제27장 STP를 이용한 네트워크 보호 기술

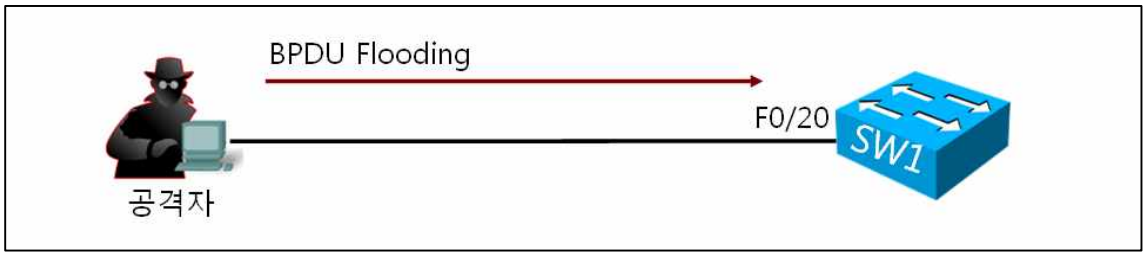
STP를 이용한 네트워크 보호 기술

STP의 기본 목적은 이중화 링크를 구현한 환경에서 발생하는 브리징 루프를 방지하는 것이다. 또한 PVST와 MST를 이용하면 VLAN 로드 분산이 가능하기 때문에 스위치 링크 사용을 효율적으로 운영할 수 있다. 대신, 링크 장애 발생시 일시적으로 발생하는 브리징 루프와 공격자에 의해서 생성된 BPDU를 수신하여 발생하는 스위치 부하 현상 등 보안적인 문제가 취약하다. 그래서 이번 장에서는 STP 네트워크 보호 기술을 이용하여 이러한 문제점들을 해결하는 방법에 대해서 알아보도록 하자.

BPDU Guard

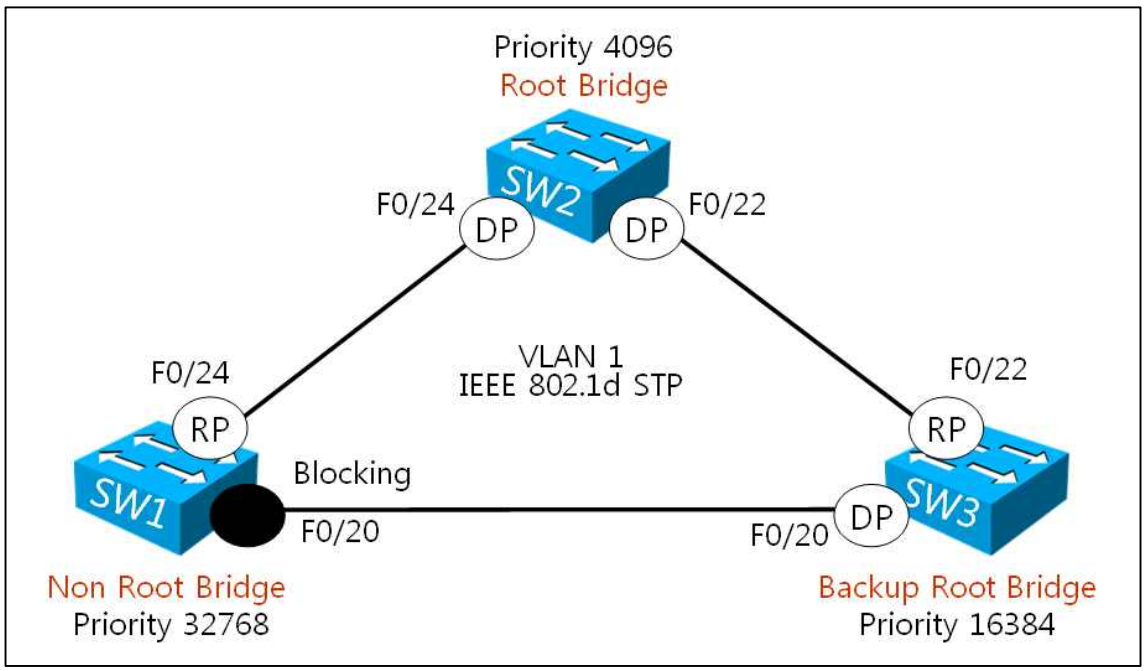
BPDU 가드는 스위치 포트로 BPDU를 수신하면 포트 상태를 Err-Disable로 전환하여, 스위치 포트를 비활성화를 시키는 기능을 수행한다. BPDU 가드는 다음과 같이 공격자에 의해서 생성된 BPDU를 수신하여 스위치 부하 현상을 방지하기 위해서 사용되거나, 또는 인가 받지 않은 스위치가 로컬 스위치에 연결되는 것을 방지하기 위해서 사용된다.

[그림 27-1] BPDU 가드 사용 예제



그럼 [그림 27-2]를 참조하여 SW1 F0/20 포트에 BPDU 가드를 설정하여 동작 과정을 알아보도록 하자.

[그림 27-2] 스위치 네트워크 토폴로지



[예제 27-1] SW1 F0/20 포트에 BPDU 가드 설정

```
SW1(config)#int fa0/20
SW1(config-if)#spanning-tree bpduguard enable
```

SW1 F0/20 포트에 BPDU 가드를 설정하면, 바로 BPDU 가드에 의해서 포트가 Err-Disable 상태로 전환되는 것을 알 수 있다.

[예제 27-2] SW1 F0/20 포트에 설정된 BPDU 가드 동작 확인

```
SW1(config-if)#
18:37:54: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/20 with BPDU Guard enabled. Disabling port.
18:37:54: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/20, putting Fa0/20 in err-disable state
SW1(config-if)#
18:37:55: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to down
SW1(config-if)#
18:37:56: %LINK-3-UPDOWN: Interface FastEthernet0/20, changed state to down
SW1#
18:38:00: %SYS-5-CONFIG_I: Configured from console by console
SW1#
SW1#show int fa0/20
FastEthernet0/20 is down, line protocol is down (err-disabled)
   Hardware is Fast Ethernet, address is 0019.e791.c296 (bia 0019.e791.c296)
~ 중간 생략 ~
SW1#
SW1#show interfaces status err-disabled

Port      Name               Status       Reason
Fa0/20                       err-disabled bpduguard
```

이렇게 Err-Disable 상태가 된 스위치 포트를 다시 동작하기 위해서는 [예제 27-3]과 같이 SW1 F0/20 포트를 'shutdown'한 다음, 'no shutdown'을 실시해야 한다.

[예제 27-3] SW1 F0/20 포트 복구 방법

```
SW1(config)#int fa0/20
SW1(config-if)#shutdown
SW1(config-if)#no shutdown
```

지금 같은 경우, SW1 F0/20 포트에 BPDU 가드 설정이 있기 때문에, 포트가 다시 Err-Disable 상태가 된다.

만약, Err-Disable 상태인 포트를 자동으로 복구하려면, [예제 27-4]와 같이 'errdisable recovery' 기능을 사용하면 된다.

[예제 27-4] 'errdisable recovery' 기능을 이용한 자동 복구 방법

```
SW1(config)#errdisable recovery cause bpduguard
SW1(config)#errdisable recovery interval 30
SW1(config)#int fa0/20
SW1(config-if)#no spanning-tree bpduguard enable
```

설정이 완료되었다면, SW1에서 다음과 같은 'errdisable recovery' 정보 확인과 SW1 F0/20 포트가 자동으로 복구되는지 확인하도록 하자.

[예제 27-5] SW1에서 확인한 'errdisable recovery' 정보 확인

```
SW1#show errdisable recovery
ErrDisable Reason      Timer Status
-----------------      --------------
udld                   Disabled
bpduguard              Enabled
security-violatio      Disabled
~ 중간 생략 ~
Timer interval: 30 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
----------     -------------------    --------------
Fa0/20         bpduguard                  18
SW1#
01:21:36: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard err-disable state
on Fa0/20
SW1#
01:21:40: %LINK-3-UPDOWN: Interface FastEthernet0/20, changed state to up
SW1#
01:21:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed
state to up
```

만약, 포트 패스트가 설정된 모든 포트에 BPDU 가드를 동작하려면, 다음과 같다.

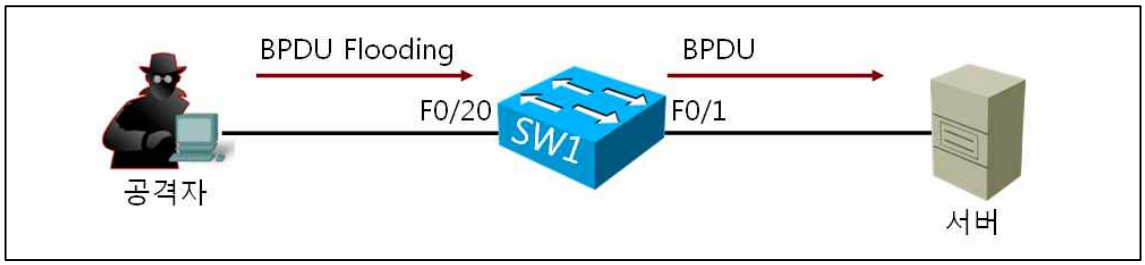
[예제 27-6] 포트 패스트에 대한 BPDU 가드 설정

```
SW1(config)#spanning-tree portfast bpduguard default
```

BPDU Filter

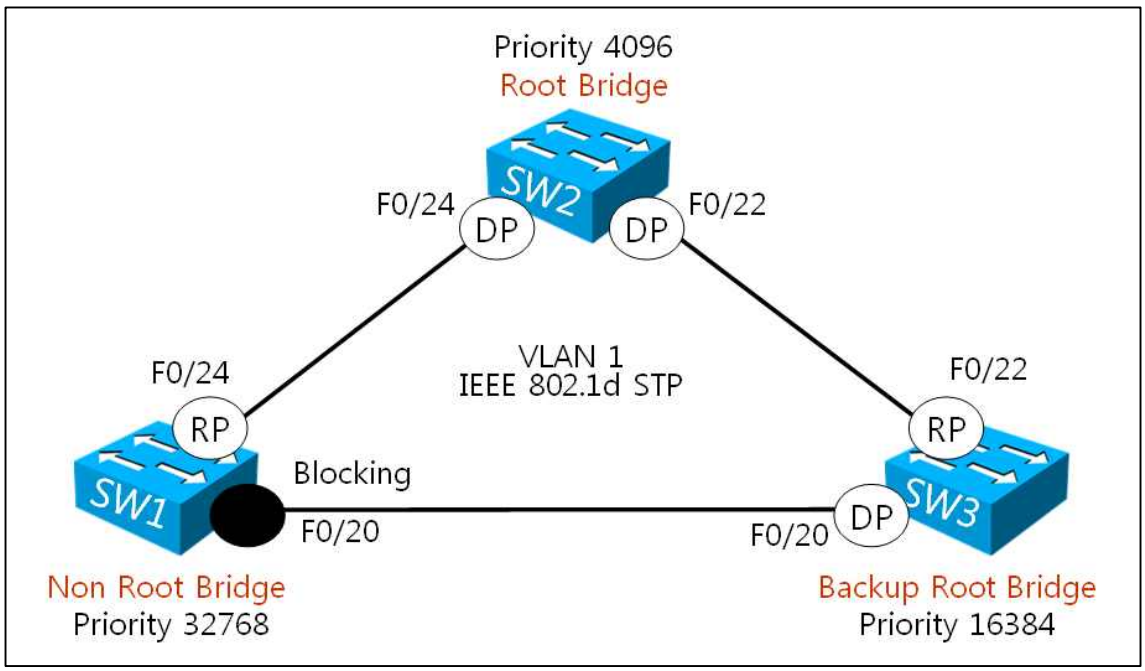
BPDP 필터는 스위치 포트로 BPDU가 송수신되는 것을 차단하는 기능을 수행한다. BPDU 필터는 다음과 같이 공격자에 의해서 생성된 BPDU를 수신하여 스위치 부하 현상을 방지하기 위해서 사용되거나, 또는 스위치 포트에 연결된 서버에게 불필요한 BPDU를 전송하지 않음으로써 부하 현상을 방지하기 위해서 사용된다.

[그림 27-3] BPDU 필터 사용 예제



그럼 [그림 27-4]를 참조하여 SW3 F0/20 포트에 BPDU 필터를 설정하여 동작 과정을 알아보도록 하자.

[그림 27-4] 스위치 네트워크 토폴로지



SW3 F0/20 포트에 BPDU 필터를 설정하면, SW1 F0/20 포트는 BPDU를 수신하지 못하기 때문에 Listening → Learning → Forwarding 순으로 이전하여 지정 포트로 동작한다. 이렇게 되면 차단 상태가 되어야할 SW1 F0/20 포트가 Forwarding 상태인 지정 포트가 되고, SW3 F0/20 포트도 Forwarding 상태인 지정 포트이기 때문에 브리징 루프가 발생한다. 그렇기 때문에 실제 환경에서는 지금과 같이 차단 상태인 SW1 F0/20 포트에 BPDU 필터를 설정하면 안된다.

[예제 27-7] SW1에서 STP 디버깅 실시

```
SW1#debug spanning-tree events
Spanning Tree event debugging is on
```

[예제 27-8] SW3 F0/20 포트에 BPDU 필터 설정

```
SW3(config)#int fa0/20
SW3(config-if)#spanning-tree bpdufilter enable
```

SW3 F0/20 포트에 BPDU 필터를 설정하면, SW1 F0/20 포트는 BPDU를 수신하지 못하기 때문에 다음과 같이 Listening → Learning → Forwarding 순으로 이전하여 지정 포트로 동작한다.

[예제 27-9] SW1에서 확인한 STP 디버깅 내용과 SW1 F0/20 포트 상태

```
SW1#
03:16:37: STP: VLAN0001 Fa0/20 -> listening
SW1#
03:16:52: STP: VLAN0001 Fa0/20 -> learning
SW1#
03:17:07: STP: VLAN0001 sent Topology Change Notice on Fa0/24
03:17:07: STP: VLAN0001 Fa0/20 -> forwarding
SW1#
SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
~ 중간 생략 ~

Interface        Role   Sts   Cost      Prio.Nbr Type
---------------- ------ ----- --------- --------- --------------------------------
Fa0/20           Desg FWD 19        128.22    P2p
Fa0/24           Root FWD 19        128.26    P2p
```

다음 내용을 알아보기 위해서 SW3 F0/20 포트에 설정한 BPDU 필터를 삭제하도록 하자.

[예제 27-10] SW3 F0/20 포트에 설정한 BPDU 필터 삭제

```
SW3(config)#int fa0/20
SW3(config-if)#no spanning-tree bpdufilter enable
```

SW3 F0/20 포트에서 BPDU 필터를 삭제하면, SW1 F0/20 포트는 다시 차단 상태로 전환된다.

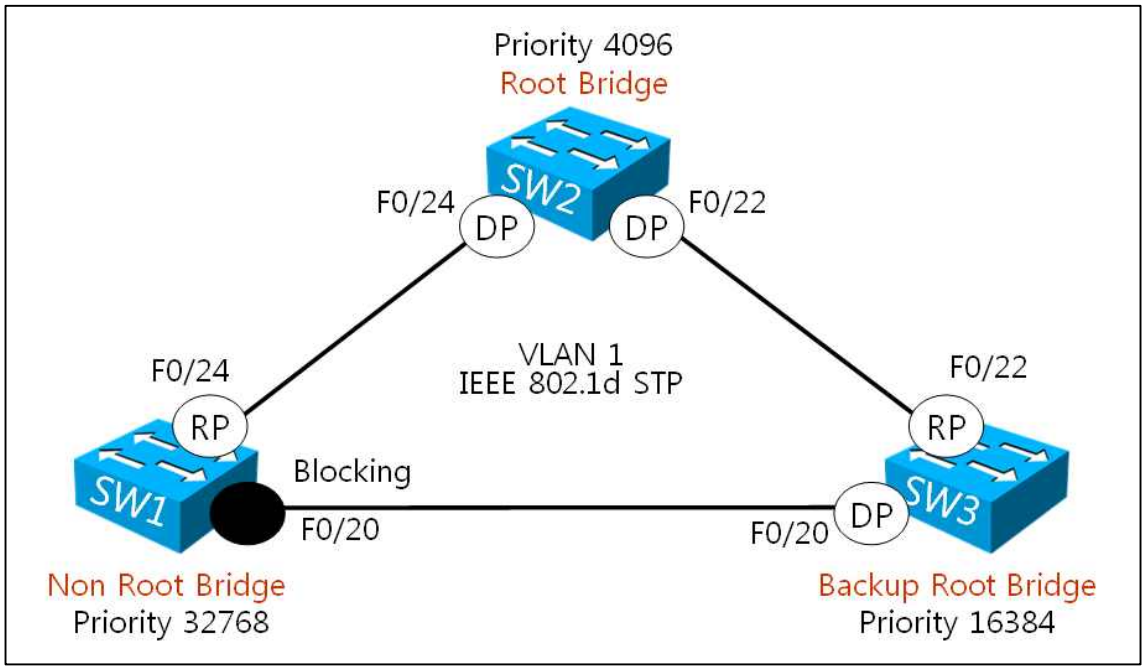
[예제 27-11] SW1에서 확인한 STP 디버깅 내용

```
SW1#
03:24:27: STP: VLAN0001 sent Topology Change Notice on Fa0/24
03:24:27: STP: VLAN0001 Fa0/20 -> blocking
```

Loop Guard

루프 가드는 방금전처럼 SW1 F0/20 포트가 BPDU를 수신하지 못하여 해당 포트가 Forwarding으로 이전하는 것을 방지하는 기능을 수행한다. 그럼 [그림 27-5]를 참조하여 SW1 F0/20 포트에 루프 가드를 설정하고, SW3 F0/20 포트에 BPDU 필터를 설정하여 루프 가드 동작을 알아보도록 하자.

[그림 27-5] 스위치 네트워크 토폴로지



SW3 F0/20 포트에 BPDU 필터를 설정하면, SW1 F0/20 포트는 BPDU를 수신하지 못하기 때문에 Listening → Learning → Forwarding 순으로 이전하여 지정 포트로 동작한다. 이렇게 되면 차단 상태가 되어야할 SW1 F0/20 포트가 Forwarding 상태인 지정 포트가 되고, SW3 F0/20 포트도 Forwarding 상태인 지정 포트이기 때문에 브리징 루프가 발생한다. 이때, SW1 F0/20 포트에 루프 가드가 설정되어 있다면, Forwarding으로 이전하는 것을 중지한다.

[예제 27-12] SW1 F0/20 포트에 루프 가드 설정

```
SW1(config)#int fa0/20
SW1(config-if)#spanning-tree guard loop
```

SW1 F0/20 포트에 루프 가드 설정이 완료되었다면, SW3 F0/20 포트에 BPDU 필터를 설정하도록 하자.

[예제 27-13] SW3 F0/20 포트에 BPDU 필터 설정

```
SW3(config)#int fa0/20
SW3(config-if)#spanning-tree bpdufilter enable
```

SW3 F0/20 포트에 BPDU 필터 설정이 완료되었다면, SW1에서 루프 가드 정보 확인을 실시하도록 하자.

[예제 27-14] SW1에서 확인한 루프 가드 처리 과정

```
SW1#
03:37:32: %SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/20
on VLAN0001.
SW1#
SW1#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
~ 중간 생략 ~

Interface        Role  Sts  Cost      Prio.Nbr Type
---------------- ------ ----- --------- --------- --------------------------------
Fa0/20           Desg BKN*19       128.22    P2p *LOOP_Inc
Fa0/24           Root FWD 19       128.26    P2p
```

정보 확인 결과, SW1 F0/20 포트는 지정 포트로 동작하지만, 루프 가드에 의해서 Forwarding으로 이전하는 것을 중지하여 해당 포트를 차단 상태(BKN)로 유지하고 있는 것을 알 수 있다.

다음 내용을 알아보기 위해서 SW3 F0/20 포트에 설정한 BPDU 필터와 SW1 F0/20 포트에 설정한 루프 가드를 삭제하도록 하자.

[예제 27-15] SW3 F0/20 포트에 설정한 BPDU 필터 삭제

```
SW3(config)#int fa0/20
SW3(config-if)#no spanning-tree bpdufilter enable
```

[예제 27-16] SW1 F0/20 포트에 설정한 루프 가드 삭제

```
SW1(config)#int fa0/20
SW1(config-if)#no spanning-tree guard loop
```

만약, 스위치 모든 포트에 루프 가드를 적용하려면, 다음과 같이 전체 설정 모드에서 루프 가드를 설정한다.

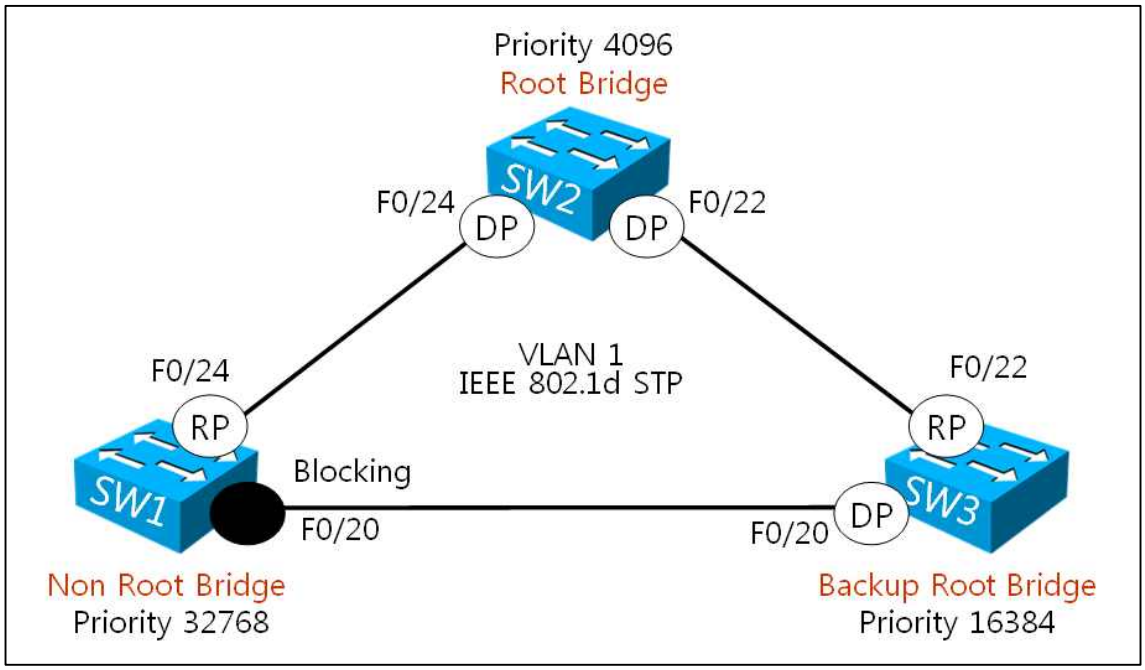
[예제 27-17] 스위치 모든 포트에 루프 가드 설정

```
SW1(config)#spanning-tree loopguard default
```

Root Guard

루트 가드는 루트 브리지로 선출된 스위치가 다른 스위치로부터 선순위 BPDU를 수신하여 루트 브리지 권한이 다른 스위치에게 인계되는 것을 방지하는 기능을 수행한다. 그렇기 때문에 루트 가드를 이용하면 ISP 업체 입장에서 원하지 않는 다른 스위치가 루트 브리지가 되어 스위치 네트워크 환경에 영향을 주는 것을 방지할 수 있다. 그럼 [그림 27-6]을 참조하여 SW2 F0/22와 F0/24 포트에 루트 가드를 설정하고, SW3에서 우선 순위를 '0'으로 설정하여 루트 가드 동작을 알아보도록 하자.

[그림 27-6] 스위치 네트워크 토폴로지



SW2 F0/22와 F0/24 포트에서 루트 가드를 설정하고, SW3에서 우선 순위를 '0'으로 설정하면, SW2 F0/22와 F0/24 포트로 선순위 BPDU를 수신하게 된다. 이때, SW2는 루트 가드에 의해서 선순위 BPDU를 수신한 F0/22와 F0/24 포트를 차단 상태로 전환하여, SW1과 SW3과의 프레임 전송 처리를 실시하지 않는다.

[예제 27-18] SW2 F0/22와 F0/24 포트에 루트 가드 설정

```
SW2(config)#int range fa0/22 , fa0/24
SW2(config-if-range)#spanning-tree guard root
```

SW2 F0/22와 F0/24 포트에 루트 가드 설정이 완료되었다면, SW3에서 우선 순위를 '0'으로 설정하도록 하자.

[예제 27-19] SW3에서 우선 순위 '0' 설정

```
SW3(config)#spanning-tree vlan 1 priority 0
```

SW3에서 우선 선위 '0' 설정이 완료되었다면, SW2에서 루트 가드 정보 확인을 실시하도록 하자.

[예제 27-20] SW2에서 확인한 루트 가드 처리 과정

```
SW2#
04:06:21: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port FastEthernet0/24
on VLAN0001.
SW2#
SW2#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
~ 중간 생략 ~

Interface        Role  Sts  Cost      Prio.Nbr Type
---------------- ------ ----- --------- --------- --------------------------------
Fa0/22           Desg BKN*19       128.24    P2p *ROOT_Inc
Fa0/24           Desg BKN*19       128.26    P2p *ROOT_Inc
```

정보 확인 결과, 선순위 BPDU를 수신한 SW2 F0/22와 F0/24 포트는 루트 가드에 의해서 차단 상태로 전환된 것을 알 수 있다.

UDLD(Unidirectional Link Detection)

UDLD는 스위치간에 단방향 링크가 발생할 경우, 해당 스위치 포트를 'err-disable'하여 강제로 셧다운하는 기능을 수행한다. 이때, 단방향 링크란 크로스오버 케이블 구성상 한쪽 내선이 단선 및 결선 오류가 되면 발생하는데, 이런 경우 브리징 루프가 발생하며 송신측에서 송신한 프레임이 중간에 사라지는 블랙홀 현상이 발생한다. 이러한 문제는 UDLD 기능을 이용하여 해결할 수 있으며, UDLD 설정 명령어는 다음과 같다.

[예제 27-21] 모든 스위치 포트에 UDLD 설정(상대방 스위치도 설정해야 한다.)

```
SW2(config)#udld ?
  aggressive      Enable UDLD protocol in aggressive mode on fiber ports except
                  where locally configured
  enable          Enable UDLD protocol on fiber ports except where locally configured
  message         Set UDLD message parameters
```

[예제 27-22] 특정 스위치 포트에 UDLD 설정(상대방 스위치 포트에도 설정해야 한다.)

```
SW2(config)#int fa0/22
SW2(config-if)#udld port ?
  aggressive    Enable UDLD protocol in aggressive mode on this interface
```

UDLD는 Normal 모드와 Aggressive 모드가 있는데, Normal 모드는 광케이블의 결선 오류로 인한 단방향 링크를 감지하며, Aggressive 모드는 광케이블뿐만 이나라, UTP 케이블의 단방향 링크도 감지한다.