

# Switches der Serien CBS 250 und 350: Fehlerbehebung beim Flapping der Verbindung

## Ziel

In diesem Artikel wird erläutert, wie Sie Probleme mit dem Flapping von Verbindungen bzw. dem Flapping von Ports auf Cisco Switches der Serie Business 350 beheben können.

## Unterstützte Geräte | Firmware-Version

- CBS 250 ([Datenblatt](#)) | 3.1 ([aktuellste Version herunterladen](#))
- CBS 350 ([Datenblatt](#)) | 3.1 ([aktuellste Version herunterladen](#))
- CBS350-2X ([Datenblatt](#)) | 3.1 ([Aktuelles Download](#))
- CBS350-4X ([Datenblatt](#)) | 3.1 ([Aktuelles Download](#))

## Inhalt

- [Identifizieren von Link-Flapping](#)
- [Bestätigen Sie, dass Sie die neueste Firmware-Version verwenden.](#)
- [Überprüfen Sie die physische Hardware des Geräts, einschließlich Kabel.](#)
- [Analyse Ihrer Topologie](#)
  - [Welche Geräte sind mit dem Switch verbunden?](#)
  - [Handelt es sich um den Port oder das Gerät?](#)
- [Konfigurieren von Link Flap Prevention](#)
- [Energy Efficient Ethernet \(EEE\) deaktivieren:](#)
- [Smartport-Funktion deaktivieren](#)

## Einleitung

Eine Verbindungs-Klappe, auch als Port-Klappe bezeichnet, ist eine Bedingung, bei der eine physische Schnittstelle am Switch kontinuierlich hoch- und herunterfährt. Dies geschieht in einer Geschwindigkeit von drei oder mehr mal pro Sekunde für eine Dauer von mindestens zehn Sekunden. Die häufige Ursache ist in der Regel ein fehlerhaftes, nicht unterstütztes oder nicht standardmäßiges Kabel oder SFP (Small Form-Factor Pluggable) oder ein Zusammenhang mit anderen Problemen bei der Link-Synchronisierung. Die Verbindungsflapping kann zeitweilig oder dauerhaft sein.

## Identifizieren von Link-Flapping

Die Verbindungsflapping ist in einem Netzwerk leicht zu identifizieren. Bestimmte Geräte werden nur gelegentlich verbunden. Das Flapping der Verbindungen kann im

Syslog des Switches angezeigt und identifiziert werden. Syslog-Meldungen enthalten Informationen zu Ereignissen, Fehlern oder ernsthaften Problemen, die im Switch auftreten. Achten Sie beim Überprüfen Ihrer Syslogs auf *Up* and *Down*-Einträge, die anscheinend innerhalb kurzer Zeit wieder zurück zu liegen scheinen. In diesen Einträgen wird auch genau beschrieben, welcher Port das Problem verursacht, damit Sie diesen bestimmten Port beheben können.

RAM Memory

RAM Memory Log Table

Clear Logs

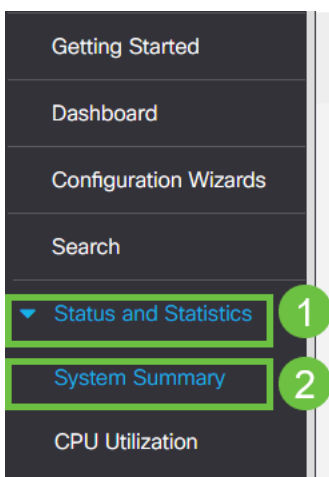
Log Index	Log Time	Severity	Description
2147482324	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
2147482325	2021-	Warning	%LINK-I-Up: gi1/0/4
2147482326	2021-	Warning	%LINK-W-Down: gi1/0/4
2147482327	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
2147482328	2021-	Warning	%LINK-I-Up: gi1/0/4
2147482329	2021-	Warning	%LINK-W-Down: gi1/0/4
2147482330	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
2147482331	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
2147482332	2021-	Informational	%LINK-I-Up: gi1/0/4
2147482333	2021-	Warning	%LINK-W-Down: gi1/0/4
2147482334	2021-	Warning	%STP-W-PORTSTATUS: gi1/0/4: STP status Forwarding
2147482335	2021-	Informational	%LINK-I-Up: gi1/0/4
2147482336	2021-	Informational	%NT_poe-l-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
2147482337	2021-	Warning	%LINK-W-Down: gi1/0/4

## Bestätigen Sie, dass Sie die neueste Firmware-Version verwenden.

Die Firmware ist das Programm, das den Betrieb und die Funktionalität des Switches steuert. Durch die Aktualisierung der Firmware wird die Leistung des Geräts verbessert, wodurch mehr Sicherheit, neue Funktionen und Fehlerbehebungen möglich sind. Die Aktualisierung der Firmware kann eine einfache Lösung sein, wenn Probleme mit Ihrem Switch auftreten.

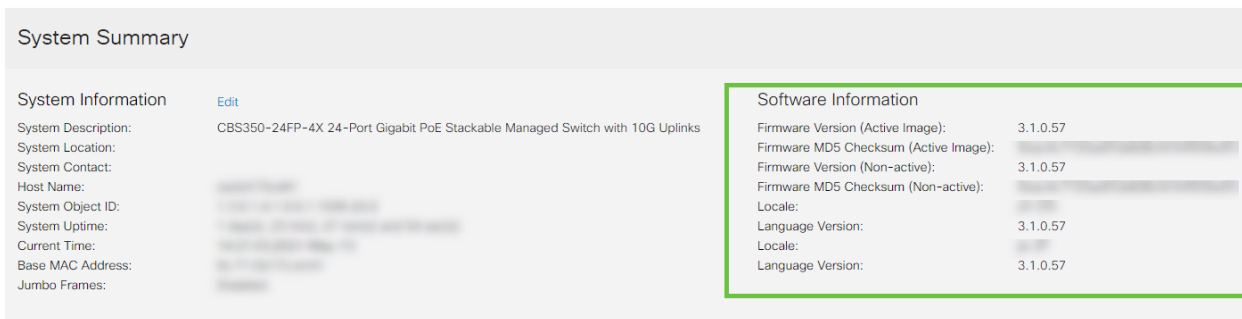
### Schritt 1

Gehen Sie zu **Status und Statistik > Systemübersicht**.



### Schritt 2

Unter *Softwareversion* finden Sie die aktuelle Firmware-Version.



The screenshot shows the 'System Summary' page. On the right side, there is a 'Software Information' table with the following data:

Software Information	
Firmware Version (Active Image):	3.1.0.57
Firmware MD5 Checksum (Active Image):	
Firmware Version (Non-active):	3.1.0.57
Firmware MD5 Checksum (Non-active):	
Locale:	
Language Version:	3.1.0.57
Locale:	
Language Version:	3.1.0.57

### Schritt 3

Navigieren Sie zu [CBS 350-Downloads auf Cisco.com](#) und überprüfen Sie die neueste verfügbare Version. Wenn Sie nicht über die neueste Version verfügen, aktualisieren Sie Ihre Firmware. [Klicken Sie hier, um eine schrittweise Anleitung zu diesem Vorgang zu erhalten.](#)

## Überprüfen Sie die physische Hardware des Geräts, einschließlich Kabel.

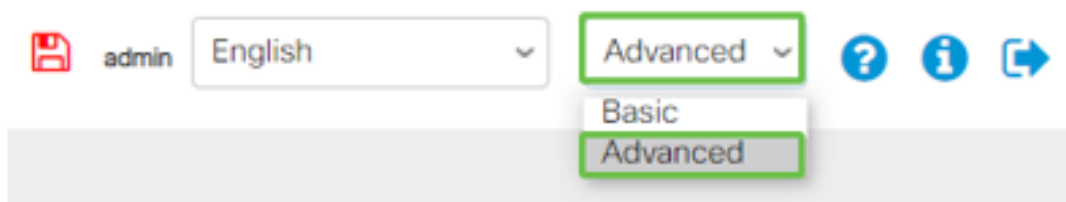
Testen Sie alle Kabel, die am Port verwendet werden. Um sicherzustellen, dass die richtigen Kabel vorhanden sind, können Sie sich das Datenblatt des Geräts [hier](#) ansehen.

### Schritt 1

Versuchen Sie, die Kabel und die Überwachung zu ändern. Wenn das Problem weiterhin besteht, fahren Sie mit dem nächsten Schritt fort.

### Schritt 2

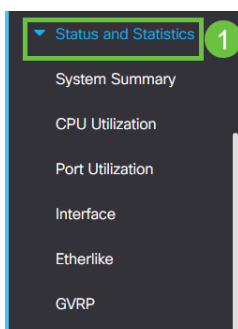
Wechseln Sie in den **erweiterten Modus**.



The screenshot shows the user interface with a dropdown menu for mode selection. The 'Advanced' option is highlighted with a green box, and the 'Basic' option is also visible below it.

### Schritt 3

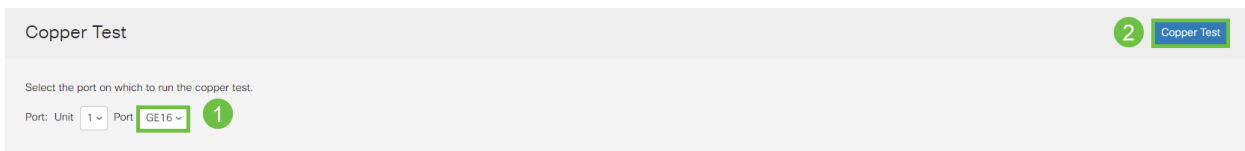
Gehen Sie zu Status and **Statistics > Diagnostics > Copper Test**.



The screenshot shows the navigation menu with 'Status and Statistics' highlighted and a green circle with the number '1' next to it.

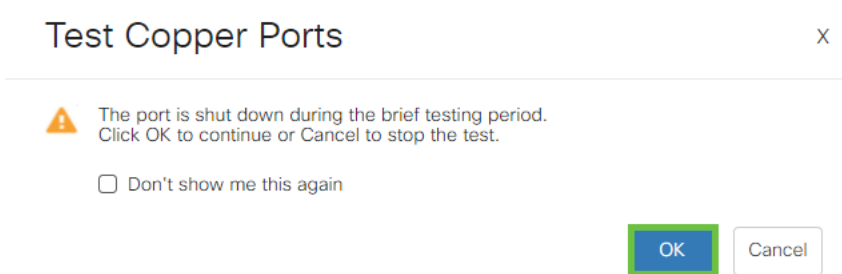
## Schritt 4

Wählen Sie einen Anschluss aus, und drücken Sie **Copper Test (Kupfertest)**.



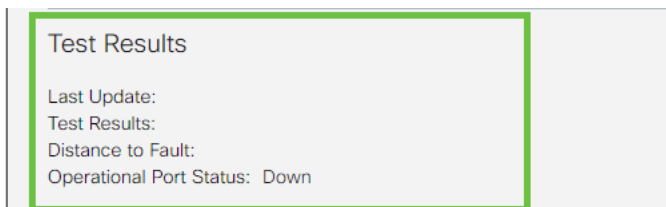
## Schritt 5

Es wird eine Warnung angezeigt, dass der Port für einen kurzen Zeitraum geschlossen wird. Klicken Sie auf **OK**.



## Schritt 6

Die Ergebnisse werden angezeigt. Wenn es zeigt, dass alles in Ordnung ist, ist es wahrscheinlich nicht das Kabel. Wenn die Ergebnisse nicht in Ordnung sind, wechseln Sie das Kabel, und wiederholen Sie den Kupfertest, um sicherzustellen, dass es sich nicht um das Kabel handelt.



## Analyse Ihrer Topologie

Beantworten Sie die folgenden Fragen, um zu bestätigen, dass es sich um ein physisches Problem und nicht um eine Konfiguration auf dem Switch handelt:

### Welche Geräte sind mit dem Switch verbunden?

Analysieren Sie jedes Gerät, das mit dem Switch verbunden ist, um festzustellen, ob das Problem vorliegt. Haben Sie Probleme mit diesen Geräten festgestellt?

### Handelt es sich um den Port oder das Gerät?

- Schließen Sie andere Geräte an diesen Port an, um festzustellen, ob das Problem weiterhin besteht. Wenn es sich um das Gerät handelt, müssen Sie sich möglicherweise an das Support-Management für dieses Gerät wenden.

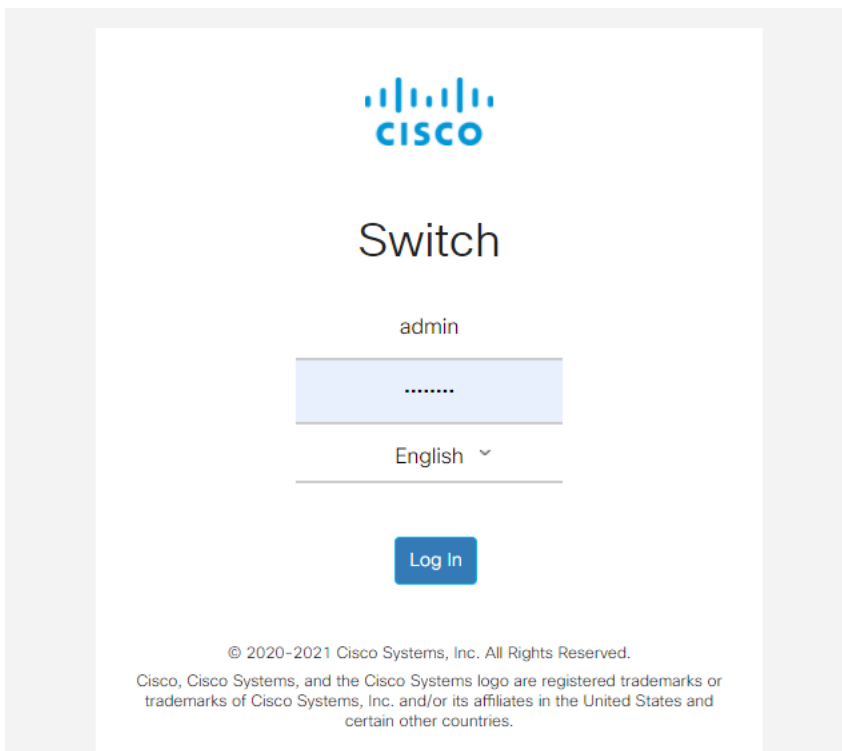
- Schließen Sie das Gerät an andere Ports an, um festzustellen, ob es Probleme an einem anderen Port verursacht. Wenn Sie feststellen, dass es sich um den Port handelt, müssen Sie feststellen, ob es sich um ein Konfigurations- oder ein physisches Problem handelt.

## Konfigurieren von Link Flap Prevention

Durch die Vermeidung von Link-Flapping wird die Unterbrechung des Switch- und Netzwerkbetriebs in einer Situation mit Link-Flapping minimiert. Es stabilisiert die Netzwerktopologie, indem die Ports, bei denen exzessive Link-Flapping-Ereignisse auftreten, automatisch *deaktiviert werden*. Dieser Mechanismus bietet auch Zeit zum Debuggen und Suchen der Ursache für das Flapping. Es wird eine Syslog-Meldung oder ein Simple Network Management Protocol (SNMP)-Trap gesendet, um eine Warnmeldung bezüglich der Link-Flapping und des Port-Shutdown zu erhalten. Die Schnittstelle wird nur dann wieder aktiv, wenn sie von Ihnen oder Ihrem Systemadministrator ausdrücklich aktiviert wurde.

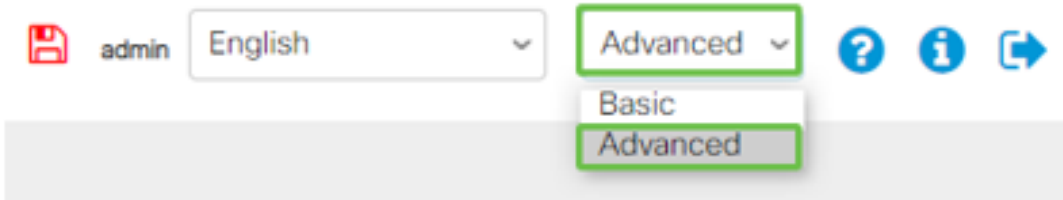
### Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche des Switches an.



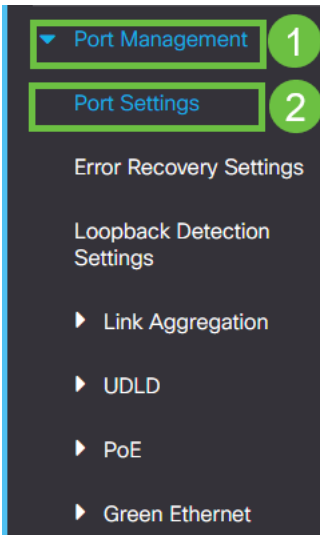
### Schritt 2

Wechseln Sie in den **erweiterten Modus**.



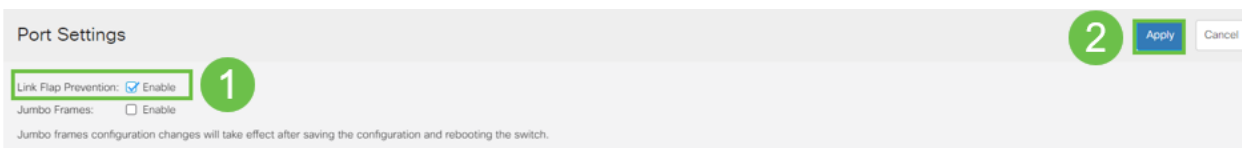
### Schritt 3

Gehen Sie zu **Port Management > Port Settings**.



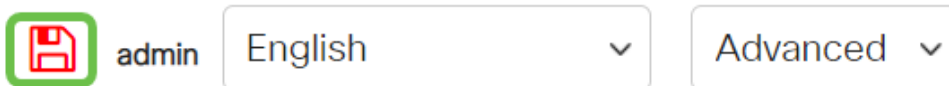
### Schritt 4

Aktivieren Sie das Kontrollkästchen Aktivieren für *Link Flap Prevention*. Drücken Sie **Übernehmen**.



### Schritt 5

Speichern Sie Ihre Konfigurationen, indem Sie das **Symbol zum Speichern** drücken.

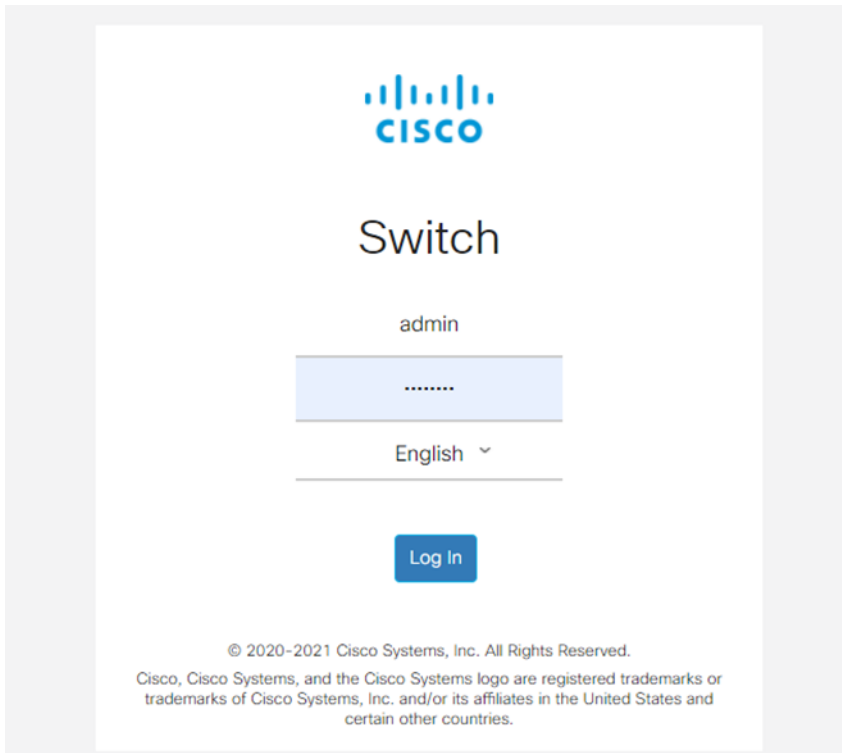


## Energy Efficient Ethernet (EEE) deaktivieren:

Wenn Sie Topologie und Geräte überprüft und die Verhinderung von Verbindungsflapping aktiviert haben, fällt der Port immer noch aus, und deaktivieren Sie Energy Efficient Ethernet (EEE). Der Zweck von EEE besteht darin, dass Ethernet-Verbindungen Leerlaufzeiten haben und Energie sparen können. Allerdings sind nicht alle Geräte mit EEE 802.3AZ kompatibel, und die Deaktivierung ist möglicherweise die beste Vorgehensweise.

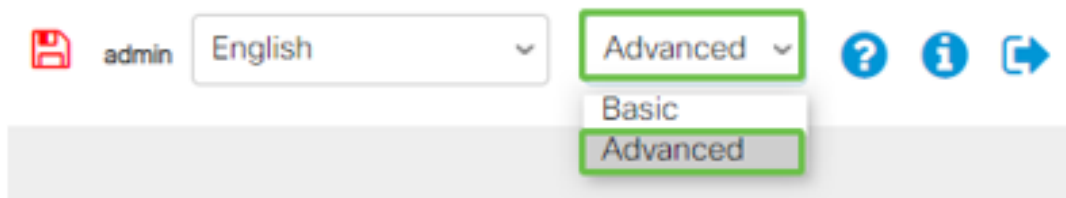
## Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche des Switches an.



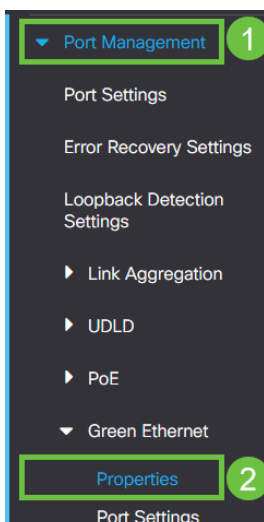
## Schritt 2

Wählen Sie **Erweiterter** Anzeigemodus in der oberen rechten Ecke des Bildschirms aus.



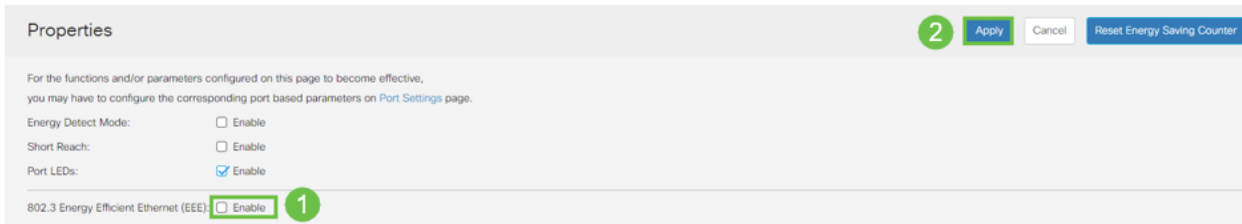
## Schritt 3

Gehen Sie zu **Port Management > Green Ethernet > Properties**.



## Schritt 4

Deaktivieren Sie 802.3 Energy Efficient Ethernet (EEE), indem Sie das Kontrollkästchen enable deaktivieren. Drücken Sie **Übernehmen**.



## Schritt 5

Speichern Sie die Konfigurationen, indem Sie das **Symbol zum Speichern** drücken.

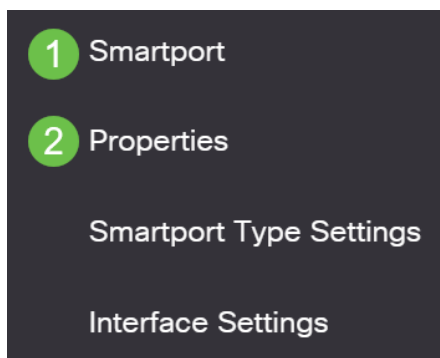


## Smartport-Funktion deaktivieren

Die SmartPort-Funktion wendet eine vorkonfigurierte Konfiguration auf diesen Switch-Port an, basierend auf dem Gerätetyp, der eine Verbindung herstellt. Mit Auto Smartport kann der Switch diese Konfigurationen automatisch auf Schnittstellen anwenden, wenn er das Gerät erkennt. Manchmal erkennt ein Smartport das Gerät jedoch falsch, was zu einem Port-Flapping führen kann. Um sicherzustellen, dass dies nicht geschieht, können Sie die Smartport-Funktion deaktivieren.

## Schritt 1

Navigieren Sie zu **Smartport > Eigenschaften**.



## Schritt 2

An dieser Stelle können Sie die Smartport-Einstellungen anzeigen oder die Funktion einfach deaktivieren, wenn Sie diese Option auswählen. Passen Sie das Programm nach Bedarf an, und klicken Sie auf **Übernehmen**.



Properties 2 Apply Cancel

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

Administrative Auto Smartport: 1  Disable Operational Auto Smartport: Disabled  
 Enable  
 Enable by Auto Voice VLAN

Auto Smartport Device Detection Method:  CDP Operational CDP Status: Enabled  
 LLDP Operational LLDP Status: Enabled

### Schritt 3 (optional)

Ändern Sie für weitere Optionen den Anzeigemodus von Basic (Einfach) in **Advanced (Erweitert)**. Diese befindet sich in der rechten oberen Ecke des Bildschirms.

admin English Basic Basic Advanced

### Schritt 4

Um Ihre Konfigurationen dauerhaft zu speichern, klicken Sie auf das **Symbol zum Speichern**.

admin English Advanced

## Schlussfolgerung

Link-Flapping kann in einem Netzwerk lähmend sein. In diesem Dokument erfahren Sie, wie Sie das Problem diagnostizieren, verhindern und beheben können.

Haben Sie andere Smartport-Probleme? [Smartports hier diagnostizieren](#).