www.zyxel.com

ZYXEL

XMG8825-B50A
Generic

Firmware Release Note

V5.17(ABMT.5)C0

Date: Jan 28, 2021
Author: Ryan Yeh
Reviewer:

TABLE OF CONTENTS

Revision History

Date	Release	Author	Description
2018/07/06	1.0	Linda Huang	V5.13(ABMT.0)b1
2018/08/17	1.1	Linda Huang	V5.13(ABMT.0)b2
2018/09/14	1.2	D. Wolf Huang	V5.13(ABMT.0)b3
2018/10/12	1.3	D. Wolf Huang	V5.13(ABMT.0)b4
2018/10/12	1.4	D. Wolf Huang	V5.13(ABMT.0)b4_D0
2018/10/31	1.5	D. Wolf Huang	V5.13(ABMT.0)C0
2018/10/31	1.6	D. Wolf Huang	V5.13(ABMT.0)D0
2018/11/01	1.7	D. Wolf Huang	V5.13(ABMT.0)D1
2018/11/20	1.8	D. Wolf Huang	V5.13(ABMT.0)D2
2018/11/30	1.9	D. Wolf Huang	V5.13(ABMT.1)b1
2019/02/22	2.0	D. Wolf Huang	V5.13(ABMT.1)b2
2019/03/19	2.1	D. Wolf Huang	V5.13(ABMT.1)C0
2019/03/21	2.2	D. Wolf Huang	V5.13(ABMT.1)D0
2019/03/27	2.3	D. Wolf Huang	V5.13(ABMT.1)D1
2019/05/31	2.4	D. Wolf Huang	V5.13(ABMT.2)b1
2019/08/06	2.5	D. Wolf Huang	V5.13(ABMT.3)b1
2019/10/04	2.6	D. Wolf Huang	V5.13(ABMT.3)b2
2019/11/19	2.7	D. Wolf Huang	V5.13(ABMT.3)b3
2019/12/11	2.8	D. Wolf Huang	V5.13(ABMT.3)b4
2020/01/14	2.9	Emily Chang	V5.13(ABMT.3)b5
2020/01/17	3.0	D. Wolf Huang	V5.15(ABMT.4)b1
2020/03/05	3.1	D. Wolf Huang	V5.15(ABMT.4)b2
2020/03/05	3.2	D. Wolf Huang	V5.15(ABMT.4)b2_D0
2020/03/10	3.3	D. Wolf Huang	V5.15(ABMT.4)b3
2020/03/10	3.4	D. Wolf Huang	V5.15(ABMT.4)b3_D0
2020/03/27	3.5	D. Wolf Huang	V5.15(ABMT.4)b4
2020/03/27	3.6	D. Wolf Huang	V5.15(ABMT.4)b4_D0
2020/05/08	3.7	D. Wolf Huang	V5.15(ABMT.4)b5_D0
2020/06/05	3.8	D. Wolf Huang	V5.17(ABMT.5)b1
2020/08/28	3.9	D. Wolf Huang	V5.17(ABMT.5)b2
2020/09/25	4.0	Wilbur Lu	V5.17(ABMT.5)b3
2020/10/28	4.1	Wilbur Lu	V5.17(ABMT.5)b4

2021/01/28	4.2	Ryan Yeh	V5.17(ABMT.5)b5
2021/01/28	4.3	Ryan Yeh	V5.17(ABMT.5)C0

Zyxel XMG8825-B50A Generic V5.17(ABMT.5)C0 Release Note

Date: Jan 28, 2021

Supported Platforms:

Zyxel XMG8825-B50A
Zyxel XMG3927-B50A
Zyxel VMG3927-B50A
Zyxel VMG3927-B60A
Zyxel VMG8825-B50A
Zyxel VMG8825-B60A

Versions:

Bootbase Version: V1.62 | 07/17/2020 13:47:29
Firmware version : V5.17(ABMT.5)C0
Kernel version: 4.1.52
Annex A/B DSL modem code version: A2pvfbH045o/B2pvfbH045o
DSL driver version: d27j
BRCM WLAN code version: 7.14.170.43
3G dongle WWAN package version: 1.20
EasyMesh: 3.0
WX3401-B0 : V5.17(ABVE.0)b5
MPro APP :
iOS: V2.1.0.200814.2
Android: 2.1.0.200814

Notes:

Bsa version command : bsa_cli version
uname –a
adsl --version
wl ver

wwanpackage info

Default Settings in Firmware

- Refer to the *.rom in the fw release package.
- Please use the website http://jsoneditoronline.org/ to open the *. rom.

Public Domain Software Announcements

Open Source Used In Product	Version	From (Source)	License Terms	Modified / Used
ares	1.1.1	ftp://athena-dist.mit.edu/pub/ATHENA/ares	OTHER	Modified
atftp	0.7.1	https://sourceforge.net/projects/atftp/	GPLv2	Modified
bridge-Utils	1.5	https://git.kernel.org/pub/scm/linux/kernel/git/shemminger/bridge-utils.git/	GPLv2	Modified
busybox	1.20.1	https://busybox.net/	GPLv2	Modified
bwm	1.1.0.org	ftp://ftp.sangoma.com/linux/utilities/	GPLv2	Used
clinkc	2.4	https://sourceforge.net/projects/clinkc/	BSD	Modified
conntrack-tools	1.4.3	https://git.netfilter.org/conntrack-tools/	GPLv2	Used
dnsmasq	2.78	http://www.thekelleys.org.uk/dnsmasq/doc.html	GPLv2/GPLv3	Modified
dropbear	2018.76	https://github.com/mkj/dropbear	MIT	Modified
ebtables	2.0.10-4	https://git.netfilter.org/ebtables/	GPLv2	Modified
eventlog	0.2.10	https://github.com/balabit/eventlog	BSD	Used
expat	1.95.8	https://github.com/libexpat/libexpat	MIT	Used
ez-ipupdate	3.0.11b8	http://ez-ipupdate.com/	GPLv2	Modified
gettext	0.16.1	http://www.gnu.org/software/gettext/	GPLv2	Used
glib	2.37.7	http://www.gtk.org/	LGPLv2	Used
iproute2	2.6.33	https://github.com/shemminger/iproute2	GPLv2	Modified
iptables	1.4.16.3	https://git.netfilter.org/iptables/	GPLv2	Modified
jpegsrc	v9a	http://www.ijg.org/	IJG	Used
json-c	0.13.1	https://github.com/json-c/json-c/downloads	MIT	Modified
libedit	20080712-2.11	http://pkgs.fedoraproject.org/repo/pkgs/libedit/libedit-20080712-2.11.tar.gz/	BSD	Modified
libffi	3.0.11	http://pkgs.fedoraproject.org/repo/pkgs/libffi/libffi-3.0.11.tar.gz/	MIT	Used
libiconv	1.11.1	http://www.gnu.org/software/libiconv/	LGPLv2	Modified
libnetfilter_conntrack	1.0.4	https://git.netfilter.org/libnetfilter_conntrack/	GPLv2	Used
libnetfilter_ct	1.0.0	https://netfilter.org/about.html	GPLv2	Modified

helper				
libnetfilter_ctti meout	1.0.0	https://netfilter.org/about.html	GPLv2	Modified
libnetfilter_qu eue	1.0.2	https://git.netfilter.org/libnetfilter_queue/	GPLv2	Used
libnfnetlink	1.0.1	https://git.netfilter.org/libnfnetlink/	GPLv2	Used
libnl-tiny	0.1	https://github.com/openwrt/openwrt/tree/master/package/libs/libnl-tiny	GPLv2/LGPLv2.1	Used
libpcap	1.1.1	www.tcpdump.org	BSD	Used
libsrtp	1.4.2	https://github.com/cisco/libsrtp	BSD 3Clauses	Modified
libtool	2.4	http://www.gnu.org/software/libtool/	GPLv2	Used
libusb	1.0.9	https://sourceforge.net/projects/libusb/	LGPL 2.1	Used
Linux/MIPS Kernel	4.1.51	http://www.linux-mips.org	GPLv2	Modified
logrotate	3.7.1	https://launchpad.net/ubuntu/hardy/i386/logrotate/	GPLv2	Modified
mailsend	1.17b15	https://github.com/muquit/mailsend/	BSD	Modified
nbtscan	1.5.1a	http://www.inetcat.org/software/nbtscan.html	GPLv2	Modified
ncurses	5.7	http://ftp.gnu.org/pub/gnu/ncurses/	MIT	Modified
net-snmp	5.8	http://www.net-snmp.org/	ISC/BSD	Modified
ntfs-3g	2013.1.13	http://ntfs-3g.org	GPLv2/LGPLv2	Used
ntpclient	2007_365	http://doolittle.icarus.com/ntpclient/	GPLv2	Modified
openssl	1.0.2n	http://www.openssl.org	OpenSSL	Modified
popt	1.16	http://rpm5.org/files/popt/	MIT	Modified
ppp	2.4.3	http://www.roaringpenguin.com/pppoe	GPLv2/BSD	Modified
pure-ftpd	1.0.30	http://pureftpd.org	ISC/BSD	Modified
radvd	1.8	http://www.litech.org/radvd/	BSD	Used
readline	5.2	http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html	GPLv2	Used
samba	3.6.25	http://www.samba.org/samba/	GPLv3	Modified
sqlite	3.6.23.1	http://www.sqlite.org/	Public Domain License	Used
syslog-ng	2.0.10	https://github.com/balabit/syslog-ng	GPLv2	Used
tcpdump	4.2.1	http://www.tcpdump.org/	BSD	Used

udhcp	0.9.8	http://udhcp.busybox.net/	GPLv2	Modified
updatedd	2.6	https://sourceforge.net/projects/updatedd/	GPLv2	Modified
usb-modeswitch	2.1.0	http://www.draisberghof.de/usb_modeswitch/	GPLv2	Used
util-linux	2.21.2	https://github.com/karelzak/util-linux/	GPLv2	Used
wide-dhcpv6	20080615	https://sourceforge.net/projects/wide-dhcpv6/	BSD	Modified
zebra	0.93a	http://www.zebra.org/	GPLv2/LGPLv2	Used
zlib	1.2.7	https://github.com/madler/zlib	zlib	Used

Known issues

1. Device will not send the beacon at channel 100 in shielding box/room. Some of configuration skip channel 100 first.

Modifications in 5.17(ABMT.5)C0

Modifications in 5.17(ABMT.5)b5

[FEATURE ENHACEMENT]

[BUG FIX]

1. [GUI] Vulnerability issue via Export_Log.
2. [Vulnerability] Arbitrary remote code execution (RCE) on the device through an HTTP request.
3. [Vulnerability] Unauthenticated Denial-of-Service effectively disabling the device's web-interface.
4. [Security] DLNA vulnerability.
5. [#210100697][System] Supervisor password does not work from WAN side after upgrade
6. [#201000137] RP FAILURE
7. Root shell obtained on the box
8. No restrictions on automount USB drive
9. [#201101559] MCS / throughput issue on WX3401 - XIAOMI,+ SAMSUNG
10. [#201201005] WX3401-B0 loses backhaul

Modifications in 5.17(ABMT.5)b4

[FEATURE ENHACEMENT]

[BUG FIX]

1. [NAT] CPE hang and show "Invalid memory segment access" when add an address mapping rule with interface "Default" then reboot CPE.

Modifications in 5.17(ABMT.5)b3

[FEATURE ENHACEMENT]

[BUG FIX]

1. [Security] WOL command injection
2. buffer overflow when upgrade FW

Modifications in 5.17(ABMT.5)b2

[BUG FIX]

1. [Security] ACL rules with scheduler does not work
2. [DDNS] Input empty characters of Username will cause CPE crash
3. [UPnP] Run XBOX application, UPnP cannot open ports automatically.

Modifications in 5.17(ABMT.5)b1

[FEATURE ENHACEMENT]

4. [#191100506]Option 61 Identifier unique for each device
5. [#200100461]Updated JSON file with modifications for Czech language
6. [#200106890]RFC 7599- Mapping of Address and Pomprt using Translation (MAP-T) and RFC 7597-Mapping of Address and Port with Encapsulation (MAP-E)
7. [#200200772]RFC 7599- Mapping of Address and Pomprt using Translation (MAP-T) and RFC 7597-Mapping of Address and Port with Encapsulation (MAP-E)
8. [#191200210]OPAL Support Device.ManagementServer.InformParameter.{i}.
9. [#191200262]OPAL Support user_startup_parameters.sh
10. [#200300859]VMG8825, TR69 watchdog log

11. OPAL Regular Q1Y20 b1_Key feature
12. OPAL Release_Remove WLAN schedule

[BUG FIX]

1. [#190900425]Device.X_ZYXEL_LoginCfg.LogGp.i.Account.i.RemoteAccessPrivilege doesn't work
2. [#190900457]The bridge client cannot run IGMP server if If Con-current WAN use PPPoE + bridge.
3. [#200100462]Other modifications for Czech language which are not available in JSON file
4. [#200100533]WAN interface with VLAN ID and default Gateway
5. [#191200311]Config DHCP client option42 on non-default interfaces
6. [#200201333]Parental control in Turkish language display incorrect
7. [#200201334]The Default of parental control in card page and advance page are not consistent
8. [#200105375]SIP NAT Problem
9. [#200300675]{Security Vulnerability] - Kr00k with BRCM/Cypress wifi chipset - Zyxel Uk
10. [#200401166]Encapsulation Type - GUI option ADSL over ATM, VDSL over PTM
11. [#200401236]VMG8825, PeriodicInformTime via CLI

Modifications in 5.15(ABMT.4)b5_D0

[BUG FIX]

1. Sometimes 5G signal will disappear when Extender connects to wifi backhaul.

Modifications in 5.15(ABMT.4)b4_D0

Based on V5.15(ABMT.4)b4 to release V5.15(ABMT.4)b4_D0

Modifications in 5.15(ABMT.4)b4

[FEATURE ENHACEMENT]

1. Parental Control page is the same as Card page

2. Add Home Security page in Security submenu

Modifications in 5.15(ABMT.4)b3_D0

Based on V5.15(ABMT.4)b3 to release V5.15(ABMT.4)b3_D0

Modifications in 5.15(ABMT.4)b3

[BUG FIX]

1. XMG3927 add extender will cause ""zyMAPSteer" daemon to Disappear

Modifications in 5.15(ABMT.4)b2_D0

Based on V5.15(ABMT.4)b2 to release V5.15(ABMT.4)b2_D0

Modifications in 5.15(ABMT.4)b2

[FEATURE ENHACEMENT]

1. Upgrade xDSL driver to A2x027e and phy code to X2pvfbH045k

[BUG FIX]

1. [eits #200200664] an admin account cannot backup trust domain info.

Modifications in 5.15(ABMT.4)b1

1. First firmware release

Modifications in 5.13(ABMT.3)b5

[BUG FIX]

1. System will dead lock a period of time.

Modifications in 5.13(ABMT.3)b4

[BUG FIX]

1. [#191100008]The Select Interfaces display abnormal when modify Interface grouping
2. [QoS] Qos classification cannot work well after reboot
3. [WAN] In PPPoE mode, MTU can't set 1500.

4. [Multy Pro_Agent] APP should not be used Net Access Schedle rule when CPE F-Secure is enable

Modifications in 5.13(ABMT.3)b3

[FEATURE ENHACEMENT]

1. [#190500612] DHCP option 43 enabled by default
2. [#190901023] FRQ VMG8825-B50B QoS / static route ro interface "drop"
3. [#191000125] EMG3525 Include GenXML utility in firmware
4. [#191000127] EMG3525 Multiple Ethernet WAN-interfaces without VLAN-tag
5. [#191100119] Language Settings : modify languages option
6. Home Cybersecurity

[BUG FIX]

1. [#190500035] VMG8825 zcmd reach the maximum number of instant, will loop endless.
2. [#190900750] Listing processes on console might output pppd auth params
3. [#190900794] Listing processes on console might output pppd auth params
4. [#191000575] XML GPV InternetGatewayDevice.LANDevice.1.LANHostConfigManagement.IPInterface.1.X_ZYXEL_DHCPv6Server.IANAPrefixes
5. [#191001109] VMG3625-T20A can't import trusted CA

Modifications in 5.13(ABMT.3)b2

[FEATURE ENHACEMENT]

1. [#190500597] OPAL Generic Feature Request for GMT timezoe of Turkey
2. [#190800211] TR069 watchdog relaunch

[BUG FIX]

1. [#190400662] DS Lite support DHCP option 64 configuration

2. [#190600041] VMG8623-T50B - VoIP - Outgoing calls dropped when the callee pick up the phone
3. [#190600082] GUI page will try to connect to a unnecessary javascript/css
4. [#190700379] Multiple TCP-based remote denial of service vulnerabilities
5. [#190700496] USB File Sharing case-sensitive issue
6. [#190800137] Pen Test Results - IZyShell Privilege Escalation
7. [#190800234] Pen test results - Vulnerable software packages - Risk [Various - See CVE score]
8. [GUI] GUI description doesn't meet with latest OPAL ES
9. [USB] GUI display a strange blank folder on Share Directory List.

Modifications in 5.13(ABMT.3)b1

[FEATURE ENHACEMENT]

1. [eITS #181200595] Support phones hook-state (on-hook/off-hook) in the web VoIP Status page.
2. [eITS #190400092] Support IGMP log on system log.
3. [eITS #190400662]Support DHCPv6 option64 for IPv6 DS-Lite
4. [eITS #190400939] Support disable LEDs function in GUI.
5. [eITS #190500612] Enable DHCP option 43 by default
6. [eITS #190500747] Support Portuguese GUI.
7. [eITS #190500597] Support Turkey GUI.
8. [eITS #190500025] Separate LAN/WLAN as different column in remote management page.
9. [eITS #190700652] Support Russian GUI.
10. Support Czech GUI.

[BUG FIX]

1. [eITS #190201272] TR-181 has DSL-errors in Eth-WAN mode.
   --> Refer to spec of TR-098 and TR-181, change not support parameter value to "4294967295".
2. [eITS #190200506] VMG8825 SNAT CPE-LAN when DMZ enabled.
3. [eITS #190600043] Correct incorrect spelling on voip call history page.
4. [eITS #190501104] Some TR069 atm parameters will be returned on eth/vdal/wwan interfaces with GPN.

5. [eITS #190600597] Upload certificate error after changed gateway IP address
6. [eITS #190700674] DHCP with one address ip(Configure LAN subnet mask to 255.255.255.252) in the pool don't work.

Modifications in 5.13(ABMT.2)b1

[BUG FIX]

1. #94227 [eits# 181200918] Missing 5ghz beacons

Modifications in 5.13(ABMT.1)D1

Based on V5.13(ABMT.1)D0 to release V5.13(ABMT.1)D1

Modifications in 5.13(ABMT.1)D0

Based on V5.13(ABMT.1)C0 to release V5.13(ABMT.1)D0

Modifications in 5.13(ABMT.1)C0

Based on V5.13(ABMT.1)b2 to release V5.13(ABMT.1)C0

Modifications in 5.13(ABMT.1)b2

[FEATURE ENHACEMENT]

1. [eits# 181200065]No reason to use telnet if SSH is available
2. [eits# 181200071]traditional session accepted in pure-ftpd config
3. [eits# 181100377]smb and telnet LAN/WAN port disabled, and never start up during CPE boot up. But no need to remove from FW

[BUG FIX]

1. [eits# 181100543]Traffic flow doesn't fail after the change in IP range

Modifications in 5.13(ABMT.1)b1

[FEATURE ENHACEMENT]

[BUG FIX]

1. XMG8825-B50A 5G WPA2 group key issue
2. [Multy Pro] No steering record in Steering Status page.
3. [GUI] According ES, The "Home" should be renaming "Connection status"
4. [LAN] IP Address range in LAN Page is different with Home Page.

5. [Multy Pro] While verifying AP roaming at rental house, it occurs all wifi client disconnect issue.

Modifications in 5.13(ABMT.0)D2

Based on V5.13(ABMT.0)D1 to release V5.13(ABMT.0)D2

Modifications in 5.13(ABMT.0)D1

Based on V5.13(ABMT.0)D0 to release V5.13(ABMT.0)D1

Modifications in 5.13(ABMT.0)D0

Based on V5.13(ABMT.0)C0 to release V5.13(ABMT.0)D0

Modifications in 5.13(ABMT.0)C0

Based on V5.13(ABMT.0)b4 to release V5.13(ABMT.0)C0

Modifications in 5.13(ABMT.0)b4_D0

Based on V5.13(ABMT.0)b4 to release V5.13(ABMT.0)b4_D0

Modifications in 5.13(ABMT.0)b4

[FEATURE ENHACEMENT]

1. [eits#181000036] customize DSL physical configuration
2. [eits#180900667] Questionable RSSI - Different Values on PC/Router/MP App

[BUG FIX]

1. [eits#180900791] Band Steering back to 5G not working.
2. [eits#181000022] 5GHz Performance issue

Modifications in 5.13(ABMT.0)b3

[FEATURE ENHACEMENT]

[BUG FIX]

1. [Security] Automatic DNS registration and autodiscovery
2. [Security] CSRF vulnerabilities.
3. [eits #180800183] Band Steering back to 5G not working

Modifications in 5.13(ABMT.0)b2

[FEATURE ENHACEMENT]

[BUG FIX]

Modifications in 5.13(ABMT.0)b1

1. First firmware release