

# Tunnel Server Setup



Most nodes will be set up as [Tunnel Clients](#). If you aren't sure, you probably don't need to follow the steps on this page.

If you'd like your node to be able to act as a Tunnel Server and allow other nodes to connect to you, you will need to make sure that your node is available over the Internet. This includes configuring a dynamic DNS entry, and making some firewall or port forwarding settings.

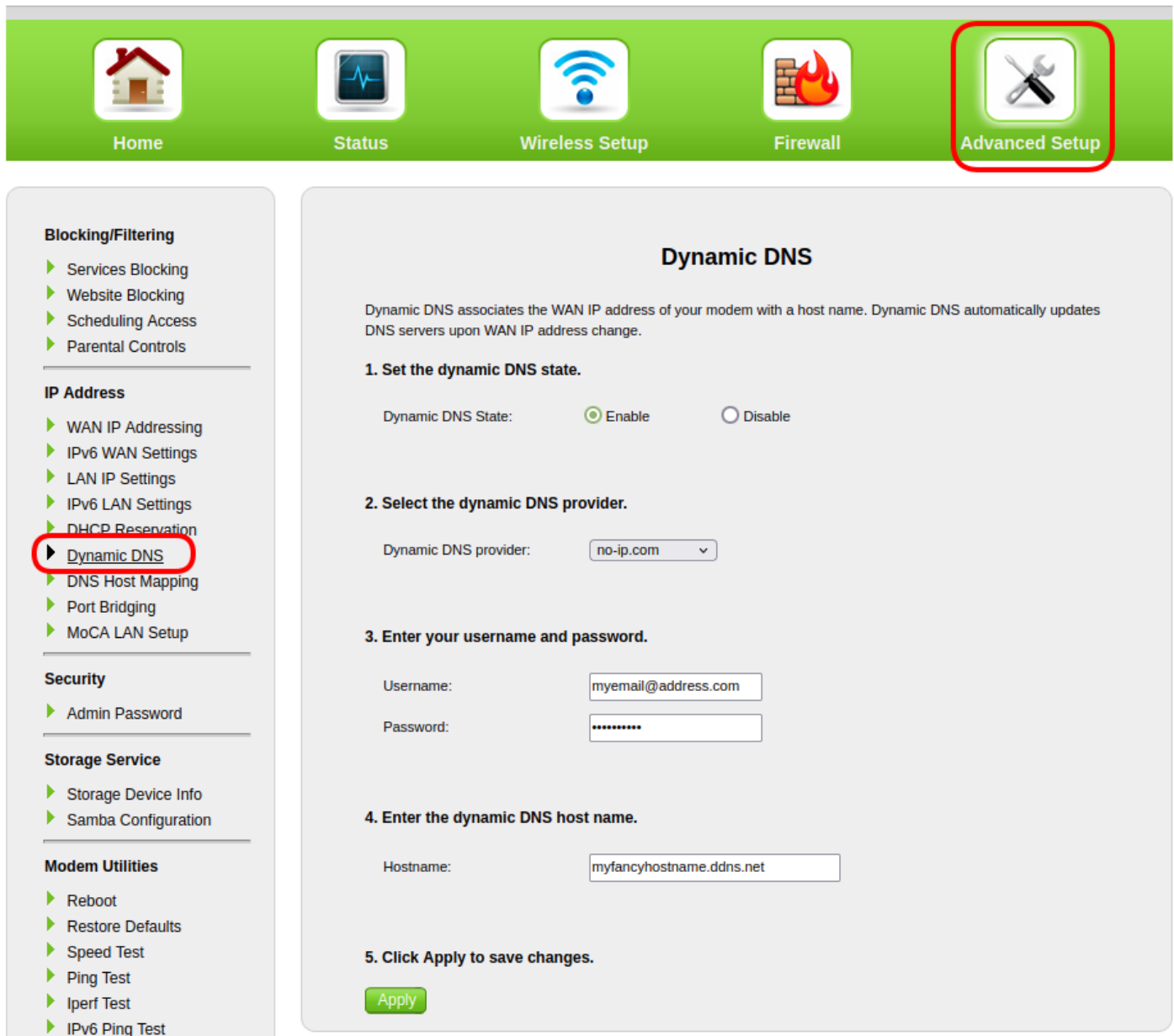
## DNS Name

Most residential internet services are given a single *dynamic* IP address, which means that the address can *change* every few days or so (or when the router power cycles). This means that when a server node suddenly gets a new public IP address, the client node can't find it anymore.

One solution is to use a [Dynamic\\_DNS](#) service like [No-IP](#). These services query your *dynamic* IP address, and translate it into a *static* hostname. It's that hostname that you then give the AREDN client (instead of your public IP address).

However, the No-IP service needs to be “told” when your dynamic IP address changes. This can be done by installing a small program that notifies them of the change, or alternatively, some routers have that function already built in. For example, the No-IP account can be entered in the Telus T3200M router here:

[Advanced Setup](#) → Dynamic DNS



**Home** **Status** **Wireless Setup** **Firewall** **Advanced Setup**

**Blocking/Filtering**

- Services Blocking
- Website Blocking
- Scheduling Access
- Parental Controls

**IP Address**

- WAN IP Addressing
- IPv6 WAN Settings
- LAN IP Settings
- IPv6 LAN Settings
- DHCP Reservation
- Dynamic DNS**
- DNS Host Mapping
- Port Bridging
- MoCA LAN Setup

**Security**

- Admin Password

**Storage Service**

- Storage Device Info
- Samba Configuration

**Modem Utilities**

- Reboot
- Restore Defaults
- Speed Test
- Ping Test
- Iperf Test
- IPv6 Ping Test

### Dynamic DNS

Dynamic DNS associates the WAN IP address of your modem with a host name. Dynamic DNS automatically updates DNS servers upon WAN IP address change.

- Set the dynamic DNS state.**  
Dynamic DNS State: ☒ Enable ☐ Disable
- Select the dynamic DNS provider.**  
Dynamic DNS provider:
- Enter your username and password.**  
Username:   
Password:
- Enter the dynamic DNS host name.**  
Hostname:
- Click Apply to save changes.**

With this setup, every time Telus gives me a new public IP address, the router notifies No-IP, which updates it so that `myfancyhostname.ddns.net` continues to point to my router.

## Port Forwarding

Port 5525 has to be forwarded to the hAP. There are two steps to this:

## DHCP Reservation

Just like Telus gives the router a *dynamic* WAN IP address, the router gives the home devices *dynamic* LAN IP addresses. The first step is to force the router to always give the same IP address to the hAP. On the T3200M this is done in:

## Advanced Setup → DHCP Reservation

The screenshot shows the 'Advanced Setup' page of a router's web interface. The top navigation bar has icons for Home, Status, Wireless Setup, Firewall, and Advanced Setup. The 'Advanced Setup' icon is highlighted with a red box. On the left sidebar, under 'IP Address', 'DHCP Reservation' is highlighted with a red box. The main content area is titled 'DHCP Reservation' and contains the following text:

DHCP reservation leases a permanent DHCP allocated address to a client.

**1. Select MAC Address, or manually enter a MAC address.**

Select MAC Address:

Manually Add MAC Address:

**2. Select an IP address to associate with a MAC address.**

IP Address:

Manually Add IP Address:

At the bottom, there is a table with the following entries:

VA7FI-HAP-1	08:5	27	192.168.1.204	<input type="button" value="Remove"/>
-------------	------	----	---------------	---------------------------------------

- Select the MAC address of the hAP from the list.
- Choose an IP address to assign it.
- Disconnect the hAP from the router and reconnect it to clear the IP.

## Port Forwarding

Now that the hAP's LAN IP address is fixed, we can forward a port to it:

## Firewall → Port Forwarding

The screenshot shows the Wcairedn.ca web interface. At the top, there is a navigation bar with five icons: Home (house), Status (heart rate), Wireless Setup (Wi-Fi), Firewall (fire), and Advanced Setup (wrench). The Firewall icon is highlighted with a red box. Below the navigation bar, on the left, is a sidebar menu under the heading "Firewall". It contains several items: Firewall, IPv6 Firewall, Port Forwarding (highlighted with a red box), Applications, DMZ Hosting, IPv6 DMZ Hosting, and UPnP. The main content area is titled "Port Forwarding". It contains the following text: "Enter ports or port ranges required to forward Internet applications to a LAN device below." Below this, there are two steps: "1. Set the LAN/WAN port and IP information." and "2. Click Apply to save changes." The first step includes several input fields: "Select LAN Device:" with a dropdown menu showing "Manually enter the IP address", "LAN IP Address:" with a text box, "External (WAN) Start Port:" with a text box, "External (WAN) End Port:" with a text box, "Internal (LAN) Start Port:" with a text box, "Internal (LAN) End Port:" with a text box, and "Protocol:" with a dropdown menu showing "TCP". Below the input fields is a green "Apply" button. At the bottom, there is a table titled "Applied Port Forwarding Rules". The table has six columns: "LAN START/ END PORT", "PROTOCOL", "LAN IP ADDRESS", "WAN START/END PORT", "MODIFY", and "REMOVE". The table contains one row of data: "5525/5525", "TCP", "192.168.1.204", "5525/5525", "Modify", and "Remove".

**Firewall**

- Firewall
- IPv6 Firewall
- Port Forwarding**
- Applications
- DMZ Hosting
- IPv6 DMZ Hosting
- UPnP

**Port Forwarding**

Enter ports or port ranges required to forward Internet applications to a LAN device below.

**1. Set the LAN/WAN port and IP information.**

Select LAN Device: Manually enter the IP address

LAN IP Address:

External (WAN) Start Port:

External (WAN) End Port:

Internal (LAN) Start Port:

Internal (LAN) End Port:

Protocol: TCP

**2. Click Apply to save changes.**

Apply

**Applied Port Forwarding Rules**

LAN START/ END PORT	PROTOCOL	LAN IP ADDRESS	WAN START/END PORT	MODIFY	REMOVE
5525/5525	TCP	192.168.1.204	5525/5525	<span>Modify</span>	<span>Remove</span>

- Select the hAP's IP address from the list
- Enter 5525 as the start and 5535 as the end (if you want to give 10 tunnels)
- Select TCP

## AREDN Server Setup

Now we can go back to AREDN and add a server:

## Tunnels

Help

**Tunnel Server**  
DNS name of this tunnel server

va7fi.ddns.net

**Add tunnel**  
Add a tunnel from a template

Wireguard Server +

Wireguard Server

VE7ABC-HAP

qT2xSAZ4fHWCvDkyTFfjYmHI 172.31.40.178:5532 Wgt

Notes...

Clipboard icon

1. add your DNS name
2. select Wireguard Server and click the +
3. enter the name of the client
4. the rest of the information will auto populate
5. click the clipboard icon and copy the information, which you'll need to send to the client.
6. click Done
7. select Commit

Pending changes: 2

Commit Revert

From:  
<https://wcaredn.ca/> - **West Coast  
AREDN**

Permanent link:  
<https://wcaredn.ca/starting/tunneling/tunnel-server-setup>

Last update: **2025/10/05 07:32**

