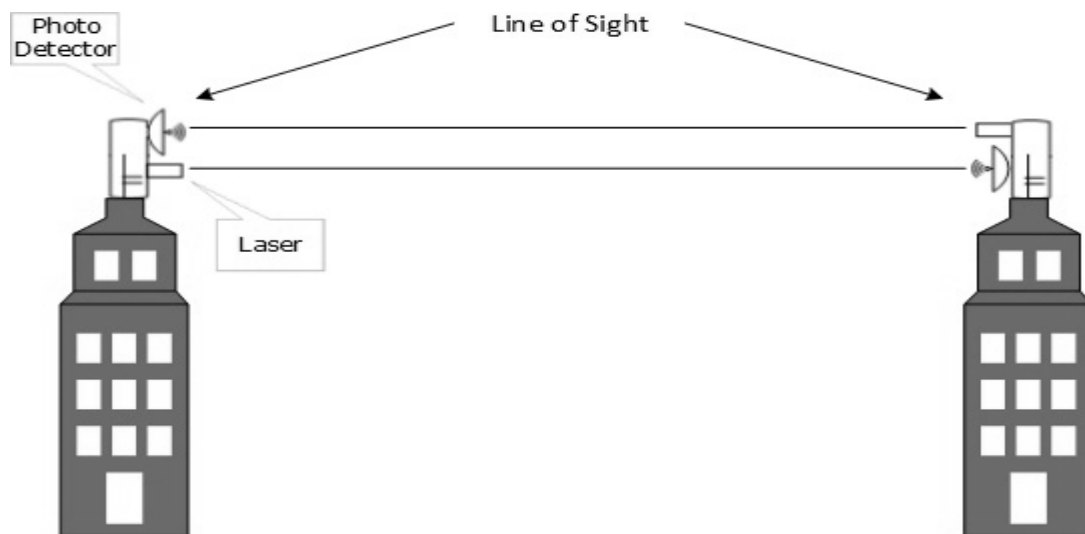
3. Infrared Transmission

Infrared wave 는 가시광선 스펙트럼과 microwaves 사이에 있다. 이것의 파장은 700nm to 1mm 이며, 주파수 범위는 300GHz 부터 430THz 이다. Infrared wave 는 텔레비전과 리모콘과 같이 초단거리 통신에서 사용된다. 적외선은 자연스럽게 직진하며, 고주파수로 인하여 벽을 투과하진 못하다.

4. Light Transmission

데이터 통신에 사용되는 가장 높은 전자기 spectrum 은 빛 또는 광학 signaling 이며, LASER 가 대표적이다.

광파는 엄격한 직진성을 갖는다. 그러므로 송수신자는 가시적 이어야 한다. laser transmission 은 일방향성이므로, 양쪽 끝에는 laser 및 photo-detector 가 있어야 한다. Laser beam 은 일반적으로 폭이 1mm 이며, 두 개의 receptors 가 레이저 광원에 정확하게 맞춰져 있어야 올바르게 작동하게 된다.



Light Transmission

Laser 는 Tx (transmitter)로 작동하고 photo-detectors 는 Rx (receiver)로 작동한다. Lasers 는 walls, rain, 그리고 thick fog 을 관통할 수 없다. 추가로 laser beam 은 진행과정에 있는 wind, atmosphere temperature, 또는 기온의 변화에 의해 왜곡되기도 한다. Laser 는 안전한 data transmission 이지만, communication channel 의 휘방없이 1mm 폭으로 레이저를 맞추는 것은 매우 어렵다.

XII. MULTIPLEXING

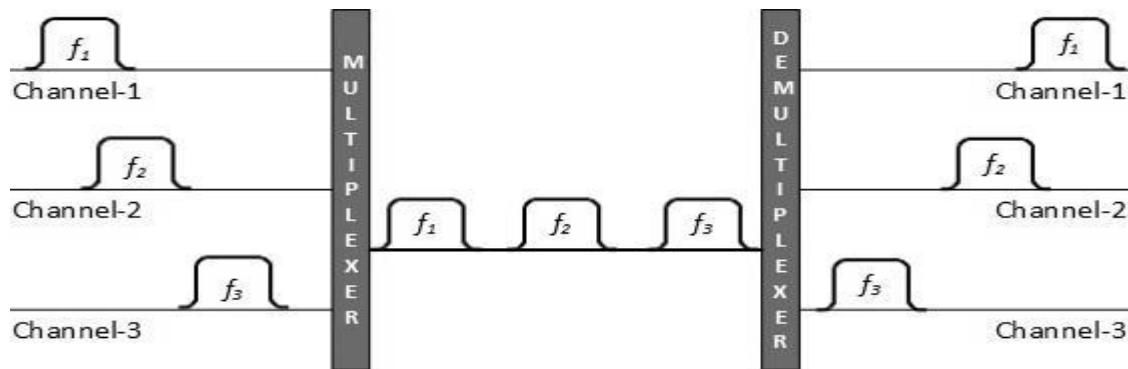
Multiplexing 이란 공유링크를 통하여 서로 다른 아날로그와 디지털의 전송 스트림을 동시에 처리하는 기법이다. Multiplexing 은 고성능의 medium 을 서로 다른 스트림을 사용하여 저성능의 논리적 medium 로 나눌 수 있다.

Communication 은 physical media (cable)와 light (optical fiber)을 사용하여 공기(radio frequency)를 통해 전달된다. 모든 매체에서는 multiplexing 이 가능하다.

다수의 센터가 단일 매체로 보낼 때, Multiplexer 라는 기기가 복수의 물리적 채널로 나누어 각 센터에 하나씩 할당한다. 통신의 반대 쪽에 있는 De-multiplexer 가 단일 매체로부터 온 데이터를 받아서 판별한 다음에 리시버로 보낸다.

1. Frequency Division Multiplexing

전달매체(carrier)가 주파수일 경우, FDM(주파수 분할 멀티플렉싱)을 사용한다. FDM 이란 아날로그 기술이다. FDM 은 논리적 채널로 스펙트럼이나 캐리어를 나눈 다음, 각각의 사용자용으로 각각의 채널에 할당한다. 사용자마다 독립적으로 channel frequency 를 사용할 수 있으며, 그것에 독립적으로 접근할 수 있다. 모든 채널은 서로 중복되지 않게 나뉘어진다.



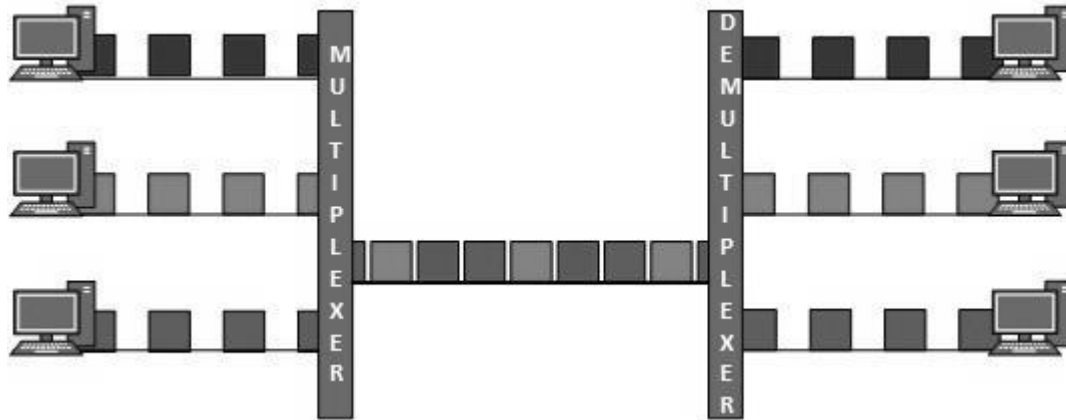
Frequency Division Multiplexing

2. Time Division Multiplexing

TDM 은 기본적으로 디지털 시그널에 적용되지만, 아날로그 시그널에도 적용될 수 있다. TDM 에서 공유 채널은 time slot 라는 방식으로 사용자들 사이에서 나뉘어진다.

사용자 마다 단지 제공된 time slot 내에서만 데이터를 전송할 수 있다. Digital signals 는 특정한 time slot 에서 전송할 수 있는 최적 크기의 프레임으로 나뉜다.

TDM 은 동기식 모드로 작동한다. 양쪽 끝의 Multiplexer 와 De-multiplexer 는 정확하게 동기식으로 작동하며, 반대방향의 채널에서는 서로 교체되기도 한다.



Time Division Multiplexing

3. Wavelength Division Multiplexing

Light 은 다양한 wavelength (colors)을 갖고 있다. fiber optic mode 에서, 다수의 optical carrier signals 은 서로 다른 파장을 사용함으로써 광섬유를 multiplexed 한다. 이것은 analog multiplexing technique 이며, 개념적으로는 FDM 과 동일한 방식으로 진행되지만, 빛을 시그널처럼 사용한다.



Wavelength Division Multiplexing

4. Code Division Multiplexing

Multiple data signals 은 Code Division Multiplexing 을 사용하여 단일 주파수로 전송될 수 있다. FDM 은 주파수를 보다 작은 채널로 나누지만, CDM 은 이용자로 하여금 full bandwidth 를 사용해서 언제든지 독특한 코드로 시그널을 전송할 수 있도록 한다. CDM 은 직교 코드(orthogonal codes)를 사용하여 시그널을 전파한다.

각 스테이션에는 chip 이라 부르는 유일 코드가 할당된다. 시그널은 독립적으로 이 코드와 함께 whole bandwidth 내에서 돌아다닌다. 따라서 리시버는 자신에게 도착하는 chip code signal 에 대하여 미리 알고 있어야 한다.

XIII. SWITCHING

Switching 이란 포트에서 포트로 패킷을 목적지로 보내는 과정이다. 데이터가 한 포트에 들어올 때, 그것을 ingress 라 부르고, 나갈 때, egress 라 부른다. 통신 시스템에는 수많은 스위치와 노드가 포함되어 있다. 크게 말해서, switching 은 두 개의 카테고리로 나눈다:

. Connectionless:

The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.

. Connection Oriented:

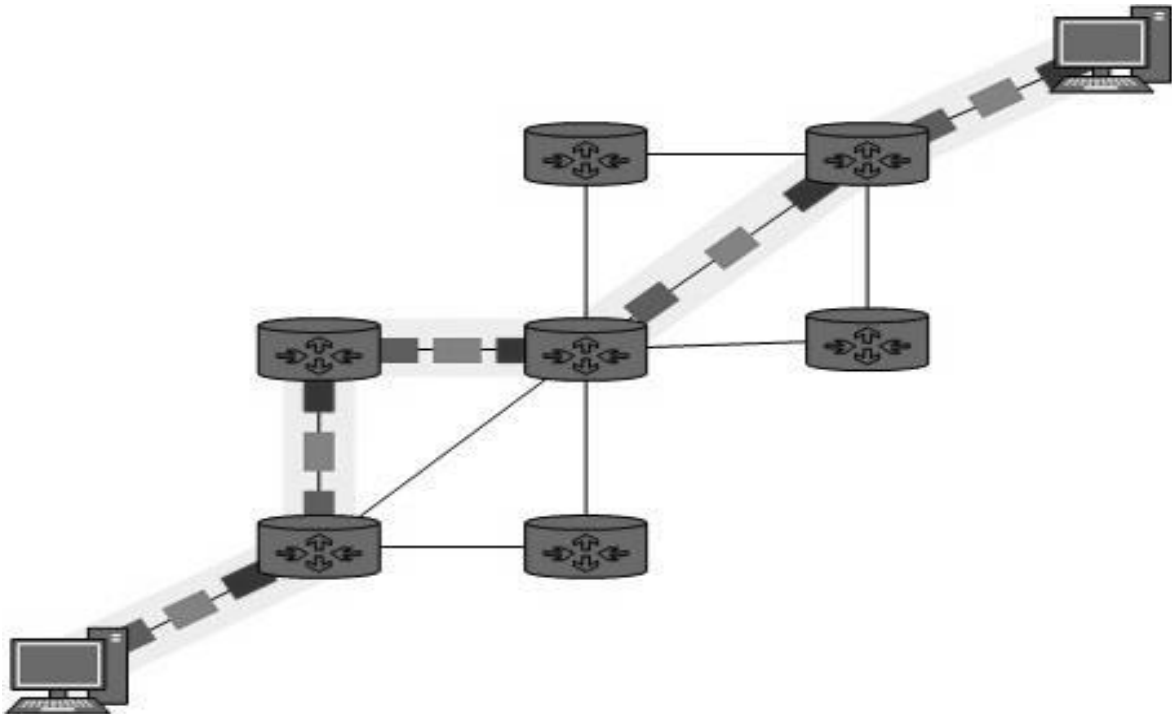
Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

1. Circuit Switching

두 노드가 전용선으로 서로 통신하는 것을 circuit switching 이라 부른다. 데이터가 다닐 수 있는 미리 정해진 루트가 필요하며, 외부의 어떠한 데이터도 허용되지 않는다. 데이터를 전송하는 circuit switching 에서, 회로(circuit)는 데이터 전송이 가능하도록 설치되어야 한다.

Circuits 는 영원할 수도 일시적일 수도 있다. circuit switching 을 사용하는 어플들은 다음과 같은 3 가지의 단계(phase)를 구성한다:

- . Establish a circuit
- . Transfer the data
- . Disconnect the circuit



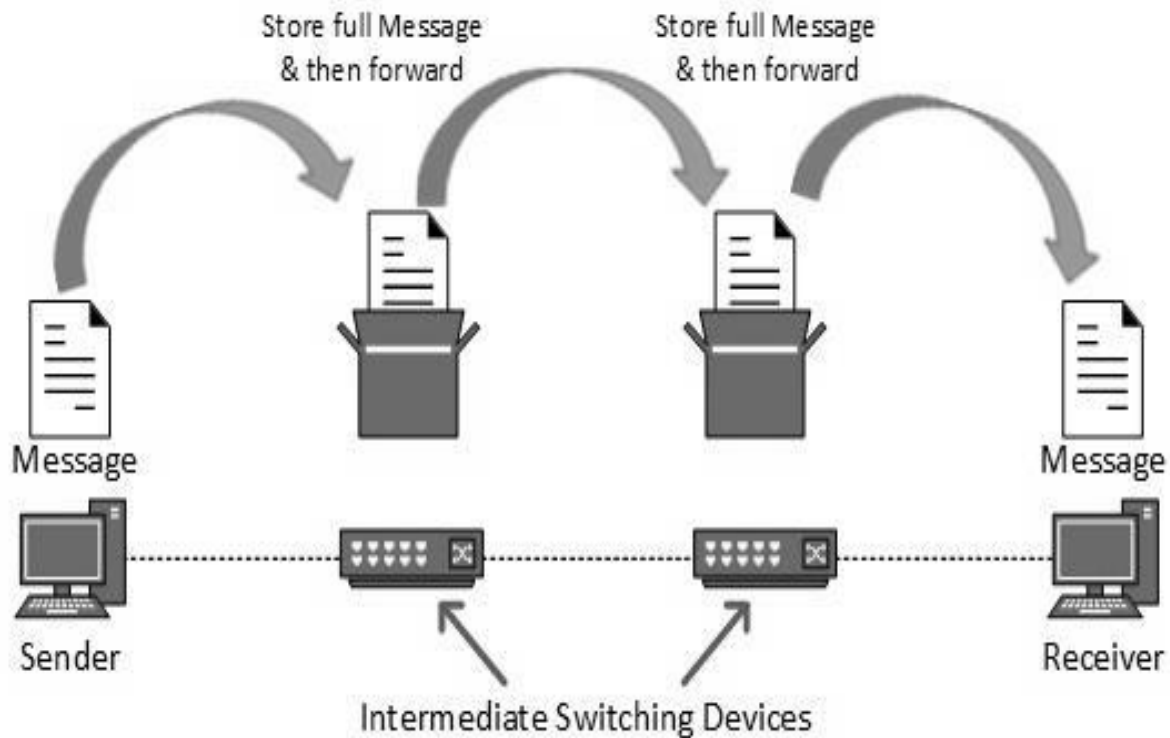
Circuit Switching

Circuit switching 은 voice applications 용으로 설계되었다. 전화는 가장 좋은 예의 circuit switching 이다. 이용자가 전화를 하기 전에, caller 와 callee 간의 가상 통로가 네트워크 전체에 설치되어야 한다.

2. Message Switching

이 기법은 circuit switching 과 packet switching 의 중간쯤에 해당된다. message switching 에서, 모든 message 는 낱개의 데이터(data unit)로 취급되어, 전체가 스위칭되어 전송된다.

message switching 에서 작동하는 스위치는 먼저 전체 메시지를 받고, 다음 단계로 전송할 수 있는 자원(기기)을 확인할 때까지 그것을 buffer 한다. 대량의 메시지를 받았으나 자원을 확인하기 어렵다면, 그 메시지는 임시로 저장되어 스위칭되기를 기다린다.



Message Switching

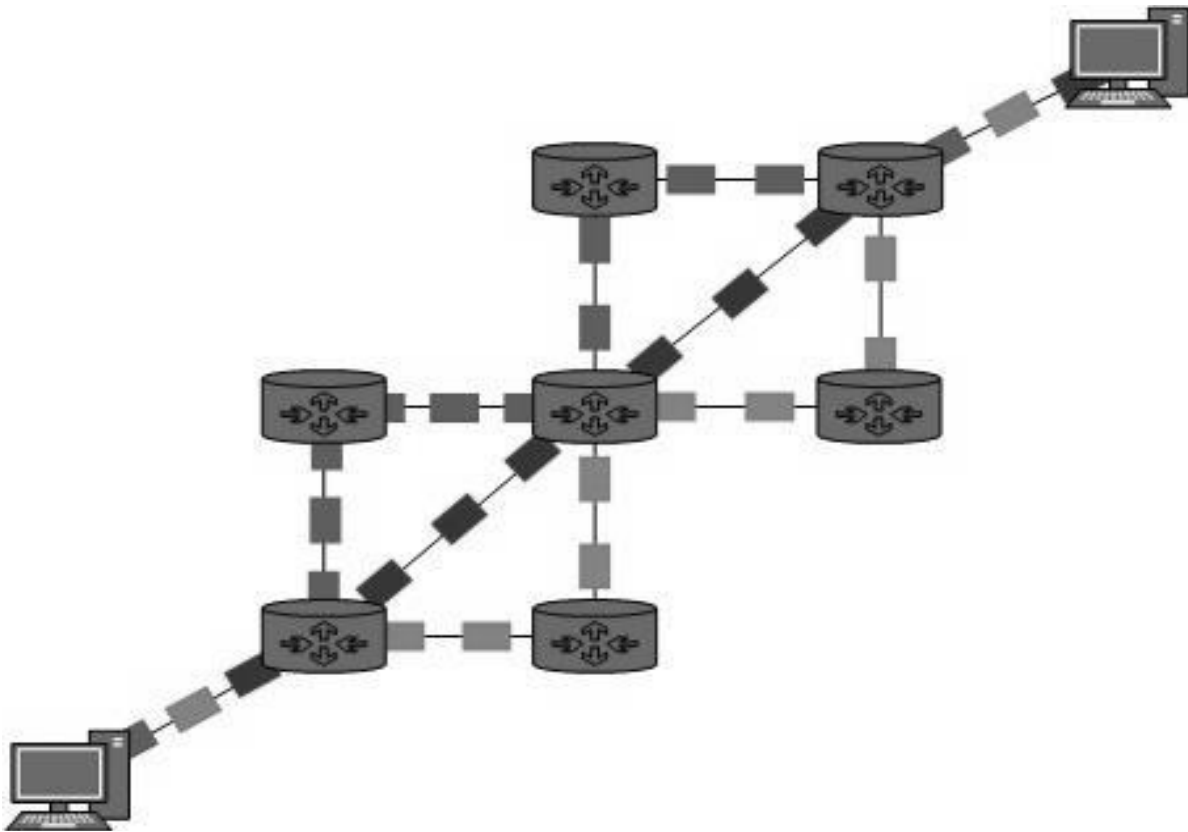
이 기법도 circuit switching 처럼 모든 통신로가 단지 두 개의 엔티티로 막혀있으므로, circuit switching 의 대체기법으로 여겨졌다. 또한 Message switching 은 packet switching 을 대신해 사용하기도 한다. Message switching 의 단점은 다음과 같다:

- . Every switch in transit path needs enough storage to accommodate entire message.
- . Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- . Message switching was not a solution for streaming media and real-time applications.

3. Packet Switching

message switching 의 단점이 packet switching 에 대한 아이디어를 발생시켰다. 이것은 전체 메시지를 패키즈라고 부르는 보다 작은 chunks 로 쪼갬다. switching information 가 각 패키즈의 헤더에 추가되어 있어서 독립적으로 전송된다.

intermediate networking devices 에서 작은 크기의 패킷즈를 저장하는 것은 보다 편리하며, 이것들은 carrier path 에서나 스위치의 internal memory 에서나 많은 자원을 필요로 하지 않는다.



Packet Switching

Packet switching 은 다수의 어플에서 발생한 packets 이 carrier 에서 multiplex 될 수 있으므로 line efficiency 를 높인다. internet 은 packet switching technique 을 사용한다.

XIV. DATA LINK LAYER INTRODUCTION

Data Link Layer 는 OSI Layered Model 의 두 번째 layer 이다. 이 레이어는 가장 복잡한 레이어들 중의 하나이며, 복잡한 기능과 의무를 가지고 있다. Data link layer 는 중요하지만 보이지 않는 하드웨어들을 포함하고 있으며, 상위 레이어에 스스로를 통신매체로 인식시키고 있다.

Data link layer 는 어떤 의미에서 직접 연결된 두 개의 호스트 사이에서 작동한다. 이러한 직접적인 연결은 point to point 나 broadcast 방식일 수도 있다.

Data link layer 는 data stream 을 각각의 비트 별로 시그널로 변환시켜서 기본 하드웨어에 보내는 책임이 있다. 수신이 종료될 때, Data link layer 는 하드웨어에서 전기시그널 형태로 되어 있는 데이터를 추출한 다음에, 그것을 수용 가능한 프레임 포맷으로 모아, 상위 레이어에 전달해 준다.

Data link layer 는 두 가지의 sub-layers 를 갖는다:

- . Logical Link Control: It deals with protocols, flow-control, and error control.
- . Media Access Control: It deals with actual control of media.

1. Functionality of Data-link Layer

Data link layer 는 상위 레이어들 대신하여 많은 임무를 수행하는데, 다음과 같다:

1)Framing:

Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver end, data link layer picks up signals from hardware and assembles them into frames.

2)Addressing:

Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

3)Synchronization:

When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

4)Error Control:

Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

5)Flow Control:

Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

6)Multi-Access:

When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

XV. ERROR DETECTION AND CORRECTION

전송되는 동안 데이터를 망가뜨리는 많은 원인이 있다: noise, cross-talk etc. 상위 레이어들은 일반적인 네트워크 구조에 맞춰 작동한다. 상위 레이어들은 시스템 간에 error-free transmission 을 기대한다. 대부분의 어플들은 에러 데이터가 발생하면 기대한 만큼 작동하지 않는다. 그러나 Voice 와 video 어플들은 영향을 덜 받아서 어떤 에러에 대해서는 잘 작동하기도 한다.

Data-link layer 는 프레임(data bit streams)들이 정확하게 전송되었는지를 확인하기 위하여 error control mechanism 을 사용한다. 그러나 에러 통제기법을 이해하기 위하여, 에러의 종류가 무엇인지 아는 것이 중요하다.

1. Types of Errors

3 종류의 에러가 있다:

1)Single bit error:



Single bit error

In a frame, there is only one bit, anywhere though, which is corrupt(오염).

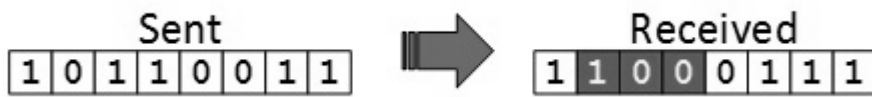
2)Multiple bits error:



Multiple bits error

Frame is received with more than one bits in corrupted state.

3)Burst error:



Burst error

Frame contains more than 1 consecutive bits corrupted.

2. Error control mechanism 은 2 가지가 있다:

- . Error detection
- . Error correction

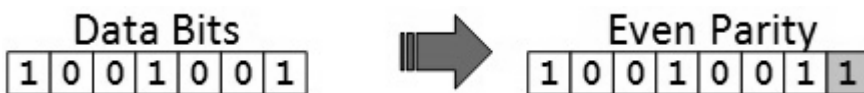
1)Error Detection

접수된 프레임의 에러들은 Parity Check 와 Cyclic Redundancy Check (CRC)를 사용하여 탐지된다. 두 경우 모두 극소수의 비트를 추가하여 실재 데이터와 함께 보내서 반대쪽에서 접수된 데이터가 보낸 것과 같은지를 확인한다. 리시버에서 counter-check 가 틀리면, 그 비트들은 오염된 것으로 간주된다.

(1-1)Parity Check:

한 개의 추가 비트를 최초의 비트와 함께 보내서 even parity 의 경우에는 odd 를, odd parity 의 경우에는 even 을 만든다.

프레임을 만들 때, 센터는 그 속에 있는 1 의 숫자를 계산한다. 예를 들어, even parity 를 사용하고, 1 의 숫자가 even 이라면, 0 인 값의 한 개 비트가 추가된다. 이 방법은 1 의 숫자를 even 으로 유지한다. 만일 1 의 숫자가 odd 라면, 1 값인 비트를 추가하여 even 으로 만든다.

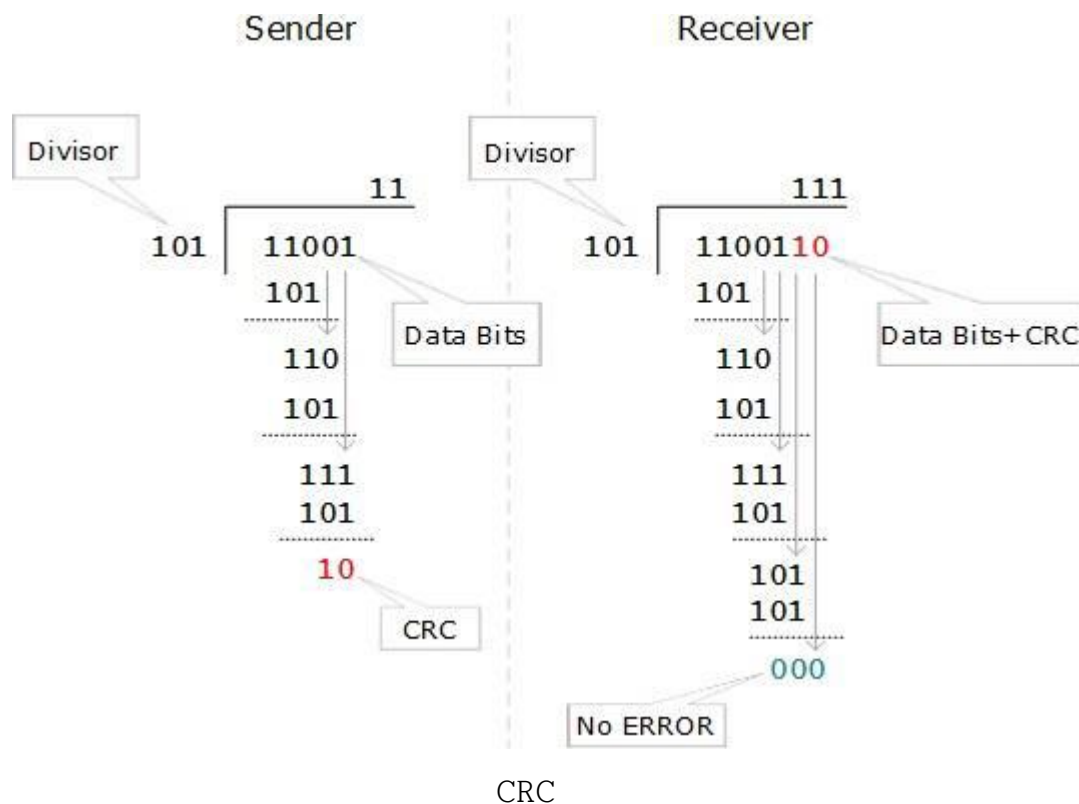


Even Parity

리시버는 단지 프레임에서 1 의 숫자만 계산한다. 1 의 숫자가 even 이고 even parity 를 사용한다면, 그 프레임은 오염되지 않은 것으로 간주되어 접수된다. 만일 1 의 숫자가 odd 이고 odd parity 를 사용한다면, 그 프레임은 아직 되지 않은 것이다.

(1-2)Cyclic Redundancy Check (CRC): 순환 중복 검사

CRC 는 접수된 프레임에 유효한 데이터가 포함되어 있는지를 탐지하는 또 다른 기법이다. 이 기법에는 전송된 데이터 비트의 이진적 분리를 포함한다. Divisor(제수)는 polynomials(다항식)을 사용하여 결과를 생산된다. 센터는 보낸 비트에 대한 division operation 을 수행하여 나머지를 계산한다. 초기의 비트를 보내기 전에, 센터는 초기 비트 끝에 그것의 나머지를 첨가한다. Actual data bits plus the remainder 를 codeword 라 부르며, 센터는 codewords 처럼 데이터를 전송한다.



반대쪽 끝에 있는 리시버도 똑 같은 CRC divisor 를 사용하여 codewords 에 관한 divisiosn operation 을 수행한다. 만일 remainder 가 모두 zeros 라면, 그 데이터는 접수된다. 그렇지 않다면, 어떤 데이터가 전송 중에 데이터 오염이 발생한 것으로 간주된다.

2)Error Correction

디지털 세상에서, error correction 에는 두 가지 방법이 있다:

(2-1) Backward Error Correction:

리시버가 접수된 데이터에서 에러를 감지하면, 센터에게 다시 보내도록 요청한다.

(2-2) Forward Error Correction:

리시버가 접수된 데이터에서 에러를 감지하면, error-correcting code 를 실행시켜서 자동으로 회복시켜 에러의 수정을 돕는다.

첫 번째인 Backward Error Correction 은 단순하며, 반송비가 비싸지 않는 경우에 효율적으로 사용된다. 예를 들어, fiber optics 이다. 그러나 무선 전송의 반송인 경우에는 비용이 엄청날 수 있다. 후자의 경우에는 Forward Error Correction 의 사용이 바람직하다.

data frame 에서 에러를 수정하기 위하여, 리시버는 그 프레임의 어떤 비트가 오염되었는지를 정확하게 알아야 한다. 에러 비트를 찾기 위하여, 에러 탐지용인 패리티 비트처럼 사용되는 추가 비트를 사용한다. 예를 들어, ASCII words (7 bits data)를 받을 때, 8 개의 information 가 필요하다: 처음 7 개는 어떤 비트가 에러인지를 말해주고, 에러가 없다는 것을 알려주는 1 개 이상의 비트.

XVI. DATA LINK CONTROL AND PROTOCOLS

Data-link layer 는 point-to-point flow 와 error control mechanism 의 실행에 책임이 있다.

1. Flow Control

data frame (Layer-2 data)이 단일매체를 통해 한 호스트에서 다른 호스트로 보내졌을 때, sender 와 receiver 는 동일한 속도로 작업해야 한다. 즉, sender 는 리시버가 접수하여 처리할 수 있는 속도로 데이터를 보내야 한다. sender 나 receiver 의 속도가 다르면 어떻게 되는가? 센더가 너무 빨리 보내서 리시버에 과부하가 걸리면(swamped), 데이터 손실이 발생할 수 있다.

데이터 통제에는 두 종류의 메커니즘이 있다:

1)Stop and Wait :

이 flow control mechanism 은 데이터 전송이 이루어지면, 보내온 데이터-프레임이 접수된 것을 인식할 때까지 센더가 멈춰서 기다린다.

2)Sliding Window:

이 flow control mechanism 에서, sender와 receiver 둘 다 acknowledgement 를 보낸 다음에, 둘 다의 데이터-프레임의 수가 일치하여야 한다. 위에서 배웠듯이, stop and wait flow control mechanism 은 자원을 낭비하므로, 이 protocol 은 가능한 한 기본 자원을 많이 사용하려고 한다.

2. Error Control

data-frame 이 전송될 때, 전송 중에 데이터를 잃어버리거나 오염되어 받을 수도 있다. 두 경우 모두, 리시버는 정확한 데이터-프레임을 받지 못하고, 센더는 어떤 손실이 발생했는지를 알지 못한다. 이런 경우에, sender 와 receiver 모두 데이터-프레임의 손실과 같은 transit errors 를 탐지할 수 있는 프로토콜을 마련하여, sender 쪽에서 data-frame 을 다시 보내거나 receiver 쪽에서 이전의 데이터-프레임을 재전송하도록 요구할 수 있도록 하여야 한다.

error control mechanism 의 필요조건은 다음과 같다:

. **Error detection:** The sender and receiver, either both or any, must ascertain that there is some error in the transit.

. **Positive ACK:** When the receiver receives a correct frame, it should acknowledge it.

. **Negative ACK:** When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

. **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout, the sender retransmits the frame, thinking that the frame or its acknowledgement is lost in transit.

XVII. NETWORK LAYER INTRODUCTION

OSI model 의 Layer-3 를 Network layer 라 부른다. Network layer 는 sub-networks 와 internetworking 을 관리하는 호스트와 network addressing 에 관한 옵션을 관리한다.

Network layer 는 subnet 안팎으로 소스로부터 목적지로 패킷을 라우팅하는 책임을 가지고 있다. 두 개의 서로 다른 서브넷은 서로 다른 addressing schemes 또는 non-compatible addressing types 을 가질 수 있다. Protocols 처럼, 서로 다른 두 개의 서브넷은 서로 호환되지 않는 다른 프로토콜에서도 운영할 수 있다. Network layer 는 서로 다른 addressing schemes 와 protocols 를 복사(mapping)하여 소스로부터 목적지까지 패킷을 라우팅할 책임을 가지고 있다.

1. Layer-3 Functionalities

Network Layer 에서 작동하는 기기들은 주로 라우팅에 초점을 맞추고 있다. Routing 에는 단일 목적지로 가기 위한 다음과 같은 여러 가지가 임무가 수행된다:

- . Addressing devices and networks.
- . Populating routing tables or static routes.
- . Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- . Internetworking between two different subnets.
- . Delivering packets to destination with best efforts.
- . Provides connection oriented and connection less mechanism.

2. Network Layer Features

표준 기능과 더불어, Layer 3 는 다양한 특징을 제공한다:

- . Quality of service management
- . Load balancing and link management
- . Security
- . Interrelation of different protocols and subnets with different schema.

- . Different logical network design over the physical network design.
- . L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Internet protocol 은 인터넷에서 end-to-end 디바이스가 통신하는 것을 돕는 Network Layer protocol 을 참조하였다. 두 가지가 있다. 수 십년 동안 세상을 지배했지만 지금은 뒤쳐진 address space 를 다루는 IPv4 와 이것을 대체하기 위해 만들어 그것의 문제점을 해결하려는 목적의 IPv6 가 그것이다.

XVIII. NETWORK ADDRESSING

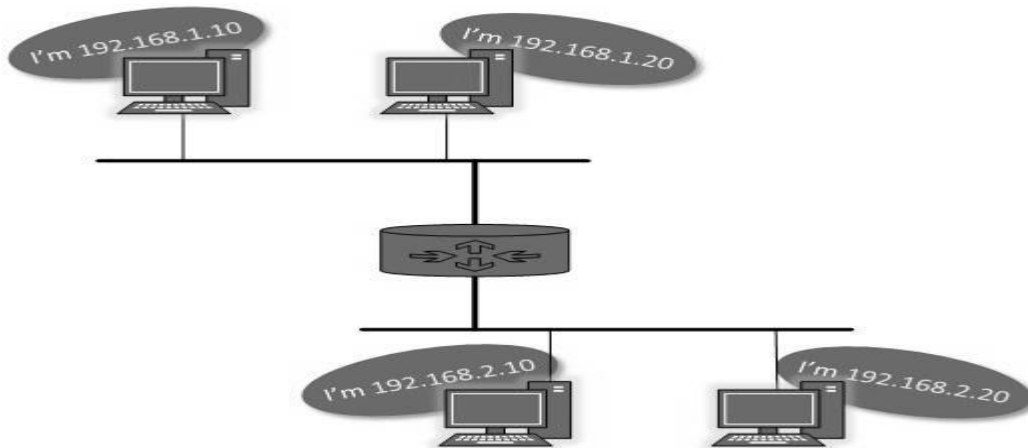
network addressing 은 Network Layer 의 주요 업무들 중의 하나이다. Network Addresses 는 항상 논리적이다. 다시 말해서, 이것들은 적합한 configurations 로 변경이 가능한 소프트웨어 의존형 어드레스이다.

network address 는 항상 host / node / server 에 포인트를 또는 전체 넷을 표현할 수 있다. Network address 는 항상 network interface card 에서 configured 되며, 일반적으로 Layer-2 communication 기기의 MAC address (hardware address or layer-2 address)를 갖고 있는 시스템에 의해 복사돼 사용(mapped) 된다.

현존하는 다양한 network addresses 는 다음과 같다:

- . IP
- . IPX
- . AppleTalk

이 글에서는 현재 실제로 사용되는 IP 에 대해서만 알아보기로 한다.



Network Addressing

IP addressing 에서는 hosts 와 network 를 차별화시키는 메커니즘을 제공한다. IP addresses 가 계층방식으로 할당되기 때문에, host 는 항상 특별한 넷에 소속된다. 자신의 섭넷 밖으로 통신하려는 호스트는 packet/data 를 보내야 하는 destination network address 를 알아야 한다.

다른 섬넛의 Host 들은 서로의 위치를 확인하는 메커니즘이 필요하다. 이러한 업무를 DNS 가 하는데, DNS 란 서로 짝(mapped)이 된 원격 호스트의 Layer-3 address 에 그것의 domain name 또는 FQDN(Fully Qualified Domain Name)을 제공하는 서버이다. host 가 원격 호스트의 Layer-3 Address (IP Address)를 파악하면, Gateway 로 그것의 모든 패키츠를 포워드 한다. Gateway 란 destination host 로 패키츠를 라우트하도록 유도하는 모든 정보를 갖고 있는 라우터이다.

Routers 는 다음과 같은 정보를 갖고 있는 routing tables 의 도움을 받는다:

- . Address of destination network
- . Method to reach the network

forwarding request 를 받자마자, 라우터는 목적지를 향해 다음의 hop (adjacent router)로 패키츠를 포워드 한다.

통신선에 있는 그 다음의 라우터도 동일한 일을 하므로, 결과적으로 데이터 패키츠가 목적지에 도달한다.

Network address 는 다음 중 하나이다:

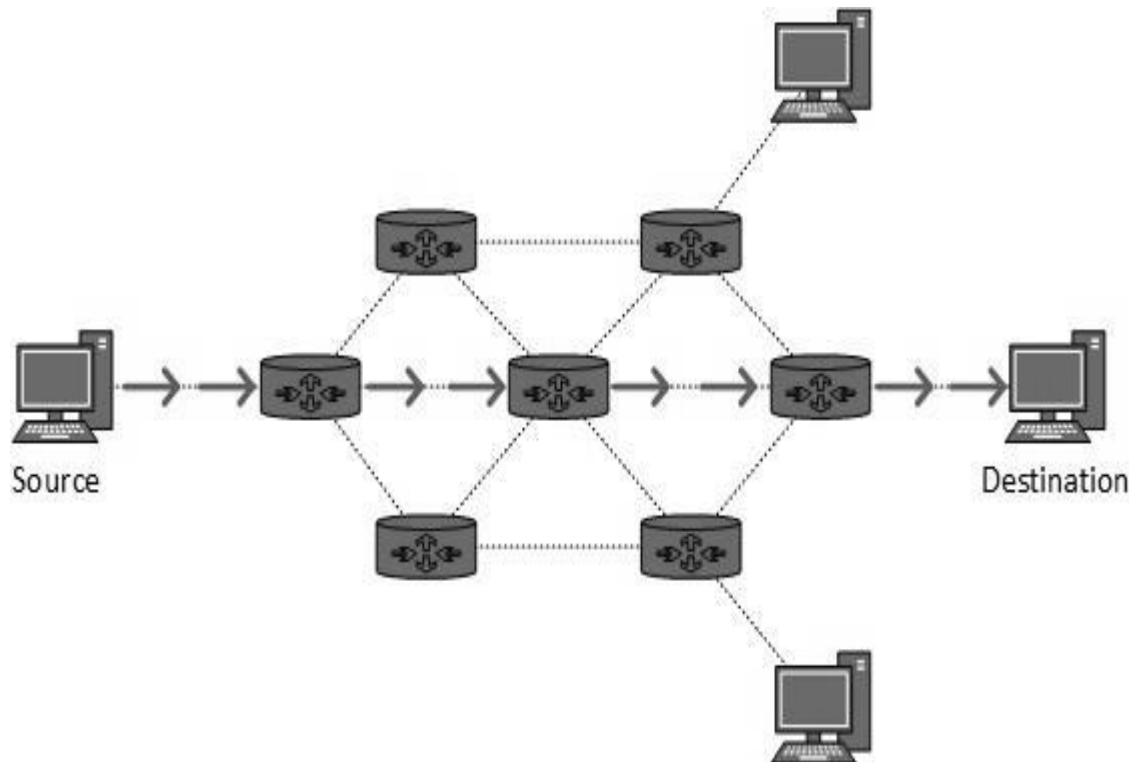
- . Unicast (destined to one host)
- . Multicast (destined to group)
- . Broadcast (destined to all)
- . Anycast (destined to nearest one)

XIX. NETWORK ROUTING

device 가 목적지에 도달하는 복수의 통로를 가지고 있을 때, 항상 다른 것보다 선호하는 특정한 통로를 선택한다. 이런 선택 과정을 Routing 이라 한다. Routing 은 routers 라 부르는 특별한 넷 기기에 의해 이루어지거나 software 에 의해 이루어진다. 그렇지만 소프트웨어 의존형 라우터는 기능성과 범위가 제한적이다.

1. Unicast routing

인터넷과 인트라넷에서 대부분의 트래픽이란 unicast data 또는 unicast traffic 이라 부르며, 특정한 목적지로 보내는 것을 말한다. 인터넷에서 unicast data 를 라우팅하는 것을 unicast routing 이라 한다. 이것은 가장 간단한 라우팅 형태인데, 그 이유는 목적지가 이미 잘 알려져 있기 때문이다. 그러므로 라우터는 단지 라우팅 테이블을 조사하여 다음의 hop 로 패킷을 포워드하면 된다.



Unicast routing

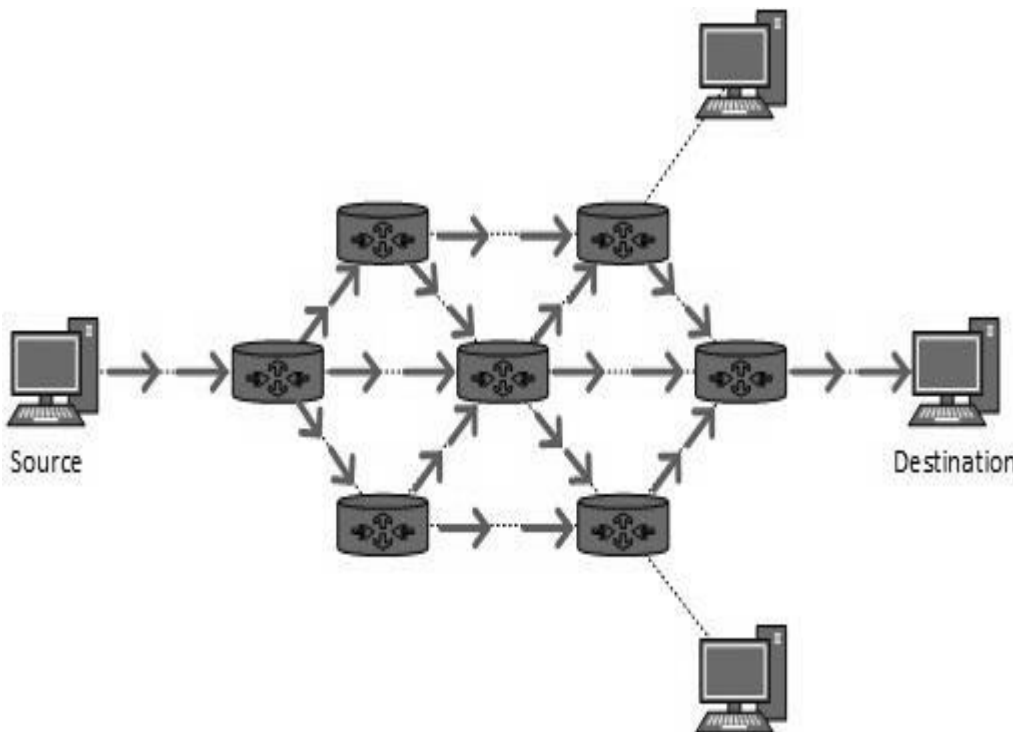
2. Broadcast routing

초기값에 의해, broadcast packets 은 어떤 넷의 라우터로 라우트되거나 포워드 되지 않는다. 먼저 Routers 는 broadcast domains 을 configured 하여야 한다.

Broadcast routing 은 두 가지 방법(algorithm)으로 이루어진다:

. A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting. This method consumes lots of bandwidth and router must destination address of each node.

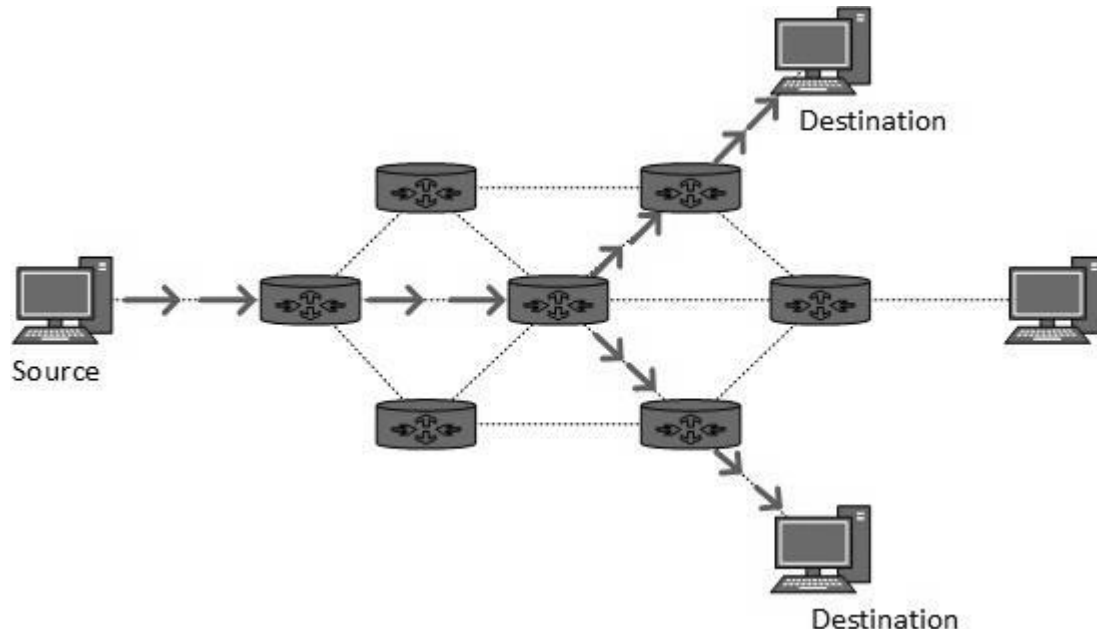
.Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.



Broadcast routing

3. Multicast Routing

Multicast routing 은 broadcast 의 특별한 경우이며, 커다란 차이가 있다. broadcast routing 에서, packets 는 비록 원치 않는다하더라도 모든 노드에 전송된다. 그러나 Multicast routing 에서 그 데이터는 단지 그 패킷을 받기 원하는 노드에만 전달된다.



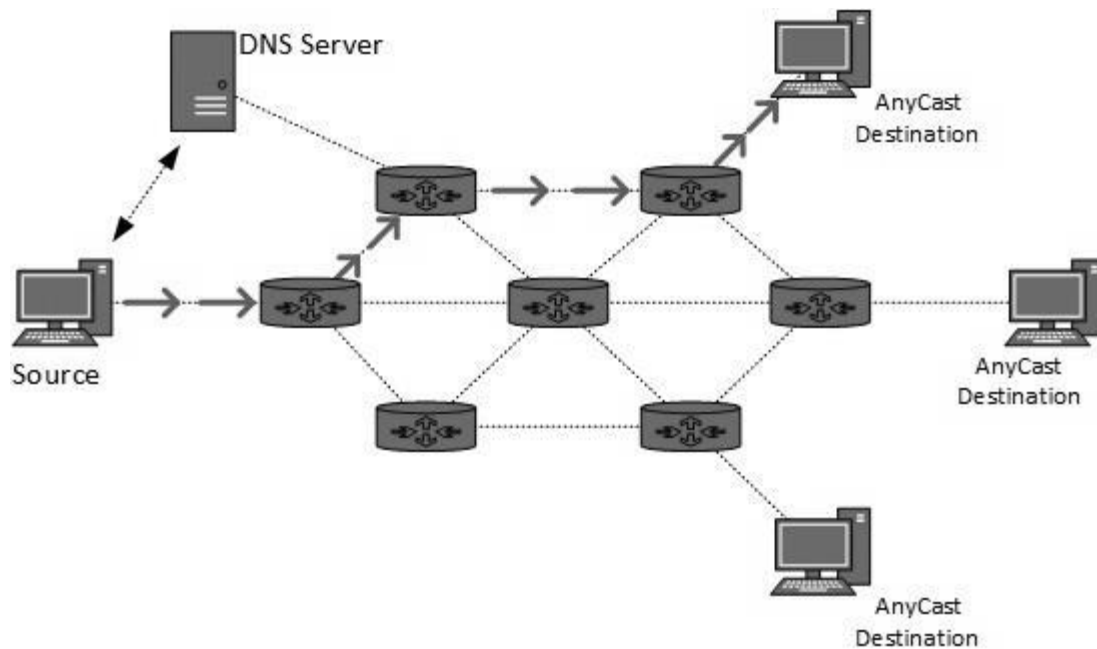
Multicast routing

Router 는 multicast packets (or stream)을 받기 원하는 노드가 있으며, 단지 그곳에만 보내야 한다는 것을 알아야 한다. Multicast routing 은 looping 을 피하기 위하여 spanning tree protocol 을 사용한다.

Multicast routing 또한 duplicates 와 loops 을 탐지하여 폐기하는 reverse path forwarding technique 을 사용한다.

4. Anycast Routing

Anycast packet forwarding 은 복수의 hosts 가 논리적으로 동일한 어드레스를 갖도록 하는 메커니즘이다. 이러한 논리적 어드레스를 갖고 있는 패킷이 접수될 때, routing topology 에서 가장 가까이 있는 호스트로 보낸다.



Anycast routing

Anycast routing 은 DNS server 의 도움을 받는다. Anycast packet 가 접수될 때마다, 그것을 보낼 DNS 를 요구한다. DNS 는 그것에 콘피겨되어 있는 가장 가까운 IP 의 IP address 를 제공한다.

5. Routing Algorithms

routing algorithms 은 다음과 같다:

1) Flooding:

Flooding 은 가장 단순한 packet forwarding 방법이다. 패킷이 접수될 때, 라우터들은 모든 인터페이스에 그것을 보내지만, 이미 접수된 것은 제외시킨다. 이것은 넷에 너무나 많은 부담을 주며, 많은 중복 패킷들이 넷에서 방황하게 된다.

Time to Live (TTL)는 패킷의 무한 루핑을 피하기 위하여 사용될 수 있다.

Selective Flooding 이라 부르는 또 다른 flooding 방법이 있는데, 이것은 넷의 overhead 를 감소시킨다. 이 방법에서 라우터는 선택된 것을 제외하고는 나머지 모든 인터페이스에 flood out 하지 않는다.

2)Shortest Path:

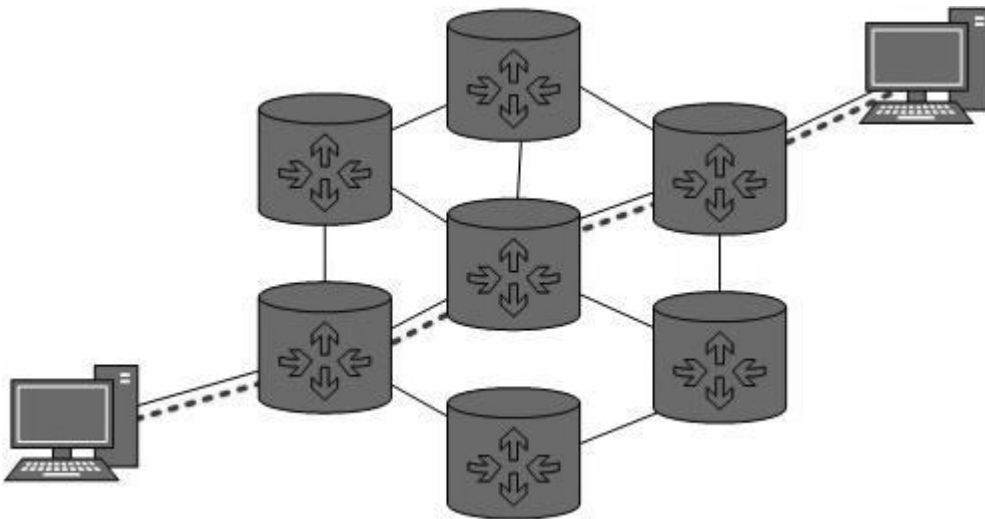
네트의 Routing decision 은 대체로 소스와 목적지 간의 비용을 근거로 이루어진다. 이 때 Hop count 는 중요한 역할을 한다. Shortest path 란 최소한의 hops 를 가진 통로를 결정하기 위하여 다양한 알고리즘을 사용하는 기법이다.

XX. INTERNETWORKING

실 세계에서, 동일한 행정 시스템의 넷들은 일반적으로 말해서 지리적으로 산재해 있다. 서로 같은 또는 서로 다른 두 가지의 넷을 연결하기 위한 조건이 있다. 이러한 두 넷 간의 Routing 을 internetworking 이라 한다.

넷들은 protocol, topology, Layer-2 network and addressing scheme 과 같은 다양한 변수(parameters)에 따라 서로 다른 것으로 여겨진다.

internetworking 에서, 라우터는 서로의 주소에 대한 지식을 가지고 있다. 이것들은 정적으로 다른 넷으로의 전송을 위해 콘피거되거나 internetworking routing protocol 을 사용하여 파악할 수 있다.

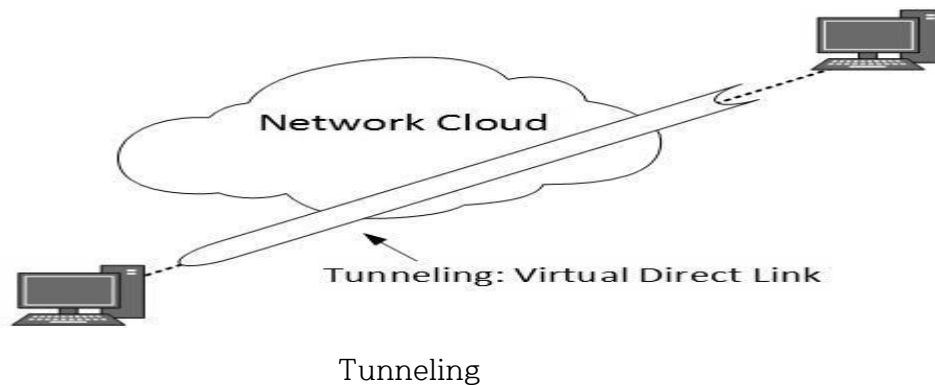


Routing

1. Tunneling

지리적으로 떨어져 있는 두 개의 넷이 있다면, 이들 간에 전용선을 깔거나, 중개 넷을 통해 데이터를 전달하여야 한다.

Tunneling 이란 intermediate networking complexities 를 패싱함으로써, 두 개 이상의 동일한 넷이 서로 통신하는 메카니즘이다. Tunneling 은 양쪽 끝에 콘피거 된다.



데이터가 터널의 한 쪽 끝에 들어올 때, 그것은 감지된다. 이렇게 감지된 데이터는 그 다음에 있는 intermediate 로 라우터되어 그 터널 반대 끝에 전송된다. 터널의 양쪽 끝은 직접적으로 연결된 것처럼 여겨지며, 감지작업(tagging)은 계속해서 network 에서 이루어진다.

2. Packet Fragmentation

대부분의 인터넷 세그먼트는 1500 바이트에 고정된 maximum transmission unit (MTU)를 가지고 있다. data packet 은 어플에 따라 패킷 길이가 크기도 하고 작기도 한다. Transit path 에 있는 기기들은 자신들의 hardware 와 software capabilities 을 가지고 있으며, 이것들이 데이터의 처리량과 처리할 수 있는 패킷의 크기를 결정한다.

data packet size 가 transit network 에서 처리할 수 있는 크기보다 작거나 같다면, 정상적으로 처리된다. 그러나 패킷이 크다면, 작은 조각으로 분해한 다음에 포워드 한다. 이러한 것을 packet fragmentation 이라 부르며, 각 fragment 에는 동일한 출발지 및 목적지 어드레스가 들어있어 transit path 로 쉽게 전달된다. 수신자의 끝 단계에서 이것은 다시 합쳐진다.

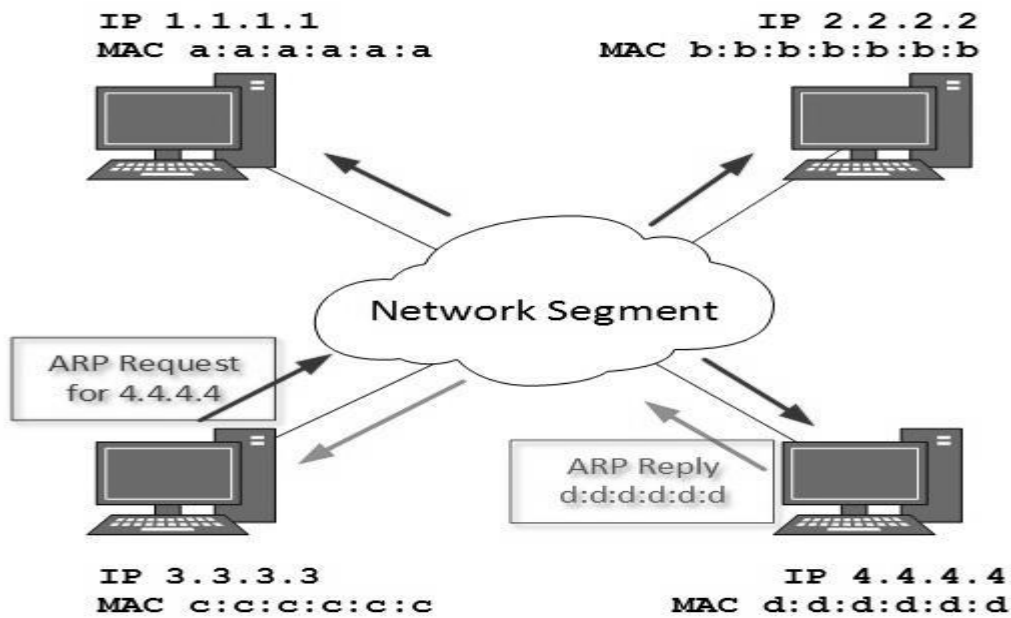
XXI. NETWORK LAYER PROTOCOLS

넷 상의 모든 컴퓨터들은 자신들을 유일하게 식별할 수 있는 IP address 를 가지고 있다. IP address 란 Layer-3 (Network Layer) logical address 이다. 이 어드레스는 컴퓨터가 재기동될 때 바뀔 수 있다. 컴퓨터는 한 타임에 하나의 IP 를, 그리고 다른 타임에는 다른 IP 를 갖는다.

1. Address Resolution Protocol (ARP)

통신하는 동안, 호스트는 동일한 브로드캐스트 도메인이나 넷에 속해 있는 목적지 컴퓨터의 Layer-2 (MAC) address 가 필요하다. MAC address 는 물리적으로 컴퓨터의 Network Interface Card (NIC)에서 인식되며, 결코 변하지 않는다.

그러나 공용 도메인의 IP address 는 드물지만 변하기도 한다. 만일 NIC 가 어떤 잘못으로 변한다면, 그 MAC address 역시 변한다. 이러한 방식으로 Layer-2 communication 이 이루어지기 때문에, 양자간의 정확한 일치(mapping)가 필요하다.



ARP Mechanism

broadcast domain 에 있는 원격 호스트의 MAC 어드레스를 알기 위하여, 통신을 시작하려는 컴퓨터는 “ Who has this IP address?” 라고 물으면서 ARP broadcast message

보낸다. 그것은 브로드캐스트이기 때문에, network segment (broadcast domain)에 있는 모든 호스트들은 이 패킷을 받아 처리한다. ARP packet 에는 destination host 의 IP 어드레스를 포함하고 있으며, 송신쪽 호스트는 수신쪽 호스트가 응답하길 원한다. 호스트가 자신을 목적지로 한 ARP 패킷을 접수할 때, 자신의 MAC 어드레스와 함께 되돌아 응답한다.

일단 호스트가 destination MAC address 을 얻으면, Layer-2 link protocol 을 사용하여 원격 호스트와 통신한다. IP mapping 을 위해 이 MACs 는 송수신 호스트 양쪽 모두의 ARP cache 에 저장된다. 나중에 통신이 필요할 때, 직접적으로 자신들 각자의 ARP cache 를 참조한다.

2. Internet Control Message Protocol (ICMP)

ICMP 는 network diagnostic and error reporting protocol 이다. ICMP 는 IP protocol 의 한 부류(suite)에 속하며, carrier protocol 로 IP 를 사용한다. ICMP packet 이 만들어진 다음에, 그것은 IP packet 속에서 봉해진다. IP 자체가 best-effort non-reliable protocol 이기 때문에, ICMP 도 마찬가지다.

넷에 대한 어떤 feedback 은 시작한 host 에 재전송된다. 넷에 어떤 에러가 발생하면, ICMP 에 의해 보고된다. ICMP 에는 수 십 가지의 diagnostic and error reporting messages 가 포함되어 있다

ICMP-echo and ICMP-echo-reply 는 end-to-end hosts 의 도달여부(reachability)를 체크하기 위하여 가장 일반적으로 사용되는 ICMP messages 이다. Host 는 ICMP-echo request 를 접수한 다음, ICMP-echo-reply 를 되돌려 보낸다. transit network 에 어떤 문제가 있다면, ICMP 이 그 문제를 알려준다.

3. Internet Protocol Version 4 (IPv4)

IPv4 는 32-bit addressing scheme 이며, TCP/IP host addressing mechanism 으로 사용된다. IP addressing 으로 TCP/IP network 의 모든 호스트를 유일하게 식별할 수 있다.

IPv4 는 계층적 addressing scheme 을 제공하므로 넷을 서브넷으로 나눌 수 있고, 각각은 잘 정의된 숫자의 hosts 를 갖는다.

IP addresses 는 다양한 카테고리로 세분된다:

. **Class A:** It uses first octet for network addresses and last three octets for host

addressing.

- . **Class B:** It uses first two octets for network addresses and last two for host addressing.
- . **Class C:** It uses first three octets for network addresses and last one for host addressing.
- . **Class D:** It provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- . **Class E:** It is used as experimental.

IPv4 또한 잘 정의된 어드레스 스페이스를 가지고 있어서 사적 용도의 addresses (not routable on internet), 그리고 공적 용도의 addresses (provided by ISPs and are routable on internet)에서 사용될 수 있다.

4. Internet Protocol Version 6 (IPv6)

IPv4 addresses 의 문제점을 해결하려는 노력이 Protocol version 6 를 탄생시켰다. IPv6 는 미래를 위해 풍부한 어드레스를 제공하기 위하여, 128 bit 의 노드를 어드레스 할 수 있다.

IPv6 에서 Anycast addressing 을 도입하고 있지만, broadcasting 의 개념은 사용하지 않았다. IPv6 는 기기들이 스스로 IPv6 address 를 확보해서 서브넷과 통신하도록 하고 있다. 이것은 auto-configuration Dynamic Host Configuration Protocol (DHCP) servers 의 의존성을 무력화 시킴으로써, 비록 서브넷의 DHCP server 가 다운되더라도, 호스트 끼리는 서로 통신할 수 있다.

IPv6 의 새로운 기능은 IPv6 mobility 이다. Mobile IPv6-equipped machines 는 자신들의 IP 어드레스를 바꿀 필요 없이 휴대할 수 있다.

XXII. TRANSPORT LAYER INTRODUCTION

OSI Model 의 다음 레이어는 Transport Layer (Layer-4)이다. Data 나 data stream 의 운반에 관한 모든 모듈과 프로시저는 이 레이어에서 이루어진다. 모든 다른 레이어처럼, 이 레이어도 원격 호스트의 동료 Transport layer 와 통신한다.

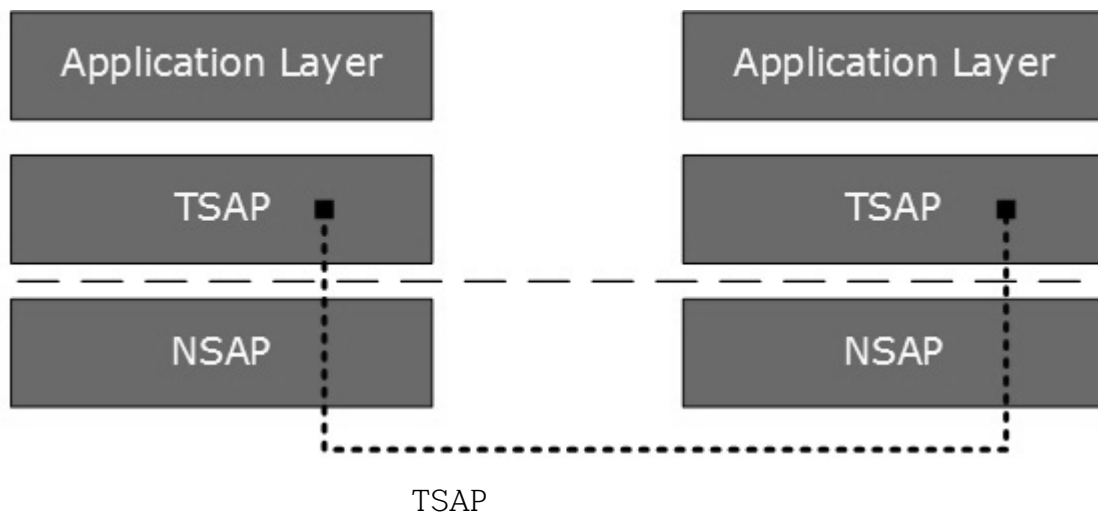
Transport layer 는 원격 호스트의 두 프로세서들 간에 peer-to-peer 와 end-to-end connection 을 제공한다. Transport layer 는 상위 레이어(예, Application layer)로 부터 데이터를 취한 다음에 보다 작은 크기의 세그먼트로 쪼개고, 각 바이트에 번호를 매긴 후, 하위 레이어(예, Network layer)로 전달한다.

1. Functions

- . 이 레이어는 먼저 Application layer 에서 공급된 정보 데이터를 세그먼트라고 부르는 보다 작은 유니트로 쪼갬다. 여기서 세그먼트에 있는 모든 바이트에 번호를 붙여서 이것들의 accounting 을 관리 한다.
- . 이 레이어는 데이터가 보낸 것과 똑 같은 순서로 접수되는 것을 보장한다.
- . 이 레이어는 똑 같은 서브 넷에 속해있든 아니든 호스트 간의 데이터를 end-to-end 방식으로 전달한다.
- . 넷에서 통신하려는 모든 서버 프로세스들은 잘 알려져 있는 Transport Service Access Points (TSAPs)나 port numbers 를 갖추어야 한다.

2. End-to-End Communication

한 호스트의 프로세스는 Port numbers 로 알려진 TSAPs 에 의해 원격 넷의 동료 호스트를 식별한다. TSAPs 는 매우 잘 정의되어 있으며, 동료와 통신하려는 프로세스는 이미 이것을 알고 있어야 한다.



예를 들어, DHCP client 가 원격 DHCP server 와 통신하고자 할 때, 그것은 항상 port number 67 에서 리퀘스트 한다. DNS client 가 원격 DNS server 와 통신하고자 할 때, 그것은 항상 port number 53 (UDP)에서 리퀘스트 한다.

두 개의 중요한 Transport layer protocols 은 다음과 같다:

1) Transmission Control Protocol

It provides **reliable** communication between two hosts.

2) User Datagram Protocol

It provides **unreliable** communication between two hosts.

XXIII. TRANSMISSION CONTROL PROTOCOL

Transmission Control Protocol (TCP)은 Internet Protocols 부류(suite)에서 가장 중요한 프로토콜들 중의 하나이다. 이것은 internet 과 같은 통신 넷에서 데이터 전송용으로 가장 널리 사용되는 프로토콜 이다.

1. Features

.TCP는 신뢰할 수 있는 protocol 이다. 즉, 리시버는 항상 데이터 패킷에 대하여 센터에게 positive 또는 negative acknowledgement 를 보낸다. 그렇게 함으로써 센터는 항상 데이터 패킷이 목적지에 도달했는지 또는 다시 보내야 하는지에 대한 분명한 단서를 얻게 된다.

.TCP는 보낼 때와 똑 같은 순서로 원하는 목적지에 도착했는지를 확인한다.

.TCP는 connection oriented 이다. TCP는 두 개의 원격 포인트들이 실제의 데이터가 보내지기 전에 연결이 설치되어 있을 것을 요구한다.

.TCP는 error-checking 과 recovery mechanism 을 제공한다.

.TCP는 end-to-end communication 을 제공한다.

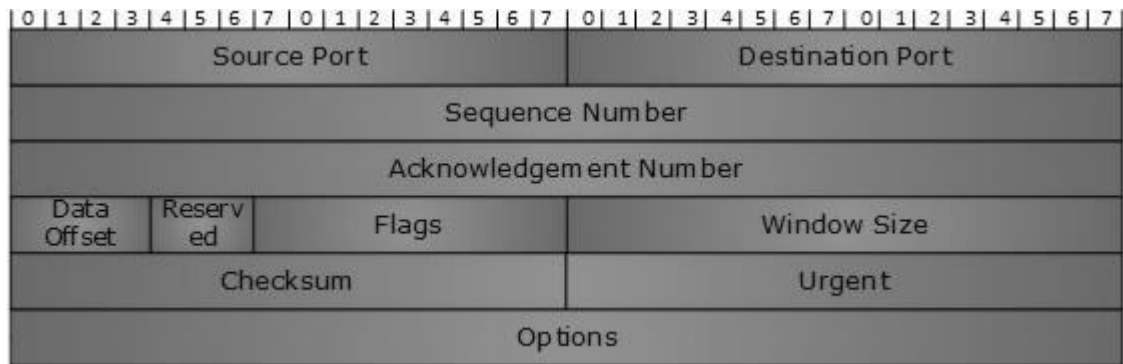
.TCP는 flow control 과 quality of service 를 제공한다.

.TCP는 Client/Server point-to-point mode 에서 운영된다.

.TCP는 full duplex server 를 제공한다. 즉, 그것은 receiver 와 sender 양쪽 모두의 역할을 수행할 수 있다.

2. Header

TCP header 의 길이는 최소 20 bytes 에서 최대 60 bytes 까지이다.



TCP Header

- . **Source Port (16-bits)**: 송신 디바이스에 있는 어플 프로세서의 source port 를 식별한다.
- . **Destination Port (16-bits)**: 수신 디바이스에 있는 어플 프로세서의 destination port 를 판단한다.
- . **Sequence Number (32-bits)**: session 에 있는 세그먼트의 데이터 바이트에 부친 sequence number.
- . **Acknowledgement Number (32-bits)**: ACK flag 가 설정될 때, 이 번호에는 예상되는 데이터 바이트의 다음 순번을 포함하고 있고, 접수한 이전 데이터의 acknowledgement 로 활동한다.
- . **Data Offset (4-bits)**: 이 필드는 TCP header (32-bit words)의 사이즈와 전체 TCP segment 에서 현재의 패킷에 있는 데이터의 offset 둘 다를 의미한다.
- . **Reserved (3-bits)**: 미래용으로 예약되어 있으며 초기값은 0 으로 세트되어 있다.
- . **Flags (1-bit each)**:
- . **Windows Size**: 이 필드는 two stations 간의 flow control 용으로 사용되며, 리시버가 세그먼트용으로 할당한 버퍼(bytes)의 크기를 나타낸다.
즉, 리시버가 얼마나 많은 데이터를 기대하고 있는가를 나타낸다.
- . **Checksum**: 이 필드에는 the checksum of Header, Data, and Pseudo Headers 가 포함되어 있다.
- . **Urgent Pointer**: 이 필드에서는 만일 URG flag 가 1 로 세트되어 있다면, 긴급한 data byte 를 포인트 한다.
- . **Options**: 이것은 정규 헤더에서 커버하지 못하는 추가 옵션을 원활하게 한다. 옵션 필드는 항상 32-bit words 로 묘사된다. 만일 이 필드가 32-bit 미만의 데이터를 포함한다면, 32-bit boundary 에 도달하기 위하여 나머지 비트를 커버하기 위하여 padding 을

사용한다.

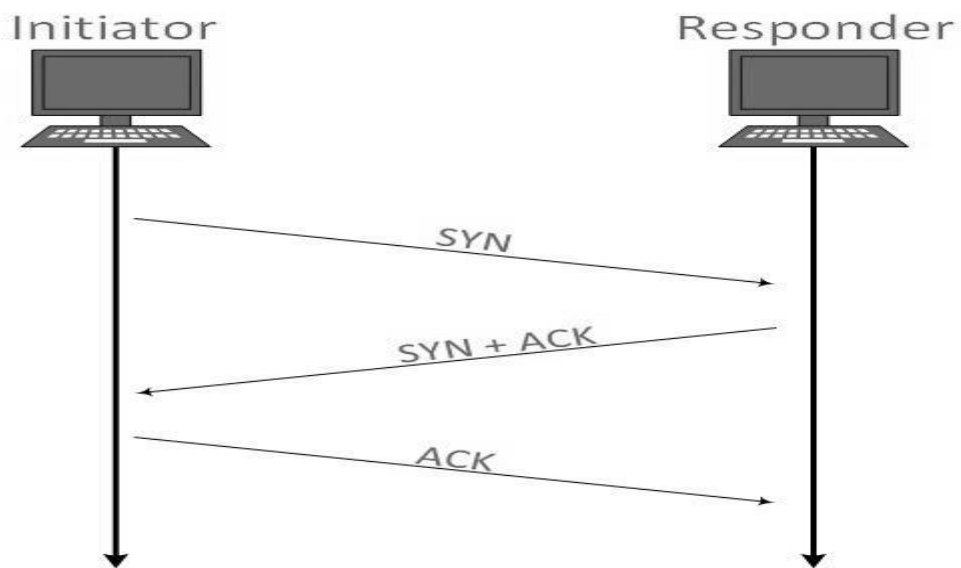
3. Addressing

두 원격 호스트 간의 TCP communication은 port numbers (TSAPs)에 의해 이루어진다. Ports numbers는 0에서부터 65535까지이며, 다음과 같이 나눈다:

- . System Ports: 0에서 1023.
- . User Ports: 1024에서 49151.
- . Private/Dynamic Ports: 49152에서 65535.

4. Connection Management

TCP communication은 Server/Client model에서 이루어진다. Client가 connection을 시작하면, 서버는 그것을 접수하거나 거절한다. connection management를 위해 three-way handshaking이 사용된다.



TCP Handshake

5. Bandwidth Management

TCP 는 Bandwidth management 의 요구를 수용하기 위하여 window size 의 개념을 이용한다. Window size 는 원격지에 있는 sender 에게 이쪽 끝에 있는 리시버가 받을 data byte segments 의 번호를 알려준다. TCP 는 window size 1 을 사용함으로써 slow start phase 를 사용하며, 각 통신이 성공적으로 이루어진 다음엔 window size 가 지수적으로 증가한다.

예를 들어, 클라이언트는 windows size 2 를 사용하여 2 bytes 의 data 를 보낸다. 이 세그먼트에 대한 인정이 접수될 때 윈도우사이즈는 2 의 곱이 될 것이며, 그 다음에 보내진 세그먼트는 길이가 4 bytes 의 데이터가 될 것이다. 또한 4 byte data segment 의 인정이 접수되면 클라이언트는 windows size 를 8 로 세트 시킨다.

만일 인정이 없으면, 즉 데이터가 transit network 에서 분실되거나 NACK 를 받으면, window size 는 반으로 줄어든다. slow start phase 가 다시 시작된다.

6. Error Control and Flow Control

TCP 는 port numbers 를 사용하여 어떠한 어플 프로세스가 데이터 세그먼트를 전달하는데 필요한지를 안다. 따라서 이것은 순번을 사용하여 원격 호스트와 자신을 동기화 시킨다. 모든 데이터 세그먼트는 순번과 함께 송수신된다. 센터는 ACK 가 접수될 때 리시버가 접수한 마지막 데이터 세그먼트에 대해 알게 된다. 리시버는 최근에 접수된 패킷의 순번을 참고함으로써 센터가 보낸 마지막 세그먼트에 대해 알게 된다.

최근에 접수된 세그먼트의 순번이 리시버가 기대한 순번과 일치하지 않는다면, 그것은 폐기되고 NACK 가 되돌려 보내진다. 만일 두 개의 세그먼트가 같은 순번으로 도달한다면 TCP timestamp value 을 비교하여 우선순위를 결정한다.

7. Multiplexing

한 세션에서 두 개 이상의 데이터 스트림을 결합하는 기법을 Multiplexing 이라 부른다. TCP client 가 서버와 연결을 시작할 때, 그것은 항상 잘 정의된 port number 를 참고하는데, 이 번호는 application process 를 의미한다. client 스스로는 private port number pools 에서부터 무작위로 생산된 port number 를 사용한다.

TCP Multiplexing 를 사용하면, 클라이언트는 수 많은 어플과 통신할 수 있다.

예를 들어, 클라이언트가 다양한 종류의 데이터(HTTP, SMTP, FTP etc.)를 포함하고 있는 web page 를 요청하면, TCP session timeout 이 늘어나서 그 세션은 보다 오랫동안 열려 있는데, 왜냐하면 three-way handshake overhead 를 피하려 하기 때문이다.

이것은 클라이언트 시스템으로 하여금 하나의 가상의 연결로 복수의 연결을 가능하도록 한다. 이러한 가상 연결은 그 timeout 이 너무 길면 서버에 좋지 않은 영향을 끼친다.

8. Congestion Control

대량의 데이터가 그것을 취급할 수 없는 시스템에 공급될 때, congestion(정체)이 발생한다. TCP 는 Window mechanism 을 사용하여 정체를 통제한다. TCP 는 반대쪽에게 얼마나 많은 데이터 세그먼트가 보내졌는지에 대해 말하도록 window size 를 설정하고 있다. TCP 는 정체를 통제하기 위한 3 가지 알고리즘을 사용하기도 한다:

- . Additive increase, Multiplicative Decrease
- . Slow Start
- . Timeout React

9. Timer Management

TCP 는 여러 가지 업무를 수행하기 위하여 다양한 종류의 timers 를 사용한다.

1)Keep-alive timer:

- . This timer is used to check the integrity and validity of a connection.
- . When keep-alive time expires, the host sends a probe to check if the connection still exists.

2)Retransmission timer:

- . This timer maintains stateful session of data sent.
- . If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

3)Persist timer:

- . TCP session can be paused by either host by sending Window Size 0.
- . To resume the session a host needs to send Window Size with some larger value.
- . If this segment never reaches the other end, both ends may wait for each other for infinite time.
- . When the Persist timer expires, the host resends its window size to let the other end know.
- . Persist Timer helps avoid deadlocks in communication.

4)Timed-Wait:

- . After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- . This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- . Timed-out can be a maximum of 240 seconds (4 minutes).

10.Crash Recovery

TCP 는 매우 신뢰할 수 있는 프로토콜 이다. 이것은 세그먼트로 보내진 각각의 바이트에 순번을 정해준다. 이것은 또한 feedback mechanism 을 제공한다. 다시 말해서, 호스트가 패킷을 받을 때, 그것이 마지막 세그먼트가 아니라면, 다음 순번의 패킷이 접수될 거라는 ACK(확신)을 갖는다.

TCP Server 가 통신 중간에 crashes 하여 그 과정의 다시 시작할 때, 그것은 모든 호스트에 TPDU broadcast 를 보낸다. 그러면 호스트들은 결코 불인정 되지 않는 마지막 데이터 세그먼트를 보내서 계속 통신이 진행되도록 한다.

XXIV. USER DATAGRAM PROTOCOL

User Datagram Protocol (UDP) 는 가장 간단한 Transport Layer communication protocol 이며, TCP/IP protocol 부류에 속한다. 이것에는 최소한의 communication mechanism 이 사용된다. UDP 는 믿을 수 없는 운송 프로토콜이라고 말하지만, 최상의 결과를 전달하기 위한 메커니즘을 제공하는 IP services 에서 사용하고 있다..

UDP 에서, 리시버는 접수된 패킷의 인정을 생산하지 않으며, 반대로 센터는 보낸 패킷의 어떠한 인정도 기다리지 않는다. 이러한 단점이 이 프로토콜을 신뢰하지 못하게 만들었지만, 프로세싱은 보다 쉬워졌다.

1. Requirement of UDP

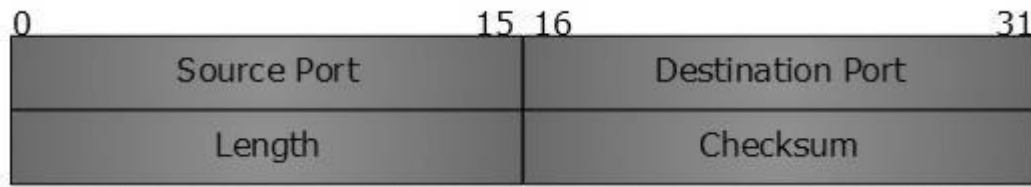
한 가지 의문이 생긴다. 왜 데이터를 전송하는데 신뢰할 수 없는 프로토콜이 필요한가? 우리가 acknowledgement packets 을 보낼 때, 실질적으로 그 데이터에 동반되는 상당한 양의 bandwidth 를 공유하는 UDP 를 사용한다. 예를 들어, video streaming 경우에, 수 천 개의 패킷이 이용자에게 포워드 된다. 모든 패킷을 인정하는 것은 문제가 있으며 거대한 양의 bandwidth wastage 를 발생시킨다. IP 프로토콜의 전달 메커니즘은 그런 패킷을 전달하는데 최상이라는 것을 보장하고 있으므로, 비록 비디오 스트림의 어떤 패킷이 오염되더라도 그 충격이 재앙적인 것은 아니므로, 쉽게 무시할 수 있다. video and voice traffic 에서 약간의 패킷 손실은 때때로 무시된다.

2. Features

- . UDP is used when acknowledgement of data does not hold any significance.
- . UDP is good protocol for data flowing in one direction.
- . UDP is simple and suitable for query based communications.
- . UDP is not connection oriented.
- . UDP does not provide congestion control mechanism.
- . UDP does not guarantee ordered delivery of data.
- . UDP is stateless.
- . UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

3. UDP Header

UDP header 는 기능이 간단하다:



UDP Header

UDP header 는 4 가지의 중요한 parameters 가 있다:

- 1) Source Port: This 16 bits information is used to identify the source port of the packet.
- 2) Destination Port: This 16 bits information is used identify application level service on destination machine.
- 3) Length: Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- 4) Checksum: This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value, it is made 0 and all its bits are set to zero.

4. UDP application

UDP 를 데이터 전송에 사용하는 몇 가지의 어플이 있다:

. Domain Name Services:

호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 하기 위해 개발되었다. 특정 컴퓨터(또는 네트워크로 연결된 임의의 장치)의 주소를 찾기 위해, 사람이 이해하기 쉬운 도메인 이름을 숫자로 된 식별 번호(IP 주소)로 변환해준다. 도메인 네임 시스템은 흔히 "전화번호부"에 비유된다. 인터넷 도메인 주소

체계로서 TCP/IP 의 응용에서, www.example.com 과 같은 주 컴퓨터의 도메인 이름을 192.168.1.0 과 같은 IP 주소로 변환하고 라우팅 정보를 제공하는 분산형 데이터베이스 시스템이다.

. Simple Network Management Protocol:

IP 네트워크상의 장치로부터 정보를 수집 및 관리하며, 또한 정보를 수정하여 장치의 동작을 변경하는 데에 사용되는 인터넷 표준 프로토콜이다. SNMP 를 지원하는 대표적인 장치에는 라우터, 스위치, 서버, 워크스테이션, 프린터, 모뎀 랙 등이 포함된다.

. Trivial File Transfer Protocol

FTP 와 마찬가지로 파일을 전송하기 위한 프로토콜이지만, FTP 보다 더 단순한 방식으로 파일을 전송한다. 따라서 데이터 전송 과정에서 데이터가 손실될 수 있는 등 불안정하다는 단점을 가지고 있다. 하지만 FTP 처럼 복잡한 프로토콜을 사용하지 않기 때문에 구현이 간단하다

. Routing Information Protocol:

UDP/IP 상에서 동작하는 라우팅 프로토콜이다. 패킷이 목적 네트워크 주소에 도착할 때까지의 최단 경로를 결정한다.

. Kerberos:

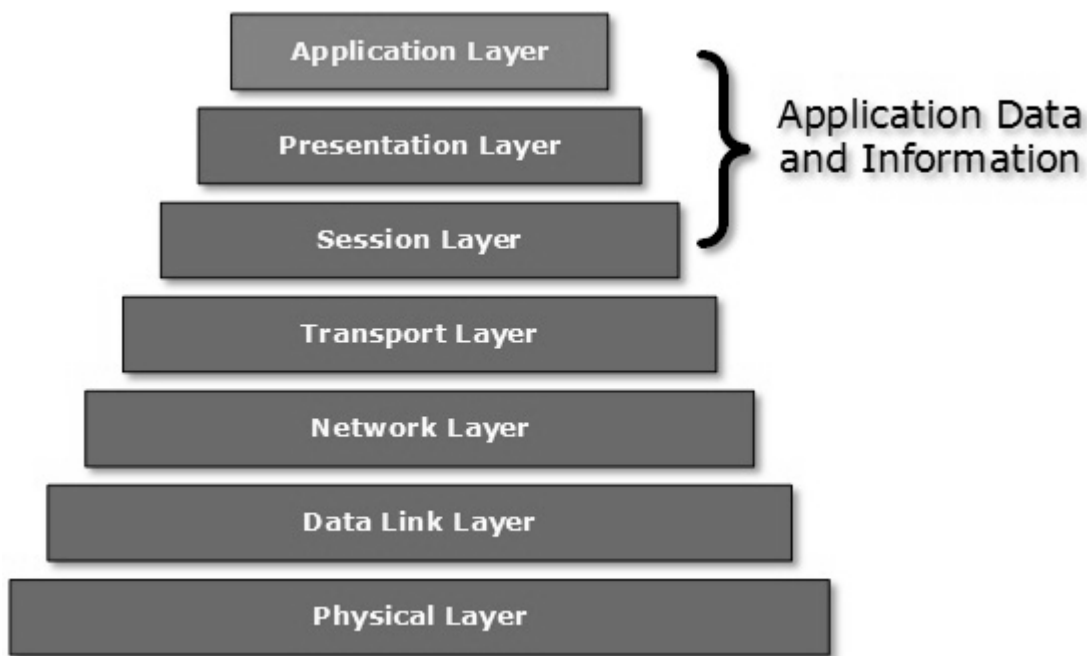
개방 네트워크상에서 인증과 통신의 암호화를 시행하여, 보안성을 확보하기 위한 알고리즘 또는 프로토콜 이다.

XXV. APPLICATION LAYER INTRODUCTION

Application layer 는 OSI 와 TCP/IP layer model 의 맨 꼭대기에 있다. 이 레이어가 양 쪽 레이어 모델에 존재하는 것은 그 만큼 중요하기 때문이다. 다시 말해서, 이것은 이용자와 이용자 어플 간의 상호작용을 위해 존재한다.

user 는 어플과 직접 상호작용할 수도 있고 안 할 수도 있다. Application layer 는 실제로 통신이 시작되고 이루어지는 곳이다. 이 레이어가 맨 꼭대기에 있기 때문에, 어떤 다른 레이어에 도움을 주진 못한다. Application layer 가 원격 호스트로 데이터를 전송하기 위해서는 Transport 와 그것의 밑에 있는 모든 레이어로부터 도움을 받아야 한다.

application layer protocol 이 원격에 있는 동료 application layer protocol 과 통신하고자 할 때, Transport layer 로부터 데이터나 정보를 양도 받는다. transport layer 는 그것 밑에 있는 모든 나머지 레이어로부터 도움을 받는다.



Application Layer

Application Layer 와 그것의 protocol 을 이해하는 데는 혼란이 존재한다. 이것의 어플들이 통신시스템과 상호작용하는 어플인 경우를 제외하고는 모든 이용자 어플들이 Application Layer 에 포함되지 않을 수 있기 때문이다. 예를 들어, 디자인용 software 나 text-editor 는 application layer programs 으로 여기지 않는다.

그러나 또 한편으로, 넷과 상호작용하기 위하여 Hyper Text Transfer Protocol (HTTP)를 사용하는 웹 브라우저에서 HTTP는 Application Layer protocol 이다.

또 다른 예는 File Transfer Protocol 인데 이것은 넷으로 text based 나 binary files 을 전송하는데 도움을 준다. 이용자는 FileZilla 나 CuteFTP 와 같은 GUI 의존형 소프트웨어에서 이 프로토콜을 사용할 수 있으며, 또한 Command Line mode 로도 FTP 를 사용할 수 있다.

그러므로 우리가 사용하는 소프트웨어와 관계없이, Application Layer 에는 소프트웨어에서 사용되는 프로토콜이 포함된다. DNS 는 HTTP 와 같은 이용자 어플 프로토콜이 자신의 일을 완수하도록 돕는 프로토콜이다.

XXVI. CLIENT-SERVER MODEL

원격 어플 프로세서는 주로 2 가지의 서로 다른 모습으로 통신할 수 있다:

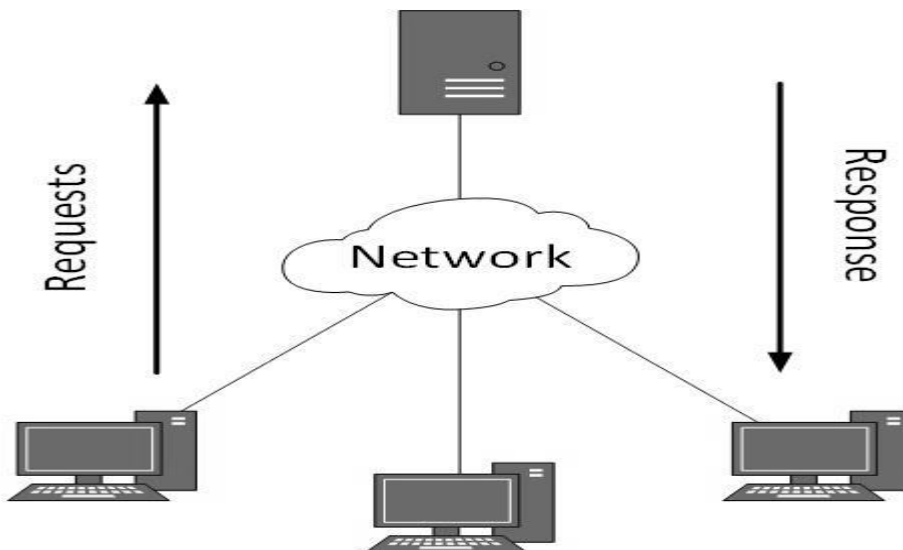
. Peer-to-peer:

Both remote processes are executing at same level and they exchange data using some shared resource.

. Client-Server:

One remote process acts as a Client and requests some resource from another application process acting as Server.

client-server model 에서, 프로세서는 Server 나 Client 로 행동한다. 이러한 결정은 기기의 종류, 크기, 또는 컴퓨팅 파워에 의해 결정되는 것이 아니라 기기가 요청을 해결하는 능력에 의해 결정된다.



http://localhost/data_communication_computer_network/images/client_server.jpg

시스템에서는 동시에 Server 로 Client 로 활동한다. 즉, 한 프로세스는 서버로, 나머지는 클라이언트로 활동한다. 이것은 동일한 기기에 클라이언트와 서버 프로세서가 공존할 때 발생 한다.

1. Communication

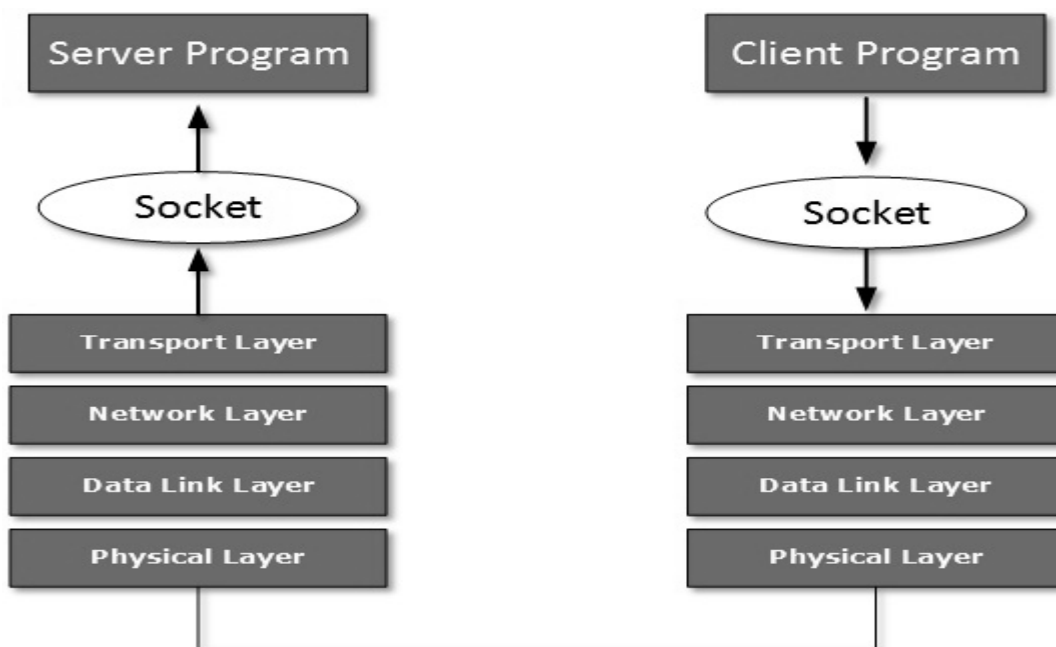
client-server model 에서 두 가지의 프로세서들이 다양한 방식으로 상호작용할 수 있다:

. Sockets

. Remote Procedure Calls (RPC)

1) Sockets

이 패러다임에서, 서버로 활동하는 프로세스는 이미 잘 알려져 있는 또는 클라이언트에 의해 알려진 포트를 사용하여 socket 을 연 다음에, 클라이언트 리퀘스트가 올 때까지 기다린다. 클라이언트로 활동하는 또 다른 프로세스 역시 socket 를 열지만, 리퀘스트를 기다리지 않고, 먼저 처리 한다.



http://localhost/data_communication_computer_network/images/sockets.jpg

2. Remote Procedure Call

이것은 하나의 메커니즘이 procedure calls 에 의해 다른 프로세스와 상호작용하도록 하는 메커니즘이다. One process (client)는 원격 호스트에 있는 procedure 를 요청한다. 이때 원격 호스트를 서버라 한다. 양 쪽 프로세스들은 업무(stubs)를 할당한다. 이런 통신은 다음과 같은 방식으로 일어난다:

- . client process 에서 client stub 를 요청한다. 그것에 있는 모든 프로그램과 관련된 파라미터를 전달 받는다.
- . 그러면 모든 parameters 가 포장(packed(marshalled)) 되고, 시스템 콜이 넷의 반대쪽으로 그것을 보낸다.
- . Kernel 이 넷 전체에 관련 data 를 보내고, 반대쪽에선 그것을 받는다.
- . 원격 호스트가 unmarshalled 된 server stub 에 데이터를 전달한다.
- . 관련 parameters 가 procedure 에 전달되어 그 procedure 가 수행된다..
- . 처리 결과가 역순과 동일한 방법으로 클라이언트에게 다시 보내진다.


XXVII. APPLICATION PROTOCOLS

Application Layer 에는 여러 개의 사용자용 프로토콜이 있으며, Application layer protocols 은 크게 두 개의 범주로 나눌 수 있다:

- . Protocols which are used by users. For example, eMail.
- . Protocols which help and support protocols used by users. For example, DNS.

몇 가지 Application layer protocols 은 다음과 같다:

1. Domain Name System

Domain Name System (DNS)  Client Server model 에서 작동한다. 이것은 transport layer communication 용의 UDP protocol 을 사용한다. DNS 는 hierarchical domain based naming scheme 을 사용한다. DNS server 는 각자 IP 어드레스로 mapped 된 Fully Qualified Domain Names (FQDN)과 email addresses 로 구성된다.

DNS server 는 FQDN 을 리퀘스트하며, 그것에 mapped 된 IP 어드레스와 함께 다시 응답한다. DNS 는 UDP port 53 을 사용한다.

2. Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP)은 서로 전자 메일을 송수신하는데 사용된다.

This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.

Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. SMTP uses TCP port number 25 and 587.

Client software 는 이메일을 받기 위하여 Internet Message Access Protocol (IMAP) 나 POP protocols 을 사용한다.

3. File Transfer Protocol

File Transfer Protocol (FTP) 는 넷으로 파일을 전송하는데 가장 널리 사용되는 프로토콜이다.

FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.

FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.

The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

4. Post Office Protocol (POP)

Post Office Protocol version 3 (POP3)은 메일 서버로부터 메일을 검색하기 위하여 User Agents (client email software)에 의해 사용되는 간단한 메일 검색 프로토콜이다.

When a client needs to retrieve mails from server, it opens a connection with the server on TCP port 110. User can then access his mails and download them to the local computer. POP3 works in two modes. The most common mode, the delete mode, is to delete the emails from remote server after they are downloaded to local machines. The second mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server.

5. Hyper Text Transfer Protocol (HTTP)

Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

XXVIII. NETWORK SERVICES

Computer systems 과 computerized systems 은 인간을 도와서 효율적으로 일을 하고 생각할 수 없는 것도 탐험하도록 한다. 이러한 기기들이 넷을 형성하도록 서로 연결될 때, 그 능력은 몇 배가 증가한다. 컴넷에서 제공할 수 있는 몇 가지 기본적인 서비스는 다음과 같다:

1. Directory Services



These services are mapping between name and its value, which can be variable value or fixed. This software system helps to store the information, organize it, and provides various means of accessing it.

2. Accounting



In an organization, a number of users have their user names and passwords mapped to them. Directory Services provide means of storing this information in cryptic form and make available when requested.

3. Authentication and Authorization



User credentials are checked to authenticate a user at the time of login and/or periodically. User accounts can be set into hierarchical structure and their access to resources can be controlled using authorization schemes.

4. Domain Name Services

DNS is widely used and one of the essential services on which internet works. This system maps IP addresses to domain names, which are easier to remember and recall than IP addresses. Because network operates with the help of IP addresses and humans tend to remember website names, the DNS provides website's IP address which is mapped to its name from the back-end on the request of a website name from the user.

5. File Services

File services include sharing and transferring files over the network.

6. File Sharing

One of the reason which gave birth to networking was file sharing. File sharing enables its users to share their data with other users. User can upload the file to a specific server, which is accessible by all intended users. As an alternative, user can make its file shared on its own computer and provides access to intended users.

7. File Transfer

This is an activity to copy or move file from one computer to another computer or to multiple computers, with help of underlying network. Network enables its user to locate other users in the network and transfers files.

8. Communication Services

1)Email

Electronic mail is a communication method and something a computer user cannot work without. This is the basis of today's internet features. Email system has one or more email servers. All its users are provided with unique IDs. When a user sends email to other user, it is actually transferred between users with help of email server.

2)Social Networking

Recent technologies have made technical life social. The computer savvy peoples, can find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos.

3)Internet Chat

Internet chat provides instant text transfer services between two hosts. Two or more people can communicate with each other using text based Internet Relay Chat services. These days, voice chat and video chat are very common.

4)Discussion Boards

Discussion boards provide a mechanism to connect multiple peoples with same interests. It enables the users to put queries, questions, suggestions etc. which can be seen by all other users. Other may respond as well.

5)Remote Access

This service enables user to access the data residing on the remote computer. This feature is known as Remote desktop. This can be done via some remote device, e.g. mobile phone or home computer.

6)Application Services

These are nothing but providing network based services to the users such as web services, database managing, and resource sharing.

7)Resource Sharing

To use resources efficiently and economically, network provides a mean to share them. This may include Servers, Printers, and Storage Media etc.

8)Databases

This application service is one of the most important services. It stores data and information, processes it, and enables the users to retrieve it efficiently by using queries. Databases help organizations to make decisions based on statistics.

9)Web Services

World Wide Web has become the synonym for internet. It is used to connect to the internet, and access files and information services provided by the internet servers.