

Schutz vor Verbindungsausfällen bei Switches der Serien Sx250 und Sx350

Ziel

Link-Flapping ist eine Situation, in der eine physische Schnittstelle auf dem Switch kontinuierlich hochfährt und ausfällt, mindestens dreimal pro Sekunde für eine Dauer von mindestens 10 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 Ursache für das Flapping von Verbindungen kann zeitweilig oder dauerhaft sein.

Der Mechanismus zur Verhinderung von Link-Flapping minimiert die Unterbrechung des Switch- und Netzwerkbetriebs in einer Situation mit Link-Flapping. Die Netzwerktopologie wird stabilisiert, indem die Ports, bei denen exzessive Link-Flapping-Ereignisse auftreten, automatisch so eingestellt werden, dass Status-Ports deaktiviert werden. Dieser Mechanismus bietet auch Zeit für das Debuggen und das Auffinden der Ursache für Flapping. Es wird eine Syslog-Meldung oder ein Simple Network Management Protocol (SNMP)-Trap gesendet, um vor Link-Flapping und Port-Shutdown zu warnen. Die Schnittstelle wird nur dann wieder aktiv, wenn sie vom Systemadministrator ausdrücklich aktiviert wurde.

Dieser Artikel enthält Anweisungen zum Aktivieren der Funktion "Link Flap Prevention", zum Konfigurieren der automatischen ErrDisable-Wiederherstellungszeit und zum erneuten Aktivieren einer ausgesetzten Schnittstelle auf Ihrem Switch der Serie Sx250 oder Sx350.

Unterstützte Geräte

Serie SF350

SG350-Serie

Serie SF250

SG250-Serie

Software-Version

- 2.1.0.63

Konfigurieren des Link-Flap-Schutzes

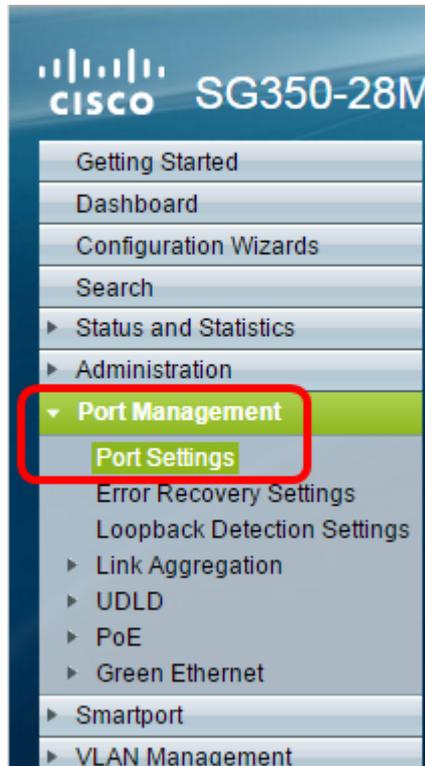
Schutz vor Link-Flapping aktivieren

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres Switches an.

Schritt 2: Wählen Sie im Dropdown-Menü Anzeigemodus die Option **Erweitert** aus.



Schritt 3: Wählen Sie **Port Management > Port Settings** aus.



Schritt 4: Aktivieren Sie das Kontrollkästchen **Enable** Link Flap Prevention.

Anmerkung: Standardmäßig ist die Funktion "Link Flap Prevention" aktiviert.



Schritt 5: Klicken Sie auf **Apply**, um die Änderungen in der aktuellen Konfigurationsdatei zu speichern.

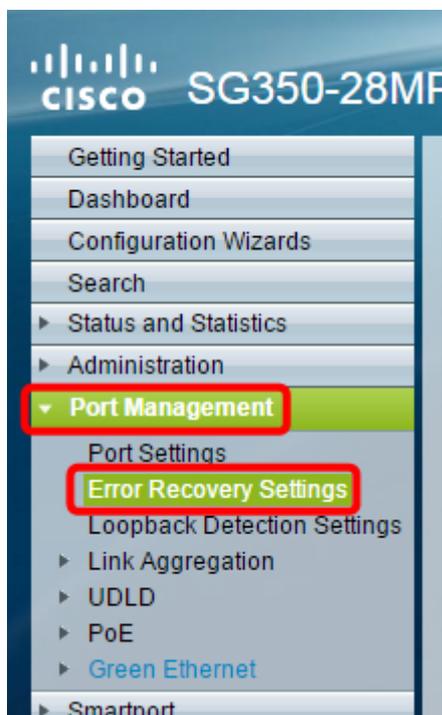
Schritt 6: Klicken Sie auf **Speichern**, um die Startkonfigurationsdatei zu aktualisieren.



Sie sollten jetzt Link Flap Prevention auf Ihrem Managed Switch der Serie Sx350 aktivieren.

Automatische ErrDisable-Wiederherstellungszeit konfigurieren

Schritt 1: Um eine Wiederherstellungszeit für ausgesetzte Schnittstelle festzulegen, gehen Sie zu **Port Management > Error Recovery Settings**.



Schritt 2: (Optional) Geben Sie im Feld *Automatisches Wiederherstellungsintervall* einen Wert in Sekunden ein.



Schritt 3: Aktivieren Sie im Bereich Automatische ErrDisable-Wiederherstellung das Kontrollkästchen **Enable** Link Flap Prevention.

Anmerkung: Der Schutz vor Link-Flap ist standardmäßig für die automatische ErrDisable-Wiederherstellung aktiviert.

cisco Language: English

P 28-Port Gigabit PoE Managed Switch

Error Recovery Settings

Automatic Recovery Interval: sec (Range: 30 - 86400, Default: 300)

Automatic ErrDisable Recovery

Port Security:	<input type="checkbox"/>	Enable
802.1x Single Host Violation:	<input type="checkbox"/>	Enable
ACL Deny:	<input type="checkbox"/>	Enable
STP BPDU Guard:	<input type="checkbox"/>	Enable
STP Loopback Guard:	<input type="checkbox"/>	Enable
UDLD:	<input type="checkbox"/>	Enable
Loopback Detection:	<input type="checkbox"/>	Enable
Storm Control:	<input type="checkbox"/>	Enable
Link Flap Prevention:	<input checked="" type="checkbox"/>	Enable

Schritt 4: Klicken Sie auf **Apply**, um die Änderungen in der aktuellen Konfigurationsdatei zu speichern.

Schritt 5: Klicken Sie auf **Speichern**, um die Startkonfigurationsdatei zu aktualisieren.

Save

P 28-Port Gigabit PoE Managed Switch

Error Recovery Settings

✓ Success. To permanently save the configuration, go to the [Copy/Save Configuration](#)

Automatic Recovery Interval: sec (Range: 30 - 86400, Default: 30)

Automatic ErrDisable Recovery

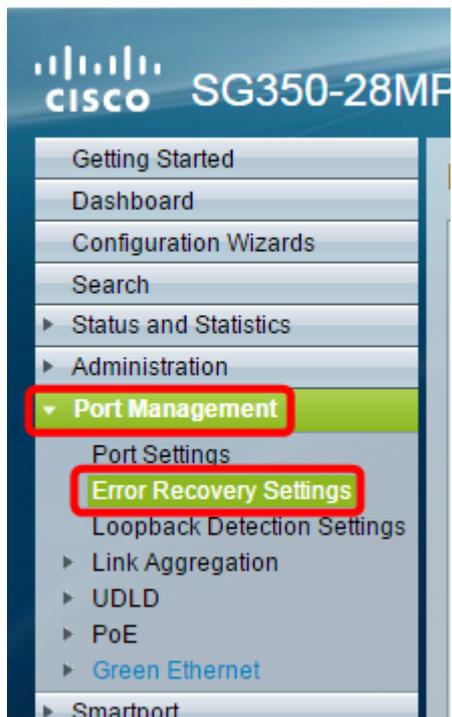
Port Security:	<input type="checkbox"/>	Enable
802.1x Single Host Violation:	<input type="checkbox"/>	Enable
ACL Deny:	<input type="checkbox"/>	Enable
STP BPDU Guard:	<input type="checkbox"/>	Enable
STP Loopback Guard:	<input type="checkbox"/>	Enable
UDLD:	<input type="checkbox"/>	Enable
Loopback Detection:	<input type="checkbox"/>	Enable
Storm Control:	<input type="checkbox"/>	Enable
Link Flap Prevention:	<input checked="" type="checkbox"/>	Enable

Apply Cancel

Sie sollten jetzt die Einstellungen für die automatische ErrDisable-Wiederherstellungszeit auf Ihrem Managed Switch der Serie Sx350 konfiguriert haben.

Deaktivieren einer ausgesetzten Schnittstelle

Schritt 1: Um den Status der Schnittstelle "errDisabled" oder "Suspended" zu überprüfen, gehen Sie zu **Port Management > Error Recovery Settings**.



Anmerkung: Wenn eine Schnittstelle aufgrund von Link Flap Prevention ausgesetzt wird, werden in der Tabelle Suspended (errDisabled) (Ausgesetzte Schnittstelle) die ausgesetzten Schnittstellen angezeigt.

cisco Language: English

P 28-Port Gigabit PoE Managed Switch

Error Recovery Settings

Automatic Recovery Interval: sec (Range: 30 - 86400, Default)

Automatic ErrDisable Recovery

Port Security: Enable

802.1x Single Host Violation: Enable

ACL Deny: Enable

STP BPDU Guard: Enable

STP Loopback Guard: Enable

UDLD: Enable

Loopback Detection: Enable

Storm Control: Enable

Link Flap Prevention: Enable

Suspended (errDisabled) Interface Table

Filter: Suspension Reason equals to

<input type="checkbox"/>	Interface	Suspension Reason
0 results found.		

Schritt 2: Aktivieren Sie das Kontrollkästchen neben der Schnittstelle, die Sie erneut aktivieren möchten.

Schritt 3: Klicken Sie auf die Schaltfläche **Reaktivieren**, um eine ausgesetzte Schnittstelle erneut zu aktivieren.

Sie sollten jetzt eine ausgesetzte Schnittstelle auf Ihrem Managed Switch der Serie Sx250 oder Sx350 erneut aktivieren.