Integrierte Paketerfassung bei Catalyst Switches der Serien 1200 und 1300

Ziel

In diesem Artikel wird die neue Funktion zur integrierten Paketerfassung (Onboard Packet Capture, OPC) von Catalyst Switches der Serien 1200 und 1300 mit der Firmware-Version 4.1.3.36 vorgestellt. In dieser Firmware kann der OPC nur über die Kommandozeile konfiguriert werden.

Unterstützte Geräte | Software-Version

- Catalyst Switches der Serie 1200 | 4.1.3.36
- Catalyst Switches der Serie 1300 | 4.1.3.36

Einleitung

In der Firmware-Version 4.1.3.36 der Catalyst Switches der Serien 1200 und 1300 wurde eine neue Funktion eingeführt, die als Onboard Packet Feature (OPC) bezeichnet wird. Wenn diese Funktion aktiviert ist, reserviert der OPC bis zu 20 MB Speicher für die Paketerfassung. Diese Funktion erfordert die Konfiguration eines Erfassungspunkts, der das Verhalten einer OPC-Instanz definiert. Über den Capture Point werden alle Einstellungen definiert, die einer OPC-Instanz zugeordnet sind. Die OPC-Funktion erweitert die Fehlerbehebungsfunktionen auf dem Gerät.

In dieser Firmware kann OPC nur über die CLI konfiguriert werden. Erfassungspunkte werden im privilegierten EXEC-Modus konfiguriert und können weder in den Konfigurationsdateien des Switches gespeichert werden, noch werden die Einstellungen nach einem Neustart des Switches gespeichert.

Es können maximal vier Erfassungspunkte auf einem Switch konfiguriert werden. Es kann jedoch jeweils nur ein Erfassungspunkt aktiv sein. Die Paketerfassung wird für die Steuerungsebene (CPU) unterstützt. Die im Speicher gespeicherten Daten können entweder im integrierten Flash-Speicher (sofern freier Speicherplatz verfügbar ist) oder auf einem angeschlossenen USB-Gerät (z. B. einem USB-Flash-Laufwerk) gespeichert werden. Da der OPC erhebliche CPU-Ressourcen beanspruchen kann, wird empfohlen, ihn nur nach Bedarf zu verwenden.

Inhalt

Befehle zum Konfigurieren von Erfassungspunkten

Schritt 1

Ein Erfassungspunkt kann mit dem Befehl monitor capture {capture-name} erstellt werden.

```
monitor capture cap1
```

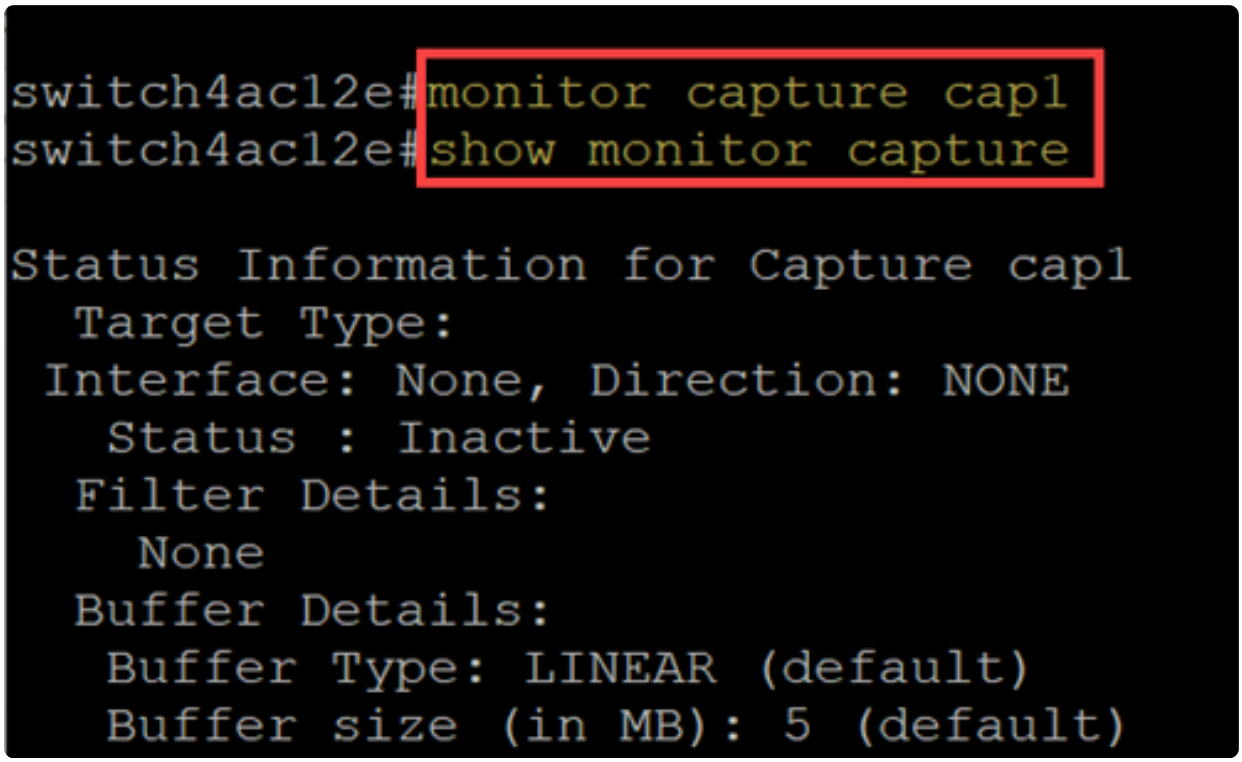
Im obigen Beispiel wurde ein Erfassungspunkt mit dem Namen cap1 erstellt.

Schritt 2

Um die Details eines konfigurierten Erfassungspunkts anzuzeigen, geben Sie den Befehl show monitor capture {capture-name} ein.

```
show monitor capture cap1
```

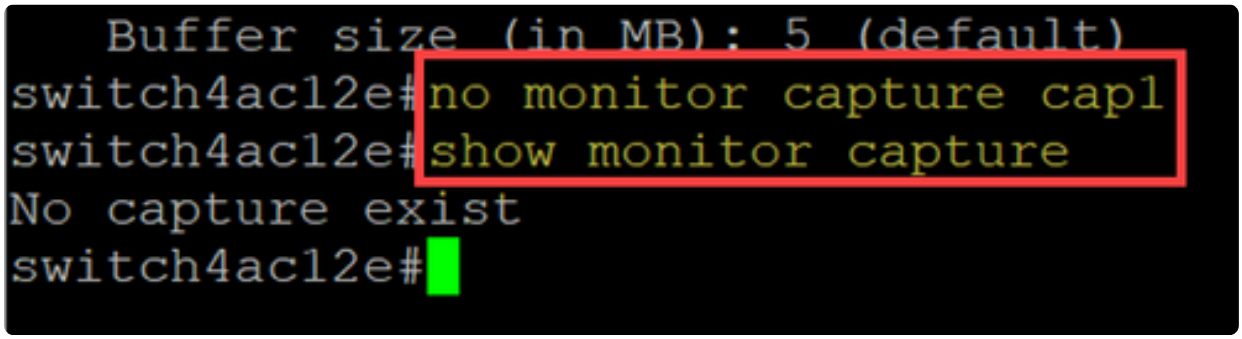
> **Note:**
> Sie können alle aktuell konfigurierten Erfassungspunkte anzeigen, indem Sie den Befehl show monitor capture verwenden, ohne einen Erfassungsnamen anzugeben.



Schritt 3

Um einen Erfassungspunkt zu löschen, verwenden Sie den Befehl no monitor capture {capture-name}.

```
no monitor capture cap1
```



Puffereinstellungen

Sie können die in einem Erfassungspunkt verwendeten Puffereinstellungen anpassen, insbesondere die Größe des Puffers und den Puffermodus.

- Die Mindestgröße des Puffers beträgt 1 MB, die Höchstgröße 20 MB.
- Wenn keine Puffergröße angegeben wird, wird eine Standardgröße von 5 MB verwendet.

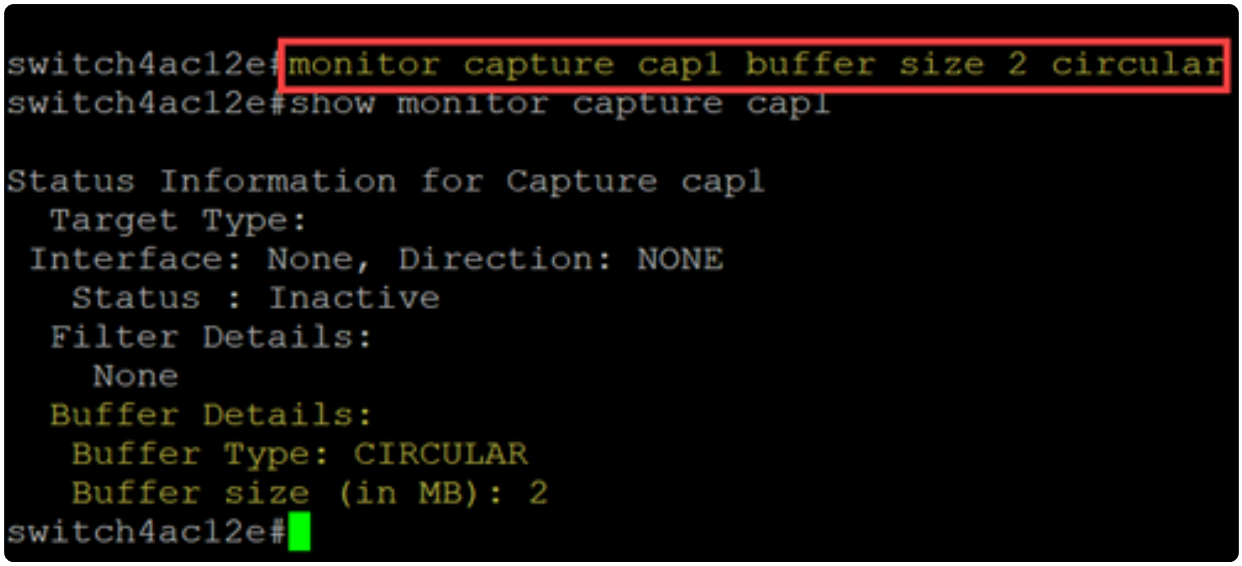
- Es können maximal 20 MB Speicher für alle Erfassungspunkte zugewiesen werden. Sie können einen einzelnen Erfassungspunkt mit 20 MB haben, aber nicht vier Erfassungspunkte mit jeweils 20 MB. Die insgesamt 20 MB werden auf alle konfigurierten Erfassungspunkte verteilt.
- Es gibt zwei Puffermodi: linear und kreisförmig.
- Der Standardmodus ist der lineare Modus. Im linearen Modus erfasst eine aktive Paketerfassung Daten, bis der konfigurierte Puffer voll ist. Anschließend wird die Erfassung beendet. Außerdem können Sie eine Paketerfassung nicht neu starten, wenn Sie die lineare Protokollierung verwenden und der Puffer bereits voll ist. In diesem Fall müssen Sie zuerst den Puffer löschen.
- Im zirkulären Puffermodus werden die zuvor mit FIFO (First In First Out) erfassten Daten überschrieben, sobald der Puffer voll ist. Eine Erfassung im zirkulären Puffermodus muss manuell angehalten werden.

Schritt 1

Der Befehl zum manuellen Konfigurieren der Puffereinstellungen lautet monitor capture {capture-name} buffer {circle [Größe Puffergröße] | size buffer-size}.

```
monitor capture cap1 buffer size 2 circular
```

In diesem Beispiel ist eine Puffergröße von 2 MB für den Capture-Punkt cap1 konfiguriert, und der Puffermodus ist kreisförmig.



Schritt 2

Mit dem Befehl no monitor capture {capture-name} buffer {circle [Größe Puffergröße] | size buffer-size} ändert den Puffermodus zurück in den linearen Standardmodus.

```
no monitor capture cap1 buffer size 2 circular
```

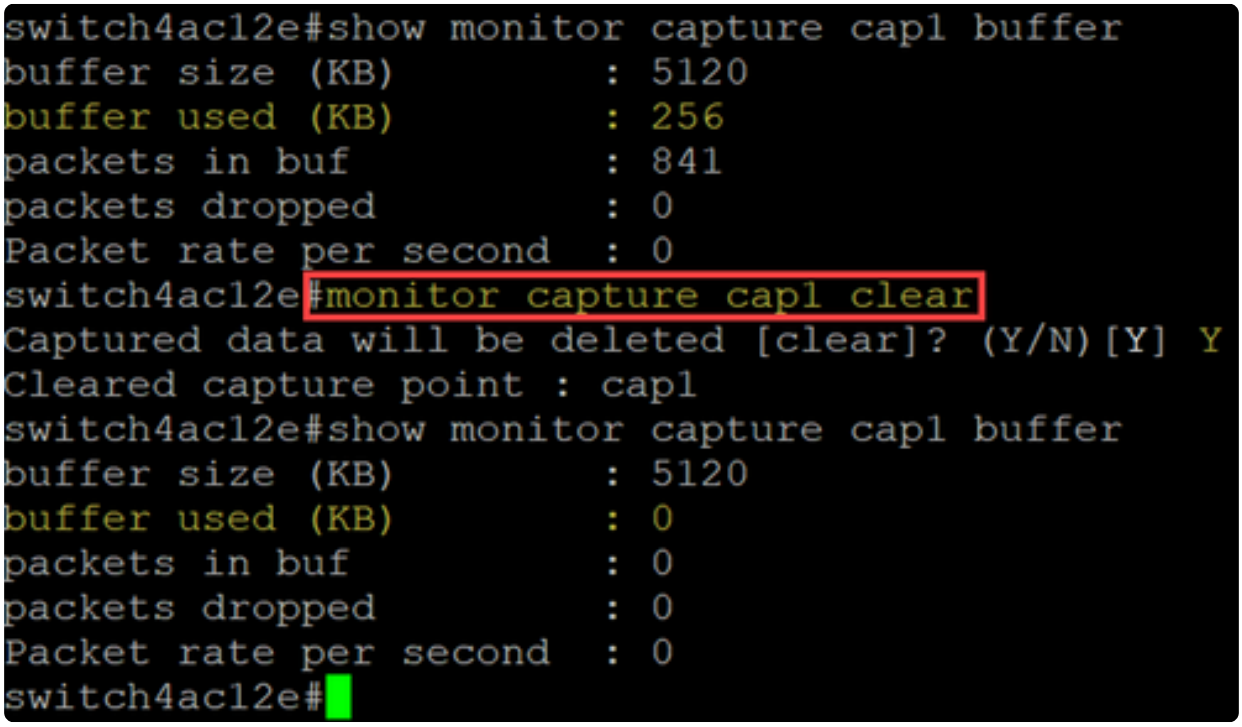
> **Note:**
> Wenn Sie den Befehl "no" ohne die [zirkular] und [size] Optionen verwenden, werden der Puffermodus und die Größe auf die Standardeinstellung eingestellt, die der lineare Modus und die Puffergröße von 5 MB ist.

Schritt 3

Um einen Puffer zu leeren, verwenden Sie den Befehl monitor capture {capture-name} clear.

```
monitor capture cap1 clear
```

In diesem Beispiel verwendete der Puffer in cap1 256 KB. Nach der Ausgabe des Befehls clear befindet sich der Puffer nun bei 0 KB.



Einstellungen für die Quellschnittstelle

Nachdem ein Erfassungspunkt erstellt wurde, muss die Quellschnittstelle für die Erfassung festgelegt werden. Die Einstellung der Quellschnittstelle ist erforderlich, um eine Erfassung zu starten.

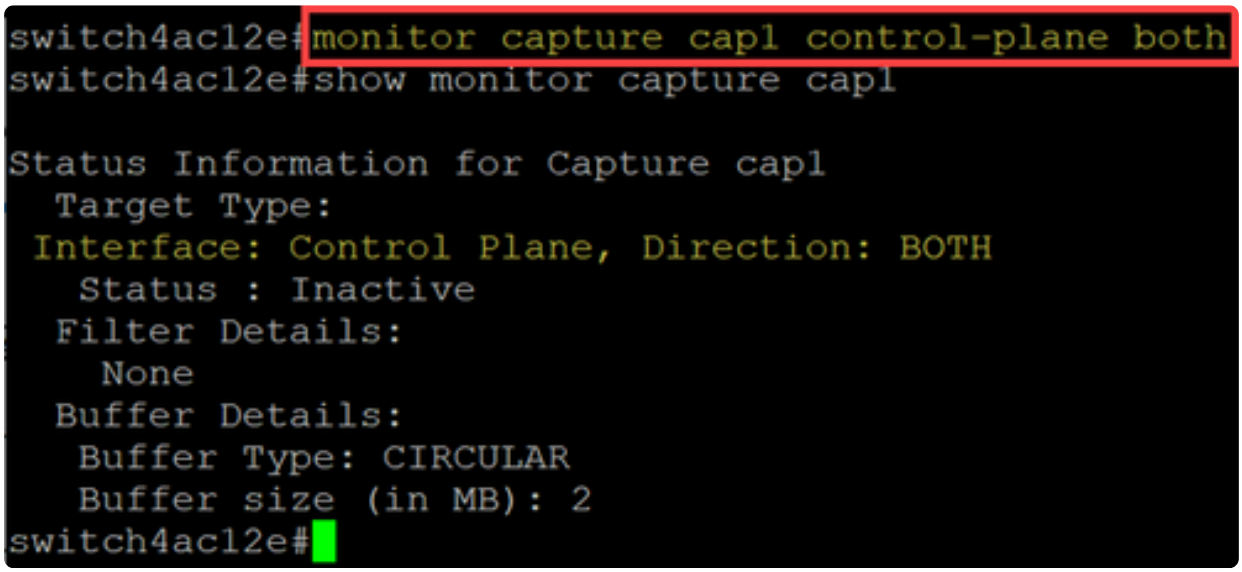
- Derzeit wird nur die Kontrollebene als Quelltyp unterstützt.

- Wählen Sie zum Festlegen der Richtung eine der folgenden Optionen aus: in (Ein), out (Aus) oder Both (Beide).
- Ein - Erfasst eingehende Pakete am Switch.
- Out - Erfasst ausgehende Pakete vom Switch.
- Beide - erfasst ein- und ausgehende Pakete.

Schritt 1

Verwenden Sie den Befehl monitor capture {capture-name} control-plane {in | Ausgang | beide}, um die Quellschnittstelleneinstellung zu konfigurieren.

```
monitor capture cap1 control-plane both
```



Schritt 2

Verwenden Sie die Kontrollebene "Kein Monitor, {Erfassungsname}" {in | Ausgang | beide} Befehl, um die Quellschnittstelleneinstellung zu entfernen.

```
no monitor capture cap1 control-plane both
```

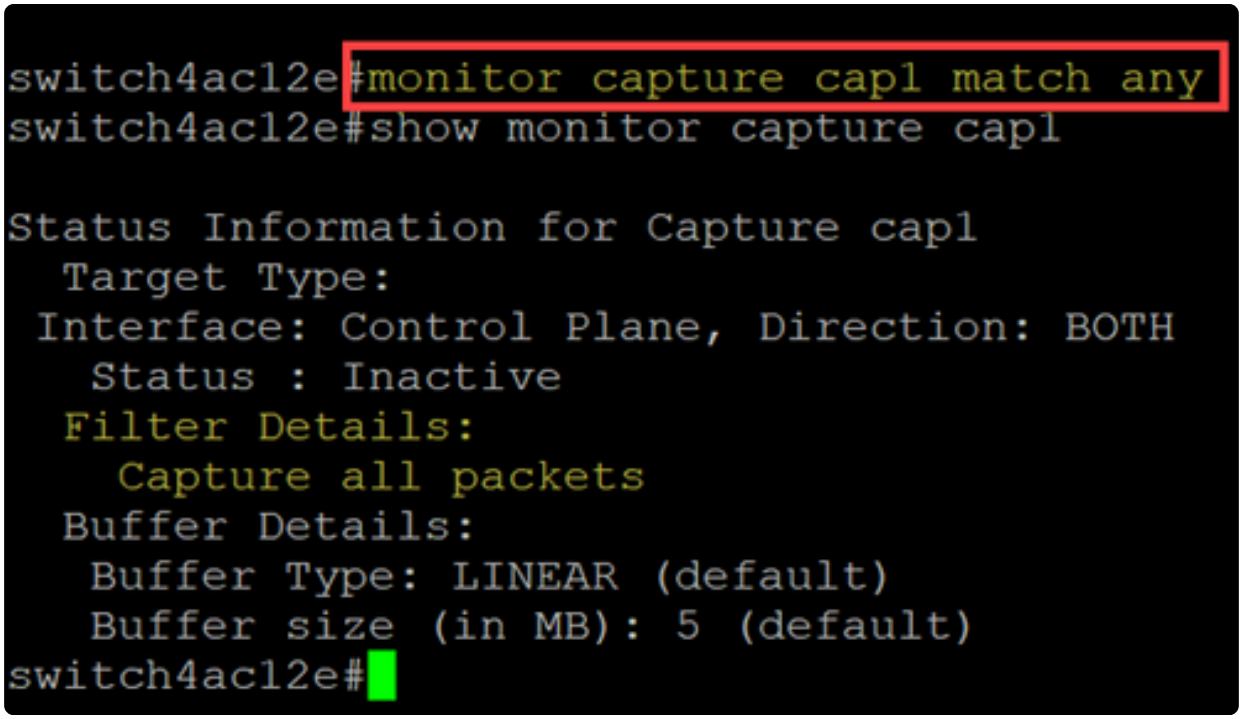
Einstellungen für Erfassungsfilter

Der Erfassungsfilter ist eine obligatorische Einstellung, die für die Paketerfassung konfiguriert werden muss. Derzeit wird der Filterbetrieb in der Firmware 4.1.3.36 nicht unterstützt. Alle Pakete an der Quellschnittstelle (die Steuerungsebene) werden erfasst. Sie müssen diesen Parameter jedoch weiterhin mit der "any"-Option konfigurieren.

Verwenden Sie den Befehl monitor capture {capture-name} match any, um die Einstellung des Erfassungsfilters zu konfigurieren.

```
monitor capture cap1 match any
```

In diesem Beispiel wurde der Erfassungspunkt "cap1" so konfiguriert, dass er mit allen Paketen übereinstimmt.



Starten und Beenden der Erfassung

Stellen Sie vor dem Starten einer Erfassung Folgendes sicher:

- Legen Sie die Quellschnittstelle und den Erfassungsfilter fest.
- Es wird empfohlen, die CPU-Auslastung vor dem Start zu überprüfen.

Es ist wichtig zu beachten, dass jeweils nur eine Aufzeichnungssitzung aktiv sein kann. Wenn eine Erfassung neu gestartet wird, nachdem sie beendet wurde, werden die neuen Pakete an den Puffer angehängt. Eine Erfassung kann jedoch nicht neu gestartet werden, wenn der Puffer voll ist und der Modus linear eingestellt ist.

Schritt 1

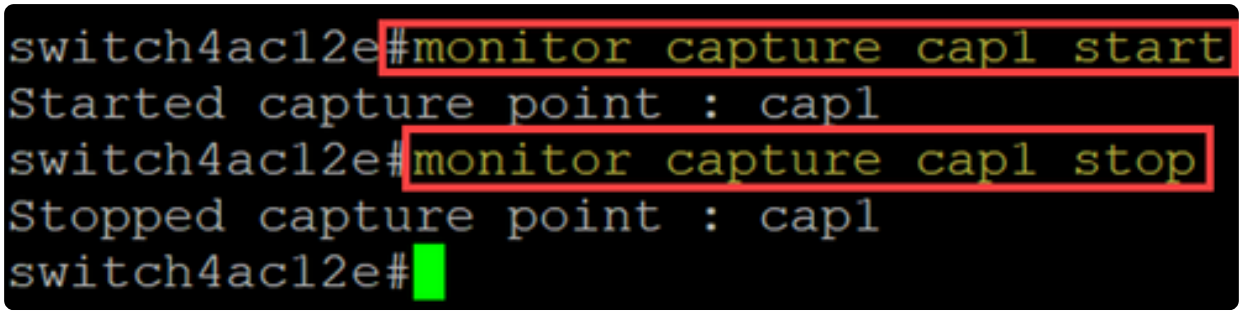
Verwenden Sie zum Starten der Erfassung den Befehl monitor capture {capture-name} start.

```
monitor capture cap1 start
```

Schritt 2

Um eine Erfassung zu stoppen, verwenden Sie den Befehl monitor capture {capture-name} stop.

```
monitor capture cap1 stop
```



Speichern der Paketerfassungsdaten

Nach Abschluss der Paketerfassung müssen die Daten im Puffer (dem RAM) gespeichert werden. Es gibt zwei Fälle, in denen die Daten gespeichert werden:

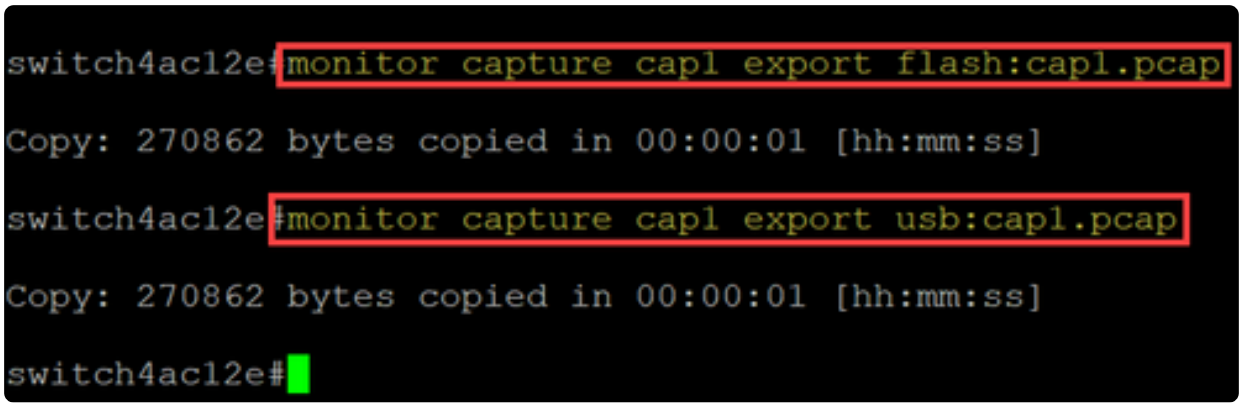
- Wird von einem Benutzer mithilfe eines CLI-Befehls ausgelöst
- Automatisch, wenn ein schwerwiegender Fehler auftritt.

Ein Benutzer kann die Paketerfassung entweder auf dem integrierten Flash-Speicher des Switches speichern, wenn dafür Platz vorhanden ist, oder auf einem angeschlossenen USB-Gerät, z. B. einem Flash-Laufwerk. Tritt bei der Paketerfassung ein schwerwiegender Fehler auf, werden die Daten automatisch im Hauptverzeichnis des Flash-Speichers gespeichert.

Um die Paketerfassung zu exportieren, verwenden Sie den Befehl zum Überwachen der Erfassung {capture-name} export {destination/filename}

```
monitor capture cap1 export flash: cap1.pcap
```

```
monitor capture cap1 export usb: cap1.pcap
```



Wenn eine Aufzeichnung im Flash-Speicher gespeichert wird, kann sie über den CLI-Befehl copy {filename} usb:/ auf ein USB-Flash-Laufwerk kopiert werden.

Die Switches C1200 und C1300 unterstützen USB-Laufwerke im FAT- und FAT32-Format. Wenn Sie kein FAT- oder FAT32-USB-Laufwerk haben, müssen Sie die Datei über TFTP vom Switch kopieren.

So kopieren Sie eine Datei des Switches über TFTP:

- Konfigurieren eines TFTP-Servers (mit TFTPD64 oder einem anderen Dienst)
- Verwenden Sie den folgenden Befehl aus der Switch-CLI: copy flash: {pcap file name} tftp://{tftp server ip}/{pcap file name}

Schlussfolgerung

Jetzt wissen Sie alles über die integrierte Paketerfassungsfunktion der Catalyst Switches der Serien 1200 und 1300 und die CLI-Befehle zum Konfigurieren der Einstellungen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.