



PM-2212 User Manual

PM-2212 Industrial Serial to Network Modem **OPERATIONS AND MAINTENANCE MANUAL**

Version ***9.2.0***

August 2024

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	PGP Group				

Disclaimer

The information contained in this manual is provided "as is" and is subject to change without notice. While every effort has been made to ensure the accuracy and completeness of this manual, Payesh Gostar Parmoon (PGP) assumes no responsibility for any errors, omissions, or inaccuracies.

PM-2212 is designed for industrial use and should be installed, operated, and maintained by qualified personnel. PGP disclaims all liability for any damages, injuries, or losses, whether direct, indirect, incidental, or consequential, resulting from the use or misuse of this product, including but not limited to, damage to property, loss of data, or operational downtime.

It is the user's responsibility to ensure that the product is used in compliance with all applicable laws, regulations, and standards, and within the environmental and electrical specifications provided. The user assumes all risks and liabilities associated with the use of this product in any application, including but not limited to, those involving safety-critical systems, hazardous environments, or where product failure could result in personal injury or property damage.

PGP shall not be held responsible for any unauthorized modifications or alterations to the product. Any such modifications may void the product warranty and could result in unsafe operation.

By using this product, the user agrees to the terms of this disclaimer and acknowledges that PGP shall not be liable for any incidental or consequential damages arising from the use of this product.

For the latest product information, updates, and documentation, please visit www.pgp.co.ir.

TABLE OF CONTENTS

1	Introduction.....	6
1.1	product overview.....	6
1.2	Package Contents.....	6
1.3	SAFETY INFORMATION.....	6
2	Technical specification.....	7
2.1	Hardware specifications.....	7
2.2	supported protocols & standards.....	8
3	Installation.....	9
3.1	Physical Installation.....	9
3.1.1	Mounting the Modem.....	9
3.1.2	Connecting RS485 and RS232 Devices.....	9
3.1.3	Powering the Modem.....	9
3.1.4	Antenna Installation (Wi-Fi/GPRS).....	10
3.2	Network Connections.....	10
3.2.1	Ethernet Connection Setup.....	10
3.2.2	Wi-Fi Configuration.....	10
3.2.3	GPRS SIM Card Installation and Setup.....	10
3.3	LED Indicators and Their Meanings.....	11
4	Configuration and setup.....	12
4.1	Accessing the web interface.....	12
4.1.1	Connecting to the Web Interface.....	12
4.2	Main Menu.....	13
4.2.1	Status Menu.....	14
4.2.1.1	Overview:.....	14
4.2.1.2	Routing:.....	15
4.2.1.3	Firewall:.....	16
4.2.1.4	System Log:.....	18
4.2.1.5	Channel Analysis:.....	18
4.2.1.6	Realtime Graphs:.....	18
4.2.2	System.....	19
4.2.2.1	System.....	19
4.2.2.2	Administration.....	20
4.2.2.3	Reboot.....	21
4.2.3	Services.....	21
4.2.3.1	Serial to network.....	21
4.2.3.2	SMS.....	21
4.2.3.3	Daily Reboot.....	22
4.2.3.4	SNMP.....	24
4.2.4	Network.....	26
4.2.4.1	Interfaces.....	26
4.2.4.2	Wireless.....	28
4.2.4.3	Routing.....	31

4.2.4.4	DHCP and DNS.....	32
4.2.4.5	Diagnostics.....	32
4.2.4.6	Firewall.....	33
4.2.4.7	SimCard Manager.....	35
4.2.5	VPN.....	36
4.2.6	User Manager.....	38
5	Rollback Mechanism.....	39
6	Key Contacts.....	40
7	Regulatory Requirements.....	40
1.	Electrical Safety Standards.....	40
2.	Electromagnetic Compatibility (EMC).....	40
3.	Radio Frequency (RF) Compliance.....	40
4.	Environmental and Energy Standards.....	41
5.	Telecommunications Compliance.....	41
6.	International Approvals.....	41
7.	Product Labeling and Documentation.....	41
8.	Compliance Responsibility.....	42
8	FAQs.....	42
8.1	General Questions.....	42
8.2	Hardware and Installation.....	42
8.3	Network Configuration.....	43
8.4	Security and Management.....	43
8.5	Firewall Rules.....	44
8.6	VPN Configuration.....	44
	Appendix A: Operations and Maintenance Manual Approval.....	46
	APPENDIX B: KEY TERMS.....	47

1 INTRODUCTION

1.1 PRODUCT OVERVIEW

The PM-2212 is a robust and versatile industrial modem designed to seamlessly convert multiple serial communication protocols into modern network interfaces. Equipped with 12 RS485 ports and 2 RS232 ports, this modem allows for easy integration of legacy devices into Ethernet, Wi-Fi, and GPRS networks, ensuring connectivity and communication in even the most demanding industrial environments.

Designed with versatility in mind, the PM-2212 supports a wide range of applications, from factory automation and process control to remote monitoring and telemetry. By bridging the gap between serial communication and modern networking technologies, this modem ensures that your existing infrastructure remains viable and scalable in the era of the Internet of Things (IoT).

With its compact design, rugged construction, and advanced features such as protocol conversion, remote access, and flexible configuration options, the [Product Name] offers a reliable solution for industrial communication needs, enhancing productivity, reducing downtime, and enabling real-time data exchange across multiple platforms

1.2 PACKAGE CONTENTS

Upon opening the package, you will find the following items:

- 1 x PM-2212 Industrial Modem
- 1 x Power Supply Unit (PSU)
- 1 x Antenna for Wi-Fi/GPRS (if applicable)
- 1 x Ethernet Cable
- 1 x Mounting Kit (for rack, wall, or DIN rail installation)
- 1 x User Manual
- 1 x Quick Start Guide

Please ensure that all items are present and in good condition. If anything is missing or damaged, contact your supplier immediately.

1.3 SAFETY INFORMATION

Before using the PM-2212, please read and follow these important safety precautions:

- **Installation:** Ensure that the modem is installed in a secure, dry location away from direct sunlight, excessive heat, and moisture. Proper ventilation should be maintained to avoid overheating.
- **Electrical Safety:** Use only the provided power supply or an equivalent one specified in this manual. Ensure that all electrical connections are secure and comply with local electrical codes.

- **Handling:** Avoid dropping or subjecting the modem to physical shock. Handle all cables and connectors with care to prevent damage.
- **Environment:** Operate the modem within the specified temperature and humidity ranges. Do not expose the device to corrosive substances or environments.
- **Network Security:** Always configure strong passwords and secure settings to protect the modem from unauthorized access.

Failure to follow these precautions may result in damage to the equipment or personal injury. For detailed safety instructions, refer to the relevant sections later in this manual.

2 TECHNICAL SPECIFICATION

2.1 HARDWARE SPECIFICATIONS

The PM-2212 industrial modem is engineered with high-performance components to ensure reliable and efficient operation across various industrial applications. Below are the detailed hardware specifications:

- **Serial Ports:**
 - **RS485 Ports:** 12 protected RS485 ports with individual settings
 - Data Rate: 300 bps to 1 Mbps
 - Signal Type: Differential, half-duplex
 - Termination: Configurable via DIP switches
 - Isolation: 2kV
 - **RS232 Ports:** 2 RS232 ports for direct connection to legacy devices
 - Data Rate: 300 bps to 115.2 kbps
 - Signal Type: Full-duplex, asynchronous
 - Connector Type: DB9 female
- **Network Interfaces:**
 - **Ethernet:**
 - Ports: 2 x 10/100/1000 Mbps RJ45 Ethernet port
 - Protocols: TCP/IP, UDP, DHCP.
 - Security: Built-in firewall, VPN support
 - **Wi-Fi:**
 - Standard: [Specify, e.g., IEEE 802.11b/g/n]
 - Frequency: 2.4 GHz
 - Security: WPA2, WPA3, SSID hiding, MAC filtering
 - Antenna: 3dB external antenna
 - **GPRS:**
 - Frequency Bands: Quad-band 850/900/1800/1900 MHz
 - Data Rate: Please refer to the EC200A-EU communication module
 - SIM Card Slot: 2 x standard SIM card slot
 - Antenna: external antenna
- **Power Supply:**
 - Input Voltage: 8 to 25 VDC
 - Included Industrial Power Supply:
 - Input: 110V to 250V AC/DC

- Output: 12 VDC
- Form Factor: DIN-RAIL mountable
- Protection: Over-voltage, over-current, reverse polarity
- **Physical Dimensions:**
 - Dimensions: 150mm x 100mm x 40mm
 - Weight: 500g
 - Mounting Options: DIN rail, wall-mount, rack-mount compatible
- **LED Indicators:**
 - Signal Strength Display: 8 LEDs indicating the received signal strength level.
 - SIM Card Presence Indicators (SIM1, SIM2): LEDs that indicate the presence of a SIM card in each slot.
 - WWAN Network Connection Indicator: Illuminates when the device obtains an IP address via the SIM card.
 - Status Display: LED that turns on under various conditions such as powering on/off the Wi-Fi or pressing the reset button.
 - APN Connection Display: Shows the connection status to the APN telecommunication network with different colors:
 - Red: No connection to the network
 - Green: Connected to the GPRS network
 - Blue: Connected to the 3G/HSPA network
 - Turquoise: Connected to the LTE network
 - WLAN Display: Indicates the connection status to the Wi-Fi network.
 - TX Display: Displays the status of data transmission from the serial ports.
 - RX Display: Displays the status of data reception by the serial ports.

2.2 SUPPORTED PROTOCOLS & STANDARDS

The PM-2212 modem supports a wide array of communication protocols and adheres to industry standards to ensure compatibility with various devices and networks:

- **Serial Communication Protocols:**
 - Custom protocols (user-configurable)
- **Network Protocols:**
 - TCP/IP (IPv4/IPv6)
 - UDP
 - DHCP/Static IP
 - DNS, NTP
 - HTTP/HTTPS for web-based management
 - FTP/TFTP for firmware updates
- **Security Standards:**
 - SSL/TLS for encrypted communication
 - VPN support (OpenVPN, IPsec)
 - Firewall with customizable rules
 - MAC address filtering
 - User authentication and access control
- **Compliance:**
 - FCC Part 15, Class A

- CE Mark
- RoHS
- Details in CH6

3 INSTALLATION

Proper installation of the industrial modem is critical for ensuring optimal performance and reliability. This section provides detailed instructions on physically installing the modem, connecting all necessary interfaces, and understanding the LED indicators that provide status information.

3.1 PHYSICAL INSTALLATION

3.1.1 Mounting the Modem

The PM-22XX industrial modem is designed for flexible installation in a variety of environments. It can be mounted in the following ways:

- **DIN Rail Mounting:**
 - Snap the modem onto the DIN rail. Ensure it is securely in place.
- **Wall Mounting:**
 - Secure the modem to the wall using screws and anchors appropriate for the wall material.

3.1.2 Connecting RS485 and RS232 Devices

The modem supports 12 RS485 ports and 2 RS232 ports, allowing for the connection of various serial devices. Follow these steps to connect your devices:

- **RS485 Connections:**
 - Identify the RS485 terminals or connectors on the modem.
 - Connect the RS485 A (+) and B (-) wires from your device to the corresponding terminals on the modem.
- **RS232 Connections:**
 - Identify the RS232 ports on the modem (usually DB9 connectors).
 - Connect your RS232 device using the appropriate serial cable.
 - Ensure the connectors are securely fastened to prevent disconnection.

3.1.3 Powering the Modem

The PM-22XX modem requires a stable DC power supply for operation. Follow these steps to power the modem:

- **Power Supply Connection:**
 - Connect the DC power supply to the modem's power input terminal.
 - Ensure the input voltage matches the specified range (12-24 VDC).
 - If necessary, secure the power connection with the included screw terminals.

- **Powering On:**
 - Once connected, switch on the power supply.
 - The modem will perform a self-test, and the power LED will illuminate to indicate the modem is powered.

3.1.4 Antenna Installation (Wi-Fi/GPRS)

If your modem includes Wi-Fi or GPRS capabilities, proper antenna installation is essential for reliable wireless communication:

- **Wi-Fi Antenna:**
 - Screw the provided Wi-Fi antenna into the designated SMA connector on the modem.
 - Adjust the antenna to a vertical position to ensure optimal signal reception.
- **GPRS Antenna:**
 - Insert the GPRS antenna into the corresponding SMA connector.
 - Ensure the antenna is properly secured and positioned to maximize signal strength.

3.2 NETWORK CONNECTIONS

To enable Ethernet, Wi-Fi, and GPRS communication, follow these steps for network connection setup:

3.2.1 Ethernet Connection Setup

- **Connect an Ethernet cable** from your network switch or router to the modem's Ethernet port.
- **Ensure the cable is securely connected** to avoid intermittent connectivity issues.
- **Verify the connection** by checking the Ethernet LED indicator. A solid or blinking green light indicates a successful connection.

3.2.2 Wi-Fi Configuration

To connect the modem to a Wi-Fi network:

- **Access the modem's web interface** (instructions in Section 4.1).
- Navigate to the **Wi-Fi settings** section.
- **Select the appropriate SSID** from the list of available networks.
- **Enter the Wi-Fi password** and configure security settings as required.
- **Apply the settings** and verify the Wlan LED indicator shows a stable connection.

3.2.3 GPRS SIM Card Installation and Setup

For GPRS connectivity:

- **Insert a SIM card** into the SIM card slot on the modem. Ensure the SIM card is properly oriented as indicated by the slot guide.
- **Configure GPRS settings** through the web interface:
 - Enter the **APN (Access Point Name)** provided by your mobile network operator.

- Input any additional credentials (username, password) if required by your network provider.
- **Apply the settings** and verify the GPRS LED indicator to ensure connectivity.

3.3 LED INDICATORS AND THEIR MEANINGS

The modem features several LED indicators that provide real-time status information. Understanding these indicators is crucial for diagnosing connection issues and monitoring device operation:

- **Power LED:**
 - **RED:** The modem is powered on and functioning normally.
 - **Off:** No power is supplied to the modem.
- **Ethernet LED:**
 - **Solid Green:** Ethernet link is up.
 - **Blinking Green:** Data is being transmitted or received over Ethernet.
 - **Off:** No Ethernet connection detected.
- **Wlan LED:**
 - **Solid Yellow:** Wi-Fi is connected and operational.
 - **Blinking Yellow:** Wi-Fi is attempting to connect or transmitting data.
 - **Off:** Wi-Fi is disabled or no connection is detected.
- **WWAN LED:**
 - **Solid Green:** GPRS connection is established.
 - **Off:** No GPRS connection or SIM card detected.
- **RS485/RS232 Port LEDs:**
 - **Green/Yellow Blinking:** Data is being transmitted (Tx) or received (Rx) on the corresponding port.
 - **Off:** No data transmission is occurring.
- **SIM1and SIM2 LED:**
 - **Solid Green: SIM card:** the SIM card is in the slot.
- **Signal Strength LED:**
 - **A row of 8 white LEDs:** indicate the strength of the received signal by the GSM Module.

4 CONFIGURATION AND SETUP

4.1 ACCESSING THE WEB INTERFACE

The PM-2212 modem offers a comprehensive configuration and monitoring interface accessible through a web browser. This user-friendly interface allows you to easily manage the modem's settings, monitor its status, and perform diagnostic tasks. Figure 1 illustrates the main page

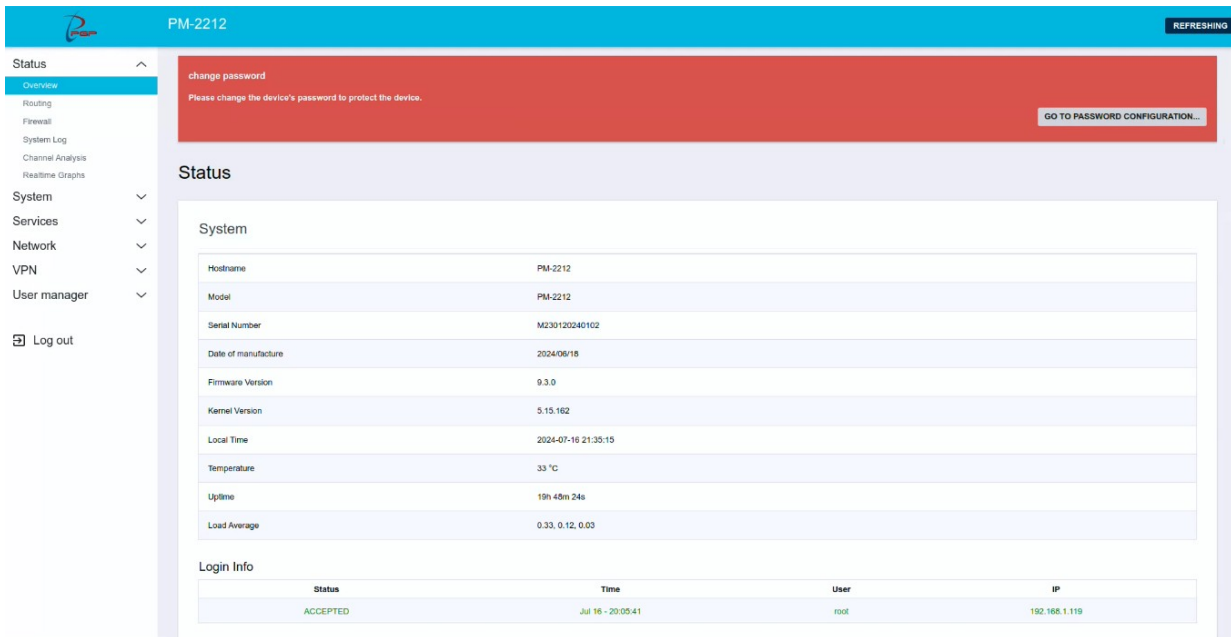


Figure 1

4.1.1 Connecting to the Web Interface

To access the web interface, follow these steps:

1- Connect the Modem to Your Network:

Ensure that the modem is properly connected to your local network via the Ethernet port, or connect to the modem's Wi-Fi network if it is enabled. To connect using Wi-Fi network use following information

SSID	PGP-wifi
Password	Parmoon!

2- Determine the Modem's IP Address:

The default IP address of the modem is typically [Default IP Address, e.g., 192.168.1.1]. If the modem is set to obtain an IP address automatically (via DHCP), you may need to check your router's DHCP client list or use a network scanner to find the assigned IP address.

3- Open a Web Browser:

On a device connected to the same network as the modem, open a web browser (e.g., Chrome, Firefox, Edge).

4- Enter the IP Address:

In the browser's address bar, type the modem's IP address (e.g., http://192.168.1.1) and press Enter.

5- Log In:

A login page will appear. Enter the default username and password (or your customized credentials if they have been changed).

Default credentials are usually:

Username: root

Password: parm@n246!#

Click Login to access the web interface.

After login it is strongly recommended to change the default credentials.

4.2 MAIN MENU

Once logged in, the main menu of the web interface is displayed. This menu provides access to all configuration, monitoring, and management functions of the modem. The main menu consists of the following sections:

- Status
- System
- Services
- Network
- VPN

Each section contains various submenus that provide detailed information and options for configuration.

4.2.1 Status Menu

The Status menu offers a comprehensive overview of the modem's current state and performance metrics. This section is crucial for monitoring the modem's operations and diagnosing issues. The Status menu is divided into the following submenus:

4.2.1.1 Overview:

The **Overview** section of the status menu provides a comprehensive snapshot of the PM2212's current operational status and configuration. It is divided into several panes, each displaying critical information about different aspects of the device:

System Information Pane This pane shows the device's general system details, such as:	○ Hostname ○ Model number ○ Serial number ○ Firmware version ○ Uptime
Login Information Pane Displays details about the current logged-in user and the time of the last login. This helps administrators track user access for monitoring purposes.	
GSM Information Pane Provides crucial data about the cellular modem status, including:	○ Hardware version ○ Software version ○ IMEI (International Mobile Equipment Identity) ○ SIM card status (SIM1, SIM2) ○ SIM card CIMI ○ SIM card ICCID ○ Current network operator name ○ APN (Access Point Name) settings ○ Frequency band in use ○ Signal strength (in dBm) ○ Assigned IP address from the mobile network
Memory Usage Status Pane Shows the current memory utilization, including both the total and available RAM, helping assess device performance.	
Storage Usage Status Pane Displays information about the internal storage capacity and the percentage currently in use.	
Network Status Pane This pane provides details about active connections across all network interfaces,	○ Ethernet ○ Wi-Fi ○ Cellular (GSM)

including:	
Wireless Status Pane Shows information about the Wi-Fi interface, including:	○ SSID (Service Set Identifier) ○ Security protocol (e.g., WPA2) ○ Channel in use ○ Associated stations (devices connected to the Wi-Fi network)
IPsec Characteristics Pane This pane provides details about any active IPsec VPN connections, such as:	○ Status of the VPN tunnel ○ Local and remote IP addresses ○ Encryption algorithms in use ○ Authentication method (e.g., preshared key or certificate)

4.2.1.2 Routing:

The **Routing Overview** section of the status menu displays critical information about the device's routing configurations for both IPv4 and IPv6 protocols. This section provides insight into the status and performance of routing within the PM2212, allowing administrators to monitor and manage network traffic efficiently.

Key components of the **Routing Overview** include:

1. Neighbors

Displays information about neighboring devices on the network that the modem-router has discovered. It shows the IP addresses and MAC addresses of these devices, along with their status (e.g., reachable, stale). This helps administrators understand the devices interacting with the PM2212.

2. Active Routes

Lists the currently active routes for both IPv4 and IPv6 protocols. This table includes details such as:

- Destination network or host
- Gateway address
- Interface associated with the route (e.g., Ethernet, GSM)
- Metric (priority) for route selection These routes direct how network traffic flows between different interfaces and external networks.

3. Active Rules

Displays any active routing rules configured on the device. Routing rules define specific conditions for how traffic is routed, based on criteria such as source or destination IP, port numbers, or packet attributes. This section helps monitor which routing rules are currently in effect.

4. Static Routes

Shows all manually configured static routes that guide traffic to specific networks or hosts. Static

routes are not dynamically updated and must be manually added or modified by an administrator. Information includes:

- Destination
- Next-hop gateway
- Interface
- Protocol (IPv4 or IPv6)

4.2.1.3 Firewall:

The **Firewall Overview** section of the status menu provides a detailed view of the PM2212's firewall activity and configuration. This section is essential for monitoring how the firewall is handling network traffic and enforcing security policies. The overview is organized into different traffic filtering and rule-processing chains that govern how packets are treated as they traverse the firewall.

Key elements of the **Firewall Overview** include:

Traffic Filter Chains	
These chains control how network traffic is handled at different stages. Each chain applies a set of rules that determine whether to allow, block, or modify packets:	
Input	Controls incoming traffic directed to the device itself
Forward	Manages traffic passing through the device between different interfaces (e.g., LAN to WAN).
Output	Governs outgoing traffic originating from the device.
Raw Prerouting	Inspects and filters traffic before connection tracking begins, offering a more direct packet filtering mechanism
Raw Output	Applies filtering rules before connection tracking for packets originating from the device
Mangle Prerouting	Alters packet headers before routing decisions are made, used for advanced traffic control
Mangle Postrouting	Modifies packet headers after routing, before packets leave the device.
Mangle Input	Handles packets destined for the device, allowing modifications to packet headers
Mangle Forward	Alters headers of packets being forwarded between interfaces
Mangle Output	Modifies packet headers for outgoing traffic.

Rule Container Chains These chains are custom rule containers for managing specific types of traffic based on network zones (LAN, WAN) or special conditions (e.g., SYN flood protection)	
Hand Reject	Manages traffic that needs to be explicitly rejected
Syn Flood	: Protects against SYN flood attacks by monitoring and blocking suspicious traffic patterns
Input LAN	Governs incoming traffic from the local network (LAN) to the device.
Output LAN	Controls outgoing traffic from the device to the local network.
Forward LAN	Manages traffic forwarded between LAN interfaces
Helper LAN	Applies connection tracking helpers for specific protocols within the LAN
Accept from LAN	Specifies rules to allow certain traffic from LAN devices.
Accept to LAN	Defines rules to allow traffic directed to the LAN
Input WAN	Governs incoming traffic from the WAN to the device
Output WAN	: Controls outgoing traffic from the device to the WAN
Forward WAN	Manages traffic forwarding between the WAN and other network interfaces.
Accept to WAN	Defines rules for allowing traffic directed to the WAN
Reject to WAN	Specifies rules for rejecting traffic headed to the WAN
NAT Action Chains These chains handle network address translation (NAT) operations, which modify the source or destination IP addresses of packets	
Dstnat	Destination NAT rewrites the destination IP address of packets to forward them to specific internal devices (e.g., port forwarding).
Srcnat	Source NAT rewrites the source IP address of outgoing packets, typically used to map internal IPs to the device's external IP.

4.2.1.4 System Log:

Contains detailed logs of system events, including startup messages, connection attempts, errors, and warnings.

4.2.1.5 Channel Analysis:

Provides an analysis of the wireless channels surrounding the modem, helping to optimize Wi-Fi performance and reduce interference. For instance, figure 2 depicts the 2GHZ band status around the modem that helps the administrator to choose the proper spectrum.

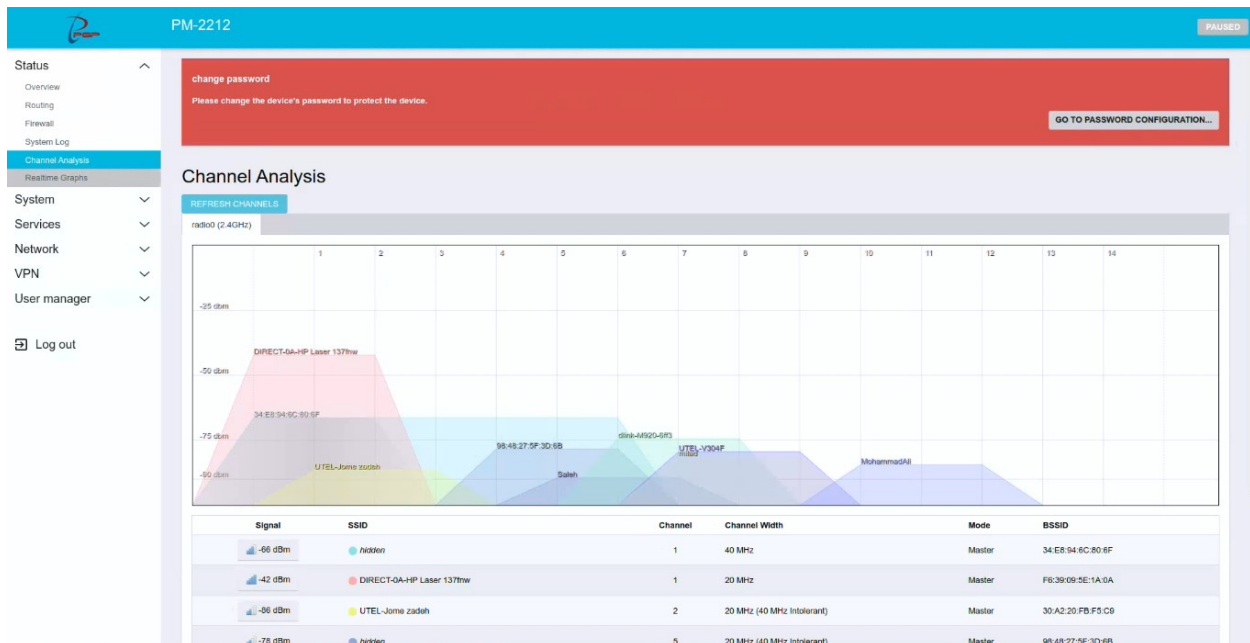


Figure 2

4.2.1.6 Realtime Graphs:

Displays real-time graphical representations of various performance metrics such as CPU usage, memory usage, network throughput, and signal strength of GSM module.

4.2.2 System

The System menu in the web interface allows you to configure and manage the fundamental settings of the modem, ensuring that it operates effectively within your network environment. This section provides options to customize the modem's system settings, manage administrative access, perform backups, update firmware, and reboot the device. The System menu is organized into the following items:

4.2.2.1 System

The **System** item is where you can define the basic operational parameters of the modem, such as its hostname and time zone. These settings ensure that the modem is correctly identified on the network and operates according to the correct time zone. The System item is divided into several tabs:

An overview is shown in figure 3

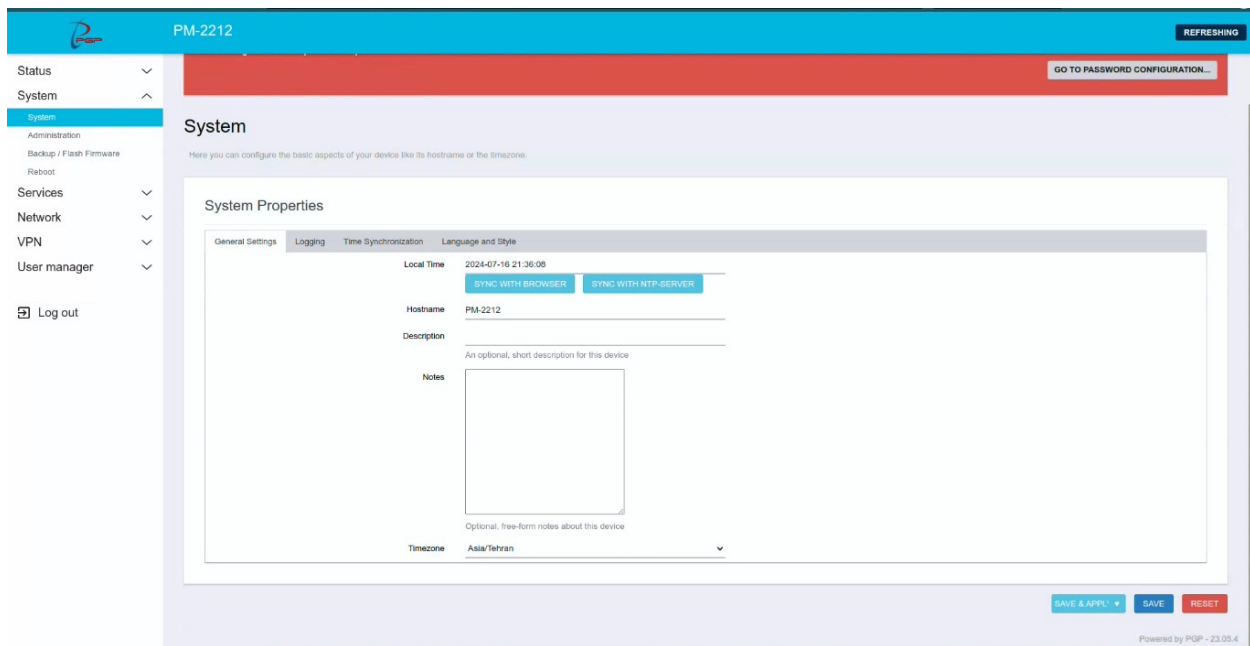


Figure 3

- **General Settings:**
 - **Hostname:** Set the name of the device as it will appear on the network.
 - **Time Zone:** Select the appropriate time zone for the modem to ensure correct logging and time-based operations.
- **Logging:**
 - **System Log Buffer Size:** Configure the size of the system log buffer, which determines how much logging data is stored on the device.
 - **External Log Server:** Specify an external server where logs can be sent for centralized storage and analysis.

- **Log Level:** Choose the severity of events to log (e.g., Debug, Info, Warning, Error).
- **Time Synchronization:**
 - **NTP Configuration:** Set up Network Time Protocol (NTP) to automatically synchronize the modem's internal clock with an external time server, ensuring accurate timekeeping.
 - **NTP Servers:** Specify one or more NTP servers for time synchronization.
- **Language Settings:**
 - **Language Selection:** Choose the preferred language for the web interface to accommodate different users.

4.2.2.2 Administration

The **Administration** item provides options for managing access to the modem's web interface and other administrative functions. This ensures that only authorized users can make changes to the modem's configuration. The Administration item is divided into the following tabs:

- **Access Management:**
 - **Password Setting:** Change the password for accessing the web interface to enhance security. Please note that the password must be a combination of numeric and none numeric characters including capital ones. More complex combinations is recommended.
 - **SSH Access Settings:** Configure Secure Shell (SSH) access, including enabling or disabling SSH, setting the SSH port, and managing SSH keys for secure remote access.
 - **HTTPS Access:** Enable or disable HTTPS for secure encrypted access to the web interface. You can also configure SSL/TLS certificates for the HTTPS connection.
- **User Management:**
 - **User Roles:** Create and manage different user accounts and roles, specifying different levels of access and permissions.

■ Backup/Flash Firmware

The **Backup/Flash Firmware** item provides tools for managing the modem's configuration and firmware. These tools help ensure that you can recover quickly from any issues by restoring a previous configuration or updating the device to the latest firmware version. The Backup/Flash Firmware item includes the following functions:

- **Configuration Backup and Restore:**
 - **Backup Current Configuration:** Save the current modem configuration to a file, allowing you to restore it later if needed.
 - **Restore Configuration:** Bring the device to the factory settings using **Perform Reset** button. Upload a previously saved configuration file to restore the modem's settings using **Reload Archive** button.
- **Firmware Update:**
 - **Upload Firmware:** Manually upload a new firmware file to update the modem. Please note that the firmware file was released by the manufacturer. Upon completing the update process, user can select whether to keep the current configuration or set back to the factory configurations settings. To complete the process, the device will be rebooted automatically during this process do not power off the device. It would be last 5 to 8 min.
 - **Firmware Version:** Displays the current firmware version installed on the device.

4.2.2.3 Reboot

The **Reboot** item allows you to restart the modem's operating system. Rebooting is sometimes necessary after making configuration changes, installing firmware updates, or troubleshooting the device. The reboot process is simple and ensures that all changes are applied and the system runs smoothly.

- **Reboot Device:** Click the reboot option to safely restart the modem. This process may take a few minutes, during which the modem will temporarily go offline and then come back online with the applied settings.

4.2.3 Services

The Services menu in the web interface provides essential tools and configurations that allow you to manage the device's communication ports, messaging, automated actions, and network monitoring services. This section is crucial for tailoring the modem's operation to meet specific industrial needs. The Services menu consists of the following submenus:

- **Serial to Network**
- **SMS**
- **Daily Reboot**
- **SNMP**

4.2.3.1 Serial to network

The Serial to Network submenu is dedicated to the configuration of the modem's RS232 and RS485 ports. This section allows you to manage how each serial port interfaces with the network, ensuring smooth and reliable data transmission. The available options include:

- **Enable/Disable Ports:** You can individually enable or disable each of the RS232 and RS485 ports based on your current requirements.
- **Baud Rate:** Set the baud rate for each port to match the communication speed of the connected devices. Available baud rates typically range from [300 bps to 115200 bps].
- **Protocol Selection:** Choose the communication protocol for each port, such as RAW, Modbus RTU, ASCII, or other supported protocols.
- **Timeout Options:** Configure the timeout settings for each port to determine how long the modem waits for data before assuming the connection is lost. This helps in maintaining efficient communication and avoiding unnecessary delays.

4.2.3.2 SMS

The SMS submenu allows you to configure the modem's Short Message Service (SMS) functionality, enabling the users which their phone numbers are stored inside the device to enquire the status of the device by sending a password included message. The configuration options include:

- **Password Protection:** Set a password to secure access to the SMS functionality, ensuring that only authorized users can send or configure SMS messages.

- **Phone Number Configuration:** Specify the phone number(s) to which SMS messages will be sent. This could be a mobile number where notifications are received in case of network issues or other important events.

In order to work properly, the sender must comply with the following format for SMS text:

Password	Command	Value
----------	---------	-------

Password: This is the password that is stored on the device for security and you need to include it in your sent package to execute the commands.

Command: The set of commands are listed in the following tables

Command	Description
Set	It is used to activate and set a feature.
Reset	Used to disable a feature.
Get	It is used to get some device parameters.

Set Commands:

Command	Description
O1	Enable Digital Output 1.

Reset Commands:

Command	Description
O1	Disable Digital Output 1.
OS	Reboot the device.
NET	Restart network interfaces.

4.2.3.3 Daily Reboot

The Daily Reboot submenu allows you to set automated rules that trigger the modem to reboot under specific conditions. This feature is useful for maintaining the modem's reliability, particularly in scenarios where it operates continuously over extended periods. To create a reboot rule, click on ADD button. In the new window the General Settings tab can be seen. The Mode option allows you to choose the reboot mode from (Ping Reboot, Periodic Reboot, Restart Interface, Run script)

Mode	Description		
Ping Reboot	Reboot this device if a ping to a specified host fails for a specified duration of time.		
Periodic Reboot	Reboot this device after a specified interval of time.		
Restart Interface	Restart a network interface if a ping to a specified host fails for a specified duration of time.		
Run Script	Run a script if a ping to a specified host fails for a specified duration of time.		
Option	Description	Applicable to	Extra
Period	it defines the longest period of time without a reply from the host to check before a reboot is triggered.	Ping Reboot Periodic Reboot Restart Interface Run script	h for hours, m for minutes and s for seconds
Host to Check	The host address to check for example (8.8.8.8 to check normal connection to internet)	Ping Reboot Restart Interface Run script	IP Address or Host Name
Address family for pinging the host	Addressing protocol	Ping Reboot Restart Interface Run script	IPv4/IPv6
Check Interval	How often to ping the host	Ping Reboot Restart Interface Run script	h for hours, m for minutes and s for seconds
Ping Packet Size		Ping Reboot Restart Interface Run script	In bytes
Force Reboot Delay	Applicable to ping and periodic reboot. It defines the delay between failed soft reboot and hard reboot	Ping Reboot Periodic Reboot Restart Interface Run script	h for hours, m for minutes and s for seconds
Interface	Defines the interface for restart	Ping Reboot Restart Interface Run script	
Name of	If using ModemManager,	Restart Interface	(lan , SIM , etc)

ModemManager Interface	you can have Watchcat restart your ModemManger interface by specifying its name		
Unlock Modem Bands	If using ModemManager, then before restarting the interface, set the modem to be allowed to use any band	Restart Interface	
Script to run	Script to run when the host has not responded for the specified duration of time. The script is passed the interface name as \$1	Run script	/etc/watchcat.user.sh

4.2.3.4 SNMP

The **SNMP** (Simple Network Management Protocol) submenu provides options for configuring the modem's SNMP service, enabling network administrators to monitor and manage the device remotely. SNMP is a widely used protocol for collecting and organizing information about managed devices on IP networks. The modem supports all three versions of SNMP, though caution is advised when using older versions:

- **SNMP v1 and v2:** While these versions are supported, they are not recommended due to security vulnerabilities inherent in their design. It is advisable to use them only if necessary for compatibility with legacy systems.
- **SNMP v3:** This version is recommended as it provides enhanced security features, including encryption and user authentication. SNMP v3 ensures that data is transmitted securely, protecting against unauthorized access and tampering.

Activate the SNMP protocol by tick the Enable SNMP agent/agentx checkbox in the general pane. Enter the location, contact and name in the system pane. The following checkboxes are available to enable read and write for different versions of SNMP:

Enable SNMP v1/v2 access

Enable SNMP v3 access

Enable SNMP read users

Enable SNMP write users

Group	OID	Description
Device Info	1.3.6.1.4.1.5590.0.0	Device Model
	1.3.6.1.4.1.5590.0.1	Firmware version
	1.3.6.1.4.1.5590.0.2	Serial number
	1.3.6.1.4.1.5590.0.3	Production date
	1.3.6.1.4.1.5590.1.0	Device temperature
	1.3.6.1.4.1.5591.0.0	GSM Model
	1.3.6.1.4.1.5591.0.1	IMEI

GSM Module Info	1.3.6.1.4.1.5591.1.0	Signal Strength
	1.3.6.1.4.1.5591.1.1	ACT
	1.3.6.1.4.1.5591.2.0	APN
	1.3.6.1.4.1.5591.2.1	Operator Name
	1.3.6.1.4.1.5591.2.2	IP Address
	1.3.6.1.4.1.5591.3.0	SIM Card CIMI
	1.3.6.1.4.1.5591.3.1	SIM Card ICCID
RS485 Serial Ports	1.3.6.1.4.1.5592.1.1	Driver Status of RS485 (P1)
	1.3.6.1.4.1.5592.1.2	Driver Status of RS485 (P2)
	1.3.6.1.4.1.5592.1.3	Driver Status of RS485 (P3)
	1.3.6.1.4.1.5592.1.4	Driver Status of RS485 (P4)
	1.3.6.1.4.1.5592.2.5	Driver Status of RS485 (P5)
	1.3.6.1.4.1.5592.2.6	Driver Status of RS485 (P6)
	1.3.6.1.4.1.5592.2.7	Driver Status of RS485 (P7)
	1.3.6.1.4.1.5592.2.8	Driver Status of RS485 (P8)
	1.3.6.1.4.1.5592.3.9	Driver Status of RS485 (P9)
	1.3.6.1.4.1.5592.3.10	Driver Status of RS485 (P10)
	1.3.6.1.4.1.5592.3.11	Driver Status of RS485 (P11)
	1.3.6.1.4.1.5592.3.12	Driver Status of RS485 (P12)
I/O	1.3.6.1.4.1.5593.0.1	Digital Output 1

4.2.4 Network

The Network menu is the central hub of the modem's management console, providing comprehensive tools for configuring and managing the modem's network interfaces and functionalities. This section is crucial for ensuring optimal network performance and connectivity. The Network menu consists of the following submenus:

- **Interfaces**
- **Wireless**
- **Routing**
- **DHCP and DNS**
- **Diagnostics**
- **Firewall**
- **SIM Card Manager**

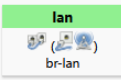
4.2.4.1 Interfaces

The Interfaces submenu is the primary area for managing the modem's network interfaces, which are crucial for connecting the modem to various networks and devices. It consists of three tabs:

- **Interfaces:**
 - This tab (figure 4) allows you to add, delete, stop, edit, and restart various network interfaces available on the modem. You can manage both physical interfaces (such as Ethernet, Wi-Fi, and cellular) and virtual interfaces (like VLANs or VPNs). Each interface can be configured with specific IP settings, connection modes, and performance parameters, ensuring that the modem integrates seamlessly with your network infrastructure.

Interfaces Devices Global network options

Interfaces

 lan br-lan	Protocol: Static address Uptime: 1d 7h 33m 13s MAC: 40:D6:3C:BA:16:C0 RX: 12.87 MB (117975 Pkts.) TX: 3.45 MB (13912 Pkts.) IPv4: 172.30.22.200/24 IPv6: fda1:ed80:13f2::1/60	RESTART STOP EDIT DELETE
 SIM	Protocol: UMTS/GPRS/EV-DO RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) IMEI:	RESTART STOP EDIT DELETE

ADD NEW INTERFACE...

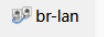
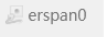
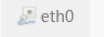
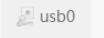
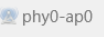
Figure 4

- Devices:**

- In this tab (figure 5), you can configure other network devices connected to the modem, such as additional network adapters, external routers, or switches. This allows you to expand the modem's connectivity options and ensure that all connected devices are properly managed and configured.

Interfaces Devices Global network options

Devices

Device	Type	MAC Address	MTU		
 br-lan	Bridge device	40:D6:3C:BA:16:C0	1500	CONFIGURE...	UNCONFIGURE
 erspan0	Network device	00:00:00:00:00:00	1450	CONFIGURE...	UNCONFIGURE
 eth0	Network device	40:D6:3C:BA:16:C0	1500	CONFIGURE...	UNCONFIGURE
 usb0	Network device	02:0C:29:A3:9B:6D	1500	CONFIGURE...	UNCONFIGURE
 phy0-ap0	Network device	40:D6:3C:BA:16:C0	1500	CONFIGURE...	UNCONFIGURE

ADD DEVICE CONFIGURATION...

Figure 5

- Global Network Options:**

- This tab (figure 6) provides options for global network settings that affect the modem's overall network performance. One key feature here is **Packet Steering**, which can be enabled to improve packet processing performance on multi-core platforms. Packet steering helps distribute network traffic across multiple CPU cores, reducing bottlenecks and improving the overall efficiency of the modem.

Interfaces
Devices
Global network options

Global network options

IPv6 ULA-Prefix

fda1:ed80:13f2::/48

Unique Local Address - in the range `fc00::/7`. Typically only within the 'local' half `fd00::/8`. ULA for IPv6 is analogous to IPv4 private network addressing. This prefix is randomly generated at first install.

Packet Steering

☐

Enable packet steering across all CPUs. May help or hinder network speed.

Figure 6

4.2.4.2 Wireless

The Wireless submenu is dedicated to configuring the modem's Wi-Fi settings, ensuring robust wireless connectivity. As figure 7 shows this submenu includes wireless overview pane and associated stations pane. Overview pane indicates the configured wireless networks. furthermore, it incorporates ADD, SCAN, RESTART, DISABLE, EDIT and REMOVE. In associated stations pane the connected hosts will be listed.

Wireless Overview

radio0

MediaTek MT7628 802.11b/g/n
Channel: 1 (2.412 GHz) | Bitrate: ? Mbit/s

RESTART

SCAN

ADD

dBm

SSID: PGP-WiFi | Mode: Master
BSSID: 40:D6:3C:BA:16:C0 | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DISABLE

EDIT

REMOVE

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

SAVE & APPLY

SAVE

Figure 7

To add a new wireless click ADD button. In the new window two parts need to be configured:

Device configuration (figure 8) which consists general and advanced settings tab and interface configuration (figure 9) which consists general, wireless security, MAC-Filter and advanced settings.

Device Configuration

General Setup **Advanced Settings**

Status  **Mode: Master | SSID: OpenWrt**
--- dBm *Wireless is not associated*

Wireless network is enabled **DISABLE**

Operating frequency Mode Channel Width
N 1 (2412 Mhz) 20 MHz

Allow legacy 802.11b rates ☐

Legacy or badly behaving devices may require legacy 802.11b rates to interoperate. Airtime efficiency may be significantly reduced where these are used. It is recommended to not allow 802.11b rates where possible.

Maximum transmit power driver default - Current power: *unknown*

Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.

Figure 8

Interface Configuration

General Setup **Wireless Security** MAC-Filter Advanced Settings

Mode Access Point

ESSID OpenWrt

Network *unspecified*

Choose the network(s) you want to attach to this wireless interface or fill out the *custom* field to define a new network.

Hide ESSID ☐

Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode ☒

Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates.

Figure 9

The configuration details are listed in the following table:

Device Configuration			
General Setup		Advanced settings	
status	Current status of the network	Country Code	Referring to a specific code that identifies the country in which a wireless device is operating
Enable/Disable	Enabling/disabling the current network	Coverage cell density (disable, normal, high, very high)	Configures data rates based on the coverage cell density
Operating Frequency	Mode (N/Legacy) Channel : the central frequency of the channel Band : the width of the channel	Distance Optimization (in km)	Distance to farthest network member in meters. Set only for distances above one kilometer; otherwise, it is harmful.
Allow legacy 802.11b rates	Compatible with older devices	Fragmentation Threshold	Maximum size of a packet that can be transmitted without fragmented
Maximum transfer power (0dbm – 11dbm)	Specifies the maximum transmit power the wireless radio may use	RTS/CTS Threshold	Determines when (Request To Send) and (Clear To Send) handshake mechanism is used
		Force 40mhz mode	Allowing wireless network to

						utilize a wider channel for increased data throughput	
				Beacon interval		Determining how often the accesspoint sends beacon frames.	
Interface Configuration							
General Setup		Wireless Security		MAC-Filter		Advanced Settings	
Mode	Access point Client Adhoc 802.11s Pseudo adhoc Monitor	Encryption	WPA2/ PSK WPA3/ SAE	Disable		Multi to unicast	ARP, IPv4 and IPv6 (even 802.1Q) with multicast destination MACs are unicast to the STA MAC address. Note: This is not Directed Multicast Service (DMS) in 802.11v. Note: might break receiver STA multicast expectations.
ESSID				Allow listed only	Allow the listed MAC to connect	Isolate Clients	Prevents client-to-client communication
Network	Choose the network(s) you want to attach to this wireless interface or fill out the <i>custom</i> field to define a new network			Allow all except listed	Treat the list as an adversary address list and reject the connection	Interface name	Override default interface name
Hide SSID	Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced			Mac-List	Inserting address into the list	MAC address	Override default MAC address - the range of usable addresses might be limited by the driver
WMM Mode	Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates					Short Preamble	Improve network performance while long preamble enhances compatibility

						DTIM Interval	Delivery Traffic Indication Message Interval
						Time interval for rekeying GTK	
						Disable Inactivity Polling	
						Station inactivity limit	802.11v: BSS Max Idle. Units: seconds
						Maximum allowed Listen Interval	
						Disassociate on low acknowledgment	Allow AP mode to disconnect STAs based on low ACK condition

4.2.4.3 Routing

The Routing submenu allows you to manage the modem's routing configurations, which control how data packets are directed through the network. This submenu is organized into four tabs, offering comprehensive options for both IPv4 and IPv6 routing:

- **IPv4 Static Routing:**
 - Configure static routes for IPv4 traffic, specifying the exact paths that data packets should take to reach their destinations. Static routes are manually defined and are useful for scenarios where specific routing paths are required for certain network traffic.
- **IPv6 Static Routing:**
 - Similar to the IPv4 tab, this allows you to set up static routes for IPv6 traffic. With the growing adoption of IPv6, this tab ensures that your network is prepared for modern internet connectivity.
- **IPv4 Rules:**
 - Set up policy-based routing rules for IPv4 traffic. These rules enable you to route traffic based on specific criteria such as source IP address, destination IP address, or type of service. This granular control helps optimize network performance and security.
- **IPv6 Rules:**
 - Configure policy-based routing rules for IPv6 traffic, allowing you to manage how IPv6 packets are handled based on various parameters. This ensures that your network can efficiently manage IPv6 traffic alongside traditional IPv4 traffic.

4.2.4.4 DHCP and DNS

The DHCP and DNS submenu manages the modem's lightweight DHCP server and DNS forwarder, which are essential for efficiently assigning IP addresses and resolving domain names within your network.

- **DHCP Server:**
 - The modem includes a lightweight DHCP server that automatically assigns IP addresses to devices on your network. You can define IP address pools, set lease times, and reserve IP addresses for specific devices. This streamlined DHCP server is designed to provide essential functionality with minimal resource usage, making it ideal for small to medium-sized networks.
- **DNS Forwarder:**
 - The modem's DNS forwarder is a lightweight service that forwards DNS queries from devices on your network to external DNS servers. This ensures that domain names are resolved quickly and accurately. The DNS forwarder can be configured with primary and secondary DNS servers, and it supports DNS caching to improve query response times.
- **DHCP Leases:**
 - View and manage the list of DHCP leases, including currently assigned IP addresses and associated devices. This allows you to monitor which devices are connected to your network and manage their IP assignments effectively.

This menu (figure 10) allows to configure DHCP and DNS profoundly

The screenshot shows the DHCP and DNS configuration interface. The 'General' tab is selected. The interface includes a top navigation bar with various configuration categories. The main content area is divided into several sections, each with a label, a checkbox, and a text input field. The 'Authoritative' checkbox is checked. The 'Resolve these locally' text field contains '/lan/'. The 'Local domain' text field contains 'lan'. The 'Expand hosts' checkbox is checked. The 'Addresses' text field contains '/router.local/router.lan/192.168.0.1'. The 'IP sets' text field contains '/example.org/ipset.ipset6'. The 'Allocate IPs sequentially' checkbox is unchecked. The 'All servers' checkbox is unchecked. Each section has a brief description of its function.

Figure 10

4.2.4.5 Diagnostics

The Diagnostics submenu provides tools for troubleshooting network issues and ensuring the modem is operating correctly. These tools help diagnose connectivity problems and verify network configurations:

- **Ping Test:**

- Perform a ping test to verify connectivity to specific IP addresses or domain names. This tool helps in identifying whether a target device or server is reachable from the modem, which is essential for troubleshooting network issues.
- **Traceroute:**
 - Use traceroute to map the path that packets take to reach a destination. This tool is useful for identifying where delays or failures occur along the network path, helping to pinpoint network bottlenecks or misconfigurations.
- **NSLookup:**
 - Perform an NSLookup (Name Server Lookup) to query DNS servers for the IP address associated with a domain name or to verify the DNS configuration. This tool is essential for troubleshooting DNS-related issues, ensuring that domain names are being resolved correctly by the DNS servers configured on the modem.

4.2.4.6 Firewall

The Firewall functionality of the modem-router, PM2212, is essential for controlling the flow of network traffic, especially as the device can serve as an edge device at the intersection of WAN and local networks. The firewall allows administrators to manage egress and ingress traffic, ensuring secure and efficient network operations. Once zones are created, you can edit or delete them as needed within the zone pane. The Firewall submenu within the Network menu comprises six tabs:

- **General Settings**

The **General** Settings tab provides overarching controls for the firewall's behavior, divided into three main panes:

General Settings Pane	Here, you can enable SYN-flood protection to safeguard the network against DDoS attacks. This pane also includes options to drop invalid pattern packets and set default actions for traffic flow:	Input: Define whether incoming traffic is accepted, rejected, or dropped. Output: Set the default action for outgoing traffic (accept, reject, drop). Forward: Control the handling of forwarded traffic across different zones.
Routing/ NAT Offloading Pane:	In this pane, you can enable software flow offloading to improve routing and NAT performance. This feature is in the experimental stage and should be used with caution as it may impact network stability.	
Zone Pane	Zones are logical groupings of network interfaces, and creating them allows for detailed control over traffic between different network segments. To create a zone:	1. Click the Add button. 2. In the Zone Settings window, choose a name for the zone. 3. Set default policies for input, output, and forwarding traffic. 4. Under Covered Networks, select the networks included in

		this zone. 5. Specify source and destination zones for traffic rules. 6. The Masquerading option enables source address translation (NAT) to the bound interface.
--	--	---

- **Port Forwards**

The Port Forwards tab enables remote access to specific computers or services by forwarding ports between different zones. This is crucial for exposing internal services to external networks (e.g., accessing a web server from the internet). To create a port forward:

1. Click the **Add** button.
2. Enter a name for the port forward.
3. Choose the protocol (IPv4/IPv6) and the transport layer protocol (TCP/UDP).
4. Select the **source zone** and **destination zone**.
5. Specify the **destination IP** and the port number to which traffic should be forwarded.

This configuration allows precise control over which services are accessible and how they are routed through the firewall.

- **Traffic Rules**

This tab defines how the modem-router handles network traffic based on a set of criteria. Traffic rules are processed from top to bottom, with the first matching rule determining the action taken on a packet. To create a new rule, Click the **Add** button at the bottom-left corner. The popped-up window contains these items:

General settings	Name: A descriptive name for the rule. Protocol: The protocol to match (e.g., TCP, UDP). Source Zone: The originating zone of the traffic. Source IP: Specific source IP addresses or ranges. Source Port: The originating port of the traffic. Output Zone: The destination zone for the traffic. Destination IP: Specific destination IP addresses or ranges. Action: The action to take (accept, drop, reject, etc.).
Advanced Settings	Match Device: Specify the device involved (inbound or outbound). Use IPSet: Apply rules to sets of IP addresses. Source MAC: Match traffic based on source MAC addresses. Match Helper: Use specific protocol helpers (e.g., FTP, RAS). Match Mark: Use marks for connection tracking. Match DSCP: Classify packets based on DSCP values (e.g., CS0-CS7, EF). Limit Matching: Rate-limit traffic matching this rule (e.g.,

	10/second). Time Restrictions: Apply the rule only during specific times or dates.
--	--

- **NAT Rules**

The **NAT Rules** tab manages Network Address Translation settings, which modify the IP addresses of packets as they pass through the modem-router. To configure a NAT rule:

General settings	Name: A name for the NAT rule. Address Family: Select between IPv4, IPv6, or automatic. Outbound Zone: The zone from which traffic is leaving. Source Address: The original IP address to be translated. Destination Address: The target IP address after translation. Action: Choose the NAT action (e.g., SNAT, Masquerade, Accept).
Advanced Settings	Outbound Device: Specify the device handling outbound traffic. Match Mark: Use connection marks for advanced routing. Limit Matching: Apply rate limits similar to traffic rules.

- **IP Sets**

The **IP Sets** tab allows you to create and manage sets of IP addresses, which can be referenced in firewall rules. This simplifies the management of large numbers of addresses by grouping them together, making it easier to apply consistent rules across your network.

- **Bruteforce Protection**

The **Bruteforce Protection** tab enhances security by automatically banning IP addresses that make too many failed login attempts within a specified time frame. This is achieved by updating the firewall rules to reject new connections from those IP addresses for a configurable duration. The key settings include:

- **Ban Time:** The duration for which the offending IP address is banned.
- **Find Time:** The time window within which failed attempts are counted.
- **Max Retry:** The maximum number of failed login attempts allowed before triggering a ban.

4.2.4.7 SimCard Manager

The SIM Card Manager menu allows you to manage and configure the SIM card slots of the PM2212 modem-router. The device supports two SIM card slots, and this menu is essential for activating and managing these SIM cards to ensure continuous and reliable cellular connectivity.

SIM Card Activation:

The SIM Card Manager provides an interface to activate and control which SIM card is in use. This is crucial for managing cellular network connections, especially in environments where redundancy or failover between SIM cards is required.

SIM Selection Mode:

The SIM Selection Mode has three options, allowing you to control which SIM card is active or whether the device should manage this automatically:

Auto-select: In this mode, the modem-router automatically selects the SIM card based on predefined criteria such as signal strength, network availability, or cost. This option is useful for ensuring the device always uses the best available network.

Select SIM 1: This option forces the modem-router to use the SIM card in the first slot exclusively, regardless of the conditions of the second SIM card. It is useful when you have a preferred network provider in the first slot.

Select SIM 2: Similarly, this option forces the device to use the SIM card in the second slot exclusively. It is useful if the second SIM card offers better connectivity or pricing at a given time.

4.2.5 VPN

The VPN Configuration menu on the PM2212 modem-router allows administrators to set up secure, encrypted tunnels between different networks, ensuring data privacy and integrity. The modem-router supports IPsec (Internet Protocol Security) as the primary VPN protocol, providing robust security features for both site-to-site and remote access VPNs. This section details each configurable item within the IPsec settings:

- **Remote ID:**
 - **Remote ID** specifies the identity of the remote VPN peer (e.g., the public IP address or FQDN). This helps in identifying and authenticating the remote endpoint with which the VPN tunnel is established.
- **First Remote Subnet:**
 - The **First Remote Subnet** defines the remote network's IP address range (e.g., 192.168.2.0/24) that will be accessible through the VPN tunnel. This subnet needs to match the configuration on the remote peer for proper routing of traffic.
- **Local ID:**
 - **Local ID** represents the identity of the local VPN endpoint. Similar to Remote ID, it can be an IP address or FQDN that identifies the local device in the VPN negotiation process.
- **First Local Subnet:**
 - The **First Local Subnet** defines the local network's IP address range (e.g., 192.168.1.0/24) that will be accessible through the VPN tunnel. This subnet should align with your local network configuration.
- **Encapsulation Mode:**
 - The **Encapsulation Mode** determines how data packets are encapsulated within the VPN tunnel. There are two options:
 - **Tunnel Mode:** This is the most common mode where the entire IP packet is encrypted and encapsulated. It is typically used for site-to-site VPNs.

- **Transport Mode:** Only the payload (not the IP header) of the IP packet is encrypted. This mode is often used for end-to-end communication between two hosts.
- **IKE Protocol (v1/v2):**
 - **IKE (Internet Key Exchange) Protocol** specifies the version of the IKE protocol used to establish a secure channel for key exchange. The options are:
 - **IKEv1:** The original version, suitable for most VPN connections.
 - **IKEv2:** An improved version with better security features and faster rekeying, recommended for new setups.
- **IKE Mode (Main, Aggressive):**
 - **IKE Mode** defines how the IKE negotiation takes place:
 - **Main Mode:** Provides the best security by exchanging identities securely. It is recommended for most environments.
 - **Aggressive Mode:** Faster than Main Mode but less secure because identities are exchanged in plaintext. This mode is used when speed is a priority, or the identity must be known quickly.
- **IKE Algorithm (Auto, Manual):**
 - The **IKE Algorithm** determines how the keys are exchanged during the IKE phase:
 - **Auto:** The system automatically selects the most appropriate algorithm based on the capabilities of both peers.
 - **Manual:** The user can manually specify the algorithm used for key exchange, which allows for customization of the VPN's security level.
- **IKE Encryption (3DES, AES128, AES192, AES256):**
 - **IKE Encryption** sets the encryption algorithm used to secure the key exchange process:
 - **3DES:** A legacy encryption standard that is now considered less secure.
 - **AES128:** Provides strong security with 128-bit key encryption.
 - **AES192:** Offers stronger encryption with a 192-bit key.
 - **AES256:** The most secure option with 256-bit key encryption, recommended for environments requiring high security.
- **IKE Hash (MD5, SHA1, SHA256, SHA512):**
 - The **IKE Hash** function is used to ensure data integrity during the IKE negotiation:
 - **MD5:** A legacy hash function with 128-bit output, less secure.
 - **SHA1:** Produces a 160-bit hash, more secure than MD5 but considered weaker than newer algorithms.
 - **SHA256:** A secure option that generates a 256-bit hash, recommended for most environments.
 - **SHA512:** The strongest hash option with a 512-bit output, providing the highest security.
- **Key Integrity:**

- **Key Integrity** settings define how often the IKE keys should be re-evaluated and renegotiated to maintain security. Regularly rekeying helps protect against potential security breaches.
- **IKE Lifetime:**
 - **IKE Lifetime** specifies the duration (in seconds) that the IKE Security Association (SA) remains active before it needs to be renegotiated. A shorter lifetime increases security by frequently re-establishing keys, but it can impact performance.
- **Lifetime:**
 - **Lifetime** refers to the overall duration (in seconds) that the IPsec SA remains active. Similar to IKE Lifetime, this setting controls how often the tunnel keys are refreshed, balancing security and performance.
- **DPD Delay (Dead Peer Detection Delay):**
 - **DPD Delay** is the interval (in seconds) between sending DPD requests to the remote peer to check if it is still responsive. This helps detect if the remote peer has gone offline or is unreachable.
- **DPD Timeout:**
 - **DPD Timeout** defines the maximum time (in seconds) to wait for a response to a DPD request before considering the peer to be dead or unresponsive. After this period, the VPN connection may be terminated or renegotiated.
- **DPD Action:**
 - **DPD Action** specifies what action to take if the remote peer does not respond within the DPD timeout period:
 - **Clear:** The tunnel is immediately brought down.
 - **Hold:** The tunnel remains up but is in a waiting state until the peer responds.
 - **Restart:** The tunnel is automatically renegotiated to restore connectivity.
- **Authentication Mode (Preshared Key, X.509 Certificate):**
 - **Authentication Mode** determines how the VPN peers authenticate each other:
 - **Preshared Key:** A simple method where both peers share a secret key. This is easier to set up but less secure than certificates.
 - **X.509 Certificate:** Uses digital certificates to authenticate peers. This method is more secure and scalable, suitable for environments requiring strong authentication.
- **Preshared Key:**
 - If **Preshared Key** is selected as the authentication mode, this field is used to enter the shared secret key that will be used to authenticate the connection. It should be strong and kept confidential to prevent unauthorized access.

4.2.6 User Manager

The User Manager Configuration menu provides a robust interface for managing user access and permissions on the PM2212 modem-router. This feature is crucial for maintaining security and ensuring that only authorized personnel can modify or view the device's configuration.

- **Create User Accounts:**

- Within the **User Manager Configuration**, administrators can create accounts for new users. Each user account is associated with a unique username and password, ensuring that access to the modem-router is both controlled and traceable.
- **Password Configuration:**
 - The **User Manager** allows for the configuration of passwords for each user account. Administrators can enforce strong password policies to enhance security, requiring passwords to meet specific complexity requirements, such as a minimum length, the inclusion of special characters, and regular password updates.
- **Fine-Grain Access Definition:**
 - One of the key features of the **User Manager** is the ability to define fine-grain access controls for each user. This allows administrators to specify exactly which configurations and functionalities each user can access or modify. The options include:
 - **Full Access:** Grants complete control over all modem settings and configurations.
 - **Read-Only Access:** Users can view configurations and logs but cannot make any changes.
 - **Denied Access:** Administrators can explicitly deny access to specific sections or functionalities of the modem. Users with **Denied Access** cannot view or modify the restricted areas, ensuring that sensitive configurations remain secure.

5 ROLLBACK MECHANISM

The Rollback feature means that if, after making changes to the settings, especially in the network or firewall, access to the device is lost or an issue arises, the system automatically reverts to the previous settings. This feature helps prevent problems with device accessibility.

How the Rollback feature works:

1. Configuration changes: When you make changes to network or firewall settings (e.g., changing the IP or DHCP settings), the system saves the changes.
2. Rollback Timer: After applying the changes, the system starts a timer (usually 30 seconds). If you don't confirm the changes within this time, the system automatically reverts to the previous settings.
3. Confirming the changes: If everything works correctly and access to the device is maintained, you need to confirm the changes to deactivate the timer and finalize the adjustments.
4. Reverting to the previous state (Rollback): If you lose access to the device or if the changes disrupt access within the timer period, the system automatically returns to the previous settings.

Benefits:

- 1- Enhanced security: If any changes result in loss of access to the device, the system automatically reverts to the previous settings.

2- Reduced risk: When making sensitive network changes, you no longer need to worry about losing access to the router.

This feature is especially useful when you're remotely connected to the device and making network changes.

6 KEY CONTACTS

7 REGULATORY REQUIREMENTS

The PM2212 modem-router is designed to meet various regulatory requirements to ensure safe operation, compliance with legal standards, and environmental responsibility. Below is an outline of the key regulatory requirements applicable to the PM2212:

1. Electrical Safety Standards

- **CE Marking (Conformité Européenne):**
 - The PM2212 complies with the CE marking requirements, ensuring it meets the safety, health, and environmental protection standards for products sold within the European Economic Area (EEA).
- **UL Certification:**
 - The device is certified by Underwriters Laboratories (UL) for electrical safety, indicating that it has been tested and meets the safety standards for electrical devices in the United States and Canada.
- **IEC 60950-1/IEC 62368-1:**
 - The PM2212 conforms to the International Electrotechnical Commission (IEC) standards for safety in information technology and audio/video equipment.

2. Electromagnetic Compatibility (EMC)

- **FCC Part 15:**
 - The device complies with the Federal Communications Commission (FCC) Part 15 regulations for electromagnetic interference (EMI) in the United States, ensuring that it does not cause harmful interference to radio communications.
- **EN 55032/EN 55024:**
 - The PM2212 adheres to the European standards for EMC, including emission requirements (EN 55032) and immunity requirements (EN 55024) for information technology equipment.
- **CISPR 32:**
 - Compliance with the International Special Committee on Radio Interference (CISPR) standards ensure the device limits its electromagnetic emissions to prevent interference with other electronic devices.

3. Radio Frequency (RF) Compliance

- **FCC Part 22/24/27:**

- The PM2212 is compliant with FCC regulations governing RF devices, including the use of frequencies for mobile communications in the U.S.
- **ETSI EN 301 511/ETSI EN 301 908:**
 - The device meets the European Telecommunications Standards Institute (ETSI) standards for RF communications, ensuring proper operation within European mobile networks.
- **SAR (Specific Absorption Rate):**
 - The PM2212 conforms to SAR limits for RF exposure, ensuring the device is safe for use in proximity to humans.

4. Environmental and Energy Standards

- **RoHS (Restriction of Hazardous Substances):**
 - The PM2212 is RoHS compliant, meaning it is manufactured without the use of hazardous materials such as lead, mercury, and cadmium, in accordance with EU Directive 2011/65/EU.
- **WEEE (Waste Electrical and Electronic Equipment):**
 - The device complies with the WEEE directive, requiring proper recycling and disposal of electronic equipment to minimize environmental impact.
- **Energy Efficiency:**
 - The modem-router meets energy efficiency standards, including compliance with the European Union's Energy-related Products Directive (ErP) and the U.S. Energy Star program, ensuring low power consumption and reduced environmental impact.

5. Telecommunications Compliance

- **GSM/UMTS/LTE Network Certification:**
 - The PM2212 is certified for operation on GSM, UMTS, and LTE networks, ensuring compatibility with global mobile networks.
- **GPRS/EDGE/HSPA Certification:**
 - The device supports GPRS, EDGE, and HSPA standards, with certification for data transmission and mobile internet access across various regions.

6. International Approvals

- **IC (Industry Canada):**
 - The PM2212 is certified by Industry Canada, ensuring it meets Canadian regulatory requirements for radio and telecommunications equipment.
- **ACMA (Australian Communications and Media Authority):**
 - The device is compliant with ACMA standards, ensuring it meets Australian regulatory requirements for EMC and telecommunications equipment.
- **Telec (Japan):**
 - The PM2212 is certified by the Telecommunications Engineering Center (Telec) in Japan, indicating compliance with Japanese radio and telecommunications standards.

7. Product Labeling and Documentation

- **Product Labels:**
 - The PM2212 includes labels indicating compliance with applicable regulatory standards, such as the CE mark, FCC ID, and other relevant certifications.
- **User Manual and Safety Information:**
 - The device is accompanied by a user manual and safety information that provides guidance on safe operation, regulatory compliance, and proper disposal of the product.

8. Compliance Responsibility

- **Manufacturer's Declaration of Conformity:**
 - The manufacturer of the PM2212 provides a Declaration of Conformity, stating that the product meets all applicable regulatory requirements.
- **Ongoing Compliance Monitoring:**
 - The manufacturer is responsible for ensuring that all products continue to meet regulatory requirements through regular testing and quality control measures.

8 FAQs

8.1 GENERAL QUESTIONS

1. **What is the PM2212 modem-router?**
 - The PM2212 is an industrial modem-router that converts 12 RS485 ports and 2 RS232 ports into Ethernet, Wi-Fi, and GPRS connections, offering robust communication solutions for various industrial applications.
2. **What types of network interfaces does the PM2212 support?**
 - The PM2212 supports Ethernet, Wi-Fi, and GPRS network interfaces, allowing flexible and reliable connectivity in diverse environments.
3. **What is the input power range for the PM2212?**
 - The modem-router operates with an input power range between 8 and 25 volts, and it includes an industrial power supply with an input of 110 V to 250 V DC/AC and an output of 12 V DC, which is DIN-RAIL mounted.
4. **How many SIM cards can the PM2212 support?**
 - The PM2212 supports two SIM cards, which can be configured to work asynchronously for redundancy or network failover.
5. **What are the main features of the PM2212's web interface?**
 - The web interface offers comprehensive configuration and monitoring options, including status monitoring, system management, network configuration, VPN setup, and more.

8.2 HARDWARE AND INSTALLATION

6. **What do the LED indicators on the PM2212 signify?**

- The LEDs display signal strength, SIM card status, WWAN network connection, device status, APN connection state, WLAN status, and TX/RX activity on the serial ports.
7. **How can I mount the PM2212?**
- The PM2212 is designed for DIN-RAIL mounting, making it suitable for industrial environments where secure and stable installation is required.
8. **What is the maximum baud rate supported by the RS232 and RS485 ports?**
- The baud rate for each RS232 and RS485 port can be individually configured based on the specific requirements of your application.
9. **Can I use the PM2212 with existing industrial equipment?**
- Yes, the PM2212 is designed to integrate with existing industrial systems through its RS232 and RS485 ports, providing a reliable means of connecting legacy equipment to modern networks.
10. **What is the function of the SIM card manager?**
- The SIM card manager allows you to activate and manage the two SIM card slots, with options for auto-selection, or manual selection of SIM 1 or SIM 2.

8.3 NETWORK CONFIGURATION

11. **How do I access the PM2212's web interface?**
- You can access the configuration and monitoring interface via a web browser by entering the device's IP address. The main menu provides access to various configuration options, including network, VPN, and firewall settings.
12. **What VPN protocols does the PM2212 support?**
- The PM2212 supports IPsec VPN configurations with options for remote ID, subnets, encapsulation modes, IKE protocols, encryption algorithms, and authentication methods.
13. **Can I configure multiple network interfaces on the PM2212?**
- Yes, the Interfaces submenu allows you to add, delete, edit, and manage multiple network interfaces, including Ethernet and wireless connections.
14. **What is the purpose of the DHCP and DNS features in the PM2212?**
- The modem-router includes a lightweight DHCP server and DNS forwarder, allowing it to manage IP address assignments and DNS requests within your network.
15. **How do I set up port forwarding on the PM2212?**
- Port forwarding is configured through the firewall settings in the web interface. You can specify rules for remote access to specific services on your network.

8.4 SECURITY AND MANAGEMENT

16. How does the PM2212 handle network security?

- The PM2212 includes robust firewall functionality with options for traffic rules, NAT rules, IP sets, and brute force protection to control and secure network traffic.

17. Can I backup and restore the PM2212's configuration?

- Yes, the backup/flash firmware feature allows you to back up your current configuration and restore it if needed, as well as update the device's firmware.

18. How do I manage user access to the PM2212?

- The user manager allows you to create accounts for new users, set passwords, and define access levels, ensuring that only authorized personnel can modify device settings.

19. What happens if the network connection fails?

- The daily reboot feature can be configured to take specific actions if a destination host becomes unreachable, helping to maintain continuous network operation.

20. Can the PM2212 be used in a high-security environment?

- Yes, the device supports advanced security features such as IPsec VPNs, firewall protection, SSH access, and HTTPS management, making it suitable for deployment in secure and critical environments.

8.5 FIREWALL RULES

21. How do I configure firewall rules on the PM2212?

- Firewall rules can be configured via the Traffic Rules tab in the firewall settings. You can define how traffic is treated by setting rules based on criteria such as source/destination IP, protocol, and ports, and specify actions like accept, drop, or reject.

22. What is the purpose of the Port Forwarding tab in the firewall settings?

- The Port Forwarding tab allows you to set up rules for directing incoming traffic from the WAN to specific devices or services within your local network, enabling remote access to those services.

23. What is the difference between NAT rules and Traffic Rules?

- NAT rules manage how IP addresses are translated between networks, such as translating private IP addresses to a public IP for internet access. Traffic Rules define how the device processes packets based on specific criteria, such as allowing or blocking traffic.

24. Can I create custom zones in the firewall?

- Yes, in the Zone Settings pane under General Settings, you can create custom zones to group network interfaces and apply specific rules for traffic entering or leaving those zones.

25. How does the PM2212 handle brute force attacks?

- The Brute Force Protection tab allows you to set parameters to ban IP addresses that make too many failed logins attempts within a specified time, protecting the device from unauthorized access attempts.

26. What is the purpose of the IP Sets tab in the firewall?

- The IP Sets tab allows you to create groups of IP addresses that can be referenced in firewall rules, simplifying the management of multiple IP addresses that share common rule sets.

27. How can I enable SYN-flood protection on the PM2212?

- SYN-flood protection can be enabled in the General Settings pane under the firewall settings. This feature helps protect the device from DDoS attacks by controlling the rate of incoming SYN packets.

8.6 VPN CONFIGURATION

28. How do I set up an IPsec VPN on the PM2212?

- IPsec VPN setup is done via the VPN configuration section. You can configure remote and local IDs, subnets, encapsulation mode, IKE protocol, encryption, hash methods, and authentication modes (preshared key or certificate).

29. What is the difference between IKEv1 and IKEv2 in the VPN settings?

- IKEv1 and IKEv2 are different versions of the Internet Key Exchange protocol used in IPsec VPNs. IKEv2 is the more modern and efficient protocol, offering improved security and faster setup times compared to IKEv1.

30. How do I manage VPN connection lifetimes on the PM2212?

- In the VPN settings, you can configure the IKE lifetime and IPsec lifetime parameters to control how long the VPN connection remains active before renegotiation is required, ensuring secure and continuous communication.

APPENDIX A: OPERATIONS AND MAINTENANCE MANUAL APPROVAL

The undersigned acknowledge they have reviewed the *<Project Name>* **Operations and Maintenance Manual** and agree with the approach it presents. Changes to this **Operations and Maintenance Manual** will be coordinated with and approved by the undersigned or their designated representatives.

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

Signature: _____ Date: _____
Print Name: _____
Title: _____
Role: _____

APPENDIX B: KEY TERMS

The following table provides definitions for terms relevant to this document.

Term	Definition
RS485	A standard defining the electrical characteristics of drivers and receivers for use in balanced digital multipoint systems.
RS232	A standard for serial communication transmission of data, used for connecting peripherals to a computer.
Ethernet	A network technology for wired local area networks (LANs), using data frames for communication over physical media such as cables.
Wi-Fi	A wireless networking technology that allows devices to connect to the internet or communicate with one another wirelessly within a particular area.
GPRS	General Packet Radio Service, a mobile data standard on 2G and 3G cellular communication networks.
SIM Card	A small card inserted into a mobile device, storing subscriber information and allowing access to a cellular network.
IPsec	Internet Protocol Security, a suite of protocols used to secure internet communications by authenticating and encrypting each IP packet in a communication session.
IKE Protocol (v1/v2)	Internet Key Exchange, a protocol used to set up a secure and authenticated communication channel, with v1 being the original version and v2 the improved version.
3DES	Triple Data Encryption Standard, a symmetric-key block cipher used for encryption.
AES	Advanced Encryption Standard, a symmetric encryption algorithm widely used across the globe to secure data.
SHA	Secure Hash Algorithm, a family of cryptographic hash functions designed to ensure data integrity.
Preshared Key	A secret key shared between two parties before use in a cryptographic protocol, used for authentication in VPNs.
X.509 Certificate	A digital certificate that uses the X.509 standard to verify

	the identity of a party in a secure communication session.
NAT (Network Address Translation)	A method used in routers to remap one IP address space into another by modifying network address information in the IP header of packets while they are in transit.
DPD (Dead Peer Detection)	A method used in VPNs to detect whether the remote peer is still active and reachable.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
DHCP	Dynamic Host Configuration Protocol, a network management protocol used to dynamically assign an IP address to each device on a network.
DNS	Domain Name System, a hierarchical system for translating human-friendly domain names into IP addresses.
SNMP	Simple Network Management Protocol, used for managing devices on IP networks.
SSH	Secure Shell, a cryptographic network protocol for secure data communication and remote command-line login.
WAN	Wide Area Network, a telecommunications network that extends over a large geographic area for the purpose of computer networking.
LAN	Local Area Network, a network that connects computers within a limited area such as a residence, school, or office building.
Encapsulation Mode	A mode that determines how data packets are encapsulated within a VPN tunnel (Tunnel or Transport mode).
SIM Selection Mode	The mode in which the modem selects which SIM card to use, with options for automatic selection or manual selection of SIM 1 or SIM 2.
APN	Access Point Name, the name of a gateway between a mobile network and another computer network, often the public internet.
Baud Rate	The rate at which information is transferred in a communication channel, measured in symbols (or pulses) per second.
DDOS Protection	A security feature that protects against Distributed Denial-of-Service (DDoS) attacks, which attempt to overwhelm a network or service with excessive traffic.
LED Indicator	A light-emitting diode used to indicate the status of various functions and connections on the modem-router

	(e.g., signal strength, SIM card status).
Signal Strength	The measure of the power level received by a wireless communication device, often displayed via LED indicators.
Firmware	The permanent software programmed into a device's read-only memory, which provides low-level control for the device's specific hardware.
DIN-Rail	A metal rail of a standard type widely used for mounting circuit breakers and industrial control equipment inside equipment racks.
Port Forwarding	A method of allowing external devices to access services on a private network by forwarding requests from a specific port to a device on the network.
Traffic Rules	Rules configured in a firewall to control how different types of traffic are handled, including allowing, blocking, or redirecting traffic.
Zone	In firewall configuration, a zone represents a group of interfaces that are treated with the same security rules and policies.
Masquerading	A form of network address translation (NAT) where the source IP address is changed to the IP address of the outbound interface.
Static Routing	A type of network routing where routes are manually entered and maintained by an administrator, as opposed to being dynamically updated by routing protocols.
SNAT (Source NAT)	A type of NAT where the source address of a packet is modified, typically used to allow multiple devices on a local network to share a single public IP address.
Brute Force Protection	A security mechanism that blocks repeated login attempts from a single IP address, typically used to prevent unauthorized access through password guessing.
Time Synchronization	The process of coordinating the system time of a device with a reference time source, such as an NTP (Network Time Protocol) server.
Syslog	A standard for message logging that allows the collection of log messages from various devices and applications on a network for monitoring and analysis.
NTP (Network Time Protocol)	A protocol used to synchronize the clocks of computers over a network to a precise time reference.
Flow Offloading	A feature that improves packet processing performance by offloading certain tasks from the main CPU to dedicated

	hardware or software processing.
Packet Steering	A technique used to distribute incoming network packets across multiple CPU cores to enhance processing efficiency in multi-core systems.
IKE Lifetime	The duration for which an IKE (Internet Key Exchange) session remains valid before needing to be renegotiated.
DPD (Dead Peer Detection)	A mechanism in VPNs to detect the loss of connectivity with the remote peer and take corrective action.
Remote ID	The identifier used by the remote VPN gateway to establish a connection.
Local ID	The identifier used by the local VPN gateway in the IPsec tunnel configuration.