ZYXEL

Software Release Note
NebulaFlex Switch XS1930 Series

Date: Dec. 26, 2022

Zyxel NebulaFlex Switch XS1930 Series

V4.80(AB__.0)C0 Release Note

Date: December 26, 2022

This document describes the features in the XS1930 series for its 4.80(AB__.0)C0 release.
XS1930 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 XS1930-10	V4.80(ABQE.0)C0	V1.00 | 08/26/2019
Zyxel XS1930-12HP	V4.80(ABQF.0)C0	V1.00 | 08/26/2019
Zyxel XS1930-12F	V4.80(ABZV.0)C0	V1.00 | 03/12/2021

New Feature and Enhancements

	Feature	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 account password and options to display user/AAA/SNMP credentials.	-	V
6.	Support auto configuration recovery on Nebula to prevent loss connection with NCC by misconfiguration.	V	-

	Feature	Cloud	Standalone
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.	V	V
21.	Support IGMP Report Proxy setting.	V	V

Feature	Cloud	Standalone
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 #211100996] Compound authentication loose mode combined with MAC-authentication should allow traffic to proper VLAN upon authentication approval, it currently moves all traffic to guest VLAN regardless of authentication status.	-	V
3. [eITS #220400279] Switch may not display LAN IP on Nebula CC.	V	-
4. [eITS #220400686] Networked AV mode wizard allow user to set different VLAN interface with same IP address.	-	V

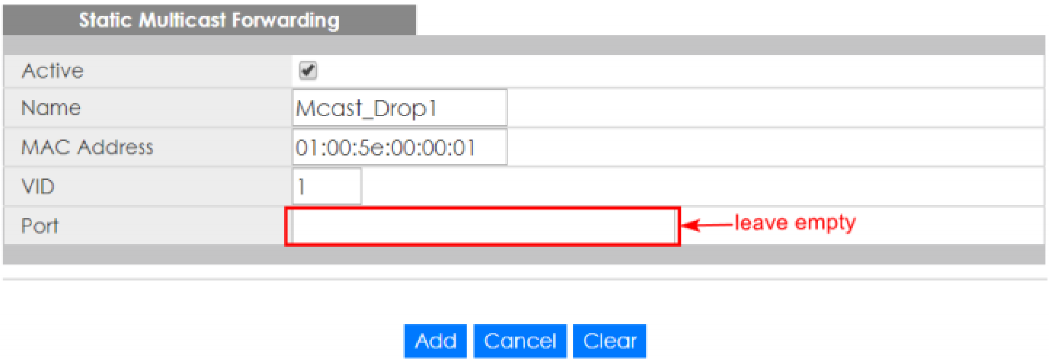
	Bug fix	Cloud	Standalone
5.	[eITS #220500960] Disabling 802.1x or guest VLAN functionality on other ports will cause the authenticated clients to disconnect and require re-authentication.	V	V
6.	[eITS #220601396] When VLAN list use “,” to segment VLAN range in policy rule, some VLAN drop rules will not apply successfully.	-	V
7.	[eITS #220700265] Firmware upgrade fails when the policy rule is bound to multiple classifiers.	-	V
8.	[eITS #221100146] LACP configuration may leads switch not handle the 802.1x authentication.	V	V
9.	[eITS #221101132] After restoring config via SFTP may cause fail due to syntax error.	V	V
10.	[eITS #221101240] Fix recording syslog may cause memory leak.	V	V
11.	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

	Known Issue	Cloud	Standalone
3.	Ingress rate limit of TCP traffic is inaccurate when value limits above 300M.	V	V
4.	The accuracy of cable diagnostic is +-15m. When without cables, the value of distance to fault would not be 0.	V	V
5.	When EEE is enabled, frame lost via EEE port, which fixed speed at 5G or 2.5G	-	V
6.	The link LED will turn on when plug-in SFP-100TX or SFP-1000T while cable is not connected.	V	V
7.	When set port speed auto and the peer port is force 100Mbps, the link will up at 10Mbps Half	V	V
8.	The switch cannot access cluster member when cluster member's password been encrypted.	-	V
9.	When auto-negotiation fails or recovery occurs, the switch does not record syslog nor send out SNMP traps.	V	V
10.	[MIB]Get "dot1qTpGroupEgressPorts" and "dot1qTpGroupLearnt" are empty.	V	V
11.	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:



Active	☑
Name	Mcast_Drop1
MAC Address	01:00:5e:00:00:01
VID	1
Port	

leave empty

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	512
7.	Multicast group	10: 256 12HP/12F: 1K	10: 256 12HP/12F: 1K
8.	IPv4 ACL	128	128
9.	IPv6 ACL	-	128
10.	IPv4 Static route max entry	32	32
11.	IPv6 Static route max entry	-	32
12.	IPv4 interface	32	32
13.	IPv6 interface	-	32
14.	Trunk groups	10: 5 12HP/12F: 6	10: 5 12HP/12F: 6
15.	Per trunk group port number	8	8
16.	MSTP instance	-	0- 16
17.	IGMP snooping VLAN	16	16
18.	IGMP snooping unknown multicast drop VLAN	8	8
19.	IGMP snooping unknown-multicast-frame querier-port forwarding maximum VLAN	8	8

Change History

- V4.80(AB__.0) | 12/26/2022
- V4.70(AB__.4) | 06/30/2022
- V4.70(AB__.3) | 05/06/2022
- V4.70(AB__.2) | 03/08/2022
- V4.70(AB__.1) | 12/22/2021
- V4.70(AB__.0) | 09/08/2021
- V4.60(ABQ_.5) | 04/08/2021
- V4.60(ABQ_.4) | 01/20/2021
- V4.60(ABQ_.2) | 09/29/2020
- V4.60(ABQ_.1) | 05/11/2020
- V4.60(ABQ_.0) | 01/14/2019