

LTE CPE B2368

User Manual

Date 03/31/2018

HUAWEI TECHNOLOGIES CO., LTD.



Copyright © Huawei Technologies Co., Ltd. 2018. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without the prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other symbols and inscriptions Huawei are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective owners.

Note

Purchased products, services and features are based on contracts between Huawei and the customer. No products or parts, services or features discussed in this document may not be within the scope of the purchased product or method of use. Unless otherwise specified in the contract, all data, information, and recommendations in this document are provided as are given without warranty or representation of any kind, whether express or implied. The information contained in this document is subject to change without notice. To ensure accuracy of content every effort was made. Any statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian,
Longgang Shenzhen 518129
People's Republic

Website: <http://www.huawei.com>

E-mail: support@huawei.com

About this document

Purpose

Equipment means LTE (Long Term Evolution) modem. Acronym ODU expresses the outdoor unit, while acronym IDU indoor unit. The LTE modem is a complete security solution simultaneously containing reliable firewall operating on the principle stateful packet inspection (SPI) and denial of service (Denial of Service, DoS).

Content

About this document	ii
Content	1
1.1 Use LTE modem	6
1.1.1 Internet access	6
1.1.2 VoIP telephony	6
1.1.3 Wireless	7
1.2 WLAN Button	7
1.3 Methods for Administration LTE modem	8
1.4 Tips for maintaining and managing the LTE modem	8
1.5 Parts of equipment	9
1.5.1 Outdoor unit	9
1.5.2 Indoor unit	10
1.5.3 RESET button	12
2 Introduction to Web configuration interface	13
2.1 Overview	13
2.1.1 For the basic settings	13
2.1.2 Access to Web configuration interface	16
2.2 Layout configuration interface	17
2.2.1 Top Panel	18
2.2.2 Main window	18
2.2.3 User account	18
2.2.4 Navigation Panel	18
3 connection status and system information	19
3.1 Overview	19
3.2 Status Screen Connection	19
3.3 Display Information System	20
4 Broadband	27
4.1 Overview	27
Screen 4.2 Broadband	27
4.2.1 Edit WAN interfaces	28
4.3 Screen SIM	30

4.3.1 Screen Blocked	31
5 Wireless WiFi 2.4 / 5 GHz	33
5.1 Overview	33
5.1.1 Wireless Network Topology	33
5.1.2 Before	35
5.2 General screen	35
5.2.1 Higher Security (WPA (2) PSK)	40
5.3 Screen More AP	41
5.3.1 Editing multiple AP	42
5.4 WPS screen	44
5.5 Technical details	45
5.5.1 Overview of wireless security	45
5.5.2 Problems with the signal	48
5.5.3 BSS	48
5.5.4 MBSSID	48
5.5.5 Connecting using WiFi Protected Setup (WPS)	49
6 Setting up a home network	54
6.1 Overview	54
6.1.1 What You Need to Know	54
6.2 LAN Settings screen	55
6.3 Static DHCP screen	58
6.3.1 Before	58
6.4 UPnP screen	60
6.5 Screen UPnP list	60
Static routing 7	62
7.1 Overview	62
7.2 Configuration of static routing	63
7.2.1 Add / Edit Static Routing	64
8 Network Address Translation (NAT)	66
8.1 Overview	66
8.1.1 What You Need to Know	66
8.2 Screen Port Forwarding	67
Screen Port Forwarding 8.2.1	67
8.2.2 Screen Edit port forwarding	69
8.3 DMZ screen	70
8.4 Screen connection	71
ALG Screen 8.5	72
8.6 Technical details	72
8.6.1 Basic definitions NAT	73
8.6.2 What happens during NAT	73

8.6.3 How NAT Works	73
9 Dynamic DNS	75
9.1 Overview	75
9.1.1 What You Need to Know	75
9.2 Dynamic DNS Screen	75
Firewall 10	76
10.1 Overview	76
10.1.1 What You Need to Know	77
Screen 10.2 General	77
10.3 Screen Services	78
10.3.1 Screen Add a new maintenance item	79
Screen Access Control 10.4	80
10.4.1 Screen Add New / Edit ACL rule	82
10.5 Screen DoS	84
10.6 Technical details about firewall	84
10.6.1 Tips to strengthen security firewall	85
10.6.2 Other safety tips	85
11 MAC address filter	86
11.1 Overview	86
11.1.1 What You Need to Know	86
11.2 Screen MAC address filter	86
12 Parental	89
12.1 Overview	89
12.2 Screen Parental	89
12.2.1 Add New / Edit PCP	90
13 L2TP VPN	93
13.1 Overview	93
13.2 Settings screen	93
13.2.1 Screen Add new tunnel / tunnel Modification	94
..... 13.3 Screen Monitor	96
4.13 Configuration Example L2TP VPN tunnel layer 3	97
5.13 Configuration Example L2TP VPN tunnel Layer 2	98
GRE VPN	100
14.1 Overview	100
14.2 Settings screen	100
14.2.1 Screen Add new tunnel / tunnel Modification	101
3.14 Configuration Example GRE VPN tunnel Layer 2	103
4.14 Configuration Example GRE VPN tunnel layer 3	104
VoIP	106

15.1 Overview	106
15.1.1 What You Need to Know	107
15.1.2 Before	108
15.2 Screen Service Provider SIP	108
15.3 Screen SIP account	114
15.3.1 Configuring SIP account	115
15.4 Screen Region	118
Screen 15.5 Rules call	119
Technical details	121
15.6.1 VoIP	121
15.6.2 SIP	121
15.6.3 Quality of Service (QoS)	126
15.6.4 Overview of additional telephone services	126
16 Status LTE	131
16.1 Overview	131
System 17 logs	132
17.1 Overview	132
17.1.1 What You Need to Know	132
17.2 System Log Screen	133
17.3 Screen Recording calls	134
17.4 Screen History VoIP calls	135
User account	136
18.1 Overview	136
18.2 Screen User Account	136
19 System	138
19.1 Overview	138
19.1.1 What You Need to Know	138
The 19.2 screen	138
19.3 Screen encryption key	139
19.3.1 Common usage: Set of indoor and outdoor unit	140
19.3.2 A new outdoor unit and indoor unit original	141
19.3.3 A new indoor unit and outdoor unit original	141
Setting the time	143
20.1 Overview	143
20.2 Settings screen time	143
Setting logging	146
21.1 Overview	146
21.2 Settings screen logging	146
Upgrade software	148

22.1 Overview	148
22.2 Screen Upgrade software	148
23 Online Update	151
23.1 Overview	151
23.2 Screen Online Update	151
23.3 Types of online updates	153
23.4 online update process	154
24 Backup / Restore	162
24.1 Overview	162
Screen 24.2 Backup / Restore	162
25 reboot screen	165
26 Diagnosis	166
26.1 Overview	166
Screen 26.2 Ping / TraceRoute	166
27 Troubleshooting	168
27.1 Overview	168
27.2 Power, hardware connections, LED indicators	168
27.3 LTE modem configuration interface and log	168
27.4 Internet access	170
27.5 Wireless Internet access	170
27.6 Telephone calls and VoIP	171
27.7 UPnP	172
28 Privacy	173

Introduction

1.1 Use LTE modem

Below are some examples of appropriate use of the LTE modem.

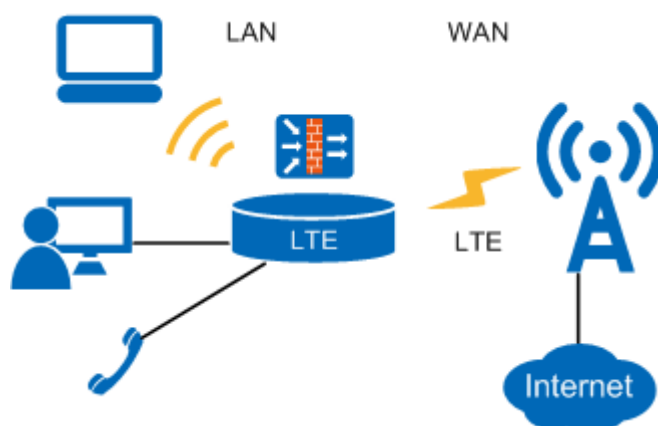
1.1.1 Internet access

Your LTE modem to access the Internet using a wireless connection to the LTE network. The LTE modem supports the following frequency bands of LTE networks. The use of a specific zone but usually decides Internet service provider (operator).

- B2368-22 B2368-66 models and supports LTE bands B38 / B40 / B41 / B42 / B43 / B1 / B3 / B7 / B8 / B20.
- B2368-57 model supports the LTE bands B40 / B41 / B42 / B4 / B7 / B28.

Figure 1-1 - computers can be connected directly to the port **ETHERNET LTE modem (or wirelessly via Wi-Fi).**

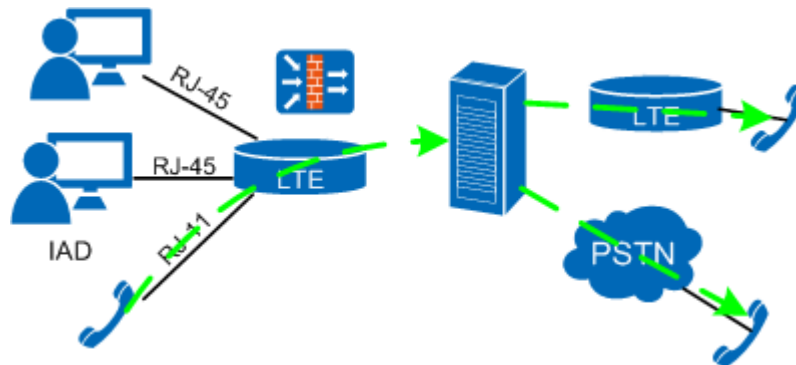
Figure 1-1 Diagram of Internet access via LTE modem



1.1.2 VoIP telephony

A single user account can be assigned to one profile SIP (Session Initiation Protocol) and use such LTE modem as a device for VoIP phone calls:

Figure 1-2 Wiring VoIP calls made using LTE modem

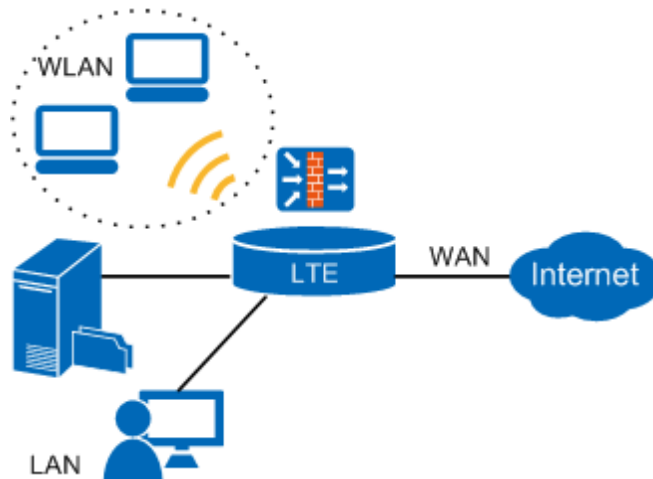


LTE modem sends your call to the SIP server VoIP service provider, where it is then forwarded to other VoIP device or telephone connected to the public switched telephone network (PSTN). For telephone support SIP and IAD on the home LAN is necessary to enable the SIP ALG this modem.

1.1.3 Wireless

By default, the WLAN broadcast LTE modem active. If a wireless network is active, the LTE modem to connect devices that support IEEE protocols 802.11b / g / n / ac and have access to network resources. You can configure the wireless network using WPS (Wi-Fi Protected Setup) or client device to manually add the network.

Figure 1-3 Diagram Wireless



1.2 WLAN Button

Press **WPS** on the back of the modem (internal unit) can wireless 2.4 GHz and 5 GHz bands on and off. The button can also be used to activate WPS, allowing you to quickly configure the wireless network with strong security.

Turning off the wireless LAN

Step 1 Make sure that the LED indicator **PWR / SYS** lights continuously.

step 2 Press and hold the WPS button for about one second. LED indicator **WLAN / WPS** with switch on or off depending on the status of the wireless network.

---- End

activation of WPS

Step 1 Make sure that the LED indicator **PWR / SYS** lights continuously.

step 2 Press and hold **WPS** at least five seconds. Press the WPS button on another devices supporting this technology, which is in range of the LTE modem. LED indicator **WLAN / WPS** LTE modem when connecting to another device via WPS flash.

---- End



NOTE

WPS function on LTE modem and the connected wireless devices must be activated within a time span of more than two minutes. For more information see 5.4 WPS screen.

1.3 Methods for Administration LTE modem

To manage LTE modem used a web interface which can be accessed by any (supported) web browser.

1.4 Tips for maintaining and managing the LTE modem

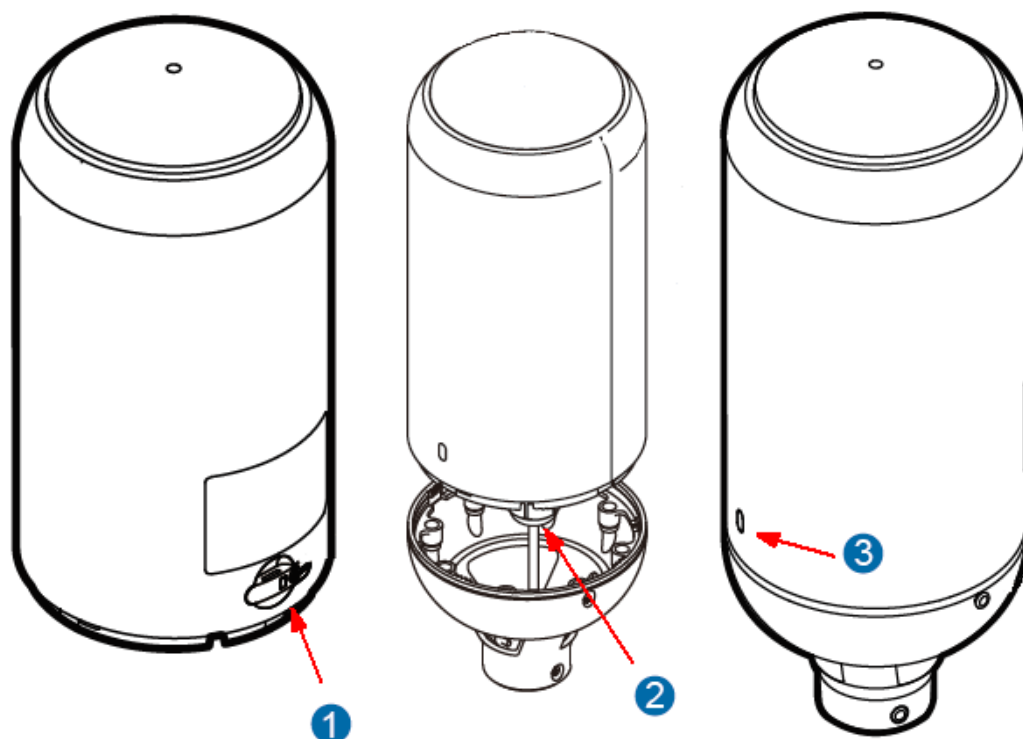
Regular exercise following to ensure maximum security and effective management LTE modem.

- **Change the default password.** Use a password that is not easily guessed, and which consists of various characters - eg. numbers and letters at the same time.
- Write down your password and store it in a safe place.
- Make a backup modem settings (and make sure you know how to restore the backup settings). Restoring from a backup modem configuration is especially useful in situations where the device becomes unstable or fault. If you forget the password to access the Web interface, you must restore the default settings LTE modem factory. If you made a backup of the settings in the configuration file, you will not have to repeat the entire setup LTE modem. Simply load the latest configuration file. Keep in mind, however, that the configuration file does not store account passwords VoIP telephony. Write down and keep safe all the information that you transmit your Internet Service Provider.

1.5 Product Components

1.5.1 Outdoor Unit

Figure 1-4 outdoor unit



First Terminal on the SIM card.

Second RJ-45 connector to connect the input connector PoE indoor unit.

Third LED.

Table 1-1 LED indicators outdoor unit

Color	Behavior	State
Off		The device is off
red	steady on	There is a fault / no jack in the SIM card
	Flashing	being updated
green	Flashing	is starting
	steady on	Powerful LTE Signal: SINR ≥ 10 db
blue	steady on	Moderate LTE signal: $10 \text{ db} > \text{SINR} \geq 4 \text{ db}$

Color	Behavior	State
Orange	steady on	Weak LTE signal: SINR <4 db
	Flashing	No LTE signal search or disconnected.

1.5.2 Indoor unit

The following picture is a diagram LED indicators and their labels.

Figure 1-5 The front panel of the indoor unit

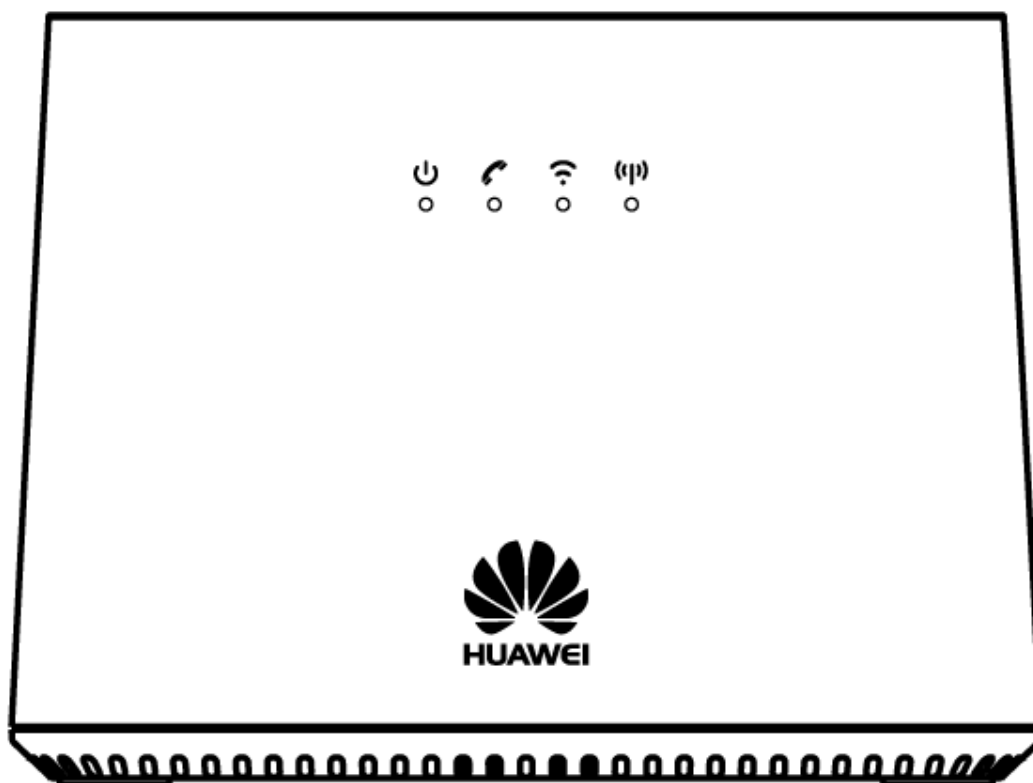
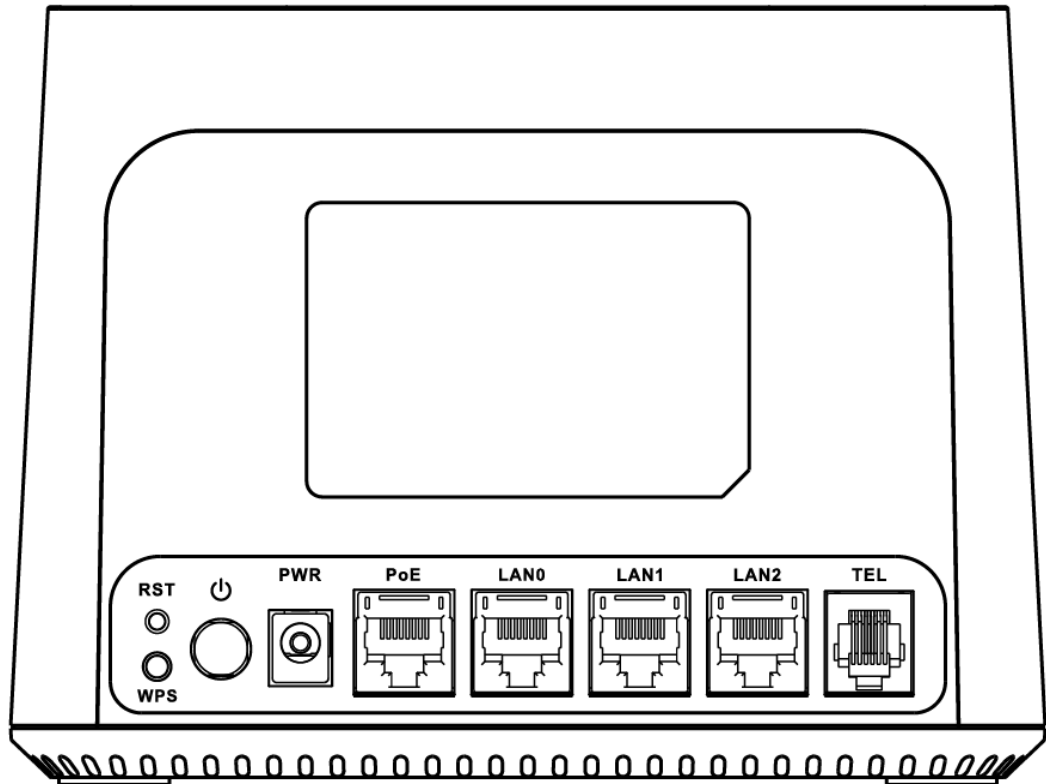




Figure 1-6 The rear panel of the indoor unit





NOTE

If there is no LTE modem plugged into the mains, will not light any LED.

Table 1-2 Description LED indicators of the indoor unit (left to right)

ICE	COLOR STATUS		Description
PWR / S YS 	green	Shines	LTE modem is connected to the network and ready for use.
		Flashing	Ongoing marketing LTE modem into operation.
	red	Shines	During the self-test fault has been detected / not inserted SIM card.
		Flashing	Firmware update is LTE modem.
Off			LTE modem is not connected to the mains.
PHONE 	Green	Shines	The telephone jack is assigned SIP account.
		Flashing	Phone connected to the socket has posted handset / device registered incoming call.
	Yellow	Shines	The telephone jack is assigned SIP account, which was delivered to the voice message.
		Flashing	The phone jack is connected to the phone and posted to the account SIP voice message was delivered.

ICE	COLOR STATUS		Description
	Off		The telephone jack is not assigned to any SIP account.
WPS / Wi-Fi 	green	Shines	Wireless IEEE 802.11ac 802.11bgn or is active.
		Flashing	LTE modem communicates with wireless client devices.
	Yellow	Flashing	Being configured connection via WPS.
	Off		The wireless network is turned off.
LTE Signal Strength 	green	Shines	Powerful LTE Signal: SINR ≥ 10 db
	blue	Shines	Moderate LTE signal: 10 db > SINR ≥ 4 db
	orange Lights		Weak LTE signal: SINR < 4 db
		Flashing	No LTE signal search or disconnected.
LAN 0 - 2	Yellow (Gigabit Ethernet above)	Shines	The LTE modem is successfully connected to the device via the LAN with a transfer at 1000 Mbps.
		Flashing	LTE device sends / receives data to / from the network at 1000 Mbps.
	Green (Fast Ethernet)	Shines	The LTE modem is successfully connected to the device via the LAN with a transfer rate of 10/100 Mbps.
		Flashing	LTE device sends / receives data to / from the network speed of 10/100 Mbps.
	Off		The LTE modem no device is connected via LAN.

More information about the physical device connection, see *Quick Start Guide*.

1.5.3 RESET button

To restart the device, simply press and hold **RESET** 3 - 10 seconds.

To restore the default factory equipment, make sure that the LED indicator **POWER** lights (flashing), then press and hold **RESET** more than 10 seconds.

If you forget the password to the Web-based interface, you can use the **RESET** on the back of the modem reset the default configuration file. This means that all settings will be lost and password for the web interface are reset to default.

2 Introduction to the web configuration interface

2.1 Overview

Web configuration tool is based on technology HTML, which allows easy device setup and management through a standard web browser. Your browser must support HTTPS security protocols and TLS1.2.

For this reason, the supported browsers include:

First Chrome 49.0 or higher

Second Firefox 45 and higher

Third Opera 36 and higher

4th Safari 10.1.2 and higher

5th Internet Explorer 11.0 and higher (on Windows 7 and later)

The recommended screen resolution is 1366 x 768 pixels.

In order to use configuration interface is needed to enable or activate the following:

- Popups internet browser you are using. By default browser in Windows 7 is active popup blocker.
- JavaScript (enabled by default).
- Permission to access Java applications (by default, granted).

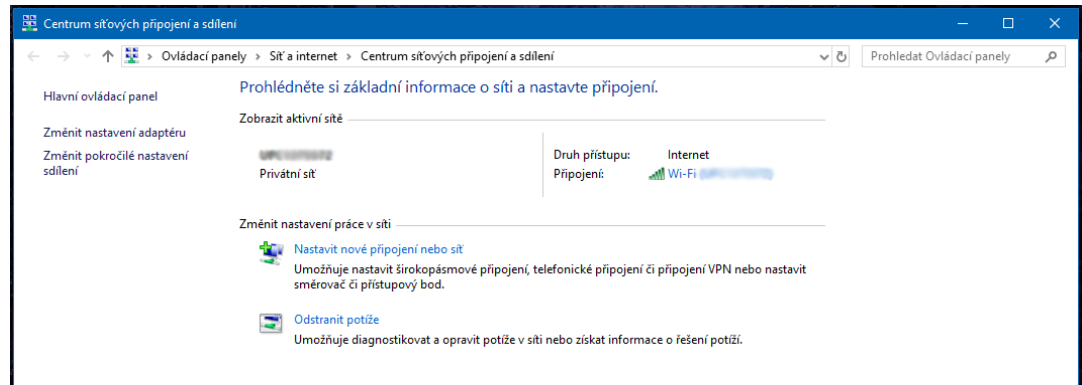
2.1.1 For the basic settings

Before you start using LTE modem, do the following.

Step 1 Go to Start> Control Panel> Network Center and Sharing.

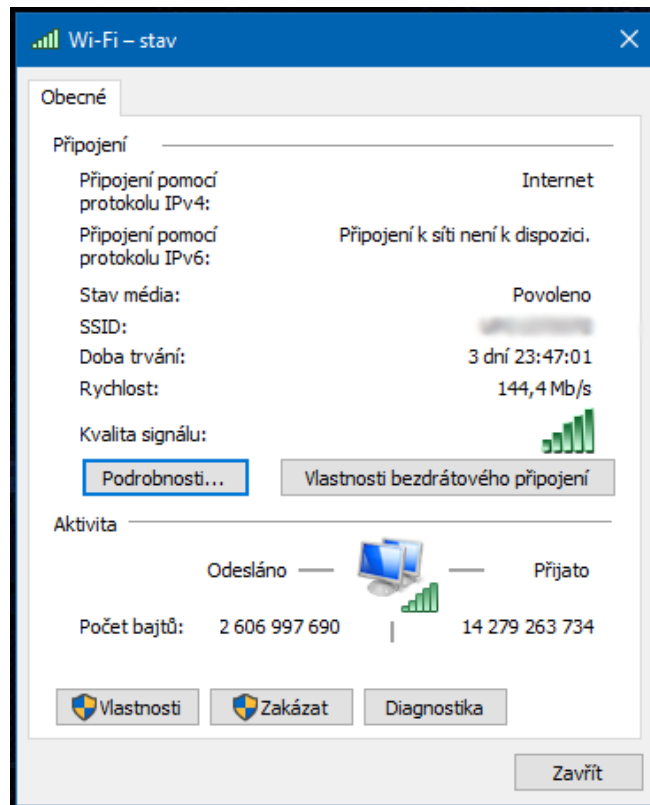
step 2 Click on the name of the network to which you have access.

Figure 2-1 Center Network and Sharing



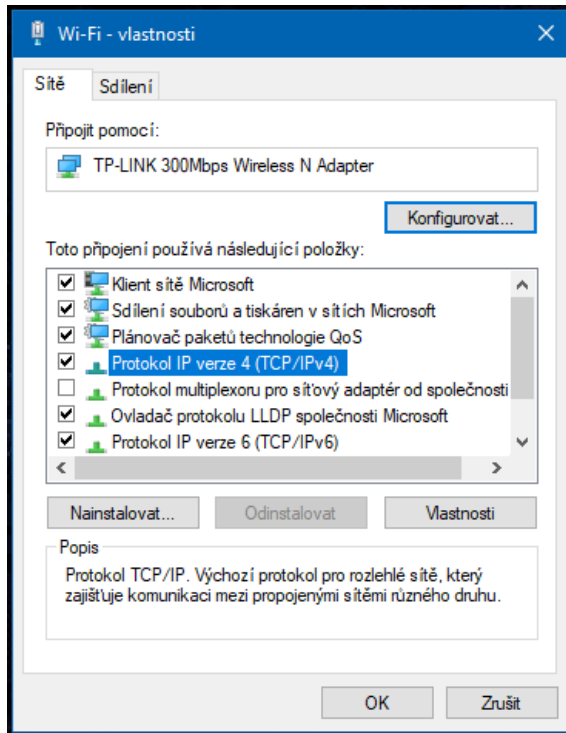
step 3 Click on **Properties**.

Figure 2-2 connection status



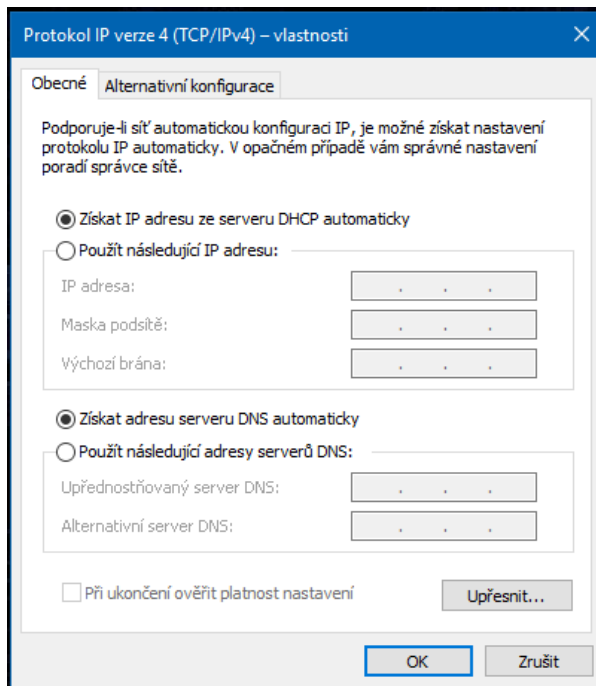
step 4 mouse to select **Internet Protocol Version 4 (TCP / IPv4)** and then click on **Properties**.

Figure 2-3 connection properties



step 5 Choose **Obtain an IP address from a DHCP server** and **Obtain DNS server address automatically** and click on **OK**. then **Close** and in the next window again **Close**.

Figure 2-4 Properties of Internet Protocol Version 4 (TCP / IPv4)



---- End

2.1.2 Access to the web-based configuration interface

Step 1 Ensure that all parts are properly connected LTE modem (for more information see Quick Start Guide).

step 2 Start your Internet browser.

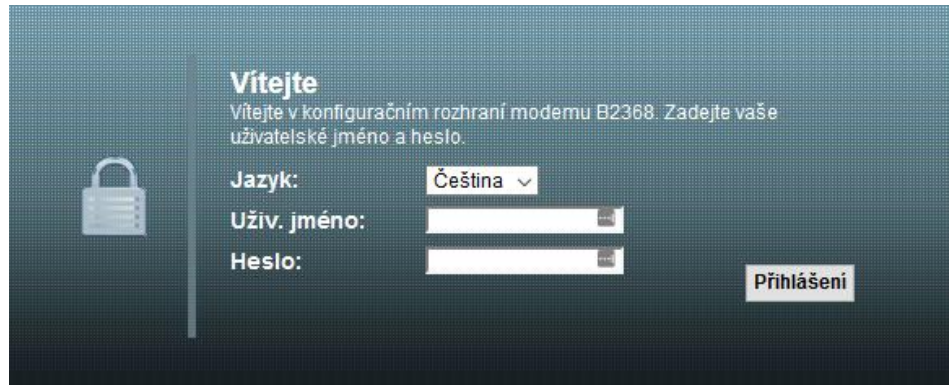
step 3 In the address bar, type " 192.168.1.1 ".

step 4 You will be prompted to enter a user name and password.

- If you want to enter the configuration interface to access user to enter a user name " user ". The password can be found on a label on the back of the modem.

Click on **Login**. If you have already changed the default password, then enter your chosen password and click **Login**.

Figure 2-5 Screen with password



The following screen appears when you enter the wrong password three times in a row.

Figure 2-6 Notification of blocked logging



NOTE

For security reasons, the configuration interface will automatically be logged off after five minutes of inactivity (by default). If this happens, simply log in again.

step 5 The following screen appears when you still did not change the default password.

We strongly recommend that you change the default password. Enter the new password, confirm it by entering it again and click on **Change**. If you do not want to change the password, you can select **Skip** and go directly to the main menu.

Figure 2-7 Screen prompting you to change your password



step 6 The default screen - **Connection status**.

Figure 2-8 connection status



step 7 Click on the link **System Information** go to the same screen that offers

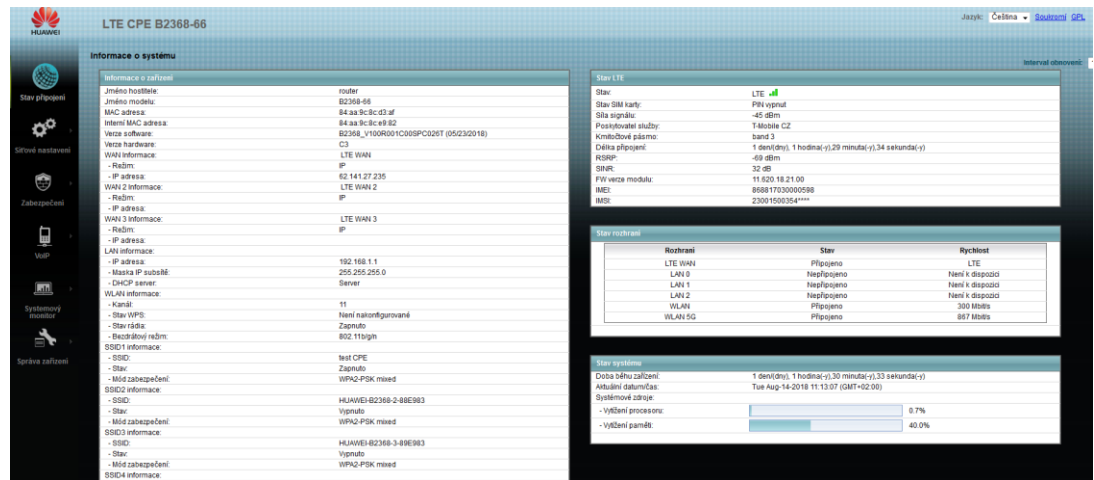
Technical data on the LTE modem and other system information.

---- End

2.2 Layout configuration interface

Click on **Connection Status> System Information** to display the following screen. (For more information see 3.3 Display Information System).

Figure 2-9 Layout configuration interface



As seen from the figures above, the main screen is divided into the following parts:

- upper panel
- main window
- navigation bar

2.2.1 Top Panel

On the top panel, a link to their privacy policy and information about the GPL (using open-source tools). Clicking on the logout icon in the upper right corner, you can log out of the configuration interface.



2.2.2 Main Window

In the main window, there is important information and a field for entering the setting values. Content main window dedicated the rest of this document.

After clicking on the button **System Information** on the screen **connection status** screen appears **Information about the system**. screen **System Information** is further discussed in Section 3.3 System Information screen.

If you click on **LAN equipment** on the screen **System Information (A in Figure 2-9)** screen displays **Connection status**. screen **connection status** is further discussed in section 3.2 Status Screen Connection.

2.2.3 User account

using the menu **Device Management > Manage Account** You can set passwords for each user account. For more information, see 18 user account.

2.2.4 Navigation Bar

The navigation pane contains individual parts of menus that allow you to set the relevant functions of an LTE modem.

3 Connection status and system information

3.1 Overview

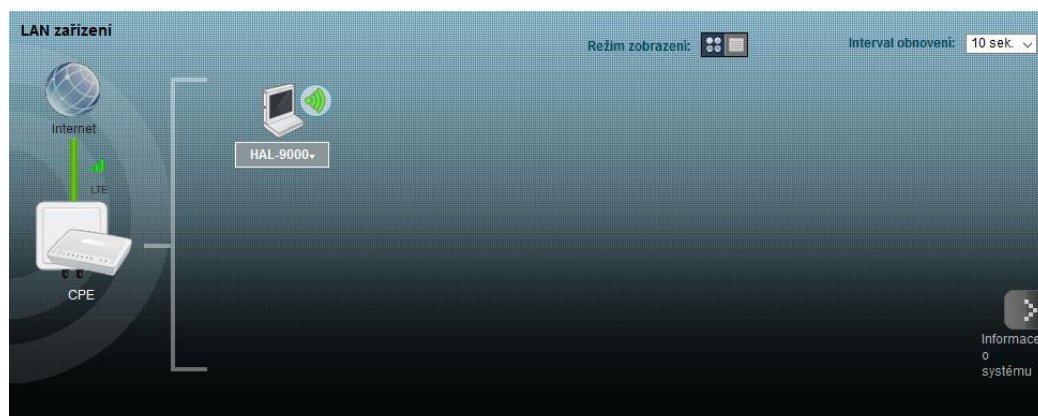
After logging into the web based configuration screen appears **Connection status**. On it displays the status of the network connection LTE modem and the client devices connected to it.

using the screen **System Information** You can look at the current status, use of system resources used interfaces (LAN, WAN and WLAN), and an overview of SIP accounts. You can also register and unregister individual SIP accounts.

3.2 Status Screen Connection

This screen provides an overview of network status information about the modem and the various connected devices. If there is a problem in the network connection is displayed on the screen warning message.

Figure 3-1 Connection status: Display Mode - icons




If you wish to connected devices appear in the list, click the button **List** in a field **Display Mode**. Use the drop-down menu **recovery interval** You can set how often you want to update this screen.

Figure 3-2 Connection status: Display Mode - list

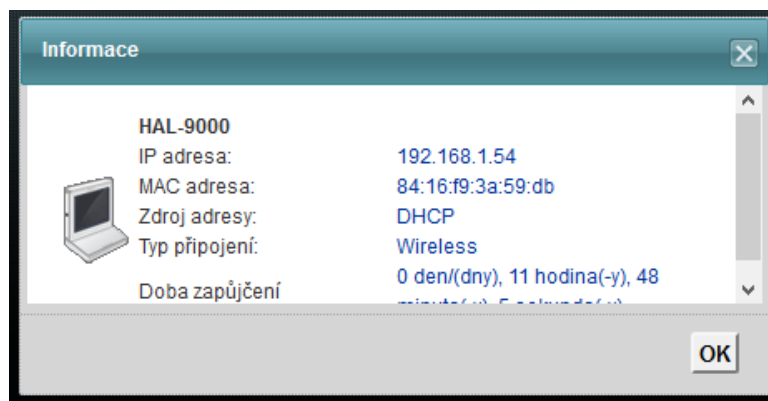


The screenshot shows a table titled "LAN zařízení" with columns for device ID, name, IP address, MAC address, source address, connection type, and connection time. A single device is listed with a laptop icon.

#	Název zařízení	IP adresa	MAC adresa	Zdroj adresy	Typ připojení	Doba zapůjčení
	HAL-9000	192.168.1.54	84:16:f9:3a:59:db	DHCP	Wireless	0 den/(dny), 11 hodina(-y), 48 minuta(-y), 47 sekunda(-y)

At **display mode - icons** You can see detailed information about the client device by clicking on its icon and then on the link **Information**.

Figure 3-3 Connection status: Display Mode - List> About



At **display mode - list** you'll see information about the client device directly.

3.3 Display Information System

Click on **Connection Status> System Information** for this screen.

Figure 3-4 Screen System Information

Informace o systému Interval obnovy: 10 sek. ▾

Informace o zařízení

Jméno hostitele: router
 Jméno modelu: B2368-22
 MAC adresa: 84:aa:9c:48:be:a5
 Interní MAC adresa: 84:aa:9c:47:7d:4d
 Verze software: B2368_V100R001C00SPC026T (05/23/2018)
 Verze hardware: C3
 WAN Informace: LTE WAN
 - Režim: IP
 - IP adresa: 100.79.13.61
 WAN 2 Informace: LTE WAN 2
 - Režim: IP
 - IP adresa:
 WAN 3 Informace: LTE WAN 3
 - Režim: IP
 - IP adresa:
 LAN informace:
 - IP adresa: 192.168.1.1
 - Maska IP sítě: 255.255.255.0
 - DHCP server: Server
 WLAN informace:
 - Kanál: 9
 - Stav WPS: Není nakonfigurované
 - Stav rádia: Zapnuto
 - Bezdrátový režim: 802.11b/g/n
 SSID1 informace:
 - SSID: HUAWEI-B2368-477D4E
 - Stav: Zapnuto
 - Mód zabezpečení: WPA2-PSK mixed
 SSID2 informace:
 - SSID: HUAWEI-B2368-2-407D4E
 - Stav: Vypnuto
 - Mód zabezpečení: WPA2-PSK mixed
 SSID3 informace:
 - SSID: HUAWEI-B2368-3-417D4E
 - Stav: Vypnuto
 - Mód zabezpečení: WPA2-PSK mixed
 SSID4 informace:
 - SSID: HUAWEI-B2368-4-427D4E
 - Stav: Vypnuto
 - Mód zabezpečení: WPA2-PSK mixed
 5 GHz WLAN informace:
 - Kanál: 153
 - Stav WPS: Není nakonfigurované
 - Stav rádia: Zapnuto
 - Bezdrátový režim: 802.11a/n/ac

Stav LTE

Stav: LTE
 Stav SIM karty: PIN vypnut
 Síla signálu: -59 dBm
 Poskytovatel služby: T-Mobile CZ
 Kmitočtové pásmo: band 3
 Délka připojení: 0 den/(dny), 0 hodina(-y), 6 minuta(-y), 13 sekunda (-y)
 RSRP: -83 dBm
 SINR: 21 dB
 FW verze modulu: 11.620.18.21.00
 IMEI: 355968053041660
 IMSI: 23001500509****

Stav rozhraní

Rozhraní	Stav	Rychlost
LTE WAN	Připojeno	LTE
LAN 0	Nepřipojeno	Není k dispozici
LAN 1	Nepřipojeno	Není k dispozici
LAN 2	Nepřipojeno	Není k dispozici
WLAN	Připojeno	300 Mbit/s
WLAN 5G	Připojeno	867 Mbit/s

Stav systému

Doba běhu zařízení: 0 den/(dny), 0 hodina(-y), 7 minuta(-y), 12 sekunda (-y)
 Aktuální datum/čas: Sun Jan-01-2017 08:06:56 (GMT+01:00)
 Systémové zdroje:
 - Vytížení procesoru: 0.5%
 - Vytížení paměti: 38.8%

5 GHz SSID1 informace:
 - SSID: HUAWEI-B2368-5G-477D4F
 - Stav: Zapnuto
 - Mód zabezpečení: WPA2-PSK mixed

5 GHz SSID2 informace:
 - SSID: HUAWEI-B2368-5G-2-407D4F
 - Stav: Vypnuto
 - Mód zabezpečení: WPA2-PSK mixed

5 GHz SSID3 informace:
 - SSID: HUAWEI-B2368-5G-3-417D4F
 - Stav: Vypnuto
 - Mód zabezpečení: WPA2-PSK mixed

5 GHz SSID4 informace:
 - SSID: HUAWEI-B2368-5G-4-427D4F
 - Stav: Vypnuto
 - Mód zabezpečení: WPA2-PSK mixed

Stav registrace

Účet	Akce	Stav účtu	URI
SIP 1	Registrovat	Nečinný	ChangeMe@ChangeMe

Individual fields are described in the following table.

Table 3-1 Screen System Information

Item	Description
recovery interval	Select how often you wish to update the information on this screen by using the drop-down menu.
Device Information	
hostname	This field shows the system name LTE modem. Used for identification. The name can be changed through the menu Device Management> System and field Host name.
model name	This is your model name.
MAC address	This is the MAC address (Media Access Control) or Ethernet address of the device, respectively. the outdoor unit.
Internal MAC address	This is the MAC address (Media Access Control) or Ethernet address of the device, respectively. the indoor unit.
software version	This field contains information about the current firmware version that is installed on the device. The firmware can be updated via the menu Device Management> Software Upgrade.
hardware version	This field shows the hardware version of your device.
WAN information	
Regime	This is the method of encapsulation used by your ISP.
IP address	This field is the current IP address LTE modem WAN.
WAN 2 Information	
Regime	This is the method of encapsulation used by your ISP.
IP address	This field is the current IP address LTE modem WAN.
LAN information	
IP address	This field is the current LTE modem IP address on the LAN.
IP subnet mask	This field is the current subnet mask on the LAN.
DHCP server	In this field there is information about what services LTE modem provides a DHCP LAN. The options are: Server - LTE modem serves as a LAN DHCP server. Dynamically assigns IP addresses to other computers on the network. None - LTE modem makes no LAN DHCP services.
WLAN information	
Channel	This is the channel number on which currently LTE modem transmits wireless network.
WPS status	is configured appears when the LTE modem <u>connected to a wireless client device, or if WPS is active and</u>

Item	Description
	They are active the appropriate security settings for the wireless network. is not configured is displayed if the WPS is active or not active if the appropriate security settings for the wireless network.
state radio	On appears every time the radio antenna WLAN active. disabled appears every time the radio antenna WLAN inactive.
SSID (1 - 4) information	
SSID	This identifier LTE modem, respectively. Wireless LAN is sending.
State	Displays the status of the on / off SSID information.
security mode	Displays the security mode wireless network that transmits LTE modem.
5 GHz WLAN information	
Channel	This is the channel number on which currently LTE modem transmits 5GHz wireless network.
WPS status	is configured is displayed if the LTE modem is connected to a wireless client device, or if WPS is active and activated the appropriate security settings for the wireless network. is not configured is displayed if the WPS is active or not active if the appropriate security settings for the wireless network.
state radio	On appears every time the radio antenna WLAN active. disabled appears every time the radio antenna WLAN inactive.
5 GHz SSID (1 - 4) information	
SSID	This identifier LTE modem, respectively. Wireless LAN is sending.
State	Displays the status of the on / off SSID information.
security mode	Displays the security mode wireless network that transmits LTE modem.
status LTE	
State	This field is shown 4G LTE in the case of a successful connection to the LTE network. Otherwise herein Not connected.
SIM Status	This field is shown PIN verified after successfully entering a PIN or PUK. If one of these codes needed to enter will be shown here PIN required or PUK required.
signal strength	In this field the signal strength LTE network by modem receives from the transmitter or base station (sometimes referred to as an eNodeB or eNB).

Item	Description
service provider	This field is the name of your Internet service provider - LTE network operators.
The frequency band in this	field is the band LTE network in the event of a successful connection. Otherwise herein Not available .
connection length	In this field the duration of LTE connectivity, and since the last successful establishment.
RSRP	In this field the signal strength RSRP LTE network by modem receives from the transmitter or base station (sometimes referred to as an eNodeB or eNB).
SINR	In this field the strength of the signal SINR LTE network by modem receives from the transmitter or base station (sometimes referred to as an eNodeB or eNB).
FW module version	This field displays the firmware version of the LTE module.
IMEI	This field indicates the number of LTE mobile device (IMEI). It is a unique number assigned by the manufacturer to identify the device.
IMSI	IMSI stands for the term international mobile subscriber identity and indicates an identifier of a SIM card. It is a unique number assigned by your mobile operator SIM card in the mobile network.
status interface	
Interface	This column is all interfaces, which has LTE modem.
State	This field indicates whether the LTE modem interface uses. For LTE WAN interface in this field stated connected if the LTE modem is connected to the LTE network, Disconnected Otherwise, ie when the LTE network is not available. For the LAN interface is specified in this field connected if the LTE modem uses this interface, and Disconnected Otherwise, ie when the network connector is not connected with any device. For WLAN is specified in this field connected if the wireless is active, Disconnected Otherwise, ie when wireless is disabled.
Speed	For LTE WAN interface in this field stated 4G LTE in the case of a successful connection to the LTE network. For the LAN interface is shown in this field speed Ethernet connector and a duplex setting. For WLAN is shown in this field the maximum transfer rate or Not available if the wireless is disabled.
system status	
runtime	In this field the runtime LTE modem, from the last

Item	Description
equipment	commissioning. LTE modem is put into operation after plugging into a wall socket, after restarting (Device Management> Restart) or restore the default settings (see 1.5.3 RESET button).
Current date / time	This field shows the current date and time in LTE modem. Change the date and time it is possible to menu Device Management> Set time.
system resources	
Processor load in this field	is the percentage use of computational resources LTE modem processor. If this value approaches 100%, LTE modem running at full capacity, which means that the transmission rate will continue to increase. In the event that you need to allocate some applications greater transmission speed, it is necessary either to terminate.
memory utilization	This field indicates the percentage of memory occupation LTE modem. In normal operation this value does not increase too. If memory usage approaches 100%, the LTE modem probably unstable, and it is advisable to restart it. See 21 Setting logging or turn off the machine (remove the plug from the socket), wait a few seconds and then on again.
registration status	
Account	This column lists all the registered SIP accounts in LTE modem.
Action	<p>This field displays the current registration status of the relevant SIP account. To use VoIP telephony, it is necessary to register a SIP account on the SIP server.</p> <p>In case you already have an account on the SIP server SIP registered,</p> <ul style="list-style-type: none"> • Click on unregister to deregister an account SIP to SIP server. This action will not lead to the removal of your SIP account, simply cancel your SIP identity mapping to appropriate IP address or domain name. • In the second field will be displayed Registered. <p>If the SIP account is not registered with a SIP server,</p> <ul style="list-style-type: none"> • Click on Register. LTE modem then attempts to register the appropriate account SIP to SIP server. • In the second field will include the reason why the account is registered. <p>Inactive - the SIP account is not active. Activation is possible via the menu VoIP> SIP> SIP account. Registration failed - the last attempt to register the SIP account SIP server error occurred. LTE modem will automatically attempt to register the SIP account the next time the modem into operation.</p>
Account balance	This field is shown Active if the SIP account has been successfully registered and is ready for use, or Idle , if the SIP account has not yet been registered.

Item	Description
URI	In this field, the account number and account SIP service domain. The values can be changed through the menu VoIP> SIP> SIP account .

4 Broadband connection

4.1 Overview

This chapter describes the screen **Broadband connection** this LTE modem. Use the settings in this section, you can set various connection parameters, eg. To enter the PIN code of the SIM card lock specific band frequency transmitter or LTE networks.

4.2 Display Broadband

Using this screen, you can lock specific band frequency transmitter or LTE networks. Enter this screen by clicking on **Network Settings> Broadband**.

Figure 4-1 Network Settings> Broadband> Broadband

Přepínač LTE připojení
Akce Připojit Odpojit Použít Zrušit

Datový roaming
Datový roaming Povolit Zakázat Použít Zrušit

Nastavení internetu

#	Povoleno	Název	APN	NAT	Upravit
1	Povoleno	Data	Auto APN	Povoleno	
2	Zakázáno	Voice	apn2	--	
3	Povoleno	DM	cpeimgmt	--	

Poznámka :
Podporováno je pouze jedno auto APN.

The following table summarizes the available fields on this screen.

Table 4-1 Network Settings> Broadband> Broadband

Item	Description
------	-------------

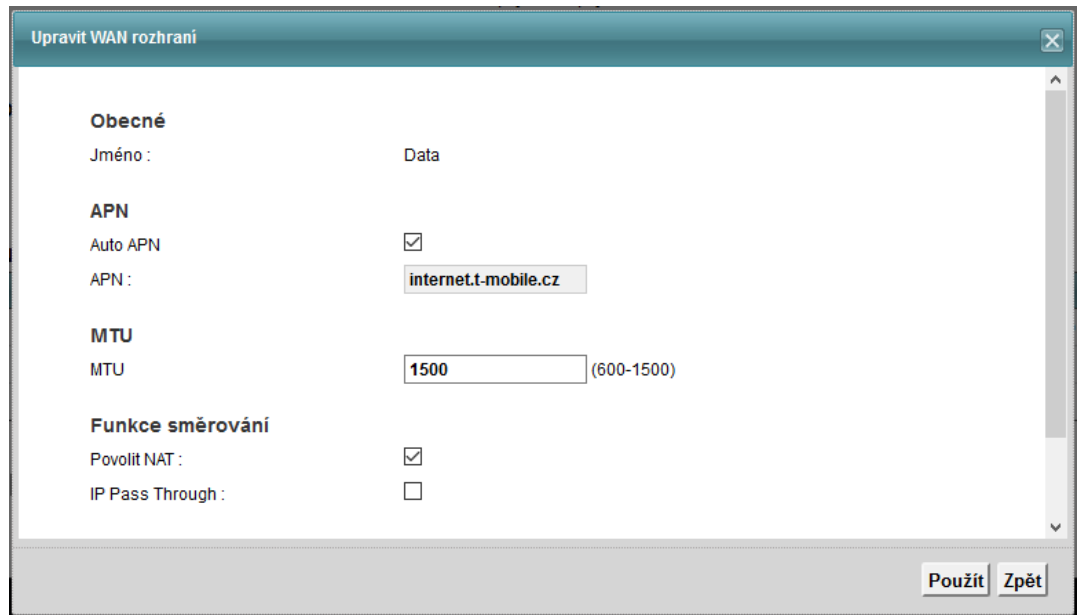
Item	Description
Switch LTE connectivity	Choose Connect LTE modem to connect to the LTE network. Choose Disconnect , if you do not want to connect the device to the LTE network.
Use	Click to save the changes made in this section.
Cancel	Click to restore previous settings in this section.
Choose Data Roaming	Allow LTE modem to connect to the LTE network of other operators. Choose Prohibit , if you do not want to LTE modem to connect to the LTE network of other operators.
Use	Click to save the changes made in this section.
Cancel	Click to restore previous settings in this section.
internet settings	
#	Serial number of broadband in the list.
Allowed	This field shows whether it is appropriate broadband connection is active or not.
Name	Name respective broadband.
APN	This is the name of the LTE network, which is carried out by the appropriate broadband connection.
NAT	This field shows whether the connection is active for NAT.
adjust	Click on the icon adjust You can also modify the interface.

4.2.1 Edit WAN Interface

Using this screen, you can adjust the WAN interface.

Click on the icon **adjust** for a front display a dialog box, as shown in the following figure.

Figure 4-2 Network Settings> Broadband> Broadband> Edit



The following table summarizes the available fields on this screen.

Table 4-2 Network Settings> Broadband> Broadband> Edit

Item	Description
Name	Name respective broadband.
Auto APN	Check this box to turn on automatic detection of the access point name APN of the LTE network. Otherwise, enter the APN manually in the field below.
APN	Enter the name APN LTE network. Name, contact your ISP.
MTU	The maximum size of the transmission unit (MTU) defines the largest possible packet size on the interface or connection. Enter the MTU value for the appropriate WAN interface.
enable NAT	Check to NAT routing for the WAN interface.
IP Pass Through	Check this box to allow access providers assign IP directly addresses devices on the LAN. This setting disables possibly setting NAT and DHCP server configuration (Network Settings> Home Network> LAN Settings). LTE modem will be managed remotely via HTTPS and SNMP. Checking this item will also receive additional parameters setting IP Pass Through.
The IP Pass Through	Select Dynamic to assign IP addresses ISP via DHCP leases 5 minutes. Select Static for assigning IP addresses via DHCP ISP only devices with specific MAC

Item	Description
	address.
Special device MAC address	If the mode function Mode IP Pass Through static enter into this field the MAC address of the device.
IP lease time Pass Through	Enter the length of time after which the client can use the LAN IP address assigned by the ISP.
Use	Clicking Use save your changes.
back	Clicking back To return to the previous screen.

4.3 SIM Screen

If the device is part of the configuration of your screen LTE modem **SIM**, You can use it to manage PIN SIM card. Enter this screen by clicking on **Network Settings> Broadband> SIM**.

Figure 4-3 Network Settings> Broadband> SIM

Zámek PIN kódu SIM karty chrání zařízení před neautorizovaným přístupem k internetu. PIN kód můžete aktivovat, upravit, nebo jeho použití vypnout PIN.
Zařízení se nemůže připojit k internetu, pokud v něm není vložena SIM karta nebo není zadán správný PIN kód.

Správa PIN

Stav SIM karty : PIN vypnut
Ověření PIN : Povolit Zakázat

Použit **Zrušit**

The following table summarizes the available fields on this screen.

Table 4-3 Network Settings> Broadband> SIM

Item	Description
SIM Status	This field displays the status of the SIM card in the system: PIN off - The SIM card is not protected by a PIN. PIN required - The SIM card is protected by a PIN code, which has not yet been specified. PIN verified - The SIM card is protected by a PIN code which has already been successfully entered. PIN locked - Too often you entered the wrong PIN and the SIM card was therefore locked. To unlock and use a SIM card, you will need the PUK code, which is available from your operator. SIM error - LTE modem does not recognize any SIM card inserted.

Item	Description
PIN verification	PIN (Personal Identification Number) is an authentication key to the SIM card. Without this code, you can not use a SIM card. Choose Allow if the SIM card is PIN-protected and requires a network operator's authentication. Choose Prohibit, when to use the SIM card is not required to enter a PIN.
enter PIN	If authentication is enabled PIN, enter in this field 4-digit PIN (eg. 0000) that you received from your service provider. In the event that your PIN is entered incorrectly too often, it can be blocked SIM card, which will then be used to access the Internet.
The remaining experiments	The remaining number of attempts to enter the correct PIN before locking the SIM card.
Use	Click to save the changes made in this section.
Cancel	Click to restore previous settings in this section.

4.3.1 Screen Blocked

If the SIM card is blocked, it can be unlocked by entering the PUK (PIN Unlock Key) on this screen.



NOTE

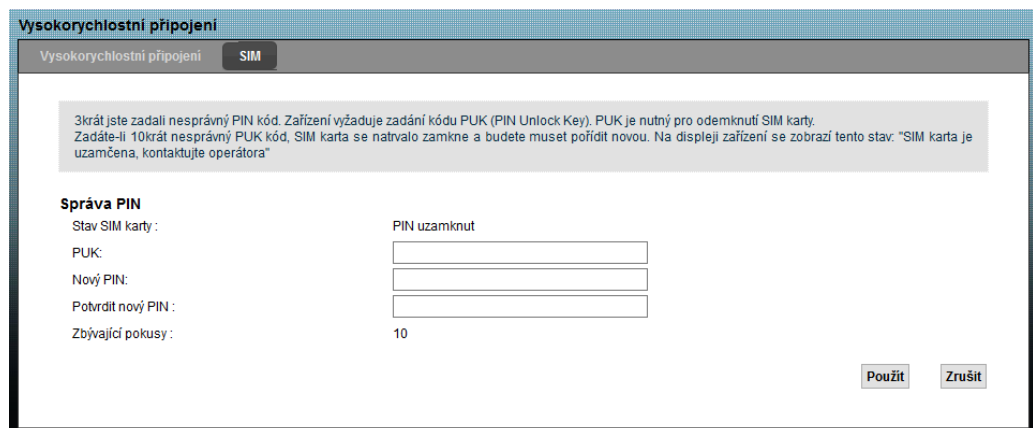
PUK code to unlock the SIM card, contact your service provider.



NOTICE

However, if you enter the wrong PUK code several times, the SIM card is discarded.

Figure 4-4 Network Settings> Broadband> SIM: Card blocked



The following table summarizes the available fields on this screen.

Table 4-4 Network Settings> Broadband> SIM: Card blocked

Item	Description
SIM Status	This field displays the status of the SIM card in the system: PIN locked - Too often you entered the wrong PIN and the SIM card was therefore locked. To unlock and use a SIM card, you will need the PUK code, which is available from your operator.
PUK	Enter the PUK (Pin Unlock Key) you received from your operator to unlock the SIM card.
new PIN	Enter a new PIN SIM card.
Confirm new PIN	Repeatedly enter a new PIN SIM card.
Remaining attempts	Remaining number of attempts to enter the correct PUK code before permanent depreciation SIM card.
Use	Click to save the changes made in this section.
Cancel	Click to restore previous settings in this section.

5 Wireless WiFi 2.4 / 5 GHz

5.1 Overview

This chapter describes the screen **Network Settings> WiFi 2.4 GHz / 5 GHz WiFi** this LTE modem. Using these screens, you can set the parameters of the wireless network broadcast LTE modem.

5.1.1 Wireless Network Topology

Wireless network consists of wireless client devices, access points (AP) and called. Bridges (routers in bridge mode).

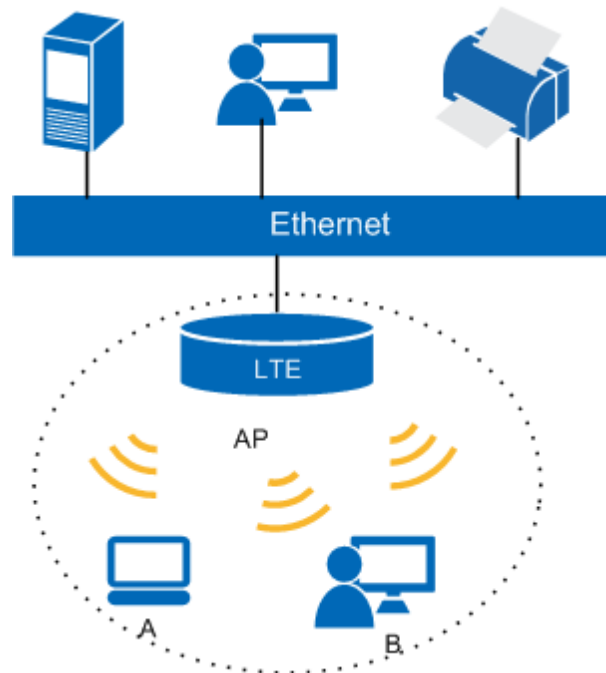
- Wireless client device means a radio receiver attached to your computer or mobile device users.
- The access point is a radio transmitter that is connected to the cable network, which can connect multiple wireless client devices and access to it through the network.
- Bridge is a radio transmitter that mediates communication between access points and client devices, ie. Increasing the reach of your wireless network.

Typically, there are two types of wireless networks.

- **Type " infrastructure " which is a part of one or more access points and several wireless client devices.** Client devices are connected directly to the access points.
- **The second type of network " ad hoc " in which there are no access points. Wireless client devices** connect to each other and exchange information.

The following image is an example of a wireless network.

Figure 5-1 One of the possible schemes wireless network



The actual wireless network is shown in the dotted circle. In this example, device **A** and **B** connect to the network through an access point (**AP**) and cooperate with other devices (eg. printer), and have access to the Internet. Your LTE modem is the access point (AP).

Each wireless network is governed by the following basic rules.

- All devices on the wireless network must use the same SSID. SSID is the name of the wireless network. It is an abbreviation of the English phrase Service Set Identifier, ie the identifier of the wireless network.
- If there are two overlapping wireless networks should each transmit on a different channel.

Like radio stations and television channels used by each wireless network to send and receive information specific channel or frequency.

- All devices on the same wireless network must use security procedures compatible with the AP.
- Security procedures prevent unauthorized devices to connect to a wireless network. It also protects the information that is sent over a wireless network.

radio frequency channels

The radio frequency spectrum is allocated certain frequency bands for unlicensed, civilian use. For wireless connectivity, these bands are divided into several channels. This allows the same place, there were many wireless networks without interference. When networking you must select the channel you want to use.

Given that unlicensed spectrum available in each country are different, so the number of available channels.

Channel means the radio frequency used by the wireless devices to transmit and receive data. The available channels depends on your geographical area. You have a choice of multiple channels (for your region) in order to reduce interference by channel different from adjacent access point (AP). Interference occurs when radio signals from different access points overlap, causing less power and bandwidth.

However, neighboring channels partially overlap. To avoid interference due to this overlap, your AP should be placed on a channel that is at least five channels from the channel used by the neighboring AP. For example, if your region has 11 channels and an adjacent AP uses channel 1, then for your network, select the channel in the range of 6 - 11th

5.1.2 Before

Before you start setting up a wireless network using the screens below, ask yourself the following questions. If any of the following terms do not know, refer to Chapter 5.5 Technical details.

- What wireless standards supported by a wireless device (eg. IEEE 802.11g)? Which standard will be the best to use?
- What safety procedures should support wireless devices (eg. WPA-PSK)?
- Which will be the best to use?
- Wireless devices support a WPS (Wi-Fi Protected Setup)? If so, the configuration is well-secured wireless network easy. Even though some devices support WPS and some that are not, you can use WPS for network and device settings without the support WPS her then manually add, though the process is somewhat more complicated.
- I want to set advanced network parameters? If so, which? If you want to make advanced settings of the wireless network, make sure that you know exactly what you are doing. Otherwise, ignore the advanced settings.



NOTE

The following chapters are screenshots of the setup routine (2.4GHz) wireless network. 5GHz network settings screen look and function similarly.

5.2 General Screen

Use this screen to wireless WiFi on or off, enter its name (SSID) and set the security level.



NOTE

If you access the configuration interface LTE modem via a wireless WiFi network and make a change to the network name (SSID) and security level, then after saving the changes, press **Use** to disconnect from the network. Then it is necessary to adjust the computer's wireless settings to match the new LTE modem settings.

the screen In general Click to enter Network Settings> WiFi 2.4 GHz / 5 GHz WiFi. Screenshots describe network setup WiFi 2.4 GHz. 5GHz network settings screen look and function similarly. All display settings check box Enable WiFi.

Figure 5-2 Network Settings> WiFi 2.4 GHz> General

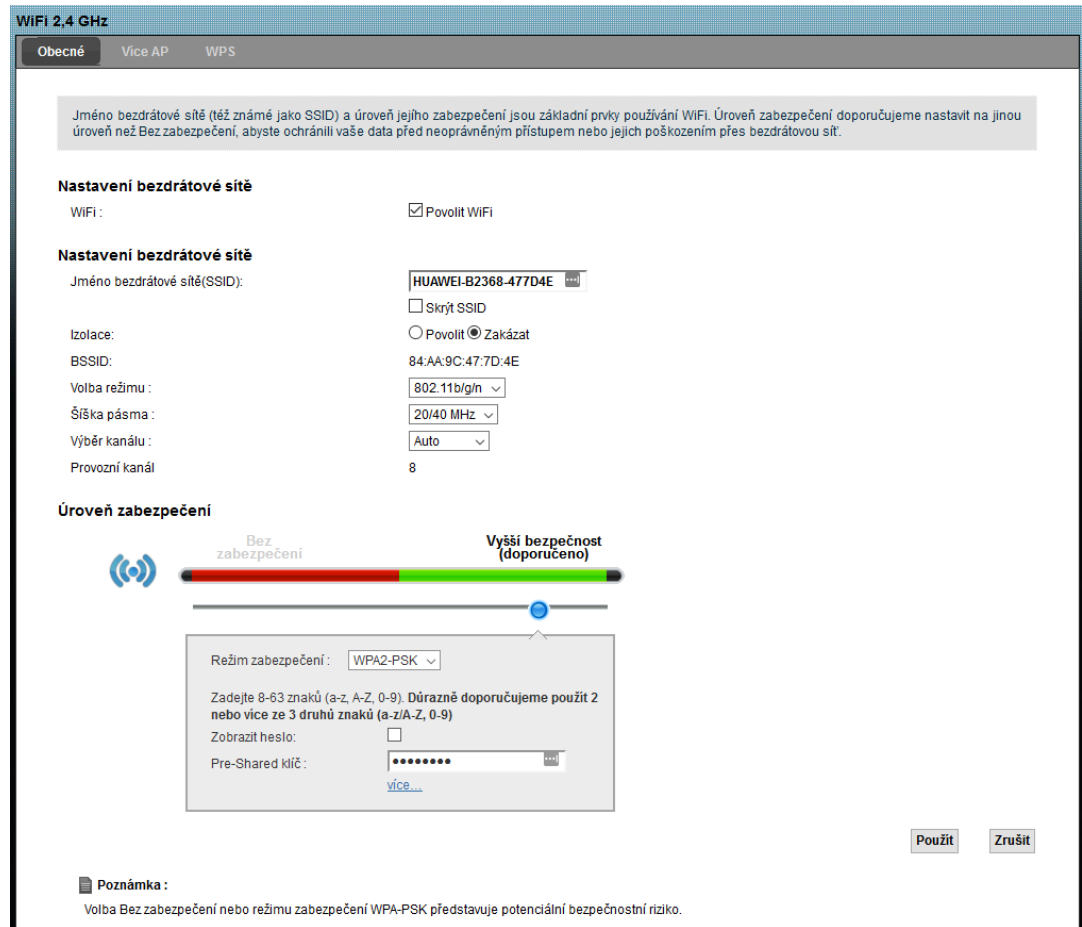
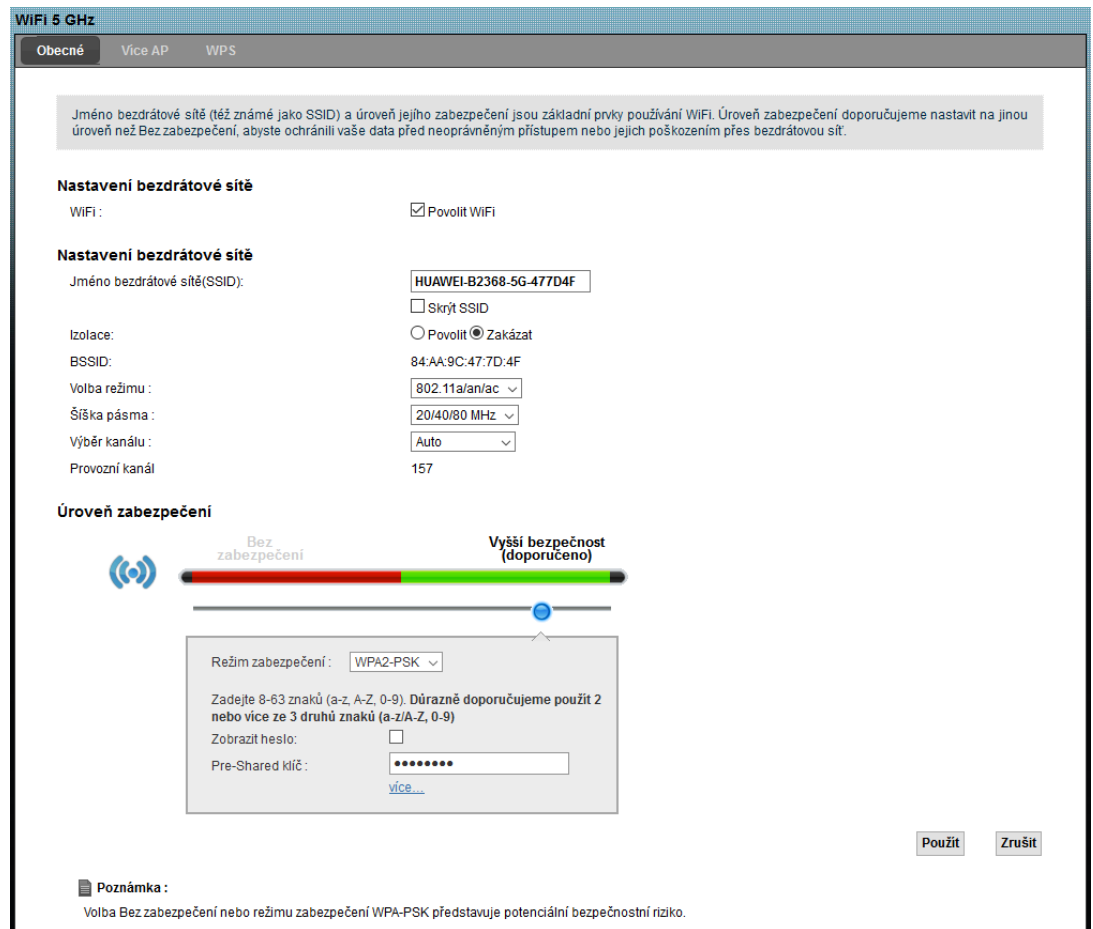


Figure 5-3 Network Settings> WiFi 5 GHz> General



The following table summarizes the available fields on this screen.

Table 5-1 Network Settings> WiFi 2.4 GHz / 5 GHz WiFi> General

Item	Description
Setting up a wireless network	
WiFi	Wireless network enable the checkbox Enable WiFi .
Setting up a wireless network	
Wireless network name (SSID)	The name of the wireless network's SSID (Service Set Identity) is used as an identifier for the wireless client devices. Wireless devices that use the Access Point (AP) must use the same SSID. Enter a descriptive name (up to 32 characters, without diacritics) wireless LAN.
Insulation	Enabling this feature prevents the individual client devices communicate with each other through the router.
Hide SSID	Check this box to hide the network identifier in the outgoing beacon frame. Wireless will be for other devices

Item	Description
	invisible.
BSSID	This field is the MAC address of the wireless interface LTE modem.
mode selection	<p>Select the mode (standard) broadcast wireless networks. On the screen WiFi 2.4 GHz> General You can set the following modes of wireless networks:</p> <ul style="list-style-type: none"> • 802.11b / g / n allows connection of all devices that support IEEE 802.11b, IEEE 802.11g and IEEE 802.11n. May reduce the transmission rate LTE modem. • 802.11g / n allows connection of all devices that support IEEE 802.11g and IEEE 802.11n. • 802.11b / g allows connection of all devices that support IEEE 802.11b and IEEE 802.11g. May reduce the transmission rate LTE modem. • 802.11n allow connections only devices that support the IEEE 802.11n standard. • 802.11 g allow connections only devices that support the IEEE 802.11g standard. • 802.11b allow connections only devices that support the IEEE 802.11b standard. On the screen WiFi 5 GHz> General You can set the following modes of wireless networks: • 802.11a / n / c allows any device that supports IEEE 802.11a, IEEE 802.11n IEEE 802.11ac. • 802.11an / ac allows connection of all devices that support IEEE 802.11n IEEE 802.11ac. • 802.11a / nn allows connection of all devices that support IEEE 802.11 IEEE 802.11n. • 802.11an allow connections only devices that support the IEEE 802.11n standard. • 802.11a allow connections only devices that support the IEEE 802.11a standard.
Bandwidth	<p>Enter bandwidth wireless LAN which LTE modem transmits.</p> <p>At 5 GHz WiFi choose 20/40/80 MHz LTE modem in order to use the 1, 2 or 3 channels for maximum throughput. If you choose 20/40 MHz LTE modem will be able to use 1 or 2 channels. If you choose 20 MHz To reduce the interference of other wireless networks and devices in your area.</p>
channel selection	<p>Choose one of the channels available in your area. Select a specific channel number or option Car, when that is automatically selected. If you encounter problems with wireless interference, changing channels can help. Select a <u>channel number, which is the farthest possible from channels that</u></p>

Item	Description
	transmitting neighboring access points (AP). The channel number, the LTE modem currently used is indicated in field Operating channel .
operating channel	This is the channel number that LTE modem currently used.
security level	
security mode	Choose Higher security, to ensure consistent security of your wireless network. Wireless client devices you want to connect to the wireless network, the security settings are applied to support. Once you select " higher security " appears on the screen next setting. You can also select No security - In this case, this wireless network will be able to connect any device without any data encryption or authentication. More information about individual security modes, summarized in the following chapters.
Use	Click on Use to save your changes settings LTE modem.
Cancel	Click on Cancel restore previous settings in this section.

No security



NOTE

If you choose **No security** will this wireless network can connect any device without any data encryption or authentication.

This means that the wireless network and all the devices connected to it will have access to all devices located within range of a wireless network.

Figure 5-4 WiFi 2.4 / 5 GHz> General: No security

Úroveň zabezpečení



The following table summarizes the available fields on this screen.

Table 5-2 WiFi 2.4 / 5 GHz> General: No security

Item	Description
security level	Move the slider to choose Without security .

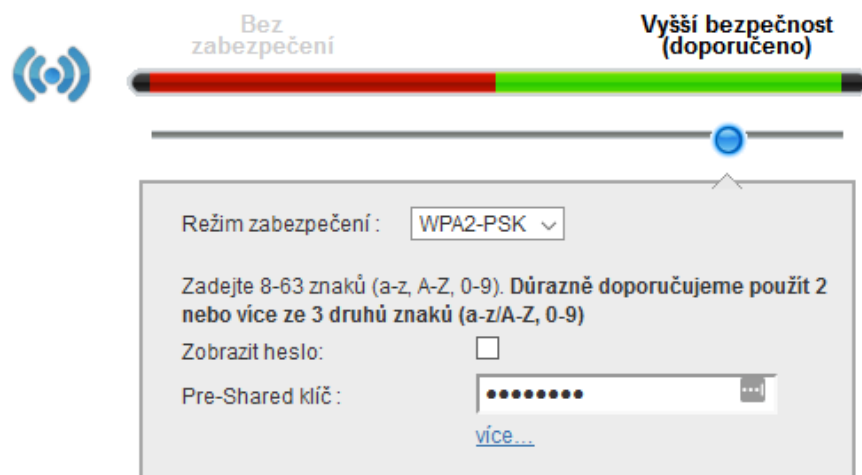
5.2.1 Higher Security (WPA (2) PSK)

Mode WPA-PSK provides data encryption and access authentication. LTE modem and the connected client device exchange PSK key that is used to verify the connection. Although this security mode is fairly robust, it is not as powerful as the newer WPA2-PSK.

the screen **In general** Click to enter **Network Settings> WiFi 2.4 GHz / 5 GHz WiFi**. Choose a security level **Higher security**. Then select from a list **security mode** selection **WPA-PSK** or **WPA2-PSK**.

Figure 5-5 Figure 1-1 WiFi 2.4GHz / 5GHz WiFi> General: Increased safety WPA (2) -PSK

Úroveň zabezpečení



The following table summarizes the available fields on this screen.

Table 5-3 WiFi 2.4 / 5GHz> General: WPA (2) -PSK

Item	Description
security level	choose higher security to activate data encryption WPA (2) PSK.
security mode	From the drop-down list, select WPA-PSK or WPA2-PSK .
Show password	Check this box to display the password in a readable format.
Pre-Shared Key Enter	the security password to connect to a WiFi network. It may consist of 8 - 63 ASCII characters, a distinction is case sensitive .
more ... / hide more	Click on more... to view additional fields. Click on hide more Again you hide.
WPA-PSK Compatible	This field will be displayed when you select WPA2-PSK like Security mode. Enable this setting if you want to enable devices supporting

Item	Description
	only WPA-PSK connect to the LTE modem. The LTE modem supports WPA-PSK and WPA2-PSK simultaneously.
encryption	<p>If the security mode is set to WPA-PSK, Encryption will be automatically set to TKIP, So on the temporal key integrity protocol (TKIP Temporal Key Integrity Protocol). If the security mode is set to WPA2-PSK and setting</p> <p>WPA-PSK Compatible is disabled, the encryption will be automatically set to AES, Thus, system advanced encryption AES (Advanced Encryption System). AES system offers significantly better security than TKIP. If the security mode is set to WPA2-PSK and setting</p> <p>WPA-PSK Compatible is enabled, encryption is automatically set to TKIPAES, Thus, the system AES and TKIP will be active simultaneously.</p>

5.3 Screen More AP

LTE modem is able to transmit up to four independent wireless network simultaneously. This means that users can connect to LTE modem through different SSIDs. Connection to each SSID profile can be secured, so that the wireless client devices connected to different SSID identifiers between themselves they can not communicate.

Use this screen to enable and configure additional wireless network infrastructure.

Click on **Network Settings> WiFi 2.4 GHz / 5 GHz WiFi> More AP**. The following screen will appear.

Figure 5-6 Network Settings> WiFi 2.4 GHz / 5 GHz WiFi> More AP

#	Aktivní	SSID	Zabezpečeni	Upravit
2		HUAWEI-B2368-5G-2-407D4F	WPA2-PSK mixed	
3		HUAWEI-B2368-5G-3-417D4F	WPA2-PSK mixed	
4		HUAWEI-B2368-5G-4-427D4F	WPA2-PSK mixed	

The following table summarizes the available fields on this screen.

Table 5-4 Network Settings> WiFi 2.4 GHz / 5 GHz WiFi> More AP

Item	Description
#	This is the serial number.
Active	This field shows whether the corresponding SSID is active. Symbol yellow light bulb means that the SSID is active. Symbol gray bulb means that the SSID is not active.
SSID	SSID profile is a set of parameters related to one of the wireless networks LTE modem. The name of the wireless network's SSID (Service Set Identity) is used as an identifier for the wireless client devices.

Item	Description
	This field contains the name of the appropriate wireless network. Once the wireless device to scan for available WiFi networks, this is the name that appears in the list.
secure it	This field is given the security mode of the SSID profile.
adjust	Click on the icon adjust You can also adjust the appropriate SSID profile.

5.3.1 Editing multiple AP

Using this screen, you can edit the SSID profile. Click on the icon **adjust** at the appropriate SSID profile screen **More AP**. The following screen will appear.

Figure 5-7 WiFi 2.4 GHz> More AP: Edit

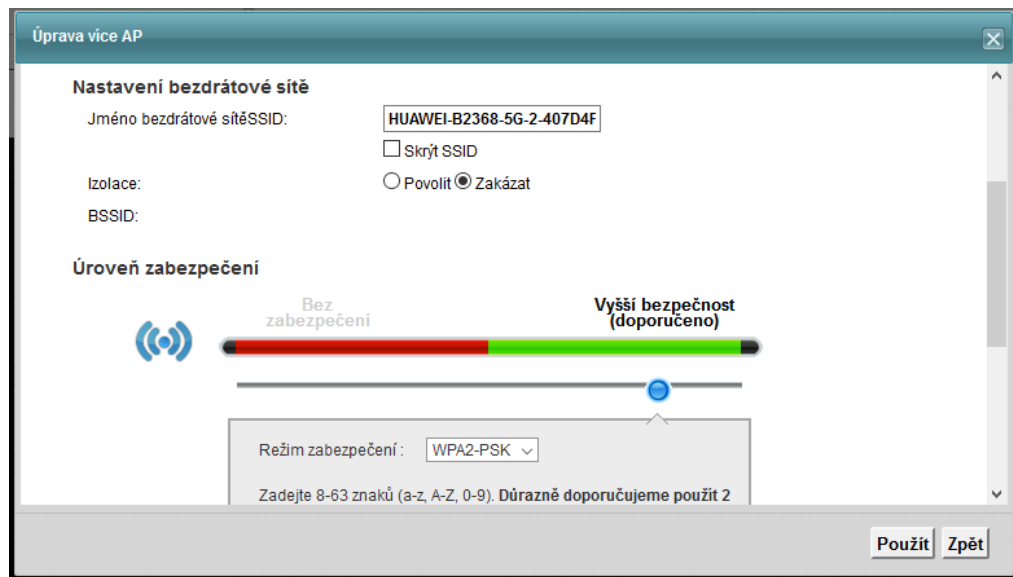
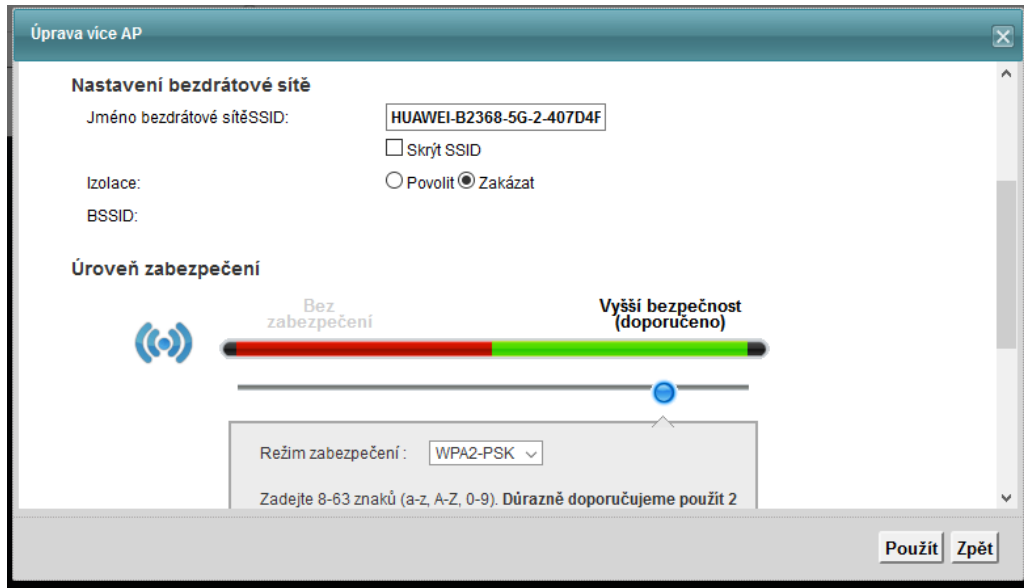


Figure 5-8 WiFi 5 GHz> More AP: Edit



The following table summarizes the available fields on this screen.

Table 5-5 WiFi 2.4 GHz / 5 GHz WiFi> More AP: Edit

Item	Description
Setting up a wireless network	
WiFi	Wireless network enable the checkbox Enable WiFi .
Setting up a wireless network	
The name of the wireless network SSID	The name of the wireless network's SSID (Service Set Identity) is used as an identifier for the wireless client devices. Wireless devices that use the Access Point (AP) must use the same SSID. Enter a descriptive name (up to 32 characters, without diacritics) wireless LAN.
Hide SSID	Check this box to hide the network identifier in the outgoing beacon frame. Wireless network will be invisible to other devices.
Insulation	Enabling this feature prevents the individual client devices communicate with each other through the router.
BSSID	This field is the MAC address of the wireless interface LTE modem.
security level	
security mode	Choose Higher Security (WPA (2) PSK) to ensure consistent security of your wireless network. Wireless client devices you want to connect to the wireless network, the security settings are applied to support. Once you select " higher security " appears on the screen next setting. You can also select No security - in which case the <u>This wireless network will be able to connect any device without any</u>

Item	Description
	data encryption or authentication. For more information, see chapter 5.2.1 Higher Security (WPA (2) PSK).
Use	Clicking Use save your changes.
back	Clicking back to exit without saving.

5.4 WPS screen

Use this screen to configure the connection to LTE modem using WiFi Protected Setup (WPS).

WPS enables quick setup wireless networks with strong security without the need for manual configuration of security parameters. WPS connection is always established between the two devices. Both devices must support WPS. For more information about WPS connection, see chapter 5.5.5 Connection using WiFi Protected Setup (WPS).



NOTE

LTE modem observe the security settings of the access profile **SSID1** (more information, see Section 5.1.2 Before). If you want to use WPS connection, it is necessary security mode profile **SSID1** set to **WPA2-PSK** or **Without security**. Profile **SSID1** It must also not be hidden.

Click on **Network Settings > WiFi 2.4 GHz / 5 GHz WiFi > WPS**. The following screen will appear. WPS activate by selecting **Allow** and then click **Use**. Then you have the next setting WPS.

Figure 5-9 Network Settings > WiFi 2.4 GHz / 5 GHz WiFi > WPS

Zapnutí Wi-Fi Protected Setup (WPS) vám umožní snadné přidání WPS-kompatibilních zařízení do vaší bezdrátové sítě. Zvolte jednu z WPS metod a k sestavení WPS spojení se řiďte pokyny. Je-li vaše bezdrátové klientské zařízení vybavené tlačítkem WPS, bude vaší preferovanou metodou provedení WPS metoda Push Button Configuration (PBC).

Obecné

WPS: Povolit Zakázat

Přidat nové zařízení metodou WPS

Metoda 1 PBC	Metoda 2 PIN
<p>Krok 1. Stiskněte tlačítko WPS </p> <p>Krok 2. Stiskněte tlačítko WPS na vašem novém bezdrátovém klientském zařízení do 120 sekund</p>	<p>Krok 1. Zadejte PIN vašeho nového bezdrátového klientského zařízení a poté klikněte na Registrovat</p> <p>Zde zadejte PIN Registrovat</p>

Poznámka :

Tato funkce je dostupná pouze když je zvolen režim WPA2-PSK nebo Bez zabezpečení a nemůže pracovat se skrytým SSID.

Použit

The following table summarizes the available fields on this screen.

Table 5-6 Network Settings> WiFi 2.4 GHz / 5 GHz WiFi> WPS

Item	Description
WPS	selecting Allow LTE modem to turn on the WPS.
Add new device using WPS	
PBC Method 1	Use this method to set up a wireless network via the WPS pressing.
WPS	Click this button to add a new wireless network devices that support WPS (which is within range of an LTE modem). WPS button on the client device may be a physical button on the outside of the device, or as a software button, like button WPS on this screen. Note: WPS button on the wireless device is required to press two minutes from clicking on this button.
Method 2 PIN	Use this method to set up a wireless network by entering PIN client device.
Register	Enter the PIN of the client device you want to connect via WPS, and then click Register to connect to a wireless network. The PIN code can be located on the outside of the device or its configuration interface. Note: The WPS on the client device also must be activated within two minutes of entering a PIN.
Use	Clicking Use save your changes.

5.5 Technical details

This chapter deals with the technical details of the wireless LAN.

5.5.1 Overview of wireless security

All radio communication is by its nature very easy to catch. For wireless data networks, this means that anyone who is within range of a wireless network without security can not read data that pass through the air waves, but also connect to the network. Once an unauthorized person gets access to the network once, can not gain access to sensitive information, but also to expand the network of malicious software with the intent network and the connected equipment damage. For this reason, many developed safety systems designed to ensure that the use of wireless networks and understanding of data flowing on the network has been designed exclusively to authorized persons.

These safety standards do two things. First used for access authentication. This means that access to the network will receive only the person or device that know the correct credentials (username and password, respectively. Key). **Second, encrypted wireless communication. This means that the information sent by air are in a readable format - They are encoded.** Only a person possessing the relevant key data they are able to read, and this key will get only persons authenticated credentials.

The effectiveness of the safety standards vary. Some safety standards are very robust, but the threat is a misuse. For example, a security standard WPA-PSK itself is very safe, if a user uses a long enough password that can not be easily guessed, such as a long string of random numbers and letters. Safety of this **standard is declining in case you choose a short password that can be easily guessed - need the three-word from the dictionary.**

Because of the potential damage that an attacker can inflict are high, should not the safety standards are only interested in people working with sensitive information. Effective security should be a priority of all those who are with your device connected to a wireless network.

A good way to think of an effective security password, is take some very important personal information we have but easy to remember, and write it in a way that acts randomly and beyond the normal syntax rules. For example, say your father owns the Dodge Challenger in 1970 and his favorite movie is Vanishing Point (which you know from the year 1971). Then, your password may be, for example,

" 70dodchal71vanpoi ".

The following chapters deal with the different types of security you can into your wireless network to implement.

SSID

In normal operation, the LTE modem acts as a beacon, which regularly broadcasts the SSID in your neighborhood. Broadcast SSID can not suppress a presence of an access point in the form of an LTE modem to hide. We recommend that you also change the default SSID to a name that is not easy to guess.

This security method is relatively weak, because there are ways in which they can gain unauthorized devices SSID. In addition, unauthorized devices can still see the data that is sent over a wireless network.

The MAC address filter

Any device that can connect to a wireless network has its own unique identification number called a MAC address. It is usually written in the form of 12 hexadecimal characters, for example. 00A0C5000002 or 00:A0:C5:00:00:02. MAC address can be found in the operating instructions or other documentation included with the device.

The MAC address filter can then be used to determine the devices that will access the wireless network. Each device, including those permitted, but will still have the right to know the access data to the network (SSID, channel and security password). If the MAC address of the device is not on the whitelist, it does not matter whether you know the access data or not.

This method of security does not protect information that is sent over a wireless network. Moreover, there are ways in which unauthorized wireless device can get some of allowed MAC addresses. The device was subsequently may be one of the authorized MAC addresses to hide.

First Some wireless devices, such as scanners, wireless networks can be connected, but they can not communicate through them. Such devices may be provided with a MAC address.

Second Hexadecimal characters refers to the number 0 - 9, the letters A - F aa - F.

user Authentication

User authentication is the process during which there is access to check the legitimacy of a particular wireless client device to the network. Wireless network as possible to secure the necessary signing. To do this it is necessary that each device in your wireless network support the IEEE 802.1x standard.

User names and passwords for each user can be stored on the RADIUS server. Use of this site is not typical for commercial rather than residential use. If you do not have a RADIUS server is available, you can not access the wireless network to make the user logon.

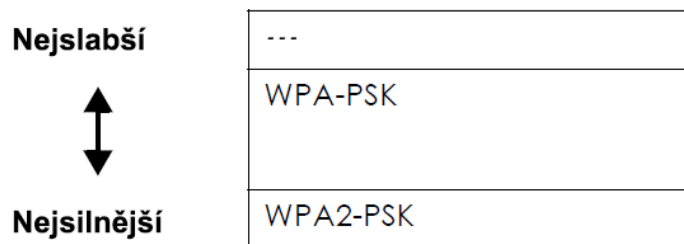
Unauthorized wireless devices can still see all the data flow in the wireless network, despite the fact that they themselves can not use the network. To do this, there are ways that attackers can obtain a valid user name and password. Then, the wireless network can simply log.

encryption

Encryption is primarily used to protect information that is sent over a wireless network. Encryption of wireless networks, like any other, works on the principle of the secret key. If you do not know the key to decrypt the message, you will not understand it.

Types of encryption that are available, depending on the authentication method.

Figure 5-10 Encryption types for different authentication methods



You can choose no security, **WPA-PSK** or **WPA2-PSK**.

We strongly recommend using the highest level of security to devices on the network support. Consider two devices that wish to access the wireless network. And while the device only supports WPA-PSK method, device B supports both WPA-PSK and WPA2-PSK. Therefore, the mode of wireless security should be **WPA-PSK**.



NOTE

It is recommended that each wireless network has been protected by encryption **WPA-PSK** or **WPA2-PSK**. Other encryption methods are on one side better than none, but the security level is relatively low and gain access data is not difficult for an attacker.

If the configuration interface LTE modem select the security mode **WPA2-PSK**, You will also have the option to select **WPA compatible**. making the network will have access and devices that only support WPA-PSK method. In the event that one of your machine supports WPA-PSK and WPA2-PSK some, set the security mode to **WPA2-PSK** and tick **WPA compatible**.

Most methods of encryption to protect information sent by the wireless network key. The longer the key, the stronger the security. Each device on the wireless network must be accessed using the same key.

5.5.2 Problems with signal

Because wireless networks are WiFi radio networks, their signal is affected by distance and interference or absorption signal.

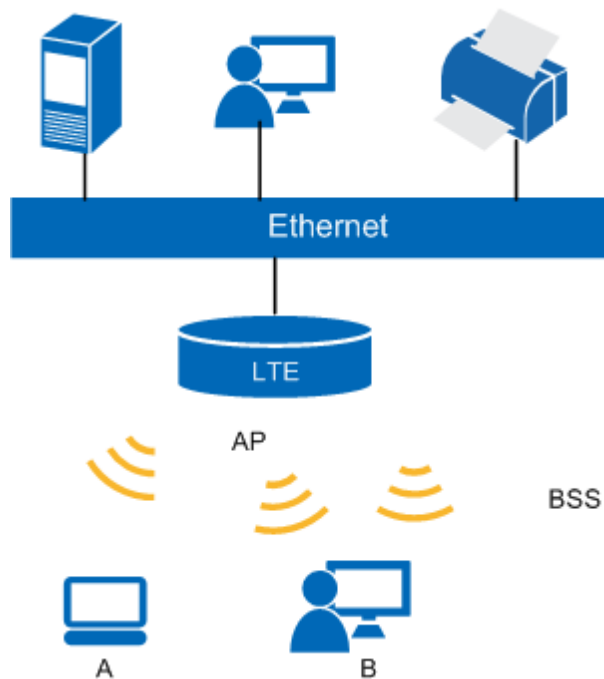
Dropouts due to distance occurs when the devices are too far apart. The problems due to interference occurs when a data signal disrupt other radio waves. Interference can come from other radio transmissions, such as military communications systems, or air traffic control, but also on devices that are only random emitters, such as electric or microwave oven. Absorption problems occur when the radio is between two physical barriers (eg. Thick walls).

5.5.3 BSS

Basic Service Set (BSS) is a set of stations that can communicate with each other at the physical layer of wireless connectivity through one access point (AP).

Independent BSS (IBSS) is a wireless transmission between stations in the basic service set. If the IBSS is prohibited individual wireless stations can access the network and communicate with each other. If the IBSS is enabled, wireless stations each can still access the network, but among themselves they can not communicate.

Figure 5-11 Core Services



5.5.4 MBSSID

To configure different basic service set (BSS) is typically necessary to use another access point (AP). In addition to the cost of another access point also threatens their interference channels. Function MBSSID (Multiple Basic Service Set Identifier) of the LTE modem enables use of a single access point to provide some

Basic Service Sets (BSS) at the same time. Each network can assign different priorities to the quality of service (QoS) and / or security modes.

Wireless devices can then use different BSSID to connect to the same access point (AP).

Note Technology MBSS

- One access point (AP) allows the establishment of a maximum of eight sub-sets BSS.
- Each set of BSS must have its own access key. If two wireless devices using different identifiers (BSSID = are located in different sets BSS), but the network communication is decrypted with the same key, it is possible to be able to intercept the second wireless communication device. Mutual communication but maybe not.
- MBSSID not a substitute for 802.1x security standard, but as an option.

5.5.5 Connecting using WiFi Protected Setup (WPS)

This method supports LTE modem WiFi Protected Setup (WPS), which is an easy way to configure a secure wireless network. WPS specification is an industry standard from the WiFi Alliance.

WPS enables quick setup wireless networks with strong security without the need for manual configuration of security parameters. Each connection using WPS works between two devices. Both devices must support WPS (information on compatibility with WPS see instructions on the device).

Depending on the type of devices you can connect WPS start pressing the button (physical button on the device or software configuration interface), or by entering a PIN (a unique password that one device helps verify the identity of the other) to both devices. After activating the WPS on one device, it is necessary to be activated WPS also on the other device, and over the next two minutes. Then there is a connection between the two devices and create a secure wireless network.

5.5.5.1 Creating a wireless network through the WPS press (PBC)

The way to create a wireless network (sometimes referred to by the acronym PBC) is initiated by pressing the WPS button on both devices to be connected. Connection then takes place automatically. No further information is required to enter.

Not all devices support WPS, however, has for this purpose a physical button. WPS button for PBC may be located, for example, in the configuration interface, as is the case in this instance LTE modem. Connecting via the WPS button pressing is as follows.

Step 1 Make sure that the two devices together you want to connect, there are close to each other.

step 2 Find the appropriate WPS button on both devices. If no physical device

WPS button not sign in to the management interface and search facilities softkey in it (see the manual of the device, the location of the WPS button, this LTE modem is described in section 5.4 Screen WPS).

step 3 Press on one of the devices (in any order). WPS button of LTE

a modem is required to press and hold at least 10 seconds.

step 4 Over the next two minutes, press a button on the other device. The registrar then sends the network name (SSID) and security key via a secure connection to the enrollee.

If you need to check whether there is a successful connection using WPS, refer to the configuration interface of the access point (AP). If you see the list of wireless client devices connected via WPS was successful.

---- End

5.5.5.2 Creating a wireless network via PIN

The method of entering a PIN ensures that the creation of wireless networks will surely required between two devices, not strictly between two nearby devices that activate WPS. The method of entering a PIN requires logging into the configuration interface of each device you want to connect.

When using the method of entering your PIN you must first enter the PIN code of the wireless client device to the LTE modem. Then, once the WPS function on the first active device will be displayed PIN for the other device. In the event that both the PIN codes are identical, the first device sends information about the network and other access devices, and enable them to access the network.

The following steps describe how to create a wireless network between the access point / wireless router (hereinafter referred to as AP) and client device by entering a PIN.

Step 1 Make sure the WPS function is activated on both devices.

step 2 Go to the section WPS AP configuration interface. The procedure can be found in the instruction manual.

step 3 Locate PIN to connect WPS client device. It can be located directly on equipment or in the respective configuration interface.

step 4 Enter the PIN code to the client device configuration interface AP.

step 5 Activate the WPS function on both devices ranging up to two minutes apart.

step 6 To activate, use the WPS configuration interface, no physical button on itself equipment.

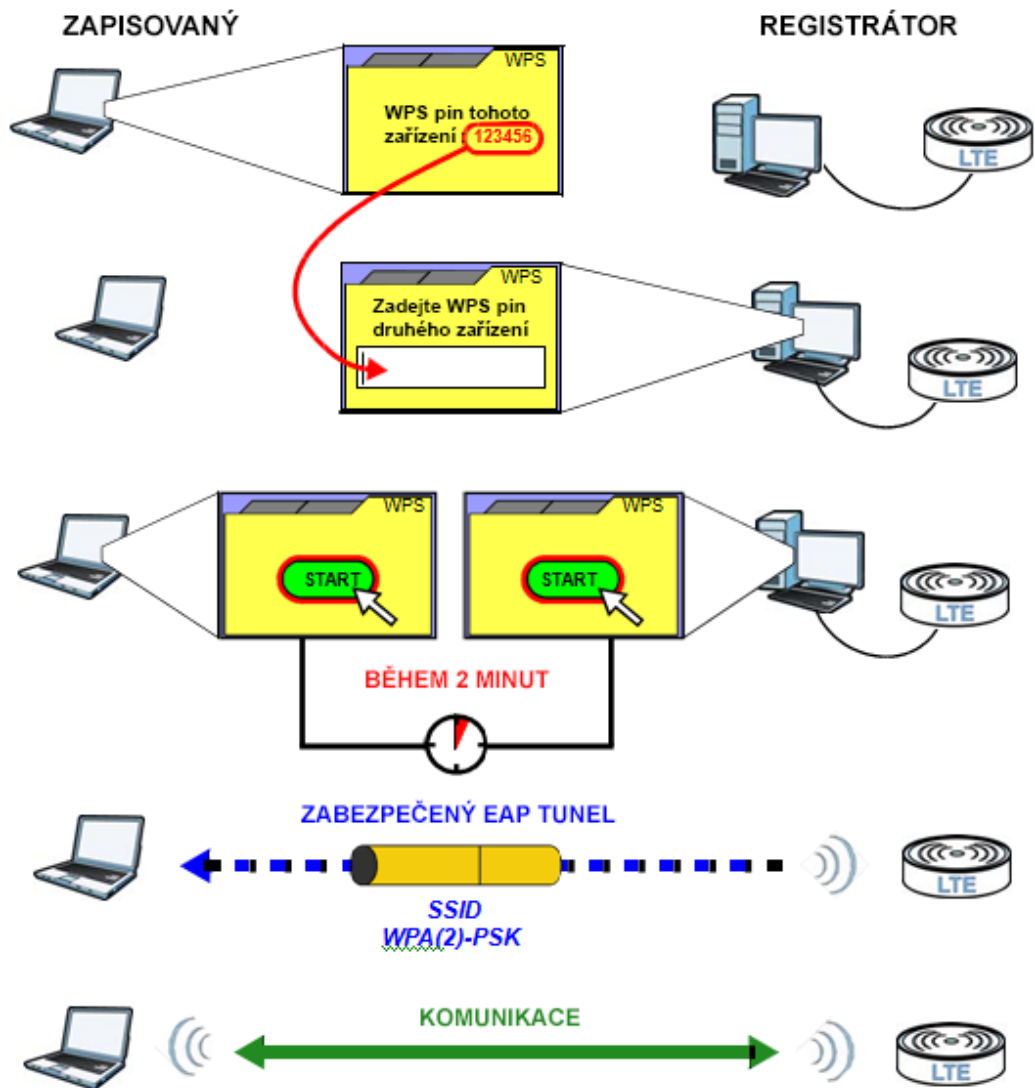
step 7 After connecting your computer to the wireless client devices try to connect to the Internet.

If the Internet is available, the network configuration via WPS successful.

If an Internet connection is not available, refer to the configuration interface of the access point (AP). If you see the list of wireless client devices connected via WPS was successful.

The following figure shows a wireless client device (laptop) that connects to the access point (AP) by entering a PIN.

Figure 5-12 Example configuration using WPS PIN input method



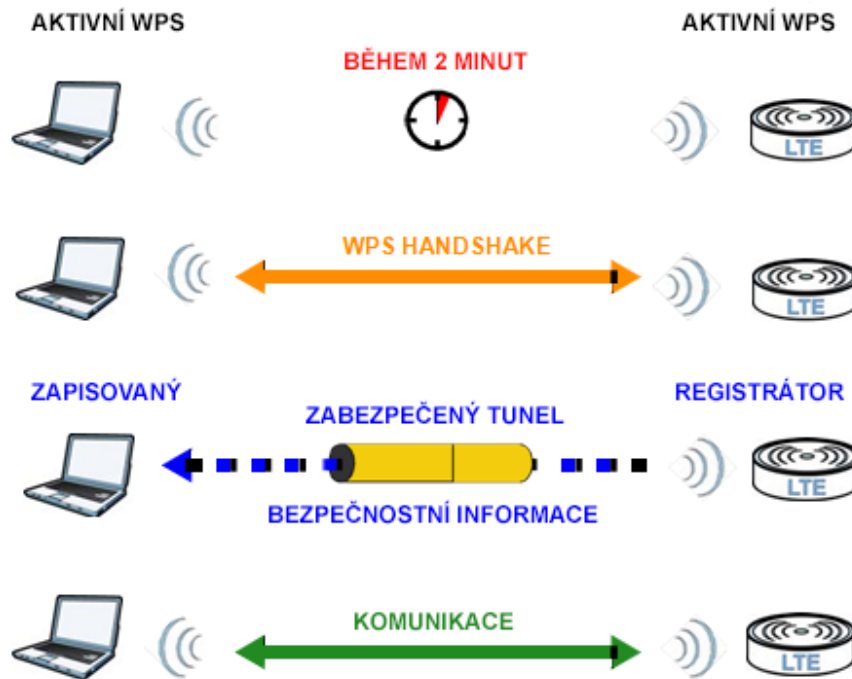
---- End

5.5.5.3 How WPS works

During connection of two devices that support WPS both devices have a different role. One device fulfills the role of the registrar (the device that provides information on network and security) and the second function enrollee (ie a device that network information and security receives). The registrar creates a secure tunnel EAP (Extensible Authentication Protocol), through which the enrollee will send the network name (SSID) and WPA-PSK or WPA2-PSK. Security Method, WPA-PSK or WPA2-PSK, depending on facilities connected devices. WPS 2.0 does not use WPA-PSK. If the registrar is already part of the network, it sends current information. If there is still no network, will generate a random password, SSID and WPA (2) PSK.

The following figure shows a wireless client device (laptop) that connects to the access point (AP).

Figure 5-13 Example configuration using WPS PIN input method



The role of the registrar and the enrollee is only valid for the duration of the configuration process, WPS (maximum two minutes). The next time you use WPS role registrar may, if necessary, take other device.

The process of connecting via WPS works like shaking hands - WPS parties to the transaction are always exactly two devices. Hence also the English name information exchange process, ie "handshake". To network the same way to connect additional devices, you must repeat the process with the fact that one of the devices will no longer be part of the network to which you want to connect a new device.

Keep in mind that LTE modem may not always be the registrar, as well as a wireless client device may be enrollee. Registrar may be any access point (AP) supporting the WPS, as well as some of the client devices.

5.5.5.4 Restrictions WPS

WPS has some limitations that must be taken into account.

- WPS works only in networks of infrastructural type, ie those that enable communication between access points and client devices. In networks, ad hoc (no access points), this technology does not work.
- WPS technology always works only between two devices. Write to the network can not be multiple devices **simultaneously - Registration must be done each separately.**

For example, if we consider the two recorded and one registrar, it is necessary to first set up the connection of the first written (either physical WPS button or entering a PIN), and after a successful registration, repeat the same procedure also for the second enrollee.

- WPS works only with properly equipped facilities. A network that was created using WPS, though it is of course possible to later add devices that support this feature.

The principle of functioning WPS automatic assignment of randomly generated passwords WPA-PSK / WPA2-PSK registrar enrollee. If the password is generated by the WPA-PSK or WPA2-PSK depending on the specifications of the device. Information on the available level of security can be found for example in the configuration interface of the registrar (if such a function of the device supports it). Thus generated can then enter a password into a device that does not support WPS, thus created a standard connection to the network (the device still must support encryption method WPA-PSK or WPA2-PSK).

- WPS 2.0 does not use WPA-PSK.
- If you choose to use PBC methods (ie press the WPS button), keep in mind that its essence is to create a **two-minute " window " during which the network can connect to any device that supports WPS. Registrar can not detect in any way " right " clerk, and therefore can not distinguish between the device wishing to actually connect and intruder.** During this period you can penetrate your network hacker.

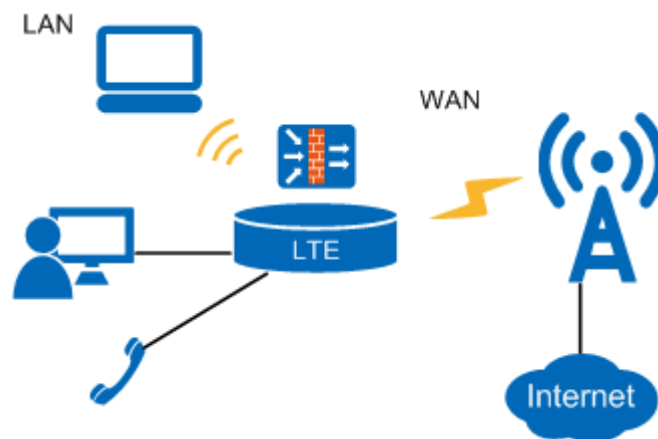
If this happened, however, can be easily verified. As already mentioned, WPS always works only between two devices. So if during the two-minute interval has been to establish a connection with another device, your device will not be able to accept the role of an enrollee and will not be able to connect to the network. If this happens, open the configuration interface of the access point and check the list of connected client devices (typically are given their MAC addresses). Independently of how there was a potential intrusion alien device, to ensure that this equipment has obtained access to your wireless network, it must be assigned to the access point. Check the MAC addresses of client devices in your home (usually on a label on the bottom of the device). If the list in the configuration interface, you can find an unknown MAC address, you can be deleted from the list. An alternative solution is to restart the access point.

6 Creating a home network

6.1 Overview

LAN (Local Area Network) is a shared communication system to which it is connected to multiple computers or mobile devices. LAN is usually made within a specific area, for example. Building or floor of the building.

Using screens LAN configuration interface can eg. To set up a DHCP server and manage IP addresses.



6.1.1 What You Need to Know

Before reading this chapter is to be familiar with the following terms.

6.1.1.1 The IP address on the LAN

Like the houses on the street shares its name, the computer within a LAN share the same IP address. This is the Internet Protocol address - IP.

subnet mask

The subnet mask specifies an IP address belonging to segment the network. LTE modem calculate subnet mask automatically based on your specified IP addresses. Subnet mask computed LTE modem does not need to be changed if the instructions say otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allocates client devices over a network connection TCP / IP. LTE modem has a built-in DHCP server, which supported client device assigns IP addresses and DNS Server.

DNS

DNS (Domain Name System) is a hierarchical domain name system mapping the domain name to the corresponding IP address and vice versa. The DNS server is extremely important because without it having to remember the IP address of each computer to which you want to connect. DNS server addresses are assigned to a client device automatically, along with the IP address and subnet mask DHCP server.

6.1.1.2 The UPnP

How do I use the UPnP device?

UPnP device appears as an icon when you open the View menu computers and devices on the network in Control Panel (Windows 10). Each UPnP devices on your network in this menu will appear separately. Double click the icon to see more information about UPnP device and its properties.

Notice regarding the UPnP device

Devices and applications that perform automated network address translation (NAT), at the same time tend to have access to the ports of the firewall, which can pose a security risk. Through these devices and applications can also in some cases to obtain information about network security.

Once connected to the network UPnP devices, announces its presence with a multicast message. For safety reasons, the LTE modem allows multicast messages only on the local network.

All UPnP devices within a network among themselves so they can communicate freely without the need for further adjustment. UPnP can be switched off if these devices do not use.

6.2 LAN Settings screen

Enter the screen **LAN settings** click on **Network Settings> Home network**. Use this screen to configure the IP address of the local network subnet mask LTE modem parameters DHCP server parameters IP addressing and DNS values.

Figure 6-1 Network Settings> Home Network> LAN Settings (DHCP enabled)

Zde uvedená LAN IP adresa je IP adresa pro vaše přihlášení ke konfiguračnímu rozhraní. Nastavení DHCP serveru určuje pravidla přiřazování IP adres LAN klientům ve vaší síti.

Nastavení IP LAN

IP adresa :

Maska subsítě :

Stav DHCP serveru

DHCP : Povolit Zakázat

Doba zapůjčení DHCP : dnů/den/dny/dní hod. min. (2 minuty až 31 dní)

Hodnoty IP adresování

Počáteční adresa IP poolu :

Velikost poolu : (1~32)

DNS hodnoty

DNS server 1 :

DNS server 2 :

DNS server 3 :

Figure 6-2 Network Settings> Home Network> LAN Settings (DHCP disabled)

Zde uvedená LAN IP adresa je IP adresa pro vaše přihlášení ke konfiguračnímu rozhraní. Nastavení DHCP serveru určuje pravidla přiřazování IP adres LAN klientům ve vaší síti.

Nastavení IP LAN

IP adresa :

Maska subsítě :

Stav DHCP serveru

DHCP : Povolit Zakázat

Stav DHCP relay

DHCP Relay Povolit Zakázat

DHCP Relay server :

The following table summarizes the available fields on this screen.

Table 6-1 Network Settings> Home Network> LAN Settings

Item	Description
IP LAN Settings	
IP address	Enter the IP address of the LAN that you want to assign LTE modem standard decimal, eg. 192.168.1.1 (the default setting).
mask	Enter the subnet mask in standard decimal, for example. 255.255.255.0 (the default setting). LTE modem calculate subnet mask automatically based on your specified IP addresses. Subnet mask computed LTE modem does not need to be changed if

Item	Description
	instructions say otherwise.
Status DHCP server	
DHCP	<p>choose Allow, if you want LTE modem automatically connected computers and mobile devices assigning an IP address, gateway and DNS servers parameters. If you choose Prohibit, You will need IP addresses assigned to each device manually.</p> <p>If DHCP is enabled, it is necessary to set the following parameters.</p>
DHCP lease time	<p>Set how long the valid IP address assigned by the DHCP server. For example - 0 days, 12 hours, 0 minutes (default setting). The minimum rental period is 2 minutes, maximum after 31 days.</p>
Values IP addressing	
Initial IP Address pool Address	In this field, enter the starting value of the IP address pool.
The size of the pool	In this field, enter the desired size IP address pool.
DNS values	
DNS server 1 - 3	<p>Choose from ISP in the event that your provider (operator) assigns DNS server information (and the public IP address LTE modem). Choose DNS proxy, if you want LTE modem send its own address to clients in the local network. Choose User-defined, if you have the IP address of the DNS server available. IP address of the DNS server then type in the box on the right. If you choose user defined and leave the IP address at 0.0.0.0. user defined After clicking Use changes to It is not. If the second DNS server in order to set user defined and enter the same IP address as in the first, the setting changes user defined after clicking Use on It is not.</p> <p>If no DNS servers do not want to set, select It is not. In this case, it is necessary that the other network DHCP server, otherwise it will be necessary for all devices manually assign DNS server address. If you do not set the DNS server, you will need to remember the IP address of each computer to which you want to connect.</p>
Status DHCP relay	
DHCP Relay	<p>These fields appear if you disable the DHCP server. Choose Allow if you have the IP address of the DHCP server. Choose Prohibit if you do not have the IP address of the DHCP server. If you use DHCP relay is enabled, it is necessary to set</p>

Item	Description
	The following parameters.
Relay DHCP server	Enter the IP address of the DHCP server that you want to use.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

6.3 Static DHCP screen

This table allows you to assign IP addresses on the LAN specific devices based on their MAC addresses.

Each device on an Ethernet network has a unique MAC address (Media Access Control). The MAC address is assigned to the device from the factory and consists of six pairs of hexadecimal characters separated by colons, e.g. 00: A0: 5: 00: 00: 02.

6.3.1 Before

If you want to add the device to the list on screen **Static DHCP** determine its MAC address.

Using this screen, you can change your static DHCP LTE modem. Enter this screen by clicking on **Network Settings> Home Network> Static DHCP**.

Figure 6-3 Network Settings> Home Network> Static DHCP

#	Stav	Jméno hostitele	MAC adresa	IP adresa	Rezervovat
1	💡	HAL-9000	84:16:f9:3a:59:db	192.168.1.54	<input type="checkbox"/>

The following table summarizes the available fields on this screen.

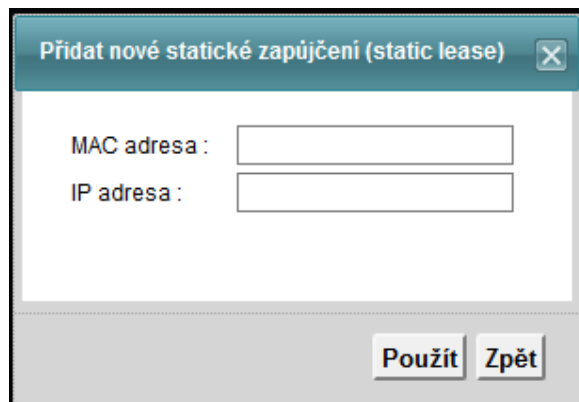
Table 6-2 Network Settings> Home Network> Static DHCP

Item	Description
Add new lending static (static lease)	Click this button to create a new record in the table.
#	This is the serial number.
State	In this field there is information on whether the device is connected to LTE modem.
Name	This field is the hostname of the client device.

Item	Description
MAC address	Each device on the LAN has a unique MAC address (Media Access Control), which consists of six pairs of hexadecimal digits separated by colons. Network interface card, eg. Ethernet adapter has a fixed address. This address is assigned based on the industry standard, which ensures that no other adapter has a similar address.
IP address	IP address of the device.
Book	By checking this box you book the IP address for the device (based on MAC addresses and host names). If you check the box in the table header will be reserved IP addresses for all devices on the list. The table can be located up to 128 entries.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.
Restore	Clicking Restore make reload the DHCP table.

If you click on the button **Add new lending static (static lease)** on the screen **static DHCP** the following dialog box.

Figure 6-4 Static DHCP: Add new lending static (static lease)



The following table summarizes the available fields on this screen.

Table 6-3 Static DHCP: Add new lending static (static lease)

Item	Description
MAC Address Enter	the MAC address of the device you want to add.
IP address	Enter the IP address you want the device with the MAC address on the network assigned.

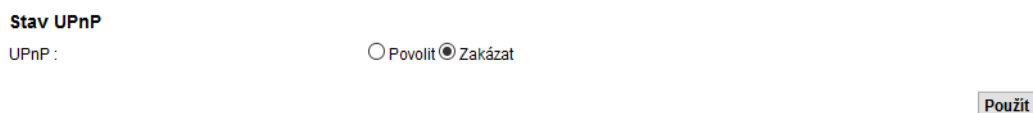
Item	Description
Use	Clicking Use save your changes.
back	Clicking back to exit without saving.

6.4 UPnP Screen

Universal Plug and Play (UPnP) is a set of networking protocols announced by the UPnP Forum. The goal of UPnP is to allow easy connection of peripheral computer components and simplify the implementation of networks in the home (data sharing, communications, and entertainment) and enterprises. UPnP device is able to dynamically join a network, obtain an IP address and identify devices on the network. If the device is not in use, it is able to automatically disconnect from the grid.

Using this screen, you can adjust your UPnP LTE modem. Click on **network settings > Home Network > UPnP**.

Figure 6-5 Network Settings> Home Network> UPnP



The following table summarizes the available fields on this screen.

Table 6-4 Network Settings> Home Network> UPnP

Item	Description
UPnP	selecting Allow activate UPnP. Please note that by using UPnP or device, anyone can open a page of the Web configuration interface without knowing the IP address LTE modem (to access it, however, will still need a user name and password).
Use	Clicking Use save your changes.

6.5 Screen UPnP list

If UPnP is enabled, this screen is a list of all UPnP devices that LTE modem network identifies.

Click on **network settings > Home Network > UPnP list**.

Figure 6-6 Network Settings> Home Network> UPnP list

#	Protokol	Cílová IP adresa	Externí port	Interní port
---	----------	------------------	--------------	--------------

The following table summarizes the available fields on this screen.

Table 6-5 Network Settings> Home Network> UPnP list

Item	Description
#	Serial number entry in the table.
Protocol	IP protocol appropriate UPnP devices or applications on the network.
Destination IP Address	IP address of the UPnP device or application on the network.
external port	External (public WAN) port that LTE modem assigned to the application.
internal port	Internal (LAN) port that LTE modem assigned to the application.
Restore	Clicking Restore make reload the table.

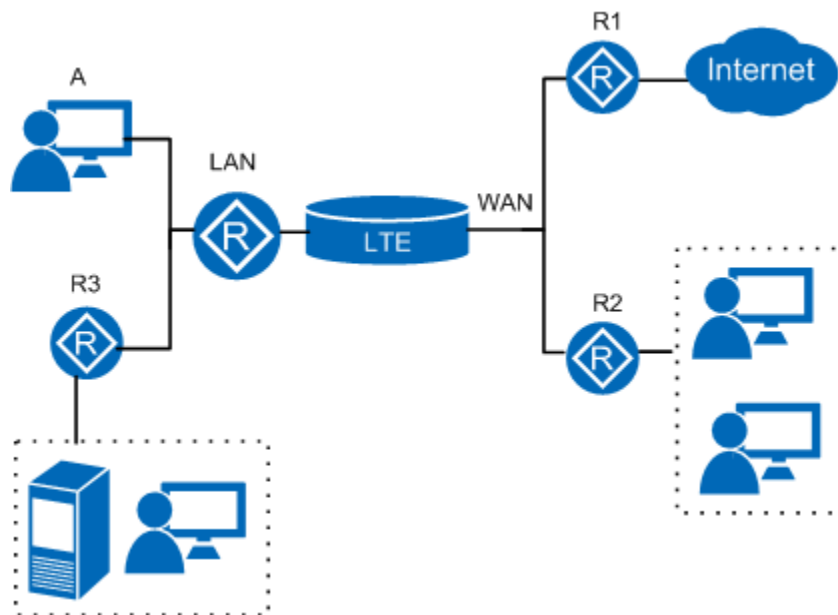
7 static routing

7.1 Overview

LTE modem normally uses the default gateway to route outgoing traffic from computers on the LAN to the Internet. To make LTE modem to send data to the devices that are not available through the default gateway, use static routing.

For example, the following image is a computer (**AND**) connected to the LAN interface LTE modem. LTE modem communication channels most from your computer **AND** on the internet through the default gateway LTE modem (**R1**). One static routing to create a connection to the services offered by your ISP - **R2**. Another route to create a separate communication networks for a router connected to the local network - **R3**.

Figure 7-1 Example static routing topology



7.2 Configuration of static routing

Use this screen to view and configure IPv4 static routing LTE modem. Enter this screen by clicking on **Network Settings> Static Routing**.

Figure 7-2 Network settings> Static Routing

#	Aktivní	Stav	Jméno směrování	Cílová IP adresa	Brána	Maska subsítě	Rozhraní	Upravit
---	---------	------	-----------------	------------------	-------	---------------	----------	---------

The following table summarizes the available fields on this screen.

Table 7-1 Network settings> Static Routing

Item	Description
Add new static routing Static Routing	Click this button to add a new static IPv4 routing LTE modem.
#	Serial number entry.
Active	This field indicates whether the static route is active or not. Symbol yellow light bulb means that the static route is active. Symbol gray bulb means that the static route is not active.
State	This field indicates whether the corresponding static routing currently used or not. Symbol yellow light bulb means that the static route is currently used. Symbol gray bulb means that the static route is currently in use.
name routing	This field is the name of the relevant static routing.
Destination IP Address	This field specifies an IPv4 network address of the destination routing. Routing is always based on the numbering on the network.
Gate	IPv4 gateway address. Gateway may be a router (router) or switch (switch) located in the same network segment as the LAN or WAN interfaces of the modem. Gateway is used to route packets to their destination.
mask	This parameter specifies the subnet mask of destination routing.
Interface	This parameter defines the interface processes the data stream processed by the competent routing.
adjust	Click on the icon adjust open the dialog for the relevant static routing. Click on the icon Remove remove the static routing.

7.2.1 Add / Edit Static Routing

Click on the button **Add new static routing** on the screen **Static routing**, or on the icon **adjust** on the right side of the table. The following dialog box. Using this window, you can set the parameters of static routing.

Figure 7-3 Static Routing: Add / Edit

The following table summarizes the available fields on this screen.

Table 7-2 Static Routing: Add / Edit

Item	Description
Active	Check to relevant rule of static routing.
name routing	Enter a name for the static routing.
Destination IP Address	This parameter specifies the IP network address of the destination routing. Routing is always based on the numbering on the network. If you want to direct the guest to a single device, use a subnet mask of 255.255.255.255. This will correspond to the numbering of the network ID of the host device.
Gate	You can specify whether you want to direct packets to IP gateway address or bound interface. To enter the IP address of the gateway, enter the gateway address for the next hop in the network. Gateway may be a router (router) or switch (switch) located in the same network segment as the LAN or WAN interfaces of the modem. Gateway is used to route packets to their destination.
mask	Enter the subnet mask.
Interface	You can specify whether you want to direct packets to IP gateway or a particular interface. If you want to use a specific interface, select the field from the drop down list, select the interface over which you want to direct the flow of data.

Item	Description
Use	Clicking Use save your changes.
back	Clicking back to exit without saving.

8 Network Address Translation (NAT)

8.1 Overview

NAT (Network Address Translation - NAT, see the definition of RFC 1631) is in computer networks method of modifying traffic passing through the router rewriting the source or destination IP addresses, or even heads higher layer protocols.

8.1.1 What You Need to Know

Before reading this chapter is to be familiar with the following terms.

Internal / external and global / local

Parameter internal / external host indicates the position relative to the LTE modem. For example, computers and devices in your home network, the internal host devices, while the web servers on the Internet are external host device.

Parameter global / local refers to the IP address of the host device in the packet as it passes through the router. The local address refers to the IP address of the host device when moving a packet on the local network, while global address is the IP address of the host device in the packet data stream identical WAN.

NAT

Basically, NAT changes the source IP address of a data packet from the customer (ie internal, local address) to another (the inside global) before directing the packet to the WAN. Once a response is received, performs NAT destination address (the inside global) back to the inside local address, before directing the visitors to the internal device.

port forwarding

Port forwarding is a list of internal (ie. Hidden behind NAT on the LAN) servers, such as Web or FTP, which can be made visible from the outside, even though it operates through NAT entire internal network from the outside as a single computer.

More information

A more detailed description of the NAT technology is contained in chapter 8.6 Technical details.

8.2 Screen Port Forwarding

using the screen **port forwarding** You can set the bridge for incoming service requests to the local network.

Redirect to the local IP address of the server can be a single port number or range. The port number is also used to identify services such as. Web service running on port 80, FTP on port 21. For example, in some cases, such as unknown services or where one server supports multiple services (such is the Web server and FTP), it is better to specify port range. That port or range can assign just one IP address.

For more information about port numbers, see RFC 1700's.



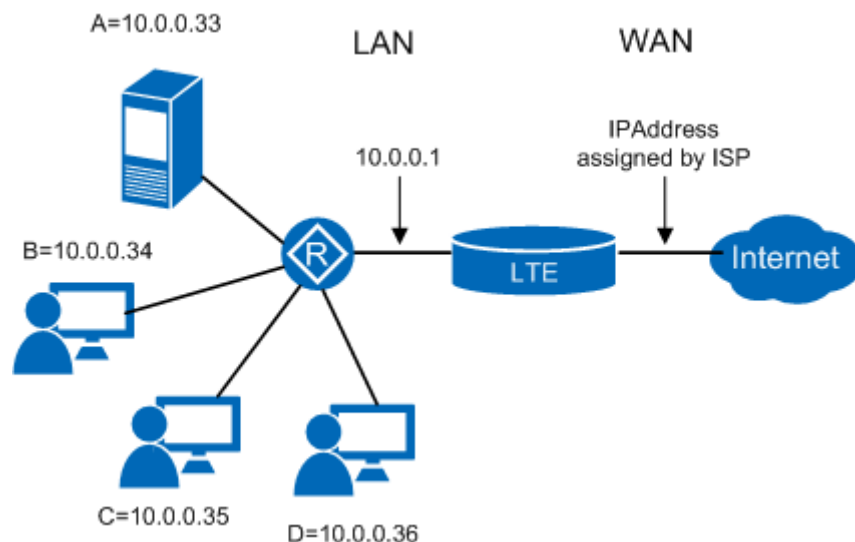
NOTE

Many ISPs not allow startup server processes (such as Web or FTP servers) from a home address. Providers may periodically verify the occurrence of such processes and in case of doubt to block your account. If you have any doubts or questions, please contact your internet service provider (operator).

Configuring Servers for port forwarding (example)

Let's say you want to assign ports 21 - 25 one server FTP, Telnet and SMTP (**AND** the figure), another port 80 (**B** pictured) and assign a default server IP address 10.0.0.35 third (**C** in the picture). While you can assign LAN IP address, Internet service provider assigns the WAN IP address. The entire network operates outside NAT (the Internet) as a single host device.

Figure 8-1 Example multiple servers hidden behind one NAT network



Screen Port Forwarding 8.2.1

Enter the screen **port forwarding** click on **Network Settings> NAT**.

Figure 8-2 Network Settings> NAT> Port Forwarding



The following table summarizes the available fields on this screen.

Table 8-1 Network Settings> NAT> Port Forwarding

Item	Description
Add new rule	Click this button to create a new port forwarding rule.
#	This is the serial number.
State	This field indicates whether the rule is active or not. Symbol yellow light bulb means that the rule is active. Symbol gray bulb means that the rule is not active.
name services	This is the name of the service. When the service was added manually, it will be shown here User Defined . This item can be adjusted by clicking on Change .
WAN interface	Identification of the WAN interface through which the service is diverted.
Initial WAN port	The first external port number identifying the service.
WAN port terminal	The number of the last external port identifying the service.
LAN start port	Internal Port Number first identifying the service.
LAN port terminal	Last number Internal Port identifying the service.
LAN IP address	This is the IP address of the server.
Protocol	IP protocol version supported by Virtual Server - TCP, UDP or TCP / UDP.
change	Click on the icon change You can modify the forwarding rule. Click on the icon Clear You can redirect the rule remove. Keep in mind that the following rules redirection after

Item	Description
	eliminate rules move one position up.

8.2.2 Screen Edit Port Forwarding

The following screen is used to add new or edit an existing port forwarding rules. Click on the button **Add new rule** on the screen **port forwarding** or click **adjust** in line with the existing rule.

Figure 8-3 Port Forwarding: Add / Edit

The following table summarizes the available fields on this screen.

Table 8-2 Port Forwarding: Add / Edit

Item	Description
service name	Names forwarding rule using standard symbols (A - Z, and - of 1 - 2 etc.).
WAN interface	Identification of the WAN interface through which the service is diverted.
Initial WAN port	The default destination port of data packets. To forward only one port, enter the same port number also in the field WAN port terminal. To redirect a range of ports, type in the box number of the start port and end port number field, enter WAN port terminal.

Item	Description
WAN port terminal	Enter the number of the terminal port default destination port from the range. To forward only one port, enter the port number in the box Initial WAN port and the same number should be here. To redirect a range of ports, type in the box end port number and port number of the initial field, enter Initial WAN port above.
LAN start port	The port number on which to LTE via a modem to forward the incoming data stream. To enter the port range in this field, enter the starting port number.
LAN port terminal	End port number redirected range.
LAN IP address	Enter the internal IP address of the virtual server that you want to use.
Protocol	Select the protocol supported by the virtual server. the options are TCP, UDP or TCP / UDP.
Use	Clicking Use save your changes.
back	Clicking back to return to the previous screen without saving.

8.3 Screen DMZ

DMZ (demilitarized zone in English) is a physical or logical subnetwork that is for safety reasons separate from other devices. All packets received WAN LTE modem will be forwarded to the default server that you set.

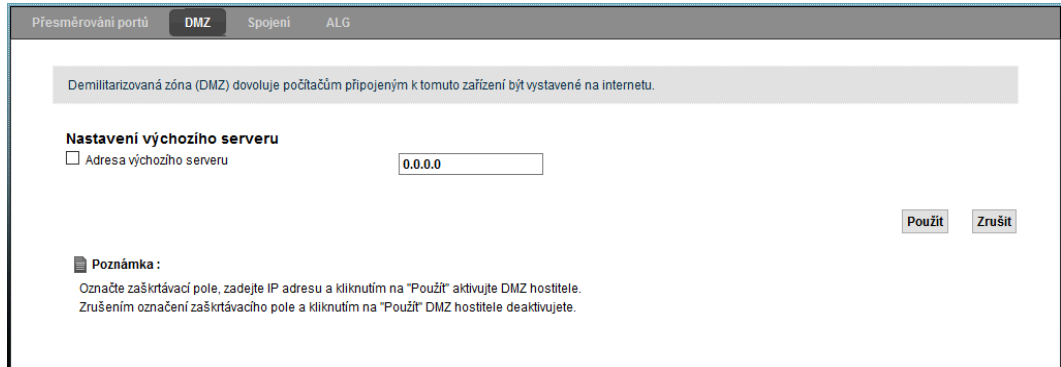
Enter this screen by clicking on **Network Settings> NAT> DMZ.**



NOTE

All settings on this screen have a higher priority than those configured on the screen **Network Settings> NAT> Port Forwarding.**

Figure 8-4 Network Settings> NAT> DMZ



The following table summarizes the available fields on this screen.

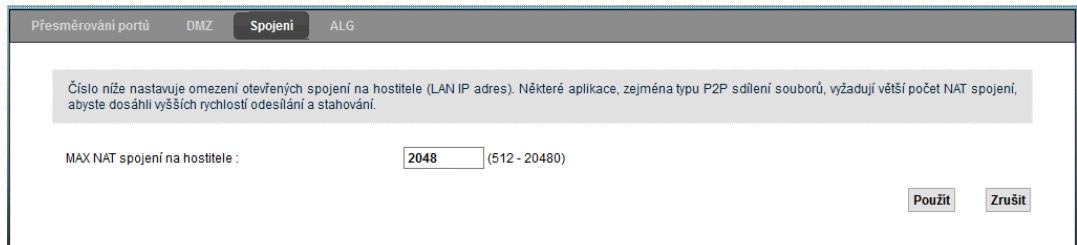
Table 8-3 Network Settings> NAT> DMZ

Item	Description
Address default server	Enter the IP address of the DMZ host, if available. Value 0.0.0.0 It means that this feature is disabled.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

8.4 Screen connection

using the screen **Connection** You can set the limit concurrent NAT connection for each client device. Enter this screen by clicking on **Network Settings> NAT> Connections**.

Figure 8-5 Network Settings> NAT> Connections



The following table summarizes the available fields on this screen.

Table 8-4 Network Settings> NAT> Connections

Item	Description
MAX NAT connection to the host	In this field, enter the maximum number of concurrent NAT connection for each client device. If applications like P2P uses only a few applications, you can use this number to increase to achieve higher download speeds. However, if a lot of these applications, it is recommended to reduce this number to prevent the depletion of available NAT connection.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

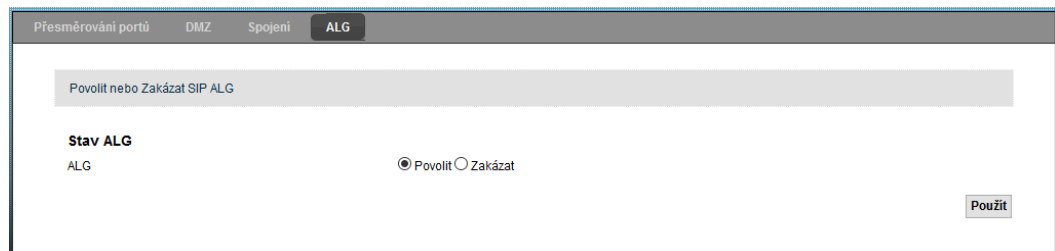
8.5 ALG Screen

using the screen **ALG** You can enable or disable the application layer gateway (ALG) for SIP. Clicking **Use** save your changes.

Gateway SIP ALG allows SIP redirect calls through the NAT data stream through NAT. After registration LTE modem for SIP server, SIP ALG gateway translates a private IP address LTE modem inside the SIP data stream to a public IP address. After activating the SIP ALG gateway eliminates the need to use any communication STUN or outbound proxy.

In an LTE network can easily be overloaded LTE interfaces for sending repeated requests for registration with the SIP server because of a timeout session. The default timeout connection with NAT (3600 seconds) reduces the likelihood of overload.

Figure 8-6 Network Settings> NAT> ALG



8.6 Technical details

The subsections below describe the technological aspects of the topics dealt with in this chapter.

8.6.1 Basic definitions NAT

Parameter internal / external host indicates the position relative to the LTE modem. For example, while computers and devices on your home network, the internal host devices, while the web servers on the Internet are external host device.

Parameter global / local refers to the IP address of the host device in the packet as it passes through the router. The local address refers to the IP address of the host device when moving a packet on the local network, while global address is the IP address of the host device in the packet data stream identical WAN.

Note that while the parameter inside / outside refers to the location of the host parameter global / local refers to the IP address of the host in the data packet. Therefore, the internal local address (ILA) IP Address internal host assuming that the packet is still in the local network, while the inside global address (IGA) is the IP address of an internal host identical, but the external network (WAN). The following table summarizes the above definition.

Table 8-5 The basic definition of NAT

Term	Description
Internal	This refers to the host on the LAN.
External	This refers to the host on the WAN.
Local	Address of the packet (source or destination) as it moves through the LAN.
Global	Packet address (source or destination) during its movement in the WAN.

While NAT never occurs to change the address (whether local or global) external host.

8.6.2 What happens during NAT

Basically, NAT changes the source IP address of a data packet from the customer (ie internal, local address) to another (internal, global) before directing the packet to the WAN. Once a response is received, performs NAT destination address (the inside global) back to the inside local address, before directing the visitors to the internal device. While NAT never occurs to change the address (whether local or global) external host.

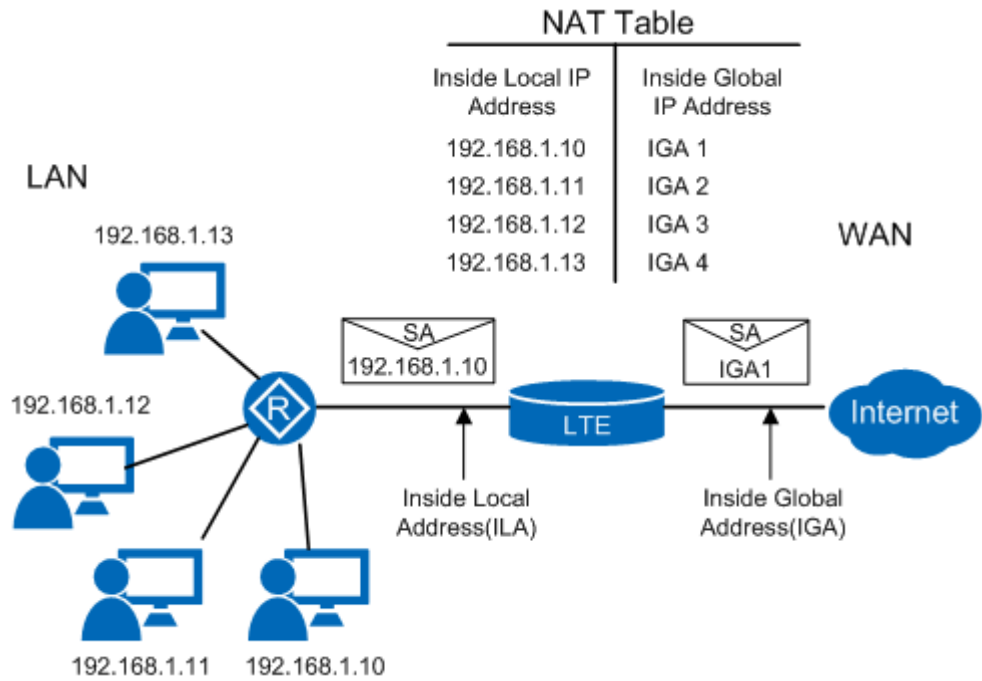
Global IP address of the internal host can be static or dynamic and is assigned ISP. In addition, you can in your local network servers to specify, such as a Web server and Telnet, which will be accessible from the outside. If you do not specify any servers, NAT offers the additional benefit in the form of firewall protection. Without a definition of specific server will LTE modem to filter all incoming requests and thus hinder possible intruders from entering the network. For more information on NAT, see the *RFC 1631, The IP Network Address Translator (NAT)*.

8.6.3 How NAT works

Each data packet has two addresses - source and destination. As for outgoing packets are concerned, internal local address (ILA) is the default address on the LAN and the inside global address (IGA) is the default address WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT translates the private (local)

IP addresses to escape the global address, which is required for communication with hosts on other networks. It replaces the original default IP address (and source port number, TCP or UDP NAT translation at N: 1 or M: N) in each packet, which is then sent to the Internet. LTE modem keeps a record of the original IP addresses and port numbers so incoming packets can easily restore the original values. The following diagram describes the principle described above.

Figure 8-7 How NAT works



9 dynamic DNS

9.1 Overview

This chapter describes how to configure your LTE modem for use with dynamic DNS. Dynamic DNS allows you to replace the existing, dynamic IP address with one or many dynamic DNS services that cause you could any external service contact (eg. In applications such as NetMeeting or CU-SeeMe) Using this feature, you can also **access your FTP server or Web the site through the domain name (eg. myhost.dhs.org where " myhost " is the name of their discretion)**, which is in contrast to the constantly changing IP address permanent. Friends and acquaintances will be able to contact you without you without knowing your IP address.

First you need to register a DDNS account with services or www.dyndns.org www.no-ip.com. It is designed for situations where the connection or the DHCP server does not assign a fixed IP address. Dynamic DNS service provider will then send the login information.

9.1.1 What You Need to Know

DynDNS Wildcard or "wild card"

Activating the function wild card causes the address * .yourhost.dyndns.org (with any prefix) will be connected to the same IP address as the domain name yourhost.dyndns.org. This feature is useful if you want to use URL www.yourhost.dyndns.org and get to the destination of your domain name.

Dynamic DNS can not be used if you have a private WAN IP address.

9.2 Dynamic DNS Screen

10 firewall

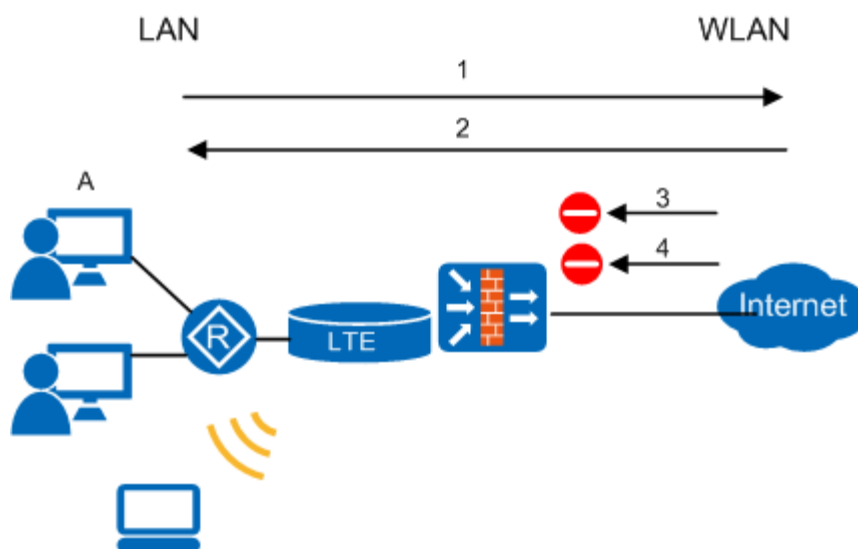
10.1 Overview

Using the menu Firewall configuration interface LTE modem can activate the firewall protection to prevent intrusion into your network attackers. By default, the firewall is set as follows:

- It allows data stream originating from computers in the LAN and WLAN to get into all the other networks.
- Blocks the flow of data from other networks from encroaching on the LAN and WLAN.

The default firewall settings are shown in the following diagram. User **AND** can initiate IM conversations from the LAN to the WAN (**1**). Reverse operation for this session is also permitted (**2**). Other data stream from the WAN is not blocked (**3** and **4**).

Figure 10-1 The default firewall settings



10.1.1 What You Need to Know

DoS

Denial of service attacks (Denial of Service, DoS) targets the devices and networks with Internet access. Their goal is not to acquire sensitive information, but to disable a device or network operation - allowing users to him will no longer have access. LTE modem is configured to known methods DoS attacks, was able to detect and avert.

firewall

Firewall LTE modem physically separates the LAN / WLAN to WAN and acts as a safety check of all data flow between networks.

The firewall also protects against denial of service attacks (DoS). The purpose of this LTE modem is to allow private LAN securely connect to the Internet. The LTE modem can be used to prevent theft, destruction or misuse of sensitive data and system logs, which may represent an important part of your network infrastructure.

LTE modem is the interface between LAN / WLAN and Internet. Because it can serve as a secure gateway for all data traffic between the Internet and LAN.

LTE modem includes two Ethernet connectors - WAN PoE (Power over Ethernet) LAN

- that network is physically divided into two parts. Connector WAN (Wide Area Network) is used to connect the outdoor unit receiving the LTE network data signal.

Connector LAN (Local Area Network) is used to connect local area networks, which must be secured from the outside. Computers that are part of the local network will have access to Internet services such as e-mail, FTP or Web pages. By default, however, the computer externally inaccessible without prior authorization to use a specific network services.



NOTE

Using a firewall can impact system performance.

ICMP

ICMP (Internet Control Message Protocol) used operating systems in a network for sending service information, such as error messages to indicate that the requested service is not available or the necessary computer or router is not reachable. ICMP messages are constructed above the IP layer; usually the IP datagram that caused the ICMP response. IP layer encapsulates the appropriate ICMP message to the new IP header (to get the ICMP message back to the original sender) and customary manner resulting datagram sends.

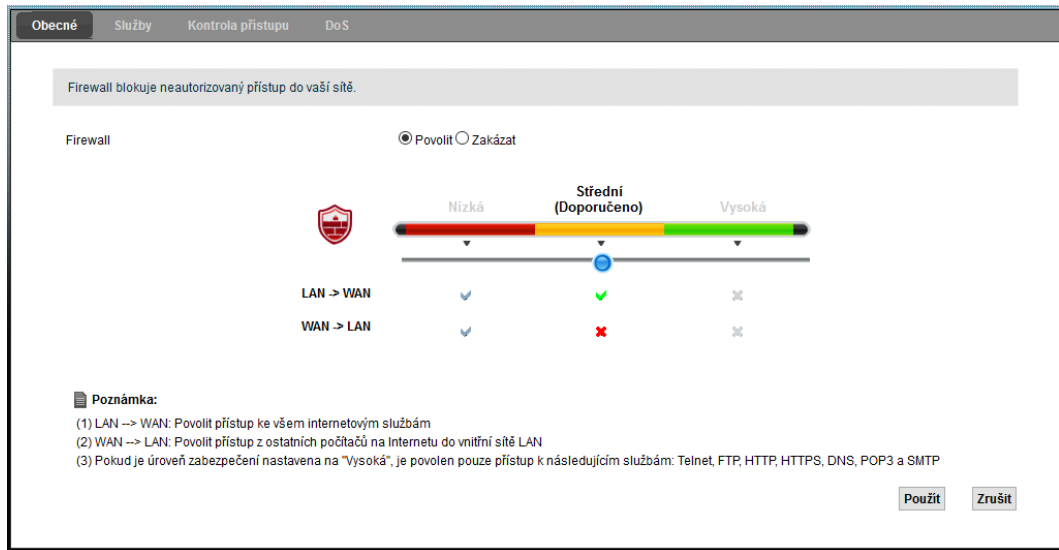
More information

For more information about firewall, see chapter 10.6 Technical details about the firewall.

10.2 General Screen

Through this screen, you can firewall enabled or disabled. screen
In general by clicking on Security> Firewall.

Figure 10-2 Security> Firewall> General



The following table summarizes the available fields on this screen.

Table 10-1 Security> Firewall> General

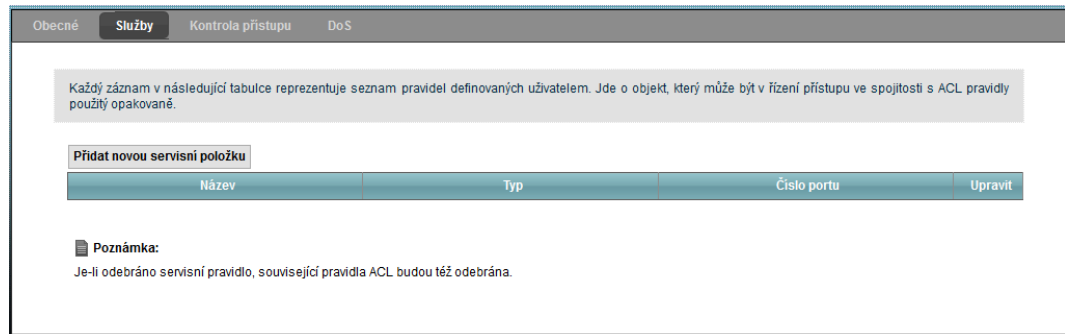
Item	Description
firewall	selecting Allow activate the firewall. LTE modem will perform access control and protect the network from attacks, denial of service (DoS).
Low / Medium / High bundles	Choice low allow all data transmissions over the LTE modem, a LAN -> WAN and WAN -> LAN. Choice Medium will only allow data flow in the direction of LAN -> WAN. All inbound traffic from the WAN will be blocked. Choice high will only allow data flow from Telnet, FTP, HTTP, HTTPS, DNS, POP3 and SMTP from the LAN to the WAN. All other data flow will be blocked.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

10.3 Screen Services

On this screen is a list of configured services / service items. To open this screen, click on **Security> Firewall> Services**. Before creating rules using the menu **Security> Firewall> Access Control> Add new ACL rule**

it is first necessary to add at least one maintenance item on this screen.

Figure 10-3 Security> Firewall> Services



Individual fields are described in the following table.

Table 10-2 Security> Firewall> Services

Item	Description
Add a new service item	Click this button to add a new service.
Name	The name of the service items.
Type	The type of protocol used by the service (TCP, UDP, ICMP or Other).
port number	In this field there are ports defining the service.
adjust	Click on the icon <i>adjust</i> You can edit the appropriate service entry. Click on the icon <i>Remove</i> You can select the appropriate service to remove. Keep in mind that the following items after removing shifted one position above. Removing service items will also lead to the removal of interconnected ACL rule set on the screen Security> Firewall> Access Control.

10.3.1 Screen Add a new maintenance item

Use this screen to configure the service to be used in the ACL rules created using the menu **Security> Firewall> Access Control> Add new ACL rule**. To access this menu, go to the screen **Security> Firewall> Services** and click on **Add a new service item**.

Figure 10-4 Security> Firewall> Services> Add new service item

Individual fields are described in the following table.

Table 10-3 Security> Firewall> Services> Add new service item

Item	Description
Name	A descriptive name for the service.
Type	The type of protocol used by the service (TCP, UDP, ICMP or Other).
Enter the protocol number	Protocol type of service.
Source port, destination port	The source port number specifies the port data stream. The destination port defines the port number of the host device to which the data stream to be directed services. choose easy if the service uses only one source or destination port, and enter the number. choose Range if the service uses two or more source or destination ports, and enter the appropriate range . For example, suppose you want to define the Gnutella service. Select a type TCP and enter the port range 6345 - 6349th
Use	Clicking Use save your changes.
back	Clicking back to exit without saving.

4.10 Screen Access Control

The following screen, click on **Security> Firewall> Access Control**

Part of the screen is a list of configured ACL rules for incoming or outgoing data stream.

Figure 10-5 Security> Firewall> Access Control

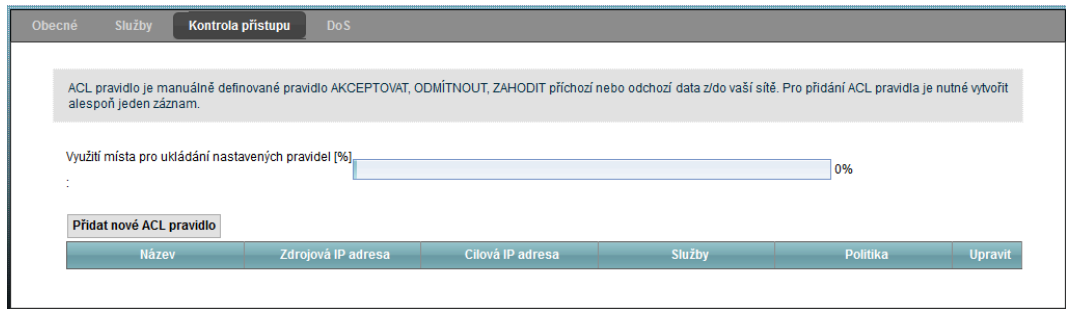
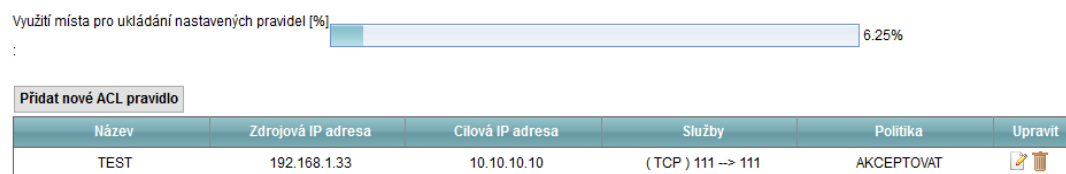


Figure 10-6 Security> Firewall> Access Control (after adding ACL rules)



Individual fields are described in the following table.

Table 10-4 Security> Firewall> Access Control

Item	Description
Use of space for storing the set of rules (%)	This indicator shows the percentage memory is full rules LTE modem. If the indicator is almost full, you may need before you add the new ACL rules to remove one of the existing ones.
Add new ACL rule	Click this button to add a rule to filter incoming or outgoing data stream.
Name	Name of the relevant rules.
Source IP address	This field is the source IP address to which the rule applies. Note that if this field is empty, it is the same as if the camera is set Any .
Destination IP Address	This field is the destination IP address to which the rule applies. Note that if this field is empty, it is the same as if the camera is set Any .
service	This field is the protocol type and port range defining a service to which the rule applies.
Policy	This field is designed to be handled according to the rules of data packets - whether they will be discarded (DISCARD) discarded with sending TCP reset packet or ICMP unreachable recipients (REFUSE) or received (ACCEPT).
adjust	Click on the icon adjust You can edit the policy.

Item	Description
	Click on the icon Clear You can remove the rule. Keep in mind that the following items after removing shifted one position above.

10.4.1 Screen Add New / Edit ACL Rule

Click on the button **Add new ACL rule** or icon **adjust** in the line of the current ACL rules to screen **Access control**. The following screen will appear.

Figure 10-7 Security> Firewall> Access Control> Add New / Edit ACL Rule

The screenshot shows a configuration window titled "Přidat nové ACL pravidlo" (Add New ACL Rule). The fields are as follows:

- Název filtru: [Text input field]
- Typ zdrojové adresy: Jednoduchá (dropdown)
- Počátek rozsahu zdrojové IP adresy: [Text input field]
- Konec rozsahu zdrojové IP adresy: [Text input field]
- Typ cílové adresy: Jednoduchá (dropdown)
- Počátek rozsahu cílové IP adresy: [Text input field]
- Konec rozsahu cílové IP adresy: [Text input field]
- Vyberte protokol: Vybrat službu (dropdown)
- Protokol: TCP (dropdown)
- Číslo protokolu: [Text input field] (0-255)
- Zdrojový port: Jednoduché (dropdown) [Text input field] - [Text input field]
- Cílový port: Jednoduché (dropdown) [Text input field] - [Text input field]
- Politika: AKCEPTOVAT (dropdown)
- Směr: LAN -> ZAŘÍZENÍ (dropdown)

Buttons at the bottom right: Použít, Zpět.

Individual fields are described in the following table.

Table 10-5 Security> Firewall> Access Control> Add New / Edit ACL Rule

Item	Description
filter name	Enter a descriptive name using 16 alphanumeric characters without spaces, hyphens, and underscores. Filter name is required for the ACL rule. If you are editing an existing ACL rule, this field is intended only for reading.
Type source address	Choose easy or Range depending on whether you want ACL rule relate to a single IP address or range. Choose

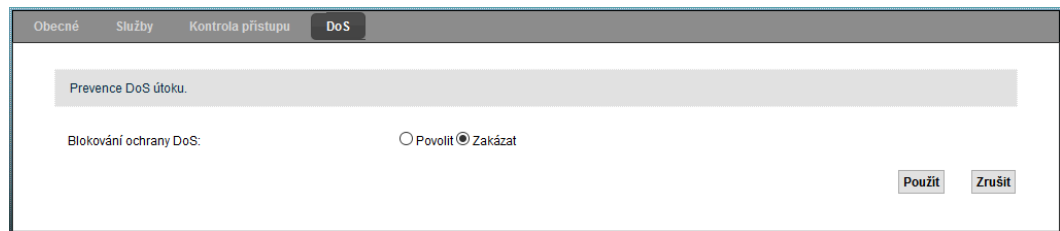
Item	Description
	any , If you want to apply the rule to all source IP addresses.
The beginning of the range of the source IP address	Enter the beginning of the range of source IP addresses.
The end of the range of the source IP address	Enter the end of the range of source IP addresses.
Select the type of destination address easy or Range depending on whether you want ACL rule relate to a single IP address or range. Choose any , If you want the rule to apply to all the destination IP addresses.	
The beginning of the destination IP address range	Enter the beginning of the target range of IP addresses or a single IP destination address.
End of the range the destination IP address	Enter the end of the range of target IP addresses.
Select Protocol	From the dropdown list name configured services or Select service to configure a new service items.
Protocol	This item will be available when the menu Select Protocol you select Select service . Select the type of protocol used by the service (TCP, UDP, ICMP or Other).
Protocol number	This item will be available when the menu Protocol you select Other. Enter the number of protocol appropriate services to which you want to relate ACL rule.
source port	This field will only be displayed if the menu Select Protocol choose Select service and the menu Protocol choose TCP or UDP. Choose easy or Range and enter the number (ie. a range of numbers) source port. Choose any , If you want the rule to apply to all source ports.
destination port	This field will only be displayed if the menu Select Protocol choose Select service and the Protocol menu select TCP or UDP. Choose easy or Range and enter the number (ie. a range of numbers) destination port. Choose any , If you want the rule to apply to all destination ports.
Policy	Use this drop-down menu to specify how it will be treated according to the rules of data packets - whether they will be discarded (DISCARD) discarded with sending TCP reset packet or ICMP unreachable recipients (REFUSE) or received (ACCEPT).

Item	Description
Direction	Use this drop-down menu to select the direction of data flow specified by this rule. Available options are LAN -> EQUIPMENT, LAN -> WAN, WAN -> LAN and WAN -> DEVICE .
Use	Clicking Use save your changes.
back	Clicking back to exit without saving.

10.5 Screen DoS

The following screen, click on **Security> Firewall> DoS**. On this screen you can enable or disable protection against DoS attacks (denial of service attacks).

Figure 10-8 Security> Firewall> DoS



Individual fields are described in the following table.

Table 10-6 Security> Firewall> DoS

Item	Description
Blocking DoS protection	The attack DoS (denial of service, in English Denial of Service) involves flooding your internet connection invalid data packets and connection requests, which leads to clogging up bandwidth preventing access to the Internet. By setting Allow DoS attack protection enabled, settings Prohibit off .
Use	Clicking Use changes made on the screen to save DoS.
Cancel	Click on Cancel restore previous settings in this section.

10.6 Technical details about firewall

The subsections below describe the technological aspects of the topics dealt with in this chapter.

10.6.1 Tips to strengthen security firewall

Step 1 Change the default password to access the web configuration interface.

step 2 Before you connect to a network, think about access control.

step 3 Restrict access to your LTE modem.

step 4 Do not enable any of the local services that do not plan to use (eg. Telnet or FTP).

Each active service may pose a potential safety hazard. A determined hacker can find a way to exploit active service access to your network.

step 5 Active local services protect against misuse. Protect them so that to allow communication only some peer protocols and set rules to block packets for the services at specific interfaces.

step 6 Keep the firewall in a secure (locked) room.

---- End

10.6.2 Other safety tips



NOTE

Incorrect firewall settings can lead to blockage harmless stream or vice versa pose a security risk to the LTE modem and your network. When creating or deleting firewall rules caution. Always test the rules created.

Before creating exceptions or rules consider the following:

Step 1 This rule does not prevent users on the LAN to access important resources on the Internet?

For example, if you block access to IRC - not connected to the network users who require this service?

step 2 It is not possible to rule better adapted to the purpose? It glycol example, according to the rules of access

IRC is blocked for all users, you can not access some of them permit?

step 3 It does not constitute a rule that allows Internet users to access resources in the local

network security risk? For example, if open FTP ports (TCP 20, 21) for Internet traffic to the local network, it may be that Internet users will be able to connect to computers running FTP servers.

step 4 Not newly created rule conflicts with an existing?

---- End

Once the answer to the above questions is a simple matter of adding rules to fill the relevant fields in the web interface.

11

The MAC address filter

11.1 Overview

This chapter deals with filtering MAC addresses.

using the screen **The MAC address filter** You can grant access to LTE modem only certain devices based on their MAC addresses. These rules apply to wired and wireless connections.

11.1.1 What You Need to Know

Each device on an Ethernet network has a unique MAC address (Media Access Control). The MAC address is assigned to the device from the factory and consists of six pairs of hexadecimal characters separated by colons, e.g. 00: A0: 5: 00: 00: 02. To add devices to the filter you need to know its MAC address.

11.2 Screen MAC address filter

using the screen **The MAC address filter** You can allow access to the LTE modem only to selected client devices. Click on **Security > MAC address filter**. selecting **Allow** displays additional options, see below.

Figure 11-1 Security> MAC address filter

Filtr MAC adres: Povolit Zakázat Filtr MAC adres vypnutý

Nastavit	Povolit	MAC adresa
1	<input type="checkbox"/>	84:16:F9:3A:59:DB
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	
8	<input type="checkbox"/>	
9	<input type="checkbox"/>	
10	<input type="checkbox"/>	
11	<input type="checkbox"/>	
12	<input type="checkbox"/>	
13	<input type="checkbox"/>	
14	<input type="checkbox"/>	
15	<input type="checkbox"/>	
16	<input type="checkbox"/>	
17	<input type="checkbox"/>	
18	<input type="checkbox"/>	
19	<input type="checkbox"/>	
20	<input type="checkbox"/>	
21	<input type="checkbox"/>	
22	<input type="checkbox"/>	
23	<input type="checkbox"/>	
24	<input type="checkbox"/>	
25	<input type="checkbox"/>	
26	<input type="checkbox"/>	
27	<input type="checkbox"/>	
28	<input type="checkbox"/>	
29	<input type="checkbox"/>	
30	<input type="checkbox"/>	
31	<input type="checkbox"/>	
32	<input type="checkbox"/>	

The following table summarizes the available fields on this screen.

Table 11-1 Security> MAC address filter

Item	Description
The MAC address filter	If you choose Allow will have LTE modem access only those devices in the lists from which the check field Allow . Device with a MAC address that is not on this list, access to the LTE modem denied. If you choose Prohibit will not have LTE modem to access the device from the list, for which the check box Prohibit . Device with a MAC address that is not on this list, access to the LTE modem enabled. If you choose The MAC address filter is switched off , will not take place any filtering device based on its MAC address.
set	This is the serial number of the MAC addresses.

Item	Description
Allow	check the box Allow , if you want the device to the appropriate MAC address to allow access to the LTE modem.
Prohibit	check the box Prohibit , if you want the device to the appropriate MAC address to disable access to the LTE modem.
MAC address	Enter the MAC address of the wireless LAN station or device that you want to allow or deny access to the LTE modem. MAC address must be entered in a valid format, ie. The six pairs of hexadecimal characters separated by colons, eg. 00: A0: C5: 00: 00: 02.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

12 parental

12.1 Overview

Parental Control allows you to block access to certain websites based on their URLs. You can also determine time intervals or days after which the parental lock is on.

12.2 Screen Parental

On this screen you can enable Parental Control, show the specific rules and timetable. The following screen, click on **Security> Parental**.

Figure 12-1 Security> Parental

Obecné
Rodičovský zámek: Povolit Zakázat (pokud je zaškrtnuto "Zakázat", nastavení nejsou aktivní)

Přidat nový PCP

#	Stav	Název PCP	Síťový uživatel (MAC)	Nastavení přístupu ke službám	Síťová služba	Blokovaná stránka	Upravit
							Použít Zrušit

Figure 12-2 Security> Parental control (after adding a new PCP)

Obecné
Rodičovský zámek: Povolit Zakázat (pokud je zaškrtnuto "Zakázat", nastavení nejsou aktivní)

Přidat nový PCP

#	Stav	Název PCP	Síťový uživatel (MAC)	Nastavení přístupu ke službám	Síťová služba	Blokovaná stránka	Upravit
1	💡	TEST	Vše	M T W T F S S 00:00-23:59	Žádná	Žádná	
							Použít Zrušit

The following table summarizes the available fields on this screen.

Table 12-1 Security> Parental

Item	Description
parental	selecting Allow activate the parental lock.
Add a new PCP	To add a new rule parental control, click this button.
#	This is the serial number of rules.
State	This field indicates whether the rule is active or not. Symbol yellow light bulb means that the rule is active. Symbol gray bulb means that the rule is not active.
name of PCP	Name of the relevant rules.
Network user (MAC)	This field specifies the MAC address of the computer users on the LAN to which the rule applies.
Setting up access to services	In this area are given days and hours when the rule will be active parental control.
network service	For information about configuring network services. If no configured not, in this field stated None .
blocked page	Information about blocking certain websites. If no configured not, in this field stated None .
adjust	Click on the icon adjust open the dialog for the relevant rules. Click on the icon Clear You can remove the rule.
Use	Click on Use to save your changes settings LTE modem.
Cancel	Click on Cancel restore previous settings in this section.

12.2.1 Add New / Edit PCP

Click on the button Add a new PCP on the screen parental to add a new rule, or click on the icon adjust next to one of the existing rules. Using this dialog box you can set a rule limiting access and configure URL filtering, which if valid rules will not be available.

Figure 12-3 Add New / Edit PCP

Obecné

Aktivní

Název PCP (Parental Control Profile):

Profile):

Síťový uživatel:

Nastavení přístupu ke službám

Den: Každý den Pondělí Úterý Středa Čtvrtek
 Pátek Sobota Neděle

Čas (Začátek - Konec): **00:00 - 24:00**

Bez možnosti přístupu Autorizovaný přístup

Síťová služba

Nastavení síťových služeb: Vybraná služba(-y)

The following table summarizes the available fields on this screen.

Table 12-2 Add New / Edit PCP

Item	Description
In general	
Active	Check this box to activate the relevant rules.
Name of PCP (Parental Control Profile)	A descriptive name for the rule restricting access.
network user	Select from the drop-down list, a user on the LAN to which you want the rule to relate. If you choose Custom settings enter the MAC address below. If you choose All , rule will apply to all users on the LAN.
Setting up access to services	
Day	Check the box days of the week in which you want to enable Parental LTE modem.
Time (start end)	Enter the time scope of the rules of parental control in 24-hour format.
Time	Use the sliders to set the time interval after which the user will have the LAN enabled access to services.
network service	
setting network If you select Block , LTE modem will block access to the web	

Item	Description
services	pages with URLs in the table below. If you select Allow, LTE modem will block access to all websites except those that are found in the table below.
Add new service	Click this button to add a new web service to list. enter Service Name, Protocol and port each rule.
#	This is the serial number of rules. Check the box to activate the rule.
name services	Name of the relevant rules.
Protocol / port	Type of protocol and port number of the rule.
adjust	After adding a new service displays icons adjust and Clear. Click on the icon adjust open the dialog for the relevant rules. Click on the icon Clear You can remove the rule.
Keyword blocked sites / URLs	The list of blocked sites by keywords in the URL. Clicking Add open a dialog box in which you can enter keywords in the URL links that you want to block. If you highlight some of the words on the list, you can remove it by clicking on Clear.
Use	Click this button to save your changes settings LTE modem.
back	Click this button to return to the previous screen without saving.

13 L2TP VPN

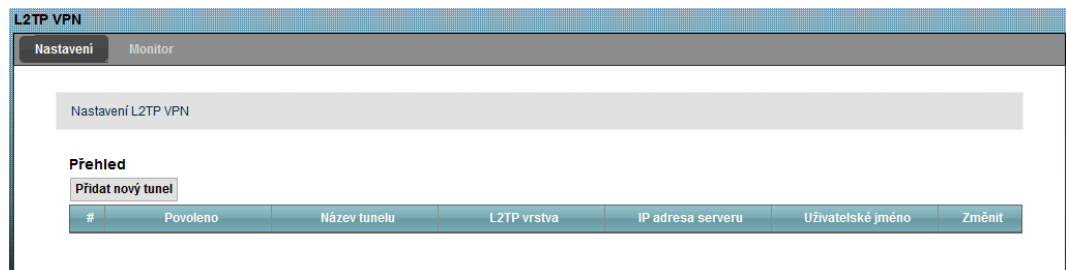
13.1 Overview

L2TP VPN tunnels forwarded to the network data flow between LTE modem and the device / server at the same level on the internet.

13.2 Settings screen

Use this screen to manage L2TP VPN tunnels. The following screen, click on **Security> L2TP VPN**.

Figure 13-1 Security> L2TP VPN> Settings



The following table summarizes the available fields on this screen.

Table 13-1 Security> L2TP VPN> Settings

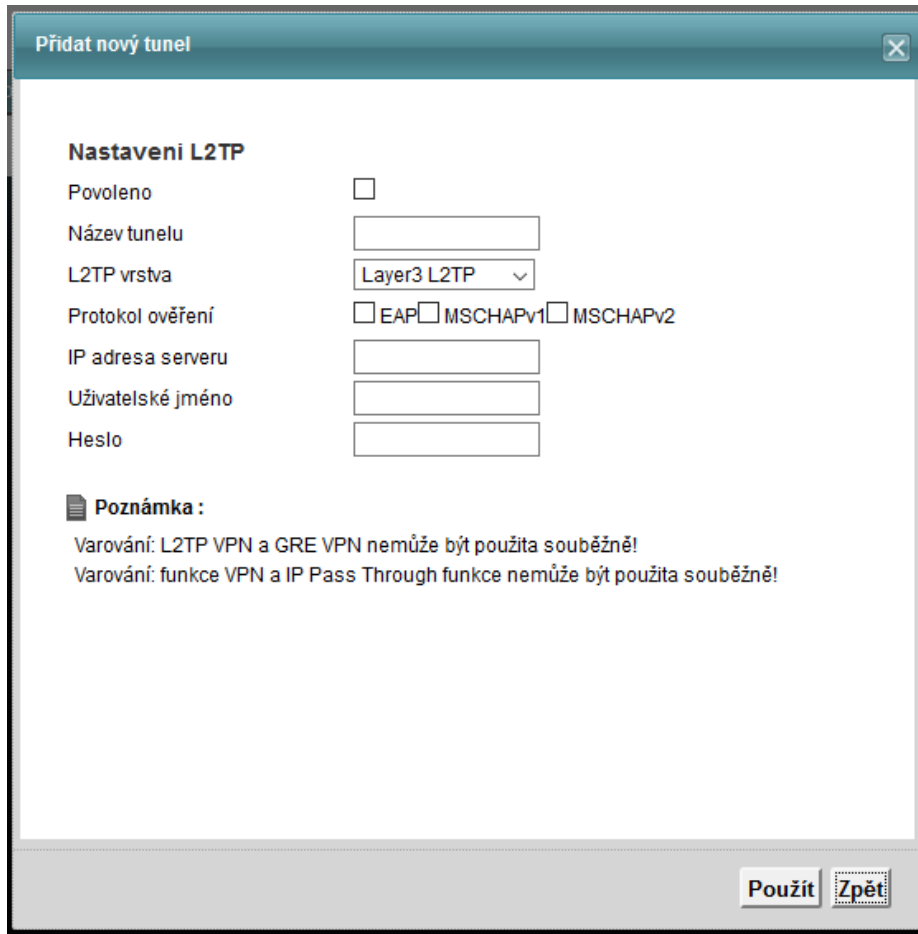
Item	Description
Add a new tunnel	Click this button to create a new L2TP tunnel.
#	This is the serial number of the L2TP tunnel.
Allowed	This field shows whether it is appropriate L2TP tunnel is active or not.
name of tunnel	Name of the tunnel.

Item	Description
L2TP layer	Layer of the OSI reference model (Layer3) the L2TP tunnel.
IP address of the server	IP address of the remote gateway with which LTE modem connection is established through the tunnel.
Username	A remote user needs to LTE modem before creating the L2TP VPN tunnel logged. This field is given a user or group of users authorized to use the L2TP VPN tunnel.
adjust	Click on the icon change open a dialog for editing the tunnel. Click on the icon Clear You can delete the tunnel.

13.2.1 Screen Add new tunnel / tunnel Modifications

Using this screen, you can create or edit L2TP VPN tunnel. The screen below by clicking on the button **Add a new tunnel** or icon **change** in line with the relevant VPN tunnel on screen **Security> L2TP VPN**.

Figure 13-2 Add new tunnel / tunnel Modifications



The following table summarizes the available fields on this screen.

Table 13-2 Add new tunnel / tunnel Modifications

Item	Description
setting L2TP	
Allowed	Check the box to activate the L2TP tunnel. Leave the box unchecked if you do not currently use the tunnel.
name of tunnel	Enter a descriptive name for the L2TP tunnel.
L2TP layer	choose Layer3 L2TP for creating a tunnel in layer 3 of the OSI reference model. choose layer2 L2TP to form in the layer 2 tunnel (tunnel BCP) OSI reference model.
authentication protocol	Select the protocol, which will run through user authentication (EAP or MSCHAPv2 MSCHAPv1).
IP address of the server	IP address of the remote gateway.

Item	Description
Username	The user or group of users authorized L2TP VPN tunnel use.
Password	User password.
Use	Click this button to save your changes settings LTE modem.
back	Click this button to return to the previous screen without saving.

13.3 Screen Monitor

This screen allows you to monitor the status of the L2TP VPN tunnel. The following screen, click on **Security> L2TP VPN> Monitor**.

Figure 13-3 Security> L2TP VPN> Monitor



The following table summarizes the available fields on this screen.

Table 13-3 Security> L2TP VPN> Monitor

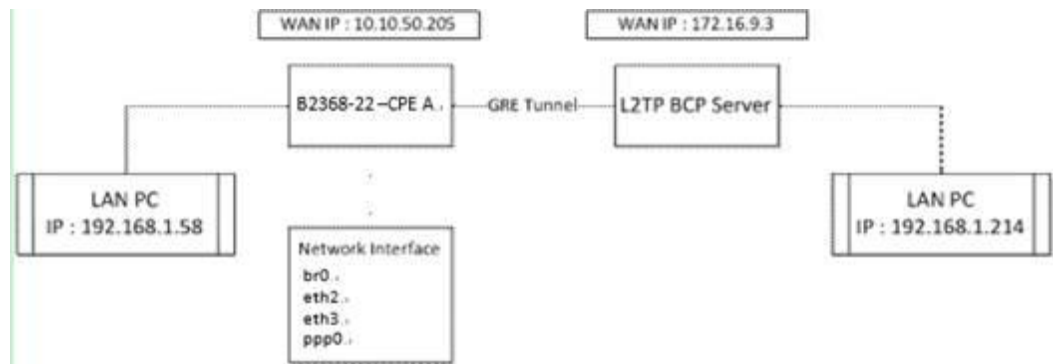
Item	Description
#	This is the serial number of rules. Check the box to activate the rule.
State	An icon indicating the L2TP VPN tunnel.
name of tunnel	Name of the tunnel.
IP address of the server	In this field the IP address of the remote gateway.
L2TP Server IP Address	In this field the IP address that LTE modem is assigned to a remote computer connected via L2TP VPN tunnel.
Local L2TP IP address	In this field the IP address of the computer connected to the LTE modem via L2TP VPN tunnel.
Current status	Text description of the current state of the connection to the L2TP VPN tunnel.

Item	Description
Restore	Click this button to update the screen.

4.13 Configuration Example L2TP VPN tunnel Layer 3

This is a diagram of a network structure in the example below:

Figure 13-4 Example of a network structure of the L2TP tunnel to the VPN Layer 3



A CPE WAN IP is 172.23.40.48, which is to the LAN connected to a computer with an IP address 192.168.1.51. L2TP server uses WAN IP 172.23.40.25 and is effected within a LAN connected computer with an IP address of 192.168.2.2. IP address of the computer on the LAN must come from a different domain subnet. L2TP VPN tunnel layer 3 can be set using the web configuration interface.

Figure 13-5 Example configuration L2TP VPN tunnel Layer 3 Add a new tunnel

Nastavení L2TP

Povoleno

Název tunelu

L2TP vrstva ▾

Protokol ověření EAP MSCHAPv1 MSCHAPv2

IP adresa serveru

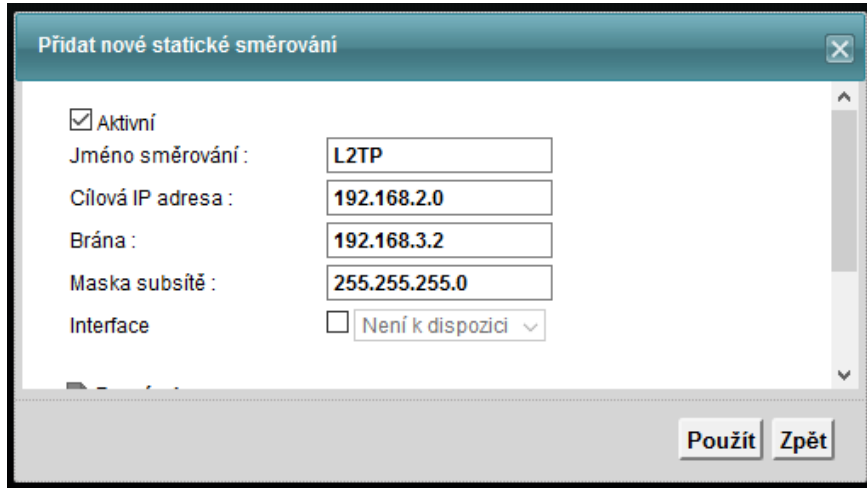
Uživatelské jméno ⋮

Heslo ⋮

Both CPE activated ppp0 interface and L2TP server assigns L2TP CPE and IP address (192.168.3.2). After creating the L2TP VPN tunnel layer 3 is also a need to create a static routing rule (click **Add new static routing** on the screen **Network Settings> Static Routing**, or on the icon **adjust** on the right side of the table). By default, the CPE does not send any data flow through the L2TP tunnel. IN

Example static routing network is set to the IP address 192.168.2.0/24 through the tunnel (gateway IP address: 192.168.3.2).

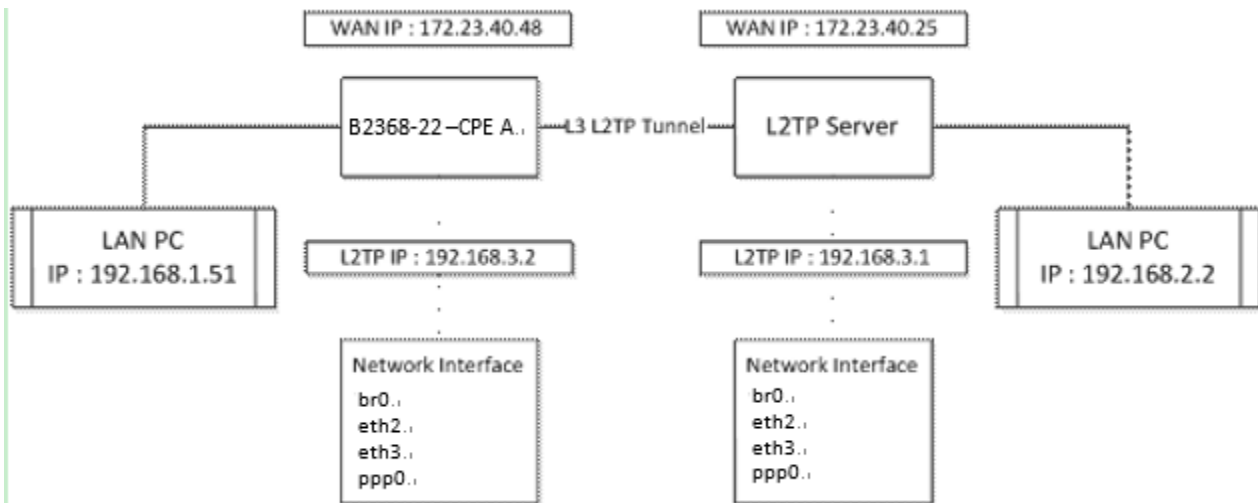
Figure 13-6 Example configuration L2TP VPN tunnel Layer 3 static routing Add new



5.13 Configuration Example L2TP VPN tunnel Layer 2

This is a diagram of a network structure in the example below:

Figure 13-7 An example of the network structure of the VPN tunnel L2TP Layer 2



A CPE WAN IP is 10.10.50.205, which is to the LAN connected to a computer with an IP address 192.168.1.58. In addition, BCP L2TP server WAN IP 172.16.9.3, which is connected to the LAN computer with the IP address 192.168.1.214. IP addresses of both computers on the LAN must come from the same domain subnet. L2TP VPN tunnel Layer 2 can be set using the web configuration screen **L2TP VPN**.

After creating the L2TP VPN tunnel Layer 2 LTE modem will send all packets from computers on the LAN (br0) via L2TP tunnel BCP (bcp0). Users can send packets from one PC on the LAN to another (ie. The address of 192.168.1.58 to 192.168.1.214).

Configuration:

Figure 13-8 Example configuration L2TP VPN tunnel Layer 2 Add a new tunnel

Nastavení L2TP

Povoleno	<input checked="" type="checkbox"/>
Název tunelu	<input type="text" value="test"/>
L2TP vrstva	<input type="text" value="Layer3 L2TP"/> ▾
Protokol ověření	<input type="checkbox"/> EAP <input type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2
IP adresa serveru	<input type="text" value="172.23.40.25"/>
Uživatelské jméno	<input type="text" value="test"/> ...
Heslo	<input type="password" value="••••"/> ...

14 GRE VPN

14.1 Overview

GRE (Generic Routing Encapsulation) protocol from the TCP / IP (transport layer, an IP protocol number 47) designed to encapsulate the packets of one protocol into another protocol. It is used in VPN to transmit IPv6 packets in IPv4 tunneling, and general. At the time of writing this LTE modem supports GRE tunneling only to transmit IPv4 packets.

14.2 Settings screen

Use this screen to manage GRE VPN tunnels. The following screen, click on **Security> VPN GRE**.

Figure 14-1 Security> GRE VPN> Settings



The following table summarizes the available fields on this screen.

Table 14-1 Security> GRE VPN> Settings

Item	Description
Add a new tunnel	Click this button to create a new GRE tunnel.
#	This is the serial number of rules. Check the box to activate the rule.

Item	Description
Allowed	This field shows whether the respective GRE tunnel is active or not.
Name GRE Tunnel	Name of the tunnel.
GRE layer	This field determines whether the GRE tunnel is in the second or third layer of the OSI reference model.
GRE IP address of the server	This is the IP address or domain name of the remote gateway to which LTE modem WAN interface tunnel stream.
Local GRE IP address	This is the local host IP address from which the tunnel LTE modem data stream to a remote gateway.
Remote GRE IP address	This is the IP address of the remote host for a remote gateway to which LTE modem tunnels stream.
adjust	Click on the icon change open a dialog for editing the tunnel. Click on the icon Clear You can delete the tunnel.

14.2.1 Screen Add new tunnel / tunnel Modifications

Using this screen, you can create or edit GRE VPN tunnel. The screen below by clicking on the button **Add a new tunnel** or icon **change** in line with the relevant VPN tunnel on screen **Security> VPN GRE**.

Figure 14-2 Add new tunnel / tunnel Modifications

The following table summarizes the available fields on this screen.

Table 14-2 Add new tunnel / tunnel Modifications

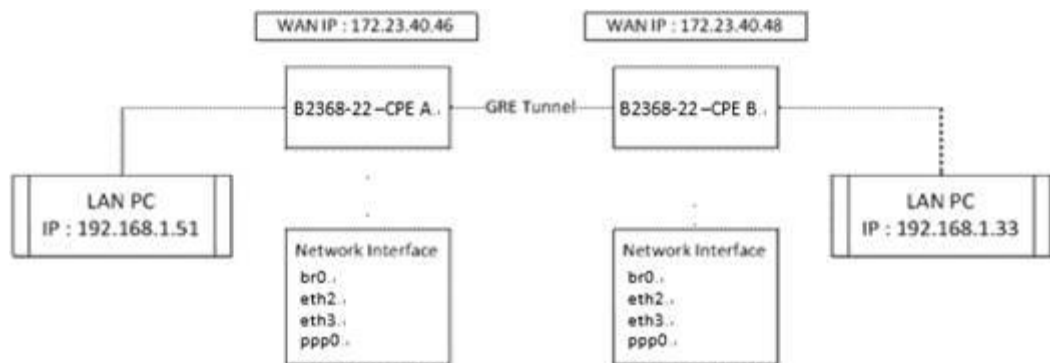
Item	Description
GRE settings	
Allowed	Check the box to activate the GRE tunnel. Leave the box unchecked if you do not currently use the tunnel.
name of tunnel	Enter a descriptive name for the GRE tunnel.
GRE layer	This field specifies which layer of the OSI reference model will GRE tunnel reside (layer2 GRE or Layer3 GRE). Use a second layer if the IP addresses of both computers on the LAN from the same subnet domain. Use a third layer, if the IP addresses of both computers on the LAN subnet in different domains.
Server IP Address	This is the IP address or domain name of the remote gateway to which WAN LTE modem interface tunnel stream.

Item	Description
Local GRE IP address	This is the local host IP address from which the tunnel LTE modem data stream to a remote gateway.
Remote GRE IP address	This is the IP address of the remote host for a remote gateway to which LTE modem tunnels stream.
Use	Click this button to save your changes settings LTE modem.
back	Click this button to return to the previous screen without saving.

3.14 Configuration Example GRE VPN tunnel Layer 2

This is a diagram of a network structure in the example below:

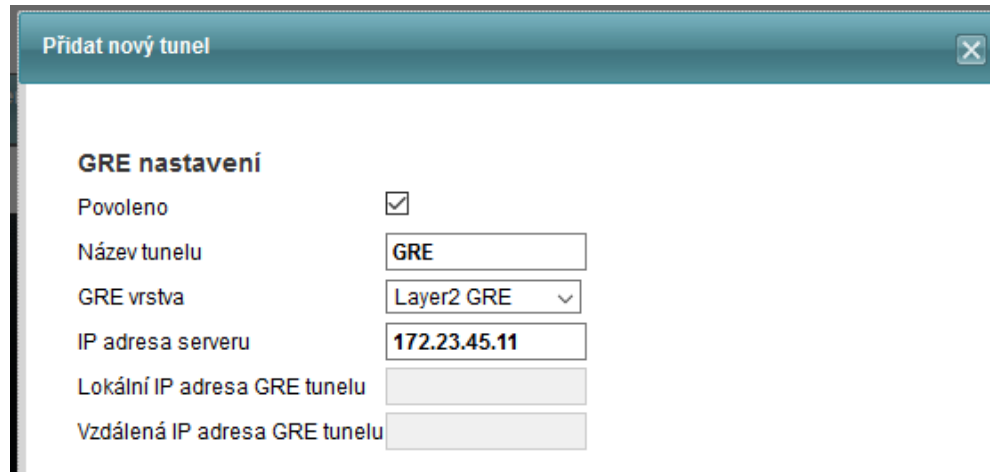
Figure 14-3 Example network structure with GRE VPN tunnel Layer 2



A CPE WAN IP is 172.23.40.46, which is to the LAN connected to a computer with an IP address 192.168.1.51. CPE B has a WAN IP 172.23.40.48, which is to the LAN connected computer with an IP address of 192.168.1.33. IP addresses of both computers on the LAN must come from the same domain subnet. To configure the CPE and enter the name of the tunnel, set the GRE layer Layer2 GER and the IP address of the server IP address of the CPE WAN B (172.23.40.48).

configuration (**Security > GRE VPN** and click on **Add a new tunnel**)

Figure 14-4 Example configuration GRE VPN tunnel Layer 2 Add a new tunnel

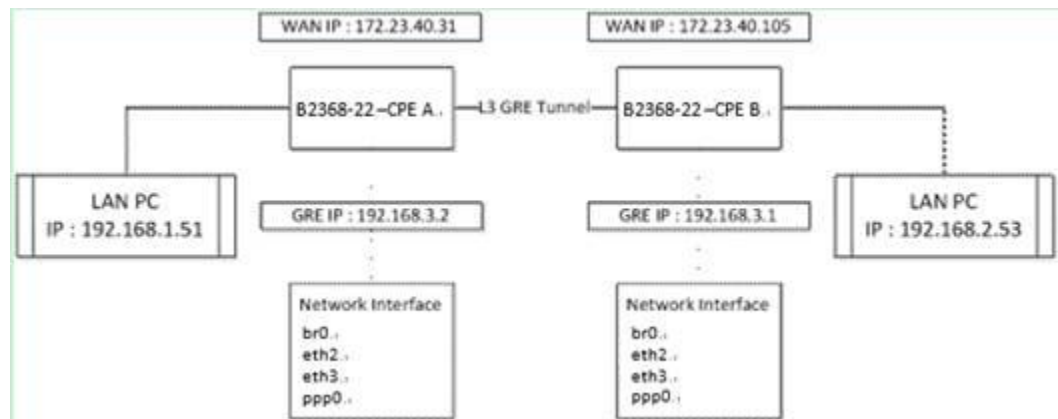


After setting GRE VPN tunnel Layer 2 CPE will send all packets from computers on the LAN through a GRE tunnel. Users can send packets from one PC on the LAN to the other through APN1.

4.14 Configuration Example GRE VPN tunnel Layer 3

This is a diagram of a network structure in the example below:

Figure 14-5 Example network structure with GRE VPN tunnel Layer 3



A CPE WAN IP is 172.23.40.31, which is to the LAN connected to a computer with an IP address 192.168.1.51. CPE B has a WAN IP 172.23.40.105 to which it is within the LAN connected computer with an IP address of 192.168.2.53. IP address of the computer on the LAN must come from a different domain subnet. A CPE Make settings as follows:

Figure 14-6 Example configuration GRE VPN tunnel Layer 3 Add a new tunnel

Přidat nový tunel

GRE nastavení

Povoleno

Název tunelu

GRE vrstva

IP adresa serveru

Lokální IP adresa GRE tunelu

Vzdálená IP adresa GRE tunelu

Both CPE interfaces tunnel activated and assigns GRE IP address. After creating a GRE tunnel VPN Layer 3 is also necessary to set the static routing to determine the data stream from the internet, which will be routed through the GRE tunnel. By default, the CPE does not send any data stream via the GRE tunnel. In the example static routing network is set to IP address 192.168.2.0/24 through the tunnel (gateway IP address: 192.168.3.2).

Figure 14-7 Example configuration GRE VPN tunnel Layer 3 static routing Add new

Přidat nové statické směrování

Aktivní

Jméno směrování :

Cílová IP adresa :

Brána :

Maska subsítě :

Interface

15 VoIP

15.1 Overview

The information in this section allows you to:

- LTE modem to connect to analog phone.
- Make phone calls over the Internet and conventional telephone network.
- Perform speed-dial settings.
- Optimize the sound quality of phone calls.
- If several APN is required to perform the following steps to ensure that the device or Softphone IAD on the LAN are routed to the correct path (ie. The second APN).

Add a static route that directs traffic on the media server (eg.

204.11.12.32 the diagram at right) through the interface **Voice** in settings **Network Settings> Static Routing> Add new static routing** (more information, see chapter 7.2.1 Add / Edit static routing). After adding a new rule of static routing wait until the timeout interval repetition registration and VoIP will not automatically connect to the server. You can also go to the screen **system monitor** and register the VoIP server manually.

Figure 15-1 Static routing via Voice

Přidat nové statické směrování

Aktivní

Jméno směrování : voice

Cílová IP adresa : 204.11.12.32

Brána :

Maska subsítě :

Interface L2tpVPN

Použít Zpět

15.1.1 What You Need to Know

Before reading this chapter is to be familiar with the following terms.

VoIP

Voice over Internet Protocol (VoIP acronym) is a technology that allows the transmission of digitized voice packets in the body of the family of protocols UDP / TCP / IP. This transfer is realized via computer networks or other media transparent to IP. It is used for making phone calls over the Internet, an intranet, or any other data connection.

ARROW

Acronym SIP is a Session Initiation Protocol, Czech Session Initiation Protocol. It is an Internet protocol for transmitting signaling between Internet telephony network devices. Within the VoIP signaling they are meant phone calls. For example, when you dial the number through your LTE device modem then through the network sends the SIP message to the target device (on the dialed number) with a request to answer the call.

SIP account

SIP account is a type of VoIP account. This is an agreement with your ISP, based on which you can perform via internet phone calls. Once LTE modem to store the information on your SIP account is then able to send all the information about the phone call to your ISP.

SIP account is not strictly necessary. SIP devices (such as the LTE modem) can make a phone call without the participation of the service provider SIP. Normally, however, this process is impractical and difficult. SIP service provider shall provide all necessary steps to direct a call session that reports of both parties arrive at the right place.

Detection of voice / silence

Detection algorithm Voice Voice Activity Detection (VAD) can recognize a human voice. This algorithm allows **reduction in load transfer capacity of the call, because no transmission " silent packets " at a time when you do not speak.**

Generating noise utvrzujícího

When using VAD algorithm LTE modem generates noise when affirming that the other party has just talking. This affirming noise is proof that the call is still active, since silence could be considered a loss of connection.

echo cancellation

G.168 is an ITU-T standard, which eliminates echoes caused " reflection " your voice in a telephone receiver during the call.

Where to learn more

For more information on SIP, see chapter 15.6 Technical details.

15.1.2 Before

- Before starting any configuration is required to have a VoIP account. If you have not yet, the creation of such an account, it is possible for a VoIP service provider on the Internet.
- The login for your VoIP account should be available before you start setting up the LTE modem.

15.2 Screen Service Provider SIP

Using this screen, you can set the information about the SIP server and other parameters associated with VoIP calls.

To access the screen **SIP Service Provider** click on **VoIP> SIP**.



NOTE

Click on **more...** to see all available fields. To set the account is not necessary to fill in all parameters. If you want to make on this screen display only the required fields, click on **Hide more**.

Figure 15-2 VoIP> SIP> SIP Service Provider

SIP

Poskytovatel služby SIP SIP účet

Poskytovatel SIP služeb nabízí služby VoIP volání (volání přes Internet). Pro správné nastavení SIP služeb je nutné požádat poskytovatele o následující parametry týkající se SIP účtu.

Obecné

Poskytovatel služby SIP : Povolit poskytovatele služby SIP

Jméno poskytovatele služby SIP : (1025-65535)

Lokální SIP port : (1025-65535)

Primární adresa SIP serveru :

Port SIP serveru : (1025-65535)

Adresa REGISTER serveru :

Port REGISTER serveru : (1025-65535)

Servisní doména SIP :

[skrýt více](#)

Podpora RFC

PRACK (RFC 3262) : (1025-65535)

Povolit DNS SRV (RFC 3263 - pokud je vybrána tato možnost, požadované změny se projeví asi za 30 sekund.)

Časovač spojení (RFC 4028)

Návěští VoIP IOP

V SIP zprávách nahraďte znak '#' znakem '%23'

V SIP zprávách z 'request-uri' odeberte ':5060' a 'transport=udp'.

V SIP zprávách odeberte hlavičku 'Route'.

V případě, že je ve zprávě SDP podporováno užití více kodeků, neodesílejte druhou stranu zprávy RE-INVITE.

V SIP ACK zprávě odeberte hlavičku 'Authentication'.

Obousměrné RTP pro SIP 183 je používáno.

Podpora SDP pro SIP 180

Odebrat hlavičku Early Media

RTP rozsah portů (Od - Do)

Počáteční port : (1025-65535)

Koncový port : (1025-65535)

DTMF mód
DTMF mód: RFC 2833 ▾

Typ transportu
Typ transportu: UDP

Odchozí Proxy
 Povolit
Adresa serveru:
Port serveru: (1025-65535)

QoS značka
Nastavení priority SIP TOS: 184 (0-255)
Nastavení priority RTP TOS: 184 (0-255)

Nastavení časovače
Čas expirace: 3600 (60-65535) sekunda
Register Re-send časovač: 512 (180-65535) sekunda
Spojení vyprší: 180 (100-3600) sekunda
Min-SE: 90 (90-1800) sekunda

Výběr intervalu vytáčení
Výběr intervalu vytáčení: 3 ▾ sekunda

Konfigurace tlačítek telefonu
Zobrazit identitu volajícího *30#
Skrýt identitu volajícího #30#
Volání stiskem tlačítka se zobrazeným číslem volajícího #31#
Volání stiskem tlačítka se skrytým číslem volajícího *31*
Povolit čekání hovoru *43#
Zakázat čekání hovoru #43#
Povolit druhý hovor *44#
Zakázat druhý hovor #44#
Předání hovoru *98#
Povolit nepodmíněné přesměrování hovoru *21*
Zakázat nepodmíněné přesměrování hovoru #21#
Povolit přesměrování hovoru v případě, že číslo neodpovídá *61*
Zakázat přesměrování hovoru v případě, že číslo neodpovídá #61#
Povolit přesměrování hovoru v případě, že je číslo obsazeno *67*
Zakázat přesměrování hovoru v případě, že je číslo obsazeno #67#
Povolit nevyrušování (Do Not Disturb) *95#
Zakázat nevyrušování (Do Not Disturb) #95#

Použit Zrušit

The following table summarizes the available fields on this screen.

Table 15-1 VoIP> SIP> SIP Service Provider

Item	Description
In general	
The service provider SIP Check	this box if you want to use the provider SIP. Leave this field is free, if you do not use a SIP provider.
The name of the service provider SIP	Enter the name of your SIP provider.
Local SIP port	Enter the port number on which LTE modem listens VoIP communication (if available). Otherwise the field

Item	Description
	<p>Leave the default value.</p> <p>NOTE</p> <p>Together FXS port and IAD devices or SIP phone to the LAN work together, check the SIP port on the IAD and SIP phones. Make sure to use a different port than local SIP LTE modem.</p>
Primary SIP server address	Enter the IP address or domain name of the SIP server that you received from your VoIP provider. You can use up to 63 printable ASCII characters. It does not matter whether the SIP proxy server, redirect server or registration.
Port SIP server	Enter the port number on which the server is listening SIP VoIP communication (if available). Otherwise field leave the default value.
REGISTER Server Address	Enter the IP address or domain name registration SIP server that you received from your VoIP provider. If you do not have that value available, enter the same address as the field The primary address of the SIP server. You can use up to 63 printable ASCII characters.
REGISTER Server Port	Enter the port number on which the registration SIP server listens VoIP communication (if available). If you do not have that value available, enter the same address as the field Port SIP server.
SIP Service Domain	Enter a name for the SIP service domain. As part of a full SIP URI address of the domain name service as part symbol "@". You can use up to 63 printable characters in the extended ASCII.
support for RFC	
PRACK (RFC 3262)	RFC 3262 defines a mechanism for providing reliable transmission of provisional SIP responses which contain information on how to handle the request. This is an extension that uses tags 100rel and a method of validating provisional response PRACK (Provisional Response Acknowledgment). If you select supported or Required, LTE include all requirements INVITE request SIP header field / support with optional label 100rel. Then, when LTE modem receives a SIP response confirming that dial phone rings LTE modem sends a message PRACK both parties on the call, which will acknowledge receipt of the message. If you select supported; will use the brand 100rel optional and supported. If you select Required, will use the brand 100rel required. selecting disabled this feature off.
Enable DNS SRV (RFC 3263)	Check this box to activate sending requests to DNS servers of your ISP to list

Item	Description
	available SIP servers. This is especially useful when your SIP server still struggling to users and thus unable to perform SIP calls.
Timer connection (RFC 4028)	<p>Checking this box will be LTE modem comply with RFC 4028th</p> <p>Timer connection ensures that a SIP session can be posted and SIP line may not always be available.</p>
<p>Label VoIP IOP - configuration settings compatibility VoIP telephony. Select the desired label VoIP IOP as instructed by your service provider.</p>	
RTP port range	
<p>The initial port</p> <p>End port</p>	<p>If this information is available to you, enter the upper limit of the range of possible ports for RTP traffic. Otherwise field leave the default value.</p> <p>To specify a single port number, enter the fields The initial port and end port the same value. To specify a range of ports,</p> <ul style="list-style-type: none"> · Enter the field The initial port Port number located at the beginning of the range. · Enter the field end port Port number located at the end of the range. <p>NOTE</p> <p>By default, the LTE modem RTP ports starting from 50,000th</p> <p>NOTE</p> <p>To avoid potential conflicts, make sure that the RTP port IAD devices and SIP phones in the network are not starting from 50000. For example, use ports 10000 and 30,000th</p>
DTMF mode	
DTMF mode	<p>This setting determines how the LTE modem handles the notes issued by pressing the phone. The settings should match the requirements of a VoIP connection.</p> <p>RFC2833 - DTMF tones will be sent through RTP packets.</p> <p>PCM - DTMF tones are sent in a voice data stream. This method is most effective if you are using the codec without compression (eg. G.711). Using compression codecs (eg. G.729 or G.726) can distort the tones.</p> <p>SIP INFO - DTMF tones will be sent through SIP messages.</p>
type of transport	
type of transport	<p>This field is read-only and indicates the transport layer protocol that uses LTE modem for SIP traffic (UDP).</p>
outbound proxy	
Allow	<p>Check this box if your service provider VoIP <u>It provides outbound SIP server for voice calls. This will allow LTE</u></p>

Item	Description
	Modem work with any type of NAT router and eliminates the need for communication STUN.
server address	Enter the IP address or domain name of the outbound SIP proxy.
server port	Enter the port number on which the outbound SIP proxy server listens VoIP communications, if available. Otherwise field leave the default value.
QoS tag	
Setting priorities SIP TOS	Enter the number of tie-breaking mechanism DSCP (DiffServ Code Point) for the transmission of messages SIP. LTE modem then creates a priority tag class of service (CoS) with the number for the corresponding data transmission SIP.
Setting priorities RTP TOS	Enter the number of tie-breaking mechanism DSCP (DiffServ Code Point) for the transmission of messages RTP. LTE modem then creates a priority tag class of service (CoS) with the number for the corresponding data transmission RTP.
setting the timer	
expiration time	Enter the expiration time SIP account under SIP registration server in seconds. LTE modem will try to repeat automatically register your SIP account, once the half time specified expiration date. (Time to expiration on the SIP registration server may vary.)
Register Re-send timer	Enter the delay in seconds, during which the LTE modem must wait before sending a repeat registration SIP account, if the first attempt fails and the modem received no response.
connection expires	Enter the delay in seconds within which can be run SIP connection idle (no streaming) before it is disconnected.
Min-SE	Enter the minimum time, in seconds, it can remain running SIP connection idle (no streaming) before it is disconnected. Once the two SIP device initiates SIP connection, must reach agreement on the time of expiration connection for idle connections. This field specifies the shortest time allowed for the LTE modem.
Selecting dialing interval	
Selecting dialing interval	Enter the number of seconds expressing the desired length of the pause between digits, and the start dialing the call. The value set by the speed of entering the phone number.
<p>Configuring the phone keys</p> <p>Use this menu to define several shortcuts to activate certain functions of an LTE modem.</p> <p><u>If you enter a shortcut key, which does not include the parameter " Call press " you hear short acknowledgment tone. If it does not, it means that you have entered a keyboard shortcut</u></p>	

Item	Description
	<p>incorrectly. Once this short acknowledgment tone is hang up and the function will be activated.</p> <p>Shortcuts with parameter " Call press " it is necessary to add the phone number you want to call. After using keyboard shortcuts with the parameter " Call press " You hear no confirmation tone.</p>
Show caller's identity	Shortcut to display the caller's identity during outgoing calls.
Caller identification hotkey to hide	hide the identity of the caller while the outgoing calls.
Call by pressing the displayed Caller ID	Shortcut to display the caller's identity, but only for one of the following call, which is going to take place.
A call by pressing a secret number of the caller	Shortcut to hide the caller's identity, but only for one of the following call, which is going to take place.
Allow call waiting	Shortcut to activate call waiting. If during an ongoing phone call, you receive another incoming call, the phone notifies you that special sound signal. Subsequently, it will be possible to hold the current call and respond to the other. Because there is no risk that you missed an important call.
Disable call waiting	Shortcut to turn off call waiting.
Allow a second call (call by pressing)	Shortcut to activate call waiting, but only for one of the following call, which is going to take place. The function is otherwise the same as in the case of keyboard shortcuts " Allow call waiting " .
Disable the second call (call by pressing)	Shortcut to turn off call waiting, but only for one of the following call, which is going to take place.
call Transfer	Shortcut to activate the possibility of transferring the incoming call to another phone.
Allow unconditional call forwarding	Shortcut for unconditional call forwarding. Incoming calls are always unconditionally forwarded to a specified number.
Disable unconditional call forwarding	Shortcut to turn off call forwarding unconditional.
Allow call forwarding if the number does not match	Shortcut to activate call forwarding if the dialed number does not match the SIP.
Disable call forwarding if the number does not match	Shortcut to turn off call forwarding if the dialed number does not match the SIP.
Allow call forwarding if it is	Shortcut to activate call forwarding if the number is busy.

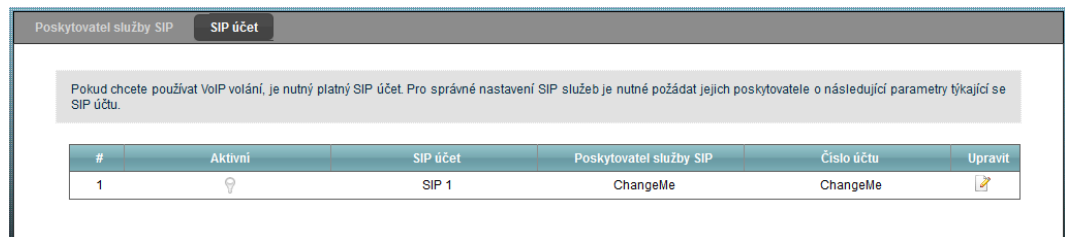
Item	Description
number is busy	
Disable call forwarding if the number is busy	Shortcut to turn off call forwarding if the number is busy.
Allow nevyrušování (Do Not Disturb)	Shortcut to activate the Do Not Disturb (Do Not Disturb). If this feature is enabled, LTE modem will forward incoming calls to a phone line.
Disable nevyrušování (Do Not Disturb)	Shortcut to turn off Do Not Disturb (Do Not Disturb).
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

15.3 Screen SIP account

LTE modem effected using an account SIP outbound VoIP calls and check whether the caller ID incoming calls to your SIP account number. To be able to make VoIP calls, you must first activate and configure the SIP account and assign it to the phone port. SIP account contains information that allows your LTE modem to connect to the VoIP provider.

To access the next screen, click on **VoIP> SIP> SIP account**.

Figure 15-3 VoIP> SIP> SIP Account



The following table summarizes the available fields on this screen.

Table 15-2 VoIP> SIP> SIP Account

Item	Description
#	This is the serial number.
Active	The icon, which shows whether the SIP account is active or not. Symbol yellow light bulb means that the SIP account is active. Symbol gray bulb means that the SIP account is not active.

Item	Description
SIP account	Name of the relevant SIP account.
SIP Service Provider	Name of the relevant SIP provider.
Account number	Number of your SIP account.
adjust	Click on the icon adjust You can also edit the corresponding SIP account.

15.3.1 Configuring SIP account

Using this screen, you can adjust the parameters of your SIP account. To access this screen, click on the icon **adjust** next to an existing account.

Figure 15-4 SIP account: Edit

Konfigurace SIP účtu

Obecné

SIP účet: Aktivní SIP účet

Číslo SIP účtu:

Autentikace

Uživatelské jméno:

Heslo:

Typ URL

Typ URL:

Hlasové funkce

Primární typ komprese:

Sekundární typ komprese:

Terciální typ komprese:

Nastavení hlasitosti mluvení:

Nastavení hlasitosti poslechu:

Aktivní G.168 (potlačení echa)

Aktivní VAD (Voice Active Detector)

Hlasové funkce

Poslat identitu volajícího

Aktivní předání hovoru

Aktivní čekání hovoru:

Časovač zamítnutí upozorňovacího tónu: (10~60) sek.

Funkce nepodmíněného přesměrování je číslo:

aktivní

Funkce přesměrování pro případ, že je číslo obsazené, je aktivní Číslo :
 Funkce přesměrování pro případ, že číslo neodpovídá, je aktivní Číslo :
 Čas vyzvánění v případě, že číslo neodpovídá (10~180) sek.
 Povolit blokování anonymních volání

Konfigurace intervalu detekce flash

Povolit konfiguraci intervalu
 Hodnota detekce horní hranice pro poklepání/flash : (101~2000) milisekund
 Hodnota detekce spodní hranice pro poklepání/flash : (100~1999) milisekund

The following table summarizes the available fields on this screen.

Table 15-3 SIP account: Edit

Item	Description
In general	
SIP account	check the box Active SIP account if you want the account to use. Leave this field is free if you do not want to use this account.
SIP account number	Enter your SIP account. Within the complete address SIP URI is the portion of the account number before the symbol "@". Enabled is plus (+) and numbers.
authentication	
Username	Enter your username SIP account, exactly in the form in which you received it. You can use up to 128 printable ASCII characters.
Password	Enter the password for the registration of SIP account, exactly in the form in which you received it. You can use up to 128 printable ASCII characters.
type URL	
type URL	Choose whether you want when sending SIP numbers also include the name of the SIP service domain. ARROW - SIP domain name service will be part of the outgoing package. TEL - SIP domain name service is not part of the outgoing package.
voice features	
The primary compression type Secondary Tertiary compression type compression type	Specify the type of codec that will be used in LTE modem sound transmission. G.711 codec offers the highest sound quality, but require a higher bit rate (64 kbps). <ul style="list-style-type: none"> • G.711MuLaw It is typically used in North America and Japan. • G.711ALaw It is typically used in Europe. • G.729 It requires a baud rate only 8 kbps. Select the primary option LTE modem for encoding / decoding

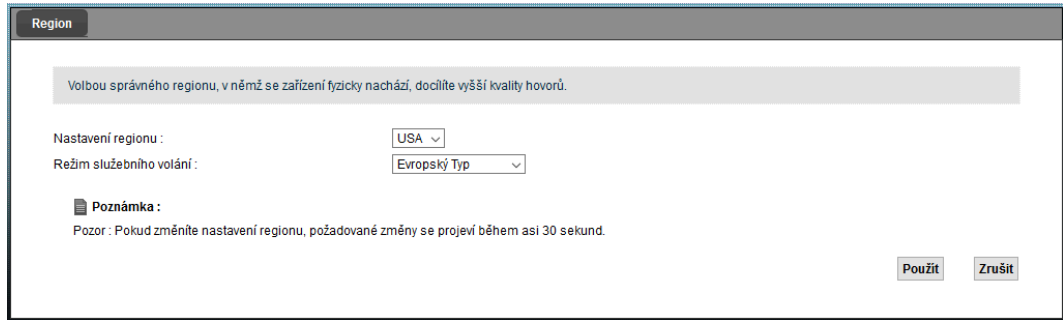
Item	Description
	<p>voice calls.</p> <p>Select a secondary option LTE modem for encoding / decoding voice calls. Choose none, if you want to use LTE modem every time a primary compression type.</p> <p>Choose a tertiary option LTE modem for encoding / decoding voice calls. Choose none, if you want to use LTE modem each time a primary or secondary compression type.</p>
Speak Volume Adjust	<p>Enter the volume level that will be LTE modem to send to the recipient. low corresponds to the lowest volume while high the highest volume.</p>
Adjusting listening volume	<p>Enter the volume level that will be LTE modem to send to your handset. low corresponds to the lowest volume while high the highest volume.</p>
Active G.168 (echo cancellation)	<p>Check this box to activate the feature, which eliminates echoes caused " reflection " your voice in a telephone receiver during the call.</p>
Active VAD (Voice Active Detector)	<p>If you check this box, the LTE modem stops sending data flow when you speak. This feature reduces the consumption data.</p>
voice features	
Send caller's identity	<p>Check this box if you want in a VoIP call to send the caller's identity. Leave this field is free if you do not want to send identity.</p>
Active call transfer	<p>Check this box if you want to activate call forwarding. This feature allows you to transfer an incoming call (received) to another phone.</p>
Active call waiting	<p>Check this box if you want to activate call waiting. This feature allows you to hold the current call and answer the second, the same telephone number.</p>
Timer rejection alerting tone	<p>Enter the time interval in seconds after which LTE modem waits before rejecting a second call, do not answer that.</p>
Unconditional call forwarding feature is activated	<p>Check this box if you want to redirect all incoming calls to a specified phone number. The number, type the field Number right.</p>
Redirection feature in case the number is busy, active	<p>Check this box if you want to redirect all incoming calls to a specified phone number in case your number is busy. The number, type the field Number right. If your number is busy and LTE modem registers another call, redirects it to the specified number if the second call reject or ignore you.</p>
redirection feature	<p>Check this box if you want all the unanswered incoming calls diverted to a specified phone number. (see Ring time when</p>

Item	Description
in the event that no answer is active	that number does not match) The number, type the field Number right.
Ring time if the number does not match	This field is important if it is active Redirection feature in case no answer. Enter the number of seconds expressing the desired length of time, after which the call will be considered adopted.
Allow anonymous call blocking	Check this box if you do not want your phone to ring when an incoming call, the caller identification.
Configuring detection interval flash	
Allow configuration interval	Using tap you can control certain functions during a call. The settings in this section to manually enter such a double-detection interval (how long press LTE devices will be regarded as signaling flash). If the configuration is not allowed interval, the interval will be set to flash detection in accordance with the regional specifications set menu VoIP> Phone> Region .
Value upper limit detection for tap / flash	Enter the longest interval to be considered flash modem. Once this period is exceeded, it will be interpreted as LTE modem hook call.
Detection lower limit value of the tap / flash	Enter the shortest interval that is considered a flash modem.
Use	Clicking Use save your changes.
back	Clicking back to return to the previous screen without saving.

15.4 Screen Region

On this screen, you can adjust the settings, which differ depending on the country you are LTE modem. To access this screen, click on **VoIP> Phone> Region**.

Figure 15-5 VoIP> Phone> Region



Individual fields are described in the following table.

Table 15-4 VoIP> Phone> Region

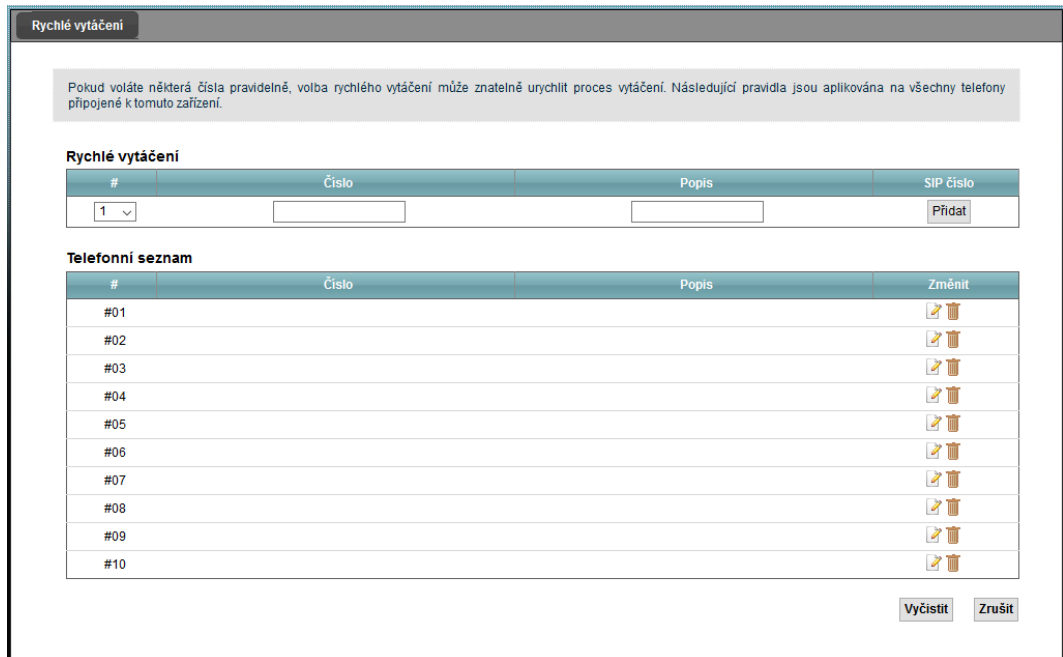
Item	Description
region settings	Choose a region in which the LTE modem is currently located.
Mode service call mode	<p>Choose a mode of additional services during the call that your service provider supports VoIP (call waiting, call waiting and three-way conference calls).</p> <ul style="list-style-type: none"> • European type - support services during a call typical for Europe. • American (USA) type - support services during a call typical for the United States. <p>These services may need to be activated before use by the service provider. For more information, contact your VoIP service provider.</p>
Use	Click to save changes made to the settings LTE modem.
Cancel	Click to return all settings on this screen to the default values.

15.5 Screen Call Rules

On this screen you can add, change and delete numbers for quick dialing outgoing calls. Speed dial is a shortcut to frequently used phone (VoIP) numbers. Using Speed Dial is essential if you want to contact SIP contacts containing letters. After setting the rules, you can speed dial the appropriate call a contact simply set a keyboard shortcut for quick dialing (eg. # 01).

To open this screen, click on **VoIP> Rules call**.

Figure 15-6 VoIP> Call Rules



Individual fields are described in the following table.

Table 15-5 VoIP> Call Rules

Item	Description
Speed dialing	Using this section you can create and modify rules on speed dial.
#	The digits to make a call to the phone number.
Number	Enter the SIP number you want to dial by pressing the speed dial keys.
Description	Enter a brief description that will identify the contact assigned to a speed dial key. You can use up to 127 printable ASCII characters.
Add	Click to add the information referred to in boxes Speed dialing To the table Phonebook below.
Phonebook	This table provides an overview of all speed dial keys and allows its modification or deletion.
#	The digits to make a call to the phone number.
Number	This field is a SIP number to be dialed by pressing the speed dial keys.
Description	In this field there is a brief description of the number to be dialed by pressing the speed dial keys.
change	Use these icons to rule the speed dial to edit or delete.

Item	Description
	<p>Click on the icon adjust values are copied to the entry section Speed dialing where you can edit it. When you are finished making changes, click Add.</p> <p>Click on the icon Clear to delete the record.</p>
Clean	Click this button to delete all entries speed dial.
Cancel	Click to return all settings on this screen to the default values.

15.6 Technical details

This chapter contains technical details about the available settings screens **VoIP** configuration interface.

15.6.1 VoIP

Voice over Internet Protocol (VoIP acronym) is a technology that allows the transmission of digitized voice packets in the body of the family of protocols UDP / TCP / IP. It is used for making phone calls over the Internet, an intranet, or any other data connection fraction of the cost compared to traditional fixed telephone line. You can also use servers to run specialized applications such as PBX or voicemail. VoIP services are usually provided by third parties, known acronym ITSP (Internet Telephony Service Provider).

Traditional telephone networks operating on the principle of switching circuits need to make a call transmission capacity of at least 64 kilobits per second. VoIP technology uses modern techniques for encoding voice compression, are therefore considerably less data intensive.

15.6.2 SIP

SIP (Session Initiation Protocol - Czech Session Initiation Protocol) is an Internet protocol for transmitting signaling in Internet telephony.

Protocol for secure VoIP connection works in conjunction with other protocols. Custom voice transmission takes place via the RTP protocol. The media, which are exchanged during the session, may use a different transmission path than signaling. SIP handles telephone calls and is able to communicate with traditional telephone networks with circuit switching.

SIP identity

SIP is the foundation of account identity (sometimes referred to as a SIP address). SIP identity as such is called a SIP URI (Uniform Resource Identifier). SIP URI identifies a user account in a similar way as the e-mail address of the appropriate account. SIP identity is written in the format of the SIP-Service-number @ domain-SIP.

SIP number

The number of SIP is the SIP URI segment located behind the symbol "@". SIP number is in spite of the name can also consist of letters, like the e-mail address - eg. johndoe@your-ITSP.com or 1122334455@VoIP-provider.com.

SIP Service Domain

Service domain SIP VoIP provider is the domain name in the SIP URI. For example, if a SIP address **1122334455@VoIP-provider.com**, then the service domain SIP " **VoIP-provider.com** ".

SIP Registration

Each individual LTE modem is a SIP user agent (UA). In order to provide voice services, has a public IP address to communicate with other servers within the SIP and RTP.

SIP user agent has to register to the SIP registration server and provide information about the user, which represents, as well as current IP address (for proper orientation for incoming SIP requests). After successful registration, SIP aware that users (identified by a dedicated SIP URI) are represented by the respective agent. He knows as to which IP address is required SIP requests and responses sent.

Registration initializes client UAC (User Agent Client) running on a VoIP gateway (eg. LTE modem). The gateway must be configured to include information about the recipient of the message REGISTER and relevant information about the user, eg. The necessary passwords.

Registration request to the SIP server has limited validity. UAC client needs during this period of validity of the registration recover. If they do not, they will be registration information removed from the database to the SIP registration server, and the connection is interrupted.

LTE modem after switching on always trying to register all active ports customers. When you turn previously inactive port customers, LTE modem immediately try to register it.

authorization requirements

SIP registration (and subsequent requests) require authentication by user name and password. These **credentials are verified using the system digestní (summary) via HTTP authentication (see RFC3261. " SIP: Session Initiation Protocol ')**.

SIP servers

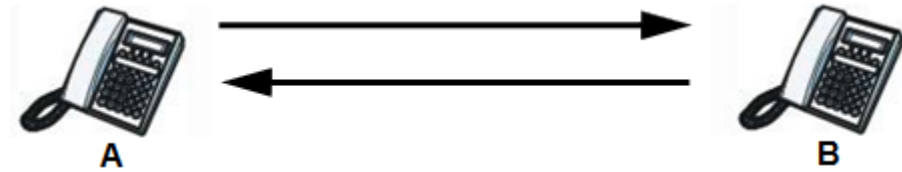
The basis of SIP is client-server architecture. SIP client is an application or device sending SIP requests. These requirements correspond SIP server.

Once started via SIP VoIP call begins at the client and server ends. SIP client can be a computer or phone. One device can be client and server SIP.

SIP user agent

SIP user agent is a device that can initiate and receive VoIP phone calls. This also means that through SIP can also initiate communications in a peer-to-peer, even though the protocol is based on client-server. The following **picture phones AND and B both of which can serve as a user agent and initiate the call. phones AND and B They can simultaneously serve as an agent for a user to answer an incoming call.**

Figure 15-7 SIP user agent



SIP proxy server

SIP proxy server

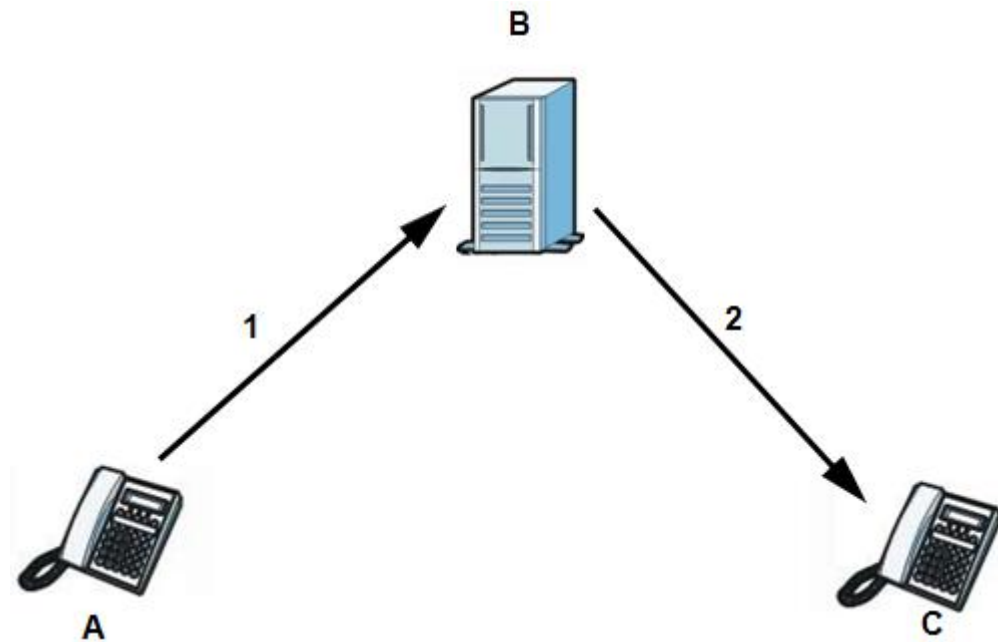
SIP proxy server receives requests from clients and forwards them to the destination server.

The following example describes a situation where a client device **AND** we call on the client device **C**.

Step 1 Client Device (**AND** pictured) sends an invitation to initiate a call to the SIP proxy server - **B**.

step 2 The SIP proxy server then invited to initiate a call sent to the device **C**.

Figure 15-8 SIP proxy server



---- End

SIP Redirect Server

SIP Redirect Server receives all SIP requests, translates the destination address to the IP address and sends the translated IP address back to a device that has sent the request. Client device that has sent the request may then send requests directly to the IP address that

received from the server redirects. Redirect servers themselves not initialized SIP requirements.

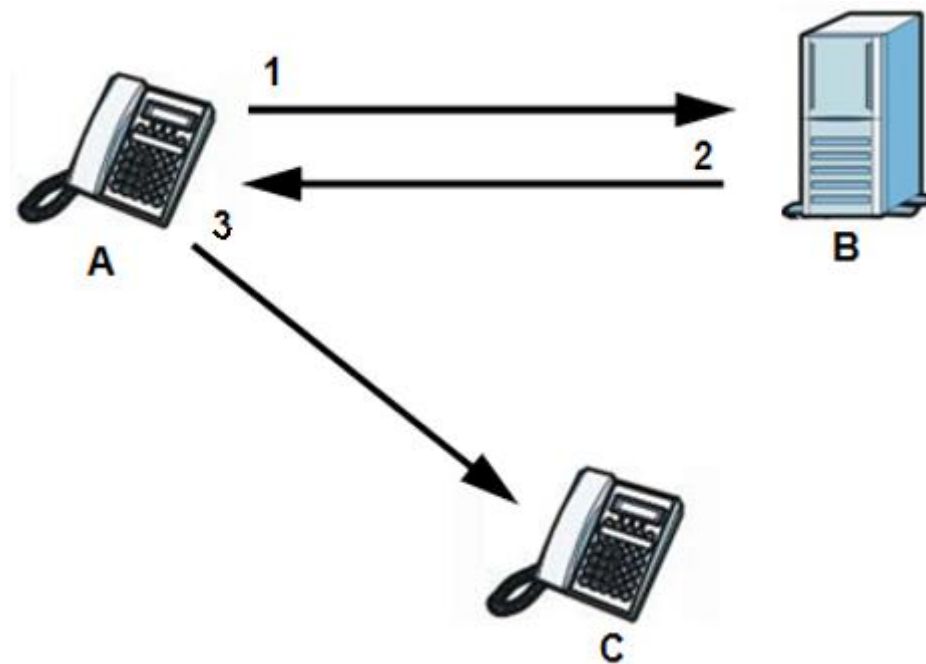
The following example describes a situation where a client device **AND** we call on the client device **C**.

Step 1 client device **AND** sends an invitation to start a conversation with the device **C** on the server
SIP redirect - **B**.

step 2 Redirect Server then sends back an invitation equipment **AND**, However complemented by IP address
(Or domain name) devices **C**.

step 3 client device **AND** then sends an invitation to initiate a call directly to the client device **C**.

Figure 15-9 SIP Redirect Server



---- End

SIP registration server

SIP registration server maintains a database of SIP identity mapping IP addresses of client devices or their domain names. During registration server authenticates the user name and password.

RTP

Real-time Transport Protocol (or RTP) is a protocol packet standardizing the delivery of audio and visual (video) data over the Internet. For more information on RTP, see RFC 3550th

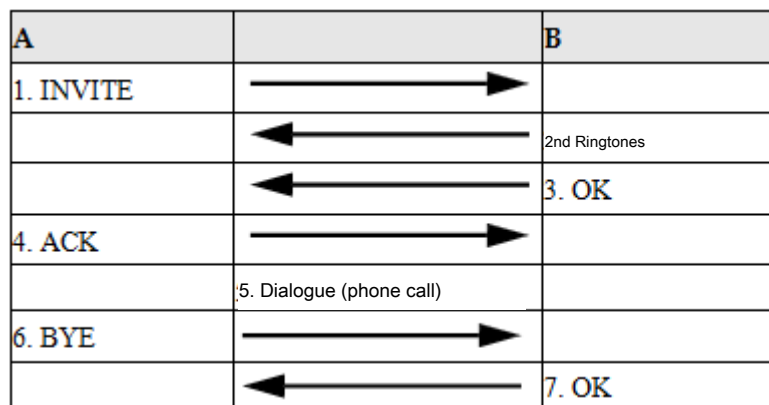
Pulse Code Modulation

Pulse Code Modulation (PCM from English Pulse-code modulation) is a modulation method of converting analog audio signal into a digital signal.

Workflow SIP call

The following chart describes the basic steps to initiate, conduct and termination of SIP call. Device A calling device B.

Figure 15-10 Workflow SIP call



Step 1 Device A sends a SIP INVITE request device B. This requirement is an invitation for B device to initiate a phone call SIP.

step 2 B sends a response that indicates that the phone is ringing.

step 3 B sends after receiving a call answer OK

step 4 A then sends a message ACK, which confirms that the B call accepted.

step 5 Now the data exchange between devices A and B (phone call).

step 6 After the call and hangs up and sends a request BYE.

step 7 B responds with OK, which acknowledges the BYE request. The call is terminated.

---- End

Coding for voice transmission

Codec (resp. The process of encoding and decoding) are used to convert the analog signal (voice) signals to digital and vice versa. The LTE modem supports the following transfer codecs.

- G.711 codec is based on pulse code modulation (PCM). Pulse Code Modulation is a modulation method of converting analog audio signal into a digital signal. Codec G.711 offers very good sound quality, but requires a bit rate of 64 Kbps.
- G.726 is based on the variation of pulse code modulation adaptive differential (ADPCM), which is less demanding in terms of bandwidth than standard PCM. ADPCM converts analog sound into digital signals based on the difference between each sound

sample and predictions based on previous samples. The pattern is similar zvukovější prediction, the less space is needed for its description. G.726 operates at transmission speeds of 16, 24, 32 or 40 Kbps.

- G.729 coding is hybrid modulated waveform synthesis method of analysis that uses a filter made based on information about how the human vocal cords produces sound. G.729 offers good sound quality and transmission speed requires only 8 Kbps.

Message Waiting Indication MWI

After activating the message waiting indicator (MWI), your phone beeps alert to the presence of new voice messages. VoIP provider must send message waiting indicator in support SIP packets, see RFC 3842nd

15.6.3 Quality of Service (QoS)

Quality of service, or QoS (from the English Quality of Service) describes how the network's ability to deliver data with minimum delay and method that uses the network for the transmission of multimedia messages in real time.

Type of Service (ToS)

Network traffic can be classified by setting the type of service or ToS (in English Type of Service), the source data stream (eg. LTE modem). The server will then be able to determine the best method of delivery of different types of data packets.

15.6.4 Overview of additional telephone services

VoIP service provider generally offers a suite of complementary telephone services, including call hold, call waiting and call forwarding. The LTE modem supports the following phone service:

- call hold
- call waiting
- Establishing a second call
- call Transfer
- Three-way conference call
- Do Not Disturb



NOTE

These services may be needed before applying by phone ports LTE modem to activate a VoIP service provider.

Flash button

deadline " flash " or tapping means holding very short (on the order of hundreds of milliseconds) the suspension phone keys. Newer phones are equipped with dedicated flash button, which sends a signal electronically. If the Flash key is not available, it is possible to simulate the function of a very short suspension by tapping the button on the phone. However it is recommended to use a dedicated button, which is much more accurate timing. When manually tapping may be too long to hold the key to the suspension assessed as call termination.

Double-click / flash is used to control additional telephone services.

Additional telephony services in Europe

This chapter describes how to use supplementary phone services when setting

Mode service call on European type. Individual commands to activate additional services are listed in the table below.

If a command is entered during the initial period expires for detecting tap / flash or enter an invalid type of command, the operation will be interrupted.

Table 15-6 Commands for additional functions tap / flash

The first button	Command	Description
Flash	None	Hold the ongoing call and preparation phone to dial the second call. Switching back to the ongoing call (does not take place if the second call).
Flash	0	Hold the ongoing call or reject an incoming call, waiting to pick up.
Flash	1	Disconnecting the current call and answer the new incoming call, if necessary. retrieve the held call.
Flash	2	1. Toggling between two ongoing calls. 2nd Hold current call and answer the second call. 3. Allocation of the ongoing conference call into two separate calls (one is attached, and the other on hold).
Flash	3	Launch of three-way conference call.
Flash	# 98 *	Transferring a call to another phone.

Call hold in Europe

Using call waiting, you can press the button to flash call (**AND**) hold.

If you register a new incoming call, press the flash button and then press 2. This will toggle between calls with caller **AND** and **B** by holding gradual.

Press the flash and press 0 to hang a call on hold and maintain the currently connected call.

Press the flash and press 1 for hanging currently connected call to resume the call. If you have an incoming call on hold and hung up the phone, the phone rings.

Call waiting in Europe

This feature allows you to hold the current call and answer the second, the same telephone number.

When the phone registers another call, notify you by an audible signal. You can do one of the following actions.

- Reject the second call.
Press the flash and then press the 0th
- Hang up the first call and answer the second call.
Press the flash and then press 1, or simply hang up the phone and lift it again after subsequent ring.
- Hold the first call and answer the second call. Press the flash key and then the second

Transferring a call in Europe

This feature allows you to transfer an incoming call (received) to another phone.

Step 1 Press Flash currently hold the ongoing call.

step 2 When you hear dial tone, press the key combination **** 98 # "** and enter the number you
To transfer the call.

step 3 After you hear another phone ringing, hang up the phone currently in use.

---- End

Three-way conference call in Europe

Here's how to make a three-way conference call.

Step 1 Once you speak to someone, press flash. This will call hold and
ringing a dial tone.

step 2 Enter the phone number to start a new call.

step 3 When the user picks up a second call, press the flash key, and then third
This will create a conference call for all participants.

step 4 To break the connection simply hang up.

step 5 To the ongoing conference call into two separate calls (one will
active and one on hold), press the flash button and then press the second

---- End

Additional phone service in the US

This chapter describes how to use supplementary phone services when setting

Mode service call on American (USA) type. Individual commands to activate additional services are listed in the table below.

If a command is entered during the initial period expires for detecting tap / flash or enter an invalid type of command, the operation will be interrupted.

Table 15-7 Commands for additional functions tap / flash

The first button	Command	Description

The first button	Command	Description
Flash	-	Hold the ongoing call and preparation phone to dial the second call. Once a successful connection of the second call, press flash again to create the conference call. Hold the ongoing call and answer a second call.
Flash	# 98 *	Transferring a call to another phone.

Call hold in the US

Using call waiting, you can press the button to flash call (**AND**) hold.

If you register a new incoming call, press the flash. This will toggle between calls with caller A and B holding the gradual.

If you have an incoming call on hold and hung up the phone, the phone rings.

Call waiting in USA

This feature allows you to hold the current call and answer the second, the same telephone number.

When the phone registers another call, notify you by an audible signal.

To hold the first call and answer the second call, press flash.

Transferring a call in the US

This feature allows you to transfer an incoming call (received) to another phone.

Step 1 Press Flash currently hold the ongoing call.

step 2 When you hear dial tone, press the key combination **** 98 # "** and enter the number you
To transfer the call.

step 3 After you hear another phone ringing, hang up the phone currently in use.

---- End

Three-way conference call in the US

Here's how to make a three-way conference call.

Step 1 Once you speak to someone, press flash. This will call hold and ringing a dial tone.

step 2 Enter the phone number to start a new call.

step 3 Once the other party accepts the new call, press the flash will create conference call.

step 4 To break the connection simply hang up.

step 5 To the ongoing conference call into two separate calls (one will active and one on hold), press the flash.

step 6 If you want to re-join participants in the conference call, press the button again flash.

step 7 To re-establish the conference call into two separate calls, press flash. This time, the call connection with a second subscriber, the first call is put on hold.

---- End

16 status LTE

16.1 Overview

Screen **status LTE** It contains detailed information on the ongoing LTE connectivity.

Figure 16-1 System Monitor> Status LTE

Na stránce níže najdete detailní informace o LTE připojení.

Interval obnovení: 5 sek. ▾

Stav zařízení			
Softwarová verze	B2368_V100R001C00SPC026T	IMEI zařízení	355968053041660
Softwarová verze modulu	11.620.18.21.00	IMSI SIM karty	23001500509****
Stav LTE			
Stav	LTE 	Čas běhu připojení	0 den/(dny), 1 hodina(-y),13 minuta(-y),3 0 sekunda(-y)
Poskytovatel služby	T-Mobile CZ	ICCID	8942001140318387022F
Síla signálu	-64 dBm	SINR	20 dB
RSRP	-86 dBm	RSRQ	-5 dB
Kmitočtové pásmo	band 3	DL EARFCN	1579
Duplexní mód	FDD	APN	Auto / cpemngmt
RANK	2	Šířka pásma	20MHz
Global Cell ID	2300140501887715	PCI	159
Stav konfigurace CA	DL	Stav aktivace CA	Deaktivováno
UL rychlost	0 kbps	DL rychlost	0 kbps
CQI	14 14	Stav datového roamingu	Domácí síť
ECGI	230011887715	ECI [HEX / DEC]	1887715 / 25720597
eNB ID [DEC]	100471	Cell ID [DEC]	21

17 system logs

17.1 Overview

Web configuration interface also allows you to specify which categories of events and / or alerts will be stored in the system log LTE modem, and then view these logs or send an e-mail address of the administrator or log server.

17.1.1 What You Need to Know

Before reading this chapter is to be familiar with the following terms.

Alerts and logs

Caution is the type of record that requires special attention. Among alerts include system failures, attacks (access control) and attempt to access blocked websites. Some level events, such as **system failure**, They consist of log and alert at the same time. Their list is on the screen **system log** and they are distinguished by color. While warnings are displayed in red, log entries are black.

Overview of system log

The protocol system log allows devices to send messages about events across the IP network to the log servers that these event messages are stored. Enabled device system log can generate a log entry and send it to the server log.

Definition of the system log is specified in RFC 3164th The RFC defines the packet format, content and other necessary information to the system log. Each message in the system log identifier and has a severity level. Identifier refers to a specific file on the server log. For more information, see the program documentation management system log. The following table describes the severity level of each entry in the system log.

Table 17-1 Severity level of system log

CODE	LEVEL
0	Emergency (EMERG): The system is unusable.
1	Alert (ALERT) is required immediate action.

CODE	LEVEL
2	Critical event (CRIT): The system is in critical condition.
3	Fault (ERROR): In a system fault has occurred.
4	Warning (WARNING): In an event has occurred that requires attention.
5	Notice (NOTICE): In an event occurred that does not adversely affect the system, but it requires attention.
6	Information (INFO): For information on current events in the system log.
7	Debugging (DEBUG) messages intended for debugging purposes.



NOTE

The LTE modem supports system log records with severity levels ERROR, INFO, and DEBUG.

17.2 System Log Screen

screen **system log** by clicking on **System Monitor> Log. Screen**

system log provides an overview of records in the system log, which can be filtered through a drop-down list in the upper left corner.

Figure 17-1 System Monitor> Log> System Log

#	Čas	Úroveň	Zpráva
1	Jan 1 08:00:19	info	Device is not on roaming status.
2	Jan 1 08:00:24	info	SIM Card Requests PIN Code [last message repeated 10 times in 51 seconds]
3	Jan 1 08:01:19	info	Temperature=33.0°C

The following table summarizes the available fields on this screen.

Table 17-2 System Monitor> Log> System Log

Item	Description
	Through the first drop-down list, select the type of record you want to view. (Available options: All DHCP, System Management, Remote Management, TR-069, NTP, ethers, DDNS, NAT, attack, ACL, LTE)
Level	Using this system, the drop-down, select the severity level. The table below displays results that match the filter settings. Once you select a certain level of severity, they will show those records that match the higher level of severity. For more information about the different levels of severity, see Table 17 to 1
Restore	Click to refresh the list of records in the system log.

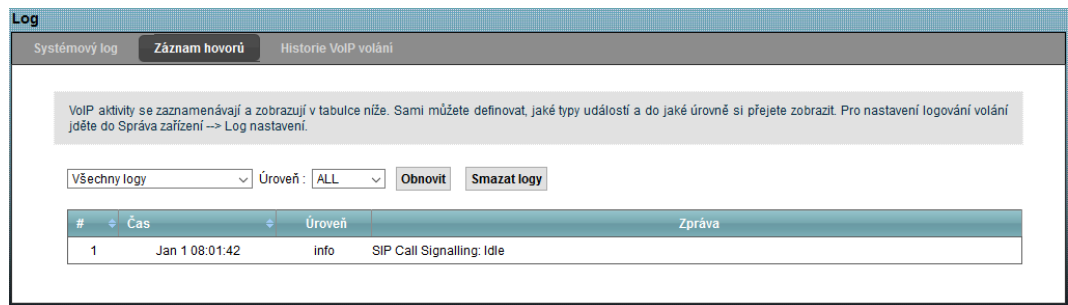
Item	Description
delete logs	Click to remove all entries in the log.
#	This field indicates the serial number only and is not connected with the corresponding item in the list.
Time	This field contains the date and time of the event record.
Level	In this field, the level of severity, the device will send to the server log.
Message	This field is a detailed description of the record.

17.3 Screen Call Recording

screen call recording by clicking on **System Monitor> Call log**.

On this screen, there is a record of calls and warning messages associated with telephony. You can adjust the type and severity level records to display.

Figure 17-2 System Monitor> Log> Call Recording



The following table summarizes the available fields on this screen.

Table 17-3 System Monitor> Log> Call Recording

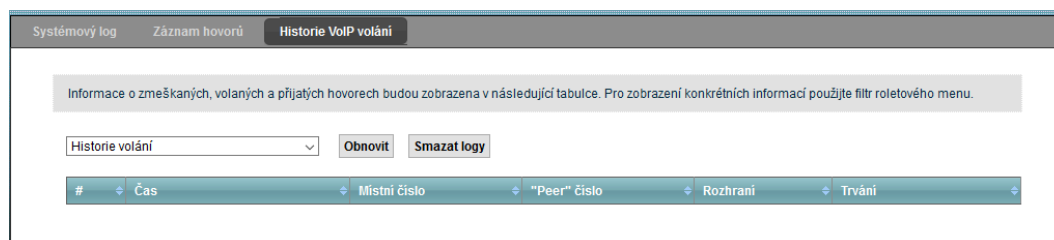
Item	Description
	From the drop-down list, select a category of alert you want to view. Choice all logs All displayed.
Level	Select the severity level you want to view.
Restore	Click to refresh the list of records in the system log.
delete logs	Click to remove all entries in the log.
#	This field indicates the serial number only and is not connected with the corresponding item in the list.
Time	This field contains the date and time of the event record.

Item	Description
Level	In this field, the level of severity, the device will send to the server log.
Message	This field is a detailed description of the record.

17.4 Screen History VoIP calls

screen **VoIP Call History** by clicking on **System Monitor> Log> History of VoIP calls**. On this screen you will see a list of calls made through VoIP LTE modem.

Figure 17-3 System Monitor> Log> History VoIP calls



The following table summarizes the available fields on this screen.

Table 17-4 System Monitor> Log> History VoIP calls

Item	Description
	From the drop-down list, select a category of alert you want to view. Choice call History displays all records.
Restore	Click to refresh the list of records in the system log.
delete logs	Click to remove all entries in the log.
#	This field indicates the serial number only and is not connected with the corresponding item in the list.
Time	This field contains the date and time of the event record.
local number	This field indicates the number that you used to make the call.
"Peer" number	This field indicates the number of the second participant of the call.
Interface	This field is the type of call.
Duration	This field specifies the duration of the call.

18 User account

18.1 Overview

Screen **User account** to set a password for each user account. For additional safety, we recommend strengthening passwords be changed regularly.

18.2 Screen User Account

On the screen **User account** You can change the password to your account.

The following screen, click on **Device Management> Manage Account**.

Figure 18-1 Device Management> Manage Account

Heslo, které používáte pro přihlášení, můžete změnit na této stránce. Heslo je platné okamžitě po změně a pro příští přihlášení je nutné použít již nové heslo. Heslo musí obsahovat 8 až 15 znaků - velká písmena, malá písmena, číslice nebo ASCII symbol.

Heslo nesmí obsahovat uživatelské jméno, a to ani pozpátku, nebo více než dva po sobě jdoucí stejné znaky.

Z důvodu zvýšení bezpečnosti doporučujeme pravidelně měnit vaše heslo.

Uživatelské jméno:

Stávající heslo:

Nové heslo:

Potvrdit nové heslo:

The following table summarizes the available fields on this screen.

Table 18-1 Device Management> Manage Account

Item	Description
Username	You can change the password to your account user (user account).
existing password	Enter the default or existing password you use to log into the configuration interface.

Item	Description
New password	Enter a new password (up to 30 characters). Keep in mind that for security reasons will be writing individual password characters appear as dots (•). After changing the password in the configuration interface LTE modem only, login with your new password.
Confirm New Password	Enter the new password again for verification.
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

19 System

19.1 Overview

Screen **System** is used to configure the system, such as host name, domain name or inactivity timer. Screen **encryption key** to update the encryption key.

19.1.1 What You Need to Know

Before reading this chapter is to be familiar with the following terms.

domain name

The network address that identifies the owner of the network connection. For example, for addresses *www.example.com/support/files* a domain name *www.example.com*.

encryption key

LTE modem works with encryption key for secure communication between outdoor and indoor unit. Before the first use of the modem are advised to update the encryption key.

19.2 Display System

using the screen **System** You can make your system settings, such as host name, domain name or inactivity timer.

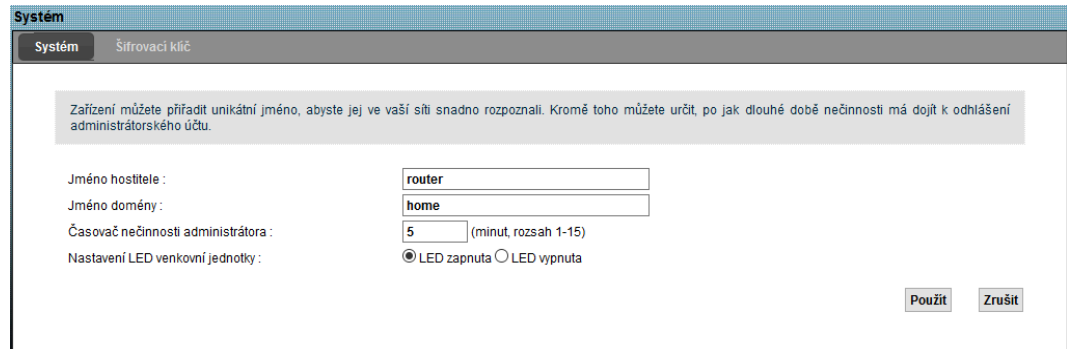
Field **hostname** used solely for identification purposes. Some ISPs verify the name, type, therefore the name of the computer you are using. The computer name can be taken from the Windows Operating System.

Right-click on **This computer** from the context menu select **Properties**.

Remember amended entries **Full computer name** and enter the name in the field **hostname** in the configuration interface.

The following screen, click on **Device Management> System**.

Figure 19-1 Device Management> System



The following table summarizes the available fields on this screen.

Table 19-1 Device Management> System

Item	Description
Host Name	Enter a descriptive hostname for identification purposes. We recommend to put into the field by a full computer name as it is listed in the Windows Operating System. The name can be up to 30 alphanumeric characters long. Spaces are not allowed, but hyphens "-" and underscores "_" Yes.
Domain name	Enter the domain name if you know it. If you leave this field empty, it is possible that your ISP will assign a domain name via DHCP. User-specified domain name takes precedence over automatically assigned.
The inactivity timer admin	Specify the length of time of inactivity will log off the administrator account from the Web configuration interface. The default is 5 minutes. After the expiration of this period it is necessary to log in again. Too long inactivity period is a potential security risk.
Setting LED outdoor unit	This setting is used to enable or disable the LED outdoor unit. choose LED is turned on, if you want the LED lights in the outdoor unit. choose LED is off, if you want LED outdoor unit go out.
Use	Click Apply to save changes made to the settings LTE modem.
Cancel	Click Cancel to discard.

Screen 19.3 Encryption Key

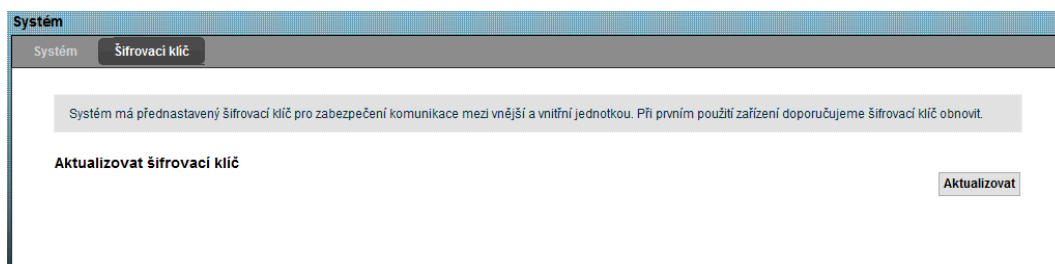
LTE modem works with encryption key for secure communication between outdoor and indoor unit. Before the first use of the modem are advised to update the encryption key.

There are three scenarios in which you should consider updating the encryption key:

19.3.1 Common usage: Set of indoor and outdoor unit

Step 1 The following screen, click on **device Management > system > Encryption key**.

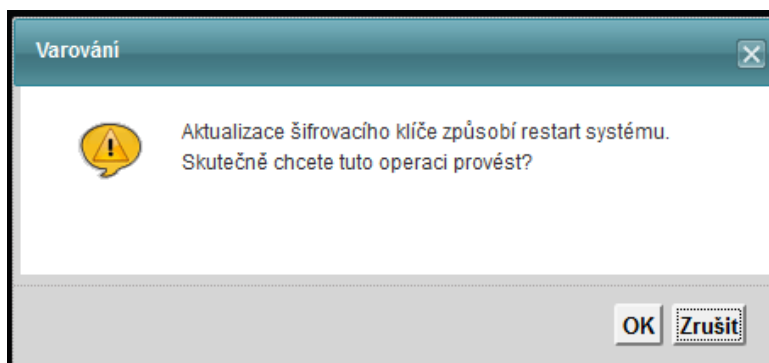
Figure 19-2 Device Management> System> Encryption Key.



step 2 To update the encryption key click **Update**.

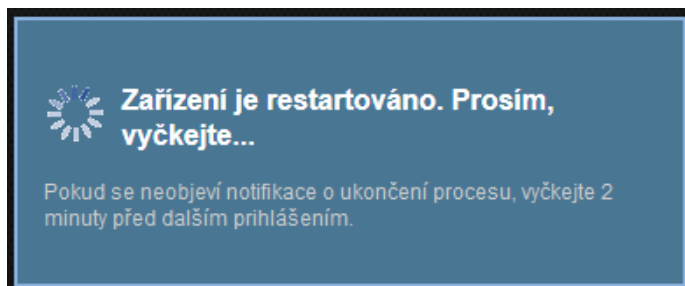
step 3 A dialog box appears to confirm the update. Click on **OK**.

Figure 19-3 Device Management> System> Encryption key> Update



step 4 Wait for the successful restart LTE modem.

Figure 19-4 Device Management> System> Encryption key> Update: Restart



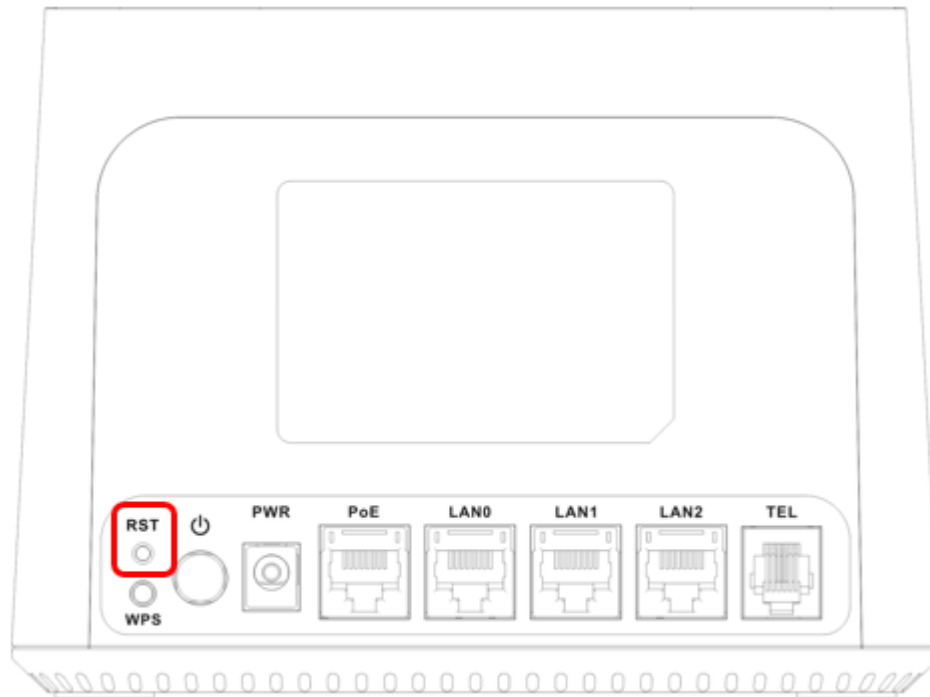
---- End

19.3.2 A new outdoor unit and indoor unit original

Perform the following procedure when replacing the outdoor unit with a new one, but you still have the original indoor unit.

Step 1 Press and hold the reset button on the indoor unit for at least 10 seconds. then wait to complete reboot the device.

Figure 19-5 RESET button on the indoor unit



step 2 Upon restart, use the username and password for the network, which is stated on the label interior unit.

---- End

19.3.3 A new indoor unit and outdoor unit original

Step 1 If you are replacing an internal drive, but you still have the original outdoor unit, update encryption key via the instructions in Section 19.3.1 Common usage: Set of indoor and outdoor units.

First screen encryption key click on **device Management > system > encryption key**.

Second To update the encryption key click **Update**.

Third A dialog box appears to confirm the update. Click on **OK**.

4th Wait for the successful restart LTE modem.

step 2 Log into the web configuration interface, go to **device Management > Backup / Restore > Back to the default settings**, click on **reset** and wait to reset the modem.

step 3 Upon restart, use the username and password for the network, which is stated on the label interior unit.

---- End

20 Time setting

20.1 Overview

Screen **Time setting** used to set the system date and time.

20.2 Settings screen time

To change the system date and time LTE modem, click on **Device Management> Set time**. The screen below. Using this screen, you can adjust the system time LTE modem based on the current time zone.

Figure 20-1 Device Management> Time Settings

Aby zařízení mohlo získávat správný čas, vyplňte adresu časového serveru, zvolte časovou zónu fyzického umístění zařízení a podle potřeby nastavte letní čas.

Aktuální datum/čas

Aktuální čas: 08:03:22
Aktuální datum: 2017-01-01

Nastavení času a data

NTP: Povolit Zakázat
Protokol času: NTP
Adresa časového serveru: 0.europe.pool.ntp.org
Manuální čas: 08 03 15 (HH/MM/SS)
Manuální datum: 2017 01 01 (RRRR/MM/DD)

Časová zóna

Časová zóna: (GMT+01:00) Berlín, Stockholm, Řím, Bern, Brusel, Vídeň, Praha
 Nastavení letního času
Datum začátku: Poslední Neděle v březnu (2017-03-26) v 2 hodin
Datum konce: Poslední Neděle v říjnu (2017-10-29) v 3 hodin

Použit Zrušit

The following table summarizes the available fields on this screen.

Table 20-1 Device Management> Time Settings

Item	Description
------	-------------

Item	Description
Current date / time	
current time	This field is given the system time LTE modem.
The current date	This field indicates the system date LTE modem.
Time and date settings	
NTP	Choose Allow, if you want to enable automatic updating of date and time from the specified NTP server. Choose Prohibit to manually enter the system time and date LTE modem.
time protocol	Time service protocol through which to communicate with the NTP server LTE modem.
Address of the time server address	Enter the IP address or URL (up to 31 characters in the extended ASCII) time server that you want to use. If you are unsure of the address, contact your ISP or network administrator.
manual time	Using these fields, you can manually enter the time in hours, minutes and seconds.
manual date	Using these fields, you can manually enter a date in years, months and days.
Time zone	
Time zone	Enter the time zone where you currently are. This parameter sets the difference between your time zone and Greenwich Greenwich Mean Time (GMT).
Daylight saving time settings	Summer time is a period from late spring to early fall when many countries set their time ahead of normal local time by one hour. The result is more daylight in the evening. Check this box if you are in your area uses daylight saving time.
start date	<p>If the option is checked Setting Daylight Saving Time Here enter the date and time of its beginning. Field hours indicates the time in 24-hour format. Here are a few examples:</p> <p>Daylight saving time starts in most parts of the United States, the second Sunday of March. Each time zone in the United States will start using daylight saving time at 2 am local time. So, if you are in the United States, enter into these fields in this order values Second, Sunday, in March and 2 the box hours.</p> <p>Daylight saving time begins in the European Union last Sunday in March. All time zones in the European Union will start using daylight saving time at the same time - at 1 am GMT or UTC. So if you are in the European Union, to enter these fields in this order values Last Sunday, in March. The time you enter in the field</p> <p>hours will vary according to the time zone you are in. For example, in Germany it will be 2 Because the time zone in Germany is one hour ahead of GMT (GMT + 1).</p>

Item	Description
end date	<p>If the option is checked Setting Daylight Saving Time Here enter the date and time of the end. Field hours indicates the time in 24-hour format. Here are a few examples: Daylight saving time ends in most parts of the United States, the first Sunday in November. Each time zone in the United States stops using Daylight Saving Time at 2 am local time. So, if you are in the United States, enter into these fields in this order values</p> <p>First, Sunday, in November and 2 the box hours.</p> <p>Daylight saving time ends in the European Union last Sunday in October. All time zones in the European Union stop using Daylight Saving Time at the same time - at 1 am GMT or UTC. So if you are in the European Union, to enter these fields in this order values Last Sunday, in October. The time you enter in the field hours</p> <p>will vary according to the time zone you are in. For example, in Germany, it will be 2 because the time zone in Germany is one hour ahead of GMT (GMT + 1).</p>
Use	Clicking Use save your changes.

21 setting up logging

21.1 Overview

Setting logging defines what types of logs and to what levels will be recorded on the screen **System log**.

21.2 Settings screen logging

To change the logging LTE modem, click on **Device Management> Log Settings**. The screen below.

Figure 21-1 Device Management> Settings logging

Nastavení logování definuje, jaké typy logů a do jaké úrovně si přejete zaznamenávat.

Aktivní log a volba úrovně	Úroveň logování
Kategorie logu	
VoIP	
<input type="checkbox"/> VoIP - statistiky hovorů	ALL
<input checked="" type="checkbox"/> VoIP - signalizace SIP volání	ALL
<input checked="" type="checkbox"/> VoIP - SIP registrace	ALL
<input type="checkbox"/> VoIP - události telefonování	ALL
<input type="checkbox"/> VoIP - různé	ALL
Systém	
<input checked="" type="checkbox"/> LTE	ALL
<input checked="" type="checkbox"/> DHCP	ALL
<input checked="" type="checkbox"/> Údržba systému	ALL
<input checked="" type="checkbox"/> Vzdálená správa	ALL
<input checked="" type="checkbox"/> TR-069	ALL
<input type="checkbox"/> NTP	ALL
<input type="checkbox"/> DDNS	ALL
<input type="checkbox"/> NAT	ALL
<input type="checkbox"/> Attack (útok)	ALL
<input type="checkbox"/> ACL	ALL

Použit **Zrušit**

The following table summarizes the available fields on this screen.

Table 21-1 Device Management> Time Settings

Item	Description
Active log and option levels	
Categories Select	Category log entries that you want to save.
Log level	Select the severity level of events that you wish to record. If you want to save all log events, select ALL .
Use	Clicking Use save your changes.
Cancel	Click on Cancel restore previous settings in this section.

22 software upgrade

22.1 Overview

This chapter describes how to update the software (firmware) of your LTE modem.



NOTICE

Only use firmware designed for your specific model. The model name can be found on a label on the back of an LTE modem.

Screen 22.2 Software Upgrade

The following screen, click on **Device Management**> **Software Upgrade**.

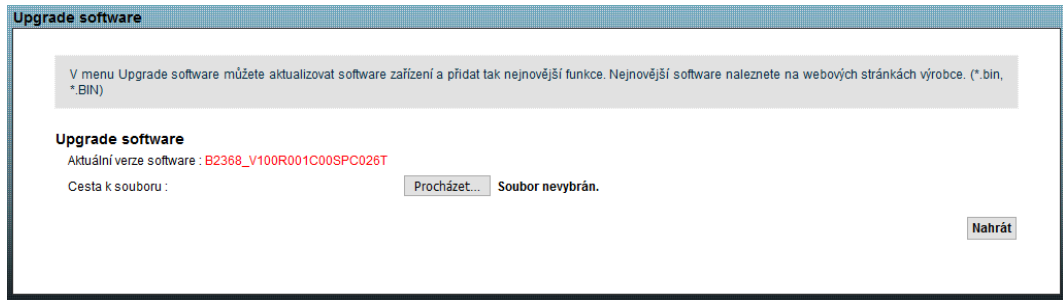
The upgrade process takes place via HTTP (Hypertext Transfer Protocol) and may take up to five minutes. After successfully uploading the update file will restart the system.



NOTICE

During the update, DO NOT turn off LTE modem fundamentally!

Figure 22-1 Device Management> Software Upgrade



The following table summarizes the available fields on this screen.

Table 22-1 Device Management> Software Upgrade

Item	Description
software upgrade	
The current version of the software	This is the current version of the device firmware.
File Path Click Browse ... and select the location of the update file.	Note: If there is a firmware update modem and router, modem firmware update first and then to the router.
Record	After setting the path to the file to start the update process by clicking Record. This process can take up to five minutes.

After updating LTE modem, wait a few minutes before re-logging into the configuration interface.

Figure 22-2 Warnings for firmware update

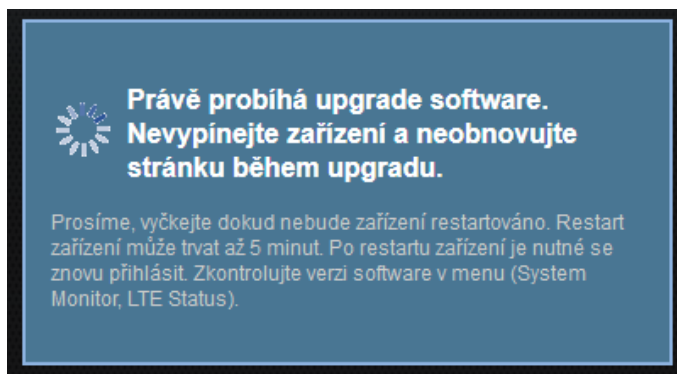
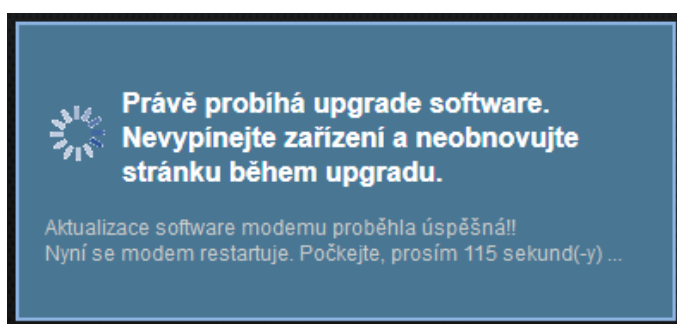


Figure 22-3 Warnings for the Firmware Update: Update in Progress

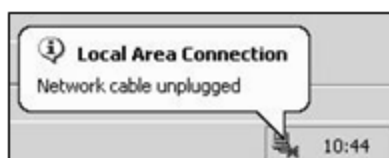


Figure 22-4 Use caution when updating the firmware: Restarting



LTE modem at this point will automatically restart, causing the network is temporarily unavailable. For some operating systems, you can see the icon in the notification area.

Figure 22-5 The network was temporarily disconnected



After two minutes, log in again to the management interface and check the new firmware version on the screen **Information** about the system.

If the firmware update failed, an error message will be displayed. Clicking **OK** to return to the screen **Upgrade software**.

23 online updates

23.1 Overview

This chapter describes how to use the screen **online updates** upload new firmware version via the Internet.



NOTICE

Only use firmware designed for your specific model. The model name can be found on a label on the back of an LTE modem.

23.2 Screen Online Update

The following screen, click on **Device Management> Online Update**.

The upgrade process is carried out using HTTPS (Secure Hypertext Transfer Protocol) or HTTP (Hypertext Transfer Protocol) and may take up to five minutes. After successfully uploading the update file will restart the system.



NOTICE

During the update, DO NOT turn off LTE modem fundamentally!


If you want to automatically check for updates online to off, select the menu **Periodic online updates possibility Prohibit**.

Figure 23-1 Device Management> Online Update: Disable

Online aktualizace

Periodická online aktualizace :

URL serveru :

 **Poznámka :**
Doba aktualizace specifická pro zařízení závisí na poskytovateli internetových služeb.

If you want to LTE modem regularly check for a new version of firmware and alert you to select the menu **Periodic online updates possibility Check software and alert**. Once LTE modem detects the presence of a new version of the firmware, a pop-up window on the screen **connection status** or **Online update**.

Figure 23-2 Device Management> Online Update: Check software and warn


Online aktualizace

Periodická online aktualizace :

Perioda kontroly :

Čas kontroly :

URL serveru :

 **Poznámka :**
Doba aktualizace specifická pro zařízení závisí na poskytovateli internetových služeb.

If you want to LTE modem periodically check for new firmware is installed and automatically select the menu **Periodic online updates possibility Check software and automatically updated**.

Figure 23-3 Device Management> Online Update: Check the software and automatically update


Online aktualizace

Periodická online aktualizace :

Perioda kontroly :

Čas kontroly :

URL serveru :

 **Poznámka :**
Doba aktualizace specifická pro zařízení závisí na poskytovateli internetových služeb.

If you select **Check software and warn** or **Check software and automatically update** you will be able to set the time in which to carry out a control (**Time controls**).

NOTICE

As the server URL, use only link that you received from your service provider!

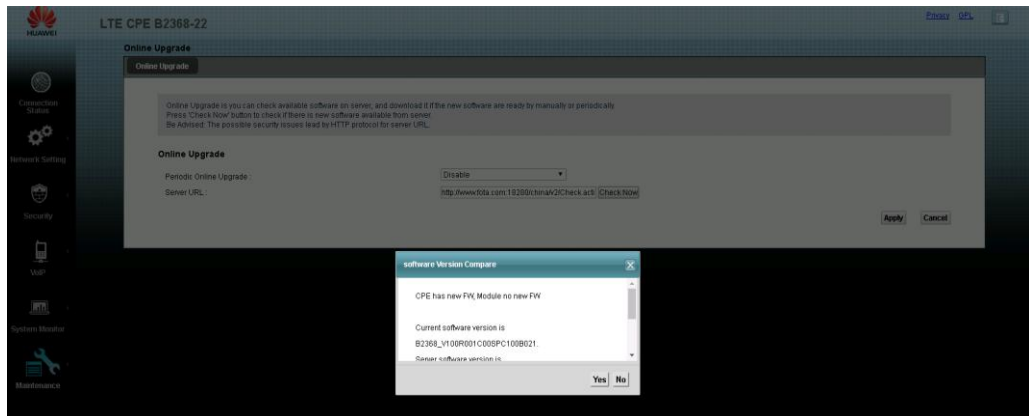
Enter the server address in the box **server URL** and click on **Use** to start the process of checking the new firmware version from the server. We recommend that you use addresses with the prefix HTTPS, while HTTP is also supported.

23.3 Types of online updates

Firmware update is possible in the following cases:

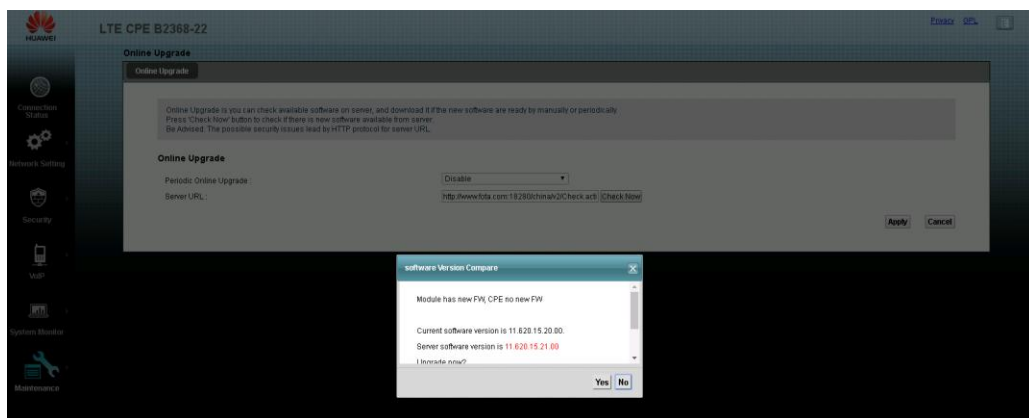
There is a new version of firmware for the LTE modem (CPE unit), but not for the LTE module.

Figure 23-4 Device Management> Online Update: Update only CPE units



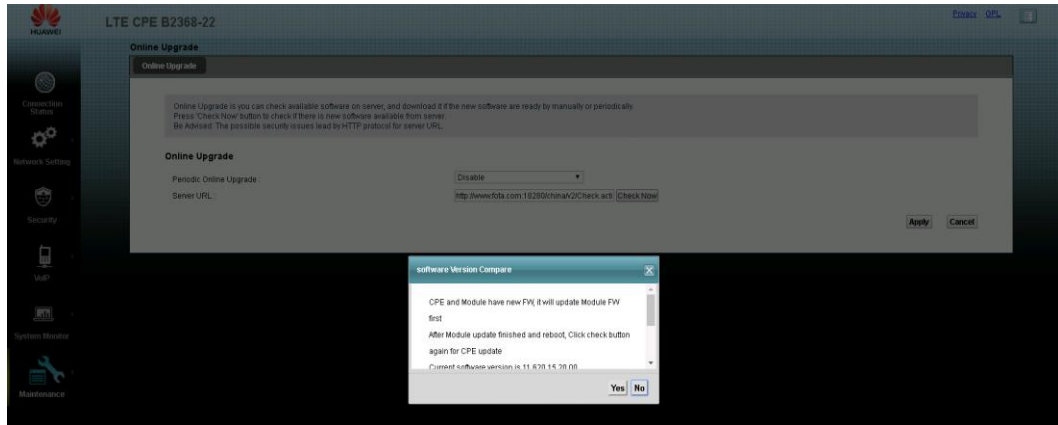
There is a new version of firmware for the LTE module, but not for LTE modem itself.

Figure 23-5 Device Management> Online Update: Update only LTE module



There is a new version of firmware for both LTE modem (CPE unit) and LTE module. In this case, the earliest date firmware upgrade LTE module.

Figure 23-6 Device Management> Online Update: Firmware update for modem and LTE module



23.4 online update process

The procedure for updating firmware LTE or LTE modem module

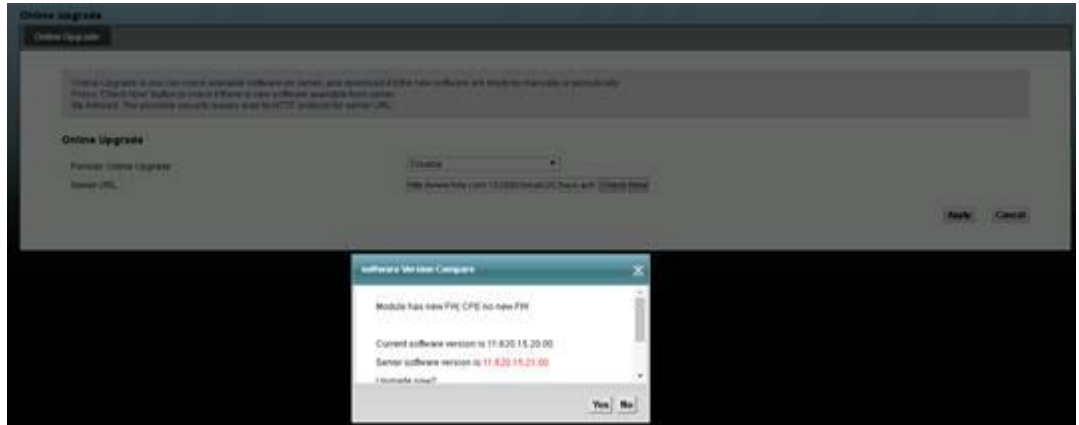
Step 1 Click on **Device Management> Online Update**. Set parameter **Periodic online update** on **Prohibit**. Fill in the URL of the site, click on **Use** and then **Check**.

Figure 23-7 Device Management> Online Update: Entering URLs



step 2 If there is a new firmware version, a pop-up window.

Figure 23-8 Device Management> Online Update: popup announcing the availability of a new firmware module



step 3 Click on the button **Yes** to start updating. During the update will be displayed Pop-up on the progress of the update. If you do not want or need the firmware update, click on **No** or click **X**. Pop-up window will close, and the update will not run.

Figure 23-9 Device Management> Online Update: Warning firmware update



Figure 23-10 Device Management> Online Update: Firmware Update progress - 25%

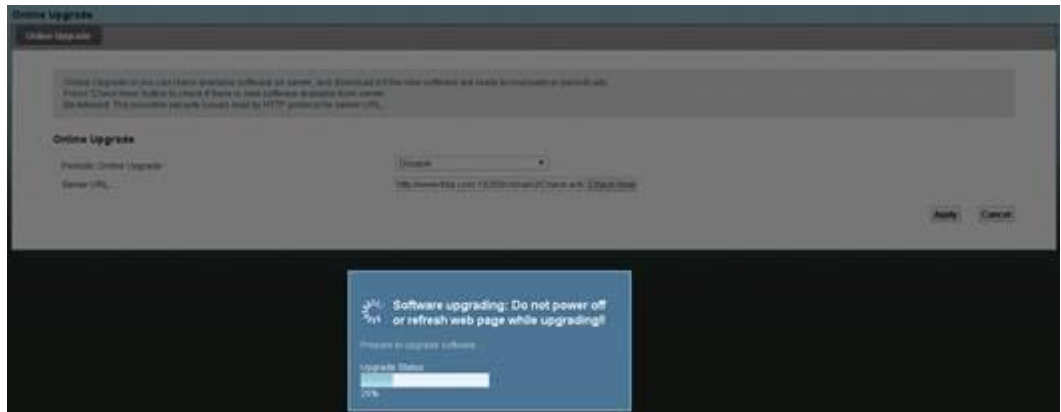


Figure 23-11 Device Management> Online Update: Firmware Update progress - 50%

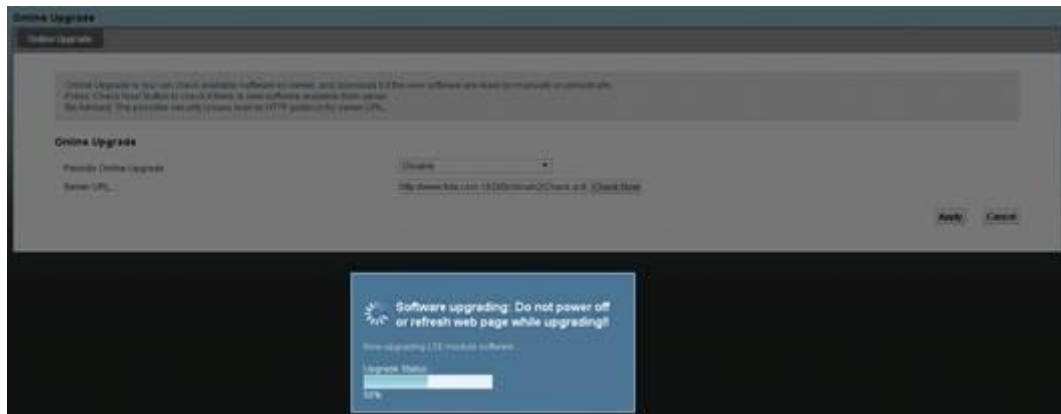
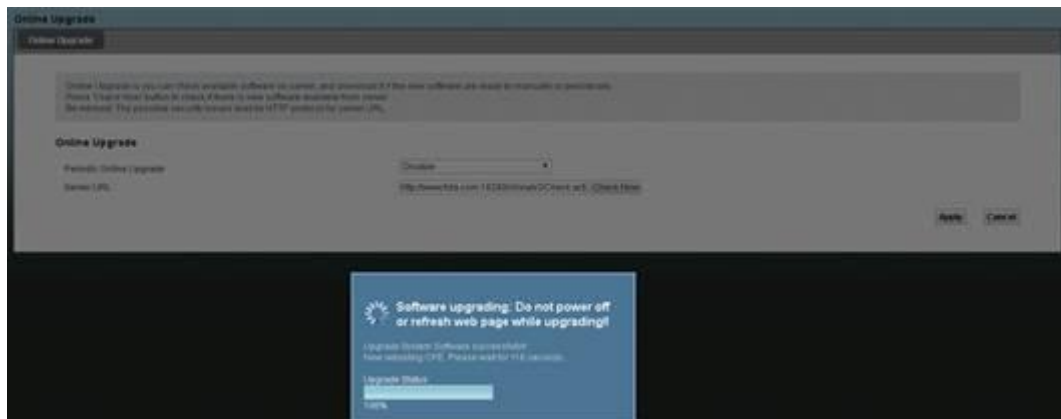


Figure 23-12 Device Management> Online Update: Firmware Update progress - 100%



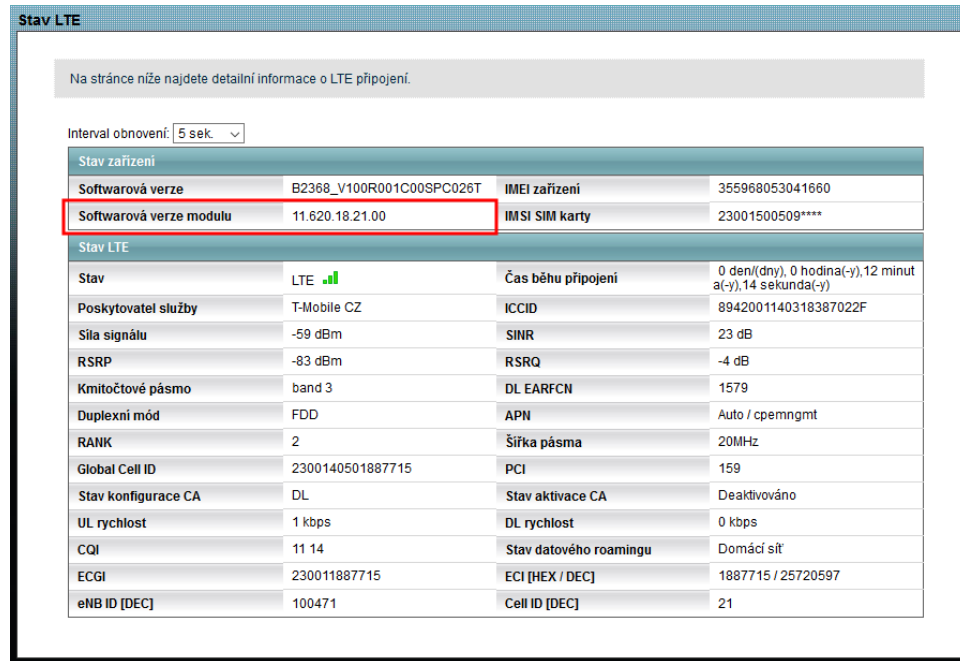
step 4 Under normal circumstances, it takes firmware updates for approximately five minutes. After a successful update login screen.

- During the update process is required only once to confirm the update. You do not need any software or hardware tools.
- If for any reason during the update error, performs LTE modem refit the previous firmware version.

step 5 Log in to the management interface and on-screen System Monitor> Status LTE

Check correct firmware version of the module.

Figure 23-13 System Monitor> Status LTE: To check the software version



---- End

The procedure for updating firmware LTE and LTE modem module simultaneously

Step 1 Click on Device Management> Online Update. Set parameter Periodic online update on Prohibit. Fill in the URL of the site, click on Check.

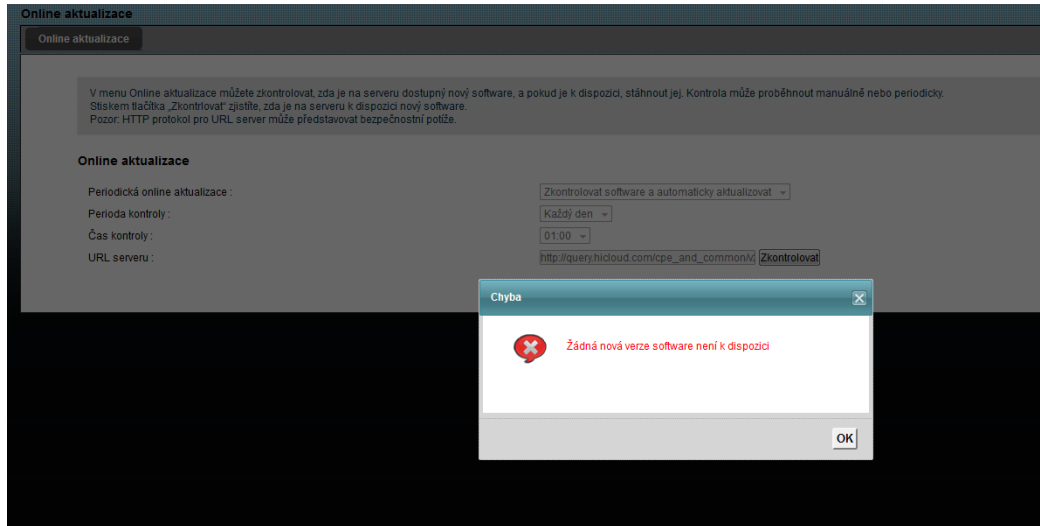
Figure 23-14 Device Management> Online Update: Entering URLs



step 2 If there is a new firmware version, a pop-up window. If the
There updating firmware and modem module will first firmware update

modem and then to LTE module. After the update completes LTE module can switch back to the screen **online updates** and perform a firmware upgrade LTE modem.

Figure 23-15 Device Management> Online Update: popup announcing the availability of a new firmware CPE unit and the LTE module



step 3 Click on the button **Yes** to start updating. During the update will be displayed **Pop-up on the progress of the update**. If you do not want or need the firmware update, click on **No** or click **X**. Pop-up window will close, and the update will not run.

Figure 23-16 Device Management> Online Update: Warning firmware update



Figure 23-17 Device Management> Online Update: Firmware Update progress - 25%

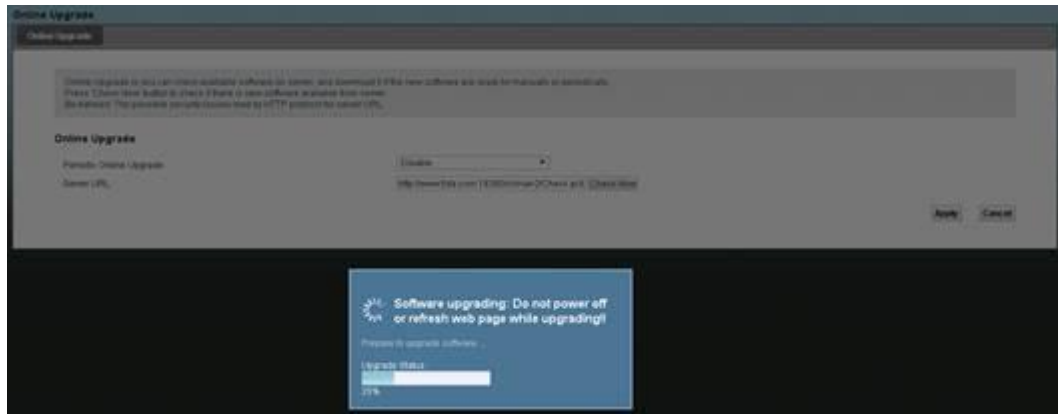


Figure 23-18 Device Management> Online Update: Firmware Update progress - 50%

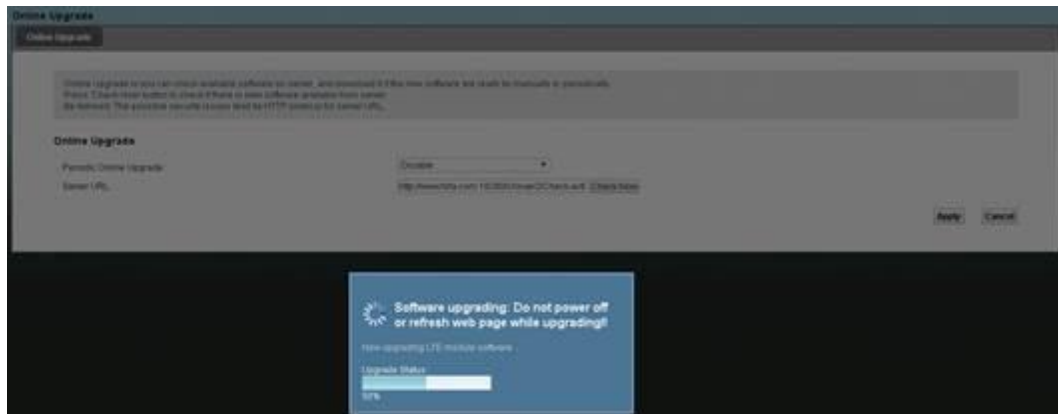
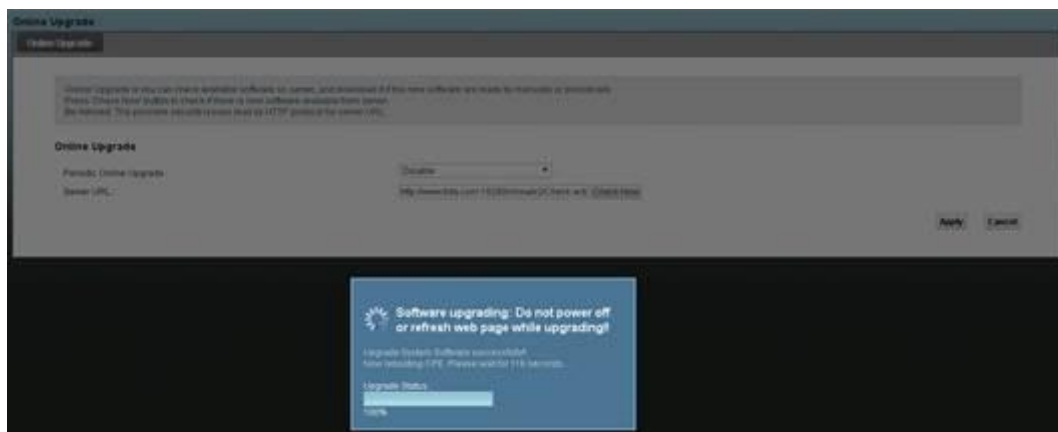
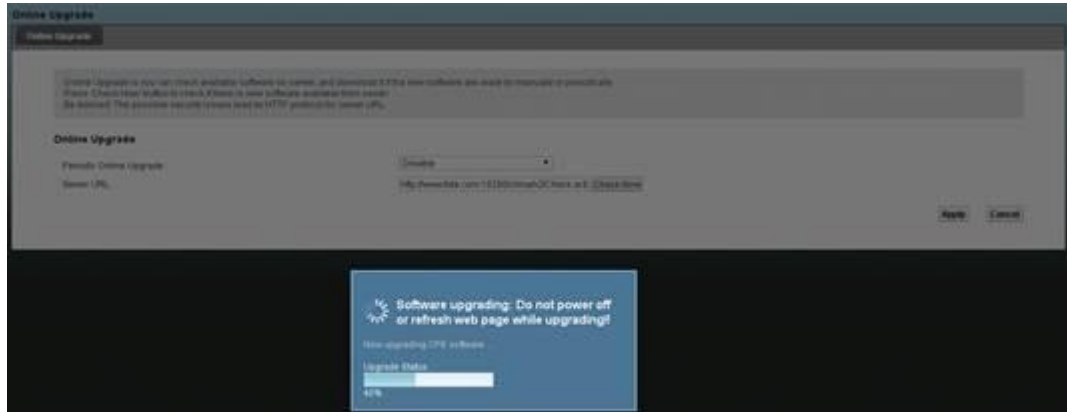


Figure 23-19 Device Management> Online Update: Firmware Update progress - 100%



step 4 After a successful update the login screen. Log in to the configuration interface and on-screen **System Monitor> Status LTE** Check correct firmware version of the module.

Figure 23-22 Device Management> Online Update: Firmware Update progress - 40%



step 6 After a successful update the login screen. Log in to the configuration interface and on-screen **System Monitor> Status LTE** Check correct firmware version.

Figure 23-23 System Monitor> Status LTE: To check the software version

Stav LTE

Na stránce níže najdete detailní informace o LTE připojení.

Interval obnovení: 5 sek. ▾

Stav zařízení			
Softwarová verze	B2368_V100R001C00SPC026T	IMEI zařízení	355968053041660
Softwarová verze modulu	11.620.18.21.00	IMSI SIM karty	23001500509****

Stav LTE			
Stav	LTE	Čas běhu připojení	0 den/(dny), 0 hodina(-y), 13 minut a(-y), 13 sekunda(-y)
Poskytovatel služby	T-Mobile CZ	ICCID	8942001140318387022F
Síla signálu	-56 dBm	SINR	22 dB
RSRP	-82 dBm	RSRQ	-5 dB
Kmitočtové pásmo	band 3	DL EARFCN	1579
Duplexní mód	FDD	APN	Auto / cpeimgmt
RANK	2	Šířka pásma	20MHz
Global Cell ID	2300140501887715	PCI	159
Stav konfigurace CA	DL	Stav aktivace CA	Deaktivováno
UL rychlost	0 kbps	DL rychlost	0 kbps
CQI	12 14	Stav datového roamingu	Domácí síť
ECGI	230011887715	ECI [HEX / DEC]	1887715 / 25720597
eNB ID [DEC]	100471	Cell ID [DEC]	21

---- End

24 Backup / Restore

24.1 Overview

Screen **Backup / Restore** allows backup and restore settings saved configurations. It also allows resetting the device to factory settings.

Screen 24.2 Backup / Restore

Step 1 Click on **Device Management> Backup / Restore**. On this screen are available

information relating to the default settings, configuration backup and restoration of configuration, as shown in the following figure.

Figure 24-1 Click on the Device Management> Backup / Restore.

Obnovením výchozích nastavení z výroby můžete zařízení resetovat.

Zpět na výchozí nastavení

Kliknutím na Reset smažete všechny uživatelem zadané konfigurační informace a vrátíte se k výchozím nastavením z výroby. Po resetu bude LAN IP adresa 192.168.1.1 DHCP se resetuje na server.

Reset

---- End

backup log

Step 1 Backup function log is used to store the backup system log file LTE modem

on your computer. If you notice that the LTE modem behaves uncharacteristically, we strongly recommend that before making any changes to back up the log. Backup system log will be useful in case you have to contact the service center.

step 2 Clicking **backup log** save the system log file LTE modem in

counting.

---- End

configuration backup

Step 1 Configuration backup function is used to store a backup of the current configuration in LTE modem file on your computer. If you notice that the LTE modem behaves uncharacteristically, we strongly recommend that before making any changes to back up your current configuration. Backup system configuration is useful if you have to restore modem settings.

step 2 Clicking **Back up save the system configuration LTE modem to a file** in counting.

---- End

restore configuration

Restore configuration function is used to load system configuration LTE modem from a backup file.

Table 24-1 restore configuration

Item	Description
File path	Click on the button Browse ... and use the File Explorer to locate the backup configuration file.
Browse ...	Click this button to select the backup file.
Record	Click this button to start recording file.

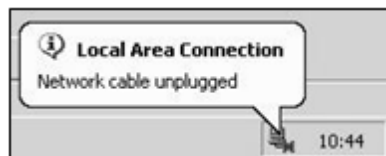


During file upload the backup configuration LTE modem fundamentally turn off.

Following the successful reconfiguration LTE modem from backup to the login screen. Log off and restart the LTE modem.

LTE modem at this point will automatically restart, causing the network is temporarily unavailable. For some operating systems, you can see the icon in the notification area.

Figure 24-2 The network was temporarily disconnected



After restoring the default configuration, you may need to change the IP address of your computer so that it is in the same subnet as the default IP address (192.168.1.1).

If the renewal failed, you will receive an error message. Clicking **OK** to return to the Settings screen.

Back to default

- Clicking **reset** delete all user-entered values and settings. LTE modem will be restored to the factory. The following window appears with a warning.

Figure 24-3 A warning message before resetting

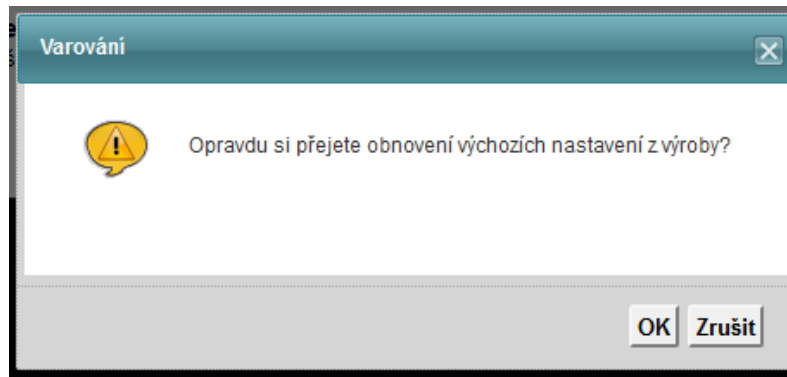
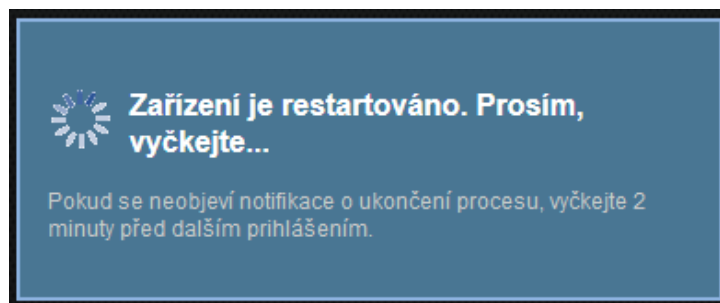


Figure 24-4 Pop-up window showing the reset



- LTE modem reset back to factory default settings, it is also possible to press **RESET** on the rear panel. More information about the key **RESET** please see chapter 1.7.

25 screen Restart

Restart the system is used for opening and closing LTE modem without the need to disconnect from the network. This procedure is suitable eg. In situations where LTE modem stops responding.

Step 1 Click on **Device Management** > **Restart**. Click on the button **restart** to restart LTE modem. Restarting will not affect the settings LTE modem.

Figure 25-1 restart

Restart provede opětovné spuštění softwaru zařízení. K zařízení se poté budete moci přihlásit až několik minut po restartu.

Restart systému

Restart

---- End

26 diagnostics

26.1 Overview

To test the connection and view detailed information, you can use various diagnostic methods. These read-only screens display information to help you identify problems with an LTE modem.

Screen 26.2 Ping / TraceRoute

Pings and traceroute help check the availability of the remote host and also in solving problems with network or internet connection. Click on **Device Management> Diagnostics** open the following screen **Ping / TraceRoute**.

Figure 26-1 Device Management> Diagnostics> Ping / TraceRoute

Ping je síťový nástroj používaný pro ověření, zda je určitý hostitel (host) dosažitelný. Zadejte IP adresu nebo jméno hostitele a kliknutím na tlačítko spustíte Ping test. Výsledek testu se zobrazí v poli níže.
TraceRoute je síťový nástroj ke stopování cesty k určitému hostiteli (host). Zadejte IP adresu nebo jméno hostitele a kliknutím na tlačítko spustíte Trace Route. Výsledek testu se zobrazí v poli níže. Test a zobrazení jeho výsledku zabere asi 2 minuty.

The screenshot shows a large, empty rectangular text area for input. At the bottom right of the screen, there are two buttons: 'Ping' and 'TraceRoute'.

The following table summarizes the available fields on this screen.

Table 26-1 Device Management> Diagnostics> Ping / TraceRoute

Item	Description
ping	Enter the IP address of the computer you wish to ping for to test its availability. Click on the button ping and the result

Item	Description
	appears in the text box on the screen Diagnostics.
TraceRoute	Click this button to perform a traceroute command. The result of this command is a breakdown of the data paths pact to a specific host.

27 troubleshooting

27.1 Overview

This chapter provides solutions to some problems that you can encounter while using the device. Potential problems are divided into the following categories.

- Power, connectivity hardware, LED indicators
- LTE modem configuration interface and log
- Internet access
- Wireless Internet access
- Phone calls and VoIP
- UPnP

27.2 Power, hardware connections, LED indicators

27.3 LTE modem configuration interface and log

I forgot / IP address and I LTE modem.

Step 1 The default IP address is 192.168.1.1 modem.

step 2 If you changed the IP address and have forgotten it, you can obtain an IP address LTE Modem

locating the IP address of the default gateway of your computer. On most computers running Windows do this by clicking **Start** > **Run**, typing **cmd** and running the command **ipconfig**. **IP address of the default gateway is listed as Default Gateway** and may be the IP address of the LTE modem (but that depends on network settings). So try to enter the address into the address bar of your Internet browser.

step 3 If this does not work, the only solution is to reset the modem to factory Settings. See 1.5.3 RESET button.

---- End

I forgot my password.

- **The default password for the user account user Yippee LTE @ Endusr. The default password for the Administrator account admin Yippee @ Huawei CPE.**
- If you can not remember the password, you will need to reset the device to factory settings. See 1.5.3 RESET button.

I can not get *login screen* configuration interface.

Step 1 Make sure that the address bar enter the correct IP address.

The default IP address is 192.168.1.1 modem.

If the address has changed, you must use the new IP address.

If the address was changed and a new IP address can not remember, see Board "I forgot / IP address and I LTE Modem".

step 2 Check the hardware connection and make sure that the LEDs behave according expectation. see also *Quick Start Guide*.

step 3 Make sure your computer has a static IP address.

step 4 Make sure your Web browser does not use a proxy.

step 5 Make sure that your web browser does not block pop-ups and has allowed scripts

JavaScript and Java.

step 6 Reset your device to factory settings and try now open the configuration interface using the default IP address. See 1.5.3 RESET button.

step 7 If the problem persists, contact your network administrator or dealer. You can also try

One of the solutions recommended in this manual.

Advanced recommendations

- Try to connect to the configuration interface via other network services, for example. Telnet. If you manage the configuration interface LTE modem to get, check the remote management and firewall and try to determine the cause of the fact that the interface is not responding to requests sent via HTTP.
- **If your computer is connected to a port WAN or via a wireless network, try connecting to port ETHERNET and try again.**

---- End

I see *login screen* configuration interface, but I can not log in.

Step 1 Make sure that you enter the correct user name and password. The default user name is **user**. All fields distinguish between uppercase and lowercase letters, so make sure that is not active Caps Lock key.

step 2 Login to the web configuration interface is not possible in case someone is LTE modem connected via Telnet. Log off from the configuration interface in all other instances, or ask Logout Login person.

step 3 Turn off and turn on the LTE modem.

step 4 If this does not work, the only solution is to reset the modem to factory Settings. See Screen 24.2 Backup / Restore.

---- End

27.4 Internet Access

Unable to connect to the Internet.

Step 1 Check the hardware connection and make sure that the LEDs behave according expectation. see also *Quick Start Guide* and section 1.5 of parts.

step 2 Make sure that you correctly entered all parameters LTE APN your service provider.

step 3 If you want to connect to the Internet via a wireless network, make sure the settings wireless LAN client devices correspond to the parameters of the access point (AP).

step 4 If you want to connect to the Internet via a wireless network, make sure that the network WLAN active, whether by pressing the WPS / WLAN or screen Network Settings> WiFi 2.4 GHz / 5 GHz WiFi> General.

step 5 Unplug all cables from the modem and repeat the steps in the Quick Start Guide.

step 6 If the problem persists, contact your ISP.

---- End

Suddenly I can not connect to the Internet. Internet access via LTE modem was normally available, but ceased to function.

Step 1 Check the hardware connection and make sure that the LEDs behave according expectation. see also *Quick Start Guide* and section 1.5 of parts.

step 2 Turn off and turn on the LTE modem.

step 3 If the problem persists, contact your ISP.

---- End

Internet connection is slow or intermittent.

Step 1 It is possible that the network bandwidth was exhausted. Check the LEDs - see Section 1.6 If LTE modem sends and receives a lot of data, try closing some applications that use the Internet, especially by sharing in peer-to-peer networks.

step 2 Turn off and turn on the LTE modem.

step 3 If the problem persists, contact your network administrator or dealer. You can also try One of the solutions recommended in this manual.

Advanced recommendations

Check the setting of quality of service (QoS). If the QoS control off, consider activating. If QoS is enabled, consider increasing or decreasing the priority for some applications.

---- End

27.5 Wireless Internet access

What factors can cause intermittent or unstable wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles such as walls, ceilings, furniture, etc..
- Building materials such as metal doors, aluminum constructions.
- Electrical devices: microwaves, monitors, electric motors, cordless phones and other wireless devices.

To optimize the speed and quality of the wireless connection, you can:

- If the signal strength is low, move wireless devices closer to the access point (AP).
- Reduce wireless interference that may cause other wireless networks or ambient electronics, for example. Cordless phones.
- Place the access point (AP), so that between the AP and the wireless client were minimal obstructions (such as walls and ceilings).
- Reduce the number of wireless clients simultaneously connecting to the same AP, or add another AP.
- Try to close some programs using the Internet, especially applications like peer-to-peer. If a wireless client sends or receives a lot of information, it is possible that there are too many programs connected to the Internet.

What wireless security mode LTE modem supports this?

Security is a key aspect of any wireless network. Protects communications between wireless stations, access points and cable networks.

Available security modes in your facility are as follows:

- **WPA2-PSK** (recommended) this method of security is based on a shared key WPA2.
- **WPA-PSK**: The modem uses WPA-PSK or WPA2-PSK depending on which security mode supports wireless client.

27.6 Telephone calls and VoIP

Phone port does not work / the headset is not heard a dial tone.

Step 1 Check your telephone cable connection and the cable itself.

---- End

I have access to the internet, but I can not make VoIP calls.

Step 1 Indicator **PHONE** should illuminate. Make sure that your phone is connected to the PHONE jack.

step 2 Status VoIP telephony can also check on the screen **Information about the system**.

step 3 If all settings are correct VoIP telephony, try using speed dial

contact another phone connected to the network. If the call is successful, it is possible that a fault has occurred SIP server. Contact your VoIP service provider.

---- End

27.7 UPnP

If using UPnP devices LTE modem restarts, I see UPnP devices on your computer.

Control Panel> View computers and devices on the network.

Step 1 Disconnect the Ethernet cable from the LTE modem from the LAN connector of your computer.

step 2 Connect the Ethernet cable back.

---- End

Icon *Local Area Connection* for UPnP devices disappeared. Restart the computer.

When using the chat application not work some functions, for example. File transfer or video.

Step 1 Wait at least three minutes.

step 2 Restart.

---- End

28

Protection of personal data

Document *Description of personal data collected LTE modem CPE B2368* describes how user data is collected by this device. User data collected in this LTE modem is necessary to process and treat them in accordance with applicable laws and regulations, such as the General Regulation on the Protection of Personal Data (GDPR) in European Union countries.