4장

스위치 이해 및 활용

- 스위치는 네트워크 중간에서 패킷을 받아 필요한 곳에만 보내주는 네트워크 중재자 역할
- 아무 설정 없이 네트워크에 연결만 해도 MAC주소를 기반으로 패킷을 전달하는 기본 동작을 수행한다.

스위치 MAC주소를 인식하고 패킷을 전달하는 스위치의 기본 동작 외에도 한대의 장비에서 논리적으로 네트워크를 분리할 수 있는 VLAN 기능과 네트워크 루프를 방지하는 스패닝 트리 프로토콜과 같은 기능을 기본적으로 가지고 있다.

```
# PDU(Protocol Data Unit)
각 계층에서 헤더와 데이터를 합친 부분
1계층 - 비트
2계층 - 프레임
3계층 - 패킷
4계층 - 세그먼트
애플리케이션,프레젠테이션,세션  - 데이터
```

계층	PDU
애플리케이션	데이터
프레젠테이션	데이터
세션	데이터
트랜스포트	세그먼트
네트워크	패킷
데이터 링크	프레임
물리	비트

스위치 장비 동작

- 스위치는 네트워크에서 통신을 중재하는 장비
- 패킷을 전송할 때 서로 경합해 네트워크 성능 저하를 방지하고자 여러 장비가 서로 간섭 없이 통신하도록 도와주는 장비가 스위치
- 여러 단말이 한꺼번에 통신할 수 있어 충돌및 대기 문제가 해결되어 통신 효율성이 증가한다.

핵심 역할

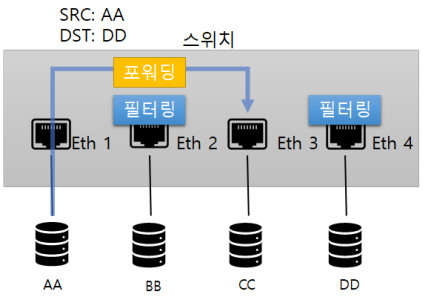
- 누가 어느 위치에 있는지 파악하여 자신이 알고 있는 위치로 패킷을 정확히 전송 하는것. MAC 주소 테이블이 필요하다.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.96d5.8401    DYNAMIC     Fa0/3
   1    0002.4ac5.7601    DYNAMIC     Fa0/1
```

MAC 주소 테이블에서 해당 주소가 어느 포트에 있는지 확인하고 패킷을 그 포트로만 전송



스위치 MAC 주소 테이블

MAC 주소	포트
AA	Eth 1
CC	Eth 3

- 테이블에 없는 도착지 주소를 가진 패킷이 스위치에 들어오면 전체 포트로 패킷을 전송한다.

스위치 동작 방식

1. 플러딩
2. 어드레스 러닝
3. 포워딩/필터링

플러딩

위치가 허브와 같이 모든 포트로 패킷을 흘리는 동작 방식

- 처음 스위치는 네트워크 관련 아무 정보가 없기 때문에 부팅하면 허브처럼 동작한다.
- 허브는 패킷이 들어온 포트를 제외하고 모든 포트로 패킷을 전달
- 즉, MAC주소 테이블에 아무것도 없으면 패킷을 모든 포트로 보낸다.
- 스위치는 LAN에서 동작하므로 자신이 정보를 갖지 않더라도 어딘가에 장비가 있다고 가정하고 이와 같은 작업을 수행한다.

- MAC주소와 포트가 매핑된 MAC주소 테이블 필요하다.
- 플러딩 동작은 정상적인 동작이지만, 많아지면 제 역할을 못하기 때문에, 패킷이 스위치에 들어오면 해당 패킷 정보의 MAC주소를 보고 이를 학습해 MAC주소 테이블을 만든 후 이를 통해 패킷을 전송한다.

> 스위치가 패킷을 플러딩한다는 것은 스위치가 제 기능을 못한다고 의심해야 한다.
> 실제로는 TCP/IP 네트워크에서는 ARP 브로드캐스트를 미리 주고 받은 후 데이터가 전달되므로 실제

```
MAC주소를 꽉 채우나 이상한 MAC주소를 학습시키는 등 스위치에 대한 공격으로 인해 플러딩 되는 경
```

```
# ARP 포이즈닝 기법
모니터링해야 할 IP의 MAC주소가 공격자 자신인것 처럼 속여 원하는 통신을 받는 방법
```

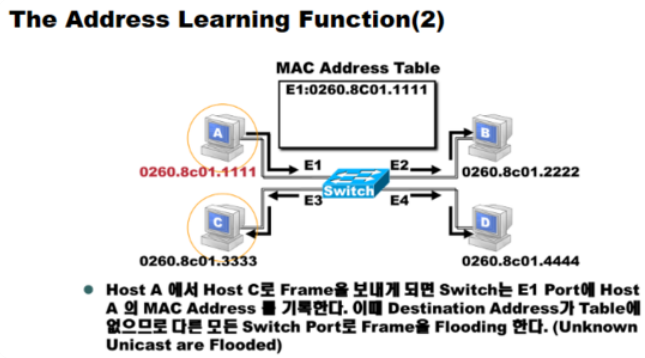
어드레스 러닝

MAC 주소 테이블을 만들고 유지하는 과정

- 스위치가 도착지 MAC주소를 확인해 원하는 포트로 포워딩하는 스위치의 역할을 정상적으로 수행하려면 MAC주소 테이블을 생성하고 유지해야 한다.
- MAC 주소 테이블은 어느 위치에 어떤 장비(MAC주소)가 연결되어있는지에 대한 정보가 저장된 임시 테이블

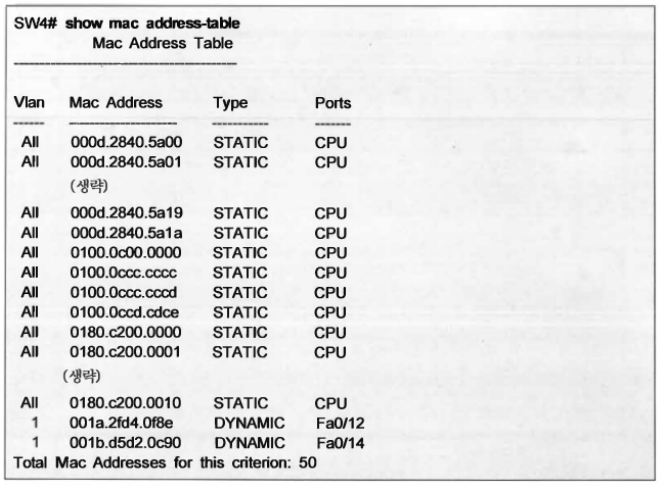
과정

1. 패킷이 특정 포트에 들어오면 스위치에는 해당 패킷의 출발지 MAC주소와 포트 번호를 MAC 주소 테이블에 기재한다.
2. 1번 포트에서 들어온 패킷의 출발지 MAC주소가 AAAA라면 1번 포트에 AAAA MAC주소를 가진 장비가 연결되어 있다고 추론한다.
3. 출발지의 MAC 주소 정보를 사용하므로, 브로드캐스트나 멀티캐스트에 대한 MAC주소를 학습할 수 없다.
4. 두 가지 모두 목적지 MAC주소 필드에서만 사용하기 때문




```
# 사전에 정의된 MAC주소 테이블
패킷을 처리하기 위한 주소가 아니라 대부분 스위치 간 통신을 위해 사용되는 주소
스위치에서 자체 처리하므로 인접 포트 정보가 없거나 CPU 혹은 관리 모듈을 지칭하는 용어로 표기
```

```
show mac address-table
```



```
SW4# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
 All    000d.2840.5a00    STATIC      CPU
 All    000d.2840.5a01    STATIC      CPU
        (생략)
 All    000d.2840.5a19    STATIC      CPU
 All    000d.2840.5a1a    STATIC      CPU
 All    0100.0c00.0000    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0ccd.cdce    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
        (생략)
 All    0180.c200.0010    STATIC      CPU
   1    001a.2fd4.0f8e    DYNAMIC     Fa0/12
   1    001b.d5d2.0c90    DYNAMIC     Fa0/14
Total Mac Addresses for this criterion: 50
```

포워딩/필터링

패킷이 스위치에 들어온 경우, 도착지 MAC주소를 확인하고 자신이 가진 MAC 테이블과 비교해 맞는 정보가 있으면 매치되는 해당 포트로 패킷을 포워딩한다.
다른 포트로는 패킷을 보내지 않으므로 이 동작을 필터링이라 한다.

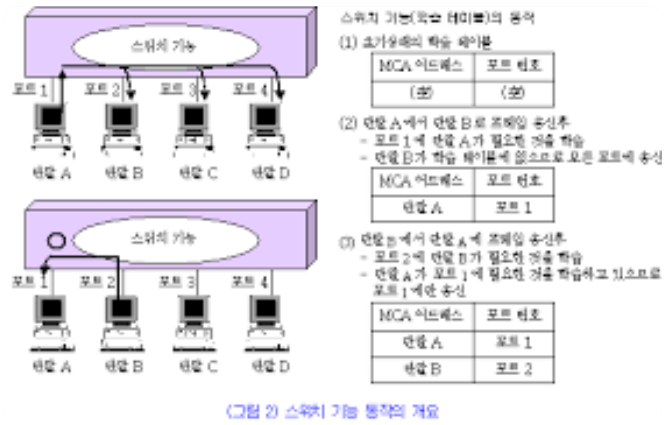
- 통신이 다른 포트에 영향을 미치지 않으므로, 기존 통신작업으로부터 독립적이기 때문에 포워딩과 필터링은 동시에 수행이 가능하다.

- 스위치는 일반적인 유니캐스트에 대해서만 포워딩과 필터링 작업을 수행한다.
- 출발지 MAC주소로 브로드캐스트나 멀티캐스트 모두 출발지가 사용되지 않으므로 이런 트래픽은 전달이나 필터링 작업을 하지 않고 모두 플러딩 한다.
- 언노운 유니캐스트도 MAC주소 테이블에 없는 주소이므로 플러딩으로 동작한다.

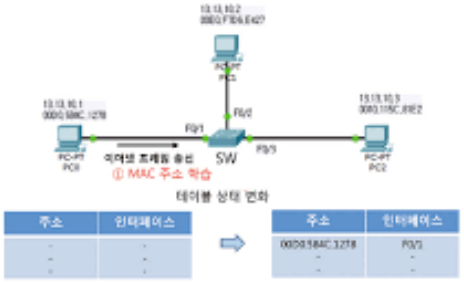
LAN에서의 ARP - 스위칭 동작

```
이더넷 TCP/IP 네트워크에서는 스위치가 유니캐스트를 플러딩하는 경우가 거의 없다.
ARP 브로드캐스트가 먼저 수행되야 하므로 유니캐스트 보다 ARP 브로드캐스트가 먼저 네트워크에 전
이 과정에서 MAC 출발지와 도착지를 습득하고 실제로 유니캐스트를 시작하면 이미 주소 테이블이 존
```

```
# 에이징 타임
ARP와 MAC테이블은 일정시간동안 지워지지 않는다.
MAC 테이블 에이징 타임 > ARP 에이징 타임
MAC 테이블 에이징 타임이 더 기므로 네트워크를 플러딩 없이 효율적으로 운영 가능
```



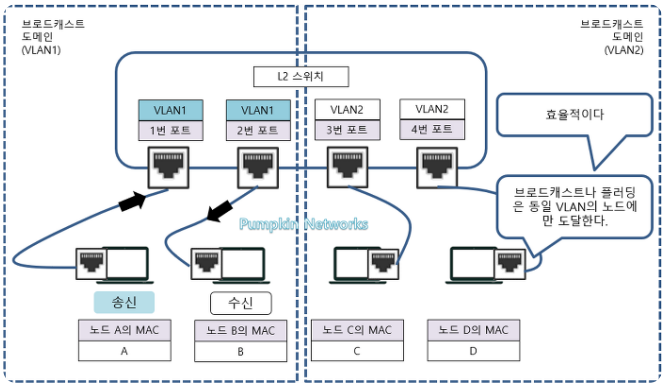
(그림 2) 스위치 기능 동작의 개요



VLAN

물리적 배치와 상관없이 LAN을 논리적으로 분할,구성하는 기술

- 조직 내에서 네트워크를 사용하기 위해서 네트워크가 분리되어 있어야함. → 브로드캐스트로 인한 단말들의 성능 저하, 보안 향상과 서비스 성격에 따른 정책 적용 등의 이유



- 한대의 스위치를 여러개의 VLAN으로 분할 가능. 동작도 별도의 스위치처럼 동작한다.
- VLAN을 사용하면 논리적으로 분할되어 있으므로, 유니캐스트 뿐 아니라 브로드캐스트 등 VLAN간 통신이 불가하다.

#VLAN(분리된 단말)간 통신을 위해서 3계층 장비가 필요하다.

- 물리적으로 다른 층에 있는 단말이 하나의 VLAN을 사용해 동일한 네트워크로 묶을 수 있다.

네트워크 리소스 보안을 높인다.

- 실제로 네트워크 그룹 이동을 하지 않아도 되기 때문에 보안 문제에 대한 우려를 줄일 수 있다.

비용을 절감할 수 있다.

- 서로 차단된 LAN 환경을 구축할 때 필요한 만큼 장비가 있어야한다.

불필요한 트래픽을 줄여준다.

- VLAN은 서로 다른 네트워크 망이기 때문에 브로드캐스트 통신시 다른 VLAN으로 전송되지 않는다.

관리자의 네트워크 설정 작업이 편리하다.

VLAN 종류와 특징

VLAN 할당 방식

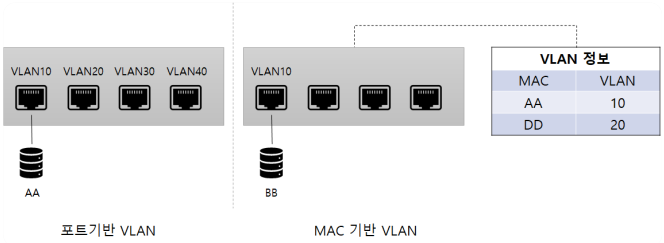
1. 포트 기반의 VLAN & Static VLAN
2. MAC 주소 기반의 VLAN & Dynamic VLAN

Static VLAN

스위치를 논리적으로 분할해 사용 하는 것이 목적인 VLAN을 포트 기반 VLAN이며, 대부분의 VLAN이 여기에 속한다.
어떤 단말이 접속하든지 스위치의 특정 포트에 VLAN을 할당하면 할당된 VLAN에 속하게 된다.
VLAN 선정 기준은 스위치의 포트

Dynamic VLAN

스위치의 고정 포트에 VLAN을 할당하는 것이 아니라 스위치에 연결되는 단말의 MAC주소를 기반으로 VLAN을 할당하는 기술
단말이 연결되면 단말의 MAC주소를 인식한 스위치가 해당 포트를 지정된 VLAN으로 변경한다. 단말에 따라 VLAN 정보가 바뀔 수 있어 다이나믹 VLAN이라 한다.
VLAN 선정 기준은 PC의 MAC 주소
예를 들어 어떤 스위치의 포트에 접속하더라도 VLAN 10이 할당된다.



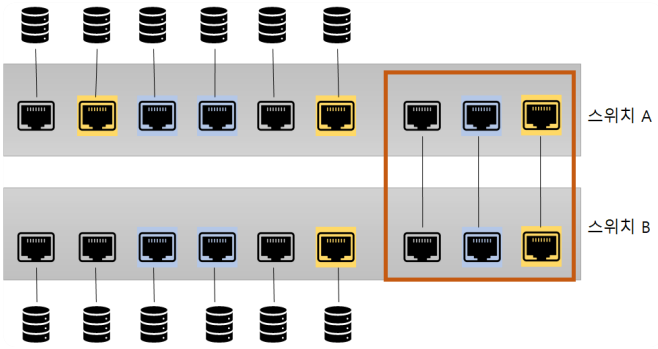
VLAN 모드 동작 방식

- 포트 기반 VLAN에서는 스위치의 각 포트에 각각 사용할 VLAN을 설정하는데 한 대의 스위치에 연결되더라도 서로 다른VLAN이 설정된 포트 간에는 통신이 불가.

- VLAN으로 구분된 네트워크는 브로드캐스트 ARP 리퀘스트가 전달이 안되므로 3계층 장비를 사용해서 서로 통신해야한다.

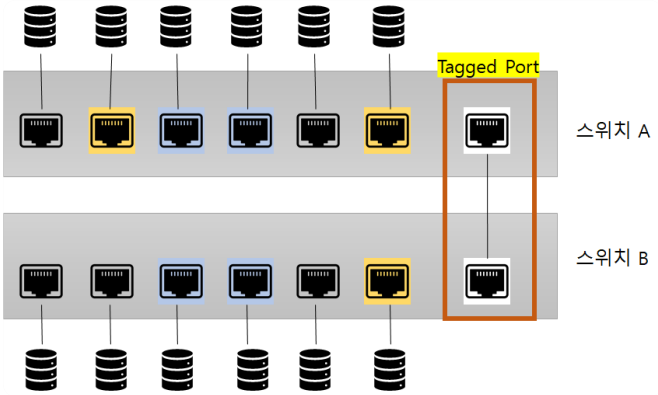
- VLAN 분리는 다수의 논리적인 스위치를 만드는 효과가 있다.

- 스위치를 서로 연결해야 하는 경우에는 각 VLAN끼리 통신하려면 VLAN 개수만큼 포트가 필요하다.
- VLAN으로 분할된 스위치는 물리적으로 별도의 스위치처럼 취급되기 때문이다. → 포트 낭비 발생

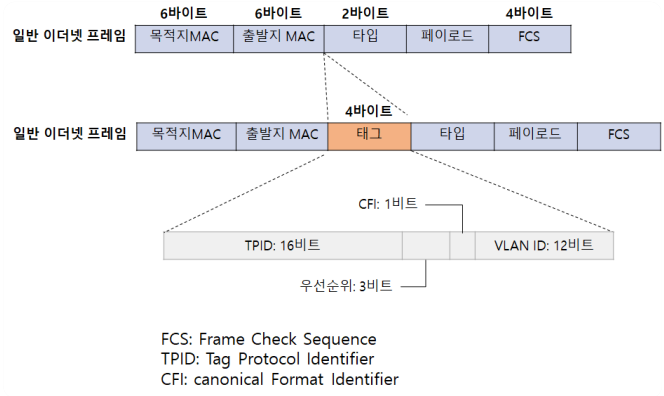


태그 포트 & 트렁크 포트(Cisco)

- 태그 포트를 이용해 스위치를 연결하여 한개의 포트로 여러 VLAN통신이 가능하다. 이 포트를 태그포트 또는 트렁크 포트라 한다.



- 여러개의 VLAN을 동시에 전송해야 하기 때문에 통신할 때 이더넷 프레임 중간에 VLAN ID필드를 끼워 넣어 이 정보를 사용한다.



FCS: Frame Check Sequence
TPID: Tag Protocol Identifier
CFI: canonical Format Identifier

> 포트 낭비가 사라짐

- 태그 포트로 패킷을 보낼 때는 ***VLAN ID***를 붙이고 -> 수신 측에서는 ***VLAN ID***를 제거하면서 VLAN ID의 VLAN으로 패킷을 보낼수 있다.
- 태그 포트 기능으로 인해 스위치의 패킷 전송에 사용하는 MAC테이블에 VLAN을 지정하는 필드가 추가됨.
- VLAN별로 MAC 주소 테이블이 존재하는 것처럼 동작한다.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.96d5.8401    DYNAMIC     Fa0/3
   1    0002.17bc.8ab9    DYNAMIC     Fa0/2
   1    0002.4ac5.7601    DYNAMIC     Fa0/1
   1    0010.118a.6139    DYNAMIC     Fa0/1
   1    00d0.d366.acad    DYNAMIC     Fa0/1
```

- VLAN을 사용하면 MAC 테이블에도 VLAN 정보가 함께 기록된다.

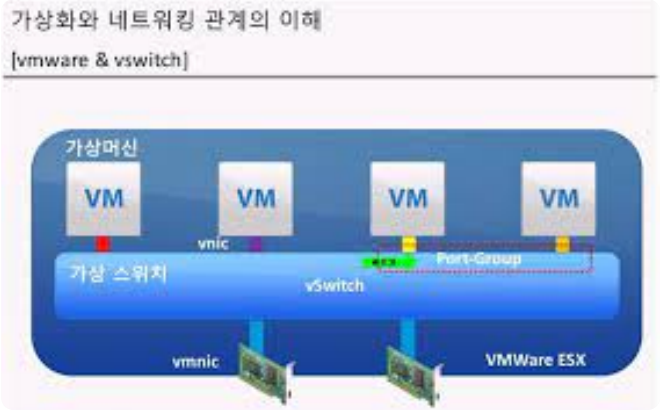
- 일반적인 포트 - 언태그 포트 & 액세스 포트
  - 여러개의 VLAN 여러 네트워크를 하나의 물리적 포트로 전달하는데 사용된다.

- VLAN 정보를 넘겨 여러 VLAN이 한꺼번에 통신하도록 해주는 포트 - 태그 포트 & 트렁크 포트
  - 하나의 VLAN에 속한 경우에만 사용된다.

> 태그 포트는 여러 네트워크가 동시에 설정된 스위치 간의 연결에서 사용되며 하나의 네트워크에 속한 서버의 경우 언태그로 설정

- 언태그 포트로 패킷이 오면 같은 VLAN으로만 패킷을 전송한다.
- 태그 포트로 패킷이 들어오면, 태그를 벗겨내면서 태그된 VLAN쪽으로 패킷을 전송한다.

가상화 서버가 연결될 때는 여러 VLAN과 통신해야 할 수도 있다.
서버와 연결된 스위치의 포트더라도 언태그 포트가 아닌 태그로 설정한다. 가상화 서버쪽 인터페이스 또한 태그된 상태로 설정해야 한다.
가상화 서버 내부에 가상 스위치가 존재하므로 스위치 간 연결로 보면 이해하기 더 쉽다.



STP

SPoF(Single Point of Failure)로 인한 장애를 피하기 위해 다양한 노력을 함.

- 하나의 시스템이나 구성 요소에서 고장이 발생했을 때 전체 시스템의 작동이 멈추는 요소를 말한다.
- 전체 네트워크가 마비되는 것을 방지하기 위해 이중화,다중화된 네트워크를 디자인하고 구성한다.

> 네트워크를 스위치 하나로 구성했을 때 그 스위치에 장애가 발생하면 전체 네트워크에 장애가 발생한다.

- SPoF를 피하기 위해 스위치 두대의 구성으로 네트워크를 디자인한다. → 패킷이 네트워크를 따라 계속 전송되서 마비될 수가 있다. 이런 상황을 루프라 한다.

루프란?

네트워크에 연결된 모양이 연결된 모양이 고리처럼 되돌아오는 형태로 구성된 상황

- 루프 상태이면 통신이 안된다.

루프의 원인

1. 두 장비 간 이중화연결은 되어 있지만 이중화 프로토콜 미사용
2. 장비 간의 연결이 단일고리 형태로 연결
3. 장비 간의 연결이 중복고리 형태로 연결

대부분 브로드캐스트 스톰으로 인한 문제

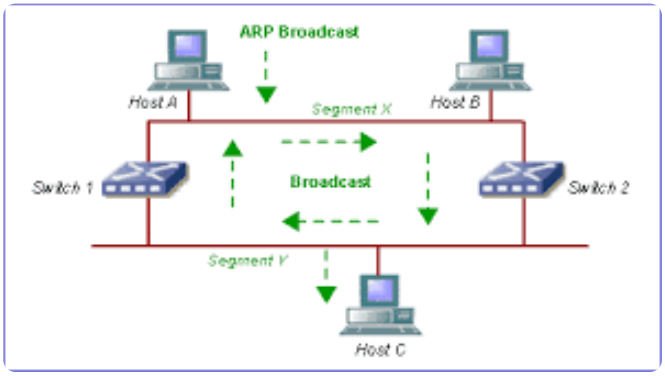
브로드캐스트 스톰

과정

1. 루프 구조로 연결된 상태
2. 단말에서 브로드캐스트를 발생시킨다.
3. 스위치는 이 패킷을 패킷이 유입된 포트를 제외한 모든 포트로 플러딩
4. 플러딩된 패킷은 다른 스위치로도 보내지고 이 패킷을 받은 스위치는 패킷이 유입된 포트를 제외한 모든 포트로 다시 플러딩

5. 과정 반복
6.

- 3계층에서는 TTL을 통해 패킷수명이 존재하지만 2계층 헤더에는 이러한 메커니즘이 부재
- 즉, 패킷이 계속 살아남아 전체 네트워크 대역폭을 차지할수 있다.



증상

1. 네트워크에 접속된 단말의 속도가 느려진다.
2. 네트워크 접속 속도가 느려진다.
3. 네트워크에 설치된 스위치에 모든 LED들이 동시에 빠른 속도로 깜빡인다.

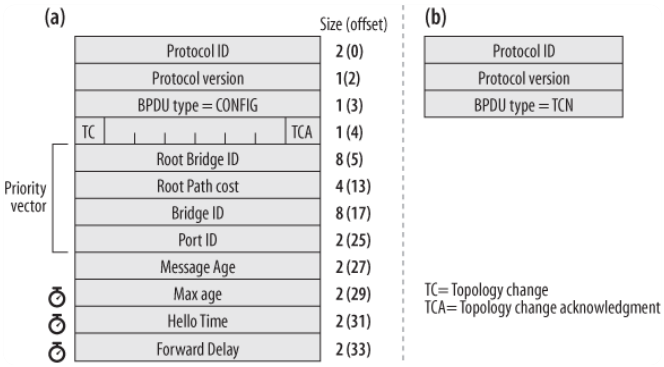
스위치 MAC 러닝 중복 문제

STP란?

스패닝 트리 프로토콜

- 루프를 확인하고 적절히 포트를 사용하지 못하게 만들어 루프를 예방하는 메커니즘

- 스위치는 BPDU라는 프로토콜을 통해 스위치 간에 정보를 전달하고 이렇게 수집된 정보를 이용해 전체 네트워크 트리를 만들어 루프 구간을 확인한다.
- BPDU에는 스위치가 갖고 있는 ID와 같은 고유값이 들어가고 이런 정보들이 스위치 간에 서로 교환되면서 루프 파악이 가능해진다.
- 루프 지점을 파악하고 해당 지점을 데이터 트래픽이 통과하지 못하도록 차단한다.



스위치 포트의 상태 및 변경 과정

- 스패닝 트리 프로토콜이 동작중인 스위치에서는 스위치 포트에 신규 스위치가 연결되면 바로 트래픽이 흐르지 않도록 차단하여 루프를 막는다.
- 트래픽을 흘리기 전 확인을 위해 BPDU를 기다려 학습하고 구조를 파악한 후 트래픽을 흘리거나 루프 구조인 경우 차단을 유지한다.

스위치 포트의 상태

Blocking : 스위치를 맨 처음 켜거나 Disabled 되어 있는 포트를 관리자가 다시 살린 상태. 이 상태에서는 데이터 전송은 불가능하고 오직 BPDU만 송수신이 가능하다. 스패닝 트리의 3가지 선정 과정이 이 블로킹 단계에서 이뤄진다.

- 패킷 데이터를 차단한 상태로 상대방이 보내는 BPDU 대기
- 20초동안 상대방 스위치에서 BPDU를 받지 못했거나 후순위 BPDU를 받았을 때 포트는 리스닝 상태로 변경
- BPDU 교환 주기는 2초 10번의 BPDU 기다림
- 맥 어드레스 러닝 불가능

Listening : 블로킹 상태에 있던 스위치 포트가 루트포트나 데지그네이티드 포트로 선정되면 포트는 바로 리스닝 상태로 넘어간다.
리스닝 상태에 있던 포트도 상황에 따라 다시 Non Designated 포트로 변할 수 있고 그러면 다시 블로킹 상태로 돌아간다.

- 총 15초 동안 대기
- 해당 포트가 전송상태로 변경되는 것을 결정하고 준비하는 단계 자신의 BPDU 정보를 상대방에게 전송하기 시작

Learing : 리스닝 상태에 있던 스위치 포트가 포워딩 딜레이 디폴트 시간인 15초 동안 계속 그 상태를 유지하면 리스닝 상태는 러닝 상태로 넘어간다. 이 상태에서야 비로소 맥 어드레스를 배워 맥 어드레스 테이블을 만들기 시작할 수 있다.

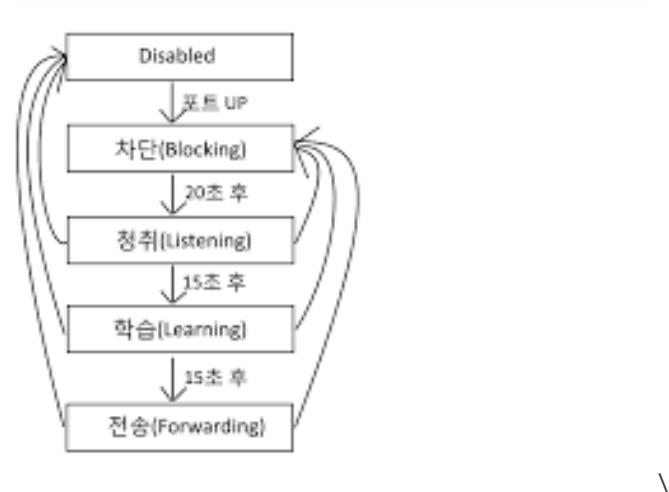
- 총 15초 동안 대기
- 러닝 상태는 이미 해당 포트를 포워딩하기로 결정하고 실제로 패킷 포워딩이 일어날 때 스위치가 곧바로 동작하도록 MAC주소를 러닝하는 단계

Fowarding : 스위치 포트가 러닝 상태에서 다른 상태로 넘어가지 않고 다시 포워딩 딜레이 디폴트 시간인 15초동안 유지하면 러닝 상태에서 포워딩 상태로 넘어가게 된다. 포워딩 상태가 되어야 스위치 포트는 드디어 데이터 프레임을 주고받을 수 있게 된다.

- 패킷을 포워딩하는 단계. 정상적인 통신 가능

> 스위치에 신규로 장비를 붙이면 통신하는데 50여초 소요된다.

- 루프를 예방하기 위해 방어적으로 동작하는데 BPDU를 일정시간 이상 기다려 스위치 여부를 파악한다. 일반 단말을 연결할때에도 동일한 시간이 필요하다.



\

- 이중화된 링크 절체(전환)도 STP의 동작 순서대로 진행된다.
- 블로킹 상태에서 포워딩까지 총 50초 후 포워딩 상태로 변경
- 다운된 링크가 자신의 인터페이스인 경우, 리스닝부터 STP 상태 변화가 즉시 이루어지므로 30초 만에 절체된다.

- STP가 활성화된 경우, 스위치 포트는 곧바로 포워딩 상태가 되지 않는다.

문제가 발생하는 예시

- 부팅시간이 빠른 OS가 DHCP 네트워크에 접속할때 부팅단계에서 IP를 요청하지만 스위치 포트가 포워딩 상태가 되지 않아 (시간이 걸려서) IP 정상적으로 할당이 안되는 경우가 많다.

STP동작 방식

루프를 없애기 위해 나무가 뿌리에서 가지로 뻗어나가는 것처럼 토폴로지를 구성
뿌리가 되는 가장 높은 스위치(루트 스위치)를 선출하고 그 스위치를 통해 BPDU가 교환되도록 한다.
BPDU를 통해 2초마다 루트 스위치임을 광고하고 교환된 BPDU에 있는 브릿지 ID 값을 비교하여 ID 값이 적은 스위치를 루트 스위치로 선정한다.

스패닝 트리 프로토콜 동작

1. 하나의 루트 스위치 선정
    - 전체 네트워크에 하나의 루트 스위치 선정
    - 자신을 전체 네트워크의 대표 스위치로 적은 BPDU를 옆 스위치로 전달
2. 루트가 아닌 스위치 중 하나의 루트 포트를 선정한다.
    - 루트 브릿지로 가는 경로가 가장 짧은 포트를 루트포트라 한다
    - 루트 브릿지에서 보낸 BPDU를 받는 포트
3. 하나의 세그먼트에 하나의 지정포트를 선정한다.
    - 스위치와 스위치가 연결되는 포트는 하나의 지정 포트를 선정
    - 이미 루트포트로 선정된 경우, 반대쪽이 지정 포트로 선정되어 양쪽 모두 포워딩 상태가 된다.

- 스위치 간 연결에서 아무도 루트포트가 아니면 한쪽은 지정 포트로 선정되고 다른 쪽은 대체포트로 되어 차단 상태가 된다.
- BPDU가 전달되는 포트이다.

```
# Port Fast
좀 더 빠른 시간안에 포워딩 상태로 변경하기 위해 설정
BPDU 대기, 습득 과정 없이 바로 포워딩 상태로 포트 사용 가능
루프가 생길 수 있어 포트를 차단하는 BPDU가드가 같이 사용되어야함.
```

스패닝 트리 프로토콜이 동작하는 네트워크에서 스위치(브리지)들 중 **단 하나만 대장브리지**(Root Bridge)가 되고 **대장 브리지의 모든 포트는 대표포트(지정포트)**이다. 대장 브리지가 아닌 브리지들은 루트 브리지로 향하는 가장낮은 스패닝 트리 코스트를 가지는 루트 포트가 존재한다. 또 물리적으로 연결된 브리지들 사이에는 **하나의 대표포트**가 존재한다.

https://blog.daum.net/esde21ws/5484044

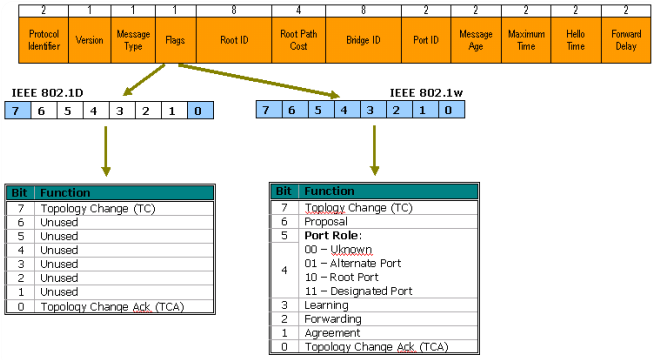
향상된 STP

스패닝 트리 프로토콜은 블로킹에서 포워딩까지 총 50초가 소요되므로, 네트워크가 끊기면 30초를 기다리지 못하다보니 STP기반 네트워크에 장애가 생기면 통신이 끊길수 있다.
또한 VLAN이 여러개면 각 VLAN별로 스패닝 트리 프로토콜을 계산하여 부하가 발생한다.

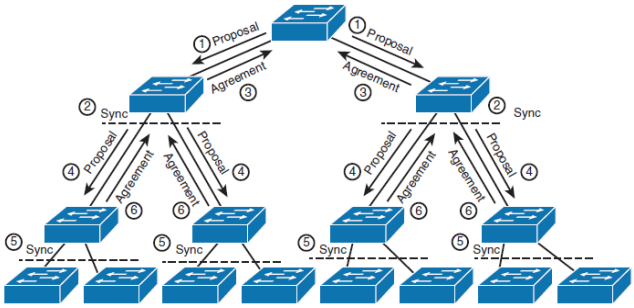
RSTP (Rapid Spanning Tree)

> 이중화된 스위치 경로 중 정상적인 경로에 문제가 발생할 경우, 백업 경로를 활성화하는데 30~50초가 걸린다.
> RSTP를 사용해 문제 해결

- RSTP는 2~3초로 절체시간이 짧아서 일반적인 TCP 기반 애플리케이션이 세션을 유지할 수 있게 된다.
- 구성과 동작방식은 STP와 동일
- BPDU 메시지 형식이 다양해서 여러가지 상태메시지 교환 가능
- STP 메세지 요소
  - TCN
  - TCA
  - BPDU
- RSTP는 8개 비트를 모두 사용해 다양한 정보를 주고 받는다.



> 기존 STP는 토폴로지가 변경되면 말단 스위치에서 루트 브릿지까지 변경 보고를 보내고 루트 브릿지가 그에 대한 연산을 다시 완료하고 이후 변경된 포톨로지 정보를 말단 스위치까지 보내는 과정을 거쳤는데 모든 스위치까지 전파되는 예비시간까지 고려해야 하므로 정보를 확정하는데 오래 걸렸다.



RSTP는 토폴로지 변경이 일어난 스위치 자신이 모든 네트워크에 토폴로지 변경을 직접 전파한다.
루트 브릿지를 거치지 않고 터미널 스위치가 다른 브리지에게 직접 전달한다.

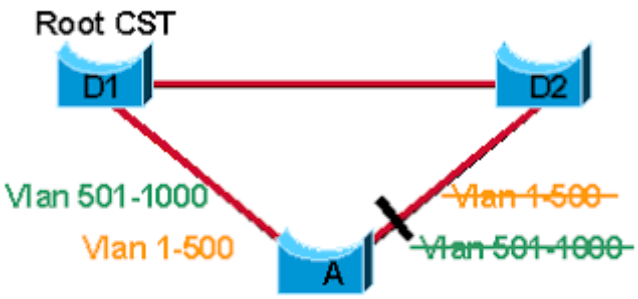
장점

- 빠른 시간 내에 토폴로지 변경 감지, 복구가 가능
- 2~3초만에 장애 복구가 가능
- 안정적으로 네트워크 운영 가능

MST

CST

- 일반 스패닝 트리 프로토콜은 CST(Common Spanning Tree)라고 부른다
- VLAN 개수와 상관없이 스패닝트리 한개만 동작하므로 부하가 적다
- 루프가 생기는 토폴로지에서 한개의 포트와 회선만 활성화되어 자원을 효율적으로 사용 못한다.
- 최적의 경로를 사용할수 없을 수도 있다. → PVST 개발(Per VLAN Spanning Tree)



PVST

- VLAN 마다 별도의 스패닝 트리 프로세스 동작
- VLAN 마다 별도의 경로와 트리를 만들 수 있다.
- VLAN마다 별도의 블록 포트를 지정해 네트워크 로드를 셰어링하도록 구성할수 있다.

단점

- 모든 VLAN마다 별도의 스패닝트리를 유지해야 하므로 많은 부담이 간다.
- CST와 PVST를 보완하기 위해 MST(Multiple Spanning Tree) 개발

MST는 여러개의 VLAN을 그룹으로 묶고 그룹마다 별도의 스패닝 트리가 동작한다.
PVST보다 적은 스패닝 트리 프로세스가 동작한다.
로드 셰어링도 사용 가능

- 리전 개념이 도입되어 1개 리전 - 스패닝 트리 1개

```
# 스패닝 트리 프로토콜 대안
많은 프로토콜이 포트가 차단되거나 늦게 포워딩 되어 불편한 점이 많음.
FortFast
UplinkFast
BackboneFast
사용을 하지만, 그래도 근본적 해결은 되지 않으므로 네트워크를 잘개 쪼개거나 대체제를 사용한다
```

- SLPP
- ExtremeSTP
- Loop Guard
- BPDU Guard

```
# 스위치의 구조와 스위치에 IP주소가 할당된 이유
스위치 관리용 컨트롤 플레인과 패킷을 포워딩하는 데이터 플레인으로 구성
컨트롤 플레인
STP,텔넷,SSH,웹과 같은 서비스 수행

일정 규모 이상의 네트워크에서 운영되는 스위치는 관리 목적으로 대부분 IP주소가 할당된다.
```