Release Notes for SPS Series Switches Software Version 1.0.6.x

November 2011

These Release Notes describe the recommended practices and known issues that apply to the Version 1.0.6.x software for the following products:

SPS2024, SPS224G4, SPS208G

Contents

Limitations and Restrictions

The following open issues exist in release 1.0.6.x:

Recommended Practices

- DHCP snooping database backup (to flash file) needs to be enabled by the administrator, and requires proper SNTP configuration. For example; configure the time setting mode to 'Use SNTP Time'.
- Most PCs run DHCP 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 an IP address was acquired via DHCP prior to successful completion of the 802.1x authentication, the assigned IP address belongs to the guest VLAN and the station looses connectivity.

  Recommended Workaround: After successful completion of the 802.1x authentication, the user might need to manually release and renew the IP address.
- It is recommended to download the configuration file from TFTP to the startup configuration file, and not to the running configuration, so that the current configuration will be replaced.
- Option 82 is added to DHCP discover packets by default. If the user doesn't want option 82 to be added to DHCP discover packets they will need to disable option 82 via the WEB GUI or the CLI.

Feature Exceptions

- The default admin status of FE ports is set to "down". For ports with the default admin status of “down”, the shutdown command appears in the configuration file. If the admin status is set to “up”, then no shutdown command appears.
- The following apply to Multicast router packets handled 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.

- When adding fiber ports to trunks, 100SFP cannot be added to a trunk (Link Aggregation) if the fiber link is down. If it is set to auto-negotiation, it will be added with a warning displayed.

  Recommended Workaround: Auto-negotiation on fiber port(s) should be disabled manually by the user, and the link status should be "up" before the fiber port(s) are added to the trunk.

- By default the switch supports tagging in analyzer port. This applies only to TX mirroring, and only if both the analyzer and source ports are FE ports.
- An HTTP certification issue with Firefox version 3 and Internet Explorer version 7 browsers may occur. The security certificate is self signed and as a result a navigation warning may be displayed.

  Recommended Workaround: Install a proper certificate signed by a trusted Certificate Authority (CA).

- Egress shaping can not be applied to a port configured with half-duplex mode.

Known Issues

- Access through the web-management interface may take several minutes to open the following pages in cases where a large amount of rules and/or configurations are involved:
  - *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.
  - *QoS -> Advance Mode*, when the ACL table is heavily populated.
  - *ACL -> IP Based ACL*, *ACL -> MAC Based ACL*, when the ACL table is heavily populated, e.g. with 1000 entries.
  - *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.

- Cable length on a Gigabit Ethernet port is calculated incorrectly on long cables (cable longer than 100 meter).
- A port with no cable attached shows open instead of "no cable".

- The DHCP Snooping database is saved periodically to FLASH file. If the device is restarted by user in between two save cycles, the newly learned entries will not be saved.
- The switch CLI allows configuration of unknown unicast storm control on an 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.
- When configuring through the web-management interface, and displaying the *Setup -> Summary* with an HTTPS login, the switch picture will be displayed after a 30 second delay.

  Recommended Workaround: Refresh this page manually or wait for 30 seconds when using HTTPS.
- When configuring through the web-management interface, and displaying the *Security Suite ->ARP Inspection List* page, trying to add more than 32 ARP Inspection List entries, a “resource unavailable” message will be displayed.
- When configuring through the web-management interface, and displaying the *Security Suite -> IP Source Guard Database* page, the IP Source Guard Database table shows entries even though IP Source Guard is disabled.
- When configuring through the web-management interface, in some cases, the page may not fit in the window after changing the window size.

  Recommended Workaround: The user should refresh the page manually.
- 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 an IP address from the DHCP Server. However, the traffic of these stations will be blocked as required.

Major Changes and Defects Corrected

- Fixed various IGMP issues that can cause the switch to reboot; including join/leave group, and Multicast TV VLAN support.
- Fixed a sporadic issue with logging into the switch through an http session, where the login may get stuck permanently due to a session timeout.
- Fixed various SNMP issues and added enhancements to SNMP.
- Fixed an issue where a DHCP request can override the current client's IP setting to 0.0.0.0 in the IP DHCP Snooping table, which resulted in inaccessibility.
- Fixed an STP issue where the switch containing a high value MAC address in the first octet would always calculate itself to be the root bridge.
- Fixed an issue with the switch dropping DHCP packets with option 82 when the messages option does not contain sub options 1 and 2.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required.
Product Documentation	
Cisco Small Business SPS Switches	www.cisco.com/en/US/products/ps10021/tsd_products_support_series_home.html
Regulatory, Compliance, and Safety Information	www.cisco.com/en/US/docs/switches/lan/csb_switching_general/rcsi/Switch_RCSI.pdf
Warranty Information	www.cisco.com/go/warranty
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Copyright © 2011