Zyxel GS2210 series V4.50(Axxx.4)C0

Release Note/Manual Supplement

Date: Jul. 10, 2020

This document describes the features in the GS2210 series product for its V4.50(Axxx.4)C0 release. This is a maintenance release to contain major bug fixes for issues occurred on GS2210 series since the previous version.

Support Models:

- Zyxel GS2210-48HP
- Zyxel GS2210-48
- Zyxel GS2210-24HP
- Zyxel GS2210-24
- Zyxel GS2210-24LP
- Zyxel GS2210-8HP
- Zyxel GS2210-8

Version:

Model	Firmware Version	Boot Version
Zyxel GS2210-48HP	V4.50(AAHW.4) | 07/08/2020	V1.05 | 12/19/2013
Zyxel GS2210-48	V4.50(AAHV.4) | 07/08/2020	V1.05 | 12/19/2013
Zyxel GS2210-24HP	V4.50(AANE.4) | 07/08/2020	V1.00 | 12/18/2013
Zyxel GS2210-24	V4.50(AAND.4) | 07/08/2020	V1.00 | 12/18/2013
Zyxel GS2210-24LP	V4.50(ABEO.4) | 07/08/2020	V1.00 | 04/14/2016
Zyxel GS2210-8HP	V4.50(AASQ.4) | 07/08/2020	V1.00 | 07/22/2014
Zyxel GS2210-8	V4.50(AASP.4) | 07/08/2020	V1.00 | 07/22/2014

Enhanced Features:

V4.50(Axxx.4)C0:

1. **[IPv6]** Enable IPv6 Address Auto Configuration by default.
2. **[DHCPv6]** Enable DHCPv6 client mode by default.
3. **[CLI]** "enable" command would be disabled by default.
4. **[LED]** Users with privilege 3 are allowed to turn on/off Locator LED.
5. **[Neighbor]** Display both IPv4/IPv6 address on neighbor page.
6. **[ZON]** ZON supports IPv6 address.
7. **[VLAN]** Support Vendor-ID based VLAN.
8. **[Web GUI]** Apply new login interface.
9. **[Surveillance]** Support Auto PD recovery.

V4.50(Axxx.3)C0:

1. **[CPU protection]** Switch supports Arp packets CPU protection by default to improve the smoothness of managing switch via WEB/CLI when there are a lot of Arp packets in the network environment.
2. **[SSH]** Switch supports SSH for IPv6

V4.50(Axxx.2)C0:

1. **[VLAN]** VLAN mapping
2. **[DHCP]** DHCP Auto configuration
3. **[CLI]** CLV Command
4. **[NTP]** NTP Server supports DNS format
5. **[System]** Enhanced dual image resilience
6. **[Security]** SHA2
7. **[Loop guard]** Loop guard enhancement
8. **[IPv6]** Show IPv6 socket
9. **[Login]** Logout all current user access after changing the device management IP
10. **[Port]** Display port utilization
11. **[CLI]** Use [Ctrl+C] to escape when executing "show running config, show log"
12. **[NTP]** Time sync (NTP) over IPv6
13. **[SNMP]** Cable diagnostic MIB
14. **[Syslog]** Syslog setup for IPv6 and UDP port
15. **[ZDP]** ZDP v1.8.3
16. **[Syslog]** Time stamp for save configuration

17. **[PoE]** POE default mode change to consumption mode, and the default config will show consumption mode setting.(POE model only)
18. **[WEB]** Web login warning page
19. **[Security]** 802.1x EAPOL flooding
20. **[Multicast]** IGMP snooping leave-proxy
21. **[System]** Custom Default configuration
22. **[Hardware]** Smart fan (designed to automatically adjust speed based on device temperature)
23. **[Bandwidth control]** Improve the bandwidth control accuracy under lower rate, especially for ISP application
24. **[WEB]** Enhanced GUI with new Zyxel logo
25. **[Multicast]** Avoid multicast group cannot be added while mac collision happens

Bug Fix:

V4.50(Axxx.4)C0:

1. eITS#170900154
   [Hardware monitor] Hardware monitor detect abnormal value.
2. eITS#180400205
   [SNMP] Snmpwalk gets error output in TIME-RANGE-MIB.
3. eITS#180701100
   [AAA] while configuring TACACS+ as login method one and local as login method two, users can log in switch from both methods. It should follow the rule that only when method one is down then method two can work.
4. eITS#180800687
   [AAA] If the shared key of TACACS+ server is mismatched, switch will not consider the server is unreachable and will not change to other login methods.
5. eITS#190200916
   [Authentication] Switch may be randomly rebooted if dot1x guest VLAN multi-secure mode is enabled.
6. eITS#190201160
   [LLDP] The device will reboot unexpectedly due to LLDP memory leak.
7. eITS#190300525
   [IPv6] Handling IPv6 routing may cause switch crash and reboot.
8. eITS#190500548

[ACL] Classifier entry cannot be deleted after the binding policy rule was deleted in inactive state.

9. eITS#190500189
   [LLDP] Switch crashes when receiving LLDP packet with incorrect length of TLV.
10. eITS#190700015
    [Web GUI] Can't display IP source guard binding info on web GUI.
11. eITS#190800016
    [PoE] PD gets an incorrect allocated power value when Power-via-MDI is enabled along with PoE Max Power.
12. eITS#190800433
    [CLI] Can't display the correct information when configuring "Show IPv6 neighbor | include".
13. eITS#190800796
    [IPv6] Switch crashes when receiving particular IPv6 MLD packets.
14. eITS#190900353
    [MGMT] Lost IPv6 management when IPv6 MLD snooping proxy is enabled.
15. eITS#191100449
    [MGMT] Switch will randomly warm-reboot after a lot of continuous SSH login.
16. eITS#200200647
    [IPSG] IPv6 DHCP snooping untrusted port is not working.
17. eITS#200500197
    [AAA] HTTP login switch will fail when using RADIUS authentication.

V4.50(Axxx.3)C0:

1. eITS#180100502
   [PoE] The secondary port of Ruckus AP R610 needs to power up with PoE+.
2. eITS#180500496
   [NTP] The switch doesn't sync with NTP server properly
3. eITS#180601097
   [System] The switch auto reboot when creating an user with a password of 24 types or configured an SNMPv3.
4. eITS#180700489
   [System] The device will reboot unexpectedly due to LACP memory leak
5. eITS#180800690

[Authentication] MAC authentication does not work when both mac authentication and port authentication are enabled.

6. eITS#180601044
   [SSH] SSH session that does not complete successful login attempt may block users that have the right access to the Switch management. Adjust SSH time out period from 300 seconds to 150 seconds to effectively terminate session that does not have successful logins.
7. eits#181000135
   [SNMP] Fix backward compatibility issue for ZyNOS 4.50 upgrade for cfm trap configuration.
8. eits#180900583
   [System] Fix switch firmware upgrade issue when the firmware version are more than 2 versions apart.
9. eits#181000206
   [SNMP] Periodically request switch for zyTransceiverDdmiCurrent (.1.3.6.1.4.1.890.1.15.3.84.1.2.1.6) causes CPU high.
10. eits#181100769
    [Link] When MGS3750 is connected with GS2210 by SFP-LX-10-D, after rebooting MGS3750, the fiber port can't link up
11. eits#181000788
    [Authentication] Switch sometimes crash when using 802.1x.
12. eits#190100411
    [Filtering] Fix Mac filter issue when enable DHCP snooping.
13. eits#190201196
    [NTP] NTP for IPv6 does not work properly.
14. eits#181200003
    [LLDP] LLDP-MED can't work due to IP phone uses IPv6 address in chassis ID and switch ignores the LLDP-MED packet.
15. eits#190300235
    [DHCP] DHCP snooping is not able to block DHCP server packet even port setting is "untrust".

V4.50(Axxx.2)C0:

1. eITS#151100702

[DHCP] When switch enable ARP inspection and DHCP snooping, it will cause DHCP packets be flooded to other ports.

2. eITS#151200455/ 170200710
   [LLDP] particular Cisco IP phone may release IP (DHCP mode) after every 180 seconds.
3. eITS#151201303
   [SNMP] SNMP GETBULK produces incorrect results when max-repetition is set greater than 55.
4. eITS#160101145
   [EAPOL] The switch cannot flood the EAPOL packets when 802.1x is disabled.
5. eITS#160200247
   [Log] Displayed port speed value is triple the actual speed for both TX and RX.
6. eITS#160300698
   [VLAN] Partial configuration loss occurs after configuring private VLAN via web GUI and rebooting switch.
7. eITS#160501171
   [MSTP] Switch cannot forward IGMP query when using MSTP.
8. eITS#161000919
   [WEB] Web GUI session does not timeout properly if user does not close the browser.
9. eITS#170100698
   [RSTP] The switch cannot auto adjust RSTP path cost according to the port speed.
10. eITS#170300428
    [PING] Switch has high ping latency periodically due to the routine runtime task.
11. eITS#170400423
    [BOOT] No longer boot up after firmware uploaded. (Only for GS2210-24LP)
12. eITS#170500473
    [MGMT] Prevent unexpected reboot caused by Avast antivirus software.
13. eITS#170500522
    [ACL] The switch may reboot unexpectedly after changing the current settings of classifiers.

14. eITS#170500863
    [SYSTEM] Switch may encounter unexpectedly reboot under a large IP network environment.

15. eITS#170600557
    [IGMP] Floods an IGMP query every time when switch receives an IGMP Leave.
16. eITS#170801018
    [SNMP] Sometimes SNMP agent returns incorrect gateway MAC address.
17. eITS#170900439
    [POE] Switch does not provide PoE power when the time range is very closed to NTP synctime.
18. eITS#171000095
    [SNMP] The SNMP ifHCInOctets/IfHCOutOctets(counter 64) cannot count exceed 2^32.
19. eITS#171000116
    [SNMP] Operator cannot modify the syslog server level via SNMP while Syslog server is activated.
20. eITS#171200272
    [IPSG/Port Security] Client traffic is unexpectedly discarded after MAC address aging time when IPSG and port security are enabled.
21. eITS# 180100999
    [Maintenance] Switch may miss configuration if upgrades to new firmware.
22. eITS# 180200048
    [WEB] Web GUI may display Syntax error when restoring configuration.
23. **[MGMT]** Enhance the UX with MacBook by changing the ASCII of the backspace to follow the industrial standard.
24. **[WEB/CLI]** Switch can't be managed via WEB/CLI smoothly when there are a lot of broadcast/multicast traffics in the network environment.

Known Issue:

1. **[Bandwidth Control]** Ingress rate limit of TCP traffic might have inaccuracy with some criteria.
2. **[Security]** Fake IP traffic cannot be filtered when a static IP binding existed.
3. **[DIAG]** The cable length resolution of Cable Diagnostic is about +-15 meter.
4. **[DIAG]** The fault distance of Cable Diagnostic is less than 1 meter without cable inserted.
5. **[MGMT]** GS2210 is cluster manager and the cluster member won't upgrade firmware via FTP if firmware size over than 4.8MB.

6. **[BPDU Guard]** Port status inconsistent when enable BPDU Guard on one port then enable link aggregation.
7. **[ZULD]** Switch doesn't receive OAM packet from neighbor device but the ZULD status keep at "Probe" status when enable error recovery.
8. **[VLAN]** The incoming traffic from specific port that does not match VLAN Mapping cannot be dropped.

Limitation of Settings:

1.	802.1Q Static VLANs	1K
2.	Static MAC forwarding entry	256
3.	MAC filtering entry	256
4.	Cluster member	24
5.	Protocol based VLAN entries per port	7
6.	Port-security max address-limit number	16K
7.	Syslog server entry	4
8.	IP source guard entry	512
9.	IP subnet based VLAN entry	16
10.	DHCP snooping binding table	16K
11.	Multicast group	1024
12.	ACL	256
13.	DHCP relay Entry	16
14.	Trunk groups	5 (8 ports)/ 14(24 ports)/ 16(48 ports)
15.	Per trunk group port number	8
16.	MSTP instance	0-15
17.	MAC-based VLAN	10(8 ports)/ 28(24 ports)/ 50(48 ports)
18.	Voice VLAN OUI entry	6
19.	ZON neighbor per-port maximum clients	10

Change History:

- V4.50(Axxx.4) | 04/22/2019
- V4.50(Axxx.3) | 04/22/2019
- V4.50(Axxx.2) | 02/27/2018
- V4.30(Axxx.0) | 09/07/2015
- V4.10(Axxx.0) | 10/03/2013