Release Note for Cisco Catalyst 1200 and 1300 Series Switches Firmware Version 4.0.0.91 - 4.1.4.1

First Published: 2024-09-11

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.4.1

September 2024

This Release Note describes the recommended practices and known issues that apply to software version 4.1.4.1 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications added to Version 4.1.4.1 compared to previous releases.

Password Complexity - Keyboard Pattern Prevention

- A new password complexity setting called Keyboard pattern prevention was added in this version.
- When enabled, the password configured by the user can’t include more than three consecutive letters or numbers keys on the QWERTY keyboard.
- This feature can be enabled or disabled using the “passwords complexity keyboard-pattern” CLI command. By default, this feature is disabled. In the current version there isn’t GUI control for this setting.
- The feature applies to the passwords configured via one of the following commands “username” (Global Configuration mode command) “enable password” (Global Configuration mode command) and “password” (Line Configuration mode command).

Masked Secret

- From this version and on the user has the option to type in a password as a masked secret, instead of a cleartext password. The masked secret is provided by the user following a prompt displayed on the screen. The masked password needs to be confirmed by the user, as follows:

  ```
  switch(config)#username example privilege 15 masked-secret

  Enter secret: ********

  secret: ******** Confirm secret: ********
  ```

- This ability was added to the following commands “username” (Global Configuration mode command) and “enable password” (Global Configuration mode command).

- The command including the password is saved to the configuration in the same format as a command entered in cleartext.

Security Syslog

Security-related messages were enhanced to include the following:

- The syslog messages which indicate firmware upgrade success or failure, includes the following information:
    - The management interface from which the firmware operation was initiated (Console, telnet, SSH, HTTP, or HTTPS).
    - The username of the management session that initiated the firmware operation.
    - The IP address of the management session that initiated the firmware operation.
- A syslog message, which includes the information detailed in the previous item, is generated when one of the following management interfaces are enabled or disabled: SSH; Telnet; HTTP/HTTPS or SNMP.

Log File Exceed Threshold

- In this version the user can configure an alarm threshold for the logging file (file messages stored to the flash).
- Once this threshold is exceeded a syslog message is generated indicating the threshold has been crossed.
- The command to set this threshold is “logging file threshold percent” where percent is a number 1–99. By default, a threshold isn’t defined - which means the syslog message won’t be generated.

Release Notes for Cisco Catalyst 1200 and 1300 Series Switches - Firmware Version 4.1.3.36

June 2024

This Release Note describes the recommended practices and known issues that apply to software version 4.1.3.36 for the Cisco Catalyst 1200 and 1300 Series Switches.

What's New

This section details new features and modifications added to Version 4.1.3.36 compared to previous releases.

Radius Change of Authorization (CoA)

Supported on the C1300 standalone and C1300 stack families.

Radius Change of Authorization (CoA) is an extension to the RADIUS protocol, allowing dynamic changes to an AAA or dot1x user session. This includes support for disconnecting users and changing authorizations applicable to a user session. The device acts as a CoA server receiving Change of Authorization (CoA) and Packet of Disconnection requests from a CoA client. CoA is supported for 802.1x sessions. the following CoA commands are supported

- “disable host port” command - included in a Cisco VSA “Cisco:Avpair=“subscriber:command=disable-host-port”
- “Bounce host port” command - included in a Cisco VSA “subscriber:command=bounce-host-port”
- “Reauthenticate host” Command - included in a Cisco VSA “Cisco:Avpair=“subscriber:command=reauthenticate”

Audit-Session-ID

Supported on the C1300 standalone and the C1300 stack families.

The Cisco Vendor Specific Audit-Session-ID RADIUS attribute is used to uniquely identify a user session. The device will include this attribute in all messages sent to the RADIUS server. The same Audit-Session-ID will be used for all authentication, authorization and accounting messages until the session is terminated.

HTTPS Server Certificate Chain/ Intermediate Certificate

Supported on all product families.

During the SSL/TLS handshake between the Switch (HTTPS server) and a browser (HTTPS client), the Switch presents its signed certificate. The browser, having the CA certificate in its trusted store, uses the CA's public key to verify the signature on the server certificate. This process establishes the authenticity of the server's identity. Once verified, the server and browser proceed to exchange cryptographic parameters, enabling the encryption of data in transit between them, ensuring a secure and authenticated connection for data transmission over HTTPS.

While server certificates can be directly signed by the root CA certificate, the use of intermediate certificates introduces a hierarchical structure that enhances the signing process. Intermediate certificates act as intermediaries between the server certificate and the root CA, offering benefits such as increased security through isolation of key compromises, flexibility in certificate management, and the ability to delegate signing authority. This hierarchical approach provides improved scalability, eases certificate renewal processes, and allows for more granular control over revocation. In essence, employing intermediate certificates enriches the signing process by providing enhanced security, flexibility, and streamlined certificate management.

The C1300 supports the following functionalities related to intermediate certificate and HTTPS server certificate chain:

- Installation of one or more intermediate certificates.
- Including the intermediate certificate(s) in the TLS handshake with the HTTPS client
- Display of intermediate certificate
- Display of the certificate chain of the device’s HTTPS server certificates

On-board Packet Capture

Supported on all product families.

The Onboard Packet Capture (OPC) provides the ability to capture packets received and sent on device interface and by CPU. The packet captures can then be displayed locally, saved to local storage, or exported for offline analysis. The OPC feature enhances troubleshooting capabilities on the device.

OPC on the C1300 supports the following:

- Creating up to 4 capture points – which are session for capturing packets. Packet capture is supported for the control plane (CPU) interface
- Define the following capture point attributes:
    - Define the capture direction (in, out or both)
    - Define the buffer mode and buffer size
- Starting or stopping a capture session (only 1 capture point can be active)
- Displaying capture buffer statistics
- Exporting the capture file to a *.pcap file on local flash or the USB.

GUI Management interface is not supported in this version.

"show diff-config" – New CLI Command

Supported on all product families.

Version 4.1.3.36 supports a new CLI command “show diff-config”. This command compares and displays the differences between the running and startup configuration file. This command is useful in cases where the user reboots the device and is prompted to save the running configuration.

CBD Connection System LED Indication

Supported on all product families.

The System LED will provide a tri color (Green, Yellow, Blue) indication. The new color (blue) will provided CBD connection info, as follows:

- Green LED (the default LED color (once the software is fully loaded)), provides the following indications:
    - No errors detected
    - The device is not connected to the CBD Dashboard
    - Supports LED flashing to indicate specific information (e.g. stack unit ID indication, reset button push duration etc) – the definition for the system LED flashing is detailed in other specifications
- Blue LED, provides the following indications:
    - No errors detected
    - New indication - The CBD agent on the device is connected to the Dashboard (Dashboard status == connected in the “show cbd” command output)
    - Supports LED flashing to indicate specific information (e.g. stack unit ID indication, reset button push duration etc) – the definition for the system LED flashing is detailed in other specifications
- Amber LED provides the following indications: error conditions exist on the device (e.g. detect HW failed, firmware failure or/and configuration file error)

The connection to the Dashboard is polled every 5 seconds. If the status of the connection changes, then the LED color will change accordingly.

If an error condition occurs, the system LED shall change from green or blue (depending on the state when error occurred) to amber. Once the error condition stops the LED will return to either green or blue color based on the latest poll indication.

CBD - add CBD Probe Mode Information

Supported on all product families.

Added CBD probe mode information to CLI Operational status field (show cbd command) and Probe Status GUI field. The probe mode is relevant only when the probe is active. The following probe modes are displayed:

- Probe Managed - The Probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard
- Direct Managed - Direct managed devices will discover other devices in the broader network and connect those devices to the Dashboard automatically then those devices become manageable.

SSL Updates

Effects all product families.

- OpenSSL version upgraded to version 3.0.11 (19 Sep 2023)
- Support for the following ciphers was removed in version 4.1.3.36:
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
    - TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072)
    - TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072)
    - TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 3072)

SSH Updates

Effects all product families.

Support for the following ciphers was added:

- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

Support for the following SSH Key Exchange methods (KEX) was removed in version 4.1.3.36:

- diffie-hellman-group1-sha1

Changed to GUI

Effects all product families.

- Added "Virtual Assistant" and CBD links to the Getting Started page
- Added to GUI mast an CBD icon which provides a link to the CBD product web page.

Known Issues

Caveats Acknowledged in Release V4.1.3.36.

Bug ID	Description
CSCwk42456	**Symptom** The SFP+ Port LEDs alternately flash green and amber when transmitting jumbo frame and jumbo frame support is disabled. This is a display issue. Jumbo frame handling is correct. **Workaround** None
CSCwk42458	**Symptom** An error message “Login banner too long” is displayed in GUI when entering a banner with more than 519 characters. **Workaround** None
CSCwk42463	**Symptom** Subject Alternative Names cannot be configured for Certificate requests generated on the device (command “crypto certificate request”). This generates an error message on browser when connecting via HTTPS. **Workaround** Generate a certificate request using an external tool.
CSCwk42465	**Symptom** When executing "show diff-config context-lines 0", the context-line count is empty instead of 1. **Workaround** None
CSCwk42467	**Symptom** The route time for RIP entries continues to increment and do not reset every 30 seconds. **Workaround** None
CSCwk42470	**Symptom** Revocation of intermediate certificate fails and secure access is provided based on this certificate **Workaround** Copy running to startup and reload the switch.

Bug ID	Description
CSCwk42473	**Symptom** On some SKUs the sflow flow-sample does not work on a port that is a member of a port-channel **Workaround** None
CSCwk42474	**Symptom** Link up may fail on some SKUs when inserting SFP-10G-T-X and set speed to 1G speed. **Workaround** None
CSCwk42476	**Symptom** RIP – routes are redistributed even if redistributing is not enabled. **Workaround** None
CSCwk42479	**Symptom** “No monitor capture control-plane” command – when using optional keywords in or out control plane is removed completely instead of just removing the specific direction. **Workaround** Remove control-plane and then re-add the required direction.
CSCwk42481	**Symptom** The Syslog Notifications Pop-Up in GUI stops working if the log table is has more than 1000 items. **Workaround** None
CSCwk42484	**Symptom** The display of time source in the GUI is "from browser" even though the time was set manually. **Workaround** Use CLI command "show clock detailed" to view correct clock source.
CSCwk42485	**Symptom** CLI command "no monitor capture match" in CLI guide is not supported. **Workaround** None.

Bug ID	Description
CSCwk42490	**Symptom** OPC captured packets from or to the standby/member units are encapsulated into IEEE802a OUI extended ethertype. **Workaround** None
CSCwk42492	**Symptom** On C1300 10G SKUs monitor session cannot capture the packets dropped by configured ACL. **Workaround** None

Resolved Issues

Caveats Resolved in Release V4.1.3.36.

Bug ID	Description
CSCwi56166	**Symptom** SSH to device fails when using RSA-SHA2-512 and RSA-SHA2-256 host key algorithm in Key exchange.
CSCwk42496	**Symptom** The 'PVST Interface settings' page on the GUI displays inconsistency type “PVID” even though the actual inconsistency type is “Port Type”.
CSCwk42499	**Symptom** Loopback detection fails when STP mode is PVST and STP is disabled.
CSCwi00760	**Symptom** Device console and GUI will not respond for about 3 minutes in the following scenario: • One or more DNS servers configured on device are not reachable. • In this state the user deletes and then adds the default SNTP servers.
CSCwe81254	**Symptom** An error message will appear on console if the DHCP pool name includes special chars (for example single quote, double quote, backslash) and user presses the “details” button in IPv4 Configuration→ DHCP Server → Network Pools GUI page.

Bug ID	Description
CSCwj13150	**Symptom** In some cases address count are not decremented on a port that is configured to port security Dynamic Lock mode. This may prevent other MACs to be learned.
CSCwj75101	**Symptom** DHCP server does not respond to Discover packet from client if the discover packet includes an option 55 (Parameter request list) with value 0.
CSCwi00359	**Symptom** In some cases stack interface LED may not light up when disconnecting then reconnecting stacking cable.

Resolved Issues 4.1.0.76

Table 1: Caveats Resolved in Release V4.1.0.76.

Bug ID	Description
CSCwi77502	**Symptom** In rare case there is slight packet loss on C1300-24XT when forwarding traffic in line rate and using long Cat6A cables.

Known Issues 4.1.0.75

Table 2: Caveats Acknowledged in Release V4.1.0.75

Bug ID	Description
CSCwi56166	**Symptom** SSH to device fails when using the RSA-SHA2-512 and RSA-SHA2-256 host key algorithm in a key exchange. **Workaround** None

Resolved Issues 4.1.0.75

Table 3: Caveats Resolved in Release V4.1.0.75.

Bug ID	Description
CSCwi54956	**Symptom** C1300-24MGP-4X port 17 cannot forward a packet at a speed of 2.5G.
CSCwi54958	**Symptom** MAC address relearning fails when a similar entry exists in the MAC forwarding table.
CSCwi54959	**Symptom** In rare cases, the Ports 45,46,47, and 48 of the C1300-48MGP-4X cannot link up after a reboot.

What's New

This section details the new features and modifications introduced in firmware version 4.1.0.72.

- Support for the new hardware platforms:
  - New PIDs are being introduced in this release and are listed in the table below:

Device PID	Description
C1300-8MGP-2X	Catalyst 1300 Series Managed Switch, 4-port 2.5GE, 4-port GE, PoE, 2x10G SFP+
C1300-24MGP-4X	Catalyst 1300 Series Managed Switch, 8-port 2.5GE, 16-port GE, PoE, 4x10G SFP+
C1300-48MGP-4X	Catalyst 1300 Series Managed Switch, 16-port 2.5GE, 32-port GE, PoE, 4x10G SFP+
C1300-12XT-2X	Catalyst 1300 Series Managed Switch, 12-port 10GE, 2x10G SFP+
C1300-12XS	Catalyst 1300 Series Managed Switch, 12-port SFP+, 2x10GE Shared
C1300-24XT	Catalyst 1300 Series Managed Switch, 24-port 10GE, 4x10G SFP+ Shared
C1300-24XS	Catalyst 1300 Series Managed Switch, 24-port SFP+, 4x10GE Shared
C1300-16XTS	Catalyst 1300 Series Managed Switch, 8-port 10GE, 8-port SFP+
C1300-24XTS	Catalyst 1300 Series Managed Switch, 12-port 10GE, 12-port SFP+

- New software features as detailed below:
- Feature updates to existing feature as detailed below:

New Software Features

Support of 1300 stackable devices supporting 10G on all Ports

This version added supports a new subtype of the Catalyst 1300 Stackable Managed Switch Series – devices supporting10G interfaces on all ports (on top of the existing Catalyst 1300 stackable devices supporting 10G uplink ports sub-type). Device of each sub-type cannot be stacked in the same stack with devices of the other sub-type. If they are stacked together, the units of one of the sub-types will be shutdown.

Feature set of the 2 sub-types is identical besides the following items:

- The following features/abilities are supported only on the devices supporting 10G interfaces on all ports subtype:
    - Physical OOB port for management – supporting IPv4
    - IPv6 Manual Tunnel
    - Automatic 6-to-4 tunnel
    - ISATAP Routing for IPv6
- The 2 sub-types have different table sizes - mainly for features which rely on hardware resources.
- Stacking interfaces
    - On the devices supporting 10G interfaces – Up to 8 stacking interfaces are supported. Any interface can be defined as a stacking interface.
    - On the devices supporting 10G uplink ports – up to 4 stacking interfaces are supported. Only the 10G uplink interfaces can be defined as a stacking interface.

PNP Agent Support

The Plug-n-Play (PNP) Agent on switch communicates with a PNP server, which allows centralized installation of configuration and image files to the switch. This allows customer to execute Zero Touch Installs of the switch in various deployment scenarios and deployment locations. PNP operation reduces customer costs associated with deployment/installation of network devices, increases the speed and reduce the complexity of deployments without compromising the security.

Cisco Business Dashboard (CBD) Support

Cisco Business Dashboard (CBD) helps you monitor and manage your Cisco network with the use of the Cisco Business Dashboard Manager. The Cisco Business Dashboard Manager is an add-on that automatically discovers your network and allows you to configure and monitor all supported Cisco devices such as Cisco switches, routers, and wireless access points.

Cisco Business Dashboard Manager is a distributed application which is comprised of two separate components or applications: one or more Probes referred to as Cisco Business Dashboard Probe and a single Manager called Cisco Business Dashboard Manager. An instance of Cisco Business Dashboard Probe is installed at each site in the network, performs network discovery and communicates directly with each Cisco device.

Certificate Authority (CA) Certificate Manager

The Cisco Business Dashboard Probe (CBD) and Plug-n-Play (PNP) features require CA certificates to establish HTTPS communication with the CBD or PNP servers. The CA Certificate Manager feature allows these applications and device managers to do the following:

- Install trusted CA certificates and to remove certificates that are no longer wanted

- Statically add certificates to device configuration file
- Manage a revocation list of untrusted certificates

HTTPS Redirection

As part of the tightening of the system security of the switch, users accessing the management GUI should use HTTPS whenever it is supported. In order to ensure the use of HTTPS, All HTTP requests will be redirected to HTTPS if HTTPS is enabled on the device.

Port Locate (beacon)

In some cases there is a need to physically identify a single or multiple interfaces on a device, using the port LED as a physical and external (device front panel) indicator. An example for such a situation is where system administrator is in a remote location and needs to guide the onsite installer or support engineer. The Port Locate/Beacon feature addresses this issue by allowing the system administrator to activate the interface LED of one or more specified interfaces (either physical interfaces or LAGs).

This feature is only supported via the CLI.

Interface LED flashing as in indication for err-disable State

When an interface moves to the err-disable state the interface LED will flash amber to provide an indication to this state.

Support of Additional Transceivers

Support for the following SFP/SFP+ Transceivers was added in this version:

- GLC-EX-SMD
- GLC-ZX-SMD
- CWDM-SFP-1470
- CWDM-SFP-1530
- CWDM-SFP-1610
- SFP-H10GB-ACU7M
- SFP-10G-AOC2M

Changes to Existing Features

This section details important changes to features which were already supported on previous versions.

Auto Surveillance VLAN (ASV)

The following 2 changes were introduced to ASV in this version:

- When changing the ID of the ASV VLAN (CLI command “surveillance-vlan vlan-id”) a confirmation message will be displayed. User will need to confirm the change is required.
- When enabling ASV the global bridge multicast filtering setting will be automatically enabled (in addition to IGMP snooping and IGMP snooping querier which were automatically enabled in previous versions).
- On some of the SKUs ASV entries will consume TCAM entries also on ports in access mode (TCAM entries utilization can be viewed using command “show system tcam utilization”. In the previous versions ASV entries consumed entries only if the interface was in general mode.

- The CoS action for ASV classified traffic was changed to “remark”, meaning that the VPT field value in the packet will be modified to the value defined in CLI command “surveillance-vlan cos” (in previous versions the CoS action was “assign” meaning the packet is assigned to the defined CoS queue but VPT field value was not modified.

Note The remark action consumes TCAM entries. These entries are in addition to TCAM entries displayed using the command **show system tcam utilization**.

Half Duplex Support

We do not support half duplex mode on any of the ports that are 10Gig on the switches listed in the table above.

Password Complexity

A more lenient interpretation is implemented for the following requirements:

- More than 2 sequential chars or numbers are not allowed.
- Prevent Usage of Known passwords in new passwords – in this release (4.1.0.72) only the beginning of the new password is compared to the known passwords, the middle will NOT be checked, In addition, the comparison doesn’t include reverse order or replacing character as follows: "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e".

Chip Protection

Added the observed and imprinted DB hash values to the output of the “show platform hardware integrity” command.

Boot-up Time Change

Bootup time in this release (4.1.0.72) increased by about 27 seconds compared to previous release (4.0.0.94). The increase in the bootup time is due to adding support to CBD feature.

Known Issues

Caveats Acknowledged in Release V4.1.0.72.

Bug ID	Description
CSCwi00331	**Symptom** The “show dying-gasp packets” command does not display the information related to the IPv6 syslog and the SNMP servers. **Workaround** None

Bug ID	Description
CSCwi00359	**Symptom** In some cases, the stack interface LED may not light up when disconnecting and then reconnecting the stacking cable. **Workaround** None
CSCwi00366	**Symptom** The switch cannot connect to the CBD Dashboard with a static DNS entry if the DNS server configured on the device is not reachable by existing host. **Workaround** Make sure that the DNS servers are reachable or remove the DNS server configuration if static DNS entries are being used.
CSCwi00368	**Symptom** In some cases, the 1G fiber interface will fail to link up if the fiber cable is disconnected and then reconnected quickly. **Workaround** Shutdown / no shutdown on the interface or Disconnect the fiber cable together with the SFP and then re-insert.
CSCwi00373	**Symptom** Loopback detection fails when STP mode is PVST and STP is disabled. **Workaround** Change the STP mode to RSTP, and then change it back to PVST/RPVST.
CSCwi00382	**Symptom** The 'PVST Interface Settings' page on the GUI displays an inconsistency type “PVID” even though the actual inconsistency type is “Port Type” . **Workaround** The inconsistency type is displayed correctly in the "PVST Inconsistent Ports" GUI page.
CSCwi00552	**Symptom** The 'PVST Interface settings' page on the GUI displays an empty inconsistency type when the inconsistency type is “Port PVID” **Workaround** The inconsistency type is displayed correctly in the "PVST Inconsistent Ports" GUI page.

Bug ID	Description
CSCwi00728	**Symptom** The CPU utilization rate does not refresh automatically (GUI page Status and Statistics > CPU Utilization). **Workaround** Refresh the page manually.
CSCwi00748	**Symptom** “show lldp local tlvs-overloading” command output - the field “Left” (bytes for TLV) displays the number of overloaded bytes instead of the bytes still available for local TLVs. **Workaround** Calculate the number of bytes available for TLV by subtracting the value displayed in the "total” field from MTU value (1500).
CSCwi00760	**Symptom** Device console and GUI will not respond for about 3 minutes in the following scenario: • One or more DNS servers configured on device are not reachable. • In this state, the user deletes and then adds the default SNTP servers. **Workaround** Disable IPv6 on all interfaces.
CSCwi00762	**Symptom** The 1G Combo interface port LED does not flash amber when the port is in err-disable state. **Workaround** The LED on these ports will be off when interface moves to the down state. In this case, use the CLI or GUI display to check if this port is in err-disable (or is down due to disconnection or manual configuration).
CSCwi00765	**Symptom** In some cases, the “Invalid perpetual restart detected, restarting board” syslog message will appear when the board is rebooted. **Workaround** There is no effect on the device functionality – board reboot and perpetual PoE support are not effected.

Bug ID	Description
CSCwi00769	**Symptom** On a stack of 6 or more members with ring topology, some of members may always reboot if using auto unit ID and stack link is a mix of Te1-2 and Te3-4. When this issue happens, by simply rebooting the whole stack can recover it and it will not happen again in next reboot. **Workaround** Connect a stack neighbor using TE1-2 or TE3-4, but don't mix them. Or do one of the following: • use a fixed unit ID • a chain topology • reboot the stack one more time
CSCwi00776	**Symptom** The ports that are not in the VLAN of "MST instance VLAN mapping" shouldn't participate in the MST calculation for this instance **Workaround** None

Resolved Issues

Caveats Resolved in Release V4.1.0.72.

Bug ID	Description
CSCwf56969	**Symptom** C1200 C1300 - PoE issue with DBS-210.
CSCwh21119/CSCwh06683	**Symptom** 802.1x MAC based authentication fails if STP mode is set to PVST/RPVST.
CSCwh58899	**Symptom** 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.”
CSCwe81251	**Symptom** Welcome Banner (configured via GUI) will be erased if the user configures via the CLI, a login banner with more than 512 characters in a single line.

Bug ID	Description
CSCwe81247	**Symptom** PoE Class display in GUI (page Port Management > PoE > Setting) is wrong for a class 0 PD.
CSCwe81236	Error message is displayed when configuring the command “"no ipv6 nd hop-limit " – and configuration is not accepted.
CSCwi00805	snmp "ipNetToMediaIfIndex" ifindex value not exist in IfTable->ifEntry->ifindex.

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.