Using Profinet communication via 5G with u-OS (beta)

Abstract:
This document contains instructions on how to connect u-OS with 5G networks and create a VXLAN tunnel for Profinet communication. It is only for **experimentation purpose** in non-critical and non-harmful applications.

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	UC20-M3000	2839150000	FW: 2.0.0 or later
2	UC20-M4000	2839160000	FW: 2.0.0 or later

Software reference

No.	Software name	Article No.	Software version
1	Recent web browser	-	
2	Recent SSH client	-	

File reference

No.	Name	Description	Version
1	20240206_UC20-M3000-M4000-FW-2.1.1-preview-kvm.swu	u-OS 2.1.1 with enabled `kvm` and `macvtab` driver in the Linux kernel	u-OS 2.1.1-preview-kvm
2	u-os-app-openwrt_24.10.1.20250415191525-175541400	u-OS App **OpenWRT preview**	20250415 OpenWrt 24.10.1
3	SBOM_openwrt-24.10.1-a768c98	ZIP archive with software bill-of-material (SBOM) JSON documents for the u-OS App **OpenWRT preview**	openwrt-24.10.1-a768c98
4	Test_report_openwrt-24.10.1-a768c98	ZIP archive with the unit test report for the u-OS App **OpenWRT preview**	openwrt-24.10.1-a768c98

Contact
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your local sales representative:
https://www.weidmueller.com/countries

Content

1 Warning and Disclaimer

Warning
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Introduction

With the advent of fifth generation (5G) cellular wireless technology, not only are public nationwide networks expanding, but private on-premises networks using licensed frequency spectrums are also gaining traction in industrial environments. The exclusive use of licensed spectrum and the coordinated medium access makes 5G a reliable and real-time capable alternative to the error-prone, best-effort Wi-Fi networks that operate in shared, interfering frequency bands. Dedicated 5G network equipment can even achieve cable-level reliability, enabling **Profinet** real-time closed-loop control applications wirelessly that were previously only possible with expensive, highly specialized wireless technologies.

The application note explains how to connect the Weidmüller controller UC20-M3000 and UC20-M4000 to a 5G private network and establish a tunnel for transparent Profinet communication based on Virtual eXtensible LAN (VXLAN).

VXLAN is a network virtualization technology that encapsulates ISO/OSI layer 2 Ethernet frames. Hence, the VXLAN tunnel enables transparent ISO/OSI layer 2 communication required for Profinet communication. The tunnel can be used in any 5G network or any other IP-based network infrastructure in general. Therefore, it lowers the barrier for the infrastructure.

VXLAN is a standard protocol by the IETF in RFC 7348. Also, third-party vendors like Siemens recommend VXLAN for Profinet utilization in private 5G networks. Therefore, the VXLAN tunnel interoperates with third-party network equipment, and it enables seamless multi-vendor Profinet applications. For further details on the Siemens-specific application example, lookup their article “Configuration of a VXLAN tunnel between a SCALANCE MUM85x-1 and a SCALANCE SC-600” (Article ID 109805209, V1.0, 07/2022) available at:

https://support.industry.siemens.com/cs/ww/en/view/109805209

The controller must be connected using a hardware and software component. The hardware component is a third-party 5G-USB-Dongle. The software component is the open-source u-OS App **OpenWRT preview** which have to be downloaded first at:

https://mdcop.weidmueller.com/mediadelivery/asset/900_328385

Disclaimer of warranty: The u-OS App **OpenWRT preview** is a community-maintained open-source software. There is no warranty for the App and possible resulting damages. Intended use of the application note is only for **experimentation purpose** in non-critical and non-harmful applications. The source code of the App is available at https://github.com/AlbrechtL/openwrt-docker

3 Commissioning using u-OS

The application note is limited to Weidmüller controller UC20-M3000 and UC20-M4000 only. The controllers must be commissioned using u-OS FW version 2.0.0 or later.

Before you start the commissioning work, the following requirements must be fulfilled:
- The controller must be completely assembled and wired up.
- The power supply must be turned on.

If these requirements are fulfilled, the controller's PWR LED lights up green.

3.1 Starting u-OS

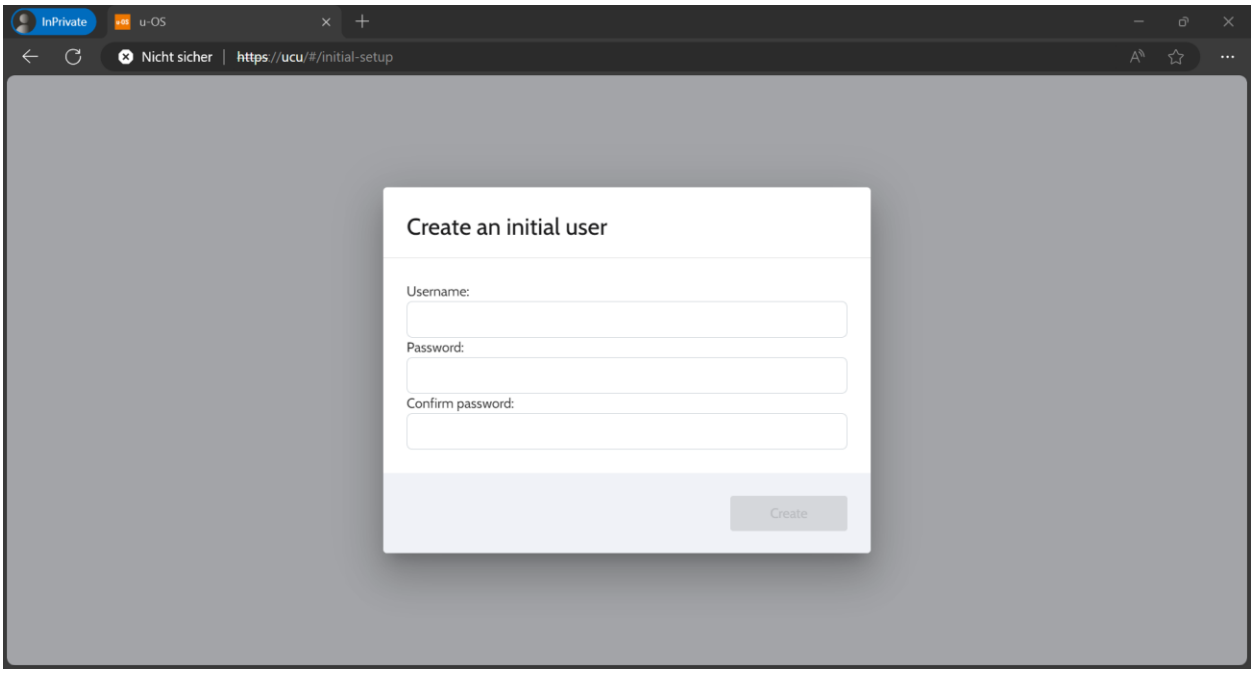
- Connect the PC to the controller using a USB cable with the USB interface X1 located under the service flap on the front.
- Open a recent web browser on the PC.
- In the address line, enter the IP address `192.168.10.202` or `ucu` in case the PC resolves hostnames with the protocol mDNS.

The browser warns you of an insecure connection when u-OS is launched for the first time.

- Click Advanced and continue the insecure connection.

u-OS is started.

The license terms are displayed when u-OS is launched for the first time.
- Read the license terms carefully.
- Confirm that you agree to the license terms and conditions.
- Click on **Accept license agreement**, to proceed to the login page.



The dialogue **Create the initial user** is opened.

- Enter a username.
- Enter a password.
- Confirm the password.
- Click **Create**.

SIGN IN is displayed.

Click **SIGN IN**.
Your login details are requested.

- Enter the initial user and the password and confirm.

3.2 Migration to Dedicated Firmware

The firmware migration enables hardware-based virtualization and networking for virtual machines which is required for the u-OS App **OpenWRT preview**. It must be completed successfully before the installation of the u-OS App **OpenWRT preview**.

- Click **u-OS Control Center** to open it.
- Click **Software & updates**.
- Click **Update & installation**.

A dialogue window opens.

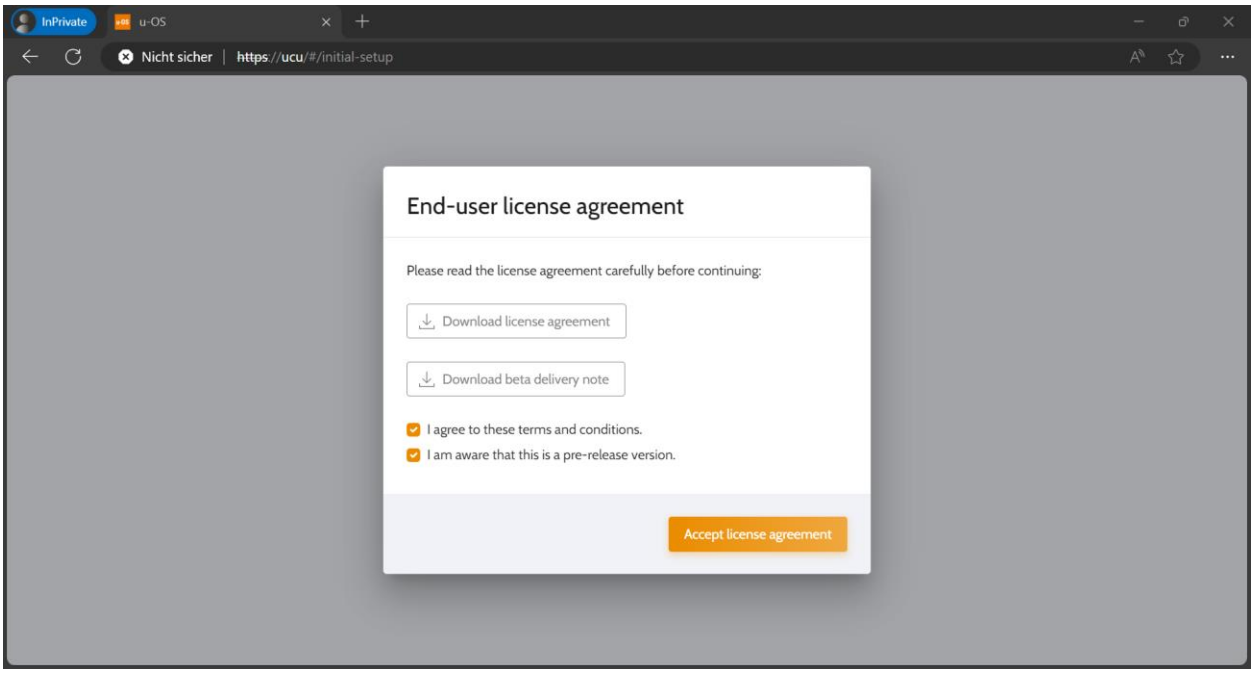
- As mentioned in Chapter 2, download and unzip the firmware from:

https://mdcop.weidmueller.com/mediadelivery/asset/900_328385

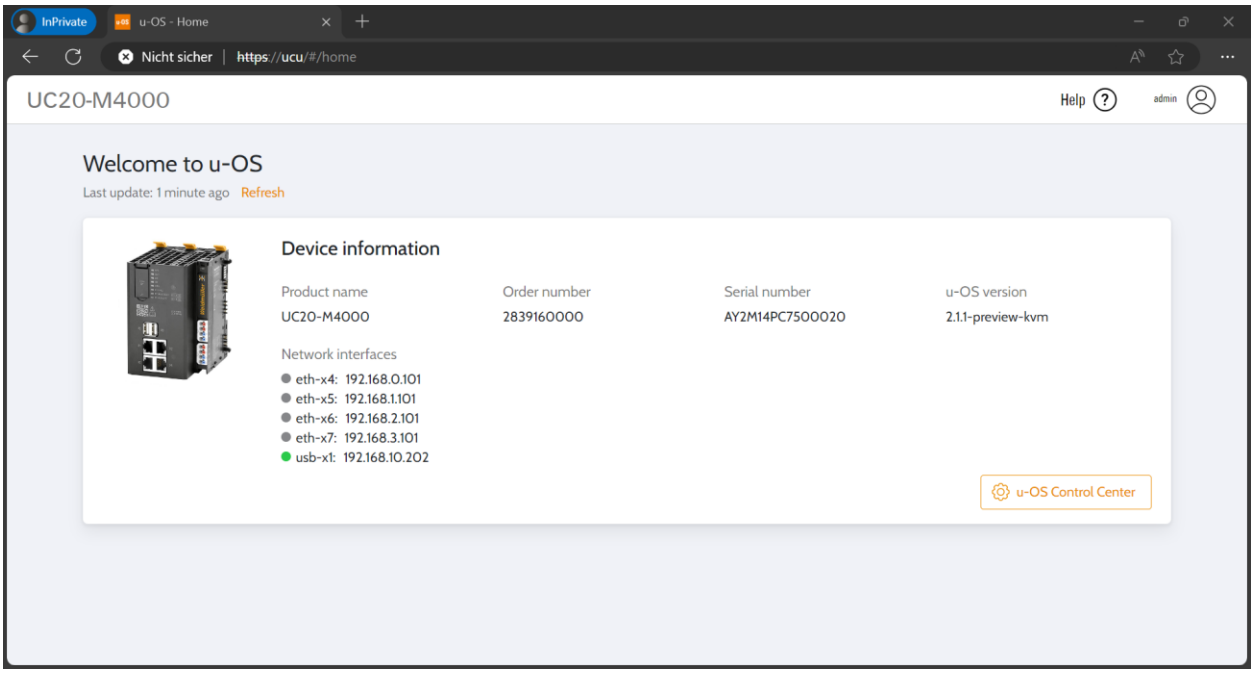
- Drag the software update file `20240206_UC20-M3000-M4000-FW-2.1.1-preview-kvm.swu` into the dialogue window.

The upload then commences. The controller is subsequently restarted.

The license terms are displayed when u-OS is launched.
- Read the license terms carefully.
- Confirm that you agree to the **license terms and conditions**.
- Confirm to be aware that this is a **pre-release version**.
- Click on **Accept license agreement**, to proceed to the login page.



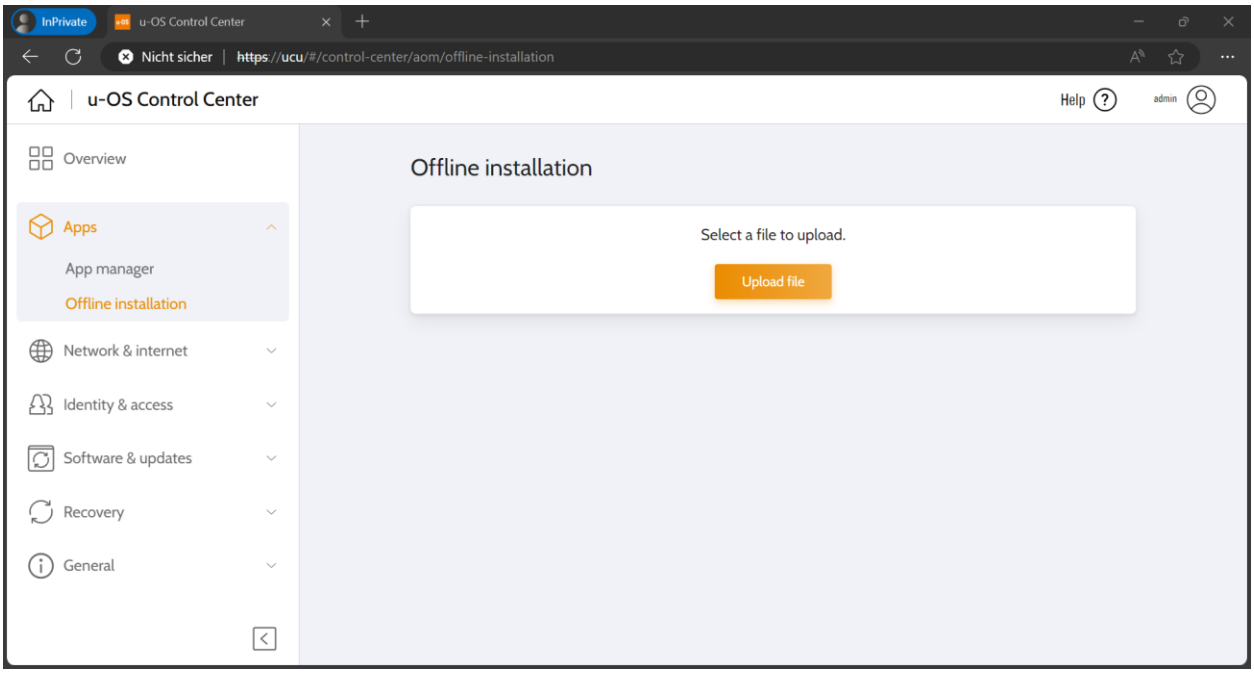
After successful login, the starting page is displayed.



3.3 Offline Installation of the u-OS App OpenWRT preview

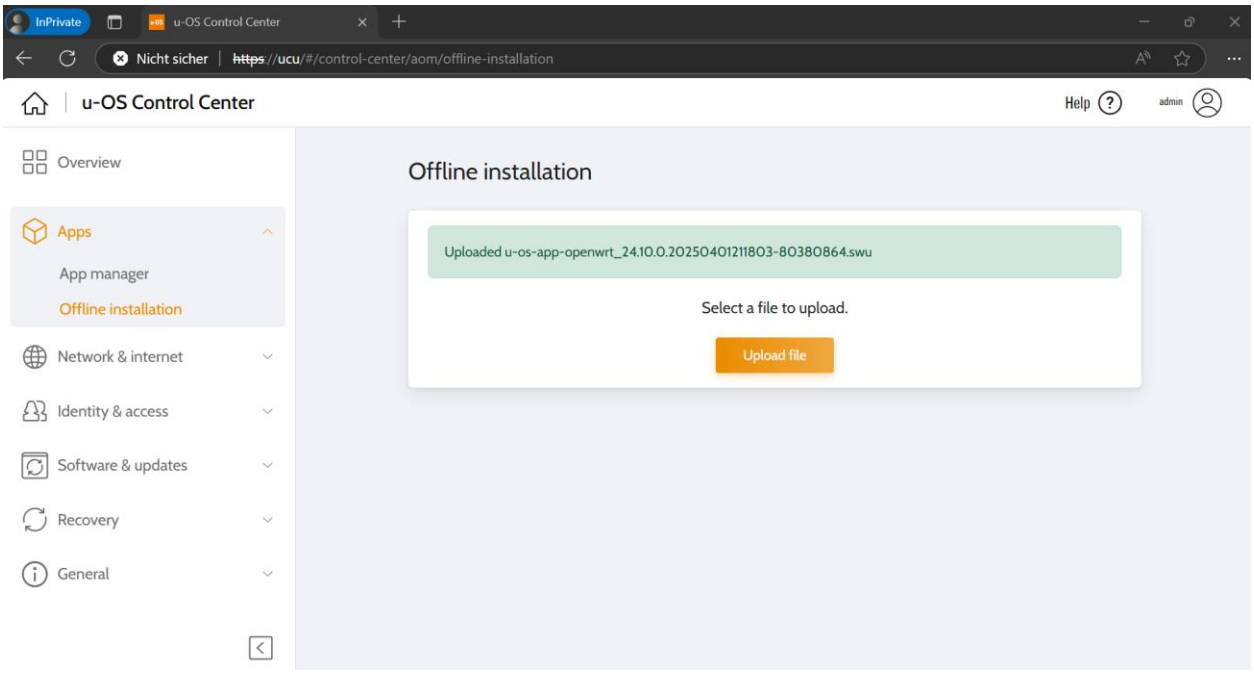
- Open the **u-OS Control Center**.
- Click **Apps** to expand the menu item.
- Click **Offline installation**.

The u-OS App **OpenWRT preview** is **not** available in the u-OS App hub and therefore cannot be installed via online installation.



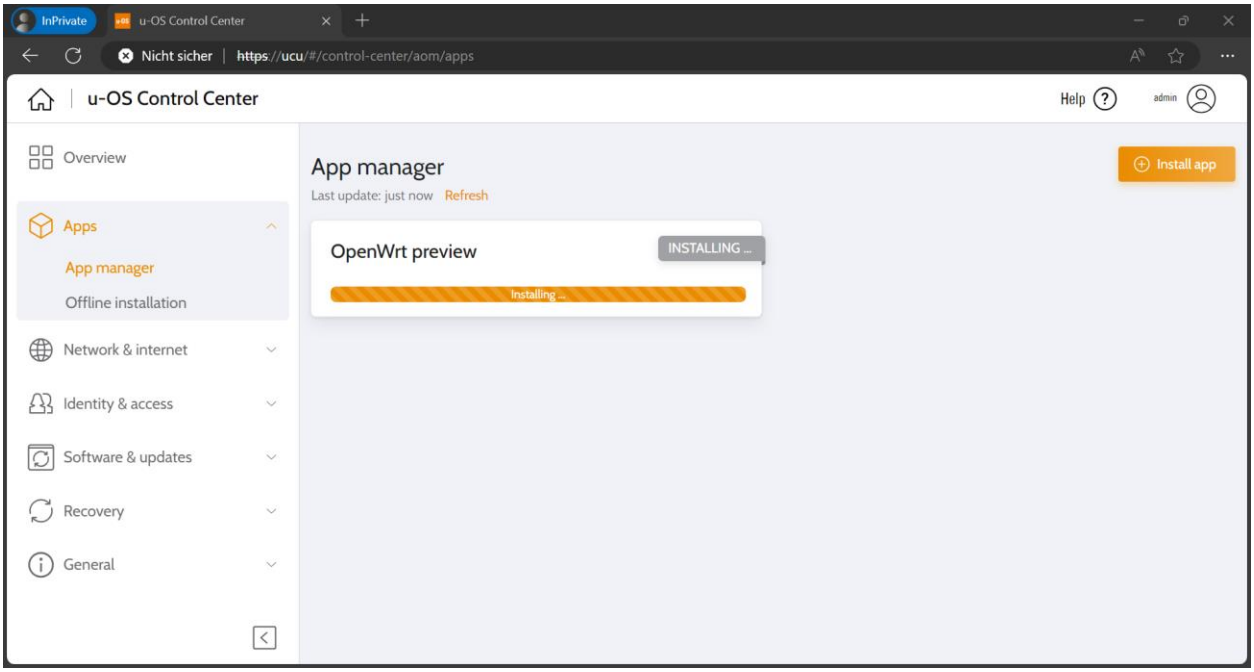
- Click Upload file.
- Select the file `u-os-app-openwrt_23.05.5.20240930200520-167538670.swu` downloaded and unzipped according Section 3.2.
- Confirm the file selection.

The upload will be started and confirmed after completion.

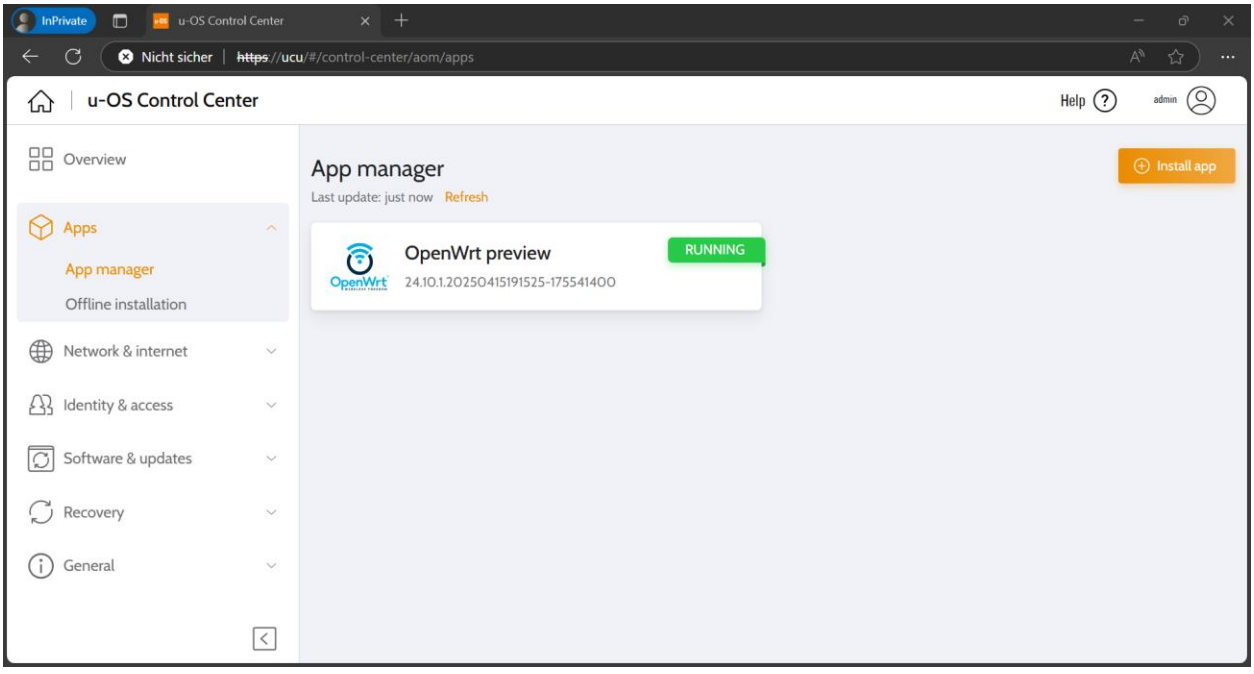


- Once the upload has finished, click **App manager**.

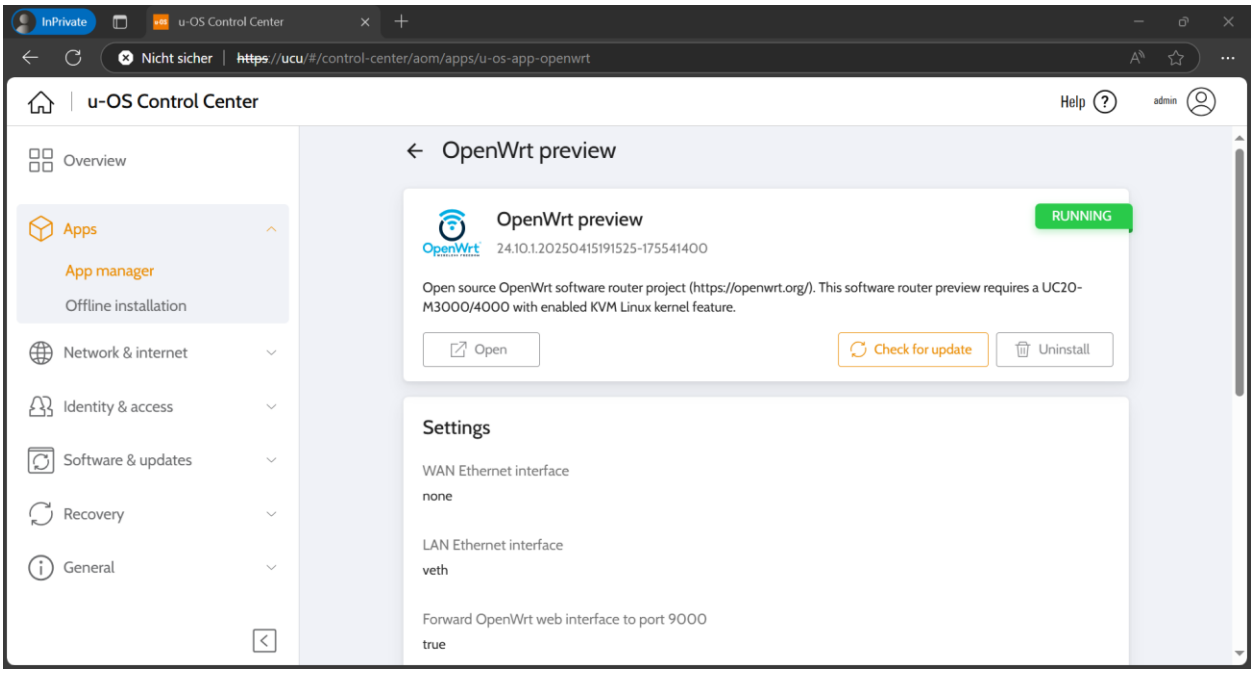
The new u-OS App **OpenWRT preview** should be listed now.



The status **INSTALLING…** indicates that the App is not installed yet. Please click **Refresh** after 5 minutes. The status should switch to **RUNNING**.



- Click **OpenWRT preview**.


InPrivate
u-OS Control Center
Nicht sicher
https://ucu/#/control-center/aom/apps/u-os-app-openwrt
u-OS Control Center
Help
admin
Overview
Apps
App manager
Offline installation
Network & internet
Identity & access
Software & updates
Recovery
General
OpenWrt preview
OpenWrt preview
24.10.1.20250415191525-175541400
RUNNING
Open source OpenWrt software router project (https://openwrt.org/). This software router preview requires a UC20-M3000/4000 with enabled KVM Linux kernel feature.
Open
Check for update
Uninstall
Settings
WAN Ethernet interface
none
LAN Ethernet interface
veth
Forward OpenWrt web interface to port 9000
true

4 Mounting and Commissioning of a 5G-USB-Dongle

Warning: Dangerous contact voltage! All work on the controller must be carried out with the power supply disconnected. Make sure that the place of installation (switch cabinet etc.) has been disconnected from the power supply!

- Select and purchase one of the listed validated 5G-USB-Dongles below.

No.	Vendor	Article	USB interface	USB VID:PID
1	Teltonika	TRM500 (Order code TRM500000000)	USB-C socket	2C7C:0801
2	Waveshare	SIM8262E-M2 5G M.2 TO ETH (SKU 26061)	USB-C socket	1E0E:9001

- Mount and wire the 5G-USB-Dongle according to the manual of the vendor including power supply and external antennas.

An additional power supply for the 5G-USB-Dongle is recommended since peripherals connected to the controller's USB interface are limited to a maximum current consumption of 500mA.

- Insert the SIM card of the 5G network according to the manual of the vendor.
- Connect the 5G-USB-Dongle USB interface to the controller USB interfaces X2 or X3 with an appropriate USB cable.

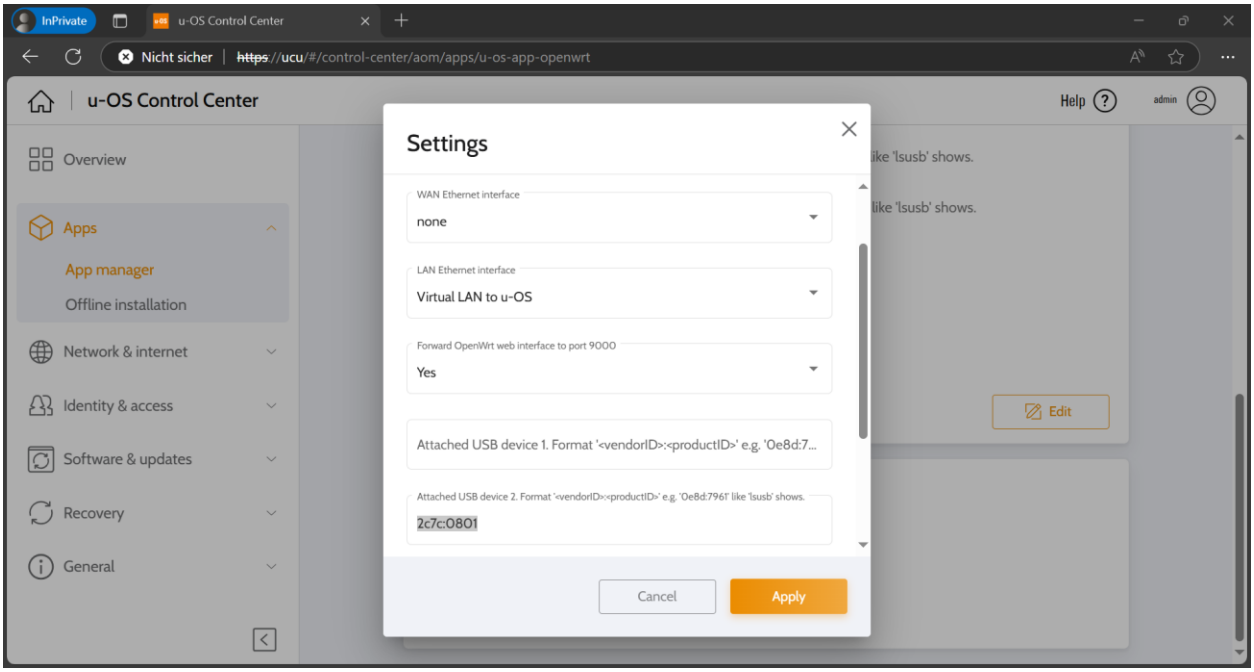
The controller USB interfaces X2 and X3 are limited to the USB 2.0 maximum data rate of 480 Mbit/s.

- Turn on the power supply of the controller and the 5G-USB-Dongle.

5 Commission OpenWRT

5.1 Setup the USB Passthrough

- After u-OS started, navigate to **OpenWRT preview** as mentioned in Section 3.3.
- Click **Edit**.



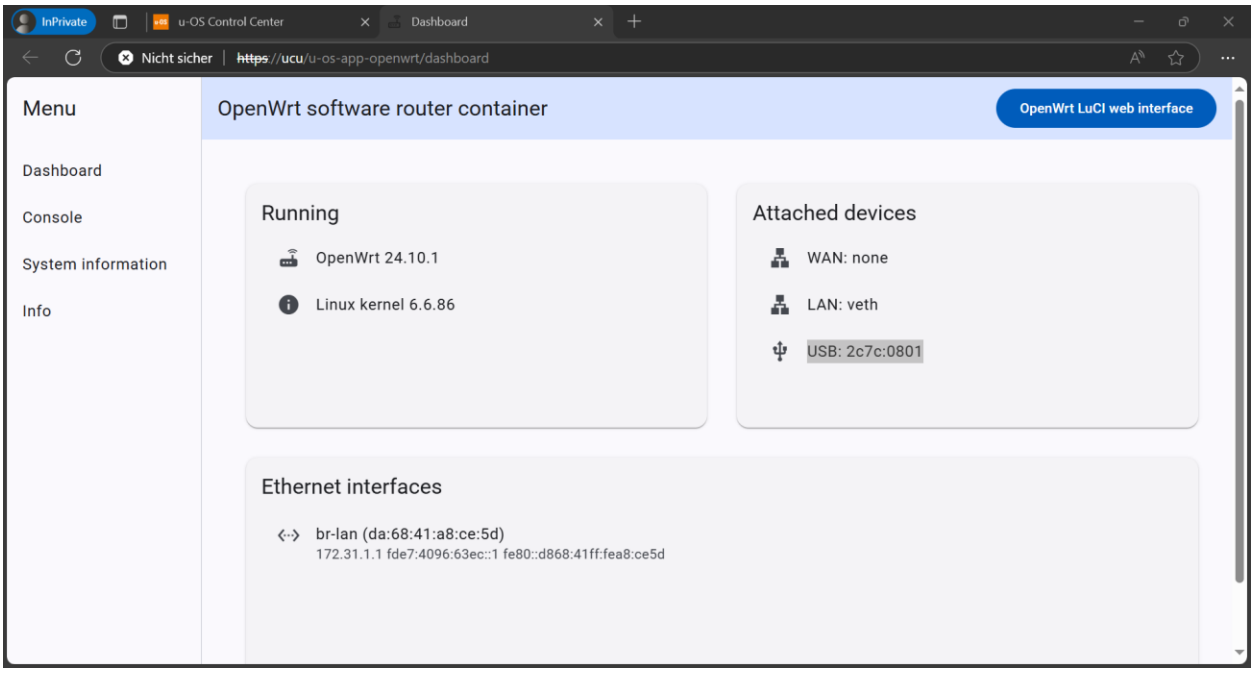
- Confirm **LAN Ethernet interface** is set to **Virtual LAN to u-OS**.
- Activate **Forward OpenWRT web interface to port 9000**.
- Set the **Attached USB device 1** to the USB Vendor ID and Product ID according to the table in Chapter 4.
- Click **Apply**.

A dialog confirms updating the App settings.

- Click **Open**.

The control interface of the u-OS App **OpenWRT preview** opens in a new browser tab.

In case u-OS successfully detects the corresponding 5G-USB-Dongle with **the USB VID and PID** as listed in Chapter 4, the device should be listed in the section **Attached devices**. In the example below, the 5G-USB-Dongle is listed with the USB VID and PID 2c7c:0801.



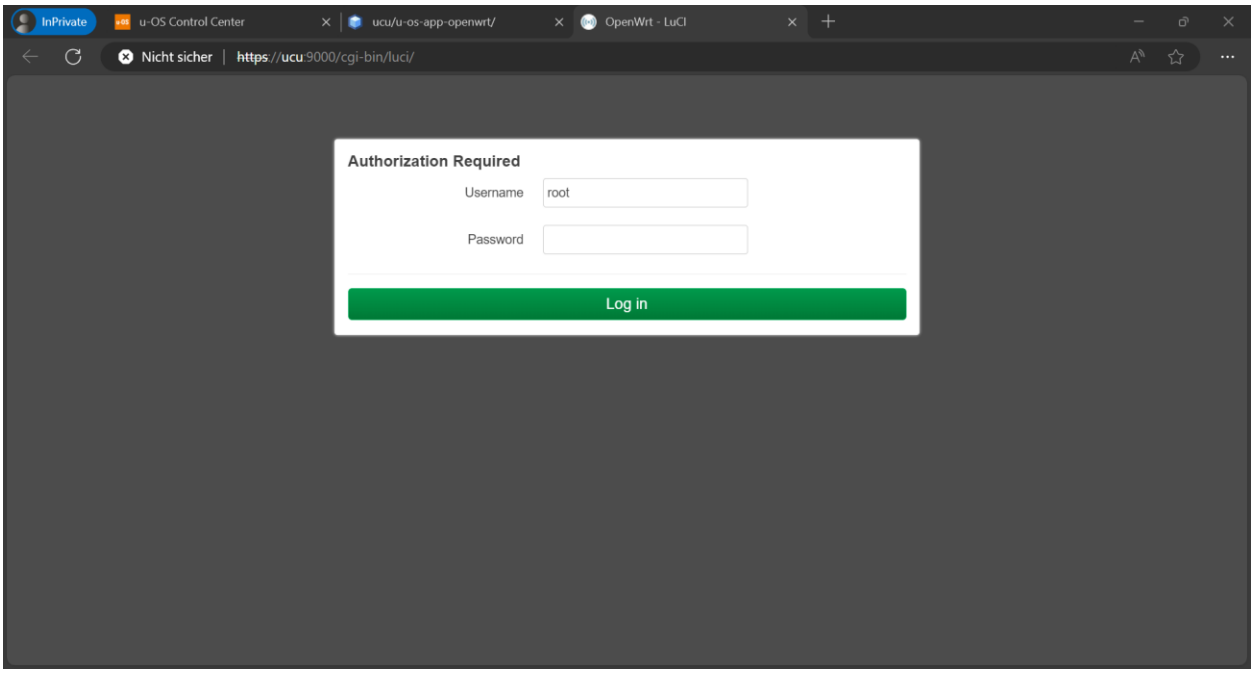
5.2 Access the OpenWRT Web Interface

▶ Click **OpenWRT LuCI web interface**.

The web interface of OpenWRT opens in a new browser tab.

The browser warns you of an insecure connection when u-OS is launched for the first time.

▶ Click **Advanced** and **continue the insecure connection**.



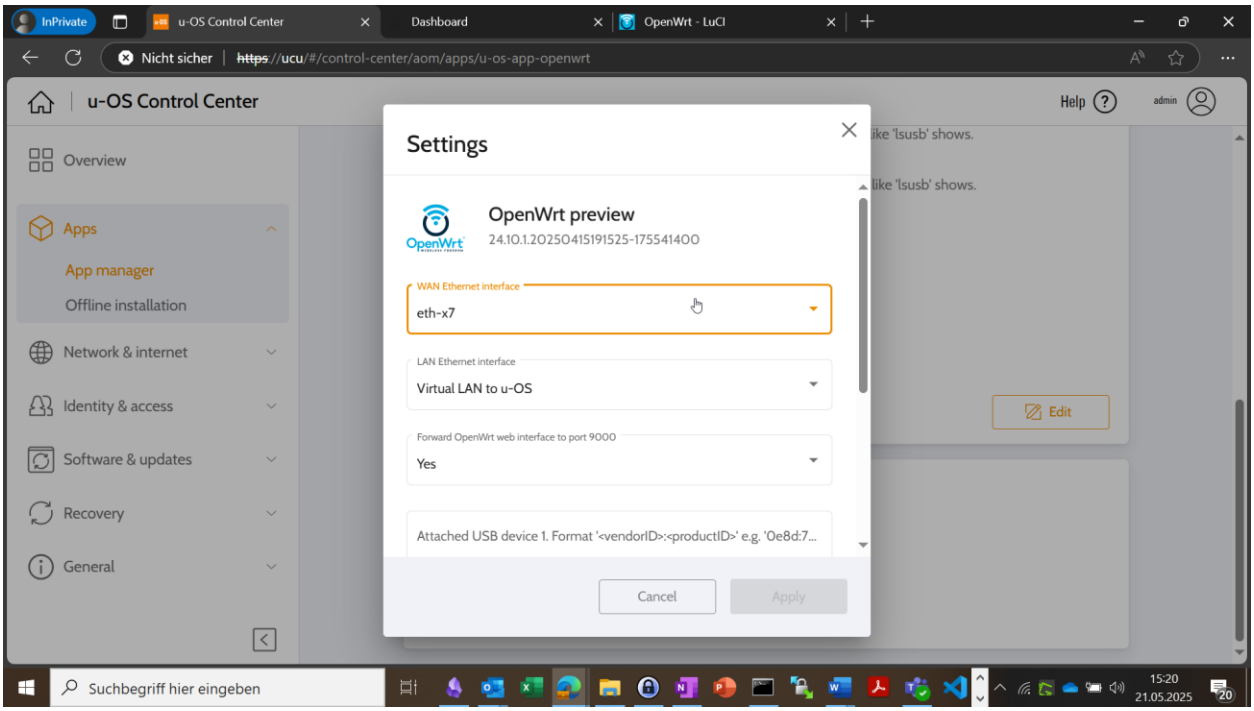
- Click **Log in** without using a password for the user **`root`**.

The OpenWRT status page is displayed.

5.3 Install additional OpenWRT Software Packages

Internet accessibility is required for OpenWRT Software Packages installation.

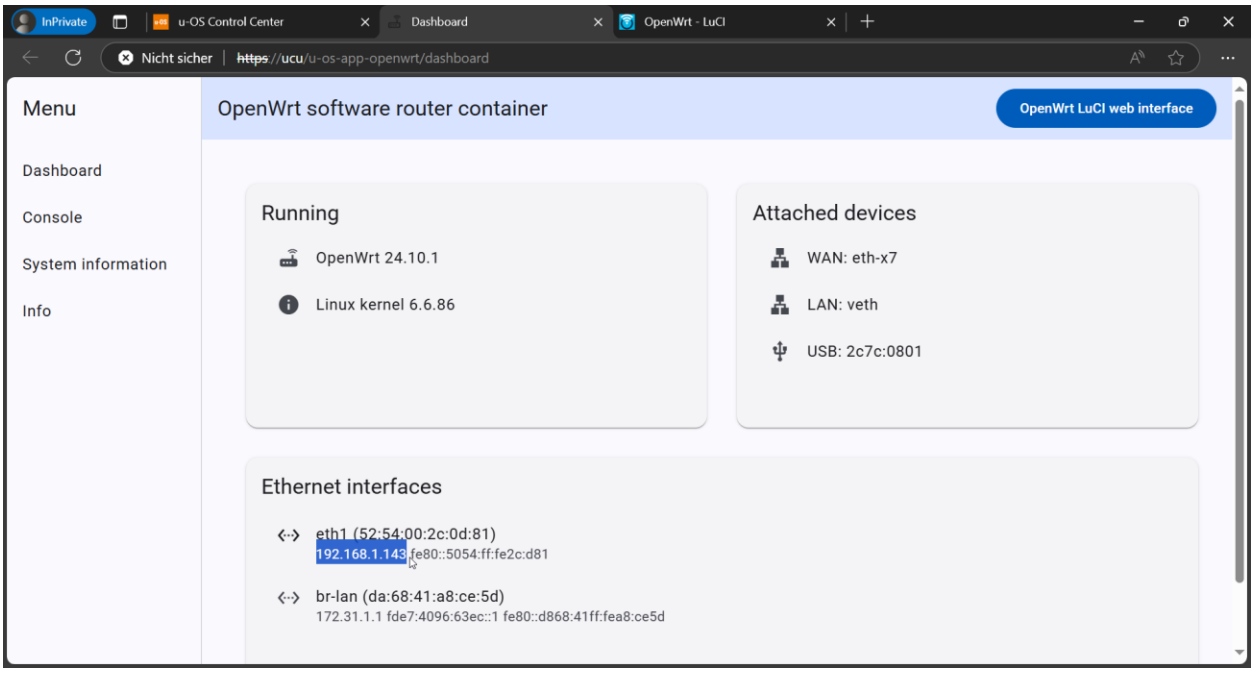
- Connect an Ethernet port of the controller e.g. **X7** to an Internet-connected Ethernet interface.
- Navigate to **OpenWRT preview** as mentioned in Section 3.3.
- Click **Edit**.
- Set **WAN Ethernet interface** to the connected Ethernet port e.g. **eth-x7**.
- Click **Apply**.



▶ Click **Open**.

The control interface of the u-OS App **OpenWRT preview** opens in a new browser tab.

In case u-OS successfully connects to the WAN interface, it mentions the connected Ethernet port e.g. **WAN: eth-x7** in the section **Attached devices**. In case IP addresses are assigned via DHCP automatically **eth1** should have an IP address e.g. **192.168.1.143** in the section **Ethernet interface**, as shown below.



In case of static IP addresses, lookup the Weidmüller application note AN0122 “Connecting u-OS to private or public 5G networks (beta)” available at: https://mdcop.weidmueller.com/mediadelivery/asset/900_324020 or the OpenWRT community documentation at https://openwrt.org/docs/start

- Click **OpenWRT LuCI web interface**.
- Click **Log in** without using a password for the user **`root`** (default).
- Click on menu item **System** and then click on the sub-item **Software**.
- Click **Update lists…**
- Upon successful download, click **Dismiss**.

Now, the list of available software packages should be filled. For the VXLAN protocol support install the following software packages.

- In the **Filter** field type **vxlan**.
- Click **Install…** next to the software package **luci-proto-vxlan** which includes the **OpenWRT LuCI Web Interface** integration including all VXLAN dependencies.
- Click **Install**.
- Upon successful download, click **Dismiss**.

For testing purposes install the utility **ARP scanner** and its database to resolve MAC addresses.

- In the **Filter** field type **arp-scan**.
- Click **Install…** next to the software package **arp-scan**
- Click **Install**.
- Upon successful download, click **Dismiss**.

- Click **Install…** next to the software package **arp-scan-database**
- Click **Install**.
- Upon successful download, click **Dismiss**.

To take effect of the additional software packages **OpenWRT** must be rebooted.

- Click on menu item **System** and then click on the sub-item **Reboot**.
- Click **Perform reboot**.

The login page should appear after a few minutes.

6 Setup VXLAN Tunnel via 5G for Profinet

The following figure illustrates the topology for the VXLAN tunnel via 5G for Profinet which will be used as example setup in the following description.

In case the 5G connectivity is not optimized for low-latency, consider Profinet RT communication according **Conformance Class A or B** with a maximum **cycle time of 64 ms** for a Profinet application with a single 5G-connected Profinet device.

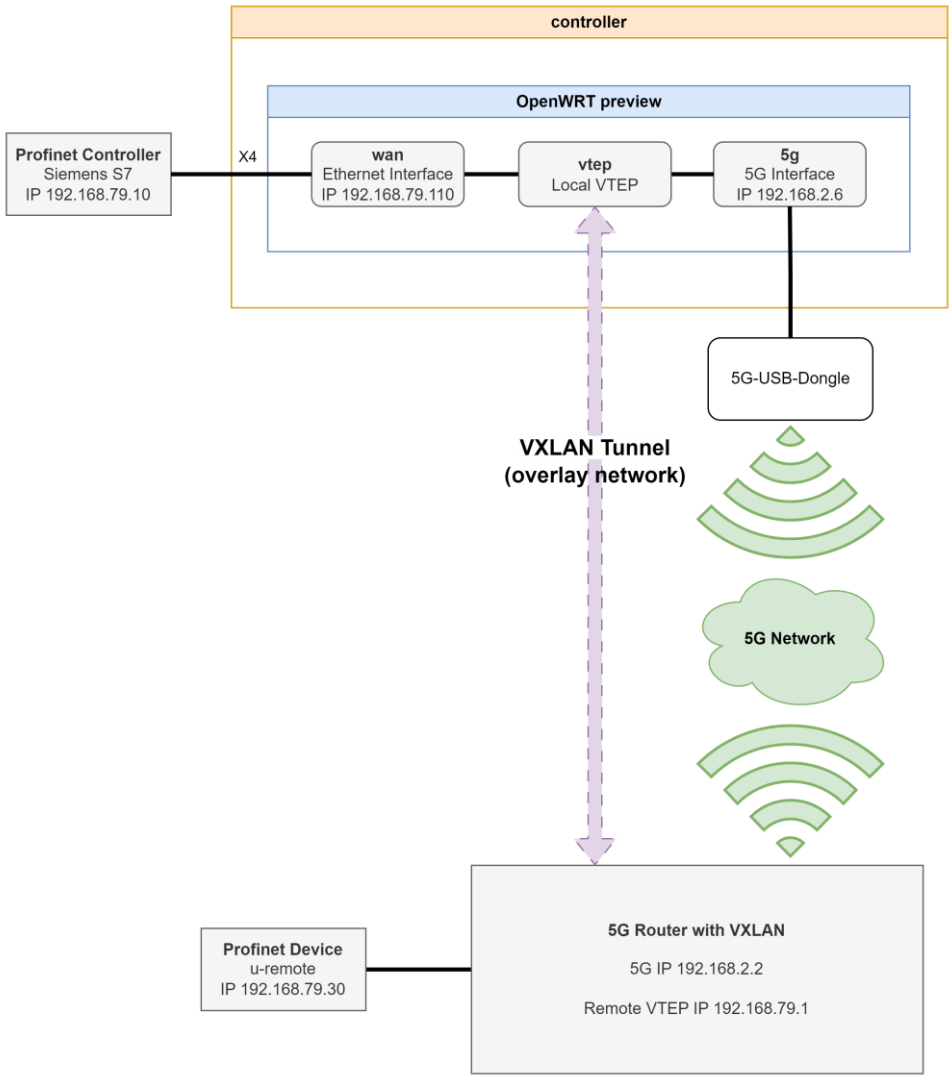


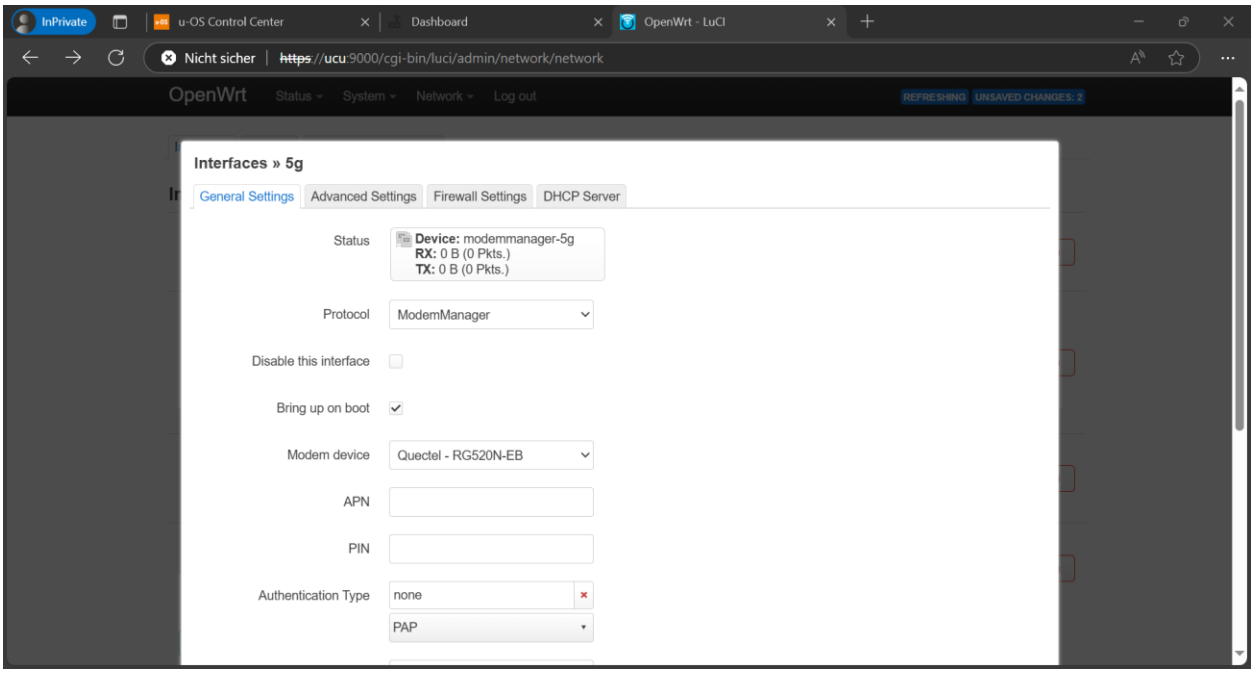
Figure 1: Example setup for the VXLAN tunnel via 5G for Profinet

VXLAN creates a virtual network, so called **overlay network**, on top of a physical network, so called underlay network. Thereby, the overlay network terminates at multiple hosts, which are called VXLAN tunnel endpoints abbreviated as **VTEPs**.

6.1 Setup the 5G Connectivity

- Access the **OpenWRT Web Interface** according to Section 5.2.
- Click on menu item **Network** and then click on the sub-item **Interfaces**.
- Click **Add new Interface…** to add the 5G network interface.
- Name the interface e.g. **5g**
- Select protocol **ModemManager**.
- Click **Create interface**.

A dialog with **ModemManager** specific parameters appears.



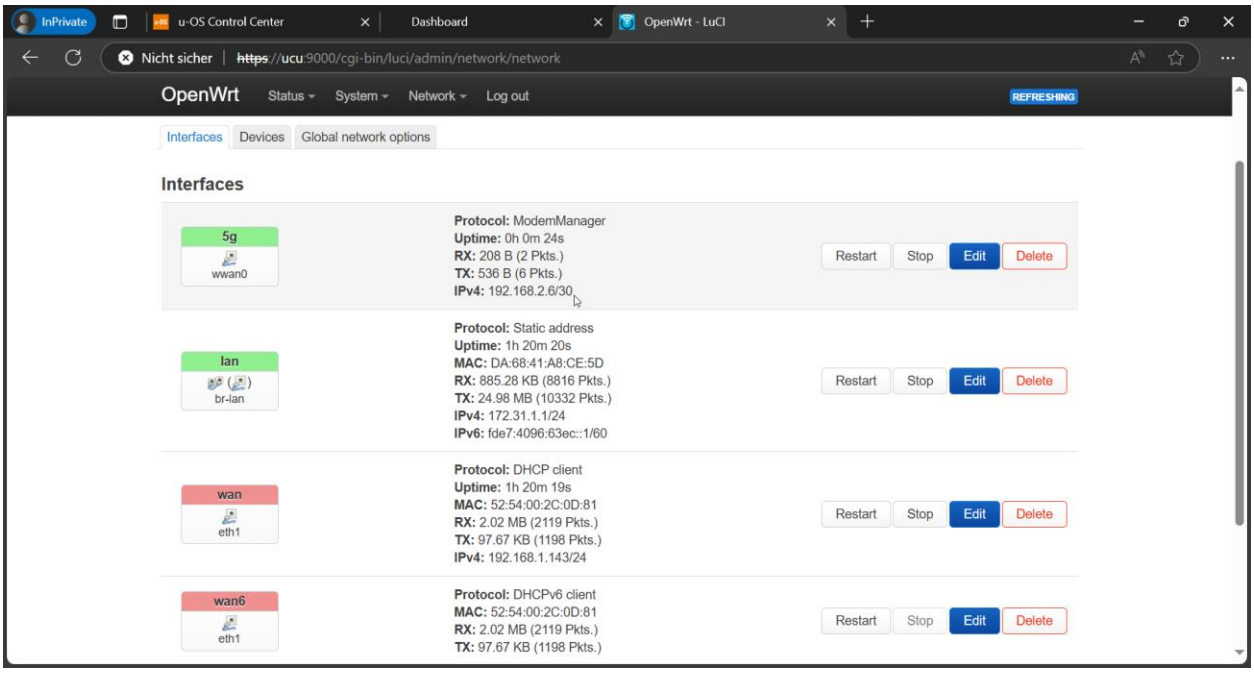
- Configure cellular parameters **provided by the 5G network provider**.

The cellular parameters depend on the **5G network setup and the provider**. They are for example the access point name (APN), the personal identification number (PIN) for the SIM card, and the authentication type and credentials.

- Navigate to **Firewall Settings**.
- Assign firewall-zone **lan** to enable incoming network traffic.
- Click **Save**.

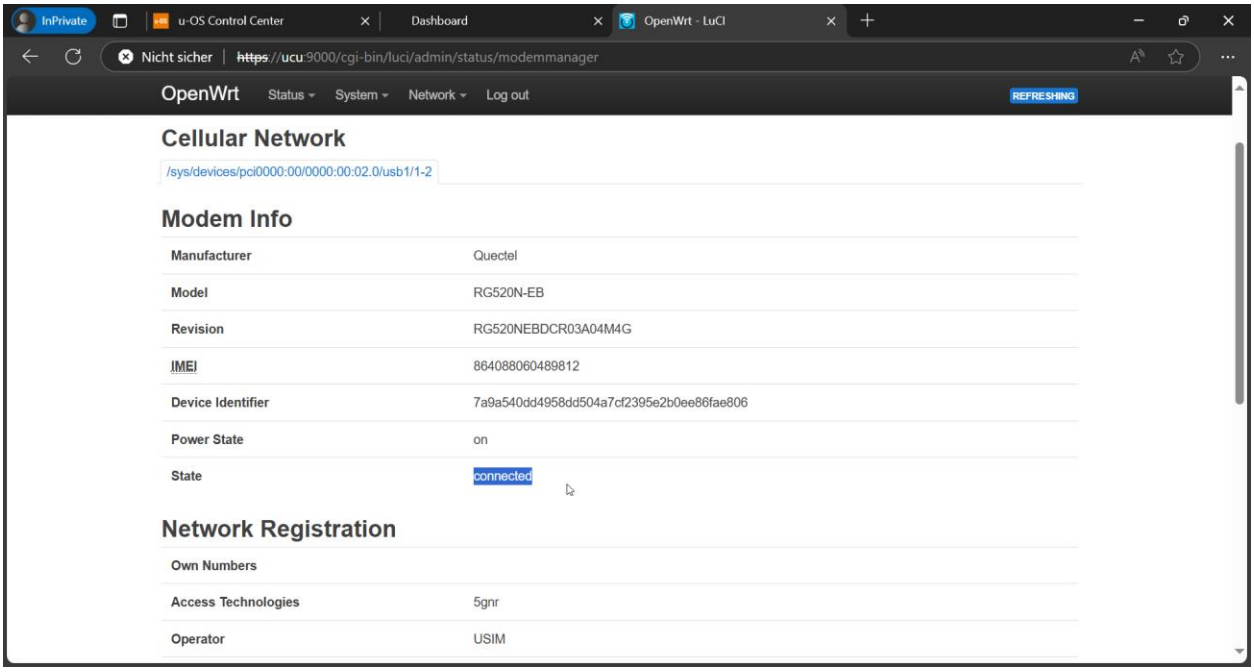
A new interface appears in the interface list with pending changes.

- Click **Save & Apply** to apply the pending changes.



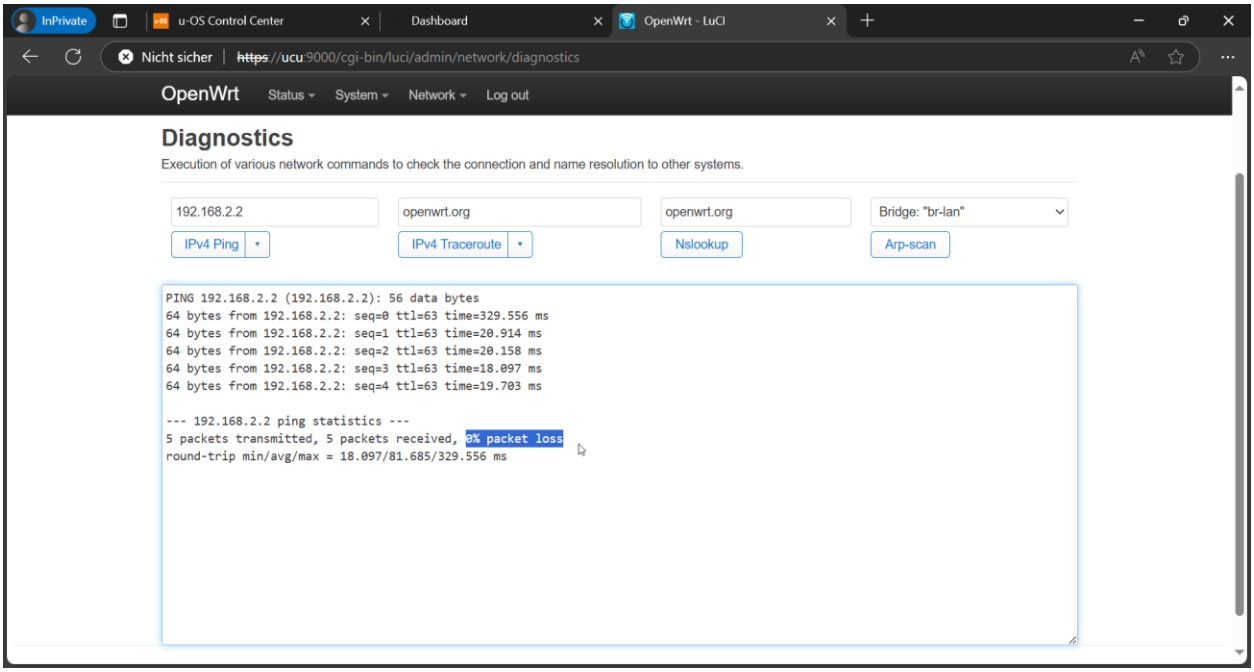
A successful assigned **IP address** and increasing **incoming (RX) network traffic** are indicators for a successful 5G network connectivity.

For 5G connectivity status details, navigate to menu sub-item **Cellular Network** within the main menu **Status**. It lists diagnostic information of the modem, SIM and the cellular network.



6.2 Test the Remote VTEP Reachability

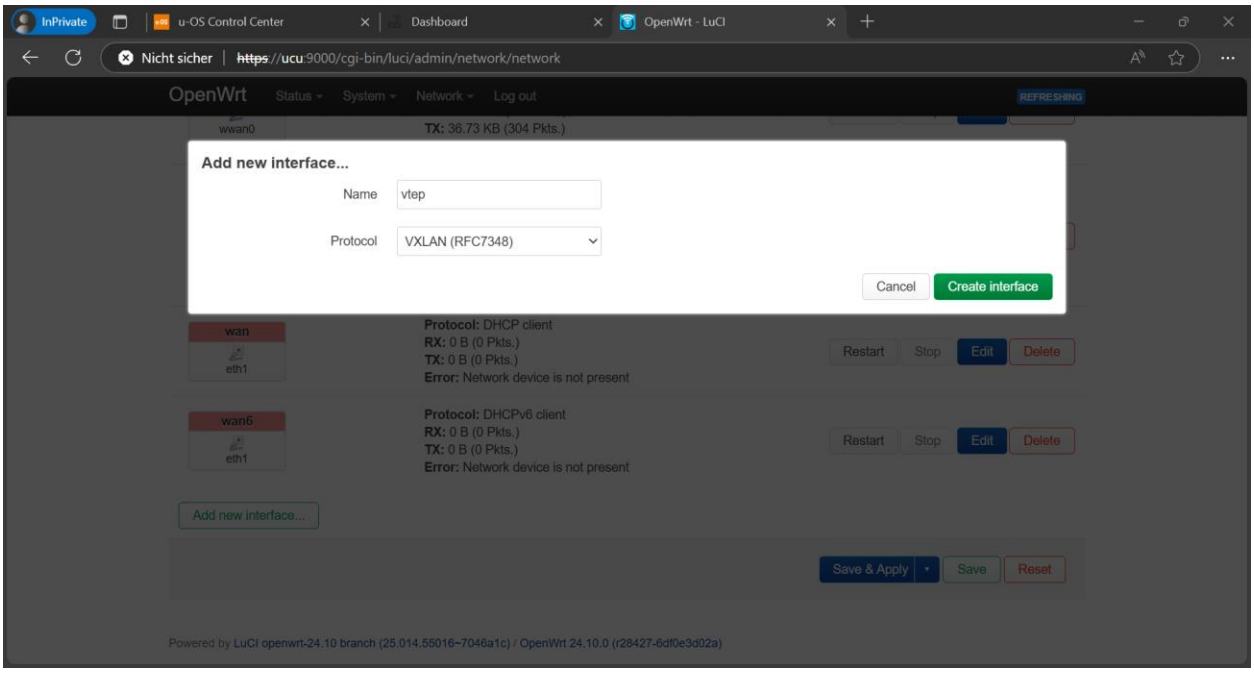
- Click on menu item **Network** and then click on the sub-item **Diagnostics**.
- Input the remote VTEP IP address in the field above **IPv4 Ping** such as **192.168.2.2** as mentioned in the Figure 1.
- Click **IPv4 Ping**.



The remote VTEP is reachable, in case of no packet loss.

6.3 Setup the VXLAN Tunnel

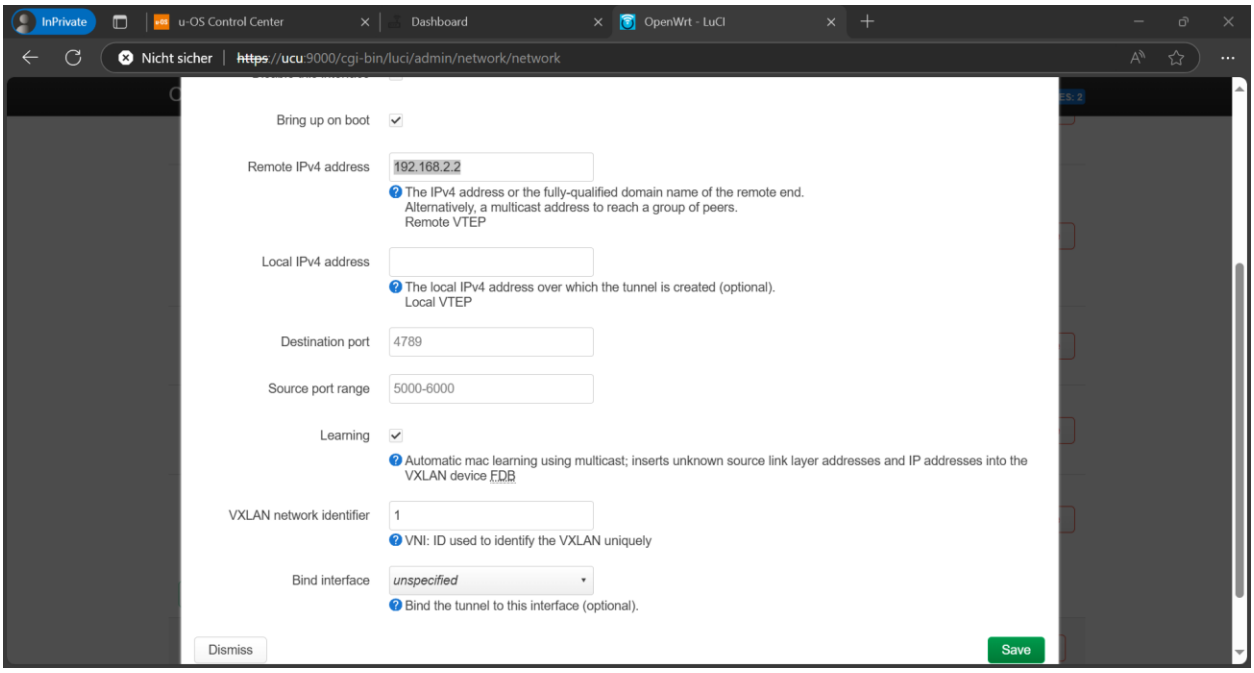
- Click on menu item **Network** and then click on the sub-item **Interfaces**.
- Click **Add new Interface…** to add the 5G network interface.
- Name the interface e.g. **vtep**
- Select protocol **VXLAN (RFC7348)**.



- Click **Create interface**.

A dialog with **VXLAN** specific parameters appears.

- Setup the **Remote IPv4** address of the remote VTEP such as **192.168.2.2** as mentioned in the Figure 1.
- Setup a unique **VXLAN network identifier** e.g. 1
- Navigate to **Firewall Settings**.
- Assign firewall-zone **lan** to enable incoming network traffic.
- Click **Save**.



- Click **Save & Apply** to apply the pending changes.

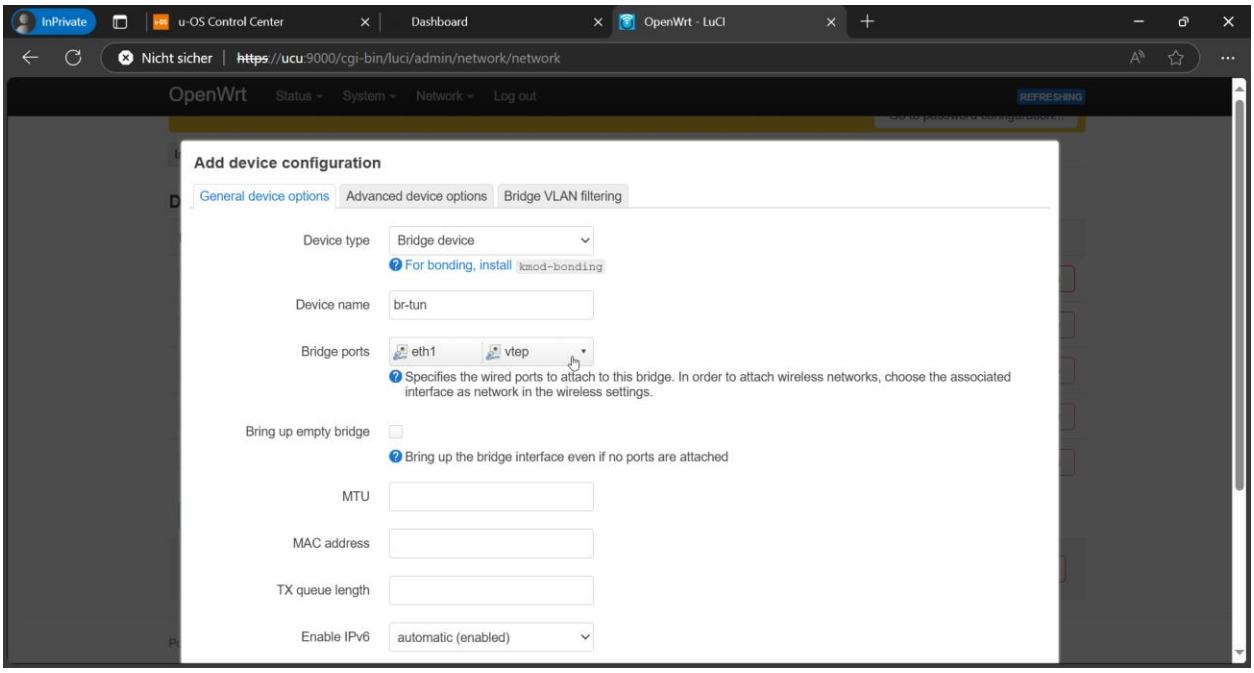
6.4 Bridge the Tunnel to Profinet Controller and Devices

Now, the Profinet device or controller must be connected to an Ethernet port.

- Connect an Ethernet port of the controller to the Profinet device or controller such as Ethernet port **X4** as mentioned in the Figure 1.
- Navigate to **OpenWRT preview** as mentioned in Section 3.3.
- Click **Edit**.
- Set **WAN Ethernet interface** to the connected Ethernet port e.g. **eth-x4**.
- Click **Apply**.

To bridge VTEP and Ethernet interfaces, a new OpenWRT bridge device must be created which acts as internal virtual switch.

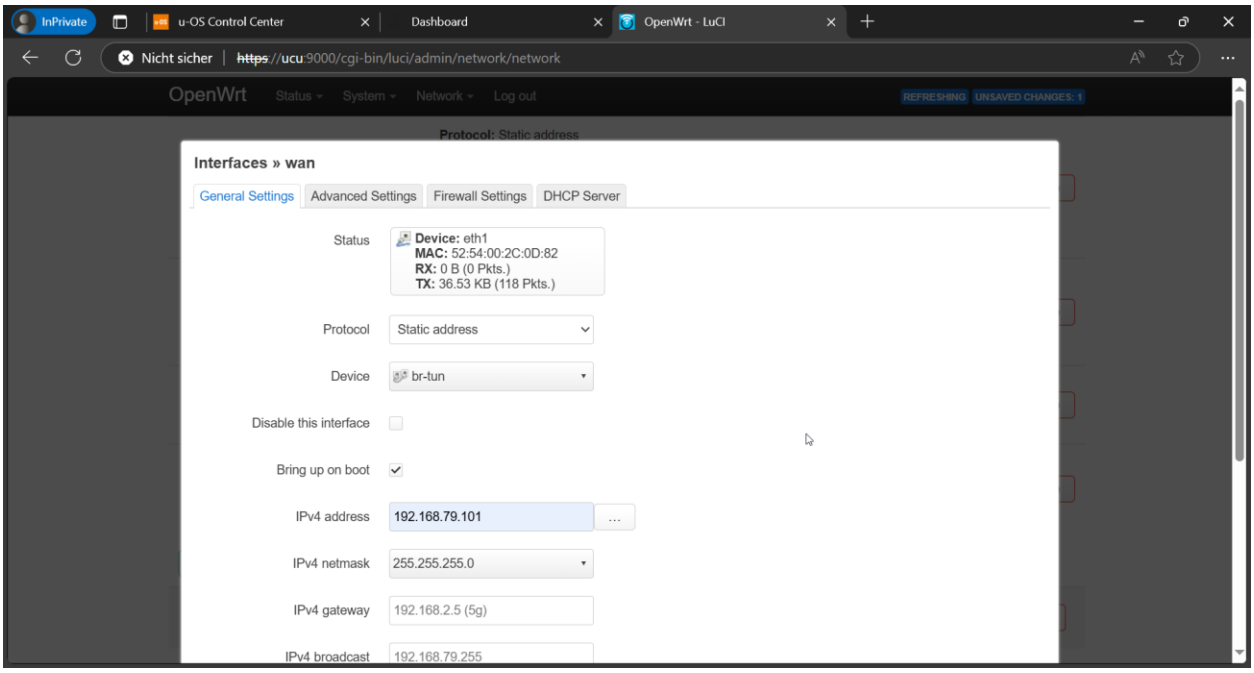
- Access the **OpenWRT Web Interface** according to Section 5.2.
- Click on menu item **Network** and then click on the sub-item **Interfaces**.
- Navigate to the tab **Devices.**
- Click **Add device configuration…**
- Select **Bridge device** for the **Device type**.
- Name the device e.g. **br-tun.**
- Select **vtep** and **eth1** as **Bridge ports**.



- Click **Save.**
- Click **Save & Apply**.

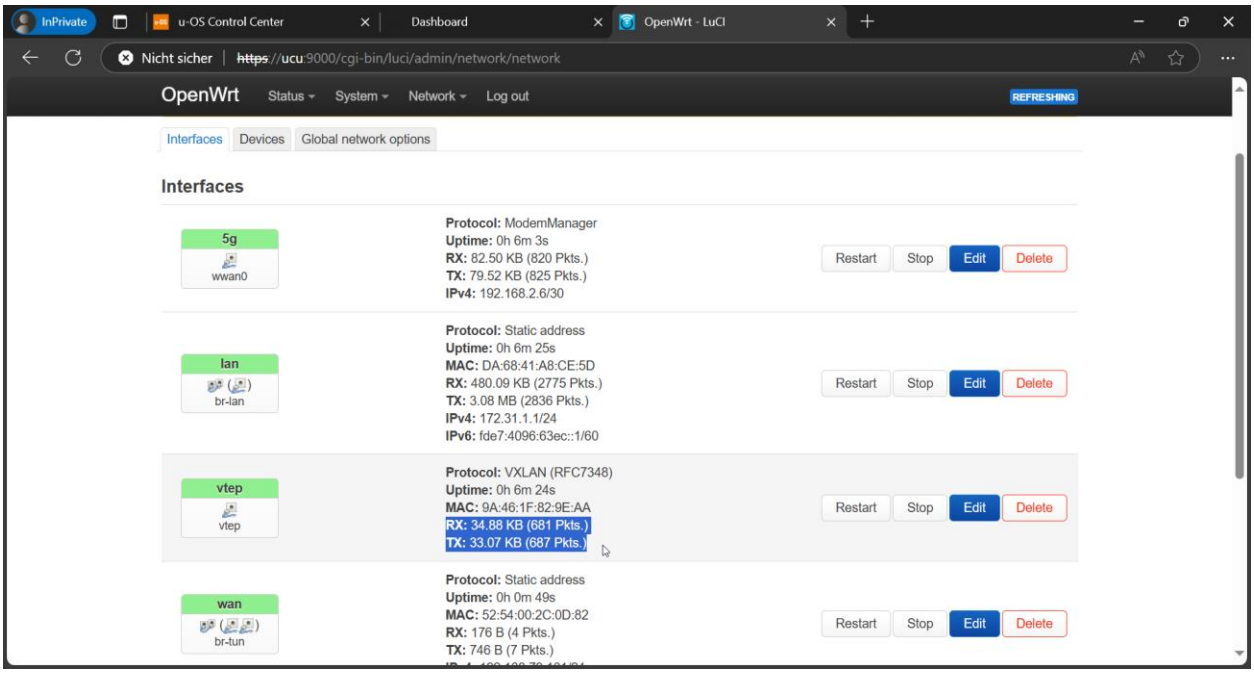
Now, the bridge device must be assigned to a network interface to be activated.

- Navigate to the tab **Interfaces.**
- Click **Edit** next to the interface **wan**.
- Select **br-tun** as **Device**.
- Select **Static address** as **Protocol**.
- Click **Switch protocol**.
- Setup an IP address such as **192.168.79.101** as mentioned in the Figure 1.
- Select IP netmask e.g. **255.255.255.0**.



- Navigate to **Firewall Settings**.
- Assign firewall-zone **lan** to enable incoming network traffic.
- Click **Save.**
- Click **Save & Apply**.

Now, the VXLAN tunnel is setup for Profinet. If the Profinet controller, the remote VTEP and some Profinet devices are connected, the VTEP interface RX and TX counter should increase as shown below.

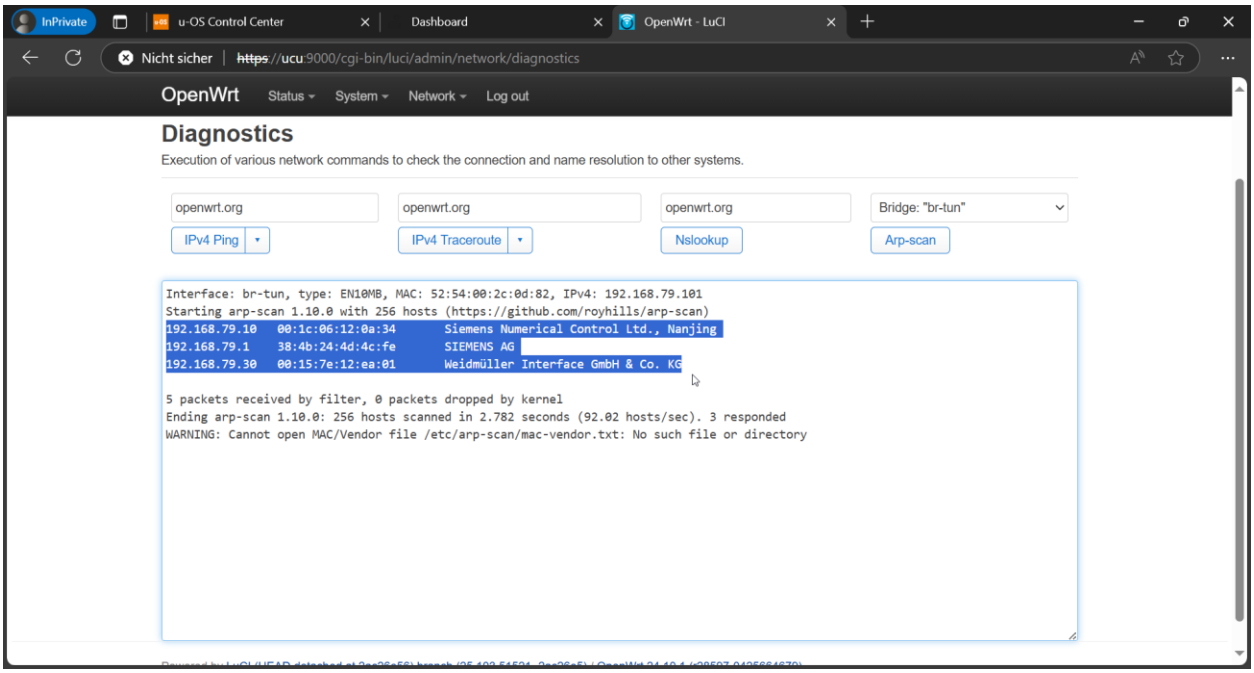


6.5 Test the Profinet Reachability

To scan all devices in the local network the utility **ARP scanner** can be used.

- Click on menu item **Network** and then click on the sub-item **Diagnostics**.
- Select **br-tun** in the dropdown field above **Arp-scan**.
- Click **Arp-scan.**

If the Profinet controller, the remote VTEP and some Profinet devices are setup correctly, they should be listed as shown below.



The setup is successfully, if all Profinet devices and controller are listed.