

Troubleshoot Unexpected Reloads on Catalyst 9000 Switches

Contents

- [Introduction](#)
- [Requirements](#)
- [Components Used](#)
- [Background Information](#)
- [Common Reload Reasons](#)
- [Collect Relevant Data](#)
- [Last Reload Reason](#)
- [Onboard Logging](#)
- [Tech-Support Command](#)
- [Commands to Collect for TAC](#)
- [Tracelogs](#)
- [System Reports](#)
- [Cisco Bugs](#)
- [Related Information](#)

Introduction

This document describes how to troubleshoot unexpected reloads and what specific information to collect post-event on the Catalyst 9000 switches.

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

There can be a variety of reasons an unexpected reload or silent reload event can occur. To troubleshoot and find the root cause, it is imperative to know the date/time of the event and collect all the information possible from the device right away. This guarantees that all the log collection is accurate and complete (not overwritten by the device as time goes on).

Common Reload Reasons

ReloadReason	Explanation	Recommendation
PowerOn	The power supply or the inlet circuit was manually shut off and on.	If power event was unexpected, confirm health of physical power,

		battery backups, UPS, and so on.
Stack Merge due to Incompatibility	The Standby switch of the stack lost communication with the Active and triggered a merge to re-elect a new Active switch.	Check the stacking data cables, make sure they are properly seated. Replace the stacking cables.
Reload Command	The command <code>reload</code> was executed on the CLI of the switch to instruct a manual software reload.	None.
LocalSoft or CPU Catastrophic Err	An error condition encountered in the software or CPU and the device was forced to be reset.	Collect data and open a TAC case.
Power failure or Unknown	The power supply of the device or inlet circuit must have suddenly failed, momentarily stopping the supply of power to the switch.	Check if the power supplies are healthy, color of the LEDs and verify the inlet input circuit.
Redundancy force-switchover	The command <code>redundancy force-switchover</code> was executed, causing the Standby to take the Active role and previous Active to go for a software reset.	None.
Image Install	The device was reloaded as a result of a new Cisco IOS® XE image installation.	None.

Collect Relevant Data

- Exact date/time of the occurrence.
- What was happening prior to the unexpected reload event? Perhaps a configuration change, log in to the device, or the device was untouched.
- Are there any Syslog messages of errors reported prior to the event? If there are any external Syslog servers, check if there are error logs related.
- Collect the `show tech-support` command from the device.
- Any other insight or observations that can help understand what preceded the event (power failures, and so on)

Caution: It is really important to collect the information right after the event occurred. There are no guarantees of providing a proper root cause if log collection happens days or weeks after the reload event took place.

Once the device is up and stable, collect this additional information to help determine the cause of the reload event.

Last Reload Reason

Check what was the last Reload Reason recorded by the system.

```
<#root>
```

```
Switch#
```

```
show version | include uptime|returned|reload|Version
```

```
Cisco IOS XE Software, Version 16.12.08
```

```
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.12.8, RELEASE SOFTWARE
```

licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes GPL code under the terms of GPL Version 2.0. For more details, see the BOOTLDR: System Bootstrap, Version 17.10.1r, RELEASE SOFTWARE (P)
Switch uptime is 3 hours, 14 minutes
System returned to ROM by Reload Command

Last reload reason: Reload Command

Next reload AIR license Level: AIR DNA Advantage
Switch Ports Model SW Version SW Image Mode
Configuration register is 0x102 (will be 0x2102 at next reload)

Onboard Logging

The device stores historical data on the latests reload events experienced. This information is important to check if the reloads have been recurrent and what was the reason recorded by the switch. The command used to see this data is `show logging onboard switch <id> uptime detail`.

<#root>

Switch#

show logging onboard switch active uptime detail

UPTIME SUMMARY INFORMATION

First customer power on : 04/28/2022 01:24:40
Total uptime : 0 years 41 weeks 2 days 9 hours 55 minutes
Total downtime : 0 years 22 weeks 4 days 7 hours 3 minutes
Number of resets : 326
Number of slot changes : 2
Current reset reason : Reload Command
Current reset timestamp : 07/19/2023 15:23:33
Current slot : 1
Chassis type : 215
Current uptime : 0 years 0 weeks 0 days 3 hours 0 minutes

UPTIME CONTINUOUS INFORMATION

Time Stamp | Reset | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours minutes

07/13/2023 17:57:49	Image Install	0	0	0	0	0
07/13/2023 18:48:58	Reload Command	0	0	0	0	40
07/14/2023 00:55:30	Reload Command	0	0	0	6	0
07/14/2023 11:15:44	Reload Command	0	0	0	10	0
07/14/2023 20:02:26	Reload Command	0	0	0	8	0
07/17/2023 11:32:29	Reload Command	0	0	2	15	0
07/17/2023 21:00:59	Reload Command	0	0	0	9	0
07/18/2023 08:36:20	Reload Command	0	0	0	11	0
07/18/2023 11:00:28	Reload Command	0	0	0	2	0
07/19/2023 07:02:14	Reload Command	0	0	0	19	0
07/19/2023 15:23:33	Reload Command	0	0	0	8	0

Tech-Support Command

This command gathers general information of the system and its current status. The commands described previously are included in this support package. This output file is requested by TAC when opening a case.

There are different ways to collect it:

- **Logged Terminal Session:** Use a terminal program and record the session to a text file. Then, from CLI, run the command `show tech-support` and wait for the collection to finish. Provide the text file to the TAC case.
- **Redirected to a File:** From the CLI, run the command `show tech-support | redirect flash: ShowTech.txt`. This creates a text file on the flash of the device with the results of the tech-support command. Afterwards, need to extract the file from the device using any transfer protocol available in your network. (TFTP, FTP, SCP, and so on).

```
<#root>
```

```
Switch#
```

```
show tech-support | redirect flash:ShowTech.txt
```

```
Switch#
```

```
dir flash: | include .txt
```

```
499721 -rw- 16090 Jul 19 2023 15:24:02 +00:00 rdope_out.txt
499728 -rw- 1328023 Jul 19 2023 19:12:57 +00:00 ShowTech.txt
```

```
Switch#
```

```
copy flash:ShowTech.txt tftp:
```

```
Address or name of remote host []? 192.168.1.1
```

```
Destination filename [ShowTech.txt]?
```

```
!!!
```

Commands to Collect for TAC

The switch stores system logging information that can be used to analyze in depth what was happening prior and after the unexpected reload event occurred. If there was a crash, the switch also stores the crash data into an encrypted file that can be analyzed by TAC experts.

Tracelogs

The tracelogs are internal logs of each process within Cisco IOS® XE. The tracelogs directory is created by default and its content is overwritten periodically. This folder can be found in the `bootflash` or `flash` of the Catalyst device.

Generate the Tracelogs

<#root>

Switch#

```
request platform software trace archive
```

Creating archive file [flash:Switch_1_RP_0_trace_archive-20230719-192115.tar.gz]

Done with creation of the archive file: [flash:Switch_1_RP_0_trace_archive-20230719-192115.tar.gz]

Switch#

```
dir flash: | include .gz
```

```
499729 -rw- 29573907 Jul 19 2023 19:21:22 +00:00
```

```
Switch_1_RP_0_trace_archive-20230719-192115.tar.gz
```

System Reports

A system report is a compressed file that collects most of the information available in the software execution when an unexpected reload occurs. The system report contains tracelogs, crashinfo, and core files. This file is automatically created in the case of an unexpected reload on Cisco IOS® XE switches that was caused by a crash or software error. The file can be found in the `crashinfo` directory. This file is encrypted and requires TAC support for decoding and analysis.

<#root>

Switch#

```
dir crashinfo: | include .gz
```

Directory of crashinfo:/

```
19 -rwx 655080 Aug 7 2013 16:31:31 +00:00
```

```
system-report_1_20130807-163050-UTC.gz
```

Note: These files ending in `.gz` extension need to be extracted out of the device using any transfer protocol available in your network. (TFTP, FTP, SCP, and so on).

Cisco Bugs

There are some of the defects that can cause an unexpected reload on Catalyst 9000 Series switches.

Note: Only registered Cisco users can access internal bug information.

Cisco bug ID CSCvp56289	9300 switch silent reload with platinum power supply (PWR-C1-350WAC-P)
Cisco bug ID CSCvv27849	Cat 9K & 3K: Unexpected reload caused by the FED process.
Cisco bug ID CSCvr77861	Cat9300/C9500/C9500H switches may reload with last reload reason as LocalSoft or CpuCatastrophicErr
Cisco bug ID CSCvu97189	Show platform forward (SPF) causes device freeze or reload

Cisco bug ID CSCwe11818	C9300L stack merge happen after switchover
--	--

Related Information

- [Cisco Technical Support & Downloads](#)