INDUSTRIAL CONNECTIVITY / ENGLISH TECHNICAL DOCUMENT

CM520-6X Series

Vehicle router - installation and configuration manual



Original source photograph



Original source photograph

Source manual V1.2 | source date 2020-01-22 (as printed) | English review edition | 19 October 2026

REVIEW EDITION - translated from the supplied Chinese document. Source inconsistencies and optional features are retained. See the final review checklist.

Inside this document

Product and configuration / Hardware and radio / Installation and operation (manual) / Source review notes

Document notices and revision history

Source pp. 1-3

CM520-6X Series Router User Manual. Xiamen CAIMORE Communication Technology Co., Ltd. Source copyright 2003-2018. Postal code 361009. Source slogan: CAIMORE Communications - connecting the world.

All contents are protected by copyright. Without written authorization from Xiamen CAIMORE Communication Technology Co., Ltd., no organization or individual may reproduce or republish the whole manual or any part, or distribute it by any means. CAIMORE, its logo and other CAIMORE marks belong to the company; other marks belong to their respective owners.

Contents may be updated because of product upgrades or other reasons. Unless otherwise agreed, the document is an operating guide; statements, information and recommendations do not constitute any express or implied warranty.

Recommended or default settings are not necessarily suitable for an application. Users must inspect every delivered configuration parameter and adjust it to their project and business needs. The source disclaims liability for incorrect configuration and communication problems caused by virus attacks; users must strengthen protection against such attacks.

English editorial treatment: all procedural text and parameter explanations are typeset in English. Original Chinese firmware screenshots are retained as reference images where useful; they do not establish an English firmware interface or universal defaults. Source figure numbers and source page references identify the original illustrations. Repeated screenshot-only examples are consolidated into translated settings tables.

Revision history as printed

Revision	Change	Release date	Author
V1.0	First official release	2017-10-11	cyq
V1.1	Added 5G description	2020-07-10	Zhengfh
V1.2	Updated descriptions of selected functions	2020-01-22	Zhengfh

Manufacturer contact

Parameter	Source specification
Company	Xiamen CAIMORE Communication Technology Co., Ltd.
Header address	Unit 802-7, Building C10, Software Park Phase III, Jimei District, Xiamen, China.
Cover contact address	Units 901 and 904, No. 63 Chengyi North Street, Software Park Phase III, Jimei District, Xiamen, China.
Telephone / fax	+86-592-5902655 / +86-592-5975885

Parameter	Source specification
Websites / email	www.caimore.com / www.caimore.com.cn / caimore@caimore.com

Guide to this English edition

Source pp. 4-5

Settings and explanations

Parameter	Source specification
Chapter 1	Product overview, pictures, naming, selection, functions, hardware and LEDs; source pp. 6-23.
Chapter 2	Packing list, panels, SIM and antenna installation; source pp. 24-26.
Chapter 3	Cellular and wired quick configuration, PC setup and support; source pp. 27-34.
Chapter 4	Network, routing, NAT/DMZ, keepalive, QoS, VPN, hotspot operations, network services and management; source pp. 35-81.
Chapter 5	Troubleshooting; source p. 82.
Appendices 1-5	SSH, serial console, factory reset, network reference and DNS; source pp. 83-91.

1.1 Product overview

Source p. 6

The router provides 2.4 GHz and 5 GHz Wi-Fi channel options with WAN VPN tunnels and WLAN security authentication, connecting wireless LAN and mobile WAN services. The overview calls the processor industrial MIPS; the hardware table calls it ARM. Both statements are preserved pending verification.

The embedded operating platform provides GRE, PPTP, L2TP, IPsec, OpenVPN and N2N; IPTABLE firewall; static/dynamic routing; PPPoE; PPP server/client; DHCP server/client; Wi-Fi client; DDNS; SNAT/DNAT; DMZ; web configuration; APN/VPDN; power-on dialing; automatic link maintenance; scheduled online/offline operation and customized scheduled power switching.

Industrial design includes CPU WDT and System Watch Protect (SWP). The source reports a 3000 V electrical test and proprietary stability technology; continuous-online and reliability statements are source claims, not measured acceptance results.

Applications include small-business/home Internet, financial and postal transactions, smart grid/transport, environmental/fire/security/water monitoring, public safety, advertising, remote surveying, industrial control,

oilfield/coal-mine/seismic/weather/instrument monitoring, water/electricity/gas meter reading, heat-network monitoring and centralized meter reading.



Original source hardware photograph



Original source hardware photograph

1.3 Product naming and model selection

Source pp. 7-8

Naming example: CM 520 - 6 2 F - (S). Fields represent the company mark, product category, hardware platform, enclosure/configuration code, network type and special version. Model codes describe available variants; the manual does not make every optional function standard.

Network suffixes

Parameter	Source specification
W	WCDMA
S	TD-SCDMA
E	EV-DO
T	LTE TDD/FDD, excluding EVDO/CDMA
F	LTE TDD/FDD, all-network version as described in the source
H	HSPA+
FS	5G

Configuration codes

Parameter	Source specification
1	Single modem; dual Wi-Fi
2	Single modem; 2.4 GHz Wi-Fi
3	Single modem; 5.8 GHz Wi-Fi
4	Single modem; dual Wi-Fi; GPS
5	Single modem; 2.4 GHz Wi-Fi; GPS
6	Single modem; 5.8 GHz Wi-Fi; GPS
7	Dual modem; dual Wi-Fi
8	Dual modem; dual Wi-Fi; GPS
9	Dual modem; 2.4 GHz Wi-Fi
A	Dual modem; 5.8 GHz Wi-Fi
B	Dual modem; 2.4 GHz Wi-Fi; GPS
C	Dual modem; 5.8 GHz Wi-Fi; GPS

Ordering notes

Parameter	Source specification
Listed base models	CM520-6A / 6B / 6C / 61 / 62 / 63 / 64 / 65 / 66 / 67 / 68 / 69.
Ethernet	All listed models show one WAN and four LAN ports.
SIM slots	Single-modem models show one SIM/UIM slot; dual-modem models show two in the procurement table.
Storage	The table marks a TF slot and SSD for the listed variants; cards and drives are customer-purchased. The software table later says the TF interface is reserved and not currently supported: NEEDS_VERIFICATION.
Optional SSD capacities	64G, 128G, 256G and 512G as printed. Later hardware text states up to 2T.
GPS	Selection depends on model; the software section also calls GPS / BeiDou non-standard and requires specifying it at purchase.

1.5 Industrial design and reliability

Source pp. 9-10

Settings and explanations

Parameter	Source specification
Vehicle power / enclosure	Secure vehicle-specific power connector; industrial metal enclosure described as reducing fire risk; I/O for vehicle fault detection/alarm and GPS location depend on configuration.
Processor	Industrial ARM; 32 KB D-cache and 64 KB I-cache. The overview says MIPS: NEEDS_VERIFICATION.
Operating system	Linux with MMU, a complete TCP/IP stack and real-time operation as described.
PCB / components	PCB follows stated 20H and 3W principles; high-quality board materials and selected industrial components.
Power protection	7-32 V DC; reverse-polarity, overvoltage and overcurrent protection.
Ethernet isolation	1.5 kV
Interference protection	Metal shielding, antenna lightning-protection design, IP31 in this section; a later physical row says IP30.
Online maintenance	Online detection, automatic redial and reset after abnormal operation.
System protection	Software protection, CPU WDT and Virtual Man Watch (VWM).
SIM / serial ESD	SIM 1.8/3/5 V push-type interface and RS232: 15 kV ESD protection.
Wireless modules	Source states CGD, FCC or CE certification; CGD is undefined.
Memory	DDR3/1066, 4 Gbit in this reliability section; hardware table later lists 4-16 Gbit.
EMC and tests	Source reports a 3000 V electrical test; CE, ROSH (source spelling), CCC, network access and CRCC. Exact test conditions and certification scope NEEDS_VERIFICATION.

1.6 Software functions

Source pp. 11-13

Factory defaults and graphical quick/batch configuration simplify commissioning. The manual includes quick-start steps. SYSLOG and serial debugging levels support operating-log inspection and fault analysis.

Access and LAN functions

Parameter	Source specification
Cellular	Single 3G/4G/5G or dual 4G/5G modules; LTE TDD/FDD, TD-SCDMA, WCDMA, EVDO, GPRS and CMDA2000 as printed; APN/VPDN, link detection, keepalive and automatic redial.
Other WAN modes	Static IP, DHCP client, PPPoE; Wi-Fi client; wired-primary/cellular-backup; switch mode; mwan3 bandwidth aggregation as described.
LAN	4 Gigabit LAN ports.
Wi-Fi modes	Dual Wi-Fi modules, 2.4/5 GHz selection; 802.11a/b/g/n/ac; AP, client, Ad-Hoc, AP WDS, client WDS and static WDS.
Local services	dnsmasq DNS/DHCP services; source repeats all-network cellular/APN/VPDN support in its LAN group.

Advanced functions and VPN

Parameter	Source specification
Networking	NAT including SNAT/DNAT, DMZ, static routes; TCP/IP, UDP, ICMP, SMTP, HTTP, POP3, OICQ, Telnet and FTP.
Services	NTP, IPTABLES firewall, packet filtering, QoS, rate limits, traffic monitoring and application filtering.
Dynamic DNS	PeanutHull, 88IP, dyndns; PeanutHull intranet version.
VPN	PPTP client/PPTPD server; L2TP client/L2TPD server; IPsec, OpenVPN and N2N.

Management and hotspot operation

Parameter	Source specification
Local management	Default LAN web access 192.168.9.1:9999; firmware upgrade with optional configuration retention; SSH shell; serial software upgrades; COM/SYSLOG diagnostics.

Parameter	Source specification
Status	Device state, packet counters by working interface and VPN state.
Custom control	3 control outputs, including source example of vehicle ignition shutdown; NOT standard, requires customization.
Hotspot functions	Wi-Fi MAC probing/reporting; user URL collection/reporting; local, inline and targeted advertisements; nginx + PHP + MySQL.
Depot updates	Multimedia updates over depot Wi-Fi, reduced cellular traffic and resume support.
Portal	WiFidog; one-click, WeChat, SMS and local authentication.
Remote platform	Status; batch settings, firmware and multimedia updates; grouping; traffic control; data reporting and analysis.
TF	One card up to 256G; reserved interface, temporarily unsupported in this software row.
SSD	One drive up to 2T, depending on market availability as stated.
Positioning	Optional GPS / BeiDou; specify when purchasing.

1.7 Hardware, interfaces and power

Source pp. 14-18

Hardware and OS

Parameter	Source specification
CPU	Industrial ARM: 1.4 GHz (dual core) main frequency; 733 MHz (dual core) secondary frequency, as written.
MMU	CPU memory-management unit.
NOR Flash	256 Mbit; do not substitute the 512 Mbit value from the separate 6XX datasheet.
DDR3	32-bit DDR3, 4-16 Gbit.
SSD	Up to 2T.
OS	Linux with MMU; real-time and upgrade capabilities as described.

Interfaces

Parameter	Source specification
WAN	1 adaptive 10/100/1000 Mbps port; Auto MDI/MDIX; PPPoE.
LAN	4 adaptive 10/100/1000 Mbps ports; Auto MDI/MDIX; 1.5 kV isolation.
Serial	1 RS232 OR RS485; 7/8 data bits; 1/2 stop bits; none/odd/even parity; 300-115200 bit/s; no flow control.
LEDs	POWER, SYS, link 1 and link 2 online status and wireless-signal indicators.
Antennas	SMA female, 50 ohm; optional 1/3/5/10 m extensions. The physical table separately says 8 RP-SMA antennas.
UIM	1.8/3/5 V push-type interface; 15 kV ESD protection.
Power connector	Aviation connector or vehicle connector.
RESET	Restores factory settings.
TF	32-256G in the interface table, conflicting with the reserved/unsupported software row.

Power table

Parameter	Source specification
Input	7-32 V DC with reverse-polarity, overvoltage and overcurrent protection.
Standard supply	9 V DC / 1.5 A.
Communication current	Average 390 mA at 9 V DC; registration peak 1.0 A at 9 V DC.
Standby	Average <56 mA at 9 V DC.
Supply systems	110 V train supply, vehicle supply or 220 V adapter supply are listed. Power-conversion/configuration requirements are not defined; do not apply these high voltages to the low-voltage input.

Physical table - retained as a separate source group

Parameter	Source specification
Enclosure	Metal shielding, interference resistance, enclosure/system isolation, lightning-protection design and power-safety requirements. This row says IP30; another row says IP31.
Body	228 x 144 x 35 mm, excluding antennas and mounting hardware.
Package	340 x 327 x 80 mm
Weight	1.02 kg
Antennas	8 RP-SMA
Consumption	Peak <=12 W; average 9 W.
Adapter	12 V DC +/-10%, conflicting with the separate standard-supply value of 9 V / 1.5 A.
Operating	-25 to +70 °C; extended -30 to +75 °C.
Storage	-40 to +80 °C
Humidity	Operating 5-95%, non-condensing; storage 0-100%, non-condensing.
Protection	IP31 in this row; IP30 elsewhere.
Certification	CCCI as printed; exact certificate name and scope NEEDS_VERIFICATION.

1.7 Cellular radio parameters

Source pp. 19-20

These are source-era modem options and theoretical rates. Band and service support vary by module; no availability inference or correction to questionable units/directions is made.

4G / 5G radio

Parameter	Source specification
Module	Industrial-grade.
Bands	5G NR: n1/n2/n3/n5/n7/n8/n20/n28/n41/n66/n71/n77/n78/n79; LTE TDD B38/39/40/41; LTE FDD B1/2/3/4/5/7/13/17/25; TD-SCDMA B34/39; GSM B2/3/8; UMTS B1/5. Overseas bands are listed in the source.

Parameter	Source specification
Schemes	LTE/UMTS/HSPA+/DC-HSPA+/HSDPA/HSUPA/WCDMA/EDGE/GSM.
5G NR	DL 3.4 Gbps / UL 350 Mbps.
LTE	TDD DL 61 Mbps / UL 18 Mbps; FDD DL 100 Mbps / UL 50 Mbps.
HSPA family	DC-HSPA+ DL 42 / UL 5.76 Mbps; HSPA+ DL 28 Mb/s (Category 18); HSDPA DL 14.4 Mb/s (Category 8); HSUPA+ DL 42 / UL 5.76 Mbps, as printed.
Legacy rates	WCDMA CS DL/UL 64 kbps; PS DL/UL 384 kbps; EDGE DL 237 / UL 118 kbps; GSM DL/UL 171 kbps, as stated.
Transmit / receive	WCDMA/HSDPA 24 dBm; LET 23 dBm (source spelling); sensitivity <-109 dBm.
Functions	Data, voice, SMS and fax.

China Unicom 3G radio

Parameter	Source specification
Module	Industrial-grade.
Rates	HAPA+ DL 21 / UL 5.76 Mbps (source spelling); HSDPA/HSUPA DL 7.2 / UL 5.76 Mbps; WCDMA DL/UL 384 kbps; EDGE DL 237 / UL 118 kbps; GPRS DL/UL 85.6 kbps; CSD UL 14.4 kbps.
Transmit / receive	<24 dBm; sensitivity <-109 dBm.
Functions	Data, voice, SMS and fax.

China Mobile 3G radio

Parameter	Source specification
Module / bands	Industrial module; TD-SCDMA 2010-2025 MHz; GSM/GPRS/EDGE 850/900/1800/1900 MHz; 3GPP class B.
Schemes	TD-SCDMA/HSDPA/HSUPA/EDGE/GPRS
Rates	DL 2.8 Mbps / UL 384 kbps
Transmit / receive	<24 dBm; sensitivity <-108 dBm.
Functions	Data, voice, SMS and fax.

China Telecom 3G radio

Parameter	Source specification
Module / bands	Industrial module; IS-95 A/B, CDMA2000 1XrTT and 1X EV-DO revisions 0/A. 800 MHz single band; optional 800/1900 MHz dual band or 450 MHz single band.
Schemes	IS-95 A/B, CDMA2000 1XrTT, 1X EV-DO.
Rates	The source labels BOTH up to 3.1 Mbps and up to 1.8 Mbps as uplink. Direction NEEDS_VERIFICATION.
Transmit / receive	<23 dBm; sensitivity <-107 dBm.
Functions	Data, voice, SMS and fax.

1.7 Wi-Fi and GPS parameters

Source pp. 21-22

Wi-Fi radio parameters

Parameter	Source specification
Modules	802.11b/g/n: dual-band 3 x 3 MIMO, 450 Mbps; 802.11ac: dual-band 3 x 3 MIMO, 1.3 Gbps, as described in the source. Exact radio architecture depends on variant.
Frequency	802.11b/g/n: 2.412-2.472 GHz, 13 channels (3 non-overlapping); 802.11a/n: 5.180-5.825 GHz.
Transmit power	23 dBm for the complete device, as stated.
MTBF	>=100,000 hours, as stated in this manual; the separate 6XX datasheet says >=20,000 hours.
Client capacity	150 simultaneous single-band users; 253 dual-band users, as stated in this manual.
Security	64/128-bit WEP; WPA-PSK/WPA2-PSK; TKIP and CCMP/AES.
Range	Up to 150 m outdoors in an unobstructed open area, a source claim without test conditions.

GPS / BeiDou parameters

Parameter	Source specification
Module	Industrial GPS / BeiDou module; available according to model.
Receiver	50 channels; L1; 1.023 MHz chip rate and C/A code. SBAS: WAAS, EGNOS, MSAS; stated GALILEO compatibility.
Position accuracy	Position: 2.5 m CPE; SBAS: 2.0 m CPE, exactly as printed. The CPE accuracy abbreviation NEEDS_VERIFICATION.
Velocity / heading accuracy	<0.01 m/s (high speed); <0.01 degree heading (50% at 30 m/s), as stated.
Time accuracy	1 microsecond, synchronized to GPS time.
Acquisition	Cold start: 27 s; assisted start: <3 s; hot start: <1 s.
Data format	NMEA-1083 and SiRD binary, as printed; terminology NEEDS_VERIFICATION.
Input	NMEA / SiRF binary: altitude, position, date and time.
Output	NMEA-0183 / SiRF binary: GGA, GSA, GSV, RMC, VTG, GLL.
Pulse output	1 pps, accuracy +/-1 microsecond.
Navigation update	5 Hz
Sensitivity	Tracking -162 dBm; cold start -147 dBm; hot start -156 dBm.

1.8 Indicator meanings

Source p. 23

LED states

Parameter	Source specification
POWER	On: powered normally. Off: not powered.
SYS	Flashing: program running. Off: no program running, as described.
Online1 / SIM1	On: registered on the network. Off: not registered.
Online2 / SIM2	On: registered on the network. Off: not registered.

Parameter	Source specification
Signal 1	1-1 off / 1-2 off: signal <12; 1-1 on / 1-2 off: >=12 and <25; both on: >=25. The source gives no unit.
Signal 2	All three signal bands (<12, >=12 and <25, >=25) are printed with 2-1 off / 2-2 off. This is inconsistent; the intended LED combinations NEEDS_VERIFICATION.

2. Installation

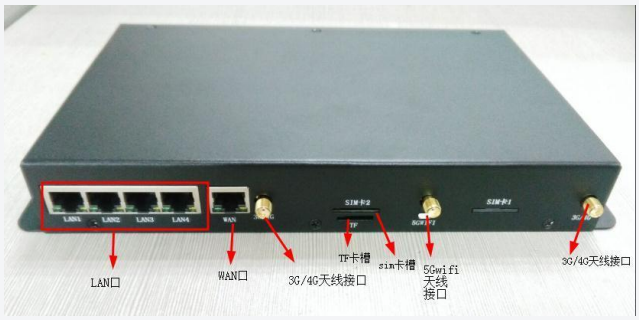
Source pp. 24-26

Unpack the equipment and check the contents against the packing list. Exact shipment contents depend on the purchased configuration.

- SIM installation: with power OFF, insert the SIM horizontally, contacts facing down and the notched edge inward. Press once to latch it in the push/push holder. The source specifies 1.8/3/5 V SIM support. Never insert or remove the SIM with power applied.
- Connect the appropriate cellular and Wi-Fi antennas to the corresponding ports shown in the original installation photographs. The source illustrates antenna placement rather than specifying torque or spacing limits.



Original front panel; numbered callouts are translated in the table



Original rear panel

Packing list

Parameter	Source specification
Gateway	1
RJ45-DB9 cable	1
9 V DC adapter	1
Straight-through Ethernet cable	1
Cellular antennas	2 for 3G/4G; 4 for 5G, as specified.

Parameter	Source specification
5.8 GHz Wi-Fi antennas	3
2.4 GHz Wi-Fi antennas	3
Manual CD	1

Front-panel numbered callouts

Parameter	Source specification
1 / 7	5 GHz Wi-Fi antenna connectors (5G here denotes Wi-Fi frequency, not cellular generation).
2 / 3	POWER / process (SYS) LEDs.
4	SIM1 and SIM2 online LEDs.
5 / 6	SIM1 / SIM2 signal LEDs.
8	RESET
9 / 11 / 13	2.4 GHz Wi-Fi antenna connectors.
10 / 12	Serial port / power socket.

3.1 Quick configuration - cellular WAN

Source pp. 27-32

The quick-start procedure checks basic hardware operation and configures WAN/LAN parameters. Windows 7 is the source example. Other settings may remain at defaults for the source example, but all delivered settings must still be checked against the project requirements stated in the document notices. The heading calls this PPPoE disable mode.

- 1. With power removed, install the SIM; identify the SIM, TF, cellular and 5 GHz Wi-Fi sockets from the panel photographs.
- 2. Connect the antennas. Connect the PC directly to a gateway LAN port using Ethernet.
- 3. On the PC, open Start > Control Panel > Network and Internet > Network and Sharing Center > Local Area Connection > Properties > Internet Protocol Version 4 (TCP/IPv4).
- 4. Method 1: obtain IP and DNS automatically. Method 2: use a static IP in the gateway subnet and the DNS shown in gateway status after dialing. If the SIM/operator changes, recheck DNS.
- 5. Static example: gateway LAN1 is 192.168.9.1; PC is 192.168.9.X, X from 2 to 254 (example 2), mask 255.255.255.0 and default gateway 192.168.9.1. Avoid duplicate PC addresses; use a mask appropriate to the

selected subnet.

- 6. Open the source example browser (IE) and enter 192.168.9.1 or 192.168.9.1:9999. The printed default credentials are admin / admin.
- 7. Select WAN Configuration, enter operator-provided dial information and submit. The source normally uses defaults, requiring changes for private APN/VPDN service; it says 4G fields are blank by default. Do not assume private-network credentials.
- 8. Power-cycle the device; SYS should flash. Wait for Online to light, then browse a website. Successful browsing verifies the source quick-start example of Internet/data access.



Original firmware reference, source p. 31. Field explanations are translated below; interface labels remain as supplied.

3.2 Wired WAN and 3.3 Support

Source pp. 32-34

- 1. Connect the antennas, and connect the gateway WAN port to the upstream network using Ethernet.
- 2. Configure the PC IP, gateway and DNS as in the cellular quick start.
- 3. Browse to 192.168.9.1 or 192.168.9.1:9999, log in, open WAN Configuration and enter the upstream-network settings. Configure LAN settings in LAN Configuration.
- 4. Power-cycle the device. Check flashing SYS and illuminated Online, then test web browsing and data access.

Settings and explanations

Parameter	Source specification
Technical support	Visit www.caimore.com for online support, or call +86-592-5908951 / +86-592-3799892 as printed in the manual. These source-era numbers have not been independently revalidated.

4.1.1 WAN configuration

Source pp. 35-39



Original firmware reference, source p. 37. Field explanations are translated below; interface labels remain as supplied.

WAN modes and fields

Parameter	Source specification
Static IPv4 (Fig. 4-1-1)	IPv4 address: same subnet as upstream WAN; mask: corresponding subnet mask. MAC: assigned automatically unless a fixed address is required. Gateway: upstream-subnet gateway. DNS: operator DNS or another usable service; the source example includes 8.8.8.8.
DHCP client (Fig. 4-1-2)	Obtain the WAN IP configuration automatically.
PPPoE (Fig. 4-1-3)	Enter the username and password supplied by the operator.
4G/5G dialing (Fig. 4-1-4)	Dial number, APN, username and password are factory-set according to network. Usually leave unchanged; enter operator-provided values for a private VPDN (source spells VPND here). Source says 4G/5G fields are blank by default. Network search is normally automatic; select the corresponding mode if dialing repeatedly fails.
Primary/backup (Fig. 4-1-5)	Primary can be static IP, DHCP client or PPPoE. Configure primary access and SIM dialing as above. Primary is preferred; cellular dialing takes over if primary cannot connect.
Switch mode (Fig. 4-1-6)	Use the gateway as a switch.
Dual-modem mode (Fig. 4-1-7)	Configure SIM dialing 1 and 2. Both modules connect simultaneously for source-described bandwidth aggregation. On dual-module hardware using single cellular dialing, the source says SIM2 is detected first: place the only SIM in slot 2.
Wi-Fi client (Fig. 4-1-8)	Enter upstream SSID and password. The upstream Wi-Fi IP subnet must differ from the gateway LAN subnet.

4.1.2 LAN configuration

Source p. 40



Original firmware reference, source p. 40. Field explanations are translated below; interface labels remain as supplied.

Settings and explanations

Parameter	Source specification
IP address	Address used by gateway Wi-Fi and LAN1-4; default 192.168.9.1.
Subnet mask	Set the mask for the local IP subnet.
MAC address	LAN1-4 MAC; automatically assigned in the source description.
Preferred / alternate DNS	Preconfigured by default; enter stable project DNS addresses if required.
Checks	Connected devices must share the gateway subnet. The source warns that restoring factory settings may reset MAC values and cause conflicts when several gateways share a LAN; check and change conflicting addresses. After dialing, verify that configured DNS resolves domain names.

4.1.3 Wi-Fi configuration - 2.4 GHz and 5 GHz

Source pp. 41-46

The source repeats nearly the same field explanations for both radios. Figures 4-1-10 to 4-1-22 cover radio and security settings. 5G Wi-Fi in this chapter means 5 GHz Wi-Fi. Some repeated radio modes/channels are inconsistent with that band and require firmware verification.



Original firmware reference, source p. 41. Field explanations are translated below; interface labels remain as supplied.

Radio and network fields

Parameter	Source specification
Channel	Choose the operating channel; normally change only if nearby AP interference is present. The source recommends 1/6/11 in BOTH sections; that advice must not be assumed valid for the 5 GHz radio.
Transmit power	Controls radio output; the source associates greater power with wider coverage.
Radio mode	Listed options: 802.11b, g, a, g+n mixed, a+n mixed, ac mixed. Select a mode supported by the actual radio and clients.
Channel width	Bandwidth occupied for the required transmission rate/quality.
Country code	Short geographic code identifying country/territory.
Distance optimization / fragmentation / RTS-CTS	Use defaults; no numeric values are supplied in the text.
Operating mode	AP, Client or Wireless Repeater.
ESSID	Wireless network name, up to 32 characters. Defaults: CaiMore_WiFi_2G and CaiMore_WiFi_5G. The source recommends changing them to avoid confusion with nearby devices.
BSSID	AP MAC address identifying its basic service set.
Hide SSID	If hidden, the network is not shown in scans; already associated clients remain connected as described.

Security options

Parameter	Source specification
None	Open network with no data encryption or password authentication.
WEP open authentication	WEP with open-system authentication; key #1 length 5, 13 or 16 characters as printed.
WEP shared key	WEP with shared-key authentication; key #1 length 5, 13 or 16 characters as printed.
WPA-PSK	Pre-shared key, 8-63 characters. Cipher options: automatic, CCMP/AES, TKIP or TKIP + CCMP/AES mixed.
WPA2-PSK	Pre-shared key, 8-63 characters; source mentions AES and also repeats automatic/CCMP/TKIP/mixed choices. Verify actual firmware choices.
WPA/WPA2 mixed	Pre-shared key, 8-63 characters; automatic/CCMP/TKIP/mixed cipher options.
Applicability	Options are translated from the legacy source, not recommendations for a new security configuration.

4.1.4 DHCP and 4.1.5 VLAN

Source pp. 47-48

DHCP automatically assigns LAN IP address, subnet mask, gateway and DNS parameters. It is enabled by default in the source; disable DHCPD if it is not needed. The source expands the acronym as Dynamic Host Control Protocol, which requires editorial correction before a public edition.



Original firmware reference, source p. 47. Field explanations are translated below; interface labels remain as supplied.

DHCP fields (Fig. 4-1-24)

Parameter	Source specification
Start address	First automatically allocated address.
Client count	Number of addresses the DHCP server allocates.

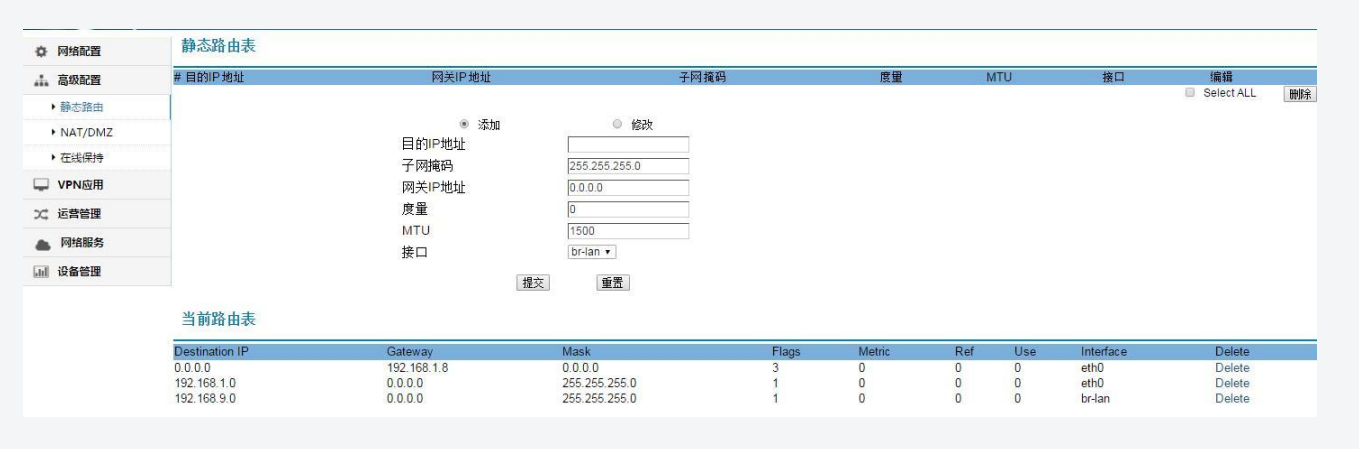
VLAN port membership (Fig. 4-1-23)

Parameter	Source specification
Off	Port is not used in that group.
Unassociated	Source wording for a port bridged directly into the group. Exact tagged/untagged UI terminology NEEDS_VERIFICATION.
Associated	Source wording for access to the group through a VLAN ID.
Precaution	The source advises that VLAN changes be made only by personnel familiar with VLAN configuration.

4.2.1 Static routing

Source pp. 49-52

The default route sends traffic toward the public network. Add routes manually for specific networks and inspect the routing information after saving. If an added route is absent, check that the destination network number is valid.



Original firmware reference, source p. 49. Field explanations are translated below; interface labels remain as supplied.

Route fields (Fig. 4-1-25)

Parameter	Source specification
Destination IP	Destination host or network.
Subnet mask	Destination mask; use 255.255.255.255 for a host route.
Gateway IP	Next-hop address; source permits 0.0.0.0 if no gateway is required.
Metric	Default 0.
MTU	Default 1500.
Interface	System interface used by the route.

Source routing example (Figs. 4-1-26 to 4-1-29)

Parameter	Source specification
Topology	Source names networks 192.168.1.0/24, 192.168.3.0/24 and 192.168.2.0/24.
Router interfaces	LAN1-4 IP 192.168.1.2; operator-assigned ppp0 110.91.69.133; ppp1 VPN-tunnel IP 192.168.2.8.
VPN server	eth0 172.16.0.1; public IP 121.204.199.230; tunnel0 192.168.2.6. These are source examples, not addresses to deploy.
Traffic objective	Host 172.16.0.2 accesses 192.168.3.2. Add a server route to 192.168.3.0/24 using the server vendor instructions.
Router route 1	Source says destination 192.168.3.0/24 goes to br-lan, because that network is on LAN1-4.
Router route 2	Source says destination 172.16.0.0/24 goes through eth0 with gateway 192.168.2.6; earlier text uses /16. Subnet/interface consistency NEEDS_VERIFICATION before applying this example.

4.2.2 NAT / DMZ

Source pp. 53-54

NAT means Network Address Translation. Port-forwarding rules map incoming WAN traffic to the specified internal host and service port. DMZ forwards incoming traffic to a selected LAN host for direct two-way connectivity as described in the source.



Original firmware reference, source p. 53. Field explanations are translated below; interface labels remain as supplied.

Port mapping (Fig. 4-2-1)

Parameter	Source specification
Rule name	Unique identifier; allowed characters are 0-9, dot, a-z and A-Z.
Protocol	TCP/UDP, TCP or UDP.
External zone	WAN.
External port	Incoming TCP/UDP destination port.
Internal IP	LAN host to receive forwarded traffic.
Internal port	Service port on the internal host.

DMZ (Fig. 4-2-2)

Parameter	Source specification
Enable	Select Enable DMZ, enter the virtual-server / internal-host IP in Destination Address, then Submit. The source notes that DMZ exposes that LAN computer to the Internet.

4.2.3 Online keepalive and 4.2.4 Bandwidth management

Source pp. 55-56

Online keepalive periodically tests the cellular data channel and automatically redials on failure, intended for unattended operation. Choose a stable destination IP and port with a functioning service; an unstable test server can cause repeated disconnections. Default interval and timeout count are sufficient for the source example.

The source warns that disabling keepalive may prevent automatic recovery after a disconnection. Its defaults target the public network; private-network deployments require reachable private targets. Otherwise frequent redialing may occur.



Original firmware reference, source p. 55. Field explanations are translated below; interface labels remain as supplied.

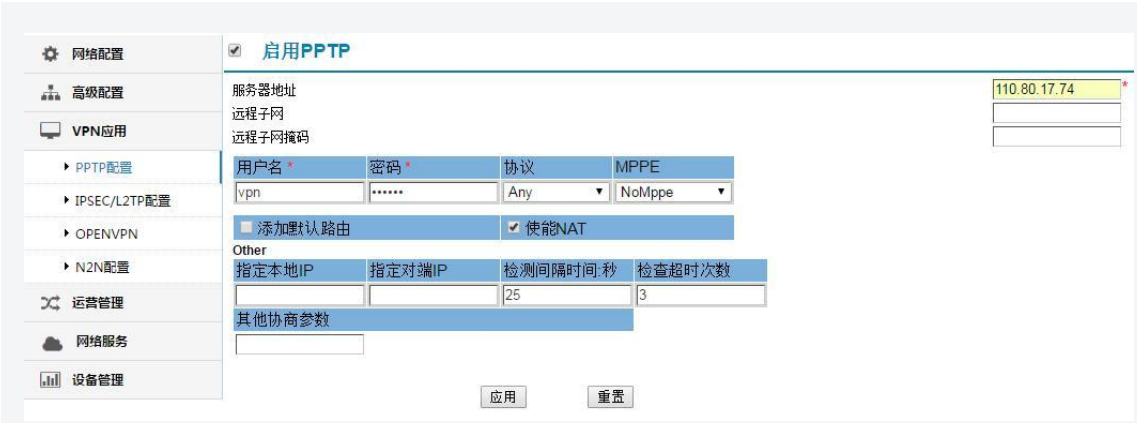
Bandwidth fields (Fig. 4-2-4)

Parameter	Source specification
Maximum upload / download	Device-wide upstream and downstream speed limits.
Rule name	Identifier for the bandwidth rule.
IP address	Host or range to limit.
Equal-share mode	Whether to divide bandwidth equally.
Upload / download bandwidth	Maximum upstream/downstream bandwidth for the rule.

4.3.1 PPTP

Source pp. 57-58

PPTP carries PPP frames over an IP network. The source describes a TCP connection for tunnel maintenance and GRE for frame transport; PPP payloads may be encrypted or compressed. It can also connect private LANs.



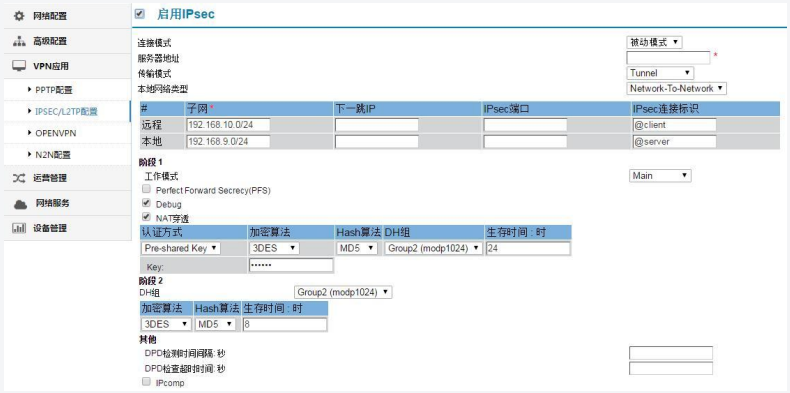
Original firmware reference, source p. 57. Field explanations are translated below; interface labels remain as supplied.

PPTP settings (Fig. 4-3-1)

Parameter	Source specification
Server address	Server IP or domain.
Remote subnet / mask	Network behind the server.
Username / password	Credentials for server access.
PPP authentication	PAP (source notes plaintext credentials and low security), CHAP, MS-CHAP, MS-CHAPv2 or Any. Source default recommendation is Any unless otherwise required.
MPPE	NoMppe: no MPPE; Mppe(40/128): MPPE40/128; Mppe-StateFul: stateful MPPE.
Add default route	Source says all traffic is sent through the VPN and attached hosts can then access only the VPN network. Adjust keepalive targets accordingly to avoid repeated redialing.
Enable NAT	Source says this allows LAN hosts to access the server through the tunnel; without it, access follows the external network in the described configuration. Actual routing requirements depend on topology.
Other parameters	Usually blank unless required by the server.
Specify local / peer IP	Requests specific PPP addresses if the server permits. The source sentence about server assignment and tunnel failure is ambiguous: NEEDS_VERIFICATION.
Check interval / timeout count	Send LCP checks at the selected interval; after the failure threshold, disconnect and request a new link.
Other negotiation options	For server-specific negotiation; example novj;novjcomp, separated by semicolons.

4.3.2 IPsec / L2TP

Source pp. 59-61



Original firmware reference, source p. 59. Field explanations are translated below; interface labels remain as supplied.

IPsec connection settings (Fig. 4-3-2)

Parameter	Source specification
Connection mode	Active: initiate locally. Passive: wait for the peer.
Server	Required IP or domain.
Transport mode	Transport for gateway-to-server use; Tunnel for gateway-to-gateway; Passthrough allows IPsec traffic through.
Local network type	Network-To-Network for devices behind both gateways; Road Warrior for a mobile client.
Subnets	Networks on both sides in Network-To-Network mode.
Next-hop IP	Upstream gateway IP when the device is behind another network.
IPsec port	Source uses this field for L2TP listening when L2TP is enabled; default L2TP port 1701.
Connection ID	Identifier supplied to the peer during negotiation.

IPsec negotiation settings

Parameter	Source specification
Phase 1	Main or Aggressive; PFS (Perfect Forward Secrecy); Debug; NAT traversal when behind source-address translation. The source explanation of phase-1/phase-2 SAs requires technical review.
Authentication	Pre-shared Key or X.509 certificates.
Encryption	DES, 3DES, AES, AES128 as listed.
Hash	SHA1 or MD5.
DH groups	Group1, Group2, Group5, Group14, Group15, Group16, Group17, Group18.
Lifetime	Negotiation validity period in seconds.
Key / Password	Shared secret for PSK; certificate key/password for X.509 mode as described.
Phase 2	Source describes exchange protected by phase-1 SA, negotiation of protocol/algorithms and key exchange. DH groups, encryption, hash and lifetime choices are repeated as above.
DPD interval / timeout	Source describes periodic LCP checks here; this protocol description is retained as a source inconsistency. On timeout, disconnect and reconnect.
IPComp	IP payload compression.

L2TP (Fig. 4-3-3)

Parameter	Source specification
Protocol	Layer Two Tunneling Protocol, a VPDN technology transporting layer-2 / PPP units inside IP or UDP across packet networks.
Server / remote network	Server IP/domain; remote subnet and mask.
Credentials	LAC username and password.
PPP authentication / MPPE	Same listed choices as PPTP: PAP, CHAP, MS-CHAP, MS-CHAPv2, Any; NoMppe, MPPE40/128, stateful MPPE.
Tunnel ID / password	LNS account and password as described.
Default route / NAT	Same source behavior described for PPTP; the L2TP text itself refers to a PPTP tunnel, a source copy/paste inconsistency.

Parameter	Source specification
Local / peer IP	Requested PPP addresses, subject to server permission; the source failure sentence is ambiguous.
LCP interval / timeout	Periodic link checks; disconnect/reconnect after failure threshold.
Other negotiation	Usually blank; server-specific options separated by semicolons, for example novj;novjcomp.

4.3.3 OpenVPN and 4.3.4 N2N

Source pp. 62-64

The source describes OpenVPN as an application-layer VPN based on OpenSSL. Set the server address, TCP or UDP protocol and tun or tap device to match the server. Obtain ca.crt, client.crt and client.key from the server administrator and upload each to the client router. After the successful-upload prompt, enter the client configuration. Start the server, then click Enable in OpenVPN to connect (Figs. 4-3-4 to 4-3-7).

N2N is described as a two-tier VPN providing peer-to-peer network connectivity over virtual IP addresses independently of the current physical network. Devices in the same N2N network can reach each other through their virtual addresses, including ping (Fig. 4-3-8).



Original firmware reference, source p. 62. Field explanations are translated below; interface labels remain as supplied.

Settings and explanations

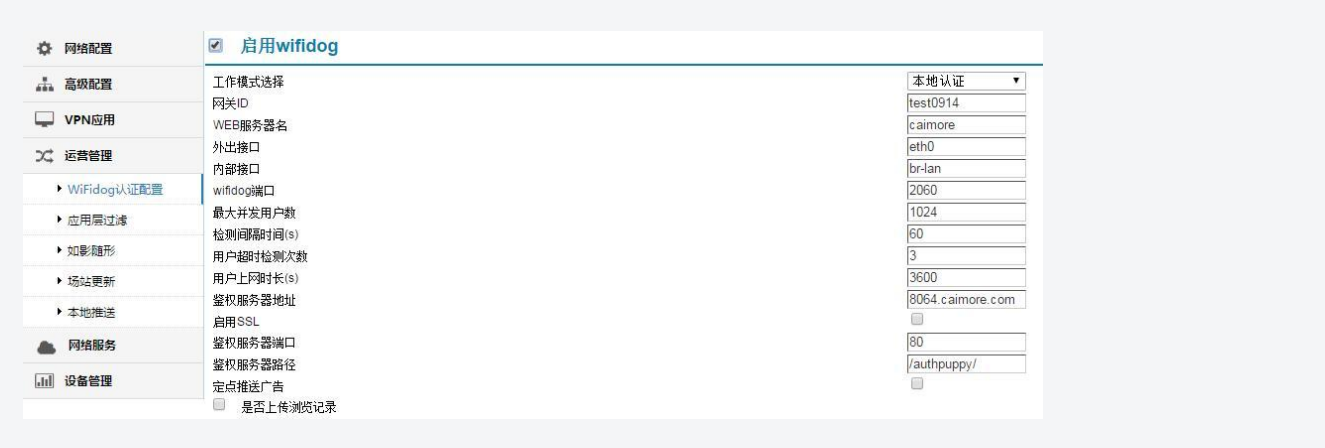
Parameter	Source specification
Interface name	Custom virtual interface name.
Local IP / mask	Tunnel-interface IP and subnet mask.
Community / password	N2N group name and shared group password.

Parameter	Source specification
Server IP / port	Server endpoint.
Physical address	MAC address associated with the interface.
MTU	Maximum transmission unit.

4.4.1 WiFidog authentication

Source p. 65

A hotspot user is directed to the configured authentication server page when requesting data; normal Internet access is allowed after successful authentication. Figure 4-4-1 shows the settings.



Original firmware reference, source p. 65. Field explanations are translated below; interface labels remain as supplied.

Settings and explanations

Parameter	Source specification
Mode	Ordinary authentication, WeChat authentication, industrial routing or local authentication.
Gateway ID	Identifier included in messages sent to the server.
Web server name	User-defined name.
External / internal interface	Total upstream-data interface / user-data interface.
WiFidog port	Port used by WiFidog.
Maximum concurrent users	Maximum simultaneous user requests.

Parameter	Source specification
Check interval (s)	Interval for checking user traffic and device status.
User timeout count	Number of checks determining that a user has timed out.
Internet session duration (s)	Authentication-free access duration after successful login.
Authentication server	Server address and port.
Enable SSL	Whether SSL is used for the server connection; the source calls this SSL decryption. Exact implementation NEEDS_VERIFICATION.
Authentication path	Server-side authentication path; include a slash at both ends.
Fixed-location advertisements	Enable or disable source-described targeted/location-based advertising.
Upload browsing records	Whether to upload user URL records.
Domain whitelist	Domains exempt from WiFidog blocking; source rule format: FirewallRule allow tcp to XXX.

4.4.2 Application filtering and 4.4.3 Inline advertisements

Source pp. 66-67

Application filtering can target video, music, downloads and URLs. Inline advertising inserts/replaces page content so that the advertisement appears at the top of a page while a connected user browses, as described in the source.



Original firmware reference, source p. 66. Field explanations are translated below; interface labels remain as supplied.

Application-filter fields (Fig. 4-4-2)

Parameter	Source specification
Rule name	Identifier for the restriction rule.
IP range	Address range subject to the rule.
Protocol type	Application class to filter, such as video/music/downloads.
Packet direction	IN, OUT or IN/OUT.
Policy	Accept or block matching data.

Inline advertising (Fig. 4-4-3)

Parameter	Source specification
Enable	Enable the source feature named Ruying Suixing (inline advertising).
Rule configuration	First line: FILTER: block-weeds. Second line: regular-expression substitution; source example translated with placeholders: s|page-content|replacement-content$0|g.
Scope	Feature behavior is translated from legacy firmware, not independently tested on encrypted modern web traffic.

4.4.4 Depot updates and 4.4.5 Local push

Source pp. 68-69



Original firmware reference, source p. 68. Field explanations are translated below; interface labels remain as supplied.

Depot-update fields (Fig. 4-4-4)

Parameter	Source specification
Depot ESSID / password	SSID and password for the depot Wi-Fi network.
Multimedia server IP	Server reachable on the same LAN as the depot Wi-Fi.
Update section	Section name configured on the server.
Local update directory	Destination path on the router.
Update username / password	Credentials allocated by the server.
Scan interval (s)	Wi-Fi scanning interval.

Local-push fields (Fig. 4-4-5)

Parameter	Source specification
Enable	Enable local push.
Advertisement name	Custom name.
Advertisement URL	URL to push.
Push interval	Interval between advertisements.

4.5.1 Dynamic DNS

Source p. 70

DDNS binds a changing dial-up IP address to a fixed domain. After each successful dial-up, the router sends its new address to the configured DDNS server. Clients such as DTUs use the domain to resolve the router address before connecting. Reachability still depends on the underlying network; the next section distinguishes public-IP access from intranet tunneling.



Original firmware reference, source p. 70. Field explanations are translated below; interface labels remain as supplied.

Settings and explanations

Parameter	Source specification
Interface	wan, lan, 4g or vpn.
Service	Register a user and domain with the selected provider, then enter assigned details and Submit. Source example selects dyndns.org and refers to www.dyndns.com.
Hostname	DDNS domain.
Username / password	Provider account credentials.
IP source	Network, interface or URL.
URL	Server address used for the selected source.
IP-change check interval	Interval value, with minutes or hours.
Forced update interval	Force-refresh interval value, with minutes or hours.

4.5.2 PeanutHull intranet service

Source pp. 71-73

The source distinguishes public and intranet versions. Public DDNS binds a domain to an available public IP. Intranet access requires a PeanutHull account enabled for NAT traversal/tunneling and associates it with the device to reach the router or downstream terminals without a public IP.

Select Enable and Submit; refresh. The source expects status online and an automatically generated SN derived from the device MAC. A unique MAC is required for a unique SN. Click Login Management to open the SN login page.

The SN is obtained automatically. The source initial password is admin. Log in, set the subsequent login password and submit; the source shows an activation-success prompt. The account then displays a dynamic domain.

If the router has a public IP, the domain addresses that router. If it is behind a LAN (the source notes that many SIM connections are), associate an account with intranet-traversal service enabled to reach the router or its LAN devices. Figures 4-5-2 to 4-5-7 illustrate registration, login, activation and account association. External service availability and UI have not been revalidated.



Original firmware reference, source p. 71. Field explanations are translated below; interface labels remain as supplied.

4.5.3 Traffic monitoring

Source p. 74

Before enabling traffic monitoring, synchronize the device time through the Wi-Fi probe/time function, as instructed in the source. Figure 4-5-8 shows the settings.



Original firmware reference, source p. 74. Field explanations are translated below; interface labels remain as supplied.

Settings and explanations

Parameter	Source specification
Clear statistics	Reset all recorded device traffic.
Traffic threshold (MB)	Maximum usage in the configured period.
Statistics period	Daily or monthly.
Action on limit	Disable Wi-Fi, wired network, both Wi-Fi and wired network, or 3G/4G.
Report traffic	Upload usage statistics to the server.
Whitelist	Source says this applies only when disabling 3G/4G: listed websites remain accessible after the limit. The mechanism needs verification. Submitting resets the traffic statistics as stated.

4.6 Device management

Source pp. 75-81



Original firmware reference, source p. 78. Field explanations are translated below; interface labels remain as supplied.

Management functions (Figs. 4-6-1 to 4-6-6)

Parameter	Source specification
4.6.1 Status	Displays system, WAN, LAN, Wi-Fi and VPN status.
4.6.2 Logs	Refresh retrieves device debugging information; Clear empties the displayed diagnostic information.

Parameter	Source specification
4.6.3 Firmware upgrade	Choose whether to retain configuration. Select the manufacturer-supplied firmware file and Submit. The device restarts automatically during upgrade. Do not disconnect power. Restore resets to factory configuration and restarts the router.
4.6.4 Wi-Fi probe frames	Displays captured frame data and signal strength.
4.6.5 Power management	Current Time displays device time; Calibration Mode can be network or manual; Manual Setting enters time directly. Mode defaults to Daily. Power-on Time begins normal operation; Power-off Time enters low-power mode.
4.6.6 GPS information	On GPS-equipped devices, displays current longitude and latitude.

5. Troubleshooting

Source p. 82

Settings and explanations

Parameter	Source specification
Frequent disconnects	Check signal strength in System Status. Check keepalive rules/parameters. If a domain is used as the target, log in to the command terminal (Appendix 1) and verify name resolution and target reachability.
Forgotten password	Restore factory settings. The source points to Appendix 4, but the actual reset procedure is Appendix 3.
LAN LED off	Check cable seating. The source suggests trying a crossover cable for direct PC connection, and connecting through a switch to check the cable/network.
Cannot dial	Verify WAN settings against operator details. Check signal and antenna connection, local network coverage and SIM status. If card status is invalid, power off before reseating/replacing the SIM.
Dialed but no web access	Check that the client default gateway points to the router. Check DNS against router status; correct wrong values. If configured DNS appears correct but fails, clear it/use automatic DNS, dial successfully, then enter the DNS shown in System Status (Appendix 5).

Appendix 1 - SSH command-line access

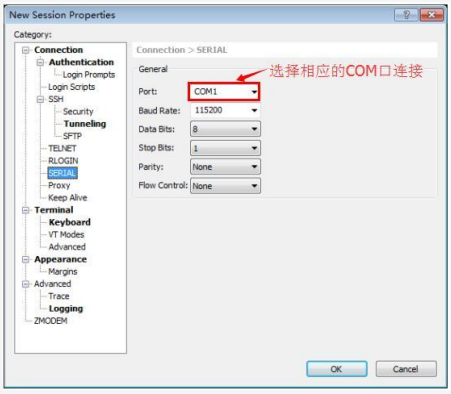
Source pp. 83-85

- 1. Open Xshell.
- 2. Enter ssh 192.168.9.1 (replace with the actual gateway address) and press Enter.
- 3. Enter the username and password in the prompted windows.
- 4. The shell prompt shown in the source indicates successful login. Do not assume that web and shell credentials are identical unless confirmed for the delivered firmware.

Appendix 2 - Serial console access

Source pp. 86-88

- 1. Open Xshell and create a new session.
- 2. Select SERIAL and the connected COM port. The original Fig. a2-3 shows COM1 (example only), 115200 baud, 8 data bits, 1 stop bit, parity None and flow control None. Confirm these console settings for the supplied firmware; they are distinct from the data-port settings.
- 3. Confirm the session to open the terminal.
- 4. Press Enter to obtain the login prompt, then enter username and password.
- 5. The resulting shell prompt indicates successful login.



Original serial-session settings screenshot; confirm COM port and console configuration

Appendix 3 - Factory reset

Source p. 89

- 1. Power on the device.
- 2. Press and hold RESET for approximately 3 seconds.
- 3. Release when all indicator LEDs illuminate.
- 4. The device resets and restarts automatically. Factory reset restores factory configuration.

Appendix 4 - Wireless network reference

Source pp. 89-90

Operator-provided information takes precedence over these source-era examples. The source normally uses factory defaults and requires changes for APN/VPDN private networks; it says 4G fields are blank by default.

Dialing reference

Network	Dial number	APN	Username	Password
GPRS	*99***1#	cmnet (Mobile) / uninet (Unicom)	Blank	Blank
EDGE	*99***1#	cmnet	Blank	Blank
TD-SCDMA	*98*1#	cmnet	Blank	Blank
CDMA	#777	Blank	card	card
EV-DO	#777	Blank	card	card
WCDMA	*99#	3gnet	Blank	Blank

Appendix 5 - Configure DNS from router status

Source pp. 90-91

- 1. Open System Status on the gateway and record the acquired DNS server addresses (Fig. a5-1).
- 2. On the source Windows example, open Start > Control Panel > Network Connections (Fig. a5-2).
- 3. Right-click Local Area Connection > Properties > Internet Protocol (TCP/IP) > Properties.
- 4. Enter the DNS addresses shown by the gateway; click OK (Fig. a5-3). Use the actual current status values rather than copying a screenshot example.

Translation and source review notes

Editorial notes, not additional manufacturer specifications

Translated from the supplied Chinese source. Repeated page headers are consolidated. Source-era claims and conflicting values are retained; NEEDS_VERIFICATION identifies unresolved technical issues. Original hardware photographs are retained. Legacy Chinese firmware screenshots are reference images, not a representation of English firmware.

Review checklist

Source / topic	Review note
Source p. 3	V1.2 is dated 2020-01-22, earlier than V1.1 dated 2020-07-10. Dates are preserved as printed.
Source pp. 6, 9, 14	Processor is MIPS in the overview and ARM later. Main/secondary dual-core frequencies require clarification.
Source pp. 8, 13, 16	TF is listed in procurement and interface tables, but the software section says reserved/temporarily unsupported. Confirm actual firmware support.
Source pp. 17-18	9 V / 1.5 A supply versus 12 V +/-10% adapter; current and power-consumption figures differ. IP30 and IP31 both occur. Verify approved specification by hardware revision.
Source pp. 19-22	HSUPA downlink, duplicate uplink labels, CPE accuracy, NMEA-1083/SiRD and other questionable radio/GPS terms retained without invented corrections.
Source p. 23	SIM2 signal indicator combinations are all off in all three signal ranges. Intended states require confirmation.
Source pp. 41-48	5 GHz section repeats 1/6/11 channel advice; WEP lengths and VLAN associated/unassociated terms require firmware review. DHCP acronym expansion is incorrect in the source.
Source pp. 50-51	Static-route example uses /16 then /24 and inconsistent interface/subnet descriptions. Do not deploy the example without topology review.
Source pp. 57-61	PPP fixed-address sentence, L2TP references to PPTP, IPsec phase descriptions and DPD/LCP explanation contain ambiguities. Confirm intended behavior.
Source pp. 65-74	Legacy portal/advertising, SSL, external PeanutHull service and whitelist behavior require current firmware validation. No live account or service was accessed.
Source pp. 82, 86-89	Troubleshooting reset cross-reference corrected to Appendix 3. Console settings visible only in the original screenshot must be confirmed for the supplied firmware.

Source / topic	Review note
Source vs 6XX datasheet	6X manual: 256 Mbit Flash, 32-256G TF with unsupported caveat, 9 V / 1.5 A power, -25 to +70 °C, MTBF >=100000 h, 253 dual-band users. 6XX datasheet differs; neither source overrides the other without revision confirmation.
Publication status	English review only. No device tests, firmware verification, upload or deployment performed. Original firmware images remain Chinese references.