후니의 쉽게 쓴 시스코 네트워킹(개정판) 정리

작성자 : 빨간펜(http://cafe.naver.com/securitygogo)

최종작성일 : 2006년 12월

e-mail : moongchiza@nate.com

Part 1. 네트워크 세상에 들어서며

■ 네트워킹이란 서로 연결하는 것이다. 정보의 공유, 자원의 공유를 하기위해서 서로 연결된 장비들끼리 대화를 주고 받을수 있게 하는것을 말한다. 터미널이라고 부르는 단말기 비슷하게 생긴 장비 여러대를 호스트 컴퓨터에 붙여서 사용을 해오다가 서버만 공유하는 것이 아니라, 프린터도 공유하고 또 한 호스트만 공유하지 않고 여러 호스트를 공유하게 되다 보니 지금의 네트워킹으로 발전하게 되었다.
정리하면 네트워킹이란 장비들을 서로 대화가 가능하도록 묶어주는 것이다.

■ 인터넷(InterNet)의 인터(Inter)라는 말은 연결을 의미한다. 인터넷이란 '여러 개의 네트워크를 묶었다'는 의미를 가진다. 앞서 말했던 네트워크처럼 네트워크를 좀더 많은 사람들과 정보를 공유하고자 서로 연결하기 시작해서 발전한것이 인터넷의 시작이다.

■ 인터넷의 특징
1. 하나의 프로토콜만 사용한다.
   - A는 한국말로 B는 영어로 말을하면 서로 대화가 안되는데 이것을 프로토콜이 다르다고 한다.
     즉, 하나의 언어, 하나의 프로토콜만을 사용해야하는데 인터넷에서 사용하는 TCP/IP라는것이있다
2. 익스플로러나 넷스케이프와 같은 웹 브라우저를 이용해서 인터넷을 탐험한다.
3. 인터넷에는 없는 정보가 없다.

■ 인트라넷(IntraNet)
- Intra는 '내부의'라는 뜻으로 내부의 네트워크라는 말이다. 사내 업무도 인터넷처럼 웹 브라우저만을 이용하게 만든것이다.
- 인트라넷 역시 TCP/IP란 프로토콜을 사용한다.

■ 엑스트라넷(ExtraNet)
- 기업의 인트라넷을 그 기업의 종업원 이외에도 협력 회사나 고객에게 사용할수 있도록 한것이다.

Part 2. 네트워크와 케이블 그리고 친구들

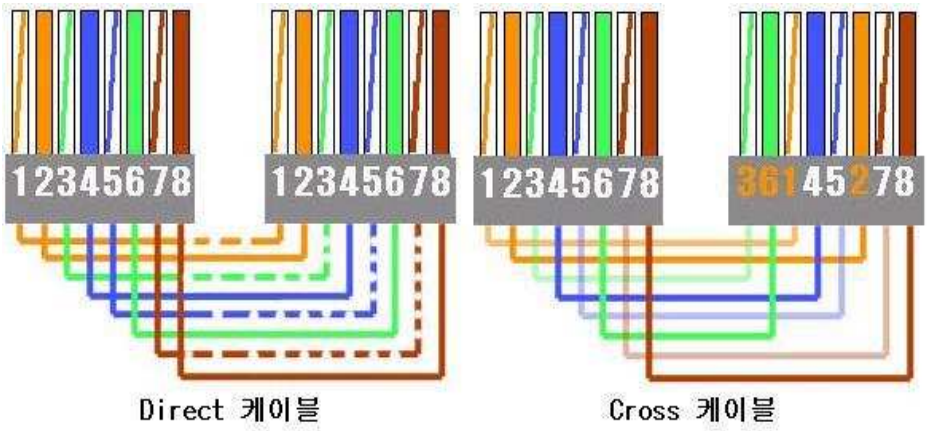
■ LAN(Local Area Network) - 어느 한정된 공간에서 네트워크를 구성한다는 것이다.
예를들어 한 사무실에 30대의 컴퓨터를 네트워크로 구성한다면 이를 사무실에 LAN을 구축한다고한다.
■ WAN은 Wide Area Network의 약자로 멀리 떨어진 지역을 서로 연결하는 경우를 말한다.
■ 이더넷(Ethernet) - 네트워킹의 한 방식인데 CSMA / CD라는 프로토콜을 사용해서 통신을 하는것이 가장 큰 특징이라고 볼 수 있다.
예) 토큰링(TokenRing), FDDI방식, ATM방식도 있다.
■ CSMA/CD는 'Carrier Sense Multiple Access/Collision Detection'을 줄여서 부르고 간단히 말하면 "대충 알아서 눈치로 통신하자"이다. 네트워크 상에 나타나는 신호(캐리어)가 있는지를 감시하는데 이것을 Carrier Sense라고 한다. 캐리어가 감지되면 데이터를 보내지 않고 기다리게된다. 그러다가 네트워크에서 통신이 없어지면 눈치를 보고 자기 데이터를 네트워크상에 실어서 보내게된다.
두 개 이상의 PC나 서버가 동시에 네트워크상에 데이터를 실어 보내는 경우가 있는데 이를 Multiple Access(다중 접근)이라고 한다. 두 개의 장비들이 데이터를 동시에 보내려다 부딪치는 경우를 충돌(콜리전, Collision)이라한다. 이더넷에서는 데이터를 네트워크에 실어서 보내고 나서 콜리전이 발생했는지 점검을 하는데 이를 Collision Detection(충돌 감지)라고 한다. 콜리전이 발생하게 되면 랜덤한 시간동안 기다린 다음 다시 데이터를 전송하게 된다.

■ 토큰링(TokenRing) - 그 네트워크에서 오직 한 PC, 즉 토큰을 가진 PC만이 네트워크에 데이터를 실어 보낼 수 있는 방식이다. IBM대형 컴퓨터들이 있는 곳에서 많이 사용중.
*이더넷의 일반적인 속도는 10Mbps이고 토큰링은 4Mbps/16Mbps이다.

*UTP케이블에 대해 알아보자.
우선 TP케이블이란 Twisted-pair, 즉 꼬인것을 말한다. 페어는 두가닥.
UTP는 Unshielled(언쉴드, 감싸지않은)TP를 말한다.
STP는 Shieled로 케이블의 주위를 어떤 절연체로 감싸서 만든것을 말한다. 좀더 비싸고 성능이 좋다.
- 카테고리 1 : 주로 전화망에 사용
- 카테고리 2 : 데이터를 최대 4Mbps의 속도로 전송
- 카테고리 3 : 10 Base T 네트워크에 사용되는 케이블
- 카테고리 4 : 토큰링 네트워크에서 사용. 최대 16Mbps의 속도로 전송
- 카테고리 5 : 최대 100Mbps를 지원하는 Fast Ethernet용으로 사용.
  기가비트 표준이 완성되어 기가비트 속도전송이 가능.

10 Base T에서 **10**이란 속도를 나타내는데 10Mbps의 속도를 지원하는 케이블을 의미한다.
Base란 말은 Baseband용 케이블을 말하고 케이블종류로 베이스밴드와 브로드밴드가 있는데
베이스밴드는 디지털 방식이고, 브로드밴드는 아날로그 방식이다.
T란 TP케이블을 나타내는데 우리가 사용하는 UTP케이블을 말한다.
맨뒷자리가 10 Base **5** 숫자이면 이 숫자는 최대 통신거리를 나타낸다. (500미터)
- 10 Base T : 10Mbps로 통신 최대 전송 거리 100미터인 UTP케이블로 카테고리 3,4,5사용 RJ45잭사용
- 10 Base FL : 10Mbps로 통신하는 광케이블. FL(fiber-optic)이 광케이블을 말함.
  ST 커넥터라는 것을 사용해서 연결하고 싱글 모드 또는 멀티 모드 케이블을 사용
- 10 Base 2 : 10 Mbps통신, 최대 200미터(정확히는 185미터). Thin케이블이라불렷고 BNC커넥터 사용
  전기줄 두께의 까만 색 케이블이고 옛날 UTP잭 옆에 동그란곳에 끼워서 사용
- 10 Base 5 : 10Mbps통신 최대 500미터. 두꺼워서 thick케이블. 옐로우 케이블이라부름.
  주로 백본케이블, 즉 중앙망 용으로 천장 위에 설치하고 트랜시버 케이블을 이용.
  랜카드 중에 AUI인터페이스(15핀 사다리꼴)를 가진 것이 이 케이블과 연결
- 100 Base TX : 카테고리 5 UTP 케이블을 사용. 100Mbps통신, 최대거리 100미터케이블
- 100 Base T2 : 이 방식을 쓰면 카테고리 3,4,5를 전부 사용해서 100M를 구하여 쓰임
- 100 Base T4 : 카테고리 3 케이블로 100Mbps용으로 사용할 때 만드는 케이블.
  대신 다른 케이블은 2페어를 사용하지만 이것은 4페어를 전부 사용함
- 100 Base FX : 100Mbps광케이블을 이용해서 구현. 전송거리는 2km ~ 10km까지 가능.
  SC라는 네모난 커넥터를 이용하여 접속
- 1000 Base SX : 1000Mbps의 속도로 전송. short wavelength라는 광케이블사용.
  최대전송거리 270미터~550미터
- 100 Base T : 1000Mbps로 UTP케이블을 통해 전송 최대거리는 100미터인 케이블 스펙.
  카테고리 5 케이블을 사용. 구성하기 위해 4페어를 다 사용해야함.

*기가비트의 경우 1000 Base LX/LH같은 스펙은 광케이블을 사용해서 최대 10킬로미터까지 전송가능.
케이블의 경우 속도가 빨라지면 빨라질수록 전송 거리는 점점 짧아진다.



Direct 케이블은 허브와 PC, 라우터와 허브의 연결등에 사용
Cross 케이블은 PC끼리나 허브끼리의 연결에 사용

■ MAC(Media Access Control)

우리가 편지를 주고 받을때 집 주소를 적는데 이에 상응하는 것이 MAC주소이다. 네트워크 상에서 서로를 구분해서 통신하기 위한 주소이다.

IP주소만 있으면 모든 통신이 일어날 것 같지만 IP주소를 다시 MAC으로 바꾸는 절차(ARP:Address Resolution Protocol)가 필요하다.

- 1옥테트 = 8비트를 묶음

네트워크에 붙는 각 장비들은 48비트(6옥테트)의 주소를 갖는데 이 주소는 랜카드 또는 네트워크 장비에 이미 고정되어 있는 주소이고 전 세계에서 유일한 주소이다. 이것을 MAC 어드레스 or 하드웨어 주소라함.
모든 랜상의 디바이스들은 반드시 유일한 MAC 어드레스를 가져야 한다.
MAC어드레스는 8자리마다 하이픈, 콜론, 점으로 구분되어지는데
예) 00-60-97-8F-4F-86 00:60:97:8F:4F:86 0060.978F.4F86
2진수로 표현하면 48자리이고 너무 길어서 16진수로 표시함.
앞쪽 6개의 16진수(00-60-97)가 벤더, 즉 생산자를 나타내는 코드로 이 코드를 OUI(Organizational Unique Identifier)라고한다. 회사마다 틀리기 때문에 어느 회사제품인지 알수있다. 나머지 6자리는 회사에서 각 장비에 분배하는 Host Identifier인데 시리얼 넘버라고 보면된다.

■ 유니캐스트 - 현재 네트워크상에서 가장 많이 사용되는 통신 방식으로 특정 목적지의 주소 하나만을 가지고 통신하는 방식이다. 그 목적지 주소가 아닌 다른 PC들은 CPU성능을 저하시키지 않는다.
그 이유는 자신의 맥어드레스가 아니라고 판단되면 랜카드가 이 프레임을 버리기 때문이다.

■ 브로드캐스트 - 로컬 랜 상에 붙어있는 모든 네트워크 장비들에게 보내는 통신방식이다.
그래서 전체적인 트래픽도 증가하게 되고 이 패킷을 받은 모든 랜카드가 CPU로 전송하여 전체 PC의 성능도 떨어뜨리게 만드는 결과를 가져온다.

■ 멀티캐스트 - 보내고자 하는 그룹 멤버들에게만 한 번에 보낼 수 있는 통신방식이다.
스위치나 라우터가 이 멀티캐스트 기능을 꼭 지원해야 한다는 제약이 있다.

■ OSI 7 Layer (1,2,3계층만 다룸)

OSI는 Open Systems Interconnection의 약자이고 통신에 관한 국제적인 표준기구인 International Organization for Standardization(ISO)에서 통신이 일어나는 과정을 7단계로 나누었다.
7개의 단계별로 표준화하여 그 효율성을 높이기 위해서 사용
- Application Layer(어플리케이션 계층)
- Presentation Layer(프레젠테이션 계층)

- Session Layer(세션 계층)
- Transport Layer(트랜스포트 계층)
- Network Layer(네트워크 계층)
- Data Link Layer(데이터 링크 계층)
- Physical Layer(물리계층)

왜 나누었을까?

데이터의 흐름이 한눈에 보이고 문제 해결하기가 편리하고 층별로 표준화가 되어있어 여러 회사 장비를 써도 네트워크가 이상 없이 돌아간다.

▪ Physical Layer - 전기적, 기계적, 기능적인 특성을 이용해서 통신 케이블로 데이터를 전송
통신단위는 비트이고 단지 데이터만 전달할 뿐 무엇인지 모른다.
대표장비로는 통신 케이블, 리피터, 허브등이 있다.

▪ Data-Link Layer - 물리계층을 통하여 송수신되는 정보의 오류와 흐름을 관리하여 안전한 정보의 전달을 수행하도록 도와주는 역할. 오류찾고, 재전송기능, 맥어드레스로 통신할수 있게 해준다
대표장비로 브리지, 스위치등이 있다.

▪ Network Layer - 데이터를 목적지까지 가장 안전하고 빠르게 전달(라우팅). 경로를 선택하고 주소를 정하고 경로에 따라 패킷을 전달해주는 역할. 스위치중에서도 라우팅기능을 수행하는 스위치가 있고 Layer 3스위치라고도한다. 대표장비 라우터.

*컴퓨터는 프로토콜로 말한다.

프로토콜이란 규약,협약이런 뜻인데 컴퓨터끼리 이런 프로토콜이 서로 같은 것끼리만 통신이 가능하다.

TCP/IP(Transmission Control Protocol/Internet Protocol)

IPX(Internetwork Packet Exchange)

AppleTalk - 매킨토시가 사용

Part 3. TCP/IP와의 만남

■ TCP/IP를 모르면 인터넷을 아는 게 아니다?

대표적인 프로토콜로 Apple Talk, IPX, NetBEUI, TCP/IP

이중 TCP/IP가 인터넷 때문에 현재 가장 많이 사용되고 있다

ARPANET에의해서 처음 개발되었고 각각의 네트워크에 접속되는 호스트들은 고유의 주소를 가지고 있어서 자신이 속해 있는 네트워크뿐만 아니라 다른 네트워크에 연결되어 있는 호스트까지도 서로 데이터를 주고받을 수 있도록 만들어져 있다.

이때 사용하는 호스트들의 고유주소는 Internet Network Information Center(InterNIC)에서 관리분배한다

똑같은 IP를 사용하게 되면 충돌했다고 표현을 한다.

이와 달리 같은 IP를 쓰는 경우도 있는데 내부 네트워크에서는 공인되지 않은 IP주소를 사용하고, 인터넷으로 나갈 때만 공인 주소(즉 유일한 IP)를 가지고 나가는 방식인 NAT(Network Address Translation)나 동일한 IP 주소를 가지고 여러 명이 인터넷에 접속하면서 포트 넘버만을 바꾸는 PAT등이 있다.

공인주소를 나눠주고 관리해주는 기관은 NIC(Network Information Center)이다.

IP주소는 210.126.12.99

네 자리의 십진수로 되어 있고 중간에 점이 찍혀있다. 한자리는 최대 255까지되고 이진수 32개로 구성

컴퓨터는 컴퓨터가 알아들을 수 있는 이진수로만 이해를 한다.

IP는 총 2의 32승개로 되어있고 IP주소방식인 버전4가 주소가 부족해서 버전6이 사용될 예정이다

▪ DHCP(Dynamic Host Configuration Protocol)서버 - 이 서버가 있는 네트워크에 연결만 하면 자동으로 부여받을 수 있도록 되어있다. PC마다 하나하나 IP주소를 미리 지정해 놓지 않아도 된다.

Part 4. 네트워크 장비들에 관한 이야기

■ 랜카드의 세팅

예전엔 수동으로 다했지만 지금은 플러그 앤 플레이를 지원해 주어서 랜 카드를 꽂고 부팅시키면 인식하고 설치, 연결하여준다.

▪ 종류로는 데스크탑용과 PCMCIA방식으로 노트북용이 있다.

데스크탑용은 PCI방식을 가장 많이 쓰고 이전에는 ISA방식을 많이 사용했음.

서버급 PC에서는 EISA방식의 버스를 사용.

▪ 속도에 따라 크게 10메가, 100메가, 10/100메가, 1기가로 나누는데 지금까지는 10Mbps용 랜카드를 많이 사용. 요즘은 100Mbps용이나 10/100Auto-sense카드도 많이 사용되고 있다.

▪ 접속하는 케이블의 종류에 따라 TP포트를 가진 랜카드, BNC나 AUI포트를 가진 랜카드, 광케이블과 접속하는 랜카드로 나눌수있다. 예전에는 AUI, BNC 방식을 많이 사용했었고 한동안은 콤보방식도 사용하지만 요즘은 UTP타입을 사용하는것이 일반적임.

■ 허브(HUB) - 직사각형의 상자에 구멍이 뚫려있는 모양으로 되어있고 개수에 따라 몇포트다라고한다

이더넷용이냐, 토큰링용이냐가 있고 또 이더넷 허브도 속도에 따라 그냥 허브(10Mbps)와 패스트(100Mbps)허브가 있다. 허브는 네트워크에서 약방에 감초처럼 없으면 안 되는 가장 기본이 되는 장비중 하나이다. 허브를 한마디로하면 멀티포트 리피터라고 할수있는데 포트가 여러개 달린 장비인데, 한 포트로 들어온 데이터를 나머지 모든 포트로 뿌려준다.

리피터라는것은 데이터 전송시 거리의 제약 때문에 중간에서 들어온 데이터를 다른 쪽으로 전달해 주는 역할을한다.

허브를 고를때는 안정성을 가장중요하게보고 사후 AS 또한 중요하다. 한 번의 콜리전이 발생하면 연결되어있는 모든 PC들이 영향을 받기 때문에 허브만으로 연결하는것은 한계가 있다.

▪ 허브의 종류

- 인텔리전트(Intelligent)허브 : NMS(네트워크 관리시스템)을 통해서 모든 데이터를 분석할수 있고 앉아서 멀리 있는 허브의 동작을 감시하고 조정까지도 가능하다. 문제의 PC가 연결된 포트를 찾아내어 자동으로 Isolation(현 네트워크에서 분리시켜서 따로 고립시킴)시켜 버린다.

또 분리된 포트는 허브에서 램프로 표시되기 때문에 바로 알수 있고 이기능을 Auto Partition이라한다.

- 더미(Dummy) 허브
- 세미더미 허브 - 더미 허브인데 인텔리전트허브와 연결하면 자기도 인텔리전트 허브가된다.

스태커블 허브라는것은 쌓을수 있는 허브를 말한다.

▪ 허브의 끝과 스위치의 시작

허브의 한계에서 아무리 빠른속도를 쓴다고 하더라도 어느 한순간에는 한 녀석만이 데이타를 보낼수 있다는거..즉 허브에 연결된 한 피시에서 발생하는 콜류젼이 다른 피시들에도 영향을 주는 콜류젼 도메인(영역)이 그 허브에 연결된 모든 피시들이다 그래서 콜류젼 도메인이 너무 커지는 상황을 항상 조심해야 한다 콜류젼 도메인이 너무커지게되면 콜류젼에 의해 영향을 받는 피시가 너무 많아지고 또 통신의 속도가 점점 떨어지게 된다. 이러한 문제 즉 콜류젼 도메인을 작게 나누기 위해서 나온 장비가 바로 스위치 인데 어디서는 스위칭 허브라고도 하는데 뒤에 허브라는 말이 사람들로하여금 조금 헷갈리게 한다. 이게 허븐지 스위친지 암튼 스위치란 말이 들어가면 일단 스위치라고 생각. 스위치는 예를 들어 1번 포트에 연결된 피시가 2번 포트에 연결된 피시와 데이타를 주고받는 동안에도 3번 포트에 연결된 피시와 4번 포트에 연결된 피시가 서로 데이타를 주고받을 수 있게 한 장비 이다. 즉 1,2번 사이에서 통신이 일어나면 나머지는 기다려야하는 허브와는 달리 다른녀석들도 동시에 통신이 가능한것이다. 이게 스위치와 허브의 가장 큰 차이다. 그래서 우린 스위치의 경우 각각에 연결된 피시가 독자적으로 10Mbps 또는 100Mbps의 속도를 갖는다고 이야기 한다. 허브보다는 스위치가 좋은데 콜류젼도메인을 작게 나누어주기 때문이다

■ 브리지/스위치의 기능
- Learning : 브리지나 스위치는 자신의 포트에 연결된 A라는 PC가 통신을 위해 프레임을 보내면 이 PC의 맥 어드레스를 읽어서 자신의 맥 어드레스 테이블에 저장하고 나중에 참고하여 다리를 건너게할지를 결정한다.
- Flooding : 들어온 포트를 제외한 나머지를 모든 포트로 뿌리는 것을 의미한다. 브로드캐스트나 멀티캐스트의 경우에도 발생함
- Forwarding : 브리지가 목적지의 맥 어드레스를 자신의 브리지 테이블에 가지고 있고, 이 목적지가 출발지의 목적지와 다른 세그먼트에 존재하는 경우에 일어난다. 한마디로 목적지가 어디 있는지를 알고 있는데 그 목적지가 다리를 건너가야만 하는 경우에 발생한다. 해당 포트로만 프레임을 뿌린다.
- Filtering : 브리지를 못 넘어가게 막는다는 뜻인데, 브리지가 목적지의 맥 어드레스를 알고 있고, 출발지와 목적지가 같은 세그먼트 상에 있는 경우 브리지를 건가지 않아도 통신이 일어날 수 있기에 이때 필터링을 하게된다. 이 기능 때문에 허브와는 다르게 콜리전 도메인을 나누어 줄수 있다.
- Aging : 나이를 먹는다는 말인데 새로운 맥 어드레스를 기억하는데 디폴트는 5분(300초 값조정가능)이다. 에이징이랑 이것에 관련된 타이머이다. 어떤 맥 어드레스를 브리지 테이블에 저장하고 나면 그때부터 Aging이 가동되어서 저장한 후 300초가 지나도록 더 이상 그 출발지 주소를 가진 프레임이 들어오지 않으면 브리지 테이블에서 삭제시킨다.
** 브리지와 스위치의 차이점
1. 이름이 다르다.
2. 가격이 다르다. - 스위치가 브리지보다 비싸다
3. 인기도가 다르다. - 스위치가 브리지보다 잘팔린다.
*** 실무적인차이점
1. 스위치는 처리 방식이 하드웨어로 이루어지기 때문에 소프트웨어적으로 프레임을 처리하는 브리지에 비해서 훨씬 빠르다.
2. 브리지는 포트들이 같은 속도를 지원하는 반면, 스위치는 서로 다른 속도를 연결기능을 제공한다
3. 스위치는 브리지에 비해 제공하는 포트 수가 훨씬 많다.
4. 스위치의 경우 cut-through or store-and-forward방식을 사용하는데 비해서 브리지는 오로지 store-and-forward방법만 사용한다.
* store-and-forward : 스위치나 브리지가 일단 들어오는 프레임을 전부 받아들인 다음 처리를 하는방식
* cut-through : 스위치가 들어오는 프레임의 목적지 주소만을 본 다음 바로 전송 처리를 시작하는 방식
* Fragment-Free : 두 방식의 장점을 결합한 방식으로 전체 프레임이 다 들어올 때까지 기다릴 필요가 없다는 측면에서 컷스루 방식을 닮았지만 처음 512비트를 보게되고 에러 감지 능력이 우수하다.

■ Looping - 프레임이 네트워크 상에서 무한정으로 뱅뱅 돌기 때문에 이더넷의 특성상 네트워크가 조용해야 데이터를 전송할 수 있는 다른 녀석들이 계속 네트워크가 조용해지기를 기다리기만 할 뿐 데이터 전송은 불가능해지는 상태를 말한다. 브리지나 스위치에 목적지까지의 경로가 두 개 이상 존재하면 반드시 루핑이 발생한다.
자동으로 루핑을 막아주는 스패닝 트리 알고리즘(Spanning Tree Algorithm)이 필요하다.

■ 폴트 톨러런트(Fault tolerant) - 네트워크 상에 어떤 문제가 발생할 때를 대비해서 미리 장애 대비를 해놓는 것을 말한다.

■ 로드 밸런싱(Load balancing) - 로드를 분산하는 것을 말하는데 인터넷 회선 하나를 이용한 인터넷 접속 대신 인터넷 회선을 두 개 사용하는것이다. 이렇게 되면 데이터들이 두 라인 중 하나르 선택해서 이용하기 때문에 로드가 분산되는 효과를 얻을 수 있다.

■ 스패닝 트리 알고리즘 - 스위치나 브리지에서 발생할 수 있는 루핑을 미리 막기 위해 두 개 이상의 경로가 발생하면 하나를 제외하고 나머지 경로들을 자동으로 막아두었다가 만약 기존 경로에 문제가 생기면 막아놓은 경로를 풀어서 데이터를 전송하는 알고리즘이다. 모든 스위치는 스패닝 트리 알고리즘을 지원하는데 살 때 확인해 보는것이 좋다. 예를 들어 시스코의 이더 채널(Ether-Channel) 기술은 여러 개의 링크가 마치 하나의 링크처럼 인식되게 하는 기술인데 게임방에서 이더 채널이 지원되는 스위치를 구매했다면 평소에도 두 배의 속도를 내고 한 링크가 끊어져도 기다리는 시간이 전혀 없이 링크가 유지되는 장점이 있다.

■ 라우팅이냐 스위칭이냐

가격 : 라우터가 스위치보다 비싸다

속도 : 스위치가 우세. 라우터는 내부에서 처리하는 일이 많아서 스위치보다 패킷처리속도가 느리다

구성의 편리함 : 스위치가 훨씬 구성이 쉽다. 스위치는 전원공급이면 가능

라우터는 라우팅 프로토콜, 네트워크설정 필터링 보안..등 구성을 해야한다.

라우터없이 아주 빠른 스위치로만으로 네트워크를 구성하면 아주 근본적인 문제에 걸리게 되는데 바로 브로드캐스트이다. CPU의 성능을 저하시키기 때문이다.

브로드캐스트 영역 나눌때의 권고사항

IP	약 500노드
IPX	300노드
Apple Talk	200노드

라우터는 로드분배의 기능을 제공해주고 프로토콜이나 데이터의 크기, 중요도 등 여러 상황에 따라 트래픽의 전송 순서를 조정해주는 QoS(Quality of Service)기능도 제공한다.

참고 URL :

http://kin.naver.com/knowhow/entry.php?d1id=8&dir_id=8&eid=1qqX7Ywtil8mN3f5+3V8nT9fdzJmfkl7s

Part 5. IP주소로의 여행

■ IP주소는 총 4개의 옥테트(1옥테트=2진수 8자리)로 이루어짐. 32bit로 구성

■ 시스코 2501의 경우 이더넷 인터페이스 1개, 인터넷과 접속하기 위한 시리얼 인터페이스 2개
시리얼 인터페이스는 DSU또는 CSU라는 전용선 모뎀에 연결됨
이 경우 라우터에 부여해야하는 IP주소는 두 개인데 각 인터페이스에 부여.
- 이더넷용은 부여받은 번호중 하나를 사용
- 시리얼은 인터넷 제공업체에 문의해서 사용

■ IP주소는 네트워크 부분과 호스트 부분으로 나누어진다.
■ 브로드캐스트 영역 - 하나의 PC가 데이터를 뿌렸을 때 라우터를 거치지 않고 받을 수 있는 영역
■ 서로 다른 네트워크에서는 호스트 부분이 같아도 되지만 같은 네트워크에서는 달라야한다.
■ IP주소 중에 네트워크 부분만이 라우터가 라우팅을 할 때 참고하는 부분이다.

클래스	네트워크 번호	호스트수
A	1.0.0.0 ~ 126.0.0.0	16,777,214개
B	128.1.0.0 ~ 191.254.0.0	65,534개
C	192.0.1.0 ~ 223.255.254.0	254개

■ 네트워크가 서로 다른 두 장비 간의 통신은 라우터를 통해서만 가능
- TCP/IP 통신 시에 라우터의 각 인터페이스 역시 IP주소를 부여해 주는 것이 좋음

■ 서브넷 마스크 - 주어진 IP주소를 네트워크 환경에 맞게 나누어 주기위해 씌워주는 이진수의 조합
- IP주소를 가지고 네트워크 부분과 호스트 부분인가를 나타내는 역할을 한다.
- 클래스 A : 255.0.0.0 (기본 서브넷 마스크)
- 클래스 B : 255.255.0.0
- 클래스 C : 255.255.255.0

1101 0010.0110 0100.0110 0100.0000 0001 = 210.100.100.1 -> IP주소
1111 1111.1111 1111.1111 1111.0000 0000 = 255.255.255.0 -> 서브넷 마스크
1101 0010.0110 0100.0110 0100.0000 0000 = 210.100.100.0 -> 서브넷 네트워크

서브넷 마스크가 이진수로 '1'인 부분이 네트워크가 되고 '0'인 부분이 호스트가 되는것을 기억해라.
* 서브네팅 - 하나의 주소를 서브넷 마스크를 씌워서 작은 네트워크로 만드는 것
* 서브넷 마스킹 - 기존 IP주소의 호스트 부분의 일부를 네트워크 부분으로 바꾸는 작업

■ 서브넷 마스크의 기본 성질
- 서브넷 마스크로 만들어진 네트워크는 서로 나뉘어진 서브넷끼리는 라우터를 통해서 통신가능
- 이진수로 썼을 때 '1'이 연속적으로 나와야 하고 중간에 0이 있으면 안된다

■ 서브넷 마스크를 이용해서 나눈 다음에도 둘 사이에 라우터를 놓는 이유는 네트워크 주소의 효율적인 이용과 브로드캐스트 도메인을 줄이기 위해서이다

■ 사용가능한 호스트 수 구하는 공식 = $2^{(\text{HOST비트 수})} - 2$
- 호스트 비트수가 3개일때 $2^3 - 2 = 6$ 사용가능한 호스트 수는 6개이다

■ 서브넷 만들기

201.222. 5. 0	11001001 11011110 00000101 00000000
255.255.255.248	11111111 11111111 11111111 11111000

: 서브넷 만들기, : 호스트 만들기

예) 서브넷 부분에 전부 0을 넣고 호스트 부분에는 000에서 111까지를 넣었을때

201.222.5.0000 0000	:	호스트가 모두 0이므로 네트워크 201.222.5.0
201.222.5.0000 0001	:	201.222.5.1
201.222.5.0000 0001	:	201.222.5.2
201.222.5.0000 0001	:	201.222.5.3
201.222.5.0000 0001	:	201.222.5.4
201.222.5.0000 0001	:	201.222.5.5
201.222.5.0000 0001	:	201.222.5.6
201.222.5.0000 0001	:	호스트가 모두 1인 브로드캐스트 주소 201.222.5.7

■ 서브네트워크는 네트워크 주소는 201.222.5.0, 서브넷 마스크는 255.255.255.248,
호스트 주소는 201.222.5.1 ~ 201.222.5.6까지이고, 브로드캐스트 주소는 201.222.5.7이다
n은 네트워크 부분, h는 호스트 부분 십진수로는 1부터 126까지이다. 디폴트 서브넷은 255.0.0.0

클래스 A : 0nnn nnnn.hhhh hhhh.hhhh hhhh.hhhh hhhh
클래스 B : 10nn nnnn.nnnn nnnn.hhhh hhhh.hhhh hhhh
클래스 C : 110n nnnn.nnnn nnnn.nnnn nnnn.hhhh hhhh
C 클래스 에서 이용할 수 있는 서브넷 마스크(네트워크 부분 생략)

* 서브넷을 만드는 목적 - IP주소를 효율적으로 쓰고 적정한 주소배정을 위함

Part 6. 스위치를 켜라!

■ 스패닝 트리 알고리즘 - 스위치나 브리지에서 발생하는 루핑을 막아주기 위한 프로토콜

- 브리지 ID - 브리지나 스위치들이 통신할 때 서로를 확인하기 위해 하나씩 가지고 있는 번호

8000	0260 8c01 1111
1000 0000 0000 0000	0000 0010 0110 0000 1000 1100 0000 0001 0001 0001 0001 0001
Bridge Priority	맥 어드레스
2바이트(16비트)	6바이트(48비트)

Bridge Priority는 디폴트로 그 중간에 해당하는 값인 32768을 사용

- Path Cost - 길을 가는데 드는 비용, 브리지가 얼마나 가까이 빠른 링크로 연결되는지를 알기위한값
  - 1000Mbps를 두 장비 사이의 링크 대역폭으로 나눈 값을 사용
  - IEEE에서 소수점이 나오지 않도록 하기위해 Path Cost값을 정의

Bandwidth(대역폭)	STP Cost(Path Cost)
4Mbps	250
10Mbps	100
16Mbps	62
45Mbps	39
100Mbps	19
155Mbps	14
622Mbps	6
1Gbps	4
10Gbps	2

■ 스위치의 루핑을 방지하기위한 기본 세 가지

- 네트워크당 하나의 루트 브리지를 갖는다.
- 루트 브리지가 아닌 나머지 모든 브리지는 무조건 하나씩의 루트 포트를 갖는다.
- 세그먼트당 하나씩의 데지그네이티드 포트를 갖는다.

*용어

루트브리지 : 스패닝 프로토콜을 수행할 때 기준이 되는 브리지(스위치)

루트포트 : 루트 브리지에서 가장 빨리 갈 수 있는 포트, 루트 브리지쪽에 가장 가까움

세그먼트 : 브리지 또는 스위치 간에 서로 연결된 링크. 즉 브리지나 스위치가 서로 연결되어 있을때 이 세그먼트에서 반드시 한 포트는 데지그네이티드 포트로 선출함

* 스패닝 트리 프로토콜에서 루트 포트나 데지그네이티드 포트가 아닌 나머지 모든 포트는 다 막아버린다 루트 포트와 데지그네이티드 포트를 뽑는 목적은 어떤 포트를 살릴지 결정하기 위함.

■ 루트 브리지, 루트 포트나 데지그네이티드 포트 정하는 순서

1. 누가 더 작은 Root BID를 가졌는가?
2. 루트 브리지까지의 Path Cost 값은 누가 더 작은가?
3. 누구의 BID가 더 낮은가?
4. 누구의 포트 ID가 더 낮은가?

브리지(스위치도같음)는 스패닝 트리 정보를 자기들기리 주고받기 위해서 특수한 BPDU프레임을 사용

BPDU에는 루트 브리지의BID(Root BID), 루트 브리지까지 가는 경로값(Root Path Cost), 보내는 브리지의 BID인 (Sender BID), 어떤 포트에서 보냈는지 (Port ID)

* 브리지나 스위치가 부팅을 하면 각각의 포트로 BPDU를 매 2초마다 내보내면서 정보를 주고받게된다

■ 스위치에서 대장 브리지 뽑기

- 자기 BID값을 보내고 받은 BID값을 자기의 것과 비교하여 크면 대장으로 받아들이고 작으면 상대 스위치가 대장이 되는 과정으로 이루어진다.
- BID가 낮은 스위치가 루트 브리지가 되며 특정 스위치를 루트 브리지로 만들려면 Bridge Priority의 값을 디폴트 값보다 낮게 설정.

시스코 스위치 Catalyst 2950에서 브리지의 Priority값을 변경시

명령 -> SW-3(config)#spanning-tree 피무 1 priority 100

- 브리지의 Priority를 디폴트 값인 32768에서 100으로 변경

Bridge Priority의 값이 바뀐 것은 'show spanning-tree'명령을 통해서 확인할 수 있다.

■ 졸병 브리지의 루트 포트 선출기

- 루트 브리지가 아닌 스위치의 포트와 루트 브리지의 포트와의 Path Cost가 낮은 한 개의 포트가 루트포트가 된다.

■ 데지그네이티드 포트 뽑기

- 루트 브리지까지의 Path Cost가 낮은 포트가 데지그네이티드 포트가 되며, Path Cost가 같을 경우 4가지 단계를 거친다.
- ND(Non Designated Port) : 즉 루트 포트나 데지그네이티드 포트가 아닌 나머지 포트

■ 스패닝 트리 프로토콜의 5가지 상태 변화

	설 명	데이터전송 유무	맥 어드레스 배우나?	BPDU 주고받나?
Disabled	포트가 고장나서 사용할 수 없거나 Shut Down 상태	X	X	X
Blocking	처음 켜거나 포트를 다시 살렸을 때	X	X	O
Listening	스위치 포트가 루트 포트나 데지그네이티드 포트로 선정	X	X	O
Learning	리스닝 상태에서 15초(디폴트 값) 동안 버티면	X	O	O
Forwarding	러닝 상태에서 15초(디폴트 값)동안 버티면	O	O	O

* 루트 브리지를 어디로 잡느냐에 따라 어떤 링크가 살고, 어떤 링크가 죽을지 결정되는 것처럼 링크의 속도에 따라서도 크게 영향을 받는다. 스위치 네트워크를 디자인할 때 염두해야할것이다.

■ Non Root Bridge들이 지정된 시간 동안 헬로패킷을 받지 못하면 중간 경로에 문제로 생각하고 스패닝 트리를 재편성하는 모드로 들어가게된다.

*용어

- Hello Time : 루트 브리지가 얼마만에 한 번씩 헬로 BPDU를 보내는지에 대한 시간
- Max Age : 브리지들이 루트브리지로부터 얼마 동안 헬로패킷을 받지 못했을 때 루트 브리지가 죽었다고 생각하고 새로운 스패닝 트리를 만들기 시작하는가에 대한 시간
- Forwarding Delay : 브리지 포트가 블로킹 상태에서 포워딩 상태로 넘어갈 때까지 걸리는 시간

p210~212 그림 참조

1. 스위치 C에서 루트브리지로부터 헬로패킷이 들어오지 않음
2. 맥스 에이지 시간이 지나도 E0포트를 통해 들어오지 않음
3. 스위치 C는 스위치 B에서 전달해 준 헬로패킷을 자신의 E1포트로 받아들여 E1포트를 루트포트로 세팅
4. 리스닝 상태에서 15초를 기다리고 러닝상태에서 15초를 그후 포워딩 상태로 넘어가고 이때 기존의 루트 포트로 포워딩 상태였던 스위치 C의 E0포트는 블로킹이됨

■ 스패닝 트리 프로토콜 개선 기법 - RSTP, Port fast, Up-link Fast, Backbone Fast

■ 카타리스트 스위치

*시스템 LED

LED의 색깔	시스템 상태
꺼짐	전원이 공급되고 있지 않은 꺼진 상태
초록색	시스템이 정상적으로 동작중
주황색(노란색)	전원은 공급되나 비정상적으로 작동중

*RPS(Redundant Power Supply) LED : 무정전 전원공급기

LED의 색깔	시스템 상태
꺼짐	RPS가 꺼져 있거나 RPS 자체가 설치되어 있지않음
초록색	RPS가 연결되어 있고 정상적으로 작동중
초록색으로 깜빡임	RPS가 스택에 연결된 다른 스위치를 백업중
주황색(노란색)	RPS가 연결되어 있으나 제대로 동작하지 않음
주황색으로 깜빡임	내부 전원 고장으로 RPS로부터 전원을 공급받아 동작중

*포트모드

포트모드 LED	포트모드	포트상태 LED 표시
STAT	Port Status	각 포트의 상태를 표시(디폴트)
UTIL	Switch Utilization	스위치의 백플레인 사용률 표시
DUPLX	Port Duplex Mode	각 포트의 Duplex 모드 표시(Half/Full)
SPEED	Port Speed	각 포트의 스피드(10/100/1000) 표시

*포트상태 LED

포트모드 LED	포트상태 LED 램프	스위치 상태
STAT (port status)	꺼져 있다.	링크 연결이 안 됨
	초록색	링크 연결됨
	초록색으로 깜빡임	링크가 살아있고 데이터 송수신중
	주황과 초록색으로 번갈아깜빡임	링크 에러 발생
	주황색(노란색)	포트 Disabled or Blocking
UTIL (Utilization)	초록색	현재 스위치의 백본 사용률
	주황색(노란색)	스위치가 켜진후 지금까지 최대 백본 사용률 도달
	초록색과 주황색	만약 스위치의 LED가 모두 초록색이고 주황색이 하나도 없으면 사용률이 50%를 넘었다는 뜻이고, 가장 오른쪽 LED가 꺼져 있으면 스위치 사용률이 25~50% 사이라는 것이고, 가장 왼쪽 LED 하나만 초록색일 경우 스위치는 전체 용량의 0.0488%만을 사용하고 있는 것이다.
DUPLX (Duplex)	꺼져 있다	포트는 Half Duplex 모드로 동작하고 있다
	초록색	포트는 Full Duplex 모드로 동작하고 있다
SPEED (Port speed)	10/100포트만으로 구성되어 있을 경우	
	꺼짐	10Mbps로 포트가 통신중
	초록색	100Mbps로 포트가 통신중
	10/100/1000포트만으로 구성되어 있을 경우	
	꺼짐	10Mbps로 포트가 통신중
	초록색	100Mbps로 포트가 통신중
	초록색으로 깜빡임	1000Mbps(1Gbps)로 포트가 통신중

■ 카타리스트 스위치 구성

- Duplex는 통신방식인데 Half Duplex와 Full Duplex로 나누어지고
  Auto로 설정하면 상대편의 상태에 따라 내가 맞추겠다는 의미이다.
  Speed 역시 상대와 속도가 맞지 않으면 문제가 발생한다.
- IP주소를 세팅하면 나중에 스위치 구성을 확인/변경할 때 텔넷을 이용한 접속이 가능하기 때문에 스위치에 IP주소를 세팅한다
- 네트워크 관리시스템(NMS) 같은 장비에서 스위치를 관리하는 데도 IP주소가 필요함
- '>' 표시 상태를 유저 모드라고한다.
- enable명령을 사용하여 프리빌리지모드에서 스위치의 구성을 확인하고 변경이 가능
  >에서 #(운영자모드)으로 바뀜
- 구성모드로 들어가는 명령은 configure terminal 이다.
  switch#에서 Switch#(config)#으로 바뀜
- exit명령을 사용하여 한 단계씩 빠져나옴
- Switch#(프리빌리지모드)에서 show interface vlan 1을 입력하면 현재 vlan 1에 할당된 IP주소를 알수있다
  IP 주소는 vlan 인터페이스 모드에서 디폴트 게이트웨이는 일반 구성모드에서 세팅

show interface 명령 - 인터페이스데 대한 구성을 볼때

■ 맥 어드레스

- 스위치나 브리지가 출발지에서 들어오는 맥 어드레스를 보고 그것을 자신의 맥 어드레스 테이블에 저장한 다음, 그 주소 테이블에 있는 맥 어드레스를 찾으면 그쪽 포트로만 보내고 나머지 포트는 막아줌으로써 스위치의 기본 기능중 하나인 콜리전 도메인을 막는 역할을 한다.

- Dynamic(자동)방식 : 맥 어드레스를 자동으로 배움 하나를 배우고 사용한지 디폴트로 300초가 지나도록 다시 사용되지 않으면 MAC 테이블에서 삭제됨(용량한계때문)
- 수동(Permanent)방식 : 절대 지워지지 않도록 맥 어드레스를 저장하는 방식
- show mac-address-table 명령 : 맥 어드레스 테이블을 볼때사용

```
          Mac Address Table
-----------------------------------
Vlan    Mac Address      Type       Ports
----  -------------  --------  ------
 1       000.f064.4b91   DYNAMIC    Fa0/1
```

패스트 이더넷 0/1쪽에 0000.f064.4b91맥 어드레스가 있는 것을 배웠다는 뜻
어느 쪽 포트에서든 이 맥 어드레스를 목적지로 갖는 녀석이 들어오면 그 패킷은 바로 패스트 이더넷 0/1쪽으로 보내준다는 의미

■ 스태틱 맥 어드레스 세팅법

- 장점 : 스태틱으로 지정해주면 시간이 지나도 지워지지 않을 뿐만 아니라 다시 이 맥 어드레스를 알기 위해 Learning과정을 거칠 필요가 없다
- 단점 : 주소가 바뀐다고 해도 자동으로 수정 불가, 메모리가 낭비

```
switch(config)#mac-address-table static aaaa.aaaa.aaaa vlan 1 interface fastEthernet 0/24
```

위의 예는 맥 어드레스 aaaa.aaaa.aaaa가 vlan 1을 통해서 들어왔을 때 목적지 인터페이스가 패스트 이더넷 0/24번이라는 것을 스태틱으로 구성

```
Switch# show mac-address-table     <--  맥 어드레스 테이블 확인 명령
        clear mac-address-table     <--  맥 어드레스 테이블 지우는 명령
```

■ 가상 랜(Virtual LAN) - 한 대의 스위치를 마치 여러 대의 분리된 스위치처럼 사용하고, 또 여러 개의 네트워크 정보를 하나의 포트를 통해 전송할수 있음.
하나의 스위이체 연결된 장비들도 브로드캐스트 도메인이 서로 다를 수 있다
- VLAN이 지원되는 라우터와 스위치를 사용하는 경우
▪ 라우터 : 스위치로 하나의 링크만을 이용해서도 3개의 네트워크 정보를 같이 실어보낼수있음
한 선에 여러 개의 네트워크 정보를 보내는 것이 가능해짐
▪ 스위치 : 여러 개의 브로드캐스트 영역을 나누어줄 수 있게됨

■ VLAN에서 꼭 기억해야 할 몇 가지
▪ 스위치에서 지원하는 기능. 허브나 브리지 EH는 라우터에서 지원안함.
▪ 한 대의 스위치를 여러 개의 네트워크로 나누기 위해서 사용
VLAN으로 나누어지면 나누어진 VLAN간의 통신은 오직 라우터를 통해서만 가능
▪ 각 포트들은 서로 다른 3개의 스위치 중 어디에도 속할수 있음.
스위치 안에 있는 스위치 각각을 우리는 VLAN이라 한다
*트렁크포트(Trunk Port) - 하나의 포트를 통해 서로 다른 여러 개의 VLAN을 전송할 수 있게 하는 포트
- 트렁크 포트가 가능하기 때문에 VLAN은 여러 대의 스위치에 구성이 가능.
즉, 같은 VLAN VLAN 1과 VLAN 1, VLAN 2와 VLAN 2, VLAN 3과 VLAN 3끼리만 통신가능
- 패킷에 VLAN정보도 같이 전송되므로 어느 VLAN소속 패킷인지 목적지에서 구분가능

■ 트렁킹 - 모든 VLAN이 하나의 링크를 통해 다른 스위치나 라우터로 이동하기 위해 만듦.
이름표에 따라 ISL 트렁킹과 IEEE802.1Q 방식으로 나눔
▪ ISL - 시스코에서 만든 프로토콜로 시스코 장비끼리만 사용하는 방식
스위치와 스위치간의 링크, 스위치와 라우터 간의 링크에서 여러 개의 VLAN정보를 함께 전달
모든 VLAN에 이름표를 붙임. 이 패킷들은 서로 다른 VLAN에 속하므로 통신은 라우터를 통해야함
▪ IEEE 802.1Q - 트렁킹 표준 프로토콜, 실제 패킷 안에서 어떻게 이름표를 붙이느냐가 서로 다름
Catalyst 2950의 경우 IEEE802.1Q만을 지원함
네이티브 VLAN - 특별 대우를 하는 이름표를 달지 않은 패킷, 모든 스위치 네트워크에서 유일.

■ VTP(VLAN Trunking Protool) - 스위치들 간에 VLAN정보를 서로 주고받아 스위치들이 가지고 있는 VLAN정보를 항상 일치시켜 주기 위한 프로토콜
▪ VTP간에 주고 받는 메시지 3가지 형식
1. Summary Advertisement : VTP서버가 자기에게 연결되어 있는 스위치들에게 매 5분마다 한 번씩 전달하는 메시지
2. Subset Advertisement : VLAN의 구성 변경시 VTP클라이언트로부터 Advertisement Request 메시지를 받았을 때 전송
3. Advertisement Request : 클라이언트가 VTP 서버에게 Summary Advertisement와 Subset Advertisement 를 요청하는 용도로 사용
▪ VTP의 세 가지 모드
1. VTP 서버 모드 : VLAN을 생성, 삭제, 이름변경, VTP 도메인 안에 있는 나머지 스위치들에게 VTP 도메인 이름과 VLAN 구성, Configuration Revision 넘버를 전달해 줄 수 있다.
VLAN정보를 NVRAM에서 관리하고, 꺼졌다 켜져도 정보를 그대로 가지고 있음.
2. VTP 클라이언트 모드 : 서버가 전달해준 VLAN정보를 받고, 그 정보를 자기와 연결된 다른 쪽 스위치에 전달. 스위치가 리부팅하면 정보를 잃게됨
3. VTP 트랜스페어런트 모드 : VTP 도메인 영역안에 있지만 서버로부터 메시지를 받아 자신의 VLAN을 업데이트하거나 자신의 VLAN을 업데이트한 정보를 다른 스위치에게 전달하지 않는다.

Part 7. 라우터만 알면 네트워크 도사?

■ 라우터
- 의미 : 자신이 가야 할 길을 자동으로 찾아서 갈 수 있는 능력을 가진 것
  - 경로결정(Path Determination) : 데이터 패킷이 목적지까지 갈 수 있는 길을 검사하고 어떤 길로 가는 것이 가장 적절한지 결정
  - 스위칭(Switching) : 길이 결정되면 그 쪽으로 데이터 패킷을 스위칭해준다
- 가장 좋은 경로를 결정하기 위해서 라우팅 알고리즘을 사용하고 라우팅 테이블을 만들어서 관리함.
- 시스코에서는 라우터에 들어가는 소프트웨어를 IOS(Internetwork Operation System)라한다

* 용어
  - 인터페이스 : 라우터에 나와있는 접속 가능한 포트(Ethernet과 Serial)
  - Ethernet : 내부 네트워크 접속시 사용
  - Serial포트 : WAN 접속을 위한 포트 DSU/CSU와 연결

■ Ethernet Port: 내부 네트워크, 즉 랜을 위한 접속 포트.

■ Serial Port: 외부 네트워크(인터넷 또는 원격지) 접속을 위한 포트로 DSU/CSU와 연결.

■ 라우팅 프로토콜 : 라우티드 프로토콜들에게 목적지까지 가장 좋은 길을 갈 수 있게 해주는 역할
- RIP, IGRP, OSPF, EIGRP등이 있다.
- 라우팅 알고리즘이라고도 한다.

■ 라우티드 프로토콜 : 목적지에 해당되는 프로토콜(TCP/IP, Apple Talk, IPX 등), 라우팅을 해주는 고객

■ 스태틱(Static) 라우팅 프로토콜
- 라우터에 사람이 일일이 경로를 입력해줌.
- 속도 빠르고 보안에 강함. 메모리적게듬
- 손수 작업해서 번거로울 뿐 아니라, 한 번 잘못되면 큰일이 발생.

■ 다이내믹(Dynamic) 라우팅 프로토콜
- 자기 판단에 따라 지정하여 편리하다
- 라우터에 부담을 주고, 속도가 Static에 비해 느리다
- RIP, IGRP, OSPF, EIGRP 등.

■ 라우팅 테이블
- 라우터는 라우팅 테이블이라는 경로에 대한 지도 정보를 유지함
- RAM에 올라가기 때문에 파워가 꺼지면 소멸
- 시스코 라우터에서 보는 명령 : show ip route (sh ip route는 TCP/IP에서 찾은 경로만 보여줌)
  ex) IPX에서의 경로 정보를 보고자 하는 경우에 sh ipx route 하면 됨

■ AS(Autonomous System)
- 하나의 네트워크 관리자에 의해서 관리되는 라우터들의 집단
- 하나의 관리 규정 아래서 운용되는 라우터의 집단 or 하나의 관리 전략으로 구성된 라우터의 집단
- 쉽게말해 한 회사나 기업, 또는 단체의 라우터 집단이라고 생각하면 됨

- 라우터를 AS라는 그룹으로 묶는 이유는 라우터 정보를 효율적으로 관리하기 위함
- 외부, 즉 AS밖으로 나갈때는 문지기라우터(ASBR)에게 정보를 물어보고 밖(인터넷)으로 나감

- AS 내부 사용 라우팅 프로토콜(IGP) : RIP, IGRP, EIGRP, OSPF등
- AS 외부 사용 라우팅 프로토콜(EGP) : EGP, BGP 등

■ 라우터 구성방법의 종류
- 콘솔(console) 케이블을 이용, 나머지 한쪽은 serial port에 연결(직렬,COM포트라고도함) : 가장강력
- 원격지 모뎀을 이용한 구성
- IP주소가 세팅된 곳에서 네트워크를 통해 접속하는 텔넷사용
- 네트워크 관리 시스템이 있는 곳에서 사용하는 NMS를 이용한 구성
- TFTP 서버로 라우터를 구성

■ 라우터의 중요한 모드
- 프리빌리지드 모드 : 운영자모드와 구성모드, 즉, Config 모드. Router> 에서 Router# 으로 바뀜
  구성모드의 변경은 오직 프리빌리지드 모드에서만 가능.
- 유저 모드: 프리빌리지드 모드로 들어가는 명령은 Enable이고 다시 유저 모드로 나오는 명령은
  Disable이다. (Router>)

■ 라우터 유용 Tip
- Ctrl+A : 명령어의 맨 앞 글자로 이동
- Ctrl+E : 명령어의 맨 뒤 글자로 이동
- Esc+B : 한 단어 뒤로 이동
- Esc+F : 한 단어 앞으로 이동
- Ctrl+F : 한 글자 앞으로 이동
- Ctrl+B : 한 글자 뒤로 이동
- [Tab]키 : 명령어 뒤에 부분을 잘 모를때

■ 라우터의 내부들여다보기
- 인터페이스 : 네트워크와 라우터에서 직접 연결되는 부분.
- 램(RAM) : 램에 올려서 고유의 운영 체제 IOS를 사용
  - 구성 파일 보는 명령 : Show running-config 또는 write terminal
- NVRAM(Non Volatile RAM): 비휘발성램, 전원이 꺼져도 정보가 날아가지 않음
  - 구성 파일 보는 명령 : Show startup-config 또는 Show config
- Flash 메모리 : IOS가 들어가는 메모리. 비휘발성.
- ROM : 라우터의 가장 기본적인 내용들이 있음. PC의 CMOS같은 기능

■ Show version : 사용하는 소프트웨어의 버전, 인터페이스의 종류, IOS가 어디서 부팅했는지등의
전반적인 내용을 볼 수 있는 명령

■ Show interface : 현재 라우터가 가진 모든 인터페이스를 다 보여주고 현재 상황을 자세히 알려줌
- 현재 구성파일 : show run 명령
- 백업 구성파일 : show start 명령

■ Show flash : 플래시 메모리를 보는 명령

■ Show processes cpu : 라우터의 동작 상태를 보여줌. 5분 1분 5초 동안의 CPU로드가 퍼센트로 나타남

■ Disatance Vector
- 거리와 방향만을 유지. 이웃 라이터와 주기적으로 라우팅 테이블을 교환.
- 메모리가 적게 들고 구성이 쉽지만 링크 변동시에 인식 시간이 길고 네트워크 크기에 제한을 둠.

■ Link State
- 한 목적지까지의 모든 경로 정보를 알고 있기 때문에 링크 변동에 따른 인식이 빠르다
- 라우팅 테이블의 교환 주기가 길다
- 링크 변동이 일어난 라우팅 테이블만 교환하기 때문에 트래픽이 적다.
- 대형 네트워크에 적합하지만, 메모리의 소모나 CPU의 로드가 많다.

■ 라우터의 패스워드 구성
- 두 가지로 구성되어있고 둘다 프리빌리지드모드로 들어가기 위한 패스워드이다
- enable password를 설정하면 패스워드가 라우터의 구성 파일에서 그대로 보인다.
- secret과 password를 동시에 세팅할 경우 secret만 패스워드만 물어본다.(암호화됨)
- 콘솔 포트, 버추얼 터미널 포트, AUX 포트에도 패스워드를 세팅할 수 있다.
- 콘솔이나 버추얼 터미널 포트 등에 타임아웃을 걸어서 사용안하는 포트를 자동으로 끊을수 있다

■ 시스코 에 연결된 장비를 찾아내는 CDP(Cisco Discovery Protocol)
- 장비의 이름과 같은 확인 정보
- IP주소와 같은 주소 정보
- 접속 포트에 대한 정보
- 접속 장비의 기능에 대한 정보
- 접속 장의 하드웨어 사양

■ Telnet을 이용한 장비 접속
- VTY 패스워드를 세팅해 놓지 않으면 기본적으로 외부에서의 텔넷 접속이 불가능.
- 텔넷 세션을 완전히 끊내지 않고 잠깐 빠져나올때 Ctrl + Shift + 6 마지막에 X
- show session 명령을 통해서 텔넷세션을 잠시끊었는지 완전 빠져나간것을 알수있다

■ 핑과 트레이스
- 라우터를 구성한 후 네트워크의 연결에 이상이 없는지를 테스트하기 위함
- 일반 PC를 사용하는 경우에도 인터넷 연결이 잘 되었는지 확인할때 사용함.
  - 단순형 핑을 사용했을때 출발지 주소는 라우터를 떠나는 쪽 인터페이스로 자동으로 잡힌다
    출발지주소를 변경하려면 반드시 확장형 핑을 사용해야한다.
  - 트레이스(Trace) : 목적지까지의 경로를 분석해 주는 기능
    TTL값을 하나 씩 증가시키면서 돌아오는 에러 메시지를 보고 경로를 확인하는 기능을 제공

Part 8. 라우팅 프로토콜과의 한판

다이나믹 라우팅 프로토콜에 대해서 알아보겠습니다.

■ RIP(Routing Information Protocol)

- 라우팅 프로토콜이다.
- 다이나믹 프로토콜이다
- 내부용 라우팅 프로토콜(IGP)이다
- 디스턴스 벡터 알고리즘이다(Distance(거리)와 Vector(방향)으로 길을 찾아가는 프로토콜)
- RIP 라우팅 프로토콜에서 라우터가 좋은 길을 결정할 때 기준이 되는 요소는 홉(Hop) 카운트이다
- RIP 라우팅 프로토콜에서 최대한 갈 수 있는 홉 카운트의 거리는 15개까지 가능 16개부터는 도착불가
- 디폴트 업데이트 주기는 30초.

■ RIP는 표준 라우팅 프로토콜이고 라우터의 메모리를 적게 사용하는 장점도 가지고있다.

- 최적의 경로를 찾는 방법이 가장 단순하고 가장 낮은 홉 카운트가 가장 좋은 경로라고 결정한다. 경로 선택을 오로지 홉 카운트에 의존하기 때문에 속도나 회선의 신뢰도, 그리고 회선의 로드 등을 확인불가
- 자신의 라우터에서 15개 이상의 라우터를 거치는 목적지의 경우 unreachable(갈 수 없음)로 정의 해버리기 때문에 커다란 네트워크상에서 사용하는데 무리가 따른다.

* 아직 RIP를 사용하는 이유는 소규모 네트워크 상에서는 효율성이 좋고, 라우터의 메모리를 적게 차지하고, 구성이 간편하고 모든 라우터에서 지원하는 표준 라우팅 프로토콜이기도하다.

■ Back to Back 구성

- 라우터와 라우터를 서로 직접 연결하면서 마치 전용선 구간에서 연결한 것처럼 만드는 기술
- 라우터 대 라우터를 V.35 케이블만을 가지고 서로 연결하는 것
- 두 라우터 중 하나는 DTE로 하나는 DCE로 동작해야 한다.

show controller 명령을 수행해서 DTE와 DCE를 확인후
DCE 케이블이 연결된 라우터의 인터페이스 구성모드에서
DCE장비는 클록을 제공해야 하기 때문에 아래와 같이 Clockrate값을 넣어서 설정.

```
Router-B(config)#int s 0
Router-B(config-if)#clockrate 56000
```

56000은 56kbps의 속도로 두 라우터가 연결된것이다.
이렇게 Back to Back 구성으로 연결되면 전용선으로 연결된 구성과 똑같이 사용할 수 있다.

RIP에 대해 더 알아보겠습니다.

```
Router(config)#router rip
Router(config_router)#network network-number
```

router rip 명령 - 일반 구성모드(Router(config)#)에서 내리는 명령으로 RIP라우팅을 사용한다는뜻
두 번째 명령은 반드시 router rip명령을 내리고 Router(config-router)# 모드로 들어와서 명령을내림
RIP 라우팅에 참가하는 네트워크를 지정해 주기 위해서 사용하는 명령이다.

■ show ip protocol - 현재 사용하고 있는 RIP의 버전 정보를 보여준다.

■ RIP환경에서 라우터는 30초동안 업데이트 정보를 받지 못했다면 180초 동안은 기다리는데(6번)이 시간을 Invalid time이라하고 180초가 지나도 업데이트가 오지 않으면 Hold down상태로 들어간다.
이때부터 라우터는 상대편이 다운됐을 거라고 판단하고 possibly down 이라는 메시지를 라우팅 테이블에 보여준다
그리고도 1분 동안 상대로부터 연락이 없으면 경로가 죽었다고 판단하고 이 경로에 대한 정보를 지워버리게 되는데 그 시간을 flush time이라고 부른다.
- RIP 버전 1에서 보낸 정보는 어떤 버전이든 받아볼 수 있지만 버전 2에서 보낸 정보는 버전 2에서만 이해할 수 있다.

■ show ip route - 라우팅 테이블보기

```
R    203.240.200.0/24  [120/1] via 203.240.150.2,  00:00:21, Serial0
```

R은 RIP로 찾아낸 길을 의미하고 203.240.200.0은 목적지 네트워크(찾아낸 목적지)
/24는 255.255.255.0 -> 서브넷 마스크를 이진수로 바꾸었을 때 1의 숫자를 의미하고
120은 RIP의 디스턴스 값을 나타낸다. 그 뒤에 있는 1은 코스트를 의미하는데
RIP에서는 코스트가 홉 카운트니까 1홉 떨어져서 목적지가 있다고 보면된다

```
C    203.240.100.0/24   is  directly connected, Ethernet0
C    203.240.100.0/24   is  directly connected, Serial0
```

C는 connect를 의미하고 라우터에 붙어있는 네트워크임을 알려줌

■ 텔넷에서 디버그 명령을 내리는 경우 terminal monitor라는 명령을 해야 텔넷 화면에서 결과 보여줌
- 디버그 명령 사용시 콘솔에서 명령을 내리는것이 좋다
- 결과치를 보고 나서는 반드시 명령을 꺼줘야한다(빨리 끄는 것이 중요)
- 계속 여러 가지 내용을 보여주기 때문에 부담되어서 다운될 수도 있음

■ Router#no debug all or Router#undebug all - 디버그 꺼주는 명령

■ 디버그하고 IP RIP라고 하면 IP RIP 상에서 라우터끼리 서로 통신하는 것을 보여주는데
- 프리빌리지 모드(운영자모드)에서 debug ip rip라고 해주면 된다
- 명령을 내리는 시점에서부터 라우터에서 rip에 대해서 주고 받는 내용을 보여준다

■ Administrative Distance 값

Route Soruce	Default Distance
Connected interface	0
Static route out an interface	0
Static route to a next hop	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	**100**
OSPF	**110**
IS-IS	115
RIP v1, v2	**120**
EGP	140
External EIGRP	170
Internal BGP	200
Unknown	255

■ Distance - Vector의 문제점

- 한번 배운 라우팅 테이블을 계속 전달하기 때문에 업데이트가 모든 네트워크에 전달되는 시간(Convergence Time)이 많이 걸린다. 이것 때문에 루핑이 발생할 수 있다.

예를들어 업데이트 주기가 30초이면 라우터 A는 30초 후에 변경된 라우팅 테이블을 라우터 B에게 보내고 라우터 B는 다시 30초 후에 라우터 C에게 보내기 때문에 라우터 C는 라우터 A가 라우팅 테이블 변화를 인지한지 60초후에 알수 있게된다.

- 루핑이 발생하게 되고 라우터가 제대로 라우팅정보를 가지지도 못하고 업데이트도 느려진다

■ 루핑 방지법

- Maximum Hop Count : 최대 홉 카운트를 15로 규정하여 넘어가면 unreachable로 간주하고 flush time이 지난 후에 라우팅 테이블에서 삭제해버린다. 15홉을 넘는 경로에는 도달할 수 없기 때문에 네트워크의 규모가 커질 경우 치명적인 약점이다
- Hold down Timer : 한 네트워크가 다운되면 물려있는 라우터가 다른 라우터에게 다운사실을 알리고 그 정보를 받은 라우터는 다운된 네트워크에 대한 Hold down 타이머를 시작한다.
  외부에서 해당 네트워크에 대한 라우팅 경로 정보를 받았을때 원래 값보다 큰 값이 들어오면 무조건 무시
  Hold down카운터가 종료되거나 목적지에 대한 새로운 경로가 가지고있는 메트릭과 같거나 좋은 경로이면 업데이트를 받아들임
  Hold down타이머는 어떤 경로가 죽었다고 판단하면 일정 시간이 지난 다음에 바꾸는 식이다.
- 스플릿 호라이즌(Split Horizon) : 라우팅 정보가 들어온 곳으로는 같은 정보를 내보낼 수 없다는 의미 두 라우터 간의 루핑만을 막기 위해서 만들어진 기술이다.
- 라우트 포이즈닝(Route Poisoning) : 네트워크가 다운되면 메트릭 값을 16으로 변경(사용할수 없는값) 이런식으로 다운된 네트워크를 먼저 무한대치로 바꾸어서 라우팅 테이블에서 지워버렸다가 잘못된 라우팅 정보를 받는 일을 미리 막을 수 있는 효과를 나타낸다
- 포이즌 리버스(Poison Reverse) : 스플릿 호라이즌의 변형. 포이즌 리버스 업데이트를 사용한 스플릿 호라이즌 라우팅 정보를 되돌려 보내기는 하되 이 값을 무한대 값으로 쓰는 방식
  경로의 정보를 아주 없애는 것보다 무한대 홉 값을 포함해서 라우팅 업데이트를 하게되면 모든 라우터들은 실수로 잘못된 경로 정보를 사용하는 경우를 줄일수 있음

■ IGRP(Interior Gateway Routing Protocol)

- RIP처럼 라우팅 프로토콜이다
- 다이나믹 프로토콜이다
- 내부용 라우팅 프로토콜(IGP)이다
- 디스턴스 벡터 알고리즘이다. 거리와 방향으로 길을 찾는 프로토콜
- 시스코에서 만들어낸 프로토콜이므로 시스코 라우터에서만 사용이 가능
- 5가지 요인을 가지고 가장 좋은 경로를 선택한다.
  - Bandwidth(대역폭, 속도) : 최적의 경로를 찾는 프로토콜들이 참고하기 위한 값
  - Delay(지연) : 경로를 통해서 도착할 때까지의 지연되는 시간
  - Reliability(신뢰성) : 목적지R지 제대로 도착한 패킷과 에러가 발생한 패킷의 비율
  - Load(부하, 하중) : 출발지와 목적지 상의 경로에 어느 정도의 부하가 걸리는지 측정
  - MTU(Maximum Transmission Unit) : 경로의 최대 전송 유닛의 크기. 바이트로 표시함

  * RIP와는 달리 경로 선택에 있어서 지능적임.
- 90초에 한 번씩 라우팅 테이블의 업데이트가 발생
- 최대 홉 카운트 255로 큰 네트워크의 적용에도 문제가 없음

■ IGRP 구성 명령어

- 일반 구성 모드에서 router igrp입력하고 뒤에는 AS번호(그룹별로 붙여 놓음) 입력
  라우터들은 서로 같은 AS번호를 가져야만 통신이 원활함.
- network명령 : IGRP 라우팅에 참가하는 네트워크를 지정.
  항상 위 명령을 내린 후 해야한다. 수정할 때도 마찬가지
  network number를 150.140.100.0이라고 입력했는데 150.140.0.0으로 인식해 버리는데
  RIP처럼 뒤의 서브넷에 대한 인식 기능이 떨어진다. 서브넷을 인터페이스별로 따로주는 방식(VLSM)을 지원못함
- RIP처럼 show ip protocol : 현재 라우팅정보
  show ip route : 라우팅 테이블정보
- 라우터 구성 후 현재 상태 점검하는 명령어들
  구성파일을 보는 명령 : show running-config, show ip route, show interface, show ip protocol,
  show ip interface(인터페이스에서의 IP프로토콜 동작 상태를 나타냄)
- 디버그 명령
  - debug ip igrp transactions (IGRP 업데이트가 보내지거나 받아졌을 때 반드시 그 사실을 알려줌)
  - 라우팅 업데이트에 포함된 네트워크 정보는 관련 메트릭 값과 함께 나오기 때문에
    업데이트된 라우팅정보도 확인이 가능
- passive interface명령 : IGRP 라우팅 업데이트가 특정 인터페이스로 날아가지 않도록 할때 사용

■ OSPF 라우팅 프로토콜

<table>
<tr><td rowspan="2">프레임헤더</td><td colspan="3">프레임 페이로드</td><td rowspan="2">C
R
C</td></tr>
<tr><td>IP헤더</td><td>프로토콜 넘버
89-OSPF
6-TCP
17-UDP</td><td>패킷 페이로드</td></tr>
</table>

- OSPF는 IP패킷 안에 프로토콜 넘버 89(십진수)로 들어가게된다.
- Convergence(컨버전스)타임 - 라우터 간에 서로 변경된 정보를 주고받는데 걸리는 시간
  OSPF는 어떤 변화가 생길 때 바로 전달이 가능하여 RIP에 비해 훨씬 빠르다.
- Area라는 개념을 사용 - 전체 OSPF 네트워크를 작은 영역으로 나누어 관리하기 때문에 빠른
  업데이트를 하면서 효율적인 관리가 가능
- VLSM을 확실하게 지원하여 IP주소 효과적 사용, 라우팅 테이블을 줄이는 효과. 이를 위해 라우트
  서머리제이션(Route summarization)을 지원하여 여러 개의 라우팅 경로를 하나로 묶는 기능탁월
- 네트워크 크기제한이 없다(15개의 라우터를 건너는 것이 가능)
- 네트워크 대역폭 활용측면 - 변화가 있을 때만 정보가 날아가고 멀티캐스트로 날아가기 때문에 실용적
- 경로설정시 많은 관련 요소를 합쳐서 선택하기 때문에 정확한 경로선택이 가능
- OSPF적용 토폴로지
  - 브로드캐스트 멀티액세스 토폴로지 : 네트워크에 두 개 이상의 라우터가 연결되는 경우로 하나의
    메시지를 내보내면 이 네트워크 상에 있는 모든 녀석들이 정보를 받을 수 있는 구조
  - 포인트 투 포인트 토폴로지 : 네트워크에 한 쌍의 라우터만 존재하는 경우(전용선)
  - NBMA토폴로지 : Non Broadcast Multi-access. 네트워크에 두 개 이상의 라우터가 연결
    브로드캐스트 능력은 없음(프레임릴레이, X.25)

■ OSPF의 이웃 사랑

▪ 주위에 있는 OSPF라우터들을 찾아서 자신의 DB에 저장하고 이 주변라우터들을 이웃이라한다.

- 주변에 어떤 이웃들이 사는지에 대한 정보를 관리

▪ 이웃을 만드는 과정

1. 이웃을 찾기 위해 Hello 패킷을 보냄(멀티캐스트 주소를 이용해서 보냄)
   - 라우터 ID : OSPF에서 서로를 구분하는 이름, 라우터의 IP 주소 중에서 제일 높은 주소를 사용
2. Init 과정을 거침(패킷을 받은 라우터들이 보낸 라우터를 이웃목록에 넣는과정)
3. 패킷을 보낸 라우터에 유니캐스트로 자신들의 정보를 보냄
4. 이웃에게서 받은 정보를 자신의 이웃리스트에 넣어서 관리

▪ Hello 패킷에 여러정보들이 들어 있는데 Hello/dead intervals, Area-ID, Authentication password, Stub area flag 최소한 이 4가지는 서로 똑같아야 이웃으로 인정해준다.

▪ 라우터 ID를 쓰기 위해서 보통 Loopback(루프백) 인터페이스를 사용하는데 이걸 사용하면 그 IP 주소의 높낮이에 관계없이 무조건 Loopback 주소가 라우터 ID가 되고 인터페이스가 다운되지 않기 때문에 라우터 ID도 바뀌지 않는다.

■ OSPF에서의 반장과 부반장

▪ OSPF 세그먼트에서는 각 라우터들이 OSPF에 참여하게 되면 DR과 BDR에게 자신의 Link State를 알리는데 그 이유는 모든 라우터들과 Link State를 교환할 경우 발생하는 트래픽을 줄이고 Link State의 Sync(일치성)를 제대로 관리하기 위해서이다.

▪ 반장(DR)이 업무를 수행하는동안 부반장(BDR)은 반장이 업무를 제대로 수행하는지 관찰하고 반장이 다운되면 BDR이 DR을 대신한다.

▪ 따라서 OSPF에서는 모든 라우터가 반드시 DR, BDR과 Link state를 Sync(일치)해야하는데 이것을 Adjacency(어드제이션시)라고 한다.

▪ DR과 BDR은 라우터 ID와 라우터의 Priority를 가지고 선출된다.

- Priority로 선출하는데 디폴트값은 1이고 이 값이 큰쪽이 DR이 되고 작은쪽은 BDR이 된다.
- Priority가 같으면 라우터 ID가 큰것이 DR, 작은것이 BDR로 선정된다
- 만일 DR이 다운되면 BDR -> DR로 BDR은 재선정하는데 Priority값이 3이더라도 BDR로 된다 여기서 라우터나 OSPF를 죽였다가 다시살리면 재선거를 해서 Priority값이 3인라우터가 DR이된다.
- DR, BDR선거에 입후보하지 않게 하려면 Priority를 0으로 세팅하면된다

Part 9. IPX에 대한 이야기

■ 노벨의 IPX 프로토콜

- TCP/IP처럼 라우티드 프로토콜이다
- IP프로토콜과의 차이점은 IP는 인터넷에서 사용되고 IPX는 내부 네트워크에서 사용됨

<table>
<tr><th colspan="2">OSI Reference Model</th><th colspan="5">Novell Netware protocols</th></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">RIP
NLSP</td><td rowspan="3">SAP</td><td rowspan="3">NCP</td><td rowspan="3">NETBIOS</td><td rowspan="2">APPLICATIONS</td></tr>
<tr><td>6</td><td>Presentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td colspan="3"></td><td>SPX</td></tr>
<tr><td>3</td><td>Network</td><td colspan="5">IPX(Internet Packet Exchange)</td></tr>
<tr><td>2</td><td>Data Link</td><td colspan="5" rowspan="2">Media Access protocols
(Ethernet, Token Ring, WAN, others)</td></tr>
<tr><td>1</td><td>Physical</td></tr>
</table>

■ SAP(Service Advertising Protocol)

- 사용 가능한 네트워크 자원을 모든 네트웨어 서버나 라우터들과 브로드캐스트를 사용해서 정보 공유
- SAP에 관련된 브로드캐스트는 매 60초마다 발생
- 16진수를 사용해서 서비스를 구분(ex. 16진수 4는 네트웨어 파일 서버, 7은 프린터 서버를 나타냄)
- 네트워크 상에 있는 PC들 역시 SAP 브로드캐스트 질의를 보내고 또 그 질의에 해당하는 답변을 받음으로써 네트워크 상에 있는 IPX/SPX 서비스를 인식
- 모든 정보가 SAP를 타고 전송되기 때문에 SAP 필터링이 가장 중요한 기술이다

■ GNS(Get Nearest Server)

- 네트워크 상에 있는 PC(Client)들이 파일 서버에 접속하려고 할때 사용
- 파일 서버를 찾을때 가장 가까이 있는 서버가 응답하라고 메시지를 보내면 하나가 대답한다. 일정 시간 동안 응답하지 않으면 IPX 구성이 되어 있는 라우터가 대신 대답한다

■ IPX의 주소체계

- IP주소와 같은 Class구분이 없고
- 총 80비트(10byte)로 구성

4바이트(32비트)	6바이트(48비트)
네트워크 주소	노드주소
0000:002A	0080:c703:3c75
16진수 8자리	16진수 12자리

- 노드부분은 MAC주소를 그대로 사용.
- 네트워크 주소를 적을때 앞에 0은 생략할수 있지만 노드주소에서는 0을 생략하지 않는다

■ IPX의 인캡슐레이션 방식

- 노벨 네트웨어 서버가 디폴트로 사용하는 인캡슐레이션이 여러개 있음
- 이 방식을 서로 맞추어주어야만 통신이 가능하게됨
- 시스코 라우터에서는 노벨의 IPX 인캡슐레이션 이름을 조금 다르게 정의하기 때문에 표참조

	Novell IPX Name	Cisco IOS Name
Ethernet	Ethernet_802.3	novell-ether
	Ethernet_802.2	sap
	Ethernet_II	arpa
	Ethernet_SNAP	snap
Token Ring	Token_Ring	sap
	Toekn_Ring_SNAP	snap
FDDI	FDDI_SNAP	snap
	FDDI_802.2	sap
	FDDI_Raw	novell-fd야

- 주로 novell-ether방식과 sap방식이 사용됨

■ IPX를 실어나르는 라우팅 프로토콜

- IP처럼 라우티드 프로토콜이기 때문에 누군가 날라줘야함(RIP가 이 역할을함)
- Ipx RIP는 다이나믹 라우팅 프로토콜이고, 디스턴스 벡터 라우팅 알고리즘임
- TCP/P에서 사용하는것과는 서로 다르다. 상호관에 호환성도 없음
- 시스코라우터에서 IPX라우팅을 설정하면 자동으로 Enable 가된다.
- NLSP(Netware Link Services protocol) - Link State 프로토콜로서 IP에서 OSPF와 유사한 프로토콜이고 RIP와 같은 역할을함. 크고 복잡한 IPX 네트워크 구성시에 유리함.
- 그 외 EIGRP도 있음(IP뿐 아니라 IPX도 실어나르는 멀티프로토콜. Apple Talk 라우팅도 지원함

■ 라우터에서 IPX의 구성

- IPX 라우팅을 사용하겠다는 것을 일반 구성모드에서 정의
- 인터페이스에 가서 IPX 네트워크주소와 인캡슐레이션방식을 지정
- ipx routing만 써줘도 IPX 라우팅을 구동할수 있음
- IPX 노드 주소를 임의 지정시 ipx routing뒤에 16진수로 노드주소를 입력하면 됨(예: ipx routing 4.4.4)
- 디폴트 인캡슐레이션을 그대로 사용하면됨
- 전체적인 IPX 세팅 확인은 show ipx interface 명령사용
- 라우팅 테이블 관리 명령 : show ipx route
- 파일 서버가 제대로 보이는지 확인명령 : show ipx server
- 맥 어드레스 확인 명령 : show ipx interface e 0 or show interface e 0
- IPX 트래픽 확인 명령 : show ipx traffic

Part 10. 라우터, 그 속으로 전진!

■ 네트워크 접근 제어 액세스 리스트(Access List)

- 액세스 리스트 - 접근을 하게 해줄까 말까를 미리 정해놓은 리스트라고 할수있다
- 주로 보안을 위해서 사용되고 있다
- 이 액세스 리스트가 모든 침입자를 완벽하게 막지 못하기 때문에 보안장비를 따로 둔다

a. 스탠더드 액세스 리스트(Standard Access List) - 일반적이고 쉬움
   - 출입통제를 할 때 출발지 주소만을 참고해서 제어
   - 어디서 왔는가를 본 다음 통과 여부를 결정함

b. 익스텐디드 액세스 리스트(Extended Access List) - 복잡 다이나믹 액세스 리스트라고도함
   - 출발지, 목적지, 프로토콜, 사용포트번호등 다 본 다음에 통과 여부를 결정

c. 유저 네임(User Name)과 패스워드에 따라 통제가 가능한 액세스 리스트

- 액세스 리스트에 걸려서 못들어가는 경우 Host Unreachable 란 메시지가 나타남

■ 액세스 리스트에서 중요한 네가지 규칙

① 윗줄부터 하나씩 차례로 수행된다

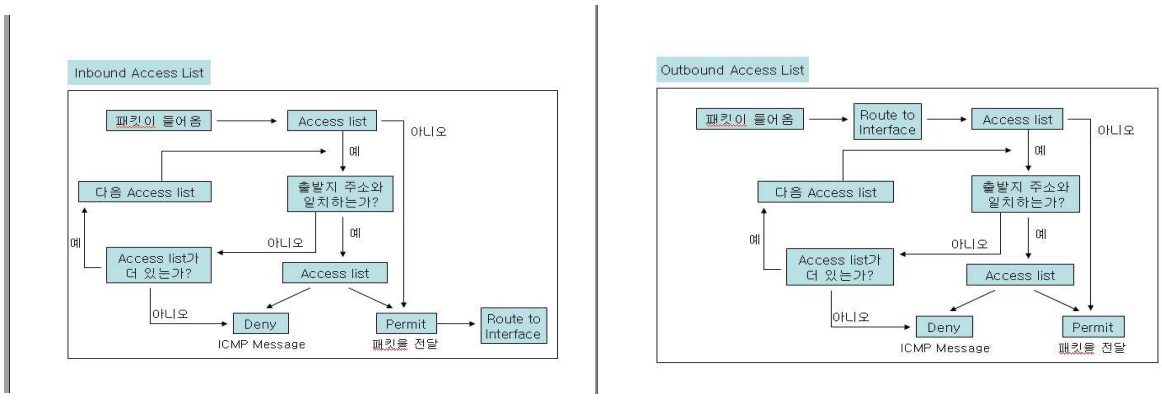
② 맨 마지막 line에 “Permit any”를 넣지 않을 경우 default로, 어느 액세스 리스트와도 match되지 않은 나머지 모든 address는 deny된다
   - 마지막줄에는 항상 모든 것을 막는 deny all이 들어 있음
   - 액세스 리스트에 해당하지 않는 주소는 마지막에 deny all에 걸려서 막힘

③ 새로운 line은 항상 맨 마지막으로 추가되므로 access-list line의 선택적 추가(selective add)나 제거(remove)가 불가능함
   - 잘못 내린명령은 no를 이용해서 지우는데 맨 마지막줄만 남기고 모두 지우게되므로 조심해야함

④ interface에 대한 액세스 리스트의 정의(define)가 되어 있지 않은 경우(즉 interface에 access-group) 명령이 들어있지 않은 경우) 결과는 permit any가 된다
   - 액세스 리스트를 거치지 않고 바로 통과되었기 때문에 당연히 permit any가 됨

- 액세스 리스트 작업시 메모장등을 열어서 그곳에서 작업하는것이 가장좋음
- 리스트 번호를 1~99까지사용. 전체 TCP/IP에 대해 제어를 한다

■ 스탠더드 액세스 리스트의 시작



- 인터페이스에 IN과 OUT으로 구성
- 처음 인터페이스로 패킷이 들어오면 액세스 리스트가 설정되었지 확인후 안되어있으면 바로통과 있다면 패킷의 출발지 주소를 비교함
- 조건이 Deny이면 패킷의 흐름을 막은 다음 ‘host unreachable’ ICMP 메시지를 보여주고 조건이 Permit이라면 패킷을 정해진 경로로 내보냄.

■ 와일드카드 마스크

- OSPF 라우팅 프로토콜을 사용할 때나 액세스 리스트를 사용하는 경우 사용되는 마스크
- 서브넷 마스크가 무엇을 하면 무조건 반대로 한다.
- 서브넷 마스크 255.255.0.0 = 1111 1111.1111 1111.0000 0000.0000 0000
  와일드카드 0.0.255.255 = 0000 0000.0000 0000.1111 1111.1111 1111

■ 텔넷포트(VTY Port)에서의 액세스 리스트

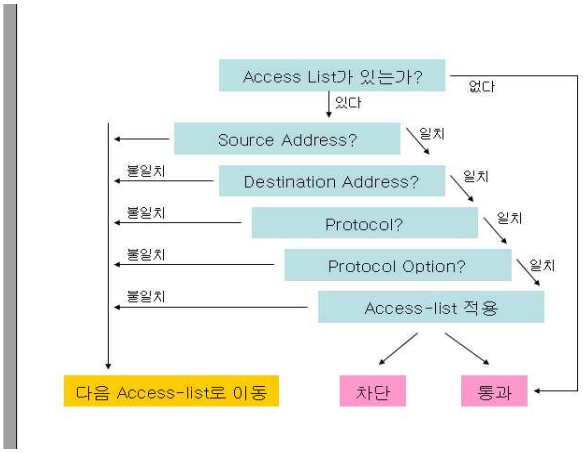
- 라우터에 텔넷을 한다는 것은 라우터의 Virtual Terminal 포트로 접속을 한다는 것을 의미
- VTY 포트에 액세스 리스트를 적용하면 텔넷으로 들어오는 Source 주소를 제어할수있다
- access-class 명령으로 액세스 리스트 번호를 지정하고
- vty 인터페이스의 IN에 적용할 것인지, OUT에 적용할 것인지를 결정
- 라우터로의 텔넷 접속을 제어하고자 하는 경우 access-class뒤에 IN을 써주게 됨
  스탠더드 방식을 주로 사용함.

```
access-list 10 permit 200.10.10.0 0.0.0.255
!
line vty 0 4
 access-class 10 in
 password cisco
!
```

- access-class 10은 앞에 있는 access-list의 번호와 일치해야함.
  즉 access-list 10 permit 200.10.10.0 0.0.255은 200.10.10.0 네트워크에 있는 (IP주소 200.10.10.1~200.10.10.254) 모든 호스트들은 이 라우터로 텔넷이 가능하고 나머지 모든 IP 주소를 가진 호스트는 이 라우터로 텔넷 접속이 불가능함을 의미한다

■ 익스텐디드 액세스 리스트(Extended Access List)

- 출발지 주소와 목적지 주소(destination address) 모두를 제어할 수 있다.
- ip, tcp, u에, icmp 등 특정 프로토콜을 지정해서 제어가능
- 100에서 199까지의 숫자를 Access-list 번호로 사용



- 출발지 주소뿐 아니라 목적지 주소, 프로토콜 등 관리하는 항목이 훨씬 많다.
- Established 옵션은 TCP 데이터그램이 ACK나 RST bit이 set되어 들어오는 경우에만 match 발생

```
access-list 104 permit tcp any 128.88.0.0 0.0.255.255 established
```

- 128.88.0.0 네트워크에 있는 호스트들은 밖으로 나갈 수 있고, 밖에서는 들어올수 없게 하는 기능

■ 라우터의 장애 대비 HSRP

- HSRP(Hot Standby Routing Protocol) - 시스코 장비에서만 사용되는 기능
- 메인 라우터가 고장나면 자동으로 두 번째 라우터가 메인 라우터의 역할을 대신하는 기능
- 디폴트 게이트웨이를 고치지 않고도 항상 인터넷 접속할수 있게한다.
- 라우터의 시리얼에 문제가 생겼을 때도 액티브 라우터를 교체해야 하는데 이것이 트래킹이다.
- Priority(우선 줄임)가 높은 라우터가 액티브 라우터가 되며 디폴트 Priority 값은 100이다

■ IP 주소의 변환 NAT(Network Address Translation)

- 한쪽 네트워크의 IP 주소가 다른 네트워크로 넘어갈 때 변환이 되어서 넘어가는 것
  - 내부 네트워크에는 비공인 IP 주소 사용 외부 인터넷으로 나가는 경우에만 공인 IP 사용하는 경우
  - ISP를 바꾸면서 내부 전체의 IP를 바꾸지 않고 기존 IP를 그대로 사용하는 경우
  - 두 개의 인트라넷을 합하려다 두 네트워크의 IP가 겹치는 경우
  - TCP 로드 분배가 필요한 경우
- Inside Local 주소 - 내부 네트워크에서 사용하는 비공인 주소
  Inside Global 주소 - 외부로 나갈 때 변환되어 나가는 주소

Part 11. 세상이 넓고 네트워킹은 계속된다

■ WAN
- 넓은 지역의 네트워킹에서도 중간에 통신 회사를 통해서 네트워킹을 구축할때사용
- 사용하는 목적, 사용료, 거리, 방법 등에 따라 다양한 종류
  - 전용선 방식(Leased Line) : 임대회선으로 볼수있음. 회선을 나 혼자 빌려쓰는것임 비용이 비쌈
  - 회선 스위칭 방식(Circuit Switched) : 내가 통신을 하는 순간에만 나에게 필요한 회선을 열어주고 통신이 끝나면 회수하는 방식. 전화와 같음
  - 패킷 스위칭 방식(Packet Switched) : 패킷 하나하나가 나누어서 통신회선을 타고 목적지까지 전달
    버추얼서킷 : 사실은 나에게 배정된 회선이 없는데 있는것처럼 통신하는 방식을 이용함.
    ex) 프레임 릴레이, ATM, X25등이 있음

■ HDLC(High-Level Data Link Control)
- 라우터의 시리얼라인에서 주로 사용
- 표준 프로토콜이다. 하지만 시스코에서 사용하는 HDLC는 표준이 아니다

■ PPP(Point-to-Point)
- 강력한 보안기능과 여러 가지 네트워크 게층 프로토콜을 한꺼번에 지원하는 장점을 가진 표준 프로토콜
- 가장 괜찮은 인캡슐레이션 방식
  - NCP(Network Control Protocol) : IP, IPX, Appletalk 등 멀티프로토콜 지원
  - LCP(Link Control Protocol) : 링크 접속에서의 보안, 에러 체크, 압축기능 및 멀티링크 PPP와 같은 다양한 접속 옵션을 제공

  LCP를 주목하는 이유는 보안기능때문인데 안전한 PPP 통신을 책임진다
- PAP(PPP Authentication Protocols or Password Authentication Protocol)
  : 간편하면서도 가장 일반적인 패스워드 확인법
  A라우터가 Host name과 Password를 B라우터로 보내면 일치여부를 바로 알려준다.(접속허가/불허)
  - 2-Way Handshake 방식인증이라고도 하는데 인증을 위해 두 번의 통신이 이루어진것이다.
  - 암호화되어 전송되지도 않고 위험성이 크다.
- CHAP(Challenge Handshake Authentication Protocol)
  - PAP처럼 중간에서 해킹할수 없게 만들었다
  - 3-Way Handshake 방식. 해킹기법을 사용하였음.
  - B라우터로 접속 시도를 하면 A라우터로 Challenge값을 보내고
    받은 챌린지 값으로 패스워드를 암호화하여 보내고 접속허가/불허를 받음
  - 해싱(Hashing) - 기존의 데이터를 어떤 코드 값을 이용해서 완전히 변형시켜서 절대 원본 데이터로 돌아갈 수 없게 만듬.

■ 프레임 릴레이(Frame-Relay) 구성
- 에러 복구와 흐름 제어 등의 데이터 처리 과정을 생략함으로써 보다 효율적인 뎅터 전송 방법
- X.25에 비해 빠르고 효과적이지만 에러 제어 기법은 거의 제공이 안됨
- DLCI(Data-Link Connection Identifier) : 프레임 릴레이 연결을 위한 주소.
  X.25의 경우 X.121이라는 주소 방식을 사용했는데 프레임 릴레이는 DLCI를 사용한다.
- LMI(Local Management Interface) : DLCI 정보와 함께 설정된 PVC 정보를 알려 줌으로써 인터페이스의 다양한 정보와 동작 상태 등을 제공하는 기능
  - 특정 동작 상태에 관련된 정보를 인접 라우터들에게 알려줌으로써 프레임 릴레이 네트워크상의 Virtual Circuit의 상태를 쉽게 파악할 수 있게 해주는 기능을 제공.

- 라우터에서 LMI를 세팅할 때 LMI 타입을 서로 맞추어 주어야 통신이 가능.
- LMI 타입으로는 시스코의 LMI, ANCI 617 Annex D LMI, ITU-T의 Q.933 Annex A LMI등 존재 ANSI 방식이 가장 널리 사용되는 방식
- 인캡슐레이션 : 프레임 릴ㄹ이 망을 통과할 때 마치 캡슐로 덮어 씌우는 것처럼 포장
- 프레임 릴레이 인캡슐레이션 방식은 Cisco 방식과 IETF 방식이 있는데 타사 라우터를 서로 같이 사용하는 경우에는 IETF 방식을 인캡슐레이션 방식으로 사용하는것이 바람직함.

  encapsulation frame-relay ietf ---> IETF 방식 인캡슐레이션

  encapsulation frame-relay ---> Cisco 방식의 인캡슐레이션

■ ISDN(Integrated Services Digital Network)

- 디지털 네트워크를 통해 여러 가지 서비스, 즉 음성, 데이터 등의 서비스를 전송하는 방식
- 전화접속 방식에 비해 상대적으로 빠른속도와 디지털 전송방식으로 여러 가지 서비스를 동시에 제공
- 일부 은행권이나 회사 등에서 백업용 회선으로 사용중.
- 종류로 BRI와 PRI가 있는데 겉보기에는 하나의 라인이지만 여러 개의 전송통로를 가진 회선이다
- BRI(Basic Rate Interface) - 두 개의 B채널과 하나의 D채널을 가짐. 주로 미국,일본에서 사용
  B(Bearer)채널 : 데이터, 음성, 영상 등의 사용자 데이터 전송을 담당. 64Kbps대역폭
  D(Delta)채널 : 제어 정보나 시그널 전송에 사용. 16Kbps대역폭
- PRI(Primary Rate Interface) - 전체 대역폭 약 1.544Mbps 23개의 B채널과 한 개의 D채널을 가짐
  E1 PRI는 약 2.048Mbps의 대역폭으로 30개의 B채널과 한 개의 D채널을 가지고 유럽에서 많이 사용