Previous SWP2 Firmware version information

V2.03.09

New Functions

- Supports RADIUS servers.
- Supports SMTPS and SMTP authentication by the email notification function.

Enhancements

- Reduced the CPU load when saving logs.
  Since the internal operation of log saving has changed, the logs in the RAM area of the main unit may not be in chronological order when the firmware is revised down.
- 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 remote paths are as follows.
    - For USER mode: config0-all
    - For DANTE mode: config1-all (export only)
- 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.
- Made the following changes in [Maintenance] -> [CONFIG management] in [Management] of Web GUI.
  - Supports import and export of all settings.
  - Enabled selection of the config surface when importing or exporting.
  - Changed the file name when exporting the config of the L2MS slave device from "slave-config" to "l2ms-slave-config."
  - Error checking has been enhanced for importing and exporting configs.
  - Prevented automatic restart under the following conditions.

- When the device OS hangs up
- When the system cannot access some of the hardware inside the system

Fixed Bugs

- Fixed a problem in which restart was executed when a large number of SNMP packets were received.
- Fixed a 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 a problem in which, when in Spanning Tree, the device may end abnormally if the shutdown by BPDU guard and the recovery by auto recovery have been repeated.
- Fixed a problem in which the automatic recovery setting of BPDU guard was invalid after rebooting in the spanning tree error detection function.
- Fixed a problem in which the IGMP/MLD snooping settings remained in the running config even if the VLAN was deleted.
- Fixed a 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.
- Fixed a problem in which the running config would not be applied correctly even if it was set by TFTP.
- Fixed a problem in which unnecessary error logs would be output when DHCP Offer was received from multiple DHCP servers.
- Fixed a 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 problems.

V2.03.06

Vulnerability Responses

- Addressed the following vulnerability issues:
    - CVE-2019-11477(JVNVU#93800789)
    - CVE-2019-11478(JVNVU#93800789)
    - CVE-2019-11479(JVNVU#93800789)

- Addressed the following SSL v3 vulnerability issues:
    - CVE-2014-3566

New Functions

- Now supports multiple VLAN function.
- Now supports MLD Snooping function.
- Added a command to control whether EAP frames can be forwarded or not.
- The following pages have been added to the WebGUI detailed settings.
  “Creating an access list”
  “Apply access list”
- When a switch works as the querier while the IGMP snooping function and spanning tree are enabled, if a route change occurs due to cable disconnection, etc., a query will be sent immediately regardless of the query interval setting. This will resume the Dante multicast flow transmission shortly.

Enhancements

- The contents displayed by the “show interface brief” command have been optimized.
- The following changes were made in port authentication.
  - Supports dynamic VLAN in multi-supplicant mode.
  - Supports logical interface (Static and LACP).
  - Supports trunk port.
  - Added the status of the custom file for Web authentication to the execution result of the “show auth status” command.
- Policy map can be applied to link aggregation logical interface by QoS.
- The following settings of QoS can be changed with link aggregation logical interfaces.
  - Trust mode.
  - Default CoS value.
  - Port priority
- Access list can be applied to received frames of link aggregation logical interfaces by the ACL function.
- The interface specification option of the “clear ip igmp snooping group” command has been removed.
- The following changes were made in the WebGUI detailed settings.
  - Enabled to configure link aggregation logical interfaces in “QoS.”
  - When assigning LAN / SFP ports to the link aggregation logical interface in "Link aggregation," the QoS settings of each port are automatically unified.
- VLAN PRESET NORMAL disabled port 11 and 12 link aggregation and enabled spanning tree instead.
- The frame buffer size allocated per port has been increased to make it difficult for packets to be dropped when burst traffic occurs.

Fixed bugs

- Fixed a problem in which if you continue to access the WebGUI via HTTPS, you would not be able to log in to the WebGUI.
- Fixed a problem in which an unnecessary error log is output under the following conditions:
    - When disabling spanning tree on a port basis
    - When the VLAN interface to which the logical interface belongs is linked up or down
    - When creating or deleting a logical interface
    - When the multicast receiver end reception with the IGMP Snooping function
- Fixed a problem when IGMP Snooping related commands are configured in the IGMP Snooping function, an error may occur when executing the “ip igmp snooping disable” command.
- Fixed a problem when IGMP Snooping is disabled in the IGMP Snooping function, IGMP packets are not forwarded.
- Fixed a problem in which in the IGMP Snooping function, when there are multiple receiving terminals for one multicast, the multicast is not flooded even if all terminals have finished receiving.
- Fixed a problem where packets were not correctly prioritized by QoS.
- Fixed a problem in which the Trust Mode setting of the interface to which the policy map is applied may not be applied when it is restarted.
- Fixed a problem in which IGMP frames loop even if loop detection is enabled.
- Fixed a problem in which an authentication screen might not be displayed by Web authentication.
- Fixed a problem that caused packet drops in communication between ports with different communication speeds.
- Fixed the following problems in the WebGUI dashboard:
    - "Port blocked" was displayed when shutting down a port with loop detection.
- Fixed the following problems in the WebGUI detailed settings:
    - In the tag VLAN screen, the combo port on the SFP side that was the uplink cannot be set as a trunk port.
    - The error message was not displayed when selecting combo port with uplink in tag VLAN screen.
- Fixed a problem in which when the VTY port in use was invalidated, the corresponding console terminal would not terminate.
- Fixed a problem in which some Dante devices were not displayed in Yamaha LAN Monitor.
- Fixed some other minor problems.