SRW2016/SRW2024 Firmware Revision History

Software version 1.2.2.30 2008/03/03
Boot version 1.0.1 2006/06/11
Hardware Version 1.2

Notes
======
This firmware supports New PHY 1240 and must be used for SRW2016/SRW2024 v1.3 with this PHY. Note that Previous firmware can't be loaded on SRW2016/SRW2024 V1.3. However, this firmware has backward compatibility and so may be loaded on SRW2016/2024 V1.1 and V1.2.

Known Issues in this release
============================
1. ACL --> IP Based ACL
(a) Rules based on an IP address must not include leading zeros in the IP address. Entering leading zeros results in unpredictable behavior. For example, writing 192.168.1.1 works, but 192.168.001.001 does not work.

2. ACL --> MAC Based ACL
Creating a MAC ACL with to permit ethertype 0800 causes all traffic to be forwarded. Configuring a MAC ACL to permit ethertype 86DD causes all traffic to be denied.
Recommended Workaround: To avoid these situations, add a rule to deny any any.

3. Admin --> Port Mirroring
After configuring port monitoring, the target port is grayed out, and cannot be modified.
Recommended Workaround: Delete the mirroring session, and reconfigure.

4. Muticast --> IGMP Snoopnig
When changing the timeout for the "Leave Timeout", the change takes effect, but is not displayed correctly in the web interface.

5. QoS --> Advanced Mode
(a) When configuring a policy with police - exceeded action - out of profile dscp, the policy must have an action: trust cos-dscp or set dscp. If you configure a policy with police - exceeded action - out of profile dscp without an action - the device configures the action to trust cos-dscp. If you configure a policy with police - exceeded action - out of profile dscp with an action set cos/queue, the device configures the action to set dscp 0.

6. Setup --> Time
(a) The prioritization between servers is not maintained when two servers are configured simultaneously.
(b) If a lower IP address is added after the first one was configured and saved, then the two IP addresses swap location and prioritization.

7. SNMP --> Communities
(a) To edit fields including the change of SNMP mode, the entry needs to be deleted, and then re-entered.

8. SNMP --> Group Membership
It is not possible to modify the user name after it has been entered.
Recommended Workaround: Delete the user and reconfigure.

9. Statistics --> RMON
(a)No trap is fired for a configured RMON alarm for SNMPv3, but it's reported to system logs (sever log + memory/flash logs).

10. Image Download
When downloading via tftp or http, performing Power off/on to the device may result in requirement for downloading the image via XMODEM after the device recovers. When downloading via XModem, the device recovers by itself.
Note: Avoid disconnecting the device from a power source during image upload

11. Web browser availability
The web management interface is best viewed using Internet Explorer 5.5 and up, with a resolution of 1024 x 768. In the current software version, certain pages cannot be viewed well using other browsers. It is recommended to apply the following workarounds.
Note: Internet Explorer web browser must be installed prior to running the following procedures.

-Using Mozilla Firefox Web Browser:
(a) Install Firefox "IE Tab" add-ons. The latest version is available on https://addons.mozilla.org/firefox/1419/
(b) Select Tools --> IE Tab. Add in the IP address of switches to Sites Fitters
    (e.g. ?http://172.18.1.27? accepts wildcard http://172.18.1.*).
(c) Ensure that cookies are enabled, by clicking "enable" to "All sites to set cookies"Tools -> Options -> Privacy -> Cookies.

-Using Netscape Web Browser: Click the icon in the left corner, and select "IE Display"

12. HTTP connections cannot be opened
In very rare situations, when management sessions are opened and closed quite frequently, TCP sessions remain open after all HTTP sessions have been closed. Since connections are limited, the user cannot open HTTP connection in this situation. Only reboot or aging (few minutes) solves the problem.
Recommended Workaround: Wait a few minutes, and try again. If this fails, then the switch must be rebooted.
Note: It is possible to manage the device using a telnet session.

13. Menu CLI - Disable Active Management Access Profile
This software version does not support Management ACL, so this option is irrelevant to the user. It is reserved for future use.
"Disable active mgmt access profile" is not working in menu console

14. Web login
a) It is possible to log-in to the device web UI using any or blank password. Once a password for the admin user via the Web UI was created, it is still possible to access the device even when you use a blank or any password.
Recommended Workaround: When the admin user’s password is changed via telnet, accessing the device was not possible when an incorrect password was used.
b) By default, the switch can be accessed by typing in admin for username and leaving the password field blank however It is not possible to change the password for default Admin user via Web.
Recommended Workaround: Use telent to define Admin password

15. Quality of Service -> Queue setings

When selecting the WRR scheduling the default weights per queue are 1-2-3-4 instead of 1-2-4-8.
Recommended Workaround:Rewrite the WRR weight and press “save setting” to apply