

# ZYXEL

## **Software Release Note Switch XGS2210 Series**

Date: October 31, 2022

# Zyxel Switch XSG2210 Series

## V4.70(AAZ\_.2)C0 Release Note

**Date: October 24, 2022**

---

This document describes the features in the XSG2210 series for its 4.70(AAZ\_.2)C0 release.

### Supported Platforms

---

Support Platform	Firmware version	Boot Version
Zyxel XSG2210-28	V4.70(AAZJ.2)C0	V1.00   01/25/2016
Zyxel XSG2210-28HP	V4.70(AAZK.2)C0	V1.00   01/25/2016
Zyxel XSG2210-52	V4.70(AAZL.2)C0	V1.00   01/25/2016
Zyxel XSG2210-52HP	V4.70(AAZM.2)C0	V1.00   01/25/2016

### New Feature and Enhancements

---

None

### Bug fix

---

1. [Vulnerability] Vulnerability protection for unauthenticated Denial-of-Service (DoS) by RpAnalyzeHttpRequest.
2. [eITS#210701300] Switch supports IGMPv3 packet for source-type of "block source" parameter.
3. [eITS#210901026] Port setup cannot be configured after setting flow-control on any static link aggregated ports by GUI.
4. [eITS#220300572] In stacking mode, if DAC cables are connected to switch stacking ports before rebooting or power up, switch won't boot up successfully.
5. [eITS#220500960] Enabling and disabling 802.1x or Guest VLAN on an unauthenticated or empty switch port causes all authenticated ports to disconnect.
6. [eITS#220700265] Firmware upgrade fails when the policy rule is bound to multiple classifiers.

- [eITS#220900301] [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).

## Known Issue

---

- ACL policy rule's priority and 802.1p queue (in Basic setting -> Port Setup) action should be combined to take effect.
- The cable diagnostic tolerance is +-10M length.
- Flow control doesn't support traffic cross stacking devices.
- Fiber ports cannot support port speed mode: Auto-Negotiation 1000M.
- DHCP Snooping VLAN Port profile displays 4094 entries at most in web page.
- Strongly recommend not to downgrade firmware from 4.40 to 4.30, to avoid Stacking status and the reloading configuration process abnormal.

## Limitation of Settings:

---

Limitation of Setting	Cloud	Standalone
1. 802.1Q Static VLANs	-	1K
2. Static MAC forwarding entry	-	256
3. MAC filtering entry	-	256
4. Cluster member	-	24
5. IP interface	-	32
6. IGMP Filtering entry	-	256
7. IGMP MVR entry	-	256
8. Protocol based VLAN entries per port	-	7
9. Port-security max address-limit number	-	16K
10. Syslog server entry	-	4
11. IP source guard entry	-	512
12. IP subnet based VLAN entry	-	16
13. MVR VLAN entry	-	5
14. MAC table	-	16K
15. DHCP snooping binding table	-	16K

Limitation of Setting	Cloud	Standalone
16. Multicast group	-	1k
17. ACL	-	384
18. DHCP option 82 profile	-	130
19. static arp entry	-	256
20. Static route max entry	-	64
21. DHCP Entry	-	16
22. Trunk groups	-	12/24
23. Per trunk group port number	-	8
24. MSTP instance	-	0-16
25. MAC-based VLAN	-	512
26. Voice VLAN OUI entry	-	10
27. IPv6 source guard binding table	-	100
28. L3 forwarding table	-	1K

## Change History

---

- V4.70(AAZ\_.2) | 10/24/2022
- V4.70(AAZ\_.1) | 06/17/2021
- V4.70(AAZ\_.0) | 01/20/2021
- V4.50(AAZ\_.2) | 05/08/2020
- V4.50(AAZ\_.1) | 05/22/2019
- V4.50(AAZ\_.0) | 08/11/2017
- V4.40(AAZ\_.0) | 10/26/2016
- V4.30(AAZ\_.0) | 03/02/2016