ZYXEL

Software Release Note
NebulaFlex Switch XMG1930 Series

Date: January 16, 2023

Zyxel NebulaFlex Switch XMG1930 Series

V4.80(ACA_.0)C0 Release Note

Date: January 16, 2023

This document describes the features in the XMG1930 series for its 4.80(ACA_.0)C0 release.
XMG1930 series is a hybrid switch with NebulaFlex technology to support operation in either Standalone mode or Nebula cloud management mode.

Supported Platforms

Support Platform	Firmware version	Boot Version
Zyxel XMG1930-30	V4.80(ACAR.0)	V1.00 | 02/10/2022
Zyxel XMG1930-30HP	V4.80(ACAS.0)	V1.00 | 02/10/2022

New Feature and Enhancements

	New Feature and Enhancement	Cloud	Standalone
1.	Support Access Layer 3 license.*1	-	V
2.	Renovate Web GUI layout for better usability of Switch management.	V	V
3.	Intuitive Cloud connection status with help message.	V	V
4.	Strengthen security for network management with built-in notification in case of abnormal login attempt.	V	V
5.	Supports "Account Security" option on WEB GUI to encrypt admin / user	-	V

	account password and options to display user/AAA/SNMP credentials.		
6.	Support Auto configuration recovery on Nebula to prevent loss connection with NCC by misconfiguration.	V	-
7.	Log information for IP conflict between Switch and gateway both obtain the same IP address.	V	V
8.	Allow to change the IP address from DHCP to static type directly for Layer 3 switch.	-	V
9.	Support user uses “setup.zyxel.com” directly to access local web GUI.	V	V
10.	Supports auto STP path cost which will determine path cost by the port's current link speed.	-	V
11.	Nebula Switch supports SSH connection to access command line for advanced features.*2	V	V
12.	Support MAC authentication by cloud authentication on NCC.	V	-
13.	Strengthen user security with the encryption of TACACS+ & Radius shared secret.	-	V
14.	Support dynamic VLAN assignment through 802.1x authentication.	V	V
15.	Extend RADIUS server support range from IPv4 to IPv6.	-	V
16.	Enhance Guest VLAN to isolate broadcast packets between VLANs.	-	V
17.	[eITS#220801409] Extend the PD negotiation time limit on Legacy and Force-802.3AT mode to improve PoE compatibility.	V	V

18.	Power-up mode supports extending Power via MDI for IEEE 802.3BT.	V	V
19.	PoE scheduling still works even if the switch is disconnected from the NCC.	V	-
20.	The interval time of Loop errdisable recovery can be configured now.	V	V
21.	Support IGMP Report Proxy setting.	V	V
22.	Provide the Nebula password reminder on login page of web GUI.	V	-
23.	NCC discovery adds reminder to save configurations.	-	V
24.	Add note on cable diagnostics to inform the operating limits for local web GUI.	-	V
25.	Provide time-stamp on filename title when backup configuration file.	V	V
26.	Support logs to indicate the cause of CPU high.	V	V
27.	The year of Time Range page starts with current system time.	V	V

*1: Please refer to User guide chapter 1.1.1 for getting more detail

*2: Configure mode is standalone license only.

Bug fix

	Bug fix	Cloud	Standalone
1.	[eITS #220900092] Fix multiple security vulnerabilities regarding OpenSSH issues. (CVE-2015-5600, CVE-2016-6515, CVE-2010-5107)	V	V
2.	[eITS #220500960] Disabling 802.1x or guest VLAN functionality on other ports	V	V

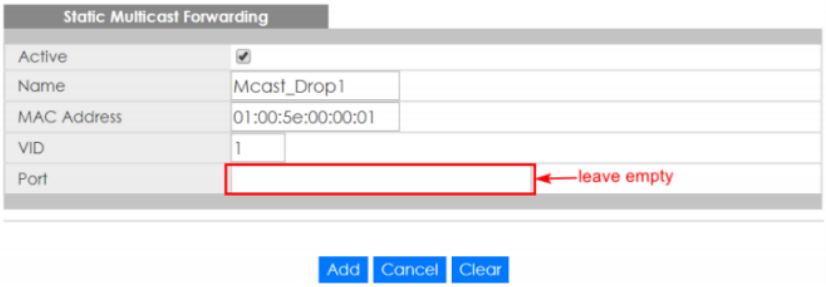
	will cause the authenticated clients to disconnect and require re-authentication.		
3.	[eITS #220601396] When VLAN list use "," to segment VLAN range in policy rule, some VLAN drop rules will not apply successfully.	-	V
4.	[eITS #220700265] Firmware upgrade fails when the policy rule is bound to multiple classifiers.	-	V
5.	[eITS #221100146] LACP configuration may leads switch not handle the 802.1x authentication.	V	V
6.	[eITS #221101132] After restoring config via SFTP may cause fail due to syntax error.	V	V
7.	[eITS #221101240] Fix recording syslog may cause memory leak.	V	V
8.	Fix the IGMP unknown multicast drop cannot operate on group "224.0.1.x" and "239.x.x.x" for IPv4.	V	V

Known Issue

	Known Issue	Cloud	Standalone
1.	Link aggregation only can use 2 criteria at the same time. Trunks using the third criteria won't link up.	-	V
2.	Force 100M will not link up when connecting a straight-through RJ45 cable, please use crossover cable.	V	V
3.	When EEE is enabled, frame lost via EEE port, which fixed speed at 5G or 2.5G.	-	V
4.	The link LED will turn on when plug-in SFP-100TX or SFP-1000T while cable is	V	V

	not connected.		
5.	The switch cannot access cluster member when cluster member's password been encrypted.	-	V
6.	The accuracy of cable diagnostic is +-15m. When without cables, the value of distance to fault would not be 0.	V	V
7.	When auto-negotiation fails or recovery occurs, the switch does not record syslog nor send out SNMP traps.	V	V
8.	[MIB]Get "dot1qTpGroupEgressPorts" and "dot1qTpGroupLearnt" are empty.	V	V
9.	Unknown multicast drop cannot operate on group "0000:00xx", "ff0x::db8:0:0/96" for IPv6. Recommended work around solution is to create static Multicast Forwarding entry with empty port for each multicast group that needs to be filtered.	-	V

* Example to setup Static Multicast Forwarding entry with empty port:



Limitation of Settings:

	Limitation of Setting	Cloud	Standalone
1.	802.1Q Static VLANs	1K	1K

2.	Static MAC forwarding entry	-	256
3.	MAC filtering entry	256	256
4.	Static ARP entry	-	256
5.	MAC table	16K	16K
6.	IP Address table	-	512
7.	Multicast group	1K	1K
8.	ACL	128	256
9.	IPv4 Static route max entry	32	32
10.	IPv6 Static route max entry	-	32
11.	IPv4 interface	32	32
12.	IPv6 interface	-	32
13.	Trunk groups	15	15
14.	Per trunk group port number	8	8
15.	MSTP instance	-	0-16
16.	IGMP snooping unknown multicast drop VLAN	8	8
17.	IGMP snooping unknown-multicast-frame querier-port forwarding maximum VLAN	8	8

Change History

- V4.80(ACA_.0) | 01/16/2023
- V4.70(ACA_.2) | 01/09/2023
- V4.70(ACA_.1) | 09/01/2022
- V4.70(ACA_.0) | 03/25/2022