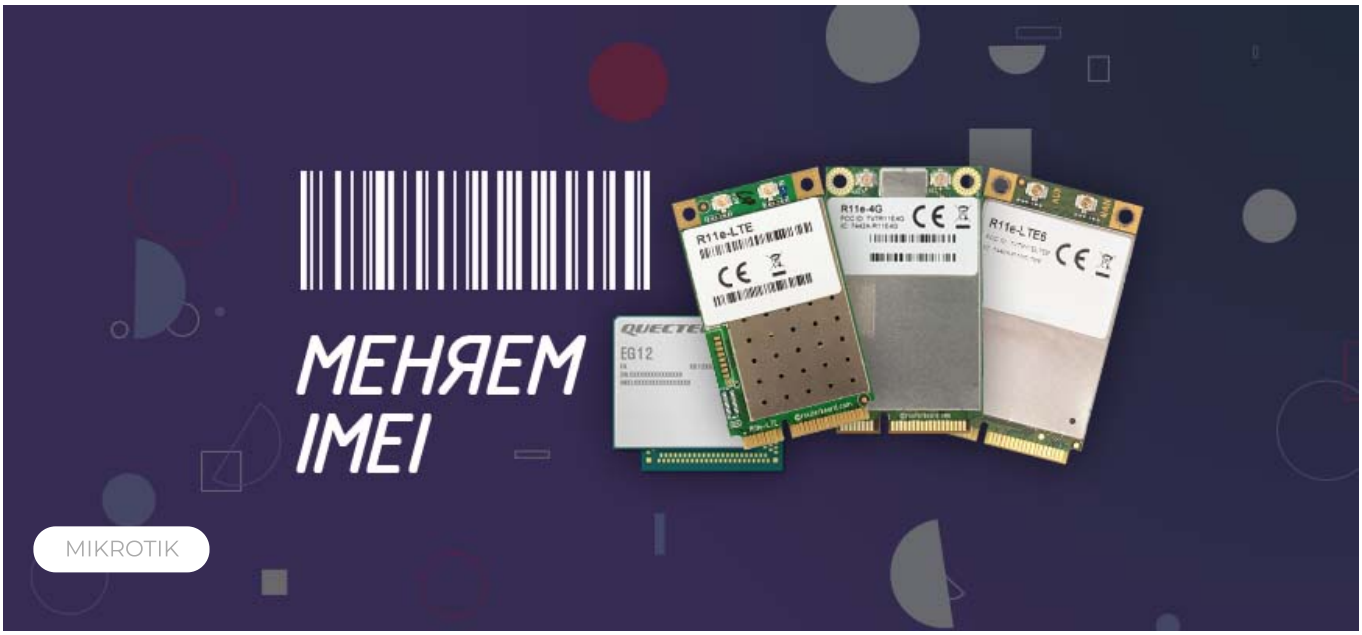
Change IMEI for R11e-LTE, R11e-4G, R11e-LTE6 and EG12-EA (Chateau LTE12)

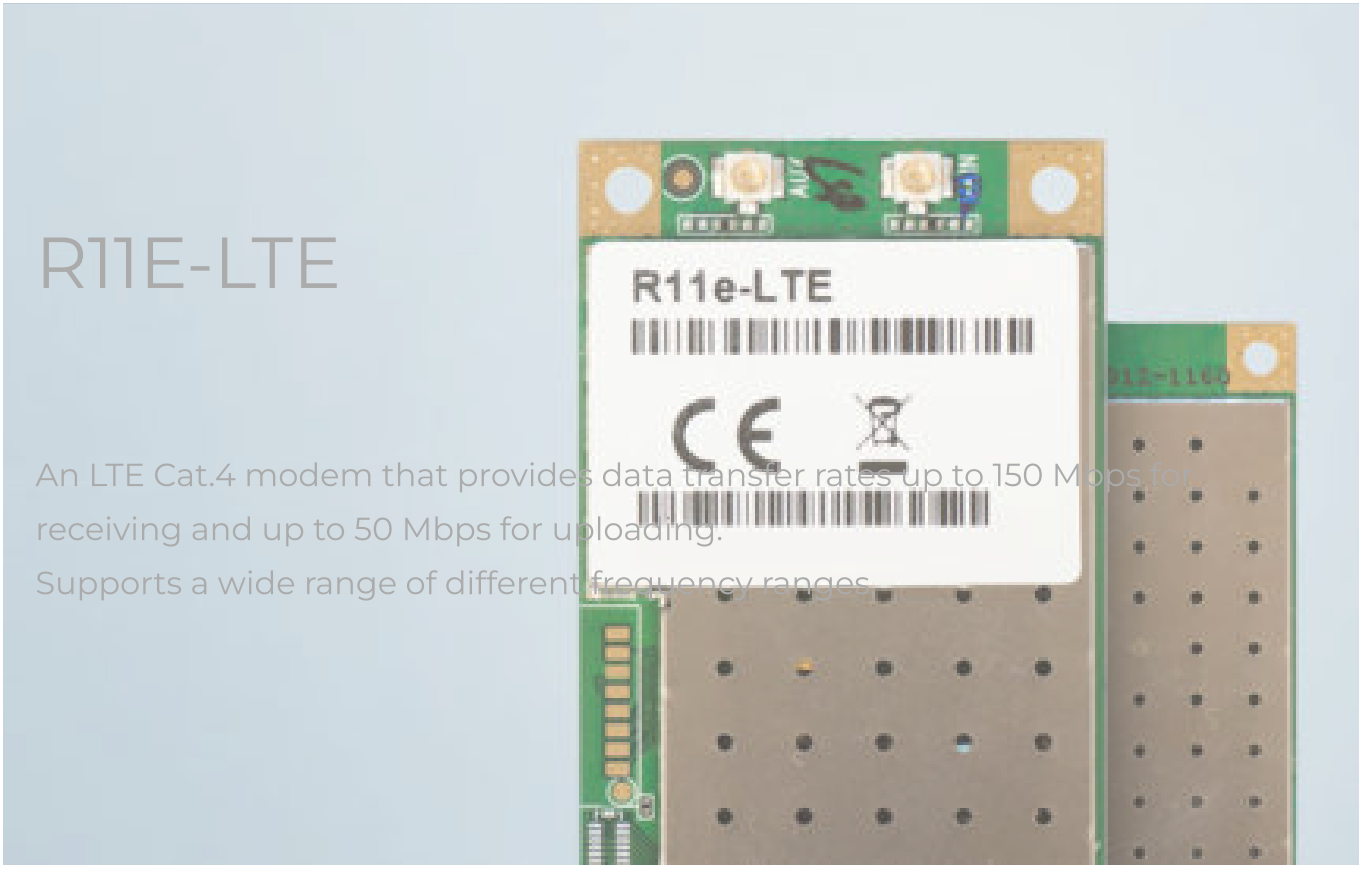


MikroTik has a number of products (LtAP, wAP, SXT, Chateau, etc.) based on their own modems and partner modems, which they have officially integrated into their solutions. And accordingly, these devices use different models of modems.
There are times when we need to check the equipment, but we only have the SIM card of the operator from our own smartphone at hand. As a rule, tariffs for such SIMs are regulated in a certain way for their type of equipment (Smartphones, Tablets and PCs). What to do in this case?

In this case, we have the opportunity to change the IMEI and make some changes to work with the TTL of the router. And how to do it for various modems, in MikroTik devices, later in this article!

It is important to understand that all actions that you perform are carried out at your own peril and risk !! The author of the article does not give any guarantees for the performance of the product after you make changes, and also does not bear any responsibility for claims or for damages.

MikroTik R11e-LTE



In fact, this is a MIFI modem on a PXA1802 stone from Luat

Change IMEI for R11e-LTE

```
/interface lte at-chat lte1 input="AT*MRD_IMEI=R"
```

We read the current IMEI and save it somewhere just in case!

```
/interface lte at-chat lte1 input="AT*MRD_IMEI=D"
```

Delete the current IMEI

```
/interface lte at-chat lte1 input="AT*MRD_IMEI=W,0101,11JAN1970,000000000000000"
```

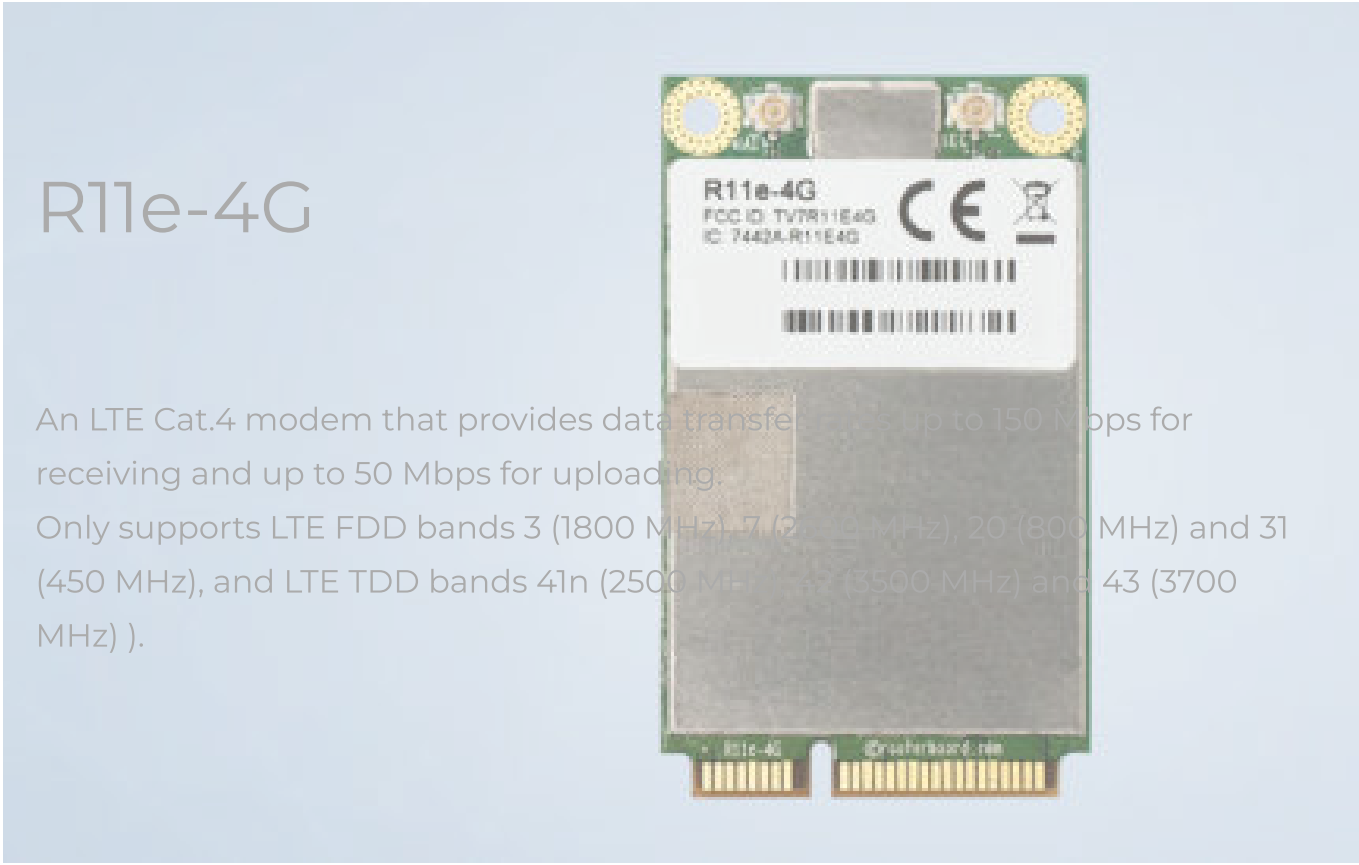
We write down a new one, where instead of **000000000000000 we** specify IMEI different from the current one

```
/interface lte at-chat lte1 input="AT+RESET"
```

Restarting the modem

AT commands for R11e-LTE
[Luat LTE Module AT Command User Manual V1.0]

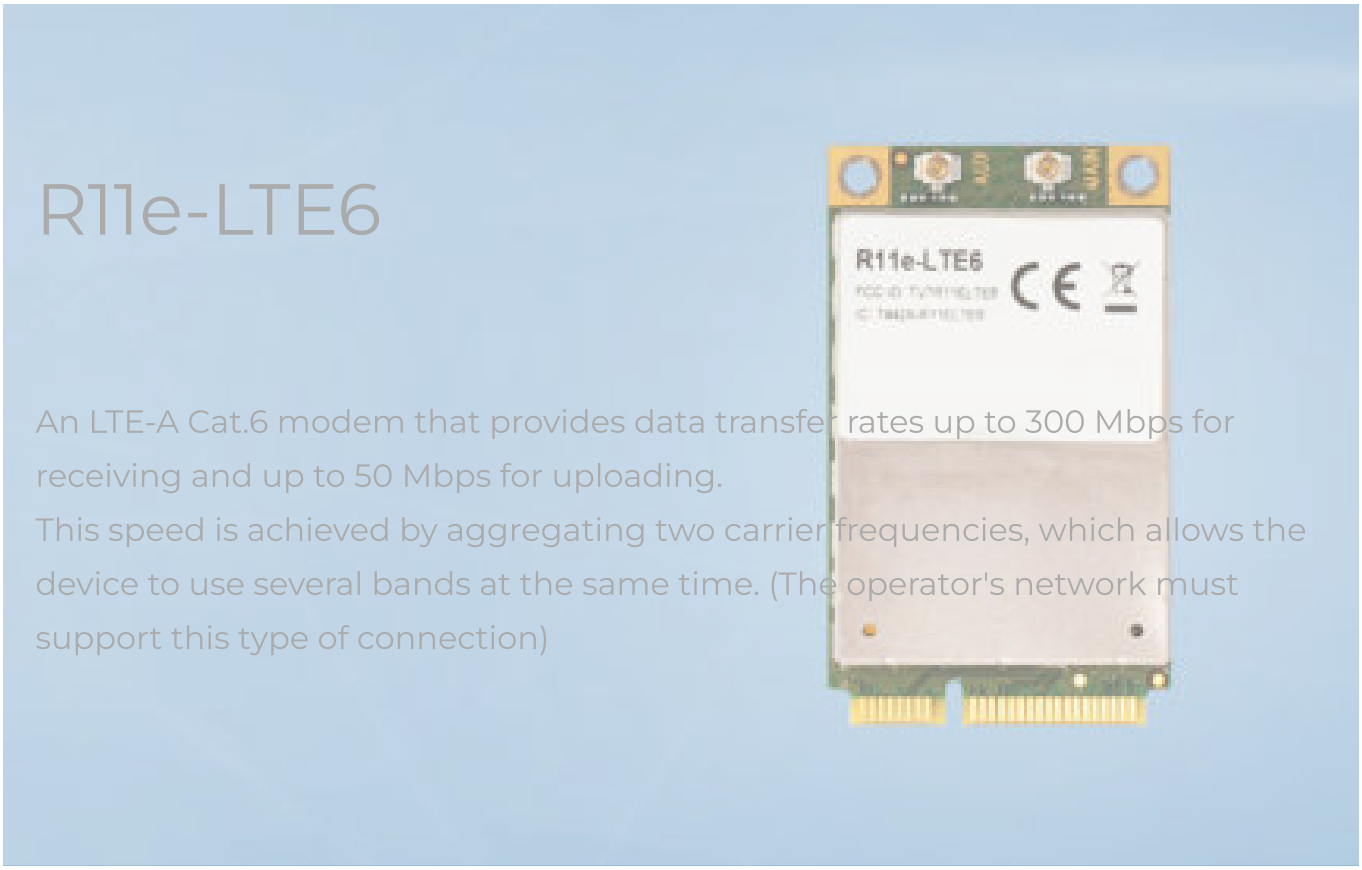
Mikrotik R11e-4G




```
/interface lte at-chat lte1 input="AT%SETCFG=\"DEBUG_IMEI\",\"000000000000000\""
```

We write down a new one, where instead of **000000000000000 we** specify IMEI different from the current one

Mikrotik R11e-LTE6



"AT*MRD_IMEI=D\W" just don't work on R11e-LTE6
Modem replies: "Output: +CME ERROR: Non-Production mode"
production mode (when power on, press SEND/END key will enter production mode)

Be sure to update to the latest firmware

```
/interface lte firmware-upgrade lte1
installed: R11e-LTE6_V020
latest: R11e-LTE6_V027
```

If we see that there is a new firmware

```
/interface lte firmware-upgrade lte1 upgrade=yes
```

Updating

We wait a couple of minutes while the firmware is downloaded.

```
/interface lte at-chat lte1 input="AT+CHECKATUPGRADE"
```

Check after download

After about 5 minutes, the modem will reboot itself.

To change IMEI

```
/interface lte at-chat lte1 input="AT*PROD=2"
```

Go to Production Mode

```
/interface lte at-chat lte1 input="AT*MRD_IMEI=R"
```

We read the current IMEI and save it somewhere just in case!

```
/interface lte at-chat lte1 input="AT*MRD_IMEI=D"
```

Delete the current IMEI

```
/interface lte at-chat lte1 input="AT*MRD_IMEI=W,0,01JAN1970,000000000000000"
```

We write down a new one, where instead of **000000000000000 we** specify IMEI different from the current one

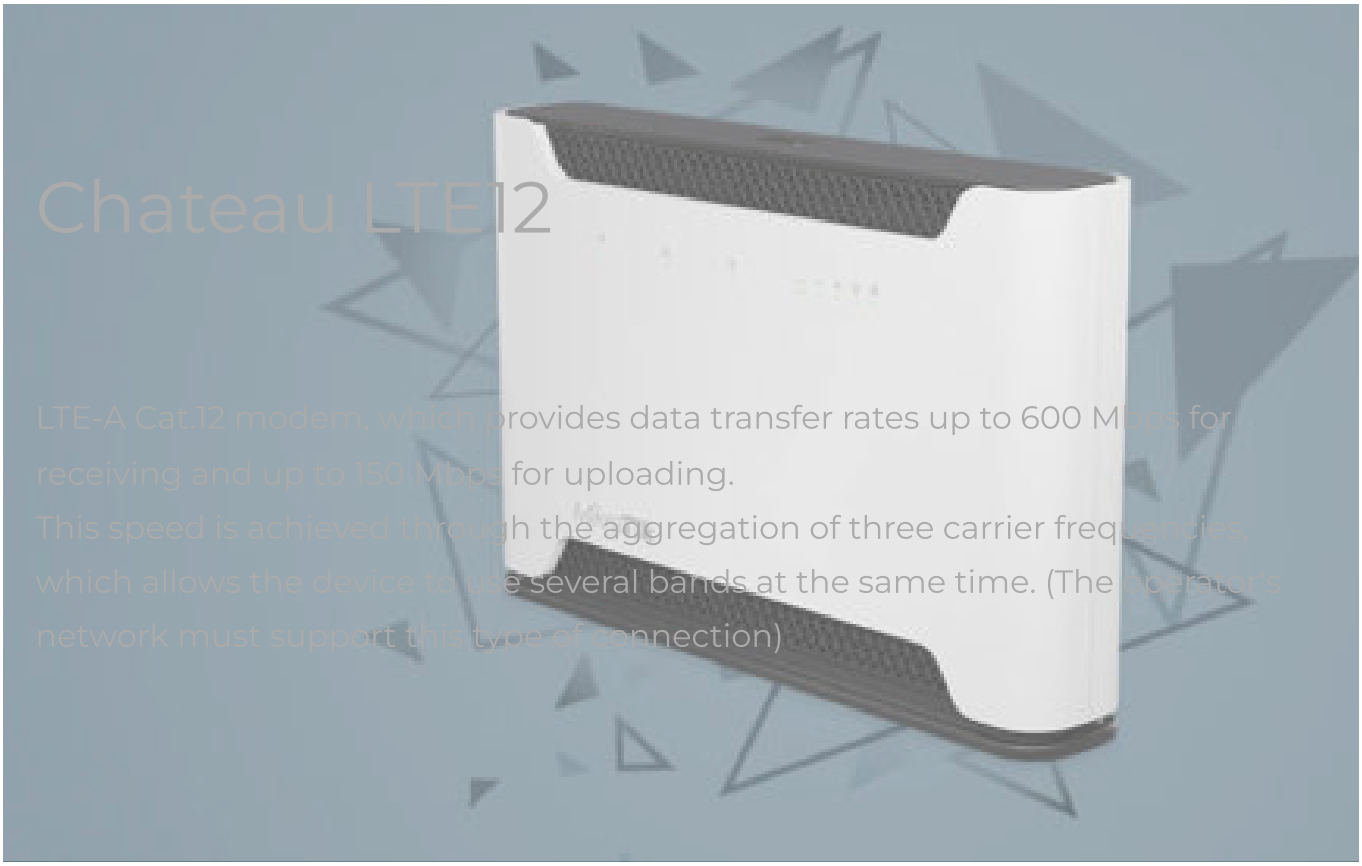
```
/interface lte at-chat lte1 input="AT*PROD=0"
```

Exit Production Mode

```
/interface lte at-chat lte1 input="AT+RESET"
```

Restarting the modem

EG12-EA aka (Chateau LTE12)



Built-in LTE-A Cat.12 modem from Quectel LTE-A EG12-EA (for EMEA/APAC/Brazil regions)

To change IMEI

```
/interface lte at-chat lte1 input="AT+GSN"
```

We read the current IMEI and save it somewhere just in case!

```
/interface lte at-chat lte1 input="AT+EGMR=1,7,\"000000000000000\""
```

We write down a new one, where instead of **000000000000000 we** specify IMEI different from the current one

```
/interface lte at-chat lte1 input="AT+GSN"
```

Check if the new IMEI is saved

Notorious TTL

TTL - **Time To Live**
The time limit or number of iterations or transitions for which a data set (package) can exist before it disappears. Those. by simple TTL sets the packet lifetime.

To determine the type of device and match the tariff (smartphone, tablet, PC), operators send packets with different TTLs to the client (for example, MTS sends TTL = 1) so that these packets are killed on the router when passing through it. In the direction of the operator, the devices send their standard packets.

To simulate a Linux, Mac, Android or iOS device (TTL=64)

```
/ip firewall mangle
add action=change-ttl chain=prerouting in-interface-list=WAN new-ttl=increment:5
passthrough=yes ttl=equal:1
add action=change-ttl chain=postrouting new-ttl=set:64 out-interface-list=WAN
passthrough=yes
```

To simulate a Windows device, WindowsPhone (TTL=128)

```
/ip firewall mangle
add action=change-ttl chain=prerouting in-interface-list=WAN new-ttl=increment:5
passthrough=yes ttl=equal:1
add action=change-ttl chain=postrouting new-ttl=set:128 out-interface-list=WAN
passthrough=yes
```

Do not use FastTrack rules when changing TTL!!!

Legislative aspect of changing IMEI

In **the Russian Federation** , changing the IMEI of a device is not regulated by any legal act!
Accordingly, if you are from another country, then before applying something from this article, you should better familiarize yourself with the legislative aspect regarding such manipulations.

> If you are not indifferent to the fate of the blog or you just want to thank the Author for his work, feel free to go to the Support page , all the information on how to do this is described there. Thank you in advance for this initiative!

Do you want to be notified when new articles are released?

Email

Then subscribe!

#at-chat #chateau #Chateau LTE12 #EG12-EA #imei #mikrotik #r11e #R11e-4G #R11e-LTE #R11e-LTE6

Gregory

The world is interesting if you are curious enough!!!

Rate the author

★★★★★

Subscription

Subscribe to be notified of new posts

Email*

Email

Subscribe

Fresh comments

Sergey on Creating a home network based on MikroTik devices: Part 7 - Firewall correct port forwarding in a network with two gateways

Zhanat on Configuring MikroTik cAP Lite as a Wi-Fi client in Bridge mode

Dmitry on Creating a home network based on MikroTik devices: Part 6 - Firewall access protection

Andrey on ASUS RT-AC66U: CFE or Changing the region on new firmware

Gregory on Creating a home network based on MikroTik devices: Part 6 - Firewall access protection

Categories

- Windows
  - Windows 10
- Iron
- Routers
  - ASUS
  - Mikrotik
- Soft
  - Proxmox
  - Raspberry Pi
- TV

About me

I have been working in the field of IT technologies for a long time.
I do not pretend to titles, medals and something like that.
Everything that is described here is the personal experience and opinion of the author, and nothing more.
I am glad to welcome dear readers, I hope you find something useful for yourself.

Meta

To come in
Tape of records
Comment feed
WordPress.org

Tags

2.4GHz asus bridge client debian dhcp DNS dude eoip filter firewall gregory gost hap ac hex ip linux lxc mikrotik nat nginx nvram openvpn plex proxmox proxmox-ve raspberry raspberry pi 3b+ rb750gr3 ros routerboard routeros RT-AC66U server snmp ssh tcp web Wi - telnet udp Fi winbox windows windows 10 setup router