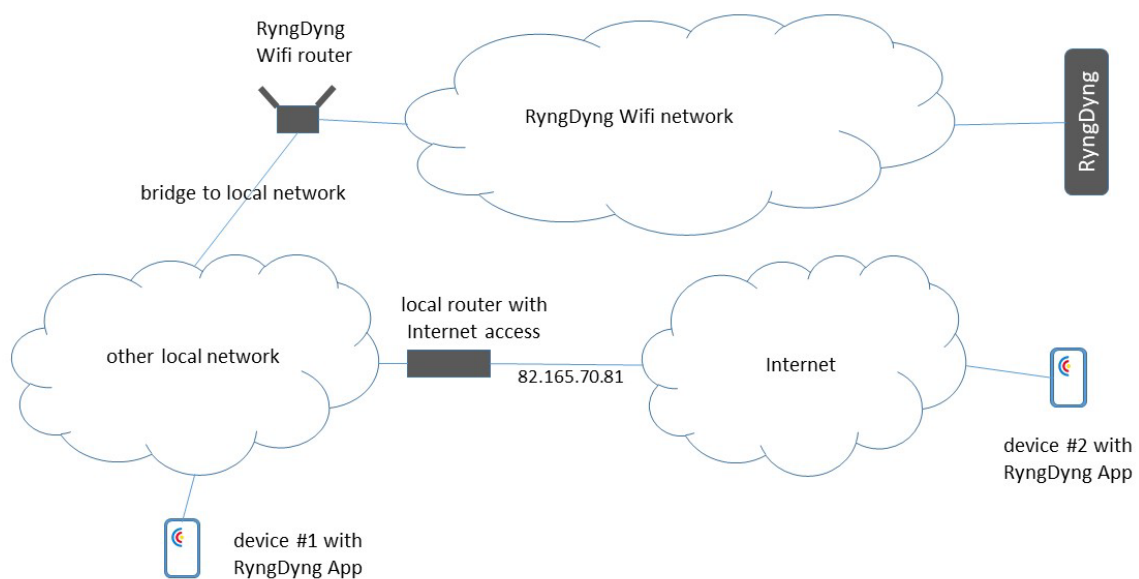


Remote Access to RyngDyng

Architecture

This document describes how to access RyngDyng systems remotely, i.e. without a direct connection to the local RyngDyng Wi-Fi network. You can achieve this by means of an **OpenVPN tunnel** from the Internet into the RyngDyng Wi-Fi router.

Example for a possible architecture:



Bridge to local network

There are two possibilities establishing a bridge between the RyngDyng Wi-Fi network and another local network. First is to use an Ethernet cable plugged into the WAN port of the RyngDyng Wi-Fi router and into a LAN port of the local router. Second option is to establish a Wi-Fi bridge.

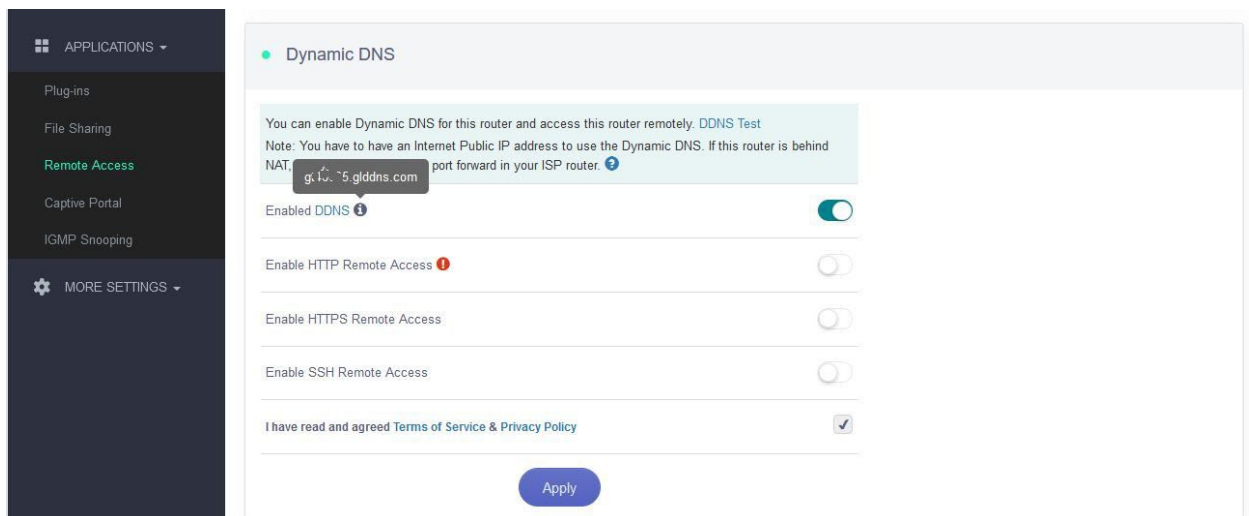
You can download a document from our server, describing these options in more detail: [How to establish Internet Access](#).

Dynamic DNS

Typically, the public IP address of your local network router changes regularly. Therefore, you need to set-up a 'follow-me' service for your public IP address, called Dynamic DNS.

The RyngDyng Wi-Fi router is prepared to do this for you. Follow these steps:

1. Connect a PC to the RyngDyng Wi-Fi network
2. Open a browser and type in the URL of the router: <http://10.10.10.254>
3. Log into the router web page using the same password that you used to connect to the Wi-Fi network
4. Go to page Applications -> Remote Access
5. Activate Enabled DDNS and check I have read and agreed Terms of Service ...
6. Press button Apply
7. Next to Enabled DDNS there is an info sign. Hover over it with the mouse and you will find an address that provides the DDNS service specifically for your router (see image below). Note it down. Typically, it is the form `gt47655.glddns.com`.¹



You can test the DDNS service in a Windows or Linux console by typing this command (use your specific DDNS service address):

```
nslookup gt47655.glddns.com 8.8.8.8
```

The response shows the current public IP address of your local router (82.165.70.81 in our example architecture image above). This will only work when the RyngDyng Wi-Fi router is powered on and connected to your local network via a bridge.

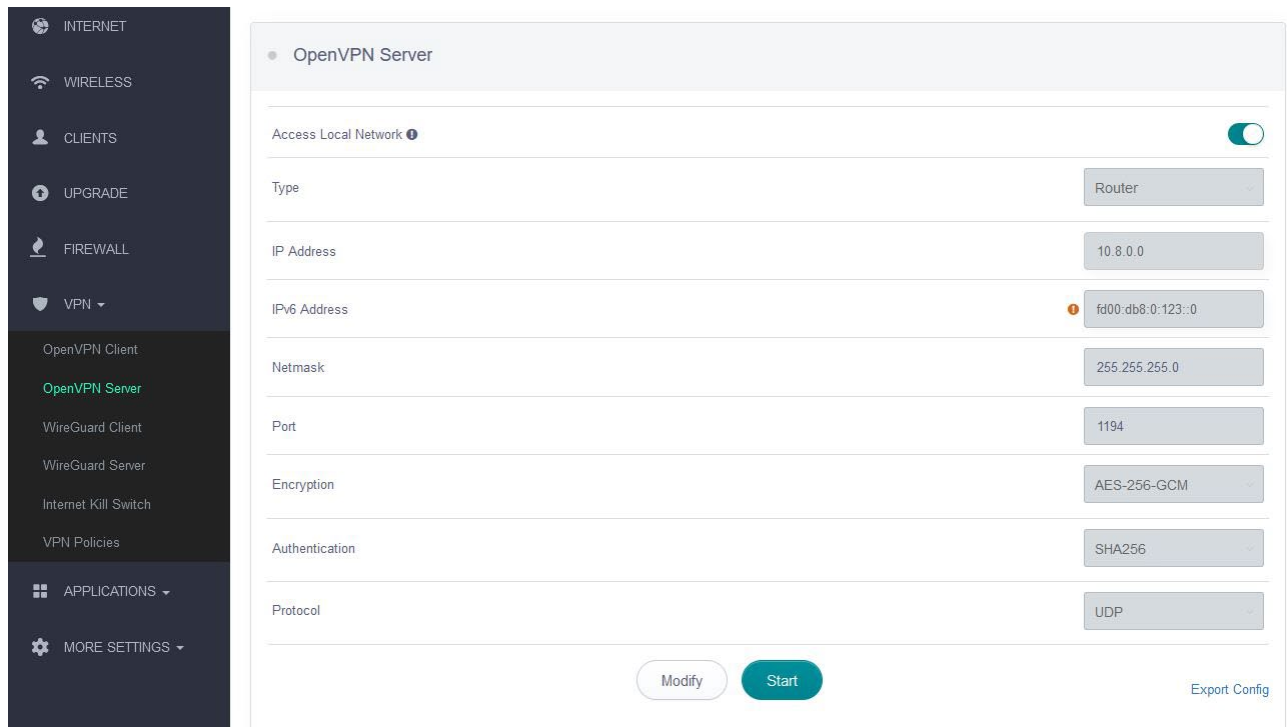
This test should work on any computer connected to the Internet.

OpenVPN Server

Next step is to activate the OpenVPN server inside the RyngDyng router.

1. Go to page VPN -> OpenVPN Server.
2. Switch on Access Local Network.
3. Press button Start
4. Click on link Export Config and save client configuration file to your computer (maybe you want to give it the file name `ryngdyng.ovpn`)

¹ This pattern gtxxxx is also printed on the back label of your router



The default value for field `Port` is `1194`. This is the TCP port used by the VPN tunnel.

Required changes to Client Configuration File

Open file `ryngdyng.ovpn` using a text editor. Change resp. add the following lines:

```
remote gt47655.glddns.com 1194
dhcp-option ADAPTER_DOMAIN_SUFFIX archery-electronics.com
dhcp-option DNS 10.10.10.254
```

Use the specific DDNS service address for your router (`gtxxxx.glddns.com`). If you changed the port 1194 when activating the OpenVPN server, use the changed port here as well.

Port Sharing

In order to build the OpenVPN tunnel through your local router, you will need to add a port sharing to your local router (sometimes called: port forwarding).

How this is done depends on the type of router. Most routers actually support port sharing.

The type of port sharing is `UDP` and the port number is `1194` (unless you changed it, see above). The port sharing is assigned to the RyngDyng router (usually, to the local router the RyngDyng router appears as a network device with hostname FunkDing).

If there are more than one router on the path from the Internet to the RyngDyng Wi-Fi router, all routers need to get this port sharing enabled.

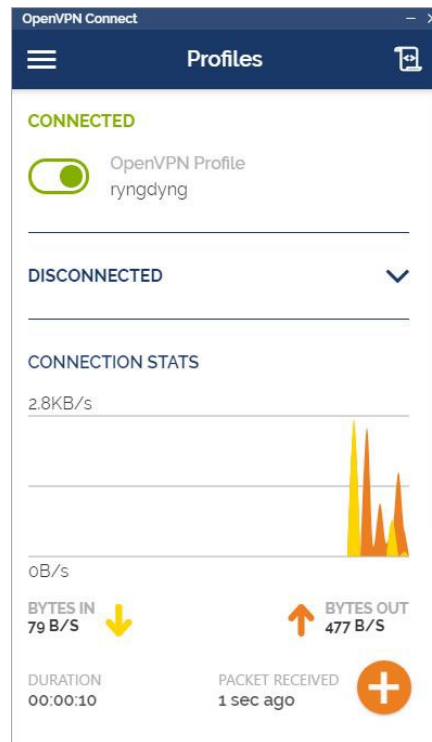
Install OpenVPN Client Software

The OpenVPN Client software is available for all operating systems such as Windows, iOS, Linux, Android etc.

Download and install the OpenVPN Client software on the device that should run the RyngDyng App remotely.

Start the OpenVPN client and add a new VPN connection profile (Plus sign). Import the previously created client configuration file `ryngdyng.ovpn`. Save the VPN connection profile.

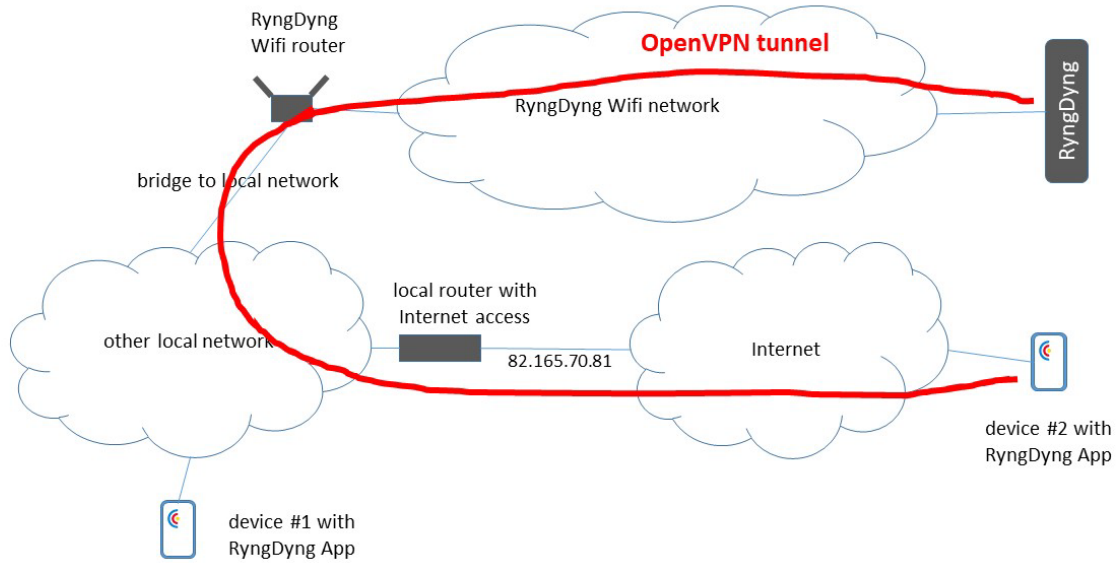
Switch on the VPN tunnel:



Now, the VPN tunnel is active and you can test it by trying to access the RyngDyng Wi-Fi router. Open a browser and type in the URL <http://10.10.10.254>. You should get the web page of the RyngDyng router.

If a powered on RyngDyng system has connection to the RyngDyng Wi-Fi network, the RyngDyng App will be able to connect to this RyngDyng via the OpenVPN tunnel.

Note that the device running the RyngDyng App does not need a direct connection to the RyngDyng Wi-Fi network. It can be connected to the other local network or, residing at another location that has Internet access. It does not matter.

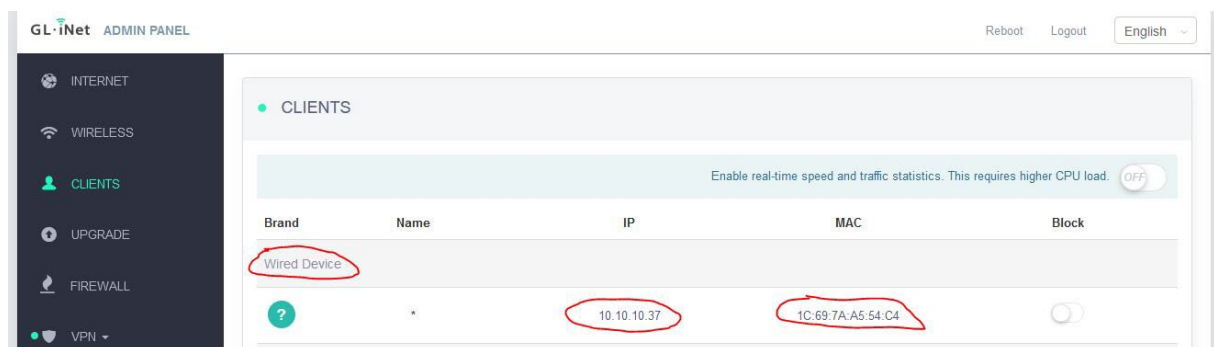


Remotely Power on RyngDyng RD720

RD720 supports Wake-On-LAN (WOL), if connected via an Ethernet cable to the RyngDyng router LAN port². The RyngDyngManager software supports the powering on, see also the manual for the RyngDyngManager software available for download [here](#).

However, if you use the RyngDyngManager remotely and connections go through the VPN tunnel, then you need some additional configurations.

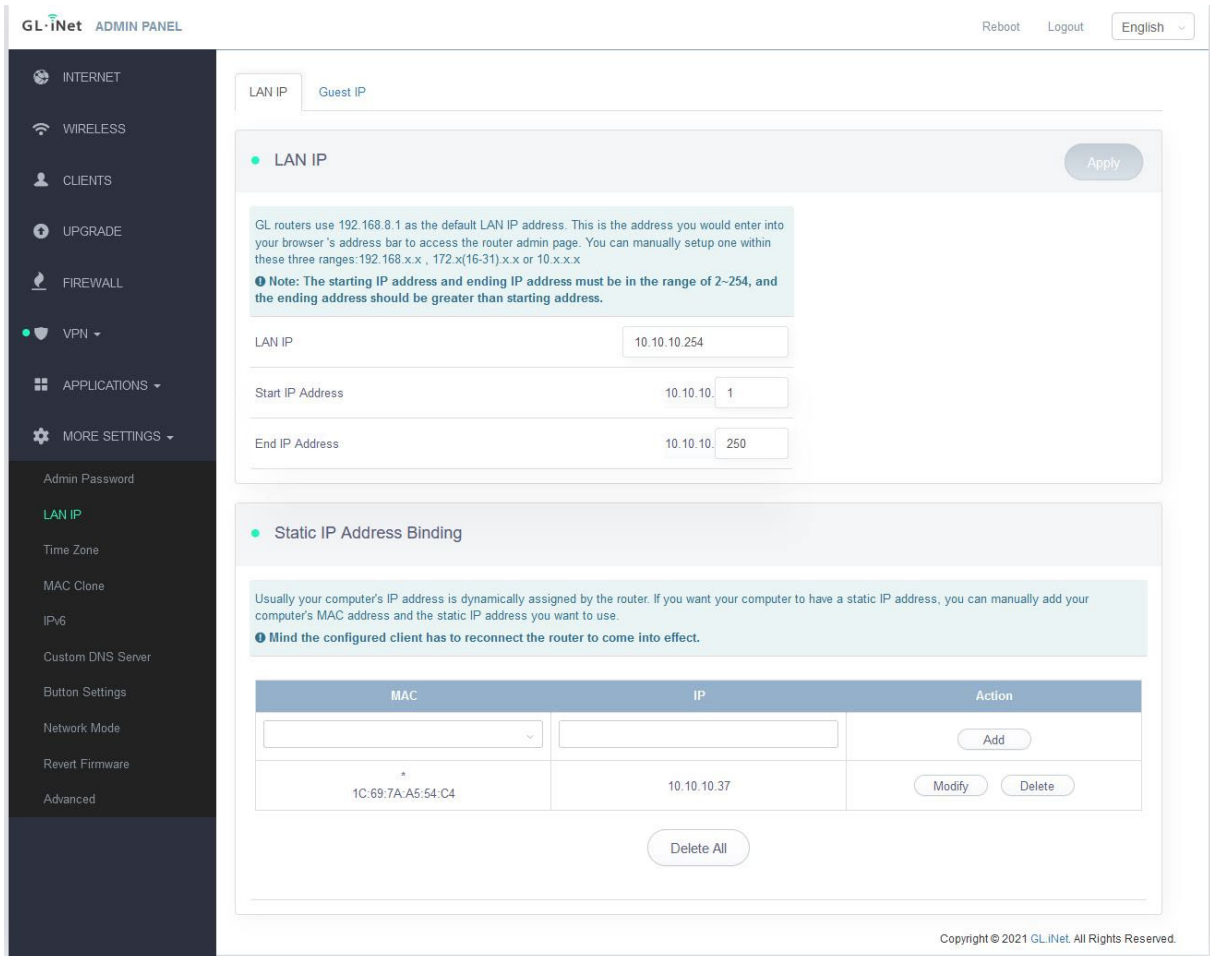
First, in the router assign a static IP address to the RyngDyng. Power on RyngDyng and open the web page of the router. On page CLIENTS you will find the IP address and the MAC address of your RyngDyng device.



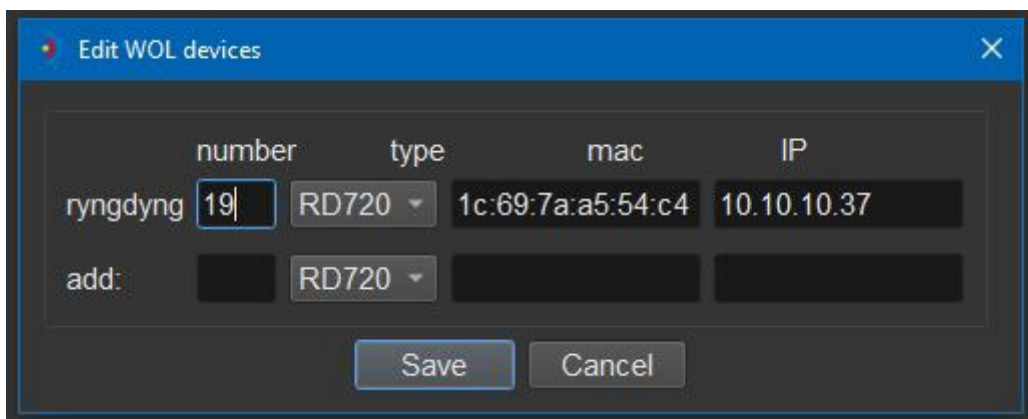
Note down the IP address and the MAC address. Make sure you take those of the Wired Devices section, i.e., those devices that have an Ethernet connection to the router.

Next step is to make this IP address a permanent one, that is static. Go to page MORE SETTINGS -> LAN IP. Select this device from the drop-down list and press the ADD button:

² There may be a switch in-between



The last step is to add this device as a WOL device to the RyngDyngManager software. In the settings menu click EDIT WOL Devices and add this device there:



Press Save.

Now you can power on the device remotely through the VPN tunnel.