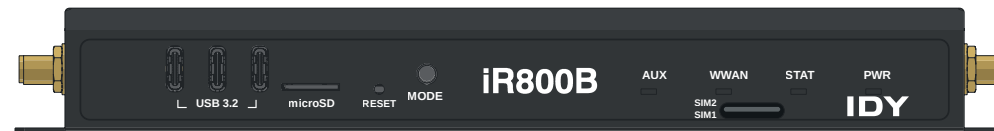




IoT Gateway iR800B Series



USER MANUAL (Basic Configuration)

Thank you for purchasing this product. Read this manual carefully before use to ensure correct operation. Keep it in a safe place for reference whenever you have questions or encounter a problem.

IDY Corporation

Rev.1.5 EN

Contents

Introduction	3	1. Cellular Module Configuration (AT Commands)	35
Safety Precautions - Handling the Product	3	2. gpsd Configuration	38
Safety Precautions - Handling the AC Adapter	5	3. Allowing LAN Hosts to Connect to gpsd	41
Operating Precautions	6	4. Using gpsd from a LAN Host	43
Product Warranty	7	5. Security Considerations	46
Chapter 1 About the Product	9	6. Reverting the Configuration	46
Package Contents	9	Firewall Configuration	48
Connecting the Antennas	10	1. Port Forwarding	49
Front Interfaces	10	2. DMZ Configuration	53
Rear Interfaces	11	3. Allowing WAN Access to This Device (Input Rules)	54
Chapter 2 Configuration	13	4. Checking the Configuration	65
SSH Connection	13	5. Removing or Reverting Settings	66
Interfaces	14	Chapter 3 LEDs	70
Restoring Factory Settings	28	Chapter 4 Specifications	71
Firmware Update	29	Chapter 5 Open-Source Licenses	75
Checking Status	30	Product Support	84
GNSS Configuration	34		

Introduction

Thank you for purchasing the iR800B IoT 5G Edge Gateway (referred to as this product). This product provides high-speed wireless or wired connectivity to the Internet and local area networks (LANs).

This manual explains the information required to use the product safely and the configuration procedures needed to start using it.

Under Japan's Telecommunications Business Act, the wired WAN and LAN ports of this product must not be connected directly to a telecommunications carrier, such as a fixed-line telephone company or Internet service provider. When connecting the wired WAN or LAN to a carrier's line, always connect through a router or similar device.

When using wireless LAN in the 5 GHz band, outdoor use of radio waves in the 5.2 GHz and 5.3 GHz bands is prohibited under Japan's Radio Act. Indoor use means use within a building enclosed by walls on all sides. Station platforms and the interiors of vehicles, including cars and trains, are treated as outdoor locations; exercise care.

For Safe and Reliable Use

Read this manual before using the product. It contains important information and precautions to prevent injury to you or others and damage to property, and to ensure safe operation. Keep it nearby so that you can refer to it whenever necessary.

Safety Precautions

Handling the Product

WARNING

If you notice unusual sounds or odors, overheating, smoke, or deformation, immediately disconnect the AC adapter plug from the product and unplug the AC adapter from the outlet. Continued use may cause fire, burns, or electric shock.



If the product or AC adapter is dropped or subjected to a strong impact, immediately disconnect the AC adapter plug from the product and unplug it from the outlet. Continued use may cause fire, electric shock, or malfunction.



Introduction

Safety Precautions (continued)

Handling the Product

WARNING

Do not disassemble, modify, or repair the product. Doing so may cause fire, electric shock, or malfunction. IDY may decline repairs if the product's labels or cover have been removed.



Prohibited

Do not cover the product or AC adapter with bedding or place it near heating appliances or on an electric carpet. Internal temperatures may rise, causing fire, burns, or malfunction.



Prohibited

Position the product, power supply, cables, and connectors out of the reach of small children. Otherwise, injury may occur.



Required

Do not use the product where water may splash, such as in a bathroom or shower, in high humidity, or where rain or mist may enter, including outdoor locations. Fire or electric shock may result.



Prohibited

Safety Precautions (continued)

Handling the Product

WARNING

Always disconnect the AC adapter plug from the product before installing or removing a USIM card, USB device, or similar item.



Required

Do not place the product on an unstable surface, such as a shaky stand or an inclined surface. It may fall or topple and cause injury.



Prohibited

Do not place containers of liquid, such as vases or cups, or metal objects, such as staples or paper clips, on or near the product. Foreign matter, including metal fragments or liquid, entering the product may cause fire or electric shock. If foreign matter enters, immediately unplug the AC adapter from the outlet.



Prohibited

Introduction

Safety Precautions (continued)

Handling the Product

WARNING

Before touching the product, discharge static electricity from your body by touching a nearby metal object, such as a doorknob or aluminum window frame. Static electricity from your body or other sources may damage the product.



Required

Safety Precautions

Handling the AC Adapter

WARNING

Do not modify, heat, or attempt to repair the AC adapter. Doing so may cause fire or electric shock.



Prohibited

When handling the AC adapter, observe all of the following precautions.



Prohibited

- Do not trap the AC adapter between a wall, rack, or other objects during installation.

Safety Precautions (continued)

Handling the AC Adapter

WARNING

- Do not place heavy objects on it or pull on it.
- Keep it away from heating appliances and do not heat it.
- Hold the plug when disconnecting the AC adapter.
- Do not handle the AC adapter with wet hands; electric shock may result.
- Do not bend the cord sharply.
- Do not move the product while the AC adapter is connected.
- Insert the power plug fully into a 100 V AC outlet. Failure to do so may cause fire or electric shock.

Always use the AC adapter supplied with the product. Using another AC adapter may cause fire, rupture, or smoke.



Required

Introduction

Operating Precautions

Operating and Storage Environment

- Do not place the product in high temperatures, such as in direct sunlight, inside a closed vehicle, or near heating equipment.
- Do not place it in extremely low temperatures or dusty locations.
- Do not use it near sources of magnetism, such as magnets, speakers, televisions, or magnetic bracelets.
- Do not place it near flames or where heat accumulates.
- Do not subject it to sudden temperature changes.
- Do not place it where vibration exceeds the warranted range or where it cannot be installed level.
- Do not install it where there is a risk of electrical leakage or water leakage.
- Do not clean it with benzine, thinner, or similar solvents. These may cause deterioration, deformation, or discoloration.

Operating Precautions (continued)

- When disposing of the product, follow local government ordinances. Contact your local authority for details.

Precautions for Wireless Operation

This product complies with the regulations concerning technical standards conformity certification for specified radio equipment under Japan's Radio Act and the regulations concerning technical standards conformity approval for terminal equipment under Japan's Telecommunications Business Act. The technical conformity mark on the label on the bottom of the product indicates this compliance.

Removing screws and modifying the interior invalidates technical conformity certification and related approvals. Do not use the product after these approvals have become invalid; doing so violates the Radio Act and the Telecommunications Business Act.

Because this product includes radio equipment, communication quality varies with the environment. Assess the installation environment and use the product at your own discretion regarding communication speed, wireless disconnections, and similar conditions.

Introduction

Operating Precautions (continued)

A contract with the relevant telecommunications carrier is required to communicate over a public network using this product. IDY is not a party to that contract.

Services provided by telecommunications carriers may incur charges depending on how the product is used. IDY is not responsible for those charges.

Product Warranty

Hardware Warranty and After-Sales Service

If a failure or defect occurs during the product warranty period under normal use in accordance with the precautions in the product manual and related documentation, IDY will repair the affected part free of charge using its prescribed method. Send the product to the retailer or distributor from which it was purchased, with a description of the failure or defect and a warranty certificate, delivery note, or other document showing the purchase date. On-site repairs and substitute-unit service are not provided.

Shipping and courier costs are borne by the customer.

Product Warranty (continued)

The following cases are not covered, even during the product warranty period.

- No warranty certificate, delivery note, or other proof of delivery is presented.
- The warranty certificate, delivery note, or other proof lacks the name of IDY, the retailer, or the distributor, or its wording has been altered.
- Failure or damage results from improper handling, such as a drop or impact while moving the product after purchase.
- Failure or damage results from misuse or unauthorized modification by the customer.
- Failure or damage results from external factors such as fire, gas damage, salt damage, earthquake, lightning, wind or flood damage, other natural disasters, or abnormal voltage.
- Failure or damage is caused by peripheral equipment or consumables connected to the product.
- Failure or damage results from handling contrary to the usage instructions or precautions in the specifications or manual.

Introduction

Product Warranty (continued)

For repaired or replacement products, the warranty remains valid for the longer of the original warranty period from purchase or delivery, or three months after repair or replacement.

This product warranty applies only when the product is used in Japan.

IDY, retailers, and distributors accept no liability for direct or indirect consequential losses caused by product failure, including data loss, service interruption due to communication problems, or charges incurred.

Chapter 1 About the Product

Before Use

The following items are supplied with the product. If any item is missing, contact IDY.

- iR800B



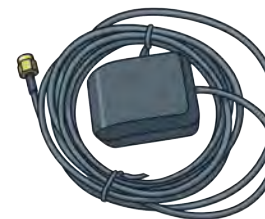
- LTE/5G antennas: 4



Illustrations may differ slightly from the actual product. Product shapes are subject to change.

Package Contents

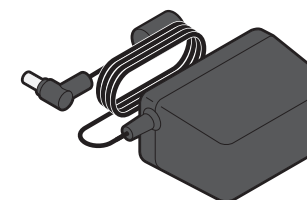
- GNSS antenna: 1



- Wireless LAN/Bluetooth antennas: 2



- AC adapter: 1



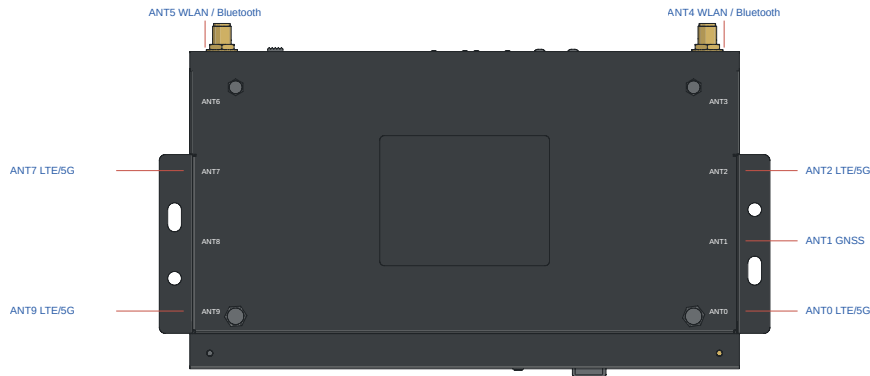
- AC adapter connector retaining hook and screw: 1 each



Chapter 1 About the Product

Connecting the Antennas

Antennas must be connected for wireless communication. Connect the antennas required for the interfaces you will use.



1. LTE/5G Antennas

- Connect to ANT0, ANT2, ANT7, and ANT9.

2. Wireless LAN/Bluetooth Antennas

- Connect to ANT4 and ANT5.

Connecting the Antennas (continued)

3. GNSS Antenna

- Connect to ANT1.

Front Interfaces



1. USB 3.2 Host Interface

- A USB 3.2 port is provided.
- Connecting an IDY iS201B also enables Dual SIM Dual Active operation.

Chapter 1 About the Product

Front Interfaces (continued)

2. Reset Button

- Insert a thin rod into this hole to restart the product without accessing the management interface.
- Use this button only when the product is not operating normally.

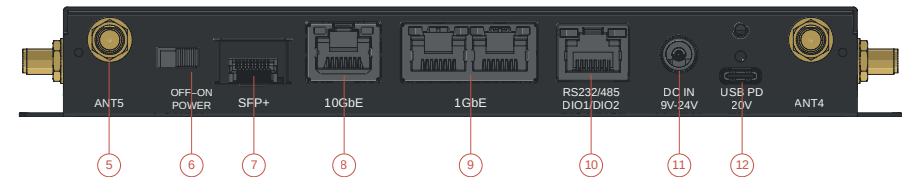
3. SIM Card Socket

- Push the black SIM card tray to release it.
- Remove the tray, place nano-SIM cards on its upper and lower sides, and reinsert the tray into the socket.
- Take care not to damage the SIM cards when inserting or removing the tray.

4. PWR Indicator

- The indicator lights when power is detected and the power switch is turned ON.

Rear Interfaces



5. SMA Connectors

- Antenna connectors are located on both sides and at the rear of the product.

6. Power Switch

- Use this switch to turn the product ON or OFF.
- Turning the switch OFF starts the power-off sequence.
- Turn this switch OFF before disconnecting the power supply.
- Turn the switch ON when supplying power again.

Chapter 1 About the Product

Rear Interfaces (continued)

7. SFP+

- Socket for a 10GBASE-R SFP+ module.

8. 10GbE

- RJ45 connector supporting 10GBASE-T.

9. 1GbE

- RJ45 connector supporting 1000BASE-T.

10. RS232/RS485 Interface

- An optional dedicated RJ45-to-D-sub 9-pin conversion cable allows use as an RS232 or RS485 interface.
- Software customization is required for this connection.

10. DIO (Digital Input/Output)

- Used to receive data from external equipment and to output control signals.
- Software customization is required for this connection.

Rear Interfaces (continued)

11. DC 9 V to 24 V Power Jack

- Connect the supplied AC adapter to supply power.

12. Power Input (USB Power Delivery)

- A USB PD AC adapter is not supplied. Use the DC power jack described above.
- A USB PD AC adapter rated at 65 W or more and capable of 20 V output may also be used.

Chapter 2 Configuration

SSH Connection

These procedures apply to firmware version iR8xxB-00.01.04 and later.

Connect to the device by SSH through a LAN port to configure its interfaces. Follow the procedure below.

- Prefix commands that require root privileges with sudo.

Connect a wired LAN port on the router to the PC's LAN port using a LAN cable.

Start terminal software, such as Tera Term, on the PC, such as a Windows PC, and connect using the following settings.

Example Settings

TCP/IP

Host: 192.168.1.1

Service: SSH

TCP port: 22

SSH version: SSH2

IP version: AUTO

Use the following login credentials if the password has not been changed.

Example Settings

ID:admin

PW:admin

Chapter 2 Configuration

SSH Connection (continued)

After logging in, change the password using the following command.

Input example

```
sudo passwd admin
```

If the device's LAN IP address has been changed in the wired Ethernet LAN settings, enter that address as the host address instead.

Interfaces

Use the following commands to switch interfaces and retrieve information.

Chapter 2 Configuration

Interfaces (continued)

LTE/5G

Insert a SIM card from your network operator, such as NTT DOCOMO or KDDI, into the SIM1 slot.

Configure the device as shown below and restart it. The device will then connect automatically.

Input example

```
admin@iR8xxB:~$ sudo config net-wwan-carrier=30 # 30=NTT DOCOMO, 31=KDDI, 0=Other (Softbank/Local 5G)
admin@iR8xxB:~$ sudo config net-wwan-apn=apn
admin@iR8xxB:~$ sudo config net-wwan-user=user
admin@iR8xxB:~$ sudo config net-wwan-password=password
admin@iR8xxB:~$ sudo config net-wwan-auth=CHAP # CHAP or PAP or none
admin@iR8xxB:~$ sudo config net-wwan-pdp_type=ipv4 # ipv4 or ipv4v6

admin@iR8xxB:~$ sudo config net-wwan-fn990-network=37 # 36= NG-RAN only, 37= NG-RAN and E-UTRAN
admin@iR8xxB:~$ sudo config net-wwan-fn990-5gctl=10 # 2=SA, 8=NSA, 10=SA and NSA
admin@iR8xxB:~$ sudo config net-wwan-fn990-band=0,0,3400A060085,0,8000000,6000,0,6000 # See FN990 AT Commands Reference
admin@iR8xxB:~$ sudo reboot
```

To check the current value of a setting, use config followed by the configuration name.

To check all settings, view the following file.

/etc/config/ir.conf

Chapter 2 Configuration

Interfaces (continued)

WiFi

Checking Settings

Wi-Fi is disabled by default.

Use the following command to check the settings.

Input example

```
admin@iR8xxB:/# sudo uci show wireless
```

Chapter 2 Configuration

Interfaces (continued)

Output example

```
wireless.radio0=wifi-device
wireless.radio0.type='mac80211'
wireless.radio0.path='soc/11300000.pcie/pci0000:00/0000:00:00.0/0000:01:00.0'
wireless.radio0.band='2g'
wireless.radio0.channel='6'
wireless.radio0.htmode='HE80'
wireless.radio0.disabled='0'
wireless.radio0.country='JP'
wireless.radio0.txpower='10'
wireless.ap_radio0=wifi-iface
wireless.ap_radio0.device='radio0'
wireless.ap_radio0.network='lan'
wireless.ap_radio0.mode='ap'
wireless.ap_radio0.ssid='iR8xxB'
```

Chapter 2 Configuration

Interfaces (continued)

Output example

```
wireless.ap_radio0.encryption='psk2'  
wireless.ap_radio0.key='12345678'  
wireless.ap_radio0.disabled='1'  
wireless.sta_radio0=wifi-iface  
wireless.sta_radio0.device='radio0'  
wireless.sta_radio0.mode='sta'  
wireless.sta_radio0.network='wlansta'  
wireless.sta_radio0.ssid='wlan-ap'  
wireless.sta_radio0.encryption='psk2'  
wireless.sta_radio0.key='12345678'  
wireless.sta_radio0.disabled='1'
```

Station Mode

Input example

```
# Scan for Wi-Fi access points  
admin@iR8xxB:~$ sudo iwinfo radio0 scan
```

Chapter 2 Configuration

Interfaces (continued)

Output example

```
Cell 01 - Address: XX:XX:XX:XX:XX:XX
ESSID: XXXXXXXXXXXX
Mode: Master Frequency: 2.412 GHz Band: 2.4 GHz Channel: 1
Signal: -67 dBm Quality: 43/70
Encryption: mixed WPA/WPA2 PSK (CCMP)
HT Operation:
    Primary Channel: 1
    Secondary Channel Offset: no secondary
    Channel Width: 20 MHz
...
```

Input example

```
# Configure a connection to a Wi-Fi access point
admin@iR8xxB:~$ sudo uci set wireless.radio0.band='band *1'
admin@iR8xxB:~$ sudo uci set wireless.sta_radio0.ssid='SSID to connect to'
admin@iR8xxB:~$ sudo uci set wireless.sta_radio0.encryption='psk2'
admin@iR8xxB:~$ sudo uci set wireless.sta_radio0.key='password'
admin@iR8xxB:~$ sudo uci set wireless.sta_radio0.disabled='0'
admin@iR8xxB:~$ sudo uci commit wireless
admin@iR8xxB:~$ sudo /etc/init.d/network restart

# Retrieve Wi-Fi information
admin@iR8xxB:~$ iwinfo phy0-sta0 info
```

Chapter 2 Configuration

Interfaces (continued)

Input example

```
# Disconnect from the Wi-Fi access point
admin@iR8xxB:~$ sudo uci set wireless.sta_radio0.disabled='1'
admin@iR8xxB:~$ sudo uci commit wireless
admin@iR8xxB:~$ sudo /etc/init.d/network restart
```

Chapter 2 Configuration

Interfaces (continued)

Access Point Mode

Input example

```
# Configure and enable a Wi-Fi access point
admin@iR8xxB:~$ sudo uci set wireless.radio0.band='band *1'
admin@iR8xxB:~$ sudo uci set wireless.radio0.channel='channel number *2'
admin@iR8xxB:~$ sudo uci set wireless.ap_radio0.ssid='SSID *3'
admin@iR8xxB:~$ sudo uci set wireless.ap_radio0.encryption='psk2'
admin@iR8xxB:~$ sudo uci set wireless.ap_radio0.key='password *4'
admin@iR8xxB:~$ sudo uci set wireless.ap_radio0.disabled='0'
admin@iR8xxB:~$ sudo uci commit wireless
admin@iR8xxB:~$ sudo /etc/init.d/network restart

# Stop the Wi-Fi access point
admin@iR8xxB:~$ sudo uci set wireless.ap_radio0.disabled='1'
admin@iR8xxB:~$ sudo uci commit wireless
admin@iR8xxB:~$ sudo /etc/init.d/network restart
```

Input example

```
# Retrieve Wi-Fi information
admin@iR8xxB:~$ iwinfo
```

*1: Set 2g for the 2.4 GHz band or 5g for the 5 GHz band.

Chapter 2 Configuration

Interfaces (continued)

For outdoor use, select 2g to use the 2.4 GHz band.

*2: With band set to 2g, select a channel from 1 to 13. With band set to 5g, select 36, 40, 44, or 48.

*3: Use ASCII letters, digits, hyphens, and underscores. The maximum length is 32 characters.

*4: Use ASCII letters, digits, hyphens, and underscores. The permitted length is 8 to 63 characters.

Bluetooth

Input example

```
admin@iR8xxB:~$ hciconfig
```

Output example

```
hci0:  Type: Primary  Bus: USB
      BD Address: XX:XX:XX:XX:XX:XX  ACL MTU: 1021:6  SCO MTU: 255:12
      UP RUNNING
      RX bytes:3403 acl:0 sco:0 events:373 errors:0
      TX bytes:69185 acl:0 sco:0 commands:373 errors:0
```

Chapter 2 Configuration

Interfaces (continued)

Input example

```
admin@iR8xxB:~$ sudo hciconfig hci0 up
```

```
# Scan for Bluetooth devices
```

```
admin@iR8xxB:~$ sudo hcitool scan
```

Output example

```
Scanning ...
```

```
XX:XX:XX:XX:XX:XX    DDDDDDDDDDD
```

Input example

```
# Scan for BLE devices
```

```
admin@iR8xxB:~$ sudo hcitool lescan
```

Chapter 2 Configuration

Interfaces (continued)

Output example

```
LE Scan ...
XX:XX:XX:XX:XX:XX (unknown)
XX:XX:XX:XX:XX:XX (unknown)
XX:XX:XX:XX:XX:XX XXXXX
...
```

Press Ctrl+C to stop scanning.

Wired Ethernet

LAN

Input example

```
# Check the settings
admin@iR8xxB:/# sudo uci show network.lan
```

Chapter 2 Configuration

Interfaces (continued)

Output example

```
network.lan=interface
network.lan.device='br-lan'
network.lan.proto='static'
network.lan.ipaddr='192.168.1.1'
network.lan.netmask='255.255.255.0'
network.lan.ip6assign='60'
```

Input example

```
# Configure a static IP address
admin@iR8xxB:~$ sudo uci set network.lan.ipaddr='IP address'
admin@iR8xxB:~$ sudo uci set network.lan.netmask='subnet mask in IP address format'
admin@iR8xxB:~$ sudo uci commit network

# Apply the settings
admin@iR8xxB:~$ sudo /etc/init.d/network restart
```

Chapter 2 Configuration

Interfaces (continued)

WAN

Input example

```
# Check the settings  
admin@iR8xxB:/# sudo uci show network.wan
```

Output example

```
network.wan=interface  
network.wan.device='br-wan'  
network.wan.proto='dhcp'
```

Chapter 2 Configuration

Interfaces (continued)

Input example

```
# Configure a static IP address
admin@iR8xxB:~$ sudo uci set network.wan.proto='static'
admin@iR8xxB:~$ sudo uci set network.wan.ipaddr='IP address'
admin@iR8xxB:~$ sudo uci set network.wan.netmask='subnet mask in IP address format'
admin@iR8xxB:~$ sudo uci set network.wan.gateway='default gateway'
admin@iR8xxB:~$ sudo uci set network.wan.dns='primary DNS'
admin@iR8xxB:~$ sudo uci add_list network.wan.dns='secondary DNS'
admin@iR8xxB:~$ sudo uci commit network

# Apply the settings
admin@iR8xxB:~$ sudo /etc/init.d/network restart
```

Chapter 2 Configuration

Interfaces (continued)

Input example

```
# Configure DHCP
admin@iR8xxB:~$ sudo uci set network.wan.proto='dhcp'
admin@iR8xxB:~$ sudo uci delete network.wan.ipaddr
admin@iR8xxB:~$ sudo uci delete network.wan.netmask
admin@iR8xxB:~$ sudo uci delete network.wan.gateway
admin@iR8xxB:~$ sudo uci delete network.wan.dns
admin@iR8xxB:~$ sudo uci commit network

# Apply the settings
admin@iR8xxB:~$ sudo /etc/init.d/network restart
```

Restoring Factory Settings

Follow the steps below to restore factory settings. Do not disconnect power during this procedure.

- (1) Wait for startup to complete.
- (2) Hold down the MODE button and turn the POWER switch OFF.
- (3) When the red STAT LED lights, release MODE and turn the POWER switch ON before the LED goes out, within 10 seconds.
- (4) The red STAT LED flashes rapidly, and the device restarts with factory settings.

Chapter 2 Configuration

Restoring Factory Settings (continued)

You can also restore factory settings from the command line using the following command.

Input example

```
admin@iR8xxB:~$ sudo router clear -a
```

Firmware Update

Use the following command to update the firmware.

First copy the firmware binary to /tmp/ using SCP or a USB flash drive, then run the command.

Replace the file name with the actual firmware binary file name.

Input example

```
admin@iR8xxB:~$ sudo router fwupdate -f /tmp/iR8xxB-01.00.00.itb
```

Chapter 2 Configuration

Checking Status

Use the following command to check the device status.

Input example

```
admin@iR8xxB:~$ router status -a
```

Chapter 2 Configuration

Checking Status (continued)

Output example

Router Status

System Info

FW Version : iR8xxB-00.01.02

FVIN : 01

System Up Time : 16:07:24 up 28 min, load average: 0.17, 0.16, 0.10

System Date : Thu Aug 14 16:07:24 JST 2025

Network Information

Connected Type : cellular

WWAN Network

WAN IP Address : 10.76.105.108

Subnet Mask : 255.255.255.255

Default Gateway : 10.76.105.108

Primary Domain Name Server : 110.163.0.5

Secondary Domain Name Server : 110.163.0.6

Local Network

Local IP Address : 192.168.1.1

Local Netmask : 255.255.255.0

MAC Address : XX:XX:XX:XX:XX:XX

Chapter 2 Configuration

Checking Status (continued)

Output example

WWAN Information

module name : FN990A40
module version : M0R.110005
module IMEI : XXXXXXXXXXXXXXXX
module HW revision : 1.00
SIM Slot : 1
SIM MSISDN : XXXXXXXXXXXX
SIM ICCID : XXXXXXXXXXXXXXXXXX
SIM IMSI : XXXXXXXXXXXXXXXX
Mobile Country Code : 440
Mobile Network Code : 10
Area Code (TAC/LAC) : 5783
Cell ID : 39515473
Network Type : NR
Access Technology : E-UTRA-NR dual connectivity
UMTS RSSI : UNAVAILABLE
LTE RSSI : -56
LTE RSRP : -85
LTE RSRQ : -8
NR RSSI : -75
NR RSRP : -89
NR RSRQ : -14

Detailed Information :

JP DOCOMO RSRP:-85 RSRQ:-8 TAC:1697 Id:25AF551 EARFCN:1850 PWR:-56dbm DRX:1280
NR_BAND:78 NR_BW:100 NR_ULBW:100 NR_CH:643296 NR_ULCH:643296 NR_PWR:-75dbm NR_RSRP:-89 NR_RSRQ:-14 NR_PCI:576 NR_SINR:90

Chapter 2 Configuration

Checking Status (continued)

Output example

```
NR_STATE:2 NR_TXPWR:195 NR_DLMOD:3 NR_ULMOD:3
LTE MIMO : 2x2 MIMO
NR MIMO : 2x2 MIMO
Modem temperature (TSENS)      :46
PA temperature                  :47
Modem LTE DSC mitigation level  :0
Modem NR DSC mitigation level   :0
Modem NR SCG DSC mitigation level :0
PA LTE SDR0 DSC mitigation level :0
PA LTE SDR1 DSC mitigation level :0
PA NR SDR0 DSC mitigation level  :0
PA NR SDR1 DSC mitigation level  :0
PA NR SDR0 SCG DSC mitigation level:0
PA NR SDR1 SCG DSC mitigation level:0
```

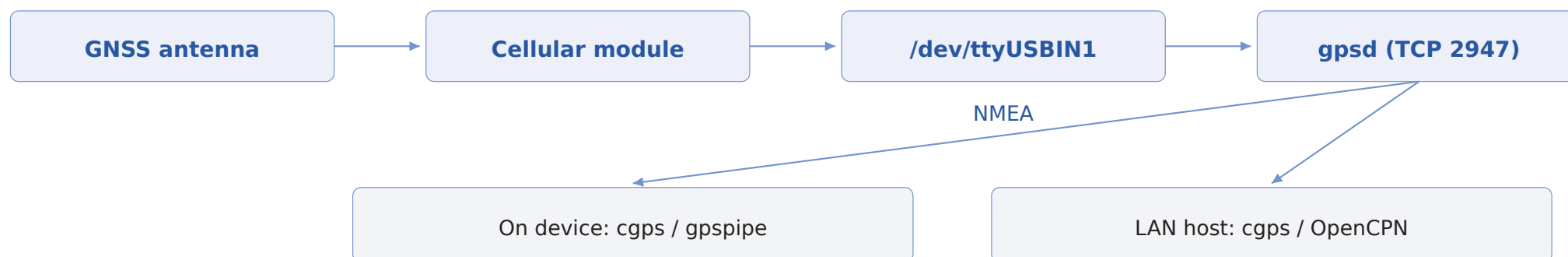
Chapter 2 Configuration

GNSS Configuration

Overview

This section explains how to enable GNSS on the iR800B's internal cellular module and obtain positioning data on the device and on hosts connected to the LAN.

Data Path Overview



All configuration is performed over SSH using uci and AT commands. Settings are saved persistently and remain effective after a restart.

Prerequisites

- Firmware iR8xxB-00.01.04 or later is required. Specifications may change without notice following a firmware update.
- SSH access to the iR800B must be available.
- Connect the GNSS antenna to the device's ANT1 port and install it with a clear view of the sky.

Chapter 2 Configuration

GNSS Configuration (continued)

1. Cellular Module Configuration (AT Commands)

Enable GNSS and NMEA output on the cellular module.

1.1 Opening the AT Command Interface Interactively

AT commands are sent to and received from the cellular module through `/dev/ttyUSBIN3`. After logging in by SSH, open this port using `sudo microcom`. Access to the serial device requires root privileges.

Input example

```
sudo microcom /dev/ttyUSBIN3
```

- When the prompt appears, enter AT commands one line at a time and press Enter to send each command. Each command returns OK or ERROR.
- Press Ctrl+X to end the session. This is microcom's default exit key.
- `/dev/ttyUSBIN3` is dedicated to AT commands. NMEA data is output through the separate port `/dev/ttyUSBIN1` and will not appear on the AT command port.

Chapter 2 Configuration

GNSS Configuration (continued)

1.2 Sending AT Commands from a Shell Script

The `microcom -t` option specifies the read timeout in milliseconds. You can pipe commands from `echo`, obtain the response, and exit automatically without an interactive session. This is useful for script automation.

Input example

```
# Single command: check the response to AT
echo -e 'AT\r' | sudo microcom -t 1000 /dev/ttyUSBIN3
```

Input example

```
# Send multiple commands to enable GNSS
{
  echo -e 'AT$GPSANTPORT=3\r'
  echo -e 'AT$GPSNMUN=1,1,1,1,1,1\r'
  echo -e 'AT$GPSP=1\r'
  echo -e 'AT$GPSSAV\r'
} | sudo microcom -t 2000 /dev/ttyUSBIN3
```

Key Points

- AT command lines must end with `\r` (CR). Always append it using `echo -e ... '\r'`. A newline, `\n` (LF), is not required; CR alone is sufficient.

Chapter 2 Configuration

GNSS Configuration (continued)

- -t <ms> sets the maximum response wait time. After the final command's response, such as OK, ERROR, or a value, is written to standard output, microcom exits when the timeout expires, even if the input stream has already closed.
- If the timeout is too short, the session may close before the response is received. As a guide, use 100 ms for commands such as AT that respond immediately, and at least 1000 ms for commands such as AT\$GPSSAV that write internally.

1.3 AT Commands for Enabling GNSS

Send the following commands in order using the interactive method in 1.1 or the shell-script method in 1.2.

AT Command	Purpose
AT\$GPSANTPORT=3	Select the GNSS antenna port for an external active antenna.
AT\$GPSNMUN=1,1,1,1,1,1,1	Enable unsolicited NMEA output for all of GGA, GLL, GSA, GSV, RMC, and VTG.
AT\$GPSP=1	Turn ON the GNSS module power.
AT\$GPSSAV	Save the settings to nonvolatile memory so they are retained after a restart.

If using interactive mode, press Ctrl+X to exit microcom after completing the configuration.

Chapter 2 Configuration

GNSS Configuration (continued)

2. gpsd Configuration

Associate the NMEA output port /dev/ttyUSBIN1 with gpsd and enable the daemon.

2.1 uci Configuration

Input example

```
sudo uci set gpsd.core.enabled='1'  
sudo uci set gpsd.core.device='/dev/ttyUSBIN1'  
sudo uci commit gpsd  
sudo /etc/init.d/gpsd restart
```

2.2 Configuration Parameters

Parameter	Description	Example Settings
enabled	Enable gpsd startup.	1
device	Device file that outputs NMEA data.	/dev/ttyUSBIN1
port	TCP listening port for gpsd; the default is 2947.	2947

Chapter 2 Configuration

GNSS Configuration (continued)

Parameter	Description	Example Settings
listen_globally	Whether to listen on all interfaces; this is changed in subsection 3 below.	0 (default)

2.3 Checking Operation on the Device (cgps)

Input example

cgps

- The left side displays position (latitude, longitude, altitude), speed, status, error estimates, time offset, grid square, ECEF coordinates, and other information.
- The right side displays each satellite's GNSS type, PRN, elevation, azimuth, SNR, and whether it is used.
- A status of 3D FIX or 2D FIX indicates successful positioning.

Chapter 2 Configuration

GNSS Configuration (continued)

Press q to quit.

Display Example (Actual Device Output)

```
+-----+-----+
| Time      2026-04-28T09:50:15.000Z (5) | Seen 13/Used 7 |
| Latitude  35.69606188 N | GNSS S PRN Elev Azim SNR Use |
| Longitude 139.77625750 E | GP 7 7 11.0 39.0 35.0 Y |
| Alt (HAE, MSL) 316.601, 195.210 ft | GP 15 15 43.0 266.0 34.0 Y |
| Speed      0.00 mph | GP 18 18 14.0 320.0 44.0 Y |
| Track (true, var) n/a, n/a deg | GP 20 20 69.0 285.0 47.0 Y |
| Climb      0.00 ft/min | GP 21 21 56.0 69.0 38.0 Y |
| Status     3D FIX (2 secs) | GP 29 29 21.0 267.0 27.0 Y |
| Long Err (XDOP, EPX) 0.79 , +/- 38.8 ft | GP 30 30 39.0 62.0 41.0 Y |
| Lat Err (YDOP, EPY) 2.07 , +/- 101 ft | GP 5 5 67.0 8.0 0.0 N |
| Alt Err (VDOP, EPV) 0.98 , +/- 165 ft | GP 6 6 0.0 150.0 0.0 N |
| 2D Err (HDOP, CEP) 0.60 , +/- 37.4 ft | GP 11 11 37.0 159.0 0.0 N |
| 3D Err (PDOP, SEP) 1.10 , +/- 194 ft | GP 14 14 3.0 102.0 0.0 N |
| Time Err (TDOP) 1.83 | GP 24 24 9.0 201.0 0.0 N |
| Geo Err (GDOP) 3.62 | SB137 50 0.0 0.0 44.0 N |
| Speed Err (EPS) +/- 138 mph |
| Track Err (EPD) n/a |
| Time offset 1.036574549 s |
| Grid Square PM95vq37 |
| ECEF X, VX n/a n/a |
| ECEF Y, VY n/a n/a |
| ECEF Z, VZ n/a n/a |
```

Chapter 2 Configuration

GNSS Configuration (continued)

Output example

```
+-----+-----+
```

- The header Seen 13/Used 7 indicates the number of satellites being tracked and the number used for positioning.
- The GNSS column identifies the satellite system: GP=GPS, SB=SBAS, GA=Galileo, BD=BeiDou, GL=GLONASS, etc.
- Only satellites marked Y in the Use column are used in the positioning calculation.

Immediately after antenna installation, a cold start may take several tens of seconds to several minutes to obtain the first fix. While Status is NO FIX, wait for the Seen/Used satellite counts to increase.

3. Allowing LAN Hosts to Connect to gpsd

With the default `listen_globally='0'`, `gpsd` listens only on loopback, `127.0.0.1:2947`, so LAN hosts cannot connect. Change the setting to listen on all interfaces.

3.1 Enabling `listen_globally`

Input example

```
sudo uci set gpsd.core.listen_globally='1'  
sudo uci commit gpsd  
sudo /etc/init.d/gpsd restart
```

Chapter 2 Configuration

GNSS Configuration (continued)

3.2 Checking the Listening State

Input example

```
sudo netstat -tunlp | grep 2947
```

Expected Output

```
tcp 0 0 0.0.0.0:2947 LISTEN <pid>/gpsd  
tcp 0 0 :::2947 LISTEN <pid>/gpsd
```

If the addresses are 0.0.0.0:2947 and :::2947 rather than 127.0.0.1:2947, connections from the LAN are also possible.

3.3 Firewall

The LAN zone has input='ACCEPT' by default, so no additional rule is needed.

Input example

```
uci show firewall | grep -A4 "@zone\[0\]"
```

Chapter 2 Configuration

GNSS Configuration (continued)

Output example

```
firewall.@zone[0].name='lan'  
firewall.@zone[0].input='ACCEPT'  
firewall.@zone[0].output='ACCEPT'  
firewall.@zone[0].forward='ACCEPT'
```

Access from the WAN zone (wwanin0, wwanex0, br-wan, phy0-sta0) remains blocked by `reject_from_wan`. The service is therefore not exposed externally. See subsection 5, Security Considerations, in this section.

4. Using `gpsd` from a LAN Host

Connect to TCP port 2947 on the iR800B's LAN IP address, which defaults to 192.168.1.1.

Chapter 2 Configuration

GNSS Configuration (continued)

4.1 gpss Client Tools

If a gpss client from the gpss-clients package is installed on the LAN host, you can open the same cgps display as on the device over the network.

OS	Installation Command
Debian/Ubuntu	<code>sudo apt install gpss-clients</code>
RHEL/Fedora	<code>sudo dnf install gpss-clients</code>
macOS (Homebrew)	<code>brew install gpss</code>

Chapter 2 Configuration

GNSS Configuration (continued)

Usage Examples

Input example

```
# Interactive display: position, speed, and satellites  
cgps 192.168.1.1
```

```
# JSON stream  
gpspipe -w 192.168.1.1
```

```
# NMEA stream  
gpspipe -r 192.168.1.1
```

```
# Read N JSON records and exit; this example reads 5  
gpspipe -w -n 5 192.168.1.1
```

Chapter 2 Configuration

GNSS Configuration (continued)

5. Security Considerations

- `gpsd` on TCP port 2947 has no authentication or encryption. With `listen_globally='1'`, every LAN host can obtain positioning data. Take care if untrusted hosts are present on the LAN.
- Access from the WAN is blocked by default. If WAN access is required, use the input-rule procedure in Firewall Configuration, Allowing WAN Access to This Device. Always combine an interface restriction, such as `device='wwanin0'`, with a source IP restriction using `src_ip`.
- When LAN access is no longer needed, set `listen_globally='0'` to restore loopback-only listening. See subsection 6, Reverting the Configuration, in this section.

6. Reverting the Configuration

6.1 Disabling LAN Access (Loopback Only)

Input example

```
sudo uci set gpsd.core.listen_globally='0'  
sudo uci commit gpsd  
sudo /etc/init.d/gpsd restart  
  
# Check: listening only on 127.0.0.1:2947 indicates success  
sudo netstat -tunlp | grep 2947
```

Chapter 2 Configuration

GNSS Configuration (continued)

6.2 Stopping gpsd

Input example

```
sudo uci set gpsd.core.enabled='0'  
sudo uci commit gpsd  
sudo /etc/init.d/gpsd stop
```

6.3 Stopping the GNSS Module

Open the AT interface with `sudo microcom /dev/ttyUSBIN3` as described in 1.1. Send the following commands, then press Ctrl+X to exit.

Input example

```
AT$GPSP=0  
AT$GPSSAV
```

Chapter 2 Configuration

Firewall Configuration

Overview

This section explains how to configure the iR800B firewall. It covers the following settings.

- Port forwarding from the WAN, such as a cellular connection, to a LAN host.
- DMZ forwarding of all ports.
- Allowing WAN access to the device itself, such as SSH access restricted to a specific interface and source IP address.

Configure the firewall over SSH using uci commands. Settings are saved persistently and remain effective after a restart.

Prerequisites

- The applicable firmware version is iR8xxB-00.01.04. Specifications may change without notice following a firmware update.
- SSH access to the iR800B must be available.
- The cellular connection must be established and a WAN IP address assigned.
- The destination LAN host must be connected.

Chapter 2 Configuration

Firewall Configuration (continued)

1. Port Forwarding

Forward only specified ports and protocols to a LAN host.

1.1 Adding a Configuration

The following example forwards UDP port 12345 on the WAN to 192.168.1.99:12345.

Input example

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='UDP-12345-to-LAN'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].proto='udp'
sudo uci set firewall.@redirect[-1].src_dport='12345'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.99'
sudo uci set firewall.@redirect[-1].dest_port='12345'
sudo uci set firewall.@redirect[-1].target='DNAT'
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Chapter 2 Configuration

Firewall Configuration (continued)

1.2 Configuration Parameters

Parameter	Description	Example Settings
name	Rule name; an identifier of your choice.	UDP-12345-to-LAN
src	Source zone.	wan
dest	Destination zone.	lan
proto	Protocol.	udp / tcp / tcpudp
src_dport	Incoming port on the WAN.	12345
dest_ip	Destination LAN IP address.	192.168.1.99
dest_port	Destination port, if port translation is required.	12345
target	Action.	DNAT

Chapter 2 Configuration

Firewall Configuration (continued)

1.3 Multiple-Port Example

Input example

```
# TCP 8080 → 192.168.1.99:8080
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='TCP-8080-to-LAN'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].proto='tcp'
sudo uci set firewall.@redirect[-1].src_dport='8080'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.99'
sudo uci set firewall.@redirect[-1].dest_port='8080'
sudo uci set firewall.@redirect[-1].target='DNAT'

# UDP 9999 → 192.168.1.99:9999
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='UDP-9999-to-LAN'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].proto='udp'
sudo uci set firewall.@redirect[-1].src_dport='9999'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.99'
sudo uci set firewall.@redirect[-1].dest_port='9999'
sudo uci set firewall.@redirect[-1].target='DNAT'
```

Chapter 2 Configuration

Firewall Configuration (continued)

Input example

```
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

1.4 Port Translation (Different WAN and LAN Ports)

Example: forward TCP port 80 on the WAN to TCP port 8080 on the LAN.

Input example

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='TCP-80-to-8080'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].proto='tcp'
sudo uci set firewall.@redirect[-1].src_dport='80'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.99'
sudo uci set firewall.@redirect[-1].dest_port='8080'
sudo uci set firewall.@redirect[-1].target='DNAT'
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Chapter 2 Configuration

Firewall Configuration (continued)

2. DMZ Configuration

Forward all incoming WAN traffic, on all protocols and ports, to a specified LAN host.

2.1 Adding a Configuration

Input example

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='DMZ-to-192.168.1.99'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].proto='all'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.99'
sudo uci set firewall.@redirect[-1].target='DNAT'
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Note: Do not specify src_dport or dest_port for DMZ configuration. All ports are included.

Chapter 2 Configuration

Firewall Configuration (continued)

2.2 Choosing Between Port Forwarding and DMZ

Method	Use	Security
Port Forwarding	Expose only specific ports.	Only the required ports are opened.
DMZ	Forward all ports to a single host.	All ports are exposed; use caution.

Security Notice: DMZ configuration forwards all WAN traffic to the destination host. Configure an appropriate firewall on that host as well.

3. Allowing WAN Access to This Device (Input Rules)

New connections from the WAN zone (br-wan, wwanin0, wwanex0, phy0-sta0) are blocked by `reject_from_wan` by default. To allow WAN connections to the router itself, add a uci firewall rule.

Port forwarding with uci firewall redirect performs DNAT to a LAN host. The uci firewall rule described here permits input to the device itself. These functions serve different purposes and must not be confused.

Chapter 2 Configuration

Firewall Configuration (continued)

3.1 Allowing SSH via wwanin0 from One Source IP

This example allows only TCP port 22 (SSH) arriving through wwanin0, the internal cellular module, from source IP 203.0.113.10. SSH from other WAN interfaces (wwanex0, br-wan, phy0-sta0) or other source IP addresses remains blocked.

Input example

```
sudo uci add firewall rule
sudo uci set firewall.@rule[-1].name='Allow-SSH-wwanin-203.0.113.10'
sudo uci set firewall.@rule[-1].src='wan'
sudo uci set firewall.@rule[-1].device='wwanin0'
sudo uci set firewall.@rule[-1].src_ip='203.0.113.10'
sudo uci set firewall.@rule[-1].proto='tcp'
sudo uci set firewall.@rule[-1].dest_port='22'
sudo uci set firewall.@rule[-1].target='ACCEPT'
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Chapter 2 Configuration

Firewall Configuration (continued)

3.2 Configuration Parameters

Parameter	Description	Example Settings
name	Rule name; an identifier of your choice.	Allow-SSH-wwanin-203.0.113.10
src	Source zone.	wan
device	Incoming interface; an iifname restriction. Specify this to restrict access further to a particular interface within the WAN zone.	wwanin0 / wwanex0 / br-wan
src_ip	Permitted source IP address; CIDR notation is supported. If omitted, all sources are permitted.	203.0.113.10 / 203.0.113.0/24
proto	Protocol.	tcp / udp / tcpudp
dest_port	Incoming port on this device.	22
target	Action.	ACCEPT / REJECT / DROP

If device is omitted, the rule applies to all interfaces in the WAN zone: wwanin0, wwanex0, br-wan, and phy0-sta0. Always specify device when restricting access to a particular interface, such as wwanin0 only.

Chapter 2 Configuration

Firewall Configuration (continued)

3.3 Allowing Multiple Source IP Addresses

Use list `src_ip` to combine multiple source IP addresses or CIDR ranges in one rule.

Input example

```
sudo uci add firewall rule
sudo uci set firewall.@rule[-1].name='Allow-SSH-wwanin-multi'
sudo uci set firewall.@rule[-1].src='wan'
sudo uci set firewall.@rule[-1].device='wwanin0'
sudo uci add_list firewall.@rule[-1].src_ip='203.0.113.10'
sudo uci add_list firewall.@rule[-1].src_ip='203.0.113.10'
sudo uci add_list firewall.@rule[-1].src_ip='198.51.100.0/24'
sudo uci set firewall.@rule[-1].proto='tcp'
sudo uci set firewall.@rule[-1].dest_port='22'
sudo uci set firewall.@rule[-1].target='ACCEPT'
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Chapter 2 Configuration

Firewall Configuration (continued)

3.4 Checking the Applied nft Rules

A uci firewall rule is inserted into the input_wan chain of the inet fw4 table, immediately before the final jump reject_from_wan, in the following form: iifname "<device>" ip saddr <src_ip> tcp dport <dest_port> accept.

Input example

```
sudo nft -a list chain inet fw4 input_wan
```

Output Example (Relevant Line)

```
iifname "wwanin0" ip saddr 203.0.113.10 tcp dport 22 counter packets 0 bytes 0 accept comment "!fw4: Allow-SSH-wwanin-203.0.113.10"  
jump reject_from_wan
```

Security Notes

- If src_ip is omitted, any WAN source can attempt SSH access, exposing the service to brute-force attacks. Always restrict the source IP address.
- Use strong SSH authentication, such as public-key authentication or a sufficiently long password.
- Remove rules promptly when they are no longer needed. See subsections 5.1 and 5.3 in this section.

Chapter 2 Configuration

Firewall Configuration (continued)

3.5 Using DMZ and Access to This Device Together

With DMZ configured as described in subsection 2, DMZ Configuration, DNAT in `dstnat_wan` rewrites the destination IP address of all incoming WAN traffic to the DMZ host during PREROUTING. This occurs before the routing decision. Packets whose destination has become the DMZ host follow the FORWARD path and never reach `input_wan`. Consequently, the input rule added in 3.1 has no opportunity to match when used with DMZ, and WAN SSH access to the device becomes unavailable.

Observed behavior: an SSH attempt from the WAN is actually DNATed to TCP port 22 on the DMZ host. If that host runs SSH, the connection reaches the DMZ host rather than the router; otherwise, the attempt may simply appear to fail.

3.5.1 Solution: Place a Redirect to This Device Before DMZ

Evaluation order in `dstnat_wan` follows the index order of `uci firewall redirect` entries. Place a redirect performing DNAT to the device's LAN IP, for example 192.168.1.1, before the DMZ entry. The packet matches that redirect first, and `conntrack` records the NAT decision, so the later DMZ DNAT is not applied. The routing decision then recognizes the destination as the device itself and sends the packet through INPUT to `input_wan`. Keep the input rule from 3.1, `firewall.@rule[*]`, to permit it there.

Chapter 2 Configuration

Firewall Configuration (continued)

3.5.2 Configuration Example

Allow TCP port 22 from 203.0.113.10 through wwanin0 to this device, while forwarding all other incoming WAN traffic to DMZ host 192.168.1.99.

Input example

```
# 1) Add the SSH redirect to this device first: @redirect[0]
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='SSH-to-router-before-DMZ'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].src_ip='203.0.113.10'
sudo uci set firewall.@redirect[-1].proto='tcp'
sudo uci set firewall.@redirect[-1].src_dport='22'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.1'
sudo uci set firewall.@redirect[-1].dest_port='22'
sudo uci set firewall.@redirect[-1].target='DNAT'
```

Chapter 2 Configuration

Firewall Configuration (continued)

Input example

```
# 2) Add the DMZ redirect afterward: @redirect[1]
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].name='DMZ-to-192.168.1.99'
sudo uci set firewall.@redirect[-1].src='wan'
sudo uci set firewall.@redirect[-1].dest='lan'
sudo uci set firewall.@redirect[-1].proto='all'
sudo uci set firewall.@redirect[-1].dest_ip='192.168.1.99'
sudo uci set firewall.@redirect[-1].target='DNAT'

sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Important: The SSH redirect must have a lower index than the DMZ redirect. If the order is reversed, DMZ matches all WAN traffic first and makes the SSH redirect ineffective. If DMZ already occupies @redirect[0], add the SSH redirect and move it to the first position using `uci reorder firewall.@redirect[-1]=0` before committing and restarting.

3.5.3 Checking the Applied nft Rules

In `dstnat_wan`, the SSH DNAT entry appears above the DMZ entry and is evaluated first.

Chapter 2 Configuration

Firewall Configuration (continued)

Input example

```
sudo nft -a list chain inet fw4 dstnat_wan
```

Input example

```
chain dstnat_wan {  
    ip saddr 203.0.113.10 tcp dport 22 dnat ip to 192.168.1.1:22 comment "!fw4: SSH-to-router-before-DMZ"  
    meta nfproto ipv4 dnat ip to 192.168.1.99 comment "!fw4: DMZ-to-192.168.1.99"  
}
```

The input rule added in 3.1 remains in input_wan and permits SSH packets that have been DNATed to the device itself.

Input example

```
sudo nft -a list chain inet fw4 input_wan
```

Relevant Line

```
iifname "wwanin0" ip saddr 203.0.113.10 tcp dport 22 accept comment "!fw4: Allow-SSH-wwanin-203.0.113.10"
```

Chapter 2 Configuration

Firewall Configuration (continued)

3.5.4 Packet Processing Flow (Summary)

For a TCP port 22 packet from 203.0.113.10 arriving through wwanin0:

1. Arrival on wwanin0 -> PREROUTING (dstnat_wan).
2. Match the SSH redirect, @redirect[0] -> rewrite the destination to 192.168.1.1:22.
3. Routing decision: 192.168.1.1 is the device's own LAN IP -> INPUT path.
4. INPUT -> input_wan; iifname=wwanin0 is retained.
5. Match the input rule Allow-SSH-wwanin-203.0.113.10 -> ACCEPT.
6. The router itself responds to SSH.

For other incoming WAN traffic:

1. PREROUTING (dstnat_wan)
2. No match on the SSH redirect -> match the DMZ redirect, @redirect[1] -> rewrite the destination to 192.168.1.99.
3. Routing decision: 192.168.1.99 is a LAN host -> FORWARD path.
4. The forward_wan rule ct status dnat accept permits forwarding to the DMZ host.

Chapter 2 Configuration

Firewall Configuration (continued)

3.5.5 Removal Precautions

To remove a combined DMZ and device-access configuration, first check the indices with `uci show firewall | grep '@redirect'`, then delete entries from the highest index downward. Deleting a lower index first shifts later entries and may cause the wrong rule to be deleted.

Input example

```
sudo uci show firewall | grep '@redirect'
# firewall.@redirect[0].name='SSH-to-router-before-DMZ'
# firewall.@redirect[1].name='DMZ-to-192.168.1.99'

# Remove DMZ only; keep the SSH path
sudo uci delete firewall.@redirect[1]
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Input example

```
# Remove both
sudo uci delete firewall.@redirect[1] # Delete the higher index first
sudo uci delete firewall.@redirect[0]
sudo uci commit firewall
sudo /etc/init.d/firewall restart 2>/dev/null
```

Chapter 2 Configuration

Firewall Configuration (continued)

4. Checking the Configuration

4.1 Listing Current Redirect Settings

Input example

```
sudo uci show firewall | grep redirect
```

4.2 Listing Current Input-Rule Settings

Input example

```
sudo uci show firewall | grep "@rule"
```

Chapter 2 Configuration

Firewall Configuration (continued)

4.3 Checking nftables Rules

Input example

```
# DNAT (destination translation) rules
sudo nft list chain inet fw4 dstnat_wan

# Forwarding permission rules for port forwarding
sudo nft list chain inet fw4 forward_wan

# Rules permitting WAN input to this device
sudo nft -a list chain inet fw4 input_wan
```

5. Removing or Reverting Settings

5.1 Deleting a Specific Redirect Rule

Input example

```
# Check the current settings and identify the index
sudo uci show firewall | grep redirect
```

Chapter 2 Configuration

Firewall Configuration (continued)

Output example

```
firewall.@redirect[0].name='UDP-12345-to-LAN'  
firewall.@redirect[1].name='TCP-8080-to-LAN'
```

Input example

```
# Delete by index; this example removes [0]  
sudo uci delete firewall.@redirect[0]  
sudo uci commit firewall  
sudo /etc/init.d/firewall restart 2>/dev/null
```

Note: Indices start at zero. Deleting an entry shifts later indices down. When deleting multiple entries, work from the highest index downward.

5.2 Checking Redirect Removal

Input example

```
# Check that no redirect remains  
sudo uci show firewall | grep redirect  
  
# Check that the nft rule has been removed  
sudo nft list chain inet fw4 dstnat_wan 2>/dev/null
```

Chapter 2 Configuration

Firewall Configuration (continued)

5.3 Deleting a Specific Input Rule

Input example

```
# Check the current rules and identify the index  
sudo uci show firewall | grep "@rule"
```

Output Example

```
firewall.@rule[9].name='Allow-SSH-wwanin-203.0.113.10'
```

Input example

```
# Delete by index; this example removes [9]  
sudo uci delete firewall.@rule[9]  
sudo uci commit firewall  
sudo /etc/init.d/firewall restart 2>/dev/null
```

Note: @rule contains many basic rules generated by fw4, such as ICMP and DHCP permissions. Always check name and delete only rules you added. Deleting a default rule by mistake may prevent communication.

Chapter 2 Configuration

Firewall Configuration (continued)

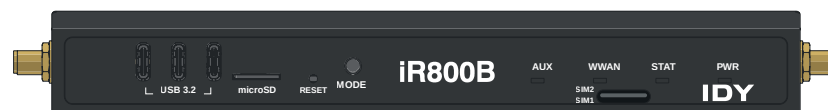
5.4 Checking Rule Removal

Input example

```
# Check that the rule you added no longer remains
sudo uci show firewall | grep "@rule" | grep -i "Allow-SSH"

# Check that the nft rule has been removed
sudo nft -a list chain inet fw4 input_wan
```

Chapter 3 LEDs



LED	Device State	Indication	Flash Cycle
PWR Green	Power switch OFF	Off	-
	Power switch ON	On	-
STAT Red	During the factory-reset operation	On	-
	Restoring factory settings	Rapid flashing	-
STAT Blue	WWAN connection disconnected	Off	-
	UMTS connected	Flashing	On 400 ms / Off 100 ms
	LTE connected (without EN-DC)	Flashing	On 2900 ms / Off 100 ms
	LTE connected (with EN-DC)	Flashing	On 4900 ms / Off 100 ms
	NR connected	On	-
WWAN Red	WWAN disconnected / Medium signal / High signal	Off	-
	Low signal strength	Flashing	-
	Out of service / Signal strength unavailable	On	-
WWAN Blue	WWAN disconnected / Low signal / Abnormal state	Off	-
	Medium signal strength	Flashing	-
	High signal strength	On	-

Chapter 4 Specifications

Product Specifications

System

Item	Specification
OS	Linux: OpenWRT
CPU	Quad-core Arm Cortex-A73 1.8GHz
RAM	DDR4 4GB (2x2GB) or 2GB (2x1GB)
eMMC	8GB
Flash	128MB
SD Card	microSD

Modem

Item	Specification
Supported Bands	LTE: B1/B3/B8/B18/B19/B26/B28/B41/B42 5G: n1/n3/n28/n41/n77/n78/n79 (NSA/SA)

Chapter 4 Specifications

Product Specifications (continued)

Item	Specification
Carrier Aggregation / Bandwidth	LTE: up to 7CA 5G: 3CC CA; bandwidth up to 200 MHz
MIMO	LTE DL: 4x4 MIMO 5G DL: 4x4 MIMO 5G UL: 2x2 MIMO
SIM	Nano-SIM x 1
Other	Release 16 support Mitigation control as temperature rises

Network and Device Interfaces

Item	Specification
Wireless LAN	802.11a/b/g/n/ac/ax (STA/AP)
Wired LAN	RJ45 10/100/1000Mbps x 2 RJ45 10Gbps x 1 SFP+ 10Gbps x 1

Chapter 4 Specifications

Product Specifications (continued)

Item	Specification
Bluetooth	V5.2
GNSS	GPS/GLONASS/BeiDou/Galileo/QZSS
USB	USB3.2 x 3

Enclosure and Power

Item	Specification
Dimensions	W 200 x H 25 x D 105 mm Excluding protrusions
Weight	650 g, excluding the power supply
Power Supply	Dedicated AC adapter or USB Power Delivery

Chapter 4 Specifications

Product Specifications (continued)

Operating Environment

Item	Specification
Operating Temperature	-10 to +60 deg C
Storage Temperature	-20 to +70 deg C
Operating Humidity	10% to 95%, non-condensing

Chapter 5 Open-Source Licenses

Open-Source Software

This product uses software made available under open-source licenses or in the public domain.

The software used is listed below.

apk-mbedtls-3.0.0_pre20241113-r1 (GPL-2.0-only)	coreutils-timeout-9.3-r1 (GPL-3.0-or-later)
base-files-1678~8c1b1b0780 (GPL-2.0)	dbus-1.14.10-r1 (AFL-2.1)
bash-5.2.32-r1 (GPL-3.0-or-later)	diffutils-3.10-r1 (GPL-3.0)
block-mount-2024.07.14~408c2cc4-r1 (GPL-2.0)	dmesg-2.40.2-r1 (GPL-2.0-only)
blockd-2024.07.14~408c2cc4-r1 (GPL-2.0)	dnsmasq-2.90-r3 (GPL-2.0)
bluelog-1.1.2-r5 (GPL-2.0)	dropbear-2024.85-r1 (MIT)
bluelog-live-1.1.2-r5 (GPL-2.0)	e2fsprogs-1.47.0-r2 (GPL-2.0)
bluez-daemon-5.72-r2 (GPL-2.0-or-later)	ethtool-full-6.10-r1 (GPL-2.0)
bluez-libs-5.72-r2 (GPL-2.0-or-later)	f2fsck-1.16.0-r3 (GPL-2.0-only)
bluez-tools-2020.10.25~f6532173-r1 (GPL-2.0-only)	fdisk-2.40.2-r1 (GPL-2.0-only)
bluez-utils-5.72-r2 (GPL-2.0-or-later)	firewall4-2024.05.21~4c01d1eb-r1 (ISC)
bluez-utils-btmon-5.72-r2 (GPL-2.0-or-later)	fitblk-2 (GPL-2.0-only)
bluez-utils-extra-5.72-r2 (GPL-2.0-or-later)	fstools-2024.07.14~408c2cc4-r1 (GPL-2.0)
busybox-1.36.1-r2 (GPL-2.0)	fwtool-2019.11.12~8f7fe925-r1 (GPL-2.0)
ca-bundle-20240203-r1 (GPL-2.0-or-later)	getrandom-2024.04.26~85f10530-r1 (GPL-2.0)
cgi-io-2022.08.10~901b0f04-r21 (GPL-2.0-or-later)	glib2-2.82.0-r1 (LGPL-2.1-or-later)
coreutils-9.3-r1 (GPL-3.0-or-later)	gpiocli-sysfs-0.0.7-r1 (LGPL-2.1-or-later)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

gpiod-tools-2.1.3-r1 (LGPL-2.1-or-later)	kmod-crypto-cmac-6.6.60-r1 (GPL-2.0-only)
gpsd-3.25-r1 (BSD-3-Clause)	kmod-crypto-crc32c-6.6.60-r1 (GPL-2.0-only)
gpsd-clients-3.25-r1 (BSD-3-Clause)	kmod-crypto-ctr-6.6.60-r1 (GPL-2.0-only)
gpsd-utils-3.25-r1 (BSD-3-Clause)	kmod-crypto-des-6.6.60-r1 (GPL-2.0-only)
hostapd-common-2024.09.15~5ace39b0-r1 (BSD-3-Clause)	kmod-crypto-ecb-6.6.60-r1 (GPL-2.0-only)
hwinform-21.71-r4 (GPL-2.0-or-later)	kmod-crypto-ecdh-6.6.60-r1 (GPL-2.0-only)
i2c-tools-4.3-r3 (GPL-2.0-or-later)	kmod-crypto-gcm-6.6.60-r1 (GPL-2.0-only)
iperf3-3.17.1-r4 (BSD-3-Clause)	kmod-crypto-geniv-6.6.60-r1 (GPL-2.0-only)
iptables-nft-1.8.10-r1 (GPL-2.0)	kmod-crypto-gf128-6.6.60-r1 (GPL-2.0-only)
iw-6.9-r1 (GPL-2.0)	kmod-crypto-ghash-6.6.60-r1 (GPL-2.0-only)
iwinform-2024.10.20~b94f066e-r1 (GPL-2.0)	kmod-crypto-hash-6.6.60-r1 (GPL-2.0-only)
jansson-4.2.14-r3 (MIT)	kmod-crypto-hmac-6.6.60-r1 (GPL-2.0-only)
jshn-2024.03.29~eb9bcb64-r1 (ISC)	kmod-crypto-hw-safexcel-6.6.60-r1 (GPL-2.0-only)
jsonfilter-2024.01.23~594cfa86-r1 (ISC)	kmod-crypto-kpp-6.6.60-r1 (GPL-2.0-only)
kernel-6.6.60~a70e9908e118ec1a5d9e56afb5bb1339-r1 (GPL-2.0-only)	kmod-crypto-manager-6.6.60-r1 (GPL-2.0-only)
kmod-bluetooth-6.6.60-r1 (GPL-2.0-only)	kmod-crypto-md5-6.6.60-r1 (GPL-2.0-only)
kmod-cfg80211-6.6.60.6.11.2-r1 (GPL-2.0-only)	kmod-crypto-null-6.6.60-r1 (GPL-2.0-only)
kmod-crypto-aead-6.6.60-r1 (GPL-2.0-only)	kmod-crypto-rng-6.6.60-r1 (GPL-2.0-only)
kmod-crypto-authenc-6.6.60-r1 (GPL-2.0-only)	kmod-crypto-seqiv-6.6.60-r1 (GPL-2.0-only)
kmod-crypto-ccm-6.6.60-r1 (GPL-2.0-only)	kmod-crypto-sha1-6.6.60-r1 (GPL-2.0-only)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

kmod-crypto-sha256-6.6.60-r1 (GPL-2.0-only)

kmod-crypto-sha3-6.6.60-r1 (GPL-2.0-only)

kmod-crypto-sha512-6.6.60-r1 (GPL-2.0-only)

kmod-eeprom-at24-6.6.60-r1 (GPL-2.0-only)

kmod-fs-autofs4-6.6.60-r1 (GPL-2.0-only)

kmod-gpio-button-hotplug-6.6.60-r5 (GPL-2.0)

kmod-hid-6.6.60-r1 (GPL-2.0-only)

kmod-hwmon-core-6.6.60-r1 (GPL-2.0-only)

kmod-hwmon-pwmfan-6.6.60-r1 (GPL-2.0-only)

kmod-i2c-core-6.6.60-r1 (GPL-2.0-only)

kmod-i2c-mux-6.6.60-r1 (GPL-2.0-only)

kmod-i2c-mux-pca954x-6.6.60-r1 (GPL-2.0-only)

kmod-input-core-6.6.60-r1 (GPL-2.0-only)

kmod-input-evdev-6.6.60-r1 (GPL-2.0-only)

kmod-ipt-core-6.6.60-r1 (GPL-2.0-only)

kmod-leds-gpio-6.6.60-r1 (GPL-2.0-only)

kmod-lib-crc-ccitt-6.6.60-r1 (GPL-2.0-only)

kmod-lib-crc16-6.6.60-r1 (GPL-2.0-only)

kmod-lib-crc32c-6.6.60-r1 (GPL-2.0-only)

kmod-libphy-6.6.60-r1 (GPL-2.0-only)

kmod-mac80211-6.6.60.6.11.2-r1 (GPL-2.0-only)

kmod-mt76-connac-6.6.60.2024.10.11.1~ecca0e77-r1 (GPLv2)

kmod-mt76-core-6.6.60.2024.10.11.1~ecca0e77-r1 (GPLv2)

kmod-mt7996-233-firmware-6.6.60.2024.10.11.1~ecca0e77-r1 (GPLv2)

kmod-mt7996-firmware-6.6.60.2024.10.11.1~ecca0e77-r1 (GPLv2)

kmod-mt7996-firmware-common-6.6.60.2024.10.11.1~ecca0e77-r1 (GPLv2)

kmod-mt7996e-6.6.60.2024.10.11.1~ecca0e77-r1 (GPLv2)

kmod-nf-contrack-6.6.60-r1 (GPL-2.0-only)

kmod-nf-contrack6-6.6.60-r1 (GPL-2.0-only)

kmod-nf-flow-6.6.60-r1 (GPL-2.0-only)

kmod-nf-ipt-6.6.60-r1 (GPL-2.0-only)

kmod-nf-log-6.6.60-r1 (GPL-2.0-only)

kmod-nf-log6-6.6.60-r1 (GPL-2.0-only)

kmod-nf-nat-6.6.60-r1 (GPL-2.0-only)

kmod-nf-reject-6.6.60-r1 (GPL-2.0-only)

kmod-nf-reject6-6.6.60-r1 (GPL-2.0-only)

kmod-nfnetlink-6.6.60-r1 (GPL-2.0-only)

kmod-nft-compat-6.6.60-r1 (GPL-2.0-only)

kmod-nft-core-6.6.60-r1 (GPL-2.0-only)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

kmod-nft-fib-6.6.60-r1 (GPL-2.0-only)	kmod-usb-core-6.6.60-r1 (GPL-2.0-only)
kmod-nft-nat-6.6.60-r1 (GPL-2.0-only)	kmod-usb-xhci-hcd-6.6.60-r1 (GPL-2.0-only)
kmod-nft-offload-6.6.60-r1 (GPL-2.0-only)	kmod-usb-xhci-mtk-6.6.60-r1 (GPL-2.0-only)
kmod-nls-base-6.6.60-r1 (GPL-2.0-only)	kmod-usb3-6.6.60-r1 (GPL-2.0-only)
kmod-phy-aquantia-6.6.60-r1 (GPL-2.0-only)	libatomic1-13.3.0-r4 (GPL-3.0-with-GCC-exception)
kmod-phylink-6.6.60-r1 (GPL-2.0-only)	libattr-2.5.2-r3 (LGPL-2.1-or-later)
kmod-ppp-6.6.60-r1 (GPL-2.0-only)	libblkid1-2.40.2-r1 (GPL-2.0-only)
kmod-pppoe-6.6.60-r1 (GPL-2.0-only)	libblobmsg-json20240329-2024.03.29~eb9bcb64-r1 (ISC)
kmod-pppox-6.6.60-r1 (GPL-2.0-only)	libbpf1-1.4.6-r1 (LGPL-2.1 OR BSD-2-Clause)
kmod-regmap-core-6.6.60-r1 (GPL-2.0-only)	libbz2-1.0-1.0.8-r1 (bzip2-1.0.8)
kmod-regmap-i2c-6.6.60-r1 (GPL-2.0-only)	libc-1.2.5-r4 (GPL-3.0-with-GCC-exception)
kmod-rtc-pcf8563-6.6.60-r1 (GPL-2.0-only)	libcomerr0-1.47.0-r2 (GPL-2.0)
kmod-rtw89-6.6.60.6.11.2-r1 (GPL-2.0-only)	libdbus-1.14.10-r1 (AFL-2.1)
kmod-rtw89-8852b-common-6.6.60.6.11.2-r1 (GPL-2.0-only)	libe2p2-1.47.0-r2 (GPL-2.0)
kmod-rtw89-8852be-6.6.60.6.11.2-r1 (GPL-2.0-only)	libelf1-0.191-r1 (GPL-3.0-or-later)
kmod-rtw89-pci-6.6.60.6.11.2-r1 (GPL-2.0-only)	libevdev-1.13.1-r1 (MIT)
kmod-sched-core-6.6.60-r1 (GPL-2.0-only)	libexpat-2.6.3-r1 (MIT)
kmod-sfp-6.6.60-r1 (GPL-2.0-only)	libext2fs2-1.47.0-r2 (GPL-2.0)
kmod-sihc-6.6.60-r1 (GPL-2.0-only)	libf2fs6-1.16.0-r3 (GPL-2.0-only)
kmod-tun-6.6.60-r1 (GPL-2.0-only)	libfdisk1-2.40.2-r1 (GPL-2.0-only)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

libffi-3.4.6-r1 (MIT)	libmount1-2.40.2-r1 (GPL-2.0-only)
libfstools-bootparam-2024.07.14~408c2cc4-r1 (GPL-2.0)	libncurses6-6.4-r2 (MIT)
libgcc1-13.3.0-r4 (GPL-3.0-with-GCC-exception)	libnftnl11-1.2.8-r1 (GPL-2.0-or-later)
libgpiod-2.1.3-r1 (LGPL-2.1-or-later)	libnl-tiny1-2023.12.05~965c4bf4-r1 (LGPL-2.1)
libi2c-4.3-r3 (GPL-2.0-or-later)	libopenssl3-3.0.15-r1 (Apache-2.0)
libical-3.0.9-r2 (LGPL-2.1-or-later)	libpcap1-1.10.5-r1 (BSD-3-Clause)
libiperf3-3.17.1-r4 (BSD-3-Clause)	libpci-3.12.0-r2 (GPL-2.0)
libiptext-nft0-1.8.10-r1 (GPL-2.0)	libpcre2-10.42-r1 (BSD-3-Clause)
libiptext0-1.8.10-r1 (GPL-2.0)	libpthread-1.2.5-r4 (GPL-3.0-with-GCC-exception)
libiptext6-0-1.8.10-r1 (GPL-2.0)	libpython3-3.11-3.11.10-r1 (Python-2.0.1)
libiwininfo-data-2024.10.20~b94f066e-r1 (GPL-2.0)	libqmi-1.34.0-r2 (LGPL-2.0-or-later)
libiwininfo20230701-2024.10.20~b94f066e-r1 (GPL-2.0)	libqrtr-glib-1.2.2-r3 (LGPL-2.1-or-later)
libjson-c5-0.18-r1 (MIT)	libreadline8-8.2-r2 (GPL-3.0-or-later)
libjson-script20240329-2024.03.29~eb9bcb64-r1 (ISC)	librespeed-cli-1.0.10-r3 (LGPL-3.0-only)
libkmod-32-r1 (LGPL-2.1-or-later)	librt-1.2.5-r4 (GPL-3.0-with-GCC-exception)
liblucihttp-ucode-2023.03.15~9b5b683f-r1 (ISC)	libsensors5-3.6.0-r1 (GPL-2.0-or-later)
liblucihttp0-2023.03.15~9b5b683f-r1 (ISC)	libsmartcols1-2.40.2-r1 (GPL-2.0-only)
libmbedtls1-3.6.2-r1 (GPL-2.0-or-later)	libss2-1.47.0-r2 (GPL-2.0)
libmbim-1.30.0-r2 (LGPL-2.0-or-later)	libsysfs2-2.1.0-r4 (LGPL-2.1)
libmnl0-1.0.5-r1 (LGPL-2.1+)	libubox20240329-2024.03.29~eb9bcb64-r1 (ISC)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

libubus2024.10.20~252a9b0c-r1 (LGPL-2.1)
libuci20130104-2023.08.10~5781664d-r1 (LGPL-2.1)
libuclient20201210-2024.10.22~88ae8f20-r1 (ISC)
libucode20230711-2024.07.22~b610860d-r3 (ISC)
libudbug-2023.12.06~6d3f51f9 (GPL-2.0)
libudev-zero-1.0.3-r1 (MIT)
libugpio-0.0.7-r1 (LGPL-2.1-or-later)
libusb-1.0-0-1.0.27-r1 (LGPL-2.1-or-later)
libustream-mbedtls20201210-2024.07.28~99bd3d2b-r1 (ISC)
libuuid1-2.40.2-r1 (GPL-2.0-only)
libxtables12-1.8.10-r1 (GPL-2.0)
lm-sensors-3.6.0-r1 (GPL-2.0-or-later)
lm-sensors-detect-3.6.0-r1 (GPL-2.0-or-later)
logd-2024.04.26~85f10530-r1 (GPL-2.0)
logger-2.40.2-r1 (GPL-2.0-only)
lsblk-2.40.2-r1 (GPL-2.0-only)
lscpu-2.40.2-r1 (GPL-2.0-only)
luci-25.044.01350~033986c (Apache-2.0)
luci-app-firewall-25.044.01350~033986c (Apache-2.0)
luci-app-package-manager-25.044.01350~033986c (Apache-2.0)

luci-base-25.044.01350~033986c (Apache-2.0)
luci-i18n-base-ja-25.044.01350~033986c (Apache-2.0)
luci-i18n-firewall-ja-25.044.01350~033986c (Apache-2.0)
luci-i18n-package-manager-ja-25.044.01350~033986c (Apache-2.0)
luci-light-25.044.01350~033986c (Apache-2.0)
luci-mod-admin-full-25.044.01350~033986c (Apache-2.0)
luci-mod-network-25.044.01350~033986c (Apache-2.0)
luci-mod-status-25.044.01350~033986c (Apache-2.0)
luci-mod-system-25.044.01350~033986c (Apache-2.0)
luci-proto-ipv6-25.044.01350~033986c (Apache-2.0)
luci-proto-ppp-25.044.01350~033986c (Apache-2.0)
luci-theme-bootstrap-25.044.01350~033986c (Apache-2.0)
mbim-utils-1.30.0-r2 (GPL-2.0-or-later)
mkf2fs-1.16.0-r3 (GPL-2.0-only)
mtd-26 (GPL-2.0+)
nand-utils-2.2.1-r1 (GPLv2)
netifd-2024.11.08~34eb11eb-r1 (GPL-2.0)
nftables-json-1.1.1-r1 (GPL-2.0)
odhcp6c-2023.05.12~bcd28363-r20 (GPL-2.0)
odhcpd-ipv6only-2024.05.08~a2988231-r1 (GPL-2.0)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

openwrt-keyring-2024.11.01~fbae29d7-r2 (GPL-2.0)

opkg-2024.10.16~38eccbb1-r1 (GPL-2.0)

pciids-0.387-r1 (GPL-2.0-or-later)

pciutils-3.12.0-r2 (GPL-2.0)

perl-5.40.0-r2 (GPL-1.0-or-later)

perlbase-base-5.40.0-r2 (GPL-1.0-or-later)

perlbase-bytes-5.40.0-r2 (GPL-1.0-or-later)

perlbase-class-5.40.0-r2 (GPL-1.0-or-later)

perlbase-config-5.40.0-r2 (GPL-1.0-or-later)

perlbase-cwd-5.40.0-r2 (GPL-1.0-or-later)

perlbase-errno-5.40.0-r2 (GPL-1.0-or-later)

perlbase-essential-5.40.0-r2 (GPL-1.0-or-later)

perlbase-fcntl-5.40.0-r2 (GPL-1.0-or-later)

perlbase-file-5.40.0-r2 (GPL-1.0-or-later)

perlbase-filehandle-5.40.0-r2 (GPL-1.0-or-later)

perlbase-i18n-5.40.0-r2 (GPL-1.0-or-later)

perlbase-integer-5.40.0-r2 (GPL-1.0-or-later)

perlbase-io-5.40.0-r2 (GPL-1.0-or-later)

perlbase-list-5.40.0-r2 (GPL-1.0-or-later)

perlbase-locale-5.40.0-r2 (GPL-1.0-or-later)

perlbase-params-5.40.0-r2 (GPL-1.0-or-later)

perlbase-posix-5.40.0-r2 (GPL-1.0-or-later)

perlbase-re-5.40.0-r2 (GPL-1.0-or-later)

perlbase-scalar-5.40.0-r2 (GPL-1.0-or-later)

perlbase-selectsaver-5.40.0-r2 (GPL-1.0-or-later)

perlbase-socket-5.40.0-r2 (GPL-1.0-or-later)

perlbase-symbol-5.40.0-r2 (GPL-1.0-or-later)

perlbase-tie-5.40.0-r2 (GPL-1.0-or-later)

perlbase-unicore-5.40.0-r2 (GPL-1.0-or-later)

perlbase-utf8-5.40.0-r2 (GPL-1.0-or-later)

perlbase-xsloader-5.40.0-r2 (GPL-1.0-or-later)

phytool-2 (GPL-2.0+)

ppp-2.5.1-r1 (BSD-4-Clause)

ppp-mod-pppoe-2.5.1-r1 (BSD-4-Clause)

procd-2024.11.06~109fa41b-r1 (GPL-2.0)

procd-seccomp-2024.11.06~109fa41b-r1 (GPL-2.0)

procd-ujail-2024.11.06~109fa41b-r1 (GPL-2.0)

python3-base-3.11.10-r1 (Python-2.0.1)

python3-light-3.11.10-r1 (Python-2.0.1)

qmi-utils-1.34.0-r2 (GPL-2.0-or-later)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

rpcd-2024.09.17~9f4b86e7-r1 (ISC)	ucode-mod-fs-2024.07.22~b610860d-r3 (ISC)
rpcd-mod-file-2024.09.17~9f4b86e7-r1 (ISC)	ucode-mod-html-1 (ISC)
rpcd-mod-iwinfo-2024.09.17~9f4b86e7-r1 (ISC)	ucode-mod-math-2024.07.22~b610860d-r3 (ISC)
rpcd-mod-luci-20240305-r1 (Apache-2.0)	ucode-mod-nl80211-2024.07.22~b610860d-r3 (ISC)
rpcd-mod-rrdns-20170710 (Apache-2.0)	ucode-mod-rtnl-2024.07.22~b610860d-r3 (ISC)
rpcd-mod-ucode-2024.09.17~9f4b86e7-r1 (ISC)	ucode-mod-ubus-2024.07.22~b610860d-r3 (ISC)
sudo-1.9.16_p2-r1 (ISC)	ucode-mod-uci-2024.07.22~b610860d-r3 (ISC)
sysfsutils-2.1.0-r4 (LGPL-2.1)	ucode-mod-uloop-2024.07.22~b610860d-r3 (ISC)
tc-full-6.11.0-r1 (GPL-2.0)	uhttpd-2023.06.25~34a8a74d-r4 (ISC)
tcpdump-4.99.5-r1 (BSD-3-Clause)	uhttpd-mod-ubus-2023.06.25~34a8a74d-r4 (ISC)
terminfo-6.4-r2 (MIT)	urandom-seed-3 (GPL-2.0-only)
tune2fs-1.47.0-r2 (GPL-2.0)	urngd-2023.11.01~44365eb1-r1 (GPL-2.0)
ubi-utils-2.2.1-r1 (GPLv2)	usbids-0.387-r1 (GPL-2.0-or-later)
uboot-envtools-2024.07-r1 (GPL-2.0)	usbutils-017-r1 (GPL-2.0-only)
ubox-2024.04.26~85f10530-r1 (GPL-2.0)	usign-2020.05.23~f1f65026-r1 (ISC)
ubus-2024.10.20~252a9b0c-r1 (LGPL-2.1)	wifi-scripts-1.0-r1 (GPL-2.0)
ubusd-2024.10.20~252a9b0c-r1 (LGPL-2.1)	wireless-regdb-2024.10.07-r1 (ISC)
uci-2023.08.10~5781664d-r1 (LGPL-2.1)	wpad-basic-mbedtls-2024.09.15~5ace39b0-r1 (BSD-3-Clause)
uclient-fetch-2024.10.22~88ae8f20-r1 (ISC)	xtables-nft-1.8.10-r1 (GPL-2.0)
ucode-2024.07.22~b610860d-r3 (ISC)	zlib-1.3.1-r1 (Zlib)

Chapter 5 Open-Source Licenses

Open-Source Software (continued)

The software and license information listed above can be downloaded from the following website.

<https://sources.openwrt.org>

For information about modified software and how it is distributed, contact IDY's support desk.

Any costs incurred in distribution are borne by the customer.

Because of the nature of open-source software, its operation is not warranted.

The product itself is covered by IDY's product warranty policy.

Contact

Product Support

IDY Corporation

Telephone: +81-3-4400-7970

Office hours: 10:00-12:00 and 13:00-17:00 (Japan time).

Monday to Friday, excluding Saturdays, Sundays, public holidays, and designated company holidays.

Email: contact@idy-design.com

Website: <https://idy-design.com/>

6F Foresta Akihabara Building, 3-9-3 Iwamoto-cho, Chiyoda-ku, Tokyo 101-0032, Japan.

