Library Technologies:

Computer, Internet, Database, Networking

DATA COMMUNICATION AND COMPUTER NETWORK

www.tutorialspoint.com- 2015

Contents

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

1. OVERVIEW

서로 연결된 computer 들과 프린터와 같은 주변기기의 시스템을 computer network 라고 부른다. computer 들간의 이러한 상호연결을 통하여 computer 들은 정보공유를 원활하게 한다. computer 들은 무선이나 유선 매체에 의하여 서로 연결될 수 있다.

1) Classification of Computer Networks

Computer network 은 여러 가지 요소를 근거로 분류될 수 있으며, 그 요소들은 다음과 같다:

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

(1-1) Geographical Span

지리적으로 network 은 다음과 같은 범주들 중의 하나라고 여겨질 수 있다;

. 책상 위에서 Bluetooth 사용기기들 간에 이루어지는 2-3 미터내의 범위
. 모든 층을 연결하기 위하기 위한 중계기기기의 경우에는 건물 전체
. 도시 전체
. 복수의 도시나 지역
. 전 세계를 포함하는 하나의 network.

(1-2) Inter-Connectivity

network 의 구성요소들은 방식에 따라 서로 달리 연결될 수 있다. 연결 모드는 논리적, 물리적, 또는 두 가지를 혼합한 모드가 있다:

. 모든 단일 기기는 network 를 구성하기 위하여 network 상의 모든 다른 기기에 연결될 수 있다.
. 지리적으로는 분리되어 있는 경우, 버스형 구조로 모든 기기를 단일 매체에 연결할 수 있다.
. 선형구조를 만들기 위해 각 기기는 단지 그것의 왼쪽과 오른쪽에 있는 peers 에 연결되어야 한다.
. 모든 기기가 단일기기에 함께 연결되면 스타형 구조를 만들 수 있다.
. 모든 기기는 hybrid 형 구조를 만들기 위해서는 모든 위의 방식으로 서로를 연결되어야 한다.

(1-3) Administration

행정가 입장에서 network 은 하나의 독립적 시스템에 속하는 개인 network 일 수 있으므로, 그것의 물리적 또는 논리적 영역을 벗어나 접근할 수 없도록 해야 한다. 모두가 network 에 접근할 수 있다면, 그것은 공용 network 이다.

(1-4) Network Architecture

Computer network 은 그것의 구조에 따라서, Client-Server, peer-to-peer 또는 hybrid 와 같이 다양한 종류로 나눈다.

. 서버로서 활동하는 하나 이상의 시스템이 있을 수 있다. 클라이언트는 리퀘스트를 처리하기 위하여 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 모두의 network 구조를 포함하는 hybrid 형 network 이 존재할 수 있다.

2) Network Applications

computer 시스템과 주변기기들은 하나의 network 를 형성하기 위하여 연결되어야 한다. 이것의 장점은 다음과 같다

. 프린터와 저장기기와 같은 자원의 공유

. 전자우편과 FTP 를 사용하여 정보를 교환

. 웹이나 internet 을 사용함으로써 정보를 공유

. 역동적인 웹 페이지를 사용함으로써 다른 사람과의 상호 교류

. IP 전화

. 비디오 회의

. 병렬식 computer 퓨팅

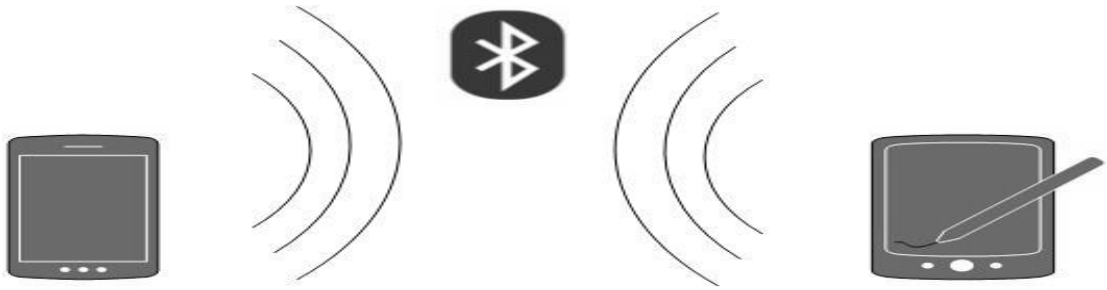
. 즉시형 메시지

2. TYPES OF COMPUTER NETWORKS

일반적으로, network 는 지리적 폭을 근거로 구분된다. Network 는 여러분의 휴대폰과 Bluetooth 헤드폰 사이의 거리만큼 짧을 수도 있고, 전세계를 포함하는 internet 처럼 클 수도 있다.

1) Personal Area Network

PAN 은 사용자에게 매우 개인적인 가장 작은 network 이다. 이것에는 Bluetooth 기기나 적외선 기기와 같은 것이 포함될 수 있다. PAN 은 10 미터 정도의 연결 범위를 가지고 있다. PAN 은 무선 computer 키보드와 마우스, Bluetooth 헤드폰, 무선 프린터, TV 리모콘 등에서 사용한다.



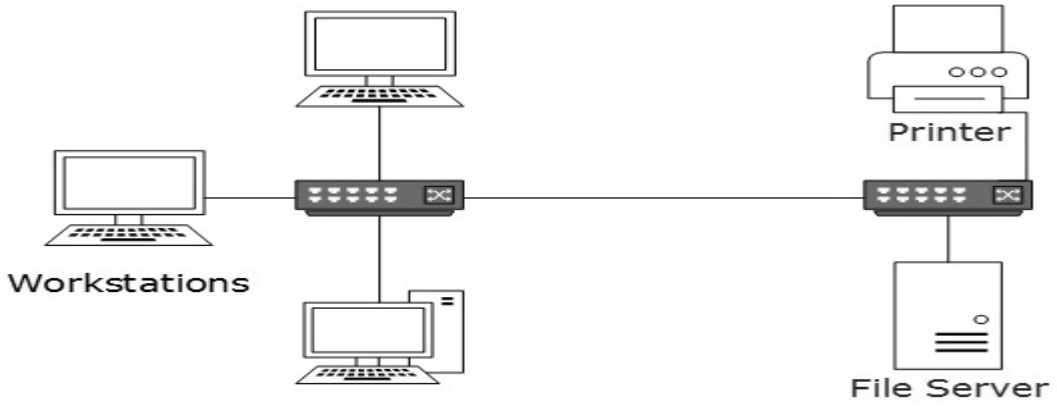
Personal Area Network

예를 들어, Piconet 은 Bluetooth PAN 이며, Master-slave fashion 으로 8 개의 기기를 함께 연결시킬 수 있다.

2) Local Area Network

어떤 computer network 은 그 범위가 빌딩 내부이며, LAN 이라 부르는 단일 행정 시스템으로 작동한다. 대체로, LAN 은 사무실, 학교, 대학교에서 사용하고 있다. LAN 에 연결된 시스템의 수는 최소한 2 개에서부터 최대한 1,600 만개까지 다양하다.

LAN 은 최종이용자들 간에 자원을 공유하는 유용한 방법을 제공한다. printers, file servers, scanners, and internet 과 같은 자원들은 쉽게 computer 들 간에 공유될 수 있다.



Local Area Network

LAN 은 저렴한 네트워킹과 라우팅 장비로 구성된다. 여기에는 파일 저장과 기타 지엽적으로 공유된 applications 을 다루는 로컬 서버가 포함되기도 한다. 이것들은 대부분이 사설 IP address 에서 운영되며, heavy routing 은 이루어지지 않는다. LAN 은 그것 자체의 로컬 도메인에 따라 운영되며 중앙식으로 통제된다.

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

LAN 은 무선, 유선, 또는 이 두 가지 모두를 사용할 수 있다.

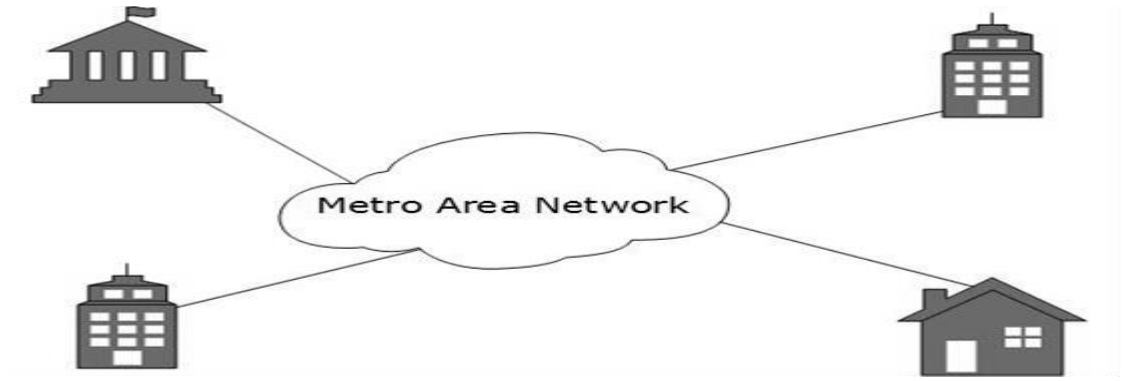
3) Metropolitan Area Network

MAN 은 일반적으로 cable TV network 처럼 한 도시 전체를 대상으로 한다. 이것은 Ethernet, Token-ring, ATM, 또는 Fiber Distributed Data Interface (FDDI)의 형태로 이루질 수 있다.

I) ATM(Asynchronous Transfer Mode) – 비동기전달모드로, 음성, 데이터 비디오 신호를 전달하기 위한 표준이다. PSTN(public switched telephone network)와 ISDN(Integrated Services Digital Network)의 backbone 으로 사용된 핵심 protocol 이며, 최근에는 Internet Protocol(IP)로 인하여 쇠퇴하였다.

II) FDDI – 최장 200km 까지 연장이 가능한 근거리통신망의 광케이블 데이터 전송의 표준이며, 토큰 링에 기반을 두고 있다.

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

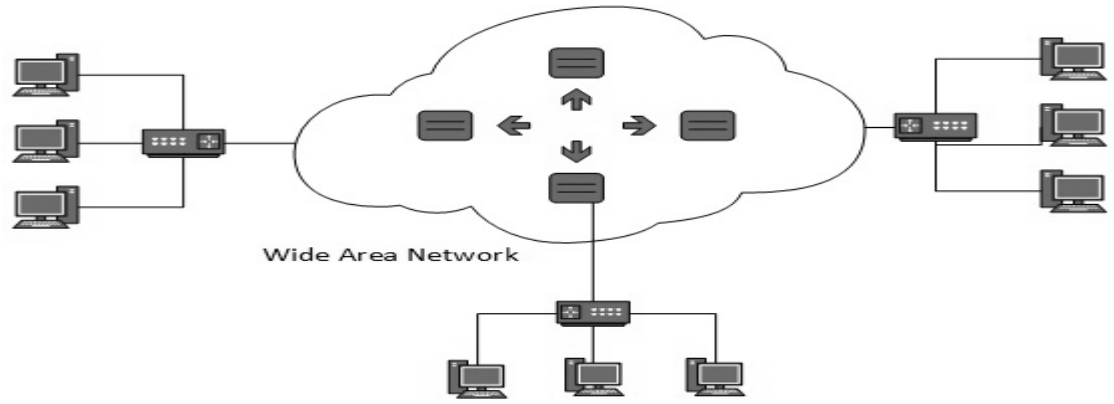


Metropolitan Area Network

MAN 의 backbone 은 고용량, 고속의 광섬유이다. MAN 은 LAN 과 WAN 사이에서 활동한다. MAN 은 WANs 나 internet 으로 LANs 용 uplink 를 제공한다.

4) Wide Area Network

이 이름이 의미하듯이, WAN 은 지역을 넘어 심지어 국가 전체를 그 범위로 설정할 만큼 넓은 지역을 담당한다. 일반적으로 telecomnetwork 은 WAN 이다. 이 network 들은 MANs 와 LANs 를 연결할 수 있다. 이것들은 초고속의 백본을 갖추고 있으므로, WANs 는 매우 값비싼 network 장비를 사용한다.



Wide Area Network

WAN 은 Asynchronous Transfer Mode (ATM), **Frame Relay**, and Synchronous Optical Network (SONET)와 같은 첨단 기술을 사용하기도 한다. WAN 은 복수로 운영되기도 한다.

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

5) Internetwork

network 들의 network 를 internet 이라 부른다. 이것은 지구상에 존재하는 가장 커다란 network 이다. internet 은 대규모로 모든 WANs 를 연결하고 있으며, LANs 와 Home network 를 연결할 수 있다. internet 은 TCP/IP protocol suite 를 사용하며 자신의 addressing protocol 로 IP 를 사용한다. 오늘날, internet 은 IPv4 를 널리 사용하고 있으나, Address spaces 의 단점으로 인하여, 점차적으로 IPv4 에서 IPv6 로 옮겨가고 있다.

internet 은 사용자로 하여금 많은 양의 정보를 공유하고 접근할 수 있도록 한다. 이것은 WWW, FTP, email services, audio and video streaming 등을 사용한다. 크게 보면, internet 은 클라이언트-서버 모델로 작동하고 있다.

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

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

internet 은 많은 프로포즈를 처리하며, 우리의 삶과 많은 관련이 있다. 이것들 중 몇 가지는 다음과 같다:

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

3. NETWORK LAN TECHNOLOGIES

다양한 LAN 기술에 대하여 간단하게 살펴보기로 한다:

1) Ethernet

Ethernet 은 널리 채택되고 있는 LAN 기술이다. 이 기술은 1970 년에 Bob Metcalfe and D.R. Boggs 에 의해 개발되었다. 이것은 1980 년에 IEEE 802.3 으로 표준화되었다.

Ethernet 은 미디어를 공유하는데, 공유된 미디어를 사용하는 network 에서는 데이터 충돌의 확률이 높다. Ethernet 은 Carrier Sense Multi Access/Collision Detection (CSMA/CD) 기술을 사용하여 이러한 충돌을 감지한다. 만약에 Ethernet 에서 충돌이 발생하면, 그것의 모든 호스트들이 roll back 하여 무작위로 짧은 시간 동안 기다린 다음에, 해당 데이터를 재전송한다.

Ethernet 코넥터는 48-bits MAC address 로 된 network interface 이다. 이것은 다른 Ethernet 기기들이 Ethernet 에서 원거리 기기를 식별하여 통신하는 것을 도와준다.

IV) MAC address(Media Access Control address): 물리적 network 세그먼트에서 통신용으로 사용되는 network interface 에 배정된 유일한 식별자이며, Ethernet 과 와이파이에서 network address 로 사용된다.

전통적인 Ethernet 은 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 사용한다. **Ethernet 은 세그먼트 길이가 100 미터까지인 스타형태를 갖는다.** 모든 기기들은 스타 모양으로 하나의 허브/스위치에 연결된다.

V) Baseband – 매우 좁은 범위의 주파수를 가지고 있는 시그널

2) Fast-Ethernet

새로운 소프트웨어와 하드웨어의 기술이 요구됨에 따라, Ethernet 은 Fast-Ethernet 으로 확대되었다. 이것은 UTP(Unshielded twisted pair cable), Optical Fiber, and wirelessly 로도 운영될 수 있다. 이것은 100MBPS 까지의 속도를 제공하며, 이것의 표준은 Cat-5 twisted pair cable 를 사용할 경우에 IEEE 803.2 에서 100BASE-T 로 지정하였다. 이것은 Ethernet 호스트들간에 공유하는 유선 미디어를 위한 CSMA/CD 기법과 무선 Ethernet LAN 을 위한 CSMA/CA (CA stands for Collision Avoidance) 기법을 사용하고 있다.

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

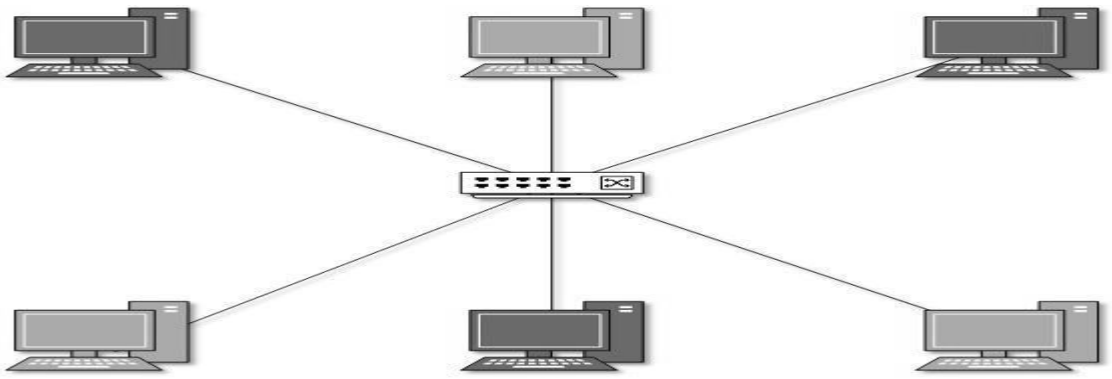
3) Giga-Ethernet

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

4) Virtual LAN

LAN 은 공유된 미디어에서 차례대로 작동하는 Ethernet 을 사용한다. Ethernet 에서 공유된 미디어는 한 개의 단일 Broadcast domain 과 한 개의 단일 Collision domain 을 만든다. Ethernet 의 Switches 은 단일 collision domain issue 를 제거한 다음, Switches 에 연결된 각 기기는 독립된 collision domain 에서 작동한다. 그러나 Switches 조차도 network 은 분리된 Broadcast domains 으로 나눌 수 없다.

Virtual LAN 은 a single Broadcast domain 을 multiple Broadcast domains 으로 나누기 위한 해결책이다. 하나의 VLAN 에 있는 호스트는 또 다른 VLAN 에 있는 호스트와는 대화할 수 없다. 따라서 초기값에 의해, 모든 호스트들은 동일한 VLAN 에 들어 있어야 한다.



Virtual LAN

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 보거나 말할 수 없다. VLAN 은 Ethernet 에서 밀접하게 작동하는 Layer-2 기술이다. 두 개의 서로 다른 VLANs 간에 packets 를 라우트하려면, Router 역할을 하는 Layer-3 기기가 필요하다.

4. COMPUTER NETWORK TOPOLOGIES

network topology 란 어떤 computer 시스템이나 network 기기들이 서로 연결된 배열형태를 말한다. topology 는 network 의 물리적 및 논리적 모습을 정의하기도 한다. 논리적 및 물리적 topology 둘 다는 동일한 network 에서 같거나 다를 수도 있다.

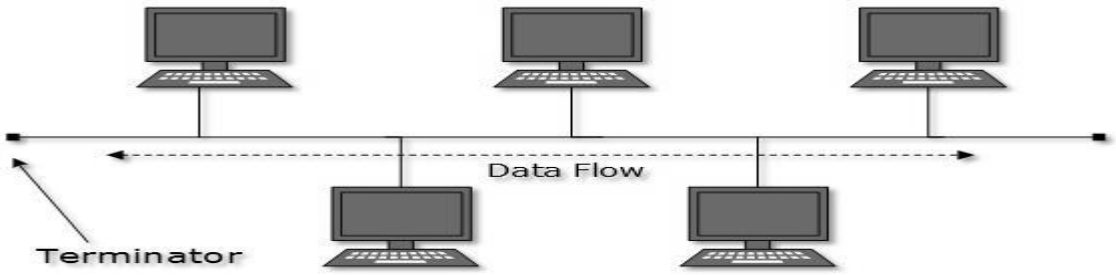
1) Point-to-Point

포인트-투-포인트 network 은 정확하게 computer 로 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 network 을 알지 못하며 마치 서로가 직접 연결된 것처럼 인식한다.

2) Bus Topology

버스 topology 의 경우에, 모든 기기들은 한 개의 통신선이나 케이블을 공유한다. 버스 topology 는 복수의 호스트가 동시에 데이터를 전송하는 경우에는 문제가 있을 수 있다. 그러므로, 버스 topology 는 CDMA/CD 기술을 사용하거나 그러한 문제를 해결하기 위하여 하나의 호스트를 Bus Master 처럼 인식한다. 이것은 특정 기기의 잘못이 다른 기기에 영향을 끼치지 않는 가장 단순한 network 형태들 중의 하나이다. 그러나 공유 통신선의 잘못은 모든 다른 기기들의 기능을 멈추게 만들 수도 있다.



Bus Topology

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

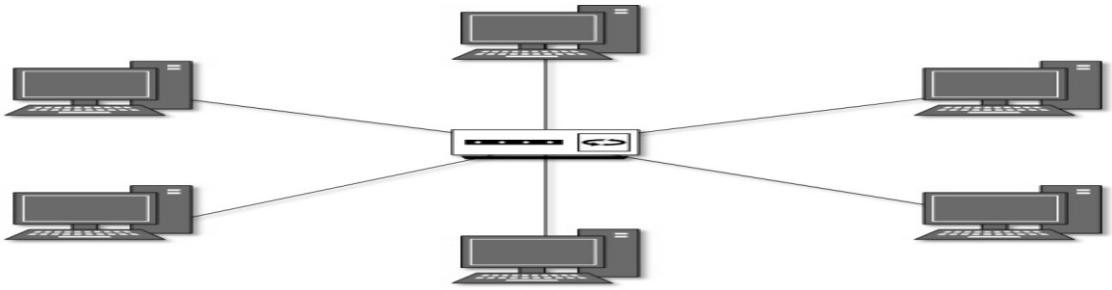
3) Star Topology

스타 topology 의 모든 호스트들은 포인트-투-포인트 연결방식을 사용하는 hub device 라 부르는 한 개의 중앙 기기에 연결되어 있다. 즉, 호스트들과 허브는 포인트-투-포인트 연결방식을 사용한다. 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



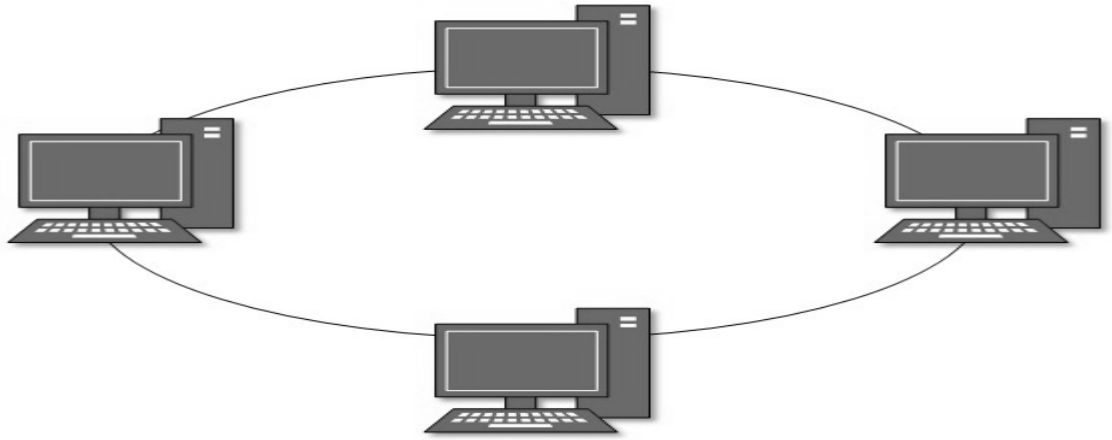
Star Topology

버스 topology 에서처럼, 허브는 하나의 포인트처럼 활동한다. 만일 허브가 잘못한다면, 모든 호스트들은 그러한 잘못에 노출된다. 왜냐하면, 호스트들간의 모든 통신은 허브만을 통해 이루어지기 때문이다. 스타 topology 는 한 개 이상의 호스트에 연결되고, 이 때엔 단지 한 개의 케이블만이 필요하며, 구성도 간단하므로 비싸지 않다.

4) Ring Topology

Ring topology 에서, 각 호스트는 원형 network 구조를 만들기 위하여 정확하게 단지 두 개의 다른 컴퓨터에만 연결된다. 한 개의 호스트가 그것에 인접해 있지 않은 또 하나의 호스트에 메시지를 보내거나 통신하려고 할 때, 그 데이터는 모든 중계 호스트를 거쳐서 전달된다.

기존 구조에 있는 하나 이상의 호스트에 연결하기 위하여, 행정가는 단지 한 개 이상의 추가 케이블이 필요할 경우도 있다.

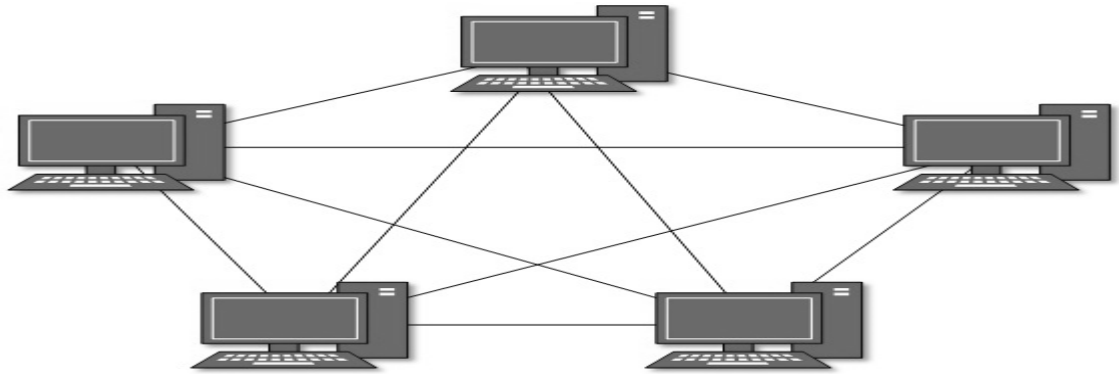


Ring Topology

어떤 호스트의 잘못은 링 전체의 잘못을 초래한다. 그러므로, 잘못을 발생시키는 하나의 포인트로 인하여 링의 모든 접속은 잘못될 수 있다. 따라서 이러한 문제를 해결하기 위하여 복수의 백업 링을 사용하는 경우도 있다.

5) Mesh Topology

이런 종류의 topology 에서, 호스트는 하나 혹은 복수의 호스트에 연결된다. 이 topology 는 모든 다른 호스트들과 포인트-투-포인트로 연결된 호스트들을 가지고 있거나 단지, 극소수의 hosts 와 포인트-투-포인트로 연결된 호스트들을 가질 수도 있다.



Full Mesh Topology

메쉬 topology 에서 호스트들은 또한 직접적인 포인트-투-포인트 링크를 갖고 있지 않은 다른 호스트를 위하여 릴레이처럼 작동하기도 한다. 메쉬 topology 는 두 가지의 유형이 있다:

(5-1) Full Mesh: 완전 메쉬

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

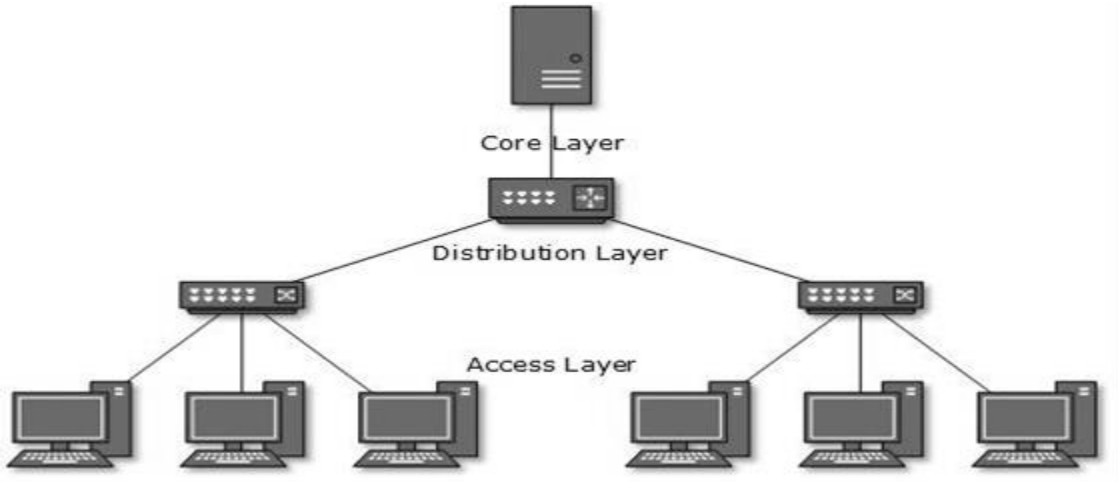
(5-2) Partially Mesh: 부분 메쉬

모든 호스트가 모든 다른 호스트에 포인트-투-포인트 방식으로 연결되어 있지는 않다. 호스트들은 약간은 임의적인 방식으로 서로 연결된다. 이러한 topology 는 우리가 모든 호스트 중에서 단지 몇 개의 호스트들에 신뢰성을 부여하고자 할 경우에 사용한다.

6) Tree Topology

계층적 topology 로 알려져 있으며, 이것은 현재 사용 중에 network topology 에서 가장 일반적인 형태이다. 이 topology 는 확장형 스타 topology 처럼 보이며, 버스 topology 의 특성을 가지고 있다.

이 topology 는 network 를 복수의 levels 이나 layers 로 나눈다. 주로 LANs 에서, 이 network 는 3 가지 유형의 network 컴퓨터들로 나눈다. 가장 낮은 쪽이 computer 들이 접속하는 access-layer 이고, 중간 layer 는 distribution layer 로 알려져 있는데 이것은 위쪽 layer 와 아래쪽 layer 간의 중계자 역할을 한다. 최상의 layer 는 core layer 라 부르며, network 의 중심점이다. 다시 말해서, 모든 node 들이 나무의 뿌리 모양을 갖추고 있다.



Tree Topology

모든 이웃 호스트들은 서로 포인트-투-포인트 방식으로 연결된다. 이것은 버스 topology 와 비슷하므로 만일에 루트가 다운된다면, 모든 network 가 비록 단일 포인트들의 잘못이 아니더라도 어려움을 겪는다.

7) Daisy Chain

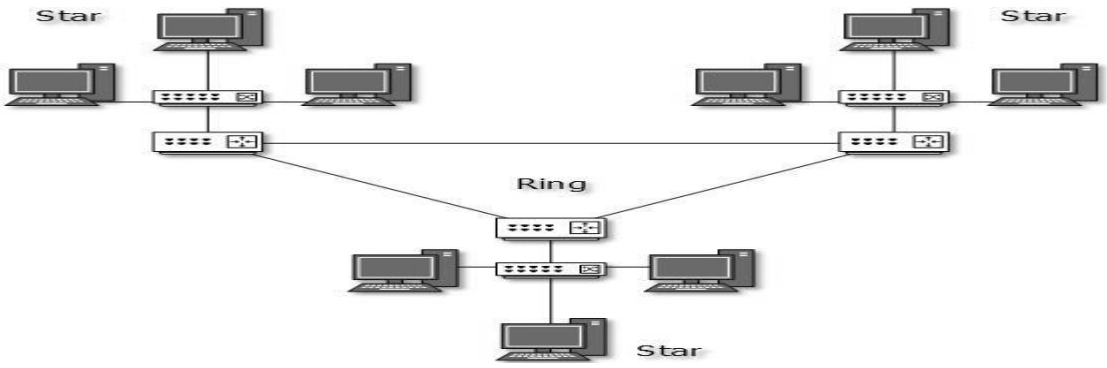
이 topology 는 모든 호스트들인 하나의 선형으로 연결되어 있다. 링 topology 와 비슷하게, 모든 호스트들은 단지 두 개의 호스트에만 연결되어 있으나, 나머지 호스트들은 그렇지 않다. 만일 데이지 체인에 있는 최종 호스트가 연결되어 있다면, 그것은 링 topology 를 나타낸 것이다.

Daisy Chain Topology

데이지 체인 topology 의 각 링크는 단일 포인트의 잘못을 표현한다. 따라서 모든 링크 잘못은 network 을 두 개의 세그먼트로 분리시킨다. 그리고 모든 중간 호스트들은 자신의 인접 호스트들을 위하여 릴레이처럼 활동한다.

8) Hybrid Topology

하나 이상의 topology 를 포함하도록 디자인된 network 구조를 hybrid topology 라 부른다. hybrid topology 는 그 안에 포함되어 있는 모든 topology 의 장단점을 갖는다.



Hybrid Topology

위의 그림은 임의적인 hybrid topology 를 표현하고 있다. 서로 결합되어 있는 이 topology 는 스타, 링, 버스, 그리고 데이지-체인 topology 의 속성을 모두 가질 수 있다. 대부분의 WANs 는 Dual-Ring topology 를 사용하여 연결되어 있으며, 이것에 연결된 network 들은 대부분 스타 topology network 들이다. internet 은 가장 커다란 hybrid topology 의 가장 좋은 예이다.

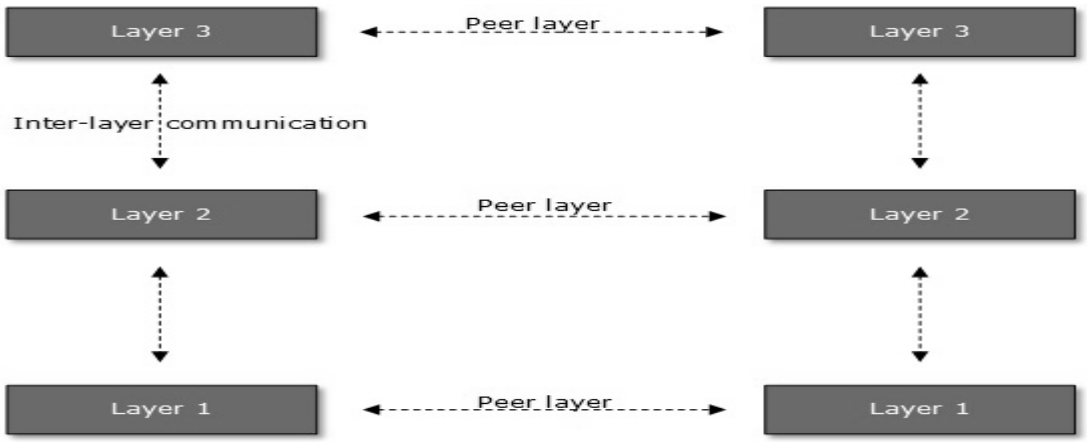
5. COMPUTER NETWORK MODEL

network 공학에서는 software, firmware, chip level engineering, hardware, and electric pulses 를 다룬다. 여기서는 네트워킹 개념 전체를 복수의 layer 로 구분하며, 각 layer 는 어떤 특별한 임무를 수행하며, 모든 다른 layer 와는 상호 독립적이다 그렇지만, 전체적으로 보면, 모든 네트워킹 임무들은 거의 모두 이러한 layer 에 의존하고 있다. layer 들은 그것들 간에 데이터를 공유하며, 단지 서로 input 을 받아 output 시키는데 의존하고 있다.

1) Layered Tasks

network 모델의 layering 구조에서, 모든 network 프로세서는 작은 임무들로 세분된다. 그런 다음에 각각의 작은 임무는 단지 그 임무만을 전문적으로 처리하는 특별한 layer 에 할당된다.

layering 화된 통신 시스템에서, 호스트의 어떤 layer 는 원거리 호스트의 동일한 레벨에 있는 그것의 상대(peer) layer 에 의해 수행되는 임무를 취급한다. 그 임무는 가장 낮은 레벨에 있거나 그 위 쪽 레벨의 layer 에 의해 대부분 시작된다. 만일 그 임무가 최상의 layer 에 의해 시작된다면, 추가적인 처리를 위하여 그것의 아래에 있는 layer 로 전달된다. 이런 하위 layer 도 같은 일을 하며, 그 임무를 처리한 후, 다시 그것의 하위 layer 에 전달한다. 만일 그 임무가 가장 낮은 layer 에서 시작된다면, 역순으로 이러한 과정이 이루어진다.



Layered Tasks

각 layer 는 자신의 임무를 수행하는데 필요한 모든 절차, 프로토콜, 그리고 방법을 가지고 있다. 모든 layer 는 encapsulation header 와 tail 의 기법을 사용하여 자신들의 상대를 식별한다.

2) OSI Model

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

OSI Model

(2-1) Application Layer:

이 layer 는 applications 이용자에게 interface 를 제공하는데 책임을 지므로, 직접적으로 이용자와 접속할 수 있는 프로트콜을 가지고 있다.

이 layer 는 network 에서 데이터를 주고 받는 프랫폼을 제공하므로, network 통신을 하는 모든 applications and utilities 은 이 layer 에 속한다.

예:

Browsers: Mozilla Firefox, Internet Explorer, Google Chrome etc

Email clients: Outlook Express, Mozilla Thunderbird etc.

FTP clients: Filezilla, sFTP, vsFTP

(2-2) Presentation Layer:

표현 layer 는 원격 호스트의 초기 포맷에 있는 데이터가 다른 호스트의 포맷에서는 어떻게 표현되는가를 정의한다.

표현 layer 에서는 데이터를 준비한다. application layer 로부터 데이터를 받아서 .doc, .jpg, .txt, .avi 등과 같은 포맷팅 코드로 표시한다. 이러한 파일 확장자들은 전달받은 파일을 특별한 형태의 applications 을 사용하여 포맷했다는 것을 쉽게 알게 해 준다. 포맷팅과 관련해서, 표현 layer 는 또한 compression and **encapsulation** 을 다룬다. 즉, 여기서 데이터 파일을 압축(computer 에서 보냄)하고 해제(computer 에서 받음)한다. 이 layer 에서도 데이터를 캡슐화하지만, 이것이 하위 layer 들 보다 더 효과적이라고는 말할 수 없다.

VI) Encapsulation: OSI 의 7 계층모델에서 정보가 응용계층으로부터 물리계층까지 전달될 때, 각 계층은 특정제어정보(주로 Header)를 추가한다(캡슐화).

(2-3) Session Layer:

이 layer 는 원격 호스트들간의 세션을 유지한다. 예를 들어, 일단 이용자/패스워드 인증이 이루어지면, 원격 호스트는 잠시 이 세션이 유지되는 시간 동안 추가로 인증을 요구하지 않는다.

세션 layer 에서는 connections 를 다룬다. 이것은 두 개의 통신 node 간에 이루어지는 세션을 시작, 관리, 종료시킨다. 이 layer 는 표현 layer 에 자신의 서비스를 제공한다. 세션 layer 는 또한 두 호스트의 표현 layer 간의 대화를 동기화시키며, 그것들의 데이터 교환을 관리한다.

예를 들어, 웹 서버에서 특정한 시간대에 많은 이용자가 서버와 통신하도록 할 수 있다. 그러므로 이용자가 어떠한 통로로 통신을 하는가를 추적하는 것은 중요하며, 세션 layer 는 그 같은 책임을 정확하게 다룬다.

(2-4) Transport Layer:

이 layer 는 호스트들 간에 end-to-end delivery 를 책임지며, 다음과 같은 서비스를 다룬다:

- 이것은 두 기기 간의 연결을 설치하고 관리한다.
- 이것은 다수의 applications 들이 동시에 데이터를 보내고 받을 수 있도록 연결을 multiplexes 한다.
- 요구조건에 따라, 데이터 전달방법은 connection oriented 이거나 connection less 이다.
- 데이터의 전달을 신뢰할 수 없을 경우, connection less method 을 사용한다.

VII) Connection-oriented communication:

telecommunications and computer networking 분야의 network communication mode 이며, 어떤 유용한 데이터가 전달되기 전에 통신 세션이나 반-영구적인 연결이 수립되어 데이터의 stream 이 그것들이 보내진 순서에 맞게 전달되는 네트워크 통신 모드이다.

이것의 대안은 connectionless communication 인데, 예를 들면 IP and UDP(User Datagram Protocol) protocols 에 의해 사용되는 datagram mode communication 이다. 이것은 서로 다른 packets 가 독립적으로 라우트되기 때문에, 데이터가 무질서하게 전달될 수 있으며, 또한 서로 다른 paths 로 전달될 수도 있다.

-Connection less method 에서는 UDP protocol 을 사용한다.

-신뢰할 수 있는 데이터의 전달일 경우, connection oriented method 이 사용된다.

-Connection oriented method 에서는 TCP(Transmission Control Protocol) protocol 을 사용한다.

-신뢰할 수 있는 연결을 설치할 때, sequence numbers and acknowledgments (ACKs)가 사용된다.

-신뢰할 수 없는 연결은 windowing 이나 acknowledgement 의 사용을 통하여 흐름을 통제한다.

VIII) sequence numbers and acknowledgments (ACKs):

TCP 는 보내온 각각의 바이트에 sequence no.를 할당하여 그 데이터를 추적한 다음, 그것에 상응하는 acknowledgement no.를 사용하여 어떤 데이터가 전송 중에 분실되었는지를 확인한다. TCP connection 초기에, 각 side 는 0 에서부터 4,294,967,295 까지인 유일한 clock value 에서 유래된 Initial Sequence Number (ISN)를 사용하여 출발한다.

(2-5) Network Layer:

network layer 는 IP address 로 알려진 논리적 주소를 제공하는데 책임을 진다. Router 는 이 layer 에서 작동된다. 이 layer 의 주요 기능은 다음과 같다:

- IP address 를 정의한다.
- 목적지에 도달하기 위하여, IP address 를 근거로 라우터를 찾는다.
- Token Ring, Serial, FDDI, Ethernet 등과 같은 서로 다른 link types 을 함께 연결시킨다.

.IP address:

IP address 는 32 bit 길이의 software address 이며, 두 개의 구성소로 이루어져 있다:

-Network component: 기기의 network 부분을 정의한다.

-Host component: 특별한 network segment 에 맞는 특별한 기기를 정의한다.

.Subnet mask 는 network component and host component 를 구분하는데 사용된다.

IP addresses are divided in five classes:

Class A addresses range from 1-126.

Class B addresses range from 128-191.

Class C addresses range from 192-223.

Class D addresses range from 224-239.

Class E addresses range from 240-254.

아래의 address 는 특별한 목적으로만 사용된다:

- 0 [Zero]는 예약되어있으며 모든 IP addresses 를 표현한다;

- 127 은 예약된 address 이며 interface 에서 loop back 과 같은 테스트용으로 사용된다.

- 255 은 예약된 address 이며, 방송목적으로 사용된다.

.IP packet:

network layer 는 transportation layer 로부터 segment 를 받아서 그것을 datagram 이라 알려진 IP header 를 가지고 감싼다.

.Datagram:

Datagram 은 packet 의 또 다른 이름이다. network layer 는 datagram 을 사용하여 node 간에 정보를 전달한다.

IX) network layer 에서는 두 종류의 packets 가 사용되는데, 하나는 data 이고 나머지는 route updates 이다.

(IX-1) Data packets:

Data packets 은 network 에서 이용자 데이터를 전송하는데 사용한다. 데이터 packets 에서 사용하는 protocol 은 routed protocol 로 알려져 있으며, IP and IPv6 가 있다.

(IX-2) Route update packets:

이 packets 는 internet 작업을 하는데 있어서 route information 을 갱신하는데 사용한다. router 는 이러한 packets 를 사용한다. route update packets 를 보내는 protocol 을 routing protocols 라 부르며, RIP, RIPv2, EIGRP, and OSPF 가 있다.

(2-6) Data Link Layer:

이 layer 는 라인으로부터 전달되거나 라인상에 있는 데이터를 읽고 쓰는데 책임을 진다. 링크 에러는 이 layer 에서 감지된다. 데이터 링크의 주요 기능은 다음과 같다:

- Media Access Control (MAC) or hardware addresses 를 정의한다.
- 연결에 필요한 physical 또는 hardware topology 를 정의한다.
- data link layer frame 에서 network layer protocol 이 encapsulated 하는 방법을 정의한다.
- connectionless 와 connection-oriented services 둘 다를 제공한다.
- 미디어에서 발생하는 Defines hardware (MAC) addresses 뿐만 아니라 communication process 를 정의한다.

X) MAC Address:

MAC address 는 48 bit long layer two address 이다. 또한 이것은 hardware address 라고도 부른다. MAC address 의 첫 번째 six hexadecimal digits 는 제조회사를 나타낸다.

MAC addresses 는 단지 방송분야에서만 유일성을 유지하고 있으므로, 우리는 다양한 방송분야에서 동일한 MAC address 를 가질 수 있다.

XI) Fame:

Data link layer 는 network layer 로부터 packets 를 받아서 frame 이라 부르는 two Header layer 를 가지고 그것을 wrap 한다. Ethernet frame 의 두 가지 specs.이 있다:.

-Ethernet II

-802

(2-7) Physical Layer: 7 장 참조.

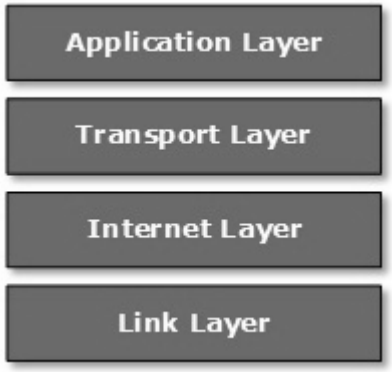
이 layer 는 hardware, cabling, wiring, power output, pulse rate etc. 을 정의한다.

물리적 layer 에서는 통신 미디어를 다룬다. 이 layer 는 데이터 링크 layer 로부터 frame 을 받아서 그것들을 bit 로 변환시킨다. 이것은 이러한 bits 를 실재로 사용하는 통신 미디어에 탑재시킨다.

미디어의 유형에 따라, 이러한 bit 값들은 single 로 변환되어. 어떤 것은 audio tones 로 사용되지만 다른 것은 state transition(voltage 가 높은 것을 낮게, 또는 낮은 것을 높게 하는 것)을 실용화(utilize)하는데 사용된다.

3) Internet Model

internet 은 internet suite 라 부르는 TCP/IP protocol suite 를 사용한다. 이것은 4 개의 layer 로 구성된 모델이다. OSI 모델은 일반적인 통신 모델이지만, internet 모델은 internet 의 모든 통신에서 사용하는 모델이다. internet 은 그것의 기저가 되는 network 구조 즉, 그것의 모델과는 독립적이다. 이 모델은 다음과 같은 4 개의 layer 를 가지고 있다:



Internet Model

(3-1) Application Layer:

이 layer 는 이용자가 network 에서 접속하는 protocol 을 정의한다. 예를 들어, FTP, HTTP etc. 이다.

BGP, DHCP, DNS, FTP, HTTP, IMAP, LDAP, MGCP, MQTT, NNTP, NTP, POP, ONC/RPC, RTP, RTSP, RIP, SIP, SMTP, SNMP, SSH, Telnet, TLS/SSL, XMPP

(3-2) Transport Layer:

이 layer 는 데이터가 호스트들 간에서 어떻게 흐르는지를 정의한다. 이 layer 에 있는 중요한 protocol 이 Transmission Control Protocol (TCP) 이다. 이 layer 는 호스트들간에 전달된 데이터가 순서에 맞는지 그리고 end-to-end delivery 로 이루어졌는지를 확인한다.

TCP, UDP, DCCP, SCTP, RSVP, more...

(3-3) Internet Layer:

IP 는 이 layer 에서 활동한다. 이 layer 는 host addressing and recognition 을 활성화 한다. 또한 이 layer 는 라우팅을 정의한다.

IP, IPv4, IPv6, ICMP, ICMPv6, ECN, IGMP, IPsec, more...

(3-4)Link Layer:

이 layer 는 실제로 데이터를 송수신하는 메커니즘을 제공한다. 이것의 상대인 OSI 모델과 달리, 이 layer 는 기저를 이루고 있는 network 구조 및 하드웨어와는 독립적이다

ARP, NDP, OSPF, Tunnels(L2TP), PPP, MAC, Ethernet, DSL, ISDN, FDDI, more...

6. COMPUTER NETWORK SECURITY

internet 초기에 이것의 사용은 연구 개발 목적으로 군대와 대학으로 제한되었다. 그 후에 모든 network 가 서로 통합되어 internet 을 형성했을 때, 그것의 데이터는 공적인 전송 network 을 통해 전달되었다. 일반인은 이러한 네트워크를 통해, 자신들의 bank credentials, username and passwords, personal documents, online shopping details, or confidential documents 와 같은 매우 민감한 데이터를 보낼 수 있게 되었다.

모든 보안상의 위협은 의도적으로 이루어진다. 다시 말해서, 그것들은 단지 고의적인 목적을 가질 때만 발생한다. 다음의 경우를 살펴보자:

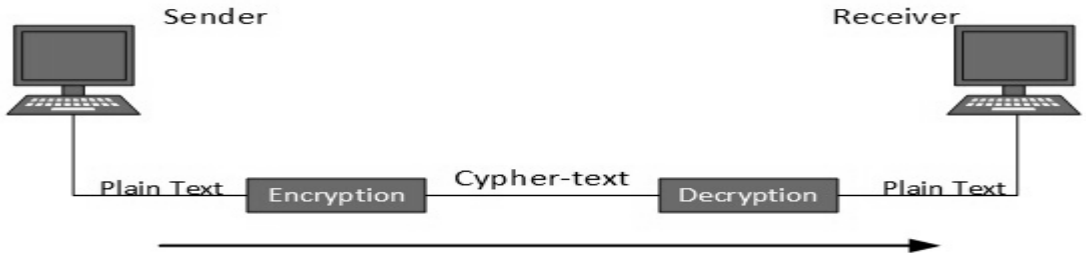
.Interruption: 인터럽션은 자원의 이용가능성을 공격하는 보안 위협이다. 예를 들어, 사용자는 웹 서버에 접근할 수 없거나 그 웹 서버를 강탈 당한다.

.Privacy-Breach(위반): 이런 상황에서, 사용자의 프라이버시는 보장받지 못한다. 접근권한을 갖지 못한 사람이 인증된 사용자가 보내거나 그가 받는 데이터에 접근하여 가로챌 수 있다.

.Integrity: 이런 종류의 위협에는 통신의 원래 내용을 변경하거나 조정하는 것이 포함된다. 공격자는 송신자가 보낸 데이터를 중간에서 가로챈 다음에, 잘못된 데이터로 변경하거나 조작해서 수신자에게 보낸다. 수신자는 원래의 송신자가 보내고 있다는 가정하에 그 데이터를 수신한다.

.Authenticity: 이러한 위협은 공격자나 보안위반자가 진짜 회원으로 인정받아 자원에 접근하거나 다른 진짜 회원과 통신할 때 발생한다.

오늘날 어떠한 기술도 100% 안전하지 않다. 그러나 데이터가 안전하지 못한 network 이나 internet 을 돌아다닐 동안, 그것을 보호하기 위한 조치들을 취할 수 있다. 가장 널리 사용되는 기법이 Cryptography(암호학)이다.



Cryptography

암호학은 plain text 데이터를 이해하거나 해석하기 어렵게 만드는 암호기법이다. 오늘날 이용 가능한 여러 가지 암호 알고리즘이 존재하며, 다음과 같다:

. Secret Key

. Public Key

. Message Digest

1) Secret Key Encryption

송수신자 모두 하나의 비밀 키를 갖는다. 이 비밀 키는 먼저 송신자 쪽에서 데이터를 암호화하는데 사용된다. 데이터가 암호화된 후, 이것은 공식 도메인을 통해 수신자에게 보내진다. 수신자가 비밀 키를 알고 있으므로, 암호화된 데이터 패킷을 쉽게 해독할 수 있다. 비밀 키 암호의 예가 Data Encryption Standard (DES)이다: 비밀 키 암호에서, network 의 모든 호스트는 서로가 처리하기 어려운 독립된 키를 가져야만 한다.

2) Public Key Encryption

이 암호화 시스템에서, 모든 사용자는 각자 자신의 비밀 키를 갖지만 그것을 공유하지 않는다. 이 비밀 키는 결코 공적 영역에 노출되지 않는다. 자신의 비밀 키와 더불어, 모든 사용자는 시스템용인 공적 키를 갖는다. 이 공적 키는 항상 공적으로만 사용되며 데이터를 암호화하기 위하여 송신자가 사용한다. 수신자가 암호 데이터를 접수했을 때, 그는 자신의 비밀 키를 사용하여 그것을 해독한다. 공적 키 암호화의 예는 Rivest-Shamir-Adleman (RSA)이다.

XII) RSA: 최초의 실용적인 public-key 암호시스템이며, 데이터 전송의 안전을 위해 널리 사용되었다.

3) Message Digest

이 방법에서는 실재 데이터를 보내지 않고, 그 대신에 해시 값을 계산해서 보낸다. 상대쪽의 최종이용자는 자신의 해시 값을 계산한 다음에 방금 접수된 해시 값과 비교한다. 양쪽의 값이 동일하다면, 그 데이터는 접수되고 그렇지 않다면 거부된다.

XIII) Hash 함수

임의적인 크기의 데이터를 고정된 크기의 데이터로 map 하는데 사용되는 함수이다. 이 함수에 의해 리턴된 값을 해시 값, 해시 코드라고 부르며, 전송된 데이터의 순수성을 확인하는데 사용한다. 이 방법의 예는 MD5 hashing 이다. 사용자 패스워드를 서버에 저장된 것과 비교 대조하여 인증하기 위해 대부분이 이 방법을 사용한다.

7. PHYSICAL LAYER INTRODUCTION

OSI 모델에서 물리적 layer 는 실재적인 하드웨어와 신호 메커니즘이 상호작용하도록 하는 역할을 한다. 물리적 layer 는 실재로 두 개의 서로 다른 스테이션을 물리적으로 연결시키는 OSI network 의 유일한 layer 이다. 이 layer 는 하드웨어 장비, cabling, wiring, frequencies, binary signals(이진 신호)를 표현하는데 사용하는 pulses 등을 정의한다.

물리적 layer 에서 Data-link layer 에 시그널을 보내면, Data-link layer 는 물리적 layer 에게 frame 들을 넘겨준다. 물리적 layer 는 그것들을 이진 데이터로 표현되는 전기 펄스로 변경시킨 다음에, 그 이진 데이터를 유무선 매체를 통해 전송한다.

1) Signals

데이터가 물리적 매체로부터 송신될 때, 그것은 전자기 신호로 먼저 바뀐다. 데이터 그 자체는 인간 음성과 같은 아날로그이거나 디스크의 파일처럼 디지털일 수 있다. 아날로그와 디지털 데이터 모두 디지털이나 아날로그 신호로 표현될 수 있다.

(1-1) Digital Signals:

디지털 신호는 성질이 이산적이며, 연속된 전압 펄스를 나타낸다. 디지털 신호는 computer 시스템의 회로에서 사용된다.

(1-2) Analog Signals:

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

2) Transmission Impairment

신호가 매체로 전달된 때, 그것들은 깨지는 경우가 있다. 이것은 다음과 같은 원인으로 발생하기도 한다:

(2-1) Attenuation(감쇠):

수신자가 실재로 데이터를 해석하기 위해서는 그 신호가 충분히 강해야 한다. 신호가 매체를 통해 전달될 때, 그것은 약해지는 경향이 있다. 거리가 늘어나면 강도를 잃게 된다.

(2-2) Dispersion:

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

(2-3) Delay distortion:

신호는 사전에 정해진 속도와 주파수로 매체간에 송수신 된다. 만일 신호의 속도와 주파수가 서로 맞지 않는다면, 그 신호는 임의의 목적지에 도달할 가능성이 있다. 디지털 매체에서, 어떤 비트들이 먼저 보낸 것들 보다 빨리 목적지에 도달한다면 이것은 매우 치명적이다.

(2-4) Noise:

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

(2-4-1) Thermal Noise:

열은 노이즈를 유발시킬 수 있는 전도체를 뜨겁게 한다. 어느 정도까지는 열에 의한 노이즈를 피할 수 없다.

(2-4-2) 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 공유하며 그것들 중의 하나가 너무나 강하거나 구성요소 그 자체가 올바로 작동하지 않는다면, 그 결과로 발생하는 주파수는 기대한 만큼 전달되지 않을 수 있다.

(2-4-3) Crosstalk(혼선):

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

(2-4-4) Impulse(충격):

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

3) Transmission Media

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

(3-1) Guided Media:

모든 통신 와이어/케이블은 UTP, coaxial cables, fiber Optics 처럼 유도 매체이다. 이 매체로, 송수신자는 직접적으로 연결되며, 그것을 통해 정보를 전송(유도)한다.

(3-2) Unguided Media:

무선이나 공중파는 비유도 매체라 부른다. 그 이유는 송수신자 간에 어떠한 직접적인 연결성도 없기 때문이다. 정보는 공중으로 날라가면, 수신기를 갖고 있는 누군가가 그 정보를 수집한다.

4) Channel Capacity

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

. Bandwidth(주파수 대역폭): 기저 매체의 물리적 한계.

. Error-rate: 노이즈의 원인이 되는 부정확한 정보의 입수

. Encoding: 시그널용으로 사용된 레벨들의 번호

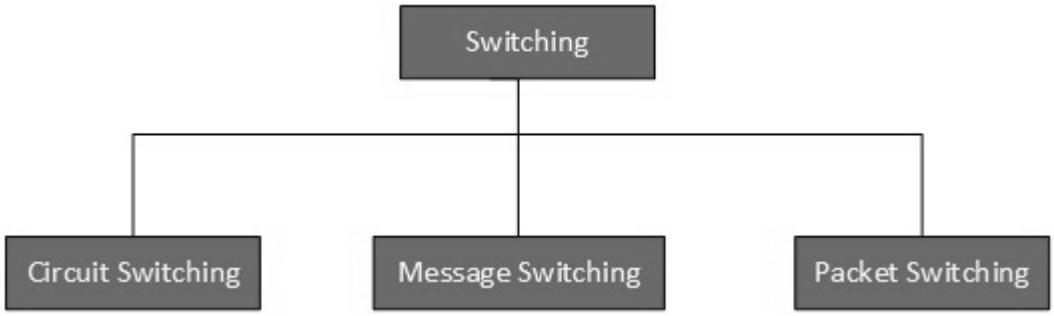
5) Multiplexing

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

6) Switching

스위칭이란 정보원에 직접 연결되지 않은 목적지로 데이터/정보를 보내는 메커니즘이다. network 들은 직접 연결된 정보원으로부터 데이터를 받아서 그것을 저장하고 분석한 다음에, 목적지에 가장 가까이 있는 두 번째의 기기로 보내는 상호연결 기기들을 가지고 있다.

스위칭의 범주는 다음과 같다:



Switching

(6-1) Circuit switching

서킷 스위칭이란 node 들이 통신하기 전에, 두 개의 node 가 network 에 전용통신 채널(서킷)을 구축하는 telecommunication network 설치방법을 말한다. 서킷은 full bandwidth 를 보장하며 통신 세션이 이루어지는 동안 접속이 지속된다. 서킷은 node 들이 물리적으로 하나의 전기선에 연결된 것처럼 작동한다.

서킷 스위치 network 의 명확한 예로는 초기의 아날로그 전화 network 이다. 한 전화기로부터 다른 전화기로 통화가 이루어질 때, 전화교환기에 있는 스위치들은 통화가 이루어지는 동안, 두 전화기 사이에서 계속해서 유선 서킷을 구성한다.

서킷 스위칭은 독립적으로 network 을 통해 전송되는 패킷으로, 데이터를 분할하는 패킷 스위칭과는 대조적이다. 패킷 스위칭에서 한번에 하나의 통신 세션에 치중하는 대신에, 서킷 스위칭에서는 여러 network 링크들이 복수의 통신 세션에서 발생한 패킷들을 공유하므로, 이것에서 제공되는 서비스의 품질은 떨어진다.

(6-2) Message switching

텔레커뮤니케이션에서, 메시지 스위칭은 한번에 one hop 로 메시지들을 telecomputer 전체로 라우트시키는 패킷 스위칭의 전신이었다. 이것은 대형 항공사, 은행, 철도회사에 판매하기 위하여 1959-1963 년 동안 캘리포니아의 Collins Radio Company 에서 최초로 만들었다.

메시지 스위칭 시스템은 현재에도 패킷 스위치 또는 서킷 스위치 데이터 network 의 상대로 대부분이 실행되고 있다. 각 메시지는 독립된 엔티티로 취급된다. 각 메시지에는 어드레싱 정보가 포함되어 있으며, 각 스위치에서 이 정보를 읽은 다음에, 전용선을 통하여 다음 스위치로 전달된다. network 조건에 따라, 여러 메시지들의 대화가 동일한 선으로 전달되지 않기도 한다. 각 메시지는 다음 스위치로 전달되기 전에, (RAM 의 한계로 인하여 대체로 하드웨어에) 저장된다. 이러한 이유로, 이것을 또한 'store-and-forward' network 라 부르기도 한다. **이메일은 메시지 스위칭을 사용하는 대표적인 applications 이다**. 두 computer 간에 실시간 데이터 전송과는 달리, 이메일을 전달하는 데는 딜레이가 허용된다.

(6-3) Packet switching

패킷 스위칭은 동시다발적인 통신 세션에서 공유하는 매체를 통해 전달될 수 있도록, 모든 전송 데이터를 패킷이라고 부르는 적당한 크기의 블록으로 집단화시키는 디지털 network 통신 방법이다. 패킷 스위칭은 network 의 효용성과 건강성을 증대시키며, 동일한 network 에서 작동하는 많은 applications 의 기술적 convergence 를 가능케 한다.

패킷은 헤더와 페이로드로 구성된다. 헤더의 정보는 network 하드웨어에 의해, 패킷이 그것의 목적지로 직행하는데 사용되며, 페이로드는 applications 소프트웨어에 의해 발췌되어 사용된다.

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

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

Connectionless protocol 의 예로는 Ethernet, Internet Protocol (IP), and User Datagram Protocol (UDP)이 있고, connection-oriented protocol 로는 X.25, Frame Relay, Multiprotocol Label Switching (MPLS), Transmission Control Protocol (TCP)가 있다.

connectionless 모드에서, 각 패킷에는 환전한 주소정보가 들어있다. 이 패킷들은 개별적으로 라우트 되므로, 그 결과가 때때로 서로 다른 통로를 사용하여 순서에 따르지 않고 전달된다. 각 패킷은 목적지 주소, 정보원 주소, 포트 번호가 표시되어 있다. 또한 그것에 패킷의 일련 번호가 표시될 수도 있다. 이것은 패킷이 목적지로 가는 길을 발견하는데 도움이 되는 전용선의 필요성을 크게 떨어뜨린다. 그러나 이것은 더 많은 정보가 패킷 헤더에서 필요로 한다는 것을 의미한다. 그러므로 헤더는 더욱 커지게 되고, 이 정보는 power-hungry content-addressable memory 에서 검사된다. 각 패킷이 발송되면 다양한 라우터를 통하여 전달될 수 있다: 잠재적으로, 이러한 시스템에서는 connection-oriented system 의 connection set-up 에서 해야 하는 것처럼 모든 패킷을 위하여 많은 일을 해야 하지만, applications 의 요구조건에 따라 적은 정보만을 가지고도 필요한 작업을 할 수 있다. 목적지에서, 본래의 메시지/데이터는 패킷의 순번을 근거로 올바른 순서로 재취합 된다. 그러므로 virtual circuit 이나 byte stream 으로 알려진 virtual connection 에서 비록 중계용 network node 들이 단지 a connectionless network layer service 만을 제공하더라도, transport layer protocol 에 의해 최종 이용자에게 제공된다.

Connection-oriented transmission 에서 어떤 패킷은 통신 패러미터의 수립을 위하여, 전달되기도 전에 각각의 관련 node 에서 설치절차가 필요하다. 패킷들은 주소정보와 더불어 연결 식별자를 포함하고 있으며, 엔드 포인트와 협정을 맺어서 순서대로 그리고 에러를 체킹하면서 전달된다. 주소정보로 목적지로의 라우트를 찾고, 엔트리는 각 network node 에 있는 스위칭 테이블에 추가로 연결되어 있는 동안에만 그 node 로 전달된다. 이 때 사용된 시그널링 protocol 은 applications 로 하여금 그것의 요구사항을 특정화하도록 하여 링크 파라미터를 찾도록 한다. 서비스 파라미터로 수용 가능한 값들은 조절할 수 있다. 패킷

헤더는 다른 패킷과 구분하기 위해 이러한 정보뿐만 아니라 length, timestamp, or sequence number 와 같은 정보만을 포함하는 작은 규모일 수도 있다.

8. DIGITAL TRANSMISSION

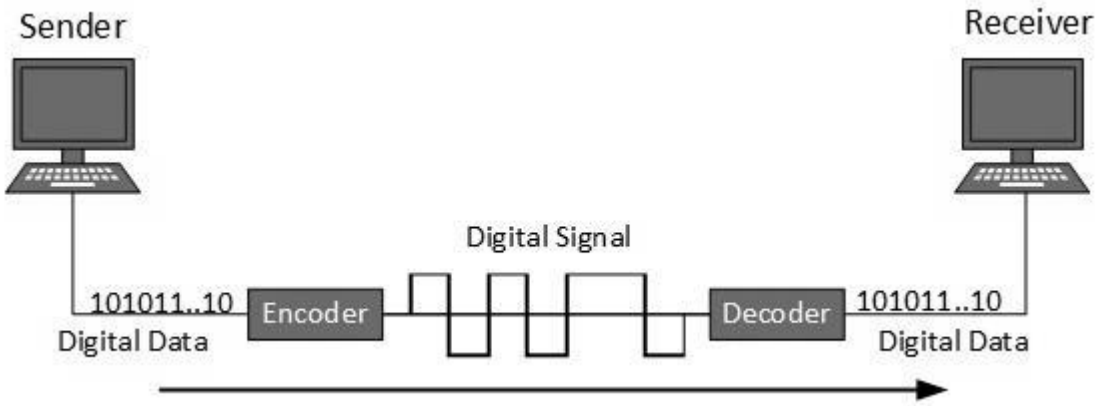
데이터나 정보는 두 가지 방법으로 저장된다: analog and digital. computer 에서 데이터를 사용하기 위하여는 discrete digital form 로 되어 있어야 한다. 데이터와 비슷하게, signals 또한 analog and digital form 이어야 한다. 데이터를 디지털로 전송하기 위해서, 먼저 디지털 형태로 그것을 변경해야 한다.

1) Digital-to-Digital Conversion

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

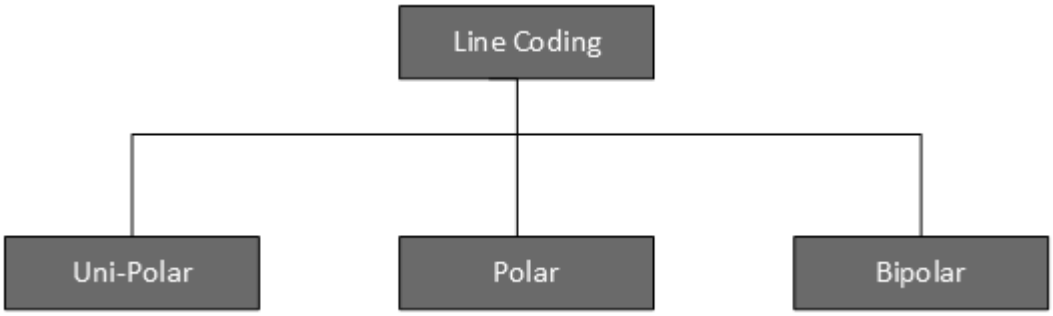
(1-1) Line Coding

디지털 데이터를 디지털 시그널로 변환시키는 절차를 Line Coding 이라 한다. 디지털 데이터는 2 진 형태로 되어 있으므로, 내부적으로 series of 1s and 0s 으로 표현되거나 저장된다.



Line Coding

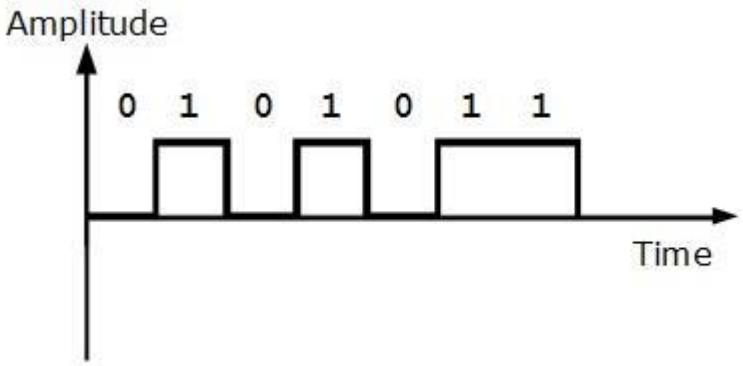
디지털 시그널은 디지털 데이터를 표현하는 discrete signal 이라 부르며, 이용할 수 있는 3 가지 종류의 line coding schemes 가 있다:



Line Coding

(1-1-1) Unipolar Encoding

Unipolar encoding schemes 는 데이터를 표현하기 위하여 single voltage level 을 사용한다. 이 경우에, 바이너리 1 을 표현하기 위하여 high voltage 가 전송되며, 0 을 표현하기 위해서는 no voltage 가 전송된다. 이것은 또한 Unipolar-Non-return-to-zero 라고도 부르는데, 그 이유는 어떠한 기타 조건도 없기 때문이다: 즉, 이것은 1 이나 0 만을 표현한다.



UniPolar NRZ Encoding

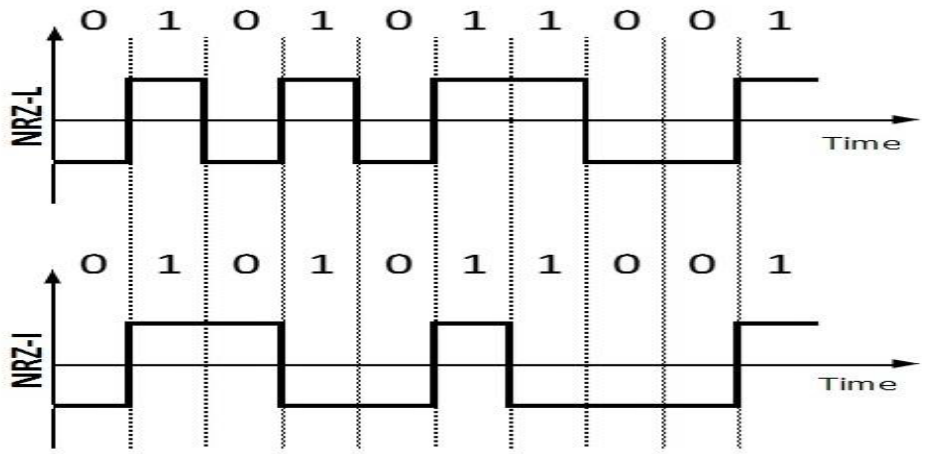
(1-1-2) Polar Encoding

Polar encoding scheme 은 binary values 를 표현하기 위하여 multiple voltage levels 을 사용한다. Polar encodings 에는 4 가지 종류가 있다:

(1-1-2-1) Polar Non Return to Zero (Polar NRZ):

이진 값을 표현하기 위하여 두 가지의 다른 voltage levels 를 사용한다. 일반적으로, positive voltage 은 1 을 그리고 negative value 은 0 을 표현한다. 이것은 또한 NRZ 인데, 그 이유는 어떠한 다른 조건도 존재하지 않기 때문이다.

NRZ scheme 에는 두 가지가 있다: NRZ−L and NRZ−I.

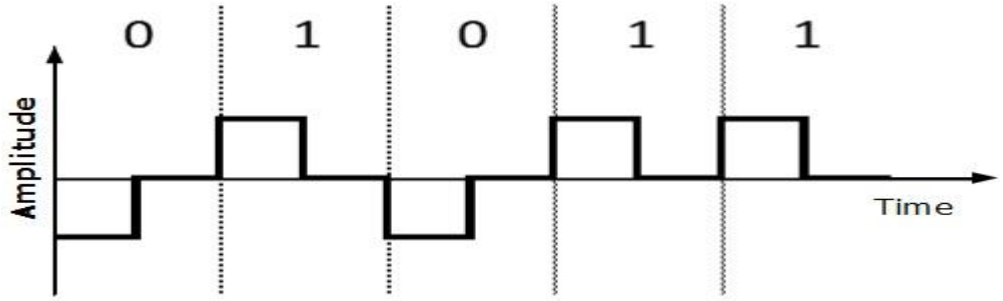


Unipolar NRZ

NRZ−L 은 서로 다른 비트가 만날 때 voltage level 을 변경하는 반면에, NRZ−I 는 1 을 만날 때 voltage 를 변경시킨다.

(1-1-2-2) Return to Zero (RZ):

NRZ 이 갖고 있는 문제는 sender 와 receiver 의 시계가 동기화되지 않는 경우에 리서버가 비트가 끝날 때와 다음 비트가 시작할 때를 conclude 할 수 없다는 것이다.



Return-to-Zero

RZ 는 3 가지의 voltage levels 을 사용한다: 1 을 표현하는 positive voltage, 0 을 표현하는 negative voltage 그리고 아무 것도 표현하지 않는 zero voltage. Signals change during bits not between bits.

(1-1-2-3) Manchester:

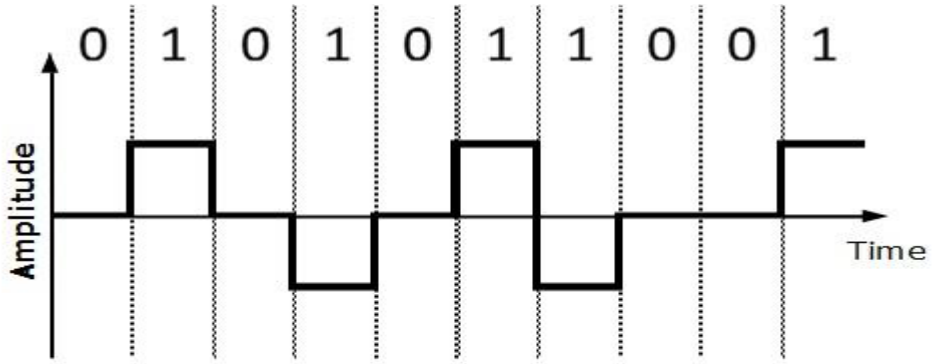
이 encoding scheme 은 RZ and NRZ-L 의 결합한 것이다. Bit time 은 two halves 로 나눈다. 이것은 비트의 중간에 전달되며 다른 비트와 만날 때 phase 가 변한다.

(1-1-2-4) Differential Manchester:

이 encoding scheme 은 RZ and NRZ-I 을 결합한 것이며, 역시 비트 중간에 전송되지만, 1 을 만날 때만 phase 를 변경한다.

(1-1-3) Bipolar Encoding

Bipolar encoding 은 three voltage levels 을 사용한다: positive, negative, and zero. Zero voltage 는 binary 0 을, 그리고 1 은 positive and negative voltages 를 altering 함으로써 표현된다.



(1-2) Block Coding

수신된 data frame 의 정확성을 보장하기 위하여, redundant bits 가 사용된다. 예를 들어, even-parity 에서, one parity bit 가 frame even 에 있는 1 들의 계산에 추가된다.

따라서 비트의 원래의 수가 증가한다. 이것을 Block Coding 이라 부른다.

Block coding 은 mB/nB 으로 표현되는데, 이 뜻은 n > m 인 경우에 m-bit block 이 n-bit block 을 대체한다는 것이다. Block coding 에는 three steps 이 있다:

> Division

> Substitution

> Combination.

block coding 이 끝나면, 그것은 전송용으로 암호화된 라인(line coded for transmission)이 된다.

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.

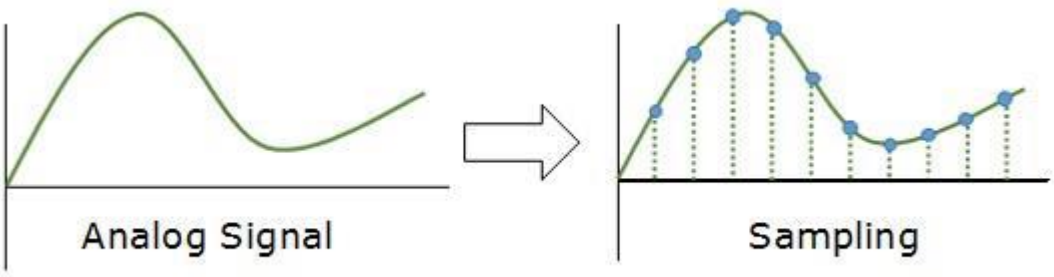
PCM 은 가장 일반적인 방법 중의 하나이며, 3 가지의 단계가 있다:

. Sampling

. Quantization

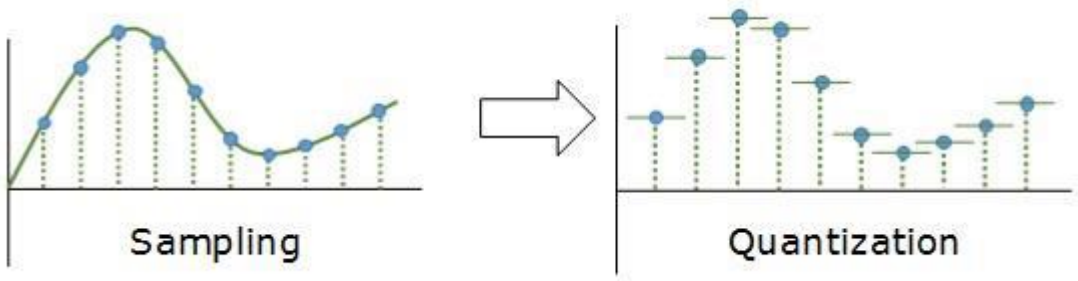
. Encoding.

(2-1) Sampling



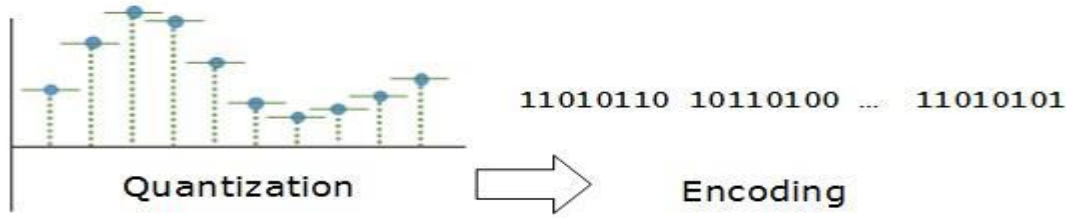
analog signal 은 모든 T interval 을 샘플한다. 샘플링에서 가장 중요한 요소는 analog signal 을 샘플하는 비율이다. Nyquist Theorem 에 따라, 샘플링 비율은 적어도 signal 의 최고 빈도의 두 배가 되어야 한다.

(2-2) Quantization



Sampling 은 연속적인 아날로그 시그널의 이산적 형태를 제공한다. 이런 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.

(2-3) Encoding



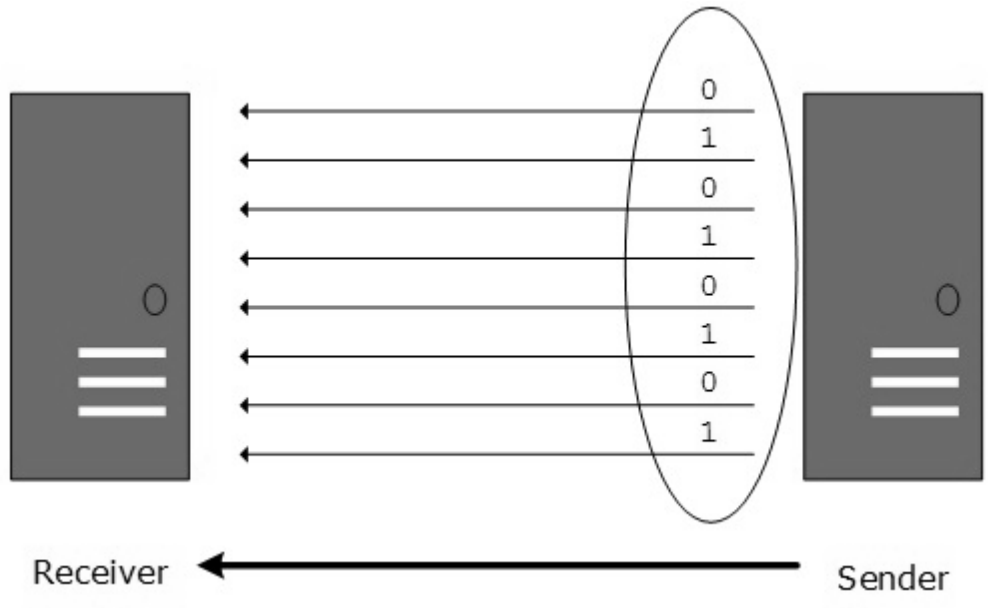
Encoding

기호화하는데 있어서, 각 근사치는 이진 포맷으로 변환된다.

3) Transmission Modes

transmission mode 에서는 두 computer 간에 데이터가 전송되는 방법을 결정한다. 1s 과 0s 로된 이진 데이터는 두 가지 모드로 보내진다: Parallel and Serial.

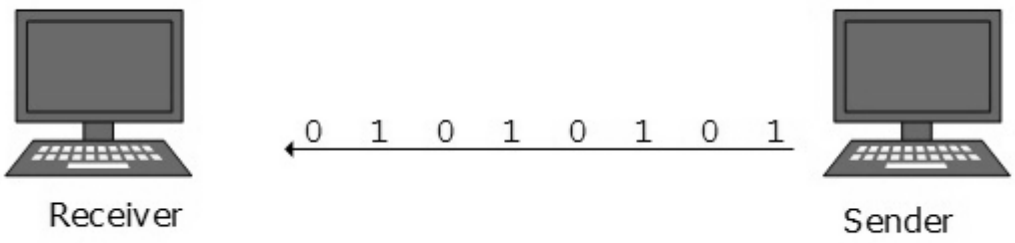
(3-1) Parallel Transmission:



이진 비트는 고정된 길이의 그룹들로 조직되어 있다. sender 와 receiver 둘 다 동일한 데이터 라인의 숫자를 갖고 병렬식으로 연결되어 있다. 양쪽 computer 들은 high order and low order data lines 간을 구별한다. sender 는 모든 라인에 한번에 모든 비트를 보낸다. 그 이유는 그룹이나 데이터 frame 에 있는 비트의 수가 동일하기 때문에, 완전한 비트 그룹(데이터 frame)을 한번에 보낼 수 있기 때문이다. Advantage of Parallel transmission 은 고속이란 것이며, 단점은 병렬식으로 보낸 데이터의 수가 많아지므로 cost of wires 이 비싸다는 것이다.

(3-2) Serial Transmission:

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



Serial Transmission

Serial transmission 은 동기식이나 비동기식으로 이루어진다.

(3-2-1) Asynchronous Serial Transmission:

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

두 개의 연속적 data-frames (bytes)의 사이에 gap 이 들어갈 수 있다.

(3-2-2) 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 가 없다. Data bits 는 bytes (8-bits) 사이의 gap 을 유지하지 않고, burst mode 로 전송된다. burst of data bits 는 바이트의 수를 포함할 수 있으므로, timing 이 매우 중요하다.

바이트에 있는 비트를 인식하고 분리하는 것은 receiver 에 달려 있다. synchronous transmission 의 장점은 고속이며, asynchronous transmission 에서처럼 extra header and footer bits 에 대한 어떠한 overhead 도 없다는 것이다.

9. ANALOG TRANSMISSION

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

. Bandpass:

필터들이 관심대상의 주파수를 필터하고 패스시키는데 사용된다. Bandpass는 필터를 패스할 수 있는 주파수의 밴드이다.

. Low-pass:

Low-pass 는 low frequencies signals 을 패스하는 필터이다.

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

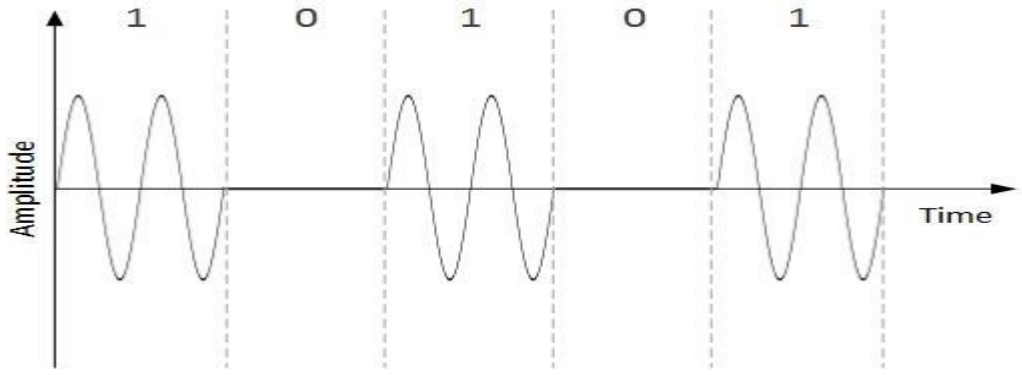
1) Digital-to-Analog Conversion

computer 의 data 를 아날로그 캐리어를 통해 다른 computer 로 보낼 때, 먼저 아날로그 시그널을 변환시켜야 한다. 즉, Analog signals 은 디지털 데이터로 변경되어야 한다.

analog signal 은 amplitude, frequency, and phase 로 구성되며, 여기에는 3 종류의 digital-to-analog conversions 이 있다:

(1-1) Amplitude Shift Keying:

이 conversion technique 에서, the amplitude of analog carrier signal 이 이진 데이터에 영향을 끼치도록 변경된다.

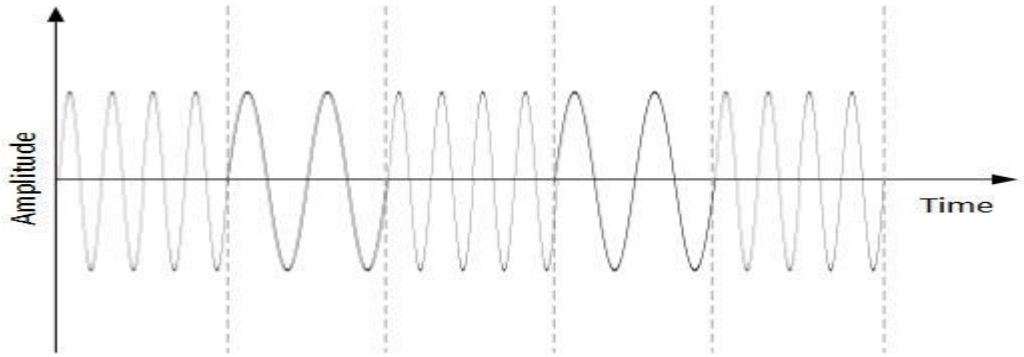


Amplitude Shift Keying

binary data 가 digit 1 을 나타낼 때, the amplitude 가 유지되지만, 그렇지 않다면, 0 으로 설정된다. frequency and phase 양쪽 다 최초의 carrier signal 과 똑같이 유지된다.

(1-2) Frequency Shift Keying:

이 conversion technique 에서, the frequency of the analog carrier signal 은 binary data 에 영향을 끼치도록 변경된다.

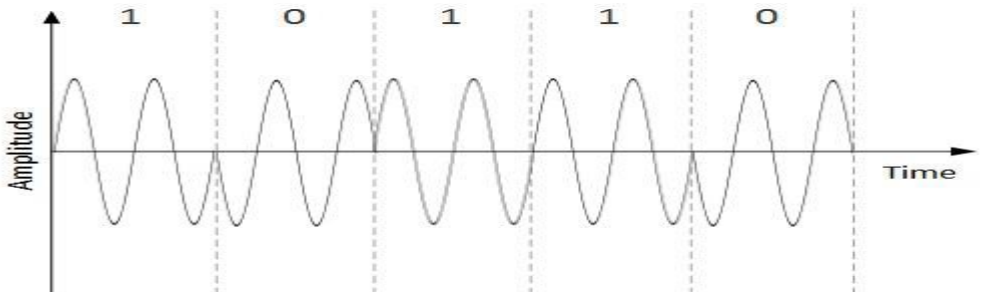


Frequency Shift Keying

이 기법에서는 두 가지 주파수인 f1 and f2 가 사용된다. 예를 들어, 이것들 중의 하나인 f1 은 binary digit 1 을 표현하기 위하여 선택되며, 나머지 하나는 binary digit 0 을 표현하기 위하여 사용된다. amplitude and phase of the carrier wave 둘 다 원형을 유지한다.

(1-3) Phase Shift Keying:

이 conversion scheme 에서, the phase of the original carrier signal 은 이진 데이터에 영향을 끼치기 위하여 변경된다.



Phase Shift Keying

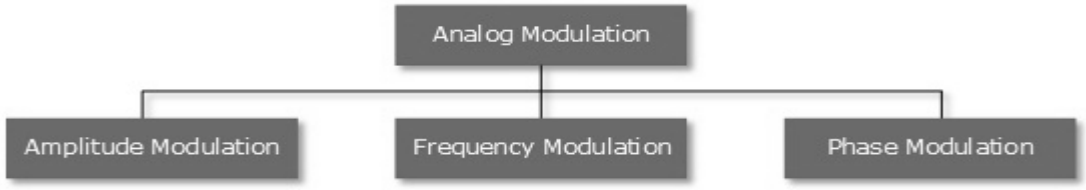
새 binary symbol 을 만날 때, the phase of the signal 이 바뀐다. Amplitude and frequency of the original carrier signal 은 원형을 유지한다.

(1-4) Quadrature Phase Shift Keying:

QPSK 는 한 번에 두 개의 이진 디지트를 반영하도록 phase 를 변경한다. 이것은 두 가지 서로 다른 phase 에서 이루어진다. The main stream of binary data 는 two sub-streams 에서 동일하게 나뉘어진다. serial data 가 both sub-streams 에서 병렬식으로 변환된 다음에 each stream 는 NRZ technique 을 사용하여 디지털 시그널로 변환된다. 그 후에, 두 digital signals 이 서로 통합된다.

2) Analog-to-Analog Conversion:

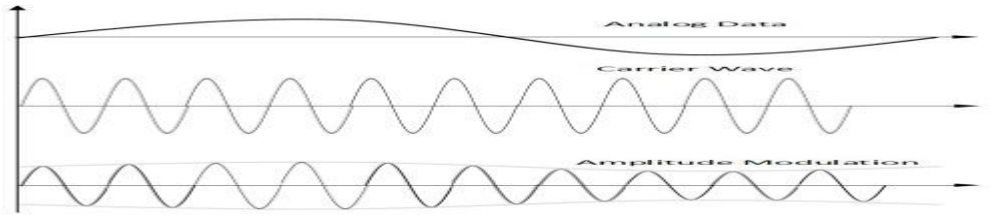
Analog signals 은 analog data 를 표현하기 위하여 변경되어야 한다. 이러한 conversion 을 Analog Modulation 이라 부른다. Analog modulation 은 bandpass 를 사용할 때 필요하다. Analog to analog conversion 은 3 가지 방법으로 이루어진다:



Analog Modulation

(2-1) Amplitude Modulation:

이 modulation 에서, the amplitude of the carrier signal 은 analog data 에 영향을 끼치도록 변경된다.

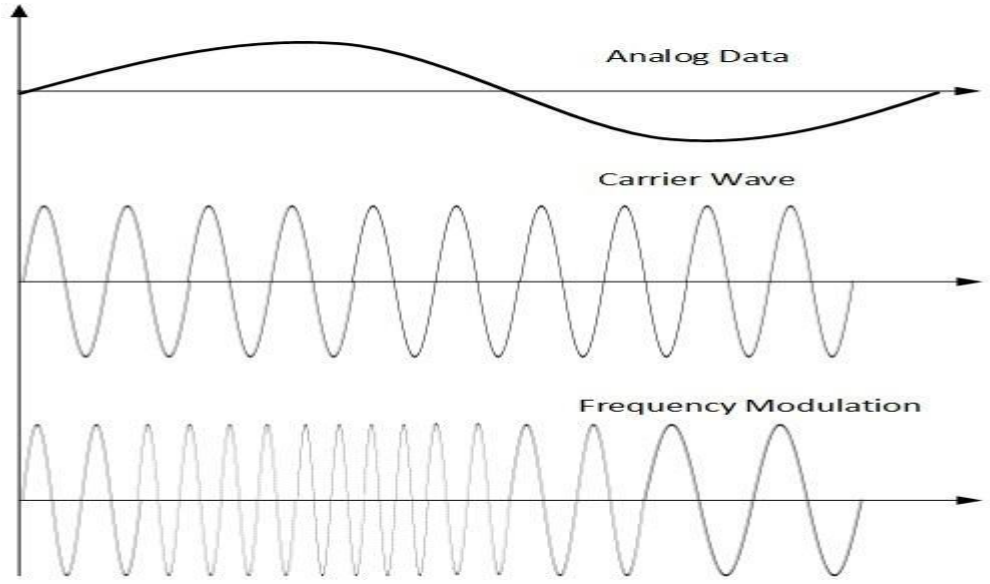


Amplitude Modulation

Amplitude modulation 은 multiplier 에 의해 실행된다. amplitude of modulating signal (analog data)는 amplitude of carrier frequency 에 의해 증폭되어, analog data 에 영향을 끼친다. frequency and phase of carrier signal 는 변하지 않는다.

(2-2) Frequency Modulation:

이 modulation technique 에서, the frequency of the carrier signal 은 the voltage levels of the modulating signal (analog data)의 변화를 반영하도록 변경된다.

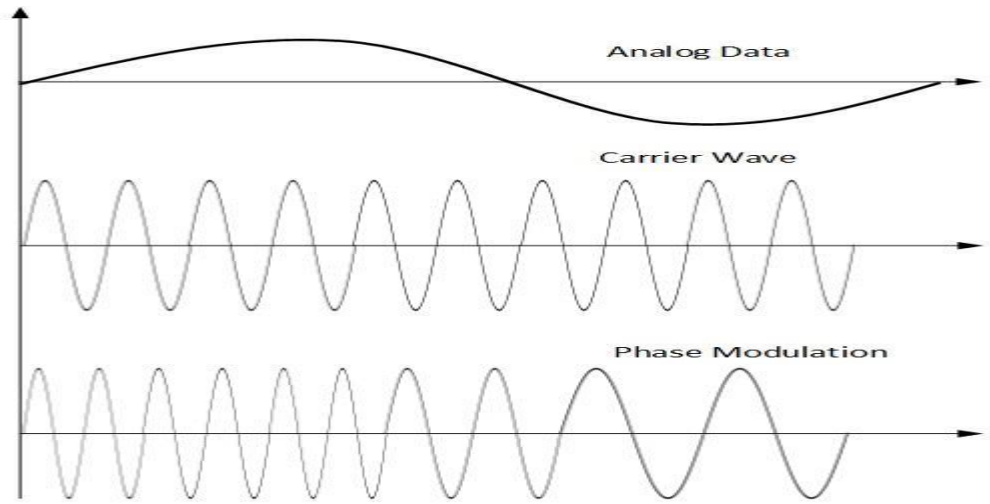


Frequency Modulation

The amplitude and phase of the carrier signal 는 변하지 않는다.

(2-3) Phase Modulation:

이 modulation technique 에서, the phase of carrier signal 은 voltage (amplitude) of analog data signal 의 변화를 반영하기 위하여 변경되어야 한다.



Phase Modulation

Phase modulation 은 실재적으로 Frequency Modulation 과 비슷하지만, Phase modulation frequency of the carrier signal 는 증가하지 않는다. Frequency of carrier signal 은 the amplitude of modulating signal 에서 voltage 변화를 반영하기 위하여 변경(made dense and sparse) 된다.

10. TRANSMISSION MEDIA

transmission media 란 computer network communication 이 가능하도록 하는 유일한 physical media 이다.

1) Magnetic Media

computer 간에 데이터를 전송하는 가장 편리한 방법 중의 하나는 network 이 탄생하기 전에도 저장 매체에 그것을 저장하여 한 스테이션에서 다른 곳으로 물리적으로 전송하는 것이다. 고속의 internet 시대인 오늘날 입장에서 비록 구식이라 하더라도, 데이터의 규모가 클 땐, 마그네틱 매체를 사용한다.

예를 들어, 은행은 고객에 대한 커다란 데이터를 취급하면서, 지리적으로 멀리 떨어져 있는 장소에 그것을 백업하여 안전하게 보관함으로써 재난을 예방할 수 있다. 은행에서 대용량의 백업 데이터가 필요하다면, internet 을 통해 그것을 전송하는 것은 쉽지 않다. WAN links 은 그 같은 고속을 지원하지 않는다. 그것들이 그렇게 한다면, 비용이 무척 비싸다.

이럴 경우에, data backup 이 magnetic tapes or magnetic discs 에 저장된 다음에, 원격지에서 물리적으로 변환시킨다.

2) Twisted Pair Cable

A twisted pair cable 은 두 개의 프라스틱으로 감싼 동선으로 되어 있으며, 두 개가 꼬여서 하나의 형태를 이루고 있다. 이 두 전선으로부터, 단지 하나만 실재 시그널을 전송하고, 나머지는 ground reference 용으로 사용된다. 전선 간의 twists 는 noise (electro-magnetic interference) and crosstalk 를 줄이는데 도움이 된다.

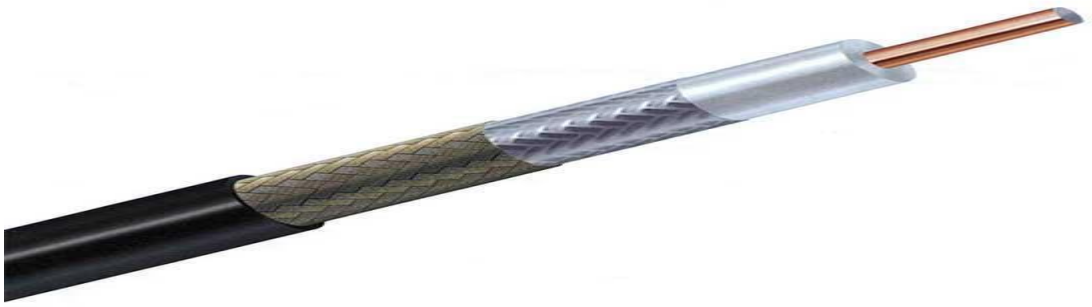
두 종류의 twisted pair cables 이 있다:

. Shielded Twisted Pair (STP) Cable: 금속막으로 감싼 twisted wire pair 로 되어 있으며, noise and crosstalk 에 대해 무반응한다.

. Unshielded Twisted Pair (UTP) Cable: 7 개의 카테고리를 갖고 있으며, 각각은 특별한 용도에 맞춰져 있다. computer networks 에서, Cat-5, Cat-5e, and Cat-6 cables 이 가장 많이 사용되며, UTP cables 은 RJ45 connectors 에 연결된다.

3) Coaxial Cable

Coaxial cable 은 two wires of copper 이다. 중심에는 core wire 가 있으며, 고체형 도체로 되어 있다. Core 는 절연되는 sheath(외장: wrapping)로 감싸여 있다. 두 번째 wire 는 sheath 로 감싸져 있으며, 또한 절연 sheath 로 다시 감싸여 있다. 이것 모두를 프라스틱 피복으로 덮여 있다.



Coaxial Cable

이러한 구조로 인하여, coax cable 은 높은 주파수의 시그널을 전달할 수 있어서, twisted pair cable 의 그것보다 우수하다. 이것의 피복 구조는 noise and cross talk 에 대한 우수한 방어막을 제공하며, Coaxial cables 은 고속의 bandwidth rates of up to 450 mbps 이 가능하다.

coax cables 에는 3 종류가 있다: RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG 란 Radio Government 의 줄인 말이다.

Cables 은 BNC connector and BNC-T 를 사용하여 연결되며, BNC terminator 는 양쪽 끝에 있는 와이어를 마감하는데 사용된다.

4) Power Lines

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

power lines 이 널리 사용되었기 때문에, PLC 는 모든 전기 기기를 통제하여 모니터할 수 있다. PLC 는 half-duplex 로 사용된다. 2 종류의 PLC 가 있다:

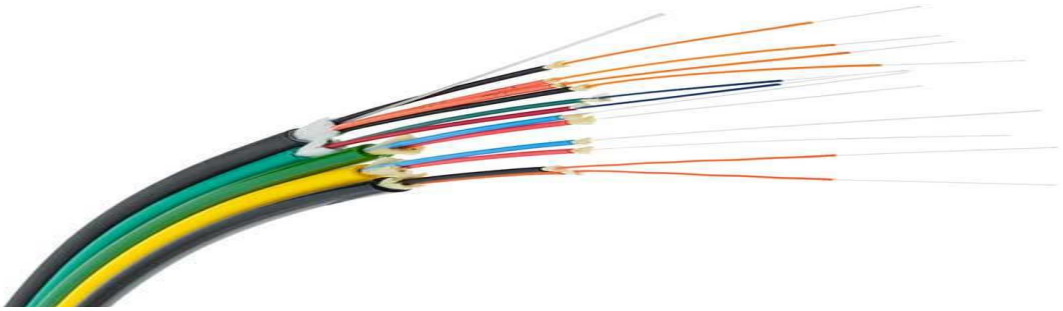
. Narrow band PLC: lower data rates up to 100s of kbps 를 제공하며, lower frequencies (3-5000 kHz)에서 작동한다. 수 키로 이상으로 확산될 수 있다.

. Broad band PLC: higher data rates up to 100s of Mbps 를 제공하며, higher frequencies (250 MHz)에서 작동한다. 이것들은 Narrowband PLC 만큼 확대될 수는 없다.

5) Fiber Optics

Fiber Optic 는 the properties of light 로 작동한다. light ray 가 critical angle 에 비칠 때, 그것을 90 도 굴절시킨다. 이러한 성질이 광섬유에서 사용되고 있다. The core of fiber optic cable 은 고순도의 glass or plastic 으로 만든다. 한 쪽 끝에서 빛이 방사되면, 선을 따라 여행한 다음에 다른 쪽 끝에 있는 light detector 에서 light stream 을 탐지한 다음에 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 a single ray of light 을 transportation 하는 반면에, multimode 는 multiple beams of light 를 전송한다.



Fiber Optics

Fiber Optic 또한 일방향성과 양방향성 기능을 갖고 있다. fiber optic 에 접근하기 위해서는 special type of connectors 가 사용되며, 이러한 것들로는 Subscriber Channel (SC), Straight Tip (ST), or MT-RJ 가 있다.

11. WIRELESS TRANSMISSION

Wireless transmission 은 a form of unguided media 이다. Wireless communication 은 두 개이상의 기기 사이에 설정된 어떠한 물리적 링크가 필요치 않다. 무선 시그널은 공중으로 퍼지며, 적절한 안테나에 의해 수집되고 해석된다.

antenna 가 electrical circuit of a computer or wireless device 에 접속할 때, digital data 는 무선 시그널로 바뀐 다음에 주파수 범위 안에서 퍼져 나간다. 상대쪽에 있는 receiptor 가 이 시그널을 받아서 다시 디지털 데이터로 변환시킨다.

electromagnetic spectrum 의 조그만 부분 만이 wireless transmission 에 사용된다.

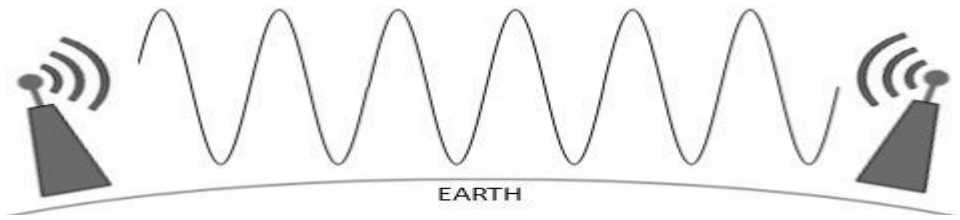
Electromagnetic Spectrum

1) Radio Transmission

Radio frequency 는 생산하기 쉬운데, 그것의 커다란 wavelength 가 벽 같은 구조물을 관통할 수 있기 때문이다. Radio waves 의 범위는 1mm 에서 100,000km 정도이며, 3Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency) 정도의 주파수 범위를 갖는다. Radio frequencies 는 six bands 로 다시 나뉜다.

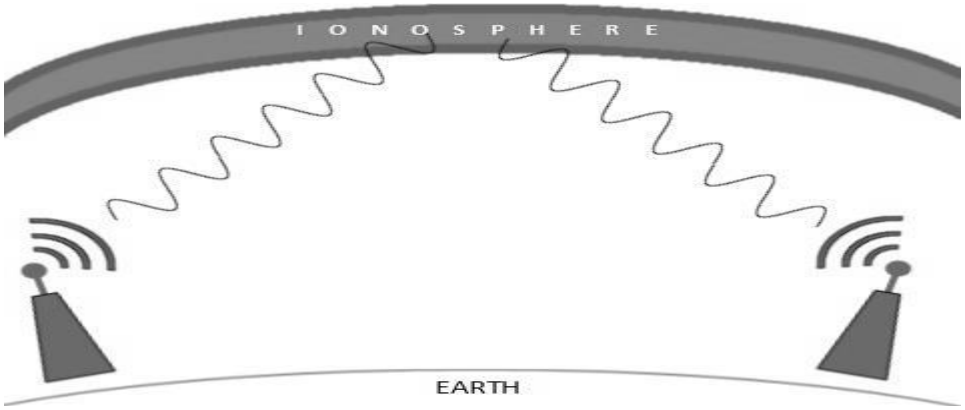
저 주파수인 Radio waves 는 벽을 통과할 수 있는 반면에, 높은 RF 는 직선으로 가며 벽에서 다시 튀어 나온다. 저 주파수의 힘은 거리가 늘어나면 급격하게 줄어든다. 반면에 High frequency radio waves 는 더 많은 파워를 갖고 있다.

VLF, LF, MF bands 와 같은 저 주파수들은 지상에서 1000 kilometers 까지 전달된다.



Radio wave – grounded

고주파의 Radio waves 는 빗물이나 기타 장애물에 흡수되기 쉽다. 이것들은 전리층(ionosphere)을 이용한다. 고주파 radio waves(HF and VHF bands 와 같은)는 윗쪽으로 확산된다. 이것들이 전리층에 도달 하면, 지상으로 다시 반사된다.

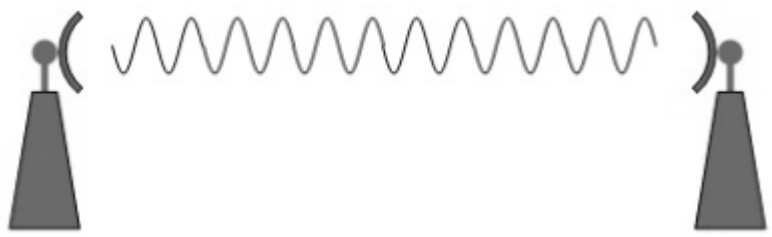


Radio wave - Ionosphere

2) Microwave Transmission

100MHz 이상의 전자기파는 직선으로 퍼지는 경향이 있으며, 이것의 시그널은 어떤 특별한 스테이션을 향해 보내지는 전파 빔에 의해 전송된다. Microwaves 가 직선으로 전파되기 때문에, sender 와 receiver 둘 다 엄격하게 line-of-sight 로 정렬돼 있어야 한다.

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



Personal Area Network

Microwave antennas 는 빔으로 만든 주파수를 모은다. 위의 그림에서처럼, 다수의 안테나들이 보다 멀리 도달하기 위하여 정렬될 수 있다. Microwaves 는 고주파이므로, 장애물인 벽을 뚫을 순 없다.

Microwave transmission 은 날씨와 사용 주파수에 크게 의존한다.

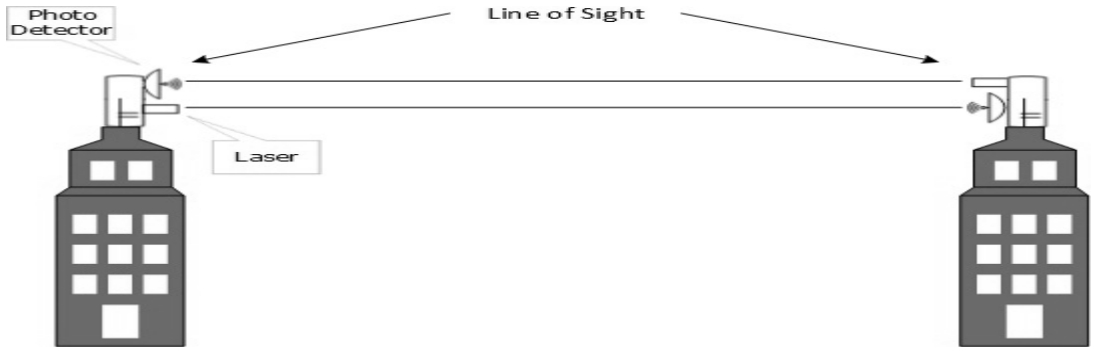
3) Infrared Transmission

Infrared wave 는 가시광선 스펙트럼과 microwaves 사이에 있다. 이것의 wavelength 는 700nm to 1mm 이며, 주파수 범위는 300GHz to 430THz 이다. Infrared wave 는 텔레비전과 리모콘과 같이 초단거리 통신에서 사용한다. 직선적인 Infrared 은 자연적으로 직진하며, 높은 주파수의 범위로 인하여 벽을 투과하진 못하다.

4) Light Transmission

데이터 통신에 사용되는 Highest most electromagnetic spectrum 은 light or optical signaling 이며, LASER 가 대표적이다.

frequency light uses 로 인하여, 이것은 엄격한 직진성을 갖는다. 그러므로 sender and receiver 는 line-of-sight 에 있어야 한다. laser transmission 은 일방성이므로, 양쪽 끝에는 the laser and the photo-detector 가 있어야 한다. Laser beam 은 일반적으로 폭이 1mm 이므로, 두 개의 receptors 가 레이저 소스에 정확하게 맞춰져 있어야 정확하게 작동하게 된다.



Light Transmission

Laser 는 Tx (transmitter)로 작동하고 photo-detectors 는 Rx (receiver)로 작동한다.

Lasers 는 walls, rain, and thick fog 을 관통할 수 없다. 추가로 laser beam 은 진행과정에 있는 wind, atmosphere temperature, or variation in temperature 에 의해 왜곡되기도 한다.

Laser 는 안전한 data transmission 이지만, communication channel 을 방해하지 않고 1mm 폭으로 레이저를 맞추는 것은 매우 어렵다.

12. MULTIPLEXING

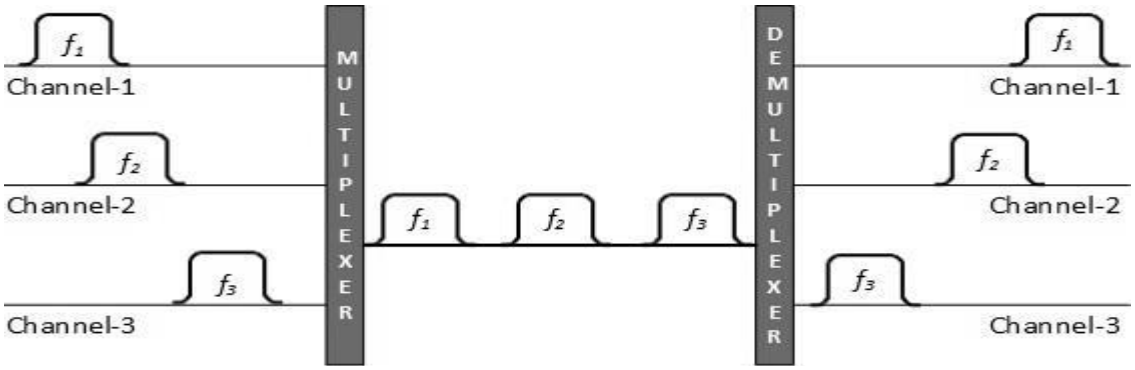
Multiplexing 이란 shared link 를 통하여 서로 다른 아날로그와 디지털의 전송 스트림을 동시에 처리하는 기법이다. Multiplexing 은 고성능의 medium 을 다양한 스트림에 사용할 수 있도록 저성능의 논리적 medium 으로 분할한다.

Communication 은 physical media (cable), 그리고 light (optical fiber)을 사용하여 공중(radio frequency)에서 이루어진다. 모든 매체는 multiplexing 이 가능하다.

다수의 송신자가 단일 매체로 다양한 데이터를 보낼 때, Multiplexer 기기는 이것을 물리적 채널로 분할하여 각각에 하나씩 할당한다. 그리고 통신의 반대쪽에 있는 De-multiplexer 는 단일 매체로부터 온 이러한 데이터를 받아서, 판별한 후에 receiver 로 보낸다.

1) Frequency Division Multiplexing

Carrier(전달객체)가 주파수일 경우, FDM 을 사용한다. FDM 이란 아날로그 기술이다. FDM 은 논리적 채널로 스펙트럼이나 캐리어를 분할한 다음, 각각의 사용자에게 각각의 채널에 할당한다. 사용자는 독립적으로 자신의 channel frequency 를 사용할 수 있으며, 그것에 독점적으로 접근할 수 있다. 모든 채널은 서로 중복되지 않게 분할된다. 채널들은 guard band 를 세분하여 사용하는 데, Guard band 란 해당 channel 에서 사용하지 않는 frequency 를 말한다.

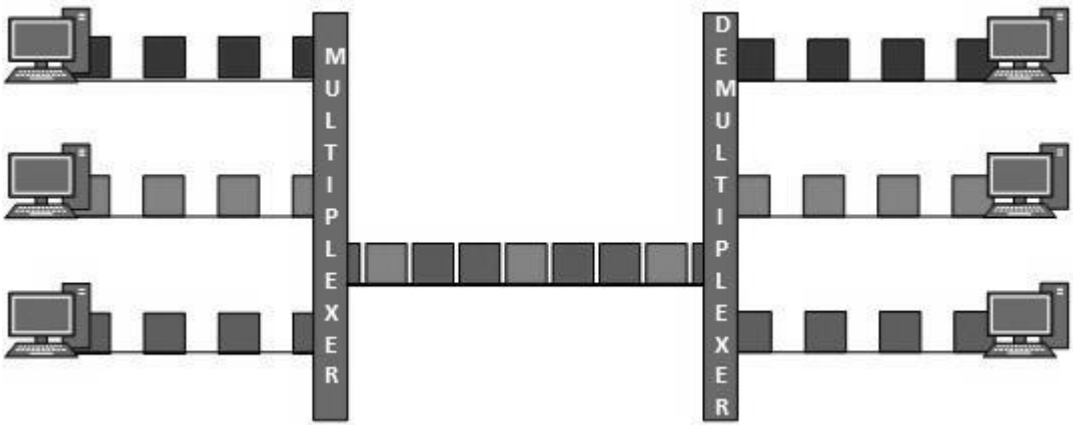


Frequency Division Multiplexing

2) Time Division Multiplexing

TDM 은 기본적으로 디지털 시그널에 적용되지만, 아날로그 시그널에도 적용될 수 있다. TDM 에서 공유되는 채널은 time slot(전송되는 데이터의 시간구분 단위)라는 방식으로 사용자들에게 분할된다. 사용자 각자는 오로지 제공된 time slot 내에서만 데이터를 전송할 수 있다. Digital signals 는 time slot 과 동등한 frames, 즉 특정한 time slot 에서 전송할 수 있는 최적의 크기의 frames 로 나눈다.

TDM 은 동기식 모드로 작동한다. 양쪽 끝의 Multiplexer and De-multiplexer 는 정확하게 동기식으로 작동하며, 다음 채널에서는 둘 다 동시에 역할이 뒤바뀌기도 한다.



Time Division Multiplexing

channel A 가 한 쪽 끝에 있는 frame 을 전송할 때, De-multiplexer 는 채널을 통해 반대쪽 끝에 있는 미디어로 그것을 전달한다. channel A's time slot 이 만료되자 마자, 이 쪽은 channel B 로 바뀐다. 반대쪽에서, De-multiplexer 도 동기식으로 작동하여, channel B 로 미디어에 전달된다. 서로 다른 채널에서 온 Signals 는 interleaved mode(신호의 부분들을 일정한 규칙에 따라 끼워 넣는 방식)으로 그 통로를 사용한다.

3) Wavelength Division Multiplexing

Light 은 다양한 wavelength (파장: 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 시그널로 사용한다는 특징이 있다.

Wavelength Division Multiplexing

더구나 각 wavelength time division 과 관련해서, multiplexing 방식을 사용하면 더 많은 데이터 시그널을 서로 통합하여 전달할 수 있다.

4) Code Division Multiplexing

Multiple data signals 은 Code Division Multiplexing 을 사용하면 단일 주파수로 전송할 수 있다. FDM 은 주파수를 보다 작은 채널로 나누지만, CDM 은 이용자로 하여금 full bandwidth 를 사용해서 언제든지 유일한 코드를 사용하여 시그널을 전송할 수 있도록 한다. CDM 은 직교코드(orthogonal codes: 수학적으로 각 요소들이 서로 독립적임을 나타내는 코드)를 사용하여 시그널을 전송한다.

각 스테이션에는 chip 이라는 유일 코드가 할당된다. 시그널은 독립적으로 이 코드와 함께 whole bandwidth 내에서 돌아다닌다. 그리고 receiver 는 자신에게 도달해야 하는 chip code signal 에 대하여 미리 알고 있다.

13. SWITCHING

Switching 이란 포트에서 포트로 packets 를 목적지로 보내는 과정을 말한다. 데이터가 한 포트에 들어올 때, 그것을 ingress 라 부르고, 데이터가 나갈 땐, egress 라 부른다. 통신 시스템에는 다수의 스위치와 node 가 포함되어 있다. 광의적으로 switching 은 두 개의 major categories 로 나눈다:

. Connectionless: 비연결성

어떠한 사전 호출/연결 설정행위가 없어도 두 호스트 시스템간에 트래픽을 교환할 수 있는 방식이다. 즉, 전송 전에 미리 연결을 설정하지 않는 방식으로 호(arc) 설정을 위한 절차가 없다.

. Connection Oriented: 연결지향성

통신이 시작되기 전에 송수신측 간에 논리적인 연결이 설정되어 있어야 한다. 두 개체 간에 1 개 이상의 메시지들이 연결상태를 유지하므로 데이터 교환이 가능하다. 데이터가 지속적이고 연속적인 흐름에 적합한 방식이다.

1) Circuit Switching

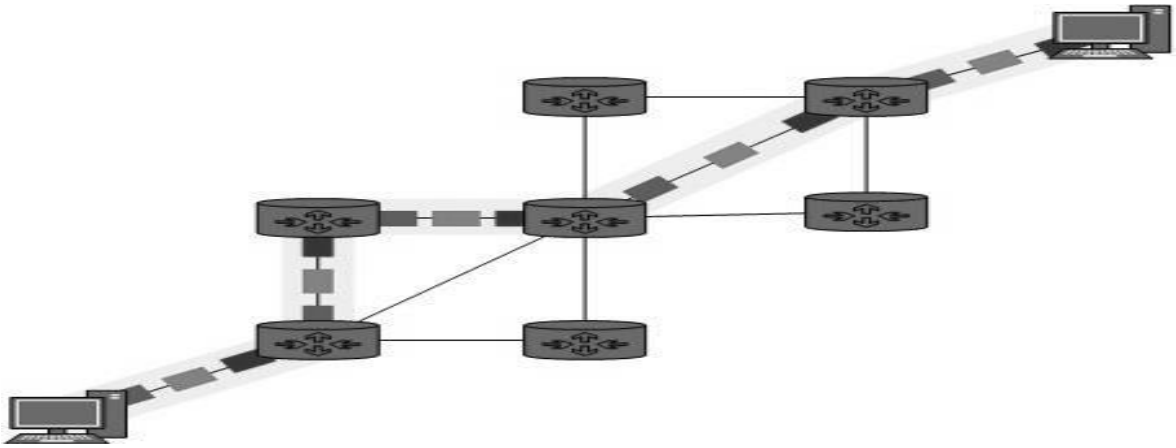
두 node 가 전용통신선으로 서로 통신할 때, circuit switching 이라 부른다. 특정 데이터를 전달하기 위하여 미리 정해진 루트가 필요하며, 그 밖의 다른 데이터는 허용되지 않는다. 데이터를 전송하는 circuit switching 에서, circuit 는 데이터 전송이 이루어지도록 설치되어야 한다.

Circuits 는 영원할 수도 일시적일 수도 있다. circuit switching 을 사용하는 applications 들은 다음과 같은 3 가지의 단계를 사용한다:

. Establish a circuit

. Transfer the data

. Disconnect the circuit



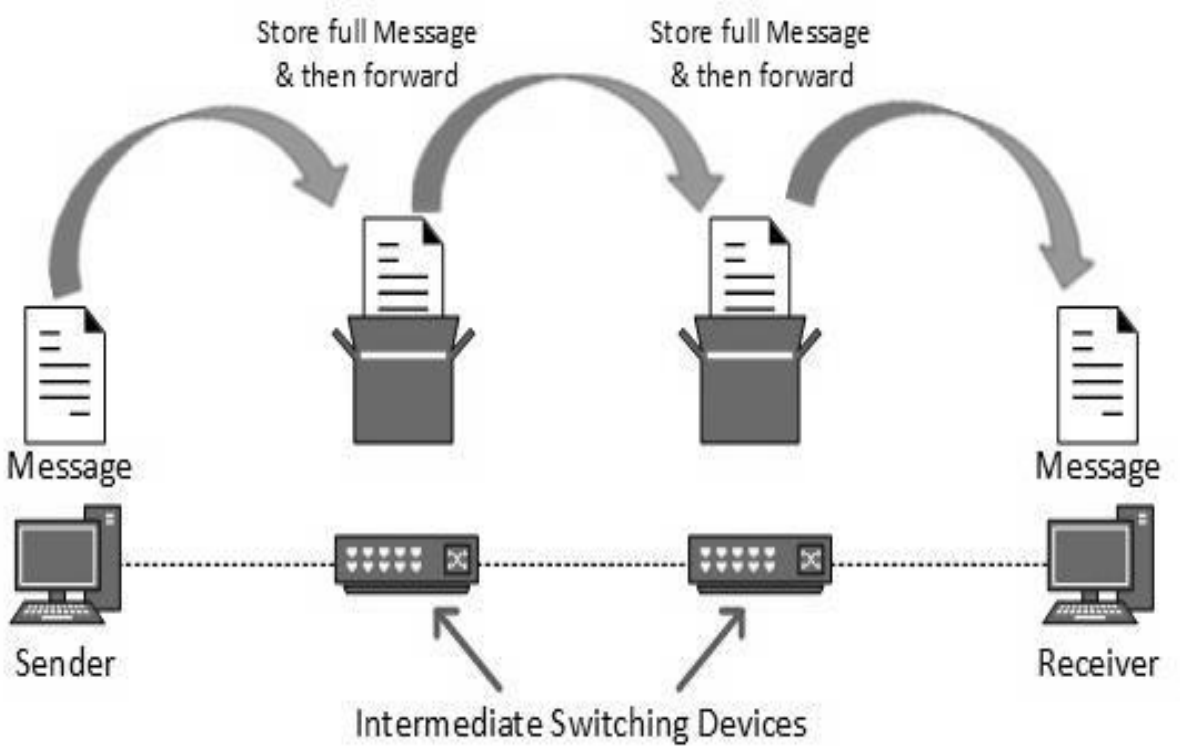
Circuit Switching

Circuit switching 은 voice applications 용으로 설계되었다. 전화는 가장 좋은 예의 circuit switching 이다. 이용자가 전화를 하기 전에, caller and callee 간의 virtual path(가상 통로: ATM 셀이 흐르도록 하는 논리적인 가상 파이프의 개념)가 network 전체에 설치돼 있어야 한다.

2) Message Switching

이 기법은 circuit switching and packet switching 의 중간 어디쯤에 해당된다. message switching 에서, 모든 message 는 data unit 로 취급되며, 전체가 스위칭되어 전송된다.

message switching 에서 작동하는 스위치는 먼저, 전체 메시지를 받은 다음, 전송할 수 있는 자원이 모일 때까지 그것을 buffer 한다. 대량의 메시지를 받기에 자원이 충분하지 않다면, 그 메시지는 저장되어 스위치를 기다린다.



Message Switching

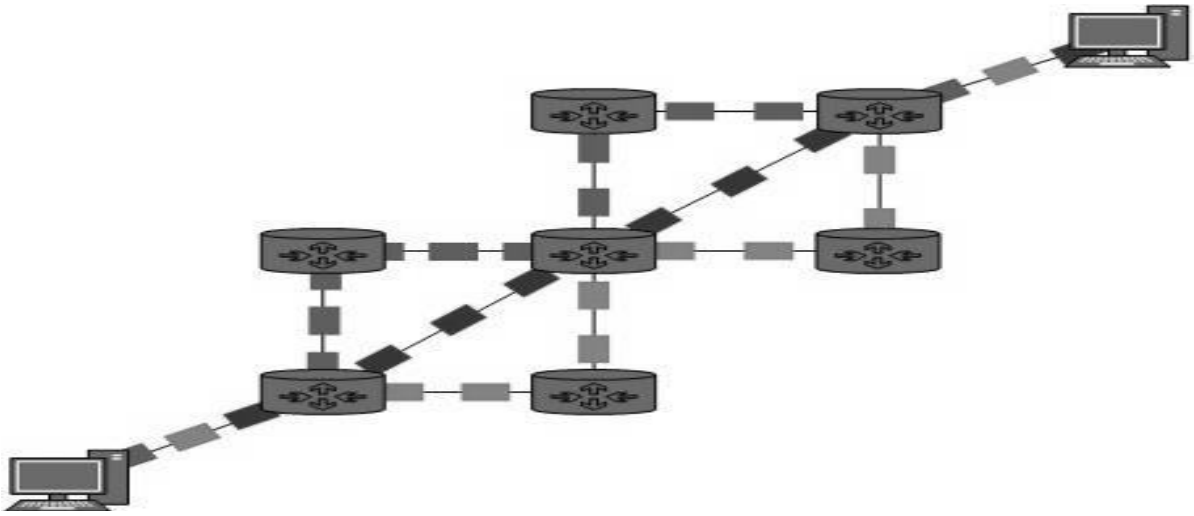
이 기법은 circuit switching 처럼 모든 통로가 단지 두 개의 엔티티에 의해 막혀있으므로, circuit switching 의 대체기법으로 여겨졌다. Message switching 은 packet switching 을 대신한 것이다. Message switching 의 단점은 다음과 같다:

. 전송통로에 있는 모든 스위치들은 메시지 전체를 저장할 수 있는 충분한 저장고를 필요로 한다.
. 자원을 이용할 수 있을 때까지 저장-그리고-전송 기법을 사용하여 대기(waits)하므로, 메시지 스위칭은 매우 느리다.
. 메시지 스위칭은 streaming media and real-time applications 을 위한 해결책은 못된다.

3) Packet Switching

message switching 의 단점이 packet switching 에 대한 아이디어를 유발시켰다. 전체 메시지를 packet 라고 부르는 보다 작은 chunks 로 쪼갠다. switching information 가 각 packet 의 헤더에 추가되어 있어서 각자 독립적으로 전송된다.

intermediate networking devices 에서 작은 크기의 packet 를 저장하는 것은 보다 편리하며, 이것들은 carrier path 에서나 internal memory of switches 에서나 많은 자원을 필요로 하지 않는다.



Packet Switching

Packet switching 은 다수의 applications 에서 발생한 packets 가 carrier 에서 multiplex 됨으로써 line efficiency 를 높인다. internet 은 packet switching technique 을 사용한다. Packet switching 은 이용자가 data streams 를 속성에 따라 분리하는 것을 가능하게 한다. Packets 는 service 의 품질을 나타내는 우선순위 별로 저장되어 발송 된다.

14. DATA LINK LAYER INTRODUCTION

Data Link Layer 는 OSI Layered Model 의 두 번째 layer 이다. 이 layer 는 가장 복잡한 레이어들 중의 하나이며, 복잡한 기능과 의무를 가지고 있다. Data link layer 는 통신 매체로서 보다 상위 layer 에서 자신을 기술하고 있는 중요한 하드웨어의 내역을 감추고 있다.

Data link layer 는 어떤 의미에서 직접 연결된 두 개의 호스트 사이에서 작동한다. 이러한 직접적인 연결은 point to point 나 broadcast 일 수 있다. broadcast network 상의 시스템은 동일한 링크에 있다고 말할 수 있다. data link layer 가 하는 일이 single collision domain 에서 복수의 호스트를 다룰 땐, 더욱 복잡해지는 경향이 있다.

Data link layer 는 data stream 을 비트 별 시그널로 변환시켜서 기본 하드웨어에 그것을 보내는 책임이 있다. 수신이 종료되면, Data link layer 는 하드웨어에서 전기시그널 형태로 되어 있는 데이터를 추출한 다음에, 인식할 수 있는 frame 포맷으로 그것들을 모아, 상위 layer 에 넘겨준다.

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

. Logical Link Control: protocols, flow-control, and error control 을 다룬다.

. Media Access Control: actual control of media 를 다룬다.

1) Functionality of Data-link Layer

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

. Framing:

Data-link layer 는 Network Layer 로부터 packets 를 받아서 그것들을 Frames 으로 캡슐화한다. 그런 다음, 그것은 하드웨어에 있는 각 frame 에 bit-by-bit 로 보낸다. 최종 수신에서, data link layer 는 하드웨어로부터 시그널들을 추출해서 그것들을 frame 에 모은다.

. Addressing:

Data-link layer 에서는 mechanism 을 addressing 하기 위하여 layer-2 hardware 를 제공하고 있다. Hardware address 는 링크할 때 유일한 것으로 여겨지고 있다. 이것은 하드웨어를 제조할 때 코드화된다.

. Synchronization:

데이터 frame 들이 링크로 보내질 때, 양쪽 컴퓨터들은 전송할 수 있도록 동기화되어야 한다.

. Error Control:

때때로 시그널들은 전송 시에 문제가 발생하여 그것의 비트들이 사라진다. 이러한 에러들은 감지되어야 하며, 처음의 데이터 비트를 회복할 수 있도록 하여야 한다. 또한 이것에서는 송신자에게 error reporting mechanism 을 제공하여야 한다.

. Flow Control:

똑같은 링크에 있는 스테이션들은 다양한 속도나 용량을 가지고 있다. Data link layer 에서는 양쪽 컴퓨터 모두 동일한 속도로 데이터를 교환할 수 있도록 flow control 을 보장하여야 한다.

. Multi-Access:

공유된 링크에 있는 호스트가 데이터를 전송하려고 할 때, 충돌의 확률이 매우 높다. Data link layer 에서는 복수의 시스템들끼리 공유하고 있는 미디어에 접근할 수 있는 성능을 갖고 있는 CSMA/CD 와 같은 메커니즘을 제공한다.

15. ERROR DETECTION AND CORRECTION

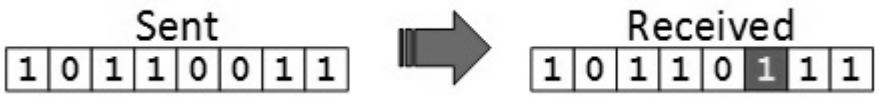
전송되는 동안 데이터를 망가뜨리는 많은 원인이 있다: noise, cross-talk etc. 상위 layer 들은 일반적인 network 구조에 맞춰 운영된다. 따라서 상위 layer 들은 시스템 간에 error-free transmission 을 기대한다. 대부분의 applications 들은 에러 데이터가 접수될 때, 기대한 만큼 작동하지 않는다. 다만 voice and video 와 같은 applications 들은 영향을 받지 않으므로, 에러가 있어도 잘 작동하기도 한다.

Data-link layer 는 frame(data bit streams)들이 정확하게 전송되었는지를 확인하기 위하여 error control mechanism 을 사용한다. 그러나 에러 통제 기법을 이해하기 위해서는 발생 가능한 에러의 종류가 무엇인지에 대하여 아는 것이 절대적이다.

1) Types of Errors

3 종류의 에러가 있다:

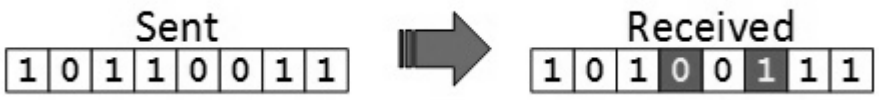
(1-1) Single bit error:



Single bit error

한 frame 안에, 어딘지 모르지만 부패한 비트가 하나만 있다.

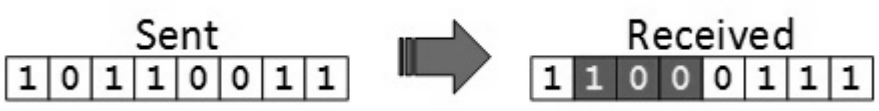
(1-2) Multiple bits error:



Multiple bits error

frame 이 부패한 상태의 복수의 비트를 수령하였다.

(1-3) Burst error:



Burst error

frame 에 하나이상의 연속된 부패 비트가 존재한다.

2) Error control mechanism 은 2 가지가 있다:

. Error detection

. Error correction

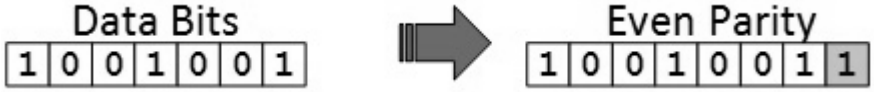
(2-1) Error Detection

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

(2-1-1) Parity Check:

한 개의 예외 비트를 초기 비트와 함께 보내서 even parity 의 경우에는 even 을, odd parity 의 경우에는 odd 를 만들도록 한다.

frame 을 만드는 동안 sender 는 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 의 값인 비트를 추가하여 even 을 만든다.



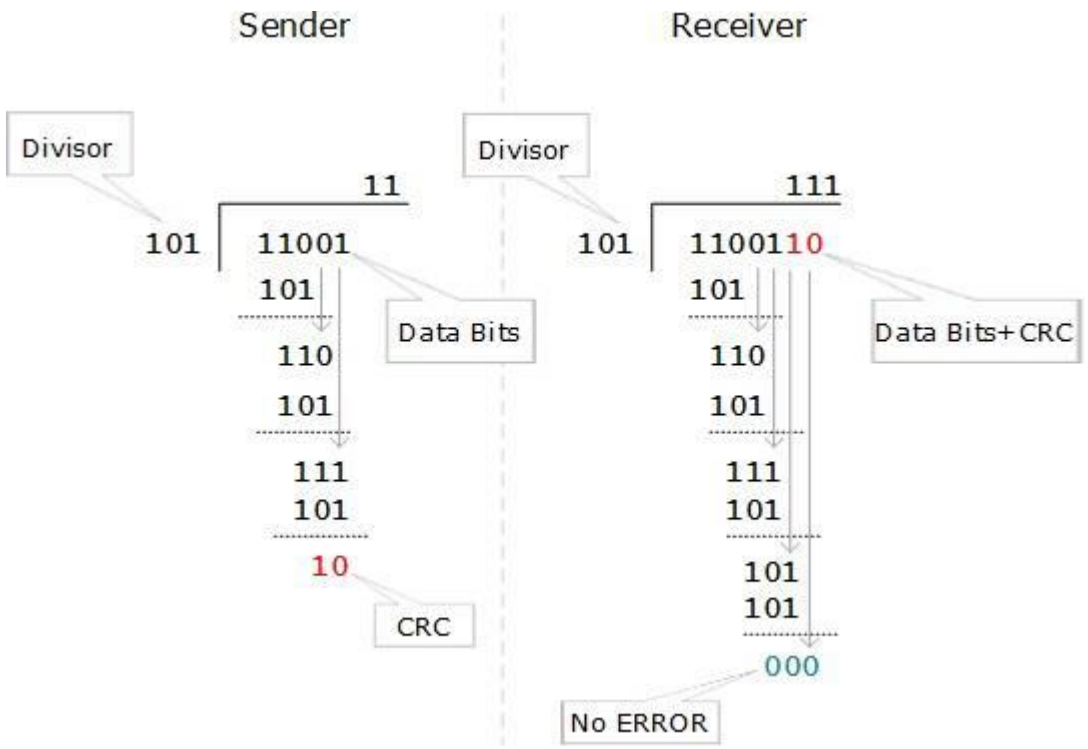
Even Parity

receiver 는 단지 frame 에서 1 의 숫자만 계산한다. 1 의 숫자가 even 이고 even parity 를 사용했다면, 그 frame 은 오염되지 않은 것으로 간주되어 접수된다. 만일 1 의 숫자가 odd 이고 odd parity 를 사용했다면 그 frame 도 아직 오염되지 않았다.

만일 싱글 비트가 전송 중에 flip 한다면, receiver 는 1 의 숫자를 계산함으로써 그것을 감지할 수 있다. 그러나, 1 개 이상의 비트가 에러라면, 그 receiver 가 에러를 탐지하기가 쉽지 않다.

(2-1-2) Cyclic Redundancy Check (CRC):

CRC 는 접수된 frame 에 유효한 데이터가 포함되어 있는지를 탐지하는 또 다른 방법이다. 이 기법에서는 전송된 데이터 비트를 이진적으로 분리를 한다. divisor 는 polynomials(다항식)을 사용하여 생산된다. sender 는 보낸 비트에 대한 division operation 을 수행하여, 나머지를 계산한다. 실재의 비트를 보내기 전에, sender 는 실재의 비트 끝에 그 나머지를 첨부한다. 이러한 Actual data bits plus the remainder 를 codeword 라 부르며, sender 는 codewords 로 데이터를 전송한다.



CRC

반대쪽 끝에, receiver 는 똑 같은 CRC divisor 를 이용하여 codewords 에 관한 divisiosn operation 을 수행한다. 만일 remainder 가 모두 zeros 라면, 그 데이터는 접수된다. 그렇지 않다면, 데이터가 전송 중에 오염된 것으로 간주한다.

(2-2) Error Correction

디지털 세상에서, error correction 에는 두 가지 방법이 있다:

(2-2-1) Backward Error Correction:

receiver 가 접수된 데이터에서 에러를 감지하면, sender 에게 다시 보내도록 요청한다.

(2-2-2) Forward Error Correction:

receiver 가 접수된 데이터에서 에러를 감지하면, error-correcting code 를 실행시켜서 자동으로 회복시키고 또한 어떤 종류의 에러는 수정처리 한다.

첫 번째인 Backward Error Correction 가 단순하며, 반송이 비싸지 않는 경우에 효율적으로 사용된다. 예가 fiber optics 이다. 그러나 무선 전송의 반송인 경우엔 비용이 엄청날 수 있다. 후자의 경우에는 Forward Error Correction 의 사용이 바람직 하다.

data frame 에서 에러를 수정하기 위하여, receiver 는 그 frame 의 어떤 비트가 오염되었는지를 정확하게 알아야 한다. 에러 비트를 찾기 위하여, 에러 탐지용인 패리티 비트 처럼 사용되는 잉여비트가 있다. 예를 들어, ASCII words (7 bits data)를 받을 때, 8 가지의 정보가 필요하다: 처음 7 개는 어떤 비트가 에러인지를 말해주고, 에러가 없다는 것을 알려주는 1 개 이상의 비트.

예를 들어, m 개의 데이터 비트에서 r 개의 잉여비트가 사용되었다. r 비트의 정보조합은 2^r 이다. m+r bit codeword 에서, 가능성이 있는 것은 r 비트들 그것들 스스로 부패될 수도 있다는 것이다. 그러므로 사용한 r 비트의 수는 m+r bit locations plus no-error information, 즉, m+r+1 이어야 한다.

$$2^r >= m+r+1$$

Required bits

16. DATA LINK CONTROL AND PROTOCOLS

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

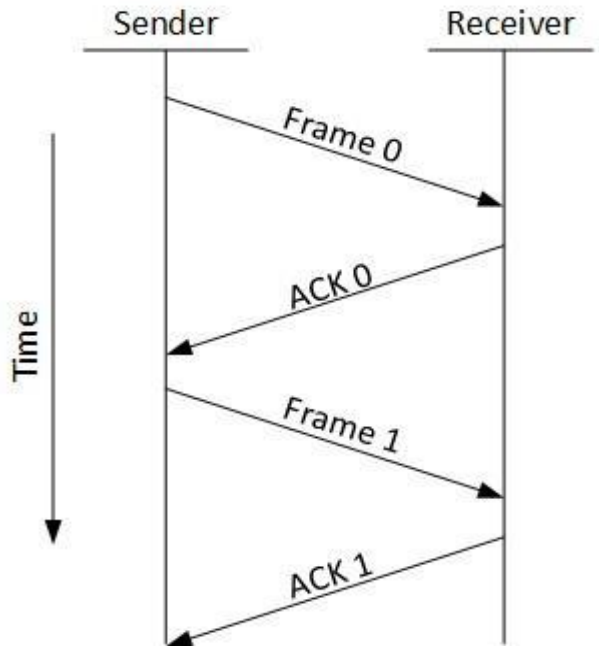
1) Flow Control

data frame (Layer-2 data)이 단일 매체를 통해 한 호스트에서 다른 호스트로 보내졌을 때, sender and receiver 는 같은 속도로 작업할 수 있어야 한다. 즉, sender 는 receiver 가 접수하여 처리할 수 있는 속도로 데이터를 보내야 한다. sender or receiver 의 속도가 다르면 어떻게 되는가? sender 가 너무 빨리 보내서 receiver 에 과부하가 걸리면(swamped), 데이터 손실이 발생할 수 있다.

데이터 통제를 위한 두 종류의 메커니즘이 있다:

(1-1) Stop and Wait :

이 flow control mechanism 은 데이터 전송이 이루어진 다음에 보내온 데이터-frame 을 접수한 것으로 인식할 때까지 sender 가 멈춰서 기다리도록 한다.



Stop and Wait

(1-2) Sliding Window:

이 flow control mechanism 에서, sender and receiver 둘 다 acknowledgement 를 보낼 때, 데이터-frame 의 수가 일치하여야 한다. 위에서 배웠듯이, stop and wait flow control mechanism 은 자원을 낭비하므로, 이 protocol 은 가능한 한 기본 자원을 많이 이용하도록 한다.

2) Error Control

data-frame 이 전송될 때, 전송 중에 데이터를 잃거나 오염돼 받을 수도 있다. 두 경우 모두, receiver 는 정확한 데이터-frame 을 받지 못하고, sender 는 어떤 손실이 있다는 것을 알지 못한다. 이런 경우에, sender and receiver 모두 데이터 손실과 같은 transit errors 를 탐지할 수 있는데 도움이 되는 protocol 을 마련하며, sender 쪽에서 data-frame 을 다시 보내거나 receiver 쪽에서 이전의 데이터-frame 을 재전송하도록 요구할 수 있어야 한다.

error control mechanism 의 필요조건은 다음과 같다:

. Error detection: 송수신자 둘 다 또는 한쪽에서 전송에 어떤 에러가 발생한 것을 확인한다.

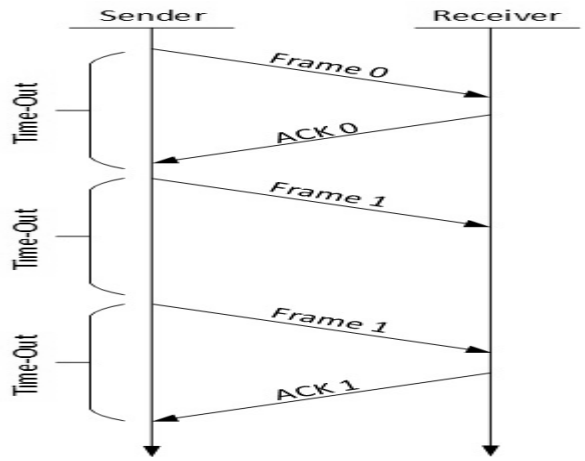
. Positive ACK: 수신자가 올바를 frame 을 수령하면 그것을 확인(acknowledge)시켜야 한다.

. Negative ACK: 수신자가 손상된 frame 이나 중복된 frame 을 접수했을 때, 그것은 송신자에게 다시 NACK 를 보내고 송신자는 다시 정확한 frame 을 전송한다.

. Retransmission: 송신자는 종료시간을 설정한다. 만일 이전에 데이터 frame 에 대한 인정이 종료시간 전에 도착하지 않는다면, 송신자는 그 frame 이나 그것에 대한 확인이 전송 중에 분실된 것으로 생각하면서, 그 frame 을 다시 전송하다.

Data-link 에서 에러를 통제하기 위하여 이용할 수 있는 3 가지 종류의 Automatic Repeat Requests (ARQ) 기법이 있다:

(2-1) Stop and wait ARQ:



Stop and Wait ARQ

다음과 같은 변환이 Stop-and-Wait ARQ 에서 발생한다:

. 송신자는 종료시간 계산을 관리한다.

. frame 이 보내지면, 송신자는 종료시간 계산을 시작한다.

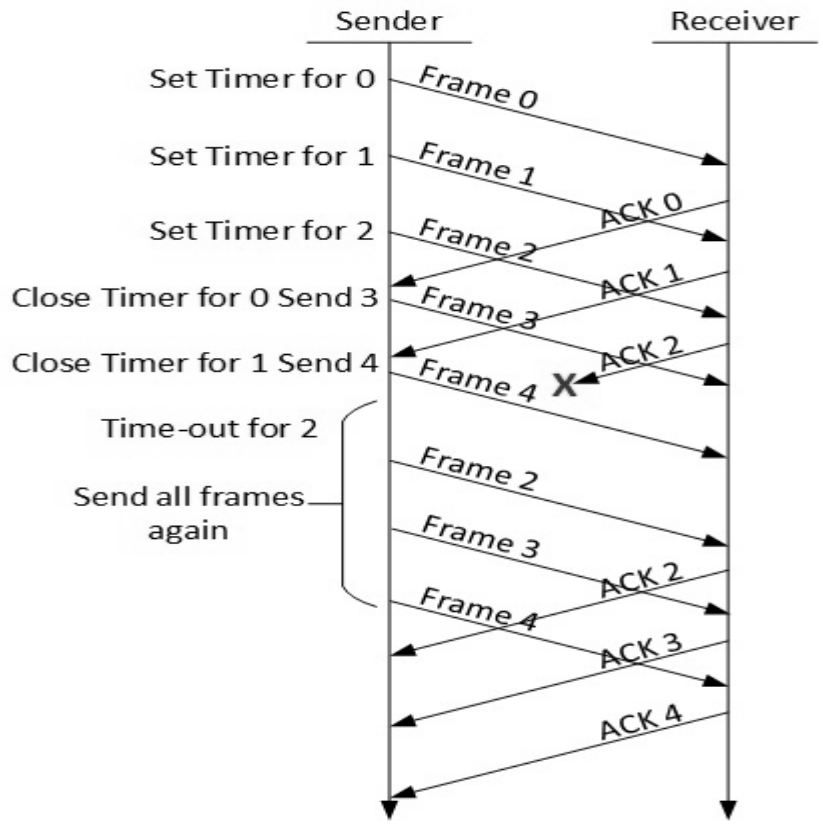
. 만일 frame 의 확인이 제 때에 오면, 송신자는 순서에 따라 다음 frame 을 전송한다.

. 만일 frame 의 확인이 제 때에 오지 않으면, 송신자는 frame 이나 그것의 확인이 전송 중에 분실된 것으로 간주한다. 송신자는 frame 을 재송신한 다음에 종료시간의 계산을 시작한다.

. 만일 부정적인 확인이 접수된다면, 송신자는 그 frame 을 다시 보낸다.

(2-2) Go-Back-N ARQ:

Stop and wait ARQ mechanism 은 자원을 최상으로 활용하지 못한다. 확인데이터(acknowledgement)가 접수될 때까지, sender 는 빈들거리면서 아무 것도 하지 않는다. Go-Back-N ARQ method 에서, sender and receiver 모두 window 를 확보하고 있다.



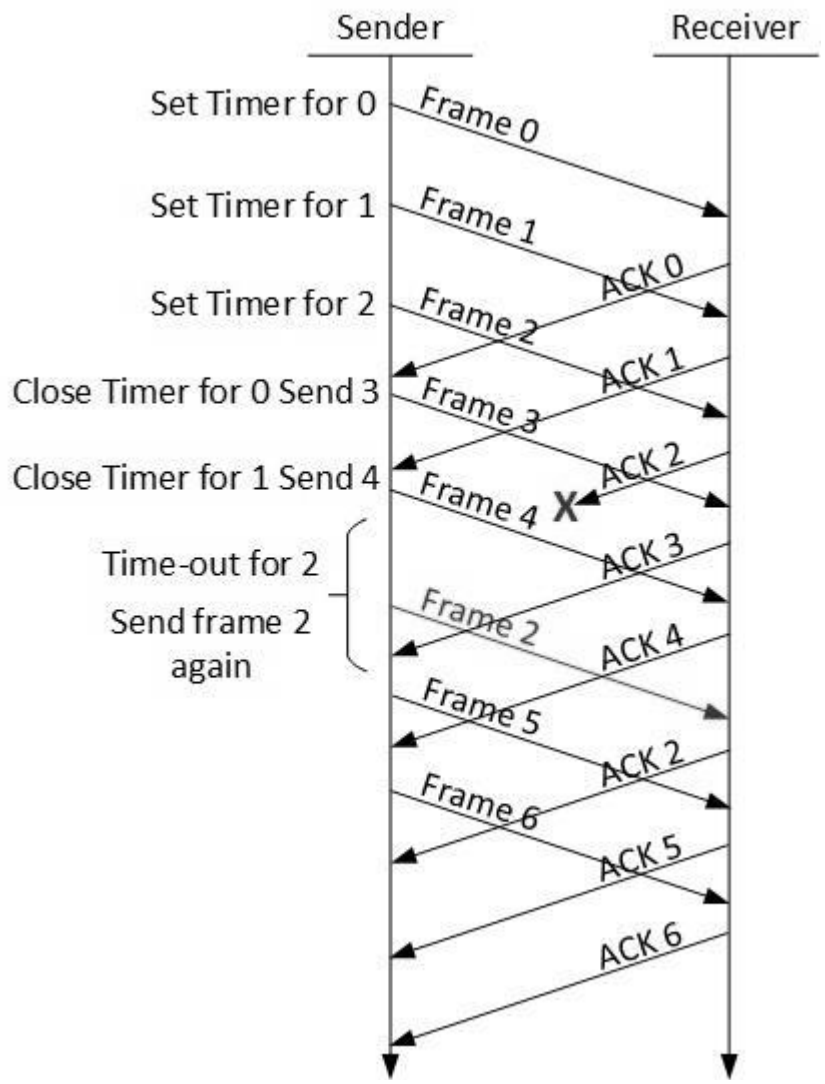
Go-back-n ARQ

sending-window size(TCP 흐름제어를 위해 송신자에게 자신의 수신 버퍼 여유용량의 크기를 지속적으로 통보하는 16 비트 필드)를 통해 sender 는 이전의 것에 대한 acknowlegdement(확인응답)를 받지 않고도 다수의 frame 을 보낼 수 있다. receiving-window 는 receiver 가 복수의 frame 을 접수하고 그것을 acknowledge 할 수 있게 한다. Receiver 는 접수된 frame 의 순서 번호를 추적한다.

sender 가 윈도우에 있는 모든 frame 을 보낼 때, 어떤 순번까지가 positive acknowledgemen 를 체크한다. 모든 frame 이 긍정적인 것으로 인정된다면, sender 는 다음 세트의 frame 을 보낸다. 만일 sender 가 NACK 을 접수했거나 특별한 frame 용으로 어떤 ACK 를 받지 못했다면, 어떠한 긍정적인 ACK 도 받지 못했으므로 모든 frame 이 반송된다.

(2-3) Selective Repeat ARQ:

Go-back-N ARQ 에서, reciever 는 윈도우 사이즈에서 어떤 버퍼 공간도 갖고 있지 않다고 가정한다. 따라서 접수될 때마다 각 frame 을 처리해야 한다. 이것은 sender 에게 인정받지 못한 모든 frame 을 반송하도록 한다.



Selective-Repeat ARQ 에서, receiver 는 순번을 추적하는 동안, 메모리에 frame 을 버퍼한 다음에 빠지거나 손상된 frame 만을 대상으로 NACK 를 보낸다. 이런 경우에, sender 는 NACK 접수용 packets 만을 보낸다.

17. NETWORK LAYER INTRODUCTION

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

Network layer 는 subnet 안팎의 소스로부터 목적지로 packets 를 라우팅하는 책임을 가지고 있다. 두 가지 서로 다른 서브 network 은 서로 다른 addressing schemes 나 non-compatible addressing types 을 가질 수 있다. protocols 와 똑같이, 두 개의 다른 서브 network 는 서로 호환되지 않는 다른 protocol 을 가지고 운영할 수 있다. Network layer 는 서로 다른 addressing schemes and protocols 를 mapping 하여 소스로부터 목적지까지 packets 를 라우팅해야 하는 책임을 가지고 있다.

1) Layer-3 Functionalities

Network Layer 에서 작동하는 기기들은 주로 라우팅에 초점을 맞추고 있다. Routing 에는 한가지 목표를 달성하기 위한 다음과 같은 여러 가지가 임무가 포함될 수 있다.

. Addressing devices 와 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 제공할 수 있다:

. 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 internet 에서 end-to-end 디바이스가 통신하는 것을 돕는 Network Layer protocol 을 참조하였다. 두 가지 모두에서 이러한 냄새가 난다. 수십 년 동안 세상을 지배했지만 지금은 뒤쳐진 address space 를 다루는 IPv4 그리고 이것을 대체하고자 만들어서 이것의 문제점을 약화시키려는 목적의 IPv6 가 그것이다.

18. NETWORK ADDRESSING

Layer 3 network addressing 은 Network Layer 의 주요 업무들 중의 하나이다. Network Addresses 는 항상 논리적이다. 다시 말해서, 이것들은 적합한 configurations(형상)으로 변경이 가능한 소프트웨어 의존형의 address 이다.

A network address 는 항상 host / node / server 를 포인트하거나, 전체 network 을 나타낼 수 있다. Network address 는 항상 network interface card 에서 configured 하며, 일반적으로 Layer-2 communication 용 컴퓨터의 MAC address (hardware address or layer-2 address)를 갖춘 시스템에 의해 mapped 된다.

현존하는 다양한 network addresses 는 다음과 같다:

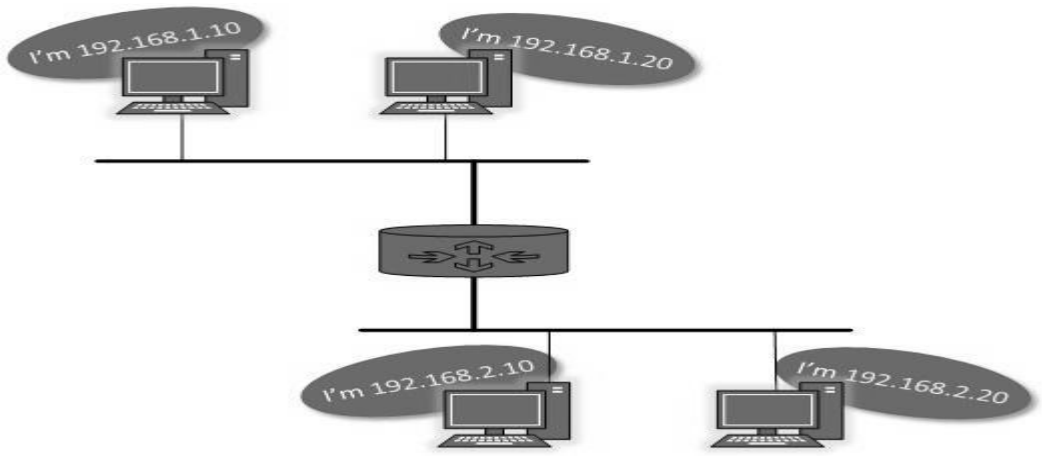
. IP

. IPX(Internetwork Packet Exchange):

IPX/SPX 프로토콜은 1980 년대 초 노벨에서 개발되었다. 따라서 노벨에서 개발된 Netware 의 기본 프로토콜이 되었다. IPX/SPX 는 IPX 와 SPX 로 구분할 수 있는데, IPX 는 TCP/IP 의 IP 의 역할을 하고, SPX 는 TCP 의 역할을 한다. IPX 주소는 노드 ID 와 네트워크 주소로 나뉜다. 노드 ID 는 48 비트로 구성된 MAC 주소를 이용하고, 네트워크 주소는 32 비트로 구성된다.

. AppleTalk:

애플사가 컴퓨터 네트워킹을 위해 개발한 프로토콜 스위트이다. 1984 년에 초기 매킨토시에 포함되었으며, TCP/IP 네트워킹의 선호로 인해 잘 쓰이지 않게 되었다. 구조적 측면에서 보면 애플의 매킨토시뿐 아니라 IBM 호환 PC 와 같은 애플이 아닌 컴퓨터와 서로 통신할 수 있으며, 프린터나 서버 등의 리소스를 주고 받을 수 있게 되어 있다.



Network Addressing

IP addressing 은 hosts 와 network 를 구별하는 메커니즘을 제공한다. IP addresses 가 계층방식으로 할당되기 때문에, host 는 항상 특별한 network 에 소속된다. 자신의 subnetwork 로 외부와 통신하려는 호스트는 packet/data 를 보내는 destination network address 를 알아야 한다.

다른 subnetwork 의 Hosts 는 서로간의 위치를 확인하는 메커니즘이 필요하다. 이러한 업무를 DNS 가 하는데, DNS 란 mapped 된 원격 호스트의 Layer-3 address 에 그것의 domain name 이나 FQDN 을 제공하는 서버이다. host 가 원격 호스트의 Layer-3 Address (IP Address)를 얻을 때, gateway 처럼 그것의 모든 packets 를 포워드 한다. Gateway 란 destination host 로 packets 를 라우트하도록 유도시키는 정보를 갖고 있는 라우터이다.

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

. 목적지 네트워크의 어드레스

. 그 네트워크에 도달하는 방법

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

통로에 있는 그 다음의 라우터도 동일한 일을 하므로, 결과적으로 데이터 packets 가 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)

Router 는 broadcast traffic 을 결코 초기 값으로 포워드하지 않는다. Multicast traffic 은 대부분의 video stream 이나 audio 에서 최우선적으로 사용된다. Anycast 는 unicast 와 비슷하지만, 복수의 목적지를 사용할 때 packets 가 가장 가까운 목적지로 전달된다는 차이가 있다.

19. NETWORK ROUTING

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

Router 는 항상 default route 로 구성(configure) 된다. default route 는 특별한 목적지용의 라우터를 발견할 수 없을 때, packets 를 포워드할 라우터를 알려준다. 같은 목적지에 도달할 수 있는 복수의 통로가 존재한다면, 라우터는 아래의 정보에 따라 그 통로를 결정한다:

. Hop Count

. Bandwidth

. Metric

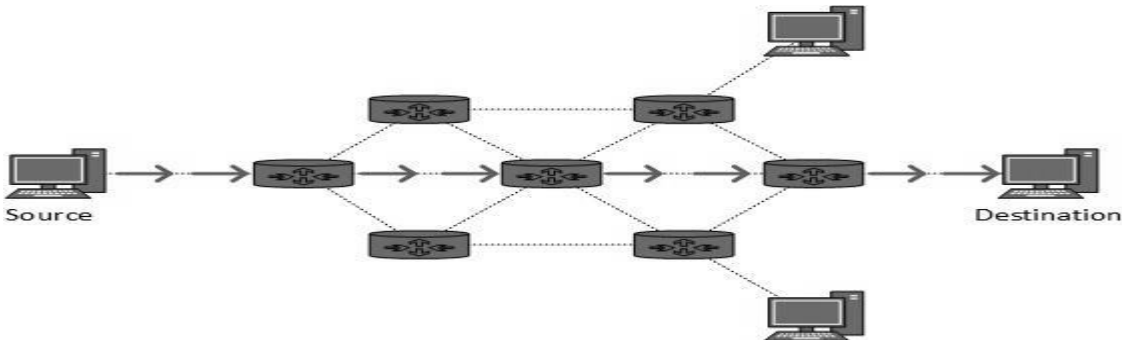
. Prefix-length

. Delay

Routes 는 statically configured or dynamically learnt 할 수 있다. Route 는 다른 기기보다 우선적으로 configure 할 수 있다.

1) Unicast routing

internet 과 intranetwork 에서 대부분의 트래픽을 unicast data or unicast traffic 이라 부르며, 특별한 목적지로 데이터를 보낸다. internet 에서 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, 다음 hop 로 packets 를 포워드하면 된다.



Unicast routing

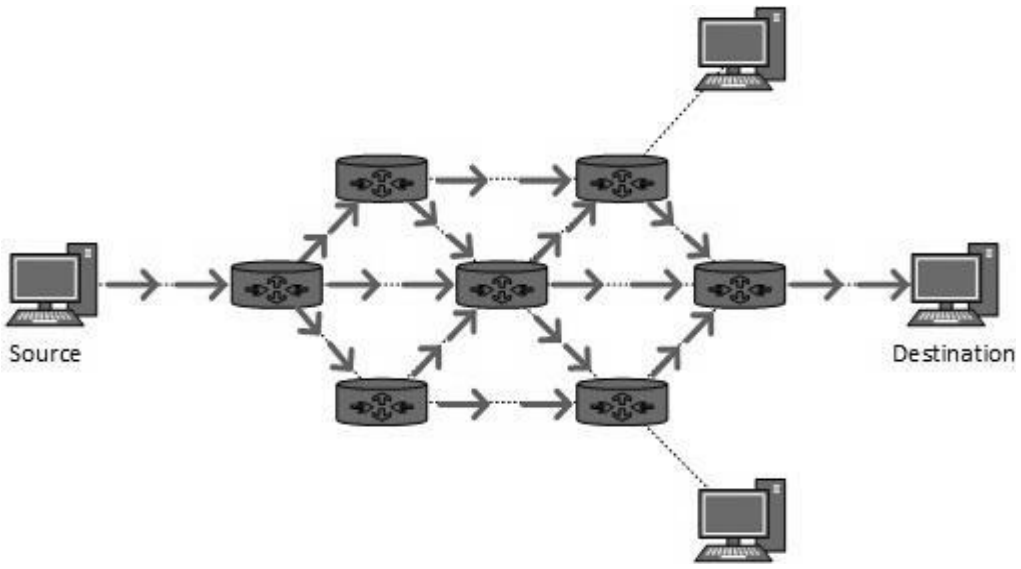
2) Broadcast routing

초기값에 의해, broadcast packets 은 특정 network 의 라우터로는 라우트 또는 포워드 되지 않는다. 왜냐하면 Routers 가 broadcast domains 을 가지고 있기 대문이다. 그렇지만, 필요하다면 어떤 특별한 경우에는 broadcast 를 포워드하도록 configured 할 수 있다.

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

> 라우터가 데이터 패킷을 만든 다음에 하나씩 각각의 호스트에 그것을 보낸다. 이러한 경우에, 그 라우터는 다양한 목적지 어드레스를 갖는 하나의 데이터 패킷의 사본을 복수로 제작한다. 모든 패킷은 unicast 로 보내지지만 그것들이 모두에게 보내지기 때문에 마치 라우터는 broadcasting 처럼 흉내를 낸다.

> 이러한 방법은 많은 bandwidth 를 소비하며 라우터는 각 노드의 목적지 정보를 갖고 있어야 한다. 두 번째로, 라우터가 broadcasted 된 패킷을 접수할 때, 그것은 모든 인터페이스로부터 발생한 이러한 패킷으로 인하여 간단하게 넘쳐난다(flood). 모든 라우터들은 동일한 방식으로 configured 되어야 한다.



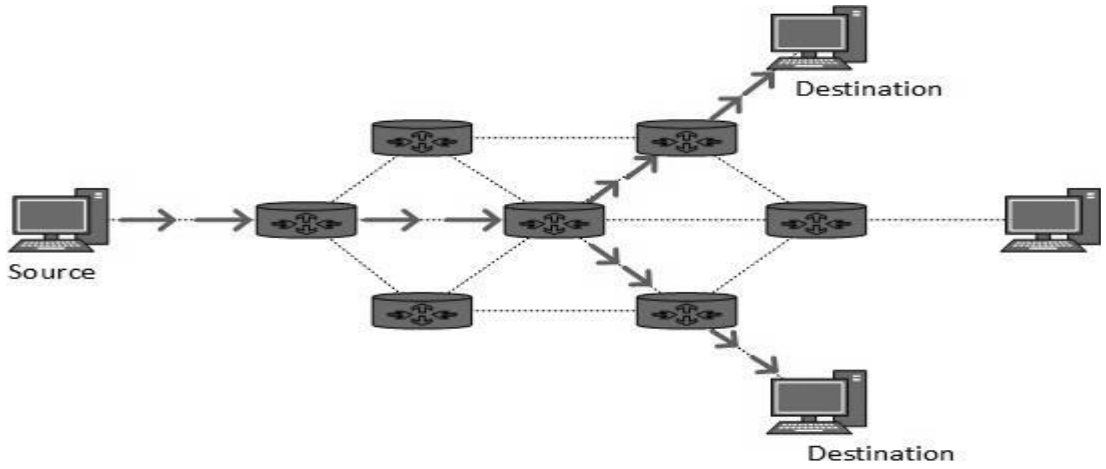
Broadcast routing

>이 방법은 라우터의 CPU 에서는 쉽지만 동료 라우트로부터 접수된 패킷이 중복되는 문제를 야기시킬 수 있다..

> Reverse path forwarding 은 하나의 기법이다. 이것은 라우터가 broadcast 를 접수해야만 하는 그것의 전임자에 대하여 미리 알고 있다는 것을 의미한다. 이 기법은 중복된 패킷을 탐지하고 폐기하는데 사용된다.

3) Multicast Routing

Multicast routing 은 broadcast 의 특별한 경우이며, broadcast 의 커다란 차이와 도전이다. broadcast routing 에서, packets 는 만일 원치 않는다면 모든 node 에 전송된다. 그러나 Multicast routing 에서 그 데이터는 단지 그 packets 를 받기 원하는 node 에만 전달된다.



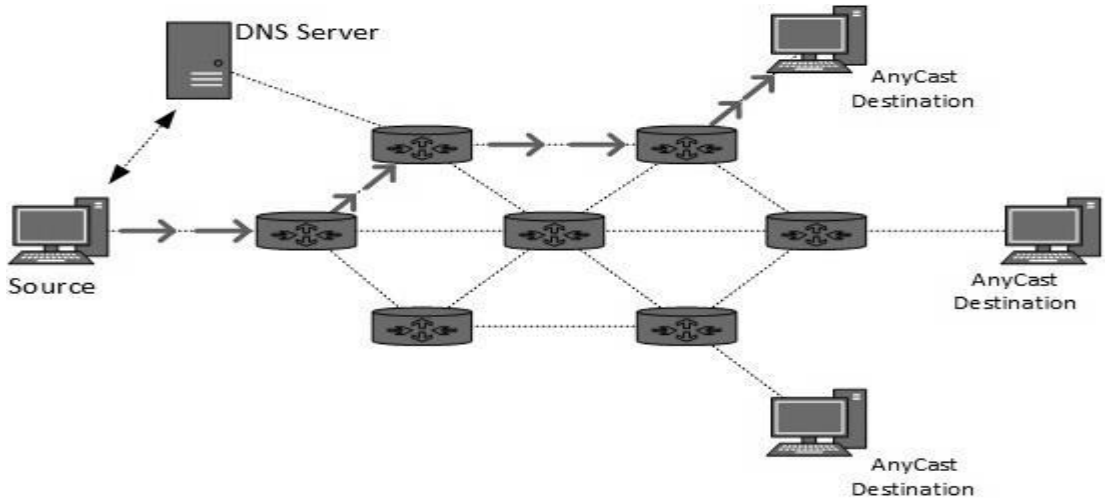
Multicast routing

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

Multicast routing 또한 duplicates and loops 을 탐지하여 폐기하는 reverse path Forwarding technique 을 사용한다.

4) Anycast Routing

Anycast packet forwarding 은 multiple hosts 가 동일한 논리적 address 를 가질 수 있도록 하는 메카니즘이다. 이러한 논리적 address 를 목표로 하는 packets 가 접수될 때, routing topology 에서 가장 가까이 있는 호스트로 보낸다.



Anycast routing

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

5) Unicast Routing Protocols

unicast packets 을 라우트할 때 사용할 수 있는 두 가지 종류의 라우팅 protocol 이 있다:

>Distance Vector Routing Protocol: Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers, for example, Routing Information Protocol (RIP).

>Link State Routing Protocol: Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. All routers then

calculate their best path for routing purposes, for example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).

6) Multicast Routing Protocols

Unicast routing protocols 은 그래프를 사용하지만, Multicast routing protocols 은 trees 를 사용한다. 다시 말해서, loops 를 피하기 위한 spanning tree(다중 경로에서 불필요한 경로 발생 시 덧붙임 경로를 제공하여 가장 효율적인 경로를 사용하는 기법)를 사용한다. 최적의 트리는 shortest path spanning tree 이다.

. DVMRP: Distance Vector Multicast Routing Protocol

. MOSPF: Multicast Open Shortest Path First

. CBT: Core Based Tree

. PIM: Protocol independent Multicast

Protocol Independent Multicast 는 현재 일반적으로 사용되며, 두 가지가 선호된다:

. PIM Dense Mode: This mode uses source-based trees. It is used in dense environment such as LAN.

. PIM Sparse Mode: This mode uses shared trees. It is used in sparse environment such as WAN.

7) Routing Algorithms

routing algorithms 은 다음과 같다:

(7-1) Flooding:

Flooding 은 가장 단순한 packet forwarding 방법이다. packets 가 접수될 때, 라우터들은 모든 interface 에 그것을 보내지만, 이미 접수된 것은 제외시킨다. 이것은 network 에 너무나 많은 부담을 주며, 많은 중복 packets 들이 network 에서 방황하게 된다.

Time to Live (TTL)는 packets 의 무한 루핑을 피하기 위하여 사용될 수 있다. Selective Flooding 이라 부르는 또 다른 flooding 방법이 있는데, 이것은 network 의 overhead 를 감소시킨다. 이 방법에서, 라우터는 선택된 것을 제외하고는 모든 interface 에 flood out 하지 않는다.

(7-2) Shortest Path:

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

일반적인 shortest path algorithms 은 다음과 같다:

. Dijkstra's algorithm:

an algorithm for finding the shortest paths between nodes in a graph, which may represent, for example, road networks. It was conceived by computer scientist Edsger W. Dijkstra in 1956 and published three years later

. Bellman Ford algorithm:

an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph. It is slower than Dijkstra's algorithm for the same problem, but more versatile, as it is capable of handling graphs in which some of the edge weights are negative numbers.

. Floyd Warshall algorithm:

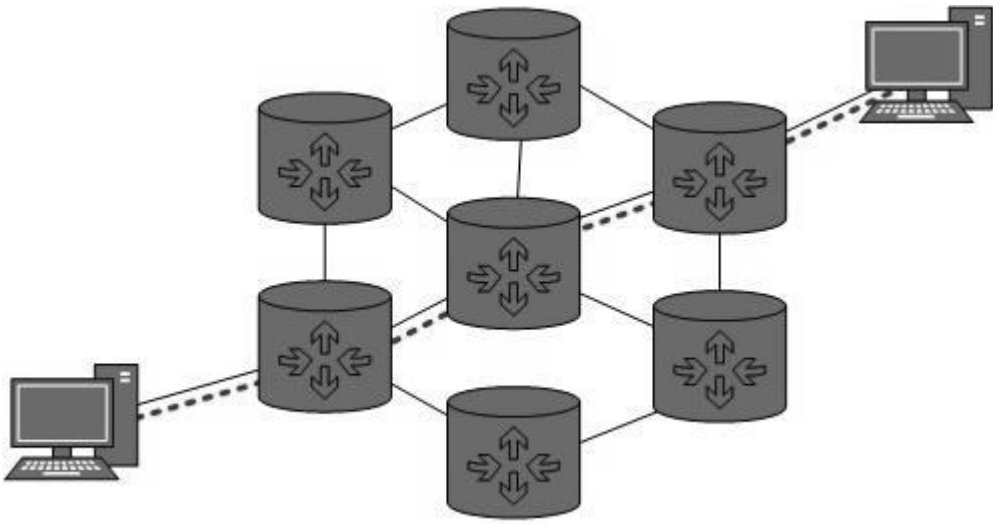
an algorithm for finding shortest paths in a weighted graph with positive or negative edge weights (but with no negative cycles)

20. INTERNETWORKING

실 세계에서, 동일한 행정하의 network 들은 일반적으로 말해서 지리적으로 산재되어 있다. 서로 같은 또는 서로 다른 두 가지의 network 을 연결하기 위한 조건이 있다. 두 network 간의 Routing 을 internetworking 이라 한다.

Networks 은 Protocol, topology, Layer-2 network and addressing scheme 와 같은 다양한 parameters 에 따라 서로 다른 것으로 여겨진다.

internetworking 에서, 라우터는 서로의 주소에 대한 지식을 가지고 있다. 이것들은 정적으로 다른 network 으로 가도록 콘피거되거나 internetworking routing protocol 을 사용하여 파악할 수 있다.



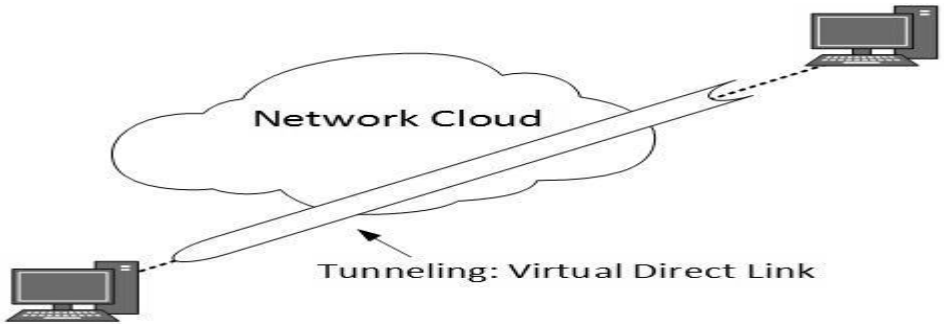
Routing

기관이나 행정기관 내에서 사용하는 Routing protocols 을 Interior Gateway Protocols 또는 IGP 하며, OSPF 는 IGP 의 한 예이다. 서로 다른 기관 간의 Routing 에서는 Exterior Gateway Protocol 을 사용할 수도 있으며, 단지 하나만의 EGP 인 Border Gateway Protocol 을 사용하여야 다.

1) Tunneling

지리적으로 떨어져 있는 두 개의 network 이 있다면, 이들 간에 전용선을 깔거나, 중개 network 을 통해 데이터를 전달하여야 한다.

Tunneling 이란 intermediate networking complexities 를 패싱하여 두 개 이상의 동일한 network 이 서로 통신하는 메카니즘이다. Tunneling 은 양쪽 끝에 콘피거 된다.



Tunneling

데이터가 터널의 한 끝으로부터 들어올 때, 그것은 tagged 된다. 이런 tagged data 는 그 다음에 the intermediate 내로 라우터되거나 터널 반대 끝에 전달하도록 network 에 전송한다. 데이터가 터널에 존재할 때, 그 태그는 제거되어 network 의 상대쪽으로 전달된다.

양쪽 끝은 직접적으로 연결된 것처럼 여겨지며, 태깅은 변경없이 transit network 로 전달되도록 한다.

2) Packet Fragmentation

대부분의 Ethernet 세그먼트는 1500 바이트에 고정된 자신들의 maximum transmission unit (MTU)를 가지고 있다. data packet 은 applications 에 따라 packets 길이가 크기도 하고 작기도 한다. Transit path 에 있는 기기들은 자신들의 hardware and software capabilities 을 가지고 있으며, 이것들은 데이터의 처리양과 처리할 수 있는 packets 의 크기를 결정한다.

data packet size 가 transit network 가 처리할 수 있는 크기보다 작거나 같다면, 중립적으로 처리된다. packets 가 크다면, 작은 조각으로 분해한 다음에 포워드 한다. 이러한 것을 packet fragmentation 이라 부르며, 각 fragment 에는 동일한 목적지와 소스 address 가 들어있어 transit path 를 통해 쉽게 전달된다. 접수 끝 단계에서 이것은 다시 모인다.

만일 packet with DF (do not fragment) bit set to 1 가 그 packets 를 다룰 수 없는 라우터에 들어온다면, 그것은 dropped 된다.

라우터에 의해 수집된 packets 가 its MF (more fragments) bit set to 1 를 가질 때, 그 라우터는 그것이 fragmented packet 이며 초기 packets 의 일부라는 것을 알게 된다.

만일 packets 가 너무 작게 fragmented 된다면, overhead 가 늘어난다. 만일 그 packets 가 너무 크게 쪼개진다면, intermediate router 는 그것에 접근할 수 없으므로 dropped 될 수도 있다.

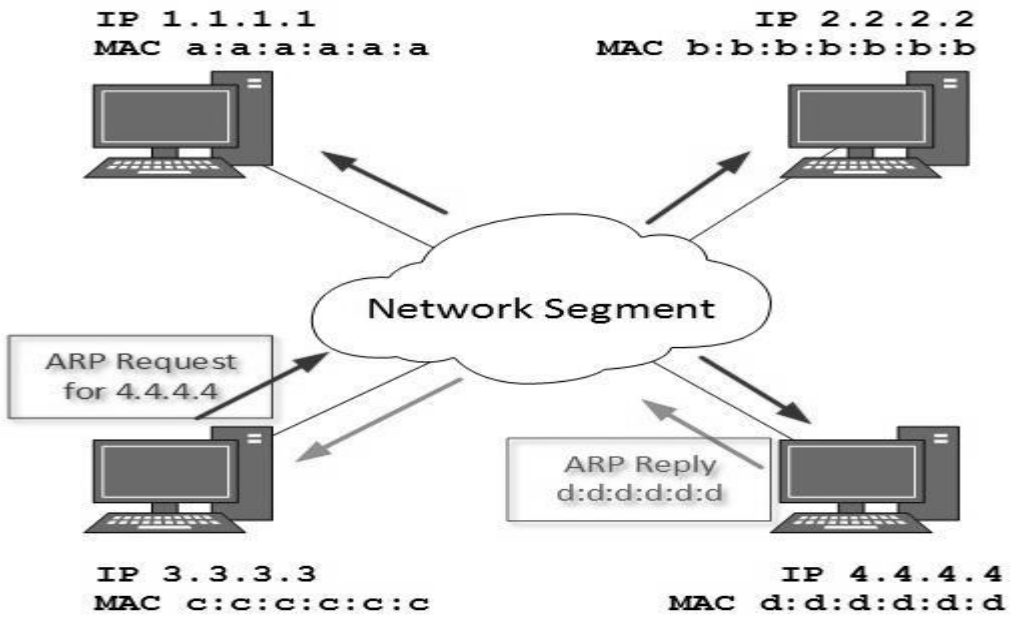
21. NETWORK LAYER PROTOCOLS

network 상의 모든 computer 들은 유일하게 식별하여 address 할 수 있는 IP address 를 가지고 있다. IP address 란 Layer-3 (Network Layer) logical address 이다. 이 address 는 computer 가 재가동될 때마다 바뀔 수 있다. computer 는 한 타임에 하나의 IP 를, 그리고 다른 타임에는 다른 IP 를 갖는다.

1) Address Resolution Protocol (ARP)

통신하는 동안, 호스트는 동일한 브로드캐스트 도메인이나 network 에 속해 있는 목적지 computer 의 Layer-2 (MAC) address 가 필요하다. MAC address 는 물리적으로 computer 의 Network Interface Card (NIC)에서 사용(burnt) 되며, 결코 변하지 않는다.

또 한편으로, 공적 도메인상의 IP address 는 드물지만 변한다. 만일 NIC 가 어떤 잘못으로 변한다면, 그 MAC address 역시 변한다. 이러한 방식으로 Layer-2 communication 이 이루어지기 때문에, 양자간의 mapping 이 필요하다.



ARP Mechanism

broadcast domain 에 있는 원격 호스트의 MAC address 를 알기 위하여, 통신을 시작하려는 computer 는 " Who has this IP address?" 라고 물으면서 ARP broadcast message 보낸다. 그것이 브로드캐스트이기 때문에, network segment (broadcast domain)에 있는 모든

호스트들은 이 packets 를 받아 처리한다. ARP packet 에는 destination host 의 IP address 를 포함하고 있으며, 송신 쪽 호스트는 이야기 걸길 원한다. 호스트가 자신을 목적으로 한 ARP packets 를 접수할 때, 자신의 MAC address 와 함께 보내면서 응답한다.

일단 호스트가 destination MAC address 을 얻으면, Layer-2 link protocol 을 사용하여 원격 호스트와 통신할 수 있다. IP mapping 을 위한 이 MACs 은 송수신 호스트 양쪽 모두의 ARP cache 에 저장되어, 다음에 만일 통신이 필요하다면, 직접적으로 자신들 각자의 ARP cache 를 참조한다.

Reverse ARP 란 호스트가 원격 호스트의 MAC address 를 알지만, 통신을 위해 IP address 를 요구하는 메커니즘이다.

2) Internet Control Message Protocol (ICMP)

ICMP 는 network diagnostic and error reporting protocol 이다. ICMP 는 IP protocol suite 에 속하며, carrier protocol 로 IP 를 사용한다. ICMP packet 이 만들어진 다음에, 그것은 IP packet 속에 봉해진다. IP 자체가 a best-effort non-reliable protocol 이기 때문에, ICMP 역시 마찬가지다.

network 에서 어떤 feedback 은 시작한 host 로 다시 보내진다. network 에 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 가 ICMP-echo request 를 접수할 때, ICMP-echo-reply 를 되돌려 보낸다. transit network 에 어떤 문제가 있다면, ICMP 이 그 문제를 보고할 것이다.

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 network 을 서브 network 으로 나눌 수 있고, 이들 각각은 well-defined number of hosts 를 가지고 있다. IP addresses 는 다양한 카테고리로 세분된다:

. Class A: 첫번째 옥텟은 network addresses 용이고 마지막 3 개의 옥텟은 host

addressing 용으로 사용한다.

!!Note:

옥텟(octet)은 컴퓨팅에서 8 개의 비트가 한데 모인 것을 말한다. 초기 컴퓨터들은 1 바이트가 꼭 8 비트만을 의미하지 않았으므로, 8 비트를 명확하게 정의하기 위해 옥텟 이라는 용어가 필요 했던 것이다. 그러나 요즘에는 바이트하고 같은 의미가 되었다.

. Class B: 처음 두개의 옥텟은 network addresses 용이고 마지막 두개은 host addressing 용으로 사용한다.

. Class C: 처음 세개의 옥텟은 network addresses 용이고 마지막 한 개는 host addressing 용으로 사용한다.

. Class D: 위의 3 클라스에서 계층구조를 사용하는 반면에 이것은 flat IP addressing 을 제공한다.

. Class E: 시험용으로 사용한다.

IPv4 또한 잘 정의된 address 스페이스를 가지고 있어서 private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet)에서 사용될 수 있다. 비록 IP 를 신뢰하지 못하더라도, 그것은 'Best-Effort-Delivery' mechanism 을 제공한다.

4) Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses 이 차세대 Protocol version 6 를 탄생시켰다. IPv6 는 미래를 위해 풍부한 address 를 제공하기 위하여, 128-bit 폭의 node 를 address 한다.

IPv6 에서 Anycast addressing 을 도입하면서, broadcasting 의 개념은 제거하였다. IPv6 는 기기들이 스스로 IPv6 address 를 얻어서 서브 network 과 통신하도록 함으로써, auto-configuration Dynamic Host Configuration Protocol (DHCP) servers 의 의존성을 무력화 시킨다. 따라서, 비록 서브 network 의 DHCP server 가 다운되더라도, 호스트끼리는 서로 통신할 수 있다.

IPv6 의 새로운 기능은 IPv6 mobility 이다. Mobile IPv6-equipped machines 는 자신들의 IP address 를 바꿀 필요 없이 돌아다닌다.

IPv6 는 아직까지 transition phase 에 있으며, 조만간 IPv4 를 완벽하게 대체할 것으로 기대되고 있다. 현재, 극소수 network 만이 IPv6 로 운영되고 있다. IPv6-enabled networks용으로 이용할 수 있는 어떤 transition mechanisms은 IPv4에서도 쉽게 서로 다른 network에 말하고 돌아다닐 수 있다. 이러한 것들은 다음과 같다:

. Dual stack implementation:

Dual-stack IP implementations provide complete IPv4 and IPv6 protocol stacks in the same network node on top of the common physical layer implementation, such as Ethernet. This permits dual-stack hosts to participate in IPv6 and IPv4 networks simultaneously. The method is defined in RFC(Request for Comment) 4213.

.Tunneling:

a tunneling protocol allows a network user to access or provide a network service that the underlying network does not support or provide directly. One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol; for example, running IPv6 over IPv4.

.NAT-PT:

Network Address Translation/Protocol Translation (NAT-PT) is defined in RFC 2766 but due to numerous problems, it has been obsoleted by RFC 4966 and deprecated to historic status. It is typically used in conjunction with a DNS application-level gateway (DNS-ALG) implementation.

.NAPT-PT:

While almost identical to NAT-PT, Network Address Port Translation + Protocol Translation which is also described in RFC 2766 adds translation of the ports as well as the address. This is done primarily to avoid two hosts on one side of the mechanism from using the same exposed port on the other side of the mechanism, which could cause application instability and/or security flaws. This mechanism has been deprecated by RFC 4966.

22. TRANSPORT LAYER INTRODUCTION

OSI Model 의 다음 layer 는 Transport Layer (Layer-4)이다. data or data stream 의 운반에 관한 모든 모듈과 프로시져는 이 layer 에서 범주화 된다. 모든 다른 layer 처럼, 이 layer 도 원격 호스트의 동료 Transport layer 와 교신한다.

Transport layer 는 원격 호스트의 두 프로세서들 간에 peer-to-peer 와 end-to-end connection 을 제공한다. Transport layer 는 상위 layer(i.e. Application layer)로 부터 데이터를 취하여, 그것을 보다 작은 크기의 세그먼트로 쪼갠 다음, 각 바이트별로 번호를 매긴 후, 하위 layer(Network Layer)로 전달한다.

1) Functions

. 이 Layer 는 가장 먼저 Application layer 에서 공급된 정보데이터를 세그먼트라고 하는 보다 작은 유니트로 쪼갠다. 그런 다음에 세그먼트에 있는 모든 바이트에 번호를 붙이며 이것들의 accounting 을 유지관리 한다.

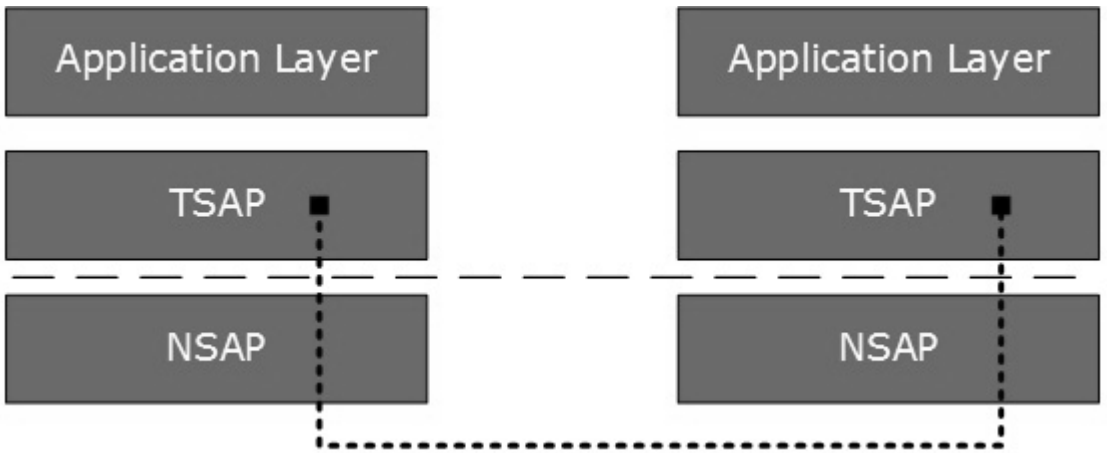
. 이 layer 는 데이터가 보낸 것과 똑 같은 순서로 접수되도록 보장한다.

. 이 layer 는 똑 같은 서브 network 에 속해있든 아니든 호스트 간의 데이터를 end-to-end 방식으로 전달한다.

. network 에서 통신하려는 모든 서버 프로세스는 잘 알려져 있는 Transport Service Access Points (TSAPs), 또는 port numbers 를 갖고 있어야 한다.

2) End-to-End Communication

한 호스트의 프로세스는 Port numbers 로 알려진 TSAPs 에 의존하여 원격 network 의 동료 호스트를 식별한다. TSAPs 는 매우 잘 정의되어 있으므로, 동료와 통신하려는 프로세스는 이미 이것에 대해 알고 있다.



예를 들어, DHCP(Differentiated Services Code Point) client 가 원격 DHCP server 와 통신하고자 할 때, 그것은 항상 port number 67 에서 리퀘스트를 보낸다. 또한 DNS(Domain Name System) client 가 원격 DNS server 와 통신하고자 할 때, 그것은 항상 port number 53 (UDP)에서 리퀘스트를 보낸다.

!!Note:

Differentiated services or DiffServ is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks

두 개의 주요한 Transport layer protocols 은 다음과 같다:

. TCP(Transmission Control Protocol):

두 호스트 간에 신뢰할 수 있는 통신을 제공한다.

. UDP(User Datagram Protocol):

두 호스트간에 신뢰할 수 없는 통신을 제공한다.

23. TRANSMISSION CONTROL PROTOCOL

Transmission Control Protocol (TCP)/Internet Protocols suite 에서 가장 중요한 protocol 들 중의 하나이다. internet 처럼, 통신 network 에서 데이터 전송용으로 가장 널리 사용되는 protocol 이다.

1) Features

.TCP 는 신뢰할 수 있는 protocol 이다. 즉, receiver 는 항상 데이터 packets 에 대하여 sender 에게 positive or negative acknowledgement 를 보낸다. 그렇게 함으로써 sender 는 항상 데이터 packets 가 목적지에 도달했는지 또는 다시 보내야 하는지에 대한 분명한 단서를 얻게 된다.

.TCP 는 보낼 때와 똑 같은 순서로 원하는 목적지에 도착했는지를 확인한다.

.TCP 는 connection oriented 이다. TCP 는 두 개의 원격 포인트들이 실재의 데이터가 보내지기 전에 연결이 설치될 것을 요구한다.

.TCP 는 error-checking and recovery mechanism 을 제공한다.

.TCP 는 end-to-end communication 을 제공한다.

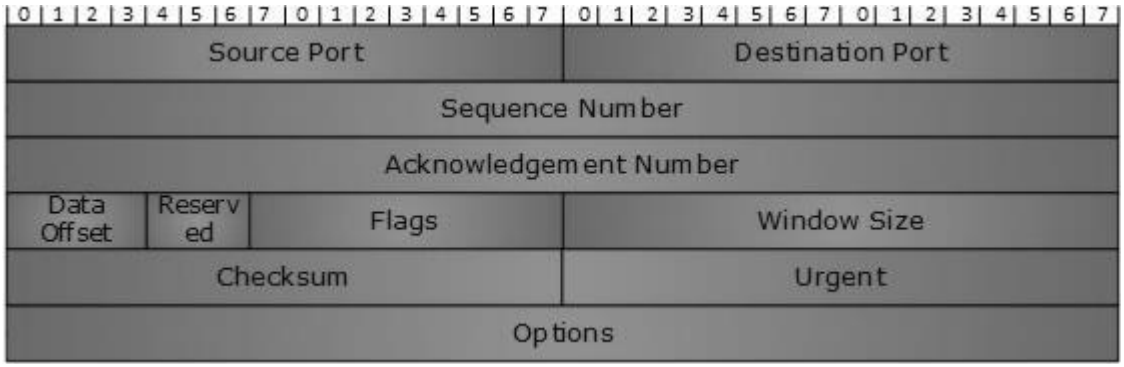
.TCP 는 flow control and quality of service 를 제공한다.

.TCP 는 Client/Server point-to-point mode 에서 운영된다.

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

2) Header 의 구성

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



TCP Header

. Source Port (16-bits): 송신용 디바이스에 있는 applications 프로세서의 source port 를 식별한다.

. Destination Port (16-bits): 수신용 디바이스에 있는 applications 프로세서의 destination port 를 규명한다.

. Sequence Number (32-bits): session 에 있는 세그먼트의 데이터 바이트에 붙여진 sequence number.

. Acknowledgement Number (32-bits): ACK flag 가 설정될 때, 이 번호에 다음 순번으로 예상되는 데이터 바이트가 포함됨으로써, 접수이전의 데이터에 대한 acknowledgement 로 사용된다.

. Data Offset (4-bits): 이 필드는 TCP header (32-bit words)의 사이즈와 전체 TCP segment 에서 현재의 packets 에 있는 데이터의 offset 둘 다를 의미한다.

. Reserved (3-bits): 미래용으로 예약되어 있으며 초기값은 0 으로 세트되어 있다.

. Flags (1-bit each):

> NS: Nonce Sum bit is used by Explicit Congestion Notification signaling process.

> CWR: When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.

> ECE: It has two meanings:

. If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.

. If SYN bit is set to 1, ECE means that the device is ECT capable.

> URG: It indicates that Urgent Pointer field has significant data and should be processed.

> ACK: It indicates that Acknowledgement field has significance. If ACK is

cleared to 0, it indicates that packet does not contain any acknowledgement.

> PSH: When set, it is a request to the receiving station to PUSH data as soon as it comes to the receiving application without buffering it.

> RST: Reset flag has the following features:

. It is used to refuse an incoming connection.

. It is used to reject a segment.

. It is used to restart a connection.

> SYN: This flag is used to set up a connection between hosts.

> FIN: This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

. Windows Size: 이 필드는 two stations 간의 flow control 용으로 사용되며, receiver 가 세그먼트용으로 할당한 버퍼(bytes)의 크기를 나타낸다. 즉, receiver 가 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 communication 은 port numbers (TSAPs)에 의해 이루어진다. Ports numbers 는 0 에서부터 65535 까지 이며, 다음과 같이 나눈다:

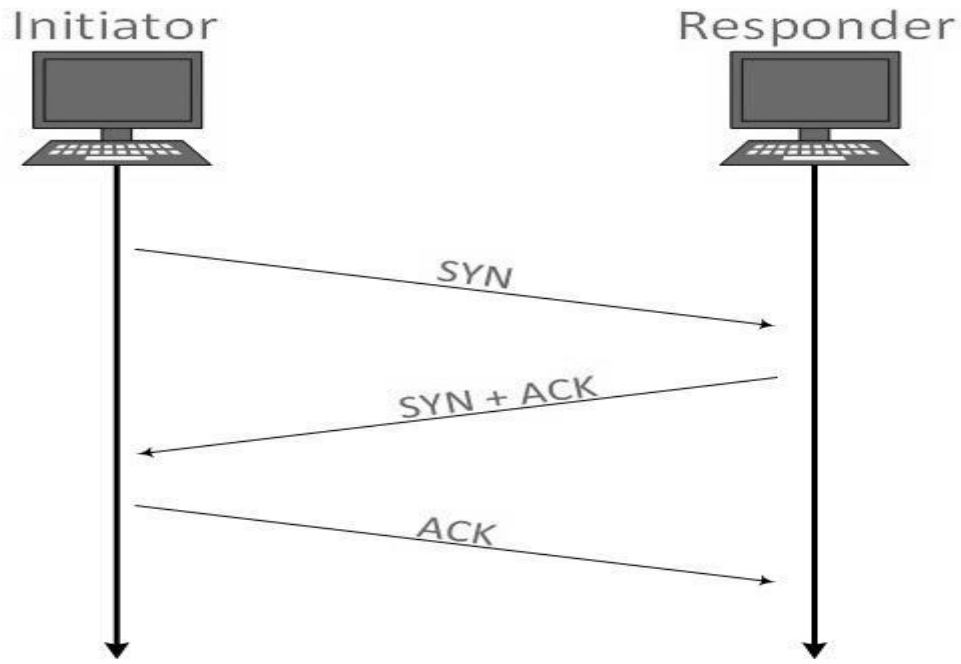
. System Ports (0 에서 1023)

. User Ports (1024 에서 49151)

. Private/Dynamic Ports (49152 에서 65535)

4) Connection Management

TCP communication 은 Server/Client model 에서 이루어진다. Client 가 connection 을 시작하고, 서버는 그것을 접수하거나 거절한다. connection management 를 위해 three-way handshaking 기법이 사용된다.



TCP Handshake

(4-1) Establishment

Client 가 connection 을 시작하고 segment 를 Sequence number 와 같이 보낸다. Server 는 클라이언트의 Sequence number 보다 한 개 더 많은 자신의 Sequence number 와 클라이언트 세그먼트의 ACK 를 되돌려 보내는 것을 확인한다(acknowledges). 세그먼트의 ACK 가 접수되면, Client 는 서버의 응답에 대한 확인(acknowledgement)을 보낸다.

(4-2) Release

server 나 client 에서 1 로 설정된 FIN flag 와 함께 TCP 세그먼트를 보낼 수 있다. 수신 쪽에서 FIN 을 ACKnowledging 하여 반응할 때, TCP communication 의 direction 은 closed 되고 connection 은 released 된다.

5) Bandwidth Management

TCP 는 Bandwidth management 의 요구를 수용하기 위하여 window size 의 개념을 이용한다. Window size 란 원격 sender 에게 receiver 가 받을 data byte segments 의 수를 알려주는 것을 말한다. 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 사용하면 2 bytes of data 를 보낸다. 이 세그먼트에 대한 인정이 접수될 때 윈도우사이즈는 2 의 곱인 4 가 될 것이며, 그 다음에 보내는 세그먼트의 길이는 4 data bytes 가 될 것이다. 4-byte data segment 의 인정이 접수될 때, 클라이언트는 windows size 를 8 로 설정한다.

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

6) Error Control and Flow Control

TCP 는 port numbers 를 사용하여 어떤 applications 프로세스가 데이터 세그먼트를 양도하는데 필요한지를 안다. 따라서 이것은 순번을 이용하여 원격 호스트와 자신을 동기화 시킨다. 모든 데이터 세그먼트는 순번과 함께 송수신된다. sender 는 ACK 가 접수될 때 receiver 가 접수한 마지막 데이터 세그먼트를 알게 되며, receiver 는 최근에 접수된 packets 의 순번을 참고하여 sender 가 보낸 마지막 세그먼트에 대해 알게 된다.

최근에 접수된 세그먼트의 순번이 receiver 가 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 applications 과 통신할 수 있다. 예를 들어, 클라이언트가 다양한 종류의 데이터(HTTP, SMTP, FTP etc.)를 포함하고 있는 web page 를 요청하면, TCP session timeout 이 증가하여 그 세션이 보다 오랫동안 열리게 되는데, 왜냐하면 three-way handshake overhead 를 피하려 하기 때문이다.

이것은 클라이언트 시스템으로 하여금 하나의 가상 연결로 복수의 연결을 가능하도록 한다. 이러한 가상 연결의 timeout 이 너무 길면 길수록 서버의 부담은 늘어난다.

8) Congestion Control

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

. Additive Increase, Multiplicative Decrease:

additive-increase/multiplicative-decrease (AIMD) algorithm is a feedback control algorithm best known for its use in TCP congestion control. AIMD combines linear growth of the congestion window with an exponential reduction when a congestion takes place. Multiple flows using AIMD congestion control will eventually converge to use equal amounts of a contended link. The related schemes of multiplicative-increase/multiplicative-decrease (MIMD) and additive-increase/additive-decrease (AIAD) do not converge.

. Slow Start

Slow-start is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting, that is, to avoid causing network congestion(밀집, 정체)

. Timeout React

9) Timer Management

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

(9-1) 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.

(9-2) 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.

(9-3) 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.

(9-4) 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 protocol 이다. 이것은 세그먼트로 보내진 각각의 바이트에 순번을 정해준다. 그리고 이것은 feedback mechanism 을 제공한다. 다시 말해서, 호스트가 packets 를 받을 때, 그것이 마지막 세그먼트가 아니라면, 다음 순번의 packets 가 접수될 거라는 ACK(확신)을 갖는다.

TCP Server 가 통신 중간에 crashes 하여 그 과정이 다시 시작될 때, 그것은 모든 호스트에 TPDU(Transport Protocol Data Unit) broadcast 를 보낸다. 호스트들은 그러면 결코 NACK 가 되지 않는 마지막 데이터 세그먼트를 보낸 다음, 계속 진행한다.

24. USER DATAGRAM PROTOCOL

User Datagram Protocol (UDP) 는 가장 간단한 Transport Layer communication protocol 이며, TCP/IP protocol suite 에 속한다. 이것에는 최소량의 communication mechanism 이 포함되어 있다. UDP 는 믿을 수 없는 운송 protocol 이라고 말하지만, 최상의 결과를 전달하는 메커니즘을 제공하는 IP services 에서 주로 사용한다.

UDP 에서, receiver 는 접수된 packets 의 인정을 생산하지 않으며, 반대로 sender 는 보낸 packets 의 어떠한 인정도 기다리지 않는다. 이러한 단점이 이 protocol 을 신뢰하지 못하게 만들었지만, 프로세싱은 보다 쉬워졌다.

1) Requirement of UDP

한 가지 의문이 생긴다. 왜 데이터를 전송하는데 신뢰할 수 없는 protocol 이 필요한가? 우리는 사실 acknowledgement packets 에 수반되는 상당한 양의 bandwidth 를 공유하는 UDP 를 사용하고 있다. 예를 들어, video streaming 경우에, 수 천 개의 packets 가 이용자에게 포워드 된다. 모든 packets 를 인정하는 것은 문제가 있으며 거대한 양의 bandwidth wastage 가 발생한다. IP protocol 의 전달 메커니즘이 그런 packets 를 전달하는데 최상이라는 것이 보장됨으로써, 비록 비디오 스트림의 packets 에 손상이 발생하더라도 그 충격이 재앙적이지는 않기 때문에, 이러한 손상을 쉽게 무시할 수 있다. 따라서 video and voice traffic 에서 약간의 packets 손실은 때때로 무시되기도 한다.

2) Features

. UDP 는 데이터의 확인이 중요하지 않는 경우에 사용된다.

. UDP 는 한 방향으로 흐르는 데이터에는 훌륭한 프로토콜이다.

. UDP 는 쿼리의존형 통신용으로는 간단하고 적합하다.

. UDP 는 connection oriented 가 아니다.

. UDP 는 congestion control mechanism 을 제공하지 않는다.

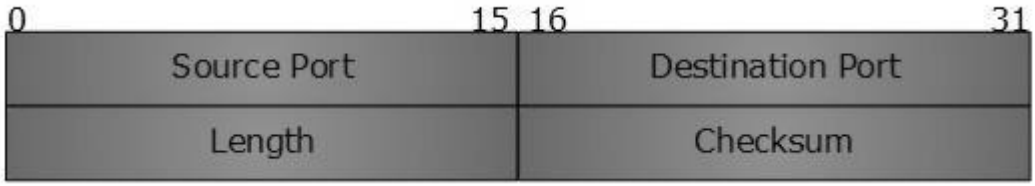
. UDP 는 정해진 순서로 데이터를 전달하지 않는다.

. UDP 는 stateless 하다.

. UDP 는 VoIP, multimedia streaming 과 같은 streaming applications 용으로는 적합한 프로토콜이다.

3) UDP Header

UDP header 는 기능이 간단하다:



UDP Header

UDP header 는 4 가지의 중요한 parameters 가 있다:

. Source Port: 16 bits information 이며 패키트의 소스 포트를 밝히는데 사용된다.

. Destination Port: 16 bits information 이며 목적지 기계에서 application level service 를 밝히는데 사용된다.

. Length: Length field 는 UDP packet (including header)의 전체 길이를 지정한다. 이것은 16-bits field 이며, 최소값은 8-byte, 즉, UDP header 그 자체의 사이즈는 8-byte 이다.

. Checksum: 이 필드에는 송신 전에 송신자가 생산한 checksum value 이 저장되어 있다. IPv4 에서 이 필드는 선택적이며, 이 필드가 어떠한 값도 갖고 있지 않을 땐, 그것은 0 으로 처리되므로, 모든 그것의 비트들은 0 으로 설정된다.

4) UDP application

UDP 를 데이터 전송에서 사용하는 몇 가지의 applications 이 있다:

. Domain Name Services

Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

. Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more

. Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) is a simple lockstep File Transfer Protocol which allows a client to get a file from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a local area network. TFTP has been used for this application because it is very simple to implement.

. Routing Information Protocol

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.

. Kerberos:

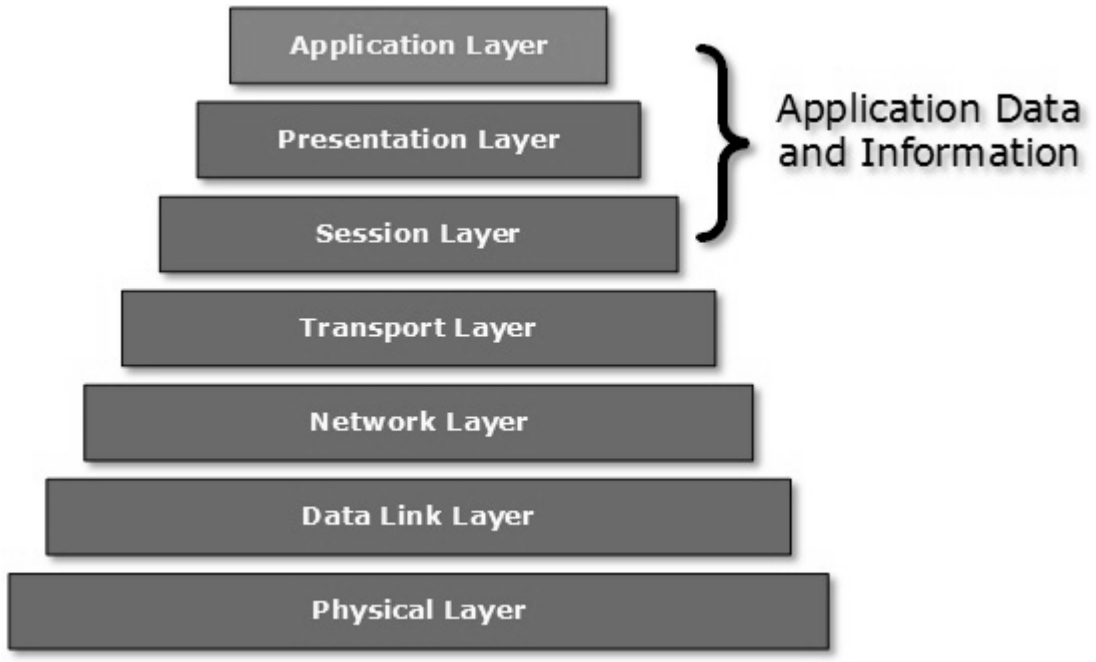
Kerberos /ˈkərbərɒs/ is a computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. The protocol was named after the character Kerberos (or Cerberus) from Greek mythology, the ferocious three-headed guard dog of Hades.

25. APPLICATION LAYER INTRODUCTION

Application layer 는 OSI 와 TCP/IP layered model 의 맨 꼭대기에 있다. 이 layer 는 양 쪽 모두의 layer 모델에 존재하는데, 왜냐하면 매우 중요하기 때문이다. 다시 말해서, 이것은 이용자와 이용자 applications 간의 상호작용을 위해 존재한다. 이 layer 는 통신 시스템의 applications 을 위한 것이다.

user 는 applications 과 직접 상호작용할 수도 있고 안 할 수도 있다. Application layer 는 실재로 통신이 시작되고 이루어지는 곳이다. 이 layer 가 맨 꼭대기에 있기 때문에, 어떤 다른 layer 에 도움을 주지 못한다. Application layer 는 원격 호스트에 데이터를 전송하거나 통신하기 위하여 Transport 와 그것의 밑에 있는 모든 layer 로부터 도움을 받는다.

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



Application Layer

Application Layer 와 그것의 프로토콜을 이해하는 것은 쉽지 않다. 이 applications 들이 통신시스템과 상호작용하는 applications 인 경우를 제외하고는 모든 이용자 applications 을

Application Layer 에 포함시키진 않는다. 예를 들어, designing software 나 text-editor 는 application layer programs 으로 간주되지 않는다.

그렇지만, network 과 상호작용하기 위하여 실재적으로 Hyper Text Transfer Protocol (HTTP)를 사용하는 웹 브라우저를 사용할 때, HTTP 는 Application Layer protocol 이다.

또 다른 예는 File Transfer Protocol 인데 이것은 network 으로 text based 또는 binary files 을 전송하는데 도움을 준다. 이용자는 FileZilla 나 CuteFTP 와 같은 GUI 의존형 소프트웨어용으로 이 protocol 을 사용할 수 있으며, Command Line mode 에서도 FTP 를 사용할 수 있다.

그러므로 우리가 사용하는 소프트웨어와는 관계없이, 이것은 위와 같은 소프트웨어를 사용하는 Application Layer 에서 고려할 protocol 이다. DNS 도 protocol 이며, 이것은 HTTP 와 같은 이용자 applications protocol 이 자신의 일을 완수하도록 돕는 protocol 이다.

26. CLIENT-SERVER MODEL

두 가지의 원격 applications 프로세서는 대부분이 2 가지의 서로 다른 모습으로 통신할 수 있다:

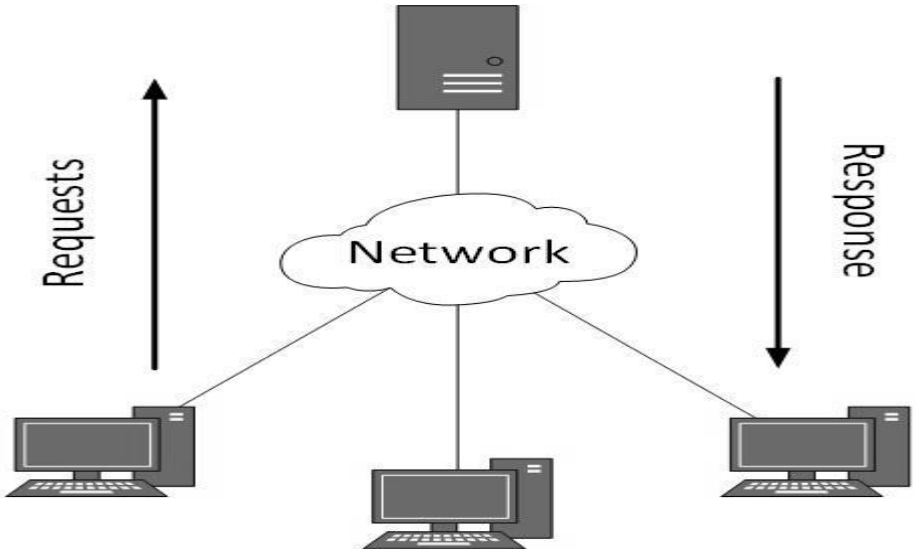
. Peer-to-peer:

양쪽의 원격 프로세스들이 동일한 수진에서 수행되며 이것들은 어떤 공유 자원을 사용하여 데이터를 교환한다.

. Client-Server:

한 개의 원격 프로세서가 클라이언트로 활동하며, 서버로 활동하는 또다른 어플리케이션 프로세서에 어떤 자원을 요청한다.

client-server model 에서, 어떤 프로세서는 Server 또는 Client 처럼 행동한다. 이 프로세서는 컴퓨터의 종류, 컴퓨터의 크기, 또는 그것을 서버로 만드는 컴퓨팅 파워에 의존하지 않는다. 또한 이것은 컴퓨터를 서버로 만드는 요청을 처리하는 능력을 갖고 있다.



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

시스템은 동시에 Server and Client 로 활동한다. 즉, 한 프로세스는 서버로, 나머지는 클라이언트로 활동한다. 이것은 동일한 컴퓨터에 클라이언트와 서버 프로세서가 공존(reside)할 때 발생하기도 한다.

1) Communication

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

. Sockets:

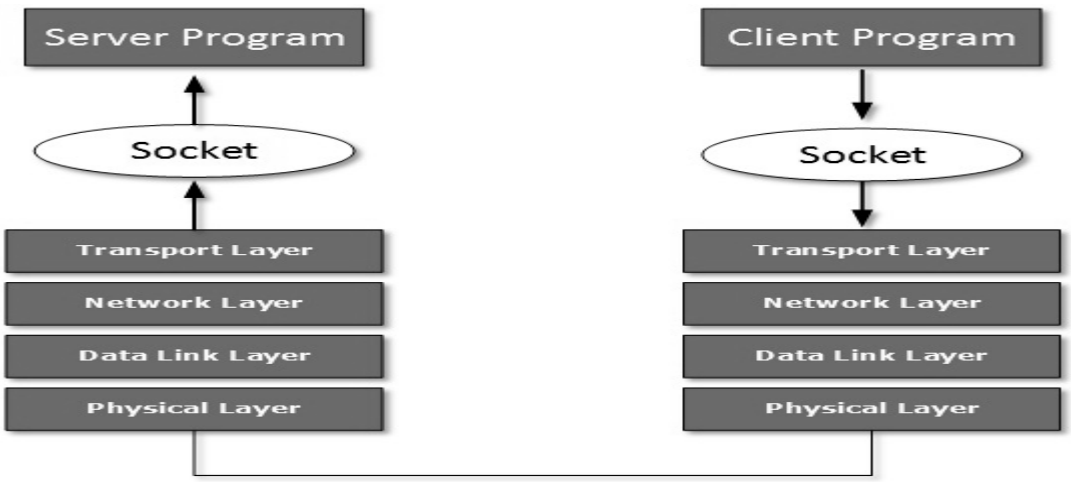
an internal endpoint for sending or receiving data within a node on a computer network.

. Remote Procedure Calls (RPC)

when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (local) procedure call, without the programmer explicitly coding the details for the remote interaction. That is, the programmer writes essentially the same code whether the subroutine is local to the executing program, or remote.

(1-1) Sockets

이 파라다임에서, 서버로 활동하는 프로세스는 이미 잘 알려 있거나 또는 클라이언트에 의해 알려진 포트를 사용하여 socket 을 연 다음에, 어떤 클라이언트 리퀘스트가 올 때까지 기다린다. 클라이언트로 활동하는 두 번째 프로세스 역시 socket 를 열지만, 리퀘스트를 기다리는 것이 아니라, 우선적으로 리퀘스트를 처리한다.



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

information sharing 이거나 resource request 일 수 있는 request 가 서버에 도달하면, 그것은 처리된다.

(1-2) Remote Procedure Call

이것은 한 메커니즘이 procedure calls 에 의해 다른 프로세스와 상호작용하는 메카니즘이다. One process (client)는 원격 호스트에 있는 procedure 를 부른다. 원격 호스트의 process 를 서버라 한다. 양 쪽 프로세스들은 stubs 을 할당한다. 이런 통신은 다음과 같은 방식으로 일어난다:

. client process 가 client stub 를 불러서, 그 곳에 있는 모든 프로그램과 관련된 파라미터를 전달한다.

. 그러면 모든 parameters 가 packed(marshalled) 되고 시스템 콜이 network 의 반대쪽으로 그것을 보낸다.

. Kernel 이 network 전체에 해당 data 를 보내면, 반대쪽에선 받는다.

. 원격 호스트가 unmarshalled 된 server stub 에 데이터를 전달한다.

. parameters 가 procedure 에 전달되고 procedure 가 수행된다..

. result 가 동일한 방법으로 다시 클라이언트에 보내진다.

27. APPLICATION PROTOCOLS

Application Layer 에서 이용자용인 여러 개의 protocol 이 있으며, Application layer protocols 은 크게 두 개의 범주로 나눌 수 있다:

. 이용자가 사용하는 Protocols. For example, eMail.

. 이용자가 사용하는 프로토콜을 지원하는 Protocols. For example, DNS.

Application layer protocols 을 살펴보면, 다음과 같다:

1) Domain Name System

Domain Name System (DNS)는 Client Server model 에서 활동한다. 이것은 transport layer communication 을 위한 UDP protocol 을 사용한다. 그리고 DNS 는 계층적 도메인을 의존하는 naming scheme 을 사용한다. DNS server 는 각각의 IP address 로 mapped 된 Fully Qualified Domain Names (FQDN)과 email addresses 로 구성되어 있다.

A DNS server 는 FQDN 을 리퀘스트하며, 그것에 mapped 된 IP address 와 함께 다시 반응한다. DNS 는 UDP port 53 을 사용한다.

2) Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP)은 서로 전자 메일을 전달하는데 사용된다. 이러한 일은 이용자가 사용하는 email client software (User Agents)에 의해 이루어진다. User Agent 는 이용자가 이메일을 작성하고 포맷하는 것을 도우며 인터넷을 이용할 수 있을 때까지 그것을 저장한다. 이메일을 보낼 때, 그것의 송신과정은 일반적으로 email client software 에 내장되어 있는 Message Transfer Agent 에서 다룬다.

Message Transfer Agent 는 uses SMTP 를 사용하여 또 다른 Message Transfer Agent (Server side)에 이메일을 보낸다. 단지 이메일을 보내기 위해서 최종이용자에 의해 SMTP 가 사용될 때, 그 서버들은 일반적으로 SMTP 를 사용하여 이메일을 송수신한다. SMTP 는 TCP port number 25 과 587 을 사용한다.

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

3) File Transfer Protocol

File Transfer Protocol (FTP) 는 network 으로 파일을 전송하는데 가장 널리 사용되는 protocol 이다. FTP 는 통신용인 TCP/IP 를 사용하며, TCP port 21 에서 작동한다. FTP 는 Client/Server Model 에서 작동한다

FTP 는 out-of-band controlling 을 사용한다. 다시 말해서, FTP 는 통제용 정보를 교환할 때는 TCP port 20 을, 그리고 실재적인 데이터를 보낼 TCP port 21 을 사용한다.

클라이언트가 서버에 파일을 요청한다. 그러면 서버는 파일용 리퀘스트를 받았을 때, 그것은 클라이언트와 TCP connection 을 열어서 해당 파일을 전송한다. 전송이 끝나면, 서버는 그 연결을 폐쇄한다. 두 번째 파일이 있다면, 클라이언트는 다시 리퀘스트하고 서버는 새로운 TCP connection 을 다시 연다.

4) Post Office Protocol (POP)

Post Office Protocol version 3 (POP3)은 메일 서버로부터 메일을 검색하기 위하여 User Agents (client email software)가 사용하는 간단한 **메일 검색 protocol** 이다.

클라이언트가 서버에서 온 메일들을 검색하고자 할 때, 이것은 TCP port 110 으로 서버와의 연결을 연다. 이용자는 그런 다음에 자신의 메일에 접근하여 그것들을 자신의 컴퓨터에 다운로드 받는다. POP3 는 두 가지 모드에서 작동한다. 가장 일반적인 모드인 삭제모드(delete mode)는 원격 서버로부터 온 이메일을 다운로드가 끝나면 삭제한다. 두 번째 모드는 보관모드(keep mode)는 메일서버에서 온 이메일을 삭제하지 않고 이용자가 나중에 메일서버에 있는 메일들에 접근할 수 있는 선택권을 제공한다.

5) Hyper Text Transfer Protocol (HTTP)

Hyper Text Transfer Protocol (HTTP)는 World Wide Web 의 기본이다. Hypertext 는 잘 짜여져 있는 문서 시스템으로 텍스트 다큐멘트에 있는 페이지를 링크시키는 hyperlink 를 사용한다. HTTP 는 client server model 에서 사용된다. 이용자가 인터넷에 있는 어떤 HTTP 페이지에 접근하고자 할 때, 이용자쪽에 있는 클라이언트 기계는 port 80 으로 서버와의 TCP connection 을 시작한다. 서버가 클라이언트의 리퀘스트를 접수하면, 클라이언트는 웹페이지에 접근할 수 있는 권한을 얻는다.

웹 페이지에 접근하기 위하여, 클라이언트는 일반적으로 웹 브라우저를 사용하는데 이것은 TCP conncetion 을 시작하고, 관리하고, 폐쇄하는 책임을 가지고 있다. HTTP 는 stateless

프로토콜인데, stateless 란 서버가 클라이언트가 이미 요청한 리퀘스트와 관련된 어떠한 정보도 갖고 있지 않다는 의미이다.

28. NETWORK SERVICES

Computer systems 과 computerized systems 은 인간을 도와서 효율적으로 일을 하면서 생각할 수 없는 것을 탐험하도록 한다. 이러한 기기들이 network 을 형성하도록 서로 연결될 때, 그 능력은 몇 배가 증가한다. computer network 에서 제공할 수 있는 몇 가지 기본적인 서비스는 다음과 같다:

1) Directory Services

이런 서비스들은 이름과 가변적일 수도 있고 고정적일 수도 있는 그것의 가치를 반영하고 있다. 이런 소프트웨어 시스템은 정보를 저장하고 조직하며 그것에 접근하는 다양한 수단을 제공하고 있다.

(1-1) Accounting

기관마다, 많은 이용자들은 자신의 사용자 이름과 그에 상응하는 패스워드를 가지고 있다. Directory Services 에서는 이러한 정보를 암호형태로 저장하여 필요할 때 이용할 수 있는 수단을 제공하고 있다.

(1-2) Authentication and Authorization

User credentials 은 로그인할 때나 정기적으로 이용자의 신분을 확인하기 위하여 체크하여야 한다. User accounts 은 계층적인 구조로 설정될 수 있으며, 자원에 접근하기 위해서는 이용자 계정이 접근권한규칙(authorization schemes) 에 의해 통제될 수 있어야 한다.

2) Domain Name Services

DNS 는 인터넷에서 작업하는 필수적인 서비스들 중잉 하나이며 널리 사용되고 있다. 이 시스템은 IP address 와 domain names 를 연결시키므로, IP address 보다 기억하고 회상하기가 쉽다. 네트워크가 IP address 의 도움을 받아 운영되고 사람들이 웹 사이트의 이름을 기억하려고 하기 때문에, DNS 는 이용자의 웹사이트 이름에 대한 리퀘스트를 맨 뒤에서부터 그것의 이름과 결부된(mapped) 웹사이트의 IP address 를 제공한다.

3) File Services

File services 에는 네트워크에서 파일을 공유하고 전달하는 것이 포함된다.

(3-1) File Sharing

네트워크가 탄생하게 된 이용중의 하나가 바로 file sharing 이다. 이것은 이용자가 자신의 데이터를 다른 사람과 공유할 수 있도록 한다. 이용자는 특별한 서버에 파일을 업로드하여 모든 관심대상의 이용자가 접근할 수 있도록 한다. 하나의 대안으로, 이용자는 자신의 컴퓨터에서 파일을 공유하도록 만듬으로서 의도된 이용자로 하여금 접근할 수 있도록 한다.

(3-2) File Transfer

이것은 파일을 네트워크의 도움을 받아 한 컴퓨터에서 다른 컴퓨터로 또는 다수의 컴퓨터로 파일을 복사하거나 이동시키는 행동이다. 네트워크는 이용자로 하여금 인터넷에서 다른 이용자의 소재지를 파악하여 파일을 전달할 수 있게 한다.

4) Communication Services

(4-1) 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.

(4-2) 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.

(4-3) 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.

(4-4) 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.

(4-5) 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.

5) Application Services

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

(5-1) Resource Sharing

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

(5-2) 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.

(5-3) 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.

FIN