Release Note for Cisco Catalyst 1200 and 1300 Series Switches Firmware Version 4.0.0.93

First Published: 2023-10-10

Introduction

Release 4.0.0.93 supports the following product series:

- Catalyst 1200 Smart Switch Series
- Catalyst 1300 Managed Switch Series
- Catalyst 1300 Stackable Managed Switch Series

This release (4.0.0.93) is a maintenance release fixing bugs found in version 4.0.0.91. It does not add any new additional features to release 4.0.0.91.

This version includes an important fix. Therefore, it is highly recommend to upgrade a device running an earlier version to version 4.0.0.93.

Downgrade from version 4.0.0.93 to previous versions is blocked.

Due to the downgrade prevention implemented in version 4.0.0.93, both active and inactive images are upgraded when upgrading from a prior version.

Caution Due to downgrade prevention applied to version 4.0.0.93 - adding a unit running version 4.0.0.93 to a stack running an earlier version will cause the new unit to shutdown due to version incompatibility.

To resolve this issue, disconnect the unit running 4.0.0.93 from the stack and reload it. Next, upgrade the existing stack to version 4.0.0.93, and then add the new unit to the stack.

Therefore, before adding a new unit, it is advised to upgrade the current stack to version 4.0.0.93 in order to prevent this behavior.

What's New in this Release

This section details new features and modifications in this release.

Release 4.0.0.93 does not support any additional features or functionalities above release 4.0.0.91 in any capacity.

Known Issues

Caveats Acknowledged in Release V4.0.0.93.

Bug ID	Description
CSCwh21119	**Symptom** MAC authentication fails when PVST command is added. **Workaround** Use STP mode other than PVST/RPVST.
CSCwh58899	**Symptom** C1200/1300 switches running firmware 4.0.0.93 may fail to boot up after performing "load golden image to factory reset" option on the Uboot "Basic Menu" (pressing **CTRL+Shift+6 key > Basic Menu > 1. load golden image to factory reset)**. **Note** The issue has little impact on users as the “Load golden image to factory reset” option is rarely used. To reset switch configuration to factory default, it can be set using the reset button or CLI or GUI or start up menu. Will be fixed in 4.1.0.x **Workaround** Contact Cisco support for assistance if the switch reaches this state after using “Load golden image to factory reset” option to reset the switch. **Recommended Action:** Avoid using the “Load golden image to factory reset” option to factory reset the switch while the switch is on firmware version 4.0.0.93.

Resolved Issues

Caveats Resolved in Release V4.0.0.93.

Bug ID	Description
CSCwh02042	**Symptom** With an extremely low probability (1/4096) the boot process may hang and the error message “hw error” will be printed to the console.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.0.0.91

August 2023

This Release Note describes the recommended practices and known issues that apply to software version 4.0.0.91 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications in this release.

Changes to Hardware Components

Reset Button Functionality

The reset button function has been updated as follows:

- System LED provides different flash indication for regular device reload and reset to factory default:
  - Regular device reload (the reset button is pressed and then released within 6-10 seconds) – the system LED will provide an indication of a slow flash.
  - Resetting device to factory default (the reset button is pressed and then released within 16-20 seconds) – the system LED will provide an indication of a rapid flash.
- Pressing the system LED and releasing within 1-2 seconds on SKUs that support PoE will provide the following indication:
  - On ports that are delivering power to connected PDs – the port LED will provide a solid amber indication for 5 seconds.
  - On ports that are not delivering power to connected PDs – the port LED will not provide any indication for 5 seconds (LED will be off).

Type-C USB Interface

The device supports a type-C USB Interface located on device front panel. This provides an additional console interface besides the RJ45 interface. The type-C USB based console has the following characteristics:

- The console is active only from OS init stage and on.
- When active, the Type C USB consoled had priority over the RJ45 console.
- The type-C USB console is agnostic to baud rate setting.

Trusted Platform Module (TPM) Support

All SKUs support a TPM component. The TPM provides hardware level protection and operation for security related features such as Chip guard and Boot Integrity Visibility. The device support TPM 2.0 specification.

Bluetooth Management Interface

The current version added support for a Bluetooth Management Interface – providing IP connectivity over Bluetooth. This device management over Bluetooth via telnet, SSH or HTTP/HTTPS GUI interface.

Support of Bluetooth is achieved by connecting a Bluetooth (BT) dongle, to the device USB port. The device will automatically detect the insertion of a supported BT dongle into device's USB port and provide Bluetooth host support. The device supports the following Bluetooth Dongles.

1. BTD-400 Bluetooth 4.0 Adapter by Kinivo
2. Bluetooth 4.0 USB Adapter by Asus
3. Bluetooth 4.0 USB Adapter by Insignia
4. Philips 4.0 Bluetooth adapter

5. Lenovo LX1815 Bluetooth 5.0 USB adapter
6. Lenovo LX1812 Bluetooth 4.0 USB adapter

Persistent PoE

The Persistent PoE feature (also referred to as Always-On PoE) minimizes the dependency of the PoE operation on the switch's status. Before the introduction of this feature, any disruption in the switch operation such as a software related reboot, would also cause a disruption in the PoE operation until the device finished coming back up. With the persistent PoE feature warm reboots such as the ones performed by the reload command will not disrupt the operation of the PoE in it's current state, allowing PDs connected to the switch to continue and operate.

Auto Surveillance VLAN (ASV)

Network communication between surveillance devices such as cameras and monitoring equipment should often be given higher priority and it is important that the various devices that comprise the surveillance infrastructure in the organization are reachable for each-other.

Normally, it falls to the network administrator to ensure that all surveillance devices are connected to the same VLAN and to setup this VLAN and the interfaces on it to allow for this high priority traffic.

The Auto Surveillance VLAN (ASV) feature automates aspects of this setup by detecting surveillance devices on the network, assigning them to a VLAN and setting their traffic priority.

MSTP Enhancements

The following MSTP related enhancements were added to this release:

- Catalyst 1300 product line supports 16 instances.
- MSTP instance ID can be in the range of 0-4094.

To allow support the range of 0-4094 for MSTP instance ID the user is required to create an MSTP instance– and assign it an instance ID. Once Instance ID is created the user can map VLANs to the created instances (in previous releases there was no need to create the instance prior to mapping VLANs to the instance.

Password Aging Enhancements

Password aging allows the administrator to force a change of a password after a predefined period. The current version added the following enhancements:

- Only a level 15 user can change passwords. A Level 1 user is presented with notice on (expected) password expiration but does not have the privilege to change the password.
- Expiration period (10 days prior to password expiration) – Upon login the (level 15) user will be presented with the option to change the password. The user can refuse the option – in which case login will be provide, or accept suggestion, in which case they will be able to change the password immediately (in previous version user would need to log in and then enter relevant configuration mode).

Attestation Certificate and Key-pair (AIK) Support

The certificate and key pair are used to validate various device information as well as signing the output of commands displaying security related information (for example Chip Guard and Boot integrity Visibility).

The current version added support for an additional certificate and key pair. This is the Attestation certificate and key pair (also known as AIK - Attestation Identity Key). The attestation certificate and keys are considered more secure than the SUDI certificate and keys, as operation using the AIK certificate is confined within the TPM. this provides a higher confidence in the validity of signed information.

Boot Integrity Visibility (BIV)

Boot integrity Visibility (BIV) feature allows a platform's software integrity information to be visible and actionable. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted and is running a trusted code. BIV on the Catalyst 1200 and 1300 product line utilizes the functionalities of the TPM component.

During the boot process, the software creates a hash record of the different images involved in the boot stages. To ensure integrity of the measurements, the measurements are stored in a hardware protected component called TPM and extended into PCRs (Platform Configuration Register). The user can then retrieve these records (via CLI commands) and compare it with Known Good Values (KGV) records maintained by Cisco. If the values do not match, the device may be running a software image that is either not certified by Cisco or has been altered by an unauthorized party.

The CLI commands allow to display the hash measurements and PCR quote for the bootloader and entire image. Optionally this information can also be signed using SUDI or attestation Keys.

Note The BIV feature works without user intervention or accepting any changes out of the box, but if end-user requires confirmation of this, an option will be provided soon to help users.

Chip Guard Enhancements

The current version added the following enhancements:

- Support of CLI command to display Chip guard information.
- Support of attestation certificate and keys for signing command output.

Random Token for Debug Access

- Certain debug interfaces (for example Linux shell) are sensitive or may cause disruption to device operation, and therefore require elevated access control and verification.
- The current version supports the enhanced requirement by generating a random challenge upon each attempt to access such debug interfaces, followed by a prompt to provide a password based on the challenge.
- In order to access the interface the challenge needs to be signed by a dedicated key managed by Cisco.

Dying Gasp

The Dying Gasp feature provides a mechanism to alert monitoring systems that a device is experiencing an unexpected loss of power due to HW failure (disconnection or disruption of power source).

When a loss of power event occurs, a hardware capacitor will delay the device shutting down for a short time. During this time, the device will send Dying Gasp messages. The messages can be sent to SNMP servers (as notification) or to syslog servers.

This feature is supported only on the 1300 product lines (standalone and stacking). It is not supported on the 1200 product line.

Golden Image Support

- The current version added Golden Image support.
- The Golden Image is a production level image, and as such underwent extensive testing cycles.

- In case the current software is corrupted and will not load – the device will automatically load the Golden Image as a fallback image. This may prevent the need to RMA such a unit. Loading the golden image may result in erase of device configuration.
- The Golden Image is burned to device flash as part of the manufacturing process. The user does not have an option update the Golden Image version. In some cases (for example secure boot key revocation) the Golden Image will be updated as part of the regular image update.

CLI Command to Reset Device to Factory Defaults

CLI commands provide the ability to not only reboot the switch but to also reset the switch back to factory defaults. For more information, please refer to the CLI Guide for detailed commends in the standalone and stackable switches.

SSL and SSH Support

The following changes were introduced in the current release:

- TLS 1.2 secure client-initiated renegotiation is disabled.
- Supported OpenSSL version – 1.1.1q
- Supported OpenSSH version - Version 7.3p1 (no change to previous version)

Known Issues

Caveats Acknowledged in Release V4.0.0.91.

Bug ID	Description
CSCwe81236	**Symptom** Error message is displayed when configuring command “"no ipv6 nd hop-limit " – and configuration is not accepted. **Workaround** Disabled IPv6 on interface.
CSCwe81238	**Symptom** Auto surveillance vlan (ASV) will not be active on general mode port if STP mode is set to PVST/RPVST. **Workaround** To activate ASV on the interface either disable and then re-enable the ASV VLAN or change STP mode to STP/RSTP and then change back to PVST/RPVST.
CSCwe81247	**Symptom** When a port is set to class mode, the PoE Class display in the GUI (**Port Management > PoE > Setting**) is wrong for a class 0 PD. **Workaround** Check class info via the CLI.

Bug ID	Description
CSCwe81251	**Symptom** Welcome Banner (configured via the GUI) will be erased if the user configures via the CLI with a login banner with more than 512 characters in a single line **Workaround** None
CSCwe81253	**Symptom** When the authentication or login default method list is updated, the Syslog messages are duplicated. **Workaround** None
CSCwe81254	**Symptom** An error message will appear on the console if the DHCP pool name includes special characters (for example single quote, double quote, backslash) and the user clicks the "**Details**" button in **IPv4 Configuration> DHCP Server>Network Pools** GUI page. **Workaround** There is no functionality effect and workaround.
CSCwe84307	**Symptom** C1200/C1300 - PoE port fault status when non PoE device connected **Workaround** Disable the port PoE by applying **power inline never** command to the PoE interface.
CSCwf56969	**Symptom** C1200 C1300 - PoE issue with DBS-210 **Workaround** No workaround
CSCwe81260	**Symptom** Pre-standard PD cannot exit power denied state caused by POE budget shortage. **Workaround** Disable then enable the POE on the problem port.
CSCwe81261	**Symptom** Sometimes the POE ports cannot recover from overload state even after a decrease of the load to normal. **Workaround** Disable then enable the POE on the problem port.