

ZeroTier Configuration

[Main Page](#) > [General Information](#) > [Configuration Examples](#) > [VPN](#) > **ZeroTier Configuration**

The information in this page is updated in accordance with the **RUTXXX_R_00_07_02** firmware version.

ZeroTier One is an open source software which can establish Peer to Peer VPN (P2PVPN) connection between various devices running various operating systems. It also provides network management possibilities such as routing and creating firewall rules.

□



Contents

- [1 Introduction](#)
- [2 Setting up a ZeroTier network](#)
- [3 Node configuration](#)
 - [3.1 Teltonika-Networks device](#)
 - [3.2 Windows device](#)
 - [3.3 Android/Apple iOS device](#)
- [4 Node authorization](#)
- [5 Private network access](#)
 - [5.1 ZeroTier routing](#)
 - [5.2 Port forwarding](#)
- [6 Bridge Configuration](#)
 - [6.1 First router](#)
 - [6.2 Second Router](#)
 - [6.3 ZeroTier Portal](#)

Introduction

This article contains step-by-step instructions on how to set up and manage a ZeroTier network using Teltonika-Networks devices along with other equipment.

Setting up a ZeroTier network

- Go to <https://my.zerotier.com/login> and log in or create an account if you haven't already.
- Open the 'Networks' tab and click the 'Create a Network' button.

- Click the newly created network to begin configuration.

- 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 this particular 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 different types of machines.

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

Teltonika-Networks device

- Log in to 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'.
 3. Click the 'Edit' button next to the newly created configuration.



- Complete the configuration.
 1. Turn the instance on.
 2. Paste the ZeroTier Network ID into the 'Networks' field.
 3. Click 'Save & Apply'.



- Go to the ZeroTier Central dashboard and [authorize](#) this node.
- To check the status of the connection from your device, go to the Services → CLI page and [log in](#).

Check connection status with this command:

```
zerotier-cli info
```

Check ZeroTier interface IP address with this command (replacing *<network>* with the ZeroTier Network ID):

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



Windows device

- Download and install ZeroTier for Windows from <https://www.zerotier.com/download/>.
- Look to the right side of the Windows taskbar and perform these actions:
 1. Click 'Show hidden icons'.
 2. Right-click the ZeroTier icon.
 3. Click 'Join Network...'
 4. Paste the ZeroTier Network ID.
 5. Click 'Join'.



- Go to the ZeroTier Central dashboard and [authorize](#) this node.
- To check the status of the connection, click 'Show hidden icons' again and click 'Show Networks...'



Android/Apple iOS device

- Open the 'Google Play Store' or the 'App Store' depending on your mobile device.
- Find the 'ZeroTier One' app and install it.
- Open the application and configure it as follows.
 1. Click the plus symbol.
 2. Enter the ZeroTier Network ID.
 3. Click 'Add Network'.
 4. Enable the connection to this network by moving the slider next to it.
 5. In the 'Connection request' pop-up click 'OK' to confirm the connection.
 6. After you have [authorized](#) the new member (your phone), the status indication at the bottom of the screen should turn to 'Online'.



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.

1. Place check marks next to nodes that 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.



Private network access

This section provides instructions on how to set up remote access to private networks behind ZeroTier nodes. For the following instruction, we'll use an example ZeroTier network that consists of three members: a Teltonika-Networks device, a computer and a phone.

For the purposes of this example, let's assume we want to provide remote access for the computer and the phone to the 192.168.1.0/24 network behind the Teltonika-Networks device.



ZeroTier routing

- Go ZeroTier Central and find the '**Managed Routes**' box in the 'Advanced' section.
- Add the following route.
 1. Specify *192.168.1.0/24* as the destination.
 2. Specify *10.147.17.23* (Teltonika device ZeroTier IP) in the 'via' field.
 3. Click 'Submit'.



- Configuring it like this will make the entire 192.168.1.0/24 network accessible to other ZeroTier nodes via the Teltonika device's ZeroTier IP address. To configure a route to a single IP address instead, you can specify the address with a /32 netmask:



Port forwarding

- Enter your Teltonika device's WebUI and navigate to the Network → Firewall → Port Forwards page.
- Find the 'Add New Port Forward' section and add rule such as this:
 1. Enter a custom name for the rule.
 2. Select *zerotier* as the external zone.
 3. Enter an external port number for listening for incoming connections.
 4. Select *lan* as the internal zone.
 5. Enter a device's IP in the local network.
 6. Enter a device's listening port number.
 7. Click 'Add'.



- Since this configuration concerns port 80, the default HTTP port, configuring it like this would eliminate WebUI access to the Teltonika device over the ZeroTier network. To maintain that access, consider using a different external port:



Bridge Configuration

ZeroTier bridge configuration will allow two (or more) LAN's in the same ZeroTier network to be interconnected. For this example, we will use two RUTX routers. Both of these routers should already have the ZeroTier package installed and be connected to the ZeroTier Portal.

First router

- Navigate to **Services** → **VPN** → **ZeroTier** and access the ZeroTier Instance created previously to edit it for the bridging of LAN's.



- From the **Bridge to** dropdown menu, select **LAN**. This option bridges The ZeroTier interface with the device's LAN interface, which extends the network and allows for Layer 2 communication via ZeroTier. Bridges operate at the data link layer and facilitate seamless communication between devices on different LAN segments
- Save & Apply settings

Second Router

- Navigate to **Services → VPN → Zerotier →** and access the ZeroTier instance, configuring it the same way as the first router.
- Navigate to **Network → LAN → General settings** and change the **IPv4 address** to an IP that is in the same subnet as the first router (We will use 192.168.1.2 for this example)
- Navigate to **Network → Interfaces → LAN → DHCP Server** and Disable **DHCP server** option
- Save & Apply settings



ZeroTier Portal

- Open your ZeroTier Portal (<https://my.zerotier.com/>) and navigate to your ZeroTier Network.
- Scroll down to Members and enable "**Allow Ethernet Bridging**" option on both devices



- Make sure to turn off **Auto-Assign from Range** in the **advanced section**. Since this is a Layer 2 bridge configuration, there is no need for IP addresses on the ZeroTier Interfaces and managed IPs. With Layer 2 bridging, devices communicate directly using their local MAC addresses, eliminating the necessity for IP address management.
- **NOTE: Make sure to remove any Managed IPs that might have stayed when the Auto-assigned feature was turned on (by default, ZeroTier keeps it on).**
- In the **Advanced section → Managed Routes**, add the LAN network route (in this case, 192.168.1.0/24), which ensures communication within the bridge. This allows devices in the ZeroTier network to communicate with devices on the LAN.



- To ensure convenience and avoid any IP or routing conflicts, it is recommended to remove any other automatically assigned routes in ZeroTier. By doing so, you can prevent routing issues and ensure smoother communication within the LAN bridge network of 192.168.1.0/24 over the ZeroTier Network.

If everything was done correctly, you should be able to ping devices connected to separate routers. Let us test this by pinging a laptop connected to the second router (192.168.1.163) from a laptop connected to the first router (192.168.1.220):



Note: If you wish to add more routers to the bridged network, you should configure them according to the second router configuration.