# CBS 250 and 350 Switches: Troubleshoot Link Flapping

# Objective

This article explains how to troubleshoot link flapping/port flapping issues on Cisco Business 350 series switches.

### **Applicable Devices | Firmware Version**

- CBS250 (Data Sheet) | 3.1 (Download latest)
- CBS350 (Data Sheet) | 3.1 (Download latest)
- CBS350-2X (Data Sheet) | 3.1 (Download latest)
- CBS350-4X (Data Sheet) | 3.1 (Download latest)

### **Table of Contents**

- Identify Link Flapping
- Confirm you are on the latest firmware version
- Check the physical hardware of the device including cables
- <u>Analyze your Topology</u>
  - What devices are connected to the Switch?
  - Is it the port or the device?
- How to configure Link Flap Prevention
- Disable Energy Efficient Ethernet (EEE):
- Disable the Smartport Feature

### Introduction

A link flap, also referred to as a port flap, is a condition in which a physical interface on the switch continually goes up and down. This occurs at a rate of three or more times a second for a duration of at least ten seconds. The common cause is usually related to bad, unsupported, or non-standard cable or Small Form-Factor Pluggable (SFP) or related to other link synchronization issues. Link flapping can be intermittent or permanent.

# **Identify Link Flapping**

Link flapping is easy to identify in a network. The connectivity of certain devices will be intermittent. Link flapping can be seen and identified in the Syslog of the switch. Syslog messages provide information about events, errors, or any serious problems that happen within the switch. When reviewing your Syslogs, look for *Up* and *Down* entries

that seem to be back-to-back in a short span of time. Those entries will also describe exactly which port is causing the issue so you can troubleshoot that specific port.

RAM	Nemo	ory		
RAM Me	emory Lo	og Table		
Clea	ar Logs			
Log In	ndex	Log Time	Severity	Description
21474	482324	2021-		and the factor is a strength in the second in the second in the second
21474	482325	2021-		
21474	482326	2021-		
21474	482327	2021-		
21474	482328	2021-		
21474	482329	2021-		
21474	482330	2021-		
21474	482331	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
21474	482332	2021-	Informational	%LINK-I-Up: gi1/0/4
21474	482333	2021-	Warning	%LINK-W-Down: gi1/0/4
21474	482334	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
21474	482335	2021-	Informational	%LINK-I-Up: gi1/0/4
21474	482336	2021-	Informational	%NT_poe-I-PowerNegStatusExpire: Port gi1/0/4 power negotiation moved to expire state, power protocol and allocation will remain at 6W (CDP) until port down/up cycle
21474	482337	2021-	Warning	%LINK-W-Down: gi1/0/4

### Confirm you are on the latest firmware version

The firmware is the program that controls the operation and functionality of the switch. Upgrading the firmware improves the performance of the device, which could provide enhanced security, new features, and bug fixes. Upgrading firmware can be a simple solution if you begin to experience issues with your switch.

### Step 1

### Go to Status and Statistics > System Summary.



### Step 2

Under Software Version you will find your current firmware version.

System Summary			
System Information	Edit	Software Information	0.1.0.57
System Leasting	CBS350-24FP-4X 24-Port Gigabit PoE Stackable Managed Switch with TUG Uplinks	Firmware Version (Active Image):	3.1.0.57
System Location:		Firmware MD5 Checksum (Active Image):	
System Contact:		Firmware Version (Non-active):	3.1.0.57
Host Name:	And the second se	Firmware MD5 Checksum (Non-active):	And the second sec
System Object ID:		Locale:	
System Uptime:	Transmission of the second second second	Language Version:	3.1.0.57
Current Time:	The second se	Locale:	
Base MAC Address:	An in the second s	Language Version:	3.1.0.57
Jumbo Frames:	Transmitter (Contraction)		

Navigate to <u>CBS350 downloads on Cisco.com</u> and check the latest version available. If you do not have the latest version, update your firmware. <u>Click for step-by-step instructions on this process</u>.

# Check the physical hardware of the device including cables

Test any cables being used on the port. To confirm you have the correct cables, you can refer to the device's data sheet found <u>here</u>.

### Step 1

Try changing cables and monitoring. If the issue persists, proceed to the next step.

### Step 2

Change to Advanced Mode.

B	admin	English	~	Advanced 🗸	8	0	•
				Basic			
				Advanced			

### Step 3

Go to status and **Statistics > Diagnostics > Copper Test**.

<ul> <li>Status and Statistics</li> </ul>	
System Summary	
CPU Utilization	
Port Utilization	
Interface	
Etherlike	
GVRP	
802.1x EAP	
ACL	
Hardware Resource Utilization	
Health and Power	
SPAN & RSPAN	

Select a port and press Copper Test.



### Step 5

A warning will appear explaining that the port will be shut down for a short period of time. Click **OK**.



### Step 6

The results will appear. If it shows that everything is okay, it is probably not the cable. If the results are not okay, change the cable and repeat the copper test to confirm that it is not the cable.

Test Results	
Last Update: Test Results: Distance to Fault: Operational Port Status:	Down

# Analyze your Topology

In order to confirm it is a physical problem and not a configuration on the switch, answer the following questions:

What devices are connected to the Switch?

Analyze each device connected to the switch to see if that is the issue. Have you experienced any issues with those devices?

### Is it the port or the device?

- Connect other devices to that port to see if the problem continues. If it is the device, you may have to contact support management for that device.
- Connect the device to other ports to see if it causes problems on another port. If you find

## How to configure Link Flap Prevention

Link flap prevention minimizes the disruption to switch and network operations in a link flap situation. It stabilizes the network topology by automatically setting the ports that experience excessive link flap events to *err-disable*. This mechanism also provides time to debug and locate the root cause for the flapping. A Syslog message or Simple Network Management Protocol (SNMP) trap is sent to alert regarding link flap and port shutdown. The interface will become active again only if specifically enabled by you or your system administrator.

### Step 1

Log into your switch Web User Interface (UI).

	cisco	
	Switch	
	admin	
	English ~	
	Log In	
© 2020-	2021 Cisco Systems, Inc. All Rights F	Reserved.
Cisco, Cisco Systems trademarks of Cisco	, and the Cisco Systems logo are reg Systems, Inc. and/or its affiliates in the certain other countries.	istered trademarks or he United States and

### Step 2

### Change to Advanced Mode.



### Step 3

Go to Port Management > Port Settings.



Check the Enable box for Link Flap Prevention. Press Apply.



### Step 5

Save your configurations by pressing the save icon.



# **Disable Energy Efficient Ethernet (EEE):**

After checking your topology, devices, and enabling link flap prevention you are still experiencing port flapping, try disabling Energy Efficient Ethernet (EEE). The purpose of EEE is that Ethernet links have idle time and the opportunity to save energy. However, not all devices are compatible with EEE 802.3AZ, and disabling it may be the best course of action.

### Step 1

Log into the switch Web UI.

	cisco	
	Switch	
	admin	
	English ~	
	Log In	
© 2020-: Cisco, Cisco Systems trademarks of Cisco	2021 Cisco Systems, Inc. All Rights I , and the Cisco Systems logo are reg Systems, Inc. and/or its affiliates in t certain other countries.	Reserved. gistered trademarks or he United States and

### Step 2

Choose Advanced display mode in the upper right corner of your screen.

B	admin	English	~	Advanced 🗸	8	0	•
				Basic			
				Advanced			

Go to Port Management > Green Ethernet > Properties.



### Step 4

Disable 802.3 Energy Efficient Ethernet (EEE) by unchecking the enable box. Press **Apply.** 

save icon
~
k

### **Disable the Smartport Feature**

The Smartport feature applies a preconfigured setup to that switch port based on the type of device that is trying to connect. Auto Smartport lets the switch apply these configurations to interfaces automatically when it detects the device. However, at times a Smartport may detect the device incorrectly, which can cause port flapping. To ensure this is not occurring, you can disable the Smartport feature.

Navigate to Smartport > Properties.



### Step 2

At this location, you can view the Smartport settings or simply disable the feature if you choose. Adjust as needed and click **Apply**.



### Step 3 (Optional)

For more options, change Display Mode from Basic to **Advanced**. This is located in the top-right corner of your screen.



### Step 4

To permanently save your configurations, click the save icon.



### Conclusion

Link flapping can be debilitating in a network and with this document you have learned how to diagnose, prevent, and help solve the problem.

Having other Smartport issues? Diagnose Smartports here.

Looking for more articles on your CBS250 or CBS350 switch? Check out any of the links below for more information!

<u>SNMP Settings SNMP Views SNMP Groups DHCP Image Upgrade Password Strength TCP</u> and UDP Settings Port Security Time Settings Upgrade Firmware Smartport Best Practices Reset Switch Troubleshoot: No IP Address Troubleshoot Smartports Create VLANs