

# 스위치의 링크 플랩 진단

## 목표

이 문서의 목적은 SG350X를 예로 사용하여 스위치의 링크 플랩 문제를 진단하고 해결하는 방법을 보여 주는 것입니다.

## 적용 가능한 디바이스 | 소프트웨어 버전

- SX350 | 2.5.7.85([최신 다운로드](#))
- SG350X | 2.5.7.85([최신 다운로드](#))
- SX550X | 2.5.7.85([최신 다운로드](#))

## 소개

링크 플랩이라고도 하는 포트 플랩은 스위치의 물리적 인터페이스가 10초 이상 지속되어 3 회 이상 작동 및 중단되는 상황입니다. 일반적인 원인은 대개 불량, 지원되지 않음 또는 비표준 케이블, SFP(Small Form-Factor Pluggable) 또는 기타 링크 동기화 문제와 관련이 있습니다. 링크 플래핑의 원인은 간헐적이거나 영구적일 수 있습니다.

링크 플래핑은 물리적 간섭이 되기 때문에 이 문서에서는 진단 및 방지를 위해 수행할 수 있는 단계와 절차를 설명합니다. 또한 이 문서에서는 링크 플랩 문제를 방지하거나 해결하기 위해 스위치에 구성할 수 있는 설정도 다룹니다.

## 목차

- [링크 플랩 식별](#)
- [케이블을 포함한 디바이스의 물리적 및 하드웨어 확인](#)
- [토폴로지 분석](#)
- [링크 플랩 방지 구성 방법](#)
- [EEE\(Energy Efficient Ethernet\) 비활성화](#)
- [Smartport 사용 안 함](#)

## 링크 플랩 식별

링크 플래핑은 네트워크에서 쉽게 식별할 수 있습니다. 특정 장치의 연결이 간헐적으로 이루어집니다. 디바이스의 syslog에서 링크 플랩을 확인하고 식별할 수 있습니다. syslog 메시지는 스위치 내에서 발생할 수 있는 이벤트, 오류 또는 심각한 문제에 대한 정보를 제공합니다. syslogs를 검토할 때 짧은 시간 내에 다시 돌아올 것으로 보이는 "Up" 및 "Down" 항목을 찾습니다. 이러한 항목에서는 어떤 포트에서 문제가 발생하는지 정확하게 설명하며, 특정 포트의 문제를 계속 해결할 수 있습니다.

Log Index	Log Time	Severity	Description
2147483594		Warning	%STP-W-PORTSTATUS: gi16: STP status Forwarding
2147483595		Informational	%LINK-I-Up: Vlan 1
2147483596		Informational	%LINK-I-Up: gi16
2147483597		Warning	%LINK-W-Down: Vlan 1
2147483598		Warning	%LINK-W-Down: gi16
2147483599		Informational	%INIT-I-Startup: Warm Startup
2147483600		Informational	
2147483601		Informational	
2147483602		Informational	
2147483603		Notice	%SYSLOG-N-LOGGING: Logging started.
2147483604		Warning	%STP-W-PORTSTATUS: gi16: STP status Forwarding
2147483605		Informational	%LINK-I-Up: Vlan 1
2147483606		Informational	%LINK-I-Up: gi16
2147483607		Warning	%LINK-W-Down: Vlan 1
2147483608		Warning	%LINK-W-Down: gi16
2147483609		Informational	%LINK-I-Up: Vlan 1
2147483610		Informational	%LINK-I-Up: gi16
2147483611		Informational	%LINK-I-Up: loopback1
2147483612		Warning	%LINK-W-Down: gi28

## 케이블을 포함한 디바이스의 물리적 및 하드웨어 확인

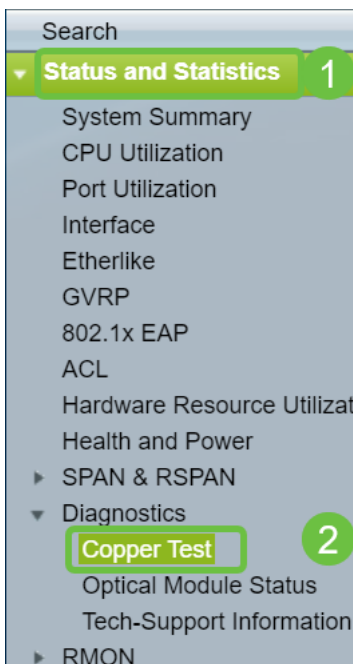
링크 플래핑의 일반적인 원인은 대개 불량, 지원되지 않음 또는 비표준 케이블, SFP(Small Form-Factor Pluggable) 또는 기타 링크 동기화 문제와 관련이 있습니다. 포트에서 사용 중인 이더넷 케이블과 케이블을 테스트하여 문제가 발생합니다. 디바이스가 최신 펌웨어에 있는지 확인합니다.

### 1단계

케이블을 변경하고 모니터해 보십시오. 문제가 계속되면 2단계로 진행합니다.

### 2단계

Status and Statistics(상태 및 통계) > Diagnostics(진단) > Copper Test(구리 테스트)로 이동합니다.



### 3단계

드롭다운 메뉴에서 Port를 선택합니다. 이 예에서는 GE16이 선택됩니다. 구리 테스트를 클릭합니다.

Copper Test

Note that basic cable test results would be accurate only if Short Reach is disabled.  
[Short Reach](#) is currently disabled.

Select the port on which to run the copper test.

Port: GE16 ▾

Copper Test

#### 4단계

경고가 나타납니다. 포트가 짧은 시간 동안 종료된다는 점에 유의하십시오. **확인**을 선택합니다.



The port is shut down during the brief testing period.  
 Click OK to continue or Cancel to stop the test.

Don't show me this again

OK Cancel

#### 5단계

테스트 결과가 표시됩니다. OK(정상)라고 표시되면 케이블이 아닐 가능성이 높습니다. 결과가 양호하지 않으면 케이블을 변경하고 구리 테스트를 반복하여 케이블이 아닌지 확인합니다.

**Test Results**

Last Update: 2021-Jan-18 09:13:50

Test Results: OK

Distance to Fault:

Operational Port Status: Up

#### 토폴로지 분석

스위치에서 구성 문제가 아닌 물리적 문제인지 확인하려면 스위치에 연결된 디바이스를 분석해야 합니다. 다음을 확인합니다.

1. 어떤 디바이스가 스위치에 연결되어 있습니까?

- 스위치에 연결된 각 디바이스를 분석합니다. 이러한 장치에 문제가 발생한 적이 있습니까?

3. 어떤 포트에서 문제가 발생하고 있으며 어떤 디바이스가 해당 포트에 연결되어 있습니까?

- 다른 디바이스를 연결하고 문제가 계속되는지 확인하여 포트를 테스트합니다.

- 디바이스가 다른 포트에서 문제를 일으키는지 확인합니다.

#### 6. 포트 또는 장치입니까?

- 포트인지 또는 디바이스인지 확인하는 과정에서 문제 해결 프로세스를 계속하는 방법이 결정됩니다.

- 디바이스인 경우 해당 디바이스의 지원 관리 팀에 문의해야 할 수 있습니다.

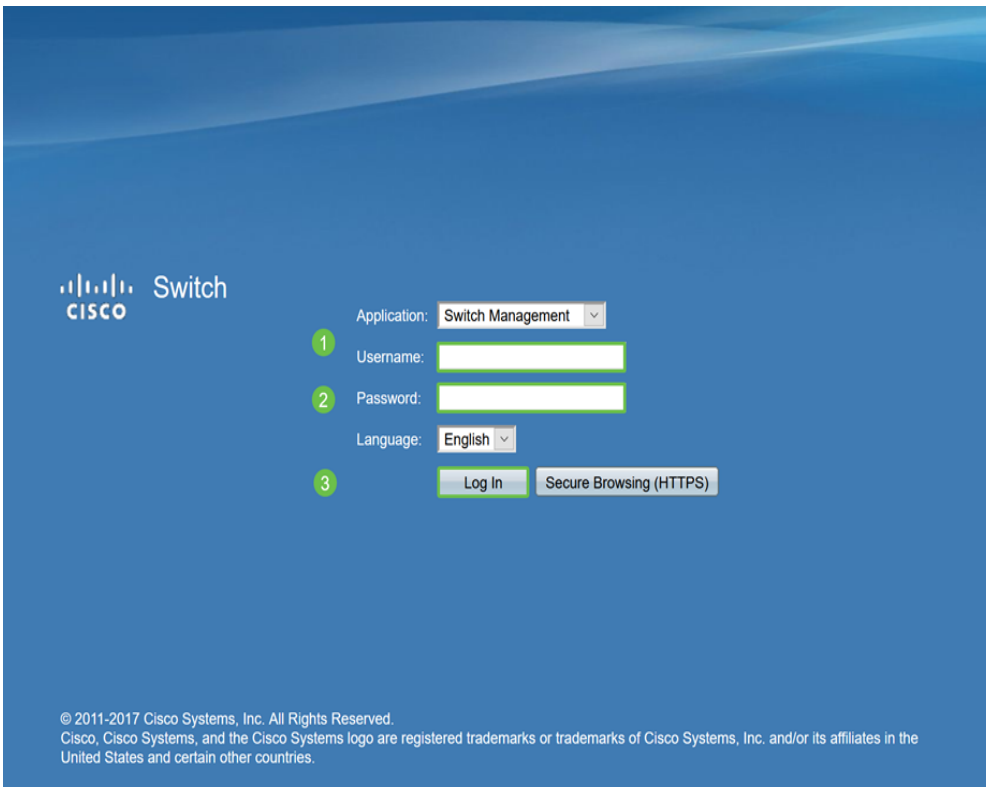
- 포트를 확인한 경우, 문제가 컨피그레이션과 관련되었는지 또는 물리적 포트와 관련되었는지 확인해야 합니다.

## 링크 플랩 방지 구성 방법

Link Flap Prevention은 스위치 및 네트워크 운영에 미치는 영향을 최소화합니다. 과도한 링크 플랩 이벤트가 발생하는 포트를 자동으로 설정하여 상태 포트를 err-disable하여 네트워크 토폴로지를 안정화합니다. 이 메커니즘은 플래핑의 근본 원인을 디버깅하고 찾는 시간도 제공합니다. 링크 플랩 및 포트 종료 관련 알림을 위해 syslog 메시지 또는 SNMP(Simple Network Management Protocol) 트랩이 전송됩니다. 시스템 관리자가 특별히 활성화한 경우에만 인터페이스가 다시 활성화됩니다. CLI 기반 지침을 보려면 CLI를 통해 [스위치에서 Configure Link Flap Prevention Settings\(링크 플랩 방지 설정 구성\) 문서를 참조하십시오.](#)

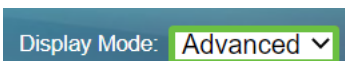
### 1단계

스위치의 GUI(그래픽 사용자 인터페이스)에 로그인합니다.



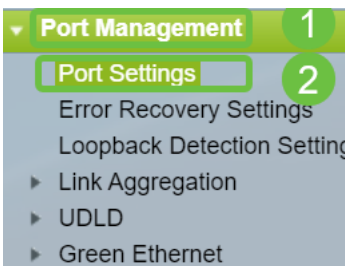
## 2단계

Advanced **Display Mode**를 선택합니다.



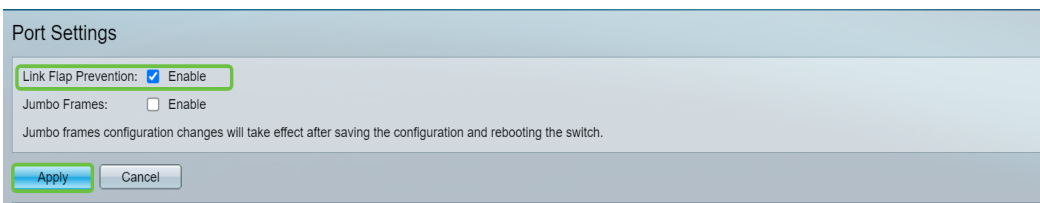
## 3단계

Port Management(포트 관리) > Port Settings(포트 설정)로 이동합니다.



## 4단계

Port Settings(포트 설정) 페이지에서 **Enable(활성화)** 상자를 선택하여 Link Flap Prevention(링크 플랩 방지)을 활성화합니다. Apply를 클릭합니다.



## 5단계

저장을 클릭합니다.

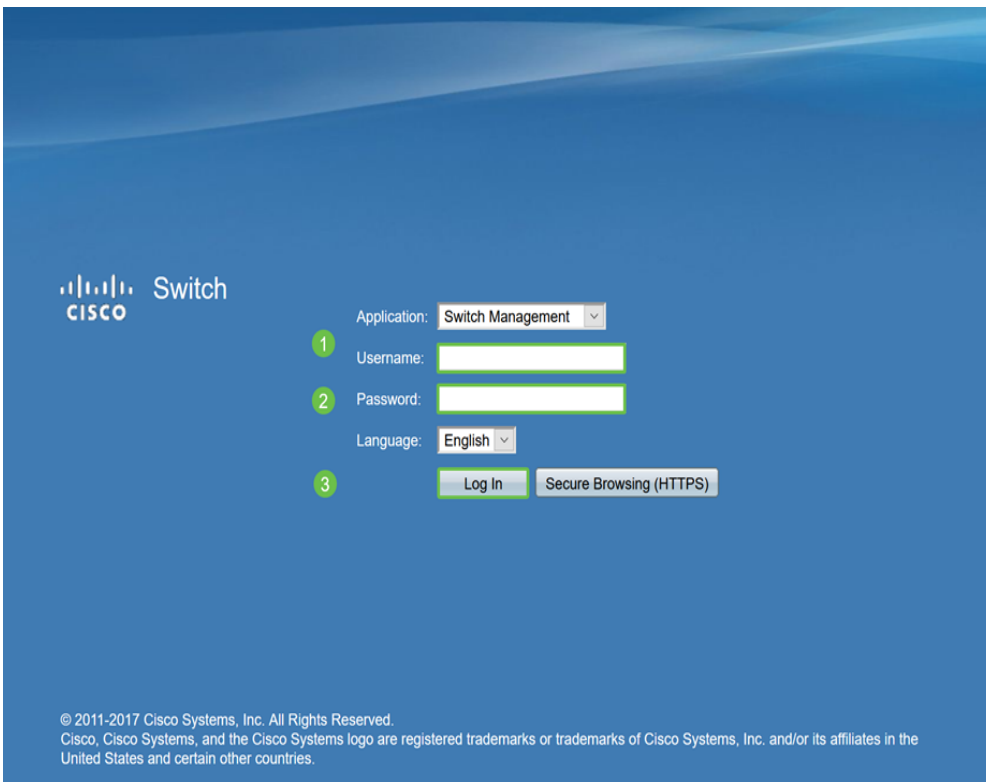
Save

## EEE(Energy Efficient Ethernet) 비활성화

토폴로지, 디바이스를 확인하고 Link Flap Prevention(링크 플랩 방지)을 활성화한 후에도 여전히 링크 플랩이 발생하고 있습니까?EEE(Energy Efficient Ethernet)를 비활성화해 보십시오. EEE의 목적은 이더넷 링크가 유휴 시간과 에너지 절약 기회를 갖는다는 것입니다.그러나 모든 디바이스가 EEE 802.3AZ와 호환되는 것은 아니며 비활성화하는 것이 가장 좋은 조치 방법이 될 수 있습니다.

### 1단계

스위치 GUI에 로그인합니다.



The image shows the Cisco Switch GUI login page. It features the Cisco logo and the text "Switch". The login form includes the following fields and buttons:

- Application: Switch Management (dropdown menu)
- 1 Username: (text input field)
- 2 Password: (text input field)
- Language: English (dropdown menu)
- 3 Log In (button)
- Secure Browsing (HTTPS) (checkbox)

At the bottom, there is a copyright notice: © 2011-2017 Cisco Systems, Inc. All Rights Reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

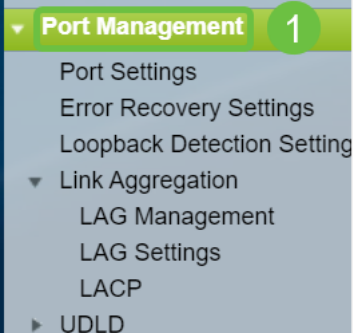
### 2단계

Advanced **Display Mode**를 선택합니다.

Display Mode: Advanced (dropdown menu)

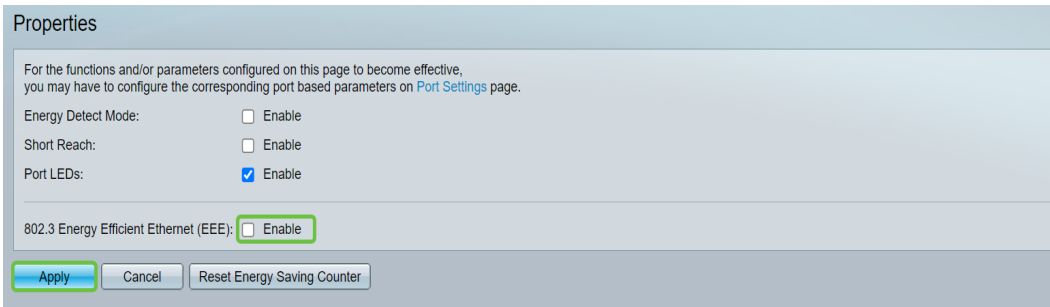
### 3단계

Port Management(**포트 관리**) > Green Ethernet(**녹색 이더넷**) > Properties(**속성**)로 이동합니다.



## 4단계

Enable(활성화) 상자의 선택을 취소하여 802.3 EEE(Energy Efficient Ethernet)를 비활성화합니다. Apply를 클릭합니다.



Properties

For the functions and/or parameters configured on this page to become effective, you may have to configure the corresponding port based parameters on [Port Settings](#) page.

Energy Detect Mode:  Enable

Short Reach:  Enable

Port LEDs:  Enable

802.3 Energy Efficient Ethernet (EEE):  Enable

Apply Cancel Reset Energy Saving Counter

## 5단계

저장을 클릭합니다.

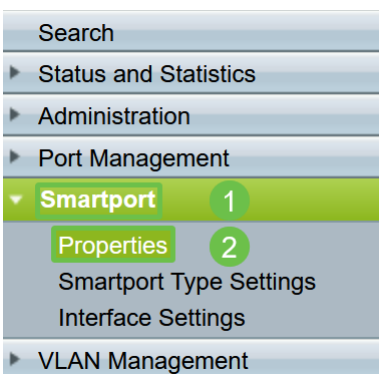


## Smartport 사용 안 함

Smartport 기능은 연결하려는 디바이스 유형에 따라 스위치 포트에 사전 구성된 설정을 적용합니다. Auto Smartport를 사용하면 디바이스가 탐지될 때 스위치에서 이러한 컨피그레이션을 인터페이스에 자동으로 적용할 수 있습니다. 경우에 따라 Smartport에서 디바이스를 잘못 탐지할 수 있으며, 이로 인해 특정 포트가 "플랩"될 수 있습니다. 이를 방지하려면 Smartport를 비활성화할 수 있습니다.

## 1단계

Smartport > 속성을 선택합니다.



## 2단계

스위치에서 **Smartport**를 전역적으로 비활성화하려면 Administrative *Auto Smartport* 옆에 있는 Disable을 선택합니다. Apply를 클릭합니다.

Properties

Telephony OUI is currently disabled. Auto Smartport and Telephony OUI are mutually exclusive.

Administrative Auto Smartport:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="radio"/> Enable by <a href="#">Auto Voice VLAN</a>	Operational Auto Smartport: Disabled
Auto Smartport Device Detection Method:	<input checked="" type="checkbox"/> CDP <input checked="" type="checkbox"/> LLDP	Operational CDP Status: Enabled Operational LLDP Status: Enabled
Auto Smartport Device Detection:	<input type="checkbox"/> Host <input checked="" type="checkbox"/> IP Phone <input checked="" type="checkbox"/> IP Phone + Desktop <input checked="" type="checkbox"/> Switch <input type="checkbox"/> Router <input checked="" type="checkbox"/> Wireless Access Point	

Apply Cancel

이렇게 하면 모든 인터페이스에서 Smartport가 비활성화되지만 수동 VLAN 컨피그레이션에는 영향을 주지 않습니다.

Smartport 문제가 있습니까? [Smartport 기능이 스위치에 문제를 일으킬 경우 이를 식별, 문제 해결 및 비활성화하는 방법을 알아봅니다.](#)

## 결론

링크 플래핑은 네트워크에서 악화될 수 있습니다. 하지만 지금까지 배운 모든 정보를 통해 링크 플랩 문제를 쉽게 진단, 방지 및 해결할 수 있습니다.