Zyxel GS1920 series V4.50(AAxx.3)C0

Release Note/Manual Supplement

Date: Jun. 1, 2020

This document describes the features in the GS1920 series product for its V4.50(AAxx.3)C0 release.

Support Models:

- Zyxel GS1920-48HP
- Zyxel GS1920-48
- Zyxel GS1920-24HP
- Zyxel GS1920-24

Version:

Model	Firmware Version	Boot Version
Zyxel GS1920-48HP	V4.50(AAOA.3) | 05/20/2020	V1.00 | 11/15/2013
Zyxel GS1920-48	V4.50(AANZ.3) | 05/20/2020	V1.00 | 11/15/2013
Zyxel GS1920-24HP	V4.50(AAOC.3) | 05/20/2020	V1.00 | 03/21/2014
Zyxel GS1920-24	V4.50(AAOB.3) | 05/20/2020	V1.00 | 03/21/2014

Enhanced Features:

V4.50(AAxx.3)C0:

1. **[IPv6]** Enable IPv6 Address Auto Configuration by default.
2. **[DHCPv6]** Enable DHCPv6 client mode by default.
3. **[LED]** Users with privilege 3 are allowed to turn on/off Locator LED.
4. **[Neighbor]** Display both IPv4/IPv6 address on neighbor page.
5. **[ZON]** ZON supports IPv6 address.
6. **[WEB]** Apply new login interface.

V4.50(AAxx.2)C0:

1. **[NTP]** NTP Server supports DNS format
2. **[System]** Enhanced dual image resilience
3. **[Security]** SHA2
4. **[IPv6]** Show IPv6 socket
5. **[MGMT]** Logout all current user access after changing the device management IP
6. **[Port]** Display port utilization
7. **[CLI]** Use [Ctrl+C] to escape when executing "show running config, show log"
8. **[NTP]** Time sync (NTP) over IPv6
9. **[Syslog]** Syslog setup for IPv6 and UDP port
10. **[ZDP]** ZDP v1.8.3
11. **[Time]** Time stamp for save configuration
12. **[PoE]** PoE default mode change to consumption mode, and the default config will show consumption mode setting. (PoE model only)
13. **[WEB]** Web login warning page
14. **[Fan]** Smart fan (designed to automatically adjust speed based on device temperature)
15. **[Configuration]** Custom Default configuration
16. **[WEB]** Enhanced GUI with new Zyxel logo
17. **[Multicast]** Avoid multicast group cannot be added while mac collision happens

Bug Fix:

V4.50(AAxx.3)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#180500496
   [NTP] The switch doesn't sync with NTP server properly
4. eITS#180601097
   [System] The switch auto reboot when creating an user with a password of 24 types or configured an SNMPv3.
5. 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.
6. 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.
7. eits#180900583
   [System] Fix switch firmware upgrade issue when the firmware version are more than 2 versions apart.
8. eits#181000788
   [Authentication] Switch sometimes crash when using 802.1x.
9. 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.
10. eITS#190200916
    [Authentication] Switch may be randomly rebooted if dot1x guest VLAN multi-secure mode is enabled.
11. eITS#190201160
    [LLDP] The device will reboot unexpectedly due to LLDP memory leak.
12. eITS#190300525
    [IPv6] Handling IPv6 routing may cause switch crash and reboot.
13. eITS#190500548

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

14. eITS#190500189
    [LLDP] Switch crashes when receiving LLDP packet with incorrect length of TLV.
15. eITS#190800016
    [PoE] PD gets an incorrect allocated power value when Power-via-MDI is enabled along with PoE Max Power.
16. eITS#190800796
    [IPv6] Switch crashes when receiving particular IPv6 MLD packets.
17. eITS#190900353
    [MGMT] Lost IPv6 management when IPv6 MLD snooping proxy is enabled.
18. eITS#191100449
    [MGMT] Switch will randomly warm-reboot after a lot of continuous SSH login.
19. eITS#200200647
    [IPSG] IPv6 DHCP snooping untrusted port is not working.
20. eITS#200500197
    [AAA] HTTP login switch will fail when using RADIUS authentication.

V4.50(AAxx.2)C0:

1. eITS#151200455/ 170200710
   [LLDP] particular Cisco IP phone may release IP (DHCP mode) after every 180 seconds.
2. eITS#151201303
   [SNMP] SNMP GETBULK produces incorrect results when max-repetition is set greater than 55.
3. eITS#160101255
   [LACP] Fail to disable LACP if disable trunk first.
4. eITS#160300698
   [VLAN] Partial configuration loss occurs after configuring private VLAN via web GUI and rebooting switch.
5. eITS#160500852
   [MGMT] GS1920-24HP can upload successfully GS2210's firmware, which will cause GS1920-24HP crash and never boot up properly after rebooting.
6. eITS#160700103
   [Log] Displayed port speed value is always 0 KB/s for both TX and RX.

7. eITS#161100122
   [MGMT] Switch does not check the password with illegal characters.
8. eITS#170100698
   [RSTP] The switch cannot auto adjust RSTP path cost according to the port speed.
9. eITS#170300312
   [MGMT] Change from DHCP to static IP and management VLAN in the same time will lose the static IP setting after DHCP lease time.
10. eITS#170300428
    [PING] Switch has high ping latency periodically due to the routine runtime task.
11. eITS#170500473
    [MGMT] Prevent unexpected reboot caused by Avast antivirus software.
12. eITS#170500863
    [SYSTEM] Switch may encounter unexpectedly reboot under a large IP network environment.
13. eITS#170700931
    [ACL] The permitted traffic will be denied when users set more than 64 classifiers.
14. eITS#171200272
    [IPSG/Port Security] Client traffic is unexpectedly discarded after MAC address aging time when IPSG and port security are enabled.
15. eITS#180100999
    [Maintenance] Switch may miss configuration if upgrades to new firmware.
16. eITS#180200048
    [WEB] Web GUI may display syntax error when restoring configuration.

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]** GS1920 is cluster manager and the cluster member won't upgrade firmware via FTP if firmware size is over than 4.8MB.

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 Entry	16
14.	Trunk groups	16
15.	Per trunk group port number	8
16.	MSTP instance	0-15
17.	MAC-based VLAN	50
18.	Voice VLAN OUI entry	6
19.	ZON neighbor per-port maximum clients	10

Change History:

- V4.50(AAxx.3) | 05/20/2020
- V4.50(AAxx.2) | 02/27/2018
- V4.30(AAxx.0) | 09/16/2015
- V4.10(AAxx.0) | 12/25/2013