네트워크 기초

① LAN (Local Area Network)

: 집, 회사, 건물 등 비교적 좁은 지역을 연결한 네트워크

'네트워크' 라는 광범위한 범위를 물리적으로 구분하여 비교적 좁은 지역을 연결한 네트워크를 LAN 이라 한다. LAN 은 직접 네트워크를 구축하고 관리해야 하지만 유지비용이 적게 들어간다는 특징을 가지고 있다.

② WAN (Wide Area Network)

: 국가간, 대륙간 등 물리적으로 넓은 범위를 연결한 광역 네트워크

각각의 LAN 을 연결한 외부의 커다란 네트워크를 WAN 이라고 하며, 일반적으로는 이미 설치가 된 ISP(인터넷 서비스 제공업체)에서 망을 빌려서 사용한다.

③ Protocol

: 장비 또는 네트워크간 원활한 통신을 위해 미리 지정된 약속 (통신규약)

장비마다 서로 통신하는 방식과 규칙이 다르다면 네트워크 통신을 할 수 없기 때문에 통신의 규칙과 절차를 미리 지정한 것을 프로토콜이라 하고, 프로토콜은 각 장비회사마다 사용하는 비 표준 프로토콜과 전세계적으로 공통적으로 사용하는 표준 프로토콜이 있다

④ OSI Model (Open System Interconnection reference model)

: 개방형 시스템 상호 참조 모델

이 모델은 7 계층(Layer)으로 구성이 되어 있고 각각 주소 지정, 흐름 제어, 오류 제어, 캡슐화, 신뢰할 수 있는 메시지 전송 등과 같은 특정한 네트워크 기능을 규정하고 있다. 하위 계층(물리적 계층)은 주로 미디어 기술에 가장 근접한 계층이고 이 하위 계층과 데이터 링크 계층은 하드웨어와 소프트웨어로 구현되며, 위의 다섯 계층 (네트워크 계층, 전송계층, 세션 계층, 표현 계층, 응용 계층)은 소프트웨어로 구성되어 있다. 최상위 계층인 응용계층은 사용자에게 가장 가까운 계층이다. 현재 OSI 모델은 네트워크 기능을 가르치고 이해하는 방법으로 일반적으로 사용되고 있다.

계층별 순서를 보면 다음과 같다.

- 7 계층 Application Layer(응용 계층)
- 6 계층 Presentation Layer(표현 계층)
- 5 계층 Session Layer(세션 계층)
- 4 계층 Transport Layer(전송 계층)
- 3 계층 Network Layer(네트워크 계층)
- 2 계층 Data-link Layer(데이터 링크 계층)

- 1 계층 Physical Layer(물리적 계층)

⑤ Physical Layer

: OSI 모델의 1 계층으로 물리적 계층이다.

이 계층에서는 기기간 물리적 링크를 작동, 유지, 해제시키는 것과 관련된 전기적, 기계적, 방법적, 기능적 규격을 정의한다. 이 계층에 속한 장비로 hub 와 Repeater, Cable connecter 들이 있다.

⑥ Data Link Layer

: OSI 모델의 2 계층으로 데이터 링크 계층이다.

물리적 주소를 기반으로 데이터의 전송형태를 결정하며, 물리적인 링크를 통해 데이터를 신뢰할 수 있게 전송하는 역할을 한다. 이 계층은 다시 두 개의 부 계층(MAC 부 계층과 LLC 부계층)으로 나눈다. 이 계층에 속한 장비로 L2-Switch 와 Bridge 가 있다.

⑦ Network Layer

: OSI 모델의 3 계층으로 네트워크 계층이다.

논리적 주소를 기반으로 전체 네트워크에서의 두 엔드시스템(end-system) 사이를 연결하고 경로를 선택할 수 있게 한다. 이 계층에서 사용되는 프로토콜은 IP, IPX 등이 있으며, 이 프로토콜에 대한 Routing 으로 경로를 결정한다. 이 계층에 속한 장비로 Router 와 L3-Switch 장비가 있다.

⑧ Transport Layer

: OSI 모델의 4 계층으로 전송 계층이다.

이 계층은 엔드노드(end-node)들 사이에서의 신뢰할 수 있는 네트워크 통신을 책임진다. 이 계층은 가상 회선 설정, 유지, 종료 장애 감지와 복구, 정보 흐름제어 등을 위한 기능들을 제공한다.

⑨ Session Layer

: OSI 모델 5 계층으로 세션 계층이다.

이 계층에선 어플리케이션 사이의 세션(연결)을 설정 및 유지하고 종료시키는 일을 하며, 상위 계층인 표현 계층의 독립체들 사이에 데이터 교환 등을 처리한다.

⑩ Presentation Layer

: OSI 모델 6 계층으로 표현 계층이다.

이 계층은 한 시스템의 어플리케이션 계층에서 보낸 정보를 다른 시스템의 어플리케이션 계층이 읽을 수 있게 보장하는 역할을 한다. 표현 계층은 프로그램이 사용하는 데이터의 구조와 관련이 있으며, 어플리케이션 계층을 대신해 데이터 전송 구문을 중재하는 일을 한다.

⑪ Application Layer (응용 계층)

: OSI 모델의 7 계층으로 응용 계층이다.

이 계층은 사용자가 프로그램을 편리하게 사용할 수 있도록 사용자 인터페이스를 제공하여 데이터를 생성할 수 있도록 도와주는 계층이다. 우리가 주로 컴퓨터를 사용하면서 만나게 되는 계층이 바로 어플리케이션 계층이며 사용자마다 개별적인 인터페이스를 제공하기 위해 사용자 인증이 일어난다.

⑫ TCP/IP Model (Trasmission Control Protocol/Internet Protocol Reference Model)

: TCP/IP 프로토콜 슈트를 기반으로 한 참조모델

1970 년대 미국의 DoD 에서 전 세계적인 인터넷 구축을 지원하기 위해서 개발한 프로토콜 모델로 현재의 인터넷을 위한 상용표준이다. OSI 와 비교되어 설명하는 경우가 많으며, 4 개의 계층 구조를 가진다.

- Application : OSI 의 5 계층~7 계층에 해당한다.
- (host-to-host)Transport : OSI 의 4 계층 전송계층에 해당한다.
- Internet : OSI 의 3 계층 네트워크 계층에 해당한다.
- Network Interface : OSI 의 2 계층과 1 계층에 해당하며, TCP/IP 에서는 하드웨어 부분을 구분하지 않으나 편의상 구분할 수 있다.

⑬ DNS (Domain Name System)

: 문자 주소인 도메인 주소를 실제 통신에 사용되는 IP 주소로 변환해주는 서비스

도메인 네임 시스템은 네트워크 호스트의 이름과 IP 주소를 맵핑해서 유저가 IP 주소 대신에 호스트이름으로 그 호스트를 찾을 수 있도록 하는 시스템이다. 이를 위해서 DNS 서버를 두어서 호스트 이름과 연관된 IP 를 관리하게 된다.

⑭ DHCP (Dynamic Host Configuration Protocol)

: IP 주소를 자동으로 할당할 수 있게 하는 프로토콜

클라이언트가 DHCP 서버에 IP 주소를 요구하고 서버는 각 클라이언트에게 자신이 관리하고 있는 IP 주소를 분배하는 역할을 한다.

⑮ FTP (File Transfer Protocol)

: 파일을 전송하는 프로토콜

주로 대용량 파일 전송에서 사용되며, 포트번호는 21 번(인증)과 20 번(데이터 전송)을 사용하고 TCP 로 동작한다.

⑯ HTTP (Hyper Text Transfer Protocol)

: 웹에서 파일 전송 시에 사용하는 프로토콜

웹 서버를 통해서 데이터를 전송 시 80 번 포트를 통해서 통신을 한다.

⑰ Telnet

: 표준 원격 접속 프로토콜

텔넷은 원격 터미널 연결을 위해서 사용되며 이것을 이용하면 사용자들이 원격 시스템으로 로그인해 시스템 리소스를 마치 로컬 시스템에 연결되어 있는 것처럼 사용할 수 있다.

⑱ TCP (Transmission Control Protocol)

: 전송 계층에서 사용되는 신뢰성을 가진 전송 제어 프로토콜

OSI 의 4 계층 전송 계층에 해당하는 연결지향적인 프로토콜로 데이터 전송 방법을 결정하고 흐름제어, 혼잡제어, 오류검출을 한다. TCP 는 three way handshake 방법을 통해서 데이터의 신뢰성을 확보하는 특성이 있다.

⑲ UDP (User Datagram Protocol)

: 전송 계층에서 사용되는 일반적인 전송 프로토콜

OSI 의 4 계층 전송 계층에 속하는 비연결형 프로토콜이다. TCP 와 다르게 UDP 는 확인 신호나 전달 보장 없이 데이터그램을 교환하는 단순한 프로토콜이며, 전송될 용량이 적거나 음성이나 영상과 같이 속도에 민감한 데이터가 UDP 를 사용한다.

⑳ ARP (Address Resolution Protocol)

: 논리적인 주소인 IP 를 통해서 물리적인 MAC 주소을 알아내는 프로토콜

네트워크 상에 IP 주소를 통해서 요청 패킷을 네트워크 상에 보내면(브로드캐스트), 해당 IP 의 장비가 응답하여(유니캐스트) MAC 주소를 알게 되고 이후에 목적지 기기와 통신이 가능하게 한다.

㉑ ICMP (Internet Control Message Protocol)

: 인터넷 제어 메시지 프로토콜로 신뢰성이 없는 IP 을 보조하기 위해서 사용

네트워크의 연결성을 확인하고 오류를 보고받기 위해 사용되는 네트워크 계층 인터넷 프로토콜이다. 대표적인 명령어로는 Ping 과 Tracert(or Traceroute)가 있다.

㉒ IGMP (Internet Group Management Protocol)

: 인터넷 그룹 관리를 위한 프로토콜

IP 호스트가 멀티캐스트 그룹 멤버십을 인접 멀티캐스트 Router 로 보내는데 사용된다. 멀티캐스트를 사용하는데 표준이 되는 프로토콜이다.

㉓ Ethernet

: OSI 2 계층 데이터 링크 계층의 LAN 구간에서 주로 사용되는 통신 프로토콜

이더넷은 LAN 구간에서 CSMA/CD 방식을 사용해서 통신을 하는 방식이며, 10Mbps 의 속도로 다양한 종류의 케이블을 통해서 통신이 일어난다.

㉔ HDLC (High-Level Data Link Control)

: OSI 2 계층에 속하는 WAN 구간에서 사용되는 통신 프로토콜

점대점, 다중점 링크 상에서 반이중, 전이중 통신 모두를 지원하도록 설계되어 컴퓨터 데이터 통신에 적합한 전송제어 방식이다. CISCO Router 에서 시리얼 라인에 Default 로 적용되는 데이터 링크 계층의 프로토콜이다

㉕ PPP (Point-to-Point Protocol)

: 동기식 또는 비 동기식회선을 통해 router-to-router 또는 host-to-network 연결방식을 제공하는 프로토콜

SLIP 는 IP 를 사용하게 설계되었지만, PPP 는 IP, IPX, ARA 등과 같은 여러 네트워크 레이어 프로토콜과 함께 사용하도록 설계되었다.

㉖ Frame-relay

: 가상회선 기반의 패킷 교환 서비스로 하나의 물리회선으로 여러 개의 논리적인 채널을 지원하는 기술이다.

㉗ Port number

: OSI 의 4 계층 전송 계층의 주소로 소프트웨어적인 입출력 인터페이스

이는 포트번호가 컴퓨터 내의 프로세서를 구별 식별하는 수단임을 말한다. 포트넘버의 길이는 16 비트 길이(0~65535)를 가진다.

㉘ IP (공인 IP, 사설 IP)

: IP 는 네트워크 계층의 논리적 주소로 비 연결성 Inter-Network 서비스를 제공한다.

IP 의 길이는 32 비트 주소이며, 8 비트씩 나누어서 10 진수로 표기한다.

- 공인 IP 는 인터넷을 통해서 연결된 세계에서 유일한 주소를 의미한다.
- 사설 IP 는 네트워크 내에서 사용되는 주소로 인터넷을 통해서 직접 통신할 수 없고 NAT 기술을 통해서 외부 인터넷과 통신이 가능하다.

㉙ MAC(Media Access Control)

: IEEE 가 정의한 데이터 링크 계층의 두 가지 서브 레이어 중의 하위 레이어

MAC 서브 레이어는 공유 미디어 엑세스 문제를 처리한다.

㉚ LLC(Logical Link Control)

: IEEE 가 정의한 데이터 링크 계층의 두 가지 서브 레이어 중에서 더 높은 레이어

오류 제어, 흐름 제어, 프레임 처리, MAC 서브 레이어 주소 지정 등을 처리한다.

LLC 타입은 3 가지가 있으며 주로 LLC 타입 1 을 사용한다.

㉛ Segment

: OSI 4 계층에서 데이터를 부르는 단위

㉜ Packet

: OSI 3 계층에서 데이터를 부르는 단위 (Datagram 이라고도 함)

패킷은 네트워크 계층 데이터 단위를 언급할 때에 자주 사용되는 용어이다.

㉝ Frame

: OSI 2 계층에서 데이터를 부르는 단위.

㉞ Unicast

: 특정 호스트 주소를 목적지로 단일 네트워크 수신 장치로 보내진 메시지이다.

하나의 네트워크에서 송신 측에서 하나의 수신 측으로 보내는 1:1 통신 방식을 의미한다.

㉟ Broadcast

: 네트워크 상의 연결된 모든 장비로 데이터가 뿌려지는 통신방식

불특정 다수에게 메시지가 뿌려지는 1:n 통신 방식을 말한다.

㊱ Multicast

: 네트워크 주소상의 특정한 그룹에게 보내는 통신방식

특정 다수에게 메시지가 전달되는 그룹 통신 방식으로, Unicast 와 Broadcast 의 통신상 장점을 합쳐놓은 방식이라고 할 수 있다.

㊲ Encapsulation

: 특정한 프로토콜(데이터)를 원래 데이터의 추가시키는 과정.

주로 상위계층에서 하위계층으로 데이터를 전달하면서 각 계층의 정보를 담은 Header 를 기존의 데이터에 붙여나가는 과정을 말한다

㊳ Decapsulation

: Encapsulation 의 반대로 캡슐화 되어있는 데이터의 역으로 풀어내는 과정.

하위계층에서 상위계층으로 데이터를 올려 보내는 과정을 말하며, 각 계층별로 캡슐화 된 해당 프로토콜이 동작한 후에 나머지 캡슐화 된 부분은 상위 부분으로 올려서 처리하게 된다.

㊴ Bandwidth (대역폭)

: 네트워크 신호용으로 사용할 수 있는 가장 높은 주파수와 가장 낮은 주파수 사이의 차이

대역폭이 넓으면 많은 데이터를 한꺼번에 처리할 수 있다. 때문에 처리 속도가 빨리지는 효과를 가지게 되어 속도의 개념으로 사용되고 있다.

㊵ Duplex

: 이중화 통신 또는 양방향 통신

방식은 전이중(full) 방식과 반이중(half) 방식이 있다.

전이중 방식은 동시에 데이터 송신과 수신이 가능하고, 반이중 방식은 송신과 수신을 동시에 하지 못하는 방식

㊶ Clock signal

: 동기화에 사용되는 주기적인 신호.

장비간 동기화를 위해서 사용되며, data signal 의 기준이 되는 것으로 통신하고자 하는 두 장비간에 동일하게 맞추지 않으면 정확한 데이터 통신이 불가능해진다.

㊷ Data signal

: 회선 상에 전송하는 정보의 형태로 이진수로 구성된다.

보내려고 하는 데이터를 0 과 1 로 구분해서 보내는 신호이다. clock signal 동기화가 정확하지 않으면 정확한 전달이 어렵다.

㊸ CSMA/CD(Carrier Sense Multiple Access/Collision Detection)

: 정보 송출에 앞서서 회선의 사용 유무를 조사하여 보내는 방식으로 충돌 감지 시 송신을 멈추고 일정시간 후에 재송하는 방식.

이더넷의 통신 방식으로 데이터를 전송하고자 할 때 먼저 현재 네트워크에 전송 중인 데이터가 있는지를 확인한 후 전송을 시작하는데, 이때 동시에 두 장비가 전송을 시작하면 충돌이 발생하게 되고 전송 장비는 이 충돌을 감지하게 된다. 충돌이 발생하면 전송 장비는 데이터를 랜덤한 시간이 흐른 뒤에 재전송을 시도하게 된다. 총 15 번의 충돌까지 재전송하고 이후에는 전송하지 않는다.

㊹ Subnet

: 하나의 네트워크에서 논리적인 분할로 세분화된 네트워크

IP Class 단위의 비효율성으로 인한 IP 주소의 낭비를 막고 보안성을 강화시키기 위해 하나의 네트워크를 논리적으로 구분 하여 나누어진 작은 네트워크를 Subnet 이라고 한다.

㊺ Subneting

: 네트워크 세분화를 위한 IP 주소 구성을 변경하는 것

IP 는 각 네트워크를 구분하기 위한 Net-ID 와 하나의 네트워크 내의 각 Host 들을 구분하기 위한 Host-ID 로 구성이 되어있다. 서브네팅은 필요한 수만큼 네트워크를 분할하여 늘리기 위해 Host-ID 부분의 Bit 를 Net-ID 로 넘겨주는 과정이다.

㊻ VLSM (Variable-Length Subnet Mask)

: 네트워크를 동일한 크기가 아닌 필요한 크기로 각각 서브네팅 하는 방식

동일한 네트워크 주소로 서로 다른 크기로 서브네팅 하여 주어진 가용 주소 공간을 최적화한다.

㊼ Subnet-mask

: IP 주소의 Net-ID 와 Host-ID 를 구분하기 위한 필터 값

Net-ID 를 1, Host-ID 를 0 으로 표시하여 구분하게 한다. IP 와 Subnet-mask 는 AND 연산을 통해 Router 가 네트워크 부분을 인식할 수 있도록 도와준다.

㊽ Prefix

: Net-ID 의 Bit 수를 표시한 것으로, 네트워크에서 변하지 않는 네트워크 부분을 의미한다.

이것은 Subnet-mask 의 연속된 1 에 해당하는 부분으로 숫자로 표기하는데,

Subnet-mask 255.255.255.0 은 prefix 로 /24 로 표현된다.

㊾ CIDR (Classless Inter-Domain Routing)

: 주어진 IP 를 클래스 구별 없이 뒤에 오는 Subnet-mask 에 따라 구분하는 방식

CIDR 는 원래의 IP 주소 클래스 체계를 쓰는 것보다 IP 를 더욱 융통성 있게 할당하고 지정하는 방식 중 하나이다..

㊿ TTL (Time To Live)

: IP 패킷 전달에 대한 생존 시간으로 거쳐갈 수 있는 Router 의 개수

대체로 유닉스 64, 윈도우 128, Router 255 의 값을 가진다. Router 를 지날 때마다 TTL 값은 1 씩 감소하며, TTL 값이 0 이 되면 해당 패킷은 소멸된다.

㊶ ToS(Type of Service)

: QoS 를 지원하기 위해 패킷의 서비스 유형을 나타내는 서비스 타입

IP 패킷 헤더 내에 있는 8 비트 필드로 요구되는 서비스의 유형을 나타내는데 사용된다. 주로 8 비트 중 3 비트만 사용하며 숫자가 높아질수록 우선순위가 높아진다.

㊷ QoS(Quality of Service)

: 전송 품질과 서비스 가용성을 알려주는 전송 시스템의 수행 성능 척도이다.

㊸ TCP three way handshake

: TCP 의 신뢰성 있는 통신을 위해 3 번의 패킷 교환을 통해 연결성을 확인하는 과정

A, B 두 장비간 연결을 위해서 A 장비가 TCP 헤더의 플래그 필드에 SYN 에 1 을 셋팅한 후에 Sequence Number 에 임의 값을 지정해서 상대편 장비에 보내면, 상대편 B 는 연결을 위해서 TCP 플래그에 ACK 와 SYN 에 1 로 셋팅한 후에 Sequence Number 는 임의 값을, Acknowledgment Number 에는 상대로 받은 Sequence Number 에 +1 한 값을 넣어서 보낸다. A 장비는 Acknowledgment Number 를 확인해서 자신이 보낸 Sequence 값과 비교확인 후에 B 장비로부터 받은 Sequence Number 를 Acknowledgment Number +1 해서 보내고 TCP 플래그에 ACK 를 1 로 셋팅해서 보내서 A,B 두 장비간 연결관계를 수립하는 방식을 말한다.

.

Cisco Device & Configuration

① HUB

: 전기신호를 증폭시켜 전달하는 1 계층의 대표 장비

이더넷 네트워크에서 여러 대의 컴퓨터, 네트워크 장비를 연결하는 장치이다. 허브로 연결된 네트워크에서는 한 컴퓨터에서 주고받는 데이터가 같은 허브에 연결된 다른 모든 컴퓨터에 전달된다. 따라서 연결된 컴퓨터의 개수가 많아질 수록 네트워크에서 충돌(collision)이 많아지고 속도가 느려진다.

② Switch

: LAN 에서 Multi-Access 를 지원해주는 2 계층의 대표 장비

사용목적은 허브와 유사하지만, 전이중 통신방식(full duplex)를 지원하기 때문에 충돌(collision) 현상이 쉽게 생기지 않고, 훨씬 향상된 속도를 제공한다. 이러한 기능을 수행하기 위해 스위치는 각 장치의 고유한 MAC Address 를 기억한다. 데이터 처리에 ASIC(Application-specific intergrated circuit)이라는 하드웨어 프로세서를 사용한다.

③ Bridge

: 동일한 프로토콜을 사용하는 LAN 과 LAN 을 연결하는 2 계층 통신 장비

이더넷 스위치와 유사하지만, 데이터 처리를 소프트웨어 적으로 처리 하기 때문에 데이터 처리 능력에 한계가 있으며 각 포트별 다른 속도를 제공하지 못한다. Frame 을 전송하기 전에 MAC 주소를 확인하고 목적지 주소를 찾지 못하면 다른 LAN 으로 전달하지 않는다. 일반적으로 스위치에 비해 포트수가 적다.

④ Router

: 논리적 주소를 기반으로 목적지에 대한 최상의 경로로 전달하는 3 계층 통신 장비

2 개 이상의 논리적인 네트워크 대역을 연결하며, 경로에 대한 정보를 가지고 있어야만 한다. 주로 LAN 구간을 WAN 구간과 연동 할 때 사용된다.

⑤ DCE (Data Circuit-Terminating Equipment)

데이터 회선 종단 장비로 불리는 DCE 는 데이터 통신 장비 (Data Communication Equipment)와 데이터 캐리어 장비 (Data Carrier Equipment)라 불리기도 한다.

DCE 는 신호 변환, 코딩, 그리고 Line Clocking 같은 기능을 수행하며, 시리얼 인터페이스로 연결된 구간에서 DTE 와 데이터 전송을 동기화 하기 위해 클럭신호를 제공한다.

⑥ DTE (Data Terminal Equipment)

데이터 단말 장치로서, 사용자의 정보를 신호로 변환하거나 수신한 신호를 재 변환하는 종단 장비이다. DTE 장비는 DCE 장비와 통신하며, DCE 장비에서 제공한 클럭신호을 받아 동기화 한다.

⑦ IOS (Internetwork Operating System)

: CISCO 사에서 장비를 구동하기 위해 제공하는 운영체제

기본적으로 CLI(command line interface)라는 TEXT 형 접근 방식를 제공한다.

⑧ CDP (Cisco Discovery Protocol)

: 이웃장비의 정보를 알아오는 CISCO 전용 프로토콜

직접 연결된 CISCO 장비의 정보를 찾아주는 프로토콜로서, 네트워크 망의 관리 용도로 사용된다.

⑨ POST (POWER ON SELF TEST)

장비의 하드웨어적 이상유무를 스스로 체크하는 과정으로, 전원을 켜고 부팅 시 제일 처음 POST 과정을 거치게 된다. 장비의 인터페이스, 메모리, CPU 등 장비를 구동하는데 주요한 부분의 이상유무를 체크 하게 된다.

⑩ Bootstrap

부트스트랩 프로그램 (bootstrap)은 장비가 부팅될 때 필요한 내용을 RAM 으로 불러오도록 적재되는 프로그램이다.

CISCO 장비는 POST 과정을 마친 뒤 Bootstrap 프로그램을 구동시켜, 일반적으로 FLASH 에 저장되어 있는 IOS 를 RAM 에 적재 하게 된다.

⑪ Configuration register

CISCO 장비 구동에 대한 설정 값을 의미 하며 16 비트로 이루어져 있다.

기본적으로 정상부팅모드인 0x2102 로 설정이 되어있고, 비밀번호를 복구하기 위한 복구모드인 0x2142 로 변경하게 되면 부팅 과정 중 저장된 장비 설정내용을 확인하지 않도록 설정된다.

⑫ Backup

장비의 IOS IMAGE 파일이나, 설정내역이 손실될 것을 대비해 해당 장비가 아닌 다른 장치에 정보를 복사 해두는 것을 뜻한다. TFTP, FTP 서버, 외장 FLASH 등을 이용한다.

⑬ Restore

TFTP, FTP, FLASH 등에 백업해 두었던 IOS 나 설정 파일 등을 장비로 불러오는 것을 말한다.

Route

① Routing

: 출발지부터 목적지까지 패킷을 전달하기 위한 일련의 과정

Source Address 로부터 Destination address 까지 패킷이 전달되는 경로를 선택하는 프로세스이다.

② Connected

: 물리적으로 직접 연결된 네트워크 정보를 학습하는 것.

케이블로 직접 연결되어 있는 네트워크를 뜻하며, 장비가 맨 처음에 학습하는 기본 정보이다. 직접 연결되어 있기 때문에 경로 선택 시 우선순위가 가장 높다.

③ Static

: 네트워크 관리자가 패킷의 경로를 직접 선택하여 입력하는 것.

통신 경로가 고정적이며 토폴로지 변화 시에는 관리자가 수동으로 변경하여야 한다.

장점 – 경로의 효율적인 관리가 가능하다. 출발지와 목적지의 통신은 가능하지만, 통신을 위해 거쳐가는 네트워크 간의 통신 여부를 제어할 수 있다.

단점 – 토폴로지 변화 시 관리자가 직접 변경하여야 하므로 대처가 느리다.

④ Dynamic

: Router 가 프로토콜들을 이용하여 자동으로 경로를 학습 하는 것.

장점 - Router 가 스스로 토폴로지 변화를 감지하고 경로를 변경하기 때문에 토폴로지 변화에 따른 대처가 빠르다.

단점 - 네트워크 상태를 계속 주시하고 있기 때문에 리소스 소모가 많다.

⑤ Redistribution

: 각기 다른 프로토콜들로 경로 정보를 학습하는 것.

Connected, Static, Dynamic 세 가지를 모두 사용한다. 각 프로토콜마다 경로 선택과 Routing 정보를 교환하는 규칙들이 다르기 때문에 네트워크 환경과 목적에 맞게 사용할 수 있다.

⑥ Routing table

: Router 가 패킷을 전달하기 위해 참조하는 최적 경로들의 집합.

Router 는 Routing Table 에 있는 경로로만 데이터를 전달할 수 있다. 만약 Routing Table 에 최종 목적지까지의 경로가 없다면, Router 는 패킷을 전달할 수 없다.

⑦ Stub network

: 하나의 내부 네트워크에서 외부 네트워크로 나가는 길이 하나 밖에 없는 구조.

⑧ Distance vector

: 경로 정보 전달 시 거리와 방향 정보를 포함하여 전달하는 Routing Protocol

특정 시간마다 주기적으로 경로 정보 전달하고 전달받은 경로 정보를 그대로 사용한다.

장점 – 스스로 경로 계산을 하지 않기 때문에 다른 프로토콜들에 비해 리소스 소모량이 적다.

단점 – 전체 네트워크를 파악하지 못하기 때문에 잘못된 정보로 인해 네트워크 혼잡이 발생할 수 있다. 토폴로지 변화에 따른 대처가 느리다. 대체 경로를 찾기 위해서 상대방에게서 경로 정보를 전달 받을 때까지 기다려야 한다.

⑨ Link state

: 물리적으로 직접 연결된 네트워크의 정보를 인접 장비와 교환하여 사용 가능한 모든 경로를 계산하여 전체 토폴로지를 파악 후 스스로 최적 경로를 선택하는 Routing Protocol

장점 – 스스로 경로 선택을 하기 때문에 잘못된 정보를 사용하지 않는다. 패킷을 전송할 수 있는 모든 경로를 알고 있기 때문에 토폴로지 변화에 대한 대처가 빠르다. 계층적 Design 에 따라 Network 확장성이 보장된다.

단점 – 패킷을 전송할 수 있는 모든 경로를 계산하므로 해당 장비의 리소스 소모량이 많다. 반드시 계층적 Design Rule 을 따라야 한다.

⑩ Advanced Distance Vector

: Distance Vector 의 특징과 Link State 의 특징을 함께 가지는 Routing Protocol

리소스 소모가 적고, 네트워크 변화에 대응이 빠르다는 장점을 가지고 있다.

⑪ Classful

: 네트워크 주소를 전달할 때 Subnet-mask 를 함께 보내지 않는 방식

Class(A,B,C,D,E) 별로 규격화 시킨 IP 주소로 나누어진 네트워크 정보를 가지고 Routing 하는 것을 말한다. Subnet-mask 가 클래스 별로 고정되어 있으므로 Subnet-mask 를 함께 전달할 필요가 없다. Routing Table 의 크기가 줄어든다는 장점이 있지만, 모든 네트워크 정보를 주 네트워크의 Class 로 축약시켜 전달하므로 경로 선택이 잘못 될 수도 있다.

⑫ Classless

: 네트워크 주소를 전달할 때 Subnet-mask 를 함께 전달하는 방식

서브네팅을 통해 나누어진 네트워크 정보를 가지고 Routing 하는 것을 말한다. 나뉘어진 Net-ID 부분을 구분하기 위해 네트워크 주소와 Subnet-mask 를 함께 전달한다.

⑬ Autonomous System

: 동일한 Routing Protocol 을 사용하는 하나 관리 영역

동일한 관리자가 동일한 정책을 통해 관리 할 수 있는 네트워크의 범위를 말한다.

⑭ Administrative Distance

: 관리자 거리값 이라고 해석할 수 있으며, Routing Table 에 최적 경로 설정 시 사용하는 프로토콜의 신뢰도.

Connected – 0, Static – 1, EIGRP – 90, OSPF – 110, RIP – 120 등…

⑮ Metric

: 프로토콜이 최적 경로 설정 시 사용하는 비용 값.

Hop Count, Bandwidth, Delay, Load, Reliability, MTU 등 여러 변수 중 Routing Protocol 들은 서로 다른 기준으로 최적경로를 선택한다.

⑯ Convergence time

: 수렴시간. 토폴로지가 변화 될 때 대체 경로를 선택할 때까지의 시간.

⑰ Loop

: 패킷이 시작된 노드로 다시 되돌아 오는 현상. Looping 이란 Loop 가 반복되는 현상을 말하는데, 불필요한 트래픽을 발생시키므로 네트워크 상의 부하가 커져 혼잡을 발생시킬 수 있다.

⑱ network (Routing 명령어에서의 network)

: 인접 Router 에게 알려줄 네트워크 정보를 설정하는 명령어

network 라는 명령어는 '광고' 라는 뜻과 '활성화' 의 두 가지의 의미를 가지고 있다.

광고(Advertisement)란 인접 Router 에게 자신에게 설정된 네트워크 정보를 알려주는 것을 의미한다.

활성화란 network 로 설정한 IP 주소가 할당된 인터페이스에 해당 Routing Protocol 이 동작되는 것을 의미한다.

⑲ Summarization

: 서브넷팅 된 네트워크의 주소를 좀 더 큰 주소 범위로 축약시키는 것.

⑳ Auto summary

: 자동 축약.

Classful Routing 프로토콜이 경로 정보를 전달 할 때 주 네트워크의 Classful 주소로 자동 축약하여 전달 하는 것.

㉑ Manual summary

: 수동 축약. Routing 테이블의 크기를 줄이기 위해 서브넷팅 된 네트워크 주소를 적절한 크기로 관리자가 수동으로 축약시키는 것.

㉒ Access List

: 접근제어리스트. Router 등의 장비에서 패킷이나 경로의 접근 여부를 제어하는 규칙.

주로 네트워크 상의 원하지 않는 트래픽을 제어하고, 보안을 위하여 허가되지 않은 사용자가 네트워크의 자원에 접근하는 것을 차단하거나 올바르지 않은 패킷을 구분하는데 사용된다.

㉓ Standard ACL

: 패킷의 헤더에서 Source IP 만을 검사한다. ACL Number 는 1~99 까지 사용한다.

㉔ Extended ACL

: 패킷의 헤더에서 Source IP 와 Destination IP 및 Application Port 번호 등을 검사한다.

㉕ Inbound ACL

: 인터페이스로 들어오는 패킷에 대해서 접근제어 리스트를 통해서 제어한다.

인터페이스에 설정을 하며, 설정 후에는 해당 인터페이스로 들어오는 패킷을 ACL 을 통해서 제어하게 된다.

㉖ Outbound ACL

: 인터페이스로 나가는 패킷에 대해서 접근제어 리스트를 통해서 제어한다.

특정 패킷이 Router 에 들어와서 Routing 을 통해서 인터페이스로 나갈 때에 나가는 인터페이스에 이 설정이 되어 있으면, ACL 을 통해서 패킷을 제어한다.

㉗ Wildcard mask

: 일부 IP 주소를 골라내기 위해 사용하는 필터 값

0 과 1 통해서 씌우는 마스크로 접속제어 리스트 또는 일부 Routing Protocol 에 쓰인다.

와일드카드 마스크는 0 과 1 로 마스크를 씌우는데, 0 인 경우에는 해당 위치의 비트 값이 그대로 와야 하는 경우, 1 인 경우에는 어떤 값이 와도 상관없는 경우이다. 주로 OSPF 네트워크의 구분을 위해서 사용되거나 ACL 과 같이 접속 제어 리스트를 작성할 때에 사용된다.

㉘ NAT (Network Address Translation)

: 내부 네트워크 주소를 외부 네트워크주소로 변환해주는 주소변환기술

주로 공인 IP 주소에 사설 IP 주소를 할당할 때 사용한다.

외부 네트워크를 사용할 수 없는 사설 IP 가 외부 네트워크를 사용할 수 있게 해준다. 공인 IP 주소를 절약할 수 있고 주소 변환을 통해 내부 실제 주소를 숨길 수 있으므로 보안에 용이하다.

㉙ Dynamic NAT

: 공인 IP 의 주소에 다량의 사설 IP 의 주소를 교대로 할당하는 방식

예를 들어 10 개의 공인 IP 를 100 명이 사용하는 경우에 남은 90 명은 대기하고 있다가 순차적으로 할당 받게 된다. 할당되는 주소가 변하기 때문에 외부에서 접속이 불가능하다.

㉚ Static NAT

: 공인 IP 주소와 사설 IP 주소를 1:1 로 mapping 하는 방식

항상 같은 주소로 할당되므로 외부에서 접속이 가능하다.

㉛ NAT/PAT

: 하나의 공인 IP 주소를 다수의 사설 IP 주소가 동시에 사용할 수 있는 방식

NAT 의 경우 하나의 공인 IP 를 한번에 하나의 사설 IP 만 사용할 수 있는데 포트 정보를 추가 시켜서 다수의 사설 IP 가 하나의 공인 IP 를 공유할 수 있도록 한다.

㉜ NAT table

: 공인 IP 와 사설 IP 의 mapping 정보가 들어 있는 테이블. 공인 IP 와 사설 IP 의 주소 변환 시 NAT table 에 있는 정보를 사용한다.

Switch

① Ethernet Frame

: 이더넷의 2 계층 데이터 송수신을 위해 사용되는 정해진 규격

데이터가 저장된 데이터 필드와, 이를 정상적으로 전송하기 위한 기타 필드가 존재 한다.

② Mac-address-table

: Layer2 전송장비인 스위치가 각 장치들이 연결된 위치를 기억하기 위해, 각 장치들의 고유한 MAC 주소와 PORT 번호를 함께 묶어서 기록해 놓은 표

③ Address learning

: Switch 의 주소학습 기능

이더넷 프레임이 스위치의 port 로 들어 왔을 때, 스위치는 프레임의 Source MAC address 를 참조하여, PORT 번호와 함께 MAC-address-table 에 기록한다.

④ Flooding

: Frame 을 받은 포트를 제외한 나머지 모든 포트로 Frame 을 전달하는 방식

스위치가 모르는 Destination MAC address 를 가진 프레임이 들어왔을 때, 스위치는 전체 포트로 해당 프레임을 전송하게 된다.

⑤ Forwarding

: 목적지 주소를 확인하여 특정 포트로만 Frame 을 전달하는 방식

스위치가 알고있는 Destination MAC address 를 가진 프레임이 들어왔을 때, 스위치는 해당 MAC address 를 가진 장치가 연결된 포트로만 프레임을 전송하게 된다.

⑥ Filtering

: Frame 이 전달되지 않도록 송신 포트를 차단하는 기능

스위치가 알고 있는 Destination MAC address 를 가진 프레임이 들어왔을 때, 스위치는 해당 MAC ADDRESS 와 상관없는 포트로는 프레임을 전송하지 않게 된다.

⑦ Aging

Aging Time 은 MAC ADDRESS TABLE 의 유효 시간을 의미하며, 기본적으로 Learning 과정 후 5 분 동안 MAC ADDRESS TABLE 이 유지된다. Aging Time 이 만료 될 동안 해당 장치와의 통신이 없으면, 해당 장치의 MAC 주소는 사라지게 되며 이를 Aging out 이라고 한다. Aging Time 이 만료 되기 전에 통신이 일어나면, 다시 aging time 은 5 분으로 갱신된다.

⑧ Transparent bridging

스위치가 수신한 이더넷 프레임을 참조하여 MAC 테이블을 생성 및 갱신하고, 이를 목적지로 전달 할 때 사용되는 프로토콜이다.

⑨ 단일 장애 점(Single Point Of Failure, SPOF)

: 단일 경로로 설정된 네트워크에서 문제가 되는 지점

단일 장애 점(Single Point Of Failure, SPOF)은 시스템 구성 요소 중에서, 동작하지 않으면 전체 시스템이 중단되는 요소를 말한다. 네트워크 설계 시 단일 장애 점을 최소화 하기 위해, 장치를 이중화 한다.

⑩ STP (Spanning Tree Protocol)

: Switch 의 Loop 방지 기술

스위치 2 대 이상을 가지고 네트워크 망을 구현하게 되면 스위치의 Flooding 동작 때문에, Loop 가 발생 할 소지가 있다. 이를 방지하기 위해 논리적으로 하나 이상의 Link 를 차단하게 되는데, 이러한 역할을 하는 것이 Spanning-Tree Protocol 이다.

⑪ BPDU (Bridge Protocol Data Unit)

: Spaning-Tree Protocol 을 지원하는 스위치들 사이에서 교환되며 각 스위치의 상태 정보를 담고 있는 메시지.

모든 스위치는 각 BPDU 의 내용을 분석하여 스위치들은 주기적으로 BPDU 를 교환하여 Loop 를 탐지하고 차단할 포트를 결정하게 된다.

⑫ Bridge ID

: Spaning-Tree 에서 각 스위치를 구분하기 위해 사용되는 고유한 번호

설정된 Priority 값과 MAC ADDRESS 의 조합으로 이루어진다. Spaning-Tree 의 중심이 되는 Root Bridge 장비를 선정하는데 사용된다.

⑬ DP(Designated port)

: Spaning-Tree 구조상 하위 단의 스위치들에게 BPDU 를 송신하는 포트

⑭ RP(Root port)

: DP 로 부터 BPDU 를 수신하는 포트

⑮ NDP(Non designated port)

: Spaning-Tree 에 의해 논리적으로 차단되는 포트

⑯ PVST (Per Vlan Spanning Tree)

: 포트 기반으로 작동하는 기존의 STP 에서 확장되어 VLAN 별로 STP 를 동작시키는 Spaning-Tree Protocol 의 일종

⑰ RSTP (Rapid Spanning-Tree Protocol)

: 수렴시간이 빠른 Spaning-Tree Protocol

경로 계산시 오랜 시간이 소요되는 STP 의 Spanning-tree 동작 과정을 변형하여 만든 Spaning-Tree Protocol 의 하나로서, 스위치간 제안/동의 과정을 거쳐 즉시 경로의 전송 상태를 변경하여, 빠른 수렴을 가지게 되는 것이 특징이다. IEEE 802.1w 로 정의된다.

⑱ SVI (switch virtual interface)

: 스위치에 생성된 특정 VLAN 에 연결된 장치들과 통신하기 위해 사용되는, 가상의 인터페이스

⑲ Port security

: 하나의 포트에 학습되는 MAC 주소의 수를 한정하는 보안 설정

보안을 목적으로 지정된 사용자만 네트워크에 접근을 허용하기 위한 CISCO 스위치의 기능이다. 단말장치의 MAC address 를 기반으로 단말을 구분하며, 보안 정책을 수립하게 된다.

⑳ VLAN (Virtual LAN)

: 논리적으로 나눈 Switching Network

하나의 스위치 안에서 LAN 을 여러 개로 분리하여, 동일한 VLAN ID 를 가지는 PORT 끼리만 Layer2 통신을 허용하는 기능. 스위치 내부적으로 Broadcast 영역을 분리 하는데 사용한다.

㉑ Static VLAN

: 각 포트별 VLAN 을 관리자가 직접 지정하여 셋팅 하여 사용하는 것을 말한다.

㉒ Dynamic VLAN

: 포트로 올라오는 FRAME 의 Source 주소를 분석하여 자동으로 VLAN 을 할당하는 것을 말한다. VLAN 을 할당하기 위해 VMPS(VLAN Membership Policy Server)가 필요하다.

㉓ Access port

: 스위치 포트 당 1 개의 VLAN 을 할당하는 방식으로, 수신된 프레임을 그대로 전달한다.

㉔ Trunk port

: 스위치 포트 당 여러 개의 VLAN 을 할당하는 방식으로, 수신된 프레임 별로 VLAN 에 맞는 TAG 를 붙여 전달하게 된다.

㉕ Tagging

: 트렁크 포트에서 각각의 프레임에 그 프레임의 VLAN 을 구분하는 붙이는 정보

㉖ Native VLAN

: 트렁크 포트로 TAG 가 붙지 않은 일반 Frame 이 들어 왔을 때 할당하는 VLAN

㉗ 802.1q

: 트렁크 포트를 사용하는 스위치 간에 VLAN 정보를 전달하는 TAGGING 방식을 정의한 것으로, IEEE 표준 방식이다.

㉘ ISL

: 트렁크 포트를 사용하는 스위치 간에 VLAN 정보를 전달하는 TAG 의 방식을 정의 한 것으로, CISCO 전용 방식이다.

㉙ VTP (VLAN Trunk Protocol)

: 스위치가 가지고 있는 VLAN Database 를 다른 스위치들에게 공유하기 위한 프로토콜.

㉚ VTP server

: VTP 로 연동된 스위치들 사이에서, VLAN 을 생성, 삭제, 변경을 수행하고 이를 전파하는 역할을 하는 스위치를 말한다.

㉛ VTP client

: VTP server 로부터 VLAN 정보를 업데이트 받는 스위치를 말한다.
VLAN 생성, 삭제, 변경이 불가능하다.

㉜ VTP transparent

: VTP server 로부터 받은 VLAN 정보를 VTP Client 로 전달하는 역할을 수행한다.
자신 스스로 VLAN 을 생성, 삭제, 변경을 할 수 있지만, 다른 스위치들에게 전파는 하지 않는다.

㉝ VTP pruning

: VTP 구간에서, 특정 스위치에서 사용하지 않는 VLAN 에 대한 정보를 차단하여 대역폭의 낭비를 줄이는 기술.