

# Template:Networking rutos configuration example Setting up a ZeroTier tunnel between RUTX devices

□

## Contents

- [1 Introduction](#)
- [2 Prerequisites](#)
- [3 Configuration scheme](#)
- [4 Setting up a ZeroTier network](#)
- [5 Node configuration](#)
  - [5.1 Teltonika-Networks RUTX device](#)
- [6 Node authorization](#)
- [7 Testing configuration](#)
  - [7.1 Ping Test](#)
  - [7.2 ZeroTier Commands](#)

## Introduction

**ZeroTier One** is an open source software product which establishes Peer to Peer VPN (P2PVPN) connection between laptops, desktops, phones, embedded devices, cloud resources, and apps.

This article contains step-by-step instructions on how to set up and manage a Zerotier network tunnel using two Teltonika-Networks RUTX devices.

## Prerequisites

You will need:

- Two Teltonika RUTX routers
- A PC to configure the routers

## Configuration scheme

✖

## Setting up a ZeroTier network

- Go to <https://my.zerotier.com/login> and log in or create an account if you haven't already.
- Click the newly created network to begin configuration.

✖

1. Open the '**Networks**' tab and click the '**Create a Network**' button.

2. Before configuring anything else, you may want to set up some basic settings.



1. Copy the **Network ID**; you will need it later for ZeroTier node configuration.
2. Optionally, set up a name and description for your network for easier management.
3. Select '**Private**' access control type; unless you want nodes to connect freely, without authorization.



- Scroll down to find the '**IPv4 Auto-Assign**' section. Select one of the provided private IP ranges for your network or click 'Advanced' and set up the range manually. For this example we'll be using the **10.147.17.\*** selection which means our network will be using the **10.147.17.0/24** IP range.



The last step concludes the ZeroTier network configuration. However, you may want to modify to the settings based on your specific requirements, but the network will function without any additional settings.

The next step is configuring members (aka nodes) for our ZeroTier network.

## Node configuration

Zerotier **nodes** or **members** are clients that can connect to a ZeroTier network. This section provides information on how to configure ZeroTier nodes on RUTX devices.

Take note that if '**Private**' access control type is selected, the nodes will only come online after they authorized by you from the ZeroTier Central dashboard. To learn how to authorize nodes, read the [Node authorization](#) section of this article.

## Teltonika-Networks RUTX device

- Log into your device's WebUI, and navigate to the **Services → Package Manager page**.
- Find the ZeroTier package in the list and install it.
- Navigate to the **Services → VPN → ZeroTier** page and create a new ZeroTier configuration.
  1. Enter a custom name for the configuration.
  2. Click '**Add**'.



- Click the '**Edit**' button and will be forwarded to the newly created configuration menu.



- Complete the configuration.
  1. Turn the configuration on.
  2. Paste the ZeroTier Network ID into the '**Networks**' field.
  3. Click '**Save & Apply**'.
  4. You will be redirected to the overview and the **node ID** will be created automatically



# Node authorization

When Access Control is set to '**Private**', you will have to approve new nodes manually from the ZeroTier dashboard before they can become members of the network.

To do this, simply scroll down to the '**Members**' section and:

1. Place check marks next to nodes you wish to authorize.
2. Additionally, you may want to add names and descriptions for your nodes to make it easier to differentiate between them.



# Testing configuration

## Ping Test

---

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 the **ZeroTier** Tunnel connection.

1. login to RUTX WebUI and go to **Services → CLI**.
2. Login with user name: **root** and the router's admin password.
3. From there you should then be able to **ping** the opposite instance's virtual IP address.
4. To use a ping command, type **ping <ip\_address>** and press the "Enter" key on your keyboard:



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

## ZeroTier Commands

---

Also it's possible to get information about the VPN tunnel configuration and status via **CLI**. If you would like to use the **zerotier-cli** commands, you need to login to the WebUI:

1. Go to **Services → CLI**.
2. Login with user name: **root** and the router's **admin password**.
3. Write **zerotier-cli help** command and press the "Enter" key on your keyboard:

The RUTX will show the commands the **zerotier-cli** can issue, for this example we'll get the VPN info/status and IP address.

1. Getting info/status:

```
zerotier-cli info
```

2. Getting IP address:

**Note: Need to write your own network ID**

```
zerotier-cli get <network ID> ip
```

