Outputs to collect in the event of crash or unexpected reload

Contents

Introduction

This document is a guide on important checks & useful outputs which should be collected in the event of crash or unexpected reboot from Cisco enterprise products. The information in this document is not meant to be exhaustive & is intended to serve as a general guide to customers especially when they are planning to open a service request with Cisco TAC.

Catalyst 9000 Series Switches

Basic Checks

- When did the reload/crash happen?
- Did the switch recover automatically after the crash?

Outputs to be collected

- show tech-support diagnostic

  Note: show tech-support output can be large and it is recommended to redirect the output to a file on flash.

```
Switch# show tech-support | redirect flash:filename
```

- **dir all**

- Any ***system report/archive*** file from flash/crashinfo directory created at the time of reload/crash.
- **request platform software archive** - This command creates an archive file on the flash memory of active switch/supervisor.
- **request platform software trace slot RP standby archive** - Run this command in case of Catalyst 9400/Catalyst 9600 high availability setup to collect Btrace from standby supervisor. This is a hidden command, configure service internal to run it. This command will create an archive file on the flash memory of the standby supervisor.
- **request platform software trace slot switch standby RP archive** - Run this command in case of Catalyst 9400 SVL setup to collect Btrace from standby supervisor. This command will create an archive file on the flash memory of the standby supervisor.

Catalyst 9800 Series Wireless LAN Controllers

Collect crashes/coredumps system-reports/AP crashes. This can be done via GUI: Navigate to Troubleshooting > CoreDump and System Report

or via CLI:

```
# more bootflash:system-report*
# copy bootflash:system-report-YYYYMMDD-HHMMSS-Timezone.tar.gz {tftp: | ftp: | https: ..}
```

OR

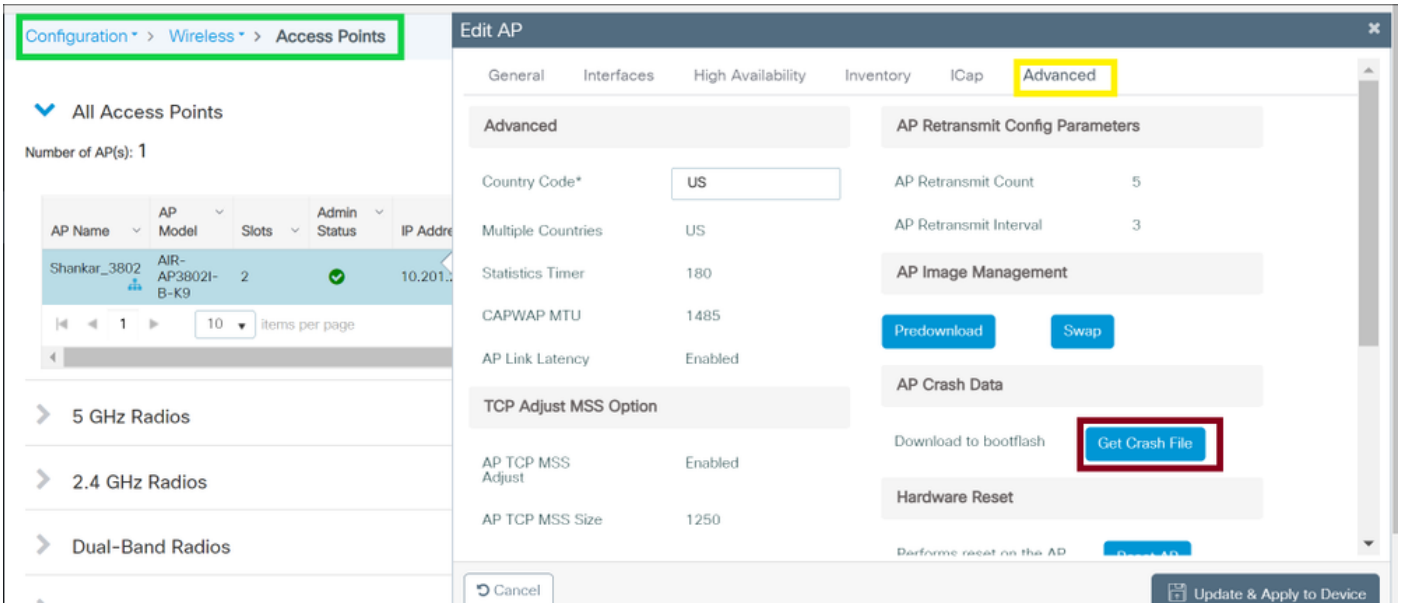
```
# more harddisk:system-report*
# copy harddisk:system-report-YYYYMMDD-HHMMSS-Timezone.tar.gz {tftp: | ftp: | https: ..}
```

Additional outputs to be collected -

```
show proc cpu platform sorted 1min
show proc mem platform accounting
show redundancy switchover history
show redundancy history
```

AP Crashes from Cat 9800 GUI:

For any AP crashes, collect the AP crash files from WLC GUI>>Configuration>>Wireless>Access Points>> Click on relevant AP >> Advanced tab



Wireless LAN Controllers running Cisco AireOS

Uploading Logs and Crash Files (GUI)

Step 1 Choose Command > Upload File. The Upload File from the Controller page appears.

Step 2 From the File Type drop-down list, choose one at a time:

Event Log

Message Log

Trap Log

Crash File

Step 3 From the Transfer Mode drop-down list, choose from the following options:

TFTP

FTP

SFTP (available in the 7.4 and later releases)

Step 4 In the IP Address text box, enter the IP address of the server.

Step 5 In the File Path text box, enter the directory path of the log or crash file.

Step 6 In the File Name text box, enter the name of the log or crash file.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

In the Server Login Username text box, enter the FTP server login name.

In the Server Login Password text box, enter the FTP server login password.

In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click Upload to upload the log or crash file from the controller. A message appears indicating the status of the upload. Repeat Step 2 for collecting the rest of the logs.

Uploading Logs and Crash Files (CLI)

Step 1 To transfer the file from the controller to a server, enter this command:

```
transfer upload mode {tftp | ftp | sftp}
```

Step 2 To specify the type of file to be uploaded, enter this command:

```
transfer upload mode datatype <datatype>
```

where datatype is one of the following options:

crashfile—Uploads the system's crash file.

errorlog—Uploads the system's error log.

panic-crash-file—Uploads the kernel panic information if a kernel panic occurs.

systemtrace—Uploads the system's trace file.

traplog—Uploads the system's trap log.

watchdog-crash-file—Uploads the console dump resulting from a software-watchdog-initiated reboot of the controller following a crash. The software watchdog module periodically checks the integrity of the internal software and makes sure that the system does not stay in an inconsistent or nonoperational state for a long period of time.

Step 3 To specify the path to the file, enter these commands:

```
transfer upload serverip server_ip_address
transfer upload path server_path_to_file
transfer upload filename filename
```

Step 4 If you are using an FTP server, also enter these commands:

```
transfer upload username username
transfer upload password password
transfer upload port port
```

Note: The default value for the port parameter is 21.

Step 5 To see the updated settings, enter this command:

```
transfer upload start
```

Step 6 When prompted to confirm the current settings and start the software upload, answer y.

Uploading Core Dumps from Controller to a Server (CLI)

Step 1 To see information about the core dump file in flash memory, enter this command:

```
show coredump summary
```

Information similar to the following appears:

```
Core Dump is enabled
Core Dump file is saved on flash
Sw Version..................................... 6.0.83.0
Time Stamp..................................... Wed Feb  4 13:23:11 2009
File Size...................................... 9081788
File Name Suffix............................... filename.gz
```

Step 2 To transfer the file from the controller to a server, enter these commands:

```
transfer upload mode {tftp | ftp | sftp}
transfer upload datatype coredump
transfer upload serverip server_ip_address
transfer upload path server_path_to_file
transfer upload filename filename
```

> **Note**: After the file is uploaded, it ends with a .gz suffix. If desired, you can upload the same core dump file multiple times with different names to different servers.

Step 3 If you are using an FTP server, also enter these commands:

```
transfer upload username username
transfer upload password password
transfer upload port port
```

> **Note**: The default value for the port parameter is 21.

Step 4 To view the updated settings, enter this command:

```
transfer upload start
```

Step 5 When prompted to confirm the current settings and start the software upload, answer y.

AP Crashes from AireOS GUI:

From WLC GUI>>Management>>Tech Support>>AP Crash Log

AP-IOS Crash

AP-IOS refers to the legacy OS in Cisco AP's. (Example: Access Points 1700/2700/3700/1600/2600/3600 series).

via CLI:

```
terminal length 0
more flash:/crashinfo-*

Find the relevant crash files using timestamp
copy ftp/tftp command to transfer crash file
```

AP-COS Crash

AP-COS refers to the latest OS in Cisco AP's. (Example: Access Points 91XX/3800/2800/1800 series).

via CLI:

```
show flash crash
show flash syslogs
```

- Find the files that match the timestamp of the crash
- More to the terminal log file, or copy the crash file listed using
  `copy sysylog <filnename>tftp:|scp: tftp|scp://x.x.x.x/`
  `(ex. copy syslogs 14.crash_log tftp: 1.2.3.4 )`
  As the URL should be in format A.B.C.D[/dir]/filename.
- Collect all files that match the event ID for good measure

Corefile

- Corefiles can only be seen and collected from the AP CLI (or WLC CLI using 'AP' commands)

```
show flash core
```

> **Note**: Corefiles are compressed into tar GZ files (.tgz). These can be uncompressed using Winzip and will contain a 'show tech' as well as copies of other logs.

- Copy the corefiles using TFTP or SCP

```
copy cores <filename> tftp:|scp X.X.X.X
```