

RK-1 7-Port Dual-WAN Gigabit Router User Guide



Introduction	4
Technical Support	4
Installing	4
Getting to know your product	5
Accessing the router	7
First-time login	8
Saving changes	8
Configure	9
Overview	11
Connections	12
Interfaces	13
Edit interface settings	13
Completing the dialog	14
Edit WAN Settings	14
Select a mode	14
Configure DNS Settings	15
DHCP	16
Static	17
PPPoE	17
Dual-Stack Lite	18
L2TP	19
Edit LAN/VLAN Settings	19
Backup/ Restore	23
Logs	
Reset to factory default settings	
Reset using the interface	
Reset using the physical RESET button	25
Advanced	26
OvrC	27
Device Settings	. 28
Enable settings	28
Settings	
Diagnostic Tools	
Factory Defaults	
DHCP Reservation	
Add a new reservation	
Manage DHCP entries	33
Remove reservations	
Dual WAN	
Dynamic DNS	
Pakedge Dynamic DNS	
Non-Pakedge DDNS	
Complete the dialog	.40

Add a secondary DDNS profile	41
Edit or delete a Dynamic DNS entry	
Firewall	
Global Settings	
Forwards	
Add new policy	
Add Firewall Policies	
Firmware	
Multicast Routing	
Complete the Multicast rule dialog	
NAT (Port Forwarding)	
Complete the NAT Policy dialog	
Parental Controls	
Block websites	
Schedule Internet	
Complete the Internet Schedule dialog	
QoS	
Restrict WAN upload and download speeds	60
Add a QoS priority setting	61
Complete the Add Priority dialog	
Static Routes	
VLAN Port Settings	
VPN	
Configure OpenVPN	
Enable the OpenVPN Server	
Create OpenVPN user profiles	
Set up the OpenVPN user profile	
OpenVPN client setup for Windows, iOS, Android	
Windows	
iOS	
Android	
Configure PPTP	
Configure PPTP Passthrough	

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

For technical support, refer to the information on the back of the Quick Start Guide.

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

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 pkdge.co/rk1-qsg. You can also visit the Dealer Portal for all the current manuals and Quick Start Guides.

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

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

Getting to know your product

Package contents:

- RK-1router
- 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 1below for more information. Table 1: LED definitions (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 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	5-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 http://192.168.1.99 or 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 **Sign in**.

	Pakedge RK-1	
Username		
Password		
		C.C.C.
	Sign In	

Important: You must change this default password. For instructions, see Username/ Password.

First-time login

The first time you log in, you are brought to the *Configure* tab. Here you can change your username and password (required), and specify the device's network information and network protocol.

For OvrC setup instructions, see the *Quick Start Guide* that came with the router or go to pkdge.co/rk1-qsg.

Saving changes

After logging in, you can edit your settings on many tabs.

Important! You must click **Apply** to save your changes. Changes will not be saved to the router until you click **Apply** at the top of the tab.

					Cancel	Apply
Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
LEDs	UPnP	Enable				
WAN Acce HTTPS	Port	Enable Sup	port Access	Port		
En	able 8443	E	nable	2223		

Configure

The *Configure* tab allows you to change the most common router settings in one screen. This is the default tab that displays after logging in.

Overview	Connections		onfigure	Inter	faces	Backup/Re	store	Logs	Advanced
dit Login Credentials									
sername	Cur	rent Password			New Password			Confirm New Password	
education				R			R		5
eneral Device Information									
iendly Device Name			Device Location						
Pakedge RK-1									
evice Settings									
me Zone	16:43:30 Th	u Apr 1 2021							
America/New York		*							
/AN1									
ode									
DHCP		*							
Address			Subnet Mask				Gateway		
4S Server 1			DNS Server 2						
AN									
Address	Sub	net Mask			DHCP Start			DHCP End	
192.168.10.1		55.255.255.0			192.168.10.100			192.168.10.198	

- Edit Login Credentials:
 - Username and Password: The first time you log in, you must change these from the defaults ("pakedge" and "pakedger") to new credentials.
- General Device Information:
 - Friendly Device Name: Give the router a descriptive name to identify it on its web interface screen and in OvrC.
 - **Device Location**: Describe the physical location of the router here.
- Device Settings:
 - Time Zone: Select the time zone used for the router's event logs.
- WAN1.

Mode: Select a network protocol (DHCP, Static, PPPoE, Dual-Stack Lite(RFC6333), L2TP) and then complete the required fields. (Examples below).

- DHCP:
 - For DHCP networks, the IP Address, Subnet Mask, and Gateway fields are readonly.
- Static:

IP Address	Subnet Mask	Gateway
2	255.255.255.192	129

• IP Address: Enter the router's IP address.

- Subnet Mask: Enter the router's subnet mask.
- Gateway: Enter the router's Gateway address.
- PPPoE:

PPPoE Username	PPPoE Password
user1	····· &

- Enter the PPPoE Username and Password.
- L2TP:

L2TP Server	PAP/CHAP Username	PAP/CHAP Password
192.168.1.149	user1	······ 🔊

- L2TP Server: Enter the remote server IP address of the L2TP server you're connecting to.
- L2TP Username/ Password: Enter the L2TP Username and Password.
- DNS Settings:
 - **DNS Server** [n] (server's IP address): For a static IP network, enter up to two DNS server IP addresses here. For a DHCP network, these fields are read-only.
- *LAN*:
 - **IP Address**: Enter the IP address for the router's local network. (For a DHCP network, this field is read-only).
 - **Subnet Mask**: Enter the router's subnet mask. (For a DHCP network, this field is read-only).
 - DHCP Start/ End: Assign the first and last IP address you would like to use in the DHCP range. You can have up to four DHCP ranges per interface.

Overview

The Overview tab gives you a quick view of the router's status and critical settings.

Paked	dge RK-1						
Over	rview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
•	Pake	dge RK-1					Pakedge _{RK-1}
Location Current		Up (for 6d 22h 25m 21s)		0	Update Firmware	() Restart Device
Service	Service Name			Se	rvice Data		
	Serial Numbe	r		RH	6		
*	Firmware			2.0	00.0.100836		
•	Uptime			60	22h 25m 21s		
	CPU Usage			0.	5%		
	Memory Usag	ge		19	%		
	Devices on ne	etwork		15			
	Active Sessio	ns		50			
	WAN1 Port S	tatus		Et	hernet Port: Up, Speed: 1Gbp	s, Mode: Full Duple	эх

On this page, you will find information on the current Firmware version, number of active sessions on the router, CPU and memory usage, uptime, serial number and the number of devices on the network.

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

- Notifications: System notifications display at the very top of the tab. This example shows a firmware update is available.
- **Device Name**: The device name (assigned in the Configure tab) appears here.
- IP Address and MAC Address: The device's assigned IP address and unique MAC address is shown here.
- Location: Displays the configured "Location" of the device.
- Current Status: Shows the router's Up/Down status.
- **Update Firmware**: Click to open the Update Firmware screen (also accessible under the Advanced tab). The screen also displays the firmware's release notes.
- **Restart Device**: Click to restart (power cycle) the router. It happens immediately, with no confirmation dialog.
- **Services**: Displays the status of current services and settings and indicates with an icon whether the service or setting is optimally configured.

Connections

The Connections tab displays a list of connected devices.

akedge RK-1							
Overview	Connections	Configure	Interfaces	Backup/R	estore	Logs	Advanced
Pakedge F	RK-1						Pakedge RK-1
Connected Clients						Update Firmware	C Restart Device
Hostname	IP Type	IP Address	MAC Address	Lease Time	ТХ	RX	
PakedgeWK-1-	DHCP	192.168.10.114		6h 50m 21s	3.43 MB	2.64 MB	
ea5-C	DHCP	192.168.10.185		9h 13m 33s	6.53 MB	15.44 MB	
triad-one-l	DHCP	192.168.10.130		10h 31m 9s	63.76 KB	41.57 KB	
AN-210-SW-8-POE	DHCP	192.168.10.109		8h 53m 29s	28.26 MB	2.63 MB	
Control4DS2DoorStation-	DHCP	192.168.10.155		9h 0m 11s	1.55 MB	972.30 KB	
ca10-	DHCP	192.168.10.198		6h 41m 49s	45.02 MB	17.25 MB	
glassedge7-	DHCP	192.168.10.164		9h 17m 36s	6.94 MB	15.07 MB	

Click any column head to sort the list by that field. Available fields are:

- Hostname
- IP Type
- IP Address
- MAC Address
- Lease Time
- TX/RX

To Reserve or Clear a DHCP Lease on a device, click the ... More icon.

MAC Address	*	Lease Time	ТΧ	RX	
00:11:22:13:db:f9		7h 30m 3s	OB	OB	•••
00:11:22:20:4b:89		7h 3m 9s	08	08 Reserve	
00:11:22:28:0b:0c		7h 46m 36s	08 C	08 lear DHCP L	ease

- **Reserve**: Click **Reserve** to have DHCP to always assign the same IP address to the selected machine.
- Clear DHCP Lease: Click Clear DHCP Lease to have the server immediately assign a new IP address to the selected machine.

Interfaces

The *Interfaces* tab gives you easy access to the router's physical and virtual interfaces. Enable/disable an interface, check port status, and view/edit interface configurations.

Overview	Connecti	ons C	Configure	Interfaces	Backup/	Restore	Logs	Advanced
Physical								
	Port 1	Port 2	Port 3	Port 4	Port 5	WAN 1	WAN 2	
	1G/Full			-		1G/Full	-	
Enable	Port		IP /	Address	Received	Sent		
	WAN1	P	orts : WAN1		6.71 GB	6.02 GB		
	WAN1v6		orts : WAN1 0:0	:0:0:0:0:0	6.71 GB	6.02 GB		
	LAN		orts : 12345 192	2.168.10.1	6.36 GB	5.55 GB	Edi	
VLANs							Reset C	ounter
Add New								
Enable	VLAN		IP /	Address	Received	Sent		
	2-Guest	PC PC	orts : 12345 192	2.168.2.1	0.00 KB	18.07 KB		

Edit interface settings

To edit an Interface's assigned IP Address, Subnet Mask, Gateway, or DHCP Settings:

1. Click the ... More icon and select Edit.



- 2. Type any adjustments (see below)
- 3. Click Continue.
- 4. Click **Apply** (at the top of the page) to save and apply your changes.

Pakedge	RK-1						Cancel	Apply
Overview	Connec	tions	Configure	Interfaces	Backup/R	lestore	Logs	Advanced
Physical								
	Port 1	Port 2	Port 3	Port 4	Port 5	WAN 1	WAN 2	
	•							
	1G/Full			-		1G/Full		
Enable	Port		IP A	ddress	Received	Sent		
	WAN1		Ports : WAN1 10.1	02.158.36	6.71 GB	5.02 GB		

Important! Your changes will not be saved until you hit Apply.

Completing the dialog

Depending on the selected device, you will see an **Edit WAN** or **Edit VLAN** dialog. For help with each dialog, see below.

		VLAN Name	VLAN ID
Mode		guest network	66
Static 👻			
		IP Address	Subnet Mask
IP Address	IP Subnet Mask	192.168.66.1	255.255.255.0
	255.255.255.192		
Gateway	Override MAC Address	DHCP Server Let	ase Time
	90:A7:C1:DD:01:80		
		Range	D 12 H 0 M
DNS Server 1	DNS Server 2	Add New	
8.8.8.8	1.1.1.1	Start	End
MTU		192.168.66.100	192.168.66.200
1500			
VLAN Tag on WAN VLAN ID		Advanced	
Enable 125		Show	
		Advanced DHCP Default Gateway	DNS Server
Reply on ICMP		O Interface IP Custom	O Interface IP O Custom
Enable			
		Interzone Forwarding	
Cancel	Apply	Allow forward TO destination zones:	
		LAN 85-video network	LAN 85-video nel
			_

(Continued...)

Edit WAN Settings

Select a mode

In the Edit WAN dialog, choose a **Mode** (DHCP, Static, PPPoE, Dual-Stack Lite(RFC6333), L2TP) for your WAN settings. The **Mode** specifies how the WAN interface will connect with

the Internet Service Provider.

*

Depending on the **Mode** you selected, the settings in the dialog change. See below for help completing the **Edit WAN** dialog.

Configure DNS Settings

Many WAN modes ask you to enter DNS settings.

DNS Server 1		DNS Server 2
8.8.8.8		1.1.1.1
UTU	PMTU	
1492	Enable	
Override MAC Address		
90:A7:C1:DD:01:80		
VLAN Tag on WAN	VLAN ID	
Enable	125	
Reply on ICMP		
Enable		
Cancel		Apply

See the table below for help configuring the DNS settings.

Field	Explanation
DNS Server 1, 2	Enter up to two WAN DNS server addresses.
МТU	Enter the WAN MTU value.
ΡΜΤυ	Enable/disable.
Override MAC Address	Specify which MAC address to use for the WAN interface.
VLAN Tag on WAN	Enable/disable.
VLAN ID	Enter the VLAN ID.
Rely on ICMP	Enable/disable. Allow the WAN interface to reply to PING requests coming from the internet.

For instructions on completing the rest of the dialog, see below.

DHCP

If you are using DHCP, configure these settings:

Edit WAN1			
Mode			
DHCP	•		
DNS Settings Add New			
8.8.8		\otimes	
1.1.1.1		\otimes	

Field	Description
DNS Server	Enter the WAN DNS server address.
DNS Settings: Add New	Add a custom DNS entry.
Override MAC Address	Specify which MAC address to use for the WAN interface.
Other settings	See DNS Settings (above).

Static

If you are using Static, configure these settings:

Edit WAN1	
Mode Static	
IP Address	IP Subnet Mask
	255.255.255.192
Gateway	Override MAC Address
	90:A7:C1:DD:01:80

Field	Description	Comments
IP Address	Enter the WAN IP address.	Tip : Cannot be in IP ranges of another WAN Interface, for example:
Gateway	Enter the WAN Gateway address from the Internet Service Provider.	 DMZ Interface VLAN Interfaces PPTP Range OpenVPN Subnet
IP Subnet Mask	Enter the WAN subnet mask.	
Other settings	See DNS Settings (above).	

PPPoE

If you are using PPPoE, configure these settings:

Edit WAN1			
Mode			
PPPoE	•		
PPPoE Username		PPPoE Password	
PPPod Username		PPPOE Password	
admin			Ś

Field	Description
PPPoE Username/ Password	Enter the PPPoE Username and Password.
Other settings	See DNS Settings (above).

Dual-Stack Lite

If you are using DSLite, configure these settings:

Edit WAN1	
Mode	
Dual-Stack Lite(RFC6333)	
DS-Lite AFTR address	
2001:0db8:85a3:0000:0000:8a2e:03	
Reply on ICMP	
Enable	
Cancel	Continue

Field	Description	Comments
DS-Lite AFTP Address	Enter the IP address of the Address Family Transition Router.	Use any valid IPv4 or IPv6 IP address.

L2TP

If you are using L2TP mode, configure these settings:

L2TP Server	PAP/CHAP Username	PAP/CHAP Password
192.168.1.149	user1	····· 🕅

Field	Description
L2TP Server	Enter the remote server IP address of the L2TP server you're connecting to.
PAP/ CHAP Username PAP/ CHAP Password	Enter the L2TP Username and Password.

Edit LAN/VLAN Settings

In the Edit LAN/VLAN dialog, specify how devices will connect to the local network(s) of the router.

Edit VLANs								
VLAN Name			VLAN ID					
guest network			66	i i				
IP Address			Subnet Mask					
192.168.66.1			25	5.255	.255.0			
DHCP								
Server	Lease	Tim	e					
	0	D		12	н	0 M		
Range								
Add New								
Start		E	nd					
192.168.66.100		192.168.66.200						
Advanced Show								
Advanced DHCP								
Default Gateway		DNS Server						
O Interface IP O Custom			0	Interf	ace IP	Custom		
Interzone Forwarding	Interzone Forwarding							
Allow forward TO destination zones:			Allow forward FROM source zones:					
LAN 85-video network			LAN 85-video network					
Cancel						Apply		

Field	Explanation
VLAN Settings	
VLAN name	Enter a descriptive name for the VLAN interface. 32 character limit.
VLAN ID	Enter the VLAN ID number (VID).
IP Address	Configure Inter-VLAN Routing for this VLAN Interface. Cannot be in IP range of WAN1/2 Interface DMZ Interface Other VLAN interfaces PPTP Range OpenVPN Subnet
Subnet Mask	Enter the device LAN Subnet Mask.
DHCP Settings	
DHCP Server (Enable/ disable)	
Lease Time (D/ H/ M)	DHCP addresses can be reassigned on a daily, hourly, and monthly basis. Select how often DHCP addresses will be regenerated for each device on the network.
Range	
Add New	Create a new DHCP IP address range. Up to four DHCP ranges are allowed per interface.
Range	Assign the first and last IP address you would like to use in the DHCP range.
Advanced	To use the Advanced features, click Show. Advanced Show
Advanced DHCP	

Default Gateway	
Interface IP	(Default setting). With this selected, DHCP provides the interface's IP address as the Gateway to client devices.
Custom	To change the default Gateway address handed out by DHCP, select Custom, type the desired IP address, and click Apply.
DNS Server	
Interface IP	(Default setting). With this selected, DHCP provides the interface's IP address as the DNS server to client devices.
Custom	To provide a different IP address for the server to the clients, select Custom, type the desired IP address, and click Apply.
Interzone Forwarding	Use Interzone Forwarding to allow different areas of the network to communicate. Check to select where traffic can flow to and from the selected LAN.
То:	
• [Another LAN]	Traffic can flow from the LAN to another LAN.
Video network	Traffic can flow from the LAN to the selected video network.
From:	
• [Another LAN]	Traffic can flow to the LAN from another LAN.
Video network	Traffic can flow to the LAN from the selected video network.

Backup/Restore

The *Backup/Restore* tab allows you to save a configuration (backup) and restore the configuration file.

Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
Create Backup						
Save Configuration	n					
Restore Configu	ration File					
Choose File N	o File Selected			Restore		

- Save Configuration: Click to save a file that contains all of this router's settings.
- Choose File: Click to select a saved configuration backup file to use for restoring settings.
- **Restore**: Click to restore router settings using the selected configuration backup file.

Logs

The Logs tab displays a record of system events effected by the router. The events are categorized and sortable by severity, timestamp, and details.

Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
Remote Sys	-					
	Server IP Address		Port			
Enal	ble 192.168.1.128		3			
Log Level						
Minor		•				
Severity	Timestamp	Detail	<u>Clear Logs</u>	Download Detailed Lo	ogs Downloa	d System Report
Minor	May 30 01:20:01	crond16623: crond:	USER root pid 32397 cn	nd /usr/local/pakedge/pr	oxy/app/cron/aut	ostart.sh 2>&1
Minor	May 30 01:20:01	crond16623: crond:	USER root pid 32400 cn	nd /usr/local/pakedge/pr	oxy/app/cron/run	betatransfer.sh 2>
Minor	May 30 01:20:01	crond16623: crond:	USER root pid 32402 cn	nd /usr/local/pakedge/pr	oxy/app/cron/pre	ventexhaustion.sh
Minor	May 30 01:20:01	sudo: root : TTY=un	known ; PWD=/root ; U	SER=root ; COMMAND=,	/usr/local/pakedg	e/proxy/app/pake

- **Remote Syslog**: Enable to save the logs on another network. You'll also need to specify the remote Syslog server IP address and port.
- Log Level: Choose to display *Minor, Major, Critical,* or *Debug* logs.
- Clear Logs: Delete all current logs.
- **Download Detailed Logs**: Download more verbose descriptions of the logged events.
- Download System Report: Download an encrypted configuration file. For use with support upon request.

Reset to factory default settings

While setting up or troubleshooting, you may need to reboot the router or restore it to its factory default settings.



Reset using the interface

To only restart the router, maintaining all settings:

1. In the Overview or Connections tab, click Restart Device. The router restarts.

To reset to factory default settings, deleting all user settings:

Caution: Performing this reset will delete all of your settings on the router.

- 1. Go to the Advanced tab and click Device Settings.
- 2. Click Factory Default, then click Yes.

Reset using the physical RESET button

Your router has a recessed RESET button accessible through a pinhole next to the Ethernet port underneath the router.

To only reboot the router, maintaining all settings:

- 1. While power is connected, insert a narrow, pointed object (such as a straightened paper clip) into the hole.
- 2. Press and release the button.

To reset to factory default settings, deleting all user settings:

Caution: Performing this reset will delete all of your settings on the router.

- 1. While power is connected, insert a narrow, pointed object (such as a straightened paper clip) into the hole.
- 2. Press and hold the button for at least ten seconds, then release it.

Advanced

The Advanced tab lets you configure Advanced settings for VPN, Firewalls, and more. See below for a summary of each feature on the Advanced tab (detailed instructions follow).

Feature	Functional summary
Device Settings	Configure basic router functionality.
DHCP Reservation	Manually assign an IP address to a client device using DHCP.
Dual WAN	Enable a secondary WAN connection for redundant access to the internet or to connect to a secondary network.
Dynamic DNS	Configure a continually updated, user-configured domain name that provides remote access even when the public IP address changes.
Firewall	Control the forwarding of traffic between network interfaces and access fine-grain control over firewall rules.
Firmware	Update the router firmware for functionality improvements and feature enhancements.
Multicast Routing	Allow the routing of multicast traffic between LAN and VLAN interfaces on the router.
NAT (Port Forwarding)	Define Network Address Translation rules for incoming traffic. Also referred to as Port Forwarding, 1:1NAT, Virtual Server, or Port Mapping.
Parental Controls	Configure rules to limit access to specific websites or restrict internet access to a device based on a schedule.
QoS	Configure Quality of Service settings to prioritize and limit traffic speeds through the router.
Static Routes	Manually configure routing rules to control the path of traffic when trying to reach a specified network.
VLAN Port Settings	Configure individual port access to VLANs.
VPN	Configure a Virtual Private Network using OpenVPN or PPTP servers.

OvrC

OvrC gives you remote device management, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

To add this device to your OvrC account:



- 1. Connect the AP to the internet
- 2. Log into OvrC (www.ovrc.com)
- 3. Add the Device (MAC address and serial numbers needed for authentication)

Device Settings

From the *Device Settings* tile, configure basic router functionality.

Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
LEDs	UPnP					
Enable	Enable					
Web GUI Time	out					
5	min					
WAN Access						
HTTPS	Port Enable S	Support Access Port	t			
Enable	8443	Enable 22	223			
Factory Default						
Diagnostic Too	IP Address / Domain					
ping 🗸		Run				
SNMP						
Enable SNMP						
Enable						

- Enable various settings. (LEDs, UPnP, WAN Access, and SNMP).
- Run **Diagnostic** tests. (Ping, traceroute, nslookup, speedtest).
- Reset the device. (Restore factory default settings).

Enable settings

With the toggle button, **Enable** or **Disable** various settings.



To enable a setting:

 Go to the Advanced tab > Device Settings, then enable/ disable LEDs, UPnP, WAN Access, and SNMP (see below). 2. When you are ready, click Apply to save your changes.



Settings

Important! For your safety, WAN Access and SNMP are disabled by default. If you enable these services, be sure to use proper security measures.

Click to Enable (slider turns blue) or Disable (slider turns white) the following settings:

- 1. **LEDs** Enable/ disable the router LEDs.
- UPnP Enable 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.
- 3. Web GUI Timeout Specify the number of minutes a user must be idle before they are automatically logged out.
- 4. WAN Access Enable WAN Access to access the router remotely.
 - a. **HTTPS**: Enable WAN HTTPS access; configure which port to use for WAN HTTPS access to the router web UI.
 - b. Enable Support Access: Enable WAN SSH access; configure which port to use for SSH access to the router CLI.
- 5. **SNMP** Enable SNMP to monitor network devices and their performance/ configuration.

Diagnostic Tools

Under *Diagnostic Tools*, easily troubleshoot your network.

Diagnostic Tools			
Туре		IP Address / Domain	
ping	*	1.1.1.1	Run
ping			
traceroute			
nslookup			
speedtest			

Easily run four types of tests:

- Ping Test communication between two devices on the network.
- **Traceroute** Show how many routers, or hops, there are between the router and a certain destination.
- **NSLookup** Find name server information for domains.
- **SpeedTest** Check the Internet speed of the router. Important! Speed tests run from the router can easily be affected by other network traffic and processor utilization on the router. It is recommended for most accurate results to run speed tests from a PC wired to the router.

To run a test:

- Go to the Advanced tab > Device Settings, then under Diagnostic Tools > Type, scroll to select the test you would like to run (ping, traceroute, nslookup, speedtest).
- 2. Type the IP address or hostname you want to test and click li.
- 3. After a few moments, your results will be displayed.

Factory Defaults

Pressing the Factory Default button will restore the router to factory default settings.

Factory Default

Important! If you are connecting remotely, access to the router may be lost until the correct WAN configuration is set.

DHCP Reservation

Overview Conn	ections	Configure	Interfaces	Backup/Restore	Logs	Advance
OHCP Reservation	L DHCP					
Host Name	Туре	IP Address		MAC Address	Lease Time	
PakedgePE-09N-53006	9 Reser	ved 192.168.1.1	24			
PakedgeWA-2200-3B01	16 Reser	ved 192.168.1.1	14			••••
	DHCP				Remove	
	DHCP				10h 58m 56	s ····
	DHCP				8h 26m 45s	

Click the *DHCP Reservation* tile to allow the router to continually assign the same IP address to a device.

Tip: To see if a device got its IP address using DHCP or if it was reserved, check the Connections tab.

Add a new reservation

If you know a device's MAC address, you can add it to the network and assign a DHCP Reservation.

To assign a DHCP reservation:

- 1. Go to the *Advanced* tab > **DHCP Reservation**, then click **Add Reservation**.
- 2. Complete the dialog (below).

DHCP Reservation	
Hostname	
IP Address	MAC Address
Cancel	Apply

- Hostname Enter a descriptive name for the device.
- IP Address Enter the device's IP Address.

- MAC Address Enter the device's MAC Address.
- 3. Click **Apply** to complete the reservation.

Tip: To remove the reservation, click the **...More** icon and select **Remove**.

	•••
Remov	e

Manage DHCP entries

Reserve or clear a DHCP lease

The DHCP Reservation tab lists all devices on the network that have obtained an IP address via DHCP.

To reserve a device's current DHCP assigned IP Address or to clear the DHCP lease from the router:

1. Go to the *Advanced* tab > **DHCP Reservation** and find the device you wish to manage. Then click the ...**More** icon.

DHCP	7h 49m 20s
DHCP	Reserve
DHCP	Clear DHCP Lease

- 2. Using the options, either **Reserve** or **Clear** the DHCP Lease.
 - **Reserve**: To have DHCP always assign the same IP address to the selected machine, click **Reserve**.
 - Clear DHCP Lease: To have the server immediately assign a new IP address to the selected machine, click Clear DHCP Lease.
- 3. Click **Apply** to complete the action.

Remove reservations

You can remove all DCHP Leases at once, or just the lease for a single device.

Important! Because DHCP persists on individual devices, if you clear a DHCP lease on the router (using the DHCP Reservation page), it clears from the router and not the device. To clear the device you must either (1) reboot the device or (2) disconnect and reconnect the device to the network (to get a new IP address).

To remove all reservations at once:

1. Go to the *Advanced* tab > **DHCP Reservation** and click **Clear All DHCP**.

DHCP Reservation
Add Reservation Clear ALL DHCP

2. Click **Apply** (at the top of the page) to finalize the action.



To remove a single reservation:

- 1. Go to the *Advanced* tab > **DHCP Reservation**.
- 2. Next to the device, and click the ...More icon and select Remove.



3. Click **Apply** (at the top of the page) to finalize the action.



Dual WAN

From the Dual WAN tile, configure network failover settings.

Dual WAN lets you use two WAN ports on the router in redundancy mode. If WAN1loses internet access, WAN2 will take over.

						Cancel	Apply
Overview	Connections	Configure	Interfaces	Backup/R	Restore	Logs	Advance
Dual WAN							
	Fail over						
Enable	Enable						
WAN1							
WAN1 Health Monitor Ir	nterval	Health Mor	nitor ICMP Host(s)		Attempts	s Before WAN Reco	overy
	nterval	→ Health Mor		•	Attempts	s Before WAN Reco	overy
Health Monitor Ir	nterval			Ť		s Before WAN Reco	
Health Monitor Ir	nterval			¥		s Before WAN Reco	
Health Monitor Ir 120 sec		▼ WAN Gat		•	5	s Before WAN Reco	¥
Health Monitor In 120 sec WAN2		▼ WAN Gat	eway nitor ICMP Host(s)	•	5		•

To configure Dual WAN:

- Go to the Advanced tab > Dual WAN, then choose whether to enable Dual WAN and/or Fail over.
 - a. Enable Dual WAN Enable a second WAN but no failover.
 - b. Enable Failover Turn on/off fail over functionality for second WAN.

With Failover enabled, 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.

- 2. Under each **WAN**, choose how and when the primary WAN should switch to the failover WAN.
 - a. **Health Monitor Interval**. Choose how frequently (in seconds) the WAN will check connectivity to make sure that it is still up and running.
 - b. Health Monitor ICMP Host(s). Ping the WAN Gateway or DNS to check if Internet connectivity has been lost.
 - c. Attempts Before WAN Recovery. Choose how many times the router should ping the failed WAN before switching to the Failover.
- 3. Click **Apply** (at the top of the page) to finalize the settings.



4. The second WAN configuration displays on the Interfaces page.

Dynamic DNS

From the Dynamic DNS tile, configure a continually updated, user-configured domain name that provides remote access even when the public IP address changes. You can use Pakedge DDNS or a custom DDNS.

	us Check			
BakPak Credentials	Password			
user1@user.com		Ŕ	Change	
Hostname				
host1	.bakpakddns.com	Check Availability	Claim Hostname	
Refresh Time				
12h	Force Refresh			
12h	Force Refresh			
Dynamic DNS				

Pakedge Dynamic DNS

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 Dynamic DNS 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 Dynamic DNS take the following steps.

Note: BakPak DDNS is only available on the RK-1, RE-2, and RT-3100.

To create a Pakedge Dynamic DNS:

- 1. Go to the Advanced tab > Dynamic DNS.
- 2. Under *Pakedge Dynamic Dynamic DNS*, click **Enable**.



3. Under BakPak Credentials,
a. If you have an existing BakPak account, enter your credentials and click Login.

BakPak Credentials			
Email	Password		
user1@user.com		Ŕ	Login

- b. 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**.
- 4. 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 *host1.bakpakddns.com* is available.

Hostname			
host1	.bakpakddns.com	Check Availability	Claim Hostname

5. 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.

Command	Result:Success	Name	is	available	
---------	----------------	------	----	-----------	--

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

Hostname			
host1	.bakpakddns.com	Check Availability	Claim Hostname

- 7. 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.
- 8. You can click Status Check to see the status of your Pakedge Dynamic DNS.



9. The router displays the status of the *Pakedge Dynamic DNS* giving you the hostname that the router is currently using.

- 10. 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**.
- 11. You can change the BakPak user on the router at any given time by entering the new credentials and clicking **Change**.

BakPak Credentia	als		
Email	Password	_	
		R	Change

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

	C	Comma	and Re	esult:Su	lcces	ss	
BakPak	user	for	this	router	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.

13. Click **Apply** (at the top of the page) to save your changes.

							Cancel	Apply
Overview	Conne	ctions	Configure	Interfaces	Backu	up/Restore	Logs	Advanced
Pakedge Dy		_						
Enab		eck						
Email		Password						
			R	Change				
Dynamic DN Add New	IS							
Enable	Service	Hostname	IP change chec	k frequency		Force Update fr	requency	
	dyndns.org	host1	10		M-	72		Н

Non-Pakedge DDNS

To configure a non-Pakedge DDNS:

- 1. Go to the *Advanced* tab > **Dynamic DNS**.
- 2. Under Dynamic DNS, click Add New.

Pakedge Dynamic DNS	S Check			
BakPak Credentials				
Email	Password			
		Ŕ	Change	
Hostname				
host1	.bakpakddns.com	Check Availability	Claim Hostname	
Refresh Time				
12h	Force Refresh			
Dynamic DNS				
Add New				

- 3. Complete the dialog (see below) and click **Continue**.
- 4. Click **Apply** (at the top of the page) to save your changes.

							Cancel	Apply
Overview	Connec	tions (Configure	Interfaces	Backup	/Restore	Logs	Advanced
Pakedge Dyn		_						
Enable Enable		eck						
Email	ientials	Password						
			R	Change				
Dynamic DN Add New	S							
Enable	Service	Hostname	IP change check	frequency	1	Force Update free	quency	
	dyndns.org	host1	10		М×	72	ł	f

Complete the dialog

Add Dynamic DN	I S
Enable	
Service	
dyndns.org 👻	
Hostname	
host1	
Username	Password
	Ŕ
Source of IP Address	Interface
Interface 👻	WAN1 +
IP change check frequency	
10	M 🕶
Force update frequency	
72	НŢ
Cancel	Continue

Field	Description
Enable	Enable/Disable this DDNS policy.
Service	Select your Dynamic DNS provider.
Hostname	Enter the full domain name that you signed up for.
Password	Enter the password for your account.
Source of IP Address	Specify where to obtain the IP address.
Interface	Specify the Interface which will provide the IP address.
IP change check frequency	Indicate how often the router will check to see if the WAN IP address has changed (in hours/minutes).
Force update frequency	Indicate when the router will force an update with the DDNS provider (in hours/ minutes).

Add a secondary DDNS profile

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 DDNS profile:

- 1. Go to the *Advanced* tab > **Dynamic DNS**.
- 2. Under **Dynamic DNS**, click **Add New**, and complete the steps outlined above.
- 3. Click **Apply** (at the top of the page) to finalize the action.



Edit or delete a Dynamic DNS entry

To edit or delete a Dynamic DNS entry:

- 1. Go to the *Advanced* tab > **Dynamic DNS**.
- 2. Next to the entry, click the ...More icon.

Dynamic D Add New	NS					
Enable	Service	Hostname	IP change check frequency		Force Update frequence	Cy
	dyndns.org	host1	10	Mv	72	H¥
						Edit
						Delete

- 3. Next, select Edit or Delete.
- 4. Click **Apply** (at the top of the page) to save your changes.

Firewall

From the Firewall tile, control the forwarding of traffic between network interfaces and get fine-control over firewall rules.

irewall									
Zone Forward	ing Policies								
Global Settings									
nput	0	utput		Forward			SIP ALG		
Allow	•	Allow	*	Reject		•	Enat	ole	
orwards									
Zone Forwar	ding		Input	Ou	itput	Forward	Masquerading	MSS Clamping	
WAN			Reject	· /	Allow 🗸	Reject 👻			
WAN1			Reject	· /	Allow 🗸	Reject 👻			
LAN	85-video network]	Allow	•	Allow 🗸	Allow 👻			
			Allow	•	Allow 🗸	Allow 👻			
66-guest									

Configure global firewall settings or set up firewall settings (by zone).

Global Settings

Under Global Settings, set rules for how firewall traffic is handled globally.

- 1. Go to the Advanced tab > Global Settings.
- 2. Under **Global Settings**, choose whether to globally **Allow/ Reject/ Drop** each type of traffic. (Traffic types include: *Input, Output, Forward*, and *SIP ALG*).

Firewall	olicies				
Global Settings					
Input	Output		Forward		SIP ALG
Allow 👻	Allow	•	Reject	-	Enable

- a. **Input** Traffic trying to reach the router itself through any Interface not tied to a Zone.
- b. **Output** Traffic originating from the router itself going through an Interface with no Zone.
- c. **Forward** Traffic passing between interfaces belonging to one Zone.
- d. **SIP ALG** Enable/ disable SIP ALG for VoIP traffic.

3. To save your changes, click **Apply** (at the top of the page).



Forwards

Under Forwards, determine where and what direction traffic should be able to go through the firewall.

Forwards							
Zone	Forwarding	Input	Output	Forward	Masquerading	MSS Clamping	
WAN		Reject 🚽	Allow 🗸	Reject 🚽			

Tip: If a network is not available under Zone or Forwarding, you can add new VLAN interfaces on the Interfaces tab.

- **Zone** (synonymous with Interface) Zones allow VLANs and LANs to communicate with each other.
- Forwarding Forwarding determines where and what direction traffic should be able to go within the firewall.
- Input Choose to Allow/Reject/Drop traffic trying to reach the router itself through any Interface not tied to a Zone.
- **Output** Choose to Allow/Reject/Drop traffic originating from the router itself going through an Interface with no Zone.
- Forward Choose to Allow/Reject/Drop traffic passing between interfaces belonging to one zone.

Check to enable Masquerading or MSS Clamping.

- **Masquerading**. Masquerading combines Source NAT, Destination NAT, and Connection Tracking to mask network traffic from multiple devices behind one interface. It is a requirement for WAN interfaces to function as a gateway to the Internet.
- **MSS Clamping** (also known as "MSS fix"). MSS Clamping makes outgoing traffic handle differing MTU values along the traffic path. Commonly used with PPPoE.

To save your changes, click **Apply** (at the top of the page).

				Cancel	Apply
	Forwarding Policies	Interfaces	Backup/Restore	Logs	Advanced
Global Set Input Allow Forwards	Output Allow	Forw ▼ Re	iect 🗸	SIP ALG	Enable
Zone	Forwarding	Input	Output	Forward	Masquerading
WAN		Reject →	Allow 🗸	Reject 🗸	
LAN	85-video network 66-guest network	Allow 🗸	Allow 🗸	Allow 🗸	

Add new policy

Add a new firewall policy to control the forwarding of traffic through the router. To add a new Firewall policy,

1. Go to the *Advanced* tab > **Firewall**, then choose **Policies** > **Add New**.

Firewall
Policies Add New

- 2. Complete the dialog (see table below), then click Continue.
- 3. To save your changes, click **Apply** (at the top of the page).

							I	Cancel Apply
Overvie	9W	Connections	Co	nfigure	Interfaces	Backup/Restore	Logs	Advanced
Firewall Cone Fe Policies Add New Enable	orwarding Polic	Protocol	From	To	Source	Destination	Service	Action
	Finance	TCP+UDP	WAN1 +	LAN ¥	192.168.1.198	192.168.1.125	All	Accept -
	Sales	Any	Any 👻	Any 👻	Any	Any	All	Accept 👻

Add Firewall Policies

For help adding Firewall Policies, see the table below.

Policies	
Enable	
Name	
Finance	
Protocol	
TCP+UDP	
From	То
WAN1 -	LAN
Source	Destination
192.168.1.198	192.168.1.125
Service	
All	
Action	
Accept 👻	
Cancel	Continue

Field	Function	Options
Enable	Enable or disable the current firewall policy.	Toggle to enable/ disable
Name	Assign a name to the current firewall policy.	Type any name (up to 32 characters)
Protocol	Select the specific protocol to match to the rule.	 Any TCP+UDP TCP UDP ICMP Custom (manual entry)
From	Select the Firewall Zone which traffic must have as its source to apply to this rule.	 Any Choose from a list of available firewall Zones
То	Select the Firewall Zone which traffic must be destined for to apply to this rule.	
Source	Select the IP address from which traffic must originate from in order to apply to this rule.	 Any Choose from a list of all available IP addresses Custom
Destination	Select the IP address which traffic must be destined in order to apply to this rule.	
Service	Designate the port number to which traffic must be destined for in order to apply to this rule.	 All Enter a port number. (Do NOT enter ports in use by the router).
Action	Accept/Reject/Drop	Accept/Reject/Drop

Firmware

Click this tile to access cloud and local firmware upgrades.



If your firmware is up to date, this screen shows your current firmware version and provides a link for that firmware's release notes.

If a firmware update is available, this screen also shows the update version and the update's release notes. Click **Upgrade** to update the firmware from the cloud.

Multicast Routing

From the *Multicast Routing* tile, allow the routing of multicast traffic between LAN and VLAN interfaces on the router.

Note: If you do not have VLANs, you cannot add Multicast Routing policies. VLANs may be configured on the Interfaces tab.

Add a new **Multicast Routing** rule to designate which direction traffic is allowed to travel.

Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
able					
le					
From	То				
LAN		uest network 👻			
66-guest netwo	rk 🗸 🛛 LAN	•			
	able e From	e From To LAN • 66-g	e From To LAN v 66-guest network v	e From To LAN v 66-guest network v	E From To LAN • 66-guest network •

To add a new Multicast rule:

1. Go to the Advanced tab > Multicast Routing. Under Policies, click Add New Rule.



- 2. Complete the dialog (see table below), then click **Continue**.
- 3. When you are ready, click **Apply** to enable your changes.

					Cancel	Apply
Multicast		Configure	Interfaces	Backup/Restore	Logs	Advanced
Policies Add New Rule	able					
Enable	From	То				
	LAN	• 66	-guest network 🗸			
	66-guest netw	ork 👻 🛛 LA	N 👻			

Complete the Multicast rule dialog

Add Multicast	
Enable	
From	To 85-video network
LAN	
Cancel	Apply

Field	Function	Options
Enable	Enable or Disable the Multicast Forward rule	Enable/ disable
From	Specify the Zone multicast traffic can originate from	All available Zones
То	Specify the Zone multicast traffic can forward to	All available zones except zone selected on From

To edit or delete a Multicast rule:

1. Go to the *Advanced* tab > **Multicast Routing**. Next to the rule you wish to edit, click the **...More** icon.

Multicast			
Enable	From	То	
	LAN 👻	66-guest	network 🗸
	66-guest network 🗸	LAN	Edit
			Delete

- 2. Edit Click Edit, complete the dialog (see table above), and click Apply to save your changes.
- 3. Delete Click Delete, then confirm.
- 4. Click **Apply** to save your changes.

NAT (Port Forwarding)

Use the NAT tile to define Network Address Translation rules for incoming traffic.

Network Address Translation allows an external port to go through the firewall to connect to an internal IP address (for example, a public-facing webserver).

Overview	Connections	Confi	gure	Interfaces	Backup	/Restore	Logs	Advance
NAT								
Policies								
Add New Rule	<u>e</u>							
Enable	Name	Mapping Type	Protocol		External Port	Internal IP	Internal F	Port
	Sample Switch	Port	TCP+UDP	¥	8001	192.168.1.146	80	
		Forward						
	OpenWRT	Port	TCP+UDP	•	8002	192.168.1.180	80	
		Forward						
	OnVLAN	Port	TCP+UDP	.	3000	192.168.66.40	80	
		Forward						

NAT is also referred to as Port Forwarding, 1:1NAT, Virtual Server, or Port Mapping.

Important! Use with caution, as this could expose the device to tampering if proper security measures have not been taken).

Two types of NAT can be managed on the NAT tile.

- **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.
- **1:1NAT** is similar to NAT (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.

To configure a new NAT policy:

1. Go to the *Advanced* tab > **NAT**. Under *Policies*, click **Add New Rule**.

NAT	
Policies	
Add New Rule	

2. Complete the **New Rule** dialog (see table below) and click **Continue**.

3. Add any other policies, then click **Apply** (at the top of the page) to save your work.

							Cancel	Apply
Overview NAT Policies Add New Rule	Connections	Config	gure	Interfaces	Backup,	/Restore	Logs	Advanced
Enable	Name	Mapping Type	Protocol		External Port	Internal IP	Internal Port	
	Sample Switch	Port Forward	TCP+UDP	•	8001	192.168.1.146	80	
	OpenWRT	Port Forward	TCP+UDP	•	8002	192.168.1.180	80	

Complete the NAT Policy dialog

NAT Policy	
Enable	
Mapping Type	
O Port Forward 1:1 NAT	DMZ
Name	Protocol
IP Camera	TCP+UDP -
External Interface	
ANY -	
External Port	Internal Port
80	80
Internal Interface	Internal IP Address
LAN -	192.168.10.101
Source NAT IP	NAT Loopback
192.168.10.1 -	Enable
Cancel	Continue

RK-1, 7-Port Dual-WAN Gigabit Router User Guide

Field	Function	Options
Enable	Enable or Disable the Port Forwarding rule.	
Mapping Type	 Specify the mapping type as Port Forward or 1:1NAT. Port Forward takes traffic destined for the WAN interface IP (external IP) and forwards specified external ports to an internal port on an internal IP. 1:1NAT does the same but allows a different External IP to be defined and adds an SNAT rule for traffic outbound from the Internal IP so traffic exiting the WAN will use the specified External IP rather than the WAN interface IP. 	 Port Forward 1:1NAT
Name	Specify a name for the port forward rule.	• Type any name (32 character limit)
External Interface	Specify the external interface watching for incoming traffic.	ANYWAN1WAN2 (if enabled)
Protocol	Select the traffic protocol to apply to the rule	TCP+UDPTCPUDP
External IP	(Only for 1:1NAT) Specify which WAN IP to watch for incoming traffic.	 Any Valid IP Address
External Port	Specify which external port to watch for incoming traffic.	Any available port
Internal Port	Specify which internal port to NAT the traffic to on the local network.	 Any available port (that is not already used by the router)
Internal		

Interface		
Internal IP Address	Specify which local IP address to forward traffic to.	 Enter a valid IP address
NAT Loopback	Enable NAT Loopback to allow devices on the local network to be able to access other local devices by the Public IP associated with the forwarding policy.	• Enable/disable

To edit or delete an existing NAT policy:

1. Go to the *Advanced* tab > **NAT**. Next to the policy you wish to edit, click the ...**More** icon.

Internal IP	Internal Port
192.168.1.146	80
192.168.1.180	Edit
	Delete

- Edit Click Edit, complete the dialog (see table above), and click Apply (at the top of the page) to save your changes.
- Delete Click Delete, then confirm.
- 2. Click **Apply** (at the top of the page) to finalize the action.



Parental Controls

On the *Parental Controls* tile, configure rules to limit access to specific websites or restrict internet access to a device based on a schedule.

Two tabs are on this page: Block Websites and Schedule Internet.



For example, you can use **Schedule Internet** to disable the internet for all of your children's smart phones after 10 pm. You can use **Block Websites** to prevent users from visiting a site like www.yahoo.com.

Block websites

To block websites by device:

1. Go to the *Advanced* tab > **Parental Controls**. Select the **Block Websites** tab.



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

Parental Controls									
Block Websites	Schedule Internet								
Enable									
Active List									
Add New									

- 3. Under **Website**, enter the name of the website that you want to block (for example, www.yahoo.com).
- 4. Click **Clients** and select the IP address(es) for the device(s) that will be blocked from accessing the website. Click **Continue**.

(You can select all clients to apply it to every device on the network).

Add Block Website								
Website yahoo.com								
Clients	192.168.1.146							
Cancel	Continue							

5. To continue adding websites, click Add New.



6. When you are finished, click **Apply** at the top of the page. The websites you entered are now blocked.

Pakedge	RK-1				Cancel	Арріу
Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
Parental Cont	rols tes Schedule Interne	t				
Enable						
Active List Add New						
Website	Clients					
yahoo.com	× 192.	168.10.104 (d4:6a:	91:94:1d:0a)			

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.

Schedule Internet

The **Schedule Internet** feature allows you want to block certain client services from accessing the internet during specific times.

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

1. Go to the *Advanced* tab > **Parental Controls** and select the **Schedule Internet** tab.



- 2. Click Add New and complete the dialog (see table below), then click Continue.
- 3. Click Apply (at the top of the page) to save your changes.

Pakedge R	K-1				Cancel	Apply
Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
Parental Control	S Schedule Internet					
Active List Add New						
Description	Client Devices			Time Range	Days	
Kid's Internet		104 (d4:6a:91:94:1d:0a) 000fff83711f (00:0f:ff:83	:71:1f)	06:30 AM - 10:30 PM	Mon Tue Wed Thu F Sun	ri Sat

Complete the Internet Schedule dialog

Add Schedul	e Internet	
Description Kids' Internet		
Client Devices	192.168.1.130	192,168,1,198
Protocols	Ports	
TCP+UDP Time Range	. 1	
06:30 AM 👻 —	10:30 PM 👻	
Days 🗸 Mon 🔽 Tue	🖌 Wed 🔽 Thu	All Weekdays Weekend
Cancel		Continue

RK-1, 7-Port Dual-WAN Gigabit Router User Guide

Field	Description	Example
Description	Give the schedule a descriptive name.	Kids' Internet
Client Devices	Click the Clients field. Select the devices that should be included in the schedule; or manually type in the IP address for a specific device.	192.168.1.135
Protocols	The Protocol field allows you to select whether you want to block TCP, UDP or both for this policy.	TCP+UDPTCPUDP
Ports	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.	Note : You can block a device from completely accessing the internet. To do this, leave both the Protocol and Ports fields blank.
Time Range	Choose the times internet will be available for the selected devices.	6:30 am – 10:30 pm
Days	Choose the days internet will be available for selected devices.	M, T, W, Th, F, S, Su All Weekdays Weekends
Continue	Continue temporarily saves the schedule. Click Apply (at the top of the page) to activate the schedule.	

QoS

On the QoStile, configure Quality of Service settings to prioritize and limit traffic speeds through the router.

Overview Connections Configure Interfaces Backup/Restore Logs Advance QoS WAN Throughput Control Speed Limits Image: Speed Limits					Cancel	Apply
WAN Throughput Control Speed Limits Enable 25 Download (Mbit/s) Priority Add New Priority Source Host Destination Host	Overview Connectio	ons Configure Inte	erfaces Backu	p/Restore	Logs	Advanced
Speed Limits Enable 25 Download (Mbit/s) 10 Upload (Mbit/s) Priority Add New Priority Source Host Destination Host						
Enable 25 Download (Mbit/s) 10 Upload (Mbit/s) Priority Add New Priority Source Host Destination Host	WAN Throughput Cont					
Priority Add New Priority Source Host Destination Host		Speed Limits				
Add New Priority Source Host Destination Host	Enable	25 Download (M	lbit/s) 10	Upload (M	lbit/s)	
Priority Source Host Destination Host	Priority					
	Add New					
High - 192.168.1.198 192.168.1.104 ···	Priority	Source Host	C	Destination Host		
	High	▼ 192.168.1.198		192.168.1.104		

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 might prioritize your work computer over your children's smart phones).

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.

Restrict WAN upload and download speeds

From the top of the page, you can restrict download and upload speeds. 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.

To restrict upload and download speeds:

- 1. Go to the *Advanced* tab > **QoS**. Under *WAN Throughput Control*, click **Enable**.
- 2. Here, you can restrict download and upload speeds.

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. At the top of the page, click **Apply** to save and enable your changes.

Add a QoS priority setting

If you want to create a new QoS policy to prioritize the data for some devices over others,

- 1. Go to the *Advanced* tab > **QoS**. Under *Priority*, click **Add New**.
- 2. Complete the dialog (details below), then click Continue.
- 3. Click Add New to add any other priorities.
- 4. At the top of the page, click **Apply** to save and enable your changes.

					Cancel	Apply
Overview Con	nections Configure	e Interfaces	Backu	p/Restore	Logs	Advanced
QoS						
WAN Throughput	Control					
	Speed Limits					
Enable	1000 Down	load (Mbit/s)	1000	Upload (Mbit/:	s)	
Priority						
Add New						
	No	QoS policies are o	onfigure	d		
	e Add New link to add a					

Complete the Add Priority dialog

Add Priority	
Priority	Source Host
Medium	▪ 192.168.1.104
Destination Host	
192.168.1.125	
Cancel	Continue

Field	Description	Values
Priority	Select the priority of the data.	HighMediumLow
Source Host	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, manually enter the IP address.
Destination Host	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.

Static Routes

On the *Static Routes* tile, manually configure routing rules to control the path of traffic when trying to reach a specified network.

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. Go to the *Advanced* tab > **Static Routes**.
- 2. Under Static Routes, click Add New.
- 3. Complete the dialog (details below) and click **Continue**.
- 4. After the information has been entered, click **Apply** at the top of the page.

					Cancel	Apply
Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
Static Routes						
Target IP Address	5 Target Subr	net Mask Inter	face	Gateway	Metric	
192.168.222.0	255.255.2	55.0 LA	N 👻	192.168.1.111	1	

Complete the dialog

Add Static Routes	
Target IP Address 192.168.222.0	Target Subnet Mask 255.255.255.0
Interface LAN •	Gateway 192.168.1.111
Metric	
Cancel	Continue

Example: 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).

Field	Function	Example
Target IP Address	<i>Target IP Address</i> will be the network which must be accessed and is not directly known by the router.	192.168.222.0
Target Subnet Mask	<i>Target Netmask</i> is the Subnet Mask of that network.	255.255.255.0
Interface	The <i>Interface</i> that Gateway traffic will be forwarded to.	LAN
Gateway	<i>Gateway</i> is the IP Address traffic should be forwarded to in order to reach that new network. 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.	192.168.1.111
Metric	<i>Metric</i> 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.	1

VLAN Port Settings

From the VLAN tile, configure individual port access to VLANs. This allows for the restriction of VLANs to only certain ports, or to create a port with untagged access to one specific VLAN.

VLAN Port Se	ttings				
	Port 1	Port 2	Port 3	Port 4	Port 5
	•				
	1G/Full	-	-	-	
ID					
LAN	Untagged 🗸	Untagged -	Untagged 👻	Untagged -	Untagged 👻
2	Tagged -				
3	Tagged 🗸	Tagged -	Tagged -	Tagged 👻	Tagged 👻
4	Tagged -				

Under the available Ports, go to each network and scroll to select Tagged, Untagged, or Off.

Notes

- LAN cannot be tagged, only Untagged or Off.
- A port cannot be set to **Untagged** on more than one VLAN.
- A port cannot be set to restrict all access to all zones.
- If a network you need is not displayed, you can add new VLAN interfaces on the *Interfaces* tab.

VPN

Use VPN to access the network remotely. On the *VPN* tile, configure a Virtual Private Network using either OpenVPN or PPTP servers.

Configure OpenVPN

OpenVPN lets you set up a single VPN profile for each user that needs remote access to the network. Your router supports OpenVPN for secure point-to-point connections.

To set up OpenVPN:

- 1. First, enable OpenVPN.
- 2. Next, create one user profile for each computer that needs to access the network remotely through VPN.
- 3. Download the profile to each computer. Once the profile is installed, VPN will be ready for use.

Enable the OpenVPN Server

In order to use OpenVPN, it must be enabled on the router.

To enable OpenVPN:

- 1. Go to the Advanced tab > VPN.
- 2. On the **OpenVPN Server** tab, click **Enable**.



3. Complete the fields below.

Field	Explanation
Enable/ disable	Turn OpenVPN Server on/off.
OpenVPN Server	Enter IP address for OpenVPN Server. Normally the WAN IP address of the router.
OpenVPN IP Subnet	Enter 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).
Subnet Mask	Enter the IP subnet mask. (Usually prepopulated).
Encryption Type	Select the encryption type. AES 256bit CBC, AES 192bit CBC, AES 128bit CBC, or Blowfish CBC.

4. Click Apply (at the top of the page).

Pakedge	RK-1				Cancel	Apply
Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
VPN - OpenVPN	Server PPTP Server	PPTP Passthroug	gh			
	OpenVPN	I Server	OpenVPN IP Subnet	Subnet Mask	Encryp	tion Type

The OpenVPN server is enabled.

Tip: Click Cancel to clear the settings on the page.

Create OpenVPN user profiles

Once OpenVPN is enabled, create each user profile. Create one profile for each computer that will need VPN access.

To create an OpenVPN user profile:

- 1. Go to the *Advanced* tab > **VPN**.
- 2. On the OpenVPN Server tab under Profiles, click Add New.
- 3. Create a profile. Type a descriptive profile name and click **Continue**.

Tip: Do not use spaces/ special characters.

- **Tip**: Profile names must be unique.
- 4. After creating all desired profiles, click Apply.

Pakedge	RK-1				Cancel	Apply
Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
VPN - OpenVPN	Server PPTP Server	PPTP Passthroug	h			
	OpenVPN	Server	OpenVPN IP Subnet	Subnet Mask	Enormal	tion Type

Important! Profiles are incomplete until Apply is selected.

- Allow the profiles to configure (this will take some time).
- 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.

- 5. Once all profiles are complete, they must be downloaded to each device needing VPN access.
 - a. Next to each profile, click the ... More and choose Download.
 - b. Take the **Download** file (.ovpn) and add it to the computer that needs to connect to VPN (profile you just created). This Configuration file can be emailed to the device that will be connecting so it can be loaded into the OpenVPN app and the connection can be made.

Set up the OpenVPN user profile

Each computer must do two things to enable VPN.

- 1. Enable OpenVPN on their computer.
- 2. Download the VPN (.ovpn) profile to their computer. (This file can be emailed or transmitted via USB).

OpenVPN client setup for Windows, iOS, Android

Windows

Each computer using OpenVPN needs an Open VPN client. OpenVPN-GUI is a popular, free, OpenVPN client for Windows.

To Use OpenVPN on a PC:

- 1. Download OpenVPN-GUI here 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 Sha	ire View			
Pin to Quick Copy Past	Copy path Paste shortcut	elete Rename Rename folder	access • Propertier	Open Select all Edit History
Clipboa	rd Organiz	e New	Ope	n Select
← → ~ ↑	This PC > OS (C:) > Program Files (x86)	> OpenVPN → config		
🖈 Quick access	Name	Date modified	Туре	Size
Curck access	RE-2T091411085-RemoteUser001.	ovpn 10/13/2016 1:07 PM	OVPN File	10 KB
	README.txt	10/13/2016 12:58	Text Document	1 KB
痜 OneDrive	README.txt	10/10/2010 12/2011		

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**.

iOS

OpenVPN Connect is a free OpenVPN client for iOS devices.

To Use OpenVPN Connect on iOS:

- 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.



RK-1, 7-Port Dual-WAN Gigabit Router User Guide



3. Tap **Copy to OpenVPN** and the OpenVPN Connect app should open automatically.

RK-1, 7-Port Dual-WAN Gigabit Router User Guide

iPad ᅙ	11:49 AM	* 87% 📼
Done	RE-2T091411085-iOS_User.ovpn	Ć
	AirDrop. Share instantly with pe turn on AirDrop from Control Ce Finder on the Mac, you'll see the tap to share.	ople nearby. If they nter on iOS or from air names here. Just
	Mail Add to Notes Copy to Open/PN	More
	RE-2T09141	
	Oper	
	More	

4. Tap "+" to import the profile.



5. Tap **Connection** to connect to the VPN.

OpenVPN Connect				
Profile	/RE-2T091411085-iOS_User Autologin profile	>		
Status	Disconnected	>		
Connection	\bigcirc			

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

OpenVPN Connect						
Profile	/RE-2T091411085-iOS_User Autologin profile					
Status	Connected >					
Connection						
CONNECTION DET	AILS					
Duration	Last packet received < 1 second ago					
Bytes In 3.2	1 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.

OpenVPN Connect							
R	OpenVP OpenVPN	N Connect	t				
			NSTALL				
			Contains ads				
10 MILLION	4.2	8					
Downloads	128,398 单	Communication	Similar				

- 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.



7. You are connected to OpenVPN.



Configure PPTP

The router also supports Point-to-Point Tunnel Protocol VPN. With PPTP VPN, you can connect to the router remotely and have access to all network resources. To enable PPTP VPN:

- 1. Go to the Advanced tab > VPN.
- 2. Switch to **PPTP Server** tab.

VPN	
└── OpenVPN Server	PPTP Server

- 3. Click Enable.
- 4. Complete the fields (see below).

Field	Explanation	
Enable/ disable	Enable or Disable the PPTP server.	
Client IP	Enter IP address for PPTP Server.	
Start	Enter start address for PPTP VPN IP addresses to be assigned.	
End	Enter end address for PPTP VPN IP addresses to be assigned.	

- 5. You can also add a second user to the VPN by clicking Add New.
- 6. Enter the username and password.
- 7. When you are done, click **Apply** at the top of the page to finalize the settings.

Pakedge RK-1 Cancel							
Overview	Connections	Configure	e Interfaces	Backup/Restore	Logs	Advanced	
VPN OpenVPN Server PPTP Passthrough							
Enable	Client IP 192.168.10.20	Start	192.168.10.29	End			

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 192.168.10.30.

Configure PPTP Passthrough

This allows PPTP VPN traffic to pass from WAN to LAN. Typically used in Double NAT topologies wherein there is a PPTP tunnel established upstream to the WAN side of this router.

To enable PPTP VPN:

- 1. Go to the *Advanced* tab > **VPN**.
- 2. Switch to **PPTP Passthrough** tab.
- 3. Click Enable.
- 4. Enter the PPTP Server IP.

Overview	Connections	Configure	Interfaces	Backup/Restore	Logs	Advanced
VPN	VPN Server PPTP Server	PPTP Passthrough]			
	PPTP Server IP					
	192.168.1.3					
Enable						



11734 S Election Road Draper, UT 84020

www.control4.com

Copyright © 2021, Wirepath Home Systems, LLC. All rights reserved. Control4 and SnapAV and their respective logos are registered trademarks or trademarks of Wirepath Home Systems, LLC, dba "Control4" and/or dba "SnapAV" in the United States and/or other countries. 4Store, 4Sight, Control4 My Home, Snap AV, Araknis Networks, BakPak, Binary, Dragonfly, Episode, Luma, Mockupancy, Nearus, NEEO, Optiview, OvrC, Pakedge, Sense, Strong, Strong Evolve, Strong Versabox, SunBriteDS, SunBriteTV, Triad, Truvision, 200-00533E TW 04072021