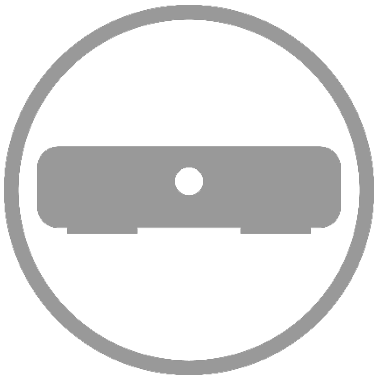
pakedge®

RE-1, RE-2, RK-1

High-Speed Gigabit AV Router

User Guide



FCC Declaration of Conformity

Pakedge Device & Software, Inc., 3847 Breakwater Avenue, Hayward, CA, declares under sole responsibility that the RK-1, RE-1, and RE-2 comply with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. These devices comply with Part 15 of FCC Rules. Operation of the devices is subject to the following two conditions: (1) These devices may not cause harmful interference, and (2) these devices must accept any interference that may cause undesired operation.

WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING WATER. CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL. CAUTION: THIS DEVICE MUST BE INSTALLED AND USED IN STRICT ACCORDANCE WITH THE MANUFACTURER'S INSTRUCTIONS AS DESCRIBED IN THE USER DOCUMENTATION THAT COMES WITH THE PRODUCT. WARNING: POSTPONE INSTALLATION UNTIL THERE IS NO RISK OF THUNDERSTORM OR LIGHTNING ACTIVITY IN THE AREA.

Safety precautions

When using this device, always follow basic safety precautions to reduce the risk of fire, electric shock, and injury to persons, including the following:

- Comply with all warning and caution statements in the instructions.
- Retain instructions for future reference.
- Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.
- Installation of this product must be in accordance with national wiring codes and must conform to local regulations.
- Avoid using this product during an electrical storm. There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug the power supply and disconnect the CAT5e.This will prevent damage to the product due to lightning and power surges.
- Give particular attention to all safety precautions.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure what type of power is supplied to your home, consult your dealer or local power company.
- It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damage to the equipment from lightning strikes and other electrical surges.
- Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.
- Keep the device free from excessive heat, humidity, vibration, and dust.
- Do not directly cover the device or block the airflow to the device with insulation or any other objects.

Contents

Introduction

The popularity and affordability of IP networking has driven audio/video and control networks to share the same physical wiring with computer networks. However, computer data can tolerate unpredictable latency in ways that audio-video streaming and control systems cannot. Sophisticated systems require the same robustness as an enterprise network to ensure that IP-based controls occur instantly and audio/video packets arrive in time.

Note: **If this is your first time installing this product, please read this manual in its entirety.**

Customer Service and Technical Support

Pakedge Device & Software, Inc. is committed to providing you with exceptional support on all of our products. If you wish to speak with one of our representatives, you may contact us at:

Customer Service

Email: **customerservice@pakedge.com**

Phone: **650.385.8701**

Technical Support

Email: **support@pakedge.com**

Phone: **650.385.8703**

Visit our website for up-to-date support information at www.pakedge.com.

Please be prepared to provide your product's model and serial number when contacting Pakedge Support. Your model and serial numbers are printed on a label located on the electronic housing.

Installing

For installation procedures, refer to the Quick Start Guide that came with the router. You can also visit the Dealer Portal on our website for all the current manuals and Quick Start Guides.

Note: If you install the router in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room temperature. Make sure you install the equipment somewhere within the recommended temperature range.

For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.

For free-standing installation, make sure that the router has at least 1.5 in. (3.75cm) of clearance on each side to allow for adequate air flow and cooling.

Getting to know your product

Package contents:

- **RK-1, RE-1, or RE-2 router**
- **Mounting brackets**
- **Power cable**
- **6ft CAT5E cable**
- **Quick Start Guide**

The front panel of the router has several blue LEDs. See the **Table 1** below for more information.

Table 1: LED Explanation (From Left to Right)

LED		Status	Operation
USB 1 - 2	LINK/ACT	Blue	USB is connected
		Flashing Blue	USB is being accessed
		Off	No device connected
WAN 1 - 2	LINK/ACT	Blue	Port is online (link established)
		Flashing Blue	Activity
		Off	No device connected
LAN 1 - 5	LINK/ACT	Blue	Port is online (link established)
		Flashing Blue	Activity
		Off	No device connected

Power	Blue	The router is powered on
	Off	The router is turned off

Note: LAN Port number 5 can be configured as a Guest network.

Below you will find a description of the interfaces on the back of the router in **Table 2**.

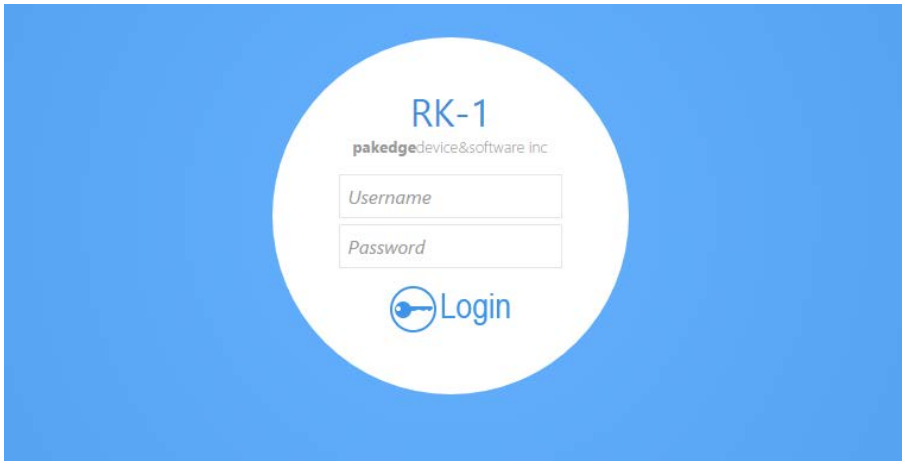
Table 2: Interface Explanation (From Left to Right)

Interface	Type	Speed	Protocol	Description
Reset Button	N/A	N/A	N/A	Hold Reset Button for 10 seconds to factory default the settings
USB 1 - 2	USB-A	Up to 5Gbps	USB 3.0	USB port used for file sharing
WAN 1 -2	RJ-45	10/100/1000 Mbps	Ethernet	WAN port used for the Internet connection from the ISP
LAN 1 - 5	RJ-45	10/100/1000 Mbps	Ethernet	4-port switch connections on the internal network
Console	RJ-45	115200	Console	Console port for maintenance use
AC Power input	AC	N/A	N/A	Power Input
Power Switch	N/A	N/A	N/A	On/Off Power Switch

Accessing the router

To access the router's GUI:

1. Plug an Ethernet cable from the router to a PC.
2. Make sure your network card is set to obtain an IP address automatically. Then open any Internet browser and go to the address http://192.168.1.99 or you can simply type **pakedgerouter.com**
   Note: For best results we recommend using Mozilla Firefox as your web browser. If you are using Internet Explorer, use version 9 or newer.
3. Enter the default username **pakedge** and the password **pakedger**. Click **login**.

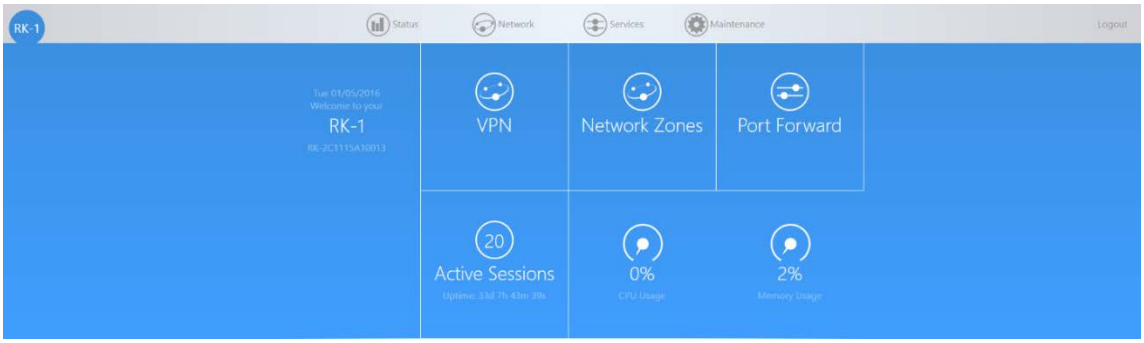


Important: Change this default password. See the section "Username/Password."

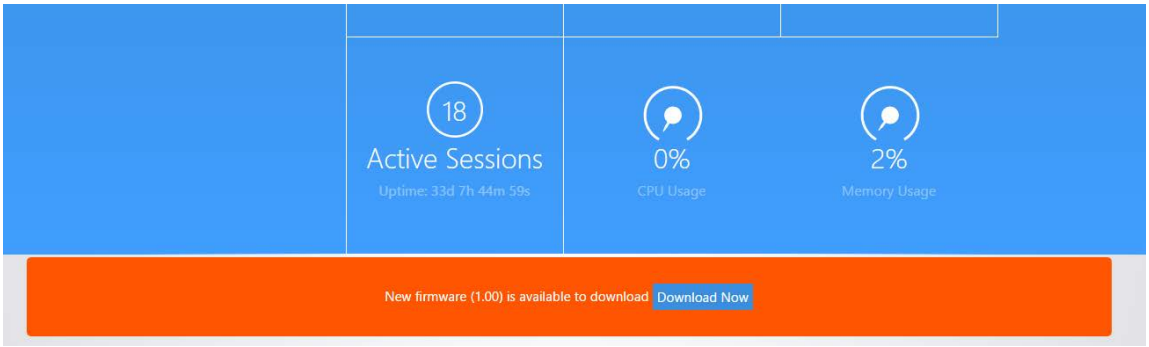
Dashboard

The dashboard provides frequently used quick links to help with more efficient set up.

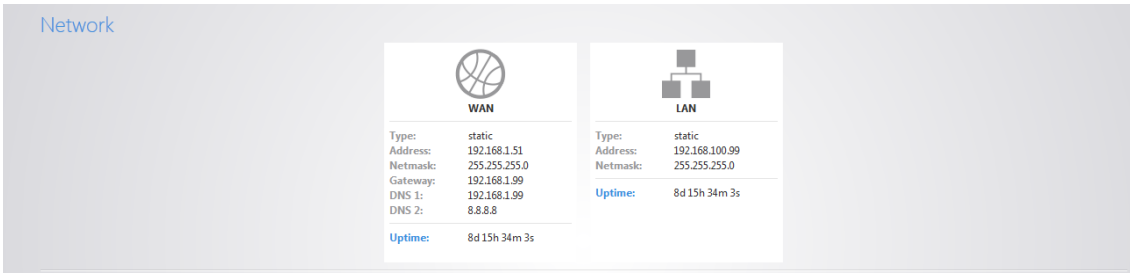
Towards the top of the page you will find information on the serial number, uptime, and the number of active sessions on the router as well as the CPU and memory usage.



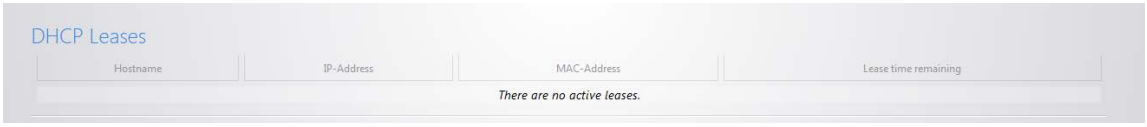
If there is new firmware available for the router, you will see a message alerting you with an option to download it.



Under **Network** you will find a summary of the network zones that are active on the router.



The **DHCP Leases** section shows the devices that have received an IP address form the router.



Other Connected Devices will display any device that has been discovered by the router. When a device on the network transmits data, the router will log its IP address. Usually devices with static IPs assigned to them will appear in this field.

Settings

Connecting to the Internet

The router supports the three main types of Internet connections:

- **DHCP** (Typically used by cable companies and DSL basic service)
- **Static IP** (Fixed public IP address mostly used by Business Class Broadband services)
- **PPPoE** (Used by DSL companies such as AT&T)

Determine what type of Internet connection you have from your Internet Service Provider (ISP), and then follow one of the three instruction sets below to connect the router to the Internet.

DHCP

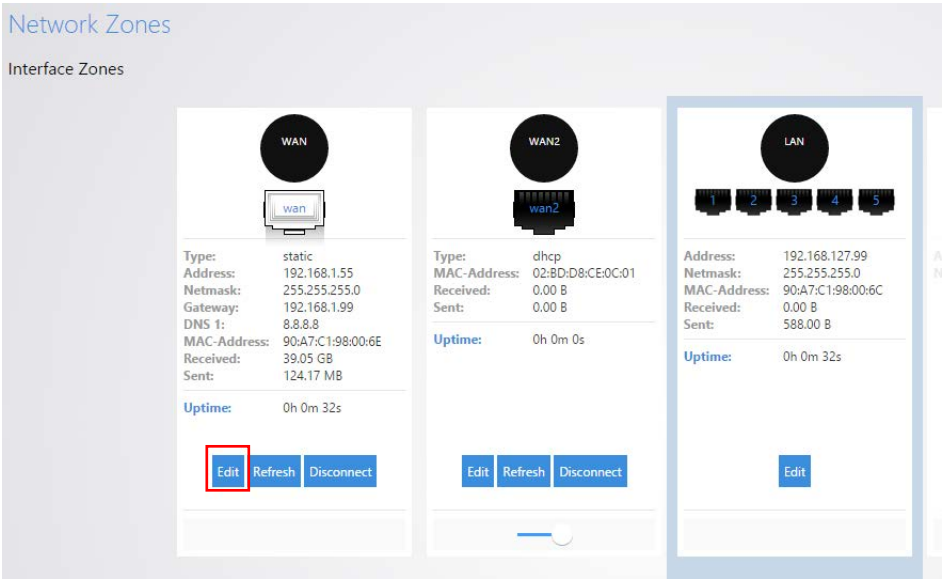
By default, the router will connect to the Internet using DHCP. If your ISP uses DHCP, you may need to reset the modem to get Internet access. If you are using a modem that has a router built into it, you may have to configure DMZ settings to allow complete functionality of the router.

Static IP

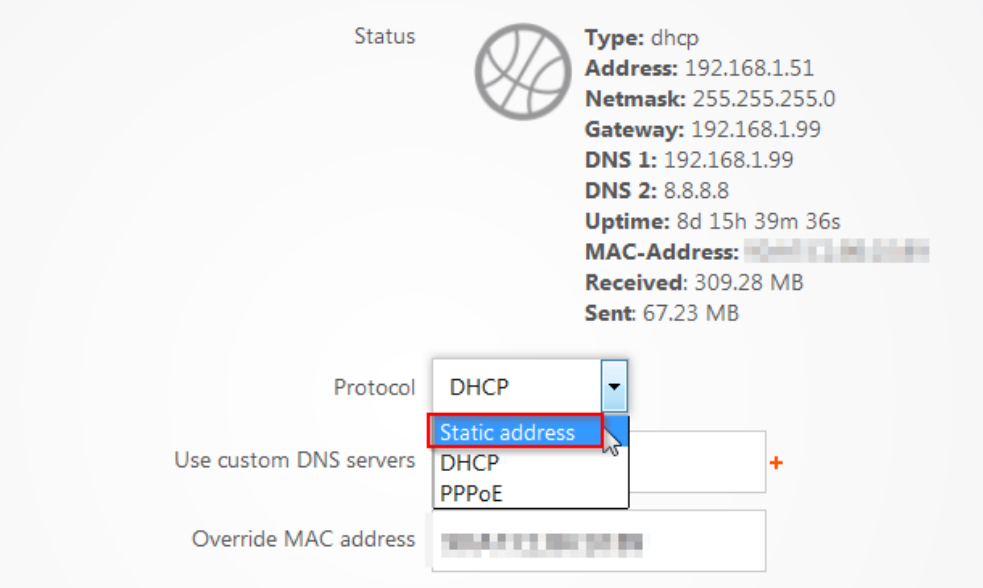
To configure the router to a static IP:

1. Hover your mouse towards the top of the page over **Network**. Click **Network Zones**.

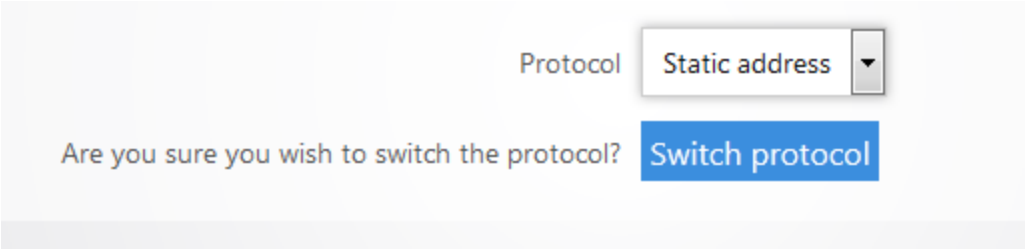
2. **Edit** the **WAN** Zone.



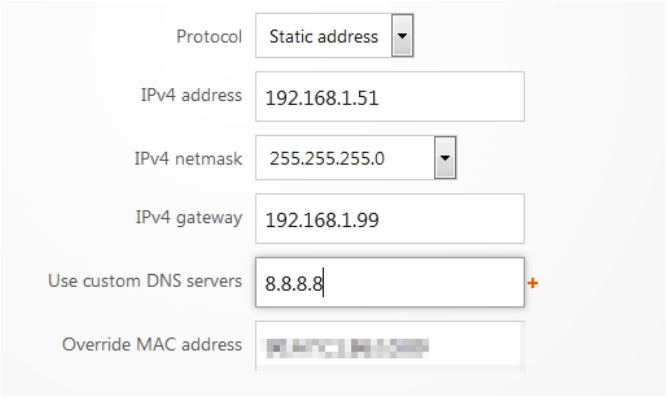
3. Select **Static Address** for the Protocol.



4. Click **Switch Protocol** to switch the **WAN** Zone to Static.



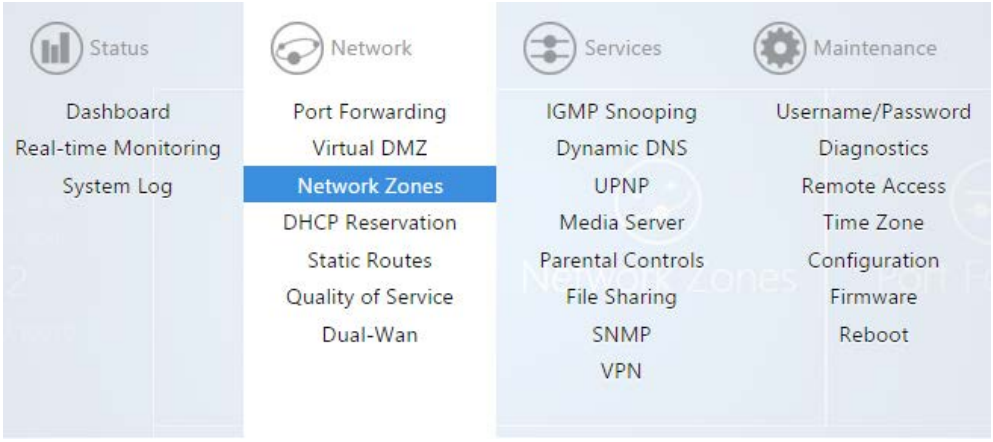
5. Enter the **IP address, subnet mask, Default Gateway** and **DNS Server** provided by your ISP. Select **custom** from the netmask drop down menu to enter a custom subnet mask. Click **Apply**. The router now has the Static IP configured on it.



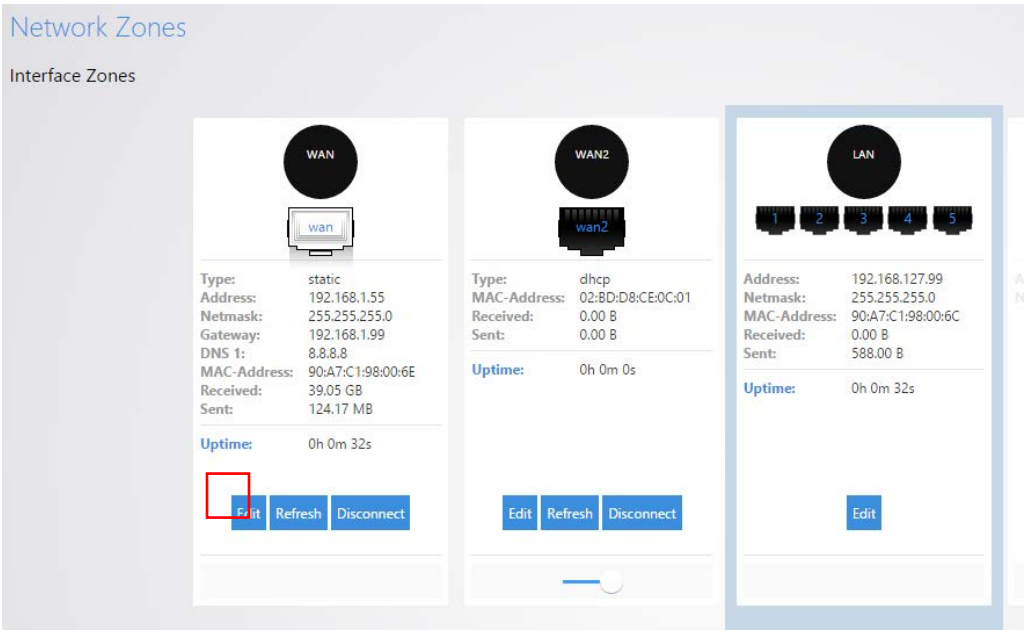
PPPoE

To configure the router using a PPPoE connection:

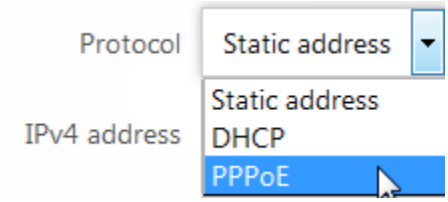
1. Log in to the router.
2. Click **Network Zones**.



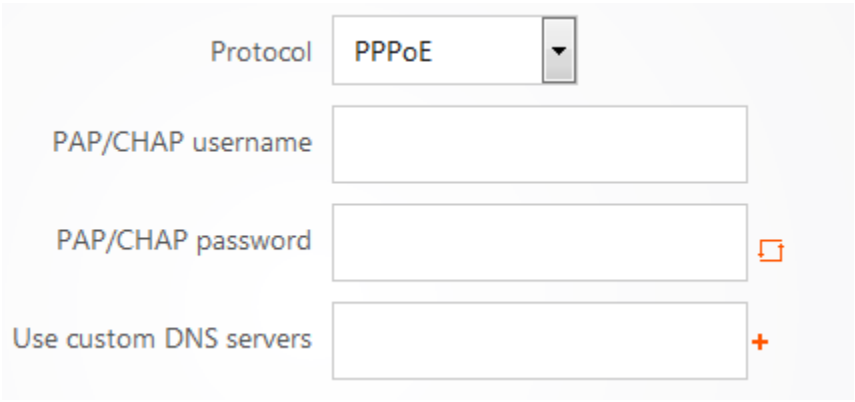
3. **Edit** the **WAN** Zone.



6. Select **PPPoE** from the Protocol drop down menu, then click **Switch Protocol**.



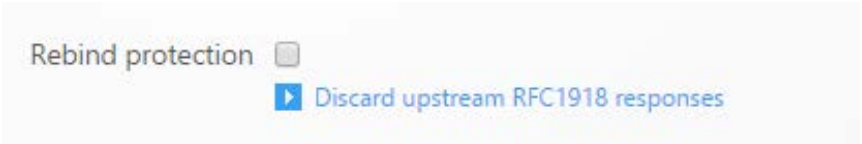
7. Enter the username that the ISP assigned under the **PAP/CHAP username** field. Enter the password in the **PAP/CHAP password** field. For the **Use custom DNS servers**, enter the DNS server you would like to use. For example, you can use 8.8.8.8. Click **Apply** when finished. The router is now setup for PPPoE.



Additional WAN Options

DNS Forwarding
The DNS Forwarding option will forward LAN DNS requests pointed to the router to the specified public DNS server.

Rebind Protection
This function protects the WAN from receiving DNS information from any “Local” non-Public IP address positioned above the router in the network. If the router is positioned behind another router, this feature should be disabled.

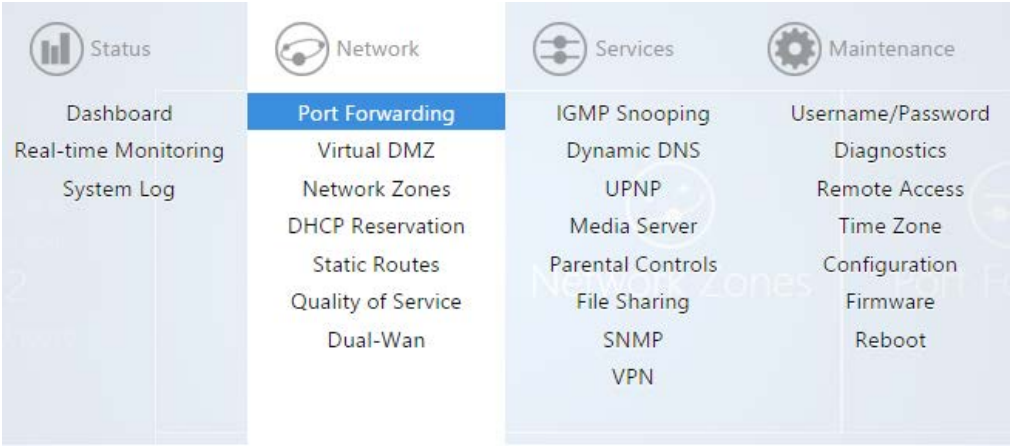


Port Forwarding

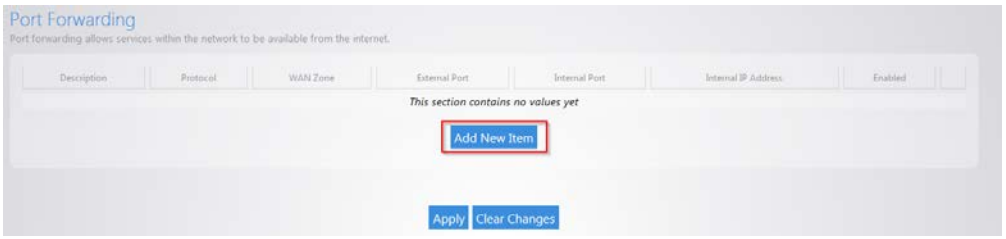
Port forwarding allows services inside the network to be available from the Internet. For example, if you have an IP camera on your network port forwarding would allow you to remotely view the camera.

To configure port forwarding:

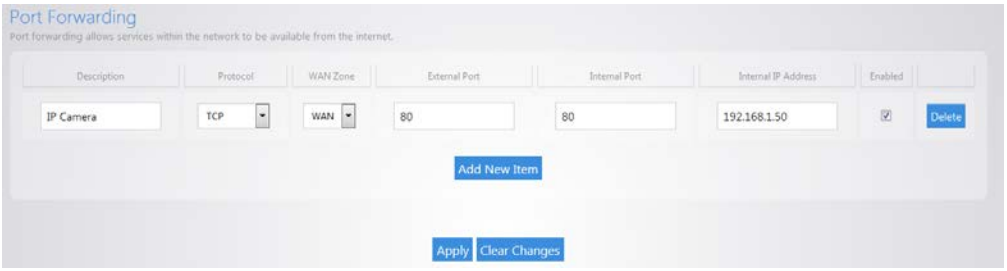
1. Navigate to **Network** >**Port Forwarding**.



2. As an example, we will forward TCP port 80 to an IP camera on the IP address 192.168.1.50. Click **Add New Item**.



3. For the **Description** enter **IP Camera**. For the **Protocol** select **TCP**. For the **WAN Zone** select **WAN**. We will enter **80** for the **External Port**. Enter **80** as the **Internal port**. For the **internal IP address** select **custom** and enter **192.168.1.50**. Leave the enable box checked. Click **Apply**. The Port forward information will be saved in this section.

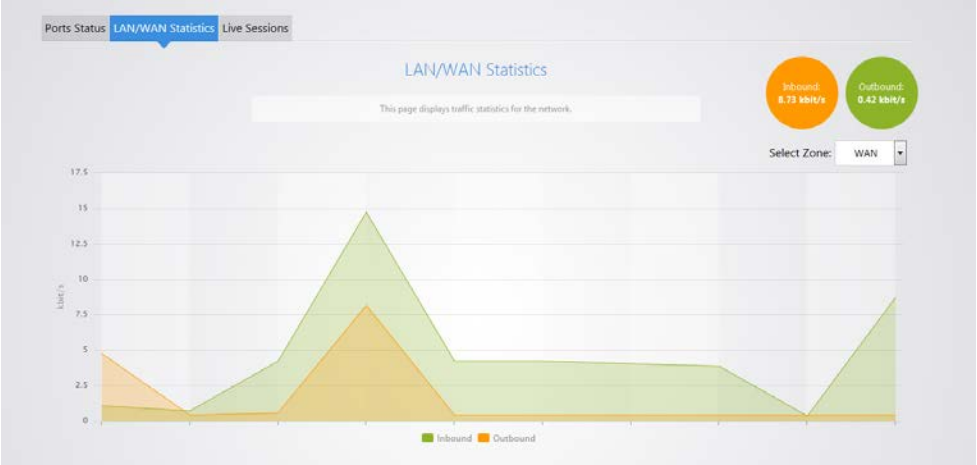


Real-Time Monitoring

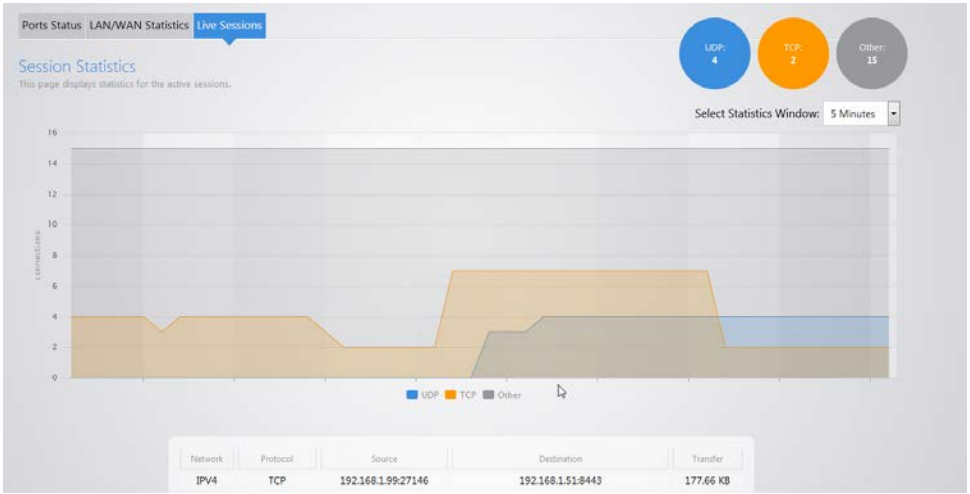
The **Real-Time Monitoring** section allows you to view statistics on the router.

The **Port Status** section will display which ports on the router are currently active.

The **LAN/WAN Statistics** will display the amount of traffic going through the LAN or WAN of the router.



The **Live Sessions** will display information on active connections. This information includes the protocol type, amount of data transferred and the destination of the data.



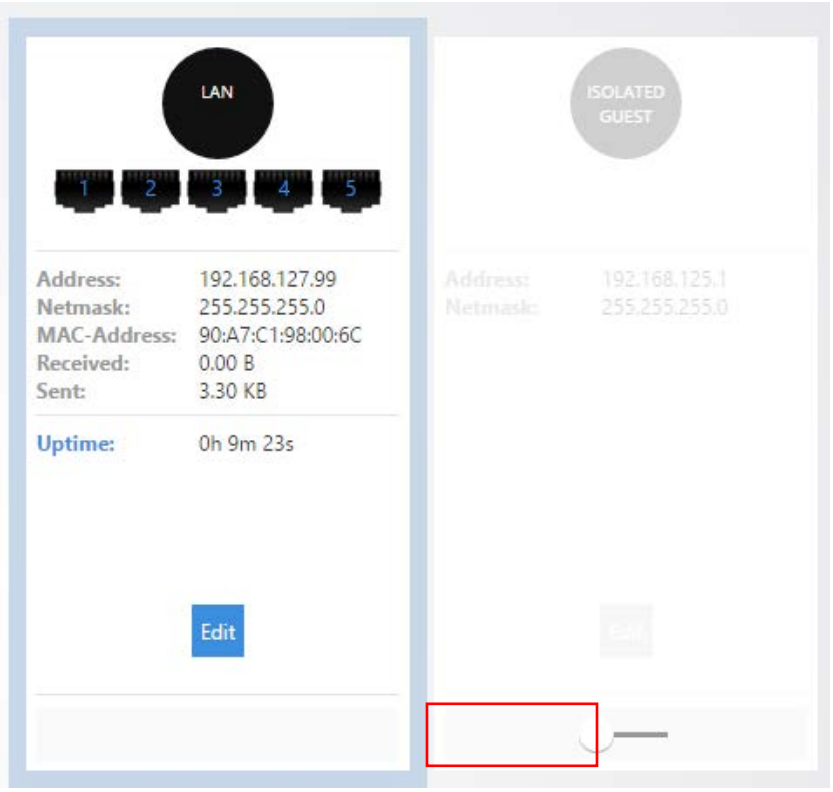
Isolated Guest network

The router has an isolated guest network option. When enabled, port 5 on the router will be turned into a guest network port. Any devices connected on that port will be placed on the Guest network. The Guest network will only have access to the Internet. It will not have access to any internal resources.

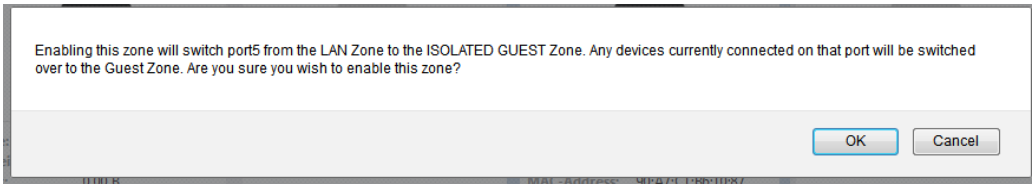
To enable the isolated guest network:

1. From the **Network** menu, click **Network Zones**.

2. Click the toggle on/off switch under the **Isolated Guest** network zone.



3. You will get a message letting you know that port 5 will be turned into the Isolation Guest network port. Click **OK** to enable the isolated guest network.

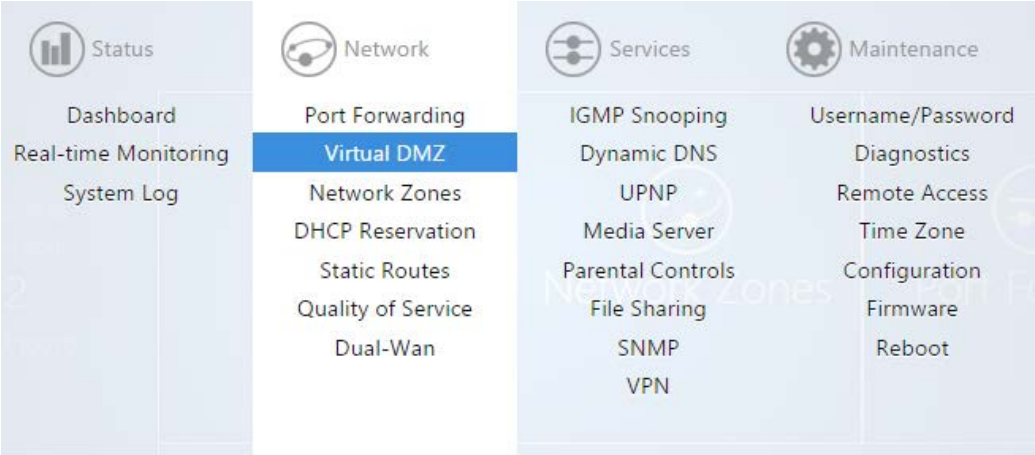


Virtual DMZ

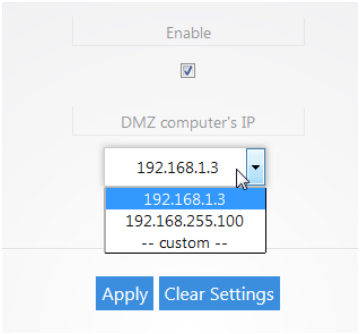
The Virtual DMZ will allow you to place a device in the network outside of the firewall. This will allow for unrestricted access to it from the Internet.

To configure the Virtual DMZ:

1. Click **Virtual DMZ**.



2. Select **Enable**. For the **DMZ computer's IP** field, you can select the device from the drop down menu. If the device is not listed you can select **custom** to manually enter the IP address of the device you would like to place in the DMZ. Click **Apply** to finalize the configuration.



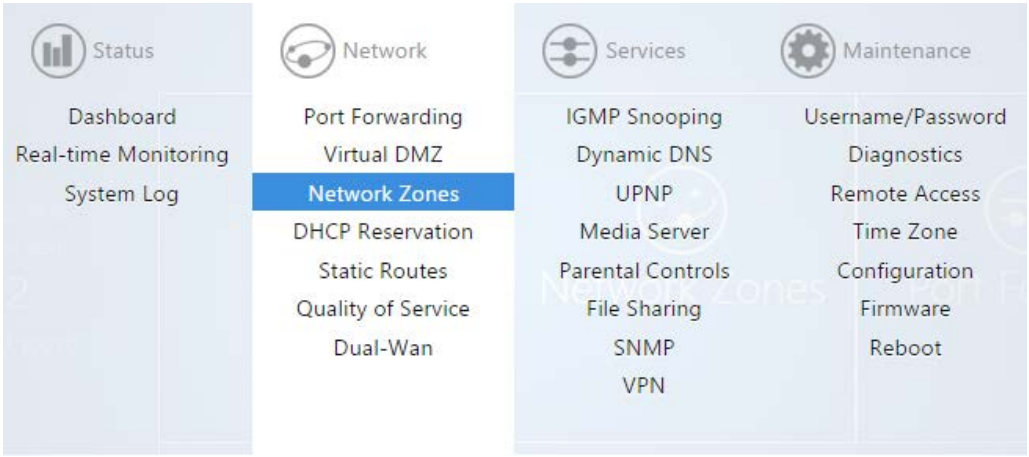
Note: When you enable the Virtual DMZ you will still be able access the routers GUI remotely via HTTPS, and you will still be able to use the VPN feature.

Changing the IP address of the LAN Zone

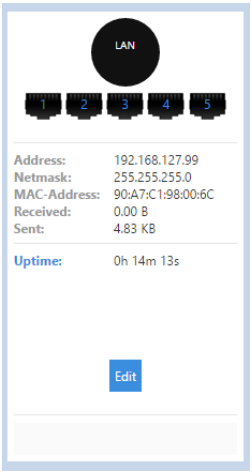
The default IP address of the router is 192.168.1.99.

To change the IP address of the router or change the entire network address:

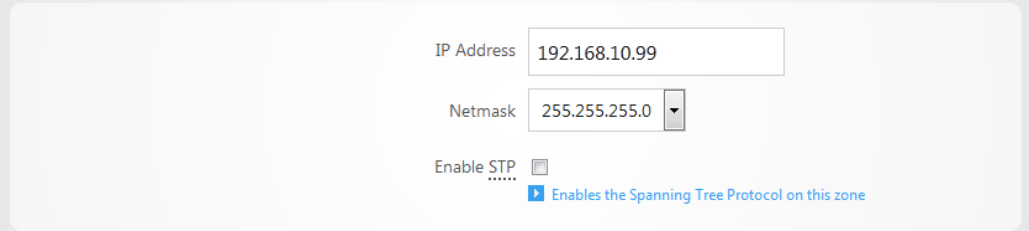
1. Click **Network Zones**.



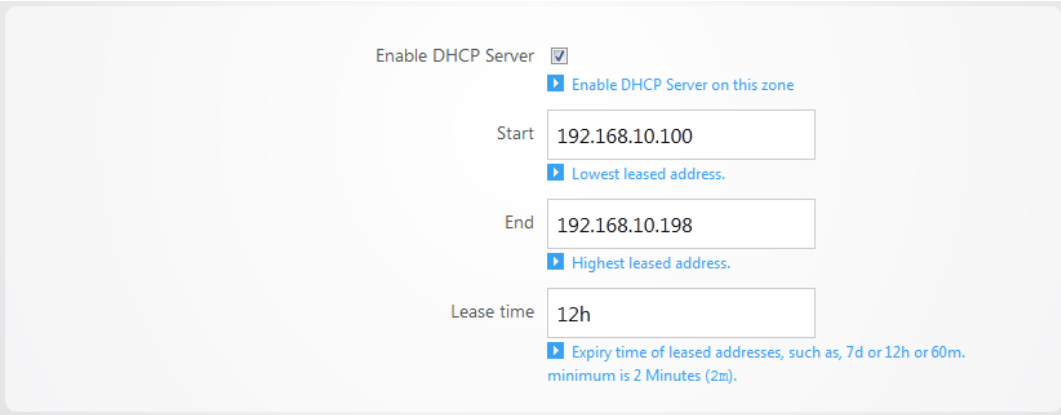
2. Click **Edit**.



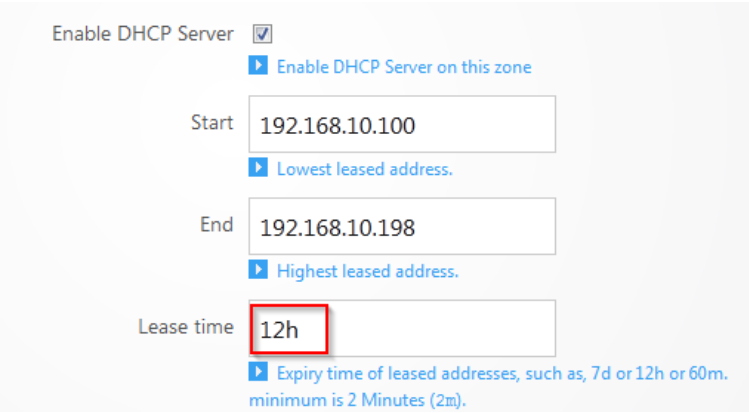
3. Enter the new IP address you wish to use in the **IP Address** field. In the following example, we change the IP address of the router to 192.168.10.99.



4. In the **DHCP Server** section, the **Start** field indicates the first IP address that will be handed out by the router. The **End** field indicates the last IP address that will be handed out. The **limit** field indicates the amount of IP addresses that the router can hand out.



5. The **Lease time** field allows you to view/modify DHCP IP address lease time. The following format must be used: A **D** represents days, an **H** represents hours and an **M** represents minutes. For example, if you wanted to change the lease time to be 3 days 2 hours and 30 minutes you would set the lease time to **3D2H30M**.



6. Click **Apply** to finalize your settings.

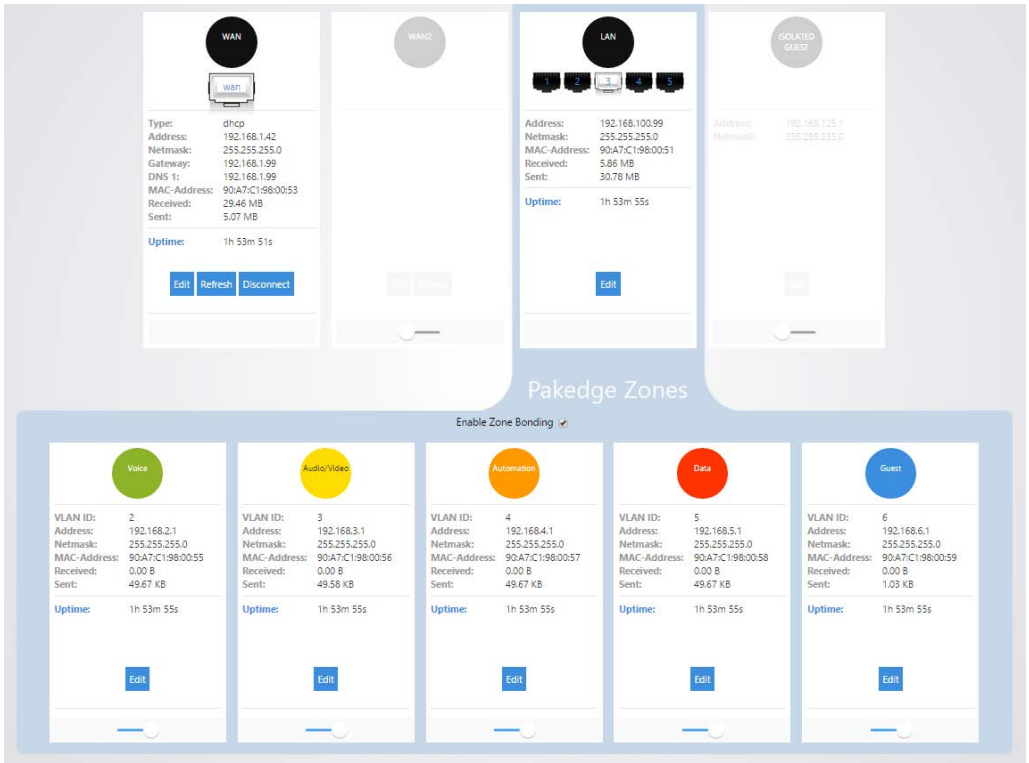
VLAN settings

The router comes configured with VLANs. VLANs allow you to separate devices into smaller networks to increase efficiency on your network. The router will come with VLANs 2-6.

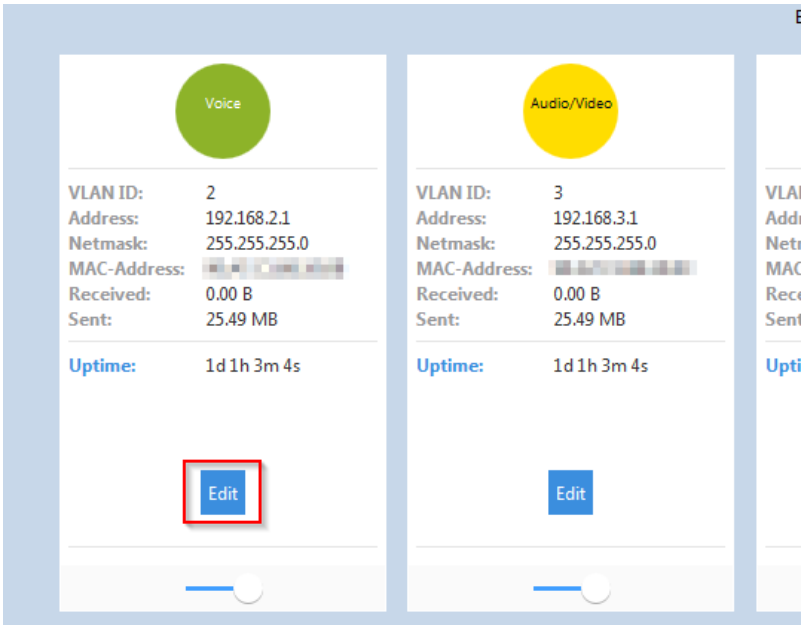
To modify any of the VLAN settings:

1. Click **Network Zones**.

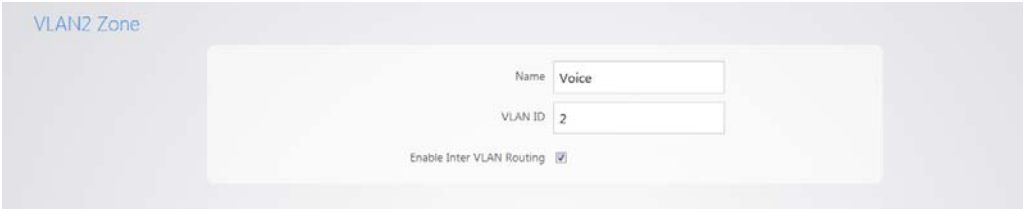
VLANs 2-6 will be displayed towards the bottom.



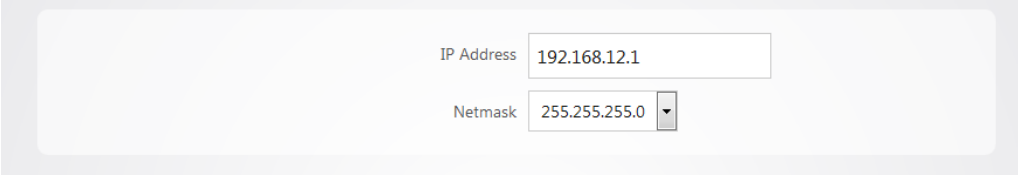
2. The **Zone Bonding** option allows devices that use multicast messaging to communicate across VLANs.
3. Click **Edit** under any of the VLANs to view its settings. As an example, we will click **Edit** under VLAN2.



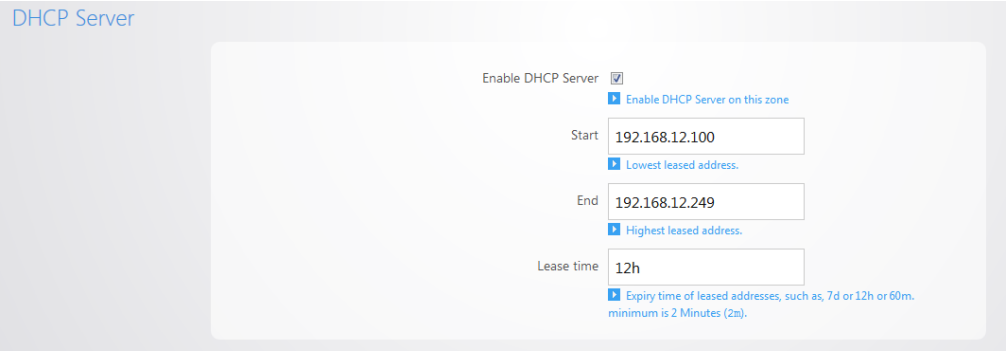
4. The **Name** field allows you to change the name of the VLAN. By default VLAN2 will be named **Voice**. The **VLAN ID** allows you to use a different VLAN ID. **Enable Inter VLAN Routing** allows this VLAN to communicate with other VLANs. Unchecking this option would give VLAN2 Internet access only. VLAN 2 would not be able to communicate with any other VLAN, and all other VLANs would not be able to communicate with VLAN2.



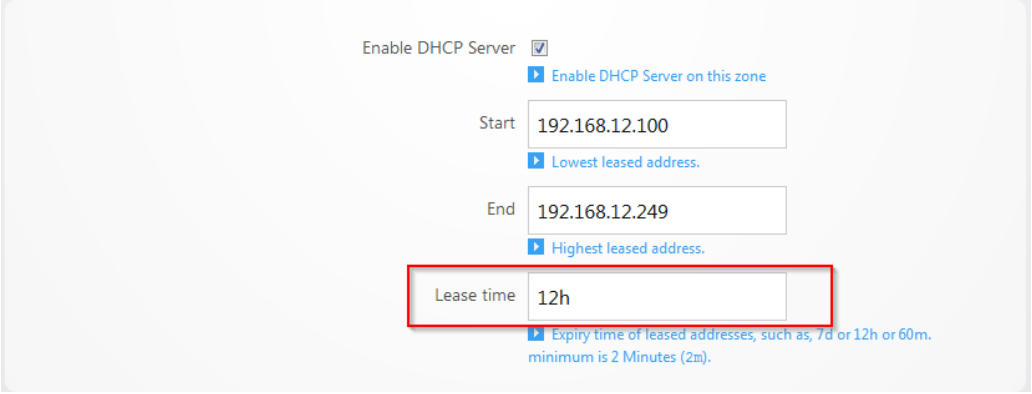
5. If you would like to change the IP address of VLAN2 you can enter the new IP in the **IP Address** field. As an example, we will change the IP address of VLAN2 to 192.168.12.1.



6. Towards the bottom you will see the DHCP server settings for VLAN2. We will change the **Start** IP address to **192.168.12.100** and the **End** IP address to **192.168.12.249** so that it matches the new IP scheme.



7. The **Lease time** field allows you to view/modify DHCP IP address lease time. The following format must be used: A **D** represents days, an **H** represents hours and an **M** represents minutes. For example, if you wanted to change the lease time to be 3 days 2 hours and 30 minutes, you would set the lease time to **3D2H30M**.

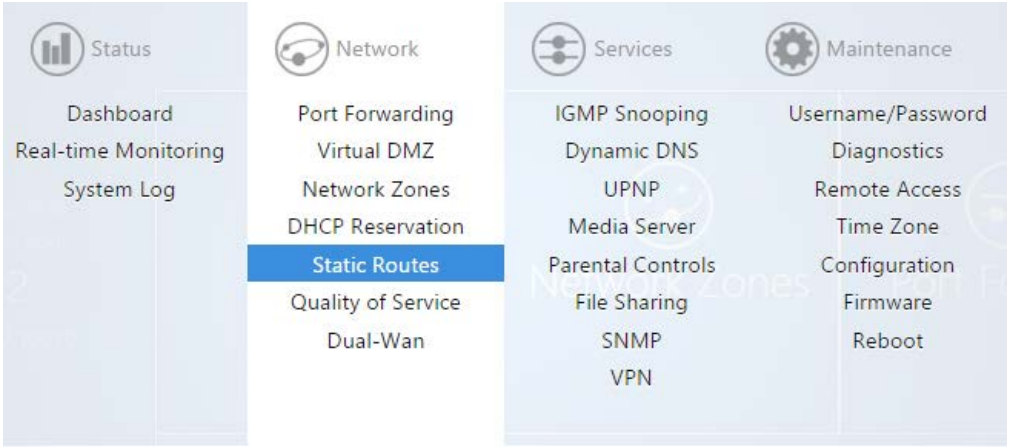


Static Route

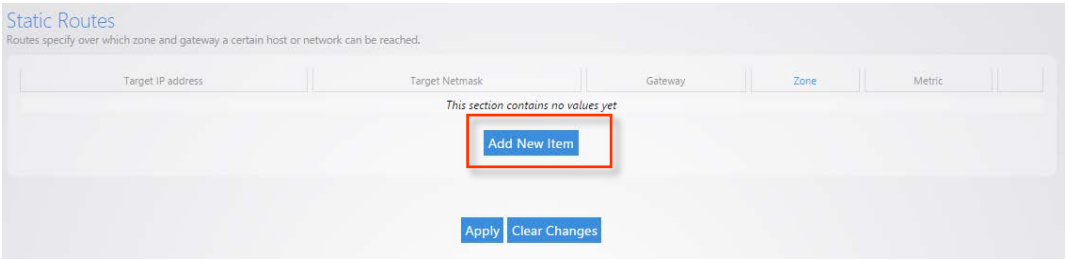
Static Routes allow the manual forwarding of traffic to networks that are not a part of the router internal routable networks.

To create a Static Route:

1. Click **Static Route**.

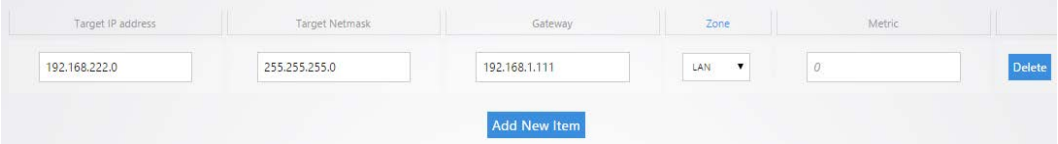


2. For our example we will be forwarding traffic destined for the unknown network (**192.168.222.0/24**) to the IP address of the Gateway device which has knowledge of that network (**192.168.1.111**). First click **Add New Item**.



3. **Target IP Address** will be the network which must be accessed and is not directly known by the router (**192.168.222.0**). **Target Netmask** is the Subnet Mask of that network (**255.255.255.0**). **Gateway** is the IP Address traffic should be forwarded to in order to reach that new network (**192.168.1.111**). An example of this would be the WAN IP address of a second router connecting to the LAN of the router. In order to reach the second routers LAN a static route must be added to inform the router of the Gateway IP that has direct knowledge of this new network. **Zone** should match the Network Zone of the Gateway traffic will be forwarded to. **Metric** can optionally be

changed to indicate precedence between two similar routes. If the higher precedence route is not accessible then the lower metric route will be taken.



4. After the information has been entered, click **Apply** at the bottom of the page.

DHCP Reservation

DHCP reservation allows the router to continually assign the same IP address to a device.

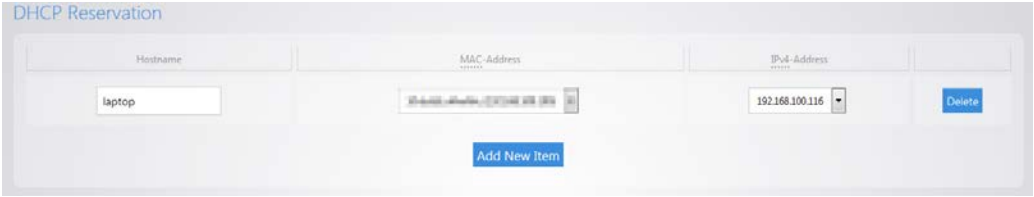
To create a DHCP reservation:

1. Click **DHCP Reservation**.

2. Click **Add New Item**.

3. For the **Hostname** field, fill out a name. For the **MAC-address** field, click the drop down menu and select the device you would like to make a reservation for. You can also manually enter the mac address of the device. When entering the mac address, use colons. For example, **aa:bb:cc:dd:ee:ff**.

In the **IPv4-Address** field, select **custom** and enter the IP address that you would like to assign to the device.



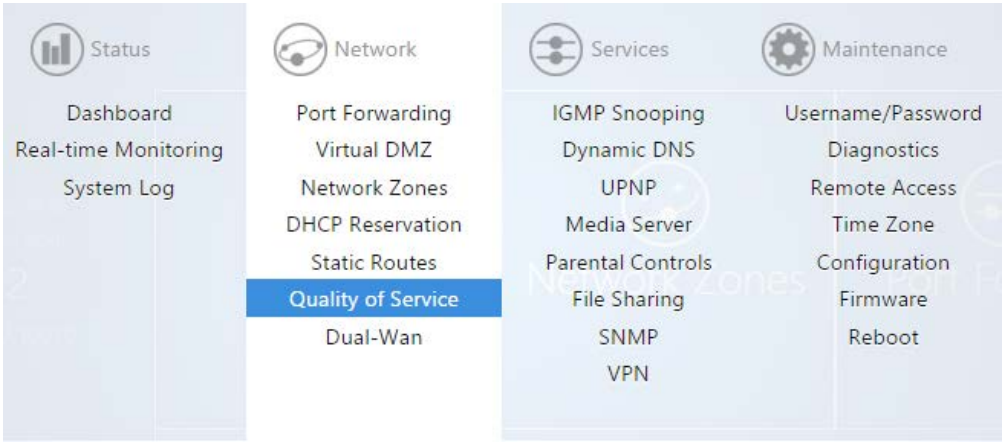
4. Click **Apply** when finished. You may need to restart the network card of your device in order for it to receive the new IP address.

Quality of service

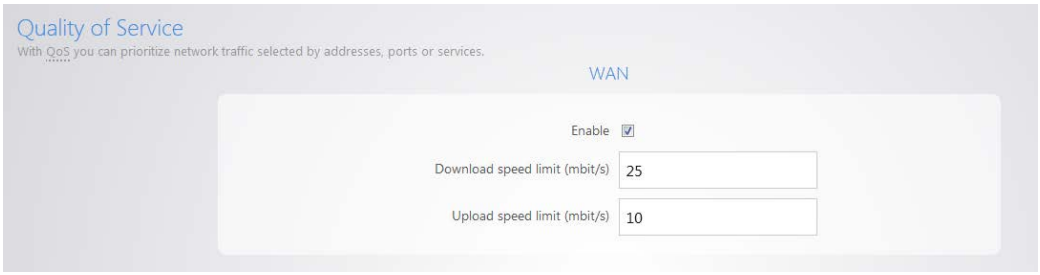
Quality of Service (QoS) allows you to prioritize data on the network. For example, there are certain applications which require the least amount of latency possible. You can prioritize this type of traffic so that it is sent ahead of other data that can function properly with some latency, such as ordinary web traffic.

To configure QoS:

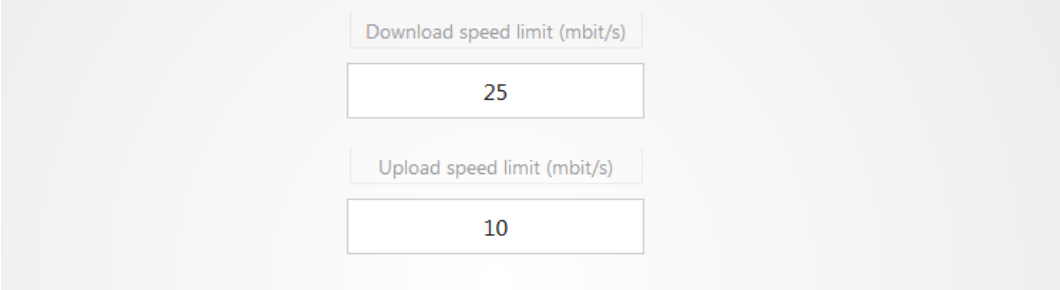
1. Click **Quality of Service**.



2. Check **Enable**.

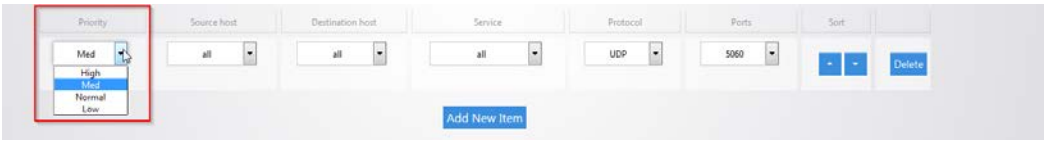


You can restrict download and upload speeds on this page. For example, in the following image we have set 25 Mbps as the limit for download and 10 Mbps as the limit for upload speeds. This setting will apply to all devices on the network.



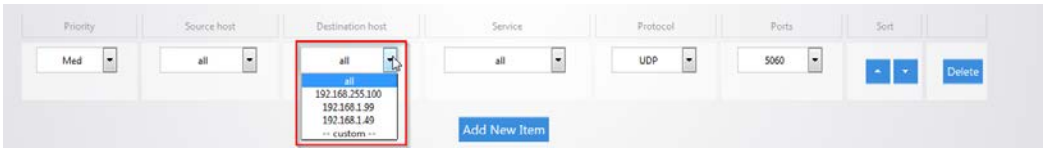
3. If you want to create a new QoS policy to prioritize certain data, click **Add New Item**.

4. The **Priority** column allows you to select the priority of the data

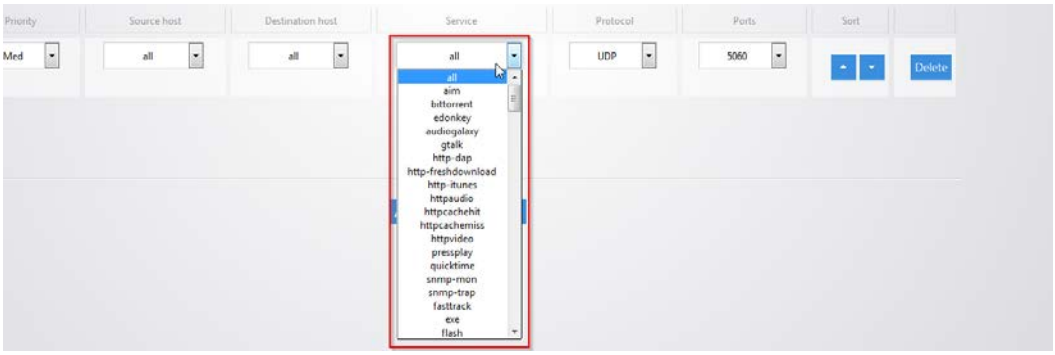


5. The **Source host** column allows you to define which source IP address the policy will apply to. If you select **all,** the policy will apply to all devices on the network. If your device is listed in the drop down menu you can select it, otherwise select **custom** and manually enter the IP address.

6. The **Destination host** column allows you to define which IP destination address the policy will apply to. If you select **all** then the policy will apply to any IP address on the Internet.

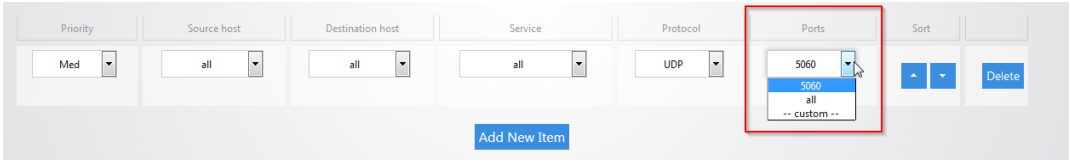


7. The **Service** column has a list of common applications that you may want to prioritize. If the application you are looking for is on the list you can select it as the service to prioritize.

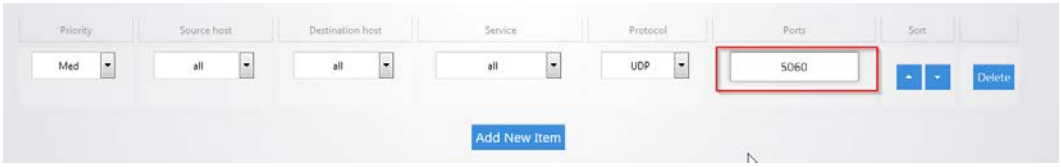


8. The **Protocol** column allows you to select whether the data that you are prioritizing is TCP or UDP. If you are unsure you can simply select all which will use both.

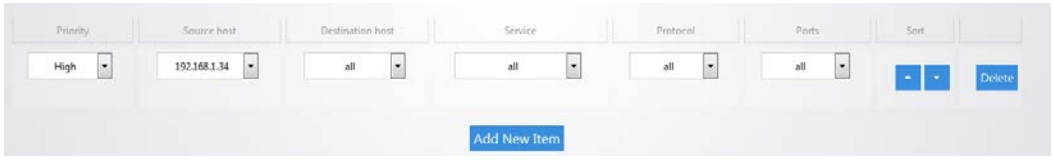
9. The **Ports** column allows you to select which ports the data you are prioritizing uses. Click the drop down menu and select **custom**.



10. You can then fill in the port number that your application uses.



11. For example, we will prioritize the data of a computer on the network. For the **priority** select **High**. Enter **192.168.1.34** as the IP address of the computer for **the source host**. For the **destination host** select **all**, this will ensure that the policy will apply no matter what destination on the Internet the computer goes to. For **service** select **all**, **protocol** will also be set to **all**. This means the policy will apply to TCP and UDP data. **Ports** is also set to **all.**



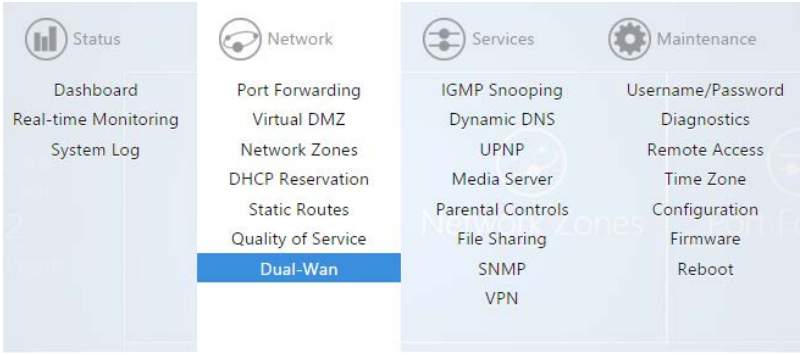
12. Click **Apply** to finalize the settings.
13. By default there is a rule defined to allow priority of Voice Over IP (**VOIP**) data.

Dual Wan

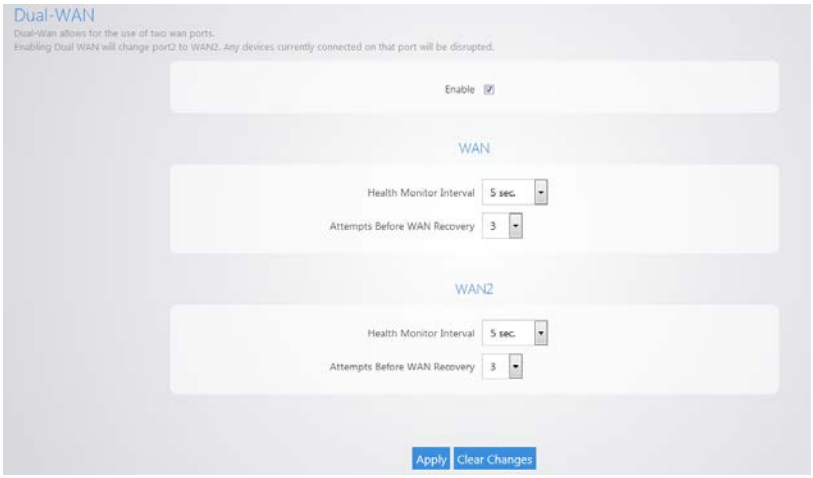
Dual Wan allows you to use two wan ports on the router in redundancy mode. If WAN1 loses Internet access WAN2 will take over.

To configure Dual Wan:

1. Click **Dual Wan**.



2. Select **Enable**. WAN1 will now check connectivity every 5 seconds to make sure that it is still up and running. When WAN1 is no longer able to get onto the Internet it will switch over to WAN2. After the router detects that WAN1 is back up it will switch back to WAN1.



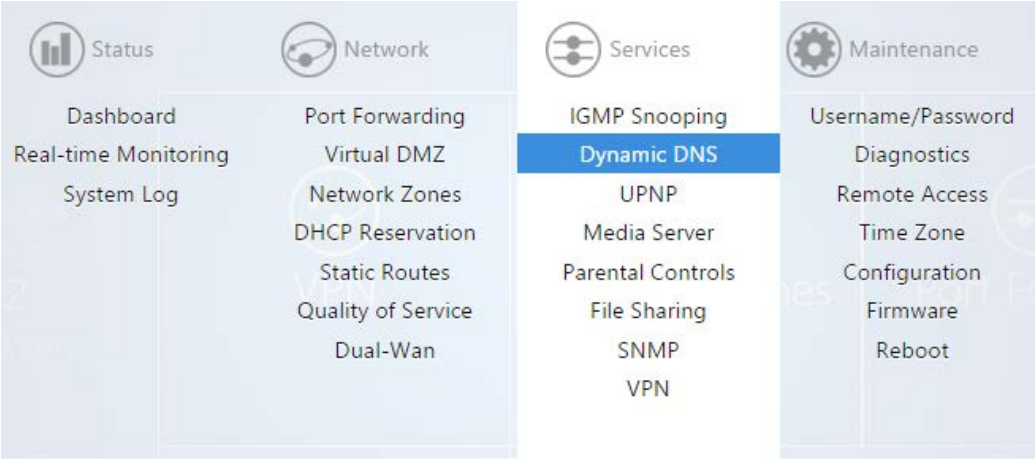
3. Click **Apply** to finalize the settings.

Dynamic DNS

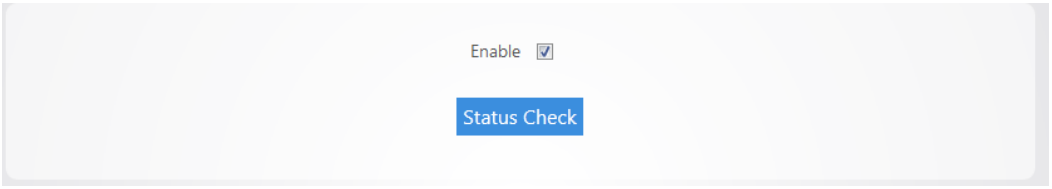
Dynamic DNS (**DDNS**) allows your router to be reached with a fixed hostname while having a dynamically changing IP address. The router has two options for DDNS. The first is under the **Pakedge DDNS** tab. Pakedge offers its own DDNS service that works alongside our BakPak cloud system.

To create a Pakedge DDNS:

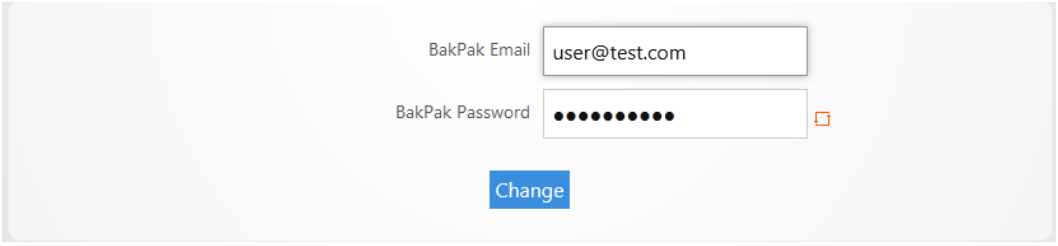
1. Click **Dynamic DNS**.



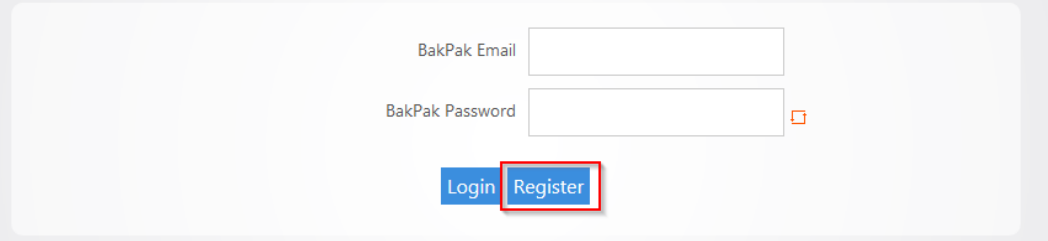
2. Under the Pakedge DDNS tab, check **Enable**.



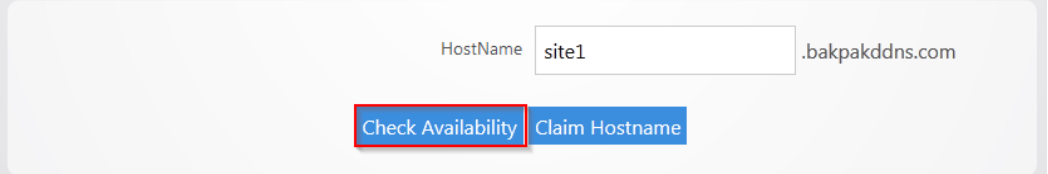
3. If you have an existing BakPak account, simply enter your credentials and click **login**.



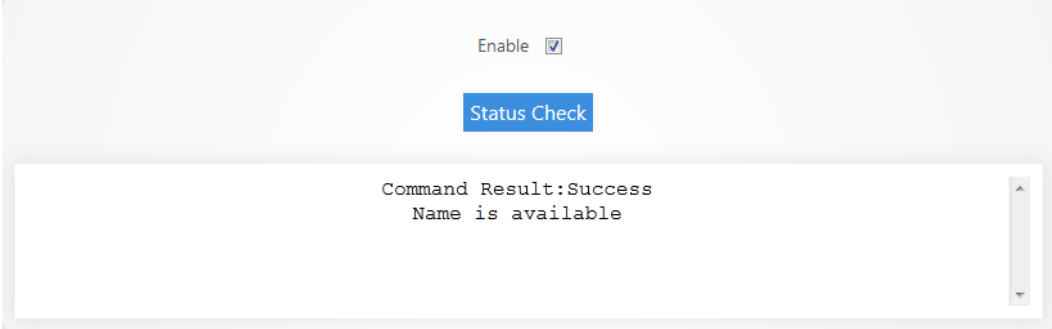
4. If you don't have a BakPak account, you can register for an account to use. Simply enter an email address and password and click **register**.



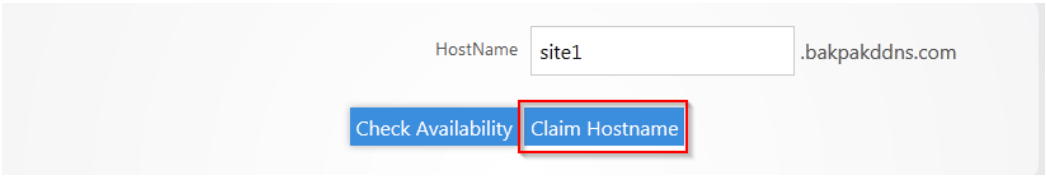
5. After you are logged in with your BakPak credentials, scroll down to the **HostName** field. Pakedge DDNS uses the *name*.BakPakddns.com namespace, where *name* is a name you choose. Enter a name you would like to use and click **Check Availability** to have the router check if that name is available. In the following example we will check to see if **site1.BakPakddns.com** is available.



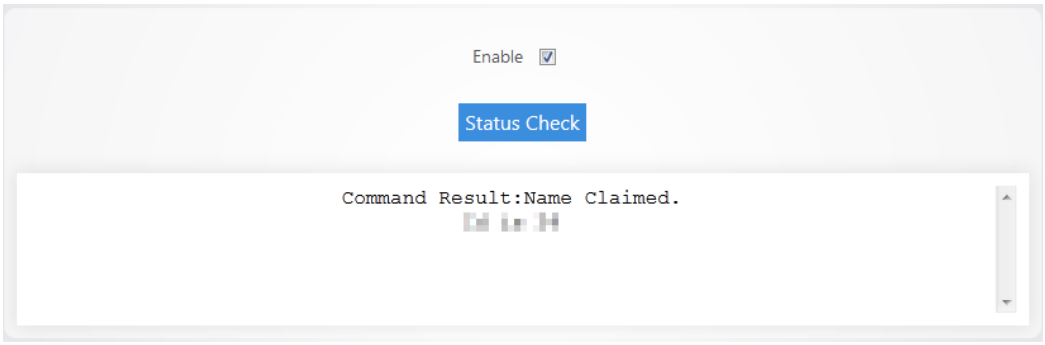
6. After you click **Check Availability**, scroll towards the top to see if your name is available. Here we can see that the name we choose is available for use.



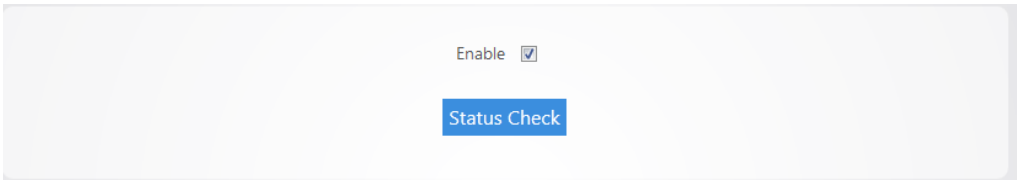
7. Now that we know the name we want is available we can click **Claim Hostname**.



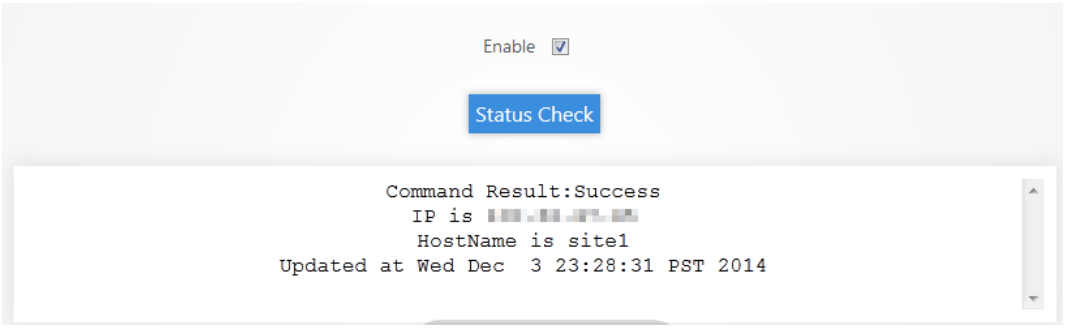
8. Scroll towards the top and you will see a message stating that you have claimed your name. The router is now using the name we have claimed.



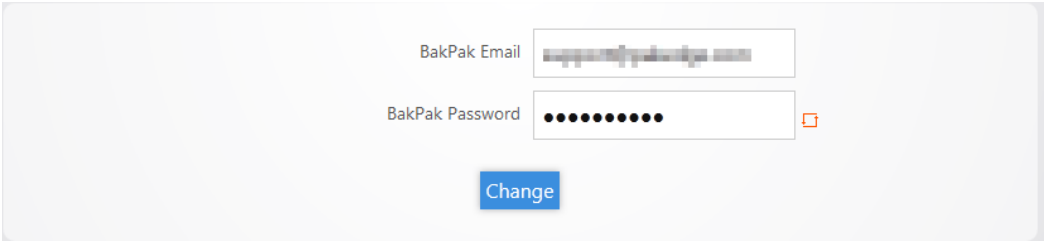
9. You can click **Status Check** to see the status of your Pakedge DDNS.



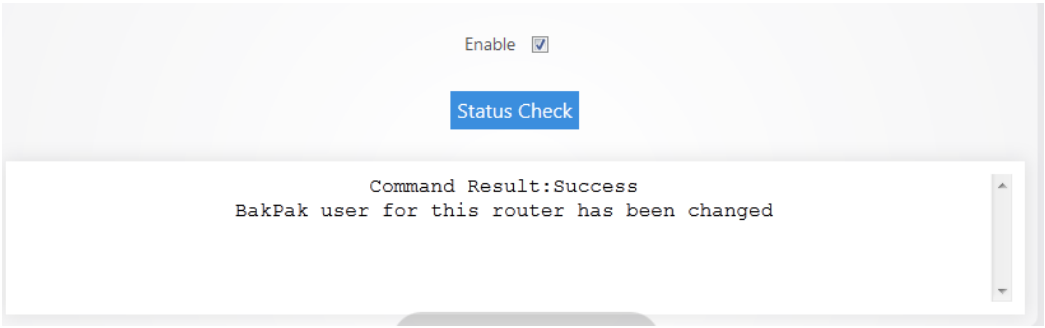
The router displays the status of the Pakedge DDNS giving you the hostname that the router is currently using.



10. You can change the hostname you are using at any given time by simply entering a new hostname into the router that is available for use and then clicking claim **hostname**.
11. You can change the BakPak user on the router at any given time by simply entering the new credentials and clicking **Change**.



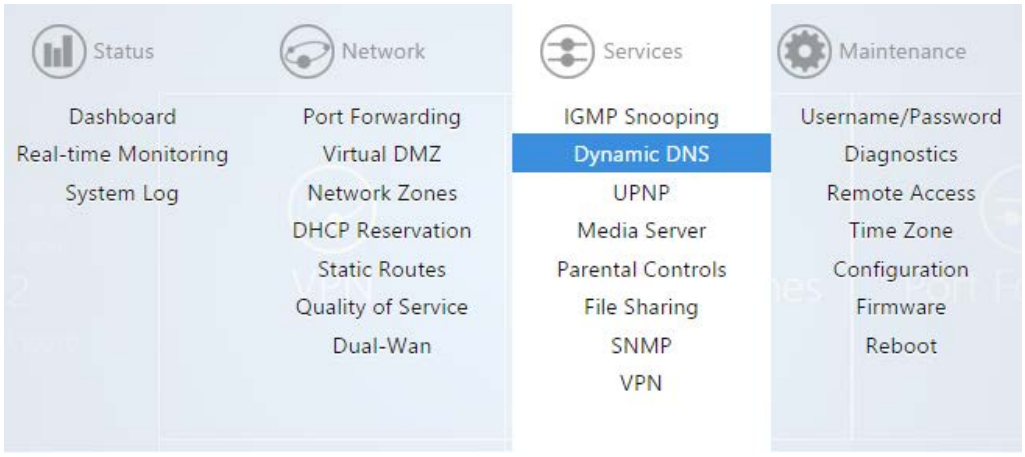
You will see a message towards the top letting you know that the BakPak user has been changed.



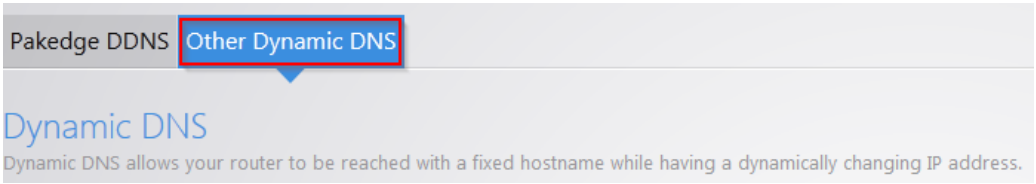
Note: You can only register for a new BakPak user once on the router. After you have registered for a BakPak user once, the register button will disappear from the GUI.

To configure a non-Pakedge DDNS:

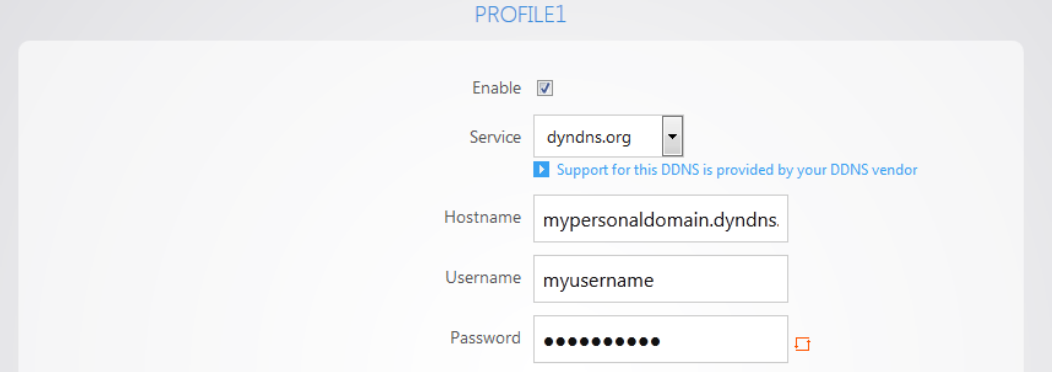
1. Click **Dynamic DNS**.



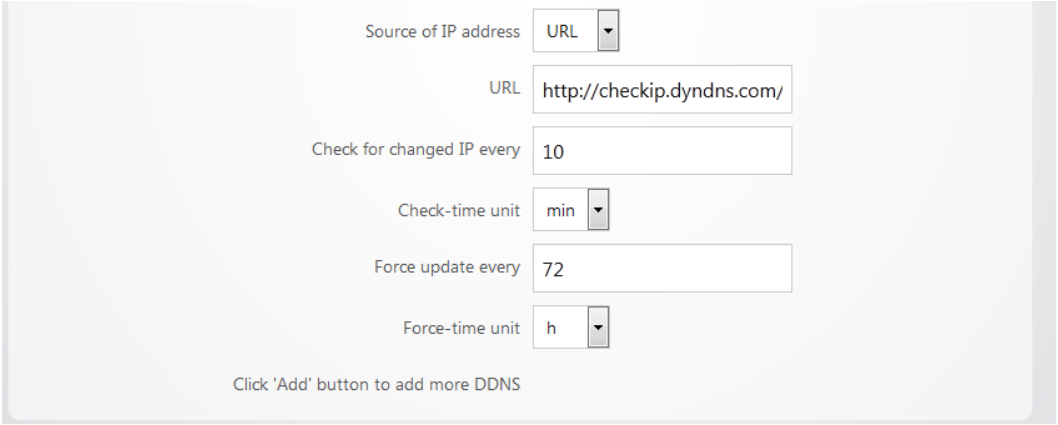
2. Click **Other Dynamic DNS**.



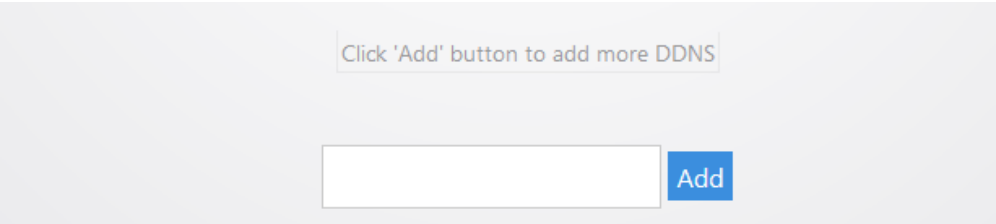
3. Select Enable. For the **Service** drop down menu, select your DDNS provider. For the **Hostname**, enter the full domain name that you signed up for. In the **Username** field enter the username for your account with your DDNS provider. For the **Password** field, enter the password for your account.



4. For the **Source of IP address** field select **Zone**. For the **Zone** field select **WAN**. The **Check for change IP every** field indicates how often the router will check to see if the WAN IP address has changed. The **Check-time unit** indicates the unit of time that is used for the **Check for changed IP every** field. The **Force update every** field indicates when the router will force an update with the DDNS provider. **The Force-time unit** indicates the unit of time that is used for the **Force update every** field. Click **Apply**.



5. You can add a secondary DDNS profile to the router. In case the first DDNS provider does not work the secondary profile can act as a backup. To add a secondary profile simply click **Add** and fill out the information as you did in steps 2 and 3.

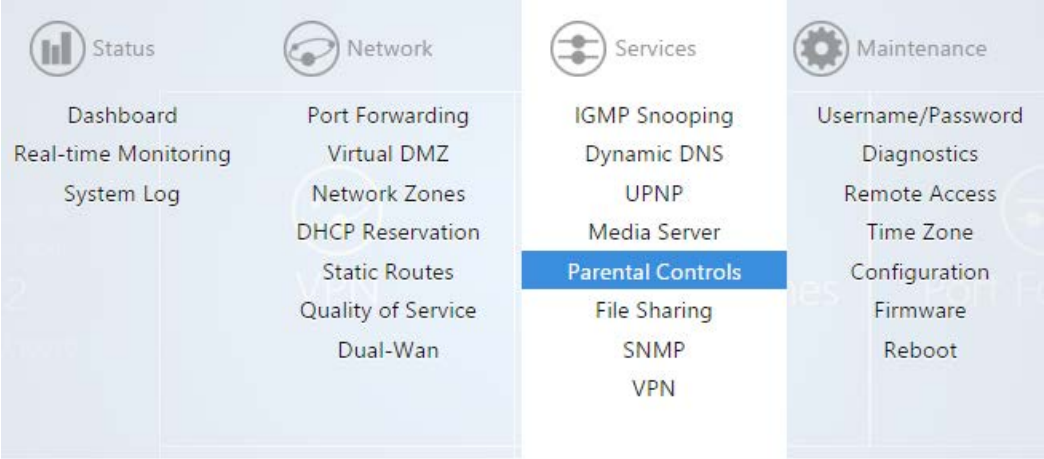


Parental controls

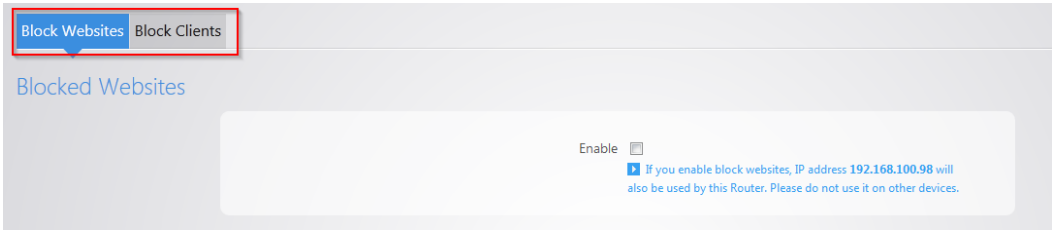
The **Parental Controls** allow you to block websites and services on your network. For example, you can prevent users from visiting www.yahoo.com or prevent any http traffic from going out to the Internet.

To configure the parental controls:

1. From the **Services** menu, click **Parental Controls**.



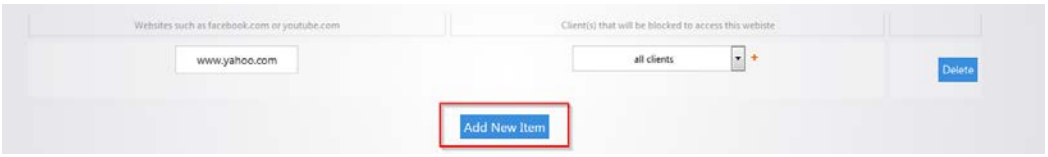
2. You will see two tabs on this page. One is **Block Websites** and the other is **Block Clients**.



3. To block a website from being accessed on the network, select the enable box under the **Block Websites** tab and then click **Add New Item**.

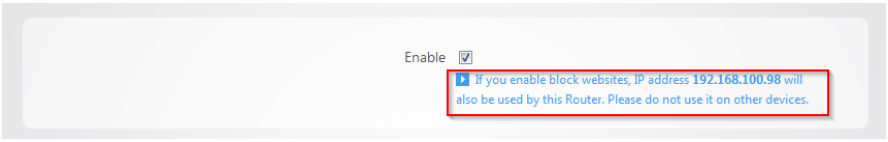
4. Enter the name of the website that you wish to block. In this example, we will block www.yahoo.com. Towards the right hand side you can select the device that you want to block the website for. You can select **all clients** to allow it for every device on the network.

5. You can continue adding websites by clicking on **Add New Item**.



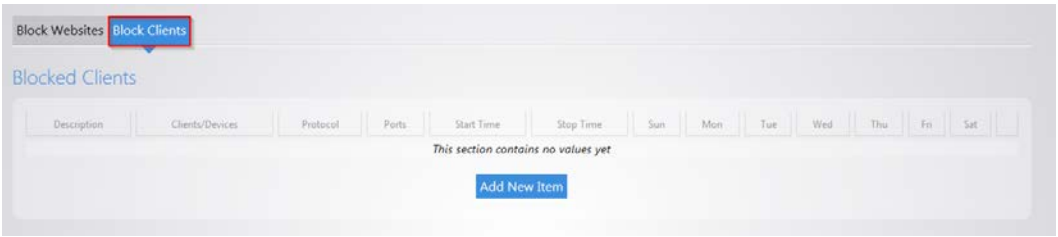
6. Click **Apply** when you are finished. The websites you entered will now be blocked.

7. If you use the Block Websites feature the router will also need to use a secondary IP address on the network. There is a message on the Block Websites page to warn you about this. Ensure that the IP address listed is not in use by any other device on the network. This secondary IP is only used for the Block Websites feature; the management GUI of the router remains unchanged.

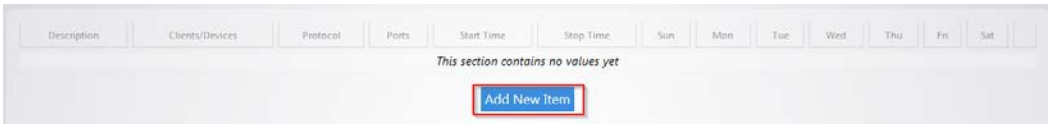


Note: After you have blocked a website on the router, you must clear the DNS cache on any devices on the network. You can do this by rebooting the devices.

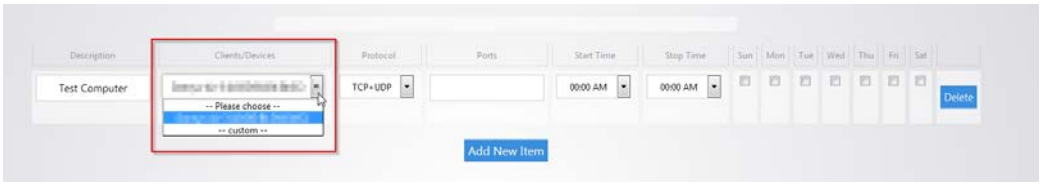
8. The Block Clients feature will allow you want to block certain services from accessing the Internet. Click **Block Clients**.



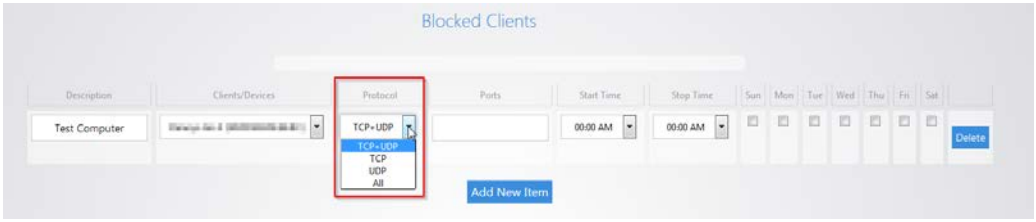
9. Click **Add New Item** in the bottom box.



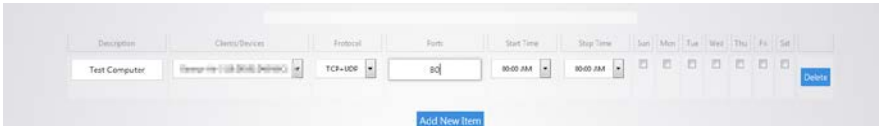
10. Enter a name in the **description** field.
11. For the **Clients/Devices**, hit the drop down menu and you will see a list of devices that the router has discovered on the network. If the device you want to apply to this policy to is listed, you can select it here. Otherwise, click **custom** and then you will be able to manually enter the IP address of the device.



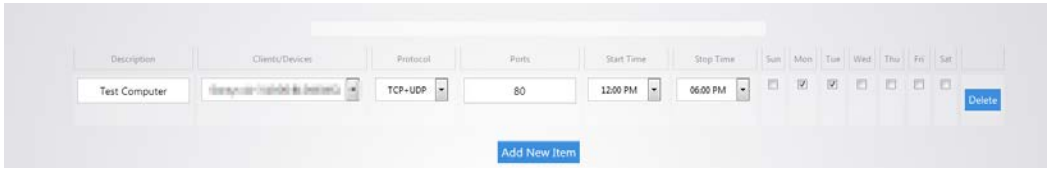
12. The **Protocol** field allows you to select whether you want to block TCP, UDP or both for this policy.



13. The **Ports** field allows you to specify which port you wish to block from going out to the Internet. For example, you can type in port 80 and that would deny any traffic that is using that port from going out to the Internet.



14. You can also apply a schedule to this policy. You can set the start time and stop time. You can also select which days you wish the policy to apply on. Click **Apply** towards the bottom to finalize the settings.



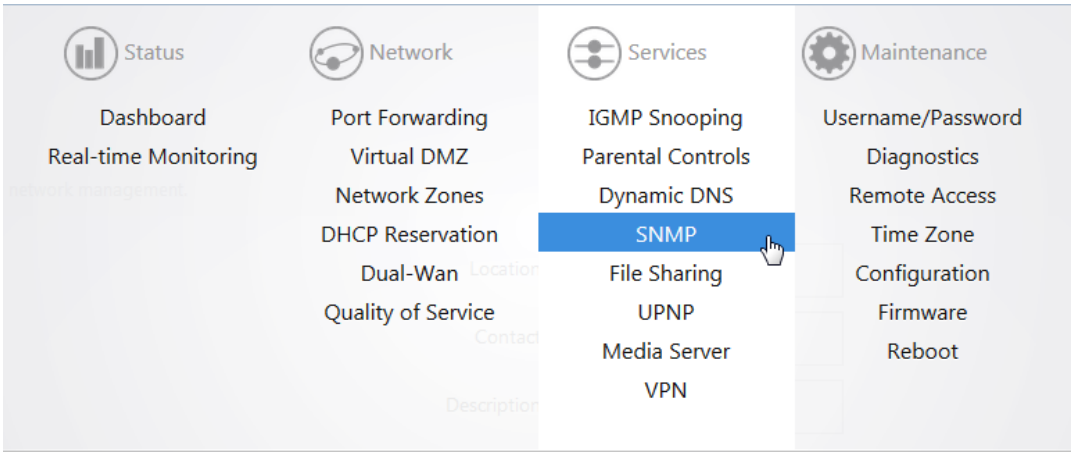
15. You can block a device from completely accessing the Internet. To do this, set the **Protocol** to **All** and leave the **Ports** field blank.

SNMP

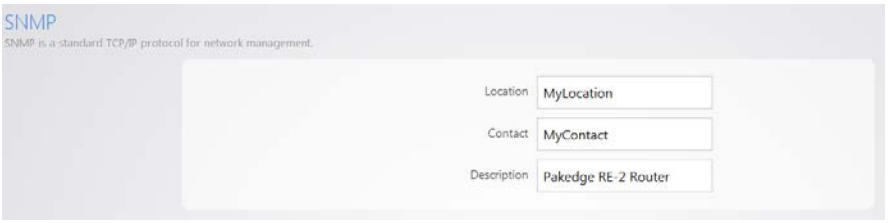
Simple Network Management Protocol (**SNMP**) is a standard protocol for network management. By default it is enabled on the router.

To view the SNMP settings:

1. Click **SNMP**.



2. On this page you will see all of the SNMP options. If you make any changes be sure to click **Apply**.

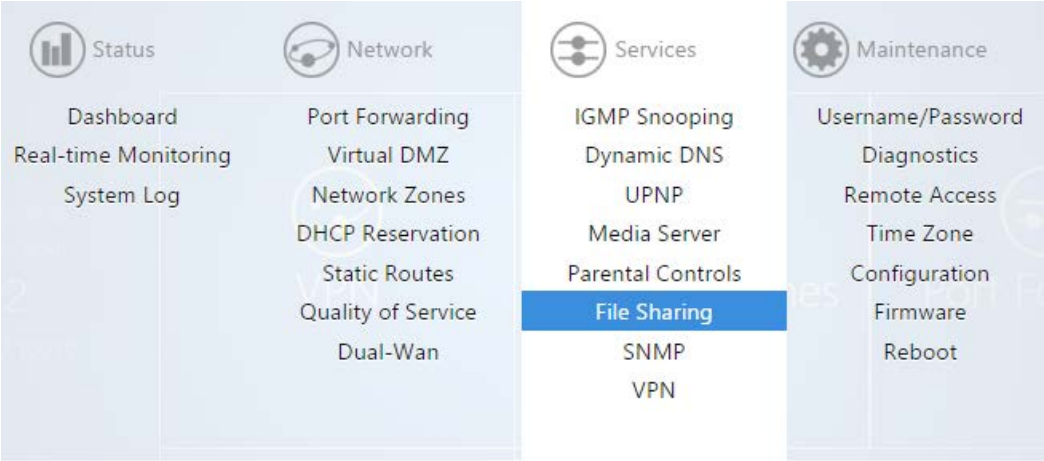


File Sharing

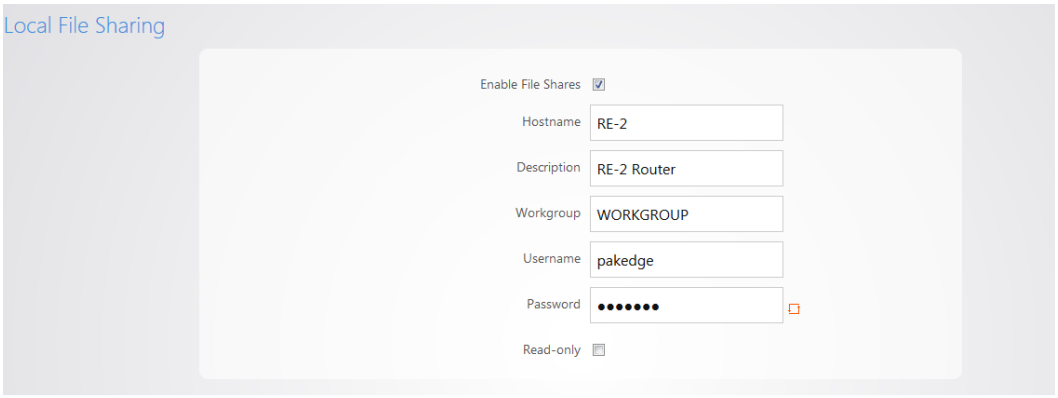
File sharing allows you to connect a USB drive onto the router and share resources. The router offers both Local and Remote file sharing. **Local File Sharing** allows you to share the contents of a USB drive on the local network.

To configure local file sharing:

1. Click **File Sharing**.



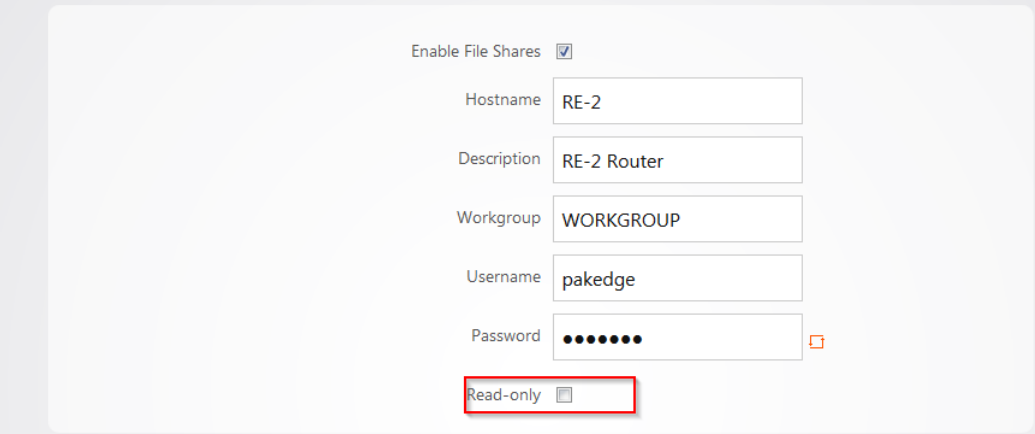
2. Under the **Local File Sharing** tab, select the enable checkbox. Click **Apply**.



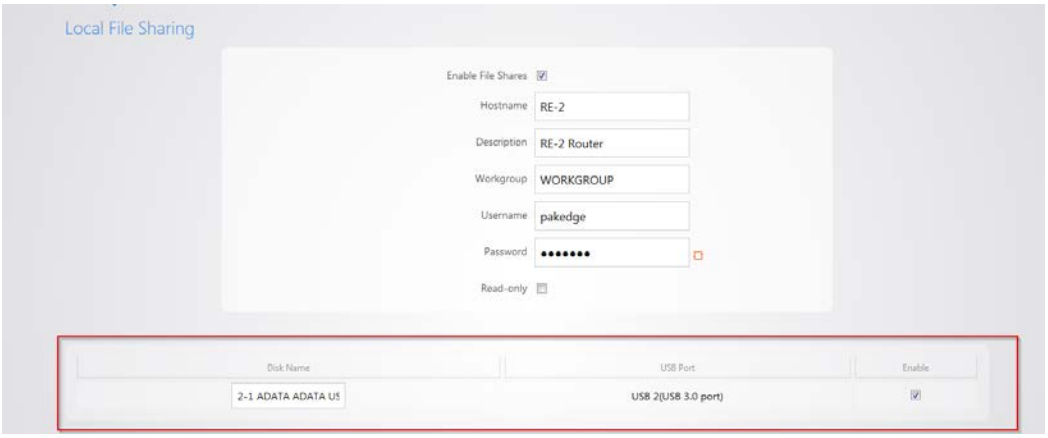
You can now access the USB drive over the local network.

3. You will be prompted to enter a username and password when attempting to access the USB drive. By default the username is **pakedge** and the password is also **pakedge**.

4. You can check the **Read-only** box so that computers on the network will only be able to read from the drive and not write to it.



5. After you have enabled the file sharing and connected a USB drive into the router, you will see your drive listed in the file shares menu.



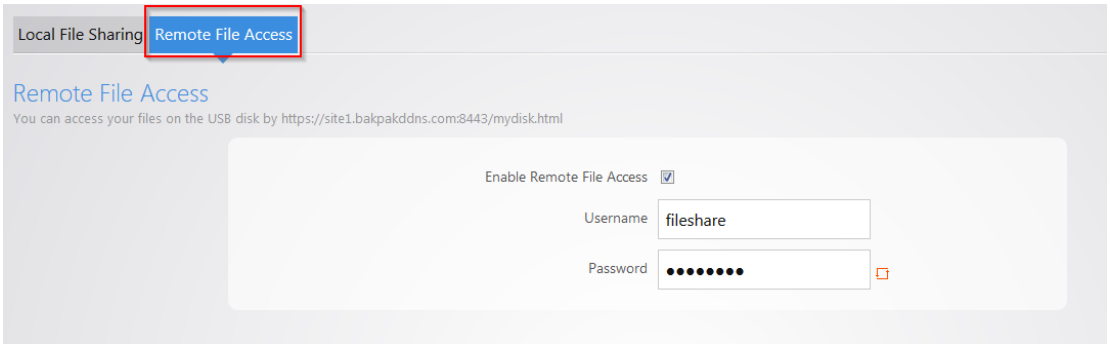
6. You can rename the **Disk Name**. Doing this can make mapping the USB drive on a computer easier.

7. Click **Apply** to finalize the settings.

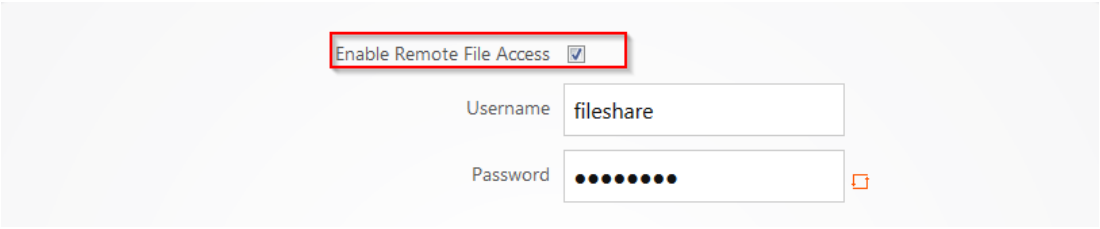
Remote File Sharing allows you to access the contents of your USB drive remotely.

To set up remote file sharing:

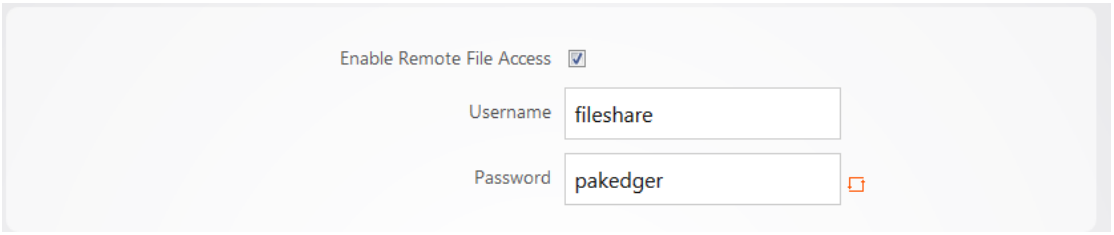
1. Click the **Remote File Access** tab.



2. Select **Enable**.



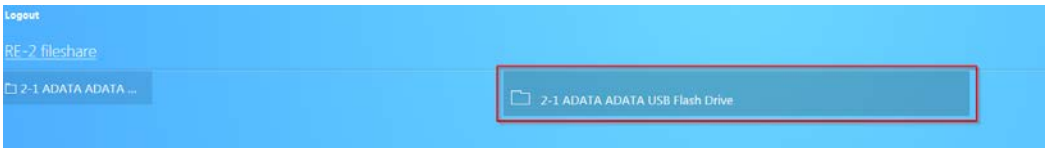
3. The default **username/password** for remote file access will be **fileshare/pakedger** Note: You can change the username and password used to remotely access the USB drive. Simply enter the new credentials and click **Apply**.



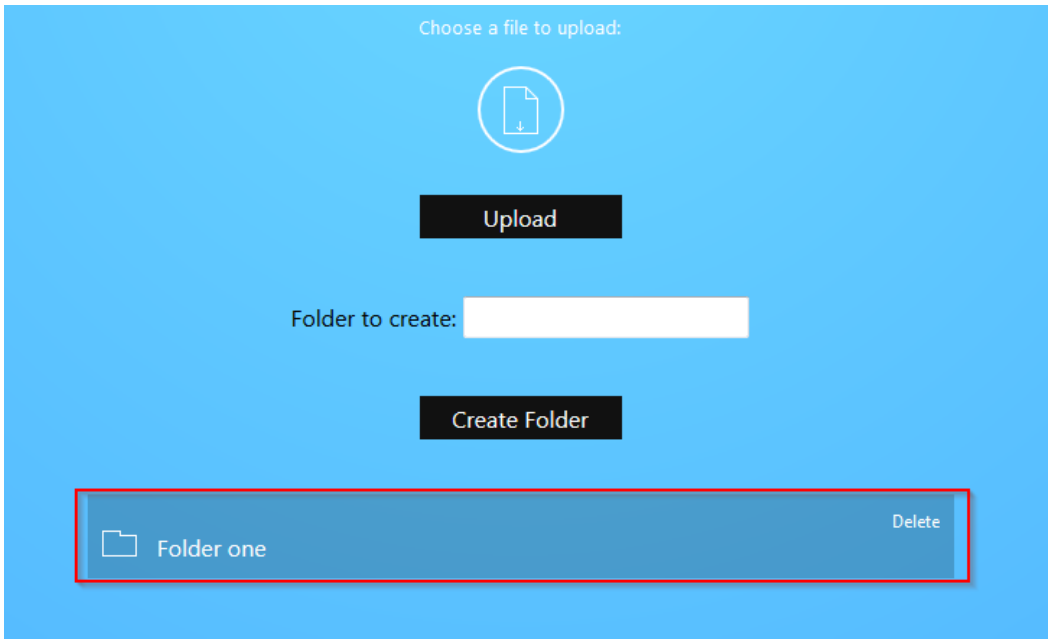
4. Click **Apply** to finalize the settings.
5. To remotely access the USB drive enter the following into a web browser https://PublicIPaddress:8443/mydisk.html and press enter. Note: if you configured DDNS on the router you can use that in place of the public IP address.

6. You will see a login screen similar to when you log into the router. Enter the credentials and click **Login**.

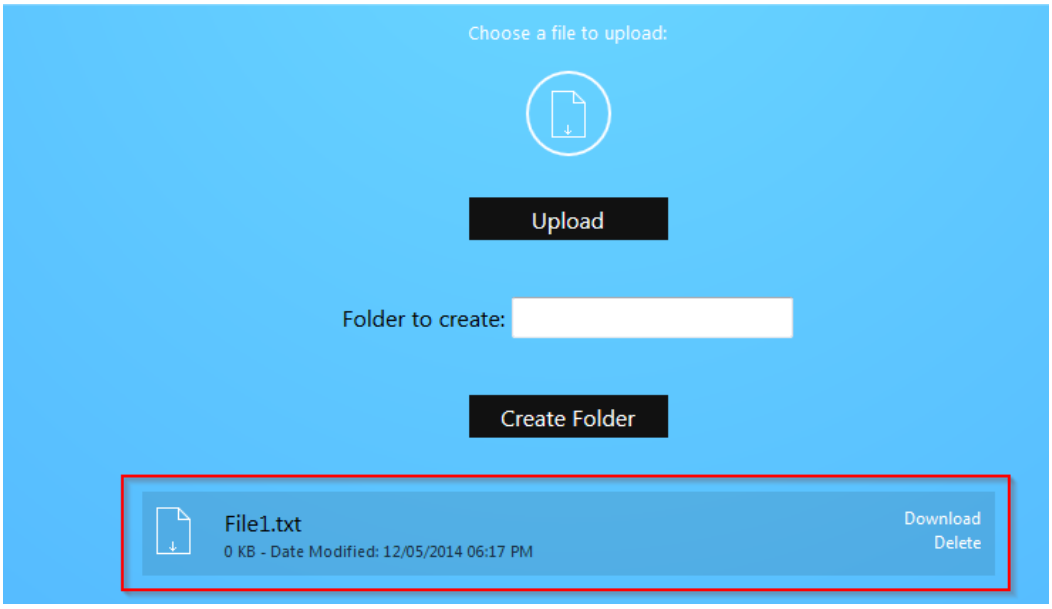
You will see the USB drive listed.



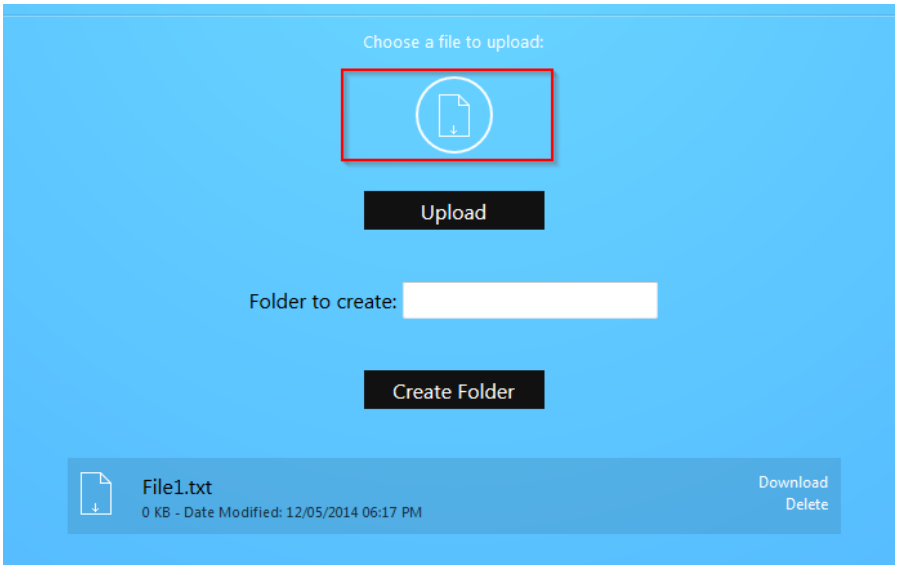
7. You can click the USB drive to view the files and folders inside of it. Click a folder to view the contents of it. In our example, we will click a folder titled **Folder one**.



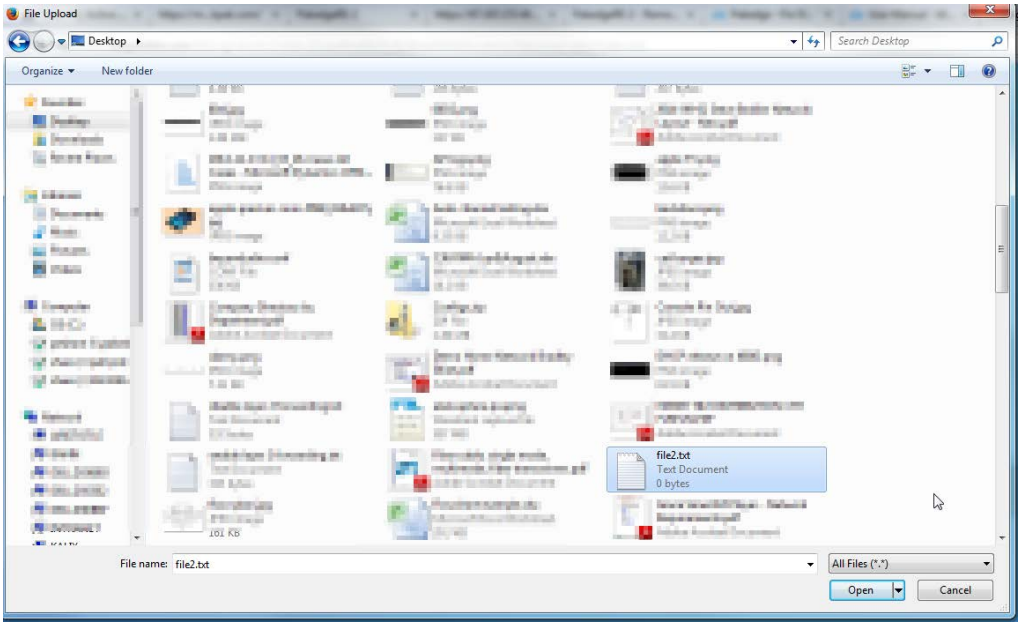
8. You will see the contents of the folder displayed. In this example, we have a single file named **File1**.



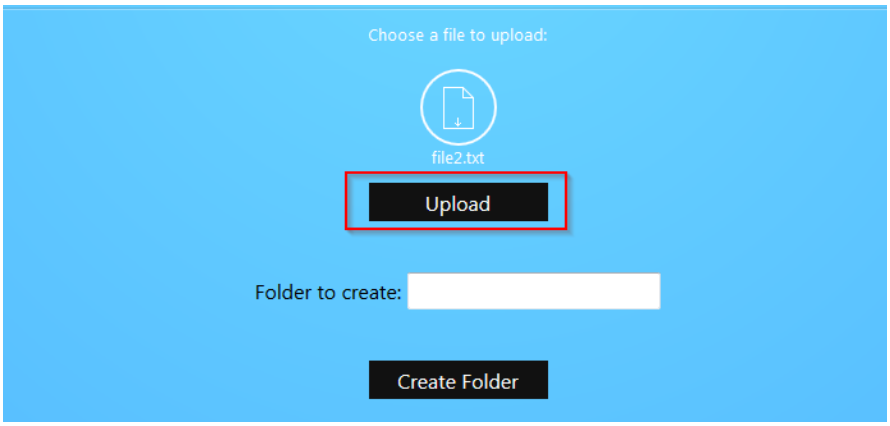
9. Click **Download** to retrieve the file from the USB drive. You can also click **Delete** to remove it.
10. You can upload a file onto the USB drive remotely. Click the file upload icon.



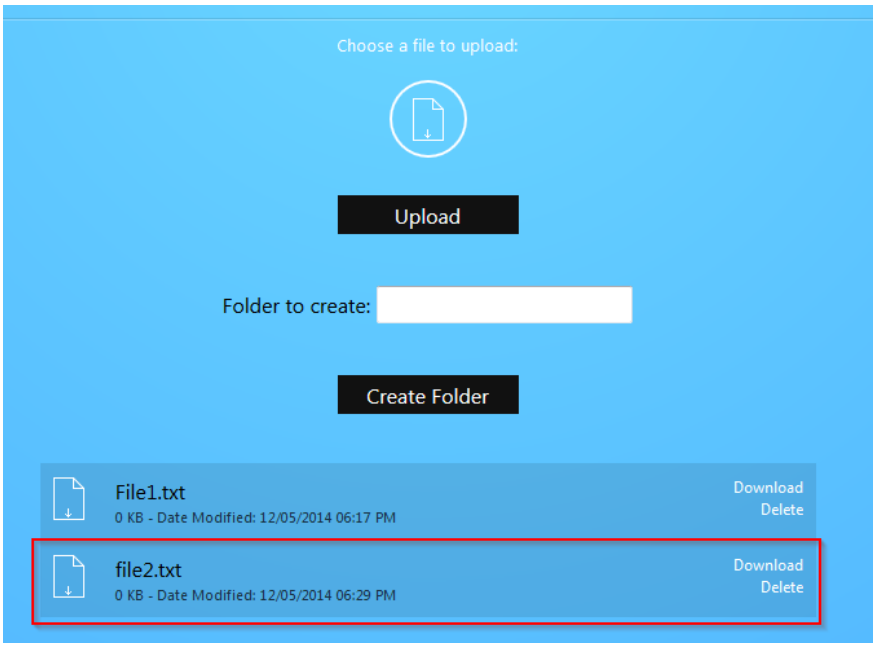
11. Navigate to the file you want to upload and select it.



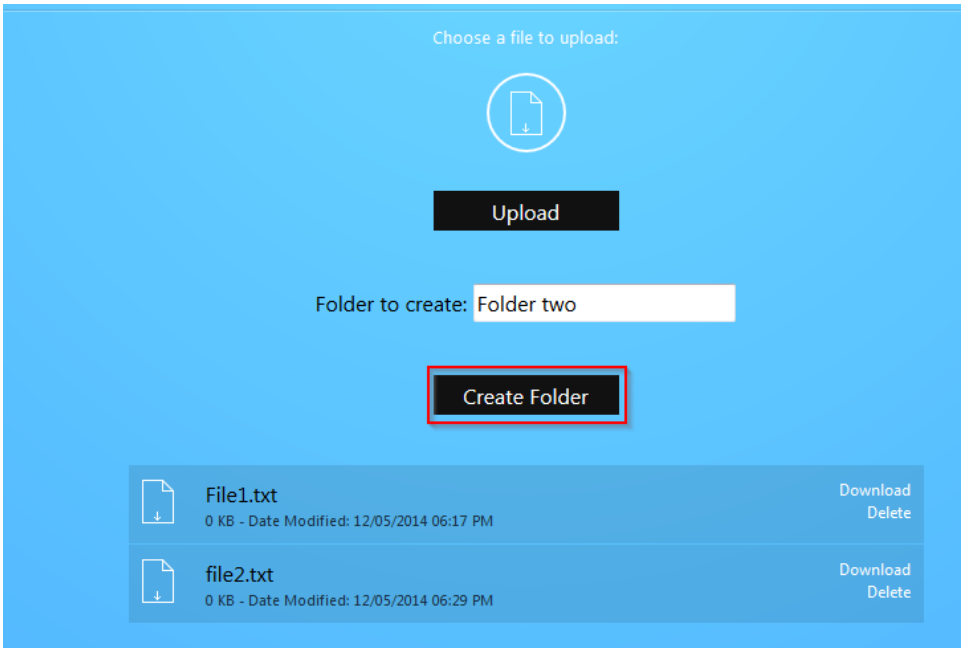
12. Click **Upload**.



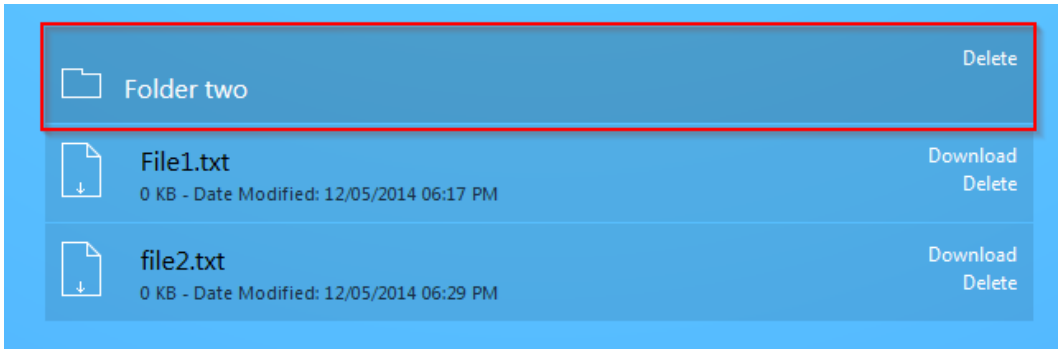
Your file will now be on the USB drive.



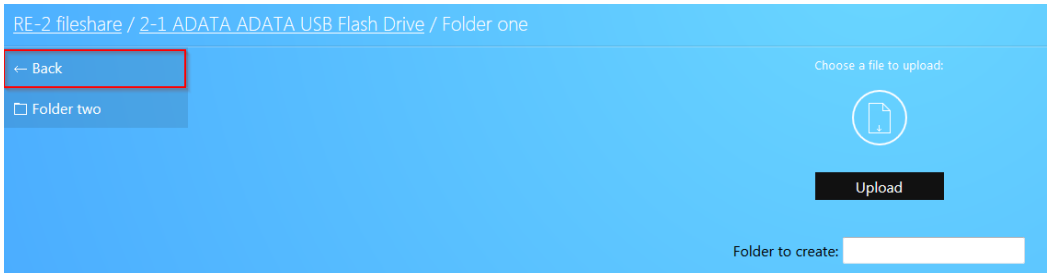
13. You can create folders, as well. Simply enter the folder name and click **Create Folder**. As an example, we will create a folder titled **Folder two**.



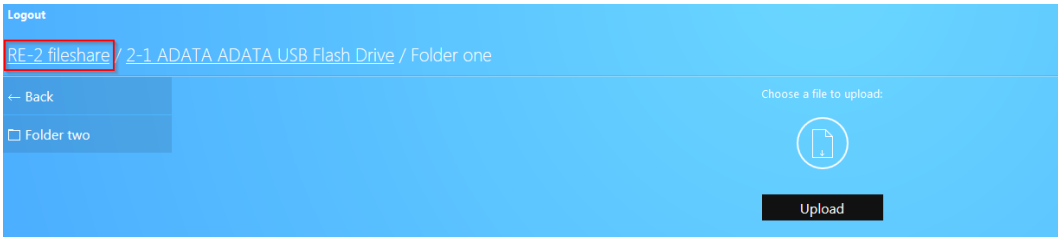
14. The folder will now be displayed.



15. To return to the previous directory, click the **Back** button.



16. Click **[model#] fileshare** to return to the root of the USB drive.



17. Finally, click **Logout** to log out of the file share.

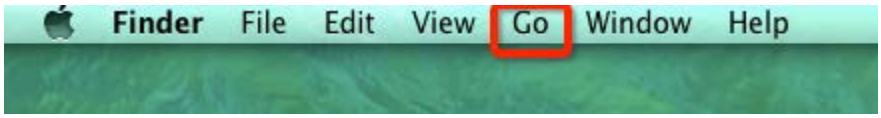
Mapping network drives

The following section will show you how to map the USB drive on the router on various operating systems.

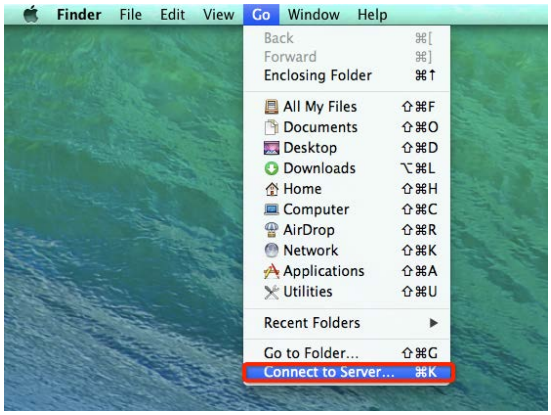
Mac OS X

To map the USB drive on Mac OS X:

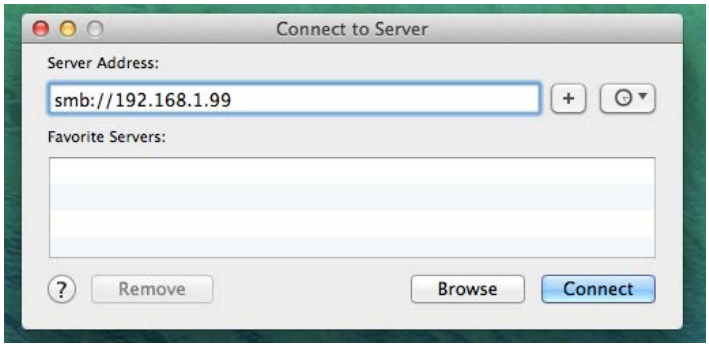
1. Click **Go** at the upper left.



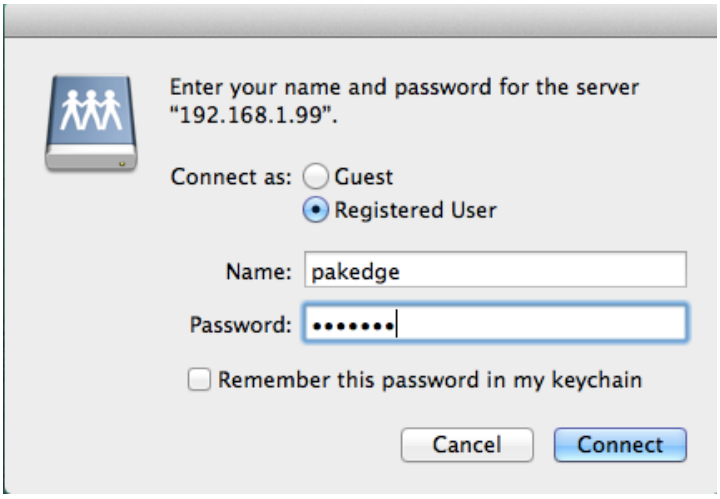
2. Click **Connect to Server**.



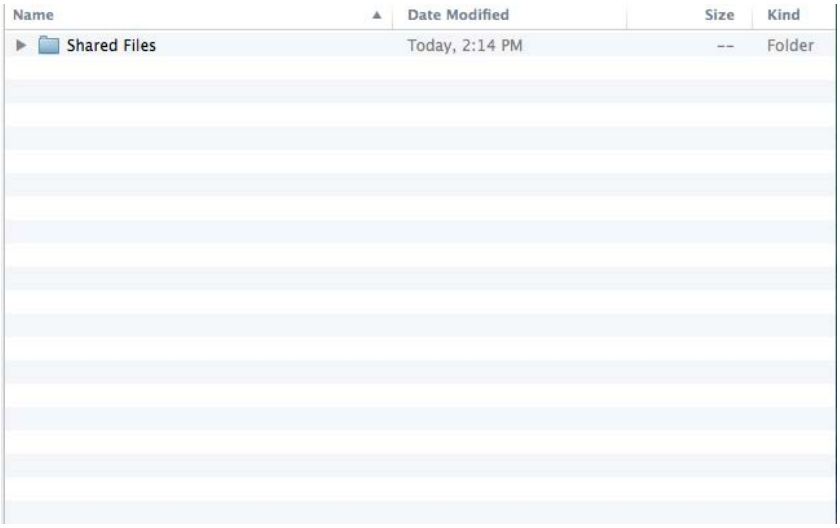
3. In the **server address field**, enter **SMB://IP address of your router**. The following image shows an example of this. Click **Connect**.



4. You will be prompted to login as a **guest** or **registered user**. Select **registered user**. In the username and password field enter the credentials you have configured on the router.



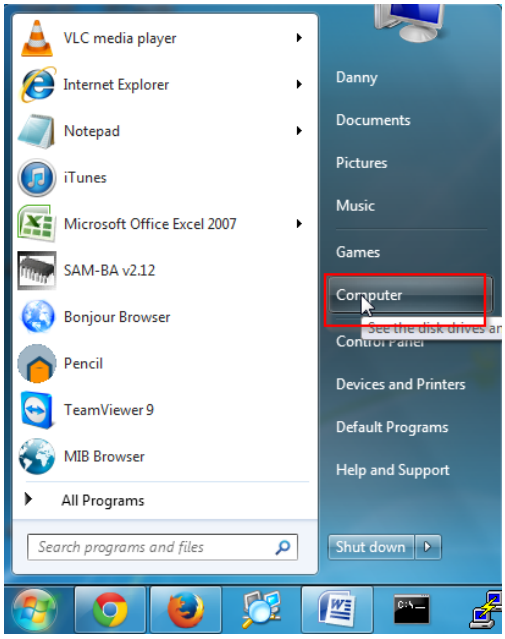
5. The USB drive will now be mapped on your computer and you will be able to access files on that drive.



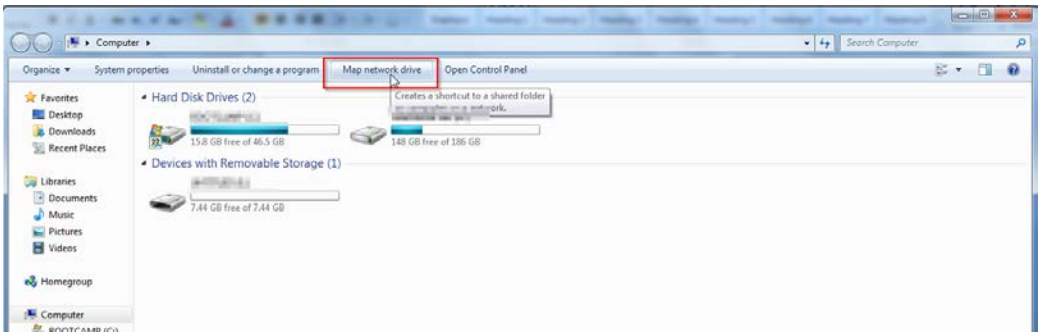
Windows 7

To map the USB drive on the device in Windows 7:

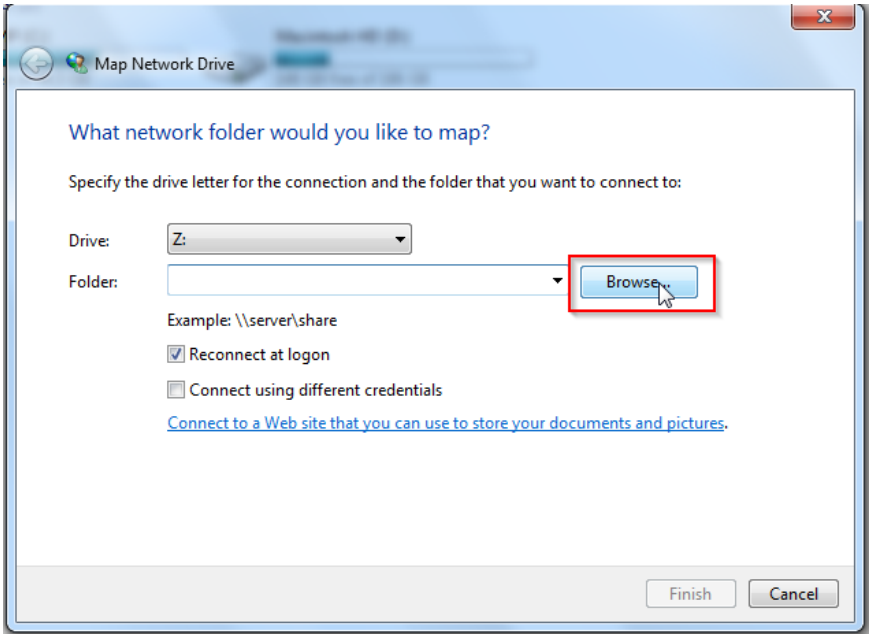
1. Click the start button at the bottom left hand side. Click **Computer**.



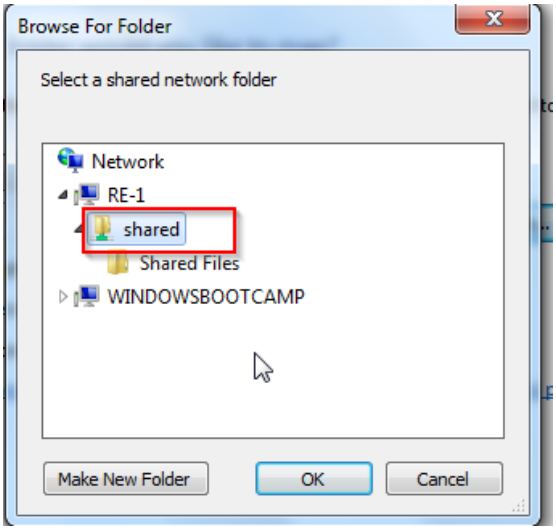
2. Click **Map Network Drive**.



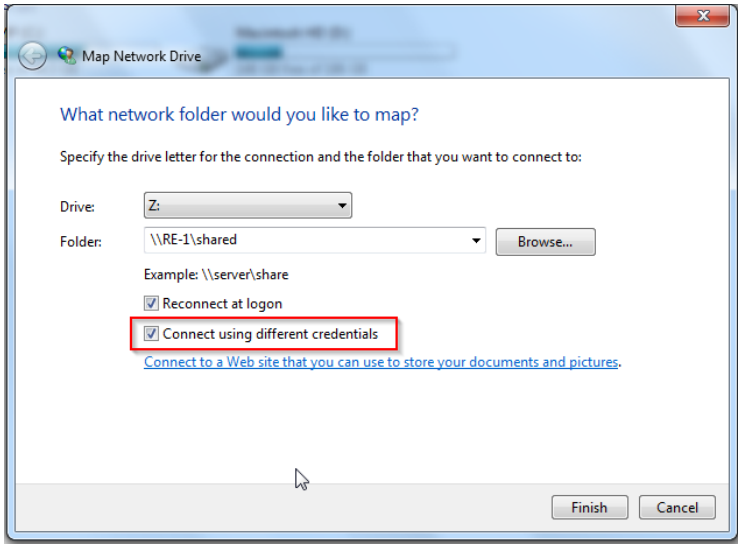
3. Click **Browse**.



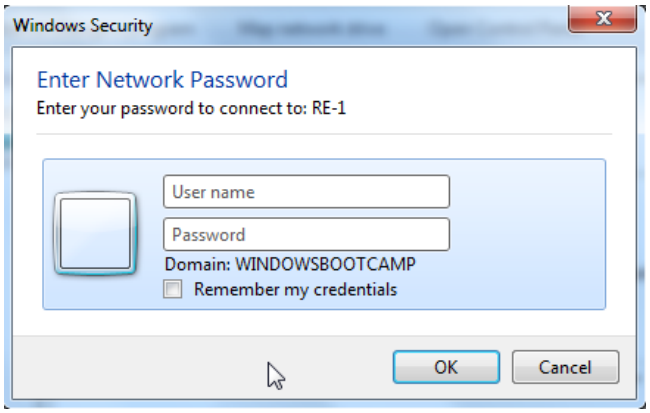
4. Click **RK-1/RE-1/RE-2** to expand it. Click the folder you want to map underneath it to select it. Click **OK**.



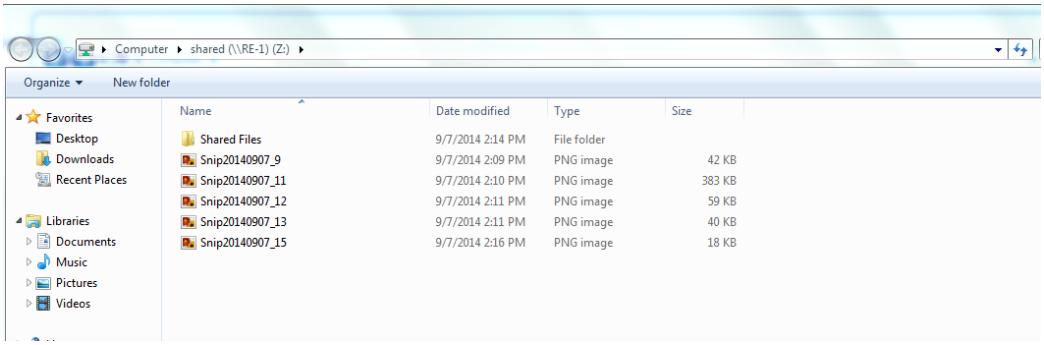
5. Check the box titled **Connect using different credentials**, then click **Finish**.



6. Enter the username and password to access the folder. Click **OK**.



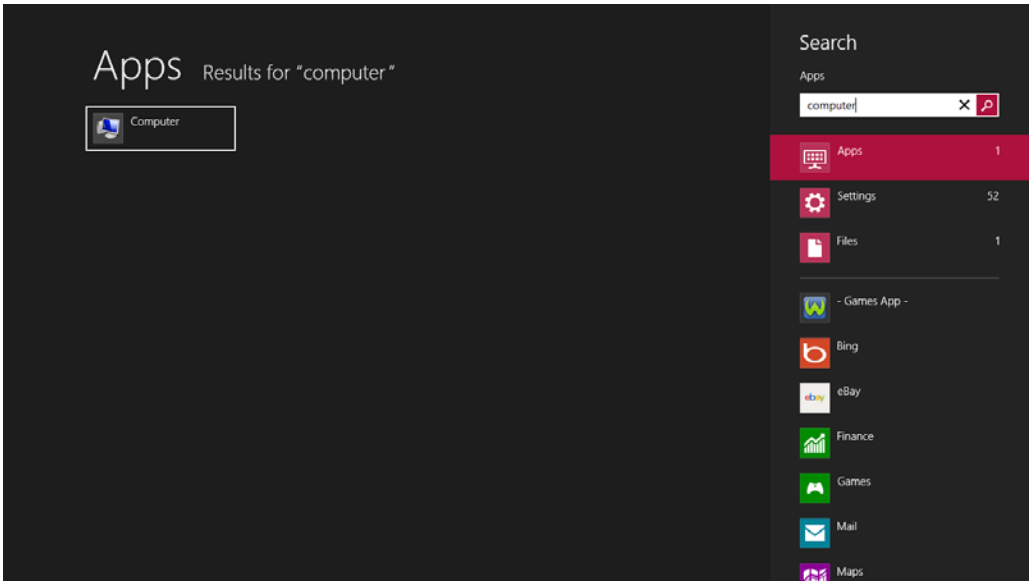
7. You will now have access to the files on the USB drive.



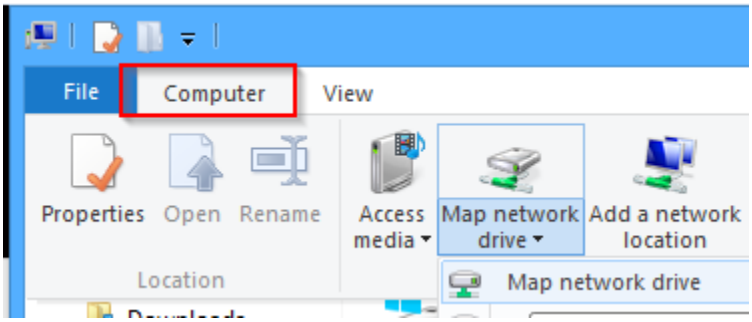
Windows 8/10

To map the USB drive on the device for Windows 8:

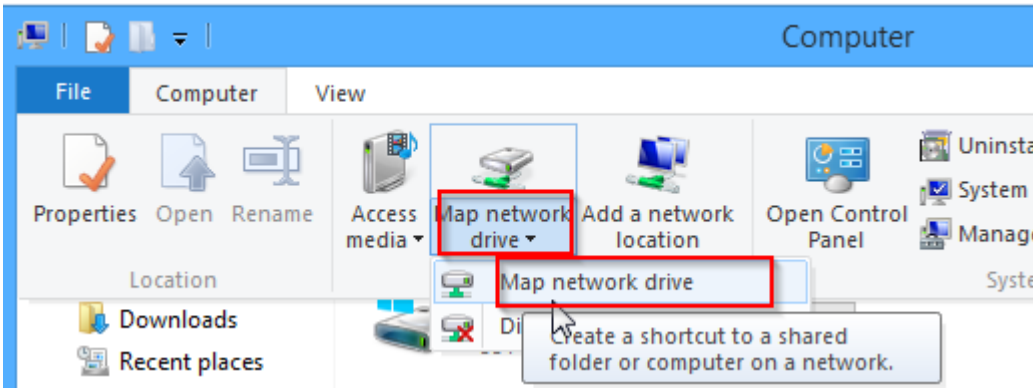
1. Press the windows button on your computer. Type **computer** and press enter.



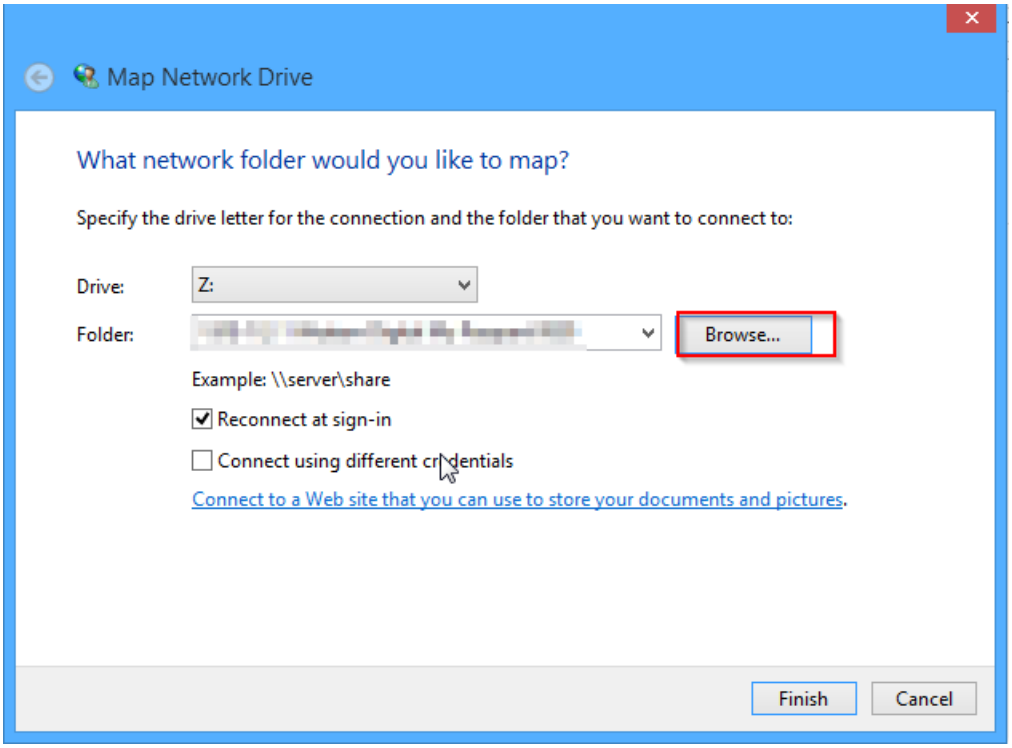
2. Click **Computer** towards the top.



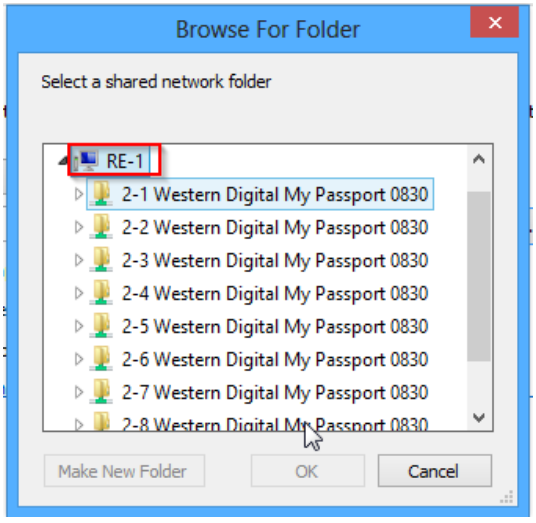
3. Click **Map network drive**.



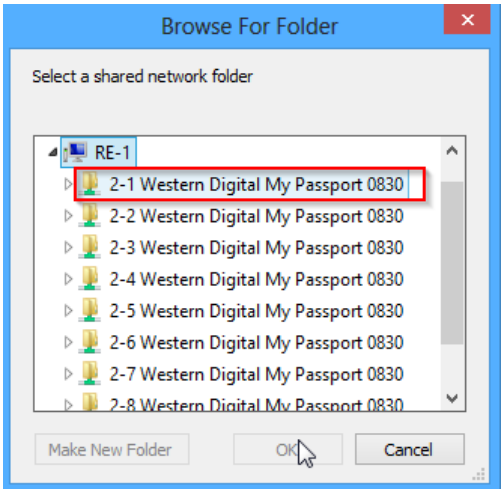
4. Click **Browse**.



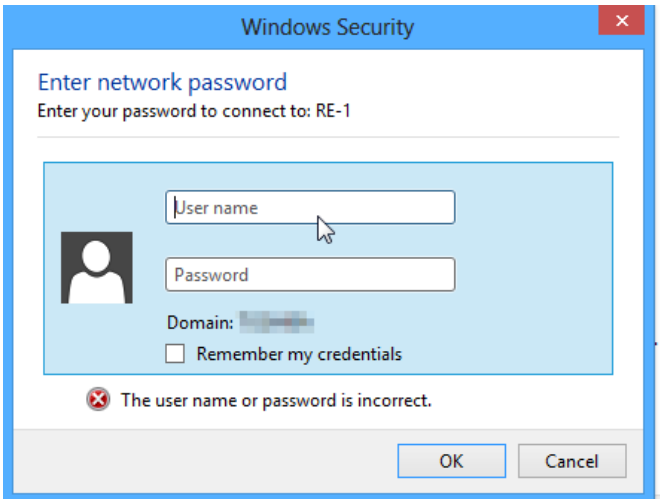
5. You will see the router listed. You will also see all of the folders on the USB drive connected to the router.



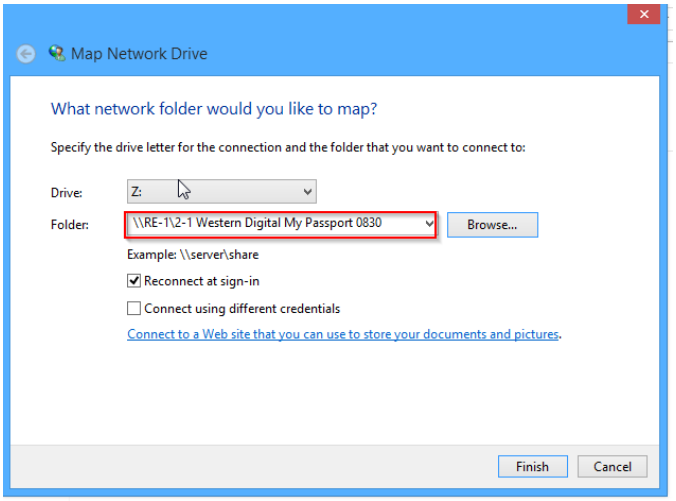
6. Select the folder you want to map and click **OK**.



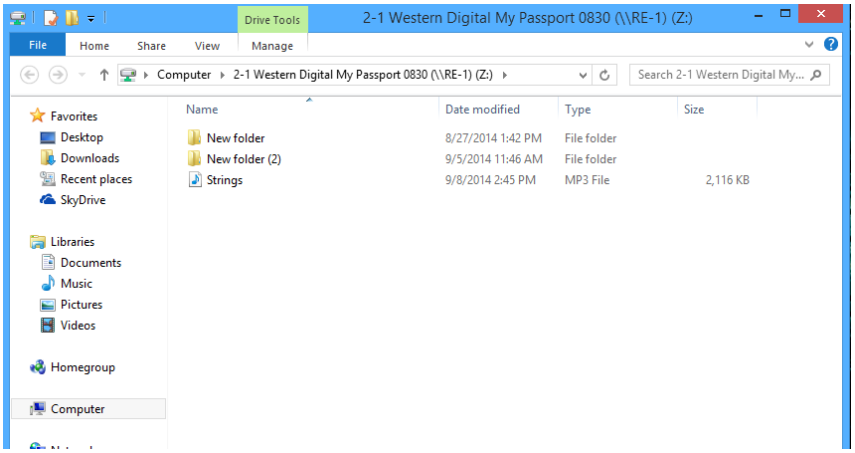
7. Enter the credentials to access the folder.



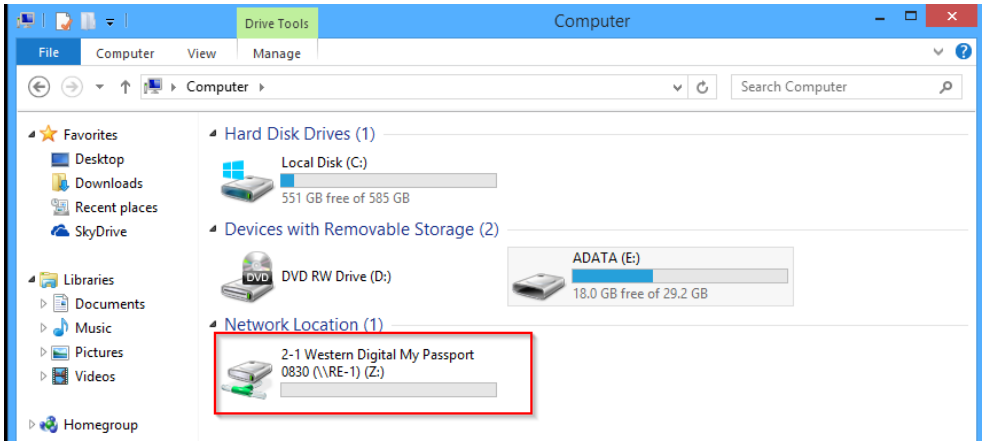
8. Your folder field will have auto populated with the name of the folder. Click **Finish**.



You will now have access to the files on the USB drive.



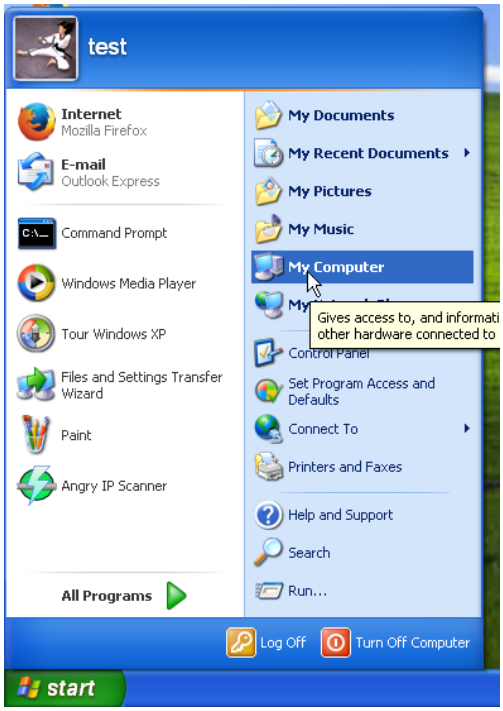
Your folder will now show up as a mapped drive.



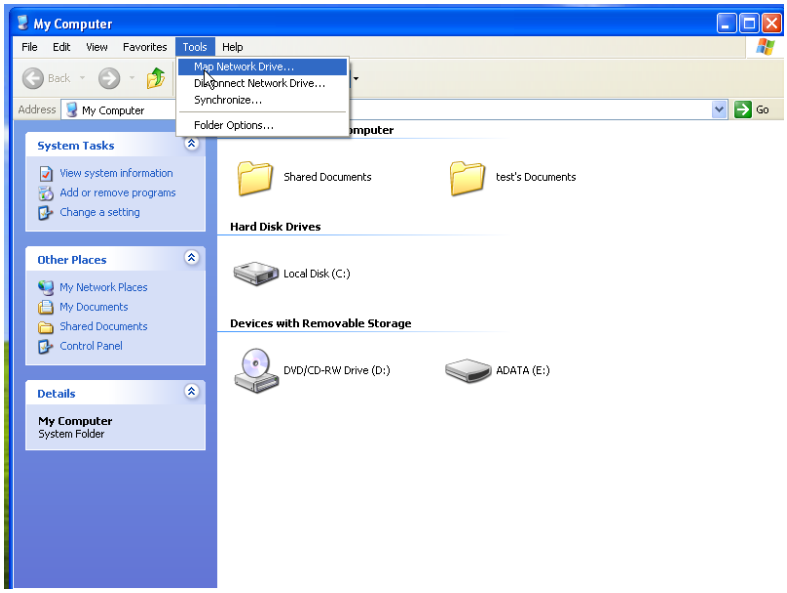
Windows XP

To map a USB drive in Windows XP:

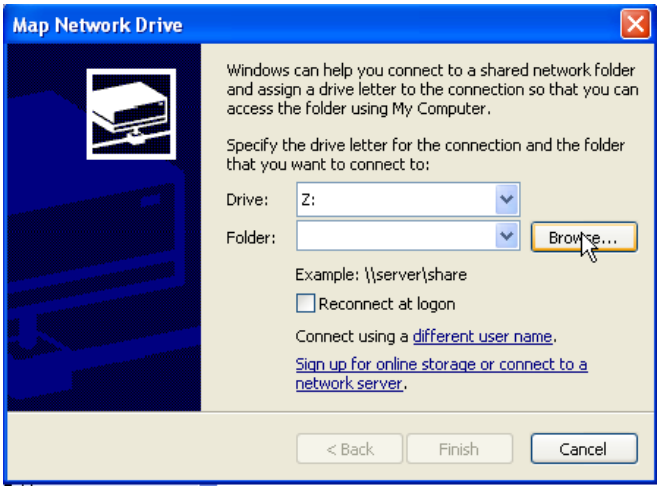
1. Click **My Computer**.



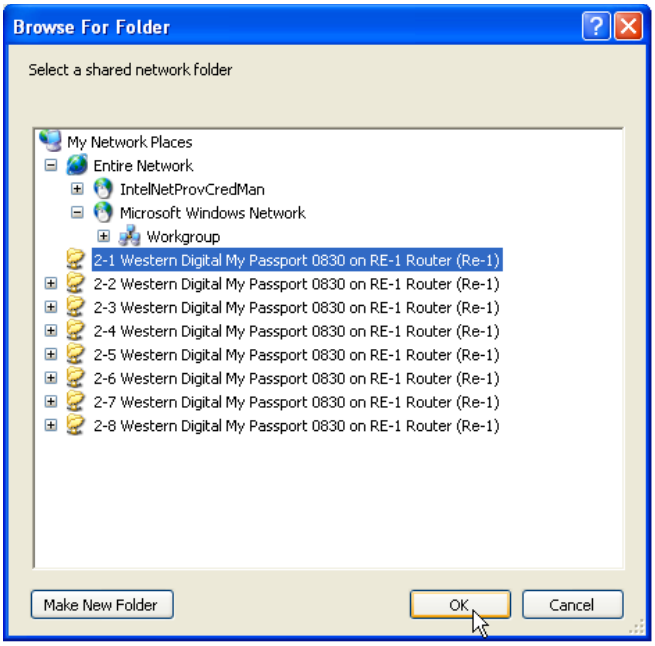
2. Click **Tools** > **Map Network Drive**.



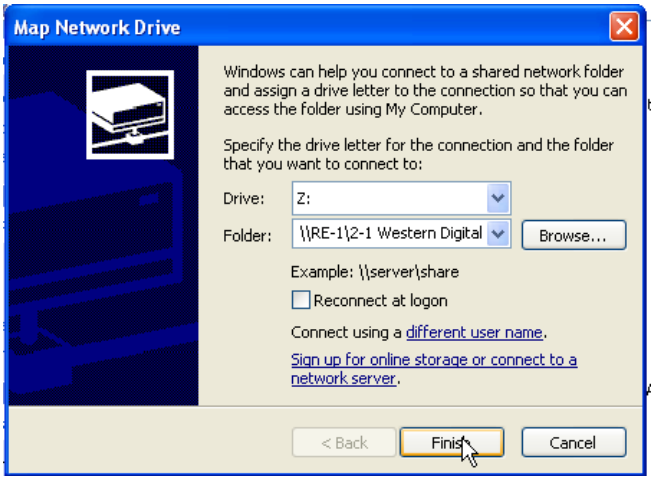
3. Click **Browse**.



4. Select the folder you want to map. Click **OK**.

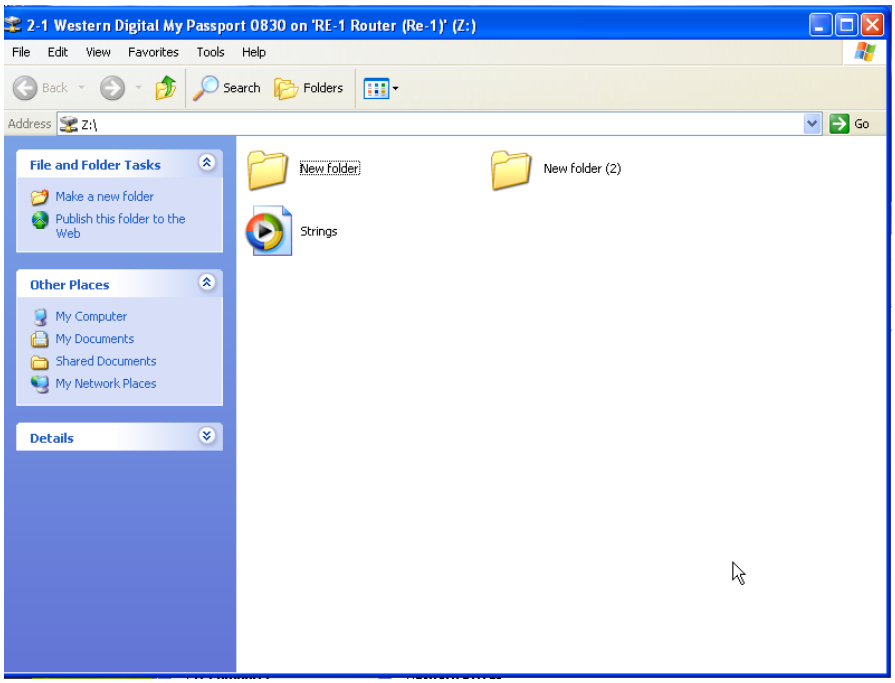


5. Click **Finish**.

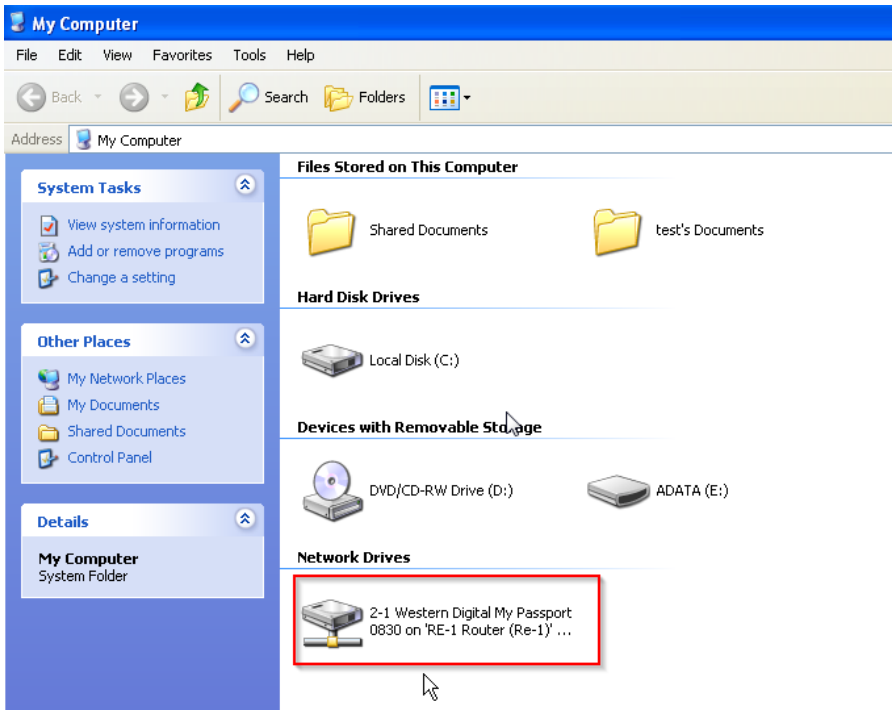


6. Enter the credentials to access the folder.

You will now have access to the folder.



Your folder will now be mapped on your computer.

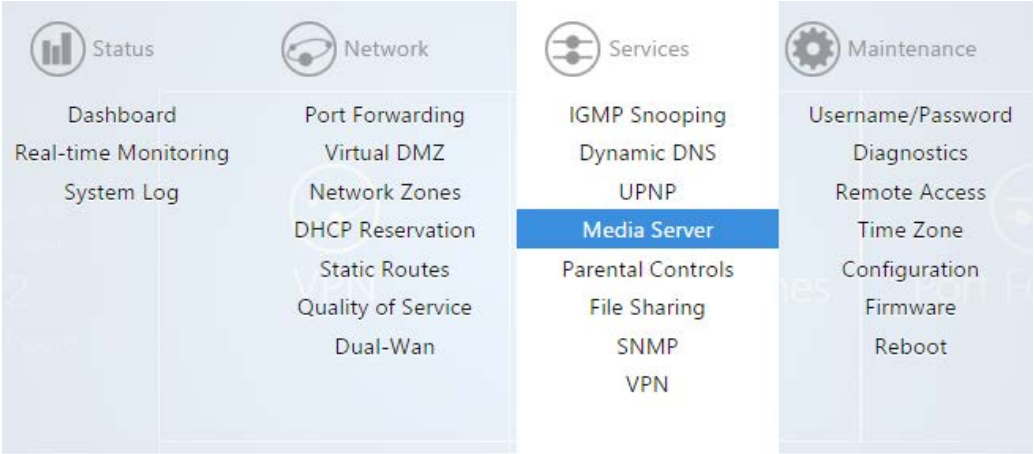


Media Server

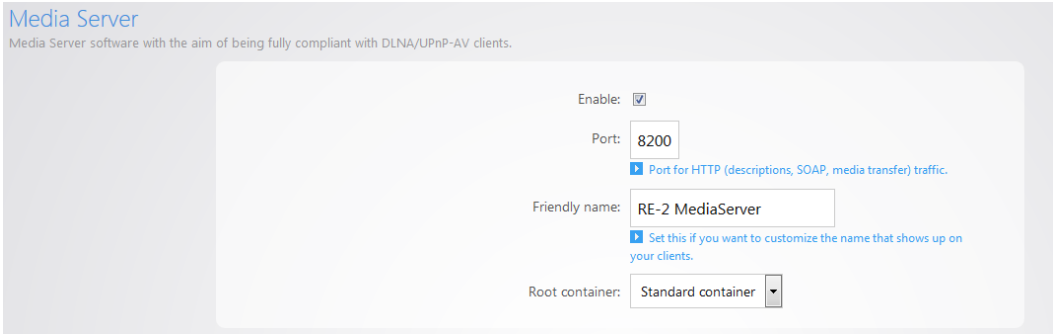
The Media Server feature allows the router to act as a media server on the network. After you enable this you can connect a USB drive to the router and use a media client on a computer to access the content of that USB drive.

To enable the media server:

1. Click **Media Server**.



2. Select **Enable**. **Port** sets the HTTP port used for media access. **Friendly Name** is the name that will be shown for this media server instance. **Root Container** describes the type of media files to be accessed through this media server.



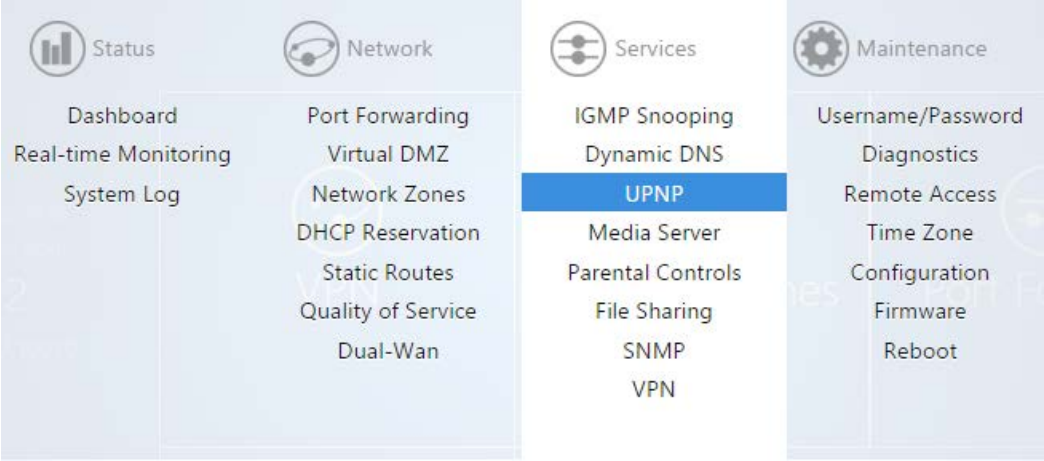
3. Click **Apply** to finalize the settings. The router will now act as a media server for your network.

UPnP

UPnP allows for automatic configuration of the router for your devices. This can be essential for certain audio/video systems and devices such as game consoles.

To enable UPnP:

1. Click **UPnP.**



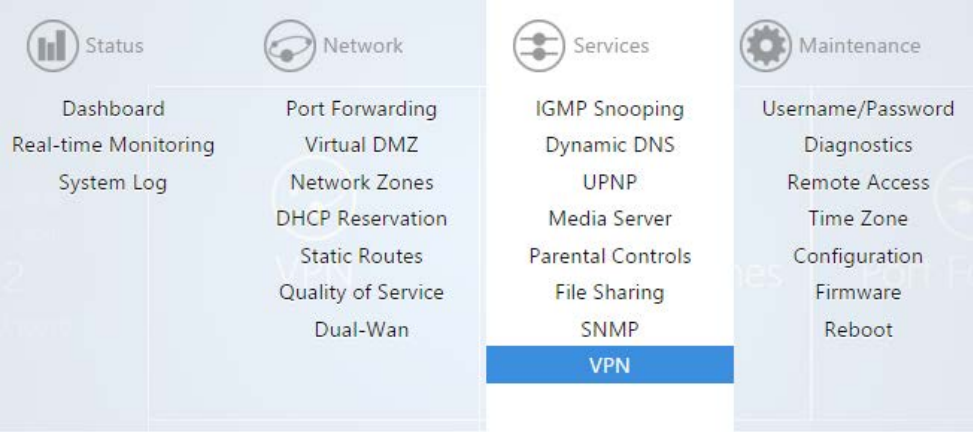
2. Select the enable box, then click **Apply** to finalize the settings.

VPN

The router supports Point-to-Point Tunnel Protocol VPN. You can connect to the router remotely and have access to all network resources.

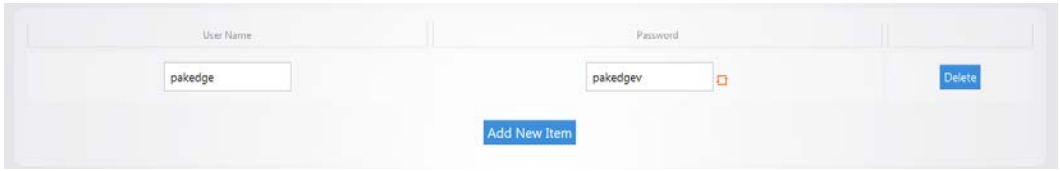
To configure the VPN:

1. Hover over **Services**, then click **VPN**.

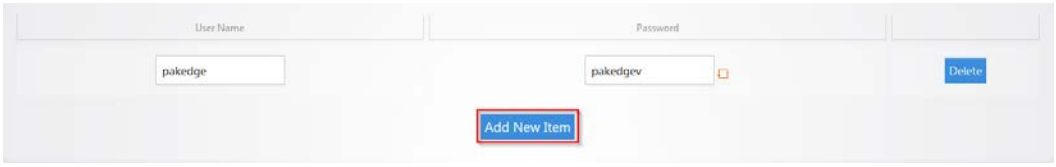


2. Select **Enable**.

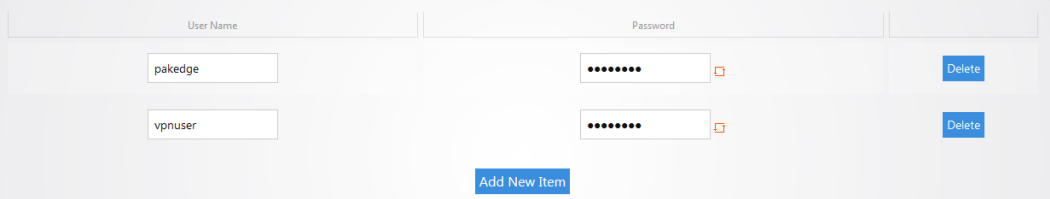
3. There is a default **pakedge** user. The default password for this user is **pakedgev**. Click **Apply** to enable the VPN with this default user.



4. You can change the username and the password.
5. You can also add a second user to the VPN by clicking **Add New Item**.



6. You can fill in a username and password. Click **Apply** to finalize the settings.



When you connect to the VPN you will have full access to all of your devices on the network.

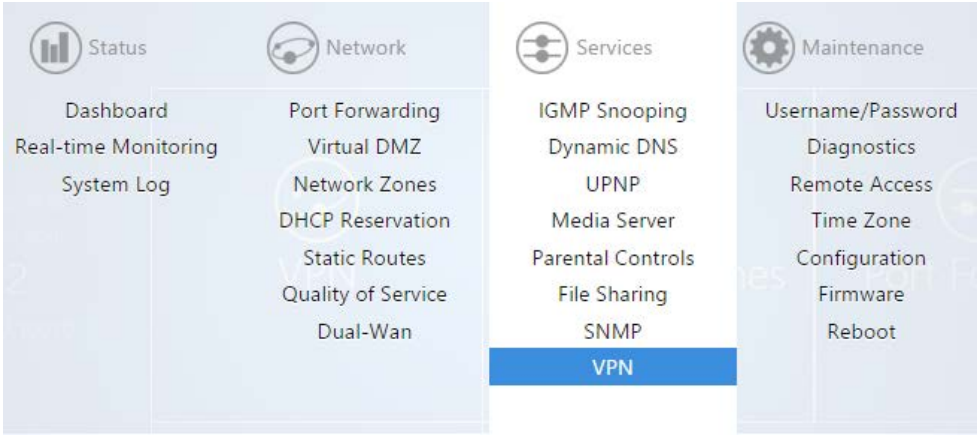
Note: When you connect to the VPN you will receive an IP address from the same IP scheme as your LAN zone. For example, if your LAN zone is setup for 192.168.1.X you will receive an IP address from the IP range of 192.168.1.20 thru 192.168.1.30. If your network LAN zone is setup as 192.168.10.X you will receive an IP address from the IP range of 192.168.10.20 thru 192.168.10.30.

OpenVPN

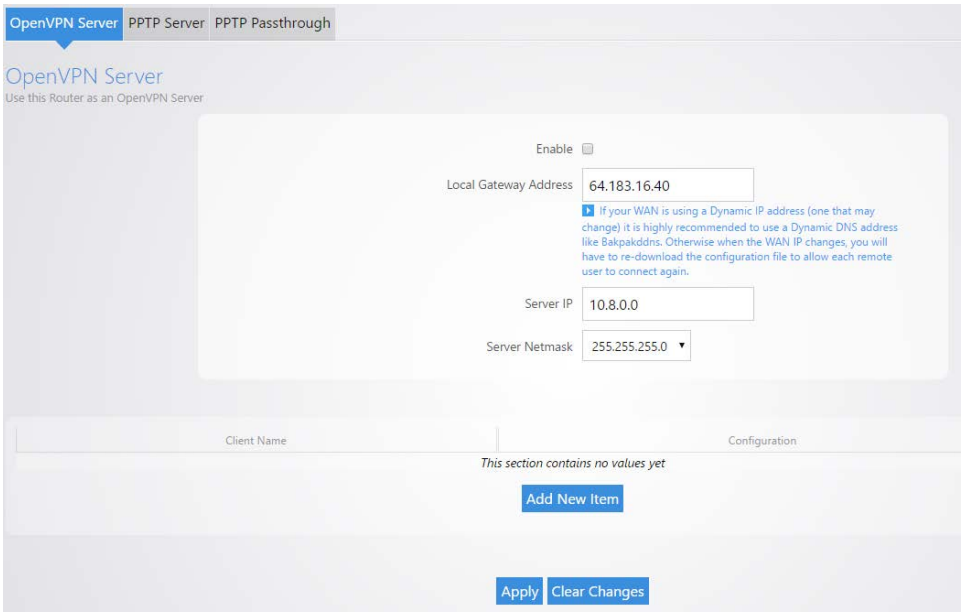
Your router supports OpenVPN for secure point-to-point connections.

To configure OpenVPN:

1. Hover over **Services**, then click **VPN**.



2. Select **Enable**, then complete the following fields:



- **Enable:** Turn OpenVPN Server on/off
- **Local Gateway Address:** The Public IP address or DDNS name of the WAN1 interface. We recommend that you use DDNS or BakPakDDNS because if the WAN IP changes, all remote clients will require new configurations made for them.
- **Server IP (OpenVPN IP):** The IP Subnet used by the OpenVPN connected clients. The OpenVPN clients will connect using their own dedicated IP subnet. This IP subnet cannot overlap with any of the local LAN or VLAN networks on the router. This is why the default is set to 10.8.0.0. This should be in IP Subnet notation (with 0 at the end of the address).
- **Server Netmask:** The subnet mask size to use for the OpenVPN network
- **Connection Profiles:** Each remote client connecting to the routers OpenVPN server will need to have a profile created for them. The profile only requires a name given to it. Then the profile is downloaded as a configuration file and sent to the device that will be connecting.
- **Client Name:** The name given to that profile. This is only to differentiate between connection profiles.
- **Configuration:** Download the ".ovpn" configuration file for that user. This Configuration file can then be emailed to the device that will be connecting so it can be loaded into the OpenVPN app and the connection can be made.
- **Delete:** Delete the profile
- **Add New Item:** Add new connection profile
- **Apply:** Apply the configuration settings.

After creating a client profile and downloading the configuration file, you need to load the configuration file into the OpenVPN program you are using.

- Each operating system has its own version of an OpenVPN client. The connecting device will need to download an OpenVPN client (which we have recommendations on below).

- If the configuration file was downloaded to a PC which is not the device that will be connecting, email the configuration file to an account that the device can access. This will allow mobile devices to open the configuration file directly to their OpenVPN app.

Important: Each configuration created for the OpenVPN server will only allow one connection at a time. Multiple users must have individual configurations created for them. If a second user attempts to connect to a configuration with a user already connected, the first user will be dropped from the connection.

OpenVPN client setup

Windows

The official OpenVPN release for Windows ships with a GUI frontend called simply "OpenVPN-GUI" and can be found in the .\bin\ subdirectory of the installation path, with shortcuts placed on the desktop and start menu unless unselected during program installation. This wiki page describes how to use this GUI frontend.

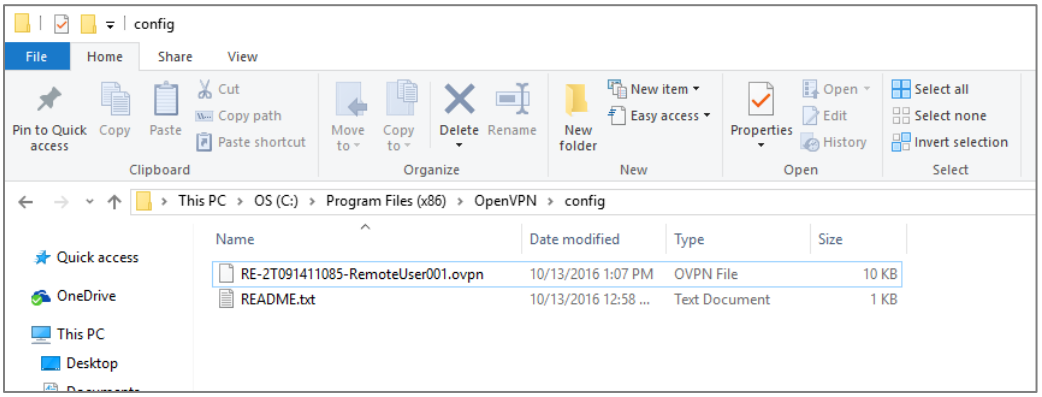
The GUI lives in the system tray, so controlling one or more VPN processes is always done through the context menu of the GUI icon. When the GUI is launched, nothing will happen beyond placing the icon in the tray. To do something useful with the GUI, you need to interact with it by right-clicking to bring up the context menu.

Note the GUI will start the VPN process in the context of the running user. When this user does not have administrative rights (or has rights limited through UAC) it will most likely fail to correctly start the VPN as routes and addressing cannot be changed by unprivileged users.

When starting the OpenVPN GUI, the standard Windows practice of right-clicking on the shortcut and selecting "Run As Administrator" will allow a UAC user to run it in administrative context. If the user lacks admin rights, it will be necessary to "Run As..." and enter credentials for an administrative user. Once started in this fashion, further interaction via the tray icon will be run in the context of the elevated user.

Creating and placing config files

By default, the GUI will present context entries to connect to any *.ovpn file under the .\config\ dir of the installation path (including subfolders.) If you do not place any config files here, the context menu in the GUI will not allow you to connect anywhere (since it has nowhere to connect to.)



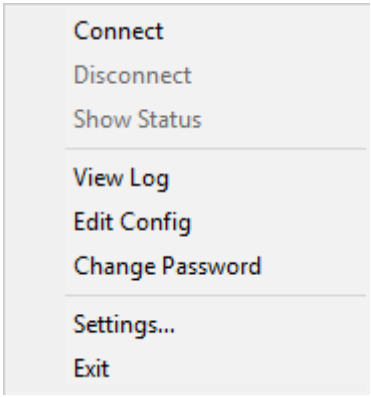
The screenshots below demonstrate use of the OpenVPN-GUI, step-by-step.

After Startup

After initially launching the OpenVPN-GUI program, the GUI icon will be show in the tray, as shown in the image below. Note that this icon can be hidden when marked "inactive" by the OS, so check the expanding arrows to the side of the system tray if it's started but not shown.

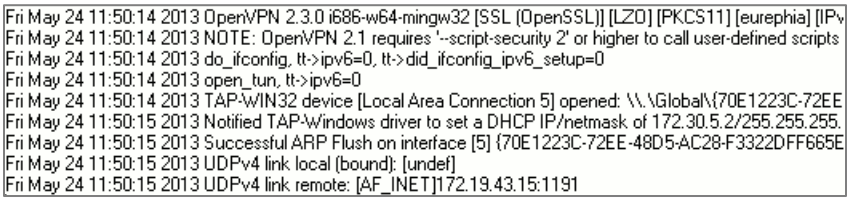
Context Menu

Right-clicking on the icon will pull up the context menu. This menu will allow you to connect any of the config files placed as explained above. Note that you must name these files with the .ovpn file extension. Windows has a bad habit of hiding "known" file extensions, so be careful not to name a config file something like “Sample.ovpn.txt” by mistake.



Connecting and Disconnecting

After you have created a config file, going into the context menu and selecting the "Connect" entry will start openvpn on that config file. A status window will open up showing the log output while the connection attempt is in progress (see screenshot below). After successful connection, the status window will be hidden, but can be viewed from the context menu if desired.



After connected, the context menu will allow that VPN to be disconnected; select that option to terminate the active connection.

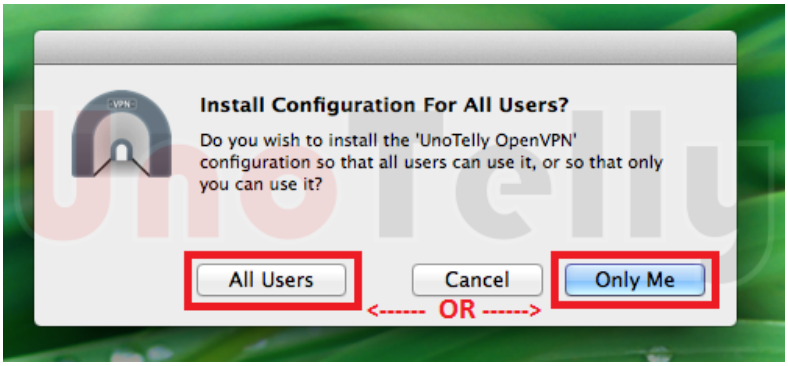
When one or more VPN instances are running from the GUI, the tray icon will change color.

OS X

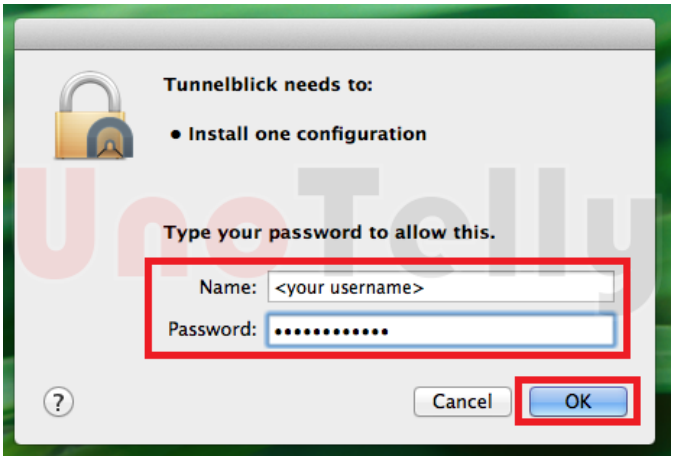
Tunnelblick is a popular, free, open source OpenVPN client for OS X.

To install Tunnelblick:

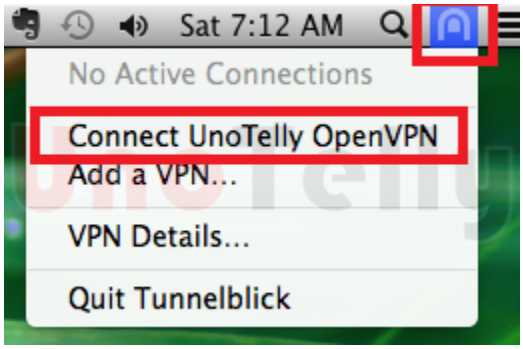
1. Download Tunnelblick here, and save it to a safe location.
2. Download the Tunnelblick OpenVPN configuration files here and save them to a safe location.
3. Double-click the **.ovpn** file you downloaded earlier. A dialog opens asking you for your configuration preference. You can choose to install the OpenVPN configuration for all users or just your account.



4. Enter your Computer username and password, then click **OK**.



5. Click the Tunnelblick icon in your menu bar, then click **Connect OpenVPN**.



If the connection is successful, you will see the following window appear briefly:

iOS

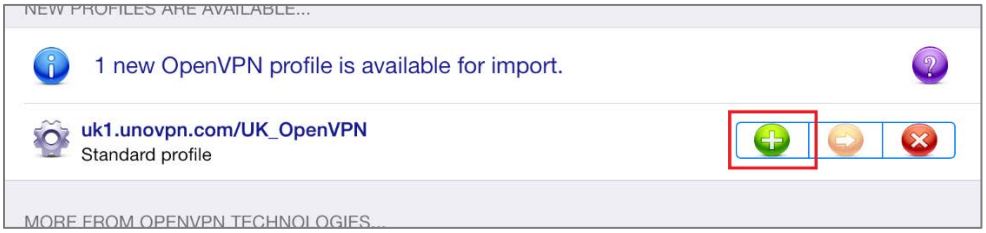
OpenVPN Connect is a free OpenVPN client for iOS devices.

To install OpenVPN Connect:

1. Download and install OpenVPN Connect from the App Store.
2. Open the email you sent yourself with the config file on your iOS device and tap the attached file.

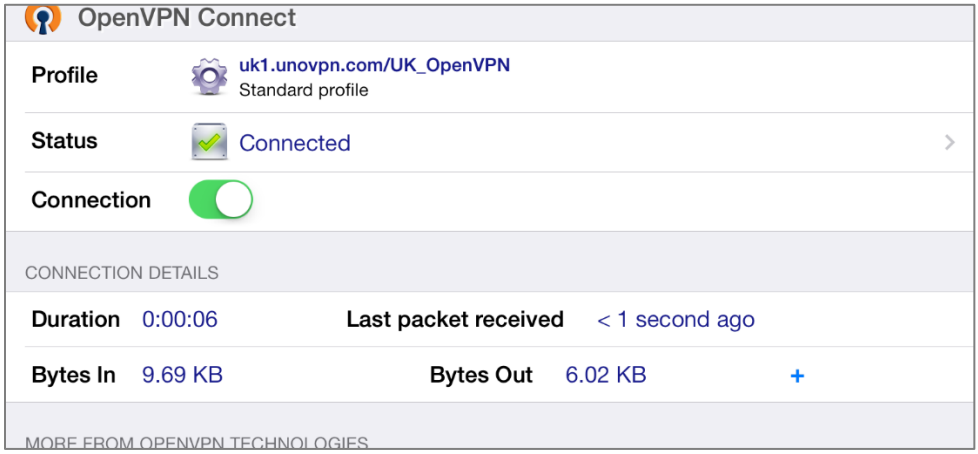
3. Tap **Open in OpenVPN** and the OpenVPN Connect app should open automatically.

4. Tap "**+**" to import the profile.



5. Type the User ID and Password for your UnoVPN account.
6. Tap **Connection** to connect to the VPN.

If connected successfully, you will see something like the following screen:

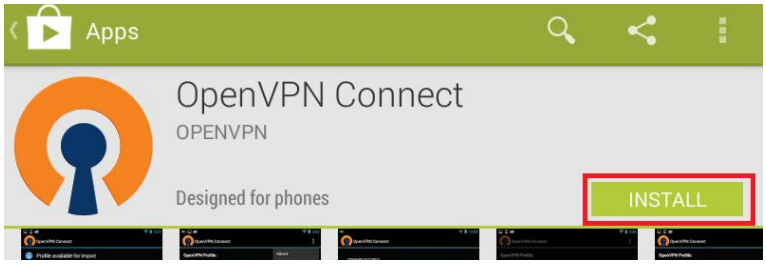


Android

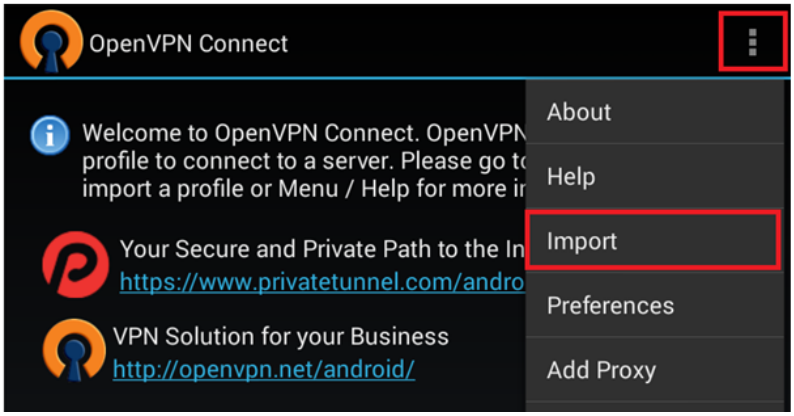
OpenVPN Connect is a free OpenVPN client for Android devices.

To install OpenVPN Connect:

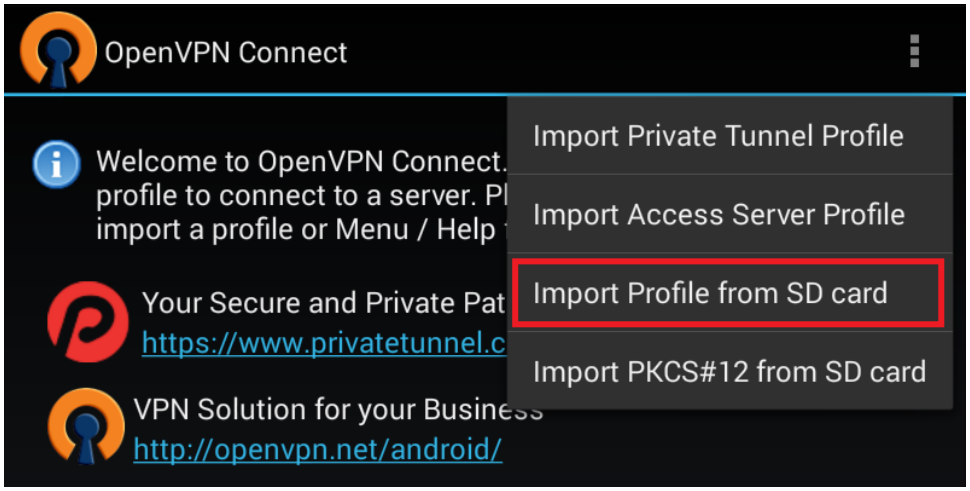
1. Download and install the OpenVPN Connect app from Google Play.



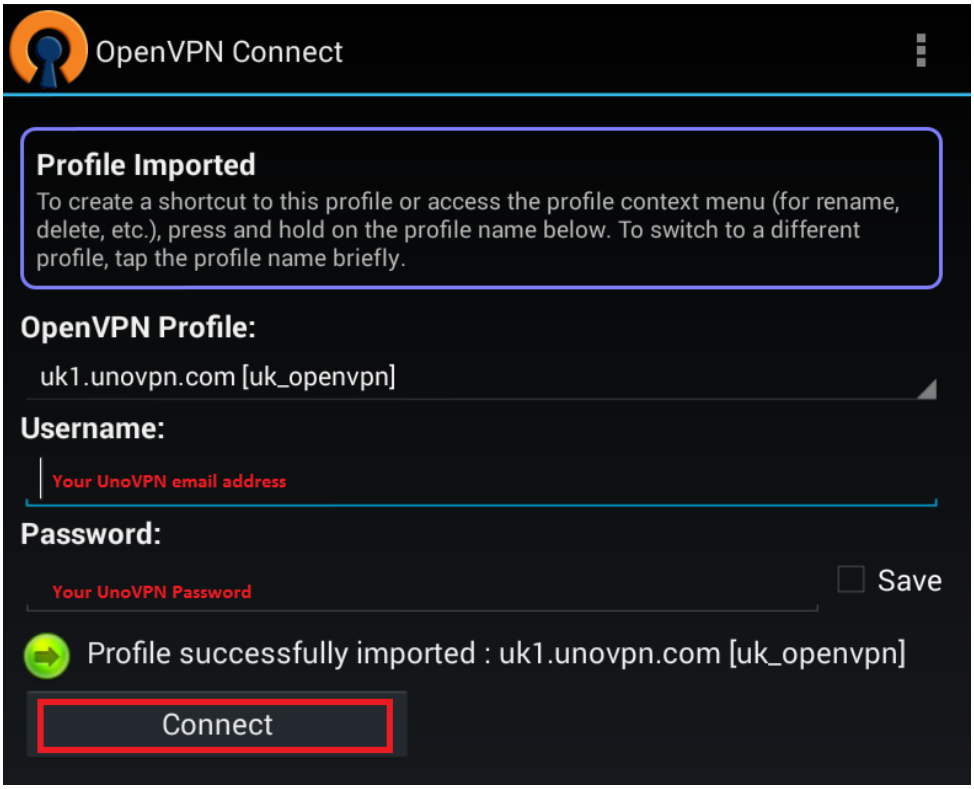
2. Download the OpenVPN Config file here and save it on your Android device.
3. Open the OpenVPN Connect app, tap its **Menu** icon, then tap **Import**.



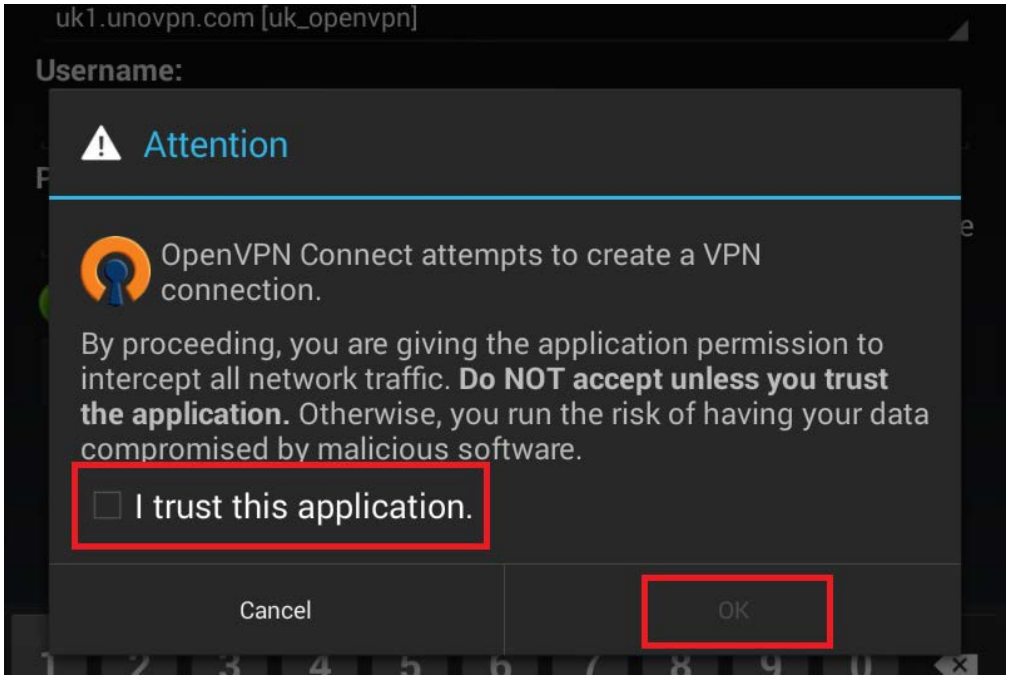
4. Tap **Import Profile from SD card**, locate your downloaded OpenVPN Config file, then tap **Select** to import the file.



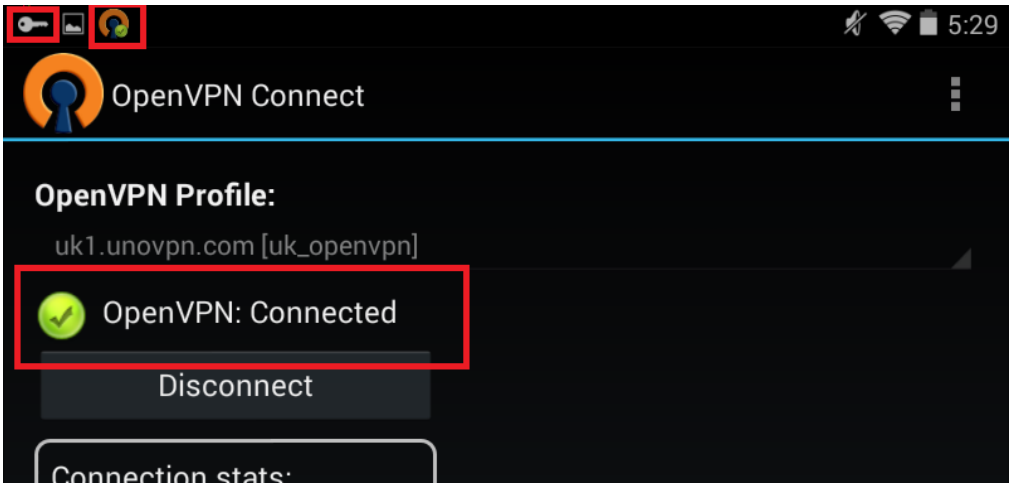
5. Enter your UnoVPN Username and Password, then tap **Connect**.



6. Allow permission to run OpenVPN by selecting **I trust this application**, then tap **OK**.



You are connected to OpenVPN.



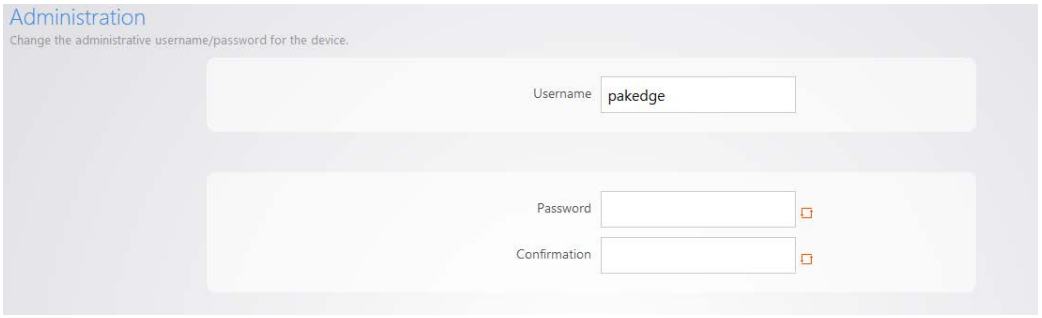
Username/Password

We strongly recommend that you change the default password for the router.

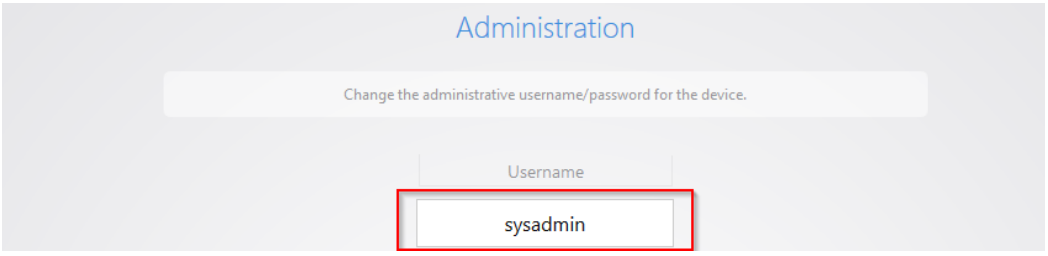
To change the password:

1. After you're logged into the router, navigate to **Maintenance >Username/Password**.

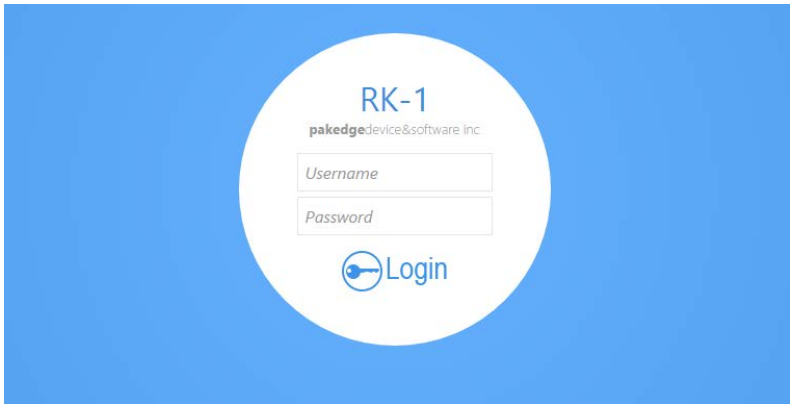
2. Enter the password you would like to use for the router. There are no specified requirements for the password. You will need to enter the password a second time to confirm it.



3. You can also change the default username. Simply type in the username you would like to use. Click **Apply** to finalize the settings.



4. You will then be prompted to log into the router with the new password.



Diagnostics

The Diagnostics page allows you to easily troubleshoot your network.

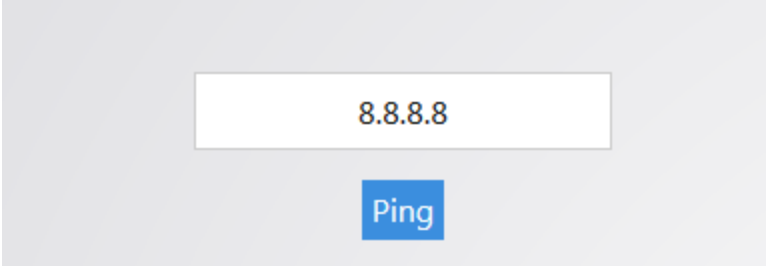
Ping

Ping allows you to test communication between two devices on the network.

To ping from the router:

1. From the **Maintenance** menu, click **Diagnostics**.

2. Click **Ping**. If you wish to ping a different IP address or hostname you may type it in instead.



3. After a few moments, your ping results will be displayed.

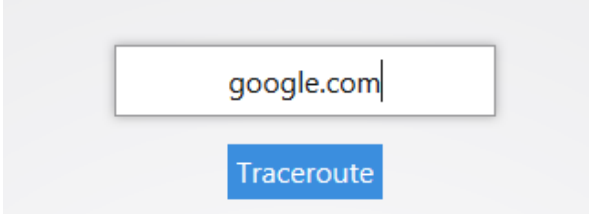
Traceroute

A traceroute allows you to see how many routers, or hops, there are between the router and a certain destination.

To perform a traceroute:

1. From the **Maintenance** menu, click **Diagnostics**.

2. Click **traceroute**. If you wish to perform a traceroute to a different website or IP address you may enter it instead.



3. After a few moments, your traceroute results will be displayed.

```
traceroute to google.com (74.125.224.129), 30 hops max, 38 byte packets
 1  192.168.1.99  0.283 ms
 2  173.60.186.1  2.204 ms
 3  100.41.196.230  8.212 ms
 4  130.81.163.248  11.813 ms
 5  *
 6  140.222.227.21  73.477 ms
 7  152.63.114.225  10.753 ms
 8  63.125.112.154  93.280 ms
 9  64.233.174.238  8.618 ms
10  209.85.250.251  6.069 ms
11  74.125.224.129  7.733 ms
```

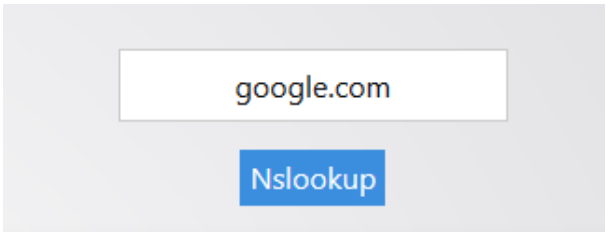
NSlookup

NSlookup allows you to find name server information for domains.

To perform an NSlookup:

1. Click **Diagnostics**.

2. Click **NSlookup**. If you wish to do an NSlookup for a different website you can type it in instead.



After a few moments your NSlookup results will be displayed.

```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      google.com
Address 1: 2607:f8b0:4007:805::1004 lax02s20-in-x04.1e100.net
Address 2: 74.125.224.130 lax02s20-in-f2.1e100.net
Address 3: 74.125.224.136 lax02s20-in-f8.1e100.net
Address 4: 74.125.224.134 lax02s20-in-f6.1e100.net
Address 5: 74.125.224.137 lax02s20-in-f9.1e100.net
Address 6: 74.125.224.142 lax02s20-in-f14.1e100.net
Address 7: 74.125.224.131 lax02s20-in-f3.1e100.net
Address 8: 74.125.224.132 lax02s20-in-f4.1e100.net
Address 9: 74.125.224.128 lax02s20-in-f0.1e100.net
Address 10: 74.125.224.135 lax02s20-in-f7.1e100.net
Address 11: 74.125.224.133 lax02s20-in-f5.1e100.net
Address 12: 74.125.224.129 lax02s20-in-f1.1e100.net
```

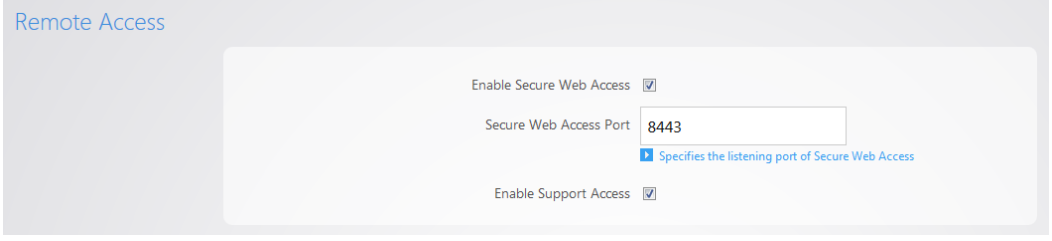
Remote Access

The **Remote Access** page allows you to change the default port used to access the router remotely.

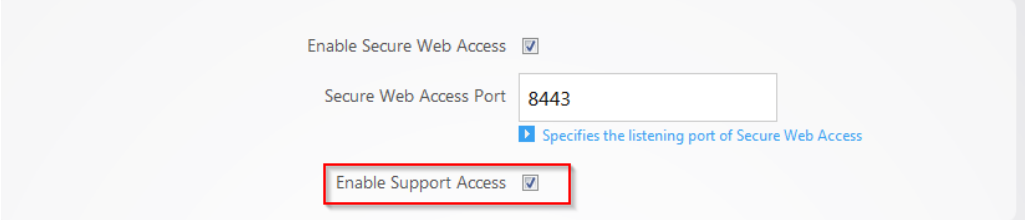
To change the secure web port:

1. Click **Remote Access**.

2. You can type a new port number into the **Secure Web Access Port** field if you wish to change it from its default. You can also disable remote access all together if you uncheck the **Enable Secure Web Access** option.



3. By default, **Enable Support Access** is enabled. This allows the support team at Pakedge to perform advanced diagnostics on your router. It is recommended that you keep this option enabled.



4. If you have made any changes on this page click **Apply** to finalize the settings.

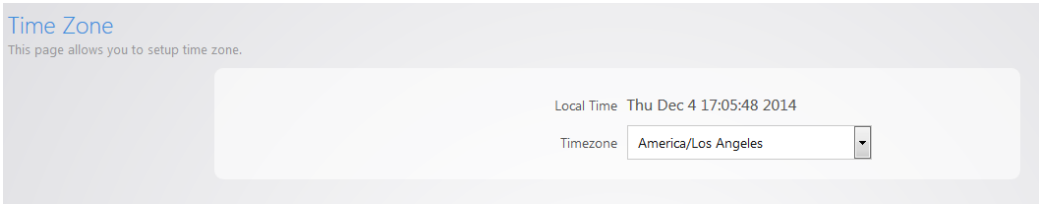
Time Zone

The time zone page allows you to set the appropriate time on the router.

To set the time zone:

1. Click **Time**.

2. Select your time zone from the drop-down menu.



3. Click **Apply** to finalize your settings.

Configuration

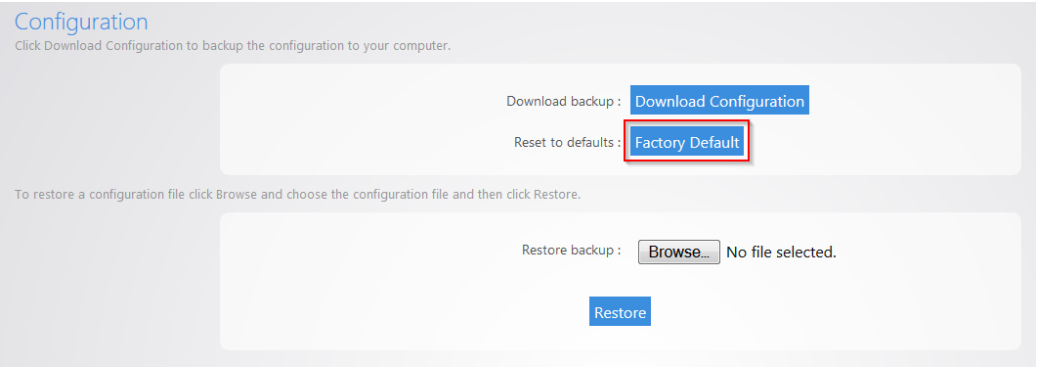
The **Configuration** page will allow you to factory default the router, download the configuration file, or restore a configuration.

Factory Default

To reset the router to factory default settings:

1. Click **Configuration**.

2. Click **Factory Default**.



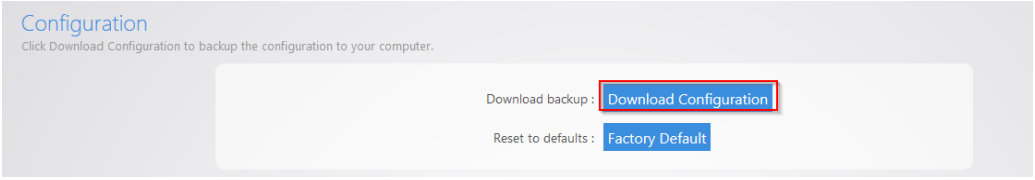
The router will now factory default itself. You can also factory default the router by pressing the pin-hole reset button on the back. Simply hold down this button for 10 seconds while the router is powered on, and then release it. The router will then factory default itself.

Download Backup

To make a backup of your configuration:

1. Click **Configuration**.

2. Click **Download Configuration**.



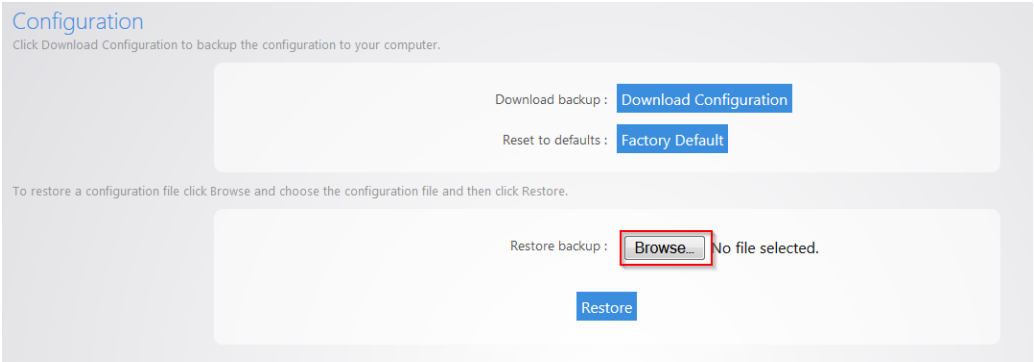
The configuration file will be downloaded to your computer.

Restore Configuration

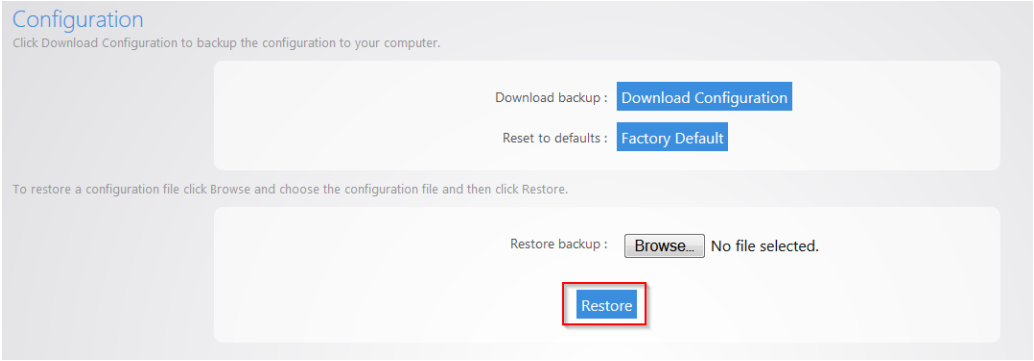
To restore a configuration from a previous backup:

1. Click **Configuration**.

2. Click **Browse**.



3. After you have selected your backup file, click **Restore**.



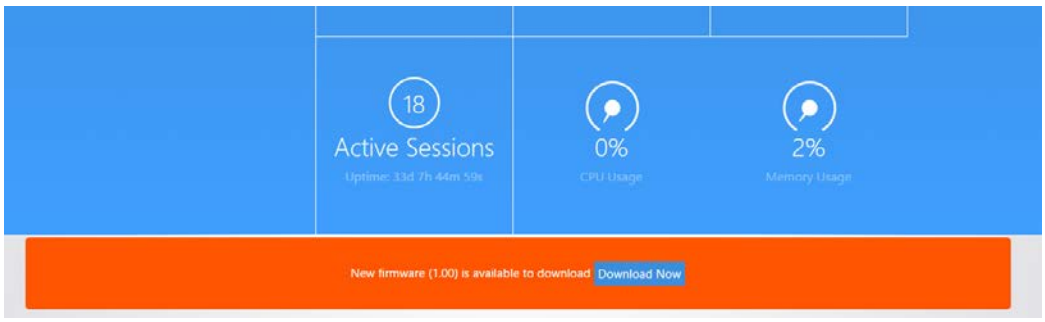
4. The router will then upload your configuration file and reboot itself.

Firmware

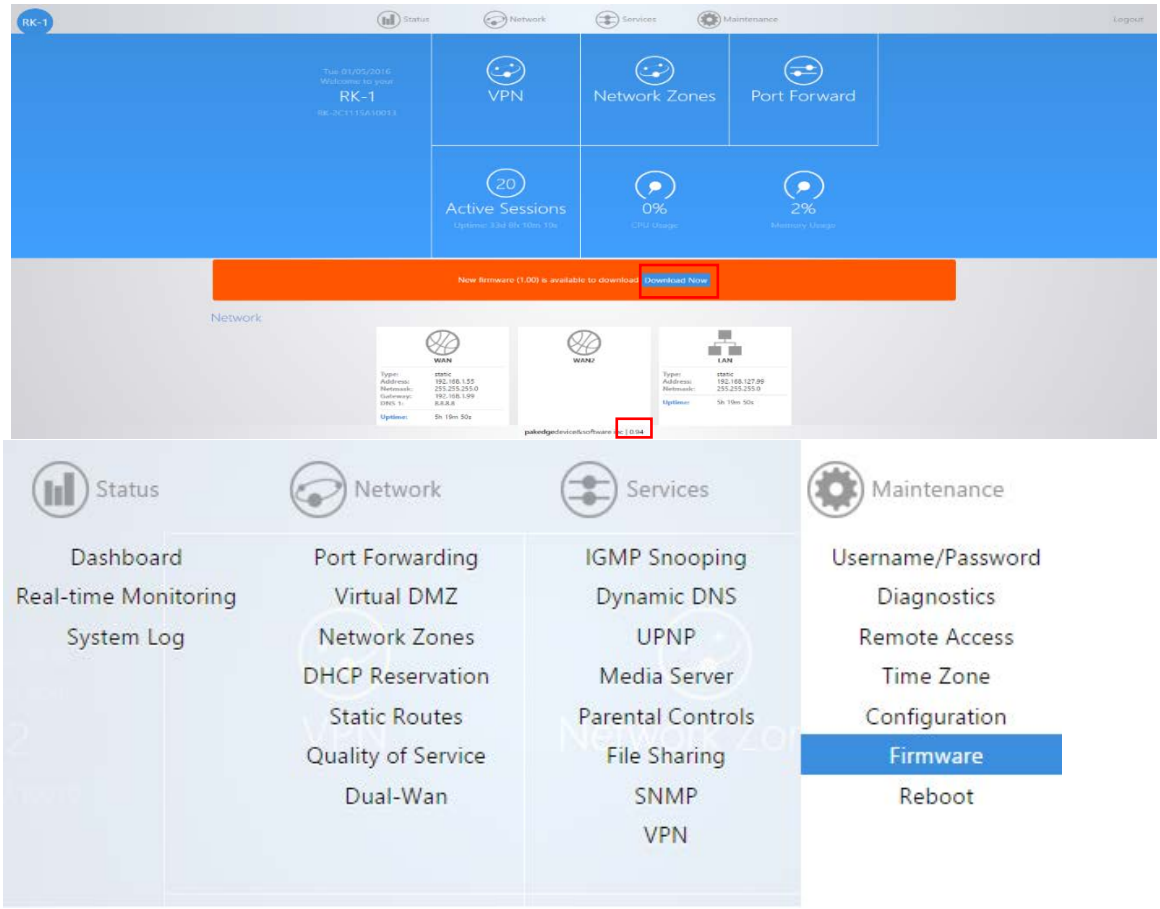
The Firmware page will allow you to update the firmware on your router.

To update the firmware:

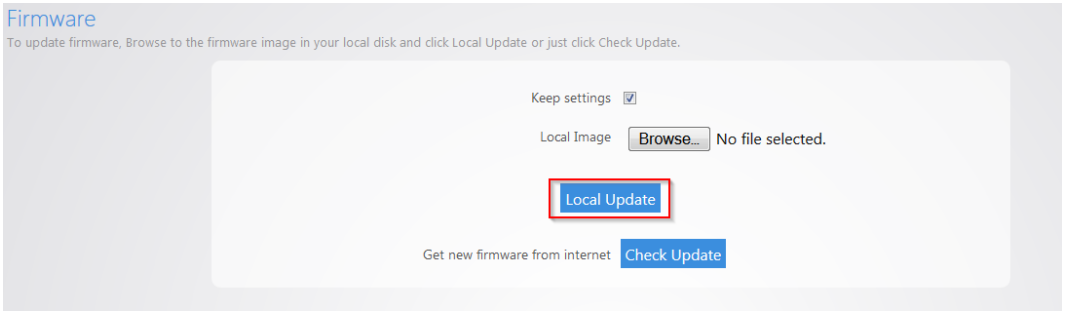
1. The current firmware version of the router is displayed towards the bottom of the page. If there is new firmware available for your router, you will see a message on the dashboard informing you. You can click **Download Now** to have the router update its firmware.



2. You can also manually download the latest firmware from the Dealer Portal on the Pakedge website. (http://www.pakedge.com/for-dealers-firmware.html)
3. Click **Firmware**.

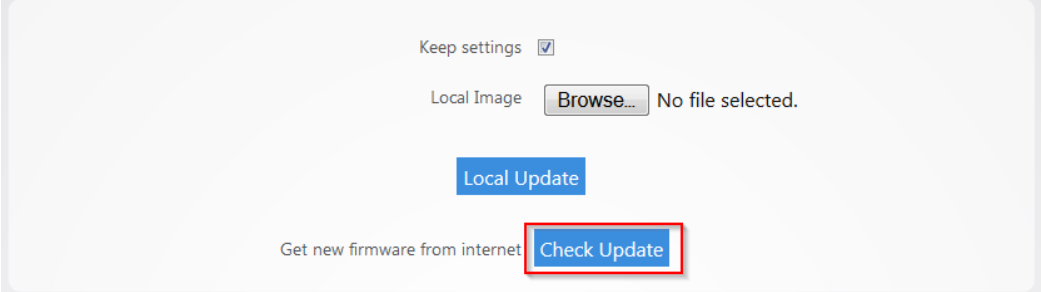


4. Browse to the firmware file and click **Local Update**. The **Keep settings** option indicates that the router will keep its configuration after the firmware update. If you uncheck this box before clicking **Update,** the router will factory default itself and come back up with the new firmware and the router's default configuration.



The firmware update will take a few minutes to complete.

5. The **Check Update** option will force the router to pull the latest firmware available and update itself.

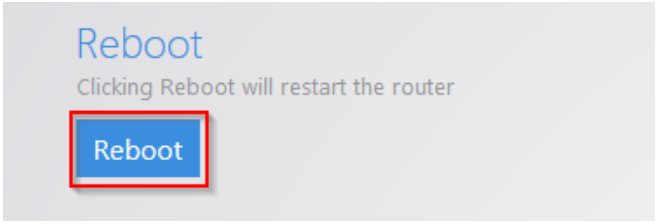


Reboot

To reboot:

1. From the **Maintenance** menu, select **Reboot**.

2. Click **Reboot**.



3. The router will now reboot.

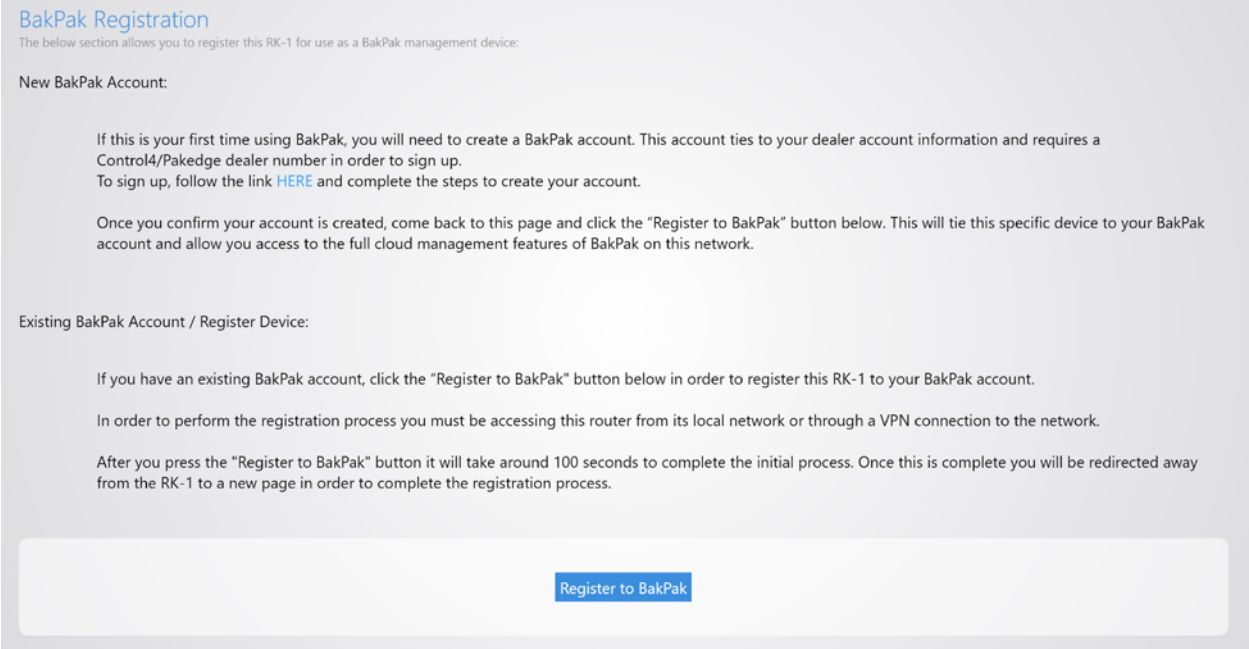
BakPak

The **BakPak** section allows you to register your router as a **BakPak Management Agent**. This functionality is only available on the RK-1 as of firmware 1.05.

Registration

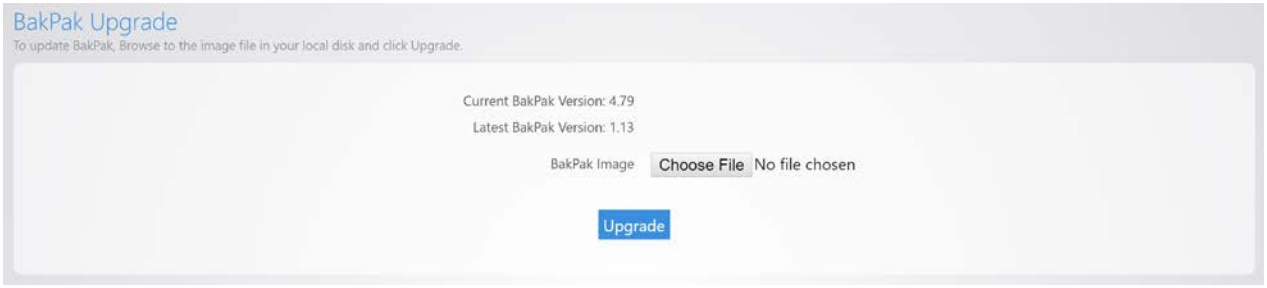
The Registration section allows you to connect this RK-1 to the BakPak cloud acting as a Management Agent. In order to connect you must first create a BakPak account with www.mybakpak.com. Then you will want to press the "Register to BakPak" button to begin the registration process.

In order to register the RK-1, you must be either connecting to the router through its local network or through a VPN to the router.



Manual Upgrade

Once registered, BakPak will perform any required updates automatically. In the situation where BakPak is unable to update itself automatically, the manual upgrade option is available for users to load a BakPak firmware file to the RK-1.
This section will also show the current version of BakPak running on the RK-1 and the most recent available version of BakPak.



Appendix A - Limited Warranty

Congratulations on your purchase of a Pakedge Device & Software product! We believe Pakedge designs and manufacture the finest home networking products on the market. With proper installation, setup, and care, you should enjoy many years of unparalleled performance. Please read this consumer protection plan carefully and retain it with your other important documents.

This is a LIMITED WARRANTY as defined by the U.S. Consumer Product Warranty and Federal Trade Commission Improvement Act.

19.1 What Is Covered Under the Terms of This Warranty

SERVICE LABOR: Pakedge will pay for service labor by an approved Pakedge service center when needed as a result of a manufacturing defect for a period of three (3) years from the effective date of delivery to the end user.

PARTS: Pakedge will provide new or rebuilt replacement parts for the parts that fail due to defects in materials or workmanship for a period of three (3) years from the effective date of delivery to the end user. Such replacement parts are then subsequently warranted for the remaining portion (if any) of the original warranty period.

19.2 What Is Not Covered Under the Terms of This Warranty

This warranty only covers failure due to defects in materials and workmanship that occur during normal use and does not cover normal maintenance. This warranty does not cover any appearance item; any damage to living structure; failure resulting from accident (for example: flood, electrical shorts, insulation); misuse, abuse, neglect, mishandling, misapplication, faulty or improper installation or setup adjustments; improper maintenance, alteration, improper use of any input signal and/or power, damage due to lightning or power line surges, spikes and brownouts; damage that occurs during shipping or transit; or damage that is attributed to acts of God.

The foregoing limited warranty is Pakedge's sole warranty and is applicable only to products sold as new by Authorized Dealers. The remedies provided herein are in lieu of a) any and all other remedies and warranties, whether expressed, implied or statutory, including but not limited to) any implied warranty of merchantability, fitness for a particular purpose or non-infringement, and b) any and all obligations and liabilities of Pakedge for damages including but not limited to: incidental, consequential or special damages, or any financial loss, lost profits or expense, or loss of network connection arising out of or in connection with the purchase, use or performance of the product, even if Pakedge has been advised of the possibility of such damages.

CAUTION: DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM IMPROPER INSTALLATION OR SETUP IS SPECIFICALLY EXCLUDED FROM COVERAGE UNDER THIS WARRRANTY. IT IS IMPERATIVE THAT INSTALLATION AND SETUP WORK BE PERFORMED ONLY BY AN AUTHORIZED PAKEDGE DEALER TO PROTECT YOUR RIGHTS UNDER THIS WARRANTY. THIS WILL ALSO ENSURE THAT YOU ENJOY THE FINE PERFORMANCE YOUR PAKEDGE PRODUCT IS CAPABLE OF PROVIDING.

19.3 Rights, Limits, and Exclusions

Pakedge limits its obligation under any implied warranties under state laws to a period not to exceed the warranty period. There are no express warranties. Pakedge also excludes any obligation on its part for incidental or consequential damages related to the failure of this product to function properly. Some states do not allow limitations on how long an implied warranty lasts, and some states do not allow the exclusion or limitation of incidental or consequential damages. In this case, the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

19.4 Effective Warranty Date

This warranty begins on the effective date of delivery to the end user. For your convenience, keep the original bill of sale as evidence of the purchase date from your authorized dealer.

19.5 Important: Warranty Registration

Please register your product at www.pakedge.com. It is imperative that Pakedge knows how to reach you promptly if we should discover a safety problem or product update for which you must be notified. In addition, you may be eligible for discounts on future upgrades as new networking standards come about.

19.6 To Obtain Service, Contact Your Pakedge Dealer.

Repairs made under the terms of the Limited Warranty covering your Pakedge product will be performed by an Authorized Pakedge Service Center. These arrangements must be made through the selling Pakedge Dealer. If this is not possible, contact Pakedge directly for further instructions. Prior to returning a defective product directly to Pakedge, you must obtain a Return Material Authorization number and shipping instructions. Return shipping costs will be the responsibility of the owner.

For additional information about this warranty, visit our website at **www.pakedge.com**.

Email: support@pakedge.com

Phone: (650) 385-8703

Appendix B - Specifications

Item	Description
Summary	
Fixed ports	7
LED Indicators	USB, 1000M and Link/Act LED, PWR
Input voltage	100V～240V AC, 0.9A, 50/60Hz
Power consumption	15.4 watts
Operating temperature	0°C～40°C
Storage temperature	-10°C～70°C
Relative humidity	20%～85% (non-condensing)
Spanning Tree	IEEE 802.1s Spanning Tree Protocol (STP)
QoS	Quality of Service
Management	
SSH	Supports limited SSH configuration mode
WEB	Supports WEB management

SNMP	Supports System configuration with SNMP v1/v2
System Log	Supported
Configuration File Download/Upload	Supports Download/Upload configuration File via WEB
Upgrade Firmware	Supports Upgrade Firmware via WEB
Debug	
PING	Supported
TRACEROUTE	Supported
NSLOOKUP	Supported
Mechanical	
L x W x H	10.5″ x 6.5″ x 2″
Weight	4 lbs

11734 Election Road

Draper, UT 84020

U.S.A

Visit us at:

www.pakedge.com

DOC-00183-C 2017-01-31 MS