

VMG4005-B50A/ VMG4005-B60A Generic

Firmware Release Note

V5.15(ABQA.2)C0

Date: NOV 16, 2022

Author: CHI-HAO,LO

Reviewer:

THIS DOCUMENT CONTAINS PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THE Zyxel AND SHOULD NOT BE DISCLOSED TO OTHERS IN WHOLE OR IN PART, REPRODUCED, COPIED, OR USED AS BASIS FOR DESIGN, MANUFACTURING OR SALE OF APPARATUS WITHOUT WRITTEN PERMISSION OF Zyxel.

TABLE OF CONTENTS

SUPPORTED PLATFORMS:	4
VERSIONS:	4
DEFAULT SETTINGS IN FIRMWARE	5
PUBLIC DOMAIN SOFTWARE ANNOUNCEMENTS	5
EXTERNAL INFORMATION:	8
KNOWN ISSUES	8
MODIFICATIONS IN 5.15(ABQA.2)C0	8
MODIFICATIONS IN 5.15(ABQA.2)B7.....	8
MODIFICATIONS IN 5.15(ABQA.2)B6.....	9
MODIFICATIONS IN 5.15(ABQA.2)B5.....	9
MODIFICATIONS IN 5.15(ABQA.2)B4.....	11
MODIFICATIONS IN 5.15(ABQA.2)B3.....	12
MODIFICATIONS IN 5.15(ABQA.2)B2.....	12
MODIFICATIONS IN 5.15(ABQA.1)C0	13
MODIFICATIONS IN 5.15(ABQA.1)B2.....	13
MODIFICATIONS IN 5.15(ABQA.1)B1.....	14
MODIFICATIONS IN 5.15(ABQA.0)C0	14
MODIFICATIONS IN 5.15(ABQA.0)B6.....	14
MODIFICATIONS IN 5.15(ABQA.0)B5.....	15
MODIFICATIONS IN 5.15(ABQA.0)B4.....	16
MODIFICATIONS IN 5.15(ABQA.0)B3.....	17
MODIFICATIONS IN 5.15(ABQA.0)B2.....	17
MODIFICATIONS IN 5.15(ABQA.0)B1.....	18

Revision History

Date	Release	Author	Description
2019/5/31	1.0	Ivan Chiang	V5.15(ABQA.0)b1
2019/6/28	1.1	Ivan Chiang	V5.15(ABQA.0)b2
2019/7/23	1.2	Ivan Chiang	V5.15(ABQA.0)b3
2019/8/12	1.3	Ivan Chiang	V5.15(ABQA.0)b4
2019/8/30	1.4	Ivan Chiang	V5.15(ABQA.0)b5
2019/9/25	1.5	Ivan Chiang	V5.15(ABQA.0)b6
2019/10/21	1.6	Ivan Chiang	V5.15(ABQA.0)C0
2019/10/21	1.7	Ivan Chiang	V5.15(ABQA.1)b1
2020/4/7	1.8	CHI-HAO.LO	V5.15(ABQA.1)b2
2020/4/10	1.9	Howard Chen	V5.15(ABQA.1)C0
2020/5/29	2.0	CHI-HAO.LO	V5.15(ABQA.2)b2
2020/7/3	2.1	CHI-HAO.LO	V5.15(ABQA.2)b3
2021/1/29	2.2	CHI-HAO.LO	V5.15(ABQA.2)b4
2021/7/2	2.3	CHI-HAO.LO	V5.15(ABQA.2)b5
2021/8/25	2.4	CHI-HAO.LO	V5.15(ABQA.2)b6
2022/11/16	2.5	CHI-HAO.LO	V5.15(ABQA.2)b7
2022/11/16	2.6	CHI-HAO.LO	V5.15(ABQA.2)C0

Zyxel VMG4005-B50A/VMG4005-B60A V5.15(ABQA.2)C0 Release Note

Date: NOV 16, 2022

Supported Platforms:

Zyxel VMG4005-B50A/ Zyxel VMG4005-B60A

Versions:

Bootbase Version: V1.57 | 01/27/2021 17:12:24

Firmware version : V5.15(ABQA.2)C0

Kernel version: 4.1.51

VMG4005-B50A Annex A DSL modem code version: A2pvfbH046y

VMG4005-B60A Annex B DSL modem code version: B2pvfbH046w

DSL driver version: d27j

Notes:

Linux console:

uname -a

adsl --version

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 (3rd party software)	Version	From (Source)	Licensing Term	Modified / Used
Bridge-Utils	1.5	http://bridge.sourceforge.net	GPLv2	Used
BusyBox	1.20.1	http://www.busybox.net/	GPLv2	Modified
clinkc	2.4	http://sourceforge.net/projects/clinkc/	BSD	Modified
dnsmasq	2.67	http://www.thekelleys.org.uk/dnsmasq/doc.html	GPLv2/GPLv3	Modified
dropbear	2018.76	http://matt.ucc.asn.au/dropbear/dropbear.html	MIT	Modified
ebtables	2.0.10-4	http://ebtables.sourceforge.net	GPLv2	Modified
eventlog	0.2.10	http://git.balabit.hu/?p=bazsi/eventlog-1.0.git;a=summary	BSD	Used
expat	1.95.8	http://expat.sourceforge.net/	MIT	Used
ez-ipupdate	3.0.11b8	http://ez-ipupdate.com/	GPLv2	Used
gettext	0.16	http://www.gnu.org/software/gettext/	GPLv2	Used
glib	2.37.7	http://www.gtk.org/	LGPLv2	Used
iproute2	2-2.6.33	http://repository.timesys.com/buildsources/i/iproute2/	GPLv2	Modified
iptables	1.4.21	http://www.netfilter.org	GPLv2	Modified
json-c	0.12	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/	LGPL (GNU)	Modified

			LIBRARY GENERAL PUBLIC LICENSE V2)	
libnetfilter_queue	1.0.2	http://www.netfilter.org/projects/libnetfilter_queue/	GPLv2	Used
libnftnl	1.0.1	http://www.netfilter.org/projects/libnftnl/	GPLv2	Used
libpcap	1.1.1	www.tcpdump.org	BSD	Used
libtool	2.4	http://www.gnu.org/software/libtool/	GPLv2	Used
logrotate	3.7.1	https://launchpad.net/ubuntu/hardy/i386/logrotate/	GPLv2	Modified
ncurses	5.7	http://ftp.gnu.org/pub/gnu/ncurses/	MIT	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 (BSD-style)	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
sqlite	3.6.23.1	http://www.sqlite.org/	Public Domain License	Used
syslog-ng	2.0.10	http://www.balabit.com/network-security/syslog-ng/	GPLv2	Used
tcpdump	4.2.1	http://www.tcpdump.org/	BSD	Used
udhcp	0.9.8	http://udhcp.busybox.net/	GPLv2	Modified
WIDE-DHCPv	20080615	http://wide-dhcpv6.sourceforge.net/	BSD	Modified

6				
zebra	0.93a	http://www.zebra.org/	GPLv2/LG PLv2	Used

External Information:

Known issues

Modules	Issue	Risk Impact Information

Modifications in 5.15(ABQA.2)C0

5.15(ABQA.2)C0 FCS based on 5.15(ABQA.2)b7

- Feature Enhancement

Modified Modules	Features Enhancement List

- Bug Fixed

Modified Modules	Bug Fixed List

Modifications in 5.15(ABQA.2)b7

5.15(ABQA.2)b7 based on 5.15(ABQA.2)b6

- Feature Enhancement

Modified Modules	Features Enhancement List

- Bug Fixed

Modified Modules	Bug Fixed List
Security	Zyxel-SI-1391 [Vulnerability] OS command injections and potential buffer overflows

	Zyxel-SI-1377 [Vulnerability] cleartext storage of sensitive information
	[Vulnerability] Infinite loop in BN_mod_sqrt() of OpenSSL when parsing certificates
	Zyxel-SI-1433 [Vulnerability] Buffer overflow vulnerabilities and command injection vulnerability

Modifications in 5.15(ABQA.2)b6

5.15(ABQA.2)b6 based on 5.15(ABQA.2)b5

● Feature Enhancement

Modified Modules	Features Enhancement List
Phy	[eits # 210700344] [A1] [Mantis-6341] New xDSL Phy

● Bug Fixed

Modified Modules	Bug Fixed List
QOS	[eits # 200201321][A1] QOS is not working as expected

Modifications in 5.15(ABQA.2)b5

5.15(ABQA.2)b5 based on 5.15(ABQA.2)b4

● Feature Enhancement

Modified Modules	Features Enhancement List
certificate	[eits # 200900419] VMG4005-B60A - how to upload the certificate via TR069
	[eits # 200100140] CETIN, VMG4005-B60A, FRQ - upload certificate via TR-069
Config	[eits #210601087] [Cetin] VMG4005-B60A default configuration change „Disable IPv4 Firewall, IPv6 Firewall and Dos Protection Blocking“
Bridge	[eits #200102989] CETIN, VMG4005-B60A -

	BridgeVlanCounter - counters (TR069)
GUI	[eits #210301552] [A1] [Mantis-6172] Missing Portforwarding-Configuration (towards untagged NATed LAN-Clients)
EOC	[eits #210501155] [CETIN] VMG4005-B60A - new EOC registry format
	[eits #210501156] [CETIN] VMG4005-B60A - EOC registry values should take effect without RTFD

● Bug Fixed

Modified Modules	Bug Fixed List
TR069	[eits #200102982] CETIN, VMG4005-B60A - BridgeVlanCounter (TR069)
	[eits #200102937] CETIN, VMG4005-B60A - DSL Line parameters (TR069)
	[eits #200102938] CETIN, VMG4005-B60A - DSL Channel parameters (TR069)
	[eits #200102951] CETIN, VMG4005-B60A - PTM Link parameters (TR069)
	[eits #200102966] CETIN, VMG4005-B60A - Ethernet Link - NumberOfEntries (TR069)
	[eits #200102971] CETIN, VMG4005-B60A - Ethernet Link - LastChange (TR069)
	[eits #200102976] CETIN, VMG4005-B60A - Ethernet VLANTermination - NumberOfEntries (TR069)
	[eits #200102981] CETIN, VMG4005-B60A - Ethernet VLANTermination - LastChange (TR069)
	[eits #200102994] CETIN, VMG4005-B60A - PPP - InterfaceNumberOfEntries (TR069)
	[eits #200103028] CETIN, VMG4005-B60A - IP Interface - number of entries (TR069)
	[eits #200103033] CETIN, VMG4005-B60A - IP interface - LAN - LastChange (TR069)
	[eits #200103040] CETIN, VMG4005-B60A - BondingGroup -

	BondedChannelNumber (TR069)
	[eits #210501559][CETIN] VMG4005-B60A - TR069 - Parameter DefaultGatewayIface cannot be changed
DSL	[eits #210501558][CETIN] VMG4005-B60A - both DSL lines are not synchronized at the same time
Time	[eits #210200498] [200814] VMG4005-B50B / NTP Sync issue in bridge mode

Modifications in 5.15(ABQA.2)b4

5.15(ABQA.2)b4 based on 5.15(ABQA.2)b3

● Feature Enhancement

Modified Modules	Features Enhancement List
FW	[eits #190800784] VMG4005-B60A - firmware banks management missing
certificate	[eits #190900339] VMG4005-B60A - local certificate used by TR-069 Client
GUI	[eits #190900329] VMG4005-B60A - DSL lines administrative status in WebGUI
Driver	[eits #210100660] New xDSL Phy
	[eits #210100664] New DSL Linedriver

● Bug Fixed

Modified Modules	Bug Fixed List
TR069	[eits #190900225] VMG4005-B60A - bonding group statistics are not collected (TR069)
	[eits #190900220] VMG4005-B60A - DSL line and channel counters show wrong data in TR069
	[eits #190900228] VMG4005-B60A - VLAN termination
Security	[Vulnerability] Arbitrary remote code execution (RCE) on the device through an HTTP request
	[Vulnerability] Unauthenticated Denial-of-Service effectively disabling the device's web-interface
	[Common][CVE-2020-1971][Openssl]Correctly compare

	EdiPartyName in GENERAL_NAME_cmp()
	Dnsmasq multiple vulnerabilities (DNSPooq)
	[Vulnerability][EESBU] Vulnerabilities in Multiple Zyxel Equipment from Sec consult

Modifications in 5.15(ABQA.2)b3

5.15(ABQA.2)b3 based on 5.15(ABQA.2)b2

● Feature Enhancement

Modified Modules	Features Enhancement List
kernel	[eits #200102928] CETIN, VMG4005-B60A - UNI Rx Errors (TR069)
	[eits #190900336] VMG4005-B60A - 64 bit counters (TR069)
	[eits #190900224] VMG4005-B60A - parameter counters of "TX and RX number of octets/bytes" are only 32 bit (TR069)
	[eits #191000361] WAN traffic status in WebGUI
	[eits #190900331] LAN traffic status in WebGUI
certificate	[eits #190900363] VMG4005-B60A - certificate management in TR069
ipv6	[eits #200103023] CETIN, VMG4005-B60A - IPv6Capable (TR069)
GUI	[eits #190700654] VMG4005-B60A - Last status change of UNI

● Bug Fixed

Modified Modules	Bug Fixed List
broadband	[eits #190900681] [Germany] Missing Annex J by VMG 4005-B60A

Modifications in 5.15(ABQA.2)b2

5.15(ABQA.2)b2 based on 5.15(ABQA.1)C0

● Feature Enhancement

Modified Modules	Features Enhancement List
------------------	---------------------------

modem	[eits #200400312] [A1] [Mantis-5607] New DSL Phy
dhcp	[eits #190801240] VMG4005-B60A - DHCP times in TR069
dhcp	[eits #190800818] VMG4005-B60A - There is no info about configuration obtained via DHCP in WebGUI
zhttpd	[eits #190900232] VMG4005-B60A - multipair DSL interface (bonding) statistics in WebGUI
Tr069	[eits #200100140] CETIN, VMG4005-B60A, FRQ - upload certificate via TR-069
webgui	[eits #190900327] VMG4005-B60A - Last status change of UNI (TR069)
webgui	[eits #190801236] VMG4005-B60A - provisioning code in WebGUI

● Bug Fixed

Modified Modules	Bug Fixed List
log	[eits #190900883] [Germany] Log Time for DHCP and TR069 not correct VMG 4005-B60A
certificates	[eits #190900368] VMG4005-B60A - wrong number of certificates in TR069

Modifications in 5.15(ABQA.1)C0

FCS based on 5.15(ABQA.1)b2

Modifications in 5.15(ABQA.1)b2

● Feature Enhancement

Modified Modules	Features Enhancement List

● Bug Fixed

Modified Modules	Bug Fixed List
libzyutil	DUT reset configuration to default if ROMFILE block has an

	error bit
GUI_Vue	WAN mac address order should be changed for VMG4005 project

Modifications in 5.15(ABQA.1)b1

● Feature Enhancement

Modified Modules	Features Enhancement List
GUI	[eits #190900895] VMG4005-B60A - NTP servers obtained via DHCP are not written to configuration

● Bug Fixed

Modified Modules	Bug Fixed List
GUI	[eits #191000604] VMG4005-B60A When accessing System Monitor > Traffic Status > WAN, system crashes
TR-069	[eits #190900327] VMG4005-B60A - Last status change of UNI (TR069)
	[eits #190900227] VMG4005-B60A - Ethernet link statistics are not collected (TR069)

Modifications in 5.15(ABQA.0)C0

● Feature Enhancement

Modified Modules	Features Enhancement List
RomFile	[eits #191000488] VMG4005-B50A The Parameter "Validate ACS certificate" must be activated by default

Modifications in 5.15(ABQA.0)b6

[FEATURE ENHANCEMENT]

1. [eits #190700655] VMG4005-B60A - Counters of frames per VLAN
2. [eits #190700758] VMG4005-B60A - QoS at Ethernet UNI
3. [eits #190800145] VMG4005-B60A - management via IPv6
4. [eits #190800150] VMG4005-B60A - MAC address limiting

5. [eits #190801084] New DSL physical modem code upgrade to A2pvfbH045o1 for VMG4005-B50A
6. [eits #190900263] New DSL physical driver to DSL-Phy 027h VMG 4005-B50A

[BUG FIX]

1. [eits #190800778] VMG4005-B60A - CPE does not send LPR (lost of power)
2. [eits #190900048] VMG4005-B60A - Insufficient input validation for NTP server
3. [eits #190900094] Port mirror can't be activate by the user "tccadmin"
4. [eits #190900677] Why Upgrade WWAN Package VMG 4005-B60A

Modifications in 5.15(ABQA.0)b5

[FEATURE ENHACEMENT]

1. [eits #190700653] VMG4005-B60A - Dropped frames counters at UNI
2. [eits #190700654] VMG4005-B60A - Last status change of UNI
3. [eits #190700760] VMG4005-B60A - DSCP of management traffic
4. [eits #190700757] VMG4005-B60A - ATM PVC assignment according to VLAN
5. [eits #190800149] VMG4005-B60A - MAC address learning
6. [eits #190800147] VMG4005-B60A - MAC address table
7. [eits #190800506] VMG4005-B60A - DHCP option 42
8. [eits #190700614] Feature request enhanced DSL Broadcom config VMG 4005-B50A
9. [eits #190700788] DSL configuration MANTIS-5263 VMG 4005_B50A
10. [eits #190800444] untypical STUN messages was send by the VMG4005
11. [eits #190800772] AW: Summary of the results ACS-Tests
12. [eits #190801162] Inventory information not correct send to the DSLAM side VMG 4005-B50A

[BUG FIX]

1. [eits #190700790] DHCP Option(121) MANTIS-5265 works not

correct VMG 4005-B50A

2. [eits #190800354] Disable the IGMP proxy and the MLD Proxy by default
3. [eits #190700789] VDSL2 SRA/G.inp Profile: Incorrect Att Bitrate on short distance loops VMG 4005-B50A
4. [eits #190800504] VMG4005-B60A - Downloading of certificate
5. [eits #190800557] VMG4005-B60A - vectoring issue

Modifications in 5.15(ABQA.0)b4

[FEATURE ENHACEMENT]

1. [eits #190600295] VMG4005-B60A - DNS server running
2. [eits #190700340] VMG4005-B60A - not enough space to store 10 certificates
3. [eits #190700615] New DSL physical driver VMG 4005-B50A
4. [eits #190700616] Feature request support FDPS VMG 4005-B50A
5. [eits #190700618] Disable the V43 G.hs toneset VMG 4005-B50A
6. [eits #190700619] Feature request LongReach-VDSL2 mode VMG 4005-B50A
7. [eits #190700656] VMG4005-B60A - Counters by different type of frame
8. [eits #190700610] Inventory information not correct send to the DSLAM side VMG 4005-B50A
9. [eits #190700883] Password Reset [MANTIS-5267] User Account 'tccadmin' VMG4005-B50A
10. [eits #190700939] VMG4005-B60A - LAN interface shall be without IP address
11. [eits #190701025] VMG4005-B60A - request to change default settings (the fixed password for the "root" user)

[BUG FIX]

1. [eits #190400800] VMG4005-B60A - Bridge interface is not fully transparent
2. [eits #190700255] VMG4005-B60A - Even if ACS certificate validation is disabled device still performs certificate validation.
3. [eits #190700673] Not possible to disable portmirror functuion VMG 4005-B50A
4. [eits #190700751] VMG4005-B60A - Blocking of some L2CP

messages

5. [eits #190700611] L2CP transparent over the bridge VMG 4005-B50A
6. [eits #190700763] VMG4005-B60A - Local management isolation
7. [eits #190700936] VMG4005-B60A - RPC call
8. [eits #190700937] VMG4005-B60A - RPC call (attributes)
9. [eits #190701013] VMG4005-B60A - There are wrong values in some TR069 data model parameters

Modifications in 5.15(ABQA.0)b3

[FEATURE ENHACEMENT]

1. [eits #190700344] VMG4005-B60A - request to change default settings (disabling of "Validate ACS certificate")

[BUG FIX]

1. [eits #190400800] VMG4005-B60A - Bridge interface is not fully transparent
2. [eits # 190400809] VMG4005-B60A - insufficient physical layer performance
3. [eits #190600822] GUI has no info show DSL bonding status
4. [eits # 190700093] 35b info does not display correctly in xDSL Statistics
5. [eits #190700311] ACS service works not as expected VMG 4005-B50A
6. [eits #190700309] NTP and DNS service works not via MGMT VLAN 4092 Prio 2 VMG 4005-B50A
7. [kernel] Multiple TCP-based remote denial of service vulnerabilities (fixed about CVE-2019-11477, CVE-2019-11478, CVE-2019-11479)

Modifications in 5.15(ABQA.0)b2

[FEATURE ENHACEMENT]

1. [eits #190600093] VMG4005-B60A - WAN MAC address changing
2. [eits #190600331] VMG4005-B60A - QoS, swapped CoS priorities
3. [eits #190600485] There is DNS server running
4. [eits #190600392] VMG4005-B60A - request to change default settings

5. [eits #190600435] VMG4005-B60A - EOC register
6. [eits #190600295] VMG4005-B60A - DNS server running

[BUG FIX]

1. [eits #190500524] VMG4005-B60A – WebGUI
2. [eits #190600483] There are functionless leafs in TR069 data model (e.g. WiFi)
3. [eits #190600484] There are wrong values in some TR069 data model parameters
4. [eits #190600337] VMG4005-B60A - Device management becomes unusable after call TR069 RPC GetParameterAttributes

Modifications in 5.15(ABQA.0)b1

[FEATURE ENHACEMENT]

1. [eits #190500522] Disable both TCP port 161 and port 38400 (UPnP)
2. [eits #190500526] Provide document of CLI commands
3. [TR000185-4] [Req 2.1.5 2.1.8] Support Ethctl command and Ethernet UNI page
4. [TR000185-4] [Req 2.1.7 4.1.2] Support JUMBO Frame
5. [TR000185-4] [Req 4.1.1] Support transparent data transmission.
6. [TR000185-4] [Req 4.3.2] CPE could be able to be set up not to learn any source MAC address of specific interfaces
7. [TR000185-4] [Req 6.1.3.3][GUI_vue] ADSL,VDSL--Dynamic IPv4 configuration
8. [TR000185-4] [Req 6.2.1] Local management via Ethernet UNI
9. [TR000185-4] [Req 6.3.4] CPE could reply LAN interface's content of 'Mac Address Table' including information of used vlan
10. [TR000185-5] [Req 2.1.3] Additional device status information
11. [TR000185-5] [Req 2.2.13.2] [User accounts] The Demarcation Device shall permit to define for each user account allowed management protocol(s) and input interface(s).
12. [TR000185-5] [Req 3.2.1] HTTP/HTTPS remote access enable to the Demarcation Device
13. [TR000185-5] [Req 3.2.2] HTTP/HTTPS local access disable to the

Demarcation Device

[BUG FIX]

1. [eits # 190400687] The System Info page does not show any values
2. [eits #190500524] When internet connection is unavailable, it slows down the loading of the WebGUI.
3. [eits #190400809] Insufficient physical layer performance
4. [eits #190400797] Low throughput with bridge mode pure IPv4 traffic .
5. [eits #190400637] VMG4005-B60A Port Mirror fail
6. [eits #190400800] Bridge interface is not fully transparent
7. [eits #190400712] Unstable remote access to Web GUI