Remote Maintenance Gateway

RMG/941C(L,N)

with DNP/9535

First Steps

SSV Software Systems GmbH
Dünenweg 5
D-30419 Hannover
Phone: +49 (0)511/40 000-0
Fax: +49 (0)511/40 000-40
Email: sales@ssv-embedded.de

Document Revision: 1.2
Date: 2022-01-27

CONTENT

1 INTRODUCTION

This documentation gives you an overview about the initial operation and the first steps of use with the RMG/941C.

1.1 Checklist

Compare the content of your RMG/941C start-up package with the checklist below.

If any item is missing or appears to be damaged, please contact SSV!

- ✓ Remote Maintenance Gateway RMG/941C
- ✓ 1x LTE/NB-IoT antenna (only for RMG/941CL and RMG/941CN)
- ✓ Adapter cable with power and RS232 connector
- ✓ Plug-in power supply

IMPORTANT!
You will need further equipment to operate the RMG/941C. Please refer to **chapter 3**.

1.2 Conventions

Convention	Usage
bold	Important terms
`monospace`	Filenames, Pathnames, program code, command lines

Table 1: Conventions used in this document

2 SAFETY GUIDELINES

Please read the following safety guidelines carefully! In case of property or personal damage by not paying attention to this manual and/or by incorrect handling, we do not assume liability. In such cases any warranty claim expires.

- The power supply should be in immediate proximity to the device.
- The power supply must provide a stable output voltage at 12 .. 24 VDC ±10%. The output power should be at least 10 W.
- Please pay attention that the power cord or other cables are not squeezed or damaged in any way when you set up the device.
- Do NOT turn on the power supply while connecting any cables, especially the power cables. This could cause damaged device components! First connect the cables and THEN turn the power supply on.
- The installation of the device should be done only by qualified personnel.
- Discharge yourself electrostatic before you work with the device, e.g. by touching a heater of metal, to avoid damages.
- Stay grounded while working with the device to avoid damage through electrostatic discharge.
- The case of the device should be opened only by qualified personnel.

3 REQUIRED EQUIPMENT

To operate the RMG/941C the following hardware is required:

- One Ethernet cross-over cable or two Ethernet patch cables and a switch.

To operate the **RMG/941CL** the following hardware is required:

- A **valid SIM card** with an appropriate mobile tariff. Please refer to **chapter 4** to see how the SIM card is inserted.

The **RMG/941CN** comes with a **preinstalled SIM card** for NB-IoT.

To configure the RMG/941C a computer with the following features is required:

- Windows 10
- Web browser (e.g. Firefox, Chrome)
- 10/100 Mbps Ethernet network controller and TCP/IP configuration

4 SIM CARD

The internal SIM card of the RMG/941CL and RMG/941CN can be changed through the slot on the backside.

To remove the SIM card just push it gently with a screw driver until you hear a soft "click". The SIM card is ejected a few millimeters and can be pulled out easily.

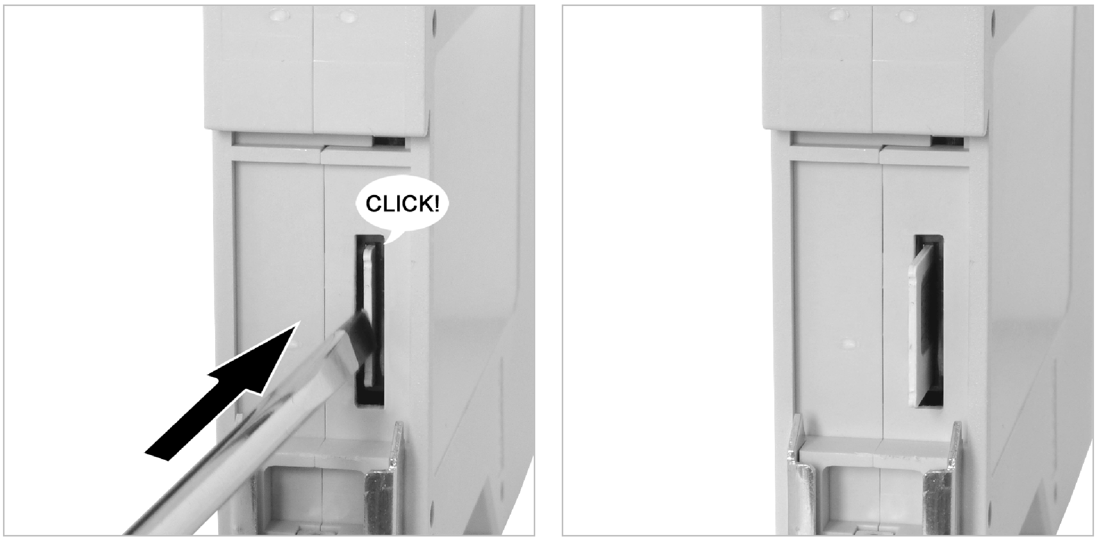


Figure 1: Removing the SIM card

To insert the SIM card just push it by hand as deep as possible into the slot.

Please note:
Pay attention to the correct orientation of the SIM card like shown in **fig. 2**!

Then use a screw driver to push it gently further into the slot until you here a soft "click".

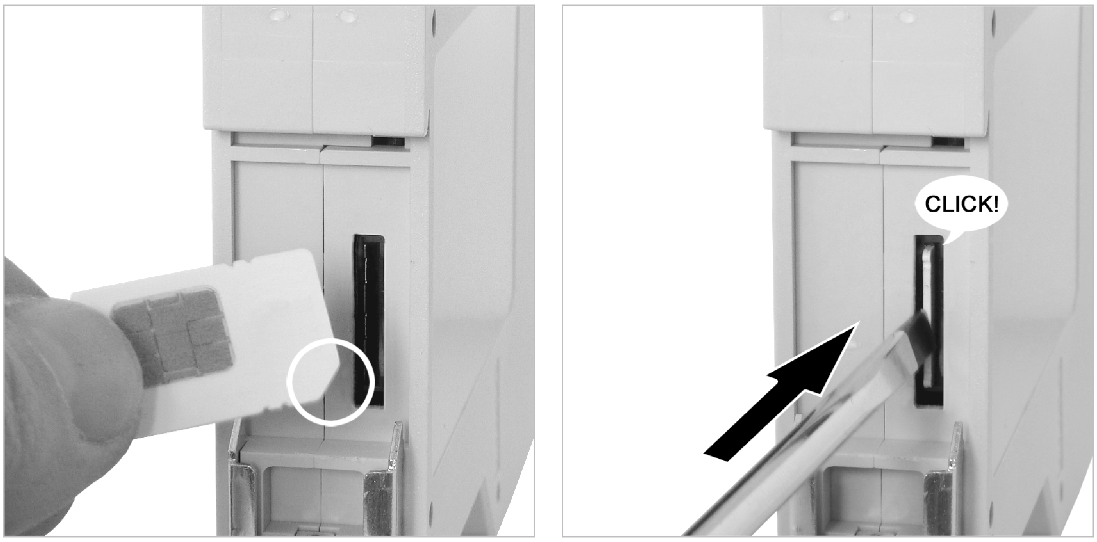


Figure 2: Inserting the SIM card

5 CABLE CONNECTIONS

For a quick and easy start with the RMG/941C there are a few cable connections necessary. The following chapters describe how these connections have to be made.

5.1 LTE/NB-IoT Antenna

Connect the LTE/NB-IoT antenna with the RMG/941C(L,N) like shown in **fig. 3** and place it where the LTE/NB-IoT signal strength is high.

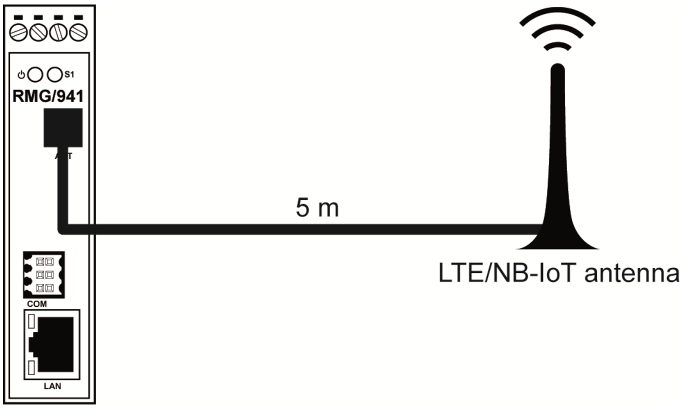


Figure 3: Connecting the LTE/NB-IoT antenna

5.1 Ethernet

The Ethernet link between the PC and **LAN** of the RMG/941C can be made on two ways:

- Direct with an Ethernet cross-over cable like shown in **fig. 4**.
- With two standard Ethernet patch cables over a hub or switch like shown in **fig. 5**.

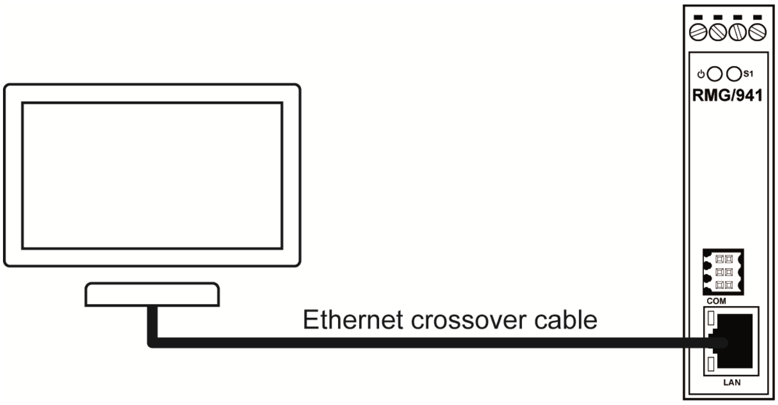


Figure 4: Ethernet link with cross-over cable

Please note:
For the Ethernet connection in **fig. 4** it is required to use a **cross-over cable**. Do not use an ordinary patch cable. Both types of cables are in most cases visual indistinguishable. But the internal wiring is fully different. Mixing up these types of cables leads to LAN errors. Hence pay attention to the label of the cable or packing.

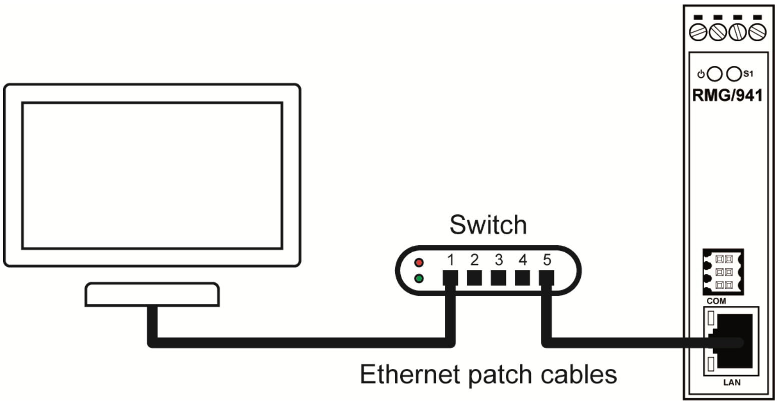


Figure 5: Ethernet link with hub or switch

The IP address of the LAN interface is ex-factory set to

`192.168.0.126`.

5.2 CAN

A CAN device can be connected to the CAN port via the screw terminal like shown in **fig. 6**.

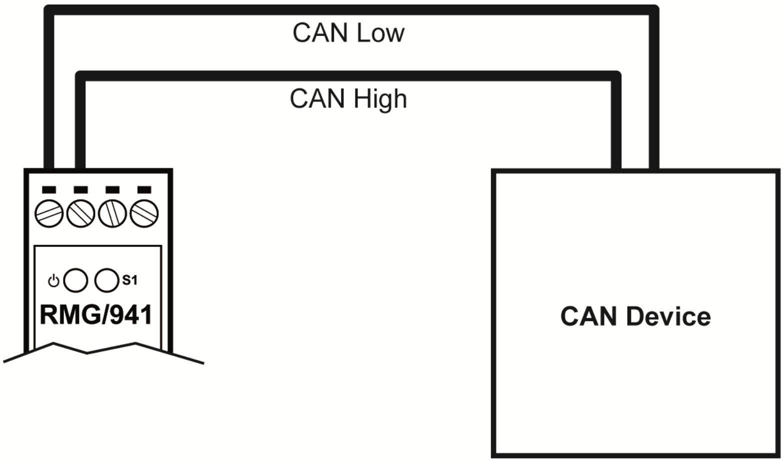


Figure 6: CAN connection

Terminal	Signal
A1	CAN Low
A2	CAN High

Table 2: Screw terminal CAN pinout

Please note:
The RMG/941C offers an **internal termination resistor**. To use the resistor it has to be enabled via the SSV/WebUI (**see chapter 8.1**).

5.3 Power Supply

The RMG/941C needs a supply voltage of 12 .. 24 VDC ±10% to work.

Connect the cables of an appropriate power supply like shown in **fig. 7**.

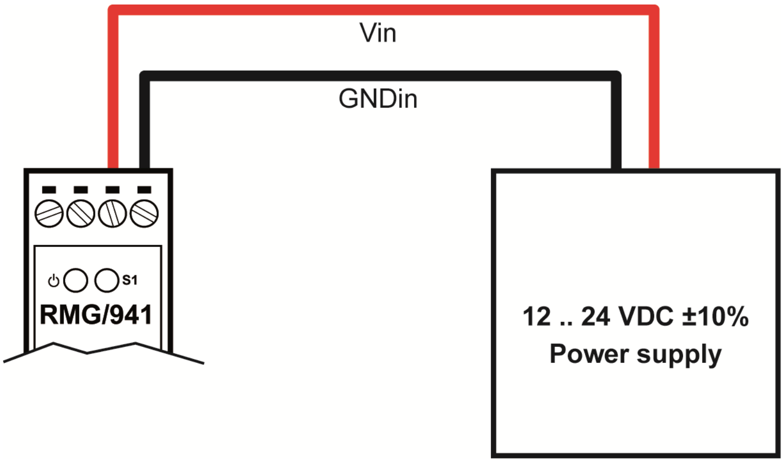


Figure 7: Power supply for the RMG/941C

Terminal	Signal
A3	Vin (12 .. 24 VDC ±10%)
A4	GNDin

Table 3: Screw terminal power

CAUTION!
Providing the RMG/941C with a higher voltage than the regular 12 .. 24 VDC ±10% could cause damaged device components!

Do **NOT** turn on the power supply while connecting it with the RMG/941C. This could cause damaged device components! First connect the power supply and **THEN** turn it on.

6 BASIC SETTINGS

6.1 Booting the RMG/941C

Just power up the RMG/941C and the boot process starts immediately. The RMG/941C boots an embedded Linux out of its Flash memory. This may take up to one minute.

6.2 Accessing the SSV/WebUI

To open the login page of the SSV/WebUI enter the ex-factory IP address and port number of LAN1 of the RMG/941C in a web browser:

```
https://192.168.0.126:7777
```

Enter your username and password and click on **[OK]**. Both username and password can be found on the **nameplate** of the RMG/941C.

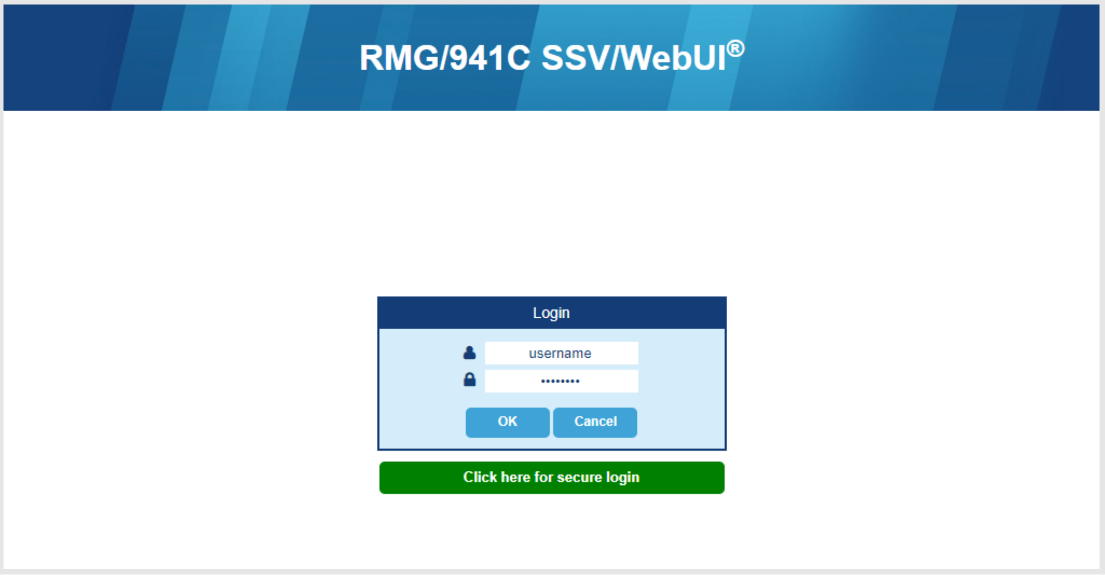


Figure 8: Login page of the SSV/WebUI

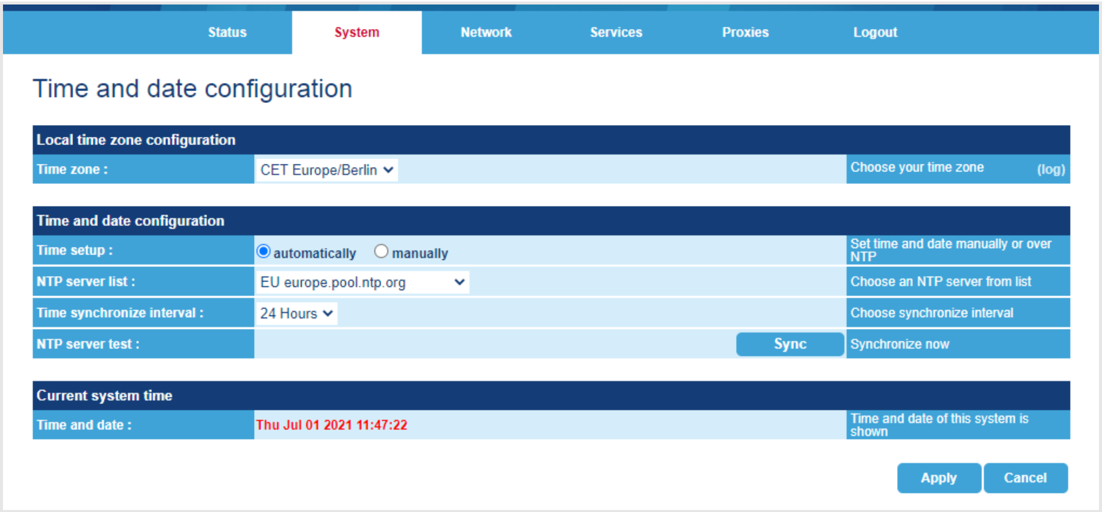
The SSV/WebUI allows to view log files and to configure the system settings of the RMG/941C with a web browser, e.g. enabling and disabling services like Telnet or changing the IP address.

Please note:
It is mandatory to set a **password** before using any remote access services like Telnet, SSH, FTP, SFTP, shellinthebox or the serial console. Therefore please refer to **chapter 6.4**.

6.3 Configuring Time and Date

Please note:
The RMG/941C does not have a backup battery for its real time clock. For this reason, the **time and date must be set during the initial configuration**. That ensures correct log entries and avoids other problems, e.g. when importing certificates.

Choose from the menu **System > Time and date**.



Time and date configuration

Local time zone configuration		
Time zone :	CET Europe/Berlin	Choose your time zone (log)

Time and date configuration		
Time setup :	● automatically ○ manually	Set time and date manually or over NTP
NTP server list :	EU europe.pool.ntp.org	Choose an NTP server from list
Time synchronize interval :	24 Hours	Choose synchronize interval
NTP server test :	Sync	Synchronize now

Current system time		
Time and date :	Thu Jul 01 2021 11:47:22	Time and date of this system is shown

Figure 9: Setting time and date automatically

The time and date configuration offers two options: **automatic** and **manual**.

We recommend to select the automatic configuration if the RMG/941C has Internet access or the LAN provides a local time server (NTP). This option has the advantage that the system synchronizes the time and date automatically after an interruption of the power supply.

Automatic setup

1. In the section **Local time zone configuration** select the appropriate time zone from the dropdown menu.
2. In the line T**ime setup** enable the radio button **automatically**.
3. In the line **NTP server list** select one of the preconfigured NTP servers from the dropdown menu. By selecting **(user defined)** you can also enter any other NTP server.
4. In the line **Time synchronize interval** select the desired time period.
5. Click on **[Sync]** to test if the synchronization works.
6. Click on **[Apply]**.

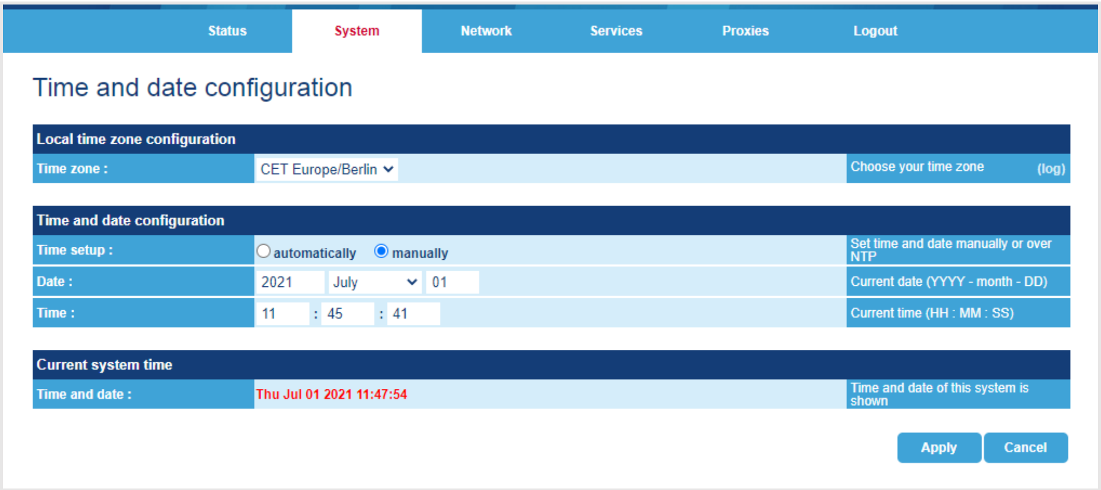
Manual setup

Please note:
If the manual setup is used the time and date must be reset each time the power supply was interrupted.

1. In the section **Local time zone configuration** select the appropriate time zone from the dropdown menu.

2. In the line **Time setup** enable the radio button **manually** and set the current time and date.

3. Click on **[Apply]**.



Time and date configuration

Local time zone configuration		
Time zone :	CET Europe/Berlin	Choose your time zone (log)

Time and date configuration		
Time setup :	○ automatically ● manually	Set time and date manually or over NTP
Date :	2021 July 01	Current date (YYYY - month - DD)
Time :	11 : 45 : 41	Current time (HH : MM : SS)

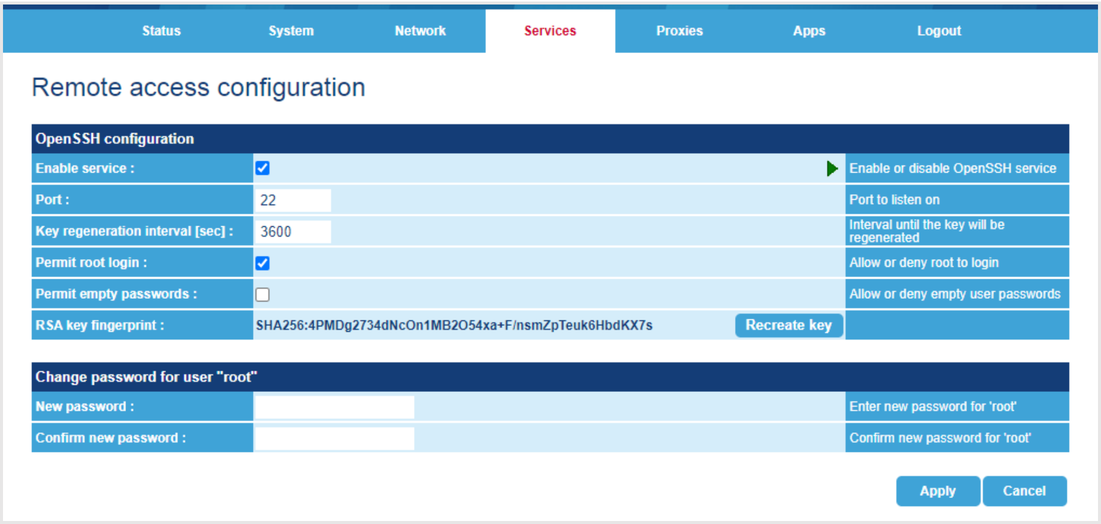
Current system time		
Time and date :	Thu Jul 01 2021 11:47:54	Time and date of this system is shown

Figure 10: Setting time and date manually

6.4 Password for Remote Access Services

It is mandatory to set a password before using any remote access services like Telnet, SSH, FTP, SFTP, shellinthebox or the serial console.

Therefore choose from the menu **Services > Remote access** and enter a password in the section **Change password for user “root”** and click on **[Apply]**.



Remote access configuration

OpenSSH configuration		
Enable service :	☑	Enable or disable OpenSSH service
Port :	22	Port to listen on
Key regeneration interval [sec] :	3600	Interval until the key will be regenerated
Permit root login :	☑	Allow or deny root to login
Permit empty passwords :	☐	Allow or deny empty user passwords
RSA key fingerprint :	SHA256:4PMDg2734dNcOn1MB2O54xa+F/nsmZpTeuk6HbdKX7s	

Change password for user "root"		
New password :		Enter new password for 'root'
Confirm new password :		Confirm new password for 'root'

Figure 11: Remote access configuration page

6.5 Accessing the SSV/WebUI with DHCP enabled

If the automatic IP address configuration of LAN1 via DHCP is enabled, you have to check the assigned IP address, which is necessary to access the RMG/941C via a Telnet client or a web browser.

Therefore open in Windows **Control Panel > Network and Internet > View network computers and devices**. The RMG/941C should show up in this list.

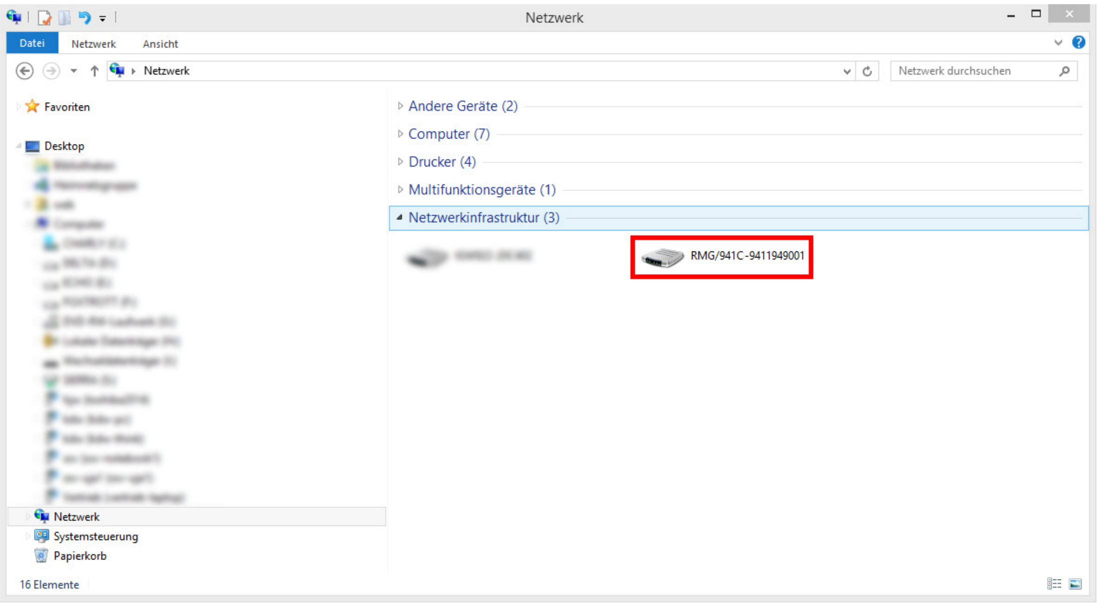
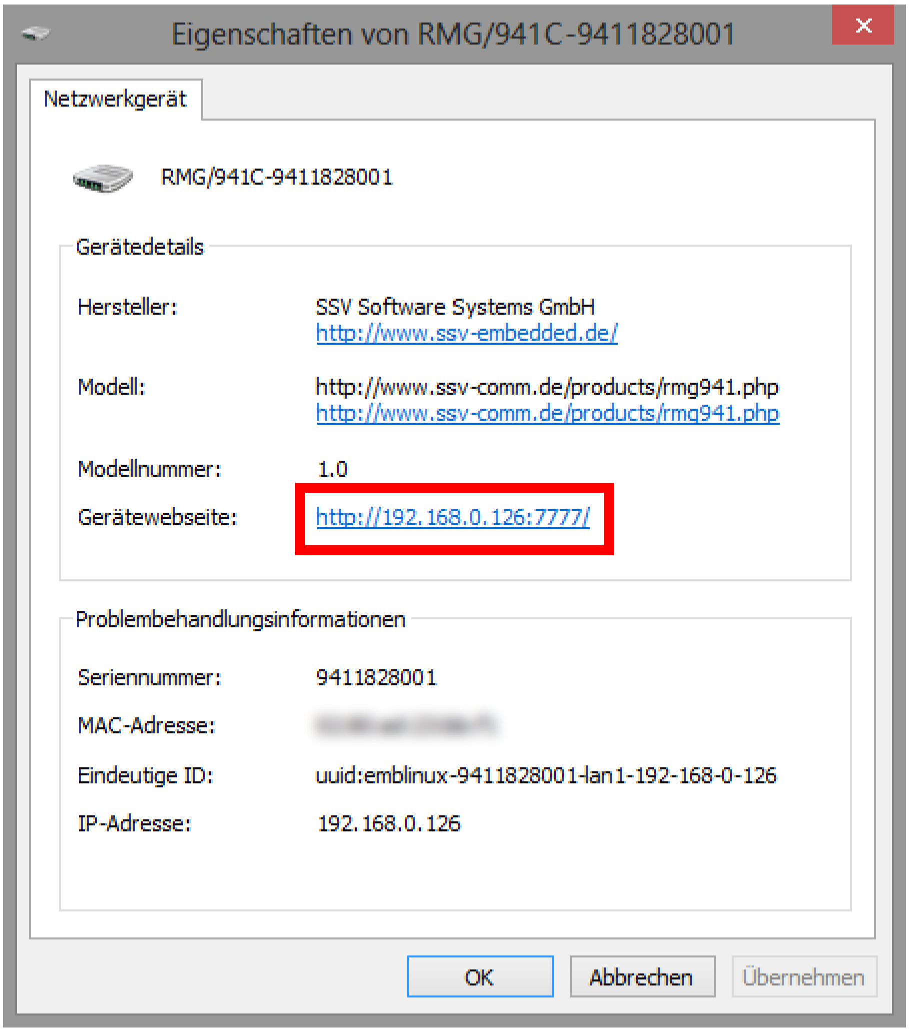


Figure 12: Selecting the RMG/941C

Just **right-click** on the RMG/941C to open the properties dialog, where you can see the current IP address of the RMG/941C like shown in **fig. 12**.

A **double-click** on the RMG/941C opens the **SSV/WebUI** in a web browser.

Please note:
To access the SSV/WebUI, it is important to add the port number **7777** to the current IP address of the RMG/941C, e.g.: **`http://192.168.0.126:7777`**!



Eigenschaften von RMG/941C-9411828001

Netzwerkgerät

RMG/941C-9411828001

Gerätedetails

Hersteller: SSV Software Systems GmbH
http://www.ssv-embedded.de/

Modell: http://www.ssv-comm.de/products/rmg941.php
http://www.ssv-comm.de/products/rmg941.php

Modellnummer: 1.0

Gerätewebseite: http://192.168.0.126:7777/

Problembehandlungsinformationen

Seriennummer: 9411828001

MAC-Adresse: [redacted]

Eindeutige ID: uuid:emblinux-9411828001-lan1-192-168-0-126

IP-Adresse: 192.168.0.126

Figure 13: The properties dialog shows the current IP address

Now you are able to access the RMG/941C via a Telnet client or a web browser.

Identification via LED

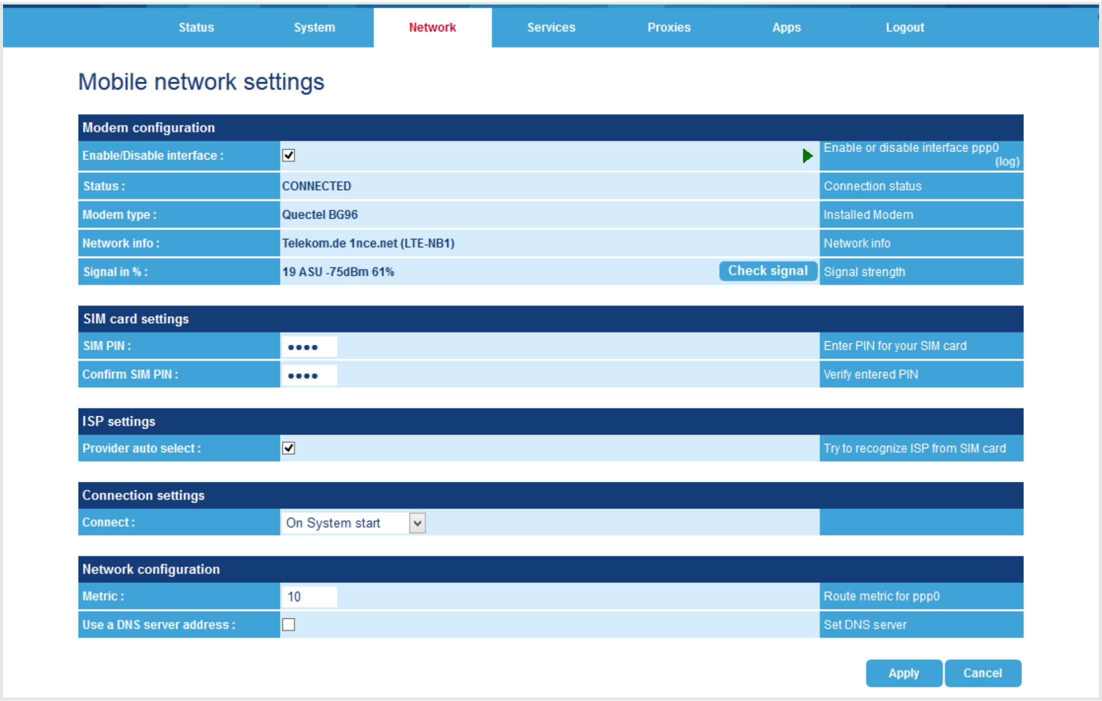
To identify which gateway you are currently logged in to, you can make the **LED S1 flash for 5 seconds**.

Therefore choose from the menu **System > System identification** and click on **[Flash]**.

6.6 RMG/941CN: Checking NB-IoT Connection

The RMG/941CN comes with a preinstalled NB-IoT SIM card with 500 MB free traffic volume.

To check if there is a connection with the NB-IoT mobile network choose from the menu **Network > Mobile**.



Mobile network settings

Modem configuration		
Enable/Disable interface :	☑	Enable or disable interface ppp0 (log)
Status :	CONNECTED	Connection status
Modem type :	Quectel BG96	Installed Modem
Network info :	Telekom.de 1nce.net (LTE-NB1)	Network info
Signal in % :	19 ASU -75dBm 61%	Signal strength

SIM card settings		
SIM PIN :	••••	Enter PIN for your SIM card
Confirm SIM PIN :	••••	Verify entered PIN

ISP settings		
Provider auto select :	☑	Try to recognize ISP from SIM card

Connection settings		
Connect :	On System start	

Network configuration		
Metric :	10	Route metric for ppp0
Use a DNS server address :	□	Set DNS server

Figure 14: Mobile network settings of the RMG/941CN

In the section **Modem configuration** the line **Status** should display **CONNECTED**.

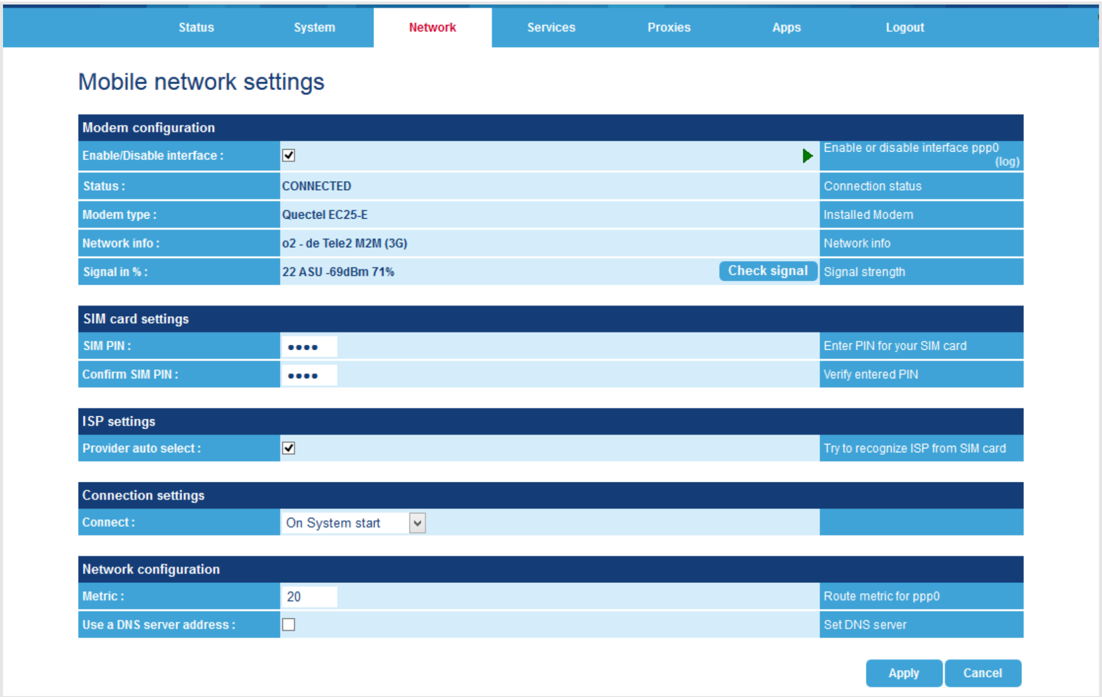
You can also check the signal strength by clicking on the button **[Check signal]**.

Please note:
If the connection to the NB-IoT network fails, the modem tries to connect with the regular mobile network with 2G!

6.7 RMG/941CL: LTE Modem Configuration

The RMG/941CL does **NOT** come with a SIM card. To connect with the LTE mobile network you have to insert a **valid SIM card** first. **Chapter 4** shows how to insert/change a SIM card.

To configure the LTE modem settings choose from the menu **Network > Mobile**.



Mobile network settings

Modem configuration		
Enable/Disable interface :	☑	Enable or disable interface ppp0 (log)
Status :	CONNECTED	Connection status
Modem type :	Quectel EC25-E	Installed Modem
Network info :	o2 - de Tele2 M2M (3G)	Network info
Signal in % :	22 ASU -69dBm 71% Check signal	Signal strength

SIM card settings		
SIM PIN :	••••	Enter PIN for your SIM card
Confirm SIM PIN :	••••	Verify entered PIN

ISP settings		
Provider auto select :	☑	Try to recognize ISP from SIM card

Connection settings		
Connect :	On System start	

Network configuration		
Metric :	20	Route metric for ppp0
Use a DNS server address :	□	Set DNS server

Figure 15: Mobile network settings

1. In the section **Modem configuration** enable the checkbox.

2. If the provider is not recognized automatically disable the checkbox in the section **ISP settings** and choose your provider manually.

3. Enter the **PIN** of the SIM card.

4. In the section Connection settings choose On System start.

5. Click on **[Apply]**.

In the section **Network configuration** you can enter a **DNS server** if needed.

In the section **Modem configuration** the line **Status** should display **CONNECTED** after the successful configuration.

You can also check the signal strength by clicking on the button **[Check signal]**.

If the mobile interface is going to be used for the **Internet connection** (e.g. to work as an **LTE router**), please make sure it is selected as **WAN interface**. Therefore choose from the menu **Network > WAN**. You can find more information about the WAN configuration in **chapter 6.8**.

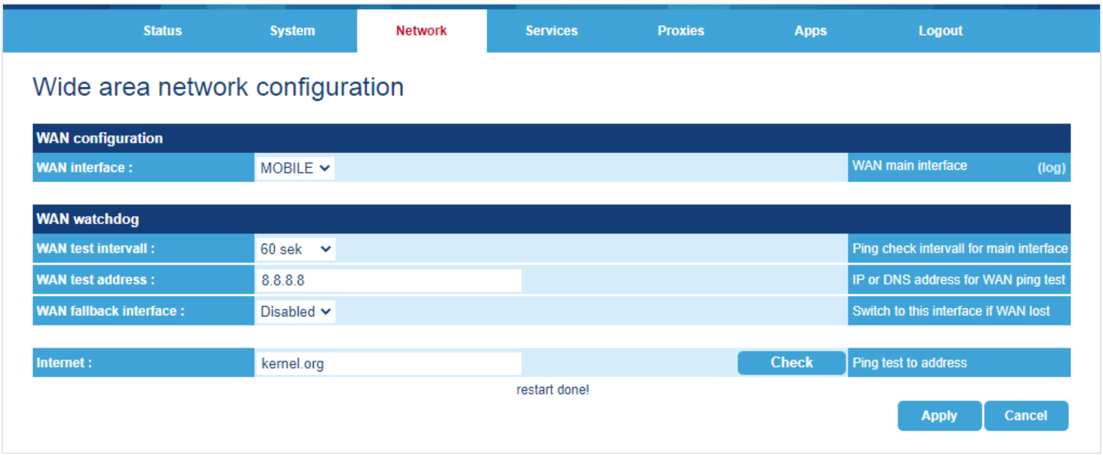
6.8 RMG/941C(L): WAN Configuration

The WAN (Wide Area Network) configuration allows to define which interface is used for the Internet connection.

The RMG/941C can only access the Internet via the LAN interface.

The RMG/941CL can additionally access the Internet via the mobile interface, e.g. to work as an **LTE router**. Therefore the WAN settings need to be configured.

Choose from the menu **Network > WAN**.



Wide area network configuration

WAN configuration		
WAN interface :	MOBILE	WAN main interface (log)
WAN watchdog		
WAN test intervall :	60 sek	Ping check intervall for main interface
WAN test address :	8.8.8.8	IP or DNS address for WAN ping test
WAN fallback interface :	Disabled	Switch to this interface if WAN lost
Internet :	kernel.org	Ping test to address

restart done!

Figure 16: WAN configuration

1. In the section **WAN configuration** you can choose the interface used for the Internet connection from the dropdown menu. For a LAN connection select **LAN1**, for a mobile network connection select **Mobile**.

2. In the section **Internet** click on **[Check]** to test the Internet connection.

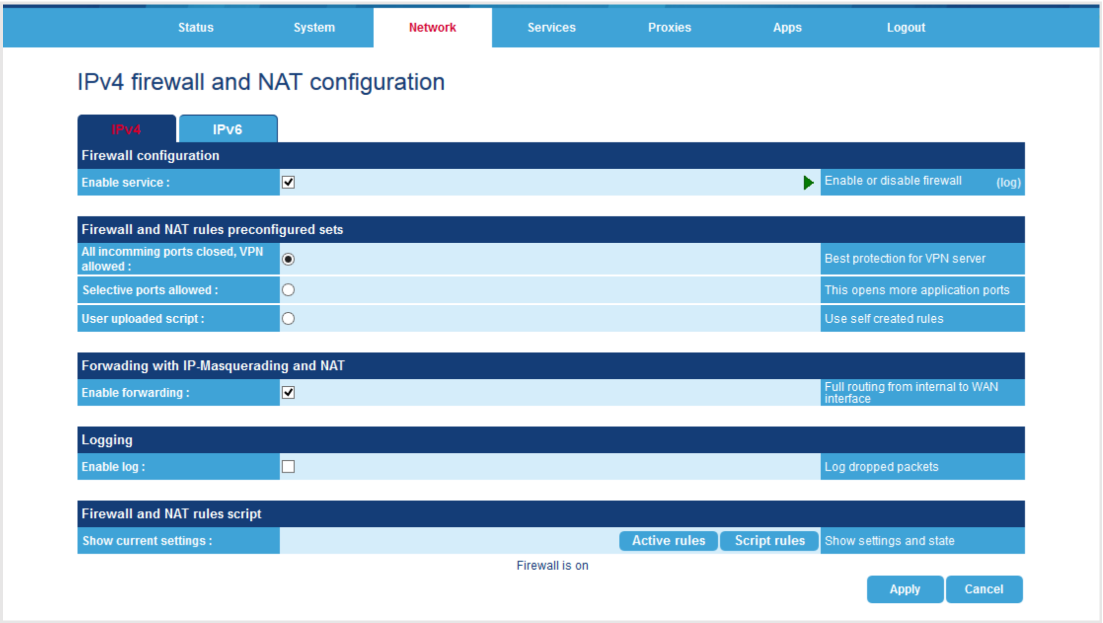
3. Click on **[Apply]**.

Please note:
If the RMG/941CL is operated as an LTE router the firewall must be enabled (please refer to chapter 6.9)!

6.9 RMG/941CL: Firewall Configuration

Please note:
If the RMG/941CL is operated as an LTE router the firewall must be enabled!

Choose from the menu **Services > Firewall and NAT**.



IPv4 firewall and NAT configuration

Firewall configuration		
Enable service :	☑	Enable or disable firewall (log)
Firewall and NAT rules preconfigured sets		
All incomming ports closed, VPN allowed :	●	Best protection for VPN server
Selective ports allowed :	○	This opens more application ports
User uploaded script :	○	Use self created rules
Forwading with IP-Masquerading and NAT		
Enable forwarding :	☑	Full routing from internal to WAN interface
Logging		
Enable log :	□	Log dropped packets
Firewall and NAT rules script		
Show current settings :	Active rules Script rules	Show settings and state

Firewall is on

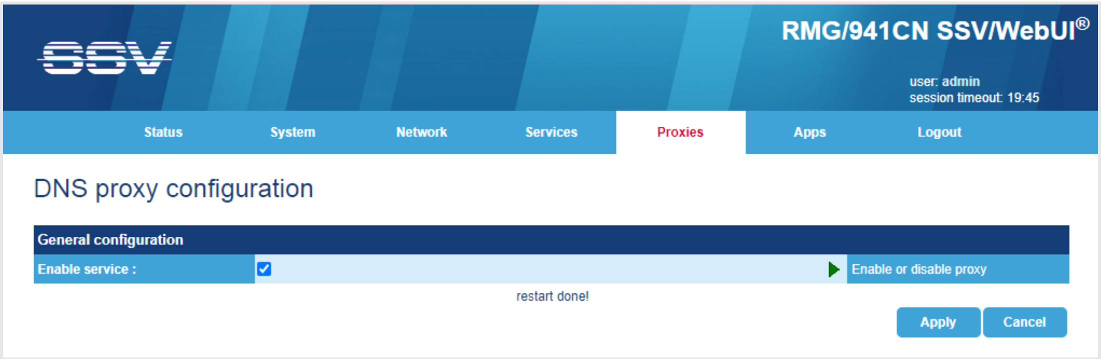
Figure 17: Firewall and NAT settings

1. In the section **Firewall configuration** enable the checkbox.
2. In the section **Forwarding with IP-Masquerading and NAT** enable the checkbox.
3. Click on **[Apply]**.

6.10 DNS Proxy

Please note:
If the RMG/941CL is operated as an LTE router the DNS proxy must be enabled!

Choose from the menu **Proxies > DNS**, enable the checkbox in the section **General configuration** and click on **[Apply]**.



DNS proxy configuration

General configuration

Enable service : ☑ Enable or disable proxy

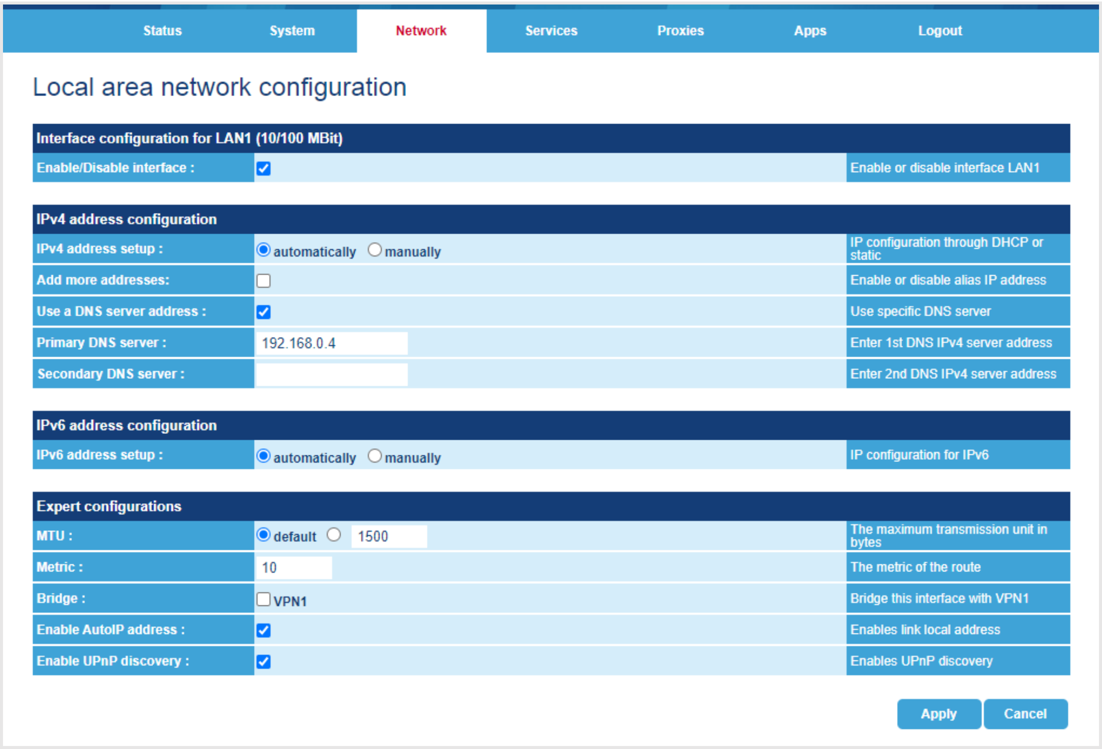
restart done!

Figure 18: **DNS proxy configuration**

6.11 LAN Configuration

The IP address of the LAN interface is ex-factory set to `192.168.0.126`.

To configure the LAN settings choose from the menu **Network > LAN1**.



Local area network configuration

Interface configuration for LAN1 (10/100 MBit)		
Enable/Disable interface :	☑	Enable or disable interface LAN1

IPv4 address configuration		
IPv4 address setup :	● automatically ○ manually	IP configuration through DHCP or static
Add more addresses:	□	Enable or disable alias IP address
Use a DNS server address :	☑	Use specific DNS server
Primary DNS server :	192.168.0.4	Enter 1st DNS IPv4 server address
Secondary DNS server :		Enter 2nd DNS IPv4 server address

IPv6 address configuration		
IPv6 address setup :	● automatically ○ manually	IP configuration for IPv6

Expert configurations		
MTU :	● default ○ 1500	The maximum transmission unit in bytes
Metric :	10	The metric of the route
Bridge :	□ VPN1	Bridge this interface with VPN1
Enable AutoIP address :	☑	Enables link local address
Enable UPnP discovery :	☑	Enables UPnP discovery

Figure 19: LAN settings

To enable the **automatic IP address assignment via DHCP** follow these steps:

1. In the section **IP address configuration** enable the radio button **automatically**.

2. You can enter up to two DNS servers if required.

3. In the section **Expert configuration** enable the checkbox **Enable AutoIP address**.

4. Click on **[Apply]**.

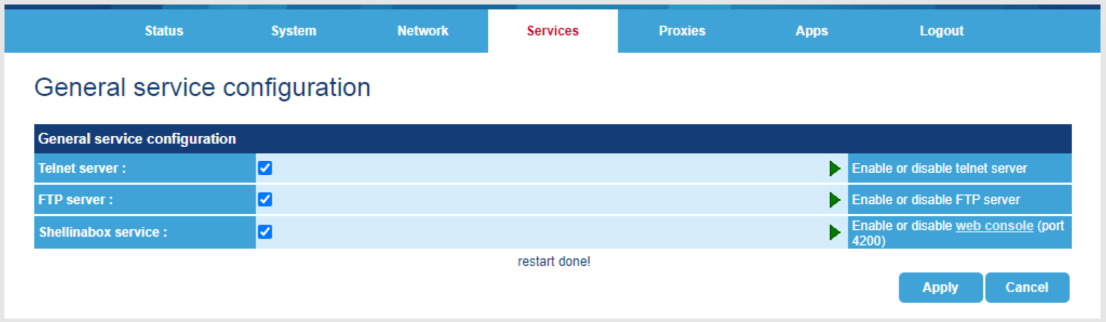
If the LAN interface is going to be used for the **Internet connection**, please make sure it is selected as **WAN interface**. Therefore choose from the menu **Network > WAN**. You can find more information about the WAN configuration in **chapter 6.8**.

Please note:
After DHCP was enabled, it is necessary to re-log into the SSV/WebUI with the new assigned IP address of LAN. Please refer to **chapter 6.5** to find out the current IP address.

6.12 Access via Telnet

The Telnet server must be enabled via the SSV/WebUI (see **fig. 20**). Therefore choose from the menu **Services > General**, enable the checkbox in the line **Telnet server** and click on **[Apply]**.

Please note:
It is mandatory to set a **password** before using Telnet. Please refer to **chapter 6.4**.



General service configuration

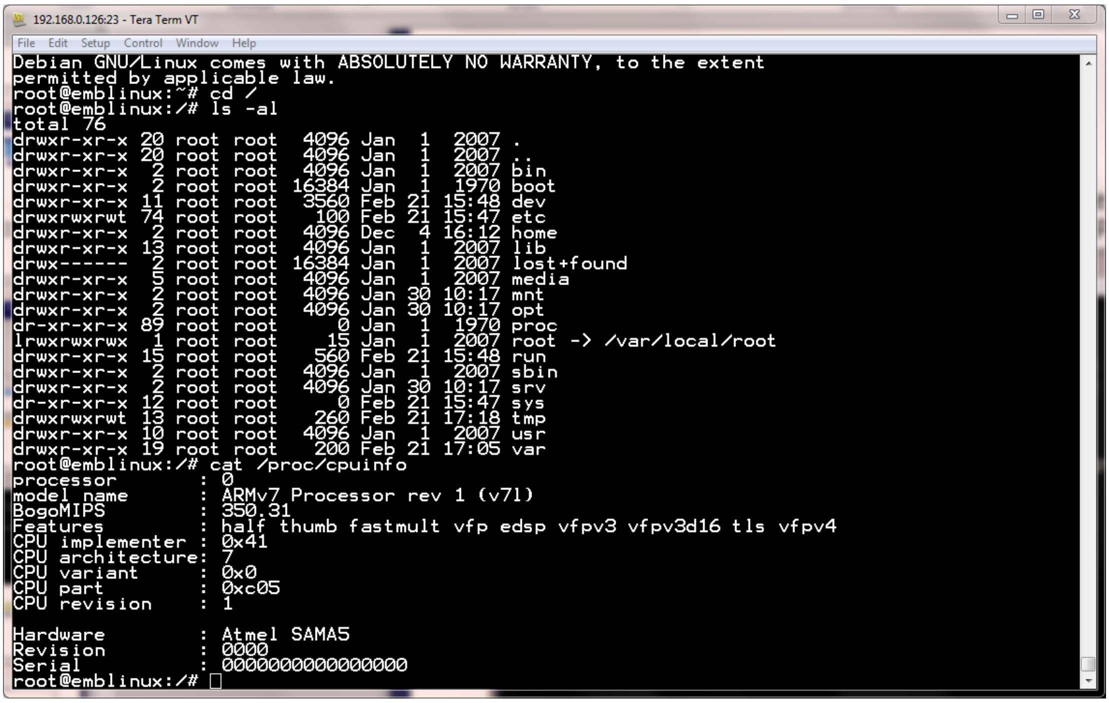
General service configuration		
Telnet server :	☑	Enable or disable telnet server
FTP server :	☑	Enable or disable FTP server
Shellinabox service :	☑	Enable or disable web console (port 4200)

restart done!

Figure 20: Enabling the Telnet server

To access the RMG/941C via Telnet open a Telnet client program (like **TeraTerm**) on your host PC and enter the current IP address of the RMG/941C to activate a Telnet session.

In the upcoming Telnet window you can enter your login data.


192.168.0.126:23 - Tera Term VT
File Edit Setup Control Window Help

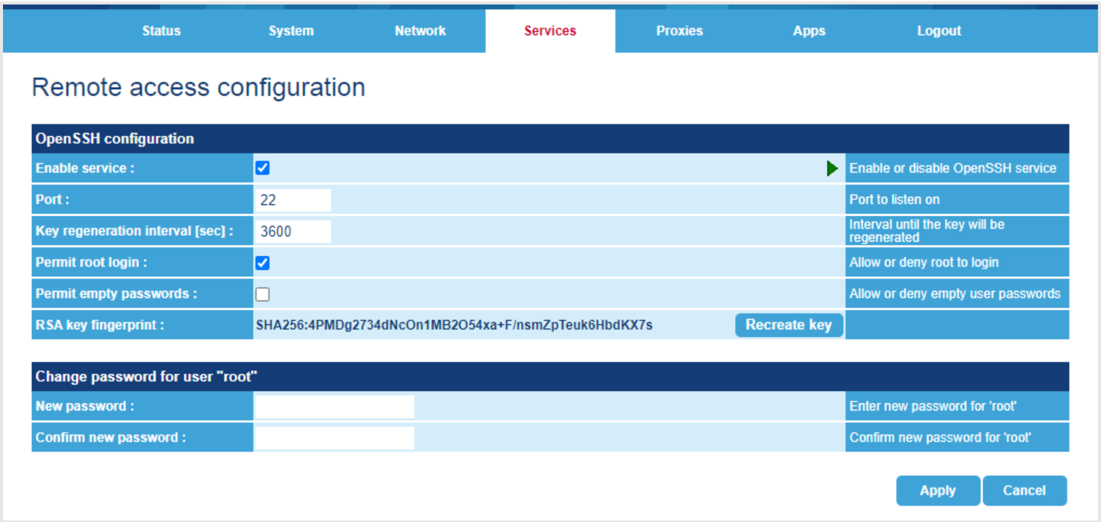
```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@emblinux:~# cd /
root@emblinux:/# ls -al
total 76
drwxr-xr-x 20 root root  4096 Jan  1  2007 .
drwxr-xr-x 20 root root  4096 Jan  1  2007 ..
drwxr-xr-x  2 root root  4096 Jan  1  2007 bin
drwxr-xr-x  2 root root 16384 Jan  1  1970 boot
drwxr-xr-x 11 root root  3560 Feb 21 15:48 dev
drwxrwxrwt 74 root root   100 Feb 21 15:47 etc
drwxr-xr-x  2 root root  4096 Dec  4 16:12 home
drwxr-xr-x 13 root root  4096 Jan  1  2007 lib
drwx------  2 root root 16384 Jan  1  2007 lost+found
drwxr-xr-x  5 root root  4096 Jan  1  2007 media
drwxr-xr-x  2 root root  4096 Jan 30 10:17 mnt
drwxr-xr-x  2 root root  4096 Jan 30 10:17 opt
dr-xr-xr-x 89 root root     0 Jan  1  1970 proc
lrwxrwxrwx  1 root root    15 Jan  1  2007 root -> /var/local/root
drwxr-xr-x 15 root root   560 Feb 21 15:48 run
drwxr-xr-x  2 root root  4096 Jan  1  2007 sbin
drwxr-xr-x  2 root root  4096 Jan 30 10:17 srv
dr-xr-xr-x 12 root root     0 Feb 21 15:47 sys
drwxrwxrwt 13 root root   260 Feb 21 17:18 tmp
drwxr-xr-x 10 root root  4096 Jan  1  2007 usr
drwxr-xr-x 19 root root   200 Feb 21 17:05 var
root@emblinux:/# cat /proc/cpuinfo
processor       : 0
model name      : ARMv7 Processor rev 1 (v7l)
BogoMIPS        : 350.31
Features        : half thumb fastmult vfp edsp vfpv3 vfpv3d16 tls vfpv4
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x0
CPU part        : 0xc05
CPU revision    : 1

Hardware        : Atmel SAMA5
Revision        : 0000
Serial          : 0000000000000000
root@emblinux:/# 
```

Figure 21: Accessing the RMG/941C via Telnet client (TeraTerm)

6.13 Access via SSH

The OpenSSH server must be enabled via the SSV/WebUI (see **fig. 22**). Therefore choose from the menu **Services > remote access**, enable the checkbox in the line **Enable service** and click on **[Apply]**.

Please note:
It is mandatory to set a **password** before using SSH. Please refer to **chapter 6.4**.



Remote access configuration

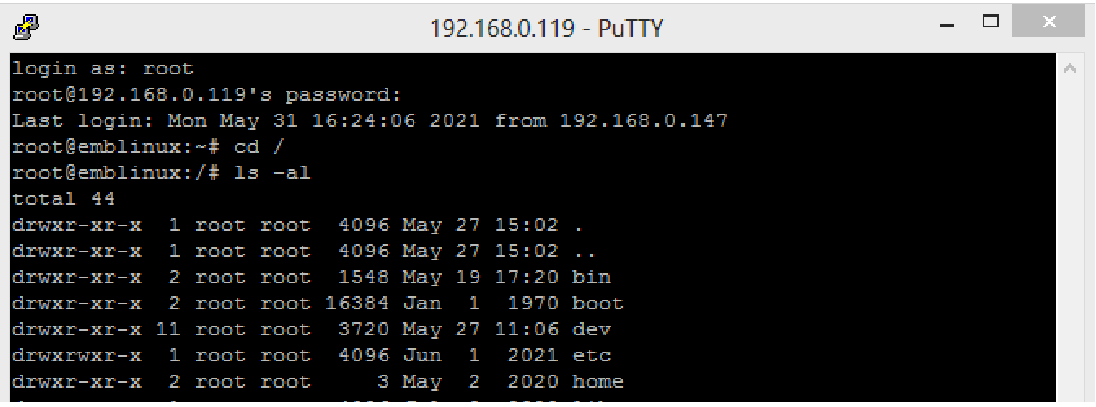
OpenSSH configuration		
Enable service :	☑	Enable or disable OpenSSH service
Port :	22	Port to listen on
Key regeneration interval [sec] :	3600	Interval until the key will be regenerated
Permit root login :	☑	Allow or deny root to login
Permit empty passwords :	☐	Allow or deny empty user passwords
RSA key fingerprint :	SHA256:4PMDg2734dNcOn1MB2O54xa+F/nsmZpTeuk6HbdKX7s Recreate key	

Change password for user "root"		
New password :		Enter new password for 'root'
Confirm new password :		Confirm new password for 'root'

Figure 22: Enabling the OpenSSH server

To access the RMG/941C via OpenSSH open an SSH client program (like **TeraTerm or PuTTY**) on your host PC and enter the current IP address of the RMG/941C and **port 22** to start an SSH session.

In the upcoming SSH window you can enter your login data.



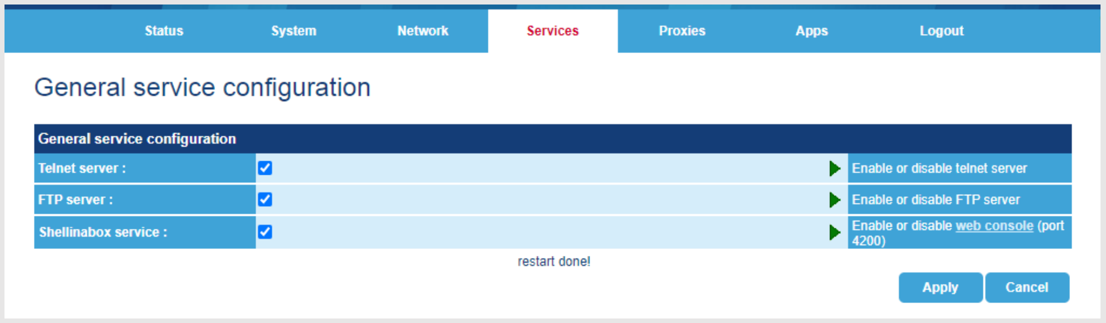
```
login as: root
root@192.168.0.119's password:
Last login: Mon May 31 16:24:06 2021 from 192.168.0.147
root@emblinux:~# cd /
root@emblinux:/# ls -al
total 44
drwxr-xr-x  1 root root  4096 May 27 15:02 .
drwxr-xr-x  1 root root  4096 May 27 15:02 ..
drwxr-xr-x  2 root root  1548 May 19 17:20 bin
drwxr-xr-x  2 root root 16384 Jan  1  1970 boot
drwxr-xr-x 11 root root  3720 May 27 11:06 dev
drwxrwxr-x  1 root root  4096 Jun  1  2021 etc
drwxr-xr-x  2 root root     3 May  2  2020 home
```

Figure 23: Accessing the RMG/941C via SSH client (PuTTY)

6.14 Access via FTP

The FTP server must be enabled via the SSV/WebUI (see **fig. 24**). Therefore choose from the menu **Services > General**, enable the checkbox in the line **FTP server** and click on **[Apply]**.

Please note:
It is mandatory to set a **password** before using FTP. Please refer to **chapter 6.4**.



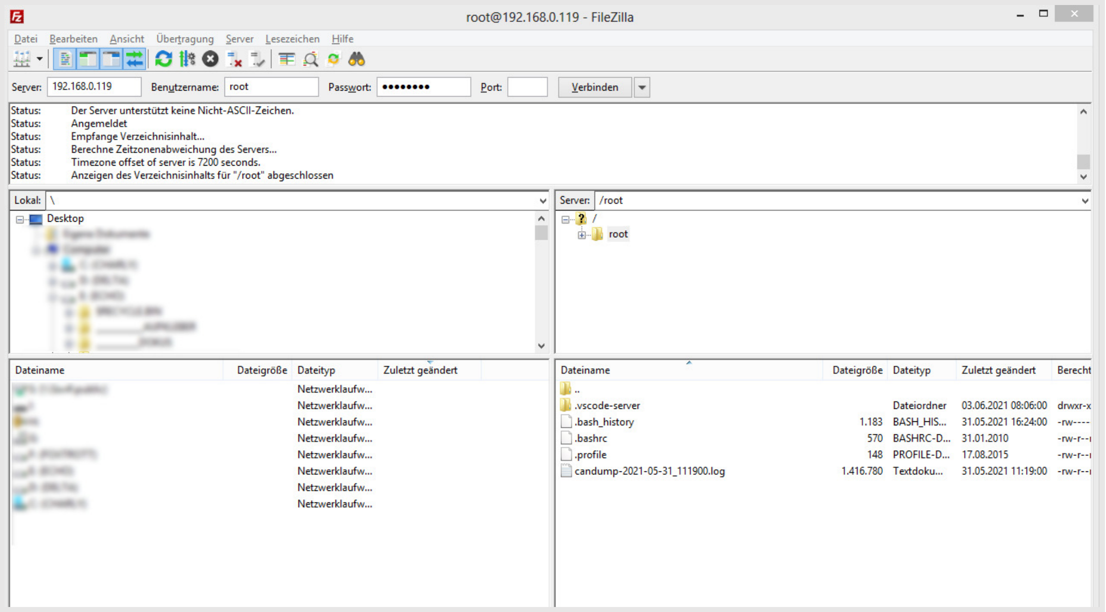
General service configuration

General service configuration		
Telnet server :	☑	Enable or disable telnet server
FTP server :	☑	Enable or disable FTP server
Shellinabox service :	☑	Enable or disable web console (port 4200)

restart done!

Figure 24: Enabling the FTP server

The RMG/941C comes with a pre-installed FTP server, which allows the file transfer via Ethernet between a PC and the RMG/941C. To access the RMG/941C via FTP use an FTP client like e.g. **FileZilla**.



Server: 192.168.0.119 Benutzername: root Passwort: •••••••• Port:

```
Status:     Der Server unterstützt keine Nicht-ASCII-Zeichen.
Status:     Angemeldet
Status:     Empfange Verzeichnisinhalt...
Status:     Berechne Zeitzonenabweichung des Servers...
Status:     Timezone offset of server is 7200 seconds.
Status:     Anzeigen des Verzeichnisinhalts für "/root" abgeschlossen
```

Lokal: \

Desktop [redacted]

Server: /root

/
root

Dateiname	Dateigröße	Dateityp	Zuletzt geändert
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	
[redacted]		Netzwerklaufw...	

Dateiname	Dateigröße	Dateityp	Zuletzt geändert	Berecht
..				
.vscode-server		Dateiordner	03.06.2021 08:06:00	drwxr-x
.bash_history	1.183	BASH_HIS...	31.05.2021 16:24:00	-rw----
.bashrc	570	BASHRC-D...	31.01.2010	-rw-r--r
.profile	148	PROFILE-D...	17.08.2015	-rw-r--r
candump-2021-05-31_111900.log	1.416.780	Textdoku...	31.05.2021 11:19:00	-rw-r--r

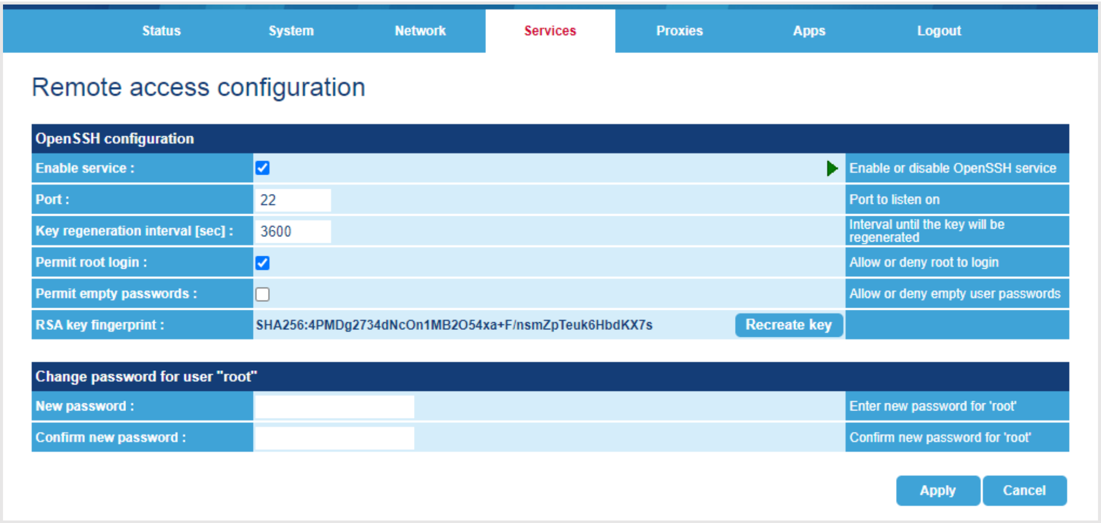
Figure 25: FileZilla as FTP client to access the FTP server

Use for the FTP login the **current IP address of the RMG/941C**.

6.15 Access via SFTP

The SFTP server is part of the OpenSSH server and must be enabled via the SSV/WebUI (see **fig. 26**). Therefore choose from the menu **Services > Remote access**, enable the checkbox in the line **Enable service** and click on **[Apply]**.

Please note:
It is mandatory to set a **password** before using SFTP. Please refer to **chapter 6.4**.



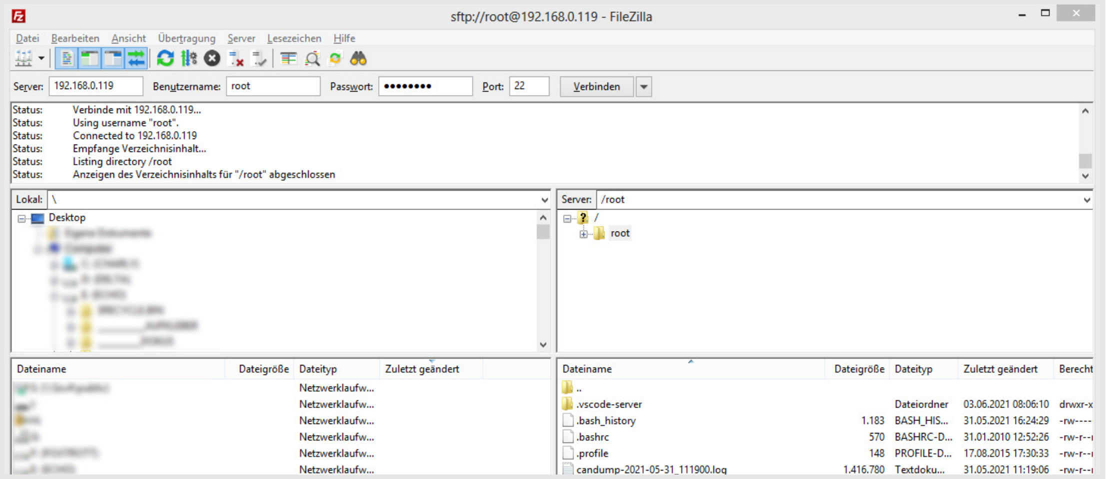
Remote access configuration

OpenSSH configuration		
Enable service :	☑	Enable or disable OpenSSH service
Port :	22	Port to listen on
Key regeneration interval [sec] :	3600	Interval until the key will be regenerated
Permit root login :	☑	Allow or deny root to login
Permit empty passwords :	☐	Allow or deny empty user passwords
RSA key fingerprint :	SHA256:4PMDg2734dNcOn1MB2O54xa+F/nsmZpTeuk6HbdKX7s	

Change password for user "root"		
New password :		Enter new password for 'root'
Confirm new password :		Confirm new password for 'root'

Figure 26: Enabling the OpenSSH server

The RMG/941C offers a pre-installed SFTP server (as part of the OpenSSH server), which allows file transfer via Ethernet between a PC and the RMG/941C. To access the RMG/941C via SFTP use an FTP client like e.g. **FileZilla**.



Server: 192.168.0.119 Benutzername: root Passwort: •••••••• Port: 22

```
Status:     Verbinde mit 192.168.0.119...
Status:     Using username "root".
Status:     Connected to 192.168.0.119
Status:     Empfange Verzeichnisinhalt...
Status:     Listing directory /root
Status:     Anzeigen des Verzeichnisinhalts für "/root" abgeschlossen
```

Lokal: \

Server: /root

Dateiname	Dateigröße	Dateityp	Zuletzt geändert
[illegible]		Netzwerklaufw...	
[illegible]		Netzwerklaufw...	
[illegible]		Netzwerklaufw...	
[illegible]		Netzwerklaufw...	
[illegible]		Netzwerklaufw...	
[illegible]		Netzwerklaufw...	

Dateiname	Dateigröße	Dateityp	Zuletzt geändert	Berecht
..				
.vscode-server		Dateiordner	03.06.2021 08:06:10	drwxr-x
.bash_history	1.183	BASH_HIS...	31.05.2021 16:24:29	-rw----
.bashrc	570	BASHRC-D...	31.01.2010 12:52:26	-rw-r--r
.profile	148	PROFILE-D...	17.08.2015 17:30:33	-rw-r--r
candump-2021-05-31_111900.log	1.416.780	Textdoku...	31.05.2021 11:19:06	-rw-r--r

Figure 27: FileZilla as FTP client to access the SFTP server

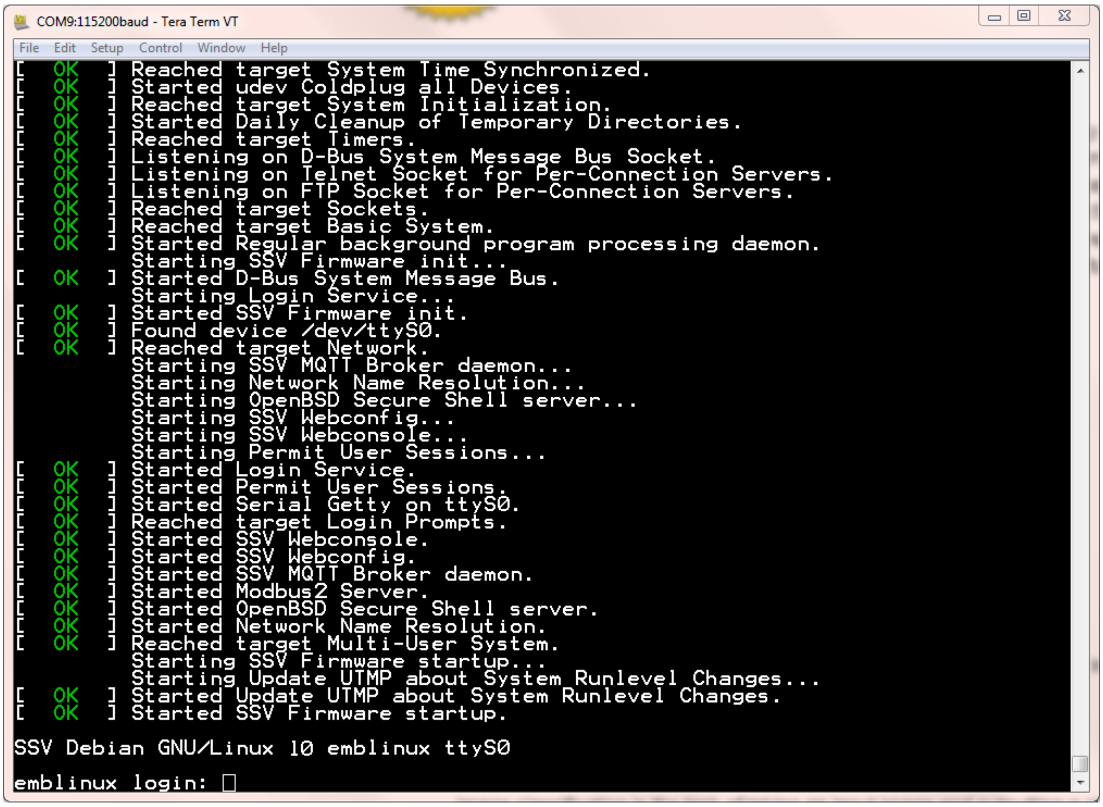
Use for the SFTP login the **current IP address of the RMG/941C and the port 22**.

6.16 Serial Console via COM1 (Service Port)

Over the serial port COM1 (service port) on the front panel of the RMG/941C a serial Linux console can be accessed.

Please note:
To create a connection between the RMG/941C and the PC an **adapter cable** and a **null modem cable** are necessary. Please refer to the **RMG/941C hardware reference** for more information.

It is mandatory to set a **password** before using the serial console. Please refer to **chapter 6.4**.


COM9:115200baud - Tera Term VT
File Edit Setup Control Window Help

```
[  OK  ] Reached target System Time Synchronized.
[  OK  ] Started udev Coldplug all Devices.
[  OK  ] Reached target System Initialization.
[  OK  ] Started Daily Cleanup of Temporary Directories.
[  OK  ] Reached target Timers.
[  OK  ] Listening on D-Bus System Message Bus Socket.
[  OK  ] Listening on Telnet Socket for Per-Connection Servers.
[  OK  ] Listening on FTP Socket for Per-Connection Servers.
[  OK  ] Reached target Sockets.
[  OK  ] Reached target Basic System.
[  OK  ] Started Regular background program processing daemon.
         Starting SSV Firmware init...
[  OK  ] Started D-Bus System Message Bus.
         Starting Login Service...
[  OK  ] Started SSV Firmware init.
[  OK  ] Found device /dev/ttyS0.
[  OK  ] Reached target Network.
         Starting SSV MQTT Broker daemon...
         Starting Network Name Resolution...
         Starting OpenBSD Secure Shell server...
         Starting SSV Webconfig...
         Starting SSV Webconsole...
         Starting Permit User Sessions...
[  OK  ] Started Login Service.
[  OK  ] Started Permit User Sessions.
[  OK  ] Started Serial Getty on ttyS0.
[  OK  ] Reached target Login Prompts.
[  OK  ] Started SSV Webconsole.
[  OK  ] Started SSV Webconfig.
[  OK  ] Started SSV MQTT Broker daemon.
[  OK  ] Started Modbus2 Server.
[  OK  ] Started OpenBSD Secure Shell server.
[  OK  ] Started Network Name Resolution.
[  OK  ] Reached target Multi-User System.
         Starting SSV Firmware startup...
         Starting Update UTMP about System Runlevel Changes...
[  OK  ] Started Update UTMP about System Runlevel Changes.
[  OK  ] Started SSV Firmware startup.

SSV Debian GNU/Linux 10 emblinux ttyS0

emblinux login: 
```

Figure 28: Serial Linux console in TeraTerm

7 INTERNET CONNECTION

The RMG/941C can access the Internet via an Ethernet LAN connection. For an **Internet connection via Ethernet LAN** please follow the instructions in **chapter 6.11**.

The RMG/941CL can additionally access the Internet via a mobile network (LTE) connection. For an **Internet connection via LTE** please follow the instructions in the **chapters 6.7 to 6.8**.

7.1 Internet for IoT Applications

The secure Internet connection for IoT applications is only established when required either via the LAN interface or via the mobile network (LTE), e.g. when an IoT application wants to send data via MQTT or HTTP request.

The RMG/941C(L) itself is virtually invisible on the Internet and cannot be reached by other applications from the outside.

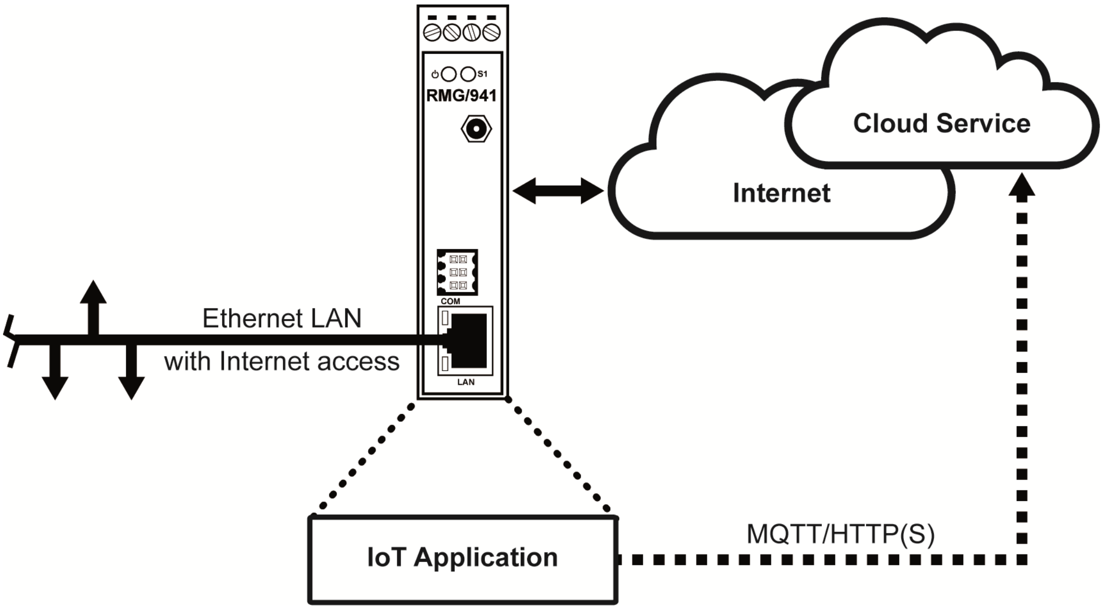


Figure 29: Example of an Internet connection for an IoT application

7.2 Internet via LTE Router

The RMG/941CL can be used as an **LTE router**, for example to transfer data from a LAN to another IP network, usually the Internet.

An RMG/941CL as LTE router thus enables local network devices to access the Internet and at the same time prevents access from the Internet to the local network by an internal firewall for security reasons.

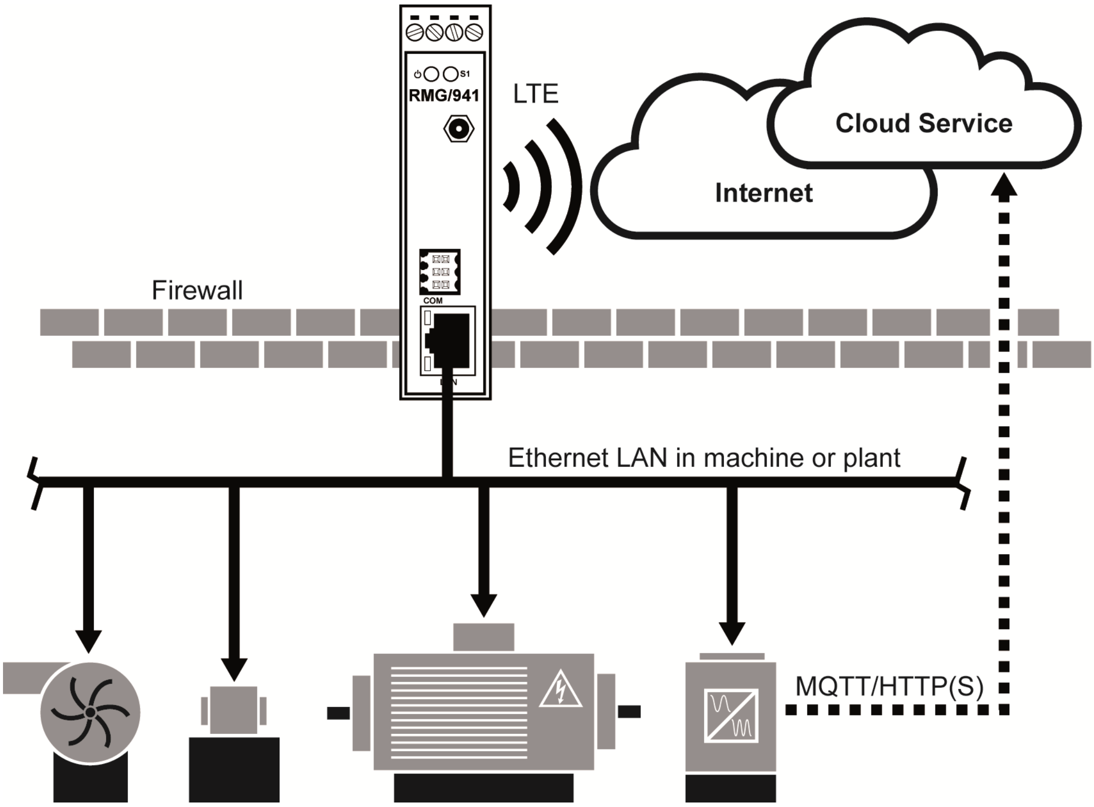


Figure 30: Example of using the RMG/941CL as an LTE router

To configure the RMG/941CL as an **LTE router** please follow the instructions in the **chapters 6.7 to 6.10**.

Please note:
If the RMG/941CL is operated as an LTE router it is highly recommended to enable the firewall (please refer to chapter 6.9)!

7.3 VPN Gateway

The RMG/941C can be used as a VPN (Virtual Private Network) gateway to enable secure access from a remote computer.

Therefore the RMG/941C uses the open source software from **OpenVPN.**

To setup your own VPN infrastructure you need the OpenVPN server and client software which can be obtained here: `https://openvpn.net`.

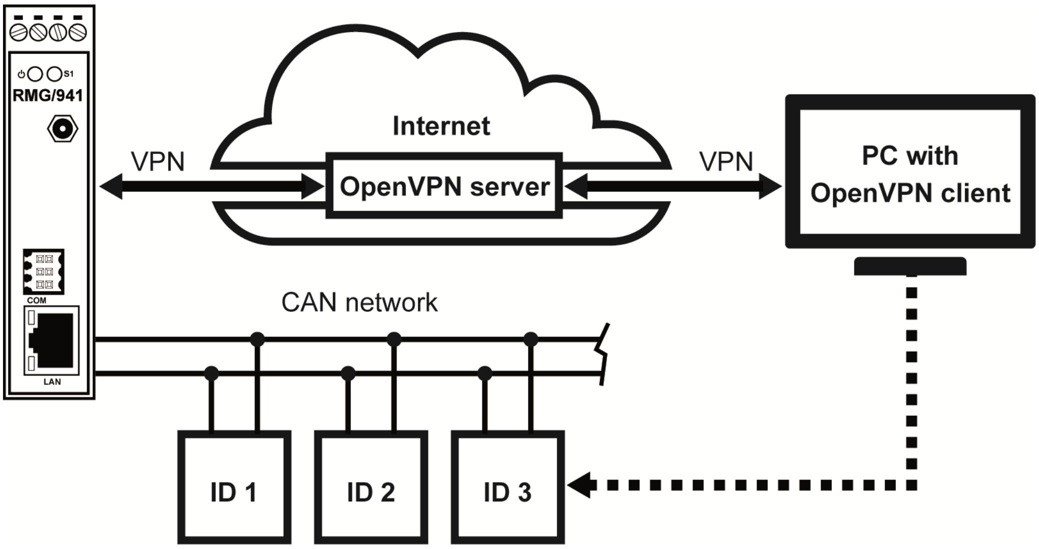


Figure 31: Example of a VPN connection

Please note:
Make sure that the RMG/941C uses the current time and date to avoid problems during the VPN configuration. We recommend using an NTP server instead of a manual setup, otherwise the RMG/941C cannot automatically reconnect to the VPN after an interruption of the power supply. Please refer to chapter 6.3!

To setup and configure a VPN choose from the menu **Services > OpenVPN.** Here you can configure each detail of a VPN like the protocol, firewall or authentication mode.

The RMG/941C can be connected with up to three different VPN's at the same time.

OpenVPN Server Docker Container for Evaluation

SSV offers a **ready-to-run Docker container with a preinstalled OpenVPN server** for evaluation purposes. All information about installation and resources can be found on GitHub:

`https://github.com/SSV-embedded/RMG-OpenVPN`

Please follow the instructions on GitHub to setup and run the OpenVPN Docker container and to create the VPN client configuration files.

IMPORTANT!
The proposed setup is NOT RECOMMENDED FOR PRODUCTION and shall be used for evaluation purposes only!
All required secrets are generated on the OpenVPN server Docker container and copied to all VPN clients. This implies that a security breach on the VPN server compromises all deployed secrets.

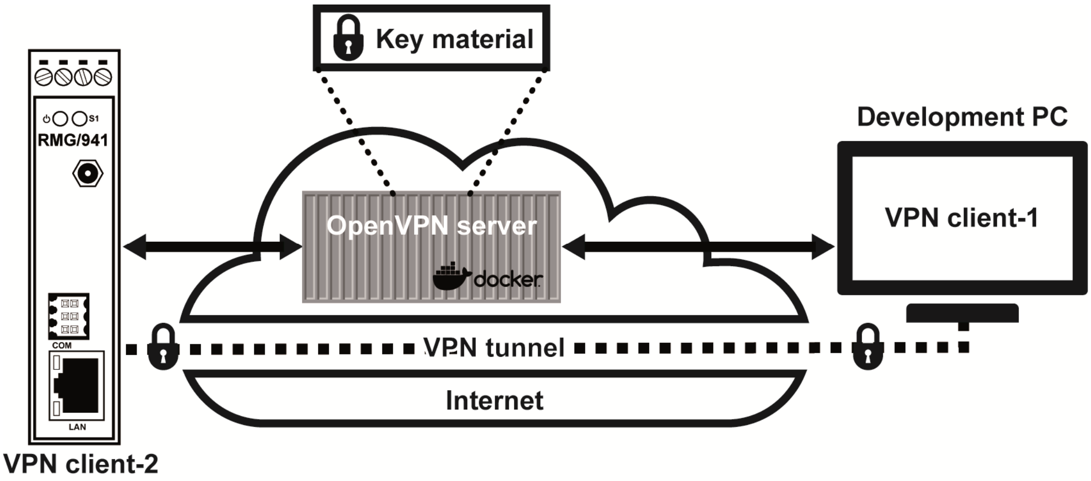


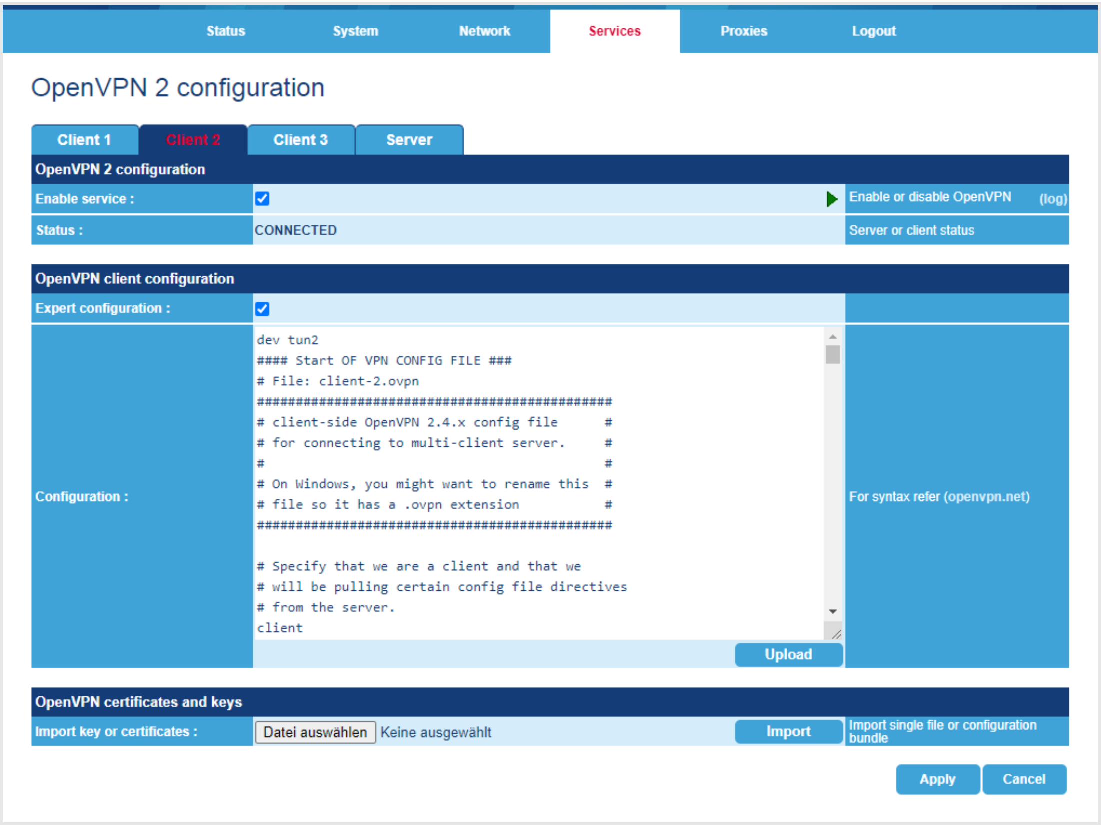
Figure 32: Schema of the OpenVPN evaluation setup

To import the VPN client configuration into the RMG/941C follow these steps:

1. Log into the SSV/WebUI and choose **Services > OpenVPN**.
2. Click on the tab **Client 2**.
3. Activate the checkbox **Enable service** and the checkbox **Expert configuration**.
4. Click on **[Apply]**.
5. Now mark all lines inside the text field **Configuration** (Ctrl-A) and paste the content of the VPN client configuration file **client-2.ovpn** into the text field.
6. Click on **[Upload]** to update the text field.
7. Click on **[Apply]**. This will start the VPN connection.
8. After a few seconds click on the tab **OpenVPN 2** to display the connection status in the line Enable service. It should now show a green arrow symbol.

Please do NOT click again on [Apply]! This would terminate the current VPN connection and start a new one.

To see some **VPN connection details** choose from the menu **System > Logging**.



OpenVPN 2 configuration

OpenVPN 2 configuration

Enable service :	☑	Enable or disable OpenVPN (log)
Status :	CONNECTED	Server or client status

OpenVPN client configuration

Expert configuration :	☑	
Configuration :	see below	For syntax refer (openvpn.net)

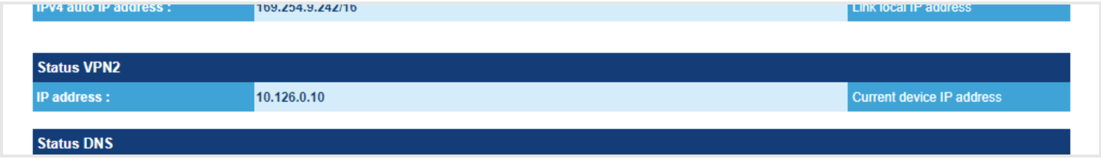
```
dev tun2
#### Start OF VPN CONFIG FILE ###
# File: client-2.ovpn
##############################################
# client-side OpenVPN 2.4.x config file      #
# for connecting to multi-client server.     #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
```

OpenVPN certificates and keys

Import key or certificates :	Datei auswählen Keine ausgewählt	Import single file or configuration bundle

Figure 33: Example of the OpenVPN settings

The **current VPN IP address** of the RMG/941C is shown on the **status page** in the section **Status VPN2**.



IPv4 auto IP address :	169.254.9.242/16	Link local IP address

Status VPN2

IP address :	10.126.0.10	Current device IP address

Status DNS

Figure 34: VPN IP address on the status page

When the RMG/941C as well as the development PC are connected with the OpenVPN server, you can **access the SSV/WebUI via VPN**.

Therefore enter the VPN IP address of the RMG/941C with the port number 7777 in your browser. For example:

```
http://10.126.0.10:7777
```

7.4 OTA Update Gateway

The RMG/941C can be used as a gateway for **automatic remote Over-the-Air (OTA) updates**, e.g. to update the firmware of CAN devices or machine learning models of smart sensors.

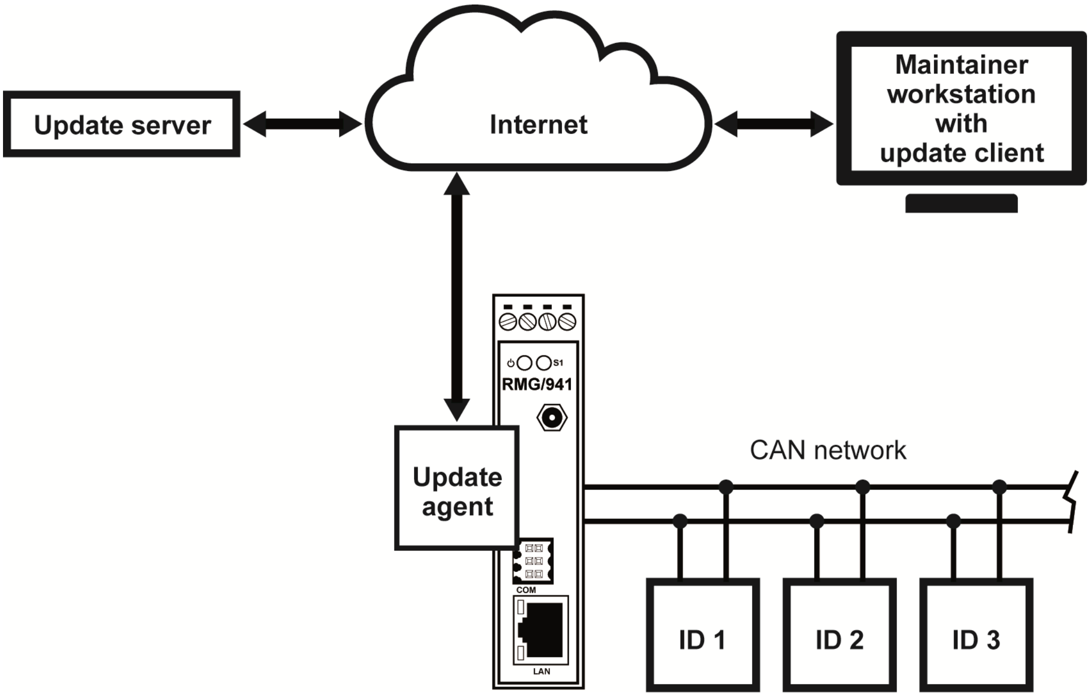


Figure 35: Schema of a simple OTA update infrastructure

The update file is edited on a **maintainer workstation** and then uploaded by **a maintainer update client** to a special **update server** on the Internet.

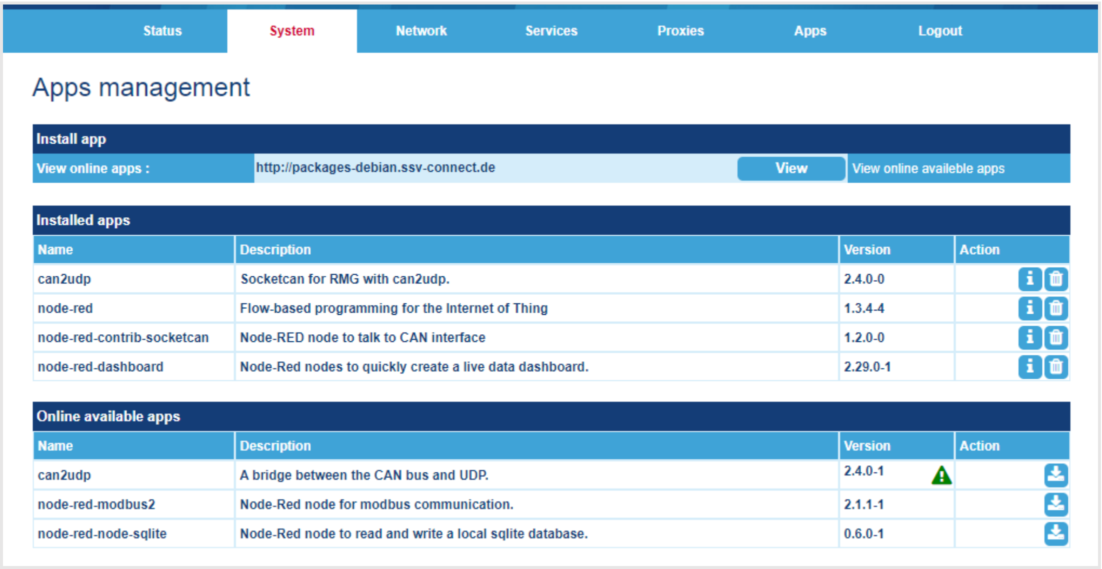
A special **update agent** runs on the RMG/941C, which regularly checks the update server, downloads the update file if it is newer than the current version, and transfers it to the individual target devices, e.g. via ISO-TP (ISO 15765-2).

To ensure the required cyber security of such an OTA solution, a **public key infrastructure** (PKI) with digital signatures and certificates is mandatory.

8 APPS

The functionality of the RMG/941C can be extended via apps.

To install/delete apps and to see a list of installed/available apps choose from the menu **System > Apps management.**



Apps management

Install app

View online apps : http://packages-debian.ssv-connect.de [View] View online availeble apps

Installed apps

Name	Description	Version	Action
can2udp	Socketcan for RMG with can2udp.	2.4.0-0	ℹ 🗑
node-red	Flow-based programming for the Internet of Thing	1.3.4-4	ℹ 🗑
node-red-contrib-socketcan	Node-RED node to talk to CAN interface	1.2.0-0	ℹ 🗑
node-red-dashboard	Node-Red nodes to quickly create a live data dashboard.	2.29.0-1	ℹ 🗑

Online available apps

Name	Description	Version	Action
can2udp	A bridge between the CAN bus and UDP.	2.4.0-1 ⚠	⬇
node-red-modbus2	Node-Red node for modbus communication.	2.1.1-1	⬇
node-red-node-sqlite	Node-Red node to read and write a local sqlite database.	0.6.0-1	⬇

Figure 36: Apps management

The list of all installed apps is displayed in the section **Installed apps**.

To delete an app click on this icon 🗑 on the right side.

Installing an App

First display the list of all available apps by clicking in the section **Install app** on **[View]**.

The app list will then be displayed at the bottom of the page in the section **Online available apps**.

This green icon ⚠ displayed next to the version number means that it is a newer version of an already installed app.

To install an app click on this icon ⬇ on the right side. The installation may take a while.

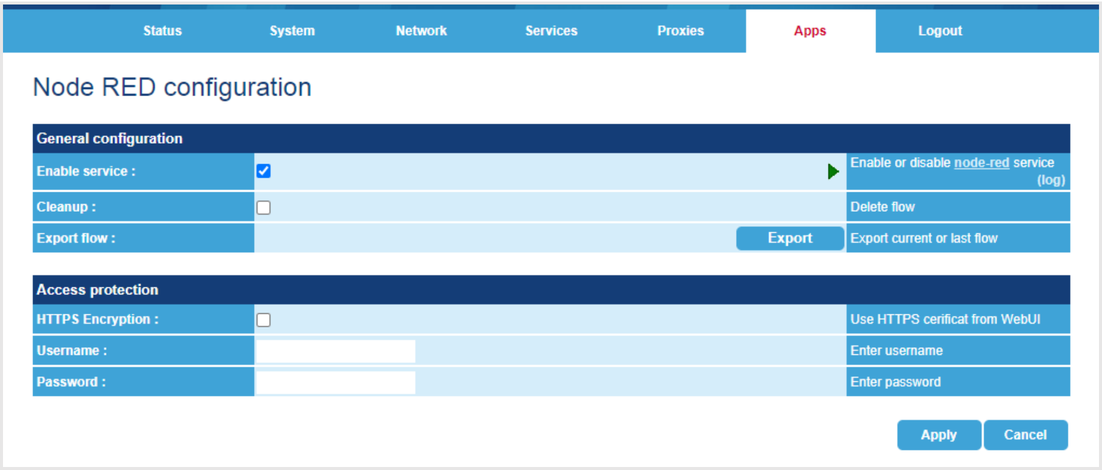
Apps on GitHub

You will find a list of all available apps with a short description on GitHub:

`https://github.com/SSV-embedded/RMG-Apps`

8.1 Node-RED

To configure the Node-RED app choose from the menu **Apps > Node-RED.**



Node RED configuration

General configuration			
Enable service :	☑	▶	Enable or disable node-red service (log)
Cleanup :	□		Delete flow
Export flow :		Export	Export current or last flow

Access protection		
HTTPS Encryption :	□	Use HTTPS cerificat from WebUI
Username :		Enter username
Password :		Enter password

Apply Cancel

Figure 37: Node-RED settings

Follow these steps to open the Node-RED workspace:

1. In the section **General configuration** enable the check box **Enable service**.

2. Click on **[Apply]**.

3. In the line **Enable service** click on the link **Node-RED** on the right side and the NodeRED workspace will open in a new browser tab. Alternatively you can enter the RMG/941C's IP address with port number 1880 (e.g. `192.168.0.126:1880`) in the address bar of the browser to open the workspace.

   If Node-RED asks for username and password, please use the same as for the SSV/WebUI. Both username and password can be found on the **nameplate** of the RMG/941C.

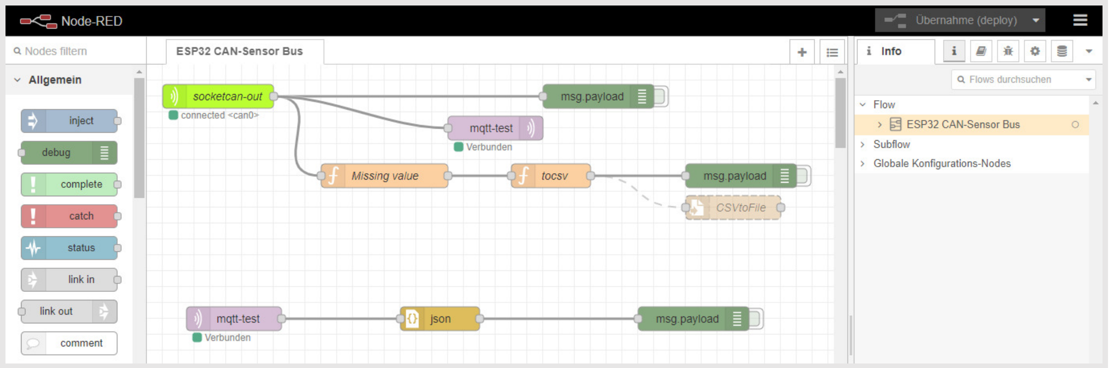


Figure 38: Example of the Node-RED workspace with some flows

Please note:
The Node-RED flows are saved in the directory `/media/data/node-red/`.

The Node-RED **palette manager** is disabled.

More information about Node-RED can be found here:

```
https://nodered.org
https://nodered.org/docs/tutorials/first-flow
```

There is also an official Node-RED YouTube channel with many video tutorials:

```
https://www.youtube.com/channel/UCQaB8NXBEPod7Ab8PPCLLAA
```

8.2 Node-RED Dashboard

The Node-RED dashboard app provides a set of nodes to quickly create a live data dashboard.

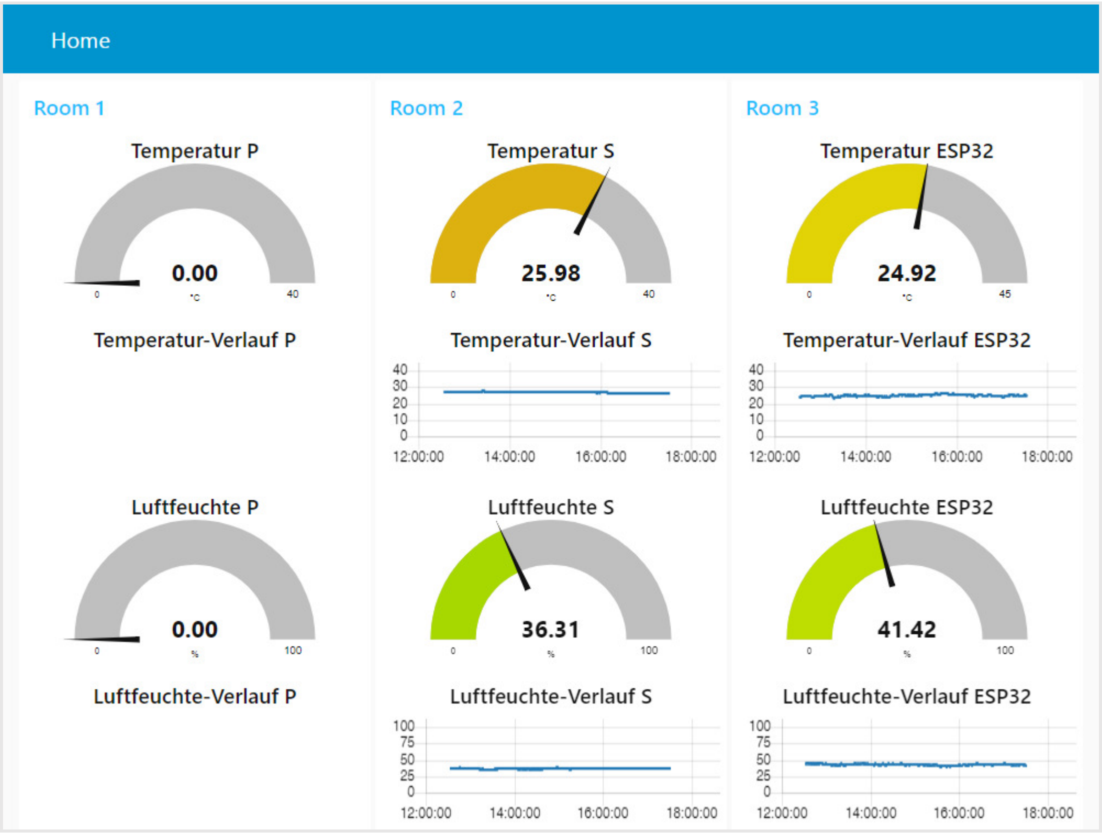


Figure 39: Example of a Node-RED live data dashboard

More information about creating a live data dashboard with Node-RED can be found here:

`https://flows.nodered.org/node/node-red-dashboard`

9 CREATING A CAN-OVER-IP BRIDGE

To connect two CAN devices via an IP network **two RMG/941C's are required**.

Figure 40 shows two setups for such a CAN-over-IP bridge:

- Directly with an Ethernet crossover cable or
- with two standard Ethernet patch cables over a hub or switch.

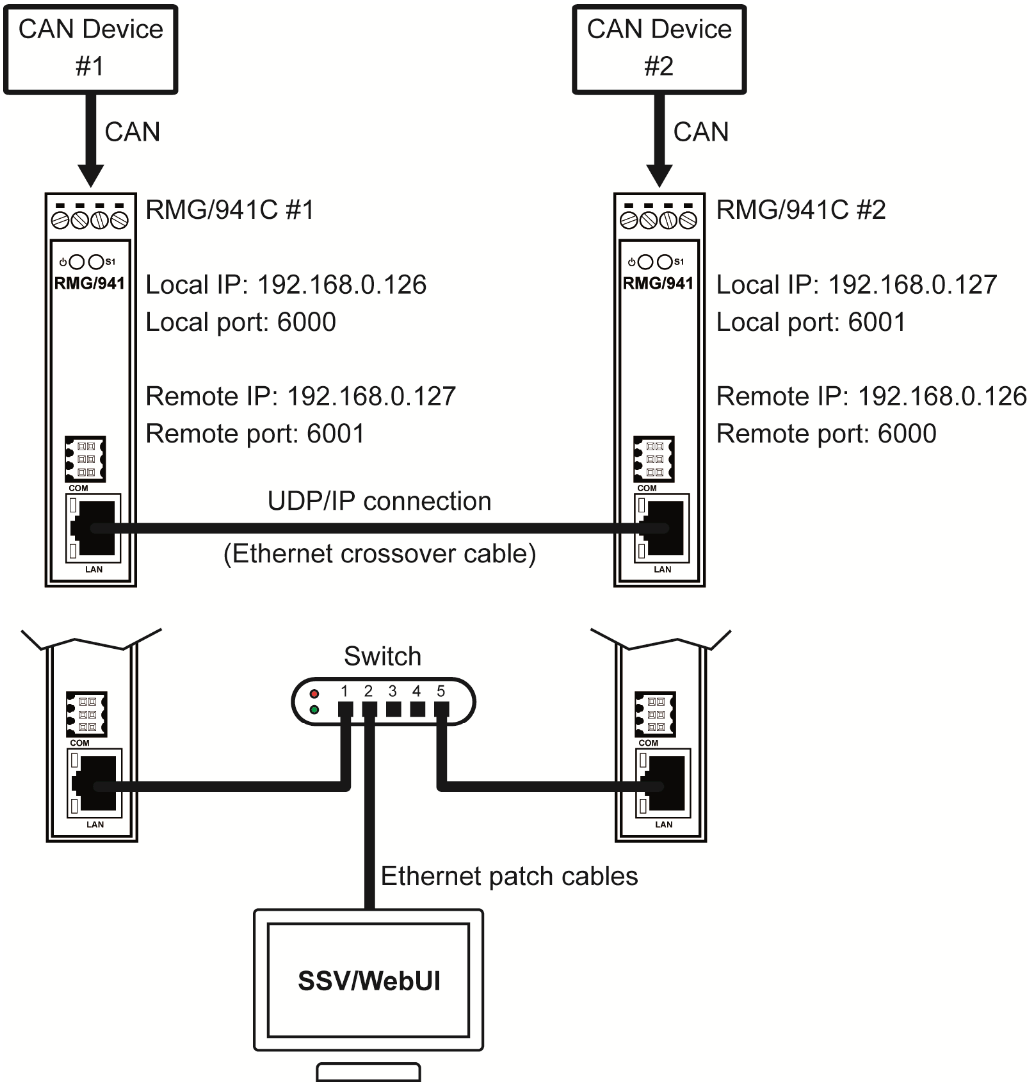
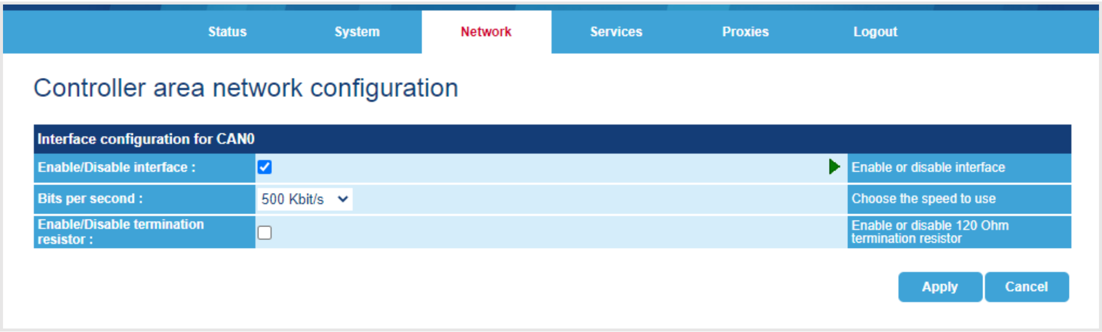


Figure 40: CAN-over-IP bridge setups

Please note:
Before establishing a CAN bridge make sure that the app **can2udp** (**see chapter 7**) is installed on each RMG/941C. Then both RMG/941C's must be configured like described in the following chapters.

9.1 Configuring the CAN Interface

Choose from the menu **Network > CAN.**



Controller area network configuration

Interface configuration for CAN0		
Enable/Disable interface :	☑	Enable or disable interface
Bits per second :	500 Kbit/s	Choose the speed to use
Enable/Disable termination resistor :	☐	Enable or disable 120 Ohm termination resistor

Figure 41: CAN interface settings

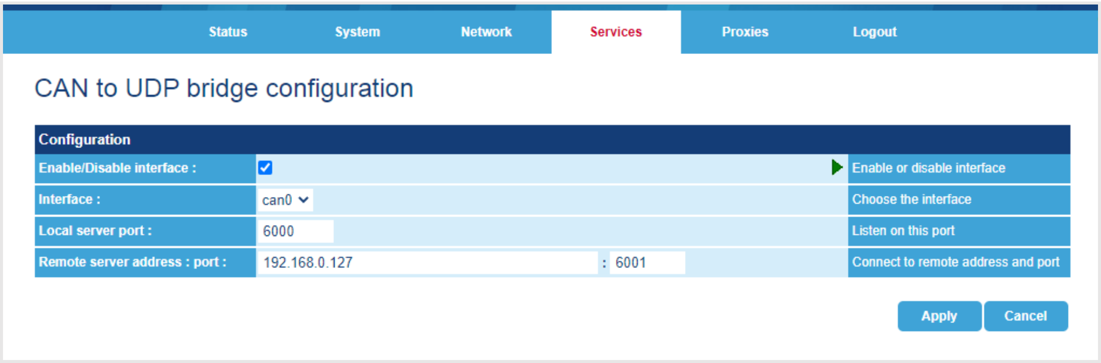
Follow these steps **on both RMG/941C's** to configure the CAN interface:

1. Click the check box to **enable the CAN interface**.
2. Choose the desired **connection speed*** from the dropdown menu.
3. Click the checkbox to enable the **CAN termination resistor** if needed.
4. Click on **[Apply]**.

***Please note:**
Make sure that you know the connection speed of your CAN devices and set it on both RMG/941C's.

9.2 Configuring the CAN to UDP Service

Choose from the menu **Services > CAN to UDP**.



CAN to UDP bridge configuration

Configuration		
Enable/Disable interface :	☑	Enable or disable interface
Interface :	can0	Choose the interface
Local server port :	6000	Listen on this port
Remote server address : port :	192.168.0.127 : 6001	Connect to remote address and port

Figure 42: CAN to UDP settings for RMG/941C #1

Follow these steps **on both RMG/941C's** to configure the CAN to UDP service:

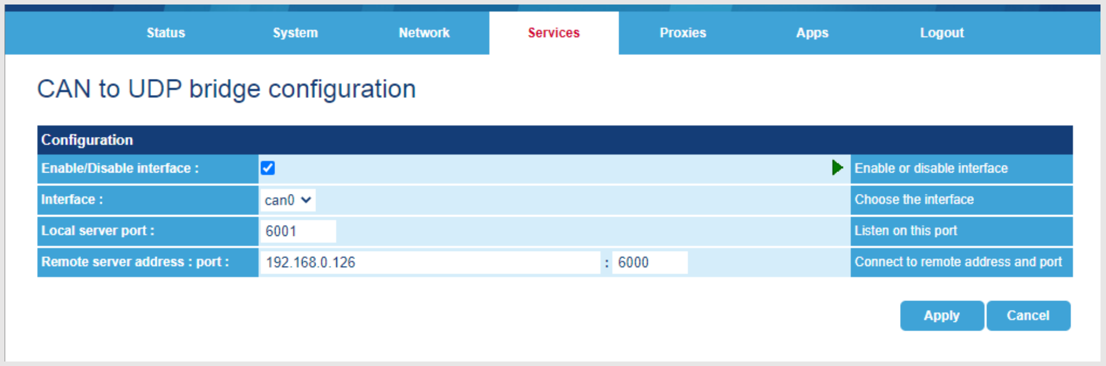
1. Click the check box to **enable CAN to UDP**.

2. Enter the local server port*.

3. Enter the **remote server IP address and port*** (this is the second/remote RMG/941C).

4. Click on **[Apply]**.

***Please note:**
Make sure to choose different UDP ports on each RMG/941C, otherwise the connection won't work. **Figure 42** shows the CAN to UDP settings for the first RMG/941C and **fig. 43** shows the settings for the second RMG/941C.



CAN to UDP bridge configuration

Configuration		
Enable/Disable interface :	☑	Enable or disable interface
Interface :	can0	Choose the interface
Local server port :	6001	Listen on this port
Remote server address : port :	192.168.0.126 : 6000	Connect to remote address and port

Figure 43: CAN to UDP settings for RMG/941C #2

10 TECHNICAL DATA

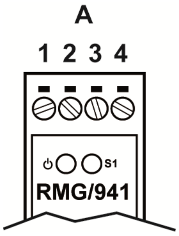
Supply voltage	12 .. 24 VDC ±10%
Weight	< 150 g
Mechanical Dimensions (LxWxH)	112 mm x 22.5 mm x 100 mm
Temperature range	0° C .. 60° C
Rel. air himudity	max. 85%

11 PINOUT SCREW TERMINALS

Table 5 shows the pinout of the screw terminals of the RMG/941C.

Terminal	Signal
A1	CAN Low
A2	CAN High
A3	Vin (12 .. 24 VDC ±10%)
A4	Power Ground

Table 4: Pinout of the screw terminals



12 HELPFUL LITERATURE

- RMG/941C hardware reference manual
- DNP/9535 hardware reference manual

CONTACT

SSV Software Systems GmbH
Dünenweg 5
D-30419 Hannover

Phone: +49 (0)511/40 000-0
Fax: +49 (0)511/40 000-40
Email: `info@ssv-embedded.de`

Website: `www.ssv-embedded.de`
Forum: `www.ssv-comm.de/forum`
Wiki: `mewi.ssv-embedded.de`
GitHub: `www.github.com/SSV-embedded`
LinkedIn: `www.linkedin.com/company/ssv-software-systems`

DOCUMENT HISTORY

Revision	Date	Remarks	Name	Review
1.0	2021-07-26	First version	WBU	ENE
1.1	2021-07-28	Added recommendation to use an NTP server in information box in chapter 7.3.	WBU	ENE
1.2	2022-01-27	Added note on username and password in chapter 6.2 and 8.1	WBU	ENE

The content of this document can change any time without announcement. There is taken over no guarantee for the accuracy of the statements. The user assumes the entire risk as to the accuracy and the use of this document. Information in this document is provided 'as is' without warranty of any kind. Some names within this document can be trademarks of their respective holders.