네트워크 초급 과정

Netwrok Begginner Class

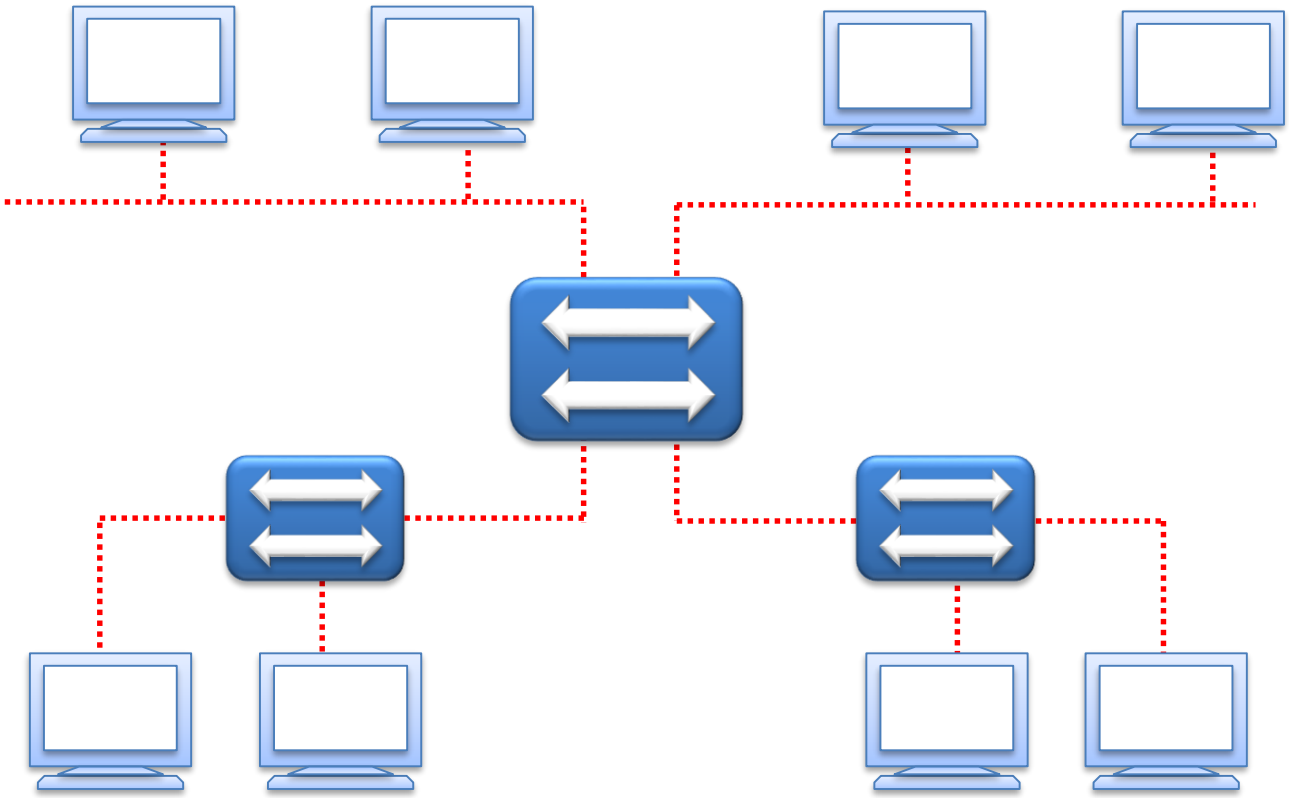
Chapter 04 Switching

01 Transparent Bridging

Basic functions of Switch

스위치에서는 데이터를 어떻게 처리하는지
기본적인 동작원리를 배워보자.

Ethernet Switches and Bridges



- Address learning
- Forwarding/Filtering
- Loop avoidance

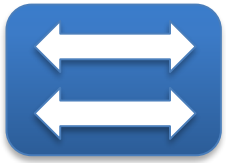
Transmitting Frames

01 Cut-through

목적지 주소를 확인한 후 즉시 전달하는 방법

V

D-mac	S-mac	Type	Data	FCS



02 Store and Forward

03 Fragment-free

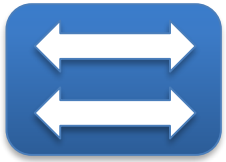
Transmitting Frames

01 Cut-through

02 Store and Forward

프레임을 모두 전송받아 검사 후전달하는 방법

D-mac	S-mac	Type	Data	FCS



03 Fragment-free

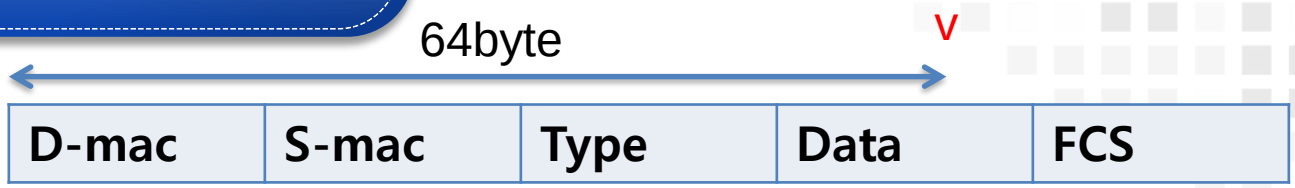
Transmitting Frames

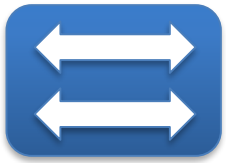
01 Cut-through

02 Store and Forward

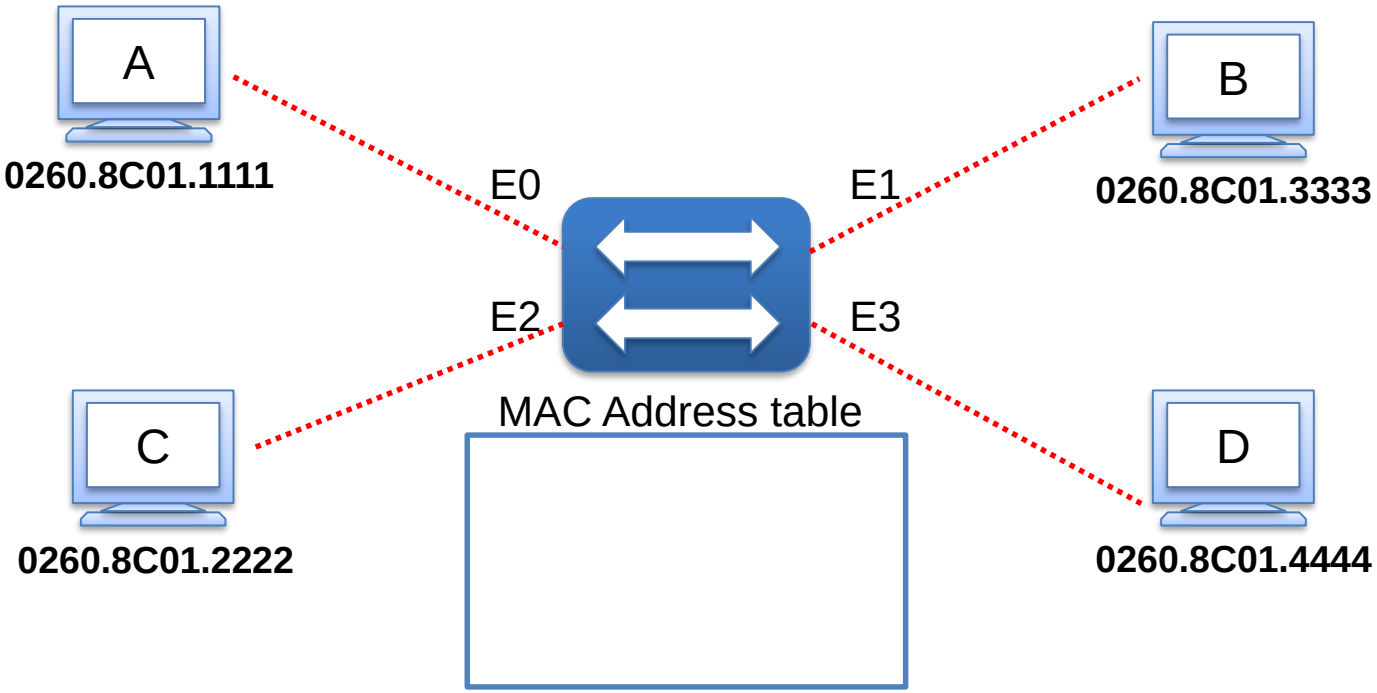
03 Fragment-free

프레임의 64byte까지 검사 후전달하는 방법



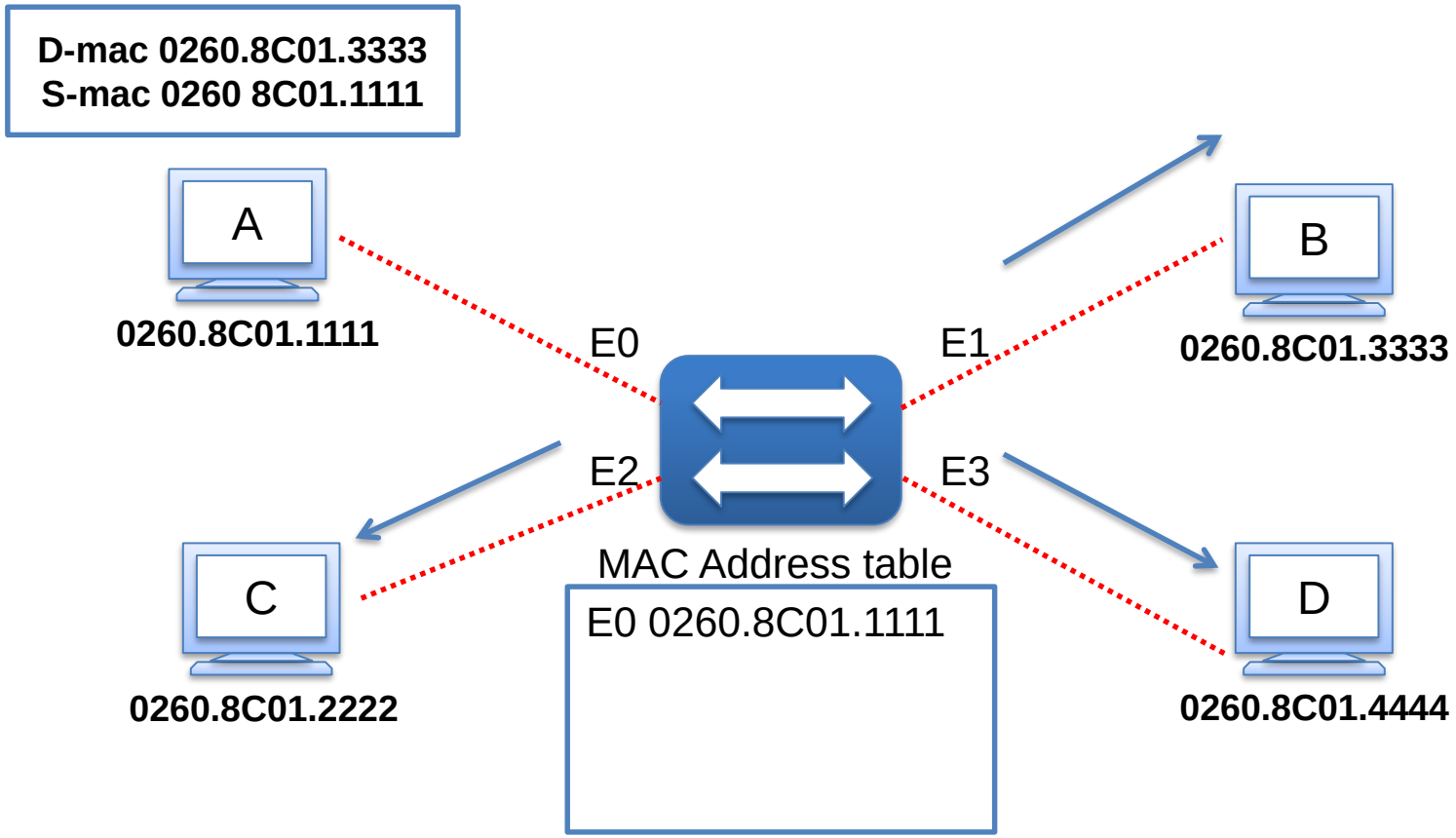


MAC Address Table



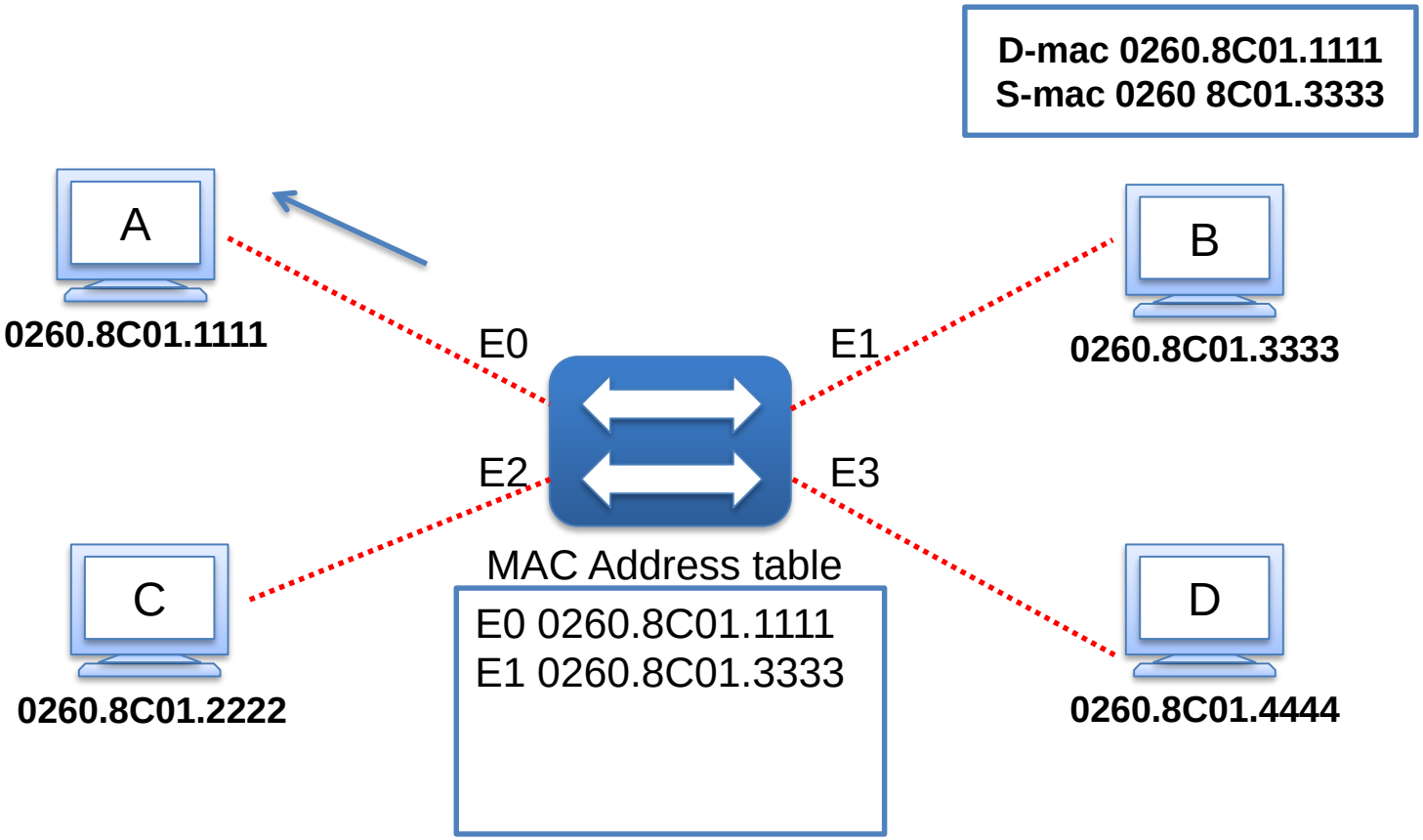
- 초기에는 MAC Address Table이 비어 있다

Transparent Bridging



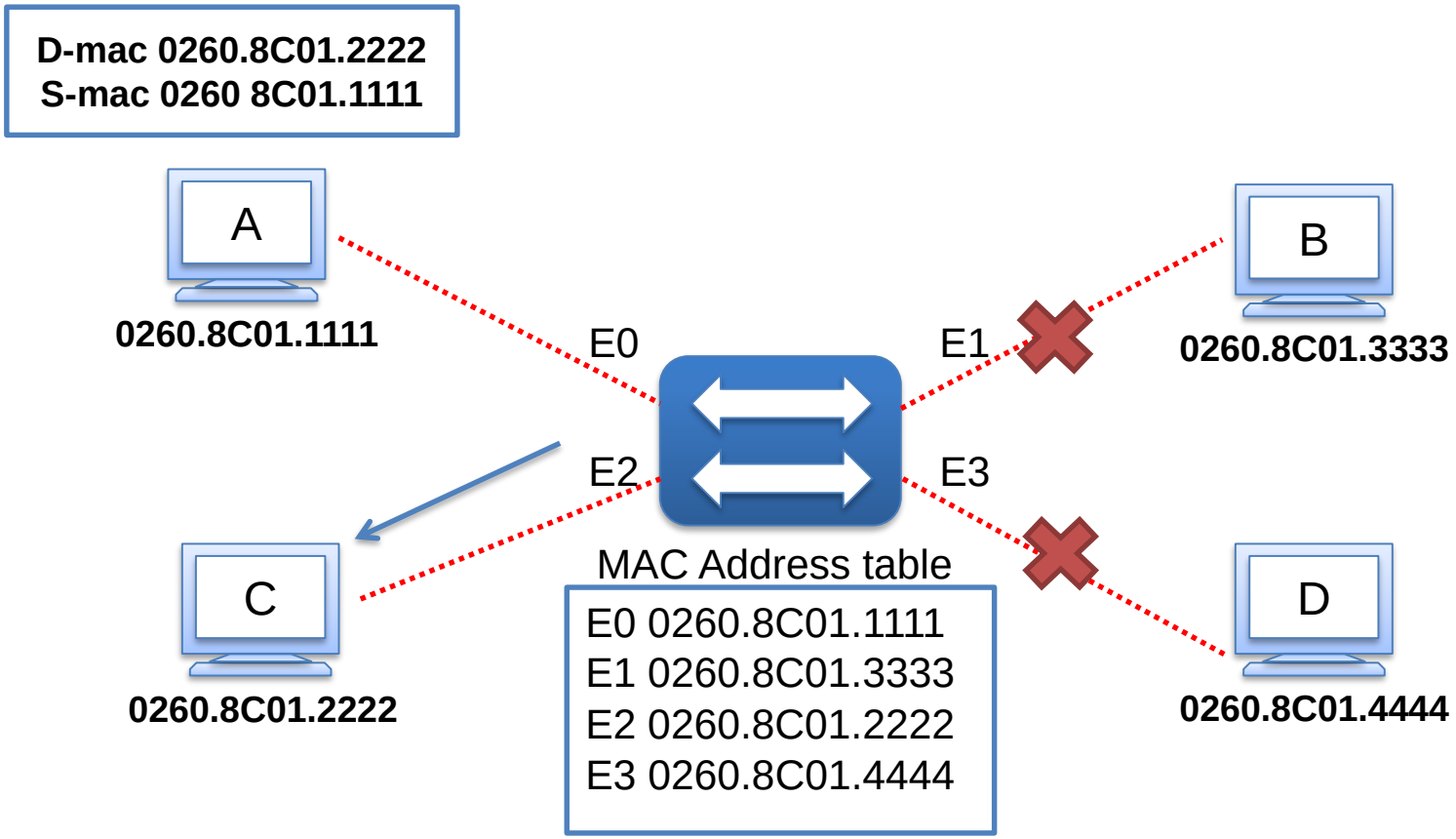
- **Host A가 Host B에게 Frame을 전달하려고 한다**

Transparent Bridging



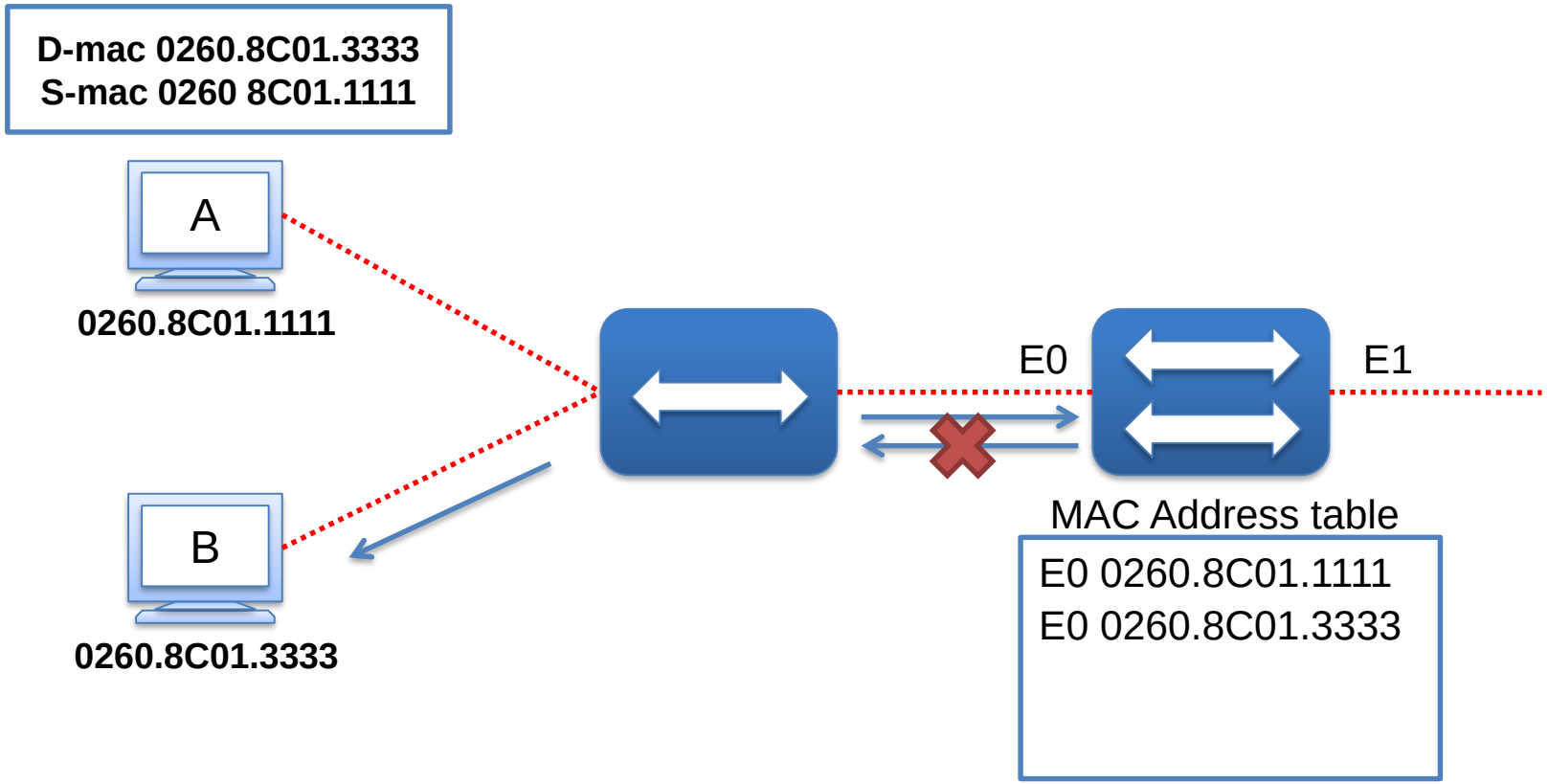
- **Host B가 Host A에게 Frame을 전달하려고 한다**

Forwarding Frames



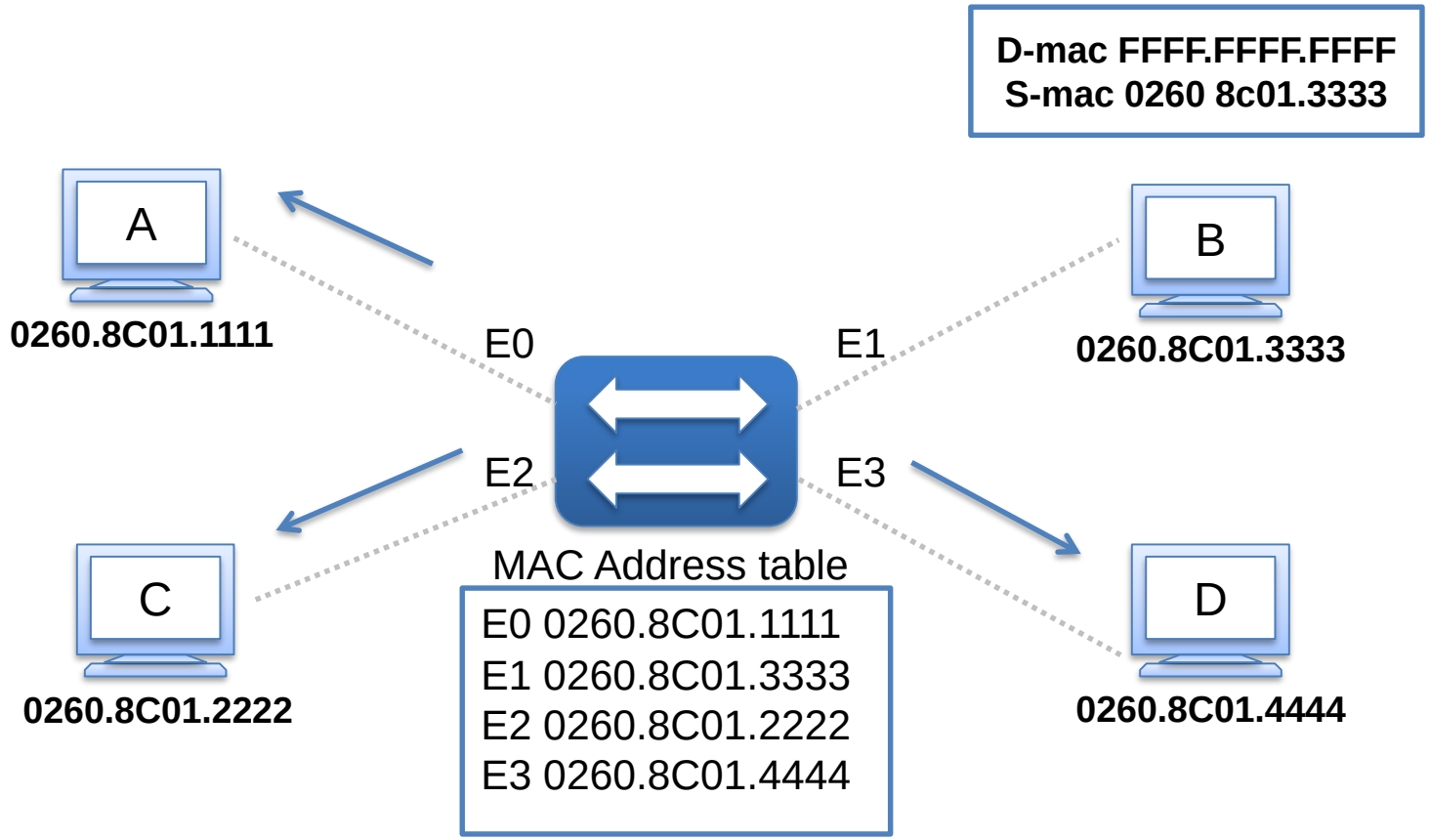
- **Host A가 Host C에게 Frame을 전달하려고 한다**
- **E2에 대한 Aging Time이 초기화 된다**

Filtering Frames



- **Host A가 Host B에게 Frame을 전달하려고 한다**

Broadcast and Multicast Frames



- **Host B가 Broadcast 또는 Multicast Frame을 전달하려고 한다**

02

Configuration a Switch

How can I Configure switch?

기본적인 스위치 설정에 대해서 알아보자.

Setting Speed and Duplex options

Switch의 interface에서 duplex와 speed 설정

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# duplex { auto | full | half }
Switch(config-if)# speed { 10 | 100 | auto }
```

Showing the Duplex options

Duplex 설정 확인

```
Switch# show interface fastethernet 0/1
FastEthernet0/3 is up, line protocol is down
  Hardware is Fast Ethernet, address is 0000.0000.0003 (bia 0000.0000.0003)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Managing the MAC Address Table

Switch의 MAC Address Table 확인

```
Switch# show mac-address- table
Dynamic Address Count:                  1
Secure Address Count:                   0
Static Address (User-defined) Count:    0
System Self Address Count:              25
Total MAC addresses:                    26
Maximum MAC addresses:                  8192
Non-static Address Table:
Destination Address     Address Type        VLAN    Destination Port
-----------------------  ------------------  -------  --------------------
0050.0f02.3372          Dynamic             1       FastEthernet0/2
```

Setting a MAC Address Static

Switch에서 MAC Address를 수동으로 설정

Switch(config)# mac-address-table static {*mac-address*} vlan {*vlan-id*} interface *type* {*slot/port*}

MAC Address 수동 설정 확인

```
Switch(config)# mac-address-table static 1111.1111.1111 vlan 1 interface fastethernet 0/1
Switch# show mac-address-table
Dynamic Address Count:                  1
Secure Address Count:                   0
Static Address (User-defined) Count:    1
….
Destination Address     Address Type        VLAN    Destination Port
-----------------------  -----------------  -------  --------------------
0050.0f02.3372          Dynamic             1       FastEthernet 0/2
1111.1111.1111          Static              1       Fastethernet 0/1
```

Clearing NVRAM

Switch의 Startup-config 삭제

```
Switch# erase startup-config
```

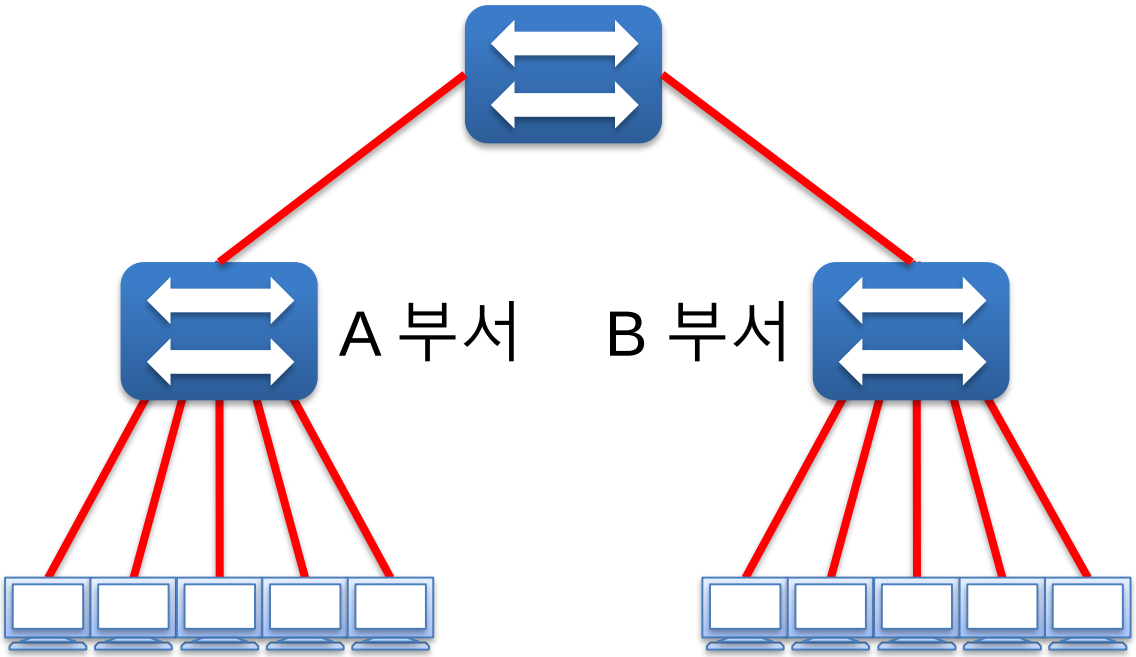
- Startup-config 파일을 제거하면 모든 구성 정보가 제거된다
- Reload를 하면 초기화 된 상태로 부팅하게 된다

03 VLAN

VLAN Concept

사용자의 증가로 LAN의 영역이 점점 커지게 되면서 많은 양의 브로드캐스트를 처리해야 하는 스위치로써는 장비의 성능이 저하되는 문제를 가지게 된다. 이 외에도 발생되는 여러 문제들을 해결하기 위해 LAN의 영역을 분리하기 위한 방법으로 VLAN을 사용하게 되었다.

VLAN Overview

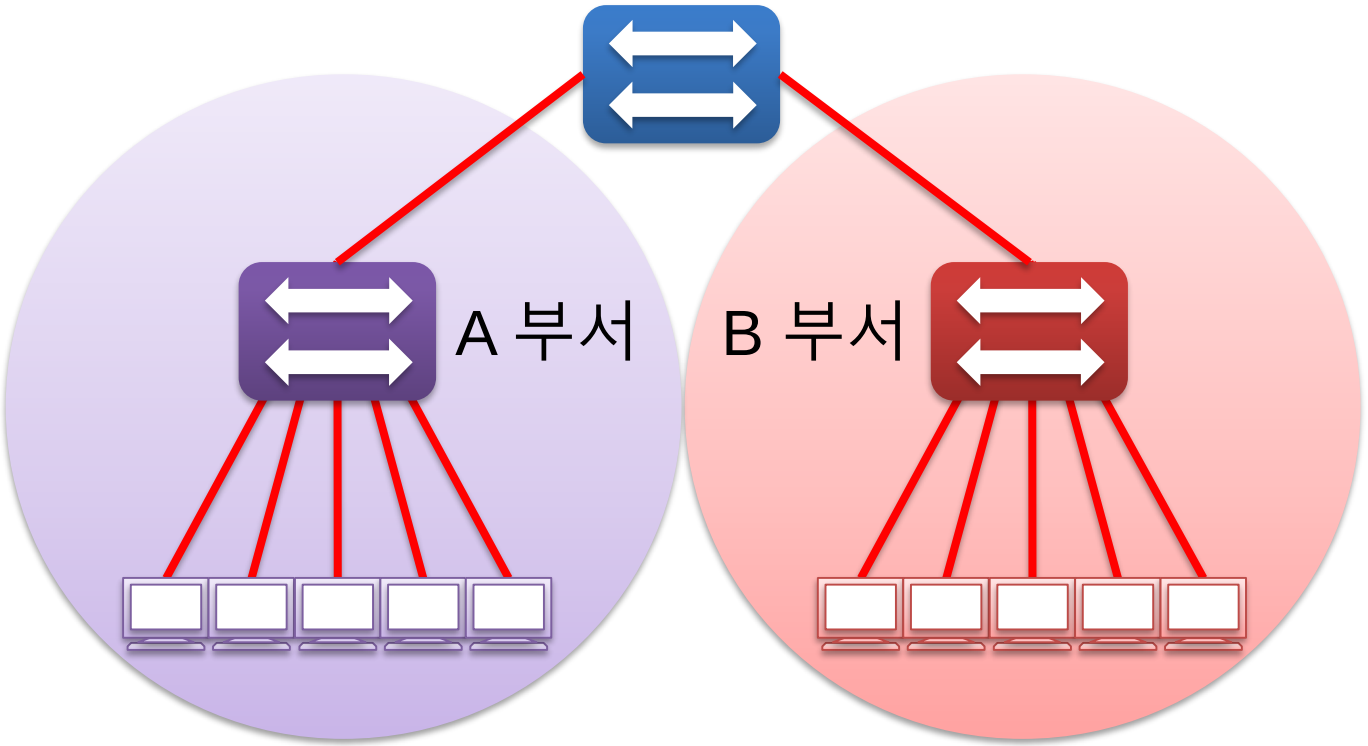


LAN

- 동일한 LAN 영역에 있는 장치들은 서로 통신을 할 수 있다.
- LAN 영역에 있는 장치의 수가 늘어나게 되면서 브로드캐스트 트래픽이 폭발적으로 증가하고 이로 인해 전체 네트워크의 가용성이 떨어지게 되었다.
- 서로 다른 부서간에 불필요한 통신을 하게 되면서 보안성도 문제가 되었다.

Local Area Network

VLAN Overview

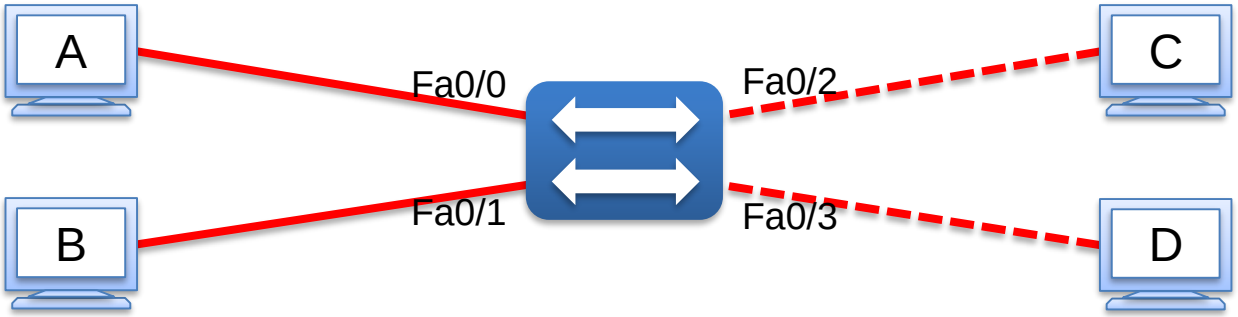


VLAN

- Switch가 가지고 있는 Port를 VLAN ID 그룹에 소속 시켜 운영 한다.
- VLAN을 통해 영역을 나눔으로 인해 불필요한 브로드캐스트 트래픽을 제한하여 네트워크의 가용성이 높아지게 된다.
- 트래픽이 제한되기 때문에 보안성이 증가 된다.

Virtual - LAN

VLAN Overview



MAC Address	VLAN ID	Port
0000.0000.000A	10	Fa0/0
0000.0000.000B	10	Fa0/1
0000.0000.000C	20	Fa0/2
0000.0000.000D	20	Fa0/3

VLAN Table

- MAC Address Table에는 Mac 주소와 Port의 정보 뿐만 아니라 VLAN ID 정보까지 기록 되어 있다.
- 이를 통해서 서로 다른 VLAN ID 그룹에 속해 있는 장치와의 통신을 차단 할 수 있게 된다.

VLAN 테이블

VLAN Overview

VLAN 정리

Virtual LAN 특징

- 하나의 LAN 영역을 여러 개의 가상의 구역으로 나누는 기술이다.
- VLAN으로 나누어진 영역은 독립된 브로드캐스트 도메인 영역으로 나누어지게 된다.
- VLAN으로 나누어진 영역은 같은 그룹에 속해 있어야 통신을 할 수 있다.
- VLAN은 VLAN ID로 구분을 지으며, 같은 VLAN ID 그룹에 속해야 통신을 할 수 있다.
- Switch에서는 Port 별로 각각의 VLAN 그룹에 소속시켜 운영한다.
- 특정 VLAN 그룹에 속하여 운영되는 Port를 Access Port라 한다.
- VLAN ID는 번호로 구분이 되며, 2^12 = 4096개의 구분 번호가 있다.
- 서로 다른 VLAN간에 통신을 하기 위해서는 Routing 기능이 있는 라우터나 멀티레이어 스위치가 필요 하다.

VLAN Configuration

Virtual LAN

VLAN Configure

VLAN 생성 및 이름 설정

SW1(config)# **vlan** *vlan-id*
SW1(config-vlan) # **name** *name*

VLAN 삭제

SW1(config)# **no vlan** *vlan-id*

Access port 설정

SW1(config)# **interface fastethernet** *slot / port*
SW1(config-if) # **switchport mode access**
SW1(config-if) # **switchport access vlan** *vlan-id*

Interface 범위 설정

SW1(config)# **interface range fastethernet** *slot / port – port*

SW1(config)# **interface range fastethernet** *slot / port* , **fastethernet** *slot / port*
SW1(config-if-range)#

VLAN Verification

VLAN 확인

SW1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10	Red	active	Fa0/1, Fa0/2
20	Blue	active	Fa0/3, Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN Verification

MAC Address Table과 VLAN

SW1# **show mac-address-table**

Mac Address Table

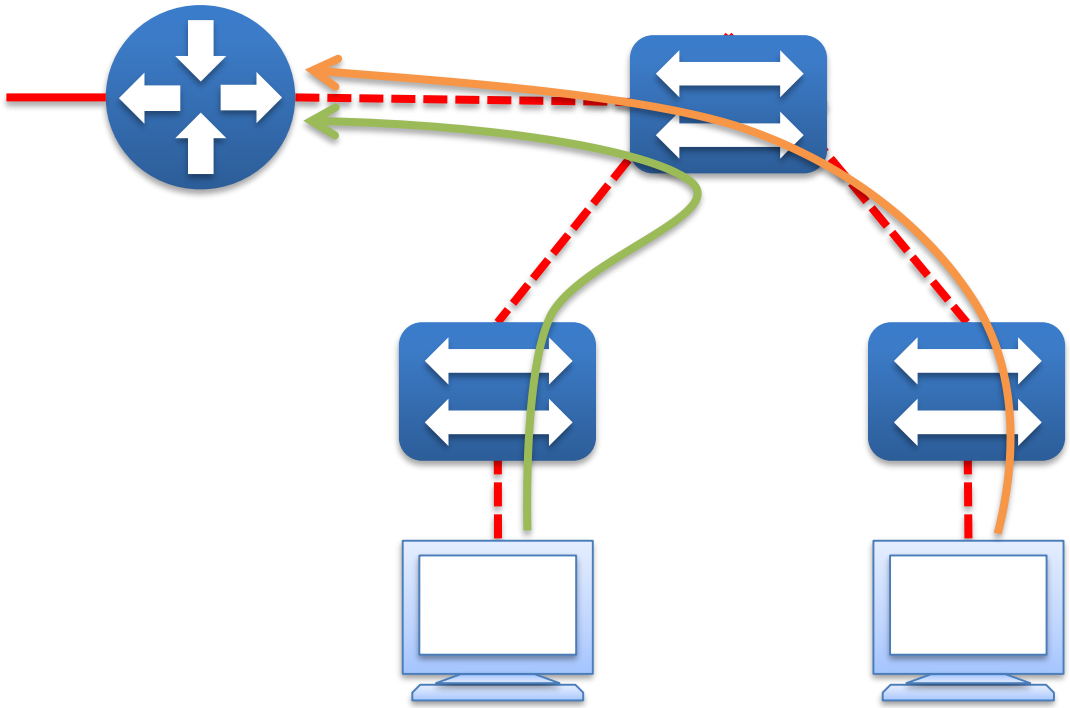
Vlan	Mac Address	Type	Ports
10	0002.17b6.a643	DYNAMIC	Fa0/1
10	0010.1189.7862	DYNAMIC	Fa0/2
20	0001.6416.aa88	DYNAMIC	Fa0/3
20	0002.4ac5.9230	DYNAMIC	Fa0/4

04 STP

Spanning Tree Protocol Concept

LAN 이중화 구성에서 발생되는 Loop 문제를 파악하고 이를 해결 할 수 있는 기술인 STP에 대해서 알아보자.

Redundancy

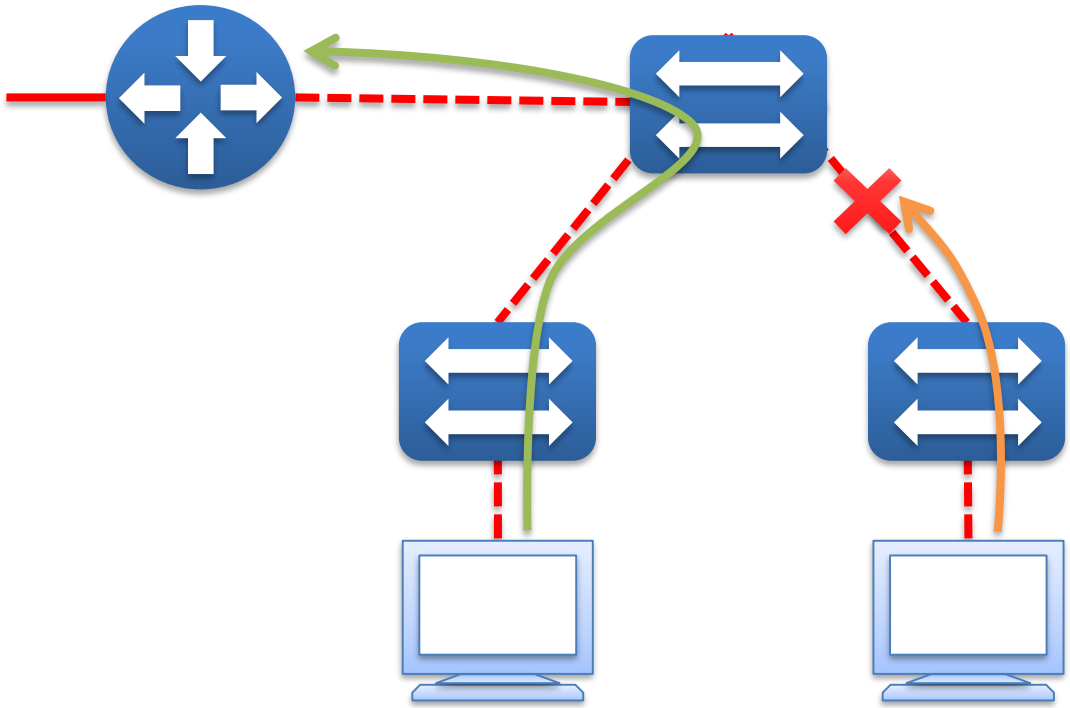


Redundancy

- 단일 경로만 존재하는 네트워크 구성은 평소에는 문제 없이 통신을 할 수 있다.
- 하지만 만일 케이블에 문제가 생겨서 더 이상 통신을 할 수 없게 되었을 경우 이 문제를 확인하고 다시 복구 하기 까지 많은 시간이 소요가 된다.

이중화

Single Pointer Of Failure

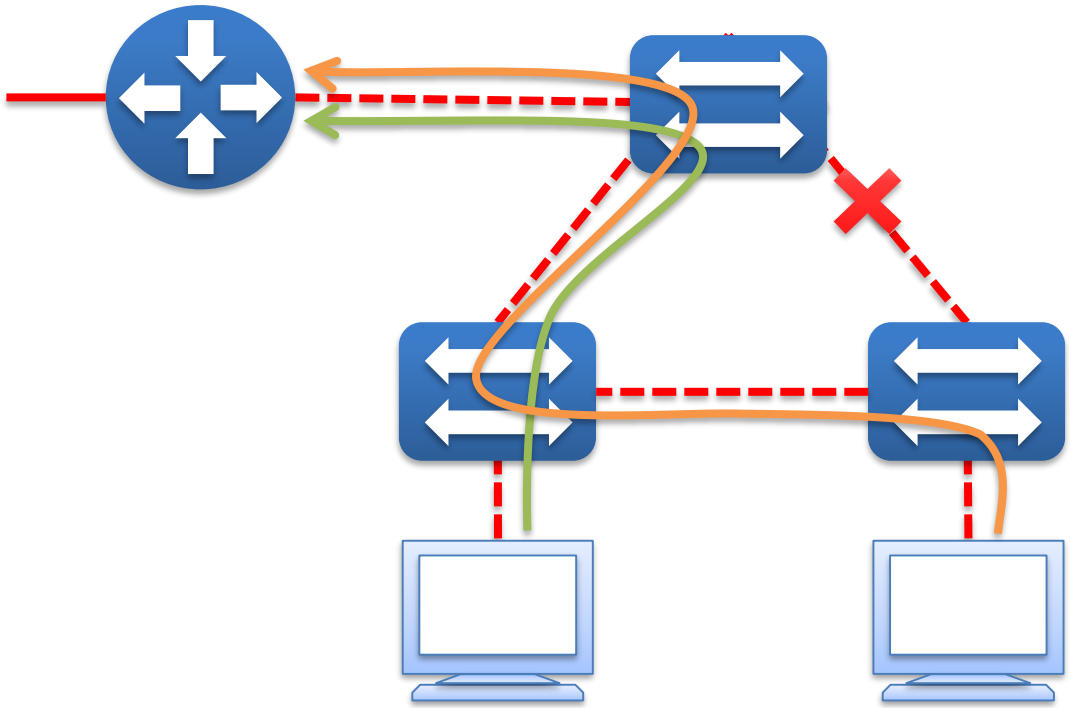


SPOF(Single Point Of Failure)

- 단일 경로에 문제가 발생하게 되면 대체 수단이 없어 통신이 안 되는 문제가 발생하게 된다.
- 어떤 하나의 문제로 인해 서비스가 중단되는 요소를 단일 장애점(SPOF) 이라 한다.
- SPOF를 해결 하기 위한 추가 작업과 이로 인한 서비스 지연의 시간이 길어 질 수록 서비스 품질이 떨어지는 결과를 가지게 된다.

단일 장애점

High Availability



HA(High Availability)

- 이러한 문제를 해결 하기 위해 대체 경로를 추가로 증설하여 지속적으로 통신을 할 수 있도록 하여 고가용성을 위한 구성을 하게 된다.
- 고가용성이란 끊김 없는 서비스를 구현 함으로써 서비스의 품질 또한 높아지게 하는 것이다.
- 고가용성을 위해서는 이중화 구성이 필수 조건이다.

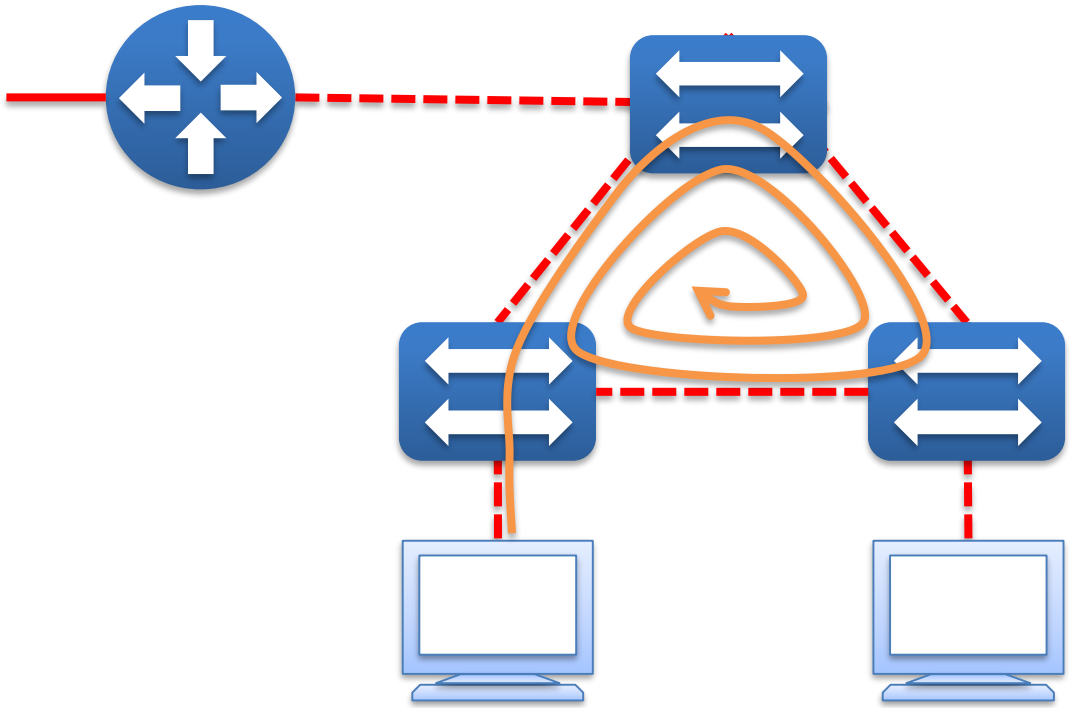
고가용성

Redundancy

이중화 특징

- 대체 경로의 수단을 제공 함으로 인해 지속적인 서비스를 유지 할 수 있게 된다.
- 경로 뿐만 아니라 장비 자체를 이중화 함으로 인해 혹시 모를 문제에 대비 할 수 있다.
- 이중화 구성을 하는 것은 고가용성(HA)을 높이기 위함이며, 이를 통해 99.999%의 서비스 가동률을 구성 할 수 있다.
- 이중화를 구성하기 때문에 비용 역시 많이 소모되게 된다.
- 이중화 구성을 통해 대체 경로를 확보하게 될 경우 L2의 특성상 Loop가 발생 되는 문제가 존재한다.

Loop Problem

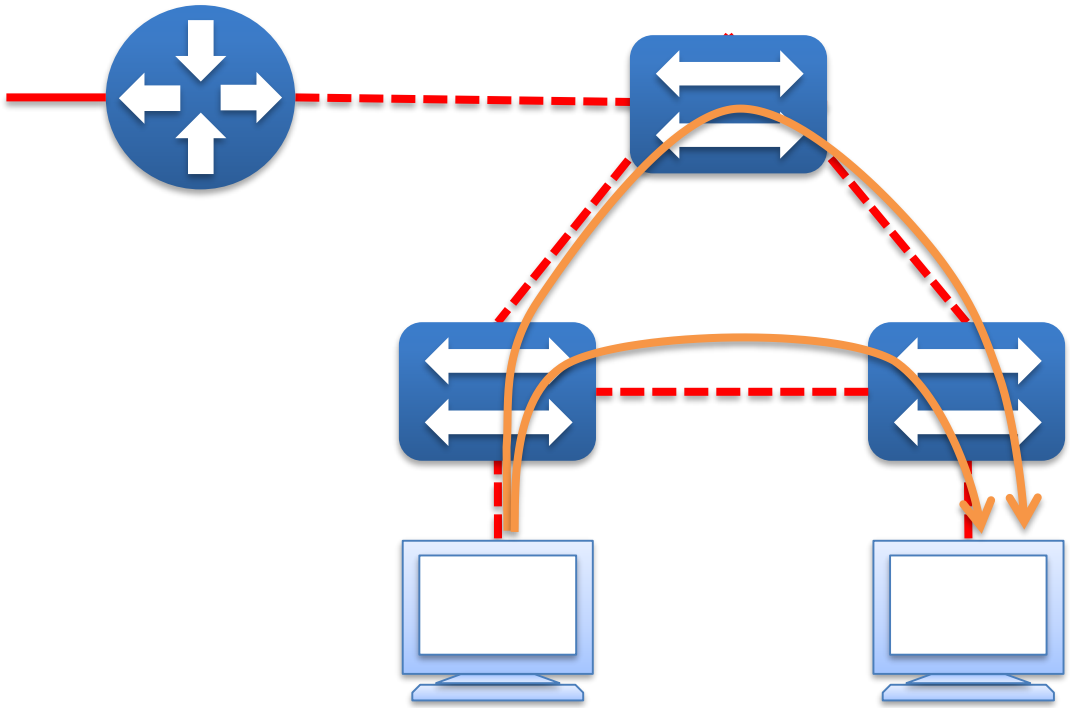


Broadcast Storm

- 단말 장치들은 ARP, DHCP Discover, NetBIOS 등과 같은 브로드캐스트 트래픽을 발생 시킨다.
- 브로드캐스트를 받은 스위치는 In-Bound Port를 제외한 모든 Port로 Flooding을 하게 되며, 결과적으로 스위치 사이에서 브로드캐스트 트래픽이 빙글빙글 돌게 된다.
- 이러한 현상이 누적 될 경우 가용 대역폭이 줄어 들어 실제 통신에서의 속도가 줄어들게 된다.

브로드캐스트 스톰

Loop Problem

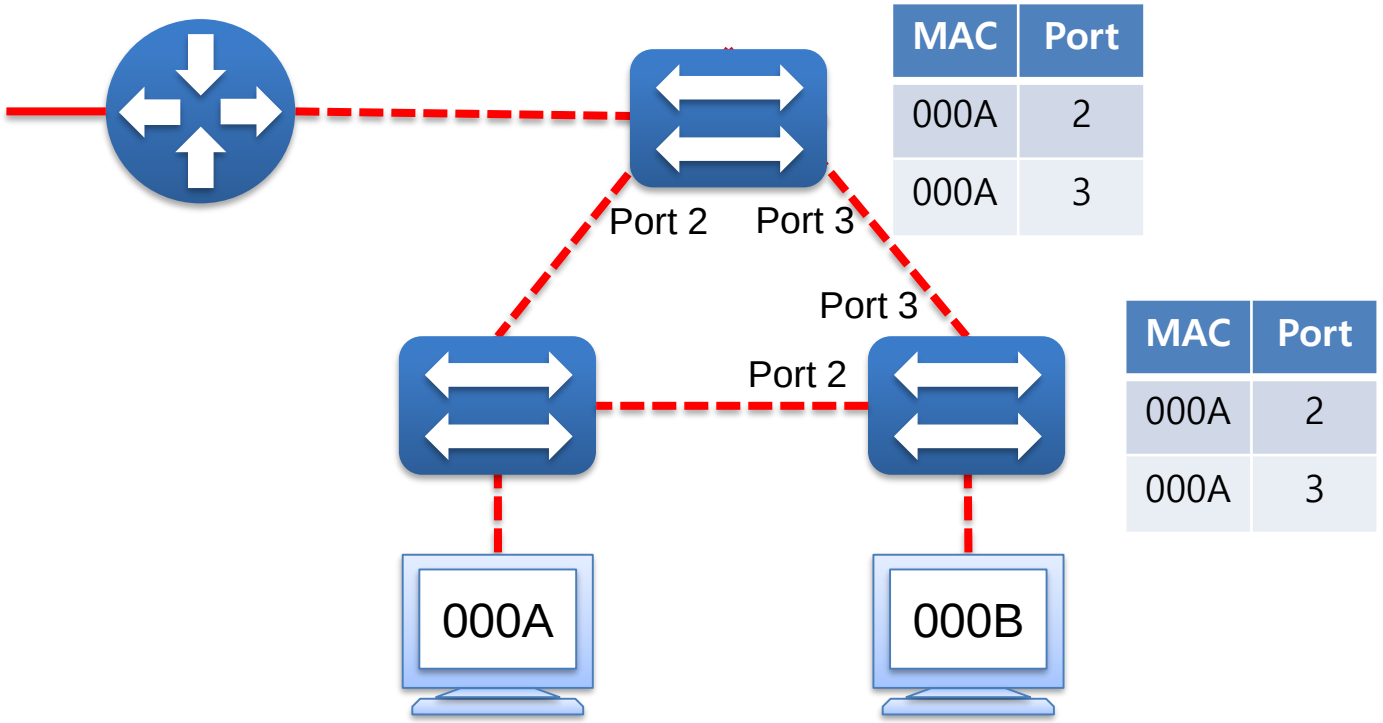


Multiple Frame Copy

- 단말 장치는 유니캐스트 통신을 시도하지만 스위치에서 목적지에 대한 MAC 주소를 모르고 있을 경우 Flooding을 통해 트래픽을 전달 하게 된다. (Unknown Unicast Frame)
- 하나의 프레임이 Flooding을 통해 복사가 이루어져 전달 되어 동일한 프레임을 2번 이상 받는 이상한 현상이 발생 된다.

프레임 다중 복사

Loop Problem



MAC	Port
000A	2
000A	3

MAC	Port
000A	2
000A	3

Mac Database Instability

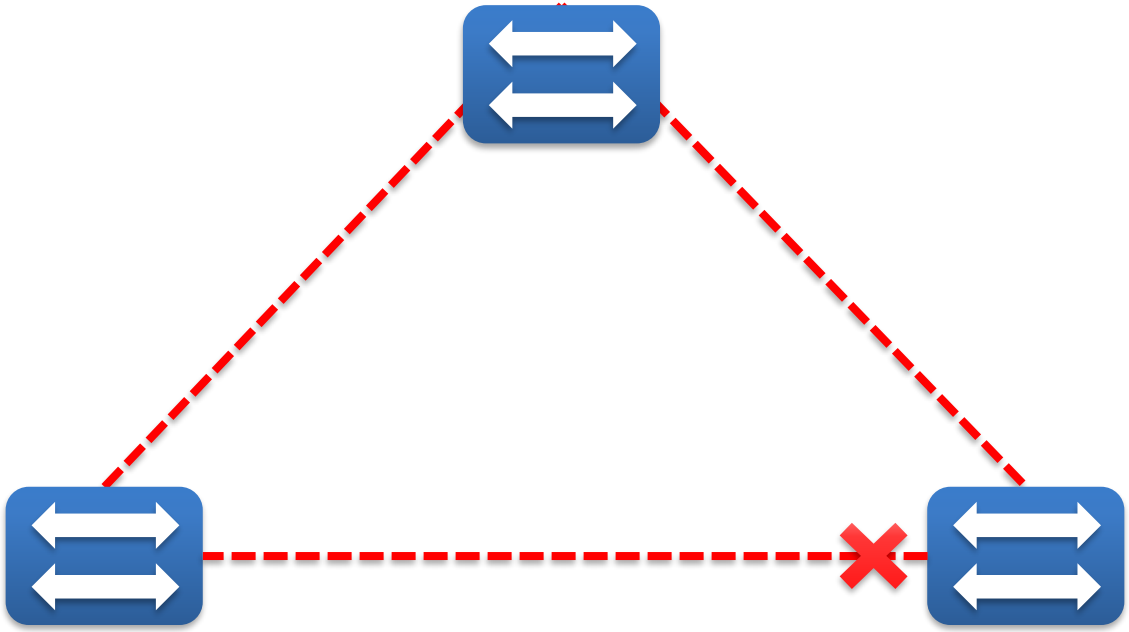
- 다중 프레임 복사와 같이 Unknown Unicast Frame이 전달 될 경우 발생 된다.
- In-Bound Port를 제외한 모든 Port로 프레임이 전달 되기 때문에 특정 목적지로 가기 위한 MAC Address Table의 학습이 부정확하게 이루어지게 된다.

MAC 데이터베이스 불안정

STP Process

Spanning Tree Protocol

STP Process

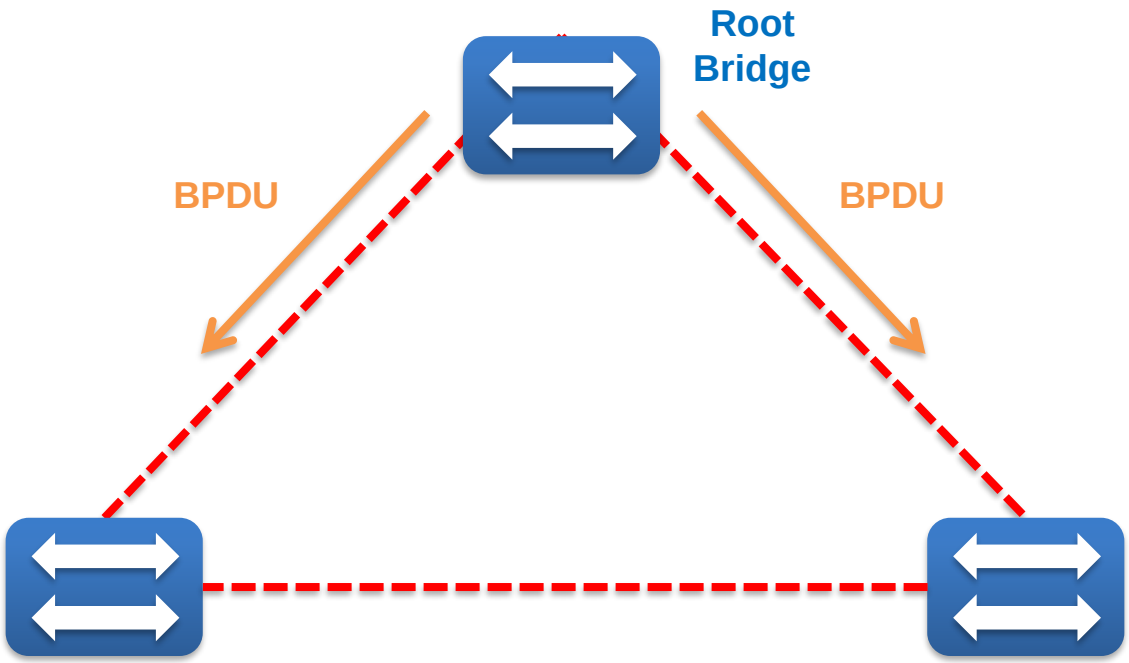


STP

- 물리적 Loop 환경을 인지하고 특정 Link에 대해 사용 하지 않도록 차단(Block)하여 Loop를 방지한다.
- 지속적으로 네트워크 환경을 모니터링 하면서 특정 포트의 장애나 토폴로지에 변화가 발생 시 재 설정을 통해 연결의 손실이나 새로운 Loop를 막는다.

Spanning Tree Protocol

STP Process

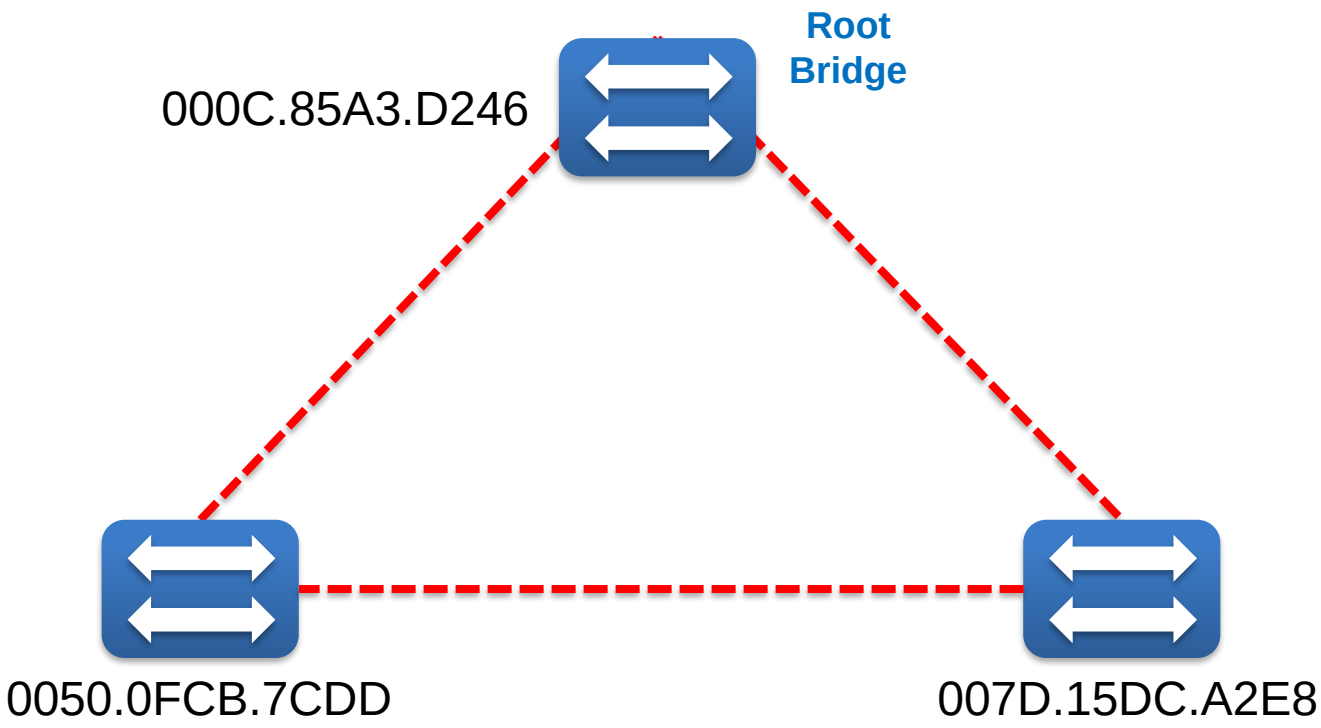


BPDU

- 현재 네트워크 환경이 Loop 환경이 구성 되어 있는지 또는 네트워크의 변화가 있는지 감시하기 위한 도구
- 지속적인 감시를 위해서 Root Bridge는 매 2초 간격으로 BPDU를 전송을 한다.
- 기본 적으로 모든 스위치는 BPDU를 생성하고 전달하지만 Root Bridge가 존재하게 될 경우 Root를 제외한 모든 스위치는 BPDU를 생성하지 못한다.

Bridge Protocol Data Unit

STP Process

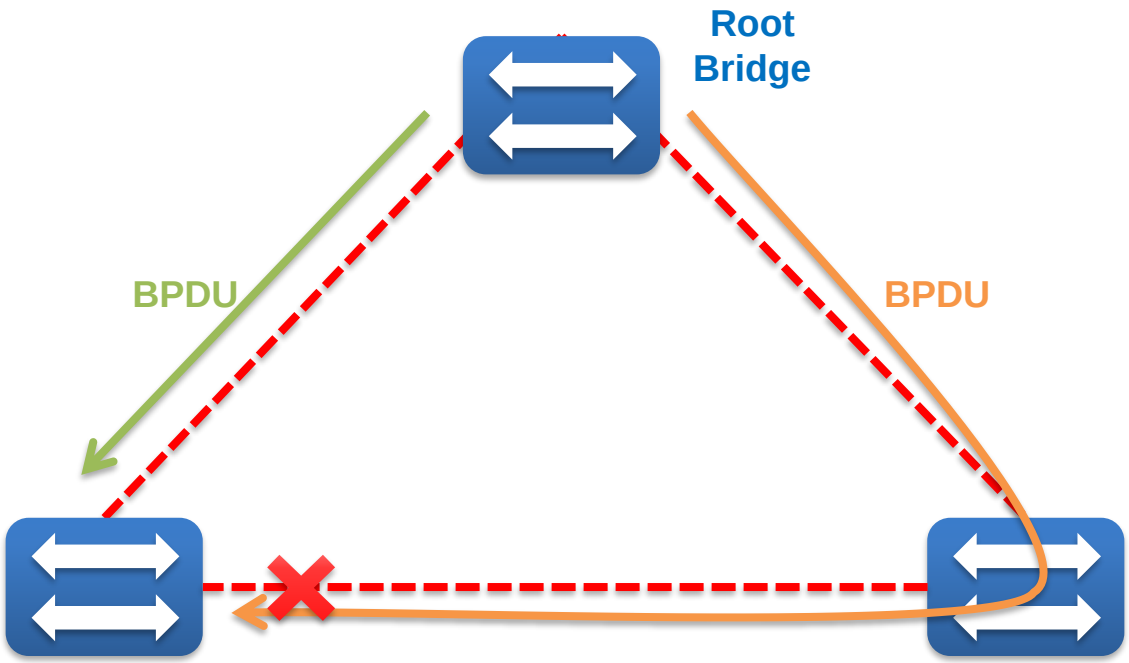


Root Bridge

- Loop를 감지하기 위해서는 기준이 될 스위치가 필요하며, 이 기준의 역할을 하는 스위치를 Root Bridge라고 한다.
- 여러 스위치들 중에서 하나의 Root Bridge를 선출하기 위해 모든 장비들이 공통적으로 가지고 있는 MAC 주소를 통해 Root Bridge(가장 낮은 MAC 주소)를 선출하게 된다.

루트 브릿지

STP Process

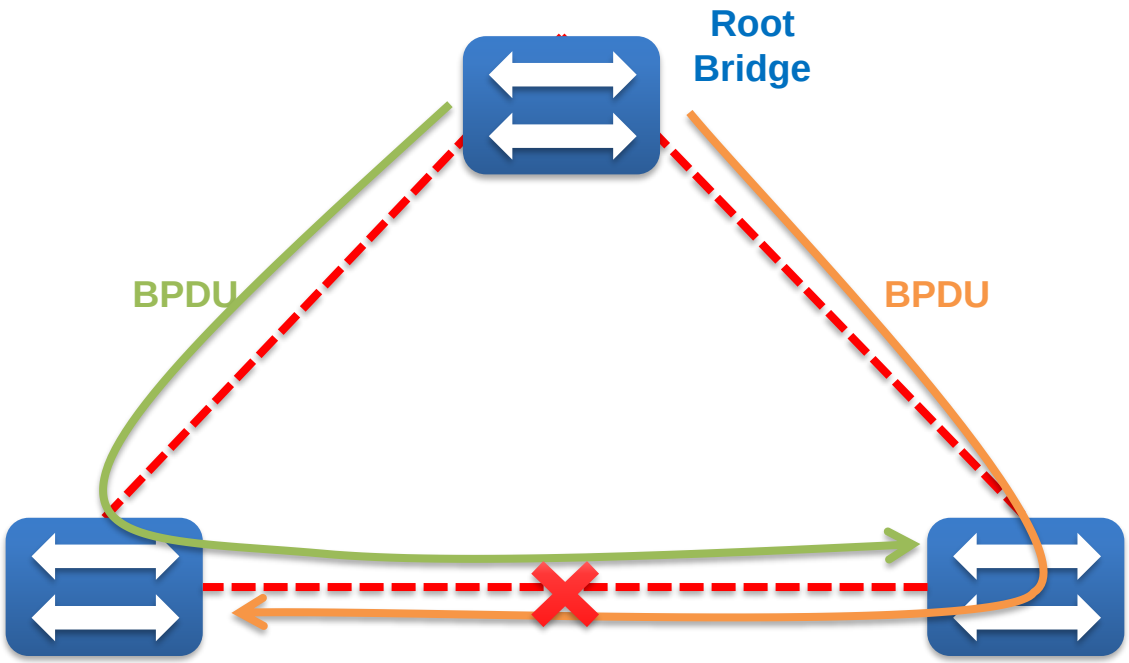


Loop Monitoring

- 스위치는 하나 이상의 Port를 통해 동일한 BPDU가 감지 될 경우 Loop가 발생 되었다고 감지를 하게 되어 하나의 Port를 제외한 나머지 Port를 차단(Block)하게 된다.

Loop 모니터링

STP Process

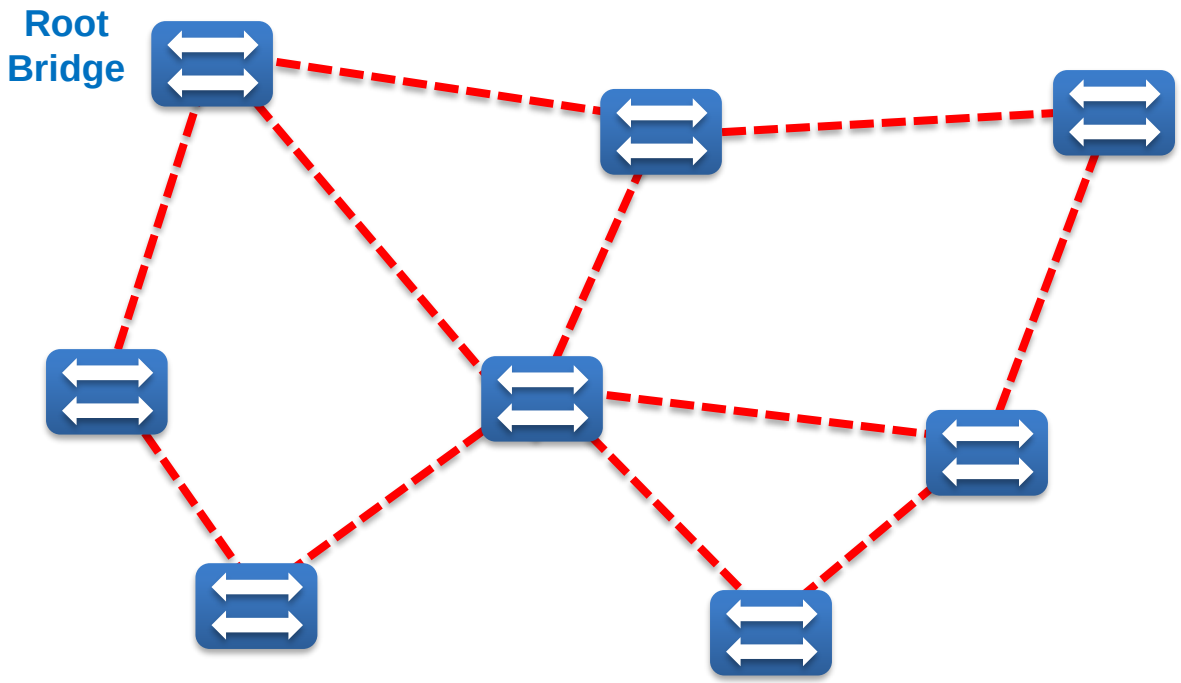


Loop Monitoring

- 스위치는 자신이 특정 Port를 통해서 BPDU를 전달했는데 동일한 Port로 동일한 BPDU가 감지 될 경우 해당 Port를 차단(Block)하게 된다.

Loop 모니터링

STP Process

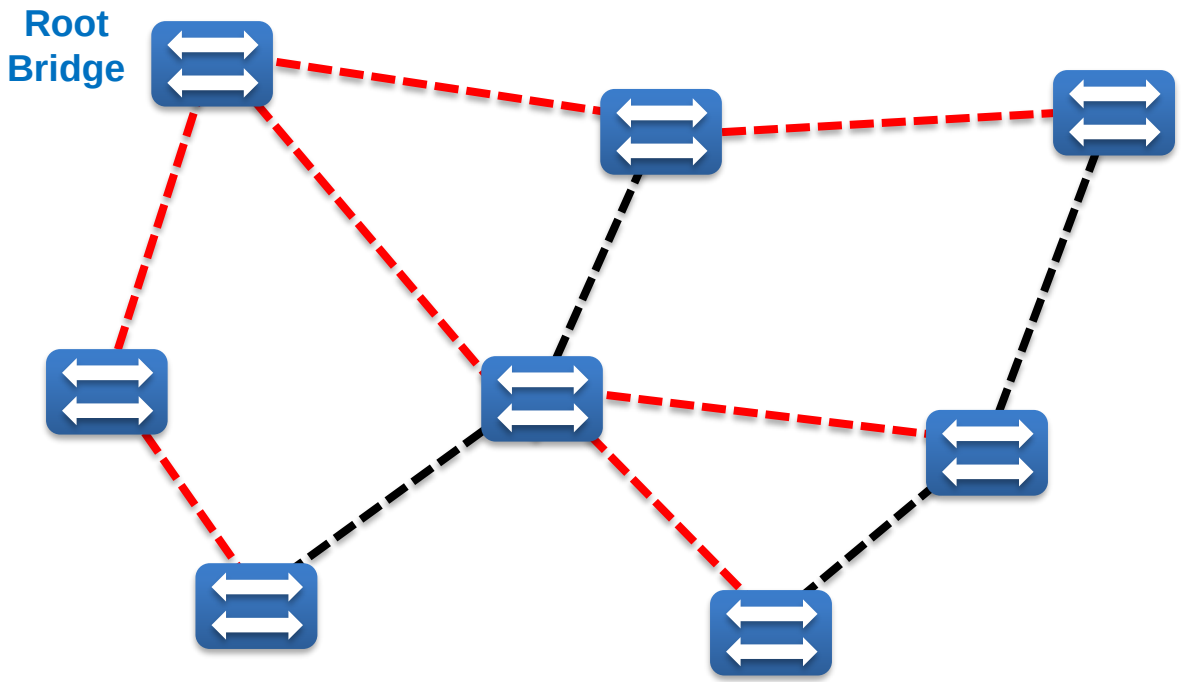


Summary

- Graph 구조 또는 Mesh 형 토폴로지에서는 하나의 장치에 문제가 발생이 되어도 대체 할 수 있는 수단이 존재한다.
- L2 네트워크의 특성상 이런 구조의 네트워크 환경에서는 Loop가 필연적으로 발생이 될 수 밖에 없다.

요약

STP Process



Summary

- Loop 가 발생 되는 구간을 BPDU를 통해 미리 감지를 하고 감지 된 Link를 사용 못 하도록 차단 (Block) 함으로 Loop가 발생 될 소지를 막아 버린다.
- 이렇게 구성을 하게 됨으로 인해서 Graph 구조 또는 Mesh 형 네트워크의 Loop 환경을 Loop가 없는 Tree 구조로 바꾸게 된다.

요약

STP Verification

Spanning Tree Protocol

STP Verification

STP 확인 (Root Bridge)

```
SW1# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID         Priority    32769
                Address     000C.85A3.D246
                This bridge is the root
                Hello Time 2 sec        Max Age 20 sec        Forward Delay 15 sec

Bridge ID       Priority    32769       (priority 32768 sys-id-ext 1)
                Address     000C.85A3.D246
                Hello Time 2 sec        Max Age 20 sec        Forward Delay 15 sec
                Aging Time 20

Interface       Role        Sts         Cost        Prio.Nbr    Type
----------------  -------     -----       ---------   ----------  --------------------------------
Fa0/1           Desg        FWD         19          128.1       P2p
Fa0/2           Desg        FWD         19          128.2       P2p
```

STP Verification

STP 확인 (non-Root Bridge)

```
SW2# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID     Priority    32769
            Address     000C.85A3.D246
            Cost        19
            Port        1(FastEthernet0/1)
            Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

Bridge ID   Priority    32769   (priority 32768 sys-id-ext 1)
            Address     0050.0FCB.7CDD
            Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec
            Aging Time 20

Interface        Role    Sts    Cost      Prio.Nbr    Type
---------------- ------- -----  --------- ----------- --------------------------------
Fa0/1            Root    FWD    19        128.1       P2p
Fa0/2            Altn    BLK    19        128.2       P2p
```