Previous SWR2310 Firmware version information

V2.04.14

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.
- 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.

- o   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:

- o   Report Suppression Function
- o   Multicast Router Port Data Forwarding Suppression Function
- SYSLOG facility values became changeable.
    - o   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.
    - o   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:
    - o   A [Multicast basic settings] page was added to the Detailed settings.
    - o   The following settings were enabled in the [Traffic control]->[QoS] field in the Detailed settings:
    - o   [CoS]->[Transmit queue mapping table] settings
    - o   [DSCP]->[Transmit queue mapping table] settings
    - o   The following settings are now displayed in the [Management]->[Dante optimization] field:
    - o   Unknown multicast frame settings
    - o   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)
- The following changes were made to the default config settings:
  LLDP functionality is enabled
  Auto-configure via LLDP functionality is enabled.
- 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.
- 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 mail 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 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 in [Management]->[Dante optimization] of the Web GUI settings.
- Inconsistencies in how some information was displayed in the Web GUI help information were corrected.

V2.04.09

New Functions

- Supports the following devices by L2MS.
    - SWX3220-16MT
    - SWX2320-16MT
- Supports alias IP addresses.
  Carefully read the external specifications before using this function.
  To use this function, the following updates have been made in [VLAN] -> [Create VLAN] of the Detailed settings screen.
    - Up to four secondary IPv4 addresses can be set to one VLAN.
    - Up to five global IPv6 addresses can be set to one VLAN.
    - A label can be set to the IPv4 addresses.
    - A host name can be set to the IPv4 addresses obtained by DHCP.
- Supports the schedule function.
  Carefully read the external specifications before using this function.
- 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 transferring the L2MS frames when the L2MS feature is disabled.
- 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 following will be processed when the fan stops or an error occurs to the temperature sensor.
    - Sends an SNMP trap.
    - Shows the "The fan speed has increased." message on the Dashboard screen of the Web GUI.
    - Shows the "The fan speed of the Yamaha switch has increased." message on the LAN map screen of the Web GUI.
- The open-source software license is now shown on the Web GUI help.

Fixed Bugs

- Fixed a problem in which, in rare cases, an invalid SYSLOG message would be output or any of the servers could not be accessed at the startup after setting the access permission for servers such as HTTP and TELNET.
- Fixed a problem in which the link became unstable when connecting an SFP/SFP+ module to the SFP/SFP+ ports.
- 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, in rare cases, the unit would not reboot in accordance with a command such as the reload command.
- Fixed a problem in which the POWER indicator may not light in orange when an abnormal temperature was detected.
- 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, when multiple VLANs were set to the logical interface of link aggregation, starting the switch would not reflect the settings to the operations.
- 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 the communication speed status of the show interface command would not be updated according to the change made for the communication speed of the SFP+ port.

- 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 pressing the Enter key several times to find connected devices on the LAN map screen of the Web GUI would show duplicate search results.
- Fixed a problem in which pressing the "port power supply" button would not activate the power supply to a switch port on the LAN map screen of the Web GUI.
- Fixed the following problems found in the tag VLAN page on the LAN map screen of the Web GUI.
  - The port number of an L2MS slave that does not support the stack function was incorrect.
  - An L2MS slave combo port did not appear.
  - The screen display corrupted by updating the display due to a topology change while selecting a port to join a VLAN group.
  - Uplink/downlink arrows for a combo port did not appear.
- 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 a problem in which a VLAN with the same existing settings as the native VAN would not be set as an access VLAN if the operation mode was switched from Trunk to Access on [VLAN] -> [Tag VLAN] in the Detailed settings screen of the Web GUI.
- Fixed a problem in which the Ingress filter setting of a trunk port would not be shown properly on [Tag VLAN] in the Detailed settings screen of the Web GUI.
- Fixed a problem in which the setting items for the IGMP snooping would be shown in an incorrect order on [IGMP snooping] in the Detailed settings screen of the Web GUI.
- Fixed a problem in which the required input items became invalidated if "Select an authentication function" was changed on [RADIUS server] -> [User management] in the Detailed settings screen of the Web GUI.
- Fixed an incorrect explanation in the input content confirmation screen for the following Detailed settings' pages of the Web GUI.
  - [RADIUS server] -> [Server settings]
  - [RADIUS server] -> [User management]
  - [RADIUS server] -> [Managing certificates]
- Fixed a problem in which a warning would appear even if a "strongest" password was set to [Access management] in the Management screen of the Web GUI.

- 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.

V2.04.04

New Functions

- Supports RADIUS servers.
- Supports SMTPS and SMTP authentication by the email notification function.
- Added the function to send a query when a topology change of spanning tree is detected by the IGMP/MLD snooping function.

Enhancements

- Expanded the number of slaves managed by L2MS from 64 to 128.
- Added the following information to the show stack command.
    - MAC address of Virtual switch
    - Serial number of Member switch
    - MAC address of Member switch
    - Link status of Stack port
- Supports the following for the configuration file control by TFTP.
    - Enables automatic restart when the startup config is updated.
    - Enables import and export of all settings of startup config.
- The following remote paths are used:
    - startup-config #0 All settings: config0-all
    - startup-config #1 All settings: config1-all
- The remote path for all the settings of Startup Config in the SD card is as follows.
    - startup-config #SD config.txt :configsd
    - startup-config #SD All settings: configsd-all
- Enables automatic adjustment of the vertical axis of the traffic information graph between 10 kbps and 10 Gbps on the dashboard of the Web GUI.
- Enables applying of the access list to the OUT direction of the VLAN interface in [Access List] in the detailed settings of Web GUI.
- Enables setting the tagged VLAN of the logical interface in [VLAN] of the detailed settings of Web GUI.

Fixed bugs

- Fixed the problem in which a memory leak would occur if the L2MS function was disabled in the state of LAN map warning detected during operating as an L2MS master.
- Fixed the problem in which restart was executed when a large number of SNMP packets were received.
- Fixed the problem in which communication may have been prevented when a slave switch with an IP address different from that of the master switch was connected by the stack function.
- Fixed the problem in which the ARP table was not updated in the Spanning Tree when a topology change had occurred and communication could have been temporarily disabled, depending on the configuration.
- Fixed the problem in which loop detection could not be performed when the switch whose stack ID was set to 2 was started in the stand-alone state, the stack was configured in the loop state, and then the stack was set to the stand-alone state again.
- Fixed the problem in which the following phenomenon occurred when stack ports were connected to form a stack while loops were detected:
    - The loop detection (shutdown) state of the slave switch was released in the stack function.
    - Congestion would occur despite the loop detection (blocking) state.
- Fixed the problem in which an incorrect snapshot warning log would be output to the slave switch in the stack function in case that the snapshot function was enabled when operating as an L2MS master during the stack configuration.
- Fixed the problem in which the following phenomenon may have occurred if the member switch was restarted in case that the 802.1X authentication was enabled on the logical interface during the stack configuration.
    - Web authentication could not be executed when Web authentication was combined on the concerned interface.
    - Could not communicate with terminals registered as static/forward on the concerned interface.
- Fixed the problem in which some frames addressed to MAC address could be flooded during the stack configuration.
- Fixed the problem in which MIB could not be acquired when a large number of SNMP packets were received during the stack configuration.
- Fixed the problem in which IPv4 link local address could not be set even if the stack was invalid on the stack compatible model.

- Fixed the problem in which the authentication screen might not be displayed if the supplicant is connected via a switch or wireless AP when Web authentication was enabled on the logical interface.
- Fixed the problem in which the automatic recovery setting of BPDU guard was invalid after rebooting in the spanning tree error detection function.
- Fixed the problem in which the IGMP/MLD snooping settings remained in the running config even if the VLAN was deleted.
- Fixed the problem in which entries of ARP table or IPv6 Neighbor table may have been illegally overwritten by the following operations when multiple static ARPs or static IPv6 Neighbors were registered to one VLAN.
    - VLAN interface was up
    - The ip/ipv6 forwarding command was run
- Fixed the problem in which the running config would not be applied correctly even if it was set by TFTP.
- Fixed the problem in which unnecessary error logs would be output when DHCP Offer was received from multiple DHCP servers.
- Fixed the problem in which packets with different port numbers would also meet the conditions even if a policy map including a port number specification was applied to an interface in QoS.
- Fixed some other minor bugs.