



Software Release Note
Switch XGS4600 Series

Date: Dec. 30, 2024

Zyxel Switch XGS4600 Series

V4.70(AB__.5)C0 Release Note

Date: Dec. 30, 2024

This document describes the features in the XGS4600 series for its 4.70(AB__.5)C0 release.

Supported Platforms

Support Platform	Firmware version	Boot Version
Zyxel XGS4600-32	V4.70(ABBH.5)C0	V1.00 09/12/2016
Zyxel XGS4600-32F	V4.70(ABBI.5)C0	V1.00 09/12/2016
Zyxel XGS4600-52F	V4.70(ABIK.5)C0	V1.00 06/08/2017

New Feature and Enhancements

1. Enhance security by forcing users to change the password after first login.
2. Expand NTP servers from 1 to 3.
3. Enhance security by supporting the ECDSA algorithm in SSH.

Bug fix

1. [eITS#220900092] Fixed OpenSSH related vulnerabilities. [CVE-2010-5107][CVE2015-5600][CVE-2016-6515].
2. [eITS#221001400] If the MAC address limit of port-security has reached, the port still cannot learn any MAC address after any link reset related (ex. port test, cable, diagnostic, or physical link up/down).

3. [eITS#221100146] LACP configuration may leads switch not handle the 802.1x authentication.
4. [eITS#221101240] Fix recording syslog may cause memory leak.
5. [eITS#221101132] After restoring config via SFTP may cause fail due to syntax error.
6. Fixed crash issue when receive an unexpected HTTPs request content.
7. [eITS#221201201] Getting logging information that contains special characters causes switch hang.
8. [eITS#230301533] Fixed reading mib zyxellpsgInfoTable fail.
9. [eITS#230301330] Fixed failing to import certificate while the file size is over 5k.
10. [eITS#230400140] [eITS#231000816] Fixed switch crashed issues that is caused by Nessus version 10.5.1 to scan SSH.
11. [eITS#230400154] Fixed failing to delete inactive classifiers even though they are not bound to any policies.
12. The fixed policy route does not adhere to the configured VID setting.
13. Fixed incorrect swif0 interface counter in standard IfEntry MIB.
14. [eITS#230801140] Fixed crash issue when enabling IPv6 and receiving an IPv6 NA packet.
15. Fixed switch crash issue caused by receiving LLDP packets with over chassis ID lengths.
16. [eITS#231001888] Fixed fail to add policy rule issue when binding the second classifier containing the same socket range as the first one
17. [eITS#240100009] Fixed memory leak issue causing packet switching failure when the switch configures a non-existent IPv6 gateway and receives numerous unknown IPv6 packets.
18. [eITS#231201249] Fixed switch may reboot automatically when receiving IPv6

packets.

19. [eITS#240401365] Switch web GUI should not allow setting different media types on link aggregation ports.
20. [eITS#240300246] The switch hangs when an IPv6 client roams.
21. [eITS#240501702] Fixed device IP address and uplink usage are not displayed correctly on Nebula.
22. [eITS#240601476] Continuously collecting the tech support file may cause the device to crash.
23. [eITS#240801076] Using SNMPwalk to query the Q-Bridge MIB will return incorrect values when voice VLAN is enabled on the device.
24. [eITS#240801706] Fixed the client could not obtain an IP address if the same IP address was configured in the IPSG static binding table.
25. [eITS#241001395] IPSG with IPv6 has lease time of only 10 seconds.
26. [eITS#241100538] Fix special characters(space, ' ,") can be allowed in username to cause configuration error.
27. [eITS#241100288] MSTP root guard cannot prevent the RSTP Superior SW from preempting the Root.
28. [eITS#220500960] Disabling 802.1x or guest VLAN functionality on other ports will cause the authenticated clients to disconnect and require re-authentication.

Known Issue

1. ACL policy rule's priority and queue action should be combined
2. RIP/OSPF only can learn 11968 routing entry
3. ACL cannot support Configuration update Layer 4 socket port range when using IPv6.
4. 10G port throughput can't reach full rate when the traffic is go through stacking port due to IC limitation. (Stacking mode only)
5. Flow control does not support traffic cross stacking devices. (Stacking mode only)
6. CA only import on master device. When master down, HTTPs session is insecurity.

Note: Please import CA on all switches before connecting the cable for stacking.

Limitation of Settings:

Limitation of Setting	Cloud	Standalone
1. Cluster member	-	24
2. Max stacking device	-	4
3. VLAN 1Q static entry	-	4K
4. Static MAC forwarding entry	-	256
5. MAC filtering entry	-	256
6. IP routing domain	-	256
7. IGMP Filtering entry	-	256
8. IGMP MVR entry	-	256
9. VRRP entry	-	64
10. Protocol based VLAN entries per port	-	7
11. Port-security max address-limit number	-	32K
12. DHCP Server	-	16
13. Syslog server entry	-	4
14. IP source guard entry	-	1K
15. IP subnet based VLAN entry	-	16
16. MVR VLAN entry	-	5
17. VLAN-stacking Selective QinQ entry	-	1K
18. VLAN-mapping entry	-	1K
19. MAC table	-	32K
20. Routing table	-	12K
21. DHCP snooping binding table	-	16K
22. Multicast group	-	1k
23. ACL	-	1K
24. Policy route	-	64
25. DHCP option 82 profile	-	130
26. Remote port monitoring vlan	-	10
27. Static ARP entry	-	256
28. Static route max entry	-	64
29. MAC-based VLAN	-	1024
30. Voice VLAN OUI entry	-	10
31. ZON neighbor per-port maximum clients	-	10
32. IPv6 source guard binding table	-	100

Limitation of Setting	Cloud	Standalone
33. WOL entry	-	32
34. L3 forwarding table (IPv4/IPv6)	-	8K/4K
35. Trunk groups (32/32F/52F)	-	Standalone: 16/16/26 Stacking: 48/48/48

Change History

- V4.70(AB__.5) | 12/30/2024
- V4.70(AB__.4) | 11/01/2022
- V4.70(AB__.3) | 04/29/2022
- V4.70(AB__.2) | 12/17/2021
- V4.70(AB__.1) | 03/10/2021
- V4.70(AB__.0) | 01/20/2021
- V4.60(AB__.0) | 03/15/2019
- V4.50(AB__.1) | 09/12/2017
- V4.50(AB__.0) | 07/27/2017
- V4.40(AB__.2) | 06/12/2017
- V4.40(AB__.1) | 12/28/2016