Previous SWX2320 Firmware version information

V2.05.13

New Functionality

- The following command can now forward multicast packets without discarding part of the multicast communication even if “l2-unknown-mcast discard” is specified.

  l2-unknown-mcast forward
- Support for “summertime” time zones was added.

  User settings for the summertime period and offset hours were added to the “clock summer-time” command.

  On the Web GUI [Management]->[Interface settings] page, a [Time zone setting] page was added for setting the time zone and summer time settings.
- Security measures were strengthened for accessing the unit.
- A new cable diagnostics function was added.

  In addition, a cable diagnostics page was added to the [Management]->[Maintenance] menu of the Web GUI.
- The SDVoE optimization function was added.
- Support for the automatic SD card booting function was enabled.
- A command for changing the authentication order was added in case the same authentication method is also used for the port authentication function.
  - auth order

- Commands that can be registered in the FDB as static entries were added to the MAC authentication function.
    - auth-mac static
- IGMP snooping features were expanded to support the following:
    - A command for enabling/disabling the report suppression function was added.
    - ip igmp snooping report-suppression
    - A command for enabling/disabling the multicast router port data forwarding suppression function was added.
    - ip igmp snooping mrouter-port data-suppression

      The following settings were added to the [Multicast]->[IGMP snooping]->[IGMP snooping settings] field in the Detailed settings screen of the Web GUI.
    - Report Suppression Function
    - Multicast Router Port Data Forwarding Suppression Function
- SYSLOG facility values became changeable.
    - syslog facility

      In addition, the ability to change/display SYSLOG facility value settings was added in the [Management]->[Maintenance]->[SYSLOG management] field of the Web GUI.
- Commands were added to restrict access to the SNMP server.
    - snmp-server access

      In addition, the [Access via SNMP] settings screen was added to the [Management]->[Access management]->[Various server settings] field of the Web GUI.
- Private MIB support was added for loop detection.

- Support for the following was added to the Web GUI:
    - A [Multicast basic settings] page was added to the Detailed settings.
    - The following settings were enabled in the [Traffic control]->[QoS] field in the Detailed settings:
    - [CoS]->[Transmit queue mapping table] settings
    - [DSCP]->[Transmit queue mapping table] settings
    - The following settings are now displayed in the [Management]->[Dante optimization] field:
    - Unknown multicast frame settings
    - QoS settings

Improvements

- The maximum number of characters in shared passwords used for port authentication and RADIUS server functionality was increased from 64 to 128.

  RADIUS server shared password setting (radius-server key)

  RADIUS server host setting (radius-server host)

  RADIUS client setting (NAS)
- If PTP functionality is enabled for the overall system and “l2-unknown-mcast discard” is specified, PTP packets are forwarded without being discarded.
- The PTP input/output delay was corrected.
- Improvements were made to multicast address registering and deleting processes for IGMP/MLD snooping.
- The following terminology was changed for Yamaha network products:

Function	Before	After
L2MS	Master	Manager
	Slave	Agent
Stack	Master	Main
	Slave	Member
URL Filter	Black-list	Reject-list
	White-list	Pass-list
Backup route	Master	Main
SNMP (Private MIB)	ysl2msFindSlave	ysl2msFindAgent

- The following ARP changes were made:
    - ARP entries are no longer generated when ARP requests are received.
    - ARP replies are now received for only a fixed period after an ARP request is sent by that unit.
- Support for the IGMP snooping fast-leave function was also included in IGMPv3.
- Improvements were made to the time required by the logical interface to link up for LACP link aggregation.

- The use of characters " ' ` and ¥ were disallowed in URLs.
- If stacking is enabled, an error message is displayed if a PTP “show”-based command is executed.
- In the Web GUI login screen, a scroll bar is displayed if the browser display is small.
- The accordion menus for Detailed settings and Management screens of the Web GUI were reorganized.
- The “Change the settings related to the community accordingly.” or “Delete from related settings as well.” checkbox can be selected when changing/deleting community settings in the Web GUI [Management]->[SNMP]->[Community] field. These settings specify which clients can access the SNMP servers that determine whether the community is now also changed/deleted accordingly.
- The explanatory text was changed for the JavaScript and Cookie settings in the Web GUI general help page.

Fixed Bugs

- A bug was fixed that caused the system sometimes to reboot if the CPU usage ratio increased after receiving a portion of the IGMP packet.
- A bug was fixed that sometimes returned unwanted IGMP reports if an IGMP report was received from a multicast router port.
- A bug was fixed that sometimes stopped multicast streams from being forwarded correctly if a LAN/SFP port associated with a logical interface is linked up/down with IGMP/MLD snooping.
- A bug was fixed that sometimes caused unwanted log events to be output if an IGMP snooping group registration was deleted.

- A bug that sometimes prevented authentication when a guest VLAN was enabled during MAC authentication was fixed.
- A bug was fixed that resulted in rebooting if an invalid LLDP frame was received.
- The possibility of rebooting was eliminated after specifying the “send from” command for the email notification function.
- A bug that prevented using the following commands to make revisions via an SSH connection was corrected.
    - firmware-update execute
    - firmware-update sd execute
- A bug that prevented obtaining tech support via an SSH connection if a stack was configured was fixed.
- In the stack function, a bug was fixed that sometimes prevented communication via a member switch port if a stack was configured concurrently starting up in standalone mode.
- A bug was fixed that enabled a user to log in to the console without a password if the “username” command was used to change only the privilege settings for an existing user without entering the password.
- A bug was fixed that resulted in not reflecting associated LAN/SFP ports in settings when there are port authentication settings for a logical interface, and VLAN access to the logical interface was changed.
- A bug was fixed that sometimes prevented properly load-balancing unicast packets during link aggregation if they were addressed to MAC addresses registered in the FDB.
- A bug that sometimes prevented communication with devices connected to member switches in stack configurations was fixed due to ARP entry inconsistencies between stacks when many ARP entries were registered or deleted simultaneously.

- A bug was fixed that sometimes prevented transmitting packets when the half-duplex mode was used for port communication.
- A bug was fixed in the SNMP function that sometimes prevented obtaining a MIB after a MIB was obtained while rebooting a member switch in a stack.
- A bug was fixed that sometimes prevented transmitting multicast packets to some ports, because IGMP snooping did not function correctly during stack reconfiguration.
- A bug that sometimes resulted in not transmitting streams requiring a multicast router port when “l2-unknown-mcast discard” is specified was fixed.
- A bug that sometimes did not reflect VLAN IP address settings in the sender IP address settings for sending IGMPv2 report messages during IGMP snooping was fixed.
- A bug was fixed that sometimes cleared authentication information before the FDB aging time was complete during MAC authentication.
- A bug was fixed that sometimes caused some functionality to become unstable after the current time setting was changed, such as after the NTP time setting was corrected.
- A bug was fixed that sometimes prevented registering received packets from being routed for stack configurations.
- A bug that prevented URL encoding values from entering HTTP proxy server settings for updating firmware was fixed.
- A bug that sometimes outputted error log events if a dashboard page was opened in the Web GUI while rebooting a stack member switch was fixed.
- A bug in the port security function was fixed that sometimes prevented the blocking status in port security information after a stack was reconfigured.
- A format error in the “no switchport multiple-vlan group” command was corrected.

- A bug that sometimes prevented properly updating information in the “Device details and settings” view in the LAN map screen of the Web GUI was fixed.
- A bug was fixed that prevented some of the physical interfaces from displaying in the [Port authentication] field in the Detailed settings screen of the Web GUI if logical interface settings are deleted after stack reconfiguration.
- A bug was fixed that prevented displaying errors correctly after trying to specify dynamic VLAN settings for trunk ports using the [Interface settings]->[Port authentication]->[Port authentication settings] in the Detailed settings screen of the Web GUI.
- A bug was fixed that resulted in an error if a VLAN had frame transmission disabled when optimization settings were executed on the following pages in the [Management] settings of the Web GUI:
    - [Dante optimization]
    - [SDVoE optimization]
- Inconsistencies in how some information was displayed in the Web GUI help information were corrected.

V2.05.07

New Functions

- Enables using LACP link aggregation with stack configuration.
- Supports web consoles.
- Added the following pages in the Detailed settings screen.

    - Port Authentication

    - Spanning Tree
- Added the Backup / Restoration pages to the Management screen of the Web GUI.
- Enables the interface gadgets to show port block status caused by the spanning tree protocol on the Dashboard screen of the Web GUI. Please note that only the corresponding CIST ports is shown.

Enhancements

- Addressed the following vulnerability in OpenSSL.
    - CVE-2020-1971(JPCERT/CC JVNVU#91053554)
- Enables the SYSLOG functions to output the following INFO level logs when more than one L2MS master is detected or the duplicate is resolved.

  [L2MS]:inf: L2MS master duplication detected. (ADDR, portX.Y)

  [L2MS]:inf: L2MS master duplication resolved. (ADDR, portX.Y)
- The open-source software license is now shown on the Web GUI help.

Fixed Bugs

- Fixed a problem in which, in rare cases, a LAN port would not be linked-up at the startup.
- Fixed a problem in which the switch would not be able to communicate through the native VLAN when launching the switch using a config where either of the following commands was set to the interface.
    - switchport trunk allowed vlan add VLAN-ID
    - switchport trunk native vlan VLAN-ID
- Fixed a problem in which a port that satisfied the following conditions could be changed to a trunk port.

    - The port authorization setting is enabled and it is not in the multi-supplicant mode.
    - A guest VLAN is set.
- Fixed a problem in which the POWER indicator may not light in orange when an abnormal temperature was detected.
- Fixed a problem in which authentication may fail if the IP address was set and there was a linked-down VLAN interface in the RADIUS server function.
- Fixed a problem in which an IP address would not appear on the Web GUI if the static IPv4 address was set to a link local address (169.254.0.0/16).
- Fixed a problem in which the performance observation function would not show the past observation information (Day and Month) on the Dashboard screen of the Web GUI when the year changed.
- Fixed a problem in which showing the list map on the LAN map screen of the Web GUI with a system that included a switch from other manufacturers would corrupt the tree display.
- Fixed several problems that occurred during stack configuration.
- Fixed a problem in which receiving a certain L2MS message would result in a memory leak when the switch worked as an L2MS slave.
- Fixed some other minor problems.