SPS224G4 Firmware Release Note
Software version 1.0.2 11/19/2008
Boot version 1.0.2 11/13/2007
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 administrator and requires proper SNTP configuration, i.e. configure the time setting mode to ‘Use SNTP Time’.

2. DHCP, 802.1x and guest VLAN coexistence
Most of the deployed stations (PCs) run DHCP procedure simultaneously with 802.1x authentication. If the supplicant is authorized, it will normally be allowed access to a VLAN other then the guest VLAN. If IP address was acquired via DHCP procedure prior to successful completion of the 802.1x authentication, the assigned IP address belongs to the guest VLAN and the station looses connectivity.
Recommended practice: After successful completion of the 802.1x authentication, the user might need to manually release & renew the IP address

3. It is recommended to download the configuration file from TFTP to the startup config file and not to the running config so that the current configuration will be replaced.

4. DHCP Option 82
In the 1.0.1 version, the default behavior of the switch was to not add option 82 to DHCP discover packets. Starting from the the 1.0.2 version option 82 is added to DHCP discover packets by default.
Implication on the customer - if the user doesn't want option 82 to be added to DHCP discover packets and in the previous version fe simply didn't do any configuration since it was the default behavior he will need to disable option 82 via the WEB GUI or the CLI.

Feature Exceptions
==================

1.Default FE port admin status is down
Starting from 1.0.2, the default admin status of FE ports is the FE ports is set to "down".
For ports with default admin status down, then the shutdown command appears in the configuration file. If the admin status is set to up, then no shutdown command appears.

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 cannot 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 (Link Aggregation) if fiber link is down. If it is set to auto-neg, it will be added with warnings.
Recommended Workaround: Auto-negotiation on fiber port/s should be disabled manually by user, and the link status should be "Up" before the fiber port/s being added to Trunk.

4. Port Mirroring
By default, this product supports tagging in analyzer port. This applies only to TX mirroring and only if both analyzer and source ports are FE ports.

5. HTTP certification issue with FF3 and IE7 browsers may occur.
Security certificate is self signed. As a result a navigation warning may be displayed. In order to apply management connectivity in secured channel (HTTPS).
Recommended Workaround: It is possible to install a proper certificate signed by a trusted Certificate Authority (CA).

6.Egress shaping could not apply to the port with half-duplex mode.

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. DHCP Snooping Database (update FLASH file)
DHCP Snooping database is saved periodically to FLASH file. If the device is restarted by user in between two save cycles, the newly learnt entries will not be saved.

4. Storm control
Device CLI allows configuration of unknown Unicast storm control on FE port (configuration per port) even though nothing would actually be configured.
Recommended Workaround: Ignore this command and use global FE ports for Unicast storm control command.

5. Web Management: Setup -> Summary
With HTTPS login, the switch picture will be displayed for 30 seconds delay.
Recommended Workaround: User should refresh this page manually or wait for 30 seconds when working on HTTPS.

6. Web Management: Security Suite->ARP Inspection List
When the user tries to add more than 32 ARP Inspection List entries, a “resource unavailable” message will be displayed.

7. Web Management: Security Suite-> IP Source Guard Database
On Web GUI IP Source Guard Database table shows entries even though IP Source Guard is disabled.

8. Web Management
In some cases, page may not fit to window after changing window size
Recommended Workaround: User should refresh page manually.

9. 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.