

GRE Tunnel configuration examples RutOS

□

Contents

- [1 Introduction](#)
- [2 Configuration overview and prerequisites](#)
- [3 Router configuration](#)
- [4 Testing the setup](#)
- [5 See also](#)

Introduction

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

This article provides an extensive configuration example with details on how to create a tunnel connection between two GRE Tunnel instances, both of which are configured on RUTxxx routers.

Configuration overview and prerequisites

Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible.

Prerequisites:

- Two RUTxxx routers of any type (excluding [RUT850](#))
- Both routers must have a Public Static or Public Dynamic IP addresses
- At least one end device (PC, Laptop, Tablet, Smartphone) to configure the routers

Configuration scheme:



As indicated by the figure above, the configuration we are trying to achieve here is very basic: it concerns two RUTxxx routers - RUT1 and RUT2. They are connected into a virtual network via a GRE Tunnel.

Router configuration

If you have familiarized yourself with the configuration scheme and have all of the devices in order, we can start configuring the routers using the instructions provided in this section:

- Login to the router's WebUI and go to **Services** → **VPN** → **GRE Tunnel**. Enter a name for the

new instance and click the "Add" button. Do this on both routers:



-
- Click the "Edit" button located to the right of the newly created GRE Tunnel instance:



-
- You will be redirected to the settings window where you can start configuring the GRE Tunnel instance. Below is a capture of configurations for both GRE Tunnel instances:



- Below are explanations of the parameters highlighted in the figure above. Other parameters (not highlighted) are defaults. You can find descriptions for these parameters in the [VPN manual page, GRE Tunnel section](#)
 - **Enable** - enables the GRE Tunnel instance
 - **Tunnel source** - select the network interface with Public IP which is used to establish the GRE tunnel.
 - **Remote endpoint IP address** - the Public IP address of the opposite router
 - **Outbound and Inbound key** - 65000 (must match other device's Inbound/Outbound key)
 - **Enable Keep alive** - enables the tunnel's keep alive function. When enabled, the instance sends ICMP packets to the specified host at the specified frequency. If no response is received, the instance attempts to restart the connection
 - **Keep alive interval** - the period (in seconds) at which Keep alive packets will be sent to the specified host in this example 200.
 - **Local GRE interface IP address** - virtual IP address the GRE Tunnel instance (make sure it is **unique** for each instance)
 - **Local GRE interface netmask** - subnet mask of the local GRE Tunnel
 - **Remote subnet IP address** - LAN IP address of opposite router
 - **Remote subnet IP address** - Netmask of opposite router

NOTE: remember to replace certain parameter values (like IP addresses) with your own relevant data.

Testing the setup

If you've followed all the steps presented above, your configuration should be finished. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. In order to test a GRE Tunnel connection, log in to one of the routers' WebUIs and go to **Services** → **CLI**. Log in with the user name: **root** and the router's admin password. From there you should then be able to **ping** the opposite instance's virtual IP address. To use a ping command, type **ping <ip_address>** and press the "Enter" key on your keyboard:



You can also test if LAN access is working the same way. Instead of pinging the opposite instance's LAN IP address, ping one of the end devices' IPs. One common issue that can be encountered here is

that the end devices **might need their DHCP leases renewed**. There are many methods of accomplishing this, but the easiest and most accessible way is to simply disconnect and reconnect the LAN cable to the device or the router that it's connected to.

If the ping requests are successful, congratulations, your setup works! If not, we suggest that you review all the steps once more.

See also

- Other types of VPNs supported by RUTxxx devices:
 - [OpenVPN configuration examples](#)
 - [IPsec configuration examples](#)
 - [PPTP configuration examples](#)
 - [L2TP configuration examples](#)