INDUSTRIAL CONNECTIVITY / USER MANUAL

CM520-57

Wireless router user manual



Original manufacturer photograph



Original manufacturer photograph

Source revision V1.3 | 18 July 2022 | English review edition | 18 October 2026

REVIEW EDITION - translated from the supplied Chinese document. Optional functions and source discrepancies are retained. See the final review checklist.

Inside this document

Safety and hardware / Quick start / WAN, LAN and Wi-Fi / VPN and routing / DTU and SNMP / System management / Troubleshooting / Appendices

Document notices and revision history

Source pp. 1-2

CM520-57 Wireless Router User Manual. Xiamen CAIMORE Communication Technology Co., Ltd. Source copyright 2021, all rights reserved. Postal code: 361021. The source slogan is translated as: CAIMORE Communications - connecting the world.

All contents of this manual are protected by copyright. Without written authorization from Xiamen CAIMORE Communication Technology Co., Ltd., no organization or individual may copy or reproduce the whole manual or any part of it, or distribute it in any form.

CAIMORE, its logo and other CAIMORE marks belong to Xiamen CAIMORE Communication Technology Co., Ltd. Other trademarks and registered trademarks mentioned belong to their respective owners.

This document may be updated because of product upgrades or other reasons. Unless otherwise agreed, it is supplied as an operating guide. Its descriptions, information and recommendations do not constitute any express or implied warranty.

English editorial treatment: procedures and parameter descriptions have been typeset as English text and tables. Legacy Chinese firmware screenshots have not been presented as a new English firmware interface. Screenshot-only values are not promoted to universal defaults. The original Chinese manual remains the visual UI reference.

Source revision history

Revision	Change	Release date	Author	Approved by
V1.0	Initial official release	2022-01-13	LHP	LGB
V1.1	Individual parameter corrections	2022-01-18	LHP	LGB
V1.2	Individual parameter corrections	2022-05-18	GYP	LGB
V1.3	Added dual-SIM instructions	2022-07-18	LHP	LGB

Manufacturer contact information

Parameter	Source specification
Company	Xiamen CAIMORE Communication Technology Co., Ltd.
Address as printed in source	Units 901 and 904, No. 63 Chengyi North Street, Software Park Phase III, Xiamen, China
Telephone / fax	+86-592-5902655 / +86-592-5975885

Parameter	Source specification
Website / email	https://www.caimore.com / caimore@caimore.com

1. Introduction and precautions

Source p. 5

This manual explains installation, configuration and operation. It is intended for technical-support personnel, installers, device users and router developers. Configure the product for its operating environment and application requirements.

- Do not disassemble the device without authorization. Servicing must be performed by qualified personnel.
- Keep the device away from heat sources and direct sunlight.
- Protect against water. Disconnect power immediately if water reaches the equipment.
- Avoid excessively humid environments; the manual specifies operation below 85% RH.
- Avoid excessively hot or cold environments. This manual gives an operating range of -30 to +70 °C.
- Check that the 3G/4G/5G antennas are connected before powering on.
- Use the original packing materials and carton for transport. The packaging is designed and tested for shock resistance.
- Avoid moving the equipment rapidly between cold and hot environments, which may cause condensation and shorten service life.
- Never insert or remove a SIM card while the device is powered on; the SIM may be damaged.

2.1 Product overview

Source pp. 5-6

The CM520-57 industrial router family uses an open software architecture, a metal enclosure, five RJ45 Ethernet ports and 2.4 GHz Wi-Fi. It supports single-modem dual-SIM configurations and 3G/4G/5G WAN access, depending on model.

The source describes proprietary online-maintenance technology, industrial hardware, protection against dust, water, temperature extremes, radiation and electromagnetic interference. The hardware table specifies IP30; the general water-protection wording is not a waterproof rating.

Functions include VPN networking, IPTABLE firewall control, routing tables, DHCP server/client, SNAT/DNAT, DMZ, network diagnostics, transparent DTU communication, user management, APN/VPDN, power-on dialing and automatic link maintenance.

Model selection

Model	Cellular	SIM slots	RS232	RS485
CM520-57F	4G	1	Yes	Optional
CM520-57FS	5G	1	Yes	Optional
CM520-57FB	4G	2	Yes	Optional
CM520-57FBS	5G	2	Yes	Optional

Shared model features

Parameter	Source specification
Interfaces	Ethernet and terminals; RS232; optional RS485.
Memory	16 MB Flash / 128 MB SDRAM.
Wi-Fi	Supported by all four models in the selection table.
SIM architecture	57F/57FS: one slot; 57FB/57FBS: two slots with one cellular modem.

2.3 Software functions

Source p. 6

- 3G/4G/5G cellular dialing for mobile-network services.
- VPN: PPTP, L2TP and IPsec; protocols include TCP/IP, UDP and ICMP.
- Online monitoring and maintenance, automatic redial, IPTABLES firewall and packet filtering.
- DHCP/DHCPD; NAT including SNAT/DNAT; DMZ host; APN/VPDN; SSH.
- One RS232 channel and one optional RS485 channel for transparent TCP/UDP DTU communication.
- Factory reset, local configuration and local upgrades; single-modem dual-SIM support.

2.4 Hardware parameters

Source pp. 6-7

Settings and explanations

Parameter	Source specification
CPU	Industrial ARM embedded processor, 650 MHz; 32 KB D-cache / 64 KB I-cache, as stated in this manual. The separate datasheet says MIPS: NEEDS_VERIFICATION.
Operating system / language	Embedded Linux; Chinese user interface.
Configuration / login	Web configuration; username and password required.
Ethernet	1 WAN, switchable to LAN; 4 default LAN ports; five adaptive 100 Mbps interfaces. Ethernet IEEE 802-3 / 802-2 as printed; 1.5 kV isolation.
Antenna connectors	3G/4G/5G and Wi-Fi antenna interfaces.
Serial	1 RS232 and 1 optional RS485; data bits 7/8; stop bits 1/2; parity none/odd/even; 300-4000000 bit/s; no/hardware/software flow control.
Indicators	POWER, WIFI and Online.
UIM	Single-modem dual-SIM models available; 1.8/3/5 V push-type interface; 15 kV ESD protection.
Power connector	3-pin terminal; optional DC socket.
RESET	Reset button restores factory settings.
Power input	6-32 V DC, typical 9 V.
Source row titled power output	+9 V, 1.5 A, as printed. Whether this denotes the adapter output NEEDS_VERIFICATION.
Operating environment	-30 to +70 °C.
Enclosure	Metal, electromagnetic shielding, isolated enclosure/system, lightning-protection design, power-safety requirements, IP30.
PCB / components	PCB follows stated 3H and 3W principles; high-quality board materials and industrial components.

2.5 Wireless-module frequency parameters

Source p. 8

The source provides 5G bands but no 5G NR data-rate row in this manual. Listed radio values describe source modem options and do not guarantee availability in every regional configuration.

Radio parameters

Parameter	Source specification
Wireless module	Industrial-grade module.
5G SA/NSA bands	n1 / n2 / n3 / n5 / n7 / n8 / n20 / n28 / n41 / n66 / n71 / n77 / n78 / n79
TDD frequency group	LTE TDD: 2600/2300 MHz; UMTS: 2100/900 MHz; GSM: 850/900/1800/1900 MHz; UMTS Rx diversity: 2100/900 MHz.
FDD frequency group	LTE FDD: 2600/2100/1800/DD800 MHz (DD800 reproduced as printed); UMTS and UMTS Rx diversity: 2100/900 MHz.
TDD rates	LTE TDD: DL 68 Mbps / UL 17 Mbps; DC-HSPA+: DL 42 Mb/s (Category 24); HSPA+: DL 28 Mb/s (Category 18); HSDPA: DL 14.4 Mb/s (Category 8); HSUPA+: DL 5.76 Mb/s (Category 6), as printed; WCDMA CS: UL/DL 64 kbps; WCDMA PS: UL/DL 384 kbps.
FDD rates	LTE FDD: DL 100 Mbps / UL 50 Mbps; other DC-HSPA+, HSPA+, HSDPA, HSUPA+ and WCDMA values are the same as the TDD table.
Transmit power	LTE: 23 dBm; WCDMA/HSDPA: 24 dBm.
Receiver sensitivity	<-109 dBm
Radio schemes	LTE/UMTS/HSPA+/HSDPA/HSUPA/WCDMA/EDGE/GSM
Module functions	Data and SMS.

2.6 Package, enclosure and indicators

Source pp. 9-10

The family uses a fully enclosed industrial aluminum structure with heat dissipation, dust protection and resistance to electromagnetic interference. Check package contents against the packing list after opening.

Standard package as listed

Parameter	Source specification
Gateway	1
9 V DC adapter	1
Cellular antennas	Six for the 5G configuration; one for other configurations, as stated. Actual shipment requires confirmation.
Wi-Fi antenna	1
Ethernet cable	1

Product views

Parameter	Source specification
Single-SIM configuration	Overall, front and rear views shown in the source.
Dual-SIM configuration	Overall, front and rear views shown in the source; SIM1 and SIM2 are visible.

LED definitions

LED	State	Meaning
POWER	On	Power normal
POWER	Off	Abnormal power supply
WIFI	On	Wi-Fi enabled
WIFI	Off	Wi-Fi disabled
Online	On	Network normal
Online	Off	Network abnormal
Online	Flashing	SIM not recognized

3. Quick start and local PC connection

Source pp. 10-11

Factory network access is set to 3G/4G/5G. With power off, insert the SIM and connect the antennas. Apply power and wait for the Online LED to illuminate. Open the router LAN address 192.168.9.1 to view configuration. Power must be off before inserting or removing the SIM.

Connect the PC to a router LAN port using an Ethernet cable. In the source Windows interface, open Control Panel > Network and Sharing Center > Local Area Connection > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties.

Method 1: select Obtain an IP address automatically and Obtain DNS server address automatically, then click OK.

Method 2: use a static IP and fixed DNS. Keep the PC in the router subnet and use a unique address. The source screenshot uses 192.168.9.2; the following source text says 192.168.9.X, X = 3-254, with X = 3 as its example. This inconsistency is retained as a review issue.

Open http://192.168.9.1 in a browser (the source names Internet Explorer). The manual gives username admin and password admin. These are historical source defaults, not a claim about every firmware release. Select WAN Configuration, enter the carrier-supplied settings and submit.

Static PC example

Parameter	Source specification
Router LAN IP	192.168.9.1
PC subnet mask	255.255.255.0; adjust to the selected subnet if changed.
Default gateway	192.168.9.1
Source DNS example	Preferred 114.114.114.114; alternate 8.8.8.8. These are source examples, not universal carrier settings.

3.3 Cellular dialing, LAN and connectivity test

Source pp. 12-13

For dual-SIM routers, enable Dual SIM Single Standby to use the dual-SIM function. This is a single-modem arrangement; it is not dual-active cellular access.

The source says normal connections can generally use factory defaults, with changes needed for APN/VPDN private networks. It gives the following legacy 3G examples and says 4G fields may remain blank by default. Use actual operator requirements when they differ.

Open LAN Configuration to set the LAN and DHCP parameters as required. Restart the device, wait for the Online LED and open a website. Successful page access indicates Internet connectivity.

For technical support, the source gives https://www.caimore.com and telephone pairs +86-592-5908952 / +86-15750764798 and +86-592-5901215 / +86-18206079361. These are historical document contacts; current support routing NEEDS_VERIFICATION.

Legacy carrier examples retained from source

Network	Dial number	APN	Username	Password
GPRS	*99***1#	cmnet (China Mobile); uninet (China 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

4.1.1 WAN configuration

Source pp. 14-15

Settings and explanations

Parameter	Source specification
Wired access	Choose DHCP, Static IP or PPPoE. MAC address is the WAN interface MAC.
4G/5G access	Set APN, username and password according to the carrier. Factory parameters are described as generally sufficient; for VPDN use operator credentials. The source says 4G fields may be blank.
Dual SIM	Enable Dual SIM Single Standby on dual-SIM routers.
Wi-Fi repeater	Click Refresh to search nearby Wi-Fi networks. Select the target SSID and enter its password. Choose DHCP or Static IP.
Primary / backup mode	Configure wired and SIM Dial settings. When wired access fails, switch to SIM access; when wired access recovers, switch back.

4.1.2 LAN configuration

Source pp. 15-16

LAN configuration sets the local IP address and DHCP service. The source factory LAN IP is 192.168.9.1. Configure the matching subnet mask and LAN MAC address.

DHCP automatically assigns LAN IP addresses using a pool and lease time. Keep the starting and ending addresses contiguous, within the router subnet and excluding the router IP. Use only one DHCP server on a LAN; competing servers can cause incorrect address assignment.

A stable DNS server address may be entered if available. Keep connected devices in the gateway subnet. The source warns that factory resets on multiple routers may restore MAC addresses that conflict; check and change MAC addresses if necessary. After dialing, verify that the configured DNS can resolve domain names.

Settings and explanations

Parameter	Source specification
LAN interface	IP address, subnet mask and MAC address.
DHCP fields	Enable address pool; starting address, client count / pool extent and lease time. The explanatory prose also refers to an ending address.
DNS	Use a reachable resolver suitable for the connected network.

4.1.3 Wi-Fi configuration

Source p. 17

Settings and explanations

Parameter	Source specification
ESSID	Wi-Fi network name.
None	Open network with no data encryption; no password is required to connect to the AP.
WEP	WEP encryption using open-system or shared-key authentication.
WPA-PSK	WPA with a pre-shared key.
WPA2-PSK	WPA2 with a pre-shared key.
Mixed WPA-PSK/WPA2-PSK	Mixed WPA/WPA2 pre-shared-key mode.

4.1.4 Online maintenance

Source pp. 17-18

Online maintenance periodically checks the data path between the router and wireless network. When an abnormal link or disconnection is detected, the software redials automatically for unattended recovery.

Enter stable test addresses appropriate to the installation. The router uses these servers as its connectivity reference. An unstable or unreachable server can cause repeated disconnections and redialing.

The Ping method sends ICMP packets to the configured test addresses. If all configured targets fail to respond, the router treats the link as interrupted, releases the connection and redials until communication is restored. Targets must remain available and permit Ping; otherwise a working connection may be misclassified as failed.

The source instructs enabling online maintenance for recovery and notes that the default configuration is intended for a public network. Reconfigure targets for private networks to avoid repeated reconnection.

Settings and explanations

Parameter	Source specification
Fields shown	Enable status; test addresses 1-3; detection interval; timeout count; retry count. Screenshot example values are not universal defaults.

4.2 Network access management

Source pp. 18-19

Network filtering controls data received or sent by the wireless router to prevent invalid or unwanted traffic. Rules can allow or deny LAN devices accessing the WAN and WAN traffic reaching the LAN.

Choose IP filtering or MAC filtering. IP rules filter by address and can also filter domain names as described. MAC rules act on the specified hardware address.

Policy 1: discard packets matching the listed rules; other packets pass. Policy 2: accept only packets matching the listed rules; all other packets are discarded.

Settings and explanations

Parameter	Source specification
Rule fields shown	Rule name, external/internal address, internal MAC, protocol and port.

4.3.1 PPTP tunnel

Source pp. 19-20

PPTP is described as a layer-2 tunneling protocol that carries PPP frames across IP networks, including the Internet and connections between private networks. It uses TCP for tunnel maintenance and GRE for encapsulated PPP transport. The source describes encryption or compression of the carried PPP payload.

If Add Default Route is enabled, traffic from attached hosts is sent through the PPTP tunnel. Such hosts can then access only the VPN path as configured. Adjust online-maintenance targets for VPN reachability to avoid repeated reconnection.

Settings and explanations

Parameter	Source specification
Server	Server IP address or domain name.
Remote subnet / mask	Network information on the server side.
Username / password	Credentials for server access.
Authentication	PAP, CHAP, MS-CHAP, MS-CHAP-V2 or Any. PAP credentials are transmitted in clear text and are described as low security. Any permits any supported method and is recommended by the source when no special requirement exists.
MPPE	NoMppe: no MPPE; Mppe (40/128): MPPE40/MPPE128; Mppe-StateFul: stateful MPPE.
Local IP request	Request a specified local PPP address if the server permits. If the server does not allocate it, tunnel establishment fails.
Detection interval / timeout count	Send LCP packets at the chosen interval. After the specified consecutive failures, disconnect and re-establish the link.
Other negotiation parameters	Normally blank unless special server parameters are required. Source examples: novj; novjcomp. Separate multiple parameters with semicolons.
Add default route	Route traffic through the PPTP tunnel; verify implications for WAN and health-check access.

4.3.2 IPsec tunnel

Source pp. 21-22

Phase 1 establishes an IPsec SA for protected data exchange. Phase 2 negotiation is protected by the phase-1 SA; messages lacking the required protection are rejected. The second phase negotiates communication algorithms and exchanges keys.

The source includes legacy algorithms and modes. Their presence is translated as a source capability list, not a recommendation for a new security policy.

Settings and explanations

Parameter	Source specification
Connection mode	Active: the local device initiates. Passive: wait for the peer.
Server	Server IP or domain; required in active mode.
Transport mode	Transport: typically router-to-server; Tunnel: typically router-to-router; Passthrough: allow IPsec traffic through.
Local network type	Network-To-Network: devices behind the two peer subnets communicate; Road Warrior: mobile client connects to a server.
Subnets	Set both peer subnets in Network-To-Network mode.
IPsec port	When using L2TP at the same time, this is the L2TP listening port; default stated 1701.
Connection identity	Identity supplied to the peer during negotiation.
Phase 1 mode	Main or Aggressive.
PFS	Perfect forward secrecy, described as protecting communications from a compromised individual key.
Debug	Enable diagnostic output.
Authentication	Pre-shared key.
Encryption algorithms	DES, 3DES, AES and AES128, as listed.
Hash algorithms	SHA1 and MD5.
Phase 1 DH groups	Group1, Group2, Group5, Group14, Group15, Group16, Group17 and Group18.
Phase 1 lifetime	SA validity in hours.
Key	Shared secret for pre-shared-key mode.

Parameter	Source specification
Phase 2 DH / lifetime	Same listed DH groups; SA validity in hours.
Phase 2 encryption / hash	DES/3DES/AES/AES128; SHA1/MD5.
Dead-peer detection	Timeout in seconds; source default 120 s.
IPComp	IP payload compression.

4.3.3 L2TP

Source p. 22

Layer Two Tunneling Protocol carries layer-2 data, such as PPP frames, encapsulated in IP or UDP across a packet-switched network such as the Internet.

Settings and explanations

Parameter	Source specification
Server	Server IP address or domain.
Remote subnet / mask	Subnet behind the server.
Username / password	LAC account and password.
Tunnel ID / tunnel password	LNS account and password, as described in the source. Confirm intended identity terminology.

4.4.1 Static routing

Source p. 23

Configure static routes and view the system routing table. The default route sends traffic to the public network. Add a route manually when a particular network needs a specific path. If an added rule does not appear as an effective route, check whether its network settings meet the requirements.

Settings and explanations

Parameter	Source specification
Destination	Host IP or network address.

Parameter	Source specification
Subnet mask	Mask for the destination; use 255.255.255.255 for a host route.
Gateway	Next-hop IP; use 0.0.0.0 when no gateway is needed.
Metric	Route metric; default 0.
MTU	Maximum packet size; source default 1500 bytes.
Interface	System interface for the route.

4.4.2 NAT and DMZ

Source pp. 23-24

Port mapping forwards incoming traffic through a configured external port to a selected LAN host and service port. The source describes NAT as Network Address Translation, mapping internal private addresses to public-network access.

A DMZ host exposes one LAN computer to the Internet for two-way communication. The router forwards incoming traffic for its public address to that virtual server. Select Enable DMZ, enter the internal server IP and click Apply. This exposure is the behavior described in the source; review access controls before use.

Settings and explanations

Parameter	Source specification
Rule name	Unique identifier using 0-9, a-z and A-Z.
Protocol	TCP/UDP, TCP or UDP.
External interface	Interface receiving external traffic.
External port	Starting TCP/UDP port for incoming requests.
Internal IP	LAN host to which traffic is mapped.
Internal port	Starting service port on the destination host.

4.5.1 Remote management

Source p. 25

The platform can manage the device remotely. The source screen includes server address, port, device ID and log settings. No production server endpoint or enrollment procedure is specified in the prose; obtain the deployment parameters from the management-platform administrator.

4.5.2 DTU data transmission

Source pp. 25-26

DTU communication is available through one RS232 or one RS485 channel, as stated here. Configure the data-center server addresses and ports. Up to three server entries are shown; filling all three is not required. An address may be an IP address or domain name.

Match the serial settings to the connected terminal. A mismatch in rate, data bits, stop bits or parity prevents communication.

Settings and explanations

Parameter	Source specification
Transport protocol	TCP or UDP; TCP is the stated default.
Transmission mode	Default CAIMORE protocol, or Custom for user-defined registration and heartbeat packets.
Device ID	Identifier used by the data center to distinguish DTUs. CAIMORE mode requires exactly four bytes. Prefix hexadecimal data with 0x; source example 0x1a2b3c4d.
Mobile number	Needed only in CAIMORE mode.
Registration packet	Registration data sent when connecting; appears in Custom mode. Hex data starts with 0x, for example 0xfe01.
Heartbeat packet	Periodic data-center heartbeat; appears in Custom mode; hexadecimal example 0xfe01.
Heartbeat interval	Time between heartbeat packets.
Reconnect interval	Retry interval after connection failure.
Reconnect count	After the configured failure limit, the router restarts its DTU function.
Serial log	Outputs data sent/received by the serial port and data center.
Baud rate	300-4000000 bit/s.

Parameter	Source specification
Data bits	5-8 in this DTU section; the hardware section lists 7/8. NEEDS_VERIFICATION.
Stop bits	1 or 2.
Parity	NONE, ODD or EVEN.

4.5.3 SNMP

Source pp. 26-27

Enable Simple Network Management Protocol to connect the device to an SNMP server and manage/configure multiple devices through a client.

Settings and explanations

Parameter	Source specification
Management-server address	IP address of the network-management server.
Management-server port	Port used by the management system; source says the default is generally sufficient.
Listening port	SNMP listening port; source says the default is generally sufficient.
Heartbeat interval	Seconds between heartbeat packets sent to the management server.
Device ID	Device identifier.
Number	Device number; source says the default is generally sufficient.
Remarks	Additional descriptive information.
Read community	Source default public.
Read/write community	Source default private.
Trap community	Source default public.
Trap timeout	Timeout in seconds.
Scheduled online duration	Minutes; source says effective only when the traffic/data limit is exceeded. Behavior NEEDS_VERIFICATION.

4.5.4 Local service

Source pp. 27-28

A LAN TCP/UDP client can connect to the router LAN IP and send commands to obtain router information. The screen provides mode and port settings. The supplied source does not provide a complete command reference; no missing command syntax is invented.

4.6 System administration

Source pp. 28-31

Settings and explanations

Parameter	Source specification
System status	Shows system, WAN, LAN and VPN information.
User management	Manage the web-login password. Enter login username, old password, new password and confirmation; click Submit to save. If the password is forgotten, restore factory defaults as described in Appendix 1.
Firmware upgrade	Select a manufacturer-provided firmware image. Choose whether to retain the current configuration. If retained, the router restores the pre-upgrade settings after a successful upgrade. Ask the manufacturer whether a version change supports retention. Do not disconnect power during the upgrade.
Restore defaults	Restore initial settings for the current firmware version. This replaces the current configuration.
Ping	Check network connectivity.
TRACERT	Trace the route.
NSLOOKUP	Query DNS records and diagnose domain-name resolution.
NTP client	Router requests time as an NTP client.
NTP server	Router distributes time as a server.
Time zone	Select the zone for the installation region.
Historical log	Log information from before the most recent router restart; maximum 3000 lines. The source warns that non-initiated restarts such as power failure do not retain this history. Click Refresh to display the diagnostic information.
System log	Click Refresh to view application logs. Click Clear to remove displayed log information.

5. Troubleshooting

Source p. 32

Settings and explanations

Parameter	Source specification
Frequent disconnections	Check signal strength in System Status. Check online-maintenance parameters and rules. If targets are domain names, use Ping and NSLOOKUP to confirm name resolution and target reachability.
Forgotten password	Restore factory defaults using Appendix 1.
LAN LED off	Check cable connections. The source suggests a crossover cable for a direct PC connection. Try a switch connection to check the cable/path. This is legacy manual guidance, not a universal cabling requirement.
Cannot dial	Check WAN parameters against carrier information. Check signal and antenna connection, local coverage, SIM status and recognition. Power off before reseating or replacing the SIM.
Connected but cannot open websites	Check that the host gateway points to the router. Check DNS. Correct an invalid manually entered DNS. The source suggests clearing manual DNS to obtain it automatically, dialing again and then copying working DNS values from System Status if fixed settings are needed.

Appendix 1. Restore factory defaults

Source p. 33

- 1. Power on the device.
- 2. Press and hold RESET for approximately 3 seconds.
- 3. Release the button after all device indicators illuminate.
- 4. The device resets and restarts automatically. Factory reset replaces the current configuration.

Appendix 2. Legacy wireless-network examples

Source p. 33

The following numbers and APNs are reference information from the historical source. If they conflict with operator instructions, use the operator-provided information. The source says normal operation generally uses factory defaults; APN/VPDN private-network use requires changes.

Legacy carrier examples retained from source

Network	Dial number	APN	Username	Password
GPRS	*99***1#	cmnet (China Mobile); uninet (China 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 3. Set PC DNS from router status

Source pp. 33-34

Open System Status and read the WAN DNS values. The source screenshot illustrates 120.196.165.7 and 221.179.38.7. These are examples from that connection, not universal DNS recommendations.

In the source Windows workflow, open Start > Control Panel > Network Connections. Right-click Local Area Connection and select Properties. Select Internet Protocol (TCP/IP), click Properties and enter the DNS values shown by the gateway. Click OK when finished.

The source PC screenshot also shows IP 192.168.9.135, mask 255.255.255.0 and gateway 192.168.9.1 as an example. Use a unique local IP suitable for the actual LAN.

Translation and source review notes

Editorial notes; not additional manufacturer specifications

English review edition translated from the supplied Chinese document. Source-era claims, optional functions and conflicting values are retained. NEEDS_VERIFICATION marks unresolved issues. Technical review is required before website upload.

Review checklist

Source / topic	Review note
Hardware revision	Manual states ARM at 650 MHz, -30 to +70 °C and +9 V / 1.5 A. Separate datasheet states MIPS, -35 to +75 °C and 9 V / 1.33 A. Confirm hardware revision before publication.
Humidity / protection	Manual precautions state below 85% RH; the datasheet states 95% non-condensing. IP30 does not substantiate the overview's general water-protection wording.
Serial scope	Manual describes RS232 plus optional RS485 in hardware, but DTU section says RS232 or RS485. Hardware data bits 7/8 vs DTU 5-8. NEEDS_VERIFICATION.
Legacy settings	Source defaults, carrier dial strings, passwords, public/private community strings and screenshots belong to the historical firmware. Verify against the intended firmware and carrier. Do not represent screenshots as a current English firmware UI.
Source inconsistencies	PC screenshot uses .2 while prose example uses .3. L2TP identity terminology and SNMP scheduled-online behavior require confirmation. Keep technical meaning rather than inventing command syntax.
Screenshot handling	All substantive procedural text and parameter explanations have been translated and re-typeset. Chinese firmware screenshots are omitted from this English text edition; they are not silently relabeled as English screens. A current English firmware screenshot set remains a publication improvement.
Operational validation	No physical router, firmware upgrade, VPN session or carrier connection has been tested. Translation checks are document checks only.