Robustel R1511 VPN Configuration with Güralp Data Centre

What is WireGuard?

WireGuard is a modern high-speed VPN protocol designed for use on embedded interfaces, utilising state-of-the-art cryptography.

Robustel R1511 Router

The Robustel R1511 router supports WireGuard VPN for secure, high-performance connectivity, ideal for remote access to industrial network configurations. A WireGuard VPN can be established on the router via the configuration web page, with no additional installation or requirements.

Güralp Data Centre Overview

Güralp Systems Data Centre software package (acquisition software package) consists of several applications with the primary purpose of acquiring, saving and re-redistributing miniSEED data. It also provides system state of health monitoring and distribution, with remote configuration capabilities.

Güralp Data Box

Güralp Data Box comes pre-installed with all the necessary software required to host and run a GDC instance. In simplest terms, it is a ‘GDC-in-a-box’ which can be further configured to monitor seismic instruments on a network, edit the parameters of instruments and share data from the self-hosted SeedLink server.

A Güralp Registry server provides communication functionality between instruments on a network and the GDC instance. To add a device to the registry, the instrument/digitiser must be configured with the registry address and a group ID, which can be edited through the device’s configuration webpage (accessible via discovery or HTTPS).

In the case of a GDB, the registry address is simply the IP address of the GDB itself.

Configuring WireGuard VPN with Güralp Data Centre

In the example provided below, we are connecting to the Güralp Data Centre "London". The details provided will vary depending on the user application and will typically be provided by the Data Centre administrator.

Summary Instructions

1. Configure the local IP address of the Robustel R1511 router to be 192.168.38.1
2. Configure the DHCP server on the router with an address range from 192.168.38.66 to 192.168.38.94
3. Configure the WireGuard VPN with the following parameters:

```
[Interface]
       Address = 172.26.0.38/24
       1280 ≤ MTU ≤ 1420
       PrivateKey = ****************************************

[1st Peer]
       AllowedIPs = 172.26.0.0/29
       Endpoint = london.guralp.com
       ListeningPort = 51820
       PersistentKeepalive = 25
       PublicKey = e6n0gHGJjKCv07K4W2dnxXXSQgBqzH8LyDo92IKBDCw=
```

Detailed Instructions

The following commands may be helpful to check and refresh the network configuration.

On a Windows PC:

ipconfig: shows the current IP configuration of the PC
ipconfig/release: deletes the current configuration
ipconfig/renew: renews the DHCP lease
arp -a: displays all IP-to-MAC address mappings for current connections

On a Linux System:

ifconfig: shows the current network configuration of connected interfaces
ip addr show: shows the current IP addresses of connected interfaces with fewer flags

Connect a PC to the ETH0 port on the Robustel router. Ensuring that the PC and router on the same subnet, enter the IP address of the router into any web browser. The default router IP address is 192.168.0.1 so we navigate to http://192.168.0.1

The username and password are set to admin by default.

Navigate to the Interface tab of the configuration page. Select LAN from the options which appear. Configure the router IP address and DHCP lease pool as shown below:

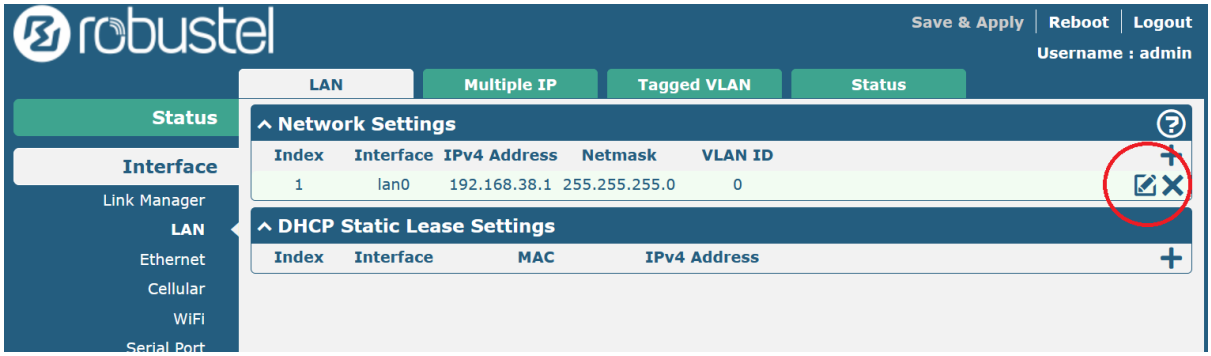

Figure 1 LAN configuration options can be accessed through the edit button in the Interface tab.

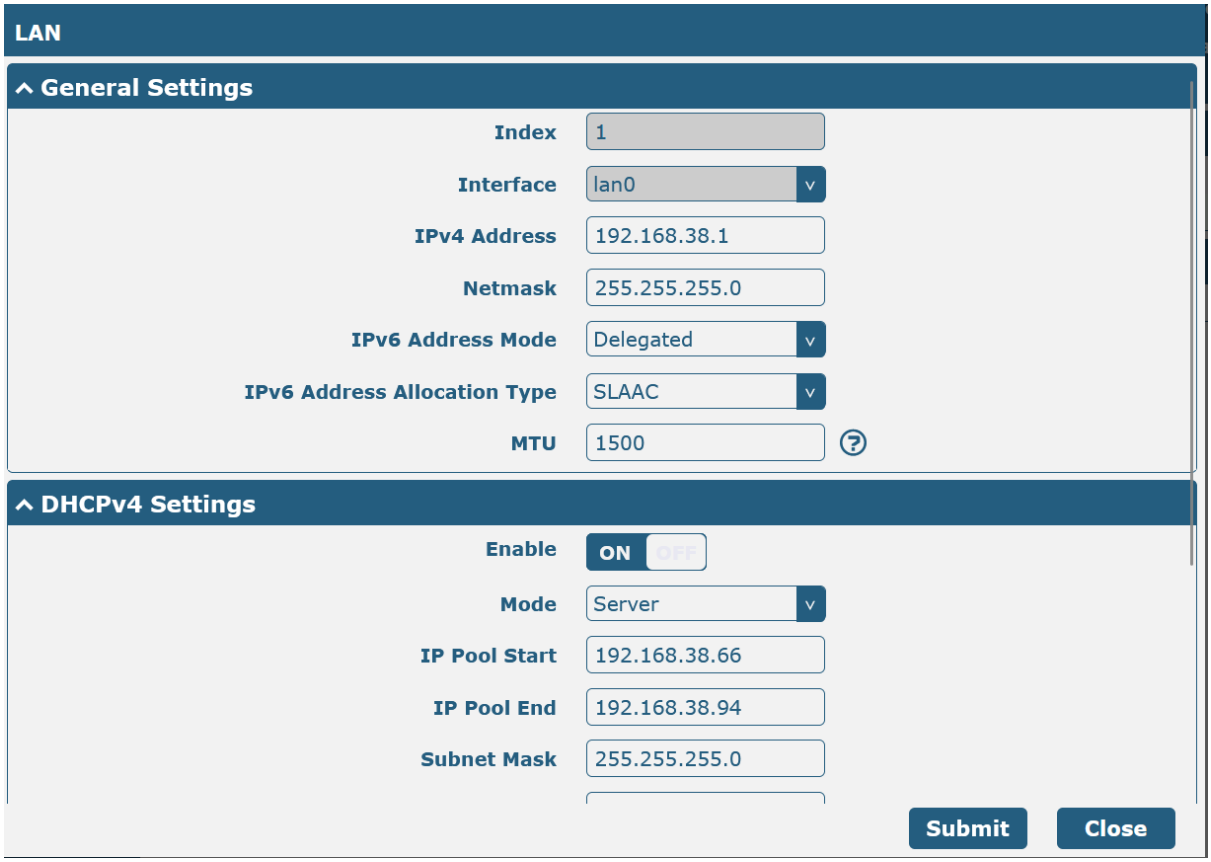

Figure 2 Example LAN configuration.

Click Submit and ensure the changes are resolved. Following this, click Save & Apply in the top right corner.

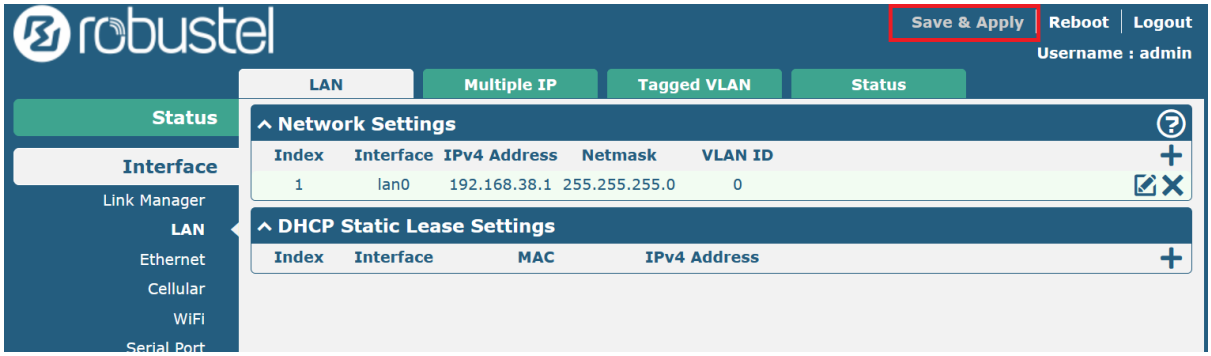

Figure 3 Changes must be saved using the Save & Apply button in the top-right of the webpage interface.

The PC will temporarily lose internet access as it must reobtain an IP via DHCP. This process should happen automatically but may require a manual refresh of the network settings. Attempt to reconnect to the router configuration webpage, this time with the new IP address http://192.168.38.1

If successful, move on to and select the VPN tab of the configuration page. Select WireGuard from the options which appear. Configure the WireGuard VPN settings as shown below. You may find it useful to copy and paste the public and private keys.

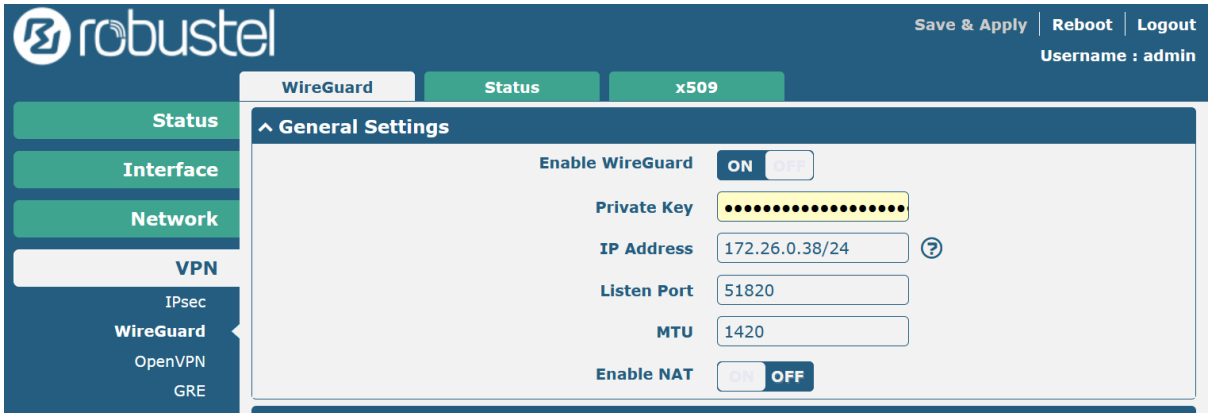

Figure 4 Example host configuration for a WireGuard VPN using london.guralp.com GDC.

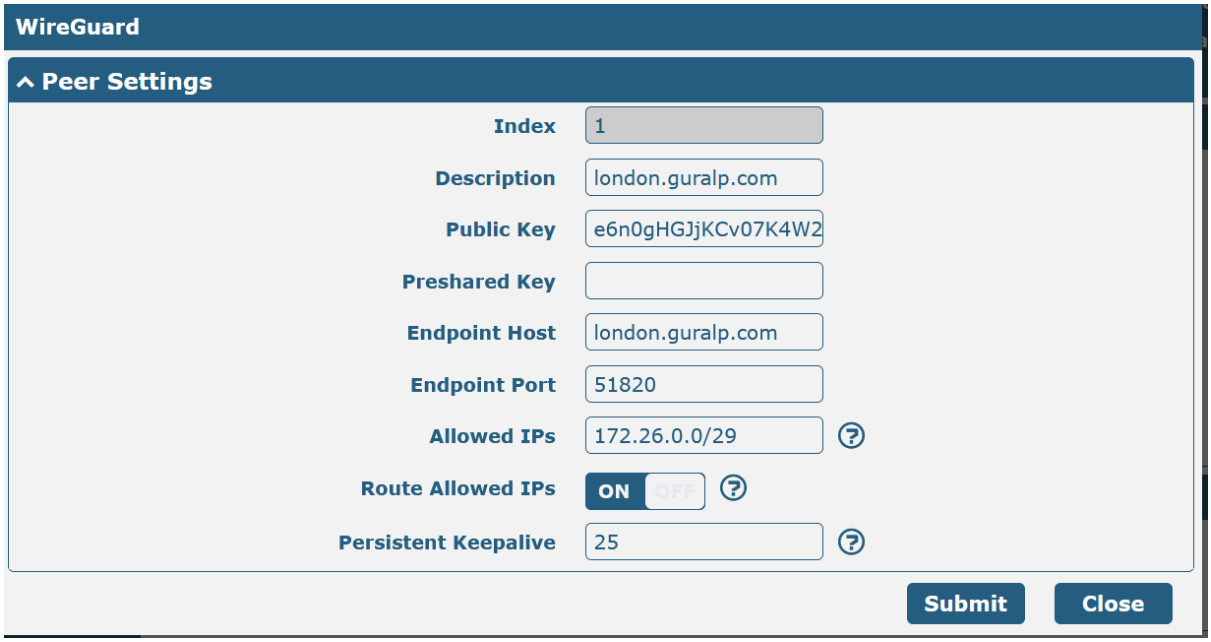

Figure 5 Example peer configuration for a WireGuard VPN using london.guralp.com GDC.

Ensure that "Enable NAT" is set to OFF. Once the configuration page has been filled out, once again click Submit, followed by Save & Apply, as before.

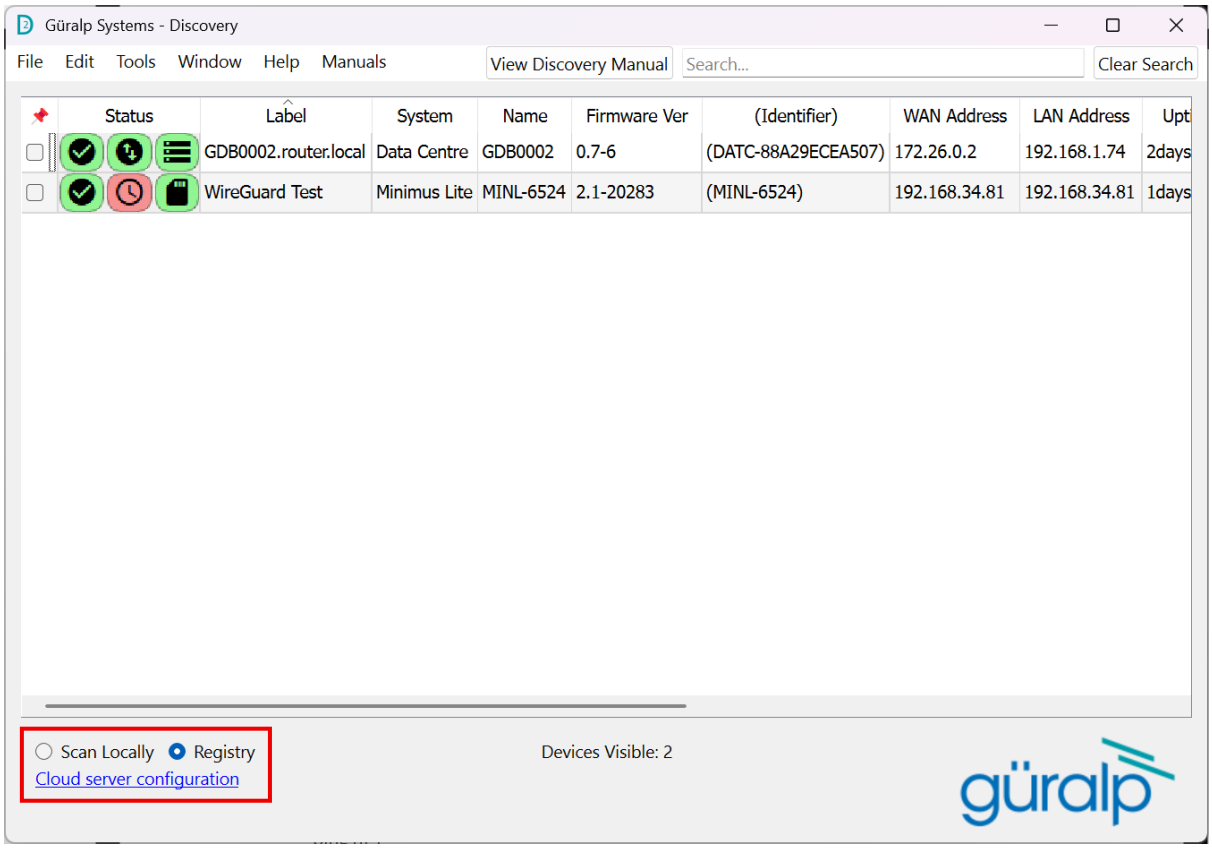

Figure 6 Discovery can switch between Scan Locally and Registry options, allowing it to display either devices on a local network or devices connected to a cloud registry endpoint.

Once the network is responsive again, you should be able to ping the endpoint address, as well as any local addresses beyond it. This can be tested by entering the following command on any platform:

ping [IP]

Where [IP] is the endpoint address, or a further local device (i.e.: a Güralp Minimus).

Güralp Discovery Software

Güralp Discovery is a standalone application dedicated to run in a desktop environment with Windows, Linux or Mac operating system. Intended as a primary interface between the user and GDB, the application provides multiple functionalities for controlling, diagnosing and monitoring Güralp Systems devices and software products. Through Discovery, the user can:

- Stream live SeedLink data from any device on the GDB network
- Download recorded data
- Quality-control between streamed and recorded data
- Configure seismic stations and digitisers
- Monitor GDB state of health

Once the GDB has been configured as a peer on the WireGuard VPN, Güralp Discovery software must be configured to use the GDB IP address as a cloud registry server. This can be done

through the “Cloud server configuration” button in the bottom left corner of the main Discovery interface.

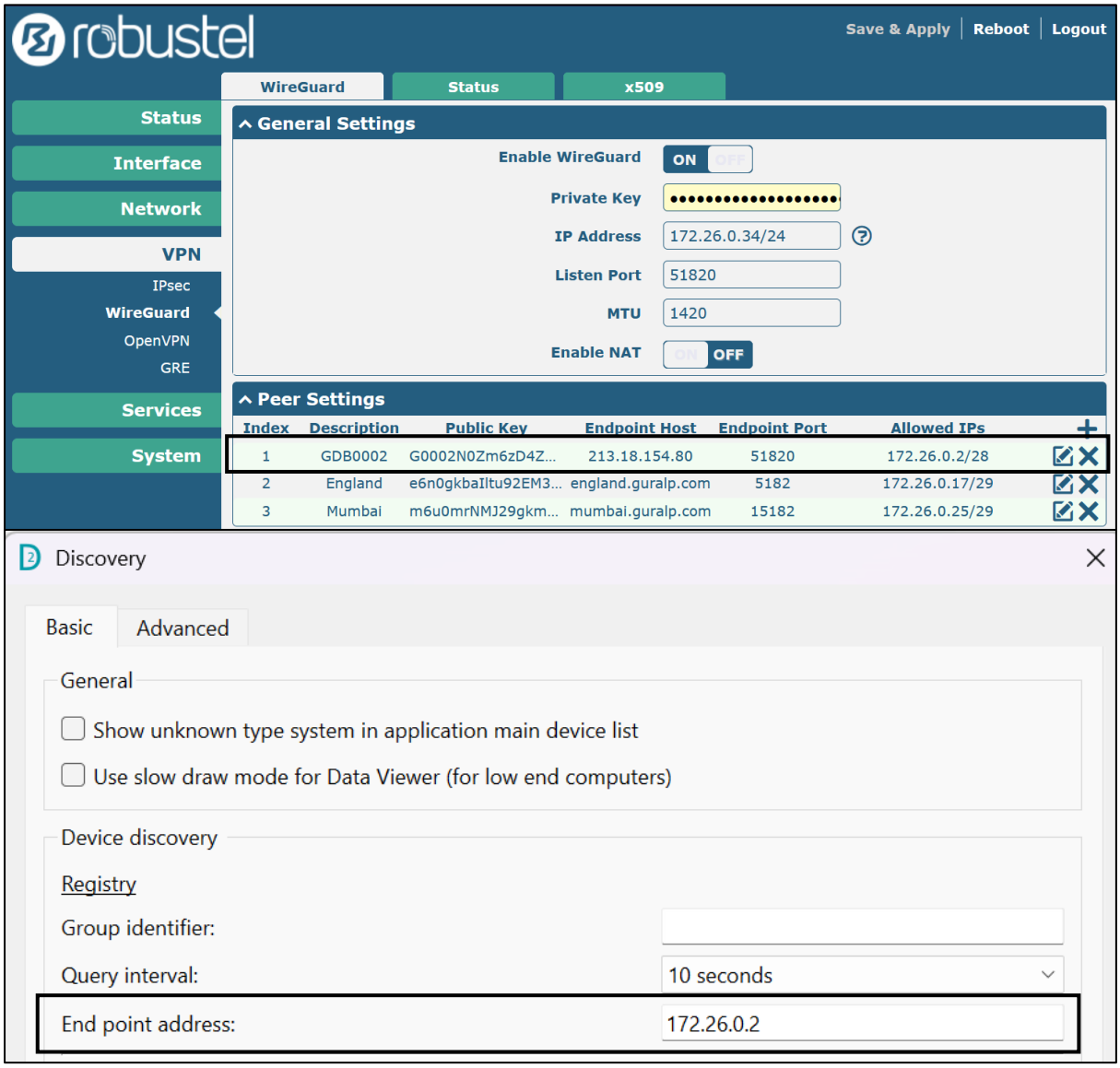

Figure 7 Güralp Data Box hosts a cloud registry server which can be configured as an endpoint in Discovery for further monitoring. Ensure that the virtual IP address of the GDB assigned by the VPN is being used.

Instructions for configuring a registry endpoint can be found in the “Guralp Discovery application” section of the GDB manual, found at:

https://london.guralp.com/documents/MAN-GDC-0001.pdf

IMPORTANT NOTE: in the case where a GDB is configured to communicate via a VPN, the virtual address of the data centre must be used rather than its standard public IP. Please see the images below for the example where private IPv4 address 172.26.0.2 has been assigned by the Robustel R1511 router to the GDB.

Configuring Remote Router Access

With a VPN enabled, the Robustel router can optionally be configured to allow remote access via SSH, Telnet or HTTP/HTTPS. These settings can be found under the Network tab, under Firewall->Filtering. Simply enable/disable access as desired by the user.

Figure 8 The router can optionally be configured to allow remote access via SSH, Telnet or HTTP/HTTPS.

Further WireGuard VPN Configuration

Configuring Primary and Backup Connection

The Robustel R1511 router can be configured with Link Manager – a network link backup function. In this example, the router is configured with a wired WAN DHCP broadband connection, with a cellular 4G SIM wireless WAN connection.

When the Primary Link in unavailable due to signal loss or other system fault, the Link Manager will switch to use the Backup Link. The backup link can be configured to run in Cold or Warm Backup mode. There is also a function for Load Balancing over both the Primary and Secondary links.

- Cold Backup: The inactive link is offline on standby.
- Warm Backup: The inactive link is offline on standby.
- Load Balancing: Use two links simultaneously. (Not available for dual SIM configurations).

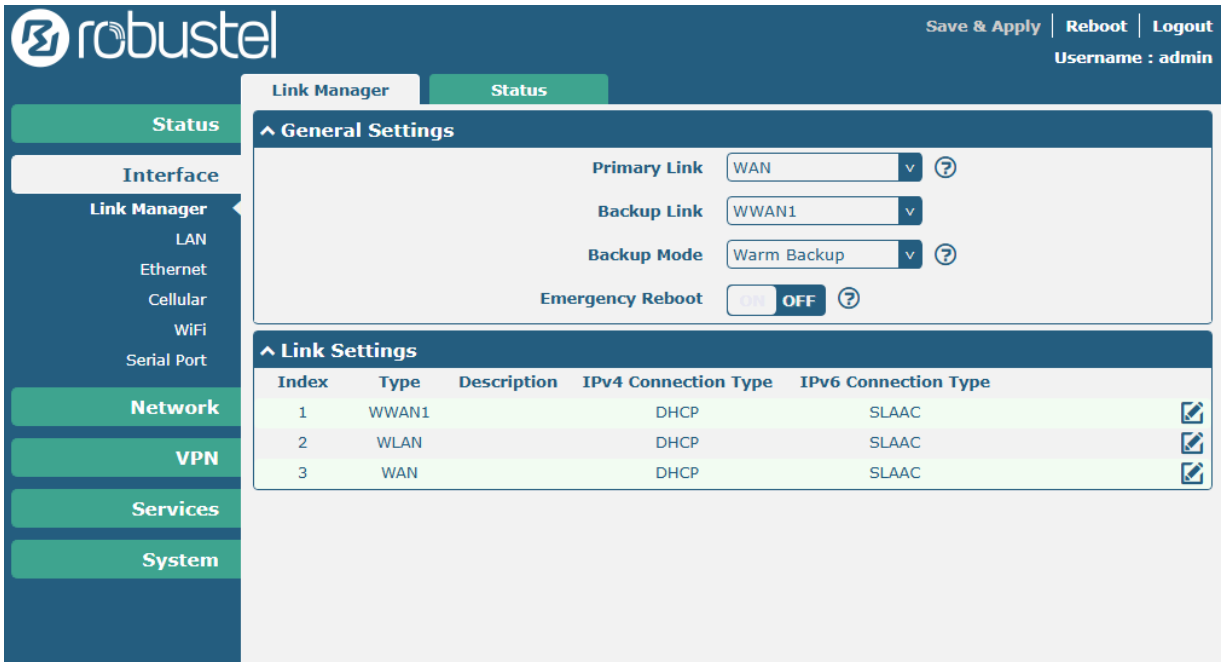

Figure 9 Link Manager configuration page with Primary Link configured as wired WAN and Backup Link configured as 4G wireless WAN (WWAN) running in Warm Backup mode.

Individual parameters may be further configured using the edit buttons next to each of the links in the table at the bottom of the page. Once finished, again click Save & Apply to save the configuration.

NOTE: For a wired ethernet WAN connection, the user must enable the ETH0 port as a WAN gateway. By default, ETH0 and ETH1 act as a local bridge. To do this, navigate to the Interface tab. From the options that appear, select Ethernet. Finally, enter the configuration page for the port named “eth0”. Change lan0 to wan, submit, then Save & Apply.

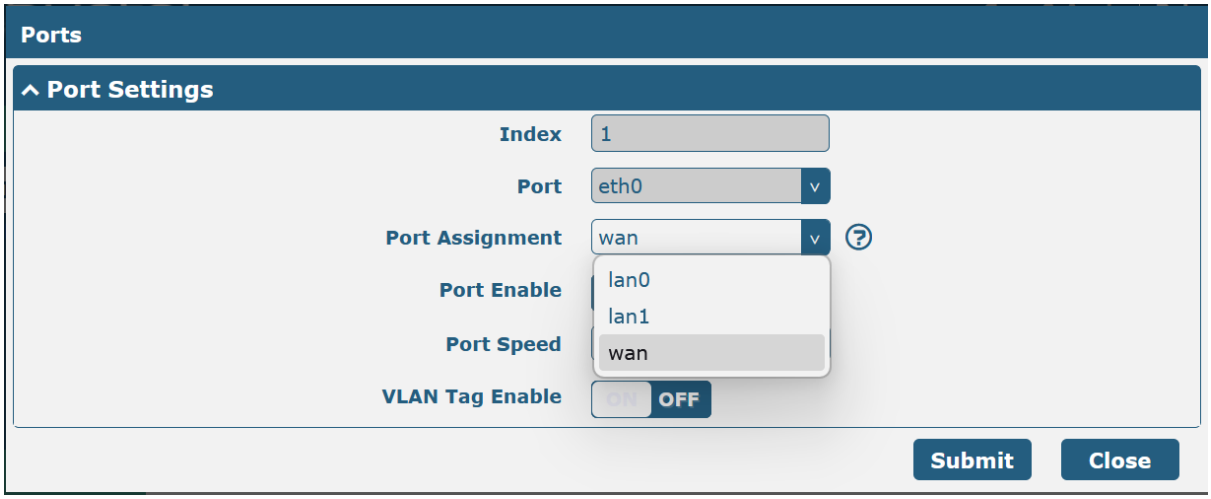

Figure 10 To enable wired ethernet WAN connection, the ETH0 port on the router must be configured as a WAN gateway.

Configuring WireGuard VPN Client on Windows

To enable access to the WireGuard network on a Windows PC, download the WireGuard installer executable from:

https://www.wireguard.com/install/

Once downloaded, you will see a blank interface with options to import tunnel configuration from a file, or to manually add a connection.

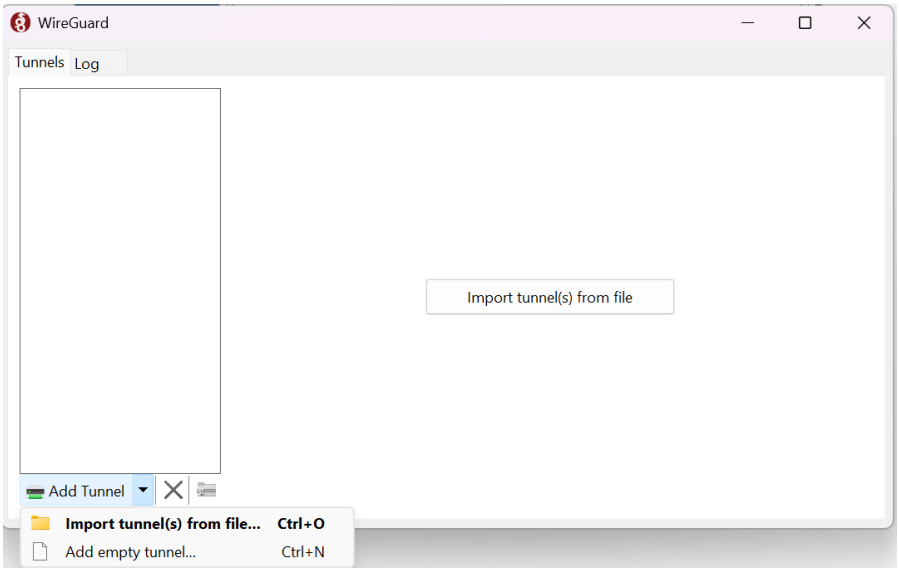

Figure 11 WireGuard client allows you to import configuration from file or to add manually

Select “Add empty tunnel” and configure the editor with your generated WireGuard keypair, allowed IP addresses and endpoint.

The configuration will vary depending on the user network and will typically be provided by the Data Centre administrator.

Generating WireGuard Keys on the GDB

To enable WireGuard Communication between the GDB and a computer on the network, all peers as well as the host must be configured with a private/public keypair. Keys are automatically generated when configuring a Windows client using the application, however, on a Linux system such as the GDB, keypairs must be manually generated.

Instructions for generating WireGuard keypairs on Linux systems can be found on the WireGuard website at:

https://www.wireguard.com/quickstart/#key-generation

Monitoring Connection Status

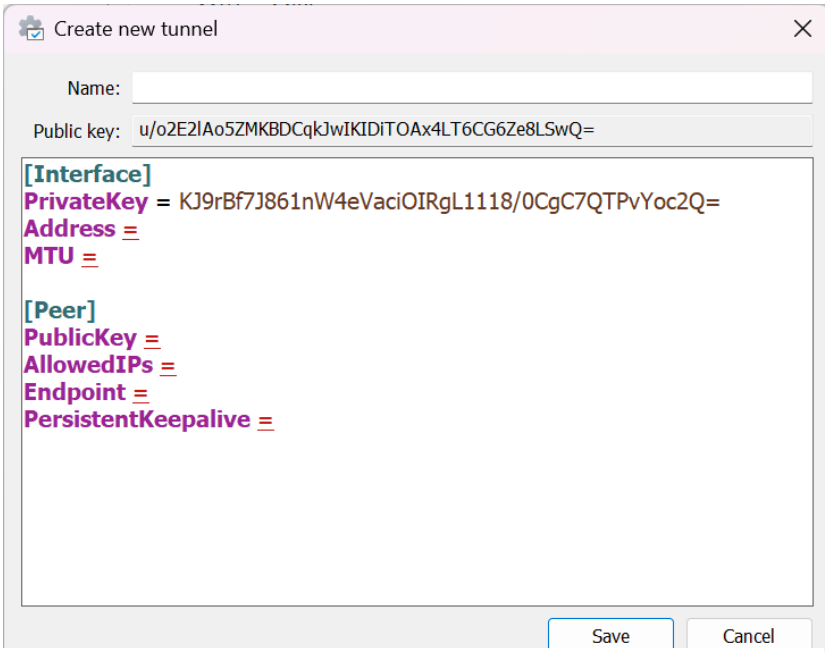

Figure 12 WireGuard tunnel configuration is dependent on your network configuration

The status of the Primary and Backup links can be monitored using a variety of methods. The first and simplest option is to view the main Status tab of the router webpage. This page will tell the user basic information including uptime, Active IPv4/6 Link type, the IP Address and Gateway address.

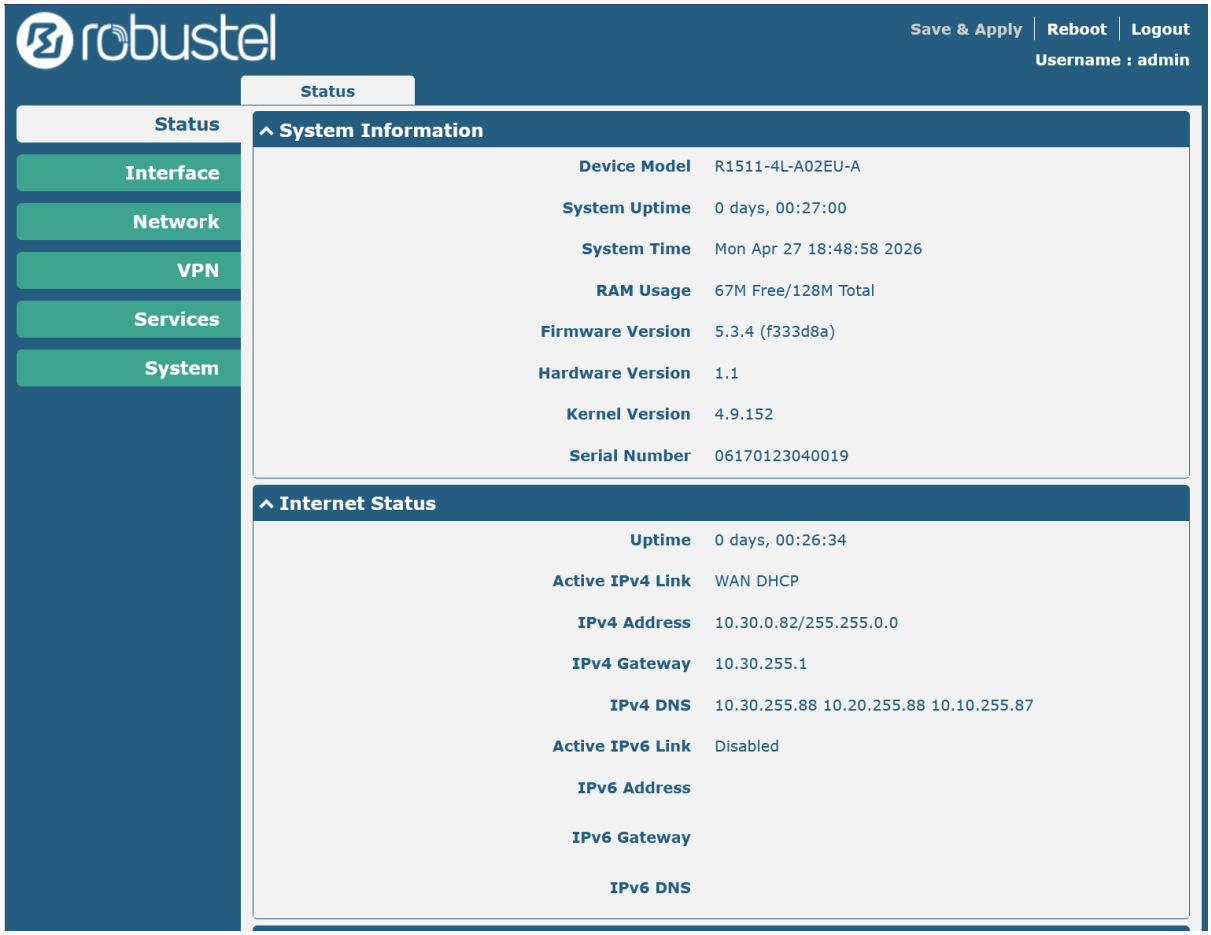

Figure 13 Status tab of the router configuration webpage displays basic information regarding internet connectivity status.

For further information, the individual connection statuses can be monitored under the Interface tab. Select the connection type relevant to the user. In our example, we are interested in Ethernet (Primary) and Cellular (Backup).

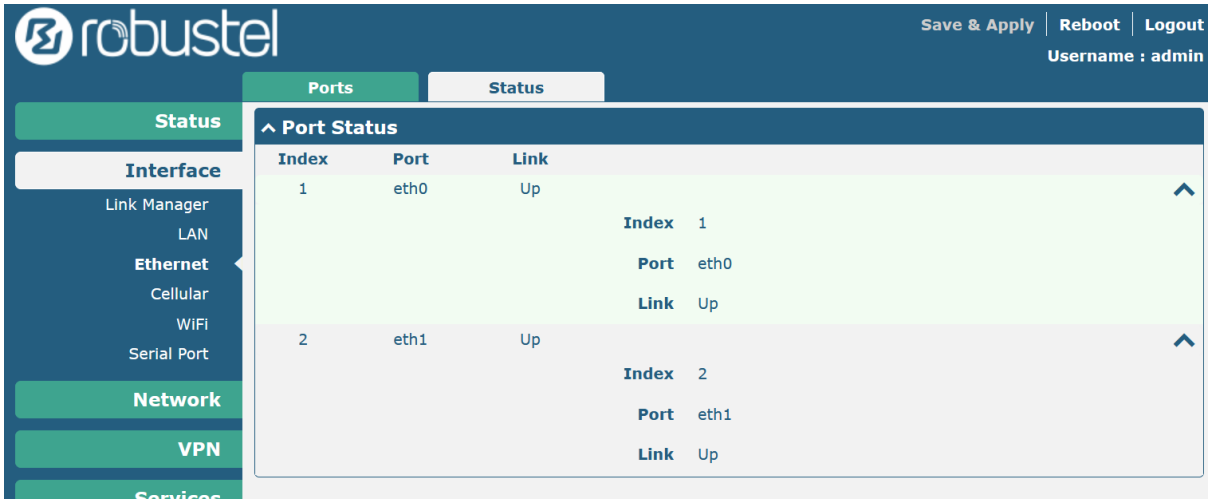

Figure 14 Ethernet connection status tab.

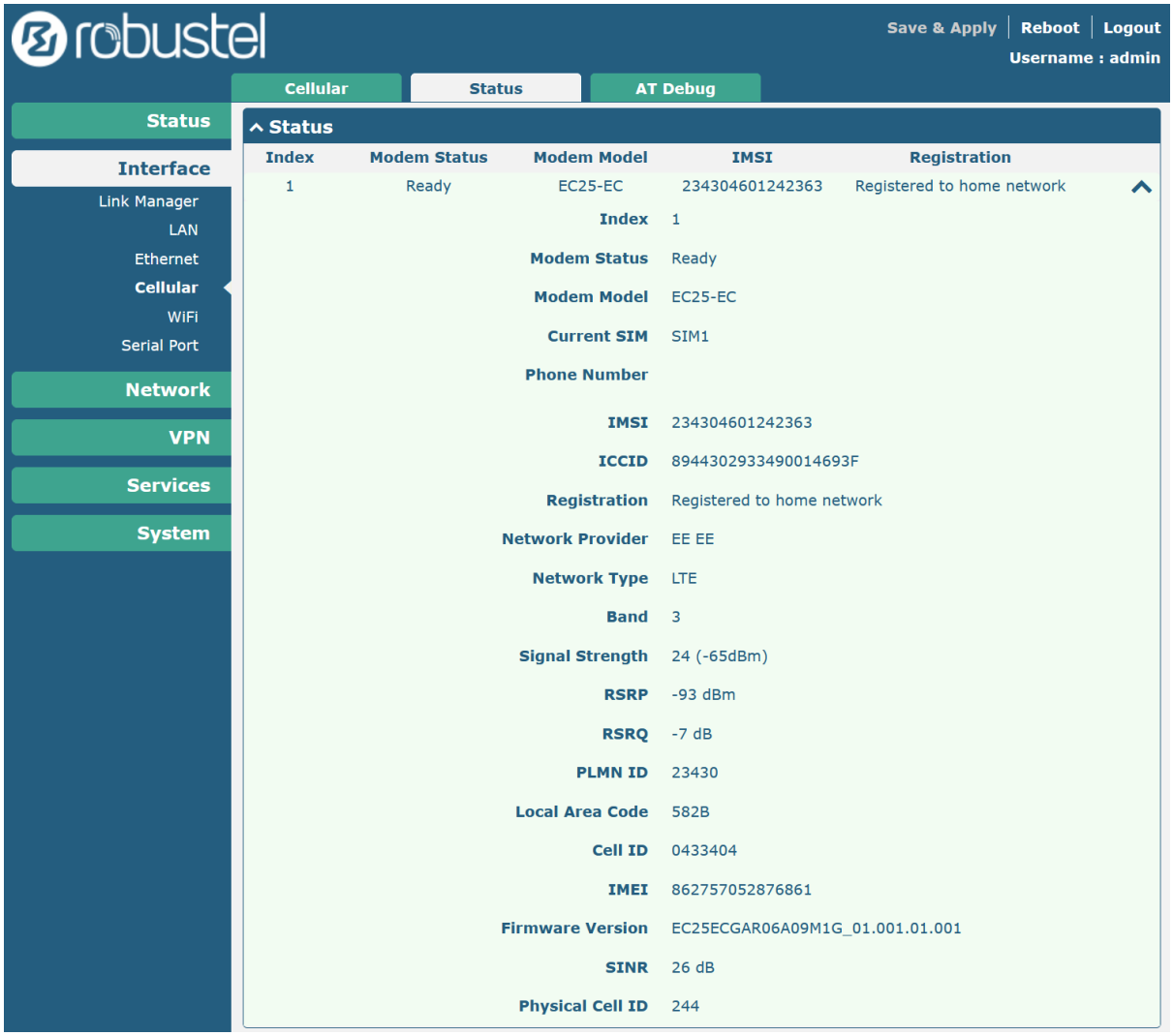

Figure 15 Cellular data connection status tab.

Finally, the R1511 router contains a system log which can be monitored for debugging and/or diagnostic purposes. For example, the Syslog provides information regarding Primary Link outage, connection to the Backup Link, and then re-connecting to the Primary Link when internet connection is restored. To reproduce these results, configure the router with a Primary ethernet WAN connection and Backup 4G cellular connection. Ensure the Backup Link is running in Warm Backup mode for minimal downtime. Once configured, navigate to the Syslog and in the Filtering field, type “link_manager”.

The log will now only display messages relating to the Link Manager function, which includes handling of Primary and Backup connections. The simplest way to cause an outage on the Primary ethernet link is to unplug the ethernet cable from the WAN interface. Once this occurs, the log will display information indicating a switch from the Primary to Backup link.

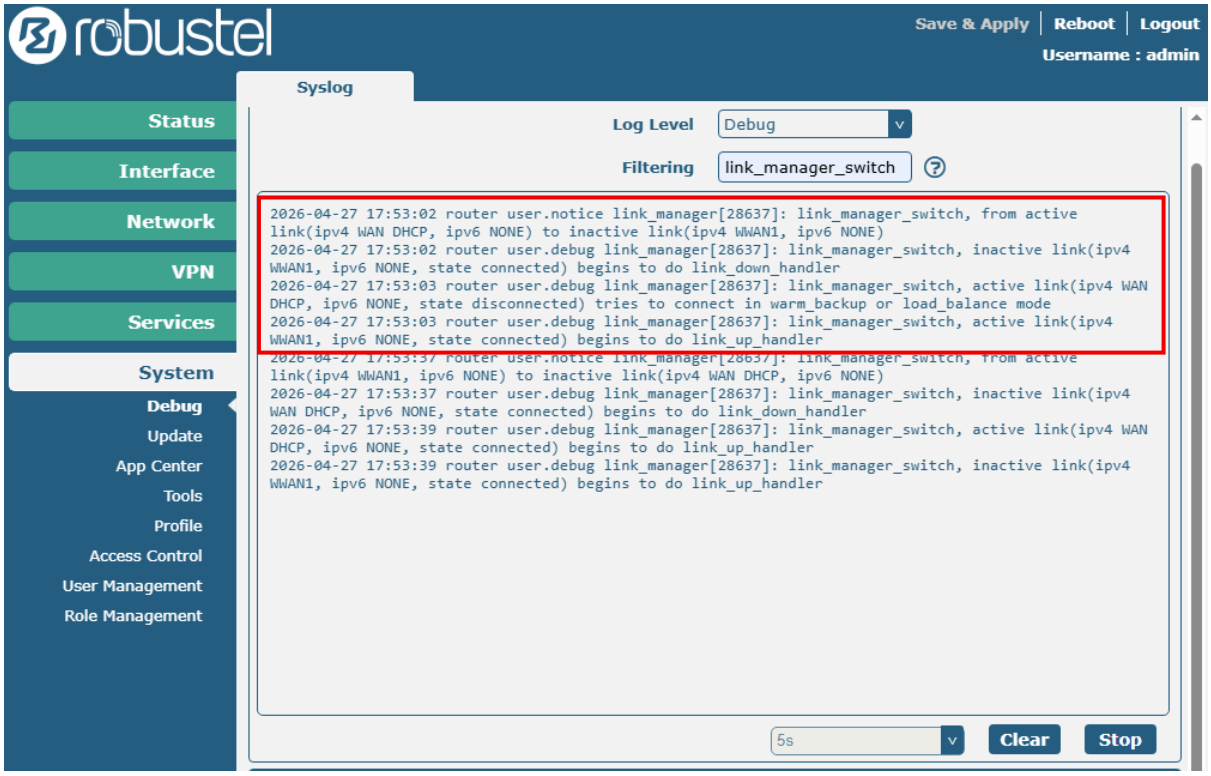

Figure 16 System log indicating a switch from the Primary (WAN DHCP) connection to the Backup (WWAN1) connection.

Once the messages are displayed, plug the ethernet connection back into the WAN interface. Similar messages will appear indicating a switch from the WWAN1 connection back to the Primary WAN DHCP connection.

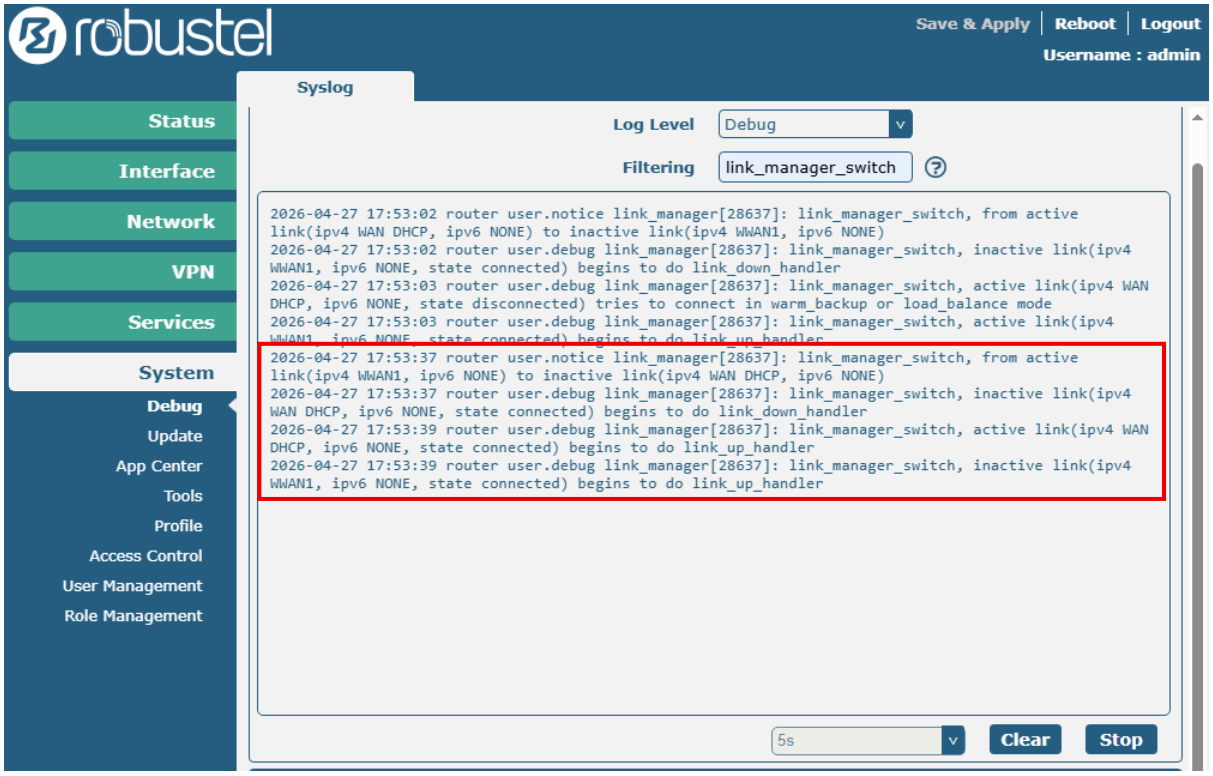

Figure 17 System log indicating a switch from the Backup (WWAN1) connection back to the Primary (WAN DHCP) connection after functionality is restored after a 34 second outage.