

RK-1

7-Port Gigabit Router with BakPak User Guide



# Contents

Introduction Technical Support	4
Installing	4
Getting to know your product	5
Accessing the router Dashboard	7 8
Quick Setup	9
Status menu Real-time monitoring System log System report	11 
Network menu Port forwarding 1:1 NAT Virtual DMZ VLAN (network zones) WAN settings	
Changing the IP address of the LAN zone Isolated guest network DNS DHCP reservation Static routes Dual WAN Quality of service	
Services menu UPnP Dynamic DNS Pakedge DDNS Non-Pakedge DDNS File sharing Local file sharing Remote file access Mapping network drives Media server SNMP Parental controls Block websites Block clients VPN PPTP OpenVPN	32 32 33 33 36 38 38 40 40 45 49 50 51 51 51 53 54 54 54 54 56
Maintenance menu Username/Password Diagnostics	65 65 66

Ping	
Traceroute	67
NSlookup	68
Remote access	69
Time zone	70
Configuration	71
Factory defaults	71
Download configuration	
Restore configuration	
Firmware	73
LEDs	75
Reboot	76
BakPak menu	
Registration	
Maintenance	77
BakPak upgrade	77
Unregister from BakPak	77
Appendix A: Specifications	

# 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.

## Technical Support

Pakedge 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:

Email: <a href="mailto:support@pakedge.com">support@pakedge.com</a> Phone: 650.385.8703

Visit our website for up-to-date support information at <u>www.pakedge.com</u>.

Be prepared to provide your product's model and serial number. 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 or go to <u>pkdge.co/rk1-ug</u>. 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 router
- Mounting brackets
- Power cable
- 2-meter (about 6 feet) CAT5E cable
- Quick Start Guide



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

LED	S	tatus	Operation
		Blue	USB is connected
USB 1 - 2	LINK/ACT	Flashing Blue	USB is being accessed
		Off	No device connected
		Blue	Port is online (link established)
WAN 1 - 2	LINK/ACT	Flashing Blue	Activity
		Off	No device connected
		Blue	Port is online (link established)
LAN 1 - 5	LINK/ACT	Flashing Blue	Activity
		Off	No device connected
	Blue		The router is powered on
Power	Off		The router is turned off

#### Table 1: LED definitions (from left to right)

**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 details (from left to right)

Interface	Туре	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 interface:

- 1. Connect an Ethernet cable to the router and a computer.
- 2. Make sure your network card is set to obtain an IP address automatically, then open any internet browser and go to the address <u>http://192.168.1.99</u>, or you can simply type **pakedgerouter.com**. Note: For best results we recommend using Mozilla Firefox as your web browser.
- 3. Enter the default username **pakedge** and the password **pakedger**, then click **Log in**.



**Important:** Change this default password. For instructions, see the section "Username/Password" on page 65.

### Dashboard

Services ( Maintenance BakPak K-1 (III) Status Network -VPN 16% 16% Network LAN 192.168.250.1 255.255.255.0 2d 21h 59m 18s

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

On this 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.

Network							
	WAN (active)			WAN 2 (inactive)		LAN	
	Type: Address: Netmask: Gateway:	dhcp 255.255.254.0	Type: Address: Netmask: Gateway:	dhcp 0.0.0.0 255.255.255.255	Type: Address: Netmask:	Static 192.168.250.1 255.255.255.0	
	DNS 1: DNS 2:		Uptime:	Oh Om Os	Uptime:	2d 21h 59m 18s	

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

DHCP Leases					
	Hostname	\$ IP Address	\$ MAC Address	\$ Lease time remaining	\$
	Galaxy-S9	192.168.250.151		7h 47m 4s	
	XboxOne	192.168.250.150		3h 43m 46s	
	SAMSUNG-SM-G928V	192.168.250.141		9h 23m 1s	
	DESKTOP-SS0AMFH	192.168.250.172		10h 17m 33s	
	amazon-d4705d108	192.168.250.149		8h 0m 0s	
	Bertha-2	192.168.250.167		10h 39m 44s	
	Eva-iPhone	192.168.250.154		10h 28m 0s	
	glassedge7	192.168.250.156		9h 36m 11s	
	DESKTOP-VE0OMLT	192.168.250.147		7h 21m 23s	
	Ander-iPhone	192.168.250.158		10h 42m 55s	

**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.

Other Connected Devices						
Zone	\$	IP Address	\$	MAC Address		
LAN		192.168.250.6				
LAN		192.168.250.15				
WAN (Internet)		140.186.138.1				
LAN		192.168.250.17				
LAN		192.168.250.4				
LAN		192.168.250.5				

# Quick Setup

On the Dashboard, the *Quick Setup* link takes you to a page where you can configure the most common router settings, all in one place. Quick Setup also loads the first time you log in to the router's interface. For more information on setting up the WAN internet connection, see "WAN settings" on page 19.

#### To complete information in the Quick Setup page:

1. From the Dashboard, click the **Quick Setup** tile to launch the *Quick Setup Page*.



In the Username/Password section, enter a new username and password.
 Caution: We strongly encourage you to change the password right away.

Username/Password		
	Username	pakedge
	New Password	
		6 Characters Minimum
	Verify Password	

3. In the *WAN Zone* section, determine the 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. For more information on these settings, see "WAN settings" on page 19.

The router supports the three main types of internet connections:

- **DHCP** (typically used by cable companies and DSL basic service). By default, the router will connect to the internet using DHCP.
- **Static IP** (Fixed public IP address mostly used by Business Class Broadband services)
- **PPPoE** (Used by DSL companies such as AT&T)

WAN Zone			
	Protocol	Static address	*
	IPv4 Address	64.183.16.40	
	IPv4 Subnet Mask	255.255.255.240	~
	IPv4 Gateway	64.183.16.33	
	Use Custom DNS Servers	8.8.8.8	+
	Enable remote WAN access	•	

 In the LAN Zone section, enter the new IP address you want to use in the IPv4 Address field. In the following example, we change the IP address of the router to 192.168.10.99. For more information, see "VLAN (network zones)" on page 17.

LAN Zone	
IPv4 Address	192.168.1.99
IPv4 Subnet Mask	255.255.255.0 *
DHCP Start	192.168.1.100
	U Lowest leased address
DHCP End	192.168.1.198
	I Highest leased address
Lease time	12h
	Expiry time of leased addresses, such as, 7d or 12h or 60m. Minimum is 2 Minutes.

- 5. Further down on the page, the **DHCP Start** field indicates the first IP address that will be handed out by the router. The **DHCP End IPv4 Address** field indicates the last IP address that will be handed out.
- 6. The *Lease Time* field indicates how long a DHCP address is valid for. **Note:** 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**.
- 7. Click **Apply** to finalize your settings.

# Status menu

## Real-time monitoring

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

1. Hover over the **Status** menu, then click **Real-time Monitoring**.

Status	Network	Services	Maintenance	BakPak
Dashboard	Port Forwarding/1:1 NAT	UPNP	Username/Password	Registration
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics	Maintenance
System Log	Network Zones	File Sharing	Remote Access	
System Report	DHCP Reservation	Media Server	Time Zone	
	Static Routes	SNMP	Configuration	
	Dual-Wan CK De	Parental Controls	VEN Firmware Net	
	Quality of Service	VPN	LEDs	
			Reboot	
	Quality of Service	VPN	LEDs Reboot	

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

Ports Status	LAN/WAN Statistics	Live Sessions				
wan	wan2		2	3	4	5
•	۰	•	•	•	•	•
WAN 1G/Full	WAN2	100M/Full	LAN 1G/Full	LAN 1G/Full	LAN 1G/Full	LAN 1G/Full

The *LAN/WAN Statistics* section displays the amount of traffic going through the LAN or WAN of the router.



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

Port	s Status LAN/WAN Statistics Live Sessions	
Ses This p	sion Statistics age displays statistics for the active sessions.	UDP: 7 40 Other: 9
		Select Statistics Window: 5 Minutes 👻
		Click and drag in the plot area to zoom in. Double-clicking will zoom you back out.
	60	<b>TCP</b> : 36
	50	
ions	40	
nect	30	
coni		
-		
	20	
	10	~ ~ ~ ~ ~
	0	

### System log

The system log records network events that have occurred in your router's network.

#### To access the system log and view its settings:

1. Hover over the **Status** menu, then click **System Log**. The *System Log* page opens.

RK-1	Status	Network	Services	Maintenance Logout						
Syster This page	n Log allows you to configure s	ystem log settings.								
		System log buffer size	10240 Buffer size is in KB							
		Enable remote system log								
		External system log server	0.0.0.0							
External system log server port 514										
Download										
	Apply Clear Changes									

- 2. To download the system log, click **Download**, then specify a download location. The report file is readable with a text editor.
- 3. Change settings, as needed, then click Apply:
  - **System log buffer size:** The amount of data the log can contain before old information drops off to make room for more data.
  - Enable remote system log: Enables an external server to record the log.
  - External system log server: Enter the IP address of the external server you want to use for the log.
  - External system log server port: Enter the port you want the external server to use.

### System report

The system report can provide information to Technical Support about your router and its network.

#### To download the system report:

1. Hover over the *Status* menu, then click **System Report**. The *System Report* page opens.

rt file to your computer.
d

2. Click **Download**, then specify a download location. The report file is readable with a text editor.

## Network menu

## 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. Hover over the **Network** menu, then click **Port Forwarding/1:1 NAT**.



As an example, we will forward TCP port 80 to an IP camera on the IP address 192.168.1.50.

- a. Click Add New Item.
- a. For the **Description**, enter **IP Camera**.
- b. For the **Protocol** select **TCP**.
- c. For the WAN Zone select WAN.
- d. Enter 80 for the External Port.
- e. Enter 80 as the Internal port.
- f. For the Internal IP address, select Custom and enter 192.168.1.50.
- g. Leave **Enable** selected.



2. Click **Apply**. The port forward information will be saved in this section.

## 1:1 NAT

1:1 NAT is similar to port forwarding in that it allows you to forward ports to any specific device on the network. This feature is useful in situations where a block of public IP addresses is available from a service provider and the user wants to assign a specific public IP to a specific device on the network. This will make any traffic originating from the device pass to the internet using the public IP specified for that device. 1:1 NAT is only supported on the RK-1 router.

#### To configure 1:1 NAT:

- 1. Hover over the **Network** menu, then click **Port Forwarding/1:1 NAT**. As an example, we will forward the public IP **1.1.1.1** to the local IP **192.168.1.51**.
- 2. Click Add New Item.
- 3. Complete the following fields:

:1 NAT (Network Address Translati	ion) is a mode of NA	T that maps one ir	iternal address to one external	address.				
Description	Protocol	WAN Zone	External IP	Internal Zone	Internal IP Address		Enabled	Action
WebServer	TCP ~	WAN	1.1.1.1	LAN ~	192.168.1.51	¥		Delete
			Ad	ld New Item				

- For Description, enter WebServer.
- For **Protocol**, enter **TCP**.
- For External IP, enter 1.1.1.1.
- For Internal Zone, select LAN.
- For Internal IP Address, enter 192.168.1.51.
- Leave the **Enable** box selected.
- 4. Click **Apply**, and the configuration will be applied.

### 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. Hover over the Network menu, then 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.



4. Click **Apply** to finalize the configuration.

**Note:** When you enable the virtual DMZ, you will still be able access the router's interface remotely via HTTPS, and you will still be able to use VPN.

## VLAN (network zones)

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

#### To modify any of the VLAN settings:

1. Hover over the Network menu, then click **Network Zones**.



VLANs 2-6 will be displayed towards the bottom.



2. Select **Zone Bonding** to allow devices that use multicast messaging to communicate across VLANs.

- E Audio/Vide VLAN ID: VLAN ID: VLA 3 Address: 192.168.2.1 Address: 192.168.3.1 Add Netmask: 255.255.255.0 Netmask: 255.255.255.0 Net 10.00 C 10.000 MAC-Address: MAC-Address: MAC Received: 0.00 B Received: 0.00 B Rece 25.49 MB 25.49 MB Sent: Sent: Sent Uptime: 1d 1h 3m 4s Uptime: 1d 1h 3m 4s Upti Edit
- 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. Deselecting 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.

VLAN2 Zone		
	Name	Voice
	VLAN ID	2
	Enable Inter VLAN Routing	V

 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.

IP Address 192.168.12.1		
	IP Address	192.168.12.1
Netmask 255.255.255.0	Netmask	255.255.255.0 🔻

6. Toward 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.

DHCP Server	
	Enable DHCP Server  Enable DHCP Server on this zone
	Start 192.168.12.100
	End 192.168.12.249
	Lease time 12h
	Expiry time of leased addresses, such as, 7d or 12h or 60m. minimum is 2 Minutes (2m).

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**.



### WAN 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)

#### DHCP

By default, the router connects 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 over the **Network** menu, then click **Network Zones**.

Status	Network	Services	Maintenance	BakPak	Logout
Dashboard	Port Forwarding/1:1 NAT	UPNP	Username/Password	Registration	
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics	Maintenance	
System Log	Network Zones	File Sharing	Remote Access		
System Report	DHCP Reservation	Media Server	Time Zone		
	Static Routes	SNMP	Configuration		
	Dual-Wan	Parental Controls	Firmware Ne		
	Quality of Service	VPN	LEDs		
			Reboot		

2. Click Edit for the WAN zone.

Network Zones						
Interface Zones						
Type: Address: Netmask: Gateway: DNS 1: DNS	WAN Wan DHCP 255:255:254.0 90: 999:53 G8 11:22 G8 2d 22h 9m 1s	Type: MAC-Address: Received: Sent: Uptime:	WAN2 Wan2 DHCP 90: 0.00 B 0.00 B 0.00 B 0.00 B	Address: Netmask: MAC-Address: Received: Sent: Uptime:	LAN 192.166.250.1 255.255.0 90: 1221.68 395.46.68 20.22h 10m 11s	1901ATED GUEST 1902.168.125.1 255.255.0550
Edit Refresh Disconnect		Edit Ref	fresh Disconnect		Edit	
			-0			0—

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

Type: dhcp Address: Netmask: 255.255.254.0 Gateway: DNS 1: DNS 2: Uptime: 2d 22h 11m 52s MAC-Address: 90: Received: 399.84 GB Sent: 11.23 GB
Static address 👻
Static address DHCP PPPoE Default MAC Address

- 4. Click Switch Protocol to confirm.
- 5. Enter the **IP address, subnet mask, Default Gateway**, and **DNS Server** provided by your ISP.
- 6. Select **custom** from the netmask drop-down menu to enter a custom subnet mask.

- Protocol Static address ▼ Static address DHCP PPPoE IPv4 Subnet Netmask 255.255.240 ▼ IPv4 Gateway 64.183.16.33 Use Custom DNS Servers 8.8.8.8 + Override MAC Address SIP ALG Enable ▼
- 7. Click **Apply**. The router now has the static IP configured.

#### PPPoE

#### To configure the router using a PPPoE connection:

1. Hover over the **Network** menu, then click **Network Zones**.

Status	Network	Services	Maintenance	BakPak	Logout
Dashboard	Port Forwarding/1:1 NAT	UPNP	Username/Password	Registration	
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics	Maintenance	
System Log	Network Zones	File Sharing	Remote Access		
System Report	DHCP Reservation	Media Server	Time Zone		
	Static Routes	SNMP	Configuration		
	Dual-Wan	Parental Controls	Firmware Ne		
	Quality of Service	VPN	LEDs		
			Reboot		

#### 2. Edit the WAN Zone.



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



- 7. Provide the following information:
- 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** field, enter the DNS server you would like to use. For example, you can use 8.8.8.8.
- Keep all other settings as they are.
- 8. Click **Apply** when finished. The router is now set up for PPPoE.

Status	Type: pppoe Received: 0.00 B Sent: 0.00 B	
Protocol	PPPoE *	
PAP/CHAP Username		
PAP/CHAP Password		Ð
Use custom DNS servers		+
MTU	1492	
Disable PMTU		
Override MAC Address	90:A7:C1:97:03:2F	
SIP ALG Enable		

### 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. Hover over the **Network** menu, then click **Network Zones**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

2. In the LAN zone square, click **Edit**.

	LAN 2 3 4
Address: Netmask: MAC-Address: Received: Sent:	192.168.1.99 255.255.255.0 90:A7:C1:97:03:2D 387.26 MB 1.79 GB
Uptime:	0h 36m 21s
	Edit

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

IP Address	192.168.10.99
Netmask	255.255.255.0

4. In the **DHCP Server** section, the **Lease time** field allows you to view/modify DHCP IP address lease time, and the **DNS** field lets you specify the DNS address that will be handed out to client devices by DHCP.

**Note:** In the *Lease Time* field, 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**.

E de c	<ul> <li>Expiry time of leased addresses, such as, 7d or 12h or 60 Minimum is 2 Minutes (2m)</li> <li>DNS</li> <li>DNS used by this network zone</li> </ul>
Enot Ded Address	DNS by this network zone
Sheek ID-d Address	
Short ID-4 Address	
Start IPV4 Address	End IPv4 Address
192.168.1.100	192.168.1.198

Further down on the page, the **Start IPv4 Address** field indicates the first IP address that will be handed out by the router. The **End IPv4 Address** field indicates the last IP address that will be handed out. You can also click **Add New Item** to specify up to four additional address ranges.

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

### 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. Hover over the **Network** menu, then click **Network Zones**.

Status	Network	Services	Maintenance	BakPak
Dashboard	Port Forwarding/1:1 NAT	UPNP	Username/Password	Registration
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics	Maintenance
System Log	Network Zones	File Sharing	Remote Access	
System Report	DHCP Reservation	Media Server	Time Zone	
	Static Routes	SNMP	Configuration	
	Dual-Wan	Parental Controls	Firmware Net	
	Quality of Service	VPN	LEDs	
			Reboot	

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



You will get a message telling you that port 5 will be turned into the Isolation Guest network port.

3. Click **OK** to enable the isolated guest network.

### DNS

At the bottom of the WAN Zone page are DNS settings.

#### **DNS forwarding**

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

DNS forwardings	example.org	+
	List of DNS servers to f	orward requests to

#### **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.



### DHCP reservation

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

#### To create a DHCP reservation:

1. Hover over the **Network** menu, then click **DHCP Reservation**.



2. Click Add New Item.

DHCP Reservation				
Hostname	MAC-Address	IPv4-Address		
	This section contains no values yet			
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.

DHCP Reservation		
Hostname	MAC-Address	IPv4-Address
laptop	21448-4449-(220428-08-8	192.168.100.116 <b>v</b> Delete
	Add New Item	

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.

### Static routes

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. Hover over the **Network** menu, then click **Static Route**.



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).

2. First click Add New Item.

This section contains no values yet

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 (192.168.1.11). 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.

Target IP address	Target Netmask	Gateway	Zone	Metric	
192.168.222.0	255.255.255.0	192.168.1.111	LAN T	0	Delete
		Add New Item			

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

### 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. Hover over the **Network** menu, then click **Dual WAN**.



2. Select **Enable**. WAN1 will now check connectivity every five 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.

Dual-WAN Dual-Wan allows for the use of two Enabling Dual WAN will change por	wan ports. 12 to WANZ, Any devices currently connected on that port will be disrupted.
	Enable 🗹
	WAN
	Health Monitor Interval 5 sec.   Attempts Before WAN Recovery 3
	WANZ
	Health Monitor Interval 5 sec.
	Apply Clear Changes

3. Click Apply to finalize the settings.

## 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. Hover over the **Network** menu, then click **Quality of Service**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

2. Check Enable.

Enable 🖉	
Download speed limit (mbit/s) 25	
Upload speed limit (mbit/s) 10	

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.



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



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.

Priority Sou	ource host Destinatio	n host	Service	Protocol	Ports	Sort
Med 🔻	all all all .168.255.100	•	all	UDP 🔻	5060 💌	▲ ▼ Delet
192. 192. ci	12.168.1.99 12.168.1.49 custom	Add	New Item			

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.

Priority Source host	Destination host	Service	Protocol	Ports	Sort
Med 💌 all 👻	all 192.168.255.100	all	UDP 💌	5060 💌	▲ ▼ Delete
	192.168.1.99 192.168.1.49 custom	Add New Item			

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.



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.



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

Priority	Source host	Destination host	Service	Protocol	Ports	Sort
Med 💌	all	all 🔻	all 💌	UDP 💌	5060	▲ ► Delete
			Add New Item		custom	

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

Priority Source host	Destination host	Service	Protocol	Ports	Sort
Med 💌 all 💌	all	all 🔻	UDP 🔻	5060	▲ ▼ Delete
		Add New Item		Ν	

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**.

Priority	Source host	Destination host	Service	Protocol	Ports	Sort	
High	192.168.1.34 💌	all	ali	all	all	▲ ▼ Delete	
			Add New Item				

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

By default, there is a rule defined to allow priority of Voice Over IP (VOIP) data.

Priority	Source host	Destination host	Service	Protocol	Ports	Sort
Med 💌	all	all 🔻	all 🔻	UDP 💌	5060 💌	▲ ▼ Delete
			Add New Item			

# Services menu

## 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. Hover over the *Services* menu, then click **UPnP**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

2. Select the Start UPnP option, then click Apply to finalize the settings.



## Dynamic DNS

### Pakedge DDNS

Dynamic DNS (**DDNS**) allows your router to be reached with a fixed hostname while having a dynamically changing IP address. In order for this to work your Pakedge router must not be placed behind another firewall/router device. 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. It is not required to have a Bakpak hardware device running on the network in order to use Pakedge DDNS. To create a Pakedge DDNS take the following steps. BakpakDDNS is only available on the RE-2 and RK-1.

#### To create a Pakedge DDNS:

1. Hover over the **Services** menu, then click **Dynamic DNS**.



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

Enable 📝
Status Check

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

BakPak Email	user@test.com					
BakPak Password	••••••	Ì				
Change						

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**.

BakPak Email		
BakPak Password		Đ
Login	egister	

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.

HostName	site1	.bakpakddns.com
Check Availability	Claim Hostname	

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.

Enable 🔽	
Status Check	
Command Result:Success Name is available	*
	Ŧ

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

HostName	site1	.bakpakddns.com
Check Availability	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.

Enable 🕼	
Status Check	
Command Result:Name Claimed.	*
	Ŧ

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

Enable 🕑
Status Check

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

Enable 📝	
Status Check	
Command Result:Success IP is HostName is site1 Updated at Wed Dec 3 23:28:31 PST 2014	1
	Ŧ

You can change the hostname you are using at any given time by entering a new hostname into the router that is available for use and then clicking claim **hostname**.

You can change the BakPak user on the router at any given time by entering the new credentials and clicking **Change**.

BakPak Email	support() paintings and		
BakPak Password	•••••	Ð	
Change			

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



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

### Non-Pakedge DDNS

#### To configure a non-Pakedge DDNS:

1. Hover over the **Services** menu, then click **Dynamic DNS**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

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.

PROF	LE1
Enable	
Service	dyndns.org
Hostname	mypersonaldomain.dyndns.
Username	myusername
Password	••••••

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 Check the unit of time that is used for the Check the unit of time that is used for the Force update every field. Click Apply.

Source of IP address	URL -
URL	http://checkip.dyndns.com/
Check for changed IP every	10
Check-time unit	min 🔻
Force update every	72
Force-time unit	h 💌
Click 'Add' button to add more DDNS	

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.

Click 'Add' button to add more DDNS
Add

# 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.

### Local file sharing

#### To configure local file sharing:

1. Hover over the **Services** menu, then click **File Sharing**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

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

Local File Sharing			
	Enable File Shares	V	
	Hostname	RE-2	
	Description	RE-2 Router	
	Workgroup	WORKGROUP	
	Username	pakedge	
	Password	•••••	•
	Read-only		

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

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**.

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.

Enable File Shares	V
Hostname	RE-2
Description	RE-2 Router
Workgroup	WORKGROUP
Username	pakedge
Password	••••••
Read-only	

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.

	Enable File Shares			
	Hostname	RE-2		
	Description	RE-2 Router		
	Workgroup	WORKGROUP		
	Username	pakedge		
	Password	•••••	•	
	Read-only			
Disk Nam	c	USB Po	rt	Enable

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

Disk Name	USB Port	Enable
AdataUSB	USB 2(USB 3.0 port)	V

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

### Remote file access

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.

Local File Sharing Remote Fi	le Access		
Remote File Access			
You can access your files on the USE	3 disk by https://site1.bakpakdans.com:8443/mydisk.html		
	Enable Remote File Access		
	Username	fileshare	
	Password	•••••	0

2. Select Enable Remote File Access.

Enable Remote File Access		
Username	fileshare	
Password	•••••	Ð

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**.

Enable Remote File Access	<b>V</b>	
Username	fileshare	
Password	pakedger	Ð

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

You will see a login screen similar to when you log in to the router. Enter the credentials and click **Log in**. You will see the USB drive listed.

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**.

Upload	
Folder to create:	
Create Folder	
Folder one	Delete

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

Upload
Folder to create:
Create Folder
File1.txt Download 0 KB - Date Modified: 12/05/2014 06:17 PM Delete

6. Click **Download** to retrieve the file from the USB drive. You can also click **Delete** to remove it.



7. You can upload a file onto the USB drive remotely. Click **Upload**.

- 8. Navigate to the file you want to upload and select it.
- 9. Click Upload.

Choose a file to upload:
file2.txt
Upload
Folder to create:
Create Folder

Upload	
Folder to create:	
File1.txt 0 KB - Date Modified: 12/05/2014 06:17 PM	Download Delete
<b>file2.txt</b> 0 KB - Date Modified: 12/05/2014 06:29 PM	Download Delete

Your file will now be on the USB drive.

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

Upload	
Create Folder	
File1.txt 0 KB - Date Modified: 12/05/2014 06:17 PM	Download Delete
file2.txt 0 KB - Date Modified: 12/05/2014 06:29 PM	Download Delete

The folder is now displayed.

C	Folder two	Delete
Ļ	File1.txt 0 KB - Date Modified: 12/05/2014 06:17 PM	Download Delete
Ļ	file2.txt 0 KB - Date Modified: 12/05/2014 06:29 PM	Download Delete

11. To return to the previous folder, click the **Back** button.

RE-2 fileshare / 2-1 Al	DATA ADATA USB Flash Drive / Folder one	
← Back		
Folder two		
	-	Upload
	Folder to create:	

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

Logout	
<u>RE-2 fileshare</u> / 2-1 Al	DATA ADATA USB Flash Drive / Folder one
🗋 Folder two	
	Upload

13. Finally, click **Log out** to log out of the file share.

### Mapping network drives

The following section shows 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** on the menu bar at the upper left.

Finder	File	Edit	View	Go	Window	Help

2. Click Connect to Server.



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

000	Connect to Server
Server Address:	
smb://192.168.1.99	+ 07
Favorite Servers:	
? Remove	Browse Connect

You will be prompted to log in as a **guest** or **registered user**.

4. Select **registered user**, then enter the credentials you have configured on the router.

Enter your name and password for the server "192.168.1.99".
Connect as: O Guest
<ul> <li>Registered User</li> </ul>
Name: pakedge
Password: •••••
Remember this password in my keychain
Cancel Connect

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

#### Windows 7 & 10

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

- 1. Windows 7: Click the start button at the bottom-left, then click **Computer**.
  - OR -

Windows 10: Click the start button at the bottom-left, type "this PC," then click **This PC**.



2. Click Map Network Drive.

		- • • ×
🔾 🗸 🖓 🗸 Comput	er > v 4 j Search Computer	Q
Organize 🔻 System p	roperties Uninstall or change a program Map network drive Open Control Panel	8 · 🗋 🔞
★ Favorites ■ Desktop ₩ Downloads ₩ Recent Places	Hard Disk Drives (2)     Creates a shortcut to a shared folder     ork.     15.8 GB (ree of 45.5 GB     148 GB free of 186 GB     Devices with Removable Storage (1)	
Eibraries Documents Music Fictures Videos	7.44 GB free of 7.44 GB	
Reference to the second		

- 3. Click Browse.
- 4. Click the **RK-1** icon to expand it, then click the folder you want to map underneath it to select it. Click **OK**.

Browse For Folder	×
Select a shared network folder	t
🗣 Network	
▲ P RE-1 ▲ P shared	
Shared Files      WINDOWSBOOTCAMP	
N	
hà	4
Make New Folder OK Cancel	

5. Select **Connect using different credentials**, then click **Finish**.

🕞 🧟 Map Ne	etwork Drive
What ne	twork folder would you like to map?
Specify the	drive letter for the connection and the folder that you want to connect to:
Drive:	Z: •
Folder:	\\RE-1\shared
	Example: \\server\share
	Reconnect at logon
	Connect using different credentials
	Connect to a Web site that you can use to store your documents and pictures.
	N
	Finish Cancel

6. Enter the username and password to access the folder, then click **OK**. You now have access to the files on the USB drive.

#### Windows XP

#### To map a USB drive in Windows XP:

- 1. Click My Computer, then Tools, then click Map Network Drive.
- 2. Click Tools > Map Network Drive.

My Computer		
File Edit View Favorites	Tools Help	
🕜 Back - 🕥 - 🏂	Map Network Drive Disponeet Network Drive Synchronize	
Address g My Computer	Folder Options	<b>U U U</b>
System Tasks	*	
View system information	Shared Documents test's Documents	
Change a setting	Hard Disk Drives	
Other Places	Local Disk (C:)  Devices with Removable Storane	
Control Banal		
Details	DVD/CD-RW Drive (D:)     ADATA (E:)	
My Computer System Folder		

- 3. Click **Browse**, select the folder you want to map, then click **OK**.
- 4. Click Finish.
- 5. Enter the router's credentials to access the folder.

Your folder is now mapped on your computer.



# Media server

Media server 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. Hover over the **Services** menu, then click **Media Server**.

Status	Network	Services	Maintenance
Dashboard Real-time Monitoring System Log	Port Forwarding Virtual DMZ Network Zones DHCP Reservation	IGMP Snooping Dynamic DNS UPNP Media Server	Username/Password Diagnostics Remote Access Time Zone
	Static Routes Quality of Service Dual-Wan	Parental Controls File Sharing SNMP VPN	Configuration Firmware Reboot

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.

Media Server	
,	
Enable:	<b>V</b>
Port:	8200
	Port for HTTP (descriptions, SOAP, media transfer) traffic.
Friendly name:	RE-2 MediaServer
	Set this if you want to customize the name that shows up on your clients
Root container:	Standard container

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

# 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. Hover over the **Services** menu, then click **SNMP**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Parental Controls	Diagnostics
	Network Zones	Dynamic DNS	Remote Access
	DHCP Reservation	SNMP	Time Zone
	Dual-Wan Location	File Sharing	Configuration
	Quality of Service	UPNP	Firmware
		Media Server	Reboot
		VPN	

On this page, you will see all of the SNMP options.

2. Make any necessary changes, then click **Apply**.

SNMP SNMP is a standard TCP/IP protocol fo	r network management.	
	Location	MyLocation
	Contact	MyContact
	Description	Pakedge RE-2 Router

# Parental controls

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

### Block websites

#### To block websites by device:

1. Hover over the **Services** menu, then click **Parental Controls**.

Status	Network	Services	Maintenance
Dashboard Real-time Monitoring System Log	Port Forwarding Virtual DMZ Network Zones DHCP Reservation	IGMP Snooping Dynamic DNS UPNP Media Server	Username/Password Diagnostics Remote Access Time Zone
	Static Routes Quality of Service Dual-Wan	Parental Controls File Sharing SNMP VPN	Configuration Firmware Reboot

Two tabs are on this page. One is **Block Websites** and the other is **Block Clients**.



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

Websites such as facebook.com or youtube.com	Client(s) that will be blocked to access this webiste
This section	contains no values yet
Ac	ld New Item

3. Enter the name of the website that you want to block. In this example, we will block <u>www.yahoo.com</u>. Towards the right side of the screen you can select the device that you want to block the website for. You can select **all clients** to apply it to every device on the network.

Websites such as facebook.com or youtube.com	Client(s) that will be blocked to access this webiste	
www.yahoo.com	all clients  +	Delete

4. To continue adding websites, click Add New Item.

Websites such as facebook.com or youtube.com	Client(s) that will be blocked to access this webiste
www.yahoo.com	all clients  + Delete
[	Add New Item

5. Click **Apply** when you are finished. The websites you entered are now blocked.

Websites such as facebook.com or youtube.com	Client(s) that will be blocked to access this webiste	
www.yahoo.com	all clients +	Delete
www.facebook.com	all clients  +	Delete

6. 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.

Enable V If you enable block websites, IP address 192.168.100.98 will also ha used by this Router, Please do not use it on other devices	
If you enable block websites, IP address 192.168.100.98 will also be used by this Bouter, Please do not use it on other devices.	Enable 🗹
also be used by this Router. Please do not use it on other devices	If you enable block websites, IP address 192.168.100.98 will
also be used by this houten i rease do not use it off other devices.	also be used by this Router. Please do not use it on other devices.

**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.

#### Block clients

The Block Clients feature allows you want to block certain client services from accessing the internet.

To block a client's services from accessing the internet:

- 1. Hover over the **Services** menu, then click **Parental Controls**.
- 2. Click Block Clients.

Block Websites Block Clients	]						
Blocked Clients							
Description	nts/Devices	Protocol Ports	Start Time	Stop Time	Sun Mon	Tue Wed	Thu Fri Sat
			This section contains	no values yet			
			Add New	Item			

3. Click Add New Item in the bottom box.

Description	Clients/Devices	Protocol	Ports	Start Time	Stop Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
This section contains no values yet													
				Add Net	w Item								

- 4. Enter a name in the **description** field.
- 5. 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.

Description	Clients/Devices	Protocol	Ports	Start Time	Stop Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
Test Computer	Please choose	TCP+UDP 💌		00:00 AM	00:00 AM								Delete
	custom		Add New Item										

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

		BI	locked Clients									
Description	Clients/Devices	Protocol	Ports	Start Time	Stop Time	Sun	Mon	Tue	/ed Thu	Fri	Sat	
Test Computer	Theory of a Distance of the	TCP+UDP TCP+UDP TCP		00:00 AM	00:00 AM							Delete
		UDP	Add New Item									

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.

	Cilens/ Devices	Protocol		Start Time	stop time	sun	Tue				Sat
Test Computer	Terry In California (1996)	TCP+UDP -	80	• MA 00:00	00:00 AM		2	23	2	2	2

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.

6. Click **Apply** towards the bottom to finalize the settings.

Description	Clients/Devices	Protocol	Ports	Start Time	Stop Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Test Computer	fampuir faithir is being 🖌	TCP+UDP	80	12:00 PM 🔻	06:00 PM 💌							

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

Description	Clients/Devices	Protocol	Ports	Start Time	Stop Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Child PC		All		• MA 00:00	• MA 00:00		V					Dele

### VPN

#### PPTP

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 PPTP VPN:

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

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

2. Select Enable.

PPTP Server		
PPTP Server Use this Router as a PPTP Server		
	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.

User Name		Password		
pakedge		pakedgev	Ð	Delete
	Add New Item			

- 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.

User Name		Password	
pakedge		pakedgev	Delete
	Add New Item	]	

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

User Name		Password		
pakedge		•••••	0	Delete
vpnuser		•••••	0	Delete
	Add New Item			

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 the **Services** menu, then click **VPN**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

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

OpenVPN Server PPTP Server PPTP Passthrough	
OpenVPN Server Use this Router as an OpenVPN Server	
	Enable
	Local Gateway Address 64.183.16.40
	If your WAN is using a Dynamic IP address (one that may change) it is highly recommended to use a Dynamic DNS address like Bakpakdns. Otherwise when the WAN IP changes, you will have to redownload the configuration file to allow each remote user to connect again.
	Server IP 10.8.0.0
	Server Netmask 255.255.255.0 •
Client Name	Configuration
	This section contains no values yet
	Add New Item
	Apply Clear Changes

- 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.
- **OpenVPN Subnet:** 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).

- **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.
- 3. 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

OpenVPN-GUI is a popular, free, OpenVPN client for Windows.

#### To Use OpenVPN-GUI:

- 1. Download OpenVPN-GUI <u>here</u> and install it on your Windows PC.
- 2. Download the Routers OpenVPN configuration file and save it to your computer.
- 3. To use the OpenVPN configuration file, it must be saved into the OpenVPN configuration folder. This folder can be found in one of two places depending on if you installed the 32 or 64 bit verion of OpenVPN-GUI.
  - a. The 32-bit version will be located in C:\Program Files (x86)\OpenVPN\config
  - b. The 64-bit version will be located in C:\Program Files\OpenVPN\config

File       Home       Share       View         Image: Share	📙   🛃 📙 🖛   config						
Image: Copy Paste Pin to Quick Copy To To Torganize       Image: Copy Pin to Quick Copy To Torganize       Image: Copy Pin to Quick Copy Torganize       Image: Copy Pin torganize </th <th>File Home Share</th> <th>View</th> <th></th> <th></th> <th></th> <th></th> <th></th>	File Home Share	View					
Clipboard     Organize     New     Open     Select       ←     →     ↑     →     >     Program Files (x86) → OpenVPN → config	Image: Pin to Quick accessCopyPaste	X Cut ≌ Copy path Paste shortcut	Move Copy to - Copy	New folder	item <del>•</del> access •	Properties	Select all Select none Invert selection
← → ∽ ↑ → This PC → OS (C:) → Program Files (x86) → OpenVPN → config	Clipboard		Organize	New		Open	Select
Name Otto modified Tune Size	← → × ↑ 📙 > Th	his PC > OS (C:) >	Program Files (x86) > OpenVPN	l → config			
Outer access	Ouick access	Name	^	Date modified	Туре	Size	
☐ RE-2T091411085-RemoteUser001.ovpn 10/13/2016 1:07 PM OVPN File 10 KB	A Guick access	RE-2T091411	1085-RemoteUser001.ovpn 1	0/13/2016 1:07 PM	OVPN Fi	le 1	0 KB
6 OneDrive README.txt 10/13/2016 12:58 Text Document 1 KB	🐔 OneDrive	README.txt	1	0/13/2016 12:58	Text Doc	ument	1 KB
This PC	💻 This PC						
Desktop	Desktop						

- 4. After placing the configuration file in the config folder, right click on the OpenVPN-GUI tray icon at the bottom righthand corner of your screen.
- 5. From the menu, click **Connect**.

#### OS X

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

#### To use Tunnelblick:

- 1. Download Tunnelblick <u>here</u>, save it to your computer, and install Tunnelblick.
- 2. Download the Routers OpenVPN configuration file and save it to your computer.

3. Double-click the **.ovpn** file you downloaded. A dialog opens asking you for your configuration preference. You can choose to install the OpenVPN configuration for all users or just your account.

(PF)	Install Configuration For All Users? Do you wish to install the 'RE-2T091411085-OS_X_User' configuration so that all users can use it, or so that only you can use it?
	All Users Cancel Only Me

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

Tunnelblick • Install or	needs to: ne configuration
User Name:	support
Password:	•••••
	Cancel OK

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





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

#### iOS

**OpenVPN Connect** is a free OpenVPN client for iOS devices.

#### To Use 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 **Copy to OpenVPN** and the OpenVPN Connect app should open automatically.



4. Tap "+" to import the profile.

	NEW PROFILES ARE AVAILABLE	
	1 new OpenVPN profile is available for import.	2
	/RE-2T091411085-iOS_User Autologin profile	
5.	Tap <b>Connection</b> to connect to the VPN.	
	OpenVPN Connect	

OpenVP	'N Connect	
Profile	/RE-2T091411085-iOS_User Autologin profile	>
Status	Disconnected	>
Connection	$\bigcirc$	

If connected successfully, you should see the notice that your connection is active:

၇ OpenVl	PN Connect	
Profile	/RE-2T091411085-iOS_User Autologin profile	
Status	Connected	>
Connection		
CONNECTION DE	TAILS	
Duration	Last packet received < 1 second ago	
Bytes In 3.	21 KB Bytes Out 2.37 KB +	

#### Android

**OpenVPN Connect** is a free OpenVPN client for Android devices.

#### To use OpenVPN Connect:

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



- 2. Open the email you sent yourself with the config file on your Android device and tap the attached file. Save it to your SD card
- 3. Open the OpenVPN Connect app, tap its More/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. Tap Connect.



6. Allow permission to run OpenVPN by tapping **OK**.



You are connected to OpenVPN.

OpenVPN Connect	MORE
<b>OpenVPN Profile:</b> 64.183.16.40 [RE-2T091411085-0p	•
OpenVPN: Connected	
Disconnect	
Connection stats:Duration0:00:06Packet received< 1 second agoBytes in69.95 KBBytes out23.93 KB	
Tap for more detail	
Your Secure and Private Pa the Internet https://www.privatetunnel.	ath to . <u>com/</u>
VPN Solution for your Busi http://openvpn.net/as/	ness

# Maintenance menu

# Username/Password

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

#### To change the password:

1. Hover over the **Maintenance** menu, then click **Username/Password**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

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.

Administration Change the administrative username/password for the device.			
	Username	pakedge	
	Password		D
	Confirmation		0

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

Administration
Change the administrative username/password for the device.
Username sysadmin

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. Hover over the **Maintenance** menu, then click **Diagnostics**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

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. Hover over the Maintenance menu, then click Diagnostics.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

2. Click **traceroute**. If you want to perform a traceroute to a different website or IP address, you may enter that instead.



After a few moments, the traceroute results are 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. Hover over the Maintenance menu, then click Diagnostics.



2. Click **NSlookup**. If you want to do an NSlookup for a different website, you can type that in instead.



After a few moments, your NSlookup results are 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. Hover over the Maintenance menu, then click Remote Access.



You can type a new port number into the **Secure Web Access Port** field if you want to change it from its default. You can also disable remote access altogether if you deselect **Enable Secure Web Access**.

Enable Secure Web Access 🐨
Secure Web Access Port 8443
Specifies the listening port of Secure Web Access
Enable Support Access 👿

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

Er	nable Secure Web Access	V	
	Secure Web Access Port	8443	
		Specifies the listening port of Secure	Web Access
	Enable Support Access		

2. 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. Hover over the **Maintenance** menu, then click **Time**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

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

Time Zone This page allows you to setup time z	zone.	
		Local Time Thu Dec 4 17:05:48 2014 Timezone America/Los Angeles 🗸

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

# Configuration

The **Configuration** page allows you to reset the router to its factory default settings, download the current configuration file, or restore a configuration.

### Factory defaults

#### To reset the router to factory default settings:

1. Hover over the **Maintenance** menu, then click **Configuration**.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

#### 2. Click Factory Default.

Configuration Click Download Configuration to backup the configuration to your computer.
Download backup : Download Configuration Reset to defaults : Factory Default
To restore a configuration file click Browse and choose the configuration file and then click Restore.
Restore backup : Browse. No file selected.
Restore

The router now resets to factory default settings. You can also do this by pressing the pinhole reset button on the back of the router. Hold down this button for 10 seconds while the router is powered on, and then release it. The router then resets to factory default settings.

### Download configuration

#### To make a backup of your configuration:

1. Hover over the Maintenance menu, then click Configuration.

Status	Network	Services	Maintenance
Dashboard Real-time Monitoring	Port Forwarding Virtual DMZ	IGMP Snooping Dynamic DNS	Username/Password Diagnostics
System Log	Network Zones	UPNP Media Server	Remote Access Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Duai-Wan	VPN	KEDOOT

2. Click **Download Configuration**, then specify the download location.

Configuration Click Download Configuration to backup the configuration to your computer.	
	Download backup : Download Configuration
	Reset to defaults : Factory Default

The configuration file is downloaded to your computer.

### Restore configuration

#### To restore a configuration from a previous backup:

1. Hover over the **Maintenance** menu, then click **Configuration**.


2. Click Browse and select your configuration backup file.

Configuration Click Download Configuration to backup the configuration to your computer.	
	Download backup : Download Configuration Reset to defaults : Factory Default
To restore a configuration file click Browse and choose the configuration file and	i then click Restore.
	Restore backup : <b>Browse</b> No file selected.
	Restore

#### 3. Click Restore.

Configuration Click Download Configuration to backup the configuration to your computer.	
Download backup : Download Configuration Reset to defaults : Factory Default	
To restore a configuration file click Browse and choose the configuration file and then click Restore.	
Restore backup : Browse No file selected.	
Restore	

The router uploads your configuration file and reboots.

### Firmware

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

#### To update the firmware:

1. The current firmware version of the router is displayed toward 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.

	18 Active Sessions Uptime: 33d 7h 44m 59s	O% CPU Usage	2% Memory Usage	
New firmware (1.00) is available to download Download Now				

You can also manually download the latest firmware from the Dealer Portal.

2. Click **Firmware**.



3. 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 reset to factory default settings, then reboot to the new firmware and the router's factory defaults.

Firmware
To update firmware, Browse to the firmware image in your local disk and click Local Update or just click Check Update.
Keep settings 🗹 Local Image <b>Browse</b> No file selected.
Local Update
Get new firmware from internet Check Update

The firmware update takes a few minutes to complete.

4. The **Check Update** option forces the router to pull the latest firmware available and update itself.



### LEDs

For aesthetics, you can turn off the router's LEDs.

#### To turn off LEDs:

1. Hover over the Maintenance menu, then click LEDs. The LEDs screen opens.

2. Select Turn off all LEDs, then click Apply.

### Reboot

#### To reboot the router:

1. Hover over the Maintenance menu, then click Reboot.

Status	Network	Services	Maintenance
Dashboard	Port Forwarding	IGMP Snooping	Username/Password
Real-time Monitoring	Virtual DMZ	Dynamic DNS	Diagnostics
System Log	Network Zones	UPNP	Remote Access
	DHCP Reservation	Media Server	Time Zone
	Static Routes	Parental Controls	Configuration
	Quality of Service	File Sharing	Firmware
	Dual-Wan	SNMP	Reboot
		VPN	

2. Click **Reboot**. The router reboots.

Reboot Clicking Rebo	oot will restart the router
Reboot	

# BakPak menu

## Registration

### To register your device to BakPak:

- 1. Hover over the **BakPak** menu, then click **Register**.
- 2. Follow the on-screen prompts to complete the registration.

### Maintenance

### BakPak upgrade

#### To upgrade the BakPak agent to a new version:

- 1. Obtain the firmware update file.
- 2. Hover over the **BakPak** menu, then click **Maintenance**.
- 3. Click **Choose File**, select the file, then click **Upgrade**.

### Unregister from BakPak

You can unregister the agent from BakPak, then re-register it under a different account. You can also only stop BakPak monitoring services, for example, when you have another management agent such as an NK-1 monitoring the network.

#### To unregister from BakPak and re-register it under a different administrator:

1. Hover over the **BakPak** menu, click **Maintenance**, then click **Unlink and Register**.

**Caution:** Clicking Unlink and Register removes any profiles created under this BakPak agent.

#### To stop BakPak services:

- 1. Hover over the **BakPak** menu, click **Maintenance**, then click **Stop Services**. The agent is still registered, but it's not monitoring.
- 2. To restore services, click **Restore Services**.

## Appendix A: Specifications

Item	Description
Summary	
Fixed ports	7
LED Indicators	USB, 1000M and Link/Act LED, PWR
Input voltage	100V~240VAC, 0.9A, 50/60 Hz
Power consumption	15.4W
Operating temperature	32°F to 104°F (0°C to 40°C)
Storage temperature	14°F to 158°F (-10°C to 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
Wweb	Supports web management
SNMP	Supports System configuration with SNMP v1/v2
System log	Supported
Configuration file	Supports download/upload configuration file
download/upload	
Upgrade firmware	Supports online upgrade
Debug	
Ping	Supported
Traceroute	Supported
NSlookup	Supported
Mechanical	
$L \times W \times H$	267 × 165 × 51 mm (10.5 × 6.5 × 2 in.)
Weight	1.81 kg (4 lbs)



# 11734 Election Road Draper, UT 84020 U.S.A

Visit us at:

### www.pakedge.com

Copyright ©2018, Control4 Corporation. All rights reserved. Control4, Pakedge, Triad, and their logos are registered trademarks or trademarks of Control4 Corporation in the United States and/or other countries. 4Store, 4Sight, Control4 My Home, Mockupancy, and BakPak are also registered trademarks or trademarks of Control4 Corporation. Other names and brands may be claimed as the property of their respective owners. All specifications subject to change without notice.

DOC-00183-D; 200-00533-D 2018-09-05 MS