1. TCP/IP

인터넷을 사용하는 모든 통신의 기본적인 프로토콜

한 개의 프로토콜이 아닌 여러 가지 프로토콜 조합

TCP/IP를 기반으로 BAN, PAN, LAN, MAN, WAN 구간의 장치들이 원활히 데이터를 주고받을 수 있음

OSI 7계층과 달리 4개의 계층으로 표현됨

TCP는 서비스를, IP는 주소를 의미함

수많은 프로토콜들이 IP 주소를 기반으로 동작함

2. TCP/IP 계층

1) 네트워크 접속 계층(Network Access Layer)

OSI 참조 모델의 물리 계층과 데이터링크 계층의 역할을 수행

프레임의 송신과 수신을 담당한다

ARP: 목적지의 MAC 주소를 모를 경우 이를 알아내기 위해서 사용하는 프로토콜

RARP: 목적지의 IP 주소를 모를 경우 이를 알아내기 위해서 사용하는 프로토콜

ARP는 Broadcast, RARP는 Unicast를 수행

NIC, 스위치와 허브는 네트워크 접속 계층을 대표하는 네트워크 장치이다

에러 검출 기능이 있으며, 패킷을 프레임화 함

ARP는 Broadcast, ARP에 대한 응답은 Unicast를 수행

2) 인터넷 계층(Internet Layer)

OSI 참조 모델의 3계층(네트워크 계층)의 역할을 수행한다

패킷의 송신과 수신을 담당하며, IP 주소 체계를 관리한다

패킷을 수신하면, IP 주소를 확인하여 패킷을 목적지로 보내는 라우팅 기능 수행

라우팅 경로는 어떠한 라우팅 프로토콜을 쓰느냐에 따라 달라질 수 있음

IP: 컴퓨터 네트워크에서 장치들을 나타내는 수단이며, v4(32bit)와 v6(128bit) 두 가지가 존재한다

ICMP: 인터넷 제어 메시지 프로토콜이며, 장치 간의 통신 가능 여부를 확인할 때 사용 ex) ping

ICMP는 Echo Request(요청) 및 Echo Reply(응답)로 구성된다.

3) 전송 계층(Transport Layer)

종단 간의 통신이 완성되는 계층이며, TCP와 UDP가 대표적이다

TCP와 UDP는 포트번호를 사용하여 통신한다

TCP는 신뢰성 있는 통신을 제공하지만 UDP는 TCP에 비해 신뢰성 있는 통신을 제공하지 않는다

UDP는 TCP보다 통신 데이터 처리 속도가 빠르다

UDP를 이용하는 응용프로그램에서 어느 정도의 신뢰성 있는 통신을 해야 할 경우 다른 프로토콜과 함께 사용하여 신뢰성을 제공할 수 있다

TCP와 UDP의 정의는 RFC1700 문서에 정확하게 제공되어지고 있다

Well-Known 포트란 대부분의 시스템 간에 널리 이용되는 애플리케이션을 위해 기본 값으로 설정되어 있는 포트 번호를 의미한다

TCP/UDP Well-Known 포트

Port 번호 Service name comment

7 Echo Echo Protocol

22 SSH SSH Remote Login Protocol

53 domain Domain Name Server

4) 응용 계층(Application Layer)

OSI 참조 모델의 세션, 표현, 응용 계층의 역할을 수행하는 계층

네트워크를 통한 실제 사용자데이터를 처리하는 계층

HTTP, HTTPS, FTP, SMTP, POP3, DNS 등이 이 계층에 해당한다

3. TCP 헤더

TCP는 연결 지향형(Connection-Oriented) 서비스를 제공하고 신뢰성 있는 데이터 전송을 보장한다. 이러한 기능은 TCP 헤더 내의 각종 필드에 의해서 가능하다

1) 출발지 포트 번호(Source Port Number)

출발지 호스트의 포트 번호를 정의한 16비트 필드이며 임의 번호를 사용

2) 목적지 포트 번호(Destination Port Number)

목적지 호스트의 포트 번호를 정의한 16비트 필드이며, 대부분 Well-Known Port Number를 사용

3) 순서 번호(Sequence Number)

TCP 세그먼트들에 대한 순서 번호를 표시한다, 목적지에서 재조립할 때 사용

4) 수신 확인 응답 번호(Acknowledge Number)

수신 장치에서 발신 장치로 세그먼트의 전송 성공 여부를 알려주기 위해 사용

5) 헤더 길이(Header Length)

TCP 헤더의 길이는 최소 20byte에서 최대 60byte가 될 수 있으며, 이를 표시

6) 예약 비트(Reserved)

현재는 사용하지 않으며, 추후 다른 목적을 위해 예약된 필드임

7) URG(Urgent)

긴급 데이터가 TCP 페이로드(payload)에 포함되어 있음을 알리는 필드로, 만약 이 비트가 1이면 우선적으로 처리한다

8) ACK(Acknowledgement)

TCP 세그먼트들에 대한 수신 확인을 알리기 위해 사용되며, 이 비트가 1이면 수신 확인 응답 번호 이전까지의 모든 세그먼트들을 잘 받았음을 의미한다

9) PSH(Push)

푸시 요청으로 긴급 데이터가 아닌 데이터를 빨리 처리하도록 요청하는 제어 비트

10) RST(Reset)

TCP 세션을 리셋 하기 위한 제어 비트이다

11) SYN(Synchronization)

통신을 개시하고자 하는 두 호스트 간의 세션을 초기화하고 순서 번호를 동기화하기 위한 제어 비트

12) FIN(Final)

TCP 세션의 전송 종료 시 사용하는 제어 비트이다

13) 윈도우 크기(Windows Size)

상대측으로부터 수신 확인 응답 번호의 수신 없이 전송할 수 있는 데이터의 양을 지정하는 필드

14) TCP 체크섬(TCP Checksum)

헤더와 세그먼트에 의해 전송되는 데이터에 대한 오류 검사를 하기 위한 필드

15) 긴급 포인터(Urgent Pointer)

TCP 페이로드 내의 어떤 곳에 긴급한 데이터가 있는지를 명시하기 위한 필드로 URG가 1로 설정되어 있을 경우에 유효하다

16) 옵션(Option)

최대 40바이트까지 옵션 정보가 있을 수 있으며, TCP 통신과 관련된 여러 가지의 추가적인 옵션이 위치하는 필드이다

4. UDP 헤더

UDP는 TCP와 마찬가지로 전송 계층에서 동작하며 포트 번호를 기반으로 통신

TCP와 달리 수신한 데이터에 대한 수신확인 응답을 하지 않는다

TCP보다 헤더가 간단하며, TCP에서 지원하는 다양한 데이터 흐름 제어 기능을 수행하지 않는다

송수신 절차가 비교적 간단하고, 오류 제어 기능은 제공하고 있으므로 소량의 데이터 전송이나 실시간 데이터 전송에 효과적으로 사용되고 있다

UDP는 송수신 장치 간에 비연결형(Connection-less) 서비스를 지원한다

비연결형 서비스를 하게 되면 데이터 그램 간의 전후 관계를 고려하지 않고 전송

UDP도 TCP와 마찬가지로 Well-Known Port를 기반으로 통신

1) 출발지 포트 번호(Source Port Number)

출발지 호스트의 포트 번호를 정의한 16비트 필드이며 임의 번호를 사용

포트 번호는 0에서 65535의 범위 내에 있다

2) 목적지 포트 번호(Destination Port Number)

목적지 호스트의 포트 번호를 정의한 16비트 필드이며, 대부분 Well-Known Port Number를 사용

어떠한 서비스에 접속하느냐에 따라 일반적으로 미리 정해져 있는 번호

3) 길이(Total Length)

헤더와 데이터를 포함한 UDP 데이터 그램의 전체 길이를 나타낸다

4) 체크섬(Checksum)

헤더와 데이터를 포함한 사용자의 데이터 그램에 대한 오류 검사를 하기 위한 필드이다

5. IP 헤더

OSI 참조 모델의 3계층인 네트워크 계층에서 사용되며, 패킷을 출발지에서 목적지까지 전달하는 데 사용한다

IP는 최선형(Best Effort) 서비스를 이용하여 패킷을 전달하지만 목적지까지 확실히 패킷이 도착하는 것은 보증하지 않는다

그렇기 때문에 도중에 패킷이 손실될 수 있다

IP 프로토콜이 가지는 최선형 서비스의 단점을 보완하기 위하여 상위 계층의 TCP와 같은 신뢰성 있는 프로토콜의 도움을 받아 이러한 단점을 보완할 수 있다

IP는 네트워크 사정상 목적지 장치에 도착한 패킷들이 순서대로 도착하지 않을 수 있다

v4가 사용되었다가 주소 부족 문제로 인해 v6가 대안으로 제시되었다

IP는 비신뢰성을 가지고 있으므로, 데이터 흐름에 관여하지 않는다

현재 인터넷에서 주로 사용되는 표준 프로토콜은 IPv4이다

1) 버전(Version)

IP가 어떤 버전을 사용하는지 나타낸다

2) 헤더 길이(Header Length)

옵션을 포함할 경우, 최대 60byte까지 사용할 수 있으며, 최소 단위는 20byte

3) TOS(Type of Service)

우선 순위를 나타내는 필드이며, 3비트의 Precedence 값 4비트의 서비스 유형 지정 비트, 그리고 사용되지 않는 1비트가 합쳐 8로 구성되어 있다

4) 전체 길이(Total Length)

헤더와 데이터를 포함한 패킷의 전체 길이를 나타낸다

5) 식별자(Identification)

생성되는 패킷마다 부여되는 고유 번호

패킷은 2계층 프로토콜의 최대 전송 단위(MTU) 값에 따라 여러 개의 Fragment로 분할하고, 원래의 패킷으로 재조립하고자 할 경우, 이 식별자 값을 기준으로 사용

6) 플래그(Flags)

IP 패킷의 분할 가능 여부와 마지막 프래그먼트인지 아닌지를 알리기 위해 사용

7) 분할 위치(Fragment Offset)

하나의 패킷이 여러 개의 프래그먼트로 분할될 때 원래 패킷 어디에 있었는지 명시

이 값을 이용하여 원래의 패킷으로 재조립

8) TTL(Time-to-Live)

패킷의 루핑 현상을 막기 위하여 사용하며, 패킷의 수명을 나타낸다

라우터를 지날 때마다 1씩 감소되며, TTL 값이 0이 되면 패킷을 폐기한다

9) 프로토콜(Protocol)

패킷에 캡슐화 되어 있는 상위 계층 PDU가 어떤 프로토콜을 사용하는지 명시하는 필드

TCP 세그먼트이면 6을, UDP 세그먼트이면 17의 값을 가진다

10) 헤더 체크섬(Header Checksum)

IP 헤더의 오류 여부를 검사하기 위한 필드

11) 출발지 IP 주소(Source IP Address)

v4인 경우, 32비트 길이의 출발지 장치의 IP 주소를 의미한다

12) 목적지 IP 주소(Destination IP Address)

v4인 경우, 32비트 길이의 목적지 장치의 IP 주소를 의미한다

13) 옵션(Option)

패킷의 전송 경로를 포함한 IP 프로토콜의 동작 옵션을 정의하는 필드이다

6. 라우터 및 스위치

라우터, 스위치, 무선 AP(Access Point)와 같은 시스코 제품들은 IOS(Internetwork Operation System)를 사용한다

IOS는 시스코 장치들의 운영체제이면서 시스템 소프트웨어로 모든 시스코 제품에 설치되어 있다

동일한 네트워크 장치라도 운영체제의 라이선스가 어떻게 구성되어 있는지에 따라서 특정 기능이 지원되지 않을 수도 있다

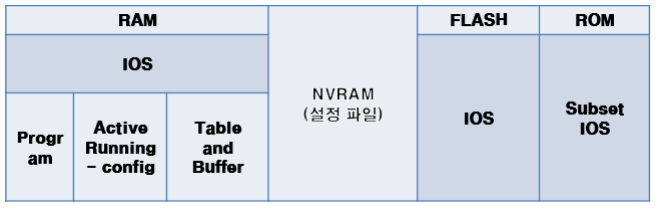
라우터와 스위치는 GUI 또는 CLI의 2가지 모드를 통해서 설정할 수 있다

GUI 설정에는 다음과 같은 별도의 전용 프로그램을 통해 설정한다 – SDM, CCP, ASDM

PC의 하드디스크에 설치되어 실행되거나 라우터의 Flash 메모리에 설치되어 http 기반으로 실행할 수 있다

패킷트레이서에도 GUI와 CLI 설정을 지원하지만, GUI의 경우 패킷트레이서에서만 사용하는 형식이고 장치에 설정할 수 있는 명령어도 극히 제한적이다. 따라서 본 강의의 모든 라우터 및 스위치 설정은 CLI 형태로 진행된다

라우터 및 스위치의 메모리 구조는 다음과 같다



라우터나 스위치의 전원을 켜면 POST(Power On Self Test)를 실시하여 장치의 이상 유무를 판단한다

이상이 없으면 ROM에 있는 Bootstrap(Booting loader)를 RAM으로 옮긴다

Bootloader가 FLASH에 위치해 있는 IOS를 RAM으로 옮긴다

RAM으로 옮겨진 IOS는 실행되며, 정상적으로 부팅이 되고 난 후, NVRAM에 있는 설정 파일을 적용한다

만약 설정 파일이 없으면 디폴트로 아무것도 설정이 안 된 상태로 부팅된다

FLASH 메모리에 있어야 할 IOS가 없거나 손상되었으면 ROM에 있는 Subset IOS를 실행시켜 부팅하는데, 이를 롬몬(rommon) 모드라고 한다

롬몬 모드는 IOS를 업데이트하거나 암호를 잊어버렸을 경우 강제로 진입하여 문제를 해결할 수 있다

PC에서 라우터 및 스위치 접속을 위하여 Console 케이블을 사용한다

Connections에서 콘솔 케이블을 선택한 후, PC의 RS232 포트와 스위치 또는 라우터의 콘솔 포트와 연결한다

7. 라우터의 역할

라우터는 OSI 7계층에서 3계층에 속하는 장치이다

라우터는 패킷을 전달하는 장치이며, IP 주소를 기반으로 한다

라우터가 패킷을 전달할 때 참고하는 것은 라우팅 테이블이다

라우터는 ARP 테이블도 가지고 있다

라우터는 라우팅 프로토콜을 기반으로 라우팅 테이블을 생성하고, 라우팅 프로토콜의 특성에 따라 보내는 패킷의 경로가 다를 수 있다

라우터는 LAN과 WAN을 연결시켜주는 중간자 역할을 하고 있다

원격 접속을 통해서도 라우터에 접근할 수 있다

Telnet: 가장 일반화된 원격 접속 프로토콜이나 보안에 약한 취약점이 있다

SSH: Telnet과 같은 일을 하지만, 주고받는 데이터를 암호화한다

원격 접속은 HTTP를 사용하여 설정하는 것도 가능하다

8. 스위치의 역할

스위치는 OSI 7계층에서 2계층에 속하는 장치이다

스위치는 프레임을 전달하는 장치이며, MAC 주소를 기반으로 한다

스위치가 프레임을 전달할 때 참고하는 것은 MAC 테이블이다

스위치는 라우터의 이더넷 포트와 연결

PC들과도 이더넷으로 연결

시뮬레이션 모드를 통해 PC에서 어떻게 목적지까지 전달되는지 쉽게 알 수 있다

스위치는 MAC 테이블을 기반으로 Frame을 전달하는 장치이다

라우터는 라우팅 테이블을 기반으로 Packet을 전달하는 장치이다

9. 라우터 및 스위치의 기본 설정

Ctrl + C를 입력하면 바로 대화형 설정이 종료

라우터 및 스위치의 명령어 모드에서 “?”를 사용하면 설정할 수 있는 명령어들을 볼 수 있다

10. 라우터 및 스위치 설정 모드

라우터 및 스위치는 동일하게 세 가지의 모드를 가진다

사용자 모드(User mode): 제한된 명령어만 사용이 가능하며, 장비 설정 불가 -> Router>

관리자 모드(Privileged mode): 현재 동작하고 있는 장비의 설정 내용 등을 볼 수 있음 -> Router#

전역 설정 모드(Global Configuration mode): 장비 설정 가능 -> Router(config)#

각 모드에서 사용 가능한 명령어가 있으므로, 라우터 및 스위치 설정 시에 모드를 잘 확인하여야 한다

ex) 전역 설정 모드의 명령어는 사용자 모드에서 실행될 수 없음, 관리자 모드의 명령어는 사용자 모드에서 실행될 수 없음

사용자 모드에서 관리자 모드로 변경하기

Router> enable 또는 en

관리자 모드에서 전역 모드로 변경하기

Router# configure terminal 또는 conf t

라우터와 스위치의 경우, 명령어 자동 완성 기능을 제공한다. 예를 들어 라우터의 사용자 모드에서 “en”이라고 명령어를 입력하고 키보드의 TAP 키를 누르면 명령어의 나머지인 “able”이 자동으로 완성되는 형식이다

11. 라우터 및 스위치 암호, 호스트 네임 등의 기본 요소 설정

1) Clock 설정

Router> en => 사용자 모드에서 관리자 모드로 변경하는 명령어

Router# show clock => 라우터의 시간을 보여주는 명령어

Router# clock set 12:00:00 02 may 2022 => clock set 명령어로 날짜 변경

2) 장치 이름 설정

시스코 장치들은 공장 출하 시에 기본적으로 장치의 명칭을 이름으로 가진다

ex) 라우터 => Router 스위치 => Switch

관리자가 원하는 별도의 장치 이름을 부여할 수 있음

문자(숫자, 기호)로 시작할 수 있고, 63글자를 넘길 수 없고, 띄어쓰기 포함 불가

hostname 명령어를 사용하여 변경

3) 암호 설정

장치 관리자는 인가되지 않은 사용자의 접근을 막기 위하여 암호를 사용할 수 있다

Console 암호: 사용자 모드로 들어가기 전에 물어보는 암호이다

Enable Password: 사용자 모드에서 관리자 모드로 들어갈 때 물어보는 암호이다

Enable Secret: Enable Password와 동일한 암호이나, 암호가 라우터에 저장될 때 암호화되어서 저장되고, Enable Password와 동시에 선언되면 Enable Secret 암호가 우선순위를 가진다

VTP Password: 텔넷을 사용하여 접속할 때 물어보는 암호이다

보안 상의 이유로 라우터나 스위치에서 암호를 입력 받을 때, 사용자가 암호를 입력해도 아무런 표시가 나지 않음

각 모드에 맞게 암호를 입력하고 엔터를 누르면 됨

콘솔 암호를 cisco로 설정하시오

R1> en

R1# conf t

R1(config)# line console 0

R1(config-line)# password cisco

R1(config-line)# login

R1(config-line)# exit

enable 암호로 cisco를 설정하시오

R1(config)# enable password cisco

enable secret 암호로 class를 설정하시오

R1(config)# enable secret class

4) 라우터 IP 설정

라우터는 LAN 구간을 연결하는 Ethernet 구간, 라우터와 라우터를 연결하는 WAN 구간으로 나뉘어짐

라우터의 LAN 인터페이스가 GigaEthernet일 경우

R1(config)# interface gi0/0

R1(config-if)# ip address IP 주소 서브넷 마스크

R1(config-if)# no shutdown

라우터의 LAN 인터페이스가 FastEthernet일 경우

R1(config)# interface fa0/0

R1(config-if)# ip address IP 주소 서브넷 마스크

R1(config-if)# no shutdown

Serial 인터페이스가 DCE일 경우

R1(config)# interface serial0/2/0

R1(config-if)# ip address IP 주소 서브넷 마스크

R1(config-if)# clock rate 64000

R1(config-if)# no shut

5) 원격 접속 설정

기본 구성이 끝났으면 라우터에 텔넷 접속 설정을 한다

R1# conf t

R1(config)# line vty 0 4

R1(config-line)# password cisco

R1(config-line)# login

R1(config-line)# exit

숫자 0과 4는 텔넷 접속으로 라우터에 접속할 수 있는 인원 설정

ex) 0, 1, 2, 3, 4이므로 첫 숫자와 마지막 숫자를 사용하여 최대 5명이 라우터에 접속할 수 있음

6) 설정 내용 확인

라우터나 스위치에 설정된 내용을 확인하거나 어떻게 동작하고 있는지 확인하기 위해 show running-config 또는 show run 명령어를 사용한다

12. RIPv1의 개념

RIP은 v1과 v2가 있다

Distance Vector 라우팅 프로토콜이며, 라우팅 정보 전송을 위해서 UDP 520번을 사용한다

설정이 간단하고 소규모 네트워크에 사용하기 좋다 (Hop Count 15까지만 지원)

그러므로 대규모의 네트워크보다는 소규모의 네트워크에 적합하다

목적지로 가는 경로 중에서 라우터를 가장 적게 거치는 경로를 선택하게 된다

가장 적은 Hop-Count를 가진 경로가 최적의 경로가 된다

네트워크 경로 설정 시 위의 한 가지 요소만 보며, 링크의 속도를 반영하지 않는다

복잡한 네트워크에서 사용될 경우 비효율적인 라우팅 경로가 만들어질 수 있다

최대 홉 카운트가 15 즉 패킷이 라우터를 15번만 거칠 수 있기 때문에 대형 네트워크에서 사용하는 것은 불가능하다

RIP으로 Full-Routing이 되어 있고, PC0에서 PC1으로 Data를 전송할 경우 R1은 R3로 보내는 것이 속도가 훨씬 빠름에도 불구하고 R2에게 직접 전송한다

30초 주기로 자신의 라우팅 테이블을 이웃하는 장치들에게 브로드캐스트 한다

복잡한 네트워크의 경우 라우팅 테이블을 주고받는 RIP의 특성으로 인해 상당한 오버헤드 트래픽이 발생하는 단점이 있다

서브넷 마스크 정보가 없는 Classful 라우팅 프로토콜

VLSM을 지원하지 않는다

13. RIPv2의 개념

RIPv2는 Classless 라우팅 프로토콜이며, 네트워크 정보와 함께 서브넷 마스크의 정보도 함께 전달한다

라우팅 정보의 전달을 위해 브로드캐스트 주소를 사용하지 않고 Multicast 주소인 224.0.0.9를 사용한다

나머지 내용은 v1과 동일하다

각 라우터에서 네트워크 경로 정보에 대한 인증을 할 수 있다 -> 보안성 강화

라우팅 경로에 대한 Auto Summary(자동 축약)를 사용하며, 이 기능이 필요 없을 때는 Manual Summary(수동 축약)를 사용할 수 있으며, no Auto Summary 명령어를 사용하여 자동 축약 기능을 해제할 수 있다

수렴 시간(Convergence Time)

Convergence: 네트워크에 변화가 생길 경우 모든 라우터가 네트워크 변화 상태에 대해 정확하고 일관된 정보를 유지하는 것

Convergence Time: 네트워크에 변화가 생겼을 경우 그 변화된 정보를 서로 인식하고 수정하는 시간

Convergence Time은 라우팅 프로토콜별로 틀리다

Convergence Time은 짧을수록 좋다

RIP 같은 경우는 Convergence Time이 30초로 느리다. 때문에 경우에 따라서 Routing Loop 문제가 발생할 수 있다

위에 설명된 몇 가지 항목을 제외한 나머지는 v1과 같다

14. RIPv1과 RIPv2의 차이점

RIPv1 RIPv2

Distance Vector Distance Vector

AD: 120 AD: 120

Metric: Hop(1-15) Metric: Hop(1-15)

Update: 30초 Update: 30초

Classful Routing Classless Routing

VLSM(X) VLSM(O)

Broadcast update Multicast(224.0.0.9) Unicast

인증(X) 인증(O)

15. RIPv1과 RIPv2 설정

1) RIPv1 설정

Router> enable

Router# conf t

Router(config)# router rip

-> 라우팅 프로토콜로 RIP을 사용할 것을 선언

Router(config-network)# network 네트워크 주소

-> network 명령어로 라우터에 직접 연결되어 있는 네트워크 주소를 입력

2) show ip int brief 명령어를 사용하여 RIP 설정 이전에 라우터 인터페이스의 설정이 정상적으로 되어 있는지 확인하고, 라우터 인터페이스의 IP 주소를 기억하고 있기 어려우므로 이를 정확히 참조

3) RIPv2 설정

RIPv2는 모든 설정 과정이 RIPv1과 같고, 단순히 Version 2 명령어만 추가하면 됨

4) RIPv2 설정 확인

Debug ip rip 명령어를 통한 확인

5) Passive-Interface 명령어

Passive-Interface 명령어를 사용하여 gi0/0으로 RIP 정보가 가지 않도록 설정

R1> en

R1# conf t

R1(config)# router rip

R1(config-router)# passive-interface gi0/0

Passive-Interface 설정 확인

R1# debug ip rip

16. IPv4

IP 프로토콜은 OSI 참조 모델의 제3계층인 네트워크 계층에서 정의

IP는 최선형(Best Effort) 서비스를 이용하여 패킷을 전달

패킷이 목적지에 도착한다고 보장하지 않음

IPv4는 32bit이며, 4개의 옥텟(Octet)으로 구분되어짐

사설 IP 대역과 공인 IP 주소 대역이 있으며, 외부로 통신하기 위해서는 반드시 공인 IP 대역의 주소를 사용하여야 함

주소 대역이 A, B, C, D, E 형태로 나뉘어져 있으며, 장치에 할당하여 사용 가능한 주소 대역은 A, B, C이며, D는 Multicast 용으로 사용되고, E의 경우 연구용으로 남겨 놓음

17. IPv6

IPv6는 IPv4가 주를 이루고 있는 현재의 네트워크 환경에서 생기는 주소 부족 문제를 해결하기 위하여 사용

IPv6는 128bit의 16진수를 사용하여 주소를 표현하며 주소 자동 생성

IPv6는 주소 생략이 가능하다

각 필드에서 선행하는 0은 생략이 가능하다

ex) 0207 => 207, 00BC => BC, 0000 => 0

연속된 0은 모두 삭제할 수 있으며, 이때 2개의 이중 콜론으로 이를 나타내며, 주소당 한 번만 사용할 수 있다

ex) BCAF:0:0:0:0:5641:F9FF:4102 => BCAF::5641:F9FF:4102

18. IPv4와 IPv6의 특징

구분 IPv4 IPv6

주소 길이 32비트 128비트

표시 방법 8비트씩 4개 부분으로 나누어 16비트씩 8개 부분으로 나누어

10진수로 표시 16진수로 표시

주소 개수 약 43억 개(2의 32승) 2의 128승 개

주소 할당 방식 A, B, C, D 등의 클래스 단위로 네트워크 규모, 단말기 수에 따라

비순차적 할당 순차적 할당

브로드캐스트 주소 있음 없음(멀티캐스트 주소 사용)

보안 IPSec 별도 설치 IPSec 지원

19. IPv6 헤더

버전(Version): IP 프로토콜의 버전을 나타낸다

트래픽 클래스(Traffic Class): IPv6 패킷의 클래스나 우선순위 표시

플로우 레이블(Flow Label): 패킷들의 어떤 특정한 흐름에 대한 특성

페이로드 길이(Payload Length): 페이로드 길이를 표시

다음 헤더(Next Header): 기본 헤더 다음에 어떤 종류의 확장 헤더가 오는지 표시

홉 제한(Hop Limit): 라우터를 지날 때마다 이 값을 1씩 감소시키며 0이면 폐기

20. IPv4 주소의 구조

32비트의 크기를 가지며, 32비트를 8bit씩 나눠서 4개의 옥텟으로 구분

IPv4 주소는 2진수로 표현되며, 이를 10진수로 변환하여 사용한다

IPv4는 2의 32승 개 즉, 4,294,967,296 개의 주소를 가진다

네트워크 장치는 고유의 IP 주소를 가진다

주소가 같은 다른 장비가 존재하면 IP 주소가 충돌하므로 데이터 통신이 이루어질 수 없다

네트워크에 연결된 장치에 할당된 IP 주소는 유일한 주소여야 한다

IP 주소는 Network 부분과 Host 부분으로 구분되어진다

ex) IP 주소 = Network ID(고정된 bit) + Host ID(고정되지 않은 bit)

Network ID에 1을 할당하고, Host ID에 0을 할당한 값을 Subnet Mask라 한다

ex) A Class는 Network ID가 8bit이고 Host ID가 24bit이다. 따라서 A Class 기본 서브넷 값은 11111111.00000000. 00000000. 00000000이므로 이를 10진수로 변환하면 255.0.0.0이 된다

IP 주소를 Network 부분과 Host 부분으로 구분해 주는 역할을 하는 것이 Subnet Mask이며 IPv4의 주소 범위 중 A Class는 8bit, B Class는 16bit, C Class는 24bit의 기본 서브넷 값을 가진다

ex) 255.0.0.0 => A Class Default Subnet Mask

255.255.0.0 => B Class Default Subnet Mask

255.255.255.0 => C Class Default Subnet Mask

서브넷 값은 2진수로 표현했을 때, 1이 연속적으로 나와야 한다

21. Class별 분류

1) A Class 주소(0.0.0.0 ~ 127.255.255.255)

0과 127로 시작하는 주소는 예약되어 있으므로 사용할 수 없다

따라서 1.0.0.0 ~ 126.255.255.255가 A Class의 실 주소 범위이다

기본 서브넷 마스크 값은 8bit(255.0.0.0)이다

10.0.0.0 ~ 10.255.255.255의 범위는 사설 IP 대역이다

Network 숫자: 126, 네트워크 당 Host 숫자: 16,777,214개(2의 24승 – 2)

2) B Class 주소(128.0.0.0 ~ 191.255.255.255)

기본 서브넷 마스크 값은 16bit(255.255.0.0)이다

172.16.0.0 ~ 172.31.255.255의 범위는 사설 IP 대역이다

Network 숫자: 16.384개, 네트워크 당 Host 숫자: 65,654개

3) C Class 주소(192.0.0.0 ~ 223.255.255.255)

기본 서브넷 마스크 값은 24bit(255.255.255.0)이다

192.168.0.0 ~ 192.168.255.255의 범위는 사설 IP 대역이다

Network 숫자: 2,097,152개, 네트워크 당 Host 숫자: 254개

4) D Class 주소(224.0.0.0 ~ 239.255.255.255)

멀티캐스트에 의해서 사용되는 주소 대역이다

일반 장치에 할당되어 사용할 수 없다

5) E Class 주소(240.0.0.0 ~ 255.255.255.255)

연구 등의 용도로 예약되어 있는 주소이다

일반 장치에 할당되어 사용할 수 없다

6) 네트워크 ID와 Broadcast 주소

호스트 필드를 모두 0으로 채우면 Network ID이다

호스트 필드를 모두 1로 채우면 Broadcast 주소이다

ex) IP 주소가 203.230.7.1/24일 경우

11001011.11100110.00000111.00000001

11111111.11111111.11111111.00000000 => 서브넷 마스크

11001011.11100110.00000111.00000000 => 네트워크 ID

11001011.11100110.00000111.11111111 => 브로드캐스트 주소

네트워크 ID와 Broadcast 주소는 IP 주소로 사용할 수 없다

사용 가능한 IP 주소: 203.230.7.1 ~ 203.230.7.254

(총 호스트의 숫자 – 2) = 사용 가능한 IP 주소의 숫자

ex) 256 – 2 = 254

22. 서브넷팅

IP 주소 자원을 효율적으로 사용하기 위하여 사용

Class별로 지정되어 있는 기본 서브넷 마스크를 사용하지 않고, 네트워크 상황에 따라 적당한 크기의 서브넷 마스크를 사용하여 IP 주소를 사용

호스트 비트로 할당된 bit 일부를 subnet bit로 지정한다

호스트 필드의 bit를 빌려 Network를 나눈다

C Class의 경우는 아래의 표를 사용하여 간단하게 서브넷팅 할 수 있다

비트 25 26 27 28 29 30 31 32

서브넷 마스크 128 192 224 240 248 252 254 255

호스트 개수 128 64 32 16 8 4 2 1

23. VLSM

Subnet 된 Network를 다시 서브넷팅 하는 것을 말한다

가장 큰 조건부터 차례로 서브넷팅을 하여야 한다

24. EIGRP

EIGRP의 전신인 IGRP는 IOS 12.2 이후로는 지원을 안 함. 현재 12.4 또는 15.0 이상의 IOS가 대부분이므로 사실상 사용하지 않는다고 봐도 무방함

Advanced Distance Vector 라우팅 프로토콜

Distance Vector의 장점 및 Link-State의 장점을 모두 가지고 있음

Cisco Router 전용 라우팅 프로토콜

224.0.0.10의 멀티캐스트 주소를 사용한다(RIPv2는 224.0.0.9)

Classless Routing Protocol: 서브넷 마스크, VLSM 지원

Partial Update: 주기적인 업데이트를 하지 않고, 경로 정보가 변화될 경우에만 업데이트를 실시한다

MD5 인증 기능이 제공되며, 설정 및 관리가 용이하다

DUAL(Diffusing Update Algorithm) 알고리즘을 사용하여 최적 경로를 선출

25. EIGRP에서 사용하는 Table

1) Neighbor Table (#show ip eigrp neighbor)

인접성을 맺은 라우터의 정보들을 볼 수 있다

2) Topology Table (#show ip eigrp topology)

목적지까지 도달할 수 있는 모든 경로들의 경우의 수가 저장되어 있고 최적 경로에 장애가 생기면 dual 알고리즘이 Topology Table을 분석하여 그 다음의 최적의 경로를 선출한다

3) Routing Table (#show ip route eigrp)

목적지에 도달할 수 있는 경로 중 최적의 경로가 등록되어 있는 테이블이며, 이 라우팅 테이블을 근거로 라우팅이 이루어진다

26. 링크 상태 라우팅 프로토콜(Link State Routing Protocol)

링크 상태 라우팅 프로토콜은 다익스트라(Dijkstra) 또는 최단 경로 우선(SPF: Shortest Path First) 알고리즘을 사용하여 목적지까지의 최단 경로를 계산한 후 이를 기초로 패킷을 전송하는 방법이다

각 라우터에 직접 연결되어 있는 링크의 정보를 같은 네트워크의 모든 라우터들에게 알려주어야 하는데 이를 위해 링크 상태 패킷(LSP: Link State Packet)을 생성

이 정보를 받은 라우터들은 링크 상태 정보를 참조하여 최단 경로를 결정한다

다익스트라 알고리즘은 출발지 장치에서 목적지 장치까지의 모든 링크를 이용하는데 소요되는 비용(Cost)를 누적 계산하여 이 값이 가장 작게 나오는 경로를 선택하는 방식이며, 이 방식을 사용하는 라우팅 프로토콜은 OSPF가 있다

27. OSPF(Open Shortest Path First)

IP Network 기반에서 동작하는 IGP Protocol 중 가장 널리 사용되고 있는 Link-state Algorithms를 사용하는 표준 개방형 Protocol (RFC 2328)

네트워크 토폴로지의 변화가 빠르다

네트워크 토폴로지에 변화가 생기며 변화된 부분, 증가된 부분만 업데이트를 실시함

업데이트할 내용이 없더라도 30분 간격의 링크 상태 재생(Link-State Refresh)를 이용하여 Update 정보를 주기적으로 교환

RIP이나 EIGRP보다 설정이 복잡하지만 계층화된 라우팅 동작을 수행하기 때문에 중대규모 네트워크에 사실상 가장 많이 사용되는 라우팅 프로토콜이다

OSPF는 라우팅 정보 업데이트 시 224.0.0.5와 224.0.0.6의 멀티캐스트 주소를 사용한다(EIGRP 224.0.0.10, RIPv2 224.0.0.9)

OSPF는 링크의 비용을 메트릭으로 사용하여 목적지 네트워크의 경로를 결정한다

OSPF 대역폭에 따른 비용 값

인터페이스 유형 및 대역폭 비용(Cost)

56 Kbps 1785

64 Kbps 1562

128 Kbps 781

T1 (1.544 Mbps) 64

E1 (2.048 Mbps) 48

Ethernet (10 Mbps) 10

FastEthernet (100 Mbps) 1

GigabitEthernet (1000Mbps) 1

10-GigabitEthernet 1

OSPF에서는 라우팅 테이블의 생성, 유지, 관리를 위하여 다음과 같은 5가지의 독특한 패킷 유형을 사용한다

Hello: 설정된 이웃 라우터들과의 인접 관계를 맺기 위해 사용하는 패킷

DBD(Database Description): 링크 상태 정보에 대한 데이터베이스. OSPF 라우터들 간의 데이터베이스 동기화를 검사하기 위해 사용한다

LSR(Link-State Request): DBD를 받은 후, 자신에게 없는 경로가 있을 경우 이 경로에 대한 상세한 링크 상태 정보를 요청할 때 사용한다

LSU(Link-State Update): LSR에 대한 응답으로 사용되며, 이웃 라우터와 경로 비용과 같은 경로 상태 정보를 LSA(Link State Advertisement)로 전송하는 것을 포함한다

LSAck(Link-State Acknowledgement): 상기의 다른 패킷 유형에 대한 수신 확인을 위해 사용한다

OSPF의 동작 방식

OSPF를 설정한 Router끼리 Hello Packet을 교환해서 Neighbor를 맺는다

Neighbor Router 간 라우팅 정보(LSA)를 서로 교환하고, 전송받은 LSA를 Link-State Database에 저장

LSA를 모두 교환하고 SPF(Shortest Path First) 또는 다익스트라(Dijkjstra) 알고리즘을 이용해서 각 목적지까지의 최적 경로를 계산 후 Routing table에 올린다

그 후에도 주기적으로 Hello packet을 교환하면서 정상 동작을 확인

네트워크의 상태가 변하면 다시 위의 과정을 반복해서 Routing table을 생성

OSPF의 Process-ID는 1부터 65535 사이의 숫자를 사용할 수 있으며, 이 번호가 라우터마다 동일할 필요는 없다

28. Static 라우팅 프로토콜

정적 경로 설정이라고 하며, 관리자가 네트워크 토폴로지를 보고 우회 경로를 비롯한 모든 경로를 직접 수동으로 설정한다

네트워크 상황 변화에 동적으로 대처할 수 없으며, 관리자가 직접 수동으로 확인하고 상황 변화에 대처하여야 한다

위와 같은 이유로 잘 사용이 되지 않는 것 같지만, 실제의 네트워크 설정에 폭 넓게 사용되고 있다

정적 경로는 동적 경로와 비교하여 설정이 간단하고, 네트워크 장비의 리소스를 적게 사용한다는 장점이 있다

대규모의 네트워크보다는 소규모의 네트워크에서 운영된다

중 및 대규모의 네트워크에서는 동적 라우팅을 설정한 후, 정적 라우팅을 설정하여 라우팅 프로토콜을 이중으로 운영하는 경우도 있다

29. Static 라우팅 설정 방법

Router(config)# ip route network-address subnet-mask {ip-address | exit-interface}

ip route: 정적 경로 설정을 위한 명령어이다

network-address: 목적지 네트워크의 네트워크 주소이다

subnet-mask: 목적지 네트워크의 서브넷 마스크이다

ip-address: 목적지 네트워크로 패킷을 전송하기 위해 사용해야 할 이웃 라우터의 인터페이스 IP 주소를 지정한다

exit-interface: 목적지 네트워크로 패킷을 전송하기 위해 사용해야 할 라우터의 출력 인터페이스를 지정한다

30. 디폴트 정적 경로(Default Static Routing) 설정

패킷의 출입 경로가 하나밖에 없는 네트워크에 대해서는 디폴트 정적 경로 설정을 적용할 수 있다

R1(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address]의 형식을 사용하여 설정한다

ip route: 정적 경로 설정을 위한 명령어이다

0.0.0.0 (앞): 쿼드 제로(quad-zero) 네트워크 주소를 의미한다

0.0.0.0 (뒤): 쿼드 제로(quad-zero) 서브넷 마스크로 어떤 IP 주소라도 서브넷 마스크로 마스킹을 하게 되면 바로 앞에 있는 네트워크 값 0.0.0.0이 될 것이다. 따라서 모든 IP 주소를 의미한다

exit-interface: 디폴트 네트워크로 가기 위한 출력 인터페이스이다

ip-address: 디폴트 네트워크로 가기 위한 이웃 라우터 인터페이스의 IP 주소이다

31. WAN

1) WAN은 LAN의 지리적인 범위를 넘어서 동작하는 데이터통신 네트워크

LAN과 WAN의 기본적인 차이는 기업체나 조직이 WAN Carrier Network Service를 사용하기 위해 WAN Service Provider에 가입해야 하는 것

WAN은 Internet에 접근하기 위해 Carrier Service가 제공하는 Data Link 사용

WAN은 동일조직 및 다른 조직의 지역간, 외부서비스, 원격사용자간 연결

WAN은 Voice, Data, Video와 같은 다양한 형태의 Traffic 전달

2) 가입자 구내 장비를 CPE(Customer Premises Equipment)라 부름

가입자는 CPE를 소유하거나 서비스 제공자로부터 CPE를 임대

구리 선이나 광케이블은 CPE를 서비스 제공자의 가까운 교환기나 CO(Central Office)와 연결 -> “Local Loop” or “Last-mile”이라 부름

3) Data를 전달하는 Local Loop를 위하여 Modem과 같은 장치 필요

Local Loop로 Data를 싣는 장치를 DCE라 부름

DCE로 Data를 전달하는 가입자 장치를 DTE라 부름

DCE는 DTE를 위한 Interface 제공: DTE/DCE Interface

HSSI(High-speed Serial Interface), V.35와 같은 물리계층 프로토콜 사용

4) WAN Link는 다양한 속도 제공: bps, Kbps, Mbps, Gbps

일반적으로 Full Duplex

5) WAN은 Service Provider로부터 제공되는 통신링크를 통해 서로 연결된 LAN의 집합체

통신링크는 LAN에 직접 접속 불가 -> 다양한 Interfacing 장비 필요

6) 전송할 Data를 가진 LAN-based Computer는 LAN과 WAN Interface를 모두 가진 Router로 Data 전송

Router는 적절한 WAN Interface로 Data 전달을 위해 3계층 주소정보 사용

7) 통신링크는 적절한 형식의 Signal 필요

디지털 라인을 위해 CSU/DSU 필요 -> Router Interface Card로 내장 가능

Local Loop 구간이 Analog인 경우 Modem 필요

신호의 변복조에 의해 음성대역의 전화회선으로 Data 전송

8) WAN은 OSI 참조모델의 1, 2계층에 초점

WAN 표준은 물리계층의 전송방법 및 물리주소, 흐름제어, Encapsulation을 포함한 데이터링크 계층의 요구사항 규정

9) 물리계층 프로토콜은 통신서비스 제공자가 제공하는 서비스에 접속하는 전기적, 기계적, 기능적, 절차적인 방법 기술

10) 데이터링크 계층 프로토콜은 원격지에 Data를 전송하기 위한 Encapsulation 방법 및 Frame을 전송하기 위한 구조 정의

ISDN, Frame Relay, ATM(Asynchronous Transfer Mode)

11) WAN 연결

임대 회선(Leased line): 점 대 점 연결 혹은 전용 연결이라고 하며, 대부분 동기 시리얼 연결로 T3/E3 또는 45M로 연결되어 있다

회선 교환(Circuit-switched): 사용자가 회선을 사용하는 동안은 계속 회선이 유지되지만, 재연결을 할 때마다 같은 회선을 사용하는 것은 아니다

패킷 교환(Packet-switched): point-to-point 또는 point-to-multipoint 링크를 서비스 제공업체에서 제공하는 공유된 인터네트워크망을 이용해서 송신지에서 수신지로 전달한다.

셀 교환(cell-switched): 고정된 길이의 셀을 이용하여 가상 회선을 통해 전송

12) WAN의 2계층 캡슐화 연결

Cisco HDLC(High-Level Data Link Protocol): 시스코 라우터는 cHDLC가 기본 캡슐화 방법이며, 점 대 점 연결과 회선 교환에 이용된다

PPP(Point-to-Point Protocol): 동기 및 비동기 회선을 포함하여 다양한 물리적 인터페이스 표준을 통해 라우터 사이와 호스트 및 네트워크 사이의 연결에 사용되는 표준 프로토콜. PAP, CHAP와 같은 보안 메커니즘 제공

프레임 릴레이(Frame-relay): X.25를 보다 발전시킨 것으로 기존의 불안정한 통신 링크 간의 에러 제어나 흐름 제어와 같은 불필요한 기능을 제거하여 빠른 전송속도를 보장할 수 있도록 함

ATM(Asynchronous Transfer Mode): 다양한 서비스 유형의 데이터를 포함한 셀을 전달하는 국제 표준이며 고정길이(53byte) 셀 교환

13) PPP PAP (Password Authentication Protocol)

양방향 인증과정을 통한 간단한 인증 방법 제공

처음 연결하는 과정에서만 인증을 거치기 때문에 CHAP보다 보안에 약함

평문 형태로 전송되므로 해킹 공격에 취약한 단점이 있음

14) PPP CHAP (Challenge Handshake Authentication Protocol)

3way Handshake 인증과정을 통한 주기적인 인증 실시

PAP 인증에 비해서 뛰어난 보안성을 제공

MD5 형태로 전송

32. VLAN

1) 스위치 장치는 LAN 구간에서 주로 사용되는 장치이며 아래와 같이 분할할 수 있다

L2 스위치: MAC 주소를 기반으로 프레임을 전달하는 장비로서 보통 스위치라고 하면 바로 L2 스위치를 말한다

L3 스위치: L2 스위치의 특성을 가지고 있으면서 L3 라우팅 기능을 가지고 있는 스위치이다

L4 스위치: TCP, UDP 등을 스위칭 하면서 RTP 등의 헤더를 사용하여 응용 프로그램에서 사용하는 프로토콜 중 어떠한 것을 우선적으로 전달할 것인지 결정할 수 있으며, 서버나 네트워크의 트래픽에 대한 로드 밸런싱(Load Balancing)을 하는 스위치

L7 스위치: URL, E-mail 제목 등의 패턴을 분석하여 패킷을 전달. 높은 보안성과 정교한 QoS 및 로드 밸런싱 지원

2) 다양한 종류의 스위치는 네트워크를 구성할 때 어떻게 디자인되는지가 중요

3) 스위치를 이용하여 네트워크를 구성할 경우 계층적인 구조를 사용해 구성하면 안정성 및 확장성은 물론 성능까지 향상되는 결과를 나타냄

4) 스위치는 세 개의 계층으로 나눌 수 있다

액세스(Access) 계층

액세스 계층은 가장 밑에 있는 계층으로서 PC, 프린터, IP 전화기, 허브, 무선 AP 등과 같은 장치가 직접적으로 연결되는 계층을 말한다. Port Security, VLAN(Voice 포함), PoE(Power of Ethernet), Link Aggregation, QoS 등의 기능을 주로 설정한다

분산(Distribution) 계층

액세스 계층으로부터 받은 프레임을 코어 계층으로 전송하기 전의 계층으로써 주로 트래픽을 분리하는 역할을 하는 계층이다. ACL, IP 라우팅, 이중화 구성, QoS 등의 기능을 주로 설정한다

코어(Core) 계층

인터넷과 연결되어 있어 외부와 패킷을 주고받을 수 있는 계층으로써, 어떠한 정책도 선언되지 않는다. 코어 계층의 주된 역할은 패킷을 빠르게 전달하는 것이다.

5) 스위치는 MAC Table을 기반으로 프레임을 전달하며, MAC Table이 만들어지는 순서는 아래와 같다

1 단계: MAC Table 초기화 상태

스위치가 부팅을 마치고 동작 모드로 들어가는 상태이다. 이때 스위치의 MAC Table에는 어떠한 내용도 없다

2 단계: Flooding

3 단계: Frame 전달

4 단계: MAC Table 완성

6) 스위치는 자신이 브로드캐스트 프레임을 받으면 Flooding을 수행하므로, 네트워크 크기가 클수록 Flooding 되는 데이터들이 늘어나는 문제점을 가진다

7) 위와 같은 문제점을 해결하기 위하여 VLAN(Virtual LAN)이 사용된다

8) VLAN은 브로드캐스트 도메인을 분할하여 브로드캐스트 트래픽으로 인한 장비 성능 저하를 막을 수 있다

9) 서로 다른 VLAN에 속한 장치들은 상호 통신이 불가능하기 때문에 보안에도 도움이 된다. 만약 다른 VLAN에 속한 장치들이 통신을 하려고 하면 반드시 L3 장치의 중계를 거쳐야만 한다

10) 기본적으로 스위치의 모든 포트는 VLAN 1번에 속해 있다

11) VLAN은 1부터 1005까지의 번호로 나눌 수 있으며, 이 번호를 VLAN ID라 한다

12) 1002~1005번은 예약되어 있으며, 이 번호를 제외한 1~1001번까지 VLAN ID로 사용할 수 있다

13) 1002~1005번은 삭제할 수 없으며, VLAN 정보는 vlan.dat 파일에 저장되고, 이 파일은 스위치의 Flash에서 확인할 수 있다

33. VLAN 구성하기

1) VLAN 생성 방법

VLAN Database를 사용하는 방식

Switch# vlan database

Switch(vlan)# vlan 10 name VLAN\_10

Switch(vlan)# vlan 20 name VLAN\_20

Switch(vlan)# vlan 30 name VLAN\_30

전역 설정모드에서 생성하는 방법

Switch> en

Switch# conf t

Switch(config)# vlan 10

Switch(config-vlan)# name VLAN\_10

Switch(config-vlan)# vlan 20

Switch(config-vlan)# name VLAN\_20

Switch(config-vlan)# vlan 30

Switch(config-vlan)# name VLAN\_30

2) VLAN 생성 확인

Switch> en

Swtich# show vlan

3) VLAN 생성 후, 토폴로지를 참조하여 VLAN 1번에 속해 있는 포트를 알맞은 VLAN으로 옮긴다

Switch> en

Switch# conf t

Switch(config)# int fa0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

34. Trunk

Frame Tagging을 사용하는 Trunking Protocol은 보다 빠른 Frame의 전달, 보다 쉬운 관리 가능

링크상으로 전송되는 Frame은 소속 VLAN을 알려주는 Tagging 필요

Ethernet Segment를 위한 2가지의 Tagging Scheme

ISL: 시스코 고유의 프로토콜

802.1Q: IEEE 표준

Cat2950 또는 2960에서 트렁크 설정하는 방법 (ex fa0/0)

Switch(config)# interface fa0/1

Switch(config-if)# switchport mode trunk

35. 가상 인터페이스

VLAN을 나누는 것은 곧 Broadcast Domain을 나누는 것으로, 서로 IP 주소가 다름

VLAN이 나누어져 있는 토폴로지에서 서로 다른 VLAN과 통신을 하기 위해서는 반드시 L3 장치를 거쳐야 함

VLAN별로 각각의 물리적 회선이 연결되는 것은 불가능함

VLAN은 스위치에 설정되므로, 스위치와 연결된 LAN 구간의 라우터 Ethernet 포트에 가상 인터페이스를 만들어 각각의 VLAN에 Default-Gateway를 할당함

라우터와 연결되는 스위치 포트는 트렁크를 설정하므로 여러 VLAN Frame을 한 개의 회선으로 주고받을 수 있도록 설정함

라우터의 Ethernet 포트에는 4,294,967,295개의 가상 인터페이스 생성 가능

가상 인터페이스를 SVI(Switch Virtual Interface)로 표현하기도 함

라우터 가상 인터페이스는 실제 인터페이스를 기반으로 구성함

Router(config)# int gi0/0

Router(config-if)# no shut

Router(config-if)# exit

Router(config)# int gi0/0.1 => 가상 인터페이스는 생성하자마자 활성화됨