User Manual

BEC 6900
4G/LTE Outdoor Router
# TABLE OF CONTENTS

## CHAPTER 1: INTRODUCTION
- **Introduction to Your Router** ........................................... 1
- **Features & Specifications** ............................................... 3
- **Hardware Specifications** .................................................. 4
- **Application Diagram** ........................................................ 5

## CHAPTER 2: PRODUCT OVERVIEW
- **Important Note for Using This Router** .................................. 6
- **Package Contents** ............................................................ 6
- **Device Description** ........................................................... 7
- **Mounting Kit Installation** .................................................. 8
- **Router Installation Instructions** .......................................... 12

## CHAPTER 3: BASIC INSTALLATION
- **Network Configuration – IPv4** ............................................. 16
  - Configuring PC in Windows 7 (IPv4) ..................................... 16
  - Configuring PC in Windows Vista (IPv4) ............................... 18
  - Configuring PC in Windows XP (IPv4) .................................. 20
  - Configuring PC in Windows 2000 (IPv4) ............................... 21
  - Configuring PC in Windows 98/ME ........................................ 22
  - Configuring PC in Windows NT4.0 ....................................... 23
- **Network Configuration – IPv6** ............................................. 24
  - Configuring PC in Windows 7 (IPv6) ..................................... 24
  - Configuring PC in Windows Vista (IPv6) ............................... 26
  - Configuring PC in Windows XP (IPv6) ................................. 28
- **Default Settings** ............................................................... 29

## CHAPTER 4: DEVICE CONFIGURATION
- ......................................................................................... 30
CHAPTER 5: TROUBLESHOOTING ..........77

Problems with the Router ..................................................77
Problem with LAN Interface .............................................77
Recovery Procedures .........................................................78
CHAPTER 1: INTRODUCTION

Introduction to your Router

Congratulations on your purchase of the RIDGEWAVE 6900 (Outdoor 4G/LTE Router). This unit is a light-weight, an industrial-grade outdoor fixed wireless router with an IP67 rated enclosure to withstand extreme weather conditions and harsh rugged deployments. With integrated IEEE802.3at power over Ethernet (PoE) support, the RidgeWave 6900 provides an easy installation from eliminating the need for a separate power and data cable. In addition to outdoor, it can be installed in environments such as: manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses or virtually any venue requiring a robust wireless solution. The RidgeWave 6900 integrates a high performance device with an embedded LTE module and advanced IP networking features enabling support of multiple high bandwidth applications at peaks speeds up to 100 (150) Mbps downlink and 50Mbps uplink.

Lightweight, Compact and unobtrusive Design

With multiple mounting options and a lightwegithed, it is easily to install the RidgeWave 6900 by single person. The RidgeWave 6900 also has a built-in passive Gigabit Power of Ethernet (GPoE) so both data and power can be sent from the unit.

Designed for Challenging / Rugged Deployments

The RidgeWave 6900 is designed for the toughest industrial environments. With IP67 hardened enclosure with industrial-grade components, the RidgeWave 6900 can be installed in manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses, etc.

4G/LTE Mobility

With 4G/LTE-based Internet connection (4G/LTE embedded module, requires an additional SIM card), you can access to the Internet through 4G/LTE whether you are seated at your desk or taking a cross-country trip.

4G/LTE Management Center

RidgeWave 6900 (4G/LTE Outdoor Router) Mobile Management Center visually displays its current 4G/LTE signal status also calculates the total amount of hours or data traffic used per month, allowing you to manage your 4G/LTE monthly subscriptions.

IPv6 Supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. The router is already supporting IPv6, you can use it in IPv6 environment no need to change device. The dual-stack protocol implementation in an operating system is a fundamental IPv4-to-IPv6 transition technology. It implements IPv4 and IPv6 protocol stacks either independently or in a hybrid form. The hybrid form is commonly implemented in modern operating systems supporting IPv6.
Quick Start Wizard

Support a WEB GUI page to install this device quickly. With this wizard, simple steps will get you connected to the Internet immediately.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.
Features & Specifications

- Outdoor 4G for high speed mobile connectivity
- 4G embedded with a built-in SIM card slot
- High-speed 4G connection up to downlink 100(150)Mbps and uplink 50Mbps data rate
- 4G Management Center for connection monitoring
- Firewall security with DoS prevention and SPI
- Quality of Service control
- Syslog monitoring
- Ease of Use with Quick Installation Wizard
- Ideal for homes, businesses, rural areas and the underserved

Operational Mode

- Bridge or Routed mode

Network Protocols and Features

- IPv4, IPv6 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- DHCPv4 / v6
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS proxy
- IGMP snooping and IGMP proxy
- MLD snooping and MLD proxy

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention including Land Attack, Ping of Death, etc
- Access control
- IP&MAC filter, URL Content Filter
- Password protection for system management
- VPN pass-through
Quality of Service Control

- Traffic prioritization management based on Protocol, Port Number and IP Address (IPv4/IPv6)

Management

- Quick Installation wizard
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP server/client/relay
- Supports SNMP v1, v2, v3, MIB-I and MIB-II
- TR-069 supports remote management

Hardware Specifications

Physical interface

- 10/100/1000 Gigabit Ethernet LAN with IEEE802.3at compliant Gigabit PoE PD
- SIM slot: (for the SIM card from Telco/ISP)
- LED Indicators: Power, LAN(PoE), LTE, and Internet

Physical Specifications

- Dimensions (W*H*D): 8.5" x 7.5" x 3" (215mm x 227mm x 91mm)
- Weight: 1.81kgs (4lbs)
- IP-67 Grade Enclosure
Application Diagram

The indoor unit broadcasts the wireless signal throughout the home.

RidgeWave 69000
4G/AT&T Outdoor Radio Unit
CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

✔ Do not remove, open or repair the case yourself. Contact with your Internet Service Provider or have it repaired at a qualified service center.

✔ Use the supplied PoE (Power-over-Ethernet) injector for indoor only or with any 802.3at capable PoE injectors to connect with the RidgeWave 6900

✔ It is mandatory to earth ground the RidgeWave 6900. Improper grounding not only could damage the unit but also all equipment connected to it.

Package Contents

✔ The RidgeWave 6900 4G/LTE Outdoor Router
✔ M25 Cable Gland
✔ Quick Start Guide
✔ 25ft Outdoor LAN cable
✔ Gigabit Power-over-Ethernet (PoE) Injector
✔ Grounding Wire
✔ Mounting Kit
## Device Description

### CONNECTORS

<table>
<thead>
<tr>
<th>CONNECTORS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM / LED / Reset</td>
<td>Insert the SIM card into the SIM slot. Press the reset button to reset device or restore to factory default settings</td>
</tr>
<tr>
<td>Gigabit LAN(PoE)</td>
<td>Connect it with the supplied PoE injector, 802.1at compliant, using an Ethernet cable.</td>
</tr>
</tbody>
</table>

### LED STATUS

<table>
<thead>
<tr>
<th>LED</th>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Power</td>
<td>Orange</td>
<td>System is either in initial startup phase or has boot failure</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>System is up and ready</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No input power</td>
</tr>
<tr>
<td>2. LAN(PoE)</td>
<td>Orange</td>
<td>Transmission speed is at 10/100Mbps</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Transmission speed is at Gigabit speed (1000Mbps)</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td>Data being transmitted/received</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No device is being connected</td>
</tr>
<tr>
<td>3. Internet</td>
<td>Orange</td>
<td>IP request failed or System is in initial booting phase</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>IP connected and traffic is passing thru the device</td>
</tr>
<tr>
<td>4. 3G/4G-LTE (Received Signal Strength Indicator)</td>
<td>Green</td>
<td>RSSI greater than -69 dBm. Excellent signal condition</td>
</tr>
<tr>
<td></td>
<td>Green Flashing quickly</td>
<td>RSSI from -81 to -69 dBm. Good signal condition</td>
</tr>
<tr>
<td></td>
<td>Orange Flashing quickly</td>
<td>RSSI from -99 to -81 dBm. Fair signal condition</td>
</tr>
<tr>
<td></td>
<td>Orange Flashing slowly</td>
<td>RSSI less than -99 dBm. Poor signal condition</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>No signal. 4G_LTE module is still in connected mode</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No LTE module or LTE module fails</td>
</tr>
</tbody>
</table>
Mounting Kit Installation

1. **Attach the Articulation Pole to the Enclosure**
   Attach the articulation pole to the back of the RidgeWave 6900 using M6*16 screws and washers.

2. **Wall or Pole Mounting**
   2.1 **Mounting on Wall**
   Fix the T-formed Bracket to the wall using wood/drywall screws.

   2.2 **Mounting on a Pole**
   2.2.1a **Mounting for pole smaller than 1.5” (38mm)**
   Attach the T-formed Bracket and the W-bar to the pole then use M6x60 bolts, spring washer and washer to fix the mounting kit onto the pole.
2.2.1b Mounting for pole larger than 1.5” (38mm)

Fix the T-formed Bracket to the pole by using the stainless hose clamp.

3. Mounting the RidgeWave 6900 to the T-formed Bracket

Attach the articulation pole (the RidgeWave 6900 enclosure) to the T-formed bracket by using M8x40 bolts, nut, spring washer and washer.

**Cross-Polarized Antenna** – The original of the source position, the nominal position, is seeing the **RidgeWave logo** when facing toward the RidgeWave 6900.
4. Position Adjustment

Find the location and best angle for getting the strongest signal from the base station. The RidgeWave 6900 must be directed towards the nearest base station.

Adjusting the router position to get a better reception and/or fine-tuning the router orientation (in horizontal/vertical position or 45 degree angle position) to have the best signal strength.
5. **Grounding the CPE to Complete the Installation**
   Attach the grounding wire to the CPE and tighten the screw
Router Installation Instructions

1. Power on your RidgeWave 6900

   **Step 1:** Assemble M25 cable gland

   ![Diagram of M25 cable gland assembly]

   **Step 2:** Unscrew the LAN (PoE) port and insert the supplied outdoor Ethernet cable (RJ-45) through material A-D, and then connect the RJ-45 Ethernet cable into the LAN (PoE) port.

   ![Diagram of cable insertion process]

   **Step 3:**
   3.1: Insert \(\text{C}\) at the back end of \(\text{D}\)
   3.2: Clip \(\text{B}\) on \(\text{C}\)
   3.3: Keep \(\text{B}\) close to \(\text{D}\)
   3.4: Then tighten \(\text{A}\).

   ![Diagram of step 3 implementation]

   **Step 4:** Insert the other end of outdoor Ethernet cable (RJ-45) to the supplied Gigabit PoE injector, IEEE 802.1at compliant, **Power+Data (P+D)/OUT** port. Connect another Ethernet cable (RJ-45) directly to the **Data/IN** port and the other end of cable to a switch or broadband router. Plug the PoE power cable to an electrical outlet to power on your RidbeWave 6900.
2. **Set up your 4G/LTE Internet Connection**

   **Step 1**: Unscrew the cap of SIM card slot.
Step 2: Slide the SIM card with the mental contacts (gold plate) facing down to the SIM slot then push it all the way in until you hear the clicking sound.

It is recommended to use an industrial-grade SIM card.

Step 3: Screw the cap back tightly.

Please power off your RidgeWave 6900 before inserting or removing the SIM card.
CHAPTER 3: BASIC INSTALLATION

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows 98 / NT /2000 / XP / ME / 7 / Vista, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed or configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router’s web interface it may also be advisable to uninstall any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC’s network environment installation. First of all, please check your PC’s network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

**NOTE:** Any TCP/IP capable workstation can be used to communicate with or through the RidgeWave 6900. To configure other types of workstations, please consult the manufacturer’s documentation.
Network Configuration – IPv4

Configuring PC in Windows 7 (IPv4)

1. Go to Start. Click on Control Panel.
2. Then click on Network and Internet.

3. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

4. Select the Local Area Connection, and right click the icon to select Properties.

6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

7. Click OK again in the Local Area Connection Properties window to apply the new configuration.
Configuring PC in Windows Vista (IPv4)

1. Go to Start. Click on Network.

2. Then click on Network and Sharing Center at the top bar.

3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window pane.

4. Select the Local Area Connection, and right click the icon to select Properties.
5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.
Configuring PC in Windows XP (IPv4)

1. Go to Start. Click on Control Panel.
2. Then click on Network and Internet.
3. In the Local Area Connection Status window, click Properties.
4. Select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.
Configuring PC in Windows 2000 (IPv4)

1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.

2. Double-click Local Area Connection.

3. In the Local Area Connection Status window click Properties.

4. Select Internet Protocol (TCP/IP) and click Properties.

5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.

6. Click OK to finish the configuration.
Configuring PC in Windows 98/ME

1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.

2. Select TCP/IP ->NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.

3. Select the Obtain an IP address automatically radio button.

4. Then select the DNS Configuration tab.

5. Select the Disable DNS radio button and click OK to finish the configuration.
Configuring PC in Windows NT4.0

1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.


3. Select the Obtain an IP address from a DHCP server radio button and click OK.
Network Configuration – IPv6

Configuring PC in Windows 7 (IPv6)

1. Go to **Start**. Click on **Control Panel**.

2. Then click on **Network and Internet**.

3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.
5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.

6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.
Configuring PC in Windows Vista (IPv6)

1. Go to Start. Click on Network.

2. Then click on Network and Sharing Center at the top bar.

3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window pane.

4. Select the Local Area Connection, and right click the icon to select Properties.
5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.

6. In the **TCP/IPv6 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.
Configuring PC in Windows XP (IPv6)

IPv6 is supported by Windows XP, but you need to install it first.

Please follow the steps to install IPv6:

1. On the Desktop, Click **Start > Run**, type **cmd**, then press **Enter** key in the keyboard, the following screen appears.

   ![Command Prompt](image1)

2. Key in command **ipv6 install**

   ![Command Prompt](image2)

   Installation of IPv6 is now completed. Please test it to see if it works or not.
Default Settings

Before configuring the router, you need to know the following default settings.

Web Interface: (Username and Password)

- Username: admin
- Password: admin

The default username and password are “admin” and “admin” respectively.

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP Settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

DHCP Server:

- DHCP server is enabled.
- Start IP Address: 192.168.1.100
- IP pool counts: 100
CHAPTER 4: DEVICE CONFIGURATION

Login to your Device

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a user name and password window prompt appears.

The default username and password is “admin” and “admin” respectively for the Administrator.

NOTE: This username / password may vary by different Internet Service Providers.

Congratulations! You have successfully logged on to your RidgeWave 6900
Once you have logged on to your RidgeWave 6900 via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

<table>
<thead>
<tr>
<th>Section</th>
<th>Status</th>
<th>Quick Start (Wizard Setup)</th>
<th>Configuration</th>
<th>Language</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Device Info</td>
<td></td>
<td><strong>Interface Setup</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Internet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- LAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Log</td>
<td></td>
<td><strong>Advanced Setup</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- NAT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Static DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Time Schedule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Remote System Log</td>
<td></td>
</tr>
<tr>
<td>Sub-Items</td>
<td>3G/4G-LTE Status</td>
<td></td>
<td><strong>Access Management</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Device Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Universal Plug &amp; Play (UPnP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Dynamic DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Packet Filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CWMP (TR-069)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Parental Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statistics</td>
<td></td>
<td><strong>Maintenance</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- User Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Time Zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Firmware &amp; Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- System Restart</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Diagnostic Tool</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP Table</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please see the relevant sections of this manual for detailed instructions on how to configure your **RidgeWave 6900** router.
In this section, you can check the router working status, including **Device Info**, **System Log**, **3G/4G-LTE Status**, **Statistics**, and **DHCP Table**.
Device Info

It contains basic information of the device.

### Device Information

**Model Name:** Name of the router for identification purpose.

**Firmware Version:** Software version currently loaded in the router

**MAC Address:** A unique number that identifies the router

**Data-Time:** Setup correct time on the RidgeWave 6900 with your PC. Check on Time Zone section for more configuration information.

**System Up Time:** Display how long the RidgeWave 6900 has been powered on.

### Physical Port Status

**Physical Port Status:** Display available connection interfaces, WAN (3G/4G-LTE) and LAN, that are supported in the RidgeWave 6900.

**WAN**

**Interface:** List current available WAN connections.

**Protocol:** Display selected WAN connection protocol

**Connection:** The current connection status.

**IP Address:** WAN port IP address.

**Default Gateway:** The IP address of the default gateway.

**LAN**

**IP Address:** LAN port IPv4 address.

**Subnet Mask/PREFIX Length:** Display LAN port IP subnet mask of IPv4 and/or Prefix length of IPv6.

**DHCP Server:** Display LAN DHCP status of IPv4 and IPv6.
- **Enable / 192.168.1.100~199**: DHCPv4 server status on or off / DHCP IP range
- **Enable / Statless**: DHCPv6 server status on or off / DHCPv6 server Type

**System Log**

In system log, you can check the operations status and any glitches to the router.

[system log screenshot]

**Refresh**: Press this button to refresh the statistics.
3G/4G-LTE Status

This page contains 3G/4G-LTE connection information.

**Status:** The current status of the 3G/4G-LTE connection.

**Signal Strength:** The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G-LTE Signal Strength LED indicates the signal strength as well.

**Signal Information:** Shows important LTE signal parameters such as RSRP (Reference Signal Receiving Power), RSRQ (Reference Signal Receiving Quality), SINR (Signal to Interference plus Noise Ratio).

- **RSRP (Reference Signal Receiving Power):** is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.
- **RSRQ (Reference Signal Receiving Quality):** measures the signal strength and is calculated based on both RSRP and RSSI.
- **RSSI (Received Signal Strength Indicator):** parameter which provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise. Please refer to the [Hardware/Front LED Indicators](#) for details.
- **SINR (Signal to Interference plus Noise Ratio):** is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput.

**NOTE:** Some LTE modules do not provide this information.

**Network Name:** The name of the LTE network the router is connecting to.

**Cell ID:** The ID of base station that the device is connected to.

**Card IMEI:** The unique identification number that is used to identify the 3G/4G-LTE module.

**Card IMSI:** The international mobile subscriber identity used to uniquely identify the 3G/4G-LTE module.

**Network Mode:** Show the using network mode.

**Network Band:** Show the using network band.

**Refresh:** Press this button to refresh the statistics.
Statistics

Take 3G/4G-LTE as an example to describe the following connection transmission information.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3G/4G-LTE</strong></td>
<td>List all available network interfaces in the router. You are currently checking on the physical status of 3G/4G-LTE interface.</td>
</tr>
<tr>
<td><strong>Transmit Frames of Current Connection</strong></td>
<td>This field displays the total number of 3G/4G-LTE frames transmitted until the latest second for the current connection.</td>
</tr>
<tr>
<td><strong>Transmit Bytes of Current Connection</strong></td>
<td>This field shows the total bytes transmitted till the latest second for the current connection.</td>
</tr>
<tr>
<td><strong>Transmit Total Frames</strong></td>
<td>The field displays the total number of frames transmitted till the latest second since system is up.</td>
</tr>
<tr>
<td><strong>Transmit Total Bytes</strong></td>
<td>This field displays the total number of bytes transmitted until the latest second since system is up.</td>
</tr>
<tr>
<td><strong>Receive Frames of Current Connection</strong></td>
<td>This field displays the number of frames received until the latest second for the current connection.</td>
</tr>
<tr>
<td><strong>Receive Bytes of Current Connection</strong></td>
<td>This field shows the total bytes received till the latest second for the current connection.</td>
</tr>
<tr>
<td><strong>Receive Total Frames</strong></td>
<td>This field displays the total number of frames received until the latest second since system is up.</td>
</tr>
<tr>
<td><strong>Receive Total Bytes</strong></td>
<td>This field displays the total frames received till the latest second since system is up.</td>
</tr>
</tbody>
</table>
## Ethernet

### Statistics

#### Traffic Statistics

**Interface:** List all available network interfaces in the router. You are currently checking on the physical status of the **Ethernet** port.

**Transmit Frames:** This field displays the number of frames transmitted until the latest second.

**Transmit Multicast Frames:** This field displays the number of multicast frames transmitted until the latest second.

**Transmit Total Bytes:** This field displays the number of bytes transmitted until the latest second.

**Transmit Collision:** This is the number of collisions on this port.

**Transmit Error Frames:** This field displays the number of error packets on this port.

#### Receive Statistics

**Receive Frames:** This field displays the number of frames received until the latest second.

**Receive Multicast Frames:** This field displays the number of multicast frames received until the latest second.

**Receive Total Bytes:** This field displays the number of bytes received until the latest second.

**Receive CRC Errors:** This field displays the number of error packets on this port.

**Receive Under-size Frames:** This field displays the number of under-size frames received until the latest second.

**Refresh:** Press this button to refresh the statistics.
DHCP Table

DHCP table displays the devices connected to the router with clear information.

<table>
<thead>
<tr>
<th>#</th>
<th>Host Name</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Expire Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>billion-17bc5f1</td>
<td>192.168.1.104</td>
<td>18:40:06:39:04:03</td>
<td>0 days 23:37:51</td>
</tr>
</tbody>
</table>

#: The index identifying the connected devices.

Host Name: Show the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

Expire Time: The total remaining interval since the IP assignment to the PC.
Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup time zone and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

For detailed instructions on configuring WAN settings, see refer to the Interface Setup section.

Click NEXT to move on to Step 1.

Step 1 – Password

Set new password of the “admin” account to access for router management. The default is “admin”. Once changed, please use this new password next time when accessing to the router. Click NEXT to continue.

Step 2 – Time Zone

Choose your time zone. Click NEXT to continue.
Step 3 – ISP Connection Type
Set up your 3G/4G-LTE Internet connection.

3.1 Click **NEXT** to continue.

3.2 Input all relevant 3G/4G-LTE parameters from your ISP.

3.3 Click **Next** to save changes.

Step 4 – Quick Start Completed
The Setup Wizard has completed. Click on BACK to make changes or correct mistakes. Click **NEXT** to save the current settings.

Go back to the **Status > Device Info** to view the status.
**Configuration**

Click to access and configure the available features in the following: **Interface Setup, Advanced Setup, Access Management**, and **Maintenance**.

These functions are described in the following sections.

**Interface Setup**

Here are the features under **Interface Setup: Internet** and **LAN**.
### Internet

#### 3G/4G-LTE

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Interface</td>
<td>3G/4G-LTE</td>
</tr>
<tr>
<td>Status</td>
<td>Activated</td>
</tr>
<tr>
<td>Network Mode</td>
<td>Automatic</td>
</tr>
<tr>
<td>TEL No.</td>
<td>Automatic</td>
</tr>
<tr>
<td>Dual APN</td>
<td>Single APN</td>
</tr>
<tr>
<td>APN</td>
<td>internet</td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td></td>
</tr>
<tr>
<td>Connection</td>
<td>Always On</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>Yes</td>
</tr>
<tr>
<td>Default Route</td>
<td>Yes</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable</td>
</tr>
</tbody>
</table>

**WAN Interface**: List all available WAN interfaces.

**Status**: Choose Activated to enable the 3G/4G-LTE connection.

**Network Mode**: There are 8 options of service standards: “Automatic”, “UMTS 3G only”, “GSM 2G Only”, “UMTS 3G Preferred”, “GSM 2G Preferred”, “GSM and UMTS Only”, “LTE Only”, “GSM, UMTS, LTE”. If you are not sure which mode to use, you may select **Automatic** to auto detect the best mode for you.

**TEL No.**: The dial string to make a GPRS / 3G/4G-LTE user internetworking call. It may provide by your mobile service provider.

**Dual APN**: RidgeWave 6900 can support up to two (2) APNs. Select Single or Dual.

**APN**: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is “internet”.

**Username/Password**: Enter the username and password provided by your service provider. The username and password are case sensitive.

**PIN**: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

**Connection**: Default set to Always on to keep an always-on 3G/4G-LTE connection.

**Keep Alive**: Select **Yes** to keep the 3G/4G-LTE connection always on.

**Default Route**: Select **Yes** to use this interface as default route interface.
**NAT:** Select this option to Disabled/Enable the NAT (Network Address Translation) function. Enable NAT to grant multiples devices in LAN to access to the Internet through a single WAN IP.

When router’s Internet configuration is finished successfully, you can go to the Status to check connection information.
LAN

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

IPv4 Parameters

**IP Address**: Enter the IP address of Router in dotted decimal notation, for example, 192.168.1.254 (factory default).

**IP Subnet Mask**: The default is 255.255.255.0. User can change it to other such as 255.255.255.128.

**Alias IP Address**: This is for local networks virtual IP interface. Specify an IP address on this virtual interface.

**Alias IP Subnet Mask**: Specify a subnet mask on this virtual interface.

**IGMP Snooping**: Select Activated to enable IGMP Snooping function, Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

**Dynamic Route**: Select the RIP version from RIP1 or RIP2.

DHCPv4 Server

DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a server.
DHCPv4 Server: If set to Enabled, your RidgeWave 6900 can assign IP addresses, default gateway and DNS servers to the DHCP client.

- If set to Disabled, the DHCP server will be disabled.
- If set to Relay, the RIDGEWAVE RidgeWave 6900 acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
- When DHCP is used, the following items need to be set.

Start IP: This field specifies the first of the contiguous addresses in the IP address pool.

IP Pool Count: This field specifies the count of the IP address pool.

Lease Time: The current lease time of client.

DNS Relay: Select Automatically obtained or Manually set. If select Manually, please specific DNS IP addresses information.

Primary / Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Fixed Host

In this field, users can map the specific IP (must in the DHCP IP pool) for some specific MAC, and this information can be listed in the following table.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
</table>

IP Address: Enter the specific IP. For example: 192.168.1.110.

MAC Address: Enter the responding MAC. For example: 00:0A:F7:45:6D:ED

When added, you can see the ones listed as showed below:

<table>
<thead>
<tr>
<th>Index</th>
<th>IP</th>
<th>MAC Address</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.110</td>
<td>23:24:5B:4B:22:33</td>
<td>X</td>
</tr>
</tbody>
</table>

IPv6 parameters

The IPv6 address composes of two parts, thus, the prefix and the interface ID.
**Interface Address / Prefix Length:** Enter a static LAN IPv6 address. If you are not sure what to do with this field, please leave it empty as if contains false information it could result in LAN devices not being able to access other IPv6 device. Router will take the same WAN's prefix to LAN side if the field is empty.

**DHCPv6 Server**

There are two methods to dynamically configure IPv6 address on hosts, **Stateless** and **Stateful**.

**Stateless auto-configuration** requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn’t configure anything on the client.

**Stateful configuration,** for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

**DHCPv6 Server:** Check whether to enable DHCPv6 server.

**DHCPv6 Server Type:** Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available.

- **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server.

- **Stateful:** If selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

**Start interface ID:** enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

**End interface ID:** enter the end interface ID.

**Leased Time (seconds):** the leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

**Router Advertisement:** Check to Enable or Disable the Issue Router Advertisement feature. This feature is to send Router Advertisement messages periodically which would multicast the IPv6 Prefix
information (similar to v4 network number 192.168.1.0) to all LAN devices if the field is enabled. We suggest enabling this field.
Advanced Setup


**Firewall**

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.

**Firewall**: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

- **Enabled**: It activates your firewall function.
- **Disabled**: It disables the firewall function.

**SPI**: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- **Enabled**: It activates your SPI function.
- **Disabled**: It disables the SPI function.
Routing

This is static route feature. You are equipped with the capability to control the routing of all the traffic across your network. With each routing rule created, user can specifically assign the destination where the traffic will be routed to.

### Configuration

<table>
<thead>
<tr>
<th>#</th>
<th>Destination IP Address</th>
<th>Subnet Mask</th>
<th>Gateway IP Address</th>
<th>Metric</th>
<th>Interface</th>
<th>Edit</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>192.168.1.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>br0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>172.16.1.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>nas10_0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>127.0.0.0</td>
<td>255.255.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>lo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>239.0.0.0</td>
<td>255.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>br0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>239.0.0.0</td>
<td>255.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>eth0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>172.16.1.254</td>
<td>0</td>
<td>nas10_0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **#:** Item number
- **Destination IP Address:** IP address of the destination network
- **Subnet Mask:** The subnet mask of destination network.
- **Gateway IP Address:** IP address of the gateway or existing interface that this route uses.
- **Metric:** It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.
- **Interface:** Media/channel selected to append the route.
- **Edit:** Edit the route; this icon is not shown for system default route.
- **Drop:** Drop the route; this icon is not shown for system default route.

### Add Route

**Destination IP Address:** This is the destination subnet IP address.

**Destination Subnet Mask:** The subnet mask of destination network.

**Gateway IP Address/Interface:** This is the gateway IP address or existing interface to which packets are to be forwarded.

**Metric:** It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.
NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

In this session, there are “VPN Passthrough”, “SIP ALG”, “DMZ” and “Virtual Server” provided to solve these nasty problems.

**NAT Status:** Enabled. It depends on ISP Connection Type in Internet settings.

**VPN Passthrough:** VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

**SIP ALG:** Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP ALG when SIP phone includes NAT-Traversal algorithm.

**Interface:** Select a WAN interface connection to allow external access to your internal network.

**Service Index:** Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

Click **DMZ** or **Virtual Server** to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.
**DMZ**

*NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.*

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

**DMZ for (3G/4G-LTE WAN Interface):** Allows outside network to connect in and communicate with internal LAN devices.

**DMZ:**
- **Enabled:** It activates your DMZ function.
- **Disabled:** It disables the DMZ function.

**DMZ Host IP Address:** Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Select the **Save** button to apply your changes.
Virtual Server

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.

In TCP/IP networks, a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the WAN configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

Virtual Server for: 3G/4G-LTE WAN interface allows outside network to connect in and communicate with internal LAN devices.

Protocol: Choose the application protocol.

Start / End Port Number: Enter a port or port range you want to forward.

(Example: Start / End: 1000 or Start: 1000, End: 2000). The starting port must be greater than zero (0). The end port must be greater than or equal to the start port.
Local IP Address: Enter your server IP address in this field.

Start / End Port Number (Local): Enter the start / end port number of the local application (service).

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at http://www.iana.org/assignments/port-numbers

### Well-known and Registered Ports

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>TCP</td>
<td>FTP Control</td>
</tr>
<tr>
<td>22</td>
<td>TCP &amp; UDP</td>
<td>SSH Remote Login Protocol</td>
</tr>
<tr>
<td>23</td>
<td>TCP</td>
<td>Telnet</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>SMTP (Simple Mail Transfer Protocol)</td>
</tr>
<tr>
<td>53</td>
<td>TCP &amp; UDP</td>
<td>DNS (Domain Name Server)</td>
</tr>
<tr>
<td>69</td>
<td>UDP</td>
<td>TFTP (Trivial File Transfer Protocol)</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>World Wide Web HTTP</td>
</tr>
<tr>
<td>110</td>
<td>TCP</td>
<td>POP3 (Post Office Protocol Version 3)</td>
</tr>
<tr>
<td>443</td>
<td>TCP &amp; UDP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>1503</td>
<td>TCP</td>
<td>T.120</td>
</tr>
<tr>
<td>1720</td>
<td>TCP</td>
<td>H.323</td>
</tr>
<tr>
<td>7070</td>
<td>UDP</td>
<td>RealAudio</td>
</tr>
</tbody>
</table>

**NOTE:**

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

**Attention**

If you have disabled the NAT option in the WAN-ISPF section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.
Example: How to setup Port Forwarding for port 21 (FTP server)
If you have a FTP server in your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway and go to Configuration / Advanced Setup / NAT / Virtual Server. FTP server uses TCP protocol with port 21.
Enter "21" to Start and End Port Number. The RidgeWave 6900 will accept port 21 requests from WAN side.
Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.1.102
Enter "21" to Local Start and End Port number. The RidgeWave 6900 will forward port 21 request from WAN to the specific LAN PC (ex:192.168.1.102) in the network.

Step 3: Click Save to save settings.
Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com can be translated into the addresses 192.0.32.10 (IPv4).

Static DNS is a concept relative to Dynamic DNS, in static DNS system, the IP mapped is static without change.

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>The IP address you are going to give a specific domain name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name:</td>
<td>The friendly domain name for the IP address.</td>
</tr>
</tbody>
</table>

Press **Save** button to apply your settings.
**Time Schedule**

The Time Schedule supports up to 16 timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications. This Time Schedule correlates closely with router’s time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.

<table>
<thead>
<tr>
<th>Rule Index</th>
<th>TimeSlot1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>00:00</td>
</tr>
<tr>
<td>End Time</td>
<td>00:00</td>
</tr>
</tbody>
</table>

**Time Index:** The rule index (0-15) for identifying each timeslot.

**Name:** User-defined identification for each time period.

**Day of Week:** Mon. to Sun. Specify the time interval for each timeslot from “Day of Week”. For example, user can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.

<table>
<thead>
<tr>
<th>Rule Index</th>
<th>TimeSlot1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>06:00</td>
</tr>
<tr>
<td>End Time</td>
<td>24:00</td>
</tr>
</tbody>
</table>

Another TimeSlot2 spanning from 09:00 to 18:00 of Friday

<table>
<thead>
<tr>
<th>Rule Index</th>
<th>TimeSlot2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>00:00</td>
</tr>
<tr>
<td>End Time</td>
<td>09:00</td>
</tr>
</tbody>
</table>
**Remote System Log**

- **Remote System Log**: Select **Activated** to enable this feature.
- **Server IP Address**: Assign the remote log server IP address.
- **Server UDP Port**: Assign the remote log server port, 514 is commonly used.

Press **Save** button to apply your settings.
Access Management

Access Management provides advanced users / administrators to grant accessibilities to authorized users or service systems. Features including Device Management, SNMP, Universal Plug & Play, Dynamic DNS, Access Control, Packet Filter, CWMP(TR-069), and Parental Control.

Device Management

Device management offers users a way to change the embedded web server accessing port, default 80. User can change the http port to 8080 or something else here.
SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. The RidgeWave 6900 serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.

SNMP: Select to enable SNMP feature.

Get Community: Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Trap Manager IP: Enter the IP of the server receiving the trap message (when some exception occurs) sent by this SNMP agent.

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Authentication Key: Set the authentication key, 8-31 characters.

Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.
Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user’s Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

**UPnP:** Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration’s login screen without entering the RidgeWave 6900’s IP address

**Auto-configured:** Select this check box to allow UPnP-enabled applications to automatically configure the RidgeWave 6900 so that they can communicate through the RidgeWave 6900, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es). But note that first users have to go to the Dynamic DNS registration service provider to register an account.

**Dynamic DNS:** Select this check box to activate Dynamic DNS.

**Service Provider:** Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

**My Host Name:** Type the domain name assigned to your RidgeWave 6900 by your Dynamic DNS provider.

**Username:** Type your user name.

**Password:** Type the password.

**Wildcard support:** Select this check box to enable DYNDNS Wildcard.

**Period:** Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.
Example: How to register a DDNS account

Note first users have to go to the Dynamic DNS registration service provider to register an account.


DDNS: [www.hometest.com](http://www.hometest.com) using username/password test/test
Access Control

Access Control Listing allows you to determine which services/protocols can access the RidgeWave 6900 interface from which computers. It is a management tool aimed to allow IPs (set in secure IP address) to access specified embedded applications (Web, etc, user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is 16.

Access Control: Select whether to make Access Control function available.

Rule Index: This is item number

Active: Select to activate the rule.

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the RidgeWave 6900. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are LAN, WAN and Both.
By default, the “Access Control” has **two default rules**.

**Default Rule 1**: (Index 1), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc). Under this situation, clients from WAN cannot access the router even from Ping.

**Default Rule 2**: (Index 2), an ACL rule to open Ping to WAN side.
Packet Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

Packet Filter - IP & MAC Filter

Filter Type: There are three types “IP & MAC Filter”, “Application Filter”, and “URL Filter” that user can select for this filter rule. Here we set IP & MAC Filter.

IP & MAC Filter Editing

Rule Index: This is item number

Individual Active: Select Yes to activate the rule.

Action: This is how to deal with the packets matching the rule. Allow please select White List or block selecting Black List.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select “IPv4” for IPv4 address, port number and protocol. Select “IPv6” for IPv6 address, port number and protocol. Select “MAC” for MAC address.

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Source Subnet Mask: Enter the subnet mask of the source network.
Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.
Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.
Destination Subnet Mask: Enter the subnet mask of the destination network.
Destination Port Number: This is the Port that defines the application. (e.g. HTTP is port 80.)
DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)
Protocol: Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

IP/MAC Filter Listing

#: Item number.
Active: Whether the connection is currently active.
Interface: show the interface the rule applied to.
Direction: show the direction the rule applied to.
Source IP (IPv6) Address/Mask (Prefix): The source IP address or range of packets to be monitored.
Destination IP (IPv6) Address/Mask (Prefix): This is the destination subnet IP address.
Source MAC Address: show the MAC address of the rule applied.
Source Port: The source port number of packets to be monitored.
Destination Port: This is the Port or Port Ranges that defines the application.
DSCP: show the set DSCP.
Protocol: It is the packet protocol type used by the application. Select either TCP or UDP or ICMP or ICMPv6.
Packet Filter - Application Filter

Application Filter: Select this option to Activated/Deactivated the Application filter.

ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video (RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

Packet Filter - URL Filter

URL Filter: Select Activated to enable URL Filter.

URL Filter Rule Index: This is item number.

Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL (Host): Specified URL which is prohibited from accessing.
CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones). At the same time the configuration of this equipment became more complicated – too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.

![Configuration](image)

**CWMP**: Select activated to enable CWMP.

**ACS Login Information**

**URL**: Enter the ACS server login URL.

**User Name**: Specify the ACS User Name for ACS authentication to the connection from CPE.

**Password**: Enter the ACS server login password.

**Connection Request Information**

**Path**: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

**Username**: Username used to authenticate an ACS making a Connection Request to the CPE.

**Password**: Password used to authenticate an ACS making a Connection Request to the CPE.
**Periodic Inform Config**

**Periodic Inform:** Select Activated to authorize the router to send an Inform message to the ACS automatically.

**Interval(s):** Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

**NATT Config** - This is a proprietary feature provided by BEC. May leave them in blank, no configuration is required.

**NATT Server:** By BEC adminstorator only.

**NATT Period:** By BEC adminstorator only.
Parental Control

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.

To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

**Parent Control Provider:** Hosted by www.opendns.com

**Parent Control:** Enable the feature by clicking the Activated

**Host Name:** It is the domain name of your OpenDNS. If you don’t have one, please leave it blink.

**Username / Password:** Put down your OpenDNS account username and password
Maintenance

Maintenance equipments the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including User Management, Time Zone, Firmware & Configuration, System Restart, and Diagnostic Tool.

User Management

User Management controls the Router Web GUI permission to the specific account.

In factory setting, the default accounts are admin/admin and user/user. The default root account admin has been authorized to web access of router. The user/user is equipment with limited access (specified by advanced users with admin account) to router web GUI. Total of 8 accounts can be created to grant access to manage the RidgeWave 6900 via the web page.

- Admin / Admin

admin/admin is the root account provided by our router.

User Setup

Index: User account index, total is 8.

User Name: Create account(s) user name for GUI management.

New Password: Enter a new password for this user account.

Confirmed Password: Re-enter the new password again; you must enter the password exactly the same as in the previous field
Time Zone

With default, RidgeWave 6900 does not contain the correct local time and date. There are several options to setup, maintain, configure current local time/date on the RidgeWave 6900. If you plan to use Time Schedule feature, it is extremely important you set up the Time Zone correctly.

Synchronize time with: Select the methods to synchronize the time.

- **NTP Server automatically**: To synchronize time with the SNTP servers to get the current time from an SNTP server outside your network then choose your local time zone. After a successful connection to the Internet, RidgeWave 6900 will retrieve the correct local time from the SNTP server this is specified.
- **PC’s Clock**: To synchronize time with the PC’s clock.
- **Manually**: Select this to enter the SNTP server IP address manually.

**Time Zone**: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

**Daylight Saving**: Select this option if you use daylight savings time.

**NTP Server Address**: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your RidgeWave 6900 provides an easy way to update the code to take advantage of the changes.

To upgrade the firmware of the RidgeWave 6900, you should download or copy the firmware to your local environment first. Press the “Browse...” button to specify the path of the firmware file. Then, click “Upgrade” to start upgrading. When the procedure is completed, the RidgeWave 6900 will reset automatically to make the new firmware work.

- **Upgrade**: Choose Firmware or Configuration you want to update.
- **System Restart with**:
  - **Current Settings**: Restart the device with the current settings automatically when finishing upgrading.
  - **Factory Default Settings**: Restart the device with factory default settings automatically when finishing upgrading.
- **File**: Type in the location of the file you want to upload in this field or click **Browse** to find it.
- **Browse**: Click **Browse...** to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.
- **Backup Configuration**: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your RidgeWave 6900 device when making false configurations and want to restore to the original settings.

Do you want to open or save romfile.cfg (35.8 KB) from 192.168.1.254?  
Open  Save  Cancel

**UPGRADE**: Click **UPGRADE** to begin the upload process. This process may take up to two minutes.
DO NOT turn off / power off the device or interrupt the firmware upgrading while it is still in process. Improper operation could damage your RidgeWave 6900.
System Restart

Click **System Restart** with option **Current Settings** to reboot your router.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to restore to factory default settings.

You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.
Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

**3G/4G-LTE**

Click START to begin to diagnose the connection.
Chapter 5: Troubleshooting

If your RIDGEWAVE RidgeWave 6900 is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>None of the LEDs is on when you turn on the router</td>
<td>Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.</td>
</tr>
<tr>
<td>You have forgotten your login username or password</td>
<td>Try the default username &quot;admin&quot; and password &quot;admin&quot;. If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.</td>
</tr>
</tbody>
</table>

Problem with LAN Interface

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot PING any PC on LAN</td>
<td>Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting. Verify that the IP address and the subnet mask are consistent for both the router and the workstations.</td>
</tr>
</tbody>
</table>
## Recovery Procedures

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>- The front LEDs display incorrectly</td>
<td>1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately.</td>
</tr>
<tr>
<td>- Still cannot access to the router management interface after pressing the RESET button.</td>
<td>2. The router’s emergency-reflash web interface will then be accessible via <a href="http://192.168.1.1">http://192.168.1.1</a> where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.</td>
</tr>
<tr>
<td>- Software / Firmware upgrade failure</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems please contact the dealer from where you have purchased the product.

Contact BEC @ http://www.bectechnologies.net

MAC OS is a registered Trademark of Apple Computer, Inc.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

• Reorient or relocate the receiving antenna.
• Increase the separation between the equipment and receiver.
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
• Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference
(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement
This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.