

EL-641M-4

USER MANUAL

Version 1.1 – Nov 2024



641M-2 & 641M-4 Industrial Cellular 4G-LTE Router



REVISION HISTORY

Revision	Date	Firmware version	Revision Details
1	Jan 2021	V1.1.7 (22a7514)	Initial release.
1.1	Dec 2024	V1.1.7 (22a7514)	New Format

Trademarks and copyright

ELPRO Technologies and the following logos, are the trademarks or registered trademarks in Australia.

**Disclaimers**

Information in this document is subject to change without notice and does not represent a commitment on the part of Elpro Technologies.

Elpro Technologies provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Elpro Technologies may make improvements and/or changes in this manual, or in the product(s) and/or the program(s) described in this manual at any time.

Information provided in this manual is intended to be accurate and reliable. However, Elpro Technologies assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

Technical Support

E-mail: support@elprotech.com

Sale: sales@elprotech.com

Web: <https://www.elprotech.com>

Interference Issues

Avoid possible radio frequency (RF) interference by following these guidelines:

The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both.

Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized.

Do not operate in locations where medical equipment that the device could interfere with may be in use.

Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.

Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.

Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected.

Follow recommendations for installation from equipment manufacturers.

Declaration of Conformity

EL-641M-4 are in conformity with the essential requirements and other relevant provisions of the CE and RoHS.



Notes

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The distance between user and products should be no less than 20cm.

Warning: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contents

1	Product Overview	5
1.0.	Overview	5
1.1.	Features and Benefits.....	5
1.1.1	Industrial internet access.....	5
1.1.1	Designed for industrial usage	5
1.1.2	Secure and reliable remote connection	5
1.1.3	Easy to use and easy maintenance	5
1.2.	General Specifications.....	6
1.3.	Mechanical Specifications	8
1.4.	Package Checklist	9
1.5.	Order Information	10
2	Installation.....	11
2.1.	Product Overview.....	11
2.1.1	Front Panel.....	11
2.1.2	Left Side Panel	11
2.2.	LED Indicators.....	12
2.3.	Ethernet Port Indicator.....	13
2.4.	PIN Definition of Terminal block.....	13
2.4.3	Serial Port & DIDO	13
2.4.4	Power Input	14
2.5.	Reset Button.....	14
2.6.	Insert SIM card	14
2.7.	Install Antenna	15
2.8.	DIN-rail Mounting.....	16
2.9.	Protective Grounding Installation	16
2.10.	Power Supply Installation.....	17
2.11.	Power On The Router	17
3	Access to Web page.....	18
3.1.	PC Configuration.....	18
3.2.	Factory Default Settings	19
3.3.	Login to Web Page.....	20
4	Web Configuration	21
4.1.	Web Interface.....	21
4.2.	Overview	22
4.2.1	Status	22
4.2.2	Syslog.....	24
4.3.	Link Management.....	25
4.3.1	Connection Manager	25
4.3.2	Cellular.....	27
4.3.3	Ethernet.....	29
4.3.4	Wi-Fi.....	36
4.4.	Industrial Interface	41
4.4.1	Serial	41

4.4.2	Digital IO	45
4.5.	Network.....	47
4.5.1	Firewall	47
4.5.2	Route	50
4.5.3	VRRP	51
4.5.4	IP Passthrough	52
4.6.	Applications.....	53
4.6.1	DDNS.....	53
4.6.2	SMS.....	55
4.6.3	Email Notifications.....	58
4.6.4	Modbus Slave	60
4.6.5	Modbus Master	62
4.6.6	Modbus Transport	67
4.6.7	Schedule Reboot.....	73
4.6.8	GPS.....	73
4.6.9	Call	75
4.7.	VPN.....	76
4.7.1	OpenVPN	76
4.7.2	IPSec	82
4.7.3	GRE	85
4.8.	Maintenance	86
4.8.1	Upgrade	86
4.8.2	Software.....	86
4.8.3	System.....	87
4.8.4	Configuration	91
4.8.5	Debug Tools	91
5	Appendix A -Glossary	93
6	Appendix B -Q&A.....	94
7	Appendix C -Digital IO Scenario.....	96
8	Appendix D - CLI	97

1 Product Overview

1.0. Overview

EL-641M-4 router offers a single, flexible platform to address a variety of wireless communications needs with over-the-air configuration and system monitoring for optimal connectivity. This router enables wireless data connectivity over public and private LTE cellular networks at 4G speeds.

EL-641M-4 router has dual SIM backup, 4 LAN ports, 1 port could be changed to Ethernet WAN connection (for fixed internet fail over to cellular). An optional 802.11 b/g/n Wi-Fi interface access point and client operations supports connectivity to IP applications in a variety of different connection scenarios. RS232 and RS485 interfaces are provided to support Serial to IP communication. EL-641M-4 router also support 2 x digital input and 2 x Digital output for alarm applications.

EL-641M-4 router supports 9 to 48 VDC wide range power inputs, designed with reverse-voltage protection mechanism for greater reliability. It is an advanced choice for universal wireless M2M applications with reliable features for data transmission.

1.1. Features and Benefits

1.1.1 Industrial internet access

- Wireless Mobile Broadband 3G / 4G Connection
- Remote access to SCADA System for Industrial Automation
- Reduce high costs for on-site maintenance

1.1.1 Designed for industrial usage

- Power Input Range 9 to 48 VDC
- Industrial designed for harsh environment
- Compact metal casing for easy mounting

1.1.2 Secure and reliable remote connection

- Connection manager ensure seamless communication
- Support Multiple VPN tunnels for data encryption
- Firewall prevents unsafe and unauthorized access

1.1.3 Easy to use and easy maintenance

User-friendly web interface for human interaction

1.2. General Specifications

Cellular Interface

- Standards: FDD-LTE/TDD-LTE, WCDMA/UMTS/HSPA/HSPA+/EDGE/GPRS,
- 2× SMA female antenna connector
- x SIM (3.0V & 1.8V)

Wi-Fi Interface

- Standards: 802.11b/g/n, 300Mbps
- SMA Female antenna connector
- Support Wi-Fi AP and Client modes
- Security: WEP, WPA and WPA2 encryption
- Encryption: TKIP, CCMP

Ethernet Interface

- Standard: IEEE 802.3, IEEE 802.3u
- Number of Ports: 4 x 10/100 Mbps, RJ45 connector
- 1 x WAN interface (configurable on Web GUI)
- 1.5KV magnetic isolation protection

Serial Interface

- 1×RS232 (3 PIN): TX, RX, GND
- 1 x RS485 (2 PIN): Data+(A), Data-(B)
- Baud rate: 300 bps to 115200 bps
- Connector: terminal block
- 15KV ESD protection

DI/DO Interface

- Type: 2 x DI + 2 x DO
- Connector: terminal block
- Isolation: 3KVDC or 2KVrms
- Absolute maximum VDC: 36VDC
- Absolute maximum ADC: 100mA

Other Interfaces

- 1× RST button
- LED instruction: 1 x SYS, 1 x NET, 1 x USR, 3 x RSSI

Software

- Network protocols: DHCP, ICMP, PPPoE, HTTP, HTTPS, DNS, VRRP, NTP...
- VPN: IPSec, GRE, OpenVPN, DMVPN
- Policy: RIPv1/RIPv2/OSPF/BGP dynamic route (optional)
- Firewall & Filter: Port forwarding, DMZ, anti-DoS, ACL
- Serial port: TCP server and client, UDP
- Management: Web

Power Supply and Consumption

- Connector: 3-pin 3.5 mm female socket with lock
- Input voltage range: 9~48VDC
- Power consumption:

- Idle: 100 mA@12V
- Data link: 400 mA (peak) @12V

Physical Specification

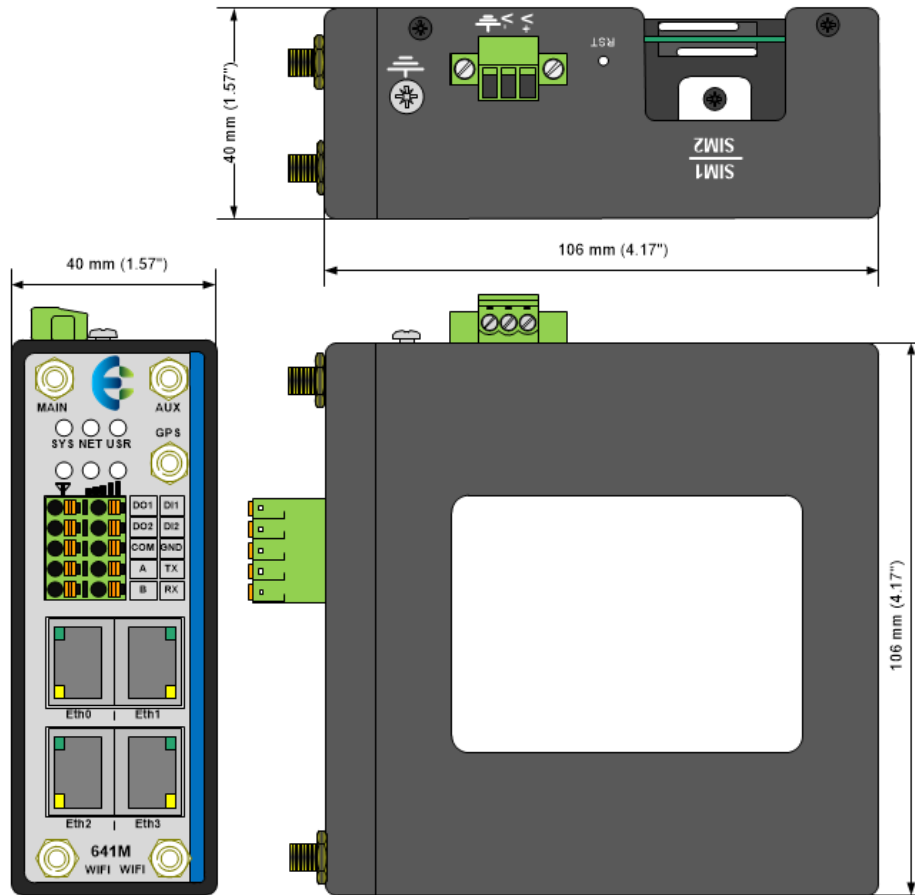
- Ingress Protection: IP30
- Housing & Weight: Metal, 300g
- Dimension: 104mm x 104mm x 38mm (excluding antenna)
- Installations: Din-rail mounting

Environmental

- Operation temperature: -40~+75°C
- Store temperature: -40~+85°C
- Operation humidity: 5% to 95% non-condensing

1.3. Mechanical Specifications

Dimension: 106mm x 106mm x 40mm (excluding antenna)



1.4. Package Checklist

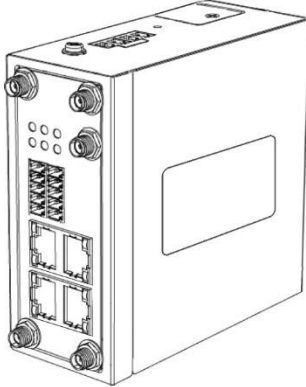
EL-641M-4 router includes the parts shown in below, please verify your components.

NOTE: if any of the below items is missing or damaged, please contact your sales representative.

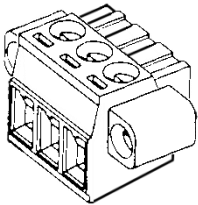
Included equipment

- 1 x Industrial Cellular 4G-LTE Router EL-641M-4 Router

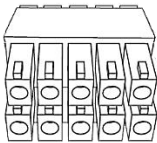
EL-641M-4 router



- 1 x 3-pin 3.5 mm male terminal block with lock for power supply



- 1 x 10-pin 3.5 mm male terminal block for RS232/RS485/DI/DO



1 x Ethernet cable



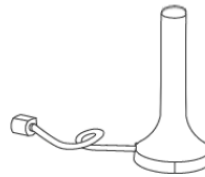
Optional Accessories (sold separately)

3G/4G cellular antenna

Stubby antenna



Magnet antenna



SMA Female Wi-Fi antenna

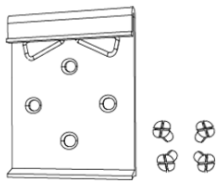
Stubby antenna



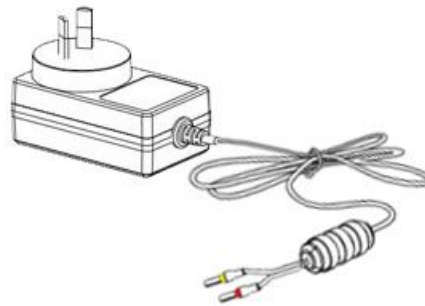
Magnet antenna



35mm Din-rail mounting kit



AC/DC power adapter (12VDC, 1.5A; AU plug)



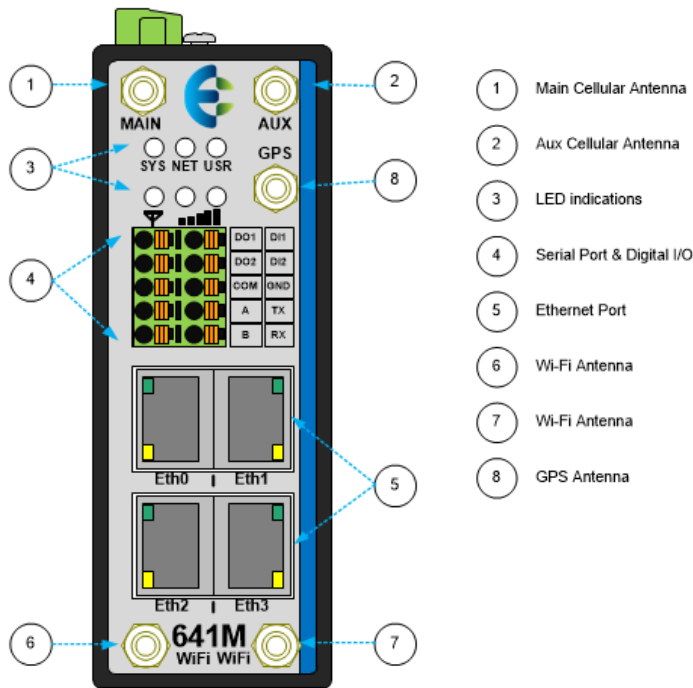
1.5. Order Information

Model	Part Number	Description
EL-641M-2	EL-641M-2-W	4G LTE, Dual SIMs, 2 x Eth, 1 x RS232 (3 PIN), 1 x RS485, 2 x DI, 2 x DO, 9 - 48VDC,
EL-641M-4	EL-641M-4-W	4G LTE, Dual SIMs, 4 x Eth, 1 x RS232 (3 PIN), 1 x RS485, 2 x DI, 2 x DO, 9 - 48VDC, 2.4GHz Wi-Fi, GPS

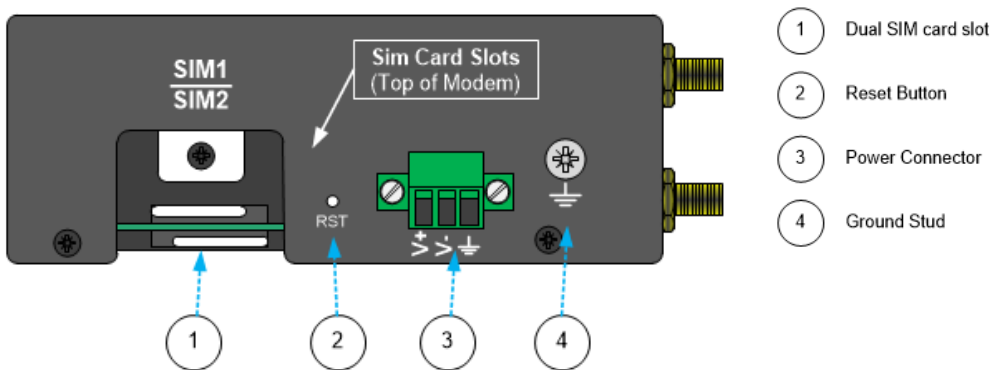
2 Installation

2.1. Product Overview


2.1.1 Front Panel



2.1.2 Left Side Panel



2.2. LED Indicators

Name	Color	Status	Description
SYS	Green	Slow Blinking (500ms duration)	Operating normally
		Fast Blinking	System initialing
		Off	Power is off
NET	Green	On	Register to Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network).
		Fast Blinking (500ms duration)	Register to Non-Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network, then WCDMA and GPRS is non-highest priority network).
		Off	Register failed
USR: SIM	Green	On	Router is trying cellular connection with SIM1
		Fast Blinking (250ms duration)	Router is trying cellular connection with SIM2
		Off	No SIM detected
USR: Wi-Fi	Green	On	Wi-Fi is enable but without data transmission
		Blinking	Wi-Fi is enabled and data transmission
		Off	Wi-Fi is disable or initialize failed
Signal Strength Indicator 	Green	On, 3 LED light up	Signal strength (21-31) is high
		On, 2 LED light up	Signal strength (11-20) is medium
		On, 1 LED light up	Signal strength (1-10) is low
		Off	No signal

2.3. Ethernet Port Indicator

Name	Status	Description
Link indicator	On	Connection is established
	Blinking	Data is being transmitted
	Off	Connection is not established

NOTE: There are two LED indicators for each Ethernet port. Due to the chipset design EL-641M-4 router would only light up the green one(Link indicator) on left side, the right LED is Off without meaning.

2.4. PIN Definition of Terminal block

2.4.3 Serial Port & DIDO



PIN	RS232	RS485	DI	DO	Direction
1	--	--	--	DO1	Router-->Device
2	--	--	--	DO2	Router-->Device
3	--	--	--	COM	--
4	--	A	--	--	Router<-->Device
5	--	B	--	--	Router<-->Device
6	--	--	DI1	--	Router<--Device
7	--	--	DI2	--	Router<--Device
8	GND	--	--	--	--
9	TX	--	--	--	Router-->Device
10	RX	--	--	--	Router<--Device

2.4.4 Power Input



PIN	Description
V+ (Red line)	Positive
V- (Yellow line)	Negative
PGND	GND

2.5. Reset Button

Function	Action
Reboot	Press the RST button within 3s under operation status
Factory Reset	Press the RST button between 3s to 10s, all LEDs blink few times then reboot the router manually.
Run Normally	Press the RST button more than 10s, router will run normally without reboot or factory reset.

2.6. Insert SIM card

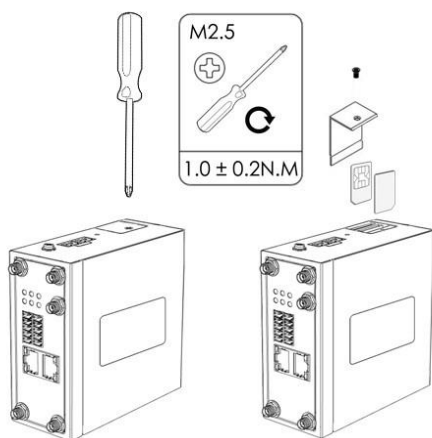
Insert / Remove SIM card

Make sure the power is disconnected.

Use a Phillips-head screwdriver to remove SIM slot cover.

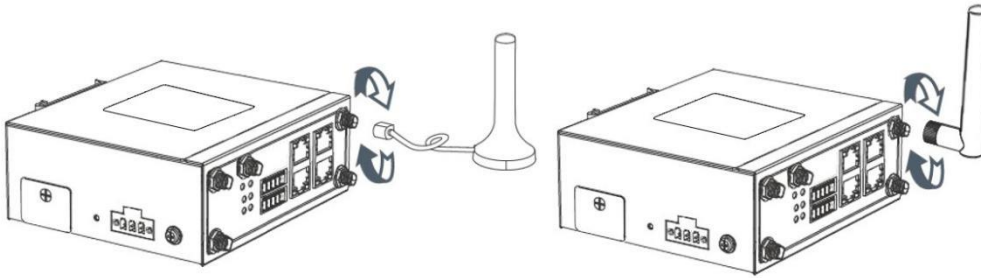
Insert the SIM card(s) in to the SIM sockets.

Replace the SIM slot cover.



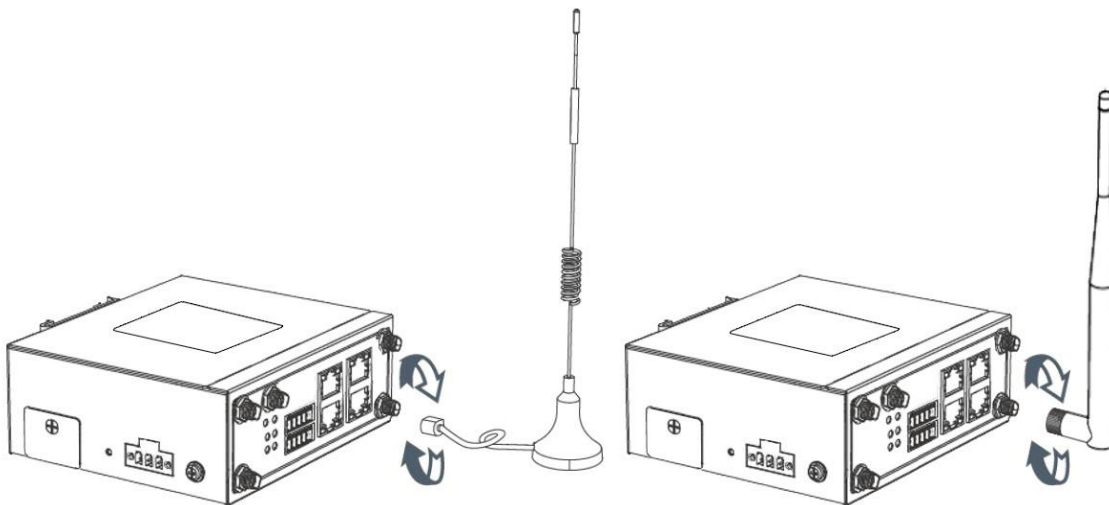
2.7. Install Antenna

- Connect the cellular antenna to the MAIN and AUX connector on the unit.



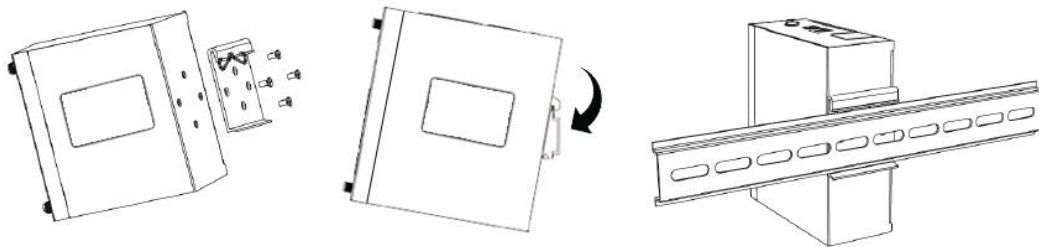
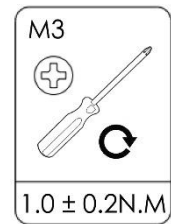
NOTE: EL-641M-4 router supports dual antennas with MAIN and AUX connectors. MAIN connector is for data receiving and transmission. AUX connector is for enhancing signal strength, which cannot be used separately.

- Connect the Wi-Fi antenna to the Wi-Fi connector on the unit.



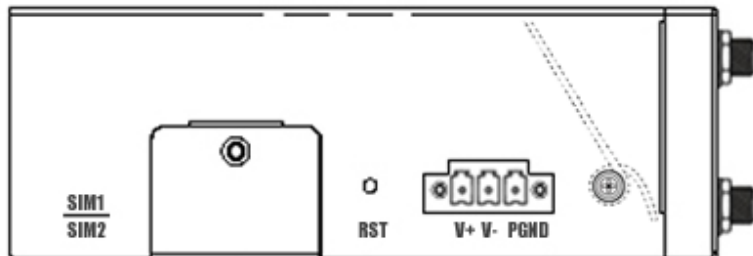
2.8. DIN-rail Mounting

- Use 4 pcs of M3x6 flat head phillips screws to fix the DIN-rail to the router.
- Insert the upper lip of the DIN-rail into the DIN-rail mounting kit.
- Press the router towards the DIN-rail until it snaps into place.



2.9. Protective Grounding Installation

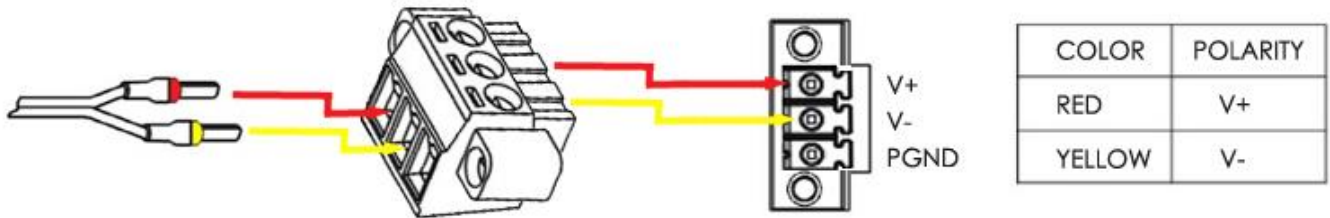
- Remove the grounding nut.
- Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.



NOTE: Strongly recommended the router to be grounded when deployed.

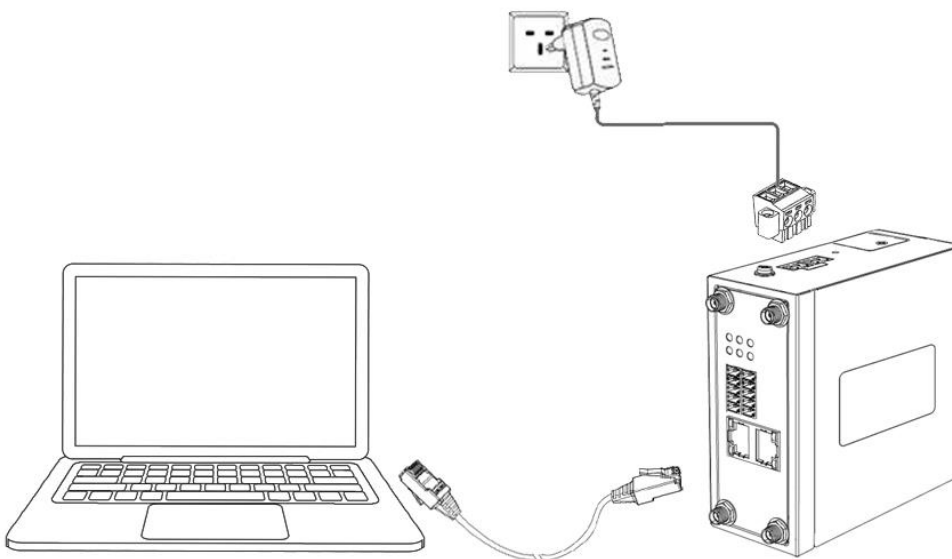
2.10. Power Supply Installation

1. Remove the pluggable connector from the unit, then loosen the screws for the locking flanges as needed.
2. Connect the wires of the power supply to the terminals.



2.11. Power On The Router

1. Connect one end of the Ethernet cable to the LAN port on the unit and the other end to a LAN port on a PC.
2. Connect the AC power to a power source.
3. Router is ready when SYS LED is blinking.



3 Access to Web page

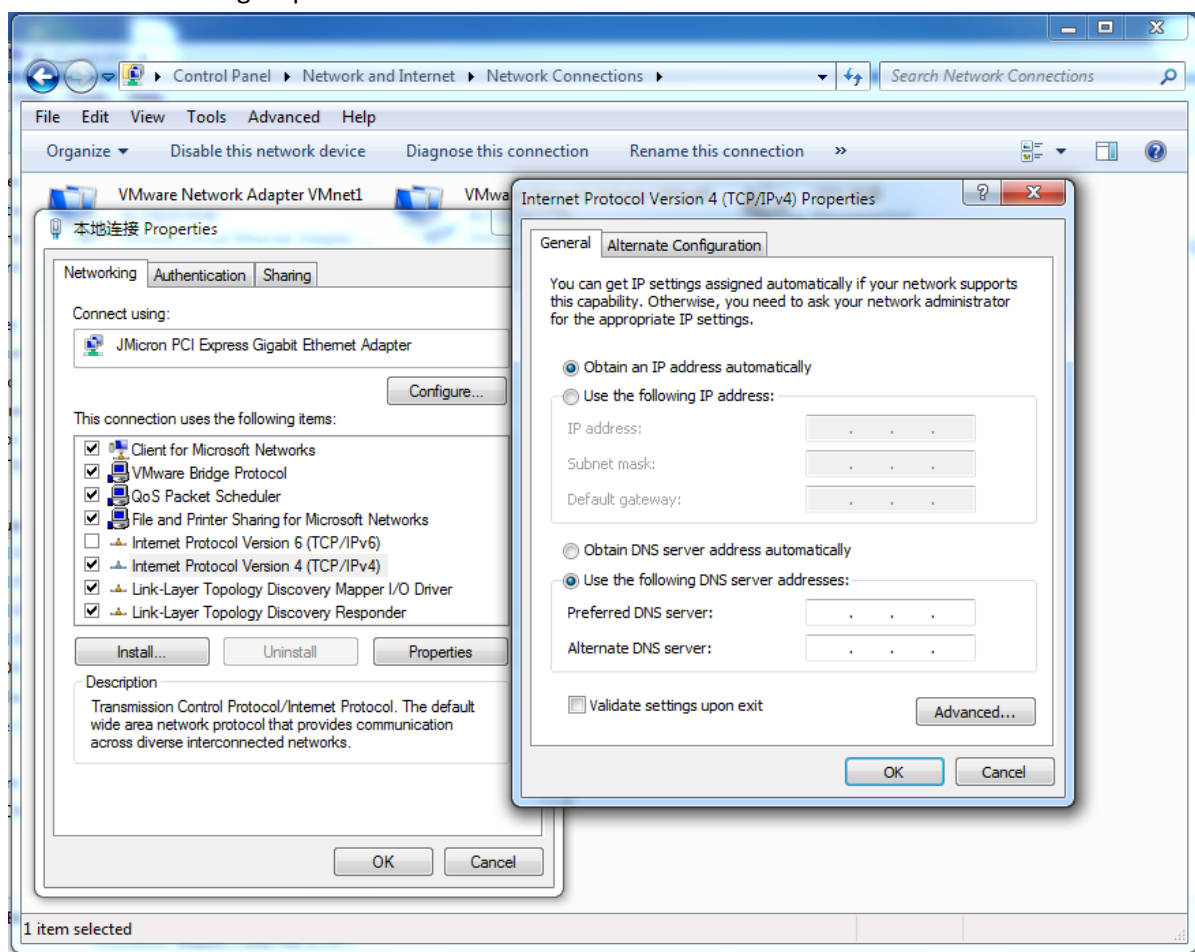
3.1. PC Configuration

EL-641M-4 router contains a DHCP server which will automatically assign an IP address to your PC, however in some cases the user may need to change the network settings on their PC to accept the IP address from the EL-641M-4. or you can configure a static IP address manually.

- Obtain an IP address automatically

The process required to do this differs depending on the version of Windows you are using.

NOTE: The following steps are based on Windows 7.



Select Start » Control Panel » Network Connections. Right click Local Area Connection and select Properties to open the configuration dialog box for Local Area Connection. Select Internet Protocol (TCP/IP) and click Properties to open the TCP/IP configuration window. On the General tab, select Obtain an IP address automatically and Obtain DNS server address automatically. Click OK to complete TCP/IP configuration.

3.2. Factory Default Settings

EL-641M-4 router supports Web-based configuration interface for management. If this is the first time for you to configure the router, please refer to below default settings.

Username: admin

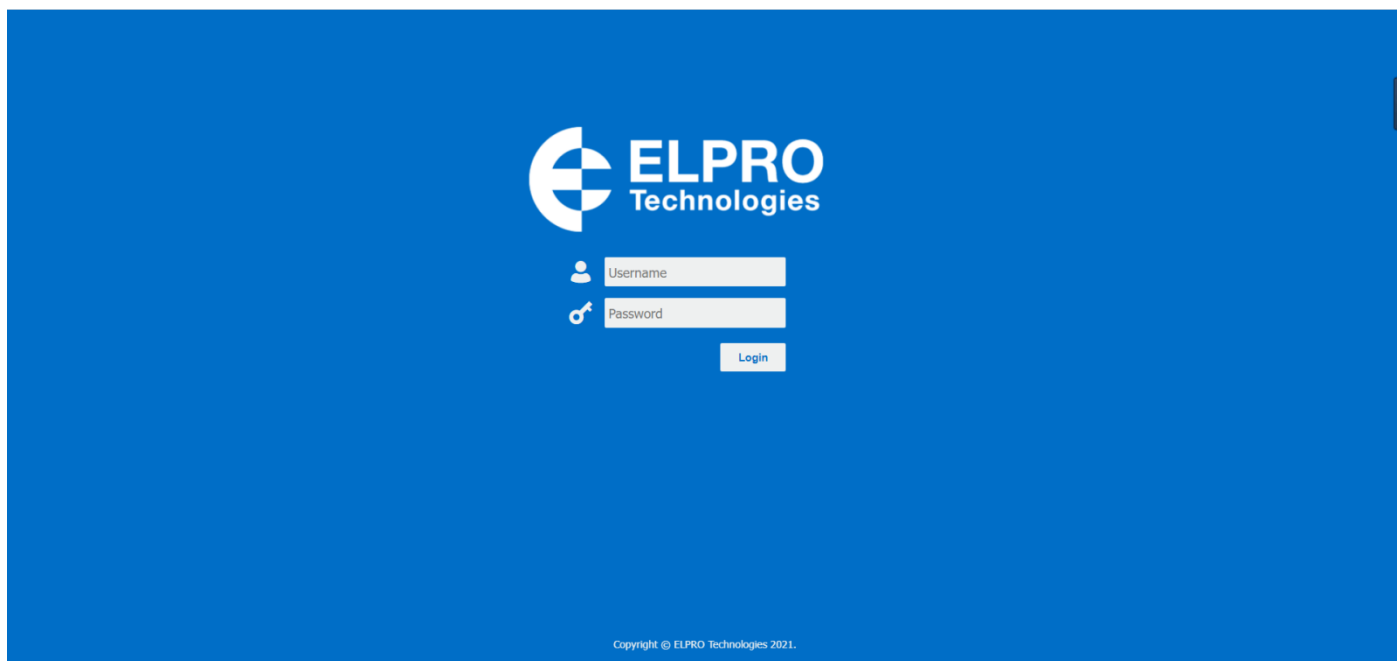
Password: admin

LAN IP Address: 192.168.1.1 (Eth0~Eth3 bridge as LAN mode)

DHCP Server: Enabled

3.3. Login to Web Page

1. Start a Web browser on your PC (Chrome and IE are recommended), enter 192.168.1.1 into the address bar of the web browser.
2. Then use the default username and password(admin/admin), to log in to the router.



4 Web Configuration

4.1. Web Interface

EL-641M-4 router Web interface is divided into two sections. In the left pane is the main navigation menu. On the right is the content area for each page.

The screenshot displays the ELPRO Technologies web interface. The top header includes the ELPRO logo, the user name 'admin', and buttons for 'Reboot' and 'Logout'. A left-hand navigation menu lists various sections: Overview, Syslog, Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance. The main content area is titled 'Status' and is divided into two sections: 'System Information' and 'Active Link Information'.

System Information	
Device Model	EL-641M-4
System Uptime	00:03:00
System Time	2022-12-07 09:35:39
RAM Usage	21M Free/18M Shared/64M Total
Firmware Version	1.1.7 (22a7514)
Kernel Version	4.4.92
Serial Number	22125147330001

Active Link Information	
Link Type	WAN
IP Address	192.168.111.154
Netmask	255.255.255.0
Gateway	192.168.111.1
Primary DNS Server	192.168.111.1
Secondary DNS Server	

Copyright © ELPRO Technologies 2021.

NOTE: The navigation menu may contain fewer sections than shown here depending on which options are installed in your unit.

- Reboot: reset the router within power disconnect.
- Logout: logout to web authorization page.



- Save: save the configuration on current page.
- Apply: apply the changes on current page immediately.



- Close: exit without changing the configuration on current page.



4.2. Overview

4.2.1 Status

You can view the system information of the router on this page.

Status		
System Information		
Device Model	EL-641M-4	
System Uptime	00:11:31	
System Time	2022-12-07 09:44:10 ↻	
RAM Usage	20M Free/18M Shared/64M Total	
Firmware Version	1.1.7 (22a7514)	
Kernel Version	4.4.92	
Serial Number	22125147330001	

System Information

Device Module

Displays the model name of router

System Uptime

Displays the duration the system has been up in hours, minutes and seconds.

System Time

Displays the current date and time.

RAM Usage

Displays the RAM capacity and the available RAM memory.

Firmware Version

Displays the current firmware version of router.

Kernel Version

Displays the current kernel version of router.

Serial Number

Display the serial number of router.

Active Link Information

Link Type	WAN
IP Address	192.168.111.154
Netmask	255.255.255.0
Gateway	192.168.111.1
Primary DNS Server	192.168.111.1
Secondary DNS Server	

Active Link Information**Link Type**

Current interface for internet access.

IP Address

Displays the IP address assigned to this interface.

Netmask

Displays the subnet mask of this interface.

Gateway

Displays the gateway of this interface. This is used for routing packets to remote networks.

Primary DNS Server

Displays the primary DNS server of this interface.

Secondary DNS Server

Displays the secondary DNS server of this interface.

4.2.2 Syslog

[Syslog](#) [Events](#)

Syslog Information

```
Dec 3 14:08:07 elpro syslog.info syslogd started: BusyBox v1.25.1
Dec 3 14:08:12 elpro user.warn modem[1736]: can not get runing sim, use SIM1 as default
Dec 3 14:08:12 elpro user.debug modem[1736]: modem power-on successfully
Dec 3 14:08:13 elpro user.debug connection_manager[1754]: setup SIM 1 as initial SIM
Dec 3 14:08:13 elpro user.debug connection_manager[1754]: wwan1 start connect
Dec 3 14:08:13 elpro daemon.info dnsmasq[1774]: started, version 2.78 cachesize 150
Dec 3 14:08:13 elpro daemon.info dnsmasq[1774]: compile time options: no-IPv6 GNU-getopt no-DBus no-i18n no-IDN DHCP no-DHCPv6 no-Lua TFTP no-conntrack no-ipset no-auth no-DNSSEC no-ID loop-detect inotify
Dec 3 14:08:13 elpro daemon.info dnsmasq-dhcp[1774]: DHCP, IP range 192.168.1.2 -- 192.168.1.200, lease time 2h
Dec 3 14:08:13 elpro daemon.info dnsmasq-dhcp[1774]: DHCP, sockets bound exclusively to interface lan0
Dec 3 14:08:13 elpro daemon.warn dnsmasq[1774]: no servers found in /etc/resolv.conf, will retry
Dec 3 14:08:13 elpro daemon.info dnsmasq[1774]: read /etc/hosts - 2 addresses
Dec 3 14:08:13 elpro user.debug connection_manager[1754]: waiting for modem to initialize using SIM 1
Dec 3 14:08:14 elpro daemon.notice procd: /etc/rc.d/S13lan: Command failed: Not found
Dec 3 14:08:15 elpro local0.debug webserver: webserver started
Dec 3 14:08:21 elpro cron.info crond[1974]: crond (busybox 1.25.1) started, log level 8
Dec 3 14:08:21 elpro daemon.info procd: - init complete -
Dec 3 14:08:41 elpro user.err modem[1736]: modem not found, try to reset modem
Dec 3 14:08:41 elpro user.notice modem[1736]: reset modem by power reset
Dec 3 14:08:43 elpro daemon.info urandom_seed[2006]: Seed saved (/etc/urandom.seed)
Dec 3 14:09:01 elpro user.err modem[1736]: modem enable failed
Dec 3 14:09:32 elpro user.err modem[1736]: cannot find AT command port of modem
Dec 3 14:09:56 elpro daemon.info dnsmasq[1774]: exiting on receipt of SIGTERM
Dec 3 14:09:56 elpro daemon.info dnsmasq[2436]: started, version 2.78 cachesize 150
Dec 3 14:09:56 elpro daemon.info dnsmasq[2436]: compile time options: no-IPv6 GNU-getopt no-DBus no-i18n no-IDN DHCP no-DHCPv6 no-Lua TFTP no-conntrack no-ipset no-auth no-DNSSEC no-ID loop-detect inotify
Dec 3 14:09:56 elpro daemon.info dnsmasq-dhcp[2436]: DHCP, IP range 192.168.1.2 -- 192.168.1.200, lease time 2h
Dec 3 14:09:56 elpro daemon.info dnsmasq-dhcp[2436]: DHCP, sockets bound exclusively to interface lan0
Dec 3 14:09:56 elpro daemon.warn dnsmasq[2436]: no servers found in /etc/resolv.conf, will retry
Dec 3 14:09:56 elpro daemon.info dnsmasq[2436]: read /etc/hosts - 2 addresses
```

[Download Diagnosis](#) [Download Syslog](#) [Clear](#) [Refresh](#)

Syslog Information

Download Diagnosis

Download the Diagnosis file for analysis.

Download Syslog

Download the complete syslog since last reboot.

Clear

Clear the current page syslog printing.

Refresh

Reload the current page with latest syslog printing.

4.3. Link Management

This section shows you the setup of link management.

4.3.1 Connection Manager

Status		Connection			
Connection Information					
Index	Type	Status	IP Address	Netmask	Gateway
1	WWAN1	Connected	123.209.123.235	255.255.255.248	123.209.123.236
2	WWAN2	Disconnected			

Connection Manager->Status

Type

Displays the connection interface

Status

Displays the connection status of this interface.

IP Address





Displays the IP Address of this interface.


Netmask

Displays the subnet mask of this interface.

Gateway

Displays the gateway of this interface. This is used for routing packets to remote networks.

Status		Connection		
General Settings				
Priority	Enable	Connection Type	Description	
1	true	WWAN1		  
2	true	WWAN2		 

Click  to add a new priority interface.

Click  to edit current interface settings.

Click  to delete current interface.

Connection Manager->Connection

Priority

Displays the priority list of default routing selection.

Enable

Displays the connection enable status.

Connection Type

Displays the name of this interface.

Description

Displays the description of this connection.

Connection Settings	
General Settings	
Priority	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Connection Type	<input type="text" value="WWAN1"/> ?
Description	<input type="text"/>
NAT Enable	<input checked="" type="checkbox"/>
ICMP Detection Settings	
Enable	<input checked="" type="checkbox"/>
Primary Server	<input type="text" value="8.8.8.8"/>
Secondary Server	<input type="text" value="114.114.114.114"/>
Interval	<input type="text" value="300"/> ?
Retry Interval	<input type="text" value="5"/> ?
Timeout	<input type="text" value="3"/> ?
Retry Times	<input type="text" value="3"/> ?
<input type="button" value="Save"/> <input type="button" value="Close"/>	

Connection Settings

Priority

Displays current index on priority list.

Connection Type

Select the available interface as outbound link.

NOTE: specify SIM1 carrier link as WWAN1, SIM2 carrier link as WWAN2.

NAT Enable

Check this box to enable NAT (Network Address Translation) on the current link.

ICMP Detection Settings->Enable

Check this box to detect link connection status based on pings to a specified IP address.

Primary Server

Enter the primary IP address that pings will be sent to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g. 8.8.8.8).

Secondary Server

Enter the secondary IP address that pings will be sent to, when the primary server is ping failed, router would try to ping the secondary server.

Interval

The duration of each ICMP detection in seconds.

Retry Interval

The interval in seconds between each ping if no packets have been received.

Timeout

Enter timeout for received ping reply to determine the ICMP detection failure.

Retry Times

Specify the retry times for ICMP detection.

4.3.2 Cellular

EL-641M-4 Router main function is connecting to Internet by cellular modem.

Status		Cellular								
Cellular Information										
Index	Modem	Registration	CSQ	Operator	Network Type	IMEI	IMSI	TX Bytes	RX Bytes	
1	EC25	Registered	High(30,-53d...	Telstra #LetsVaxx Te...	LTE	866989050372660	505016004153555	12.67 KB	16.13 KB	
	Index 1 Modem EC25 Registration Registered CSQ High(30,-53dBm) Operator Telstra #LetsVaxx Telstra Network Type LTE IMEI 866989050372660 PLMN ID 50501 Local Area Code 7038 Cell ID 8B53B1F IMSI 505016004153555 TX Bytes 12.67 KB RX Bytes 16.13 KB Modem Firmware EC25AUFAR06A06M4G									

Copyright © ELPRO Technologies 2021.

Cellular->Status

Modem

Displays the module of the modem used by this WWAN interface.

Registration

Displays the registration status of SIM card.

CSQ

Displays the signal strength of the carrier network.

Operator

Displays the wireless network provider.

Network Type

Displays the RF technology currently active. Example: LTE, UMTS, or CDMA.

IMEI

International Mobile Electronic Identifier. Depending on the carrier and technology used, this may be required for the carrier when activating the data contract. In some cases, this will be blank.

PLMN ID

Displays the current PLMN ID, including MCC, MNC, LAC and Cell ID.

Local Area Code

Displays the location area code of the SIM card.

Cell ID

Displays the Cell ID of the SIM card location.

IMSI

International Mobile Subscriber Identity, as read from the SIM. This is the user’s network subscription.

TX Bytes

Displays the total bytes transmitted since the time the unit was connected. EL-641M-4 router would record this data with same SIM card, reboot would not erase this data.

RX Bytes

Displays the total bytes received since the time the unit was connected. EL-641M-4 router would record this data with same SIM card, reboot would not erase this data.

Modem Firmware

Displays firmware version of the module used by the WWAN interface.

Status		Cellular	
Modem General Settings			
Index	SIM Card	Auto APN	
1	SIM1	false	
2	SIM2	true	

Cellular

SIM Card

Displays the SIM card support on this unit.

Auto APN

Displays the Enable status of auto APN function.

SIM Card Settings

Modem General Settings

Index:

SIM Card:

Auto APN:

Dial Number:

Authentication Type:

PIN Code: ?

Monthly Data Limitation: ?

Monthly Billing Day: ?

Data Roaming:

Override Primary DNS:

Override Secondary DNS:

Expert Options: ?

Modem Network Settings

Network Type:

Use All Bands:

SIM Card Settings

SIM Card

Displays the current SIM card settings.

Auto APN

Check this box enable auto checking the Access Point Name provided by the carrier.

Dial Number

Enter the dial number of the carrier.

Authentication Type

Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.

PIN Code

Enter a 4-8 characters PIN code to unlock the SIM.

Monthly Data Limitation

Enter the data total amount for SIM card, SIM card switchover when data reach limitation.

Monthly Billing Day

Enter the date of renew data amount every month.

Data Roaming

Enable or disable the data roaming function on the router.

Override Primary DNS

Enter the primary DNS server will override the automatically obtained DNS.

Override Secondary DNS

Enter the secondary DNS server will override the automatically obtained DNS.

Network Type

Select the mode of operation of the cell module (Auto, 4G Firstly, 4G Only, etc.).

Use All Bands

Check this box to enable all bands selection or choose specified bands.

4.3.3 Ethernet

The same instructions apply to settings for all Ethernet interfaces.

<u>Status</u>	Port Assignment	LAN	VLAN	
Ethernet Port Information				
Index	Name	Status		
1	ETH0	Down		
2	ETH1	Up		
Interface Information				
Index	Name	MAC Address		
1	lan0	00:12:AF:40:00:04		
DHCP Lease Table				
Index	MAC Address	IP Address	Lease Expires	Hostname

Ethernet->Status

Ethernet Port Information

Displays the port physical connected states.

Interface Information

Displays the name and MAC address of Ethernet interface.

DHCP Lease Table

Displays the current IP address assigned to DHCP client.

Ethernet->Port Assignment

Port

Displays the port states and numbers of this unit.

Interface

Displays the port states of belong subnet.

The screenshot shows a 'Port Settings' dialog box with a 'General Settings' section. It contains three input fields: 'Index' with the value '1', 'Port' with a dropdown menu showing 'Eth0', and 'Interface' with a dropdown menu showing 'LAN0'. At the bottom right, there are two buttons: 'Save' and 'Close'.

Note: Please make sure LAN0 is assigned and existing.

Ethernet->Port Settings

Port

Indicate the current configurate port.

Interface

Select belong subnet for current configurate port.

The screenshot shows a configuration page with tabs for 'Status', 'Port Assignment', 'WAN', 'LAN', and 'VLAN'. The 'WAN' tab is active. Under 'General Settings', the 'Connection Type' is set to 'DHCP'. Under 'Advanced Settings', the 'MTU' is set to '1500', and there are empty input fields for 'Override Primary DNS' and 'Override Secondary DNS'.

Ethernet->WAN

Connection Type

If you select DHCP Client, external DHCP server will assign an IP address to this unit.

MTU

Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.

Override Primary DNS

Enter the primary DNS server will override the automatically obtained DNS.

Override Secondary DNS

Enter the secondary DNS server will override the automatically obtained DNS.

Ethernet->WAN->Secondary Wan Settings

IP Address

Enter the IP address of secondary wan interface.

Netmask

Enter the netmask of secondary wan interface.

EL-641M-4 also support WAN connection type set to Static IP and PPPoE mode.

The screenshot shows the WAN configuration page with the following sections:

- General Settings:**
 - Connection Type: Static IP (dropdown menu)
 - IP Address: [text input]
 - Netmask: [text input]
 - Gateway: [text input]
 - Primary DNS: [text input]
 - Secondary DNS: [text input]
- Advanced Settings:**
 - MTU: 1500 (text input)
 - Override Primary DNS: [text input]
 - Override Secondary DNS: [text input]
- Secondary Wan Settings:**
 - Table with columns: Index, IP Address, Netmask, and a plus icon (+).

Ethernet->WAN->Static IP or PPPoE

IP Address

Static address for this interface. It must be on the same subnet as the gateway.

Netmask

Will be assigned by the gateway.

Gateway

IP address of the Gateway (DHCP Host). If not known this can be left as all zeros.

Primary DNS

IP address of the primary DNS server.

Secondary DNS

IP address of the secondary DNS server.

Authentication Type

Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.

Username

Username to provide when connecting.

Password

Password to provide when connecting.

Status	Port Assignment	WAN	LAN	VLAN
General Settings				
	Connection Type	PPPoE		
	Authentication Type	Auto		
	Username	<input type="text"/>		
	Password	<input type="text"/>		
Advanced Settings				
	MTU	1500		
	Override Primary DNS	<input type="text"/>		
	Override Secondary DNS	<input type="text"/>		

Ethernet->LAN

Interface



Displays current name of LAN subnet.

IP Address

Displays LAN IP address of this subnet.

Netmask

Displays subnet mask for this subnet.

Status	Port Assignment	WAN	LAN	VLAN
General Settings				
Index	Interface	IP Address	Netmask	
1	LAN0	192.168.1.1	255.255.255.0	 
Multiple IP Settings				
Index	Interface	IP Address	Netmask	

The screenshot shows the LAN Settings configuration page. It is divided into three sections: General Settings, DHCP Settings, and MAC Binding IP Settings. The General Settings section includes fields for Index (1), Interface (LAN0), IP Address (192.168.1.1), Netmask (255.255.255.0), and MTU (1500). The DHCP Settings section includes a checked 'Enable' checkbox, a 'Mode' dropdown set to 'Server', and input fields for IP Pool Start (192.168.1.2), IP Pool End (192.168.1.200), Netmask (255.255.255.0), Lease Time (120), Gateway, Primary DNS, Secondary DNS, and WINS Server. At the bottom right, there are 'Save' and 'Close' buttons.

This is a close-up of the DHCP Settings section from the previous screenshot. It shows the 'Enable' checkbox checked, the 'Mode' dropdown menu set to 'Relay', and an empty 'Relay Server' input field. 'Save' and 'Close' buttons are visible at the bottom right.

Ethernet->LAN

Interface

Select the configure LAN port of this subnet.

IP Address

Enter LAN IP address for this interface.

Netmask

Enter subnet mask for this subnet.

MTU

Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.

Enable

Check this box to enable DHCP feature on current LAN port.

Mode

Select the DHCP working mode from "Server" or "Relay".

Relay Server

Enter the IP address of DHCP relay server.

IP Pool Start

External LAN devices connected to this unit will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.

IP Pool End

This is the end of the pool of IP addresses.

Netmask

Subnet mask of the IP address obtained by DHCP clients from DHCP server.

Lease Time

The lease time of the IP address obtained by DHCP clients from DHCP server.

Gateway

The gateway address obtained by DHCP clients from DHCP server.

Primary DNS

Primary DNS server address obtained by DHCP clients from DHCP server.

Secondary DNS

Secondary DNS server address obtained by DHCP clients from DHCP server.

WINS Server

Windows Internet Naming Service obtained by DHCP clients from DHCP server.

MAC Binding IP Settings

MAC Binding IP Settings

Index

Enable

Description

Host MAC Address ?

Host IP Address

IP Pool Start

Ethernet->LAN->MAC Binding IP Settings

Enable

Check this box to enable MAC binding IP feature.

Description

Enter the description for MAC binding IP feature.

Host MAC Address

Enter the host MAC address.

Host IP Address

Enter the host IP address.

The screenshot shows a configuration window titled "Multiple IP Settings". It contains a sub-header "Multiple IP Settings" and four input fields: "Index" (text box with "1"), "Interface" (dropdown menu with "LAN0"), "IP Address" (text box), and "Netmask" (text box). At the bottom right, there are "Save" and "Close" buttons.

Ethernet->LAN->Multiple IP Settings

Interface

Select the configurate LAN port of this subnet.

IP Address

Enter multiple IP address for this interface.

Netmask

Enter subnet mask for this subnet.

The screenshot shows a configuration window titled "Trunk Settings". It contains a sub-header "VLAN Trunk Settings" and five input fields: "Index" (text box with "1"), "Interface" (dropdown menu with "LAN0"), "VID" (text box with "10"), "IP Address" (text box), and "Netmask" (text box). At the bottom right, there are "Save" and "Close" buttons.

Ethernet->VLAN->VLAN Trunk Settings

Interface

Select the LAN port for VLAN trunk.

VID

Specify the VLAN ID for VLAN trunk.

IP Address

Enter IP address for this VLAN trunk.

Netmask

Enter subnet mask for this VLAN trunk.

4.3.4 Wi-Fi

EL-641M-4 router could only be set to function as either a Wi-Fi Client or a Wi-Fi Access Point, but not both simultaneously. Select Wi-Fi (Access Point) from the main navigation menu to Wi-Fi (default as Access Point) page, which contains tabs for configuration of the Wi-Fi Access Point interface.

You could review the Wi-Fi connection status as below.

[Status](#) [Basic](#) [WiFi AP](#)

WiFi Status

Status	Ready
SSID	Elpro
MAC Address	a8:3f:a1:e0:3b:b5
Current Channel	6
Channel Width	40 MHz
TX Power	20.00 dBm

Associated Station

Index	MAC Address	Signal	Station Name
-------	-------------	--------	--------------

[Status](#) [Basic](#) [WiFi AP](#)

Basic Settings

Running Mode	<input type="text" value="AP"/>
Country Code	<input type="text" value="CN"/>

Wi-Fi->Basic

Running Mode

Select the configurate Wi-Fi mode from AP or Client.

Country Code

Enter the country where the AP is located.

Wi-Fi AP

Wi-Fi AP settings page as below.

The screenshot shows the configuration interface for the Wi-Fi AP. It includes the following settings:

- WiFi AP Settings:**
 - Enable:
 - SSID:
 - Enable Broadcast SSID:
 - Security Mode: ?
- Advanced Settings:**
 - Channel: ?
 - Wireless Mode:
 - Channel Width: ?
 - Beacon TX Rate HT MCS Index: ?
 - TX Power:
 - Beacon Interval:
 - DTIM Period:
 - Max Client Support:
 - Enable Short GI:
 - Enable AP Isolate:

Buttons: **Save** and **Apply**

Wi-Fi->Wi-Fi AP

Enable

Check this box will enable the Wireless interface.

SSID

The SSID is the name of the wireless local network. Devices connecting to the EL-641M-4 router WiFi access will identify the Access Point by this SSID.

Enable Broadcast SSID

When the checkbox is not checked, SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.

Security Mode

Select security mode from "None", "WEP" or "WPA PSK".

WPA Type

Select WPA Type from "Auto", "WPA" and "WPA2".

Encryption Type

Select the encryption method. Options are "Auto", "TKIP", or "CCMP". Because these options depend on the authentication method selected, some options will not be available.

Channel

Select the Wi-Fi channel the module will transmit on. If there are other Wi-Fi devices in the area the EL-641M-4 router should be set to a different channel than the other access points. Channels available for selection depend on the selected Band.

Wireless Mode

Select the Wi-Fi 802.11 mode: B, G, or N. Available selections depend on selected Band.

Channel Width

Select the width of the Wi-Fi channel. 20 MHz will limit the channel to 20 MHz wide; 20/40 MHz will enable the use of a 40 MHz wide channel when available.

Beacon TX Rate HT MCS Index

Modulation and Coding Scheme, The MCS modulation coding table is a representation proposed by 802.11n to characterize the communication rate of the WLAN. The MCS takes the factors affecting the communication rate as the columns of the table and uses the MCS index as a row to form a rate table.

TX power

Select the transmission power for the AP from “High”, “Medium” and “Low”.

Beacon Interval

Enter the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.

DTIM Period

Enter the delivery traffic indication message period and the router AP will multicast the data according to this period.

Max Client Support

Enter the maximum number of clients to access when the router is configured as AP.

Enable Short GI

Check this box to enable Short GI(guard interval), Short GI is a blank time between two symbols, providing a long buffer time for signal delay.

Enable AP Isolate

Check this box to enable AP isolate, the route will isolate all connected wireless devices.

Wi-Fi Client

Wi-Fi Client settings page as below.

Status	Basic	<u>WiFi Client</u>
WiFi Client Settings		
Enable	<input checked="" type="checkbox"/>	
Connect to Hidden SSID	<input type="checkbox"/>	
SSID	<input type="text"/>	
Password	<input type="text"/>	
IP Address Settings		
Connection Type	DHCP	

Status	Basic	<u>WiFi Client</u>
WiFi Client Settings		
Enable	<input checked="" type="checkbox"/>	
Connect to Hidden SSID	<input type="checkbox"/>	
SSID	<input type="text"/>	
Password	<input type="text"/>	
IP Address Settings		
Connection Type	Static IP	
IP Address	<input type="text"/>	
Netmask	<input type="text"/>	
Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	

Wi-Fi->Wi-Fi Client

Enable

Check this box will enable the Wireless interface.

Connect to Hidden SSID

Check this box will enable connect to hidden SSID.

SSID

The SSID of external access point.

Password

Enter the password of external access point.

Connection Type

Select from DHCP Client or Static IP address.

IP Address

Static address for this interface. It must be on the same subnet as the gateway.

Netmask

Will be assigned by the gateway.

Gateway

IP address of the Gateway.

Primary DNS

Enter the primary DNS server will override the automatically obtained DNS.

Secondary DNS

Enter the secondary DNS server will override the automatically obtained DNS.

4.4. Industrial Interface

The Industrial page contains tabs for making configuration settings for Serial RS232 and RS485, Digital input and output. Select Serial & Digital IO from the main navigation menu to navigate to this page.

4.4.1 Serial

You could review the status of serial connection.

Status		Connection					
Serial Information							
Index	Enable	Serial Type	Transmission Method	Protocol	TX Bytes	RX Bytes	Connection Status
1	false	RS485	Transparent	TCP Client			Disconnected
2	false	RS232	Transparent	TCP Client			Disconnected

Serial->Status

Enable

Displays status of current serial function.

Serial Type

Displays the serial type of COM port.

Transmission Method

Displays the transmission method of this serial port.

Protocol

Displays the protocol used by this serial port.

Connection Status

Displays the connection status of this serial port.

Status		Connection				
Serial Connection Settings						
Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

Serial->Connection

Enable

Displays status of current serial function.

Port

Displays the serial type of COM port.

Baud Rate

Displays the serial port baud rate.

Data Bits

Displays the serial port Data Bits.

Stop Bits

Displays the serial port Stop Bits.

Parity

Displays the serial port parity.

Connection Settings

Serial Connection Settings

Index	<input type="text" value="1"/>
Enable	<input type="checkbox"/>
Port	<input type="text" value="COM1"/>
Baud Rate	<input type="text" value="115200"/>
Data Bits	<input type="text" value="8"/>
Stop Bits	<input type="text" value="1"/>
Parity	<input type="text" value="None"/>

Transmission Settings

Transmission Method	<input type="text" value="Transparent"/>
MTU	<input type="text" value="1024"/> ?
Protocol	<input type="text" value="TCP Client"/>
Remote Address	<input type="text"/>
Remote Port	<input type="text" value="2000"/>
Sync to Secondary Address	<input type="checkbox"/>

Serial->Connection Settings

Baud Rate

Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.

Data Bits

Select the values from 7 or 8.

Stop Bits

Select the values from 1 or 2.

Parity

Select values from none, even, odd, mark, space.

Transmission Method

Select the transmission method for serial port. Optional for "Transparent", "Modbus RTU Gateway" and "Modbus ASCII Gateway".

MTU

Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.

Protocol

Select the mode for Serial IP communication. Supported modes are UDP, TCP Server, or TCP Client.

Remote IP Address

Enter the IP address of the remote server.

Remote Port

Enter the port number of the remote server.

Sync to Secondary Address

Check this box to enable the data send to secondary remote server for data backup.

Remote Secondary Address

Enter the remote backup server IP address.

Remote Secondary Port

Enter the remote backup server port.

Below window displays different settings when you select TCP Server on Protocol.

Transmission Settings	
Transmission Method	Transparent <input type="button" value="v"/>
MTU	1024 <input style="float: right;" type="button" value="?"/>
Protocol	TCP Server <input type="button" value="v"/>
Local IP Address	<input type="text"/>
Local Port	2000 <input type="text"/>

Serial->Connection Settings

Local IP Address

Enter the IP Address of the local endpoint.

Local Port

The port number assigned to the serial IP port on which communications will take place.

Below window displays different settings when you select UDP on Protocol.

Transmission Settings	
Transmission Method	Transparent <input type="button" value="v"/>
MTU	1024 <input style="float: right;" type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Local IP Address	<input type="text"/>
Local Port	2000 <input type="text"/>
Remote Address	<input type="text"/>
Remote Port	2000 <input type="text"/>

Serial->Connection Settings

Local IP Address

Enter the IP Address of the local endpoint.

Local Port

The port number assigned to the serial IP port on which communications will take place.

Remote IP Address

Enter the IP address of the remote server.

Remote Port

Enter the port number of the remote server.

4.4.2 Digital IO

This section allows you to set the Digital IO parameters. The Digital input could be used for triggering alarm, and Digital output could be used for controlling the slave device by digital signal.

You could review the status of Digital IO as below.

Status		Digital IO	
Digital Input Information			
Index	Enable	Logic Level	Status
1	false	High	Alarm OFF
2	false	High	Alarm OFF
Digital Output Information			
Index	Enable	Logic Level	Status
1	false	Low	Alarm OFF
2	false	Low	Alarm OFF

Digital IO->Status

Enable

Displays status of current digital IO function.

Logic Level

Displays the electrical level of digital IO port.

Status

Displays the alarm status of digital IO port.

Digital Input

Digital Input Settings

Index

Enable

Alarm ON Mode

Alarm ON Content ?

Alarm OFF Content ?

Digital IO->Digital Input

Enable

Check this box to enable digital Input function.

Alarm ON Mode

Select the electrical level to trigger alarm. Option are “Low” and “High”.

Alarm ON Content

Specify the alarm on content to be sent out via SMS message.

Alarm OFF Content

Specify the alarm off content to be sent out via SMS message.

NOTE Alarm Content can also include special parameters: \$DI_INDEX, \$DATE, \$SERIAL_NUMBER, \$DEVICE_MODEL, \$FIRMWARE_VERSION, \$SYSTEM_UPTIME, \$LINK_TYPE, \$IP_ADDRESS, \$MODEM_MODEL, \$CSQ, \$OPERATOR, \$NETWORK_TYPE, \$IMEI, \$PLMN_ID, \$LOCAL_AREA_CODE, \$CELL_ID, \$IMSI, \$MODEM_FIRMWARE

Digital Input

Digital Input Settings

Index	<input style="width: 90%;" type="text" value="1"/>	
Enable	<input type="checkbox"/>	
Alarm ON Mode	<input style="width: 90%;" type="text" value="Low"/>	▼
Alarm ON Content	<input style="width: 90%;" type="text"/>	?
Alarm OFF Content	<input style="width: 90%;" type="text"/>	?

Digital IO->Digital Output

Enable

Check this box to enable digital output function.

Alarm Source

Select from "Digital Input1", "Digital Input2" or "SMS", Digital output triggers the related action when there is alarm comes from Digital Input or SMS.

Alarm ON Action

Select from "High", "Low" or "Pulse". High means high electrical level output. Low means low electrical level output. Pulse will generate a square wave as specified in the pulse mode parameters when triggered.

Alarm OFF Action

Initiates when alarm disappeared. Select from "High", "Low" or "Pulse". High means high electrical level output. Low means low electrical level output. Pulse will generate a square wave as specified in the pulse mode parameters when triggered.

Pulse Width

This parameter is available when select "Pulse" as "Alarm ON Action/Alarm OFF Action". The selected digital output channel will generate a square wave as specified in the pulse mode parameters.

4.5. Network

4.5.1 Firewall

Firewall rules are security rule-sets to implement control over users, applications or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement.

The screenshot shows a configuration menu with tabs for ACL, Port Mapping, DMZ, NAT, and URL Filter. The ACL tab is active. Under 'General Settings', the 'Default Policy' is set to 'Accept'. Below this is the 'ACL Rule Settings' section, which contains a table with columns: Index, Description, Chain, Protocol, Source Address, Source Port, Destination Address, and Destination Port. A plus sign icon is visible at the end of the table header.

Firewall->ACL

Default Policy

Select the “Accept” or “Drop” from the list, the packets which are not included in the access control list will be processed by the default filter policy.

An access control list (ACL), with respect to a [computer file system](#), is a list of [permissions](#) attached to an [object](#). An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

The screenshot shows the 'ACL Settings' window with the 'ACL Rule Settings' section expanded. It contains the following fields: 'Index' (text input with '1'), 'Description' (text input), 'Chain' (dropdown menu with 'FORWARD'), 'Protocol' (dropdown menu with 'All'), 'Source Address' (text input with a help icon), and 'Destination Address' (text input with a help icon). At the bottom right are 'Save' and 'Close' buttons.

Firewall->ACL

Description

Add a description for this rule.

Chain

Specify the forward rule of ACL, choose from "FORWARD" and "INPUT".

Protocol

All: Any protocol number.

TCP: The TCP protocol.

UDP: The UDP protocol.

TCP & DUP: both TCP and UDP protocol

ICMP: The ICMP protocol.

Source Address

A specific host IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).

Destination Address

A specific IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).

Port Mapping Settings

Port Mapping Rule Settings

Index	<input style="width: 95%;" type="text" value="1"/>	
Description	<input style="width: 95%;" type="text"/>	
Protocol	<input style="width: 95%;" type="text" value="All"/> ?	
Remote Address	<input style="width: 95%;" type="text"/>	?
Remote Port	<input style="width: 95%;" type="text"/>	?
Local Address	<input style="width: 95%;" type="text"/>	
Local Port	<input style="width: 95%;" type="text"/>	?

Firewall->Port Mapping

Description

Add a description for this rule.

Protocol

All: Any protocol number.

TCP: The TCP protocol.

UDP: The UDP protocol.

Remote Address

Enter a WAN IP address that is allowed to access the unit.

Remote Port

Enter the external port number range for incoming requests.

Local Address

Sets the LAN address of a device connected to one of the Fusion's LAN interfaces. Inbound requests will be forwarded to this IP address.

Local Port

Sets the LAN port number range used when forwarding to the destination IP address.

ACL Port Mapping **DMZ** NAT URL Filter

General Settings

Enable

Remote Address ?

DMZ Host Address

Firewall->DMZ

Enable

Check this box to enable DMZ function.

Remote Address

Optionally restricts DMZ access to only the specified WAN IP address.

NOTE: If set to 0.0.0.0/0, the DMZ is open to all incoming WAN IP addresses.

DMZ Host Address

The WAN IP address which has all ports exposed except ports defined in the Port Forwarding configuration.

1-1 NAT Settings

1-1 NAT Settings

Index

Description

Interface Address

Host Address

Interface To Host

Firewall->NAT

Description

Enter a description of 1-to-1 NAT setting.

Interface Address

Specify the interface address that need to be accessed before NAT.

Host Address

Specify the host address that need to be accessed after NAT.

Interface To Address

Specify the interface that connected to host, like lan0, lan1, lan2, lan3.

URL Filter Settings

URL Filter Settings

Index

URL

Firewall->URL Filter

URL

Enter the URL to block the data traffic to go to the website. For example, www.google.com

4.5.2 Route

Static Routing refers to a manual method of setting up routing between networks. Select the Static Routing tab to add static routes to the Static Route Table.

Please refer current route table as below.

Status		Static Route			
Route Table Information					
Index	Destination	Netmask	Gateway	Metric	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	0	lan0
2	192.168.9.0	255.255.255.0	0.0.0.0	0	lan0

Route->Route Table Information

Destination

Displays the destination of routing traffic.

Netmask

Displays the subnet mask of this routing.

Gateway

Displays the gateway of this interface. This is used for routing packets to remote networks.

Metric

Displays the metric value of this interface.

Interface

Displays the outbound interface of this route.

Static Route Settings

Static Route Settings

Index	<input type="text" value="1"/>
Description	<input type="text"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
Metric	<input type="text" value="0"/> ?
Interface	<input type="text"/> ?

Route->Static Route Settings

Description

Enter the description of current static route rule.

IP Address

Enter the IP address of the destination network.

Netmask

Enter the subnet mask of the destination network.

Gateway

Enter the IP address of the local gateway.

Metric

Enter the metric value of current static route rule. The smaller value, the higher priority.

Interface

Please refer to the Network->Route->Status interface.

4.5.3 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup. If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.

VRRP Network Settings	
Index	1
Enable	<input checked="" type="checkbox"/>
Interface	LAN0
Virtual Router ID	1
Authentication Type	None
Priority	100
Interval	1
Virtual IP Address	

Network->VRRP

Enable

Check this box will enable VRRP.

Interface

Select the interface of Virtual Router.

Virtual Router ID

User-defined Virtual Router ID. Range: 1-255.

Authentication Type

Select the authentication type for VRRP.

Priority

Enter the VRRP priority range is 1-254 (a bigger number indicates a higher priority).

Interval

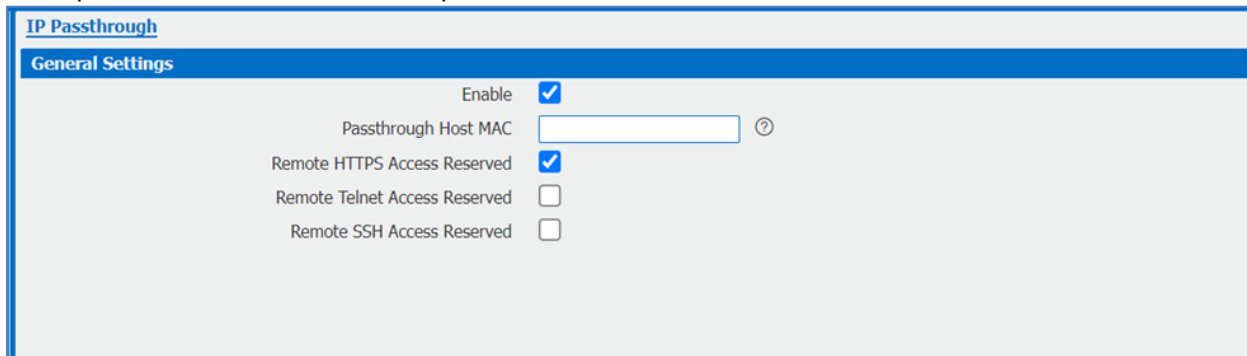
Heartbeat package transmission time interval between routers in the virtual IP group. Range: 1-255.

Virtual IP Address

Enter the virtual IP address of virtual gateway.

4.5.4 IP Passthrough

IP Passthrough mode disables NAT and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of [Network Address Translation](#) (NAT) in order to make the router "transparent" in the communication process.



The screenshot shows the 'IP Passthrough' configuration page. At the top, there is a blue header with the text 'IP Passthrough' and 'General Settings'. Below the header, there are four settings:

- Enable**: A checkbox that is checked.
- Passthrough Host MAC**: A text input field with a help icon (a circle with a question mark) to its right.
- Remote HTTPS Access Reserved**: A checkbox that is checked.
- Remote Telnet Access Reserved**: An unchecked checkbox.
- Remote SSH Access Reserved**: An unchecked checkbox.

Network->IP Passthrough

Enable

Check this box will enable IP Passthrough.

Passthrough Host MAC

Enter the MAC of passthrough host to receive the WAN IP address.

Remote HTTPS Access Reserved

Check this box to allow to remote access the router via https while enable IP Passthrough mode.

Remote Telnet Access Reserved

Check this box to allow to remote telnet to the router while enable IP Passthrough mode.

Remote SSH Access Reserved

Check this box to allow to remote SSH to the router while enable IP Passthrough mode.

4.6. Applications

4.6.1 DDNS

DDNS is a system that allows the domain name data of a computer with a varying (dynamic) IP addresses held in a name server to be updated in real time in order to make it possible to establish connections to that machine without the need to track the actual IP addresses at all times. A number of providers offer Dynamic DNS services (DDNS), free or for a charge.

You could review the status of DDNS as below.

The screenshot displays the DDNS configuration page. At the top, there are tabs for 'Status' and 'DDNS'. Below this is a 'DDNS Status' table with columns for Index, Status, Hostname, and Public IP Address. The table contains one entry with Index 1, Status 'Updating', and Hostname 'elpromqtt2.ddns.net'. Below the table is a 'DDNS Settings' dialog box. The dialog has a title bar 'DDNS Settings' and contains the following fields: Index (text input with value 2), Enable (checkbox checked), Provider (dropdown menu with 'no-ip' selected), Hostname (text input), Enable SSL (checkbox checked), Username (text input), and Password (text input). At the bottom of the dialog are 'Save' and 'Close' buttons.

DDNS

Status

Display the DDNS status.

Hostname

Display the hostname of DDNS.

Public IP Address

Display the public IP address.

Check IP Interval

Enter the interval, the modem will update the Dynamic DNS server of its carrier assigned IP address.

Log Level

Select the log output level from "none", "Error", "Notice", "Info" and "Debug".

Enable

Check this box to enable the DDNS service.

Provider

Select the DDNS provider from the list, options from "DynDNS", "no-ip", "3322" and custom.

DDNS Server

The internet address to communicate the Dynamic DNS information to. This option is available after you select custom on DDNS Provider.

DDNS Path

DDNS path for custom type.

Check IP Server

Check IP Server for custom type

Check IP Path

Check IP Path for custom type.

Enable SSL

Enable SSL for connection.

Username

Enter the username used when setting up the account. Used to login to the Dynamic DNS service.

Password

Enter the password associated with the account.

Hostname

Enter the hostname associated with the account.

4.6.2 SMS

SMS allows user to send the SMS to control the router or get the running status of the router.

The screenshot shows the configuration page for SMS Gateway. At the top, there are tabs for 'SMS', 'Gateway', and 'Notification'. The 'SMS' tab is active. Under 'General Settings', there are three options: 'Enable' (checked), 'Enable SMS Control' (checked), and 'Authentication Type' (set to 'Password'). Below this is a table for 'Allow Phone Book' with columns for 'Index', 'Description', and 'Phone Number'. A 'Phone Number Settings' dialog is open, showing 'Allow Phone Book' with input fields for 'Index' (1), 'Description', and 'Phone Number', and 'Save' and 'Close' buttons.

Application->SMS

Enable

Check this box to enable SMS feature.

Enable SMS Control

Check this box to enable SMS control feature.

Authentication Type

Specify the authentication mode for SMS, optional for “None” and “Password”.

Description

Enter the description of the Phone Book

Phone Number

Enter the special phone number and only allow this phone number to send SMS to the router

SMS Gateway allow to send SMS messages by using a valid syntax from serial device or ethernet device.

The screenshot shows the configuration page for SMS Gateway. At the top, there are tabs for 'SMS', 'Gateway', and 'Notification'. The 'Gateway' tab is active. Under 'General Settings', there are three options: 'Enable' (unchecked), 'Authentication Type' (set to 'Password'), and 'SMS Source' (set to 'Serial Port'). Below this is the 'Serial Port Settings' section with dropdown menus for 'Serial Port' (COM1), 'Baud Rate' (115200), 'Data Bits' (8), 'Stop Bits' (1), and 'Parity' (None).

Application->SMS>Gateway

Enable

Check the box will enable SMS gateway.

Authentication Type

Specify the authentication mode for SMS, optional for "None" and "Password".

SMS Source

Specify SMS source to receive valid syntax, optional for "Serial Port" and "HTTP(S) GET/POST".

SMS Message Format

Specify the SMS format between "Text" and "PDU" when reading SMS or reading SMS list via "HTTP(S) GET/POST"

Serial Port

Select the serial port from COM1 or COM2.

Baud Rate

Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.

Data Bits

Select the values from 7 or 8.

Stop Bits

Select the values from 1 or 2.

Parity

Select values from none, even, odd, mark, space.

SMS Notification feature allow to send SMS notification to the pre-setting phone number when some of router status changed.

The screenshot shows a configuration window with two sections. The top section, titled "Notification Settings", includes fields for "Index" (set to 1), "Enable" (checked), "Description", "Phone Number", and "Enable Timestamp" (checked). The bottom section, titled "Status Notify Settings", lists various system events with checkboxes: Startup, Reboot, NTP Update, LAN Port, WAN Port, WWAN Port, Active Link, Digital Input, Digital Output, IPSec Connection, Openvpn Connection, and Modbus Alarm. At the bottom right of the window are "Save" and "Close" buttons.

Application->SMS>Notification**Index**

Display the index of the notification channel, maximum is 10.

Description

Add the description for notification channel.

Phone Number

Pre-setting phone number to receive the notification

Timestamp

Check this box to enable timestamp on the SMS notify.

Startup

Send SMS notification to the pre-setting phone number when system startup.

Reboot

Send SMS notification to the pre-setting phone number when system reboot.

NTP Update

Send SMS notification to the pre-setting phone number when NTP update successfully.

LAN Port Status

Send SMS notification to the pre-setting phone number when LAN port status changed.

WAN Port Status

Send SMS notification to the pre-setting phone number when WAN port status changed.

WWAN Port

Send SMS notification to the pre-setting phone number when WWAN port status changed.

Active Link

Send SMS notification to the pre-setting phone number when active link status changed.

Digital Input

Send SMS notification to the pre-setting phone number when DI status changed.

Digital Output

Send SMS notification to the pre-setting phone number when DO status changed.

IPSec Connection

Send SMS notification to the pre-setting phone number when IPSec connection status changed.

OpenVPN Connection

Send SMS notification to the pre-setting phone number when OpenVPN Connection Status changed.

Modbus Alarm

Send SMS notification to pre-setting phone number when trigger Modbus alarm.

4.6.3 Email Notifications

Email notification application allows the 641M to be able to send email based on configured events in the device such as Startup, Reboot, Digital I/O, VPN status or Modbus Alarm.

Email Notification

Email Settings

Enable

Enable TLS/SSL

Enable STARTTLS

SMTP Host

Port ?

Username

Password

From

TLS Connect Timeout ?

Enable Verbose Log

Notification List

Index	Enable	Addressee	Subject
+			

Application->Email Notification

Enable

Check this box to enable Email Notification feature.

Enable TLS/SSL

Check this box to enable TLS/SSL.

Enable STARTTLS

Check this box to enable STARTLS.

SMTP Host

Mail server host address to connect for sending email.

Port

Mail server host port.

Username

Email exchange server login username

Password

Email exchange server login password

From

Sending email address.

TLS Connect Timeout

Connection timeout configuration for TLS/SSL connections.

Enable Verbose Log

Checkbox to enable detailed logging in system log.

Notification Settings

Index

Enable

Addressee

Subject

Enable Timestamp

Status Notify Settings

Startup

Reboot

NTP Update

LAN Port

WAN Port

WWAN Port

Active Link

Digital Input

Digital Output

IPSec Connection

Openvpn Connection

Modbus Alarm

4.6.4 Modbus Slave

This application allows the 641M to function as a Modbus TCP/IP or RTU slave device. The Modbus slave can be accessed externally from a Ethernet or serial connected master or using the 641M Modbus master software function.

Status		Modbus Slave	
Modbus Slave Status			
Enable	True	Protocol	TCP Server
Connection Status	Connected		
DI Status			
Index	Logic Level		
1	Low		
2	High		
DO Status			
Index	Logic Level	Pulse Width	
1	Low		
2	Low		
Status		Modbus Slave	
General Settings			
Enable	<input checked="" type="checkbox"/>	Protocol	TCP/IP
Slave ID	10	Enable Verbose Log	<input type="checkbox"/>
TCP Settings			
Local IP	192.168.1.1	Local Port	502

Application->Modbus Slave

Enable

Check this box to enable Modbus Slave feature.

Protocol

Select either TCP/IP or RTU protocol.

Slave ID

Configuration of the Modbus slave ID of the device.

Enable Verbose Log

Check to enable detailed function logging in system log file.

Local IP

IP address used for slave device.

Local Port

IP Port used for slave device.

Status	Modbus Slave
General Settings	
Enable	<input checked="" type="checkbox"/>
Protocol	RTU
Slave ID	10
Enable Verbose Log	<input type="checkbox"/>
COM Settings	
COM type	RS485
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
DO Trigger Event Content	
DO 1 High Level	true ?
DO 1 Low Level	false ?
DO 1 Pulse	?
DO 2 High Level	ON ?
DO 2 Low Level	OFF ?
DO 2 Pulse	?

Modbus RTU Settings

COM type

Connected to Modbus master through either RS-485 or RS-232 port.

Baud Rate

Select serial data rate, 300 to 115200 baud.

Data Bits

Number of data bits to transmit, set to 8 only.

Stop Bits

Number of stop bits to transmit, set to 1 or 2.

Parity

Data byte parity, set to None, Odd, Even, Mark, Space

DO 1 High Level

Value to be used for digital output high level. See note below.

DO 1 Low Level

Value to be used for digital output low level. See note below.

DO 1 Pulse

Value to be used for digital output pulse. See note below.

DO 1 High Level

Value to be used for digital output high level. See note below.

DO 1 Low Level

Value to be used for digital output low level. See note below.

DO 1 Pulse

Value to be used for digital output pulse. See note below.

The Trigger Event Content controls the values used for notifications with other applications for each of the configured states of the output. This is a text field that can be used for simple text or expressions. There is several internal field values available to be used to form this text output. Field values can be used singly or combined with other fields or text. These are listed below:

\$DI_INDEX, \$DATE, \$SERIAL_NUMBER, \$DEVICE_MODEL, \$FIRMWARE_VERSION, \$SYSTEM_UPTIME, \$LINK_TYPE, \$IP_ADDRESS, \$MODEM_MODEL, \$CSQ, \$OPERATOR, \$NETWORK_TYPE, \$IMEI, \$PLMN_ID, \$LOCAL_AREA_CODE, \$CELL_ID, \$IMSI, \$MODEM_FIRMWARE

4.6.5 Modbus Master

This application provides a Modbus Master feature to poll internal or external slave devices and collecting register values for applications to use when sending or receiving messages.

The Modbus master poll configuration is also used by other applications such as MQTT, Sparkplug and DNP3 as the source of register values. In each of these applications the Connection index is used as the reference.

Status
Modbus Poll
Modbus Alarm
Modbus Write

Channel Status

Index	Description	Connection Index	Type	Slave ID	Register Address	Function Code	Status	Value
1	Inputs	1	RS485	1	0	2	Reading	0, 0, 1, 0, 0, 0, 0...
2	115S#1 Diag	1	RS485	1	32	4	Read successfully	33056
3	Start	1	RS485	1	4	1	Read successfully	0, 0, 0, 0
4	PUMP#	3	RS485	2	0	2	Read successfully	1, 0, 0, 0
5	DI	2	TCP	10	13800	2	Read successfully	0, 1

Connection List

Index	Enable	Description	Scan Rate	Reconnect Interval	Connection Type	Baud Rate	Parity	Server Address	Server Port	
1	true	115S-12#1	1000	60	RS485	9600	None		502	
2	true	Local	100	100	TCP	9600	None	192.168.1.1	502	
3	true		30000	60	RS485	9600	None		502	

Connection Settings

Index:

Enable:

Description:

Scan Rate: ?

Response Timeout: ?

Delay Between Polls: ?

Connection Type:

Enable Show Status:

Enable Verbose Log:

Serial Settings

Baud Rate:

Parity:

Data Bits:

Stop Bits:

Channel List

Index	Enable	Description	Slave ID	Function Code	Register Address	
1	true	Inputs	1	02-Input-Status	0	
2	true	115S#1 Diag	1	04-Input-Registers	32	

Application->Modbus Slave

Enable

Check this box to enable Modbus master poll.

Description

Descriptive name used as a reference for poll.

Scan Rate

Rate at with scan or poll occurs in milli-seconds.

Response Timeout

Timeout used if there is not a response received from the slave in milliseconds.

Delay Between Polls

Delay time to wait between sending poll messages in milliseconds.

Connection Type

RS-232, RS485 or TCP.

Enable Show Status

Show on status page.

Enable Verbose Log

Check to enable detailed function logging in system log file.

Baud Rate

Select serial data rate, 300 to 115200 baud.

Data Bits

Number of data bits to transmit, set to 8 only.

Stop Bits

Number of stop bits to transmit, set to 1 or 2.

Parity

Data byte parity, set to None, Odd, Even, Mark, Space.

Channel Settings

Channel List

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text" value="Inputs"/>
Slave ID	<input type="text" value="1"/>
Function Code	<input type="text" value="02-Input-Status"/>
Register Address	<input type="text" value="0"/>
Data type	<input type="text" value="Bool"/>
Multiple Register	<input checked="" type="checkbox"/>
Quantity	<input type="text" value="8"/>

Enable

Check this box to enable this channel.

Description

Enter descriptive text for channel.

Slave ID

Polled slave ID address to be used for poll.

Function Code

Modbus function code to use to reference register.

Register Address

Modbus register to use for poll.

Data type

Data type to use for value. Bool for Coils and Inputs. Uint16, Int16, Uint32, Int32, Float or Double64 other 16 bit and 32 bits register types. Type must match register references to avoid poll error.

Multiple Register

Check if a block of multiple registers to be polled.

Quantity

Number of registers to poll.

Status Modbus Poll <u>Modbus Alarm</u> Modbus Write									
Channel List									
Index	Enable	Description	Alarm Mode	Connection Index	Filter Items	Channel Index	Slave ID	Register Address	
+									

Channel Alarm Settings

Channel List

Index	<input type="text" value="1"/>									
Enable	<input checked="" type="checkbox"/>	Description	<input type="text"/>	Alarm Mode	<input type="text" value="Normal"/> ▼		?	Connection Index	<input type="text" value="1"/> ▼	?
		Filter Items	<input type="text" value="Channel Index"/> ▼	Channel Index	<input type="text" value="1"/>		?	Logical Operation Type	<input type="text" value="Logical AND"/> ▼	?

Contrast Rule List

Index	Enable	Description	Contrast Type	Threshold	
+					

Trigger Alarm List

Index	Enable	Trigger Alarm Type	Phonenum	
+				

Enable

Check this box to enable.

Description

Enter descriptive text for channel.

Alarm Mode

Configure alarm mode for Normal, Continuous or Every operation.

Connection Index

Connection Index to link Alarm

Filter Items

Apply filter to alarm using Channel Index, Slave ID or Register Address.

Channel Index

Channel on configured connection or use or leave empty for all channels.

Logical Operation Type

Apply a logical AND or OR to the rules.

Contrast Rule List

Index

Enable

Description

Contrast Type

Threshold

Application->Modbus Slave

Enable

Check this box to enable Rule.

Description

Description text for rule.

Contrast Type

Operand to use for rule: <, >, <=, >=, !=, !, |, &, ^

Threshold

Value to use.

Trigger Alarm Settings

Trigger Alarm List

Index

Enable

Trigger Alarm Type ?

Application->Modbus Master

Enable

Check this box to enable.

Trigger Alarm Type

Select the output type to use for this alarm. Digital Output1, Digital Output2, Event Notification, SMS.

Status	Modbus Poll	Modbus Alarm	Modbus Write
General Settings			
Connection Index	<input type="text" value="1"/>		
Slave ID	<input type="text" value="1"/>		?
Function Code	<input type="text" value="06-Write-Single-Register"/>		
Register Address	<input type="text" value="0"/>		?
Data Endian	<input type="text" value="AB"/>		
Value	<input type="text" value="0"/>		

Application->Modbus Master-> Modbus Write

Slave ID

Slave ID to use for write command.

Function Code

Modbus Function Code to use for register.

Register Address

Register Address to use.

Data Endian

Endian conversion to make byte order correct.

4.6.6 Modbus Transport

Internal Modbus transport that uses connections to the master or slave application applications or protocols. The Modbus Transport application is included when installing the Modbus Master software application.

This can be used to collect Modbus register values for TCP Client, MQTT, FTP, Google Cloud and SparkplugB.

Status Modbus Transport X.509 Certificate								
Connection List								
Index	Enable	Description	Protocol	Server Address	Server Port	Reconnect Interval	Data Format	
1	true	AWS	MQTT	• a6h2rqek0on7b...	1883	60	\$DATE,\$CHANNEL_...	

Connection Settings

Connection List

Index

Enable

Description

Protocol TCP-Client ▾

Server Address

Server Port

Reconnect Interval ?

Connection Timeout ?

Enable Verbose Log

Transport Data Settings

Data Location NULL ▾ ?

Data Format ?

Line Break

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address	
<div style="display: flex; justify-content: flex-end; gap: 10px;"> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Save</div> <div style="background-color: #0070c0; color: white; padding: 5px 15px; border-radius: 3px;">Close</div> </div>							

Application->Modbus Transport

Enable

Check this box to enable Modbus Slave feature.

Description

Description text for channel.

Protocol

Configure for TCP Client, MQTT, FTP or Google Cloud.

Connection List							
Index	<input type="text" value="2"/>						
Enable	<input checked="" type="checkbox"/>						
Description	<input type="text"/>						
Protocol	TCP-Client <input type="button" value="v"/>						
Server Address	<input type="text"/>						
Server Port	<input type="text" value="20100"/>						
Reconnect Interval	<input type="text" value="60"/> <input type="button" value="?"/>						
Connection Timeout	<input type="text" value="10"/> <input type="button" value="?"/>						
Enable Verbose Log	<input type="checkbox"/>						
Transport Data Settings							
Data Location	NULL <input type="button" value="v"/> <input type="button" value="?"/>						
Data Format	\$SERIAL_NUMBER,\$DATE,\$S <input type="button" value="?"/>						
Line Break	<input checked="" type="checkbox"/>						
Modbus Channel							
Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address	<input type="button" value="+"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>							

Application->Modbus Transport->TCP Client

Server Address

TCP server IP or Domain Name.

Server Port

TCP server port.

Reconnect Interval

FTP reconnect interval in seconds.

Connection Timeout

FTP connection timeout in seconds.

Enable Verbose Log

Enable detailed logging for system log file.

Data Location

NULL, RAM or Flash configurable allows short term storage of data if connection is down.

Data Format

String that configures the data format for transmitted data on this connection.

Line Break

Check to enable line break to be send after data is transmitted.

Connection List	
Index	<input type="text" value="2"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Protocol	<input type="text" value="MQTT"/>
Server Address	<input type="text"/>
Server Port	<input type="text" value="20100"/>
Enable SSL	<input type="checkbox"/>
Username	<input type="text"/>
Password	<input type="text"/>
Client ID	<input type="text"/> ?
Subscribe Topic	<input type="text"/> ?
Keepalive	<input type="text" value="60"/> ?
Reconnect Interval	<input type="text" value="60"/> ?
Connection Timeout	<input type="text" value="10"/> ?
Enable LWT	<input type="checkbox"/>
Enable Verbose Log	<input type="checkbox"/>

Application->Modbus Transport->TCP Client

Server Address

TCP server IP or Domain Name.

Server Port

TCP server port.

Enable SSL

Check to enable SSL with TLS. Note that certificate needs parameters will need to be configured.

Username

Broker connection username.

Password

Broker connection password.

Client ID

Client ID to use for broker connection. May be empty.

Subscribe Topic

Subscribe topic to use for writing output data.

Keepalive

TCP or TLS keep alive time for connection to broker.

Reconnect Interval

FTP reconnect interval in seconds.

Connection Timeout

FTP connection timeout in seconds.

Enable LWT

Enable Last Will and Testament. If enabled, then LWT Topic and Payload can be entered.

Enable Verbose Log

Enable detailed logging for system log file.

Data Location

NULL, RAM or Flash configurable allows short term storage of data if connection is down.

Data Format

String that configures the data format for transmitted data on this connection.

Line Break

Check to enable line break to be send after data is transmitted.

Connection List	
Index	<input type="text" value="2"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Protocol	<input type="text" value="FTP"/>
Server Address	<input type="text"/>
Server Port	<input type="text" value="20100"/>
Username	<input type="text"/>
Password	<input type="text"/>
Connection Timeout	<input type="text" value="10"/> ?
Try To Send	<input type="text" value="3"/> ?
Enable Verbose Log	<input type="checkbox"/>

Transport Data Settings	
Data Location	<input type="text" value="NULL"/> ?
Add CSV File Title	<input checked="" type="checkbox"/>
File Name	<input type="text" value="\$SERIAL_NUMBER_\$DATE.cs"/> ?
Upload Interval	<input type="text" value="30"/> ?
Data Format	<input type="text" value="\$SERIAL_NUMBER,\$DATE,\$S"/> ?

Application->Modbus Transport->FTP

Server Address

FTP server IP or Domain Name.

Server Port

FTP server port.

Username

Server connection username.

Password

Server connection password.

Connection Timeout

FTP connection timeout in seconds.

Try to Send

Number of times to resend connection request on failure to connect.

Enable Verbose Log

Enable detailed logging for system log file.

Data Location

NULL, RAM or Flash configurable allows short term storage of data if connection is down.

Add CSV File Title

Include title in CSV file

File Name

String configuration of file number. \$ expressions can be used for internal values.

Upload Interval

Time interval to send the FTP file in seconds. 1- 86400 seconds.

Data Format

Format of data to send in FTP file. \$ expressions can be used for internal values.

Connection List

Index	<input type="text" value="2"/>	
Enable	<input checked="" type="checkbox"/>	
Description	<input type="text"/>	
Protocol	<input type="text" value="Google Cloud"/>	▼
Server Address	<input type="text"/>	
Server Port	<input type="text" value="20100"/>	
Project ID	<input type="text"/>	
Region	<input type="text" value="us-central1"/>	▼
Registry ID	<input type="text"/>	
Device ID	<input type="text"/>	
Algorithm	<input type="text" value="RS256"/>	▼
Subscribe Topic	<input type="text"/>	?
Keepalive	<input type="text" value="60"/>	?
Reconnect Interval	<input type="text" value="60"/>	?
Connection Timeout	<input type="text" value="10"/>	?
Enable Verbose Log	<input type="checkbox"/>	

Transport Data Settings

Data Location	<input type="text" value="NULL"/>	?
Data Format	<input type="text" value="\$SERIAL_NUMBER,\$DATE,\$S"/>	?
Line Break	<input checked="" type="checkbox"/>	

Application->Modbus Transport->Google Cloud

Server Address

FTP server IP or Domain Name.

Server Port

FTP server port.

Project ID

Google Cloud project ID to connect.

Region

Google Cloud server region to connect.

Registry ID

Device registry ID configuration.

Device ID

Device ID configuration, must be unique.

Algorithm

Signature algorithm to use for token, RS256 or HS256.

Subscribe Topic

Topic to use to send Modbus data.

Keepalive

Google cloud connection keepalive time in seconds, 1- 86400.

Reconnect Interval

Connection reconnect time in seconds, 1-600.

Connection Timeout

Connection timeout in seconds.

Try to Send

Number of times to resend connection request on failure to connect.

Enable Verbose Log

Enable detailed logging for system log file.

Data Location

NULL, RAM or Flash configurable allows short term storage of data if connection is down.

Data Format

String that configures the data format for transmitted data on this connection.

Line Break

Check to enable line break to be send after data is transmitted.

Application->Modbus Transport->Channel Settings

Enable

Check this box to enable channel.

Connection Index

Modbus channel connection index to use for this link.

Filter Items

Filter Modbus connection by Channel Index, Slave ID or Register Address.

Channel Index

Channel index to listen on for Modbus data. If empty then listen on all channels.

4.6.7 Schedule Reboot

Schedule reboot allows user to define the time for router reboot itself.

Enable

Check this box to enable schedule reboot feature.

Time to Reboot

Enter the time of each day to reboot device. Format: HH(00-23):MM(00-59).

Day to Reboot

Enter the day of each month to reboot device. 0 means every day.

4.6.8 GPS

GPS (Global Positioning System) is a high-precision radio navigation positioning system based on satellites. It can provide the accurate positioning, speed measurement and high precision standard time.

Status

Displays current GPS status.

Satellites Visible

Displays the number of the visible satellites.

Satellites Used

Displays the number of the visible satellites in using.

Latitude

Displays the latitude of GPS.

Longitude

Display the longitude of GPS.

Altitude

Display the altitude of GPS.

Horizontal speed

Display the horizontal speed of GPS.

Status (Channel)

Display the transmission protocol of the channel.

Remote Address

Display the remote IP address of the channel.

Remote Port

Display the remote port of the channel.

Status (Channel)

Display the status of the channel.

Status GPS

General Settings

Enable

Enable A-GPS

Channel Settings

Report Channel Settings

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Report GSV	<input checked="" type="checkbox"/>
Report GGA	<input checked="" type="checkbox"/>
Report VTG	<input checked="" type="checkbox"/>
Report RMC	<input checked="" type="checkbox"/>
Report GSA	<input checked="" type="checkbox"/>
Report Interval	<input type="text" value="5"/>
NMEA Prefix	<input type="text"/> ?
Protocol	<input type="text" value="TCP Client"/>
Remote Address	<input type="text"/>
Remote Port	<input type="text" value="2000"/>

Application->GPS->GPS

Enable

Check this box to enable GPS.

Enable A-GPS

Check this box to enable A-GPS (Assisted Global Positioning).

Description

Specify the description of the GPS transmission channel.

Report GSV

Check this box to enable to send the GPS data with GSV format.

Report GGA

Check this box to enable to send the GPS data with GGA format.

Report VTG

Check this box to enable to send the GPS data with VTG format.

Report RMC

Check this box to enable to send the GPS data with RMC format.

Report GSA

Check this box to enable to send the GPS data with GSA format.

Report Interval

Specify the interval time to send the GPS data to remote server.

NMEA Prefix

Self-defined the GPS data prefix to send to remote server.

Protocol

Specify the transmission protocol of the channel.

Remote Address

Specify the remote IP address to receive the GPS data.

Remote Port

Specify the remote port to receive the GPS data.

4.6.9 Call

Call reboot allow the user to make a call to the router to control it restart.

[Call](#)

General Settings

Enable Call Control

Call Reboot

Allow Phone Book

Index	Description	Phone Number
+		

Phone Number Settings

Allow Phone Book

Index	1
Description	
Phone Number	

Save
Close

Application->Call

Enable Call Control

Check this box to enable call control feature.

Call Reboot

Check this box to enable call reboot feature.

Description

Define the description of the phone book

Phone Number

Specify the phone number that allow to make a call to the router.

4.7. VPN

4.7.1 OpenVPN

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

You could review all OpenVPN connection as below.

Status	OpenVPN	X.509 Certificate	Configuration Files			
OpenVPN Information						
Index	Enable	Description	Mode	Status	Uptime	Local Virtual IP
OpenVPN Server Status						
Index	Common Name	Status	Uptime	Remote Virtual IP	Remote IP	Remote Port

VPN->OpenVPN->Status>OpenVPN Information

Enable

Displays current OpenVPN settings is enable or disable.

Mode

Displays current working mode of OpenVPN.

Status

Displays the current VPN connection status.

Uptime

Displays the connection time since VPN is established.

Local Virtual IP

Displays the virtual IP address obtain from remote side.

VPN->OpenVPN->Status>OpenVPN Server Status

Common Name

Displays the common name of OpenVPN client.

Status

Displays the current VPN connection status.

Uptime

Displays the connection time since VPN is established.

Remote Virtual IP

Displays the virtual IP address of OpenVPN client.

Remote IP

Displays the remote IP address of OpenVPN client.

Remote Port

Displays the remote port obtain of OpenVPN client.

OpenVPN Settings

Index	<input type="text" value="1"/>	
Enable	<input checked="" type="checkbox"/>	
Description	<input type="text"/>	
Mode	<input type="text" value="Client"/>	▼
Protocol	<input type="text" value="UDP"/>	▼
Connection Type	<input type="text" value="TUN"/>	▼
Server Address	<input type="text"/>	
Server Port	<input type="text" value="1194"/>	
Authentication Method	<input type="text" value="X.509"/>	ⓘ
Encryption Type	<input type="text" value="BF-CBC"/>	▼
Renegotiate Interval	<input type="text" value="3600"/>	
Keepalive Interval	<input type="text" value="20"/>	
Keepalive Timeout	<input type="text" value="60"/>	ⓘ
Fragment	<input type="text" value="0"/>	ⓘ
Private Key Password	<input type="text"/>	
Output Verbosity Level	<input type="text" value="3"/>	

Advanced Settings

Enable NAT

VPN->OpenVPN

Enable

Check this box to enable OpenVPN tunnel.

Description

Enter a description for this OpenVPN tunnel.

Mode

Select from "P2P", "Client" or "Server".

Protocol

Select from "UDP", "TCP Client" or "TCP Server"

Connection Type

Select from "TUN", "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.

Server Address

Enter the IP address or domain of remote server.

Server Port

Enter the negotiate port on OpenVPN server.

Max Client

Allow max OpenVPN client connect to OpenVPN server.

Authentication Method

Select from "X.509", "Pre-shared", "Password", and "X.509 And Password".

Encryption Type

Select from "BF-CBC", "DES-CBC", "DES-EDE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".

Username

Enter the username for authentication when selection from "Password" or "X.509 And Password".

Password

Enter the password for authentication when selection from "Password" or "X.509 And Password".

Local IP Address

Enter the local virtual IP address when select "P2P" and "OpenVPN Server" mode.

Remote IP Address

Enter the remote virtual IP address when select "P2P" mode.

Local Port

Specify the OpenVPN Server port, default is 1194.

Topology

Select the possible topology from "Subnet" and "Net30"

Subnet: The recommended topology for modern servers. Note that this is not the current default. Addressing is done by IP & netmask.

Net30: This is the old topology for support with Windows clients running 2.0.9 or older clients. This is the default as of OpenVPN 2.3, but not recommended for current use. Each client is allocated a virtual /30, taking 4 IPs per client, plus 4 for the server.

Subnet

Specify the subnet for the OpenVPN client. Default is 10.8.0.0

Subnet Netmask

Specify the subnet netmask for OpenVPN client. Default is 255.255.255.0

TAP Bridge

Select the specified LAN that bridge with OpenVPN tunnel when select "TAP" connection type.

Renegotiate Interval

Enter the renegotiate interval if connection is failed.

Keepalive Interval

Enter the keepalive interval to check the tunnel is active or not.

Keepalive Timeout

Enter the keepalive timeout, once connection is failed it will trigger the OpenVPN reconnect.

Fragment

Enter the fragment size, 0 means disable.

Private Key Password

Enter the private key password for authentication when selection from "X.509" or "X.509 And Password".

Output Verbosity Level

Enter the level of the output log and values.

Advanced Settings

Enable NAT

Enable PKCS#12

Enable X.509 Attribute nsCertType

Enable HMAC Firewall

Enable Compression LZ0

Additional Configurations ?

Save Close

VPN->OpenVPN->Advanced Settings**Enable NAT**

Check this box to enable NAT, the source IP of host behind router will be disguised before accessing the remote end.

Enable Default Gateway

Check this box to enable default gateway, all the data traffic will go through the VPN tunnel.

Enable PKCS#12

It is an exchange of digital certificate encryption standard, used to describe personal identity information.

Enable CRL

Check this box to enable CRL(Certificate Revocation List).

Enable Client to Client

Check this box to allow client to communicate with each other.

Enable Duplicate CN

Check this box allow multiple clients connect to the server with the same certificate/key files or common names.

Enable IP Persist

Check this box to keep the IP address unchanged.

Enable X.509 Attribute nsCertType

Require that peer certificate was signed with an explicit nsCertType designation of "server".

Enable HMAC Firewall

Add additional layer of HMAC authentication on the top of the TLS control channel to protect against DoS attacks.

Enable Compression LZO

Compress the data.

Additional Configurations

Enter some other options of OpenVPN in this field. Each expression can be separated by a `;`.

Status	OpenVPN	X.509 Certificate	Configuration Files
X.509 Certificate Import			
OpenVPN Mode	Client <input type="button" value="v"/>		
Connection Index	1 <input type="button" value="v"/>		
CA Certificate	Choose File	No file chosen	<input type="button" value="📁"/>
Local Certificate File	Choose File	No file chosen	<input type="button" value="📁"/>
Local Private Key	Choose File	No file chosen	<input type="button" value="📁"/>
HMAC Firewall Key	Choose File	No file chosen	<input type="button" value="📁"/>
Pre-shared Key	Choose File	No file chosen	<input type="button" value="📁"/>
PKCS#12 Certificate	Choose File	No file chosen	<input type="button" value="📁"/>
User-Password File	Choose File	No file chosen	<input type="button" value="📁"/>
Private Key Password File	Choose File	No file chosen	<input type="button" value="📁"/>
X.509 Certificate Files			
Index	File Name	File Size	Date Modified

VPN->OpenVPN->X.509 Certificate**OpenVPN Mode**

Select OpenVPN working mode between Server and Client.

Connection Index

Displays the current connection index for OpenVPN channel.

CA Certificate

Import CA certificate file.

Local Certificate File

Import Local Certificate file.

Local Private Key

Import Local Private Key file.

DH File

Import DH file when works as OpenVPN server.

HMAC Firewall Key

Import HMAC Firewall Key file.

Pre-shared Key

Import the pre-shared key file.

PKCS#12 Certificate

Import PKCS#12 Certificate.

User-Password File

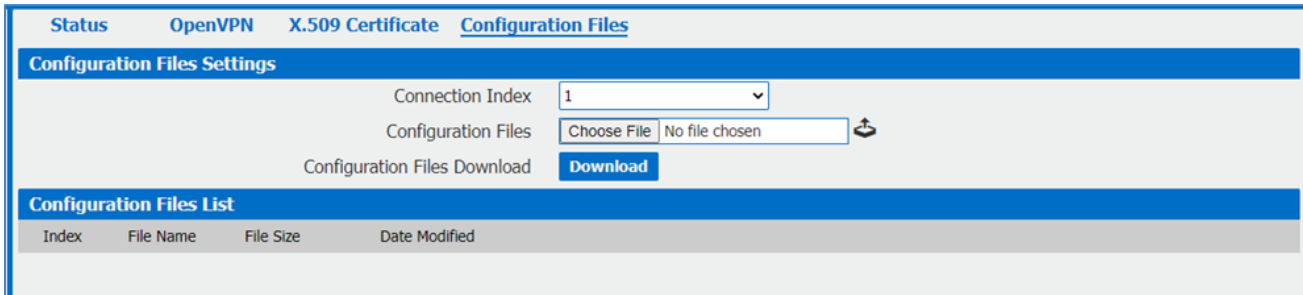
Import the username and password file when import the OpenVPN client file.

Private Key Password File

Import the private key password file when import the OpenVPN client file.

CRL File

Import CRL file.



VPN->OpenVPN->Configuration Files

Connection Index

Select OpenVPN connection index.

Configuration Files

Import the OpenVPN client file.

Configuration Files Download

Download the OpenVPN client configuration.

Configuration Files List

Display the imported OpenVPN client file.

4.7.2 IPSec

IPSec facilitates configuration of secured communication tunnels. The various tunnel configurations will be displayed in the Tunnel Table at the bottom of the page. All tunnels are create using the ESP (Encapsulating Security Payload) protocol.

Status		IPSec		
IPSec Information				
Index	Enable	Description	Status	Uptime

VPN->IPSec->Status

Enable

Displays current IPSec settings is enable or disable.

Description

Displays the description of current VPN channel.

Status

Displays the current VPN connection status.

Uptime

Displays the connection time since VPN is established.

IPSec Settings	
Index	1
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Remote Gateway	<input type="text"/>
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Main
Authentication Method	Pre-shared Key
Local Subnet	<input type="text"/> ?
Local Pre-shared Key	<input type="text"/>
Local ID Type	IPv4 Address
Remote Subnet	<input type="text"/> ?
Remote ID Type	IPv4 Address

VPN->IPSec

Enable

Select Enable will launch the IPSec process.

Description

Enter a description for this IPSec VPN tunnel.

Remote Gateway

Enter the IP address of the remote endpoint of the tunnel.

IKE Version

Internet Key Exchange, select from “IKEv1” or “IKEv2”.

Connection Type

Select from “Tunnel” or “Transport”.

Tunnel: In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create [virtual private networks](#) for network-to-network communications.

Transport: In transport mode, only the payload of the IP packet is usually [encrypted](#) or authenticated. The routing is intact, since the IP header is neither modified nor encrypted.

Negotiation Mode

Select from “Main” or “Aggressive”.

Authentication Method

Select from “Pre-shared Key” or “Pre-shared Key and Xauth”.

Local Subnet

Enter the IP address with mask if a network beyond the local LAN will be sending packets through the tunnel. Multiple subnets separated by commas.

NOTE: The Remote subnet and Local subnet addresses must not overlap!

Local Pre-shared Key

Enter the pre-shared key which match the remote endpoint.

Local ID Type

The local endpoint's identification. The identifier can be a host name or an IP address.

Xauth Identity

Enter Xauth identity after “Pre-shared Key and Xauth” on authentication Method is enabled.

Xauth Password

Enter Xauth password “Pre-shared Key and Xauth” on authentication Method is enabled.

Remote Subnet

Enter an IP address with mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address. Multiple subnets separated by commas.

NOTE: The Remote subnet and Local subnet addresses must not overlap!

Remote ID Type

The authentication address of the remote endpoint.

IKE Proposal Settings		
Encryption Algorithm	AES-256	
Hash Algorithm	SHA2 256	
Diffie-Hellman Group	Group5(modp1536)	
Lifetime	1440	
ESP Proposal Settings		
Encryption Algorithm	AES-256	
Hash Algorithm	SHA2 256	
Diffie-Hellman Group	Group5(modp1536)	
Lifetime	60	
Advanced Settings		
DPD Interval	30	?
DPD Timeout	90	?
Additional Configurations		?
<input type="button" value="Save"/> <input type="button" value="Close"/>		

VPN->IPSec

- **Encryption Algorithm (IKE)**
Select 3DES AES-128, AES-192, or AES-256 encryption.
- **Hash Algorithm (IKE)**
Select from MD5, SHA1, SHA2 256, SHA2 384 or SHA2 512 hashing.
- **Diffie-Hellman Group (IKE)**
Negotiate (None) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) etc.
- **Lifetime (IKE)**
How long the keying channel of a connection should last before being renegotiated.
- **Encryption Algorithm (ESP)**
Select 3DES AES-128, AES-192, or AES-256 encryption.
- **Hash Algorithm (ESP)**
Select from MD5, SHA1, SHA2 256, SHA2 384 or SHA2 512 hashing.
- **Diffie-Hellman Group (ESP)**
Negotiate (None) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) etc.
- **Lifetime (ESP)**
How long a particular instance of a connection should last, from successful negotiation to expiry.
- **DPD Interval**
Enter the interval after which DPD is triggered if no IPsec protected packets is received from the peer.
- **DPD Timeout**
Enter the remote peer probe response timer.
- **Additional Configurations**
Enter some other options of IPsec in this field. Each expression can be separated by a ‘;’.

4.7.3 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends.

Status		GRE		
GRE Information				
Index	Enable	Description	Mode	Status

VPN->GRE->Status

- **Enable**
Displays current GRE settings is enable or disable.
- **Description**
Displays the description of current VPN channel.
- **Mode**
Displays the current VPN mode.
- **Status**
Displays the current VPN connection status.

GRE Settings

General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Mode	<input type="text" value="Layer 3"/>
Remote Gateway	<input type="text"/>
Local Virtual IP	<input type="text"/>
Local Virtual Netmask	<input type="text" value="255.255.255.252"/>
Tunnel key	<input type="text"/> ?
Enable NAT	<input type="checkbox"/>
Enable Default Route	<input type="checkbox"/>

Advanced Settings

Binding Interface	<input type="text"/> ?
-------------------	------------------------

VPN->GRE

- **Enable**
Check this box to enable GRE.
- **Description**
Enter the description of current VPN channel.
- **Mode**

Specify the running mode of GRE, optional are “Layer 2” and “Layer 3”.

- **Remote Gateway**
Enter the remote IP address of peer GRE tunnel.
- **Local Virtual IP**
Enter the local tunnel IP address of GRE tunnel.
- **Local Virtual Netmask**
Enter the local virtual netmask of GRE tunnel.
- **Tunnel Key**
Enter the authentication key of GRE tunnel.
- **Enable NAT**
Check this box to enable NAT function.
- **Bridge Interface**
Specify the bridge interface work with Layer 2 mode.
- **Enable Default Route**
Check this box to make all the traffic go through VPN tunnel.
- **Binding Interface**
Only specified interface turn into active WAN will start the VPN tunnel.

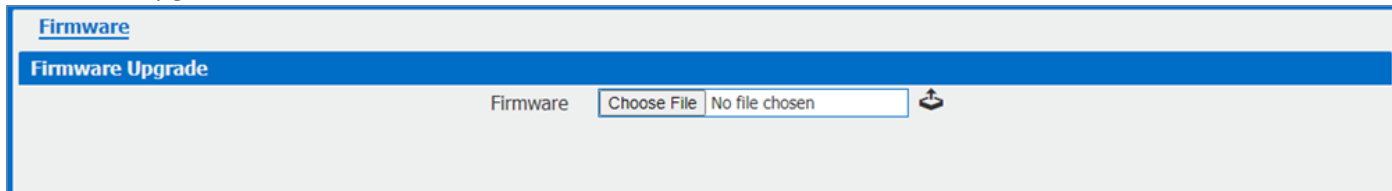
4.8. Maintenance

4.8.1 Upgrade

When newer versions of EL-641M-4 firmware become available, the user can manually update the unit by uploading a package to the unit.

NOTE: The unit need manually reboots once the upload completes, thus taking the EL-641M-4 router out of service during approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.

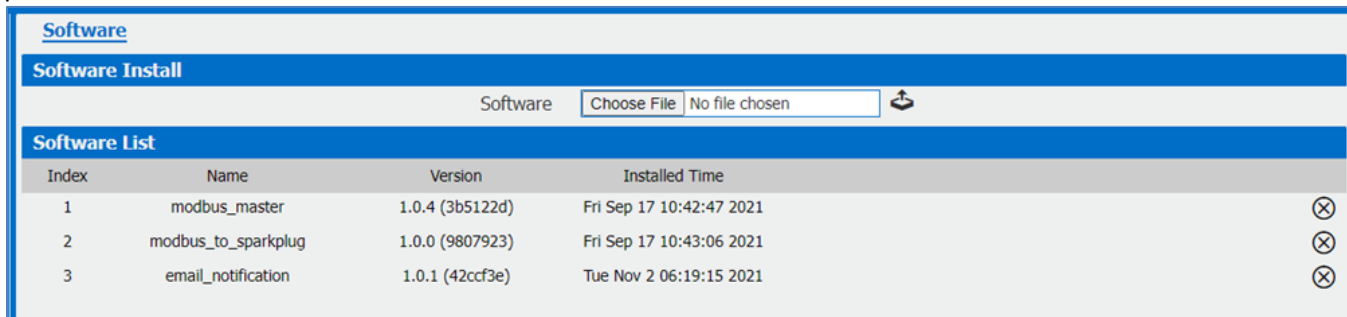
CAUTION: It is important to have a stable power source and ensure that power to the Fusion is not interrupted during a firmware upgrade.



4.8.2 Software

When release a new feature (APP Package) of EL-641M-4 router, the user can manually install to the unit by uploading a package. Or user can uninstall this feature (APP Package) from router.

NOTE: The unit need manually reboots once the upload/uninstall completes, thus taking the EL-641M-4 router out of service during approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.



Click  to upload the APP Package.

Click  to delete the APP Package.

Note: We are working different kinds of the APP Packages. Please contact us to get them in case of you would like to test.

4.8.3 System

This section allows you to review the device system settings.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
General Settings						
Hostname		<input type="text" value="elpro.router"/>				
User LED Type		<input type="text" value="None"/>				
Time Zone Settings						
Time Zone		<input type="text" value="UTC+08:00"/>				
Customized Time Zone		<input type="text"/> ?				
Time Synchronisation						
Enable		<input checked="" type="checkbox"/>				
Primary NTP Server		<input type="text" value="pool.ntp.org"/>				
Secondary NTP Server		<input type="text" value="1.pool.ntp.org"/>				
Synchronize Modem Time		<input type="checkbox"/>				
Enable NTP Server		<input type="checkbox"/>				
System->General						

- **Hostname**
User-defined router name, which might be use for IPSec local ID identify.
- **User LED Type**
Defined the User LED behavior.
- **Time Zone**
Select the zone where the device is in use.
- **Customized Time Zone**
Customized the zone where the device is in use.
- **Enable (NTP Client)**
Selected Enabled to utilize the NTP client to synchronize the device clock over the network using a time server (NTP server).
- **Primary NTP Server**
Enter the IP address (or host name) of the primary time server.
- **Secondary NTP Server**
Enter the IP address (or host name) of the secondary time server.
- **Synchronize Modem Time**
Synchronize the time from cellular module.
- **Enable NTP Server**
Check the box to make the router as a NTP server.

The screenshot shows the 'Accounts' configuration page. At the top, there are navigation tabs: General, Accounts (selected), Syslog, Web Server, Telnet, SSH, and Security. Below the tabs, there are two main sections: 'Account Settings' and 'Visitor Settings'. The 'Account Settings' section contains four input fields: 'Administrator' (with the value 'admin'), 'Old Password', 'New Password', and 'Confirm Password'. The 'Visitor Settings' section has a table with columns for 'Index', 'Username', and 'Password'. A plus sign icon is visible in the bottom right corner of the table area.

System->Account

- **Administrator**
Displays the name of current administrator, default as “admin”.
- **Old Password**
Enter the old password of administrator.
- **New Password**
Enter the new password of administrator.
- **Confirm Password**
Confirm the new password of administrator.

This screenshot shows the 'Account Settings' page with the 'Visitor Settings' section expanded. It contains three input fields: 'Index' (with the value '1'), 'Username', and 'Password'. At the bottom right of the section, there are two buttons: 'Save' and 'Close'.

System->Account



- **Username**
Enter a username of visitor privilege
- **Password**
Enter the new password of current visitor account.

Syslog displays system logs that are stored in the log buffers.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
General Settings						
		Log Location	RAM			
		Log Level	Debug			
Remote Syslog Settings						
		Enable Remote Syslog	<input type="checkbox"/>			
		Remote Syslog Server				
		Remote Syslog Port	514			

System->Syslog

- **Log Location**
Select the log store location from “RAM” or “Flash”.
- **Log Level**
Select the log output level from “Debug”, “Notice”, “Info”, “Warning” or “Error”.
- **Enable Remote Syslog**
Check this box to enable remote syslog connection.
- **Remote Syslog Server**
Enter the IP address of remote syslog server.
- **Remote Syslog Port**
Enter the port for remote syslog server listening.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
General Settings						
		HTTP Port	80			
		HTTPS Port	443			
Certificate Settings						
		Private Key	Choose File	No file chosen		
		Certificate File	Choose File	No file chosen		

System->Web Server

- **HTTP Port**
Enter the port for Hypertext Transfer Protocol. A well-known port for HTTP is port 80.
- **HTTPS Port**
Enter the port for HTTPS Protocol. A well-known port for HTTPS is port 443.
- **Private Key**
Import private Key file for HTTPS connection.
- **Certificate File**
Import certificate file for HTTPS connection.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
General Settings						
		Telnet Port	23			

System->Telnet

- **Telnet Port**

Enter the port for telnet access. A well-known port for HTTP is port 23.



- **System->SSH**

- **SSH Port**

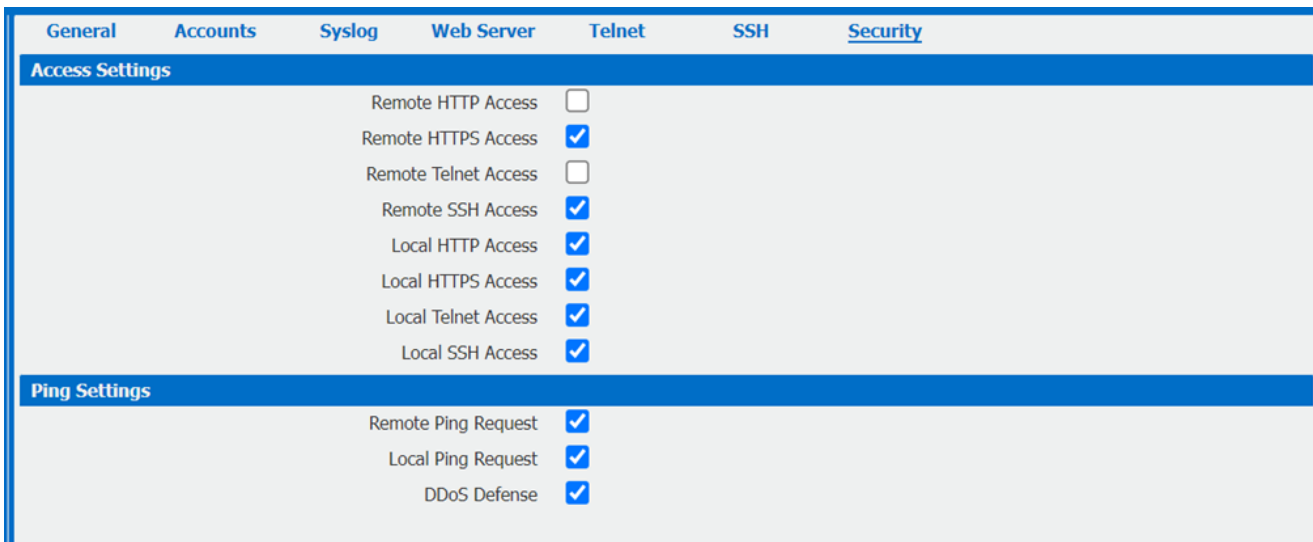
Enter the port for SSH access. A well-known port for HTTP is port 22.

- **Allow Password Authentication**

Check this box to enable SSH authentication.

- **Public Key**

Enter the public Key SSH authentication.



System->Security

- **Remote HTTP Access**

Check this box to allow remote HTTP access.

- **Remote HTTPS Access**

Check this box to allow remote HTTPS access.

- **Remote Telnet Access**

Check this box to allow remote Telnet access.

- **Remote SSH Access**

Check this box to allow remote SSH access.

- **Local HTTP Access**

Check this box to allow local HTTP access.

- **Local HTTPS Access**

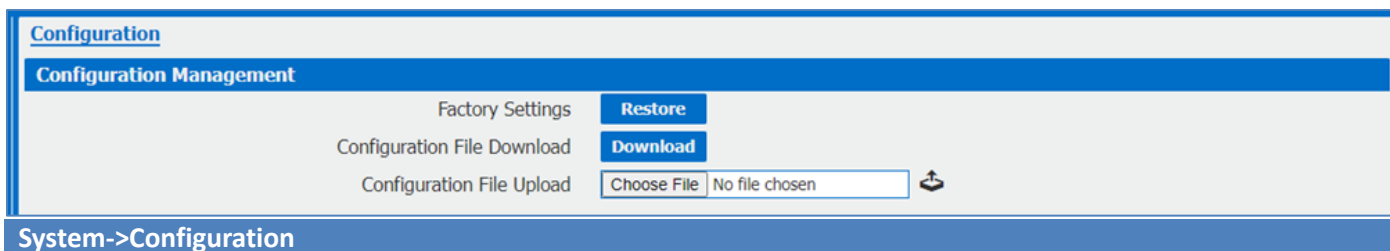
Check this box to allow local HTTPS access.

- **Local Telnet Access**

- Check this box to allow local Telnet access.
- **Local SSH Access**
Check this box to allow local SSH access.
- **Remote Ping Request**
Check this box to allow remote ping request.
- **Local Ping Request**
Check this box to allow local ping request.
- **DDoS Defense**
Check this box to enable DDoS defense.

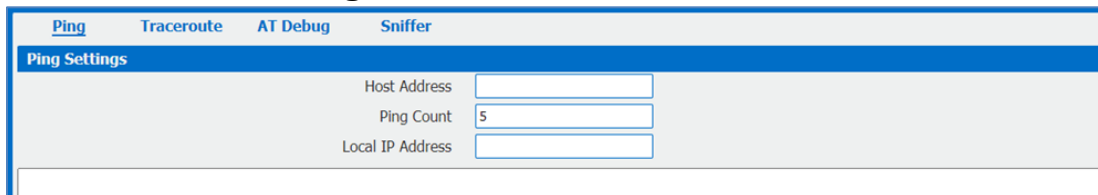
4.8.4 Configuration

The Unit Configuration tab allows you to save parameters (settings in the Web interface) to a file. Conversely, if you have saved settings from the EL-641M-4 router to a file, you can Import these previously-saved configuration settings to the EL-641M-4 router as well.

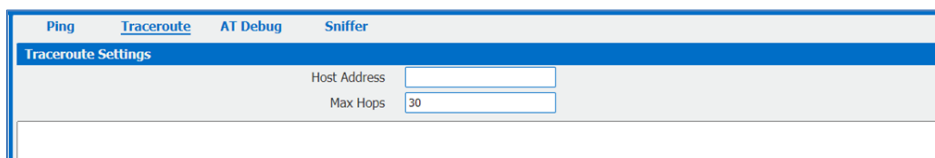


- **Restore**
Reset the unit to factory default settings.
- **Download**
Download the configuration file from EL-641M-4 router.
- **Configuration File Upload**
Import previously saved configuration file.

4.8.5 Debug Tools



- **Host Address**
Enter a host IP address or domain name for ping.
- **Ping Count**
Enter the ping times.
- **Local IP Address**
Enter the ping source IP address or leave it blank.



Debug Tools->Traceroute

- **Host Address**
Enter a host IP address or domain name for traceroute.
- **Max Hops**
Enter the max hops for traceroute.

Ping	Traceroute	AT Debug	Sniffer
AT Debug Settings			
AT Command		<input type="text"/>	

Debug Tools->AT Debug

- **AT Command**
Enter the AT command of the module.

Ping	Traceroute	AT Debug	Sniffer
Sniffer Settings			
Source Host	<input type="text"/>		
Source Port	<input type="text"/>		
Destination Host	<input type="text"/>		
Destination Port	<input type="text"/>		
Interface	<input type="text"/>		
Sniffer Files List			
Index	File Name	File Size	Date Modified

Debug Tools->Sniffer

- **Source Host**
Enter the source host IP address.
- **Source Port**
Enter the source port.
- **Destination Host**
Enter the destination host IP address.
- **Destination Port**
Enter the destination port.
- **Interface**
Enter the interface that the data traffic goes through.
- **File Name**
Display the file name of the packages.
- **File Size**
Display the size of the package.
- **Date Modified**
Display the date of the package.

5 Appendix A -Glossary

APN:	Access Point Name
GPRS:	General Packet Radio Service
HSPA:	High Speed Packet Access
HSDPA:	High-Speed Downlink Packet Access
HSUPA:	High-Speed Uplink Packet Access
LTE:	3GPP Long Term Evolution
IMEI:	International Mobile Equipment Identity
ICCID:	Integrated Circuit Card Identifier
PIN:	Personal Identification Number
PPP:	Point-to-Point Protocol
RSSI:	Received Signal Strength Indication
SIM:	Subscriber Identity Module
SMS:	Short Message Service
DHCP:	Dynamic Host Configuration Protocol
LAN:	Local Area Network
LED:	Light-Emitting Diode
NTP:	Network Time Protocol
SMA:	SubMiniature version A (connector)
SSID:	Service Set Identifier
TCP/IP:	Transmission Control Protocol / Internet Protocol
UDP:	User Datagram Protocol
VPN:	Virtual Private Network
Wi-Fi or WiFi:	Wireless Fidelity
VDC:	Voltage, Direct Current

6 Appendix B - Q&A

No Signal

Phenomenon

EL-641M-4 Router modem status show no signal.

Possible Reason

- Antenna installation is wrong.
- Modem failure.

Solution

- Check the LTE antenna or replace with new one.
- Check the cellular page confirm modem is detected correctly or not.

Cannot detect SIM card

Phenomenon

EL-641M-4 Router cannot detect SIM card, cellular is not failed to connect to base station.

Possible Reason

- SIM card damage.
- SIM bad contact.

Solution

- Replace SIM card.
- Re-install SIM card.

Poor Signal

Phenomenon

EL-641M-4 Router no signal or poor signal.

Possible Reason

- Antenna installation is wrong.
- Area signal weak.

Solution

- Check the antenna and re-connect it.
- Contact Telecom Operator to confirm signal problem.
- Change to high-gain antenna.

IPSec VPN established, but LAN to LAN cannot communicate

Phenomenon

IPSec VPN established, but LAN to LAN cannot communicate

Possible Reason

- Both subnets are not match the interested traffic.
- IPSec second phase (ESP) settings is not match.

Solution

- Check both subnet settings.
- Check IPSec second phase (ESP) setting.

Forget Router Password

Phenomenon

Forget router login password.

Possible Reason

- User has changed the password.

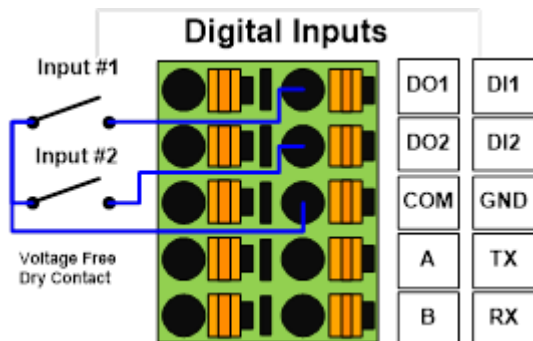
Solution

- After router power on, press RESET button between 3 to 10 seconds then release, router need manually reboot and reset to factory default settings (Username/Password is admin/admin).

7 Appendix C - Digital IO Scenario

Digital Input

Typical Application Diagram



Digital Input Electrical Specifications

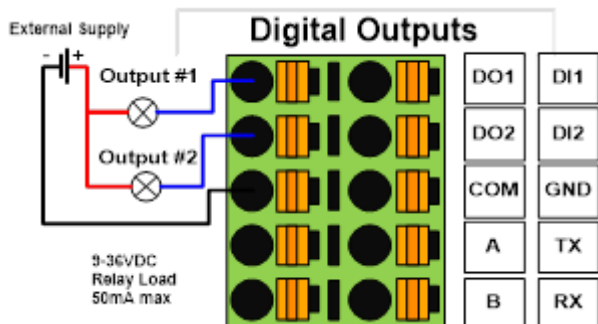
Galvanic Isolation

Over-voltage protection: 36Vdc

Over-current projection: 100mA per channel @25°C

Digital Output

Typical Application Diagram



Digital Output Electrical Specifications

Switch ON: close to V-

Switch OFF: open (high impedance)

DO ELECTRICAL CHARACTERISTICS

1. Galvanic isolation
2. Over-Voltage Protection: 36 VDC
3. Over-Current Protection: 50mA per channel @ 25°C

Wet Contact Typical Application

DO Logic LOW: Switch ON (Led ON)

DO Logic HIGH: Switch OFF (Led OFF)

8 Appendix D - CLI

Command-line interface (CLI) is a software interface that provide another configurable way to set parameters on our router. We could use Telnet or SSH connect to our router for CLI input.

EL-641M-4 CLI Access

Elpro.router login: admin

Password: admin

>

CLI reference commands

>?

config	Change to the configuration mode
exit	Exit this CLI session
help	Display an overview of the CLI syntax
ping	Ping
reboot	Reboot system
show	Show running configuration or running status
telnet	Telnet Client
traceroute	TraceRoute
upgrade	Upgrade firmware
version	Show firmware version

e.g.

> **version**

1.1.7 (22a7514)

> **show wifi**

```
wifi
{
  "status":"Ready",
  "mac":"a8:3f:a1:e0:ab:81",
  "ssid":"Elpro",
  "channel":"6",
  "width":"40 MHz",
  "txpower":"20.00 dBm"
}
```

> **ping www.baidu.com**

```
PING www.baidu.com (14.215.177.38): 56 data bytes
64 bytes from 14.215.177.38: seq=0 ttl=54 time=10.826 ms
64 bytes from 14.215.177.38: seq=1 ttl=54 time=10.284 ms
64 bytes from 14.215.177.38: seq=2 ttl=54 time=10.073 ms
64 bytes from 14.215.177.38: seq=3 ttl=54 time=10.031 ms
64 bytes from 14.215.177.38: seq=4 ttl=54 time=10.347 ms
```

```
--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.031/10.312/10.826 ms
>
```

How to Configure the CLI

CONTEXT SENSITIVE HELP

[?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

AUTO-COMPLETION

The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.

[space] - Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS

[CTRL-A] - Move to the start of the line

[CTRL-E] - Move to the end of the line.

[up] - Move to the previous command line held in history.

[down] - Move to the next command line held in history.

[left] - Move the insertion point left one character.

[right] - Move the insertion point right one character.

DELETION KEYS

[CTRL-C] - Delete and abort the current line

[CTRL-D] - Delete the character to the right on the insertion point.

[CTRL-K] - Delete all the characters to the right of the insertion point.

[CTRL-U] - Delete the whole line.

[backspace] - Delete the character to the left of the insertion point.

ESCAPE SEQUENCES

!! - Substitute the the last command line.

!N - Substitute the Nth command line (absolute as per 'history' command)

!-N - Substitute the command line entered N lines before (relative)