

스패닝 트리 PortFast BPDU 가드 개선 사항 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[배경 정보](#)

[기능 설명](#)

[그림 1](#)

[그림 2](#)

[설정](#)

[CatOS 명령](#)

[Cisco IOS® Software 명령](#)

[CatOS 명령](#)

[Cisco IOS Software 명령](#)

[모니터링](#)

[명령 출력](#)

[CatOS 명령](#)

[Cisco IOS Software 명령](#)

[관련 정보](#)

소개

이 문서에서는 STP(스패닝 트리 프로토콜)의 BPDU(PortFast Bridge Protocol Data Unit) 가드 개선 기능에 대해 설명합니다.

사전 요구 사항

요구 사항


이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이러한 소프트웨어 버전에는 STP PortFast BPDU 가드가 도입되었습니다.

- Catalyst 4500/4000(Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G 및 2980G 플랫폼용 Catalyst OS(CatOS) 소프트웨어 버전 5.4.1
- Catalyst 6500/6000 플랫폼용 Cisco IOS® 소프트웨어 릴리스 12.0(7)XE
- Catalyst 4500/4000 Supervisor Engine III용 Cisco IOS 소프트웨어 릴리스 12.1(8a)EW

- Catalyst 4500/4000 Supervisor Engine IV용 Cisco IOS 소프트웨어 릴리스 12.1(12c)EW
- Catalyst 2900XL 및 3500XL 시리즈용 Cisco IOS 소프트웨어 릴리스 12.0(5)WC5
- Catalyst 3750 Series 스위치용 Cisco IOS Software 릴리스 12.1(11)AX
- Catalyst 3750 Metro 스위치용 Cisco IOS 소프트웨어 릴리스 12.1(14)AX
- Catalyst 3560 Series 스위치용 Cisco IOS 소프트웨어 릴리스 12.1(19)EA1
- Catalyst 3550 Series 스위치용 Cisco IOS 소프트웨어 릴리스 12.1(4)EA1
- Catalyst 2970 Series 스위치용 Cisco IOS Software 릴리스 12.1(11)AX
- Catalyst 2955 Series 스위치용 Cisco IOS 소프트웨어 릴리스 12.1(12c)EA1
- Catalyst 2950 Series 스위치용 Cisco IOS 소프트웨어 릴리스 12.1(6)EA2
- Catalyst 2950 LRE(Long-Reach Ethernet) 스위치용 Cisco IOS Software 릴리스 12.1(11)EA1
- Catalyst 2940 Series 스위치용 Cisco IOS Software 릴리스 12.1(13)AY

 참고: STP PortFast BPDU Guard는 Catalyst 8500 Series, 2948G-L3 또는 4908G-L3 스위치에서 사용할 수 없습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

배경 정보

이 문서에서는 PortFast BPDU(Bridge Protocol Data Unit) 보호 기능을 설명합니다. 이 기능은 Cisco에서 생성한 STP(Spanning Tree Protocol) 개선 사항 중 하나입니다. 이 기능은 스위치 네트워크의 안정성, 관리 효율성 및 보안을 향상시킵니다.

기능 설명

STP는 메시 토폴로지를 루프 없는 트리와 같은 토폴로지로 구성합니다. 브리지 포트의 링크가 작동하면 해당 포트에서 STP 계산이 수행됩니다. 계산의 결과는 포트가 전달 또는 차단 상태로 전환되는 것입니다. 결과는 네트워크의 포트 위치 및 STP 매개변수에 따라 달라집니다. 이 계산 및 전환 기간은 일반적으로 약 30 내지 50초가 걸린다. 이 때 사용자 데이터는 포트를 통해 전달되지 않습니다. 일부 사용자 애플리케이션은 해당 기간 동안 시간 초과될 수 있습니다.

포트를 전달 상태로 즉시 전환할 수 있도록 하려면 STP PortFast 기능을 활성화합니다. PortFast는

링크할 때 포트를 STP 전달 모드로 즉시 전환합니다. 포트가 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트는 결국 STP 차단 모드로 전환됩니다.

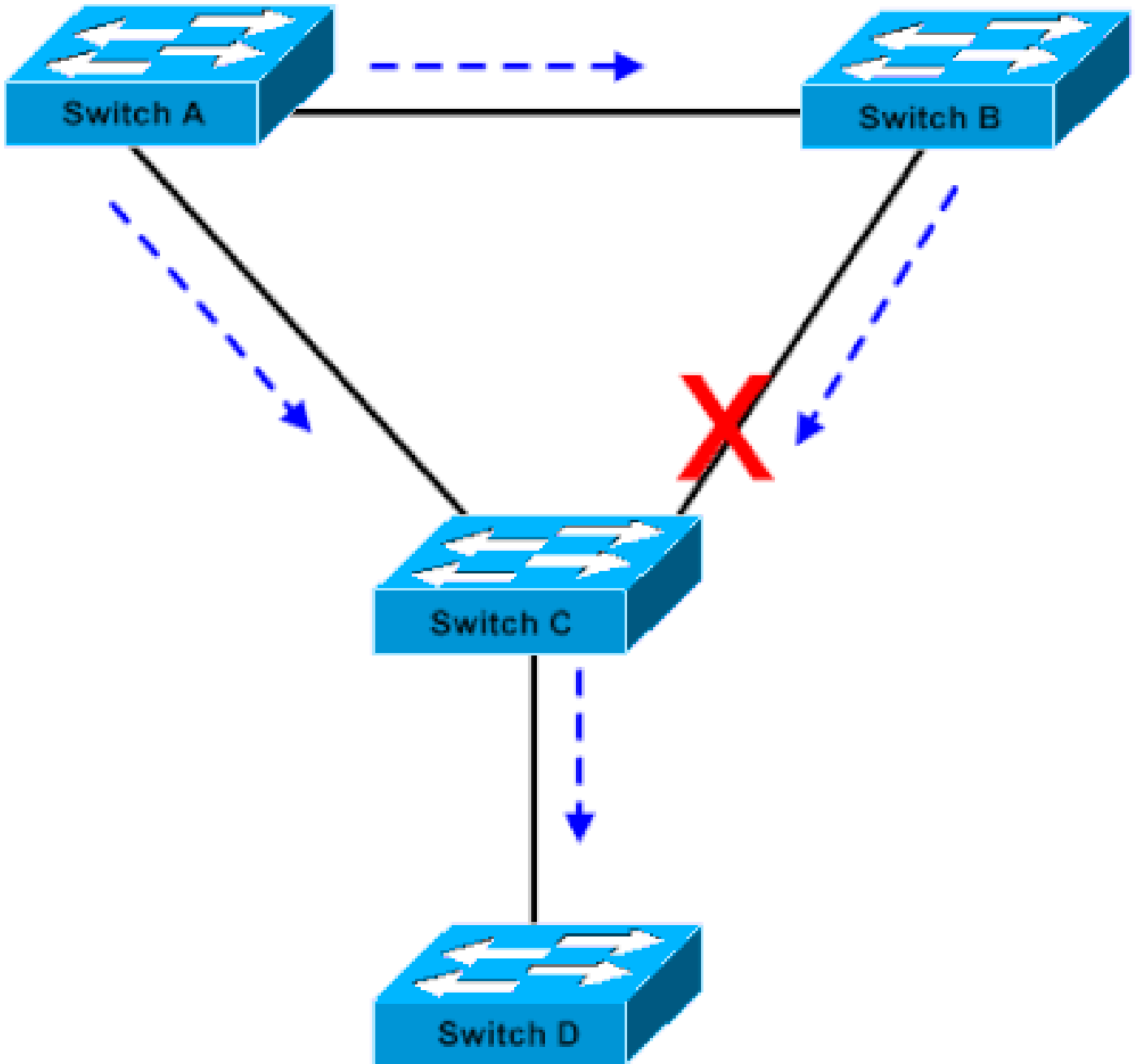
포트가 STP에 참여하는 한, 일부 디바이스는 루트 브리지 기능을 가정하고 활성 STP 토폴로지에 영향을 줄 수 있습니다. 루트 브리지 기능을 가정하기 위해 디바이스가 포트에 연결되고 현재 루트 브리지보다 낮은 브리지 우선순위로 STP를 실행합니다. 다른 디바이스가 이러한 방식으로 루트 브리지 기능을 가정하는 경우 네트워크가 최적화되지 않습니다. 이는 네트워크에 대한 간단한 DoS(denial of service) 공격입니다. 브리지 우선순위가 낮은 STP 장치를 임시로 도입하고 나중에 제거하면 영구적인 STP 재계산이 발생합니다.

STP PortFast BPDU 가드 개선을 통해 네트워크 설계자는 STP 도메인 경계를 적용하고 활성 토폴로지를 예측 가능하게 유지할 수 있습니다. STP PortFast가 활성화된 포트 뒤에 있는 디바이스는 STP 토폴로지에 영향을 줄 수 없습니다. BPDU를 수신할 때 BPDU 가드 작업은 PortFast가 구성된 포트를 비활성화합니다. BPDU 가드는 포트를 errdisable 상태로 전환하며 콘솔에 메시지가 나타납니다. 이 메시지는 다음과 같은 예입니다.

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.  
Disabling 2/1  
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

다음 예를 고려하십시오.

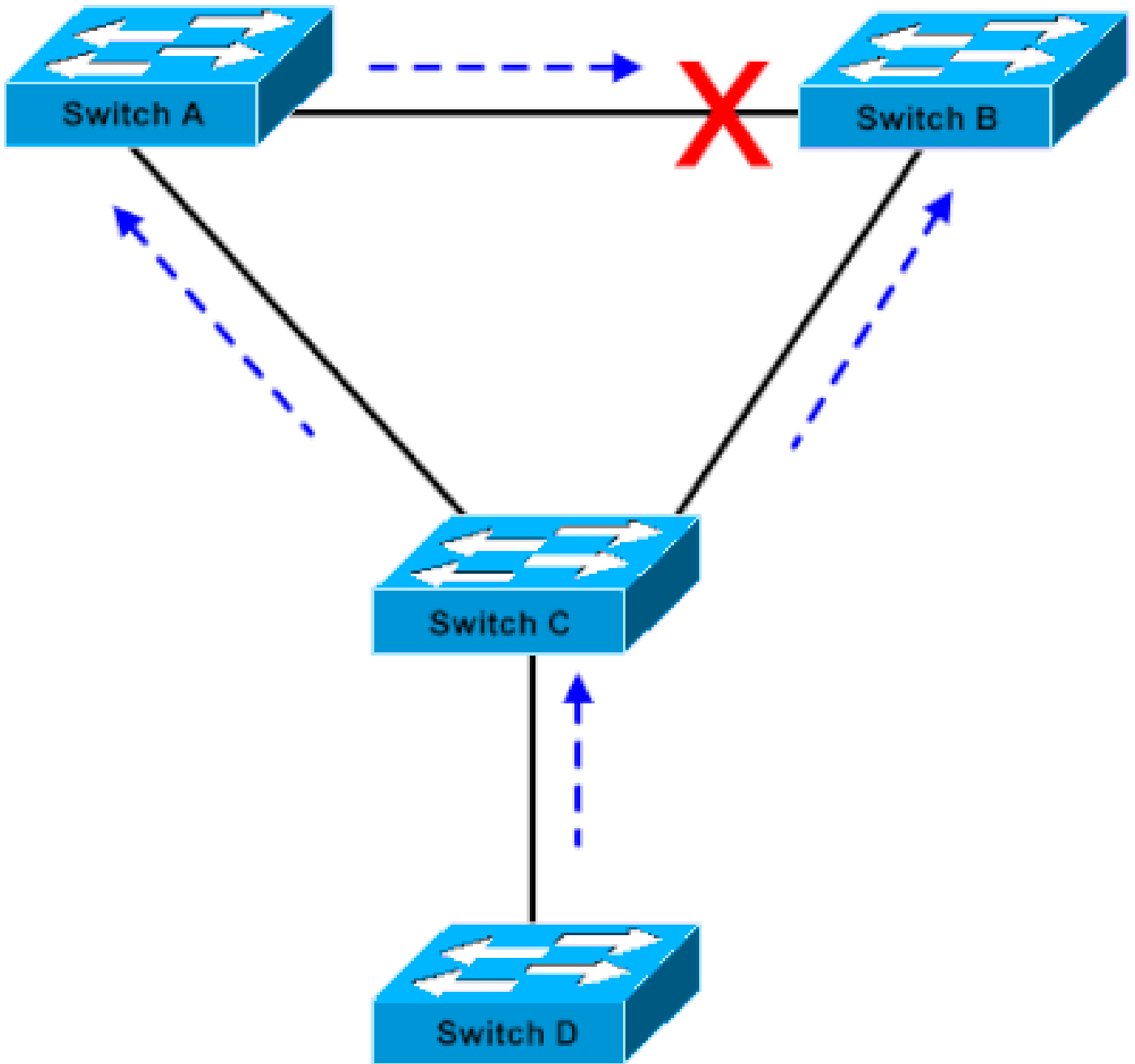
그림 1



브리지 연결

브리지 A는 우선순위 8192를 가지며 VLAN의 루트입니다. 브리지 B는 우선순위 16384을 가지며 동일한 VLAN에 대한 백업 루트 브리지입니다. 기가비트 이더넷 링크가 연결하는 브리지 A와 B가 네트워크의 핵심을 구성합니다. 브리지 C는 액세스 스위치이며 장치 D에 연결되는 포트에 PortFast가 구성되어 있습니다. 다른 STP 매개변수가 기본값인 경우 브리지 B에 연결되는 브리지 C 포트는 STP 차단 상태입니다. 장치 D(PC)는 STP에 참여하지 않습니다. 점선 화살표는 STP BPDU의 흐름을 나타낸다.

그림 2



Linux 기반 브리지 애플리케이션이 PC에서 실행됨

그림 2에서 디바이스 D는 STP에 참여하기 시작했습니다. 예를 들어 Linux 기반 브리지 애플리케이션이 PC에서 실행됩니다. 소프트웨어 브리지의 우선순위가 0 또는 루트 브리지의 우선순위보다 작은 값이면 소프트웨어 브리지가 루트 브리지 기능을 대신합니다. 두 코어 스위치를 연결하는 기가비트 이더넷 링크가 차단 모드로 전환됩니다. 이렇게 하면 해당 VLAN의 모든 데이터가 100Mbps 링크를 통해 이동합니다. VLAN의 코어를 통한 데이터 흐름이 링크가 수용할 수 있는 것보다 많을 경우 프레임 드롭이 발생합니다. 프레임 드롭은 연결 중단으로 이어집니다.

STP PortFast BPDU 가드 기능은 이러한 상황을 방지합니다. 이 기능은 브리지 C가 디바이스 D에서 STP BPDU를 수신하는 즉시 포트를 비활성화합니다.

설정

전역 기반으로 STP PortFast BPDU 가드를 활성화하거나 비활성화할 수 있으며, 이는 PortFast가 구성된 모든 포트에 영향을 미칩니다. 기본적으로 STP BPDU 가드는 비활성화되어 있습니다. 스위치에서 STP PortFast BPDU 가드를 활성화하려면 다음 명령을 실행합니다.

CatOS 명령

<#root>

Console> (enable)

```
set spantree portfast bpdu-guard enable
```

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)

Cisco IOS® Software 명령

<#root>

CatSwitch-IOS(config)#

```
spanning-tree portfast bpduguard
```

CatSwitch-IOS(config)

STP BPDU 가드가 포트를 비활성화하면 포트가 수동으로 활성화되지 않는 한 포트는 비활성 상태로 유지됩니다. errdisable 상태에서 자동으로 다시 활성화하도록 포트를 구성할 수 있습니다. 다음 명령을 실행하여 errdisable-timeout 간격을 설정하고 시간 제한 기능을 활성화합니다.

CatOS 명령

<#root>

Console> (enable)

```
set errdisable-timeout interval 400
```

Console> (enable)

```
set errdisable-timeout enable bpdu-guard
```

Cisco IOS Software 명령


```
<#root>
```

```
CatSwitch-IOS(config)#
```

```
errdisable recovery cause bpduguard
```

```
CatSwitch-IOS(config)#
```

```
errdisable recovery interval 400
```

 참고: 기본 시간 제한 간격은 300초이며, 기본적으로 시간 제한 기능은 비활성화되어 있습니다.

모니터링

이 기능이 활성화되었는지 아니면 비활성화되었는지 확인하려면 다음 해당 명령을 실행합니다.

명령 출력

CatOS 명령

```
<#root>
```

```
Console> (enable)
```

```
show spantree summary
```

```
Root switch for vlans: 3-4.
```

```
Portfast bpdu-guard enabled for bridge.
```

```
Uplinkfast disabled for bridge.
```

```
Backbonefast disabled for bridge.
```

```
Summary of Connected Spanning Tree Ports By VLAN:
```

```
Vlan Blocking Listening Learning Forwarding STP Active
```

```
-----  
1          0          0          0          1          1  
3          0          0          0          1          1  
4          0          0          0          1          1  
20         0          0          0          1          1
```

```
Blocking Listening Learning Forwarding STP Active
```

```
-----
```

Total 0 0 0 4 4

Console> (enable)

Cisco IOS Software 명령

<#root>

CatSwitch-IOS#

show spanning-tree summary totals

Root bridge for: none.

PortFast BPDU Guard is enabled

UplinkFast is disabled

BackboneFast is disabled

Spanning tree default pathcost method used is short

Name	Blocking	Listening	Learning	Forwarding	STP Active
-----	-----	-----	-----	-----	-----
1 VLAN	0	0	0	1	1

CatSwitch-IOS#

관련 정보

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.