Development Documention of DR185

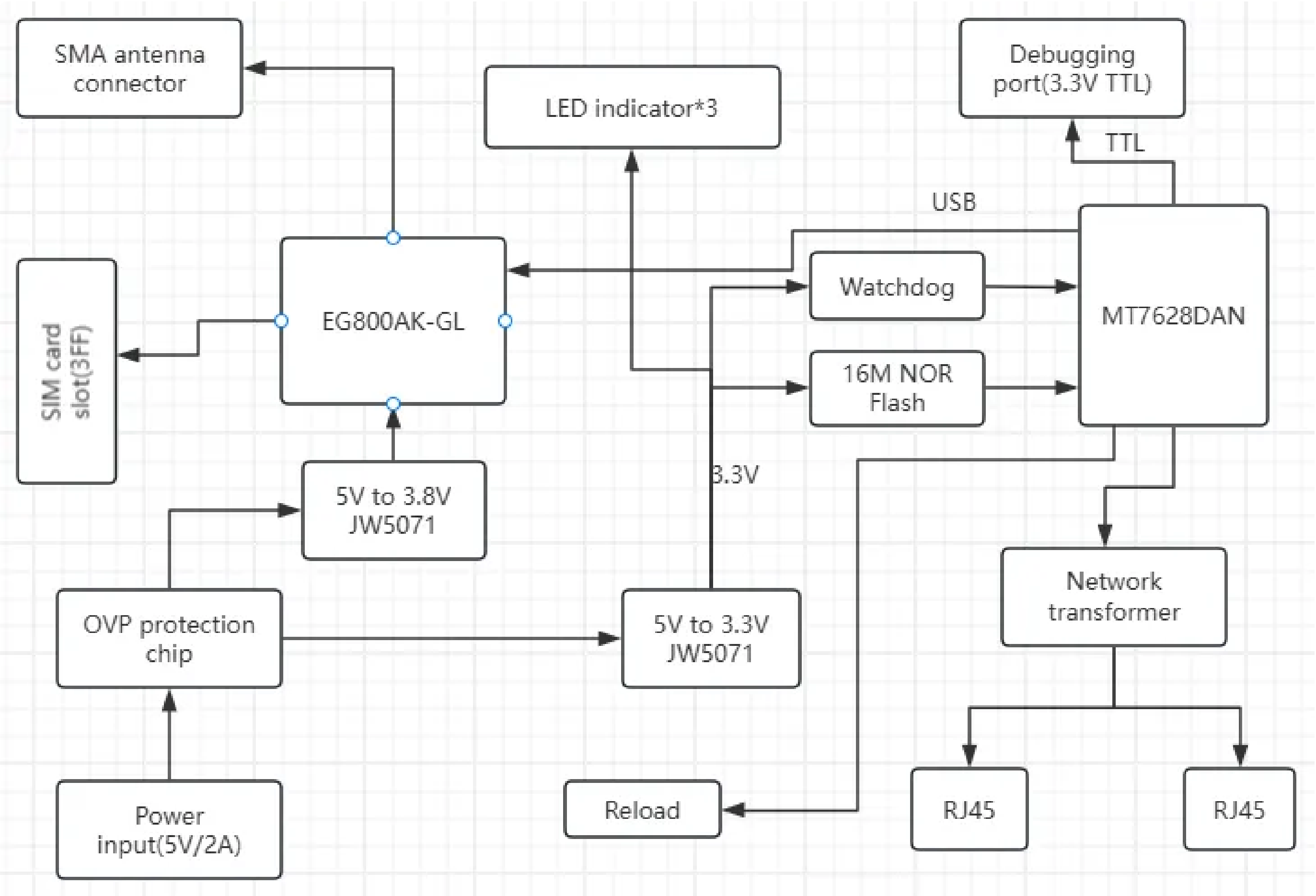
USR-DR185 Overview

USR-DR185 is an LTE Cat 1 industrial router designed for industrial IoT applications, featuring extensive open-source capabilities for secondary development. Based on the OpenWrt system, it provides a complete SDK and programmable interfaces for easy customization and integration. The device offers stable cellular network connectivity and two Ethernet ports, facilitating local device networking.

Hardware Specifications

Diagram

图片加载失败



Processor

- **CPU:** MediaTek MT7628DAN
- **RAM:** 64MB
- **FLASH:** 16MB Flash

Cellular

- **Module Model:** EG800AK–GL

  LTE–FDD: B1/ 2/ 3/ 4/ 5/ 7/ 8/ 12/ 13/ 14 17/ 18/ 19/ 20/ 25/ 26/ 28/ 66/ 71

  LTE–TDD: B34/ 38/ 39/ 40/ 41
- **Network Standard:** LTE Cat 1
- **Antenna Connector:** SMA female
- **SIM:** Micro–SIM（3FF）

Ethernet

- **Ethernet Ports**: 2× RJ45
- **Speed**: 10/100Mbps Auto-negotiation
- **Configuration**: 1 x WAN/LAN + 1 x LAN

Indicator

- **system**: System status indicator—flashes during startup, stays solid during normal operation, blinks rapidly during firmware updates, and blinks slowly in fail-safe mode.
- **NET-green**: Cellular network green indicator (strong signal).
- **NET-blue**: Cellular network blue indicator (medium signal).
- **NET-red**: Cellular network red indicator (weak signal).

Buttons

- **reset**: Reset button—short press (<1 second) to reboot the device; long press (>5 seconds and release) to restore factory settings.

Power

- **Power input connector**: XH 2.54 connector
- **Input voltage**: DC 5V ±5%
- **Working current**: ⩽2A
- **Rated power**: 10W

Debugging Interface

- **Type**: 4-Pin serial port
- **Signal level**: 3.3V TTL
- **Baud rate**: 57600 bps
- **Data bits**: 8 bit
- **Stop bits**: 1 bit
- **Parity bit**: None
- **Flow control**: None

Physical Characteristics

- **Operating Temperature:** –25℃ ~ +75℃

Pin Description

LED Indicator Pin

Items	GPIO	Label	Active Level
system	GPIO#3	system	GPIO_ACTIVE_HIGH
wwan–red	GPIO#0	wwan–red	GPIO_ACTIVE_HIGH
wwan–green	GPIO#2	wwan–green	GPIO_ACTIVE_HIGH
wwan–blue	GPIO#44	wwan–blue	GPIO_ACTIVE_HIGH

Cellular Module Pin

Function	GPIO	Label	Active Level	Device Tree Configuration
Power control	GPIO#41	wwan–power	GPIO_ACTIVE_HIGH	Exported as a manually controllable GPIO signal, defaults to high–level output

Button Pin

Function	GPIO	Label	Active Level	Device Tree Configuration

Reset	GPIO#11	reset	GPIO_ACTIVE_LOW	Polled GPIO button; triggers a KEY_RESTART event when pressed

Watchdog Pin

Function	GPIO	Label	Active Level	Device Tree Configuration
Watchdog Trigger	GPIO#39	(None)	GPIO_ACTIVE_LOW	Implements watchdog functionality by toggling the signal level every 35 seconds using a hardware toggle algorithm.

SPI Flash

DR185 uses 16MB SPI NOR Flash with the following partition layout:

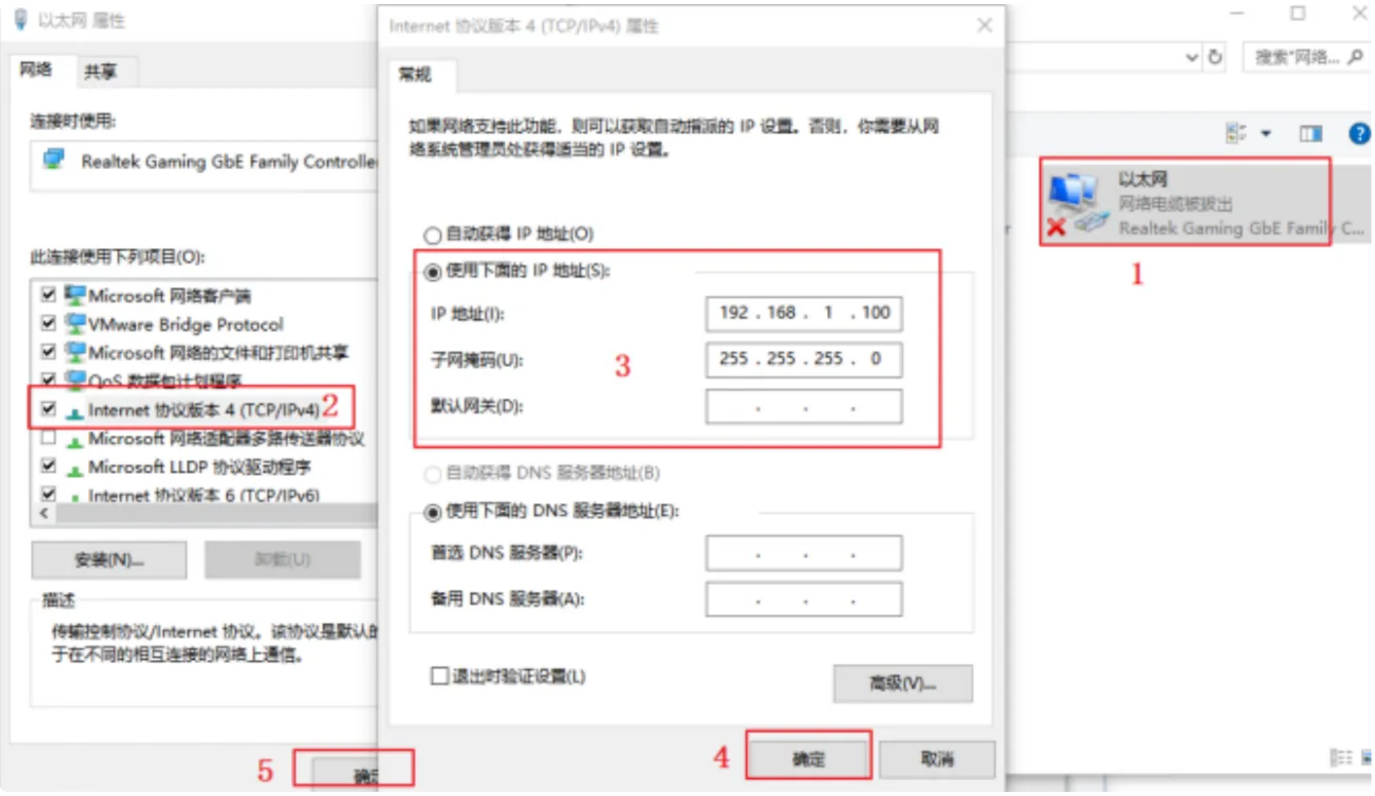
Partition	Start Address	Size	Attributes	Description
u-boot	`0x0`	`0x30000` (192 KB)	`read-only`	Stores the system bootloader (U-Boot)（U-Boot)
u-boot-env	`0x30000`	`0x10000` (64K B)	`read-only`	Stores U-Boot environment variables

factory	`0x40000`	`0x10000` (64KB)	Read/Write	Stores unique device calibration data (e.g., MAC address, wireless parameters)
firmware	`0x50000`	`0xea0000` (~14.63MB)	Read/Write	**Core firmware**, containing the kernel and a read-only root file system
factory_bk	`0xef0000`	`0x10000` (64KB)	Read/Write	Backup partition for `factory` (Unused)
config_bk	`0xf00000`	`0x80000` (512KB)	Read/Write	**Backup partition for UCI configuration**(unused)
backup_mnt	`0xf80000`	`0x80000` (512KB)	Read/Write	**Parameter snapshot partition**, for storing system state snapshots, etc. (unused)

Firmware Flashing

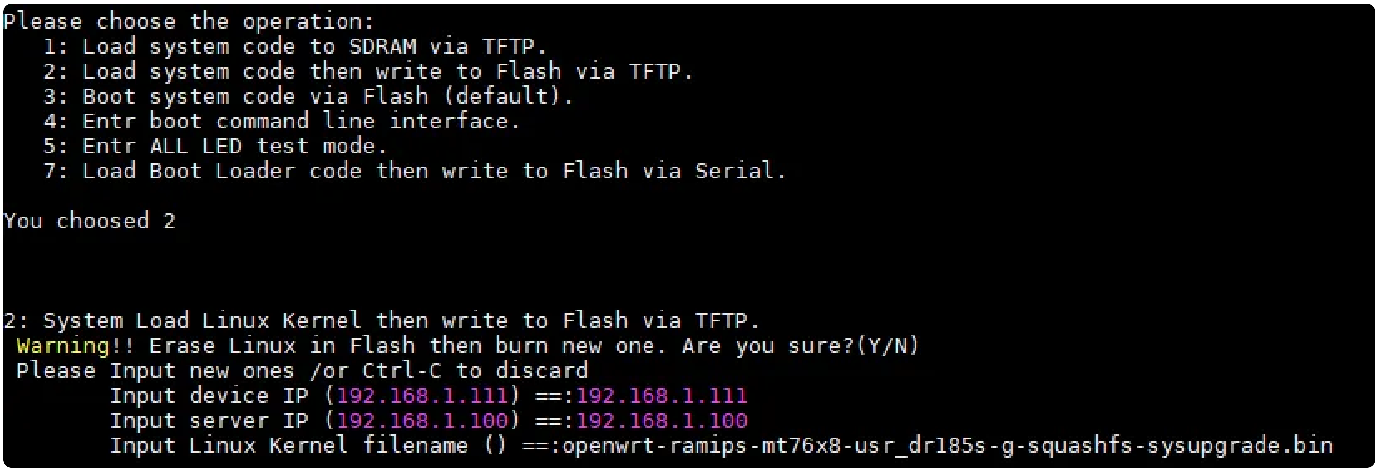
Flashing via U-Boot

1. Configure the computer's IP address as static. Reference configuration below:

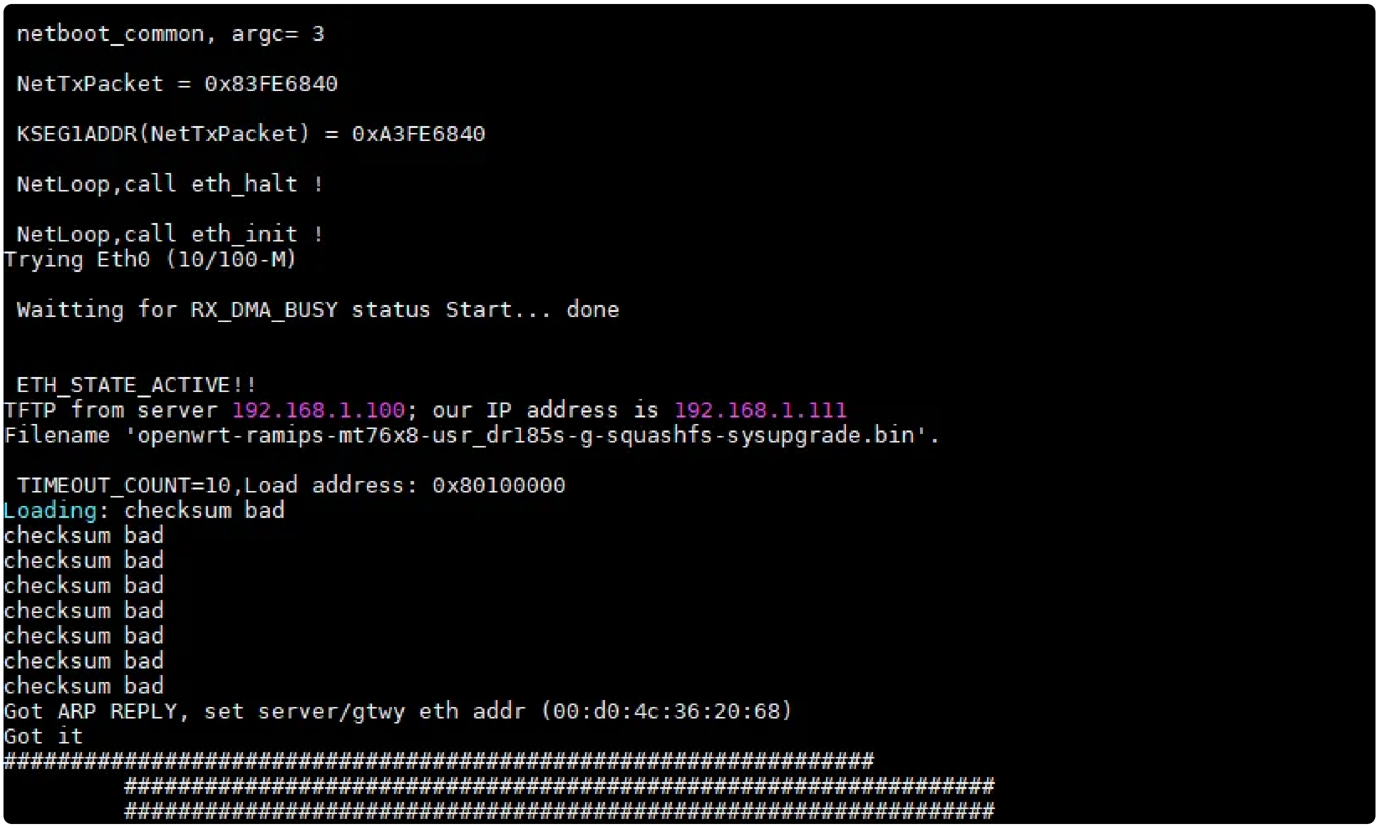


以太网 属性
网络
共享
连接时使用:
Realtek Gaming GbE Family Controlle
此连接使用下列项目(O):
☑ Microsoft 网络客户端
☑ VMware Bridge Protocol
☑ Microsoft 网络的文件和打印机共享
☑ QoS 数据包计划程序
☑ Internet 协议版本 4 (TCP/IPv4)
2
□ Microsoft 网络适配器多路传送器协议
☑ Microsoft LLDP 协议驱动程序
☑ Internet 协议版本 6 (TCP/IPv6)
安装(N)...
卸载(U)
描述
传输控制协议/Internet 协议。该协议是默认的
于在不同的相互连接的网络上通信。
5
确定
Internet 协议版本 4 (TCP/IPv4) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。
○ 自动获得 IP 地址(O)
● 使用下面的 IP 地址(S):
IP 地址(I): 192 . 168 . 1 . 100
子网掩码(U): 255 . 255 . 255 . 0
默认网关(D): . . .
3
○ 自动获得 DNS 服务器地址(B)
● 使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): . . .
备用 DNS 服务器(A): . . .
□ 退出时验证设置(L)
高级(V)...
4
确定
取消
搜索"网络...
以太网
网络电缆被拔出
Realtek Gaming GbE Family C...
1

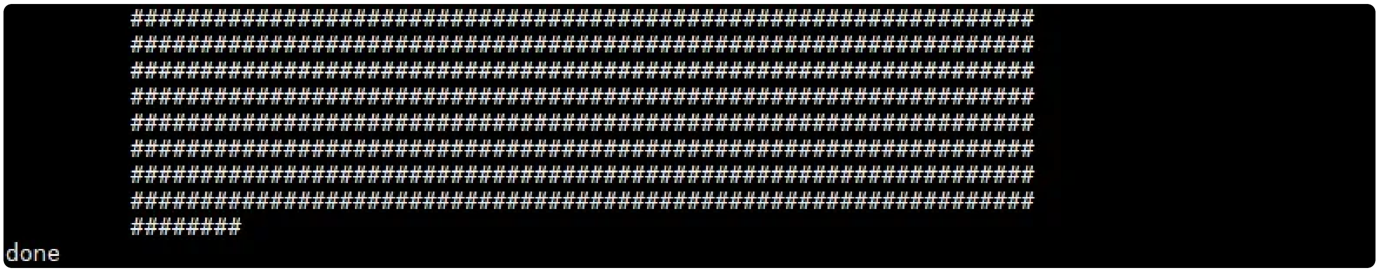
2. Start the TFTP service using tftpd32.
3. Connect the DR185's Ethernet port directly to the computer via an Ethernet cable, or connect it to the same LAN as the computer.
4. Connect the debug serial port using a serial cable first, then power on the device. When "Please choose the operation:" appears, enter the number **2**, then enter **y**, Next, change the device IP to another IP address within the same subnet as the computer, change the server IP to the computer's IP, enter the firmware name for Linux Kernel filename and finally press Enter. Wait for the flashing to complete.
5. After successful flashing, **done** will be printed, and the device will reboot automatically.



```
Please choose the operation:
   1: Load system code to SDRAM via TFTP.
   2: Load system code then write to Flash via TFTP.
   3: Boot system code via Flash (default).
   4: Entr boot command line interface.
   5: Entr ALL LED test mode.
   7: Load Boot Loader code then write to Flash via Serial.

You choosed 2



2: System Load Linux Kernel then write to Flash via TFTP.
 Warning!! Erase Linux in Flash then burn new one. Are you sure?(Y/N)
 Please Input new ones /or Ctrl-C to discard
        Input device IP (192.168.1.111) ==:192.168.1.111
        Input server IP (192.168.1.100) ==:192.168.1.100
        Input Linux Kernel filename () ==:openwrt-ramips-mt76x8-usr_dr185s-g-squashfs-sysupgrade.bin
```



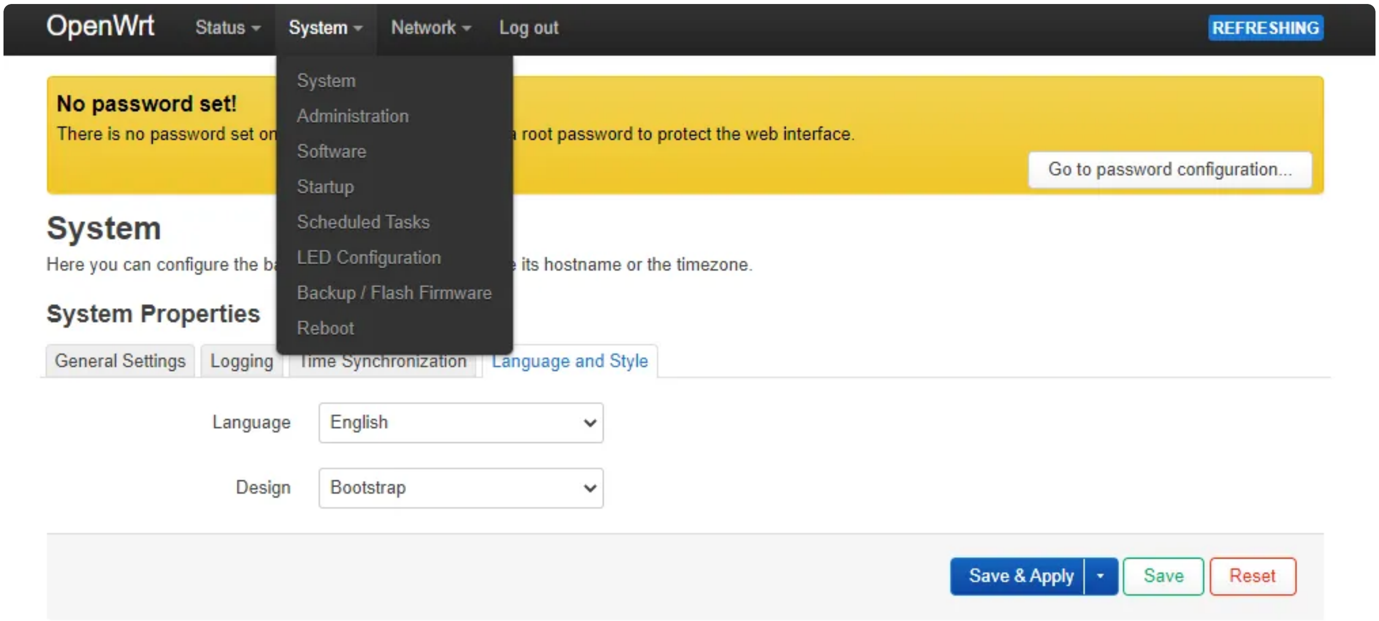
```
 netboot_common, argc= 3

 NetTxPacket = 0x83FE6840

 KSEG1ADDR(NetTxPacket) = 0xA3FE6840

 NetLoop,call eth_halt !

 NetLoop,call eth_init !
Trying Eth0 (10/100-M)

 Waitting for RX_DMA_BUSY status Start... done


 ETH_STATE_ACTIVE!!
TFTP from server 192.168.1.100; our IP address is 192.168.1.111
Filename 'openwrt-ramips-mt76x8-usr_dr185s-g-squashfs-sysupgrade.bin'.

 TIMEOUT_COUNT=10,Load address: 0x80100000
Loading: checksum bad
checksum bad
checksum bad
checksum bad
checksum bad
checksum bad
checksum bad
checksum bad
Got ARP REPLY, set server/gtwy eth addr (00:d0:4c:36:20:68)
Got it
#################################################################
         #################################################################
         #################################################################
```



```
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         ########
done
```

Flashing via Web Interface

1. Connect computer to DR185s-G via an Ethernet cable.
2. Log in to the web interface and navigate to **System → Backup/Flash firmware**.



No password set!

There is no password set on … root password to protect the web interface.

System

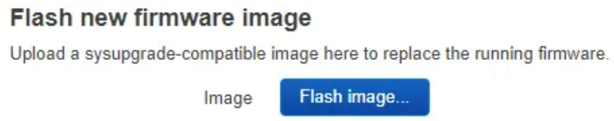
Here you can configure the b… its hostname or the timezone.

System Properties

Language: English

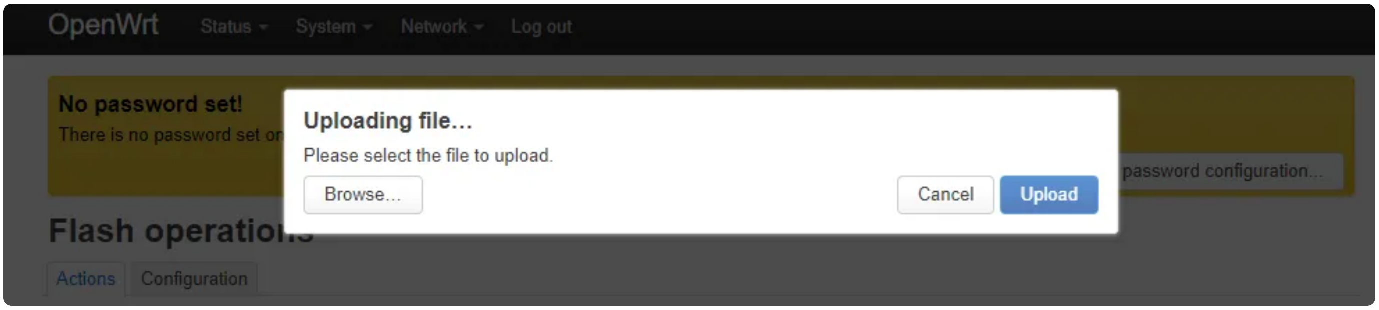
Design: Bootstrap

3. Click “**Flash image...**” to enter the upgrade page，click “**Browse...**” to select the image file，then click “**Upload**”，this will upload the firmware image file.



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware.



No password set!

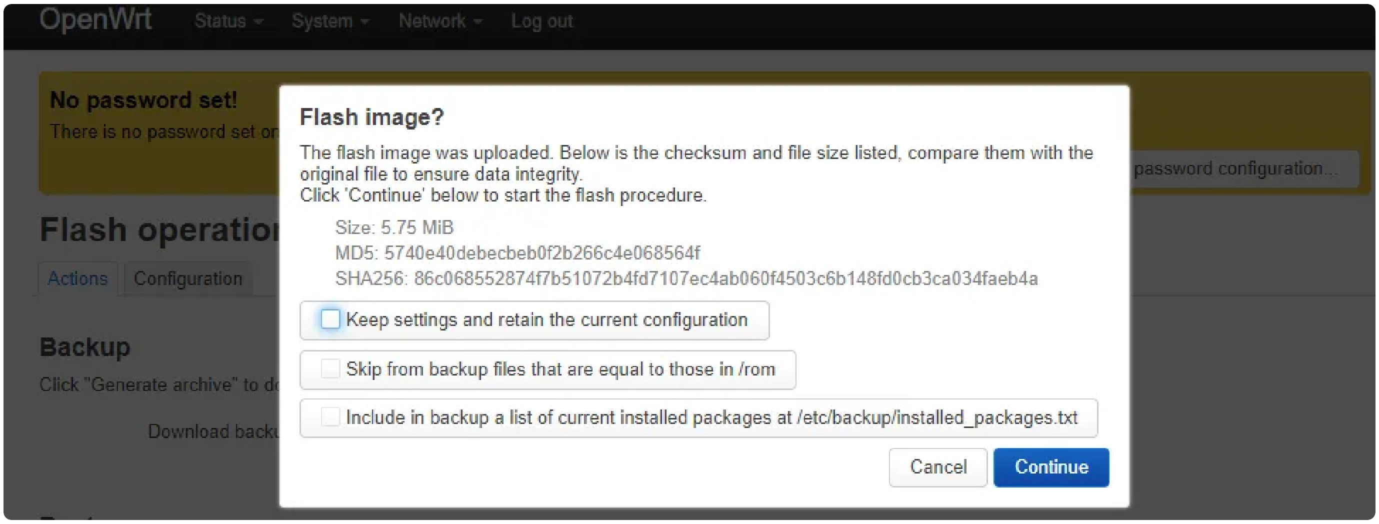
There is no password set or

Uploading file...

Please select the file to upload.

Flash operations

4. If you do not wish to keep the current configuration, uncheck “Keep settings and retain the current configuration”
5. If the checksum matches, click “Continue”. This will start the upgrade process, displaying a rotating progress bar and the message “DO NOT POWER OFF THE DEVICE!”
6. The process may take several minutes. The router will upload the firmware image, write it to flash ROM, and finally reboot.



Flash image?

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click 'Continue' below to start the flash procedure.

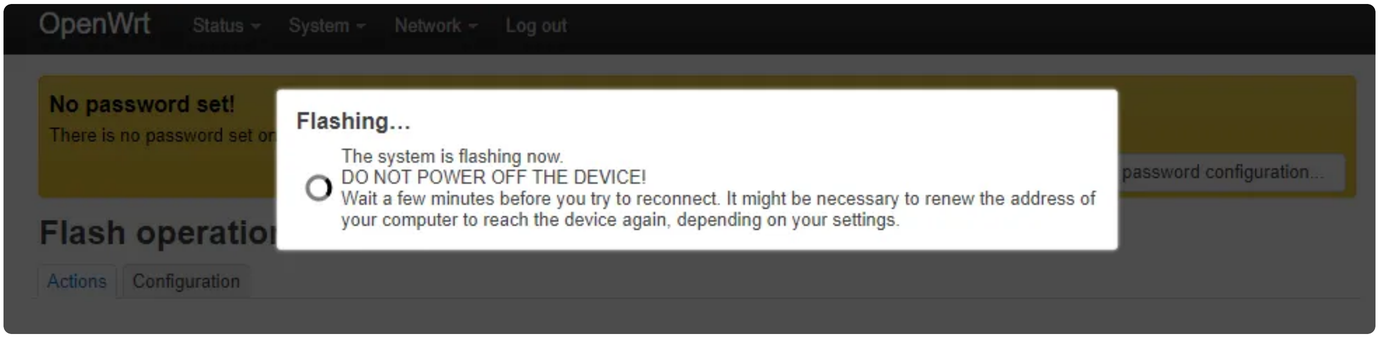
Size: 5.75 MiB
MD5: 5740e40debecbeb0f2b266c4e068564f
SHA256: 86c068552874f7b51072b4fd7107ec4ab060f4503c6b148fd0cb3ca034faeb4a

□ Keep settings and retain the current configuration

□ Skip from backup files that are equal to those in /rom

□ Include in backup a list of current installed packages at /etc/backup/installed_packages.txt

Cancel | Continue

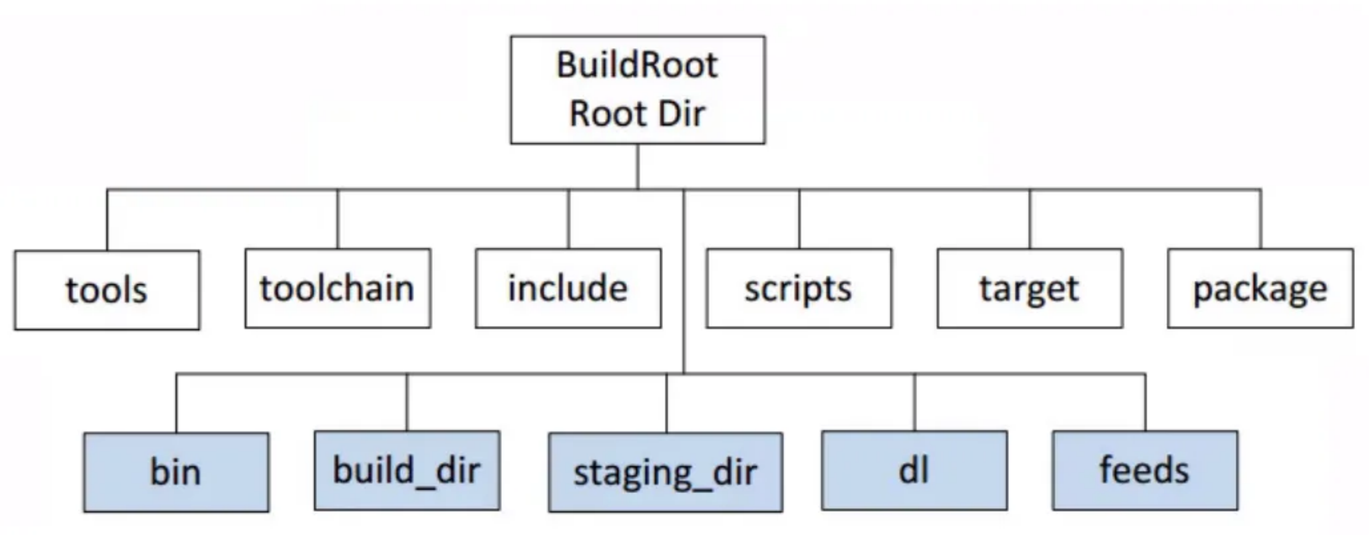


Flashing...

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

SDK Overview

openwrt Source code introduction



The above picture is the shows the directory structure of openwrt, The first row shows the original directories, and the second row shows the directories generated during the compilation process.

- tools – Contains the tools required for compilation and the commands to fetch and compile them. It consists of Makefiles, some may include patches. Each Makefile contains `$(eval $(call HostBuild))` , indicating the tool is compiled for host machine use.
- toolchain – Contains commands for fetching kernel headers,C library, bin–utils, compiler, debugger
- target – Defines the firmware and kernel compilation process for different platforms. Device tree files are located here.
- package – Contains Makefiles for individual software packages. OpenWrt defines a set of Makefile templates. Each package defines its own information, such as version, download URL, compilation method, and installation path, following this template.
- include – Stores OpenWrt's main Makefiles.
- scripts – Contains Perl scripts for package management.
- dl – Downloaded software packages are stored in this directory.
- build_dir – Software packages are extracted and compiled in this directory.
- staging_dir – The final installation directory. Tools, toolchain, and the root filesystem are installed here.
- feeds –Contains the software package suites required for the OpenWrt environment.
- bin – After compilation, the firmware and all ipk packages are placed in this directory.

Overview of PUSR programs

usr_cellular(Cellular Dialer Program)

This program employs a state machine architecture to manage the dial–up connection and network maintenance of the 4G module, ensuring automatic recovery in case of network abnormalities.

Configuration File

cellular is the cellular network configuration file for setting up connection parameters and network settings for the cellular module.

```
config cellular 'cellular'
    # APN address configuration method
    # autocheck: Automatically detect APN address
    # Alternatively, manually specify a specific APN address
    option apnaddr 'autocheck'

    # Authentication type
    # none: No authentication required
    # pap: PAP authentication
    # chap: CHAP authentication
    option authtype 'none'

  # PDP packet type
    # IPV4: IPv4-only connection
    # IPV6: IPv6-only connection
    # IPV4V6: IPv4/IPv6 dual-stack connection
    option pdptype 'IPV4V6'

    # PIN code enable status
    # 0: Disable PIN code verification
    # 1: Enable PIN code verification
    option pinenable '0'

    # SIM card PIN code
    # Used when pinenable is 1, for unlocking the SIM card
    option pincode '1234'

  # Heartbeat detection function switch
    # 0: Disable heartbeat detection
    # 1: Enable heartbeat detection
    option ping_en '1'

    # Heartbeat detection interval (seconds)
    # Sets the time interval for sending ping packets to the server to check network connectivity
    option ping_interval '10'

    # Primary ping server address
    # Primary server IP address used for network connectivity detection
    option ping_first '8.8.8.8'

    # Secondary ping server address
    # Alternative detection server used when the primary server is unavailable
    option ping_second '8.26.56.26'

    # Ping failure count threshold
    # Number of consecutive ping failures; exceeding this value indicates network abnormality
    option ping_fail_num '4'

    # SMS failure maximum count
    # Maximum retry count for SMS sending failures
    option sms_fail_max '3'

    # Maximum Transmission Unit (bytes)
    # Sets the maximum size of data packets; 1500 is the standard Ethernet MTU value
    option mtu  '1500'
```

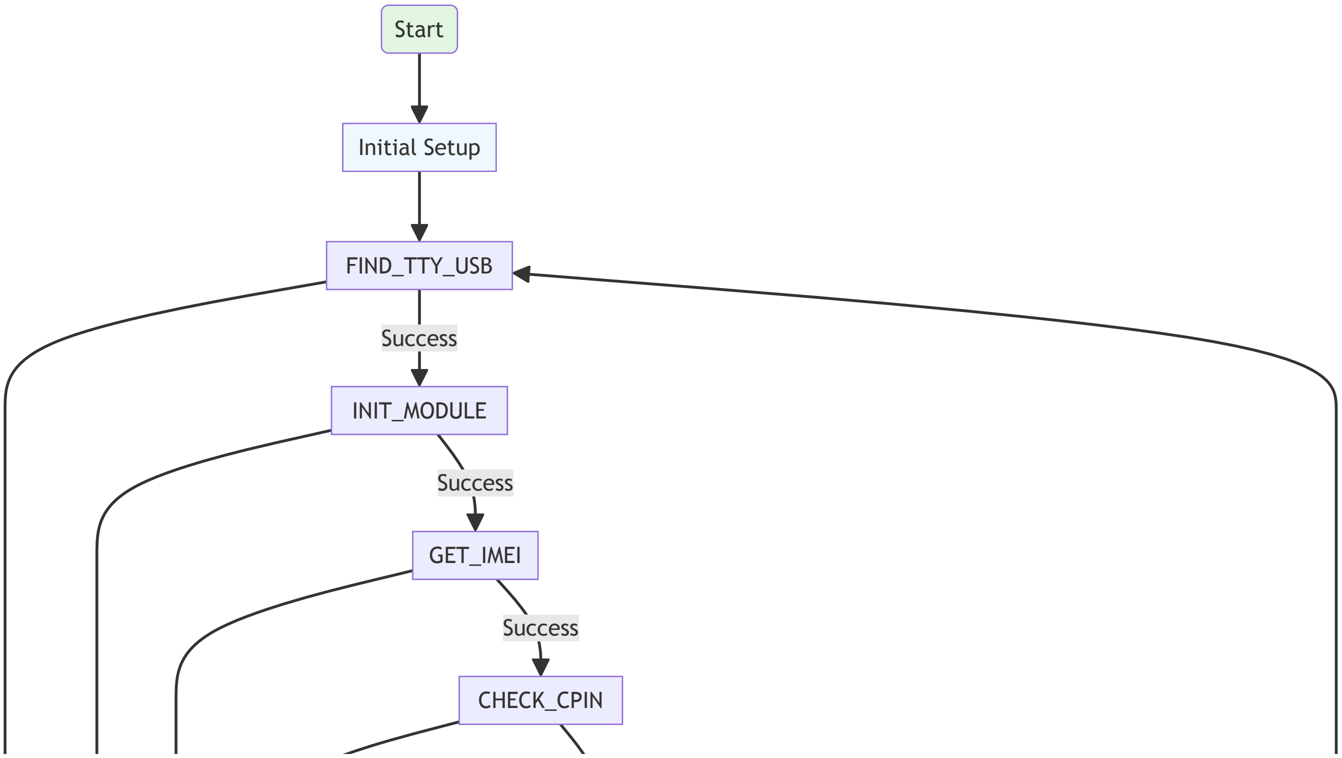
Startup Script

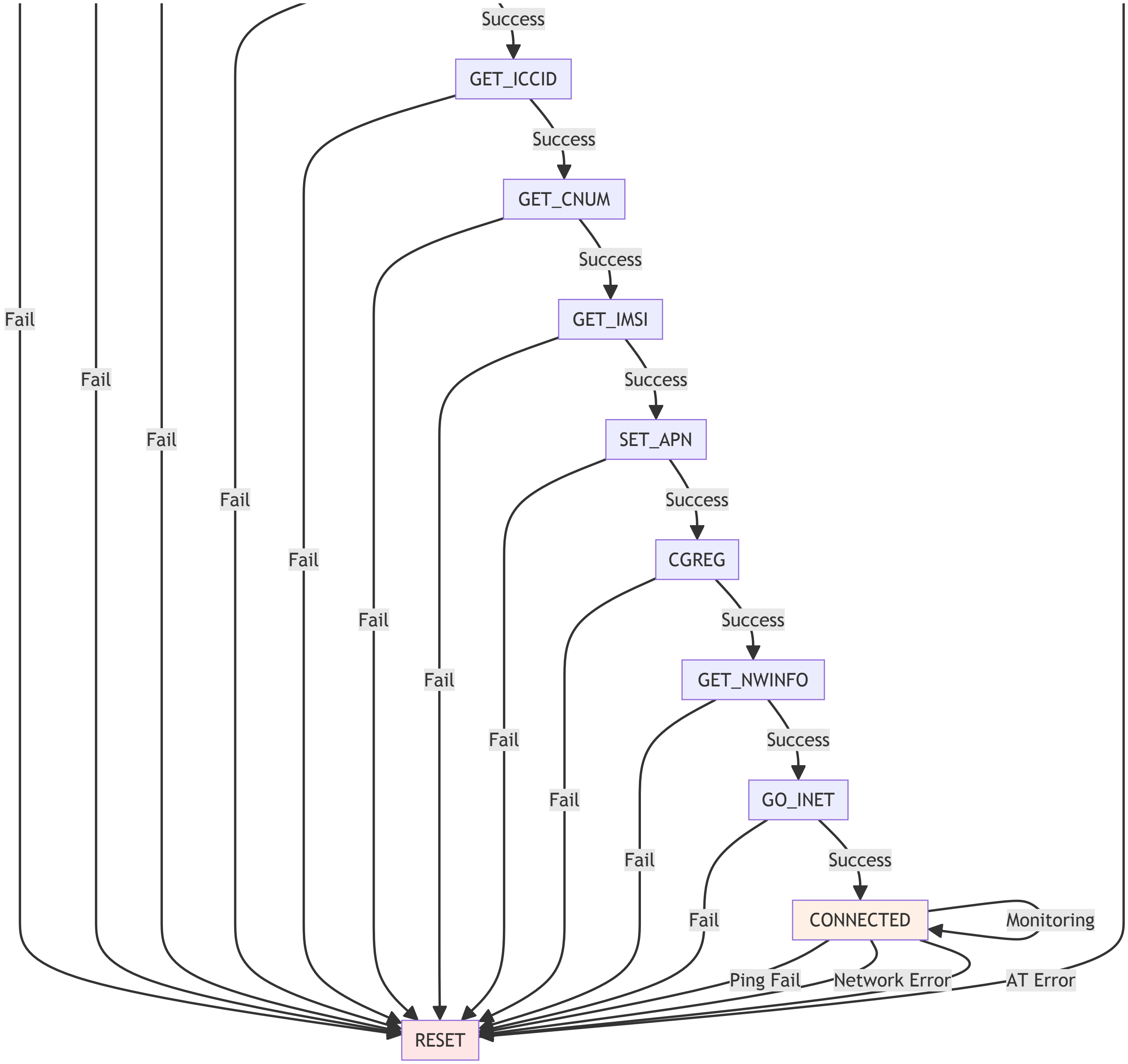
`usr_lte_service` is an auto-start script based on the **procd process management framework**.It automatically starts on device power-up and restarts the process if it exits abnormally.

Dialer Program

`usr_cellular` is the dialer program. This program employs a state machine architecture to manage the dial-up connection and network maintenance of the 4G module, ensuring automatic recovery in case of abnormalities.

State Machine Diagram





State Machine Detailed Workflow

Phase 1: Initial Setup

After program startup, it first reads system parameter configurations and sets the initial state to **LTE_STA_FINDTTYUSB**。

Phase 2: Sequential Dial-up

This phase consists of 11 mandatory sequential states. The next state is entered only upon successful completion of the current state. Failure in any state leads to a jump to the **LTE_STA_RESET** state, triggering a restart. The specific state flow is as follows:

1. **LTE_STA_FINDTTYUSB**：Locate and identify the 4G module on the USB port. If successful, proceed to module initialization; if it times out after 150 seconds, fail and restart.
2. **LTE_STA_INITMODULE**：Send initialization AT commands to the module. On success, proceed to get IMEI; on failure, restart.
3. **LTE_STA_IMEI**：Read the device's IMEI identifier. On success, check SIM card status; on failure, restart.
4. **LTE_STA_CPIN**：Check if the SIM card status is READY. On success, get the SIM card ICCID; if it times out after 30 seconds, fail and restart.
5. **LTE_STA_ICCID**：Read the SIM card serial number (ICCID). On success, get the local phone number.
6. **LTE_STA_CNUM**：Read the local phone number. On success, get the IMSI.
7. **LTE_STA_IMSI**：Read the International Mobile Subscriber Identity (IMSI). On success, configure the APN.
8. **LTE_STA_APN**：Set the Access Point Name (APN) parameters. On success, check network registration.
9. **LTE_STA_CGREG**：Wait for the module to register with the carrier network. On success, get network information; if it times out after 180 seconds, fail and restart.
10. **LTE_STA_NWINFO**：Get signal strength (CSQ), network mode, and other information, and start the network interface. On success, establish a data connection.
11. **LTE_STA_GOBINET**：Use quectel-CM for dial-up internet access to obtain an IP address. On success, enter the connection monitoring phase; on failure, restart.

After all states are executed sequentially and successfully, the program enters the connection monitoring phase.

Phase 3: Connection Monitoring

Upon entering the **LTE_STA_CONNECTED** state, the program cyclically executes network monitoring tasks, including:

- **Ping Connectivity Check**：Verifies network reachability. If the cumulative failure count exceeds the configured threshold, it jumps to the reset state.
- **Network Status Monitoring**：Checks module registration status, SIM card status, and IP address validity. Any detected anomaly triggers a jump to reset.
- **Signal Strength Update**：Continuously updates the CSQ signal strength indicator.
- **Logging**：Records network status information.

Conditions that trigger a reset include: Ping failure count exceeding the threshold, abnormal network status (e.g., not registered, SIM card error, invalid IP), or failure of AT commands querying network status.

Phase 4: Reset and Recovery

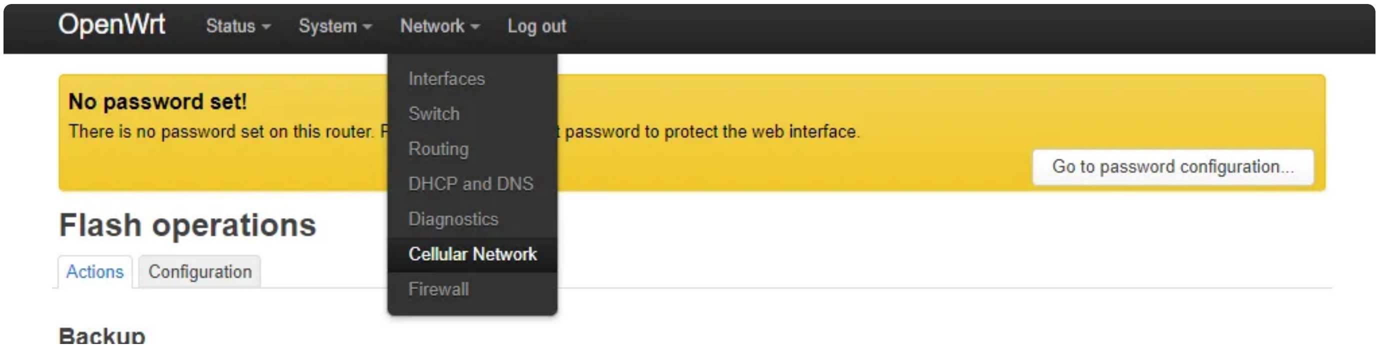
In the **LTE_STA_RESET** state, the program executes the module reset recovery process: first, it closes the current network connection, then performs a software or hardware reset of the module, and finally clears all failure counters and status flags. Upon completion, the state machine restarts the entire dial-up process from the **LTE_STA_FINDTTYUSB** state.

Message Handling Mechanism

While the state machine runs in a loop, it concurrently processes external AT command requests via a message queue: upon receiving an external AT command, it sends the command to the 4G module via the serial port and eventually returns the command response to the caller.

Web Interface

`luci-app-cellular` contains the web interface code, with the actual effect as shown below:

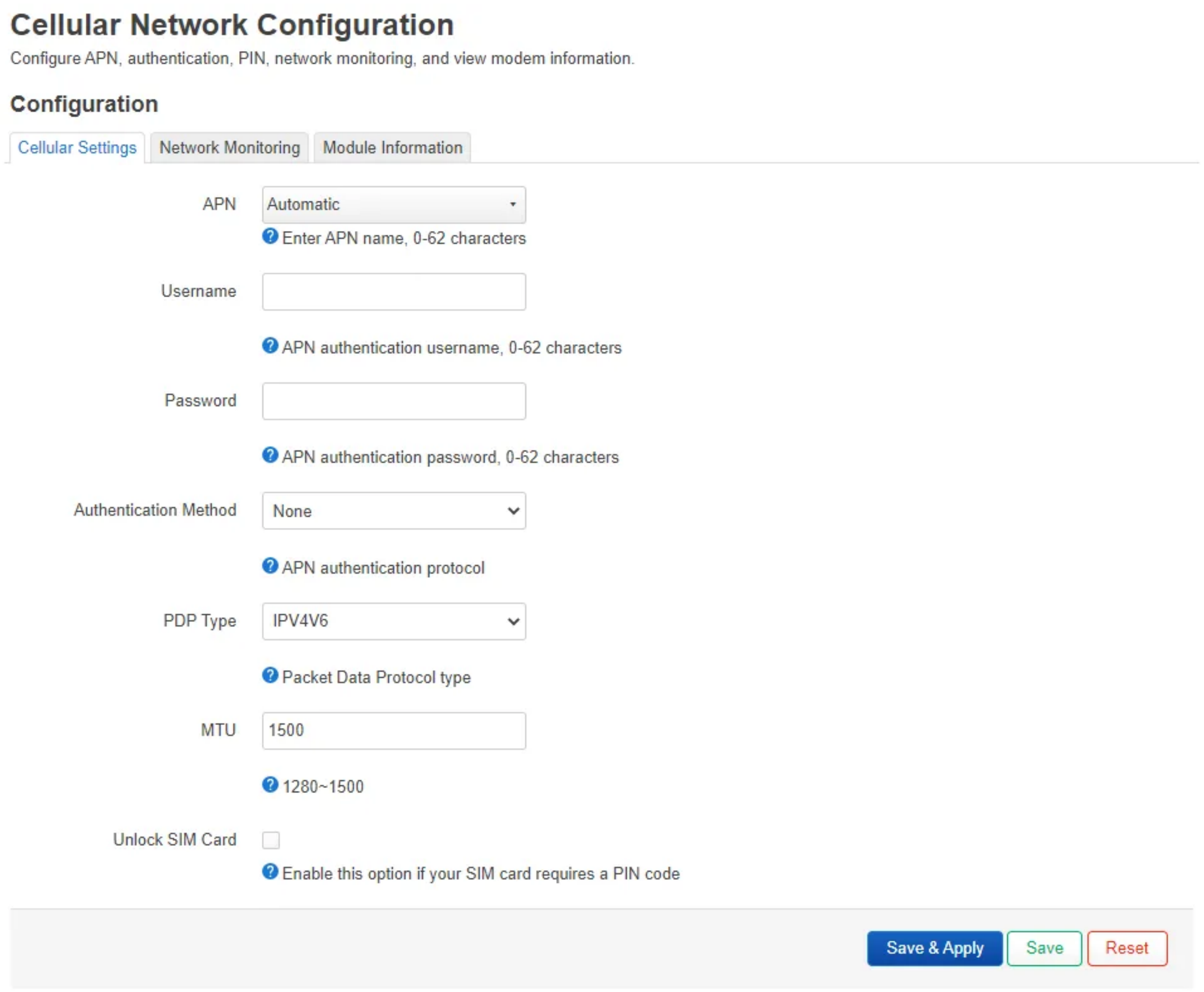


No password set!

There is no password set on this router. P password to protect the web interface.

Flash operations

Backup

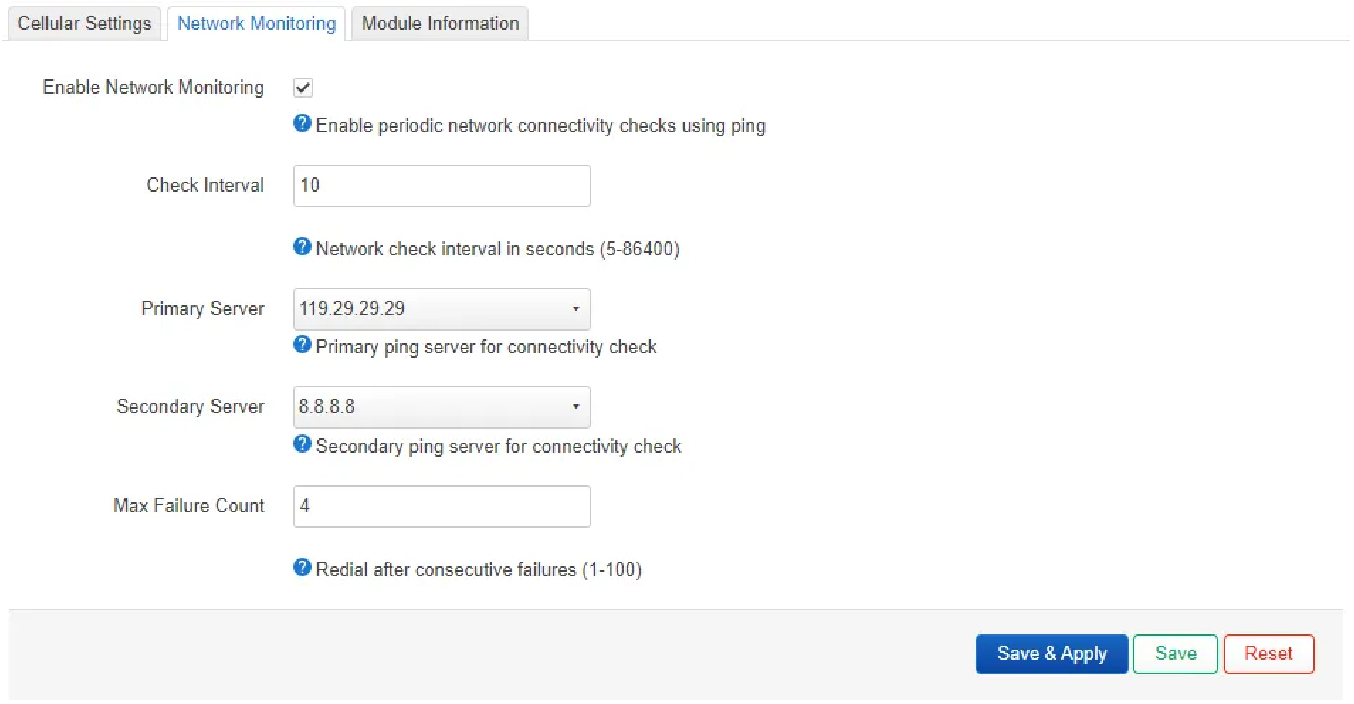


Cellular Network Configuration

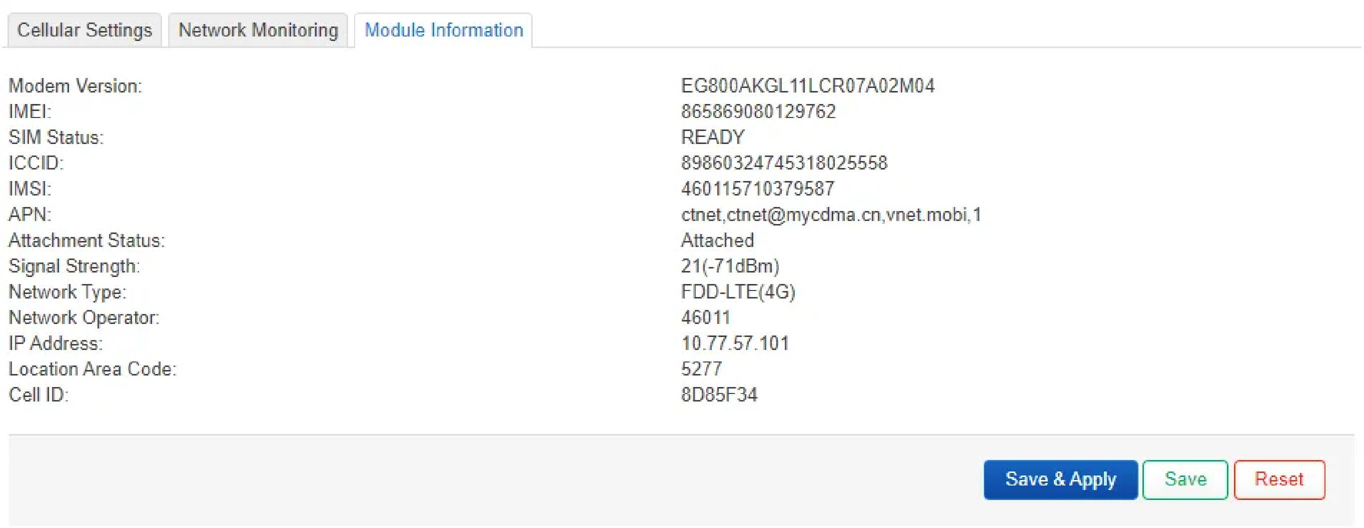
Configure APN, authentication, PIN, network monitoring, and view modem information.

Configuration

APN	Automatic
	Enter APN name, 0-62 characters
Username	
	APN authentication username, 0-62 characters
Password	
	APN authentication password, 0-62 characters
Authentication Method	None
	APN authentication protocol
PDP Type	IPV4V6
	Packet Data Protocol type
MTU	1500
	1280~1500
Unlock SIM Card	□
	Enable this option if your SIM card requires a PIN code



Enable Network Monitoring	☑
	Enable periodic network connectivity checks using ping
Check Interval	10
	Network check interval in seconds (5-86400)
Primary Server	119.29.29.29
	Primary ping server for connectivity check
Secondary Server	8.8.8.8
	Secondary ping server for connectivity check
Max Failure Count	4
	Redial after consecutive failures (1-100)



Modem Version:	EG800AKGL11LCR07A02M04
IMEI:	865869080129762
SIM Status:	READY
ICCID:	89860324745318025558
IMSI:	460115710379587
APN:	ctnet,ctnet@mycdma.cn,vnet.mobi,1
Attachment Status:	Attached
Signal Strength:	21(-71dBm)
Network Type:	FDD-LTE(4G)
Network Operator:	46011
IP Address:	10.77.57.101
Location Area Code:	5277
Cell ID:	8D85F34

cellularat(4G Module AT Command Tool)

`cellularat` is a command–line utility for AT command communication with the 4G module, offering two operation modes: When the 4G dialer service (`usr_lte`) is running on the system, it communicates via message queue; otherwise, it interacts directly with the 4G module via the serial port using AT commands.

语法格式

```
cellularat -m "AT command" [-t timeout]
```

Parameter Description

Parameter	Description	Default	Example
`-m`	AT command content	Required parameter	`-m "AT"`
`-t`	Response timeout in seconds	6 seconds	`-t 10`

Usage Examples

```
# Query SIM card status
cellularat -m "AT+CPIN?"

# Query IMSI number
cellularat -m "AT+CIMI"

# Query ICCID
cellularat -m "AT+TCCID"
```

libusr（PUSR Programs' Internal Library）