SPS2024 Firmware Revision History

Software version 1.0.2 2009/03/23
Boot version 1.000.1 2008/01/11
Hardware Version 1.0

Recommended Practice
==========
1. DHCP Snooping Database Backup to the flash file
DHCP snooping database backup (to flash file) needs to be enabled by the operator and requires proper SNTP configuration, i.e. set the time setting mode is set to ‘Use SNTP Time’.

2. If IP address used for managing the device is configured on the default VLAN, than change of ID for default VLAN, is allowed without any warning. This change will cause that after reload the previously configured IP will be removed from the VLAN, so the system becomes unmanageable from remote.
Recommended Workaround: Join port to be member of the new VLAN before making the change

Feature Exceptions
==========
1. When the switch is using the default IP address 192.16.1.254, the DHCP IP Address mode cannot be enabled.
Recommend Workaround: Avoid using the default IP address before enable the DHCP IP Address mode

2. Multicast router packets handling by Forbidden Forward All interfaces (command bridge multicast forbidden forward-all):
- The port is allowed to become a multicast router (it will forward all IGMP reports to connected MRouter)
- The port can not dynamically join to any multicast group – and will not forward any multicast streams
- The use of the command is to forbid a port to forward multicast data

3. Adding fiber ports to trunks
100SFP cannot be added to Trunk if fiber link is down, or if it is set to auto-neg it will be added with warnings.
Recommended Workaround: Fiber port/s should be configured by user to “no auto-negotiation” and be in status up before being added to Trunk.

4. PVE and DHCP relay coexistence
PVE cannot be configured on a port in the VLAN X, on which DHCP Relay is enabled. Otherwise, the following message is displayed: "can’t have protected portmember and IP interface simultaneously".

Known Issues in this release
==========

1. Web Management Access may take several minutes to open the following pages in case of large amount of rules/configurations involved

1a. TCAM Usage: In cases of large amount of Ternary Content Addressable Memory (TCAM) rules configuration process for application such as ACL configuration, IP Source Guard and ARP.

1b. QoS ->Advance Mode page
When the ACL table is heavily populated on QoS "Advance Mode" page

1c. ACL->IP Based ACL, ACL->MAC Based ACL
When the ACL table is heavily populated, e.g. with 1000 entries,

1d. Multicast-> Bridge Multicast
When the bridge table is heavily populated,

Recommended Workaround: Provide the necessary time for the page to load. If the browser popup a warning message for delayed script, please select the option that enables application to proceed with its task or use CLI.

2. VCT
2a. VCT - Cable length on Giga Ethernet port is calculated incorrectly on long cables (cable longer than 100 meter).
2b. VCT - port with no cable shows open instead of “no cable”

3. 802.1X maximal number of session is less than 536
802.1X maximal number of sessions is 512 plus number off connected ports (24) that sums up to 536

4. Web Management: vlan management pages
If there are 255 vlans configured WebUI may take about 1 minute to open

5. Web Management: Port Management --> Port Settings
The PVE configuration is not displayed on the WebUI when port link is down

6. Web Management: multicast -> bridge multicast
When the user tries to add more than 32 IGMP group entries statically, a “resource unavailable” message will be displayed.

7. CLI Command: show ip igmp snooping groups
The CLI command "show ip igmp snooping groups" displays 0.0.0.0 in querier column while it should display 'Yes' or 'No'.

8. Multiple hosts may get the IP address behind the port with 802.1x enabling

When a port with 802.1x enabling is the member of the VLAN, which supports DHCP Snooping, an unauthenticated host behind this port could receive IP address from the DHCP Server. However, the traffic of these stations will be blocked as required.