

SRW2008/SRW2008P/SRW2008MP Firmware Release Note

Software version 1.0.4
Boot version 1.0.1

09/11/2007
06/13/2006

=====

1. Support of 100SFP

This release introduces an enhancement to support 100SFP module. The device can automatically set up proper port setting for supported 100SFP modules: Linksys MFELX1 and MFEFX1.

.

2. CPU Utilization Display

The application provides the ability to enable and disable the CPU utilization mechanism and display its output. This application is controlled by WEB base management to display the system CPU utilization. The display will be graphic, showing history point per second over the user-selected period. If Java Virtual Machine (JVM) is not installed on the client PC, the graph is not displayed. Refer the link of <http://www.java.com> for JVM installation.

3. Power allocation per Port - SRW2008P,SRW2008MP

With this software release an enhancement to the PoE standard is introduced, whereby the user configures the allocated power. If a Power Device (PD) on a PoE port consumes more power than the specified allocate power, the port will be shut down. If the user does not configure the power allocation, the PoE classification is kept.

4. Total PoE Power set the max capacity- SRW2008P

Starting this release, one can upgrade the SRW2008P to support full power allocation for all eight ports. After connecting the power supply of SRW2008MP/SRW208MP, the user can use the web interface of Port Management--> PoE Power setting to select "Extended" on the Power Supply Type drop-down menu.

Known Issues

=====

1. 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.

2 . Setup --> network setting

Changing any field on the Network Settings Tab will result in sending a DHCP release and than Discover which may lead to in IP address change.

3. Admin --> Cable Test

When testing cable with advanced test only (without simple test before), the results are incorrect.

4. 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.

5. QoS --> Basic Mode (Double Check this Bug)

The "Trust Mode Table" is not functional. Attempting to disable the trust mode on an interface of the trust mode table results in an error message, and does not disable the trust mode on a per port basis.

6. QoS --> Advanced Mode

(a) Newly created entries in the Advanced Mode are displayed in the table only after refreshing the table. For example, after creating a new policy, using the pop-up window, it is displayed only after refreshing the main window.

(b) Under one policy, one can only select either Single or Aggregate police type but not both.

(c) It is not possible to create two identical policers with the same settings and action.

(d) QoS advanced mode page will refresh twice if browsed to it.

7. Security --> TACACS+

It is impossible to update the key string, after a server has already been configured.

Recommended Workaround: To update the key string, the server must be deleted, and then re-configured.

8. Setup --> Time

(a) The DST dates cannot be edited after selecting different radio boxes.

Recommended Workaround: Refresh the page, and configure.

(b) Configuring Daylight Savings Time in conjunction with SNTP servers may result in unclear errors.

(c) The prioritization between servers is not maintained when two servers are configured simultaneously.

(d) If a lower IP address is added after the first one was configured and saved, then the two IP addresses swap location and prioritization.

9. SNMP --> Communities

To edit fields including the change of SNMP mode, the entry needs to be deleted, and then re-entered.

10. SNMP --> Group Membership

It is not possible to modify the user name after it has been entered.

Recommended Workaround: Delete the user and reconfigure.

11. 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

12. Timestamps

The order of the month and day in the dates presented in syslog messages is the European fromat (dd/mm/yy), and not the US format.

13. Security--> Storm Control (Need to double check)

Configuring Unknown Unicast mode results in an error message.

14. 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".

15. Management --> Password

User can not change the default password from the web UI

Recommended Workaround: Use the console menu

16. VLAN Management --> VLAN to Port

When VLAN to Port is set the action is performed successfully and then an error message is displayed on the window.

Recommended Workaround: Ignore error message