<용어 정리집> - 시스템, 네트워크

<네트워크, 시스템 (Linux & Windows Server) 개념 및 용어 정리>

🔎 LAN, MAN, WAN
LAN(Local Area Network, 근거리 통신망)
한정된 공간에서의 연결
회사에서 사용하는 업무환경 LAN

MAN(Metropolitan area network)
도시권 통신망은 큰 도시 또는 캠퍼스에 퍼져 있는 컴퓨터 네트워크이다. LAN과 WAN의 중간 크기를 갖는다. DSL 전화망, 케이블 TV 네트워크를 통한 인터넷 서비스 제공이 대표적인 예이다.

WAN(Wide Area Network, 원거리 통신망)
=LAN + LAN + LAN++++
LAN이 여러개 모이면 WAN
WAN = Internet service
전 세계 어디서든 접속 가능한 네트워크 환경

🔎 Unicast, Multicast, Broadcast
Unicast
1:1 통신, 카카오톡, 기타 메신저 등 1:1 채팅, 한방향 통신
내가 통신하고자 하는 대상을 정해서 그 대상과 통신하는 것
Multicast
1:N 통신, 카카오톡 단톡방, 기타 메신저 등 1:N 채팅
선택한 사람들끼리 하는 통신하는 것
Broadcast
1:all 통신, 라디오방송, 이장님방송, 아파트 관리실 방송
내 의지와 상관없이 무조건 들어야(받아들어야)하는 통신
주위에 있는 불특정 다수의 라우터에 통신을 보냄

ISP(Internet Service Provider)
인터넷 서비스 공급자로, 다양한 회선 상품을 제공하며 기업마다 서비스가 다름
KT, LG U+, SK broadband(SKB)가 대표적이다.

VPN(Virtual Private Network)
가상사설망, ISP 즉 제 3자에 정보를 넘겨주지 않고 익명성을 유지하여 인터넷에 접속
익명성이 보장된 상태에서 안전하게 인터넷을 사용할 수 있는 기술

IP(Internet Protocol) Address
컴퓨터 네트워크에서 기기들이 서로를 인식하고 통신하기 위해 사용하는 식별번호

네트워크로 연결된 모든 장비들은 각각 고유의 IP주소를 가지고 있음

IP 클래스 종류
1) IP : 네트워크로 데이터를 전달하는 프로토콜, 인터넷 주소 결정
2) A클래스 : 1.0.0.0 ~ 126.255.255.255 (국가나 대형 네트워크)
3) B클래스 : 128.0.0.0 ~ 191.255.255.255 (중대형 네트워크)
4) C클래스 : 192.0.0.0 ~ 223.255.255.255 (소형 네트워크)
5) D클래스 : 224.0.0.0 ~ 239.255.255.255 (IP 멀티캐스트에 이용)
6) E클래스 : 240.0.0.0 ~ 255.255.255.255 (연구용, 일반PC 설정불가)

IPv6
1) IPv6 : IP 주소 부족을 해결하기 위한 IP 주소체계
2) 표기법 : 128비트 체계의 16진수로 표기한다. 4개의 16진수를 콜론(:)으로 구분

공인 IP/ 사설 IP
공인 IP: External/Public IP, 공유기를 거치기 전
사설 IP: Internal/Privacy IP, 공유기를 거치고 난 이후
내 의도가 반영된 IP = 사설 IP(NAT)

NAT [Network Address Translation]
한정된 하나의 공인IP를 여러개의 내부 사설 IP로 변환하여 공인 IP를 절약하고, 외부 침입에 대한 보안성을 높이기 위한 기술입니다. 인터넷선에 할당되어 있는 하나의 IP를 여러 명이 사용하기 위해 사용됩니다. 내부 사설 IP를 사용함 으로서 보안성이 향상되고 장비에 연결된 PC 관리가 쉽다.

NAT의 A, B, C Class 대역
- Class A 규모 : 10.0.0.0 ~ 10.255.255.255 (10.0.0.0/8)
- Class B 규모 : 172.16.0.0 ~ 172.31.255.255 (172.16.0.0/12)
- Class C 규모 : 192.168.0.0 ~ 192.168.255.255 (192.168.0.0/16)

옥텟 : . 단위로 IP를 구분하는 것(IP주소는 4개의 옥텟으로 구성되어 있음)

서브넷 마스크, 라우팅
서브넷 마스크
1) 서브넷 마스크 : IP 주소의 공간낭비를 해결하기 위한 개념
2) 할당방법 : 맨 왼쪽 비트부터 연속된 1이 표시된 부분까지 네트워크 파트, 그 외에는 호스트 파트
3) 기본 서브넷 마스크 : 서브넷이 없는 경우 기본적으로 적용하는 서브넷 마스크

와일드 마스크
– 서브넷 마스크와 구분하기 위해서 '0'과 '1'을 반대로 사용한다.

– 맨 앞에 비트부터 '1'과 '0'이 불연속이 가능한 32bit 체계 마스크
– 서브넷 마스크와 달리 앞에서부터 '1'이 연속되어야 하는 규칙이 없음
– EIGRP, OSPF, ACL 사용

라우팅
데이터 패킷을 전송하기 위한 경로를 설정하는 것

라우팅 종류
1) 정적 라우팅 : 목적지까지의 경로가 고정되어 있음, 수동으로 매핑 필요
2) 동적 라우팅 : 목적지까지의 경로가 상황에 따라 변경, 트래픽에 따라 자동으로 변경

라우팅 프로토콜
패킷을 목적지까지 전송하기 위한 경로를 설정, 제어하는 프로토콜

라우팅 프로토콜 종류
1) RIP (Round Information Protocol) : 라우터 홉수(최대 15홉)에 따라 최단거리를 결정하는 프로토콜
2) BGP (Border Gateway Protocol) : AS사이에 사용되는 EGP 라우팅 프로토콜, 거리벡터 라우팅을 사용
3) IGP vs EGP : IGP는 내부경로를 설정, EGP는 외부경로를 설정
4) AS (Autonomous System) : 동일한 내부라우팅, 보안정책을 사용하는 망의 집합
5) OSPF : 목적지 거리를 라우터의 연결속도로 계산

DHCP (Dynamic Host Configuration Protocol)
관리자가 수동으로 IP주소를 입력하지 않고 클라이언트에 자동으로 제공하는 프로토콜, IP 주소의 추적이 가능하다.

Cable
컴퓨터와 네트워크 장비들 사이에서 전기적 신호를 운반하는 전송매체
UTP(Unshielded Twisted Pair) Cable = LAN선 = 인터넷선
현업에서 많이 사용하는 UTP Category 5(100Mbps)~6(1Gbps)
Cat 숫자 차이는 회선의 대역폭(도로의 차선)

▶ L2 스위치 : 스위칭 허브 기능

데이터링크 계층에 위치하여 서로 다른 데이터링크간을 스위치해주는 장비
패킷의 MAC 주소를 읽어 스위칭을 하고, MAC이 OSI 계층 중 2 계층에 해당하기 때문에 Layer 2 스위치라 한다.
기본적인 동작은 브리지나 스위칭 허브는 모든 자료를 보내는 곳으로 수신 번지를 전송한다.
장점 : 구조가 간단하며, 신뢰성이 높다. / 가격이 저렴하고, 성능이 높다.

단점 : Broadcast 패킷에 의해 성능 저하가 발생한다. - 라우팅이 불가능 / 상위 레이어 프로토콜을 이용한 스위칭이 불가능 하다.

▶ L3 스위치 : 라우터 기능
네트워크 계층에 위치하여 서로 다른 네트워크간을 연결해 주는 장비
(즉, 데이터의 네트워크 주소를 보고 스위칭해주는 장비)
해당 프로토콜을 쓰는 패킷을 스위칭이 가능하며, IP나 IPX 주소가 OSI 7 계층 중 3 계층에 해당하기 때문에 Layer 3 스위치라 한다.
L2 스위치에 라우팅(Routing) 기능을 추가하고, 대부분의 고성능 하드웨어를 기초로 하였다. - 기본 구성은 L2와 동일
장점 : Broadcast 트래픽으로 전체 성능 저하를 막을 수 있다. / 트래픽 체크, 가상 랜 등의 많은 부가 기능을 갖고 있다.
단점 : 특정 프로토콜을 이용해야 스위칭을 할 수 있다. / 대부분의 트래팩이 서브텟의 한계를 넘는다.

▶ L4 스위치 : 라우터 기능
L3과 같이 프로토콜을 기반으로 하며, 어플리케이션별로 우선 순위를 두어 스위칭이 가능하다.
여러대의 서버를 1대처럼 묶을 수 있는 부하 분산 (Load Balancing) 기능을 제공한다.
웹 트래픽, FTP 트래픽과 같이 정해진 서비스 포트를 보고 트래픽을 스위칭해주는 장비
장점 : 보안성이 높고 고급 스위칭 설정이 가능하다. - 상황에 적절한 설정 / 용량에 관계 없이 네트워크의 성능 개선에 기여한다.
단점 : 프로토콜에 의존적이며, 설정이 복잡하다. / 고가의 장비로 L2,L3 스위치와 적절한 혼합 배치가 필요하다.

Load Balancing, 로드 밸런싱(부하분산)
1개의 서버나 방화벽, 네트워크 등에 트래픽이 집중되는 것을 분산시키기 위한 스위칭 기술
과부하 방지 및 네트워크 속도 향상, 장애 허용, 고가용성 등을 이룰 수 있다.

OSI 7 Layers

OSI 7 계층

계층	이름	단위(PDU)	예시	프로토콜(Protocols)	디바이스 (Device)
7	응용 계층 (Application Layer)	Data	텔넷(Telnet), 구글 크롬, 이메일, 데이터베이스 관리	HTTP, SMTP, SSH, FTP, Telnet, DNS, modbus, SIP, AFP, APPC, MAP	
6	표현 계층 (Presentation Layer)	Data	인코딩, 디코딩, 암호화, 복호화	ASCII, MPEG, JPEG, MIDI, EBCDIC, XDR, AFP, PAP	
5	세션 계층 (Session Layer)	Data		NetBIOS, SAP, SDP, PIPO, SSL, TLS, NWLink, ASP, ADSP, ZIP, DLC	
4	전송 계층 (Transport Layer)	TCP-Segment, UDP-datagram	특정 방화벽 및 프록시 서버	TCP, UDP, SPX, SCTP, NetBEUI, RTP, ATP, NBP, AEP, OSPF	게이트웨이
3	네트워크 계층 (Network Layer)	Packet	라우터	IP, IPX, IPsec, ICMP, ARP, NetBEUI, RIP, BGP, DDP, PLP	라우터
2	데이터링크 계층 (DataLink Layer)	Frame	MAC 주소, 브리지 및 스위치	Ethernet, Token Ring, AppleTalk, PPP, ATM, MAC, HDLC, FDDI, LLC, ALOHA	브릿지, 스위치
1	물리 계층 (Physical Layer)	Bit	전압, 허브, 네트워크 어댑터, 중계기 및 케이블 사양, 신호 변경(디지털,아날로그)	10BASE-T, 100BASE-TX, ISDN, wired, wireless, RS-232, DSL, Twinax	허브, 리피터

ARP(Address Resolution Protocol)

IP 주소를 통해 MAC 주소를 알아오기 위해 사용하는 통신 방법

Router(라우터)
네트워크에서 통신을 위한 데이터를 목적지 까지 전달하기 위한 장치
데이터를 전달하기 위해서 IP주소를 활용하게 됨

Switch(스위치)
네트워크에서 통신을 위한 데이터를 목적지 까지 전달하기 위한 장치
데이터를 전달하기 위해 MAC 주소를 활용하게 됨

WWW(World Wide Web. W3)
네트워크에 연결된 컴퓨터들을 통해 사람들이 정보를 공유할 수 있는 전 세계적인 정보 공간. 간단히 Web이라 부름

Interface
유형 또는 무형의 장치 간에 연결하고 통신하기 위한 접속장치

Internet
네트워크와 네트워크를 연결하여 하나의 통신망 안에 연결하고자 하는 의미로 Inter + Network를 줄여서 Internet이라고 함

MAC Address(Media Access Control Address)
IP주소처럼 네트워크에서 Host장비를 식별하기 위한 주소로 사용이 됨
하지만 MAC Address주소의 경우 NIC에 고정적으로 부여된 주소로 변경이 불가능 함

NIC(Network Interface Card)
네트워크에 연결하기 위해서 사용하는 인터페이스 장치

Port
Device 장치 간에 연결을 위해서 사용하는 연결단.(USB Port, LAN Port)
TCP/UDP에서 상위 계층과의 연결을 위해서 사용하는 주소

DHCP(Dynamic Host Configuration Protocol)
IP주소를 자동으로 할당할 수 있게 하는 프로토콜

Telnet
표준 원격 접속 프로토콜
텔넷은 원격 터미널 연결을 위해서 사용되며 이것을 이용하면 사용자들이 원격 시스템으로 로그인해 시스템 리소스를 마치 로컬 시스템에 연결되어 있는 것과 같이 사용가능 함

SSH이란?

시큐어 셸(Secure SHell, SSH)은 네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 응용 프로그램 또는 그 프로토콜을 가리킨다. 즉, 네트워크 프로토콜 중 하나로 컴퓨터와 컴퓨터가 인터넷과 같은 Public Network를 통해서 서로 통신을 할 때 보안적으로 안전하게 통신을 하기 위해 사용하는 프로토콜이다.
대표적인 사용 : 데이터 전송, 원격 제어

사용이유 :
보안때문에 FTP나 Telnet과 같은 다른 컴퓨터 통신을 사용하지 않는다.
SSH는 보안적으로 훨씬 안전한 채널을 구성한 뒤 정보를 교환하기 때문에 보다 보안적인 면에서 뛰어나다.
어떤 방식으로 서로 다른 컴퓨터가 안전하게 통신하게 하는가?

Public Key and Private Key(공개키와 개인키)
SSH는 다른 컴퓨터와 통신할 때 일반적으로 사용하는 비밀번호 입력을 통한 접속을 하지 않는다.
기본적으로 SSH는 한 쌍의 Key를 통해 접속하려는 컴퓨터와 인증 과정을 거친다.
이 한 쌍의 Key는 다음과 같다.

Public Key : 단어 뜻 그대로 공개되어도 비교적 안전한 Key.
이 키를 통해 메세지를 전송하기 전 암호화를 한다.
암호화는 가능하지만 복호화는 불가능하다.

Private Key : 절대로 외부에 노출되어서는 안되는 Key. 본인의 컴퓨터 내부에 저장하게 되어있다.
암호화된 메세지를 복호화 할 수 있다.

복호화란?
암호화 : 어떤 데이터를 암호화 해서 직접 그 의미를 알지 못하도록 하는 작업
복호화 : 암호화된 데이터를 해독하는 것

FTP [File Transfer Protocol]
FTP는 인터넷을 통한 파일 송수신 만을 위해 고안된 서비스(또는 프로토콜)이기 때문에 동작 방식이 대단히 단순하고 직관적이다. 그런 만큼 사용법도 간단하다. 무엇보다 WWW 방식보다 파일을 빠른 속도로 한꺼번에 주고 받을 수 있다는 것이 FTP의 가장 큰 장점이다.

잘 알려진 포트(Well-Known Port)
FTP(20(전송), 21(제어)) - TCP, SSH(22) - TCP, Telnet(23) - TCP, SMTP(25) - TCP
DNS(53) - TCP/UDP, HTTP(80) - TCP, POP3(110) - TCP, IMAP(143) - TCP, HTTPS(443) - TCP

ICMP(Internet Control Message Protocol)

인터넷 제어 메시지 프로토콜로 신뢰성이 없는 IP를 보조하기 위해 사용, 네트워크의 연결성을 확인하고 오류를 보고받기 위해 사용되는 네트워크 계층 인터넷 프로토콜

IGMP(Internet Group Management Protocol)
인터넷 그룹 관리를 위한 프로토콜, IP호스트가 멀티캐스트 그룹 멤버십을 인접 멀티캐스트 Router로 보내는데 사용됨

PPP(Point-too-Point Protocol)
동기식 또는 비 동기식 회선을 통해 router-to-router또는 host-to-network 연결방식을 제공하는 프로토콜

Frame-relay
가상회선 기반의 패킷 교환 서비스로 하나의 물리회선으로 여러 개의 논리적인 채널을 지원하는 기술

Port number
OSI의 4계층 전송 계층의 주소로 소프트웨어적인 입출력 인터페이스

Packet
OSI 3계층에서 테이터를 부르는 단위 (Datagram이라고도 함), 패킷은 네트워크 계층 데이터 단위를 언급할 때에 자주 사용되는 언어임

CSMA/CD(Carrier Sense Multiple Access/Collision Detection)
정보 송출에 앞서서 회선의 사용 유무를 조사하여 보내는 방식으로 충돌 감지 시송선을 멈추고 일정한 수에 재송하는 방식

HUB
전기신호를 증폭시켜 전달하는 1계층의 대표 장비, 이더넷 네트워크에서 여러 대의 컴퓨터, 네트워크 장비를 연결하는 장치

Bridge
동일한 프로토콜을 사용하는 LAN과 LAN을 연결하는 2계층 통신 장비

IOS(Internetwork Operating System)
CISCO 사에서 장비를 구동하기 위해 제공하는 운영체계

Routing
출발지부터 목적지까지 패킷을 전달하기 위한 일련의 과정

Static
네트워크 관리자가 패킷의 경로를 직접 선택하여 입력하는 것

Dynamic
Router가 프로토콜들을 이용하여 자동으로 경로를 학습 하는 것

Ethernet
이더넷의 2계층 데이터 송수신을 위해 사용되는 정해진 규격

Mac-address-table
Layer2 전송장비인 스위치가 각 장치들이 연결된 위치를 기억하기 위해 각 장치들의 고유한 MAC주소와 PORT 번호를 함께 묶어서 기록해 놓은 표

TCP 3-way Handshake 란?
TCP는 장치들 사이에 논리적인 접속을 성립(establish)하기 위하여 three-way handshake를 사용한다.
TCP 3 Way Handshake는 TCP/IP프로토콜을 이용해서 통신을 하는 응용프로그램이 데이터를 전송하기 전에 먼저 정확한 전송을 보장하기 위해 상대방 컴퓨터와 사전에 세션을 수립하는 과정을 의미한다.

트러블 슈팅(troubleshooting)
문제 해결의 일종으로, 망가진 제품, 또는 기계 시스템의 망가진 프로세스를 수리하는 일에 주로 적용된다. 문제 해결을 위해 문제의 원인을 논리적이고 체계적으로 찾는 일이며 제품이나 프로세스의 운영을 재개할 수 있게 한다. 트러블슈팅은 증상 식별에 필수적이다.

NAS(Network Attached Storage)
네트워크 결합 스토리지. 쉽게 말하면 LAN으로 연결하는 외장 하드디스크. 반대 개념은 컴퓨터에 직접 연결해서 쓰는 DAS(직접 결합 저장장치, Direct Attached Storage)로, 내장형 하드디스크나 eSATA 규격 외장 하드디스크가 여기에 해당된다.

컴퓨터에 직접 연결하지 않고 네트워크를 통해 데이터를 주고 받는 저장장치이다.
개인이 용도에 따라 맞춤형으로 구축할 수 있다.

<NAS 장점과 단점>
장점
간편한 데이터 공유, 저장장치를 가지고 다닐 필요가 없다, 다양한 용도(NAS의 원래 목적은 파일 서버의 목적인 데이터의 공유였다. 하지만 지금은 성능과 소프트웨어가 개선되어 기능이 계속해서 늘어나 영상 스트리밍, 트랜스코딩 스트리밍, 토렌트, 데이터 백업, 채팅 봇, 음악 스트리밍, 가상머신, 이메일 서버, CCTV DVR, 웹페이지 호스팅 등 용도가 다양해지는 상황이다.), 저렴한 유지비, 독립적인 개인 저장소

단점
네트워크 연결은 필수, 성능의 한계, 인터넷 요금제에 따른 속도 제한, 설정의 복잡함, 관리의 어

려움, 보안

파일시스템
파일에 구별을 위한 이름을 붙이고, 어디에 위치시킬 것인지 결정하는 것

OS별 파일시스템
1) 윈도우 : FAT16, FAT32, NTFS
2) 리눅스 : EXT2, EXT3, raiserFS

NTFS (NT File System)
윈도우의 기본설정 파일 시스템, FAT에서 불가능한 일부 디스크 관련 오류를 자동으로 복구해준다. (파일 시스템 장애는 FAT에 비해 복구가 어렵다)

FAT (File Allocation Table)
윈도우 NT4에서 사용할 수 있는 가장 단순한 파일 시스템, 호환성이 우수하다. (FAT에서 NTFS 변환은 가능하지만 역은 불가능)

Active Directory
1) Active Directory : 시스템에서 원하는 개체를 관리하고 찾기위한 도구, 관련 정보를 저장하고 있는 일종의 데이터베이스 역할
2) 구성요소 : 도메인, 조직단위(OU), 도메인 트리, 포리스트, 글로벌 카탈로그, 도메인 컨트롤러, 사이트

프로비저닝(Provisioning) 이란?
기 설치된 시설을 활용하여 이용자의 요구에 따라 서비스를 개통/해지/유지/관리 등 서비스 구성을 위한 일련의 활동을 말함(서비스의 유지 보수 등을 의미)

Ansible (앤서블)은 여러 개의 서버를 효율적으로 관리할 수 있게 해주는 환경 구성 자동화 도구

도커(docker):

도커는 컨테이너 기반의 오픈소스 가상화 플랫폼입니다.
다양한 프로그램, 실행환경을 컨테이너로 추상화하고 동일한 인터페이스를 제공하여 프로그램의 배포 및 관리를 단순하게 해줍니다. 백엔드 프로그램, 데이터베이스 서버, 메시지 큐등 어떤 프로그램도 컨테이너로 추상화할 수 있고 조립PC, AWS, Azure, Google cloud등 어디에서든 실행할 수 있습니다.

on-premise(온프레미스):

-on-premise란 소프트웨어 등 솔루션을 클라우드 같이 원격 환경이 아닌 자체적으로 보유한 전산실 서버에 직접 설치해 운영하는 방식을 말합니다.

-온프레미스는 클라우드 컴퓨팅 기술이 나오기 전까지 기업 인프라 구축의 일반적인 방식이었기

때문에 이전 또는 전통적인 이라는 단어와 함께 사용됩니다.

-일반적으로 온프레미스 시스템을 구축하는데 시간이 수개월 이상 걸렸고 비용 또한 많이 들어, 퍼블릭 클라우드가 나올 당시만 해도 온프레미스 환경이 금방이라도 모두 사라질 것 같았습니다.

-하지만 보안 적인 이유로 비즈니스에 중요하고 보안이 필요한 서비스와 데이터는 온프레미스 환경에서, 덜 중요한 것은 퍼블릭 클라우드 환경을 사용하는 하이브리드 IT 인프라가 대세를 이루고 있습니다.

DevOps의 의미
DevOps는 Development와 Operations의 합성어이며, 기존의 개발 업무와 운영 업무로 나뉘어진 두 역할 사이의 커뮤니케이션, 협업, 통합을 강조하는 개념이다.

IaaS
Infrastructue as a Service
사용자는 OS를 직접 올리고 사용할 수 있다. 클라우드에서는 하드웨어와 물리적인 장치, 네트워크 환경을 제공해준다.

PaaS
Platform as a Service
사용자가 어플리케이션만 개발하고 서비스 가능. 사용자는 소스코드만 적어서 빌드하고, 컴파일은 클라우드에서 하여 결과만 가져오는 것. 관리가 매우 편리함. 플랫폼간의 이동이 어려울 수 있다.

SaaS
Software as a Service
소비 관점에서 제공되는 IT방식의 서비스. 구독 방식이나 트래픽 기반으로 돈을 번다. 데이터 노출의 위험이 있다.

클라우드란?
클라우드 컴퓨팅이란 인터넷 기반의 컴퓨팅을 말합니다. 인터넷 상의 가상화된 서버에 프로그램을 두고 필요할때마다 컴퓨터나 스마트폰 등에 불러와 사용하는 서비스입니다.

장점
웹서비스 운영자 입장에서 클라우드를 바라본다면 다음과 같은 장점이 있습니다.

서버를 직접 구매할 때 고려해야 할 전력, 위치, 확장성을 고민하지 않고
데이터 센터 어딘가에 이미 준비되어 있는 서버를 사용하며,
서버 세팅 등을 신경쓰지 않고 서비스 운영에만 집중 가능

퍼블릭 클라우드(Public Cloud, 공공 클라우드, 개방형 클라우드)

특정 기업이나 사용자를 위한 서비스가 아닌 인터넷에 접속 가능한 모든 사용자를 위한 클라우드 서비스 모델입니다. 클라우드 서비스 제공자(CSP)가 하드웨어, 소프트웨어를 관리합니다. 데이터나 기능, 서버 같은 자원은 각 서비스에서 사용자 별로 권한 관리가 되거나 격리 되어, 서비스 사용자 간에는 전혀 간섭이 없다는 장점이 있습니다.

간혹, 공공기관이 도입하는 공공 클라우드와 퍼블릭 클라우드의 공공 클라우드를 혼동하는 케이스가 있습니다. 공공기관이 도입하는 공공 클라우드는 Government Cloud, 공용 인터넷망에 연결된 공공 클라우드는 Public Cloud입니다.

프라이빗 클라우드(Private Cloud, 사설 클라우드, 폐쇄 클라우드)
제한된 네트워크 상에서 특정 기업이나 특정 사용자만을 대상으로 하는 클라우드로 서비스의 자원과 데이터는 기업 내부에 저장됩니다. 또한 기업이 자원의 제어권을 갖고 있습니다. 따라서 보안성이 매우 뛰어나며, 개별 고객의 상황에 맞게 클라우드 기능을 커스터마이징 할 수 있다는 장점이 있습니다.

하이브리드 클라우드(Hybrid Cloud)
하이브리드 클라우드는 퍼블릭 클라우드와 프라이빗 클라우드를 병행해 사용하는 방식으로 여겨져 왔으나, 최근에는 개념이 모호해진 경향이 있어 클라우드(가상서버)와 온프레미스(물리서버)를 결합한 형태를 말하기도 합니다. 이럴 경우 퍼블릭 클라우드의 유연성, 경제성, 신속성과 물리 서버의 보안성, 안정성 등을 함께 취할 수 있는 장점이 있습니다.

최근 클라우드를 도입하려는 움직임이 늘면서, 전체 워크로드를 클라우드(가상서버)로 이전하기보다 주요 데이터는 온프레미스(물리서버)에 남겨 두고 이벤트 또는 신규 서비스처럼 트래픽을 예측할 수 없는 워크로드는 클라우드로 이용하는 구성이 증가하는 추세입니다.

커널(Kernel)
운영체제의 핵심, 실행중 프로그램관리와 시스템에 대한 전반적인 자원을 관리하는 역할을 수행

쉘(Shell)
Hardware와 Kernel에 사용자가 직접 접근할 수 있는 방법이 없음- 쉘은 커널과 사용자 사이에서 사용자의 명령어를 해석하여 커널에 질의하고 결과를 사용자에게 해석해 주는 역할을 하게 됨.- 운영체제에 따라 기본쉘이 달라지는데 sh, csh, ksh, bash 등이 있음

퍼미션 및 소유권
일반적으로 유닉스 계열에서 파일과 자원에 대한 결정권은 오직 해당 객체의 사용자에게 할당된 권한에 의해 다뤄지게 됨- 퍼미션은 읽거나, 쓰거나, 실행 권한에 대한 행위를 말하며 해당 자원에 액세스 여부를 결정 하게 됨.- 소유권은 각 사용자로 하여금 접근 권한을 부여하기 위해 소유권을 부여하는데, 특정 파일에 대하여 소유자와 그룹소유자, 그리고 기타 사용자로 나눠지게 됨.

사용자
시스템에 접근하기 위해서는 계정과 접근시 인증받아야 할 패스워드가 있어야 함 - 이중 root사

용자는 슈퍼유저라고도 부르며 최고 권한을 갖고 있는 사용자임

VI Editor
유닉스 계열의 대표적인 파워풀한 텍스트 문자 편집기로서 대기모드, 편집모드, 명령모드의 세 가지 step으로 구성됨

Cron
Cron Daemon에 의해 사용자가 원하는 작업을 예약해 두고 정해진 시간에 주기적인 반복 수행할 수 있도록 함
/etc/cron.allow, cron.deny에 의해 일반사용자의 접근제어가 가능함.

리눅스 디렉토리- 물리적인 HDD를 특정 OS가 임의의 디렉토리인 마운트 포인트를 통하여 접근하여 사용할 수 있는 논리적인 공간을 의미함- OS마다 파일시스템의 유형은 다르며 리눅스계열의 파일시스템 포멧은 ext2, ext3, ext4 등이 있음

MOUNT
물리적인 파일시스템을 임의의 디렉토리인 마운트포인트를 이용하여 해당 파일시스템에 접근가능하도록 하는 일련의 행위

Quota
유닉스/리눅스를 사용하는 사용자들에게 일정 용량의 디스크 사용량을 지정함으로써 시스템 자원을 효율적으로 관리할 수 있게 해줌.

액티브 디렉터리 도메인 서비스 (AD DS)
네트워크상에 존재하는 사용자, 그룹, 컴퓨터 등의 개체들에 대한 정보를 저장하고 해당 정보를 사용자가 컴퓨터가 사용할 수 있도록 하는 기능.

도메인 (Domain)
사용자, 컴퓨터 계정을 모아 놓은 것
조직단위 (OU)
도메인 내에서 디렉터리의 형태로 사용자, 컴퓨터 계정 등을 하나의 단위에 포함하는 것.- 그룹 정책의 설정이나 관리 권한의 위임이 가능함.

포리스트 (Forest)
다양한 도메인이 계층적으로 연결된 구조

도메인 컨트롤러 (Domain Controller)
액티브 디렉터리 도메인 서비스가 설치되어 있는 컴퓨터
액티브 디렉터리와 관련된 정보를 가지고 있음.

권한

특정한 자원으로의 접근을 제어(허가 or 거부)하기 위해 사용함

ACL (Access Control List)
권한을 제어할 수 있는 항목의 리스트
ACE (Access Control Entry) 각각의 권한 하나 하나를 의미함
NTFS 권한 (Permission) 파일 및 폴더 등에 사용자, 그룹, 컴퓨터가 접근할 수 있는 권한을 말함.
사용자 권한 (User right)
사용자, 그룹, 컴퓨터가 시스템에 접근할 수 있는 권한

파티션 (Partition)
물리적인 디스크를 논리적인 여러 부분으로 분리하여 놓은 것

볼륨 (Volume)
하드 디스크의 저장할 수 있는 영역
하나의 하드디스크에 여러 개의 볼륨이 있을 수도 있고, 여러 개의 하드디스크에 하나의 불륨이 있을 수도 있음

DNS (Domain Name System)
컴퓨터 이름을 도메인 이름에 포함시켜 이용하는 방식
계층적인 구조를 가지며 각각의 이름은 (.)으로 구별됨

Root Hint
DNS 루트 서버의 IP 주소 정보를 저장하는 파일

DNS 영역
주 영역 : 레코드의 생성, 수정 삭제가 가능한 영역, 실질적으로 도메인 이름으로 서비스하는 영역

DHCP (Dynamic Host Configuration Protocol)
윈도 NT를 기본으로 하는 근거리망(LAN)에 접속하는 컴퓨터에 IP 주소를 할당하는 마이크로소프트사 기술- 컴퓨터가 네트워크에 접속하면 DHCP 서버가 자신의 목록에서 IP 주소를 선택하여 할당해주는 것을 말함

IPSEC (Internet Protocol Security Protocol)
암호화 통신을 위한 보안프로토콜의 모음

VPN (Vitual Private Network)
개인과 원격네트워크간 전용 터널을 제공하여 네트워크에 가상으로 참여하는 효과를 주는 방식
실제 망구성 비용이 절감되며, 재택근무, 출장시 유용하게 사용됨
터널을 구성하는 방식을 터널링 프로토콜이라 함

Tunneling
컴퓨터 네트워크 에서 터널링 프로토콜 은 캡슐화를 이용하여 한 네트워크에서 다른 네트워크로 데이터를 이동할 수 있는 통신 프로토콜로 게이트웨이 이중화에 주로 이용이 된다.

HSRP (Hot Standby Router Protocol)
내결함성 기본 게이트웨이 이중화를 설정하기 위한 Cisco 전용 프로토콜

GLBP(게이트웨이 로드 밸런싱 프로토콜)
기본 로드 밸런싱 기능 을 추가하여 기존 중복 라우터 프로토콜의 한계를 극복하려고 시도 하는 Cisco 독점 프로토콜 입니다.

VRRP (가상 라우터 중복 프로토콜)
여러 대의 라우터를 그룹으로 묶어 하나의 가상 IP주소를 부여하여, 마스터로 지정된 라우터에 장애 발생 시 VRRP그룹 내의 백업 라우터가 마스터로 자동 전환되는 라우터 프로토콜.
이에 따라 마스터 라우터의 장애로 인한 네트워크 서비스의 중단을 예방할 수 있다.

STP (Spanning Tree Protocol)
이더넷 네트워크 를 위한 루프 없는 논리적 토폴로지 를 구축하는 네트워크 프로토콜
Blocking, Listening, Learning, Forwarding, Disabled의 포트상태로 구성

루트 브리지와 브리지 ID
스패닝 트리 의 루트 브리지 는 가장 작은(가장 낮은) 브리지 ID를 가진 브리지입니다. 각 브리지에는 구성 가능한 우선 순위 번호와 MAC 주소가 있습니다. 브리지 ID는 브리지 우선 순위와 MAC 주소를 연결 한 것입니다. 예를 들어, 우선 순위가 32768이고 MAC 0200.0000.1111 인 브리지의 ID 는 32768.0200.0000.1111 입니다. 브리지 우선 순위 기본값은 32768이며 4096의 배수로만 구성할 수 있다.

루트 브리지 경로
가장 잘 수신된 BPDU(루트에 대한 최상의 경로)를 결정하기 위한 이벤트 시퀀스는 다음과 같습니다.

최저 루트 브리지 ID(BID) - 루트 브리지를 결정합니다.
루트 브리지에 대한 최저 비용 - 루트 비용이 가장 적은 업스트림 스위치를 선호합니다.
가장 낮은 발신자 브리지 ID - 여러 업스트림 스위치의 루트 비용이 동일한 경우 순위결정 역할을 합니다.
가장 낮은 발신자 포트 ID - 스위치에 단일 업스트림 스위치에 대한 다중(비 EtherChannel) 링크가 있는 경우 순위결정 역할을 합니다. 여기서:
브리지 ID = 우선 순위(4비트) + 로컬로 할당된 시스템 ID 확장(12비트) + ID [MAC 주소](48비트); 기본 브리지 우선 순위는 32768이고
포트 ID = 우선순위(4비트) + ID(인터페이스 번호)(12비트); 기본 포트 우선 순위는 128입니다.

EtherChannel
여러 물리적 이더넷 링크를 그룹화하여 스위치, 라우터 및 서버 간의 내결함성 및 고속 링크를 제공할 목적으로 하나의 논리적 이더넷 링크를 생성할 수 있습니다.
EtherChannel은 2~8개의 활성 고속, 기가비트 또는 10기가비트 이더넷 포트 에서 생성할 수 있으며 , 다른 활성 포트에 장애가 발생하면 1~8개의 비활성(장애 조치) 포트가 추가로 활성화됩니다.

Stub Network
하나의 네트워크에서 외부의 네트워크로 나가고 들어오는 경로가 오직 하나 뿐인 경우
즉, 외부에서 들어와 결국은 종료되는 네트워크를 말함

OSPF Stub Area
Backbone Area에 단 하나의 링크로만 접속되어 있는 고립된 영역

Stub Area 구분
- 일반 Stub Area
- Totally Stubby Area : 완전 스터브 영역. 시스코 장비에 한함
- NSSA(Not-So-Stubby-Area) : 변형된 특수한 스터브 영역

RAID
여러 개의 디스크를 하나로 묶어서 사용하는 방식
RAID란 Redundant Array of Independent Disks 혹은 Redundant Array of Inexpensive Disks의 약자로, 원래 목적은 저렴한 저용량의 디스크 여러 개를 하나의 비싼 대용량의 디스크로 사용하고자 하는 것이었습니다.
RAID는 구성 방식에 따라서 입출력 성능의 향상이나, 디스크 결함 허용(Fault Tolerance, 여러 개의 디스크 중에서 하나 또는 일부가 고장나도 데이터의 안전을 보장)의 특징을 갖게 할 수 있습니다.
RAID는 크게 하드웨어 RAID와 소프트웨어 RAID 두 가지로 나눌 수 있습니다.

단순 볼륨 - volume
단순 볼륨은 디스크 1개로 1개의 볼륨을 만듭니다. [그림 1]의 예에서 'ABCEDF'라는 데이터를 저장하면 그냥 해당 디스크에 데이터가 저장됩니다.

스팬 볼륨 - Spanned Volume: Linear RAID
스팬 볼륨은 2개 이상의 디스크로 1개의 볼륨을 만든 것입니다. [그림 1]에서 디스크별로 용량이 1TB라면, 스팬 볼륨의 용량은 2TB가 된다. 즉, 공간 효율이 100%가 되는 것이며, 이는 구성된 디스크 용량의 총합을 전부 사용한다는 의미도 됩니다. 저장되는 방식은 그림에서 보는 바와 같이 첫 번째 디스크에 데이터가 도무 꽉 찬 후에, 두 번째 디스크를 사용한다. [그림 1]의 예에서 'ABCEDF'를 저장하고 디스크가 꽉 찼다면, 두 번째 디스크에 'F'를 저장하는 방식입니다.

스트라이프 볼륨 - Striped Volume: RAID 0

스트라이프 볼륨은 2개 이상의 디스크로 1개의 볼륨을 만드는 것으로, 스팬 볼륨과 결과적으로는 동일하지만 내부적으로 저장되는 방식에는 차이가 있습니다. [그림 1]에서 보이듯이 'ABCDEF'를 저장할 때 A는 첫 번째, B는 두 번째 저장하는 방식입니다. 이렇게 저장하면 A와 B를 동시에 저장하기 때문에 디스크의 입출력 속도가 꽤 향상됩니다. 한 글자당 1초의 저장 시간이 걸린다고 가정하면, 단순 볼륨과 스팬 볼륨은 'ABCDEF'를 저장하는데 6초의 시간이 필요하지만 스트라이프 볼륨은 동시에 저장되는 방식으므로, 3초면 저장됩니다. 그래서 스트라이프 볼륨은 입출력 성능이 가장 뛰어난 방식으로 사용됩니다.

2개의 디스크를 스트라이프 볼륨으로 구성하면 이론적으로는 두 배 빨라져야 하지만, 여러 가지 요인에 의해서 2배가 빨라지지 않을 수는 있습니다. 하지만, 기존보다 입출력 성능이 월등히 좋아지는 것은 확실합니다.

스트라이프 볼륨은 성능은 우수하지만, 만약 두 개의 디스크 중 하나라도 고장 난다면 모든 데이터를 잃어버리게 됩니다. 또한 스트라이프 볼륨은 3개 이상으로도 구성이 가능합니다. 만약 10개의 디스크로 스트라이프 볼륨을 구성했다면 입출력 속도는 더더욱 좋아지겠지만, 10개의 디스크 중 1개라도 고장 나면 모든 데이터를 잃어버리는 위험성이 생깁니다. 그래서 이 볼륨 방식에 데이터를 저장하는 경우에는 데이터가 손실되더라도 큰 문제가 되지 않는 데이터를 저장해야 합니다.

미러 볼륨 - Mirrored Volume: RAID 1
미러 볼륨은 용어에서도 알 수 있듯이 거울처럼 똑같은 디스크를 구성하는 것입니다. 두 개의 디스크에 모두 'ABCDEF'를 저장하게 된다. 그래서 디스크 하나에 문제가 생기더라도 데이터는 잘 보존됩니다. 실무에서 중요한 데이터를 저장할 때 많이 사용되는 방식입니다. 디스크의 공간 효율은 50%가 됩니다. 미러 볼륨은 RAID 5와 함께 디스크 결함 허용을 지원하는 방식입니다.

RAID 5
RAID 5는 미러 볼륨 처럼 데이터의 안전성이 어느정도 보장되면서 공간 효율성도 좋은 방식입니다.
RAID 5는 최소한 3개 이상의 하드디스크가 있어야만 구성이 가능하며 실무에서 사용할 때는 대부분 5개 이상의 하드디스크로 구성합니다. 구성 원리는 데이터의 저장 시에 패리티를 이용함으로써, 디스크에 문제가 발생 시 원래의 데이터를 예측할 수 있는 방식입니다.
RAID 5의 장점은 어느정도 결함은 허용하며, 또한 저장 공간의 효율도 좋다는 것입니다.

RAID 10
RAID 0 과 RAID 1의 장점만을 결합한 형태.
한 디스크에서 장애가 발생할 경우, 데이터 무결성에 영향을 주지 않고 모든 데이터를 다른 미러에서 제공할 수 있고 고장난 드라이브만 교체하면 된다.

NMS
네트워크 관리 시스템 (NMS, Network Management System/Network Monitoring System)은 컴퓨터 네트워크 또는 네트워크들을 모니터링하고 관리하는데 사용되는 하드웨어와 소프트웨어의

조합을 총칭한다.

SNMP
네트워크 관리를 위해, 관리 정보 및 정보 운반을 위한 프로토콜

SSO
Single Sign-on (싱글사인온)
단 한 번의 로그-인(Log-in) 만으로, 시스템 간 계정 관리를 따로따로 하지 않고,
관련된 전 시스템에 걸쳐 각종 업무나 인터넷 서비스에 접속할 수 있게 해주는 것의 총칭

Round Robin
먼저 들어온 순서대로 처리하는 프로세스

HTTPS
HTTPS와 HTTP
HTTP(Hypertext Transfer Protocol)은
HyperText인 html을 전송하기 위한 통신규약을 의미한다.
마지막에 S를 붙인다면 Secure라는 뜻으로 보안이 강화된 통신규약을 의미한다.
HTTP는 암호화가 되어있지 않은 방법으로 서버에 데이터를 전송하기 때문에
서버와 클라이언트가 서로 주고받는 메시지를 알아내기가 쉽다.
그러므로 서버로 비밀번호나 계좌번호 등 중요한 데이터를 서버로 전송할 경우에는
HTTPS 프로토콜을 사용하여 통신하는 것이 중요하다.

HTTPS와 SSL
HTTPS는 SSL 프로토콜을 기반으로 돌아가는 프로토콜 중 하나다.

SSL
Secure Sockets Layer은 암호규약(프로토콜)이다.
(영어: Transport Layer Security, TLS)
(과거 명칭: 보안 소켓 레이어/Secure Sockets Layer, SSL)
TLS는 클라이언트/서버 응용 프로그램이 네트워크로 통신을 하는 과정에서
도청, 간섭, 위조를 방지하기 위해서 설계되었다.
그리고 암호화를 해서 최종단의 인증, 통신 기밀성을 유지시켜준다.

SSL과 TLS
SSL과 TLS는 같은 뜻으로 말하며 TLS1.0은 SSL3.0을 계승한다.
쉽게 생각하면 SSL의 New Version이 TLS이다.
하지만 TLS라는 이름보단 SSL이라는 이름으로 더 많이 사용되고 있다.

SSL 인증서 정의
SSL 인증서란 클라이언트와 서버간의 통신을 제 3자가 보증을 해주는 문서이다.

클라이언트가 서버에 접속하면
서버는 클라이언트에게 인증서를 전달한다.

그러면 클라이언트는 이 인증서를 보고
신뢰할 수 있는 사람인지 확인 후 데이터를 보내는 등 다음 절차를 수행하게 된다.

SSL 장점
전달되는 내용이 다른 사람에게 노출되는 것을 막을 수 있다.
클라이언트가 접속하려는 서버가 신뢰할 수 있는 서버인지 알 수 있다.
전달되는 내용이 악의적으로 변경되는 것을 막을 수 있다.

SSL 암호화 종류
대칭키
대칭키 방식은 동일한 키로 암호화와 복호화를 할 수 있는 기법을 말한다.

ex) 123를 사용하여 암호화하였다면 복호화도 123를 입력해야 가능하다.
암호화(=암호를 만드는 행위)를 할 때 사용하는 비밀번호를 키(key)라고 한다.

이 키에 따라서 암호화된 결과가 달라지기 때문에
키를 모른다면 암호를 푸는 행위인 복호화도 할 수 없다.

단점
클라와 서버는 대화를 하기 위해서 반드시 대칭 키를 알고 있어야 한다.
그렇기 때문에 통신을 하기 앞서 키를 전달해야하는 과정이 필요하다.
(= 키 배송 문제)
그런데 만약 중간에 대칭키가 유출된다면
키를 획득한 공격자는 암호화된 데이터를 복호화하여 볼 수 있다는 단점이 있다.
공개키 암호화 방식의 알고리즘은 계산이 느리다는 단점이 있다.