ZYXEL
COMMUNICATIONS

LTE5388-M804

Generic Version

Firmware Release Note

V1.00(ABSQ.4)C0

Date: Dec. 13, 2022

Author: Chin-Fu Ku

Reviewer:

ZYXEL
COMMUNICATIONS

TABLE OF CONTENTS

Revision History

Date	Release	Author	Description
2019/10/16	1.0	Chin-Fu Ku	V1.00(ABSQ.0)b0 fw release
2019/12/11	1.1	Chin-Fu Ku	V1.00(ABSQ.0)b1 fw release
2020/01/14	1.2	Chin-Fu Ku	V1.00(ABSQ.0)b2 fw release
2020/03/05	1.3	Chin-Fu Ku	V1.00(ABSQ.0)b3 fw release
2020/03/16	1.4	Chin-Fu Ku	V1.00(ABSQ.0)C0 fw release
2020/04/15	1.5	Chin-Fu Ku	V1.00(ABSQ.1)b0 fw release
2020/05/25	1.6	Chin-Fu Ku	V1.00(ABSQ.1)b1 fw release
2020/06/30	1.7	Chin-Fu Ku	V1.00(ABSQ.1)b2 fw release
2020/07/17	1.8	Chin-Fu Ku	V1.00(ABSQ.1)b3 fw release
2020/08/07	1.9	Chin-Fu Ku	V1.00(ABSQ.1)b4 fw release
2020/08/11	1.10	Chin-Fu Ku	Update the V1.00(ABSQ.1)b4 fw known issue and bug fix items.
2020/08/13	1.11	Chin-Fu Ku	V1.00(ABSQ.1)b5 fw release
2020/08/18	1.12	Chin-Fu Ku	V1.00(ABSQ.1)C0 fw release
2020/08/20	1.13	Chin-Fu Ku	V1.00(ABSQ.2)b1 fw release
2022/04/11	1.14	Chin-Fu Ku	V1.00(ABSQ.2)b6 fw release
2022/05/05	1.15	Chin-Fu Ku	V1.00(ABSQ.2)b7 fw release
2022/06/06	1.16	Chin-Fu Ku	V1.00(ABSQ.2)C0 fw release
2022/07/04	1.17	Chin-Fu Ku	V1.00(ABSQ.3)b1 fw release
2022/07/05	1.18	Chin-Fu Ku	V1.00(ABSQ.3)C0 fw release
2022/11/16	1.19	Chin-Fu Ku	V1.00(ABSQ.4)b1 fw release
2022/12/13	1.20	Chin-Fu Ku	V1.00(ABSQ.4)C0 fw release

ZYXEL

COMMUNICATIONS

ZYXEL LTE5388-M804 Generic
V1.00(ABSQ.4)C0
Release Note

Date: Dec. 13, 2022

Supported Platforms

ZYXEL LTE5388-M804

Versions

Bootbase version : U-Boot 1.1.3 (Jul 26 2019 - 21:28:53)
Firmware version : V1.00(ABSQ.4)C0
Kernel version: 3.10.14
WLAN code version: V4.4.2.1_20170829
LTE Module FW version: EG12EAPA**R01A12**M4G

Firmware image information

Image	Version	File name	MD5 sum
Uboot Image-1: Pre-programming	U-Boot 1.1.3 (Jul 26 2019 - 21:28:53)	uboot-5388-20190826.bin	513e972ffcad8c3188eaa96e741771c9
Uboot Image-2: Zyxel uboot update		100ABSQ4C0.bm	4feeecef5565c618d4d122741f70f133
FW Image	**V1.00(ABSQ.4)C0**	**100ABSQ4C0.bin**	**181854aa26948eb96e764817843ec2b1**

Notes:

There are two Bootbase files :

uboot-5388-20190826.bin is used for manufacturing PROGRAMMER to program on the NAND flash

100ABSQ4C0.bm is for zyxel bootloader update usage, **This file with zyxel header and must not directly program to flash. Wrong action will cause the failure of boot.**

Default Settings in Firmware

- Refer to the *.rom in the fw release package.

- Refer to the *.config and *.predef for human readable default configuration.

- *.config define the default value of writable parameters, *.predef define the default value of read only parameters.

- Please use the website http://jsoneditoronline.org/ to open the *.config and *predef files.

Modifications in V1.00(ABSQ.4)C0

Based on the V1.00(ABSQ.4)b1 version , change to FCS version.

Modifications in V1.00(ABSQ.4)b1

[Configuration Modification]
N/A

[FEATURE ENHACEMENT]
N/A

[BUG FIX]
1. Zyxel SI-1433 Post authentication buffer overflow.

2. [Vulnerabilities] Unsafe for SAMBA:

    a. SAMBA shares Unsafe Symbolic Link folder

    b. Unsafe User-Controlled Configuration Data.

3. Double quotation mark will execute the shell command via pass phrase by system function in the end.

4. Rooting device via shell command injection by using execlp.

5. Ticket #221000626 [338584]: Web GUI switching Bands issue.

Modifications in V1.00(ABSQ.3)C0

Based on the V1.00(ABSQ.3)b1 version , change to FCS version.

Modifications in V1.00(ABSQ.3)b1

[Configuration Modification]

1. Enable the MRD password.
   A. The WEB login account: admin and supervisor, default login password is stored in the MRD by random generate.
   B. The admin default password is stored in MRD password index 1.
   C. The supervisor/root default password is stored in MRD password index 2.
   D. The WiFi PSK key default password is stored in MRD password index 1.

[FEATURE ENHACEMENT]
N/A

[BUG FIX]
N/A

Modifications in V1.00(ABSQ.2)C0

Based on the V1.00(ABSQ.2)b7 version , change to FCS version.

Modifications in V1.00(ABSQ.2)b7

[Configuration Modification]
N/A

[FEATURE ENHACEMENT]

N/A

[BUG FIX]

1. Issue #123: DUT can't work well while Roaming feature is off.

Modifications in V1.00(ABSQ.2)b6

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

1. Support Speed Test.

2. Support Neighbour Cells.

3. Update Italian language string.

4. Support Cell Lock.

5. Support TR-069 Delay Reboot.

6. The WEB admin and supervisor default login password is stored in the MRD by random generate.

(MRD password index 1 and index 2)

[BUG FIX]

1. Fix the USB power control issue.

2. Fix that USB no unmount cause some wrong case.

3. [Vulnerability] clear text storage of sensitive information issue.

4. [Vulnerability] Infinite loop in BN_mod_sqrt() of OpenSSL when parsing certificates.

   Update the OpenSSL to 1.1.1n

** Skip the modifications for V1.00(ABSQ.2)b2 ~ V1.00(ABSQ.2)b5. **

Modifications in V1.00(ABSQ.2)b1

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

1. Enable the Auto APN Multi Search feature.

[BUG FIX]

1. Issue 94: Even auto APN attach failed, UE always send first APN that meet PLMN in the apnlist.txt list and attempt to attach again.

Modifications in V1.00(ABSQ.1)C0

1. Change to FCS version.
2. Based on the 1.00(ABSQ.1)b5 version, remove the Auto APN Multi Search feature.

Modifications in V1.00(ABSQ.1)b5

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

1. Add the Auto APN Multi search feature.

[BUG FIX]

1. Issue #91: When PPPoE with VLAN interface down and up, the device will not be able to access WebGUI/Telnet/SSH/Console, and the HW reboot/reset button function will be invalid.

2. Issue #92: GSM alphabet long SMS content display abnormal (GSM alphabet become Unicode)

3. Issue 94: Even auto APN attach failed, UE always send first APN that meet PLMN in the apnlist.txt list and attempt to attach again.

Modifications in V1.00(ABSQ.1)b4

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

1. Change the APN search order for SFR mobile in apnlist.txt due to the front line request.

[BUG FIX]

1. Issue #31: SMS Inbox GSM alphabet content display abnormal (Char. become Unicode Hex) after received unicode content SMS.

2. Issue #61: If user hangs up immediately after making a call and repeats this action several times, the call status account will always accumulate and duration continue counting.

Software action: Use a workaround code to fix the repeats call cause the hardware SLIC abnormal issue.

3. Issue #76: UE can't display received SMS anymore after receiving a long SMS content.

4. Issue #77: Old SMS messages disppear (can't be displayed normal) if UE receiving a long SMS content.

5. Issue #78: System show the repeat message with specific condition and steps

6. Issue #80: UE-initiated Detach not work when device reboot or reset.

7. Issue #81: If user set the preferred Access Technology with invalid value "3G" or "4G" via TR-069 ACS, the setting will be applied and the Access Technology field displayed empty on WebGUI.

8. Issue #82: If user setting device not support LTE Band via TR-069 ACS, device will be applied the setting and disconnect with internet, need to setting the correct Cellular Band again.

9. Issue #85: The Website Blocked content is displayed empty on the Parental Control page.

10. Issue #91: When PPPoE with VLAN interface down and up, the device will not be able to access WebGUI/Telnet/SSH/Console, and the HW reboot/reset button function will be invalid.

Modifications in V1.00(ABSQ.1)b3

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

1. Add Ethernet WAN VLAN tag support.

[BUG FIX]

1. Issue #69: Short length packet may cause system call trace and reboot.

Modifications in V1.00(ABSQ.1)b2

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

N/A

[BUG FIX]

1. Issue #25: DHCP lease time is too long to wait with IP Passthrough Mode.
2. Issue #27: Select to Voice mode from VoIP to VoLTE, the VoIP status page still display "Register action" enabled and registered.
3. Issue #39: Enable Ethernet WAN (primary WAN) and disconnect LTE, the internet LED indicator will become "off"
4. Issue #42: WIFI password and SSID can't be empty or spaces.
5. Issue #64: The Parental Control Profile function not work normally.
6. Issue #67: Guest WiFi Settings display incorrect on home page.
7. Issue #68: Guest1~3 WiFi behavior not consistant after 2.4G/5G WiFi Setting disable and enable.
8. Issue #72: User can't disable IPPT mode if FIX mode didn't specify the MAC address.
9. Issue #73: WiFi SSID issue.
10. Issue #74: WiFi QR-Code issue.

Modifications in V1.00(ABSQ.1)b1

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

N/A

[BUG FIX]

1. Issue #14: System should show the current interface of WAN (Cellular/Ether WAN) when user operate.

2. Issue #23: When select the log level then pressing refresh on Web GUI, system will display all the category log. System should only display the assigned category.

3. Issue #33: CPE does't support IR-92 SS (Supplementary Services) and configurations.

    There is no clarify VoLTE support function in PS document

4. Issue #34: While WAN IP change, VoIP service will lost register to server.

    (EX: APN change or WAN back up active, Cellular WAN <=> Ethernet WAN)

    Need to disable and enable to register again.

5. Issue #36: WebGUI display wired connected devices under IP Passthrough mode abnormal.

    WebGUI display "0" device while connecting two clinets to LAN1 and LAN2 port under

    IP Passthrough mode abnormal. (Please refer to remark picture)

6. Issue #38: When Ethernet WAN fail over to Cellular WAN (Ethernet WAN backend disconnect), the WAN information still show Ethernet WAN IP on systen info page.

7. Issue 39: Enable Ethernet WAN and disconnect LTE, the internet LED indicator will become "off"

8. Issue #43: Enable SMS inbox function will cause webGUI crash with FET SIM Card
    After enable "SMS Inbox Enable", GUI pop-up Warning message "It is impossible to retrieve the information now. Please try again". (FET SIM Card only)

9. Issue #48: WPS Method 3 mode fail issue.

10. Issue #54: User cannot set SSID with special characters normally.

11. Issue #67: Guest WiFi Settings display incorrect on home page

Modifications in V1.00(ABSQ.1)b0

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

N/A

[BUG FIX]

1. Issue #2: Setting the lease time of DHCP server as 1 min but the lease time is 2 min when we capture the DHCP packet by Wireshark.
    ⇨ Change the minimal lease time to 2 minute.

2. Issue #22: System can't generate the any log on LAN PC.

3. Issue #24: Device should follow the Syslog Protocol "RFC 5424" to define the log category.

4. Issue #26: With IP Passthrough Mode, VoLTE function can't work and register to server, voice indicator LED also off.

5. Issue #28: DDNS could not active after CPE reboot.

6. Issue #32: Web word description error on Ethernet WAN setting page (LAN port4).

7. Issue #35: VoIP call waiting function abnormal. Need to reboot device.

8. Issue #39: Enable Ethernet WAN and disconnect LTE, the internet LED indicator will become "off"

9. Issue #40: Select VoLTE mode, enable Ethernet WAN and disconnect LTE, internet traffic passthrough by Ether WAN, but the voice LED indicator keep displaying "on".

10. #Issue 42: User can enter empty WIFI SSID and WIFI Password, and the setting could be applied successfully on home page (WiFi Settings).
    Empty Password will become 64 character password automatically. User can enter empty WIFI SSID, and the setting could be applied successfully on home page (Guest WiFi Settings).

11. Issue 47: WiFi Encryption key Input 64 charators and apply seting on WIFI page, the Encryption key will disappear.

12. Issue #49: Voice mode setting page disappeared except for English, user can't setting and select VoIP/VoLTE mode.

13. Issue #50: WIFI 2.4G Zyxel_63A5_guest3 invalid (BSSID 00:00:00:00:00:00).

14. Issue #53: In APN IPv6 enabled environment, the system will always crash during LTE connection after accumulating 128 times IPv6 Up and down.
    Abnormal behavior of CPE under IPv4v6 dual stack is active.
    The file, zcfg_tr98_map.json, is enlarged with appending IPv6 Addr/Prefix mapping while the IPv6 is active, but not removed from it while IPv6 is inactive.

15. Issue #62: WPS HW button function is not working

16. Issue #63: DHCP server only distributes one IP address when DHCP server pool setting 2 IP address.

17. Issue #67: The File Sharing Services is not working, and the power LED didn't displayed blue.

Modifications in V1.00(ABSQ.0)C0

[Configuration Modification]

Change the version number from 1.00(ABSQ.0)b3 to 1.00(ABSQ.0)C0

[FEATURE ENHACEMENT]

N/A

[BUG FIX]

N/A

Modifications in V1.00(ABSQ.0)b3

[Configuration Modification]

N/A.

[FEATURE ENHACEMENT]

1. Add VoIP/VoLTE feature.
2. Add SMS feature.
3. Improve the WebGUI display wired connected device under IP Passthrough mode.

[BUG FIX]

1. Fix the issue: Vulnerability: pppd vulnerable to buffer flow due to logic error.

2. Fix the issue: Ticket # 200200305 LTE3301-PLUS / Dynamic DNS problem

Modifications in V1.00(ABSQ.0)b2

[Configuration Modification]

N/A.

[FEATURE ENHACEMENT]

1. WAN backup feature.
2. Re-arrange the LAN/WAN icon to fit the real hardware position and label in the system info page.

[BUG FIX]

1. Fix the issue that WEB GUI does not show correct SCC information issue.

   (Issue ID #7)

2. Fix the issue that when enable IP pass through mode, the internet LED abnormal.

   (Issue ID #16)

3. Fix the issue that if the USB is plugged in before the device starts, the USB LED does not work properly.

4. Fix the issue that iPhone can't connect WIFI by scanning QR code.

   (Issue ID #3)

5. Fix the issue that 5G WiFi SSID can't be searched by client with BW:20MHz.

   (Issue ID #5)

6. Fix the issue for the WiFi client number setting cannot work properly.

(Issue ID #6)

7. Fix the issue that WebGUI doesn't display wired connected devices on IP Passthrough mode.

(Issue ID # 8)

8. Fix the issue for the WiFi WPS LED scenario.

(Issue ID #12, #13)

9. Fix the issue that about the command injection in Wifi SSID parameter setting.

(Issue ID: #1)

Modifications in V1.00(ABSQ.0)b1

[Configuration Modification]

1. Add new schema item for WAN backup.

[FEATURE ENHACEMENT]

1. Add WAN backup feature.

2. Add multiple-SSID feature.

3. Add Multiple-Language feature.

4. Support PCM test for manufacture.

5. Support new APP API.

[BUG FIX]

1. Fix the internet LED issue.

2. Fix the WEB GUI system info page LAN/WAN status incorrect issue.

Modifications in V1.00(ABSQ.0)b0

[Configuration Modification]

N/A

[FEATURE ENHACEMENT]

N/A

[BUG FIX]

N/A

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	GPL	Used
BusyBox	1.20.1	http://www.busybox.net/	GPL	Modified
ebtables	2.0.10-4	http://ebtables.sourceforge.net	GPL	Modified
pure-ftpd	1.0.30	http://pureftpd.org	BSD	Modified
iproute2	2-2.6.33	http://repository.timesys.com/buildsources/i/iproute2/	GPL	Modified
iptables	1.4.16.3	http://www.netfilter.org	GPL	Modified
udhcp	0.9.8	http://udhcp.busybox.net/	GPL	Modified
zebra	0.93a	http://www.zebra.org/	GPL	Used
ppp	2.4.3	http://www.roaringpenguin.com/pppoe	GPL/BSD	Modified
dropbear	0.55	http://matt.ucc.asn.au/dropbear/dropbear.html	MIT	Modified
openssl	1.1.1n	http://www.openssl.org	Openssl (BSD-style)	Modified
radvd	1.8	http://www.litech.org/radvd/	BSD	Used
ntfs-3g	2013.1.13	http://ntfs-3g.org	GPL	Used

WIDE-DHCPv6	20080615	http://wide-dhcpv6.sourceforge.net/	BSD	Modified
usb-modeswitch	2.1.0	http://www.draisberghof.de/usb_modeswitch/	GPL	Used
libusb	1.0.9	http://www.libusb.org/	LGPL 2.1	Used
samba	3.0.37	http://www.samba.org/samba/	GPL	Modified
dnsmasq	2.67	http://www.thekelleys.org.uk/dnsmasq/doc.html	GPL	Modified
ez-ipupdate	3.0.11b8	http://ez-ipupdate.com/	GPL	Used
libpcap	1.1.1	www.tcpdump.org	BSD	Used
expat	1.95.8	http://expat.sourceforge.net/	OTHERS	Used
tcpdump	4.2.1	http://www.tcpdump.org/	BSD	Used
eventlog	0.2.10	http://git.balabit.hu/?p=bazsi/eventlog-1.0.git;a=summ ary	BSD	Used
glib	2.37.7	http://www.gtk.org/	GPL	Used
gettext	0.16	http://www.gnu.org/software/gettext/	GPL	Used
libiconv	1.11.1	http://www.gnu.org/software/libiconv/	LGPL	Modified
libffi	3.0.11	http://pkgs.fedoraproject.org/repo/pkgs/libffi/libffi-3.0.11.tar.gz/	GPL	Used
libedit	20080712-2.11	http://pkgs.fedoraproject.org/repo/pkgs/libedit/libedit-20080712-2.11.tar.gz/	GPL	Modified
libnfnetlink	1.0.0	http://www.netfilter.org/projects/libnetfilter_queue/	GPL	Used

libusb	1.0.9	http://libusb.wiki.sourceforge.net/	LGPL 2.1	Used
libqmi	1.8.0	http://www.freedesktop.org/wiki/Software/libqmi	GPLv3	Used
readline	6.2	http://cnswww.cns.cwru.edu/php/chet/readline/rltop.ht ml	GPL	Used
popt	1.7	http://rpm5.org/files/popt/	MIT	Modified
libnetfilter_qu eue	1.0.0	http://www.netfilter.org/projects/libnetfilter_queue/	GPL	Used
logrotate	3.7.1	https://launchpad.net/ubuntu/hardy/i386/logrotate/	GPL	Modified
ntpclient	2007_365	http://doolittle.icarus.com/ntpclient/	GPLv2	Modified
net-snmp	5.7.2	http://www.net-snmp.org/	GPL/BSD	Modified
syslog-ng	2.0.10	http://www.balabit.com/network-security/syslog-ng/	GPL/LGPL	Used
libtool	2.4	http://www.gnu.org/software/libtool/	GPL	Used
ncurses	5.7	http://ftp.gnu.org/pub/gnu/ncurses/	MIT	Modified
json-c	0.9	https://github.com/json-c/json-c/downloads	MIT	Modified
clinkc	2.4	http://sourceforge.net/projects/clinkc/	BSD	Modified
sqlite	3.6.23.1	http://www.sqlite.org/	Piblic Domain License	Used