

EX7501-B0_Generic

Firmware Release Note

V5.18(ACHN.0.1)C0

Date: February 23, 2024

Author: Yuan Lin

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

REVISION HISTORY.....	3
SUPPORTED PLATFORMS:	4
VERSIONS:.....	4
NOTES:.....	4
PUBLIC DOMAIN SOFTWARE ANNOUNCEMENTS	5
KNOWN ISSUES	7
MODIFICATIONS IN V5.18(ACHN.0.1)C0	7
MODIFICATIONS IN V5.18(ACHN.0.1)B1	7
MODIFICATIONS IN V5.18(ACHN.0)C0	7
MODIFICATIONS IN V5.18(ACHN.0)B6	7
MODIFICATIONS IN V5.18(ACHN.0)B5	8
MODIFICATIONS IN V5.18(ACHN.0)B4	8
MODIFICATIONS IN V5.18(ACHN.0)B3	9
MODIFICATIONS IN V5.18(ACHN.0)B2	10
MODIFICATIONS IN V5.18(ACHN.0)B1	14

Revision History

Date	Release	Author	Description
2023/02/24	1.0	Yuan Lin	FW release for V5.18(ACHN.0)b1
2023/04/28	1.1	Yuan Lin	FW release for V5.18(ACHN.0)b2
2023/06/16	1.2	Yuan Lin	FW release for V5.18(ACHN.0)b3
2023/07/28	1.3	Yuan Lin	FW release for V5.18(ACHN.0)b4
2023/08/11	1.4	Yuan Lin	FW release for V5.18(ACHN.0)b5
2023/09/01	1.5	Yuan Lin	FW release for V5.18(ACHN.0)b6
2023/09/22	1.6	Yuan Lin	FW release for V5.18(ACHN.0)C0
2024/02/23	2.1	Yuan Lin	FW release for V5.18(ACHN.0.1)b1
2024/02/23	2.2	Yuan Lin	FW release for V5.18(ACHN.0.1)C0

EX7501-B0_Generic V5.18(ACHN.0.1)C0 Release Note

Date: February 23, 2024

Supported Platforms:

Zyxel EX7501-B0

Versions:

Bootbase version : V2.0 | 04/28/2023 10:07:40

Firmware version : V5.18(ACHN.0.1)C0

Kernel version: 4.19.183

WLAN code version: 17.10.188.75

3G WWAN package version: 1.24

Notes:

Linux console:

uname -a

adsl --version

wl ver

wwanpackage info

Public Domain Software Announcements

Open Source Used In Product	Version	From (Source)	License Terms	Modified / Used
attr	2.5.1	http://savannah.nongnu.org/projects/attr	GPLv2	Used
atftp	0.7.4	https://sourceforge.net/projects/atftp/	GPLv2	Modified
bridge-Utils	1.7.1	https://git.kernel.org/pub/scm/linux/kernel/git/shemminger/bridge-utils.git/	GPLv2	Modified
busybox	1.31.1	https://busybox.net/	GPLv2	Modified
clinkc	2.4	https://sourceforge.net/projects/clinkc/	BSD	Modified
conntrack-tools	1.4.5	https://git.netfilter.org/conntrack-tools/	GPLv2	Used
dnsmasq	2.85	http://www.thekelleys.org.uk/dnsmasq/doc.html	GPLv2/GPLv3	Modified
dropbear	2019.78	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	2.2.9	https://github.com/libexpat/libexpat	MIT	Used
ez-ipupdate	3.0.11b8	http://ez-ipupdate.com/	GPLv2	Modified
gettext	0.19.8.1	http://www.gnu.org/software/gettext/	GPLv3	Used
glib	2.68.1	http://www.gtk.org/	LGPLv2.1	Used
iproute2	5.7.0	https://github.com/shemminger/iproute2	GPLv2	Modified
iptables	1.8.5	https://git.netfilter.org/iptables/	GPLv2	Modified
jpegsrcc	v9c	http://www.iijg.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	3.3	http://pkgs.fedoraproject.org/repo/pkgs/libffi/libffi-3.0.11.tar.gz/	MIT	Used
libnetfilter_conntrack	1.0.7	https://git.netfilter.org/libnetfilter_conntrack/	GPLv2	Used
libnetfilter_queue	1.0.3	https://git.netfilter.org/libnetfilter_queue/	GPLv2	Used

libnfnetwork	1.0.1	https://git.netfilter.org/libnfnetwork/	GPLv2	Used
libpcap	1.9.1	www.tcpdump.org	BSD	Used
libtool	2.4.6	http://www.gnu.org/software/libtool/	GPLv2	Used
libusb	1.0.9	https://sourceforge.net/projects/libusb/	LGPL 2.1	Used
Linux/Arm Kernel	4.19.183		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
ncurses	6.1	http://ftp.gnu.org/pub/gnu/ncurses/	MIT	Modified
net-snmp	5.8	http://www.net-snmp.org/	ISC/BSD	Modified
ntfs-3g	2017.3.23	http://ntfs-3g.org	GPLv2/LGPLv2	Used
ntpclient	2007_365	http://doolittle.icarus.com/ntpclient/	GPLv2	Modified
openssl	1.1.1f	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	8.0	http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html	GPLv2	Used
samba	3.6.25	http://www.samba.org/samba/	GPLv3	Modified
sqlite	3.31.0	http://www.sqlite.org/	Public Domain License	Used
syslog-ng	3.38.1	https://github.com/balabit/syslog-ng	GPLv2	Used
tcpdump	4.9.3	http://www.tcpdump.org/	BSD	Used
udhcp	0.9.8	http://udhcp.busybox.net/	GPLv2	Modified
usb-modeswitch	2.1.0	http://www.draisberghof.de/usb_modeswitch/	GPLv2	Used
util-linux	2.34	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

Known issues

Modules	Issue	Risk Impact Information

Modifications in V5.18(ACHN.0.1)C0

Based on V5.18(ACHN.0.1)b1 to release V5.18(ACHN.0.1)C0

- Feature Enhancement
- Bug Fixed

Modifications in V5.18(ACHN.0.1)b1

- Feature Enhancement
- Bug Fixed

Modified Modules	Bug Fixed List
Vulnerability	[Vulnerability] [Vulnerability] Zyxel-SI-1506 [Vulnerability] Post-authentication buffer overflow in VMG3625-T50B [Vulnerability] Zyxel-SI-1536 [Vulnerability] Buffer overflow vulnerability in the "traceroute" command of DX3300-T1 CPE

Modifications in V5.18(ACHN.0)C0

Based on V5.18(ACHN.0)b6 to release V5.18(ACHN.0)C0

- Feature Enhancement
- Bug Fixed

Modifications in V5.18(ACHN.0)b6

- Feature Enhancement
- Bug Fixed

Modified Modules	Bug Fixed List
MPro Mesh	[#196500] [MPro Mesh] EX7501 Perform Mesh Full Factory Reset --- test failed

Modifications in V5.18(ACHN.0)b5

- Feature Enhancement
- Bug Fixed

Modified Modules	Bug Fixed List
GUI	[GUI] Diagnostic page doesn't work. except Nslookup.

Modifications in V5.18(ACHN.0)b4

- Feature Enhancement

Modified Modules	Features Enhancement List
Wi-Fi	[eITS #230501371] SSID naming logic when disabling mesh and allowing separate SSIDs

- Bug Fixed

Modified Modules	Bug Fixed List
MPro Mesh	[MPro Mesh] AP_agent's beacon disapper after press WPS button.
GUI	[GUI] GUI will display "Backup WAN" page
WAN	[WAN] After reboot / stress, Bridge WAN will inactive. need to apply again. [WAN] WAN LED will off when it link up with 5Gbps [WAN] use DS-Lite DHCP, LAN Client can NOT ping ipv4 (ex: 8.8.8.8) successfully [WAN] In GUI, PPPoE wan display IPoE wan's IPv6 address.
System	[System] GUI to change other language, some description will show English (ex: Dutch). Other(ex: title、options) will still show English, NAT > PCP page always show English. [System] Sometimes Web GUI can not change to others page until refresh it
Security	[Security] Parental Control typesetting issue
USB	[USB] Default admin account can't access security folder

Modifications in V5.18(ACHN.0)b3

Modified Modules	Features Enhancement List
System	[eITS#221101418] OPAL, Partial factory reset option with firmware upgrades.
GUI	[OPAL Generic] GUI translation_ES_NL

● Bug Fixed

Modified Modules	Bug Fixed List
MPro Mesh	[MPro Mesh_Android] When client run Internet Speed test, the Upload value always display 4.46Mbps. [MPro Mesh] Band steering test process controller does not have any 11v action records.
Security	[eITS#230500907] Possible security flaw that allows to retrieve root password. [Security] The subject is null after importing or creating certificate.
GUI	[GUI] Parental control page display incorrect after add two parental control rule. [GUI] Scheduler Rule time should display same as Parental control page. [GUI] In Maintenance > Diagnostic, GUI display "Unknown Host or Unreachable Network!" after key in "www.google.com" and click Trace Route / Trace Route 6 / Nslookup. [System] Some words contain "@@" when the language is Español. [GUI] Some words contain "@@" when the language is Dutch or Türkçe.
SNMP	[SNMP] Use SNMP to get CPE's description, but it does not match the description on CPE box.
TR-069	[TR-069] CPE upgrade firmware from 0b1 to 0b2 via TR-069, but it will upgrade again after connecting to ACS.

	<p>[TR-069] ACS GPV ['Device.DeviceInfo.Description'], but it does not match the description on CPE box.</p> <p>[TR-069] The value format of TR-069 cnonce not hexadecimal.</p>
VoIP	[VoIP] VoIP Region Setting not match with PS.
System	<p>[LED] When Ethernet LAN link speed is 5G, the 10G LAN LED cannot blink.</p> <p>[System] System Log/Security Log can't display correct time.</p>
WAN	<p>[WAN] In PPPoE mode with IPv6 only, CPE does not get IPv6 address after wan type change (ex: IPv4 only <-> IPv6 only). [fail rate: 60%(3/5)]</p> <p>[WAN] DS-Lite tunnel cannot be created when it's configured by DHCPC automatically.</p> <p>[WAN] DS-Lite work fail with AFTR</p> <p>[WAN] In PPPoE mode with IPv4/v6 dual, CPE does not get IPv6 address after wan type change (IPv4/v6 <-> IPv4 only). [fail rate: 60%(3/5)]</p>

Modifications in V5.18(ACHN.0)b2

● Feature Enhancement

Modified Modules	Features Enhancement List
System	<p>[eITS #220901661] Configurable WiFi Country Code (ISO 3166-1 alpha-2)</p> <p>[eITS #220701077][System] [220701077] OPAL, Feature proposal/request - Soft-Reset feature</p> <p>[OPAL Regular] support APP 3.0</p> <p>[ETSI EN 303 645] 5.3-2: When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.</p>
TR-069	[eITS #230200423] TR-098 support for WiFi X_ZYXEL_CountryCode
MPro Mesh	[eITS #221000063] change the wording in SteerStatus
GUI	<p>[eITS #220901550] Translation error WIFI password strength</p> <p>[eITS #221101418] OPAL, Partial factory reset option with</p>

	firmware upgrades. (tr069/gui) 220701077 [GUI] Compact help link adding ito GUI
VoIP	[eITS #221101135][VoIP] SIP TLS encapsulation - supports SIP-over-TLS.
WAN	[eITS #230201111] iperf -R not implemented [eITS #230100744][eITS#230100744] bridge config improvement Interface grouping enhancement with TS enable for BCM solution
DHCP	[eITS #220900410] DHCP option providing CPE firmware version

● Bug Fixed

Modified Modules	Bug Fixed List
DNS	[eITS #230400106] DNSProxy issue when Primary DNS unreachable
TR-069	[eITS #230301653] CurrentTime not reporting in accordance to the TR-069 standard [eITS #230201161] enable/disable SSH via ACS [eITS #230300897] iPerf from tr069 fail, DownloadDiagnostics not ok, UploadDiagnostics ok [TR-181] Lifemote agent not work. [TR-181] TR-069 Script execute cannot work. [TR-181] WiFi GUI not support WEP-64 and WEP-128 security mode but GPV include [eITS #230300429] certificate Common Name doesn't match host name
GUI	[eITS #230300494] GUI menu visible prior to login [GUI] Certificate option of TR-069 Client page can't display correctly. [eITS #230100382] Not possible too enable 5GHz WiFi in GUI, if WiFi first is turned off by physical button [GUI] In Security page, parental Control page does not logout GUI after Idle Timeout. [GUI] In Parental control page, PCP schedule time rule display

	<p>incorrect when start time is empty.</p> <p>[GUI] In Parental control page, PCP schedule rule only display last schedule time when it create 3 schedule time rule.</p> <p>[GUI] LAN IPv6 prefix incorrect after Delegate prefix from WAN is change.</p> <p>[GUI] LAN PC login GUI fail with admin account. In console mode, login admin account without password. (test with production FW)</p> <p>[GUI] 10G LAN display 2.5G LAN on GUI</p> <p>[GUI] Connectivity page should display "Topology" and "list"</p> <p>CPE just will create one Static DHCP entry for STB Vendor ID devices</p>
Security	<p>[Security] GUI display duplicate Scheduler Rule rule.</p> <p>[Security] L2TP function work fail with more AP.</p> <p>[Security] L2TP function will disconnect after modify L2TP rule.</p>
WLAN	<p>[WLAN] WPS Method 2/3 should grayed out when use admin account.</p>
MPro Mesh	<p>[MPro Mesh_Agent] The wifi client's connection type show "Wired" in APP when clients connected guest wifi.</p> <p>[MPro Mesh] The "stale=Yes" scenario occurs during the AP roaming test.</p> <p>[MPro Mesh_Agent] After using "MPro Mesh" APP to logout or swipe up the screen to close it or enable wifi guest, it will always lead APP relogin fail.</p> <p>[MPro Mesh] RP Agent's GUI show wrong SSID after modify main or guest-1 SSID to special characters then turn on WIFI.</p> <p>[MPro Mesh_APP][ACTS] APP keep loading</p> <p>[MPro Mesh] After RP_Agent Onboarding and auto configure success, WX5600 Power LED light will twinkling again.</p> <p>[MPro Mesh] The online wifi client "stale" will be displayed as "Yes" during the AP roaming test</p> <p>[MPro Mesh] EX7501 disable mesh fail via CFG.</p> <p>[MPro Mesh] Agent's info disappear in connectivity page after on-boarding.</p>
MGMT	<p>[MGMT] MGMT remote page to enable SNMP WAN, CPE SNMP</p>

	<p>page function should not auto enable.</p> <p>[MGMT] Hide SSID of Guest/More AP of Wireless 2.4G and 5G can not be enabled via TR-069</p>
QoS	<p>[QoS] GUI will allow user to add a QoS queue with duplicate name "default queue"</p>
WAN	<p>[WAN] In PPPoE mode with IPv6 only, CPE does not get IPv6 address after wan type change (ex: IPv4 only <-> IPv6 only).</p> <p>[WAN] In System Monitor > Log, click Refresh button then GUI will keep loading when CPE has PPPoE WAN.</p> <p>[WAN] PPPoE Passthrough cannot work</p> <p>[WAN] In PPPoE mode with IPv4/v6 dual, CPE does not get IPv6 address after wan type change (IPv4/v6 <-> IPv4 only).</p> <p>[WAN] LAN PC get new IPv6 prefix after click home networking page two times.</p> <p>[WAN] DUT cannot upgrade firmware via DHCP option 43 mechanism.</p> <p>[WAN] CPE not support MAP-E/MAP-T function.</p> <p>[WAN] CPE does not send release packet before CPE reboot.</p> <p>[WAN] In IPv4/v6 mode, CPE does not send release packet when click release button.</p> <p>[WAN] VLAN Auto-Hunt function work fail and LAN PC does not access GUI.</p>
System	<p>[System] System Log/Security Log can't display correct time.</p> <p>[System] CPE LAN LED will not Flickering, when traffic is ongoing</p> <p>[LED] LAN LED can NOT Flickering Green even there is traffic be transmitted.</p> <p>[System] after unplug/plug IPoE WAN cable, syslog can't not display on GUI</p> <p>[System] CPE does not match DST</p> <p>[System] CPE should support "Restore Partial Default Settings After Firmware Upgrade"</p> <p>[System] CPE should support "Partial Factory Reset"</p> <p>[System] after upload ROM file can't use GUI.</p> <p>[eITS #221200930] romd backup include option 125 devices</p>

	specific option value [eITS #230101319] Lifemote trigger uncontrolled memory usage with script that is working for all other device types
VoIP	[VoIP] The Region Setting of VoIP that CPE supports are not match to PS [VoIP] When set Call Waiting Reject Timer of SIP Account to illegal value "empty", CPE should take correct values after pop warning message
LAN	[LAN] The photo of devices in Topology page should match to List page [LAN] RA packet that send from CPE LAN lack some option [LAN] Auto reserve IP for the same host works fail [LAN] When connect only one LAN Client to CPE and set Device Name of LAN Client to 64 characters, CPE cannot be display properly in the connectivity Topology page. [LAN] GUI display DHCP state is enable, but LAN PC can't get IP from CPE , LAN set static IP and it can not access internet (test with production FW)
Wireless	[OPAL Generic] Max wireless clients limited to 32 pr band

Modifications in V5.18(ACHN.0)b1

● Feature Enhancement

Modified Modules	Features Enhancement List
DHCP	[eITS #220900410] DHCP option providing CPE firmware version
DS-Lite	[eITS #221200506] Configuration of the AFTR should be possible with URL
System	Console redirect / Zconsole monitor [eITS #220301182] add possibility periodically reboot CPE using standard scheduler
GUI	[GUI] Compact help link adding it to GUI Networks Topology
Security	[ETSI EN 303 645] 5.8-2: The confidentiality of sensitive personal data communicated between the device and associated

	services shall be protected, with cryptography appropriate to the properties of the technology and usage [ETSI EN 303 645] The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces
Http	Support Web http redirect to https.
Wifi	[eITS #210900469][OPAL Generic] Change WPS button trigger condition redmine, subnet configurable for TS enable

● Bug Fixed

Modified Modules	Bug Fixed List
GUI	warning message for IP conflict when TS enable
System	[eITS #230100138]rom-d backup
WAN	[eITS #221101734]No Management connection with new FW Version
Wifi	[eITS #220601144]WiFi button not working correct (behavior change)
Security	[CVE-2022-4203,4304,4450] [CVE-2023-0215~0217,0286,0401] [Zyxel-SI-1464] [Vulnerability] OpenSSL multiple vulnerabilities
TR-069	[eITS #221100865]TransferComplete messages without Start/Complete Time value [eITS #221200452]Activate IPV6 Default gateway by TR069 [eITS #220900371]NTP Time Server URL cannot support "-" [eITS #220401035][TR-069] SPV WiFi BeaconType failed [eITS #221101357]Issues with setting some parameters via TR069
ZYEE	[System]Refresh button in ZyEE Monitor page works fail [System] The Active and Idle button for EU cannot work